Adding Scale & Resilience to Imperva Deployments using Ixia Visibility

Best Practice Deployment Guide

August 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 Imperva 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 / Sniffing Mode</td>
<td>8</td>
</tr>
<tr>
<td>Scenario 2: Inline Network Resiliency</td>
<td>12</td>
</tr>
<tr>
<td>Scenario 3: Load Balanced Inline Deployment (also supports out of band)</td>
<td>17</td>
</tr>
<tr>
<td>Scenario 4: Advanced Failover Mechanisms</td>
<td>25</td>
</tr>
<tr>
<td>Scenario 5: Servicing Multiple Network Links</td>
<td>28</td>
</tr>
<tr>
<td>Scenario 6: Service Chaining Multiple Inline Tools (and filtering)</td>
<td>34</td>
</tr>
<tr>
<td>Products Tested in preceding deployment examples</td>
<td>41</td>
</tr>
<tr>
<td>Who to contact for further information on the Imperva Ixia joint solution</td>
<td>41</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

Imperva SecureSphere includes an industry leading Web Application Firewall (WAF) 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) complement Imperva’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 Imperva SecureSphere Web Application Firewall (WAF) 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 SecureSphere. The use cases defined in this document were tested and are ready to be demonstrated with the intent of accelerating sales cycles, provide mechanisms to “land and expand” Imperva SecureSphere sales and avoid technical pitfalls at deployment.

By closely linking Imperva SecureSphere and Ixia NVS products to build a system level solution, Imperva and Ixia’s mutual channel partners will gain the benefit of increasing sales dollars per engagements. This will have a secondary benefit of increased incentives and mindshare for Imperva and Ixia for new customer discovery by the channel.

The paper spells out how to integrate Imperva SecureSphere with Ixia’s NVS to proactively:

- Enhance Inline network resiliency
- Dynamically load balanced workloads across multiple Imperva WAFs
- Maximize Imperva WAF utilization by accessing multiple network links across the data center to Imperva WAFs
- 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 Imperva devices to achieve these goals are provided in the Scenario examples later in this document.

Note: For this guide we tested with Imperva WAF, however similar concepts apply to other inline Imperva models.

Target Audience

This Best Practice Deployment Guide is intended to assist Imperva and partner technical resources who help their customers with planning, deploying, and managing Imperva 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 Imperva Admin and User guides for complete technical details on the referenced products.
HOW TO MITIGATE IMPERVA DEPLOYMENT CHALLENGES

The following list of typical problem areas can negatively impact successful Imperva WAF 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 Imperva deployments. (Details of how to configure such solutions are provided later in this document)

Table 1: Solutions to typical Imperva deployment challenges

<table>
<thead>
<tr>
<th>Problem Areas</th>
<th>Problem Details</th>
<th>How Ixia helps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flexibility</td>
<td>Switching from passive monitoring to active inline protection (and back)</td>
<td>During POCs and initial Security product deployments, IT organizations may run Imperva as a passive monitoring tool and later rewire the network to support inline protection. This causes delays while the necessary maintenance windows are obtained. Ixia bypass switches provide a mechanism to create a common physical connection topology that supports both passive tap monitoring or active inline protection (configurable in software).</td>
</tr>
<tr>
<td></td>
<td>Need to coexist with other security or monitoring tools</td>
<td>Ixia NPBs allow for sharing of traffic amongst many tools to ensure the right traffic is forwarded to the right tools and in the right sequence. From existing network interfaces, tools can be added or removed while the NPB delivers workloads from tool to tool.</td>
</tr>
<tr>
<td>Resilience</td>
<td>Tools fail or require maintenance</td>
<td>Over time tools require maintenance or fail. When this happens Inline protection tools may shut down the services that they are intended to protect. Ixia bypass switches and NPB use heartbeats to check the health and functionality of the tool and keep the network fully operation until remediation is accomplished on the tool.</td>
</tr>
<tr>
<td>Scalability</td>
<td>Too much traffic</td>
<td>Ixia NPBs prevent oversubscribing WAFs by load balancing and filtering traffic. Additional Imperva WAFs can be added to the NPB seamlessly without any downtime to protected services</td>
</tr>
<tr>
<td></td>
<td>Mix of network link speeds (1G, 10G, 40G)</td>
<td>Ixia NPBs can aggregate various link speeds and forward to WAFs across 1G, 10G, or 40G interfaces with the option of load balancing, filtering, and de-duplication. A variety media types are supported.</td>
</tr>
<tr>
<td></td>
<td>Maximize tool efficiency</td>
<td>Ixia’s iBypass family allow for traffic capture on multiple segments that can be aggregated with Ixia NPBs before forwarding to a WAF or WAF pool for full visibility. The NPB ensures consistency of traffic by link.</td>
</tr>
<tr>
<td>High Availability</td>
<td>Fully redundant state-sharing</td>
<td>Ixia NVS solutions can be implemented as fully redundant high availability designs to support Active/Active or Active/Standby tools with heartbeat monitoring to ensure availability.</td>
</tr>
<tr>
<td>Coexistence</td>
<td>Don’t want to lose investment of existing tools</td>
<td>Ixia NPBs allow existing and new tools to coexist. For instance, traffic sent to Imperva WAF for intrusion prevention, while also being sent to preexisting tools (e.g. IPS, APM).</td>
</tr>
</tbody>
</table>
Key Ixia technologies

