Adding Scale & Resilience to FirePOWER Deployments using Ixia Visibility

Best Practice Deployment Guide

June 2016
COPYRIGHT AND DISCLAIMER

© Keysight Technologies, 2017

This publication may not be copied, in whole or in part, without Ixia's consent.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

Ixia, the Ixia logo, and all Ixia brand names and product names in this document are either trademarks or registered trademarks of Ixia in the United States and/or other countries.

All other trademarks belong to their respective owners.

The information herein is furnished for informational use only, is subject to change by Ixia without notice, and should not be construed as a commitment by Ixia. Ixia assumes no responsibility or liability for any errors or inaccuracies contained in this publication.
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>4</td>
</tr>
<tr>
<td>Target Audience</td>
<td>4</td>
</tr>
<tr>
<td>How To Mitigate FirePOWER Deployment challenges</td>
<td>5</td>
</tr>
<tr>
<td>Key Ixia technologies</td>
<td>6</td>
</tr>
<tr>
<td>Access Credentials</td>
<td>7</td>
</tr>
<tr>
<td>Best Practice Deployment Guides</td>
<td>8</td>
</tr>
<tr>
<td>Scenario 1: Out of Band Monitoring / Passive Mode</td>
<td>8</td>
</tr>
<tr>
<td>Scenario 2: Inline Network Resiliency</td>
<td>11</td>
</tr>
<tr>
<td>Scenario 3: Load Balanced Inline Deployment (also supports out of band)</td>
<td>15</td>
</tr>
<tr>
<td>Scenario 4: Advanced Failover Mechanisms</td>
<td>23</td>
</tr>
<tr>
<td>Scenario 5: Load Balancing Multiple Links</td>
<td>26</td>
</tr>
<tr>
<td>Scenario 6: Service Chaining Multiple Inline Tools (and filtering)</td>
<td>30</td>
</tr>
<tr>
<td>Products Tested in preceding deployment examples</td>
<td>37</td>
</tr>
<tr>
<td>Who to contact for further information on the Cisco Ixia joint solution</td>
<td>37</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

Cisco FirePOWER is an industry leading NGIPS solutions with powerful features and impressive specifications. However, in today’s competitive security market, IT customers are looking for system level security solutions that can cost effectively scale and change to their growing networks needs and resilient to outages. Ixia’s Network Visibility Solutions (NVS), including bypass switches and network packet brokers (NPB), complement Cisco’s security products to create the best-in-class scalable and resilient security solutions that IT professional need and want to purchase.

This best practice document draws on industry trends and lessons learned to add scalability and resilience to Cisco FirePOWER Next Generation Intrusion Prevention System (NGIPS) deployments. The methods and suggestions outlined in this document are provided to answer IT customer question on “how to” accomplish their scalability and resilience goals with FirePOWER. The use cases defined in this document are tested by Ixia, deployed at customers and are ready to be demonstrated with the intent of accelerating evaluation cycles, avoid technical pitfalls at deployment, and helping customers scale their Cisco FirePOWER deployments.

By closely linking Cisco FirePOWER and Ixia NVS products to build a system level solution, Cisco and Ixia’s mutual channel partners will gain the benefit of providing customers a complete highly scalable solution that is easy to deploy.

The paper spells out how to integrate Cisco FirePOWER with Ixia’s NVS to proactively:

- Enhance Inline network resiliency
- Dynamically load balanced workloads across multiple Cisco NGIPSs
- Maximize Cisco NGIPS utilization by accessing multiple network links across the data center to a pool of Cisco NGIPSs
- Implement advanced failover mechanisms to prevent outages and minimize maintenance downtime
- Build high availability into mission critical deployments

Specific details of how to configure the Ixia and Cisco devices to achieve these goals are provided in the Scenario examples later in this document

Target Audience

This Best Practice Deployment Guide is intended to assist Cisco and partner technical resources who help their customers with planning, deploying, and managing Cisco security solutions. This document highlights key considerations to avoid pitfalls, operational challenges, and customer constraints by leveraging Ixia’s Network Visibility Solutions. The document also provides specific configuration details for the use case scenarios covered.

This document is not intended to be a full set of documentation. Please consult Ixia Network Visibility, and Cisco Next Generation IPS Admin and User guides for complete technical details on the referenced products.
HOW TO MITIGATE FIREPOWER DEPLOYMENT CHALLENGES

The following list of typical problem areas can negatively impact successful Cisco FirePOWER POCs, technical designs, deployments and create unnecessary support calls.

