NGIPS Recommended Practices F5 BIG-IP and Cisco/Sourcefire NGIPS load balancing

The F5 Local Traffic Manager (LTM) allows companies to secure their enterprises and provides the scale necessary to prevent variable attack presentations while offering uncompromising...

White Paper

by Matt Quill

Concept

The F5 Local Traffic Manager (LTM) allows companies to secure their enterprises and provides the scale necessary to prevent variable attack presentations while offering uncompromising visibility to data traffic traversing diverse security zones. Integration with an industry-leading IPS or an Intrusion Prevention System product like the one from Sourcefire, combined with a strong DDoS strategy, is a necessary component of perimeter security.

Protecting the enterprise from malware, bots, and other attacks can provide a comprehensive protection posture. To achieve this seamless integration, F5 partnered with Sourcefire to validate and produce reference architectures for integration with the BIG-IP LTM product and the Sourcefire NGIPS product. The testing and validation of this design were conducted at the F5 lab facilities utilizing both virtual and physical Sourcefire-managed devices.

Note: BIG-IP is deployed in redundant pairs. For simplicity a single BIG-IP is depicted in the network topology diagrams to reduce the overall BIG-IP node count. The topology can be reduced to a single redundant pair of BIG-IPs. Strict route domains are required. These topological decisions are site- specific and beyond the scope of this document.

This guide is designed to help administrators identify and deploy validated configurations for common- use cases. The customer scenarios defined here address IPS policy– based traffic steering and blocking, and SSL visibility and control.

User Scenarios

IPS Policy–Based Traffic Steering and Blocking

IPS Policy–Based Traffic Steering and Blocking leverages the BIG-IP LTM to allocate traffic flows to different resources based on load. Or based on business intelligence utilizing features such as Centralized Policy Management or iRules for deeper decision-making process for which NGIPS resources to leverage for inspection. For example, Application A can be directed to one pool of NGIPS servers with a ruleset specialized to monitor signatures specific to its environment, while Application B is directed to another pool. Integration with the Sourcefire remediation API allows the system to dynamically react to reduce the demand on NGIPS infrastructure by leveraging a BIG-IP iRule to populate an IP address into a blacklist. Traffic from the identified offender is blocked before entering the NGIPS for a preset period of time. One strategy of attackers is to provide an overwhelming amount of distracting traffic in order to mask the real attack. This remediation tactic can allow the NGIPS to focus resources on identifying new attacks without having to remediate already identified bad actors.

SSL Visibility and Control

SSL termination is resource-intensive. F5 BIG-IP devices include dedicated hardware processors specializing in SSL processing. In both inbound and outbound deployment scenarios, utilizing F5 NGIPS solution will provide uncompromising visibility into SSL traffic.

Inbound applications are rarely being deployed without high availability in mind, and SSL termination on BIG-IP ensures secure and enhanced application delivery while providing visibility into SSL traffic to NGIPS sensors. Where security policy dictates, traffic can be re-encrypted to the back-end servers.

With the proliferation of websites now leveraging SSL encryption to protect users, this poses a challenge to NGIPS sensor pools in their mission to eliminate malware and attacks for outbound. With BIG-IP, SSL intercept can be leveraged to provide full visibility into user traffic.

Common Validated Deployment Deployment Architectures

Air Gap Architecture: Ingress Traffic Protection

The air gap architecture that we validated was a load-balanced pool of Sourcefire NGIPS managed devices front-ending web and FTP application server pools. This maximizes the effectiveness of the combined Sourcefire and F5 solution, and addresses both the SSL visibility and control and traffic management and blocking. The air gap gets its name from the small gap in infrastructure where the traffic is decrypted long enough to be inspected by the Sourcefire IPS and re-encrypted before traversing untrusted networks. Security and compliance would dictate that one ensures that this gap exists only within a trusted infrastructure to avoid tampering or unauthorized visibility into the data.

In the diagram in Figure 2, the IPS pool resides in the IPS client– side pool and inspects, blocks, and reports on all network flows. After traffic traverses the NGIPS managed device, it is then routed back through the BIG-IP to the IPS Protected virtual instances. This ensures that traffic can be inspected, and, if necessary, IP addresses can be blocked before forwarding on to their respective server pools. In this instance both the forwarding virtual server and the IPS-protected application servers will have the same IP address. However, the forwarding virtual server will allow connections on all ports, where the actual virtual server will allow traffic only on its designated port. (i.e., 443, 80)

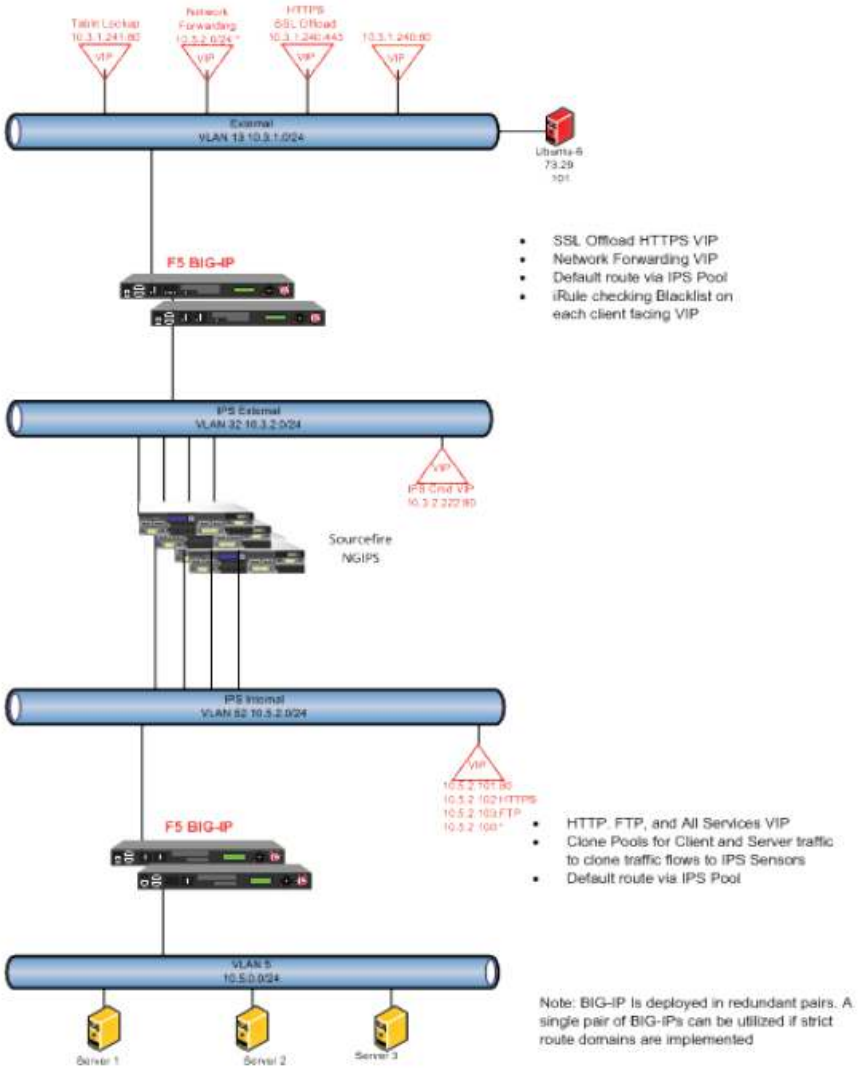

Figure 1: Sourcefire NGIPS and F5 Routed Configuration

Air Gap Architecture: Egress Traffic Protection

We next validated the network architecture to protect internal clients from Internet-based threats. This is the network example for internal clients performing egress traffic access to the Internet. The approach to the network setup is similar to that for ingress network forwarding. The first hop of the egress access is an any IP address and any protocol Layer 3 forwarding virtual servers listening on the internal VLANs. The client access the near-side network forwarder virtual as the client's default gateway. This virtual server load-balances using gateway pool static routes to the NGIPS-managed devices. The NGIPS will forward the traffic to the Internet side listening L3 forwarding virtual hosted by BIG-IP#1. That virtual server pool can forward traffic based on static, dynamic, or pooled routers. The auto-last hop feature is used to ensure flow affinity across the NGIPS-managed devices. This feature is enabled by default.