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

In the figure below, the different modes of operation are illustrated:

- **Inline Mode**
  - Active Inline monitoring
  - iBypass acts like a wire
  - Full-duplex traffic on both WAF Ports
  - Heartbeat packets transmitted
  - WAF in Inline Mode

- **Bypass Mode**
  - WAF is bypassed
  - Heartbeat packets monitored to return to inline mode

- **TAP Mode**
  - Passive out-of-band monitoring
  - iBypass acts like a network Tap
  - Full-duplex traffic on two separate ports
  - No heartbeat packet
  - WAF in receive only mode

Figure 1 - Ixia iBypass Modes of Operation

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 Imperva WAFs 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 Imperva WAF 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.

Figure 2 Ixia Vision ONE Network Packet Broker
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*

**Imperva**

**Imperva SecureSphere MX (management console for WAF units)**

Initial management configuration via CLI (see Imperva Admin Guide for details)

Username: *root*     password: *webco123*

Then access Imperva MX GUI via https://<ip-address>:8083

   username: *admin*     password: set during initial configuration
Scenario 1: Out of Band Monitoring / Sniffing Mode

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

![Figure 3 - bypass switch set to TAP Mode](image-url)
How to Configure

- **Imperva**

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

Configure WAF Gateway to be in *Sniffing* mode

(eth2 will receive traffic in the external network to client network direction, while eth3 will receive traffic in the internal to external direction. Web servers being monitored are on the internal network)

Login to Imperva WAF Gateway via CLI using root user (in this example we configure WAF3)

Note: if using remote SSH instead of the console, you must first enable remote root login via console using the following command;

- [root@WAF3 ~]# impctl hardening config --root-source-ip-exception=<ip-address>

Open an SSH connection to the WAF Gateway, login as root, then issue the following CLI command to enter configuration mode

- [root@WAF3 ~]# impcfg
  
  o type 2 and hit Enter to Manage the SecureSphere Gateway
  
  ▪ type 4 and hit Enter to Change Operating Mode
  
  ▪ type 1 and hit Enter to choose Sniffing mode
  
  ▪ your screen will now look similar to the following

```
1) Perform actions (start, stop, etc.).
2) Change gateway name.
3) Change Management Server address/password.
4) Change operation mode.
5) Manage hardware security modules (HSM).
6) Manage remote agents.
7) Manage interfaces and routes.
8) Change virtual gateway model.
9) Change Cluster configuration.
```

- type t and hit Enter to return to the Top Level menu

- type A and hit Enter to Apply Changes

- type C and hit Enter when prompted to finish applying the change
Once the Top Level menu returns, type 2 and hit Enter to Manage Gateway

- type 7 and Hit Enter to Manage Interfaces
- type 1 and Hit Enter to Set Sniffing Interfaces
- type eth2 eth3 and hit Enter

- type A and hit Enter, then type C and hit Enter to Apply Change

Next, Login to the Imperva SecureSphere MX GUI as user **admin**

- You must configure the **Protected IPs** for the web **Servers** that you wish to monitor (otherwise you will not see detailed monitoring metrics show up). Do this from the **Setup -> Screen**

- In **Definitions** specify the Gateway Group to which your sniffing GW is assigned

**Note:** Please see Imperva WAF User Guide for further details
• **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 Imperva WAF can help customers actively block web vulnerabilities, 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** | • Imperva WAF can be configured to actively block malicious web intrusions.  
• Traffic continuity is preserved in case of Imperva WAF failure or traffic overload  
• WAF can be taken out of service for upgrade or repair without taking down the network  
• Chose in configuration whether to all allow or block network traffic if the WAF 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 of Inline Bypass with Heartbeat](image)

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

- Imperva

Configure WAF Gateway to be in *Bridge* mode, for inline monitoring.

