ExtremeCloud SD-WAN

User Guide

Release 23.5.0

Updated: 21 August 2023

www.extremenetworks.com

Contents

1 ExtremeCloud SD-WAN overview

This section helps you understand the ExtremeCloud SD-WAN concepts. It contains an overview of the provided services.

- "Presentation"
- "Prerequisites"

Presentation

Delivered based on a cloud-native system architecture, ExtremeCloud SD-WAN closely integrates a key set of solution components:

- ExtremeCloud SD-WAN Orchestrator, cloud-hosted and part of ExtremeCloud, providing a single pane of glass interface for configuration and policy definition across the entire WAN. Policy includes SD-WAN appliances, SD-WAN topology, security profiles and Applications Anywhere automated SaaS and IaaS on-ramp rules. All of this topped with end-to-end Quality of Experience (QoE) policy enforcement and application performance reporting.
- Hardware SD-WAN Appliances offering a range of deployment modes (routed, route/bridge hybrid, bridge) and site resiliency features designed to ensure a risk-free SD-WAN technology introduction. These are proprietary hardware appliances deployed on site, between the WAN devices and the LAN switch. SD-WAN Appliances are provided by Extreme, as part of the ExtremeCloud SD-WAN solution.
- Site-DC-IaaS connectivity established over any WAN transport, creating flexible secure overlay topologies including hub and spoke and full mesh or remote connections to public clouds; Proprietary Dynamic WAN Selection algorithm is used to distribute the traffic across different transport networks, based on the application performance driven Experience Quality Score. Integration between Extreme Fabric Extend and ExtremeCloud SD-WAN allows extending an existing campus network-based Fabric, with all the functionalities, towards remote sites equipped just with Internet connectivity.
- Full security stack featuring a Zone-Based Firewall used for VPN traffic segmentation and Internet traffic steering (direct to internet, backhauling in DC, web gateways) and cloud-based advanced networking platform EdgeSentry (powered by Check Point) designed to bolster Site-based security using FWaaS and SWG (including Web filtering, HTTPs inspection, DLP, and more).
- Unrivaled Application Performance including layer 7 Application Performance Monitoring analyzing all application flows traversing the SD-WAN overlay, an Application Performance Monitoring and Control algorithm enforcing an advanced, end-to-end, per-session QoS across the entire SD-WAN and WAN optimization for usage on highly congested networks; Application Performance specific data is immediately available for Customer analysis in the SD-WAN Orchestrator Reporting Module.

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
	Upgrade	https	443
	NTP clock synchronization	UDP	123

Appliances in IPsec overlays

- Spoke Site: UDP:500 and UDP:4500 outbound connections
- Hub Site: local port forwarding of UDP:500 and UDP:4500 inbound from the public IP address to the hub appliance

2 Logging in

Use the following procedure to log in to the ExtremeCloud SD-WAN platform.

1. Log in to ExtremeCloud IQ with your user email address and your defined password.
2. On the ExtremeCloud Apps page, select **ExtremeCloud SD-WAN**.

SD-WAN Setup

Follow the setup steps listed on the first page of the Onboard Wizard and configure the basic components of your network.

3 Onboarding

Follow the steps of the Onboard Wizard to create the basic components of your network. Subsequently, you can also use the **Settings** function in the main menu.

1. Configure Policy
2. Create sites and appliances
3. Configure appliances
4. Deploy the configuration

Configuring the Network Policy

The network policy is a combination of configuration settings that manage the behavior of the whole SD-WAN network. It includes network security, appliance templates, overlay management and application group policy.

This topic guides you through the basic steps to enable ExtremeCloud SD-WAN appliances to provide clients with network access.

> **Note:** ExtremeCloud SD-WAN requires only one network policy for all network appliances.

There are multiple tabs as part of the network policy configuration process:

- Templates
- Overlays
- Security
- Application Group Policy

Create the Network Policy

1 Start with the **Policy Configuration** step in the SD-WAN Onboard Wizard (subsequently, select **Settings -> Policy Configuration** from the left main menu).

2 Enter the Policy name and description.

Advanced Settings

3 WAN Optimization is enabled by default. You may disable this parameter.

4 Enter the NTP Server IP address or check the **Auto** option to use a default IP address.

5 To enable log export of NATted DTI connections by SD-WAN appliances, you must define one (or several) Syslog Server(s) in your network.

After you have clicked **Add Syslog Server**, enter the server Name, type its IP Address (preferably in your private network), Protocol (TCP or UDP) and Port. When NAT entries are created, logs are sent to the Syslog Server in syslog format.

Click **Add Server**.

> **Warning:** log export is not available on VRRP backups (with unmounted tunnels).

6 Fabric Support

- Enable **Fabric Support** to benefit from Fabric Connect functions on ExtremeCloud SD-WAN appliances and facilitate network setup through Zero Touch deployment.

- Fabric Extend IP Network: enter the IPv4 address of the global subnet that will be used to automatically allocate subnets per LAN interface.

> **Warning:** when you enable Fabric Support, any existing configurations of SD-WAN appliances are deleted.

The following SD-WAN functions cannot be configured with Fabric Support; their related parameters are greyed out in the ExtremeCloud SD-WAN application windows:

- WAN Optimization
- Bypass
- Link State Propagation
- Routing Loop Prevention
- BGP, OSPF, HA
- DHCP Service
- Dynamic LAN Routing
- SWG, DTI, Internet Backhauling
- LAN2
- Syslog Server
- etc.

> **Note:** with Fabric Support, the WAN Interfaces are always in Router Mode. The Bridge Mode is not available.

For more information about Fabric Support, refer to the Fabric Engine User Guide and ExtremeCloud IQ Site Engine User Guide

7 Overlay Routing

- Overlay IP Network: subnet where ExtremeCloud SD-WAN selects the addresses of the appliance internal interfaces.
- AS Number Range: the SD-WAN application uses this range of values to configure Site autonomous systems automatically.
- 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`

8 Routing Loop Prevention

To prevent OSPF routing loops 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.

9. Then click **Apply** at the bottom of the window.

   The Policy Configuration window is refreshed with new data in the Application Group Policy panel.

Creating Appliance Templates

A template allows you to configure default settings for several SD-WAN appliances. After you configure a template, you can apply this appliance template and its configuration settings to large numbers of appliances of the same type, and apply different templates to other appliances in the network policy.

> **Warning:** you will need to create a template for every appliance deployment type that will be used in your network. An appliance is always associated with a template.

> **Note:** some template parameters can be overwritten when you configure the appliance.

Before creating a template, remember that 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 ExtremeCloud SD-WAN application enables you to build an overlay network of site connections through IPsec tunnels.

> **Note:** if **Fabric Support** is enabled, many of the following parameters are greyed out because they are not compatible with this specific deployment mode.

Description of Parameters

Overview

- Template Name: always enter a consistent template name.
- Description: this description will help you identify the template in a significant list of appliance templates.

Setup

Interface Configuration

- LAN Setup: select both LAN1 and LAN2 to enable the MultiPath mode. It implements two traffic paths: from LAN1 to WAN1 and from LAN2 to WAN2.
- 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
- WAN Setup: : define each interface, WAN1, WAN2 and WAN3, in either Bridge or Router mode.

Advanced Settings

- Role in Hub & Spoke: define the appliance as a Spoke (Branch Office) or a Hub (Data Center). Tunnels (generated on Router interfaces) are always built from the spokes to the hub.
- Bypass (LAN1 <-> WAN1 and LAN2 <-> WAN2 if you selected the multipath mode) : when this option is activated, 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.

  > **Warning:** To configure a hybrid appliance template, always start configuring WAN1 in bridge mode because of the Bypass function.

- Link State Propagation:
  - LAN -> WAN: this function copies 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.
  - WAN -> LAN
  - Disable
- Time Synchronization Server: using a Time Server located inside the Customer private network is recommended. Then, you can select 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.

Check this option to define a hub appliance as Time Synchronization Server. Appliance synchronization is used for correlation, hence for Delay/Jitter/Loss measurement.

- 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 helps improving quality by accelerating delay sensitive applications and by reducing bandwidth consumption.

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

- Internet Backhauling: select this option to identify the appliance as a Backhauling Site. The traffic is routed to the hub appliance (through underlay or overlay according to the deployment) which must be able to route it to a firewall or proxy.

  Backhauling can be activated on hub appliances (in Router or Bridge-Router mode) and on appliances in Bridge mode.

  - 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

> **Note:** if Fabric Support is enabled, LAN2 is deactivated, Path Mode is set to Dynamic, WAN Setup is in Router mode only and Bypass, Link State Propagation, WAN Optimization, Internet Backhauling are deactivated.

Configuration

LAN

VLAN - Add VLAN

- To create a New VLAN, enter its Name, Description and ID. You can define it as the Main VLAN.
- To Add a DHCP Service, define the following parameters:
  - Name
  - Description
  - Service: either select DHCP Server or DHCP Relay Agent (the appliance needs to relay host requests).
  - Primary DHCP Server: enter the server IP address.
  - Secondary DHCP Server: enter the server IP address.

Additional Settings

- LAN Interface Speed: this parameter is set to Auto by default 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.
- Dynamic LAN Routing:
  - None: there is no additional subnet or sub-interface to define for configuring BGP peering or OSPF adjacencies
  - BGP: select this option for configuring BGP
  - OSPF: select this option for configuring OSPF
- High Availability: select this option for configuring High Availability.

> **Note:** if Fabric Support is enabled, Add VLAN, Dynamic LAN Routing and High Availability are deactivated.

WAN1, WAN2, WAN3

Bridge Mode

- Description
- Bandwidth Up and Bandwidth Down: define the up and down bandwidth (in megabits per second) allocated to the WAN.
- WAN Service: select either MPLS or a WAN Service you created.
- Additional Settings:
  - Interface Speed: this parameter is set to Auto by default to let the system define the speed of the WAN interfaces, or you can force the speed to 100FD or 1000FD. The full duplex speed is expressed in megabits per second.
  - Min Bandwidth Up, Min Bandwidth Down (Mbps)
  - Default BGP Local Preference

Router Mode

- Description
- Bandwidth Up and Bandwidth Down: define the up and down bandwidth (in megabits per second) allocated to the WAN.
- WAN Service: select either Internet or a WAN Service you created.
- DTI: when you activate this option, this interface is eligible to DTI.
- NAT: directly derived from the activated Eligible DTI option, keep the NAT mode activated. This is a source-NAT where the LAN IP addresses are replaced with the WAN 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 NAT mode which controls the firewall, incoming connections from the WAN are allowed to go to the LAN.

- Secure Gateway (optional): you may either select from the list one of the Security Gateways that you have configured or select EdgeSentry to activate it on the interface. Refer to "Configuring traffic redirection to a Secure Web Gateway" and "EdgeSentry".
- Overlay (optional): you may select an Overlay you previously created and apply it to the interface. You can also create an overlay from this panel instead of returning to the Policy Configuration window. Refer to "Configuring Overlays".
- Additional Settings
  - Interface Speed: this parameter is set to Auto by default 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.
  - Min Bandwidth Up, Min Bandwidth Down (Mbps)
  - Default BGP Local Preference: enter the same Preference value as the local Preference value of the CE router.
  - MTU: enter the MTU value which corresponds to the maximum number of bytes loaded in the Payload. The default value is 1500.

Note: if Fabric Support is enabled, DTI, NAT and Secure Gateway are deactivated.

Create a template for a Hybrid SD-WAN Spoke appliance - first example

To configure the template of a hybrid SD-WAN spoke appliance with 2 MPLS links and 1 Internet Access link, proceed as follows:

1. Click **Add Template** in the Template panel of the Policy Configuration window.

   The Template Wizard displays the main steps of the procedure. Click **Continue**.

Overview

2. Enter the Template Name.
3. Type a description that will help you identify the template in a significant list of appliance templates. Click **Next - Setup Interface**.

Setup

4. On the displayed Setup graph:
   - select LAN1
   - select Dynamic as Path Mode
   - enable WAN1 and WAN2 in Bridge mode, WAN3 in Router mode
5. Select the role of the appliance as a Spoke.

6 Check LAN -> WAN as Link State Propagation: this function copies the state of the LAN to its related WAN. LAN1/WAN1 state synchronization is useful when the LAN interface breaks down.

7 Leave the other parameters to their default values.

8 Click **Next - Configure Interface** in the lower right corner of the wizard.

Configuration

LAN

9 In the LAN panel, leave all the parameters to their default values.

10 Click **Next - WAN Settings** in the lower right corner of the wizard or select the WAN tab next to the Configure Interface title.