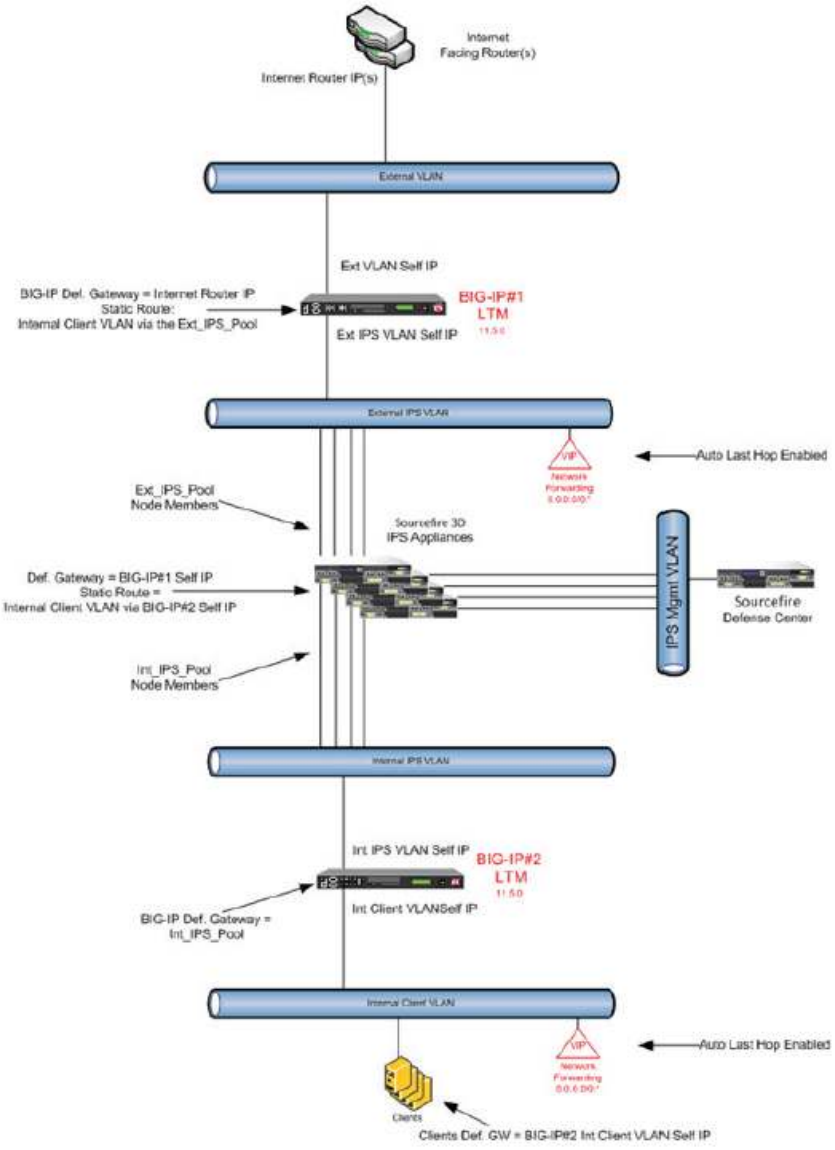

Figure 2: Sourcefire NGIPS and F5 Routed Configuration

Air Gap BIG-IP Configuration Steps

In this guide we will outline the necessary steps to deploy the Sourcefire NGIPS in a layer-3 environment. Although a non-routed inline layer-2 setup is also functional, accommodating the scale and performance characteristics of an application requires a layer-3 setup.

A familiarity with BIG-IP deployment concepts and technology as well as basic networking is essential for configuring and deploying the LTM components of the BIG-IP product portfolio. For further details on the configuration and networking setup of the BIG-IP, please visit the F5 support site at https:// support.f5.com.

The recommended approach for this solution is to build out a routed configuration. To avoid complexity with direct server return or asymmetrical routing, the following configuration will be based on a two cluster BIG-IP approach. The NGIPS managed device pool is deployed between the two BIG-IP clusters. The client-facing BIG-IP is where the IPS configuration is defined. The IPS pool and members are defined first; then the virtual servers are created; and finally the iRule is applied to the virtual servers.

Create Nodes

In order to ensure that traffic flows are seen by the NGIPS managed devices, we will add the IPS node IP addresses to the platform. In this arrangement we will configure nodes to handle both FTP traffic as well as HTTP traffic through the NGIPS-managed devices. Nodes need to be defined on both BIG-IP devices.

On the External BIG-IP (BIG-IP#1), create the nodes. Within the GUI, select Local Traffic→ Nodes→Node list and then choose create. Create a node entry for each of the follow nodes.

Node Name	Node Address
IPS-1	Sourcefire NGIPS node IP address on the External IPS VLAN
IPS-2	Sourcefire NGIPS node IP address on the External IPS VLAN
IPS-3	Sourcefire NGIPS node IP address on the External IPS VLAN
IPS-4	Sourcefire NGIPS node IP address on the External IPS VLAN. Repeat for each NGIPS node
WEB	Web server member is the HTTP virtual server IP address on the internal BIG-IP (BIG-IP#2).
FTP	The FTP member is the FTP Virtual server IP address on the internal BIG-IP (BIG-IP#2).

On the Internal BIG-IP (BIG-IP#2), create the nodes. Within the GUI select Local Traffic→ Nodes→Node list, and then choose create. Create a node entry for each of the follow nodes.

Node Name	Node Address
Int_IPS-1	Sourcefire NGIPS node IP address on the Internal IPS VLAN
Int_IPS-2	Sourcefire NGIPS node IP address on the Internal IPS VLAN
Int_IPS-3	Sourcefire NGIPS node IP address on the Internal IPS VLAN
Int_IPS-4	Sourcefire NGIPS node IP address on the Internal IPS VLAN. Repeat for each NGIPS node
Int_Web Server	The IP address of the Web Server on the Internal Client VLAN. Repeat for each web server.
Int_FTP Server	The IP Address of the FTP server on the Internal Client VLAN

Create Pools

The previously created nodes need to be assigned in LTM Pools.

On the External BIG-IP (BIG-IP#1), create the pools. Within the GUI, select Local Trafficg→ Pools→Pool List, and then choose create.

Pool Name	Function and Members
IPS-Pool	IPS pool load balancing to the internal BIG-IP. Node Members are IPS-1 through IPS-4. Add as many members as there are NGIPS devices.
WEB Pool	Web Server Pool containing the WEB node name
FTP_Pool	FTP Traffic Pool containing the FTP node name

On the Internal BIG-IP (BIG-IP#2) create the following pools:

Pool Name	Function and Members
Int IPS-Pool	IPS Internal VLAN pool members (Int_IPS-1 through 4)
Web Pool	The Web Server nodes
FTP_Pool	The FTP server node

Virtual Server Configuration

On the External BIG-IP (BIG-IP#1), the following virtual servers will be created:

VS	Name Function	
IPS-Protected HTTPS	HTTPS virtual server with SSL offload	Standard Virtual, Host IP, and SSL Client Profile
IPS-Protected WEB	HTTP Virtual Server	Standard Virtual and Host IP
IPS-Protected Network	Forwarding IP Virtual Server to the Internal IPS VLAN	Forwarding IP Virtual Server, IP Network address and Mask.
IPS-Protected FTP	FTP Virtual Server	Standard Virtual, Host IP, FTP Profile

On the Internal BIG-IP (BIG-IP#2), the following virtual servers will be created:

VS Name	Function	
HTTPS-Services	HTTPS virtual server with SSL offload	Standard Virtual, Host IP, and SSL Client Profile
Web-Services	HTTP Virtual Server	Standard Virtual and Host IP
FTP-Services	FTP Virtual Server	Standard Virtual, Host IP, FTP Profile

Configure iRules and Associate the Virtual Server

In the layer-3 setup and configuration, we will create two iRules. These iRules will be associated to the virtual servers. The first iRule is used to receive blacklist data from the Sourcefire Remediation API. The Second iRule is used to refer to the internal blacklist table when a connection request is made. If the client IP is on the blacklist table, the request is dropped. For details and tutorials on iRules, please consult the F5 DevCentral site at https://devcentral.f5.com.