Note: depending on Imperva deployment, interface names/numbers may vary, as tested here eth2 connects to the external network, and eth3 to the internal network. Protected web servers are on the internal network.

Login to Imperva WAF Gateway via CLI using root user (in this example we use WAF3)

  Note: if using remote SSH instead of the console, you must first enable remote root login via console using the following command;

  - [root@WAF3 ~]# impctl hardening config --root-source-ip-exception=<ip-address>

Open an SSH connection to the WAF Gateway, login as root, then issue the following CLI command to enter configuration mode

- [root@WAF3 ~]# impcfg

  - type 2 and hit Enter to Manage the SecureSphere Gateway
  - type 4 and hit Enter to Change Operating Mode
  - type 3 and hit Enter to choose Bridge IMPVHA
  - your screen will now look similar to the following

    ![Configuration Screen](image)

    - type t and hit Enter to return to the Top Level menu
    - type A and hit Enter to Apply Changes
    - type C and hit Enter when prompted to finish applying the change
Once Top Level menu returns, type 2 and hit Enter to Manage Gateway
  • type 7 and Hit Enter to Manage Interfaces
    - confirm Used interfaces are eth2 eth3 (this is default)

Next Login to the Imperva SecureSphere MX GUI as user admin

- In the Setup -> Gateways screen confirm the WAF is assigned to your desired Gateway Group

- You must configure the Protected IPs for the web servers that you wish to protect (otherwise you will not see detailed monitoring, and blocking of vulnerabilities will not occur). Do this from the Setup -> Sites Screen, in the Servers sub-menu add your web servers, click Add to Protected IPs and Save.

- In the Definitions sub-menu specify Operation Mode Active if you wish to actively block web vulnerabilities (Simulation is you just want to get alerts about them)
• **Ixia** Login to Ixia iBypass switch GUI, then go to the *Configuration* tab

  • In the *System* section do the following
    
    o Set the *Bypass Mode* to *Fail-Open*. Set *Bypass Detect* to *Off*. Then click *Apply*
    
    o 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 connected network devices that the link is unavailable)
    
