ExtremeCloud SD-WAN Orchestrator

User Guide

Release 22.3.1

Updated: 26 October 2022

www.extremenetworks.com

Contents

1 SD-WAN Orchestrator overview

This section helps you understand the ExtremeCloud SD-WAN Orchestrator concepts. It contains an overview of the provided services and introduces the basic components of the product.

Presentation

As a Service in the Cloud, ExtremeCloud SD-WAN Orchestrator enables you to easily configure network appliances and manage the applications over the network.

Each defined Customer corresponds to a set of physical appliances positioned at the measurement or control points of a network. The appliances build the connections between the sites and when routing the traffic, they also control, compress and accelerate it on the entire network.

In this documentation, Use Case 1 and Use Case 2 illustrate a simple network where the connections of three sites are done through/over the MPLS, or over the Internet, or both.

- Use Case 1 architecture corresponds to a hybrid mode network (with at least one bridge appliance, one bridge/router appliance and one full router appliance).
- Use Case 2 corresponds to a full router mode network (all appliances are deployed in router mode).Both Use Cases are used to describe the configuration procedure required by the Orchestrator to build the underlay and overlay network of site connections.

SD-WAN Orchestrator management includes the following features:

- Application Visibility to understand application usage and performance over the entire network. The system provides clear application performance KPIs, high level consolidated reports, and very detailed information at the flow level.
- Application Control to guarantee user experience by controlling each application flow in real-time, depending on the network resources.
- WAN Optimization to accelerate delay sensitive applications and reduce bandwidth consumption.
- Dynamic WAN Selection to guarantee application performance across hybrid [MPLS + Internet] networks, improve business communication continuity, exploit large network capacity at low cost, benefit from Internet immediacy and ubiquity, eliminate complex policy based routing and unify the management of hybrid networks. The system automatically and dynamically selects the best path for each application flow across the various networks.
- Management of the network devices (in bridge, full router or hybrid mode) to configure the connections between the sites and route the applications over the network.

Description of Services

This section introduces the features automatically provided with your SD-WAN appliances.

- "Application Visibility"
- "Application Control"
- "WAN Optimization"
- "Dynamic WAN Selection"
- "Network Management"

Application Visibility

The primary goal of Application Visibility is to understand application usage and performance over the entire network.

To reach that goal, applications are classified in Application Groups (AGs), and each AG has specific QoS performance objectives (nominal bandwidth per session and two thresholds, maximum for one-way-delay, jitter, packet loss, RTT, SRT and TCP retransmission ratio), thus allowing to check whether performance objectives are met or not, and to calculate an Experience Quality Score (EQS) accordingly.

Application Visibility is:

- comprehensive (see the list of metrics below),
- highly accurate, relying on time synchronization from the network,
- very precise and non-intrusive: measurements are made on the actual data packets and not on test packets nor simulated flows,
- exhaustive: ***all*** IP packets are measured,
- independent from the operator network access and core technology (measurements are made at the IP layer level),
- confidential: the contents of user packets are not, at any time, stored, saved or even transmitted between the different system components.

Application Visibility provides the following metrics:

- the number of packets and bytes transmitted and received,
- the number of sessions,
- the following one-way metrics:
  - Delay,
  - Jitter,

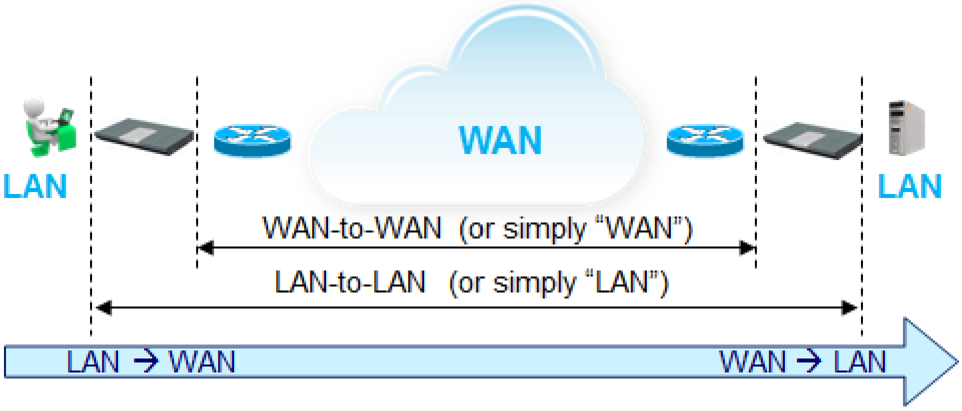
  - Packet Loss,

  all three (called D/J/L) in both:

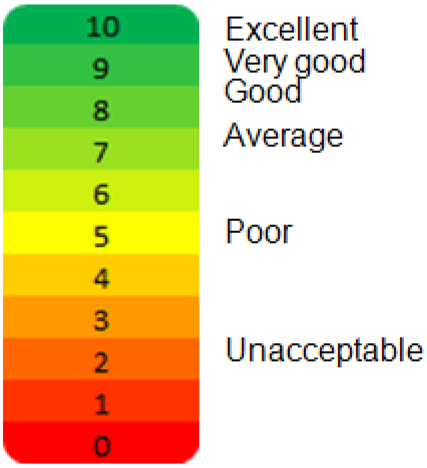
  - ingress (from the LAN to the WAN) and
  - egress (from the WAN to the LAN),

  both:

  - between the LAN interfaces of the appliances (LAN-to-LAN metrics, simply called LAN) and
  - between their WAN interfaces (WAN-to-WAN metrics, simply called WAN):



- the following TCP metrics:
  - RTT (Round Trip Time),
  - SRT (Server Response Time),
  - TCP retransmission ratio,
- the following composite metrics:
  - Voice MOS (Mean Opinion Score),
  - all flow EQS (Experience Quality Score).



Individual measurements are aggregated and analyzed according to multiple criteria (source and destination sites, source and destination subnets, Application Groups, applications, etc.). The results are presented in the form of detailed flows lists, real-time graphs, charts, etc., and archived with periodic aggregations. They are made available for subsequent processing or reference, and can be used to generate alarms, analyze long-term trends, forecast future traffic increase to estimate optimum network sizing, etc.

Users can specify their own aggregation criteria, thus taking into account their enterprise organization (e.g. the different countries, departments, services, etc.).

Time Synchronization

Appliance synchronization for the Client is used for correlation, hence for Delay/Jitter/Loss measurement.

Monitoring

The Monitoring dashboard function provides a real-time view of the performance and activity of the observed traffic through graphs.

Application Control

End-to-end QoS depends on both network infrastructures (transmission lines, access lines, traffic engineering policies) and user traffic.

Network bottlenecks result in congestions and may limit optimum bandwidth to well below its rated value. Transmitting more traffic will only result in increased transfer time and loss, thereby degrading QoS and application "goodput".

The goal of the Application Control feature is to anticipate and avoid congestions, and to guarantee the users' experience by adjusting each application flow in real-time.

To reach that goal, Application Group attributes include:

- the business criticality of the application flow (top, high, medium or low)
- the bandwidth objective (bandwidth requirements of the application flow, necessary and sufficient to provide it with good quality)
- the traffic type (real time, transactional or background)
- compression capabilities

thus allowing the controlling agent to protect the business critical flows dynamically and efficiently, also taking into account the demand in real time.

> **Note:** There is no need to set low-level network or device-specific policy rules.

Using these parameters provides the following information:

- business criticality: the higher the criticality of the flow, the more it will be protected
- bandwidth objective: bandwidth that the system will try to provide to the application flow, even when the available bandwidth is scarce; the higher the criticality of the flow, the more likely its bandwidth objective will be met at all times
- traffic type: priorities between the different queues depending on the sensitivities of the flows to avoid Delay and Jitter, knowing that:
    - real time flows are sensitive to Delay **and** Jitter; examples: VoIP and Video conference
    - transactional flows are sensitive to Delay (but not to Jitter); examples: Telnet, Citrix
    - background flows are not sensitive at all; examples: file transfer, e-mail
- compression capabilities: to know whether the flow can be compressed

Congestion anticipation and avoidance is performed by comparing the available bandwidth (or network capacity) and the bandwidth used by all the flows currently running (network usage).

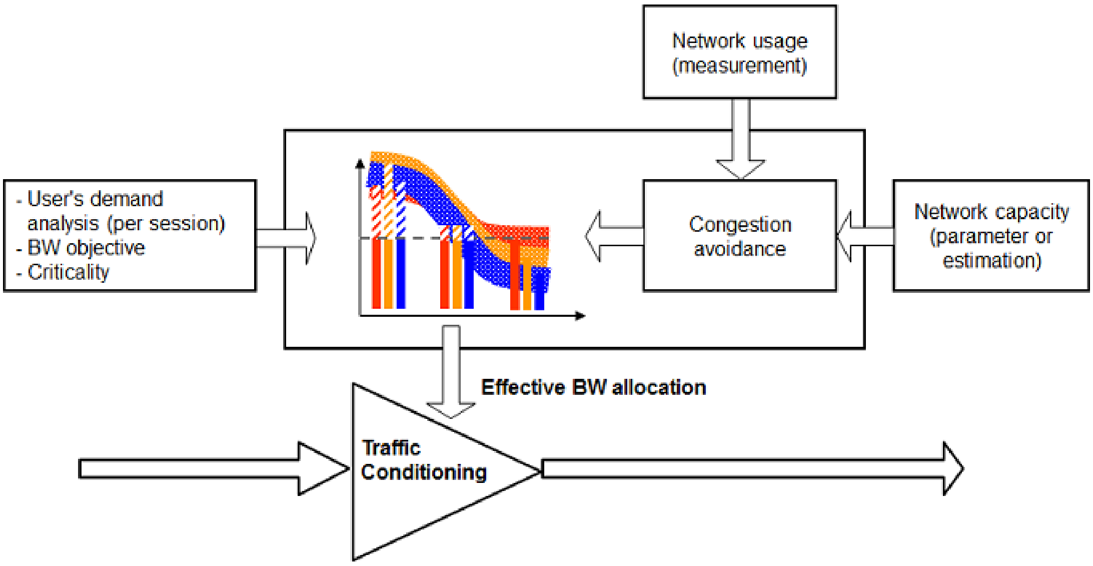
The comparison is performed on the access links, ingress and egress, and possibly end-to-end (namely if the available bandwidth between any pair of sites is not fix and guaranteed).

- If the network usage reaches about 95% of the network capacity, then Application Control triggers and starts controlling the bandwidth allocation.
- The network usage is known very precisely, thanks to Application Visibility which measures every packet crossing the SD-WAN Appliances.
- The network capacity is:
    - either fix (and defined in the WAN access parameters),
    - or (if it varies) automatically and dynamically estimated by the Tracking function.

      The Tracking function is activated in the appliance WAN configuration window (see "Configuring the WAN(s)"), where up and down throughput values are defined for access bandwidth:

      If the down throughput is less than the up throughput, then the Tracking function instantaneously estimates the bandwidth, at any moment, between these two thresholds.

      The Tracking function also anticipates and avoids end-to-end congestions.


Network usage (measurement)
- User's demand analysis (per session)
- BW objective
- Criticality
Congestion avoidance
Network capacity (parameter or estimation)
Effective BW allocation
Traffic Conditioning

Application Control can be summarized as follows:

- it globally and dynamically controls bandwidth allocation between all access points
- it adapts QoS policies to the current network performance and real user demand
- it selects, for each traffic flow, the right Class of Service in terms of performance

based on:

- the traffic requirements (criticality, bandwidth objectives)
- the bandwidth demand
- the network performance

WAN Optimization

End-to-end quality of application flows depends on the capacity of the links and on the end-to-end delays. WAN Optimization, that leverages the Application Control feature, helps improving quality by accelerating delay sensitive applications and by reducing bandwidth consumption.

Compression

For many reasons, it can be difficult to increase the bandwidth of a link (cost, operator delay, etc.). Compression overcomes this problem, by increasing the volume of traffic that can be sent on the network. To achieve that goal, compression is used: it is a transparent mechanism that uses a TCP proxy and stores the redundant patterns, at the stream level, on the appliances and exchanges small signatures instead, thus reducing bandwidth consumption.

It is particularly efficient to compress big flows such as large file transfers, for instance.

Compression also accelerates TCP, by using window scaling (RFC 1323) between the two proxies.

Dynamic WAN Selection

The goal of Dynamic WAN Selection (DWS) is to combine multiple physical networks (hybrid networks, e.g. MPLS and Internet) into one unified logical network, maximizing both Quality of Experience & business continuity.

To achieve that goal, this service:

- automatically and dynamically selects the best traffic path, according to Application Groups and WAN access configuration,
- the SD-WAN Appliance handles dynamic traffic conditioning according to the destination of the flows.

This maximizes application performance, security and network usage based on:

- network quality and availability
- application Performance SLAs
- user configured rules

Network Management

Network Management consists of building the underlay and overlay network of site connections and routing the traffic.

Refer to "Use Case 1" and "Use Case 2" which are typical configuration examples illustrating this Service.

Checking the Overview Dashboard information

When you log in to the SD-WAN Orchestrator, an **Overview dashboard** enables you to check your network at a glance.

Counters

The left pane of the dashboard displays the following counters for the whole network:

- number of network issues reported through Critical, Warning and Information alarms,
- the EQS for all Top, High, Medium and Low application flows for the Customer according to Quality Summary data of the Monitoring Views,
- traffic 1 minute average throughput and highest throughput; average number of flows against the highest number of flows,

The right pane of the dashboard displays the following counters for the whole network:

- configured appliances, unreachable appliances, not configured appliances and configured RVC destinations,
- configured hubs, unreachable hubs, configured spokes, unreachable spokes
- Site to Site supervised and broken tunnels
- supervised and broken connections to External Gateways
- supervised and broken cloud connections to AWS and Azure
- CloudMesh and EdgeSentry supervised and broken connections

Click the ⊞ Overview per Network button in the top right corner of the dashboard to display the same information as before for every transport network you have defined; use the **Network** filter and select any network from the list. Click ⊞ Overview to return to the dashboard for the whole network.

Drilling down on Alarm counters

Click any colored alarm counter to display detailed information about the current issues on the Active Alarms dashboard.

You can also access event history and tunnel status statistics by selecting the Supervision functions from the SD-WAN Orchestrator top menu.

The Supervision Toolbar

The Supervision toolbar is displayed at the left of the window. It contains several icons that enable you to access some functions.

☰ Click this icon to go back to the General Supervision/Overview default dashboard.

🔍 Click this icon to display the dashboard list and search for a dashboard by entering its name.

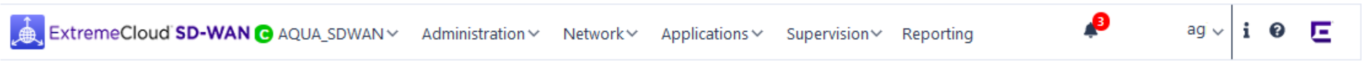
⊞ Click this icon to manage the dashboards and folders.

👤 Click this icon to access the Preferences parameters. You can select a dark or light UI Theme. Note that the other parameters can only be modified by your Administrator.

? Click this icon to access a list of keyboard shortcuts.

Using the Main Menu

Use the SD-WAN Orchestrator menu bar to access all the functions of the interface. Since this menu bar is displayed at the top of all the windows, you may easily navigate through your administration, configuration, monitoring, supervision and reporting pages.



AQUA_SDWAN	The first information after the Product Name corresponds to your Customer Name.
Administration	This menu gives access to the Users, Appliances, Licenses, Cloud Access and Settings windows.
Network	This menu gives access to Network Configuration, External Gateways, Zone-Based Firewall and Advanced Configuration windows.
Applications	This menu gives access to Application Configuration and Monitoring, and SSL Configuration windows.
Supervision	This menu gives access to Active Alarms, Event History, Overview, Tunnel Status and Notification Settings dashboards.
Reporting	This menu gives access to Reporting dashboards.
🔔3	Informs you of the number of active alarms. The color of this counter corresponds to alarm highest severity, i.e. if there is at least one critical alarm, the counter is red. Click this icon to display the Active Alarms dashboard containing detailed information about all the raised alarms.
ag	User Name
ℹ	Displays the SD-WAN Orchestrator version and the list of open source products used to create the SD-WAN Orchestrator with their respective licenses.
❓	Displays on-line help.
	Extreme Networks logo
ExtremeCloud SD-WAN	Click the product name to go back to the landing page from any other window of the interface.

Administration

This section describes the Customer administration functions of the SD-WAN Orchestrator.

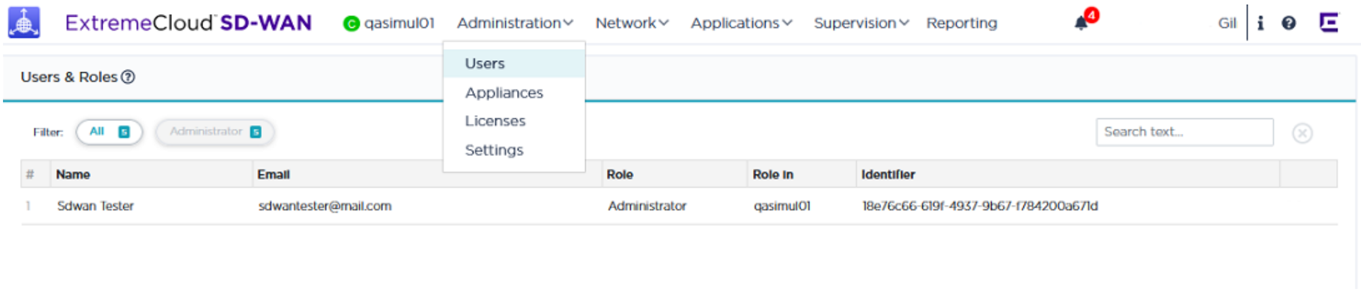
- "Viewing Users"
- "Viewing Appliances"
- "Viewing Licenses"
- "Managing Cloud Access"
- "Selecting the Reporting Mode"

Viewing Users

As the Administrator of a Customer account, you can view the users of this account. This function is not visible to user profiles with no administration roles.

> **Warning:** Creating, inviting and managing users is done in **ExtremeCloud IQ**. Refer to ExtremeCloud IQ documentation.

1 Select the **Administration -> Users** function from the SD-WAN Orchestrator main menu. The following image shows the number of Users defined for the Customer. You may filter them by Role by clicking any filter button.



#	Name	Email	Role	Role in	Identifier
1	Sdwan Tester	sdwantester@mail.com	Administrator	qasimul01	18e76c66-619f-4937-9b67-f784200a671d

The Search field also enables you to find any User through his other data. Click the ⊗ button to delete the Search filters.

When the window contains a significant number of Users, the navigation functions at the bottom of the window enable you to navigate through the list.

- By default, one page includes 50 rows. 20 and 100 are the other options.
- The total number of pages is specified. This number changes if you select a different number of rows per page.
- You can display a particular page by directly selecting it from the stack or by clicking the ‹ and › buttons to move from one page forward and backward.

- Click « to view the first page and » to view the last page of the list.

User Roles

A user is related to one Customer only. In **ExtremeCloud IQ**, several roles can be defined and assigned to a SD-WAN Orchestrator user.

Each role authorizes access to a specific list of operations in ExtremeCloud SD-WAN. A role determines the CRUD (Create, Read, Update, Delete) rights for each type of entity.

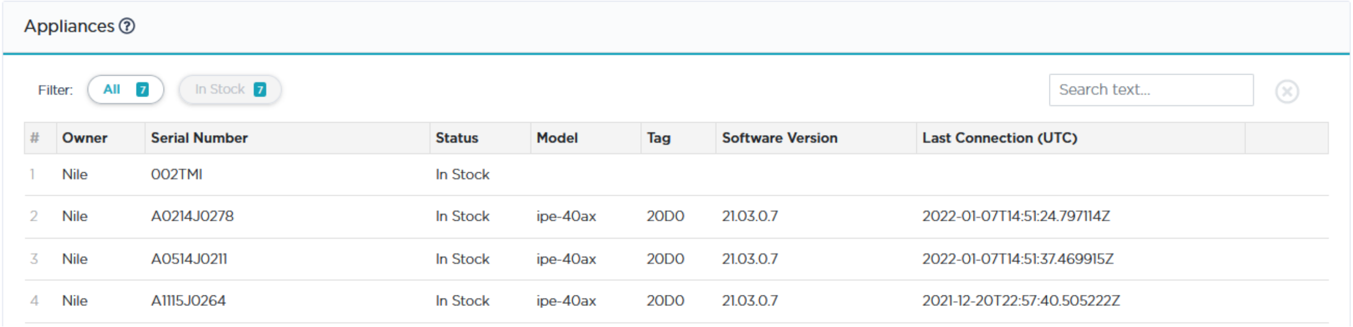
The table below lists the User Role rights for managing the SD-WAN Orchestrator entities.

Entity/User Role	Administrator	Operator (Domain Manager)	Monitor & Observer (Viewer)
Users	CRUD		R
Appliances	R	R	R
Licenses	R	R	R
Settings	CRUD		
Applications	CRUD	CRUD	R
Network	CRUD	CRUD	R
Reporting	R	R	R

Viewing Appliances

From the SD-WAN Orchestrator main menu, select the **Administration -> Appliances** function to view the assigned appliances.

The following image shows that three ip|e 40ax have been assigned to Customer 'Nile'. You may use the filters at the top of the window for exclusive display.



#	Owner	Serial Number	Status	Model	Tag	Software Version	Last Connection (UTC)
1	Nile	002TMI	In Stock				
2	Nile	A0214J0278	In Stock	ipe-40ax	20D0	21.03.0.7	2022-01-07T14:51:24.797114Z
3	Nile	A0514J0211	In Stock	ipe-40ax	20D0	21.03.0.7	2022-01-07T14:51:37.469915Z
4	Nile	A1115J0264	In Stock	ipe-40ax	20D0	21.03.0.7	2021-12-20T22:57:40.505222Z

Appliance Parameters

Owner

Customer name.

Serial Number

The Serial Number is made of 12 characters as follows: MmmyyEnnnnRr, where:

- M: Manufacturer initials
- mm: month of manufacture (01 to 12)
- yy: year of manufacture (18 for 2018)
- E: engine (appliance) type

W	ip|e 30so
X	ip|e 30ax
I	ip|e 40so
J	ip|e 40ax
U	ip|e 40so V2
V	ip|e 40ax V2
K	ip|e 400ax
A	ip|e 2000ax-T

B	ip|e 2000ax-Sx
C	ip|e 2000ax-Lx
D	ip|e 2000ax-10GSr
E	ip|e 2000ax-10GLr

- nnnn: serial n° (0001 to 9999)
- Rr: revision (R for major revision, r for minor revision): starting with A0

Example: `A0218X0001A0` corresponds to a Serial Number of the first ip|e 30ax manufactured by Aaeon on February 2018.

Status

An appliance is **In Stock** when available or **Assigned** when it has been assigned to the current Customer.

Model

Refer to the previous table of appliance types.

Tag

ZTP appliance tag code.

Software Version

Version of software services.

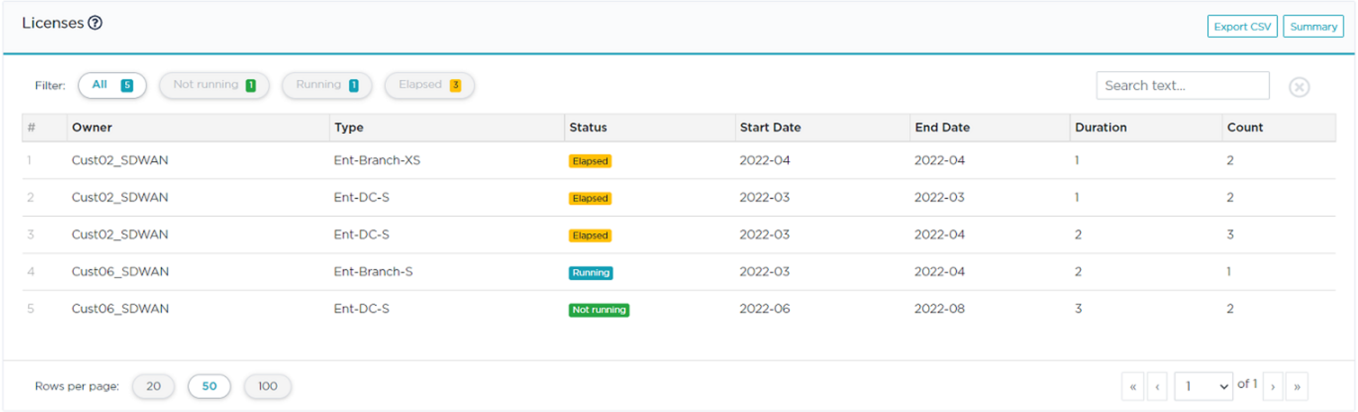
Last Connection (UTC)

Last time when the SD-WAN Orchestrator synchronized data with the ZTP Server.

Viewing Licenses

1. From the SD-WAN Orchestrator main menu, select the **Administration -> Licenses** function to view the assigned licenses.

   The following image example shows the number of licenses that have been assigned to two customers, 'Cust02_SDWAN' and 'Cust06_SDWAN'. They may be filtered by Type and Status (running, not running, elapsed). Simply click any filter button.



#	Owner	Type	Status	Start Date	End Date	Duration	Count
1	Cust02_SDWAN	Ent-Branch-XS	Elapsed	2022-04	2022-04	1	2
2	Cust02_SDWAN	Ent-DC-S	Elapsed	2022-03	2022-03	1	2
3	Cust02_SDWAN	Ent-DC-S	Elapsed	2022-03	2022-04	2	3
4	Cust06_SDWAN	Ent-Branch-S	Running	2022-03	2022-04	2	1
5	Cust06_SDWAN	Ent-DC-S	Not running	2022-06	2022-08	3	2

   The Search field also enables you to find any license through its other data (Owner). Click the ⊗ button to delete the Search filters.

   When the window contains a significant number of licenses, the navigation functions at the bottom of the window enable you to navigate through the list.

   - By default, one page includes 50 rows. 20 and 100 are the other options.
   - The total number of pages is specified. This number changes if you select a different number of rows per page.
   - You can display a particular page by directly selecting it from the stack or by clicking the ‹ and › buttons to move from one page forward and backward.
   - Click « to view the first page and » to view the last page of the list.

   For a description of columns, refer to "The Licensing Model".

2. Click the **Summary** button to display a quick overview of the running (started) licenses during the current month. They can have the following Status values:

   - Used: licenses used by an appliance
   - Not used: licenses not used by an appliance
   - Missing: license breaches

3. Click **Back** to return to the Licenses window.
4. Click **Export CSV** to export the data of the Licenses window as a `licenses.csv` file.

CSV Column Name	Field Name in the Licenses window
tenantId	Identifier
tenantName	Owner
licenseType	Type (see "The Licensing Model")
status	Status (running, not running, elapsed)
startDate	Start Date (YYYY-MM)
expirationDate	End Date (YYYY-MM)
duration	Duration (in months)
count	Count

The Licensing Model

The licensing model covers the resources used by a Customer, including both Hardware (appliances) and Software capabilities (services). A license has a start date (month/year), a duration in months with a value ranging from [1-72] and a type. The start date of the license triggers license use.

There are three categories of license packages:

- Enterprise Package
- Add-On Package for HA
- Optional Add-On Package

Enterprise Package Licenses

These licenses are the main licenses for accessing the ExtremeCloud SD-WAN Orchestrator. They only differ by the maximum bandwidth that can be reached by each appliance. For example, if an appliance has a total bandwidth of 125 Mbps, it must be paired with an Ent-Branch-M license or any higher license.

Note: There is one license per SD-WAN appliance.

Enterprise Package License	Maximum Bandwidth
Ent-Branch-XS	50 Mbps
Ent-Branch-S	100 Mbps
Ent-Branch-M	250 Mbps

Enterprise Package License	Maximum Bandwidth
Ent-DC-S	500 Mbps
Ent-DC-M	1 Gbps
Ent-DC-L	2 Gbps

> **Warning:** RVC destination sites do not use these licenses. Refer to the table of Domain Level licenses below.

Add-On Package for HA Licenses

These licenses are paired with HA appliances. An appliance needs HA if it uses VRRP or has the same virtual IP address as another appliance on the same Site.

HA License	Maximum Bandwidth
Ent-HA-Branch-XS	50 Mbps
Ent-HA-Branch-S	100 Mbps
Ent-HA-Branch-M	250 Mbps
Ent-HA-DC-S	500 Mbps
Ent-HA-DC-M	1 Gbps
Ent-HA-DC-L	2 Gbps

Optional Add-On Packages

For WAN Optimization Licenses

WANopt License	Description
Ent-WANopt-Branch	WAN Optimization activation license for a Branch Site. This Site already has an Ent-Branch-* license.
Ent-WANopt-DC	WAN Optimization activation license for a Data Center Site. This Site already has an Ent-DC-* license.

For Licenses at the Domain Level (Services)

License	Description
Ent-Remote-V_and_C-5	For 5 RVC destinations, stackable. There must exist as many licenses as the total number of RVC destinations divided by 5.
Ent-EnhancedReporting-5	Full reporting (13 months) for 5 Sites, stackable. There must exist as many licenses as the total number of Enterprise (non HA) appliances divided by 5 (RVC destinations are not included).
Ent-EdgeSentry-10	The number of licenses must correspond to the summed bandwidth divided by 10 of all the appliances using the EdgeSentry feature. For example, if for 5 appliances, the sum of their bandwidths is 420 Mbps (10 + 30 + 30 + 100 + 250), then 42 licenses are necessary.

License Checking

License checking is executed every month or after a configuration modification, or after a license has been added, modified or deleted by Extreme Networks and is based on your current stock of running licenses.

License Breach Notification

When a license breach is detected, e-mail messages are regularly sent to your administrator and to Extreme Networks until the breach is resolved.

Managing Cloud Access

Cloud access is the starting point for redirecting traffic to a Cloud Gateway.

When you own an account or subscription on a IAAS platform where some virtual networks, virtual machines, applications or other resources are hosted, the ExtremeCloud SD-WAN Orchestrator helps you connect your branches to these Cloud resources if it can access the Cloud account or subscription.

1 From the SD-WAN Orchestrator main menu, select the **Administration -> Cloud Access** function to display the Cloud Access Definition window.

  This window shows the number of cloud access objects that have been defined. They may be filtered by Type (AWS, Azure, etc.).

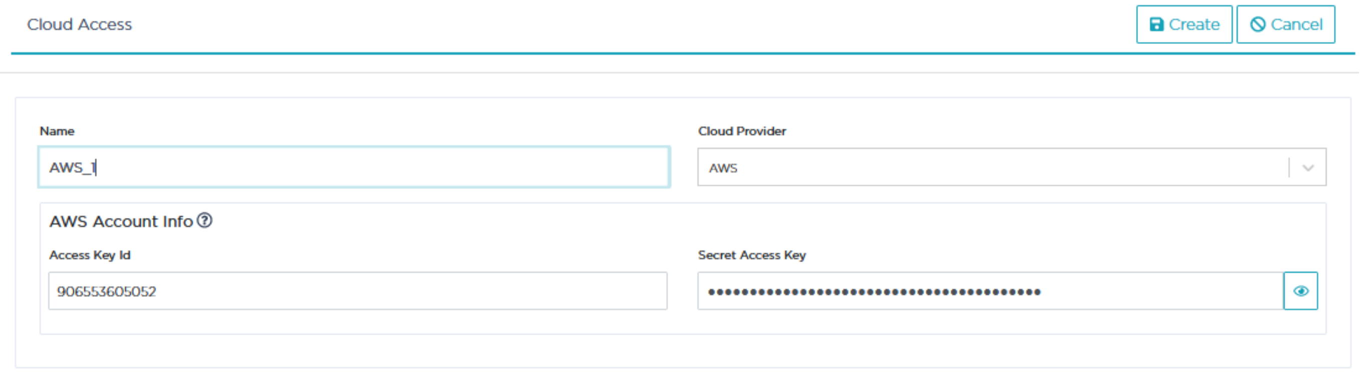
  The Search field also enables you to find any Cloud Access object through its other data (Account ID, User or Subscription Name). Click the ⊗ button to delete the Search filters.

  When the window contains a significant number of objects, the navigation functions at the bottom of the window enable you to navigate through the list.

  - By default, one page includes 50 rows. 20 and 100 are the other options.
  - The total number of pages is specified. This number changes if you select a different number of rows per page.
  - You can display a particular page by directly selecting it from the stack or by clicking the ‹ and › buttons to move from one page forward and backward.
  - Click « to view the first page and » to view the last page of the list.

2 Click the **Add Cloud Access** button to create a new object and define the following parameters:

  AWS



Name: AWS_1

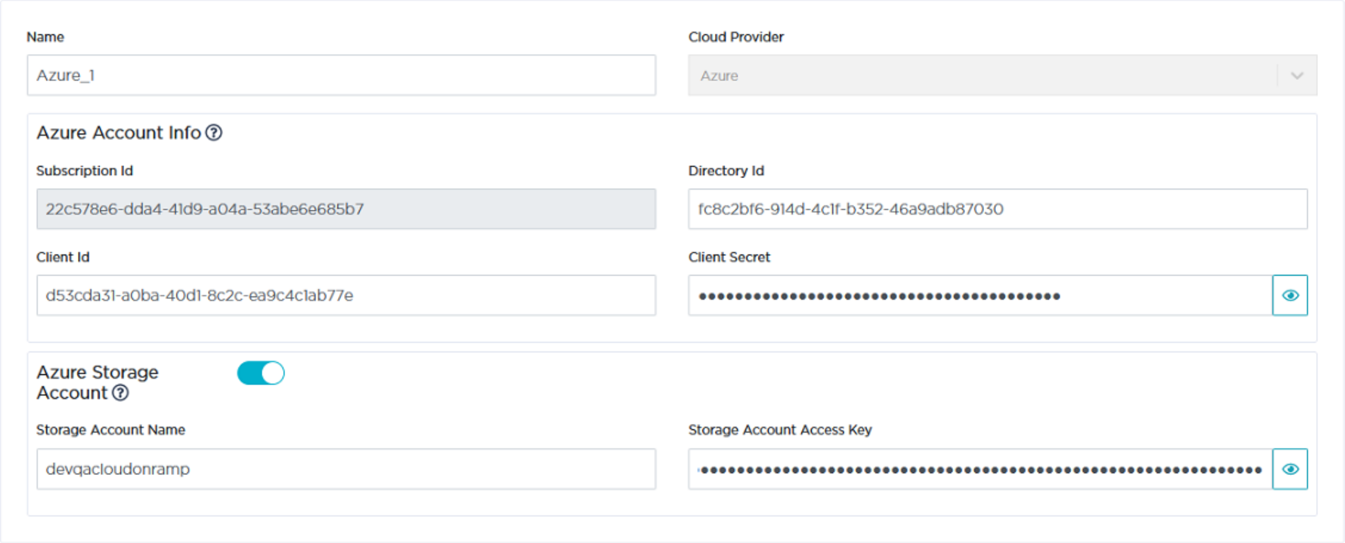
Cloud Provider: AWS

AWS Account Info

Access Key Id: 906553605052

Secret Access Key: ••

Azure



Name

Azure_1

Cloud Provider

Azure

Azure Account Info ⓘ

Subscription Id

22c578e6-dda4-41d9-a04a-53abe6e685b7

Directory Id

fc8c2bf6-914d-4c1f-b352-46a9adb87030

Client Id

d53cda31-a0ba-40d1-8c2c-ea9c4c1ab77e

Client Secret

••

Azure Storage Account ⓘ

Storage Account Name

devqacloudonramp

Storage Account Access Key

••

- Name: enter the cloud access name. This name identifies the Cloud account in the ExtremeCloud SD-WAN Orchestrator.
- Cloud Provider: select the Cloud Provider (AWS, Azure, GCP, etc.).

Note: Only AWS and Azure are supported in the current version.

Warning: Refer to AWS Prerequisites and Azure Prerequisites.

AWS

If the selected Cloud Provider is AWS, specify the *AWS Account* following information:

Access Key ID: enter the Access Key ID provided by AWS when the IAM (Identify and Access Management) user with programmatic access is created. This key includes 20 characters in [A-Z2-7]{20} format.

Secret Access Key: enter the Secret Access Key provided by AWS when the IAM (Identify and Access Management) user with programmatic access is created. This key includes 40 characters in [A-Za-z0-9+/]{40} format.

Azure

If the selected Cloud Provider is Azure, specify the *Azure Account* following information:

Subscription ID: enter the Subscription ID provided by Azure Subscription service. This key includes 32 hexadecimal characters grouped as 8-4-4-4-12.

Directory ID: enter the Directory ID provided by Azure Active Directory service. This key includes 32 hexadecimal characters grouped as 8-4-4-4-12.

Client ID: enter the Application (Client) ID provided by Azure Active Directory service after the application has been created. This key includes 32 hexadecimal characters grouped as 8-4-4-4-12.

Client Secret: enter the secret key provided by Azure. This key includes 40 alpha-numeric characters.

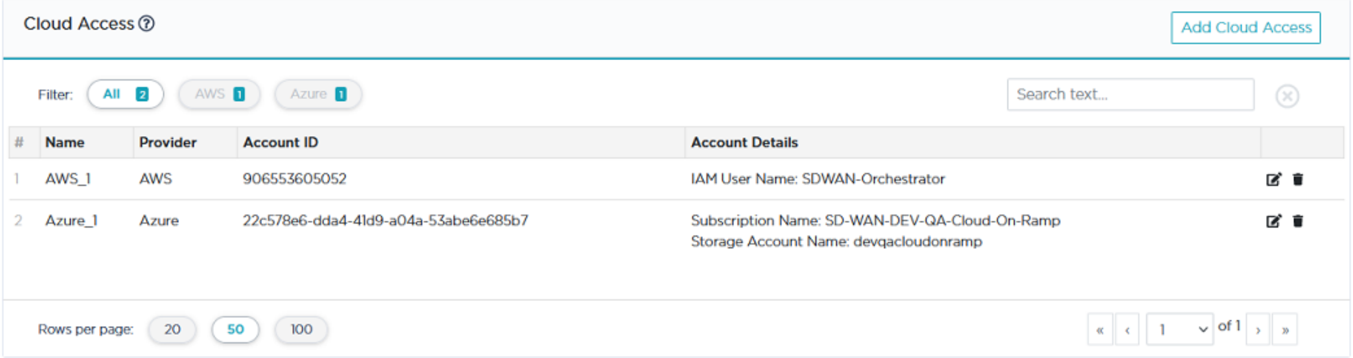
Azure Storage Account- the following information is necessary for Virtual Hub VPN gateways:

Storage Account Name: enter the name of the storage account that will be used by the SD-WAN Orchestrator to generate VPN configuration information. This name is between 3 and 24 characters and contains numbers and lowercase letters.

Storage Account Access Key: this access key is a 512-bit string of 88 characters in length.

3 Click **Create** in the top right corner of the window.

The new cloud access object appears in the Cloud Access Definition window:



Cloud Access

#	Name	Provider	Account ID	Account Details
1	AWS_1	AWS	906553605052	IAM User Name: SDWAN-Orchestrator
2	Azure_1	Azure	22c578e6-dda4-41d9-a04a-53abe6e685b7	Subscription Name: SD-WAN-DEV-QA-Cloud-On-Ramp Storage Account Name: devqacloudonramp

Note: You can edit or delete a Cloud access object at any time.

4 Then, configure Cloud Access.

5 Finally, connect a Branch Office to a Cloud Gateway and configure cloud connection parameters.

- AWS
- Azure

Selecting the Reporting Mode

As the Administrator of a Customer account, you may select the enhanced Reporting Mode of the SD-WAN Orchestrator if your license authorizes it. You can also disable Reporting.

1 Select the **Administration -> Settings** function from the SD-WAN Orchestrator main menu and select a Reporting Mode option.

2 Click **Update**.

Prerequisites

To ensure a smooth connection between every SD-WAN appliance and the components/devices to be reached in the Cloud for deploying your network, check that the following ports are open.

From SD-WAN appliance	to Server/Portal in the Cloud	Type of Communication	Port
	ZTP provisioning and configuration	https	443
	SD-WAN Orchestrator	https	443
	Supervision	kafka	443
	Reverse SSH troubleshooting	TCP	22
	Upgrade	http https	80 443
	NTP clock synchronization	UDP	123

2 Deploying the Network

This documentation is based on Use Cases to explain, step by step, how you can configure the routing components of your network. From Use Case 1 and Use Case 2 which guide you through two basic deployments, the subsequent complementary use cases describe how you progressively enrich your network by configuring more complex elements.

There are two types of network:

A **hybrid network** includes SD-WAN appliances deployed in three different modes:

- **Bridge** mode deployment when all the WAN interfaces are configured in Bridge mode (L2). A WAN interface is in Bridge mode when all the traffic crossing this interface is bridged between this WAN interface and the LAN interface, or the other WAN interfaces in Bridge mode.
- **Bridge-Router** mode deployment when some WAN interfaces are configured in Bridge mode (L2) and some others are in Router mode (L3).
- **Router** mode deployment when all the WAN interfaces are configured in Router mode (L3). A WAN interface is in Router Mode when all the traffic crossing this interface is routed between :
  - hosts/routers connected to the LAN interface and hosts/routers connected to this WAN interface
  - hosts/routers connected to a Bridge mode WAN interface and hosts/routers connected to this WAN interface
  - hosts/routers connected to a Router mode WAN interface and hosts/routers connected to this WAN interface

A **full Router Mode network** includes SD-WAN appliances with WAN interfaces deployed in Router mode only. The SD-WAN Orchestrator enables you to build an overlay network of site connections through IPsec tunnels.

List of Use Cases

The following table enables direct access to the network Use Case diagrams included in this documentation.

Use Case 1	Hybrid Mode Network - Standard Deployment
Use Case 2	Full Router Mode Network - Standard Deployment
Use Case 3	Configuring CloudMesh for Sites
Use Case 4A	Configuring a multi-appliance Router Data Center through iBGP This first deployment uses two appliances with the same AS in the same subnet without access to the Core Router. It ensures network connectivity.
Use Case 4B	Configuring a multi-appliance Router Data Center through iBGP This second deployment uses two appliances with the same AS but two subnets and two local peers. It also requires a static route from the first appliance to the second one. This deployment case ensures transit traffic routing, i.e. the two appliances are used to interconnect two regional networks.
Use Case 4C	Configuring a multi-appliance Hybrid Data Center through iBGP This third deployment is identical to Use Case 4B except that the appliances are in hybrid mode (L2 and L3 interfaces).
Use Case 5	Configuring a multi-appliance Hybrid Data Center through OSPF
Use Case 6	Configuring a multi-appliance Branch Office through VRRP
Use Case 7	Configuring a multi-appliance Branch Office through IHAP
Use Case 8	Configuring traffic redirection to Cloud Security (EdgeSentry)
Use Case 9	Configuring traffic redirection to a Zscaler Web Security Gateway
Use Case 10	Configuring traffic redirection to a Cloud Gateway
Use Case 11	Configuring traffic redirection to an External Gateway
Use Case 12	Configuring a Zone-Based Firewall

General Rules

Appliance identification

You can precisely identify the type of any SD-WAN appliance in your network through its Serial Number.

Serial Number Format

The Serial Number is made of 12 characters as follows: MmmyyEnnnnRr, where:

- M: Manufacturer initials
- mm: month of manufacture (01 to 12)
- yy: year of manufacture (18 for 2018)
- E: appliance type

W	ipe-30so
X	ipe-30ax
U	ipe-40so-v2
V	ipe-40ax-v2
K	ipe-400ax
Y	ipe-420ax
A	ipe-2000ax-T
D	ipe-2000ax-SR-10G
E	ipe-2000ax-LR-10G

- nnnn: serial n° (0001 to 9999)
- Rr: revision (R for major revision, r for minor revision): starting with A0

Example: `A0218X0001A0` corresponds to a Serial Number of the first ipe-30ax manufactured by Aaeon in February 2018.

> **Note:** The Serial Numbers provided as examples in the use cases of the current documentation are virtual.

IP Address allocation

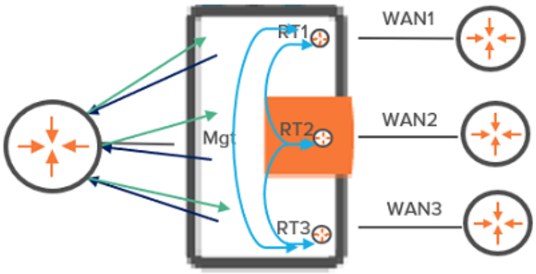
The following diagrams display SD-WAN Orchestrator **automatic** LAN side IP address allocation with an appliance in full router, hybrid and bridge modes. All three WAN interfaces of the appliance are enabled. Note that you may also configure these addresses manually.

You must configure the Management IP address in the SD-WAN Orchestrator.

- Light blue arrows represent iBGP automatic connections
- Dark blue arrows represent iBGP connections you must configure in the SD-WAN Orchestrator
- Green arrows represent the connections you must configure on the Core Router (the SD-WAN Orchestrator is not used)

> **Warning:** iBGP configuration is done with the internal LAN interfaces of the embedded RT routers of the appliance.

Full Router Mode

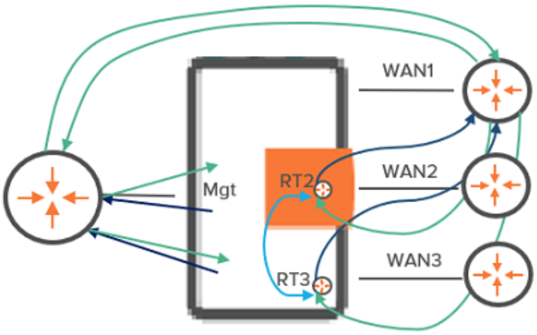


RT1 IP address = Mgt IP address +1

RT2 IP address = Mgt IP address +2

RT3 IP address = Mgt IP address +3

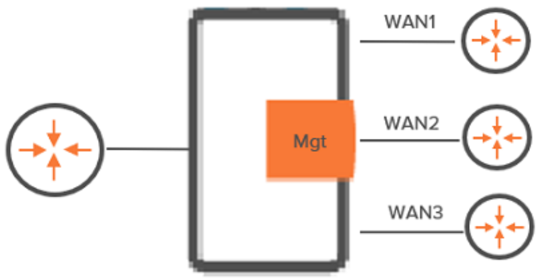
Hybrid Mode



RT2 IP address = Mgt IP address +2

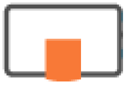
RT3 IP address = Mgt IP address +3

Bridge Mode



There is no automatic LAN side IP address allocation with an appliance in bridge mode.

Graph legend

		Mgt	RT1/RT2/RT3
SD-WAN appliance	router	Management IP address	Router 1/Router 2/Router 3 IP address

Note: A router may be a CE Router (MPLS router), an Internet Access Router or a Core Router.

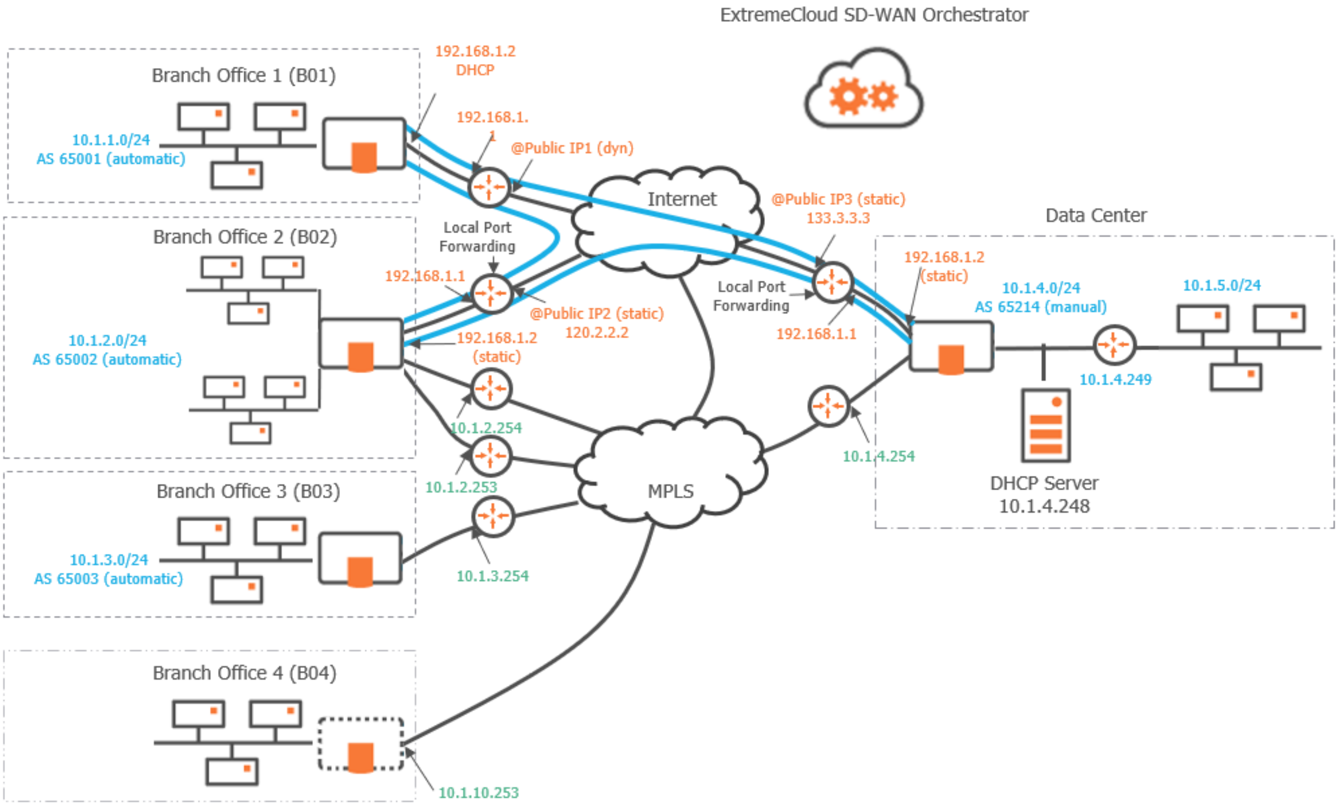
Hybrid Mode Standard Deployment

This section describes the main steps for configuring a hybrid network. It is based on a typical use case illustrating a simple deployment where three branch office appliances are connected to a Data Center appliance through/over either the MPLS private network, or over the Internet, or both. This deployment consists of configuring the appliances.

- B01 is deployed in router mode and is connected to the Data Center through one tunnel over the Internet.
- B02 is deployed in bridge/router mode with a multi-path LAN. It is connected to the Data Center directly through MPLS and over the Internet via one tunnel. A third tunnel connects B02 to B01.
- B03 is deployed in bridge mode and is connected to the Data Center through the MPLS private network.
- B04 is a RVC destination managed by remote appliances.

■ "Configuring the Data Center appliance"
■ "Configuring the Branch Office appliances"
■ "Advanced Configuration"

Use Case 1



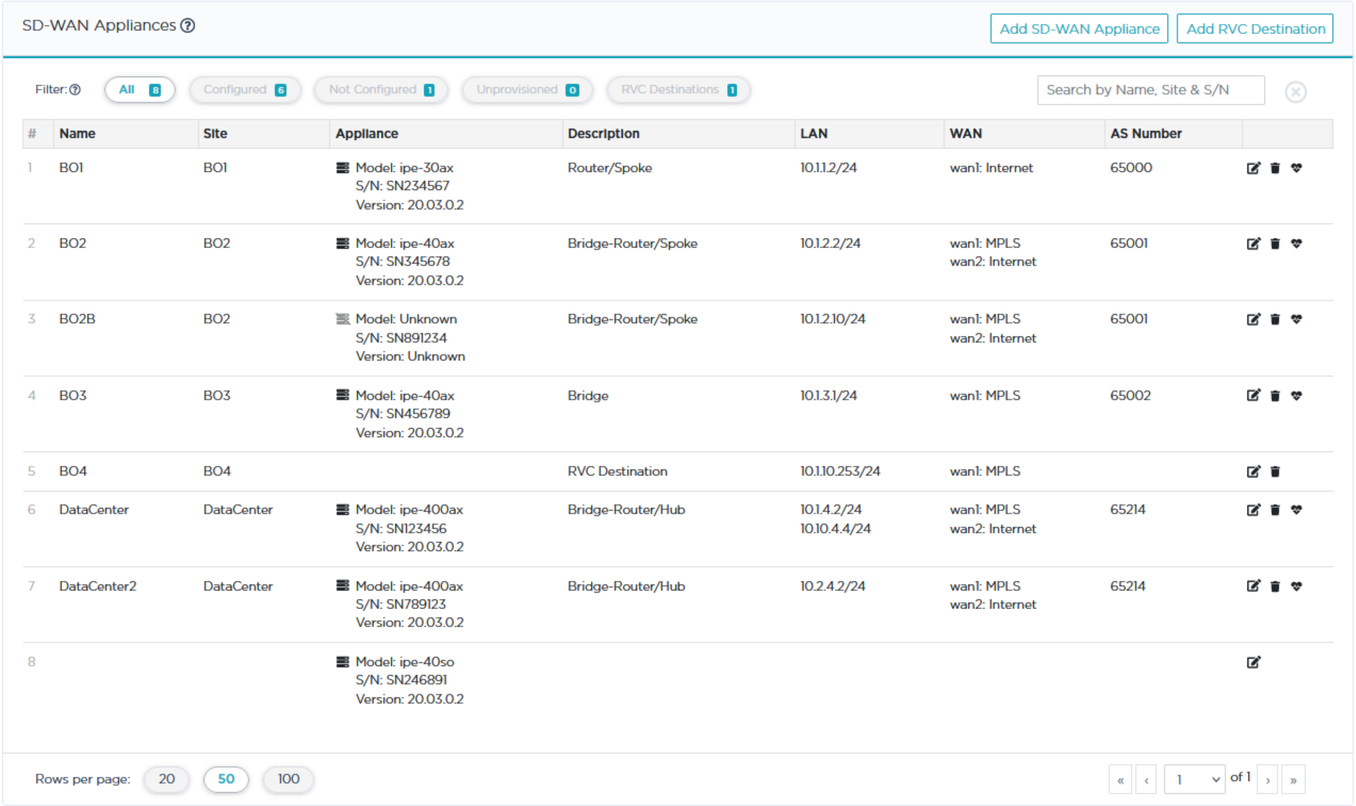
Graph legend

▭	⊕	⬚	🖧	▭	▤	Blue connection	Grey connection
SD-WAN appliance	router	RVC destination	subnet	host in a subnet	server	IPsec tunnel	physical connection between devices

> **Note:** A router may be a CE Router (MPLS Router), an Internet Access Router or a Core Router.

Configuring the appliances

To configure your network SD-WAN appliances, select **Network -> Configuration** from the Orchestrator main menu.



#	Name	Site	Appliance	Description	LAN	WAN	AS Number
1	BO1	BO1	Model: ipe-30ax S/N: SN234567 Version: 20.03.0.2	Router/Spoke	10.1.1.2/24	wan1: Internet	65000
2	BO2	BO2	Model: ipe-40ax S/N: SN345678 Version: 20.03.0.2	Bridge-Router/Spoke	10.1.2.2/24	wan1: MPLS wan2: Internet	65001
3	BO2B	BO2	Model: Unknown S/N: SN891234 Version: Unknown	Bridge-Router/Spoke	10.1.2.10/24	wan1: MPLS wan2: Internet	65001
4	BO3	BO3	Model: ipe-40ax S/N: SN456789 Version: 20.03.0.2	Bridge	10.1.3.1/24	wan1: MPLS	65002
5	BO4	BO4		RVC Destination	10.1.10.253/24	wan1: MPLS	
6	DataCenter	DataCenter	Model: ipe-400ax S/N: SN123456 Version: 20.03.0.2	Bridge-Router/Hub	10.1.4.2/24 10.10.4.4/24	wan1: MPLS wan2: Internet	65214
7	DataCenter2	DataCenter	Model: ipe-400ax S/N: SN789123 Version: 20.03.0.2	Bridge-Router/Hub	10.2.4.2/24	wan1: MPLS wan2: Internet	65214
8			Model: ipe-40so S/N: SN246891 Version: 20.03.0.2				

You generally configure an automatically provisioned appliance. In some specific cases, you may also configure an appliance which is still undefined on the ZTP Server. Refer to "Identifying the appliance".

A RVC destination is a ghost appliance which is never provisioned on the ZTP Server. Refer to "Configuring the B04 Branch Office RVC destination".

The basic procedure for defining an appliance consists of the following steps:

- Identifying the auto-provisioned appliance
- Configuring the LAN
- Configuring the WAN

In Use Case 1, you first configure the Data Center appliance, and then the three other branch office appliances (B01, B02 and B03). You may also configure a branch office RVC destination, B04.

The **Network -> Configuration** window lists the appliances of your network. You may filter them in several ways.

Filtering by Status

- Configured: these appliances are provisioned and totally configured. They are operational in your network.
- Not Configured: the appliances have been automatically provisioned in the SD-WAN Orchestrator from the ZTP Server. They are only visible through their Serial Number and must be further identified and configured.
- Unprovisioned: though these appliances are displayed and configured, they are not defined on ZTP and consequently are not operational in your network.
- RVC destination: though these ghost appliances are displayed and configured, they are never defined on ZTP and are managed by operational remote appliances.

Note that:

- the ▤ sign before Appliance information means that these appliances have been defined in the SD-WAN Orchestrator but are not provisioned on the ZTP Server,
- the ▤ sign before Appliance information means that these appliances have been defined in the SD-WAN Orchestrator and on the ZTP Server (operational status),
- the ⚠ replacing the Appliance information of any appliance means that this appliance is no longer provisioned on the ZTP Server.

Searching for an appliance

You can look for an appliance by typing its Name, Site or Serial Number in the **Search** field. Click the ⊗ button to delete the Search filters. Note that the Status filters adapt to the search results.

List Navigation

When the **Network -> Configuration** window contains several thousands of appliances, the navigation functions at the bottom of the window enable you to navigate through the list.

- By default, one page includes 50 rows. 20 and 100 are the other options.
- The total number of pages is specified (24 in the example below). This number changes if you select a different number of rows per page.
- You can display a particular page by directly selecting it from the stack or by clicking the ‹ and › buttons to move from one page forward and backward.
- Click « to view the first page and » to view the last page of the list.

Modifying, replacing or deleting an appliance

- Click ✎ to edit the configuration of an appliance. Modify any values and click Update to save your settings.

Replacing an appliance

> **Warning:** When replacing an appliance by another one, NEVER delete the appliance to be replaced in the SD-WAN Orchestrator because its configuration will be lost.

If the appliance is auto-provisioned:

1. Your system administrator deletes it on the ZTP Portal; the deleted appliance is listed as 'Unprovisioned' in the SD-WAN Orchestrator.
2. In the Network -> Configuration list, **edit** the unprovisioned appliance (which is still configured) and enter its new Serial Number.
3. **Update** the configuration.

- Click 🗑 if you want to delete an appliance and its configuration. The system asks you to click the icon a second time to confirm your action.
- Click ♥ to check appliance detailed information; refer to "Surveying SD-WAN appliance details".

Configuring the Data Center appliance

In "Use Case 1", start configuring your network with the Data Center appliance.

This hybrid Data Center includes two subnets (10.1.4.0 and 10.1.5.0) and a DHCP Server.

There is also one prerequisite which is the necessary configuration of Port Forwarding on the Internet Access router. This rule authorizes sending the UDP packets to the appliance on ports 500 (IKEv2) and 4500 (IPsec NAT Traversal). For this reason, you must apply a static IP address to the Data Center WAN2 interface.

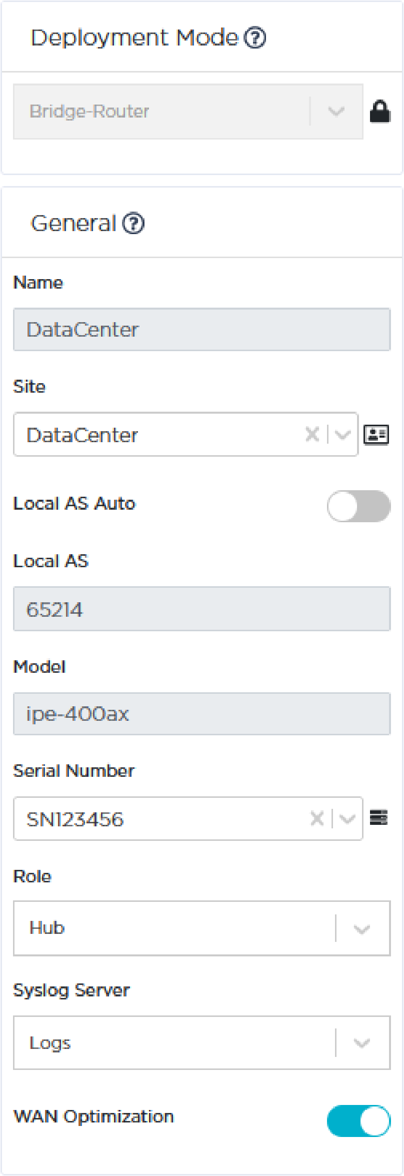
- "Identifying the appliance"
- "Configuring the LAN"
- "Configuring the WAN(s)"

Identifying the appliance

After the Data Center appliance with the 'SN123456' Serial Number (and its Model/Version information) has been automatically provisioned in the SD-WAN Orchestrator from the ZTP Server, as indicated via the 🗄 sign, it appears under the 'Not Configured' tab of the Network -> Configuration window.

Proceed as follows to identify and further configure the appliance.

1. In the Network -> Configuration window, click ✎ to edit the appliance.
2. In the **Deployment Mode** panel, select the Bridge-Router option and click the 🔓 icon to enable the related panels and functions of the interface.



Deployment Mode

Bridge-Router

General

Name

DataCenter

Site

DataCenter

Local AS Auto

Local AS

65214

Model

ipe-400ax

Serial Number

SN123456

Role

Hub

Syslog Server

Logs

WAN Optimization

3 In the General panel, enter the **Name** of the appliance as well as the name of the related **Site**.

4 Manually enter 65214 for the Local Autonomous System. It corresponds to the Autonomous System configured on the 10.1.4.249 router.

If you check the **Auto** option (not possible in the current Use Case), the related field is automatically populated with a number selected by the Orchestrator from the **AS Number Range** you have specified in the Overlay Routing panel of the Advanced Configuration window.

5 Through the **Role** field, define the appliance as a Hub since it identifies here a Data Center (receives tunnel requests on L3 interfaces). A spoke corresponds to a Site appliance (generates tunnel requests on L3 interfaces). Tunnels are always built from the spokes to the hub.

6. Since NATted DTI traffic is enabled on the WAN2 interface, select the Syslog Server you defined in "Advanced Configuration" to enable log export.
7. WAN Optimization is activated by default on this appliance if the matching license is available.

Also see how to identify:

- a Branch Office appliance

Configuring the LAN

As a second step, configure the Data Center LAN which includes one physical interface.

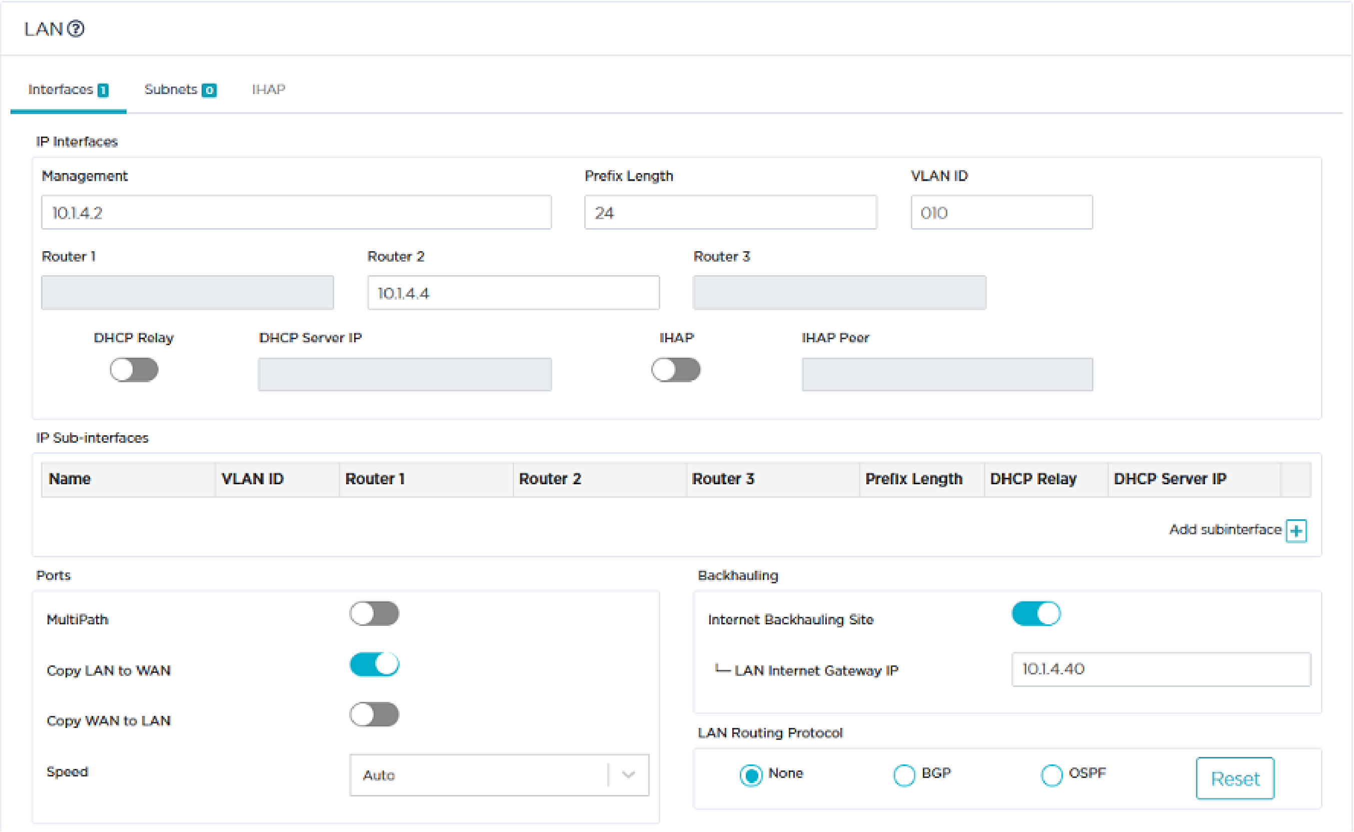
Refer to "Use Case 1" diagram where the LAN information is displayed in blue.

1. Click the **Interfaces** tab.
2. Enter the appliance Management IP address (10.1.4.2), Prefix Length (24).

   The Management IP address is used for communicating with other appliances, the ZTP Server and the Orchestrator.
3. Use the default **Auto Generated** option (creation window only) to let the system allocate LAN addresses automatically to the Routers (Router X IP = Management IP + X) linked to the WANs in Router mode that you will configure for this appliance. Also refer to "IP Address allocation".

   In this example, only Router 2 IP address will be automatically defined as it corresponds to WAN2 in Router mode.
4. Do not activate the DHCP Relay function since the Data Center hosts can directly access the DHCP Server. The appliance does not need to relay host requests.
5. Do not enter any VLAN ID. Note that the grey values appearing in some fields of the interface are only given as examples and are not taken into account in the configuration.
6. Do not activate the MultiPath function.
7. Enable the Copy LAN to WAN function to copy the state of the LAN to its related WAN. This LAN/WAN state synchronization is useful when the LAN interface breaks down.
8. Leave the Speed parameter to Auto to let the system define the speed of the interface, or you can force the speed to 100FD or 1000FD. The full duplex speed is expressed in megabits per second.
9. Define this Data Center hub appliance as a Backhauling Site. This means it can receive Internet traffic through the overlay and route it to a firewall in the LAN: specify the LAN Internet Gateway IP address as 10.1.4.40

The following window displays the validated settings.



LAN

Interfaces 1 | Subnets 0 | IHAP

IP Interfaces

Management	Prefix Length	VLAN ID
10.1.4.2	24	010

Router 1	Router 2	Router 3
	10.1.4.4	

DHCP Relay: off | DHCP Server IP: | IHAP: off | IHAP Peer:

IP Sub-interfaces

Name	VLAN ID	Router 1	Router 2	Router 3	Prefix Length	DHCP Relay	DHCP Server IP

Add subinterface

Ports

MultiPath	off
Copy LAN to WAN	on
Copy WAN to LAN	off
Speed	Auto

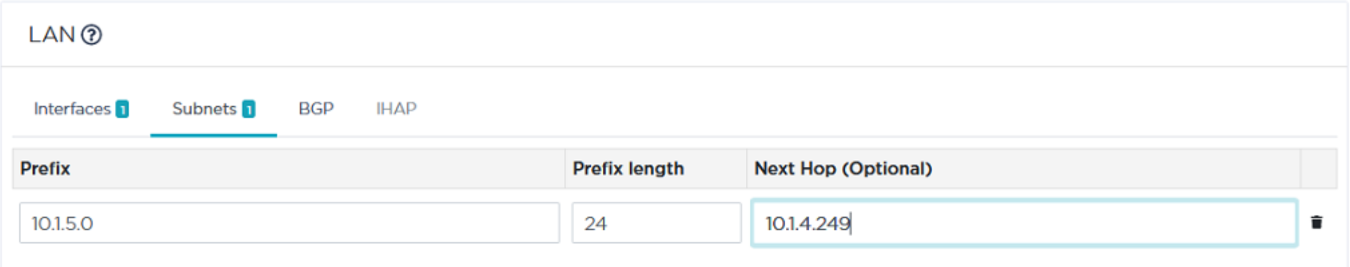
Backhauling

Internet Backhauling Site	on
└ LAN Internet Gateway IP	10.1.4.40

LAN Routing Protocol

● None ○ BGP ○ OSPF Reset

Defining additional Subnets



LAN

Interfaces 1 | Subnets 1 | BGP | IHAP

Prefix	Prefix length	Next Hop (Optional)
10.1.5.0	24	10.1.4.249

In Use Case 1, there is one additional subnet you must specify because the system is unable to detect it automatically. Subnets enable you to classify, measure and control the traffic coming from and going to specific hosts and servers.

10 Click the **Subnets** tab and the Add subnet icon ⊞.

11 Define the additional subnet by entering its prefix (10.1.5.0), prefix length (24) and next hop (10.1.4.249).

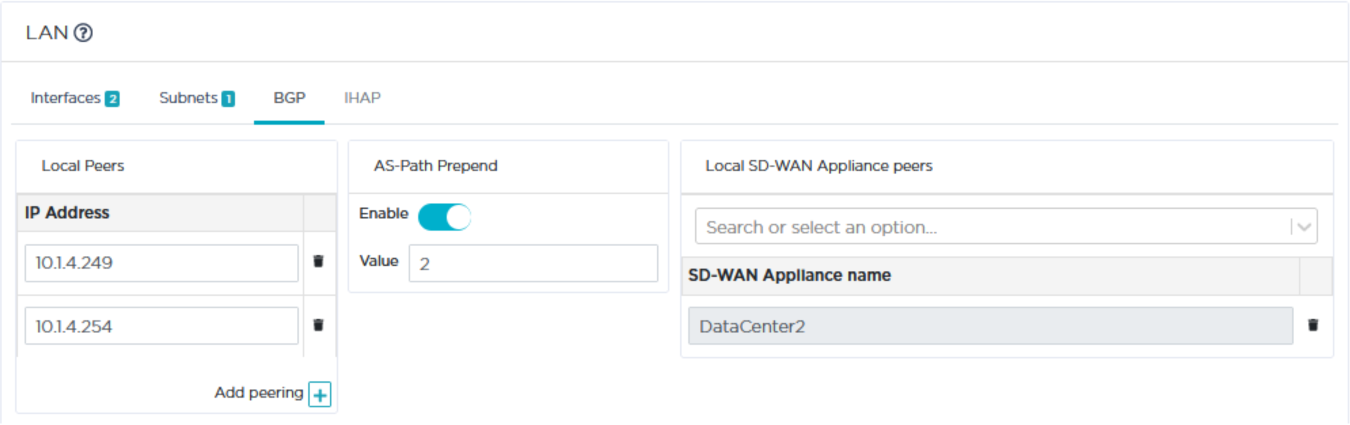
> **Note:** The Next Hop field is optional and you can leave it empty if you enable BGP or OSPF.

12 The Data Center appliance exchanges its routing tables with the local router using **either BGP or OSPF**. Refer to the following procedures which are mutually exclusive.

Configuring BGP

1 In the Interfaces window, select BGP as the LAN Routing Protocol.

2 Click the **BGP** tab and the Add peering icon ⊞.



Local Peers

IP Address: 10.1.4.249

IP Address: 10.1.4.254

AS-Path Prepend

Enable: ●

Value: 2

Local SD-WAN Appliance peers

Search or select an option...

SD-WAN Appliance name: DataCenter2

3 Enter the IP address of the BGP local peers (10.1.4.249 and 10.1.4.254).

4 Activate AS Path Prepending and enter 2 in the Value field. The authorized range is [1-10].

An AS Path is a BGP route attribute and corresponds to the list of autonomous systems that routing information passes through to get to a specified router. AS path length represents the sequence of AS hops that a BGP route follows from a particular AS (the traffic sender) towards the origin AS (the traffic receiver).

Since BGP prefers the shortest AS path to get to the destination, the MPLS CE router (10.1.4.254) will probably re-route the traffic to the hybrid Data Center appliance router (10.1.4.4) and use the Internet route towards B02 instead of using the MPLS route towards the same appliance (see "Use Case 4C" and "Use Case 1" diagrams). To avoid this behavior and enable the DWS Service to operate correctly, you can manipulate AS path length by extending the AS path with multiple copies of the AS number of the first AS path hop.

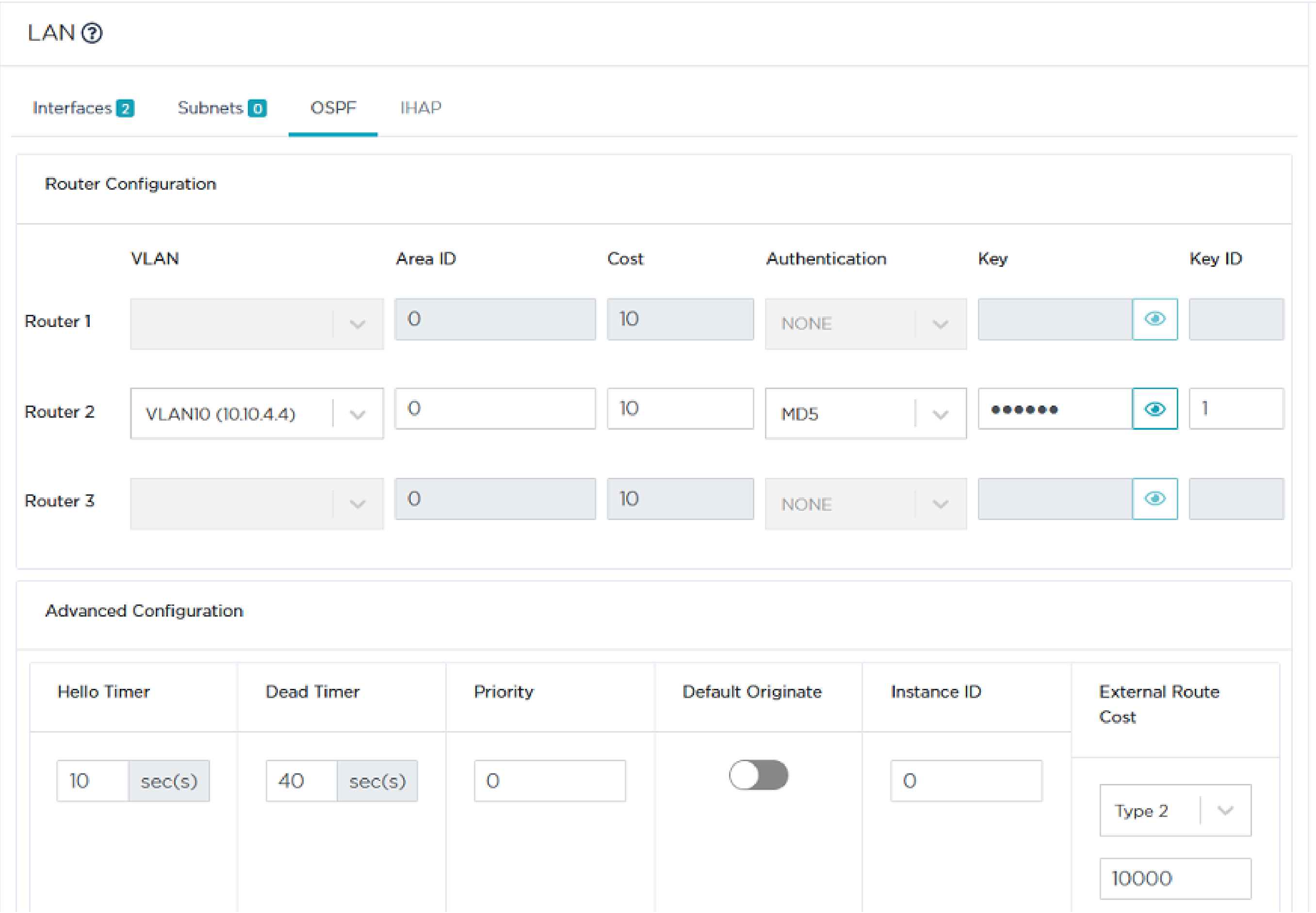
By entering 2 as AS Path Prepending value, you define three AS path hops (2 + the initial one) from the Data Center to B02 for the Internet route. It corresponds to AS_PATH=[65002, 65002, 65002] and is not shorter than AS_PATH=[65500,65002] for the MPLS route (where 65500 represents the MPLS hop).

Configuring OSPF

1 In the Interfaces window, select OSPF as the LAN Routing Protocol.

2 Click the Add subinterface icon ⊞. Enter 10 as VLAN ID, 10.10.4.4 as the sub-interface IP address for Router 2 and 24 as Prefix Length. Each VLAN corresponds to an OSPF network area.

3 Click the **OSPF** tab.



LAN ⓘ

Router Configuration

	VLAN	Area ID	Cost	Authentication	Key	Key ID
Router 1		0	10	NONE		
Router 2	VLAN10 (10.10.4.4)	0	10	MD5	••••••	1
Router 3		0	10	NONE		

Advanced Configuration

Hello Timer	Dead Timer	Priority	Default Originate	Instance ID	External Route Cost
10 sec(s)	40 sec(s)	0	○	0	Type 2 10000

4 Configure Router 2 as follows:

- VLAN: select VLAN ID 10 you defined in the previous step. You can also select the 'None' option to take into account the ip address of the router.
- Area ID: by default, Area 0 which is the backbone area or the core of the OSPF network. It corresponds to the area including the CE router. All other areas are connected to it and all the traffic between areas must traverse it.

  In this example, enter 1 as Area 1 ID.
- Cost: use the 10 default value which corresponds to the interface cost of Router 2 (10.1.4.4).
- Authentication: select one authentication method among MD5, SHA1, HMAC SHA256, HMAC SHA384 and HMAC SHA512. By default, there is no authentication (NONE option).
- Key: enter your authentication password. Use the 👁 icon different statuses to either display or hide the key.
- Key ID: enter 1 as the password identifier. This value must match the key ID of the Core Router password.

5 Specify OSPF Advanced Configuration parameters which are common to all the routers:

- Hello Timer: time between each Hello packet sent by the router to the interface(s). Hello packets enable the system to establish adjacencies and router keepalive messages to notify neighbors that links are up and active.
- Dead Timer: time after the last Hello packet is sent by a router and before the router is considered as dead. Dead Timer cannot be smaller than Hello Timer x 3.
- Priority: with the Broadcast network type (only network type supported), the network elects one Designated Router (DR) and one Backup Designated Router (BDR). They are in charge of transferring topology modifications to all the routers of the area. The priority mechanism determines which router is DR and which one is BDR.

  The router with the highest priority value is the DR router which is the main router for distributing the routes. If both DR and BDR routers have the same priority value, the router with the highest IP address is selected as the DR. In the current example, keep the 0 default value, i.e. this router is neither DR nor BDR (it does not participate in the election).
- Default Originate: only check this option if you want to redistribute a default route through OSPF.
- Instance ID: set this field to 0 to ensure this parameter is not currently used by routers.
- External Route Cost: select the Type 2 option and enter 10000. This parameter is also used for implementing high availability between two appliances. Refer to "Configuring a multi-appliance Hybrid Data Center through OSPF".

6 Define BGP Community and OSPF Tag parameters to avoid routing loops; refer to "Routing Loop Prevention".

7 Click **Update**.

> **Note:** The Reset button in the LAN Routing Protocol area of the LAN window enables you to delete BGP or OSPF configurations and restore the default values. When you click this button and confirm the operation, either BGP local peers are deleted or OSPF authentication data are cleared.

Also see how to configure:

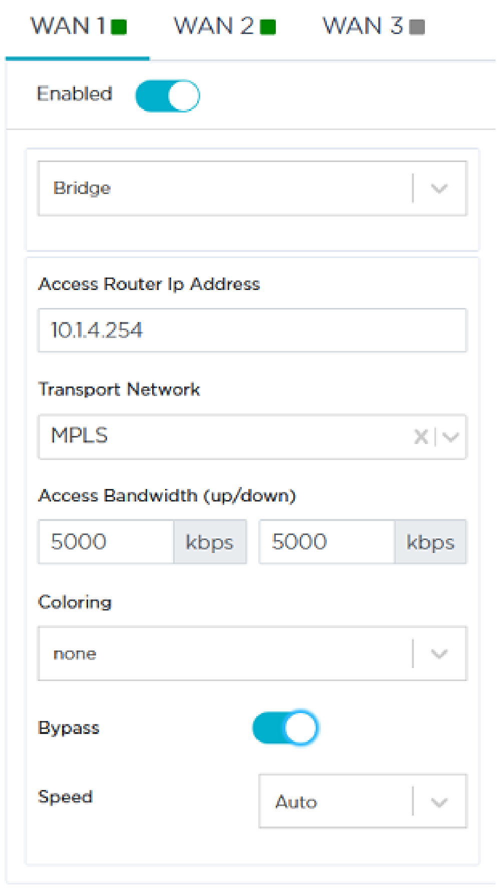
- a Branch Office appliance LAN

Configuring the WAN(s)

As a third step, configure the two WANs linked to the Data Center appliance: MPLS and Internet.

> **Warning:** To configure a hybrid appliance, always start configuring WAN1 in bridge mode (because of the Bypass function which is activated by default).

Refer to "Use Case 1" diagram where WAN1 (MPLS) details are displayed in green.



Enabled: ●

Bridge

Access Router Ip Address: 10.1.4.254

Transport Network: MPLS

Access Bandwidth (up/down): 5000 kbps 5000 kbps

Coloring: none

Bypass: ●

Speed: Auto

1 Activate the WAN through the ● icon. You may now enter field data.

2 Select the **Bridge** option for this L2 interface.

3 Enter the CE router IP Address, 10.1.4.254. It must correspond to the LAN Interface IP Address.

4 Type 'MPLS' as Transport Network type.

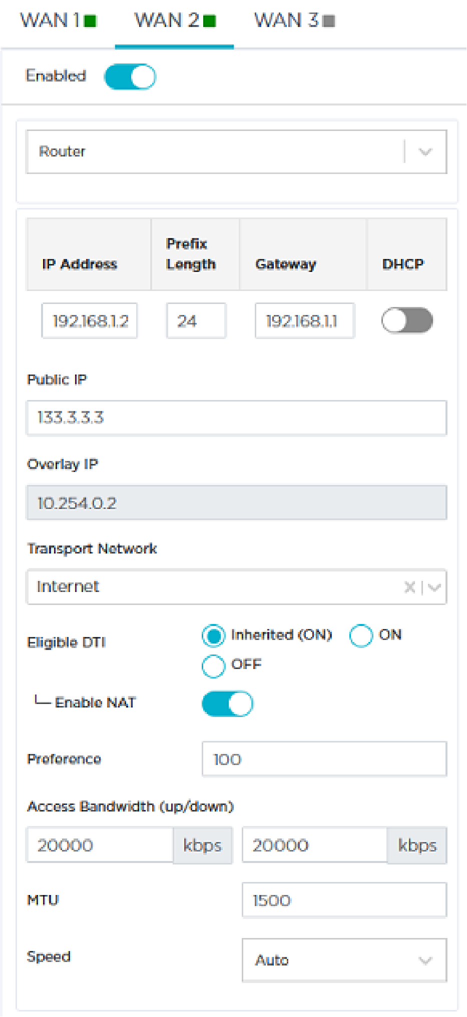
5 In the Access Bandwidth fields, define the up and down throughput (in kilobits per second) allocated to the WAN: 5000.

6 Select from the Coloring stack of values any Coloring Policy you have previously configured through the Applications -> Configuration -> System Provisioning -> Coloring function. The default value 'none' means that all the packets are processed as if they were uncolored. Refer to "Configuring Coloring".

7 The Bypass option is activated by default, i.e. the system will bypass the traffic in case of failure (e.g. power failure). When bypass is executed, services such as Visibility, Control, Optimization etc. are of course not available.

8 Leave the Speed parameter to Auto to let the system define the speed of the interface, or you can force the speed to 100FD or 1000FD. The full duplex speed is expressed in megabits per second.

Refer to "Use Case 1" diagram where WAN2 (Internet) details are displayed in orange.



WAN 1 🟩 WAN 2 🟩 WAN 3 ▨

Enabled: on

Router

IP Address	Prefix Length	Gateway	DHCP
192.168.1.2	24	192.168.1.1	off

Public IP: 133.3.3.3

Overlay IP: 10.254.0.2

Transport Network: Internet

Eligible DTI: ● Inherited (ON) ○ ON ○ OFF

└ Enable NAT: on

Preference: 100

Access Bandwidth (up/down): 20000 kbps 20000 kbps

MTU: 1500

Speed: Auto

1 Activate the WAN through the icon. You may now enter field data.

2 Select the **Router** option for this L3 interface.

3 Do not activate the DHCP function to proceed with Step 4.

4 Enter the WAN2 interface static information, 192.168.1.2 as IP Address, 24 as Prefix length. This address must be static to enable the configuration of Port Forwarding on the Internet Access router.

5 Enter the Default Gateway: 192.168.1.1

6 Define the Public IP address (133.3.3.3) which corresponds to the WAN side of the Internet Access router to which the WAN2 interface is connected. The Port Forwarding

configuration of the Internet Access router enables this device to send the UDP packets to the appliance WAN2 on ports 500 (IKEv2) and 4500 (IPsec NAT Traversal). The Internet Access router also modifies the Egress packets in order to replace its 133.3.3.3 public address with the 192.168.1.2 WAN2 static address as destination address.

7. When configuring a WAN for the first time, type the name of the network you are connected to, 'Internet' in the current example. Clearly identify each name through customization. Once a Transport Network type has been defined, you can select it from the stack when configuring subsequent WANs.
8. This interface is automatically eligible to DTI (Inherited ON) because you globally activated this policy for the 'Internet' Transport Network (refer to Advanced Configuration -> Transport Network Settings). You may also manage DTI individually for this Internet L3 interface by checking the ON or OFF options.
9. Directly derived from the activated Eligible DTI option, keep the Enable NAT mode activated. This is a source-NAT where the LAN IP addresses (10.1.4.0 or 10.1.5.0) are replaced with the 192.168.1.2 WAN2 IP address. This NAT only applies to the traffic sent over the Internet. The traffic to the Branch Offices/Sites is transferred through the IPsec tunnels.

   If you deactivate the Enable NAT mode which controls the firewall, incoming connections from the WAN are allowed to go to the LAN.
10. Enter the same Preference value as the local Preference value of the CE router (10.1.4.254).
11. In the Access Bandwidth fields, define the up and down throughput (in kilobits per second) allocated to the WAN: 20000.
12. Enter the MTU value which corresponds to the maximum number of bytes loaded in the Payload. The default value is 1500.
13. Leave the Speed parameter to Auto to let the system define the speed of the interface, or you can force the speed to 100FD or 1000FD. The full duplex speed is expressed in megabits per second.
14. Validate your input by hitting the **Create** button.

    If the appliance already exists and you modify any data, click the **Update** button.

> **Note:** The Internal Tunnels, External Gateways and Local Port Forwarding configuration panels are not used for this interface.

15. In the Network -> Advanced Configuration window, add this 'DataCenter' hub appliance as Time Synchronization Server. Then click **Update**.

Also see how to configure:

- Branch Office appliance WANs

Configuring the Branch Office appliances

After you have configured the Data Center appliance (in "Use Case 1"), you must configure the B01, B02 and B03 Branch Office appliances. Then, configure the B04 Branch Office RVC destination.

- "Configuring the B01 Branch Office appliance"
- "Configuring the B02 Branch Office appliance"
- "Configuring the B03 Branch Office appliance"
- "Configuring the B04 Branch Office RVC destination"

Configuring the B01 Branch Office appliance

B01 is configured in full router mode and is connected to the Data Center through one tunnel over the Internet. Another tunnel connects B01 to B02.

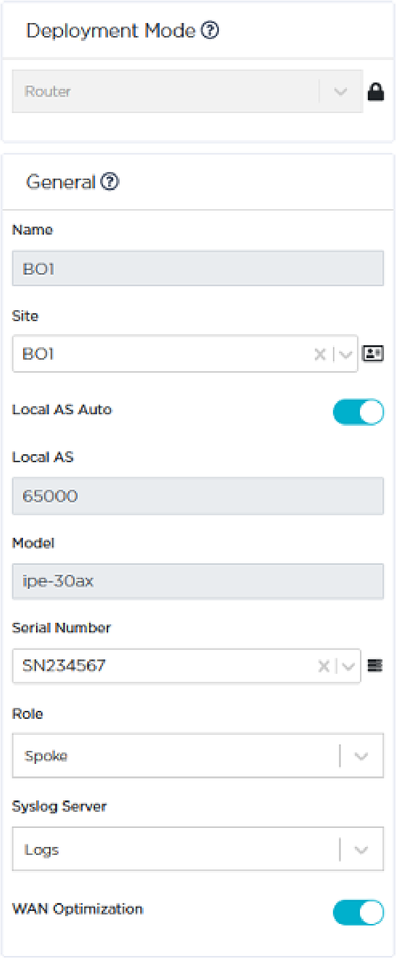
Identifying the appliance

After the B01 appliance with the 'SN234567' Serial Number (and its Model/Version information) has been automatically provisioned in the SD-WAN Orchestrator from the ZTP Server, as indicated via the ≣ sign, it appears under the 'Not Configured' tab of the Network -> Configuration window.

Proceed as follows to identify and further configure the appliance.

1 In the Network -> Configuration window, click ✎ to edit the appliance.

2 In the Deployment Mode panel, select the Router option and hit the 🔓 icon to enable the related panels and functions of the interface.



Deployment Mode ⓘ

Router 🔒

General ⓘ

Name: B01

Site: B01

Local AS Auto: on

Local AS: 65000

Model: ipe-30ax

Serial Number: SN234567

Role: Spoke

Syslog Server: Logs

WAN Optimization: on

3. In the General panel, enter the **Name** of the appliance as well as the name of the related **Site** (B01)**.**

   The 🪪 button at the right of the Site Name enables you to display the Site subnets.

4. Select the **Auto** option of the Local AS parameter. The related field is automatically populated with a number selected by the Orchestrator from the **AS Number Range** you have specified in the Overlay Routing panel of the Advanced Configuration window.

   This parameter is used in the B01 WAN for tunnel mapping between this Site and the other Sites it will be connected to (Data Center and B02).

5. Through the **Role** field, define the appliance as a Spoke since it identifies a Branch Office appliance (generates tunnel requests). Tunnels are always built from the spokes to the hub.
6. Since NATted DTI traffic is enabled on the WAN1 interface, select the Syslog Server you defined in "Advanced Configuration" to enable log export.
7. WAN Optimization is activated by default on this appliance if the matching license is available.

Configuring the LAN

As a second step, configure the B01 appliance LAN which includes one physical interface. Refer to "Use Case 1" diagram where the LAN information is displayed in blue.

1. Click the **Interfaces** tab.
2. Enter the appliance Management IP address (10.1.1.2), Prefix Length (24).

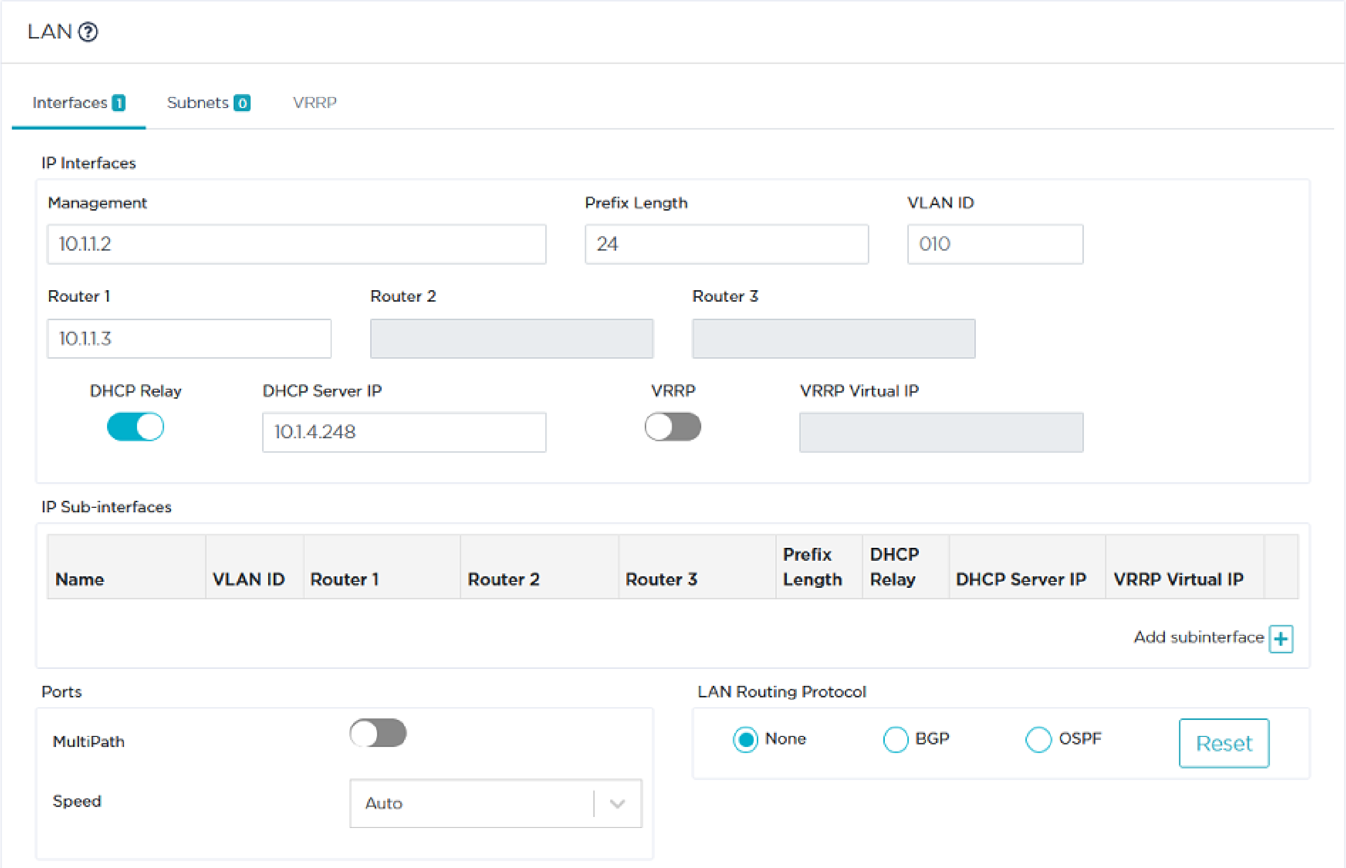
   The Management IP address is used for communicating with other appliances, the ZTP Server and the Orchestrator.

3. Use the default **Auto Generated** option (creation window only) to let the system allocate LAN addresses automatically to the Routers (Router X IP = Management IP + X) linked to the WANs in Router mode that you will configure for this appliance. Also refer to "IP Address allocation".

   In this example, only Router 1 IP address will be automatically defined as it corresponds to WAN1.

4. Do not enter any VLAN ID. Note that the grey values appearing in some fields of the interface are only given as examples and are not taken into account in the configuration.
5. Since there is no router in the B01 LAN for exchanging routing tables, there is no additional subnet or sub-interface to define for configuring BGP peering or OSPF adjancencies.
6. Leave the Speed parameter to Auto to let the system define the speed of the interface, or you can force the speed to 100FD or 1000FD. The full duplex speed is expressed in megabits per second.

The following window displays the validated settings.



LAN

Interfaces 1 | Subnets 0 | VRRP

IP Interfaces

Management: 10.1.1.2

Prefix Length: 24

VLAN ID: 010

Router 1: 10.1.1.3

Router 2:

Router 3:

DHCP Relay: on

DHCP Server IP: 10.1.4.248

VRRP: off

VRRP Virtual IP:

IP Sub-interfaces

Name	VLAN ID	Router 1	Router 2	Router 3	Prefix Length	DHCP Relay	DHCP Server IP	VRRP Virtual IP

Add subinterface +

Ports

MultiPath: off

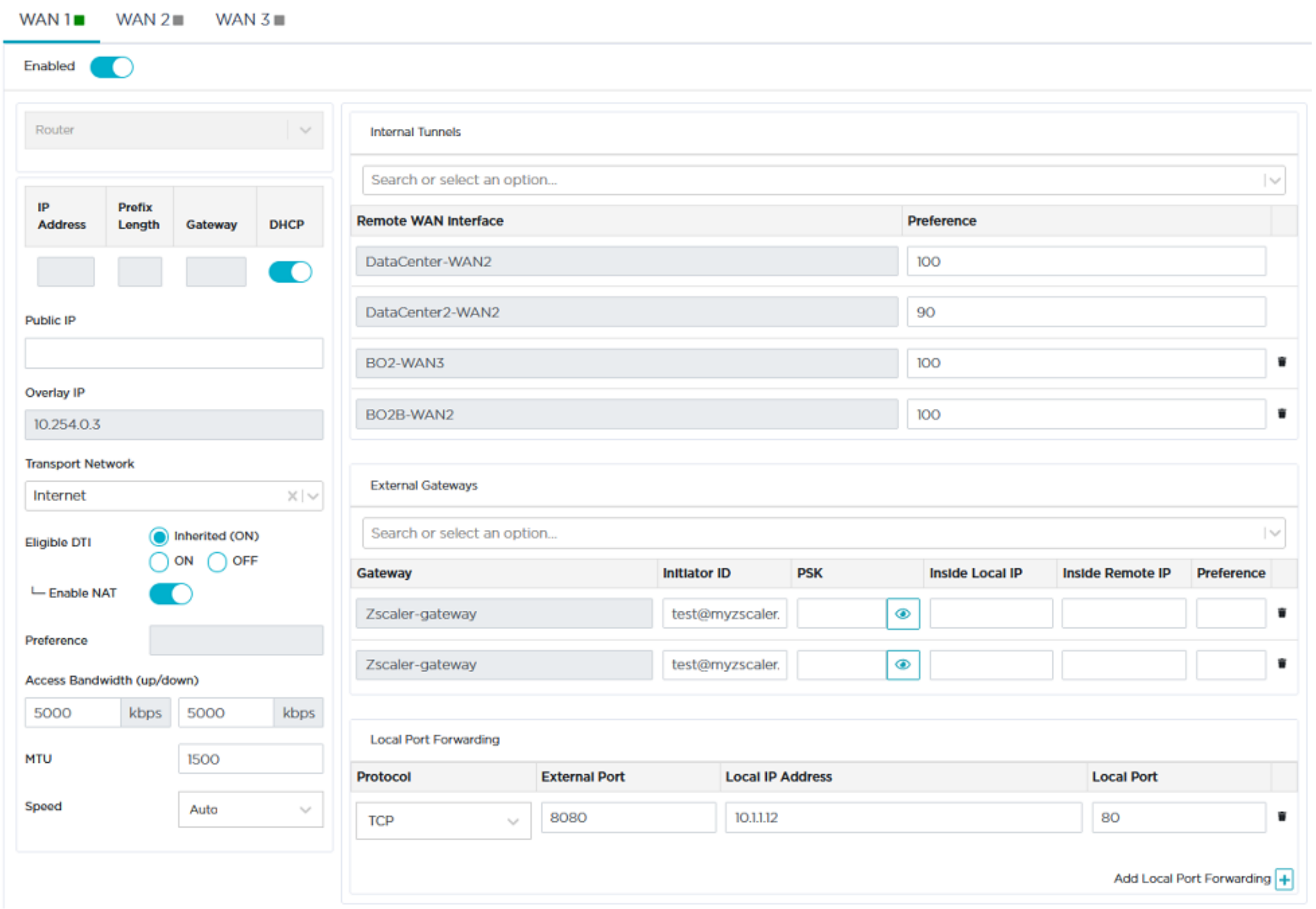
Speed: Auto

LAN Routing Protocol

● None ○ BGP ○ OSPF

Configuring the WAN

As a third step, configure the WAN linked to the B01 appliance: Internet. Refer to "Use Case 1" diagram where WAN1 (Internet) details are displayed in orange.



WAN 1 🟩 WAN 2 ■ WAN 3 ■

Enabled ●

Router

IP Address	Prefix Length	Gateway	DHCP
			●

Public IP

Overlay IP: 10.254.0.3

Transport Network: Internet

Eligible DTI: ● Inherited (ON) ○ ON ○ OFF

Enable NAT ●

Preference

Access Bandwidth (up/down): 5000 kbps 5000 kbps

MTU: 1500

Speed: Auto

Internal Tunnels

Search or select an option...

Remote WAN Interface	Preference
DataCenter-WAN2	100
DataCenter2-WAN2	90
BO2-WAN3	100
BO2B-WAN2	100

External Gateways

Search or select an option...

Gateway	Initiator ID	PSK	Inside Local IP	Inside Remote IP	Preference
Zscaler-gateway	test@myzscaler.				
Zscaler-gateway	test@myzscaler.				

Local Port Forwarding

Protocol	External Port	Local IP Address	Local Port
TCP	8080	10.1.1.12	80

Add Local Port Forwarding +

1 Activate the WAN through the ● icon. You may now enter field data.

2 Define this interface in Router mode.

3 With the DHCP parameter activated by default, the interface IP Address, Prefix Length and Default Gateway are dynamically allocated (by the DHCP server of the Internet Access Router) to the interface, since this WAN interface is connected to the Internet.

4 As you already defined the 'Internet' type of Transport Network for the Data Center WAN2, select it from the stack.

When configuring a WAN for the first time, type the name of the network you are connected to, 'Internet' in the current example. Clearly identify each name through customization. Once a Transport Network type has been defined, you can select it from the stack when configuring subsequent WANs.

5 This interface is automatically eligible to DTI (Inherited ON) because you globally activated this policy for the 'Internet' Transport Network (refer to Advanced Configuration

-> Transport Network Settings). You may also manage DTI individually for this Internet L3 interface by checking the ON or OFF options.

6 Directly derived from the activated Eligible DTI option, keep the Enable NAT mode activated. This is a source-NAT where the LAN Management IP address (10.1.1.2) is replaced with the 192.168.1.2 WAN1 IP address. This NAT only applies to the traffic sent over the Internet. The traffic to the Data Center and to other Sites is transferred through the IPsec tunnels.

   If you deactivate the Enable NAT mode which controls the firewall, incoming connections from the WAN are allowed to go to the LAN.

7 The Preference parameter is not available for a Spoke appliance.

8 In the Access Bandwidth fields, define the up and down throughput (in kilobits per second) allocated to the WAN: 5000.

9 Enter the MTU value which corresponds to the maximum number of bytes loaded in the Payload. The default value is 1500.

10 Leave the Speed parameter to Auto to let the system define the speed of the interface, or you can force the speed to 100FD or 1000FD. The full duplex speed is expressed in megabits per second.

11 The Internal Tunnels stack of values contains the WAN interfaces of the remote sites connected to the same network as the B01 WAN1 interface. These interfaces are automatically detected by the Orchestrator. In "Use Case 1", the system offers 'B02-WAN3' you can add as additional connection to create a tunnel between B01 and B02.

   The Preference parameter is meaningless in this Use Case because there is only one Data Center appliance.

12 The External Gateways panel is used to connect this WAN interface to a Web Security Gateway. Refer to "Use Case 9".

13 Define Local Port Forwarding by selecting the TCP Protocol, typing 8080 as External Port, 10.1.1.12 as the Local IP Address and 80 which is the generally used Local Port for HTTP traffic.

14 Validate your input by hitting the **Create** button. The Overlay IP address is generated by the system.

   If the appliance already exists and you modify any data, click the **Update** button.

Also see how to configure:

- traffic redirection to an external gateway
- traffic redirection to a web security gateway
- traffic redirection to a cloud gateway
- traffic redirection to EdgeSentry

Configuring the B02 Branch Office appliance

In "Use Case 1", B02 is deployed in bridge/router mode. It is connected to the Data Center directly through the MPLS private network and over the Internet via one tunnel.

A second tunnel connects B02 to B01. For this reason, Port Forwarding must have been configured on the Internet Access router. This rule authorizes sending the UDP packets to the appliance on ports 500 (IKEv2) and 4500 (IPsec NAT Traversal). You must apply a static IP address to the B02 WAN2 interface.

B02 is also connected to an external gateway as explained in Use Case 11.

- "Identifying the appliance"
- "Configuring the LAN"
- "Configuring the WAN(s)"

Identifying the appliance

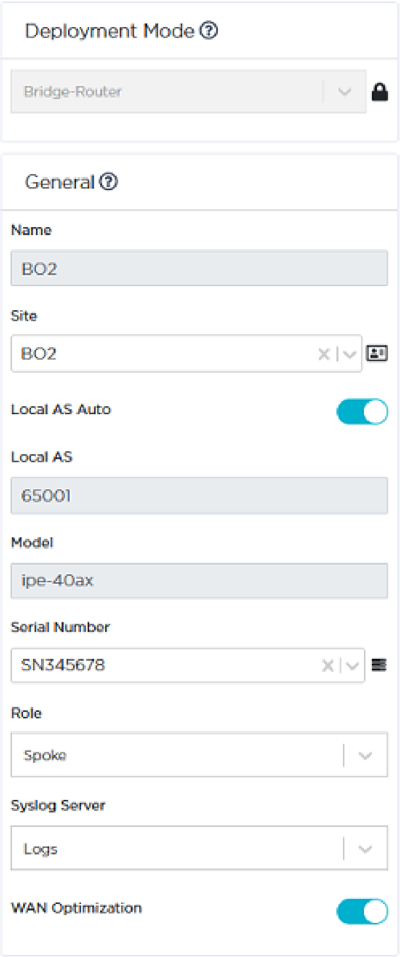
Identifying an auto-provisioned appliance

After the B02 appliance with the 'SN345678' Serial Number (and its Model/Version information) has been automatically provisioned in the SD-WAN Orchestrator from the ZTP Server, as indicated via the ≣ sign, it appears under the 'Not Configured' tab of the Network -> Configuration window.

Proceed as follows to identify and further configure the appliance (refer to "Use Case 1").

1 In the Network -> Configuration window, click ✎ to edit the appliance.

2 In the **Deployment Mode** panel, select the Bridge-Router option and hit the 🔓 icon to enable the related panels and functions of the interface.



Deployment Mode

Bridge-Router

General

Name: BO2

Site: BO2

Local AS Auto: on

Local AS: 65001

Model: ipe-40ax

Serial Number: SN345678

Role: Spoke

Syslog Server: Logs

WAN Optimization: on

3 In the General panel, enter the **Name** of the appliance as well as the name of the related **Site** (B02)**.**

The 🪪 button at the right of the Site Name enables you to display the Site subnets.

4 Select the **Auto** option of the Local AS parameter. The related field is automatically populated with a number selected by the Orchestrator from the **AS Number Range** you have specified in the Overlay Routing panel of the Advanced Configuration window.

This parameter is used in B02 WAN3 for tunnel mapping between this Site and the other Sites it will be connected to (Data Center and B01).

5 Through the **Role** field, define the appliance as a Spoke since it identifies a Branch Office appliance (generates tunnel requests on L3 interfaces). Tunnels are always built from the spokes to the hub.

6 Since NATted DTI traffic is enabled on the WAN3 interface, select the Syslog Server you defined in "Advanced Configuration" to enable log export.

7 WAN Optimization is activated by default on this appliance if the matching license is available.

Serial Number Format

The Serial Numbers provided as examples in the use cases of the current documentation are virtual. To know how to identify the type of any appliance through its Serial Number, refer to "General Rules"

Identifying an appliance in the SD-WAN Orchestrator only

You may identify an appliance in the SD-WAN Orchestrator even if it is still unprovisioned, in order to configure it in advance.

1. In the General panel, enter the **Name** of the appliance as well as the name of the related **Site** (B02)**.**

   The ▤ button at the right of the Site Name enables you to display the Site subnets.

2. Select the **Auto** option of the Local AS parameter. The related field is automatically populated with a number selected by the Orchestrator from the **AS Number Range** you have specified in the Overlay Routing panel of the Advanced Configuration window.
3. Enter the appliance Serial Number (Create "SN"). The ▤ sign means that this appliance is not defined on the ZTP Server and consequently is not operational in your network.
4. Through the **Role** field, define the appliance as a Spoke since it identifies a Branch Office appliance.
5. Since NATted DTI traffic is enabled on the WAN3 interface, select the Syslog Server you defined in "Advanced Configuration" to enable log export.
6. WAN Optimization is activated by default on this appliance if the matching license is available.

As soon as the appliance is provisioned on ZTP, you only need to update its Serial Number in the SD-WAN Orchestrator.

Also see how to identify a Data Center appliance.

Configuring the LAN

As a second step, configure the B02 appliance LAN which includes two physical interfaces in multi-path mode. Refer to "Use Case 1" diagram where the LAN information is displayed in blue.

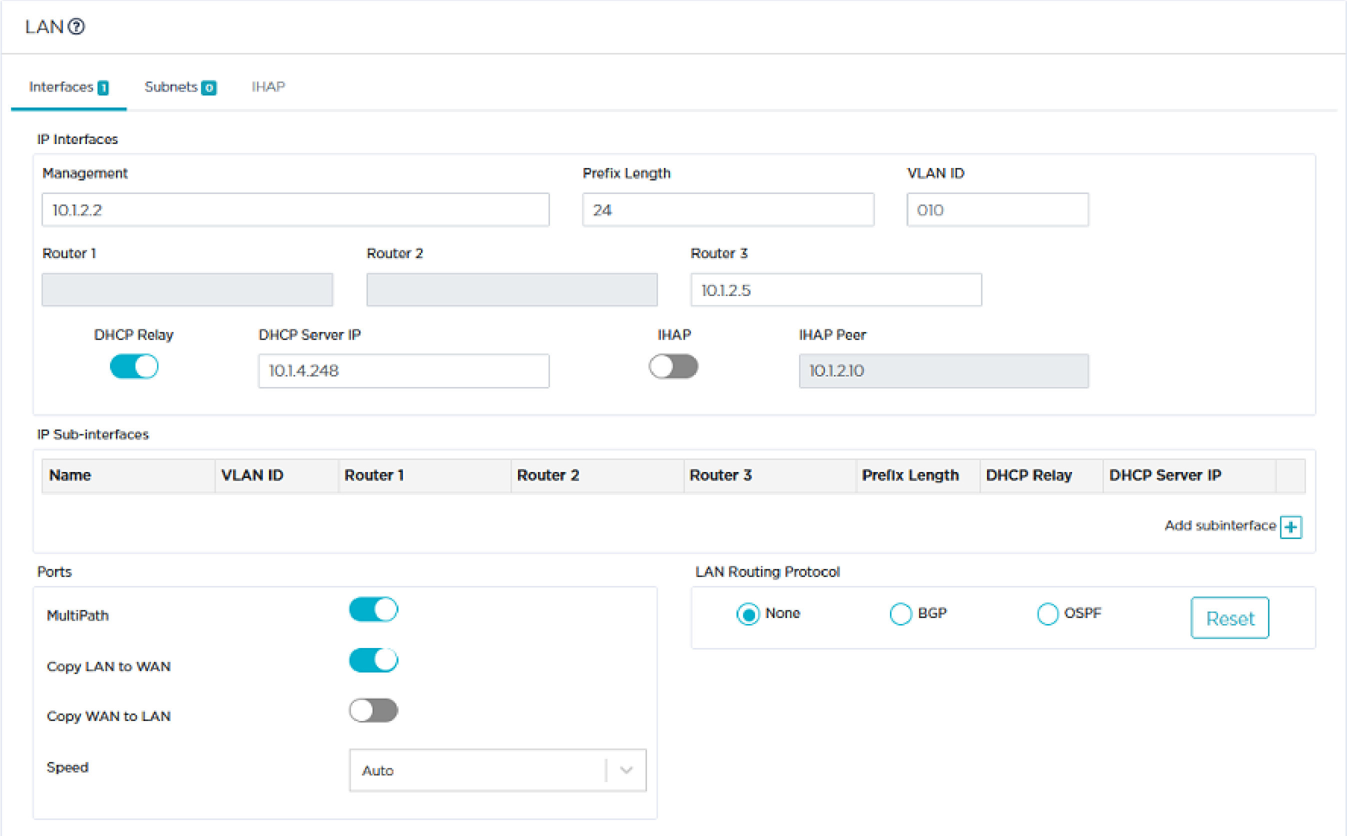
1 Click the **Interfaces** tab.

2 Enter the appliance Management IP address (10.1.2.2), Prefix Length (24).

The Management IP address is used for communicating with other appliances, the ZTP Server and the Orchestrator.

3 Use the default **Auto Generated** option to let the system allocate LAN addresses automatically to the Routers (Router X IP = Management IP + X) linked to the WANs in Router mode that you will configure for this appliance. Also refer to "IP Address allocation".

In this example, only Router 3 IP address will be automatically defined as it corresponds to WAN3 in Router mode - see the result image below.



LAN

Interfaces 1 | Subnets 0 | IHAP

IP Interfaces

Management: 10.1.2.2

Prefix Length: 24

VLAN ID: 010

Router 1:

Router 2:

Router 3: 10.1.2.5

DHCP Relay: on

DHCP Server IP: 10.1.4.248

IHAP: off

IHAP Peer: 10.1.2.10

IP Sub-interfaces

Name	VLAN ID	Router 1	Router 2	Router 3	Prefix Length	DHCP Relay	DHCP Server IP

Add subinterface +

Ports

MultiPath: on

Copy LAN to WAN: on

Copy WAN to LAN: off

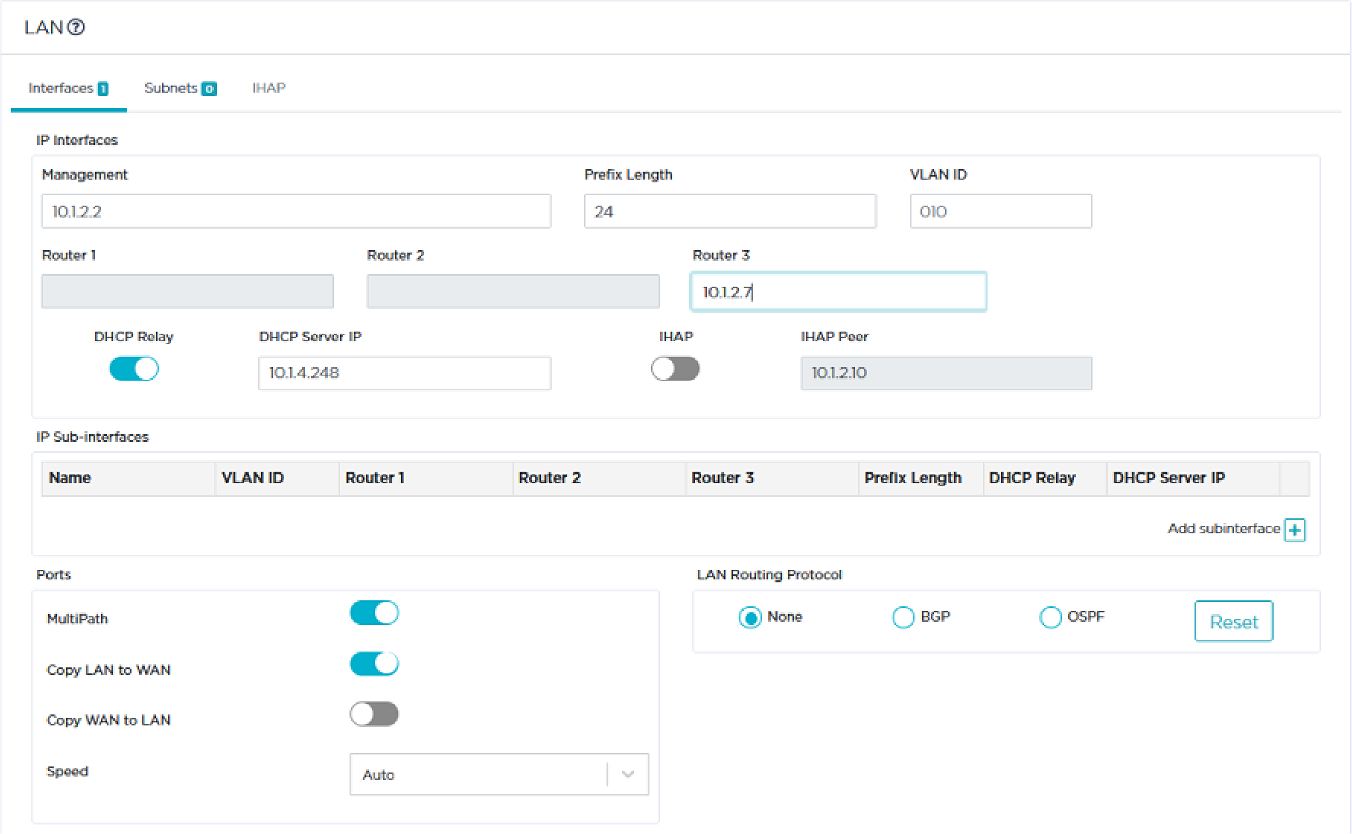
Speed: Auto

LAN Routing Protocol

● None ○ BGP ○ OSPF

Reset

Note that you can also configure the IP addresses of the Routers manually inside the Management IP subnet, by deselecting the Auto Generated option. Accordingly, in this example, you would type in (or modify) the IP address of Router 3.



LAN

Interfaces 1 | Subnets 0 | IHAP

IP Interfaces

Management	Prefix Length	VLAN ID
10.1.2.2	24	010

Router 1	Router 2	Router 3
		10.1.2.7

DHCP Relay	DHCP Server IP	IHAP	IHAP Peer
On	10.1.4.248	Off	10.1.2.10

IP Sub-interfaces

Name	VLAN ID	Router 1	Router 2	Router 3	Prefix Length	DHCP Relay	DHCP Server IP

Add subinterface +

Ports

MultiPath	On
Copy LAN to WAN	On
Copy WAN to LAN	Off
Speed	Auto

LAN Routing Protocol

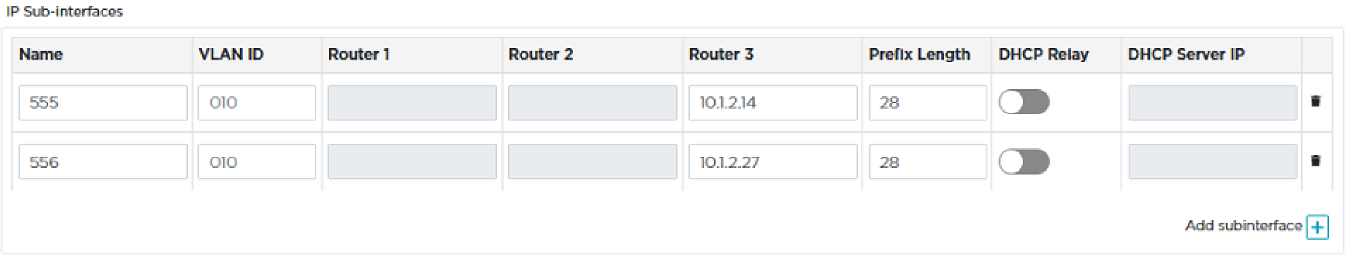
● None ○ BGP ○ OSPF Reset

4 Enable the DHCP Relay function and enter the DHCP Server Address (10.1.4.248). DHCP requests from the B02 appliance are propagated to the DHCP Server in the Data Center LAN.

5 In the current example, do not enter any VLAN ID. Note that the grey values appearing in some fields of the interface are only given as examples and are not taken into account in the configuration.

Moreover, if you define any additional VLAN IDs, you must assign a LAN sub-interface to every Router of the VLAN IDs. DHCP parameters are optional.

When sub-interfaces are added, the number of interfaces is incremented on the tab.



IP Sub-interfaces

Name	VLAN ID	Router 1	Router 2	Router 3	Prefix Length	DHCP Relay	DHCP Server IP
555	010			10.1.2.14	28	Off	
556	010			10.1.2.27	28	Off	

Add subinterface +

6 Enable the MultiPath mode. It implements two traffic paths: from LAN1 to WAN1 and from LAN2 to WAN2.

Note that since WAN3 is a Router L3 interface, Dynamic WAN Selection is used.

7. Enable the Copy LAN to WAN function to copy the state of the LAN to its related WAN. The LAN1/WAN1 or LAN2/WAN2 state synchronization is useful when the LAN interface breaks down.
8. Leave the Speed parameter to Auto to let the system define the speed of the LAN interfaces, or you can force the speed to 100FD or 1000FD. The full duplex speed is expressed in megabits per second.
9. Since there is no router in the B02 LAN for exchanging routing tables, there is no additional subnet or sub-interface to define for configuring BGP peering (refer to "Configuring BGP") or OSPF adjacencies (refer to "Configuring OSPF").

   If there was a router in the B02 LAN, the prerequisites for using OSPF would be the following:

   - deactivating MultiPath
   - configuring the Core Router with two OSPF processes and no route redistribution between the processes. The first process would be between the Core Router and the appliance router; the second process would be established between the Core Router and the MPLS CE Router.

Also see how to configure:

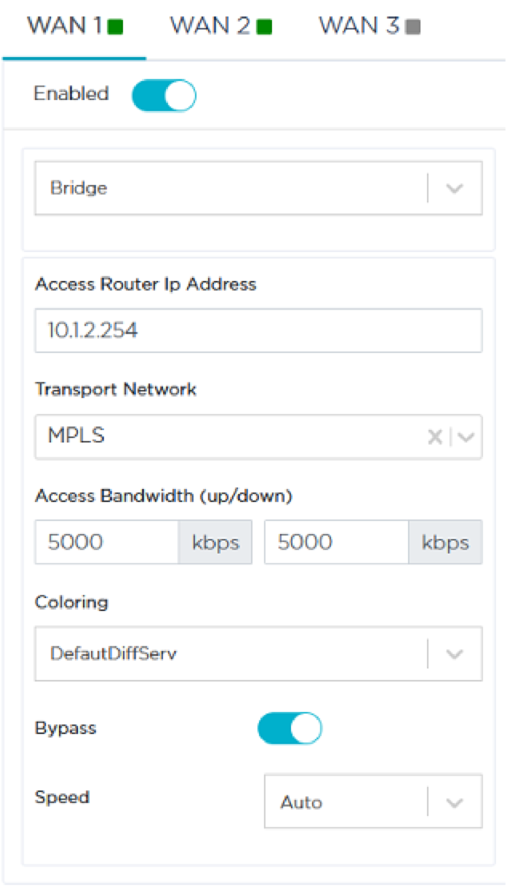
- a Data Center LAN

Configuring the WAN(s)

As a third step, configure the three WANs linked to the B02 appliance: 2 MPLS and 1 Internet.

> **Warning:** To configure a hybrid appliance, always start configuring the first WAN(s) in bridge mode (because of the Bypass function which is activated by default).

Refer to "Use Case 1" diagram where WAN1 (MPLS) details are displayed in green.



Enabled ●

Bridge

Access Router Ip Address: 10.1.2.254

Transport Network: MPLS

Access Bandwidth (up/down): 5000 kbps 5000 kbps

Coloring: DefautDiffServ

Bypass ●

Speed: Auto

1 Activate the WAN through the ● icon. You may now enter field data.

2 Select the **Bridge** option for this L2 interface.

3 Enter the CE router IP Address, 10.1.2.254. It must correspond to the LAN Interface IP Address.

4 As you already defined the 'MPLS' type of Transport Network for the Data Center WAN2, select it from the stack.

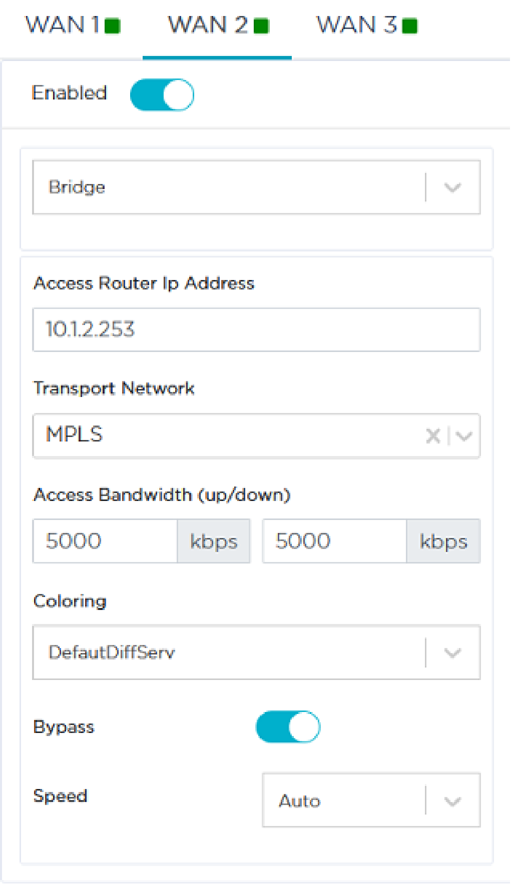
5 In the Access Bandwidth fields, define the up and down throughput (in kilobits per second) allocated to the WAN: 5000.

6 Select from the Coloring stack of values any Coloring Policy you previously configured through the Applications -> Configuration -> System Provisioning -> Coloring function (in this example, the default Coloring Policy for the DiffServ service). Refer to "Configuring Coloring".

7 The Bypass option is activated by default, i.e. the system will bypass the traffic in case of failure (e.g. power failure). When bypass is executed, services such as Visibility, Control, Optimization etc. are of course disabled.

8 Leave the Speed parameter to Auto to let the system define the speed of the interface, or you can force the speed to 100FD or 1000FD. The full duplex speed is expressed in megabits per second.

Refer to "Use Case 1" diagram where WAN2 (MPLS) details are displayed in green.



WAN 1 🟩 WAN 2 🟩 WAN 3 🟩

Enabled ●

Bridge

Access Router Ip Address: 10.1.2.253

Transport Network: MPLS

Access Bandwidth (up/down): 5000 kbps 5000 kbps

Coloring: DefautDiffServ

Bypass ●

Speed: Auto

1 Activate the WAN through the ● icon. You may now enter field data.

2 Select the **Bridge** option for this L2 interface.

3 Enter the CE router IP Address, 10.1.2.253. It must correspond to the LAN Interface IP Address.

4 Select the 'MPLS' type of Transport Network.

5 In the Access Bandwidth fields, define the up and down throughput (in kilobits per second) allocated to the WAN: 5000.

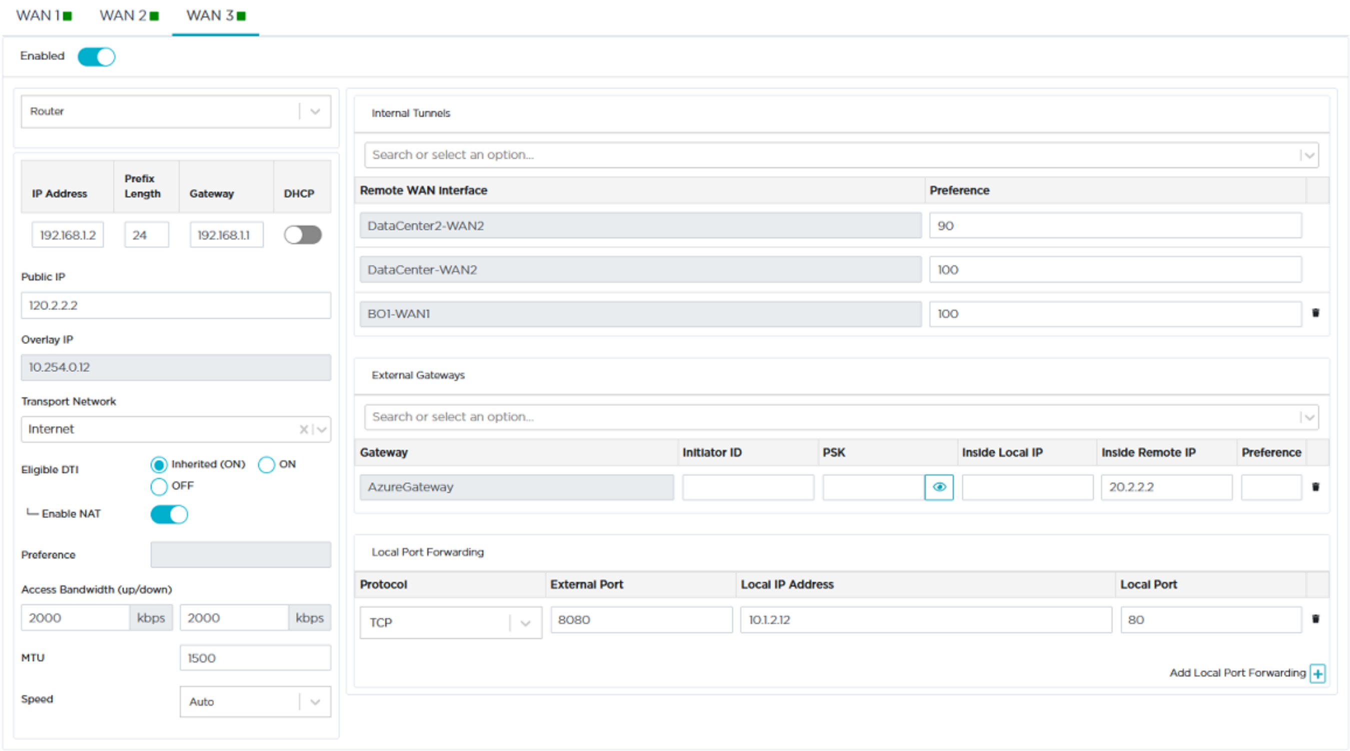
6 Select from the Coloring stack of values any Coloring Policy you previously configured through the Applications -> Configuration -> System Provisioning -> Coloring function (in this example, the default Coloring Policy for the DiffServ service). Refer to "Configuring Coloring".

7 The Bypass option is activated by default, i.e. the system will bypass the traffic in case of failure (e.g. power failure). When bypass is executed, services such as Visibility, Control, Optimization etc. are of course disabled.

8 Leave the Speed parameter to Auto to let the system define the speed of the interface, or you can force the speed to 100FD or 1000FD. The full duplex speed is expressed in megabits per second.

> **Note:** Since both WAN1 and WAN2 are configured with MPLS as Transport Network and because DWS is used, MPLS traffic will be sent to the best of these two WANs.

Refer to "Use Case 1" diagram where WAN3 (Internet) details are displayed in orange.



Enabled ●

Router

IP Address	Prefix Length	Gateway	DHCP
192.168.1.2	24	192.168.1.1	○

Public IP: 120.2.2.2

Overlay IP: 10.254.0.12

Transport Network: Internet

Eligible DTI: ● Inherited (ON) ○ ON ○ OFF

└ Enable NAT ●

Preference:

Access Bandwidth (up/down): 2000 kbps 2000 kbps

MTU: 1500

Speed: Auto

Internal Tunnels

Search or select an option...

Remote WAN Interface	Preference
DataCenter2-WAN2	90
DataCenter-WAN2	100
BO1-WAN1	100

External Gateways

Search or select an option...

Gateway	Initiator ID	PSK	Inside Local IP	Inside Remote IP	Preference
AzureGateway				20.2.2.2	

Local Port Forwarding

Protocol	External Port	Local IP Address	Local Port
TCP	8080	10.1.2.12	80

Add Local Port Forwarding +

1 Activate the WAN through the ● icon. You may now enter field data.

2 Select the **Router** option for this L3 interface.

3 Do not activate the DHCP function to proceed with Step 4.

4 Enter the WAN3 interface static information, 192.168.1.2 as IP Address, 24 as Prefix length. This address must be static to enable the configuration of Port Forwarding on the Internet Access router.