WAN1, WAN2, WAN3

11 Configure the WAN1 interface:

- Enter a Bandwidth Up value and a Bandwidth Down value.
- Either select MPLS as the Transport Network or **create a Transport Network**. Then, you can select the new Transport Network you have created.
- Leave Additional Settings to their default values.

12 Configure the WAN2 interface by using the same procedure as for WAN1.

13 Configure the WAN3 interface:

- Enter a Bandwidth Up value and a Bandwidth Down value.
- Either select Internet as the Transport Network or **create a Transport Network**. Then, you can select the new Transport Network you have created.
- Activate the DTI and NAT options.
- Leave Additional Settings to their default values.

14 Click **Next - Summary** in the lower right corner of the template wizard.

15 Click **Create Template**.

The new template is displayed in the Template panel of the Policy Cofiguration window.

Create a template for a Hybrid SD-WAN Hub appliance - second example

1 Configure another template for a hybrid SD-WAN hub appliance. Compared to the previous spoke appliance template, the following parameters are specific to a hub template:

- Time Synchronization Server: check this option to define the hub appliance as Time Synchronization Server. Appliance synchronization is used for correlation, hence for Delay/Jitter/Loss measurement.

- Select the role of the appliance as a Hub.

Configuring Overlays

From the main menu, select **Settings** to display the Policy Configuration window.

The Overlays section enables you to define overlays used by your appliances,

- either Hub & Spoke overlays to create standard VPN connections between appliances and exchange traffic or
- External VPN Gateway overlays enabling the appliances to connect to an external provider by creating a new VPN connection to this provider (Microsoft Azure, etc.)

Create a Hub & Spoke Overlay

1. Click **Add Overlay** and select Hub & Spoke as Type.
2. Enter the Name of the overlay.
3. Define the following parameters:

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)
- Authentication: integrity drop-down list to choose the data integrity hash method
- 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 Concentrator authentication

If a Pre-Shared key is already configured, you can directly select it from the list.

This Pre-Shared key is used for all the tunnels between appliances. Though it is automatically generated by the system 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.

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,
- Authentication: 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) - optional: 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.

4. Click **Save**.

   Your new overlay is displayed in the Overlays section of the Policy Configuration window. Click any overlay to edit its parameters. Use **View All** if you want to delete any overlay(s).

Apply the Hub & Spoke Overlay to the Appliances

1. From the main menu, select **Appliances**.
2. Select the Spoke appliance and the WAN tab.
3. Select the appropriate WAN interface in Router mode and from the Overlay list, select the Hub & Spoke overlay that will establish the VPN tunnel. Click **Done**.
4. Select the Hub appliance and the WAN tab.
5. Select the appropriate WAN interface in Router mode and apply the same Hub & Spoke overlay as for the Spoke appliance.
6. Click **Done**. The tunnel is created.

Create an External VPN Gateway Overlay

This section describes how to configure an external gateway from a site appliance over the Internet. 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.

One tunnel is created after you have defined the appropriate parameters in **both** ExtremeCloud SD-WAN and in Microsoft Azure.

1. Click **Add Overlay** and select External VPN Gateway as Type.
2. Enter the Name of the overlay.
3. Enter the VPN gateway Primary Public IP Address.

Routing

> **Warning:** There is one prerequisite which is the necessary configuration of the gateway parameters in Microsoft Azure.

4. You can define how the traffic is routed through the tunnel by using subnet information (static configuration) or BGP (dynamic configuration).

- If you select **Static** routing, define (Add Subnet) the remote Microsoft Azure subnet IP address by entering its prefix and prefix length. Note that you also defined this IP address in Microsoft Azure. Click **Add** to validate.
- 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. Also specify the default Local Preference.

5. For IKE Policy, IPsec Concentrator Authentication and IPsec Policy parameters, refer to the "Create a Hub & Spoke Overlay" description.

Apply the External VPN Gateway Overlay to the Appliances

1. From the main menu, select **Appliances**.
2. Select the Spoke appliance and the WAN tab.
3. Select the appropriate WAN interface in Router mode and from the Overlay list, select the External VPN Gateway overlay that will establish the VPN tunnel. Click **Done**.
4. Select the Hub appliance and the WAN tab.
5. Select the appropriate WAN interface in Router mode and apply the same External VPN Gateway overlay as for the Spoke appliance.
6. You may edit Tunnel Customization parameters as follows:
   - Only specify an Initiator ID when authentication with Microsoft Azure or Cisco is executed through an address different from the public IP address.
   - 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.

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.

Use the icon different statuses to either display or hide the key.

- 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.
- When the VPN gateway is configured in static mode, specify the Inside Remote IP address which corresponds to the tunnel termination interface 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.
- The BGP Local Precedence parameter is not used when there is only one external gateway. In the case there are two gateways with the same subnet, the Precedence value enables you to define which tunnel has priority to route the traffic.

  The highest Precedence value implies priority.

7 Click **Done**. The tunnel is created.

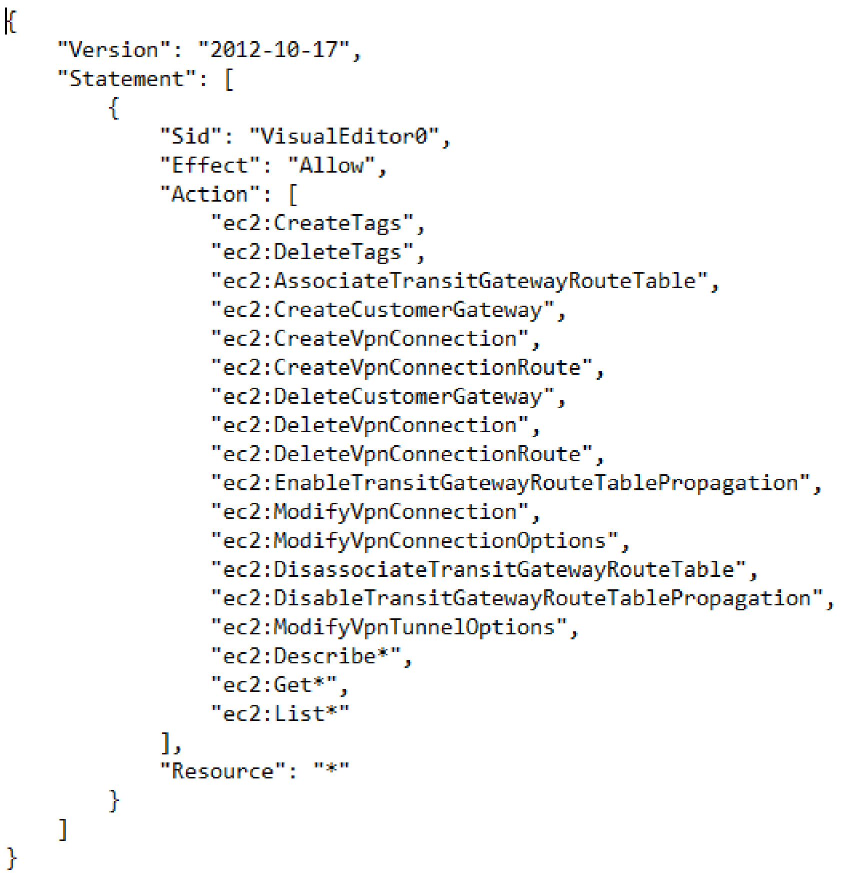
Connecting an Appliance to a Cloud Gateway

Prerequisites

The following prerequisites describes the necessary configuration actions in AWS and Azure for the Cloud gateways the SD-WAN Application 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 Application 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 Application 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 3 (client secret) for authentication.
- The role to be associated with the Azure AD application on the targeted subscription is 'Network Contributor'.
- A Storage Account is necessary for storing the configuration information of the VPN tunnels when there are connections to Virtual Hubs. 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.
- the Vnet Gateway following SKUs are supported:
  - VpnGw1
  - VpnGw1AZ
  - VpnGw2
  - VpnGw2AZ
  - VpnGw3
  - VpnGw3AZ
  - VpnGw4
  - VpnGw4AZ
  - VpnGw5
  - VpnGw5A
- 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 modify the selection of regions related to the chosen Cloud Access object and define tunnel parameters.
3. Connect the selected Spoke 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 SD-WAN Application and in AWS or Azure.

Connecting a Spoke appliance to an AWS Gateway

1 From the main menu, select **Appliances**.

2 Select the appropriate Spoke appliance and click **Edit Configuration**.

3 Select the appropriate WAN interface in Router mode.

4 From the Tunnels -> Overlay stack, select the AWS gateway overlay that will establish the VPN tunnel. It is then displayed in the Applications Anywhere list.

5 Click **Configure Tunnel**.

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 corresponds to its name in AWS (if it exists) or its ID in AWS (vgw-xxxxx or tgw-xxxxx).

The SD-WAN Application retrieves the AS number of the Cloud gateway. The AS number of the Cloud gateway:

- must not be included in the AS number range
- or must be defined as an exclusion
- and should be different from any other appliance ASN in the domain

  Refer to "Overlay Routing ".

6 Since PSK is the only authentication type currently supported, the SD-WAN Application automatically generates a pre-shared key. This authentication type requires a WAN interface public IP address to be specified.

7 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 Application retrieves the list of transit gateway route tables. For every route table, its name and ID are specified.

8 You can enable VPN Acceleration and define the Association Route Table and Propagation Route Tables. Transit Gateway route tables are objects that enable network segmentation, i.e. they define whether attachments can communicate with one another.

- Association Route Table: select one of the route tables or none for association.
- Propagation Route Tables: select several route tables or none for propagation.

For all the Gateways

9 **Save** 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 Spoke appliance to an Azure Gateway

1 From the main menu, select **Appliances**.

2 Select the appropriate Spoke appliance and click **Edit Configuration**.

3 Select the appropriate WAN interface in Router mode.

4 From the Tunnels -> Overlay stack, select the Azure gateway overlay that will establish the VPN tunnel. It is then displayed in the Applications Anywhere list.

5 Click **Configure Tunnel**.

There are two types of Azure managed gateways:

- Vnet Gateway (Virtual Network Gateway in Azure): a Vnet Gateway is a resource associated with a Virtual Network that provides connectivity to this Vnet (through site-to-site VPN or ExpressRoute)
- Virtual Hub VPN Gateway (Virtual Hub VPN Gateway in Azure): a Virtual Hub 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

The SD-WAN Application retrieves the AS number of the Cloud gateway. The AS number of the Cloud gateway:

- must not be included in the AS number range
- or must be defined as an exclusion
- and should be different from any other appliance ASN in the domain

  Refer to "Overlay Routing ".

6 Since PSK is the only authentication type currently supported, the SD-WAN Application automatically generates a pre-shared key. This authentication type requires a WAN interface public IP address to be specified.

7 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 only

VPN acceleration 'enabled' corresponds to routing via "Microsoft global network" whereas VPN acceleration 'disabled' corresponds to routing over public Internet (refer to routing preference).

8 You can define the Association Route Table and Propagation Route Tables. Virtual Hub route tables are objects that enable network segmentation, i.e. they define whether attachments can communicate with one another.

- Association Route Table: select the route table for association, either the Default one or any other route table.
- Propagation Route Tables: select one or more route table(s) for propagation, or the None option.
- Propagation Labels: you may enter one or more labels for propagation.

  Make sure that your choices for association and propagation follow the guidelines from Azure (see Additional considerations).

For all the Gateways

9 **Save** 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 Network Security

The **Security** panel of the Policy Configuration window enables you to create a zone-based firewall in order 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).

