Hawkeye

Release 6.0.7

Vision E1S User Guide

KEYSIGHT

202512091302+05:30

913-2427-01 Rev A

Notices

Copyright Notice

© Keysight Technologies 2016–2025

No part of this document may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Keysight Technologies, Inc. as governed by United States and international copyright laws.

Warranty

The material contained in this document is provided “as is,” and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Keysight disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Keysight shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Keysight and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

U.S. Government Rights

The Software is "commercial computer software," as defined by Federal Acquisition Regulation ("FAR") 2.101. Pursuant to FAR 12.212 and 27.405-3 and Department of Defense FAR Supplement ("DFARS") 227.7202, the U.S. government acquires commercial computer software under the same terms by which the software is customarily provided to the public. Accordingly, Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at http://www.keysight.com/find/sweula. The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or (2) Relinquish to, or otherwise provide, the government rights in excess of these rights customarily provided to the public to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation. No additional government requirements beyond those set forth in the EULA shall apply, except to the extent that those terms, rights, or licenses are explicitly required from all providers of commercial computer software pursuant to the FAR and the DFARS and are set forth specifically in writing elsewhere in the EULA. Keysight shall be under no obligation to update, revise or otherwise modify the Software. With respect to any technical data as defined by FAR 2.101, pursuant to FAR 12.211 and 27.404.2 and DFARS 227.7102, the U.S. government acquires no greater than Limited Rights as defined in FAR 27.401 or DFAR 227.7103-5 (c), as applicable in any technical data. 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

Contacting us

Keysight headquarters

1400 Fountaingrove Parkway
Santa Rosa, CA 95403-1738
Email address: support@keysight.com

Support

Location	Phone number	Local time
Americas		
US, Canada	1-888-829-5558	8h00 – 17h00
Brazil	0800-892-0522	8h00 – 17h00
Mexico	001-888-829-5558	8h00 – 17h00
Other	+1-719-273-6516	8h00 – 17h00
EMEAI		
Belgium	0800-18686	8h30 – 17h30
Finland	0800-913-352	8h30 – 17h30
France	0800-917228	8h30 – 17h30
Germany	0800-0824099	8h30 – 17h30
India	1800-18-02552	8h30 – 17h30
Ireland	1800-949245	8h30 – 17h30
Israel	1-809-454975	8h30 – 17h30
Italy	0800-790571	8h30 – 17h30
Luxembourg	0800-25112	8h30 – 17h30
Netherlands	0800-022-9086	8h30 – 17h30

Romania	0213 015 699	8h30 – 17h30
Spain	800-654386	8h30 – 17h30
Sweden	0201-202266	8h30 – 17h30
United Kingdom	0800-0293882	8h30 – 17h30
Asia and Australia		
Australia	1-800-370-558	8h30 – 17h00
China Mainland	800-810-0005	8h30 – 17h30
	400-810-0005	8h30 – 17h30
Hong Kong	800-931-613	9h00 – 18h00
Japan	0120-421-621	9h00 – 17h30
Malaysia	1800-819 092	8h30 – 17h30
South Korea	080-770-0800	8h30 – 17h30
Singapore	800-101-3797	8h30 – 17h30
Taiwan	0800-699-880	9h00 – 18h00
Other	+65 6215 7600	8h30 – 17h30 (Singapore)

Table of Contents

Contacting us **3**

Chapter 1 Hawkeye Vision E1S Management **8**

Introducing the Vision Edge 1S 10

License requirement 11

First Time Installation 12

Package Contents 12

Installation Prerequisites 13

Mount the Device 13

Optionally Ground the Vision E1S Device 14

Connect Power to the Vision E1S 14

Verify the Vision E1S Is Powered On 15

Connect Network Cables to the Vision E1S 15

Connect to the Vision E1S Console Port 16

Perform Initial Configuration of the Vision E1S 17

Log in to Hawkeye to Continue Your Configuration 19

Access Software Updates and Additional Documentation 20

Getting Started with Vision E1S Local Manager 20

Getting Started with Vision E1S on Hawkeye 20

Configure Vision E1S Firewall 21

Vision E1S Port Mapping and System Performance 21

Select the Hawkeye Application Landing Page 23

Vision E1S Page 23

Vision E1S Use Cases 24

Configure Vision E1S Use Case 1 28

Configure Vision E1S Use Case 1 31

Configure Vision E1S Use Case 2 35

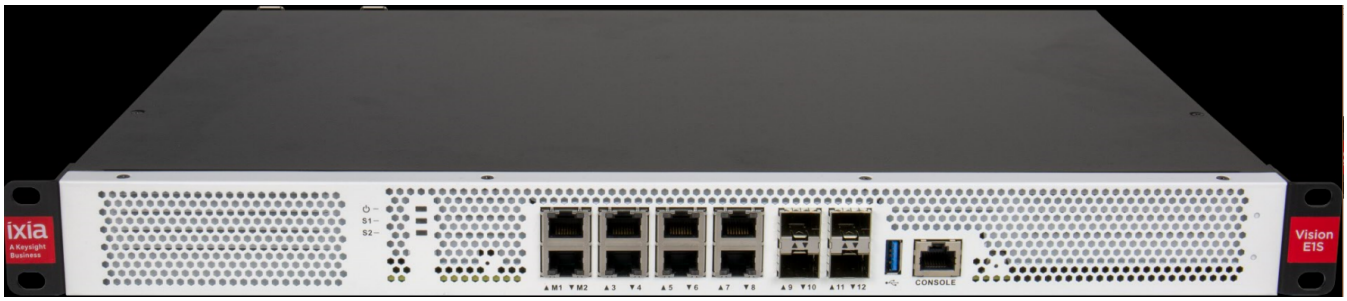
Configure Vision E1S Use Case 3 37
Configure Vision E1S Use Case 4 41
Configuring Vision E1S 44
Order of Operations for Configuring NETSTACK Traffic 44
Configure NETSTACK 44
Use Vision E1S NetStack Filter Parameters 45
Add NETSTACK Filters 48
Map NETSTACK Ports, Limit Traffic, and Replicate It to Multiple Tools 50
Terminate GRE tunnels 54
Originate GRE Tunnels 55
Terminate VxLAN Tunnels 56
Originate VxLAN Tunnels 59
Replicate Traffic 60
Aggregate Traffic 61
Deduplicate Packets 62
Configure APPSTACK 63
Monitor APPSTACK Statistics Related to the Top Filters and Applications 64
Filter APPSTACK Traffic Based on Criteria 64
Egress APPSTACK Filtered Traffic 65
Send NetFlow/IxFlow Records to NetFlow Collectors 66
Capture Filtered Traffic and Save It 69
Forward APPSTACK Filtered Traffic to an Outside Tool 70
Active Monitoring Tests 71
Convert 10G NETSTACK Port for Active Monitoring Test Execution 71
Upgrade the Vision E1S 73
Update with Hawkeye 73
Upgrade in Local Manager Mode 73
UI update process 75
CLI update process 77
XR-E1S Probe - Install and Configure 78
XR-E1S Prerequisites 78

XR-E1S Installation 78
XR-E1S - Configuration 78
E1S CLI Commands 79
Index **82**

CHAPTER 1

Hawkeye Vision E1S Management

The Vision Edge 1S (E1S) is a next generation packet broker that is managed by the Hawkeye server/controller. This section explains how to configure and use the Vision E1S.



In this chapter:

Introducing the Vision Edge 1S **10**

License requirement **11**

First Time Installation **12**

Package Contents 12

Installation Prerequisites 13

Mount the Device 13

Optionally Ground the Vision E1S Device 14

Connect Power to the Vision E1S 14

Verify the Vision E1S Is Powered On 15

Connect Network Cables to the Vision E1S 15

Connect to the Vision E1S Console Port 16

Perform Initial Configuration of the Vision E1S 17

Log in to Hawkeye to Continue Your Configuration 19

Access Software Updates and Additional Documentation 20

Getting Started with Vision E1S Local Manager **20**

Getting Started with Vision E1S on Hawkeye **20**

Configure Vision E1S Firewall 21

Vision E1S Port Mapping and System Performance 21

Select the Hawkeye Application Landing Page 23

Vision E1S Page 23

Vision E1S Use Cases **24**

Configure Vision E1S Use Case 1 28
Configure Vision E1S Use Case 1 31
Configure Vision E1S Use Case 2 35
Configure Vision E1S Use Case 3 37
Configure Vision E1S Use Case 4 41
Configuring Vision E1S 44
Order of Operations for Configuring NETSTACK Traffic 44
Configure NETSTACK 44
Use Vision E1S NetStack Filter Parameters 45
Add NETSTACK Filters 48
Map NETSTACK Ports, Limit Traffic, and Replicate It to Multiple Tools 50
Terminate GRE tunnels 54
Originate GRE Tunnels 55
Terminate VxLAN Tunnels 56
Originate VxLAN Tunnels 59
Replicate Traffic 60
Aggregate Traffic 61
Deduplicate Packets 62
Configure APPSTACK 63
Monitor APPSTACK Statistics Related to the Top Filters and Applications 64
Filter APPSTACK Traffic Based on Criteria 64
Egress APPSTACK Filtered Traffic 65
Send NetFlow/IxFlow Records to NetFlow Collectors 66
Capture Filtered Traffic and Save It 69
Forward APPSTACK Filtered Traffic to an Outside Tool 70
Active Monitoring Tests 71
Convert 10G NETSTACK Port for Active Monitoring Test Execution 71
Upgrade the Vision E1S 73
Update with Hawkeye 73
Upgrade in Local Manager Mode 73
UI update process 75
CLI update process 77

XR-E1S Probe - Install and Configure **78**

XR-E1S Prerequisites 78

XR-E1S Installation 78

XR-E1S - Configuration 78

E1S CLI Commands **79**

Introducing the Vision Edge 1S

The Vision E1S helps you get insight from your users, network, and services at the edge of your network. The Vision E1S provides visibility at the edge into network performance, monitoring, diagnostics, and troubleshooting.

The Vision E1S enables you to distribute network brokers at the edge of the network enabled with NetFlow/IxFlow plus active monitoring for remote site visibility and diagnostics. In your branch sites, use the Vision E1S to:

- Distribute network packet brokers (NPBs) to aggregate traffic with local tools or tunneled traffic to centralized Vision NPBs or analytics tools
- Understand the network with NetFlow metadata, bandwidth, utilization, top applications, top talkers, and top performers
- Perform synthetic monitoring of visibility and diagnostics on remote connectivity to the cloud, internet, WAN, and LAN

The Vision E1S gives you visibility into the edgeless enterprise packet, flow, and active diagnostics in one with the following family of "stack" features:

- **NetStack**
  - Mapping (1:1)
  - Aggregation (M:1)
  - Replication (1:N)
  - Line rate 10G
- **PacketStack**
  - L2GRE origination
  - L2GRE termination
  - Line rate 10G
- **AppStack**
  - IxFlow generation
  - App-based filtering
  - PCAP catpure/export
  - 2Gbps application ingress processing
- **Active Monitoring/Hawkeye Test Execution**
  - Node to Node tests
  - Test Execution Mesh

- One-arm real tests (Real Service)
- Generate 10Gbps of TCP/UDP flows

In addition, the Vision E1S provides **unified management** of:

- On-premise server or cloud-based
- All Vision E1S systems centrally
- SLA-based approach for performance management
- Reporting and analytics of metrics
- Data warehouse for years and trending

License requirement

A Hawkeye server fully manages a Vision E1S. With any Vision E1S deployment (one or many), you may deploy a Hawkeye server to control it or utilize the Local Manager Interface without a license.

With your Vision E1S order, you receive:

- The Vision E1S hardware appliance
- A perpetual license activation code for its Hawkeye server

If the appliance is a demo unit or a spare unit, the license is not provided. For a demo unit, contact your Ixia representative to get a temporary license. For a spare unit, it uses the main unit license because it replaces that unit as its spare.

When you first install it, the Hawkeye server comes unlicensed. If you only activate the Hawkeye server for active monitoring, then you cannot manage Vision E1S units nor register Vision E1S probes on the Hawkeye server.

On the other hand, if you only enable the Hawkeye server with a Vision E1S license, then you can only use the Hawkeye server to manage Vision E1S functions – packet broker, packet capture, application monitoring, and filtering. You cannot use the Hawkeye server for active monitoring.

But if you activate the Hawkeye server for both active monitoring and Vision E1S management, then you can you use it for both of those functions. You use the Hawkeye server to manage Vision E1S units and run active monitoring on Vision E1S units and on any other probes that are registered to the Hawkeye server.

Your start page, after you log in, depends on the license you have installed on your computer:

- If you have both the licenses activated on your Hawkeye server (active monitoring bundle + Vision E1S), then you can configure Hawkeye to set either **Main Dashboard** or **Vision E1S** to be your start page. See Select the Hawkeye Application Landing Page on page 23.
- If you have only the Vision E1S license activated, **Vision E1S** is your start page.

NOTE You only require an enabled Hawkeye license to perform active monitoring Tests. You only require an enabled Vision E1S license to perform NetStack, PacketStack, and AppStack tests.

First Time Installation

This section covers the information you need for the first time installation of your Vision Edge 1S device:

Package Contents **12**

Installation Prerequisites **13**

Mount the Device **13**

Optionally Ground the Vision E1S Device **14**

Connect Power to the Vision E1S **14**

Verify the Vision E1S Is Powered On **15**

Connect Network Cables to the Vision E1S **15**

Connect to the Vision E1S Console Port **16**

Perform Initial Configuration of the Vision E1S **17**

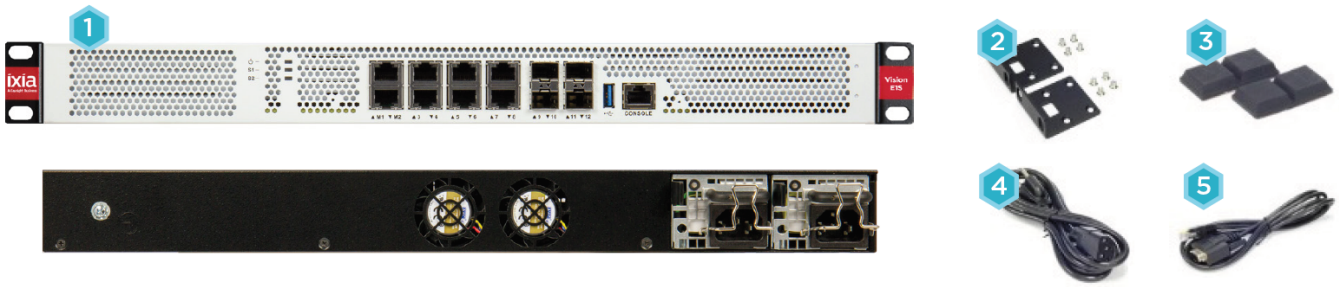
Log in to Hawkeye to Continue Your Configuration **19**

Access Software Updates and Additional Documentation **20**

Package Contents

The Vision Edge 1S ships with the following package contents:

1. Ixia Vision Edge 1S device
2. Rackmount Kit: 2 brackets and 8 screws
3. Four adhesive foot pads
4. Relevant power cords for your geographical location: US, Continental Europe, UK, or Asia
5. Console cable: RJ45-to-DB9



Installation Prerequisites

As a prerequisite to complete the initial configuration found later in this guide, first deploy the Hawkeye server.

1. Go to the following location on the Ixia Customer Support portal: https://support.ixiacom.com/software-downloads/186
2. Download the following:
   a. **Hawkeye software** (OVA or QCOW2)
   b. ***Hawkeye Getting Started Guide***, which contains the complete instructions on installation requirements, deployment options, and steps to license the Hawkeye server for managing Vision Edge 1S systems

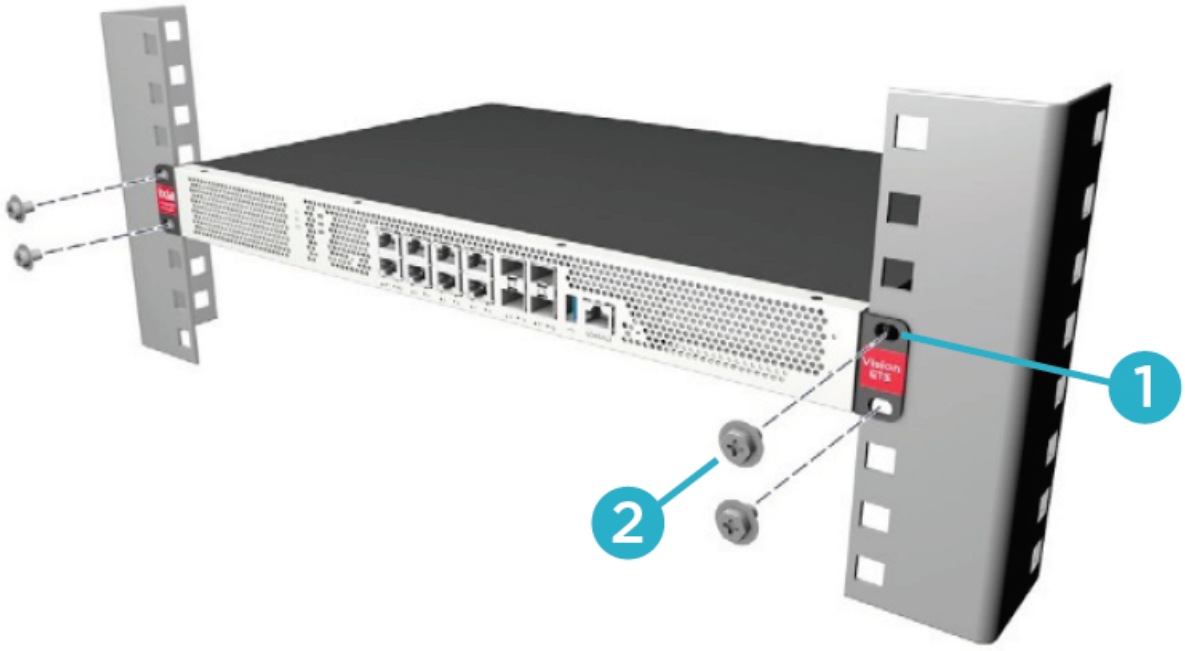
Mount the Device

Either rack mount or desktop mount the Vision E1S device.

Rack Mount

To rack mount the Vision E1S device:

1. Attach the bracket ears to the front left and right of the device.

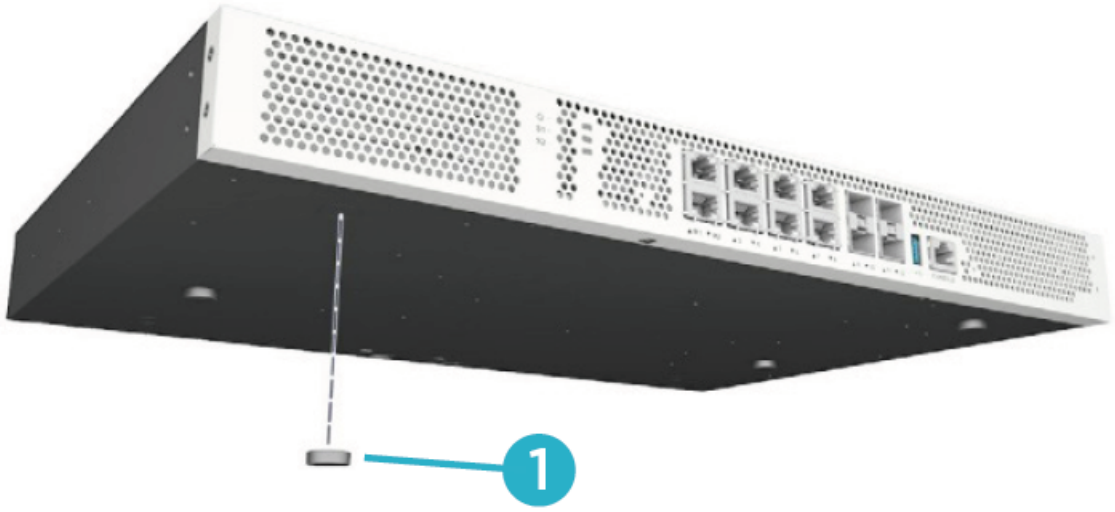


2. Use the screws and cage nuts supplied with the rack to secure the device in the rack.

Desktop Mount

To desktop mount the Vision E1S device:

1. Affix the included adhesive rubber foot pads to the bottom of the device.



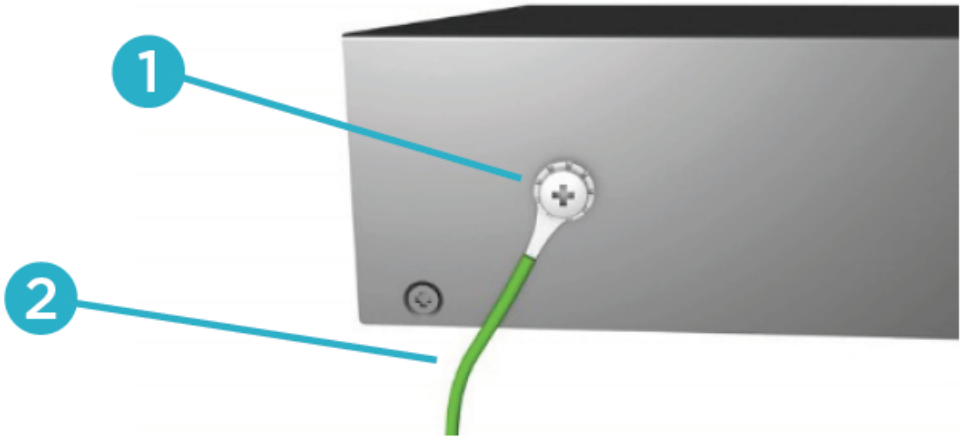
2. Carefully set the device down on a desktop with plentiful airflow space around the Vision E1S.

Optionally Ground the Vision E1S Device

IMPORTANT Ensure that the rack is properly grounded and in compliance with ETSI ETS 300 253. Verify that there is a good electrical connection to the grounding point on the rack (with no paint or isolating surface treatment).

To ground the Vision E1S device (optional):

1. Attach the grounding wire (#18 AWG) to the grounding point on the device rear panel.



2. Connect the other end of the wire to the rack ground.

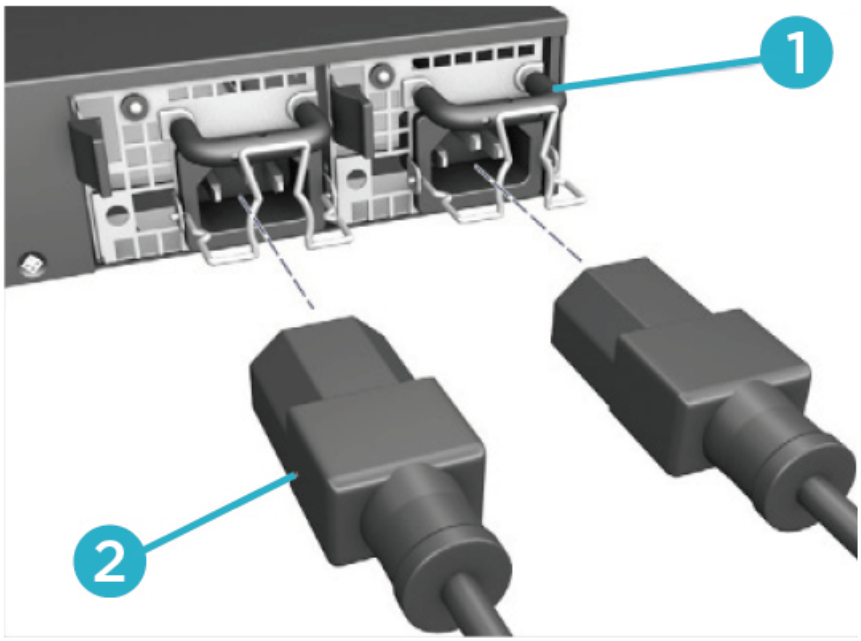
IMPORTANT **Caution**: The earth connection must not be removed unless all supply connections have been disconnected.

Attention: Le raccordement à la terre ne doit pas être retiré sauf si toutes les connexions d'alimentation ont été débranchées.

Connect Power to the Vision E1S

To connect power to the Vision E1S device:

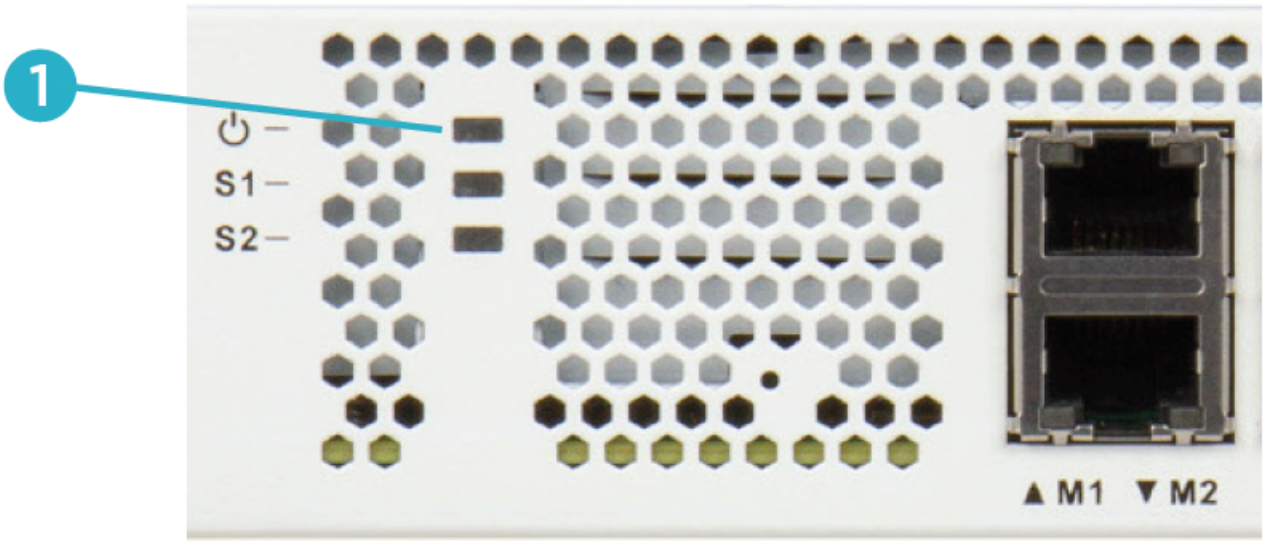
1. Connect one or two AC power cords to the PSU(s) to power up the system.



Verify the Vision E1S Is Powered On

To verify that the Vision E1S is powered on:

1. Check the Power LED located on the left front of the device.
   When operating normally, the power LED is **green**.

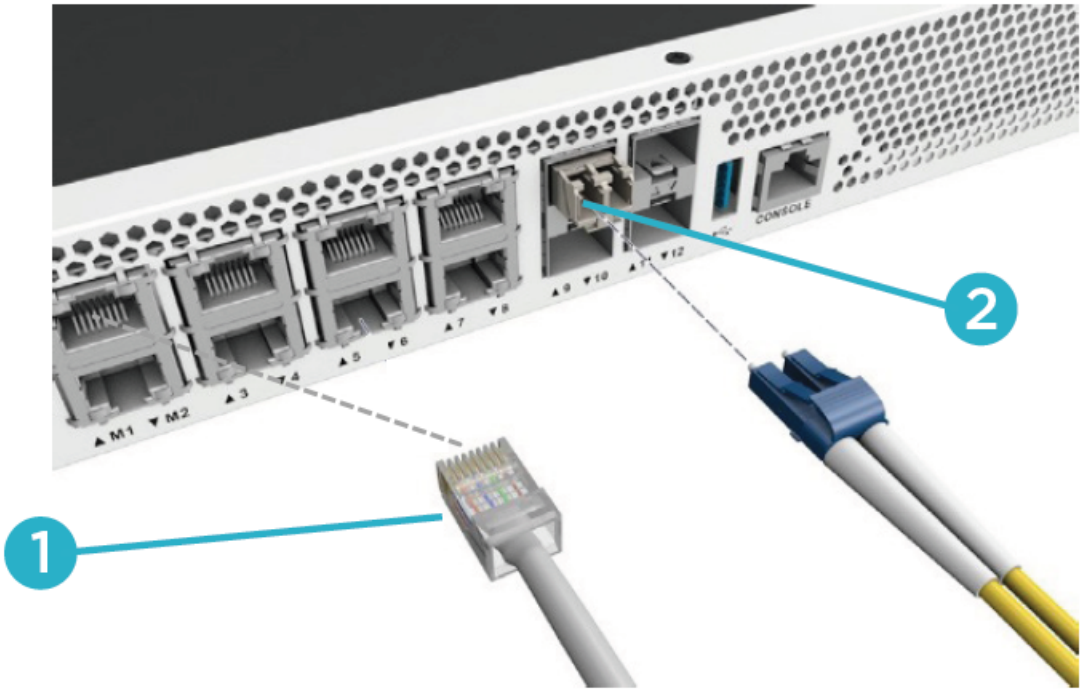


Connect Network Cables to the Vision E1S

To connect network management and transceiver cables to the Vision E1S:

1. Connect a Category 5e or better cable to the network management port labeled **M1**.

   NOTE A DHCP server must be available or set a static IP address as outlined later in this guide.



2. Install SFP+ transceivers.

   NOTE The following transceiver is supported in the SFP+ ports:
   - 10G SFP+ (SR) Keysight PN: MM850-PLUS
   - 10G SFP+ (LR) Keysight PN: SM1310-PLUS
   - 10G SFP+ CU Keysight PN: SFP-10GBASE-T-XCVR

   NOTE The SFP+ ports on the Vision E1S do not support the use of any 1G SFP or 1G Copper transceivers.

3. Connect fiber optic cabling to the transceiver ports.
4. As you make the connections, check the port status LEDs to ensure that the links are valid and working properly.

Connect to the Vision E1S Console Port

To manage the Vision E1S, connect to its console port and configure the port.

To connect to the Vision E1S console port and configure it:

1. Connect a PC to the serial console port using the included console cable.

2. Configure the PC's serial port as follows:
   a. 115200 bps
   b. 8 data bits
   c. No parity
   d. One stop bit
   e. No flow control
3. Log in to the Vision Edge 1S system using the default settings.
   a. Username: **ksuser**
   b. Password: **keysight**
4. After logging in the first time, change the default password **keysight** for username **kuser**, following your company's standards for passwords, using the supported Linux command:

```
-bash-4.2$ changePasswd
Changing password for user ksuser.
New password:
```

Perform Initial Configuration of the Vision E1S

To perform the initial configuration of your Vision E1S:

1. If you are using Static IPv4/6 addresses on the Management Interfaces, please run `interfaceConfigure`. When prompted, select the interface you want to configure, and answer the questions to complete the interface configuration.

