Purview Deployment Guide

PN: 9034969

Legal Notices

Extreme Networks, Inc., on behalf of or through its wholly-owned subsidiary, Enterasys Networks, Inc., reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see: www.extremenetworks.com/company/legal/trademarks/

Support

For product support, including documentation, visit: www.extremenetworks.com/support/

Contact

Extreme Networks, Inc.
145 Rio Robles
San Jose, CA 19534

Tel: +1 408-579-2800
Toll-free: +1 888-257-3000

Software License Agreement

This document is an agreement ("Agreement") between You, the end user, and Enterasys Networks, Inc., ("Enterasys") a wholly owned subsidiary of Extreme Networks, Inc., on behalf of itself and its Affiliates (as hereinafter defined) that sets forth your rights and obligations with respect to the Licensed Software.

BY INSTALLING THE LICENSE KEY FOR THE SOFTWARE ("License Key"), COPYING, OR OTHERWISE USING THE LICENSED SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE LICENSE KEY TO ENTERASYS OR YOUR DEALER, IF ANY, OR DO NOT USE THE LICENSED SOFTWARE AND CONTACT ENTERASYS OR YOUR DEALER WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A REFUND. IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT LegalTeam@extremenetworks.

1. DEFINITIONS. "Affiliates" means any person, partnership, corporation, limited liability company, or other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. "Server Application" shall refer to the License Key for software installed on one or more of Your servers. "Client Application" shall refer to the application to access the Server Application. "Licensed Materials" shall collectively refer to the licensed software (including the Server Application and Client Application), Firmware, media embodying the software, and the documentation. "Concurrent User" shall refer to any of Your individual employees who You provide access to the Server Application at any one time. "Firmware" refers to any software program or code imbedded in chips or other media. "Licensed Software" refers to the Software and Firmware collectively.

2. TERM. This Agreement is effective from the date on which You install the License Key, use the Licensed Software, or a Concurrent User accesses the Server Application. You may terminate the Agreement at any time by destroying the Licensed Materials, together with all copies, modifications and merged portions in any form. The Agreement and Your license to use the Licensed Materials will also terminate if You fail to comply with any term of condition herein.

3. GRANT OF SOFTWARE LICENSE. Enterasys will grant You a non- transferable, non-exclusive license to use the machine-readable form of the Licensed Software and the accompanying documentation if You agree to the terms and conditions of this Agreement. You may install and use the Licensed Software as permitted by the license type purchased as described below in License Types. The license type purchased is specified on the invoice issued to You by Enterasys or Your dealer, if any. YOU MAY NOT USE, COPY, OR MODIFY THE LICENSED MATERIALS, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT.

4. LICENSE TYPES.
   - *Single User, Single Computer*. Under the terms of the Single User, Single Computer license, the license granted to You by Enterasys when You install the License Key authorizes You to use the Licensed Software on any one, single computer only, or any replacement for that computer, for internal use only. A separate license, under a separate Software License Agreement, is required for any other computer on which You or another individual or employee intend to use the Licensed Software. A separate license under a separate Software License Agreement is also required if You wish to use a Client license (as described below).

- *Client*. Under the terms of the Client license, the license granted to You by Enterasys will authorize You to install the License Key for the Licensed Software on your server and allow the specific number of Concurrent Users shown on the relevant invoice issued to You for each Concurrent User that You order from Enterasys or Your dealer, if any, to access the Server Application. A separate license is required for each additional Concurrent User.

5. AUDIT RIGHTS. You agree that Enterasys may audit Your use of the Licensed Materials for compliance with these terms and Your License Type at any time, upon reasonable notice. In the event that such audit reveals any use of the Licensed Materials by You other than in full compliance with the license granted and the terms of this Agreement, You shall reimburse Enterasys for all reasonable expenses related to such audit in addition to any other liabilities You may incur as a result of such non-compliance, including but not limited to additional fees for Concurrent Users over and above those specifically granted to You. From time to time, the Licensed Software will upload information about the Licensed Software and the associated devices to Enterasys. This is to verify the Licensed Software is being used with a valid license. By using the Licensed Software, you consent to the transmission of this information. Under no circumstances, however, would Enterasys employ any such measure to interfere with your normal and permitted operation of the Products, even in the event of a contractual dispute.

6. RESTRICTION AGAINST COPYING OR MODIFYING LICENSED MATERIALS. Except as expressly permitted in this Agreement, You may not copy or otherwise reproduce the Licensed Materials. In no event does the limited copying or reproduction permitted under this Agreement include the right to decompile, disassemble, electronically transfer, or reverse engineer the Licensed Software, or to translate the Licensed Software into another computer language.

   The media embodying the Licensed Software may be copied by You, in whole or in part, into printed or machine readable form, in sufficient numbers only for backup or archival purposes, or to replace a worn or defective copy. However, You agree not to have more than two (2) copies of the Licensed Software in whole or in part, including the original media, in your possession for said purposes without Enterasys' prior written consent, and in no event shall You operate more copies of the Licensed Software than the specific licenses granted to You. You may not copy or reproduce the documentation. You agree to maintain appropriate records of the location of the original media and all copies of the Licensed Software, in whole or in part, made by You. You may modify the machine-readable form of the Licensed Software for (1) your own internal use or (2) to merge the Licensed Software into other program material to form a modular work for your own use, provided that such work remains modular, but on termination of this Agreement, You are required to completely remove the Licensed Software from any such modular work. Any portion of the Licensed Software included in any such modular work shall be used only on a single computer for internal purposes and shall remain subject to all the terms and conditions of this Agreement. You agree to include any copyright or other proprietary notice set forth on the label of the media embodying the Licensed Software on any copy of the Licensed Software in any form, in whole or in part, or on any modification of the Licensed Software or any such modular work containing the Licensed Software or any part thereof.

7. TITLE AND PROPRIETARY RIGHTS
   a. The Licensed Materials are copyrighted works and are the sole and exclusive property of Enterasys, any company or a division thereof which Enterasys controls or is controlled by, or which may result from the merger or consolidation with Enterasys (its "Affiliates"), and/or their suppliers. This Agreement conveys a limited right to operate the Licensed Materials and shall not be construed to convey title to the Licensed Materials to You. There are no implied rights. You shall not sell, lease, transfer, sublicense, dispose of, or otherwise make available the Licensed Materials or any portion thereof, to any other party.
   b. You further acknowledge that in the event of a breach of this Agreement, Enterasys shall suffer severe and irreparable damages for which monetary compensation alone will be inadequate. You therefore agree that in the event of a breach of this Agreement, Enterasys shall be entitled to monetary damages and its reasonable attorney's fees and costs in enforcing this

Agreement, as well as injunctive relief to restrain such breach, in addition to any other remedies available to Enterasys.

8. PROTECTION AND SECURITY. In the performance of this Agreement or in contemplation thereof, You and your employees and agents may have access to private or confidential information owned or controlled by Enterasys relating to the Licensed Materials supplied hereunder including, but not limited to, product specifications and schematics, and such information may contain proprietary details and disclosures. All information and data so acquired by You or your employees or agents under this Agreement or in contemplation hereof shall be and shall remain Enterasys' exclusive property, and You shall use your best efforts (which in any event shall not be less than the efforts You take to ensure the confidentiality of your own proprietary and other confidential information) to keep, and have your employees and agents keep, any and all such information and data confidential, and shall not copy, publish, or disclose it to others, without Enterasys' prior written approval, and shall return such information and data to Enterasys at its request. Nothing herein shall limit your use or dissemination of information not actually derived from Enterasys or of information which has been or subsequently is made public by Enterasys, or a third party having authority to do so.

   You agree not to deliver or otherwise make available the Licensed Materials or any part thereof, including without limitation the object or source code (if provided) of the Licensed Software, to any party other than Enterasys or its employees, except for purposes specifically related to your use of the Licensed Software on a single computer as expressly provided in this Agreement, without the prior written consent of Enterasys. You agree to use your best efforts and take all reasonable steps to safeguard the Licensed Materials to ensure that no unauthorized personnel shall have access thereto and that no unauthorized copy, publication, disclosure, or distribution, in whole or in part, in any form shall be made, and You agree to notify Enterasys of any unauthorized use thereof. You acknowledge that the Licensed Materials contain valuable confidential information and trade secrets, and that unauthorized use, copying and/or disclosure thereof are harmful to Enterasys or its Affiliates and/or its/their software suppliers.

9. MAINTENANCE AND UPDATES. Updates and certain maintenance and support services, if any, shall be provided to You pursuant to the terms of an Enterasys Service and Maintenance Agreement, if Enterasys and You enter into such an agreement. Except as specifically set forth in such agreement, Enterasys shall not be under any obligation to provide Software Updates, modifications, or enhancements, or Software maintenance and support services to You.

10. DEFAULT AND TERMINATION. In the event that You shall fail to keep, observe, or perform any obligation under this Agreement, including a failure to pay any sums due to Enterasys, or in the event that you become insolvent or seek protection, voluntarily or involuntarily, under any bankruptcy law, Enterasys may, in addition to any other remedies it may have under law, terminate the License and any other agreements between Enterasys and You.
    a. Immediately after any termination of the Agreement or if You have for any reason discontinued use of Software, You shall return to Enterasys the original and any copies of the Licensed Materials and remove the Licensed Software from any modular works made pursuant to Section 3, and certify in writing that through your best efforts and to the best of your knowledge the original and all copies of the terminated or discontinued Licensed Materials have been returned to Enterasys.
    b. Sections 1, 7, 8, 10, 11, 12, 13, 14 and 15 shall survive termination of this Agreement for any reason.