Table 1 outlines the ways Ixia’s Network Visibility solutions help you get over typical scalability and resilience challenges in FirePOWER deployments. (Details of how to configure such solutions are provided later in this document)

<table>
<thead>
<tr>
<th>Table 1: Solutions to typical FirePOWER deployment challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Problem Areas</strong></td>
</tr>
<tr>
<td>flexibility</td>
</tr>
<tr>
<td>Resilience</td>
</tr>
<tr>
<td>Scalability</td>
</tr>
<tr>
<td>Mix of network link speeds (1G, 10G, 40G)</td>
</tr>
<tr>
<td>Maximize tool efficiency</td>
</tr>
<tr>
<td>High Availability</td>
</tr>
<tr>
<td>Coexistence</td>
</tr>
</tbody>
</table>
Key Ixia technologies

Ixia Network Visibility Solutions works in concert with Cisco FirePOWER to protect customer networks. Ixia NVS provides Inline bypass switch and load balancing technology for offering highly resilient, fault-tolerant, and scalable FirePOWER deployments. FirePOWER deployments can be upgraded or expanded as the customer’s traffic and protection needs increase, without the need to take the current FirePOWER units out of service. Ixia NVS may also be used out of band.

iBypass

Ixia offers a family of bypass switches providing failsafe inline protection to fit any size network. Today’s enterprise networking environment uses many security, performance and analytics tools. Over months of continuous operation, tools require rebooting, maintenance and upgrades as business needs grow. All of Ixia’s bypass switches safeguard networks with automated failover protection ensuring temporary tool outages do not become network outages.

Network Packet Broker

The Ixia Vision ONE is a purpose-built network packet broker (NPB) for monitoring high-speed network traffic, letting you share the network’s rapidly increasing traffic load among multiple Cisco security solutions via load balancing. Vision ONE allows inline tool deployment in serial, parallel, or combined mode, and provides failover features to maximize scalability and resiliency of Cisco FirePOWER deployments.

Key Benefits

- Inline security tools can be deployed very flexibly to meet varying customer requirements. They can be deployed in serial (for service chaining) or in parallel (for load balancing), or both to maintain maximum flexibility
- Tool-sharing reduces costs by allowing multiple departments in an organization to utilize the same monitoring tool to monitor multiple links throughout the organization
- Filtering increases efficiency and maximizes tool utilization by sending each tool only the traffic it needs.
ACCESS CREDENTIALS

The following are factory default login credentials for the products referenced in the deployment use cases in this document. Login credentials may differ in your environment.

**Ixia**

**iBypass**

Initial management port IP address configuration via console cable (see iBypass User Guide for details)

then access via https://<ip-address>

username: admin  password: ixiacom

**Vision ONE**

Initial management port IP address configuration via Craft port cable (see Vision ONE Install Guide for details)

then access via http://<ip-address>

username: admin  password: admin

**Cisco**

FireSIGHT Defense Center (management console for FirePOWER units)

Initial management port IP address configuration via CLI (see FireSight System Installation Guide for details)

Then access via https://<ip-address>

username: admim  password: Cisco  (for some versions password may be Sourcefire)
Scenario 1: Out of Band Monitoring / Passive Mode

<table>
<thead>
<tr>
<th>Description</th>
<th>Solution features</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out of band deployment of Cisco security solutions can help customers monitor &amp; alert for intrusions, with minimal impact on network operations</td>
<td>• Ixia external iBypass Switch (configured in TAP mode for out of band monitoring)</td>
<td>• Traffic continuity is preserved in case of Cisco FirePOWER IPS failure or traffic overload</td>
</tr>
<tr>
<td></td>
<td>• (Depending on iBypass Model) Passive monitoring of 1G, or 10G links</td>
<td>• FirePOWER can be taken out of service for upgrade or repair without taking down the network</td>
</tr>
<tr>
<td></td>
<td>• Various copper or fiber media options (depending on model &amp; connected SFPs)</td>
<td>• FirePOWER connected in passive tap mode can later converted to inline intrusion blocking mode without significant downtime or having to rewire the connections</td>
</tr>
<tr>
<td></td>
<td>• Link Fail Detect options (configurable)</td>
<td>• Proven bypass switch technology addresses customer objections of single point of failure</td>
</tr>
<tr>
<td></td>
<td>• Easily switch over to inline mode when ready</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 3 - bypass switch set to TAP Mode**

external network

Ixia iBypass (in TAP Mode)

eth1

eth2

Cisco FirePOWER NGIPS

internal network
How to Configure

- Cisco

(for this configuration, a physical deployment as shown in Figure 3 is assumed to have been wired up)