The following iRule listens for HTTP requests from the Sourcefire-managed device. Sourcefire then responds via its Remediation API and sends an HTTP Request containing an IP Address and a timeout value. The address will be the source IP that is to be blocked by the BIG-IP; the BIG-IP will continue to block for the duration of the timeout period.

Create a new iRule entry on the External BIG-IP (BIG-IP#1). Within the GUI, select **Local Traffic→ iRules→iRule List**, and then choose **create**. Specify a name and copy the following text in the graphics below into the iRule. This iRule will be associated with the Control VIP.

```
                    when HTTP _ REQUEST {
  if { [URI::query [HTTP::uri] "action"] equals "blacklist" } {
            set blockingIP [URI::query [HTTP::uri] "sip"]
          set IPtimeout [URI::query [HTTP::uri] "timeout"]
     table add -subtable "blacklist" $blockingIP 1 $IPtimeout
 HTTP::respond 200 content "$blockingIP added to blacklist for $IP
                             timeout
                             seconds"
                               return
                                }
HTTP::respond 200 content "You need to include an ? action query"
                                }
```

Figure 3: Remediation API Control iRule

On the protected VIP, you will associate the following iRule to ensure that IP addresses are blocked from the application itself.

Create another new iRule entry on the External BIG-IP (BIG-IP#1). Within the GUI, select **Local Traffic→Rules→iRule List**, and then choose **create**. Specify a name and copy the following text in the graphics below into the iRule. This iRule will be associated with the Protected VIPs.

```
                    when CLIENT _ ACCEPTED {
                   set srcip [IP::remote _ addr]
    if { [table lookup -subtable "blacklist" $srcip] != "" } {
                               drop
              log local0. "Source IP on black list "
                              return
                               }
                              }
```

Figure 4: Remediation API Protect iRule

For example, the virtual server IPS_Protected_HTTPS will have the following iRule associated to it. The assignment of this iRule to the VIP can be done when the virtual server is created. Or the virtual server can be modified to add this iRule. To modify the virtual server within the GUI, select **Local Traffic→Virtual Servers→Virtual Server List**. Select the virtual server to modify and then select the **Resources** tab.

Figure 5: Protect iRule Virtual Server Resource Assignment

Configuration of Virtual Servers

This section will detail how to create the HTTPS and Network Forwarding Virtual Servers. These tasks can be repeated for each virtual server on the Internal and the External BIG-IPs.

Network Forwarding Virtual Server

On the External BIG-IP (BIG-IP#1), perform the following configuration steps:

From the LTM section of the management UI, create a new virtual server by selecting Local Trafficg• Virtual ServersgVirtual Server List, and then choose create.

Specify a name for the virtual server; for Type, select Forwarding (IP). For Destination, select Network and specify a network IP address and mask. The Service Port is * All Ports. For Source Address Translation, select None, which will ensure the NGIPS-managed devices receive the true client source IP while inspecting the traffic flows. Enable this virtual server on only the external VLAN.

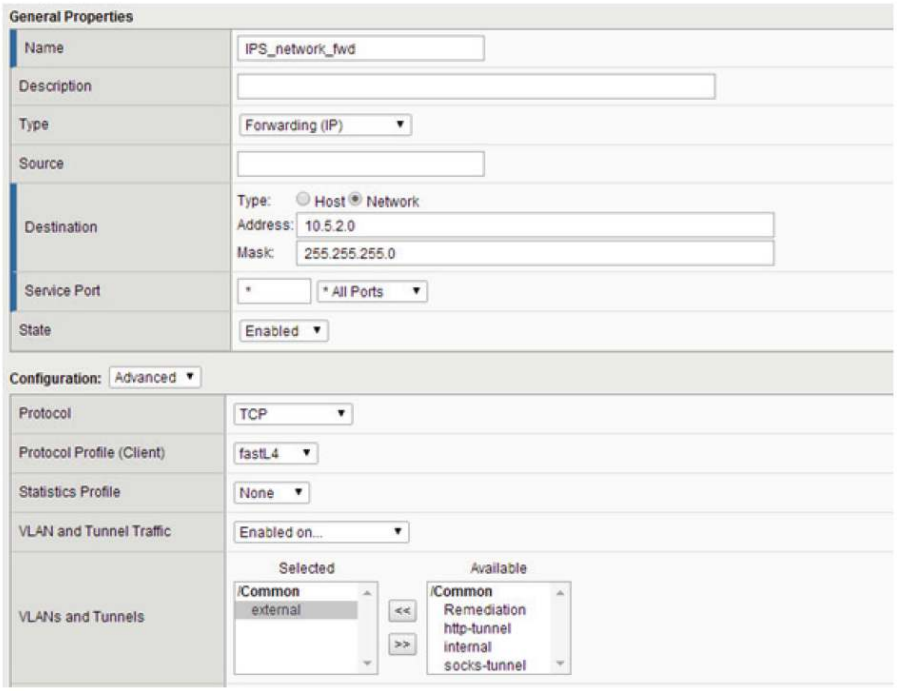

Figure 6: Network Forwarding Virtual Server

Within the resource section of the virtual server configuration, enable the Protection iRule. Move the iRule into the Enabled column.

Figure 7: Network Forwarding Virtual Server iRule Definition

For each of the Internet-facing IPS-protected virtual servers, be sure to include the protection iRule.

Create Application Virtual Servers

In this section the application virtual servers will be created. These server attributes are a bit different from the network-forwarding virtual servers in that the IP addresses are host IP addresses. The External BIG-IP (BIG-IP#1) virtual servers will use pool members that are hosted by the Internal BIG-IP (BIG-IP#2). The Internal BIG-IP (BIG-IP#2) virtual server pool members are the application server IP addresses.

External BIG-IP Application Virtual Servers

Create the application virtual servers. These will be standard HTTPS, Web, and FTP virtual servers.

On the External BIG-IP (BIG-IP#1), the following virtual servers will be created:

Virtual Server Name	IP Address	Pool	iRule
IPS_Protected_HTTPS	10.3.1.240	Web	Protection iRule
IPS_Protected_WEB	10.3.1.241	Web	Protection iRule
IPS_Protected_FTP	10.3.1.242	FTP_Pool	Protection iRule
IPS_Command_VS	172.30.73.39	None Control iRule	

Create the Application based Virtual servers by selecting Local TrafficgVirtual ServersgVirtual Server List, and then choose create.

Specify a name; For type, select Standard; for Destination, select Host and enter an IP address; for Port, enter 443.

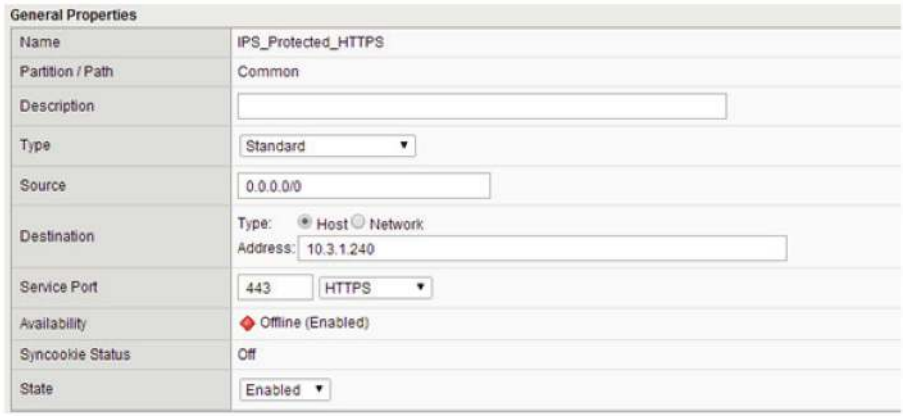

Figure 8: Network Forwarding Virtual Server iRule Definition

Select TCP for the Protocol and tcp for the Protocol Profile.