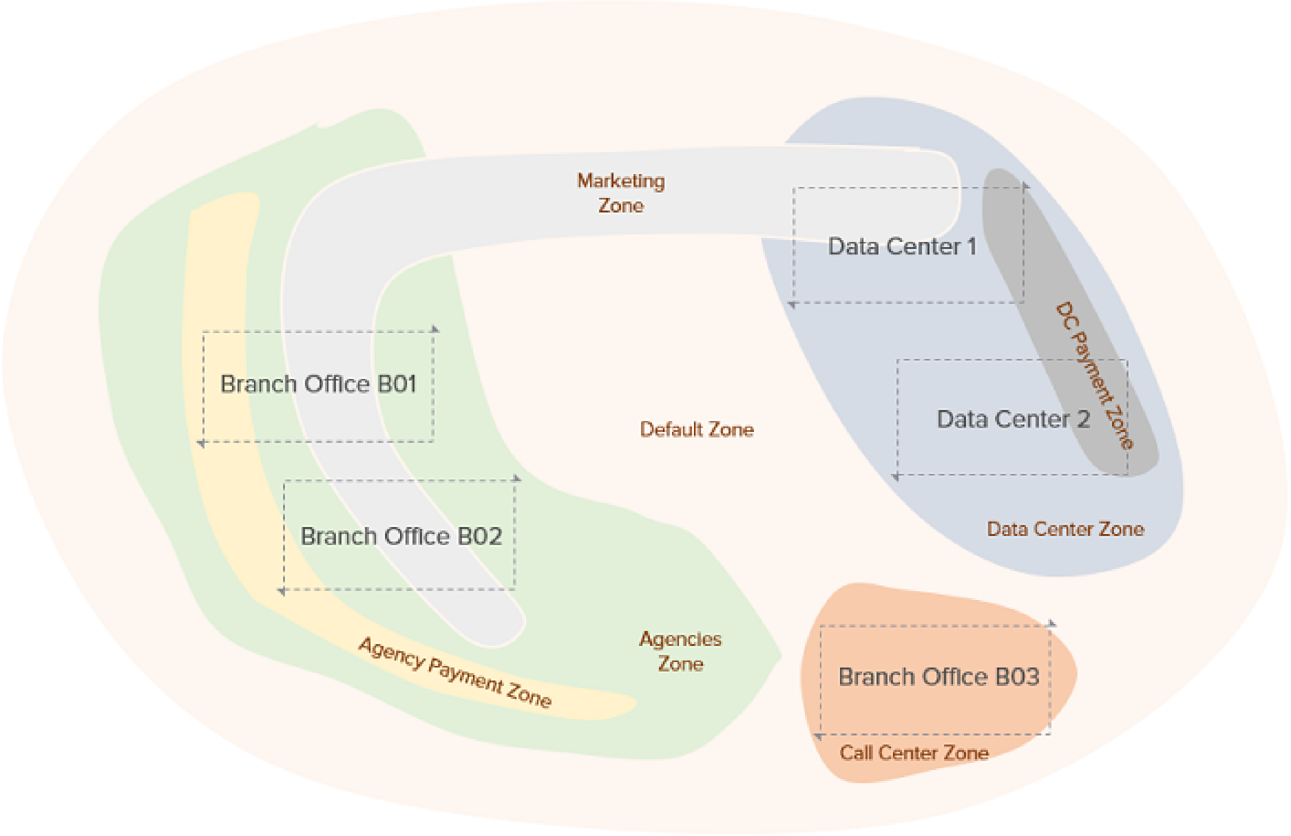
Security policies are configured globally for the network; the SD-WAN application then translates each global policy into a local routing/firewalling rule for each involved SD-WAN appliance.

> **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 Internet Access Control Lists 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".

- "Defining VPN Zones"
- "Setting VPN Segmentation Policies"
- "Defining Application Sets"
- "Setting Internet Access Control Lists"

VPN Segmentation Use Case



To create a Security 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 the Use Case 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).

Define the Agencies zone

In the VPN Segmentation panel of the Security window, the Default Zone with its subnets is already displayed. You cannot modify it.

1. Click the **Add VPN Zone** button.
2. Type 'Agencies' as the Name of the zone.
3. 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.
4. From the Sites list which includes all the Sites you have configured, select B01 and B02 Sites.

   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.
5. Click **Save Changes** to validate.

6 Use the **View All** function to display the VPN Segmentation matrix and continue adding VPN Zones.

Define the Call Center zone

1 Click the **Add VPN Zone** button.

2 Type 'Call Center' as the Name of the zone.

3 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.

4 From the Sites list which includes all the Sites you have configured, select the B03 Site.

5 Click **Save Changes** to validate.

Define the Data Center Zone

1 Click the **Add VPN Zone** button.

2 Type 'Data Center' as the Name of the zone.

3 Enter a low Priority (4) for this zone because it is clearly identified with no subnet overlap.

4 DataCenter and DataCenter2 are two appliances on the same Site named DataCenter. From the Sites list which includes all the Sites you have configured, select the DataCenter Site.

5 Click **Save Changes** to validate.

Define the DC Payment zone

1 Click the **Add VPN Zone** button.

2 Type 'DC Payment' as the Name of the zone.

3 Enter a high Priority value (2) for this zone because of the acuteness of its subnet definition.

4 Use the Subnets panel to identify DC Payment two subnets: 10.1.4.128/26 and 10.2.4.128/26.

5 Click **Save Changes** to validate.

Define the Agency Payment zone

1 Click the **Add VPN Zone** button.

2 Type 'Agency Payment' as the Name of the zone.

3 Enter a high Priority value (1) for this zone because of the acuteness of its subnet definition.

4 Use the Subnets panel to identify Agency Payment two subnets: 10.1.1.128/26 and 10.1.2.128/26.

5 Click **Save Changes** to validate.

Define the Marketing zone

1. Click the **Add VPN Zone** button.
2. Type 'Marketing' as the Name of the zone.
3. Enter an average Priority value (3) for this zone.
4. 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.
5. Click **Save Changes** to validate.

Modifying or deleting a VPN Zone

In the VPN Segmentation window:

- Click any VPN Zone row to edit its configuration. Modify any values and click **Save Changes**.
- Click 🗑 if you want to delete a VPN zone. The system asks you to click the icon a second time to confirm your action.

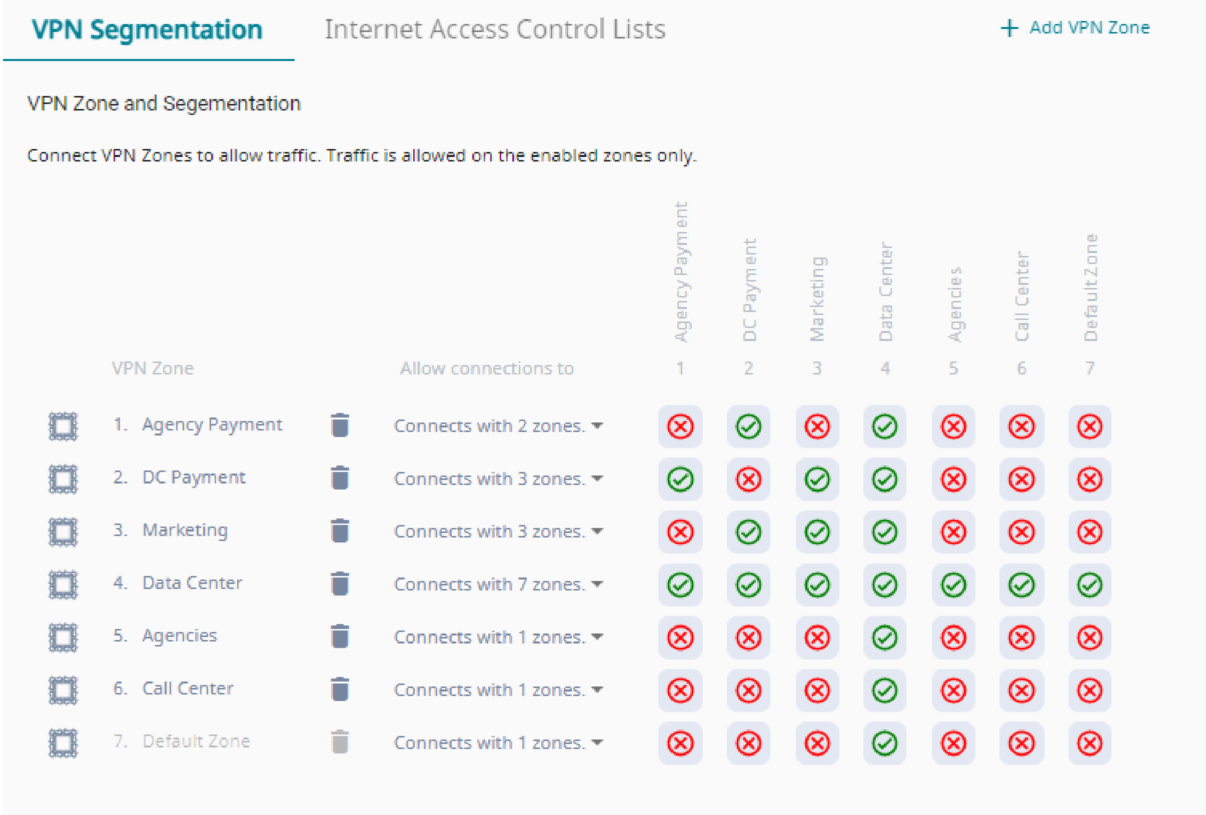
After you have defined your VPN zones, you must apply VPN Segmentation Policies to these zones.

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 Security 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 Zone and Segementation

Connect VPN Zones to allow traffic. Traffic is allowed on the enabled zones only.

VPN Zone	Allow connections to	Agency Payment 1	DC Payment 2	Marketing 3	Data Center 4	Agencies 5	Call Center 6	Default Zone 7
1. Agency Payment	Connects with 2 zones.	✗	✓	✗	✓	✗	✗	✗
2. DC Payment	Connects with 3 zones.	✓	✗	✓	✓	✗	✗	✗
3. Marketing	Connects with 3 zones.	✗	✓	✓	✓	✗	✗	✗
4. Data Center	Connects with 7 zones.	✓	✓	✓	✓	✓	✓	✓
5. Agencies	Connects with 1 zones.	✗	✗	✗	✓	✗	✗	✗
6. Call Center	Connects with 1 zones.	✗	✗	✗	✓	✗	✗	✗
7. Default Zone	Connects with 1 zones.	✗	✗	✗	✓	✗	✗	✗

You can also use the **Allow Connections to** lists to select the appropriate VPN zones.

This configuration implements the following policies (refer to the Use Case diagram):

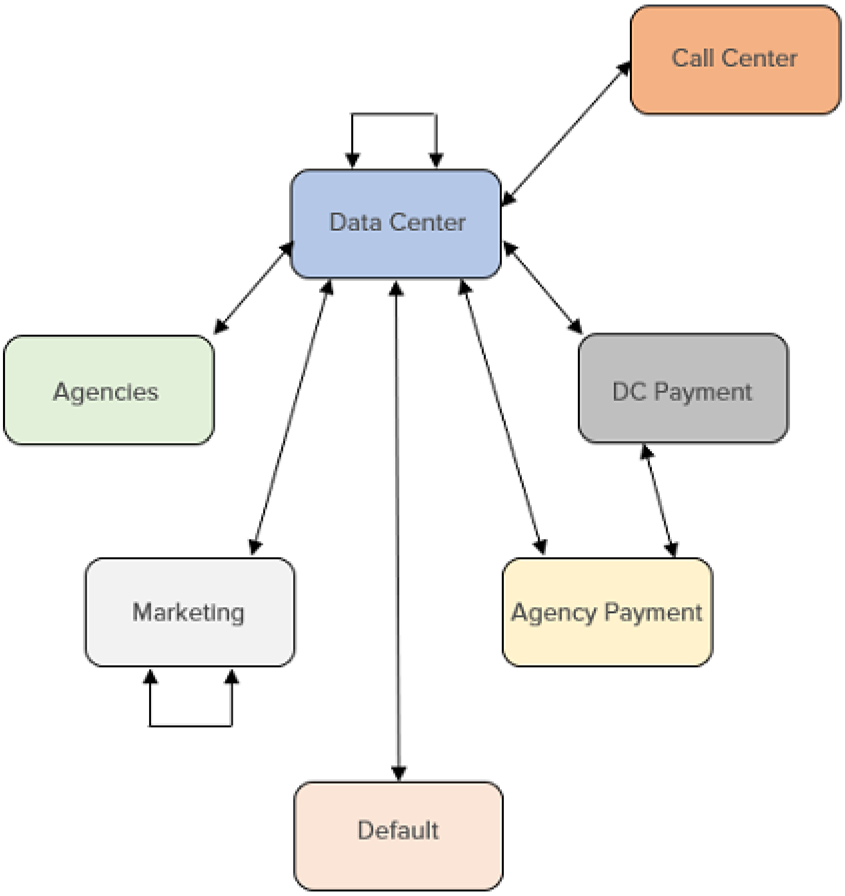
- the appliances that do not belong to any other zone than the Default Zone can communicate with the appliances of the Data Center zone
- the appliances in the Data Center zone can communicate with all the other zones, including appliances of other sites in the Data Center zone

> **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.

In the current Use Case, 5 application sets are created: Business, Communication, Marketing, Development and Call Center. Default Internet contains all the other applications.

Define the Business application set

1. Click **Add Application Set** in the top right corner of the Internet Access Control Lists window.
2. Type 'Business' as the Name of the application set.
3. From the list of SaaS Applications, select 'Salesforce'. 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.
4. Click **Save Changes** to validate.