NOTE `enp2s0` is port **M1**, and `enp3s0` is port **M2**.

```
#interfaceConfigure
```

```
0 : M1 (enp2s0)
1 : M2 (enp3s0)
```

```
e : EXIT
```

```
Please select an interface to configure: 1
Chosen interface is: enp3s0
```

```
1 : IPv4 Only
2 : IPv6 Only
3 : Both IPv4 and IPv6
e : EXIT
```

```
Config interface as: 3

The current DEFROUTE interface is enp2s0
Would you like enp3s0 to be the IPv4 default route? (Y/n):
Would you like to configure the IPv4 MTU size on this interface? (y/N):

Interface enp3s0 currently configured for dhcp.
```

```
1 : dhcp
2 : static
e : EXIT
```

```
Config IPv4 interface as: 1

Would you like enp3s0 to be the IPv6 default route? (y/N): y
Would you like to configure the IPv6 MTU size on this interface? (y/N):

Interface enp3s0 currently configured as static.
IPv6 Address: 2690:11bf:ac36:c080::b:8008
```

```
1 : dhcp
2 : static
e : EXIT
```

```
Config IPv6 interface as: 2

Enter static IPv6 address (2690:11bf:ac36:c080::b:8008): 2690:11bf:ac36:c080::b:4004
Would you like to enter an IPv6 default gateway? (Y/n):
Enter IPv6 Gateway (2690:11bf:ac36:c080::b:1):

Current DNS servers (Maximum 3):
```

```
8.8.8.8
8.8.4.4
```

```
Would you like to delete any current DNS servers? (y/N):
Would you like to enter an IPv4 DNS server? (y/N):
Would you like to enter an IPv6 DNS server? (y/N):
```

```
0 : 8.8.8.8
1 : 8.8.4.4
n : No
```

```
Would you like to order your DNS Servers (Select number of first DNS Server or n for
No): n
#
```

Changes are applied when the script is completed, and you can verify changes with the `ip a` command.

2. Set the host name of your new Vision E1S if necessary.

```
-bash-4.2$ changeHostname <new_Hostname>
```

3. Change the default password **keysight** for username **ksuser**, using the `changePasswd` command.

```
-bash-4.2$ changePasswd
Changing password for user ksuser.
New password:
```

4. Configure the systems for connections to the Hawkeye Server that controls this Vision E1S.

```
-bash-4.2$ probeConfigure
Probe/Host Name (e1s-lax-01):
<New_ProbeName_If_Desired>
Hawkeye Server (hawkeye-server-ip-address):
<Hawkeye_Server_Hostname_or_IP>
Error connecting to server: <urlopen error [SSL:
CERTIFICATE_VERIFY_FAILED] certificate verify failed
(_ssl.c:600)>
Use this server anyway? (y/N): y
Using anyway
Require valid server certificates? (y/N):n
```

NOTE

The Hawkeye Server image ships with a Self-Signed SSL Certificate. This triggers the error shown above: "`<urlopen error [SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:600)>`".

Even if you have not already replaced the SSL certificate with one from a Certifying Authority (CA), as explained in the *Hawkeye Getting Started Guide*, for the question `Use this server anyway?`, select **`y`** (yes) to use this server anyway.

For the question `Require valid server certificates?`, if you have an SSL certificate from a Certifying Authority (CA), then you can select **`y`** (yes) instead of n (no) to require a valid server certificate and use your certificate.

Log in to Hawkeye to Continue Your Configuration

The Vision E1S is now ready for operation.

To log in to the Hawkeye server/controller:

1. Browse to the Hawkeye server:
   https://hawkeye-server-ip
2. Log in to continue configuring the system.

Access Software Updates and Additional Documentation

To access software updates and additional documentation like the Hawkeye and Vision Edge 1S user guides:

1. Select the following link or navigate your browser to:
   https://support.ixiacom.com/
2. Select **Software Downloads** > **Hawkeye**.

Getting Started with Vision E1S Local Manager

The following is the order of operations for setting up the Vision E1S to be controlled by its local manager:

1. Install the Vision E1S.
   See First Time Installation on page 12.
   a. Rack the Vision E1S.
   b. Apply power to the Vision E1S.
   c. Connect to the Vision E1S through its **Console** (Ethernet) port on the front of the Vision E1S.
   d. Change the default password from **ksuser** to a unique password, according to your company's password standards.
   e. Configure the interface if needed (which is DHCP by default).
   f. Through a CLI, run the `probeConfigure` command.
      i. Set the Hawkeye server IP address to 127.0.0.1.
2. Use a browser to connect to the management IP address of the Vision E1S:
   https://<E1S IP or Hostname>

NOTE Local manager is introduced as part of Release 4.0. If your E1S is running release 3.x, you must upgrade through a Hawkeye Server 4.x Installation.

Locally managed Vision E1S devices are always in secure mode. Please continue to Vision E1S Port Mapping and System Performance.

Getting Started with Vision E1S on Hawkeye

The following is the order of operations for setting up a Hawkeye controller and connecting Vision E1S Network Packet Brokers to it to configure and manage them:

1. Deploy the Hawkeye server.
   See the ***Hawkeye Getting Started Guide***, located on the Ixia Customer Support portal.
   Select **USER GUIDES** > **Hawkeye**.

a. License the Hawkeye server.
   i. Install the Vision E1S License (required).
   ii. Install the Hawkeye license suite (optional).

2. Install the Vision E1S.
   See First Time Installation on page 12.
   a. Rack the Vision E1S.
   b. Apply power to the Vision E1S.
   c. Connect to the Vision E1S through its **Console** (Ethernet) port on the front of the Vision E1S.
   d. Change the default password from **ksuser** to a unique password, according to your company's password standards.
   e. Configure the interface if needed (which is DHCP by default).
   f. Through a CLI, run the `probeConfigure` command.
      i. This requires either the Hawkeye server **IP** address or **Hostname**.

Configure Vision E1S Firewall

NOTE Firewall configuration is applied globally across all connected Vision E1S devices.

To configure Vision E1S firewall options:

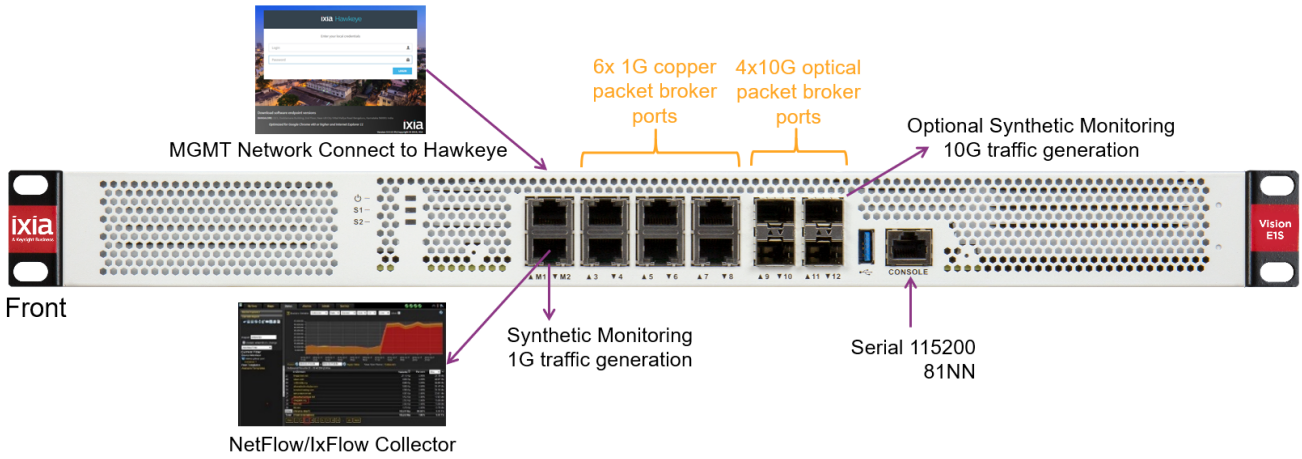
1. Select **Administration** > **Preferences** > **Traffic Port Management** and then choose one of the following from **Vision E1S Firewall Configure** drop-down list.
   - **Secure**: Recommended when *not* performing Active Monitoring Node to Node Test, this option closes all the ports (except for ssh and dhcpv6-client protocols), and the Vision E1S device acts as private probe to any public probe. You cannot pass traffic between two Vision E1S devices by using this mode when performing Active Monitoring Node to Node Tests.

     NOTE Secure mode is intended for use when the Vision E1S is being used for NetStack and AppStack operations with the capability of running Active Monitoring Real Service tests and private to public Node to Node tests (private to public as noted on the Probe Management Screen or on the SYSTEM tab of the Vision E1S.)

   - **Configure**: This option helps you configure the firewall based on the option you choose from **Destination Port Conf Option** drop-down list.
     - **0**: This option shuts down the local firewall opening all ports on all management and Active Monitoring interfaces.
     - **1** and **2**: Recommended when performing Active Monitoring Node to Node Tests, these options open the port range you specify in the **First Destination Port** and **Last Destination Port** for all management and Active Monitoring interfaces.
2. Select the **SAVE** button.

Vision E1S Port Mapping and System Performance

The following figure shows the port mapping to stacks and the system performance.



Port Mapping

- Two 1G management ports for connection to the Hawkeye server (**M1** for LAN1, and **M2** for LAN2)
- Management ports can also be used for:
  - Active monitoring
  - NetFlow/IxFlow generation to a flow collector
- Six (6) 1G copper ports for packet broker use
- Four (4) 10G ports for packet broker use
  - These ports are 10G only.
- Configurable for Hawkeye traffic generation
  - Use management port **M2** for 1Gbps traffic
  - One of the 10G ports for 10Gbps traffic (reserved)

System Performance

Performance may vary with use of multiple functions simultaneously and based on the incoming traffic mixes on the NetStack and AppStack functions.

<table>
<tr><td rowspan="8">NetStack/PacketStack</td><td colspan="3">Lossless Traffic Ingress to Egress</td></tr>
<tr><td>Packet Size</td><td>1G Interface</td><td>10G Interface</td></tr>
<tr><td>IMIX *</td><td>Line rate</td><td>Line rate</td></tr>
<tr><td>64 bytes</td><td>0.6 Gbps</td><td>1.5 Gbps</td></tr>
<tr><td>256 bytes</td><td>0.9 Gbps</td><td>5.6 Gbps</td></tr>
<tr><td>512 bytes</td><td>Line rate</td><td>9.0 Gbps</td></tr>
<tr><td>1024 bytes</td><td>Line rate</td><td>Line rate</td></tr>
<tr><td>1518 bytes</td><td>Line rate</td><td>Line rate</td></tr>
<tr><td colspan="3">* IMIX traffic refers to typical internet traffic mix. For benchmarks, the following repartition was used: 17% of 64-byte packets, 51% of 512-byte packets, 32% of 1518-byte packets.</td></tr>
<tr><td>AppStack</td><td colspan="3">Up to 2 Gbps of typical application mixed traffic.</td></tr>
<tr><td>Active Monitoring</td><td colspan="3">Up to line rate for 1G and 10G interfaces for TCP and UDP.</td></tr>
</table>

Select the Hawkeye Application Landing Page

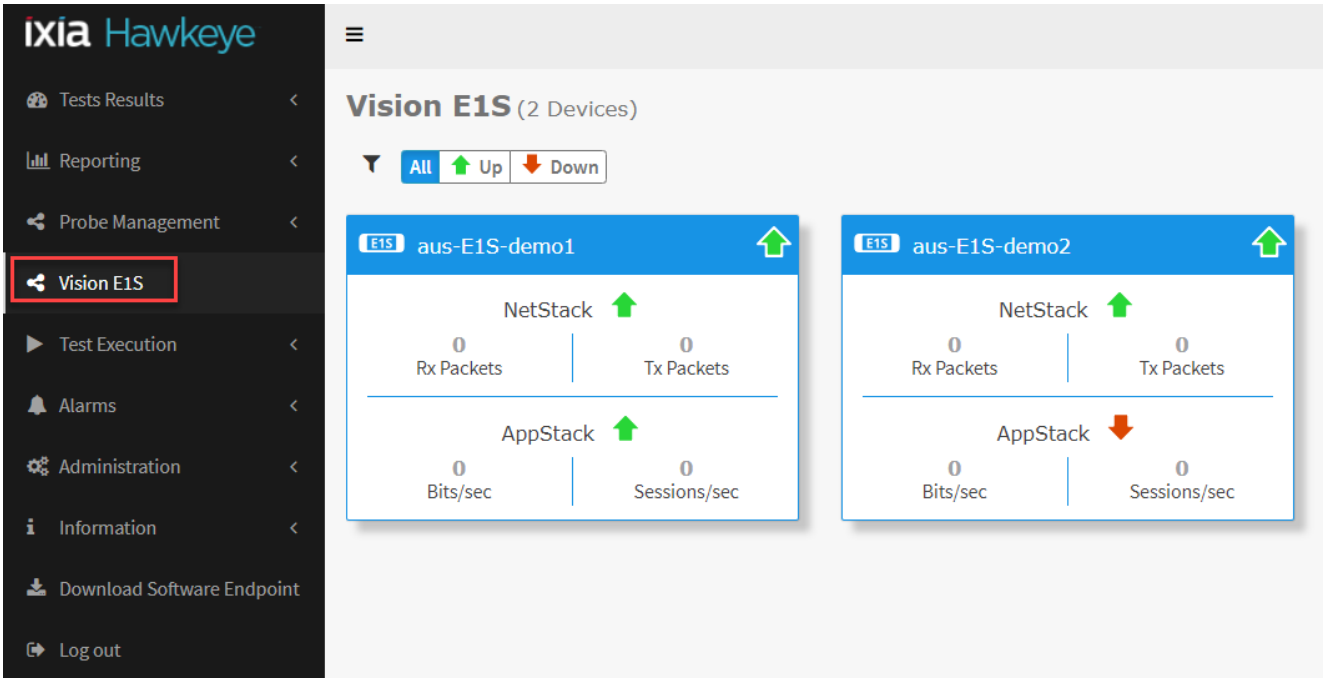
You must have both the Hawkeye and Vision E1S licenses installed to set you your landing page after user log in. This is global to any user.

To set the start page, complete the following steps:

1. Select **Administration** > **Preferences** > **Vision E1S** and then choose one of the following:
   - **Main Dashboard**: This options sets **Main Dashboard** as your start page.
   - **Vision E1S**: This options sets **Vision E1S** as your start page
2. Select the **SAVE** button.

Vision E1S Page

On this page, you can view the status of all the Vision E1S devices you have installed.



- **Green** arrow means the device is up and running.
- **Red** arrow means the device is down or not configured – for example, the AppStack for demo2 in the figure above is not configured.
- **Yellow** arrow means there is a service on the Vision E1S that is not working.

Vision E1S uses 2 ports to connect to the Hawkeye server:

- **TCP Port 443** (from the Vision E1S to the Hawkeye server)—this is required for the remote configuration of all Vision E1S management, and it is *mandatory* for any Vision E1S operations.
- **TCP port 10117** (from the Vision E1S to the Hawkeye server)—this is required for running active monitoring and Node to Node. It is only necessary if the Vision E1S is used for active monitoring with Node to Node tests.

Vision E1S Use Cases

The following use cases show how the Vision E1S can benefit you:

Configure Vision E1S Use Case 1 ..... **28**

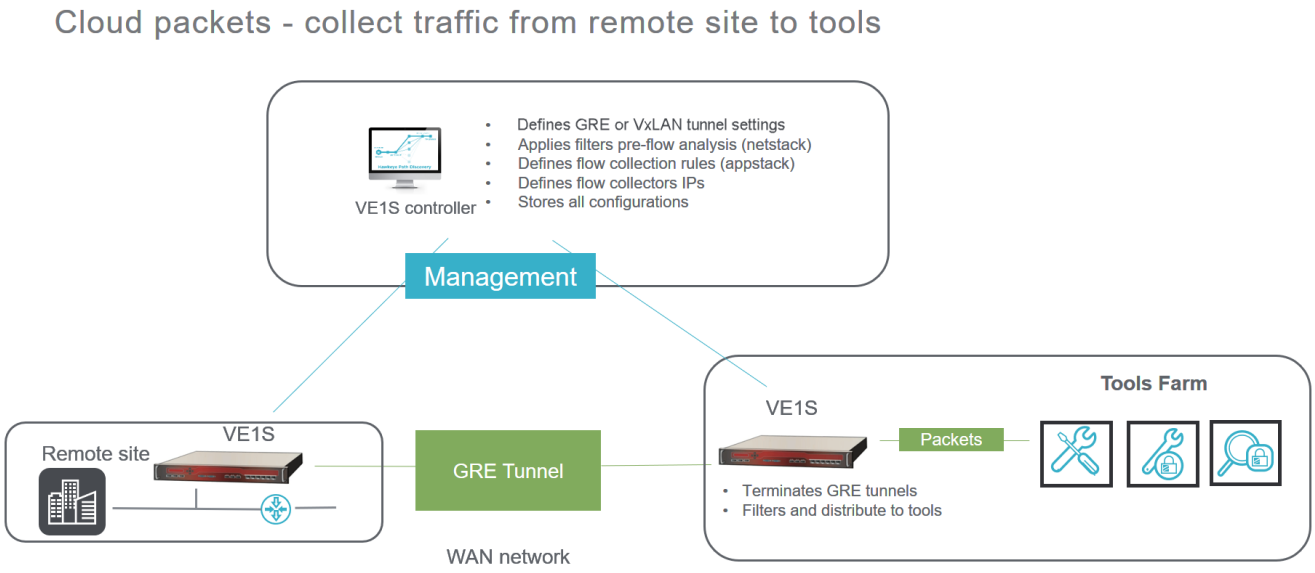
Configure Vision E1S Use Case 1 ..... **31**

Configure Vision E1S Use Case 2 ..... **35**

Configure Vision E1S Use Case 3 ..... **37**

Configure Vision E1S Use Case 4 ..... **41**

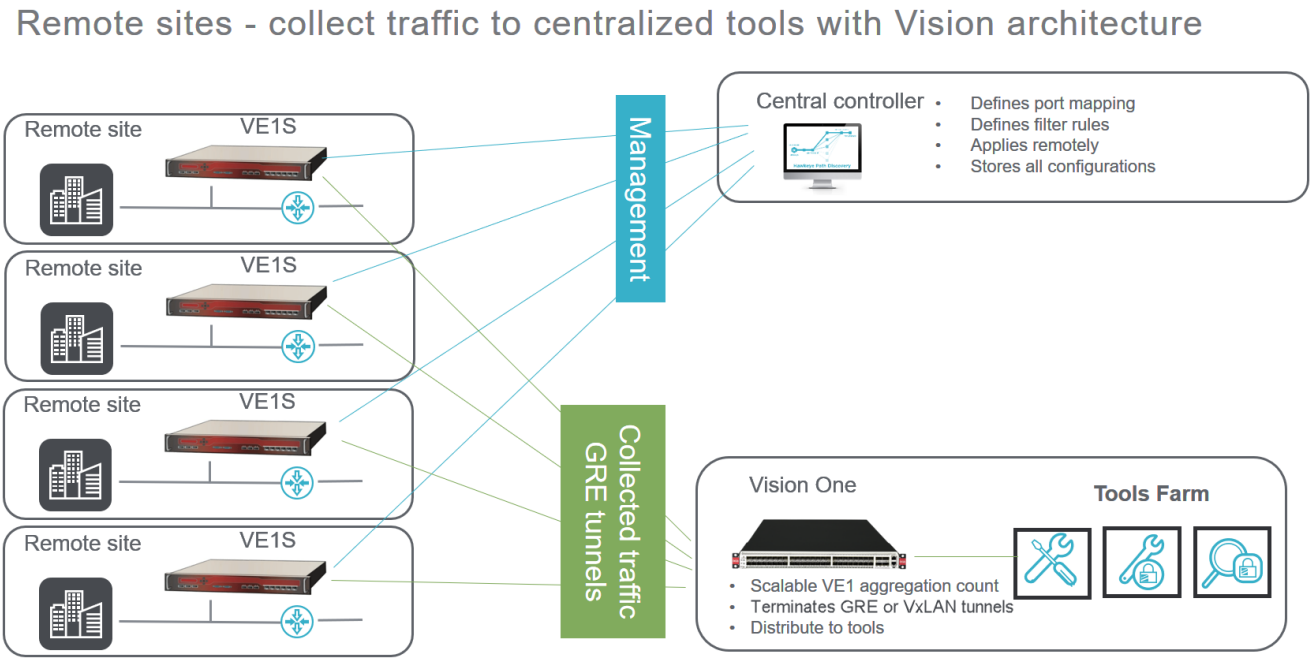
Use Case 1



Use case 1 does not require a filter, although you can apply a filter to either limit the amount of traffic sent into the GRE tunnel or to aggregate which packets come out of the GRE tunnel and go to the tools you designate. Use the NetStack configuration table to configure GRE by changing the ingress (GRE termination) or egress (GRE origination) from port Mode **Raw** to port Mode **IP Enabled**.

See Configure Vision E1S Use Case 1 on page 28.

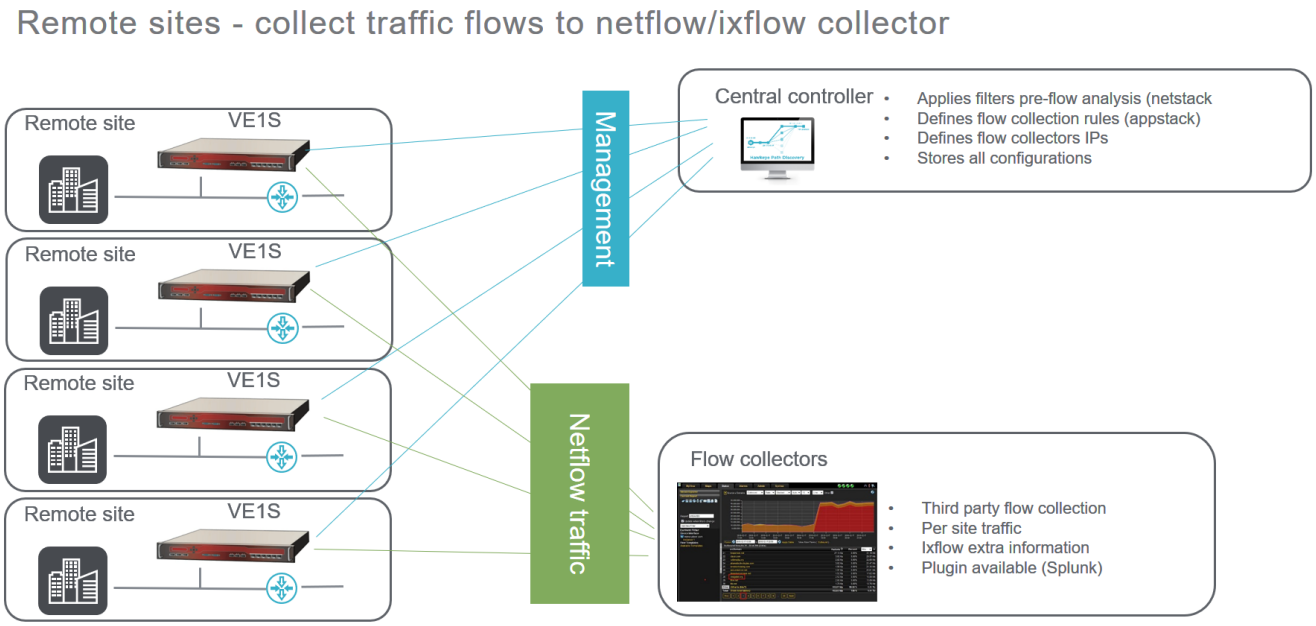
Use Case 2



Use case 2 is similar to use case 1 but requires you to configure multiple ports on the ingress side of the Tools Farm network packet broker (a Vision ONE in the image above) with one Tool/Egress port configuration on each of the Remote site Vision E1S devices.

See Configure Vision E1S Use Case 1 on page 31.

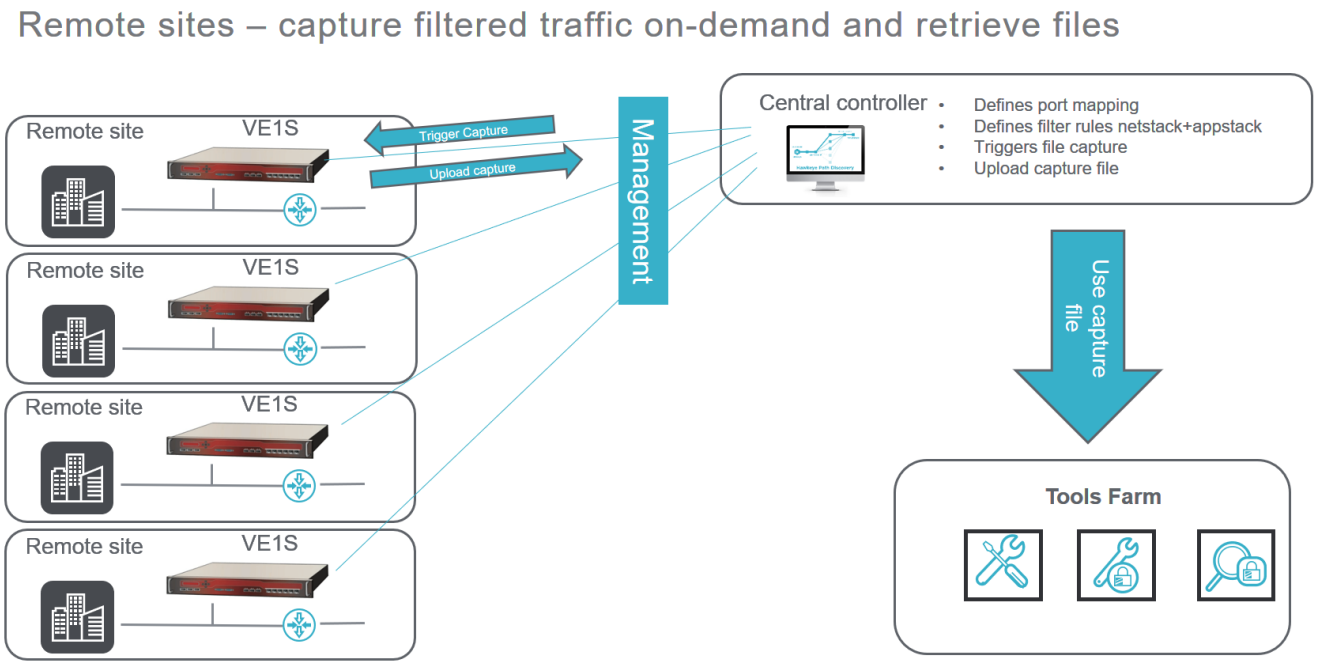
Use case 3



For use case 3, configure the **NetStack** tab on the Vision E1S devices to ingress data from the remote site taps and egress it to **AppStack**. Configure the **AppStack** > **Settings** tab for NetFlow / IxFlow and NetFlow collectors for traffic flowing from the Vision E1S to the NetFlow collectors. Configure the **AppStack** > **Filters** tab to filter out what is needed to be converted to NetFlow and sent to NetFlow collectors.

See Configure Vision E1S Use Case 2 on page 35.

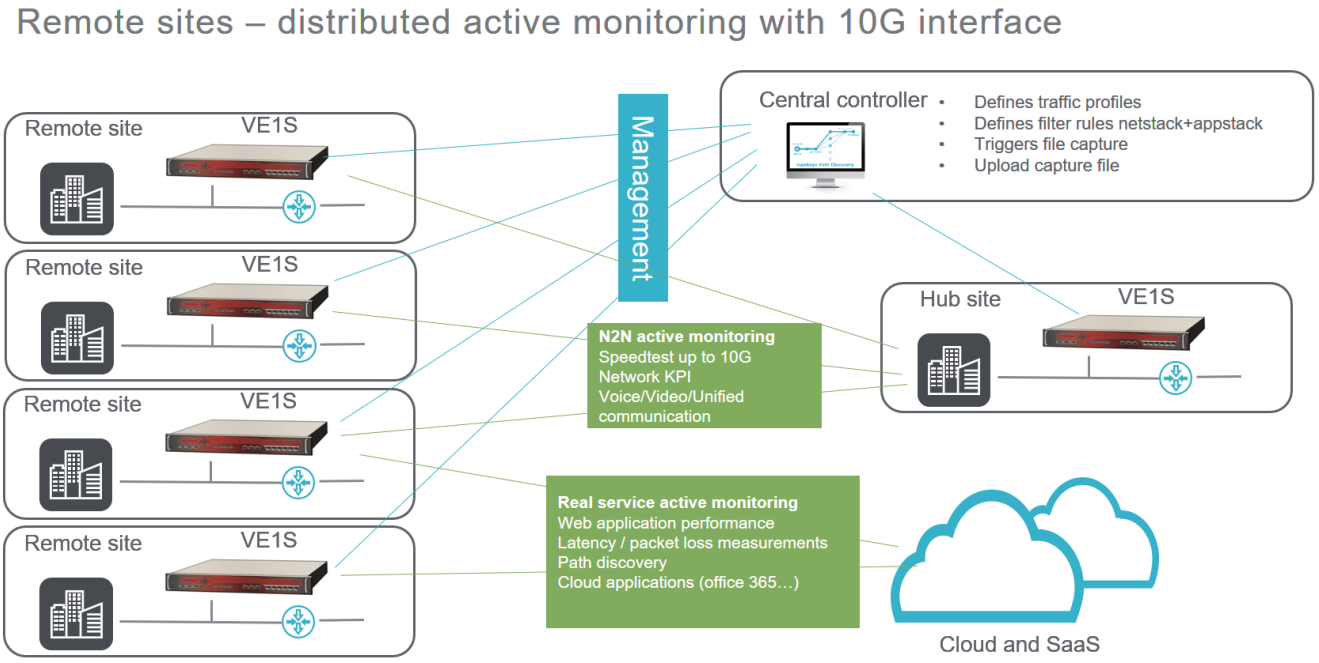
Use Case 4



Use case 4 is similar to use case 3 for NetStack configuration. Configure an AppStack filter and then generate a PCAP from the AppStack component based on a filter of 100MB or less. After that, you can download the PCAP from the Hawkeye user interface (UI) to use it in other tools.

See Configure Vision E1S Use Case 3 on page 37.

Use Case 5



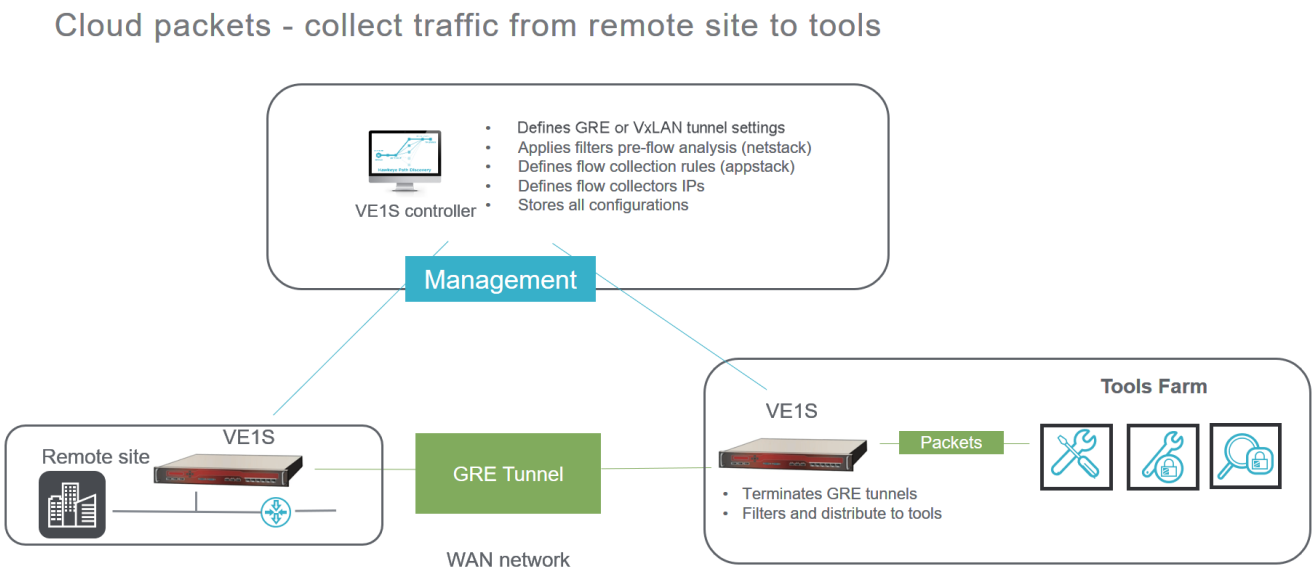
For use case 5, use the Hawkeye UI to perform 10G active monitoring, where you configure Real Service and Node to Node tests.