11. EXPORT REQUIREMENTS. You are advised that the Software is of United States origin and subject to United States Export Administration Regulations; diversion contrary to United States law and regulation is prohibited. You agree not to directly or indirectly export, import or transmit the Software to any country, end user or for any Use that is prohibited by applicable United States regulation or statute (including but not limited to those countries embargoed from time to time by the United States government); or contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or Use.

12. UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The Licensed Materials (i) were developed solely at private expense; (ii) contain "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Enterasys and/or its suppliers. For Department of Defense units, the Licensed Materials are considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth herein.

13. LIMITED WARRANTY AND LIMITATION OF LIABILITY. The only warranty Enterasys makes to You in connection with this license of the Licensed Materials is that if the media on which the Licensed Software is recorded is defective, it will be replaced without charge, if Enterasys in good faith determines that the media and proof of payment of the license fee are returned to Enterasys or the dealer from whom it was obtained within ninety (90) days of the date of payment of the license fee.

    NEITHER ENTERASYS NOR ITS AFFILIATES MAKE ANY OTHER WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, WITH RESPECT TO THE LICENSED MATERIALS, WHICH ARE LICENSED "AS IS". THE LIMITED WARRANTY AND REMEDY PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE EXPRESSLY DISCLAIMED, AND STATEMENTS OR REPRESENTATIONS MADE BY ANY OTHER PERSON OR FIRM ARE VOID. ONLY TO THE EXTENT SUCH EXCLUSION OF ANY IMPLIED WARRANTY IS NOT PERMITTED BY LAW, THE DURATION OF SUCH IMPLIED WARRANTY IS LIMITED TO THE DURATION OF THE LIMITED WARRANTY SET FORTH ABOVE. YOU ASSUME ALL RISK AS TO THE QUALITY, FUNCTION AND PERFORMANCE OF THE LICENSED MATERIALS. IN NO EVENT WILL ENTERASYS OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR SPECIAL, DIRECT, INDIRECT, RELIANCE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF DATA OR PROFITS OR FOR INABILITY TO USE THE LICENSED MATERIALS, TO ANY PARTY EVEN IF ENTERASYS OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL ENTERASYS OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU OR ANY OTHER PARTY EXCEED THE LICENSE FEE YOU PAID FOR THE LICENSED MATERIALS. Some states do not allow limitations on how long an implied warranty lasts and some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation and exclusion may not apply to You. This limited warranty gives You specific legal rights, and You may also have other rights which vary from state to state.

14. JURISDICTION. The rights and obligations of the parties to this Agreement shall be governed and construed in accordance with the laws and in the State and Federal courts of the State of California, without regard to its rules with respect to choice of law. You waive any objections to the personal jurisdiction and venue of such courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.

15. GENERAL.
    a. This Agreement is the entire agreement between Enterasys and You regarding the Licensed Materials, and all prior agreements, representations, statements, and undertakings, oral or written, are hereby expressly superseded and canceled.
    b. This Agreement may not be changed or amended except in writing signed by both parties hereto.
    c. You represent that You have full right and/or authorization to enter into this Agreement.
    d. This Agreement shall not be assignable by You without the express written consent of Enterasys. The rights of Enterasys and Your obligations under this Agreement shall inure to the benefit of Enterasys' assignees, licensors, and licensees.

e. Section headings are for convenience only and shall not be considered in the interpretation of this Agreement.
f. The provisions of the Agreement are severable and if any one or more of the provisions hereof are judicially determined to be illegal or otherwise unenforceable, in whole or in part, the remaining provisions of this Agreement shall nevertheless be binding on and enforceable by and between the parties hereto.
g. Enterasys' waiver of any right shall not constitute waiver of that right in future. This Agreement constitutes the entire understanding between the parties with respect to the subject matter hereof, and all prior agreements, representations, statements and undertakings, oral or written, are hereby expressly superseded and canceled. No purchase order shall supersede this Agreement.
h. Should You have any questions regarding this Agreement, You may contact Enterasys at the address set forth below. Any notice or other communication to be sent to Enterasys must be mailed by certified mail to the following address:

Extreme Networks, Inc.
145 Rio Robles
San Jose, CA 95134 United States
ATTN: General Counsel

Contents

About This Guide

This document describes how to design your Purview solution deployment.

Who Should Use This Guide

This document is intended for experienced network administrators who are responsible for implementing and maintaining communications networks.

Related Documents

Enterasys NetSight Software Release Notes are available on the Network Management Suite (NMS) Documentation web page:

http://extranet.enterasys.com/downloads/pages/default.aspx

After entering your email address (username) and password, follow this path to the document:
Visibility & Control > Network Management Suite (NMS) > Documentation > Manuals & Release Notes > select a version of NetSight > NetSight Suite.

Typographical Conventions

The following typographical conventions and icons are used in this document.

bold type	Actual user input values or names of screens and commands.
italic type	User input value required.
`courier`	Used for command-level input or output.
purple type	Indicates a hypertext link. When reading this document online, click the text in purple to go to the referenced figure, table, or section.
📝	**Note:** Calls the reader's attention to any item of information that may be of special importance.
⚠	**Caution:** Contains information essential to avoid damage to the equipment. **Precaución:** Contiene información esencial para prevenir dañar el equipo. **Achtung:** Verweißt auf wichtige Informationen zum Schutz gegen Beschädigungen.
⚡	**Warning:** Warns against an action that could result in personal injury or death. **Advertencia:** Advierte contra una acción que pudiera resultar en lesión corporal o la muerte. **Warnhinweis:** Warnung vor Handlungen, die zu Verletzung von Personen oder gar Todesfällen führen können!

⚠	**Electrical Hazard:** Warns against an action that could result in personal injury or death. **Riesgo Electrico:** Advierte contra una acción que pudiera resultar en lesión corporal o la muerte debido a un riesgo eléctrico. **Elektrischer Gefahrenhinweis:** Warnung vor sämtlichen Handlungen, die zu Verletzung von Personen oder Todesfällen – hervorgerufen durch elektrische Spannung – führen können!

Getting Help

For additional support related to Purview or this document, contact Extreme Networks using one of the following methods:

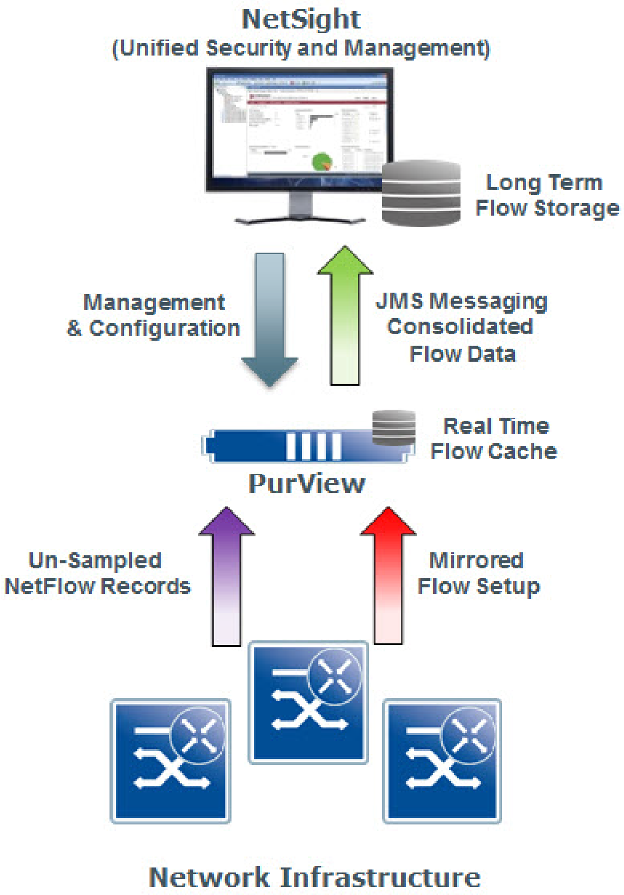
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-603-952-5000 For the Extreme Networks Support toll-free number in your country: www.extremenetworks.com/support/enterasys-support/contact/
Email	support@extremenetworks.com To expedite your message, type **[NetSight]** in the subject line.
Website	www.extremenetworks.com/support/
Address	Extreme Networks 145 Rio Robles San Jose, CA 95134 (USA)

1 Introduction

Deployment Overview

Figure 1 shows the simplified architecture and information flows of a Purview deployment.

Figure 1 Simplified Architecture and Information Flows



An Extreme S- or K-Series CoreFlow2 switch forwards the following to a Purview appliance:

- Unsampled NetFlow, which provides an accurate statistical representation of all flows mirrored for application identification.
- The first 15 packets of each flow, via a forensic policy mirror.

  The mirrored traffic can be delivered to the Purview appliance by two methods:

  - A local traffic mirror
  - Remote mirroring through GRE (Generic Routing Encapsulation) L2 tunneling. Through remote mirroring, a single Purview appliance can receive traffic feeds from multiple switches in the network without being directly connected to them.

On the Purview appliance, the application stream is assembled and fingerprints are applied to identify the applications. This information is then combined with the corresponding NetFlow record. The combined record, which provides IP and TCP/UDP information, application name and category, TCP and application response times, and application metadata, is sent to the NetSight server for graphing and storage.

Deployment Requirements

Deploying a Purview solution requires the following:

- Extreme S- or K-Series CoreFlow2 switches
- Purview appliance—Available as a hardware appliance or a virtual appliance.

  For deployments requiring more than 10G monitored bandwidth, you can install the PV-A-300-10G-UG I/O module in the Purview appliance to enhance the interface bandwidth. Refer to *Purview Appliance PV-A-300 Installation Guide* for information on installing a 10G interface.