Edit FirePOWER IPS Device Ports for Passive Monitoring, first eth1, then eth2
(eth1 will receive traffic in the external network to client network direction, while eth2 will receive traffic in the internal to external direction)

Login to Cisco FireSIGHT Defense Center which is managing the relevant Cisco FirePOWER NGIPS

- From Devices -> Device Management screen click the IP address of the desired NGIPS device
- Click the Interfaces tab, then click the pencil icon beside eth1
  - Change the mode to Passive
  - Normally leave other settings default, then click Save
- Click the pencil icon beside eth2
  - Change the mode to Passive
  - Normally leave other settings default, then click Save

You must next apply the changes to the IPS device

- Click the Apply Changes button near the top right hand corner of the screen
(It can take a few minutes to finish applying, you’ll see a link to check status)
Ixia

- Login to Ixia iBypass switch GUI, then go to the Configuration tab
- Set the Bypass Mode to TAP. Then click Apply
  - Note: other system values can normally be set as shown below, most of these are default. You can optionally set LFD (link fail detect) to On, so that if one network Port fails it will bring the other network port down (signaling to the connect network devices that the link is unavailable)

Traffic will continue to flow normally between network PORT A and PORT B in both directions, at the same time a copy of A -> B traffic will be sent to Monitor Port 1, and a copy of B -> A traffic will be sent to Monitor Port 2

Looking at the Statistics tab, you can confirm traffic shows up on network ports A & B, as well as monitor ports 1 & 2
## Scenario 2: Inline Network Resiliency

<table>
<thead>
<tr>
<th>Description</th>
<th>Inline bypass combined with Cisco security solutions can help customers actively block intrusions, while overcoming network resiliency concerns.</th>
</tr>
</thead>
</table>
| Solution features | - Ixia iBypass external bypass switch  
- Active inline access for 1G or 10G links (depending on model)  
- Various copper or fiber media options (depending on model & connected SFPs)  
- Automatic Fail-Open and Fail-Closed options (configurable)  
- Heartbeat health check technology |
| Benefits | - Cisco FirePOWER can be configured to actively block malicious intrusions.  
- Traffic continuity is preserved in case of Cisco FirePOWER IPS failure or traffic overload  
- FirePOWER can be taken out of service for upgrade or repair without taking down the network  
- Chose in configuration whether to allow or block network traffic if the FirePOWER is unavailable (Fail-Open of Fail-Closed)  
- Heartbeats detect soft failures above and beyond hardware problems  
- Proven bypass switch technology addresses concern of single point of failure |

![Diagram](image-url)  

*Figure 4 - Inline Bypass with Heartbeat*
How to Configure

- **Cisco**

(for this config, a physical deployment as shown in Figure 4 is assumed to have been wired up)

Edit IPS Device Ports for Inline Monitoring, first eth1, then eth2

(note: depending on Cisco deployment interface names/numbers may vary, as tested here eth1 connects to the external network, and eth2 to the internal network)

Login to Cisco FireSIGHT Defense Center which is managing the relevant Cisco FirePOWER NGIPS

- From Devices -> Device Management screen click the IP address of the desired NGIPS device

  - Click the Interfaces tab, then click the pencil icon beside eth1
    - Change the mode to Inline
    - Select Security Zone of External
    - Select Inline Set of Default Inline Set (unless you use another set)
    - Make sure Enabled box is checked, and click Save

  - Next click the pencil icon beside eth2
    - Change the mode to Inline
    - Select Security Zone of Internal
    - Select Inline Set of Default Inline Set (unless you use another set)
    - Make sure Enabled box is checked, and click Save

- You must next apply the changes to the IPS device

  Click the Apply Changes button near the top right hand corner of the screen

  (It can take a few minutes to finish applying, you’ll see a link to check status)
Ixia Login to Ixia iBypass switch GUI, then go to the Configuration tab

In the System section do the following

- Set the Bypass Mode to Fail-Open. Set Bypass Detect to Off. Then click Apply
  - Note: other system values can normally be set as shown below, most of these are default. You can optionally set LFD (link fail detect) to On, so that if on network Port fails it will bring the other network port down (signaling to the connected network devices that the link is unavailable)
  - Note: You can optionally set Bypass Mode to Fail-Closed so that if the FirePOWER NGIPS where to be out of service, the network link would be forced down. This provides the strictest security possible, at the expense of potential lost connectivity.