For Node to Node tests, choose the IP of the 10G interface and route from the 10G interface to the opposite side of the Node to Node test.

Real Service tests depend on the default route in the Vision E1S device. If the default route is set on the 10G interface, then you can run all Real Service tests of the 10G interface without any additional configuration.

See Configure Vision E1S Use Case 4 on page 41.

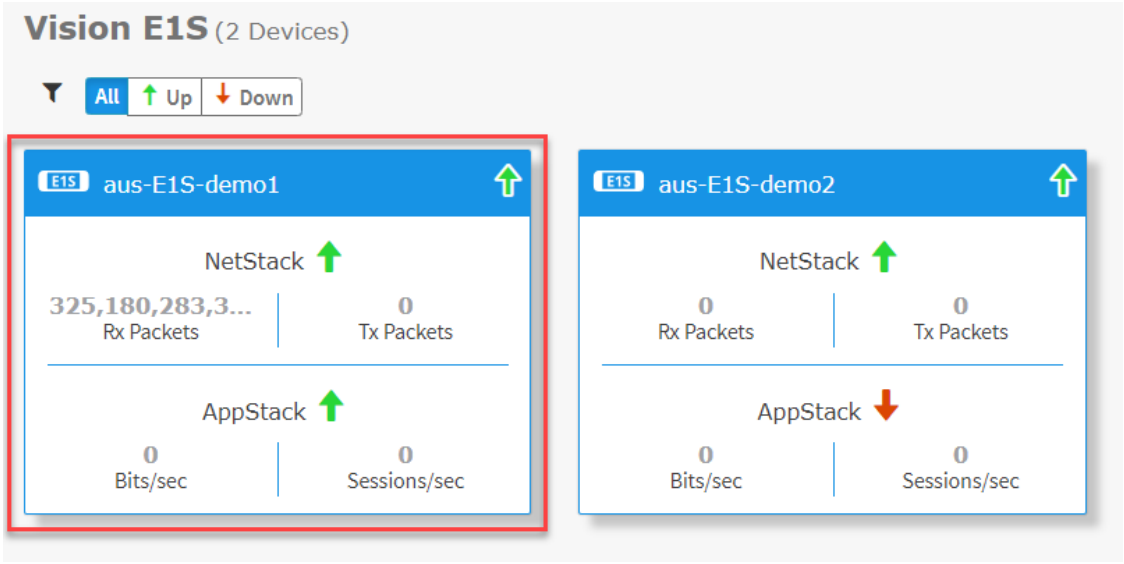
Configure Vision E1S Use Case 1



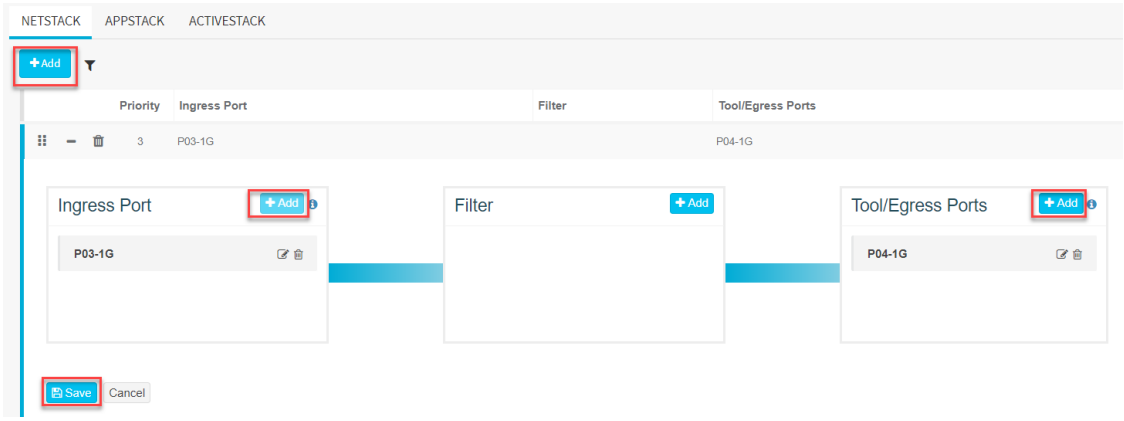
Use case 1 does not require a filter, although you can apply a filter to either limit the amount of traffic sent into the GRE tunnel or to aggregate which packets come out of the GRE tunnel and go to the tools you designate. Use the NetStack port configuration table to configure GRE by changing the Ingress Port (GRE termination) or Tool/Egress Port (GRE origination) from port Mode **Raw** to port Mode **IP Enabled**.

To configure use case 1:

1. Select the relevant remote site Vision E1S Network Packet Broker (NPB).



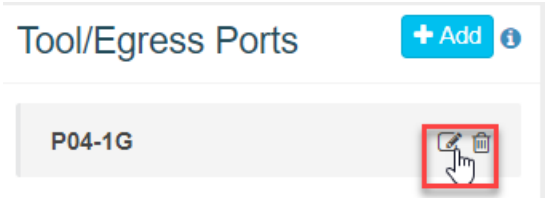
2. On the **NetStack** tab, select **Add**.
   The Ingress Port, Filter, and Tool/Egress Ports appear.



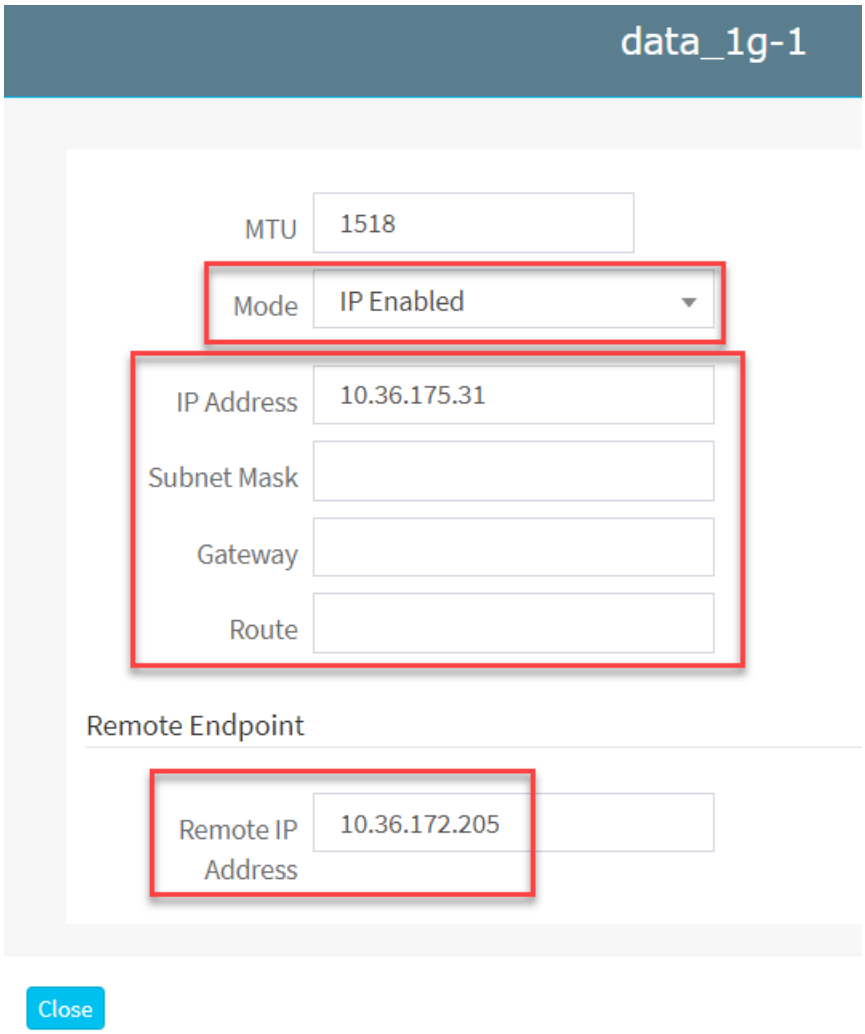
3. For the Ingress and Tool/Egress Ports, select **Add** and select a port – for example, Ingress Port P03-1G and Tool/Egress Port P04-1G.

   NOTE To configure ports, the Vision E1S requires a port pair, that is, both an Ingress port and a Tool/Egress port.

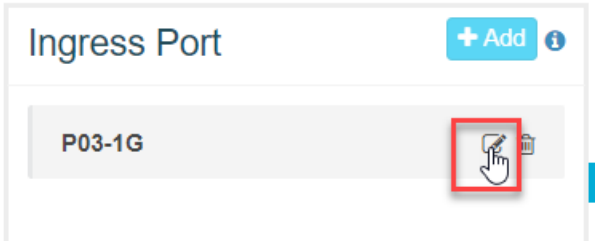
4. For the Tool/Egress Port, select the edit icon.



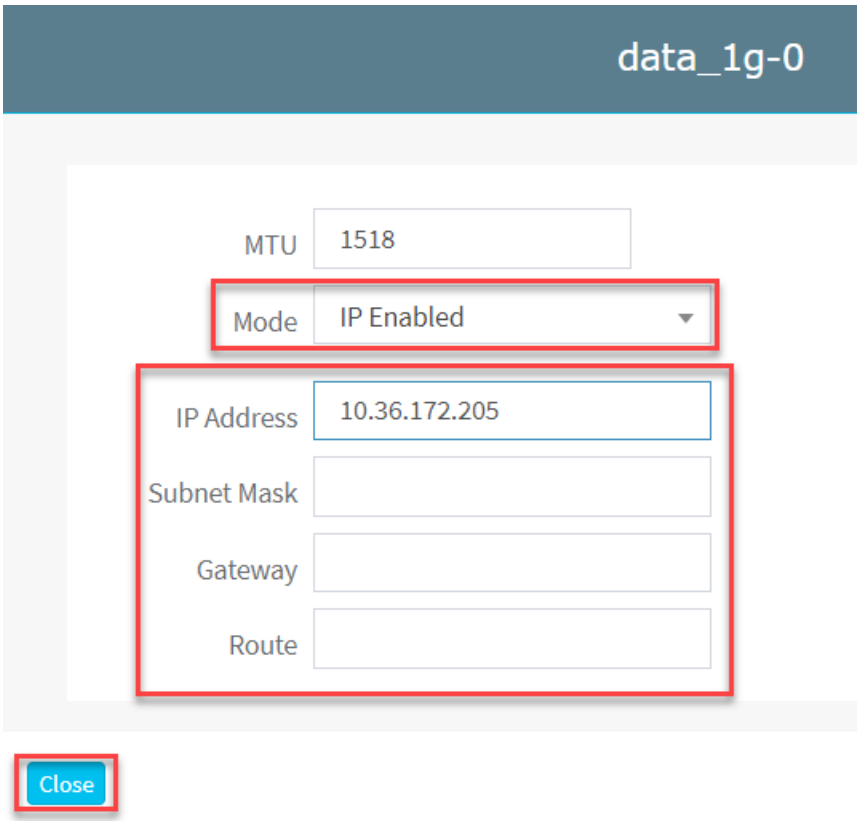
5. Open the **Mode** drop-list and select **IP Enabled**.



6. For this Vision E1S, enter the **IP Address**, **Subnet Mask**, **Gateway**, and **Route**.
7. For the Tools Farm Vision E1S (the Remote Endpoint), enter the **Remote IP Address**.
   This creates a GRE tunnel from this port to the Remote Endpoint (the Tools Farm Vision E1S).
8. Select **Close**.
9. Select **Save** to save this configuration on the Remote site Vision E1S.
10. On the Tools Farm Vision E1S, to terminate the GRE tunnel, open a NetStack Ingress Port.

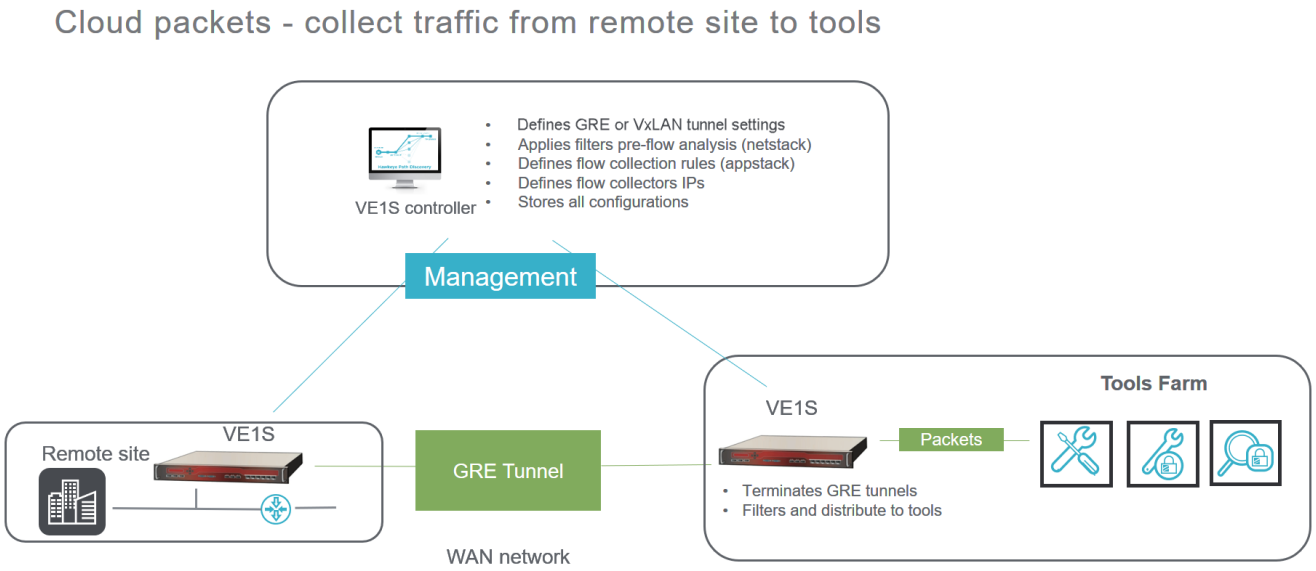


11. Open the **Mode** drop-list and select **IP Enabled**.



12. Enter the **IP Address**, **Subnet Mask**, **Gateway**, and **Route** for this Vision E1S.
13. Select **Close**.
14. Select **Save** to save this configuration on the Tools Farm Vision E1S.

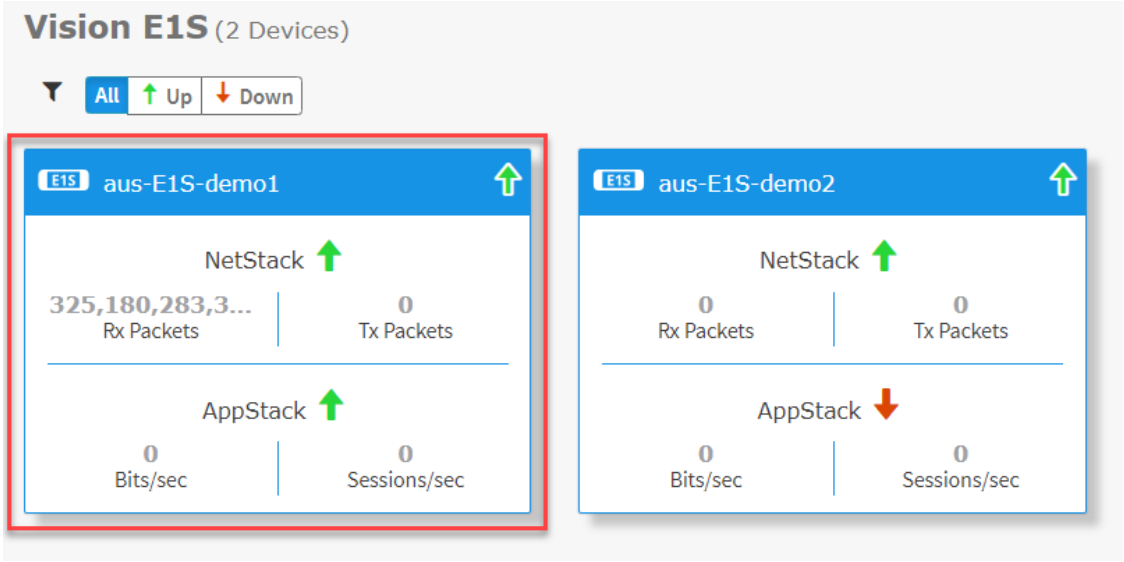
Configure Vision E1S Use Case 1



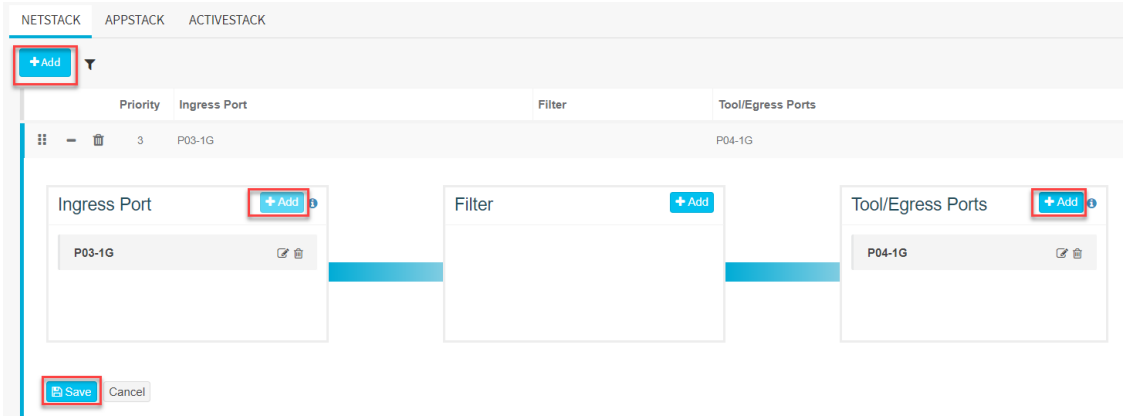
Use case 1 does not require a filter, although you can apply a filter to either limit the amount of traffic sent into the GRE tunnel or to aggregate which packets come out of the GRE tunnel and go to the tools you designate. Use the NetStack port configuration table to configure GRE by changing the Ingress Port (GRE termination) or Tool/Egress Port (GRE origination) from port Mode **Raw** to port Mode **IP Enabled**.

To configure use case 1:

1. Select the relevant remote site Vision E1S Network Packet Broker (NPB).



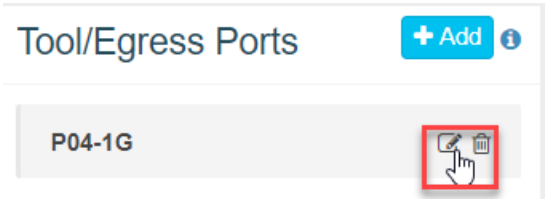
2. On the **NetStack** tab, select **Add**.
   The Ingress Port, Filter, and Tool/Egress Ports appear.



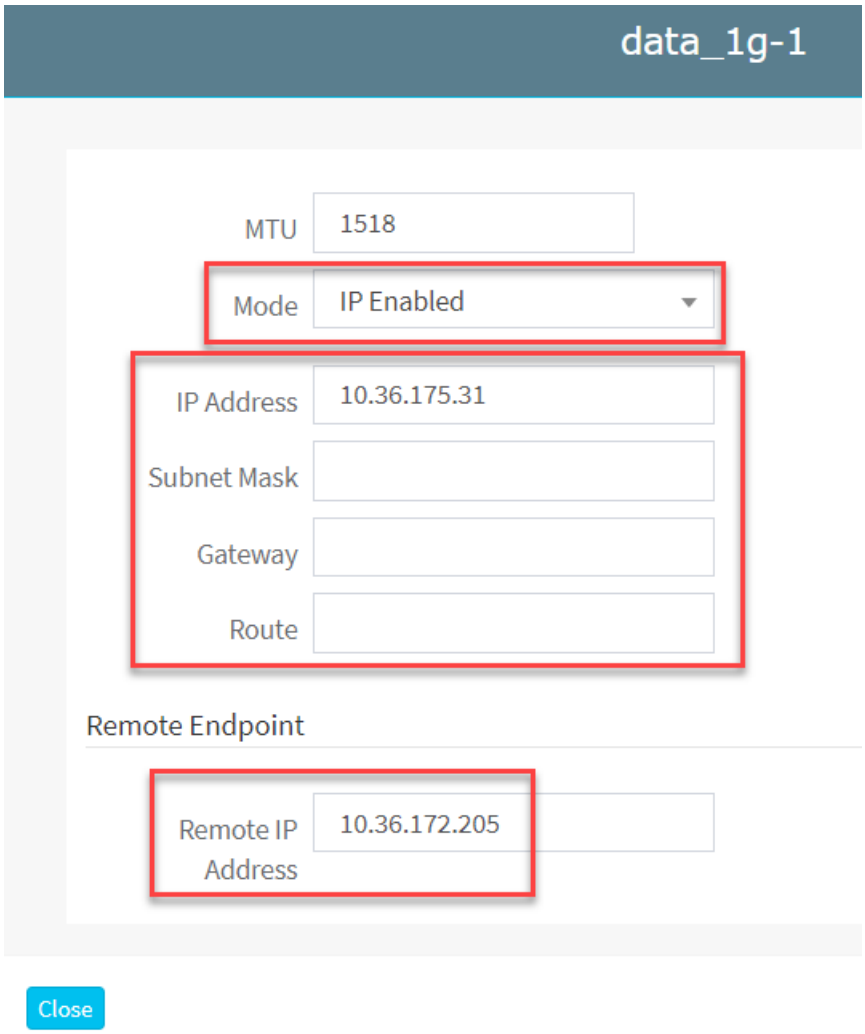
3. For the Ingress and Tool/Egress Ports, select **Add** and select a port – for example, Ingress Port P03-1G and Tool/Egress Port P04-1G.

   NOTE To configure ports, the Vision E1S requires a port pair, that is, both an Ingress port and a Tool/Egress port.

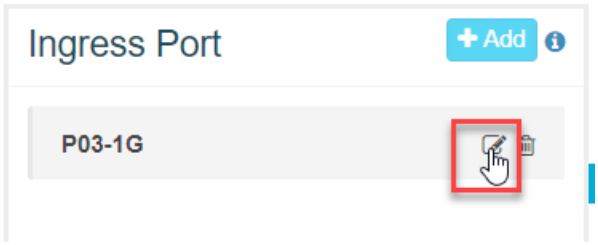
4. For the Tool/Egress Port, select the edit icon.



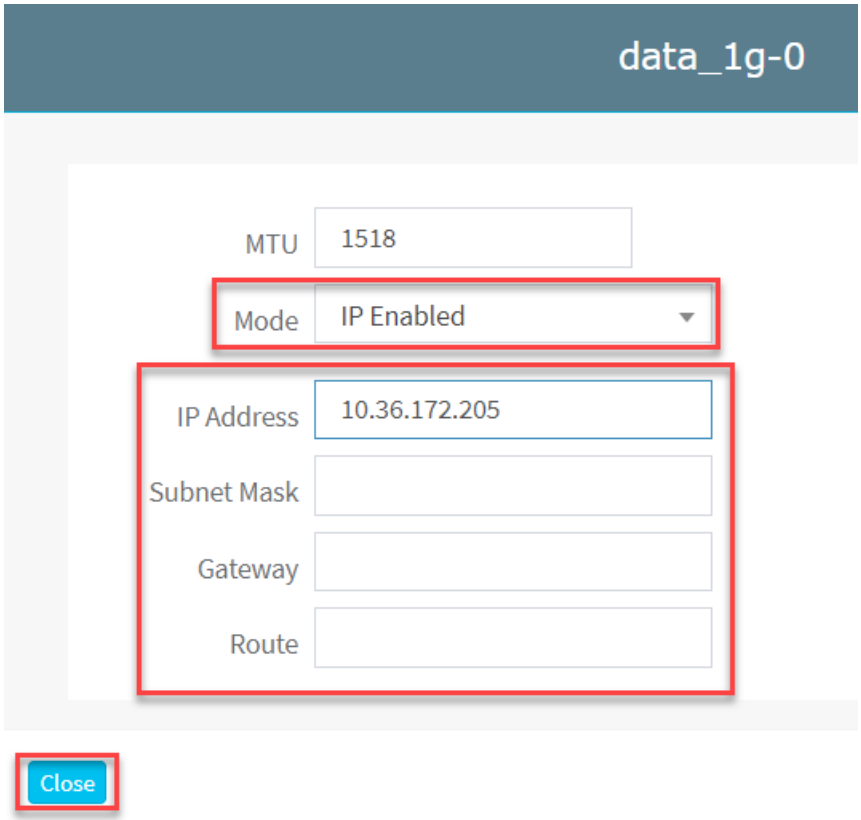
5. Open the **Mode** drop-list and select **IP Enabled**.



6. For this Vision E1S, enter the **IP Address**, **Subnet Mask**, **Gateway**, and **Route**.
7. For the Tools Farm Vision E1S (the Remote Endpoint), enter the **Remote IP Address**.
   This creates a GRE tunnel from this port to the Remote Endpoint (the Tools Farm Vision E1S).
8. Select **Close**.
9. Select **Save** to save this configuration on the Remote site Vision E1S.
10. On the Tools Farm Vision E1S, to terminate the GRE tunnel, open a NetStack Ingress Port.

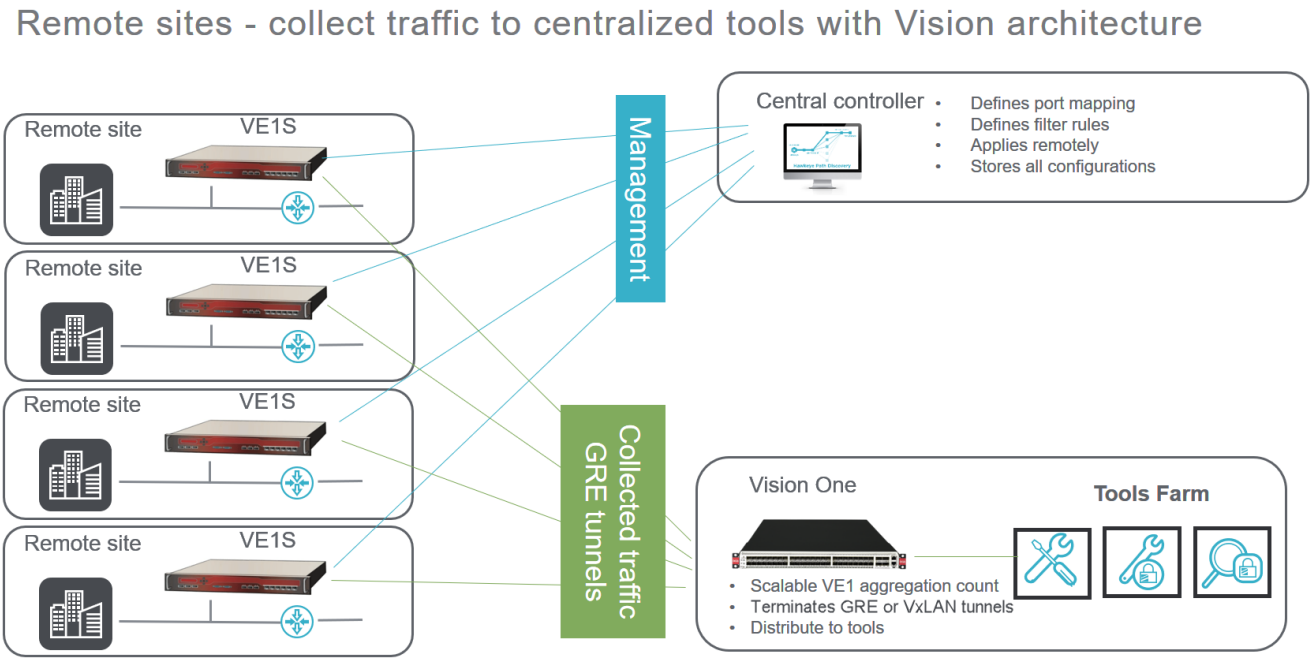


11. Open the **Mode** drop-list and select **IP Enabled**.



12. Enter the **IP Address**, **Subnet Mask**, **Gateway**, and **Route** for this Vision E1S.
13. Select **Close**.
14. Select **Save** to save this configuration on the Tools Farm Vision E1S.

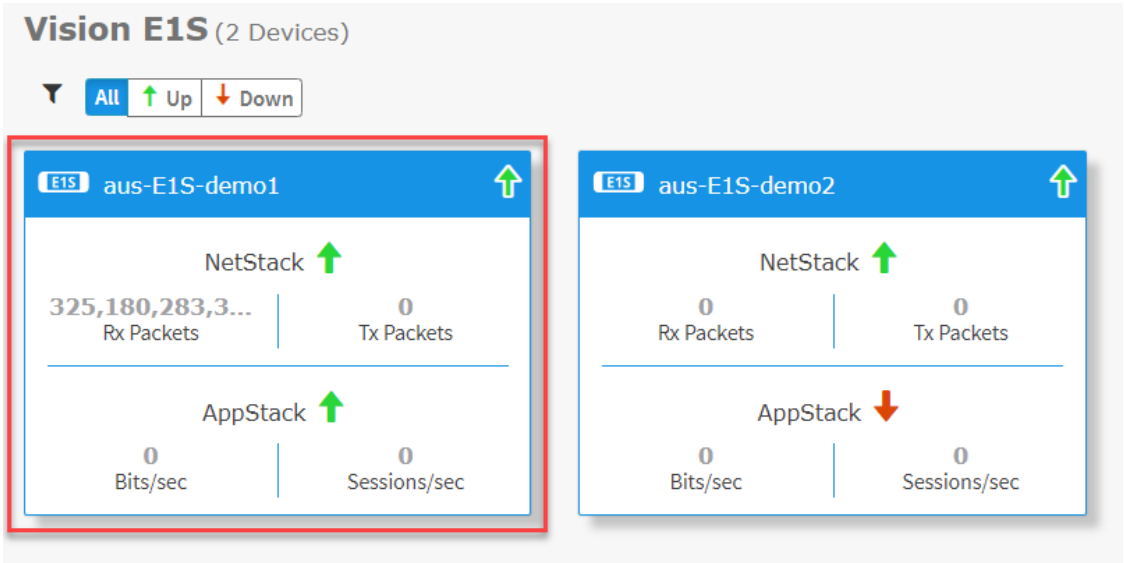
Configure Vision E1S Use Case 2



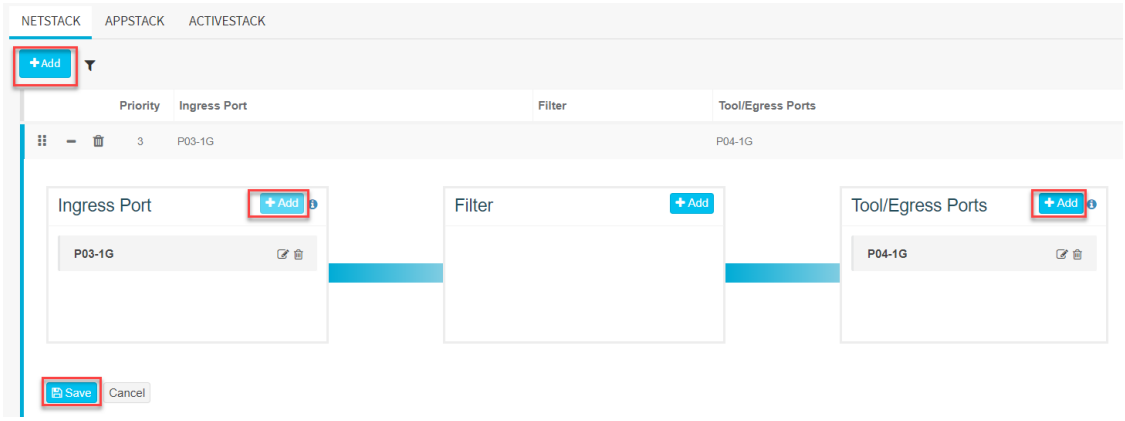
Use case 2 is similar to use case 1 but requires you to configure multiple ports on the ingress side of the Tools Farm network packet broker (a Vision ONE in the image above) with one egress port configuration on each of the Remote site Vision E1S devices.