Note: Virtual Purview appliances are bandwidth-bound by the underlying host interface bandwidth. If the host interface can operate at 10Gbps, the virtual interface can be reassigned to a new hardware interface without any change in the Purview appliance.

- NetSight management—Besides the configuration and monitoring of the Purview solution, NetSight provides the long term storage and reporting, presenting the correlated data with contextual information. Additionally, NetSight provides that data to other IT systems via the OneFabric Connect API.
- Licenses
  - NMS-ADV (NetSight Advanced License)—Purview management and configuration requires an NMS-ADV license.
  - PV-FPM (Purview Flow License)—Enables the Purview flow processing capability on the Purview appliance.
  - Feature-specific licenses—CoreFlow2 features such as GRE tunneling may require a specific license depending on the version of firmware running in your CoreFlow2 switch

2 Designing Your Purview Deployment

To design a reliable and accurate Purview deployment, you must consider the following:

- Traffic Domains
- Monitored Points
- CoreFlow2 Switch Deployment
- Purview Appliance Deployment
- Traffic Mirror Forwarding Methods
- Common Flow Collection Issues

Traffic Domains

To ensure that a Purview appliance does not receive duplicate traffic, split your network into non-overlapping functional or topological traffic domains. Assign one traffic domain to each Purview appliance in your deployment.

Delivering traffic from only one traffic domain provides each Purview appliance with an accurate representation of the traffic in the domain and keeps the mirrored traffic within the scalability limits of the appliance.

Use the following guidelines when creating your traffic domains:

- Physical network layers: Edge, distribution, core.
- IP network boundaries, such as Internet, intranet, and DMZ. These network boundaries are easily identified and provide easily monitored points for the Purview appliance.
- Functional domains, such as sales and R&D. Isolating traffic from one functional domain or another can be difficult. To simplify your deployment, you should identify a single port for each functional domain to use for traffic monitoring.
- NAT boundaries: Use NAT boundaries as Purview traffic domain boundaries. A NAT section inside a traffic domain can lead to unexpected results because the Purview appliance will not be able to identify the original flow and the NAT flow. If a traffic domain contains the original flows and the NAT flows, the flows will be counted twice for the two different source addresses.

Monitored Points

You must establish monitored points in the CoreFlow2 switch provide a reliable and accurate traffic sample to a Purview appliance. In a reliable and accurate traffic sample, the statistics obtained are the same statistics that would be obtained from all the traffic in the domain. Ensure that your traffic samples meet the following requirements:

- Every flow in the traffic domain must be represented in the sample. To do this, you must carefully plan the points where the traffic is sampled or mirrored.
- Every flow in the traffic domain must appear only once in the sample. Your deployment must avoid traffic samples that contain multiple copies of the same flow.

To minimize the collection of unidirectional or duplicate flows:

- Map all ingress (that is, RX) pathways where network traffic can enter into a particular traffic domain
  - The ingress pathways can traverse multiple switches and therefore will usually require a detailed and accurate network diagram to pinpoint them.
  - If any ingress ports to the traffic domain are left out of the deployed configuration, the result will be inaccurately tagged unidirectional flows.
- Ensure that any multi-pathed traffic is delivered to the same Purview appliance.
- Do not include intra traffic domain pathways built for redundancy between switches as these links will lead to duplicate flows.
- Configure the ingress network pathways isolated during the planning process to capture only the inbound traffic to the port. For each switch involved in a traffic domain, ensure that NetFlow and the Purview traffic mirror on the isolated ports are enabled in the RX direction only.

For scenarios that can lead to traffic capture issues, see “Common Flow Collection Issues” on page 6.

You can establish your monitored points at various locations in your network.

- Edge
- Distribution
- Core
- DMZ

Edge

Extreme CoreFlow2 switches can provide NetFlow statistics and traffic mirroring capabilities on all edge ports. By deploying all uni-directional mirrors, all traffic flows are captured only when entering the network. Assuming that all edge traffic is delivered to another edge point, this strategy ensures a complete traffic sample. If edge devices exchange traffic with devices in other areas of the network, such as the data center, DMZ, or internet, you can ensure that all traffic is captured by adding monitored points in other network layers.

Distribution

In terms of configuration and scalability, monitoring all traffic in the edge layer can be difficult. Mirroring at the distribution layer provides a similar level of accuracy and, because it requires fewer mirroring configurations, greater scalability. The risk with this strategy is the loss of traffic switched locally at the edge.

Core

If you expect highly centralized traffic flows, such as edge to data center or edge to internet, establishing monitored points at the core level offers the greatest visibility with the fewest configuration requirements.

DMZ

The DMZ traffic domain is an independent network area, usually a set of VLANs or even network devices that connect with the rest of the network through firewalls. These firewall interfaces can provide the required traffic sample for all ingress and egress traffic. You should assume that most of the traffic in the DMZ will be with systems and users outside of the DMZ. If you expect a large amount of intra-DMZ traffic, you must adapt the traffic sampling strategy to account for this and replicate the strategy used in an edge or core deployment.

Common Flow Collection Issues

Ensure that your Purview deployment accounts for the following potential problem areas:

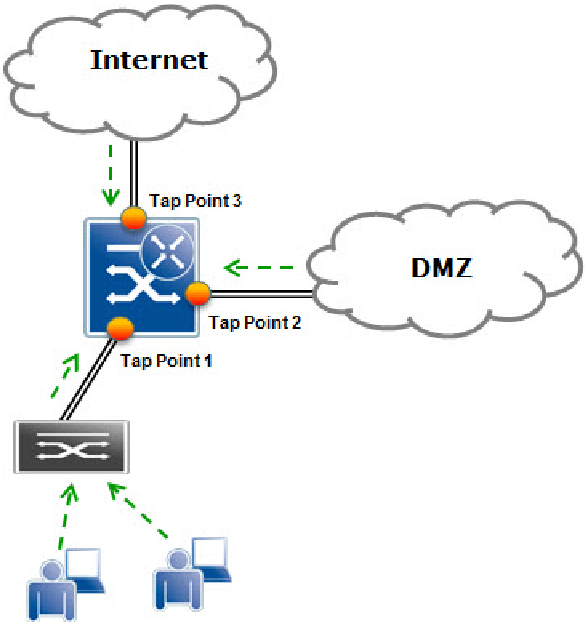
- Unidirectional Flows
- Duplicate Flows
- Asymmetric Routing
- Network Load Balancing

Unidirectional Flows

By default, the Extreme CoreFlow2 switches forward NetFlow and the application traffic mirror for all ingress flows. This configuration can cause unidirectional flows if not deployed properly.

In Figure 1, three tap points are configured on a switch. When a user accesses the Internet, the traffic is captured by Tap Point 1 on the way out to the Internet and at Tap Point 3 for the return traffic. Include both tap points in the traffic domain.

Figure 1 Unidirectional flows

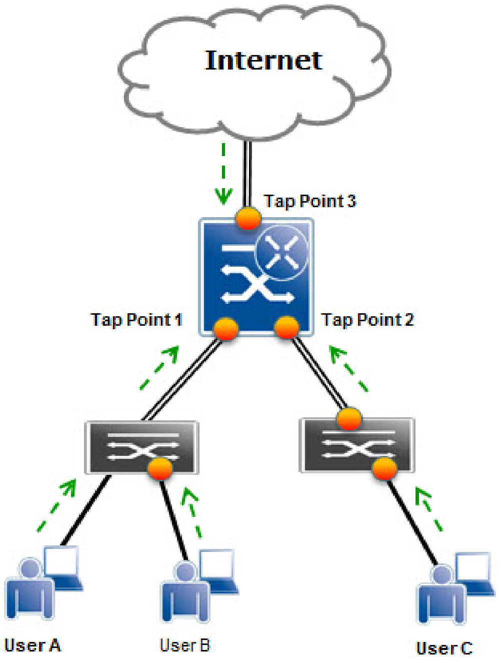


Duplicate Flows

Duplicate flows occur when the same flow is seen at multiple tap points included in a Purview traffic domain.

In Figure 2, User A's traffic, which is logged once on each path to and from the Internet, is counted correctly. User B's traffic is seen twice on the way to the Internet and once on the return path from the Internet. User C's traffic is logged twice in both directions. To avoid duplicate flows, limit the collection locations or create multiple traffic domains to keep the duplicate information separated.

Figure 2 Duplicate flows



Asymmetric Routing

Asymmetric routing occurs when a packet takes a path from source A to destination B but then the return packet from B takes a different path back to A. Because there are no perceived performance issues associated with asymmetric routing for normal applications traveling across the network, network administrators are often unaware that asymmetric routing is occurring. The issue becomes evident once NetFlow or a port mirror is enabled for a specific path and only one half of a TCP conversation is seen. This causes the Purview solution to produce erroneous results.

Network Load Balancing

If your network includes a load balancing configuration, ensure that all necessary links are covered by the Purview solution. If covering all links is impossible because of physical constraints or possible flow duplication, your Purview deployment may require collection at specific network choke points.

CoreFlow2 Switch Deployment

You can deploy a CoreFlow 2 switch for the Purview solution in two ways:

- In-line—If you have CoreFlow2 switches in your network, the NetFlow and traffic mirroring capabilities can be provided by the network itself. See "In-Line Deployment" on page 8.
- Overlay—If you do not currently have CoreFlow2 switches installed in your network, you can install CoreFlow2 switches as overlays to provide the required NetFlow and traffic mirroring capabilities. See "Overlay Deployment" on page 8.

In-Line Deployment

Extreme S- and K-Series CoreFlow2 switches can capture traffic directly traversing them and sample the flow to provide the Purview appliance with an accurate representation of the application data.