In the HeartBeat section you will need to modify the default heartbeat packet for both Port 1 and Port 2. As a starting point, you can copy and post the value below (which has been tested with Cisco FirePOWER) into the Heartbeat Packet field for both ports.

00 50 c2 3c 60 00 00 50 c2 3c 60 01 81 37 FF FF 00 3c 18 d2 00 00 80 01 0a ff 0a 02 01 dc 0a 01 01 12 08 00 37 5c 02 00 14 00 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69

Edit the Destination MAC and Source MAC portions of the packet so that if you have multiple iBypass switches in your environment, Vision ONE won’t mistake the heartbeats as conflicting and drop them. This can be accomplished by editing the 6th and 12th Hex pairs for Port 1 and Port 2 as highlighted below. (use different Heartbeat DMAC & SMAC values for each iBypass switch and Vision ONE in your environment)

Best practice it to set Heartbeat Retries to more than 1, we have used 4 in this example.

- Once your Heartbeat Packets are edited, click Apply
• Go to the Status tab
  o If Heartbeats are traversing the FirePOWER tool successfully, then the Bypass status will show **Off**

  ![FirePOWER Status](image)

• Cisco

• Returning to your FireSIGHT GUI you can check that the system is seeing traffic and events. One place to do this is in the Analysis -> Content Inspection screen (you may need to press the Reload button to see fresh results)

  ![FireSIGHT GUI](image)

• You can also confirm that reports about traffic & blocked intrusions are providing data. For example in the Overview -> Dashboard -> Application -> Intrusion Events page

  ![FireSIGHT Intrusion Events](image)

Note: this is a sample report from our test environment, specific report data shown in your environment will depend on actual network traffic, and proper configuration of FirePOWER NGIPS.
Scenario 3: Load Balanced Inline Deployment (also supports out of band)

Description
Individual FirePOWER IPS Appliances may not have sufficient capacity to fully protect busy network links, especially in the case of high speed connections and bandwidth intensive applications.

Solution Features
- Ixia Vision ONE inline Load Balancing
- Load balance 10/40G network traffic across multiple FIREPower NGIPS Appliances
- 2 or more inline IPS Appliances, up to 20 per load balanced group
- Symmetry awareness, specific session uses same IPS in both directions
- Intelligent inline 5 tuple filtering to exclude non-essential traffic from IPS inspection
- Configurable options to pass through or block non-essential traffic on network
- Also supports a mix of inline and out of band deployments
- Configurable Heartbeat health check technology

Benefits
- Wire speed protection for 10/40G network traffic & bandwidth intensive applications
- Heartbeat technology protects against “brown out” type issues - i.e. degraded performance due to too much traffic going through IPS appliance, removes appliance from group until heartbeats return
- Improve capacity by filtering and forwarding only relevant protocols to NGIPS appliances
- Support for inline as well as out of band deployments
- Easily scale additional FirePOWER NGIPS appliances as traffic loads and protection needs grow
- Proven bypass switch technology addresses customer objections of single point of failure

Figure 5 Load balance across Tools
How to Configure

(in this configuration example, a physical deployment as shown in Figure 5 is assumed to be wired up)

• **Cisco**

  Login to Cisco FireSIGHT Management Console
  - Add a 2nd (or more) FirePOWER Appliances
    - Use same inline configuration (as in Scenario 2) for the additional appliance.
    - Start from Devices -> Device Management screen, then click Add Device
      (note: please consult Cisco FireSIGHT docs for further details of the process of adding additional FirePOWER Devices)

  ![Cisco FireSIGHT Management Console](image)

• **Ixia**

  Configure Ixia Bypass Switch in same manner as described in Scenario 2

  Configure Ixia Vision ONE for inline load balancing between the Bypass Switch ports (P17 & P18 in this example), and two inline FirePOWER units (port pairs P11/P12 & P13/P14 in this example)
  - Login to the Vision ONE GUI and click the Inline Diagram tab
  
  ![Ixial Vision ONE Inline Diagram](image)
  
  - Create the Bypass Port Connections by double clicking Add Bypass Port Pair
    - In the General tab provide a name for the bypass link and click OK

  ![Add Bypass Port Pair](image)
In the **Ports** tab, first click **Add** in the Side A Ports section, then select an available port from the list to use for the Connection to Bypass Switch Port A – & click **OK**

- In same way add the Side B Port for the connection to Bypass Switch Port B

Click **OK** to save both the ports you just added to the configuration.
• Create a tool group for your FirePOWER appliances by clicking **Add Inline Tool Resource**