To configure one egress port on each of the Remote site Vision E1S devices:

1. Select the relevant remote site Vision E1S Network Packet Broker (NPB).



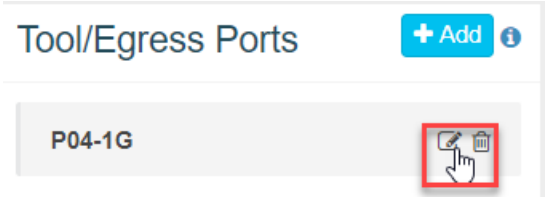
2. On the **NetStack** tab, select **Add**.
   The Ingress Port, Filter, and Tool/Egress Ports appear.



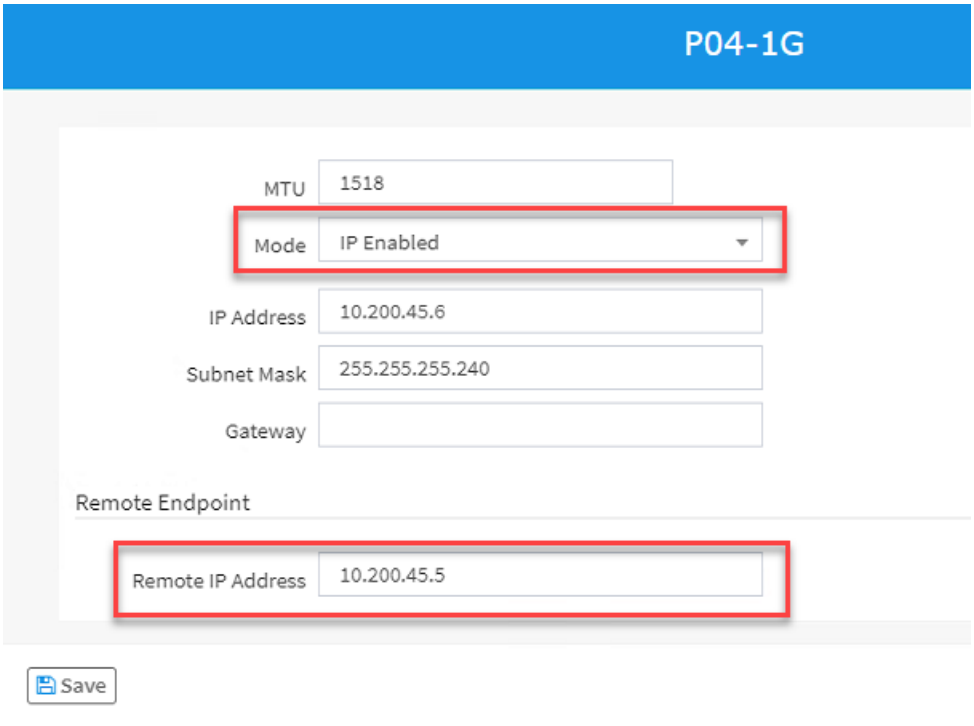
3. For the Ingress and Tool/Egress Ports, select **Add** and select a port – for example, Ingress Port P03-1G and Tool/Egress Port P04-1G.

   NOTE To configure ports, the Vision E1S requires a port pair, that is, both an Ingress port and a Tool/Egress port.

4. For the Tool/Egress Port, select the edit icon.



5. Open the **Mode** drop-list and select **IP Enabled**.



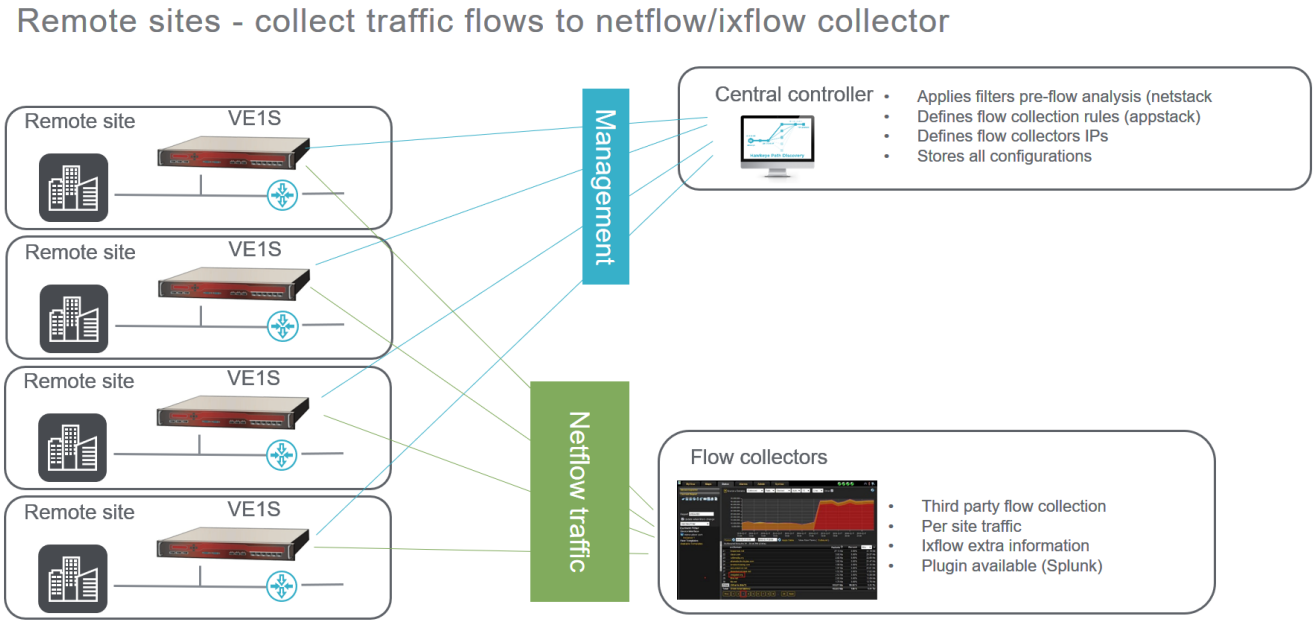
6. For this Vision E1S, enter the **IP Address**, **Subnet Mask**, **Gateway**, and **Route**.

7. For the Tools Farm Vision E1S (the Remote Endpoint), enter the **Remote IP Address**.
   This creates a GRE tunnel from this port to the Remote Endpoint (the Tools Farm Vision E1S).
8. Select **Close**.
9. Select **Save** to save this configuration on the Remote site Vision E1S.

To configure the ingress side of the Tools Farm Vision ONE network packet broker, see **Tunneling Tab (Network Ports Only)** in the *Ixia Vision ONE User Guide*, located on the Ixia Customer Support Portal.

- Select **User Guides** > **Vision Network Packet Broker (NPB)** > **Ixia Vision ONE User Guide**.

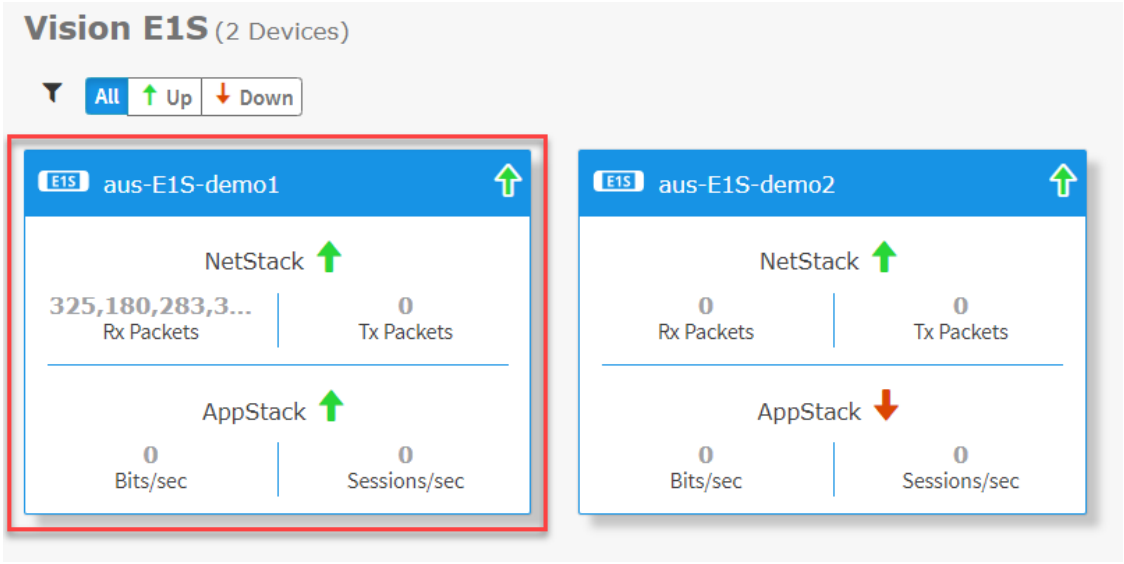
Configure Vision E1S Use Case 3



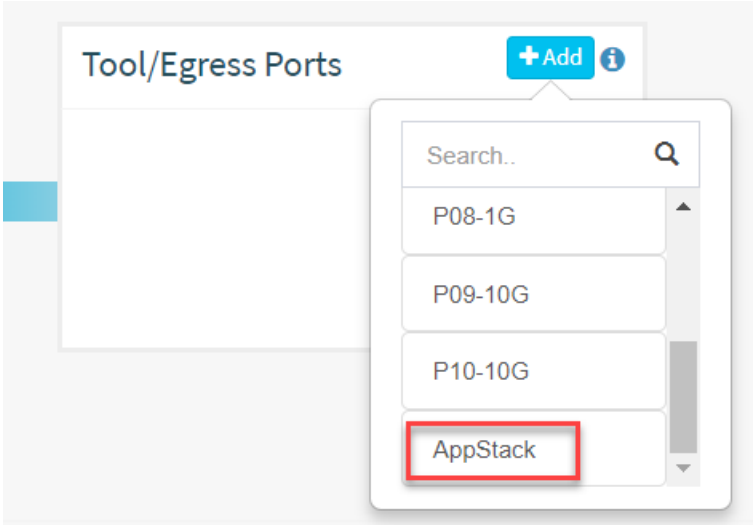
For use case 3, configure the **NetStack** tab on the Vision E1S devices to ingress data from the remote site taps and egress it to **AppStack**. Configure the **AppStack** > **Settings** tab for NetFlow / IxFlow and NetFlow collectors for traffic flowing from the Vision E1S to the NetFlow collectors. Configure the **AppStack** > **Filters** tab to filter out what is needed to be converted to NetFlow and sent to NetFlow collectors.

To configure use case 3:

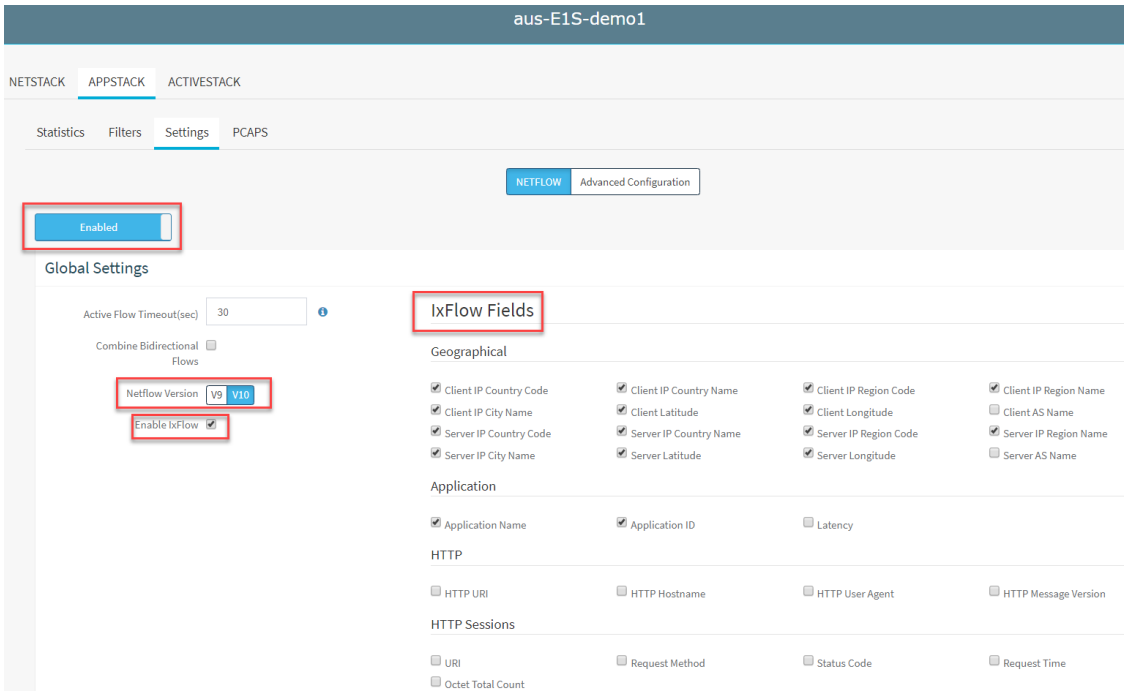
1. Select the relevant remote site Vision E1S Network Packet Broker (NPB).



2. On the **NetStack** tab, select **Add**.
   The Ingress Port, Filter, and Tool/Egress Ports appear.
3. For the Ingress Port, select **Add** and select the port where the tap is cabled into the Vision E1S – for example, Port P12-10G.
4. For the Tool/Egress Port, select **Add**, scroll down, and select **AppStack**.



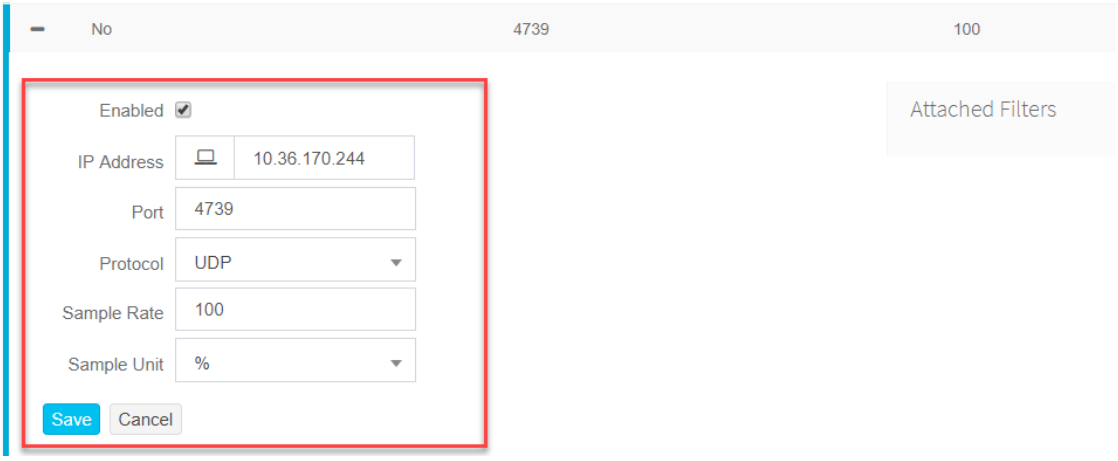
5. Select the **AppStack**> **Settings** tab.



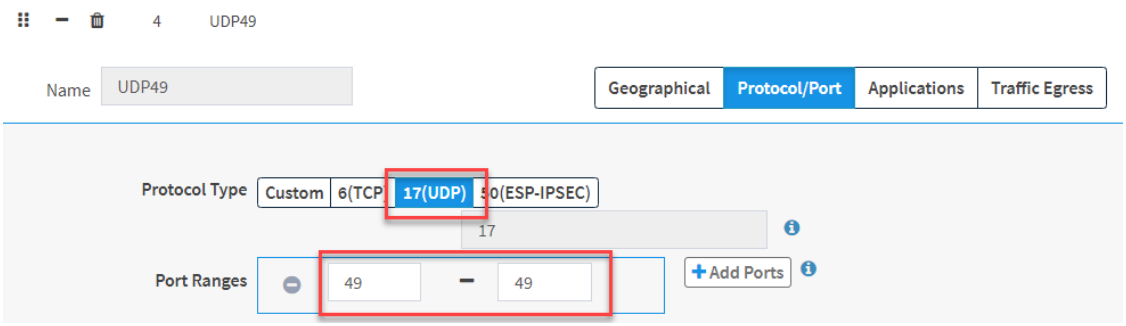
6. Select **Enabled**, **NetFlow Version**, **Enable IxFlow**, and the **IxFlow** fields you want to include.

   NOTE NetFlow Version 10 supports the IxFlow fields. If you select NetFlow Version 9, the IxFlow fields are grayed out (unselectable).

7. Select **Save** to save the Netflow Version and IxFlow fields.
8. Scroll down to **NetFlow Collectors** and open a + icon.



9. Select **Enabled** and enter an **IP address**, **Port**, **Protocol**, **Sample Rate**, and **Sample Unit**.
10. Select **Save**.
11. Select the **AppStack** > **Filters** tab.
12. Select **Add** and the appropriate filter – Geographical, Protocol/Port, or Applications – for example, **Protocol/Port**.

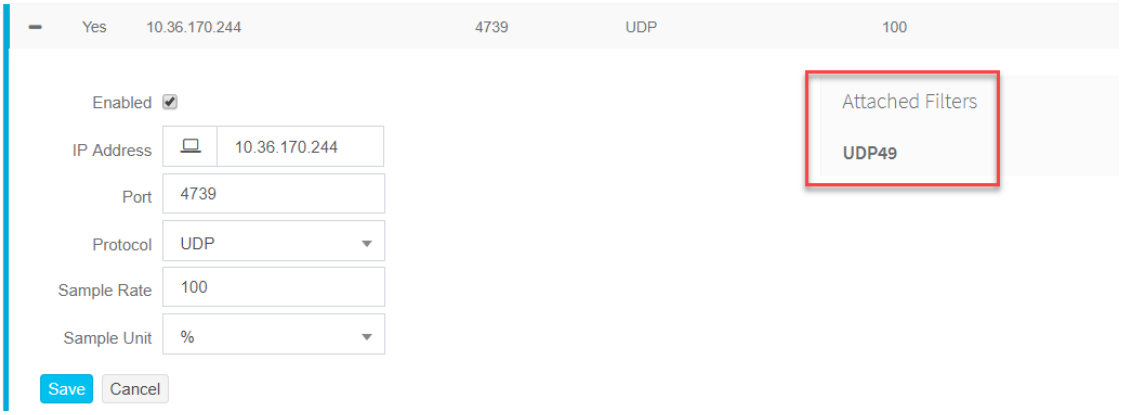


13. In the **Protocol Type** area, select a protocol – for example, **UDP**.
14. In the **Port Ranges** area, select a port or range of ports – for example, **49**.
15. Select **Traffic Egress**.
16. Select **NetFlow** and the relevant IP address you created in the **AppStack** > **Settings** tab for a **NetFlow Collector**.

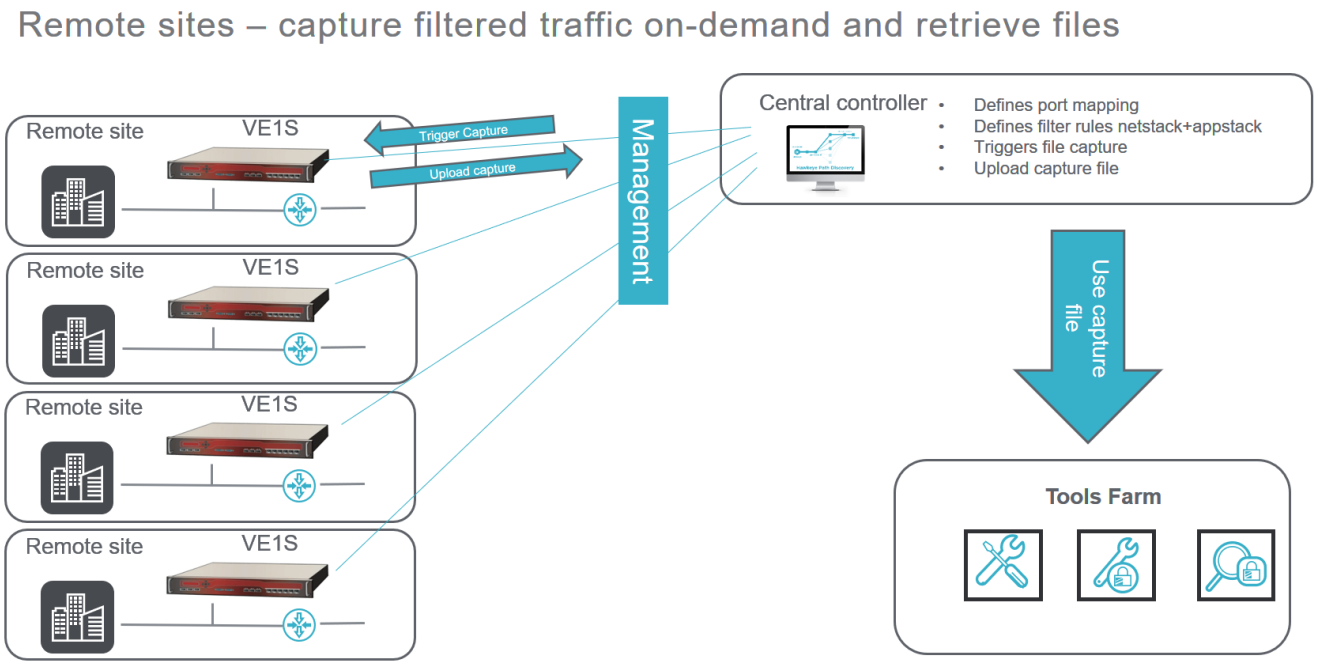
17. Enter a name for this filter – for example, **UDP49**.
18. Select **Save** to save this filter.

NOTE

If you return to the **AppStack** > **Settings** tab to the NetFlow collector whose IP address you just selected for this filter, you now see this filter as an Attached Filter.



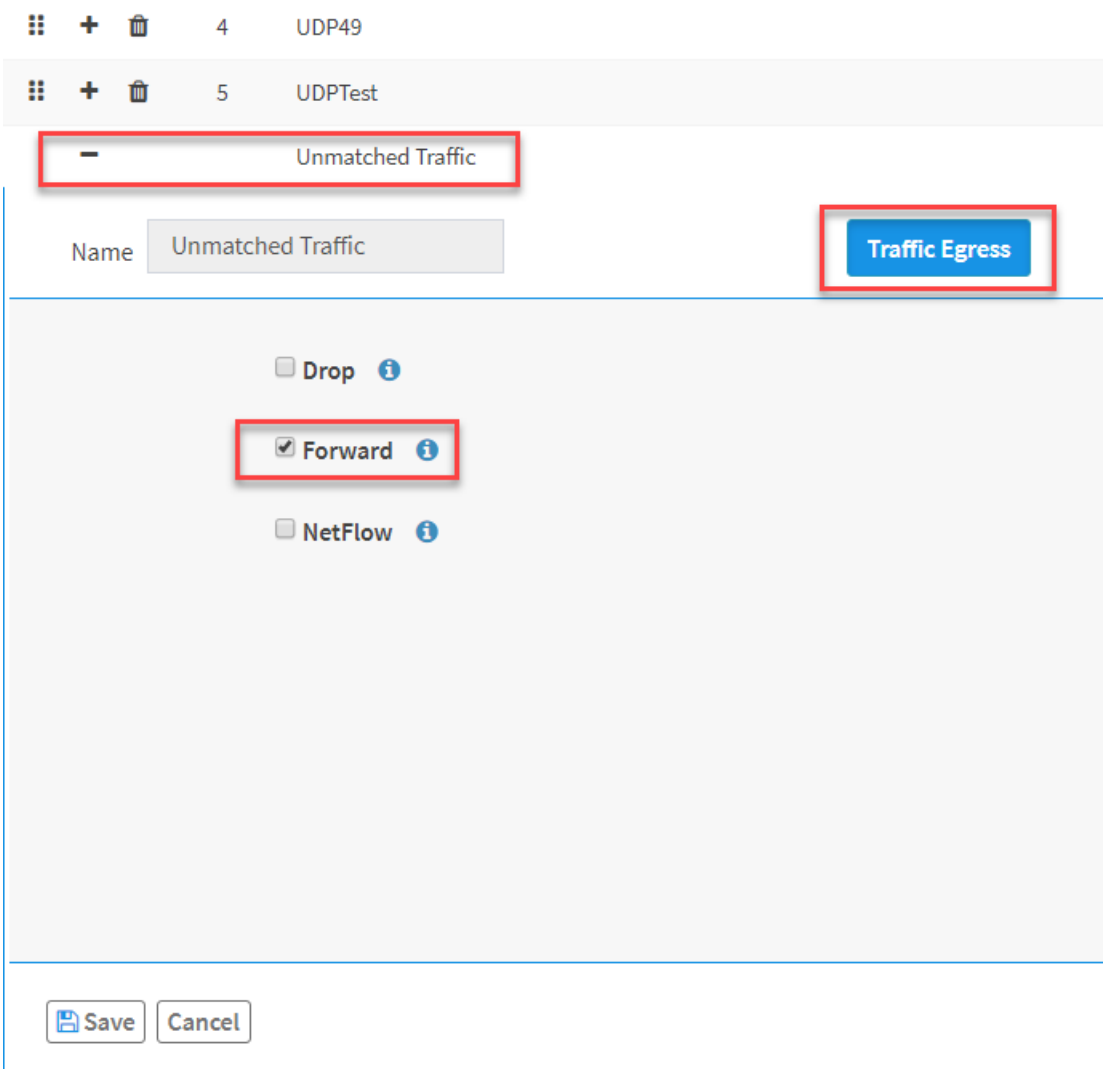
Configure Vision E1S Use Case 4



Use case 4 is similar to use case 3 for NetStack configuration. Configure an AppStack filter and then generate a PCAP from the AppStack component based on a filter of 100MB or less. After that, you can download the PCAP from the Hawkeye user interface (UI) to use it in other tools.

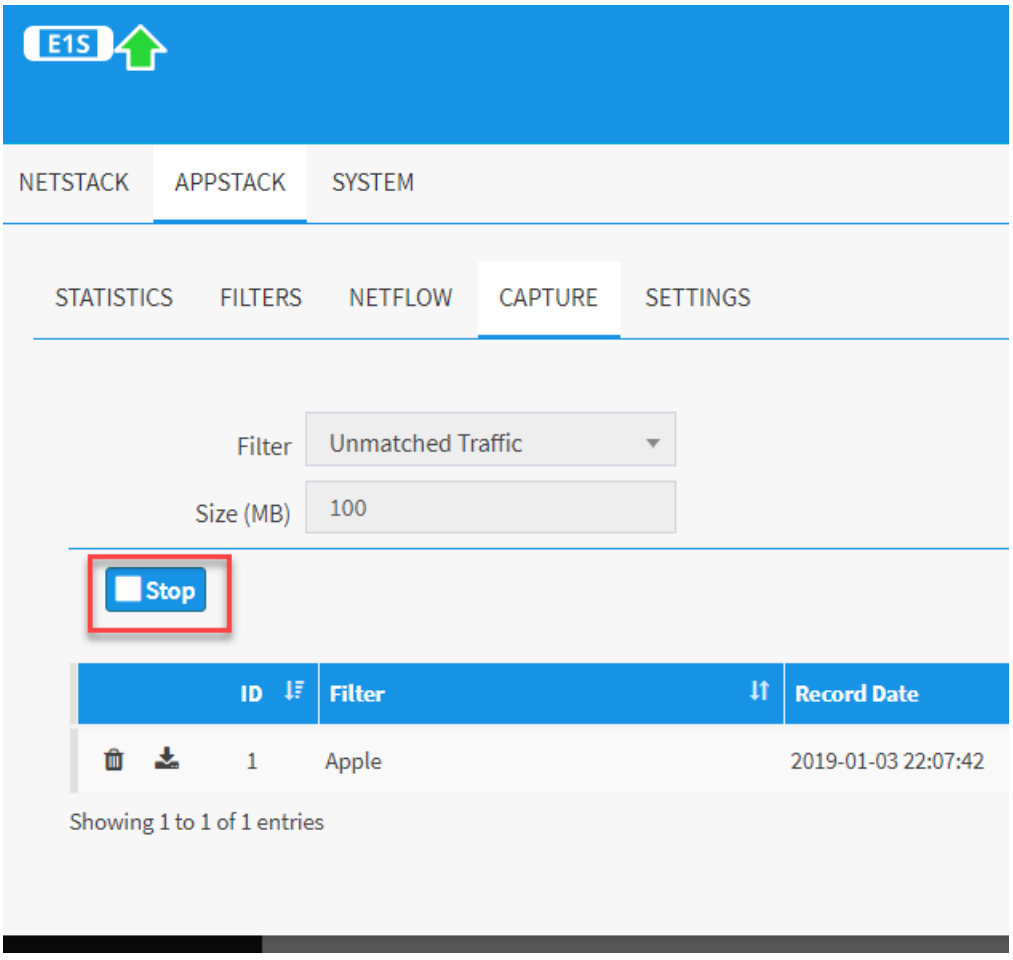
To configure use case 4:

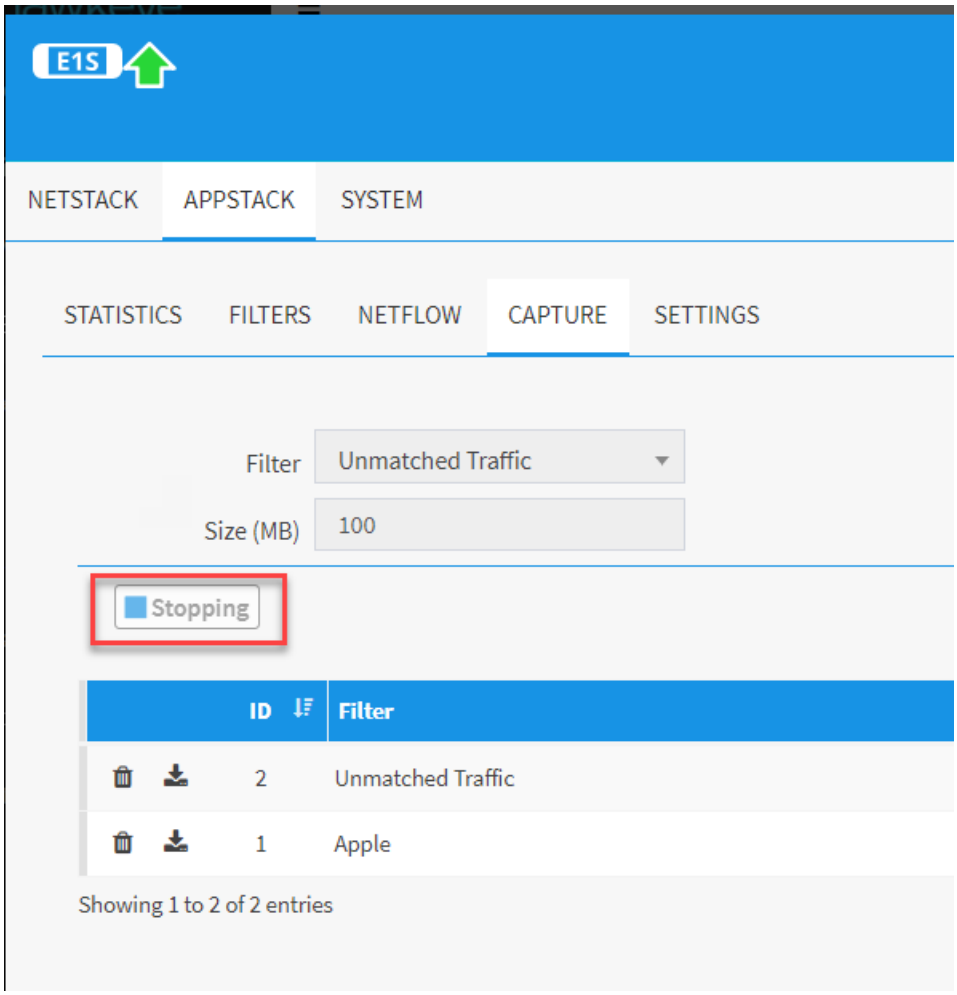
1. See use case 3 for the NetStack configuration.
2. Select the **AppStack** > **Filters** tab.
3. Create or open an AppStack filter - for example, **Unmatched Traffic**.