Define the Communication, Marketing and Development application sets

Proceed exactly as for the previous Business application set:

- Communication: Communication - Social Network (2 application sets)
- Marketing: Marketing
- Development: Development

Define the Call Center application set

This application set is based on Protocol and Port.

1. Click **Add Application Set** in the top right corner of the Internet Access Control Lists window.
2. Type 'Call Center' as the Name of the application set.
3. Select the **Port Range** option and click **Add Port-Based App.**
4. From the Protocol list, select 'UDP' and enter '255;300' as Ports.
5. Define the parameters of the second application. From the Protocol list, select 'TCP' and enter * as Port (all the available ports are taken into account).
6. Click **Save Changes** to validate.

Modifying or deleting an Application Set

In the Internet Access Control Lists window:

- Click any Application Set name to edit its configuration. Modify any values and click **Save Changes**.
- You may also click any Application Set name and use the **Delete Application Set** button.

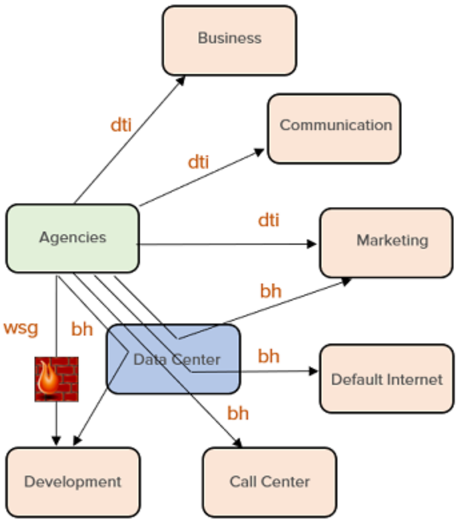
After you have defined your application sets, you must apply Internet Access Policies to them.

Setting Internet Access Control Lists

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 Security matrix and select one option among bh, dti, dti+, wsg and wsg+ and deny. This configuration is kept after any ExtremeCloud SD-WAN upgrade.

The following diagram illustrates the Internet Access Control List that has been defined for the Agencies VPN zone to access the applications in the Business, Communication, Marketing, Development, Call Center and Default Internet application sets (see "VPN Segmentation Use Case").



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 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 Secure Web Gateway in the Cloud. This policy is only available with Internet interfaces when EdgeSentry is activated or when there is a configured Secure Web 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 secure web gateway, 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	tunnel to	drop

Interface/Policy	dti	dti+	wsg	wsg+	bh	deny
				dc	dc	
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. When positioning your cursor over the exclamation mark, you may know which appliance(s) are involved.

The same rule applies to 'wsg'.

In these error cases, the traffic is dropped and all the ExtremeCloud SD-WAN services are deactivated.

Configuring traffic redirection to a Secure Web Gateway

The purpose of this function 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 a Branch Office appliance over the Internet.

One tunnel is created after you have defined the appropriate parameters in **both** ExtremeCloud SD-WAN and in Zscaler.

Create a Secure Web Gateway

1. In the **Settings -> Policy Configuration -> Security** pane, select the Secure Web Gateway tab.
2. Click **Add SWG**.
3. Enter the Name of the Secure Web gateway.
4. Enter the gateway Primary Public IP Address.
5. Enter the gateway Secondary Public IP Address. Traffic will be routed through the secondary tunnel as soon as the primary tunnel goes down.
6. Define the IPsec tunnel parameters as follows:

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)
- Authentication: integrity drop-down list to choose the data integrity hash method
- 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

- Authentication: 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]
- Enter the MTU value.
- 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) if the connected appliance public IP address is dynamic and unknown from ExtremeCloud SD-WAN. For example, 'test@myzscaler.com'.

  Note that defining an Initiator ID is irrelevant if the appliance Public IP address is static; in that case, ExtremeCloud SD-WAN uses that IP address.
- Use the IPsec Pre-Shared key field as follows:
  - If on the Zscaler Portal, the Secure Web gateway is configured with only one default Pre-Shared Key for all the tunnels connected to this gateway, enter this key in ExtremeCloud SD-WAN. Specifying a Pre-Shared key is mandatory with a Zscaler Secure Web 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 **Save Changes**.

The new Secure Web Gateway is displayed in the section of the Policy Configuration window. Click any gateway to edit its parameters. Use **View All** if you want to delete any element(s).

Apply the Secure Web Gateway to the Appliance

1 From the main menu, select **Appliances**.

2 Select the Spoke appliance and the WAN tab.

3 Select the appropriate WAN interface in Router mode and from the Security Gateway list, select the Secure Web Gateway that will establish the VPN tunnel.

4 You can define the following Tunnel Customization parameters:

- Click the Edit icon for the primary Destination.
  - 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) if the appliance public IP address is dynamic and unknown from ExtremeCloud SD-WAN. For example, 'test@myzscaler.com'.

  Note that defining an Initiator ID is irrelevant if the appliance Public IP address is static; in that case, ExtremeCloud SD-WAN uses that IP address.

  - Use the IPsec Pre-Shared key field as follows:

    If on the Secure Web 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.

    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 appliance. You can either display or hide the key.

  - Inside Local IP address of the tunnel termination interface
  - Inside Remote IP address

- Click the Edit icon for the secondary Destination and follow the same procedure as for the first Destination. The second destination is used as a backup tunnel when the primary destination fails.

5. **Save** your settings. The tunnel is created.

Configuring the Application Group Policy

From the main menu, select **Settings** to display the Policy Configuration window.

The Application Group Policy section enables you to define settings for application performance. Click **View All**.

Application Groups are listed and each AG is characterized by:

- a name,
- the applications of the Application Group,
- a Business criticality level associated with the application(s) in this Application Group,
- a QoS profile that enables QoS objectives for the application(s) in this Application Group,
- how DWS applies to this Application Group,
- the capability to be compressed,

> **Warning:** The position of the Application Groups in the list is important because it determines the classification of the packets. Classification is performed by running the list downwards. Any packet is classified with the first applicable classification met. 'other' is positioned at the bottom of the tree.

In the Application Group window, click every column for each Application Group and follow the instructions of the popup windows. Refer to "Configuring Application Groups (AGs)".

Configuring Application Groups (AGs)

Applications

Refer to "Creating Applications"

Business Criticality

In the Application Group window, click the Business Criticality column for the selected Application Group. Then select one option from the list: the higher the criticality of the flow, the more it will be protected.

QoS Profile

Refer to "Configuring QoS Profiles"

DWS Policy

Refer to "Configuring DWS Policy"

WAN Optimization

Activate the **Enabled** option to use WAN Optimization.

Adding an Application Group

1. In the Application Group window, click **Add Group.**
2. Enter the following information:
   - Application Group Name
   - Description (optional)
   - QoS Profile: select from the list one of the existing QoS profiles or create a new QoS Profile.
   - Business Criticality: select it from the list
   - WAN Optimization
3. Click **Next**.
4. **Search** for applications or create an application through the Add New Application and Add New SaaS Application functions.
5. Configure the DWS Policy.
6. Click **Add Group**. The new Application Group appears in the list of Application Groups.

Deleting an Application Group

1 Click ⋮ to delete the selected Application Group.

2 Click **Save** to validate your settings.

Creating Applications

Adding an Application

In the Application Group window, click the content of the Applications column for the selected Application Group. You can add an application in four different ways:

- searching for a recognized application in the default application dictionary
- adding a customized DPI application
- adding a SaaS application from the SaaS dictionary
- adding a customized SaaS application

A default Application Dictionary is available for each configuration. You can also access this Dictionary through **Settings -> Application Dictionary** where you can also add, modify or delete recognized applications.

The system recognizes about 200 protocols (HTTP, ICMP, FTP, RTP/RTCP, H.225, SAP, Citrix, Skype, VMware, SaaS....; refer to "Application Recognition".

> **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).

New applications can be created, described by a protocol plus an attribute, possibly on certain subnets or hosts specifically.

Adding a customized DPI Application

1 Click **Add New Application** and define the following parameters:

- Application Name
- Description
- Application Category: select it from the drop-down list
- 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

  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

   - for other protocols, no further information is required.
- Subnet Filter: this optional parameter can be used to identify an application by the IP address of a server or client, or a list of servers or clients (up to 30). It is possible to choose the server or client from a drop-down list of 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).
   - Client/Server: 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).

2 Click **Done**.

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.

Adding a SaaS Application

1 Click **Add New SaaS Application**, check **From Catalog** and select the application(s) from the dictionary list.

2 Click **Done**.

Adding a Customized SaaS Application

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 Click **Add New SaaS Application** and check **Custom Application**.

2 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.

3 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.

4 In the FQDN/Server Subnets field, enter one or several FQDN(s) and/or Server Subnet(s) separated by commas. A Fully Qualified Domain Name can be in 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.

5. You can also create a Client subnet for the new SaaS application (as for other applications) by clicking Add Subnet.

   A custom SaaS application based on IP addresses will only work for server ports 443;80;3128;8080

6. Click **Done** to validate.

> **Note:** you can also add applications from the **Settings -> Application Dictionary** window.

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).

Configuring QoS Profiles

To create a QoS Profile, click **Add Group** in the Application Group window and then **Add QoS Profile**.

To edit a QoS Profile, click the content of the QoS Profile column for the selected Application Group in the Application Group window.

The following settings 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.

- Name: to identify the QoS profile (character string)
- Description
- Type: to identify the application flow type:
  - Realtime: 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 DWS Policy

You can configure DWS Policy through the following parameters:

- Primary Network: check the favorite WAN Service(s) for this Application Group.

- Secondary Network: check the second favorite WAN Service(s) for this Application Group.
  - Performance Based (default): the Secondary Network can be selected instead of the Primary one (if the Primary Network is broken), or if the quality of this Application Group is better on the Secondary Network than on the Primary Network.
  - Backup: the Secondary Network can be selected instead of the Primary Network if this one is broken, and only in that case.
- Tertiary Network: check the last acceptable WAN Services for this Application Group. If several WAN Services are selected, then load balancing will be applied between them.
  - Performance based (default): the Tertiary Network can be selected instead of the Secondary Network if it is broken, or if the quality of this Application Group is better on the Tertiary Network than on the Secondary Network.
  - Backup: the Tertiary Network can be selected instead of the Secondary Network if this one is broken, and only in that case.
- Advanced Parameters:
  - The first two parameters, Return path and Granularity are dedicated to Advanced Users. Always call Extreme Networks Support.
  - Default Action: if no decision is made, traffic is either sent on “NAP 0” (forward) or dropped.

Creating Sites and Appliances

From the interface main menu, select **Onboard**.

Create Sites

1. Click **Add Site.**
2. Enter the Site Name, Street Address, City, State/Province, Country and Postal Code. Click **Save Site**.

   The Site is displayed on the map and the system asks you to confirm this new site. Click **Save Site**.
3. Click **Add Site** and create a second Site. Click **Save Site** twice.
4. Click **Next** to provision some appliances.

Provision Appliances

Appliance identification (for all the appliances except ipe-2200ax-T and ipe-2200ax-F)

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

The Serial Number is made of 12 characters and is indicated on the appliance chassis.

Appliance identification (only for ipe-2200ax-T and ipe-2200ax-F)

The Serial Number is made of 15 characters and is indicated on the appliance chassis.

Procedure

1. Click **Add Appliance**.
2. Enter the Serial Number of one of your appliances.
3. Assign the appliance to one Site by selecting it from the list.
4. Select from the list the appropriate Template. The listed templates are those you created previously (see "Creating Appliance Templates"). Click **Save**.
5. Repeat the procedure for a second appliance.

   > **Note:** instead of entering appliance identification data manually, you can also provision all your appliances through the Import CSV file function.
6. Click **Next - Review Configuration**. The different models of provisioned appliances are displayed with their serial numbers.

7. Click **Next - Deploy Configuration** or from the main menu, select **Appliances** to further configure your appliances.

Configuring Appliances

1. From the main menu, select **Appliances** to finish the configuration of your appliances.

   All your provisioned appliances are listed with their names, configuration statuses, assigned Sites, serial numbers and Mac addresses.

2. Select every appliance line and consecutively edit the configuration of all the appliances by entering **some remaining mandatory parameters** that are still undefined in the General, LAN and WAN panes. These parameters were not extracted from the applied template because they are specific to each appliance.

   You can notice that most parameters cannot be changed because they belong to the template. Modifying these parameters overwrites the configuration of the template and a message informs you that the current appliance is no longer associated with any template.

General

3. You can change the Appliance Name.

4. If you select another template, all default parameters are updated according to the default configuration of the new appliance template.