- In the **General Tab**, give the tool group a Name, & select **CiscoFIREPOWER** from the **Heartbeat** pulldown

FYI ONLY: if you wish, you may examine the Heartbeat packet format, click Library -> Tool Hearbeats then select the heartbeat you assigned in the last step. You’ll notice the Heartbeat is similar to that configured in the Bypass switch during Scenario 2, other than the different Source / Destination MACs

**NOTE**: it is important that the overall heartbeat interval of the Vision ONE be less than that of the iBypass switch configured in Scenario 2. Here we use the default interval of 1000ms with 3 retries, which is less than the 1000ms internal with 4 retries configured earlier on the iBypass.
In the Inline Tool Ports tab, click Add in the Side 1 Ports section to add a tool port which faces the Port 1 side of the network (aka external)

- Select an available port from the list and click OK
- Repeat previous step this time clicking the Add button in the Side 2 Ports to add corresponding tool port that faces Port 2 side of the network (internal).
- Give your newly added ports an Inline Tool Name, then click Create Tool Pair
- Repeat the previous steps to add additional tool pairs for other FirePOWER appliances that you want to belong to the inline load balanced group.
- You will now see a list of tools in your load balanced group, by default they will all be ACTIVE meaning traffic is balanced across the members of the load balanced groups in a session aware manner. Click OK to activate your new load balanced inline tool group.
Next Click *Add Service Chain* to make a connection between your FirePOWER tool group, and the Bypass Switch Port Pair

- In the *General Tab*, provide a suitable Name, and ensure the *Service Chain Traffic Direction* is bi-directional as shown below.

- In the *Bypass Port Pairs* tab click *Add* and select the Bypass you added in the earlier step, then click *OK*.

- Note: The *Criteria* tab can be left with the default filter of Pass All, unless you wish to limit types of traffic to traverse the FirePOWER tools, in which case you can use Ixia’s filters to do so (see example in Scenario #6).

- In the *Inline Tool Resource* tab, click *Add* to assign the FirePower Inline Tool Resource you created previously, then click *OK*.
The default failure action is *Fail Closed*, this is invoked if all members of the FirePOWER load balance group fail to pass traffic. The IXIA iBypass switch will see the failed condition, and react accordingly. The bypass was configured earlier to *Fail-Open*, meaning network traffic passes even when FirePOWER IPS protection is not available.

Click *OK* to activate the Service Chain Option: If desired this iBypass switch setting can be changed to *Fail-Closed*, meaning the network link be be unable when all FirePOWER IPS in the load balanced group are not available.

- You can now return to the iBypass Switch status screen, if the Bypass status is *OFF*, you know that heartbeats are still making it through the Load Balanced group and FirePOWER IPS protection is thus available.

Below is what the completed FirePower Inline Load Balanced tool group will look like in the *Inline Diagram*. If the Tool Resource shows Green then all tool in the group are passing Heartbeats and are available, if the Tool Resource is Yellow some portion of the Load Balanced Tools are failing to pass Heartbeats, and if the Tool Resource is Red ALL this means members of the tool group are unavailable.
To validate that live network traffic volumes other than heartbeats are actively passing through the tool members of the load balanced group, go to the Ports menu, select the Statistics option, and look at the utilization of the applicable ports (in this example P11/P12 & P13/P14 are both seeing traffic).

- **Cisco** (Optional) you can further validate load balancing within the Cisco FireSIGHT Management Console. Go the **System -> Monitoring/Statistics. Select Device for of** the FirePOWER Devices in turn and take note that both are processing Intrusion Events. (depending on traffic patterns it may take time for these metrics to update)
Scenario 4: Advanced Failover Mechanisms

Description
In event that an FirePOWER IPS unit fails or requires maintenance, ensure that remaining units automatically take over inspection of the units traffic in a fault tolerant, session aware manner.

Solution

- Ixia Vision ONE inline protection with Active and Standby security tools
- Automatic failover to Standby based on link down or loss of Heartbeats through Active tool
- Option to manually take Active tool Offline
- Load balancing features continue to be available (as per Scenario 3)

Features

- Graceful algorithm minimizes session disruption when appliances fail
- Flexibility to support any combination of Active/Active and Active/Spare failover
- Automatic hot standby failover
- Take units out of service for maintenance without disruption the network
- Ability to support multiple different inline tools in load balanced groups, so that FIREPower can be integrated in any existing customer environment
- Also supports out-of-band deployments

Benefits

- Ixia Vision ONE (load balancing)

![Diagram of Active Standby Failover]