5 Enter the Default Gateway: 192.168.1.1

6 Define the Public IP address (120.2.2.2) which corresponds to the WAN side of the Internet Access router to which the WAN3 interface is connected. The Port Forwarding configuration of the Internet Access router enables this device to send the UDP packets to the appliance WAN3 on ports 500 (IKEv2) and 4500 (IPsec NAT Traversal). The Internet Access router also modifies the Egress packets in order to replace its 120.2.2.2 public address with the 192.168.1.2 WAN3 static address as destination address.

7 As you already defined the 'Internet' type of Transport Network for the Data Center and B01 WANs, select it from the stack.

When configuring a WAN for the first time, type the name of the network you are connected to, 'Internet' in the current example. Clearly identify each name through customization. Once a Transport Network type has been defined, you can select it from the stack when configuring subsequent WANs.

8 This interface is automatically eligible to DTI (Inherited ON) because you globally activated this policy for the 'Internet' Transport Network (refer to Advanced Configuration -> Transport Network Settings). You may also manage DTI individually for this Internet L3 interface by checking the ON or OFF options.

9 Directly derived from the activated Eligible DTI option, keep the Enable NAT mode activated. This is a source-NAT where the Management IP address (10.1.2.2) is replaced with the 192.168.1.2 WAN3 IP address. This NAT only applies to the traffic sent over the Internet. The traffic to the Data Center and to other Sites is transferred through the IPsec tunnels.

If you deactivate the Enable NAT mode which controls the firewall, incoming connections from the WAN are allowed to go to the LAN.

10 The Preference parameter is not available for a Spoke appliance.

11 In the Access Bandwidth fields, define the up and down throughput (in kilobits per second) allocated to the WAN: 2000.

12 Enter the MTU value which corresponds to the maximum number of bytes loaded in the Payload. The default value is 1500.

13 Leave the Speed parameter to Auto to let the system define the speed of the interface, or you can force the speed to 100FD or 1000FD. The full duplex speed is expressed in megabits per second.

14 The Internal Tunnels stack of values contains the remote WAN interfaces automatically detected by the Orchestrator (DataCenter-WAN2). Since you also connected the current appliance to the B01 appliance, the additional 'B01-WAN1' remote WAN interface is

automatically specified in the list of interfaces and enables you to validate the tunnel between B02 and B01. See "Configuring the WAN" for the B01 appliance.

15 The External Gateways panel is used to connect this WAN interface to a configured External Gateway. Refer to "Configuring traffic redirection to an External Gateway".

16 Define Local Port Forwarding by selecting the TCP Protocol, typing 8080 as External Port, 10.1.2.12 as the Local IP Address and 80 which is the generally used Local Port for HTTP traffic.

17 Validate your input by hitting the **Create** button. The Overlay IP address is generated by the system as soon as the tunnel is created.

If the appliance already exists and you modify any data, click the **Update** button.

Also see how to configure:

- Data Center appliance WANs
- traffic redirection to an external gateway
- traffic redirection to a web security gateway
- traffic redirection to a cloud gateway
- traffic redirection to EdgeSentry

Configuring the B03 Branch Office appliance

B03 is deployed in bridge mode and is connected to the Data Center through the MPLS private network.

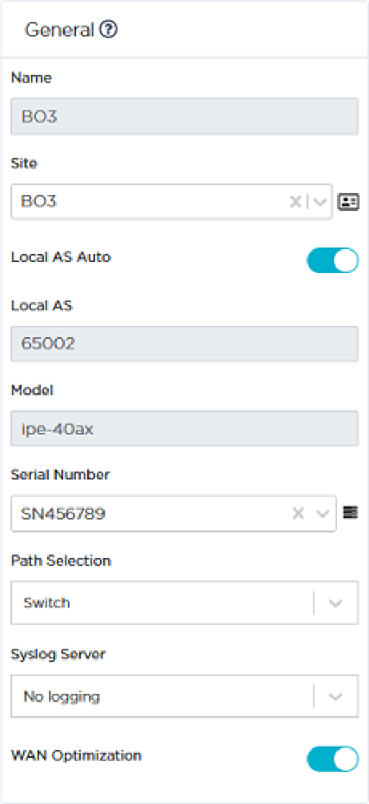
Identifying the appliance

After the B03 appliance with the 'SN456789' Serial Number (and its Model/Version information) has been automatically provisioned in the SD-WAN Orchestrator from the ZTP Server, as indicated via the ≣ sign, it appears under the 'Not Configured' tab of the Network -> Configuration window.

Proceed as follows to identify and further configure the appliance.

1 In the Network -> Configuration window, click ✎ to edit the appliance.

2 In the Deployment Mode panel, select the **Bridge** option and hit the 🔓 icon to enable the related panels and functions of the interface.



General ⓘ

Name: B03

Site: B03

Local AS Auto: ●

Local AS: 65002

Model: ipe-40ax

Serial Number: SN456789 ≣

Path Selection: Switch

Syslog Server: No logging

WAN Optimization: ●

3 In the General panel, enter the **Name** of the appliance as well as the name of the related **Site** (B03)**.**

The 🪪 button at the right of the Site Name enables you to display the Site subnets.

4 Select the **Auto** option of the Local AS parameter. The related field is automatically populated with a number selected by the Orchestrator from the **AS Number Range** you have specified in the Overlay Routing panel of the Advanced Configuration window.

5 Path Selection is only available on a bridge appliance. In the current example, this parameter is not taken into account because B03 is not in multi-path mode.

The available options for this parameter are:

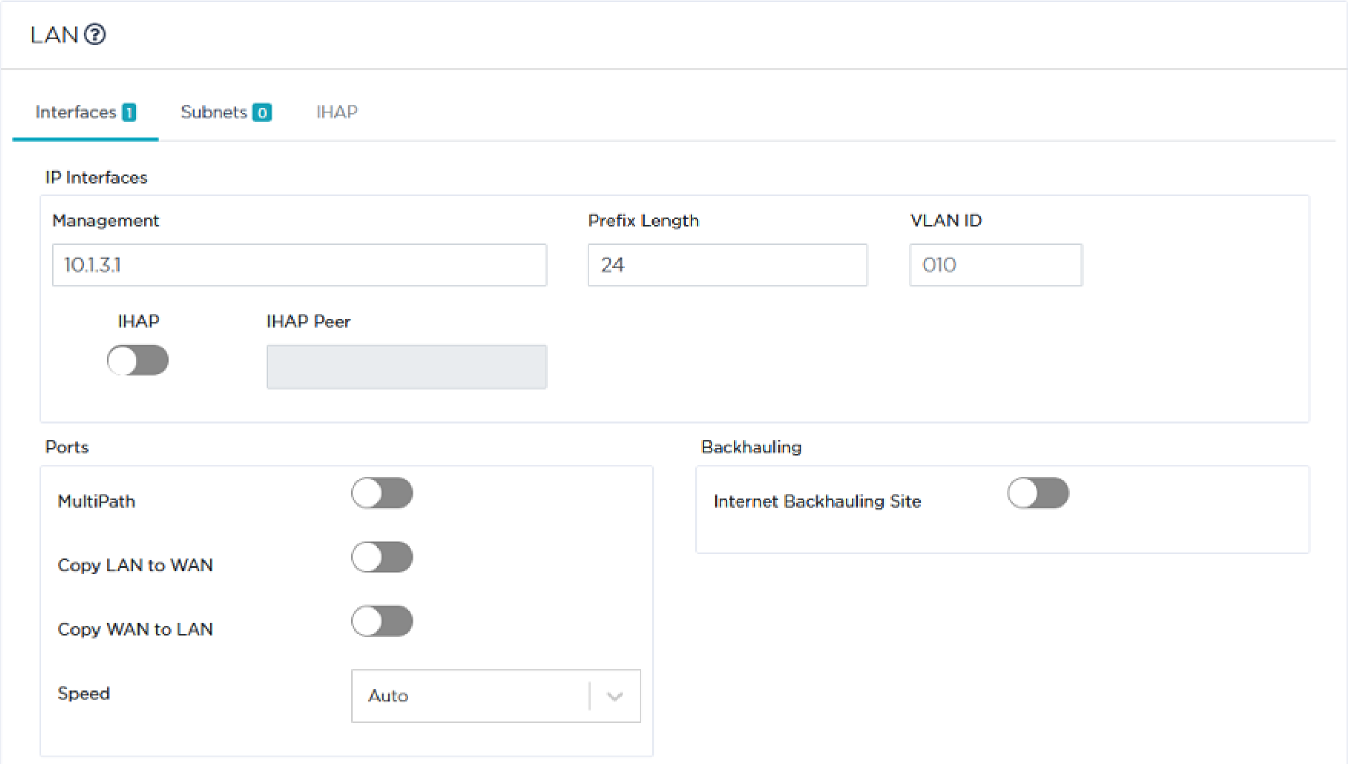
- Wire: traffic is automatically forwarded from LAN1 to WAN1 and from LAN2 to WAN2
- Switch: traffic is forwarded to the gateway physical address
- Dynamic: dynamic wan selection is applied

6 Do not specify any Syslog Server (related to DTI Eligibility). B03 appliance has only one Bridge (MPLS) interface which is not compatible with DTI.

7 WAN Optimization is activated by default on this appliance if the matching license is available.

Configuring the LAN

As a second step, configure the B03 appliance LAN which includes one physical interface. Refer to "Use Case 1" diagram where the LAN information is displayed in blue.



LAN ⓘ

Interfaces 1 Subnets 0 IHAP

IP Interfaces

Management: 10.1.3.1

Prefix Length: 24

VLAN ID: 010

IHAP: off

IHAP Peer:

Ports

MultiPath: off

Copy LAN to WAN: off

Copy WAN to LAN: off

Speed: Auto

Backhauling

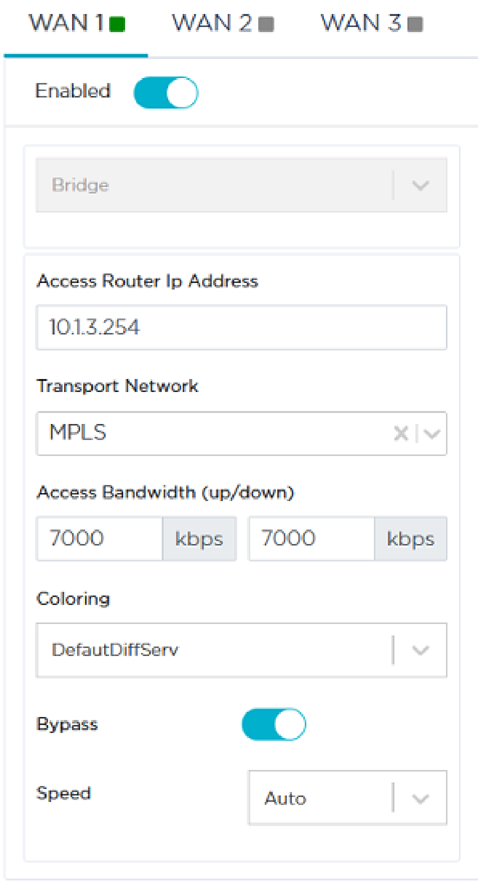
Internet Backhauling Site: off

1 Click the **Interfaces** tab.
2 Enter the appliance Management IP address (10.1.3.1), Prefix Length (24). The Management IP address is used for communicating with other appliances, the ZTP Server and the Orchestrator.
3 Leave all the other parameters to their default values.

You may define this Branch Office appliance as a Backhauling Site. This means it can receive Internet traffic through the underlay (MPLS) network.

Configuring the WAN

As a third step, configure the WAN linked to the B03 appliance: MPLS. Refer to "Use Case 1" diagram where WAN1 (MPLS) details are displayed in green.


WAN 1 🟩 WAN 2 ▨ WAN 3 ▨

Enabled

Bridge

Access Router Ip Address: 10.1.3.254

Transport Network: MPLS

Access Bandwidth (up/down): 7000 kbps 7000 kbps

Coloring: DefautDiffServ

Bypass

Speed: Auto

1 Activate the WAN through the icon. You may now enter field data.

2 Select the **Bridge** option for this L2 interface.
3 Enter the CE Router IP Address, 10.1.3.254. It must correspond to the Management IP Address.
4 As you already defined the 'MPLS' type of Transport Network for the Data Center WAN1 and B02 WAN1, select it from the stack.

5 In the Access Bandwidth fields, define the up and down throughput (in kilobits per second) allocated to the WAN: 7000.

6 Select from the Coloring stack of values any Coloring Policy you previously configured through the Applications -> Configuration -> System Provisioning -> Coloring function (in this example, the default Coloring Policy for the DiffServ service). Refer to "Configuring Coloring".

7 The Bypass option is activated by default, i.e. the system will bypass the traffic in case of failure (e.g. power failure). When bypass is executed, services such as Visibility, Control, Optimization etc. are of course not available.

8 Leave the Speed parameter to Auto to let the system define the speed of the interface, or you can force the speed to 100FD or 1000FD. The full duplex speed is expressed in megabits per second.

9 Validate your input by hitting the **Create** button. If the appliance already exists and you modify any data, click the **Update** button.

Configuring the B04 Branch Office RVC destination

B04 is a RVC destination, i.e. there is no SD-WAN appliance on the related Site.

The SD-WAN Orchestrator allows traffic of an unequipped Site to be measured and controlled by the appliances of the remote equipped Sites (B02 and B03 in "Use Case 1"). For this reason, B04 is called a RVC destination Site. Only one RVC destination is authorized per Site. A RVC destination is mainly identified by one or several LAN subnet(s).

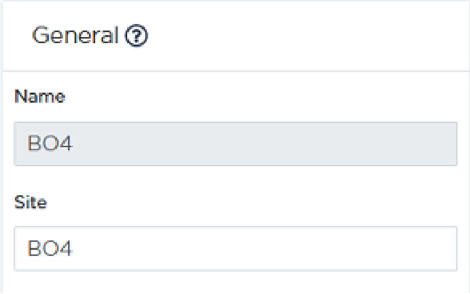
A group of remote appliances cooperate to measure the traffic (Application Visibility) and detect flow congestions (Application Control) of the RVC destination. Note that the following measurements are not done for a RVC:

- Delay/Jitter/Loss
- measurement and control of shadow traffic (traffic between RVC destination sites)
- end-to-end bandwidth tracking

Identifying the RVC destination

Since a RVC destination is never provisioned on the ZTP Server, you must configure it manually in the SD-WAN Orchestrator.

1 In the **Network -> Configuration** window, click Add RVC Destination



General

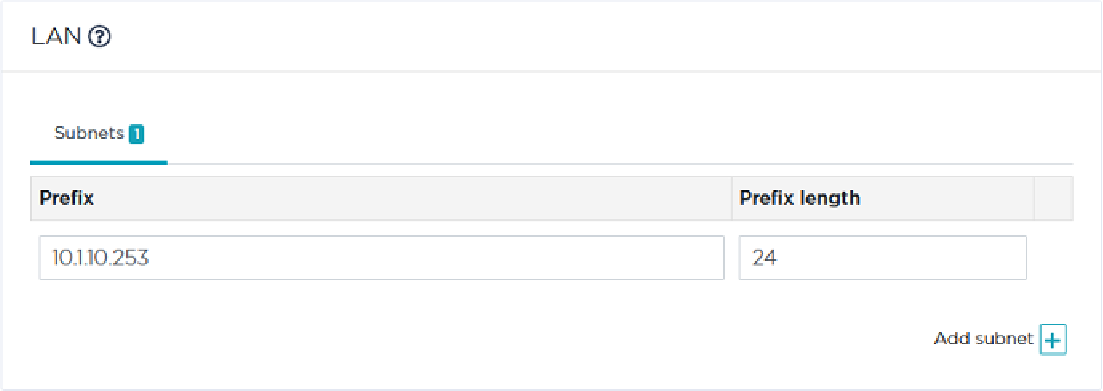
Name: B04

Site: B04

2 In the General panel, enter the **Name** of the RVC destination as well as the name of the related **Site** (B04)**.**

Configuring the LAN Subnet

As a second step, configure the LAN of the B04 RVC destination which includes one subnet at least. Refer to "Use Case 1" diagram where the LAN information is displayed in green.



LAN

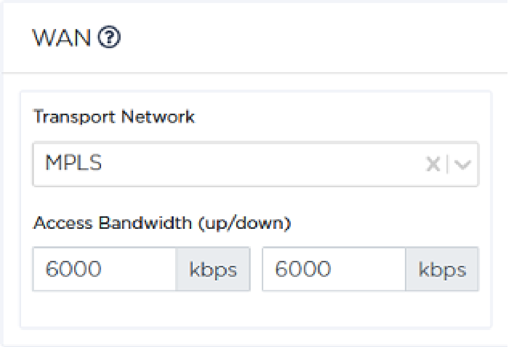
Subnets 1

Prefix	Prefix length
10.1.10.253	24

1 Enter the Subnet IP Address (10.1.10.253) and Prefix Length (24).

Configuring the WAN

As a third step, configure the unique WAN linked to the B04 RVC destination: MPLS.



WAN

Transport Network: MPLS

Access Bandwidth (up/down): 6000 kbps 6000 kbps

1 As you already defined the 'MPLS' type of Transport Network for the Data Center WAN1 and B02 WAN1, select it from the stack.

When configuring a WAN for the first time, type the name of the network you are connected to, 'MPLS' in the current example. Clearly identify each name through customization. Once a Transport Network type has been defined, you can select it from the stack when configuring subsequent appliance or RVC WANs.

Note that the 'Not Specified' option corresponds to any network or a combination of several networks.

2 In the Access Bandwidth fields, define the up and down throughput (in kilobits per second) allocated to the WAN: 6000.

3 Validate your input by clicking the **Create** button.

If the RVC destination already exists and you modify any data, click the **Update** button.

Also see how to configure:

- a Data Center appliance
- a Branch Office appliance

Checking the results of your Network Configuration

After a five minute delay during which the SD-WAN Orchestrator processes the last created or updated configuration, click the Extreme Networks logo in the interface top bar to display the Overview Dashboard.

The number of configured appliances and the number of created IPsec tunnels are specified. Check them with respect to Use Case diagrams.

Router Mode Standard Deployment

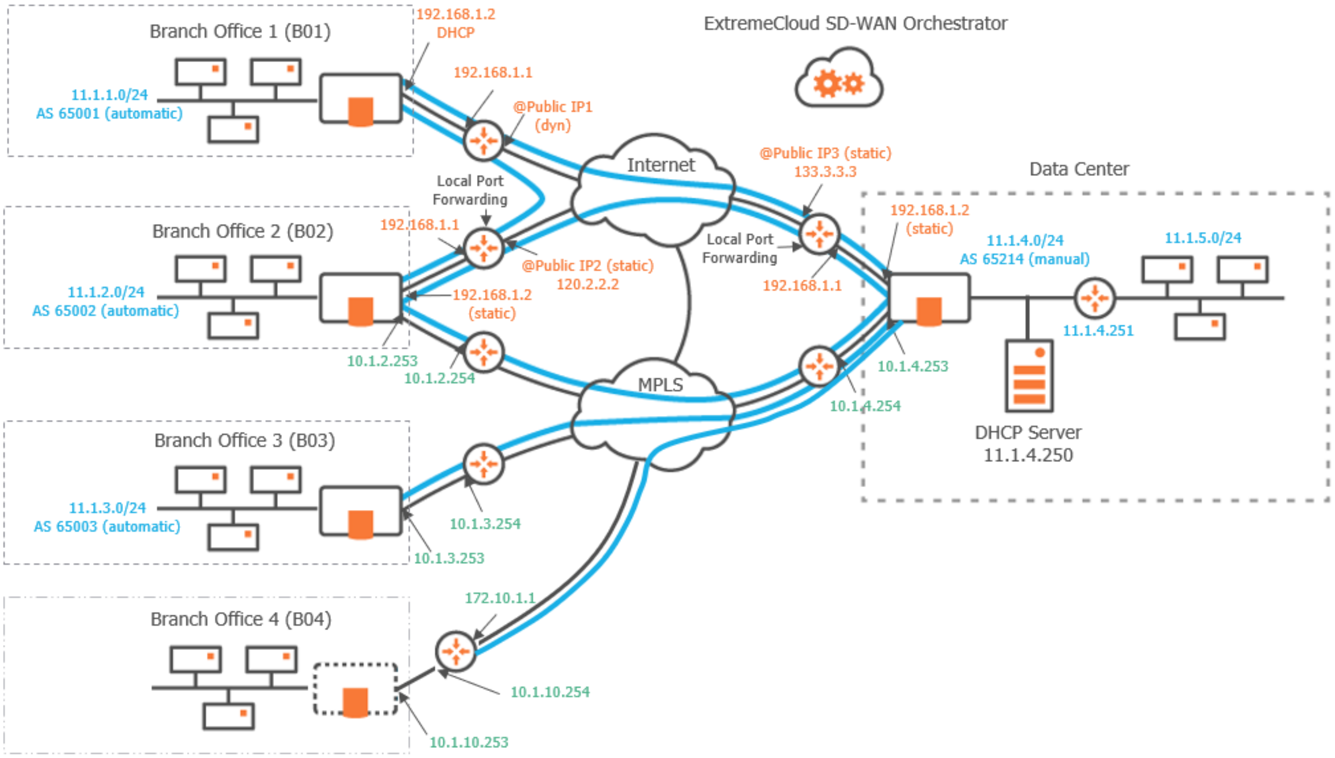
This section describes the main steps for configuring a Router Mode network. It is based on a typical use case illustrating a simple deployment where three branch office appliances are connected to a Data Center appliance over either the MPLS private network, or the Internet, or both. This deployment consists of configuring the appliances and creating IPsec tunnels.

A full Router Mode network includes appliances with WAN interfaces deployed in Router mode only. The SD-WAN Orchestrator enables you to build an overlay network of site connections through IPsec tunnels.

- B01 is connected to the Data Center through one tunnel over the Internet. Another tunnel connects B01 to B02.
- B02 is connected to the Data Center through two tunnels, one over the Internet and the other one over MPLS. A third tunnel connects B02 to B01.
- B03 is connected to the Data Center through one tunnel over the MPLS private network.
- B04 is a RVC destination managed by remote appliances; there is a tunnel from the B04 CE router to the Data Center appliance.

■ "Configuring the Data Center appliance"
■ "Configuring the Branch Office appliances"
■ "Advanced Configuration"

Use Case 2



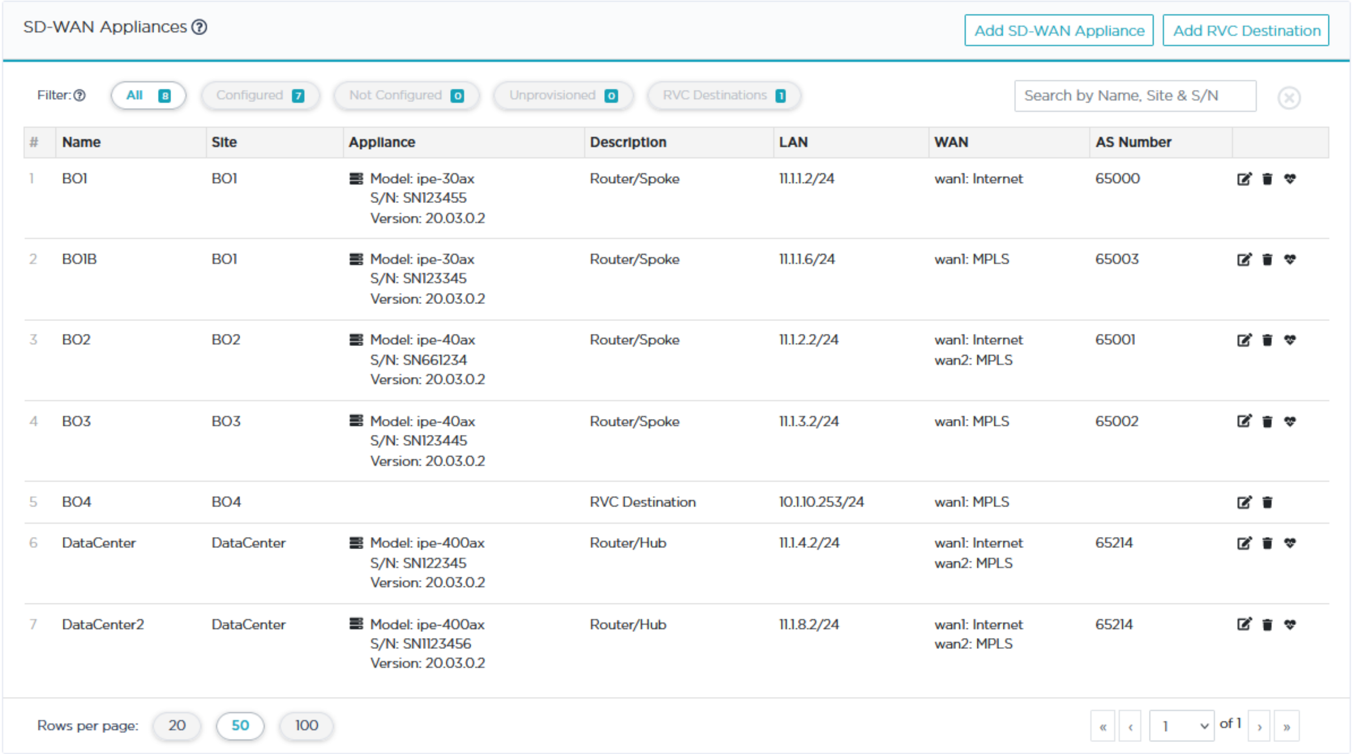
Graph legend

						Blue connection	Grey connection
SD-WAN appliance	router	RVC destination	subnet	host in a subnet	server	IPsec tunnel	physical connection between devices

Note: A router may be a CE Router (MPLS Router), an Internet Access Router or a Core Router.

Configuring the appliances

Refer to "Configuring the appliances" in the Hybrid Mode Standard Deployment section.



SD-WAN Appliances ?

#	Name	Site	Appliance	Description	LAN	WAN	AS Number
1	BO1	BO1	Model: ipe-30ax S/N: SN123455 Version: 20.03.0.2	Router/Spoke	11.1.1.2/24	wan1: Internet	65000
2	BO1B	BO1	Model: ipe-30ax S/N: SN123345 Version: 20.03.0.2	Router/Spoke	11.1.1.6/24	wan1: MPLS	65003
3	BO2	BO2	Model: ipe-40ax S/N: SN661234 Version: 20.03.0.2	Router/Spoke	11.1.2.2/24	wan1: Internet wan2: MPLS	65001
4	BO3	BO3	Model: ipe-40ax S/N: SN123445 Version: 20.03.0.2	Router/Spoke	11.1.3.2/24	wan1: MPLS	65002
5	BO4	BO4		RVC Destination	10.1.10.253/24	wan1: MPLS	
6	DataCenter	DataCenter	Model: ipe-400ax S/N: SN122345 Version: 20.03.0.2	Router/Hub	11.1.4.2/24	wan1: Internet wan2: MPLS	65214
7	DataCenter2	DataCenter	Model: ipe-400ax S/N: SN1123456 Version: 20.03.0.2	Router/Hub	11.1.8.2/24	wan1: Internet wan2: MPLS	65214

Configuring the Data Center appliance

In "Use Case 2", start configuring your network with the Data Center appliance.

This Data Center includes two subnets (11.1.4.0 and 11.1.5.0) and a DHCP Server.

There is also one prerequisite which is the necessary configuration of Port Forwarding on the Internet Access router. This rule authorizes sending the UDP packets to the appliance on ports 500 (IKEv2) and 4500 (IPsec NAT Traversal). For this reason, you must apply a static IP address to the Data Center WAN1 interface.

- "Identifying the appliance"
- "Configuring the LAN"
- "Configuring the WAN(s)"

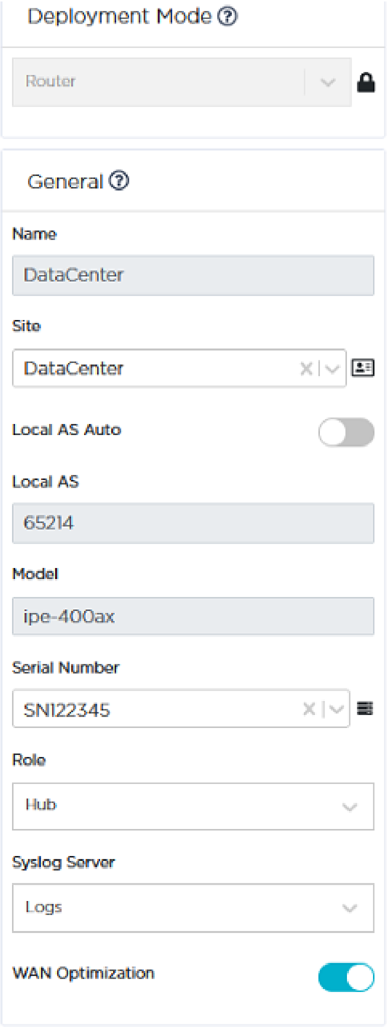
Identifying the appliance

After the Data Center appliance with the 'SN122345' Serial Number (and its Model/Version information) has been automatically provisioned in the SD-WAN Orchestrator from the ZTP Server, as indicated via the ≣ sign, it appears under the 'Not Configured' tab of the Network -> Configuration window.

Proceed as follows to identify and further configure the appliance.

1 In the Network -> Configuration window, click ✎ to edit the appliance.

2 In the **Deployment Mode** panel, select the Router option and hit the 🔓 icon to enable the related panels and functions of the interface.



Deployment Mode

Router

General

Name: DataCenter

Site: DataCenter

Local AS Auto: ○

Local AS: 65214

Model: ipe-400ax

Serial Number: SN122345

Role: Hub

Syslog Server: Logs

WAN Optimization: ●

3 In the General panel, enter the **Name** of the appliance as well as the name of the related **Site**.

4 Manually enter 65214 for the Local Autonomous System. It corresponds to the Autonomous System configured on the 11.1.4.251 router.

If you check the **Auto** option (not possible in the current Use Case), the related field is automatically populated with a number selected by the Orchestrator from the **AS Number Range** you have specified in the Overlay Routing panel of the Advanced Configuration window.

5 Through the **Role** field, define the appliance as a Hub since it identifies here a Data Center (receives tunnel requests). A spoke corresponds to a Site appliance (generates tunnel requests). Tunnels are always built from the spokes to the hub.

6 Since NATted DTI traffic is enabled on the WAN1 interface, select the Syslog Server you defined in "Advanced Configuration" to enable log export.

7 WAN Optimization is activated by default on this appliance if the matching license is available.

Also see how to identify:

- a Branch Office appliance

Configuring the LAN

As a second step, configure the Data Center LAN which includes one physical interface.

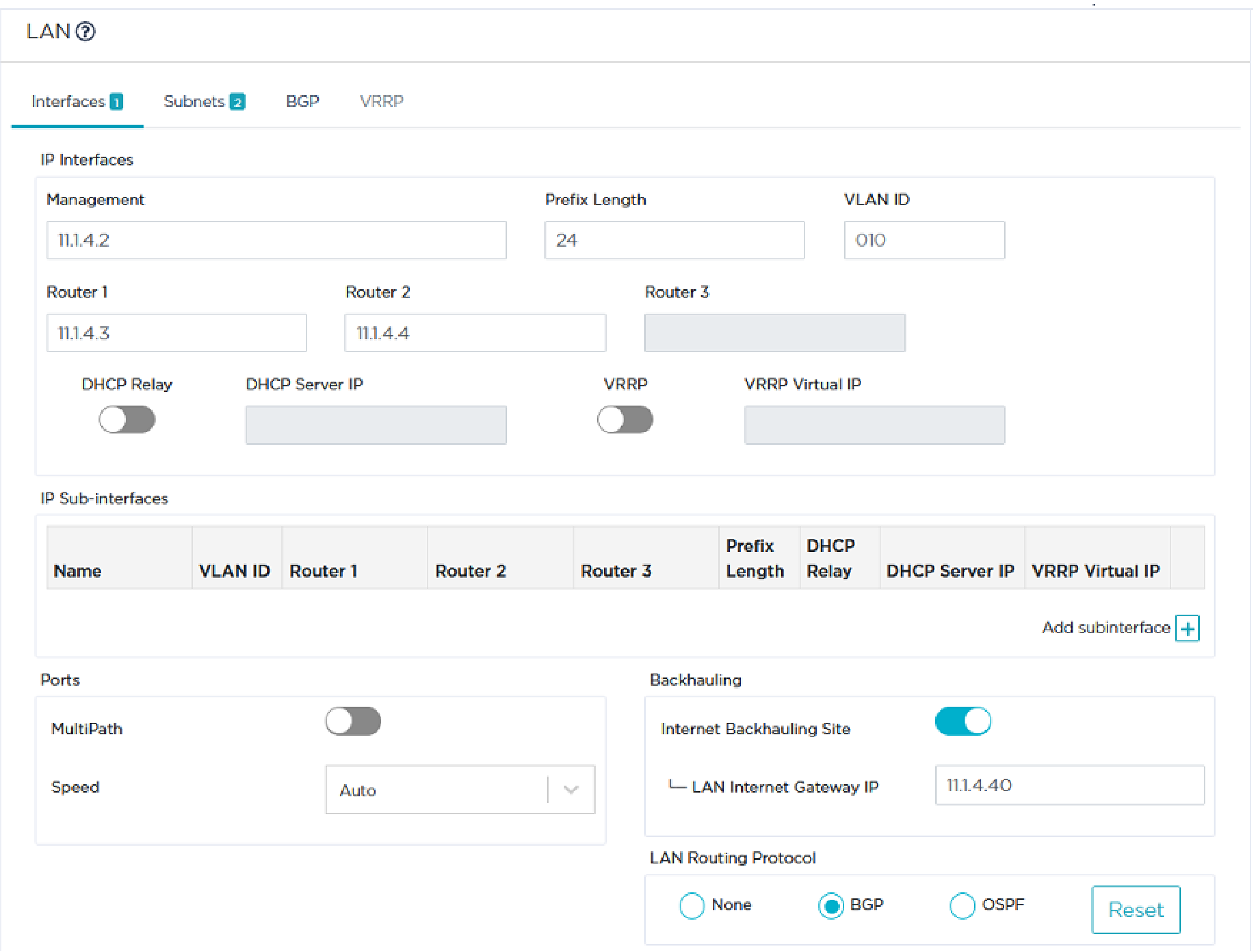
Refer to "Use Case 2" diagram where the LAN information is displayed in blue.

1. Click the **Interfaces** tab.
2. Enter the appliance Management IP address (11.1.4.2), Prefix Length (24).

   The Management IP address is used for communicating with other appliances, the ZTP Server and the Orchestrator.
3. Use the default **Auto Generated** option (creation window only) to let the system allocate LAN addresses automatically to the Routers (Router X IP = Management IP + X) linked to the WANs that you will configure for this appliance. Also refer to "IP Address allocation".

   In this example, Router 1 and Router 2 IP addresses will be automatically defined as they respectively correspond to WAN1 and WAN2.
4. Do not activate the DHCP Relay function since the Data Center hosts can directly access the DHCP Server. The appliance does not need to relay host requests.
5. Do not enter any VLAN ID. Note that the grey values appearing in some fields of the interface are only given as examples and are not taken into account in the configuration.
6. Do not use High Availability.
7. Leave the Speed parameter to Auto to let the system define the speed of the interface, or you can force the speed to 100FD or 1000FD. The full duplex speed is expressed in megabits per second.
8. Define this Data Center hub appliance as a Backhauling Site. This means it can receive Internet traffic through the overlay and route it to a firewall in the LAN: specify the LAN Internet Gateway IP address as 11.1.4.40
9. Select BGP as LAN Routing Protocol.

The following window displays the validated settings.



IP Interfaces

Management: 11.1.4.2
Prefix Length: 24
VLAN ID: 010

Router 1: 11.1.4.3
Router 2: 11.1.4.4
Router 3:

DHCP Relay: off
DHCP Server IP:
VRRP: off
VRRP Virtual IP:

IP Sub-interfaces

Name	VLAN ID	Router 1	Router 2	Router 3	Prefix Length	DHCP Relay	DHCP Server IP	VRRP Virtual IP

Ports

MultiPath: off
Speed: Auto

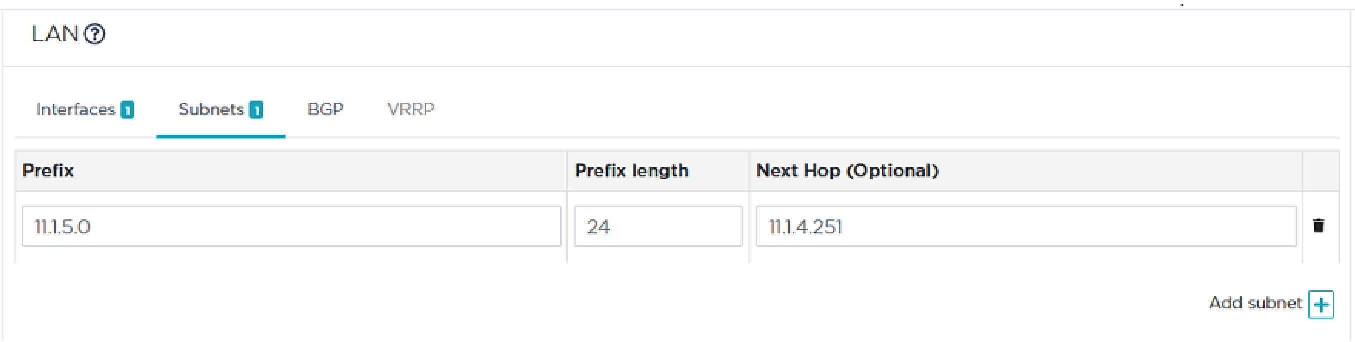
Backhauling

Internet Backhauling Site: on
└ LAN Internet Gateway IP: 11.1.4.40

LAN Routing Protocol

○ None ● BGP ○ OSPF

Defining additional Subnets



Prefix	Prefix length	Next Hop (Optional)
11.1.5.0	24	11.1.4.251

In Use Case 2, there is one additional subnet you must specify because the system is unable to detect it automatically. Subnets enable you to classify, measure and control the traffic coming from and going to specific hosts and servers.

10 Click the **Subnets** tab and the Add subnet icon +.

11 Define the additional subnet by entering its prefix (11.1.5.0), prefix length (24) and next hop (11.1.4.251). The Next Hop field enables you to define the route from the BGP local peer router (see below) to the Data Center in the private area of the network, where addresses are not NATted and cannot be identified automatically.

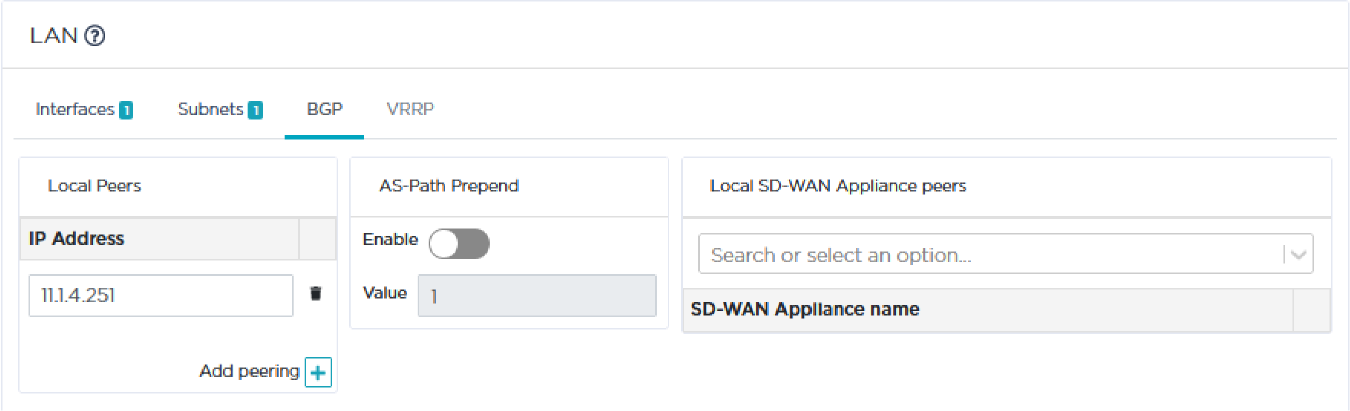
> **Note:** The Next Hop field is optional and you can leave it empty if you enable BGP or OSPF.

Also note that the number of subnets is incremented on the tab.

12 The Data Center appliance exchanges its routing tables with the local router using **either BGP or OSPF**. Refer to the following procedures which are mutually exclusive.

Configuring BGP

The Data Center appliance exchanges its routing tables with the local router using BGP.



LAN ⓘ

Interfaces 1 | Subnets 1 | BGP | VRRP

Local Peers

IP Address	
11.1.4.251	🗑

Add peering +

AS-Path Prepend

Enable ○

Value 1

Local SD-WAN Appliance peers

Search or select an option...

SD-WAN Appliance name	

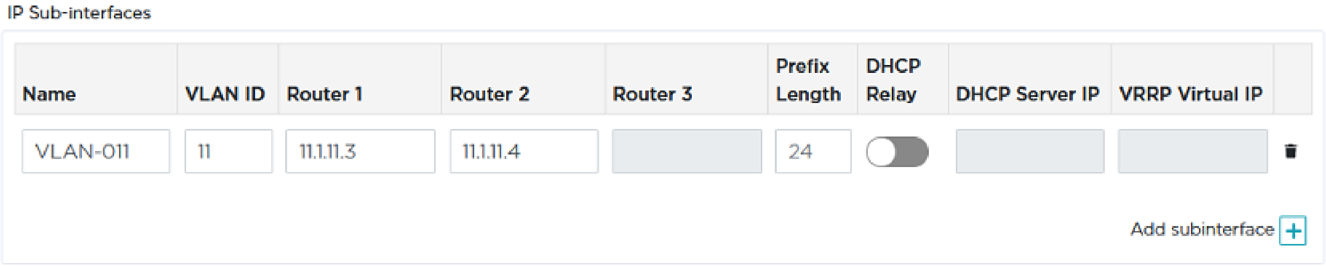
1 Click the **BGP** tab and the Add peering icon +.

2 Enter the IP address of the BGP local peer (11.1.4.251).

Configuring OSPF

1 In the Interfaces window, select OSPF as the LAN Routing Protocol.

2 Click the Add subinterface icon +. Enter 11 as VLAN ID, 11.1.11.3 as the sub-interface IP address for Router 1, 11.1.11.4 as the sub-interface IP address for Router 2 and 24 as Prefix Length. Each VLAN corresponds to an OSPF network area.

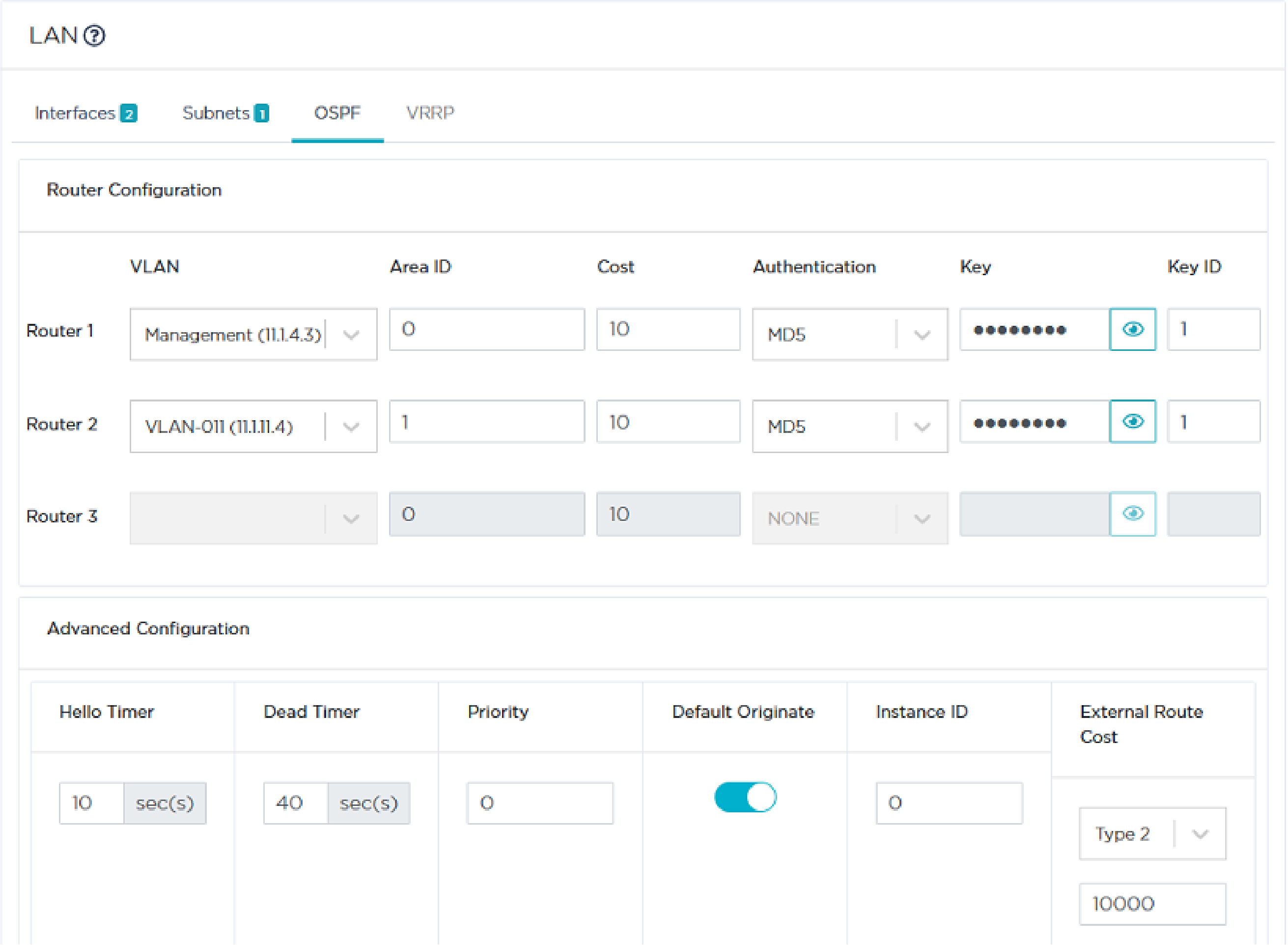


IP Sub-interfaces

Name	VLAN ID	Router 1	Router 2	Router 3	Prefix Length	DHCP Relay	DHCP Server IP	VRRP Virtual IP	
VLAN-011	11	11.1.11.3	11.1.11.4		24	○			🗑

Add subinterface +

3 Click the **OSPF** tab.



LAN ?

Interfaces 2 | Subnets 1 | OSPF | VRRP

Router Configuration

	VLAN	Area ID	Cost	Authentication	Key	Key ID
Router 1	Management (11.1.4.3)	0	10	MD5	●●●●●●●● 👁	1
Router 2	VLAN-011 (11.1.11.4)	1	10	MD5	●●●●●●●● 👁	1
Router 3		0	10	NONE	👁	

Advanced Configuration

Hello Timer	Dead Timer	Priority	Default Originate	Instance ID	External Route Cost
10 sec(s)	40 sec(s)	0	●	0	Type 2 10000

4 Configure Router 1 and Router 2 as follows:

- VLAN: for Router 1, select the 'None' option to take into account the ip address of the router. For Router 2, select VLAN ID 11 you defined in the previous step.
- Area ID: by default, Area 0 which is the backbone area or the core of the OSPF network. It corresponds to the area including the CE router. All other areas are connected to it and all the traffic between areas must traverse it.

  In this example, keep the 0 default value for Router 1 and enter 1 as Area 1 ID for Router 2.
- Cost: use the 10 default value which corresponds to the interface cost of Router 1 (11.1.4.3) and of Router 2 (11.1.4.4).
- Authentication: for each router, select one authentication method among MD5, SHA1, HMAC SHA256, HMAC SHA384 and HMAC SHA512. By default, there is no authentication (NONE option).
- Key: for each router, enter your authentication password. Use the 👁 icon different statuses to either display or hide the key.
- Key ID: for each router, enter 1 as the password identifier. This value must match the key ID of the Core Router password.

5 Specify OSPF Advanced Configuration parameters which are common to all the routers:

- Hello Timer: time between each Hello packet sent by the router to the interface(s). Hello packets enable the system to establish adjacencies and router keepalive messages to notify neighbors that links are up and active.
- Dead Timer: time after the last Hello packet is sent by a router and before the router is considered as dead. Dead Timer cannot be smaller than Hello Timer x 3.
- Priority: with the Broadcast network type (only network type supported), the network elects one Designated Router (DR) and one Backup Designated Router (BDR). They are in charge of transferring topology modifications to all the routers of the area. The priority mechanism determines which router is DR and which one is BDR.

  The router with the highest priority value is the DR router which is the main router for distributing the routes. If both DR and BDR routers have the same priority value, the router with the highest IP address is selected as the DR. In the current example, keep the 0 default value, i.e. this router is neither DR nor BDR (it does not participate in the election).
- Default Originate: only check this option if you want to redistribute a default route through OSPF.
- Instance ID: set this field to 0 to ensure this parameter is not currently used by routers.
- External Route Cost: select the Type 2 option and enter 10000. This parameter is also used for implementing high availability between two appliances. Refer to "Configuring a multi-appliance Hybrid Data Center through OSPF".

6 Click **Update**.

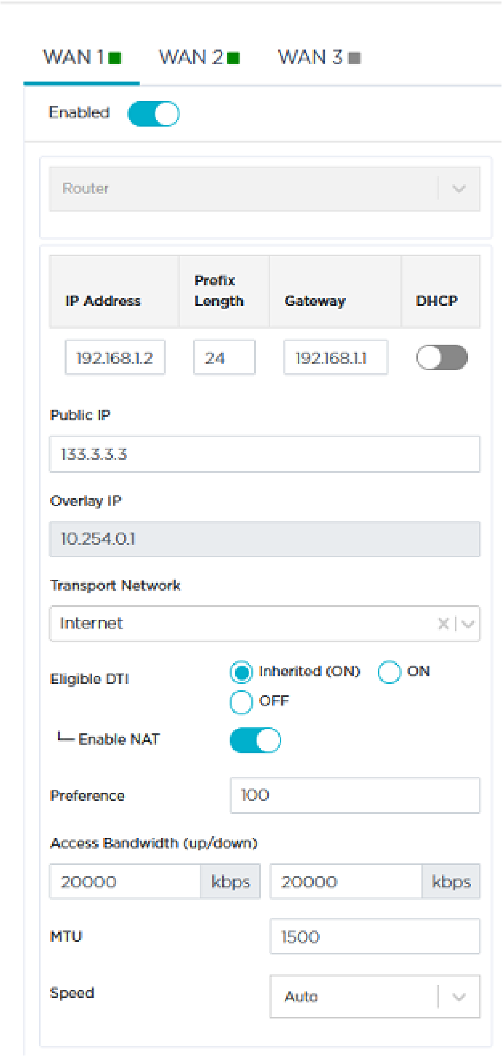
Also see how to configure:

- a multi-appliance Data Center
- a Branch Office appliance LAN
- a multi-appliance Branch Office Site

Configuring the WAN(s)

As a third step, configure the two WANs linked to the Data Center appliance: Internet and MPLS.

Refer to "Use Case 2" diagram where WAN1 (Internet) details are displayed in orange.



WAN 1 🟩 WAN 2 🟩 WAN 3 ■

Enabled ●

Router

IP Address	Prefix Length	Gateway	DHCP
192.168.1.2	24	192.168.1.1	○

Public IP: 133.3.3.3

Overlay IP: 10.254.0.1

Transport Network: Internet

Eligible DTI: ● Inherited (ON) ○ ON ○ OFF

└ Enable NAT ●

Preference: 100

Access Bandwidth (up/down): 20000 kbps 20000 kbps

MTU: 1500

Speed: Auto

1 Activate the WAN through the icon. You may now enter field data.

2 Select the **Router** option for this L3 interface.

3 Do not activate the DHCP function to proceed with Step 4.

4 Enter the WAN1 interface static information, 192.168.1.2 as IP Address, 24 as Prefix length. This address must be static to enable the configuration of Port Forwarding on the Internet Access router.

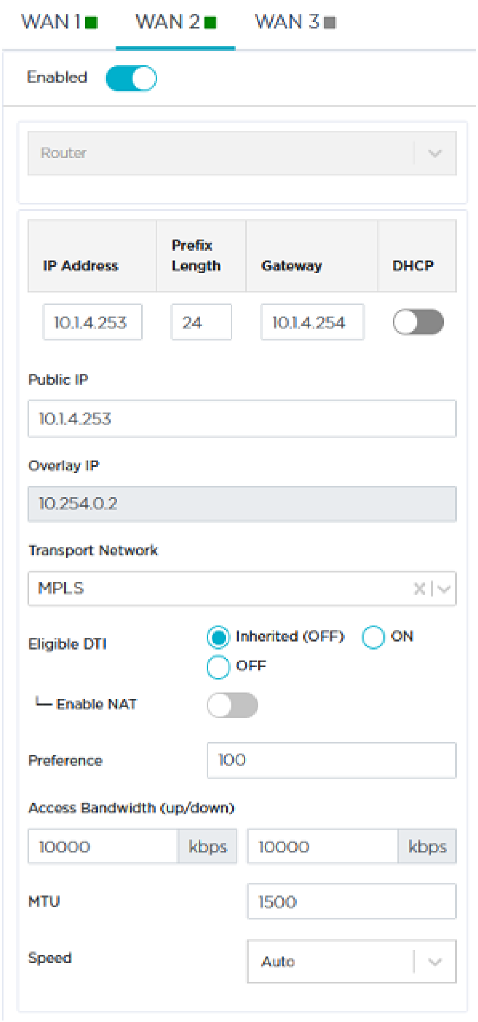
5 Enter the Default Gateway: 192.168.1.1

6. Define the Public IP address (133.3.3.3) which corresponds to the WAN side of the Internet Access router to which the WAN1 interface is connected. The Port Forwarding configuration of the Internet Access router enables this device to send the UDP packets to the appliance WAN1 on ports 500 (IKEv2) and 4500 (IPsec NAT Traversal). The Internet Access router also modifies the Egress packets in order to replace its 133.3.3.3 public address with the 192.168.1.2 WAN1 static address as destination address.
7. When configuring a WAN for the first time, type the name of the network you are connected to, 'Internet' in the current example. Clearly identify each name through customization. Once a Transport Network type has been defined, you can select it from the stack when configuring subsequent WANs.
8. This interface is automatically eligible to DTI (Inherited ON) because you globally activated this policy for the 'Internet' Transport Network (refer to Advanced Configuration -> Transport Network Settings). You may also manage DTI individually for this Internet L3 interface by checking the ON or OFF options.
9. Directly derived from the activated Eligible DTI option, keep the Enable NAT mode activated. This is a source-NAT where the LAN IP addresses (11.1.4.0 or 11.1.5.0) are replaced with the 192.168.1.2 WAN1 IP address. This NAT only applies to the traffic sent over the Internet. The traffic to the Branch Offices/Sites is transferred through the IPsec tunnels.

   If you deactivate the Enable NAT mode which controls the firewall, incoming connections from the WAN are allowed to go to the LAN.
10. The Preference parameter is meaningless in this Use Case since there is only one Data Center appliance.
11. In the Access Bandwidth fields, define the up and down throughput (in kilobits per second) allocated to the WAN: 20000.
12. Enter the MTU value which corresponds to the maximum number of bytes loaded in the Payload. The default value is 1500.
13. Leave the Speed parameter to Auto to let the system define the speed of the interface, or you can force the speed to 100FD or 1000FD. The full duplex speed is expressed in megabits per second.

> **Note:** The Internal Tunnels, External Gateways and Local Port Forwarding configuration panels are not used for this interface.

Refer to "Use Case 2" diagram where WAN2 (MPLS) details are displayed in green.



WAN 1 🟩 WAN 2 🟩 WAN 3 ■

Enabled ◉

Router

IP Address	Prefix Length	Gateway	DHCP
10.1.4.253	24	10.1.4.254	○

Public IP: 10.1.4.253

Overlay IP: 10.254.0.2

Transport Network: MPLS

Eligible DTI: ● Inherited (OFF) ○ ON ○ OFF

└ Enable NAT ○

Preference: 100

Access Bandwidth (up/down): 10000 kbps 10000 kbps

MTU: 1500

Speed: Auto

1. Activate the WAN through the ◉ icon. You may now enter field data.
2. Select the **Router** option for this L3 interface.
3. Enter the interface information, 10.1.4.253 as IP Address, 24 as Prefix length.
4. Enter the Default Gateway: 10.1.4.254
5. Do not activate the DHCP function since the IP address of the WAN2 interface is static to enable the Branch Office appliances creating tunnels.
6. In the 'Public IP' field, re-enter the interface IP address (10.1.4.253) which is not public in this case but a private address in the addressing scheme of the MPLS private network.
7. Type 'MPLS' as Transport Network type.
8. Leave the Eligible DTI parameter to 'Inherited (OFF)'. It corresponds to your configuration in Advanced Configuration -> Transport Network Settings where you did not activate eligibility to DTI for MPLS interfaces.
9. Do not activate the Enable NAT mode since a private network is used (MPLS).

10 The Preference parameter is meaningless in this Use Case since there is only one Data Center appliance.

11 In the Access Bandwidth fields, define the up and down throughput (in kilobits per second) allocated to the WAN: 10000.

12 Enter the MTU value which corresponds to the maximum number of bytes loaded in the Payload. The default value is 1500.

13 Leave the Speed parameter to Auto to let the system define the speed of the interface, or you can force the speed to 100FD or 1000FD. The full duplex speed is expressed in megabits per second.

14 Validate your input by hitting the **Create** button.

If the appliance already exists and you modify any data, click the **Update** button.

> **Note:** The Internal Tunnels and External Gateways configuration panels are not used for this interface.

15 In the Network -> Advanced Configuration window, add this 'DataCenter' hub appliance as Time Synchronization Server. Then click **Update**.

Also see how to configure:

- Branch Office appliance WANs
- a multi-appliance Data Center
- a multi-appliance Branch Office Site

Configuring the Branch Office appliances

After you have configured the Data Center appliance (in "Use Case 2"), you must configure the B01, B02 and B03 Branch Office appliances. Then, configure the B04 Branch Office RVC destination.

- "Configuring the B01 Branch Office appliance"
- "Configuring the B02 Branch Office appliance"
- "Configuring the B03 Branch Office appliance"
- "Configuring the B04 Branch Office RVC destination"

Configuring the B01 Branch Office appliance

B01 is connected to the Data Center through one tunnel over the Internet. Another tunnel connects B01 to B02.

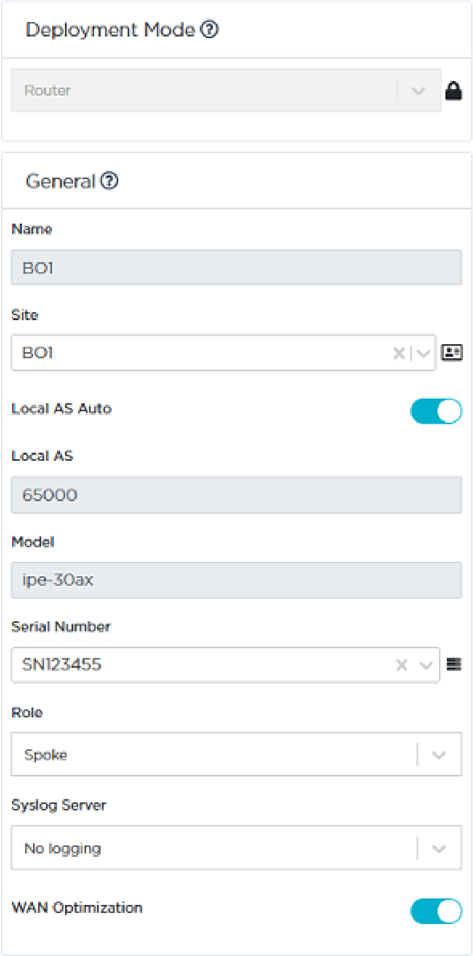
Identifying the appliance

After the B01 appliance with the 'SN123455' Serial Number (and its Model/Version information) has been automatically provisioned in the SD-WAN Orchestrator from the ZTP Server, as indicated via the ≣ sign, it appears under the 'Not Configured' tab of the Network -> Configuration window.

Proceed as follows to identify and further configure the appliance.

1 In the Network -> Configuration window, click ✎ to edit the appliance.

2 In the **Deployment Mode** panel, select the Router option and hit the 🔓 icon to enable the related panels and functions of the interface.



Deployment Mode ⓘ

Router 🔒

General ⓘ

Name: B01

Site: B01

Local AS Auto: on

Local AS: 65000

Model: ipe-30ax

Serial Number: SN123455 ≣

Role: Spoke

Syslog Server: No logging

WAN Optimization: on

3 In the General panel, enter the **Name** of the appliance as well as the name of the related **Site** (B01)**.**

The ▤ button at the right of the Site Name enables you to display the Site subnets.

4 Select the **Auto** option of the Local AS parameter. The related field is automatically populated with a number selected by the Orchestrator from the **AS Number Range** you have specified in the Overlay Routing panel of the Advanced Configuration window.

This parameter is used in the B01 WAN for tunnel mapping between this Site and the other Sites it will be connected to (Data Center and B02).

5 Through the **Role** field, define the appliance as a Spoke since it identifies a Branch Office appliance (generates tunnel requests). Tunnels are always built from the spokes to the hub.

6 Since NATted DTI traffic is enabled on the WAN1 interface, select the Syslog Server you defined in "Advanced Configuration" to enable log export.

7 WAN Optimization is activated by default on this appliance if the matching license is available.

Configuring the LAN

As a second step, configure the B01 appliance LAN which includes one physical interface. Refer to "Use Case 2" diagram where the LAN information is displayed in blue.

1 Click the **Interfaces** tab.

2 Enter the appliance Management IP address (11.1.1.2), Prefix Length (24).

The Management IP address is used for communicating with other appliances, the ZTP Server and the Orchestrator.

3 Use the default **Auto Generated** option (creation window only) to let the system allocate LAN addresses automatically to the Routers (Router X IP = Management IP + X) linked to the WANs in Router mode that you will configure for this appliance. Also refer to "IP Address allocation".

In this example, Router 1 IP address will be automatically defined as it corresponds to WAN1.

4 Enable the DHCP Relay function and enter the DHCP Server Address (11.1.4.250). DHCP requests from the B01 appliance are propagated to the DHCP Server in the Data Center LAN.

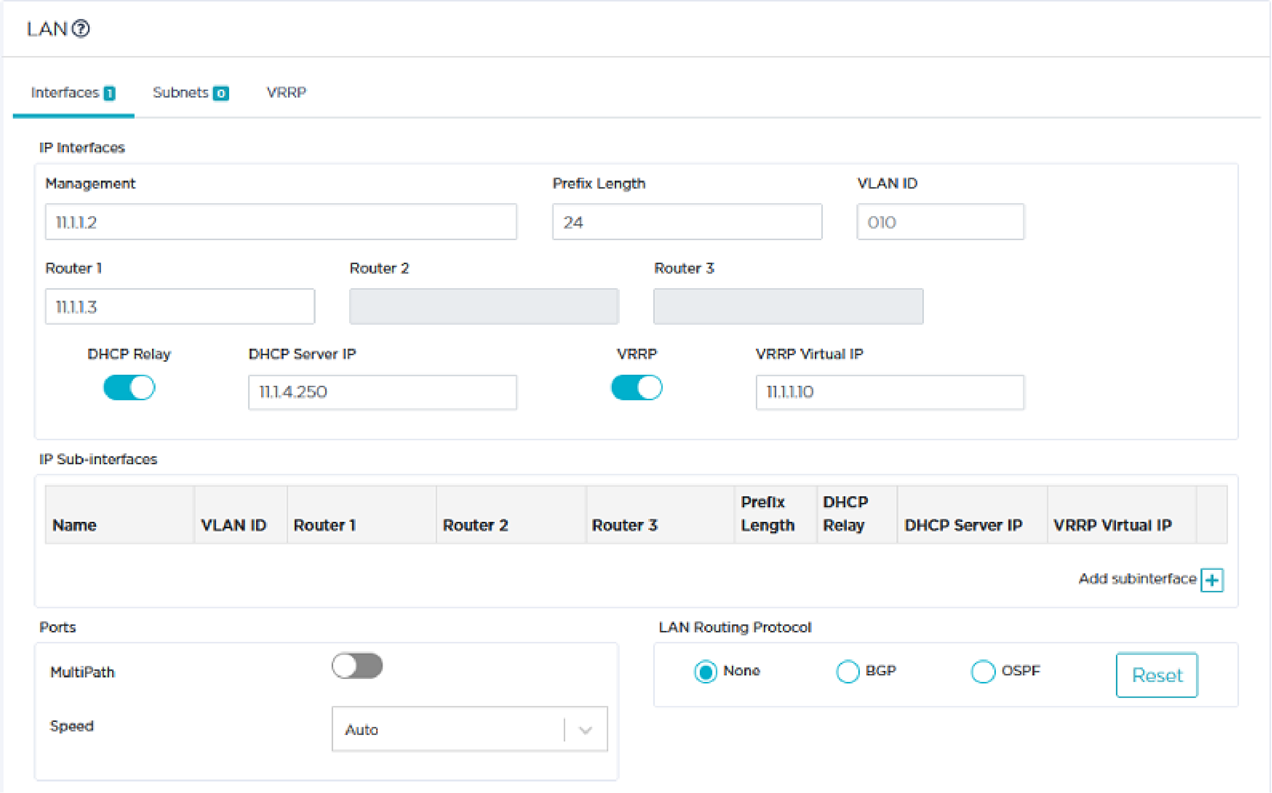
5 Do not enter any VLAN ID. Note that the grey values appearing in some fields of the interface are only given as examples and are not taken into account in the configuration.

6 Since there is no router in the B01 LAN for exchanging routing tables, there is no additional subnet or sub-interface to define for configuring BGP peering (refer to "Configuring BGP") or OSPF adjacencies (refer to "Configuring OSPF").

> **Note:** High Availability VRRP is enabled because B01 is used for "Use Case 6" configuration.

7 Leave the Speed parameter to Auto to let the system define the speed of the interface, or you can force the speed to 100FD or 1000FD. The full duplex speed is expressed in megabits per second.

The following window displays the validated settings.



LAN

Interfaces 1 | Subnets 0 | VRRP

IP Interfaces

Management: 11.1.1.2
Prefix Length: 24
VLAN ID: 010
Router 1: 11.1.1.3
Router 2:
Router 3:
DHCP Relay: on
DHCP Server IP: 11.1.4.250
VRRP: on
VRRP Virtual IP: 11.1.1.10

IP Sub-interfaces

Name	VLAN ID	Router 1	Router 2	Router 3	Prefix Length	DHCP Relay	DHCP Server IP	VRRP Virtual IP

Add subinterface +

Ports

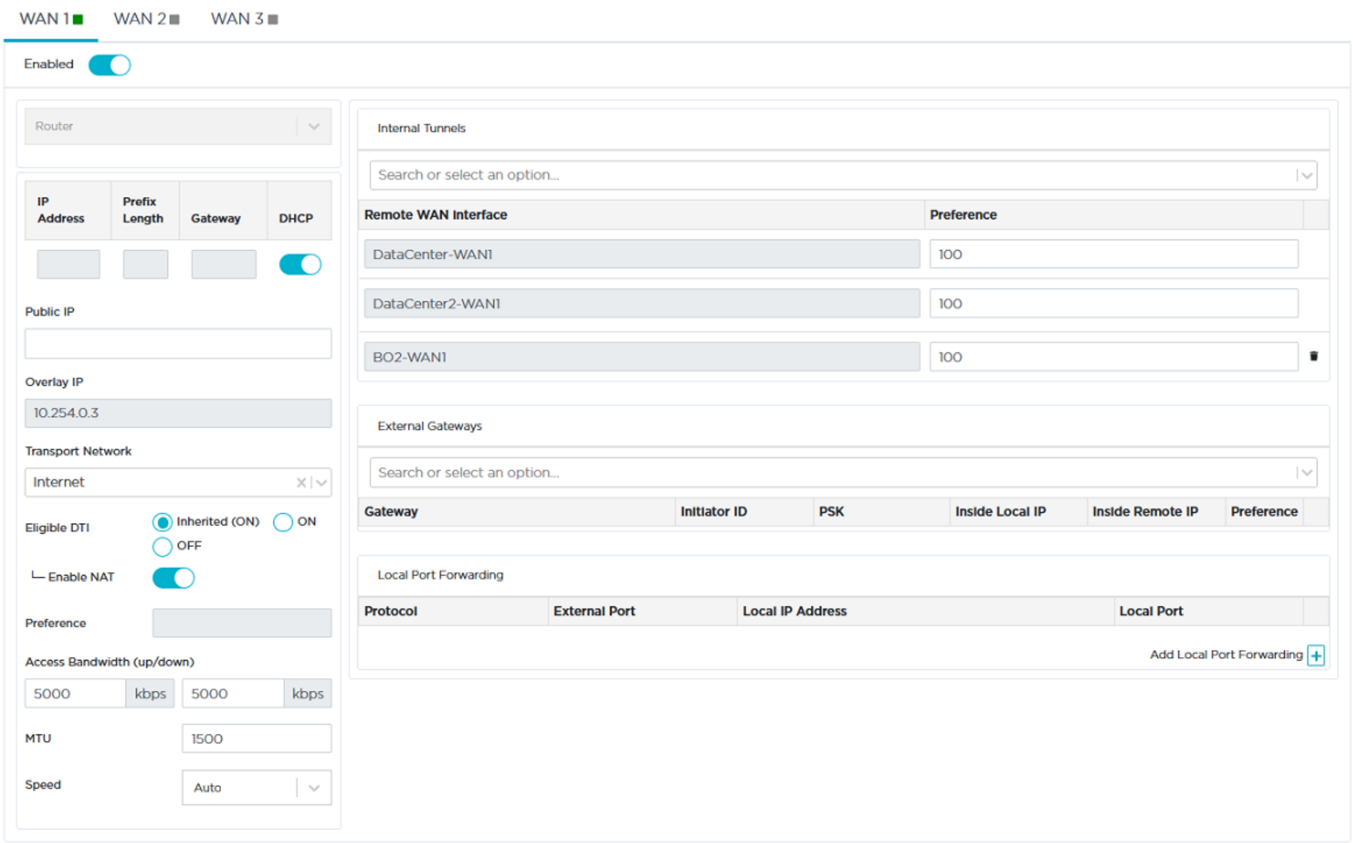
MultiPath: off
Speed: Auto

LAN Routing Protocol

● None ○ BGP ○ OSPF Reset

Configuring the WAN

As a third step, configure the WAN linked to the B01 appliance: Internet. Refer to "Use Case 2" diagram where WAN1 (Internet) details are displayed in orange.



WAN 1 🟩 WAN 2 ■ WAN 3 ■

Enabled ◉

Router

IP Address	Prefix Length	Gateway	DHCP
			◉

Public IP

Overlay IP: 10.254.0.3

Transport Network: Internet

Eligible DTI: ● Inherited (ON) ○ ON ○ OFF

└ Enable NAT ◉

Preference

Access Bandwidth (up/down): 5000 kbps 5000 kbps

MTU: 1500

Speed: Auto

Internal Tunnels

Search or select an option...

Remote WAN Interface	Preference
DataCenter-WAN1	100
DataCenter2-WAN1	100
BO2-WAN1	100

External Gateways

Search or select an option...

Gateway	Initiator ID	PSK	Inside Local IP	Inside Remote IP	Preference

Local Port Forwarding

Protocol	External Port	Local IP Address	Local Port

Add Local Port Forwarding +

1 Activate the WAN through the ◉ icon. You may now enter field data.

2 Select the **Router** option for this L3 interface.

3 With the DHCP parameter activated by default, the interface IP Address, Prefix Length and Default Gateway are dynamically allocated (by the DHCP server of the Internet Access router) to the interface, since this WAN interface is connected to the Internet.

4 As you already defined the 'Internet' type of Transport Network for the Data Center WAN, select it from the stack.

When configuring a WAN for the first time, type the name of the network you are connected to, 'Internet' in the current example. Clearly identify each name through customization. Once a Transport Network type has been defined, you can select it from the stack when configuring subsequent WANs.

5 This interface is automatically eligible to DTI (Inherited ON) because you globally activated this policy for the 'Internet' Transport Network (refer to Advanced Configuration -> Transport Network Settings). You may also manage DTI individually for this Internet L3 interface by checking the ON or OFF options.

6. Directly derived from the activated Eligible DTI option, keep the Enable NAT mode activated. This is a source-NAT where the Management IP address (11.1.1.2) is replaced with the 192.168.1.2 WAN1 IP address. This NAT only applies to the traffic sent over the Internet. The traffic to the Data Center and to other Sites is transferred through the IPsec tunnels.

   If you deactivate the Enable NAT mode which controls the firewall, incoming connections from the WAN are allowed to go to the LAN.
7. The Preference parameter is not available for a Spoke appliance.
8. In the Access Bandwidth fields, define the up and down throughput (in kilobits per second) allocated to the WAN: 5000.
9. Enter the MTU value which corresponds to the maximum number of bytes loaded in the Payload. The default value is 1500.
10. Leave the Speed parameter to Auto to let the system define the speed of the interface, or you can force the speed to 100FD or 1000FD. The full duplex speed is expressed in megabits per second.
11. The Internal Tunnels stack of values contains the WAN interfaces of the remote spoke sites which are connected to the same network as the B01 WAN1 interface. These interfaces are automatically detected by the Orchestrator. In "Use Case 2", the system offers 'B02-WAN1' you can add as additional connection to create a tunnel between B01 and B02.

> **Note:** The External Gateways and Local Port Forwarding configuration panels are not used for this interface.

12. Validate your input by hitting the **Create** button. The Overlay IP address is generated by the system as soon as the tunnel is created.

    If the appliance already exists and you modify any data, click the **Update** button.

Also see how to configure:

- a multi-appliance Branch Office Site
- traffic redirection to an external gateway
- traffic redirection to a web security gateway
- traffic redirection to a cloud gateway
- traffic redirection to EdgeSentry
- a multi-appliance Data Center

Configuring the B02 Branch Office appliance

In "Use Case 2", B02 is connected to the Data Center through two tunnels, one over the Internet and the other one over the MPLS private network.

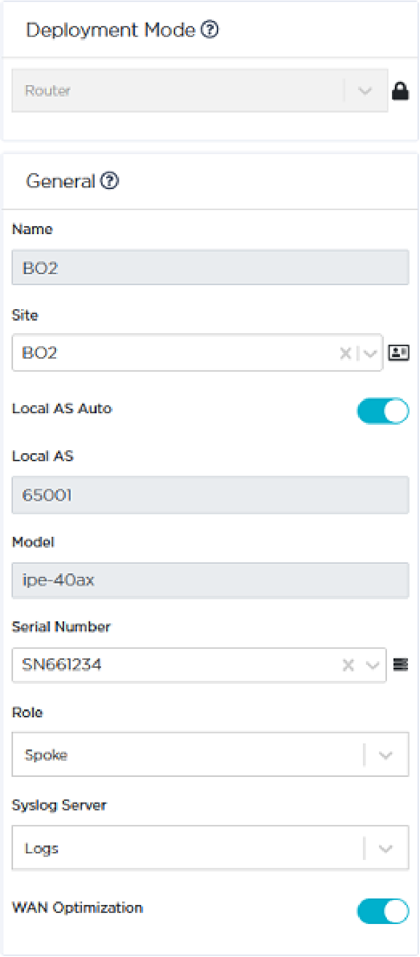
A third tunnel connects B02 to B01. For this reason, Port Forwarding must have been configured on the Internet Access router. This rule authorizes sending the UDP packets to the appliance on ports 500 (IKEv2) and 4500 (IPsec NAT Traversal). You must apply a static IP address to the B02 WAN1 interface.

- "Identifying the appliance"
- "Configuring the LAN"
- "Configuring the WAN(s)"

Identifying the appliance

After the B02 appliance with the 'SN661234' Serial Number (and its Model/Version information) has been automatically provisioned in the SD-WAN Orchestrator from the ZTP Server, as indicated via the 🗄 sign, it appears under the 'Not Configured' tab of the Network -> Configuration window.

Refer to the procedure described in the Hybrid Mode Deployment Use Case to identify the appliance as follows:



Deployment Mode

Router

General

Name: BO2

Site: BO2

Local AS Auto

Local AS: 65001

Model: ipe-40ax

Serial Number: SN661234

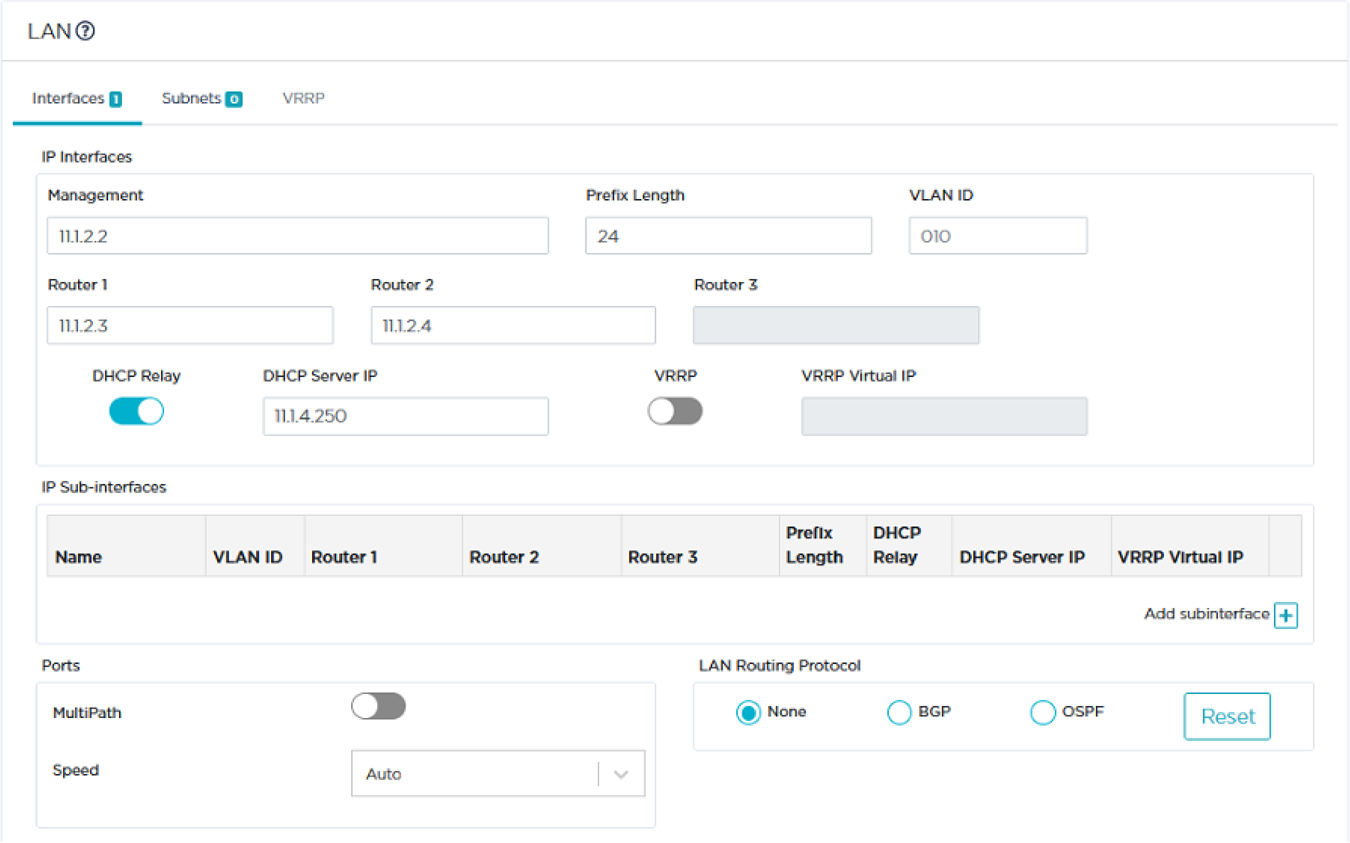
Role: Spoke

Syslog Server: Logs

WAN Optimization

Configuring the LAN

As a second step, configure the B02 appliance LAN which includes one physical interface. Refer to "Use Case 2" diagram where the LAN information is displayed in blue, and to the procedure describing B01 appliance LAN configuration to define the following parameters. Do not specify any VRRP settings.



IP Interfaces

Management: 11.1.2.2

Prefix Length: 24

VLAN ID: 010

Router 1: 11.1.2.3

Router 2: 11.1.2.4

Router 3:

DHCP Relay: on

DHCP Server IP: 11.1.4.250

VRRP: off

VRRP Virtual IP:

IP Sub-interfaces

Name	VLAN ID	Router 1	Router 2	Router 3	Prefix Length	DHCP Relay	DHCP Server IP	VRRP Virtual IP

Ports

MultiPath: off

Speed: Auto

LAN Routing Protocol

● None ○ BGP ○ OSPF

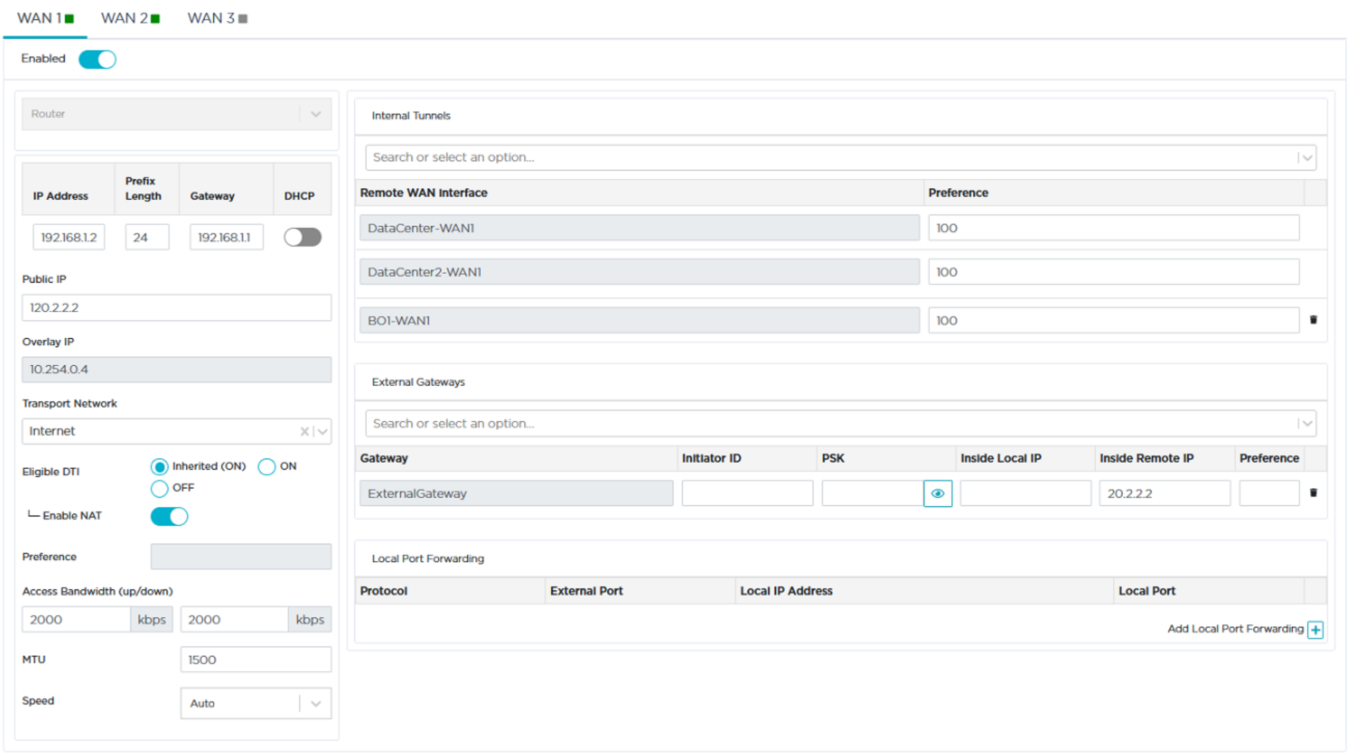
Also see how to configure:

- a multi-appliance Branch Office Site
- a Data Center LAN
- a multi-appliance Data Center

Configuring the WAN(s)

As a third step, configure the two WANs linked to the B02 appliance: Internet and MPLS.

Refer to "Use Case 2" diagram where WAN1 (Internet) details are displayed in orange.



Enabled

Router

IP Address	Prefix Length	Gateway	DHCP
192.168.1.2	24	192.168.1.1	

Public IP: 120.2.2.2

Overlay IP: 10.254.0.4

Transport Network: Internet

Eligible DTI: ● Inherited (ON) ○ ON ○ OFF

└ Enable NAT

Preference

Access Bandwidth (up/down): 2000 kbps 2000 kbps

MTU: 1500

Speed: Auto

Internal Tunnels

Search or select an option...

Remote WAN Interface	Preference
DataCenter-WAN1	100
DataCenter2-WAN1	100
B01-WAN1	100

External Gateways

Search or select an option...

Gateway	Initiator ID	PSK	Inside Local IP	Inside Remote IP	Preference
ExternalGateway				20.2.2.2	

Local Port Forwarding

Protocol	External Port	Local IP Address	Local Port

Add Local Port Forwarding +

1 Activate the WAN through the icon. You may now enter field data.

2 Select the **Router** option for this L3 interface.

3 Do not activate the DHCP function to proceed with Step 4.

4 Enter the WAN1 interface static information, 192.168.1.2 as IP Address, 24 as Prefix length. This address must be static to enable the configuration of Port Forwarding on the Internet Access router.

5 Enter the Default Gateway: 192.168.1.1

6 Define the Public IP address (120.2.2.2) which corresponds to the WAN side of the Internet Access router to which the WAN1 interface is connected. The Port Forwarding configuration of the Internet Access router enables this device to send the UDP packets to the appliance WAN1 on ports 500 (IKEv2) and 4500 (IPsec NAT Traversal). The Internet Access router also modifies the Egress packets in order to replace its 120.2.2.2 public address with the 192.168.1.2 WAN1 static address as destination address.

7 As you already defined the 'Internet' type of Transport Network for the Data Center and B01 WANs, select it from the stack.

When configuring a WAN for the first time, type the name of the network you are connected to, 'Internet' in the current example. Clearly identify each name through customization. Once a Transport Network type has been defined, you can select it from the stack when configuring subsequent WANs.

8 This interface is automatically eligible to DTI (Inherited ON) because you globally activated this policy for the 'Internet' Transport Network (refer to Advanced Configuration

-> Transport Network Settings). You may also manage DTI individually for this Internet L3 interface by checking the ON or OFF options.

9 Directly derived from the activated Eligible DTI option, keep the Enable NAT mode activated. This is a source-NAT where the LAN Management IP address (11.1.2.2) is replaced with the 192.168.1.2 WAN1 IP address. This NAT only applies to the traffic sent over the Internet. The traffic to the Data Center and to other Sites is transferred through the IPsec tunnels.

If you deactivate the Enable NAT mode which controls the firewall, incoming connections from the WAN are allowed to go to the LAN.

10 The Preference parameter is not available for a Spoke appliance.

11 In the Access Bandwidth fields, define the up and down throughput (in kilobits per second) allocated to the WAN: 2000.

12 Enter the MTU value which corresponds to the maximum number of bytes loaded in the Payload. The default value is 1500.

13 Leave the Speed parameter to Auto to let the system define the speed of the interface, or you can force the speed to 100FD or 1000FD. The full duplex speed is expressed in megabits per second.

14 The Internal Tunnels stack of values contains the WAN interfaces of the remote spoke sites which are connected to the same network. These interfaces are automatically detected by the Orchestrator. Since you connected the current appliance to the B01 appliance, the 'B01-WAN1' remote WAN interface is automatically specified in the list of interfaces and enables you to validate the tunnel between B02 and B01. See "Configuring the WAN" for the B01 appliance.

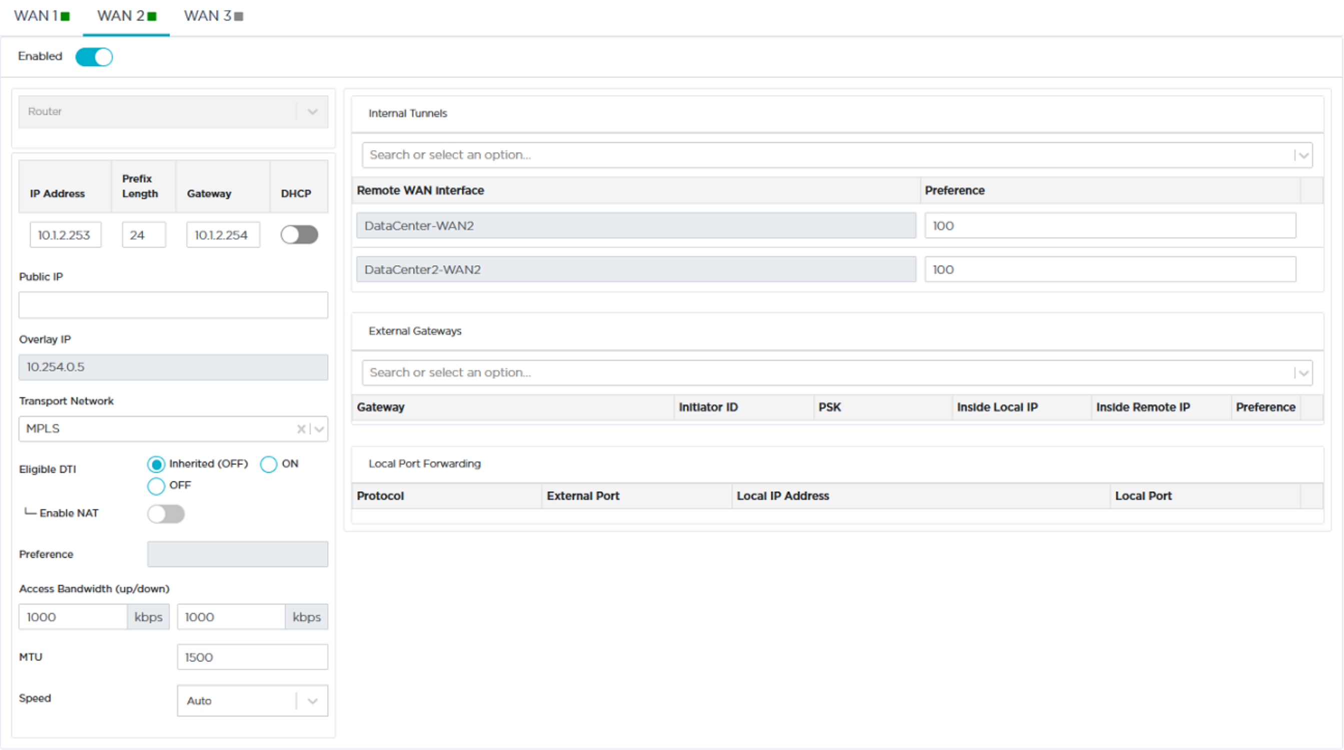
15 This WAN1 interface is also connected to an external gateway; refer to "Configuring traffic redirection to an External Gateway".

Note: The Local Port Forwarding configuration panel is not used for this interface.

16 Validate your input by hitting the **Create** button. The Overlay IP address is generated by the system as soon as tunnels are created.

If the appliance already exists and you modify any data, click the **Update** button.

Refer to "Use Case 2" diagram where WAN2 (MPLS) details are displayed in green.



WAN 1 🟩 WAN 2 🟩 WAN 3 ■

Enabled

Router

IP Address	Prefix Length	Gateway	DHCP
10.1.2.253	24	10.1.2.254	

Public IP

Overlay IP
10.254.0.5

Transport Network
MPLS

Eligible DTI ● Inherited (OFF) ○ ON ○ OFF

└ Enable NAT

Preference

Access Bandwidth (up/down)
1000 kbps 1000 kbps

MTU 1500

Speed Auto

Internal Tunnels

Search or select an option...

Remote WAN Interface	Preference
DataCenter-WAN2	100
DataCenter2-WAN2	100

External Gateways

Search or select an option...

Gateway	Initiator ID	PSK	Inside Local IP	Inside Remote IP	Preference

Local Port Forwarding

Protocol	External Port	Local IP Address	Local Port

1. Activate the WAN through the icon. You may now enter field data.
2. Select the **Router** option for this L3 interface.
3. Enter the interface information, 10.1.2.253 as IP Address, 24 as Prefix length.
4. Enter the Default Gateway: 10.1.2.254
5. Do not activate the DHCP function since the IP address of the WAN2 interface is static.
6. As you already defined the 'MPLS' type of Transport Network for the Data Center WANs, select it from the stack.

   When configuring a WAN for the first time, type the name of the network you are connected to, 'MPLS' in the current example. Clearly identify each name through customization. Once a Transport Network type has been defined, you can select it from the stack when configuring subsequent WANs.
7. Leave the Eligible DTI parameter to 'Inherited (OFF)'. It corresponds to your configuration in Advanced Configuration -> Transport Network Settings where you did not activate eligibility to DTI for MPLS interfaces.
8. Do not activate the Enable NAT mode since a private network is used (MPLS).
9. The Preference parameter is not available for a Spoke appliance.
10. In the Access Bandwidth fields, define the up and down throughput (in kilobits per second) allocated to the WAN: 1000.

11. Enter the MTU value which corresponds to the maximum number of bytes loaded in the Payload. The default value is 1500.
12. Leave the Speed parameter to Auto to let the system define the speed of the interface, or you can force the speed to 100FD or 1000FD. The full duplex speed is expressed in megabits per second.
13. Validate your input by hitting the **Create** button. The Overlay IP address is generated by the system as soon as the tunnel is created.

    If the appliance already exists and you modify any data, click the **Update** button.

Also see how to configure:

- Data Center appliance WANs
- a multi-appliance Branch Office Site
- traffic redirection to an external gateway
- traffic redirection to a web security gateway
- traffic redirection to a cloud gateway
- traffic redirection to EdgeSentry
- a multi-appliance Data Center

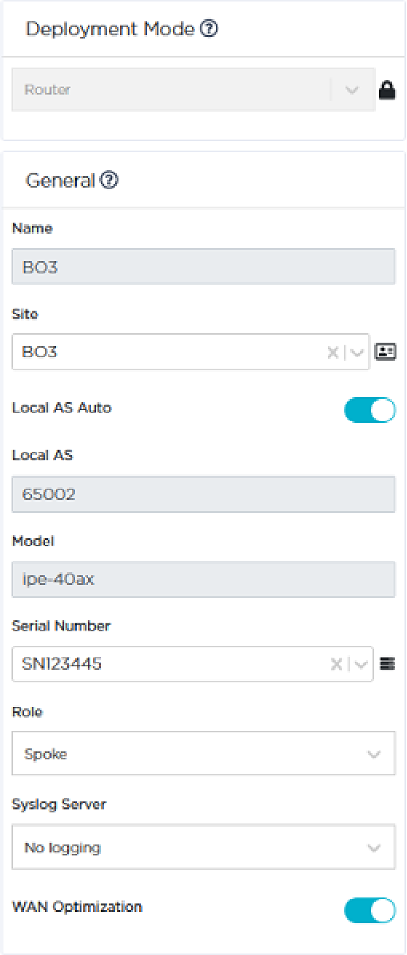
Configuring the B03 Branch Office appliance

B03 is connected to the Data Center through one tunnel over the MPLS private network.

Identifying the appliance

After the B03 appliance with the 'SN123445' Serial Number (and its Model/Version information) has been automatically provisioned in the SD-WAN Orchestrator from the ZTP Server, as indicated via the ☰ sign, it appears under the 'Not Configured' tab of the Network -> Configuration window.

Refer to the procedure described in "Configuring the B01 Branch Office appliance" to identify the appliance as follows:



Deployment Mode

Router

General

Name: BO3

Site: BO3

Local AS Auto: on

Local AS: 65002

Model: ipe-40ax

Serial Number: SN123445

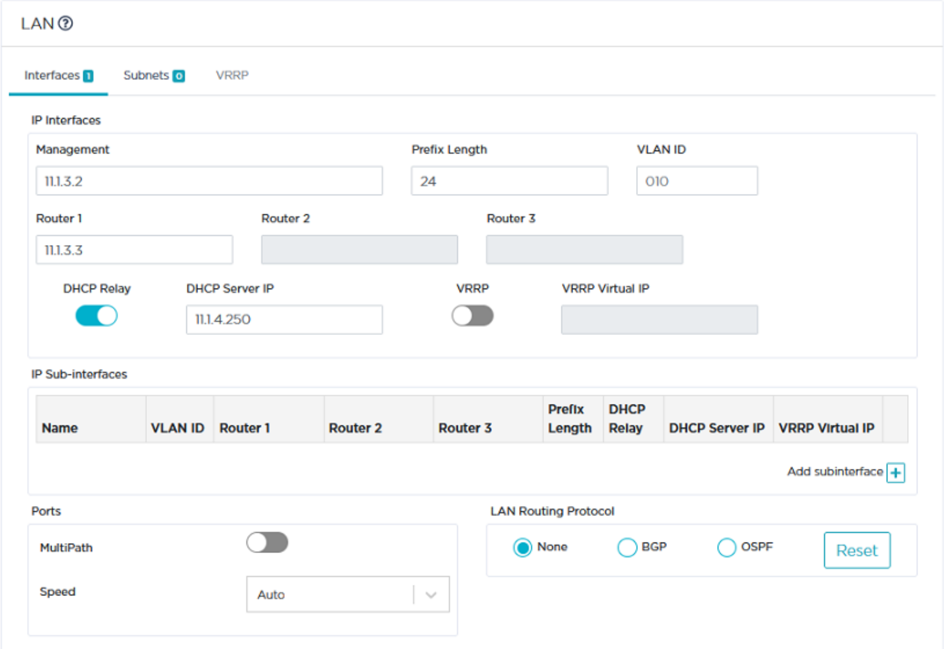
Role: Spoke

Syslog Server: No logging

WAN Optimization: on

Configuring the LAN

As a second step, configure the B03 appliance LAN which includes one physical interface. Refer to "Use Case 2" diagram (LAN information is displayed in blue) and to the procedure describing B01 appliance LAN configuration to define the following parameters. Do not specify any VRRP settings.



LAN

Interfaces 1 | Subnets 0 | VRRP

IP Interfaces

Management	Prefix Length	VLAN ID
11.1.3.2	24	010

Router 1	Router 2	Router 3
11.1.3.3		

DHCP Relay	DHCP Server IP	VRRP	VRRP Virtual IP
ON	11.1.4.250	OFF	

IP Sub-interfaces

Name	VLAN ID	Router 1	Router 2	Router 3	Prefix Length	DHCP Relay	DHCP Server IP	VRRP Virtual IP

Add subinterface

Ports

MultiPath: OFF

Speed: Auto

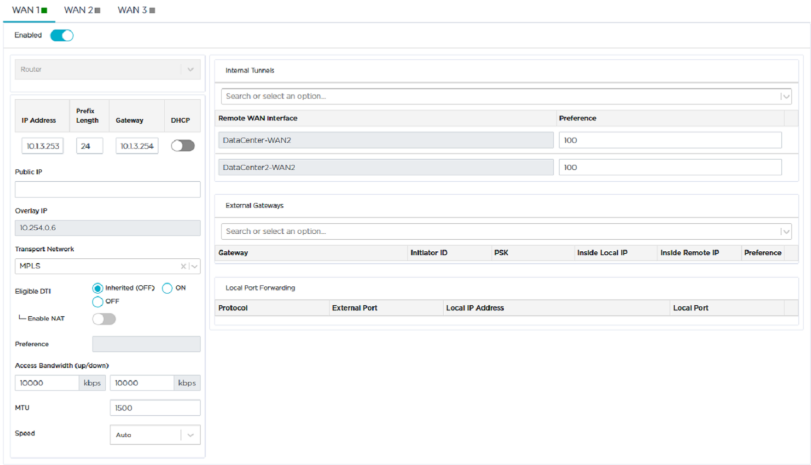
LAN Routing Protocol

● None ○ BGP ○ OSPF

Reset

Configuring the WAN

As a third step, configure the WAN linked to the B03 appliance: MPLS. Refer to "Use Case 2" diagram where WAN1 (MPLS) details are displayed in green. Also refer to the configuration procedure of B02 appliance WAN2 to define the following parameters:



WAN 1 | WAN 2 | WAN 3

Enabled: ON

Router

IP Address	Prefix Length	Gateway	DHCP
10.1.3.253	24	10.1.3.254	OFF

Public IP:

Overlay IP: 10.254.0.6

Transport Network: MPLS

Eligible DTI: ● Inherited (OFF) ○ ON ○ OFF

└ Enable NAT: OFF

Preference:

Access Bandwidth (up/down): 10000 kbps 10000 kbps

MTU: 1500

Speed: Auto

Internal Tunnels

Search or select an option...

Remote WAN Interface	Preference
DataCenter-WAN2	100
DataCenter2-WAN2	100

External Gateways

Search or select an option...

Gateway	Initiator ID	PSK	Inside Local IP	Inside Remote IP	Preference

Local Port Forwarding

Protocol	External Port	Local IP Address	Local Port

Also see how to configure:

- a multi-appliance Branch Office Site
- traffic redirection to an external gateway
- traffic redirection to a web security gateway
- traffic redirection to a cloud gateway
- traffic redirection to EdgeSentry
- a multi-appliance Data Center

Configuring the B04 Branch Office RVC destination

Refer to "Configuring the B04 Branch Office RVC destination" in the Hybrid Mode Deployment section.

Then, to create the tunnel from the Data Center appliance to the B04 CE router in "Use Case 2", refer to "Configuring traffic redirection to an External Gateway"

Also see how to configure:

- a Data Center appliance
- a Branch Office appliance

Checking the results of your Network Configuration

After a five minute delay during which the SD-WAN Orchestrator processes the last created or updated configuration, click the Extreme Networks logo in the interface top bar to display the Overview Dashboard.

The number of configured appliances and the number of created IPsec tunnels are specified. Check them with respect to Use Case diagrams.

Configuring CloudMesh for Sites

The purpose of this Use Case, which is based on "Use Case 1", is to provide full mesh connectivity between all the Branch Office Sites. The user traffic between the Branch Office Sites is managed and routed by the CloudMesh Core infrastructure and exits the CloudMesh private network through the Internet at the closest of the destination Sites.

This section describes how to configure CloudMesh in your network, between Branch Office 1 appliance and Branch Office 2 appliance.

One tunnel is created per WAN Router interface after you have defined the appropriate parameters in the SD-WAN Orchestrator.

> **Note:** Using CloudMesh requires that all appliances are defined as 'spokes'.

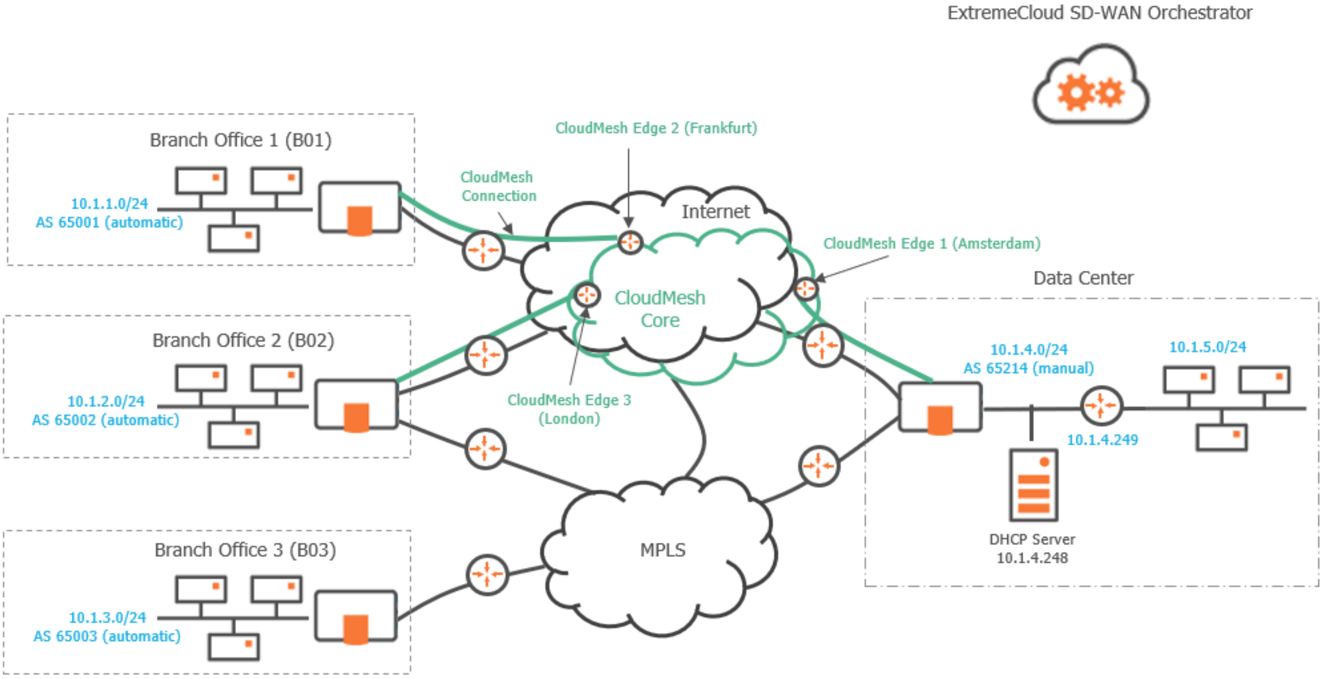
Prerequisites

You can use the CloudMesh feature of the SD-WAN Orchestrator if:

- you have purchased two licenses: Ent-Branch-* or Ent-HA-Branch-* for the appliance, and CloudMesh for the domain. Refer to "Viewing Licenses"
- Extreme Networks has activated CloudMesh for your Customer account

- "Step by Step Procedure"

Use Case 3



Graph legend

▣	⊕	🖧	▭	🗄	Green connection	Grey connection
SD-WAN appliance	router	subnet	host in a subnet	server	CloudMesh IPsec tunnel	physical connection between devices

> **Note:** A router may be a CE Router (MPLS Router), an Internet Access Router or a Core Router.

Step by Step Procedure

Refer to "Use Case 3" diagram where CloudMesh information is displayed in green.

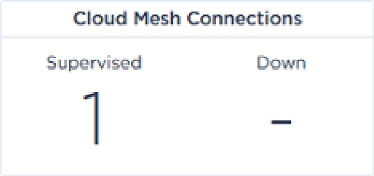
Activating CloudMesh

1. Connect Branch Office 1 appliance WAN1 router interface to CloudMesh by checking the option.
2. Select the CloudMesh Edge which is closest to the appliance (Frankfurt). Note that Edge information is common to all the WAN interfaces of the appliances on the same Site, for which CloudMesh has been activated.

   Eligible interfaces are WAN Router interfaces on hybrid or full router appliances.
3. Click **Update**.
4. Connect Branch Office 2 appliance WAN2 router interface to CloudMesh by checking the option.
5. Select the CloudMesh Edge which is closest to the appliance (London).
6. Click **Update**.
7. From the SD-WAN Orchestrator main menu, select **Network -> Advanced Configuration** and open the CloudMesh pane. Check the Overlay IP network address range and the AS Number that are used by the system for cloudmeshing; you cannot edit nor reuse these parameters.

Checking CloudMesh Connections

1. Verify whether the CloudMesh configuration is operational by checking that there are supervised connections in the CloudMesh Connections panel of the Supervision -> Overview dashboard.

   Cloud Mesh Connections

Supervised	Down
1	-

   For each connected WAN router interface, one tunnel is created; refer to Use Case 3 diagram. If CloudMesh connections are displayed in the 'Down' column, check the alarms raised for the configured CloudMesh appliance in the Active Alarms and Event History dashboards.
2. On the Supervision -> Tunnel Status dashboard, check that the CloudMesh tunnels are up.

3 On the Network -> Configuration window, click the ♥ icon for the appropriate appliance. In the displayed window, select **Tunnels -> IPsec** to analyze the details of the created CloudMesh tunnels.

Configuring multi-appliance Sites

You may configure data centers and Branch Office sites with multiple appliances. The objectives of these deployments are:

- High Availability (HA) to ensure network connectivity between the Data Center or Branch Office and the remote Sites in the case of appliance failure. **Even though iBGP, VRRP or OSPF protocols may be used for configuring all multi-appliance Sites**, they are described in the Use Cases of this documentation as follows:
    - iBGP protocol is used between the Core Router and the appliances of a Data Center (Use Case 4A, Use Case 4B and Use Case 4C)
    - OSPF protocol is used between the Core Routers and the appliances of a Data Center (Use Case 5)
    - VRRP protocol is used between the appliances of a Branch Office (Use Case 6)
    - IHAP (Ipanema High Availability Protocol) is used between the hybrid or bridge appliances of a Branch Office (Use Case 7)
- Transit Traffic Routing in the Data Center to interconnect several regional networks (Use Case 4B and Use Case 4C)

- "Configuring a multi-appliance Data Center through iBGP"
- "Configuring a multi-appliance Hybrid Data Center through OSPF"
- "Configuring a multi-appliance Branch Office Site through VRRP"
- "Configuring a multi-appliance Branch Office Site through IHAP"

Configuring a multi-appliance Data Center through iBGP

This section describes how to configure a Data Center with two appliances through iBGP. The objectives of this deployment are the following:

- high availability: if one hub appliance is in bad health, the other appliance is used as backup appliance
- load balancing: if your network includes many spokes, you may distribute traffic on several hub appliances
- transit traffic routing: the two appliances are used to interconnect several regional networks

iBGP peering is possible:

- between two or more SD-WAN appliances
- when the SD-WAN appliances have the same AS number
- when the SD-WAN appliances are connected to the same LAN or VLAN
- when the SD-WAN appliances are connected to different LANs or VLANs via a Core Router

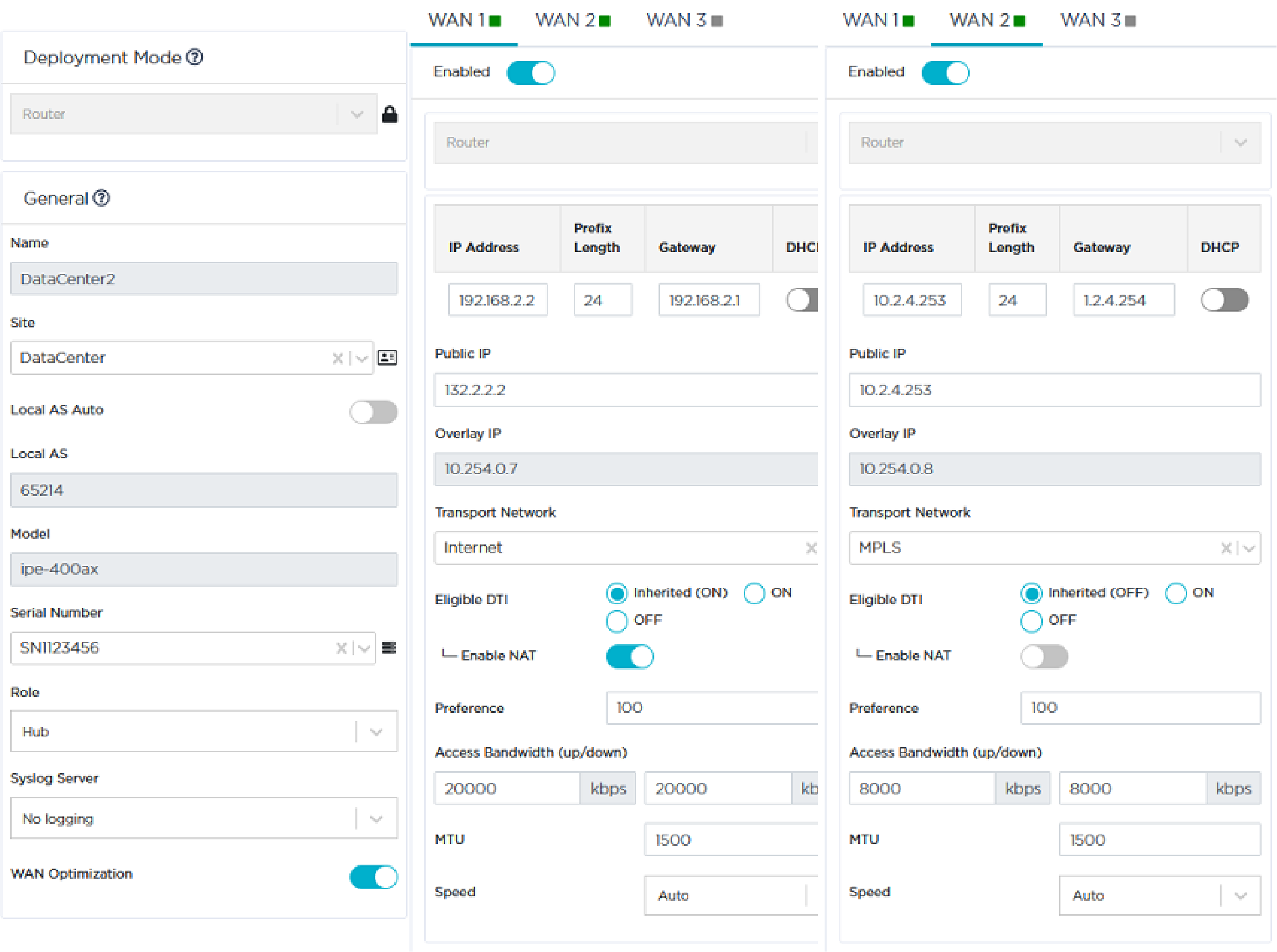
The following configuration Use Cases are complementary to both Use Case 1 and Use Case 2.

- Use Case 4A and Use Case 4B refer to a multi-appliance Data Center configured in Router Mode
- Use Case 4C refers to a multi-appliance Data Center configured in Hybrid Mode

Router Mode

For Use Case 4A and Use Case 4B which are complementary to "Use Case 2", there is one prerequisite which is the necessary configuration of the second hub appliance of the Data Center.

1 Configure the hub appliance as follows:



Deployment Mode: Router

General

Name: DataCenter2

Site: DataCenter

Local AS Auto: off

Local AS: 65214

Model: ipe-400ax

Serial Number: SN1123456

Role: Hub

Syslog Server: No logging

WAN Optimization: on

WAN 1 🟩 | WAN 2 🟩 | WAN 3 ■ (WAN 1 selected)

Enabled: on

Router

IP Address	Prefix Length	Gateway	DHC
192.168.2.2	24	192.168.2.1	off

Public IP: 132.2.2.2

Overlay IP: 10.254.0.7

Transport Network: Internet

Eligible DTI: ● Inherited (ON) ○ ON ○ OFF

└ Enable NAT: on

Preference: 100

Access Bandwidth (up/down): 20000 kbps 20000 kb

MTU: 1500

Speed: Auto

WAN 1 🟩 | WAN 2 🟩 | WAN 3 ■ (WAN 2 selected)

Enabled: on

Router

IP Address	Prefix Length	Gateway	DHCP
10.2.4.253	24	1.2.4.254	off

Public IP: 10.2.4.253

Overlay IP: 10.254.0.8

Transport Network: MPLS

Eligible DTI: ● Inherited (OFF) ○ ON ○ OFF

└ Enable NAT: off

Preference: 100

Access Bandwidth (up/down): 8000 kbps 8000 kbps

MTU: 1500

Speed: Auto

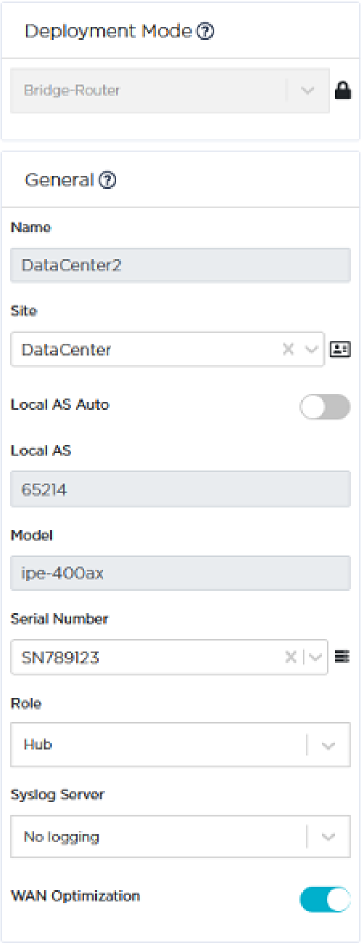
2 Check that you use the same Local Autonomous System as for the Data Center first appliance: 65214.

3 Then configure its LAN to meet Use Case 4A and Use Case 4B requirements as described on the following pages.

Hybrid Mode

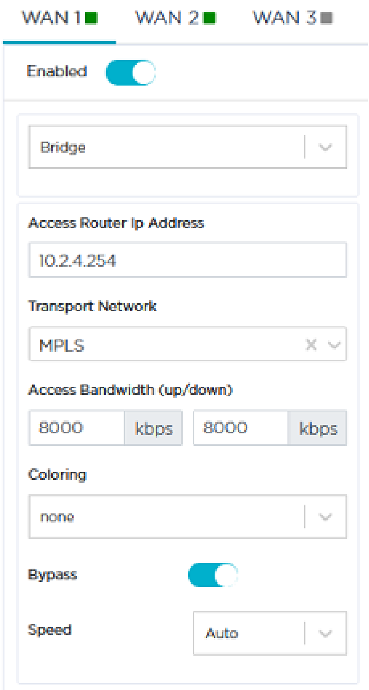
For Use Case 4C which is complementary to "Use Case 1", there is one prerequisite which is the necessary configuration of the second hub appliance of the Data Center.

1 Configure the hub appliance as follows:

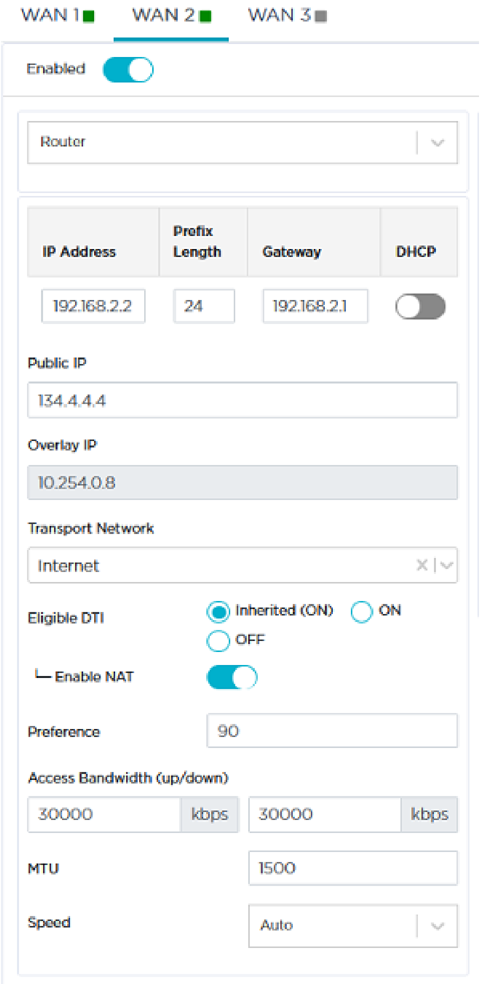


Deployment Mode
Bridge-Router

General
Name: DataCenter2
Site: DataCenter
Local AS Auto: off
Local AS: 65214
Model: ipe-400ax
Serial Number: SN789123
Role: Hub
Syslog Server: No logging
WAN Optimization: on



Enabled: on
Bridge
Access Router Ip Address: 10.2.4.254
Transport Network: MPLS
Access Bandwidth (up/down): 8000 kbps 8000 kbps
Coloring: none
Bypass: on
Speed: Auto



Enabled: on
Router

IP Address	Prefix Length	Gateway	DHCP
192.168.2.2	24	192.168.2.1	off

Public IP: 134.4.4.4
Overlay IP: 10.254.0.8
Transport Network: Internet
Eligible DTI: ● Inherited (ON) ○ ON ○ OFF
└ Enable NAT: on
Preference: 90
Access Bandwidth (up/down): 30000 kbps 30000 kbps
MTU: 1500
Speed: Auto

2 Check that you use the same Local Autonomous System as for the Data Center first appliance: 65214.

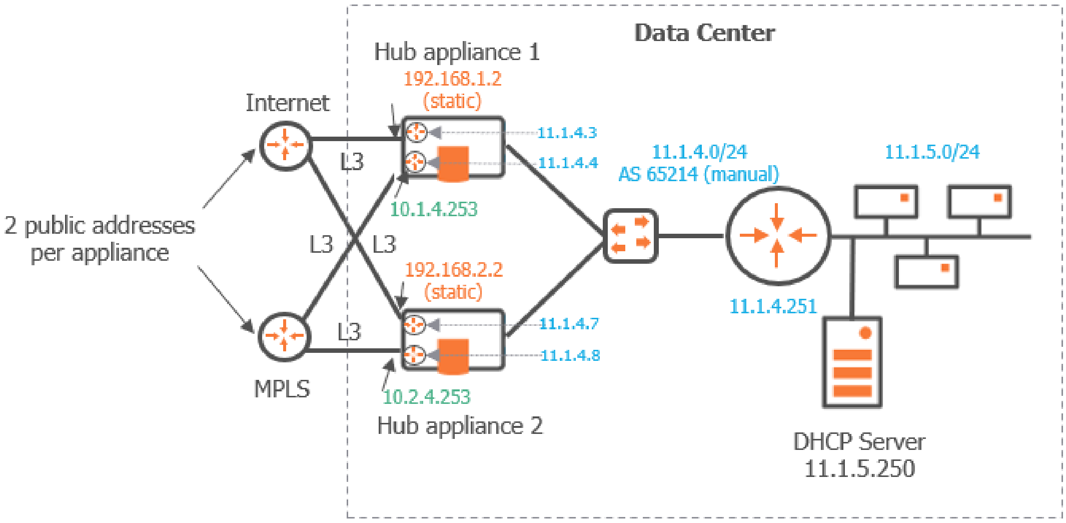
3 Then configure its LAN to meet Use Case 4C requirements as described on the following pages.

Configuring a multi-appliance Router Data Center through iBGP - First Deployment

This first Data Center deployment uses two appliances with the same AS in the same subnet without access to the Core Router. It ensures network connectivity. It is complementary to "Use Case 2".

This configuration is done on the LAN panel of each appliance.

Use Case 4A

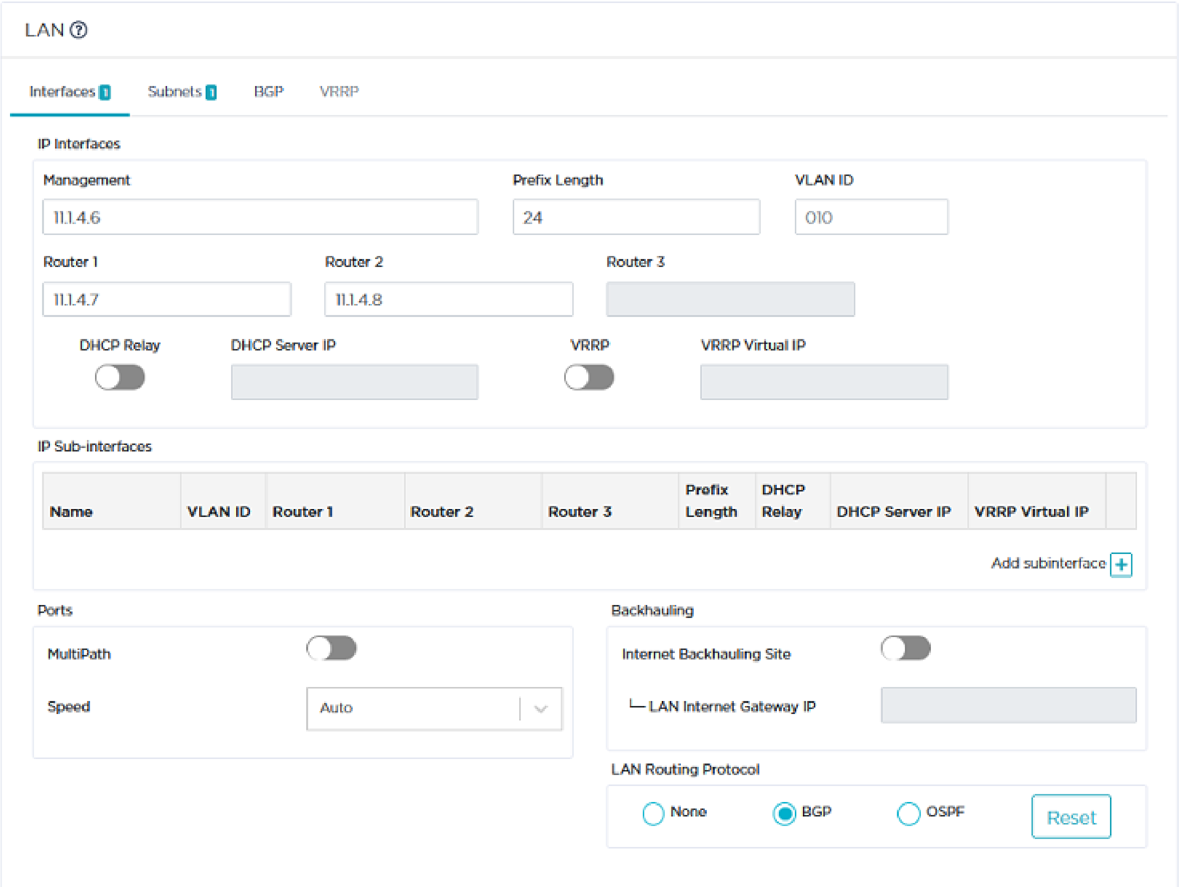


Graph legend

						Grey connection
SD-WAN appliance	router	switch	subnet	host in a subnet	server	connection between devices

> **Note:** A router may be a CE Router (MPLS Router), an Internet Access Router or a Core Router.

1. After you have defined the interfaces of the Data Center second hub appliance (see "Router Mode"), configure its LAN. On "Use Case 4A" diagram, LAN information is displayed in blue.



LAN ?

Interfaces 1 | Subnets 1 | BGP | VRRP

IP Interfaces

Management: 11.1.4.6

Prefix Length: 24

VLAN ID: 010

Router 1: 11.1.4.7

Router 2: 11.1.4.8

Router 3:

DHCP Relay: off

DHCP Server IP:

VRRP: off

VRRP Virtual IP:

IP Sub-interfaces

Name	VLAN ID	Router 1	Router 2	Router 3	Prefix Length	DHCP Relay	DHCP Server IP	VRRP Virtual IP

Add subinterface +

Ports

MultiPath: off

Speed: Auto

Backhauling

Internet Backhauling Site: off

└ LAN Internet Gateway IP:

LAN Routing Protocol

○ None ● BGP ○ OSPF

Reset

2 Click the **Interfaces** tab.

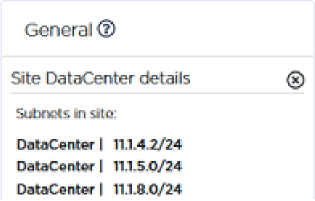
- Enter the appliance Management IP Address (11.1.4.6), Prefix Length (24). The Management IP address is used for communicating with other appliances, the ZTP Server and the Orchestrator.
- Use the default **Auto Generated** option (creation window only) to let the system allocate LAN addresses automatically to the Routers (Router X IP = Management IP + X) linked to the WANs that you configured for this appliance. Also refer to "IP Address allocation".

> **Note:** Since the three IP addresses directly following the Management IP address (11.1.4.2) of the Data Center first appliance are used for its WAN routers, enter 11.1.4.6 as the Management IP Address of the second appliance.

- Do not activate the DHCP Relay function since the Data Center hosts can directly access the DHCP Server. The appliance does not need to relay host requests.
- Do not enter any VLAN ID. Note that the grey values appearing in some fields of the interface are only given as examples and are not taken into account in the configuration.

3 Defining any subnet is unnecessary because you already defined (in the first Data Center appliance LAN) the subnet used by both hub appliances (11.1.5.0/24). Simply click the 🪪

icon at the right of the Site Name in the identification panel of the second appliance. The existing subnet is displayed:



General ⓘ

Site DataCenter details ⊗

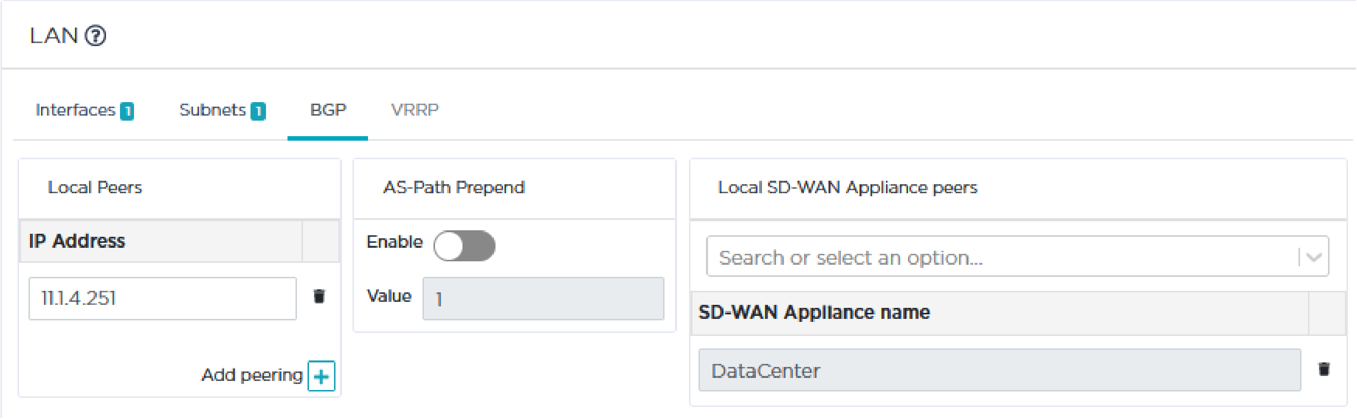
Subnets in site:

DataCenter | 11.1.4.2/24
DataCenter | 11.1.5.0/24
DataCenter | 11.1.8.0/24

Also, the Next Hop address in the Subnet panel is useless because you will define the BGP Local Peer router ip address in the BGP parameter block (see below).

4 Select BGP as LAN Routing Protocol, click the **BGP** tab and the Add peering icon ⊞.

The Data Center appliance exchanges its routing tables with the local router using iBGP.



IP Address
11.1.4.251

Enable: off

Value: 1

SD-WAN Appliance name
DataCenter

- Enter the IP address of the BGP local peer (11.1.4.251).
- Validate your settings by hitting the **Create** or **Update** buttons.

5 For high availability, define the master appliance through which traffic routing has priority over routing through the backup appliance. If you want the first appliance (DataCenter) to be the master, set its WAN1 and WAN2 Preference values to 200. To specify the second appliance as the backup appliance (DataCenter2), set its WAN1 and WAN2 Preference values to 100 (default). The highest Preference value implies priority.

If WAN Preference values are identical, the system gives priority to the highest IP addresses. By default, Hub Preference values and Spoke Preference values are the same for a specific tunnel; if you modify any Spoke Preference value, it is automatically edited on the related Hub.

Validate your configuration.

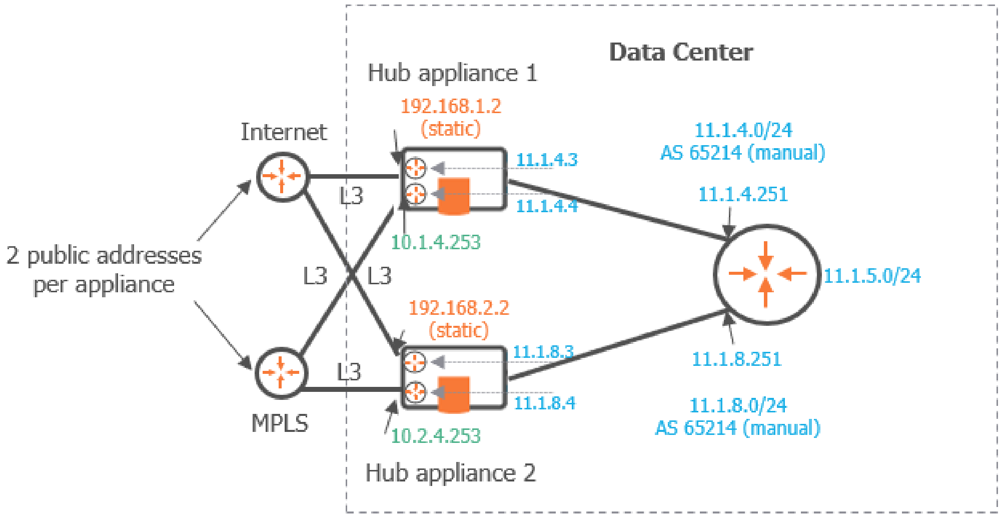
6 In the Network -> Advanced Configuration window, add the 'DataCenter2' hub appliance as Time Synchronization Server. Then click **Update**.