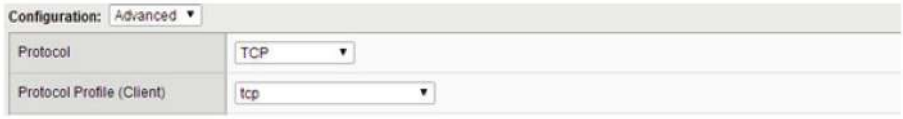

Figure 9: Network Forwarding Virtual Server iRule Definition

This virtual server is the HTTPS with SSL offload. Be sure to specify the SSL Client Profile.

Figure 10: Network Forwarding Virtual Server iRule Definition

Enable the virtual server to listen only on the external VLAN.

Figure 11: Network Forwarding Virtual Server iRule Definition

Select Web for the virtual server Default Pool. This pool is an HTTP-only member pool. BIG-IP will send unencrypted traffic to these pool members. The Pool member is the internal BIG-IP (BIG-IP#2) Web-Services Virtual Server.

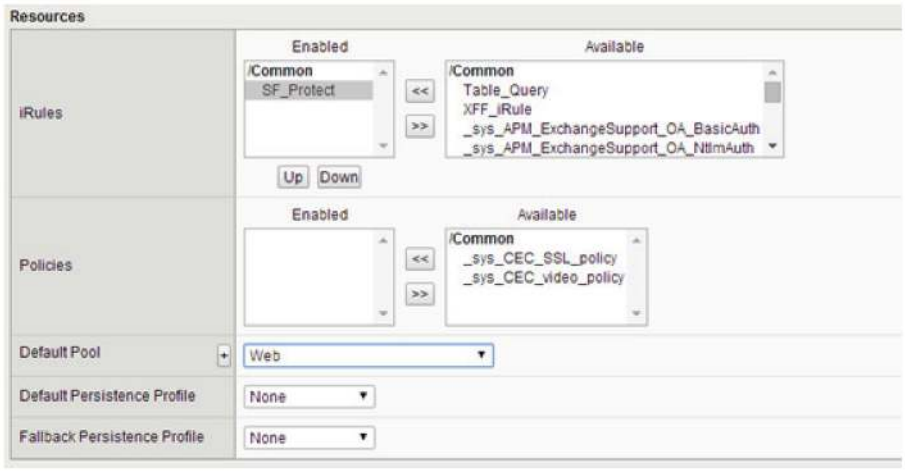

Figure 12: Network Forwarding Virtual Server iRule Definition

Repeat these steps for each of the application virtual servers.

Create Remediation API Control Virtual Servers

In this section the Remediation API control virtual server will be created. This virtual server is an HTTP- profile virtual server, which is listening for Remediation messages from the Sourcefire Defense center. This is an out-of-band connection between the management interface of the Defense Center to the BIG-IP virtual server IP address. This virtual server is required to manage the internal table of blacklisted client IPs.

Create the Remediation Control Virtual Server by selecting Local TrafficgVirtual ServersgVirtual Server List, and then choose create.

Specify a name; for Type, select Standard; for Destination, select Host and enter an IP address; for Port, enter 80.

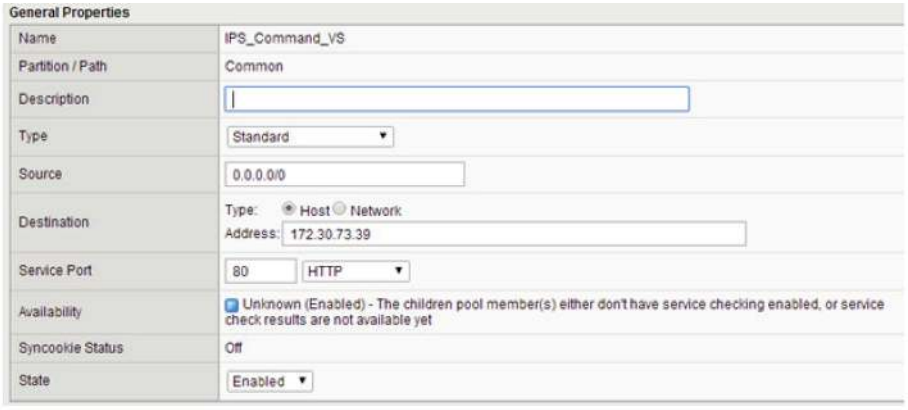

Figure 13: Network Forwarding Virtual Server iRule Definition

Select TCP for the Protocol and tcp for the Protocol Profile.

Figure 14: Network Forwarding Virtual Server iRule Definition

Enable the virtual server to listen only on the Remediation VLAN. This is the VLAN the Sourcefire Defense Center is connected to or reachable from.

Figure 15: Network Forwarding Virtual Server iRule Definition

Make sure the Control iRule is assigned to this virtual server and that there is no default pool.

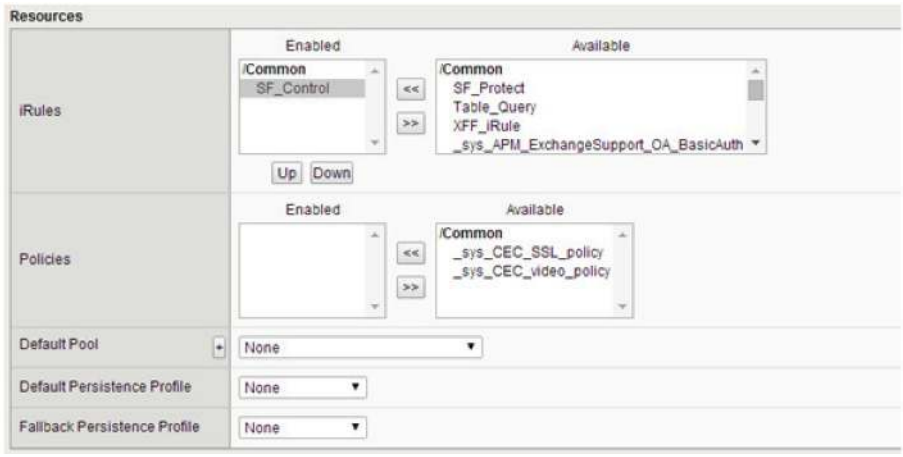

Figure 16: Network Forwarding Virtual Server iRule Definition

The Control iRule is configured and available to receive remediation event data.

Internal BIG-IP Application Virtual Servers

On the Internal BIG-IP (BIG-IP#2) the following Virtual Servers will be created:

Virtual Server Name	IP Address	Pool
WEB-Service-VS	10.5.2.101	Web
FTP_Services-VS	10.5.2.103	FTP_Pool

Create the Internal BIG-IP Application–based virtual servers by selecting Local **Traffic→Virtual Servers→Virtual Server List**, and then choose **create**.

Specify a name; for the Type, select **Standard**; for the Destination, select **Host** and enter an IP address; for Port, enter **80**.

Figure 17: HTTP Virtual Server General Properties

For the Protocol, select TCP, and for the Protocol Profile, select tcp.

Figure 18: HTTP Virtual Server Protocol Profile

Enable the Virtual Server to listen only on the external VLAN.

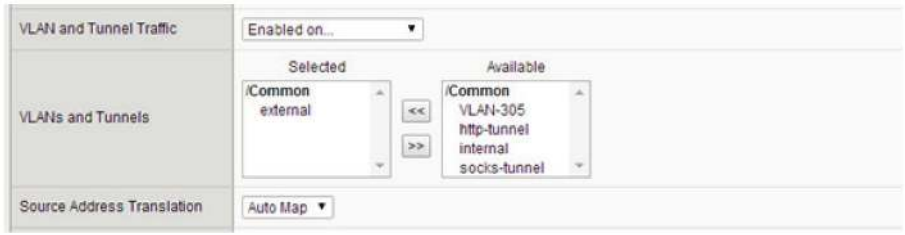

Figure 19: HTTP Virtual Server VLAN Assignment

Be sure to enable the Auto Last Hop feature so BIG-IP can remember which L2 device sent the traffic flow. In turn, when BIG-IP responds to the requests, it will be forwarded through the same L2 device. This ensures TCP flow affinity with respect to the NGIPS devices.