   All the other parameters are extracted from the applied template.

LAN

5. If you defined one or several VLAN(s) in the appliance template, enter the **VLAN Prefix Length, Management IP address and Router 1, 2, 3 IP addresses**. This information is mandatory.

6. If you activated Fabric Support, you can modify the Fabric Switch LAN and IS-IS Metric values.

   Note that you can add VLAN(s) without overwriting the appliance template.

   All the other parameters are extracted from the applied template. You can override them to configure the appliances in BGP, VRRP, OSPF, IHAP, etc.

   - VLAN

     IP Interfaces

     Fabric Switch LAN: the Fabric Switch LAN IPv4 address is used as the Fabric extend tunnel source IP address. This value is automatically generated by the system according to the Fabric Extend IP Network global subnet you defined when you activated Fabric Support. You can modify this value.

     Remote Fabric Extend Tunnel Endpoint

This set of parameters is also automatically displayed by the SD-WAN application. It specifies the Site, IP address and name of the Remote appliance. The default IS-IS Metric value is used for the Fabric-extend (FE) tunnel. Click ✎ if you want to modify this IS-IS Metric value for the local appliance as for the remote appliance.

- Dynamic LAN Routing

  iBGP protocol is used between the Core Router and the appliances of a Data Center

  OSPF protocol is used between the Core Routers and the appliances of a Data Center
- High-Availability (HA)

  VRRP protocol is used between the appliances of a Branch Office

  IHAP (Ipanema High Availability Protocol) is used between the hybrid or bridge appliances of a Branch Office
- Static Route
- Subnet

WAN

7. Consecutively select the WAN1, WAN2 and WAN3 interfaces.
8. For an interface in Bridge mode, enter the mandatory **Access Router IP Address**.
9. For an interface in Router mode, enter the data in the Optional Settings section. Refer to "Creating Appliance Templates".

IP Addresses

- **Public IP Address** which corresponds to the WAN side of the Internet Access router to which the WAN interface is connected. The Port Forwarding configuration of the Internet Access router enables this device to send the UDP packets to the appliance WAN on ports 500 (IKEv2) and 4500 (IPsec NAT Traversal). The Internet Access router also modifies the Egress packets in order to replace its public address with the WAN static address as destination address.
- If DHCP has been activated in your template, you can deactivate it in this section and enter new attributes.

10. Define and customize the network tunnels as described below.

Tunnels

Overlay (optional)

You may select an Overlay you previously created and apply it to the interface. You can also edit and customize the selected overlay from this panel. Refer to "Configuring Overlays".

- Hub & Spoke: the selected Hub & Spoke overlay name is displayed. Click **Configure Tunnel** to edit this overlay and modify any parameters. Refer to "Create a Hub & Spoke Overlay". **Update** the new configuration.
- External VPN Gateway: the name of the selected External VPN Gateway overlay is displayed. Click **Configure Tunnel** to edit this overlay and modify any parameters. Refer to "Create an External VPN Gateway Overlay". **Update** the new configuration.
- Applications Anywhere: the name of the selected Cloud Gateway overlay is displayed. Click **Configure Tunnel** to edit this overlay and modify any parameters. Refer to "Connecting an Appliance to a Cloud Gateway". **Update** the new configuration.

Security Gateway (optional)

You may select a Security Gateway you previously created and apply it to the interface. You can also edit and customize the selected gateway from this panel.

- External Secure Web Gateway: the name of the selected Secure Web Gateway is displayed. Click **Configure Tunnel** to edit this overlay and modify any parameters. Refer to "Configuring traffic redirection to a Secure Web Gateway".
- If you select EdgeSentry, there is nothing to configure. The system uses the Site address associated with the appliance to define the Cloud location where the Internet traffic should be secured and automatically creates the tunnels. Refer to "EdgeSentry".

Site-to-Site Tunnels

- Click **Add Site-to-Site Tunnel** to create a tunnel between two Sites. Select the parameter values from the field stacks and click **Add Tunnel**. Use the **Configure Tunnel** function if you want to modify the BGP Local Preference parameter or select another Overlay. **Update** the configuration.

11 When you have configured all your appliances, click **Save**.

12 Finally, click **Deploy Configuration** on the **Appliances** window to send your appliance configurations to the system.

13 From the main menu, select **Dashboard**. Your sites and associated appliances are displayed on the Google map.

Dynamic LAN Routing

BGP

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

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

1. Select BGP as the Dynamic LAN Routing Type and the **Add Peering** function.
2. Enter the IP address of the BGP local peers.
3. Activate AS Path Prepend and enter a value between [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).

   For 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. For example, by entering 2 as AS Path Prepend value, you define three AS path hops (2 + the initial one) from a Hub to a Spoke 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).
4. Select the Peer SD-WAN appliances.

OSPF

1 Select OSPF as the Dynamic LAN Routing Type.

2 Click the **VLAN** tab and add VLANs for Routers 1, 2 or 3. Each VLAN corresponds to an OSPF network area.

3 Return to the **LAN -> Dynamic LAN Routing -> OSPF** page and configure the routers as follows:

- VLAN: either select the 'None' option to take into account the ip address of the router or another VLAN ID 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.
- Cost: 10 is the default value.
- Authentication: for each router, select one authentication method. By default, there is no authentication (NONE option).
- Key: for each router, enter your authentication password.
- Key ID: for each router, enter the password identifier value. This value must match the key ID of the Core Router password.

4 Specify OSPF Advanced Settings 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. With the 0 default value, the 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: implements high availability between two 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. Note that a low cost has the priority over a higher cost.

  Metric value: this E1 value corresponds to a distance. The lowest value is the best one for routing the traffic.

  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.

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

5 Click **Save**.

High Availability (HA)

IHAP

High Availability (HA) ensures network connectivity between the Data Center or Branch Office and the remote Sites in the case of appliance failure. The objective of this deployment is to use the backup appliance if the nominal appliance fails.

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

Create a IHAP Profile

1. Select the High-Availability function and activate it.
2. Check IHAP as HA Type and click the **Add New Profile** button.
3. Type the Name of the new IHAP profile and configure it as follows:

> **Note:** A Default IHAP Profile with predefined configuration parameters is available.

- Appliance 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.
- 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 appliance and become active again.

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

Configure the SD-WAN appliances

Nominal appliance

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

> **Note:** Disable the Bypass option (enabled by default) on any WAN interface to avoid loops when the appliance reboots.

1. Select the Peer Appliance (backup appliance).
2. Select the Nominal Role and choose a Profile, either the default one or a profile you have created.

   The parameters associated with the selected IHAP Profile are displayed in read only mode.
3. **Save** your configuration.

Backup appliance

4. Select the Peer Appliance (nominal appliance).
5. Select the Backup Role and choose the same IHAP Profile as for the Nominal appliance.

   The parameters associated with the selected IHAP Profile are displayed in read only mode.
6. **Save** your configuration.

Check peering connections in the SD-WAN application

1. On the Appliances page, select each HA appliance and check its HA Status in **Advanced Troubleshooting -> Routing -> HA**.
2. If the HA configuration is not operational, check if there are any HA alarms related to the configured HA Site on the Alarms Management page.

VRRP

VRRP (Virtual Router Redundancy Protocol). This configuration is done on the LAN panel of each appliance.

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

Configure the SD-WAN appliances

Backup appliance

1. Select the High-Availability function and activate it.
2. Check VRRP as HA Type and select the VRRP Virtual router.
3. Enter a value between 1 and 255 in the Virtual Router ID field.
4. Select Backup as Initial State. This means that this appliance is used as the backup machine if its associated appliance fails.

5. Health Check; by default, all existing WAN interfaces are checked. Modify these settings if necessary.
6. **Save** your configuration.

Master appliance

Follow the same procedure as for the Backup appliance, except that Master should be selected as Initial State.

Optionally customize the VRRP Settings

> **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

IP Address allocation

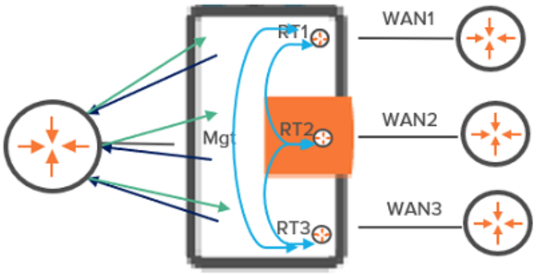
The following diagrams display SD-WAN Orchestrator manual LAN side IP address allocation with an appliance in full router, hybrid and bridge modes. All three WAN interfaces of the appliance are enabled.

You must configure these IP addresses in the SD-WAN Orchestrator.

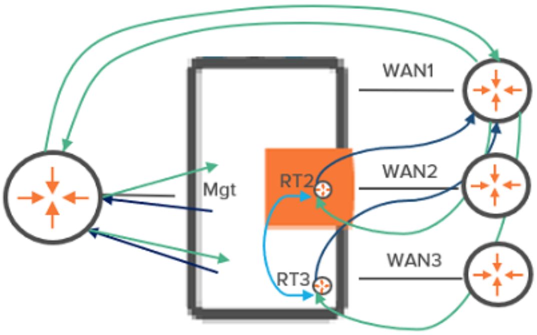
- Light blue arrows represent iBGP automatic connections
- Dark blue arrows represent iBGP connections you must configure in the SD-WAN Orchestrator
- Green arrows represent the connections you must configure on the Core Router (the SD-WAN Orchestrator is not used)

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

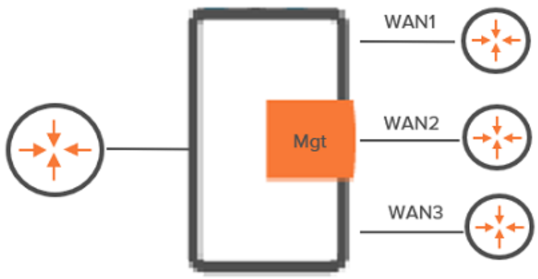
Full Router Mode



Hybrid Mode



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.

Application Dictionary

Refer to "Creating Applications".

Remote Visibility and Control

From the main menu, select **Settings -> Remote Visibility and Control** to add and manage RVC destinations.

A RVC destination means that there is no SD-WAN appliance on the related Site. ExtremeCloud SD-WAN allows traffic of an unequipped Site to be measured and controlled by the appliances of some remote equipped Sites. 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

Adding a RVC destination

1 In the General panel, enter the **Name** of the RVC destination**.**

2 Configure the LAN of the RVC destination which includes one subnet at least: click **Add Subnet** twice and enter the Subnet IP Address and Prefix Length (24).

3 Click **Done**.

4 Configure the WAN linked to the RVC destination by selecting the WAN Service from the list, if it has been already define, otherwise, create the WAN Service.

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

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

6 Optionally select an Overlay; you can also create one.

7 Validate your input by clicking **Done**.

All RVC destinations are listed in the Remote Visibility and Control list. You can enable/disable or delete them.

Cloud Access Accounts

Cloud access is the starting point for connecting your branches to your virtual private Cloud resources.

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 application helps you connect your branches to these Cloud resources if it can access the Cloud account or subscription.

1 From the main menu, select **Settings -> Cloud Access Accounts**.

The displayed window shows the number of cloud access objects that have been defined. They may be filtered by Type (AWS, Azure, etc.), Status (Active, Inactive). Without defining filters, you can group objects by Cloud Provider or Status.

- The Search field enables you to find any Cloud Access object through its other data (Account ID, User or Subscription Name).
- Use the ▼ button to filter data display. Select the appropriate elements and click **Apply Filters** to validate. You can clear the defined filters at any time.
- When the window contains a significant number of objects, the page navigation functions at the bottom of the window enable you to navigate through the list.
- Use ↻ to refresh data display.

Adding a Cloud Access object

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

Cloud Access Details

Warning: Refer to AWS Prerequisites and Azure Prerequisites.

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

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

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

- Application (client) ID: enter the Application (client) ID provided by Azure Active Directory service after the AD 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 alphanumeric 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 **Validate Account**.
4. Click **Next** to configure Cloud Access.

Configuring Cloud Access

The selected gateways will be available as overlays when you configure an appliance WAN interface or define templates. Use the Cloud Gateway List to select related Regions and define tunnel parameters.

In the Cloud Gateways selection pane, the discovered gateways are grouped by region and are identified by their name and number of connections.

- Name: Cloud Gateway name. This name identifies the Cloud account in the ExtremeCloud SD-WAN application.
- # of connections: number of Cloud Connections linked to the Cloud Gateway. A Cloud connection is counted as soon as it is configured (manually on the appliance WAN interface or automatically via a template), even if the configuration is not deployed.