Configuring a multi-appliance Router Data Center through iBGP - Second Deployment

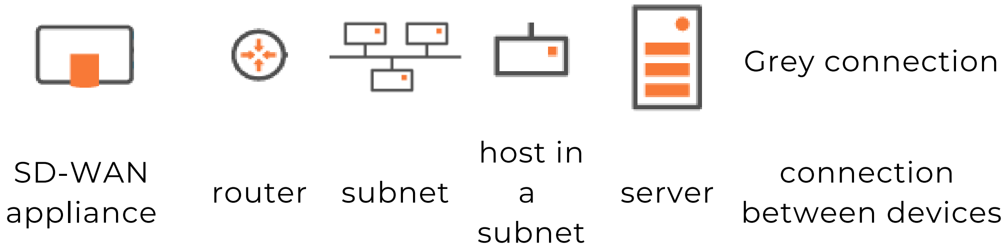
This second deployment uses two appliances with the same AS but two subnets and two local peers. It also requires a static route from the first appliance to the second one. This Data Center deployment case ensures transit traffic routing, i.e. the two appliances are used to interconnect two regional networks. It is complementary to "Use Case 2".

This configuration is done on the LAN panel of each appliance.

Use Case 4B

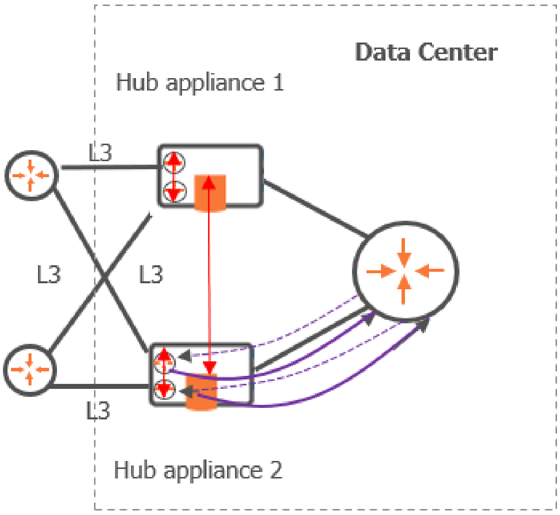


Graph legend



> **Note:** A router may be a CE Router (MPLS Router), an Internet Access Router or a Core Router.

The arrows on the following diagram correspond to the configuration steps explained below.

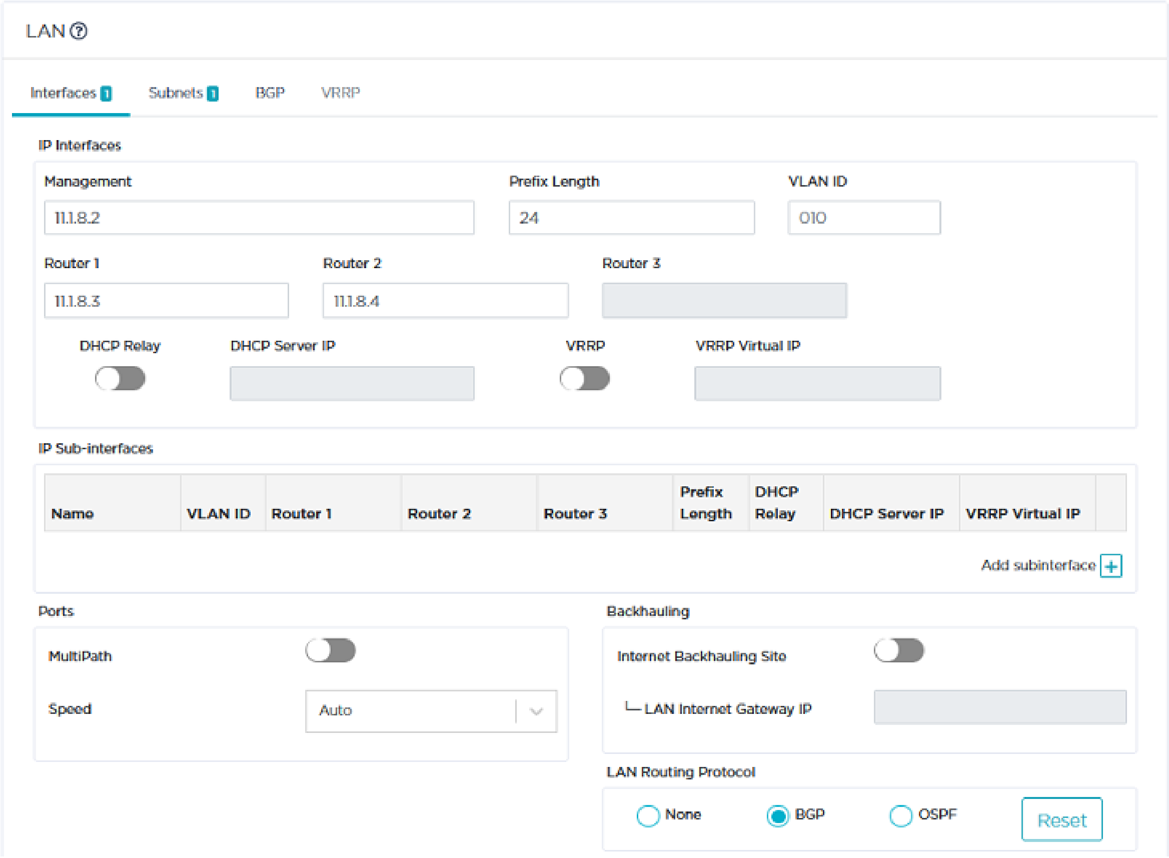


As you already configured the Data Center first hub appliance in Use Case 2, refer to "Configuring the LAN".

Data Center second hub appliance

First Step (solid purple arrows)

1 After you have defined the interfaces of the Data Center second hub appliance (see "Router Mode"), configure its LAN. On "Use Case 4B" diagram, LAN information is displayed in blue.



IP Interfaces

Management: 11.1.8.2
Prefix Length: 24
VLAN ID: 010
Router 1: 11.1.8.3
Router 2: 11.1.8.4
Router 3:
DHCP Relay: off
DHCP Server IP:
VRRP: off
VRRP Virtual IP:

IP Sub-interfaces

Name	VLAN ID	Router 1	Router 2	Router 3	Prefix Length	DHCP Relay	DHCP Server IP	VRRP Virtual IP

Add subinterface +

Ports

MultiPath: off
Speed: Auto

Backhauling

Internet Backhauling Site: off
└ LAN Internet Gateway IP:

LAN Routing Protocol

○ None ● BGP ○ OSPF Reset

2 Click the **Interfaces** tab.

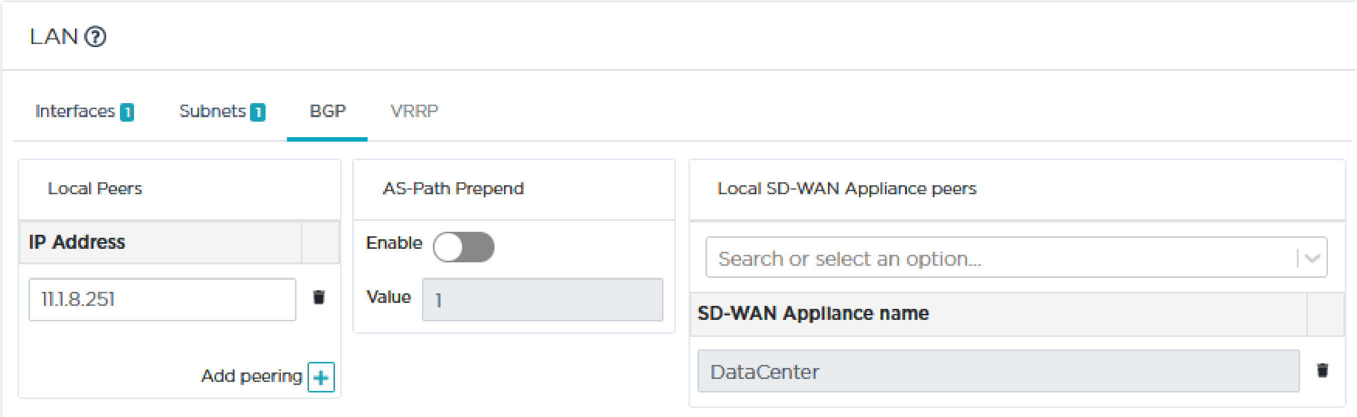
- Enter the appliance Management IP address (11.1.8.2), Prefix Length (24). The Management IP address is used for communicating with other appliances, the ZTP Server and the Orchestrator.
- Use the default **Auto Generated** option (creation window only) to let the system allocate LAN addresses automatically to the Routers (Router X IP = Management IP + X) linked to the WANs that you configured for this appliance. Also refer to "IP Address allocation".

  In this example, Router 1 and Router 2 IP addresses will be automatically defined as they correspond to WAN1 and WAN2.
- Do not activate the DHCP Relay function. The appliance does not need to relay host requests.
- Do not enter any VLAN ID. Note that the grey values appearing in some fields of the interface are only given as examples and are not taken into account in the configuration.

3 Leave the **Subnets** panel blank. Click the ▤ icon at the right of the Site Name in the identification panel of the second appliance. The existing subnets are displayed.

4 Select BGP as LAN Routing Protocol, click the **BGP** tab and the Add peering icon ⊞.

The Data Center appliance exchanges its routing tables with the local router using iBGP.



IP Address
11.1.8.251

Enable: ○

Value: 1

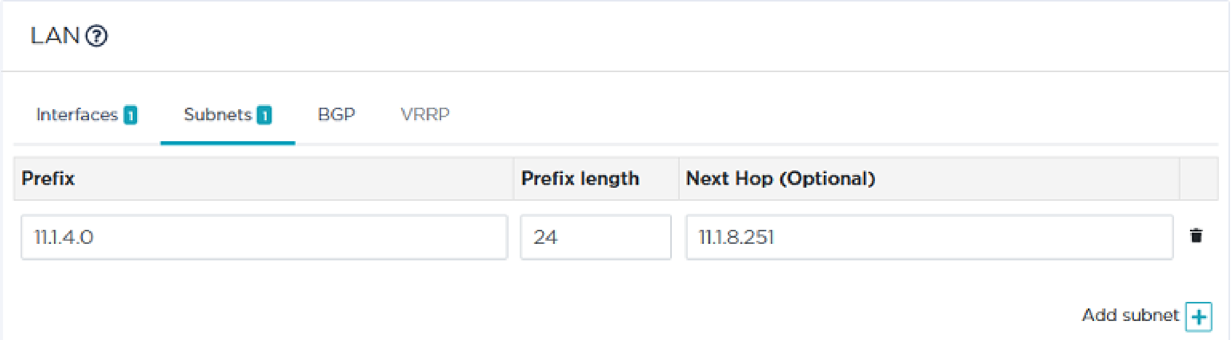
SD-WAN Appliance name
DataCenter

- Define the Core Router as the appliance BGP local peer (11.1.8.251).
- Validate your settings by hitting the **Create** or **Update** buttons.

Second Step (red arrows)

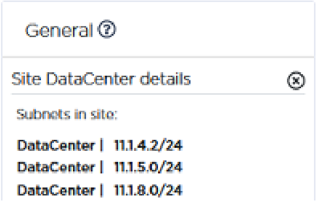
5 Define a static route between the two Data Center appliances as follows:

- Click the **Subnets** tab and the Add subnet icon ⊞.



Prefix	Prefix length	Next Hop (Optional)
11.1.4.0	24	11.1.8.251

- Enter the subnet of the Data Center **first** appliance by entering its prefix (11.1.4.0), prefix length (24) and next hop (11.1.8.251).
- On the **BGP** panel, select the first appliance name (DataCenter) from the stack of appliance names.
- Validate your settings by hitting the **Update** button.
- Check the existing subnets in the identification panel of the appliance:



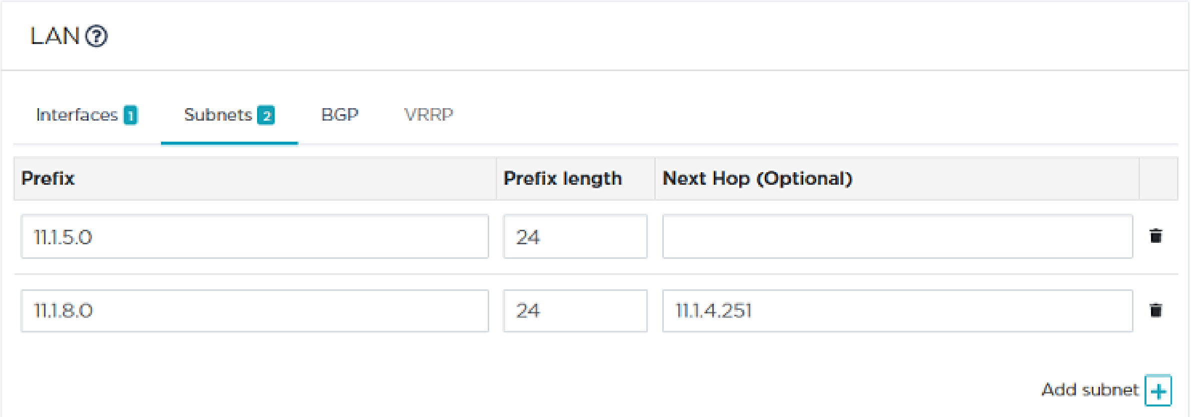
Site DataCenter details

Subnets in site:

DataCenter | 11.1.4.2/24
DataCenter | 11.1.5.0/24
DataCenter | 11.1.8.0/24

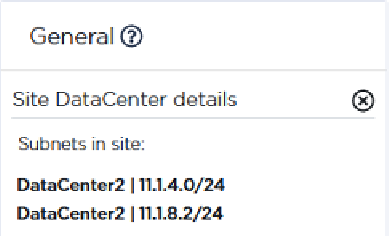
Data Center first hub appliance

- Click the **Subnets** tab and the Add subnet icon + .



Prefix	Prefix length	Next Hop (Optional)
11.1.5.0	24	
11.1.8.0	24	11.1.4.251

- Enter the subnet of the Data Center **second** appliance by entering its prefix (11.1.8.0), prefix length (24) and next hop (11.1.4.251).
- Validate your settings by hitting the **Update** button.
- Check the existing subnets in the identification panel of the appliance:



Subnets in site:

DataCenter2 | 11.1.4.0/24
DataCenter2 | 11.1.8.2/24

6 Define traffic routing priorities through the WAN1/WAN2 Preference values of each appliance. The highest Preference value implies priority.

If WAN Preference values are identical, the system gives priority to the highest IP addresses. By default, Hub Preference values and Spoke Preference values are the same for a specific tunnel; if you modify any Spoke Preference value, it is automatically edited on the related Hub.

Validate your configuration.

Third Step (dashed purple arrows)

This configuration cannot be done through the SD-WAN Orchestrator; you must configure these connections manually. However, the IP addresses of appliance routers are specified in the LAN section.

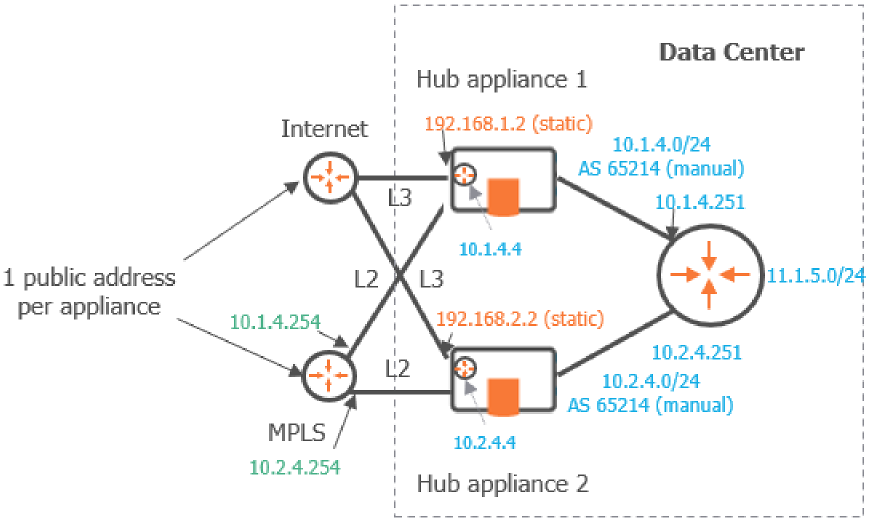
7 In the Network -> Advanced Configuration window, add the 'DataCenter2' hub appliance as Time Synchronization Server. Then click **Update**.

Configuring a multi-appliance Hybrid Data Center through iBGP

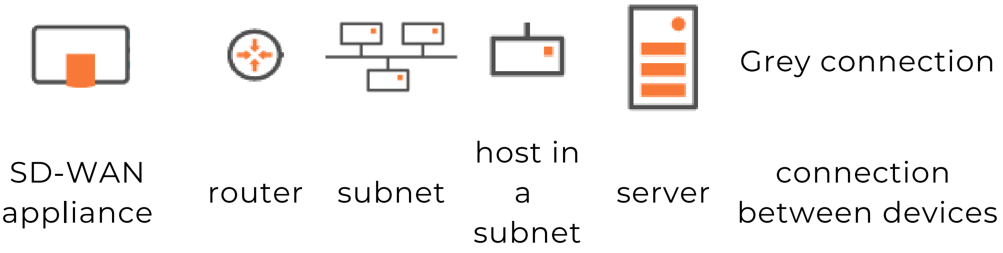
This deployment uses two appliances with the same AS but two subnets and two local peers. It also requires a static route from the first appliance to the second one. This Data Center deployment case ensures transit traffic routing, i.e. the two appliances are used to interconnect two regional networks. It is complementary to "Use Case 1".

This configuration is done on the LAN panel of each appliance.

Use Case 4C

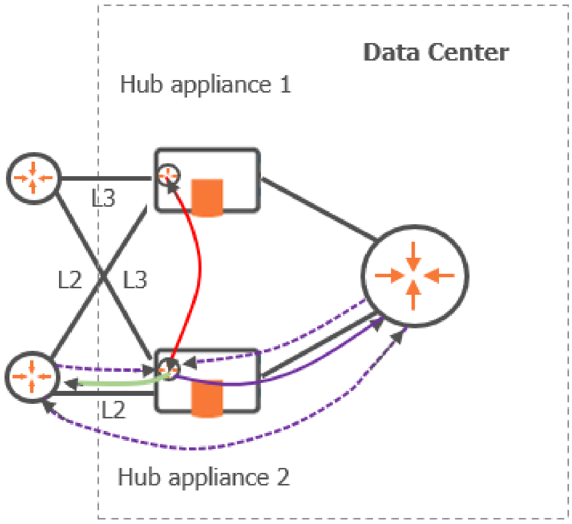


Graph legend



Note: A router may be a CE Router (MPLS Router), an Internet Access Router or a Core Router.

The arrows on the following diagram correspond to the configuration steps explained below.

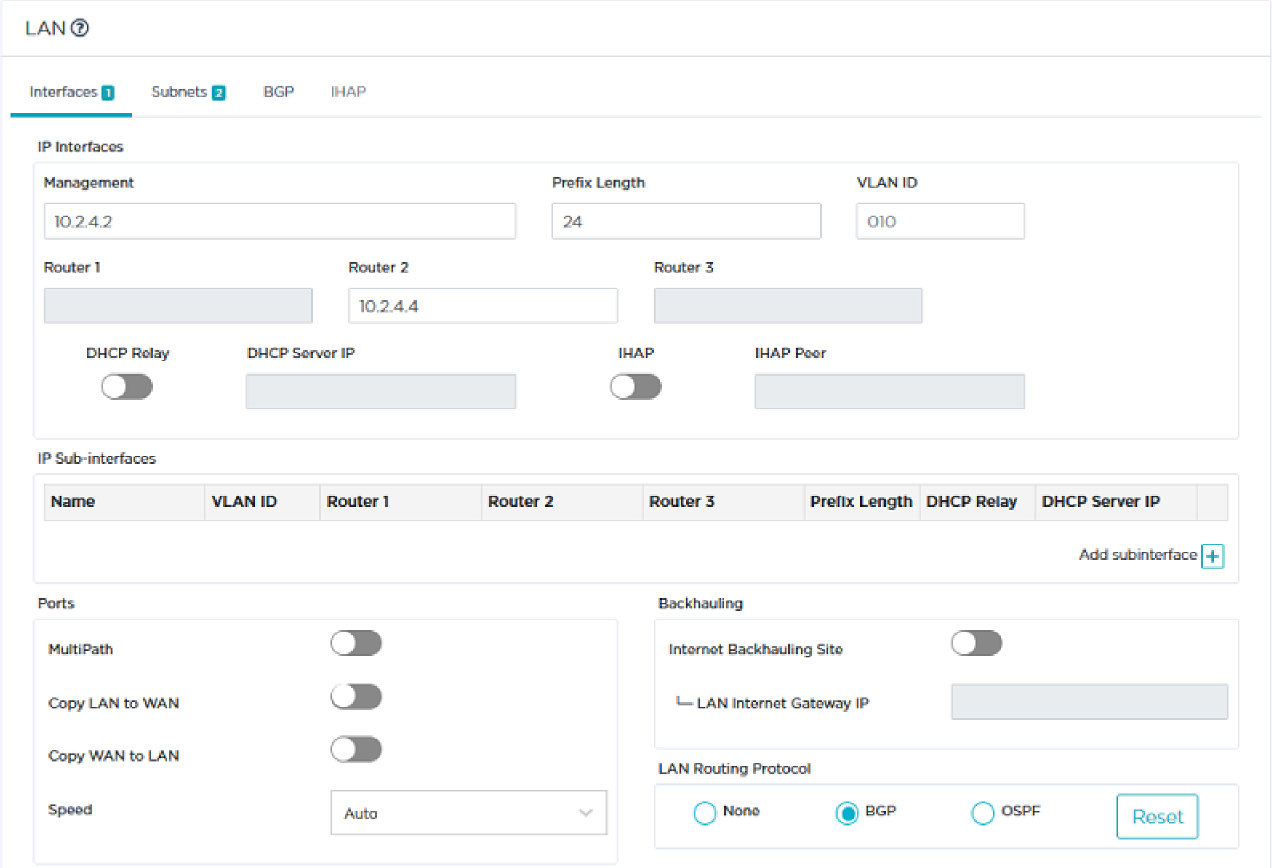


As you already configured the Data Center first hub appliance in Use Case 1, refer to "Configuring the LAN".

Data Center second hub appliance

First Step (solid purple arrow)

1 After you have defined the interfaces of the Data Center second hub appliance (see "Hybrid Mode"), configure its LAN. On "Use Case 4C" diagram, LAN information is displayed in blue.



LAN ⓘ

Interfaces 1 | Subnets 2 | BGP | IHAP

IP Interfaces

Management: 10.2.4.2

Prefix Length: 24

VLAN ID: 010

Router 1:

Router 2: 10.2.4.4

Router 3:

DHCP Relay: off

DHCP Server IP:

IHAP: off

IHAP Peer:

IP Sub-interfaces

Name	VLAN ID	Router 1	Router 2	Router 3	Prefix Length	DHCP Relay	DHCP Server IP

Add subinterface ⊞

Ports

MultiPath: off

Copy LAN to WAN: off

Copy WAN to LAN: off

Speed: Auto

Backhauling

Internet Backhauling Site: off

└ LAN Internet Gateway IP:

LAN Routing Protocol

○ None ● BGP ○ OSPF

Reset

2 Click the **Interfaces** tab.

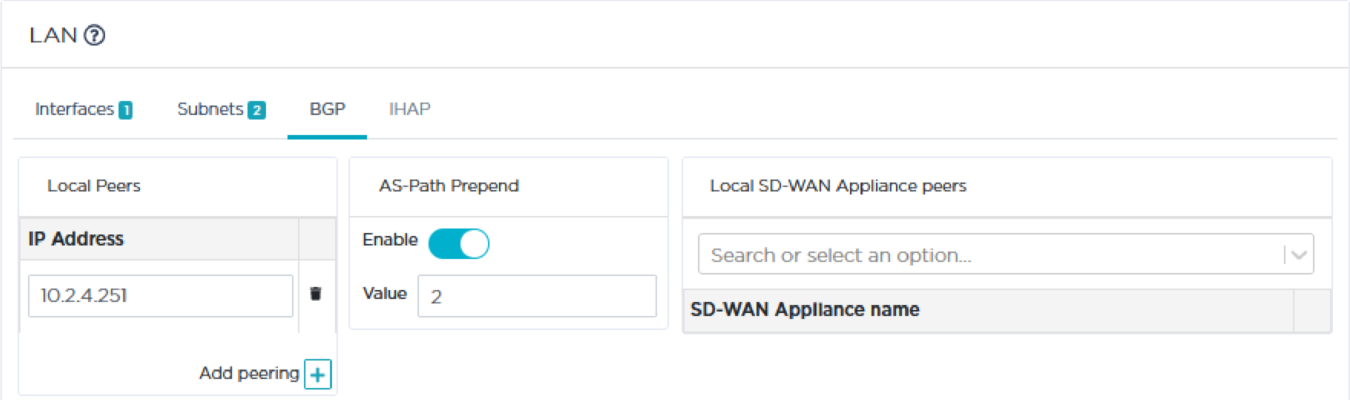
- Enter the appliance Management IP address (10.2.4.2), Prefix Length (24).
- Use the default **Auto Generated** option (creation window only) to let the system allocate LAN addresses automatically to the Routers (Router X IP = Management IP + X) linked to the WANs in Router mode that you configured for this appliance. Also refer to "IP Address allocation".

  In this example, Router 2 IP address will be automatically defined as it corresponds to WAN2.
- Do not activate the DHCP Relay function. The appliance does not need to relay host requests.
- Do not enter any VLAN ID. Note that the grey values appearing in some fields of the interface are only given as examples and are not taken into account in the configuration.

3 Click the **Subnets** tab and the Add subnet icon ⊞. Enter the 11.1.5.0 subnet IP Address, Prefix length (24).

4 Select BGP as LAN Routing Protocol, click the **BGP** tab and the Add peering icon ⊞.

The Data Center appliance exchanges its routing tables with the local router using iBGP.



LAN

Interfaces 1 Subnets 2 BGP IHAP

Local Peers

IP Address

10.2.4.251

Add peering

AS-Path Prepend

Enable: on

Value: 2

Local SD-WAN Appliance peers

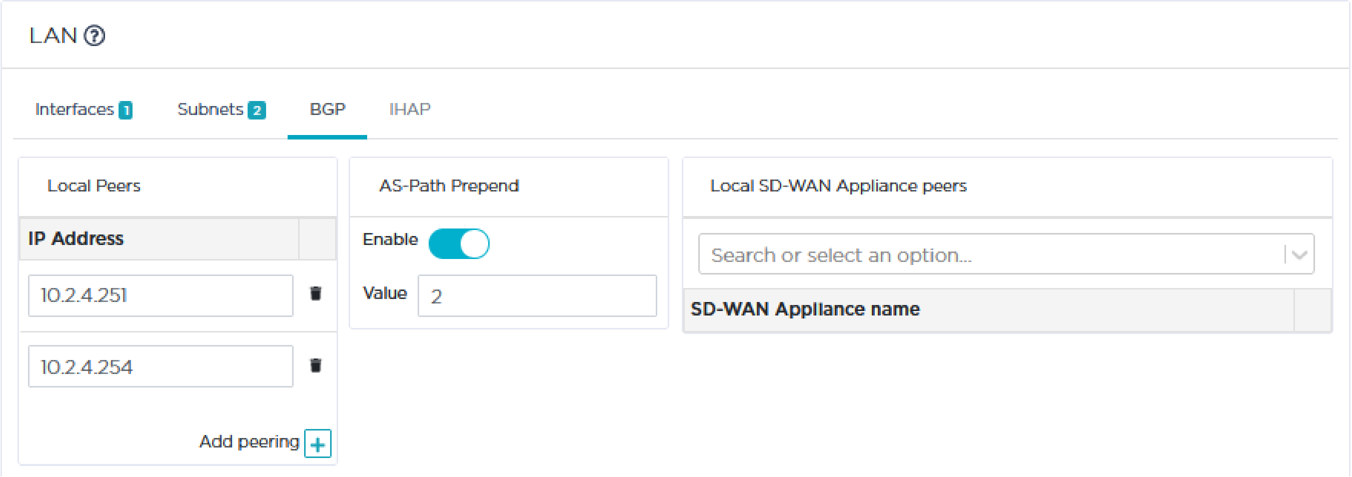
Search or select an option...

SD-WAN Appliance name

- Define the Core Router as the appliance BGP local peer (10.2.4.251).
- Activate AS Path Prepending and enter 2 in the Value field. Refer to "Configuring BGP".

Second Step (green arrow)

5 On the **BGP** panel of the Data Center second hub appliance (DataCenter2), enter 10.2.4.254 as the second Local Peer IP Address.



LAN

Interfaces 1 Subnets 2 BGP IHAP

Local Peers

IP Address

10.2.4.251

10.2.4.254

Add peering

AS-Path Prepend

Enable: on

Value: 2

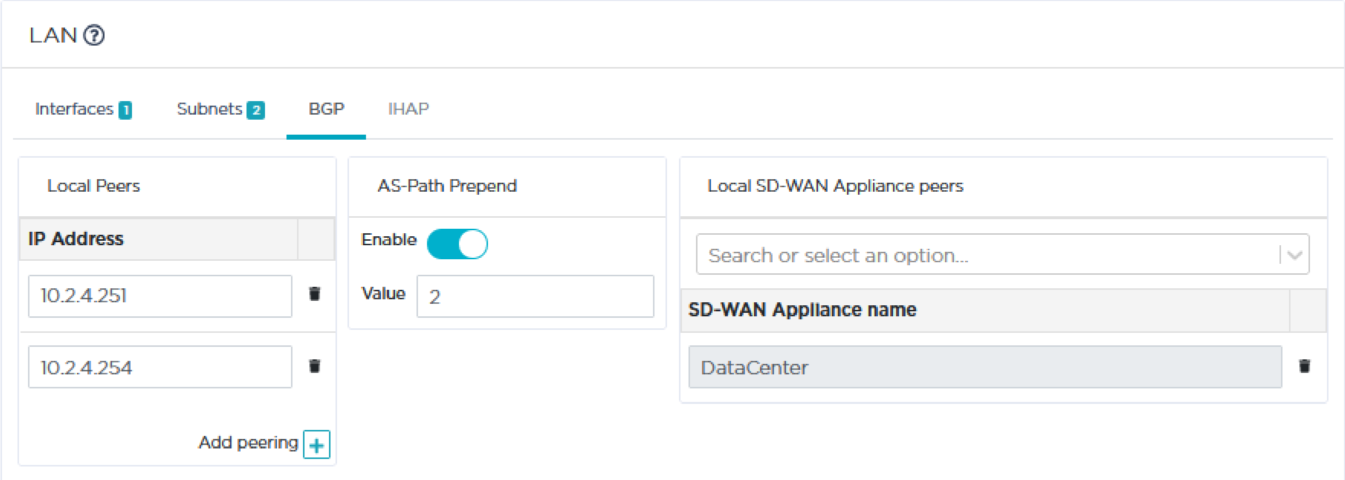
Local SD-WAN Appliance peers

Search or select an option...

SD-WAN Appliance name

Third Step (red arrow)

6 Still on the **BGP** panel of the Data Center second hub appliance (DataCenter2), select the first appliance name (DataCenter) from the stack of appliance names.



Local Peers

IP Address
10.2.4.251
10.2.4.254

AS-Path Prepend

Enable ●

Value 2

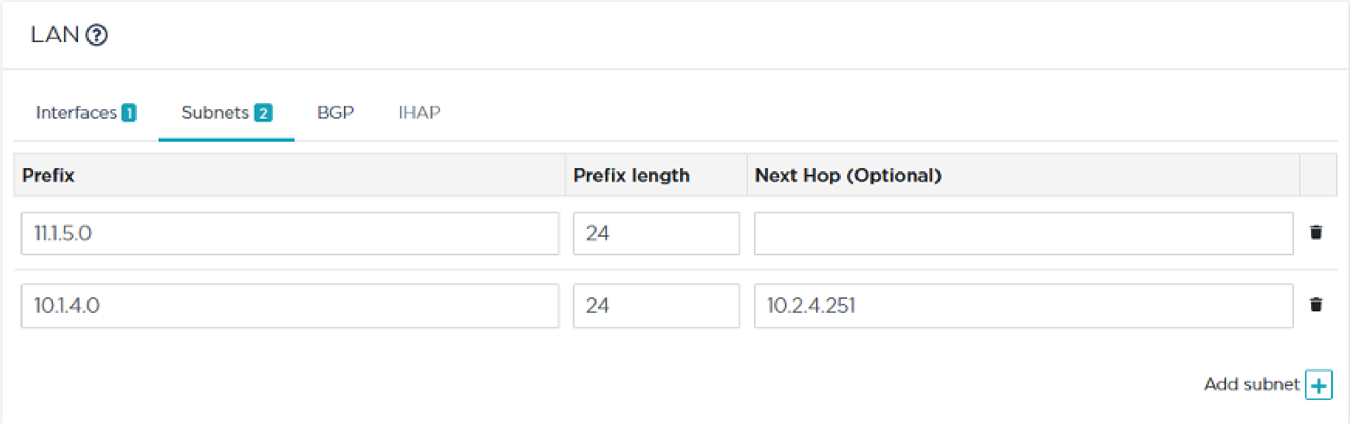
Local SD-WAN Appliance peers

Search or select an option...

SD-WAN Appliance name
DataCenter

7 Define a static route between the two Data Center appliances as follows:

- Click the **Subnets** tab and the Add subnet icon + .



Prefix	Prefix length	Next Hop (Optional)
11.1.5.0	24	
10.1.4.0	24	10.2.4.251

- Enter the subnet of the Data Center **first** appliance by entering its prefix (10.1.4.0), prefix length (24) and next hop (10.2.4.251).

8 Validate your settings by hitting the **Update** button.

Data Center first hub appliance

9 Execute the same configuration steps as those described in the previous section for the Data Center second hub appliance.

10 Define traffic routing priorities through the WAN2 Preference values of each appliance. The highest Preference value implies priority.

If WAN Preference values are identical, the system gives priority to the highest IP addresses. By default, Hub Preference values and Spoke Preference values are the same for a specific tunnel; if you modify any Spoke Preference value, it is automatically edited on the related Hub.

11 Validate your configuration.

Fourth Step (dashed purple arrows)

This configuration cannot be done through the SD-WAN Orchestrator; you must configure these connections manually. However, the IP addresses of appliance routers are specified in the LAN section.

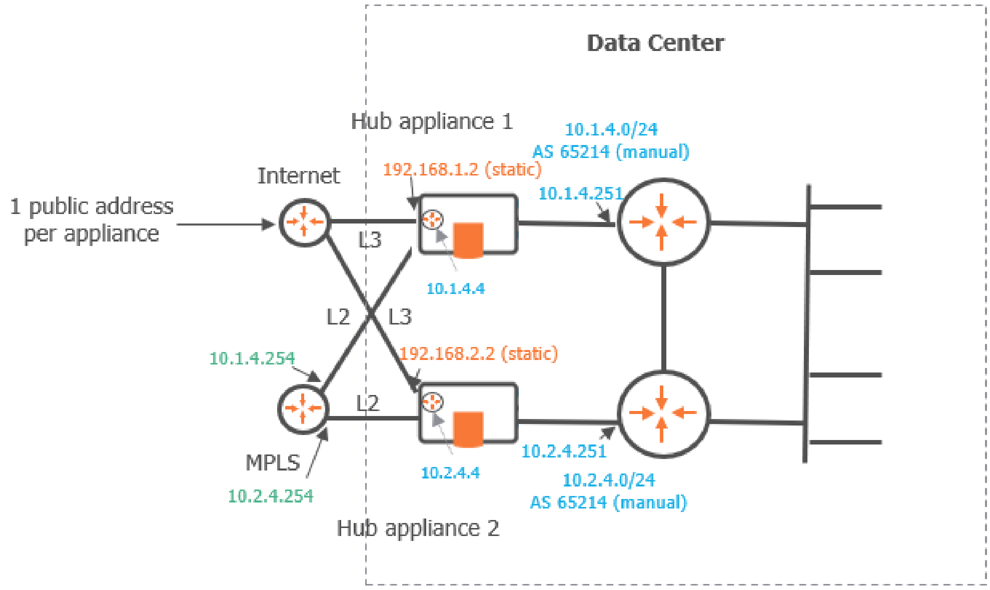
12 In the Network -> Advanced Configuration window, add the 'DataCenter2' hub appliance as Time Synchronization Server. Then click **Update**.

Configuring a multi-appliance Hybrid Data Center through OSPF

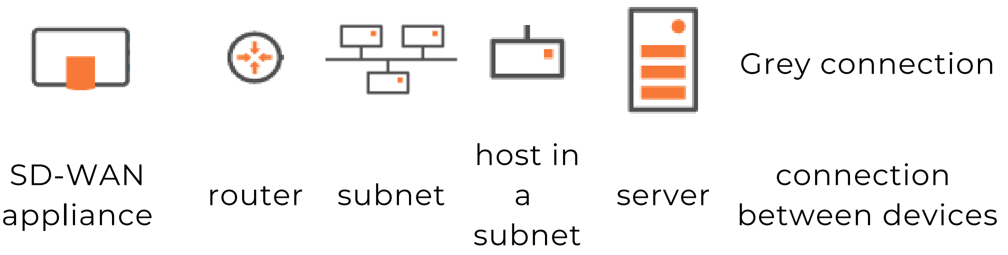
This deployment describes how to configure a Data Center with two appliances through OSPF. The objectives of this deployment is high availability: if one hub appliance is in bad health, the other appliance is used as backup appliance. It is complementary to "Use Case 1".

This configuration is done on the LAN panel of each appliance.

Use Case 5



Graph legend



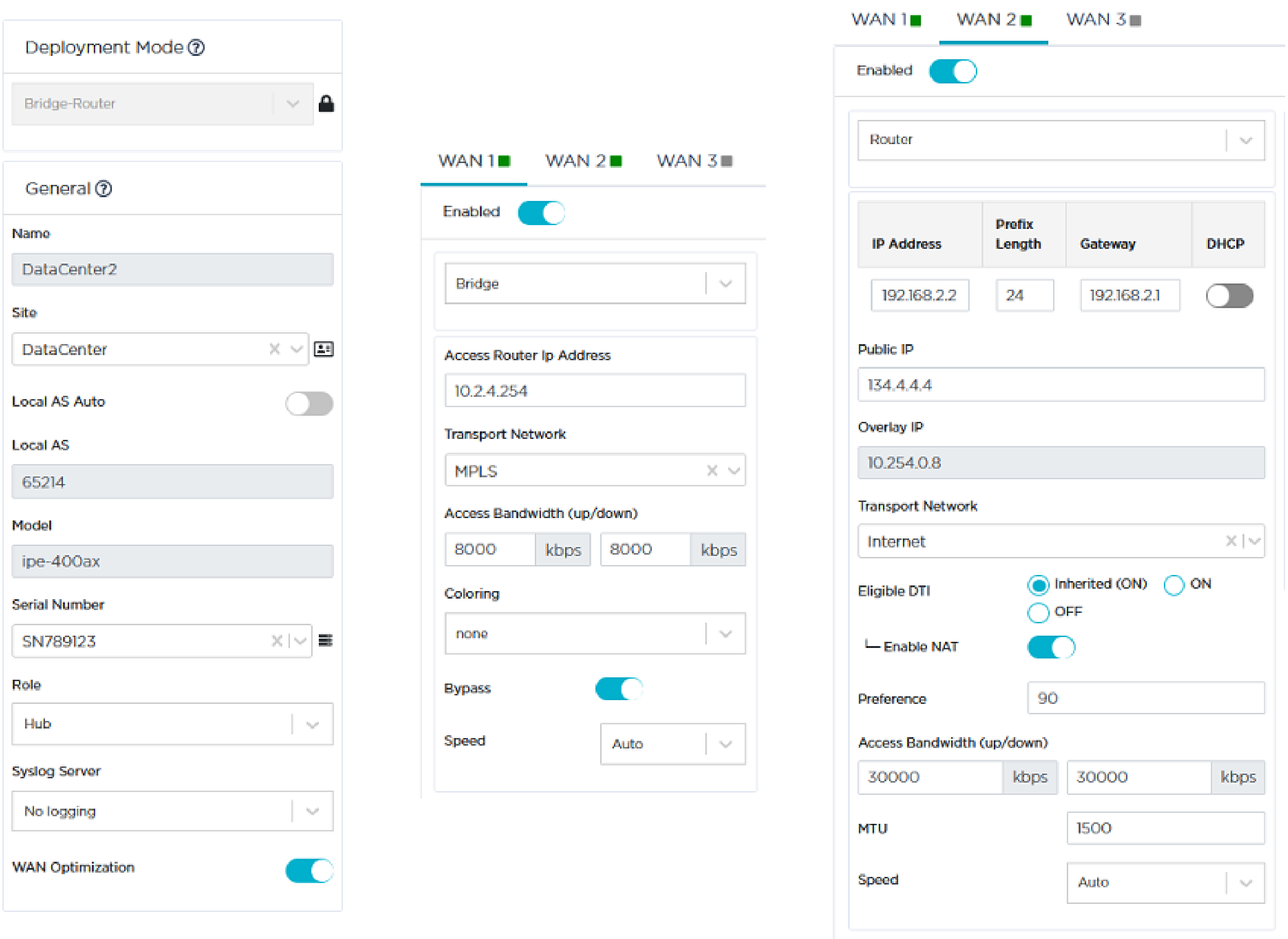
> **Note:** A router may be a CE Router (MPLS Router), an Internet Access Router or a Core Router.

As you already configured the Data Center first hub appliance in Use Case 1, refer to "Configuring the LAN".

There is one prerequisite which is the necessary configuration of the second hub appliance of the Data Center.

Data Center second hub appliance

1 Identify and configure the hub appliance WANs as follows:



Deployment Mode
Bridge-Router

General
Name: DataCenter2
Site: DataCenter
Local AS Auto: off
Local AS: 65214
Model: ipe-400ax
Serial Number: SN789123
Role: Hub
Syslog Server: No logging
WAN Optimization: on

WAN 1 🟩 | WAN 2 🟩 | WAN 3
Enabled: on
Bridge
Access Router Ip Address: 10.2.4.254
Transport Network: MPLS
Access Bandwidth (up/down): 8000 kbps / 8000 kbps
Coloring: none
Bypass: on
Speed: Auto

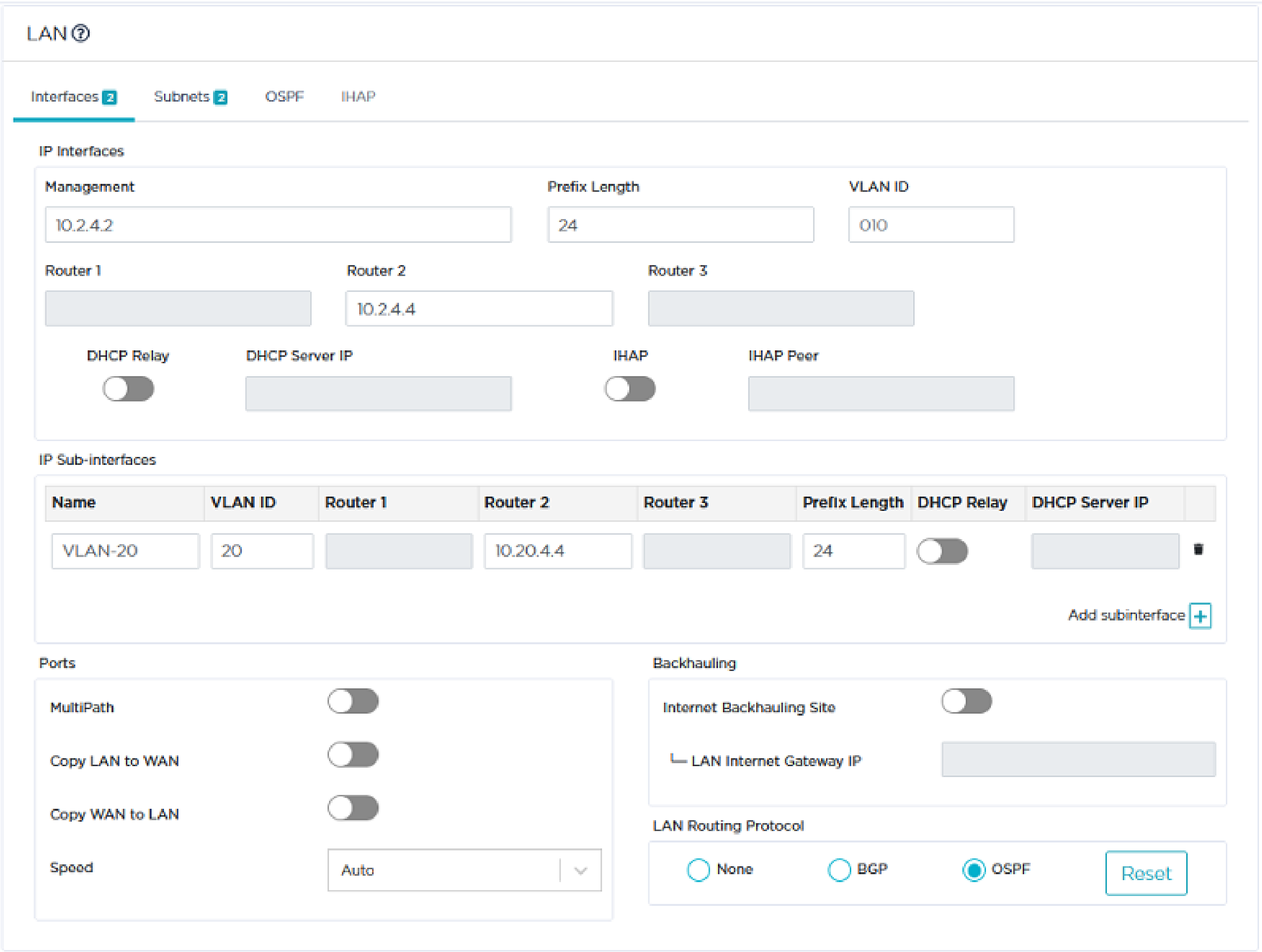
WAN 1 🟩 | WAN 2 🟩 | WAN 3
Enabled: on
Router

IP Address	Prefix Length	Gateway	DHCP
192.168.2.2	24	192.168.2.1	off

Public IP: 134.4.4.4
Overlay IP: 10.254.0.8
Transport Network: Internet
Eligible DTI: ● Inherited (ON) ○ ON ○ OFF
└ Enable NAT: on
Preference: 90
Access Bandwidth (up/down): 30000 kbps / 30000 kbps
MTU: 1500
Speed: Auto

2 Then configure its LAN. In the Interfaces window, select OSPF as the LAN Routing Protocol.

3 Click the Add subinterface icon +. Enter 20 as VLAN ID, 10.20.4.4 as the sub-interface IP address for Router 2 and 24 as Prefix Length. Each VLAN corresponds to an OSPF network area.



LAN ⓘ

IP Interfaces

Management: 10.2.4.2	Prefix Length: 24	VLAN ID: 010
Router 1:	Router 2: 10.2.4.4	Router 3:

DHCP Relay: ○ DHCP Server IP: IHAP: ○ IHAP Peer:

IP Sub-interfaces

Name	VLAN ID	Router 1	Router 2	Router 3	Prefix Length	DHCP Relay	DHCP Server IP
VLAN-20	20		10.20.4.4		24	○	

Ports

MultiPath ○

Copy LAN to WAN ○

Copy WAN to LAN ○

Speed: Auto

Backhauling

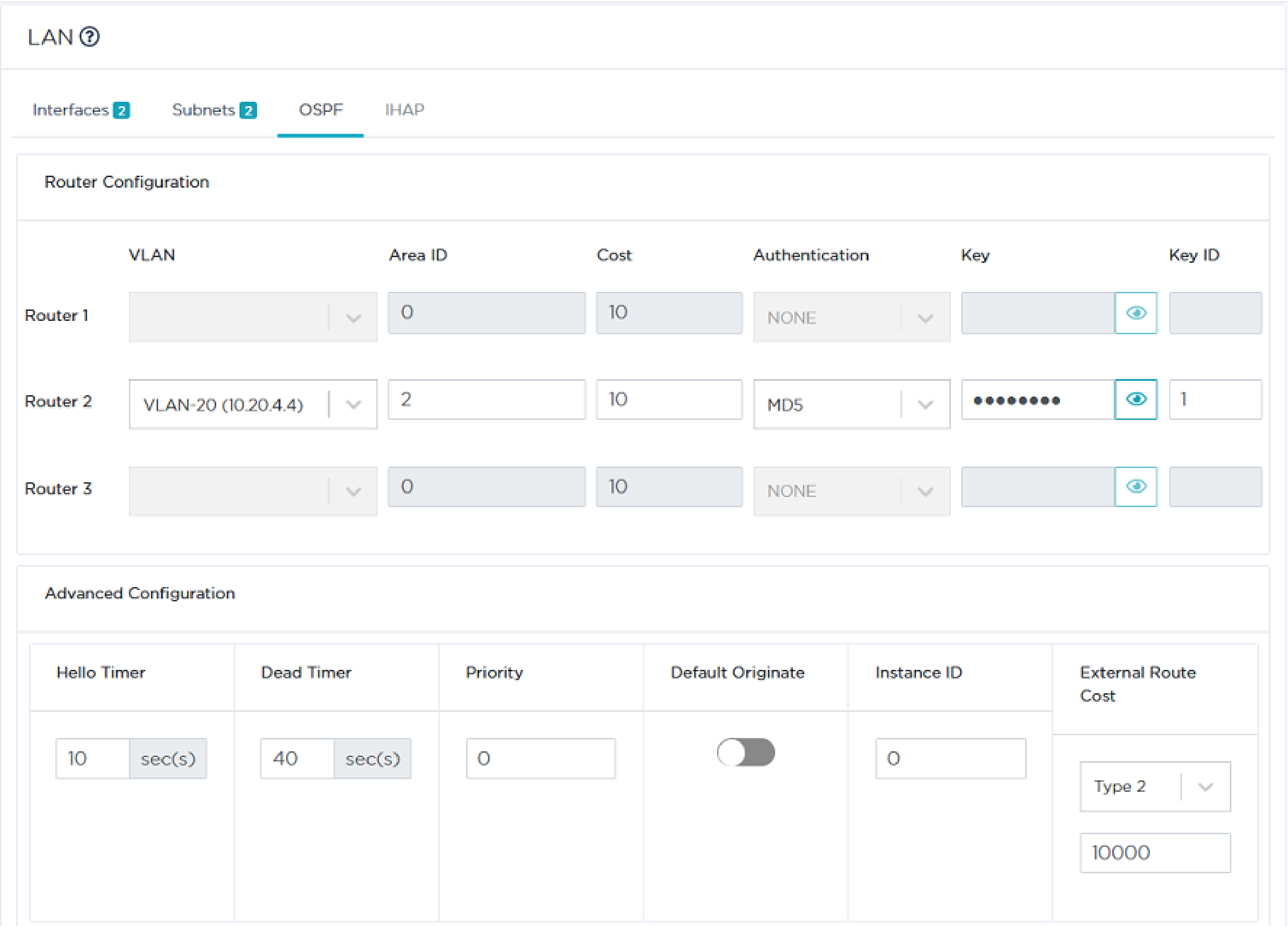
Internet Backhauling Site ○

└ LAN Internet Gateway IP

LAN Routing Protocol

○ None ○ BGP ● OSPF

4 Click the **OSPF** tab.



Router Configuration

	VLAN	Area ID	Cost	Authentication	Key	Key ID
Router 1		0	10	NONE		
Router 2	VLAN-20 (10.20.4.4)	2	10	MD5	••••••••	1
Router 3		0	10	NONE		

Advanced Configuration

Hello Timer	Dead Timer	Priority	Default Originate	Instance ID	External Route Cost
10 sec(s)	40 sec(s)	0		0	Type 2 10000

5 Configure Router 2 as explained in "Configuring OSPF" for the Data Center first hub appliance.

Enter 2 in the Area ID field.

6 In the Advanced Configuration panel, define the **External Route Cost** specific parameter which implements the high availability mechanism between the two Data Center appliances.

An external route corresponds to the traffic received by the appliance from the overlay.

- **Type 1**: the Metric value and the Cost of each link are taken into account to route the traffic.

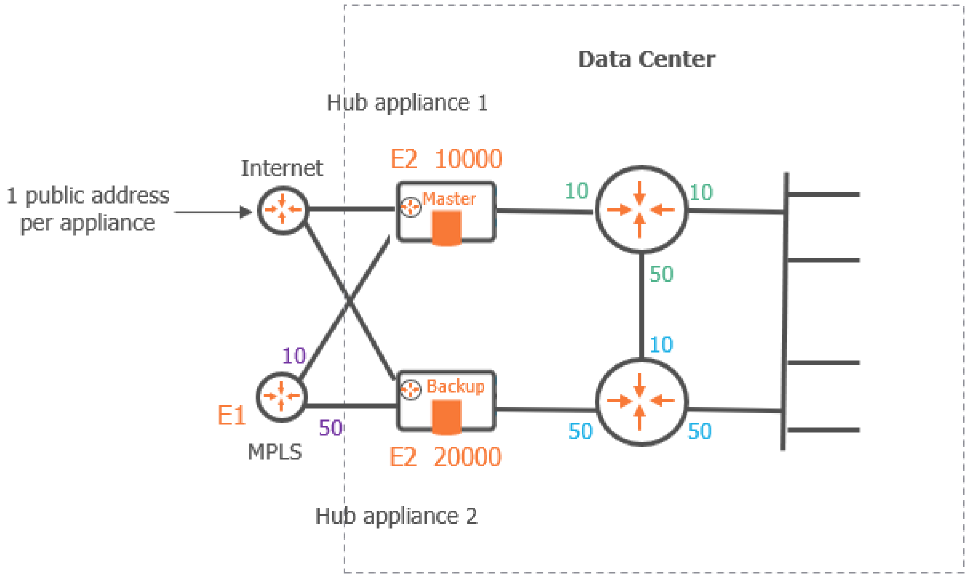
  Cost: this parameter must be configured on your personal routers. The following image illustrates a consistent configuration of link costs. Note that a low cost has the priority over a higher cost.

  Metric value: this value corresponds to a distance. The lowest value is the best one for routing the traffic.

  To summarize Type 1 procedure, configure the MPLS CE router as E1. Then, adjust interface costs on your customer routers.

- **Type 2**: only the Metric value (distance) is taken into account. Set a E2 lower metric value on the Master appliance than on the Backup appliance.

  For the second appliance of the current Use Case, select Type 2 and enter 20000 as the Metric value.



> **Note:** Type 1 takes priority over Type 2.

Data Center first hub appliance

7 Execute the same configuration as described in the previous step.

8 In the External Route Cost fields, check that you selected Type 2 and entered 10000 as the Metric value.

  Since only the Metric values are taken into account for both Data Center appliances (Type 2), the first hub appliance with the lowest value is the Master whereas the second hub appliance is the Backup.

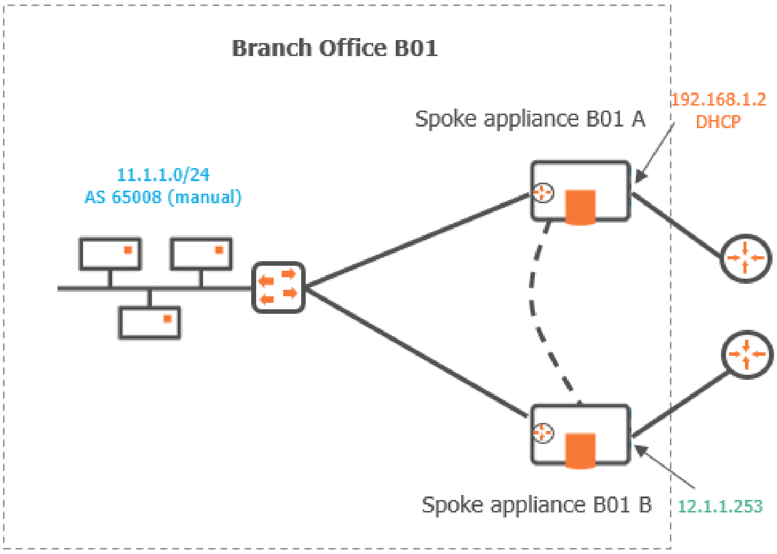
9 Click **Update**.

Configuring a multi-appliance Branch Office Site through VRRP

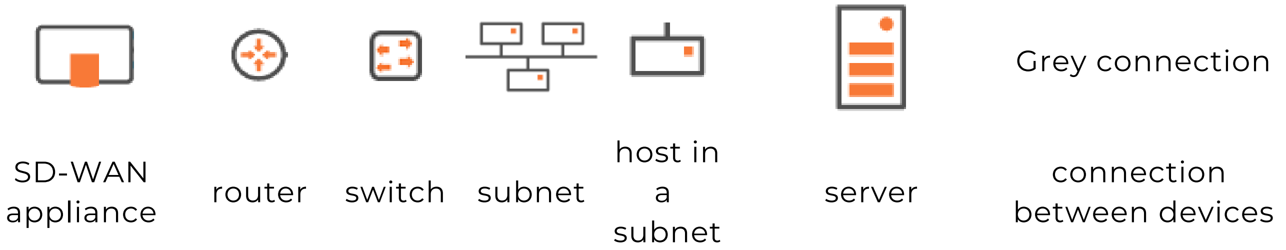
This section describes how to configure a Branch Office Site with two appliances having the same AS in the same subnet, through VRRP (Virtual Router Redundancy Protocol). The objective of this deployment is high availability, i.e. if the master appliance is in bad health, the other appliance is used as backup appliance.

> **Warning:** VRRP deployment is not supported for a Branch Office Site with two full router appliances in multipath mode.

Use Case 6



Graph legend

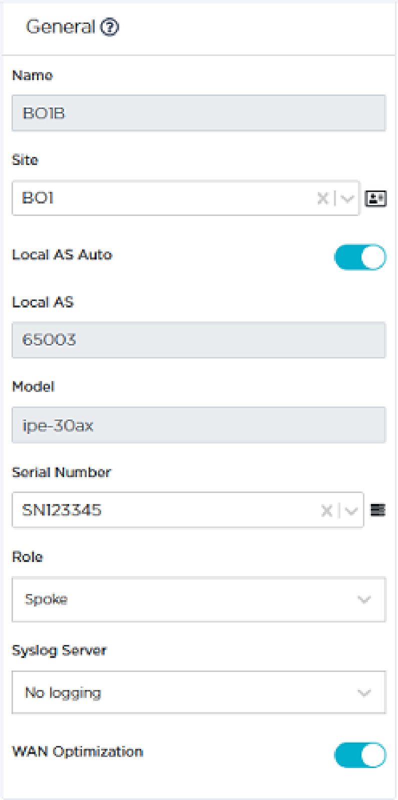


> **Note:** A router may be a CE Router (MPLS Router), an Internet Access Router or a Core Router.

Since the following Use Case is complementary to "Use Case 2", there is one prerequisite which is the necessary configuration of the second spoke appliance for

Branch Office 1. For detailed explanations, refer to "Configuring the Branch Office appliances".

1 Identify this spoke appliance as follows:



General

Name: B01B

Site: B01

Local AS Auto: on

Local AS: 65003

Model: ipe-30ax

Serial Number: SN123345

Role: Spoke

Syslog Server: No logging

WAN Optimization: on

2 Configure its LAN as follows:

- Click the **Interfaces** tab.
  - Enter the appliance Management IP Address (11.1.1.6), Prefix Length (24). The Management IP address is used for communicating with other appliances, the ZTP Server and the Orchestrator.

    > **Note:** Since the three IP addresses directly following the Management IP address (11.1.1.2) of the B01 first appliance are used for its WAN routers, enter 11.1.1.6 as the Management IP Address of the second appliance.

  - Use the default **Auto Generated** option (creation window only) to let the system allocate LAN addresses automatically to the Routers (Router X IP = Management IP + X) linked to the WANs that you configured for this appliance. Also refer to "IP Address allocation".

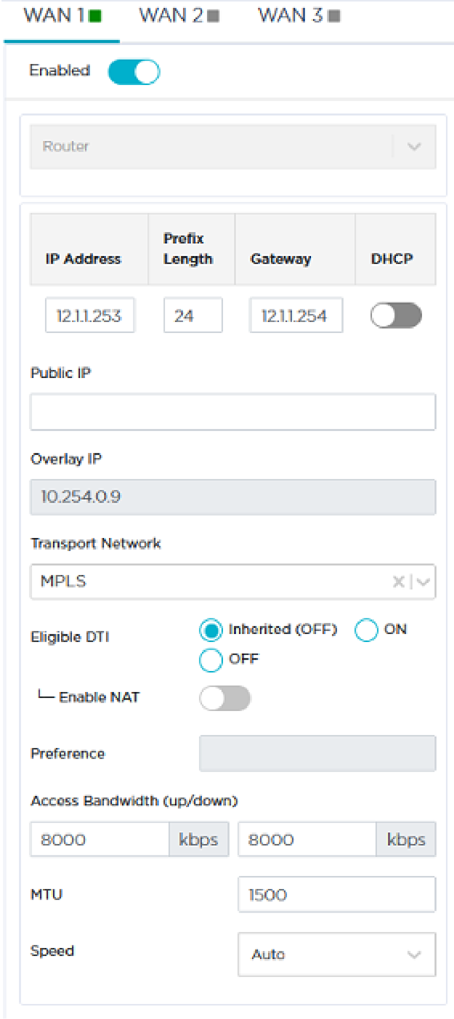
    In this example, Router 1 IP address will be automatically defined as it corresponds to WAN1.

  - Enable the DHCP Relay function and enter the DHCP Server Address (11.1.4.250). DHCP requests from the B01B appliance are propagated to the DHCP Server in the Data Center LAN.

- Do not enter any VLAN ID. Note that the grey values appearing in some fields of the interface are only given as examples and are not taken into account in the configuration.

- Do not define any **Subnets.**

3 Define its WAN1 interface as follows:



WAN 1 🟩 WAN 2 ■ WAN 3 ■

Enabled ●

Router

IP Address	Prefix Length	Gateway	DHCP
12.1.1.253	24	12.1.1.254	○

Public IP:

Overlay IP: 10.254.0.9

Transport Network: MPLS

Eligible DTI: ● Inherited (OFF) ○ ON ○ OFF

└ Enable NAT ○

Preference:

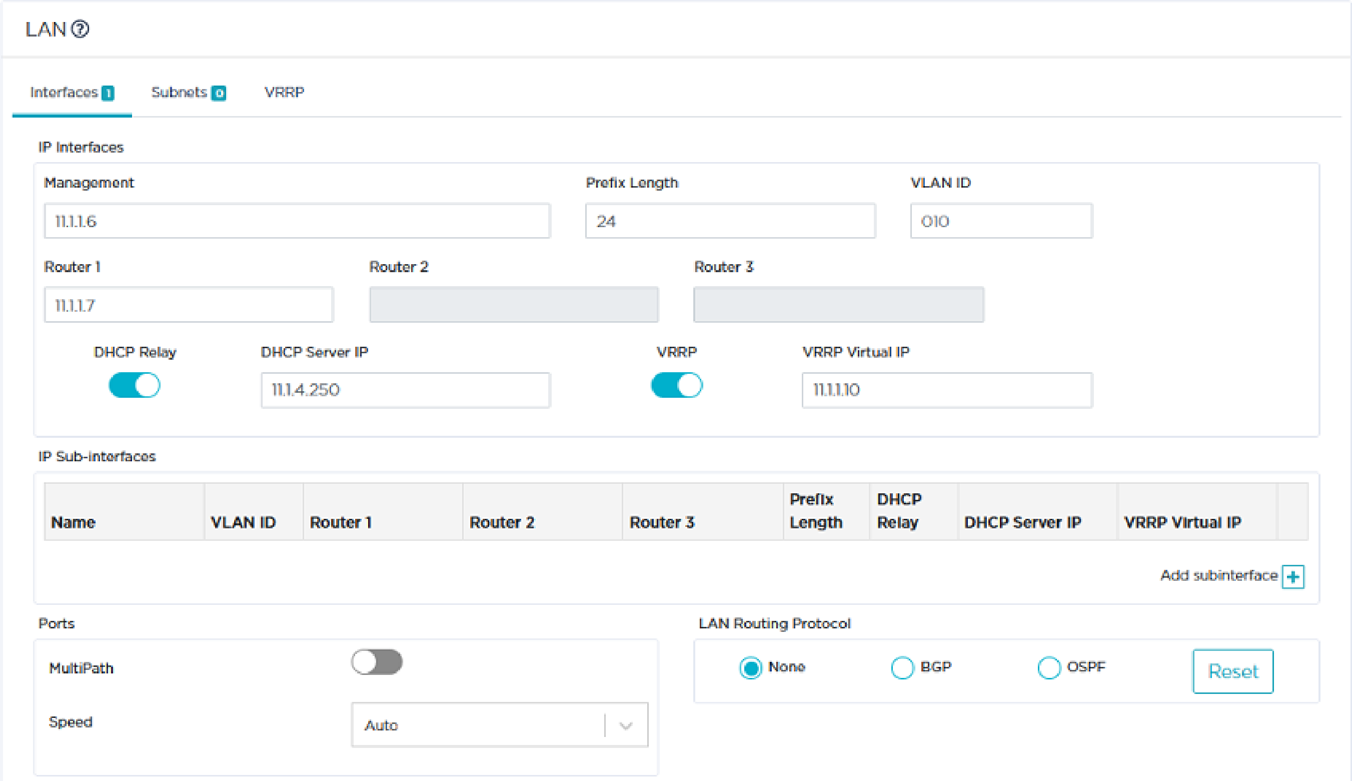
Access Bandwidth (up/down): 8000 kbps 8000 kbps

MTU: 1500

Speed: Auto

4 Then define the VRRP parameters of the **B01B appliance** to enable high availability between the two spoke appliances as illustrated in "Use Case 6" diagram.

- On the LAN panel, enable VRRP.
- Enter the VRRP Virtual router IP address: 11.1.1.10



LAN ⓘ

Interfaces 1 Subnets 0 VRRP

IP Interfaces

Management: 11.1.1.6 Prefix Length: 24 VLAN ID: 010

Router 1: 11.1.1.7 Router 2: Router 3:

DHCP Relay: on DHCP Server IP: 11.1.4.250 VRRP: on VRRP Virtual IP: 11.1.1.10

IP Sub-interfaces

Name	VLAN ID	Router 1	Router 2	Router 3	Prefix Length	DHCP Relay	DHCP Server IP	VRRP Virtual IP

Add subinterface +

Ports

MultiPath: off

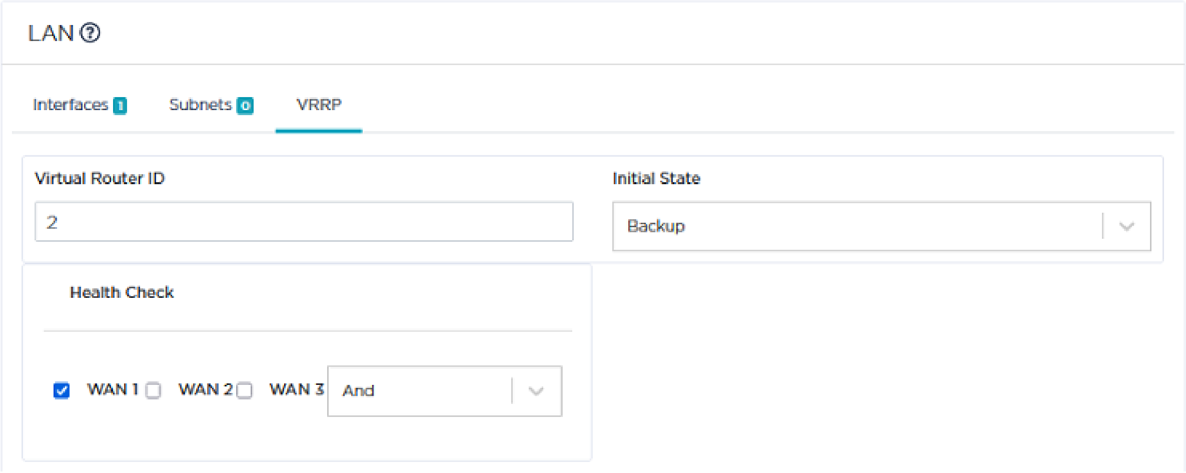
Speed: Auto

LAN Routing Protocol

● None ○ BGP ○ OSPF Reset

- Click the **VRRP** tab.
- Enter a value between 1 and 255 in the Virtual Router ID field.
- Select Backup as Initial State. This means the B01B appliance is used as the backup machine if B01 fails.

  By default, all existing WAN interfaces are checked.



LAN ⓘ

Interfaces 1 Subnets 0 VRRP

Virtual Router ID: 2

Initial State: Backup

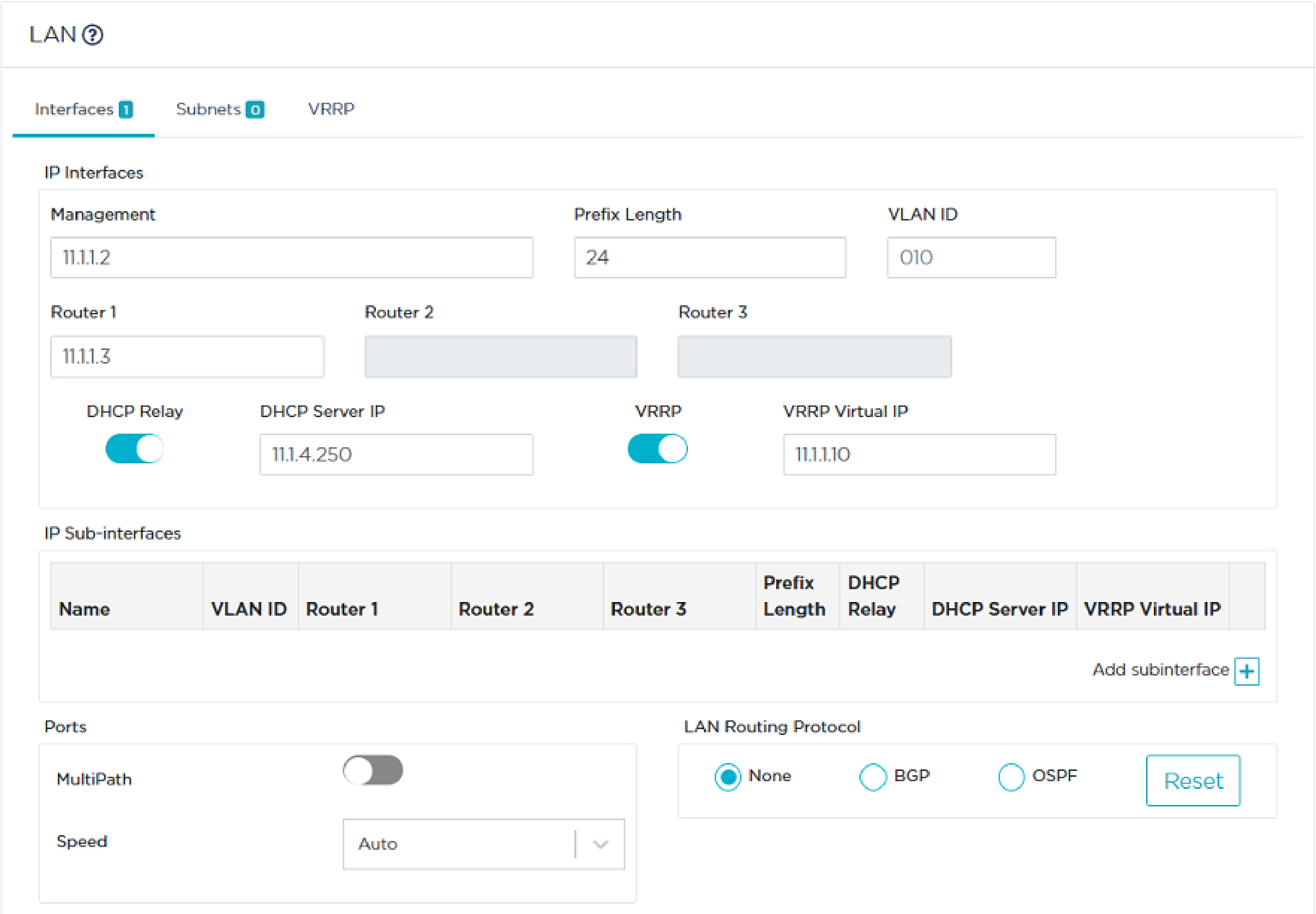
Health Check

☑ WAN 1 □ WAN 2 □ WAN 3 And

5 Validate your settings by clicking the **Create** or **Update** buttons.

6 **Edit B01 appliance**.

- On the LAN panel, enable VRRP.
- Enter the VRRP Virtual router IP address: 11.1.1.10



LAN

Interfaces 1 Subnets 0 VRRP

IP Interfaces

Management: 11.1.1.2

Prefix Length: 24

VLAN ID: 010

Router 1: 11.1.1.3

Router 2:

Router 3:

DHCP Relay: on

DHCP Server IP: 11.1.4.250

VRRP: on

VRRP Virtual IP: 11.1.1.10

IP Sub-interfaces

Name	VLAN ID	Router 1	Router 2	Router 3	Prefix Length	DHCP Relay	DHCP Server IP	VRRP Virtual IP

Add subinterface +

Ports

MultiPath: off

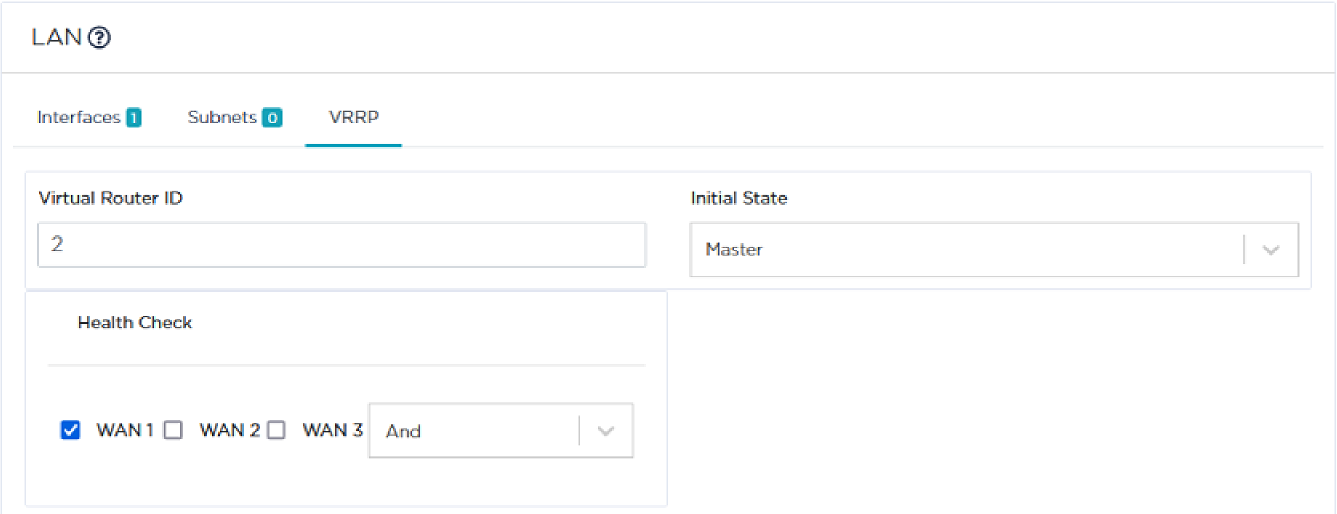
Speed: Auto

LAN Routing Protocol

● None ○ BGP ○ OSPF

- Click the **VRRP** tab.
- Enter 2 as Virtual Router ID (same ID defined for B01B).
- Select Master as Initial State.

  By default, all existing WAN interfaces are checked.



LAN

Interfaces 1 Subnets 0 VRRP

Virtual Router ID: 2

Initial State: Master

Health Check

☑ WAN 1 □ WAN 2 □ WAN 3 And

7 Validate your settings by hitting the **Create** or **Update** buttons.

8. You may optionally customize the SD-WAN Orchestrator VRRP Settings through the Advanced Configuration menu.

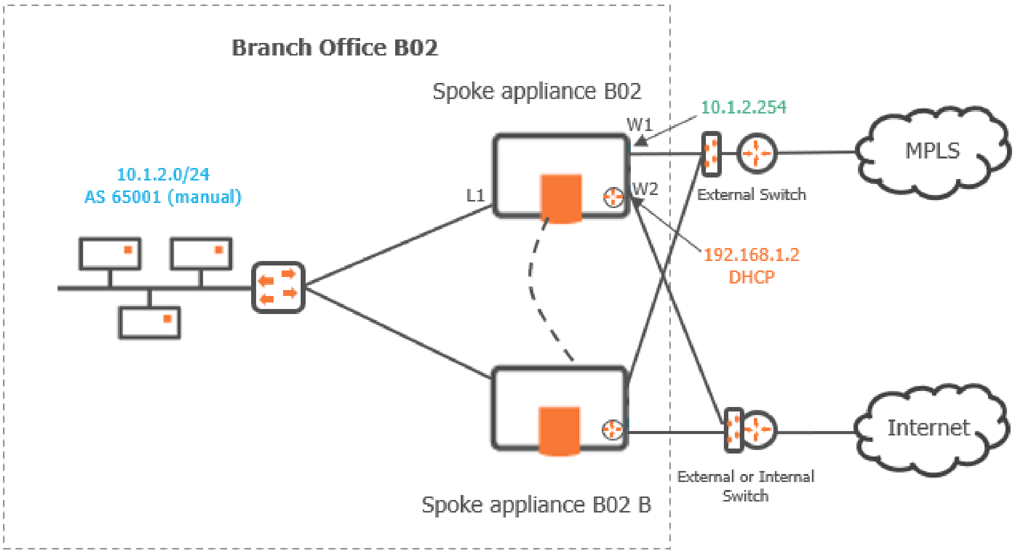
Configuring a multi-appliance Branch Office Site through IHAP

This section describes how to configure a **Hybrid Branch Office Site** with two appliances through IHAP (**Ipanema High Availability Protocol)**. The objective of this deployment is to use the backup appliance if the nominal appliance fails.

This configuration is also necessary for any Branch Office Site in **Bridge mode**.

The following Use Case illustrates a Site upgrade for HA deployment. It uses the appliance of Branch Office 2 of "Use Case 1" as the nominal appliance, and a new appliance as backup. As a reminder, B02 is deployed in bridge/router mode and is connected to the Data Center directly through the MPLS private network and over the Internet via one tunnel. Refer to "Configuring the B02 Branch Office appliance"

Use Case 7

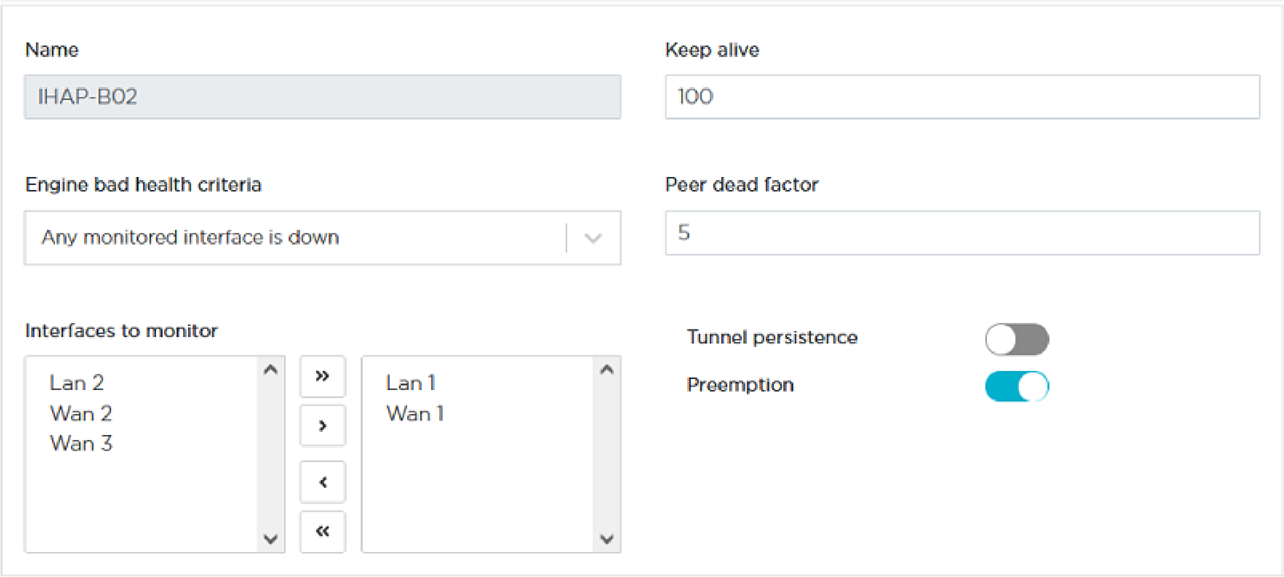


Configuring a IHAP Profile for the Site

1 Select **Network -> Advanced Configuration -> IHAP** and click the **Add Profile** button.

> **Note:** Though a Default IHAP Profile is available, it is not used in this example.

2 Type IHAP-B02 as the name of the new IHAP profile and configure it as follows:



Name: IHAP-B02

Keep alive: 100

Engine bad health criteria: Any monitored interface is down

Peer dead factor: 5

Interfaces to monitor:

Lan 2 Wan 2 Wan 3	Lan 1 Wan 1

Tunnel persistence: off

Preemption: on

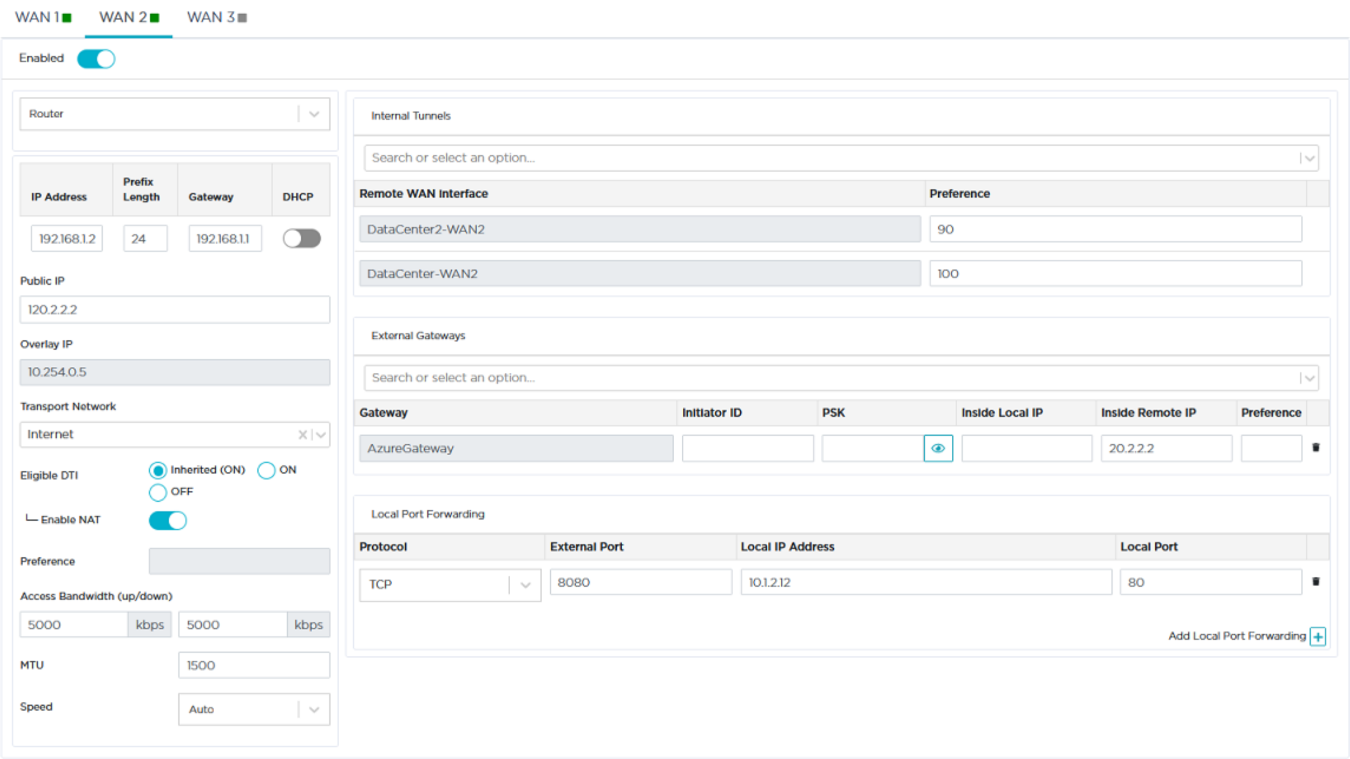
3 Refer to "IHAP" for a detailed description of the displayed parameters.

4 Click **Create** to validate your settings.

Configuring the SD-WAN appliances

Configure the existing B02 nominal appliance

1 Reconfigure B02 WAN2 interface with the current WAN3 parameters. Then disable WAN3. Click **Update**.



Enabled: on

Router

IP Address	Prefix Length	Gateway	DHCP
192.168.1.2	24	192.168.1.1	off

Public IP: 120.2.2.2

Overlay IP: 10.254.0.5

Transport Network: Internet

Eligible DTI: ● Inherited (ON) ○ ON ○ OFF

└ Enable NAT: on

Preference:

Access Bandwidth (up/down): 5000 kbps 5000 kbps

MTU: 1500

Speed: Auto

Internal Tunnels

Search or select an option...

Remote WAN Interface	Preference
DataCenter2-WAN2	90
DataCenter-WAN2	100

External Gateways

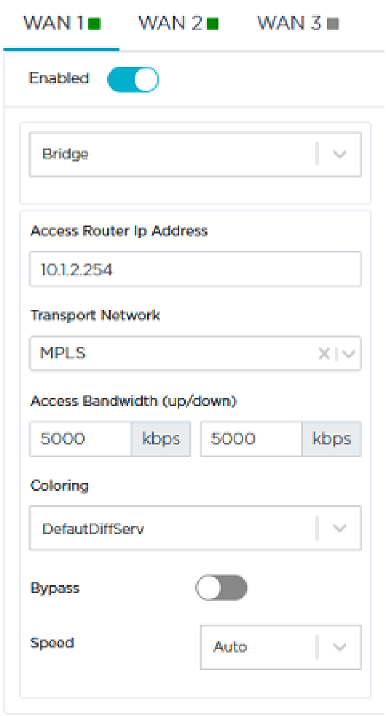
Search or select an option...

Gateway	Initiator ID	PSK	Inside Local IP	Inside Remote IP	Preference
AzureGateway				20.2.2.2	

Local Port Forwarding

Protocol	External Port	Local IP Address	Local Port
TCP	8080	10.1.2.12	80

2 Disable the Bypass option (enabled by default) on B02 WAN1 Bridge interface to avoid loops when the appliances reboot. Click **Update**.



Enabled ●

Bridge

Access Router Ip Address
10.1.2.254

Transport Network
MPLS

Access Bandwidth (up/down)
5000 kbps 5000 kbps

Coloring
DefautDiffServ

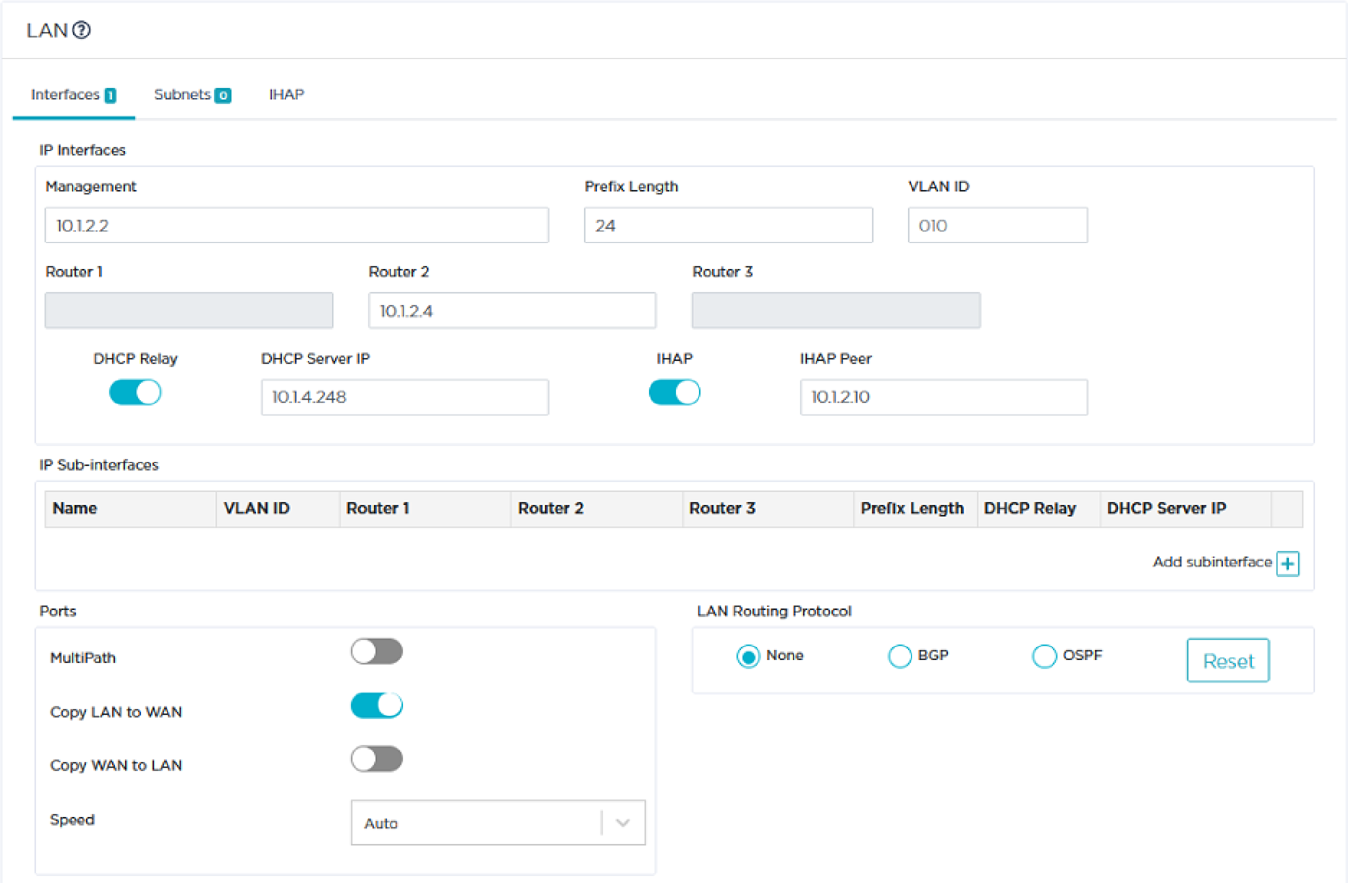
Bypass ○

Speed
Auto

3 Disable the MultiPath mode (LAN) of the B02 appliance - the Multi-WAN mode is used in this Use Case.

> **Note:** Both MultiPath and MultiWAN modes are supported for this type of HA deployment.

4 Activate the **IHAP** option and enter 10.1.2.10 as the IHAP Peer IP address (IP address of the B02B appliance).



LAN

Interfaces 1 | Subnets 0 | IHAP

IP Interfaces

Management: 10.1.2.2	Prefix Length: 24	VLAN ID: 010
Router 1:	Router 2: 10.1.2.4	Router 3:
DHCP Relay: On	DHCP Server IP: 10.1.4.248	IHAP: On
IHAP Peer: 10.1.2.10		

IP Sub-interfaces

Name	VLAN ID	Router 1	Router 2	Router 3	Prefix Length	DHCP Relay	DHCP Server IP

Ports

MultiPath	Off
Copy LAN to WAN	On
Copy WAN to LAN	Off
Speed	Auto

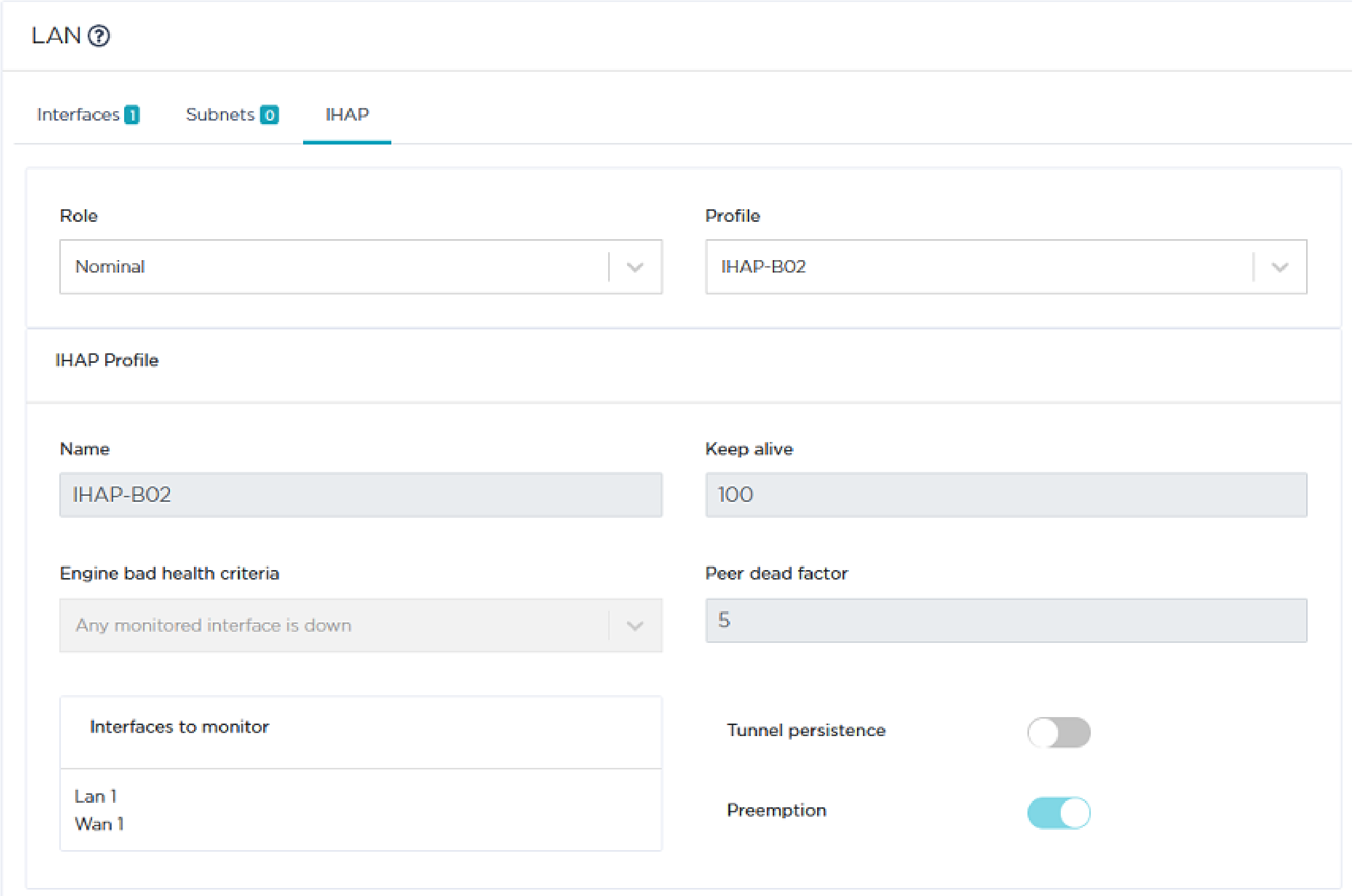
LAN Routing Protocol

● None ○ BGP ○ OSPF

5 Select the **IHAP** tab at the top of the LAN window.

6 Select the Nominal Role for the B02 appliance and the IHAP-B02 Profile you have created at the beginning of this configuration procedure.

The parameters associated with the selected IHAP Profile are displayed in read only mode.



LAN ⓘ

Role: Nominal

Profile: IHAP-B02

IHAP Profile

Name: IHAP-B02

Keep alive: 100

Engine bad health criteria: Any monitored interface is down

Peer dead factor: 5

Interfaces to monitor

Lan 1
Wan 1

Tunnel persistence: off

Preemption: on

7 **Update** your configuration.

Configure the new B02B backup appliance

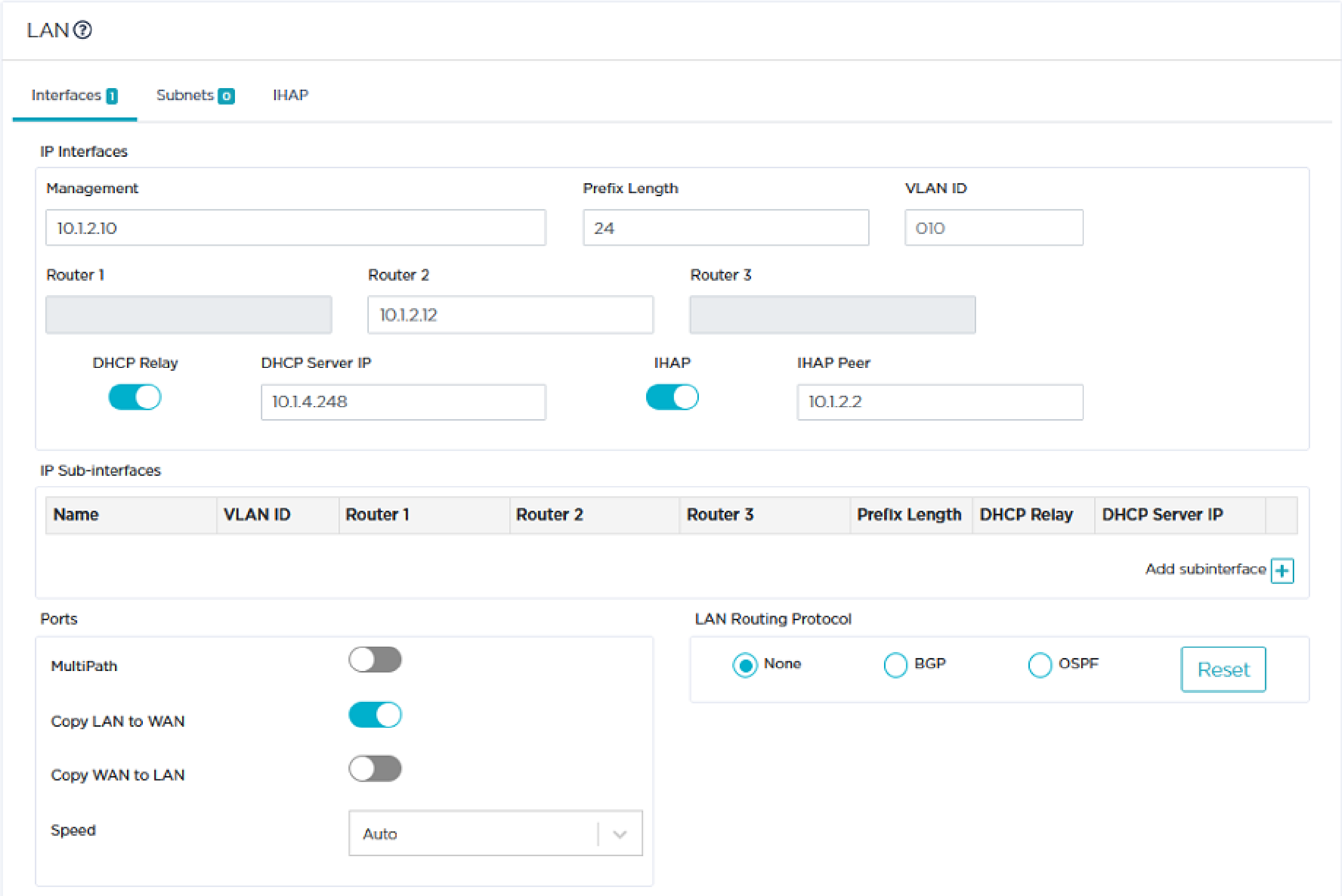
1 For identifying the B02B appliance refer to "Identifying an appliance in the SD-WAN Orchestrator only". Check that you use the same Local Autonomous System as for the Branch Office first appliance: 65001.

2 Configure its LAN as follows:

- Management IP address: 10.1.2.10, Prefix Length: 24
- Define the DHCP Server address: 10.1.4.248

3 Configure WAN1 and WAN2 that should correspond to WAN1 and WAN2 of the B02 appliance.

4 To configure IHAP on this B02B appliance, activate the **IHAP** option on the LAN window and enter 10.1.2.2 as the IHAP Peer IP address (IP address of the B02 appliance).



LAN

IP Interfaces

Management: 10.1.2.10

Prefix Length: 24

VLAN ID: 010

Router 1:

Router 2: 10.1.2.12

Router 3:

DHCP Relay: ☑

DHCP Server IP: 10.1.4.248

IHAP: ☑

IHAP Peer: 10.1.2.2

IP Sub-interfaces

Name	VLAN ID	Router 1	Router 2	Router 3	Prefix Length	DHCP Relay	DHCP Server IP

Ports

MultiPath ☐

Copy LAN to WAN ☑

Copy WAN to LAN ☐

Speed: Auto

LAN Routing Protocol

● None ○ BGP ○ OSPF

5 Select the **IHAP** tab at the top of the window.

6 Select the Backup Role for the B02B appliance and the same IHAP Profile as for B02, IHAP-B02. Then, **Update** your configuration.

Physically installing the two appliances

Refer to the appropriate section in the SD-WAN appliance Quick Installation Sheet.

Checking peering connections in the SD-WAN Orchestrator

1 On the Network -> Configuration window, click the ♥ icon for each HA appliance. In the displayed window, select **Routing -> HA** and check the HA Status of both appliances.

2 If the HA configuration is not operational, check if there are any 'HA peer unreachable' and/or 'HA configuration mismatch' alarms related to the configured HA Site in the Active Alarms and Event History dashboards.

Configuring traffic redirection to EdgeSentry

The purpose of this Use Case, which is complementary to "Use Case 1", is to provide a Branch Office with Cloud advanced security of its Internet traffic.

EdgeSentry which is ExtremeCloud SD-WAN's Cloud Security feature, is delivered from the Cloud through Check Point, a renowned Security Vendor. It offers the following services:

- Access Control, i.e. access rules define which Internet traffic is allowed or blocked
- Threat Prevention that includes a set of mechanisms like Intrusion Prevention System (IPS), anti-virus, anti-bot and sandboxing
- HTTPs Inspection with basic and full inspection levels
- Logs, events, dashboards and weekly reports on the Internet traffic

This section describes how to configure EdgeSentry in your network, from Branch Office 1 appliance over the Internet.

Two tunnels are created per WAN Router interface after you have defined the appropriate parameters in the SD-WAN Orchestrator.

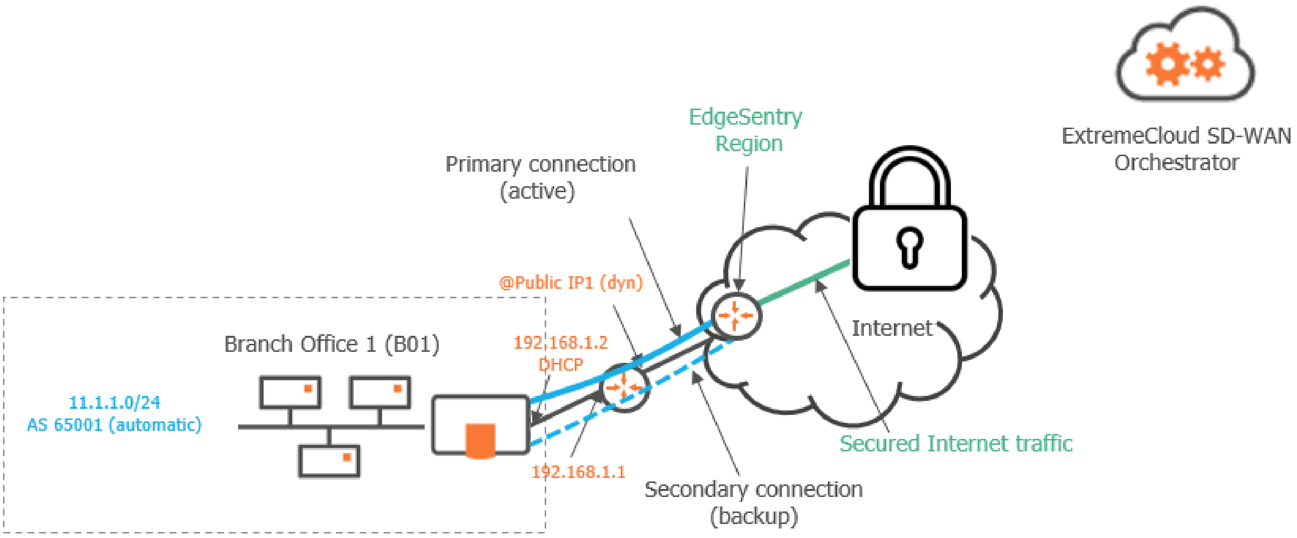
Prerequisites

You can use the EdgeSentry feature of the SD-WAN Orchestrator if:

- you have purchased two licenses: Ent-Branch-* or Ent-DC-* for the appliance, and Ent-EdgeSentry-10 for the domain. Refer to "Viewing Licenses"
- Extreme Networks has activated EdgeSentry for your Customer account

- "Step by Step Procedure"

Use Case 8



Graph legend

					Blue connection	Grey connection
SD-WAN appliance	router	subnet	host in a subnet	server	IPsec tunnel	physical connection between devices

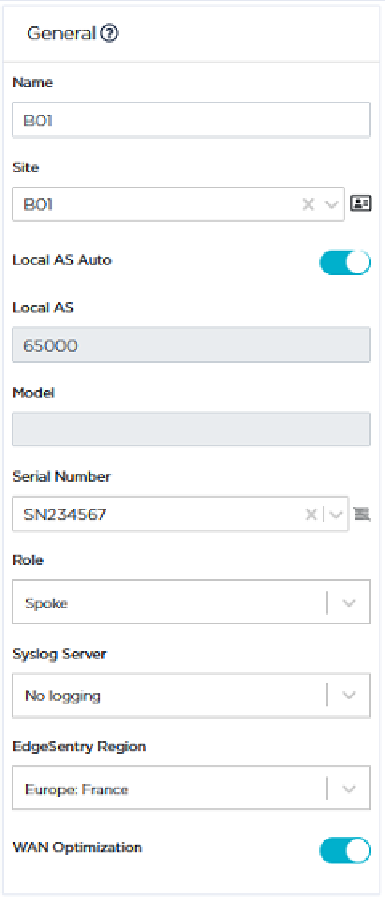
> **Note:** A router may be a CE Router (MPLS Router), an Internet Access Router or a Core Router.

Step by Step Procedure

Refer to "Use Case 8" diagram where EdgeSentry information is displayed in green.

Activating EdgeSentry

1 In the General panel of the Branch Office 1 appliance (B01) Configuration window, select the EdgeSentry Region. It is the closest region to the appliance. Note that region information is common to all the WAN interfaces of the appliances on the same Site, for which EdgeSentry has been activated.



General

Name: B01

Site: B01

Local AS Auto: ●

Local AS: 65000

Model:

Serial Number: SN234567

Role: Spoke

Syslog Server: No logging

EdgeSentry Region: Europe: France

WAN Optimization: ●

2 Connect B01 WAN1 router interface to EdgeSentry by checking the option. The EdgeSentry Region you selected in the previous step is automatically displayed.

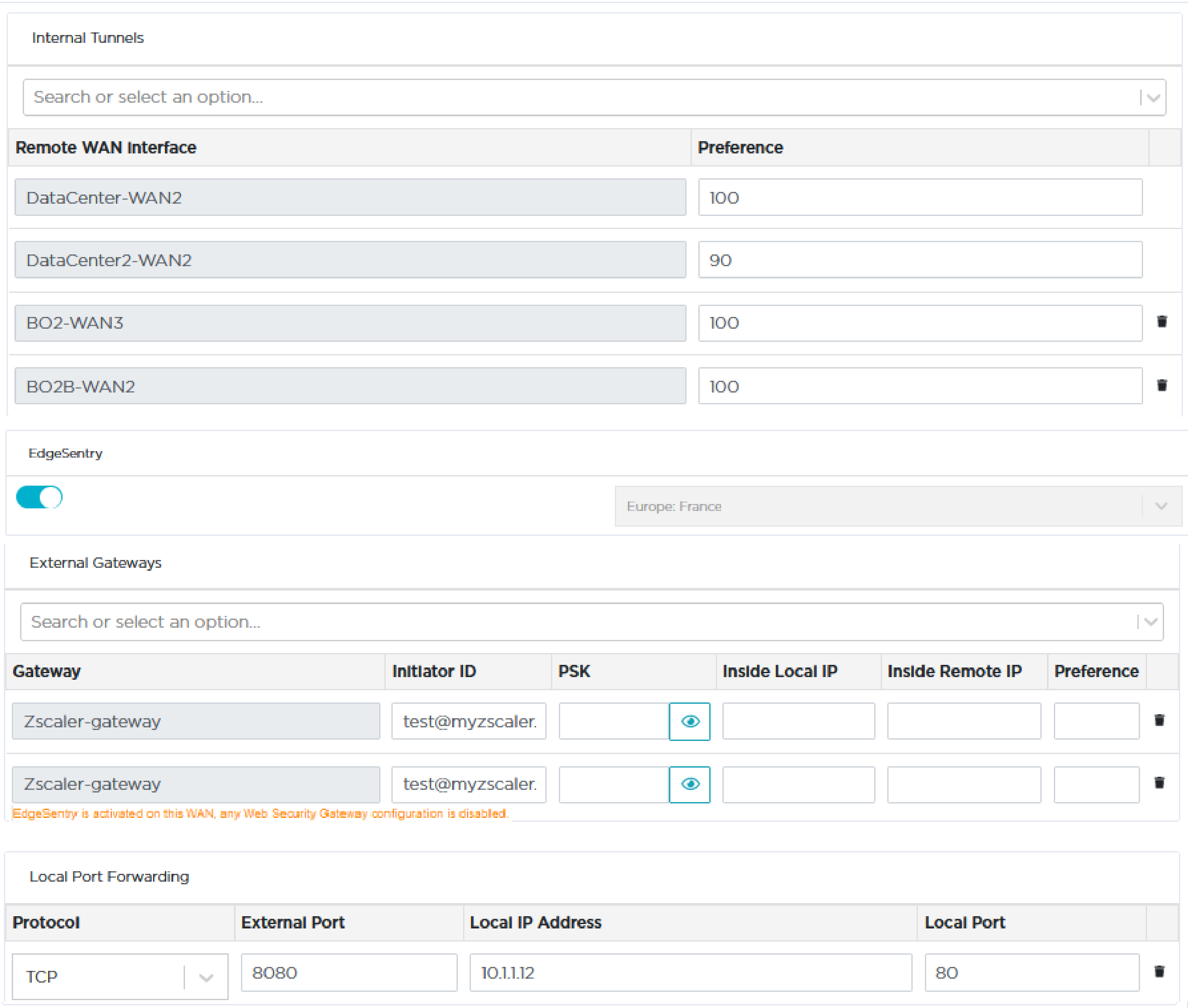
Eligible interfaces are WAN Router interfaces on hybrid or full router appliances.

3 Click **Update**.

> **Warning:** The same WAN interface cannot be connected to EdgeSentry and to a Web Security Gateway at the same time.

Since this interface is also connected to a Zscaler Web Security Gateway (see "Use Case 9"), this configuration is automatically disabled when you activate EdgeSentry.

If you disable EdgeSentry, the Web Security Gateway configuration is enabled again.



Internal Tunnels

Search or select an option...

Remote WAN Interface	Preference	
DataCenter-WAN2	100	
DataCenter2-WAN2	90	
BO2-WAN3	100	🗑
BO2B-WAN2	100	🗑

EdgeSentry

Europe: France

External Gateways

Search or select an option...

Gateway	Initiator ID	PSK	Inside Local IP	Inside Remote IP	Preference	
Zscaler-gateway	test@myzscaler.	👁				🗑
Zscaler-gateway	test@myzscaler.	👁				🗑

EdgeSentry is activated on this WAN, any Web Security Gateway configuration is disabled.

Local Port Forwarding

Protocol	External Port	Local IP Address	Local Port	
TCP	8080	10.1.1.12	80	🗑

4 From the SD-WAN Orchestrator top menu, connect to the Cloud Security Partner's portal by selecting **Network -> EdgeSentry Portal**.

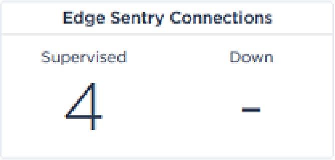
5 Configure Security Policies according to the procedure described in the Cloud Security Partner's documentation.

6 Define the traffic to forward to EdgeSentry through the wsg or wsg+ Internet Access Policies of the Zone-Based Firewall. Refer to "Internet Access Policies".

7 Click **Update** to validate the configuration.

Checking EdgeSentry Connections

1 Verify whether the EdgeSentry configuration is operational by checking that there are supervised connections in the EdgeSentry Connections panel of the Supervision -> Overview dashboard.



Edge Sentry Connections

Supervised	Down
4	-

For each connected WAN router interface, a primary connection and a secondary connection are created; refer to Use Case 8 diagram. If EdgeSentry connections are displayed in the 'Down' column, check the alarms raised for the configured EdgeSentry appliance in the Active Alarms and Event History dashboards.

2 On the Supervision -> Tunnel Status dashboard, check that the EdgeSentry tunnels are up.

3 On the Network -> Configuration window, click the ♥ icon for the appropriate appliance.

In the displayed window, select **Tunnels -> IPsec** to analyze the details of the created EdgeSentry tunnels.

Also see how to configure a Web Security Gateway.

Configuring traffic redirection to a Web Security Gateway

The purpose of this Use Case, which is complementary to "Use Case 1", is to enable the connection to a Zscaler Web Security Gateway delivered from the cloud. The Zscaler platform defends against malware, advanced threats, phishing, browser exploits, malicious URLs and botnets. As well as web security, the service offers web filtering, firewalls and anti-spam functions.

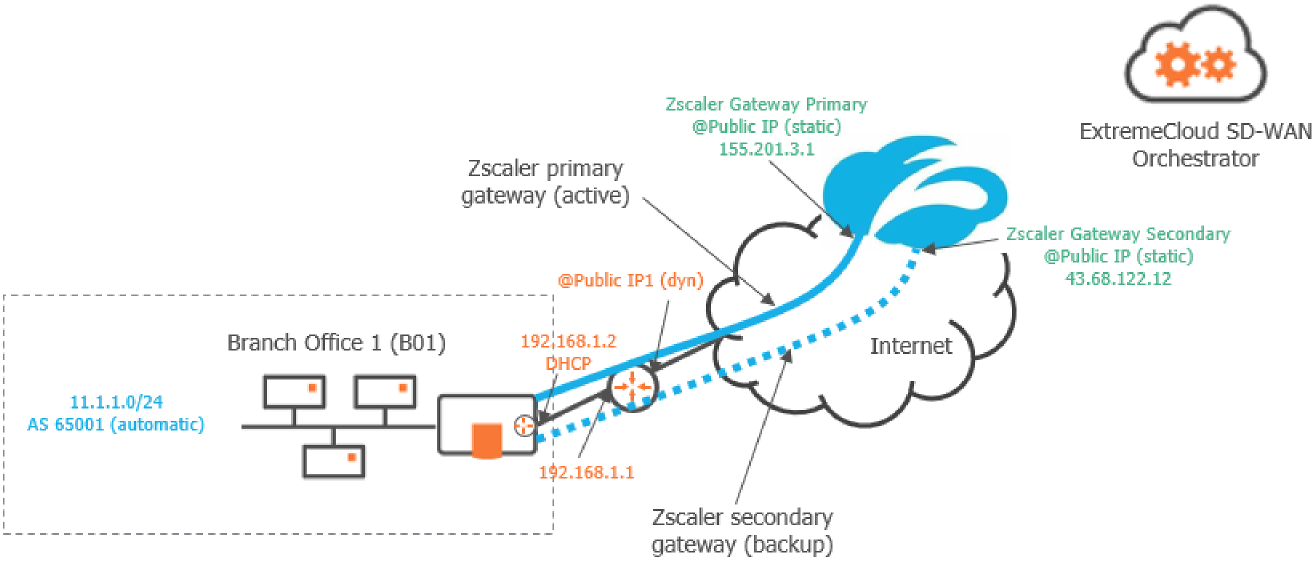
This section describes how to configure this gateway in your network, from Branch Office 1 appliance over the Internet.

One tunnel is created after you have defined the appropriate parameters in **both** the Orchestrator and in Zscaler.

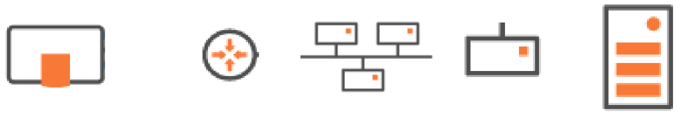
> **Note:** Only Zscaler is supported in this SD-WAN Orchestrator version. It is likely that other web security gateways can be defined.

- "Defining the Web Security Gateway"
- "Connecting the Branch Office appliance to the Gateway"

Use Case 9



Graph legend

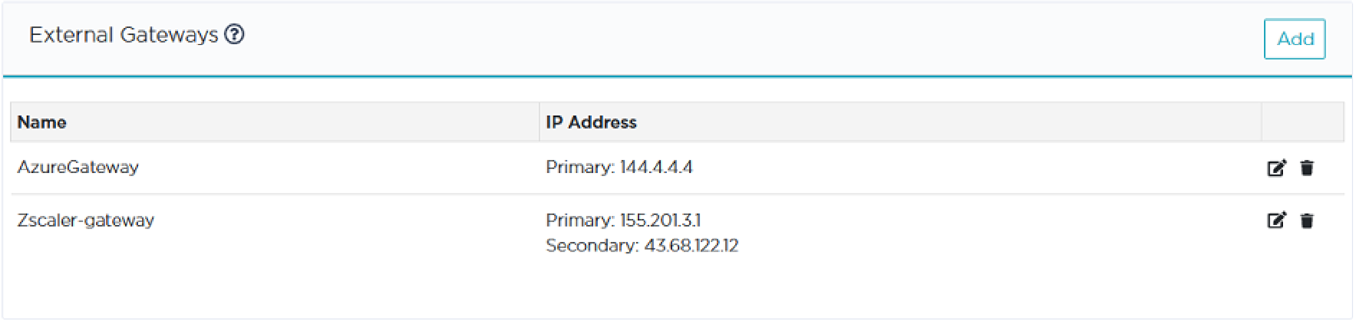


					Blue connection	Grey connection
SD-WAN appliance	router	subnet	host in a subnet	server	IPsec tunnel	physical connection between devices

> **Note:** A router may be a CE Router (MPLS Router), an Internet Access Router or a Core Router.

Creating a Web Security gateway

Select **Network -> External Gateways** from the Orchestrator main menu.



Name	IP Address	
AzureGateway	Primary: 144.4.4.4	📝 🗑
Zscaler-gateway	Primary: 155.201.3.1 Secondary: 43.68.122.12	📝 🗑

On the displayed window, click the **Add** button to display the form. The basic procedure for defining a web security gateway consists of the following steps:

- Identifying the gateway
- Defining the Public IP addresses of both the Zscaler Gateway and the Branch Office appliance it is connected to. The Public IP addresses of the Zscaler security gateway include a primary address and a secondary backup address used to set up two tunnels in active/backup configuration.
- Defining the IPSec tunnel parameters.

Refer to the following sections for detailed explanations.

Modifying or deleting a Web Security gateway

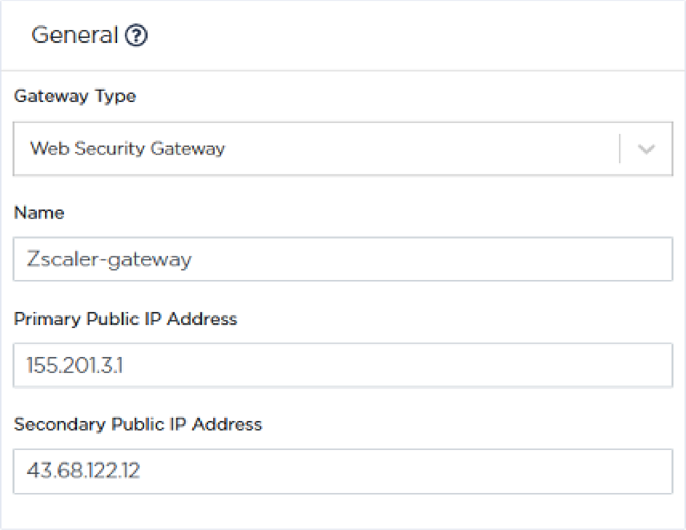
- Click 📝 to edit the configuration of a web security gateway. Modify any values and hit Update to save your settings.
- Click 🗑 if you want to delete a web security gateway. The system asks you to click the icon a second time to confirm your action.

Defining the Web Security Gateway

Refer to "Use Case 9" diagram where the Zscaler web security gateway information is displayed in green.

Also see how to define an External VTI Gateway ("Use Case 11").

Identifying the web security gateway



Gateway Type: Web Security Gateway

Name: Zscaler-gateway

Primary Public IP Address: 155.201.3.1

Secondary Public IP Address: 43.68.122.12

1 In the General panel of the Configuration window, select 'Web Security Gateway' as type of gateway.

2 Enter the Name (Zscaler-gateway) of the Web Security gateway.

3 Enter the gateway Primary Public IP Address (155.201.3.1).

4 Enter the gateway Secondary Public IP Address (43.68.122.12). Traffic will be routed through the secondary tunnel as soon as the primary tunnel goes down.

Routing

Since Zscaler does not support static nor dynamic routing (the IPsec tunnel is policy-based only), the Routing panel of the Configuration window is useless.

IPsec tunnel parameters

5 Use IKE policy (default values for Zscaler are automatically displayed) and IPsec policy values as you defined them in Zscaler. Also enter the MTU value.

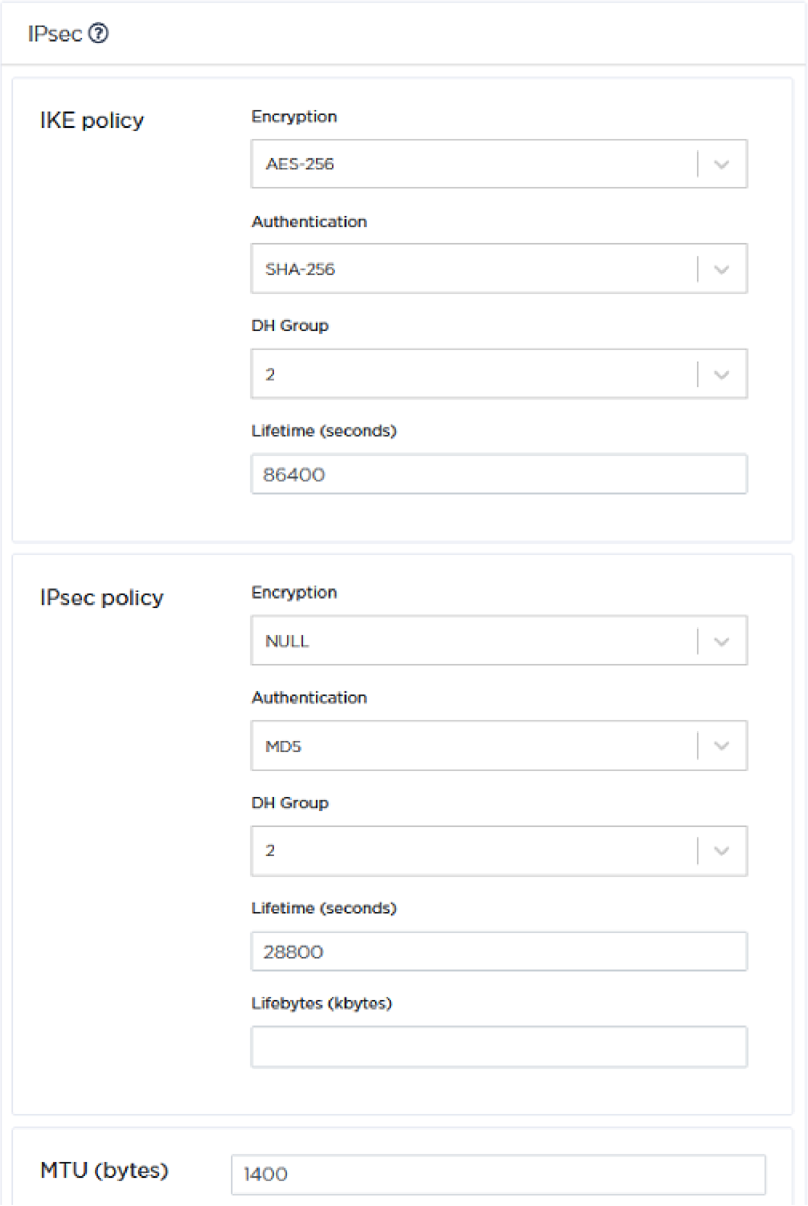
6 Use the IPsec Pre-Shared key field as follows:

- If on the Zscaler Portal, the Web Security gateway is configured with only one default Pre-Shared Key for all the tunnels connected to this gateway, enter this key in the SD-WAN Orchestrator. Specifying a Pre-Shared key is mandatory with a Zscaler Web Security gateway.

- You can override this default Pre-Shared Key with a new key when configuring the connection between the appliance and the gateway.

7 Click **Create**.

For a detailed description of all the fields, refer to "Advanced Configuration".



IPsec

IKE policy

Encryption: AES-256

Authentication: SHA-256

DH Group: 2

Lifetime (seconds): 86400

IPsec policy

Encryption: NULL

Authentication: MD5

DH Group: 2

Lifetime (seconds): 28800

Lifebytes (kbytes):

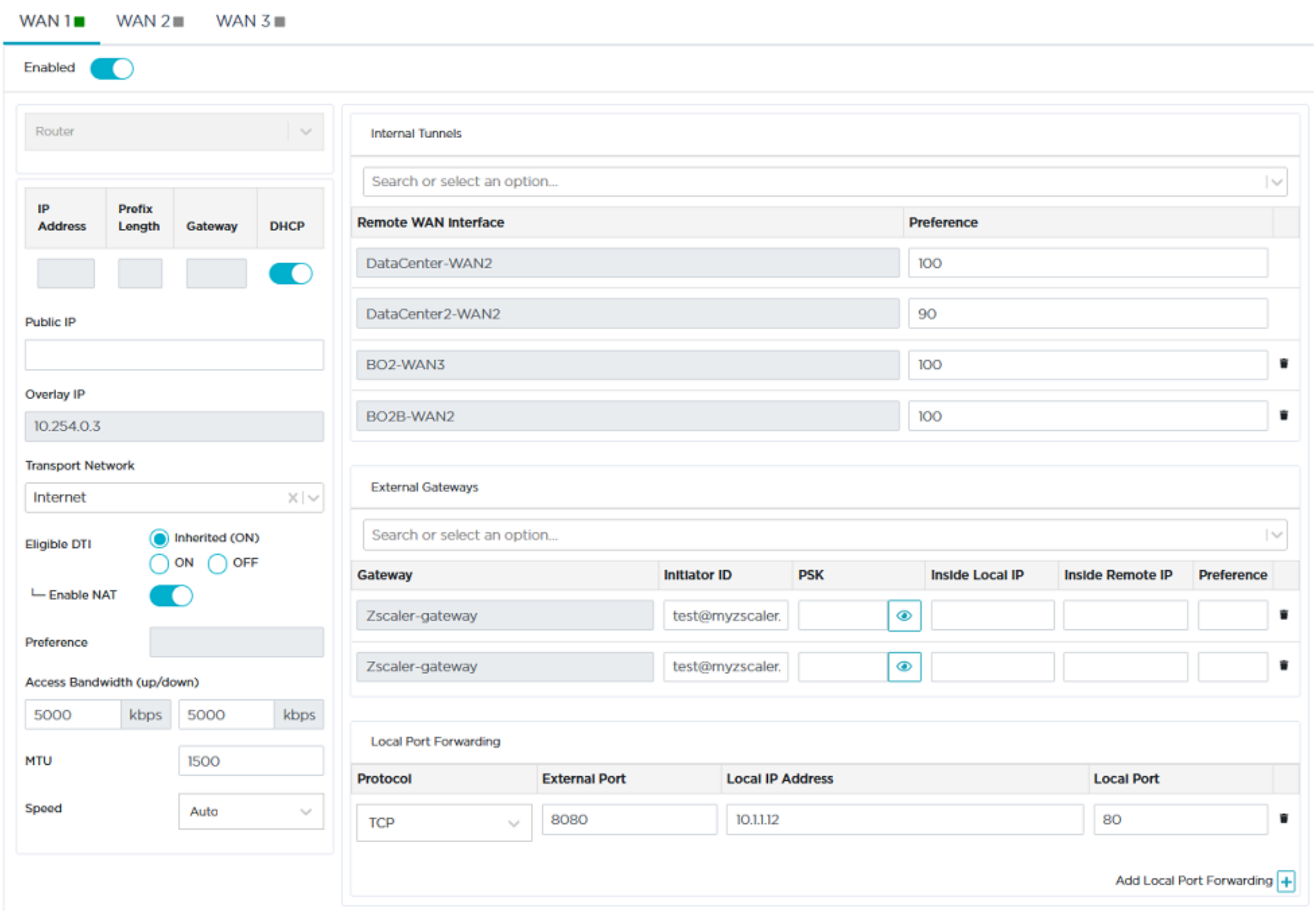
MTU (bytes): 1400

8 Then connect the gateway to the Branch Office appliance. Refer to the following section.

Connecting the Branch Office appliance to the Gateway

To connect Branch Office 1 appliance to the gateway (see "Use Case 1"), edit its WAN1 parameters by completing the External Gateways panel.

Refer to "Use Case 9" diagram where the appliance information is displayed in orange.



Enabled

Router

IP Address	Prefix Length	Gateway	DHCP
			ON

Public IP

Overlay IP: 10.254.0.3

Transport Network: Internet

Eligible DTI: ● Inherited (ON) ○ ON ○ OFF

Enable NAT

Preference

Access Bandwidth (up/down): 5000 kbps 5000 kbps

MTU: 1500

Speed: Auto

Internal Tunnels

Search or select an option...

Remote WAN Interface	Preference
DataCenter-WAN2	100
DataCenter2-WAN2	90
BO2-WAN3	100
BO2B-WAN2	100

External Gateways

Search or select an option...

Gateway	Initiator ID	PSK	Inside Local IP	Inside Remote IP	Preference
Zscaler-gateway	test@myzscaler.				
Zscaler-gateway	test@myzscaler.				

Local Port Forwarding

Protocol	External Port	Local IP Address	Local Port
TCP	8080	10.1.1.12	80

Add Local Port Forwarding

1. From the stack of External Gateways names, select 'Zscaler-gateway - primary'.
2. Since B01 Public IP address is dynamic and unknown to the Orchestrator, you must enter an Initiator ID which corresponds to the information you defined on the Zscaler Portal (when specifying an FQDN for the VPN credentials). For example, enter 'test@myzscaler.com'.

   Note that defining an Initiator ID would be irrelevant if B01 Public IP address was static; in that case, the SD-WAN Orchestrator would use that IP address.
3. Use the IPsec Pre-Shared key field as follows:

- If on the Web Security Gateway Platform (Zscaler), the gateway is configured with only one default Pre-Shared Key for all the tunnels connected to this gateway, leave this field blank in the SD-WAN Orchestrator (current Use Case).
- If in Zscaler, the gateway has a specific PSK value for each tunnel, you should enter a Pre-Shared Key for this tunnel of the B01 appliance.