Design your flow mirror configuration according to the guidelines in Traffic Domains and Monitored Points to ensure the domain does not include duplicate flows.

The best practice is to do the following:

- Configure unidirectional port mirrors (RX or TX only)
- Deploy the monitored ports in such a way that all potential egress or ingress ports in a domain are mirrored.

RX, or ingress, is the default for policy mirrors and NetFlow configurations. Unless you require egress configurations, ingress configurations are highly recommended.

For full visibility, an in-line flow collection deployment should have CoreFlow2 switches deployed across the edge, distribution, core, data center and/or DMZ of the network. You can use an already deployed CoreFlow2 switch infrastructure or deploy CoreFlow2 switches at one layer of the network to collect application tagged flows from all of the previously defined traffic domains.

To ensure a smooth migration and integration of non-intelligent network layers and segments, you can start by enabling the Purview solution for just one or two layers, such as data center and distribution.

Overlay Deployment

An overlay flow collection deployment is similar to an in-line deployment in that flow collection can take place across the edge, distribution, core, data center, and DMZ. An overlay deployment is appropriate if your network consists of network switches that lack the capabilities of CoreFlow2 switches to provide mirror traffic feed and unsampled NetFlow statistics to the Purview appliance. You can use a passive network tap to direct traffic to an out-of-band CoreFlow2 switch that generates the required unsampled NetFlow stats and traffic mirror.

A full mirror of the desired traffic is pulled from the existing network infrastructure using mirroring, span, or passive tap solutions and is forwarded into a CoreFlow2 switch, which then performs the Purview flow and packet processing on the forwarded traffic.

For a complete Purview overlay mode deployment, each defined traffic domain requires the same network pathway planning and traffic collection to ensure that you have selected the correct choke point ports for Purview monitoring.

Note: For a successful overlay mode deployment, your network infrastructure must be capable of a bi-directional line rate mirror for the designated choke point ports.

Purview Appliance Deployment

The Purview appliance supports multiple deployment modes to suit different network environments and connectivity characteristics:

- Single Interface—A single interface is used for both management and monitoring traffic. You must configure a GRE tunnel for traffic monitoring.
- Dual Interface Mirrored—Separate interfaces are configured for management and monitoring traffic. The monitoring interface will be put into tap mode for traffic monitoring.
- Dual Interface Tunnel Mirrored—Separate interfaces are configured for management and monitoring traffic. The monitoring interface will get its own IP address. You must configure GRE tunnels for traffic monitoring.

For more information on configuring the Purview appliance deployment mode, see the *Installation Guide* for your Purview appliance.

Traffic Mirror Forwarding Methods

Use one of the following methods to deliver the traffic mirror from a CoreFlow2 switch to a Purview appliance:

- A direct physical connection from the CoreFlow2 destination mirror port(s) to an Ethernet interface on the Purview appliance
- A GRE tunnel
  - For remote networks, GRE tunnels provide an affordable solution to transfer the mirror traffic to a centralized Purview appliance, eliminating the need for individual Purview appliances at the remote locations.
  - For data center deployments, GRE tunnels reduce the number of Ethernet monitoring interfaces required on a Purview appliance, which can be especially critical for Purview deployments built upon VMware.

  Using a GRE tunnel, each CoreFlow2 switch wraps the Purview mirror into a GRE tunnel that terminates either inside the Purview appliance or, for scalability reasons, on a CoreFlow2 switch in front of the Purview appliance. Once the GRE header is removed from the Purview mirror traffic, the Purview processing continues as if the mirror was physically connected.

If you use GRE tunnels, ensure the following:

- Traffic delay and bandwidth availability along the path of the mirroring tunnels do not impair the capability of the Purview appliance to calculate application statistics
- Jumbo Ethernet frame functionality is enabled

You must configure the GRE tunnels on both the CoreFlow2 switch and the Purview appliance. For an example of configuring a GRE tunnel on a CoreFlow2 switch, see Chapter 3, Sample CoreFlow2 Switch Configurations. For information on configuring GRE tunnels in a Purview appliance, see the *Installation Guide* for your Purview appliance.

Note: Do not use WAN links to transport mirrored traffic to the Purview appliance.

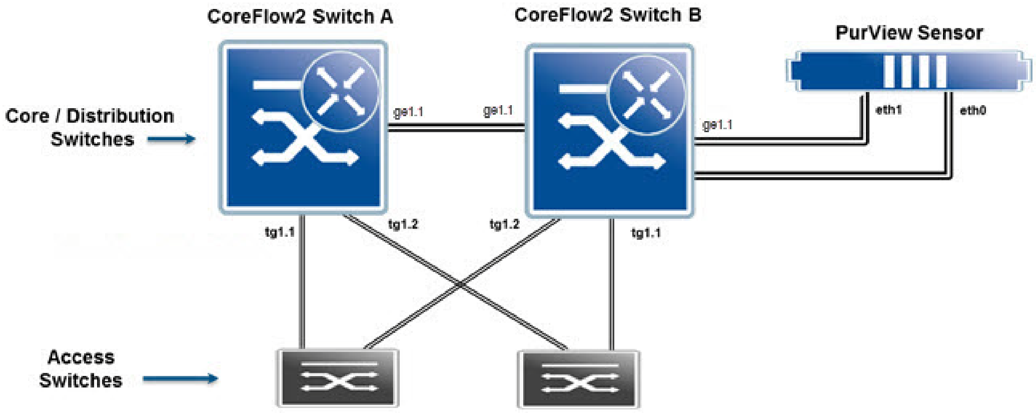
3 Sample CoreFlow2 Switch Configurations

This chapter contains sample configurations for CoreFlow2 switches.

- In-Line (ToR Switches)
- In-Line (Bonded CoreFlow2 Switch)
- Overlay Mode

The sample configurations assume that you have configured the Purview appliance with the corresponding interfaces and GRE tunnels. For more information, see the *Installation Guide* for your Purview appliance.

In-Line (ToR Switches)



The servers in this network are connected to the ToR switches and must traverse core switches Switch A and Switch B to reach their clients. It is assumed that spanning tree will keep a loop-free topology and no load traffic balancing algorithms are run in the interfaces between the ToR/EoR switches and Switch A and Switch B.

In this example, the traffic inside the ToR switches is considered irrelevant as the deployment focuses on the traffic going through core switches Switch A and B. Because Switch A needs to traverse Switch B to reach the Purview appliance, Switch A will use a GRE tunnel to direct its mirror to port eth1 of the appliance.

The setup of a GRE tunnel in CoreFlow2 switches requires an unused physical port assigned as an endpoint of the GRE tunnel. Port ge.1.3 is used in Switch A.

- Switch A management IP: 192.168.10.11/24
- Switch B management IP: 192.168.10.12/24
- Purview appliance eth0: 192.168.20.100/24
- Purview appliance eth1: 192.168.30.100/24

GRE tunnels can be started from any interface in the origin switch. To avoid management and interface availability issues, use loopback interfaces as originators of the GRE traffic in Switch A and Switch B. The state of the loopback interfaces is not related to the egress state of VLANs in the switch so these interfaces are always up and available. You must set up routing appropriately so that the loopback interface can reach eth1 of the Purview appliance and the default gateway of the Purview appliance can reach the loopback interface.

Switch A Configuration

1. Ensure that ports used for GRE tunnels are statically configured for speed and duplex.

   ```
   set port duplex ge.1.1-3 full
   set port speed ge.1.1-3 1000
   ```

2. Enable NetFlow reporting in the monitored port and export its data to the NetFlow receiver (eth1 interface) in the Purview appliance.

   ```
   set netflow export-interval 1
   set netflow export-destination 192.168.30.100 2055
   set netflow export-version 9
   set netflow port tg.1.1-2 enable rx
   set netflow template refresh-rate 30 timeout 1
   set netflow cache enable
   ```

3. Create the policy mirror that will sample the traffic flows. This mirror will deliver only relevant application information to the Purview appliance.

   ```
   set mirror create 1
   set mirror 1 mirrorN 15
   set mirror ports ge.1.3 1
   ```

4. Create a policy using this mirror. In this case, the traffic should continue flowing in the switch, so a PVID of 4095 is configured in the policy.

   ```
   set policy profile 1 name Application pvid-status enable pvid 4095 mirror-
   destination 1
   set policy rule admin-profile port tg.1.1-2 mask 16 port-string tg.1.1-2
   admin-pid 1
   ```

5. Create a GRE tunnel to transport this mirror to the eth1 interface of the Purview appliance. This example assumes that the IP address 10.10.10.1 is routable in the network.

   From the routing configuration terminal in the CoreFlow2 switch:

   ```
   interface loop.0.1
     ip address 10.10.10.1 255.255.255.255 primary
     no shutdown
      exit
   interface tun.0.1
     tunnel destination 192.168.30.100
     tunnel mode gre l2 ge.1.3
     tunnel mirror enable
     tunnel source 10.10.10.1
     no shutdown
     exit
   ```

6. Enable jumbo frames on the physical interfaces where GRE traffic will traverse.

   ```
   set port jumbo enable ge.1.1
   ```

Switch B Configuration

1. Ensure that ports used for GRE tunnels are statically configured for speed and duplex.

   ```
   set port duplex ge.1.1-3 full
   set port speed ge.1.1-3 1000
   ```

2. Enable NetFlow reporting in the monitored port and export its data to the NetFlow receiver (eth1 interface) in the Purview appliance.