4. In this example, Traffic Egress is the only choice, but for other filters, select **Traffic Egress**.
5. Select **Forward**.
6. Select **Save** to save changes to this filter.
   Traffic now forwards from this Vision E1S filter to AppStack, where you can capture it in PCAPs.
7. Select the **Capture** tab.
8. Open the **Filter** drop-list and select a filter that forwards to AppStack - in our example, **Unmatched Traffic**.
9. Either accept the default 100MB **Size** or select or enter a smaller size for the PCAP.

10. Select **Start**.
11. The capture automatically stops when the file reaches the size limit you set, but you can select the **Stop** button sooner.





12. To download a PCAP file, select the download icon for the relevant capture file and save it to your PC or a network directory.

Configuring Vision E1S

The Vision E1S has multiple configuration options for NETSTACK and APPSTACK, which are available by selecting those tabs. On the SYSTEM tab, you can see Hawkeye server information and, if needed, reboot the selected Vision E1S.

Order of Operations for Configuring NETSTACK Traffic

To configure NETSTACK traffic, the following is the order of operations:

1. Add NETSTACK filters.
2. Map NETSTACK ports (one ingress and one or more egress ports).
3. Add one or more NETSTACK filters to the mapped ports.

Configure NETSTACK

The following are some of the ways you can configure NETSTACK traffic:

Use Vision E1S NetStack Filter Parameters **45**
Add NETSTACK Filters **48**
Map NETSTACK Ports, Limit Traffic, and Replicate It to Multiple Tools **50**
Terminate GRE tunnels **54**
Originate GRE Tunnels **55**
Terminate VxLAN Tunnels **56**
Originate VxLAN Tunnels **59**
Replicate Traffic **60**
Aggregate Traffic **61**
Deduplicate Packets **62**

Use Vision E1S NetStack Filter Parameters

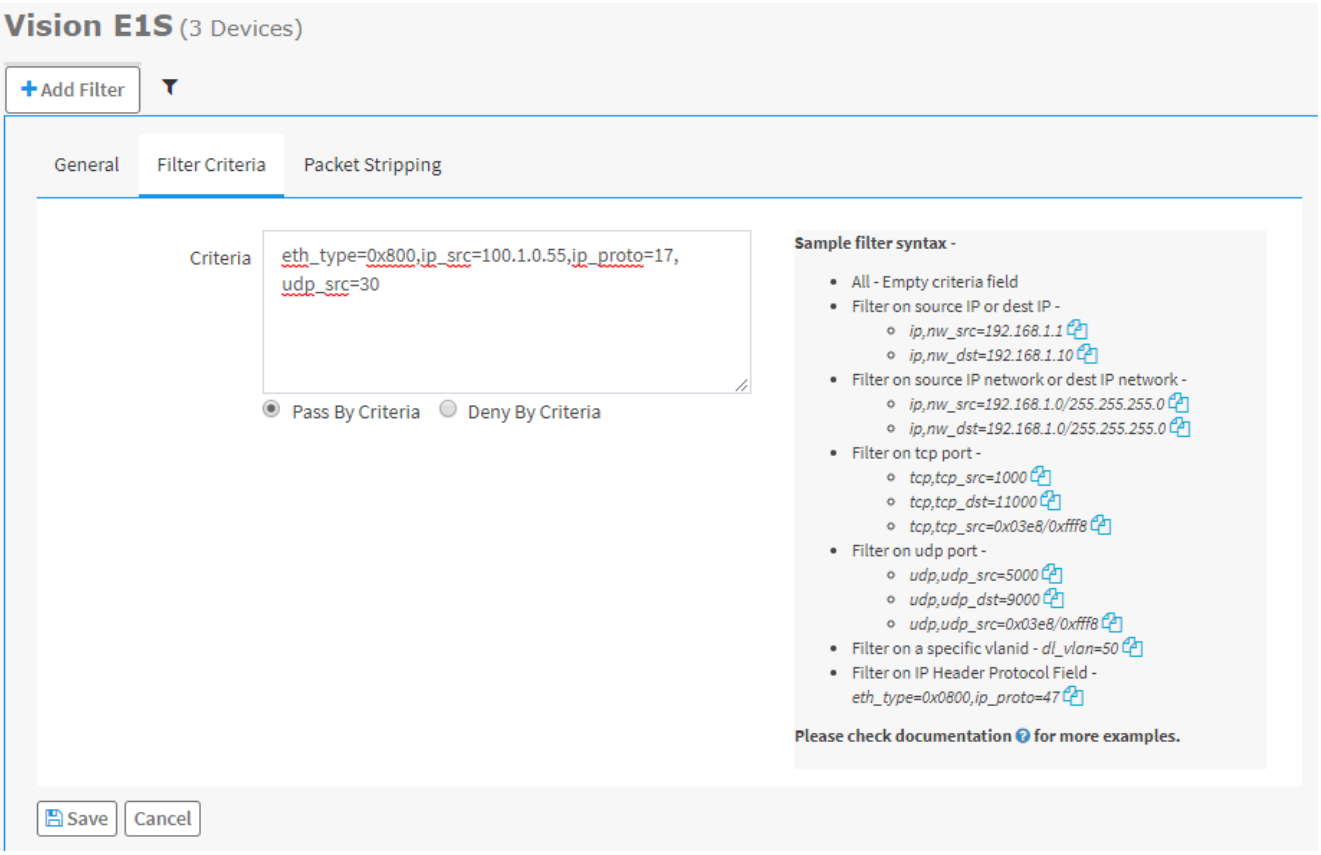
Many of the NetStack filter parameters require a prerequisite command to precede them with appropriate formatting and order. For example:

```
udp, udp_dst=0x3C/0xFF
< prerequisite from short hand list> , <filter type>=<Exact decimal value or
Hexidecimal>/<bitwise mask (type dependent on value type preceding the /) >
```

And then if you like you can remove the use of the prerequisite from the shorthand list and it can be replaced with something like the following to allow you to filter both the ip source address and udp source port.

```
Eth_type=0x0800,ip_src=100.1.0.55,Ip_proto=17,udp_source=30
```

The following figure shows the multiple filter above on the NetStack **Filter Criteria** tab:



The following are the commands you can add to a NetStack filter string.

NOTE For the fields below, (b) means this field supports <value>/<bitmask>.

```
icmp_code
icmp_type
sctp_src
sctp_dst
udp_dst (b)
udp_src (b)
tcp_flags (b)
tcp_src (b)
tcp_dst (b)
arp_tha (b)
arp_sha (b)
arp_tpa (b)
arp_spa (b)
arp_op
ip_dscp
nw_tos
ip_frag
nw_ttl
nw_proto
ipv6_dst (b)
ipv6_src (b)
ipv6_label (b)
```

```
nw_ecn aka ip_ecn
ip_src (b) aka nw_src
ip_dst (b) aka nw_dst
mpls_ttl
mpls_bos
mpls_tc
mpls_label
vlan_tci (b)
vlan_pcp
vlan_vid
dl_vlan
dl_vlan_pcp
eth_type aka dl_type
eth_dst (b)
eth_src (b)
```

Shorthand Value Definitions

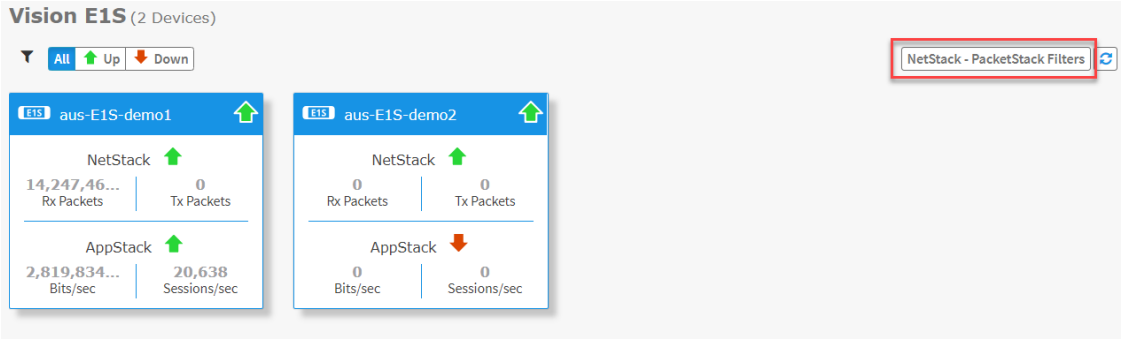
Shorthand Value	Definition
eth	packet_type=(0,0)
ip	eth_type=0x0800
ipv6	eth_type=0x86dd
icmp	eth_type=0x0800,ip_proto=1
icmp6	eth_type=0x86dd,ip_proto=58
tcp	eth_type=0x0800,ip_proto=6
tcp6	eth_type=0x86dd,ip_proto=6
udp	eth_type=0x0800,ip_proto=17
udp6	eth_type=0x86dd,ip_proto=17
sctp	eth_type=0x0800,ip_proto=132
sctp6	eth_type=0x86dd,ip_proto=132
arp	eth_type=0x0806
rarp	eth_type=0x8035
mpls	eth_type=0x8847
mplsm	eth_type=0x8848

Add NETSTACK Filters

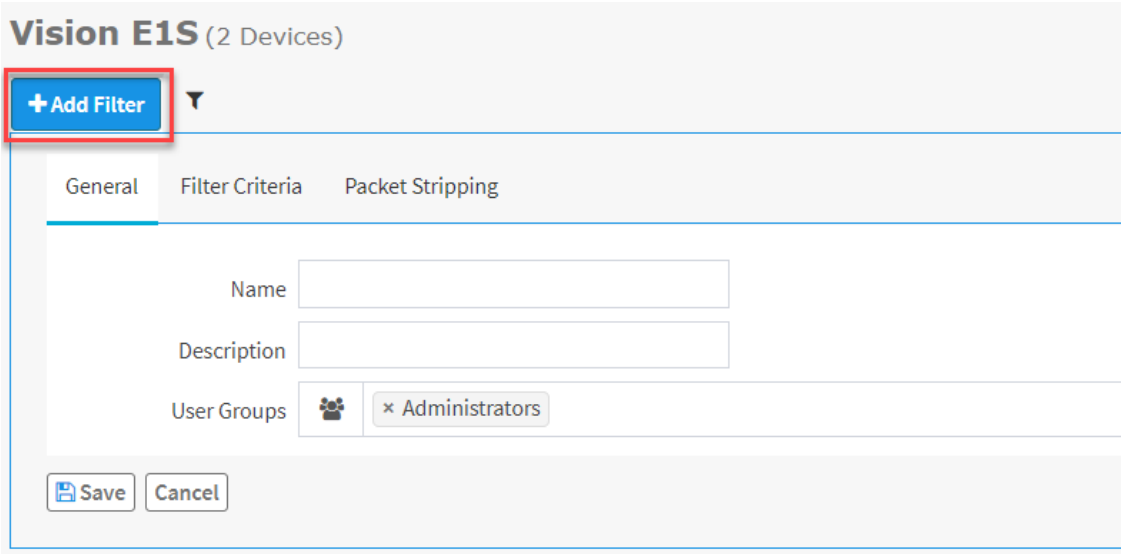
NetStack filters are defined globally on the Hawkeye system so they can be created and applied to multiple Vision E1S devices.

To add NetStack filters:

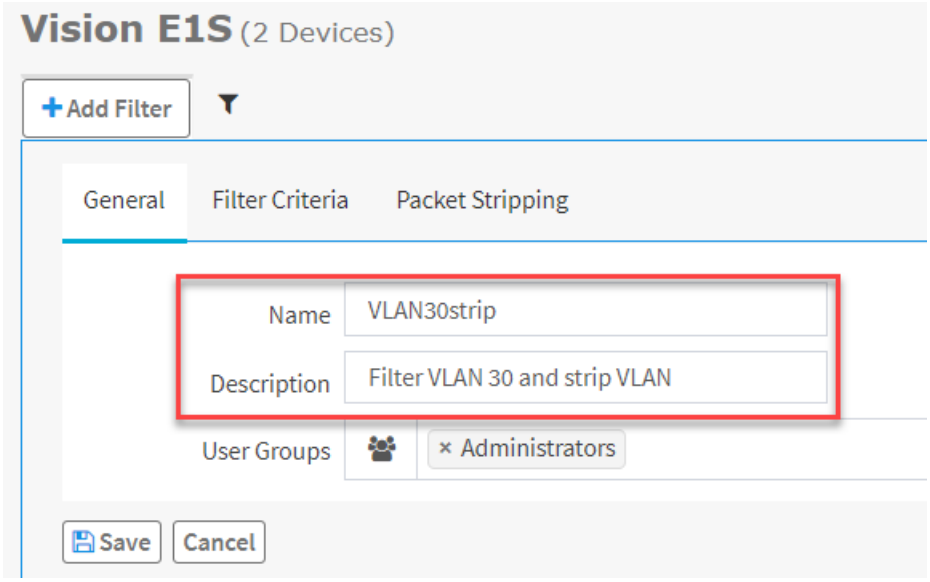
1. Select the **NetStack - PacketStack Filters** button.



2. Select the **Add Filter** button.



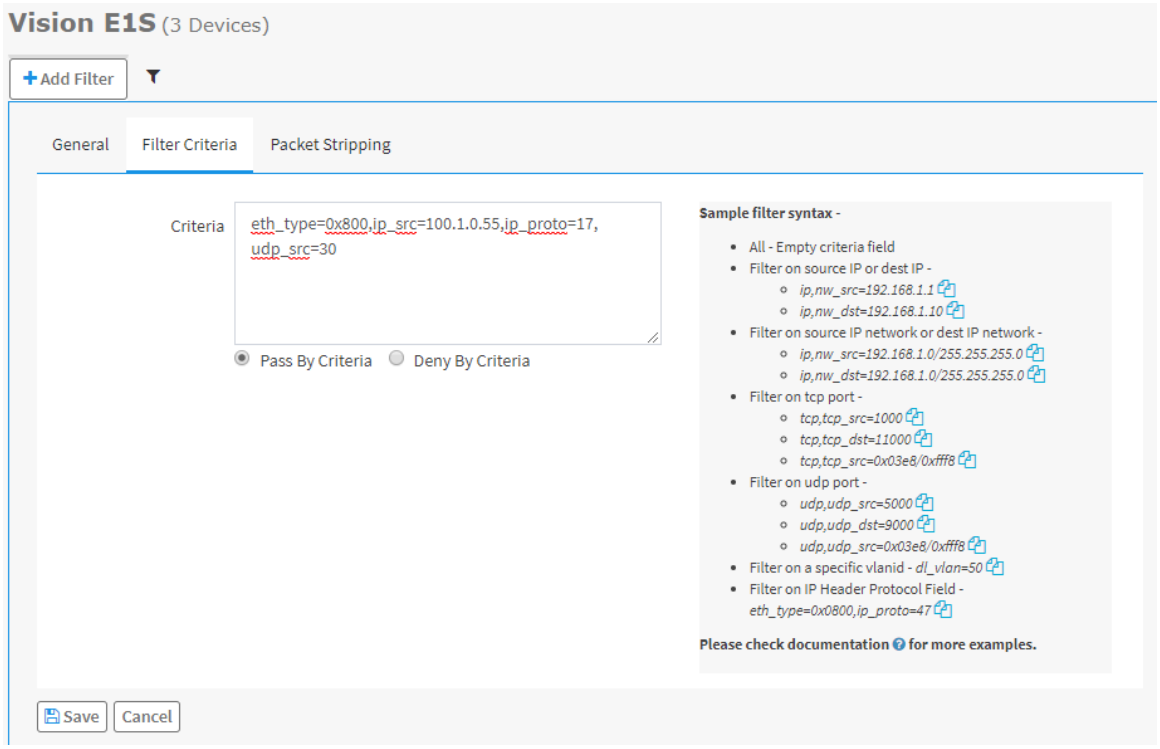
a. On the **General** tab, enter a name and description for the filter.



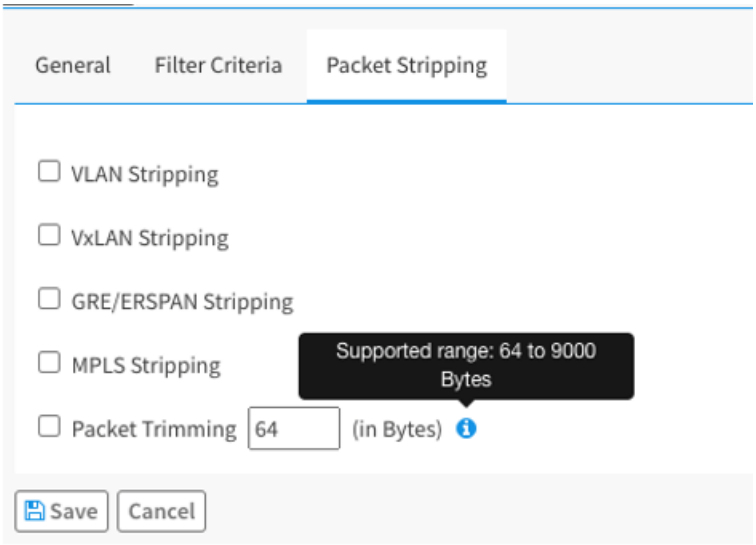
b. On the **Filter Criteria** tab, select either **Pass by Criteria** or **Deny by Criteria** option and specify the criteria for this filter. Default option is **Pass by Criteria**.

TIP

To use and adapt the common filter templates in the **Sample filter syntax**, select the copy/paste icon, paste it into the **Criteria** field, and change the value for your purpose. In the example below, we changed the template value 50 to 30.



c. On the **Packet Stripping** tab, select the relevant option you want to apply to the filter – in this example, select **VLAN Stripping**.



NOTE

- Traffic should be filtered to include only frames that you desire stripping to be performed.
- Packet Trimming supports final trim size of 64 to 9000 bytes.

3. Select the **Save** button.
   After you save a filter, it becomes available to ***ALL*** installed and enabled Vision E1S devices.

NOTE When defining a filter, the filter can be made available to one or several groups of users so they can be shared among users.

IMPORTANT When you apply changes to a filter, it instantly updates the filter in all the Vision E1S units where that filter is used.

IMPORTANT ***Not*** all OVS filters are supported on the Vision E1S units.

TIP If you're experimenting with a filter to see what it will do, create a ***new*** filter rather than using an existing filter. That way, you avoid applying an experimental filter globally to all units, a filter that may not work properly. You can search online for OVS filters to find one that does what you want. Then you can try it experimentally on a Vision E1S unit.

Example Filters

Purpose	Filter
Get VxLAN Traffic	udp, upd_dst=4789
Get GRE Traffic	ip, ip_proto=47

Map NETSTACK Ports, Limit Traffic, and Replicate It to Multiple Tools

For NETSTACK, you can define port mapping rules so you can filter packets, aggregate packets, and more. You can also perform packet stripping and packet forwarding.

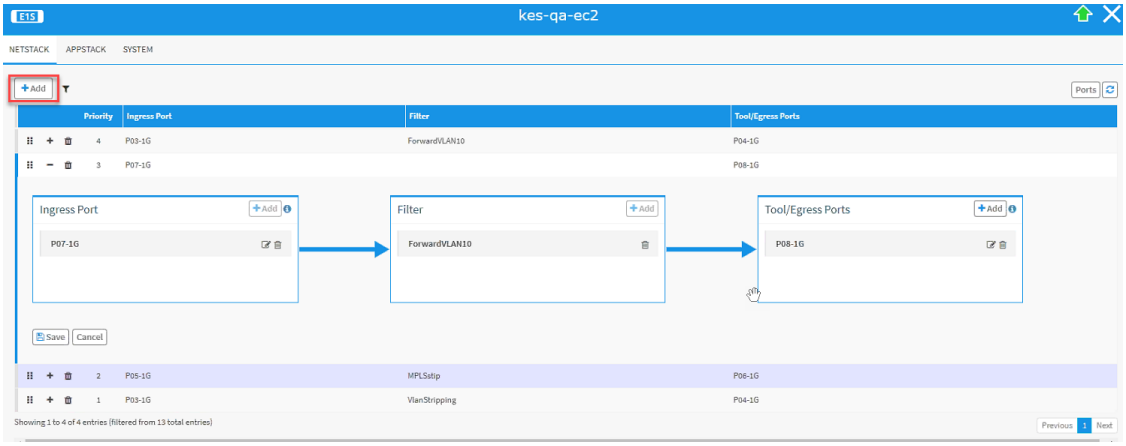
Port Mapping Priority

A higher priority value will receive traffic before a lower priority value because proper ordering of port mappings are required. Any traffic that matches a higher priority filter will have the action of filter applied and not be passed to a lower priority filter.

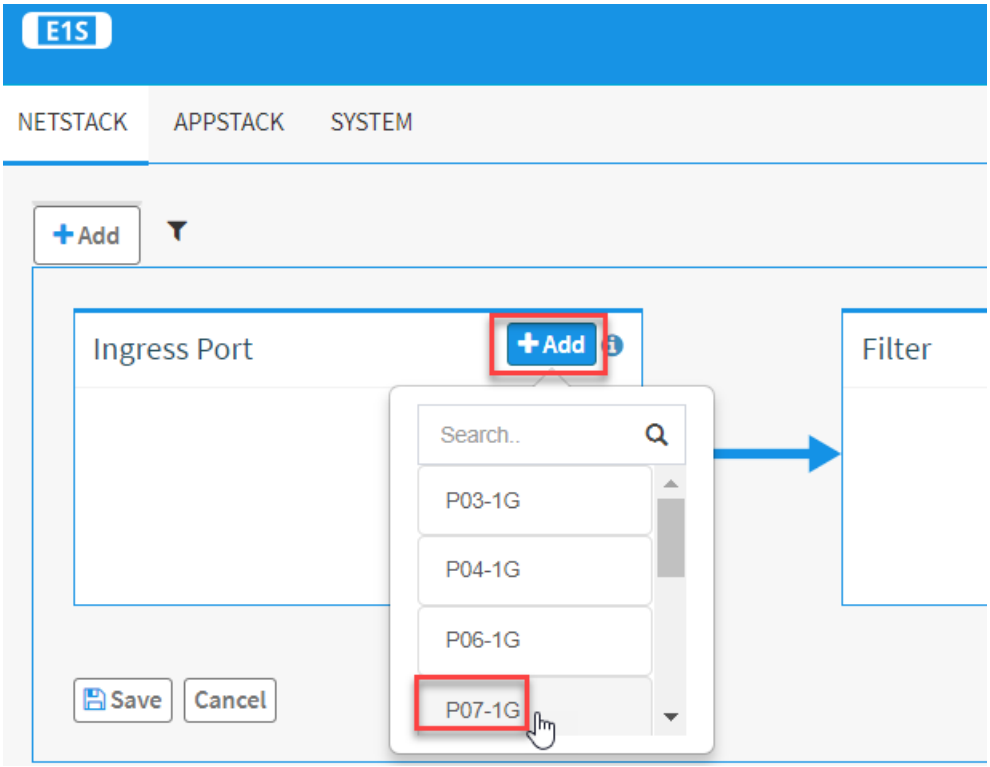
NOTE For Port Priorities 1-10, Port Priority 1 is lowest and 10 is highest.

To configure NetStack port mapping:

1. Select the relevant Vision E1S device.
2. On the **NETSTACK** tab, select the **Add** button to set up the traffic flow.



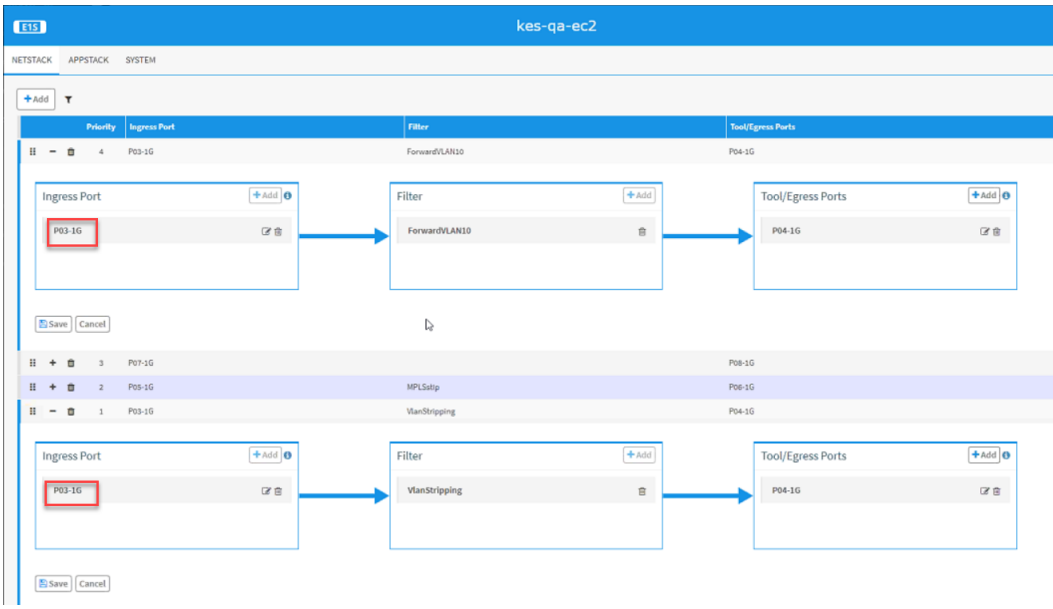
a. To add an Ingress Port, in the **Ingress Port** section, select the **Add** button and select a port – for example, **P07-1G**.



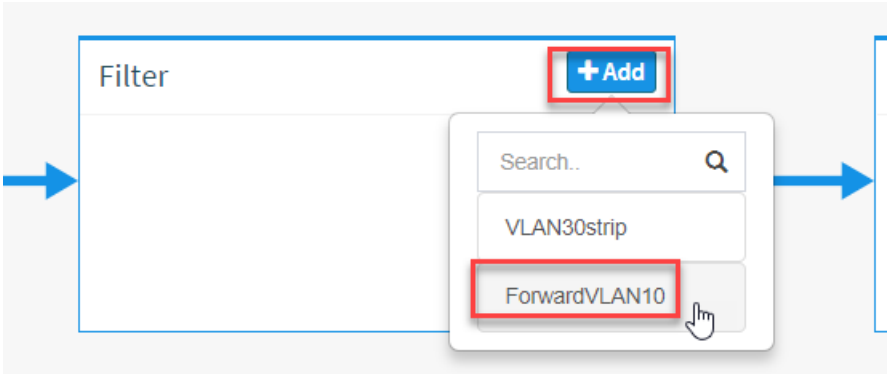
NOTE

You can only have one (1) Ingress Port in an Ingress/Egress port pair, but you can have multiple Tool/Egress Ports

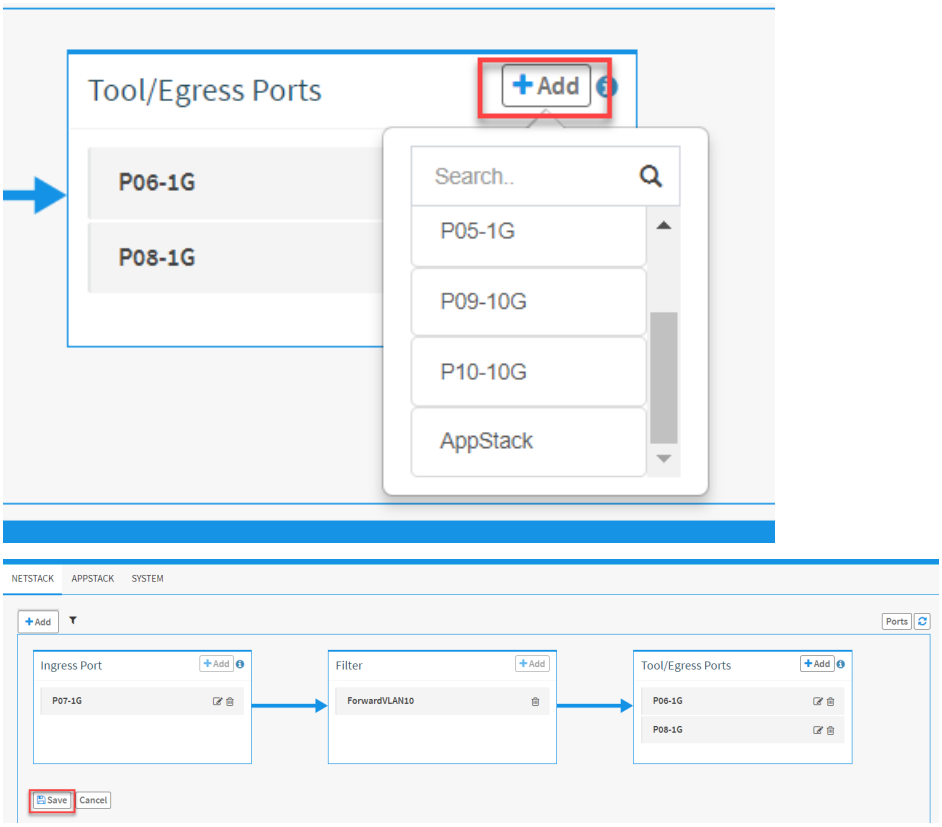
Once you designate a port as an Ingress Port, you cannot use it as a Tool/Egress Port. You can, however, use the same port for multiple filtering, stripping, or forwarding.



b. To add a Filter, in the Filter section, select the **Add** button and select one of the NETSTACK filters you have previously created - for example, **ForwardVLAN10**.