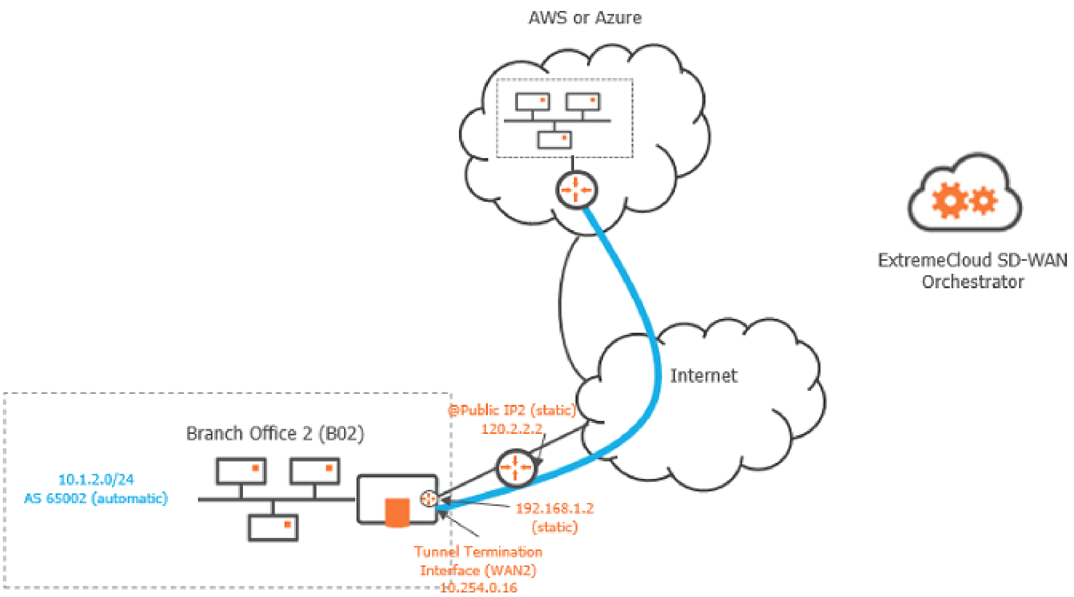
Use the 👁 icon different statuses to either display or hide the key.

4. The tunnel Inside Local IP address and Remote IP address fields are not used; leave them blank.
5. You may filter the redirected traffic by local subnet. By default, the subnets defined under the Subnets tab of the LAN panel are automatically applied for filtering. However, if any subnets are configured and listed in the Local Subnets fields of the External Gateways panel, only these subnets are taken into account for filtering (up to 8 subnets are authorized); they overwrite the LAN subnets of the appliance.
6. The Preference parameter is meaningless.
7. From the stack of External Gateways names, select 'Zscaler-gateway - secondary' and follow the same procedure as for the first Zscaler gateway. 'Zscaler-gateway - secondary' is used as backup tunnel when 'Zscaler-gateway - primary' fails.
8. **Update** your settings. The tunnel is created.

Configuring traffic redirection to a Cloud Gateway

The purpose of this Use Case, which is complementary to "Use Case 1", is to enable access to a Cloud Gateway from Branch Office 2 appliance.

Use Case 10

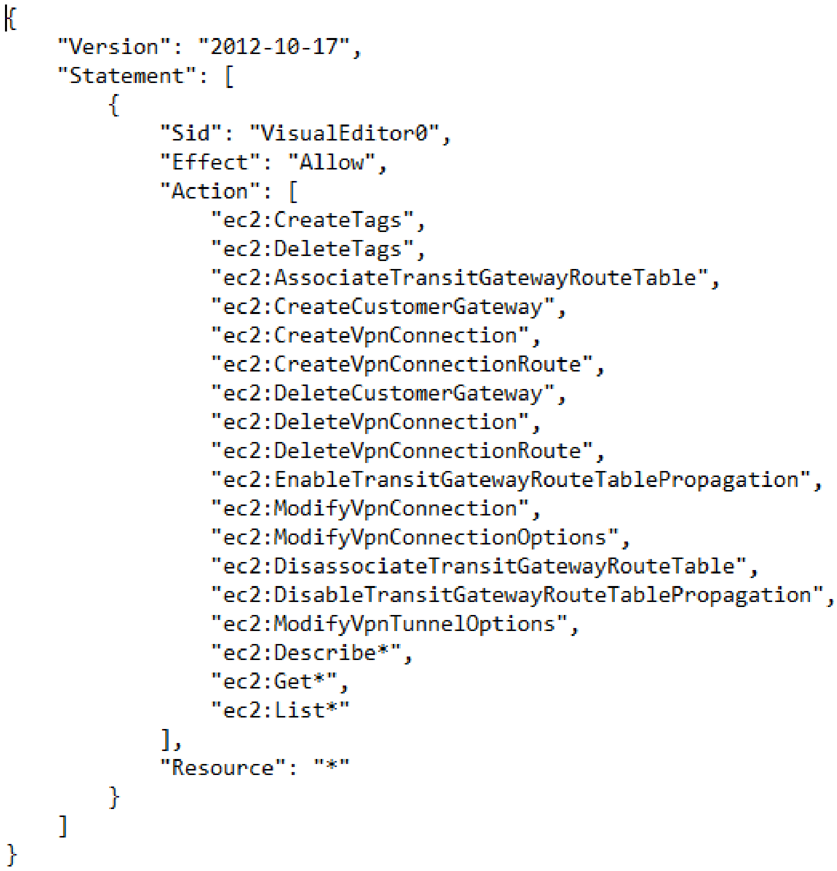


Prerequisites

The following prerequisites describes the necessary configuration actions in AWS and Azure for the Cloud gateways the SD-WAN Orchestrator will connect to.

AWS

- Your administrator should create an IAM user with programmatic access on the AWS account. Both Access Key ID and Secret Access Key values needed to create a Cloud Access object in the SD-WAN Orchestrator are generated when you create an IAM user in AWS.
- The required IAM policy describes the programmatic access set of permissions, i.e. the actions the SD-WAN Orchestrator can execute:



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:AssociateTransitGatewayRouteTable",
                "ec2:CreateCustomerGateway",
                "ec2:CreateVpnConnection",
                "ec2:CreateVpnConnectionRoute",
                "ec2:DeleteCustomerGateway",
                "ec2:DeleteVpnConnection",
                "ec2:DeleteVpnConnectionRoute",
                "ec2:EnableTransitGatewayRouteTablePropagation",
                "ec2:ModifyVpnConnection",
                "ec2:ModifyVpnConnectionOptions",
                "ec2:DisassociateTransitGatewayRouteTable",
                "ec2:DisableTransitGatewayRouteTablePropagation",
                "ec2:ModifyVpnTunnelOptions",
                "ec2:Describe*",
                "ec2:Get*",
                "ec2:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

- The two types of AWS managed gateways, i.e. Virtual Private Gateways and Transit Gateways are supported and must be configured with dynamic routing (BGP activated).
- The AS number is unique for each AWS gateway and should not conflict with the AS number range used for the SD-WAN overlay.
- Routing between VPCs and gateways is managed by you.

Azure

- Your administrator should define an Azure AD application and service principal dedicated to the SD-WAN Orchestrator through Azure Portal or Azure CLI. Refer to Azure documentation at https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal. Select Option 2 for authentication.
- The role to be associated with the application on the targeted subscription is 'Network Contributor'.
- A Storage Account is necessary for storing the configuration information of the VPN tunnels. Any type of storage account is authorized except 'FileStorage'. Access to the storage account is done through a 'full permission' access key.
- vnet gateways of type VPN and virtual hubs with an instantiated VPN gateway are supported.
- vnet gateways must be route-based with BGP enabled.
- The AS number is unique for each vnet gateway and should not conflict with the AS number range used for the SD-WAN overlay.

Procedure

1. Create and manage Cloud Access objects.
2. Optionally select the regions related to the chosen Cloud Access object and define tunnel parameters.
3. Connect the selected Branch Office appliance to the Cloud Gateway:
   - AWS
   - Microsoft Azure
4. Configure cloud connection parameters.

Depending on the gateway, two tunnels are created after you have defined the appropriate parameters in **both** the Orchestrator and in AWS or Azure.

Connecting a Branch Office appliance to an AWS Gateway

To connect Branch Office 2 appliance to the gateway (see "Use Case 1"), edit its WAN3 parameters by completing the Cloud Gateways panel.

1 From the stack of Cloud Gateways names, select one AWS gateway.

There are two types of AWS managed gateways:

- VGW: a Virtual Private Gateway is a resource associated with a VPC (Virtual Private Cloud in AWS) that provides connectivity to this VPC (through site-to-site VPN or Direct Connect).
- TGW: a Transit Gateway is a resource associated with VPCs in the same region and acts as a hub providing:

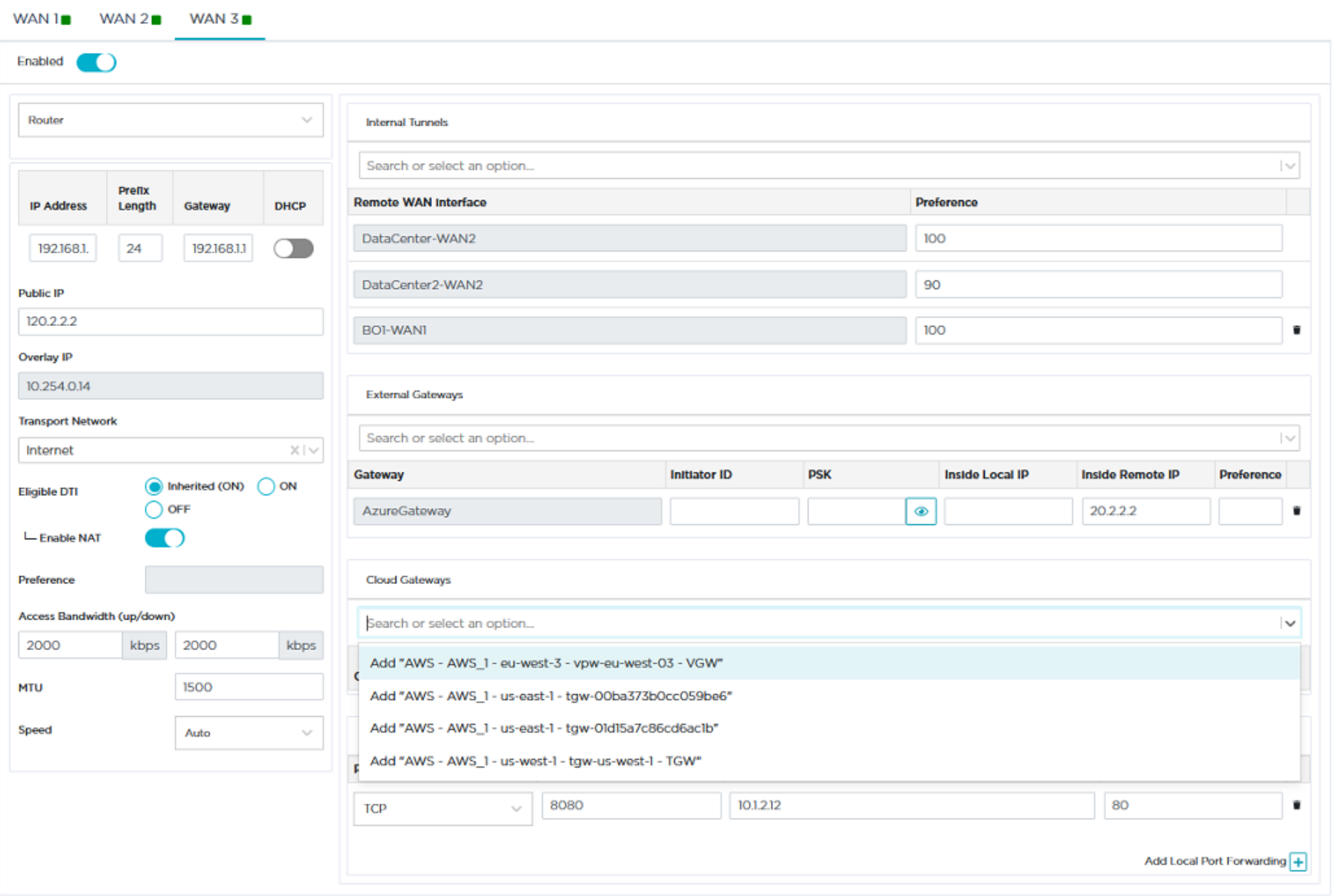
  - connectivity between remote sites and these VPCs (through site-to-site VPN or Direct Connect),

  - routing between these VPCs,

  - routing with VPCs that are associated with other Transit Gateways (possibly in other regions)

An AWS Cloud gateway name includes:

- the Cloud access type, AWS in this case
- the Cloud access name
- the name of the AWS region where it is deployed
- the gateway name in AWS (if it exists) and its type, VGW or TGW
- or the gateway ID in AWS (vgw-xxxxx or tgw-xxxxx)



WAN 1 🟩 WAN 2 🟩 WAN 3 🟩

Enabled ●

Router

IP Address	Prefix Length	Gateway	DHCP
192.168.1.	24	192.168.1.1	○

Public IP: 120.2.2.2

Overlay IP: 10.254.0.14

Transport Network: Internet

Eligible DTI: ● Inherited (ON) ○ ON ○ OFF

└ Enable NAT ●

Preference

Access Bandwidth (up/down): 2000 kbps 2000 kbps

MTU: 1500

Speed: Auto

Internal Tunnels

Search or select an option...

Remote WAN Interface	Preference
DataCenter-WAN2	100
DataCenter2-WAN2	90
BO1-WAN1	100

External Gateways

Search or select an option...

Gateway	Initiator ID	PSK	Inside Local IP	Inside Remote IP	Preference
AzureGateway				20.2.2.2	

Cloud Gateways

Search or select an option...

Add "AWS - AWS_1 - eu-west-3 - vpw-eu-west-03 - VGW"

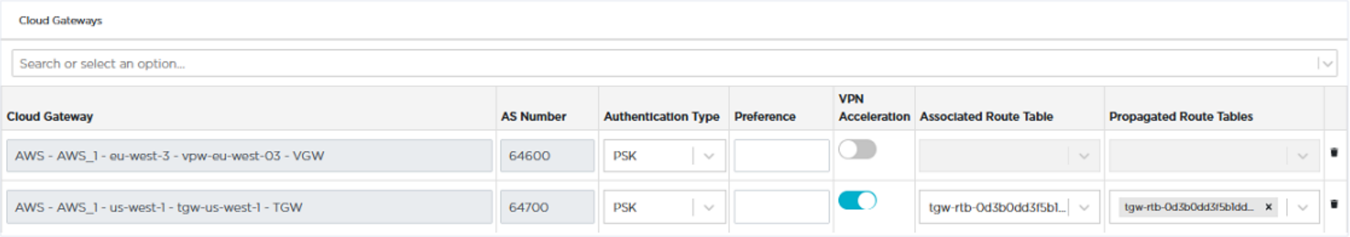
Add "AWS - AWS_1 - us-east-1 - tgw-00ba373b0cc059be6"

Add "AWS - AWS_1 - us-east-1 - tgw-01d15a7c86cd6ac1b"

Add "AWS - AWS_1 - us-west-1 - tgw-us-west-1 - TGW"

TCP	8080	10.1.2.12	80

Add Local Port Forwarding +



Cloud Gateways

Search or select an option...

Cloud Gateway	AS Number	Authentication Type	Preference	VPN Acceleration	Associated Route Table	Propagated Route Tables
AWS - AWS_1 - eu-west-3 - vpw-eu-west-03 - VGW	64600	PSK		○		
AWS - AWS_1 - us-west-1 - tgw-us-west-1 - TGW	64700	PSK		●	tgw-rtb-0d3b0dd3f5b1...	tgw-rtb-0d3b0dd3f5b1dd... ×

The SD-WAN Orchestrator retrieves the AS number of the Cloud gateway and displays it beside the gateway name. The AS number of the Cloud gateway:

- must not be included in the AS number range (see Advanced Configuration > Overlay routing)
- or must be defined as an exclusion
- and should be different from any other appliance ASN in the domain

2 Since PSK is the only authentication type currently supported, the SD-WAN Orchestrator automatically generates a pre-shared key. This authentication type requires a WAN interface public IP address to be specified.

3 When there are several Cloud gateways, you can enter Preference values to define the priority of tunnels to route the traffic. The highest Preference value implies priority. The default value is 100.

For Transit Gateways (TGW) only

When you select a TGW gateway, the SD-WAN Orchestrator retrieves the list of transit gateway route tables. For every route table, its name and ID are specified.

4. You can enable VPN Acceleration and define the Associated Route Table and Propagated Route Tables. Transit Gateway route tables are objects that enable network segmentation, i.e. they define whether attachments can communicate with one another.
    - Associated Route Table: select the route table by default for association or use the None option.
    - Propagated Route Tables: select one or more route table(s) for propagation.

For all the Gateways

5. **Update** your settings. Two connections are defined and the two matching tunnels are set up on the appliance.

Note: You can edit or delete a Cloud connection at any time.

Connecting a Branch Office appliance to an Azure Gateway

To connect Branch Office 2 appliance to the gateway (see "Use Case 1"), edit its WAN3 parameters by completing the External Gateways panel.

1 From the stack of Cloud Gateways names, select one Azure gateway.

   There are two types of Azure managed gateways:

   - vnet: a vnet gateway is a resource associated with a Vnet (Virtual Network) that provides connectivity to this Vnet (through site-to-site VPN or ExpressRoute)
   - vWAN VPN: a Virtual WAN VPN gateway is a resource associated with a Virtual Hub in a Virtual WAN; Vnets in the same region are connected to the same Virtual Hub which provides:

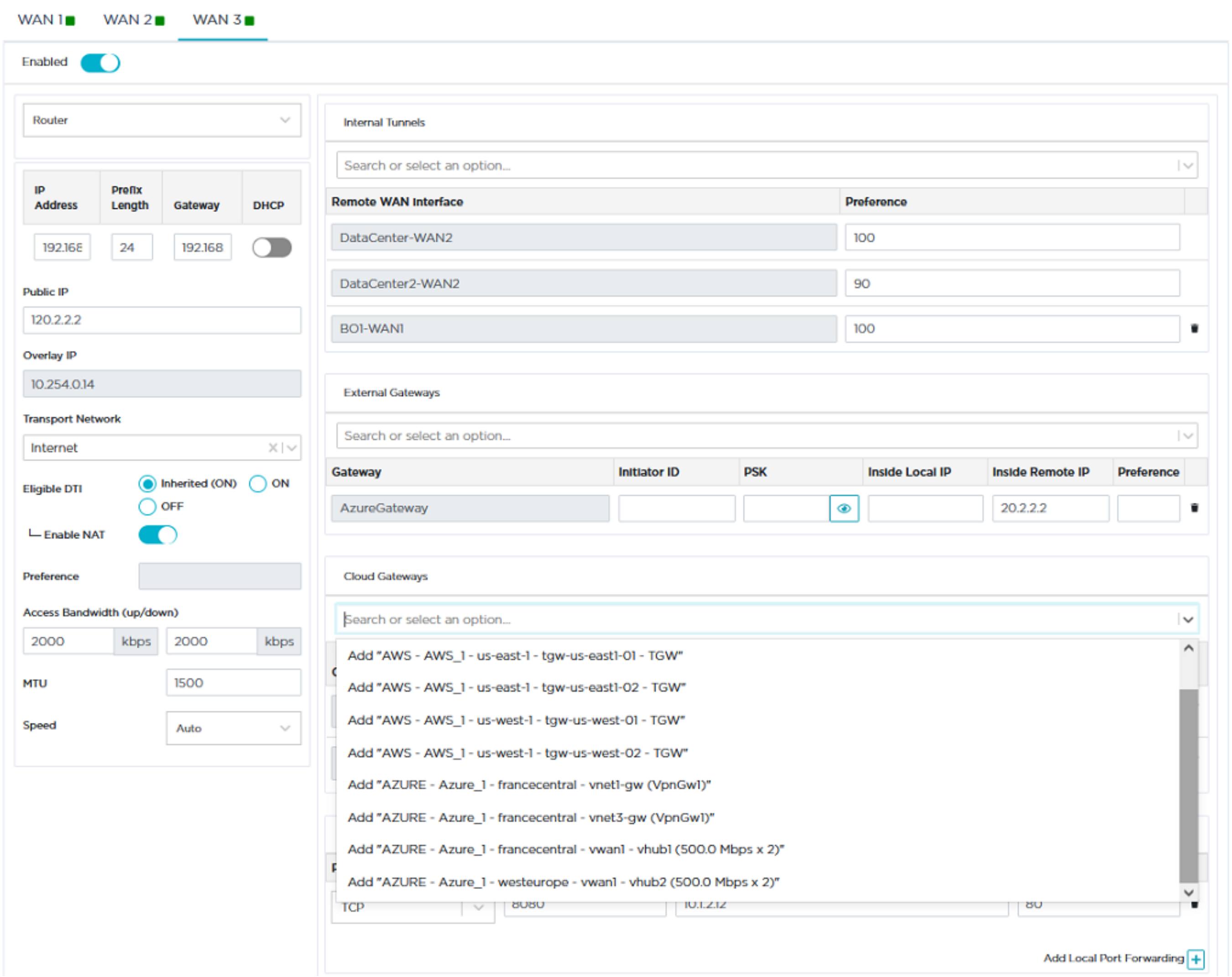
     - connectivity between remote sites and these Vnets (through site-to-site VPN or ExpressRoute),

     - routing between these Vnets,

     - routing with Vnets that are connected to other Virtual Hubs (possibly in other regions) of the same Virtual WAN

   An Azure Cloud gateway name includes:

   - the Cloud access type, AZURE in this case
   - the Cloud access name
   - the name of the Azure location where it is deployed
   - the vnet gateway name or the virtual WAN name + virtual Hub name
   - its SKU for a vnet gateway or the bandwidth of the virtual Hub VPN gateway



WAN 1 🟩 WAN 2 🟩 WAN 3 🟩

Enabled ●

Router

IP Address	Prefix Length	Gateway	DHCP
192.168	24	192.168	○

Public IP: 120.2.2.2

Overlay IP: 10.254.0.14

Transport Network: Internet

Eligible DTI: ● Inherited (ON) ○ ON ○ OFF

└ Enable NAT ●

Preference

Access Bandwidth (up/down): 2000 kbps 2000 kbps

MTU: 1500

Speed: Auto

Internal Tunnels

Search or select an option...

Remote WAN Interface	Preference
DataCenter-WAN2	100
DataCenter2-WAN2	90
BO1-WAN1	100

External Gateways

Search or select an option...

Gateway	Initiator ID	PSK	Inside Local IP	Inside Remote IP	Preference
AzureGateway				20.2.2.2	

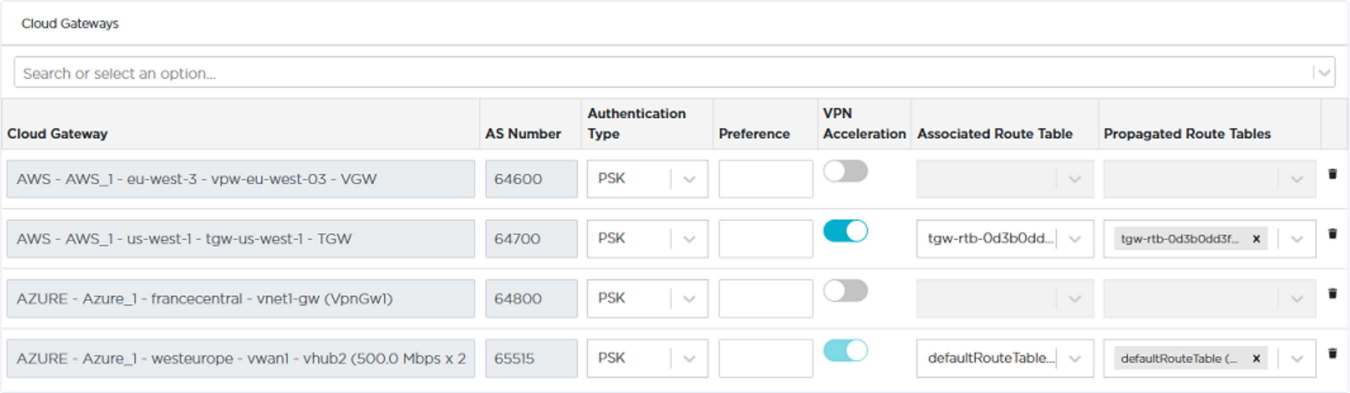
Cloud Gateways

Search or select an option...

- Add "AWS - AWS_1 - us-east-1 - tgw-us-east1-01 - TGW"
- Add "AWS - AWS_1 - us-east-1 - tgw-us-east1-02 - TGW"
- Add "AWS - AWS_1 - us-west-1 - tgw-us-west-01 - TGW"
- Add "AWS - AWS_1 - us-west-1 - tgw-us-west-02 - TGW"
- Add "AZURE - Azure_1 - francecentral - vnet1-gw (VpnGw1)"
- Add "AZURE - Azure_1 - francecentral - vnet3-gw (VpnGw1)"
- Add "AZURE - Azure_1 - francecentral - vwan1 - vhub1 (500.0 Mbps x 2)"
- Add "AZURE - Azure_1 - westeurope - vwan1 - vhub2 (500.0 Mbps x 2)"

TCP 8080 10.1.2.12 80

Add Local Port Forwarding +



Cloud Gateways

Search or select an option...

Cloud Gateway	AS Number	Authentication Type	Preference	VPN Acceleration	Associated Route Table	Propagated Route Tables
AWS - AWS_1 - eu-west-3 - vpw-eu-west-03 - VGW	64600	PSK		○		
AWS - AWS_1 - us-west-1 - tgw-us-west-1 - TGW	64700	PSK		●	tgw-rtb-0d3b0dd...	tgw-rtb-0d3b0dd3f...
AZURE - Azure_1 - francecentral - vnet1-gw (VpnGw1)	64800	PSK		○		
AZURE - Azure_1 - westeurope - vwan1 - vhub2 (500.0 Mbps x 2	65515	PSK		●	defaultRouteTable...	defaultRouteTable (...

The SD-WAN Orchestrator retrieves the AS number of the Cloud gateway and displays it beside the gateway name. The AS number of the Cloud gateway:

- must not be included in the AS number range (see Advanced Configuration > Overlay routing)
- or must be defined as an exclusion

- and should be different from any other appliance ASN in the domain

2 Since PSK is the only authentication type currently supported, the SD-WAN Orchestrator automatically generates a pre-shared key. This authentication type requires a WAN interface public IP address to be specified.

3 When there are several Cloud gateways, you can enter Preference values to define the priority of tunnels to route the traffic. The highest Preference value implies priority. The default value is 100.

For Virtual Hub VPN Gateways (vWAN - vHub) only

The SD-WAN Orchestrator retrieves and displays the VPN acceleration setting (not editable) that is configured on the Virtual Hub VPN Gateway. VPN acceleration 'enabled' corresponds to routing via "Microsoft global network" whereas VPN acceleration 'disabled' corresponds to routing over public Internet (refer to routing preference).

4 You can define the Associated Route Table and Propagated Route Tables. Virtual Hub route tables are objects that enable network segmentation, i.e. they define whether attachments can communicate with one another.

- Associated Route Table: select the route table for association, either the Default one or any other route table.
- Propagated Route Tables: select one or more route table(s) for propagation, or the None option.

For all the Gateways

5 **Update** your settings. Either one or two connections are defined - there are two connections with a virtual hub - and the matching tunnels are set up on the appliance.

Note: You can edit or delete a Cloud connection at any time.

Configuring traffic redirection to an External Gateway

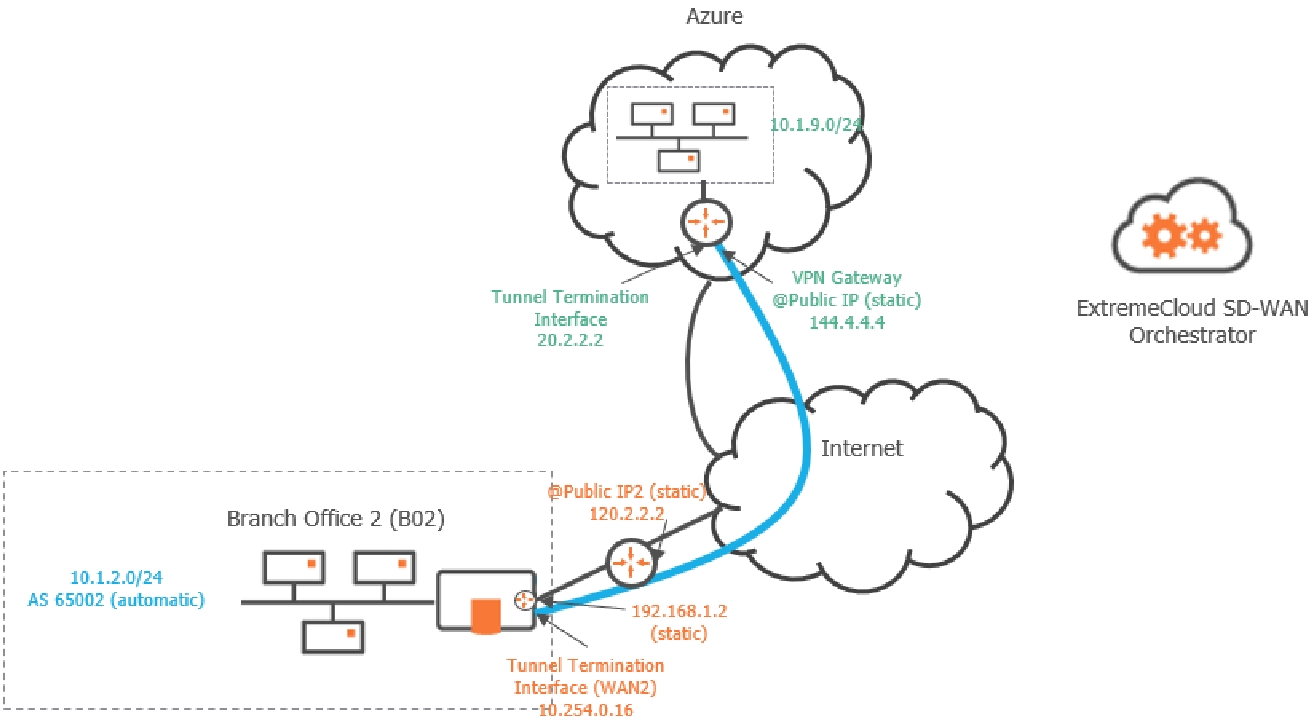
The purpose of this Use Case, which is complementary to "Use Case 1", is to enable access to a site where there is no appliance. This section describes how to configure an external gateway from Branch Office 2 appliance over the Internet.

One tunnel is created after you have defined the appropriate parameters in **both** the Orchestrator and in Microsoft Azure.

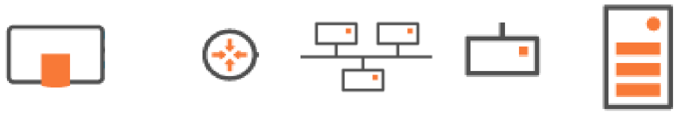
> **Note:** Only Microsoft Azure and Cisco devices are supported in this SD-WAN Orchestrator version.

- "Defining the External Gateway and Routing parameters"
- "Connecting the Branch Office appliance to the Gateway"

Use Case 11


Azure
10.1.9.0/24
Tunnel Termination Interface 20.2.2.2
VPN Gateway @Public IP (static) 144.4.4.4
ExtremeCloud SD-WAN Orchestrator
Internet
Branch Office 2 (B02)
10.1.2.0/24
AS 65002 (automatic)
@Public IP2 (static) 120.2.2.2
192.168.1.2 (static)
Tunnel Termination Interface (WAN2) 10.254.0.16

Graph legend

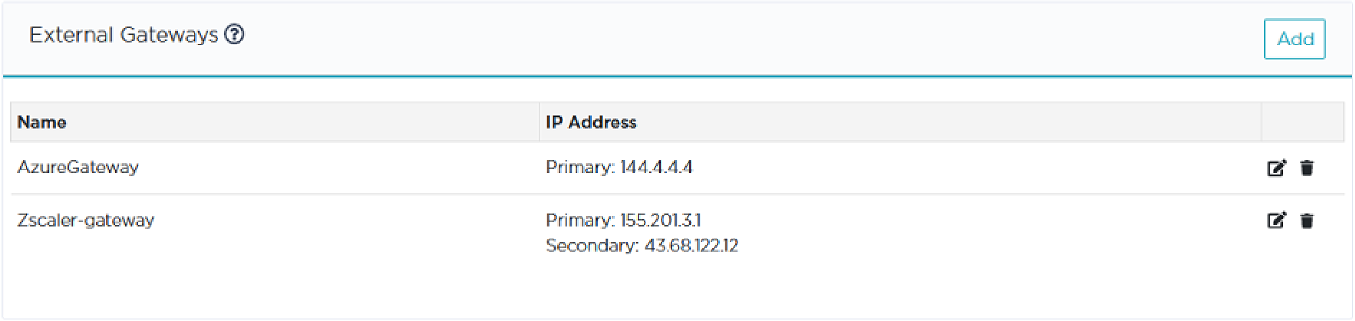


					Blue connection	Grey connection
SD-WAN appliance	router	subnet	host in a subnet	server	IPsec tunnel	physical connection between devices

> **Note:** A router may be a CE Router (MPLS Router), an Internet Access Router or a Core Router.

Creating an external gateway

Select **Network -> External Gateways** from the Orchestrator main menu.



External Gateways ⓘ

Add

Name	IP Address	
AzureGateway	Primary: 144.4.4.4	✎ 🗑
Zscaler-gateway	Primary: 155.201.3.1 Secondary: 43.68.122.12	✎ 🗑

On the displayed window, click the **Add** button to display the form. The basic procedure for defining an external gateway consists of the following steps:

- Identifying the external gateway
- Defining the Public IP addresses of both the VPN Gateway and the Branch Office appliance it is connected to. The IP addresses of the tunnel termination interfaces are also required.
- Defining how the traffic is routed through the tunnel by using subnet information (static configuration) or BGP (dynamic configuration).
- Defining the IPSec tunnel parameters.

Refer to the following sections for detailed explanations.

Modifying or deleting an external gateway

- Click ✎ to edit the configuration of an external gateway. Modify any values and hit Update to save your settings.

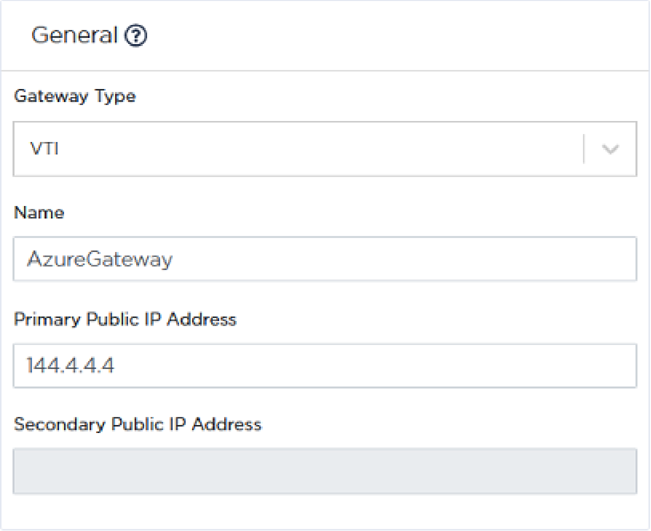
- Click 🗑 if you want to delete an external gateway. The system asks you to click the icon a second time to confirm your action.

Defining the External Gateway and Routing parameters

Refer to "Use Case 11" diagram where the external gateway information is displayed in green.

Also see how to define a Web Security Gateway ("Use Case 9").

Identifying the external gateway



General ?

Gateway Type

VTI

Name

AzureGateway

Primary Public IP Address

144.4.4.4

Secondary Public IP Address

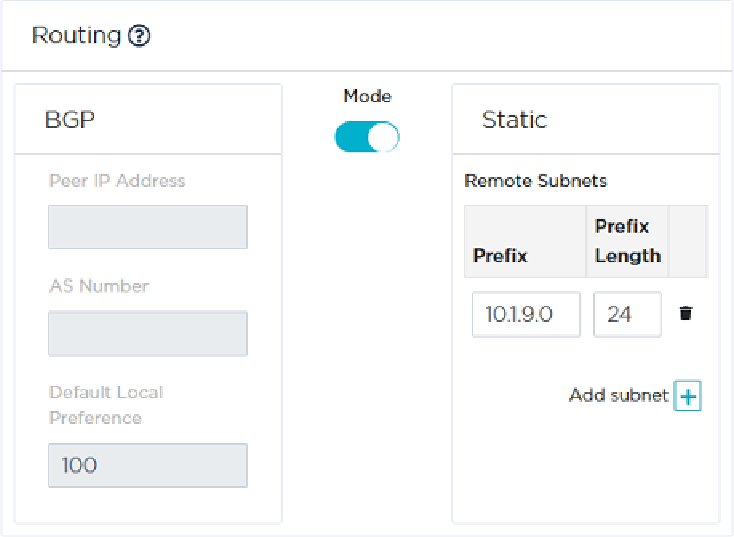
1. In the General panel of the Configuration window, select 'VTI' as type of gateway (Virtual Tunnel Interface VPN).
2. Enter the Name (AzureGateway) of the VTI gateway.
3. Enter the VTI gateway Primary Public IP Address (144.4.4.4).

Also refer to "Identifying the web security gateway".

Routing

> **Warning:** There is one prerequisite which is the necessary configuration of the VTI gateway parameters in Microsoft Azure.

Also refer to the "Routing" parameters of a Web Security Gateway.



Routing

BGP

Peer IP Address

AS Number

Default Local Preference: 100

Mode

Static

Remote Subnets

Prefix	Prefix Length
10.1.9.0	24

You can define how the traffic is routed through the tunnel by using subnet information (static configuration) or BGP (dynamic configuration). The current example uses static configuration.

4 Set the Mode button to Static.

5 Define the remote Azure subnet IP address by entering its prefix (10.1.9.0) and prefix length (24). Note that you also defined this IP address in Microsoft Azure.

If you use BGP, enter the IP address of the BGP local peer and the Autonomous System value as they are specified on the Microsoft Azure Portal. With a Cisco router, you can find the required information in the router configuration file.

IPsec tunnel parameters

6 Use IKE policy and IPsec policy values as you defined them in Microsoft Azure or for your Cisco router. Also enter the MTU value.

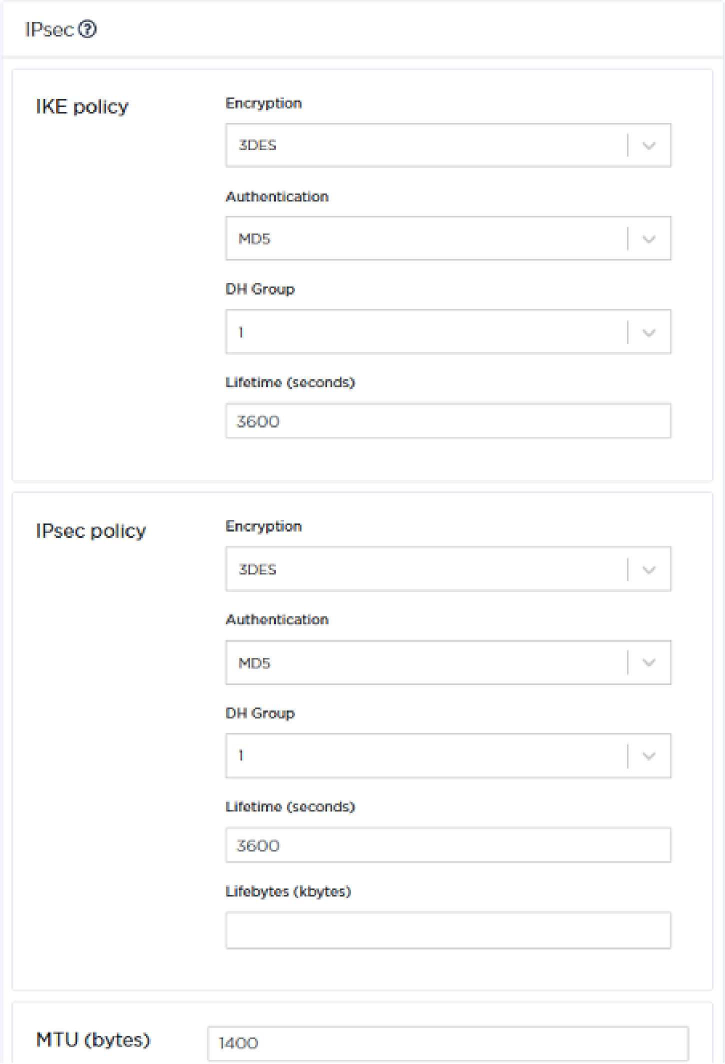
7 Use the IPsec Pre-Shared key field as follows:

- If in Microsoft Azure, the VPN gateway is configured with only one default Pre-Shared Key for all the tunnels connected to this gateway, enter this key in the SD-WAN Orchestrator. Specifying a Pre-Shared key is mandatory with an external gateway.
- You can override this default Pre-Shared Key with a new key when configuring the connection between the appliance and the external gateway.

8 Click **Create**.

For a detailed description of all the fields, refer to "Advanced Configuration".

Also see the "IPsec tunnel parameters" of a Web Security Gateway.



IPsec

IKE policy

Encryption: 3DES

Authentication: MD5

DH Group: 1

Lifetime (seconds): 3600

IPsec policy

Encryption: 3DES

Authentication: MD5

DH Group: 1

Lifetime (seconds): 3600

Lifebytes (kbytes):

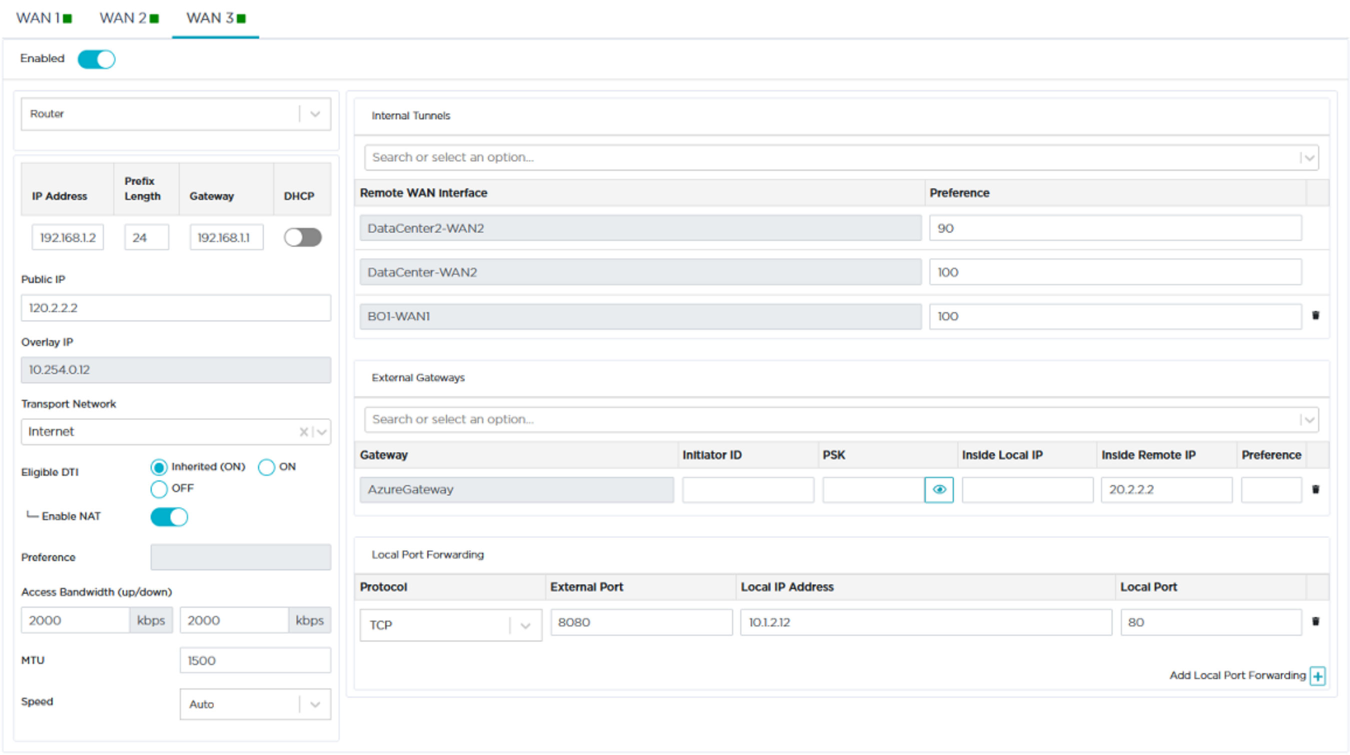
MTU (bytes): 1400

9 Then connect the gateway to the Branch Office appliance. Refer to the following section.

Connecting the Branch Office appliance to the Gateway

To connect Branch Office 2 appliance to the gateway (see "Use Case 1"), edit its WAN3 parameters by completing the External Gateways panel.

Refer to "Use Case 11" diagram where the appliance information is displayed in orange.



WAN 1 🟩 WAN 2 🟩 WAN 3 🟩

Enabled: ON

Router

IP Address	Prefix Length	Gateway	DHCP
192.168.1.2	24	192.168.1.1	OFF

Public IP: 120.2.2.2

Overlay IP: 10.254.0.12

Transport Network: Internet

Eligible DTI: ● Inherited (ON) ○ ON ○ OFF

Enable NAT: ON

Preference:

Access Bandwidth (up/down): 2000 kbps 2000 kbps

MTU: 1500

Speed: Auto

Internal Tunnels

Search or select an option...

Remote WAN Interface	Preference
DataCenter2-WAN2	90
DataCenter-WAN2	100
BO1-WAN1	100

External Gateways

Search or select an option...

Gateway	Initiator ID	PSK	Inside Local IP	Inside Remote IP	Preference
AzureGateway				20.2.2.2	

Local Port Forwarding

Protocol	External Port	Local IP Address	Local Port
TCP	8080	10.1.2.12	80

Add Local Port Forwarding +

1. From the stack of External Gateways names, select 'AzureGateway'.
2. Defining an Initiator ID is irrelevant in the current Use Case, since Microsoft Azure uses the 120.2.2.2 public IP address. Only specify an Initiator ID when authentication with Microsoft Azure or Cisco is executed through a different address.
3. Use the IPsec Pre-Shared key field as follows:
   - If in Microsoft Azure, the VPN gateway is configured with only one default Pre-Shared Key for all the tunnels connected to this gateway, leave this field blank in the SD-WAN Orchestrator (current Use Case).
   - If in Microsoft Azure, the VPN gateway has a specific PSK value for each tunnel, you should enter a Pre-Shared Key for this tunnel of the B02 appliance.

   Use the 👁 icon different statuses to either display or hide the key.

4. You do not need to define the Inside Local IP address of this tunnel termination interface since the system uses the Overlay IP address it automatically generated when previous tunnels were created (refer to "Configuring the WAN(s)").
5. As AzureGateway is configured in static mode, specify the Inside Remote IP address which corresponds to the tunnel termination interface (20.2.2.2) of the VPN gateway configured in Microsoft Azure. When an external gateway is configured in BGP mode, the Inside Remote IP field remains blank even though its BGP configuration address is sent to the appliance.
6. The Local Subnets field is no used with a VTI gateway.
7. The Preference parameter is meaningless in this Use Case because there is only one external gateway. In the case there are two gateways with the same subnet, the Preference value enables you to define which tunnel has priority to route the traffic.

   The highest Preference value implies priority. The default value is 100.
8. **Update** your settings. The tunnel is created.

Advanced Configuration

To configure some security, authentication, time and routing and cloud access parameters, select **Network -> Advanced Configuration** from the Orchestrator main menu.

> **Note:** the values displayed in the forms are default values.

Local Breakout

According to your deployment, you may deactivate the Local Breakout rule, i.e. the capacity of Branch Office Sites to access directly to the Internet.

By default, Local Breakout is activated if at least one Branch Office Site in your network has a direct Internet Access. To change this behavior and, for example, specify that all the Internet traffic must be routed through MPLS, select MPLS from the Transport Network stack of values.

You can also totally deactivate the function by disabling it ✖.

Overlay Routing

- Overlay IP Network: subnet where the Orchestrator selects the addresses of the appliance internal interfaces.
- AS Number Range: the Orchestrator uses this range of values to configure Site autonomous systems automatically (refer to "Configuring the LAN").
- AS Number Exclusion: values or range of values you want to exclude from the AS Number Range; reserved values. Authorized separators are ",|;"
  - Simple values: N where 1<= N <= 65535
  - Value ranges: N-M where N<M and 1 <= N, M <= 65535

  Multi-format example: `65002,65012-65024|65042;65122`

Validate your input by hitting the **Create** button. To modify any advanced configuration data, click the **Update** button. The last modification date and owner are specified in the right top corner of the form.

Routing Loop Prevention

To prevent OSPF routing loops (refer to "Configuring OSPF") from a Hybrid Data Center to a Hybrid Site, define a BGP Community and an OSPF Tag.

- BGP Community: four bytes value split in half by ':'

  - The first half of the value corresponds to 0001 - FFFE (FFFE is the default). 0000 and FFFF are forbidden.
  - The second half of the value corresponds to 0000 - FFFF (FF01 is the default).
- OSPF Tag: the authorized value range is [1 - 65535]. The default value is 6976.

For example, in "Use Case 1", the MPLS CE router (10.1.4.254) will probably re-route the traffic to the hybrid Data Center appliance router (10.1.4.4) and use the Internet route towards B02 instead of using the MPLS route towards the same appliance. To avoid this behavior:

- The B02 appliance router sets the BGP Community you define on the routes exported into the overlay BGP, which enables the Data Center appliance router to identify these routes, tag them with the tag you define and redistribute them into OSPF.
- After you have manually configured the MPLS CE router accordingly, it will be able to reject any tagged routes coming from the Data Center, or not redistribute them into MPLS VPN's BGP.

Overlay Security

The following parameters only apply to the tunnels

- between SD-WAN appliances
- between SD-WAN appliances and external gateways
- between SD-WAN appliances and cloud gateways

IKE policy

Internet Key Exchange (IKE) is a key management protocol that is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and to automatically establish IPsec security associations (SAs). Refer to RFC 5996.

- Encryption: drop-down list to choose the encryption algorithm (mandatory): AES-128 CBC, AES-192 CBC, AES-256 CBC, AES-128 GCM, AES-192 GCM, AES-256 GCM, AES-128 GMAC, AES-192 GMAC, AES-256 GMAC and 3DES,
- Integrity drop-down list to choose the data integrity hash method: SHA1, SHA-256, SHA-384, SHA-512 and MD5,
- DH Group drop-down list to choose the Diffie-Hellman group: 1 (768-bit), 2 (1024-bit), 5 (1536-bit), 14, 19, 20, 21 and 24,
- SA lifetime (seconds) Security Association lifetime (86,400 (= 24 h) by default). The authorized range of values is [120 -172800].

IPsec policy

- Encryption: drop-down list to choose the encryption algorithm (mandatory). The available options are the same as for IKE policy encryption plus NULL,

- Integrity drop-down list to choose the data integrity hash method (mandatory); see IKE policy integrity,
- DH Group (PFS only): drop-down list to choose the Diffie-Hellman group: 1 (768-bit), 2 (1024-bit) or 5 (1536-bit), 14, 19, 20, 21, 24 and PFS disabled (PFS ensures that the same key will not be generated again, so forces a new Diffie-Hellman key exchange. Both sides of VPN should support PFS in order for PFS to work. Therefore using PFS provides a more secure VPN connection),
- SA lifetime (seconds) Security Association lifetime (86,400 s that is: 24 hours by default; mandatory). The authorized range of values is [120 -172800],
- Lifebytes (kbytes): number of kilobytes sent through the tunnel before it is renewed; the tunnel is renewed after the SA lifetime period of after the Lifebytes period, whichever expires first. Valid values are in the range [5120 - 2147483648 kbytes],
- MTU (bytes): maximum number of bytes loaded in the Payload. The default value is 1400. This value applies to all IPsec tunnels.

IPsec Concentrator authentication

If a Pre-Shared key is already configured, this field is displayed in green and may remain empty.

This Pre-Shared key is used for all the tunnels between appliances. Though it is automatically generated by the Orchestrator for each Customer, you may also enter a new Pre-Shared key as a string of 32 characters at least. Use the 👁 icon different statuses to either display or hide the key.

CloudMesh

The information of the CloudMesh Overlay Routing section is for consultation only.

- Overlay IP Network: subnet where the Orchestrator selects the addresses of the appliance internal interfaces to connect to CloudMesh Edges. You cannot use this range in your network.
- AS Number: CloudMesh Core uses this AS number. You cannot reuse or modify this parameter.

Syslog Servers

To enable log export by SD-WAN appliances about NATted DTI connections, you must define one (or several) Syslog Server(s) in your network.

After you have clicked 'Add Server', enter the server Name, type its IP Address (preferably in your private network) or FQDN, Protocol (TCP or UDP) and Port. When NAT entries are created, logs are sent to the Syslog Server in `syslog` format.

> **Warning:** log export is not available on VRRP backups (with unmounted tunnels).

Time Synchronization

- Define the Time Server by entering an IP address.

  Using a Time Server located inside the Customer private network is recommended.
- Then select from the stack up to 5 hub appliances to be used as Synchronization Servers.

  These appliances are synchronized with the Time Server; they are used as synchronization references for all the other appliances of the Customer network.

Transport Network Settings

You may activate eligibility to DTI globally by selecting the appropriate Transport Network. If you select 'Internet', all Internet L3 WAN interfaces of all the appliances in your network will be eligible to DTI.

VRRP

> **Warning:** only VRRP Version 2 is supported. Delays can only be defined in seconds or in milliseconds divisible by 1000.

General

- Advertising Interval (seconds): the virtual router (master) sends VRRP advertisements to other VRRP routers in the same group. The priority and group ID of the virtual router master are carried in the advertisements. Advertisements are sent every second by default.
- Priorities - Master, Backup and Failed Check: priority values for the VRRP preemption mechanism. The device with the highest priority within the group becomes the master.
- If Preemption is activated (by default), the following rules apply by decreasing order of preference:
  - the virtual router backup that is elected to become the master remains the master until the original virtual router master recovers and becomes the master again (master/backup deployment).

    Mechanism:

    if the LAN interface is down, it is in FAULT state

    with the And logical operator, any health checked WAN interface that goes down degrades the priority by the specified Failed Check

    with the Or logical operator, the priority is not degraded until all health checked interfaces are down
- If preemption is disabled:

  - the virtual router backup that is elected to become the master remains the master until the original virtual router master recovers and becomes the master again (master/backup deployment)
  - the virtual router backup that is elected to become the master remains the master until it is in FAULT state. The other backup virtual router becomes the master and remains the master until it is in FAULT state; if both virtual routers are down, traffic stops. When the first backup virtual router recovers (from FAULT state to Backup state), it becomes the master again (backup/backup deployment).

    Mechanism:

    if the LAN interface is down, it is in FAULT state

    with the And logical operator, any health checked WAN interface that goes down triggers a router switch to FAULT state

    with the Or logical operator, the virtual router switches to FAULT state if all health checked WAN interfaces are down

> **Warning:** when preemption is disabled, there is no progressive health degradation. This can lead to a Site being isolated even if there is still a working WAN interface. For this reason, activating preemption is strongly recommended.

- Delay (seconds): delays VRRP transition to the master by the number of seconds specified (1 by default). This delay prevents the backup from becoming the master very frequently, in cases of network flapping.
- Health Check Interfaces:
  - Interval (milliseconds): by default, health check on interfaces is executed every second
  - Fall: number of failed health checks before the device is considered in bad health
  - Rise: number of successful health checks before the device is considered in good health again

Gratuitous ARP

A Gratuitous ARP is an ARP Response that was not prompted by an ARP Request. The Gratuitous ARP is sent as a broadcast, as a way for a node to announce or update its IP to MAC mapping to the entire network.

- Master:
  - Delay (seconds): delay for a second set of Gratuitous ARP messages after transition to Master. Default: 5. Enter 0 for no second set.
  - Repeat (count): number of Gratuitous ARP messages to send at a time after transition to Master. Default: 5
  - Refresh delay (seconds): minimum time interval for refreshing Gratuitous ARP messages while Master. Default: 0

  - Refresh repeat (count): number of Gratuitous ARP messages to send at a time while Master. Default: 5
- Lower priority:
  - Delay (seconds): delay for a second set of Gratuitous ARP messages after a lower priority advert has been received when Master. Default: 5. Enter 0 for no second set.
  - Repeat (count): number of Gratuitous ARP messages to send at a time after a lower priority advert has been received when Master. Default: 5.

Tuning

- Protocol Version: 2
- VRRP multicast group: IPv4 address of the group that corresponds to the abstract representation of the master and backup routers.
- Strict RFC adherence: check this option to ignore any customized settings and strictly adhere to VRRP rules.
- When master, do not send advert after receiving lower priority advert: optional
- When master, send advert after receiving higher priority advert: optional
- Do not send second GARP burst of packets: optional
- GARP Interval (microseconds): default interval between Gratuitous ARP messages sent on an interface
- ARP NA Interval (microseconds): default interval between unsolicited NA messages sent on an interface

IHAP

The following parameters identify the IHAP Profile you create or update.

> **Note:** A Default IHAP Profile with predefined configuration parameters is available.

- Name: name of the IHAP profile which is applied to both the nominal appliance and backup appliance of the Site.
- Engine bad health criteria for recognizing a failover condition:
  - any (default): failover condition is confirmed when any monitored interface is down
  - all: failover condition is confirmed when all the monitored interfaces are down
- Interfaces to monitor: select the interfaces you want to monitor by moving them from the left pane to the right pane.
- Keep alive: keep alive time in milliseconds. The authorized range is [50 - 10000]. The default value is 100 ms.

- Peer dead factor: used to tune up the waiting time of the backup appliance before acknowledging the unresponsive active peer as down. The authorized range is [3 - 10]. The default value is 5.
- Tunnel persistence: by default, this option is disabled, i.e. there are no mounted tunnels on the standby appliance.
- Preemption: this option is enabled by default. It means that the nominal standby appliance can preempt the backup active engine and become active again.

Cloud Access

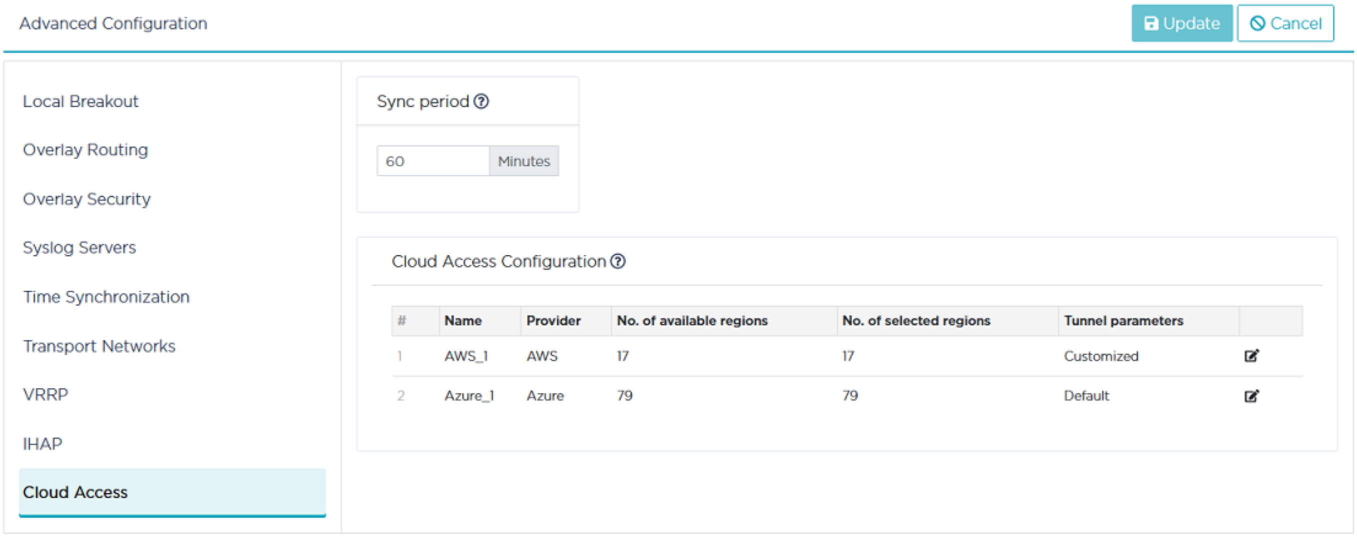
This section lists all the defined Cloud Access objects (AWS or Azure) and enables you to select related Regions and define tunnel parameters.

Sync Period

By default, the SD-WAN Orchestrator checks the configuration of VPN connections in AWS or Azure every 60 minutes. The Sync Period minimum value is 15 minutes; its maximum value is 1 day. This parameter applies to all Cloud Access objects, whichever the Cloud Provider may be.

Cloud Access Configuration

This window section enables you to modify the default configuration of any Cloud access object. Click ✎ on the Cloud Access object to be modified.



Sync period: 60 Minutes

Cloud Access Configuration

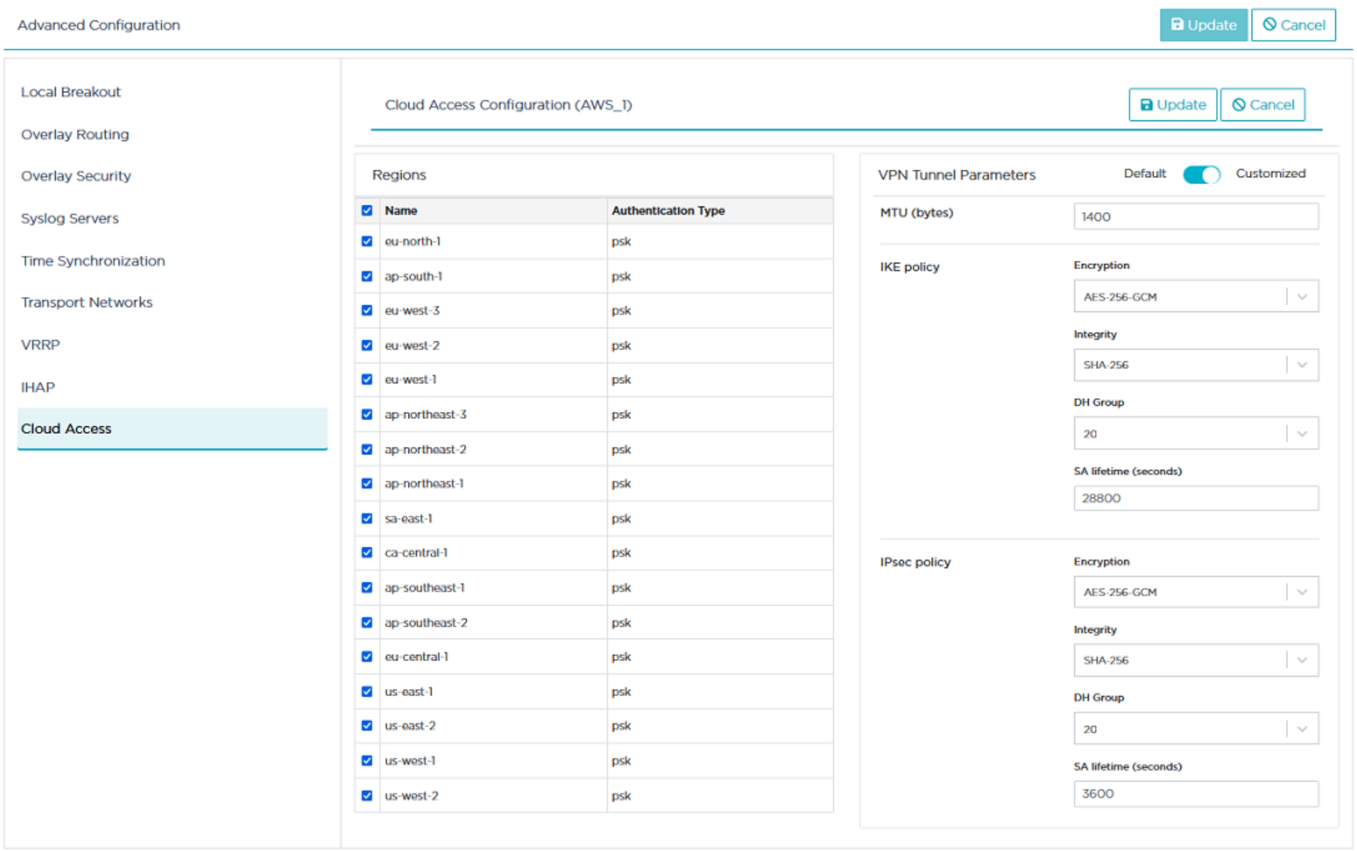
#	Name	Provider	No. of available regions	No. of selected regions	Tunnel parameters	
1	AWS_1	AWS	17	17	Customized	✎
2	Azure_1	Azure	79	79	Default	✎

- Name: Cloud Access name. This name identifies the Cloud account in the ExtremeCloud SD-WAN Orchestrator.
- Provider: Cloud Provider (AWS, Azure).
- No of available regions: by default, all the regions enabled on the AWS or Azure account are selected.
- No of selected regions:

- with AWS, this field specifies the number of regions you selected if you disabled some regions from the default list. Note that the SD-WAN Orchestrator will not discover any gateways in disabled regions.
- with Azure, this field specifies all the regions of the default list; you cannot disable any regions.

- Tunnel parameters: you can customize VPN Tunnel Parameters values instead of using the default ones. Refer to "Overlay Security"

AWS



Cloud Access Configuration (AWS_1)

Regions

☑	Name	Authentication Type
☑	eu-north-1	psk
☑	ap-south-1	psk
☑	eu-west-3	psk
☑	eu-west-2	psk
☑	eu-west-1	psk
☑	ap-northeast-3	psk
☑	ap-northeast-2	psk
☑	ap-northeast-1	psk
☑	sa-east-1	psk
☑	ca-central-1	psk
☑	ap-southeast-1	psk
☑	ap-southeast-2	psk
☑	eu-central-1	psk
☑	us-east-1	psk
☑	us-east-2	psk
☑	us-west-1	psk
☑	us-west-2	psk

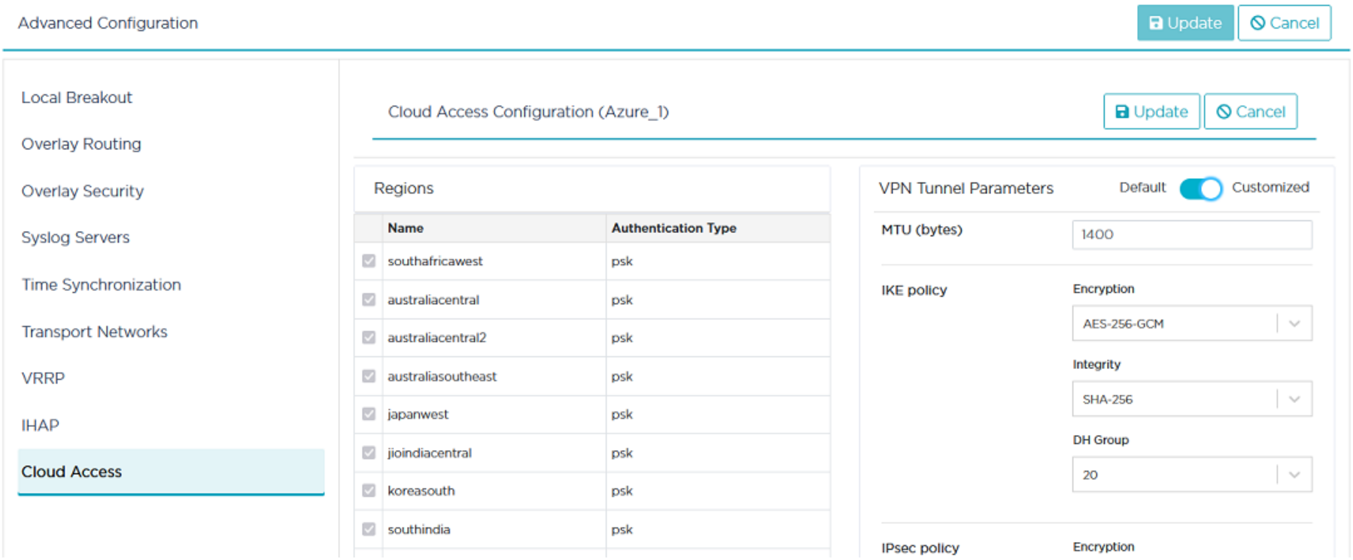
VPN Tunnel Parameters Default ● Customized

MTU (bytes) 1400

IKE policy
Encryption AES-256-GCM
Integrity SHA-256
DH Group 20
SA lifetime (seconds) 28800

IPsec policy
Encryption AES-256-GCM
Integrity SHA-256
DH Group 20
SA lifetime (seconds) 3600

Azure



	Name	Authentication Type
☑	southafricawest	psk
☑	australiacentral	psk
☑	australiacentral2	psk
☑	australiasoutheast	psk
☑	japanwest	psk
☑	jioindiacentral	psk
☑	koreasouth	psk
☑	southindia	psk

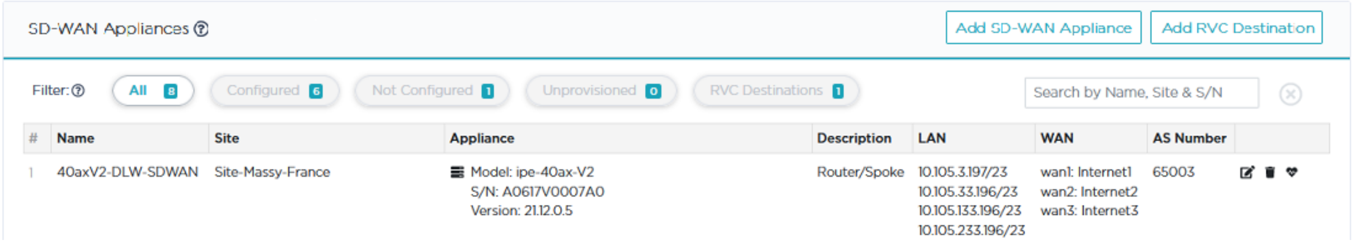
MTU (bytes): 1400

IKE policy
- Encryption: AES-256-GCM
- Integrity: SHA-256
- DH Group: 20

IPsec policy
- Encryption

Surveying SD-WAN appliance details

You can access this information window by clicking the ♥ icon for any appliance on the **Network -> Configuration** window.



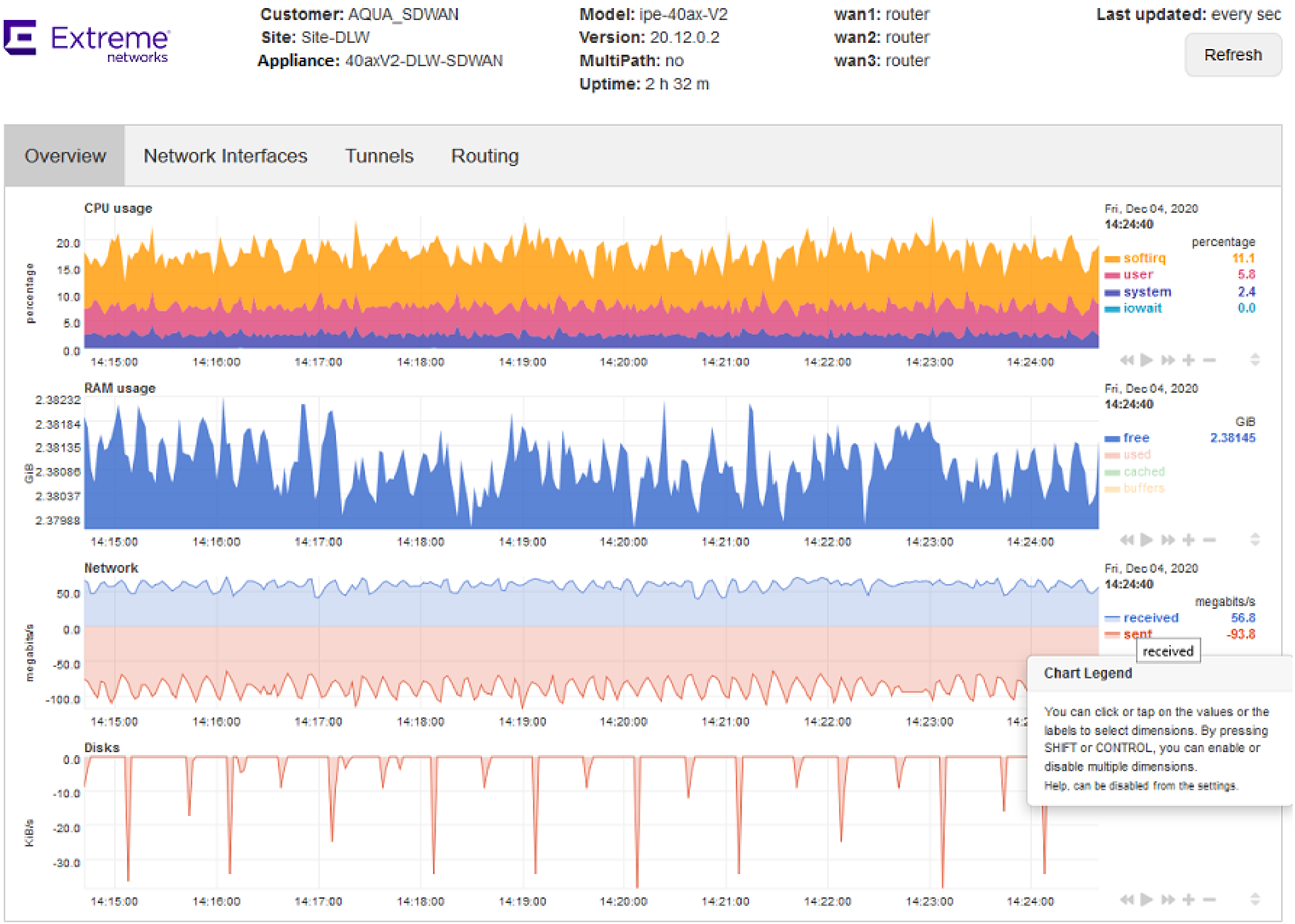
SD-WAN Appliances ⓘ

#	Name	Site	Appliance	Description	LAN	WAN	AS Number	
1	40axV2-DLW-SDWAN	Site-Massy-France	Model: ipe-40ax-V2 S/N: A0617V0007A0 Version: 21.12.0.5	Router/Spoke	10.105.3.197/23 10.105.33.196/23 10.105.133.196/23 10.105.233.196/23	wan1: Internet1 wan2: Internet2 wan3: Internet3	65003	

This window is divided into four sections/tabs that enable your network administrator to check detailed configuration information for a specific appliance before troubleshooting. The process of data collection only starts when you open the window.

The main parameters of this appliance are specified at the top, beside the Extreme Networks logo.

Except for the Overview section where data are refreshed every second, the **Last updated** incrementing counter in the other sections of the window lets you know when data display was last refreshed. Note that when the connection with the appliance is lost, this counter is blinking: **Last updated:** 3 m 11 s ago



Customer: AQUA_SDWAN
Site: Site-DLW
Appliance: 40axV2-DLW-SDWAN

Model: ipe-40ax-V2
Version: 20.12.0.2
MultiPath: no
Uptime: 2 h 32 m

wan1: router
wan2: router
wan3: router

Last updated: every sec

Chart Legend

You can click or tap on the values or the labels to select dimensions. By pressing SHIFT or CONTROL, you can enable or disable multiple dimensions.

Help, can be disabled from the settings.

Overview

This section displays:

- the current CPU usage in percentage and an evolution graph of CPU usage over the last 15 minutes
- the current RAM usage in percentage and an evolution graph of RAM usage over the last 15 minutes
- the current traffic received from and sent to the network in bits/s and an evolution graph of received/sent traffic over the last 15 minutes
- the current reads and writes (I/O) on disks in bytes/s and an evolution graph of them over the last 15 minutes

The previous metrics are refreshed every 1 to 5 seconds whereas the time span of the graphs corresponds to the last 15 minutes with 1s to 5s data points. Note that you can also refresh the data manually by clicking Refresh in the top right corner of the window.

> **Note:** the curves that represent sent traffic on the Network graph and out traffic on the Disks graph are not negative but displayed that way for distinctness.

In the legend, click the labels or values to limit graph display to specific curves. Simultaneously press the Shift or Control key and click a label/value to enable or disable curve display.

The following sections (Network Interfaces, Tunnels and Routing) include tables of data and no graphs. You may filter table information by entering a filter in the top row of every column. You may sort table information by clicking the heading name of each column.

Network Interfaces

This section provides the status of the physical and logical network interfaces. Table data are collected every 10s.

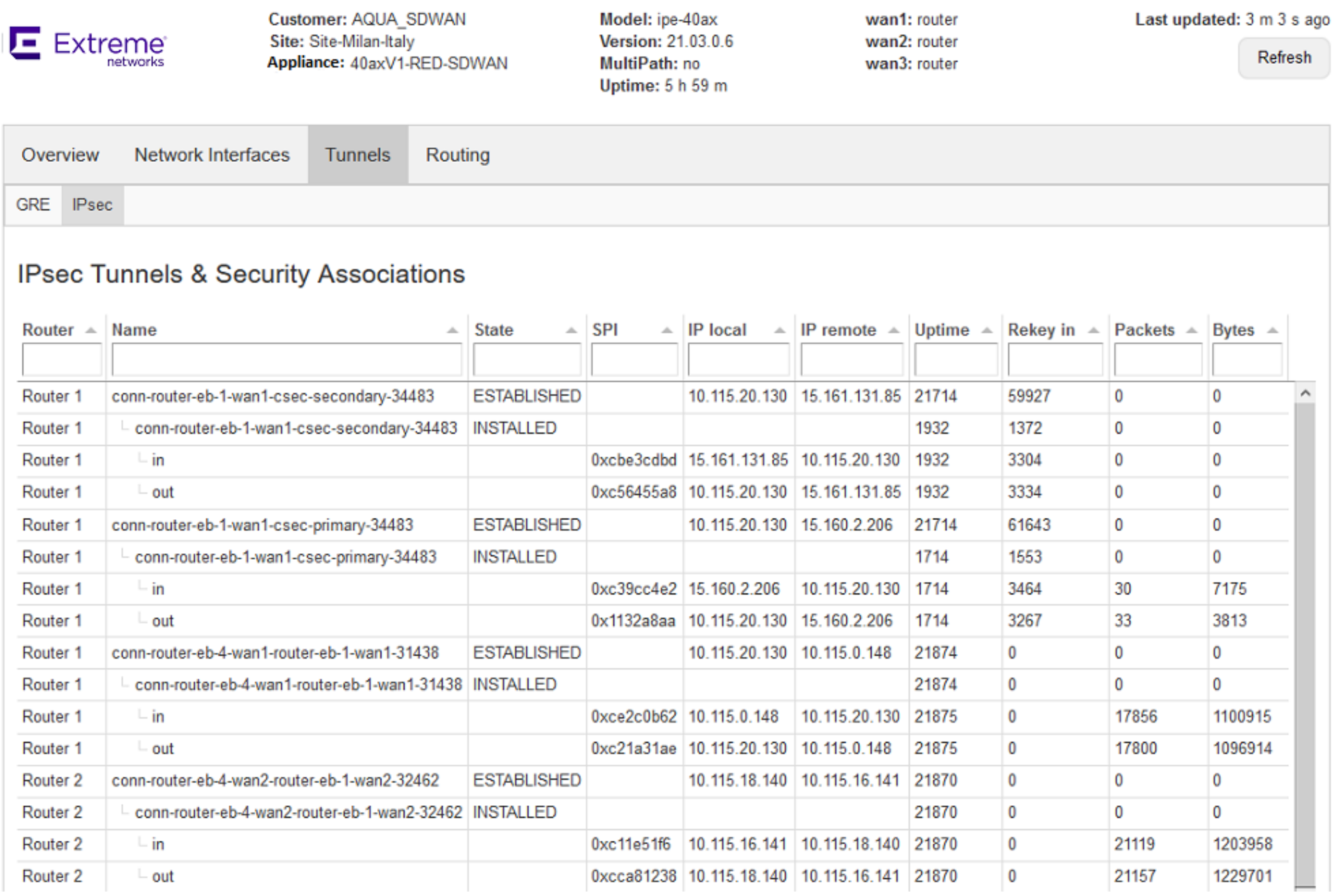
Note that the Router column of both tables specifies either the appliance itself (Local) or one appliance embedded router (Router 1/2/3) related to a WAN interface.

Tunnels

This section contains two sub-tabs, GRE and IPsec.

- The GRE Tunnels table lists the entry points of the GRE tunnels between the appliances of your network. Table data are collected every 10s.
- The IPsec Tunnels and Security Association table provides detailed information about the tunnels created by interface. Table data are collected every 30s.

In the example below, the first two IPsec tunnels are EdgeSentry tunnels.



Customer: AQUA_SDWAN
Site: Site-Milan-Italy
Appliance: 40axV1-RED-SDWAN

Model: ipe-40ax
Version: 21.03.0.6
MultiPath: no
Uptime: 5 h 59 m

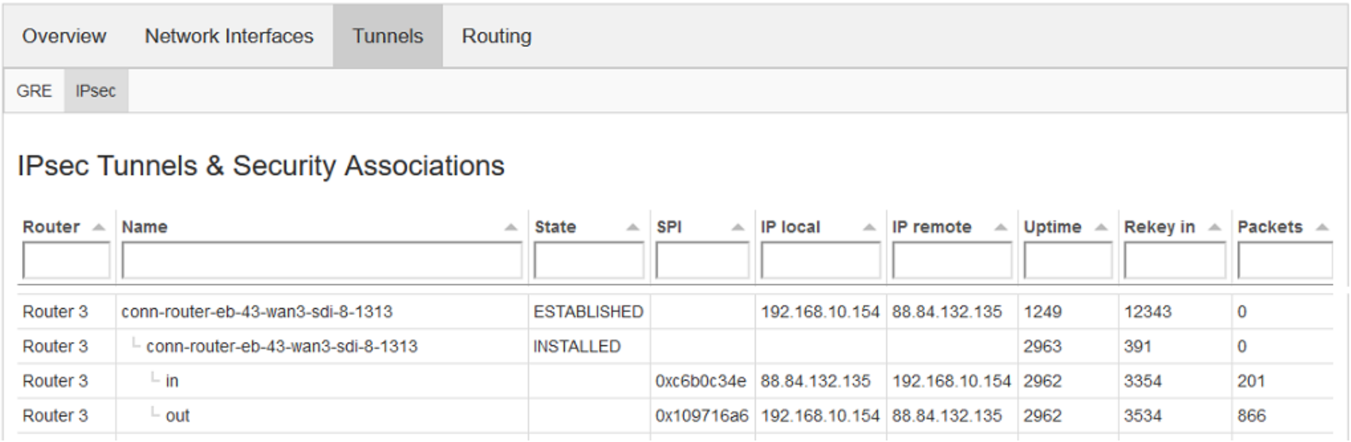
wan1: router
wan2: router
wan3: router

Last updated: 3 m 3 s ago

IPsec Tunnels & Security Associations

Router	Name	State	SPI	IP local	IP remote	Uptime	Rekey in	Packets	Bytes
Router 1	conn-router-eb-1-wan1-csec-secondary-34483	ESTABLISHED		10.115.20.130	15.161.131.85	21714	59927	0	0
Router 1	└ conn-router-eb-1-wan1-csec-secondary-34483	INSTALLED				1932	1372	0	0
Router 1	└ in		0xcbe3cdbd	15.161.131.85	10.115.20.130	1932	3304	0	0
Router 1	└ out		0xc56455a8	10.115.20.130	15.161.131.85	1932	3334	0	0
Router 1	conn-router-eb-1-wan1-csec-primary-34483	ESTABLISHED		10.115.20.130	15.160.2.206	21714	61643	0	0
Router 1	└ conn-router-eb-1-wan1-csec-primary-34483	INSTALLED				1714	1553	0	0
Router 1	└ in		0xc39cc4e2	15.160.2.206	10.115.20.130	1714	3464	30	7175
Router 1	└ out		0x1132a8aa	10.115.20.130	15.160.2.206	1714	3267	33	3813
Router 1	conn-router-eb-4-wan1-router-eb-1-wan1-31438	ESTABLISHED		10.115.20.130	10.115.0.148	21874	0	0	0
Router 1	└ conn-router-eb-4-wan1-router-eb-1-wan1-31438	INSTALLED				21874	0	0	0
Router 1	└ in		0xce2c0b62	10.115.0.148	10.115.20.130	21875	0	17856	1100915
Router 1	└ out		0xc21a31ae	10.115.20.130	10.115.0.148	21875	0	17800	1096914
Router 2	conn-router-eb-4-wan2-router-eb-1-wan2-32462	ESTABLISHED		10.115.18.140	10.115.16.141	21870	0	0	0
Router 2	└ conn-router-eb-4-wan2-router-eb-1-wan2-32462	INSTALLED				21870	0	0	0
Router 2	└ in		0xc11e51f6	10.115.16.141	10.115.18.140	21870	0	21119	1203958
Router 2	└ out		0xcca81238	10.115.18.140	10.115.16.141	21870	0	21157	1229701

The example below displays a CloudMesh tunnel.



IPsec Tunnels & Security Associations

Router	Name	State	SPI	IP local	IP remote	Uptime	Rekey in	Packets
Router 3	conn-router-eb-43-wan3-sdi-8-1313	ESTABLISHED		192.168.10.154	88.84.132.135	1249	12343	0
Router 3	└ conn-router-eb-43-wan3-sdi-8-1313	INSTALLED				2963	391	0
Router 3	└ in		0xc6b0c34e	88.84.132.135	192.168.10.154	2962	3354	201
Router 3	└ out		0x109716a6	192.168.10.154	88.84.132.135	2962	3534	866

An additional table contains IPsec Log entries. Log data are collected every 5s.

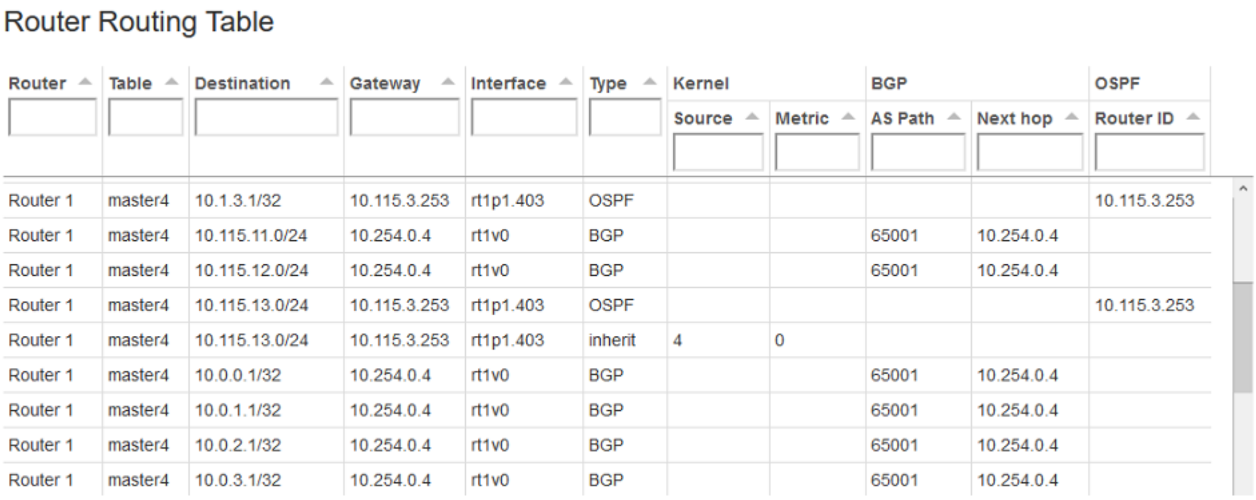
Routing

The Routing section contains five sub-tabs: Routes, OSPF, VRRP, HA, ARP and Logs.

The information of all Routing sub-tab tables is not automatically refreshed when you navigate from one sub-tab to another; this behavior enables you to compare the different data for the same data collect. To refresh the information of all Routing sub-tab tables, do it manually by clicking Refresh in the top right corner of the window.

The data of all these tables are collected every 30s, except Log data which are collected every 5s.

- The Local/Router Routing tables lists the IP routes between Sites.

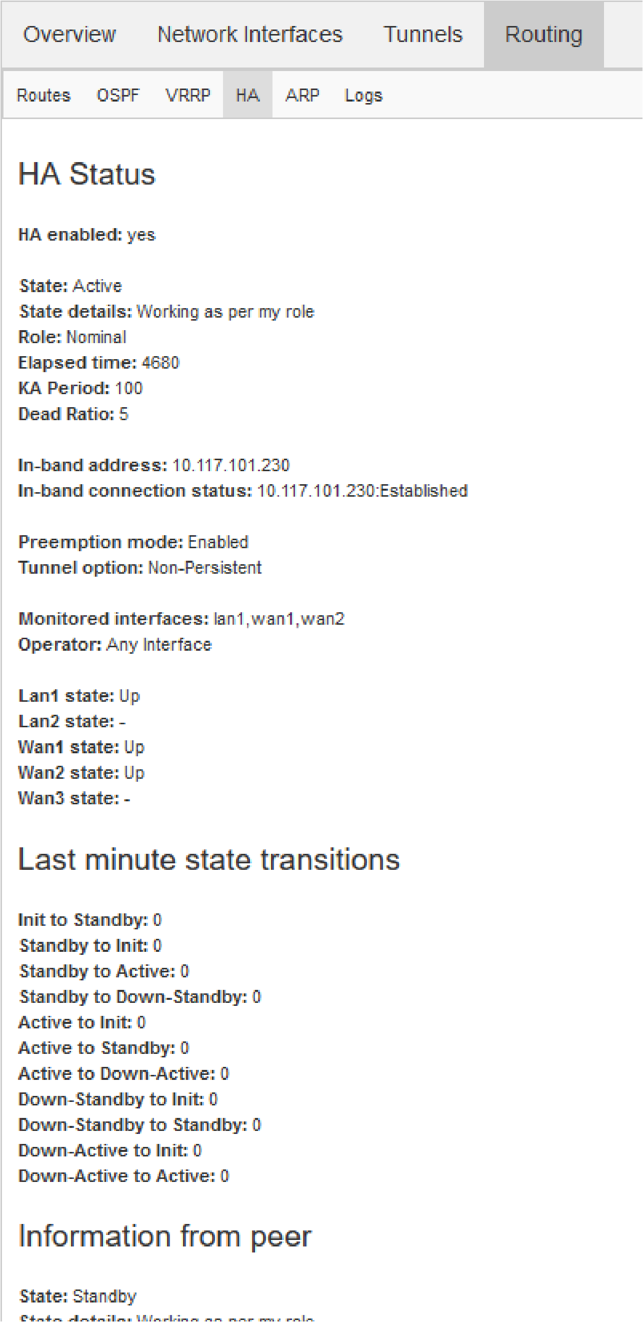


Router Routing Table

Router	Table	Destination	Gateway	Interface	Type	Kernel		BGP		OSPF
						Source	Metric	AS Path	Next hop	Router ID
Router 1	master4	10.1.3.1/32	10.115.3.253	rt1p1.403	OSPF					10.115.3.253
Router 1	master4	10.115.11.0/24	10.254.0.4	rt1v0	BGP			65001	10.254.0.4	
Router 1	master4	10.115.12.0/24	10.254.0.4	rt1v0	BGP			65001	10.254.0.4	
Router 1	master4	10.115.13.0/24	10.115.3.253	rt1p1.403	OSPF					10.115.3.253
Router 1	master4	10.115.13.0/24	10.115.3.253	rt1p1.403	inherit	4	0			
Router 1	master4	10.0.0.1/32	10.254.0.4	rt1v0	BGP			65001	10.254.0.4	
Router 1	master4	10.0.1.1/32	10.254.0.4	rt1v0	BGP			65001	10.254.0.4	
Router 1	master4	10.0.2.1/32	10.254.0.4	rt1v0	BGP			65001	10.254.0.4	
Router 1	master4	10.0.3.1/32	10.254.0.4	rt1v0	BGP			65001	10.254.0.4	

- The VRRP table data let you know whether your VRRP configurations (if any) are working or not. Refer to "Configuring a multi-appliance Branch Office Site through VRRP".
- The OSPF table data let you know whether OSPF configurations (if any) are working properly.

  Select the Router (1/2/3) for which you want to display OSPF Neighbors and OSPF Areas information. By default, all the available routers are selected. Refer to "Configuring a multi-appliance Hybrid Data Center through OSPF".
- The HA Status data let you know whether IHAP configurations are working properly. This information is provided for each selected HA appliance. Refer to "Configuring a multi-appliance Branch Office Site through IHAP".



HA Status

HA enabled: yes

State: Active
State details: Working as per my role
Role: Nominal
Elapsed time: 4680
KA Period: 100
Dead Ratio: 5

In-band address: 10.117.101.230
In-band connection status: 10.117.101.230:Established

Preemption mode: Enabled
Tunnel option: Non-Persistent

Monitored interfaces: lan1,wan1,wan2
Operator: Any Interface

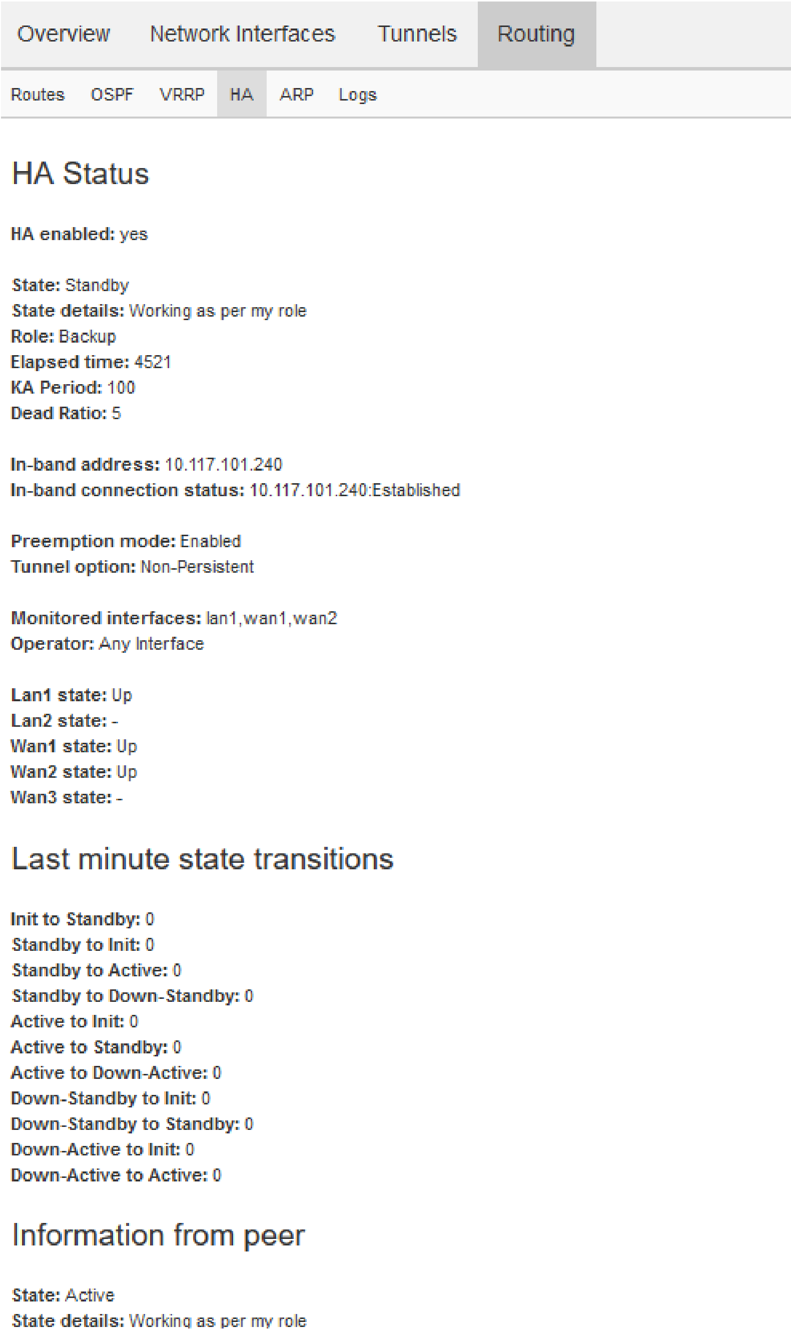
Lan1 state: Up
Lan2 state: -
Wan1 state: Up
Wan2 state: Up
Wan3 state: -

Last minute state transitions

Init to Standby: 0
Standby to Init: 0
Standby to Active: 0
Standby to Down-Standby: 0
Active to Init: 0
Active to Standby: 0
Active to Down-Active: 0
Down-Standby to Init: 0
Down-Standby to Standby: 0
Down-Active to Init: 0
Down-Active to Active: 0

Information from peer

State: Standby
State details: Working as per my role



HA Status

HA enabled: yes

State: Standby
State details: Working as per my role
Role: Backup
Elapsed time: 4521
KA Period: 100
Dead Ratio: 5

In-band address: 10.117.101.240
In-band connection status: 10.117.101.240:Established

Preemption mode: Enabled
Tunnel option: Non-Persistent

Monitored interfaces: lan1,wan1,wan2
Operator: Any Interface

Lan1 state: Up
Lan2 state: -
Wan1 state: Up
Wan2 state: Up
Wan3 state: -

Last minute state transitions

Init to Standby: 0
Standby to Init: 0
Standby to Active: 0
Standby to Down-Standby: 0
Active to Init: 0
Active to Standby: 0
Active to Down-Active: 0
Down-Standby to Init: 0
Down-Standby to Standby: 0
Down-Active to Init: 0
Down-Active to Active: 0

Information from peer

State: Active
State details: Working as per my role

- The ARP Cache displays all necessary data.
- The Logs table displays BIRD logs.

3 Configuring and Monitoring Applications

This section describes how to configure and monitor applications. It addresses the following topics:

- "Using the Web Client Interface"
- "System Provisioning Tools"
- "Application Provisioning"
- "SSL Optimization"
- "Monitoring"

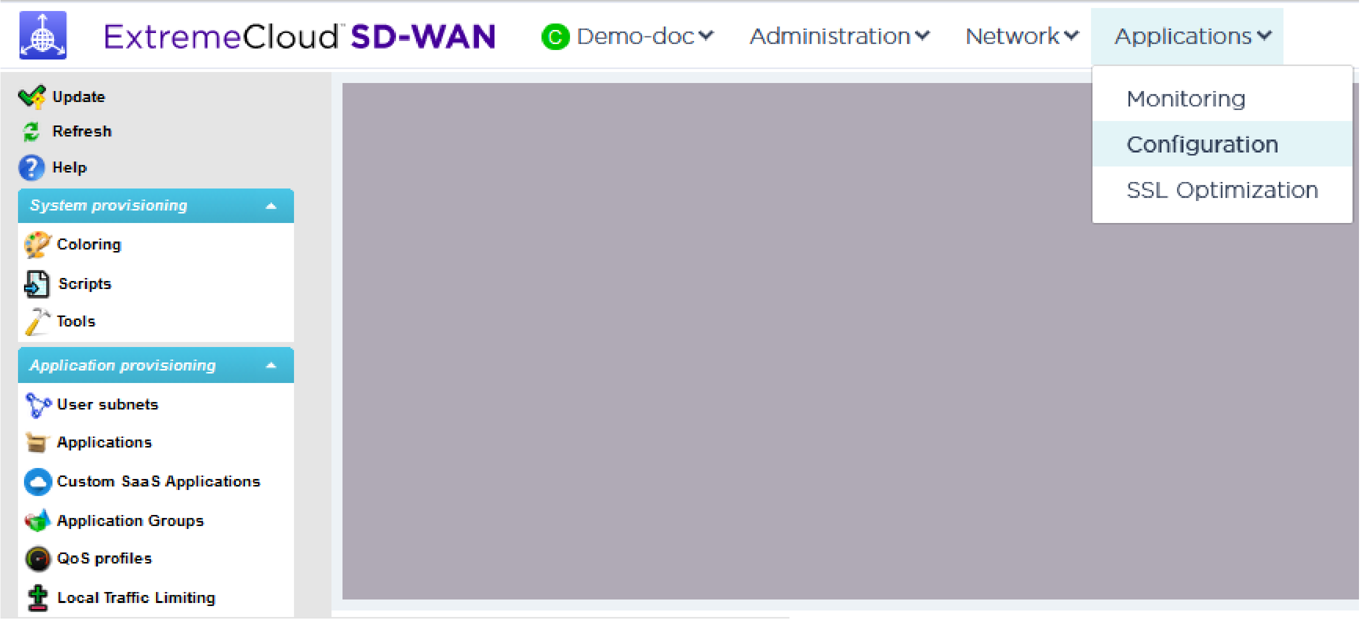
Using the Web Client Interface

This chapter addresses the following topics:

- "Connection"
- "Application Configuration Toolbar"
- "Application Configuration Table View and Toolbar"
- "Exporting Objects"

Connection

From the SD-WAN Orchestrator main menu, select **Applications -> Configuration**.

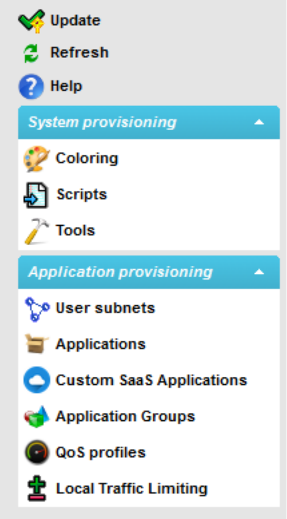


The main window is divided into two parts:

- A toolbar, on the left: it is composed of menus and icons which give access to the different functions of the software. It depends on the profile of the connected user.
- A working space.

Application Configuration Toolbar

The content of the toolbar depends on the profile of the connected User.



Global functions

Save/Update: saves/updates the configuration; flashes when an update is necessary

Refresh: refreshes the view

Help: gives access to online help

Coloring: configures the coloring rules

Scripts: launches scripts

Tools: starts the following management features:

- software upgrade
- reboot
- advanced configuration

User subnets: configures the User subnet addresses

Applications: configures the applications

Custom SaaS Applications: configures customized SaaS applications

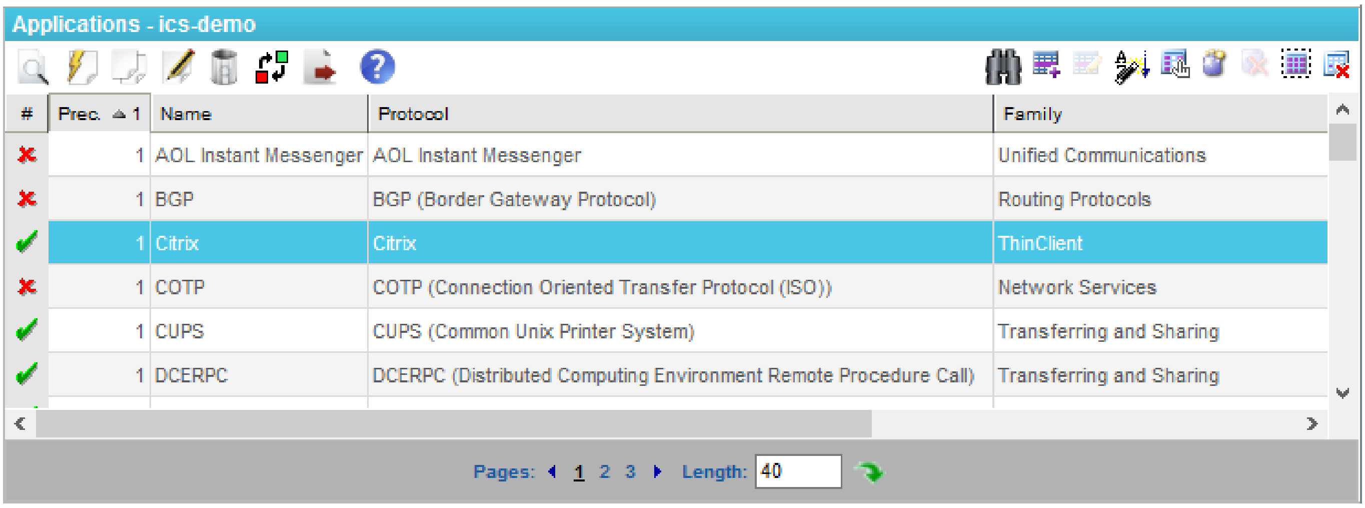
Application Groups: configures the Application Groups

QoS Profiles: configures the QoS Profile

Local Traffic Limiting: configures traffic limiting rules per Site

Application Configuration Table View and Toolbar

Typical window with a table view:



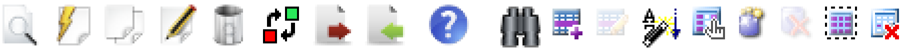
Applications - ics-demo

#	Prec. ▲ 1	Name	Protocol	Family
✗	1	AOL Instant Messenger	AOL Instant Messenger	Unified Communications
✗	1	BGP	BGP (Border Gateway Protocol)	Routing Protocols
✓	1	Citrix	Citrix	ThinClient
✗	1	COTP	COTP (Connection Oriented Transfer Protocol (ISO))	Network Services
✓	1	CUPS	CUPS (Common Unix Printer System)	Transferring and Sharing
✓	1	DCERPC	DCERPC (Distributed Computing Environment Remote Procedure Call)	Transferring and Sharing

Pages: ◂ 1 2 3 ▸ Length: 40

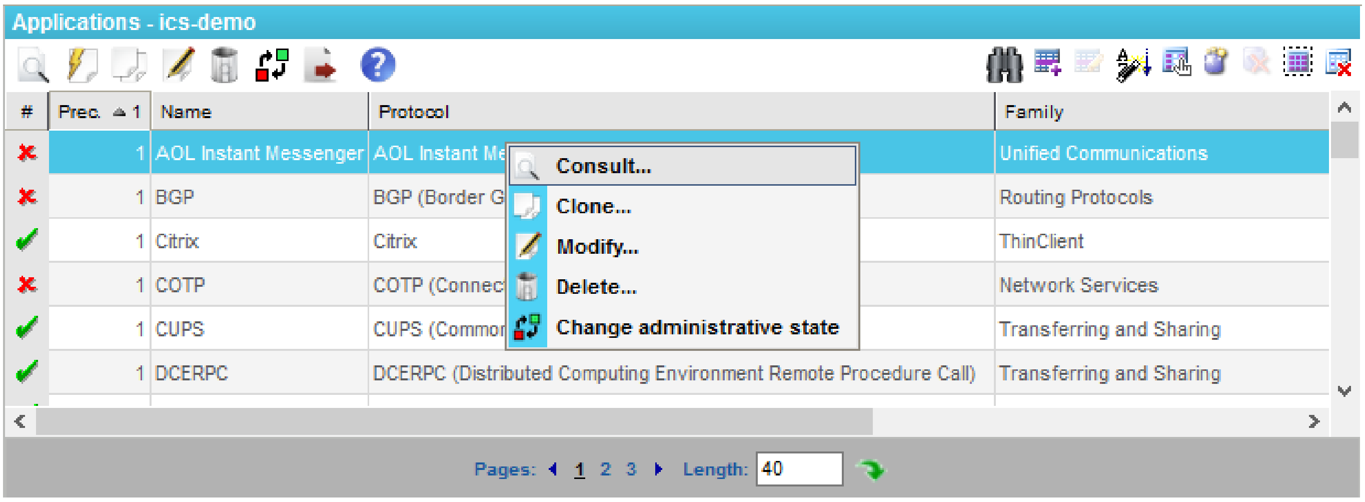
A table view shows:

- a toolbar in two parts:



,

- a list of objects.
  - **Selection**: you can select any object in the list by clicking on its line. To select other objects, you have to click on their lines while pressing the CTRL key. To select a range of objects, click the first object then the last one while keeping the Shift key down. You can use the Select All and Unselect All buttons to select/unselect all the objects on the list.
  - **Sort**: you can sort the list according to one column by clicking on this column header (by clicking on the header a second time, you change the ascending-descending order). By clicking on several columns while pressing the CTRL key, you make a sort on multiple columns.
  - **Edition**: you can consult and edit any object by right-clicking the object line. These right-click functions are also available as function buttons in the toolbar.



#	Prec. 1	Name	Protocol	Family
✗	1	AOL Instant Messenger	AOL Instant Me	Unified Communications
✗	1	BGP	BGP (Border G	Routing Protocols
✓	1	Citrix	Citrix	ThinClient
✗	1	COTP	COTP (Connec	Network Services
✓	1	CUPS	CUPS (Commor	Transferring and Sharing
✓	1	DCERPC	DCERPC (Distributed Computing Environment Remote Procedure Call)	Transferring and Sharing

The toolbar contains the same icons for most windows:

(**Consult**): to consult the properties of an object

(**New**): to create a new object

(**Clone**): to create an object from another one

(**Modify**): to modify one or more objects

(**Delete**): to delete one or more objects

(**Change administrative state**): to change the administrative state of one or more objects

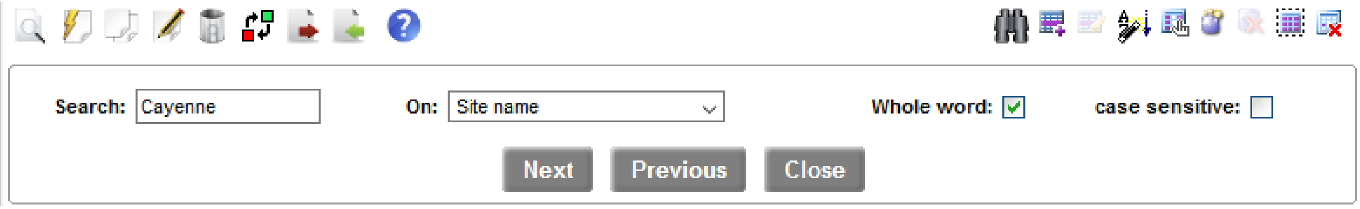
(**Export**): to export the content of a list to a text file

(**Import**): to import the content of a list from a text file

(**Help**): to display on-line documentation

(**Search**): to search for objects matching various criteria

Opens a dialog box enabling you to find all the objects through an attribute containing the specified text. The first matching object is highlighted in the table. Navigation between the found objects is made with the Next/Previous buttons.



Search: Cayenne

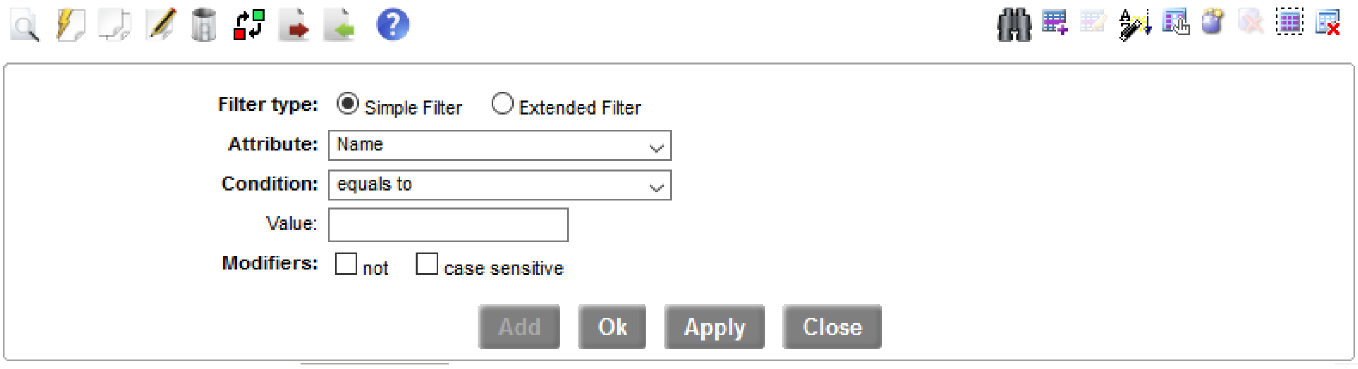
On: Site name

Whole word: ☑

case sensitive: □

(**New Filter**): to filter the data

You may create display filters on the list. As a result, only the objects matching the defined criteria are displayed.



Filter type: ● Simple Filter ○ Extended Filter

Attribute: Name

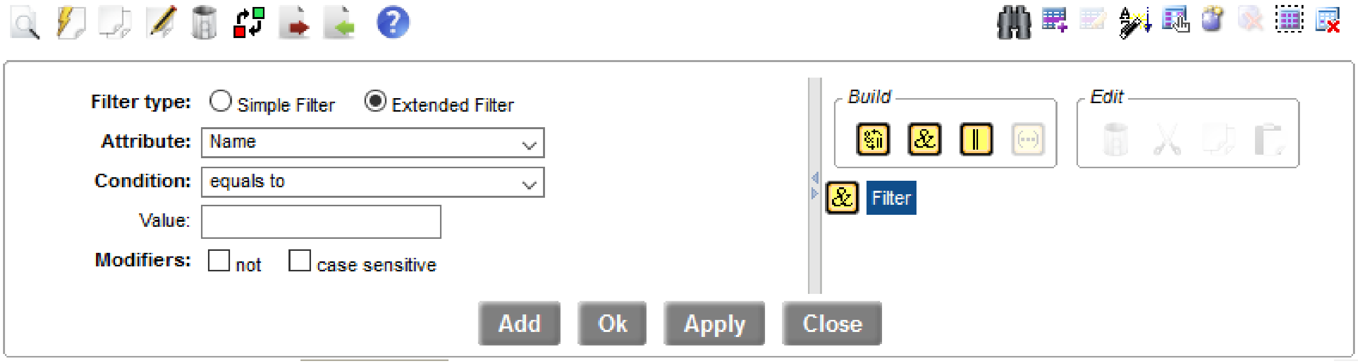
Condition: equals to

Value:

Modifiers: □ not □ case sensitive

You can choose between two filtering types:

- A Simple Filter works with only one field,
- An Extended Filter is a combination of simple filters (using AND, OR, NOT logical operators):



Filter type: ○ Simple Filter ● Extended Filter

Attribute: Name

Condition: equals to

Value:

Modifiers: □ not □ case sensitive

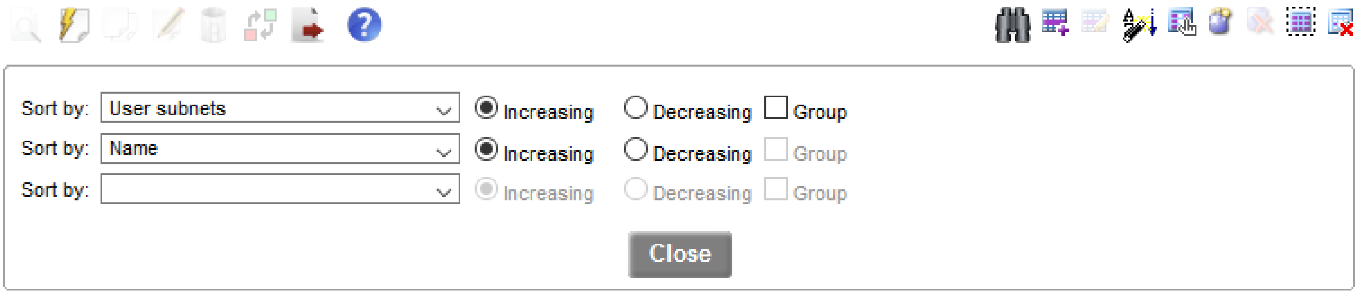
Select the filter criteria and use the Add, Ok, Apply and Close buttons to perform the corresponding actions.

When a filter is active, a tip is displayed at the bottom of the table view with the number of displayed objects out of the total number of objects. You can activate/deactivate a filter by double-clicking the tip icon Activated filter (1 object out of 106)

(**Modify Filter**): to modify filters

(**Sort by**): to sort the data

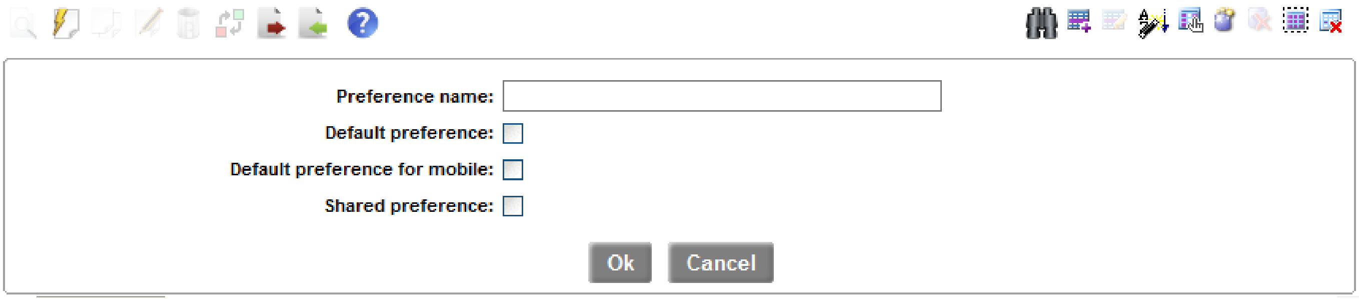
Sorts the data (by any value or combination of several values). You may also execute the sort operation in increasing/decreasing order, or by group.



Sort by: User subnets ● Increasing ○ Decreasing □ Group
Sort by: Name ● Increasing ○ Decreasing □ Group
Sort by: ○ Increasing ○ Decreasing □ Group

(**Choose Columns**): to choose the columns to display

(**Save preferences**): to save the view displaying the filters



Preference name:
Default preference: □
Default preference for mobile: □
Shared preference: □

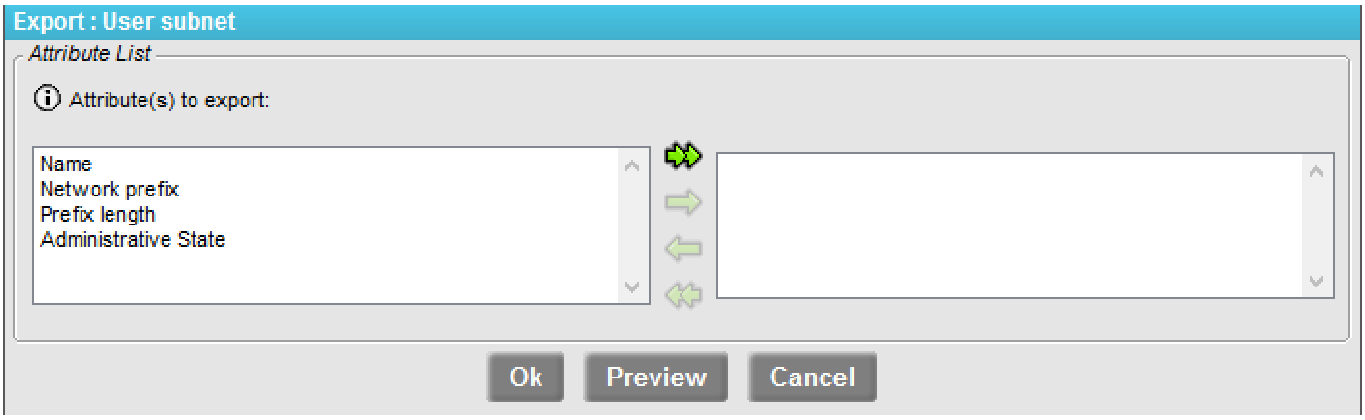
When you save a preference, give it a name (Preference name, e.g. my preferred view) and select whether you want it to be your default view (check the Default preference box), the default view for mobiles (check the Default preference for mobile box), whether you want it to be accessible by other users (check the Shared preference box). A drop-down list appears at the right of the toolbar, my preferred view, and enables you to select this preference, other saved preferences or the view with no filters (All).

(**Delete preferences**): to delete previously saved preferences.

Exporting Objects

Most objects (User subnets, Application Groups, etc.) can be exported.

In the window containing the objects you want to export, click on the Export icon or select the **File** menu, then **Export**. The following window opens:



Export : User subnet

Attribute List

Attribute(s) to export:

Name
Network prefix
Prefix length
Administrative State

1. Select the attributes you want to export by pushing them to the right with the double right-pointing arrow (objects will be exported with all their attributes) or with the single arrow to the right (objects will be exported with the selected attributes only). One attribute at least must be selected (otherwise, there would be no data to be exported at all; in that case, all of them are exported, as if the double arrow had been clicked).

   If some objects were selected before using the Export function, an Export selection check box enables you to export your selection only. If no object was selected or if the Export selection box is not checked, all objects are exported.

2. Click OK. A dialog box appears, allowing you to either open the result file (_exportXXX.res) or save it.

The first line of the result file (wrapped in the example below) is the description of the fields present, and the subsequent lines are the exported objects with the selected attributes:

```
@ipboss_name|ipboss_topology_subnet_network_prefix|ipboss_topology_subnet
 _prefix_length|ipboss_topology_subnet_site|ipboss_administrative_state|
 Lan_Augsburg|10.49.4.0|24|Site\Augsburg|0
 Lan_Bangalore|10.91.2.0|24|Site\Bangalore|0
```

System Provisioning Tools

The System Provisioning menu provides access to the following tools:

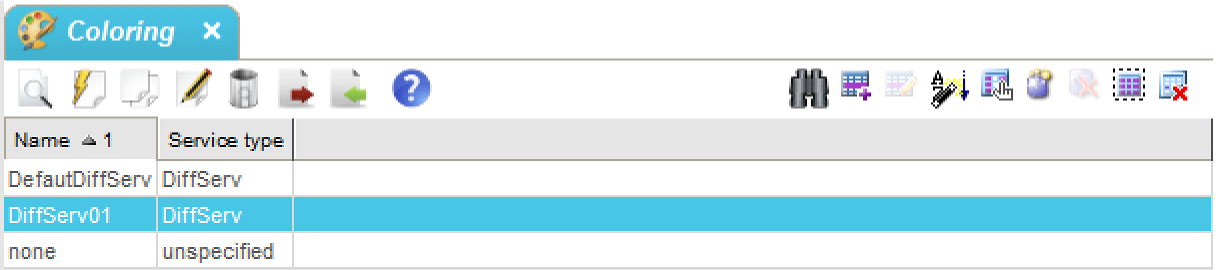
- "Configuring Coloring"
- "Scripts"
- "Upgrading the appliances"
- "Rebooting"
- "Configuring Advanced Settings"

Configuring Coloring

The Coloring Policy is used with Application Control. This facility modifies the TOS or DiffServ field in the IP header according to the type and criticality of the packet.

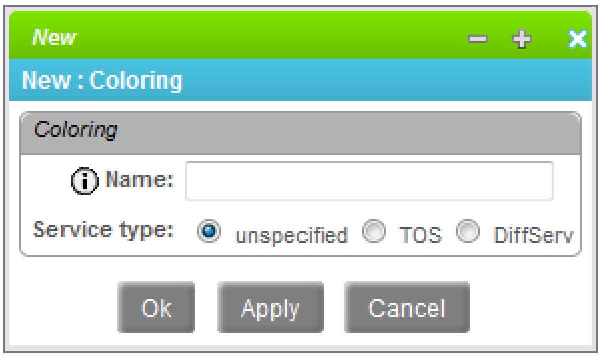
The default mode is Color-Blind (all packets are processed as if they were uncolored).

1 In the System provisioning Toolbar, select Coloring:



Name ▲ 1	Service type
DefautDiffServ	DiffServ
DiffServ01	DiffServ
none	unspecified

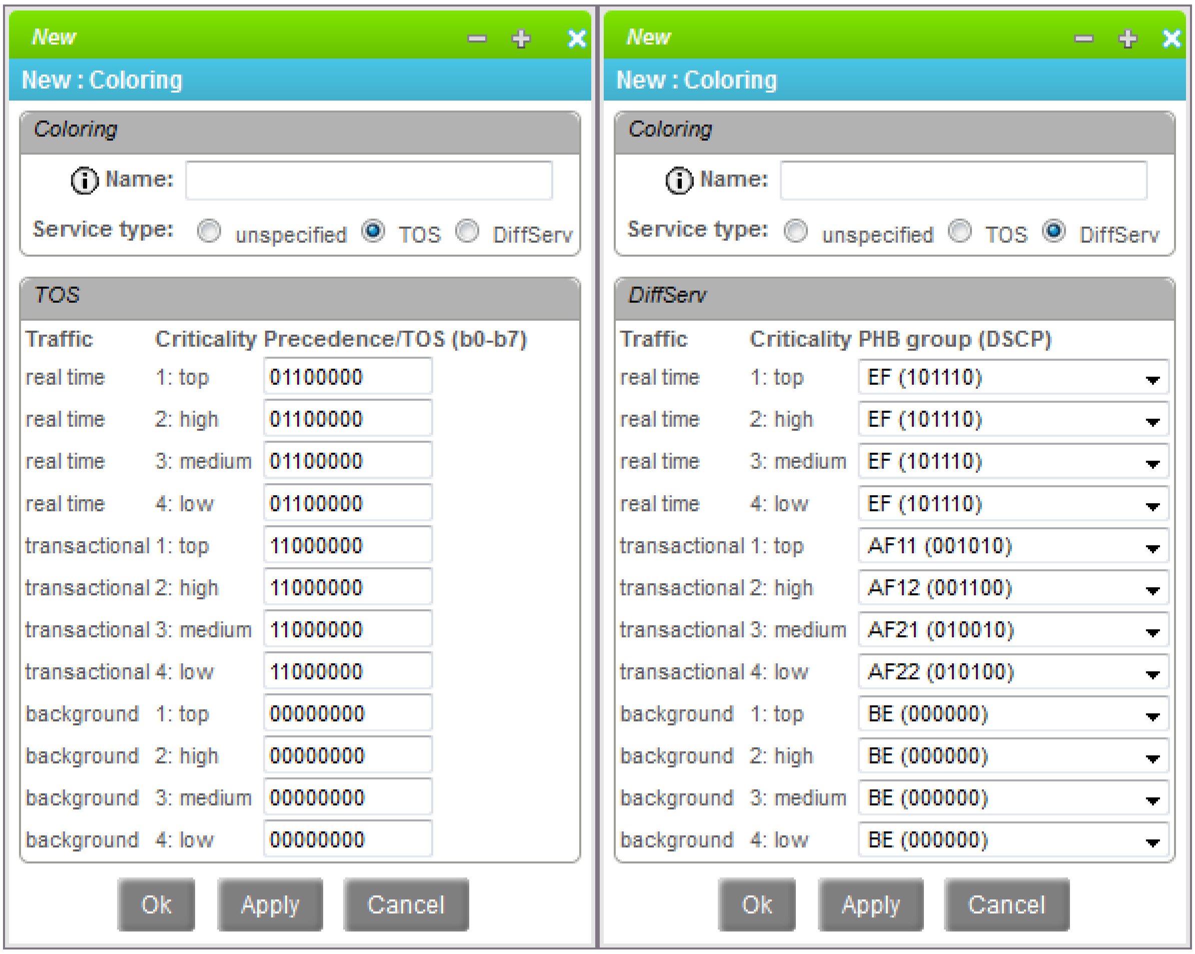
2 By clicking on the New button , the creation window of a new coloring rule is displayed.



Name:

Service type: ● unspecified ○ TOS ○ DiffServ

Coloring directory with TOS and DiffServ selections:



Name:

Service type: ○ unspecified ● TOS ○ DiffServ

TOS

Traffic	Criticality	Precedence/TOS (b0-b7)
real time	1: top	01100000
real time	2: high	01100000
real time	3: medium	01100000
real time	4: low	01100000
transactional	1: top	11000000
transactional	2: high	11000000
transactional	3: medium	11000000
transactional	4: low	11000000
background	1: top	00000000
background	2: high	00000000
background	3: medium	00000000
background	4: low	00000000

Name:

Service type: ○ unspecified ○ TOS ● DiffServ

DiffServ

Traffic	Criticality	PHB group (DSCP)
real time	1: top	EF (101110)
real time	2: high	EF (101110)
real time	3: medium	EF (101110)
real time	4: low	EF (101110)
transactional	1: top	AF11 (001010)
transactional	2: high	AF12 (001100)
transactional	3: medium	AF21 (010010)
transactional	4: low	AF22 (010100)
background	1: top	BE (000000)
background	2: high	BE (000000)
background	3: medium	BE (000000)
background	4: low	BE (000000)

This window defines the coloring policies to apply to the Bridge WANs (you can create as many Coloring rules as you want). The coloring parameters specify the type of service (ToS) or DSCP values by traffic type and criticality level. They include:

- Name: to identify the coloring policy (string of characters). By default , the name 'none' is defined and is associated with an unspecified service type. The name is used to identify the Coloring policy.
- Service type: to select the type of coloring policy to set up. The service is selected from several options. The values offered are:
  - TOS: the TOS field of the frame is set to the value specified by the Code point setting. It then contains the value of the IP PRECEDENCE and the TOS specified for the Class of Service.
  - DiffServ: "Differentiated Service" type service. The TOS field of the frame is set to the value specified by the PHB Group (DSCP) setting, in accordance with RFC 2474 (definition of the Differentiated Services Fields (DS Field) in the IPv4 and IPv6 headers), RFC 2597 (Assured Forwarding PHB group), RFC 2598 (Express Forwarding PHB group).
  - unspecified: not specified
- a Coloring zone: to define or modify the coloring for type of Traffic and Criticality level:

  - PHB Group (DSCP): when DiffServ is the selected Service Type, the value for each peer (type of Traffic and criticality level) is selected from a drop-down list
  - Precedence/TOS (b0-b7): when ToS is the selected Service Type
- a display zone in the form of a table corresponding to the data previously entered.

3 Click **Apply** to validate your settings and then **Update** in the main Toolbar to refresh the configuration.

4 Refer to "Configuring the WAN(s)" to apply any defined Coloring Policies to the Bridge WAN interfaces of appliances configured in Bridge Mode or Bridge/Router Mode.

Configuration: DiffServ and TOS default settings

Type of traffic	Criticality level	Service type	PHB group	DSCP value	TOS value
Real time	Top	Express Forwarding	EF	101110	6
	High		EF	101110	6
	Medium		EF	101110	6
	Low		EF	101110	6
Transactional	Top	Assured Forwarding	AF11	001010	3
	High		AF12	001100	3
	Medium		AF21	001100	3
	Low		AF22	001100	3
Background	Top	Best Effort	BE	000000	0
	High		BE	000000	0
	Medium		BE	000000	0
	Low		BE	000000	0

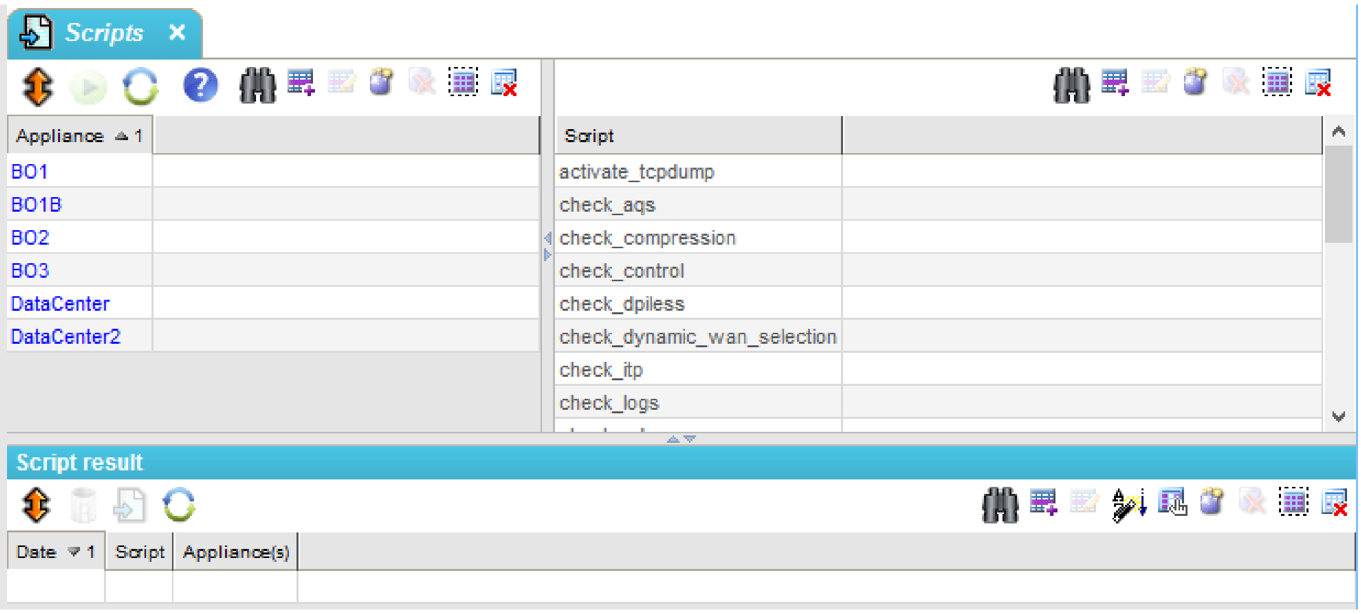
By default, coloring is set to 'none' and the Service Type to 'unspecified'.

The entered values should correspond to the Class of Service of the Operator.

Scripts

In the System provisioning toolbar, select Scripts.