**Figure 6 – Active Standby Failover**

- In this example FIREPower IPSs are connected to port pairs 11&12, 13&14. The IPS on ports 13 and 14 is declared as a spare in this configuration. This means it will only receive traffic when the other IPS becomes unavailable (loss of link, or failure of Heartbeats to traverse the IPS).
- Optional (not shown here) multiple Active FirePOWER IPSs could have been configured. In that case the Standby tool would become active if any one member of the Active tools became unavailable.
How to Configure

(in this config example, a physical deployment as shown in Figure 6 is assumed to be wired up)

- **Cisco**
  
  - No changes are required to Cisco NGIPS configuration that was specified in regular load balancing Scenario 3

- **Ixia**
  
  - No changes to Ixia Bypass Switch, configured in same manner as described in Scenario 2

  - Configure Ixia Vision ONE for inline connection to/from two inline FirePOWER units (port pairs P11/P12 as Active, and P13/P14 as Standby). Starting point is configuration from Scenario #3.
    
    o Login to the Vision ONE GUI and click the Inline Diagram tab.
    
    o Double click the FirePOWER Inline Tool Resource & click the Inline Tool Ports tab
    
    o Change the 2nd FirePOWER tool in the list from Active to Standby, then click OK

- Returning to the Ports tab, and viewing Statistics, you will note that traffic is no longer traversing the P13/P14 pair (the FirePOWER unit you just put into Standby).

And if you return to look at your Inline Tool Resource screen, you also note FirePOWER-2 tool status has changed to Standby.
• The Standby tool can take over for the Active tool when the Active tool becomes unavailable. This occurs when link is lost on the Active tool, or Heartbeats fail to pass through the Active tool. In the example below, we simulated a downed tool by disabling the link on FirePOWER #1. Note that its Tool Status changes to Offline, while the Tool Status of FirePOWER #2 changes to Active.

• Alternatively, we could have manually taken the Active tool out of service by changing the Configured Tool Role to Offline Mode, and configuring FirePOWER #2 as Active (note: one Active tool pair must always be configured per Inline Tool Resource in order for traffic to pass). For example, this might be done when scheduled maintenance is being performed on FirePOWER #1. (below shows what the Inline Tool Resource would look like after making the change).
Scenario 5: Load Balancing Multiple Links

Description
Customer wants to distribute traffic from multiple network links across a common FIREPower IPS appliance (or load balanced group of FirePOWER appliances).

Solution

Features
- Ixia iBypass and Vision ONE for inline protection of multiple network links
- Traffic that comes into Vision ONE from a particular network link is sent back out the same link
- Can be used in conjunction with Vision ONE inline load balancing
- All features applied to single network link continue to be available (as per previous sections)

Benefits
- Maximize resource utilization, using a pool of FirePOWER NGIPSs for multiple network links
- Maximize Cisco FirePOWER capacity when combined with Ixia Vision ONE load balancing
- Resiliency via Active/Active and Active/Standby failover options.
- High Availability topology options

Figure 7 Load Balance Multiple Links to NGIPS Farm

Topology is the same as in Scenario #3, except that an additional bypass switch has been added on a 2nd network link, and that Bypass switch has been connected to ports P19 and P20 of the Vision ONE load balancer. In our example we will assume these network links are separate and unrelated to each other. In this scenario we’ll assume we want to maintain network connectivity in any situation, and thus leave the iBypass switches configured as Fail-Open.

High Availability topology option: However if these two network links were part of a redundant network topology, we might instead choose to configure the Bypass switch as Fail-Closed, in this case if one path became unavailable, the network routing/switching would be aware of the outage and would route/switch the traffic through the other iBypass switch.)
How to Configure

- **Cisco**

  - Configuration of the FirePOWER NGIPS devices is unchanged from Scenario 3

- **Ixia**

  - Bypass Switch #2 is configured the same way as Bypass switch #1 (from Scenario 2), with following exception:
    - The 6th and 12th Hex pairs of the Port 1 and Port 2 Heartbeat packets must be changed so that they are different from those of Bypass Switch #2 and the Vision ONE NPB. This gives the Heartbeats from Bypass Switch #2 different Destination & Source MAC addresses than Bypass Switch #1.
    - Go to the Configuration page of Bypass Switch #2, edit the two Heartbeat packets, then click **Apply**

  - Add 2nd Bypass Tool Pair to the Cisco-FirePower Service Chain configured during Scenario #3

    Login to Vision ONE and click the **Inline Diagram** tab
    - Double Click the **Add Bypass Port Pair** area, the dialog below opens
      - In the **General** tab, give the Bypass Pair a suitable name
In the *Ports* tab, *Add* Vision ONE ports P19 and P20 as the Side A and Side B Ports respectively, then click *OK*

- With your mouse, drag a connection between your new Bypass Port Pair, and the Cisco-FirePOWER Service Chain that was setup during Scenario #3.
  - You will be prompted to accept *Tool Sharing* (i.e. share the tools between the bypass pair links), click OK.