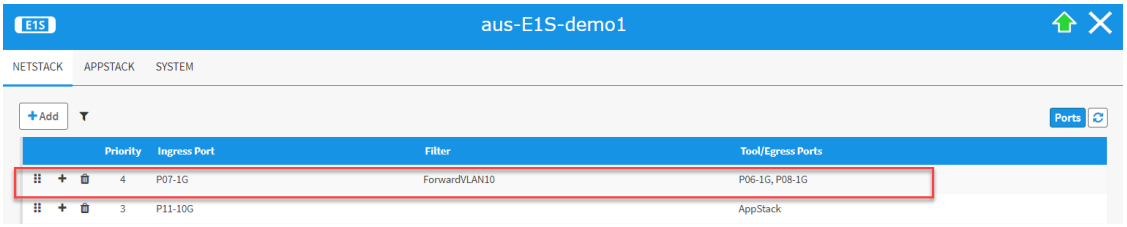


c. To add one or more Tool/Egress Ports, in the Tool/Egress Ports section, select the **Add** button and select one or more egress ports - for example, **P06-1G** and **P08-1G**.

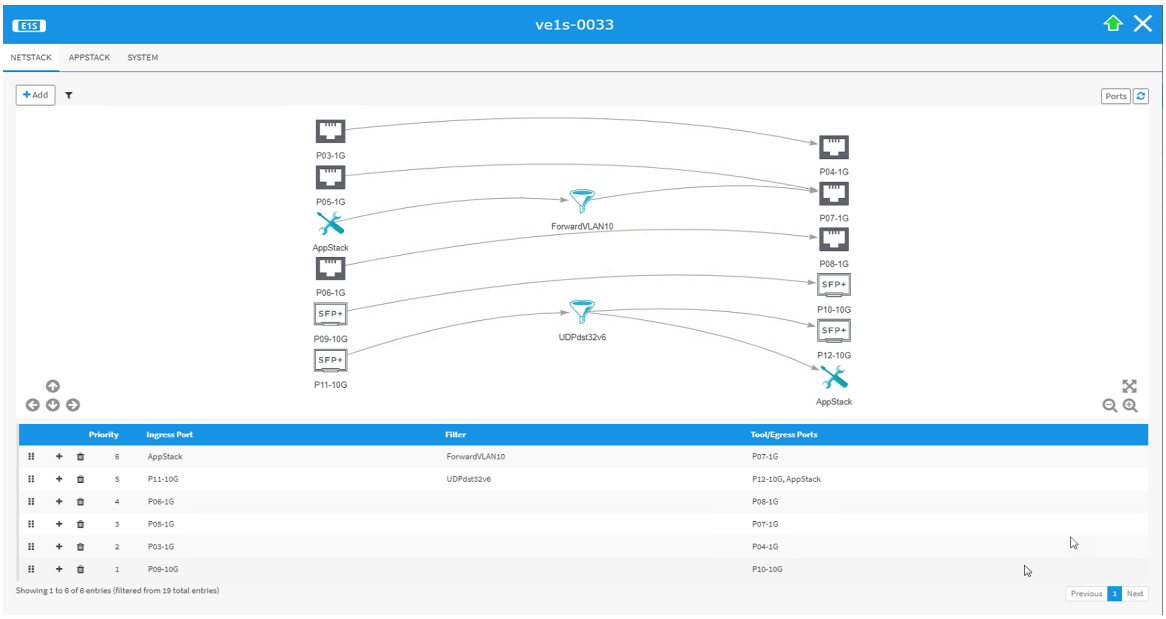


3. Select the **Save** button.

   The resulting port map looks like this, where you replicate forwarding VLAN 10 traffic to two Tool ports connected to two different tools:



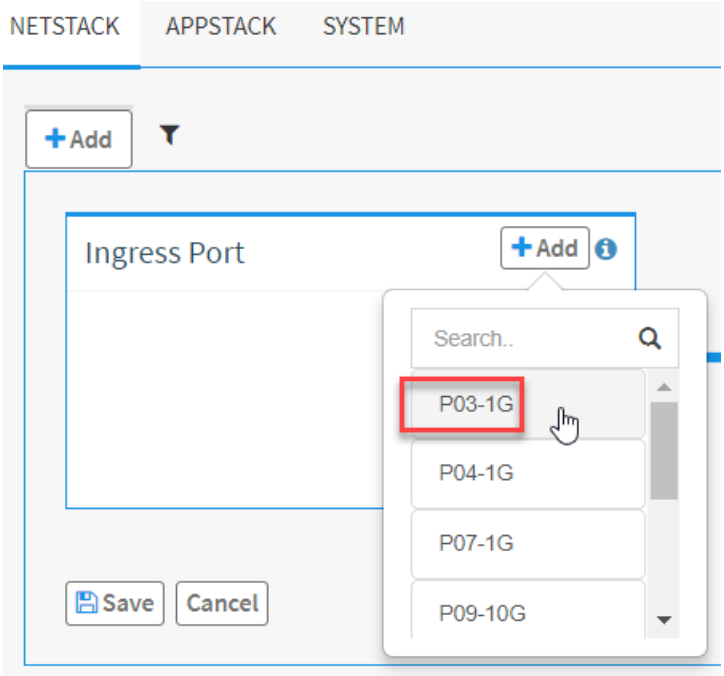
   The following is an example of a much more complex port mapping that includes the new port mapping images at the top of the screen that visually represent the tabular port mapping at the bottom of the screen:



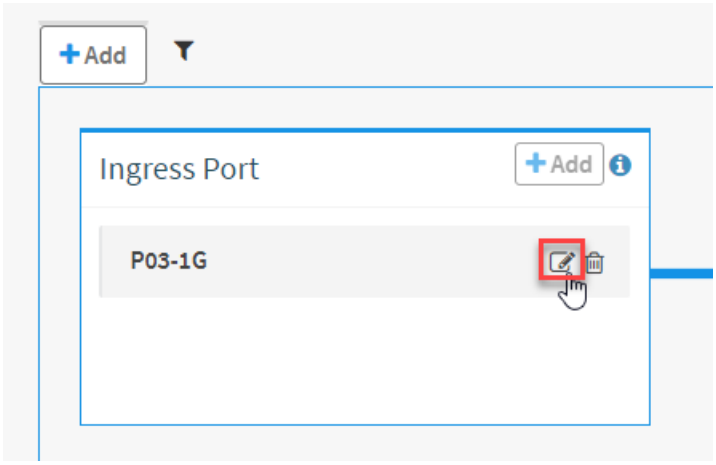
Terminate GRE tunnels

To terminate GRE tunnels:

1. Select the relevant Vision E1S.
2. On the **NETSTACK** tab, select **Add**.
3. In the **Ingress Port** section, select **Add** and select an available port – for example, **P03-1G**.



4. Select the edit icon.



5. Select the Mode drop-list and select **IP Enabled.**

6. Enter the **IP Address**, **Subnet Mask**, and **Gateway**.
7. In the **Tool/Egress Ports** section, select **Add** and select a port – for example, **P04-1G**.

   NOTE You can only map ports in pairs, with one Ingress Port and one or more Tool/Egress Ports.

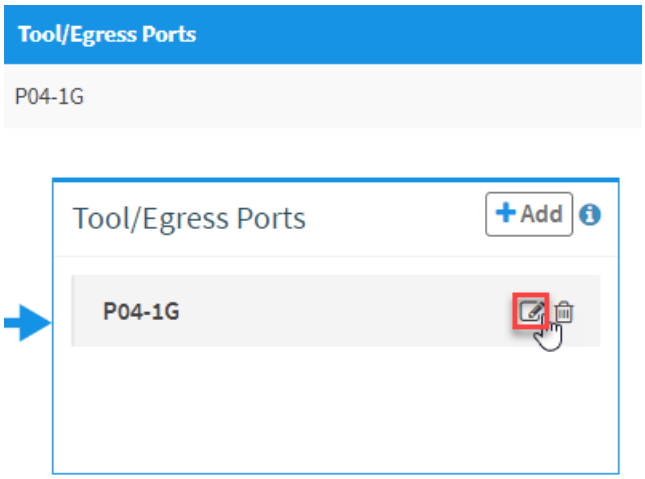
8. Select **Save** to save the GRE termination on the Ingress Port which forwards packets to the Tool/Egress Port(s).

Originate GRE Tunnels

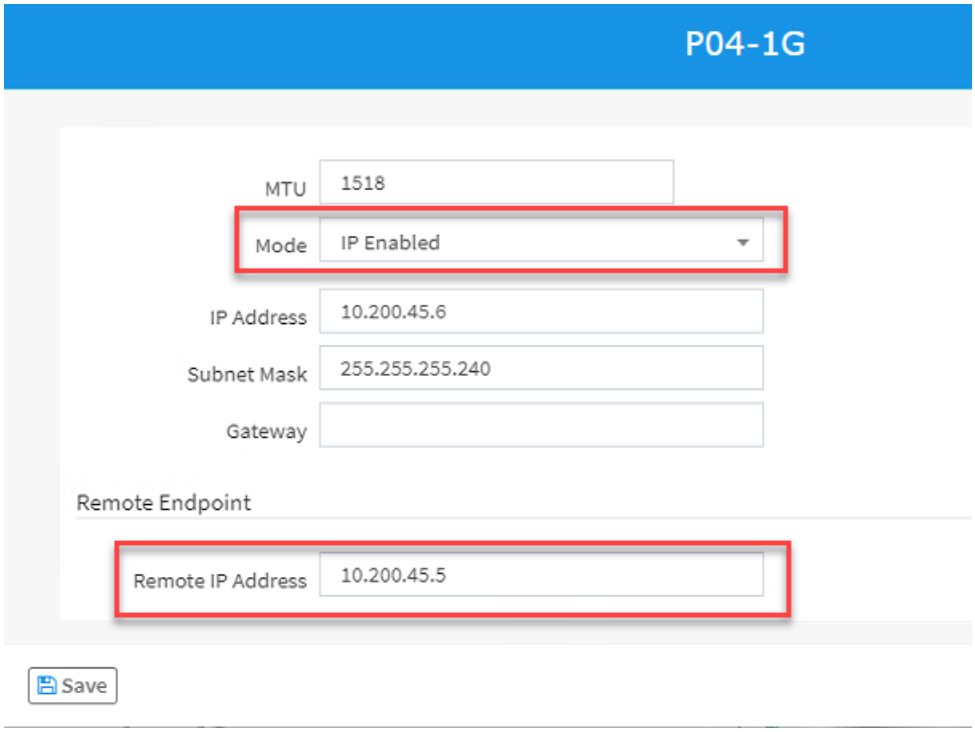
To originate GRE tunnels:

1. Select the relevant Vision E1S.
2. On the **NETSTACK** tab, select **Add**.
3. In the **Ingress Port** section, select **Add** and select an available port – for example, **P03-1G**.
4. In the **Tools/Egress Ports** section, select **Add** and select an available port – for example, **P04-1G**.

5. Select the edit icon.



6. Open the **Mode** drop-list and select **IP Enabled**.



7. Enter the IP Address, Subnet Mask, Gateway, and Remote IP Address.

   NOTE You must enter a Remote IP Address so the GRE tunnel has a place to go, the Remote Endpoint.

8. Select **Save** to save the GRE tunnel origination.
9. Select **Save** to save changes to the port pair – the Ingress and Egress ports.

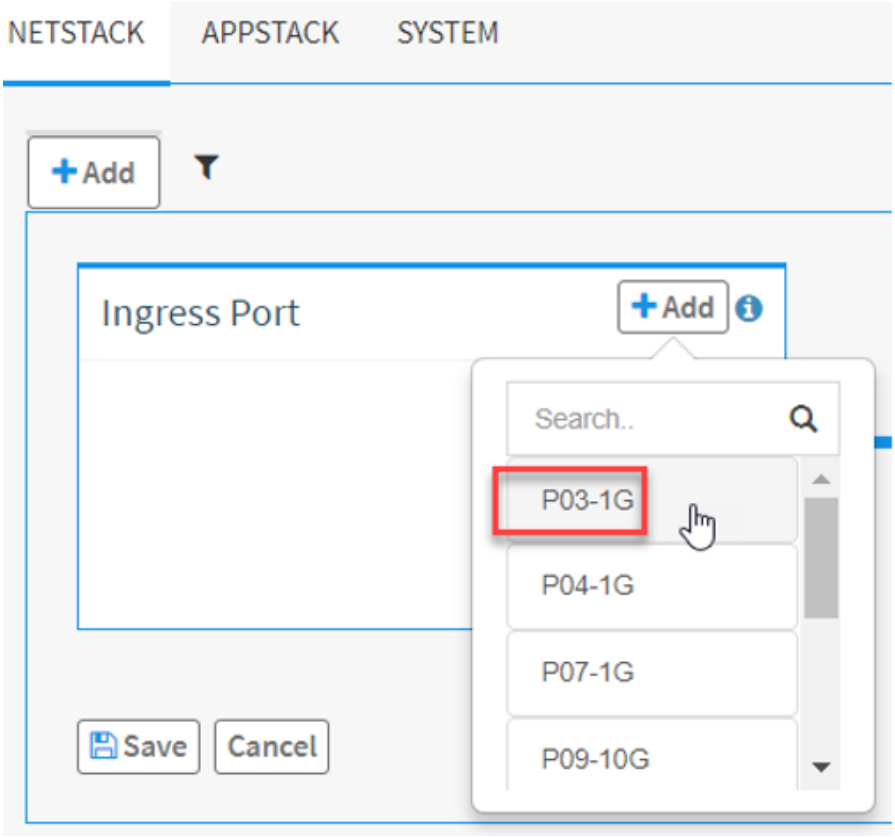
Terminate VxLAN Tunnels

When an Ingress port is set to VxLAN the following rules apply:

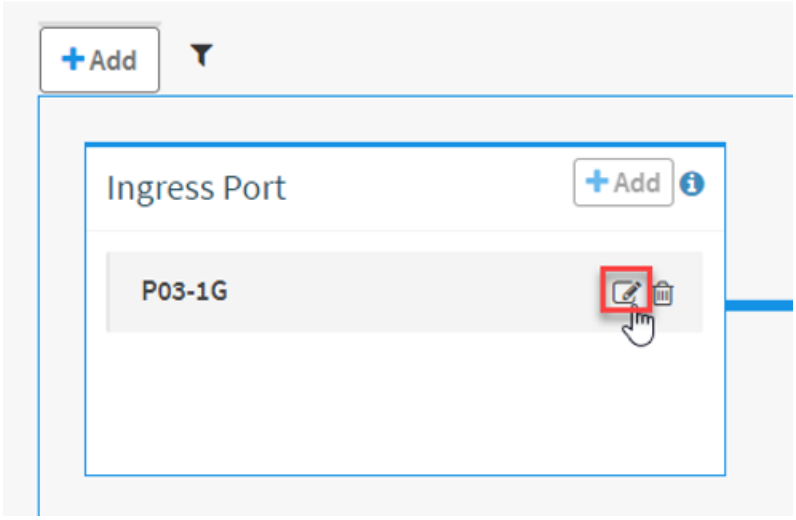
- Accepts UDP Traffic with Destination Port set to 4789
- Is not dependent on VNI setting
- All other traffic is dropped
- Does not support Cisco's implementation of VxLAN

To terminate VxLAN tunnels:

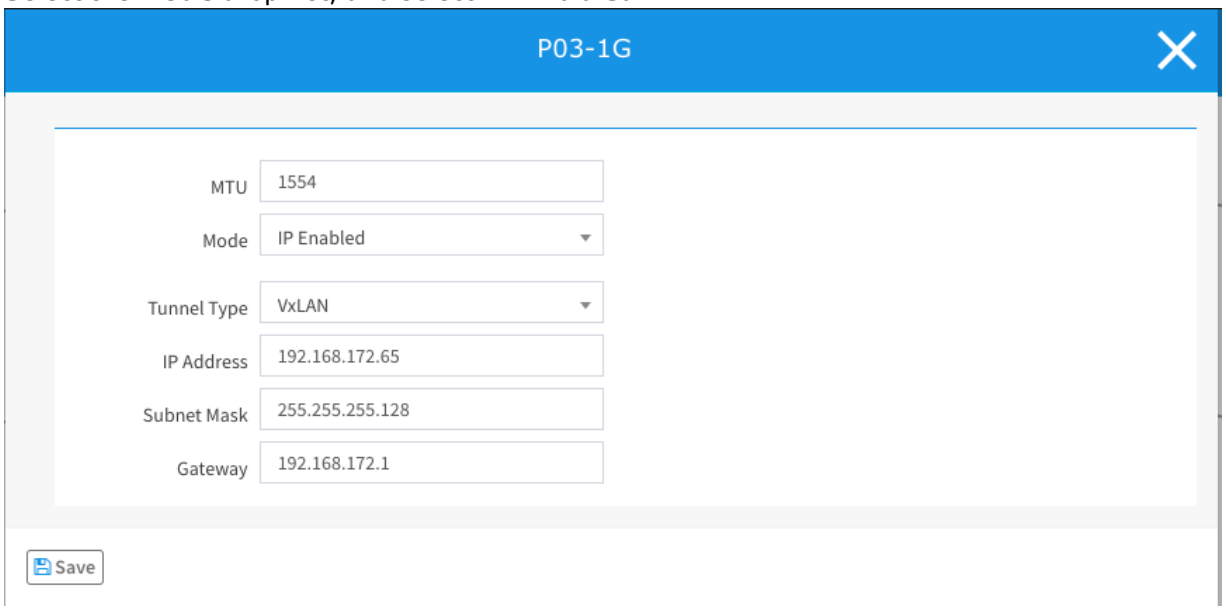
1. Select the relevant Vision E1S.
2. On the **NETSTACK** tab, select **Add**.
3. In the **Ingress Port** section, select **Add** and select an available port – for example, **P03-1G**.



4. Select the **edit** icon.



5. Select the **Mode** drop-list, and select **IP Enabled**.



6. Select the **Tunnel Type** drop-list, and Select **VxLAN**.
7. Enter the **IP Address**, **Subnet Mask**, and **Gateway**.
8. In the **Tool/Egress Ports** section, select **Add**, and select a port – for example, **P04-1G**.

   NOTE You can only map ports in pairs, with one Ingress Port and one or more Tool/Egress Ports.

9. Select **Save** to save the VxLAN termination on the Ingress Port, which forwards packets to the Tool/Egress Port(s).

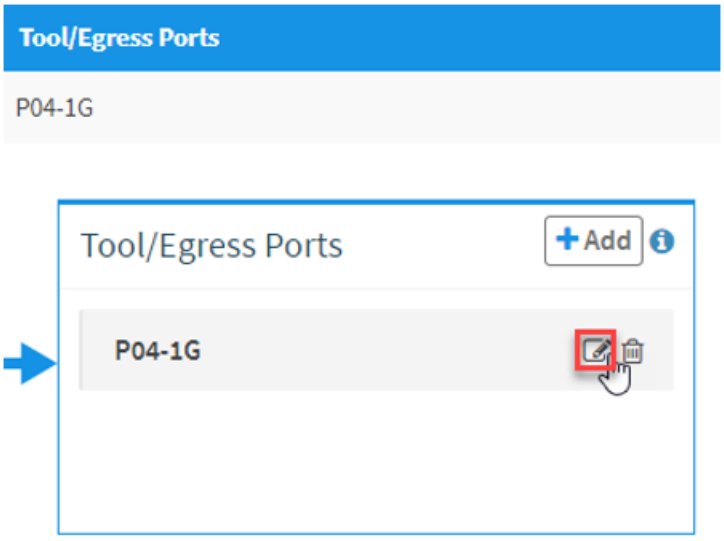
Originate VxLAN Tunnels

When an Egress port is set to VxLAN the following rules apply:

- Tunnel must be able to ARP and PING the address of the remote end
- Traffic will be transmitted using UDP dest. port 4789.
- VNI is configurable.

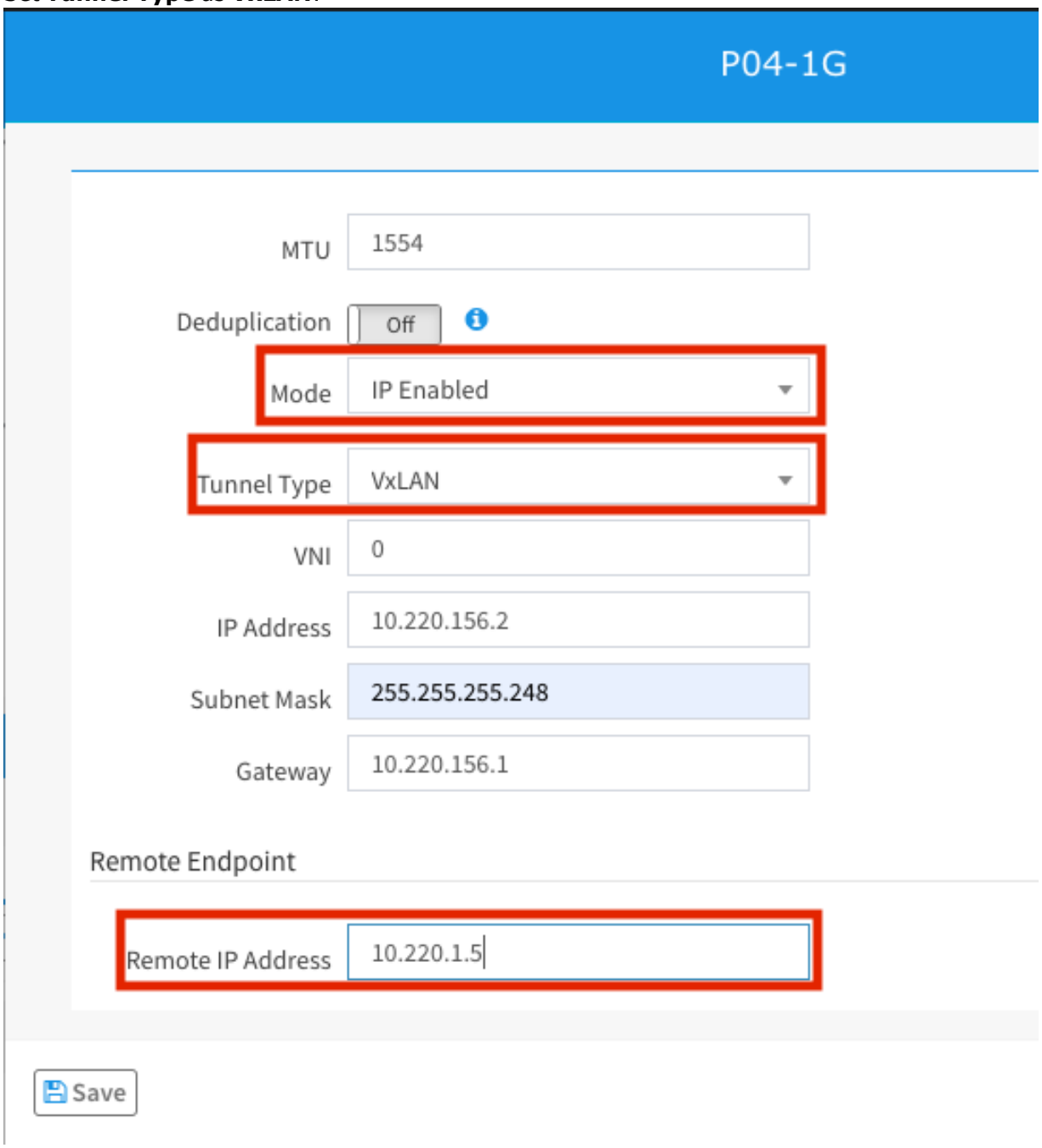
To originate VxLAN tunnels:

1. Select the relevant Vision E1S.
2. On the **NETSTACK** tab, select **Add**.
3. In the **Ingress Port** section, select **Add**, and select an available port – for example, **P03-1G**.
4. In the **Tools/Egress Ports** section, select **Add**, and select an available port – for example, **P04-1G**.
5. Select the **edit** icon.



6. Open the **Mode** drop-list, and **select IP Enabled**.

7. Set **Tunnel Type** as **VxLAN**:



8. Enter the IP Address, Subnet Mask, Gateway, and Remote IP Address.

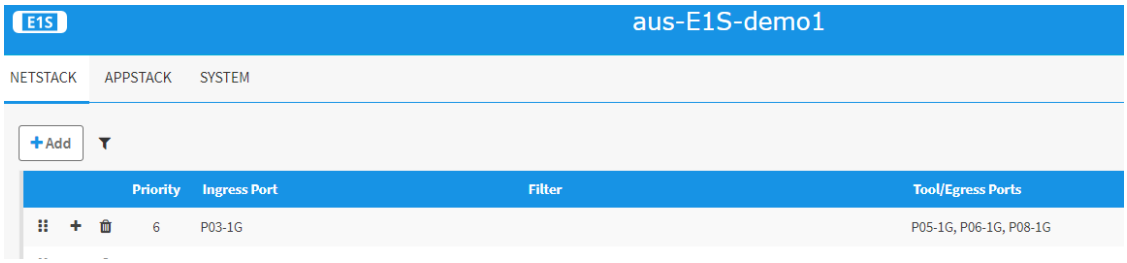
   NOTE You must enter a Remote IP Address so the GRE tunnel has a place to go, the Remote Endpoint.

9. Select **Save** to save the GRE tunnel origination.
10. Select **Save** to save changes to the port pair – the Ingress and Egress ports.

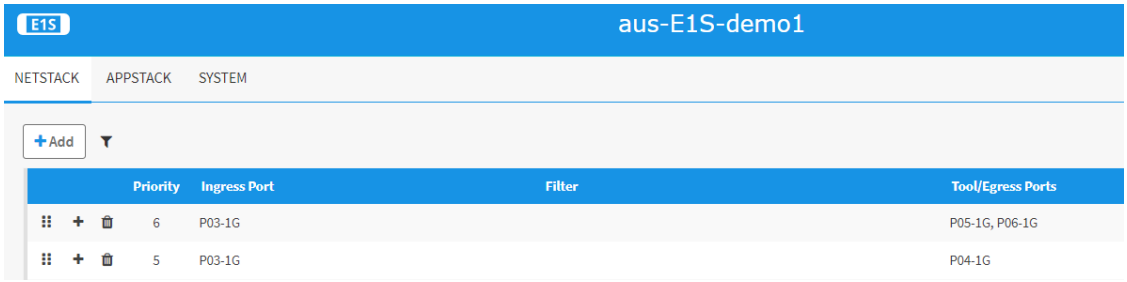
Replicate Traffic

The following are a few of the ways you can replicate traffic to multiple tools:

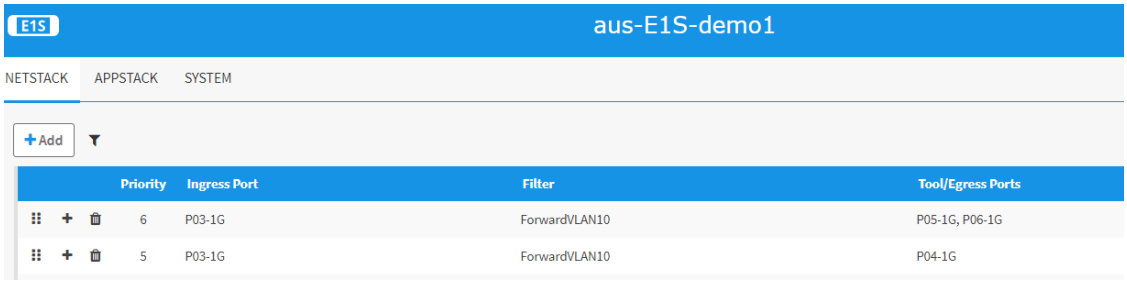
- One Ingress Port to multiple Tool/Egress Ports



- Two instances of one Ingress Port to multiple Tool/Egress Ports



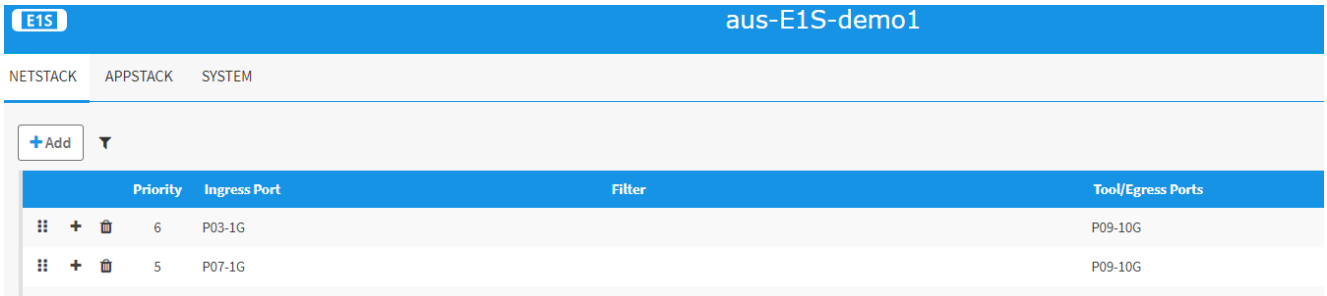
- Two instances of one Ingress Port with same filter to multiple Tool/Egress Ports



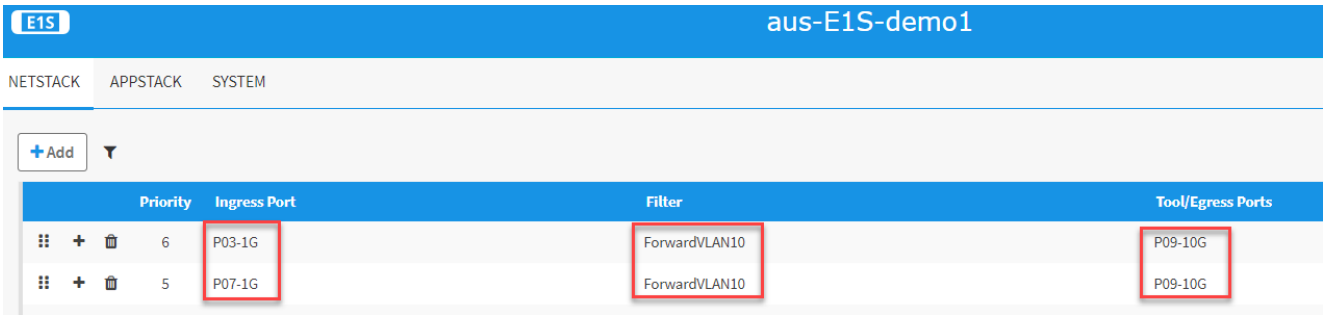
Aggregate Traffic

The following are a couple of ways to aggregate traffic:

- Aggregate all traffic from two 1G ports to one 10G port



- Aggregate the same filtered traffic from two 1G ports to one 10G port



Deduplicate Packets

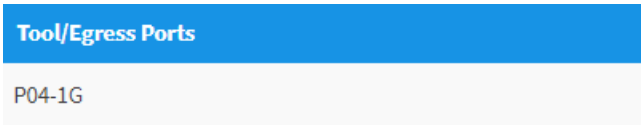
The deduplication functionality operates on L3+ basis. Deduplication will treat an encapsulated packets, such as in the case of VxLAN, as a payload.