The following window is displayed:



Appliance ▲ 1
BO1
BO1B
BO2
BO3
DataCenter
DataCenter2

Script
activate_tcpdump
check_aqs
check_compression
check_control
check_dpiless
check_dynamic_wan_selection
check_itp
check_logs

Date ▼ 1	Script	Appliance(s)

The window displays the following input fields:

- Appliance: list of all the Appliances for the Customer
- Script: list of the available scripts. These scripts are in the directory `~/ipboss/server/scripts`
- Command buttons:

  (Select all): selects all the Appliances

  (Launch): to launch the script on all the selected Appliances. A confirmation window is displayed: click OK. Depending on the number of selected Appliances, a message informs you that it may take a long time... .

  (Refresh): refreshes the view

  (Help): opens a contextual Help window

The Execution script result frame displays the scripts being launched, and allows downloading and deleting them:

- Result table fields:
  - Date: when the scripts were launched

  - Script: name of the scripts that were launched
  - Appliance(s): Appliances that ran the scripts
- Command buttons:

  (Select all): selects all the script results

  (Delete): deletes the selected script results (the data will be deleted from the server)

  (Download script result): allows downloading a zip file with the selected script results and other information (see below)

  (Refresh): refreshes the view

The zip file that can be downloaded is called `ExecutionScriptResult.zip` and has the following structure:

- root: one `<yymmdd-hhmm>` folder by selected script result, where `yymmdd-hhmm` are the date and time when the scripts were launched.

  The root folder has three subfolders, containing five files:

  - `ipboss`:

    `__active__.ipmconf`: current configuration at the Customer level

    `ip_boss_00<X>.log`: log file at the Customer level
  - `ipengines`:

    `<alias><ip|e's IP address>.ipmres`: script result in itself
  - `script`:

    `<script name>.ipmscp`: launched script (encrypted file)

    `ipengine.txt`: list of dumped Appliances (alias+@ip)

The user can send this zip file (by E-mail or FTP) to Extreme Networks Support.

Different script files are available. The main ones are :

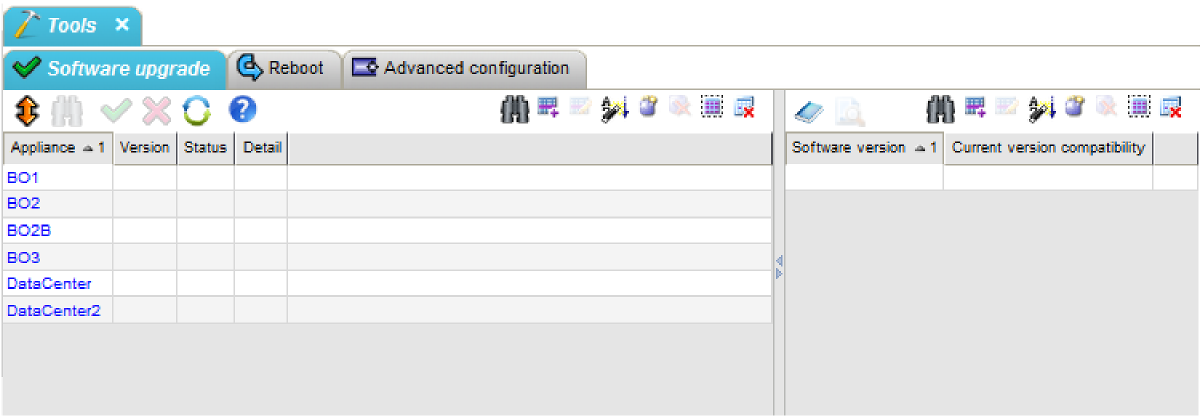
- default: dumps information from the Appliance,
- flows: dumps all the flows crossing the Appliance,
- check_visibility: dumps information about the Application Visibility agent,
- check_control: dumps information about the Application Control agent,
- check_compression: dumps information about the Compression agent,
- check_dynamic_wan_selection: dumps information about the Dynamic WAN Selection agent,
- check_itp: dumps information about the Time synchronization agent,

- check_sdwan: dumps information about the SD-WAN agent,
- restart_visibility: restarts the Application Visibility agent,
- restart_control: restarts the Application Control agent,
- restart_compression: restarts the Compression agent,
- restart_itp: restarts the Time synchronization agent,
- process: dumps information about the running processes.

Upgrading the appliances

In the System provisioning toolbar, select Tools and go to the **Software upgrade** tab.

The following window is displayed:



Appliance ▲ 1	Version	Status	Detail
BO1			
BO2			
BO2B			
BO3			
DataCenter			
DataCenter2			

Software version ▲ 1	Current version compatibility

This window is made of two frames:

- the list of appliances to be upgraded (left frame),
- the list of software versions (right frame).

The procedure is as follows:

1 When you select this tab for the first time, the list of configured appliances is displayed in the left frame. The Version column is not filled in. Select some appliances (or all of them with the Select All button) and click the Status button to see the actual software versions and statuses of the selected devices.

  The statuses can be:

  - upgraded: the appliance is up-to-date with the software release which is specified in the Version field,
  - download scheduled: the appliance will be upgraded,
  - install scheduled: the appliance is currently being upgraded,
  - error occurred: possible reason of failure:

    No Space left for file: no more space on the appliance to download the file,

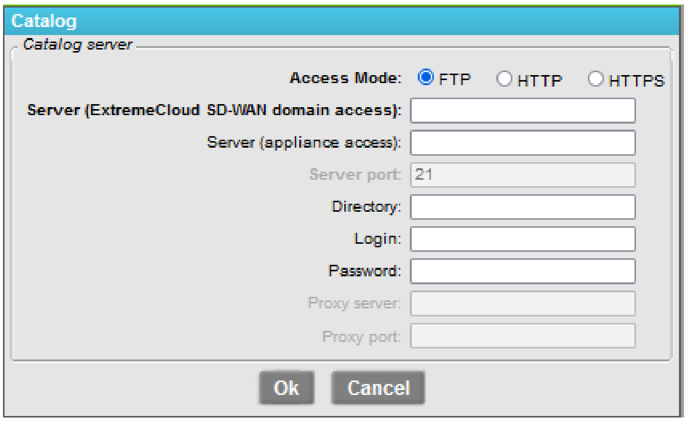
    Cannot connect to server (check address/routes): the FTP server is unreachable,

    Access to server denied (check login/password): there is a login/password problem on the FTP server,

    File not found: xxxxxxx: the file is not in the right directory on the FTP server or the directory is wrong, Error while downloading: the connection between the FTP server and the appliance is broken,

No disk space left for file: no more space to uncompress the software package.

2 In the right frame, click on the Get Catalog button



Catalog

Catalog server

Access Mode: ● FTP ○ HTTP ○ HTTPS

Server (ExtremeCloud SD-WAN domain access):

Server (appliance access):

Server port: 21

Directory:

Login:

Password:

Proxy server:

Proxy port:

The Catalog Server window contains the following parameters:

- **Access Mode**: three radio buttons enable you to choose between FTP, HTTP or HTTPS.
- **Server (ExtremeCloud SD-WAN domain access)**: host name or IP address of the server reachable by SD-WAN (which reads the appliance versions present on the server).
- Server (appliance access): host name or IP address of the server reachable by the appliances (they will download the new software version from that server). This server can be different from the previous one in case of NATting; if it is the same, you do not need to enter it again.
- Server port: allows changing the default port for HTTP (80 by default) and HTTPS (443 by default). For FTP, only the default port (21) can be used; in this case the field is greyed out.
- Directory: the server directory containing the software files.
- Login: user name to use to get the files.
- Password: user's password.
- Proxy server (for HTTP and HTTPS only): IP address of the proxy, if any.
- Proxy port (for HTTP and HTTPS only): port number of the proxy, if any.

The list of software versions on the server is displayed.

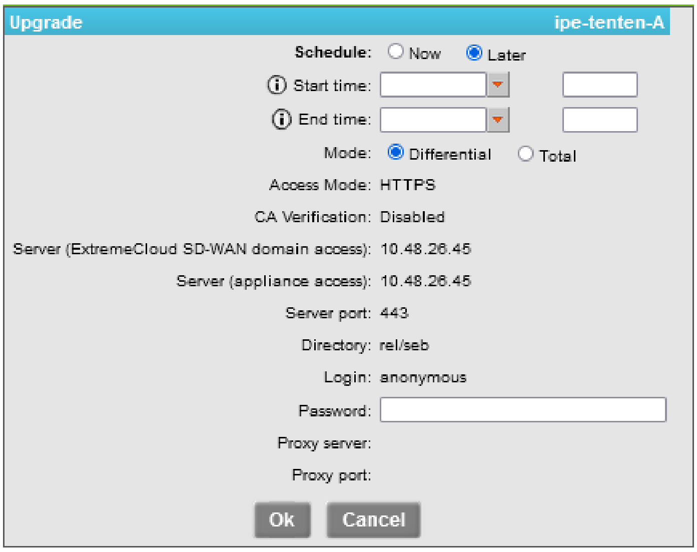
This table contains two columns:

- software version: list of the available software versions,

- Current version compatibility: shows the compatibility with the running version of Application Configuration software (compatible or not).

3 Select the appliances to be upgraded in the left frame and the software version in the right frame, then click the Upgrade button ✓.

4 The displayed scheduling window reminds you of the defined parameters and enables you to schedule the upgrade (during the night for example), or to launch it immediately by clicking Ok without specifying any date or time:



Upgrade ipe-tenten-A

Schedule: ○ Now ● Later

Start time:

End time:

Mode: ● Differential ○ Total

Access Mode: HTTPS

CA Verification: Disabled

Server (ExtremeCloud SD-WAN domain access): 10.48.26.45

Server (appliance access): 10.48.26.45

Server port: 443

Directory: rel/seb

Login: anonymous

Password:

Proxy server:

Proxy port:

This window contains the following fields:

- Start time: enter the start date and time of the upgrade (this must be a future date, not the current date). The Start time corresponds to the date when downloading from the FTP/HTTP/HTTPS server will start. The chronological sequence of downloads is managed automatically by the system.
- End time: enter the end date and time of the upgrade (this must be a future date, not the current date). The End time corresponds to the date when downloading will end and when the appliance will reboot for the new version to be applied.
- Mode:

  Differential: download only files necessary to upgrade the current version to the new version,

  Total: download all the files.
- Password: re-enter the password.

Click on Ok when done. The restart of appliances after upgrade is automatically performed at the date/time specified by the "End time" field.

If the Start time and End time fields are empty, the upgrade starts immediately on the selected Appliances.

A message confirms that the selected Appliances have received the upgrade order.

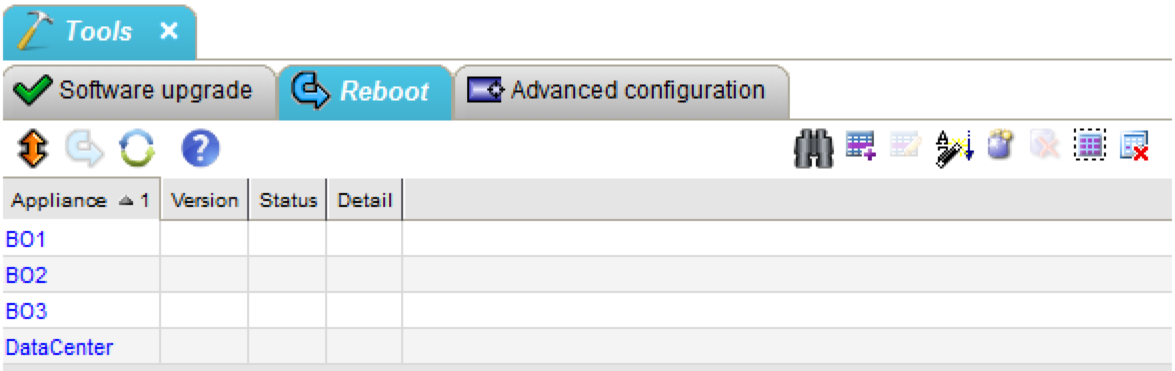
A Cancel button ✖ allows you to cancel the upgrade request. Canceling an upgrade is possible before or during the download of the software new version, but before the Appliance has started swapping.

5. Check that the upgrade has been completed correctly by selecting the appropriate Appliances and by clicking on the Status button 🔍.

Rebooting

In the System provisioning Toolbar, select Tools and hit the **Reboot** tab.

The Reboot window is displayed:



Appliance ▲ 1	Version	Status	Detail
B01			
B02			
B03			
DataCenter			

This window contains:

- the list of appliances,
- the following command buttons:

  (Select all): selects all the Appliances

  (Reboot): all the selected Appliances receive a reboot order

  (Refresh): refreshes the view

  (Help): opens the contextual Help window

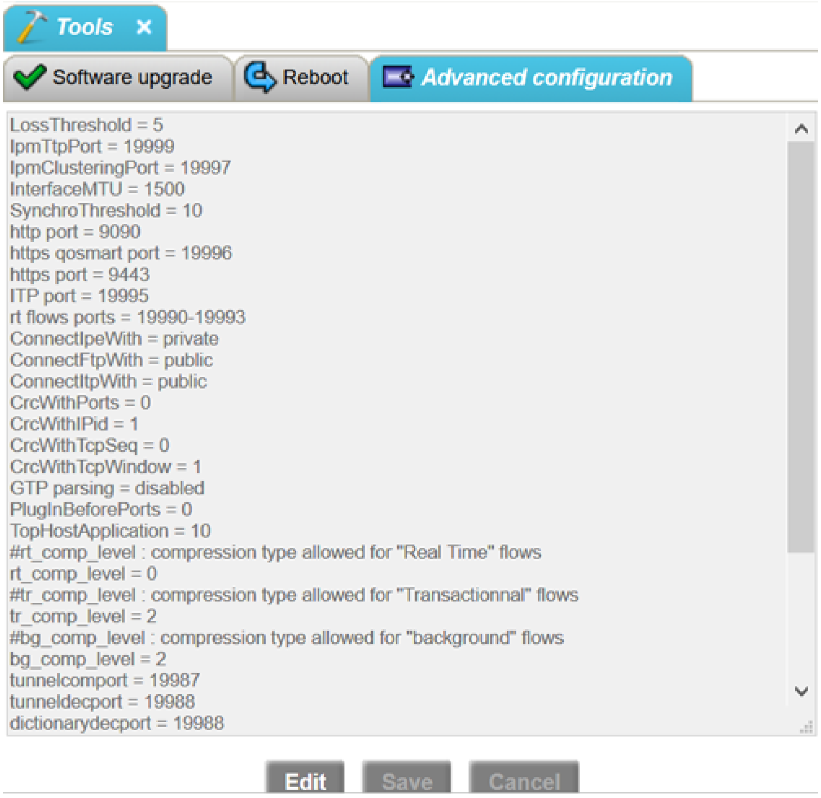
Configuring Advanced Settings

In the System provisioning Toolbar, select Tools, then the **Advanced configuration** tab.

Warning: This function is dedicated to Advanced Users. Always call Extreme Networks Support team.

The `[V5 sentry tuning]` section of the domain configuration file is displayed (`__active__.ipmcconf`).

If necessary, you may modify some parameters of this file.



```
LossThreshold = 5
IpmTtpPort = 19999
IpmClusteringPort = 19997
InterfaceMTU = 1500
SynchroThreshold = 10
http port = 9090
https qosmart port = 19996
https port = 9443
ITP port = 19995
rt flows ports = 19990-19993
ConnectIpeWith = private
ConnectFtpWith = public
ConnectItpWith = public
CrcWithPorts = 0
CrcWithIPid = 1
CrcWithTcpSeq = 0
CrcWithTcpWindow = 1
GTP parsing = disabled
PlugInBeforePorts = 0
TopHostApplication = 10
#rt_comp_level : compression type allowed for "Real Time" flows
rt_comp_level = 0
#tr_comp_level : compression type allowed for "Transactionnal" flows
tr_comp_level = 2
#bg_comp_level : compression type allowed for "background" flows
bg_comp_level = 2
tunnelcomport = 19987
tunneldecport = 19988
dictionarydecport = 19988
```

Application Provisioning

The Application Provisioning menu provides access to the following configuration functions:

- "Configuring User Subnets"
- "Configuring Applications"
- "Creating customized SaaS applications"
- "Configuring Application Groups (AGs)"
- "Configuring QoS Profiles"
- "Configuring Local Traffic Limiting"

Configuring User Subnets

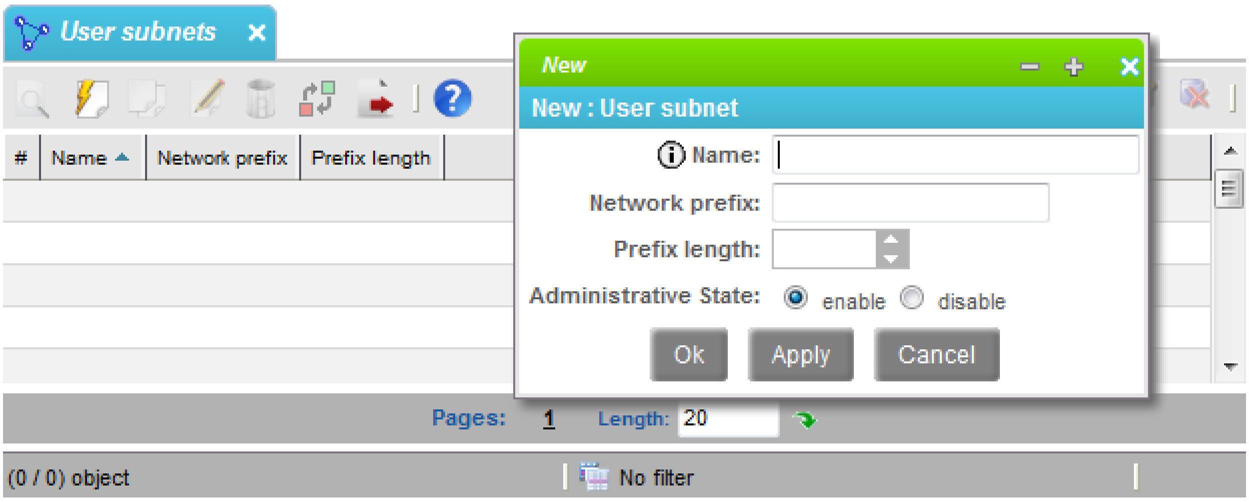
User Subnets can be used for Application Visibility and for Application Control, so as to identify specific hosts, servers or subnets on which measurement and control are required. They can be used as filters in the Applications and Application Groups.

Note: User subnets are optional. Only create them in case of specific subnets or hosts.

1 In the Application provisioning Toolbar, select **User subnets**.

The User subnets list window is displayed (it is empty by default).

2 By clicking on the New button, the creation window of a new User subnet is displayed.



It contains the following input fields and check boxes:

- Name: string of characters used to identify the user subnet
- Network prefix: user subnet prefix
- Prefix length: prefix length of the user subnet
- Administrative State:
  - Enable: the user subnet is taken into account
  - Disable: the user subnet is not taken into account

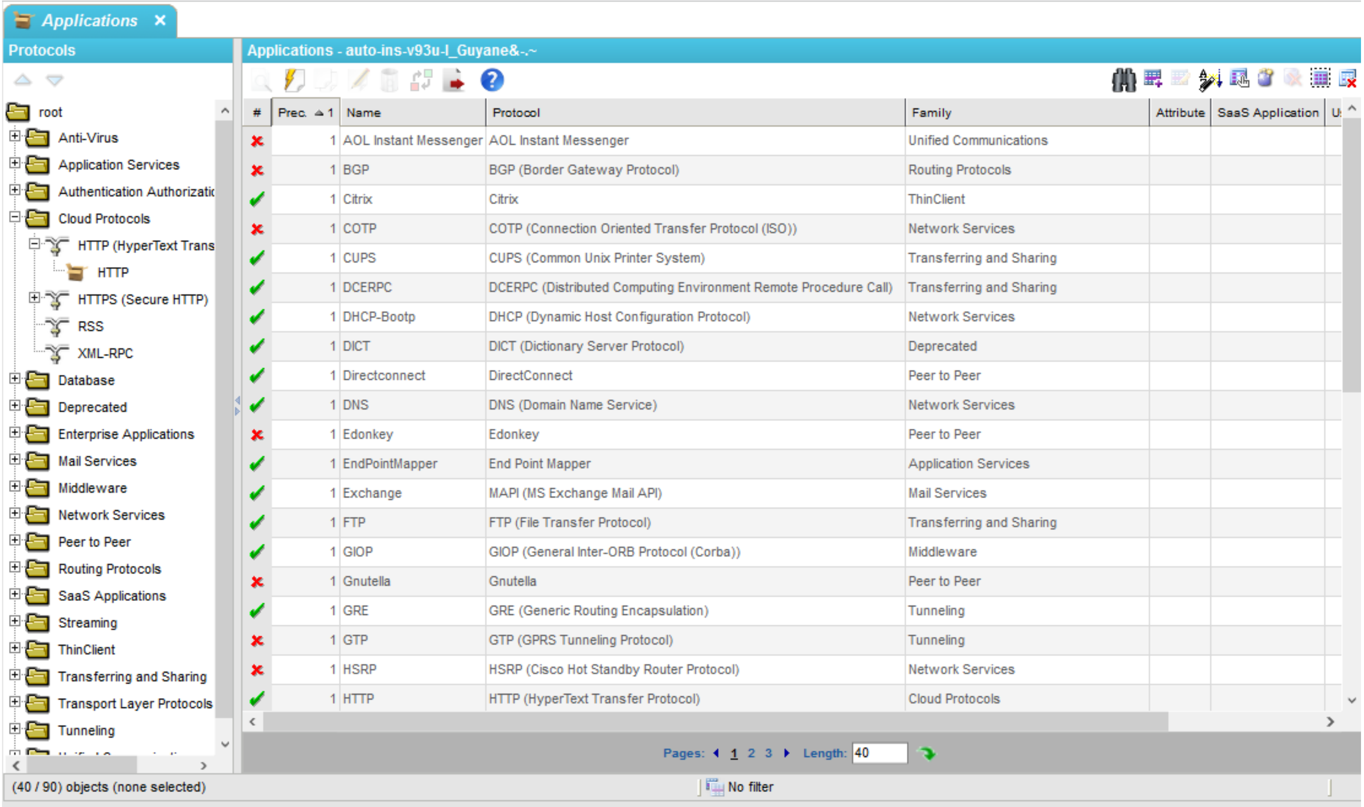
Configuring Applications

A default applications dictionary is available for each configuration. Applications can be added to, removed from or modified in this dictionary.

This dictionary is used by Application Visibility and Application Control functions.

1 In the Application provisioning Toolbar, select Applications.

The **Applications** window is displayed:



- root
  - Anti-Virus
  - Application Services
  - Authentication Authorizatic
  - Cloud Protocols
    - HTTP (HyperText Trans
      - HTTP
    - HTTPS (Secure HTTP)
    - RSS
    - XML-RPC
  - Database
  - Deprecated
  - Enterprise Applications
  - Mail Services
  - Middleware
  - Network Services
  - Peer to Peer
  - Routing Protocols
  - SaaS Applications
  - Streaming
  - ThinClient
  - Transferring and Sharing
  - Transport Layer Protocols
  - Tunneling

#	Prec.	Name	Protocol	Family	Attribute	SaaS Application	U
✗	1	AOL Instant Messenger	AOL Instant Messenger	Unified Communications			
✗	1	BGP	BGP (Border Gateway Protocol)	Routing Protocols			
✓	1	Citrix	Citrix	ThinClient			
✗	1	COTP	COTP (Connection Oriented Transfer Protocol (ISO))	Network Services			
✓	1	CUPS	CUPS (Common Unix Printer System)	Transferring and Sharing			
✓	1	DCERPC	DCERPC (Distributed Computing Environment Remote Procedure Call)	Transferring and Sharing			
✓	1	DHCP-Bootp	DHCP (Dynamic Host Configuration Protocol)	Network Services			
✓	1	DICT	DICT (Dictionary Server Protocol)	Deprecated			
✓	1	Directconnect	DirectConnect	Peer to Peer			
✓	1	DNS	DNS (Domain Name Service)	Network Services			
✗	1	Edonkey	Edonkey	Peer to Peer			
✓	1	EndPointMapper	End Point Mapper	Application Services			
✓	1	Exchange	MAPI (MS Exchange Mail API)	Mail Services			
✓	1	FTP	FTP (File Transfer Protocol)	Transferring and Sharing			
✓	1	GIOP	GIOP (General Inter-ORB Protocol (Corba))	Middleware			
✗	1	Gnutella	Gnutella	Peer to Peer			
✓	1	GRE	GRE (Generic Routing Encapsulation)	Tunneling			
✗	1	GTP	GTP (GPRS Tunneling Protocol)	Tunneling			
✗	1	HSRP	HSRP (Cisco Hot Standby Router Protocol)	Network Services			
✓	1	HTTP	HTTP (HyperText Transfer Protocol)	Cloud Protocols			

Pages: ◂ 1 2 3 ▸ Length: 40

(40 / 90) objects (none selected)

No filter

This window contains two frames:

- The recognized **Protocols** are displayed on the left, grouped by types,
- The **Applications** dictionary is displayed on the right. It lists the applications that are recognized.

Application Recognition

The ExtremeCloud SD-WAN System recognizes application flows using the opening negotiations of the client/server session conversation (SYN, SYN-ACK, ACK, i.e. layers 3 and 4 information), then it checks the syntax of the application (layer 7 information) thanks to a syntax engine to uniquely identify it without any possible error, regardless the ports being used; this also allows to classify particular applications (such as Codecs, published application names, peer-to-peer applications, URLs or URIs, etc.)

The SD-WAN Appliance engine uses DPI (deep packet inspection) to detect application signatures data patterns that uniquely identify a particular application. (Mechanisms such as this are also commonly used for virus recognition.) We are inspecting the start of the conversation (and only the start) to detect these patterns to classify the applications.

It is also possible to declare applications on the ports being used (you have defined an application as traffic on a specific port/server); in this case, it is the port number that prevails to regnosize the application.

When a SD-WAN Appliance has not observed this start of the conversation, or if the application cannot be recognized thanks to its syntax or declared port number, it falls back to RFC1700 ("well known ports" definition).

The order of recognition of applications is as follows:

1. Declared Port (you have defined an application as traffic on a specific port/server)
2. Syntax engine (the SD-WAN System uses its inbuilt application detection capabilities)
3. Well known port (RFC 1700)

Applications that are not recognized or enabled in the dictionary are implicitly grouped on their lower layer protocol (e.g. TCP or UDP).

Recognized applications, by type

Anti-Virus	AVG, Avira, Bitdefender, F-Secure, Kaspersky, McAfee, NOD32, Norton, Panda, TrendMicro
Application Services	End Point Mapper, Microsoft Office Groove, NSPI, Port Mapper, SrvLoc, SSDP
Authentication Authorization Accounting	Diameter, Identification Protocol, ISAKMP, Kerberos, LDAP, LDAPS, OCSP, RADIUS, YPPasswd, YPServ
Cloud Protocols	HTTP, HTTPS, RSS, XML-RPC
Database	DRDA, IBM-DB2, IBM Informix, MobiLink, MySQL, Oracle, Postgres,

	Sybase, TDS (= MS SQL)
Deprecated	Audiogalaxy, DICT, ICQ, Load Balancing, MCS, Napster, OpenFT, Quake
Enterprise Apps	SAP, Siebel
Mail Services	DIMP, IMAP, IMAPS, Lotus Notes, MAPI (MS Exchange), POP3, POP3S, SMTP, SMTPS
Middleware	GIOP, GIOPS, RPC, SOAP, TIBCO-RV
Network Services	COTP, DHCP, DNS, EIGRP, HSRP, ICMP, IGMP, NARP, Netbios, Netflow, NTP, RLP, RSVP, SNMP, Syslog, SVN, T38, VRRP
Peer to Peer	Applejuice, Ares, BitTorrent, DirectConnect, Edonkey, Filetopia, Foxy, GNUnet, Gnutella, GoBoogy, iMesh, Kazaa, KuGou, Manolito (MP2P), Mute, Pando, SopCast, Soulseek, WINMX, uTP (Torrent)
Routing Protocols	BGP, OSPF, PIM, RIP v1, RIP v2, RIPng
SaaS Applications	At the same location as the SaaS Dictionary, the complete list of recognized SaaS applications is available on Extreme Portal.
Streaming	BBC iPlayer, Flash, Icecast, Silverlight, Voddler
Thin Client	Citrix (possibility to recognize Citrix published applications), PC Anywhere, Radmin, RDP, Remote Shell, RFB (VNC), Rlogin, SSH, Telnet, TelnetS, TNVIP, VMWare, X.11
Transferring and Sharing	AIM Transfer, Altiris, CUPS, DCERPC, FTP, FTPS, IPP, JetDirect, LPR, Mainframe CFT, Microsoft ActiveSync, Mount, NFS, NLockMgr, RQuota, RStat, RSync, RUsers, SharePoint, SMB, Sync, TFTP, WINS, YPUpdate
Transport Layer Protocols	DTLS, IPComp, SCTP, SSL, TCP, UDP, WTP
Tunneling	EtherIP, GRE, GTP, GTPv2, HTTP tunnel, IPsec, L2TP, openVPN, PPP, PPTP, Socks, STUN, XoT
Unified Communications	Adobe Connect, AIM Express, AOL Instant Messenger, Cisco Unified MeetingPlace, Gizmo, H.225, H.245, IAX, IBM Lotus Sametime, iCall, IRC, IRCS, Jabber, MGCP, MMS, MPEG-TS, MS Communicator, MSN Messenger, NNTP, NNTPS, ooVoo, PalTalk, Q.931, RDT, RTMP, RTSP, RTP/RTCP (G.711a, G.711u, G.723, G.729), Secure AIM, SHOUTcast, SIP, Skinny Client Control Protocol, Skype, UCP, Webex, Yahoo Messenger. Dynamic Codecs (Audio and Video, such as H.264, Speex, etc., by inspection of SIP signalling), Voddler, BBC Player, Inter Asterisk eXchange

Creating new applications

The system recognizes about 200 protocols (HTTP, ICMP, FTP, RTP/RTCP, H.225, SAP, Citrix, Skype, VMware, SaaS....; refer to "Application Recognition".

New applications can be created, described by a protocol plus an attribute, possibly on certain subnets or hosts specifically.

> **Note:** Applications that are not recognized by appliances, and not explicitly named and enabled in the Application dictionary are implicitly grouped on the lower layer protocol (e.g. TCP or UDP).

By clicking on the New button , the creation window of a new application is displayed. It contains the following input fields:

- Name: character string used to identify the application
- Administrative State:
  - Enable: the application is taken into account
  - Disable: the application is not taken into account
- Protocol: select a protocol from the drop-down list
- Attribute: depends on the protocol; this field is enabled or not and provides access to a list or free fields
  - for TCP or UDP - Port(s): port numbers as they appear in the Server port fields of TCP/UDP headers (either source or destination). This field can contain several ports, separated by a ; or a range of ports, separated by a -.
  - for HTTP - URL (www.extremenetworks.com for example)

    Do not start the URL by http://.

    You can put a URL like *.extremenetworks.* (see below).

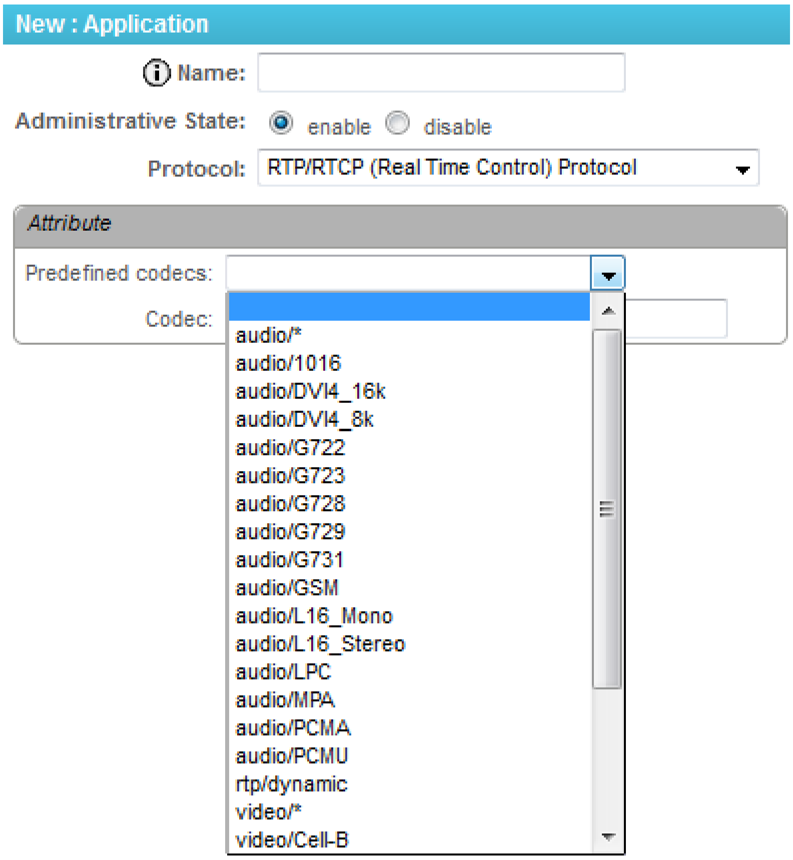
Syntax:

?	a unique character
*	any character string (included empty)
%	shortest word (non empty, separated by spaces)
$	longest word (non empty, separated by spaces)
;	separator in a list

Examples:

www.google.fr	any URL of the site
www.google.*	all google incarnations (.fr, .com, .de ....)
www.google.*/*.gif	all .gif documents in any page of any google
/.gif	all .gif documents in any page of any server
Specific cases:	
host/*	"any" URI
host/	empty URI
*/full/uri	"any" HOST
/full/uri	empty HOST

- for HTTPS - Common Name (usually the FQDN (Fully Qualified Domain Name) of the web site; it is displayed in the Certificate)
- for Citrix - Application(s): name of published applications (Word, Excel for example) when the applications are not multiplexed in the same TCP session
- for RTP/RTCP - Predefined codecs: name of an audio or video codec, to be selected from a drop-down list:



New : Application

Name:

Administrative State: ● enable ○ disable

Protocol: RTP/RTCP (Real Time Control) Protocol

Attribute

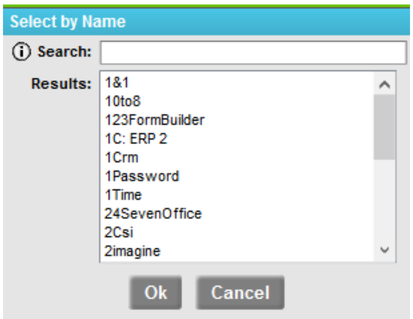
Predefined codecs:

Codec:

Codec: name of an audio or video codec, to be written with the following syntax: audio/<audio codec name> or video/<video codec name> (for instance, to create the speex codec, enter audio/speex).

To be able to recognize the dynamic codecs (as per RTP), SIP application recognition must be enabled for SIP signalling to be decoded.

- for SaaS, select a SaaS application from the SaaS dictionary:



Select by Name

Search:

Results:
1&1
10to8
123FormBuilder
1C: ERP 2
1Crm
1Password
1Time
24SevenOffice
2Csi
2imagine

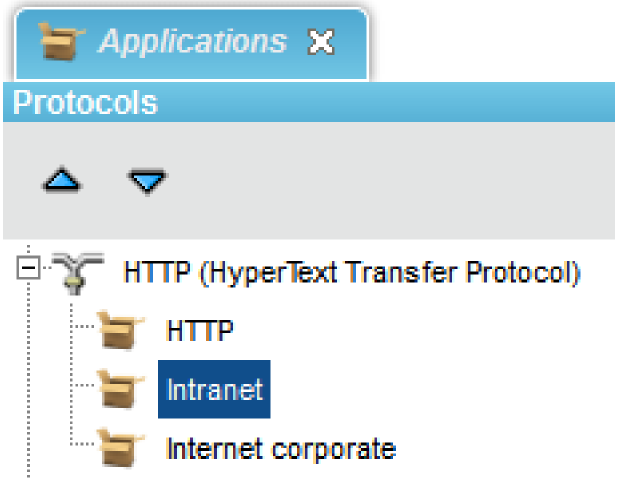
- For other protocols, no further information is required.

- User Subnets filter: this optional parameter can be used to identify an application by the IP address of a server or client, or list of servers or clients (up to 30). It is possible to choose the server or client from a drop-down list of the User subnets, or directly:
  - Prefix/Length: set the subnet with the following notation X.X.X.X/Y where X.X.X.X is the IP address and Y the length integer between 0 and 32; a list of IP addresses can be configured (; separator).
  - C/S Side: specify if the application must be recognized on the server side or on the client side (it is recognized on the Server side by default).

Order of recognition

When describing different applications using the same protocol (e.g. for HTTP: Intranet (= intranet.company.com), Internet corporate (= *.company.com) and Internet (= the rest of http)), place the **more specific applications first** (the Intranet, then Internet corporate in the example) and finally the generic one (the Internet), so that the specific ones can be recognized as such.

This ordering is achieved by selecting an application and by moving it up with the left blue arrow (move up) if it is more specific than the one above it, or moving it down with the right blue arrow (move down) if it is more generic than the one below it, and by repeating this for as many applications as necessary until they are all sorted from the most specific one (at the top) to the most generic one (at the bottom).



Applications
Protocols
HTTP (HyperText Transfer Protocol)
HTTP
Intranet
Internet corporate

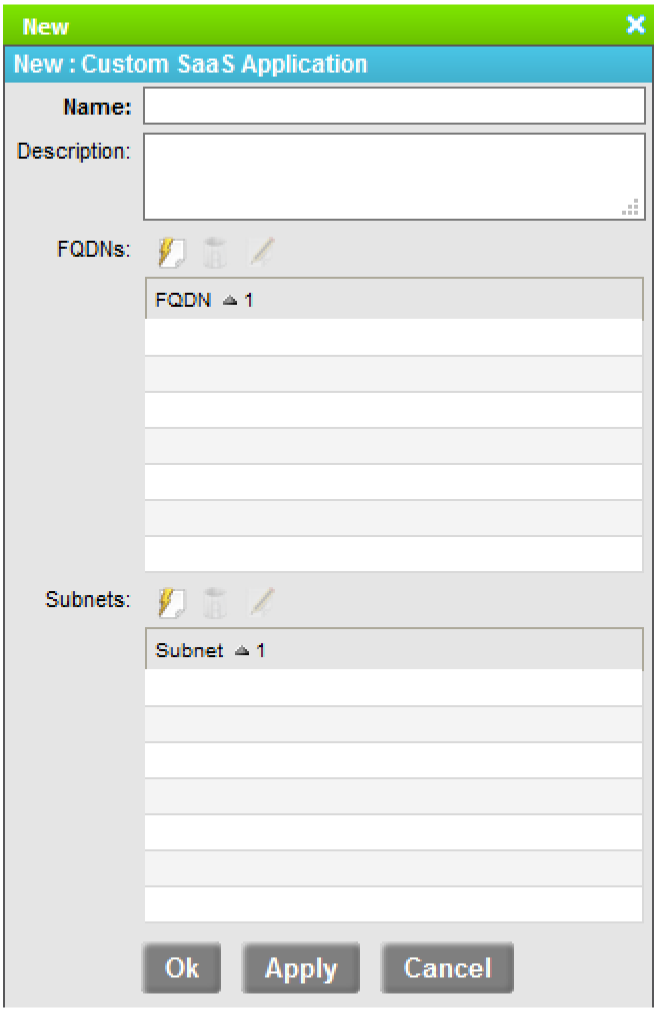
Creating customized SaaS applications

In addition to the SaaS dictionary, you may use a customized dictionary by creating your own SaaS applications.

This additional dictionary is defined per Customer.

1 In the Application provisioning Toolbar, select Custom Saas Applications:

2 By clicking on the New button in the **Custom SaaS Applications** window, the creation window is displayed:



3 Enter the Name of the SaaS application. In the case of a duplicate name, the system informs you that this name already exists in the SaaS dictionary and automatically renames your customized application.

4 You may enter a detailed description of the application.

You must declare the new SaaS application through either a FQDN or a subnet, or both of them.

5. Click ⚡ in the FQDNs panel and enter a Fully Qualified Domain Name according to the following format:
   - https://www.extremenetworks.com/products/ => FQDN is www.extremenetworks.com
   - https://www.google.com/analytics/ => FQDN is www.google-analytics.com

   With HTTP, the FQDN is extracted from the URL. With HTTPS, the Common Name is used.
6. You can also click ⚡ in the Subnets panel and specify a subnet for the new SaaS application (as for other applications).
7. Click **OK** and **Apply** to validate.

Configuring Application Groups (AGs)

Users specify high-level business objectives through Application Groups. The Customer traffic is classified using a mix of the user's applications and organization data. The Application Group attributes include:

- business criticality,
- QoS performance objectives (nominal bandwidth per application session, delay, jitter, packet loss, SRT, RTT and TCP retransmission),
- the enabling of compression.

The user's objectives are the only input to the system. There is no need to set low-level, network and device specific policy rules.

The Application Configuration system performs:

- the configuration of high-level QoS objectives
- Application Control in accordance with the AGs
- Compression in accordance with the AGs
- Dynamic WAN Selection for the flows in accordance with the AGs

Application Groups are independent of Application Visibility, Application Control, Compression and Dynamic WAN Selection.

Application Groups are given in a tree structure, each AG is characterized by:

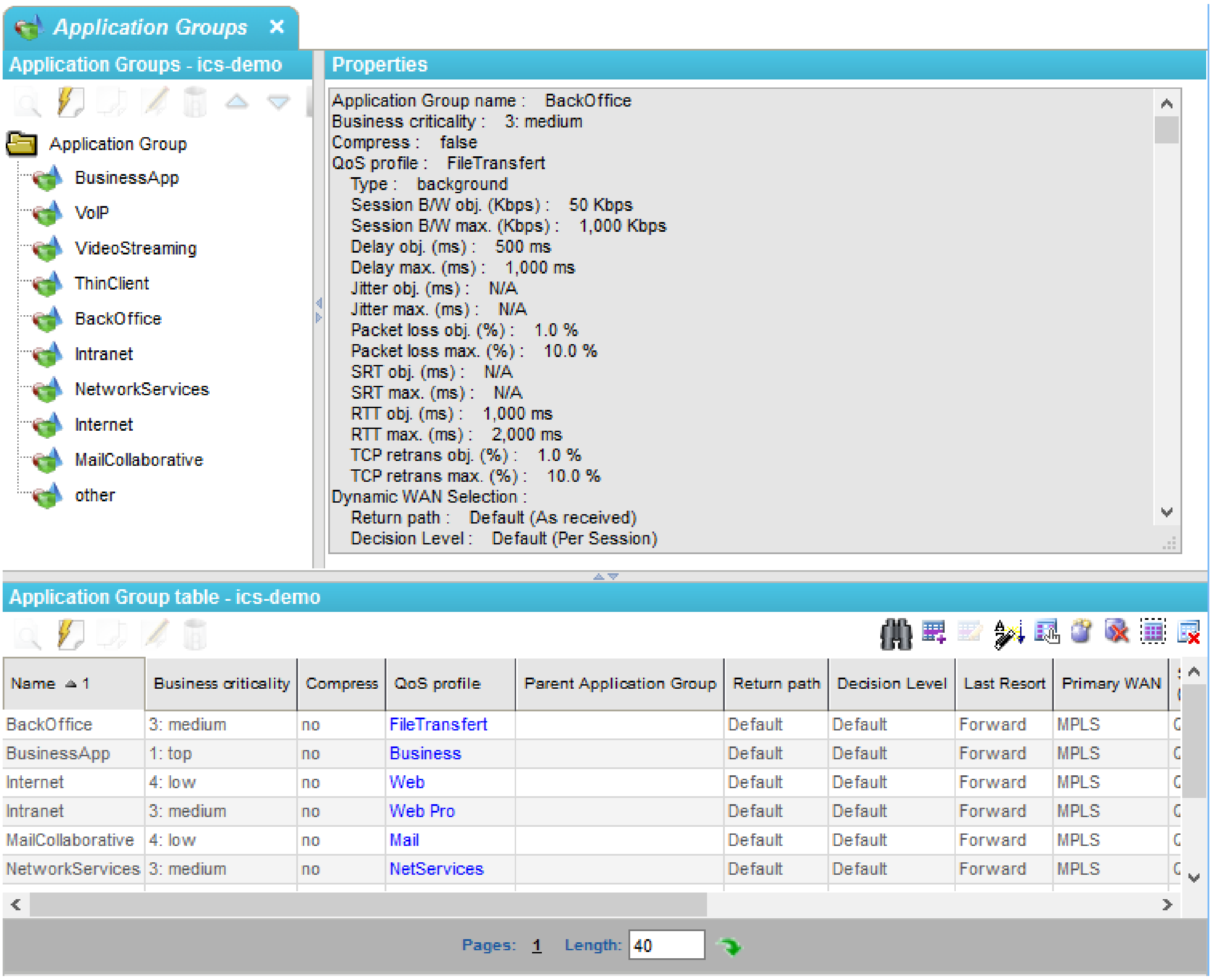
- a name,
- filters to define the rules of traffic classification corresponding to the AG,
- a criticality level associated with the application(s) in this AG,
- a QoS profile that enables QoS objectives for the application(s) in this AG,
- the capability to be compressed.

> **Warning:** The position of the Application Groups in the tree structure is important because it determines the classification of the packets. Classification is performed by running the structure tree downwards. Any packet is classified with the first applicable classification met. 'Other' is positioned at the bottom of the tree.

The configuration of the Application Groups is necessary for Application Control.

1 In the Application provisioning Toolbar, select Application Groups:

The Application Groups window is displayed:



Application Groups ✕
Application Groups - ics-demo
Properties
Application Group table - ics-demo

- Application Group
  - BusinessApp
  - VoIP
  - VideoStreaming
  - ThinClient
  - BackOffice
  - Intranet
  - NetworkServices
  - Internet
  - MailCollaborative
  - other

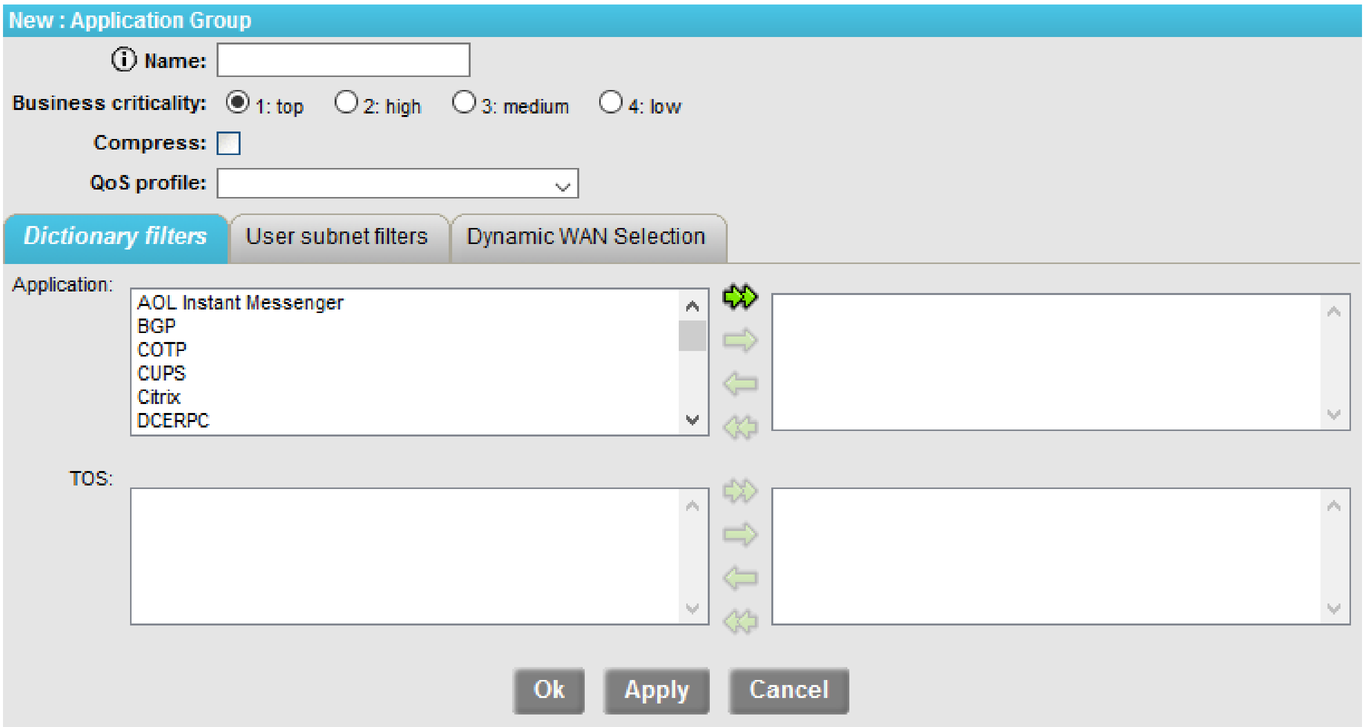
```
Application Group name :   BackOffice
Business criticality :   3: medium
Compress :   false
QoS profile :   FileTransfert
   Type :   background
   Session B/W obj. (Kbps) :   50 Kbps
   Session B/W max. (Kbps) :   1,000 Kbps
   Delay obj. (ms) :   500 ms
   Delay max. (ms) :   1,000 ms
   Jitter obj. (ms) :   N/A
   Jitter max. (ms) :   N/A
   Packet loss obj. (%) :   1.0 %
   Packet loss max. (%) :   10.0 %
   SRT obj. (ms) :   N/A
   SRT max. (ms) :   N/A
   RTT obj. (ms) :   1,000 ms
   RTT max. (ms) :   2,000 ms
   TCP retrans obj. (%) :   1.0 %
   TCP retrans max. (%) :   10.0 %
Dynamic WAN Selection :
   Return path :   Default (As received)
   Decision Level :   Default (Per Session)
```

Name ▲ 1	Business criticality	Compress	QoS profile	Parent Application Group	Return path	Decision Level	Last Resort	Primary WAN
BackOffice	3: medium	no	FileTransfert		Default	Default	Forward	MPLS
BusinessApp	1: top	no	Business		Default	Default	Forward	MPLS
Internet	4: low	no	Web		Default	Default	Forward	MPLS
Intranet	3: medium	no	Web Pro		Default	Default	Forward	MPLS
MailCollaborative	4: low	no	Mail		Default	Default	Forward	MPLS
NetworkServices	3: medium	no	NetServices		Default	Default	Forward	MPLS

This window contains:

- An Application Groups zone which shows the tree of AGs,
- A Properties zone which shows the configuration of the selected AG,
- An Application Group table which summarizes all the AGs.

2 Click on the New icon to open the AG creation window:



New : Application Group

Name:

Business criticality: ● 1: top ○ 2: high ○ 3: medium ○ 4: low

Compress: □

QoS profile:

Dictionary filters | User subnet filters | Dynamic WAN Selection

Application:

AOL Instant Messenger
BGP
COTP
CUPS
Citrix
DCERPC

TOS:

This window contains:

- A zone displaying the characteristics of the selected Application Group:
  - Name of the AG,
  - Business criticality: top, high, medium or low,
  - Compress: the compression capability for the flows belonging to the AG,
  - QoS profile: the QoS profile that will apply to this AG (the QoS profile contains the Type of traffic, the Bandwidth objective and maximum values, the D/J/L, RTT, SRT and TCP retransmit objective and maximum values),
  - Sensitivity, Routine or Business: when the sites are connected through various networks (e.g. MPLS and Internet), or use various Network Access Points to the same network, the Sensitivity is used in the path decision to route traffic to a WAN access with at least the same Trust Level (defined on the WAN accesses). Dynamic WAN Selection must be activated in the license.
- A zone with four tabs, to define filtering rules for traffic classification in the corresponding AG:
  - Dictionary filters
  - User subnet filters
  - Dynamic WAN Selection

In this zone, the selection zones depend on the selected tab (see below).

- the left zone shows a list of elements of the Dictionaries (Applications, ToS values), User subnets (source and destination)
- the right zone shows the selected filters for the AG

3 Select elements (you can select several elements simultaneously, using the SHIFT or CTRL keys) and move them from one zone to the other thanks to the simple arrows, or move all the elements at a time using the double arrows.

> **Note:** A logical Or is applied for the different elements inside a filter (for example filter Applications: HTTP ***or*** HTTPS).

> **Note:** A logical And is applied for the different types of filters (for example Applications: HTTP ***or*** HTTPS ***and*** subnet-src=LAN-192).

Dictionary filters tab

This tab contains two filters:

- Application
- TOS

This is the main tab to use. Others are optional and lead to the creation of local rules, so use them with care.

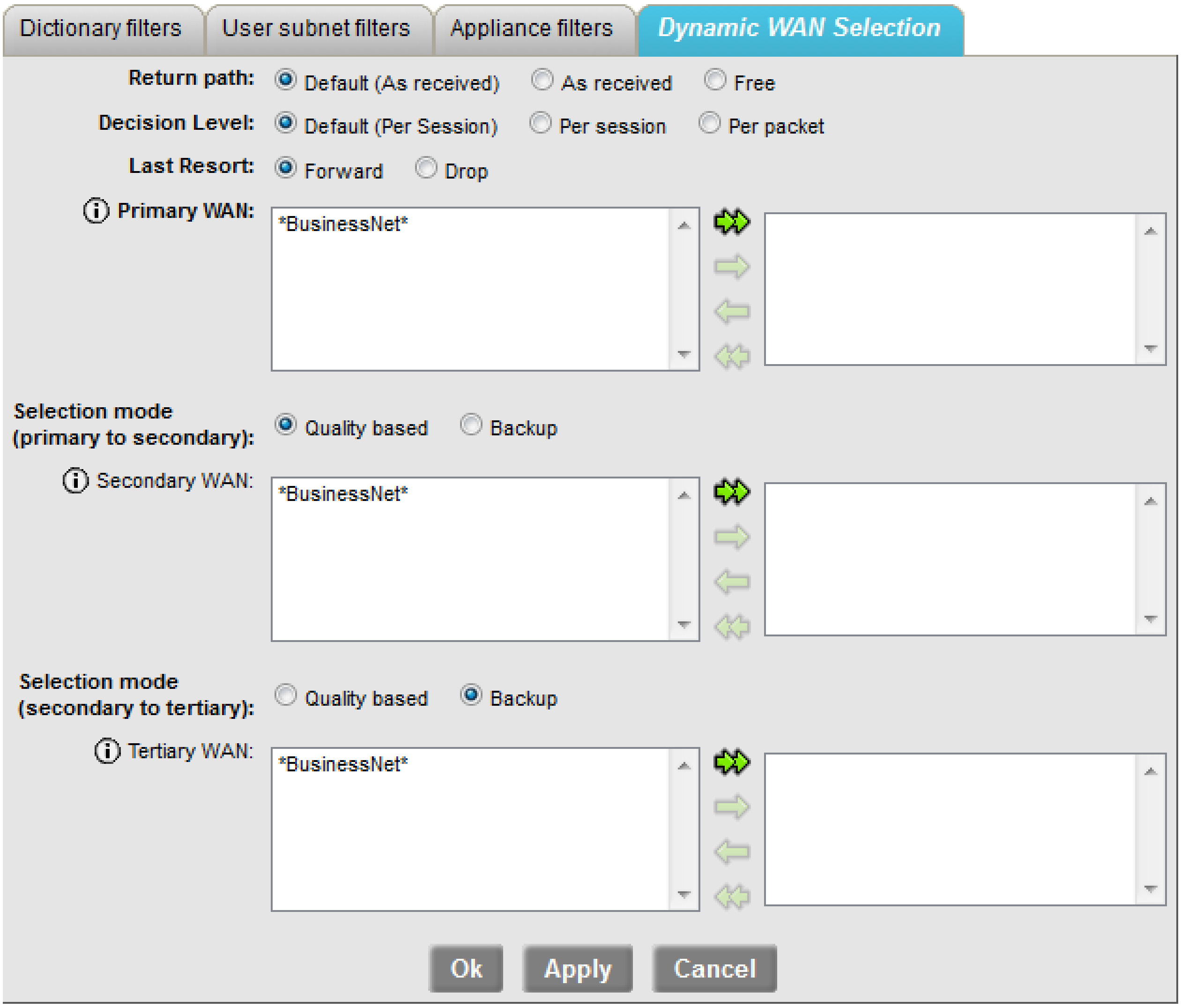
User Subnet filters tab

This tab contains two filters:

- Sources: User subnets directory to be used as sources
- Destinations: User subnets directory to be used as destinations

> **Warning:** By selecting Subnets with this tab, you create local rules that will apply only to those Subnets! Do this only if really needed. Otherwise, use global parameters only (Dictionary filters).

Dynamic WAN Selection tab



Return path: ● Default (As received) ○ As received ○ Free

Decision Level: ● Default (Per Session) ○ Per session ○ Per packet

Last Resort: ● Forward ○ Drop

Primary WAN: *BusinessNet*

Selection mode (primary to secondary): ● Quality based ○ Backup

Secondary WAN: *BusinessNet*

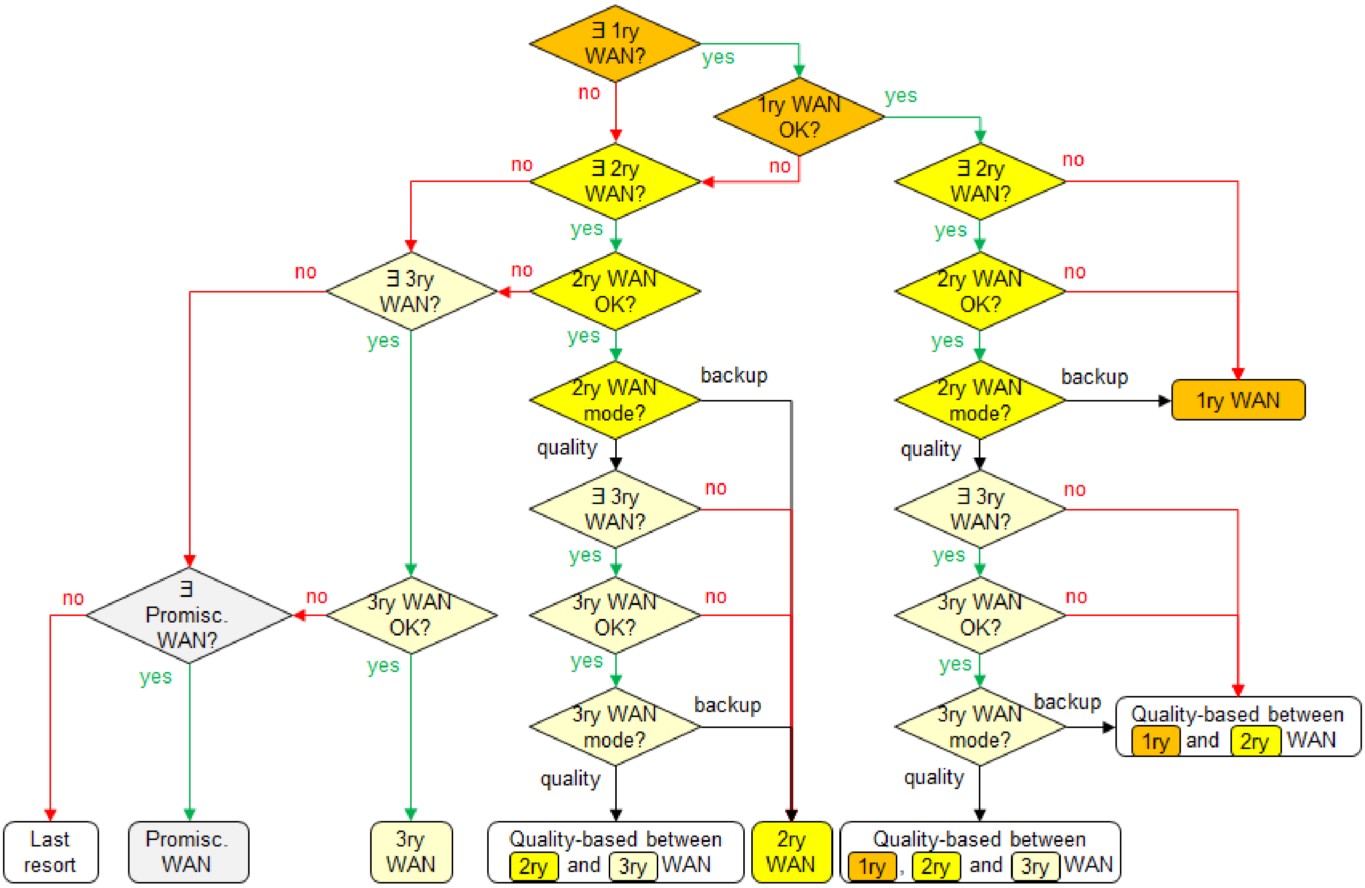
Selection mode (secondary to tertiary): ○ Quality based ● Backup

Tertiary WAN: *BusinessNet*

This tab contains Dynamic WAN Selection parameters.

- The first two parameters, **Return path** and **Decision Level**, are also present in the System provisioning > Tools > Advanced configuration menu (refer to "Configuring Advanced Settings").
  - They will take the global values selected there if set to "Default" here (the global values are indicated into brackets).
  - The global values can be overwritten by selecting different values here.
- **Last Resort**: if no decision is made (no "good" WAN Access to be selected), traffic is:
  - either sent on “NAP 0” (Forward)
  - or dropped.
- **Primary WAN**: specify the favorite WAN for this Application Group by selecting it in the left frame and pushing it to the right with the single right arrow. If several WANs are selected, then load balancing will be applied between them.

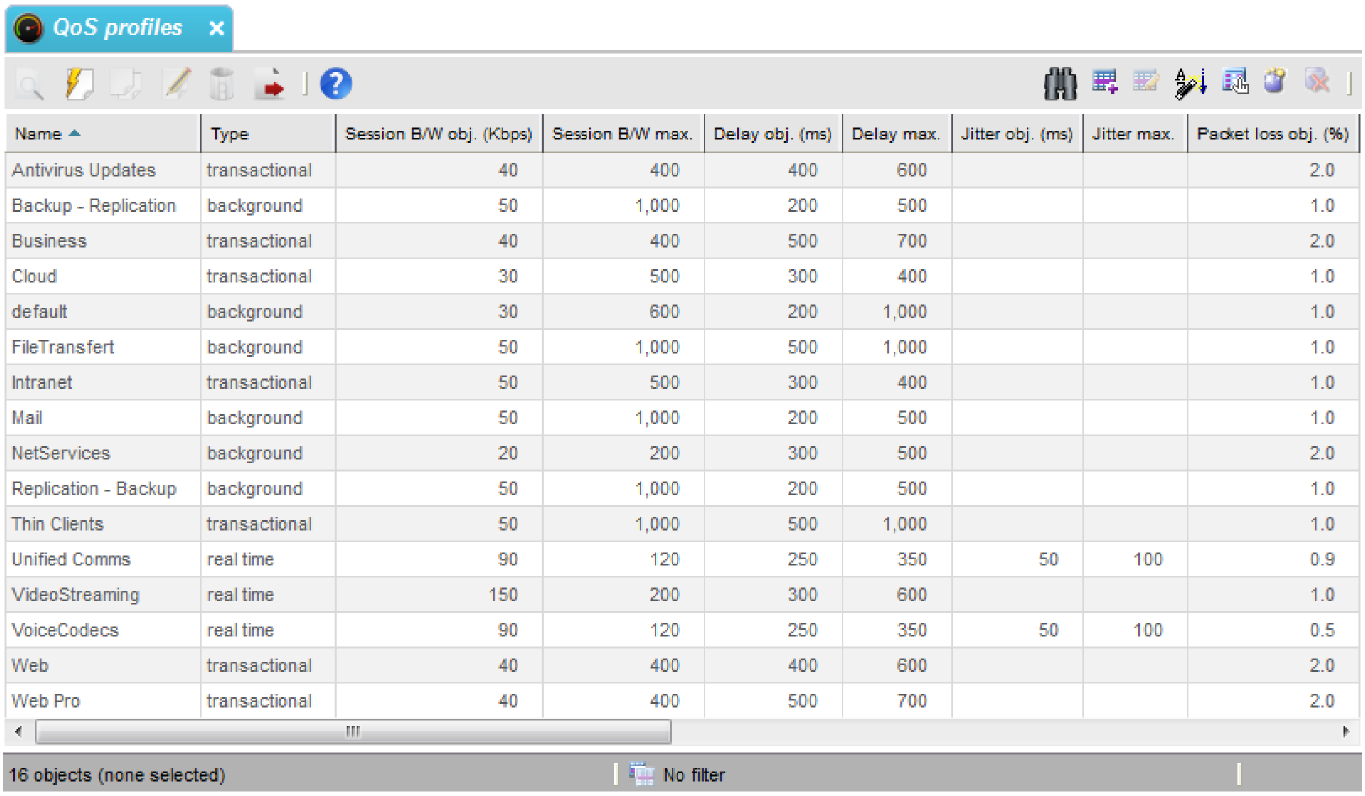
- **Selection mode (primary to secondary)**:
  - Quality based (default): the Secondary WAN can be selected instead of the Primary WAN (if the Primary WAN is broken), or if the quality of this Application Group is better on the Secondary WAN than on the Primary WAN,
  - Backup: the Secondary WAN can be selected instead of the Primary WAN if this one is broken, and only in that case.
- **Secondary WAN**: specify the second favorite WAN for this Application Group by selecting it in the left frame and pushing it to the right with the single right arrow. If several WANs are selected, then load balancing will be applied between them.
- **Selection mode (secondary to tertiary)**:
  - Quality based (default): the Tertiary WAN can be selected instead of the Secondary WAN if it is broken, or if the quality of this Application Group is better on the Tertiary WAN than on the Secondary WAN,
  - Backup: the Tertiary WAN can be selected instead of the Secondary WAN if this one is broken, and only in that case. The decision diagram below summarizes the whole mechanism (where 1ry stands for Primary, 2ry stands for Secondary, 3ry stands for Tertiary, Promisc. stands for Promiscuous [a WAN Access that has no WAN specified is considered to be attached to an internal WAN called “Promiscuous”] and ∃ ...? stands for "Does ... exist?" - or "Is there a ... available?").
- **Tertiary WAN**: specify the last acceptable WAN for this Application Group by selecting it in the left frame and pushing it to the right with the single right arrow. If several WANs are selected, then load balancing will be applied between them.



Note: there can be several Primary, several Secondary and several Tertiary WANs, but a given WAN cannot be both Primary and Secondary. For instance, if the decision is “Primary WAN”, and if two of them are defined, then the final decision is load- and quality-based between the two WANs.

Configuring QoS Profiles

1 In the Application provisioning Toolbar, select QoS profiles:



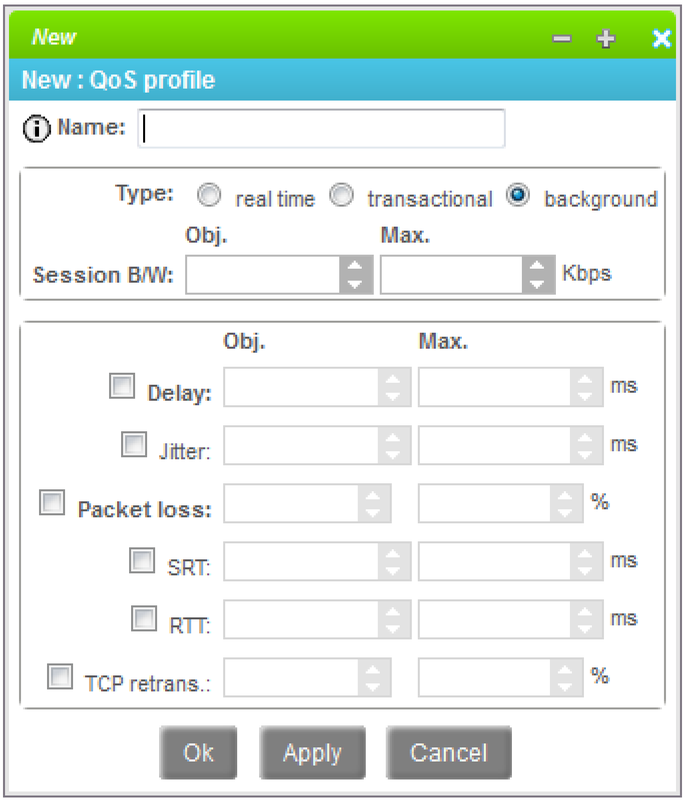
Name	Type	Session B/W obj. (Kbps)	Session B/W max.	Delay obj. (ms)	Delay max.	Jitter obj. (ms)	Jitter max.	Packet loss obj. (%)
Antivirus Updates	transactional	40	400	400	600			2.0
Backup - Replication	background	50	1,000	200	500			1.0
Business	transactional	40	400	500	700			2.0
Cloud	transactional	30	500	300	400			1.0
default	background	30	600	200	1,000			1.0
FileTransfert	background	50	1,000	500	1,000			1.0
Intranet	transactional	50	500	300	400			1.0
Mail	background	50	1,000	200	500			1.0
NetServices	background	20	200	300	500			2.0
Replication - Backup	background	50	1,000	200	500			1.0
Thin Clients	transactional	50	1,000	500	1,000			1.0
Unified Comms	real time	90	120	250	350	50	100	0.9
VideoStreaming	real time	150	200	300	600			1.0
VoiceCodecs	real time	90	120	250	350	50	100	0.5
Web	transactional	40	400	400	600			2.0
Web Pro	transactional	40	400	500	700			2.0

16 objects (none selected)

No filter

The settings made in this window enable you to define the QoS objectives. A QoS objective associated with an Application Group is used by the system to measure and control the traffic according to the application requirements.

2 Hit the New icon to display the QoS Profile creation window.



New

New : QoS profile

Name:

Type: ○ real time ○ transactional ● background

This window contains the following input fields:

- Name: to identify the QoS profile (character string),
- Type: to characterize application flow type:
  - real-time: real-time flow (VoIP, video) sensible to delay, jitter and loss,
  - transactional: transactional flow (SAP, Telnet), sensible to delay,
  - background: different from those listed above,
- Session B/W (kbps): to specify the bandwidth per session; the value is used by Application Control,
  - Obj. (objective): nominal bandwidth per session (mandatory parameter).

    The objective bandwidth per session is operational during congestion.
  - Max. (maximum): maximum bandwidth allowed per session (not mandatory).

    If it is not defined, a value of 500 times the Objective is applied.

    Most of the time, the limit remains the WAN access so that you rarely can experience this parameter. It can only be observed when the customer declares a low objective (e.g. 20 kbps) and the WAN access is large with low activity (e.g. 100 Mbps available), and there are only a few sessions (based on that QoS Profile) running at that moment.

    If it is defined, it always applies when Application Control is enabled (i.e., even when there is no congestion and when Application Control does not control the bandwidth).

- Delay (ms), Jitter (ms), Packet loss (%), SRT (server response time, ms), RTT (round trip time, ms), TCP retrans. (%): to specify, for each flow, the Objective and Maximum values for that QoS profile. You enable these parameters by checking their boxes.

Configuring Local Traffic Limiting

Local Traffic Limiting allows traffic limiting rules to be configured for each site, when this is necessary. These rules take the enterprise organization, user subnets and applications implemented between these different entities into account. They are used by Application Control.

These rules are defined for outgoing (LTL Ingress) or incoming (LTL Egress) traffic on the selected site.

LTLs are used to limit the bandwidth used by the different networks of the departments, services (user subnets) or applications according to specific criteria taking the following constraints into account:

- source subnet,
- remote subnet,
- applications,
- TOS/CP values.

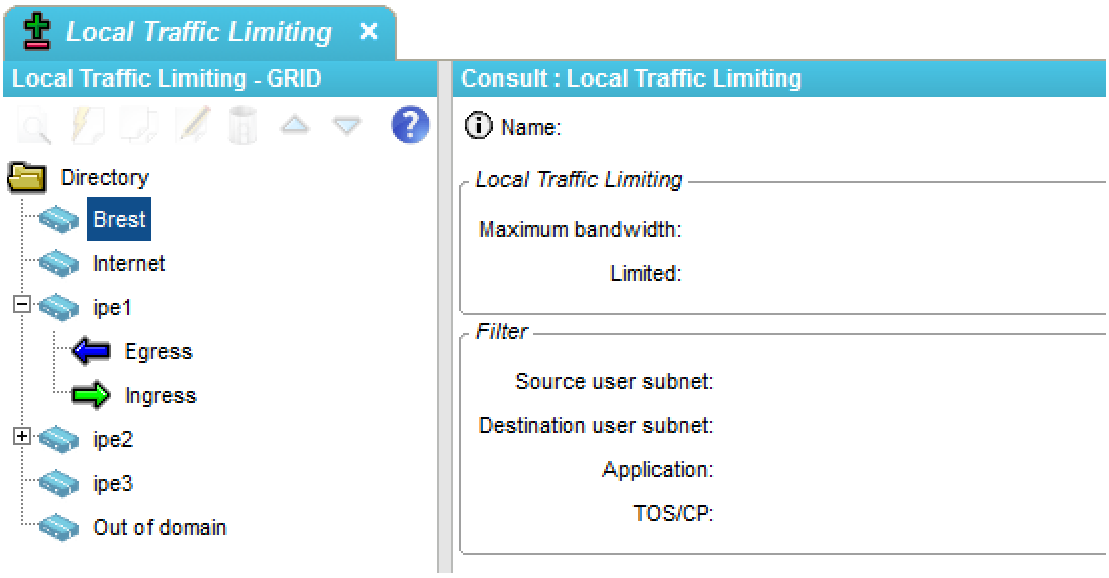
Traffic Limiting is given in a tree structure, each LTL is characterized by:

- a name
- filters to define the rules for classifying the traffic that corresponds to the LTL
- a limit on the bandwidth that can be used by the class

> **Note:** LTL rules are enabled if and only if Application Control is activated on the Appliance.

1 In the Application provisioning Toolbar, select Local Traffic Limiting.

The Local Traffic Limiting Tree window is displayed.



Name:

Local Traffic Limiting

Maximum bandwidth:

Limited:

Filter

Source user subnet:

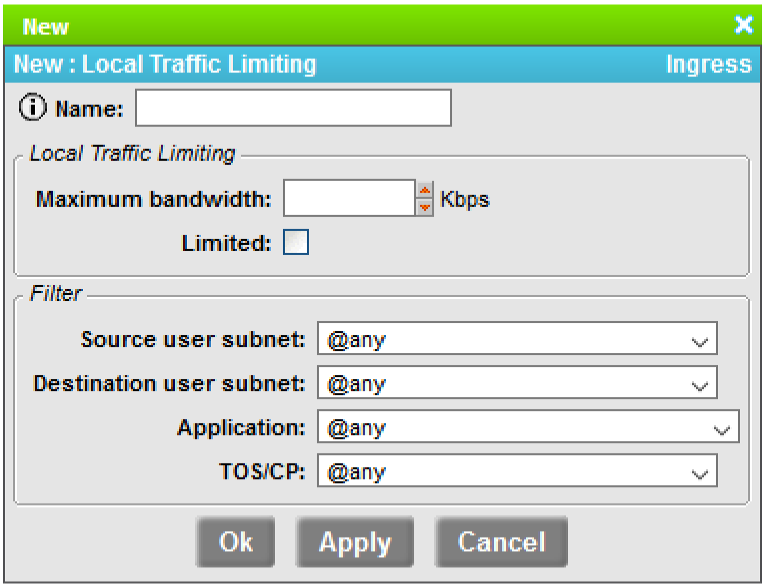
Destination user subnet:

Application:

TOS/CP:

This window contains a Local Traffic Limiting tree structure per Appliance.

2 To create a new policy, select the Appliance and the direction (ingress or egress). Then click the New icon to display the following window:



Name:

Local Traffic Limiting

Maximum bandwidth: Kbps

Limited: □

Filter

Source user subnet: @any

Destination user subnet: @any

Application: @any

TOS/CP: @any

This window contains the following parameters:

- Name: Name of the LTL policy,

Local Traffic Limiting

- Maximum bandwidth (kbps): to specify the limit bandwidth for a LTL. If the value 0 is specified, all the traffic is dropped.
- Limited: to enable or disable the limiting rule.

Filters

You may filter the traffic related to a LTL. The available options are:

- Source user subnet: to filter the traffic by Source User subnet. Select it from a drop-down list that corresponds to the "User subnets" directory,
- Destination user subnet: to filter the traffic by Destination User subnet. Select it from a drop-down list that corresponds to the "User subnets" directory,
- Application: to filter the traffic by application. Select it from a drop-down list that corresponds to the "Applications" dictionary,
- TOS/CP: to filter the traffic by TOS value. Select this value from a drop-down list that corresponds to the "TOS/CP" dictionary.

SSL Optimization

This section addresses the following topics:

- "SSL Optimization overview"
- "Connection"
- "Configuring trusted proxy CA credentials"
- "Selecting SSL proxy enabled Sites and SSL Servers"
- "Customizing the SSL Proxy Certificate Trust Store"

SSL Optimization overview

The SSL feature is actually an enabler for applying any SD-WAN optimization service to the SSL encrypted flows (mainly Compression).

Deployment

SSL Optimization can apply wherever there are Compression-capable appliances deployed on the flows path, on both sides of the WAN (branch-side and datacenter-side).

Applications

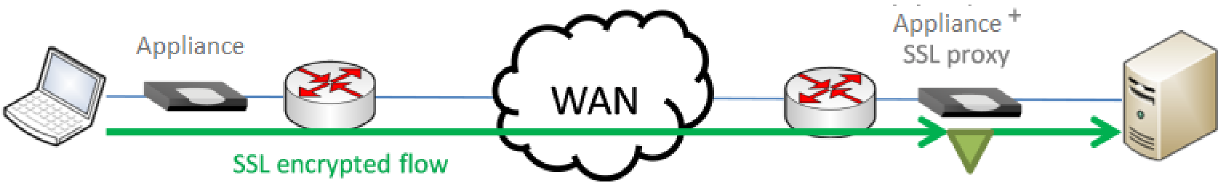
SSL Optimization applies to any application over SSL. This includes (but is not limited to):

- 443 HTTPS (HTTP over SSL),
- 636 LDAPS (LDAP over SSL),
- 992 TelnetS (Telnet over SSL),
- 993 IMAPS (IMAP over SSL),
- 994 IRCS (IRC over SSL),
- 995 POP3S (POP3 over SSL),
- 5061 SIPS (SIP over SSL).

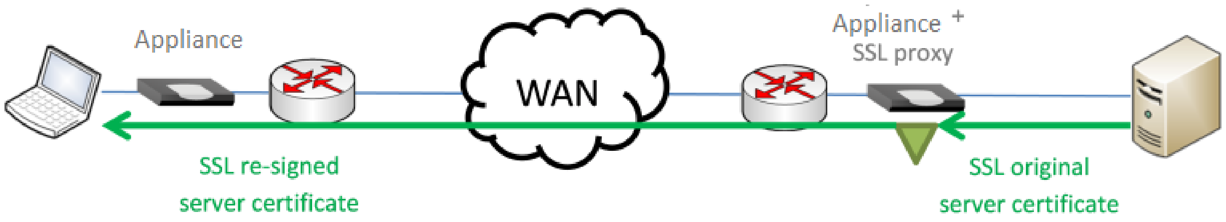
SSL Optimization does ***not*** apply to applications that are not over SSL (whatever is over IPsec, encrypted MAPI, encrypted SMBv2, SSH).

Principles

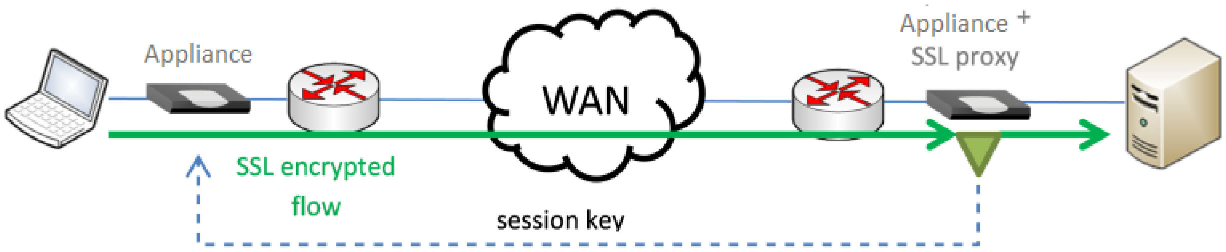
The datacenter-side Appliance acts as a SSL proxy and intercepts the SSL handshake between the client and the server.



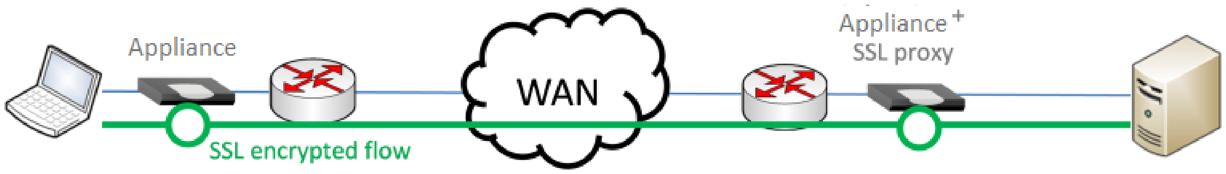
The SSL proxy re-signs server certificates on the fly, using a proxy CA certificate that is provided by the end-user company IT. Therefore, it is not the original certificate that the client application (e.g. HTTPS browser) presents, but rather a clone of this certificate, issued by the SSL proxy and signed with the proxy CA certificate.



Once the security parameters are negotiated on both sides of the proxy connection (client-to-proxy and proxy-to-server), the session keys are sent over a secure encrypted tunnel to the branch-side Appliance.



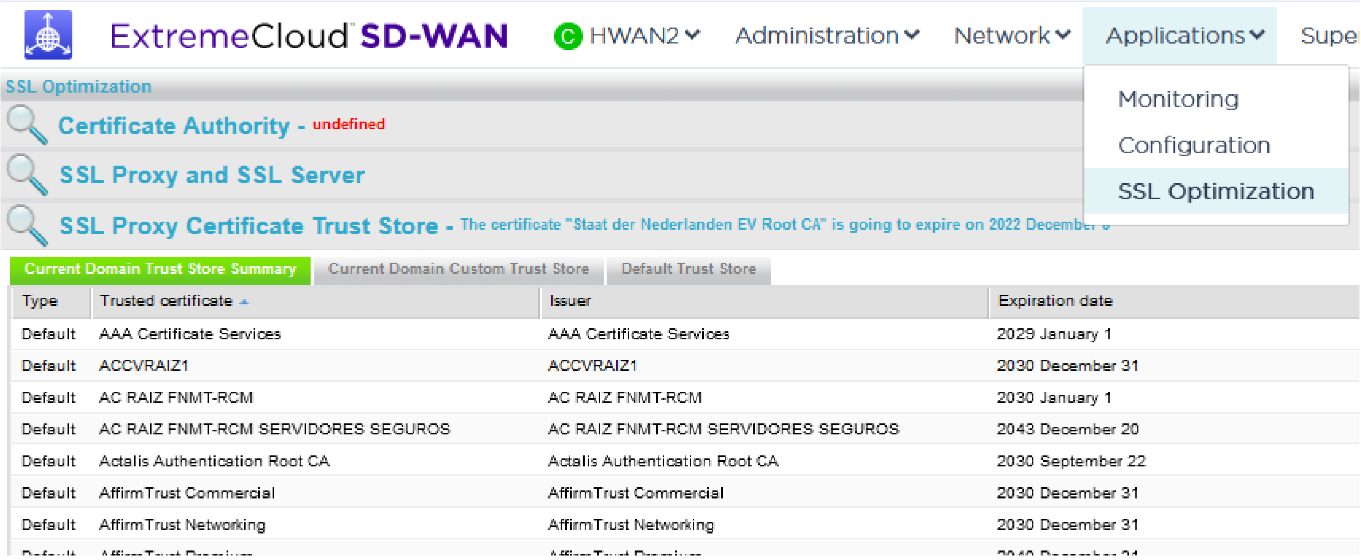
Then both Appliances can decrypt and re-encrypt the flows, hence enabling any optimization service to work on the decrypted traffic.



Connection

From the SD-WAN Orchestrator main menu, select **Applications -> SSL Optimization**.

Enabling SSL optimization requires a simple three-step configuration process on the SSL Optimization page.



Certificate Authority - undefined

SSL Proxy and SSL Server

SSL Proxy Certificate Trust Store - The certificate "Staat der Nederlanden EV Root CA" is going to expire on 2022 December

Current Domain Trust Store Summary
Current Domain Custom Trust Store
Default Trust Store

Type	Trusted certificate	Issuer	Expiration date
Default	AAA Certificate Services	AAA Certificate Services	2029 January 1
Default	ACCVRAIZ1	ACCVRAIZ1	2030 December 31
Default	AC RAIZ FNMT-RCM	AC RAIZ FNMT-RCM	2030 January 1
Default	AC RAIZ FNMT-RCM SERVIDORES SEGUROS	AC RAIZ FNMT-RCM SERVIDORES SEGUROS	2043 December 20
Default	Actalis Authentication Root CA	Actalis Authentication Root CA	2030 September 22
Default	AffirmTrust Commercial	AffirmTrust Commercial	2030 December 31
Default	AffirmTrust Networking	AffirmTrust Networking	2030 December 31

This page contains three frames:

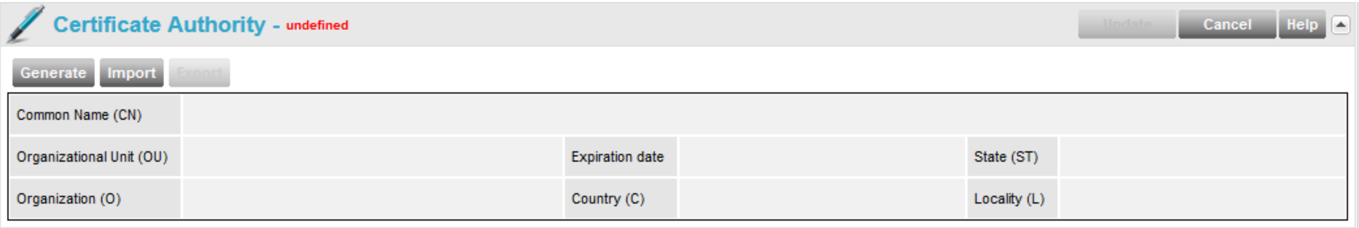
- **Certificate Authority** to configure trusted proxy Certificate Authority credentials
- **SSL Proxy and SSL Server** to select SSL proxy enabled sites and optimization enabled SSL servers
- **SSL Proxy Certificate Trust Store** to customize the SSL Proxy Certificate Trust Store (optional)

To modify the parameters, click the **Edit** button at the top of the page. It is then displayed in Edition mode (indicated by a ✎ icon instead of the 🔍 icon).

SSL Optimization configuration steps are described in the following sections.

Configuring trusted proxy CA credentials

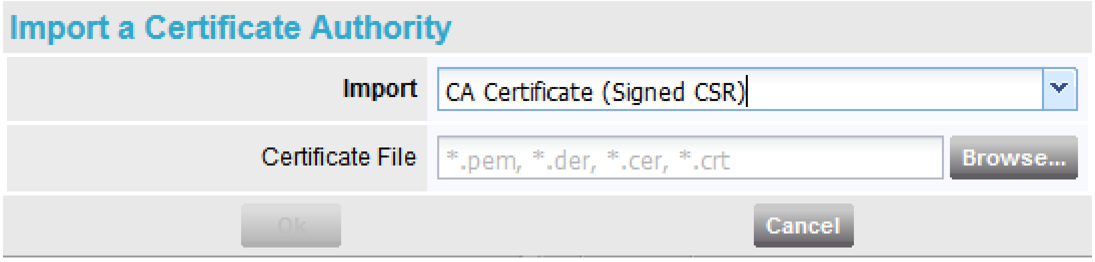
To configure trusted proxy CA credentials (certificate and private key), **edit** the **Certificate Authority** frame:



Common Name (CN)					
Organizational Unit (OU)		Expiration date		State (ST)	
Organization (O)		Country (C)		Locality (L)	

From this window, you can:

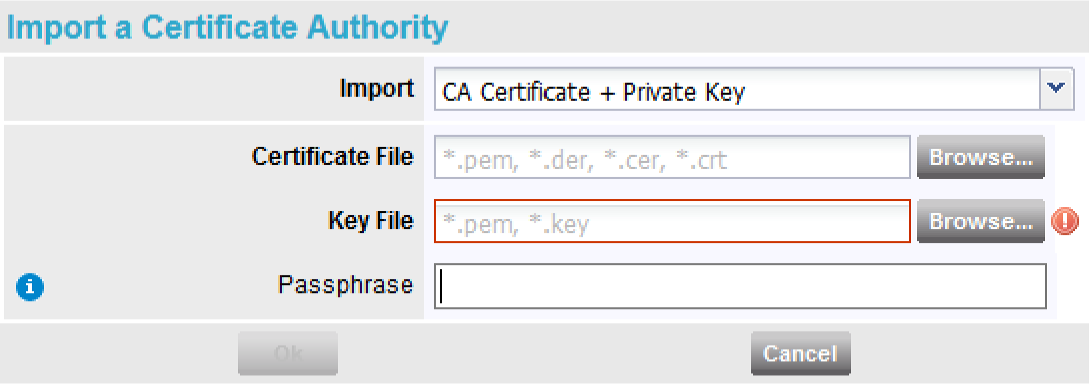
- either import a Certificate existing in your IT environment, by clicking the **Import** button:
  - you can choose to import a CA Certificate (Signed Certificate Signing Request):



Import: CA Certificate (Signed CSR)

Certificate File: *.pem, *.der, *.cer, *.crt

  - or a CA Certificate + a Private Key:



Import: CA Certificate + Private Key

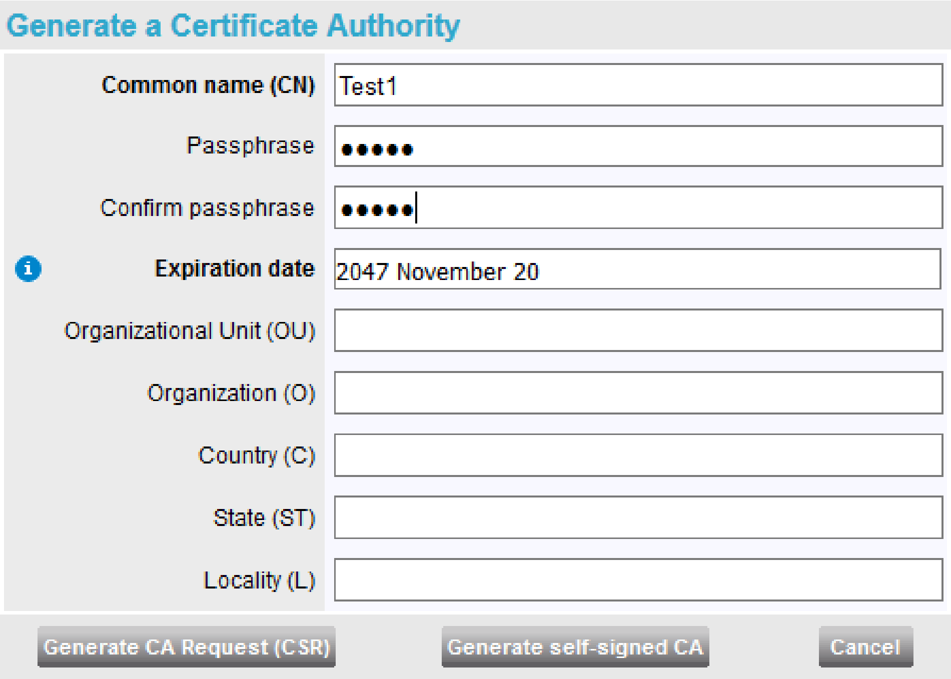
Certificate File: *.pem, *.der, *.cer, *.crt

Key File: *.pem, *.key

Passphrase:

If the Proxy CA Private key you import is encrypted with a passphrase, this passphrase must also be provided to the Appliances belonging to SSL proxy enabled Sites.

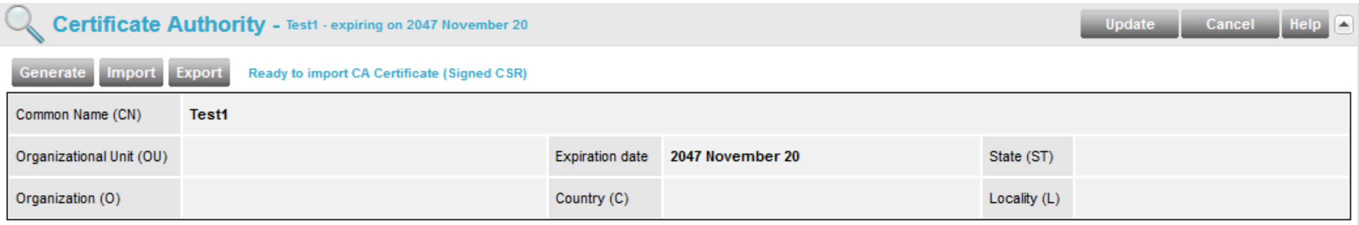
- or generate a Certificate after defining the following parameters (parameters in bold characters are mandatory, other parameters are optional):



Generate a Certificate Authority

Common name (CN)	Test1
Passphrase	●●●●●
Confirm passphrase	●●●●●
Expiration date	2047 November 20
Organizational Unit (OU)	
Organization (O)	
Country (C)	
State (ST)	
Locality (L)	

- **Common name (CN)**,
- Passphrase (has to be entered twice, if used): use it if you want the Proxy CA Private key to be encrypted with a passphrase, to raise the security level of SSL Optimization.
- **Expiration date**
- Organizational Unit (OU)
- Organization (O)
- Country (C)
- State (ST)
- Locality (L)
- Click the **Generate self-signed CA** button to generate the certificate which is immediately displayed:



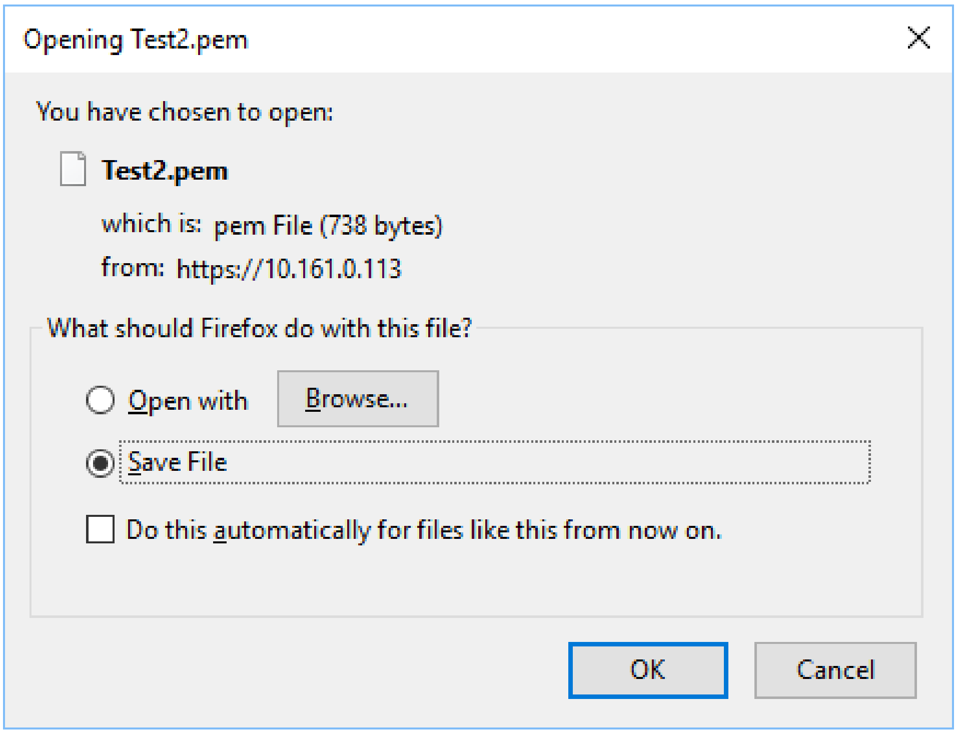
Certificate Authority - Test1 - expiring on 2047 November 20

Ready to import CA Certificate (Signed CSR)

Common Name (CN)	Test1				
Organizational Unit (OU)		Expiration date	2047 November 20	State (ST)	
Organization (O)		Country (C)		Locality (L)	

or

- Click the **Generate CA Request (CSR)** button to generate a certificate request which needs to be sent and signed by a Certification Authority. The system automatically asks you to save the file. Hit **OK** to confirm.



Opening Test2.pem

You have chosen to open:

Test2.pem

which is: pem File (738 bytes)

from: https://10.161.0.113

What should Firefox do with this file?

○ Open with

● Save File

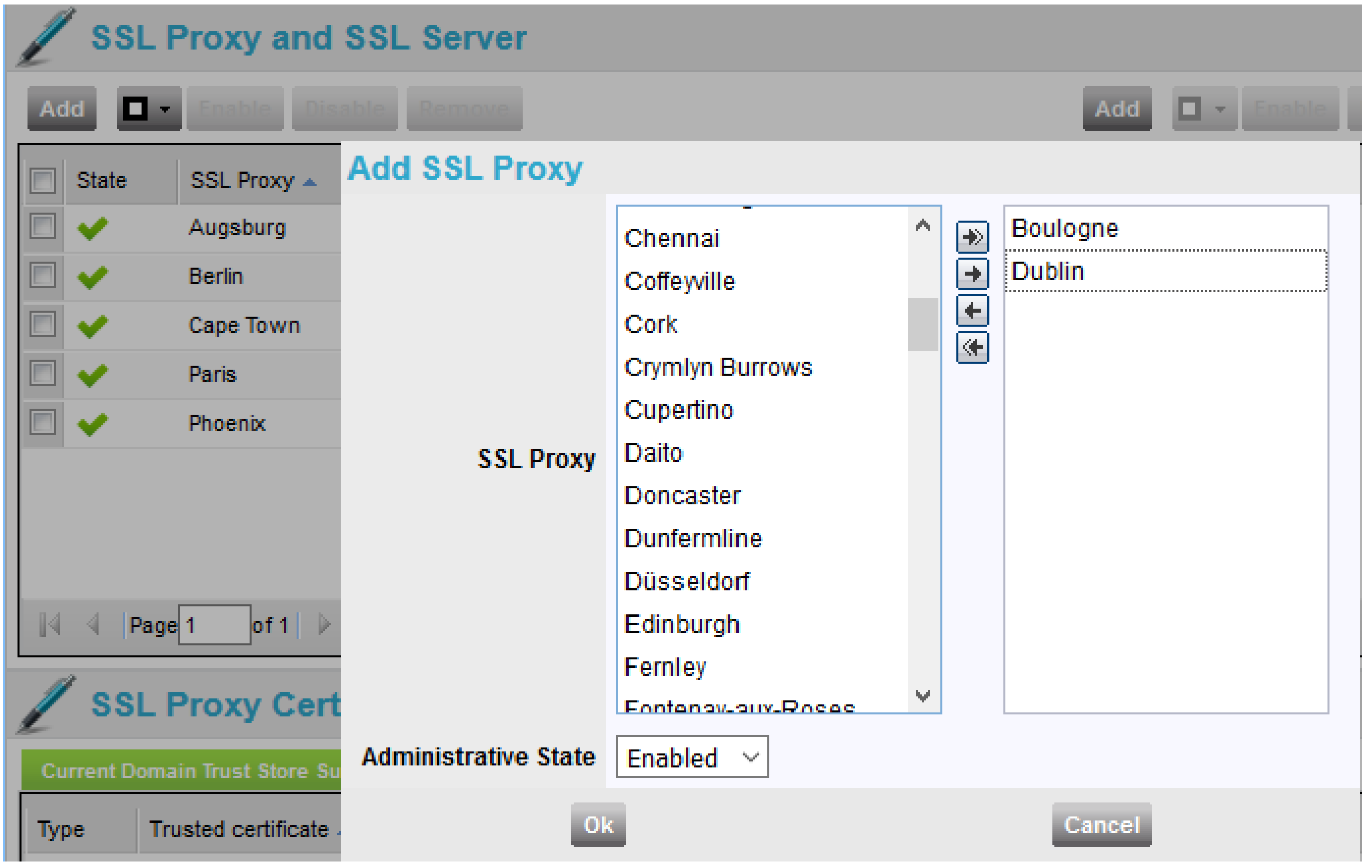
□ Do this automatically for files like this from now on.

The proxy CA certificates must be in your workstation trust-store.

Selecting SSL proxy enabled Sites and SSL Servers

The **SSL Proxy and SSL Server** frame enables you to select the SSL proxy enabled sites and SSL servers.

The left part of the frame is used to select the SSL proxies:



□	State	SSL Proxy
□	✓	Augsburg
□	✓	Berlin
□	✓	Cape Town
□	✓	Paris
□	✓	Phoenix

SSL Proxy

- Chennai
- Coffeyville
- Cork
- Crymlyn Burrows
- Cupertino
- Daito
- Doncaster
- Dunfermline
- Düsseldorf
- Edinburgh
- Fernley
- Fontenay-aux-Roses

- Boulogne
- Dublin

Administrative State: Enabled

1 Click **Add** and select the Sites you want to enable by pushing them to the right with the single arrow pointing to the right (the double arrow icon can be used to select all the Sites in one click).

2 Select 'Enabled' as Administrative State and click **OK**.

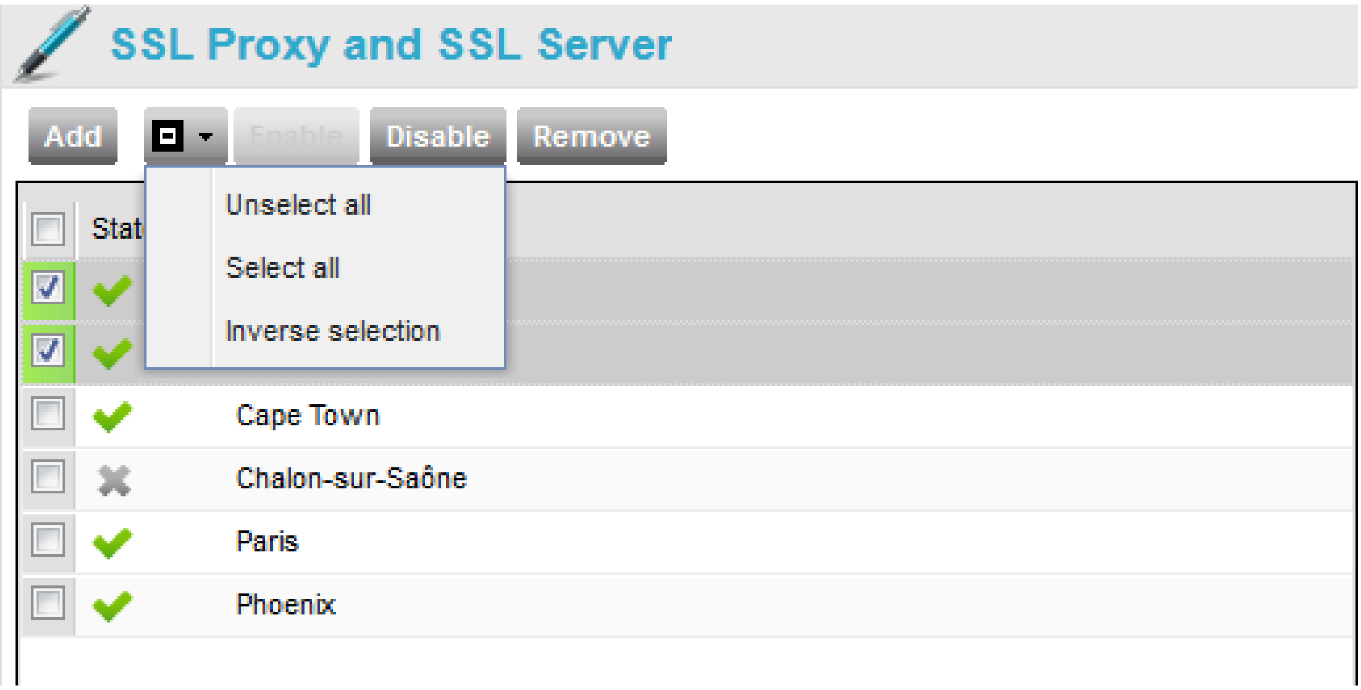
The selected Sites appear with a green status sign in the State column.

All Appliances that belong to these Sites (and only those) will be able to proxy SSL flows. All the Sites hosting enabled SSL servers should be on that list.

If you want to optimize traffic to the Cloud, the Site where your gateway is hosted should also be listed.

> **Note:** You may select Sites you do not want to be SSL proxies, by selecting 'Disabled' in the Administrative State field. These Sites are tagged with a grey status sign in the State column.

3. You can select the declared Sites (enabled or disabled) by checking them or by using the selection menu:

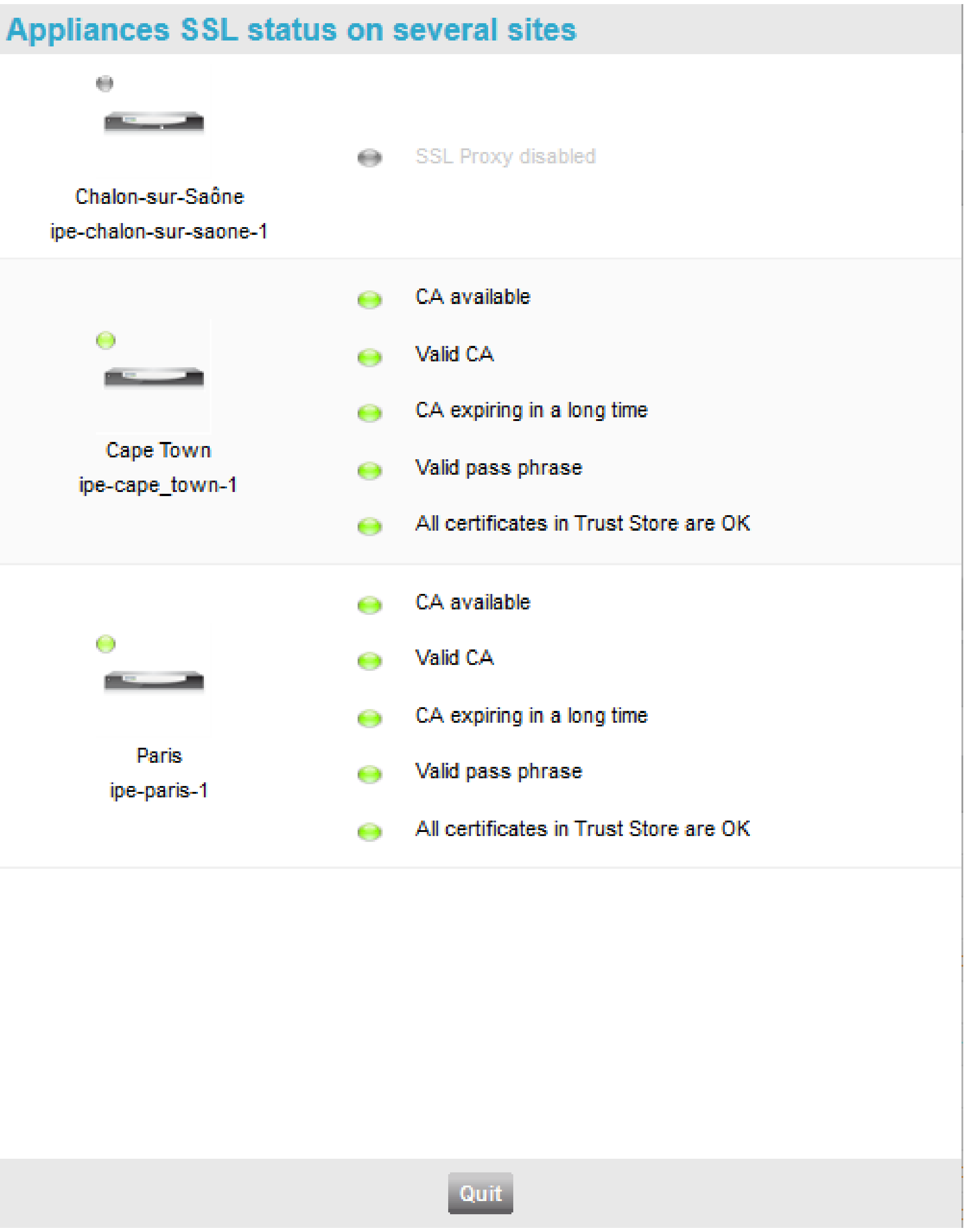


□	Stat	
☑	✓	
☑	✓	
□	✓	Cape Town
□	✗	Chalon-sur-Saône
□	✓	Paris
□	✓	Phoenix

You can perform the following operations:

- reversing the selection
- enabling or disabling the selected Sites
- removing the selected Sites

4. Click the **Update** button in the upper right corner of the page to validate your settings.
5. By right-clicking one or several Sites, you can use the **Show Status** function to display an SSL status summary of their appliances:



Appliances SSL status on several sites

Chalon-sur-Saône
ipe-chalon-sur-saone-1

- SSL Proxy disabled

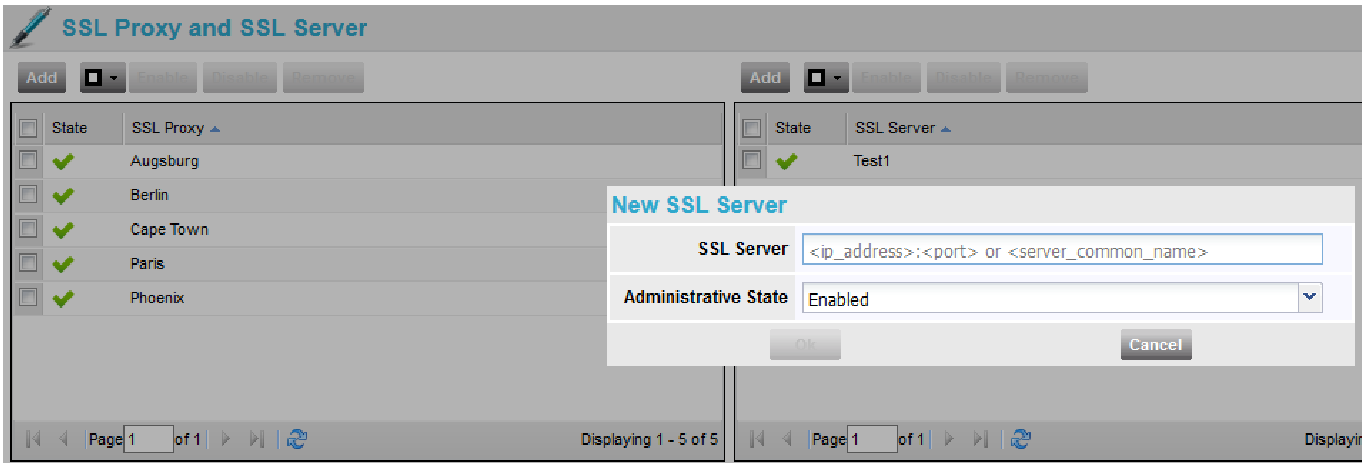
Cape Town
ipe-cape_town-1

- CA available
- Valid CA
- CA expiring in a long time
- Valid pass phrase
- All certificates in Trust Store are OK

Paris
ipe-paris-1

- CA available
- Valid CA
- CA expiring in a long time
- Valid pass phrase
- All certificates in Trust Store are OK

The right part of the frame is used to select SSL servers:



State	SSL Proxy
✓	Augsburg
✓	Berlin
✓	Cape Town
✓	Paris
✓	Phoenix

State	SSL Server
✓	Test1

SSL Server	<ip_address>:<port> or <server_common_name>
Administrative State	Enabled

1. Click **Add**.
2. In the 'New SSL Server' dialog box, enter:
   - either the SSL Server IP V4 address, followed by the port number if needed (example: 1.1.1.1:123)
   - or the SSL Server common name (example: *.extremenetworks.*)
3. Select the 'Enabled' option as Administrative State.
4. Click **OK**.

All the operations available for SSL Proxies can also be used with SSL Servers.

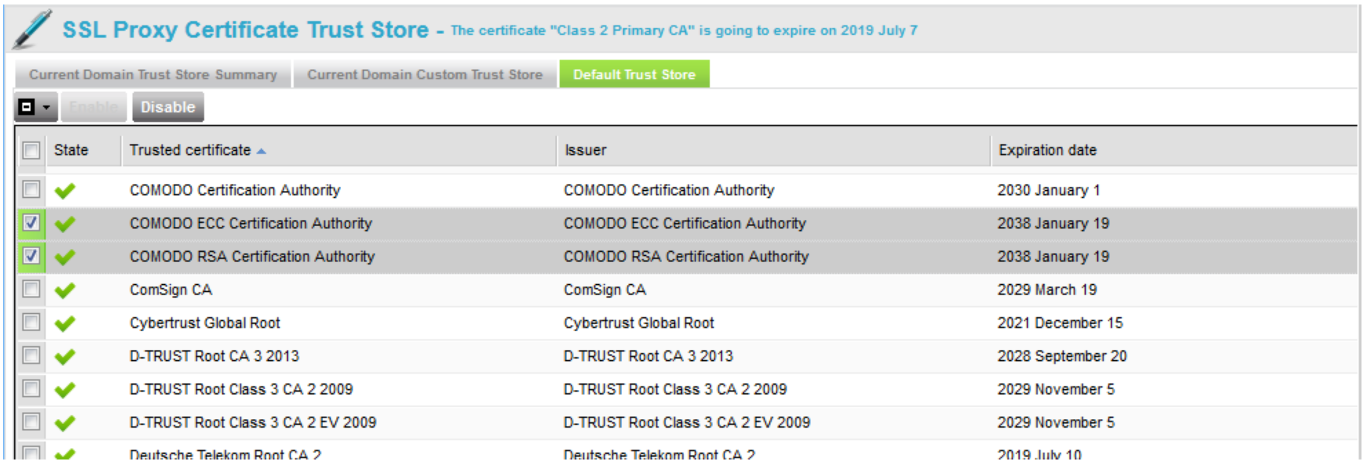
All the flows to these SSL Servers can be deciphered and optimized by the Appliance before being re-ciphered and forwarded.

> **Note:** You may select SSL Servers you do not want to decipher nor optimize, by selecting 'Disabled' in the Administrative State field. These Servers are tagged with a grey status sign in the State column.

Customizing the SSL Proxy Certificate Trust Store

The **SSL Proxy Certificate Trust Store** frame enables you to customize the SSL Proxy Certificate Trust Store.

It is configured with a set of standard institutional certificates by default . You can add your own corporate CA certificates, and/or remove all those you do not need.



SSL Proxy Certificate Trust Store - The certificate "Class 2 Primary CA" is going to expire on 2019 July 7

Current Domain Trust Store Summary
Current Domain Custom Trust Store
Default Trust Store
Enable
Disable

□	State	Trusted certificate ▲	Issuer	Expiration date
□	✓	COMODO Certification Authority	COMODO Certification Authority	2030 January 1
☑	✓	COMODO ECC Certification Authority	COMODO ECC Certification Authority	2038 January 19
☑	✓	COMODO RSA Certification Authority	COMODO RSA Certification Authority	2038 January 19
□	✓	ComSign CA	ComSign CA	2029 March 19
□	✓	Cybertrust Global Root	Cybertrust Global Root	2021 December 15
□	✓	D-TRUST Root CA 3 2013	D-TRUST Root CA 3 2013	2028 September 20
□	✓	D-TRUST Root Class 3 CA 2 2009	D-TRUST Root Class 3 CA 2 2009	2029 November 5
□	✓	D-TRUST Root Class 3 CA 2 EV 2009	D-TRUST Root Class 3 CA 2 EV 2009	2029 November 5
□	✓	Deutsche Telekom Root CA 2	Deutsche Telekom Root CA 2	2019 July 10

This frame contains three windows, accessible through three tabs:

- Current Domain Custom Trust Store, where you can import Trusted Certificates, enable/disable them or remove them,
- Default Trust Store that shows the list of standard institutional certificates; they can be enabled or disabled,
- Current Domain Trust Store Summary that displays a summary of the current Domain Trust Store.

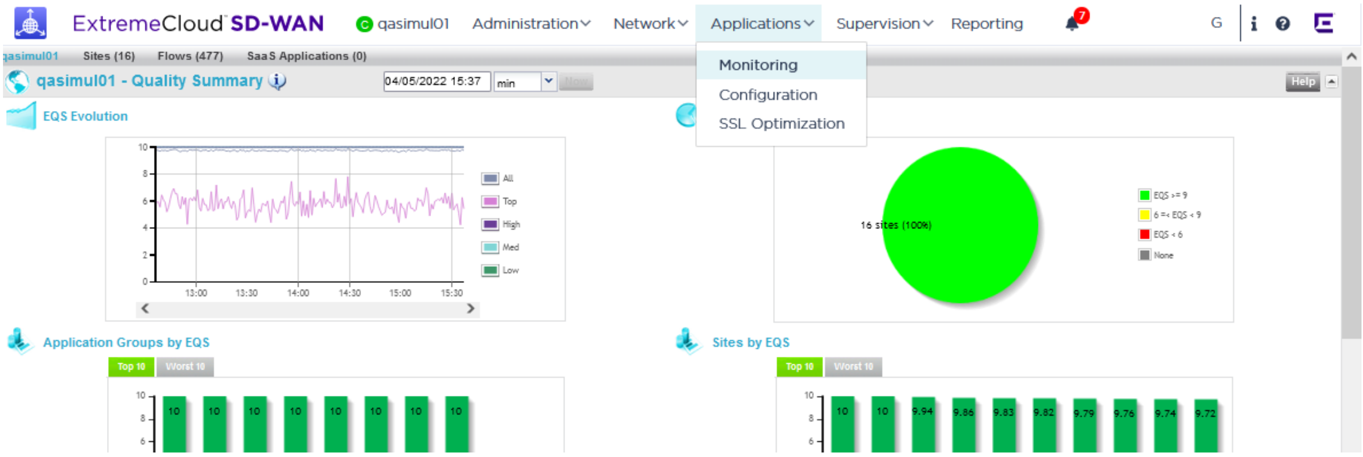
Monitoring

This section describes the usage and capabilities of the Application Monitoring dashboard.

- "Connection"
- "Frames and Timing"
- "Reading the Dashboard Contents"
- "Customer View"
- "Flows View"
- "Sites View"
- "Single Site View"
- "SaaS Applications View"

Connection

From the SD-WAN Orchestrator main menu, select **Applications -> Monitoring**.



The Application Monitoring dashboard window is made of two parts:

1. The View bar
2. The main space

From the View bar, you can select the following views:

- **<Customer_name>**: displays Client-level information
- **Sites (<number>)**: shows the list of Sites with their usage and quality
- **Flows (<number>)**: shows the list of flows at the Client level
- **SaaS Applications (<number>)**: shows the list of SaaS Applications at the Client level
- **<Site_name>** (only displayed when you click on a Site name or graph in one of the previous views): enables you to see more details for the selected Site; several Site views can be open simultaneously. You can close a Site view by clicking on the white cross next to its name: ☒.

The main space shows the different views:

- <Customer_name> with three frames:

<Customer> - Quality Summary

<Customer> - Activity Summary

<Customer> - WANs and Applications

- Sites (<number>) with two frames (<number> is the number of Sites currently configured):

Overview

Sites

- Flows (<number>) with two frames (<number> is the number of Flows measured during the last polling period):

Overview

Application flows

- <Site_name>, with up to six frames, depending on the User rights:

<Site> - Quality Summary

<Site> - Activity Summary

<Site> - Throughput Summary per NAP

<Site> - WANs and Applications

<Site> - Application flows

<Site> - Discovery

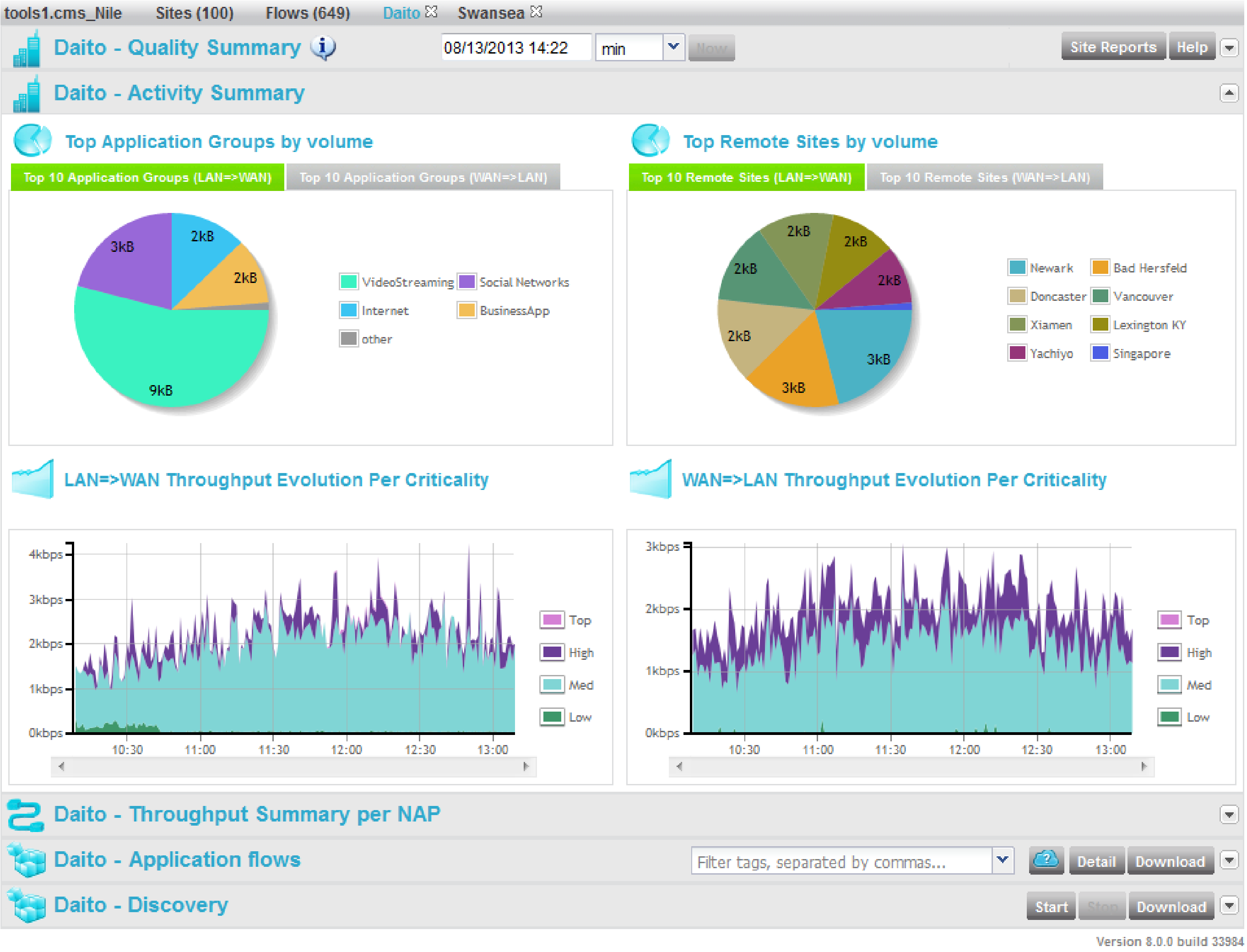
- SaaS Applications (<number>), with one frame (<number> is the number of SaaS Applications discovered during the selected polling period):

SaaS Applications over the last Hours

Frames and Timing

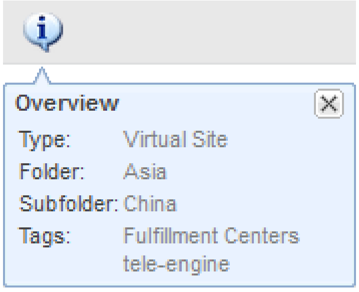
The frames in the different views can be expanded or collapsed by clicking on their headers (grey bars).

The following example illustrates a Site view with one frame expanded and all other frames collapsed.



The first frame header of each view (at the top of the main space, just below the menu and view bar) contains, after the name of the frame:

- a tooltip ⓘ (Client and individual Site views): shows additional information:



Overview

Type: Virtual Site

Folder: Asia

Subfolder: China

Tags: Fulfillment Centers
tele-engine

- a date and time area 07/01/2013 06:30 min ▾ : allows searching historical data (up to the last 4320 minutes of data) by clicking on this area and scrolling in the past in the pop-up calendar that opens;
- a drop-down list: allows choosing the time span:
  - min: evolution quadrants display 3 hours of per minute* information and you can scroll in the past; the flows list displays values averaged over one minute*,

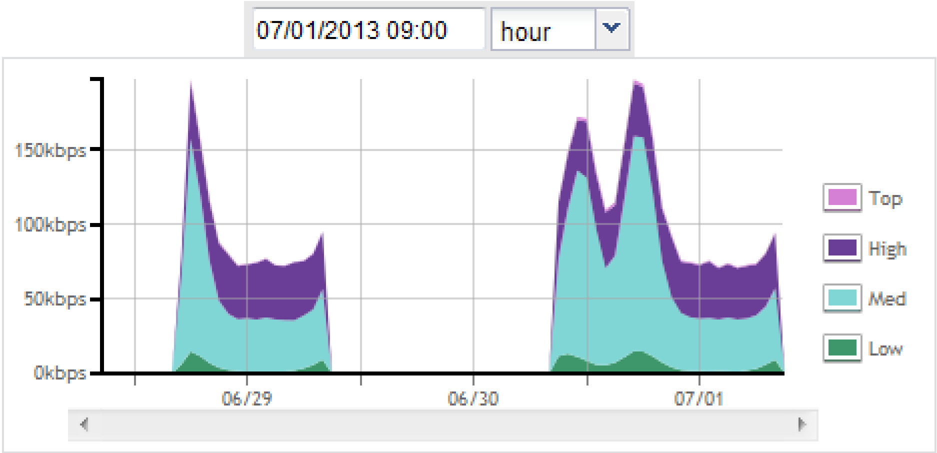
    All views (unless frozen) are automatically refreshed every minute*.

> **Note:** * The period can also be 5 or 15 minutes, if the Collect period has been set to 5 or 15 minutes respectively.

  - hour: evolution quadrants display up to 3 days of hourly aggregated information; the flows list displays values averaged over one hour;

    All views (unless frozen) are automatically refreshed every hour.

Throughput Evolution quadrant, with time span: hour



> **Note:** The lifetime of the data and the ability to aggregate hourly data depend on the Storage Parameters.

- a button to set the date and time to Now and unfreeze the view (the view is frozen when a date and time have been selected; the button is greyed when clicked);
- a Help button, providing contextual access to this documentation.

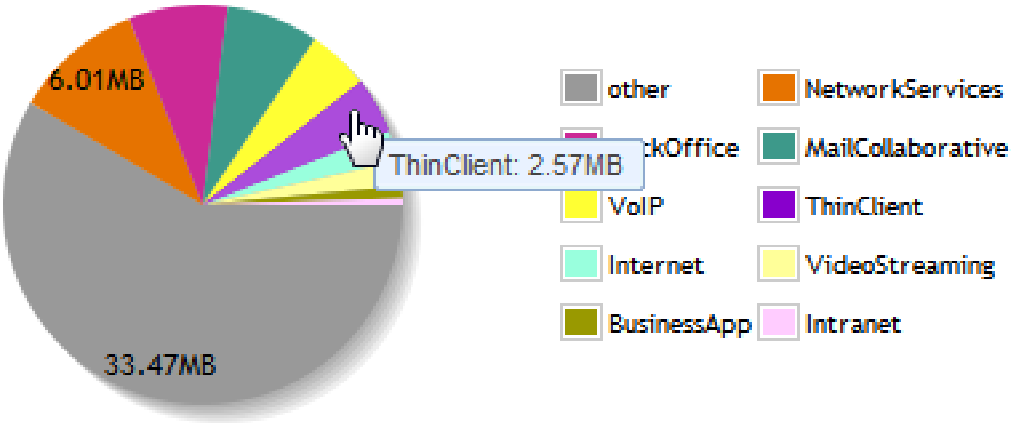
Reading the Dashboard Contents

The Application Monitoring dashboard displays bar graphs, historical graphs, pie charts, cord diagrams and tables.