    o Note: You can optionally set *Bypass Mode to Fail-Closed* so that if the WAF 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 Imperva WAF) into the Heartbeat Packet field for both ports.

```
00 50 c2 3c 60 00 00 50 c2 3c 60 01 81 37 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 3c 60 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 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.

  o Once your Heartbeat Packets are edited, click *Apply*

• Go to the *Status* tab
• If Heartbeats are traversing the WAF tool successfully, then the Bypass status will show Off

• Imperva
  • Returning to your Imperva MX GUI you can check that the GW is seeing inline traffic, go to the Monitor -> Dashboard screen, you should notice CPU Load and Throughput if traffic is present

• To check for presence of traffic related to the Protected IP servers which you configured earlier, change the pull down to check for the presence of Connections / Sec

• At this point you can go to Monitor -> Violations to view details of web intrusion attempts (depending on configured WAF Policies, these can be automatically blocked)

Note: this is a sample result from our test environment, specific monitoring data shown in your environment will depend on actual network traffic, and proper configuration of the WAF. Please see Imperva WAF User Guide for further details.
**Scenario 3: Load Balanced Inline Deployment (also supports out of band)**

<table>
<thead>
<tr>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual Imperva WAF appliances may not have sufficient capacity to fully protect busy network links, especially in the case of high speed connections and bandwidth intensive applications.</td>
<td></td>
</tr>
</tbody>
</table>

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

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

![Figure 5 Load balance across Tools](image)

Note: WAF #1 was available but not used in this test

Note: up to 18 additional load balanced Imperva units are possible, but are not shown here.

Note: test examples in the section show virtual Imperva appliances, but setup is the same for physical.

Note: ports number on Vision ONE are based on our test lab, they can differ in other environments.
How to Configure

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

• Imperva

Note: WAF-2 and WAF-3 are used in this example (WAF-1 is not used)

Login to Imperva MX GUI

• From Setup -> Gateways screen confirm that at least two Gateways are present & running. Both should be configured for inline as IMPVHA Bridge mode

![Imperva MX GUI Gateway screen](image)

• If multiple Gateways are not present, consult the Imperva SecureSphere Administration Guide for instructions on how to complete initial configuration of a new Gateway, and to register that Gateway with the Imperva MX.

• 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 WAF units (port pairs P13/P14 & P15/P16 in this example)

• Login to the Vision ONE GUI and click the Inline Diagram tab

![Ixia Vision ONE Inline Diagram](image)

• Create the Bypass Port Connections by double clicking Add Bypass Port Pair

  o In the General tab provide a name for the bypass link and click OK
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 WAF appliances by clicking *Add Inline Tool Resource*

  ![Add Inline Tool Resource](image)

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

  ![General Tab](image)

  **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. For the Imperva WAF heartbeat, the default interval is 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 the Port 2 side of the network (aka 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 WAF appliances (WAF-3) that will 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 double click Add Service Chain to make a connection between your WAF 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.

![Image of General Tab](image)

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

![Image of Bypass Port Pairs Tab](image)

- 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 WAF tools, in which case you can use Ixia’s filters to do so (see example Scenario #6).

- In the Inline Tool Resource tab, click Add to assign the WAF Inline Tool Resource you created previously, then click OK.

![Image of Inline Tool Resource Tab](image)

The default failure action is Fail Closed, this is invoked if all members of the WAF 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 WAF 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 WAF 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 WAF protection IS thus available.

Below is what the completed WAF Inline Load Balanced tool group will look like in the Inline Diagram. (you can ignore the IPS Inline Tool Resource for now, that will be used in a later Scenario) If the Tool Resource shows Green then all tools 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 P13/P14 & P15/P16 are both seeing traffic).

- Imperva

You can further validate load balancing within the Imperva MX GUI. Go the Monitor -> Dashboard. Choose the Connections / Sec pulldown. Notice from the graph that both WAF-2 and WAF-3 are actively monitoring connections and protecting the web servers.
Scenario 4: Advanced Failover Mechanisms

Description
In event that an Imperva WAF unit fails or requires maintenance, ensure that remaining units automatically take over inspection of the unit’s 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)

Benefits
- 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 Imperva can be integrated in any existing customer environment
- Also supports out-of-band deployments

Figure 6 – Active Standby Failover
- In this example Imperva WAFs are connected to port pairs 13&14, 15&16. The WAF on port pair on 15 and 16 is declared as a spare in this configuration. This means it will only receive traffic when the other WAF becomes unavailable (loss of link, or failure of Heartbeats to traverse the WAF).
- Optional (not shown here) multiple Active WAFs 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

- **Imperva**
  - No changes are required to Imperva WAFs configuration that was specified in regular load balancing Scenario 3. WAF-2 and WAF-3 are used in this example (WAF-1 is not used)

- **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 WAF units (port pairs P13/P14 as Active, and P15/P16 as Standby). Starting point is configuration from Scenario #3.
    - Login to the Vision ONE GUI and click the Inline Diagram tab.
    - Double click the Imperva Inline Tool Resource & click the Inline Tool Ports tab
    - Change the 2nd WAF-3 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 P15/P16 pair (the WAF unit you just put into Standby).

And if you return to look at your Inline Tool Resource screen, you also note WAF-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 WAF-2. Note that its Tool Status changes to Offline, while the Tool Status of WAF-3 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 WAF-3 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 WAF-2. (below shows what the Inline Tool Resource would look like after making the change).

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 5: Servicing Multiple Network Links

<table>
<thead>
<tr>
<th>Description</th>