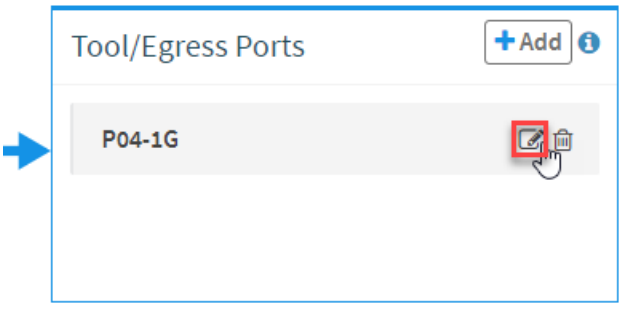
Order of operations for Deduplication and Tunnel Types enabled on the same Egress port is tunneling encapsulation first, then deduping, then sending of the packet over the physical port.

flows ---> VxLAN/GRE encapsulation -->dedup -> phyPort -> pkt_out

To configure Deduplication:

1. Select the relevant Vision E1S.
2. On the **NETSTACK** tab, select **Add**.
3. In the **Ingress Port** section, select **Add** and select an available port – for example, **P03-1G**.
4. In the **Tools/Egress Ports** section, select **Add** and select an available port – for example, **P04-1G**.
5. Select the edit icon.





6. Set the **Deduplication** slider to **On**.

7. Select **Save** to save the Deduplication configuration.
8. Select **Save** to save changes to the port pair – the Ingress and Egress ports.

Configure APPSTACK

You can use APPSTACK to:

Monitor APPSTACK Statistics Related to the Top Filters and Applications **64**

Filter APPSTACK Traffic Based on Criteria **64**

Egress APPSTACK Filtered Traffic **65**

Send NetFlow/IxFlow Records to NetFlow Collectors **66**

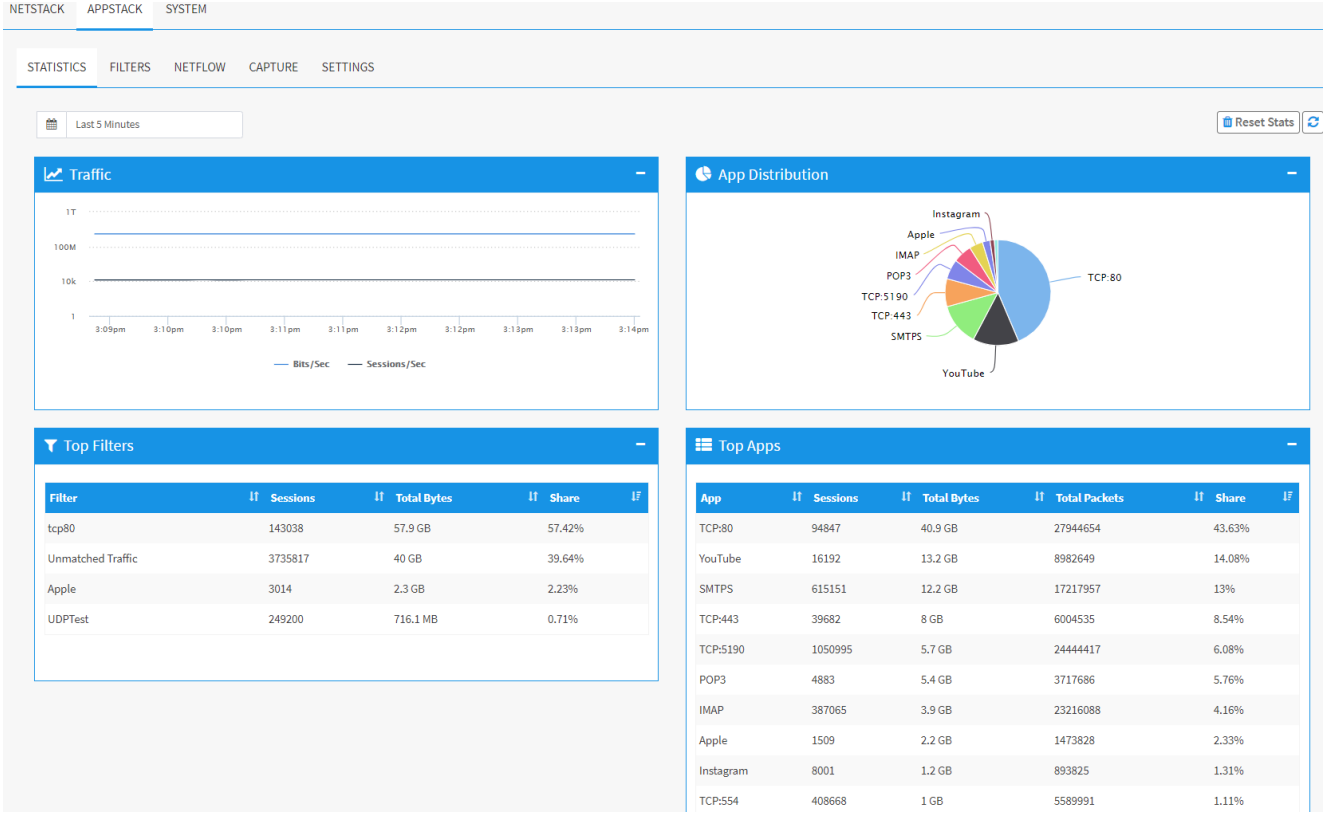
Capture Filtered Traffic and Save It **69**

Forward APPSTACK Filtered Traffic to an Outside Tool **70**

Monitor APPSTACK Statistics Related to the Top Filters and Applications

To monitor the statistics related to the top filters and top applications detected in the analyzed traffic:

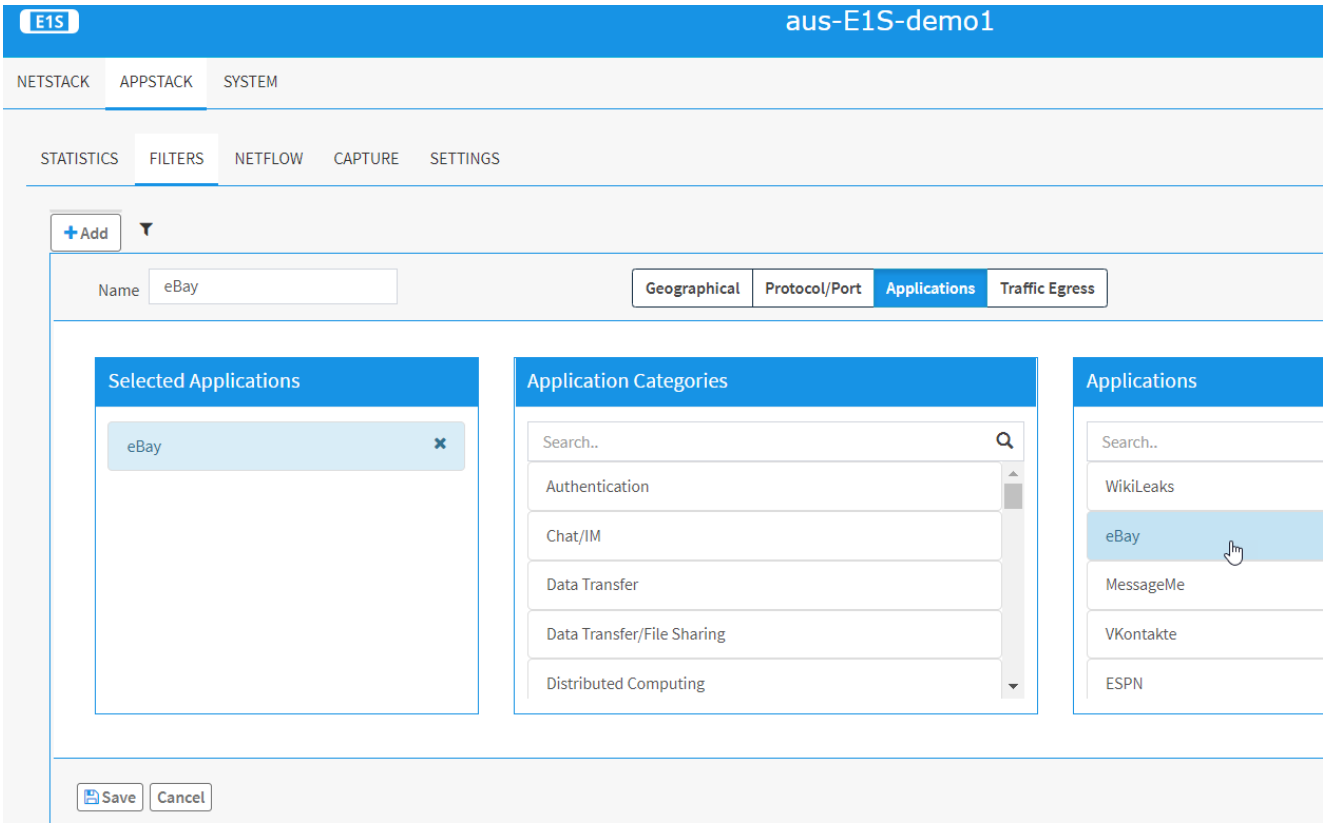
1. Select the relevant Vision E1S.
2. Select the **APPSTACK** tab.
3. Select the **STATISTICS** tab.



Filter APPSTACK Traffic Based on Criteria

To filter traffic based on criteria:

1. Select the relevant Vision E1S.
2. Select the **APPSTACK** tab.
3. Select the **Filters** tab.
4. Select the **Add** button.

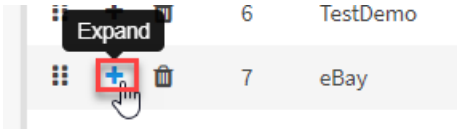


5. To filter on applications, select the **Applications** tab.
6. Select an application – for example, **eBay**.
7. Select **Save** to save this filter.

Egress APPSTACK Filtered Traffic

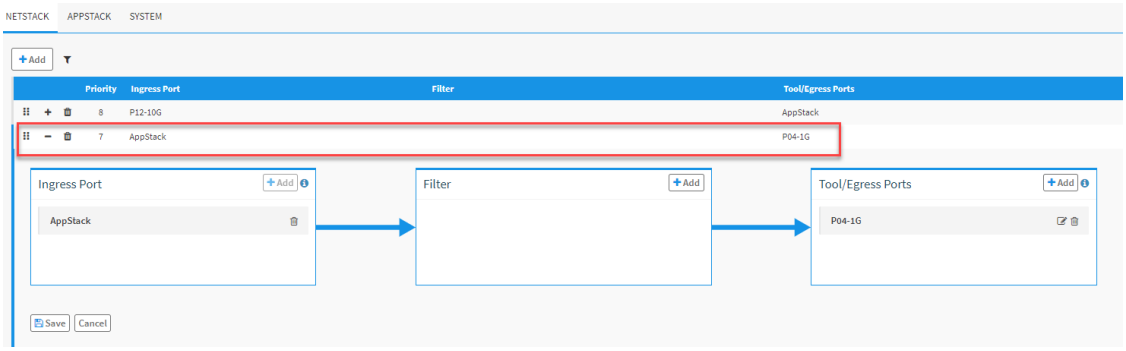
To egress APPSTACK filtered traffic:

1. Select the relevant Vision E1S.
2. Select **APPSTACK**.
3. Select **FILTERS**.
4. Open the expand plus icon for the relevant filter – for example, **eBay**.



5. Select **Traffic Egress**.
6. Select an egress action – for example, **Forward**.
7. Select **Save** to save this egress action for this APPSTACK filter.
8. To use this forwarded APPSTACK traffic, select the **NETSTACK** tab.
9. Select the **Add** button.
10. In the **Ingress Port** section select **Add** and select **AppStack**.

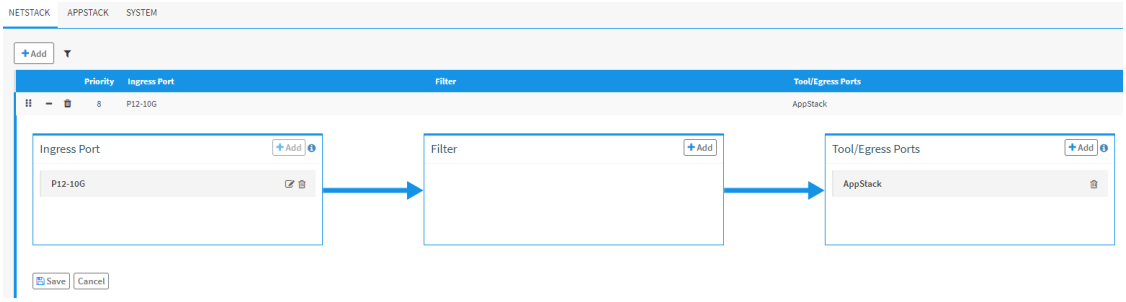
11. In the **Tool/Egress Ports** section, select **Add** and select an egress port – for example, **P04-1G**.



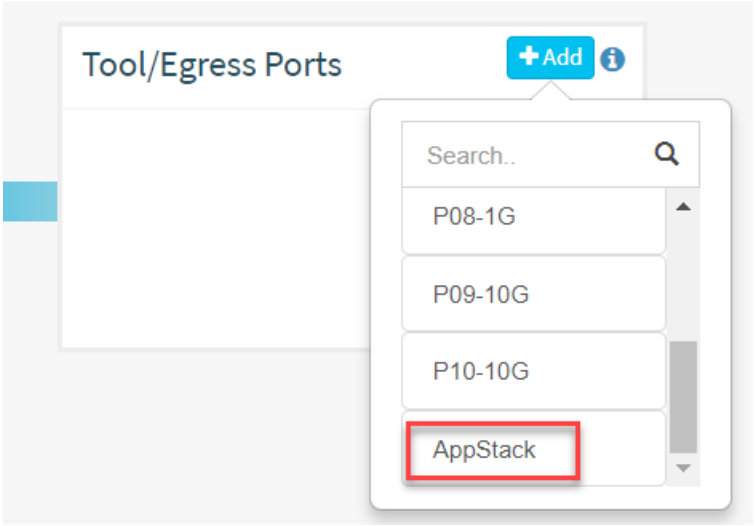
12. Select **Save** to save this APPSTACK egress action and NETSTACK port mapping.

Send NetFlow/IxFlow Records to NetFlow Collectors

1. Select the relevant Vision E1S.
2. On the **NETSTACK** tab, select **Add**.
3. For the **Ingress Port,** select **Add** and select the port where the tap is cabled into the Vision E1S – for example, port **P12-10G**.

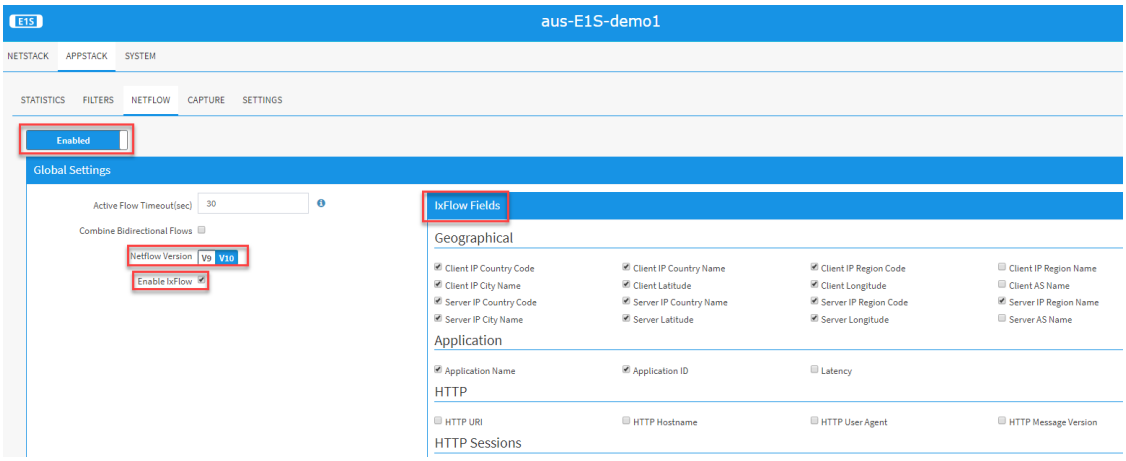


4. For the **Tool/Egress Port**, select **Add**, scroll down, and select **AppStack**.



5. Select the **APPSTACK** > **NETFLOW** tab.

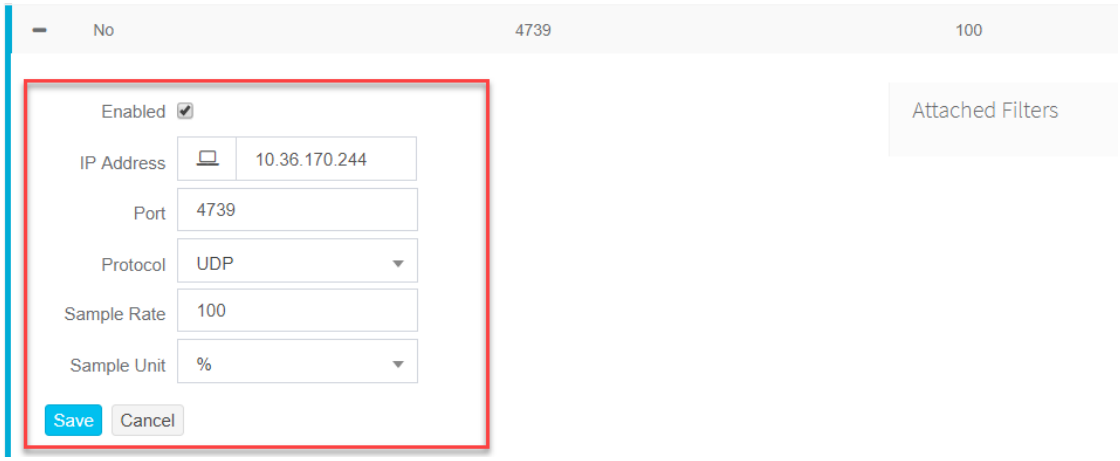
TIP Expand the IxFlow Fields section to see and configure it, and minimize it to focus more on the NetFlow Collectors.



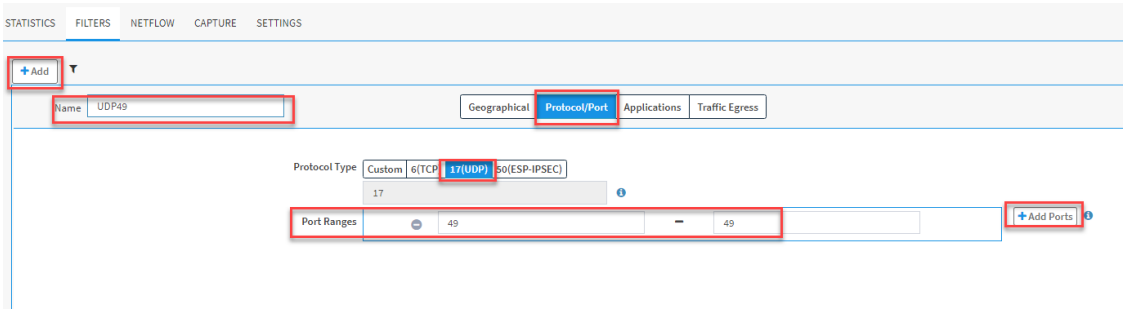
6. Select **Enabled**, **NetFlow Version**, **Enable IxFlow**, and the **IxFlow** fields you want to include.

NOTE NetFlow Version 10 supports the IxFlow fields. If you select NetFlow Version 9, the IxFlow fields are grayed out (unselectable).

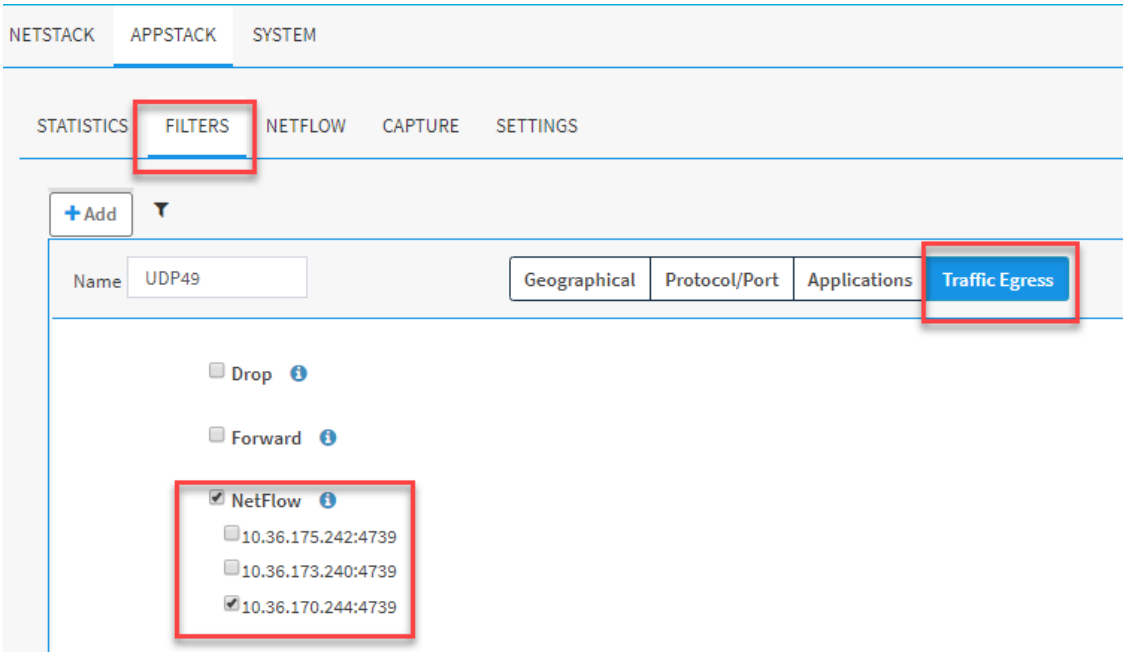
7. Select **Save** to save the Netflow Version and IxFlow fields.
8. Either minimize the **IxFlow Fields** or scroll down to the **NetFlow Collectors** section and open a + icon.



9. Select **Enabled** and enter an **IP Address**, **Port**, **Protocol**, **Sample Rate**, and **Sample Unit**.
10. Select **Save**.
11. Select the **AppStack** > **Filters** tab.



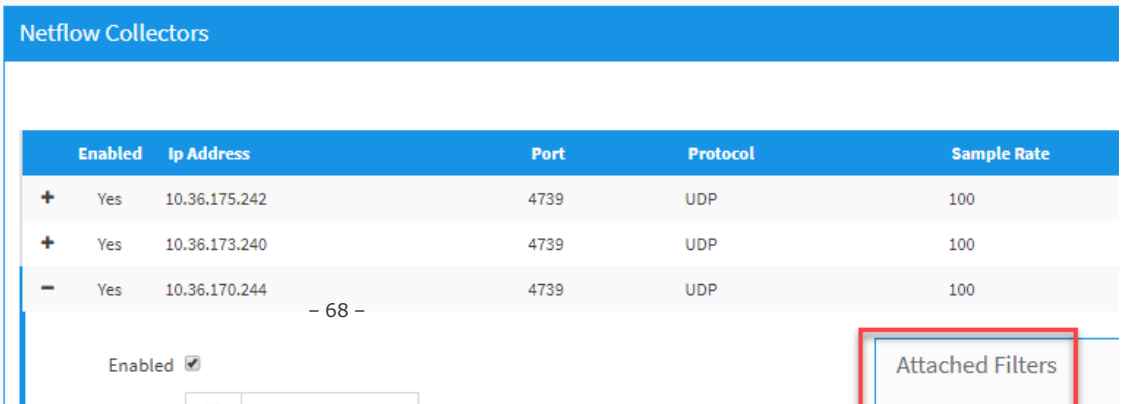
12. Select **Add**.
13. Enter a meaningful **Name** like **UDP49** and the appropriate filter – Geographical, Protocol/Port, or Applications – for example, **Protocol/Port**.
14. In the **Protocol Type** area, select a protocol – for example, **UDP**.
15. In our example, select **Add Ports** to enter the **Port Ranges** for this UDP filter – for example, **49**.
16. Select **Traffic Egress**.
17. Select **NetFlow** and the relevant IP address you created in the **AppStack** > **NetFlow** tab for the **NetFlow Collector** in step 8 above.



18. Select **Save** to save this APPSTACK FILTER.

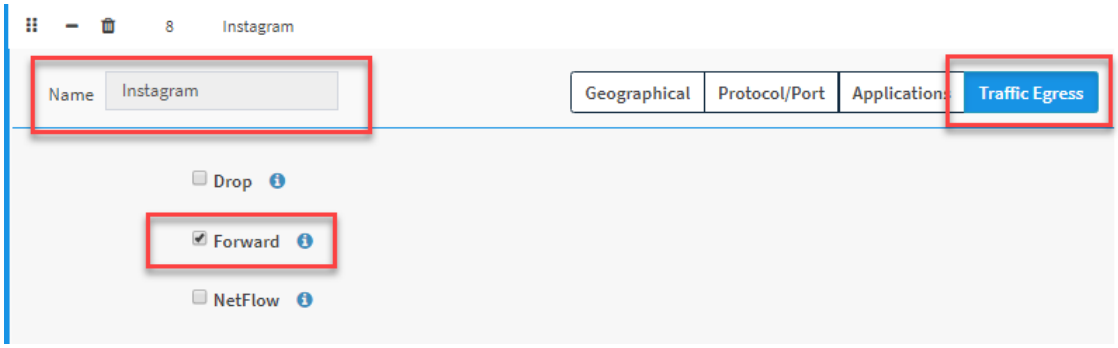
NOTE

If you return to the **APPSTACK** > **NETFLOW** tab to the NetFlow Collector whose IP address you just selected for this filter, you now see this filter as an Attached Filter.

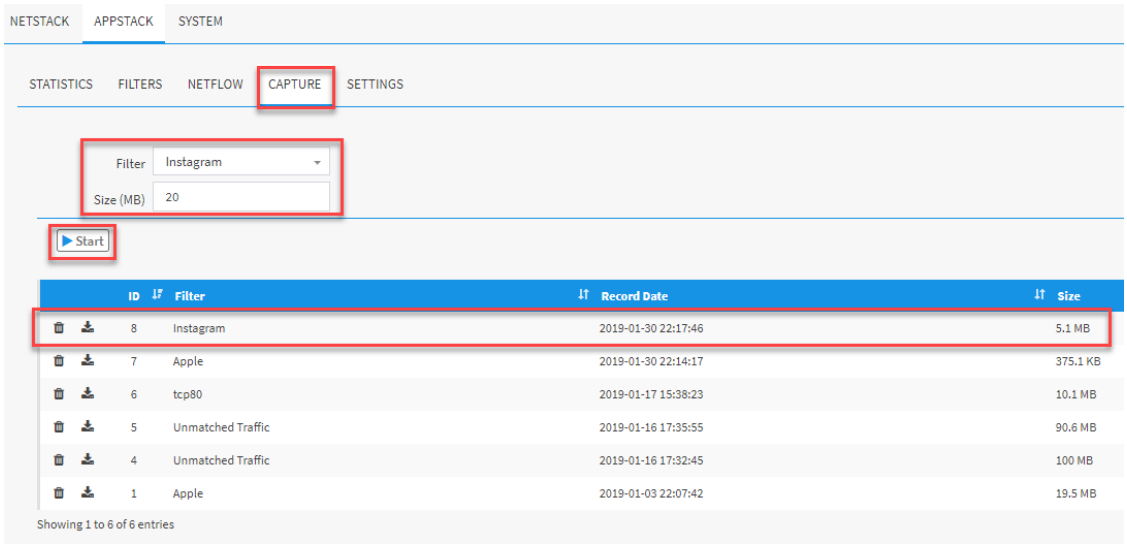


Capture Filtered Traffic and Save It

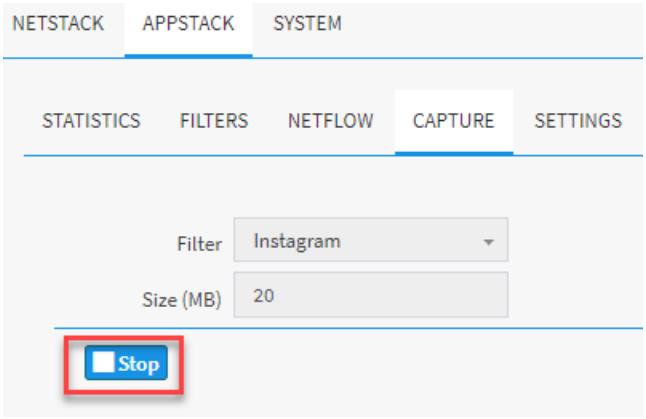
1. Select the **APPSTACK** > **FILTERS** tab.
2. Create or open an **APPSTACK FILTER** – for example, **Instagram**.
3. Select **Traffic Egress**.



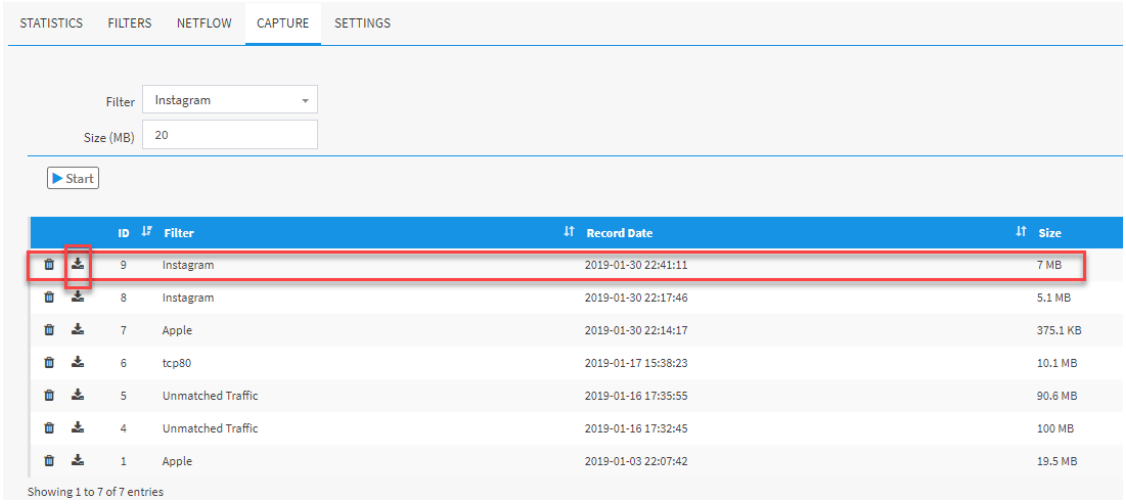
4. Select **Forward**.
5. Select **Save** to save changes to this filter.
   Traffic now forwards from the APPSTACK FILTER Instagram.
6. Select the **CAPTURE** tab.
7. Open the **Filter** drop-list and select an APPSTACK FILTER set to Forward - in our example, **Instagram**.