The exact values of the various curves, fields, etc. can be read precisely:

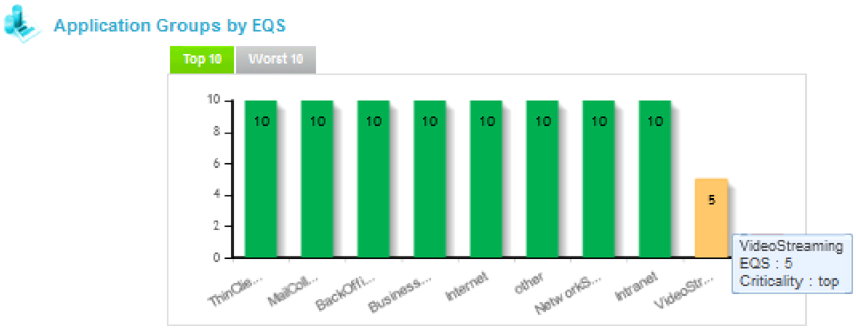
Bar graphs and pie charts

- You can read the exact values on a bar graph or on a pie chart, by moving your mouse over them. A small pop-up appears with the field name and its value:

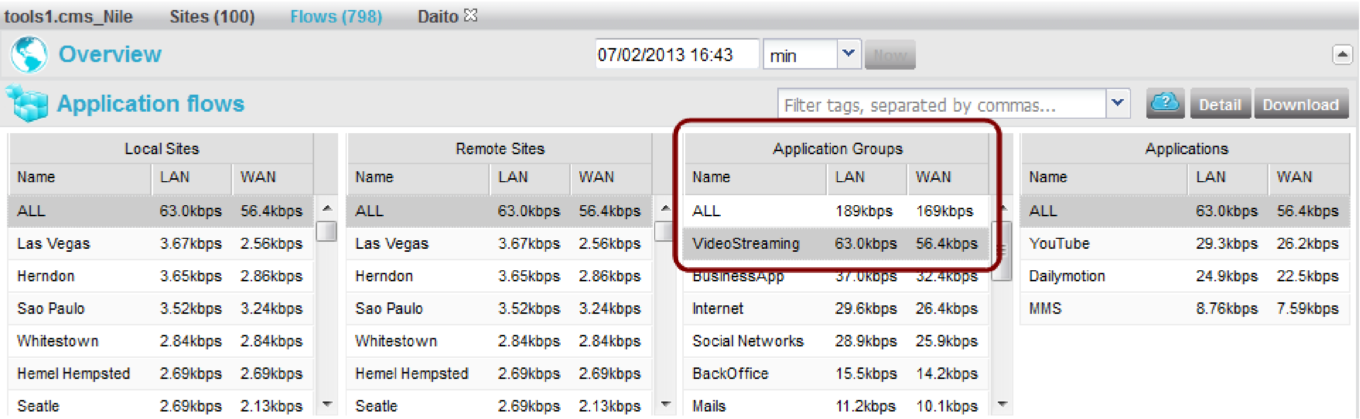


- You can access a Site view by clicking on its bar in a bar graph.
- You can access the Flows view filtered out to match an Application Group by clicking this AG in a bar graph or in a pie chart. For instance, clicking on VideoStreaming in the Application Groups by EQS graph in the Client view shows the flows belonging to the VideoStreaming AG:

  Filtering the flows list by clicking on a graph (1)



  Filtering the flows list by clicking on a graph (2)



07/02/2013 16:43 min

Local Sites		
Name	LAN	WAN
ALL	63.0kbps	56.4kbps
Las Vegas	3.67kbps	2.56kbps
Herndon	3.65kbps	2.86kbps
Sao Paulo	3.52kbps	3.24kbps
Whitestown	2.84kbps	2.84kbps
Hemel Hempsted	2.69kbps	2.69kbps
Seatle	2.69kbps	2.13kbps

Remote Sites		
Name	LAN	WAN
ALL	63.0kbps	56.4kbps
Las Vegas	3.67kbps	2.56kbps
Herndon	3.65kbps	2.86kbps
Sao Paulo	3.52kbps	3.24kbps
Whitestown	2.84kbps	2.84kbps
Hemel Hempsted	2.69kbps	2.69kbps
Seatle	2.69kbps	2.13kbps

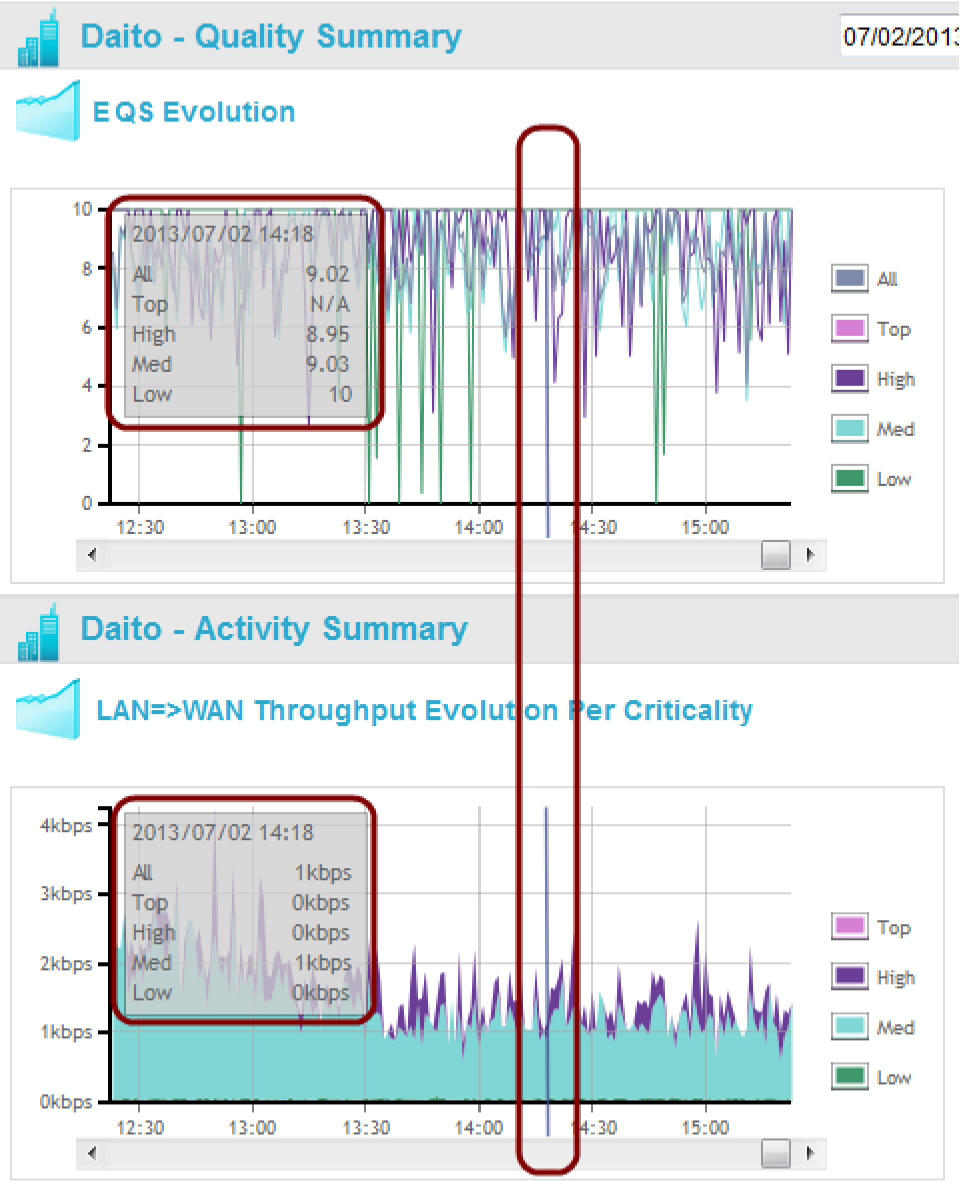
Application Groups		
Name	LAN	WAN
ALL	189kbps	169kbps
VideoStreaming	63.0kbps	56.4kbps
BusinessApp	37.0kbps	32.4kbps
Internet	29.6kbps	26.4kbps
Social Networks	28.9kbps	25.9kbps
BackOffice	15.5kbps	14.2kbps
Mails	11.2kbps	10.1kbps

Applications		
Name	LAN	WAN
ALL	63.0kbps	56.4kbps
YouTube	29.3kbps	26.2kbps
Dailymotion	24.9kbps	22.5kbps
MMS	8.76kbps	7.59kbps

Historical graphs

- You can read the exact values of historical graphs by moving your mouse over them. A vertical bar then appears on the graph, with a pop-up indicating the exact time and the exact values of each curve; the same vertical bar and pop-up also appear in the other historical graphs of the view, thus allowing a synchronized navigation and reading of all the graphs:

  Reading various historical graphs' exact values at the same time



Daito - Quality Summary 07/02/201

EQS Evolution

2013/07/02 14:18

All	9.02
Top	N/A
High	8.95
Med	9.03
Low	10

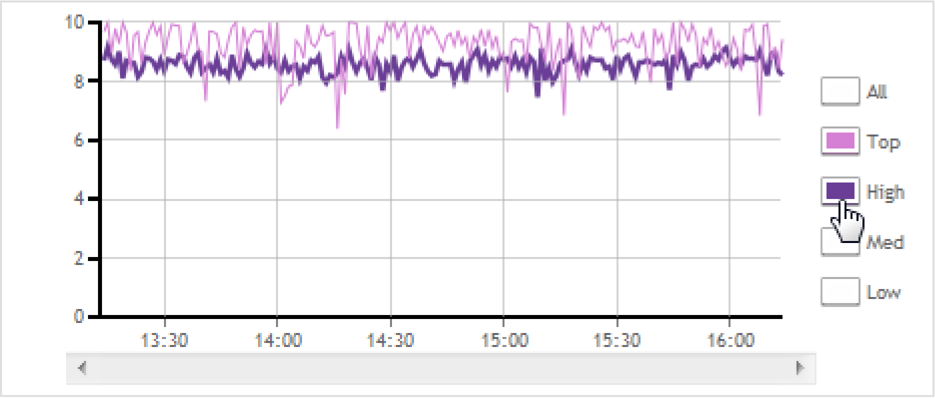
Daito - Activity Summary

LAN=>WAN Throughput Evolution Per Criticality

2013/07/02 14:18

All	1kbps
Top	0kbps
High	0kbps
Med	1kbps
Low	0kbps

- You can change the time (of the entire page) by clicking anywhere in these graphs; the time then changes to the clicked moment.
- You can highlight any curve by rolling over its legend, and you can hide or show it by clicking its legend. In the example below, you display the Top and High traffic, highlighting the High curve.



- You can export any graph, both in PNG and CSV formats, by right-clicking it.

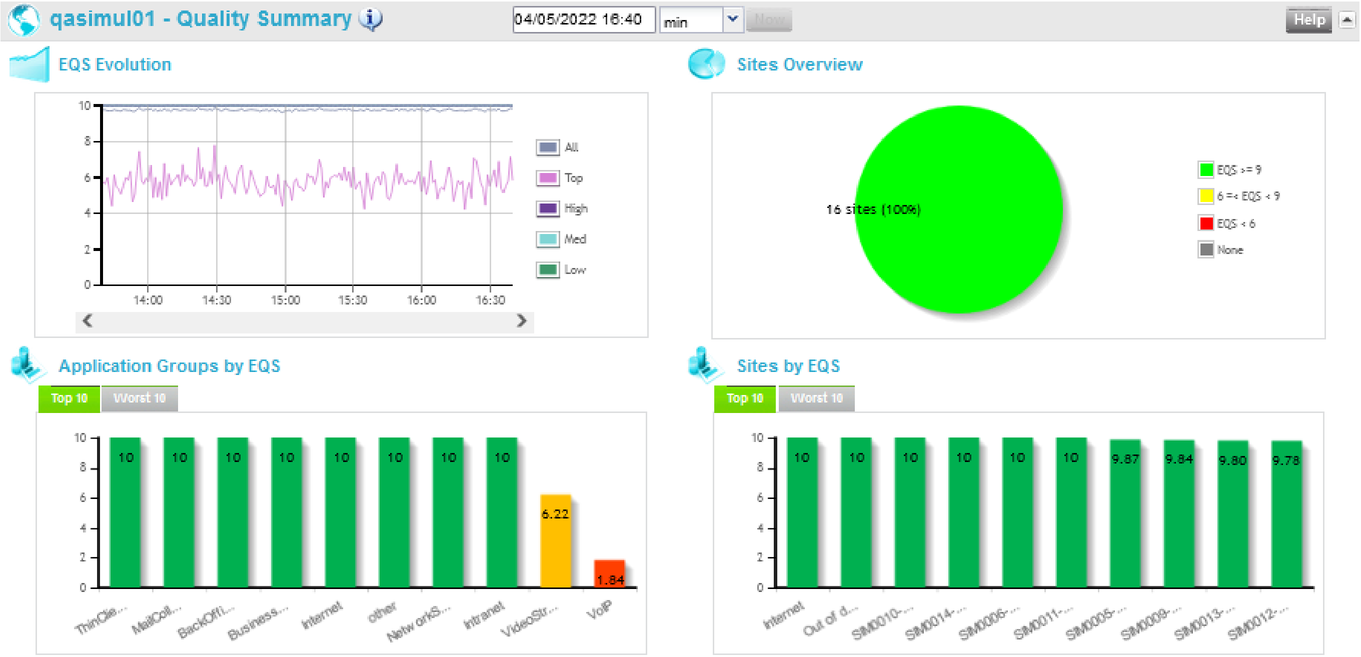
Customer View

The Customer View contains three frames:

- "Quality Summary"
- "Activity Summary"
- "WANs and Applications"

Quality Summary

This frame shows four graphs with the following information:



EQS Evolution

Historical graph showing the evolution of the EQS for all flows, and for the Top, High, Medium and Low flows. The covered period and the granularity of the data depend on the time span (see "Frames and Timing"): it can be three hours of per-minute information, if the time span is the minute (then you can scroll the past hours with the horizontal scroll bar at the bottom of the graph), or it can be the last three days of hourly averaged information, if the time span is the hour.

Site Overview

Pie chart showing the number of Sites (and the percentage of the total they represent):

- with an EQS higher or equal to 9 (in green),
- with an EQS between 6 and 9 (in yellow),
- with an EQS lower than 6 (in red),
- where the EQS could not be computed (none, in grey).

Application Groups by EQS

- Bar graph showing the Top 10 Application Groups (i.e. the 10 AGs with the best quality) sorted by decreasing quality (the best AG is displayed in the first bar on the left), with their EQS values displayed both as a number (between 0 and 10 with two decimals) and as a colored bar (the height of the bar indicates the value on the vertical axis and the color can take any hue between green (EQS = 10) and red (EQS = 0)).
- By clicking on Worst 10 at the top of the bar graph, the 10 worst Application Groups are displayed, sorted by increasing quality (the worst AG is displayed in the first bar on the left), with their EQS values.

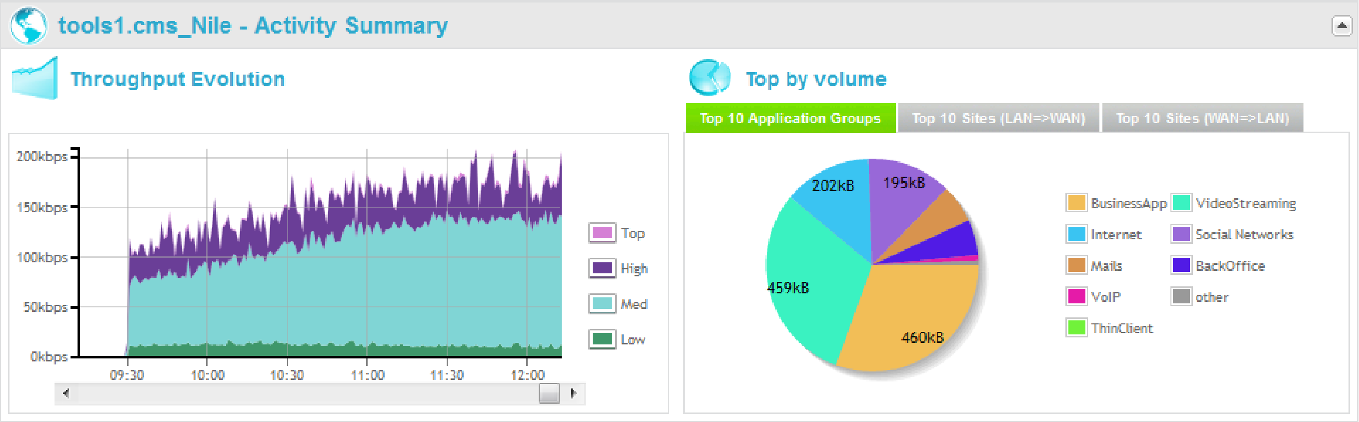
Sites by EQS

- This bar graph shows the Top 10 Sites (i.e. the 10 Sites with the best quality) sorted by decreasing quality (the best Site is displayed in the first bar on the left), with their EQS values displayed both as a number (between 0 and 10 with two decimals) and as a colored bar (the height of the bar indicates the value on the vertical axis and the color can take any hue between green (EQS = 10) and red (EQS = 0)).
- By clicking on Worst 10 at the top of the bar graph, the 10 worst Sites are displayed, sorted by increasing quality (the worst Site is displayed in the first bar on the left), with their EQS values.

By clicking on a bar, a new window opens and shows detailed information for the selected Site.

Activity Summary

This frame shows two graphs with the following information:



Throughput Evolution

Historical graph showing the evolution of the WAN throughput for the Top, High, Medium and Low flows (or any combination of these, according to the selection in the legend; by default, it shows all of them, i.e. the total WAN throughput). The covered period and the granularity of the data depend on the time span (see "Frames and Timing"): it can be three hours of per-minute information, if the time span is the minute (then you can scroll the past hours with the horizontal scroll bar at the bottom of the graph), or it can be the last three days of hourly averaged information, if the time span is the hour.

Top by volume

Pie chart showing the names and volumes of the top 10:

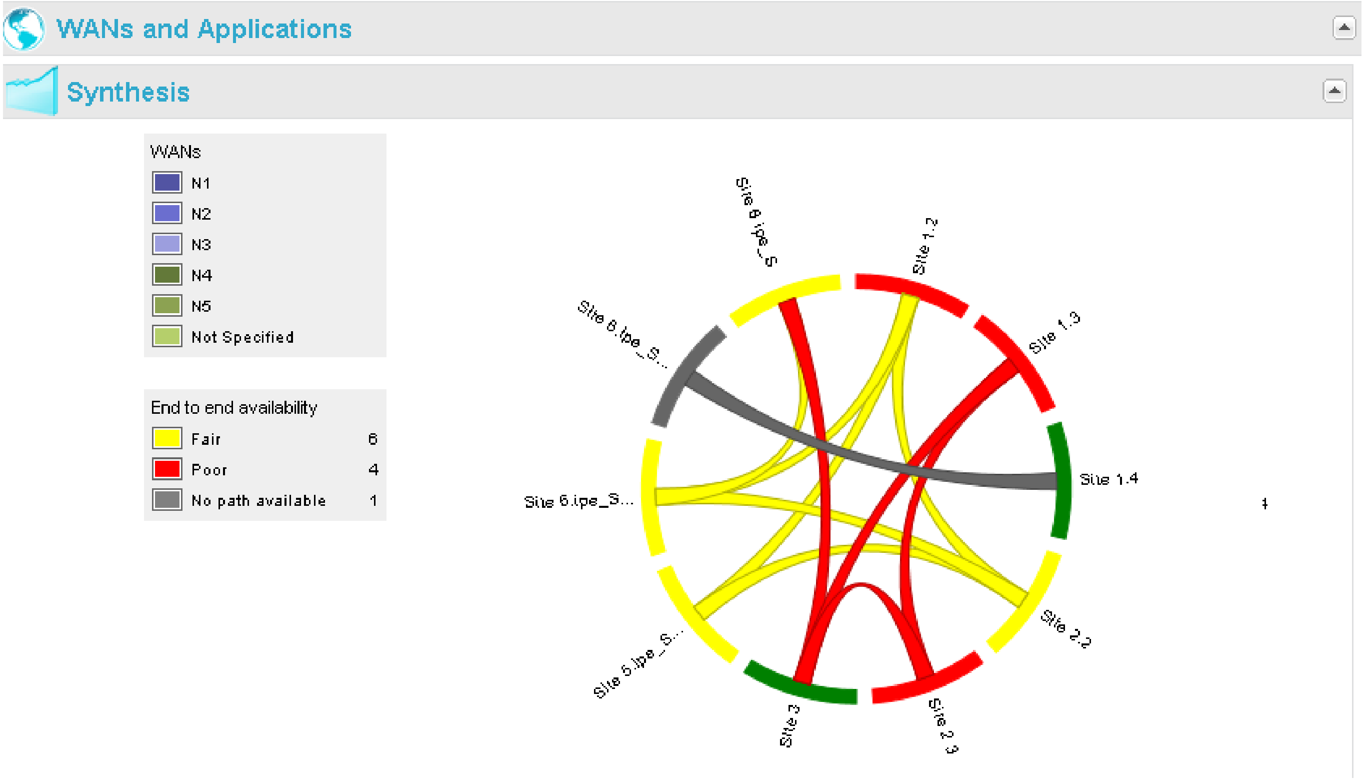
- Application Groups in volume (by clicking Top 10 Application Groups at the top of the graph; this is the default view),
- Sites in volume of outgoing traffic (by clicking Top 10 Sites (LAN => WAN)),
- Sites in volume of incoming traffic (by clicking Top 10 Sites (WAN => LAN)).

WANs and Applications

This frame displays for the Client:

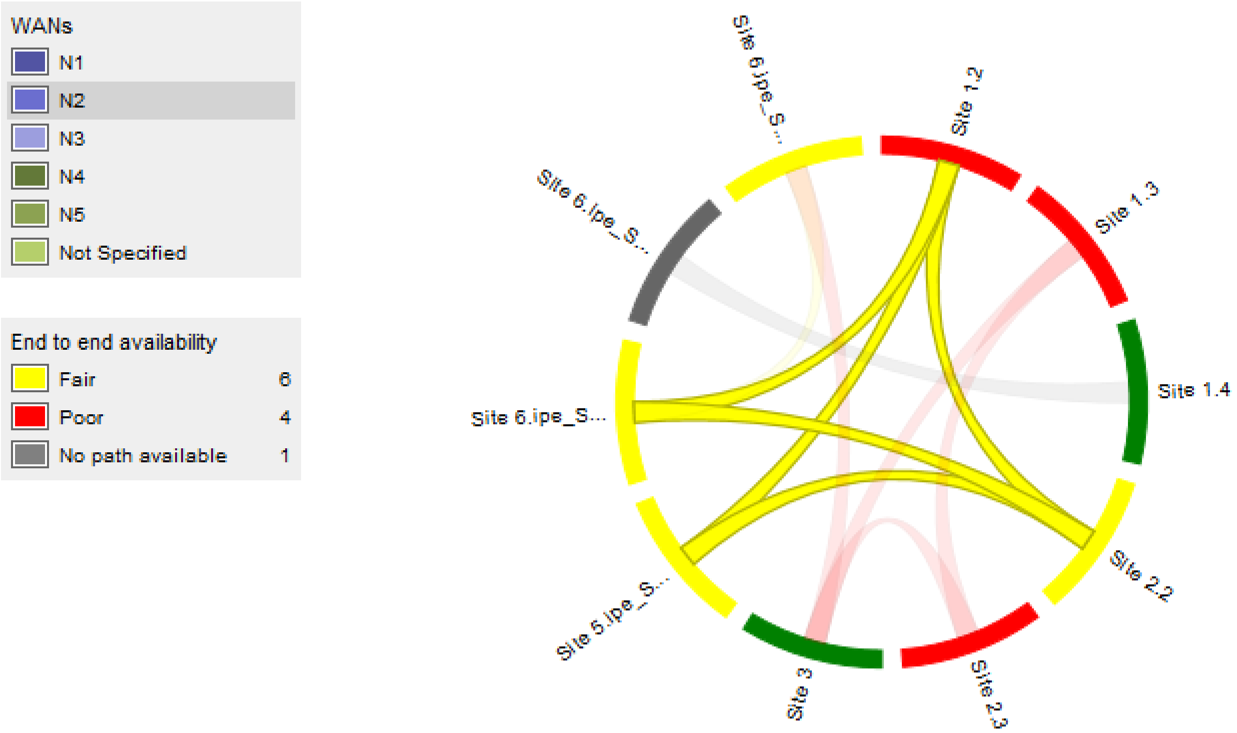
- 2 **Synthesis** diagrams of connectivity and traffic
- 2 **Details** graphs, one historical graph showing the evolution of the WAN throughput on each WAN and one detailed graph for connectivity

Synthesis - WAN Connectivity

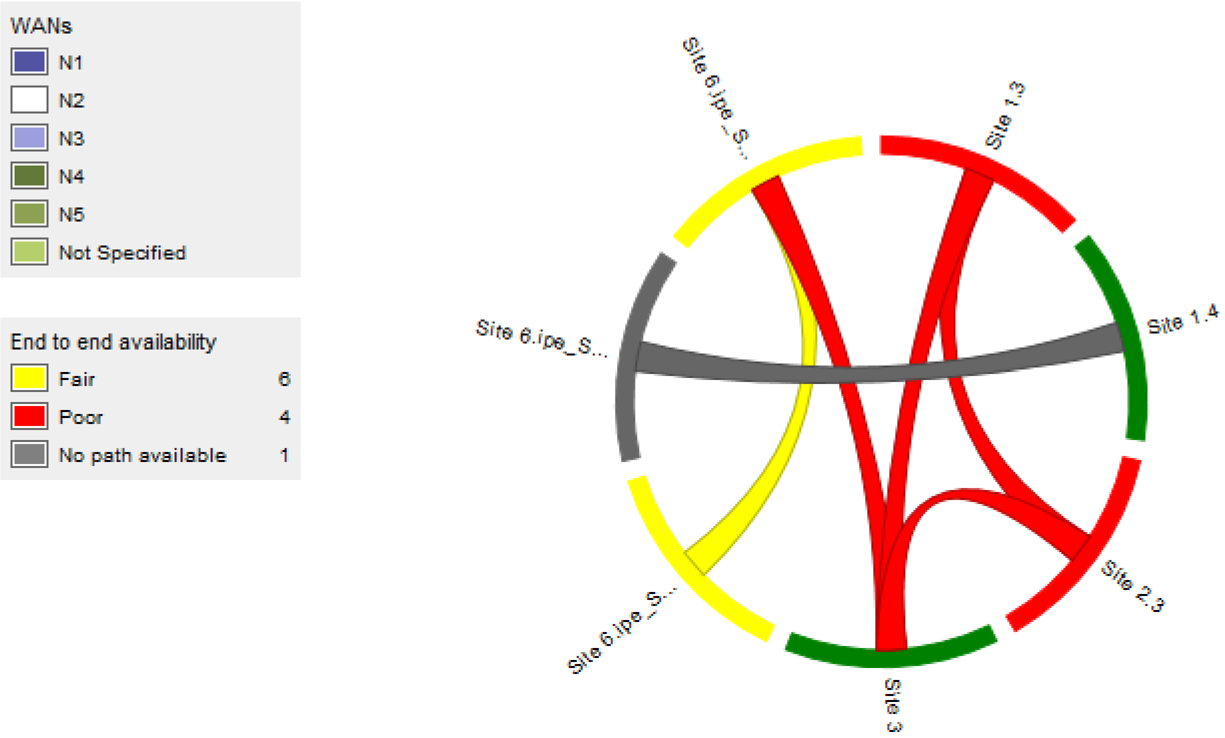


This chord diagram shows the end-to-end connectivity issues between the different Sites across the different WANs.

By moving your mouse over a WAN in the legend, you can highlight the traffic across the corresponding WAN:



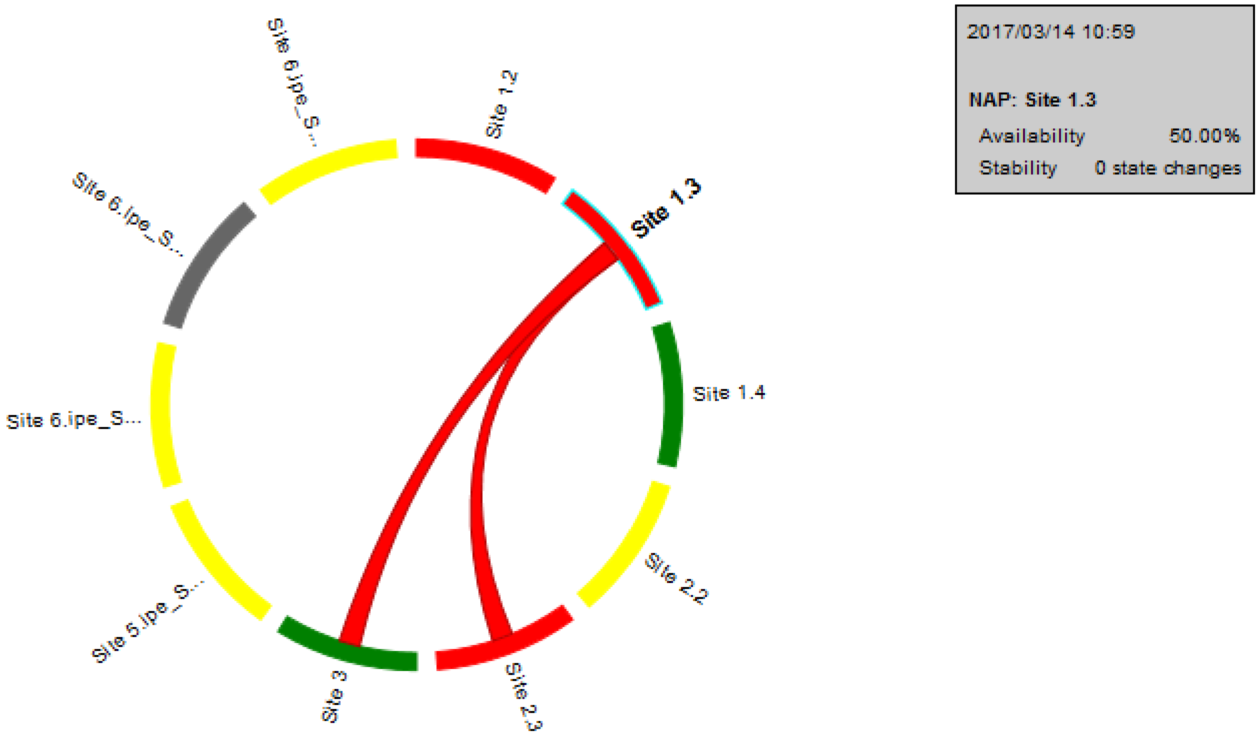
By clicking that WAN, you can remove it from the display (then it turns blank in the legend):



Click it again to show it again.

The same applies in the second legend, End-to-end availability. The latter can be "Fair" (99-80% of availability), "Poor" (< 80% of availability) or "No path available" (the normal state is "good", but it is not displayed so as to avoid saturating the graph).

By moving your mouse over an arc (i.e., a Site) in the diagram, you can show the traffic of the corresponding Site, only. A pop up shows the Availability (in percentage) and Stability (in number of state changes) of the network between this Site and the remote ones:



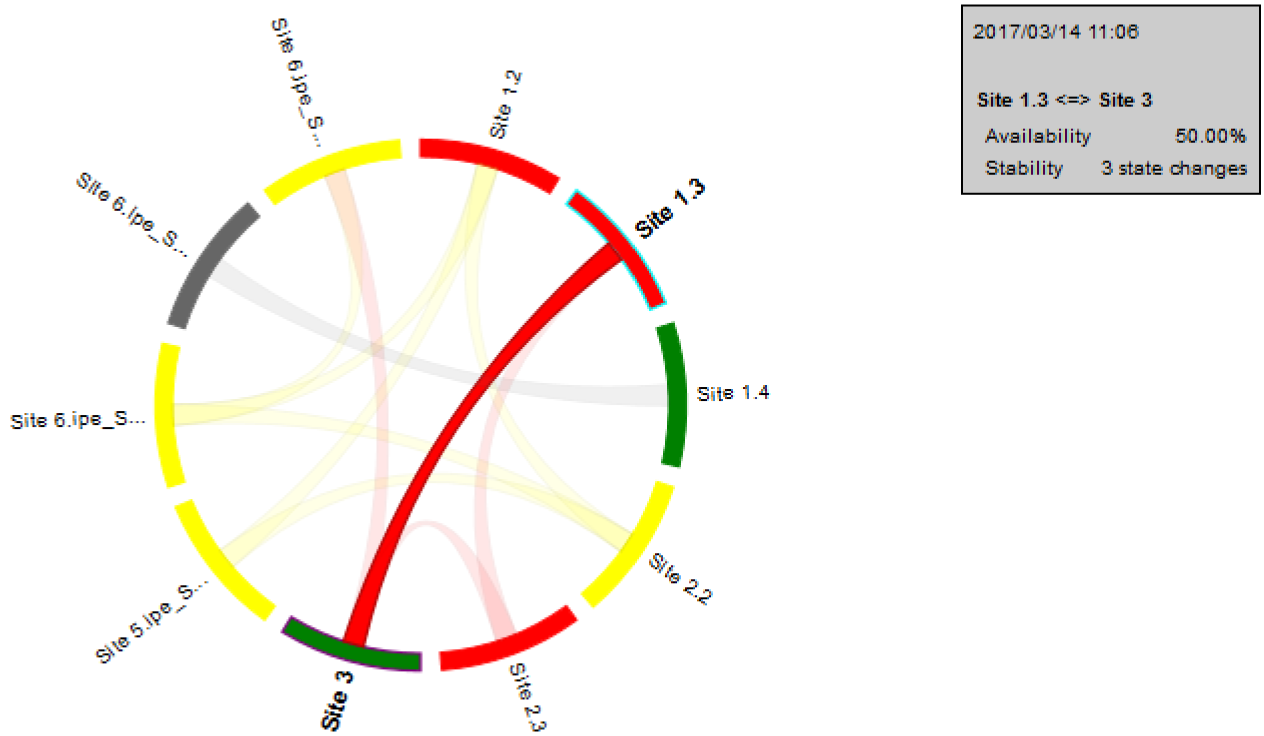
2017/03/14 10:59

NAP: Site 1.3

Availability	50.00%
Stability	0 state changes

By clicking that Site, you can open a new view in the dashboard, on the selected Site.

By moving your mouse over a chord (i.e., a flow between two Sites) in the diagram, you can highlight it. A pop up shows the Availability and Stability of the network between these two Sites:



2017/03/14 11:06

Site 1.3 <=> Site 3

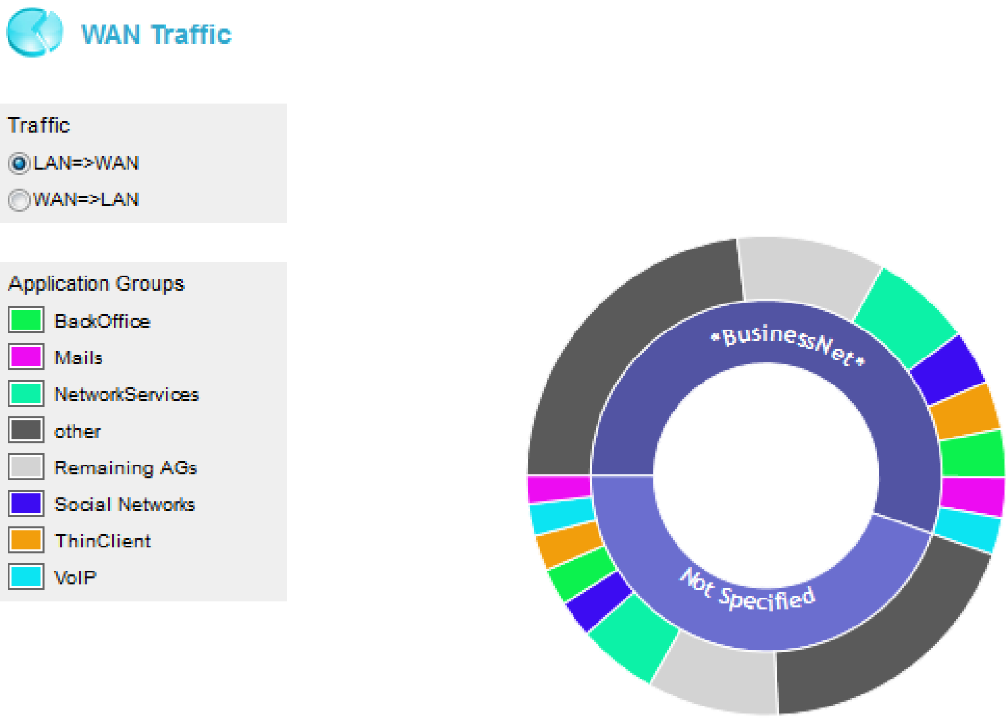
Availability 50.00%

Stability 3 state changes

By clicking that flow, you can open a new view in the dashboard, on the first (in alphabetical order) of the two Sites*' Activity Summary.

Synthesis - WAN Traffic

This donut diagram shows the instantaneous (dashboard time) throughput and distribution of the top 7 Application Groups per WAN. One slice represents the remaining Application Groups.



WAN Traffic

Traffic

● LAN=>WAN

○ WAN=>LAN

Application Groups

🟩 BackOffice

🟪 Mails

🟩 NetworkServices

⬛ other

⬜ Remaining AGs

🟦 Social Networks

🟧 ThinClient

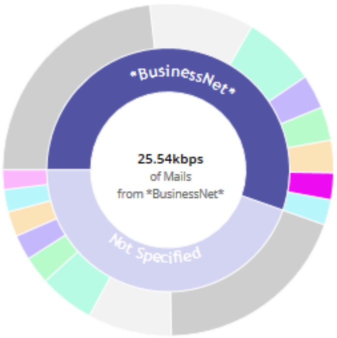
🟦 VoIP

Either select LAN -> WAN or WAN->LAN for defining ingress or egress directions.

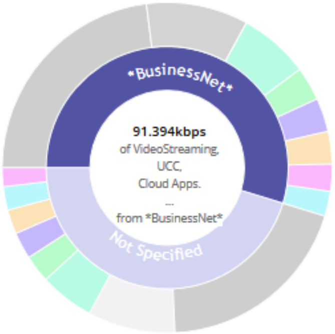
In the current diagram, the two internal slices of the donut correspond to two WANs, respectively named 'BusinessNet' and 'Not Specified'.

By moving your mouse cursor over the external colored slices which correspond to the application groups of both WANs, you can display the throughput of each application group in the middle of the donut.

The following picture highlights the throughput, in kilobits per second, of the 'Mails' application group from the 'BusinessNet' network.

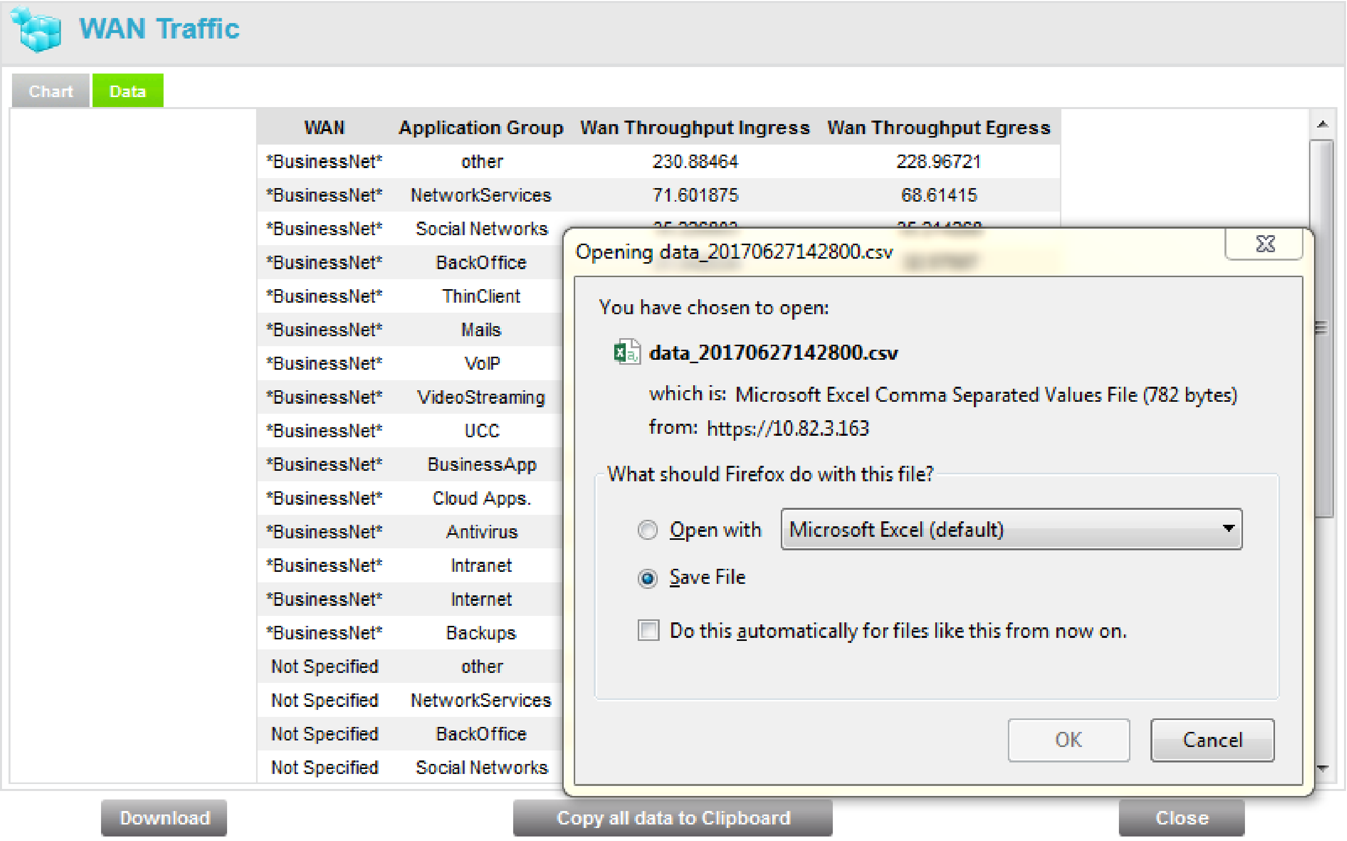


Note that the 'Remaining AGs' slice represents the remaining application groups per WAN, which are not included in the top 7 AGs. The provided value is an aggregation of the remaining AGs throughput values. The top 3 application groups are specified. The 'Other' slice corresponds to unrecognized traffic.



As with the WAN Connectivity chart, you may export the WAN Traffic diagram and data by right-clicking an AG and selecting the **Export** function. You can either download:

- the chart as a .png image or
- all data as a .csv file



WAN	Application Group	Wan Throughput Ingress	Wan Throughput Egress
BusinessNet	other	230.88464	228.96721
BusinessNet	NetworkServices	71.601875	68.61415
BusinessNet	Social Networks	[illegible]	[illegible]
BusinessNet	BackOffice		
BusinessNet	ThinClient		
BusinessNet	Mails		
BusinessNet	VoIP		
BusinessNet	VideoStreaming		
BusinessNet	UCC		
BusinessNet	BusinessApp		
BusinessNet	Cloud Apps.		
BusinessNet	Antivirus		
BusinessNet	Intranet		
BusinessNet	Internet		
BusinessNet	Backups		
Not Specified	other		
Not Specified	NetworkServices		
Not Specified	BackOffice		
Not Specified	Social Networks		

Opening data_20170627142800.csv

You have chosen to open:

data_20170627142800.csv

which is: Microsoft Excel Comma Separated Values File (782 bytes)

from: https://10.82.3.163

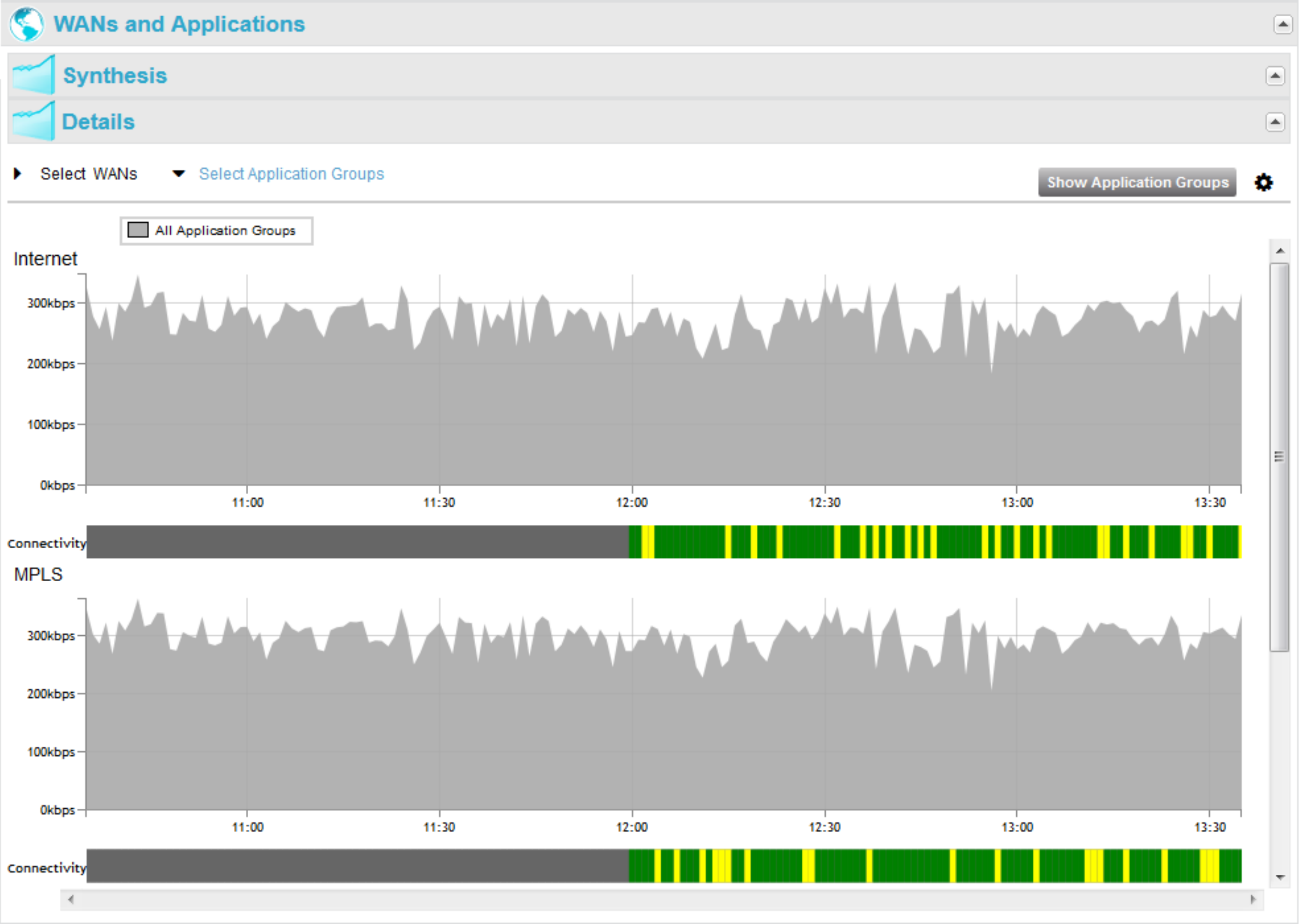
What should Firefox do with this file?

○ Open with Microsoft Excel (default)

● Save File

□ Do this automatically for files like this from now on.

WANs and Applications - Details



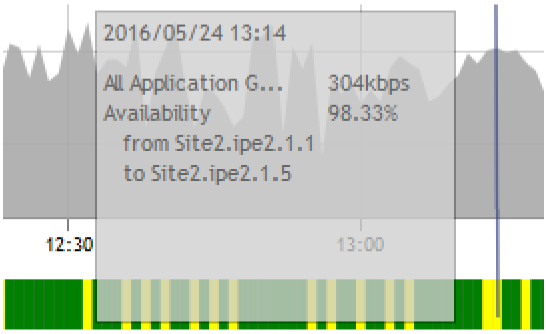
The covered period and the granularity of the data in the **Details** graphs depend on the time span: it can be three hours of per-minute information, if the time span is the minute (you can scroll the past hours with the horizontal scroll bar at the bottom of the graph), or it can be the last three days of hourly average information, if the time span is the hour.

The **Connectivity** graphs show the connectivity state of the available WANs. They can have four colors:

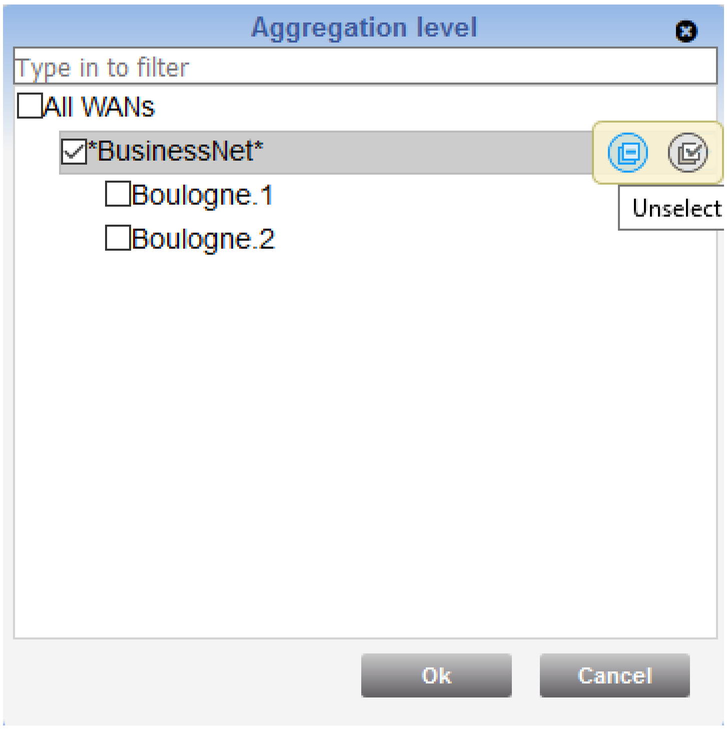
- green: 100% of connectivity
- yellow: 80%-99%
- red: < 80%
- grey: not measured

Exclamation marks indicate problem of stability (i.e. more than two changes during a collect).

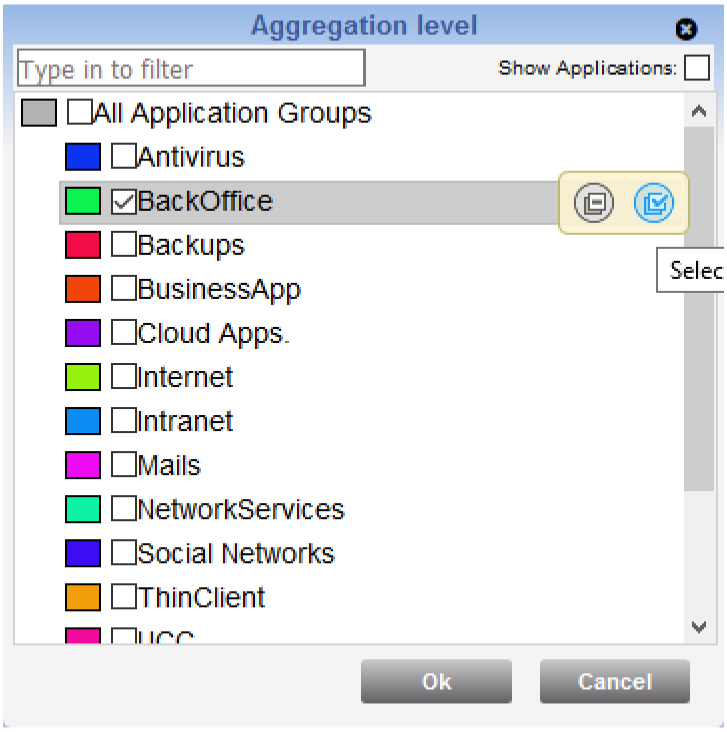
Connectivity problems are indicated in the pop-up when pointed with the mouse:



It is possible to show the graphs WAN by WAN (default view) or aggregated for all WANs, or for some WANs only, with a click on the arrow before **Select WAN** followed by a click on one of the WAN names. Modify your selection in the popup window through the Select Siblings/Unselect Siblings button and click **OK** to validate.



In the same way, it is possible to show the graphs for all Application Groups (default view) or for some Application Groups only, with a click on the arrow before **Select Application Group** followed by a click on one or several Application Group name(s) in the popup window. If you selected one Application Group, you can use the Select Siblings button to select again all the Application Groups. Click **OK** to validate.



Aggregation level

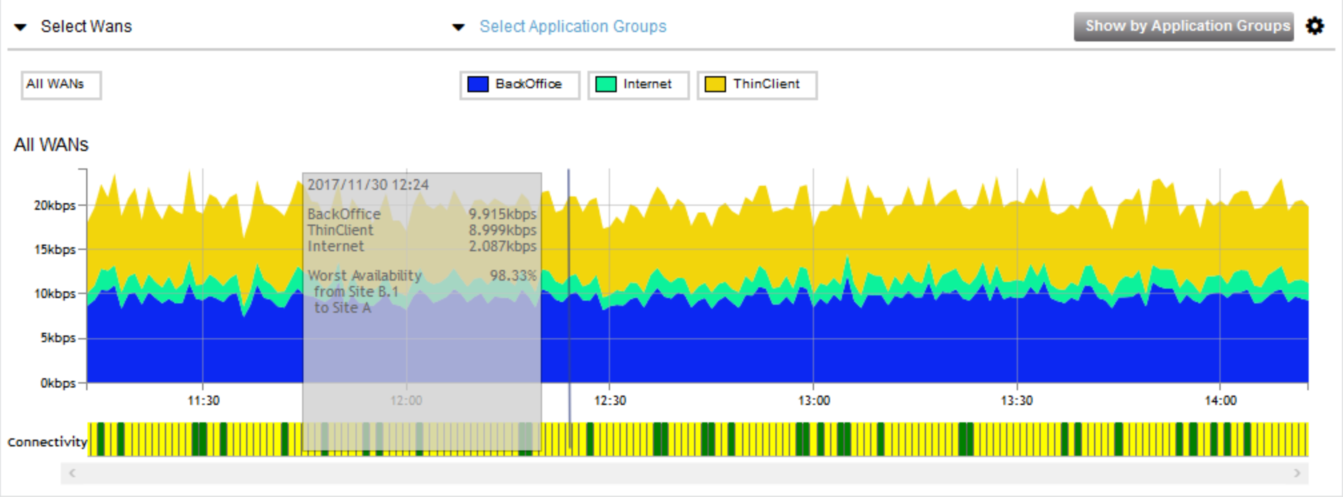
Type in to filter Show Applications: □

- 🟫 □ All Application Groups
  - 🟦 □ Antivirus
  - 🟩 ☑ BackOffice
  - 🟥 □ Backups
  - 🟧 □ BusinessApp
  - 🟪 □ Cloud Apps
  - 🟩 □ Internet
  - 🟦 □ Intranet
  - 🟪 □ Mails
  - 🟩 □ NetworkServices
  - 🟦 □ Social Networks
  - 🟧 □ ThinClient
  - 🟥 □ UCC

Selec

Ok Cancel

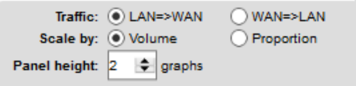
As a result, it shows the distribution of the selected Application Groups on each selected WAN:



2017/11/30 12:24

BackOffice	9.915kbps
ThinClient	8.999kbps
Internet	2.087kbps
Worst Availability from Site B.1 to Site A	98.33%

Hit the ⚙ icon in the upper right corner of the frame to modify your display through the following options:

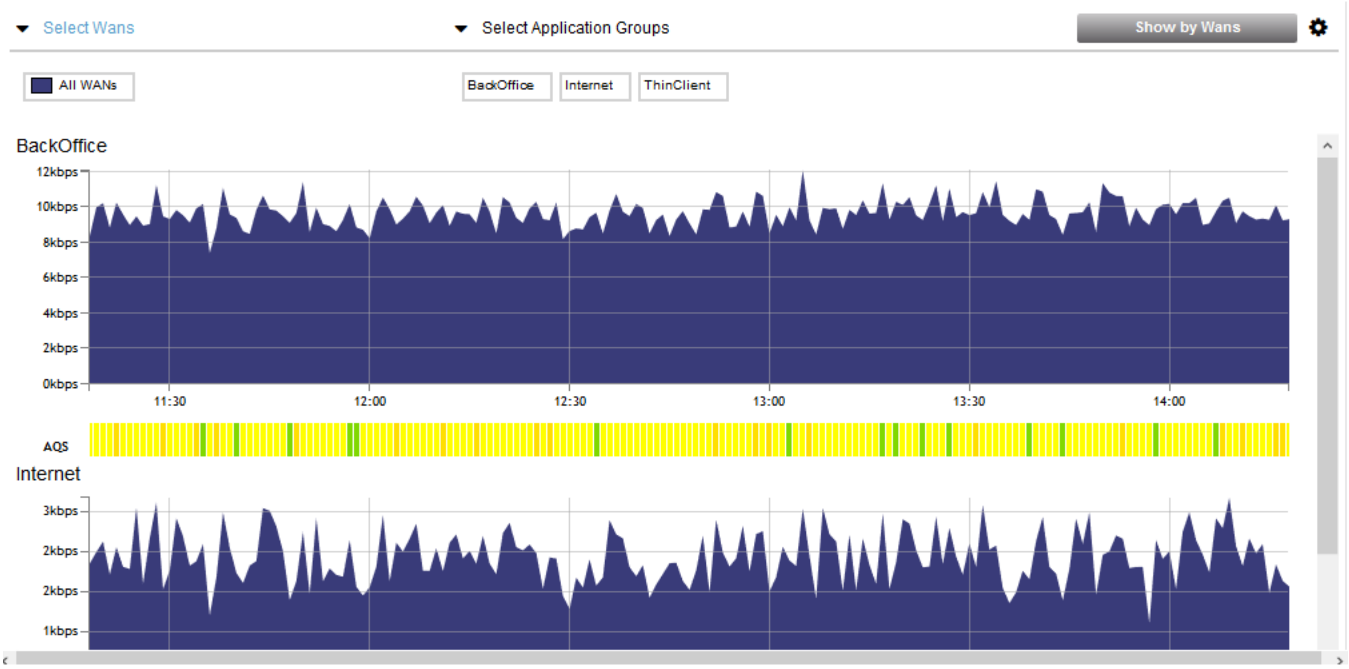


Traffic: ● LAN=>WAN ○ WAN=>LAN
Scale by: ● Volume ○ Proportion
Panel height: 2 graphs

- **Traffic**: select traffic direction from the LAN to the WAN or from the WAN to the LAN.

- **Scale**: if you select the 'Volume' option, throughput is specified in kilobits per second. If you select the 'Proportion' option, throughput is specified in percentage of the volume, with respect to the Y left axis.
- **Panel height - number of graphs**: according to the number of available WANs, you may define the number of graphs to display. The default option is 2. WAN graphs are displayed in alphabetical order.

The **Show by Application Groups** button toggles the view and shows the throughput evolution per Application Group and its EQS:



So instead of showing the distribution of the selected Application Groups on each selected WAN, this view shows the throughput evolution of the selected WANs for each selected Application Group.

The **Show by WANs** button toggles back to the previous view.

Also see "WANs and Applications" for the Site.

Flows View

The Flows View contains two frames:

"Overview"

"Application Flows"

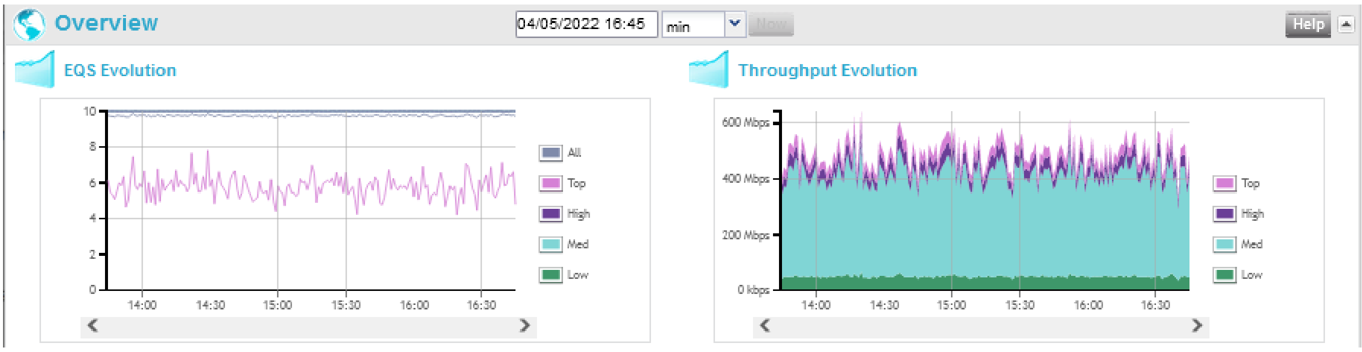
This section also addresses the following topics:

- "Real Time Graphs"
- "Discovery"

> **Note:** A flow groups all the sessions of a given application, from a given source to a given destination.

Overview

This frame shows two graphs with the following information:



EQS Evolution

Historical graph showing the evolution of the EQS for all the flows, and for the Top, High, Medium and Low flows for all the flows of the Client. It is identical to the EQS Evolution graph described in the "Quality Summary"frame of the Client View.

Throughput Evolution

Historical graph showing the evolution of the WAN throughput for the Top, High, Medium and Low flows for all the flows of the Client. It is identical to the Throughput Evolution graph described in the "Activity Summary" frame of the Client view.

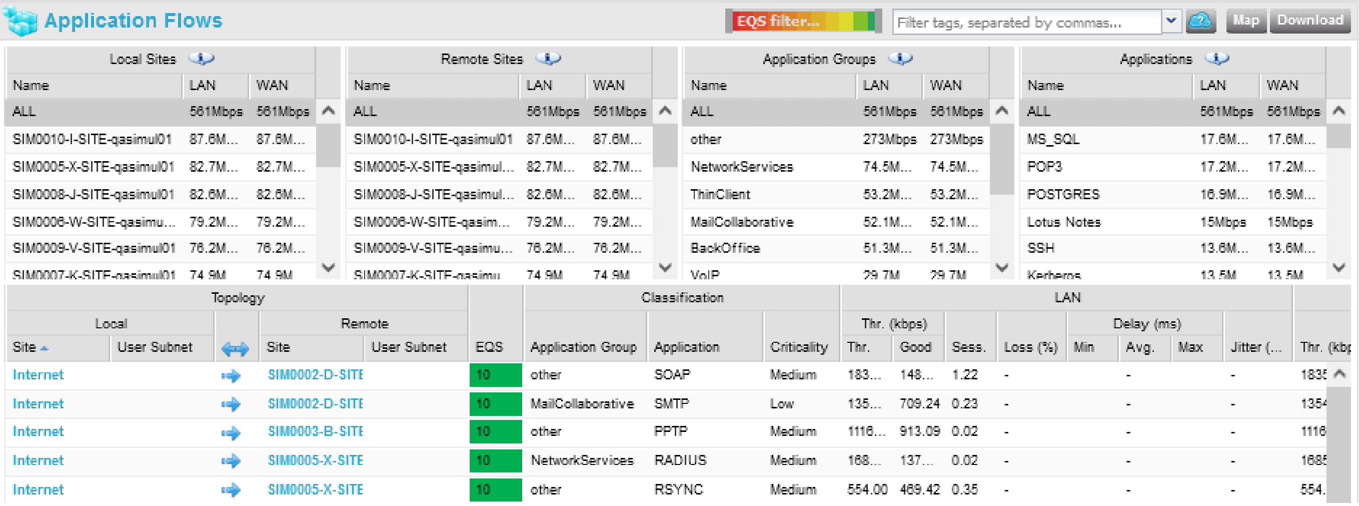
Application Flows

The top of the frame contains four filters and the rest of the frame displays:

- either the detailed flows list (by default); see "Application Flows - Filters"
- or a flows map (chord diagram); see "Application Flows - Flows map"

One can toggle between the two display options through the Detail / Map button.

In either case, the displayed information matches the selected filters (all the flows of the Client if no filter was selected).



Local Sites		
Name	LAN	WAN
ALL	561Mbps	561Mbps
SIM0010-I-SITE-qasimul01	87.6M...	87.6M...
SIM0005-X-SITE-qasimul01	82.7M...	82.7M...
SIM0008-J-SITE-qasimul01	82.6M...	82.6M...
SIM0006-W-SITE-qasimu...	79.2M...	79.2M...
SIM0009-V-SITE-qasimul01	76.2M...	76.2M...
SIM0007-K-SITE-qasimul01	74.9M	74.9M

Remote Sites		
Name	LAN	WAN
ALL	561Mbps	561Mbps
SIM0010-I-SITE-qasimul01	87.6M...	87.6M...
SIM0005-X-SITE-qasimul...	82.7M...	82.7M...
SIM0008-J-SITE-qasimul...	82.6M...	82.6M...
SIM0006-W-SITE-qasim...	79.2M...	79.2M...
SIM0009-V-SITE-qasimu...	76.2M...	76.2M...
SIM0007-K-SITE-qasimu	74.9M	74.9M

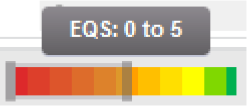
Application Groups		
Name	LAN	WAN
ALL	561Mbps	561Mbps
other	273Mbps	273Mbps
NetworkServices	74.5M...	74.5M...
ThinClient	53.2M...	53.2M...
MailCollaborative	52.1M...	52.1M...
BackOffice	51.3M...	51.3M...
VoIP	29.7M	29.7M

Applications		
Name	LAN	WAN
ALL	561Mbps	561Mbps
MS_SQL	17.6M...	17.6M...
POP3	17.2M...	17.2M...
POSTGRES	16.9M...	16.9M...
Lotus Notes	15Mbps	15Mbps
SSH	13.6M...	13.6M...
Kerberos	13.5M	13.5M

Topology						Classification			LAN								
Local			Remote						Thr. (kbps)				Delay (ms)				
Site	User Subnet	⇔	Site	User Subnet	EQS	Application Group	Application	Criticality	Thr.	Good	Sess.	Loss (%)	Min	Avg.	Max	Jitter (...	Thr. (kbp
Internet		➡	SIM0002-D-SITE		10	other	SOAP	Medium	183...	148...	1.22	-		-		-	1835
Internet		➡	SIM0002-D-SITE		10	MailCollaborative	SMTP	Low	135...	709.24	0.23	-		-		-	1354
Internet		➡	SIM0003-B-SITE		10	other	PPTP	Medium	1116...	913.09	0.02	-		-		-	1116
Internet		➡	SIM0005-X-SITE		10	NetworkServices	RADIUS	Medium	168...	137...	0.02	-		-		-	1685
Internet		➡	SIM0005-X-SITE		10	other	RSYNC	Medium	554.00	469.42	0.35	-		-		-	554.

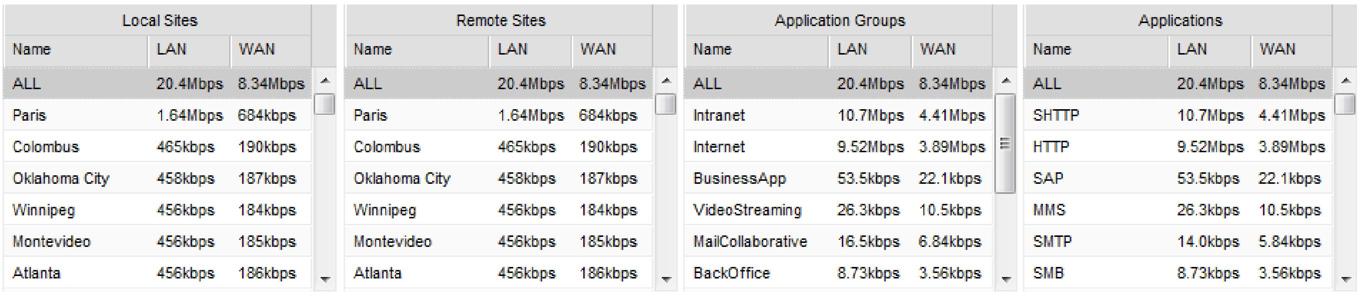
Application Flows - Filters

It is possible to filter the flows by EQS, moving the two cursors of the EQS filter at the top of the frame (e.g. to see the bad flows only (EQS <5), as in the example below):



A text field enables you to filter the flows through Site tags, a button opens a map where the flows can be filtered when you click these tags, and a Download button enables you to download or open a zipped CSV file containing all the flows' information displayed in this frame.

Moreover, the Application Flows frame has four filters: Local Sites, Remote Sites, Application Groups and Applications with, for each of them, their name, LAN throughput and WAN throughput:



Local Sites		
Name	LAN	WAN
ALL	20.4Mbps	8.34Mbps
Paris	1.64Mbps	684kbps
Colombus	465kbps	190kbps
Oklahoma City	458kbps	187kbps
Winnipeg	456kbps	184kbps
Montevideo	456kbps	185kbps
Atlanta	456kbps	186kbps

Remote Sites		
Name	LAN	WAN
ALL	20.4Mbps	8.34Mbps
Paris	1.64Mbps	684kbps
Colombus	465kbps	190kbps
Oklahoma City	458kbps	187kbps
Winnipeg	456kbps	184kbps
Montevideo	456kbps	185kbps
Atlanta	456kbps	186kbps

Application Groups		
Name	LAN	WAN
ALL	20.4Mbps	8.34Mbps
Intranet	10.7Mbps	4.41Mbps
Internet	9.52Mbps	3.89Mbps
BusinessApp	53.5kbps	22.1kbps
VideoStreaming	26.3kbps	10.5kbps
MailCollaborative	16.5kbps	6.84kbps
BackOffice	8.73kbps	3.56kbps

Applications		
Name	LAN	WAN
ALL	20.4Mbps	8.34Mbps
SHTTP	10.7Mbps	4.41Mbps
HTTP	9.52Mbps	3.89Mbps
SAP	53.5kbps	22.1kbps
MMS	26.3kbps	10.5kbps
SMTP	14.0kbps	5.84kbps
SMB	8.73kbps	3.56kbps

Applying a filter

The flows in the chord diagram and in the detailed flows list can be filtered out by clicking on any filter or any combination of filters.

One can select several filters in a column by maintaining the CTRL key pressed during the selection. To select all filters between line A and line Z, select line A, press the SHIFT key and select line Z while maintaining the SHIFT key pressed.

Several filters from several columns can be applied simultaneously.

To remove the filters, click the first line (ALL; this is the default view).

Interactions between filters

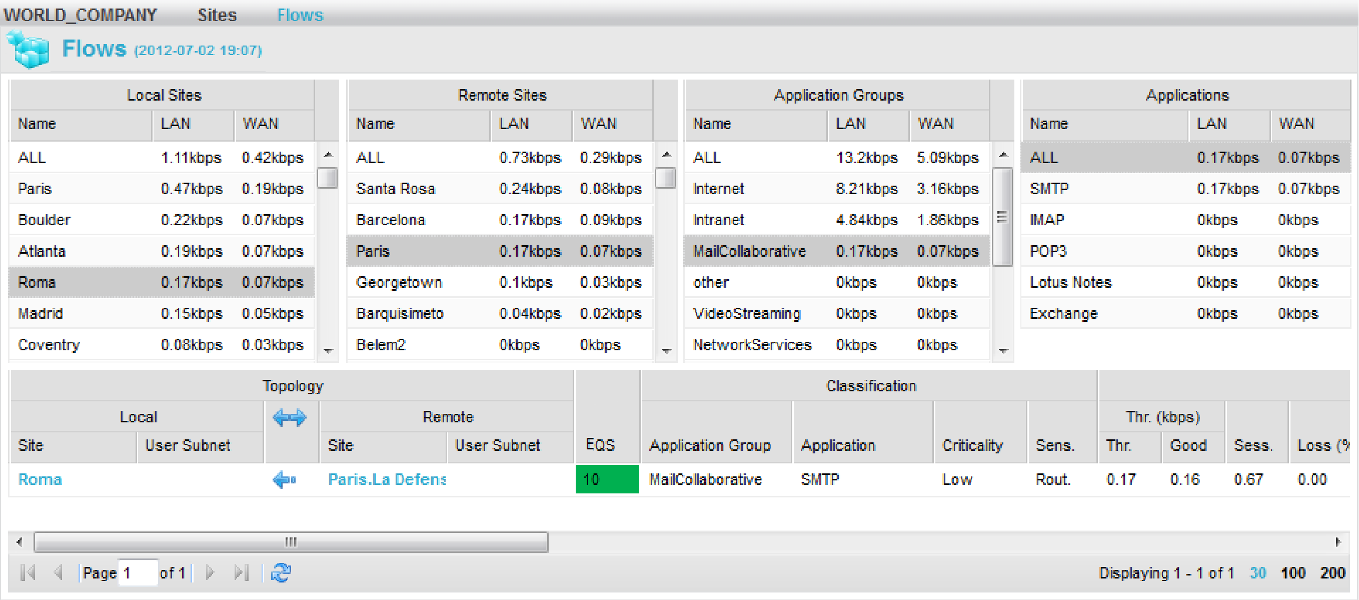
When a filter is applied, the other filters are updated accordingly. For instance, if FTP is selected in the Application Groups filter, the Applications filter table only displays the applications belonging to that Group and the throughput values displayed in the Remote Sites filter correspond to the throughput for that Group only.

Sorting the filter data

You may sort the data in these filters by clicking on the column headers: click once to sort the data incrementally (an up arrow ▲ then appears next to the header), click twice to sort the data in the reverse order (▼).

(ALL shows all flows with the total values, and it always appears at the top of the filter tables, whatever the sorting criteria.)

The following image illustrates how only MailCollaborative between Roma and Paris is shown in the flows list



WORLD_COMPANY Sites Flows

Flows (2012-07-02 19:07)

Local Sites		
Name	LAN	WAN
ALL	1.11kbps	0.42kbps
Paris	0.47kbps	0.19kbps
Boulder	0.22kbps	0.07kbps
Atlanta	0.19kbps	0.07kbps
Roma	0.17kbps	0.07kbps
Madrid	0.15kbps	0.05kbps
Coventry	0.08kbps	0.03kbps

Remote Sites		
Name	LAN	WAN
ALL	0.73kbps	0.29kbps
Santa Rosa	0.24kbps	0.08kbps
Barcelona	0.17kbps	0.09kbps
Paris	0.17kbps	0.07kbps
Georgetown	0.1kbps	0.03kbps
Barquisimeto	0.04kbps	0.02kbps
Belem2	0kbps	0kbps

Application Groups		
Name	LAN	WAN
ALL	13.2kbps	5.09kbps
Internet	8.21kbps	3.16kbps
Intranet	4.84kbps	1.86kbps
MailCollaborative	0.17kbps	0.07kbps
other	0kbps	0kbps
VideoStreaming	0kbps	0kbps
NetworkServices	0kbps	0kbps

Applications		
Name	LAN	WAN
ALL	0.17kbps	0.07kbps
SMTP	0.17kbps	0.07kbps
IMAP	0kbps	0kbps
POP3	0kbps	0kbps
Lotus Notes	0kbps	0kbps
Exchange	0kbps	0kbps

Topology						Classification							
Local		⇔	Remote							Thr. (kbps)			
Site	User Subnet		Site	User Subnet	EQS	Application Group	Application	Criticality	Sens.	Thr.	Good	Sess.	Loss (%
Roma		⇐	Paris.La Defens		10	MailCollaborative	SMTP	Low	Rout.	0.17	0.16	0.67	0.00

Page 1 of 1 Displaying 1 - 1 of 1 30 100 200

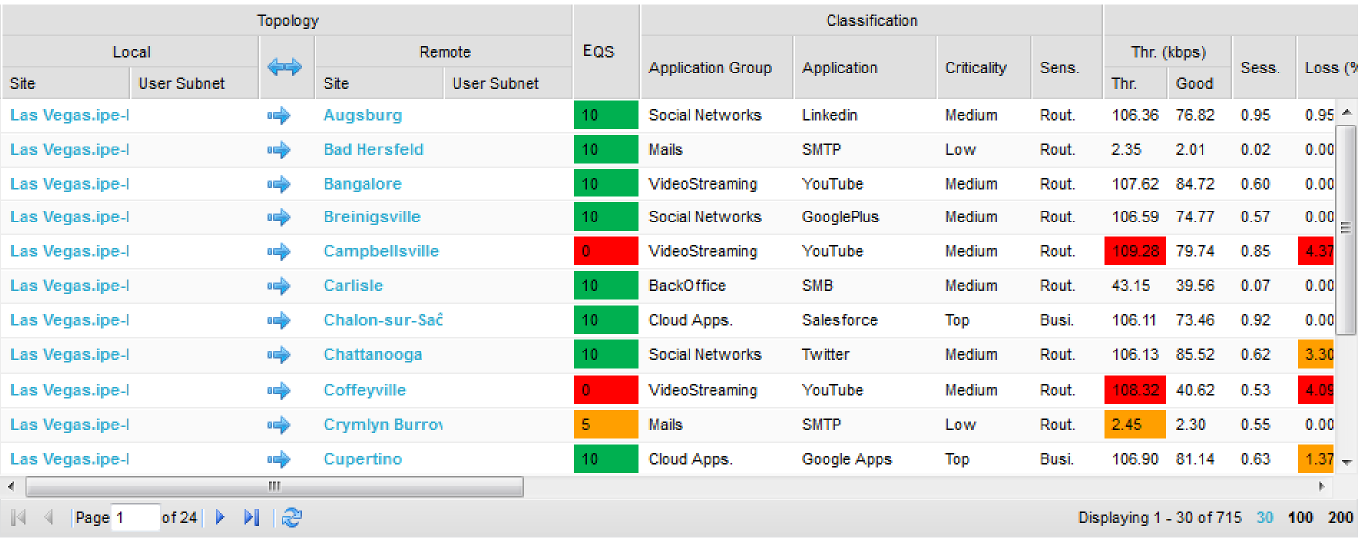
Application Flows - Detailed flows list

The Detailed flows list shows a table with each active flow displayed on a separate line. A flow becomes active and is displayed in the window as soon as a packet belonging to it is detected during the session.

You can toggle between this view and the flows map with the Detail / Map button.

Both views are different representations of the same data, with the same filters applied.

Flows - Application flows:



Topology					EQS	Classification							
Local		↔	Remote			Application Group	Application	Criticality	Sens.	Thr. (kbps)		Sess.	Loss (%
Site	User Subnet		Site	User Subnet						Thr.	Good		
Las Vegas.ipe-l		➡	Augsburg		10	Social Networks	Linkedin	Medium	Rout.	106.36	76.82	0.95	0.95
Las Vegas.ipe-l		➡	Bad Hersfeld		10	Mails	SMTP	Low	Rout.	2.35	2.01	0.02	0.00
Las Vegas.ipe-l		➡	Bangalore		10	VideoStreaming	YouTube	Medium	Rout.	107.62	84.72	0.60	0.00
Las Vegas.ipe-l		➡	Breinigsville		10	Social Networks	GooglePlus	Medium	Rout.	106.59	74.77	0.57	0.00
Las Vegas.ipe-l		➡	Campbellsville		0	VideoStreaming	YouTube	Medium	Rout.	109.28	79.74	0.85	4.37
Las Vegas.ipe-l		➡	Carlisle		10	BackOffice	SMB	Medium	Rout.	43.15	39.56	0.07	0.00
Las Vegas.ipe-l		➡	Chalon-sur-Saĉ		10	Cloud Apps.	Salesforce	Top	Busi.	106.11	73.46	0.92	0.00
Las Vegas.ipe-l		➡	Chattanooga		10	Social Networks	Twitter	Medium	Rout.	106.13	85.52	0.62	3.30
Las Vegas.ipe-l		➡	Coffeyville		0	VideoStreaming	YouTube	Medium	Rout.	108.32	40.62	0.53	4.09
Las Vegas.ipe-l		➡	Crymlyn Burrov		5	Mails	SMTP	Low	Rout.	2.45	2.30	0.55	0.00
Las Vegas.ipe-l		➡	Cupertino		10	Cloud Apps.	Google Apps	Top	Busi.	106.90	81.14	0.63	1.37

Page 1 of 24

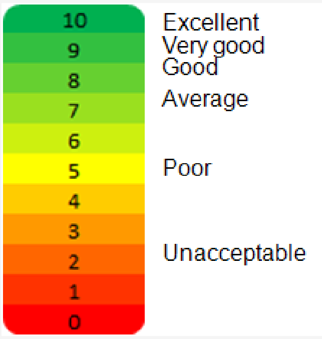
Displaying 1 - 30 of 715 30 100 200

The table contains the following columns:

Topology	
Local Site	name of the selected Appliance
Local User Subnet	name of the User subnet on the local Site (this field is empty if the local IP address does not belong to any User subnet defined on the Site)
↔	direction of the flow: ➡ outgoing (the local Site is the source) or ⬅ incoming (the local Site is the destination)
Remote Site	name of the remote Appliance (where the flow is going to or coming from)
Remote User Subnet	name of the remote User subnet
EQS	

Experience Quality Score of the flow: score between 0 (extremely bad quality) and 10 (excellent quality), displayed with two decimals.

The color of the field also represents the quality, with the following meaning:



> **Note:** Note: Excellent, Very good, etc., are only a *typical* interpretation of the EQS with *typical* parameters. It may vary according to the users' sensibility and according to the QoS profile parameters.

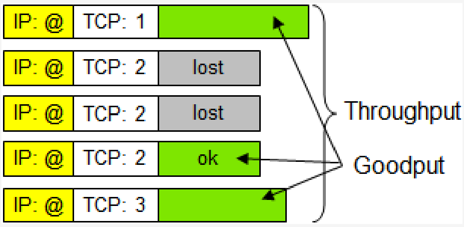
When the EQS is not good, the parameters (delay, jitter, loss, etc.) that triggered an average or a bad quality score are also highlighted with the same color, so that you can easily find which parameters objectives were not met (yellow) or which parameters maximum values were exceeded (red).

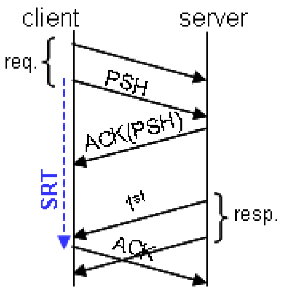
100 is a reserved value used when the EQS cannot be computed.

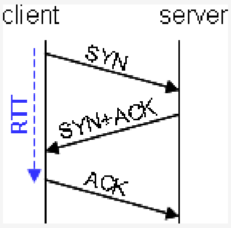
The quality of a flow cannot be computed when all the three following conditions are met:

- it is a real time flow (the bandwidth is not a criteria) or the bandwidth objective of the flow is not met (the quality is measured thanks to the other parameters),
- the flow is not qualified (D/J/L cannot be measured),
- the flow runs over UDP (RTT, TCP retransmission and SRT cannot be measured either) or those parameters are not activated in the QoS profile.

Classification	
Application Group	name of the Application Group where the flow is classified
Application	name of the application

Criticality	criticality level of the flow (Top, High, Medium or Low)
LAN	
Thr. (kbps)	LAN throughput (number of bits per second sent at the IP layer level) Good: LAN goodput (number of useful bits received at the application layer i.e. payload of the TCP and UDP packets received on the downstream side; retransmitted, out of sequence and lost packets are not counted). Throughput vs Goodput, example:  IP: @ TCP: 1 IP: @ TCP: 2 lost IP: @ TCP: 2 lost IP: @ TCP: 2 ok IP: @ TCP: 3 Throughput Goodput
Sess.	number of sessions, represented by the average activity for the duration of the Correlation Record (by default: T = 1 minute). For example, 1 session running during T plus 1 session running during half this period of time will give 1 + 0.5 = 1.5 session. A session is identified by the following parameters: • for TCP or UDP: source address, destination address, protocol (TCP or UDP), source port and destination port. • for others protocols over IP (for example ICMP): source address, destination address, protocol.
Loss (%)	LAN loss rate (measured between the LAN port of the source Appliance and the LAN port of the destination Appliance)
Delay (ms)	LAN one-way-delay (in ms) measured between the LAN port of the source Appliance and the LAN port of the destination Appliance • Min: minimum LAN one-way-delay • Avg: average LAN one-way-delay • Max: maximum LAN one-way-delay
Jitter (ms)	LAN jitter (delay variation measured between the LAN port of the source Appliance and the LAN port of the destination Appliance)
WAN	
Thr. (kbps)	WAN throughput (number of bits per second sent at the IP layer

	level)
Loss (%)	WAN loss rate (measured between the WAN port of the source Appliance and the WAN port of the destination Appliance)
Delay (ms)	WAN one-way-delay (in ms) measured between the WAN port of the source Appliance and the WAN port of the destination Appliance • Min: minimum WAN one-way-delay • Avg: average WAN one-way-delay • Max: maximum WAN one-way-delay
Jitter (ms)	WAN jitter (delay variation measured between the WAN port of the source Appliance and the WAN port of the destination Appliance)
Comp	
Ratio	compression ratio for the flow (when applicable)
TCP	
SRT (ms)	The Server Response Time measures the delay (in ms) between the last packet sent by the client during a request (PSH) and the emission of the acknowledgement to the first packet received from the server (ACK). When an Appliance is installed on the client side, it measures this response time and reports it to **SALSA domain configuration** server; otherwise, it is the Appliance installed on the server side that does it (and the measurement is made between the reception of the PSH and the reception of the ACK). If the same Appliance does not see the two ways of the TCP connection (in case of a cluster with asymmetric routing), the SRT will not be measured unless the two Appliances of the cluster are connected together and the ASR feature is configured.  client server req. PSH ACK(PSH) SRT 1st resp. ACK • Min: shortest Server Response Time • Avg: average Server Response Time • Max: longest Server Response Time

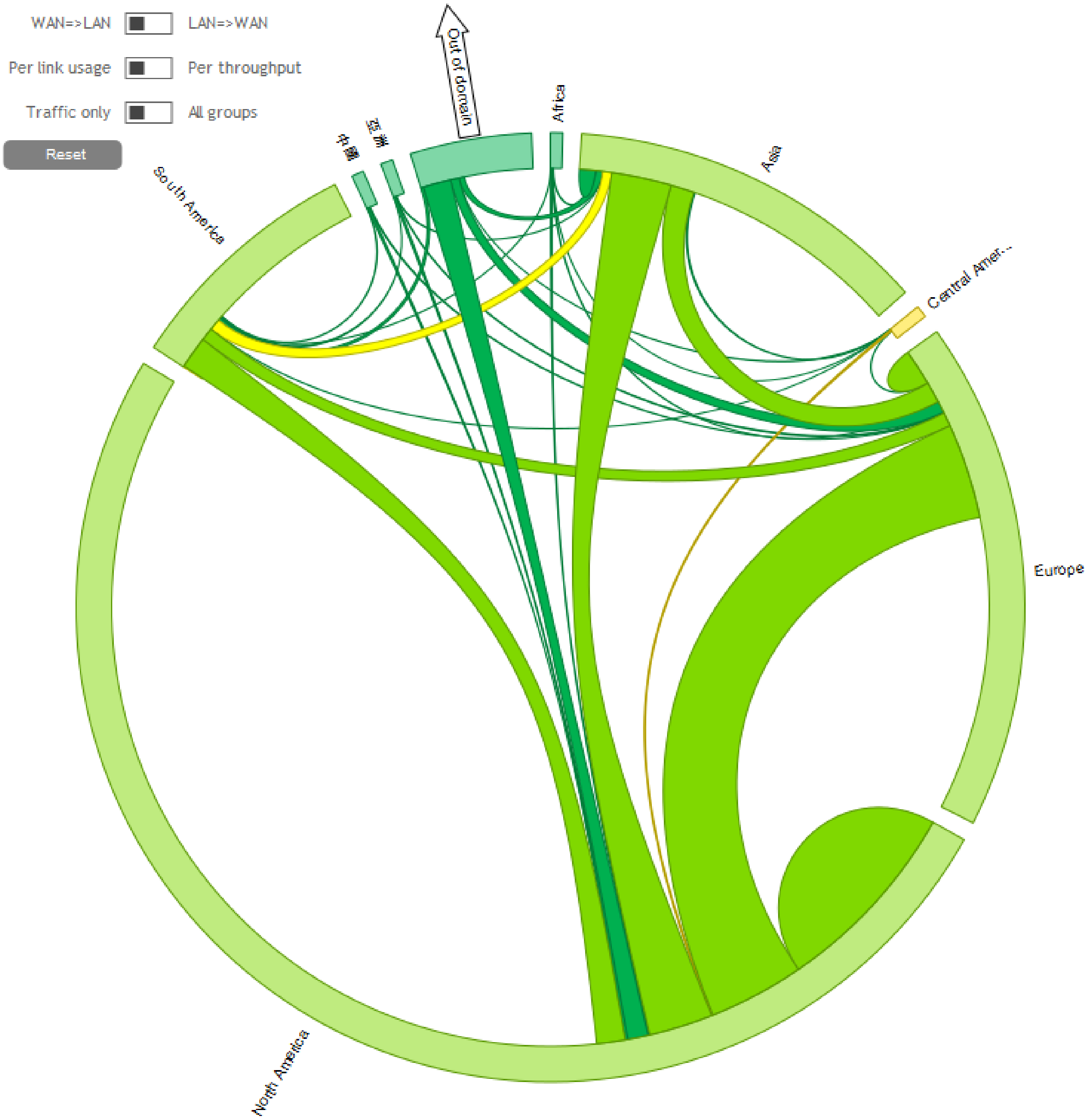
RTT (ms)	The Round Trip Time measures the time of establishment of a TCP connection (3-way handshake: SYN, SYN+ACK, ACK), i.e the delay (in ms) between the emission of the SYN and the emission of the ACK. When an Appliance is installed on the client side, it measures this RTT and reports it to **SALSA domain configuration** server; otherwise, it is the Appliance installed on the server side that does it (and the measurement is made between the reception of the SYN and the reception of the ACK). If the same Appliance does not see the two ways of the TCP connection (in case of a cluster with asymmetric routing), the RTT will not be measured unless the two Appliances of the cluster are connected together and the ASR feature is configured.  • Min: shortest Round Trip Time • Avg: average Round Trip Time • Max: longest Round Trip Time
Ret. (%)	percentage of TCP retransmissions
Comp.	compression status: Yes if the flow is compressed, No otherwise
Accu.	accuracy of the current measurement: High if the flow is qualified, Low otherwise
Al.	this field indicates, when at 'yes', the presence of an alarm on the Appliance. Check its status for further information. In case of alarm, the correlation records are ignored.
TOS / DSCP	
	name of the TOS / DSCP value used to recognize the application, when applicable

This table is refreshed about every minute (according to the Appliance collect period option).

Application Flows - Flows map

The flows map is a dynamic and interactive chord diagram of the flows.

You can toggle between this view and the Detailed flows list with the Detail / Map button. Both views are different representations of the same data, with the same filters applied.



It displays the flows matrix with a hierarchical structure:

1 Folders (e.g. continents*),

2 Subfolders (e.g. countries*),

3 Sites (e.g. called by the name of the cities),

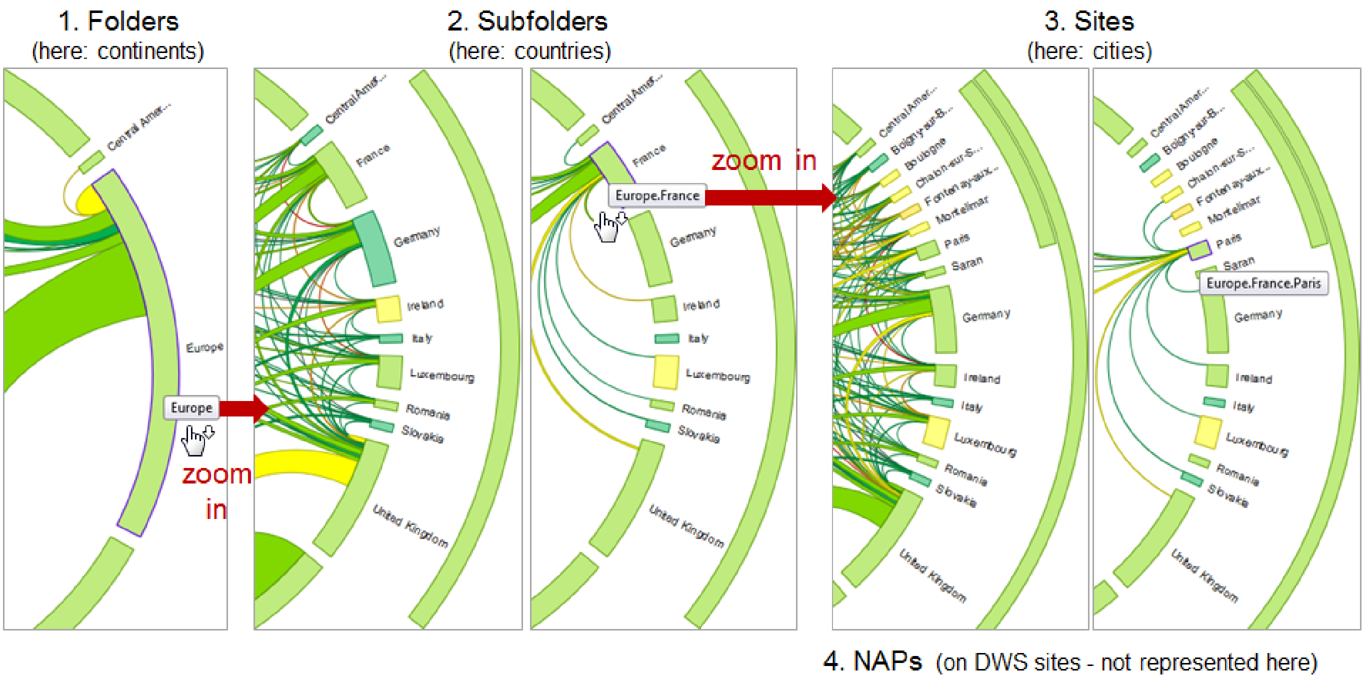
4 NAPs (if the Site has several NAPs, when Dynamic WAN Selection is used).

* Folders and Subfolders are defined in the Appliances creation window. For instance (as in the example above), they can be used to sort the Sites continent by continent (Folders = continents), then country by country (Subfolders = countries).

You can zoom in and zoom out these four levels:

- zoom in by clicking on the arcs or on their names (in the example below: Europe > France > Paris); the cursor shows a down arrow: ; the zoom level is represented by external arcs
- zoom out by clicking on the external arcs; the cursor shows an up arrow:

Zooming in the flows map:



1. Folders (here: continents)

2. Subfolders (here: countries)

3. Sites (here: cities)

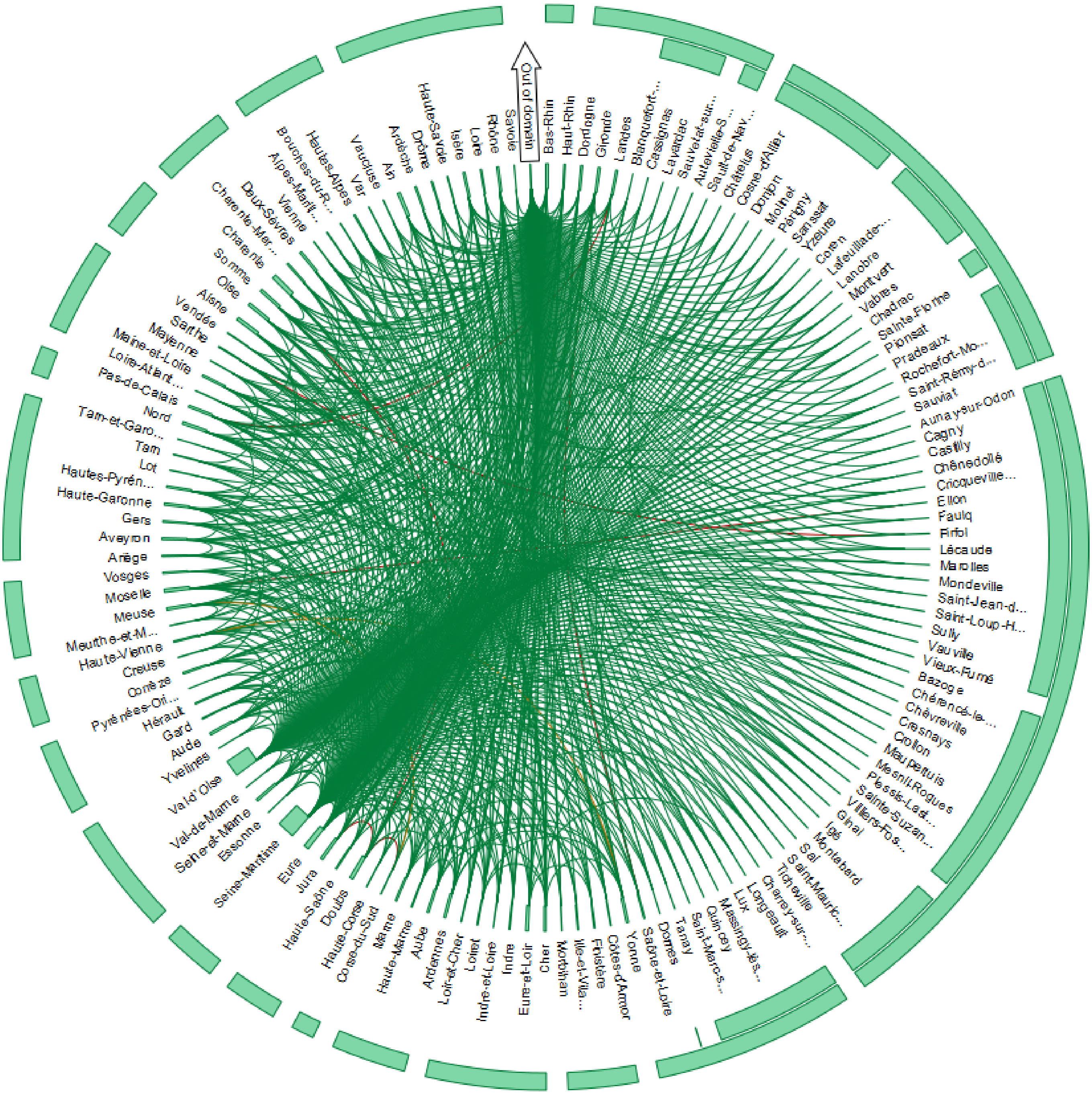
4. NAPs (on DWS sites - not represented here)

Hovering the mouse on any arc (without clicking down) shows the flows between that arc and the others only (instead of the whole matrix between all pairs of arcs) (see below).

The colors of the flows and their extremities indicate the quality (between green (EQS = 10) and red (EQS = 0)). The color is strong for the flows, pale for the extremities. The exact EQS of both the flows and their extremities can be displayed by hovering the mouse on these objects.

There is a maximum number of flows that can be displayed simultaneously (a diagram showing thousands of flows would be unreadable anyway, so it would be completely useless). If this maximum number is exceeded, the map is replaced by a message telling you that there are too many groups to display, and that you should refine your filter: use the filters to concentrate on the flows you want to see.

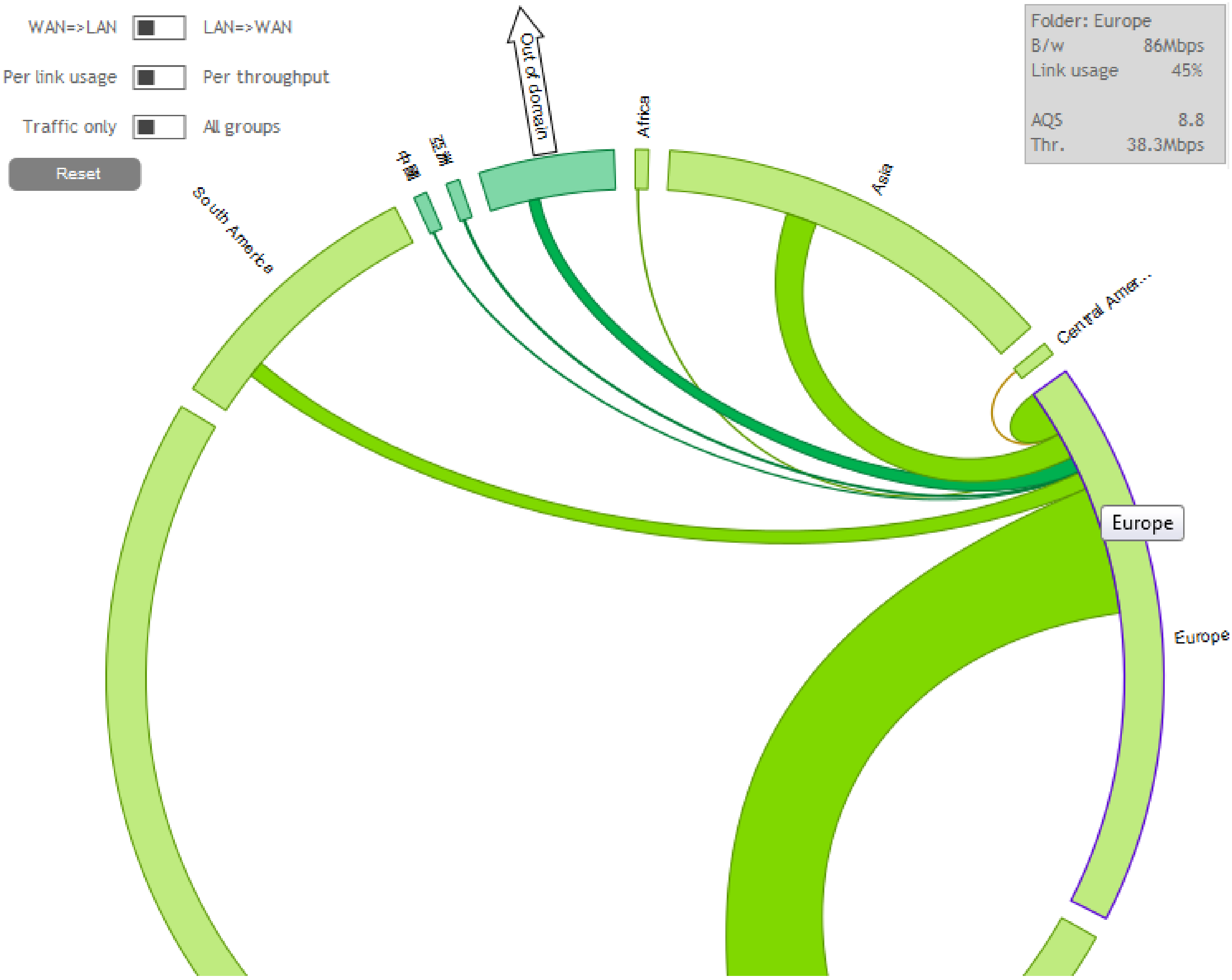
Flows map with too much zoom and too many chords displayed:



When the map is opened, it shows the Folders level (e.g. the flows between continents). Out of Domain is displayed on its own, indicated by an arrow.

Hovering the mouse on an extremity hides the traffic between the other extremities and displays this extremity's details (volume and quality) in a pop-up. Here for instance, you can see the traffic between Asia and the rest of the world.

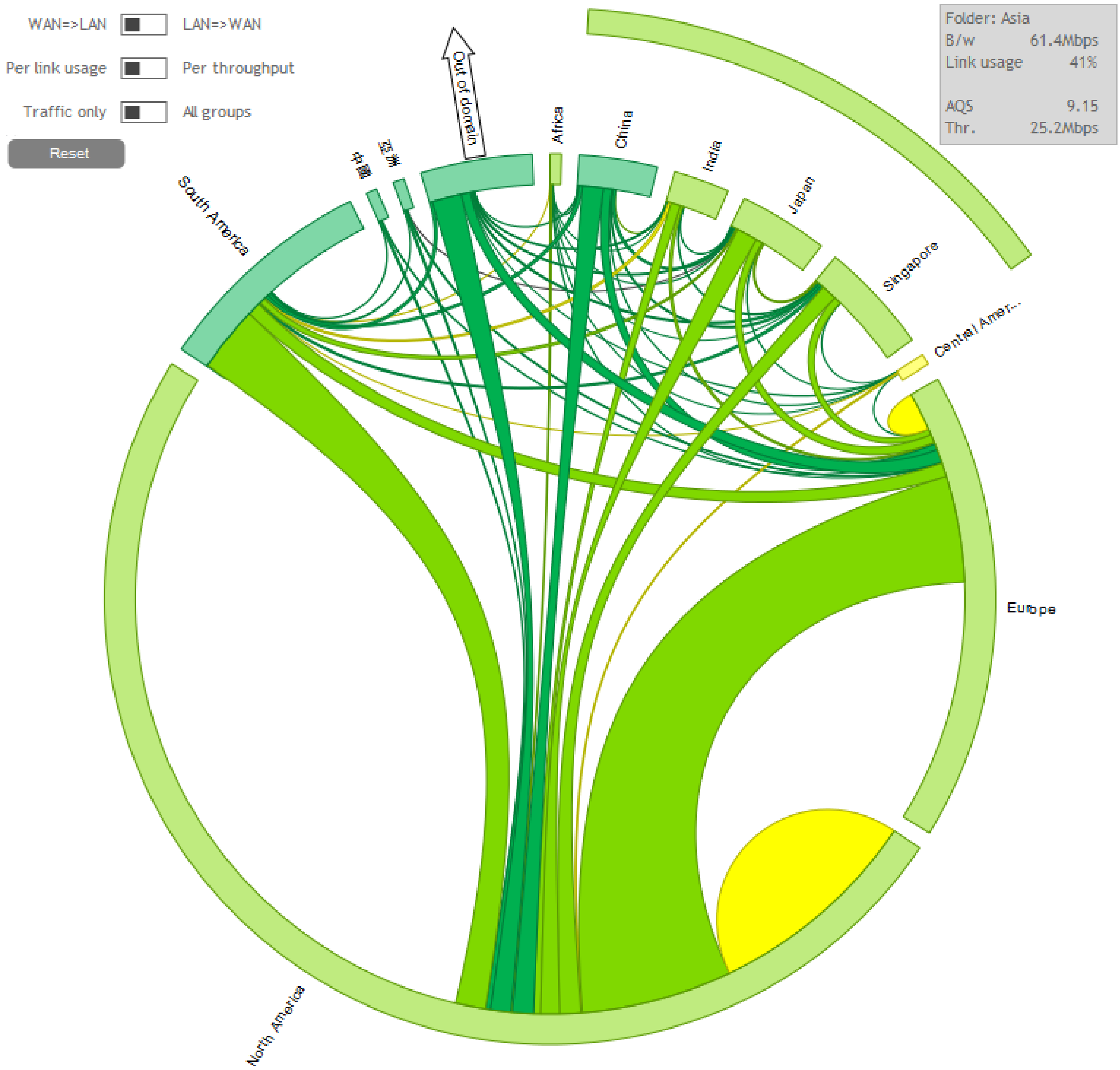
Flows map, showing the traffic flows of one extremity:



Folder: Europe
B/w 86Mbps
Link usage 45%
AQS 8.8
Thr. 38.3Mbps

Clicking on an extremity or on its name (e.g. Asia) allows zooming in this extremity (e.g. continent), breaking it up into the next level (here: countries). Here for instance, we are zooming into Asia to see the traffic between each Asian country and the rest of the world (still displayed as continents).

Flows map, zooming from a continent (folder) into its countries (subfolders):



WAN=>LAN ■ LAN=>WAN

Per link usage ■ Per throughput

Traffic only ■ All groups

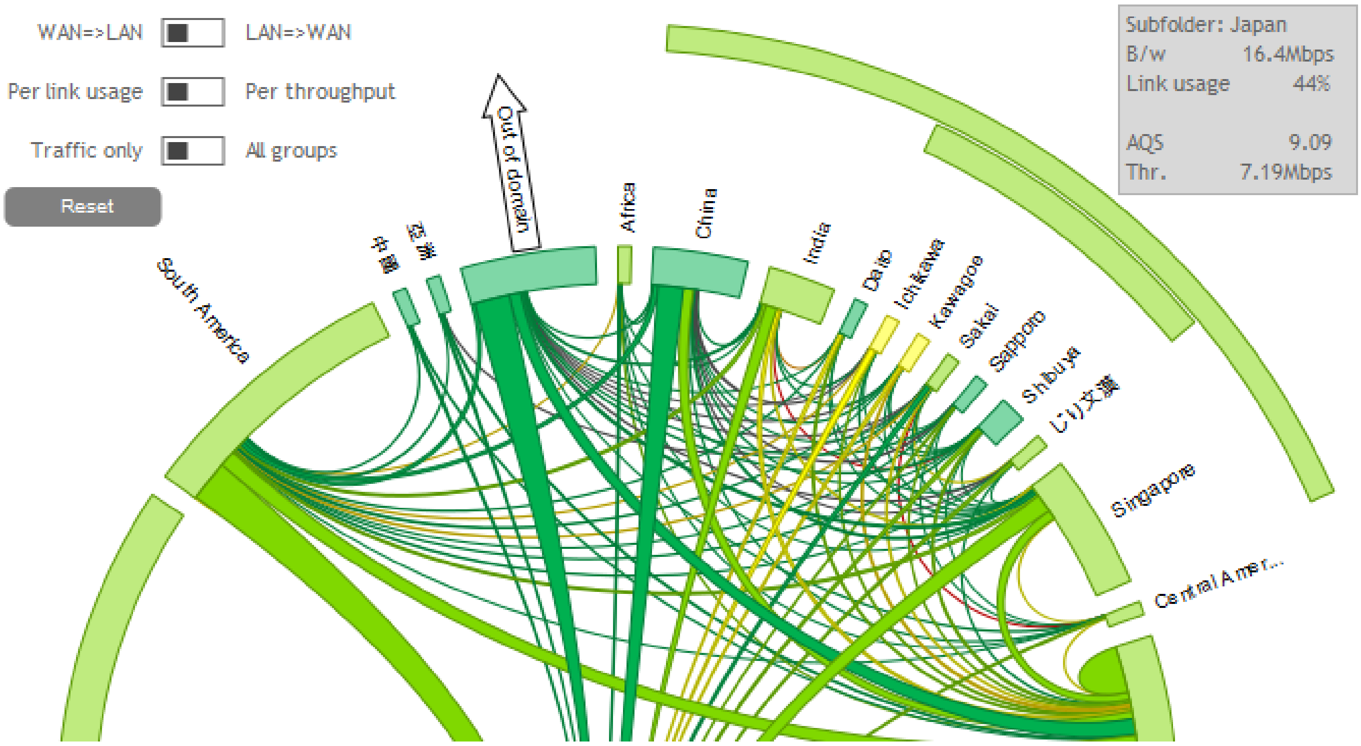
Reset

Folder: Asia
B/w 61.4Mbps
Link usage 41%

AQS 9.15
Thr. 25.2Mbps

It is possible to zoom in again, from a country (subfolder) to its Sites.

Flows map, zooming from country (subfolder) to its Sites:



Subfolder: Japan
B/w 16.4Mbps
Link usage 44%

AQS 9.09
Thr. 7.19Mbps

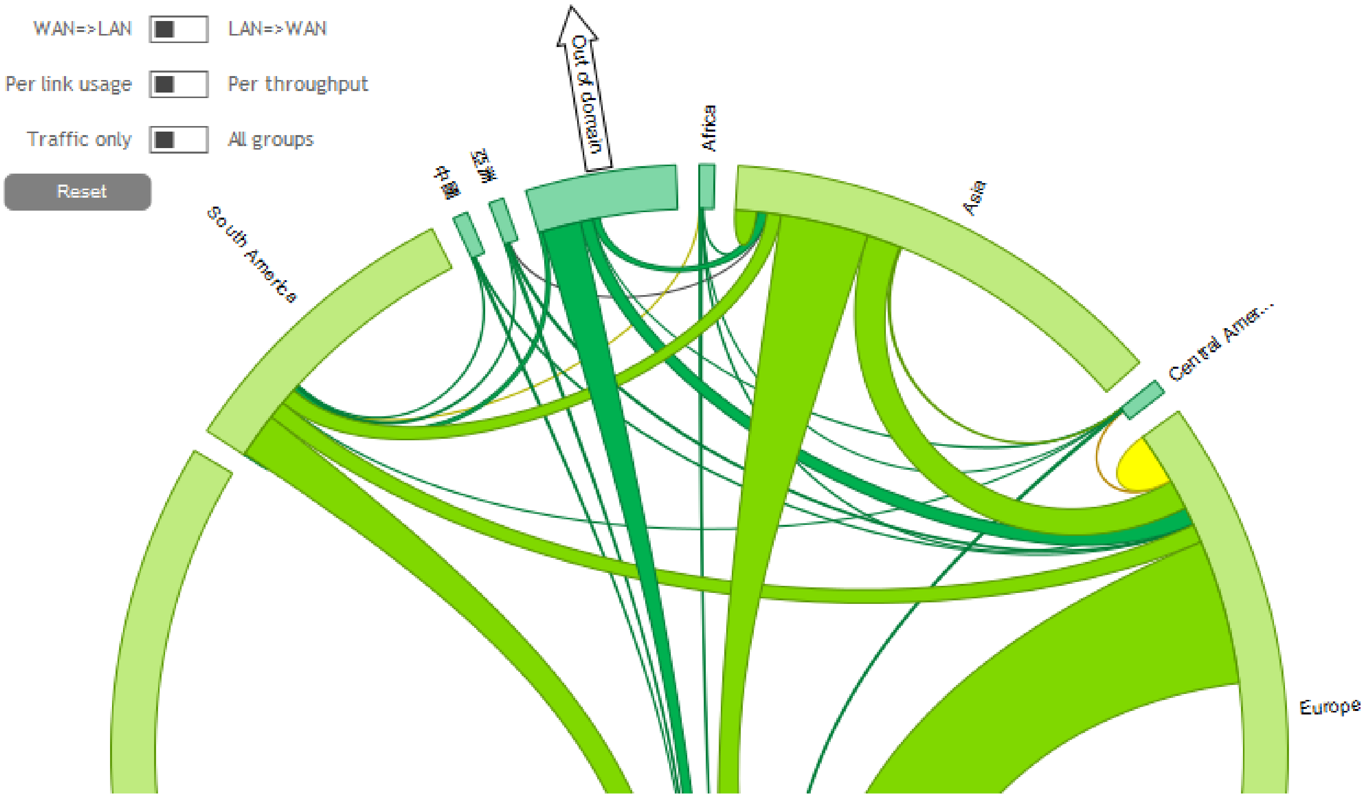
... and from a Site to its NAPs (when there are several NAPs on the Site).

Use the Reset button to reset the view.

The three switches at the top left of the diagram allow changing some display settings: LAN=>WAN / WAN=> LAN, Per link usage / Per throughput and Traffic only / All groups.

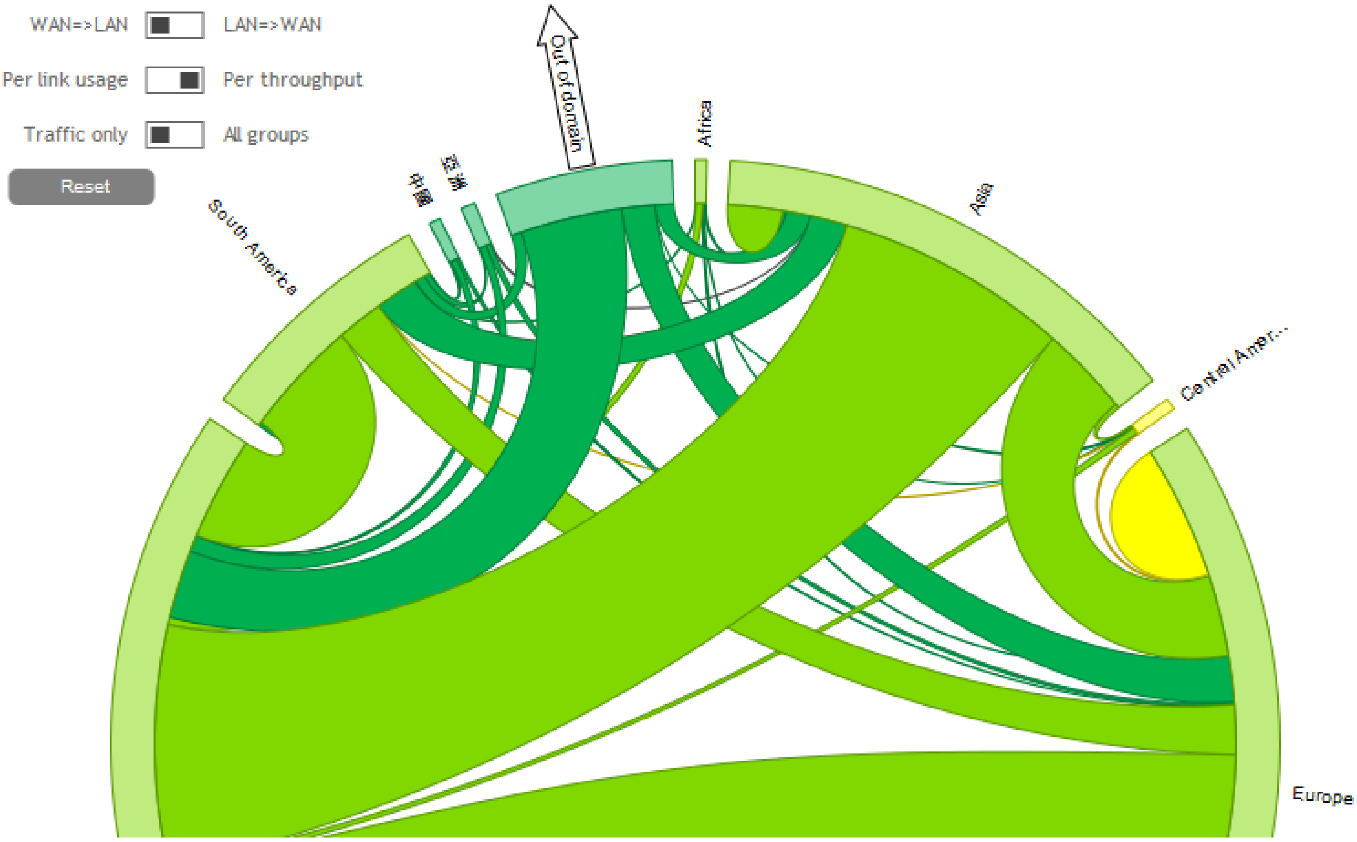
By default, the three switches are in the LAN=>WAN, Per link usage and Traffic only positions:

Flows map, with the three switches in their default positions



- The [LAN=>WAN / WAN=> LAN] switch allows changing the direction of the displayed flows.
- [Per link usage / Per throughput] allows showing traffic chords with a size proportional to:
  - the links (Per link usage); arc = available bandwidth; chords = traffic; in the example above, you can see that in South America, about a third of the bandwidth is used (you can read the exact percentage by hovering the mouse on the arcs);
  - the throughput (Per throughput); arc = sum of the chords = total traffic: the traffic is displayed independently of the available bandwidth.

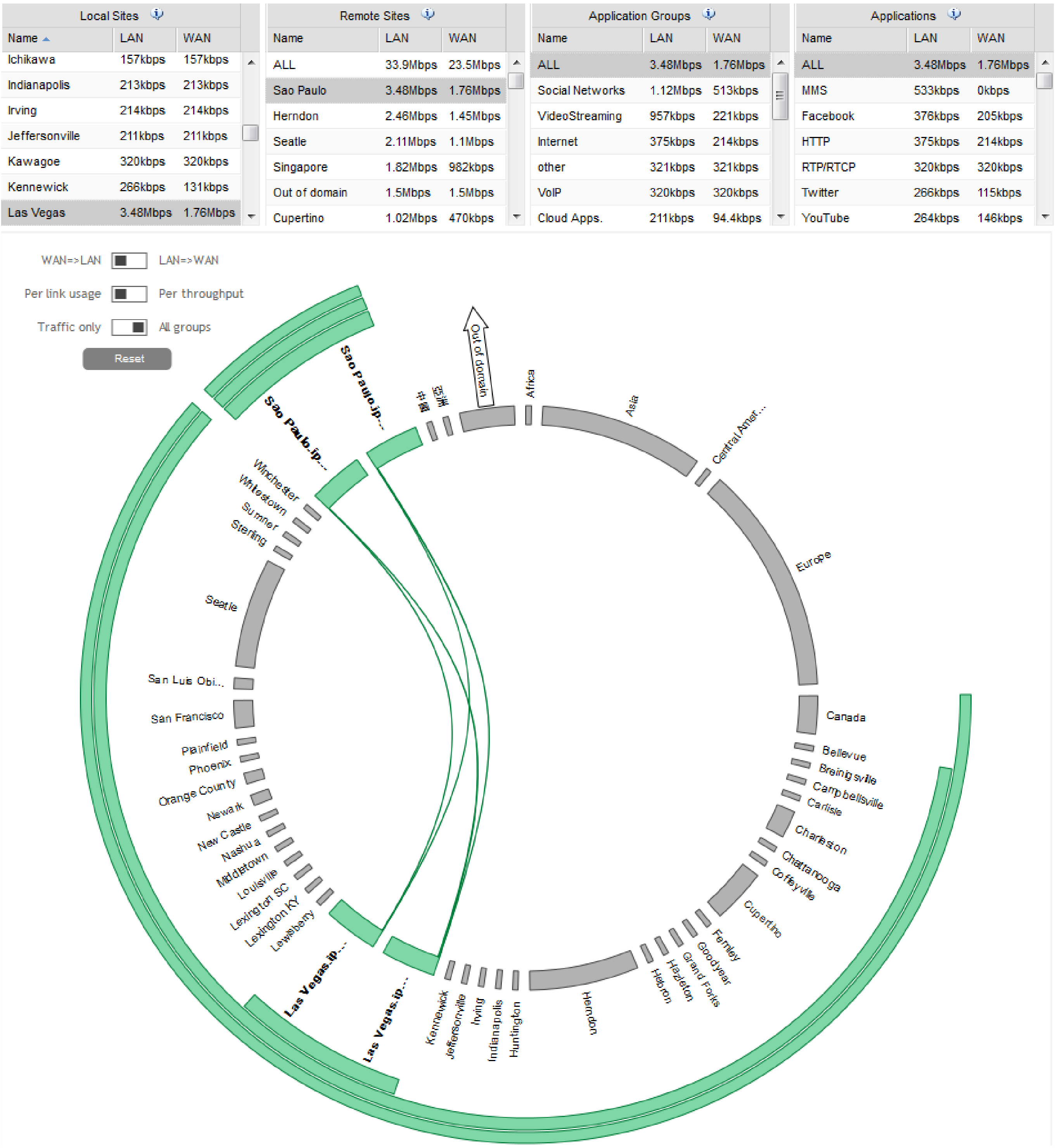
Flows map, displaying the link usage (Per link usage):



- [Traffic only / All groups] allows displaying extremities with traffic matching the filters only (Traffic only) or all the groups where traffic is also present (but without matching the selected filters).

The three switches can be combined to display the desired information. Here for instance, you want to see the traffic from Las Vegas to Sao Paulo (LAN=>WAN) as a proportion of the links on these Sites (Per link usage), showing the other links as well (All groups), so that you can see what the traffic from Las Vegas to Sao Paulo represents.

Flows map, displaying the link usage between two Sites, on the whole Domain:



Local Sites

Name	LAN	WAN
Ichikawa	157kbps	157kbps
Indianapolis	213kbps	213kbps
Irving	214kbps	214kbps
Jeffersonville	211kbps	211kbps
Kawagoe	320kbps	320kbps
Kennewick	266kbps	131kbps
Las Vegas	3.48Mbps	1.76Mbps

Remote Sites

Name	LAN	WAN
ALL	33.9Mbps	23.5Mbps
Sao Paulo	3.48Mbps	1.76Mbps
Herndon	2.46Mbps	1.45Mbps
Seatle	2.11Mbps	1.1Mbps
Singapore	1.82Mbps	982kbps
Out of domain	1.5Mbps	1.5Mbps
Cupertino	1.02Mbps	470kbps

Application Groups

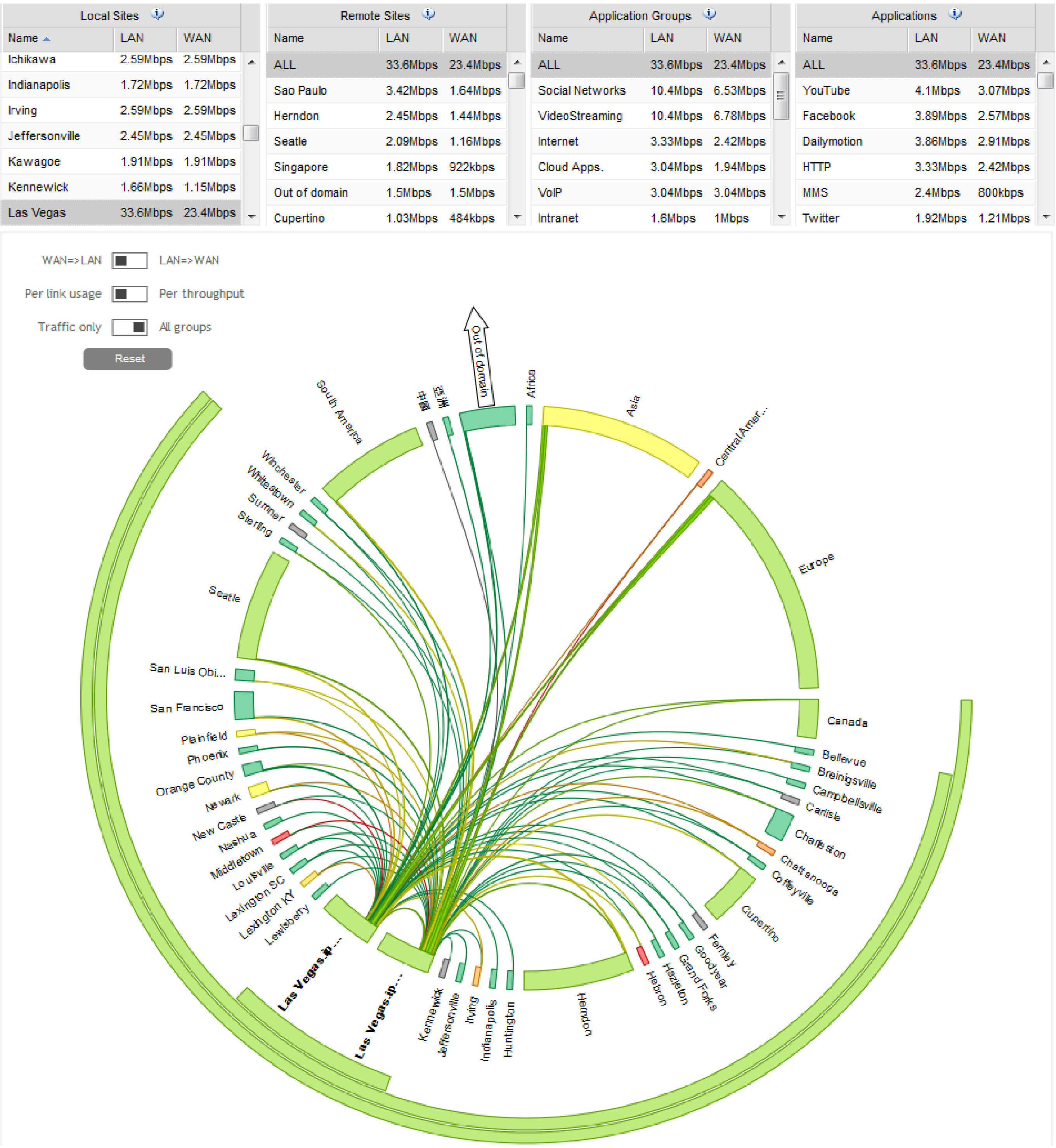
Name	LAN	WAN
ALL	3.48Mbps	1.76Mbps
Social Networks	1.12Mbps	513kbps
VideoStreaming	957kbps	221kbps
Internet	375kbps	214kbps
other	321kbps	321kbps
VoIP	320kbps	320kbps
Cloud Apps.	211kbps	94.4kbps

Applications

Name	LAN	WAN
ALL	3.48Mbps	1.76Mbps
MMS	533kbps	0kbps
Facebook	376kbps	205kbps
HTTP	375kbps	214kbps
RTP/RTCP	320kbps	320kbps
Twitter	266kbps	115kbps
YouTube	264kbps	146kbps

By removing the Remote Sites filter, you can now see, on the same diagram, the traffic from Las Vegas to all the remote sites (with the one between Las Vegas and Sao Paulo highlighted).

Flows map, displaying the link usage between a Site and all the remote ones:



Local Sites

Name ▲	LAN	WAN
Ichikawa	2.59Mbps	2.59Mbps
Indianapolis	1.72Mbps	1.72Mbps
Irving	2.59Mbps	2.59Mbps
Jeffersonville	2.45Mbps	2.45Mbps
Kawagoe	1.91Mbps	1.91Mbps
Kennewick	1.66Mbps	1.15Mbps
Las Vegas	33.6Mbps	23.4Mbps

Remote Sites

Name	LAN	WAN
ALL	33.6Mbps	23.4Mbps
Sao Paulo	3.42Mbps	1.64Mbps
Herndon	2.45Mbps	1.44Mbps
Seatle	2.09Mbps	1.16Mbps
Singapore	1.82Mbps	922kbps
Out of domain	1.5Mbps	1.5Mbps
Cupertino	1.03Mbps	484kbps

Application Groups

Name	LAN	WAN
ALL	33.6Mbps	23.4Mbps
Social Networks	10.4Mbps	6.53Mbps
VideoStreaming	10.4Mbps	6.78Mbps
Internet	3.33Mbps	2.42Mbps
Cloud Apps.	3.04Mbps	1.94Mbps
VoIP	3.04Mbps	3.04Mbps
Intranet	1.6Mbps	1Mbps

Applications

Name	LAN	WAN
ALL	33.6Mbps	23.4Mbps
YouTube	4.1Mbps	3.07Mbps
Facebook	3.89Mbps	2.57Mbps
Dailymotion	3.86Mbps	2.91Mbps
HTTP	3.33Mbps	2.42Mbps
MMS	2.4Mbps	800kbps
Twitter	1.92Mbps	1.21Mbps

WAN=>LAN ■□ LAN=>WAN

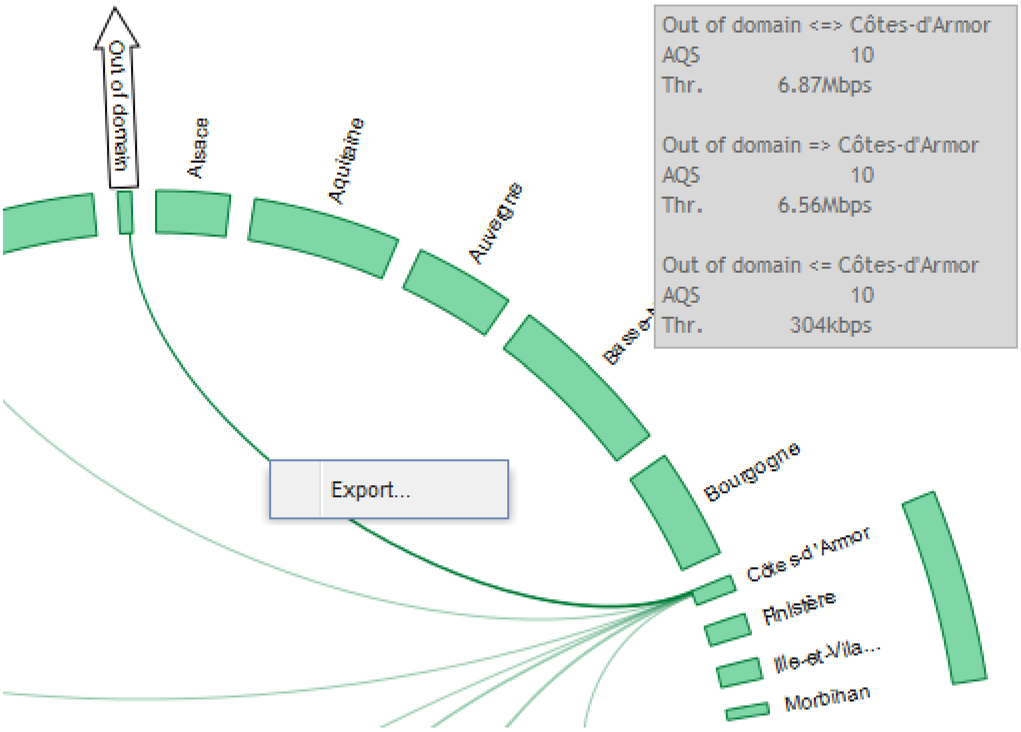
Per link usage ■□ Per throughput

Traffic only □■ All groups

At any level of the map, clicking on a chord opens the flows list, automatically filtered out to display the flows corresponding to the selected chord.

Exporting the maps

When right-clicking the map, a contextual menu enables you to export it, either as a graph (PNG format) or as raw data (CSV format):



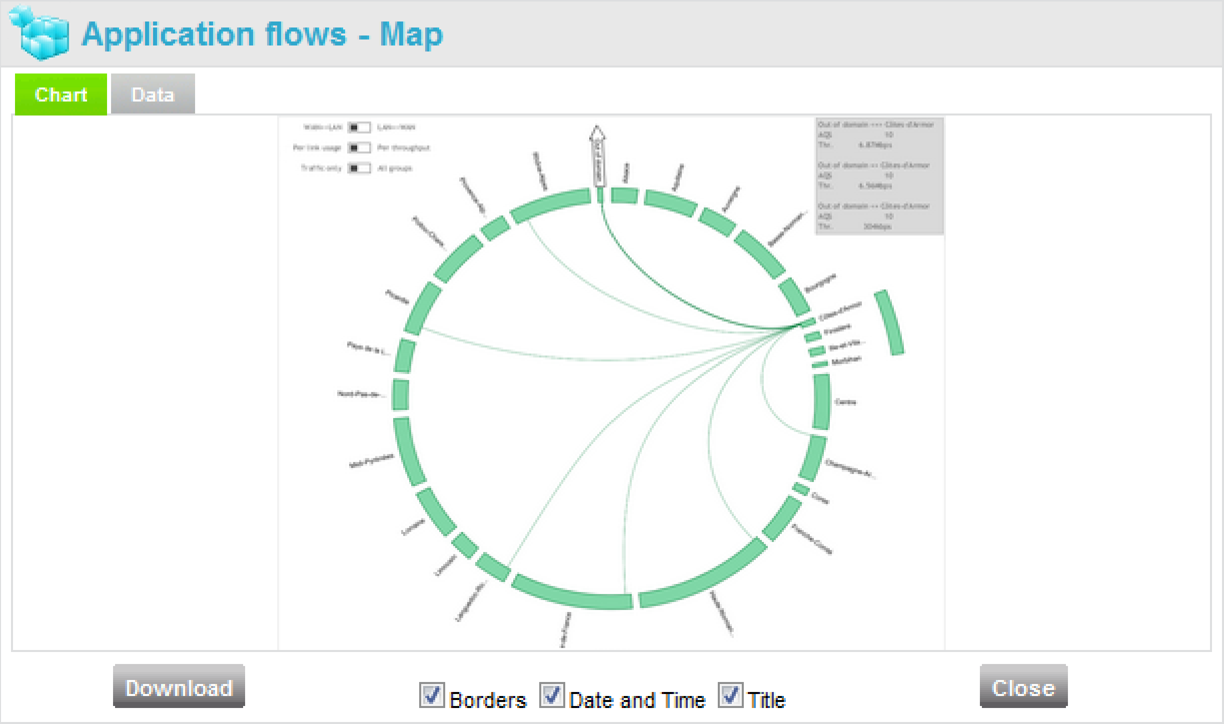
```
Out of domain <=> Côtes-d'Armor
AQS             10
Thr.        6.87Mbps

Out of domain => Côtes-d'Armor
AQS             10
Thr.        6.56Mbps

Out of domain <= Côtes-d'Armor
AQS             10
Thr.         304kbps
```

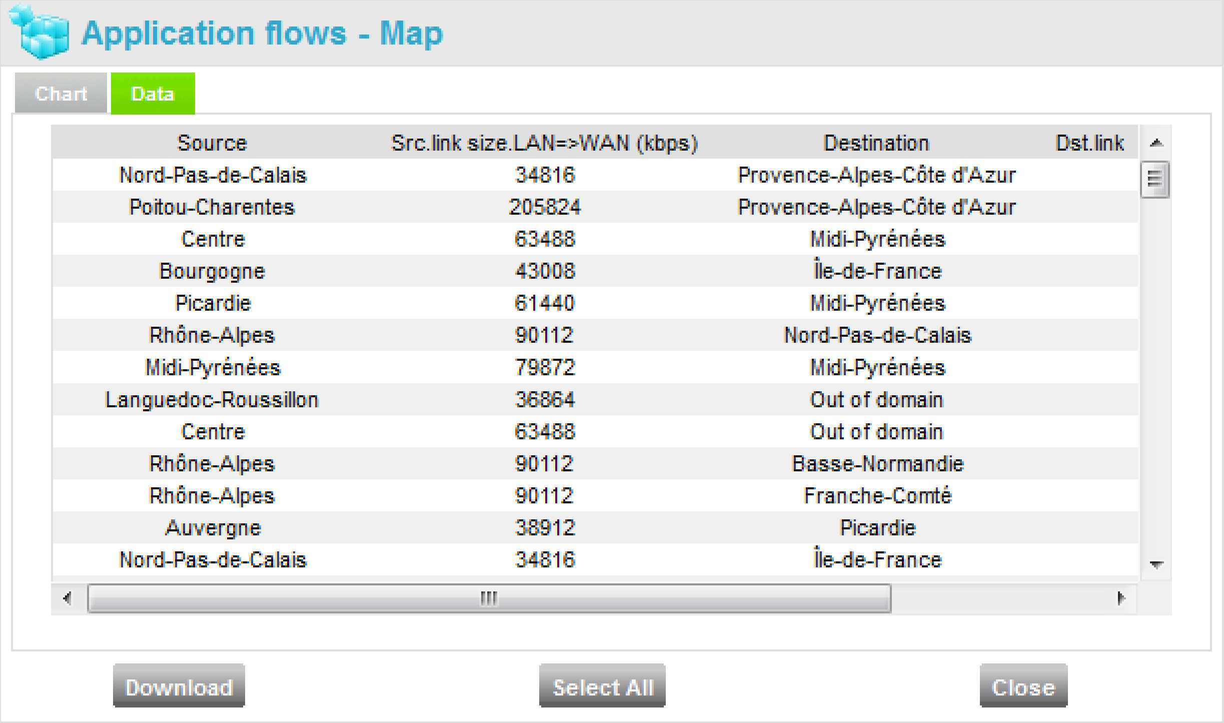
The frame that opens has two tabs:

- Chart, allowing to download the map as a PNG image:



Three check boxes allow displaying or hiding the Borders, the Date and Time and the Title.