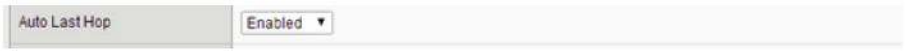

Figure 20: HTTP Virtual Server Auto Last Hop

For the Default Pool, select **Web**.

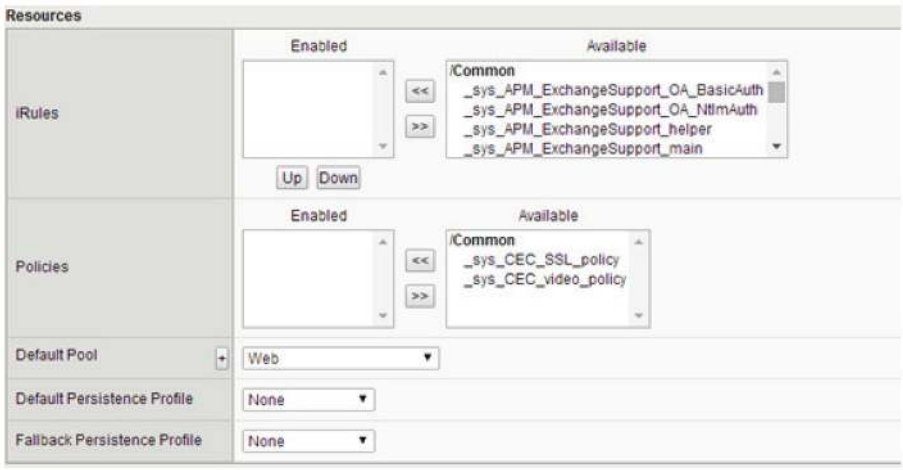

Figure 21: HTTP Virtual Server Default Pool

Repeat these steps to create the FTP virtual server. Make sure to select FTP for the Default Persistence Profile. If additional information is needed to configure the pools, virtual servers, profiles, or other device attributes, please visit https://support.f5.com. Configure network static route on the External BIG-IP (BIG-IP#1), configure a new static route to reach the Internal Client VLAN 10.5.2.0/24 network via the IPS Pool. This will allow the traffic passing through the IPS-managed devices to be load-balanced across the IPS Pool members.

Within the GUI, select **Network→Routes**, and then select **create**. Specify the name, destination IP address (10.5.2.0), and mask (255.255.255.0). For the Resource, select Use Pool, and for the Pool, select IPS-pool.

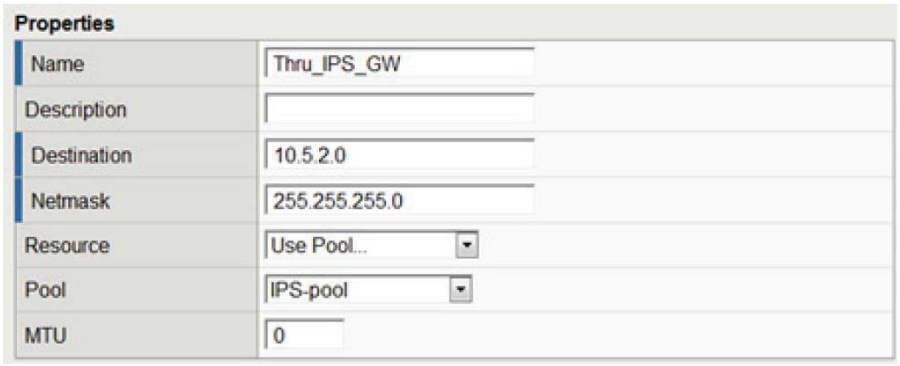

Figure 22: Create Gateway Pool Static Route

Repeat the previous step for any other internal networks that need to be reached via the NGIPS devices.

On the Internal BIG-IP (BIG-IP#2), configure the Default Gateway route to use the Int IPS Pool. Within the GUI, select **Network→Routes** and then enter **external_default_gateway** in the Name field . For the Resource field, select **Use Pool**, and for the Pool field, select **Int_IPS_Pool**.

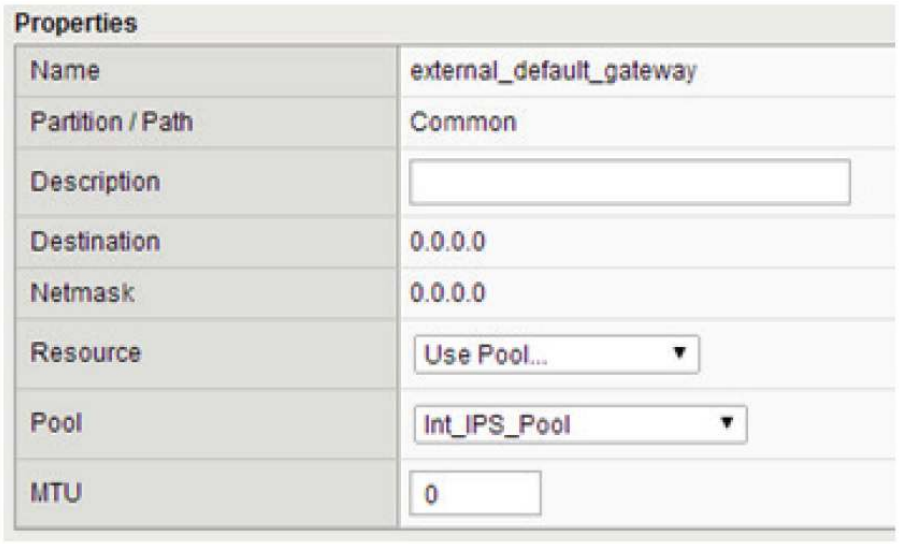

Figure 23: Internal BIG-IP Default Gateway

This modification will load-balance response traffic or externally facing flows across each NGIPS node IP addresses.

BIG-IP Basic Egress Access Configuration

Client egress access to the Internet via Sourcefire NGIPS–managed devices is configured much like an ingress network forwarding virtual. The only difference is which VLAN the virtual servers are configured on. Figure 24 is a network topology diagram with the Internet at the top and the clients at the bottom.