By default, all the regions enabled on the AWS or Azure account are selected. Also, relevant Cloud Gateways are automatically selected whereas irrelevant gateways are greyed out (a message gives you further information).

5. Expand Regions and deselect any Region(s) if the default list does not suit you.

   The number associated with each region specifies the number of relevant Cloud Gateways under it.

6. In the VPN Tunnel Configuration pane, click **Customize Configuration** if you want to modify the default configuration of any Cloud Access object. Refer to "Configuring Overlays".

7. Click **Next**.

   A configuration summary is displayed.

8. Click **Add Account**. The new object appears in the Cloud Access Accounts window.

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

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

   - AWS
   - Azure

EdgeSentry

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 a Branch Office appliance over the Internet.

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

Prerequisites

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

- you have purchased the right licenses for both the appliance and the domain
- Extreme Networks has activated EdgeSentry for your Customer account. Select **Settings -> EdgeSentry** and verify that the EdgeSentry Status is set to 'Active'.

Configuring EdgeSentry

1. In the General panel of the Appliance Configuration window, select the appropriate WAN interface in Router mode and select EdgeSentry as the **Tunnels -> Security Gateway** value. According to the Site address where the appliance is deployed, the system will choose 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.

   Eligible interfaces are WAN Router interfaces on hybrid or full router appliances.

   > **Note:** to activate EdgeSentry on several appliances, you can also use a template where you configured this function. Refer to "Creating Appliance Templates".

2. Click **Save**.

   > **Warning:** The same WAN interface cannot be connected to EdgeSentry and to a Secure Web Gateway at the same time.

3 Select **Settings -> EdgeSentry** and connect to the Cloud Security Partner's portal by clicking **Access Check Point Infinity Portal**.

4 Configure Security Policies and Logs & Events parameters according to the procedure described in the Check Point Harmony Connect Administration Guide.

   In the Policy section, refer to the following pages:

   - Internet Access
   - Threat Prevention: a single profile, not configurable, is applied but exceptions can be defined
   - SSL Inspection
   - Policy Revisions

   Also refer to the Logs & Events section.

5 Define the traffic to forward to EdgeSentry through the wsg or wsg+ Internet Access Policies of the Zone-Based Firewall. Refer to "Setting Internet Access Control Lists".

6 Click **Save Changes** to validate the configuration.

> **Note:** provisioning a Site configured with EdgeSentry may take several minutes in Check Point.

Checking EdgeSentry Connections

1 Verify whether the EdgeSentry configuration is operational by checking that there are connected Sites on the EdgeSentry map. Note that the graphical representation of the tunnels does not contain geographic information.

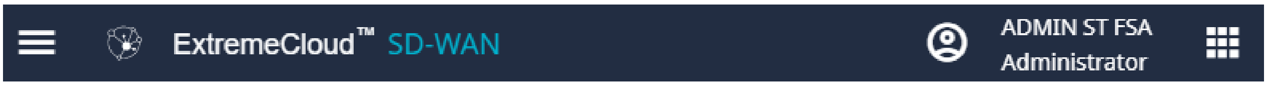
   Also check the alarms raised for the configured EdgeSentry appliance in the Active Alarms and Cleared Alarms dashboards.

2 On the Tunnels Overview dashboard, check that the EdgeSentry tunnels are up.

3 On the Appliances -> Appliance -> Advanced Troubleshooting window, select **Tunnels -> IPsec** to analyze the details of the created EdgeSentry tunnels.

4 Using the Main Menu

Use the ExtremeCloud SD-WAN vertical menu bar to access all the functions of the interface. Since this menu bar is displayed at the left of all the windows, you may easily navigate through your dashboard, onboarding, settings, sites, applications, appliances, wan, reporting and alarms pages.



Displays the dashboard which provides a graphical overview of your network and also enables you to access ExtremeCloud SD-WAN supervision functions.

Displays the Sites page for an overview of all the Sites and some detailed information for every single Site.

Enables you to onboard by creating the Network Policy, Sites and Appliances, and to deploy your network.

Displays the Applications page used for supervising applications and application flows.

Displays the Appliances page used for managing, upgrading and troubleshooting appliances.

Displays the WAN page used for supervising WAN Services.

The Reports page enables you to create and manage reports.

The Settings page enables you to configure and edit your Network Policy which is the basis of a healthy and efficient network.

Displays the Alarms Management page.

Displays on-line help.

Enables you to go back to the ExtremeCloud Apps page.

Displays the ExtremeCloud SD-WAN build and version.

ADMIN ST FSA Administrator User Name

5 Checking the Dashboard information

When you log in to ExtremeCloud SD-WAN, a Dashboard enables you to check your network at a glance. After navigating the interface windows, you can always go back to the Dashboard by clicking ⊞ in the left main menu of the application.

The system lets you know whether Fabric Support is enabled.

Connections

The Google map displays your network Sites (Hub Sites, Branch Sites, External VPN Gateways, Security Gateways, ...) all over the world with their connections.

1. Click any Site icon to view the Site summary: name, associated appliance (up or down), throughput, EQS and active alarms.
2. Click any connection line between two Sites to know if there are several tunnels and check whether they are all up or if any of them is down.
3. Click ◈ Options in the right top corner of the map to monitor connection display; either select or deselect these options (connection status, connection type, overlays).
4. Click ☰ to display the Tunnels/Connections dashboard. This dashboard lists all the connections you have configured and indicates whether they are up or down.

Quick Actions

- Onboarding Wizard
- Advanced Network Analysis
- Configure Fabric over SD-WAN

Counters

The widgets at the bottom of the dashboard display the following counters for the whole network:

- connected and disconnected appliances; click the widget header to display the Appliances page
- total number of configured sites and average throughput; click the widget header to display the Sites page
- number of DPI applications and SaaS applications with average EQS; click the widget header to display the Applications page

- number of WANs, click the widget header to display the WAN page
- number of alarms; click the widget to display the Alarms Management page

List of Tunnels/Connections

Time Range Selector and Timeline for Alerts

1. Select a Time Range period by selecting it from the list : Last Day (default), Last Week, Last Month, Custom.
2. According to the chosen time range, the Time Span selectors listed below are displayed at the right side of the Time Range Selector. Use these selectors to modify the time span of the displayed data:

   1hour, 2 hours, 4 hours, 8 hours, 24 hours, 1 day, 2 days, 7 days, 14 days, 30 days, 90 days

   You can customize the time span by defining the date and time manually.
3. A Timeline evolution graph, showing Raised, Active and Cleared Alerts curves, corresponds to the chosen Time Range. Position you cursor over any point of the evolution curves to view the number of Alerts at a specific time.
   - Click every curve label to either display or hide the curve.
   - You can either show or hide the timeline.
   - You can zoom the timeline curves by dragging your mouse over a specific time range; click Reset zoom to return to the default time settings of the curves.
4. Click ↻ to reset the chart to its default time settings (Last Day, 24 hours).
5. Click the **Notification Rules** button to configure alarm notification in order to be informed of the Critical, Warning and Information alarms that have been raised or cleared by ExtremeCloud SD-WAN.

Tunnels - Overview

The Tunnels Overview table lists your network connections. You can filter displayed data by:

- tunnel
- type of tunnel
- tunnel status (up, down or unknown)
- source site and destination site
- source appliance and destination appliance

You can clear the defined filters at any time through ⊽. Use ↻ to refresh data display.

Click ⭳ to download the table data as a `Tunnel_Data.csv` file.

Advanced Network Analysis

Time Range Selector and Timeline

1. Select a Time Range period by selecting it from the list : Last Day (default), Last Week, Last Month, Custom.
2. According to the chosen time range, the Time Span selectors listed below are displayed at the right side of the Time Range Selector. Use these selectors to modify the time span of the displayed data:

   1hour, 2 hours, 4 hours, 8 hours, 24 hours, 1 day, 2 days, 7 days, 14 days, 30 days, 90 days

   You can customize the time span by defining the date and time manually.
3. A Timeline evolution graph, showing Throughput, EQS and Raised Alerts curves, corresponds to the chosen Time Range. Position you cursor over any point of the evolution curves to view the Throughput, EQS and Raised Alerts values at a specific time.
   - Click every curve label to either display or hide the curve.
   - You can either show or hide the timeline.
   - You can zoom the timeline curves by dragging your mouse over a specific time range; click Reset zoom to return to the default time settings of the curves.
4. Click ⟳ to reset the chart to its default time settings (Last Day, 24 hours).

Insights - Counters

- Traffic with Appliances: sum of all 'With Appliance' column cell values, i.e. for all the appliances in the domain.
- Traffic with RDC: sum of all 'RVC Destination' column cell values, i.e. for all the appliances in the domain.
- Not Correlated: sum of all 'No Correlation' column cell values, i.e. for all the appliances in the domain.
- Transit Traffic: sum of all 'Transit' column cell values, i.e. for all the appliances in the domain.
- Out of Domain: sum of all 'Out of Domain' column cell values, i.e. for all the appliances in the domain.
- Locally Rerouted: sum of all 'Rerouted' column cell values, i.e. for all the appliances in the domain.
- Other: sum of all 'Other' column cell values, i.e. for all the appliances in the domain.

Domain Analysis

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.

As an advanced user, you may check that the configuration matches the network usage and identify some issues.

- Site
- Appliance Name
- With Appliance
- RVC Destination
- No Correlation: uncorrelated traffic
- Transit: traffic transiting in an appliance, not reported nor controlled
- Out of Domain: some Sites are not configured
- Locally Rerouted: are there routing issues ?
- Other: shadow IT traffic

Use the ▼ button to filter data display by Site and Appliance. Select the appropriate elements and click **Apply Filters** to validate. You can clear the defined filters at any time.

Click ⤓ to download the table data as a `Config_Troubleshoot_Metric.csv` file.

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) (locally rerouted, out of domain, no correlation, transit, with RVC destinations, with appliances, other) in both the LAN=>WAN and WAN=>LAN directions.

Configuring Fabric over SD-WAN

Appliance Configuration

This dashboard enables you to quickly check and modify the configuration of the SD-WAN appliances used with Fabric Support.

- Appliance Name
- Prefix
- Management IP Address
- Router 1, 2, 3
- Fabric Switch LAN
- Role
- Default IS-IS

Refer to "Configuring Appliances".

6 Sites

You can access the Sites page by clicking 📍 in the left main menu of ExtremeCloud SD-WAN or in the Sites widget on the Dashboard.

Time Range Selector and Timeline

These display parameters are visible at the top of all Sites windows and apply to the displayed data.

1. Select a Time Range period by selecting it from the list : Last Day (default), Last Week, Last Month, Custom.
2. According to the chosen time range, the Time Span selectors listed below are displayed at the right side of the Time Range Selector. Use these selectors to modify the time span of the displayed data:

   1hour, 2 hours, 4 hours, 8 hours, 24 hours, 1 day, 2 days, 7 days, 14 days, 30 days, 90 days

   You can customize the time span by defining the date and time manually.
3. A Timeline evolution graph, showing Throughput, EQS and Raised Alerts curves, corresponds to the chosen Time Range. Position you cursor over any point of the evolution curves to view the Throughput, EQS and Raised Alerts values at a specific time.
   - Click every curve label to either display or hide the curve.
   - You can either show or hide the timeline.
   - You can zoom the timeline curves by dragging your mouse over a specific time range; click Reset zoom to return to the default time settings of the curves.
4. Click ⟳ to reset Sites windows to their default time settings (Last Day, 24 hours).

The Sites page displays an Overview table.

By clicking any Site line in the Overview table, you can view detailed information for this single Site through three tabs:

- Overview
- Site Performance
- Flows

All Sites Overview

The View EQS Direction dashboard contains, for the LAN -> WAN and WAN -> LAN directions, the following information for all the Sites:

- Site/Appliance/WAN interface: name of the Site, associated appliance, WAN interface. 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:
    - throughput
    - capacity: WAN access throughput (max BW),
    - utilization: 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.
- You can download the EQS Direction data as a `Site_Overview.csv` file.
- Click any Site name to display detailed information about this selected Site.

This dashboard is automatically refreshed every minute (or every 5 or 15 minutes).

Single Site

By clicking any Site line in the All Sites Overview table, you can view detailed information for this single Site through three tabs:

- Overview
- Site Performance
- Flows

Single Site Overview

The Overview dashboard for one selected Site displays the following charts:

- Lowest 10 EQS per Application and Application Group (bar chart)
- Top 10 Volume per Application and Application Group (bar chart)
- Throughput per Application Group, Criticality, Top 10 Applications (line chart)
- EQS per Application Group, Criticality, Worst 10 Applications (line chart)
- Throughput and EQS per WAN Service (line chart)
- Table of WAN Services (table)

The Overview dashboard is an overview of EQS, Volume and Throughput per Application/Application Group/Criticality/Top 10 Applications/Worst 10 Applications/WAN Service for the selected Site during the last 24 hours (default time range of this dashboard).