- Data, allowing to download the map as CSV data:



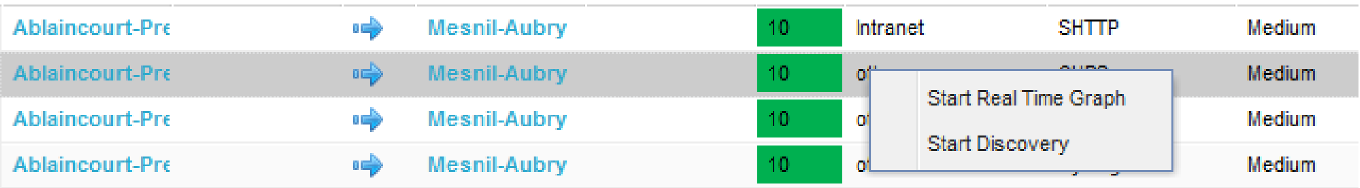
Source	Src.link size.LAN=>WAN (kbps)	Destination	Dst.link
Nord-Pas-de-Calais	34816	Provence-Alpes-Côte d'Azur	
Poitou-Charentes	205824	Provence-Alpes-Côte d'Azur	
Centre	63488	Midi-Pyrénées	
Bourgogne	43008	Île-de-France	
Picardie	61440	Midi-Pyrénées	
Rhône-Alpes	90112	Nord-Pas-de-Calais	
Midi-Pyrénées	79872	Midi-Pyrénées	
Languedoc-Roussillon	36864	Out of domain	
Centre	63488	Out of domain	
Rhône-Alpes	90112	Basse-Normandie	
Rhône-Alpes	90112	Franche-Comté	
Auvergne	38912	Picardie	
Nord-Pas-de-Calais	34816	Île-de-France	

In either case, use the Download button to download the data.

Real Time Graphs

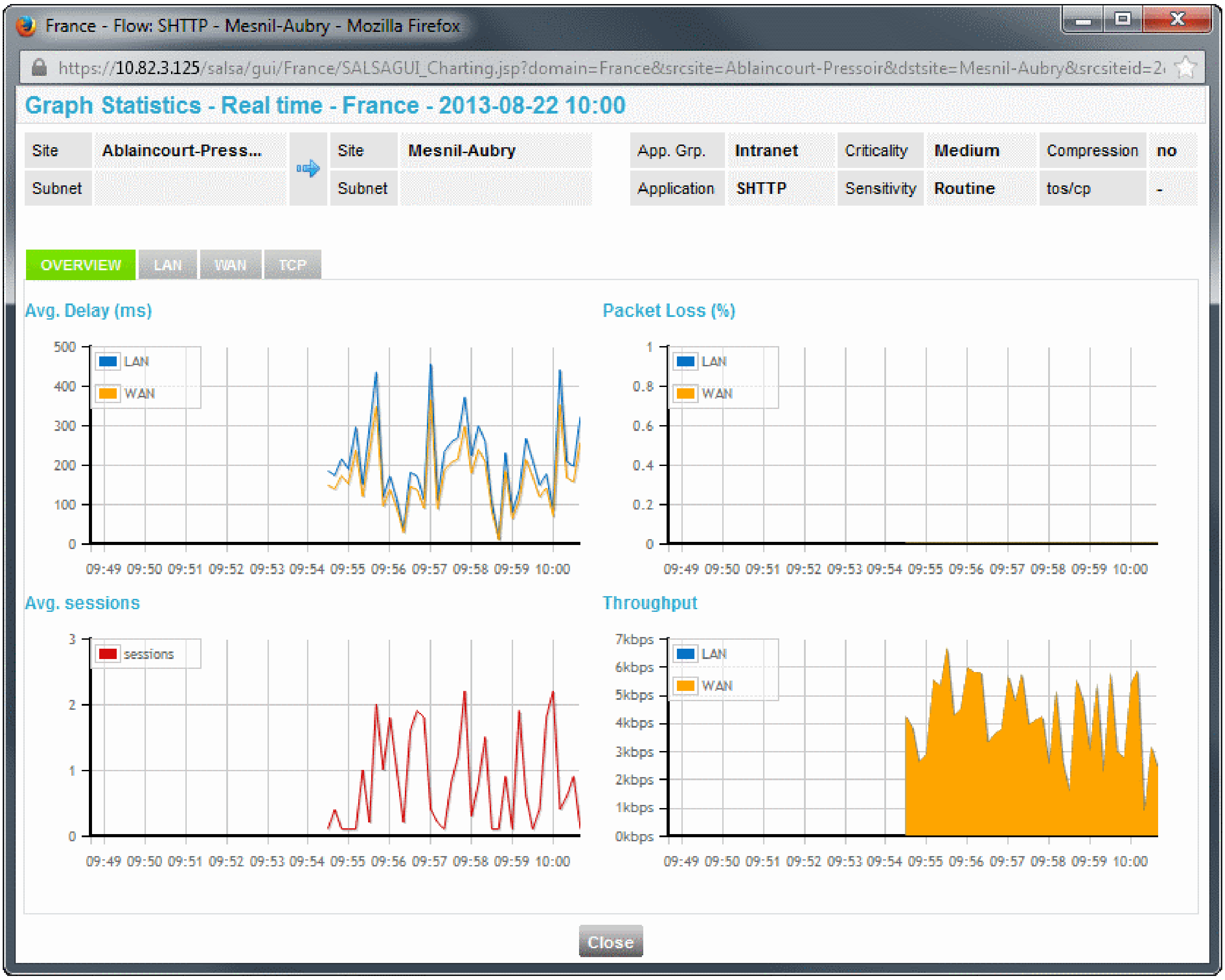
From any flow in the Detailed flows list described above, you can open a Real Time Graph which is a 12-minute window showing the evolution of the above metrics with additional polling every 10 seconds. You can open up to four graphs simultaneously.

To access the Real Time Graphs, right click on a flow and select Start Real Time Graph:



Ablaincourt-Pre	➪	Mesnil-Aubry	10	Intranet	SHTTP	Medium
Ablaincourt-Pre	➪	Mesnil-Aubry	10	o		Medium
Ablaincourt-Pre	➪	Mesnil-Aubry	10	o		Medium
Ablaincourt-Pre	➪	Mesnil-Aubry	10	o		Medium

Note: Pop-up windows must not be blocked in your web browser.



France - Flow: SHTTP - Mesnil-Aubry - Mozilla Firefox

https://10.82.3.125/salsa/gui/France/SALSAGUI_Charting.jsp?domain=France&srcsite=Ablaincourt-Pressoir&dstsite=Mesnil-Aubry&srcsiteid=2

Graph Statistics - Real time - France - 2013-08-22 10:00

Site	Ablaincourt-Press...	➪	Site	Mesnil-Aubry	App. Grp.	Intranet	Criticality	Medium	Compression	no
Subnet			Subnet		Application	SHTTP	Sensitivity	Routine	tos/cp	-

A Real Time Graph is empty when it starts. You can see some data after 10 to 20 seconds.

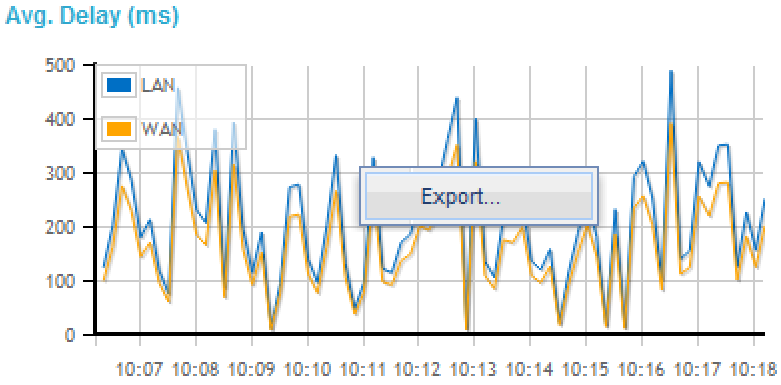
The graph window contains four tabs, and each tab is made of 4 graphs, displayed simultaneously:

Tab	Graphs	What is shown
Overview	Avg. Delay (ms)	LAN-to-LAN (in blue) and WAN-to-WAN (in orange) average delays
	Packet loss (%)	LAN-to-LAN (in blue) and WAN-to-WAN (in orange) packet losses
	Avg. sessions	Average number of sessions
	Throughput (kbps)	LAN-to-LAN (in blue) and WAN-to-WAN (in orange) Throughputs
LAN	Delay (ms)	LAN-to-LAN maximum (in red), average (in blue) and minimum (in green) delays
	Packet loss (%)	LAN-to-LAN packet loss
	Jitter (ms)	LAN-to-LAN jitter
	Throughput (kbps)	LAN-to-LAN layer 3 (in blue) and layer 4 (in green) throughputs
WAN	Delay (ms)	WAN-to-WAN maximum (in red), average (in blue) and minimum (in green) delays
	Packet loss (%)	WAN-to-WAN packet loss
	Jitter (ms)	WAN-to-WAN jitter
	Throughput (kbps)	WAN-to-WAN layer 3 throughput
TCP	SRT (ms)	Maximum (in red), average (in blue) and minimum (in green) Server Response Time
	RTT (ms)	Maximum (in red), average (in blue) and minimum (in green) Round Trip Time
	Retransmission (%)	TCP retransmissions
	Throughput (kbps)	Layer 3 (in blue) and layer 4 (in green) TCP throughputs

Note: In case of control and/or compression, the differences between LAN and WAN values may be very different.

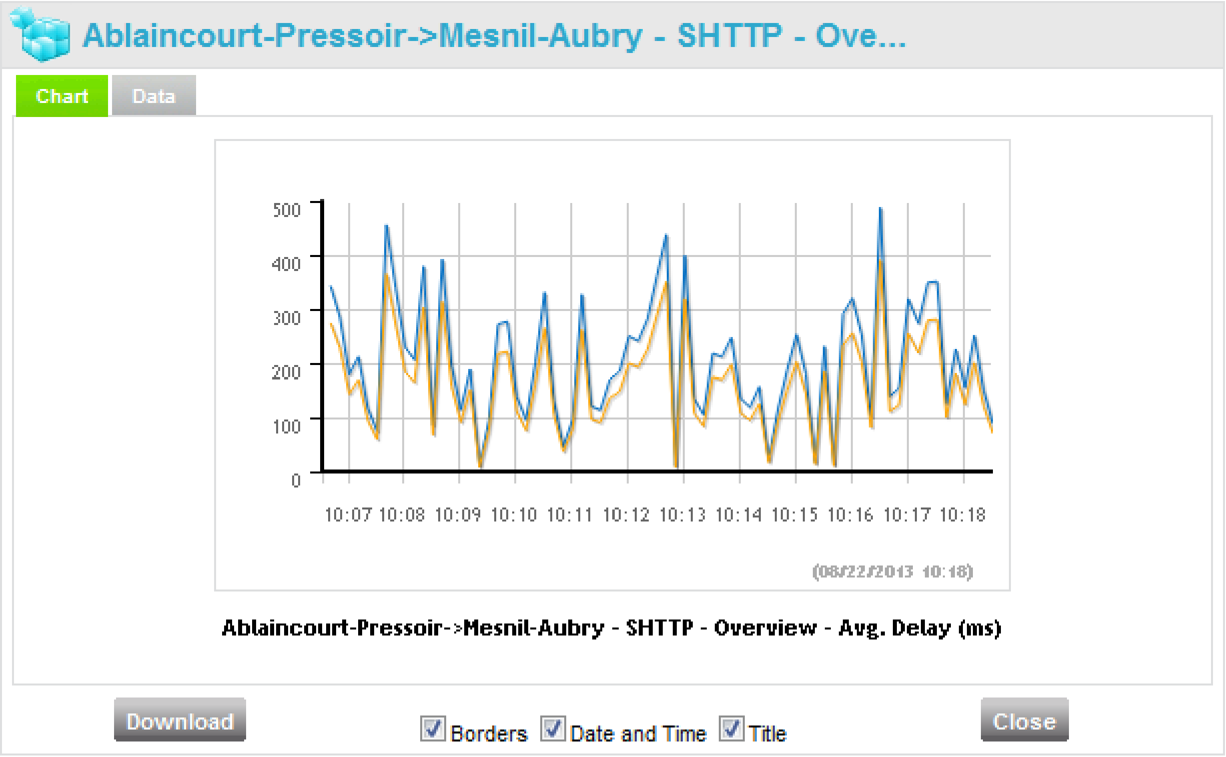
Exporting the graphs

By right-clicking any graph, you display a contextual menu enabling you to export the graph, either as a graph (PNG format) or as raw data (CSV format):



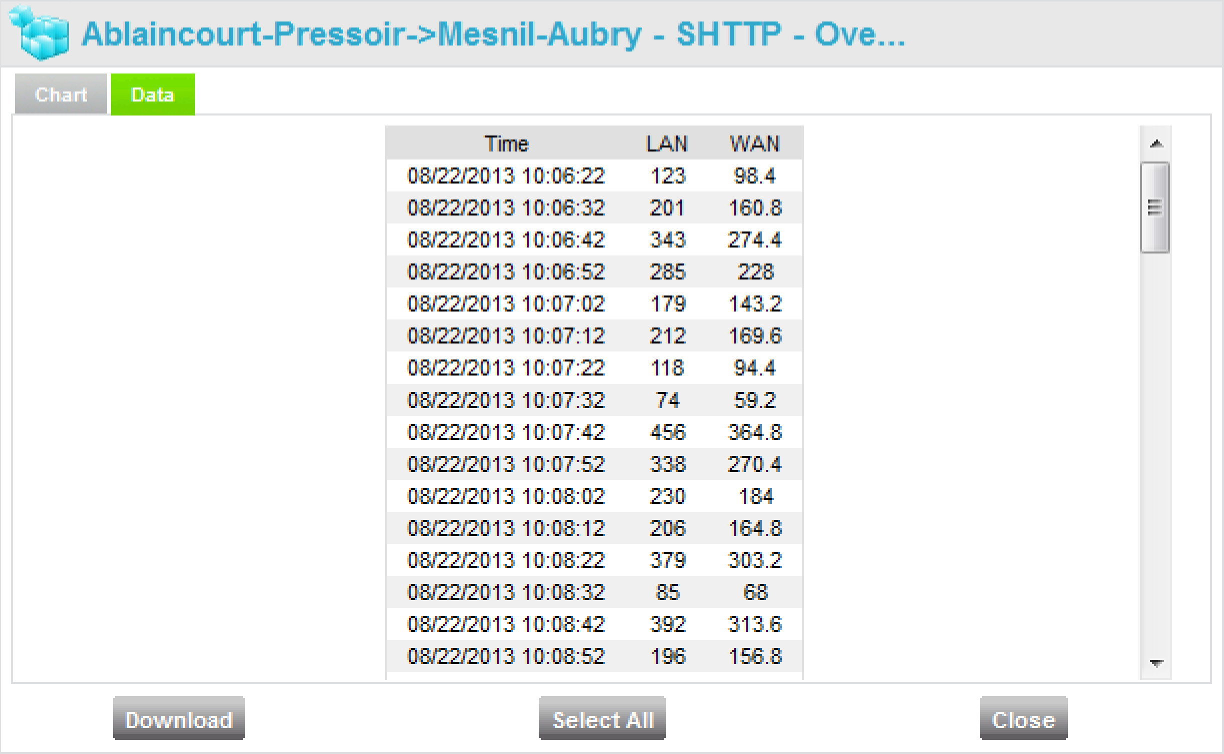
The frame that opens has two tabs:

- Chart, allowing to download the graph as a PNG image:


Ablaincourt-Pressoir->Mesnil-Aubry - SHTTP - Ove...
Chart
Data
500
400
300
200
100
0
10:07 10:08 10:09 10:10 10:11 10:12 10:13 10:14 10:15 10:16 10:17 10:18
(08/22/2013 10:18)
Ablaincourt-Pressoir->Mesnil-Aubry - SHTTP - Overview - Avg. Delay (ms)
Download
☑ Borders ☑ Date and Time ☑ Title
Close

  Three check boxes allow displaying or hiding the Borders, the Date and Time and the Title.

- Data, allowing to download the graph as CSV data:

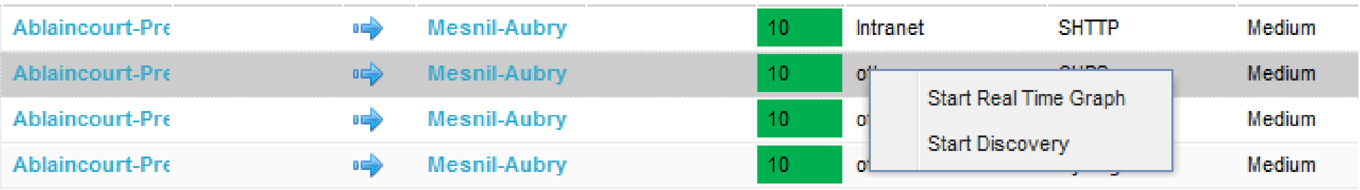


Time	LAN	WAN
08/22/2013 10:06:22	123	98.4
08/22/2013 10:06:32	201	160.8
08/22/2013 10:06:42	343	274.4
08/22/2013 10:06:52	285	228
08/22/2013 10:07:02	179	143.2
08/22/2013 10:07:12	212	169.6
08/22/2013 10:07:22	118	94.4
08/22/2013 10:07:32	74	59.2
08/22/2013 10:07:42	456	364.8
08/22/2013 10:07:52	338	270.4
08/22/2013 10:08:02	230	184
08/22/2013 10:08:12	206	164.8
08/22/2013 10:08:22	379	303.2
08/22/2013 10:08:32	85	68
08/22/2013 10:08:42	392	313.6
08/22/2013 10:08:52	196	156.8

Discovery

From any flow in the Detailed flows list, you can open a Discovery agent which polls additional information on the selected Appliance.

To access the Discovery function, right click on a flow and select Start Discovery:



Ablaincourt-Pre	➡	Mesnil-Aubry	10	Intranet	SHTTP	Medium
Ablaincourt-Pre	➡	Mesnil-Aubry	10	ot		Medium
Ablaincourt-Pre	➡	Mesnil-Aubry	10	ot		Medium
Ablaincourt-Pre	➡	Mesnil-Aubry	10	ot		Medium

It opens a Single Site view for the selected Local Site. Refer to the next section.

Sites View

The Sites View contains two frames:

"Overview"

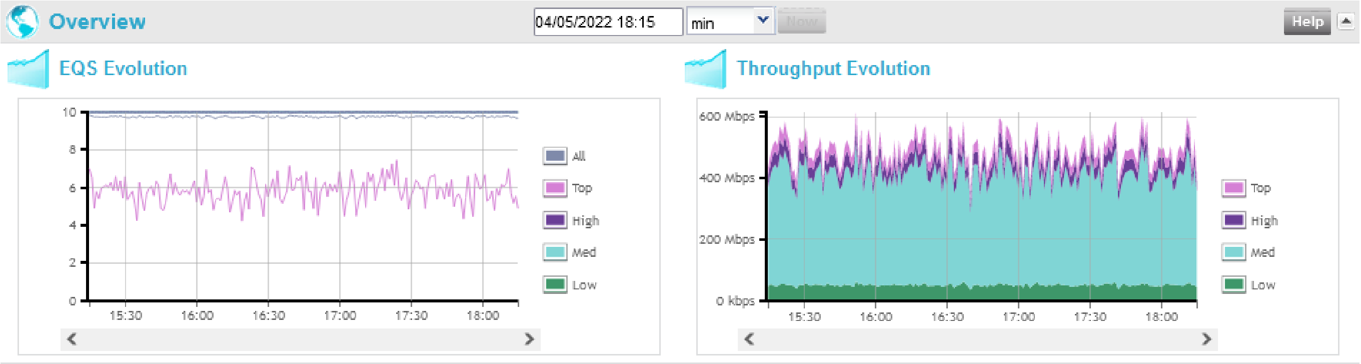
"Sites"

This section also addresses the following topics:

- "Searching for Sites / Filtering the Sites"
- "Downloading the data"

Overview

This frame shows two graphs with the following information:



Overview

04/05/2022 18:15 | min | Now

EQS Evolution

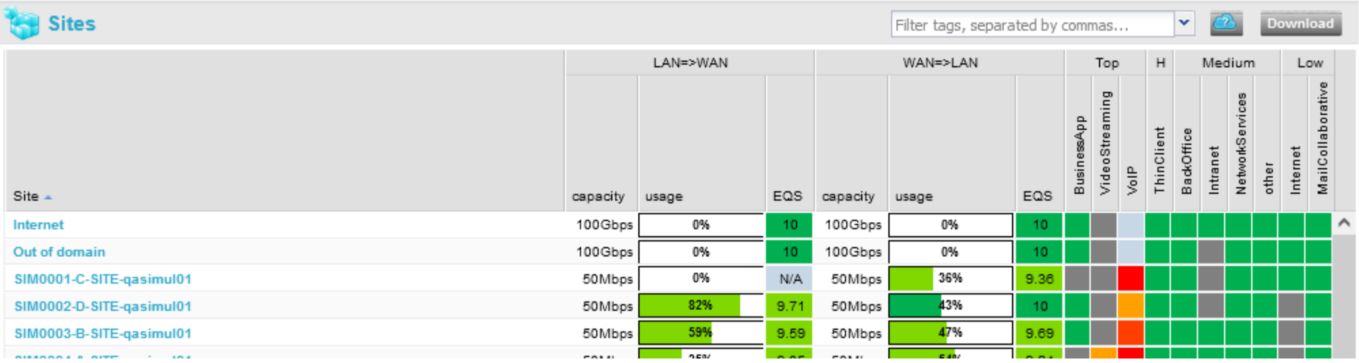
Historical graph showing the evolution of the EQS for all the flows, and for the Top, High, Medium and Low flows on all the Sites of the Client. It is identical to the EQS Evolution graph described in the "Quality Summary"frame of the Client View.

Throughput Evolution

Historical graph showing the evolution of the WAN throughput for the Top, High, Medium and Low flows on all the Sites of the Client. It is identical to the Throughput Evolution graph described in the "Activity Summary" frame of the Client view.

Sites

This frame shows, for all the Sites, the following information:



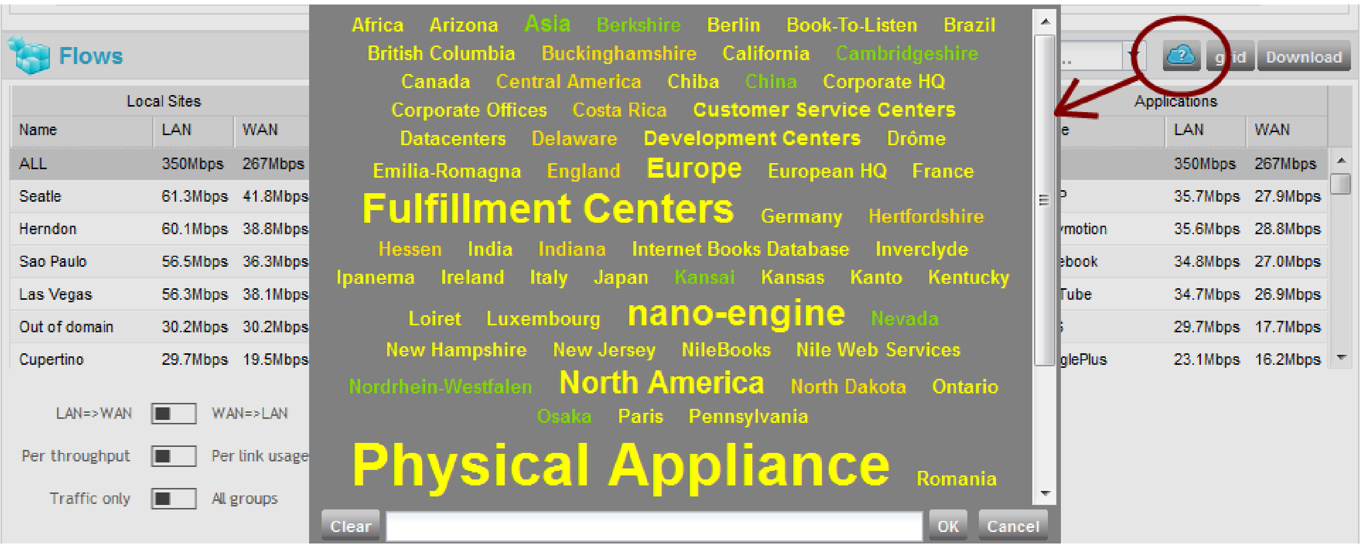
	LAN=>WAN			WAN=>LAN			Top			H	Medium				Low	
Site ▲	capacity	usage	EQS	capacity	usage	EQS	BusinessApp	VideoStreaming	VoIP	ThinClient	BackOffice	Intranet	NetworkServices	other	Internet	MailCollaborative
Internet	100Gbps	0%	10	100Gbps	0%	10	🟩	▨	⬜	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Out of domain	100Gbps	0%	10	100Gbps	0%	10	🟩	▨	⬜	🟩	🟩	▨	🟩	🟩	🟩	🟩
SIM0001-C-SITE-qasimul01	50Mbps	0%	N/A	50Mbps	36%	9.36	▨	▨	🟥	🟩	🟩	▨	🟩	🟩	🟩	🟩
SIM0002-D-SITE-qasimul01	50Mbps	82%	9.71	50Mbps	43%	10	🟩	▨	🟧	🟩	🟩	🟩	🟩	🟩	▨	🟩
SIM0003-B-SITE-qasimul01	50Mbps	59%	9.59	50Mbps	47%	9.69	🟩	▨	🟥	🟩	🟩	🟩	🟩	🟩	▨	🟩

- Site: name of the Site; by clicking on that name, a new window opens with more details on the selected Site.
- The Sites' links usage and quality with, for each direction (LAN => WAN and WAN => LAN), the following fields:
  - capacity: WAN access throughput (max BW),
  - usage: usage of the link, displayed both as a percentage of the link size and as a bar, the size of which is proportional to the usage,
  - EQS: quality of the link, displayed both as an EQS value (between 0 and 10) and as a color (between green (EQS = 10) and red (EQS = 0)).
- The Sites' Application Groups volume and quality, sorted by Criticality levels (Top, High, Medium, Low), with each cell color representing the quality of the corresponding Application Group (in the same column) for the corresponding link (on the same line); it can take any hue between green (EQS = 10) and red (EQS = 0).
  - you can read the exact values by hovering your mouse on the cells;
  - clicking on a cell opens a new window for the corresponding Site, where it filters the flows in the Site's Real Time Flows list according to the selected Application Group: thanks to this feature, you can immediately access the details of any Application Group for any Site.

This view is automatically refreshed every minute (or every 5 or 15 minutes).

Searching for Sites / Filtering the Sites

At the top of the frame, one can use the text field to filter the Sites with their tags (corresponding to the fields Folder, Subfolder or Tag in the Appliances creation window), or use the button next to this text field to open a map where the sites can be filtered by clicking their tags:



Local Sites

Name	LAN	WAN
ALL	350Mbps	267Mbps
Seatle	61.3Mbps	41.8Mbps
Herndon	60.1Mbps	38.8Mbps
Sao Paulo	56.5Mbps	36.3Mbps
Las Vegas	56.3Mbps	38.1Mbps
Out of domain	30.2Mbps	30.2Mbps
Cupertino	29.7Mbps	19.5Mbps

LAN=>WAN ■ WAN=>LAN

Per throughput ■ Per link usage

Traffic only ■ All groups

Applications

e	LAN	WAN
	350Mbps	267Mbps
ᵖ	35.7Mbps	27.9Mbps
ymotion	35.6Mbps	28.8Mbps
ebook	34.8Mbps	27.0Mbps
Tube	34.7Mbps	26.9Mbps
s	29.7Mbps	17.7Mbps
glePlus	23.1Mbps	16.2Mbps

In this map, the size of the names is a representation of the size of the Sites, and their colors represent their quality the exact EQS can be displayed by hovering the mouse on the names.

If several names are selected, they will all be displayed and applied in the filter. They can be cleared by clicking the Clear button, applied by clicking the OK button or cancelled by clicking the Cancel button.

Downloading the data

It is possible to download a zipped CSV file containing all the sites' information displayed in this frame, or to open it, with the Download button.

Single Site View

A Single Site view can be opened for any Site by clicking on its name or bar in the Client/Flows/Sites views

The Single Site View contains the following frames:

<Site> - "Quality Summary"

<Site> - "Activity Summary"

<Site> - "Throughput Summary per NAP"

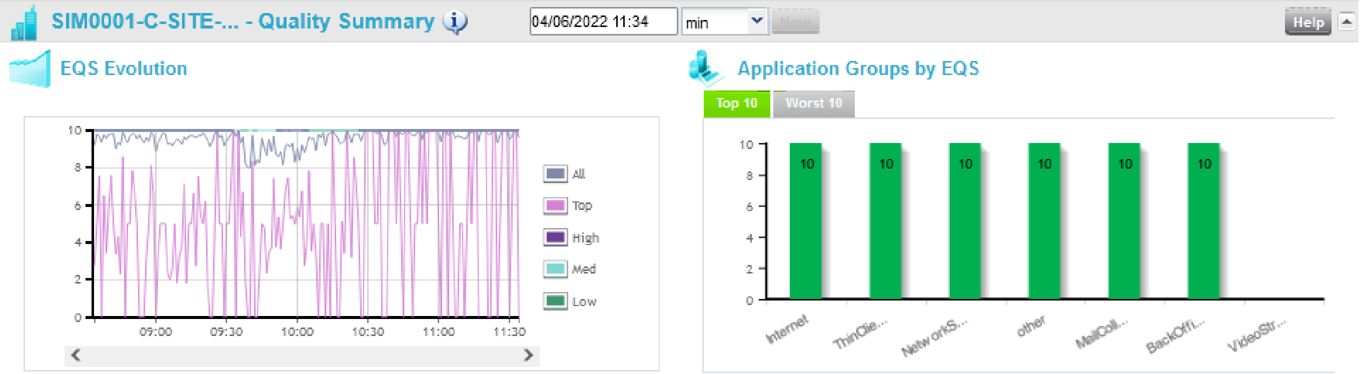
<Site> - "WANs and Applications"

<Site> - "Application Flows"

<Site> - "Discovery"

Quality Summary

This frame shows two graphs with the following information:



EQS Evolution

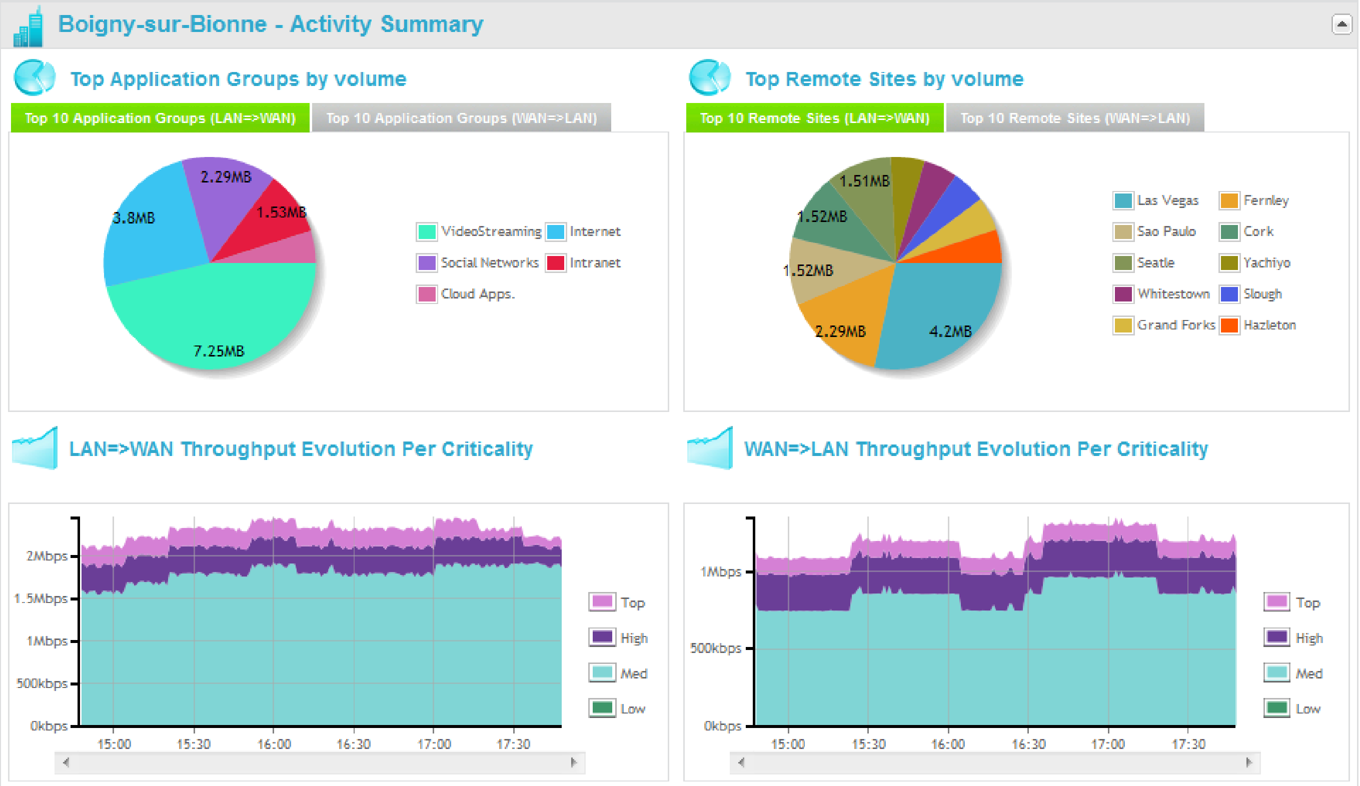
Historical graph showing the evolution of the EQS for all the flows, and for the Top, High, Medium and Low flows, on the selected Site.

Application Groups by EQS

- This bar graph shows the Top 10 Application Groups (i.e. the 10 Application Groups with the best quality) sorted by decreasing quality (the best Application Group of the Site is displayed in the first bar on the left), with their EQS values displayed both as a number (between 0 and 10 with two decimals) and as a colored bar (the height of the bar indicates the value on the vertical axis and its color can take any hue between green (EQS = 10) and red (EQS = 0)).
- By clicking on Worst 10 at the top of the bar graph, the 10 worst Application Groups are displayed, sorted by increasing quality (the worst Application Group of the Site is displayed in the first bar on the left), with their EQS values.

Activity Summary

This frame shows four graphs with the following information:



Top Application Groups by volume

This pie chart shows the top 10 AGs, with their names and volumes:

- top 10 in volume of outgoing traffic (Top 10 Application Groups (LAN => WAN) tab),
- top 10 in volume of incoming traffic (Top 10 Application Groups (WAN => LAN) tab),

Clicking on an AG in the chart automatically filters the traffic for that AG in the Application Flows frame below.

Top Remote Sites by volume

> **Note:** This pie chart is available if and only if history has been enabled for the application flows (Per minute application flows lifetime parameter in **SALSA platform configuration**'s Domain window, e.g. 72, 72, 0, 0).

This pie chart shows the top 10 Remote Sites, with their names and volumes:

- top 10 in volume of traffic sent to these Sites (Top 10 Remote Sites (LAN => WAN) tab),
- top 10 in volume of traffic received from these Sites (Top 10 Remote Sites (WAN => LAN) tab),

LAN => WAN Throughput Evolution Per Criticality

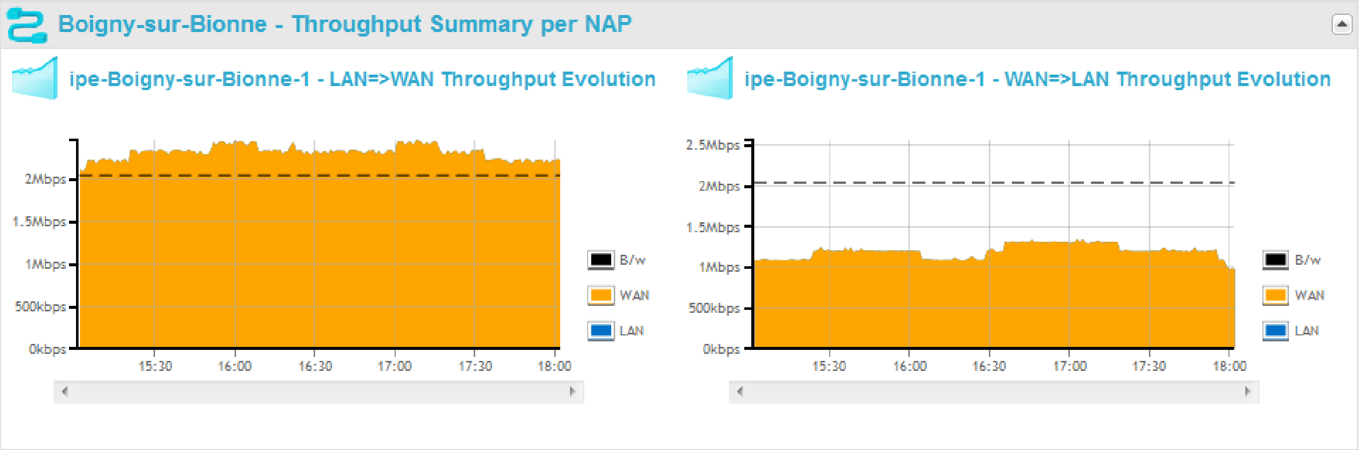
This historical graph shows the evolution of the WAN throughput of the outgoing traffic, by criticality level (Top/High/Medium/Low).

WAN => LAN Throughput Evolution Per Criticality

This historical graph shows the evolution of the WAN throughput of the incoming traffic, by criticality level (Top/High/Medium/Low).

Throughput Summary per NAP

This frame shows two graphs with the following information:


Boigny-sur-Bionne - Throughput Summary per NAP
ipe-Boigny-sur-Bionne-1 - LAN=>WAN Throughput Evolution
2Mbps
1.5Mbps
1Mbps
500kbps
0kbps
15:30
16:00
16:30
17:00
17:30
18:00
B/w
WAN
LAN
ipe-Boigny-sur-Bionne-1 - WAN=>LAN Throughput Evolution
2.5Mbps
2Mbps
1.5Mbps
1Mbps
500kbps
0kbps
15:30
16:00
16:30
17:00
17:30
18:00
B/w
WAN
LAN

<Site_name>-<NAP_number> - LAN => WAN Throughput Evolution

This historical graph shows:

- the ingress bandwidth of the Site (B/w, dotted black line), corresponding to the Ingress max. B/W in the WAN access configuration window,
- the evolution of the ingress LAN throughput (measured on the LAN interface of the Appliance, LAN, in blue and in the background),
- the evolution of the ingress WAN throughput (measured on the WAN interface of the Appliance, WAN, in orange and in the foreground),

> **Note:** As the WAN-to-WAN throughput is displayed in front of the LAN-to-LAN throughput, when both are equal (i.e., when the traffic is not compressed), only the WAN-to-WAN throughput (orange area) is visible. It can be hidden by clicking WAN in the legend, thus revealing the LAN-to-LAN throughput (blue area) behind it (LAN-to-LAN throughput can also be hidden, by clicking LAN in the legend).

> **Note:** When the LAN-to-LAN throughput is higher than the WAN-to-WAN throughput (i.e., when the traffic is compressed), the blue area above the orange area corresponds to the bandwidth saved thanks to compression (difference between LAN-to-LAN throughput and WAN-to-WAN throughput).

<Site_name>-<NAP_number> - WAN => LAN Throughput Evolution

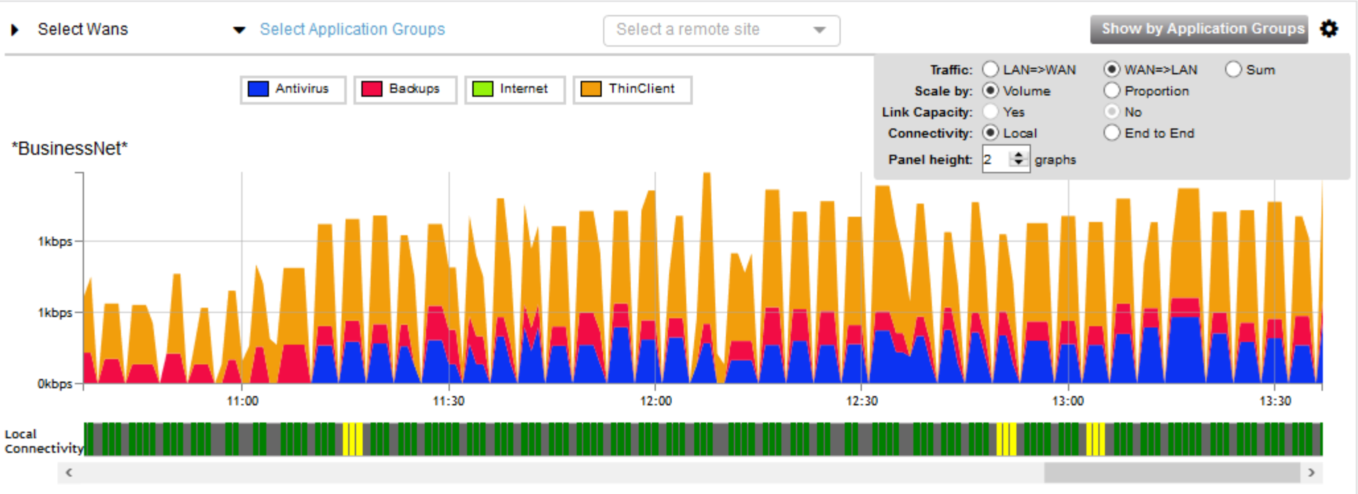
This historical graph shows:

- the egress bandwidth of the Site (B/w, dotted black line), corresponding to the Egress max. B/W in the WAN access configuration window,
- the evolution of the egress LAN throughput (measured on the LAN interface of the Appliance, LAN, in blue and in the background),
- the evolution of the egress WAN throughput (measured on the WAN interface of the Appliance, WAN, in orange and in the foreground),

The same two graphs are displayed for each NAP.

WANs and Applications

For the selected Site, this frame displays 2 sets of graphs, one set showing throughput evolution and site connectivity on each WAN, and the other set of graphs showing the throughput per Application Group/Application with its EQS.



Traffic: ○ LAN=>WAN ● WAN=>LAN ○ Sum

Scale by: ● Volume ○ Proportion

Link Capacity: ○ Yes ○ No

Connectivity: ● Local ○ End to End

Panel height: 2 graphs

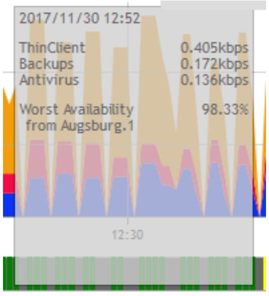
The covered period and the granularity of the data in the graphs depend on the time span. It can be three hours of per-minute information if the time span is the minute (you can scroll the past hours with the horizontal scroll bar at the bottom of the graph), or it can be the last three days of hourly average information, if the time span is the hour.

The **Connectivity** graphs show the connectivity state of the available WANs. They can take four colors:

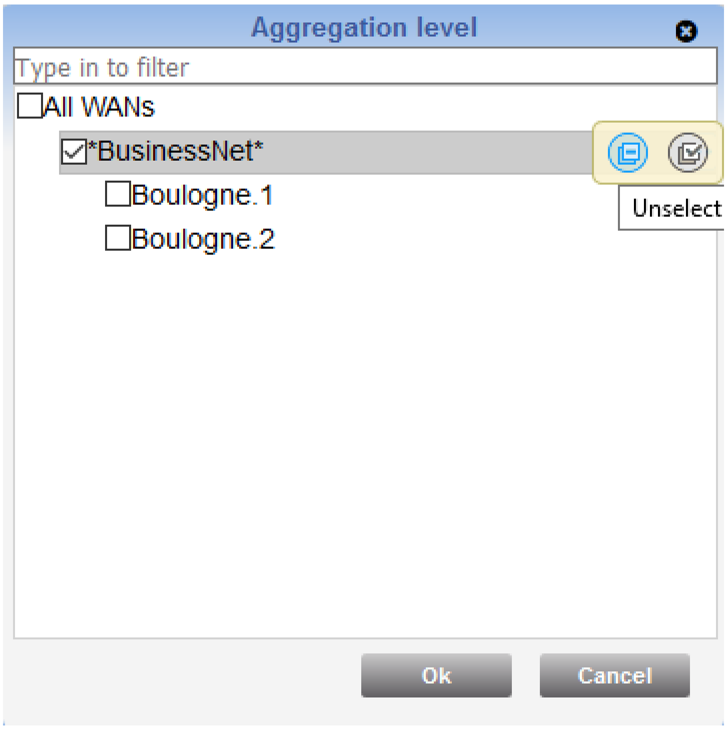
- green: 100% of connectivity
- yellow: 80%-99%
- red: < 80%
- grey: not measured

Exclamation marks indicate problem of stability (i.e. more than two changes during a collect).

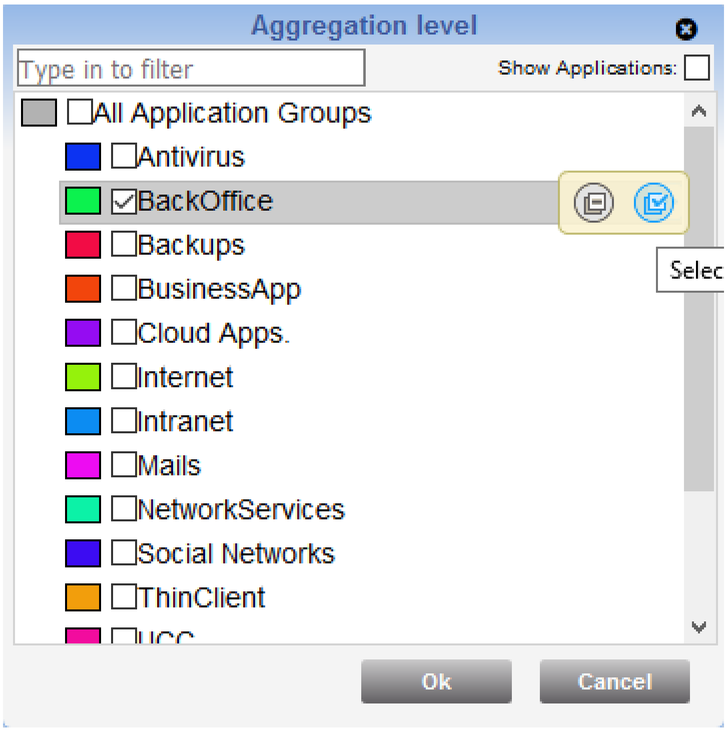
Connectivity problems are indicated in the pop-up when pointed with the mouse:



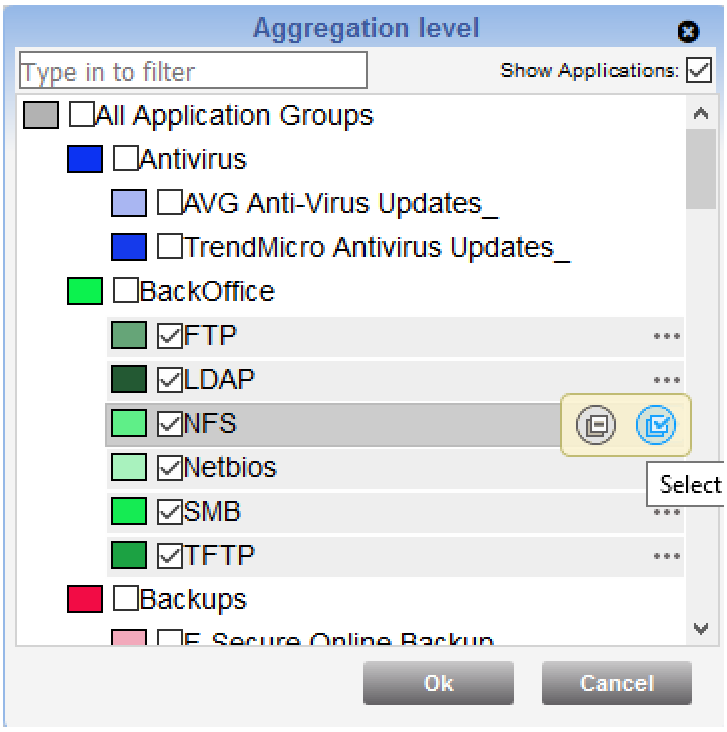
It is possible to show the graphs WAN by WAN (default view) or aggregated for all WANs, or for some WANs only, with a click on the arrow before **Select WAN** followed by a click on one of the WAN names. Modify your selection in the popup window through the Select Siblings/Unselect Siblings button and click **OK** to validate.



Similarly, you can display the graphs for all Application Groups (default view) or for some Application Groups only, with a click on the arrow before **Select Application Group** followed by a click on one or several Application Group name(s) in the popup window. If you selected one Application Group, you can use the Select Siblings button to select again all the Application Groups. Click **OK** to validate.

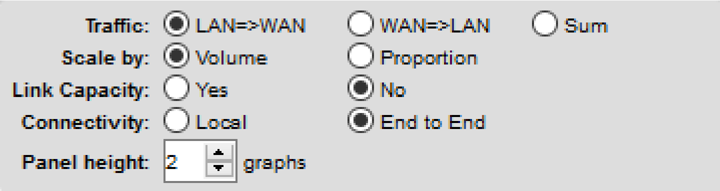


You can also check the **Show Applications** checkbox to optimize your selection and select some applications. Through the Select Siblings button, you can select all the Applications in one Application Group. Click **OK** to validate.



As a result, the graph shows the distribution of the selected Application Groups or Applications on each selected WAN.

Hit the ⚙ icon in the upper right corner of the frame to modify your display through the following options:

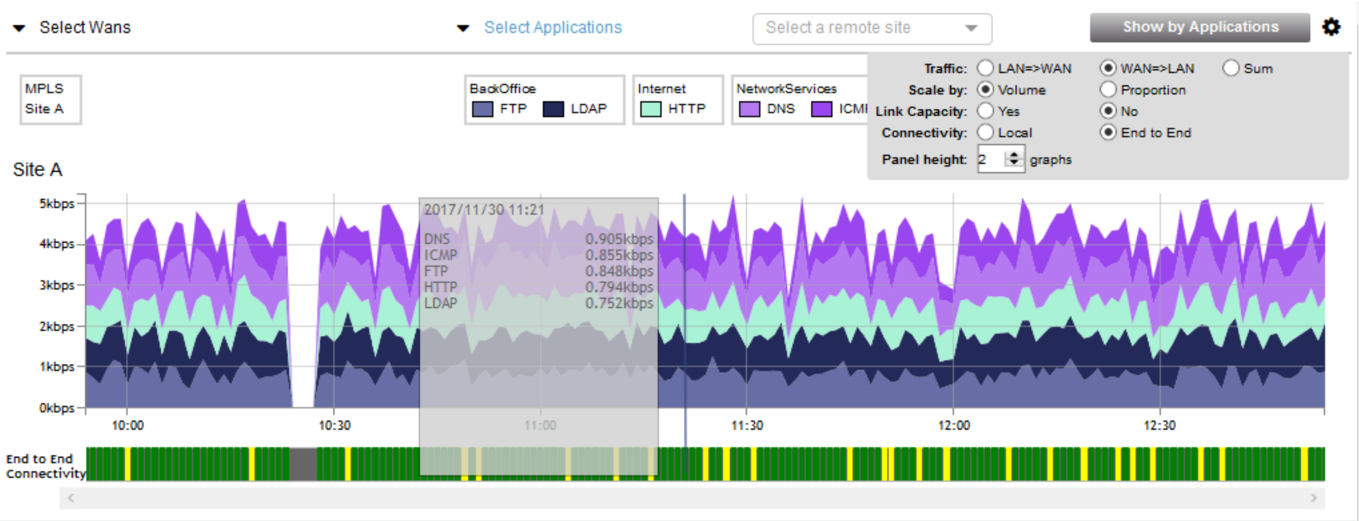


Traffic: ● LAN=>WAN ○ WAN=>LAN ○ Sum
Scale by: ● Volume ○ Proportion
Link Capacity: ○ Yes ● No
Connectivity: ○ Local ● End to End
Panel height: 2 graphs

- **Traffic**: select traffic direction from the LAN to the WAN or from the WAN to the LAN. The 'Sum' option displays both direction.
- **Scale**: if you select the 'Volume' option, throughput is specified in kilobits per second. If you select the 'Proportion' option, throughput is specified in percentage of the volume, with respect to the Y left axis.
- **Link Capacity**: if the 'Yes' option is available, it displays a limit line which corresponds to the maximum capacity of the link.
- **Connectivity**: either select 'Local' site connectivity or 'End to End' site connectivity. The status bar at the bottom of the graph differs accordingly.
- **Panel height - number of graphs**: according to the number of available WANs, you may define the number of graphs to display. The default option is 2. WAN graphs are displayed in alphabetical order.

Also note that you can select a **Remote Site** from the drop-down list.

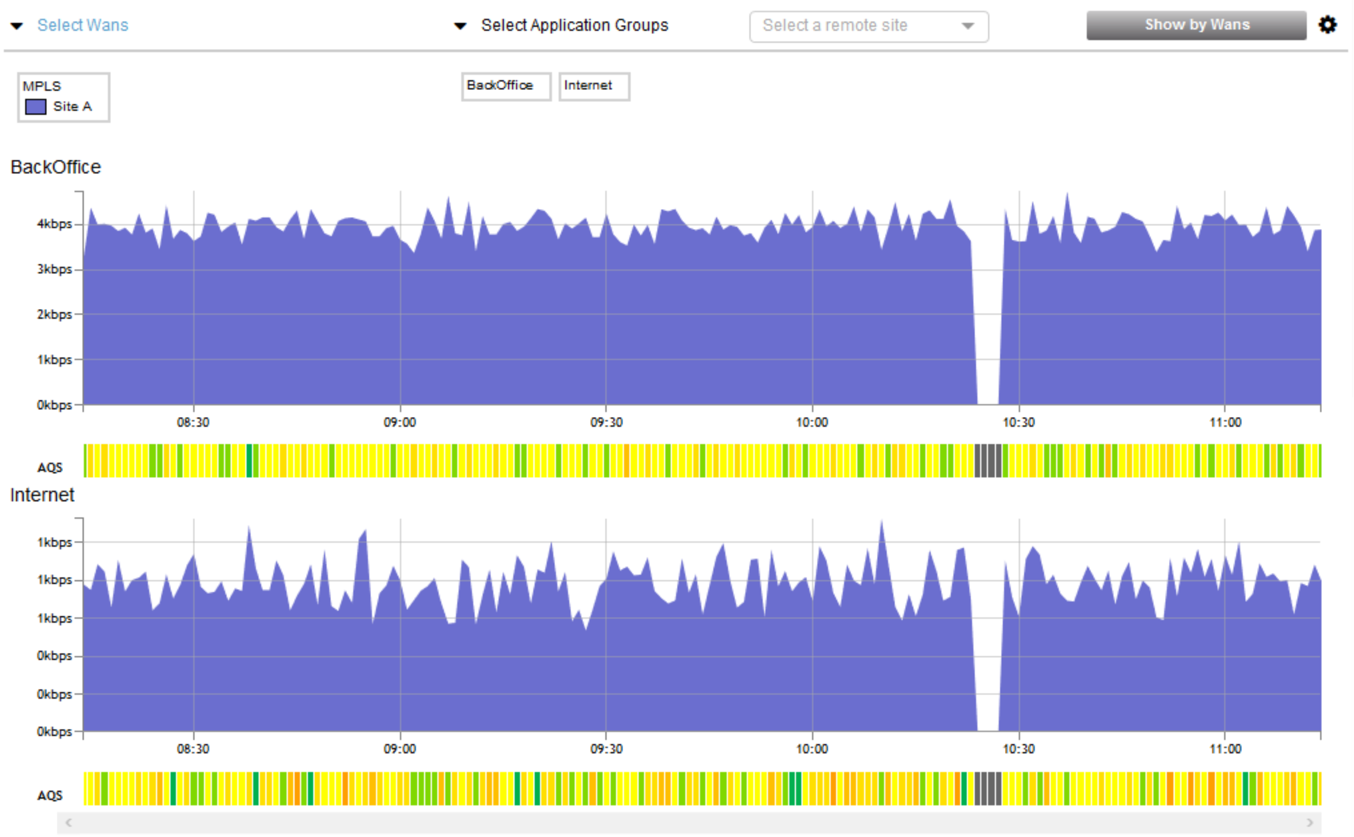
In the following example, there is only one selected WAN:



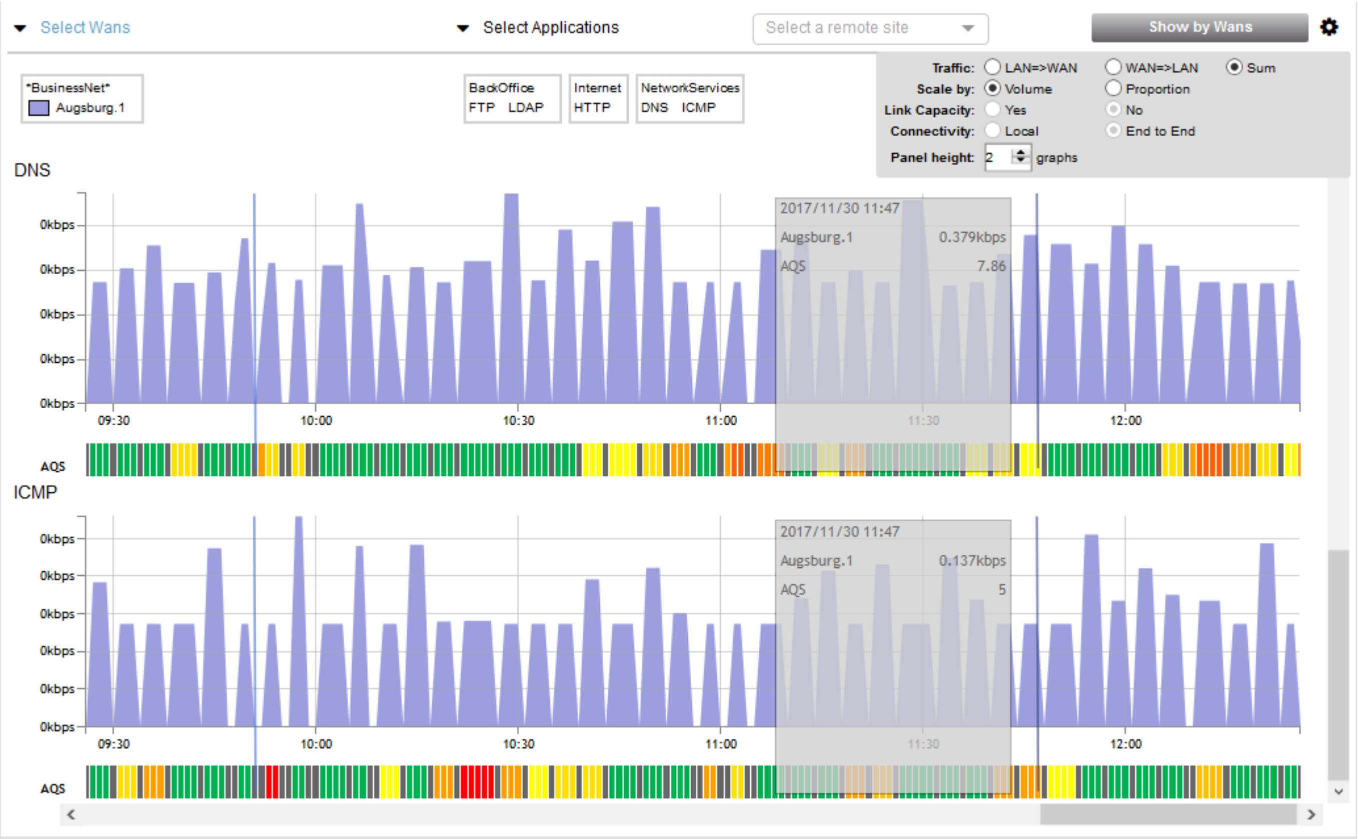
Traffic: ○ LAN=>WAN ● WAN=>LAN ○ Sum
Scale by: ● Volume ○ Proportion
Link Capacity: ○ Yes ● No
Connectivity: ○ Local ● End to End
Panel height: 2 graphs

2017/11/30 11:21
DNS 0.905kbps
ICMP 0.855kbps
FTP 0.848kbps
HTTP 0.794kbps
LDAP 0.752kbps

The **Show by Application Groups** button toggles the view and shows the throughput per Application Group and its EQS. Note that this button appears if you only selected Application Groups without Applications.



The **Show by Applications** button appears if you selected Applications.



Traffic: ○ LAN=>WAN ○ WAN=>LAN ● Sum
Scale by: ● Volume ○ Proportion
Link Capacity: ○ Yes ○ No
Connectivity: ○ Local ○ End to End
Panel height: 2 graphs

2017/11/30 11:47
Augsburg.1 0.379kbps
AQS 7.86

2017/11/30 11:47
Augsburg.1 0.137kbps
AQS 5

So instead of showing the distribution of the selected Application Groups or Applications on each WAN, this view shows the throughput evolution of the selected WANs for each selected Application Group or Application.

Hit the ⚙ icon in the upper right corner of the frame to modify your display as explained before.

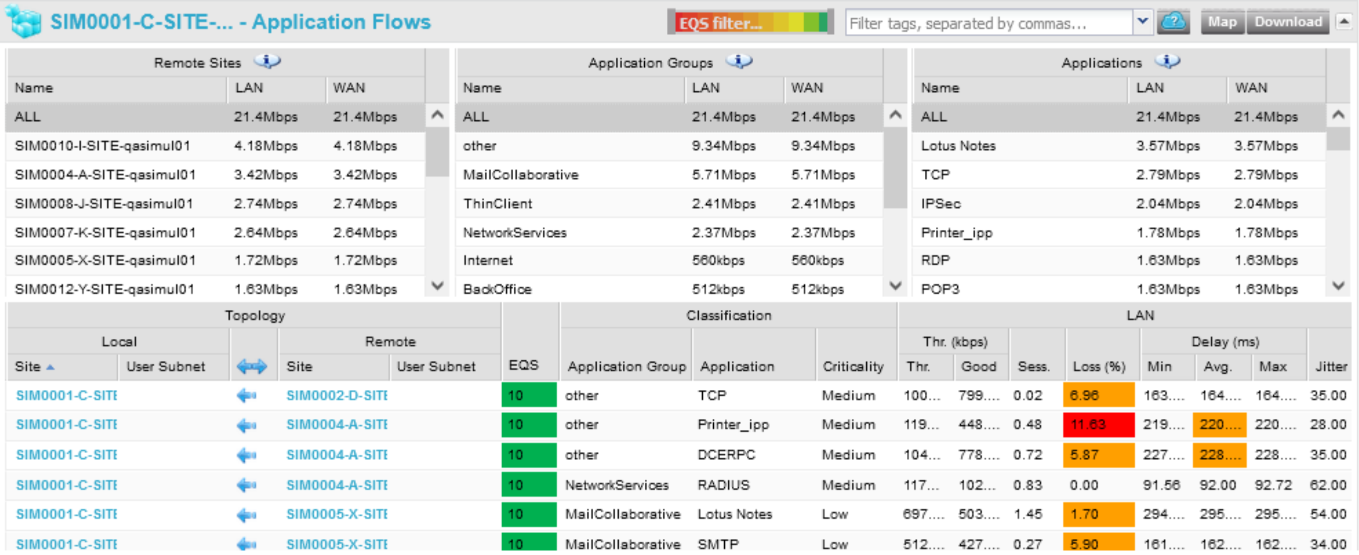
The **Show by WANs** button toggles back to the previous view.

Also see "WANs and Applications" for the Client.

Application Flows

This frame shows the same information as in the "Flows View", but for the selected Site as the Local Site.

Site - Application flows, Detail:


SIM0001-C-SITE-... - Application Flows
EQS filter...
Filter tags, separated by commas...
Map
Download

Remote Sites

Name	LAN	WAN
ALL	21.4Mbps	21.4Mbps
SIM0010-I-SITE-qasimul01	4.18Mbps	4.18Mbps
SIM0004-A-SITE-qasimul01	3.42Mbps	3.42Mbps
SIM0008-J-SITE-qasimul01	2.74Mbps	2.74Mbps
SIM0007-K-SITE-qasimul01	2.64Mbps	2.64Mbps
SIM0005-X-SITE-qasimul01	1.72Mbps	1.72Mbps
SIM0012-Y-SITE-qasimul01	1.63Mbps	1.63Mbps

Application Groups

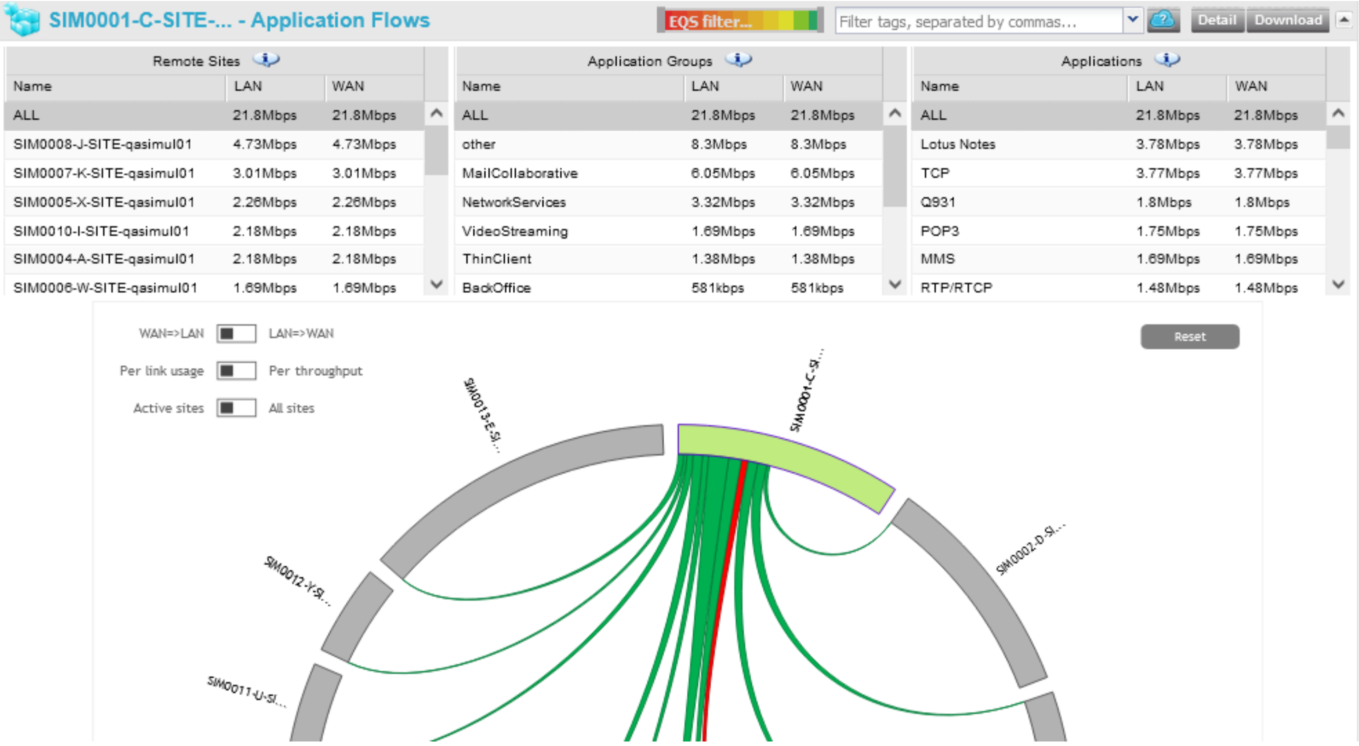
Name	LAN	WAN
ALL	21.4Mbps	21.4Mbps
other	9.34Mbps	9.34Mbps
MailCollaborative	5.71Mbps	5.71Mbps
ThinClient	2.41Mbps	2.41Mbps
NetworkServices	2.37Mbps	2.37Mbps
Internet	560kbps	560kbps
BackOffice	512kbps	512kbps

Applications

Name	LAN	WAN
ALL	21.4Mbps	21.4Mbps
Lotus Notes	3.57Mbps	3.57Mbps
TCP	2.79Mbps	2.79Mbps
IPSec	2.04Mbps	2.04Mbps
Printer_ipp	1.78Mbps	1.78Mbps
RDP	1.63Mbps	1.63Mbps
POP3	1.63Mbps	1.63Mbps

Topology						Classification			LAN							
Local			Remote						Thr. (kbps)				Delay (ms)			
Site ▲	User Subnet	⇔	Site	User Subnet	EQS	Application Group	Application	Criticality	Thr.	Good	Sess.	Loss (%)	Min	Avg.	Max	Jitter
SIM0001-C-SITE		⇦	SIM0002-D-SITE		10	other	TCP	Medium	100...	799....	0.02	6.96	163....	164....	164....	35.00
SIM0001-C-SITE		⇦	SIM0004-A-SITE		10	other	Printer_ipp	Medium	119...	448....	0.48	11.63	219....	220....	220....	28.00
SIM0001-C-SITE		⇦	SIM0004-A-SITE		10	other	DCERPC	Medium	104...	778....	0.72	5.87	227....	228....	228....	35.00
SIM0001-C-SITE		⇦	SIM0004-A-SITE		10	NetworkServices	RADIUS	Medium	117...	102...	0.83	0.00	91.56	92.00	92.72	62.00
SIM0001-C-SITE		⇦	SIM0005-X-SITE		10	MailCollaborative	Lotus Notes	Low	697....	503....	1.45	1.70	294....	295....	295....	54.00
SIM0001-C-SITE		⇦	SIM0005-X-SITE		10	MailCollaborative	SMTP	Low	512....	427....	0.27	5.90	161....	162....	162....	34.00

Site - Application flows, Map:



SIM0001-C-SITE-... - Application Flows

Remote Sites

Name	LAN	WAN
ALL	21.8Mbps	21.8Mbps
SIM0008-J-SITE-qasimul01	4.73Mbps	4.73Mbps
SIM0007-K-SITE-qasimul01	3.01Mbps	3.01Mbps
SIM0005-X-SITE-qasimul01	2.26Mbps	2.26Mbps
SIM0010-I-SITE-qasimul01	2.18Mbps	2.18Mbps
SIM0004-A-SITE-qasimul01	2.18Mbps	2.18Mbps
SIM0006-W-SITE-qasimul01	1.69Mbps	1.69Mbps

Application Groups

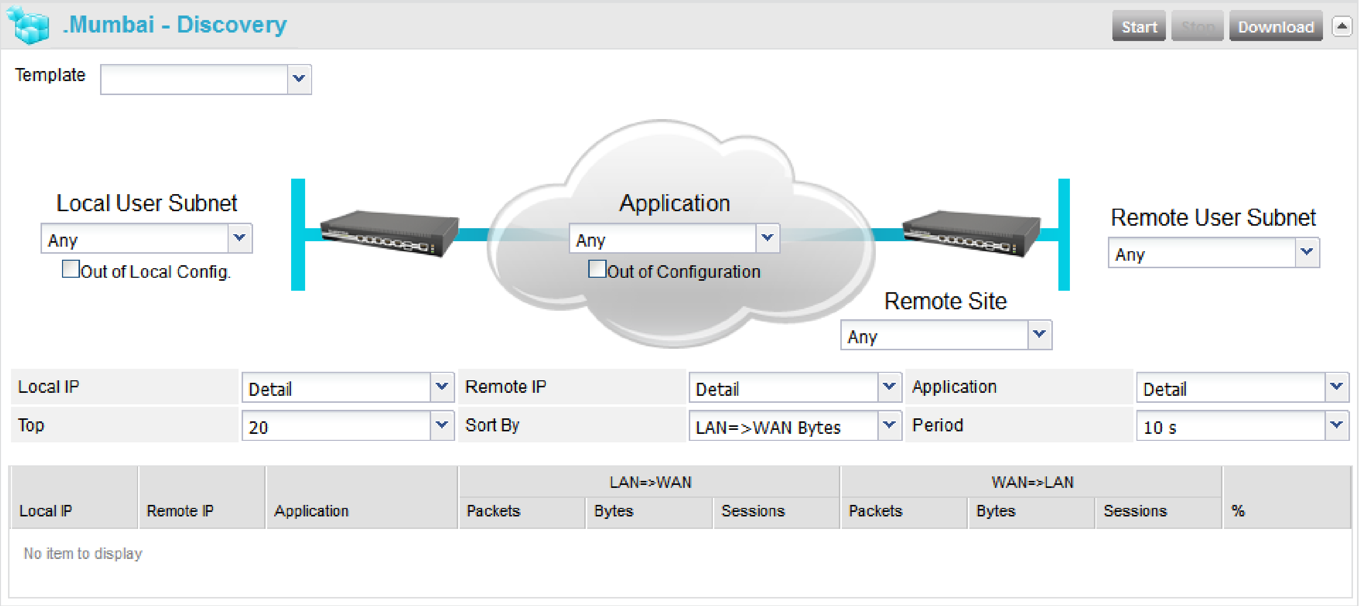
Name	LAN	WAN
ALL	21.8Mbps	21.8Mbps
other	8.3Mbps	8.3Mbps
MailCollaborative	6.05Mbps	6.05Mbps
NetworkServices	3.32Mbps	3.32Mbps
VideoStreaming	1.69Mbps	1.69Mbps
ThinClient	1.38Mbps	1.38Mbps
BackOffice	581kbps	581kbps

Applications

Name	LAN	WAN
ALL	21.8Mbps	21.8Mbps
Lotus Notes	3.78Mbps	3.78Mbps
TCP	3.77Mbps	3.77Mbps
Q931	1.8Mbps	1.8Mbps
POP3	1.75Mbps	1.75Mbps
MMS	1.69Mbps	1.69Mbps
RTP/RTCP	1.48Mbps	1.48Mbps

Discovery

This frame allows polling more information from an Appliance.



Template:

Local User Subnet: Any

□ Out of Local Config.

Application: Any

□ Out of Configuration

Remote User Subnet: Any

Remote Site: Any

Local IP	Detail	Remote IP	Detail	Application	Detail
Top	20	Sort By	LAN=>WAN Bytes	Period	10 s

			LAN=>WAN			WAN=>LAN			
Local IP	Remote IP	Application	Packets	Bytes	Sessions	Packets	Bytes	Sessions	%

No item to display

The Discovery function consists in creating a Discovery agent for the selected Appliance (one agent maximum per Appliance) to collect additional data (as compared to the data already collected and displayed in the Real Time Flows list see above).

To use the Discovery function:

1. Set the ad hoc filters
2. Start the Discovery agent
3. Check the results
4. Stop the Discovery agent

Filters

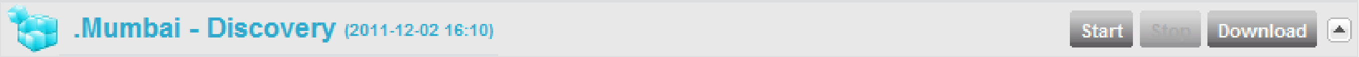
The flows can be filtered according to multiple criteria, using the 5 drop-down lists and 2 check boxes surrounding the network diagram:

- Template: three templates can be used to filter:
    - Out of local subnets: (= out of local config) packets crossing the Appliance, but where neither the source IP address nor the destination IP address belong to one of its Topology subnets (this traffic is called in Transit); these flows are not measured individually by the Appliance; instead, only their global volume is measured and reported (i.e., these flows are not present in the Real Time Flows list nor in any report, except in the Site Analysis reports, which show the volume of Transit traffic).

  - Unrecognized Application: packets belonging to applications which are not recognized by the Appliance's syntax engine, which were not declared and which do not use well-know ports,
  - Out of Domain: sent packets with a destination IP address which does not belong to a declared Topology subnet, or received packets with a source IP address which does not belong to a declared Topology subnet (in either case, these packets will match Out of Domain Topology subnet which is in the system by default, so it does not have to be declared , 0.0.0.0/0).
- Local User Subnet: to filter the data using a User subnet declared for the local Site,
  - An Out of Local Config. check box allows, if checked, to display the traffic which does not belong to the local configuration only (see Out of local subnets above)
- Remote User Subnet: to filter the data using a User subnet declared for a remote Site,
- Remote Site: to filter the data using a User subnet declared for a remote Site,
- Application: to filter the data according to one application,
  - An Out of config check box, allows, if checked, to discover the port number used by the unrecognized applications (see above).

Start/stop a Discovery agent

A Discovery agent can be started or stopped with the Start and Stop buttons at the right of the <Site> - Discovery frame header:



> **Note:** If the Start button is greyed Start and the Stop button is visible Stop, it means that a Discovery agent is running on the Appliance. Discovery agents consume resources, and they are not meant to run permanently. So when you have found what you were looking for thanks to a Discovery agent, do not forget to stop it.

Result table

According to the configuration rules, this Discovery agent will collect the following data and send them to the Application Configuration server:

Local IP	local IP address
Remote IP	remote IP address
Application	name of the application, displayed as follows: • when the application is recognized: A (b), where A is the declared

	name and b is the application recognized by the syntax engine: • for a standard application (e.g. FTP) it reads: FTP (ftp), • for an application with a specific declaration (e.g. Ping_X is declared as follows: protocol: ICMP; User subnet: X), it reads: Ping_X (icmp) • for an application which is not recognized by the Appliance' syntax engine, but which is declared, it reads: <Application_name> (unknown) • when the application is not recognized (it is not recognized by the Appliance and it has not been defined), it displays the layer 4 protocol and the port number.
LAN => WAN Packets	number of ingress packets
LAN => WAN Bytes	number of ingress bytes
LAN => WAN Sessions	number of ingress sessions
WAN => LAN Packets	number of egress packets
WAN => LAN Bytes	number of egress bytes
WAN => LAN Sessions	number of egress sessions
%	percentage of traffic that each line represents over the total, in terms of LAN=>WAN Packets, LAN=>WAN Bytes, LAN=>WAN Sessions, WAN=>LAN Packets, WAN=>LAN Bytes or WAN=>LAN Sessions, according to the Sort by choice

Note: The counters are cleared at each start of a Discovery agent.

The result can be downloaded in CSV format by clicking on the Download button at the right of the <Site> - Discovery frame header.

Display settings

The results can be displayed in different ways, thanks to 6 drop-down lists below the network diagram:

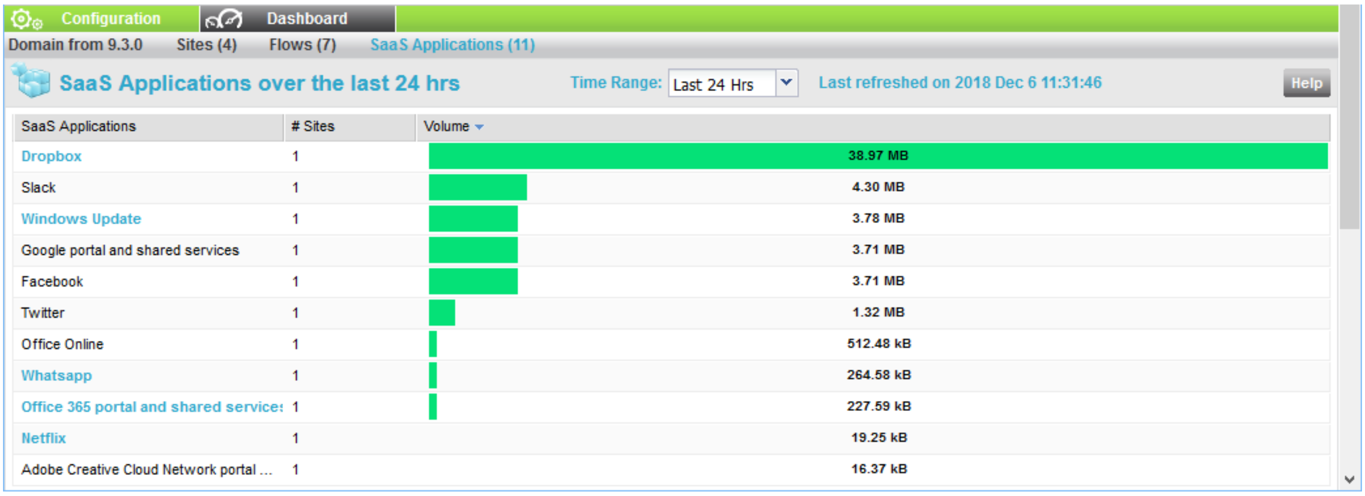
- Local IP:

  - Detail: the local IP addresses are displayed (so different local IP addresses will always be displayed on different lines),
  - Group: the local IP addresses are not displayed (and all flows with the same remote IP address and same application will be merged on one line, even if they have different local IP addresses).
- Remote IP:
  - Detail: the remote IP addresses are displayed (so different remote IP addresses will always be displayed on different lines),
  - Group: the remote IP addresses are not displayed (and all flows with the same local IP address and same application will be merged on one line, even if they have different remote IP addresses).
- Application:
  - Detail: the application names are displayed (so different applications will always be displayed on different lines),
  - Group: the application names are not displayed (and all flows with the same local IP address and same remote IP address will be merged on one line, even if different applications are running between these two addresses).
- Top:
  - 20: shows the 20 most significant results (in Packets, Bytes or Sessions, according to the field used to sort the data),
  - 50: shows the 50 most significant results,
  - 100: shows the 100 most significant results.
- Sort by: it is possible to sort the data according to the number of:
  - LAN => WAN Bytes,
  - LAN => WAN Packets,
  - LAN => WAN Sessions,
  - WAN => LAN Bytes,
  - WAN => LAN Packets,
  - WAN => LAN Sessions.

  It is also possible to sort the data by clicking on the column headers.
- Period:
  - 10 s: the results are refreshed every 10 seconds,
  - 1 mn: the results are refreshed every minute,
  - 5 mn: the results are refreshed every 5 minutes.

SaaS Applications View

In the Dashboard header bar, the total number of SaaS Applications listed in the dashboard table is displayed between parenthesis (11 on the image below):



SaaS Applications over the last 24 hrs

Time Range: Last 24 Hrs

Last refreshed on 2018 Dec 6 11:31:46

SaaS Applications	# Sites	Volume
Dropbox	1	38.97 MB
Slack	1	4.30 MB
Windows Update	1	3.78 MB
Google portal and shared services	1	3.71 MB
Facebook	1	3.71 MB
Twitter	1	1.32 MB
Office Online	1	512.48 kB
Whatsapp	1	264.58 kB
Office 365 portal and shared service:	1	227.59 kB
Netflix	1	19.25 kB
Adobe Creative Cloud Network portal ...	1	16.37 kB

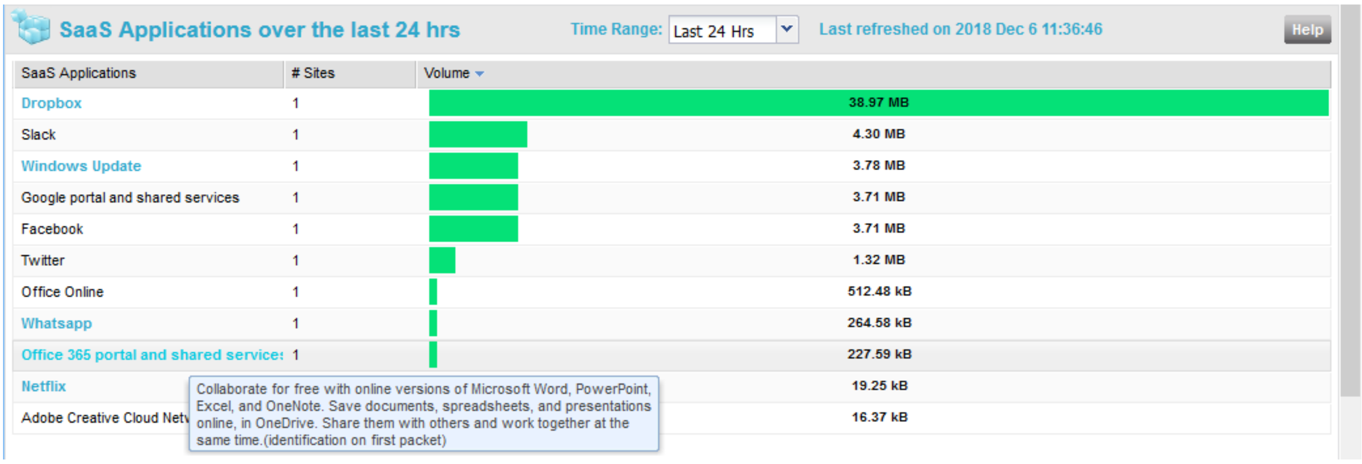
The SaaS Applications view displays one frame:

"SaaS Applications over the last Hours/Days"

SaaS Applications over the last Hours/Days

This view displays the list of the most common SaaS applications discovered on the network over the selected period.

After you have defined the Time Range (Last hour/4 hours/12 hours/ 24 hours and last 7 days) of the displayed list, this list is automatically refreshed and the number of SaaS applications specified in the dashboard header is updated.



SaaS Applications over the last 24 hrs
Time Range: Last 24 Hrs
Last refreshed on 2018 Dec 6 11:36:46
Help

SaaS Applications	# Sites	Volume
Dropbox	1	38.97 MB
Slack	1	4.30 MB
Windows Update	1	3.78 MB
Google portal and shared services	1	3.71 MB
Facebook	1	3.71 MB
Twitter	1	1.32 MB
Office Online	1	512.48 kB
Whatsapp	1	264.58 kB
Office 365 portal and shared service	1	227.59 kB
Netflix		19.25 kB
Adobe Creative Cloud Netv		16.37 kB

Collaborate for free with online versions of Microsoft Word, PowerPoint, Excel, and OneNote. Save documents, spreadsheets, and presentations online, in OneDrive. Share them with others and work together at the same time.(identification on first packet)

- The displayed SaaS Applications have been discovered by the appliance during the last 24 hours (current example).

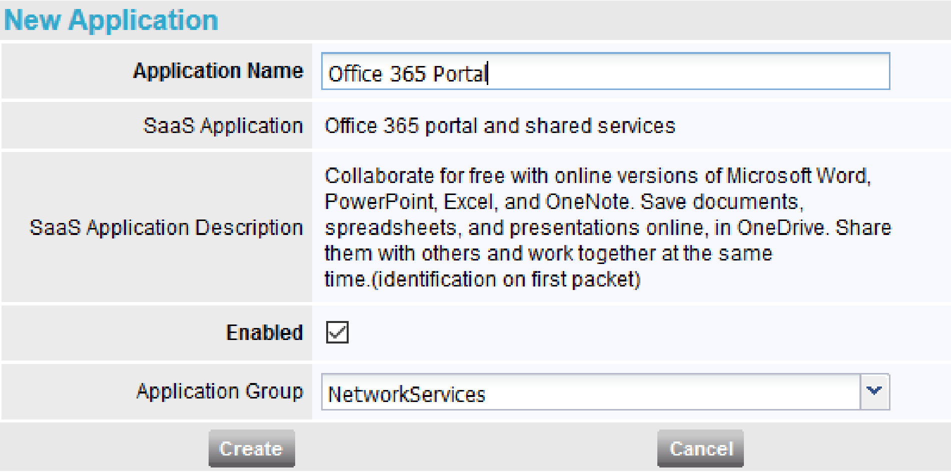
  You can view the description of each application by hovering over its name with your mouse. Note that SaaS applications associated with subnet information in the SaaS dictionary are identified through the "**(identification on first packet)**" label at the end of their respective descriptions.

  > **Note:** SaaS applications listed in black have been recognized and provisioned while applications displayed in blue remain to be defined and optionally assigned to an Application Group. See the procedure below.

- The second column specifies the number of Sites linked to each SaaS Application.
- The approximative Volume value is given for each SaaS application for all the Sites of the Domain.

Provisioning a SaaS Application

1 From the dashboard list, click a SaaS application name displayed in blue.



New Application

Application Name	Office 365 Portal
SaaS Application	Office 365 portal and shared services
SaaS Application Description	Collaborate for free with online versions of Microsoft Word, PowerPoint, Excel, and OneNote. Save documents, spreadsheets, and presentations online, in OneDrive. Share them with others and work together at the same time.(identification on first packet)
Enabled	☑
Application Group	NetworkServices

2 You may keep the application name by default or enter a new Name.

3 Keep the Enabled administrative state checked (default) to activate the application.

4 From the stack of already defined Application Groups, select one AG the current application will be assigned to.

5 Hit **Create**.

The original SaaS Application name is now displayed in black on the dashboard.

The SaaS Application appears in the Applications window under its new name (if you changed its original name); see "Configuring Applications".

Also see "Creating new applications"and "Creating customized SaaS applications".

4 Configuring a Zone-Based Firewall

The purpose of this Use Case, based on "Use Case 1", is to create a zone-based firewall in order to:

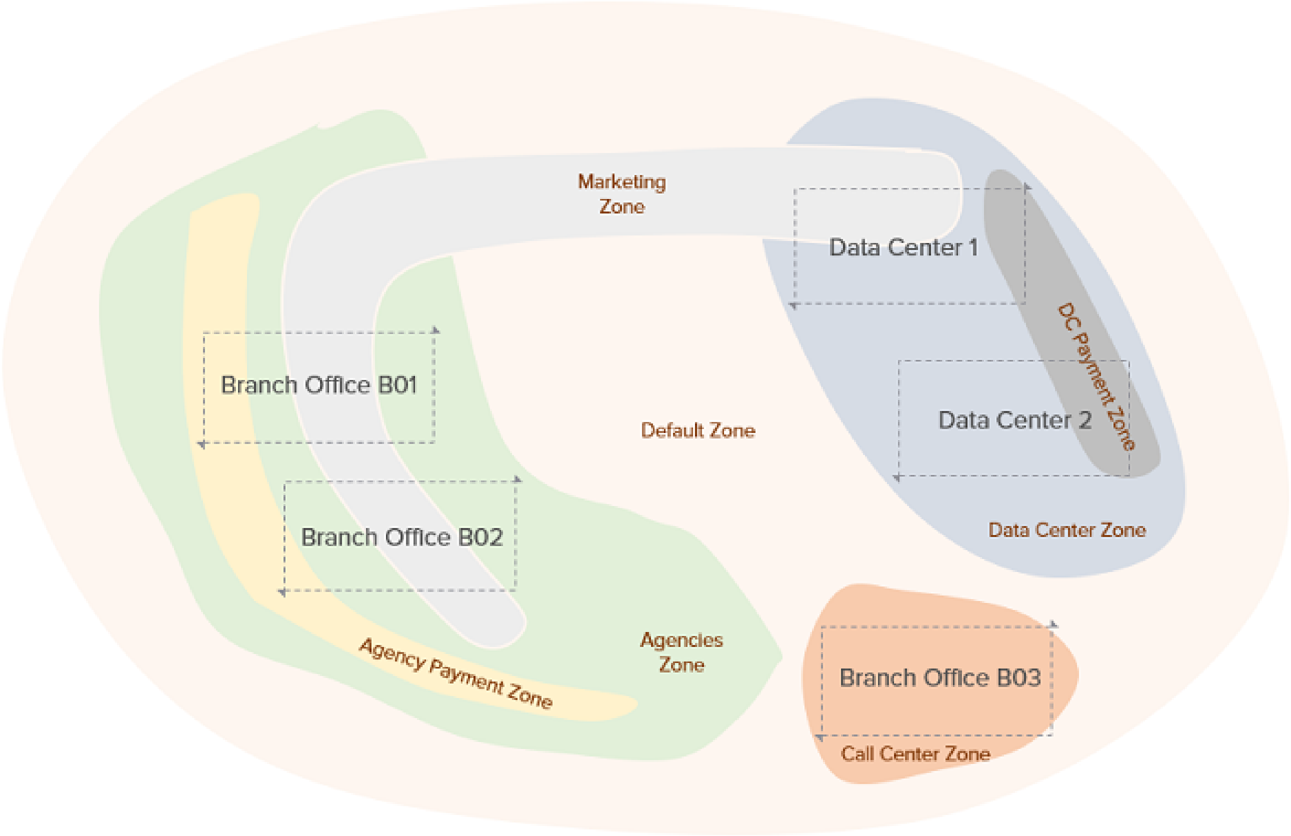
- provide you with the possibility to strengthen the segmentation of your private network (communication between sites/subnets)
- manage the Internet traffic, i.e. the connection from a site/subnet to any application (through backhauling (bh) via the Data Center, directly to the Internet (dti), via a web security gateway (wsg) or the traffic may be simply dropped).

Zone-based firewall policies are configured globally for the network; the SD-WAN Orchestrator then translates each global policy into a local routing/firewalling rule for each involved SD-WAN appliance.

> **Warning:** all the Network spoke appliances must have at least one WAN interface that is eligible to DTI or backhauling to be able to access Applications and Monitoring functions.

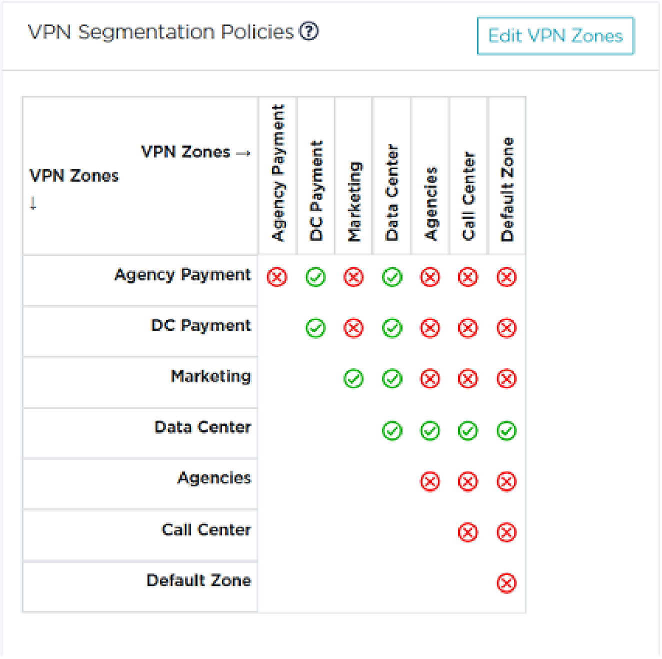
The zone-based firewall Internet Access management function impacts on DWS since this service must choose an interface that is eligible for strengthening the policy (for example, the system cannot select an MPLS interface if the traffic is Direct to Internet). Refer to "Internet Access Policies".

Use Case 12

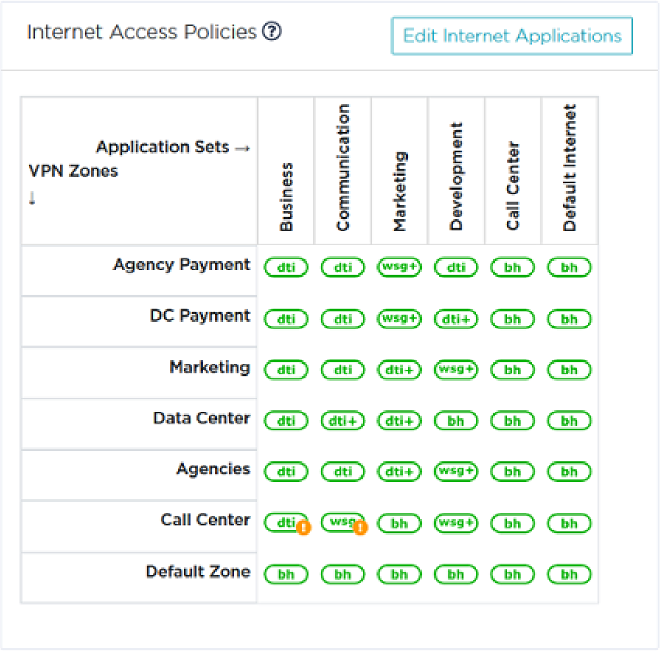


Accessing the Zone-Based Firewall function

Select **Network -> Zone-Based Firewall** from the Orchestrator main menu.



VPN Zones → VPN Zones ↓	Agency Payment	DC Payment	Marketing	Data Center	Agencies	Call Center	Default Zone
Agency Payment	⊗	✓	⊗	✓	⊗	⊗	⊗
DC Payment		✓	⊗	✓	⊗	⊗	⊗
Marketing			✓	✓	⊗	⊗	⊗
Data Center				✓	✓	✓	✓
Agencies					⊗	⊗	⊗
Call Center						⊗	⊗
Default Zone							⊗



Application Sets → VPN Zones ↓	Business	Communication	Marketing	Development	Call Center	Default Internet
Agency Payment	dti	dti	wsg+	dti	bh	bh
DC Payment	dti	dti	wsg+	dti+	bh	bh
Marketing	dti	dti	dti+	wsg+	bh	bh
Data Center	dti	dti+	dti+	bh	bh	bh
Agencies	dti	dti	dti+	wsg+	bh	bh
Call Center	dti !	wsg !	bh	wsg+	bh	bh
Default Zone	bh	bh	bh	bh	bh	bh

On the displayed windows, VPN Segmentation Policies and Internet Access Policies, click the **Add** buttons to display the forms. To create a zone-based firewall, you must define:

1. the VPN zones for organizing your private sites and/or subnets; a subnet must be part of the private IP address range
2. the segmentation policies of the VPN zones, i.e. the ability of these zones to communicate with one another
3. the application sets for organizing your collection of Internet applications based on the SaaS dictionary or on Protocol and Port
4. the Internet Access policies that manage the communication between the VPN zones and the application sets (ability to communicate and used method - DTI, WSG or backhauling).

Refer to the following sections for detailed explanations.

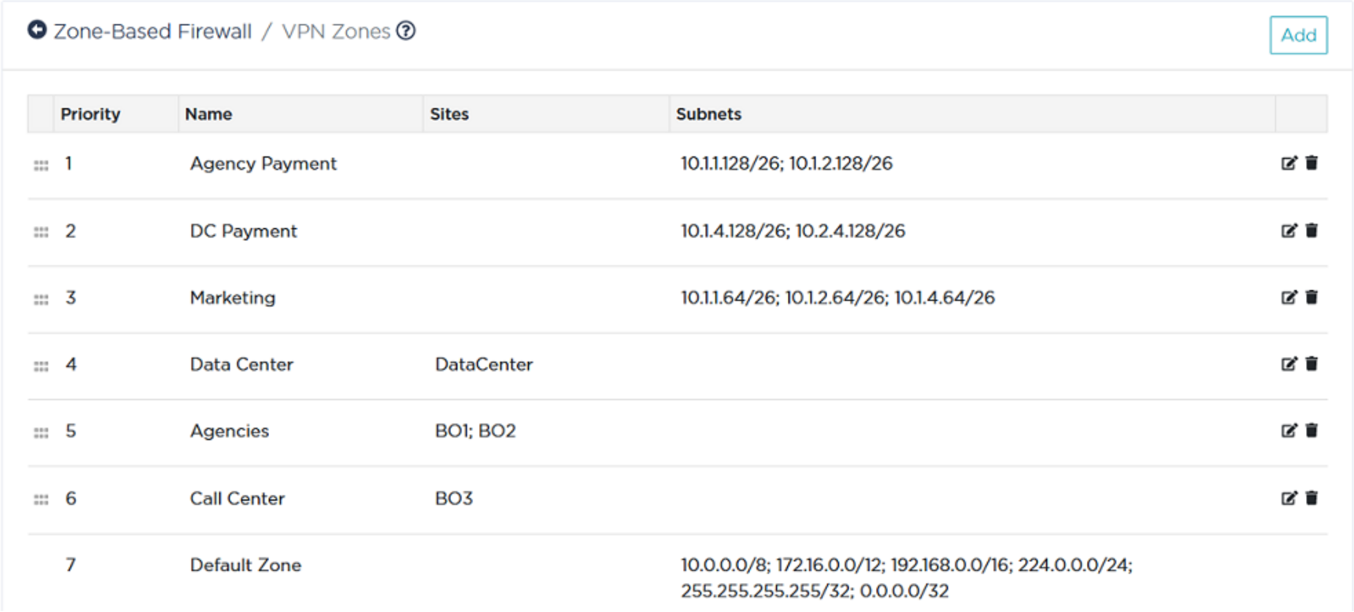
Defining VPN Zones

Refer to "Use Case 12" diagram where 6 zones are defined:

- Default Zone: this zone contains all the subnets of the private IP address range. This zone is configured by default and cannot be modified.
- Data Center: geographical zone that contains all the subnets of the Data Center site (DataCenter and DataCenter2); these subnets are not included in higher priority zones.
- Agencies: geographical zone that contains all the subnets of the Agency sites (B01, B02); they are not included in higher priority zones.
- Call Center: geographical zone that contains the subnets of the B03 site; they are not included in higher priority zones.
- DC Payment: logical zone that contains sets of subnets that may belong to one or several sites. DC Payment subnets are included in the Data Center zone (DataCenter and DataCenter2).
- Agency Payment: logical zone that contains sets of subnets that may belong to one or several sites. Agency Payment subnets are included in the Agencies zone (B01 and B02).
- Marketing: logical zone that contains sets of subnets that may belong to one or several sites. Marketing subnets are included in both the Agencies zone and DataCenter zone (B01, B02 and DataCenter).

Note: High priority VPN zones are included in low priority VPN zones.

Warning: for system performance reasons, do not define more than 30 VPN zones. Also favor subnet definition over site hosts selection (/32).



Priority	Name	Sites	Subnets
1	Agency Payment		10.1.1.128/26; 10.1.2.128/26
2	DC Payment		10.1.4.128/26; 10.2.4.128/26
3	Marketing		10.1.1.64/26; 10.1.2.64/26; 10.1.4.64/26
4	Data Center	DataCenter	
5	Agencies	BO1; BO2	
6	Call Center	BO3	
7	Default Zone		10.0.0.0/8; 172.16.0.0/12; 192.168.0.0/16; 224.0.0.0/24; 255.255.255.255/32; 0.0.0.0/32

Defining the Agencies zone

1 In the VPN Segmentation Policies panel of the Zone-Based Firewall window, click the Edit VPN Zones button.

The Default Zone with its subnets is already displayed. You cannot modify it.

2 Click Add in the top right corner of the window to view the VPN Zone form.

3 Type 'Agencies' as the Name of the zone.

4 Enter a low Priority (5) for this zone because it is clearly identified with no subnet overlap. 1 corresponds to the highest priority, 6 is the lowest priority value.

> **Note:** at any time, you may change the priority of a VPN zone by positioning the cursor over the ⠿ icon and dragging the line to the desired position. The priority values of all the VPN zones automatically adjust to the new list order.

5 From the Sites list which includes all the Sites you have configured in "Use Case 1", move B01 and B02 Sites to the right list through the middle arrow bar.

Note that you can find a specific Site through the Search fields.

You do not need to specify Subnets since identification was done via Site Names.

6 Click **Create** to validate.

Defining the Call Center zone

1 In the VPN Segmentation Policies panel of the Zone-Based Firewall window, click the Edit VPN Zones button.

2 Click Add in the top right corner of the window to view the VPN Zone form.

3 Type 'Call Center' as the Name of the zone.

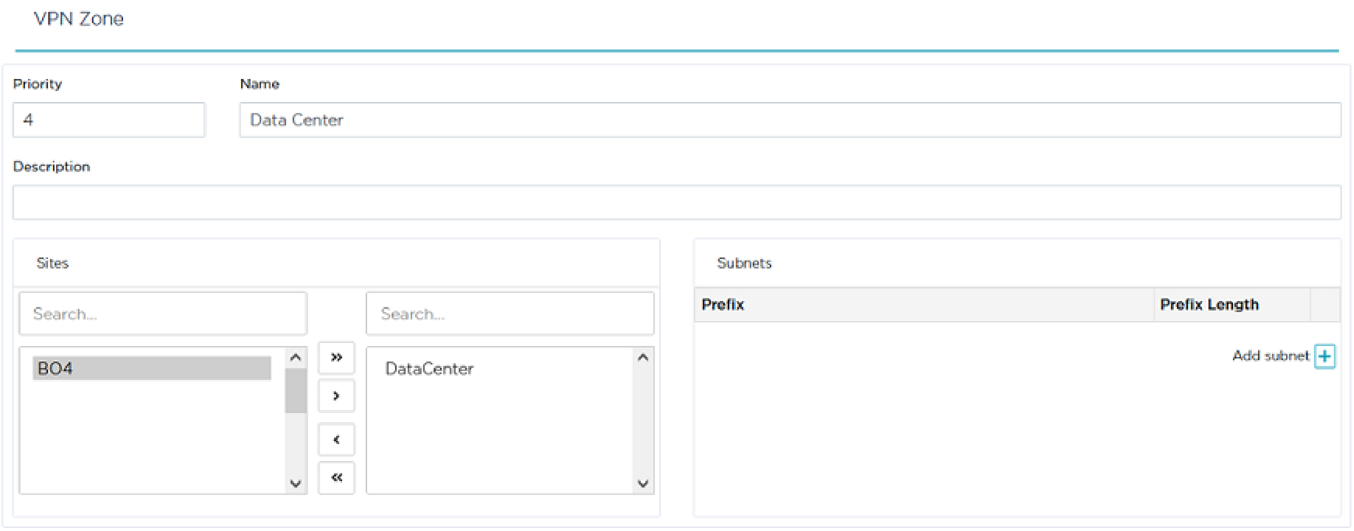
4 Enter a low Priority (6) for this zone because it is clearly identified with no subnet overlap. 1 corresponds to the highest priority, 6 is the lowest priority value.

5 From the Sites list which includes all the Sites you have configured in "Use Case 1", move the B03 Site to the right list through the middle arrow bar.

Note that you can find a specific Site through the Search fields.

6 Click **Create** to validate.

Defining the Data Center Zone



VPN Zone

Priority: 4

Name: Data Center

Description:

Sites: B04 → DataCenter

Subnets

Prefix	Prefix Length

1 In the VPN Segmentation Policies panel of the Zone-Based Firewall window, click the Edit VPN Zones button.

2 Click Add in the top right corner of the window to view the VPN Zone form.

3 Type 'Data Center' as the Name of the zone.

4 Enter a low Priority (4) for this zone because it is clearly identified with no subnet overlap.

5 DataCenter and DataCenter2 are two appliances on the same Site named DataCenter ("Use Case 1"). From the Sites list which includes all the Sites you have configured, move the DataCenter Site to the right list through the middle arrow bar.

Note that you can find a specific Site through the Search fields.

6 Click **Create** to validate.

Defining the DC Payment zone

1 In the VPN Segmentation Policies panel of the Zone-Based Firewall window, click the Edit VPN Zones button.

2 Click Add in the top right corner of the window to view the VPN Zone form.

3 Type 'DC Payment' as the Name of the zone.

4 Enter a high Priority value (2) for this zone because of the acuteness of its subnet definition.

5 Use the Subnets panel to identify DC Payment two subnets: 10.1.4.128/26 and 10.2.4.128/26.

6 Click **Create** to validate.

Defining the Agency Payment zone

1 In the VPN Segmentation Policies panel of the Zone-Based Firewall window, click the Edit VPN Zones button.

2 Click Add in the top right corner of the window to view the VPN Zone form.

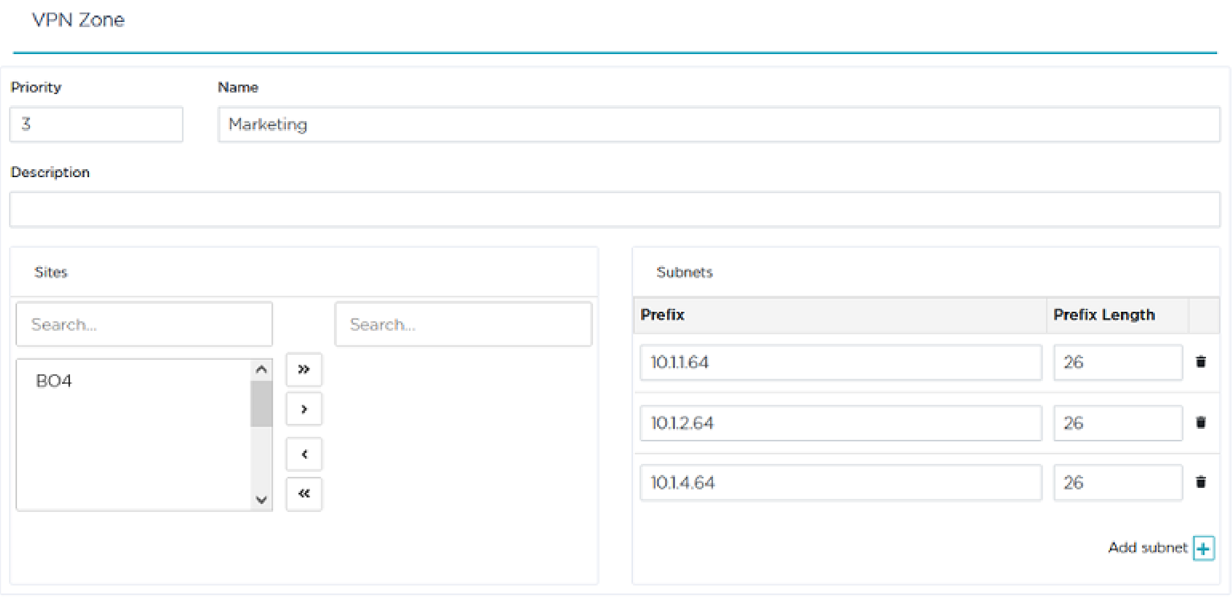
3 Type 'Agency Payment' as the Name of the zone.

4 Enter a high Priority value (1) for this zone because of the acuteness of its subnet definition.

5 Use the Subnets panel to identify Agency Payment two subnets: 10.1.1.128/26 and 10.1.2.128/26.

6 Click **Create** to validate.

Defining the Marketing zone



VPN Zone

Priority: 3

Name: Marketing

Description:

Sites

Search...

BO4

Search...

Subnets

Prefix	Prefix Length
10.1.1.64	26
10.1.2.64	26
10.1.4.64	26

1 In the VPN Segmentation Policies panel of the Zone-Based Firewall window, click the Edit VPN Zones button.

2 Click Add in the top right corner of the window to view the VPN Zone form.

3 Type 'Marketing' as the Name of the zone.

4 Enter an average Priority value (3) for this zone.

5 Use the Subnets panel to identify the Marketing zone three subnets: 10.1.1.64/26, 10.1.2.64/26 and 10.1.4.64/26.

6 Click **Create** to validate.

Modifying or deleting a VPN Zone

In the Zone-Based Firewall / VPN Zones window:

- Click ✎ to edit the configuration of a VPN zone. Modify any values and press Update to save your settings.
- Click 🗑 if you want to delete a VPN zone. The system asks you to click the icon a second time to confirm your action.

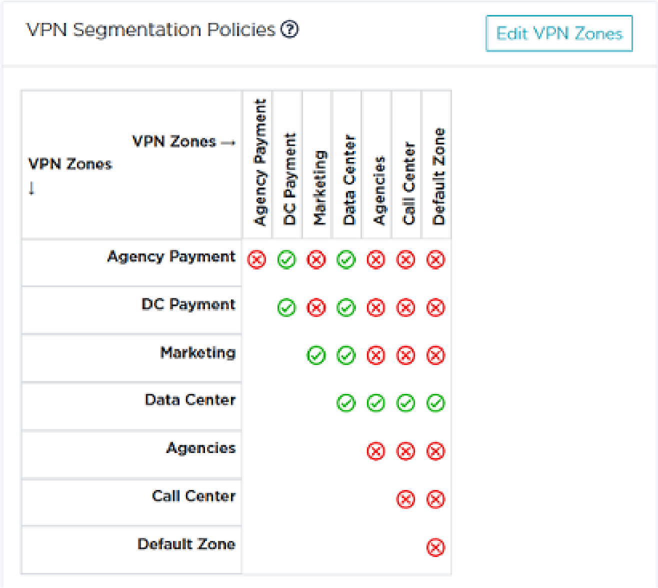
After you have defined your VPN zones, you must apply VPN Segmentation Policies to these zones.

Setting VPN Segmentation Policies

By default, all the VPN Zones are able to communicate with one another (✓).

To change this status, simply click the icon for each VPN Zone pair in the VPN Segmentation Policies matrix.

> **Note:** This matrix is symmetrical, i.e. the segmentation policy between two VPN zones is the same in both directions and needs to be configured only once. For example, the policy is the same for Data Center-Agencies and Agencies-Data Center.



VPN Zones → VPN Zones ↓	Agency Payment	DC Payment	Marketing	Data Center	Agencies	Call Center	Default Zone
Agency Payment	✗	✓	✗	✓	✗	✗	✗
DC Payment		✓	✗	✓	✗	✗	✗
Marketing			✓	✓	✗	✗	✗
Data Center				✓	✓	✓	✓
Agencies					✗	✗	✗
Call Center						✗	✗
Default Zone							✗

This configuration implements the following policies (refer to "Use Case 12" diagram):

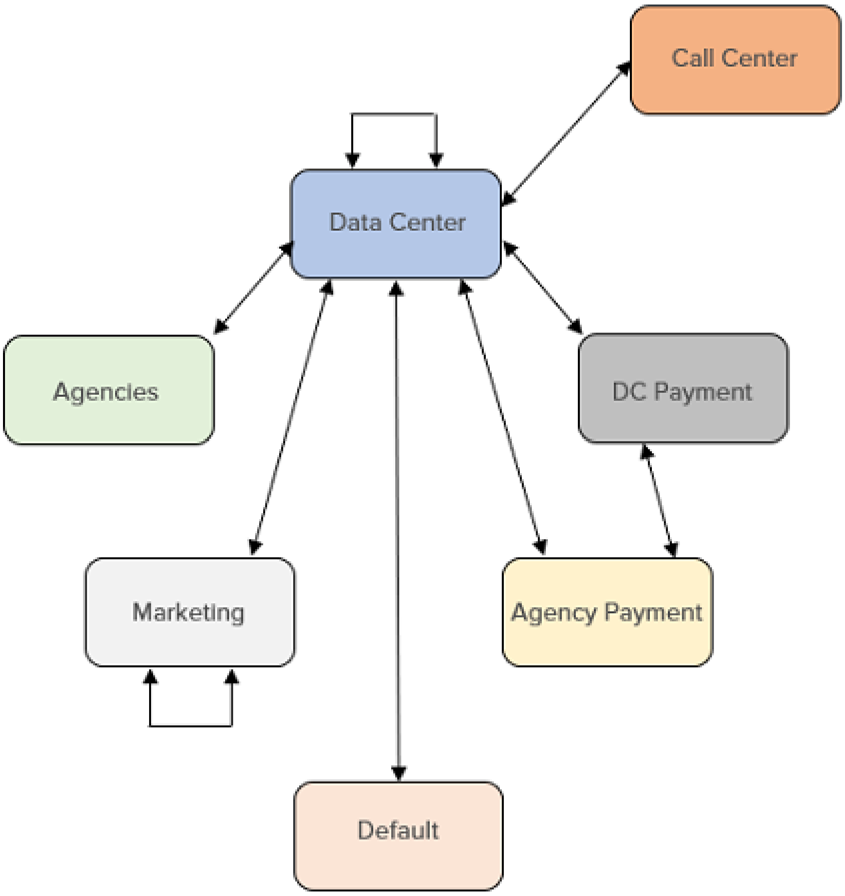
- the appliances that do not belong to any other zone than the Default Zone can communicate with the appliances of the Data Center zone
- the appliances in the Data Center zone can communicate with all the other zones, including appliances of other sites in the Data Center zone

  > **Warning:** some appliances belong to Data Center 1 and Data Center 2 but not to the Data Center zone since they belong to higher priority zones such as Marketing and DC Payment.

- the appliances in the Agencies zone can only communicate with appliances in the Data Center zone. They cannot communicate with one another if they are not on the same site

  > **Warning:** some appliances belong to B01 and B02 sites but not to the Agencies zone since they belong to higher priority zones such as Marketing and Agency Payment.

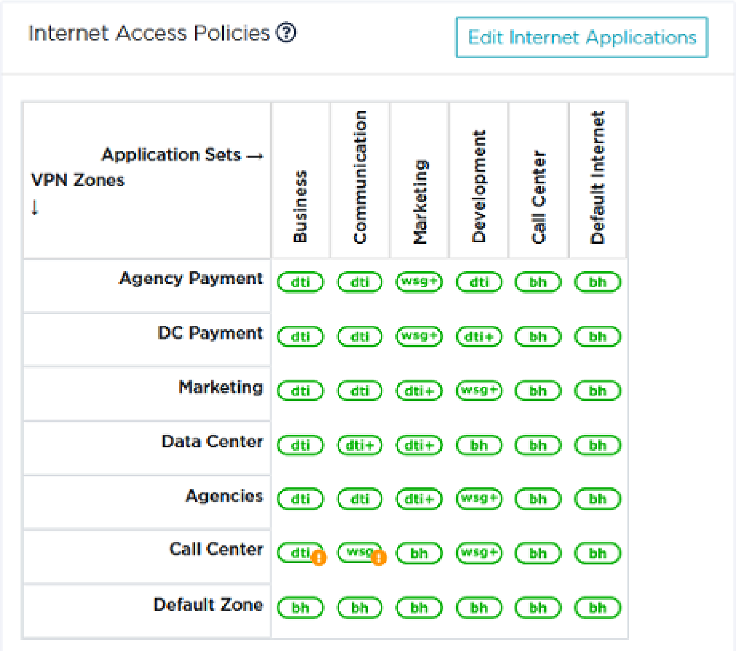
- the appliances in the Marketing zone can all communicate with one another, whichever site they are related to
- the appliances in the DC Payment zone can communicate with appliances in the Agency Payment zone



Defining Application Sets

In order to manage the Internet traffic, i.e. the connection from a site/subnet in your private network to any application, the first step consists in creating collections of applications (application sets) based on the SaaS dictionary **or** on Protocol and Port.

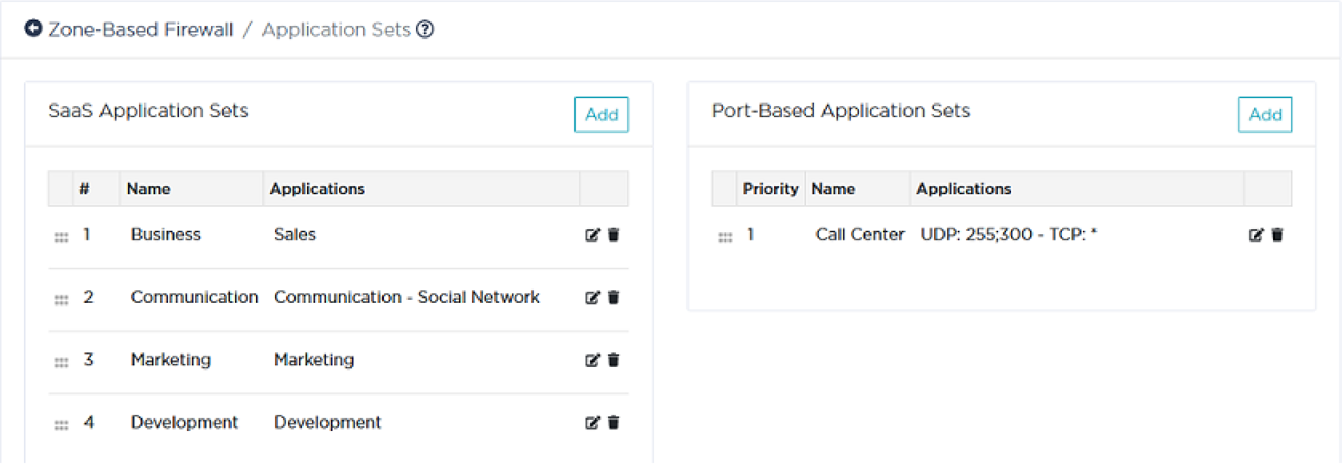
> **Warning:** for system performance reasons, do not define more than 15 Application Sets.



Internet Access Policies ⓘ

Application Sets → VPN Zones ↓	Business	Communication	Marketing	Development	Call Center	Default Internet
Agency Payment	dti	dti	wsg+	dti	bh	bh
DC Payment	dti	dti	wsg+	dti+	bh	bh
Marketing	dti	dti	dti+	wsg+	bh	bh
Data Center	dti	dti+	dti+	bh	bh	bh
Agencies	dti	dti	dti+	wsg+	bh	bh
Call Center	dti !	wsg !	bh	wsg+	bh	bh
Default Zone	bh	bh	bh	bh	bh	bh

In the current Use Case, 5 application sets are created: Business, Communication, Marketing, Development and Call Center. Default Internet contains all the other applications.



Zone-Based Firewall / Application Sets ⓘ

SaaS Application Sets

#	Name	Applications
1	Business	Sales
2	Communication	Communication - Social Network
3	Marketing	Marketing
4	Development	Development

Port-Based Application Sets

Priority	Name	Applications
1	Call Center	UDP: 255;300 - TCP: *

Defining the Business application set

1. In the Internet Access Policies panel of the Zone-Based Firewall window, click the Edit Internet Applications button.
2. Click Add in the top right corner of the SaaS Application Sets panel to view the form.
3. Type 'Business' as the Name of the application set.
4. From the list of Applications, select 'Sales' and move it to the right list through the middle arrow bar. The listed applications correspond to existing SaaS applications that were created from the SaaS dictionary. They are associated with subnet information and identified through the "(identification on first packet)" label at the end of their respective descriptions.

   Note that you can find a specific application through the Search fields.

   > **Note:** Each application can only belong to one application set.

5. Click **Create** to validate.

Defining the Communication, Marketing and Development application sets

Proceed exactly as for the previous Business application set. Note that the Communication application set includes two SaaS applications.

Defining the Call Center application set

This application set is based on Protocol and Port.

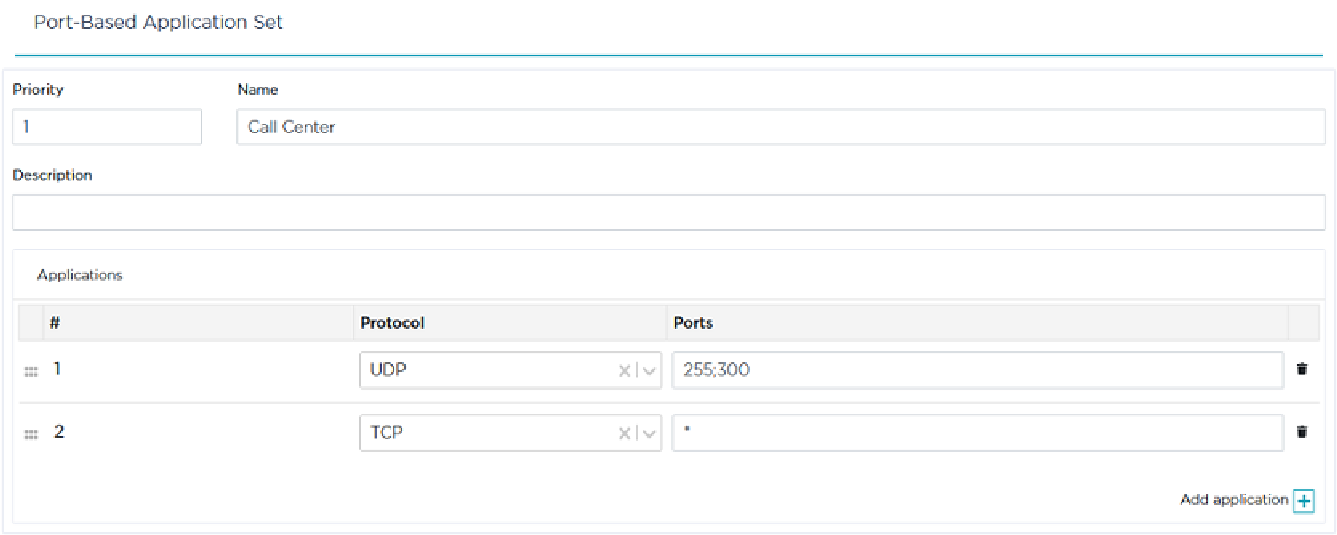
1. In the Internet Access Policies panel of the Zone-Based Firewall window, click the Edit Internet Applications button.
2. Click Add in the top right corner of the Port-Based Application Sets panel to view the form.
3. Modify the Priority for this application set (1) if needed. 1 corresponds to the highest priority, 6 is the lowest priority value.

   High priority applications may overlap some lower priority applications.

4. Type 'Call Center' as the Name of the application set.
5. In the bottom right corner of the Applications panel, click **Add Application**. The creation form is displayed.
6. From the Protocol list, select 'UDP' and enter '255;300' as Ports.

> **Note:** at any time, you may change the list position of an application by positioning the cursor over the ⠿ icon and dragging the line to the desired position.

7 Define the parameters of the second application. Instead of selecting the TCP protocol from the list, type 6 in the Protocol field (refer to **iana** list of protocol numbers). Enter * as Port (all the available ports are taken into account).



Port-Based Application Set

Priority: 1

Name: Call Center

Description:

Applications

	#	Protocol	Ports	
⠿	1	UDP	255;300	🗑
⠿	2	TCP	*	🗑

Add application +

8 Click **Create** to validate.

> **Note:** in the Zone-Based Firewall / Applications Sets window, you may change the priority of a Port-Based Application Set by positioning the cursor over the ⠿ icon and dragging the line to the desired position. The priority values of all the Port-Based Application Sets automatically adjust to the new list order.

Modifying or deleting a VPN Zone

In the Zone-Based Firewall/Application Sets window:

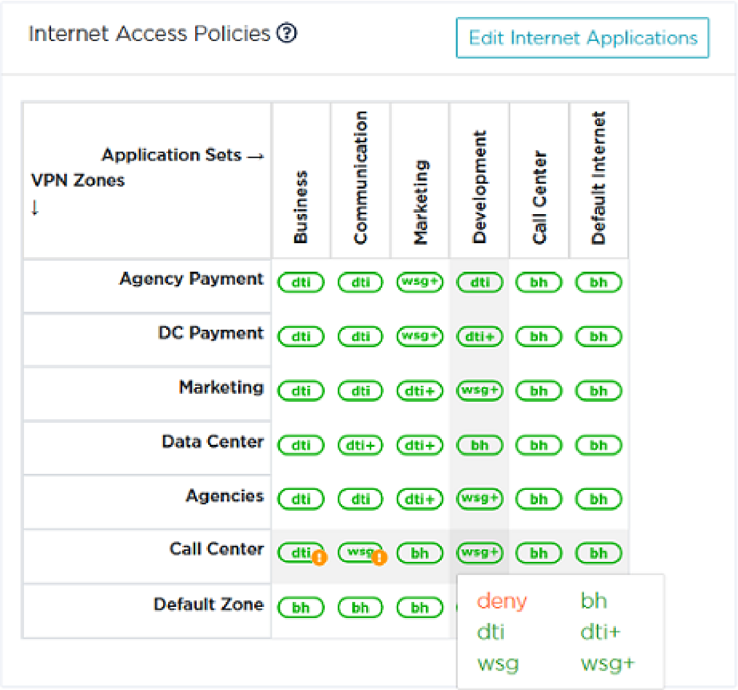
- Click ✎ to edit the configuration of an Application Set. Modify any values and click Update to save your settings.
- Click 🗑 if you want to delete an Application Set. The system asks you to click the icon a second time to confirm your action.

After you have defined your application sets, you must apply Internet Access Policies to them.

Setting Internet Access Policies

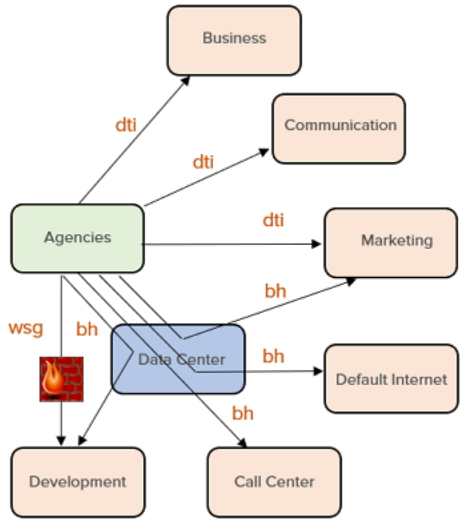
By default, VPN Zones cannot reach Internet applications (⊗) except the Default Zone which can access the Internet in backhaul (bh) mode (see below). Indeed, Internet access is by default authorized in the LAN, either through the underlay (MPLS) or through the overlay.

To change the default status, click the icon for each VPN Zone/Application Set pair in the Internet Access Policies matrix and select one option among bh, dti, dti+, wsg and wsg+ and deny. This configuration is kept after any SD-WAN Orchestrator upgrade.



Application Sets → VPN Zones ↓	Business	Communication	Marketing	Development	Call Center	Default Internet
Agency Payment	dti	dti	wsg+	dti	bh	bh
DC Payment	dti	dti	wsg+	dti+	bh	bh
Marketing	dti	dti	dti+	wsg+	bh	bh
Data Center	dti	dti+	dti+	bh	bh	bh
Agencies	dti	dti	dti+	wsg+	bh	bh
Call Center	dti !	wsg !	bh	wsg+	bh	bh
Default Zone	bh	bh	bh			

The following diagram illustrates the Internet Access Policies that have been defined for the Agencies VPN zone to access the applications in the Business, Communication, Marketing, Development, Call Center and Default Internet application sets ("Use Case 12").



Internet Access Policies

deny	The traffic is dropped.
bh	Backhaul: the traffic is routed to the Data Center appliance (through underlay or overlay according to the current deployment) which must be able to route it to a firewall or proxy. • with an MPLS L2 interface, the traffic is sent via the underlay and routed by the MPLS network • with an MPLS L3 or Internet L3 interface, the traffic is sent via the overlay to the Data Center appliance Backhauling can be activated on hub appliances (in Router or Bridge-Router mode) and on appliances in Bridge mode.
dti	Direct to Internet: the traffic is directly sent to the Internet. This policy is only available for Internet interfaces. With an interface which is not eligible for DTI (for example, MPLS interface), the traffic is dropped. You may activate eligibility to DTI globally in Advanced Configuration -> Transport Network Settings or individually on any Internet L3 interface. As a consequence, NAT is automatically enabled since DTI traffic must be NATted by the WAN interface. Also, Local Port Forwarding parameters may be specified for this interface.
dti+	Direct to Internet or Backhauling: the traffic is either sent in DTI if the interface authorizes it (Internet interface), or backhauled to the

	Data Center (for a MPLS interface). To activate this policy, refer to the **bh** and **dti** options.
wsg	EdgeSentry or Web Security Gateway: the traffic is routed via an IPsec tunnel to EdgeSentry or to a web security gateway in the Cloud. This policy is only available with Internet interfaces when EdgeSentry is activated or when there is a configured Web Security Gateway. The traffic is dropped on an interface if either EdgeSentry is not activated on it or this interface is not eligible for WSG (there is no configured WSG tunnel).
wsg+	EdgeSentry or Web Security Gateway or Backhauling: the traffic is either routed to EdgeSentry (with an interface where EdgeSentry is activated) or to a web security gateway (with an interface eligible for WSG), or the traffic is backhauled to the Data Center (EdgeSentry is not activated and there is no configured WSG tunnel). To activate this policy, refer to the **wsg** and **bh** options.