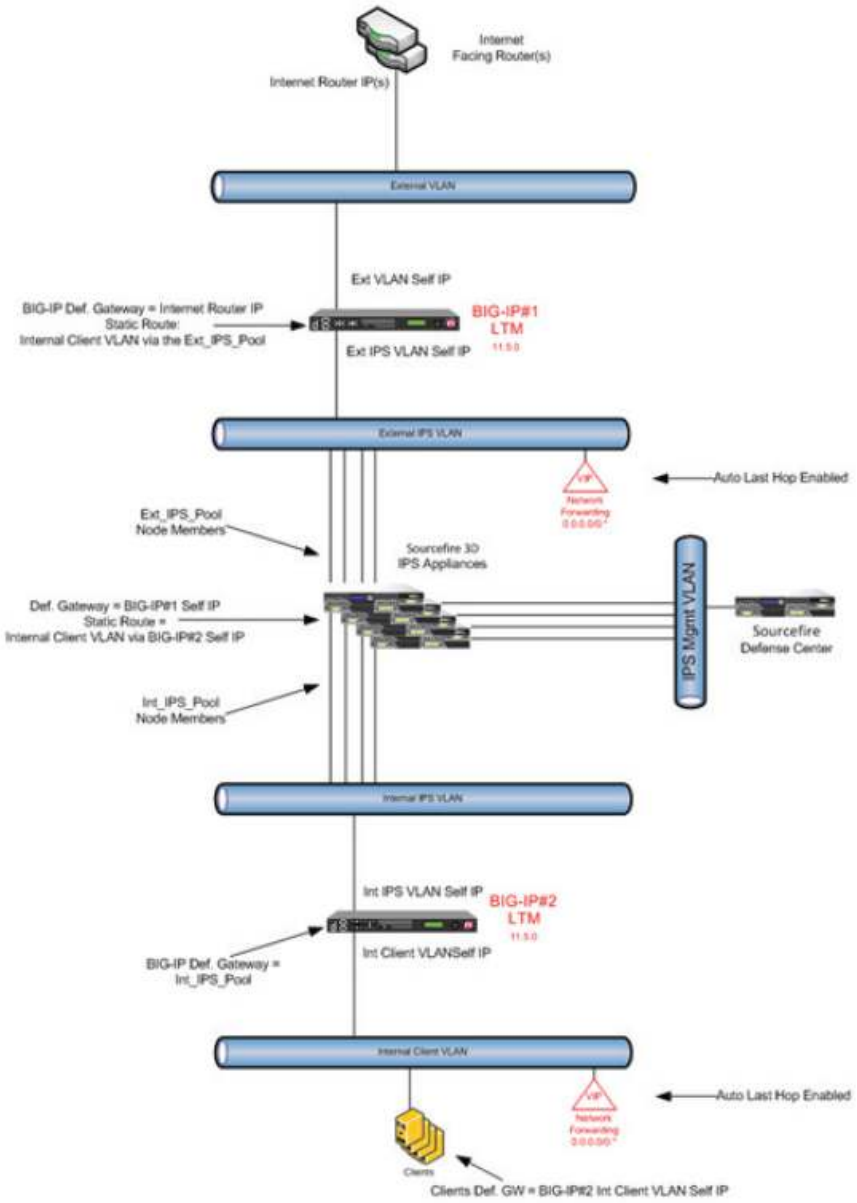

Figure 24: Egress Access Network Topology

When the client's IP address is configured, the BIG-IP self IP address is the gateway node address the client should be using. The any IP address any protocol port network forwarding virtual servers listen on the BIG-IP VLAN self IP address. BIG-IP #2 Network forwarding virtual is listening on the Internal Client VLAN. As traffic traverses this virtual server, it naturally routes through the Sourcefire NGIPS–managed devices using the Gateway Pool feature in BIG-IP.

The Sourcefire NGIPS–managed devices have the default gateway defined to be the BIG-IP #1 External IPS VLAN self IP address. BIG-IP #1 has a Network Forwarding virtual server on that same VLAN.

The BIG-IP feature Auto last hop is enabled by default. If it is not enabled by default, then specify it on a per-virtual server basis. Ensure this is the case for both virtual server definitions.

Egress Inspection with SSL Intercept

In order to inspection egress traffic that is SSL-encrypted, the BIG-IP Forward Proxy with SSL Intercept can be configured. This configuration operates much like the simple egress access use case. The difference is that it adds the SSL decryption utilizing intermediate certificate keys. The certificates also need to be loaded into the client browser as a trusted intermediate CA.

The encrypted session in an SSL/TLS communication is ultimately dependent on the private key of the service, which the reverse proxy would possess. But in a forward proxy, the private key would be controlled by some remote host and inaccessible to the forward proxy service. To get around this problem, BIG-IP LTM provides a capability called "Forward SSL Proxy." For the IPS Inspection use case, this feature is called SSL Intercept. This capability essentially allows the forward proxy to "spoof" the SSL/TLS services provided by the remote host. This section describes how to augment this solution with a physical "air gap" so that outgoing communications can be inspected.

Per the official Forward SSL Proxy guide (https://support.f5.com/kb/en-us/products/big-ip_ltm/ manuals/product/ltm-implementations-11-4-0/14.html), here is how the SSL Intercept feature works:

1. The client establishes a three-way TCP handshake with a wildcard IP address on the LTM and then initiates the SSL session (CLIENTHELLO message).
2. The LTM establishes a three-way TCP handshake with the remote host and initiates a separate SSL session (CLIENTHELLO message).
3. The remote host responds with its certificate (SERVERHELLO and CERTIFICATE messages).
4. The LTM generates a server certificate on the fly to match the properties of the remote host's server certificate and presents that to the client to complete the

client side SSL negotiation. The LTM is equipped with a subordinate certifying authority certificate (and private key), and the internal clients must be configured to trust this local authority.

The Forward SSL Proxy configuration involves a client SSL profile and a server SSL profile in "SSL Forward Proxy Feature" mode. This setting, when applied to the server SSL profile, tells the server SSL profile to allow the initial SSL handshake to pass unencumbered. After the initial client side SSL handshake is complete, the server SSL profile initiates a new (proxied) SSL session with the remote host. Between the client SSL session and the server SSL session is unencrypted data that can be inspected and/or manipulated.

Prerequisites

The section requires that the BIG-IPs is installed and have network connectivity configured. This section leverages the same configuration as previous sections . If Basic Egress Access was configured. Then remove the two IP forwarding virtual servers those will be replaced with Performance L4 Virtual Servers in this section.

Static Routes are already configured for traffic forwarding through the IPS sensors.

Configuring SSL Intercept on the Internal BIG-IP

The configuration steps for SSL intercept begin with the Internal BIG-IP (BIG-IP#2); the second part of the configuration steps will occur on the External BIG-IP (BIG-IP#1). The external BIG-IP is the closest to the Internet-facing router. The Internal BIG-IP services the internal network client's egress access requests.

For forward SSL proxy to work, the internal LTM (BIGIP#2) must possess a subordinate certificate authority (CA) certificate that it will use to issue new server certificates. Import this certificate and key via the management GUI by selecting SystemgFile ManagementgSSL Certificate ListgImport. Import both the certificate and the key. In the example below, they are named Cert-1 and Key-1. The long names for these are /Common/Cert-1.crt and /Common/Key-1.key

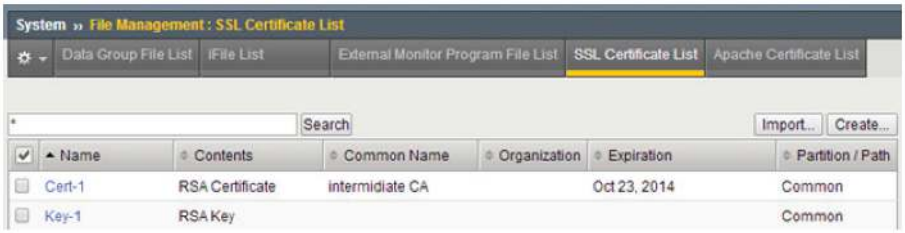

Figure 25: Intermediate CA Certificate

Next create a client SSL profile, enable the SSL Forward Proxy Feature option, and customize the SSL Forward Proxy section as required. Create the profile by selecting in the GUI Local **Traffic→Profiles→SSL→Client**, and then select **create**. In the example below, the client profile is called **basic_clientssl_intercept**. Select the certificate and key that were previously installed, and then add them to the Key Chain. Base the profile on the clientssl profile.

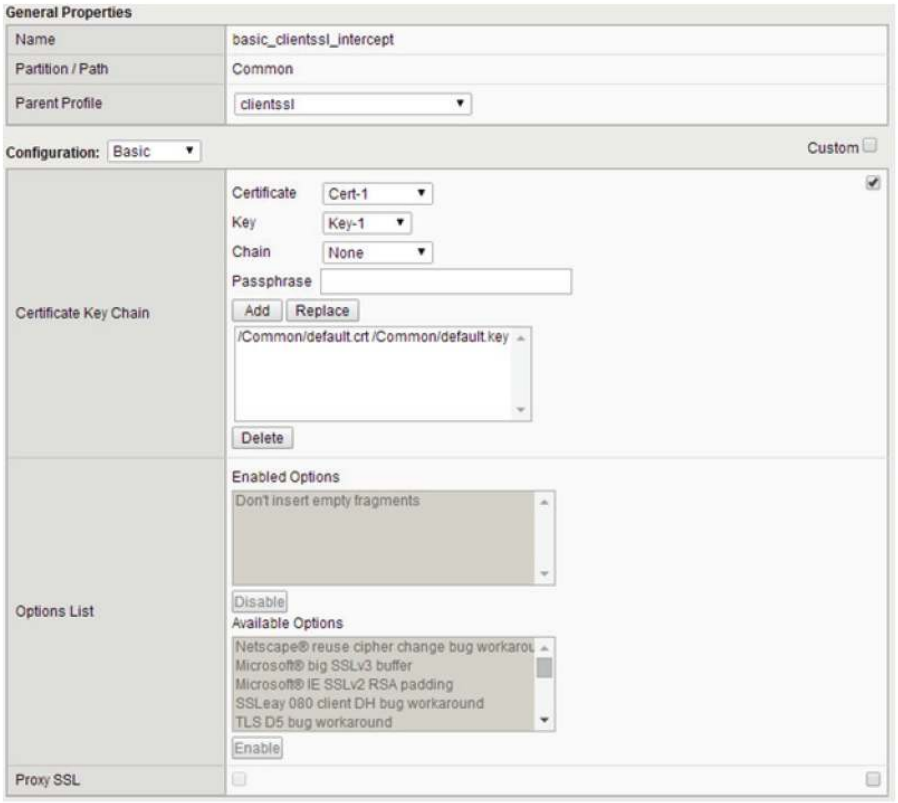

Figure 26: SSL Client Profile Configuration

Scroll down to the SSL Forward Proxy section. Enable SSL Forward Proxy and specify the certificate and key, and then enable SSL Forward Proxy Bypass.