- Your *Inline Diagram* will look as follows. Vision ONE automatically makes sure that traffic arriving on a particular link, goes out that same link. This is accomplished by Vision ONE adding a VLAN tag at the ingress of the Service Chain (the VLAN tag is stripped at the egress of the Service Chain).

- The VLAN tags used by each Bypass Port Pair can optionally be edited. VLAN IDs must be unique for tech Bypass Port Pair.
• If you examine the Status screen of the 2nd iBypass Switch, you’ll notice that the Bypass status is now OFF, indicating traffic is also flowing from the 2nd link through the Vision ONE and the connected inline FirePOWER tools.

• As a further check, go back to your Vision ONE GUI, select the Ports tab, click the Statistics radio button. Assume there is network traffic present, you will now see utilization on both Bypass Port Pairs (P17/P18 and P19/P20). You will also notice traffic traversing both FirePOWER Tool Pairs (P11/P12 and P13/P14).

ASIDE: if your POC environment does not allow for live network traffic, Ixia has a variety of test tools available, such as Ixia BreakingPoint, which can generate realistic application and security threat traffic. Ixia tests could be connected to the Network Ports of the Ixia iBypass switches to create a realistic test environment. Please contact Ixia for further information on these solutions.
Scenario 6: Service Chaining Multiple Inline Tools (and filtering)

<table>
<thead>
<tr>
<th>Description</th>
<th>Customer wants to deploy Cisco FirePOWER IPS alongside additional monitoring tools, both inline and out of band</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solution Features</td>
<td></td>
</tr>
<tr>
<td>• Send same network traffic inline through Cisco FirePOWER NGIPS, and through other specialized inline tools which a customer might have (e.g. Web Application Filter).</td>
<td></td>
</tr>
<tr>
<td>• Ixia Vision ONE filters traffic so that only relevant types relevant to particular tools gets sent to it</td>
<td></td>
</tr>
<tr>
<td>• Optionally, send copy of the network traffic to out of band tools for purposes other than Security (e.g. Application Performance Monitoring)</td>
<td></td>
</tr>
<tr>
<td>• Compatibility with load balancing, multilink, and all scenarios discussed earlier in this document</td>
<td></td>
</tr>
<tr>
<td>Benefits</td>
<td></td>
</tr>
<tr>
<td>• Allows deployment of Cisco FirePOWER alongside existing customer tools.</td>
<td></td>
</tr>
<tr>
<td>• Improves capacity by filtering and forwarding only relevant protocols to the particular tools that need to see them.</td>
<td></td>
</tr>
<tr>
<td>• Proven bypass switch technology addresses customer objections of single point of failure</td>
<td></td>
</tr>
<tr>
<td>• Add additional monitoring tools as traffic loads and customer protection needs grow</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 8 Service Chaining Multiple Monitoring Tools**

- Example configuration is as per Scenario #3, but just a single FirePOWER unit connected to P11/P12 belongs to the FirePOWER Inline Tool Resource. From there traffic is sent through Inline WAF connected to P15/P16, before being sent back to the Bypass Port Pair. Traffic is filtered for HTTP/HTTPS only.
- In addition an unfiltered of all copy of packets is sent from P17 to and out-of-band APM on P27
How to Configure

- **Cisco**
  - No changes to FirePower Configuration required, same as in Scenario 3

- **Ixia**
  - No changes to Bypass Switch Configuration required, same as Scenario 2

Configure Vision ONE. In this example scenario we will configure a single inline Cisco FirePOWER to identify intrusion threats, and from there pass the traffic to an inline WAF so that the WAF can stop specific unauthorized web transactions. In this example the FirePOWER and WAF are protecting a Web server farm, there is no need to pass traffic other than HTTP / HTTPS through the Service Chain, so we will filter other traffic out.

In addition we will configure Vision ONE to send an unfiltered copy of all traffic from the external network port of the Bypass Switch, over to an Application Performance Monitor tool which will measure metrics such as application response time on all traffic.