<th>Customer wants to distribute traffic from multiple network links across a common Imperva WAF appliance (or load balanced group of WAF appliances)</th>
</tr>
</thead>
</table>
| 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 WAF (or pool of WAFs) for multiple network links  
• Maximize Imperva WAF capacity when combined with Ixia Vision ONE load balancing  
• Resiliency via Active/Active and Active/Standy failover options.  
• High Availability topology options |

**Figure 7 Send Traffic from Multiple Links to WAF 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. Also, due to limitation of our lab environment, we tested this scenario separately from the others using an Imperva X4500 connected to ports P9 and P10 – in real world the scenarios may be combined.

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

- Imperva
  - Configuration of the Imperva X4500 WAF is similar to WAF configuration in Scenario 2 (except that only a combined management server + gateway appicance, i.e. onebox, is used in this e.g.)

- 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

NOTE: Vision ONE config examples here are abbreviated, but similar in workflow to Scenario #3

- In our example, create a Service Chain named Multi-Link Imperva (or you may use another existing Service Chain if available in your environment.
  - Login to Vision ONE and click Inline Diagram tab, then Add Service Chain. Give it a Name and ensure Traffic Direction is A <-> B (i.e. bi-directional), click OK to save.
• **click Add Inline Tool Resource** to create an ITL for the X4500 WAF, select Hearbeat Imperva WAF, then Add P9 (Side 1) and P10 (Side 2) to the Inline Tool Ports

• Add your Imperva X4500 WAF appliance as an Inline Tool Resource of Multi-Link Service Chain

• Add your 1st Bypass Tool Pair from Scenario 3 to the Service Chain

• Add the 2nd Bypass Tool Pairs to your Service Chain
  (first you will need to create the 2nd Bypass Tool Port Pair)
    o 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 Multi-Link Imperva Service Chain that was setup earlier in this Scenario.
- 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 each 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 the 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 the Imperva X4500 WAF Port Pair (P9/P10)
As a further check, you can login to your Imperva X4500 Management GUI, go to the Monitor -> Dashboard page, and note that traffic is present and connections are being inspected. Because two network links are being inspected by Imperva, you might notice a greater number of Connections/Sec than during previous examples.

**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>
</tr>
</thead>
<tbody>
<tr>
<td>Customer wants to deploy Imperva WAF alongside additional monitoring tools, both inline and out of band</td>
</tr>
</tbody>
</table>

#### Solution Features

- Send same network traffic inline through Imperva WAF, and through other specialized inline tools which a customer might have e.g. Intrusion Prevention System (IPS).
- Ixia Vision ONE filters traffic so that only types relevant to particular tools gets sent to it.
- Optionally, send a copy of the network traffic to out of band tools for purposes other than Security (e.g. Application Performance Monitoring).
- Compatibility with load balancing, multilink, and scenarios discussed earlier in this document.

#### Benefits

- Allows deployment of Imperva WAF alongside existing customer tools.
- Improves capacity by filtering and forwarding only relevant protocols to the particular tools that need to see them.
- Proven bypass switch technology addresses customer objections of single point of failure.
- Add additional monitoring tools as traffic loads and customer protection needs grow.

#### Figure 8 Service Chaining Multiple Monitoring Tools

- Example configuration is as per Scenario #3, but first traffic is sent through an inline IPS connected to P11/P12, before being sent through a single Imperva WAF unit connected to P13/P14, before being sent back to the Bypass Port Pair. Traffic is filtered for HTTP/HTTPS only.
- In addition an unfiltered copy of packets is sent from P17 to and out-of-band APM on P27.

#### How to Configure

(in this config example, a physical deployment as shown in Figure 8 is assumed to be wired up)
- Imperva
  - No changes to WAF Configuration required, same as in Scenario 2 (WAF-3 is used in this example)

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

  Configure Vision ONE. In this example scenario we will configure an inline IPS so that the IPS can identify general traffic threats, and from there pass the traffic to a single inline Imperva WAF to block more specific web vulnerabilities. In this example since the WAF and IPS 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 to reduce the load on the inline tools.

  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 WAF Inline Tool Resource, click the X beside WAF-2 and click OK. *(this leaves a single WAF 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 from the 2nd Web Protection Service Chain. We’ll also apply our HTTP/HTTPS filter to the 1st Web Protection Service Chain.

  - Right click the connection between Bypass Switch #2 and the Web Protection Link #2 Service Chain, the select Delete
- Double Click the 1st Web Protection 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.

  o Repeate the previous step to add another Criteria of HTTPS to the Web Protection Service Chain. You must first select the Match Any (OR) button.

  o You'll probably need to allow DNS as well, so that the web queries can be resolved by name.

  o 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 iBypass #1 Heartbeat packets (as per the MAC address used in Scenario #2).
Finally, review your three configured Criteria fields, then click OK.

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

- If not already present, you will need to add the IPS Inline Tool. Double Click the Add Inline Tool Resource area, in the General tab give the Inline Tool a Name, and choose a suitable Heartbeat (in our test example, CiscoFirePOWER) 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 P11 and P12 respectively). Provide an *Inline Tool Name*, and click *Create Port Pair*.

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

- Next, Double click the *Web Protection 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 IPS 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.
- Also use the Arrows to put IPS first in the list. Since Imperva WAF provides the most specific Web vulnerability blocking, it should go closest to the protected web servers on the internal network.
- Click OK to save the change

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

Note: that Side A uses Port Group 1 (PG1), you’ll need this 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 statics 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/DNS 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)*

**Imperva**

*(note, other models of Imperva WAF can also be used)*

- Imperva MX Management Server  
  VM150 Virtual Appliance  – Version 11.5.0
- Imperva WAF Gateway  
  V4500 Virtual Appliance  – Version 11.5.0
- Imperva X4500 MX+WAF  
  X4500 Apppliance in OneBox mode  - Version 11.5.0

---

# WHO TO CONTACT FOR FURTHER INFORMATION ON THE IMPERVA IXIA JOINT SOLUTION

imperva@ixiacom.com