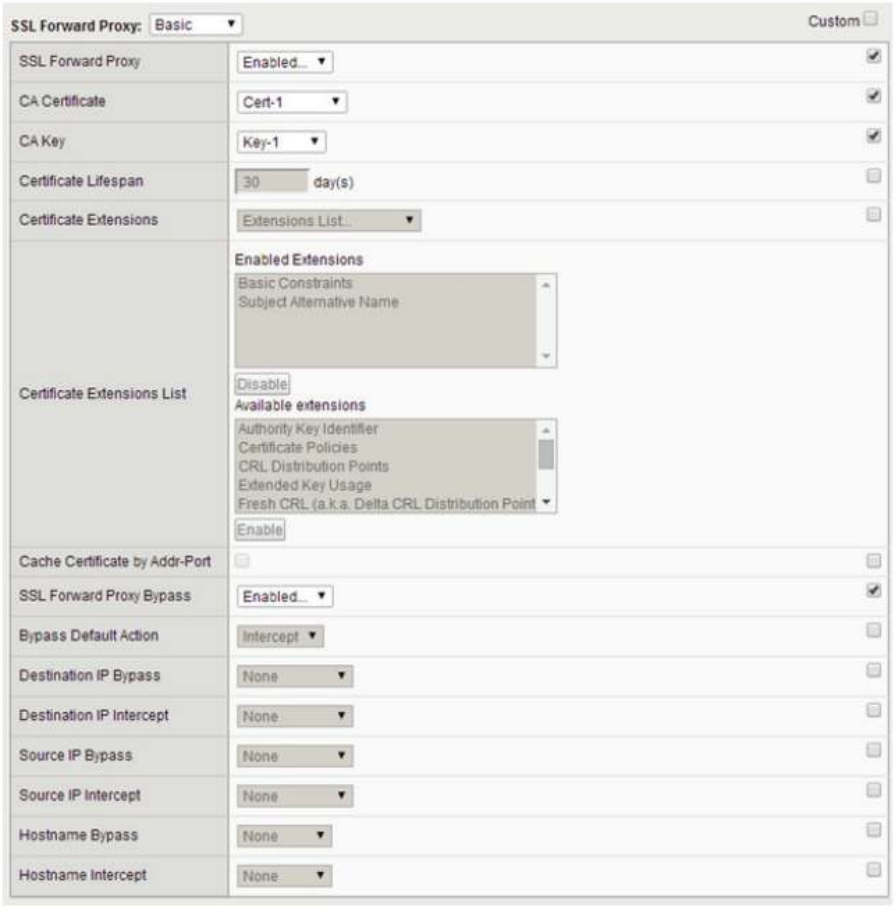

Figure 27: SSL Client Profile Forward Proxy Settings

Create the SSL Server Profile by selecting in the GUI Local **Traffic→ProfilesgSSL→Server**, and then select **create**. In the following example, the profile was named **basic_serverssl_intercept**. Base the profile on the **serverssl** profile. Select the Advanced configuration option. Customize the following values:

For SSL Forward proxy, select Enabled; for SSL Forward Proxy Bypass, select Enabled; define the Ciphers as **!SSLv2:!EXPORT:!DH:RSA+AES:RSA+DES:RSA+3DES:ECDHE+AES:ECDHE+3DES:@SPEED.**

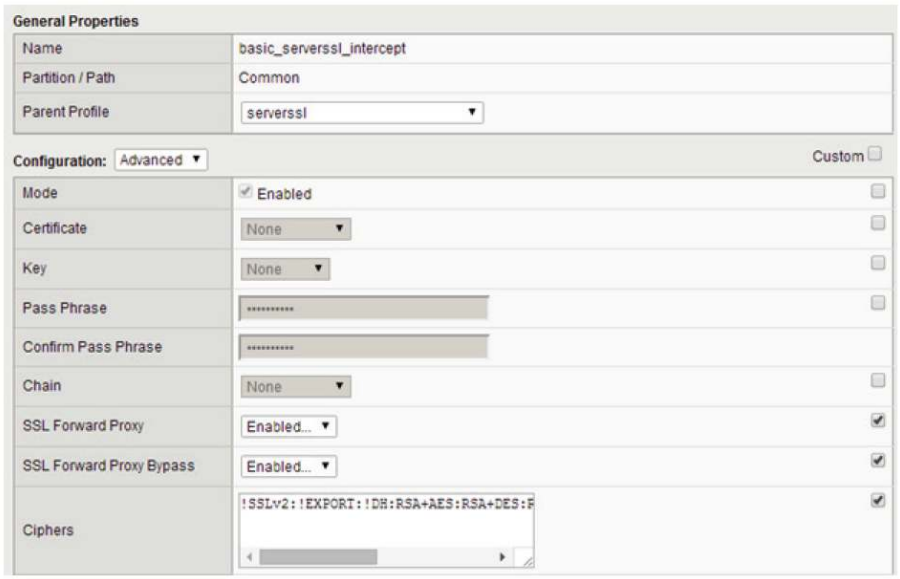

Figure 28: SSL Server Profile Forward Proxy settings

Scroll down and set the Secure Renegotiation to Request.

Figure 29: SSL Client Profile Secure Renegotiation

Create a new node which is the self IP address of the External BIG-IP. This node will be added to two new pools in the next section. Within the GUI, select Local **Traffic→Nodes→Node List**, and then choose create. Specify a name and an IP address.

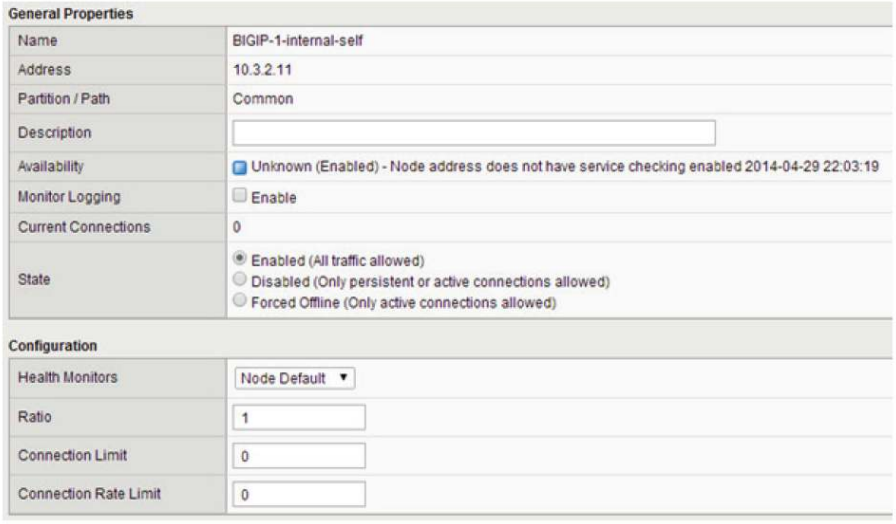

Figure 30: BIG-IP Node

Next create two new pools. These pools will be for port 80 traffic with the second handling any wildcard traffic too. Within the GUI, select Local **Traffic→Pools→Pool list**, and then select **create**. Specify a name for each pool. In the following examples they're called **ssl-intercept-pool-80** and **ssl-intercept-pool-ANY** respectively. Specify an Health Monitor and add a New Member. For Priority Group Activation, select **Node List**. Choose the node name from the previous step; for Service Port, enter **80**; and then click **Add**.