- Use the ▼ button to filter data display by Destination Site, Local WAN Service, Destination WAN Service, Application, Application Group, Criticality and Flows Direction. Select the appropriate elements and click **Apply Filters** to validate. You can clear the defined filters at any time.
- For each chart, click **View Summary** to display the matching Summary table. You can sort displayed data by Applications, Application Groups and Criticality.
  - Use ↻ to refresh data display.
  - Click ⤓ to download the Summary table as an `Application-Summary.csv` file or a `Wan_Overview_Data.csv` file.

Site Performance

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, Application Group, Criticality, Destination Site, Source WAN Service, Destination WAN Service and Flows Direction during the selected time range.

For a definition of these metrics, refer to Applications -> Applications Flows.

Application Flows

This dashboard shows the same information as in the Applications -> Application Flows table, but for the selected Site.

7 Applications

You can access the Applications page by clicking in the left main menu of ExtremeCloud SD-WAN or in the Applications widget on the Dashboard.

Time Range Selector and Timeline

These display parameters are visible at the top of all Applications windows and apply to the displayed data.

1. Select a Time Range period by selecting it from the list : Last Day (default), Last Week, Last Month, Custom.
2. According to the chosen time range, the Time Span selectors listed below are displayed at the right side of the Time Range Selector. Use these selectors to modify the time span of the displayed data:

   1hour, 2 hours, 4 hours, 8 hours, 24 hours, 1 day, 2 days, 7 days, 14 days, 30 days, 90 days

   You can customize the time span by defining the date and time manually.
3. A Timeline evolution graph, showing Throughput, EQS and Raised Alerts curves, corresponds to the chosen Time Range. Position you cursor over any point of the evolution curves to view the Throughput, EQS and Raised Alerts values at a specific time.
   - Click every curve label to either display or hide the curve.
   - You can either show or hide the timeline.
   - You can zoom the timeline curves by dragging your mouse over a specific time range; click Reset zoom to return to the default time settings of the curves.
4. Click ↻ to reset Applications windows to their default time settings (Last Day, 24 hours).

The Applications page contains three tabs:

- Overview
- SaaS Applications
- Application Flows

Overview

The Applications -> Overview dashboard displays the following graphs:

- Lowest 10 EQS per Application and Application Group (bar chart)
- Top 10 Volume per Application and Application Group (bar chart)
- Throughput per Application Group, Criticality, Top 10 Applications (line chart)
- EQS per Application Group, Criticality, Worst 10 Applications (line chart)

The Overview dashboard is an overview of EQS, Volume and Throughput per Application/Application Group/Criticality/Top 10 Applications/Worst 10 Applications during the last 24 hours (default time range of this dashboard).

- Use the ▼ button to filter data display by Source Site, Destination Site, Source WAN Service or Destination WAN Service. Select the appropriate elements and click **Apply Filters** to validate. You can clear the defined filters at any time.
- For each chart, click **View Summary** to display the matching Summary table. You can sort displayed data by Applications, Application Groups and Criticality.
    - Use ↻ to refresh data display.
    - Click ⤓ to download the Summary table as an `Application-Summary.csv` file.

SaaS Applications

This dashboard displays the list of the most common SaaS applications discovered on the network over the selected period.

After you have defined the Time Range of the displayed list, this list is automatically refreshed.

For each SaaS application, the category, number of Sites, active sessions and approximate volume is given.

Click ▼ to filter SaaS application by Source Site.

Provisioning a SaaS Application

1. From the view list, click 📦 for the SaaS application you want to provision.
2. Check the Enabled status to activate the application.
3. From the stack of already defined Application Groups, select one AG the current application will be assigned to.
4. Click **Done**.

   The SaaS application is now displayed without the 📦 icon.
5. Go to Settings -> Application Dictionary and check that the Status of the SaaS application is Active.

Application Flows

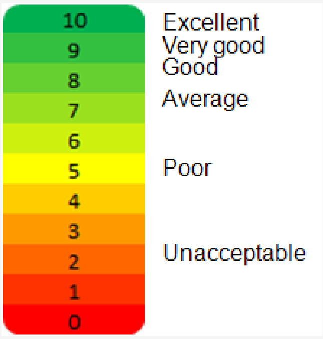
The top of the dashboard contains four filters (Local Site, Remote Site, Application Group and Application) and the rest of the dashboard displays the detailed flows list and a real-time graph.

The displayed information matches the selected filters (all the flows if no filter was selected).

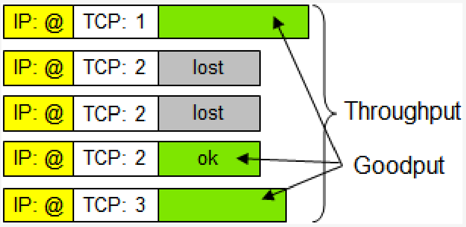
The flows list shows a table with each active flow displayed on a separate line. A flow becomes active and is displayed in the window as soon as a packet belonging to it is detected during the session.

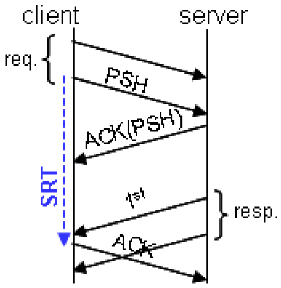
You may sort the data by clicking on the column headers: click once to sort the data incrementally (an up arrow then appears next to the header), click again to sort the data in the reverse order. When a filter is applied, the other filters are updated accordingly.

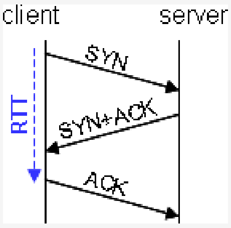
The table contains the following columns:

Topology	
Local Site/App/WAN	Name of the local Site, name of the Appliance, number of WANs
Direction	Direction of the flow: outgoing (the local Site is the source) or incoming (the local Site is the destination)
Remote Site/App/WAN	Name of the remote Site, name of the Appliance (where the flow is going to or coming from), number of WANs
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 specifies the quality level, with the following meaning:  10 9 8 7 6 5 4 3 2 1 0 Excellent Very good Good Average Poor Unacceptable

	Note: Excellent, Very good, etc., correspond to a *typical* interpretation of the EQS with *typical* parameters. It may vary according to the users' sensitivity 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 parameter objectives were not met (yellow) or which parameter maximum values were exceeded (red). 100 is a reserved value used when the EQS cannot be computed. The quality of a flow cannot be calculated when all the three following conditions are met: • it is a real time flow (the bandwidth is not a criterion) 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	
Throughput (kbps)	LAN throughput (number of bits per second sent at the IP layer level) 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 TCP: 2 lost lost ok TCP: 3 Throughput Goodput
Sessions	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	
Throughput (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)
Compression	
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; 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 directions 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; 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 directions 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
Retransmission (%)	Percentage of TCP retransmissions
Compression	Compression status: Yes if the flow is compressed, No otherwise
Actions	Click 📊 to display the real-time graph of the selected flow. Refer to "Real Time Graphs".

This dashboard is refreshed about every minute (according to the Appliance collect period option).

Real Time Graphs

From any flow in the Application Flows table 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.

Note: Pop-up windows must not be blocked in your web browser.

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 loss
	Avg. sessions	Average number of sessions

Tab	Graphs	What is shown
	Throughput (kbps)	LAN-to-LAN (in blue) and WAN-to-WAN (in orange) throughput
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) throughput
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 throughput

Note: In case of control and/or compression, the differences between LAN and WAN values may be very different.

8 Appliances

You can access the Appliances page by clicking 🖥 in the left main menu of ExtremeCloud SD-WAN or in the Appliances widget on the Dashboard.

Overview

The Overview dashboard displays the appliances of your network with the following column information:

- Appliances: name of the appliance
- Site: associated site
- Status: connected or disconnected in the network
- Fabric LLDP Signaling: LLDP including Fabric Extend TLVs is received or not (due to missing configuration, LLDP exception, etc.). Only appears if Fabric Support is enabled.
- Configuration Status
- Serial Number
- Firmware: build number
- Management IP: Management IP address
- Template: associated template
- Last update: date when the appliance was updated
- Action: enables you to delete the appliance

Note that you can sort appliances by clicking each column header. Also use:

- ≡ to auto-size the current column or all columns. Pinning the selected column displays it in a separate part of the table
- ▥ to search, add or remove parameter columns

Appliance Details

In the Overview table, click the **Appliance Name**.

- The left pane of the window is a summary of the appliance configuration and policy. You can edit both of them. Refer to "Configuring Appliances", "Creating Appliance Templates", "Configuring the Network Policy"
- The Fabric Support summary contains Fabric Switch information and status as well as Peering information. It also enables you to display the corresponding Fabric Engine page in ExtremeCloud IQ Site Engine.
  - Click the **Peers** link to display The Peering Status table.

  This table enables you to monitor the state of Vxlan tunnels (Fabric Extend tunnels) thanks to the Remote SD-WAN Appliance name, GRE/IPSEC aggregated state, Fabric Switch name and IS-IS adjacency state without using any other tool such as ExtremeCloud IQ Site Engine.

  - Click the **XIQSE** link under Managed by -> Application to display the appropriate Device page of ExtremeCloud IQ Site Engine. Refer to the Devices section of the ExtremeCloud IQ Site Engine User Guide.

- The Appliance Connections are shown on the map with the number of existing alarms. Click the Alarms widget to view alarm details. Refer to "Alarms Management"
  - Click the **Summary** button to display the connection details, i.e. the overlays with their status (up or down), their destination site and destination appliance/interface. You can download this information as a `Connectionlist_Data.csv` file.
- Refer to the following sections for a complete description of the functions:
  - Run Scripts
  - Upgrade
  - Advanced Troubleshooting

In the Overview table, click the **Site Name** associated with each appliance. Refer to "Sites".

Upgrade

In the top right corner of the Appliance Details page, click **Upgrade**.

1. You can choose to upgrade the appliance to the latest firmware version which is specified, or to a specific version you can select from the stack.
2. Either select immediate activation or schedule the activation by specifying a date and time.
3. Click **Upgrade Device**.

Advanced Troubleshooting

In the top right corner of the Appliance Details page, click **Advanced Troubleshooting**.

This window is divided into four sections/tabs that enable you 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 in the left margin of the window.

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.

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 ⟳ 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.

  An additional table contains IPsec Log entries. Log data are collected every 5s.

Routing

The Routing section contains several sub-tabs: Routes, OSPF, VRRP, HA, ARP, LLDP 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 ↻ in the top right corner of the window.

- The Local/Router Routing tables lists the IP routes between Sites.
- The VRRP table data let you know whether your VRRP configurations (if any) are working or not. Refer to "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 "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 "IHAP".
- The ARP Cache displays all necessary data.

- The LLDP tab displays information sent and received from the LLDP Neighbor and lets you know whether the LLDP features are working properly. This tab only appears if Fabric Support is enabled.
- The Logs table displays BIRD logs.

Run Scripts

In the top right corner of the Appliance Details page, click **Run Scripts**.

1. For the selected appliance, select the Script from the list.
2. Click **Execute Now** to launch the script.
3. Click ↻ to refresh the Execution details list and display the executed script.
4. You can delete the script through 🗑 or download the script as an `ExecutionScriptResult.zip` file.

You can send this zip file to Extreme Networks Support.

9 WAN

You can access the WAN page by clicking ≋ in the left main menu of ExtremeCloud SD-WAN or in the WAN widget on the Dashboard.

Time Range Selector and Timeline

These display parameters are visible at the top of the WAN page and apply to the displayed data.

1. Select a Time Range period by selecting it from the list : Last Day (default), Last Week, Last Month, Custom.
2. According to the chosen time range, the Time Span selectors listed below are displayed at the right side of the Time Range Selector. Use these selectors to modify the time span of the displayed data:

   1hour, 2 hours, 4 hours, 8 hours, 24 hours, 1 day, 2 days, 7 days, 14 days, 30 days, 90 days

   You can customize the time span by defining the date and time manually.
3. A Timeline evolution graph, showing Throughput, EQS and Raised Alerts curves, corresponds to the chosen Time Range. Position you cursor over any point of the evolution curves to view the Throughput, EQS and Raised Alerts values at a specific time.
   - Click every curve label to either display or hide the curve.
   - You can either show or hide the timeline.
   - You can zoom the timeline curves by dragging your mouse over a specific time range; click Reset zoom to return to the default time settings of the curves.
4. Click ↻ to reset the WAN page to its default time settings (Last Day, 24 hours).