   ```
   set NetFlow export-interval 1
   set NetFlow export-destination 192.168.30.100 2055
   set NetFlow export-version 9
   set NetFlow port tg.1.1-2 enable rx
   set NetFlow template refresh-rate 30 timeout 1
   set NetFlow cache enable
   ```

3. Create the policy mirror.

   ```
   set mirror create 1
   set mirror 1 mirrorN 15
   set mirror ports ge.1.3 1
   ```

4. Create a policy using this mirror. In this case, the traffic should continue flowing in the switch, so a PVID of 4095 is configured in the policy.

   ```
   set policy profile 1 name Application pvid-status enable pvid 4095 mirror-
   destination 1
   set policy rule admin-profile port tg.1.1-2 mask 16 port-string tg.1.1-2
   admin-pid 1
   ```

5. Create a GRE tunnel to transport this mirror to the eth1 interface of the Purview appliance. This example assumes that the IP address 10.10.10.2 is routable in the network.

   From the routing configuration terminal in the CoreFlow2 switch:

   ```
   interface loop.0.1
     ip address 10.10.10.2 255.255.255.255 primary
     no shutdown
      exit
   interface tun.0.1
     tunnel destination 192.168.30.100
     tunnel mode gre l2 ge.1.3
     tunnel mirror enable
     tunnel source 10.10.10.2
     no shutdown
     exit
   ```

6. Enable jumbo frames on the physical interfaces where GRE traffic will traverse.

   ```
   set port jumbo enable ge.1.1
   ```

In-Line (Bonded CoreFlow2 Switch)

In in-line mode, if Switches A and B are two bonded CoreFlow2 switches, the Purview engine is directly connected to the bonding so there is no need to use a GRE tunnel to forward mirrored traffic from Switch A to the Purview appliance. In addition, a 10 gigabit port is used for connectivity from Switch B to the Purview appliance.

Assuming that both switches are S4 switches, Switch A is chassis 1 in the bonded pair, and Switch B is chassis 2, the port numbering is as follows:

Table 1 In-Line Mode Virtual Switch Bonding Port Numbers

Switch	Switch port number	VSB port number
Switch A	tg.1.1	tg.1.1
	tg.1.2	tg.1.2
Switch B	tg.1.1	tg.5.1
	tg.1.2	tg.5.2
	tg.1.3	tg.5.3

Connectivity remains the same. In a redundant bonded pair, ports tg.1.1 and tg.1.2 in both switches are aggregated as a LAG. Assuming that lag.0.1 and lag.0.2 have been created in the bonded pair with the following assignment, port numbering follows the bonded pair numbering convention:

- Lag.0.1 -> tg.1.1;tg.5.1
- Lag.0.2 -> tg.1.2;te.5.2

The configuration in this example is the same as the configuration presented in "In-Line (ToR Switches)" on page 11 with the following changes:

- VSB port numbering and LAGs are used
- A GRE tunnel is not created

1. Enable NetFlow reporting in the monitored port and export its data to the NetFlow receiver (eth1 interface) in the Purview appliance. In this case the monitored ports are the LAGs.

```
set netflow export-interval 1
set netflow export-destination 192.168.30.100 2055
set netflow export-version 9
set netflow port lag.0.1-2 enable rx
set netflow template refresh-rate 30 timeout 1
set netflow cache enable
```

2. Create the policy mirror.

```
set mirror create 1
set mirror 1 mirrorN 15
set mirror ports tg.5.3 1
```

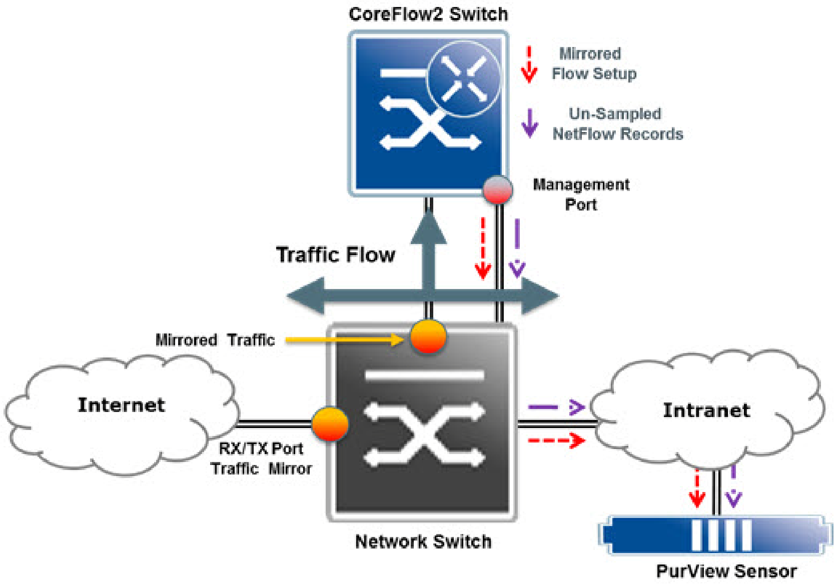
3. Create a policy using this mirror. In this case, the traffic needs to continue flowing through the switch so a PVID of 4095 is configured in the policy.

```
set policy profile 1 name Application pvid-status enable pvid 4095 mirror-destination 1
set policy rule admin-profile port lag.0.1 mask 16 port-string lag.0.1 admin-pid 1
set policy rule admin-profile port lag.0.2 mask 16 port-string lag.0.2 admin-pid 1
```

Note: If you plan to use GRE tunneling as part of this setup to mirror traffic to a remote location, VSB only allows GRE configuration if dedicated bonding ports are in use.

Overlay Mode

The overlay mode configuration is generally used at a choke point of a network consisting of third-party gear or Extreme switches that do not support the policy mirroring (mirrorN) capabilities of the CoreFlow2 switches. In this example configuration, a bidirectional port mirror is created for all traffic coming from or going to the Internet. To filter the data from that mirror and generate the NetFlow records, an overlay SSA is used. Because this is a situation with less traffic, a single interface is used on the Purview appliance to converge all policy mirrored traffic, all NetFlow, and all management traffic. A GRE tunnel is used to forward the mirror traffic from the SSA to the Purview appliance. Port ge.1.5 is used on the SSA overlay switch for management and GRE tunneling.



This example uses the following IP addresses:

- CoreFlow2 switch management IP address: 192.168.10.11
- Purview appliance eth0 IP address: 192.168.30.100

1. Ensure that port ge.1.24, which is used for GRE tunneling, is statically configured for speed and duplex. Ensure that spanning tree configuration keeps ports ge.1.3, ge.1.24 and ge.1.5 loop free and forwarding traffic.

   ```
   set port duplex ge.1.24 full
   set port speed ge.1.24 1000
   set spantree portadmin ge.1.3 disable
   ```

2. Enable NetFlow reporting for the monitored port and export its data to the NetFlow receiver (eth0 interface) in the Purview appliance.

   ```
   set netflow export-interval 1
   set netflow export-destination 192.168.30.100 2055
   set netflow export-version 9
   set netflow port ge.1.3 enable rx
   set netflow template refresh-rate 30 timeout 1
   set netflow cache enable
   ```

3. Create the policy mirror.

   ```
   set mirror create 1
   set mirror 1 mirrorN 15
   set mirror ports ge.1.24 1
   ```

4. Create a policy using this mirror. In this case, the traffic should be dropped after the switch forwards the relevant frames to the Purview appliance, so a PVID of 0 is configured in the policy.

   ```
   set policy profile 1 name Application pvid-status enable pvid 0 mirror-destination 1
   set policy rule admin-profile port ge.1.3 mask 16 port-string ge.1.3 admin-pid 1
   ```

5. Create a GRE tunnel to transport this mirror to the Purview appliance. In this example the GRE tunnel follows the path through the management interface connecting the CoreFlow2 switch to the network for management. Ensure that proper routing exists to reach the Purview appliance from the management interface of the overlay SSA.

   ```
   interface loop.0.1
     ip address 10.10.10.1 255.255.255.255 primary
     no shutdown
      exit
   interface tun.0.1
     tunnel destination 192.168.30.100
     tunnel mode gre l2 ge.1.24
     tunnel mirror enable
     tunnel source 10.10.10.1
     no shutdown
     exit
   ```

6. Enable jumbo frames on the physical interfaces through which GRE traffic will traverse. You must enable jumbo frames on each interface that the GRE traffic traverses across the entire network.

   ```
   set port jumbo enable ge.1.5
   ```

4 Alternative Designs

You can adapt the Purview solution to your network requirements. This chapter describes deployment changes for the following scenarios:

- More Than Two Ethernet Interfaces
- More Than Four GRE Tunnels
- VMWare TAP Interface

Note: Use the designs in this chapter only if your deployment requirements are not met by the designs previously described in this guide.

More Than Two Ethernet Interfaces

In cases of specific bandwidth restraints or design requirements, more than two Ethernet interfaces may be needed.

In examples in Chapter 3, Sample CoreFlow2 Switch Configurations, the mirrorN feature of CoreFlow2 switches redirected only the first 15 packets of each flow to the Purview appliance. This reduces the traffic managed by the appliance to under 1Gbps for most deployments. If, however, your total bandwidth is still greater than 1Gbps, you can enable more Ethernet interfaces for traffic monitoring in the appliance.

1. Add the following lines to the /etc/network/interfaces file on the Purview appliance for each additional interface. In the example below, eth2 is being added.

```
auto eth2
iface eth2 inet manual
    up ifconfig eth2 0.0.0.0 up
    up ip link set eth2 promisc on
    down ip link set eth2 promisc off
    down ifconfig eth2 down
```

If the additional Ethernet interfaces are used to terminate GRE tunnels, additional commands must be added. In the example below eth2 will be used as a GRE interface 2 with the IP address of 192.168.40.100.

```
# The secondary network interface
auto eth2
iface eth2 inet manual
    up ifconfig eth2 192.168.40.100 up
    up ip link set eth2 promisc on
    down ip link set eth2 promisc off
    down ifconfig eth2 down



#GRE tap interfaces
auto gre2
iface gre2 inet static
```

```
    address 0.0.0.0
    pre-up ip  link add gre2 type gretap remote $SWITCH_IP local
192.168.40.100 ttl 255
    post-down ip link del gre2
```

The newly created interfaces can be used as NetFlow destinations or GRE traffic endpoints in the switches' configurations.