8. Either accept the default 100MB Size limit or enter a lower size - for example, **20MB**.
9. Select the **Start** button.
10. Either allow the packet capture (PCAP) to stop when it reaches the limit you set, or select the **Stop** button to end the PCAP sooner.



The newest PCAP appears at the top of the list.

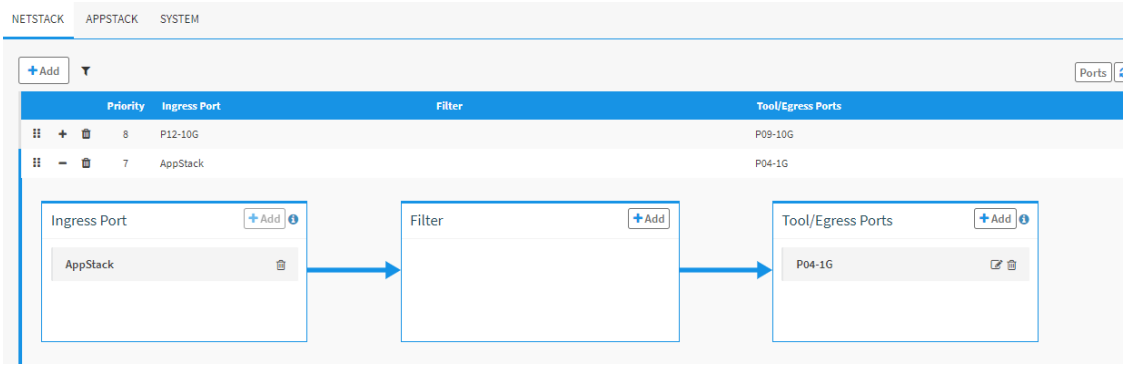


11. To download a PCAP file, select the download icon for the relevant capture file and save it to your PC or network directory.

Forward APPSTACK Filtered Traffic to an Outside Tool

To forward APPSTACK filtered traffic to an outside tool:

1. Select the relevant Vision E1S.
2. Select **NETSTACK**.
3. Select **Add**.

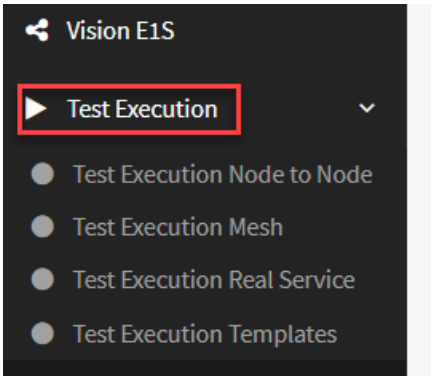


4. In the **Ingress Port** section, open the **Add** button and select **AppStack**.
5. In the Tool/Egress Ports section, open the Add button and select the relevant port – for example, **P04-1G**.

   NOTE Ensure the port you select is cabled to the relevant tool to analyze this AppStack filtered traffic.
6. Select the **Save** button.

Active Monitoring Tests

Active monitoring testing is same as Hawkeye**Test Execution**.



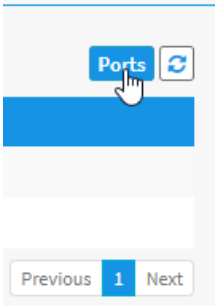
See Hawkeye Test Types for information on testing.

Convert 10G NETSTACK Port for Active Monitoring Test Execution

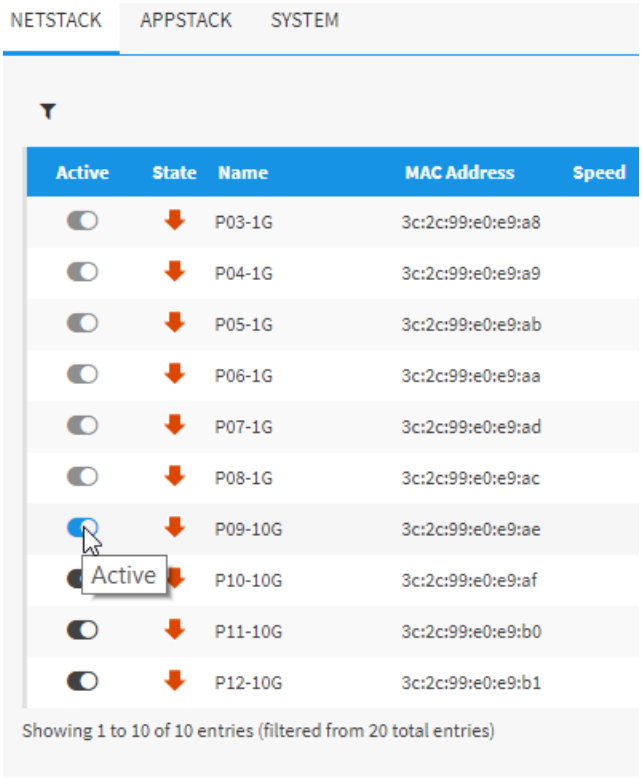
To make a 10G port on a Vision E1S available to use for active monitoring/Hawkeye test execution, you disable the 10G port.

To disable a 10G NETSTACK port:

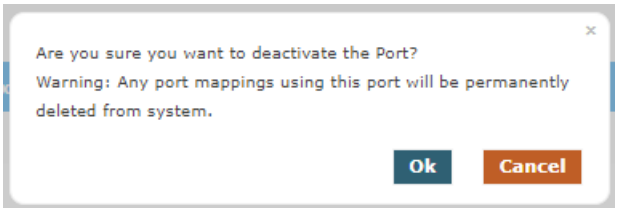
1. Select the relevant Vision E1S.
2. On the **NETSTACK** tab, select the **Ports** button.



3. Choose a 10G port that you are ***not*** using in any port mappings, and select the **Active** button to dectivate that port for NETSTACK use.



4. Select **OK** in the deactivate confirmation.



Face Plate	Hawkeye Server NetStack User Interface	Kernel Ownership (Active Monitoring/Hawkeye)
M1	N/A	enp2s0
M2	N/A	enp3s0
3	P03-1G	enp4s0*
4	P04-1G	enp5s0*
5	P05-1G	enp6s0f0*
6	P06-1G	enp6s0f1*
7	P07-1G	enp6s1f0*
8	P08-1G	enp6s1f1*
9	P09-10G	enp10s0f0

10	P010-10G	enp10s0f1
11	P011-10G	enp11s0f0
12	P012-10G	enp11s0f1

* These ports only appear in the CLI prior to establishing a connection between the Vision E1S and the Hawkeye Server. Once the connection is established, these ports are added to the NetStack configuration and are configurable from the Hawkeye Server's NetStack User Interface.

Upgrade the Vision E1S

You can upgrade the Vision E1S in both online and offline processes.

Update with Hawkeye

If the Vision E1S Device is connected to a Hawkeye Server for management, the Hawkeye server automatically updates the Vision E1S to the required version to work with the Hawkeye server.

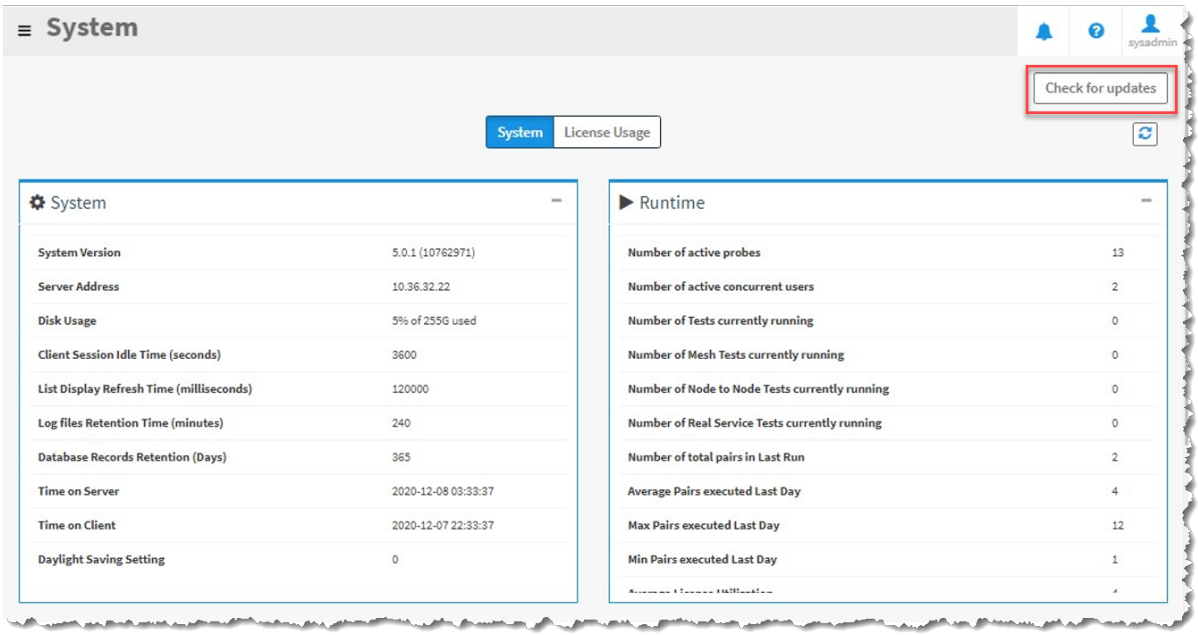
Upgrade in Local Manager Mode

You can upgrade the Vision E1S in Local Manager mode with both online and offline processes.

Online update

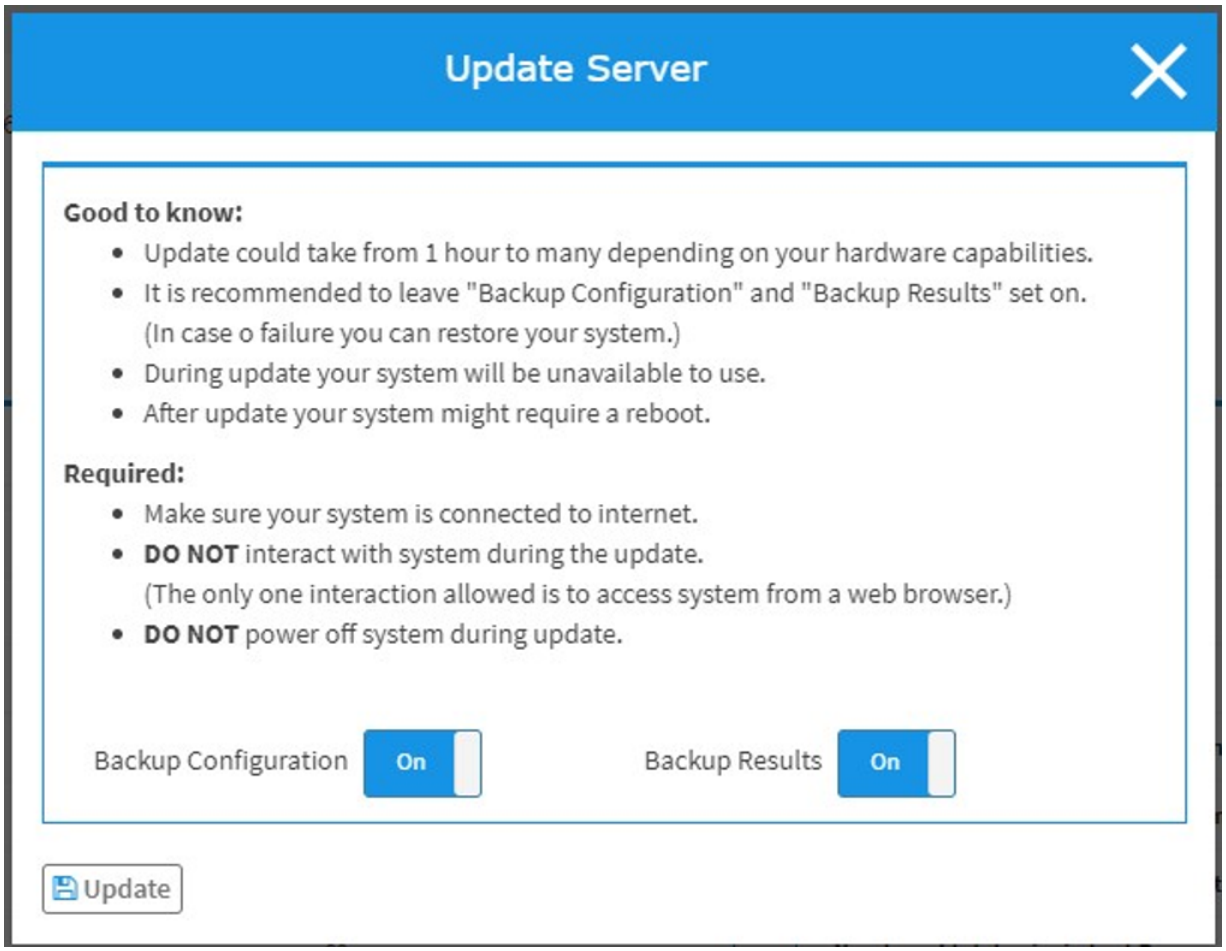
You can upgrade the Vision E1S running XR Version 5.0.1 or later versions with a connection to the internet to the latest release of XR Version from the UI:

1. Select **System** from the side bar, and select the **Check for updates** button:



   If an update is available, the **Update Server** button appears.

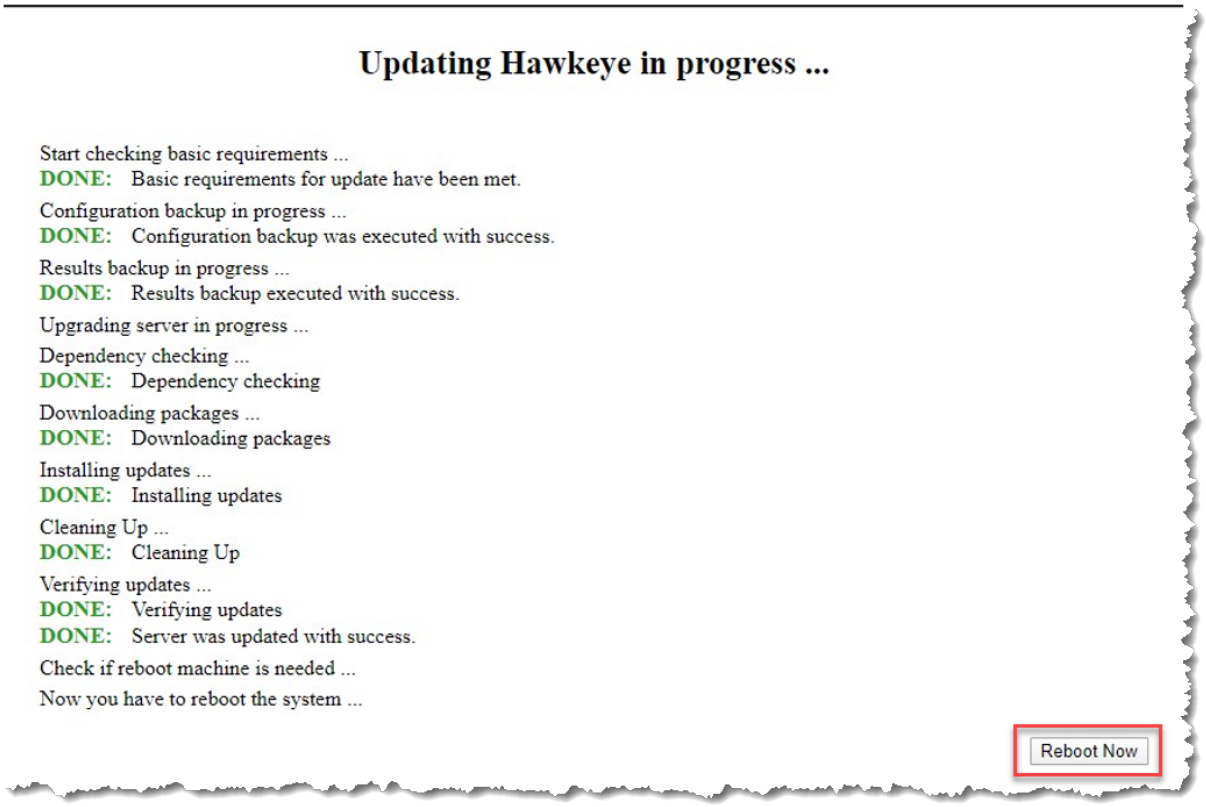
2. Select the **Update Server** button to open the **Update Server** dialog box.



3. Optionally select **Backup Configuration** and **Backup Results** to back up your configuration or results, and then select **Update**.

   A confirmation dialog box appears.

4. Select **OK** to start the update.
5. After the update starts, the system directs you to an **Update Status** page.



This page reports when each step in the update is done and checks to see if the system needs to be rebooted once the update is complete. If a reboot is required, you are prompted to reboot by selecting the **Reboot Now** button. If a reboot is not required, you are redirected to the login page when the update completes.

NOTE During the update the system will not be available for access by other users.

Offline update

You can upgrade the Vision E1S in Local Manager mode in offline update mode either from the user interface (UI) or from the command line program (CLI). This section describes both of these processes.

UI update process

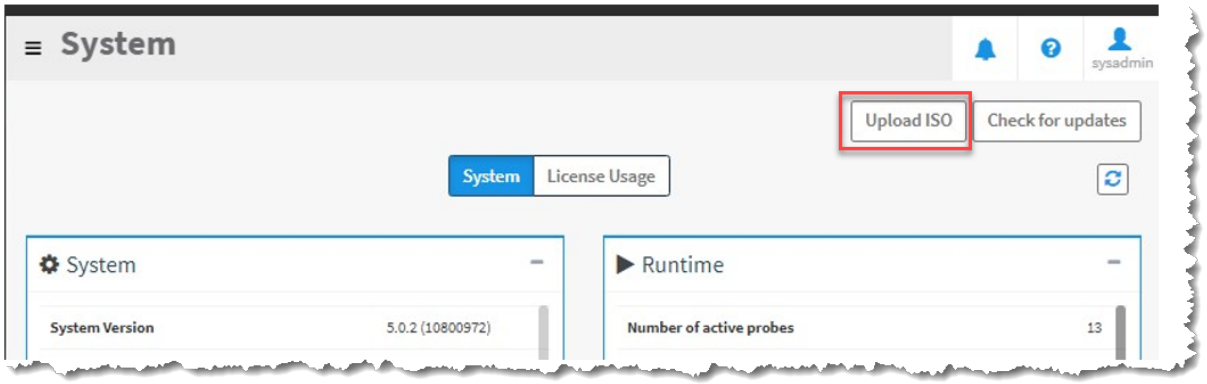
A Vision E1S must be running version 5.0.2 or later to support offline upgrade from the user interface (UI).

To update the Vision E1S from the UI:

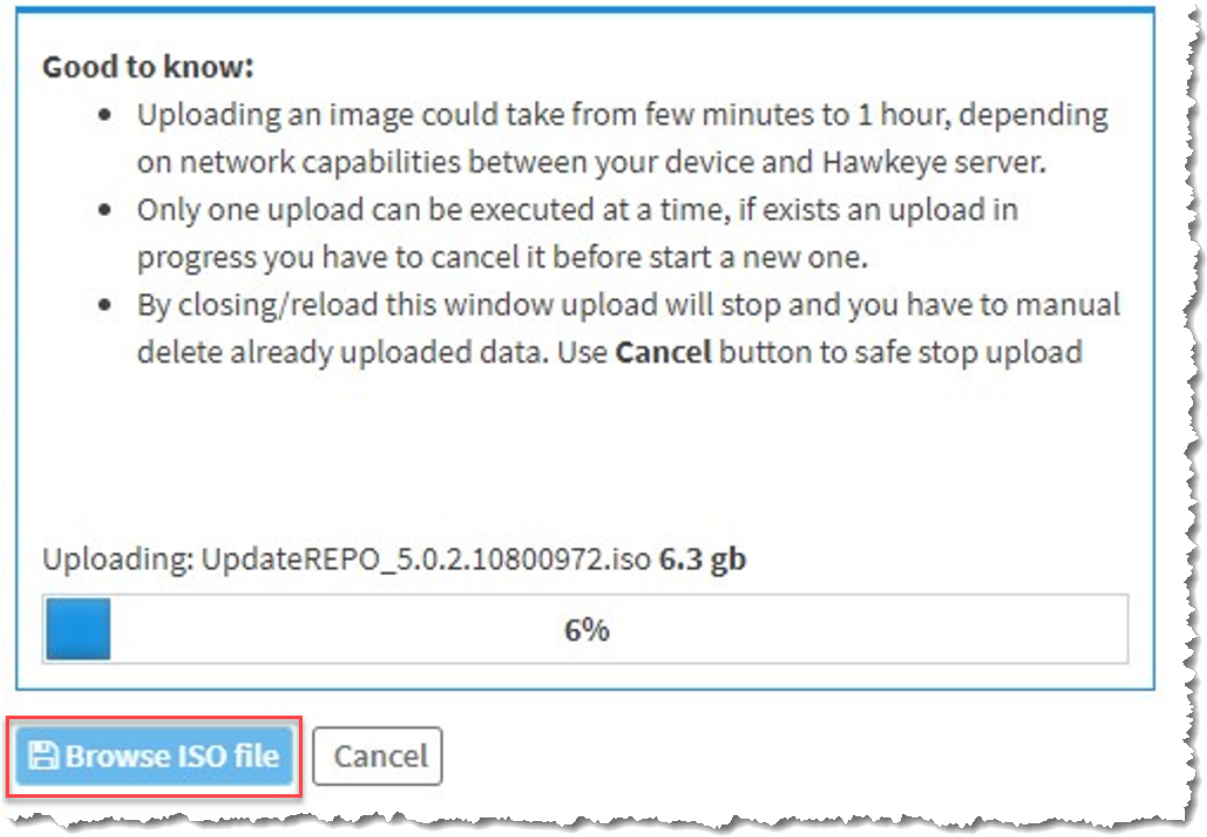
1. Download the UpdateRepo.iso file from support.ixiacom.com to your local machine.

   TIP Download the .iso file ahead of time, before you begin the UI update process.

2. Select **System** from the side bar, and then select the **Upload ISO** button.



The Upload dialog box opens in a new browser window.

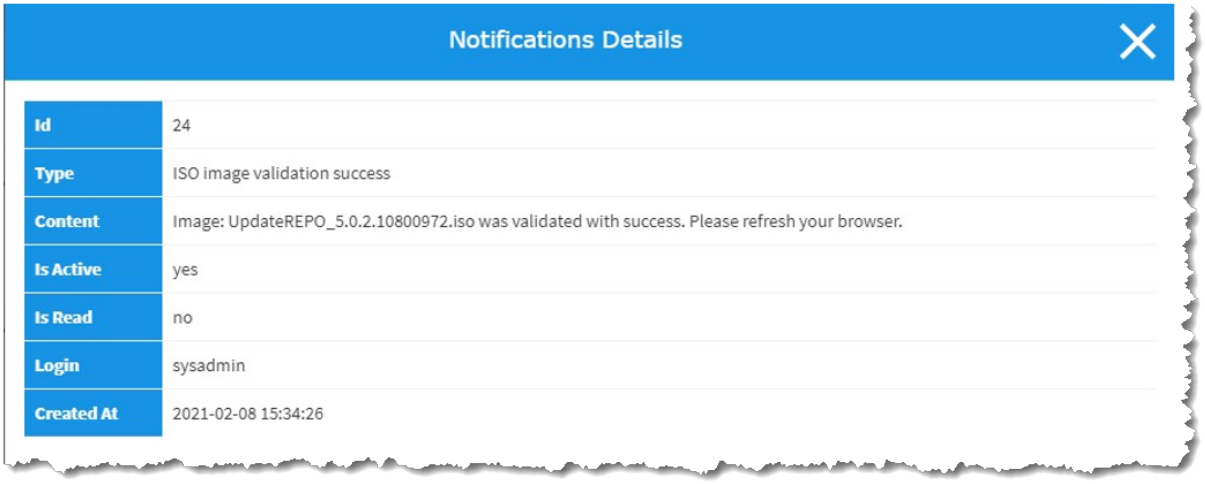


3. Select the **Browse ISO file** button, and then navigate to and select the **UpdateRepo.iso** file that you previously downloaded.
4. Select **Open**.

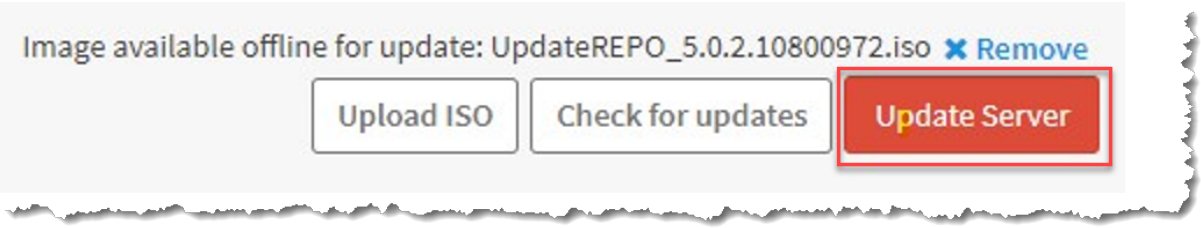
   The upload begins immediately after you select Open.

   If you do not refresh or close this browser window, the update continues while you continue to use Hawkeye and E1S.

   After the upload completes, the system validates that it is a Keysight update repository ISO file and shows a notification in the Hawkeye UI.



After Hawkeye validates the image, it displays the image available offline for update on the **System** page.



5. Select the **Update Server** button to start and continue the update process, similar to online update.

CLI update process

You can upgrade the Vision E1S in Local Manager mode running 5.0.1 or higher versions offline to the latest release of Hawkeye from the CLI.

To upgrade the Vision E1S with the CLI:

1. Download the .iso image from support.ixiacom.com.

   TIP Do this ahead of time, before you start the CLI upgrade process.

2. Transfer the .iso image to the /tmp directory of your Vision E1S, and run the following CLI command:

   ```
   #updateServer --offline <path to .iso file>
   ```

   If a reboot is required, the Vision E1S prompts you to reboot the system after the upgrade.

   NOTE The `updateServer` command can also perform backups and check for available updates if the server has an internet connection. To see other options available, run the following command:

   ```
   #updateServer -h
   ```

XR-E1S Probe - Install and Configure

The XR-E1S is a CentOS 7 based probe derived from the Vision E1S. It is the replacement for the Vision E1S to provide more performance for the Endpoint, less restrictions on routing, and full root access at the cost of no NETSTACK and no APPSTACK.

XR-E1S Prerequisites

The XR-E1S runs on the Vision E1S hardware. The XR-E1S requires the Vision E1S image 5.2 or newer.

NOTE If your vision E1S does not have the command `install_xr_ e1s`, please contact Keysight support for next steps.

XR-E1S Installation

To install the XR-E1S:

1. Log in to the Vision E1S as user `ksuser`.

   NOTE Do not change the interface Configuration prior to running `install_xr_ e1s`

2. Run the SR-E1S installation script from the command line: `install_xr_e1s`
   The system auto installs and reboots to the new image when the installation is complete.

   NOTE The interface configuration is not maintained between modes: Vision vs XR. You must configure each mode that is to be used.

XR-E1S - Configuration

After the successful deployment of the provided OVA or QCOW2 image in your Virtualization environment, connect to your Hawkeye Server.

To connect to your Hawkeye Server:

1. Sign in to the XR-E1S.
2. Change the default password.
3. Optionally configure an IP address (the default is configured for DHCP).
4. Connect to the Hawkeye Server.

Sign in to the XR-E1S

After deployment, use your serial connection or ssh to the XR-E1S to access the CLI.

The following is the default login information for the XR-E1S:

- username: `root`
- password: `keysight`

Change the default password

Please use the `passwd` command to change the password for root.

```
#passwd
Changing password for user root.
```

```
Changing password for root.
(current) UNIX password:
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
#
```

Connect to the Hawkeye Server

After your system is configured with access to the network, you can point it to your Hawkeye 5.2 or later Server using the `probeConfigure` command.

NOTE Note the `probeConfigure` command will set the linux hostname.

```
# probeConfigure
Probe/Host Name (xr-e1s):
Hawkeye Server (hawkeye-server):<HawkeyeServerName_IP>
```

XR-E1S CLI commands

The XR-E1S probe supports the following CLI commands:

Command	Options	Description
probeStatus	-v	Checks the Status of the XR-E1S system. -v option shows verbose output including status of individual components of the total system.
collectLogs	-a	Collects all the open log files.
probeVersion		Software version of the XR-E1S probe.
probeConfigure		Configure the probe name and Hawkeye Server.
systemInformation		Display system information: Serial Number, UUID, BIOS Vender, BIOS Version.
switch_mode		Switch between Vision E1s (PacketBroker Mode) and XR-E1S (Endpoint Mode).

E1S CLI Commands

The Vision E1S supports the following CLI commands:

Command	Options	Description
probeStatus	-v	Checks the Status of the E1S system. -v option shows verbose output including status of individual components of the total system.
collectLogs	-a	Collects all the open log files and snap shots of the Packet Broker configuration.
probeReboot		Reboots the Vision E1S device.
probeShutdown		Turn off the VisionE1S. The device will need to be power cycled to restart.
systemInformation		Display system information: Serial Number, UUID, BIOS Vender, BIOS Version
ksTcpdump	all tcpdump options	ksusers rtcpdump. Limits what interfaces can be used.
mountISO <filename.iso>		Filename of ISO, mount the ISO at /mnt/ks-iso and update the upgrade repository to point to the mount.
unmountISO		Unmout anything mounted at /mnt/ks-iso update the upgrade repository to point to the Keysight Repository.
chariotMode <disable|enable>		disable = turn on the firewall enable = turn off the filrewall
changeHostname <NewHostName>		Change the hostname of the Vision E1S device.

Command	Options	Description
linkstat	-v	Ethernet device link status
interfaceConfigure		Configure Ethernet interfaces for the Vision E1S device.
changeRepo	--url <URL>	Set Repo base URL
	--release <RELEASE>	Set desired Release version
updateServer	-h | --help	Prints help menu.
	-c | --backupConfiguration	Create a backup for configuration (MariaDB)
	-r | --backupResults	Create a backup for results (ElasticSearch)
	-v | --releaseVersion	Set a fix release version; ex: 5.0
	-a | --abort	Stop static files server, restart Hawkeye services
	-C | --checkVersionOnly	Check the current version and the possible update version
	-f | --force	Must force if the update is a Major Version change
	-u | --ui	(DO NOT USE) Request is performed from UI
	--offline <ISO Path>	Perform an update from a local Hawkeye Server ISO

Index

C

customer assistance 3

P

product support 3

T

technical support 3

© Keysight Technologies, 2025

This information is subject to change without notice.

www.keysight.com

913-2427-01 Rev A