Overview

The WAN -> Overview dashboard is an overview of Throughput and EQS per WAN Service during the last 24 hours (default time range of this dashboard). It displays the following graphs:

- Throughput and EQS per WAN Service (bar chart and line chart)

WAN Services

This table lists the WAN Services of your network with the traffic metrics explained in "Application Flows".

- Use the ▼ button to filter data display by Source Site, Destination Site, Source WAN Service or Destination WAN Service, Application, Application Group, Criticality and Source WAN Interface. Select the appropriate elements and click **Apply Filters** to validate. You can clear the defined filters at any time.
- Click 🔍 to search for a specific element.
- Click ⤓ to download the table data as a `Wan_Overview_Data.csv` file.

Networks

This dashboard contains outbound and inbound traffic EQS and availability metrics you need to troubleshoot any issues occurring on your WAN Services.

Meaning of some symbols and metrics

Outbound	Outbound represents the direction of the flow(s) in relation to a selected Site, i.e. coming from its LAN and going to its WAN (alias LAN => WAN or ingress or upload)
Inbound	Inbound represents the direction of the flow(s) in relation to a selected Site, i.e. coming from its WAN and going to its LAN (alias WAN => LAN, or egress or download)

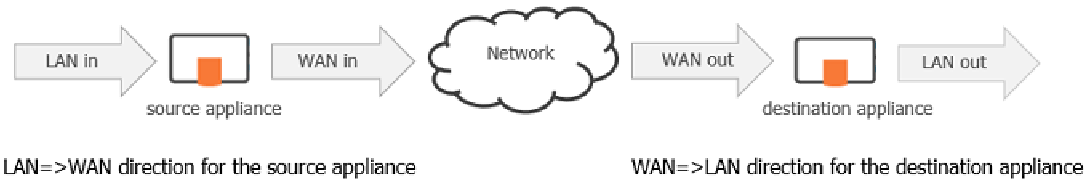
LAN and WAN Metrics

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 in
source appliance
WAN in
Network
WAN out
destination appliance
LAN out
LAN=>WAN direction for the source appliance
WAN=>LAN direction for the destination appliance

10 Reports & Templates

You can access the Reports & Templates page by clicking 📊 in the left main menu of the interface. This page contains the Reports and Templates tabs. Since a report always uses a graphical content template, create the template first.

Creating Templates

1 Select the Templates tab.

2 Click Create Template

3 Enter the Template Name and an optional Description.

4 Select the Widgets to be included in your template. The available categories are Application Overview, SaaS Applications, Site Overview and WAN Overview.

For each category, select any widget(s) from the list and validate through **Create Template**.

> **Note:** there are two predefined templates, Application Overview and Site Overview, that you can use right away without creating any new template if their graphical content suits your needs.

Viewing Generated Templates

All your created templates and the two predefined templates are listed with the following information:

- Template Name
- Template Usage: specifies the number of reports using the template
- Last Modified On: creation or modification date and time
- Actions: you can
  - clone (⧉) all the templates to create new templates
  - delete (🗑) the templates you have created. The predefined templates provided by ExtremeCloud SD-WAN cannot be deleted
  - edit (✎) the templates you have created. The predefined templates provided by ExtremeCloud SD-WAN cannot be modified

Use ⟳ to refresh data display.

Click ⤓ to download the Templates data as a `Template_Overview.csv` file.

Creating Reports

1 Select the Reports tab.

2 Click Create Report and **Continue** in the Create Report Flow wizard.

3 Enter the Report Name and an optional Description.

4 Select a template from the list. Its associated widgets are automatically specified.

5 For each category of report widgets, you can define filters by clicking the ▼ button. Data display may be filtered by Source Site, Destination Site, Source WAN Service, Destination WAN Service, etc. Select the appropriate elements and click **Apply Filters** to validate. You can clear the defined filters at any time.

6 Click **Next - Report Schedule** in the wizard. You can choose to create the report immediately or to schedule it.

If you select 'Create now':

- select the Data Range: last 24 hours, yesterday, last week, last month or Custom Range

  If you select Custom Range, manually pick your report date/time range.

If you select 'Schedule for later':

- select the Data Range: daily, weekly or monthly
- select the Report Frequency

> **Note:** you can edit a scheduled report at any time.

7 You may optionally use email notification by adding recipients.

8 The only available format is PDF.

9 Click **Next - Report Summary** in the wizard and check your report configuration.

10 Validate with **Create Report**.

Viewing Generated Reports

All the report executions are listed. When the PDF report is available, it is displayed on a sub-line with the following information:

- Schedule Type: displays 'Once' for a report created immediately or displays the report frequency for a scheduled (repeated) report
- Report Generated Time: creation date and time of the generated report
- Status:
  - report definition: 'Inactive' for Once reports and for Repeated reports where scheduling is deactivated
  - generated report: 'Report Generated' or 'Report Generation failed'

- Actions: you can
  - download (⤓) all the generated reports
  - delete (🗑) all the reports (already generated or not)
  - edit (✎) scheduled reports

11 Alarms Management

You can access the Alarms Management page by clicking 🔔 in the left main menu of ExtremeCloud SD-WAN or in the Alarms widget on the Dashboard.

Time Range Selector and Timeline

These display parameters are visible at the top of all Alarms windows and apply to the displayed data.

1. Select a Time Range period by selecting it from the list : Last Day (default), Last Week, Last Month, Custom.
2. According to the chosen time range, the Time Span selectors listed below are displayed at the right side of the Time Range Selector. Use these selectors to modify the time span of the displayed data:

   1hour, 2 hours, 4 hours, 8 hours, 24 hours, 1 day, 2 days, 7 days, 14 days, 30 days, 90 days

   You can customize the time span by defining the date and time manually.
3. A Timeline evolution graph, showing curves for Raised, Active and Cleared alarms, corresponds to the chosen Time Range. Position you cursor over any point of the evolution curves to view the number of alarms at a specific time.
   - You may display or hide the evolution curve of each type of alarm separately by clicking the category label in the graph legend.
   - You can either show or hide the timeline.
   - 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. Click Reset zoom to return to the default time settings of the curves.
4. Click ↻ to reset Alarms windows to their default time settings (Last Day, 24 hours).

Alarm Dashboards

The Alarms Management page contains two tabs to display Active and Cleared Alarms dashboards.

It also enables you to configure alarm notifications rules.

Active Alarms

This dashboard displays the active Critical, Major and Minor alarms, i.e. their status is still 'raised' at the time specified by the time range. You may filter these alarms by:

- severity
- category
  - 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 components (Orchestrator, etc.)
- alarm
- local site
- local appliance: first appliance in the case of tunnel failure or end-to-end connectivity lost issue
- remote site
- remote appliance: second appliance in the case of tunnel failure or end-to-end connectivity lost issue

You can clear the defined filters at any time through .

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 Major and grey for Minor. The raised time for each alarm is specified.

You may sort column data by clicking the column header names.

- Click 🔍 to search for specific alarms.
- Use ↻ to refresh data display.
- Click ⤓ to download the Active Alarms dashboard as an `Active_Alarms_Data.csv` file.

Cleared Alarms

The Cleared Alarms dashboard contains the same filters as the Active Alarms dashboard.

For each alarm, both Raised Time and Cleared Time are specified.

Configuring Alarm Notification

At any time, to be informed of the Critical, Major and Minor alarms that have been raised or cleared by ExtremeCloud SD-WAN without displaying the Active Alarms dashboard, you may configure alarm notification through the **Notification Rules** function.

> **Note:** This function is only available to the Administrator and Network Manager profiles.

Set an Alarm Notification Rule

1. Click the Notification Rules button at the top of the Alarms page.
2. Click Add Rule
3. Enter the Name of the Notification Rule.
4. From the Category 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 components (Orchestrator, etc.)
   - All: all the categories are taken into account
5. 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.
6. From the Severity stack of values, define the type of alarm (minor, major and critical) which must trigger the notification messages.
7. Enter the email address of one or several Recipients. All the recipients will be notified of this alarm by email.
8. Finally, click **Create**.

   The new Notification Rule appears in the Notification Rule Details table with its parameters.

   - You can deactivate the Notification Rule by modifying the State option.

- Click ⤓ to download the table of Notification Rules as an `Alarm_Notification_Data.csv` file.
- Click 🗑 to delete any Notification Rule.

Alarms by Category

The table below lists the ExtremeCloud SD-WAN alarms by category and briefly describes the recovery procedure to use when an alarm condition occurs.

As a reminder, categories 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 components

Underlay

Alarm	Severity	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	Minor	Status change alarm.
HA state change	Minor	Status change alarm.
Configuration mismatch	Critical	There is a configuration version mismatch between the SD-WAN application and the appliances. Contact ExtremeCloud SD-WAN Support.
HA Configuration mismatch	Critical	Check the Alarms window to identify the issue. Check the Routing section of the Troubleshooting window (Appliances -> Advanced Troubleshooting) and verify

Alarm	Severity	Troubleshooting
		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	Severity	Troubleshooting
Disconnected from the overlay	Major	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 Alarms window to identify the issue. Check the Tunnels/Connections supervision table you access from the main Dashboard and verify the state of the GRE/IPsec tunnels. Fix your appliance configuration.
External tunnel failure (External Gateway)	Critical	Check that the definition of the External VPN Gateway and the configuration of tunnels match the configuration of the remote VPN gateway the appliance tries to connect to.
EdgeSentry authentication failure	Critical	The SD-WAN application is not able to authenticate in Check Point's Harmony Connect service. Contact ExtremeCloud SD-WAN Support.
EdgeSentry configuration failure	Major/Critical	May be raised when the definition of a site cannot be created or updated in Harmony Connect. Contact ExtremeCloud SD-WAN Support.

Alarm	Severity	Troubleshooting
Harmony Connect failure	Critical	A site in Check Point Harmony Connect is in failure. Contact ExtremeCloud SD-WAN Support.
LAN BGP peering failure	Major	Check the Local Peer IP address in the LAN and the Site AS number.
Connection to AWS failure	Major/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	Major/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 connection failure	Critical	Check that the cloud gateway still exists and prerequisites are met.
Invalid Credentials	Critical	Check the Cloud Access definition and contact your cloud account administrator.
Cloud connection cannot be created	Major/Critical	Check the Cloud Access definition and contact your cloud account administrator.
Cloud connection cannot be modified	Major/Critical	Check that the cloud gateway still exists and prerequisites are met.
Cloud connection cannot be deleted	Major/Critical	Check that the cloud gateway still exists and prerequisites are met.
IS-IS adjacency lost	Critical	May be raised when no IS-IS adjacency is detected by the LLDP TLV 127 subtype 7 received from the SD-WAN appliances. Check the IS-IS adjacency state on the neighbor switch and contact

Alarm	Severity	Troubleshooting
		ExtremeCloud SD-WAN Support.
LLDP neighbor disappears	Critical	May be raised when a LLDP neighbor disappears (detected by the absence of LLDP frames received from an SD-WAN appliance). Check the LLDP tx status on the neighbor switch and contact ExtremeCloud SD-WAN Support.

Services

Alarm	Severity	Troubleshooting
Visibility down	Major	Contact ExtremeCloud SD-WAN Support.
Control down	Major	Contact ExtremeCloud SD-WAN Support.
WAN Optimization down	Major	Contact ExtremeCloud SD-WAN Support.
Synchronization lost	Major	Contact ExtremeCloud SD-WAN Support.
DTI traffic overload	Major	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	Major	Check network connectivity between the SYSLOG server and the appliance.

EQS

Alarm	Severity	Troubleshooting
Site EQS for Top Applications dropped below 5	Major	The alarm is cleared when this value increases.
Site EQS for High Applications dropped below 5	Major	The alarm is cleared when this value increases.
End-to-end connectivity lost	Major	Check end-to-end connectivity between Site A and Site B for the specified WAN Service (broken NAP).

Resources

Alarm	Severity	Troubleshooting
Disk is almost full (<5% left) on the volume [volume name]	Major	For hardware resource alarms, contact ExtremeCloud SD-WAN Support.
Disk failure	Major	
Reboot	Minor	
Traffic overload	Major	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	Severity	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	Major	One or several SD-WAN platform components are disconnected (either never connected or not recently connected) from ZTP (Zero Touch Provisioning server). Contact ExtremeCloud SD-WAN Support.