2. Restart the appliance to enable the newly created interfaces.

   Once you have created the interfaces, you must declare the interfaces to the Purview appliance to use them as monitoring interfaces.

3. Add the following lines to the /opt/appid/conf/appidconfig-local.xml file:

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <Configuration>
     <Interfaces>
       <Interface name="eth1"/>
       <Interface name="eth2"/> /*one line per each newly created interface
     </Interfaces>
   </Configuration>
   ```

   If the file does not exist, create it.

   If the file exists and contains the `<Configuration>` tag, add the interface lines between the `<Configuration></Configuration>` tags.

   ```
       <Interface name="eth2"/>
       <Interface name="eth3"/> /*one line per each newly created interface
   ```

4. Restart the server process for the new configuration to take effect.

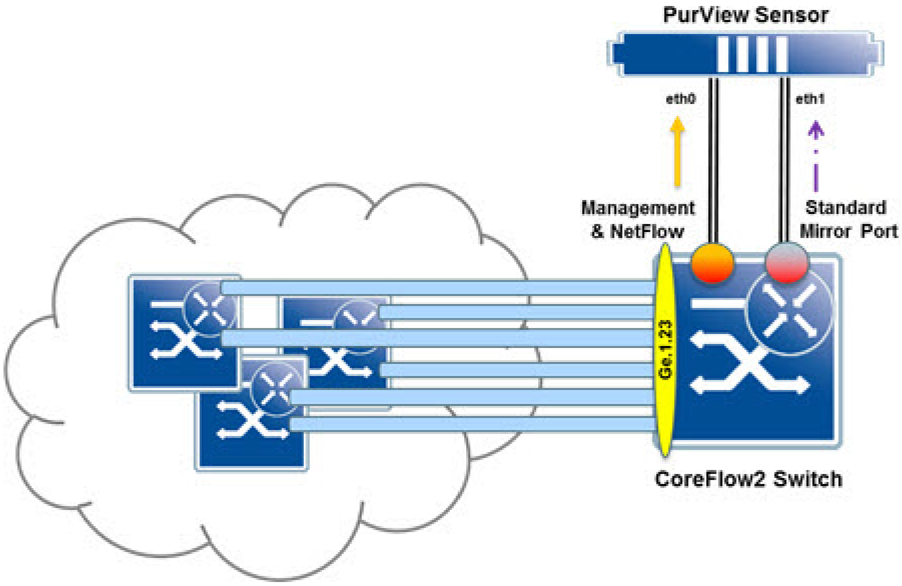
   ```
   appidctl restart
   ```

Note: Virtual Purview appliances are bandwidth-bound by the underlying host interface bandwidth. They can grow up to the bandwidth that the virtualization platform can offer in a virtual interface.

More Than Four GRE Tunnels

Purview appliances can support up to four GRE tunnels. If your deployment requires more than four GRE tunnels, the GRE tunnels can be terminated in a CoreFlow2 switch and the traffic can be delivered to the Purview appliance using standard traffic mirroring, as shown in Figure 1.

Figure 1 More than Four GRE Tunnels



In Figure 1, the CoreFlow2 switch is terminating six tunnels from other switches and delivering the content of the tunnels in port ge.1.23.

The tunnels terminate at the same loopback IP address in the CoreFlow2 switch, 10.10.10.10. The other switches have addresses 10.10.10.1 through 10.10.10.5.

The setup in the CoreFlow2 switch, which assumes that the loopback interface 10.10.10.10 has been already created, is as follows:

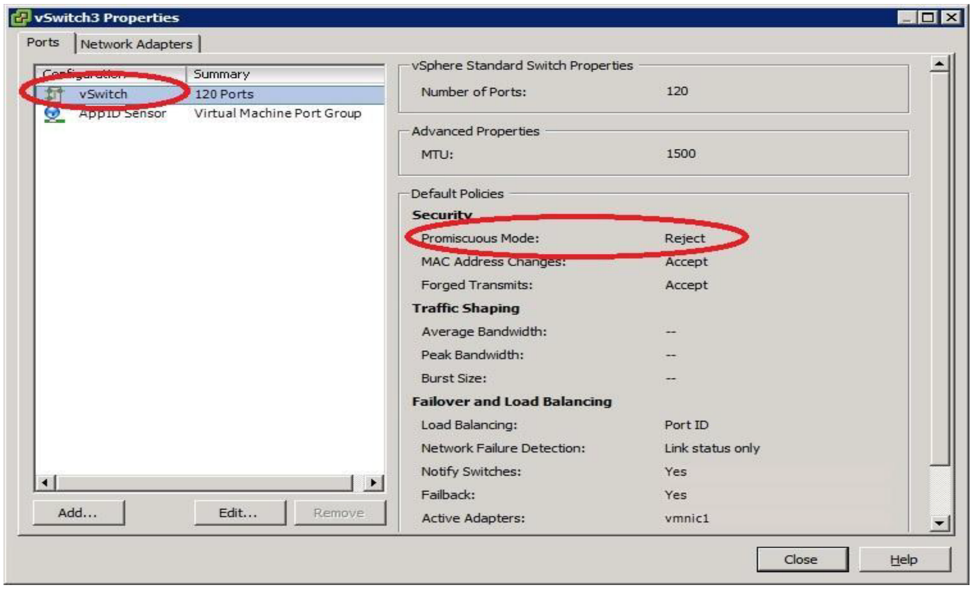
```
interface tun.0.1
  tunnel destination 10.10.10.1
  tunnel mode gre l2 ge.1.23
  tunnel mirror enable
  tunnel source 10.10.10.10
  no shutdown
  exit
interface tun.0.2
  tunnel destination 10.10.10.2
  tunnel mode gre l2 ge.1.23
  tunnel mirror enable
  tunnel source 10.10.10.10
  no shutdown
  exit
```

Additional interfaces are added for each GRE tunnel. Note that jumbo frames must be enabled for each interface that will be passing the GRE traffic.

VMWare TAP Interface

If you are using a vSwitch's TAP interface, you must enable promiscuous mode on the vSwitch to allow the Purview appliance to capture packets. Promiscuous mode, which is typically used for packet sniffing, will allow the virtual Purview appliance to see all of the mirrored traffic.

By default, promiscuous mode for a newly created vSwitch is disabled (that is, set to Reject).



Configuration	Summary
vSwitch	120 Ports
AppID Sensor	Virtual Machine Port Group

vSphere Standard Switch Properties

Number of Ports: 120

Advanced Properties

MTU: 1500

Default Policies

Security

Promiscuous Mode: Reject

MAC Address Changes: Accept

Forged Transmits: Accept

Traffic Shaping

Average Bandwidth: --

Peak Bandwidth: --

Burst Size: --

Failover and Load Balancing

Load Balancing: Port ID

Network Failure Detection: Link status only

Notify Switches: Yes

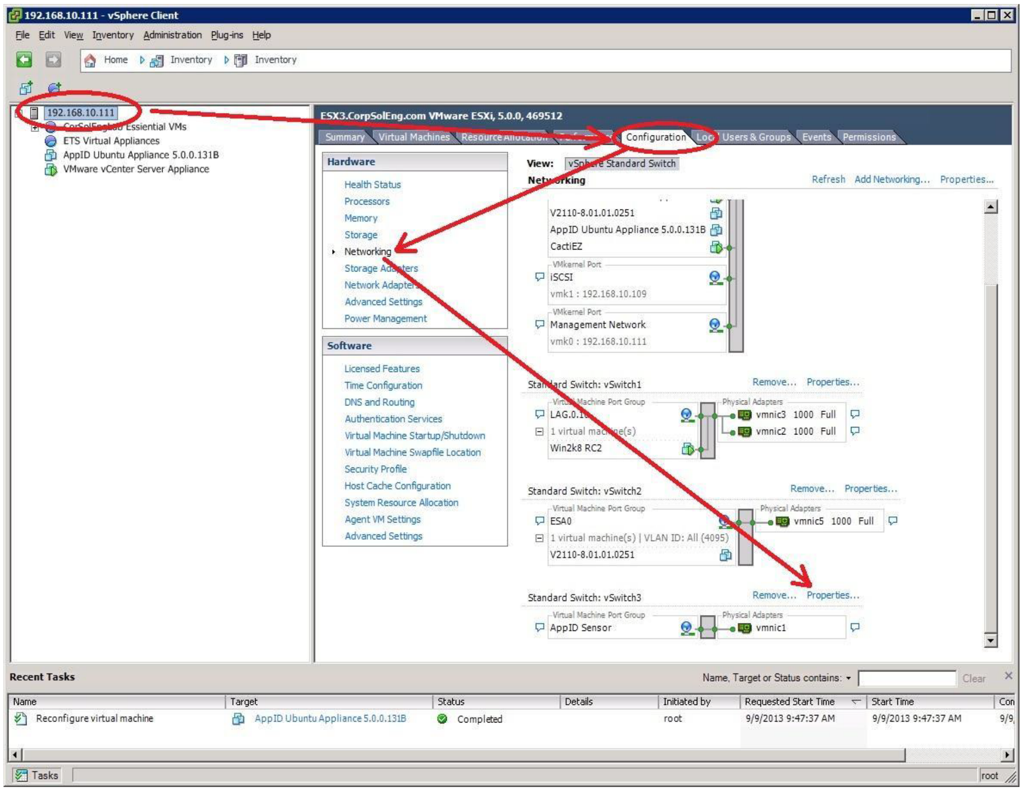
Failback: Yes

Active Adapters: vmnic1

To enable promiscuous mode on the vSwitch:

1. Select the desired ESXi host from the device tree in the left-hand panel.
2. Click the **Configuration** tab.

3. Click **Properties** to the right of the vSwitch that is used by the Purview monitor interface.


192.168.10.111 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
192.168.10.111
CorpSolEngLab Essential VMs
ETS Virtual Appliances