- **Login to GUI of Vision ONE, and click Inline Diagram**
  - Click the FirePower Inline Tool Resource, click the X beside FirePOWER-2 and click OK. *(this leaves a single FirePOWER tool. Although it is possible to Service Chain a load balanced Tool Resource, to another tool resource, we are no doing so in this example)*

  - Although Service Chaining supports multiple Bypass Links in this example we are protecting a single Bypass link, so we remove Bypass Switch #2, and disable Tool Sharing in the Service Chain for Bypass Switch #1. We’ll also apply our HTTP/HTTPS filter.
    - Right click the connection between Bypass Switch #2 and the Cisco-FirePOWER Service Chain, the select Delete
Double Click your Cisco-Firepower Service Chain, then select the *Bypass Port Pairs* tab. Ensure the *Enable Tool Sharing* option is UNCHECKED, then click OK.

Double Click the Cisco-FirePower Service Chain, then select the *Criteria* Tab. Choose Filter Mode of Pass by Criteria, then click *L4 Port*, then choose HTTP from the Port Set pull down, choose *Type Source or Destination*, then click OK.

- Repeate the previous step to add another Criteria of HTTPS to the Cisco-FirePower Service Chain.
- One more thing for your filter, remember that the Bypass Switch is sending Heartbeat packets to test the availability of the inline tools, you must also allow those through or the Bypass Switch will go into Bypass mode. The Heartbeat packets are not HTTP or HTTPS, so add a criteria for the MAC address of the Bypass Heartbeat packets (as per the MAC address used in Scenario #2).
o Finally, in the Criteria tab, select the Match Any (OR) button, then click OK to apply the change to the configuration.

Note: Filtering Criteria could also have optionally been used in Scenarios 3, 4, & 5

• Next add the WAF tool. Double Click the Add Inline Tool Resource area, in the General tab give the Inline Tool a Name, and choose a suitable Heartbeat from the list.
Click the **Inline Tool Ports** tab, **Add** a port to Side 1 (external) and Side 2 (internal) of the network (in our example P15 and P16 respectively). Provide an Inline Tool Name, and click **Create Port Pair**.

You’ll now see your new Inline Tool Resource for the WAF listed, click **OK** to save it to the Vision ONE configuration.

Next, Double click the Cisco-FirePOWER Service Chain, select the **Inline Tool Resource** and **Click Add**. You will see your WAF Inline Tool Resource listed, select it then click **OK** to add the WAF to the Service Chain.
- (the default Failure Action is Fail Closed, which stops traffic flow if the Inline Tool Fails to pass Heartbeats. Optionally you can change this to Fail Open). Click OK to save the change to the Vision ONE configuration.

- The Service Chain will now look as follows in the Inline Diagram

Note: Hover your mouse over Side A of TechPtnr-Bypass1, make a mental note for the next step that Side A uses Port Group 1 (PG1), you’ll need this information to configure the Out Of Band tool.

Next we’ll add the out of band tool, click the Diagram tab of the GUI to configure this.

- From the Diagram, right click the Port connected to the out of band tool (in our example P27), configure it as a Tool Port, selected Enabled State, then click OK.
From the Diagram, right click the network side of PG1 and select Connect To to make a connection from it to your newly configured Tool Port.

- Specify P27 as the Tool Port, then click OK

- The Diagram now shows the connection from PG1 to the Out of Band tool port, double click on the Filter connecting the port, ensure it is configured as Pass All (Deny All is the default), then click OK to allow unfiltered traffic to the Out of Band APM tool.

- If we examine utilization stats on PG2 (Internal Side of Inline Service Chain), we notice fewer packets being inspected than on F8 (the filter connected to P27, the Out of Band tool). This is expected behavior as we are only sending HTTP/HTTPS through the Inline Service Chain, but all application traffic to P27.
PRODUCTS TESTED IN PRECEDING DEPLOYMENT EXAMPLES

**Ixia**

iBypass 3 copper IBP-HBCU3 - Version 1.0.0.21  *(note, other Ixia iBypass models with Heartbeats can also be used)*

Vision ONE SYS-VISION-ONE - Version 4.4.1.7  *(chassis)*

LIC-SYS-V-ONE  *(license to add inline capabilities to the chassis)*

**Cisco**  *(note, other models of FireSIGHT / FirePOWER can also be used)*

FireSIGHT Console  3D Virtual Defense Center (64 bit) – Version 5.4.0

FirePOWER Devices  Virtual Device (64 bit) – Version 5.4.0

WHO TO CONTACT FOR FURTHER INFORMATION ON THE CISCO IXIA JOINT SOLUTION

cisco-security@ixiacom.com