Policy Behavior by Interface type and configuration

Interface/Policy	dti	dti+	wsg	wsg+	bh	deny
L2	drop	allow	drop	allow	allow	drop
L2 + eligible DTI	not available					
L3	drop	tunnel to dc	drop	tunnel to dc	tunnel to dc	drop
L3 + eligible DTI	dti	dti	drop	tunnel to dc	tunnel to dc	drop
L3 + WSG	drop	tunnel to dc	tunnel to gateway	tunnel to gateway	tunnel to dc	drop
L3 + DTI + WSG	dti	dti	tunnel to gateway	tunnel to gateway	tunnel to dc	drop

Impact on the Network Services

If at least one appliance within the VPN Zone has no WAN interface that supports 'dti', a yellow exclamation mark is displayed on the Internet Access Policy icon: dti!. When positioning your cursor over the exclamation mark, you may know which appliance(s) are involved. The same information is displayed at the top of the **Network -> Zone-Based Firewall** main window.

The same rule applies to 'wsg'.

In these error cases, the traffic is dropped and all the SD-WAN Orchestrator services are deactivated.

5 Supervising the Network

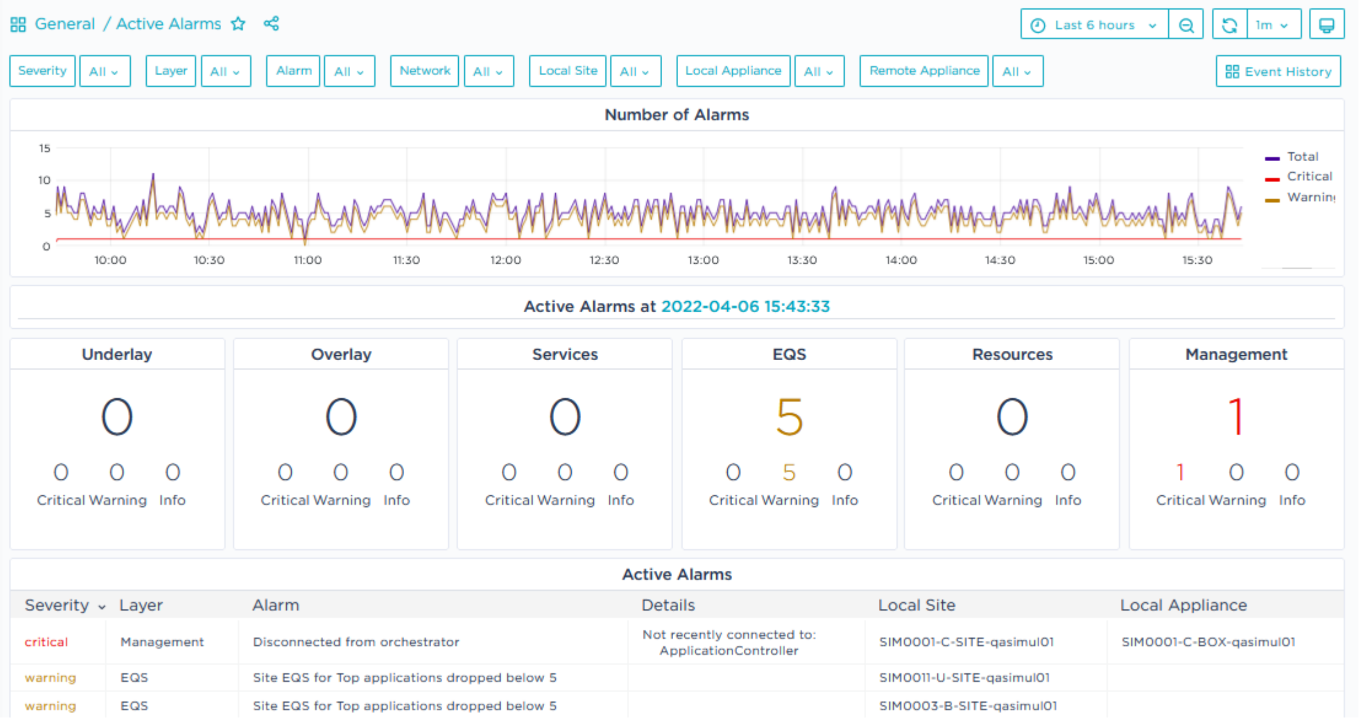
This section describes how to check the network health by supervising alarm and event activity. It also explains how you can configure alarm notification.

Checking Active Alarms

You can access this dashboard by

- selecting the **Supervision -> Active Alarms** function from the SD-WAN Orchestrator main menu,
- drilling down on any colored alarm counter in the Overview dashboard,
- clicking the Active Alarms button in the top right corner of the Event History dashboard.

  Navigating between the Active Alarms and Event History dashboards enables you to keep the defined time range and filters,
- clicking the Notification counter 🔔3 in the SD-WAN Orchestrator main menu.



Active Alarms at 2022-04-06 15:43:33

Underlay	Overlay	Services	EQS	Resources	Management
0	0	0	5	0	1
0 Critical 0 Warning 0 Info	0 Critical 0 Warning 0 Info	0 Critical 0 Warning 0 Info	0 Critical 5 Warning 0 Info	0 Critical 0 Warning 0 Info	1 Critical 0 Warning 0 Info

Active Alarms

Severity	Layer	Alarm	Details	Local Site	Local Appliance
critical	Management	Disconnected from orchestrator	Not recently connected to: ApplicationController	SIM0001-C-SITE-qasimul01	SIM0001-C-BOX-qasimul01
warning	EQS	Site EQS for Top applications dropped below 5		SIM0011-U-SITE-qasimul01	
warning	EQS	Site EQS for Top applications dropped below 5		SIM0003-B-SITE-qasimul01	

This dashboard displays the active Critical, Warning and Information alarms, i.e. their status is still 'raised' at the time specified on the second pane (Active Alarms at). This time also corresponds to the last point at the right end of the graph. You may filter these alarms by:

- severity
- layer
  - Underlay: physical connection between devices (LAN, WAN), VRRP or HA state change, appliance configuration
  - Overlay: connection between appliances or external gateways through IPsec tunnels

  - Services: services provided with the appliances such as application visibility, application control, WAN optimization, firewall
  - EQS: site EQS for applications and site connectivity
  - Resources: device local resources, i.e. hardware monitoring
  - Management: connection to Azure components (Orchestrator, ZTP Server, etc.)
- alarm
- network
- local site
- local appliance: first appliance in the case of tunnel failure or end-to-end connectivity lost issue
- remote appliance: second appliance in the case of tunnel failure or end-to-end connectivity lost issue

The Alarm Filter stack of values only contains the alarms that have already been raised (not all the system alarms).

The severity of alarms is specified by the following colors: red for Critical, orange for Warning and green for Information.

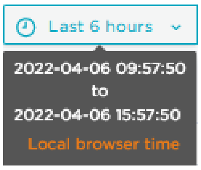
The filters you select at the top of the dashboard apply to all three panes and to the Event History dashboard when you call it from the top button.

The last dashboard pane lists the active alarms with the network objects they apply to.

Navigating the Dashboard

Selecting the Display Criteria

From the button toolbar located in the top right corner of the dashboard, click the Time Range button. It specifies the current time range.



2022-04-06 09:57:50
to
2022-04-06 15:57:50
Local browser time

You can modify the default time range by applying an Absolute Time Range you have defined, or by selecting a Relative Time Range from the list.

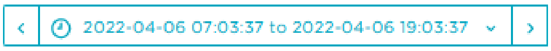
The dashboard default time zone (local browser time) is displayed in orange. You can modify this value by selecting **Change time settings** in the Time Range selector.

If you want your dashboard to be refreshed automatically, select a period from the Refreshing stack:

Instead of defining an automatic refresh period, you can refresh the dashboard manually by hitting the ⟳ button.

Zooming Out

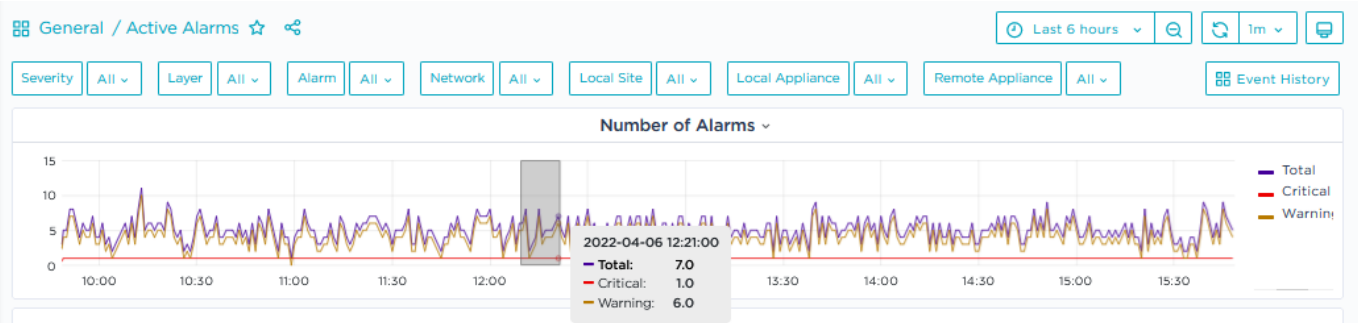
Click the ⊖ button in the top right button toolbar to zoom out dashboard display. The time range is extended as specified at the top of the window:

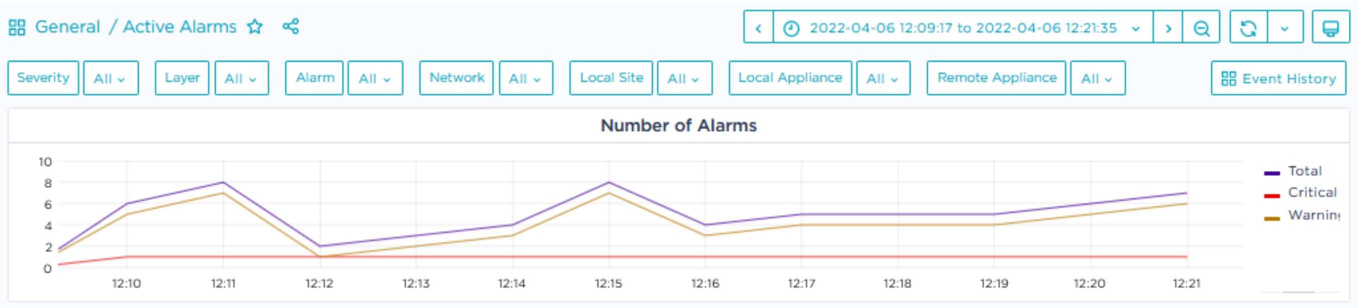


You can use the arrows on both sides of the time range to move forward and backward (one time range shifts).

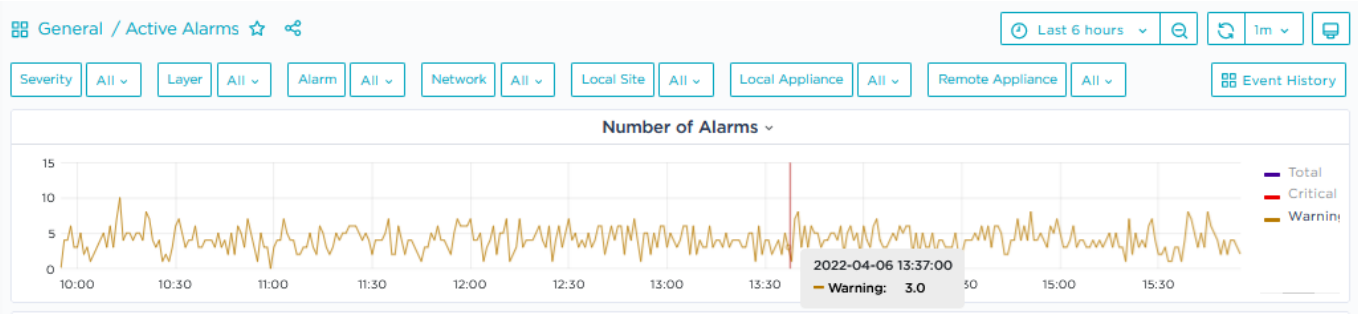
Zooming In

Zoom in on the time series graph by positioning your cursor on a specific section of the graph and dragging to the right. The result graph displays more points at a lower display rate. You can continue zooming in until you reach the necessary detailed report.



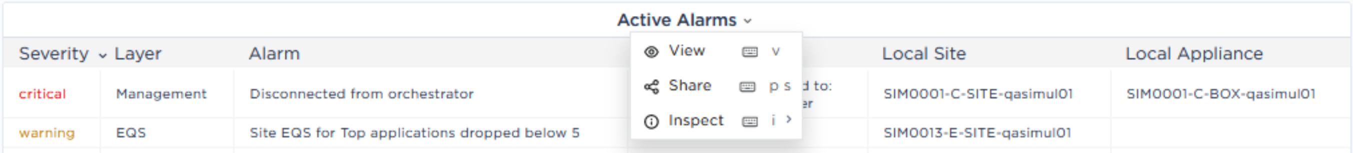


On any time series graph, you may display the evolution curve of each type of alarm separately by selecting the alarm category in the graph legend. The image below only displays Warning alarms. To go back to Total display, subsequently click all the categories while holding down the CTRL key of your keyboard.



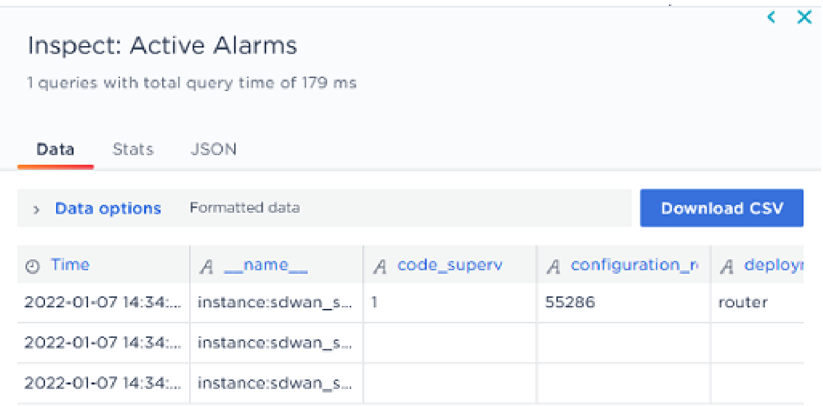
Using Dashboard Cell functions

Click the title of any cell/pane in the dashboard to display the functional menu. The available functions depend on the type of presentation (time series graph, table, etc.).



Severity	Layer	Alarm		Local Site	Local Appliance
critical	Management	Disconnected from orchestrator	d to: er	SIM0001-C-SITE-qasimul01	SIM0001-C-BOX-qasimul01
warning	EQS	Site EQS for Top applications dropped below 5		SIM0013-E-SITE-qasimul01	

- Use the **View** function to fully display this dashboard cell.
- Use the **Share** function to link, embed or take a snapshot of this dashboard cell.
- Use the **Inspect -> Data** function to export the cell data as a .csv file, display statistics and JSON panels, etc.



Time	__name__	code_superv	configuration_r	deployr
2022-01-07 14:34:...	instance:sdwan_s...	1	55286	router
2022-01-07 14:34:...	instance:sdwan_s...			
2022-01-07 14:34:...	instance:sdwan_s...			

Click Download CSV, then open the file in MS Excel and save it.

- Use the **More -> Toggle legend** function to hide/display the legend when the cell contains a graph. You can also click legend elements for exclusive display.

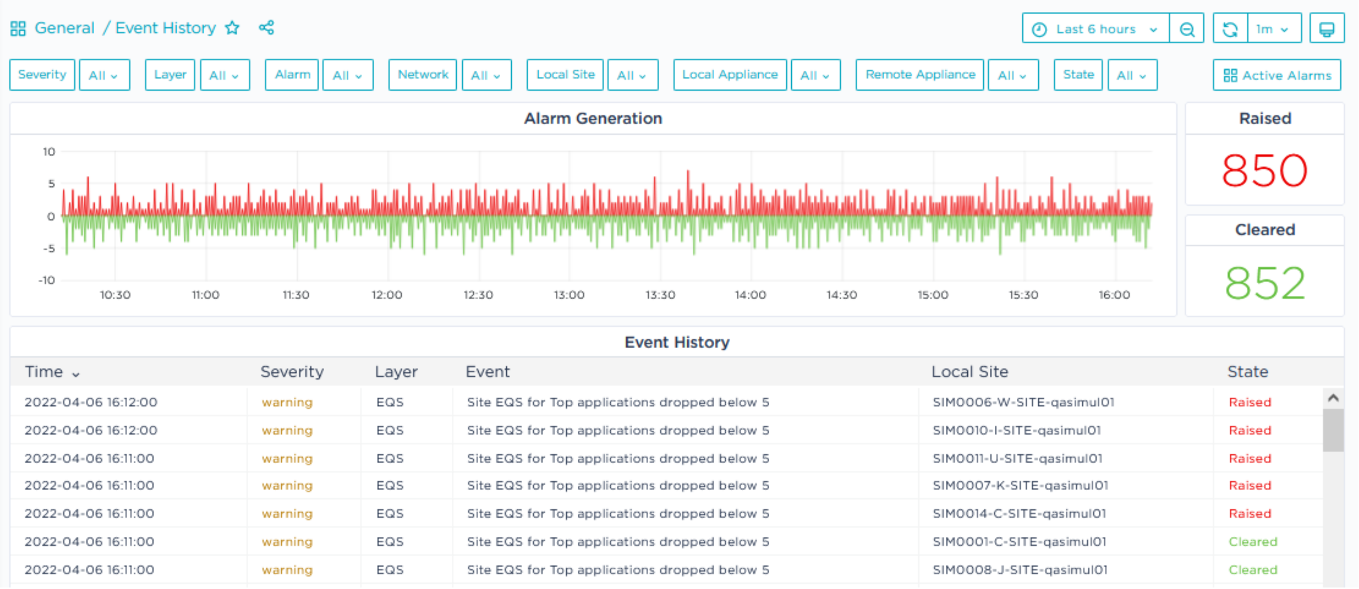
Sorting Table columns

On a table, you may sort column data by clicking the column header names.

Viewing Event History

Select the **Supervision -> Event History** function from the SD-WAN Orchestrator main menu to display the following dashboard. You can also access this dashboard by clicking the Event History button in the top right corner of the Active Alarms dashboard.

Navigating between the Active Alarms and Event History dashboards enables you to keep the defined time range and filters.



Event History

Time	Severity	Layer	Event	Local Site	State
2022-04-06 16:12:00	warning	EQS	Site EQS for Top applications dropped below 5	SIM0006-W-SITE-qasimul01	Raised
2022-04-06 16:12:00	warning	EQS	Site EQS for Top applications dropped below 5	SIM0010-I-SITE-qasimul01	Raised
2022-04-06 16:11:00	warning	EQS	Site EQS for Top applications dropped below 5	SIM0011-U-SITE-qasimul01	Raised
2022-04-06 16:11:00	warning	EQS	Site EQS for Top applications dropped below 5	SIM0007-K-SITE-qasimul01	Raised
2022-04-06 16:11:00	warning	EQS	Site EQS for Top applications dropped below 5	SIM0014-C-SITE-qasimul01	Raised
2022-04-06 16:11:00	warning	EQS	Site EQS for Top applications dropped below 5	SIM0001-C-SITE-qasimul01	Cleared
2022-04-06 16:11:00	warning	EQS	Site EQS for Top applications dropped below 5	SIM0008-J-SITE-qasimul01	Cleared

- The first pane of the dashboard displays the time series graph of the Raised and Cleared alarms during the selected Time Range.

  > **Note:** The Event History Time Range cannot exceed the last 15 days. The Relative Time Ranges higher than 15 days which are available from the Time Range selector are useless. To avoid blank data, use the Absolute Time Range option and enter 'now-15d'; then click **Apply**.

  The counters at the right of the panel show the number of Raised and Cleared alarms for the whole Time Range. Position the cursor on a point of the graph to display, through a tooltip, the number of alarms at a specific time in the time range.

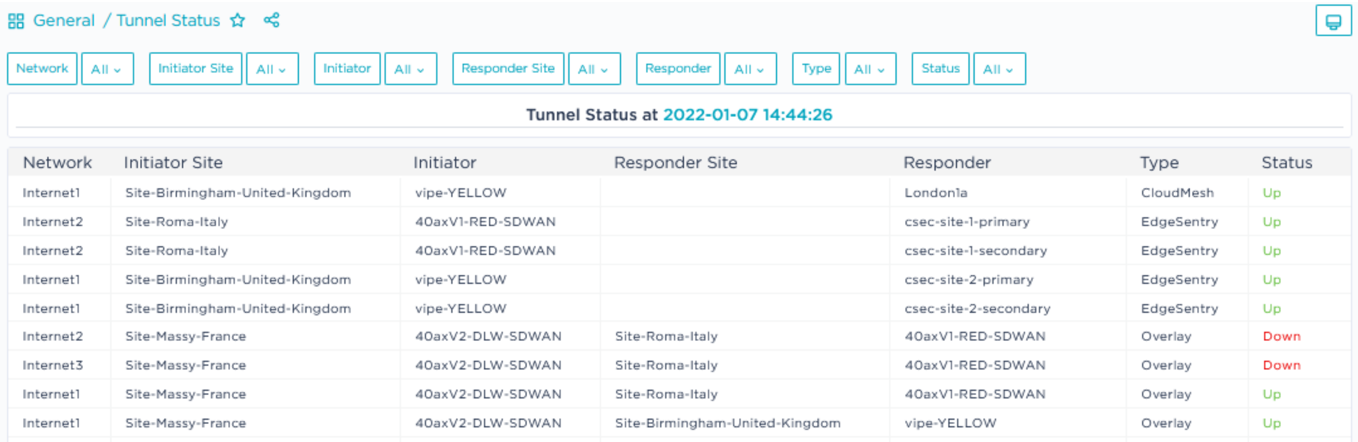
- The second pane of the dashboard lists the Critical, Warning and Information alarms raised or cleared at the specified Time during the selected Time Range. The State field identifies the event, i.e. whether the alarm is still raised/active, already cleared, updated (the error code has changed) or logged (there is a change in VRRP configuration).

Also see how to navigate the dashboard.

Checking Tunnel Status

Select the **Supervision -> Tunnel Status** function from the SD-WAN Orchestrator main menu to display the following dashboard.

This dashboard lists all the tunnels you have configured and indicates whether they are up or down at the specified time (Tunnel Status at).



Tunnel Status at 2022-01-07 14:44:26

Network	Initiator Site	Initiator	Responder Site	Responder	Type	Status
Internet1	Site-Birmingham-United-Kingdom	vipe-YELLOW		London1a	CloudMesh	Up
Internet2	Site-Roma-Italy	40axV1-RED-SDWAN		csec-site-1-primary	EdgeSentry	Up
Internet2	Site-Roma-Italy	40axV1-RED-SDWAN		csec-site-1-secondary	EdgeSentry	Up
Internet1	Site-Birmingham-United-Kingdom	vipe-YELLOW		csec-site-2-primary	EdgeSentry	Up
Internet1	Site-Birmingham-United-Kingdom	vipe-YELLOW		csec-site-2-secondary	EdgeSentry	Up
Internet2	Site-Massy-France	40axV2-DLW-SDWAN	Site-Roma-Italy	40axV1-RED-SDWAN	Overlay	Down
Internet3	Site-Massy-France	40axV2-DLW-SDWAN	Site-Roma-Italy	40axV1-RED-SDWAN	Overlay	Down
Internet1	Site-Massy-France	40axV2-DLW-SDWAN	Site-Roma-Italy	40axV1-RED-SDWAN	Overlay	Up
Internet1	Site-Massy-France	40axV2-DLW-SDWAN	Site-Birmingham-United-Kingdom	vipe-YELLOW	Overlay	Up

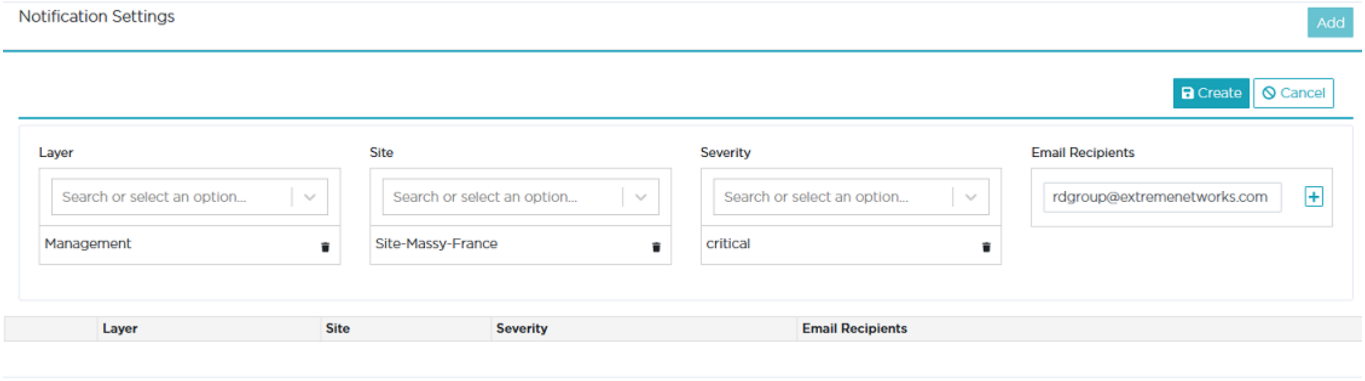
Configuring Alarm Notification

At any time, to be informed of the Critical, Warning and Information alarms that have been raised or cleared by the SD-WAN Orchestrator without displaying the Active Alarms dashboard, you may configure alarm notification through the **Supervision -> Notification Settings** function.

> **Note:** This function is only available to the Administrator and Network Manager profiles.

Set an Alarm Notification instance (or Alert)

1. Click the **Add** button.
2. From the Layer stack of values, select one or several options:
   - Underlay: physical connection between devices (LAN, WAN), VRRP state change, appliance configuration
   - Overlay: connection between appliances or external gateways through IPsec tunnels
   - Services: services provided with the appliances such as application visibility, application control, WAN optimization, dynamic WAN selection, firewall
   - EQS: site EQS for applications and site connectivity
   - Resources: device local resources, i.e. hardware monitoring
   - Management: connection to Azure components (Orchestrator, ZTP Server, etc.)
   - blank: if you do not select any option, all the layers are taken into account
3. From the Site stack of values, select one or several sites in your network. You'll be notified of alarms related to these sites only.
4. From the Severity stack of values, define the type of alarm (information, warning and critical) which must trigger the notification messages.
5. Enter the email address of one or several Recipients.



Notification Settings

Layer	Site	Severity	Email Recipients
Search or select an option...	Search or select an option...	Search or select an option...	rdgroup@extremenetworks.com
Management	Site-Massy-France	critical	

Layer	Site	Severity	Email Recipients

6. Finally, click **Create**.

Whenever the SD-WAN Orchestrator raises a critical alarm about any connection issue to Azure components (Orchestrator, ZTP Server, etc.) for Site Massy, all the recipients included in rdgroup@extremenetworks.com are notified of this alarm by email.

Note that the

counter in the Main Menu also keeps you informed of the number of active alarms.

The color of this counter corresponds to alarm highest severity, i.e. if there is at least one raised critical alarm, the counter is red. The counter tooltip displays alarm distribution per category (information, warning, critical).

You may click this icon to display the Supervision -> Active Alarms dashboard.

Supervision Alarms by Layer

The table below lists the SD-WAN Orchestrator alarms by layer and briefly describes the recovery procedure to use when an alarm condition occurs.

As a reminder, layers are the following:

- Underlay: physical connection between devices (LAN, WAN), VRRP or HA state change, appliance configuration
- Overlay: connection between appliances or external gateways through IPsec tunnels
- Services: services provided with the appliances such as application visibility, application control, WAN optimization, firewall
- EQS: site EQS for applications and site connectivity
- Resources: device local resources, i.e. hardware monitoring
- Management: connection to Azure components (Orchestrator, ZTP Server, etc.)

Underlay

Alarm	Severiy	Troubleshooting
Network interface down [interface name]	Critical	Check physical connections with the device.
Bad network interface configuration [interface name]	Critical	Check the interface configuration parameters.
No IP address [Transport Network Identifier name]	Critical	Define a correct IP address for the configured WAN interface.
No default gateway [Transport Network Identifier name]	Critical	Define a default gateway for the configured WAN interface.
VRRP state change	Information	Status change alarm.
HA state change	Information	Status change alarm.
Configuration mismatch	Critical	There is a configuration version mismatch between the SD-WAN Orchestrator and the appliances. Contact ExtremeCloud SD-WAN Support.
HA Configuration mismatch	Critical	Check the information of the Event History window to identify the issue. Check the Routing section of the Troubleshooting window (by clicking

Alarm	Severiy	Troubleshooting
		the ♥ icon on the **Network -> Configuration** window) and verify the status of the HA appliances. Fix your HA configuration.
HA Peer unreachable	Critical	The HA connection may be broken due to an appliance reboot, an unplugged cable, a power failure or an incident on another client device (for example, port down on a switch). Contact ExtremeCloud SD-WAN Support.

Overlay

Alarm	Severiy	Troubleshooting
Disconnected from the overlay	Warning	The specified site is fully isolated from the rest of the network (zero overlay tunnel). Check your appliance configuration and define at least one IPsec tunnel.
Tunnel failure (appliance)	Critical	Refer to the Event History window to identify the issue. Check the Tunnels section of the Troubleshooting window (by clicking the ♥ icon on the **Network -> Configuration** window) and verify the state of the GRE/IPsec tunnels. Fix your appliance configuration.
External tunnel failure (External Gateway)	Critical	Check the configuration of the external gateway connection.
CloudMesh failure	Critical	Contact ExtremeCloud SD-WAN Support.
EdgeSentry failure	Critical	Contact ExtremeCloud SD-WAN Support.
LAN BGP peering failure	Warning	Check the Local Peer IP address in the LAN and the Site AS number.

Alarm	Severiy	Troubleshooting
Connection to AWS failure	Warning/Critical	May be raised when the connection is being created. If the issue persists, check that the corresponding AWS resources (Customer Gateway and VPN connection) still exist and contact ExtremeCloud SD-WAN Support.
Connection to Azure failure	Warning/Critical	May be raised when the connection is being created. If the issue persists, check that the corresponding Azure resources (local network gateway and vnet gateway connection or VPN sites and connections for Virtual WAN) still exist. Contact ExtremeCloud SD-WAN Support.
Cloud gateway failure	Critical	Check that the cloud gateway still exists and prerequisites are met.
Cloud account failure	Critical	Check the Cloud Access definition and contact your cloud account administrator.

Services

Alarm	Severiy	Troubleshooting
Visibility down	Warning	Contact ExtremeCloud SD-WAN Support.
Control down	Warning	Contact ExtremeCloud SD-WAN Support.
WAN Optimization down	Warning	Contact ExtremeCloud SD-WAN Support.
Synchronization lost	Warning	Contact ExtremeCloud SD-WAN Support.
DTI traffic overload	Warning	The number of DTI connections exceeds 95% of the maximum threshold of authorized connections. The alarm is cleared when this value decreases.
Connection to the SYSLOG server is lost	Warning	Check network connectivity between the SYSLOG server and the appliance.

EQS

Alarm	Severiy	Troubleshooting
Site EQS for Top Applications dropped below 5	Warning	The alarm is cleared when this value increases.
Site EQS for High Applications dropped below 5	Warning	The alarm is cleared when this value increases.
End-to-end connectivity lost	Warning	Check end-to-end connectivity between Site A and Site B for the specified Transport Network (broken NAP).

Resources

Alarm	Severiy	Troubleshooting
Disk is almost full (<5% left) on the volume [volume name]	Warning	For hardware resource alarms, contact ExtremeCloud SD-WAN Support.
Disk failure	Warning	
Reboot	Information	
Traffic overload	Warning	Throughput or the number of flows exceeds the capacity of the appliance, or packet loss occurs on Ethernet interfaces. Contact Extreme Networks Support. They will determine whether a more powerful appliance needs to be installed.

Management

Alarm	Severiy	Troubleshooting
Disconnected from Orchestrator	Critical	One or several SD-WAN platform components are disconnected (either never connected or not recently connected) from the Orchestrator. Contact ExtremeCloud SD-WAN Support.
Connectivity with Orchestrator impaired	Warning	One or several SD-WAN platform components are disconnected (either never connected or not recently

Alarm	Severiy	Troubleshooting
		connected) from ZTP (Zero Touch Provisioning server). Contact ExtremeCloud SD-WAN Support.

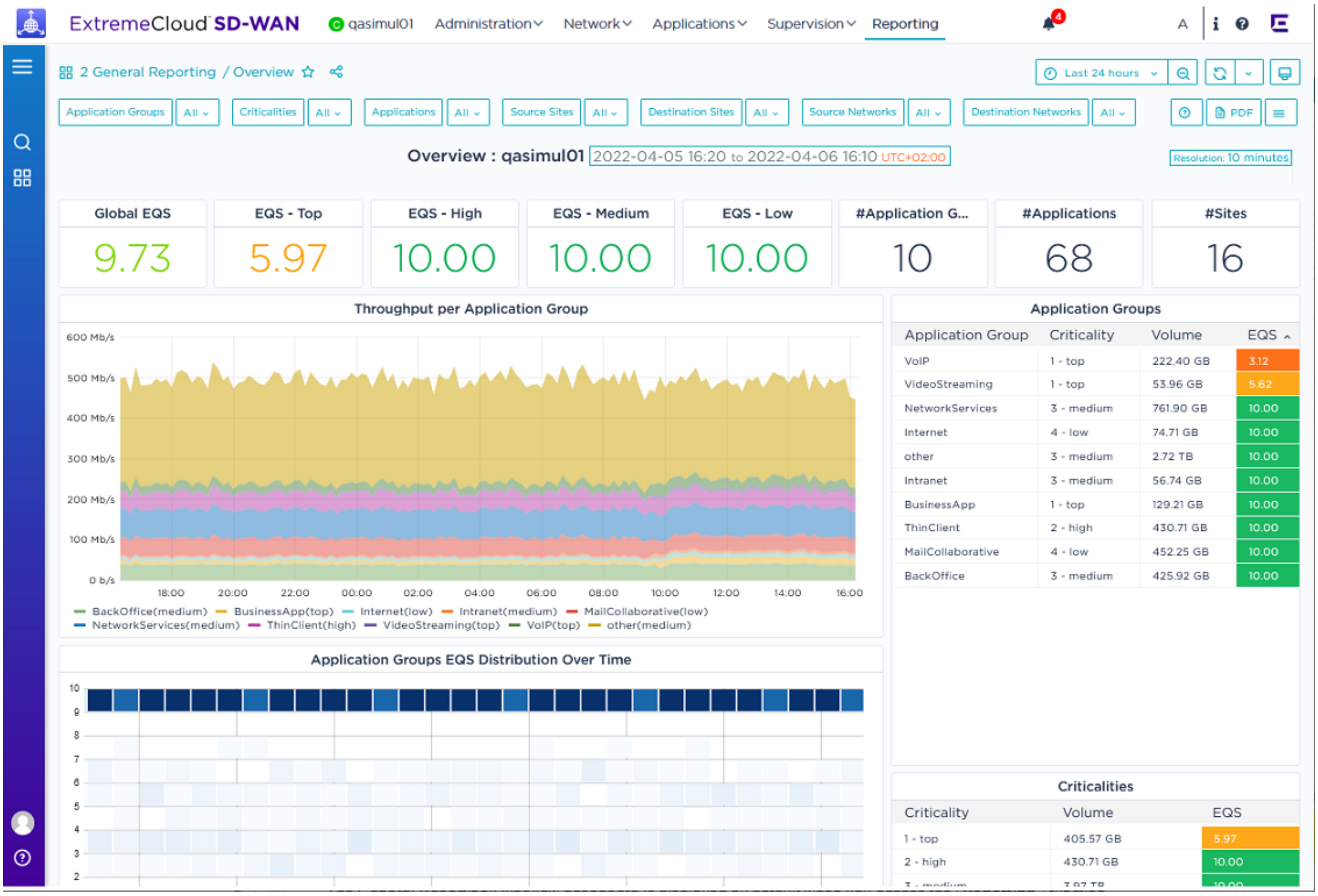
6 Reporting

This section mainly describes how you can navigate dashboards through a simple Use Case.

- "Accessing the Reporting Dashboards"
- "Predefined Dashboard Categories"
- "Navigating a Dashboard - Use Case"
- "The Reporting Toolbar"

Accessing the Reporting Dashboards

Select the **Reporting** function from the SD-WAN Orchestrator main menu to display the following dashboard:



Overview : qasimul01 2022-04-05 16:20 to 2022-04-06 16:10 UTC+02:00

Resolution: 10 minutes

Global EQS	EQS - Top	EQS - High	EQS - Medium	EQS - Low	#Application G...	#Applications	#Sites
9.73	5.97	10.00	10.00	10.00	10	68	16

Application Groups

Application Group	Criticality	Volume	EQS
VoIP	1 - top	222.40 GB	3.12
VideoStreaming	1 - top	53.96 GB	5.62
NetworkServices	3 - medium	761.90 GB	10.00
Internet	4 - low	74.71 GB	10.00
other	3 - medium	2.72 TB	10.00
Intranet	3 - medium	56.74 GB	10.00
BusinessApp	1 - top	129.21 GB	10.00
ThinClient	2 - high	430.71 GB	10.00
MailCollaborative	4 - low	452.25 GB	10.00
BackOffice	3 - medium	425.92 GB	10.00

Criticalities

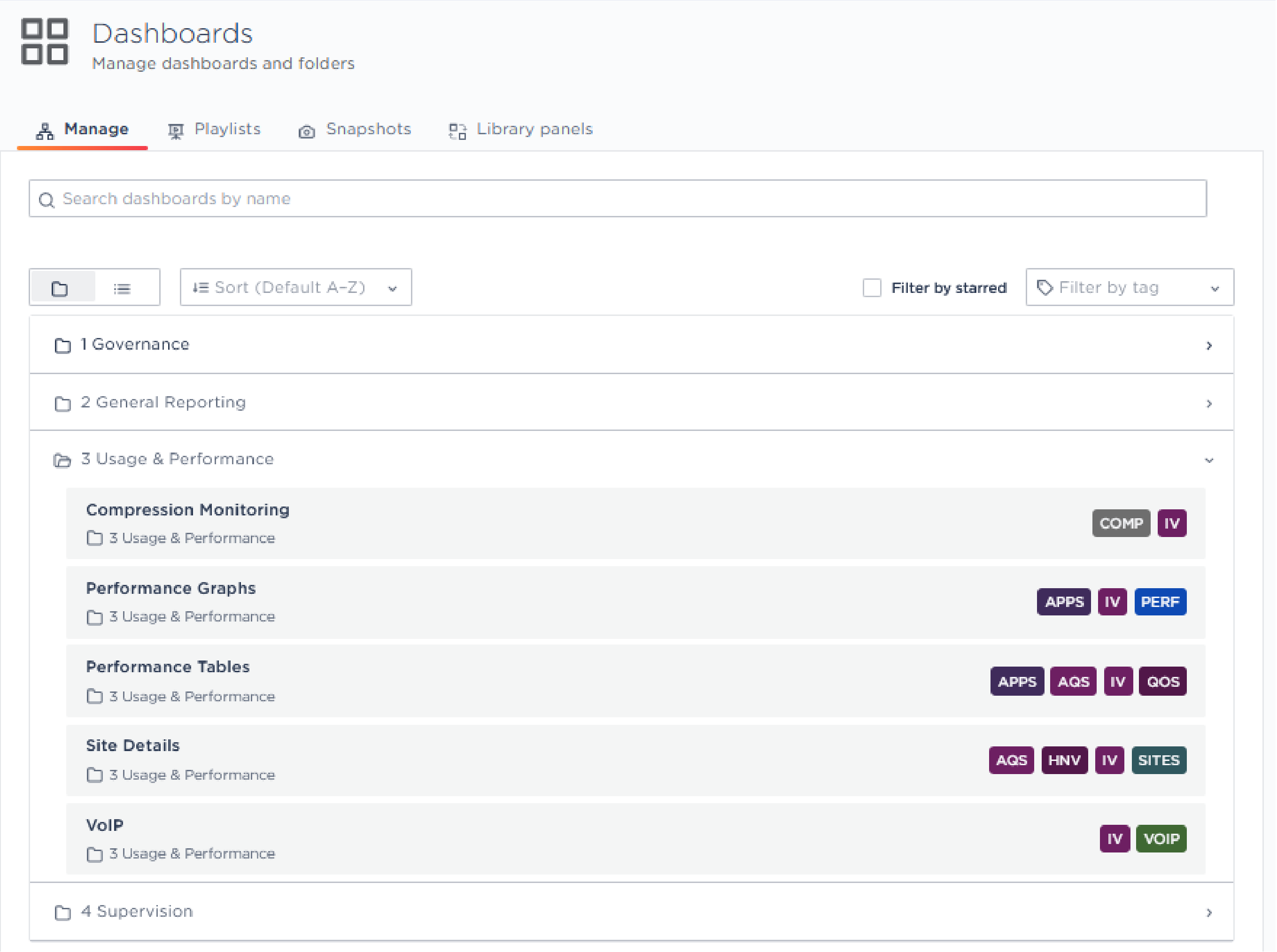
Criticality	Volume	EQS
1 - top	405.57 GB	5.97
2 - high	430.71 GB	10.00
3 - medium	3.97 TB	10.00

The General Reporting/Overview dashboard is displayed by default when you access the **Reporting** function.

Predefined Dashboard Categories

Viewing the list of predefined dashboard categories

In the Reporting toolbar at the left of the window, click the ⊞ icon and select the **Manage** function. The list of predefined dashboard categories is displayed.



Dashboards
Manage dashboards and folders

1 Governance

2 General Reporting

3 Usage & Performance

- Compression Monitoring — 3 Usage & Performance — COMP IV
- Performance Graphs — 3 Usage & Performance — APPS IV PERF
- Performance Tables — 3 Usage & Performance — APPS AQS IV QOS
- Site Details — 3 Usage & Performance — AQS HNV IV SITES
- VoIP — 3 Usage & Performance — IV VOIP

4 Supervision

- **1 Governance** dashboards provide information such as access congestion, application distribution, capacity planning and enable you to study the interaction between the SD-WAN Orchestrator and your network. These dashboards are designed for long-term decision-making by management.
- **2 General Reporting** dashboards provide an overview of your main applications and sites.
- **3 Usage and Performance** dashboards display low-level object indicators enabling troubleshooting.
- **4 Supervision** dashboards enable you to monitor the appliance infrastructure.

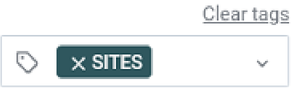
Displaying a dashboard

From the Dashboard List

Select the dashboard from the right category in the list.

You can also filter that list by

- using tags in order to limit your selection choice. For example, if you select the Sites filter, only the dashboards displaying Site information are listed,



- typing the name of the dashboard in the Search field at the very top of the window. Again, the list adjusts to your request.

Finally, click the appropriate dashboard name to display the dashboard.

From a specific dashboard

- Click the first element of the dashboard title to display the list of dashboards in the same category. For example, in 'General Reporting / Overview', click 'General Reporting'.
- Click the second element of the dashboard title, i.e. 'Overview' to display the list of dashboard categories.
- In any case, use 'Go to Folder' to navigate.

Meaning of some symbols and metrics

Here is a definition of the symbols and specific metrics that are used in the dashboards. For a definition of the standard metrics, such as EQS, Delay, Jitter, packet Loss, RTT, SRT, TCP retransmission, etc., refer to "Application Flows - Detailed flows list"

LAN=>WAN

LAN=>WAN represents the direction of the flow(s) in relation to the selected Site, i.e. coming from its LAN and going to its WAN (alias ingress or outbound or upload)

WAN=>LAN

WAN=>LAN represents the direction of the flow(s) in relation to the selected Site, i.e. coming from its WAN and going to its LAN (alias egress or inbound or download)

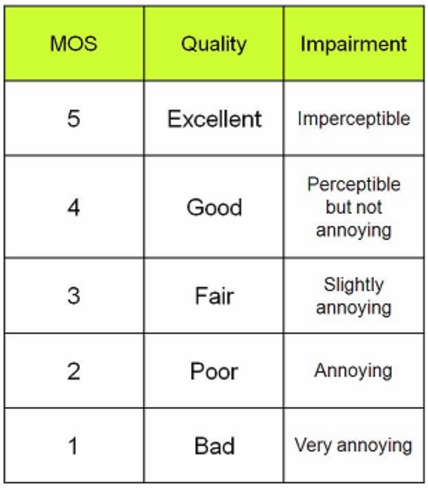
Session

A session is identified:

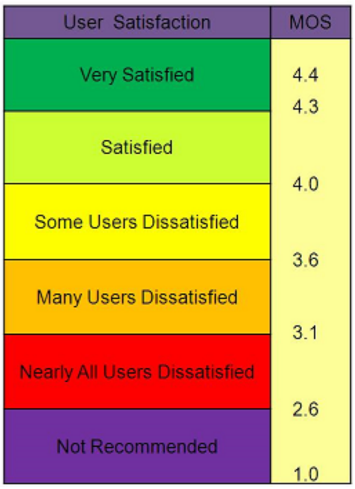
- For TCP or UDP by the following parameters: source IP address, destination IP address, protocol (TCP or UDP), source port and destination port.

- For other protocols over IP (for example: ICMP) by the following parameters: source IP address, destination IP address, protocol.

MOS (1 to 5)



MOS	Quality	Impairment
5	Excellent	Imperceptible
4	Good	Perceptible but not annoying
3	Fair	Slightly annoying
2	Poor	Annoying
1	Bad	Very annoying



User Satisfaction	MOS
Very Satisfied	4.4 4.3
Satisfied	4.0
Some Users Dissatisfied	3.6
Many Users Dissatisfied	3.1
Nearly All Users Dissatisfied	2.6
Not Recommended	1.0

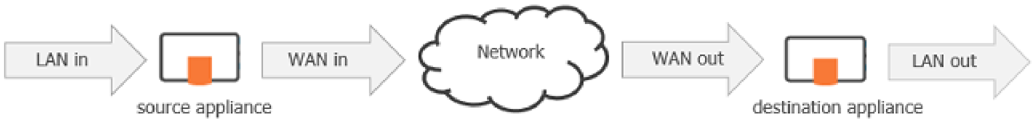
LAN and WAN Metrics

Reporting dashboards contain graphs and tables displaying both application and network information.

As a general rule,

- the metrics in graphs and tables related to applications are LAN metrics
- the metrics in graphs and tables related to networks are WAN metrics

For this reason, the volumes provided in the dashboards with both application and network data are calculated differently according to whether they are LAN side metrics or WAN side metrics.



LAN=>WAN direction for the source appliance

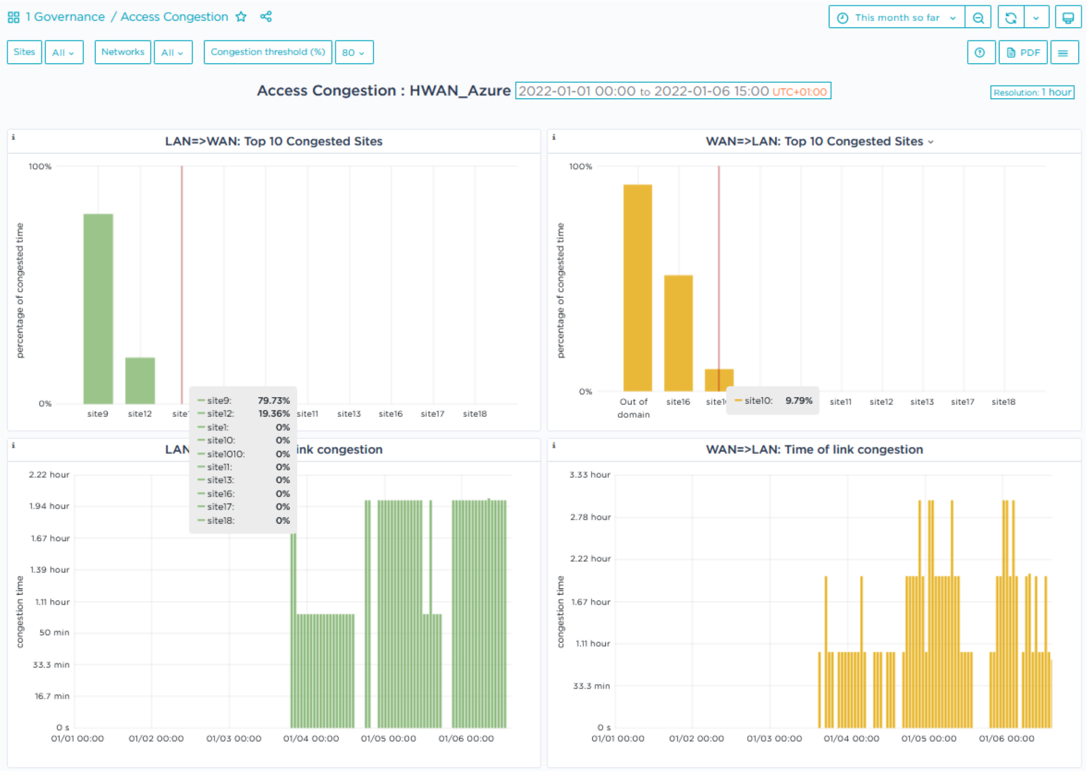
WAN=>LAN direction for the destination appliance

Governance Dashboards

Governance dashboards provide information such as access congestion, application distribution, capacity planning and enable you to study the interaction between the SD-WAN Orchestrator and your network. These dashboards are designed for **long-term decision-making by management**.

Also refer to "Navigating a Dashboard - Use Case"and "The Reporting Toolbar".

Access Congestion

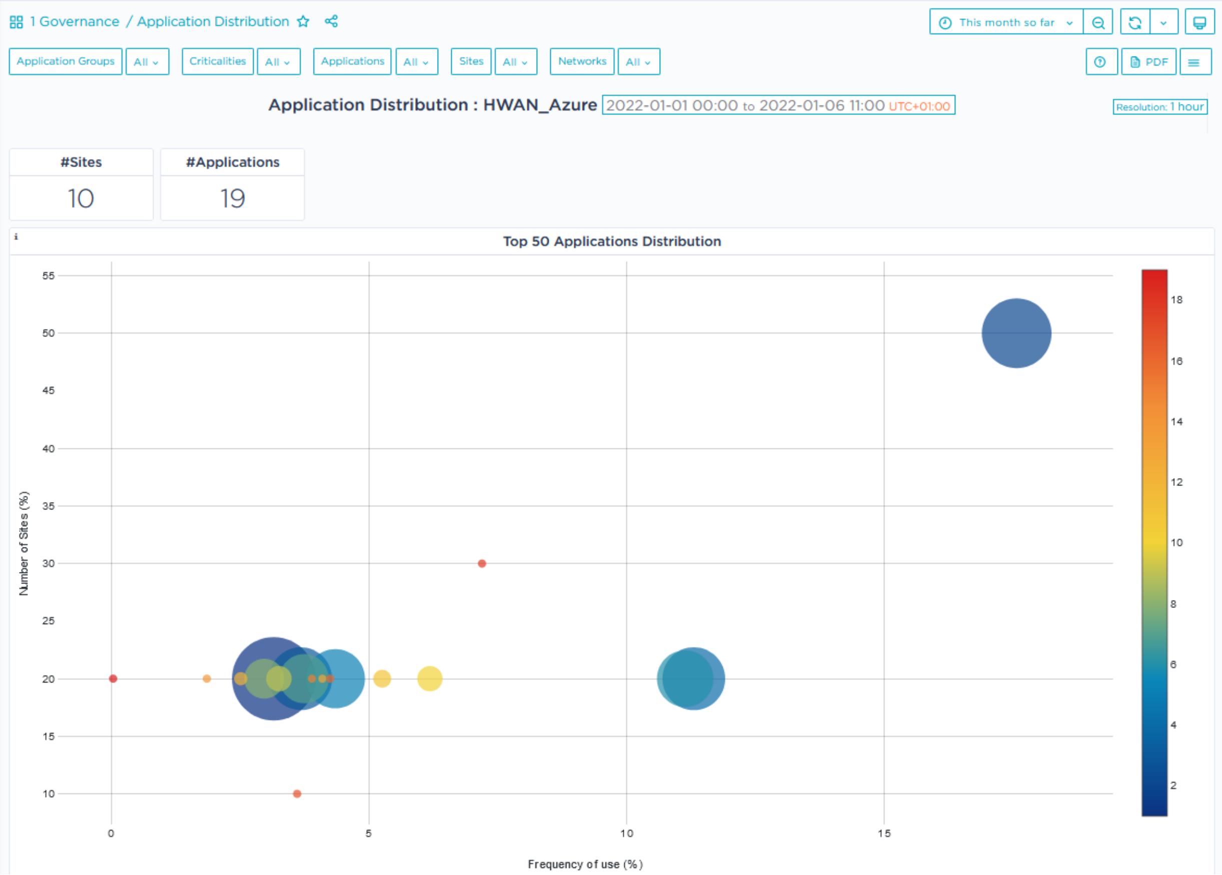


This dashboard enables you to anticipate network access required sizing by showing the congestion trend of network access during the last month (default time range of this dashboard).

This dashboard displays the percentage of congestion time for the top 10 congested sites in both the LAN=>WAN and WAN=>LAN directions. The second pane of the dashboard shows the total congestion time in milliseconds for each link in both directions, from the LAN to the WAN and from the WAN to the LAN.

You can filter dashboard display by site, network and congestion threshold in percentage: 80, 90 and 95 are the values by default. You can also type any other percentage.

Application Distribution



Application Distribution : HWAN_Azure 2022-01-01 00:00 to 2022-01-06 11:00 UTC+01:00

#Sites	#Applications
10	19

The scatter plot diagram of this dashboard showing Top 50 Application Distribution enables you to check how often and on how many sites an application is seen by the system during the last month (default time range of this dashboard).

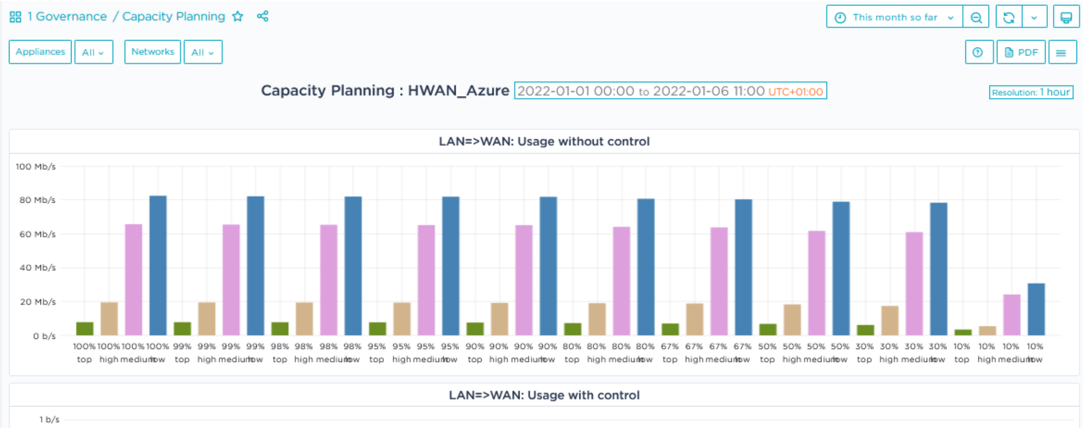
The Y axis represents the number of sites in percentage whereas the X axis corresponds to the frequency of use in percentage.

With respect to the right color bar, the size and color of each application circle varies according to volume and volume rank.

When you position your cursor over an application circle, the displayed popup window indicates the previous information, i.e.:

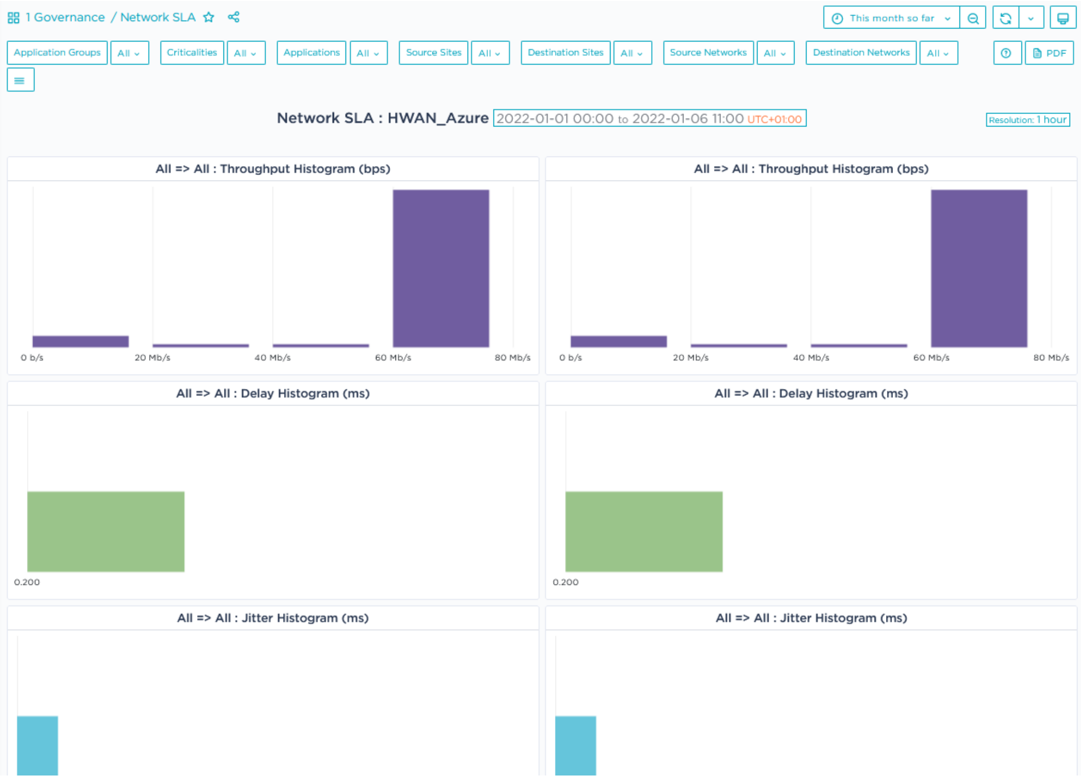
- application name
- usage frequency as the first value and the number of sites (in percentage) as the second value
- volume
- rank

Capacity Planning


1 Governance / Capacity Planning
This month so far
Appliances All
Networks All
PDF
Capacity Planning : HWAN_Azure 2022-01-01 00:00 to 2022-01-06 11:00 UTC+01:00
Resolution: 1 hour
LAN=>WAN: Usage without control
100 Mb/s
80 Mb/s
60 Mb/s
40 Mb/s
20 Mb/s
0 b/s
100% top 100% high 100% medium 100% low
99% top 99% high 99% medium 99% low
98% top 98% high 98% medium 98% low
95% top 95% high 95% medium 95% low
90% top 90% high 90% medium 90% low
80% top 80% high 80% medium 80% low
67% top 67% high 67% medium 67% low
50% top 50% high 50% medium 50% low
30% top 30% high 30% medium 30% low
10% top 10% high 10% medium 10% low
LAN=>WAN: Usage with control
1 b/s

This dashboard enables you to determine network access size based on the amount of protection you want for your applications. The default time range of this dashboard is the last month.

Network SLA


1 Governance / Network SLA
This month so far
Application Groups All
Criticalities All
Applications All
Source Sites All
Destination Sites All
Source Networks All
Destination Networks All
PDF
Network SLA : HWAN_Azure 2022-01-01 00:00 to 2022-01-06 11:00 UTC+01:00
Resolution: 1 hour
All => All : Throughput Histogram (bps)
0 b/s
20 Mb/s
40 Mb/s
60 Mb/s
80 Mb/s
All => All : Throughput Histogram (bps)
0 b/s
20 Mb/s
40 Mb/s
60 Mb/s
80 Mb/s
All => All : Delay Histogram (ms)
0.200
All => All : Delay Histogram (ms)
0.200
All => All : Jitter Histogram (ms)
All => All : Jitter Histogram (ms)

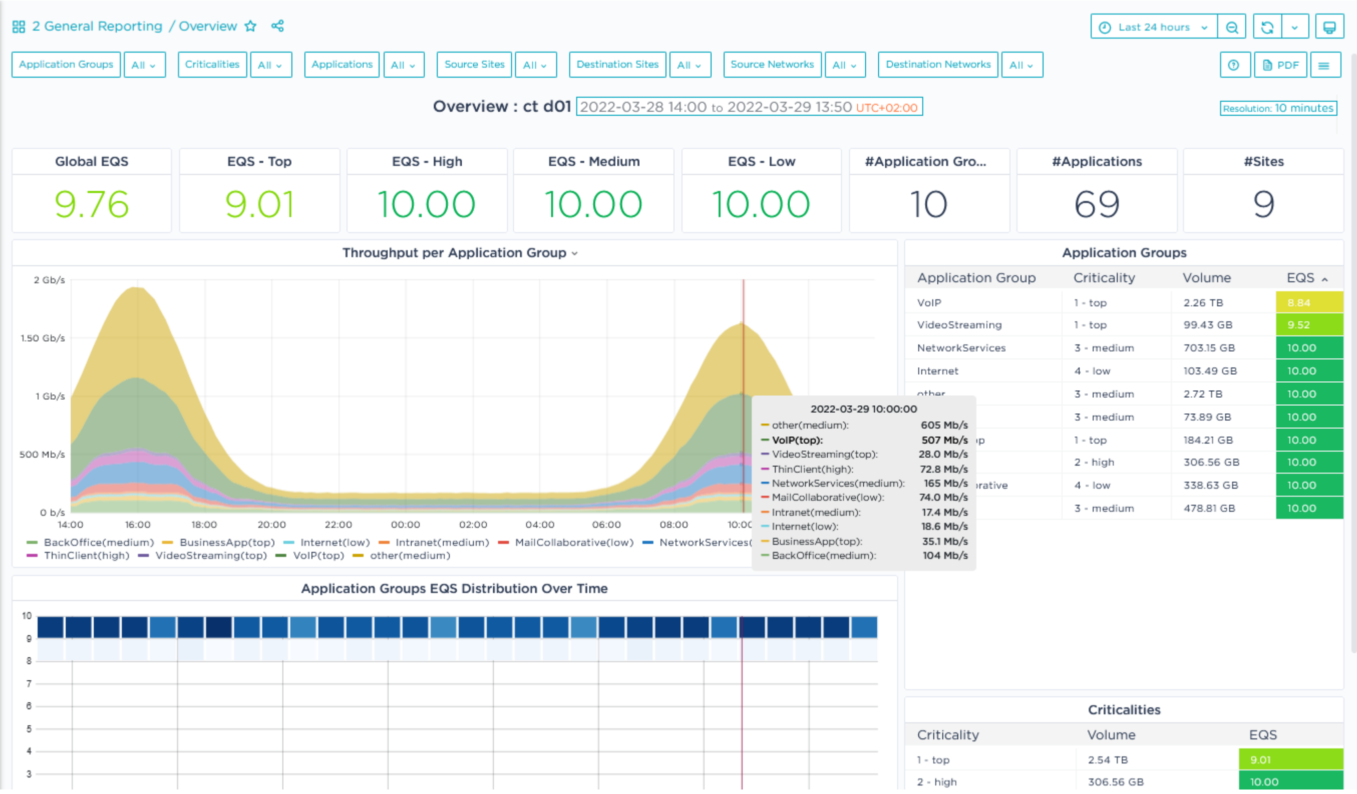
This dashboard enables you to follow up Service Level Agreement typical performance metrics of the network service provided by network providers. Histograms of throughput, delay, jitter, packet loss and link availability are displayed. The default time range of this dashboard is the last month.

General Reporting Dashboards

General Reporting dashboards provide an **overview** of your main applications and sites. The default time range of these dashboards corresponds to the last 24 hours.

Also refer to "Navigating a Dashboard - Use Case"and "The Reporting Toolbar".

Overview



Overview : ct d01 2022-03-28 14:00 to 2022-03-29 13:50 UTC+02:00

Resolution: 10 minutes

Global EQS	EQS - Top	EQS - High	EQS - Medium	EQS - Low	#Application Gro...	#Applications	#Sites
9.76	9.01	10.00	10.00	10.00	10	69	9

2022-03-29 10:00:00

other(medium):	605 Mb/s
VoIP(top):	**507 Mb/s**
VideoStreaming(top):	28.0 Mb/s
ThinClient(high):	72.8 Mb/s
NetworkServices(medium):	165 Mb/s
MailCollaborative(low):	74.0 Mb/s
Intranet(medium):	17.4 Mb/s
Internet(low):	18.6 Mb/s
BusinessApp(top):	35.1 Mb/s
BackOffice(medium):	104 Mb/s

Application Groups

Application Group	Criticality	Volume	EQS ⌃
VoIP	1 - top	2.26 TB	8.84
VideoStreaming	1 - top	99.43 GB	9.52
NetworkServices	3 - medium	703.15 GB	10.00
Internet	4 - low	103.49 GB	10.00
other	3 - medium	2.72 TB	10.00
	3 - medium	73.89 GB	10.00
p	1 - top	184.21 GB	10.00
	2 - high	306.56 GB	10.00
rative	4 - low	338.63 GB	10.00
	3 - medium	478.81 GB	10.00

Criticalities

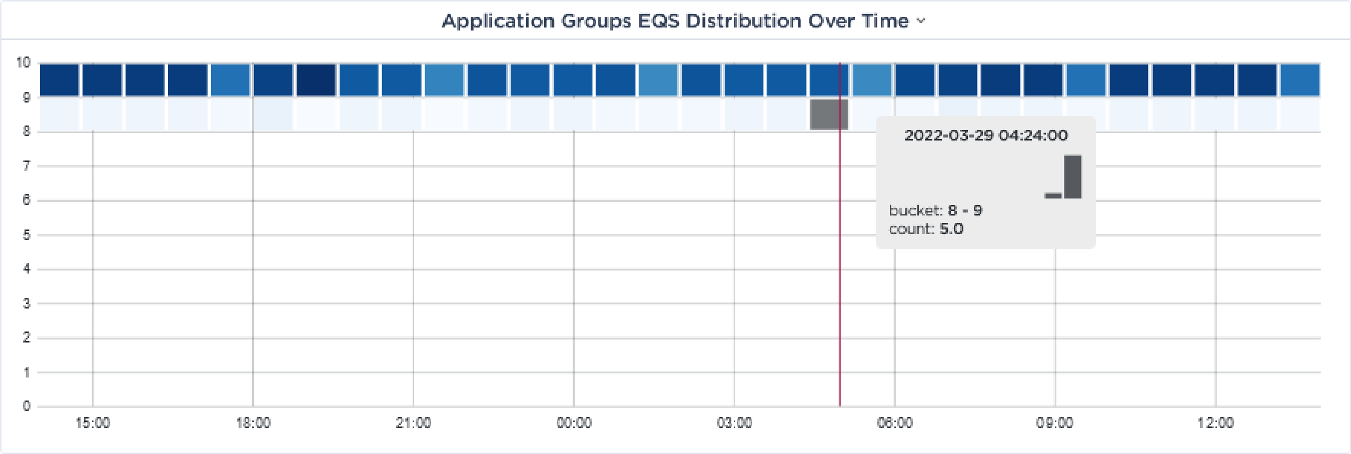
Criticality	Volume	EQS
1 - top	2.54 TB	9.01
2 - high	306.56 GB	10.00

The General Reporting/Overview dashboard is displayed by default when you access the Reporting function. This dashboard is an overview of EQS (see "Application Flows - Detailed flows list"), Volume and Throughput per Application/Application Group/Site/Network during the last 24 hours (default time range of this dashboard).

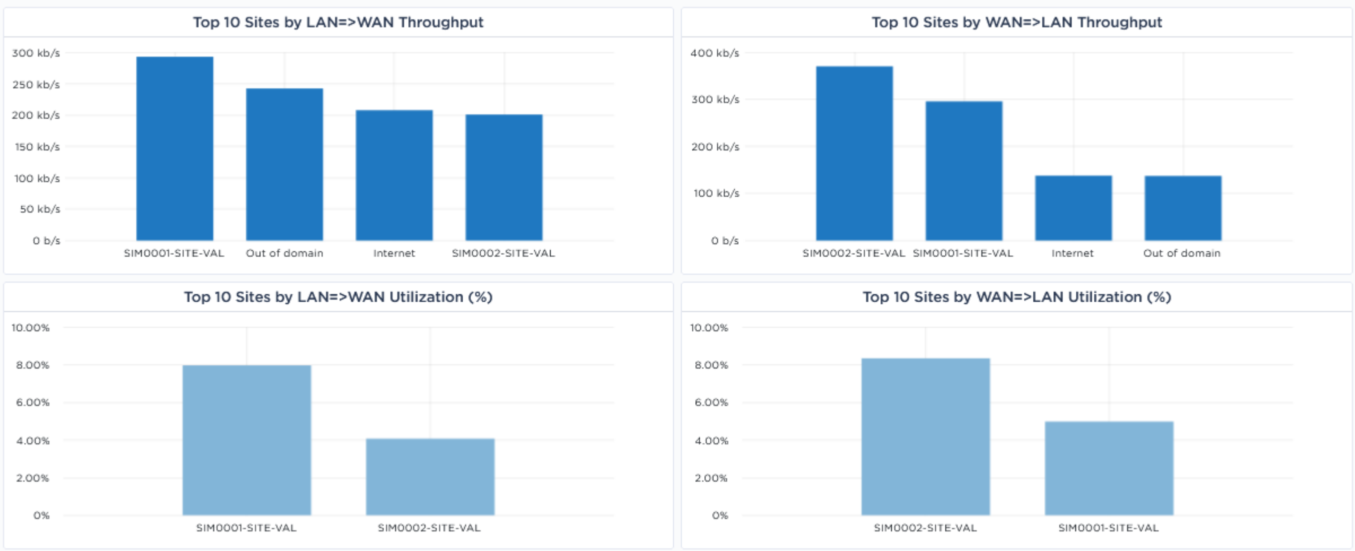
The **Application Group EQS Distribution Over Time** graph is a Heat Map chart showing the EQS distribution of the selected applications. The darker the cells, the more occurrences of this EQS are found by the system. The Y axis represents EQS whereas the X axis corresponds to application usage time intervals.

When you position your cursor over an historical series of cells, the displayed popup window indicates the number of applications matching the EQS which corresponds to the shown interval (bucket). EQS intervals are calculated by the SD-WAN Orchestrator.

The bar chart presentation shows EQS distribution for the column of cells.

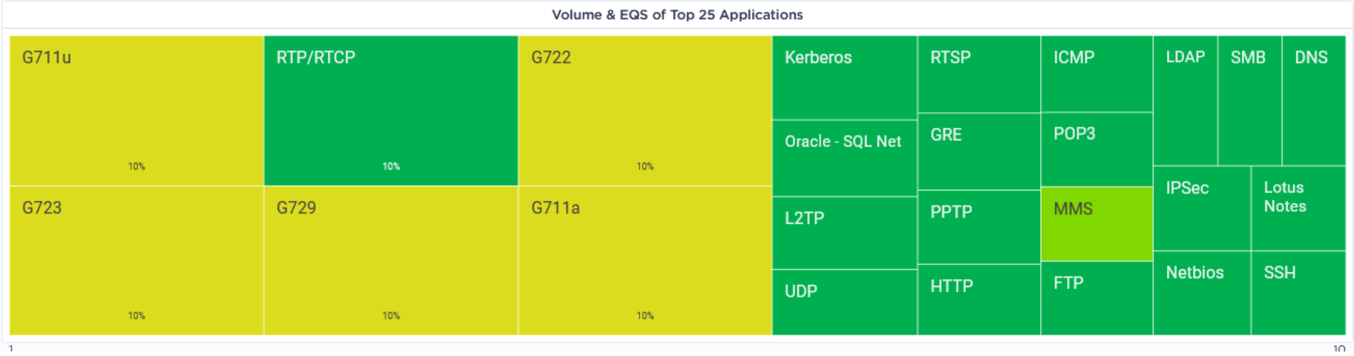


The **Top 10 Sites by LAN=>WAN and WAN=>LAN Throughput/Utilization** bar chart graphs display the throughput and utilization in percentage from the LAN to the WAN and from the WAN to the LAN of the top 10 sites.

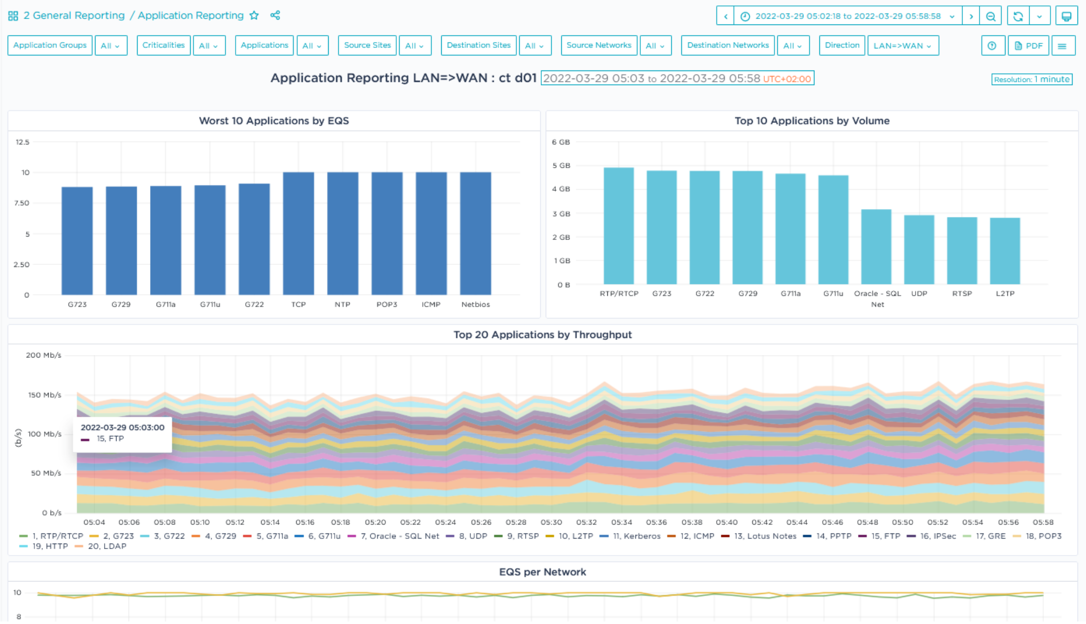


The **Volume & EQS of top 25 Applications** graph is a Tree Map chart where the size of cells decreases from the top left corner of the set of nested cells (biggest cells) to the bottom right corner where the smallest cells are located.

The volume and EQS of each application determines its location in the chart.

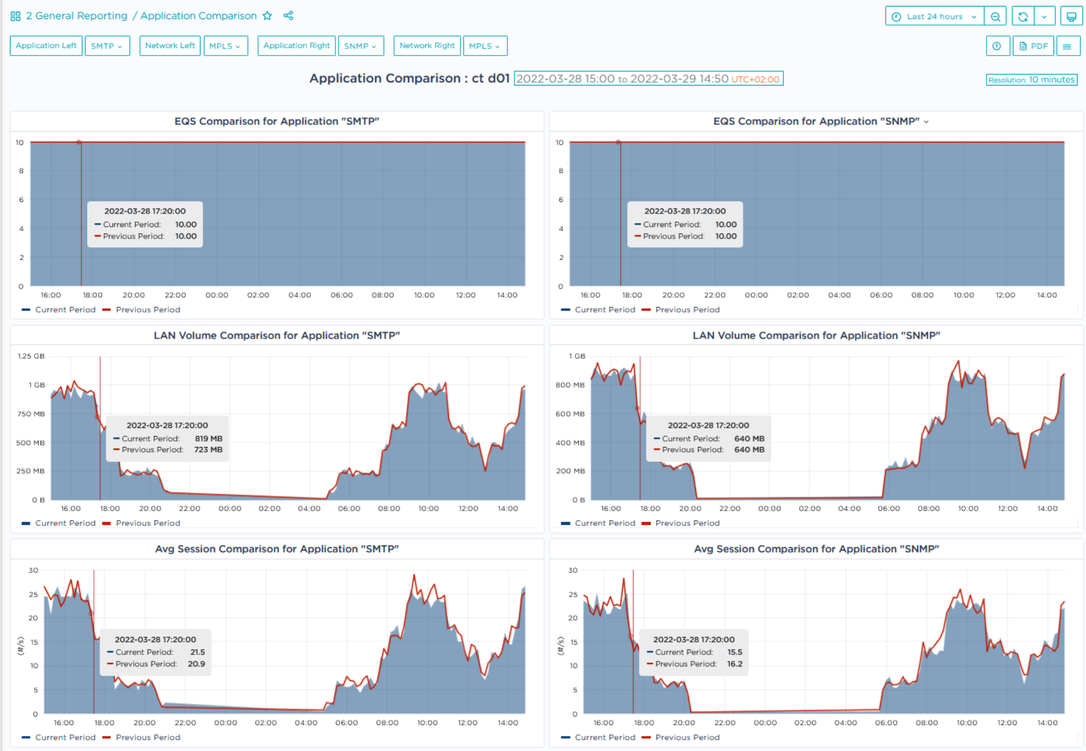


Application Reporting



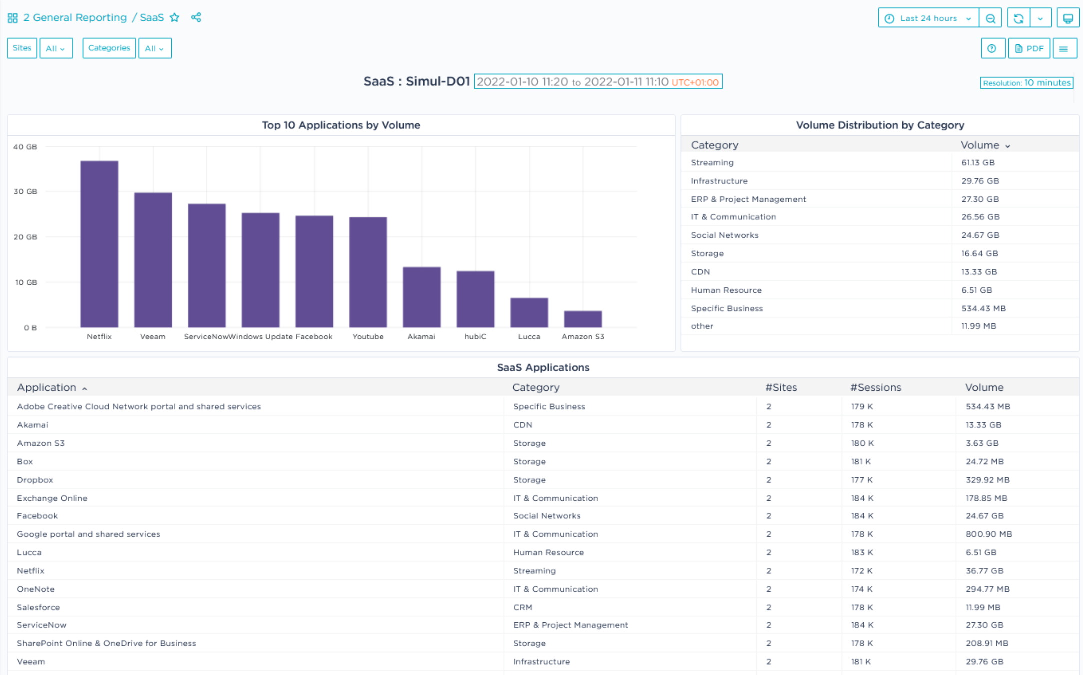
This dashboard enables you to display the top 10 applications with the worst EQS and the top 10 applications with the biggest volume. Other evolution graphs show throughput of the top 20 applications in LAN=>WAN and WAN=>LAN directions (LAN side metrics), EQS, throughput and number of sessions per network (WAN side metrics) during the last 24 hours (default time range of this dashboard).

Application Comparison



This dashboard is useful for comparing the same application on two different networks or during two different periods. You can also compare two applications on the same network (previous example). The default time range of this dashboard corresponds to the last 24 hours.

SaaS



SaaS : Simul-D01 2022-01-10 11:20 to 2022-01-11 11:10 UTC+01:00

Resolution: 10 minutes

Volume Distribution by Category

Category	Volume
Streaming	61.13 GB
Infrastructure	29.76 GB
ERP & Project Management	27.30 GB
IT & Communication	26.56 GB
Social Networks	24.67 GB
Storage	16.64 GB
CDN	13.33 GB
Human Resource	6.51 GB
Specific Business	534.43 MB
other	11.99 MB

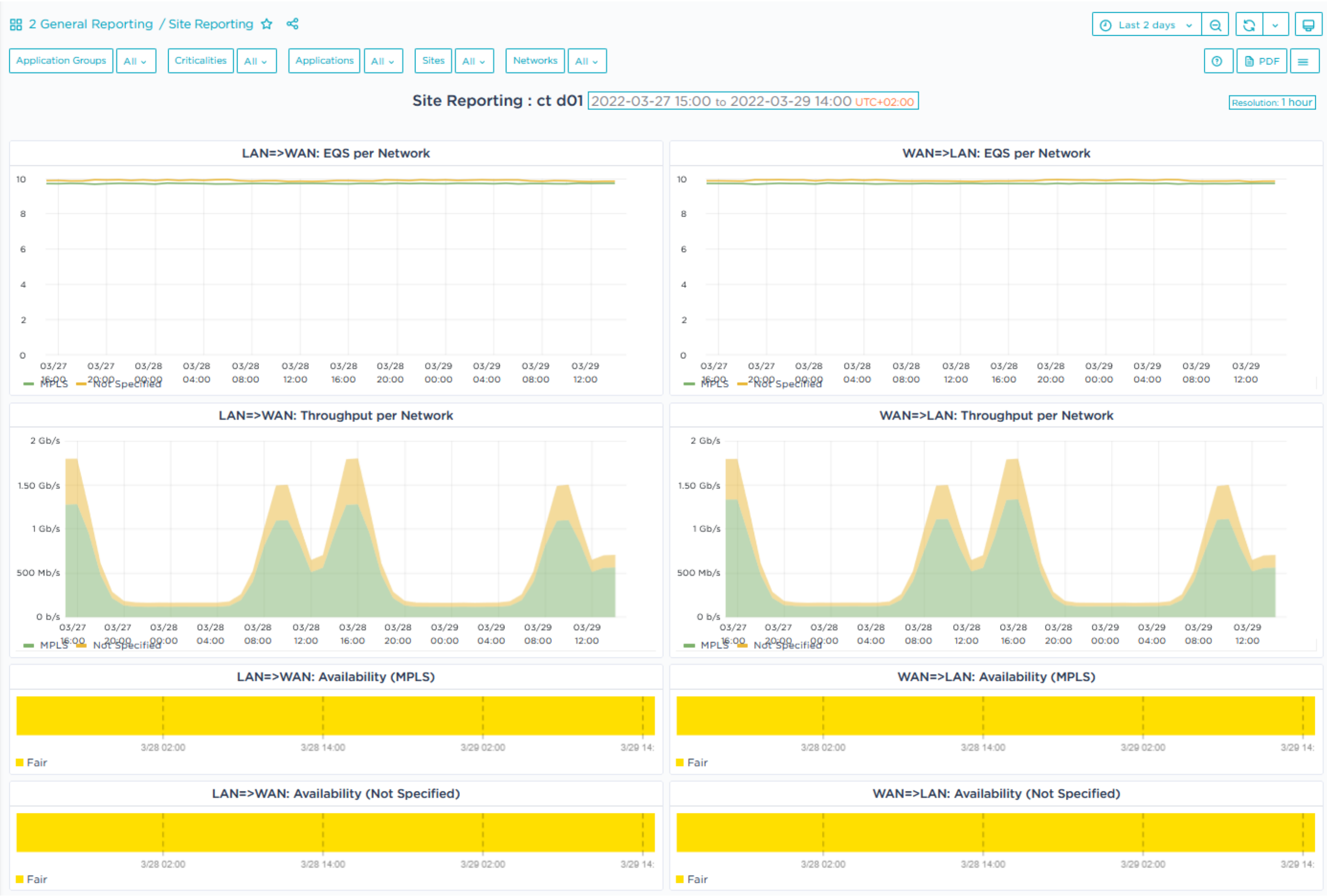
SaaS Applications

Application	Category	#Sites	#Sessions	Volume
Adobe Creative Cloud Network portal and shared services	Specific Business	2	179 K	534.43 MB
Akamai	CDN	2	178 K	13.33 GB
Amazon S3	Storage	2	180 K	3.63 GB
Box	Storage	2	181 K	24.72 MB
Dropbox	Storage	2	177 K	329.92 MB
Exchange Online	IT & Communication	2	184 K	178.85 MB
Facebook	Social Networks	2	184 K	24.67 GB
Google portal and shared services	IT & Communication	2	178 K	800.90 MB
Lucca	Human Resource	2	183 K	6.51 GB
Netflix	Streaming	2	172 K	36.77 GB
OneNote	IT & Communication	2	174 K	294.77 MB
Salesforce	CRM	2	178 K	11.99 MB
ServiceNow	ERP & Project Management	2	184 K	27.30 GB
SharePoint Online & OneDrive for Business	Storage	2	178 K	208.91 MB
Veeam	Infrastructure	2	181 K	29.76 GB

This dashboard enables you to track Shadow IT by displaying the SaaS Applications detected during the selected time range. You may filter these applications by Site and by SaaS Application category.

Site Reporting

This dashboard provides a general view of Sites. It gives throughput, quality and connectivity information in both directions for the selected Sites during the selected time range (the last 24 hours by default).



2 General Reporting / Site Reporting
Last 2 days
Application Groups
All
Criticalities
All
Applications
All
Sites
All
Networks
All
PDF
Site Reporting : ct d01 2022-03-27 15:00 to 2022-03-29 14:00 UTC+02:00
Resolution: 1 hour
LAN=>WAN: EQS per Network
WAN=>LAN: EQS per Network
10
8
6
4
2
0
03/27 16:00
03/27 20:00
03/28 00:00
03/28 04:00
03/28 08:00
03/28 12:00
03/28 16:00
03/28 20:00
03/29 00:00
03/29 04:00
03/29 08:00
03/29 12:00
MPLS
Not Specified
LAN=>WAN: Throughput per Network
WAN=>LAN: Throughput per Network
2 Gb/s
1.50 Gb/s
1 Gb/s
500 Mb/s
0 b/s
LAN=>WAN: Availability (MPLS)
WAN=>LAN: Availability (MPLS)
LAN=>WAN: Availability (Not Specified)
WAN=>LAN: Availability (Not Specified)
3/28 02:00
3/28 14:00
3/29 02:00
3/29 14:
Fair

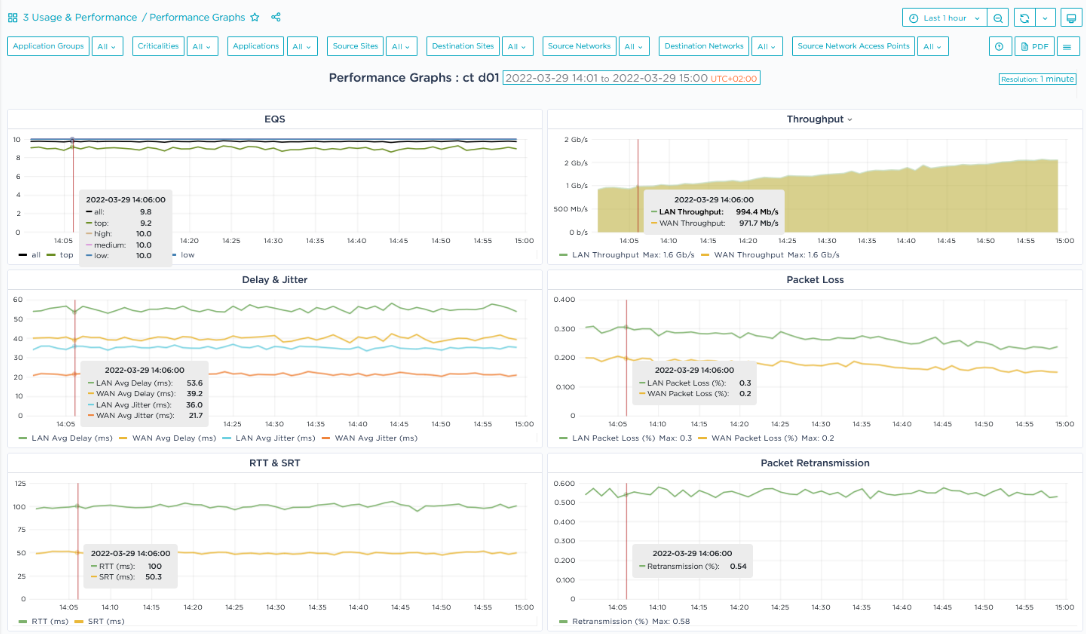
The lower part of the dashboard displays availability scores per Site in both directions.

Usage & Performance Dashboards

Usage & Performance dashboards display low-level object indicators enabling **troubleshooting**. The default time range of this dashboard is the last hour.

Also refer to "Navigating a Dashboard - Use Case"and "The Reporting Toolbar".

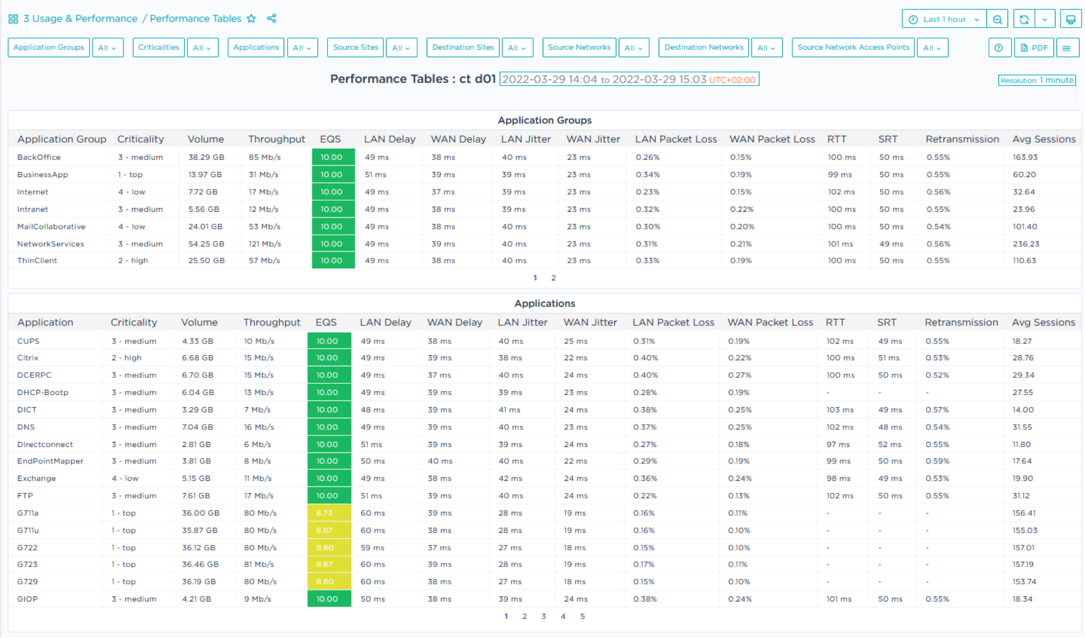
Performance Graphs



The graphs of this dashboard display low-level metrics such as EQS, Throughput, Delay and Jitter, Packet Loss, RTT and SRT, Packet Retransmission and Number of Sessions per application during the selected time range.

For a definition of these metrics, refer to "Application Flows - Detailed flows list"

Performance Tables



Performance Tables : ct d01 2022-03-29 14:04 to 2022-03-29 15:03 UTC+02:00

Application Groups

Application Group	Criticality	Volume	Throughput	EQS	LAN Delay	WAN Delay	LAN Jitter	WAN Jitter	LAN Packet Loss	WAN Packet Loss	RTT	SRT	Retransmission	Avg Sessions
BackOffice	3 - medium	38.29 GB	85 Mb/s	10.00	49 ms	38 ms	40 ms	23 ms	0.26%	0.15%	100 ms	50 ms	0.55%	163.93
BusinessApp	1 - top	13.97 GB	31 Mb/s	10.00	51 ms	39 ms	39 ms	23 ms	0.34%	0.19%	99 ms	50 ms	0.55%	60.20
Internet	4 - low	7.72 GB	17 Mb/s	10.00	49 ms	37 ms	39 ms	23 ms	0.23%	0.15%	102 ms	50 ms	0.56%	32.64
Intranet	3 - medium	5.56 GB	12 Mb/s	10.00	49 ms	38 ms	39 ms	23 ms	0.32%	0.22%	100 ms	50 ms	0.55%	23.96
MailCollaborative	4 - low	24.01 GB	53 Mb/s	10.00	49 ms	38 ms	40 ms	23 ms	0.30%	0.20%	100 ms	50 ms	0.54%	101.40
NetworkServices	3 - medium	54.25 GB	121 Mb/s	10.00	49 ms	39 ms	40 ms	23 ms	0.31%	0.21%	101 ms	49 ms	0.56%	236.23
ThinClient	2 - high	25.50 GB	57 Mb/s	10.00	49 ms	38 ms	40 ms	23 ms	0.33%	0.19%	100 ms	50 ms	0.55%	110.63

1 2

Applications

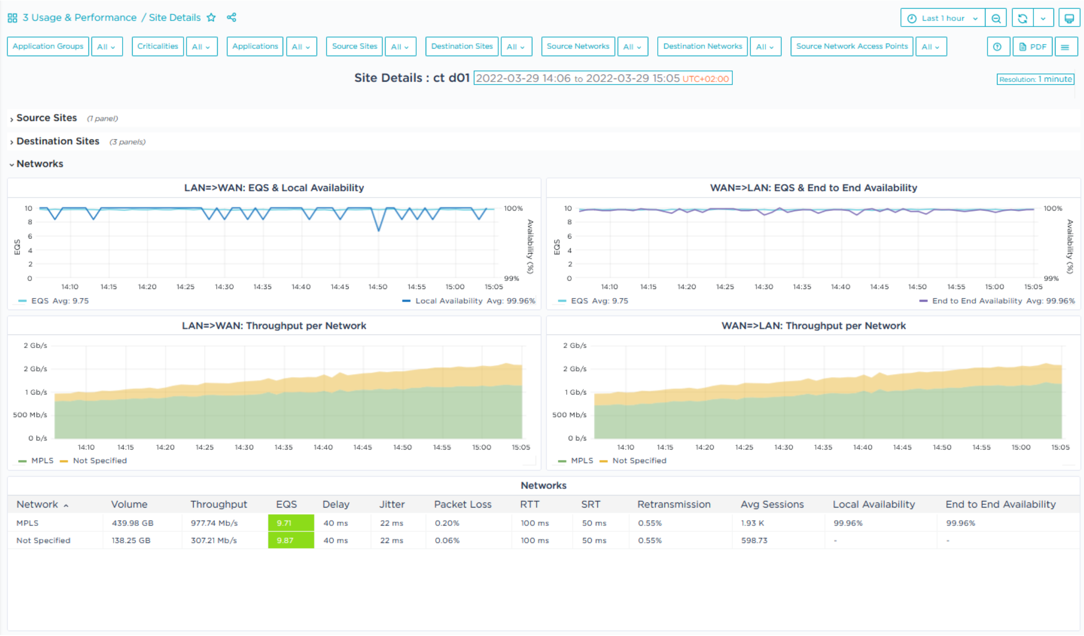
Application	Criticality	Volume	Throughput	EQS	LAN Delay	WAN Delay	LAN Jitter	WAN Jitter	LAN Packet Loss	WAN Packet Loss	RTT	SRT	Retransmission	Avg Sessions
CUPS	3 - medium	4.33 GB	10 Mb/s	10.00	49 ms	38 ms	40 ms	25 ms	0.31%	0.19%	102 ms	49 ms	0.55%	18.27
Citrix	2 - high	6.68 GB	15 Mb/s	10.00	49 ms	39 ms	38 ms	22 ms	0.40%	0.22%	100 ms	51 ms	0.53%	28.76
DCERPC	3 - medium	6.70 GB	15 Mb/s	10.00	49 ms	37 ms	40 ms	24 ms	0.40%	0.27%	100 ms	50 ms	0.52%	29.34
DHCP-Bootp	3 - medium	6.04 GB	13 Mb/s	10.00	49 ms	39 ms	39 ms	23 ms	0.28%	0.19%	-	-	-	27.55
DICT	3 - medium	3.29 GB	7 Mb/s	10.00	48 ms	39 ms	41 ms	24 ms	0.38%	0.25%	103 ms	49 ms	0.57%	14.00
DNS	3 - medium	7.04 GB	16 Mb/s	10.00	49 ms	39 ms	40 ms	23 ms	0.37%	0.25%	102 ms	48 ms	0.54%	31.55
Directconnect	3 - medium	2.81 GB	6 Mb/s	10.00	51 ms	39 ms	39 ms	24 ms	0.27%	0.18%	97 ms	52 ms	0.55%	11.80
EndPointMapper	3 - medium	3.81 GB	8 Mb/s	10.00	50 ms	40 ms	40 ms	22 ms	0.29%	0.19%	99 ms	50 ms	0.59%	17.64
Exchange	4 - low	5.15 GB	11 Mb/s	10.00	49 ms	38 ms	42 ms	24 ms	0.36%	0.24%	98 ms	49 ms	0.53%	19.90
FTP	3 - medium	7.61 GB	17 Mb/s	10.00	51 ms	39 ms	40 ms	24 ms	0.22%	0.13%	102 ms	50 ms	0.55%	31.12
G711a	1 - top	36.00 GB	80 Mb/s	8.73	60 ms	39 ms	28 ms	19 ms	0.16%	0.11%	-	-	-	156.41
G711u	1 - top	35.87 GB	80 Mb/s	8.87	60 ms	38 ms	28 ms	19 ms	0.16%	0.10%	-	-	-	155.03
G722	1 - top	36.12 GB	80 Mb/s	8.80	59 ms	37 ms	27 ms	18 ms	0.15%	0.10%	-	-	-	157.01
G723	1 - top	36.46 GB	81 Mb/s	8.87	60 ms	39 ms	28 ms	19 ms	0.17%	0.11%	-	-	-	157.19
G729	1 - top	36.19 GB	80 Mb/s	8.80	60 ms	38 ms	27 ms	18 ms	0.15%	0.10%	-	-	-	153.74
GIOP	3 - medium	4.21 GB	9 Mb/s	10.00	50 ms	38 ms	39 ms	24 ms	0.38%	0.24%	101 ms	50 ms	0.55%	18.34

1 2 3 4 5

The tables of this dashboard display low-level metrics such as EQS, Throughput, Delay and Jitter, Packet Loss, RTT and SRT, Packet Retransmission and Number of Sessions per application during the selected time range.

For a definition of these metrics, refer to "Application Flows - Detailed flows list"

Site Details



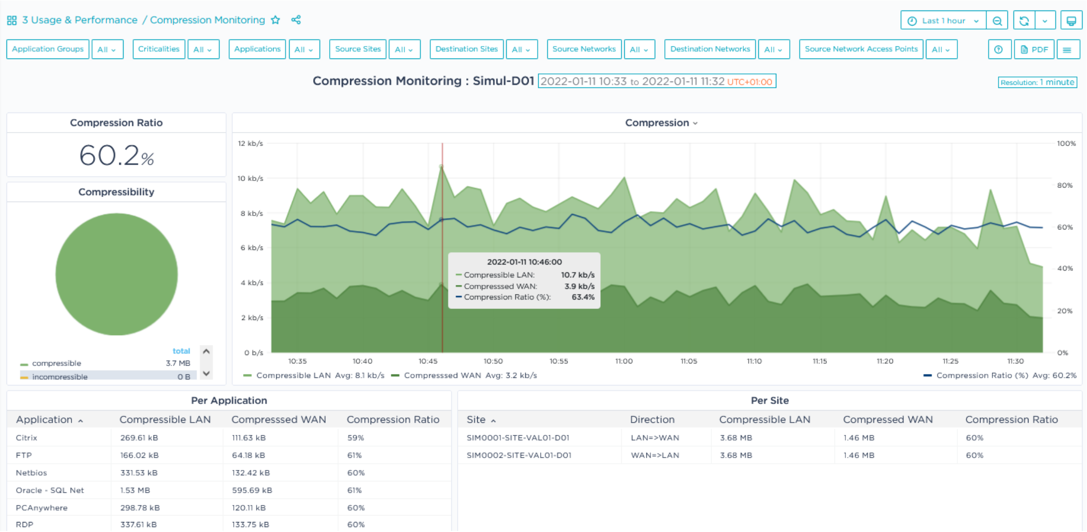
Site Details : ct d01 2022-03-29 14:06 to 2022-03-29 15:05 UTC+02:00

Networks

Network	Volume	Throughput	EQS	Delay	Jitter	Packet Loss	RTT	SRT	Retransmission	Avg Sessions	Local Availability	End to End Availability
MPLS	439.98 GB	977.74 Mb/s	9.71	40 ms	22 ms	0.20%	100 ms	50 ms	0.55%	1.93 K	99.96%	99.96%
Not Specified	138.25 GB	307.21 Mb/s	9.87	40 ms	22 ms	0.06%	100 ms	50 ms	0.55%	598.73	-	-

This dashboard contains all the detailed metrics you need to troubleshoot any issues occurring on your Sites.

Compression Monitoring



Compression Monitoring : Simul-D01 2022-01-11 10:33 to 2022-01-11 11:32 UTC+01:00

Compression Ratio

60.2%

Per Application

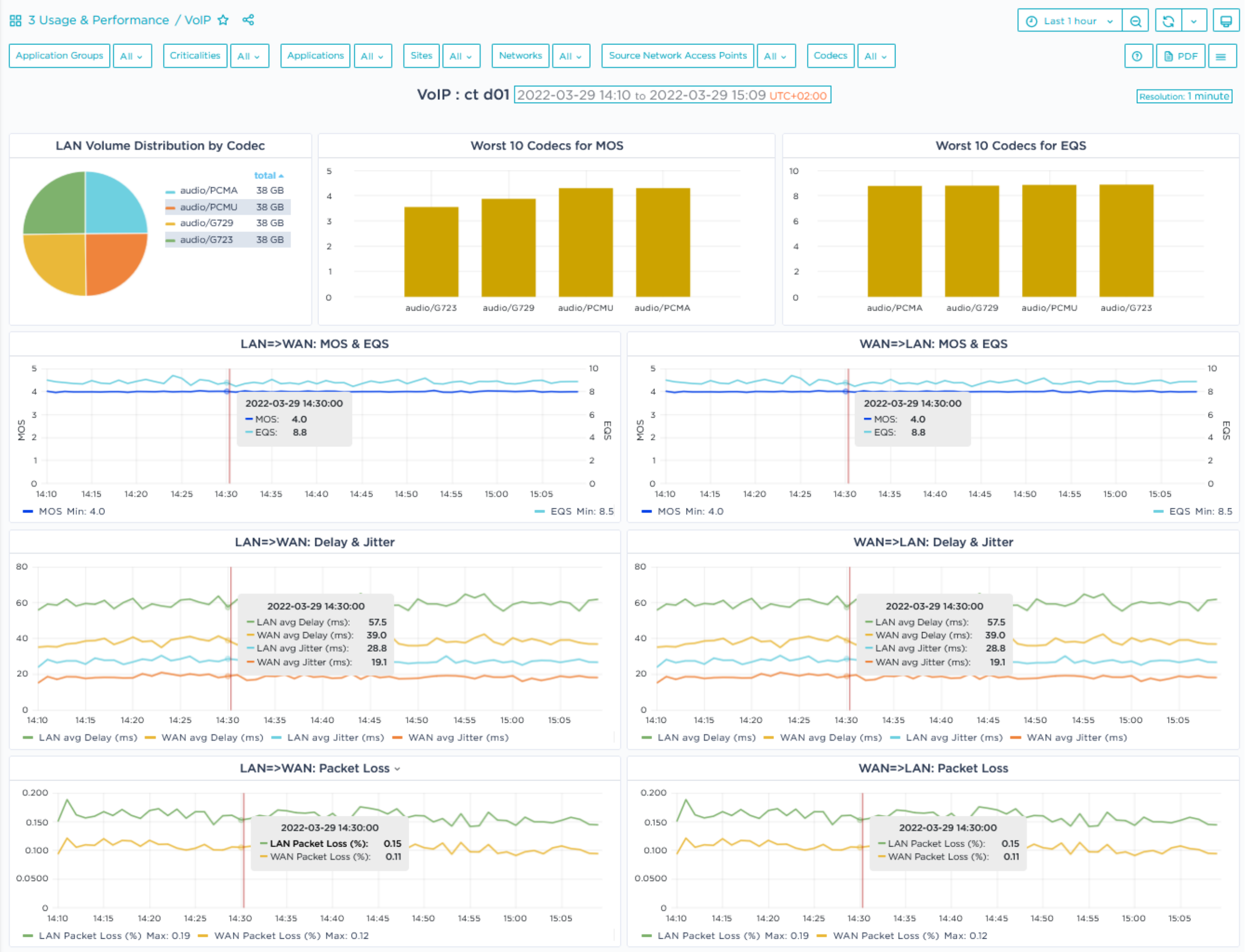
Application	Compressible LAN	Compresssed WAN	Compression Ratio
Citrix	269.61 kB	111.63 kB	59%
FTP	166.02 kB	64.18 kB	61%
Netbios	331.53 kB	132.42 kB	60%
Oracle - SQL Net	1.53 MB	595.69 kB	61%
PCAnywhere	298.78 kB	120.11 kB	60%
RDP	337.61 kB	133.75 kB	60%

Per Site

Site	Direction	Compressible LAN	Compressed WAN	Compression Ratio
SIM0001-SITE-VAL01-D01	LAN=>WAN	3.68 MB	1.46 MB	60%
SIM0002-SITE-VAL01-D01	WAN=>LAN	3.68 MB	1.46 MB	60%

This dashboard enables you to track and adjust application compression by providing you with relevant measurements of the compression ratios.

VoIP



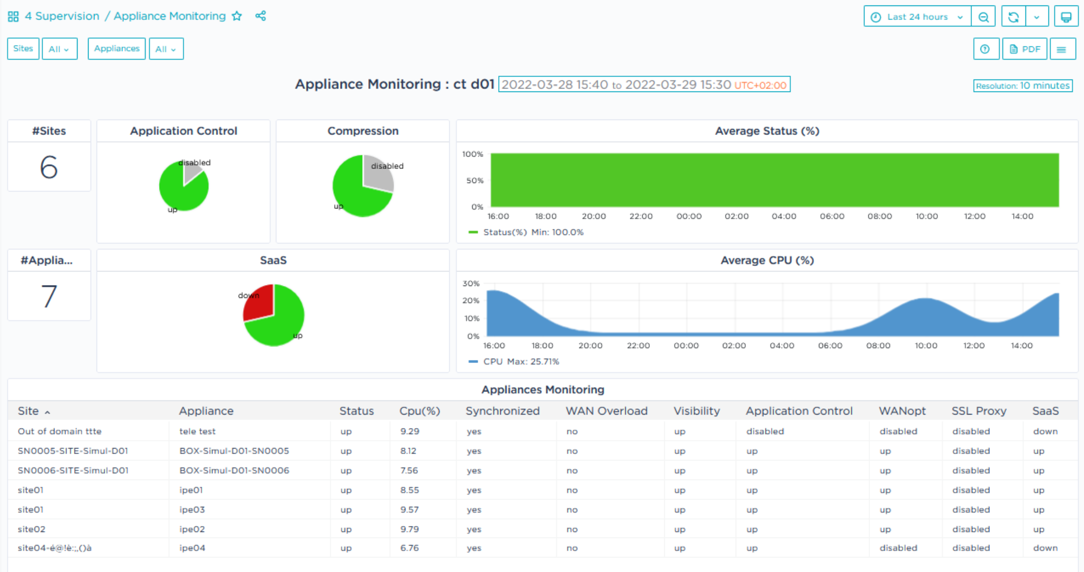
This dashboard is dedicated to VoIP quality monitoring.

Supervision Dashboards

Supervision dashboards enable you to monitor the **appliance infrastructure**. The default time range of these dashboards corresponds to the last 24 hours.

Also refer to "Navigating a Dashboard - Use Case"and "The Reporting Toolbar".

Appliance Monitoring



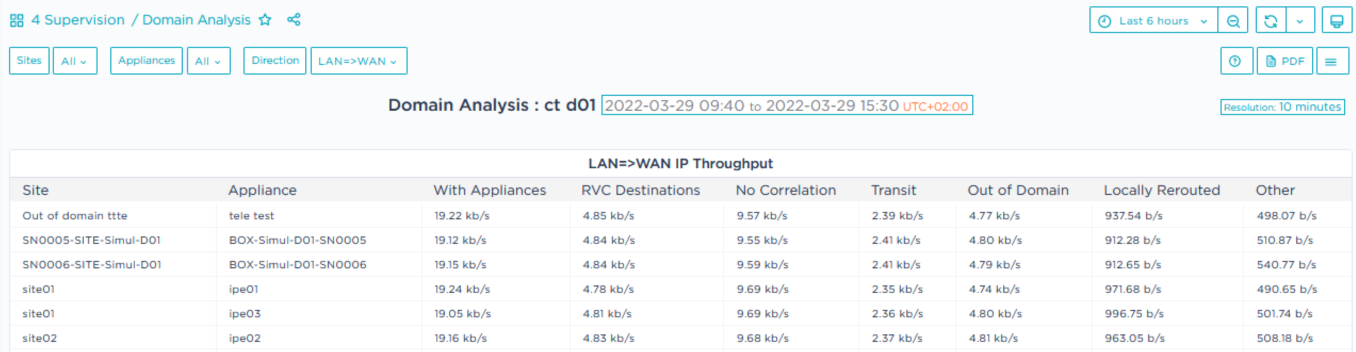
Appliance Monitoring : ct d01 2022-03-28 15:40 to 2022-03-29 15:30 UTC+02:00

Appliances Monitoring

Site	Appliance	Status	Cpu(%)	Synchronized	WAN Overload	Visibility	Application Control	WANopt	SSL Proxy	SaaS
Out of domain ttte	tele test	up	9.29	yes	no	up	disabled	disabled	disabled	down
SN0005-SITE-Simul-D01	BOX-Simul-D01-SN0005	up	8.12	yes	no	up	up	up	disabled	up
SN0006-SITE-Simul-D01	BOX-Simul-D01-SN0006	up	7.56	yes	no	up	up	up	disabled	up
site01	ipe01	up	8.55	yes	no	up	up	up	disabled	up
site01	ipe03	up	9.57	yes	no	up	up	up	disabled	up
site02	ipe02	up	9.79	yes	no	up	up	up	disabled	up
site04-é@!è:,()à	ipe04	up	6.76	yes	no	up	up	disabled	disabled	down

This dashboard informs you of the health and status of deployed Appliances. You may filter the data of this dashboard by Site and by Appliance.

Domain Analysis



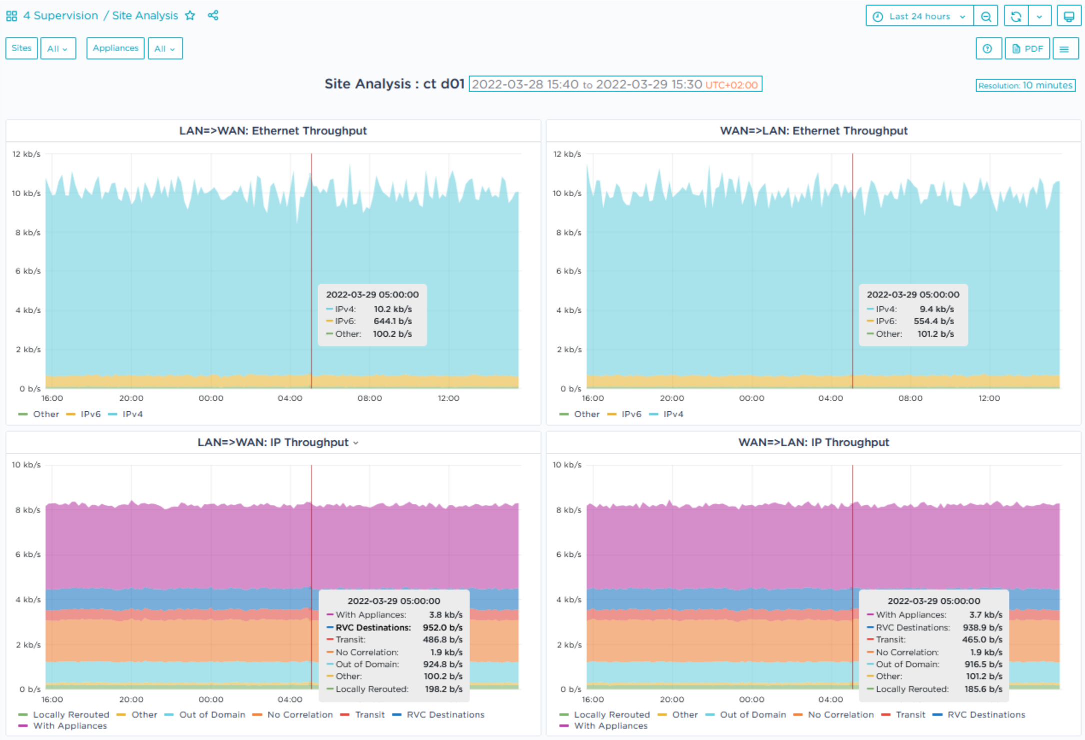
Domain Analysis : ct d01 2022-03-29 09:40 to 2022-03-29 15:30 UTC+02:00

LAN=>WAN IP Throughput

Site	Appliance	With Appliances	RVC Destinations	No Correlation	Transit	Out of Domain	Locally Rerouted	Other
Out of domain ttte	tele test	19.22 kb/s	4.85 kb/s	9.57 kb/s	2.39 kb/s	4.77 kb/s	937.54 b/s	498.07 b/s
SN0005-SITE-Simul-D01	BOX-Simul-D01-SN0005	19.12 kb/s	4.84 kb/s	9.55 kb/s	2.41 kb/s	4.80 kb/s	912.28 b/s	510.87 b/s
SN0006-SITE-Simul-D01	BOX-Simul-D01-SN0006	19.15 kb/s	4.84 kb/s	9.59 kb/s	2.41 kb/s	4.79 kb/s	912.65 b/s	540.77 b/s
site01	ipe01	19.24 kb/s	4.78 kb/s	9.69 kb/s	2.35 kb/s	4.74 kb/s	971.68 b/s	490.65 b/s
site01	ipe03	19.05 kb/s	4.81 kb/s	9.69 kb/s	2.36 kb/s	4.80 kb/s	996.75 b/s	501.74 b/s
site02	ipe02	19.16 kb/s	4.83 kb/s	9.68 kb/s	2.37 kb/s	4.81 kb/s	963.05 b/s	508.18 b/s

This dashboard displays detailed throughput data in the LAN=>WAN and WAN=>LAN directions for the Sites of the Domain. You can filter the information by Site, Appliance and Direction.

Site Analysis



This dashboard affords a clear insight into traffic recognition by Appliances.

You may filter the data of this dashboard by Site and by Appliance.

The top pane displays Ethernet throughput per type of traffic (IPv4, IPv6 or Other) in both the LAN=>WAN and WAN=>LAN directions for the selected appliance(s).

The bottom pane of the dashboard displays IP throughput by specifying how traffic is identified by the selected appliance(s) (..., virtual, out of domain, transit,...) in both the LAN=>WAN and WAN=>LAN directions.

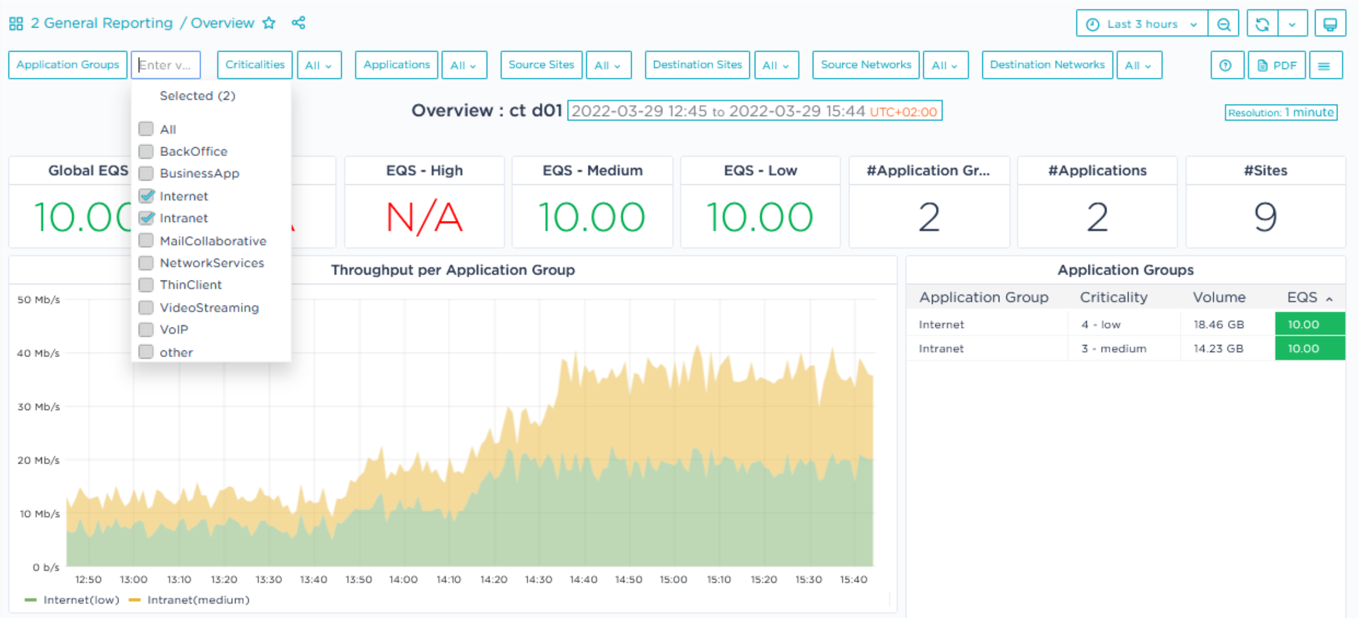
Navigating a Dashboard - Use Case

The **General Reporting/Overview** dashboard is displayed by default when you access the Reporting function. This dashboard is an overview of EQS (see "Application Flows - Detailed flows list"), Volume and Throughput per Application, Application Group, Site and Network.

The following functions affect all the dashboard cells.

Filtering objects

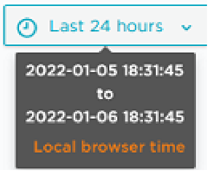
All your objects are displayed by default. You may select some specific objects to analyze in each filtering stack.



Application Group	Criticality	Volume	EQS
Internet	4 - low	18.46 GB	10.00
Intranet	3 - medium	14.23 GB	10.00

Selecting the Display Criteria

1 From the button toolbar located in the top right corner of the dashboard, click the Time Range button. It specifies the current time range.



2022-01-05 18:31:45
to
2022-01-06 18:31:45
Local browser time

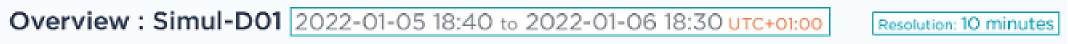
Depending on the dashboard category, default time range values are the following:

- **1 Governance**: last month
- **2 General Reporting**: last 24 hours

- **3 Usage and Performance**: last hour
- **4 Supervision**: last 24 hours

You can modify the default time range by applying an Absolute Time Range you have defined, or by selecting a Relative Time Range from the list.

2 The report default time zone (local browser time) is displayed in orange in the report sub-title. You can modify this value by selecting **Change time settings** in the Time Range selector.



Overview : Simul-D01 2022-01-05 18:40 to 2022-01-06 18:30 UTC+01:00 Resolution: 10 minutes

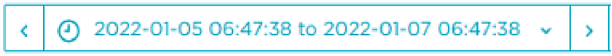
3 Data resolution is specified in blue at the right of the report sub-title. It indicates the statistics period or granularity of the displayed information.

4 If you want your dashboard to be refreshed automatically, select a period from the Refreshing stack: ↻ 5m ⌄

Instead of defining an automatic refresh period, you can refresh the dashboard manually by clicking the ↻ button.

Zooming Out

Click the 🔍 button in the top right button toolbar to zoom out dashboard display. The time range is extended as specified at the top of the window:

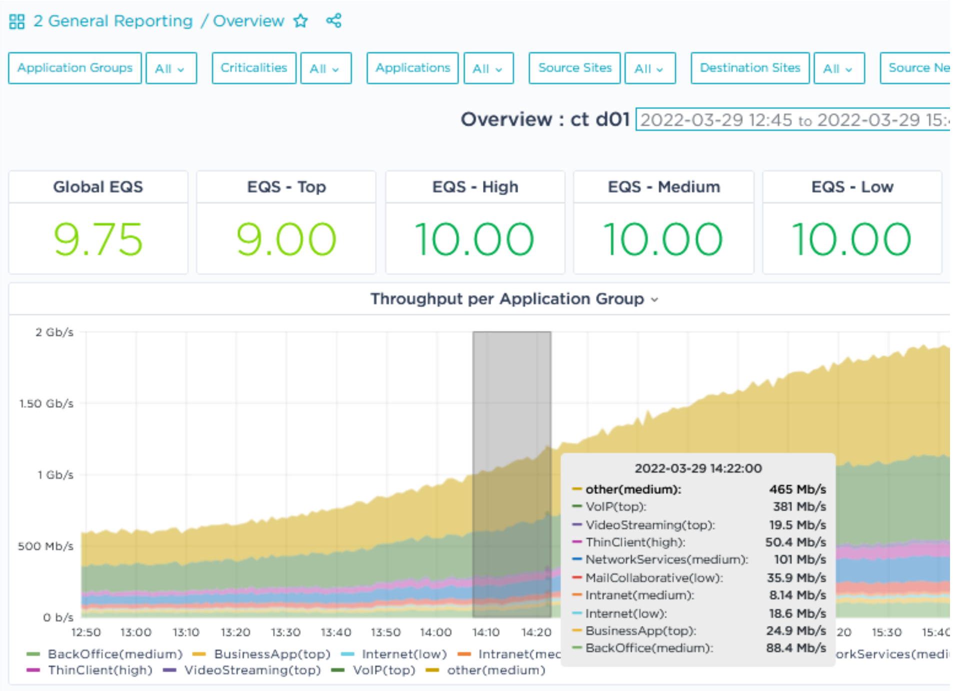


‹ 2022-01-05 06:47:38 to 2022-01-07 06:47:38 ⌄ ›.

You can use the arrows on both sides of the time range to move forward and backward (one time range shifts).

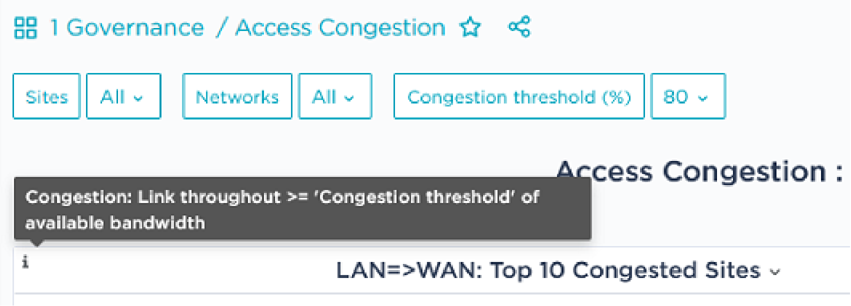
Zooming In

Zoom in on any time series graph by positioning your cursor on a specific section of the graph and dragging to the right. The result graph displays more points at a lower display rate. You can continue zooming in until you reach the necessary detailed report.


2 General Reporting / Overview
Application Groups All
Criticalities All
Applications All
Source Sites All
Destination Sites All
Source Ne
Overview : ct d01 2022-03-29 12:45 to 2022-03-29 15:
Global EQS 9.75
EQS - Top 9.00
EQS - High 10.00
EQS - Medium 10.00
EQS - Low 10.00
Throughput per Application Group
2 Gb/s
1.50 Gb/s
1 Gb/s
500 Mb/s
0 b/s
12:50 13:00 13:10 13:20 13:30 13:40 13:50 14:00 14:10 14:20 20 15:30 15:40
2022-03-29 14:22:00
other(medium): 465 Mb/s
VoIP(top): 381 Mb/s
VideoStreaming(top): 19.5 Mb/s
ThinClient(high): 50.4 Mb/s
NetworkServices(medium): 101 Mb/s
MailCollaborative(low): 35.9 Mb/s
Intranet(medium): 8.14 Mb/s
Internet(low): 18.6 Mb/s
BusinessApp(top): 24.9 Mb/s
BackOffice(medium): 88.4 Mb/s
BackOffice(medium) BusinessApp(top) Internet(low) Intranet(mec orkServices(medi
ThinClient(high) VideoStreaming(top) VoIP(top) other(medium)

Displaying Tooltips

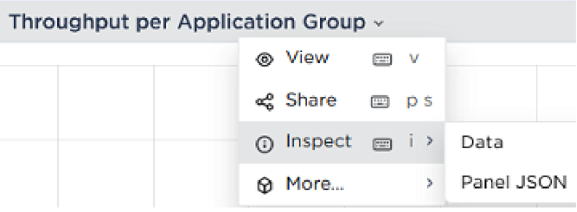
Click the i icon in the cell top left corner of some dashboards to display short information about cell display. These tooltips may help you read some special graphs.


1 Governance / Access Congestion
Sites All
Networks All
Congestion threshold (%) 80
Access Congestion :
i
LAN=>WAN: Top 10 Congested Sites

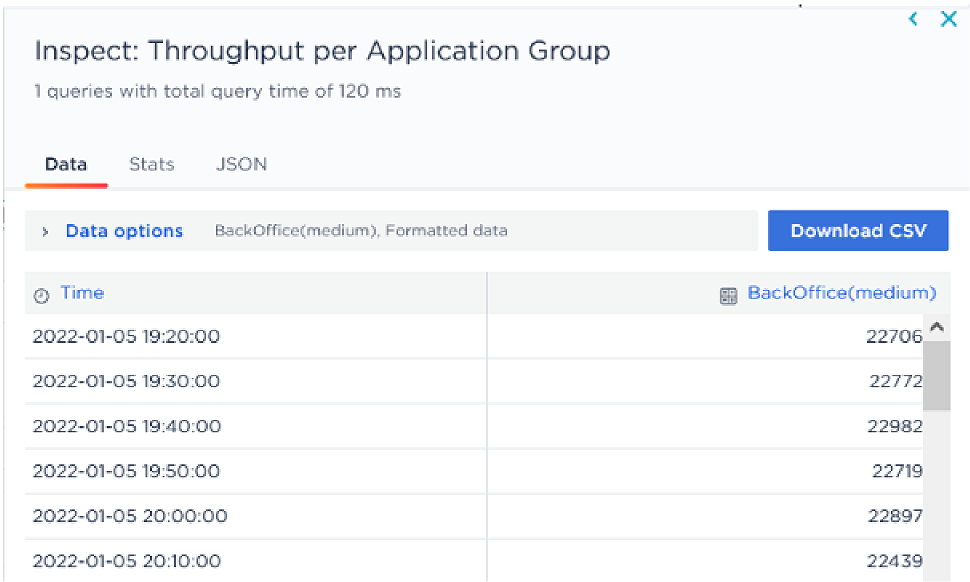
Congestion: Link throughout >= 'Congestion threshold' of available bandwidth

Using Dashboard Cell functions

Click the title of any cell in the dashboard to display the functional menu. The available functions depend on the type of presentation (pie chart, bar chart, time series graph, table, etc.).



- Use the **View** function to fully display this dashboard cell on the Reporting window.
- Use the **Share** function to link, embed or take a snapshot of this dashboard cell. Refer to "Sharing the dashboard".
- Use the **Inspect -> Data** function to export the cell data as a .csv file, display statistics and JSON panels, etc.



Inspect: Throughput per Application Group

1 queries with total query time of 120 ms

BackOffice(medium), Formatted data

Time	BackOffice(medium)
2022-01-05 19:20:00	22706
2022-01-05 19:30:00	22772
2022-01-05 19:40:00	22982
2022-01-05 19:50:00	22719
2022-01-05 20:00:00	22897
2022-01-05 20:10:00	22439

- Use the **More -> Toggle legend** function to hide/display the legend when the cell contains a graph.

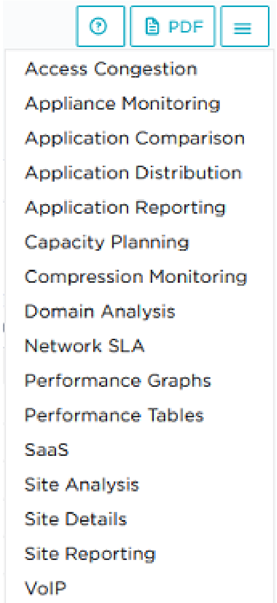
  You can also click legend elements for exclusive display. If you want to display a few curves only, keep the CTRL key pressed down and click the appropriate legend elements.

Sorting Table columns

On a table, you may sort column data by clicking the column header names.

Accessing other dashboards

Through the ≡ button located beside the object filters at the top of the window, you can select all the other predefined dashboards. They are displayed in new windows, with the same time range and the same filters as the initial dashboard.



You may define the most frequently used dashboards as favorites through the ☆ button located at the right of the dashboard title. You can filter these 'starred' dashboards in the list of predefined dashboard categories.

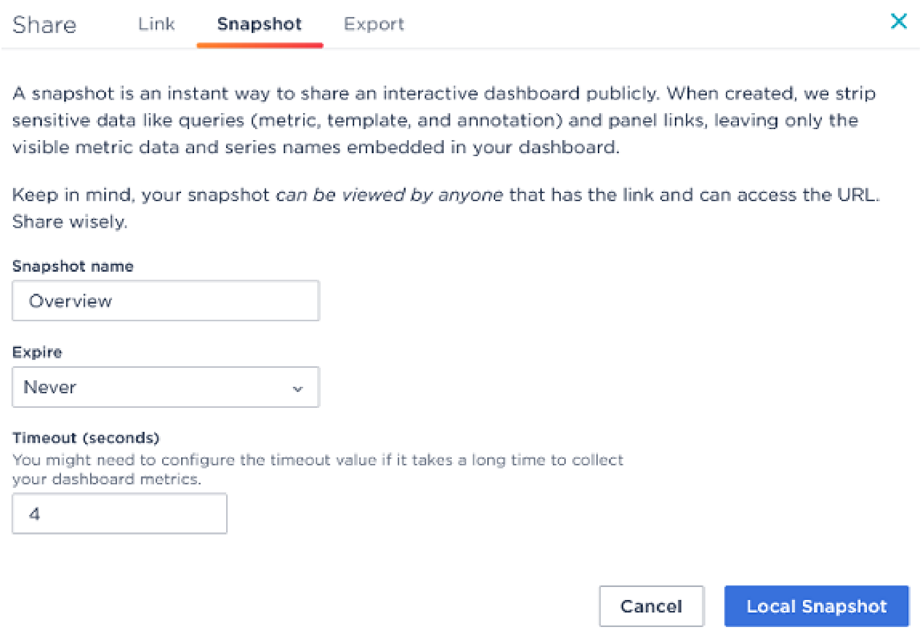
Exporting the dashboard as a PDF file

Through the PDF button located beside the object filters at the top of the window, you can export the current dashboard as a PDF file.

Sharing the dashboard

Through the ⋖ button at the right of the dashboard title, you may share a dashboard by creating a link to it, creating a snapshot of this dashboard or exporting it.

- From the **Link** tab, you can create a link to the current dashboard via an URL.
- Hit the **Snapshot** tab and define your parameters. After clicking the Local Snapshot button, copy the generated URL.



A snapshot is an instant way to share an interactive dashboard publicly. When created, we strip sensitive data like queries (metric, template, and annotation) and panel links, leaving only the visible metric data and series names embedded in your dashboard.

Keep in mind, your snapshot *can be viewed by anyone* that has the link and can access the URL. Share wisely.

Snapshot name: Overview

Expire: Never

Timeout (seconds)
You might need to configure the timeout value if it takes a long time to collect your dashboard metrics.
4

Then, the snapshot URL appears in the Management list.

- From the **Export** tab, you can export the dashboard through a JSON file to be shared externally.

Accessing Help

Through the Help button ⓘ located beside the object filters at the top of the window, you can access help for each dashboard.

The Reporting Toolbar

The Reporting toolbar is displayed at the left of the window. It contains several icons that enable you to access the Reporting functions.

☰	Click this icon to go back to the General Reporting/Overview default dashboard.
🔍	Click this icon to display the dashboard list and search for a dashboard by entering its name.
⊞	Click this icon to manage the dashboards and folders. Refer to "Predefined Dashboard Categories".
👤	Click this icon to access the Preferences parameters. You can select a dark or light UI Theme. Note that the other parameters can only be modified by your Administrator.
?	Click this icon to access a list of keyboard shortcuts.