AppID Ubuntu Appliance 5.0.0.131B
VMware vCenter Server Appliance
ESX3.CorpSolEng.com VMware ESXi, 5.0.0, 469512
Summary Virtual Machines Resource Allocation Performance Configuration Local Users & Groups Events Permissions
Hardware
Health Status
Processors
Memory
Storage
Networking
Storage Adapters
Network Adapters
Advanced Settings
Power Management
Software
Licensed Features
Time Configuration
DNS and Routing
Authentication Services
Virtual Machine Startup/Shutdown
Virtual Machine Swapfile Location
Security Profile
Host Cache Configuration
System Resource Allocation
Agent VM Settings
Advanced Settings
View: vSphere Standard Switch
Networking
Refresh Add Networking... Properties...
V2110-8.01.01.0251
AppID Ubuntu Appliance 5.0.0.131B
CactiEZ
VMkernel Port
iSCSI
vmk1 : 192.168.10.109
VMkernel Port
Management Network
vmk0 : 192.168.10.111
Standard Switch: vSwitch1
Remove... Properties...
Virtual Machine Port Group
LAG.0.10
1 virtual machine(s)
Win2k8 RC2
Physical Adapters
vmnic3 1000 Full
vmnic2 1000 Full
Standard Switch: vSwitch2
Remove... Properties...
Virtual Machine Port Group
ESA0
1 virtual machine(s) | VLAN ID: All (4095)
V2110-8.01.01.0251
Physical Adapters
vmnic5 1000 Full
Standard Switch: vSwitch3
Remove... Properties...
Virtual Machine Port Group
AppID Sensor
Physical Adapters
vmnic1
Recent Tasks
Name, Target or Status contains:
Clear
Tasks
root

Name	Target	Status	Details	Initiated by	Requested Start Time	Start Time	Con
Reconfigure virtual machine	AppID Ubuntu Appliance 5.0.0.131B	Completed		root	9/9/2013 9:47:37 AM	9/9/2013 9:47:37 AM	9/9,

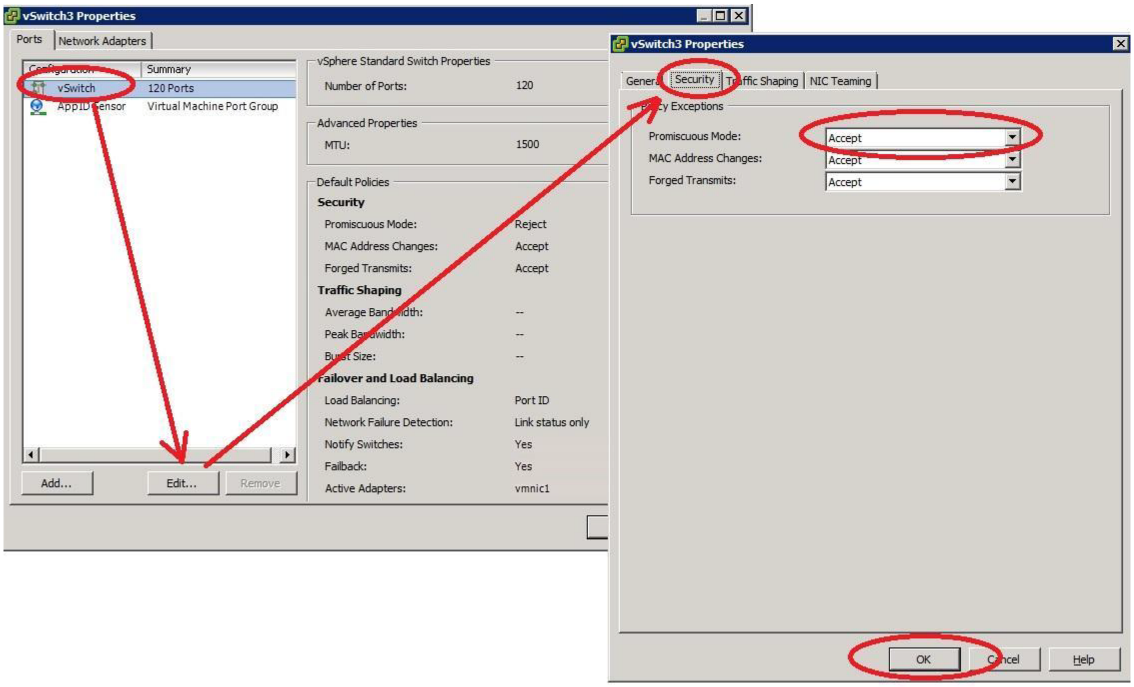
4. On the **Ports** tab of the **vSwitch Properties** window, select the appropriate vSwitch.

5. Click **Edit**.

6. Select the **Security** tab.

7. In the Promiscuous Mode drop down list, change the value from Reject to Accept.

8. Click **OK**.



Configuration	Summary
vSwitch	120 Ports
AppID Sensor	Virtual Machine Port Group

vSphere Standard Switch Properties
Number of Ports: 120

Advanced Properties
MTU: 1500

Default Policies
Security
Promiscuous Mode: Reject
MAC Address Changes: Accept
Forged Transmits: Accept
Traffic Shaping
Average Bandwidth: --
Peak Bandwidth: --
Burst Size: --
Failover and Load Balancing
Load Balancing: Port ID
Network Failure Detection: Link status only
Notify Switches: Yes
Failback: Yes
Active Adapters: vmnic1

Policy Exceptions
Promiscuous Mode: Accept
MAC Address Changes: Accept
Forged Transmits: Accept

Promiscuous mode is now enabled for the newly created port group TAP interface. On the **Ports** tab, the Promiscuous Mode setting for the appropriate vSwitch should indicate that promiscuous mode is now set to Accept (that is, enabled).

5 Troubleshooting

This chapter presents ways to troubleshoot the following deployment issues:

- Network Connectivity
- Unidentified Entries in Purview

Network Connectivity

1. After configuring NetFlow on an Extreme CoreFlow2 switch, verify that NetFlow packets are being forwarded from the switch with the following command:

   ```
   show NetFlow statistics
   ```

2. Ensure that NetSight can ping the Purview appliance's eth0 interface.
3. If the status of the Purview appliance doesn't change to green in OneView, check the SNMPv3 configuration in the appliance and in NetSight.
4. Check the GRE tunnels, if used. The GRE interfaces should be listed and their status should be UP.

   ```
   ifconfig
   eth0      Link encap:Ethernet  HWaddr 00:50:56:8d:2c:22
            inet addr:192.168.30.136  Bcast:192.168.30.255  Mask:255.255.255.0
             inet6 addr: fe80::250:56ff:fe8d:2c22/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:233517 errors:0 dropped:0 overruns:0 frame:0
             TX packets:32157 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:52578402 (52.5 MB)  TX bytes:23198996 (23.1 MB)

   eth1      Link encap:Ethernet  HWaddr 00:50:56:8d:2c:23
             inet6 addr: fe80::250:56ff:fe8d:2c23/64 Scope:Link
             UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
             RX packets:21708377 errors:0 dropped:0 overruns:0 frame:0
             TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:14737338317 (14.7 GB)  TX bytes:468 (468.0 B)

   gre1      Link encap:Ethernet  HWaddr d6:05:a1:a0:21:82
             inet6 addr: fe80::d405:a1ff:fea0:2182/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST  MTU:1462  Metric:1
             RX packets:198332 errors:0 dropped:193599 overruns:0 frame:0
             TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:38016139 (38.0 MB)  TX bytes:468 (468.0 B)
   ```

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2199776 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2199776 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:780936519 (780.9 MB)  TX bytes:780936519 (780.9 MB)
```

5. Verify, on all interfaces carrying GRE traffic, that GRE traffic is received on the interface. If GRE traffic is received, the decoded packets will contain the protocol `GREv0`.

```
tcpdump -i eth0 ip proto 47


tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
11:20:33.462765 IP 192.168.10.11 > AppID51.demo.com: GREv0, length 208: STP
Unknown STP protocol (0x04)
11:20:33.809119 IP 192.168.10.11 > AppID51.demo.com: GREv0, length 235: IS-
IS, p2p IIH, src-id 20b3.9992.b666, length 214
11:20:33.809307 IP 192.168.10.11 > AppID51.demo.com: GREv0, length 235: IS-
IS, p2p IIH, src-id 20b3.9992.b666, length 214
11:20:35.462599 IP 192.168.10.11 > AppID51.demo.com: GREv0, length 208: STP
Unknown STP protocol (0x04)
11:20:35.578897 IP 192.168.10.11 > AppID51.demo.com: GREv0, length 235: IS-
IS, p2p IIH, src-id 20b3.9992.b666, length 214
11:20:35.578942 IP 192.168.10.11 > AppID51.demo.com: GREv0, length 235: IS-
IS, p2p IIH, src-id 20b3.9992.b666, length 214
11:20:37.443832 IP 192.168.10.11 > AppID51.demo.com: GREv0, length 350: IP
0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from
00:50:56:8d:b4:63 (oui Unknown), length 300
11:20:37.462472 IP 192.168.10.11 > AppID51.demo.com: GREv0, length 208: STP
Unknown STP protocol (0x04)
11:20:37.508985 IP 192.168.10.11 > AppID51.demo.com: GREv0, length 235: IS-
IS, p2p IIH, src-id 20b3.9992.b666, length 214
11:20:37.509044 IP 192.168.10.11 > AppID51.demo.com: GREv0, length 235: IS-
IS, p2p IIH, src-id 20b3.9992.b666, length 214
11:20:39.218957 IP 192.168.10.11 > AppID51.demo.com: GREv0, length 235: IS-
IS, p2p IIH, src-id 20b3.9992.b666, length 214
11:20:39.219410 IP 192.168.10.11 > AppID51.demo.com: GREv0, length 235: IS-
IS, p2p IIH, src-id 20b3.9992.b666, length 214
11:20:39.462607 IP 192.168.10.11 > AppID51.demo.com: GREv0, length 208: STP
Unknown STP protocol (0x04)
11:20:40.829045 IP 192.168.10.11 > AppID51.demo.com: GREv0, length 235: IS-
IS, p2p IIH, src-id 20b3.9992.b666, length 214
11:20:40.829220 IP 192.168.10.11 > AppID51.demo.com: GREv0, length 235: IS-
IS, p2p IIH, src-id 20b3.9992.b666, length 214
```

```
11:20:41.462537 IP 192.168.10.11 > AppID51.demo.com: GREv0, length 208: STP Unknown STP protocol (0x04)
11:20:41.999060 IP 192.168.10.11 > AppID51.demo.com: GREv0, length 200: IS-IS, L1 CSNP, src-id 20b3.9992.b666.00, length 179
11:20:41.999072 IP 192.168.10.11 > AppID51.demo.com: GREv0, length 200: IS-IS, L1 CSNP, src-id 20b3.9992.b666.00, length 179
11:20:42.579115 IP 192.168.10.11 > AppID51.demo.com: GREv0, length 235: IS-IS, p2p IIH, src-id 20b3.9992.b666, length 214
11:20:42.579138 IP 192.168.10.11 > AppID51.demo.com: GREv0, length 235: IS-IS, p2p IIH, src-id 20b3.9992.b666, length 214
```

6. Verify that traffic is received through the GRE tunnel.

```
Tcpdump –i gre1
root@AppID51.demo.com:~$ tcpdump -i gre1
tcpdump: WARNING: gre1: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on gre1, link-type EN10MB (Ethernet), capture size 65535 bytes
11:26:03.250600 IS-IS, p2p IIH, src-id 20b3.9992.b666, length 214
11:26:03.250768 IS-IS, p2p IIH, src-id 20b3.9992.b666, length 214
11:26:03.465581 STP Unknown STP protocol (0x04)
11:26:05.030617 IS-IS, p2p IIH, src-id 20b3.9992.b666, length 214
11:26:05.030625 IS-IS, p2p IIH, src-id 20b3.9992.b666, length 214
11:26:05.465612 STP Unknown STP protocol (0x04)
11:26:06.700610 IS-IS, p2p IIH, src-id 20b3.9992.b666, length 214
11:26:06.700706 IS-IS, p2p IIH, src-id 20b3.9992.b666, length 214
11:26:07.465432 STP Unknown STP protocol (0x04)
9 packets captured
9 packets received by filter
0 packets dropped by kernel
```

7. Ensure the Purview appliance is receiving NetFlow records.

   Sniff the interface containing NetFlow records. In a configuration that does not use GRE tunnels, NetFlow exists on the management interface (eth0) for NetFlow traffic. Enter CTRL-C to interrupt sniffing:

   ```
   $ tcpdump -i eth0 udp port 2055
   ```

   Allow adequate time to observe for NetFlow frames. The time may vary depending on the amount of traffic monitored. A good rule of thumb is twice the export-interval value. The conventional configuration would equate to 2 minutes.

   If there are NetFlow frames, proceed to step 9.

   If there are NO NetFlow frames, access the CLI on the CoreFlow2 switch and enter the following command:

   ```
   show config netflow
   ```

There should be an entry for an export-destination for the IP address on the Purview appliance associated with the interface expected to receive NetFlow traffic.

If the entry exists, ping the address of the Purview interface expected to receive NetFlow. In instances where asymmetric routing occurs, it may be necessary to view these frames through tcpdump on the Purview appliance.

If not, enter the following line into the CoreFlow2 switch CLI:

```
set NetFlow export-destination (IP address) 2055
```

8. Verify that the tunnel source switches are reachable from the Purview appliance interfaces.

   In this example, the tunnel is established between 192.168.10.11 and the Purview appliance 192.168.30.136.

   ```
   root@AppID51.demo.com:~$ ping 192.168.10.11 -I 192.168.30.136
   PING 192.168.10.11 (192.168.10.11) from 192.168.30.136 : 56(84) bytes of
   data.
   64 bytes from 192.168.10.11: icmp_req=1 ttl=63 time=2.24 ms
   64 bytes from 192.168.10.11: icmp_req=2 ttl=63 time=2.01 ms
   64 bytes from 192.168.10.11: icmp_req=3 ttl=63 time=1.61 ms
   --- 192.168.10.11 ping statistics ---
   3 packets transmitted, 3 received, 0% packet loss, time 2002ms
   rtt min/avg/max/mdev = 1.618/1.958/2.248/0.264 ms
   ```

9. Ensure the Purview Management Upstart service is running:

   ```
   $ appidctl status
   ```

   The `status` command will display the state of the two processes running on the Purview appliance. Both services should be in a state of start/running and have a process ID associated with them.

   If the processes are listed with state of start/running, go to step 10.

   If the processes have a state other than start/running:

   a. View the contents of /var/log/appidmgmtserver.log. If there are any stack traces or notable errors, forward content to Extreme support.

   b. Restart the service.

      ```
      $ appidctl restart
      ```

   c. Wait 30 seconds.

   d. Check the status of the processes.

      ```
      $ appidctl status
      ```

      Assuming the processes are listed with state of start/running, go to step 10.

10. Ensure the Java process is running.

    ```
    $ ps -eaf | grep java
    ```

11. Ensure the Purview management process is listening on NetFlow 2055.

```
$ netstat -pan | grep java
```

12. Ensure that reverse path check is disabled. Some Purview multi-interface configurations discard packets if reverse path check is enabled. Reverse path check should be disabled during by the interface configuration script.

    ```
    root@AppID51.demo.com:~$ sysctl -a | grep -F '.rp_filter'
    net.ipv4.conf.all.rp_filter = 1
    net.ipv4.conf.default.rp_filter = 1
    net.ipv4.conf.eth0.rp_filter = 1
    net.ipv4.conf.eth1.rp_filter = 0
    net.ipv4.conf.gre0.rp_filter = 1
    net.ipv4.conf.gre1.rp_filter = 1
    net.ipv4.conf.lo.rp_filter = 1
    ```

    A value of 0 means reverse path check is disabled for that interface.

Unidentified Entries in Purview

If entries are displayed but unidentified in the Purview Application Flows view, do the following:

1. Ensure the monitoring interface contains what appears to be mirrored traffic. On the Purview appliance, execute the following command on the monitoring interface:

   ```
   tcpdump -i eth1 -s 0 -nn -c 100
   ```

   This will capture, at most, 100 frames. If the process does not terminate quickly, execute CTRL-C to exit the tcpdump capture process.

   - If there are frames that appear to be the monitored traffic, go to step 2.
   - Ensure the Java process is running:

     ```
     $ ps -eaf | grep java
     ```

   a. Ensure the Purview management process is listening on NetFlow 2055:

      ```
      $ netstat -pan | grep java
      ```

      If no frames appear to be representative of the traffic being mirrored, examine the CoreFlow2 switch configuration.

      (1) On the CoreFlow2 switch, execute the following commands:

      ```
      show config policy
      show config mirror
      show running-config (If GRE is enabled)
      ```

      (2) Ensure the policy profile configuration contains the port for the traffic mirror.

      (3) Ensure the mirror configuration contains the port for the mirror interface connection.

(4) Verify the GRE tunnel configuration is correct. Execute the following commands:

```
config
show tunnel
```

The affected interface should have an Admin status of Enabled and an Oper status of Up.

(5) Verify the port statuses of connections to the CoreFlow2 switch. Execute the following command:

```
show port status -interesting
```

This command will only list ports with an Oper status of Up. Ensure relevant connections are Up.

(6) View packet counters on the mirror feed:

```
show port counters (mirror feed interface)
```

Execute this command a few times and note the changes in the interface and switch counters. If there are no changes or few changes, the external port mirror configuration may be incorrect or there may be no traffic mirrored.

2. Ensure IPFIX records are being generated. On the Purview appliance, execute the following command on the loopback interface (use CTRL-C to terminate):

   ```
   tcpdump -i lo udp port 9191
   ```

   If IPFIX records exist, go to step 3.

   If IPFIX records do not exist:

   a. Ensure the Purview service is running.

      ```
      $ appidctl status
      ```

      Execute this command couple times sequentially to ensure the process is not restarting continually.

   b. Navigate to /opt/appid/conf/appidconfig.xml and confirm the Interface tag is designated to the correct interface. Also confirm the IPFIX host destination is itself: 127.0.0.1 with port 9191.

3. Ensure the Purview management process is listening on NetFlow 9191:

   ```
   $ netstat -pan | grep java
   ```

   An entry should indicate that the Purview management process is listening on all interfaces on UDP 9191.