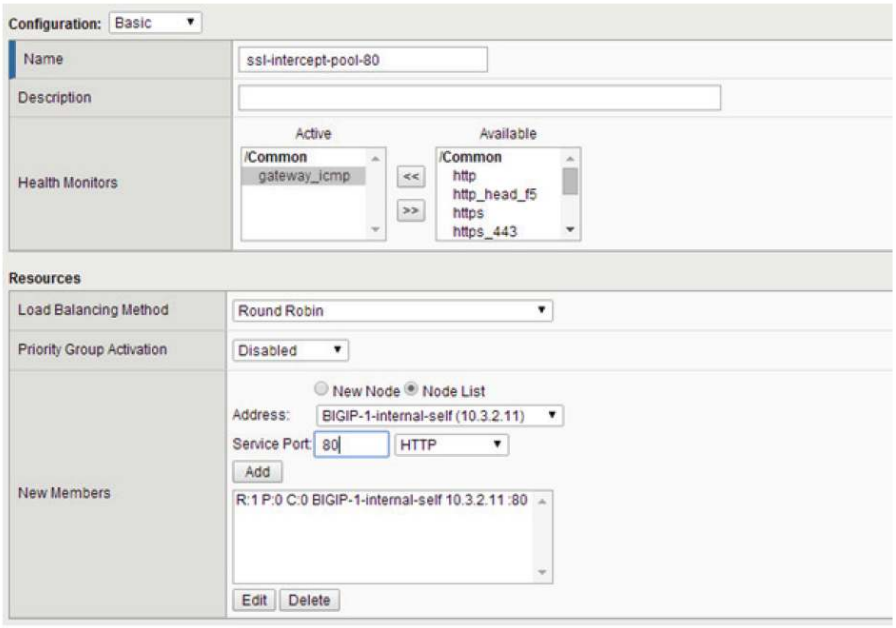

Figure 31: SSL intercept Internal BIG-IP port 80 pool

Repeat the previous step and create a second pool for service all ports.

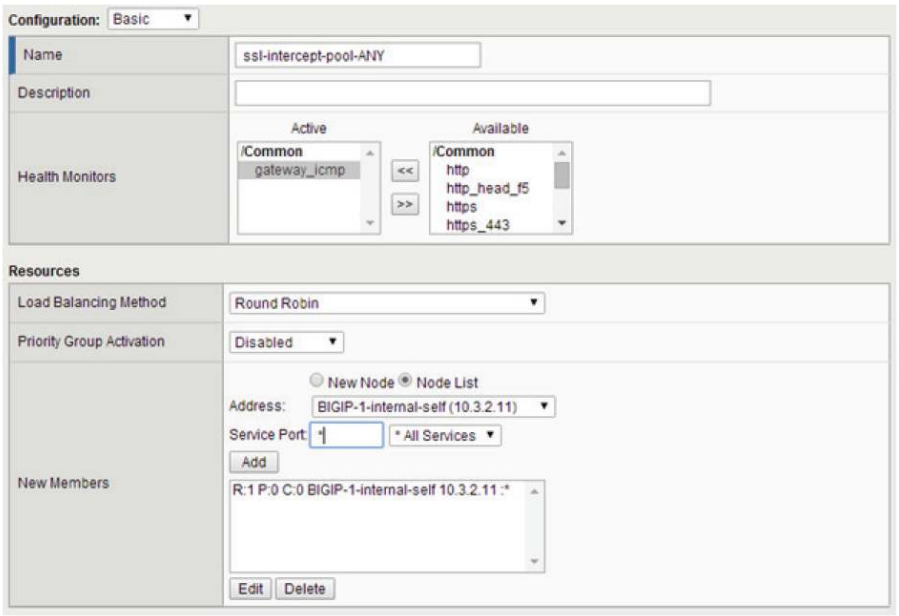

Figure 32: SSL intercept Internal BIG-IP port ANY pool

Create the following iRule. Within the GUI, select Local **Traffic→iRules→iRule List**, and then select **create**. Specify a name and copy the code in the following graphic. Rename the pool accordingly. It should be the name of the port 80 pool.

```
when HTTP _ REQUEST {
HTTP::header insert X-Proxy-HTTPS 1
pool ssl-intercept-pool-80
SSL::disable serverside
}
```

Figure 33: Internal BIG-IP iRule

Figure 34: Internal BIG-IP iRule

Create a standard virtual server with a network destination of 0.0.0.0 and mask of 0.0.0.0, and service port 443. Within the GUI, select Local **Traffic→Virtual Servers→Virtual Server List**, and then select **create**.

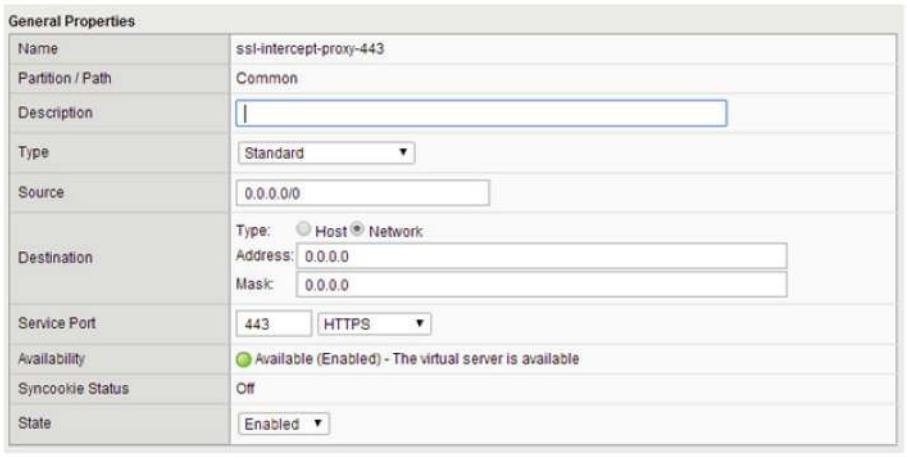

Figure 35: Internal BIG-IP HTTPS Virtual Server General Properties

For Protocol, select TCP and for HTTP Profile, select http.

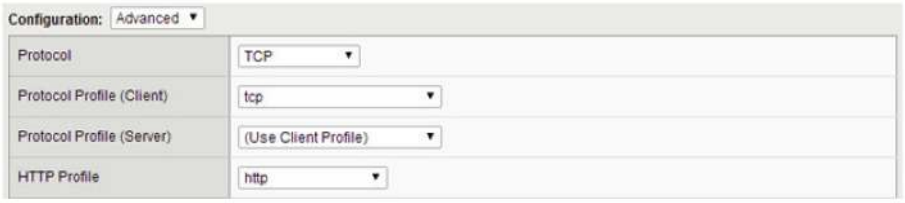

Figure 36: Internal BIG-IP HTTPS Virtual Server Advanced Properties

Within the SSL Profile section, select the client and server profiles created earlier.

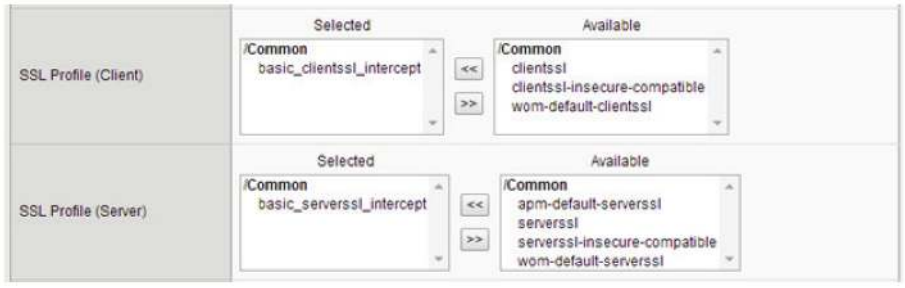

Figure 37: Internal BIG-IP HTTPS Virtual Server SSL Profiles

Enable this Virtual Server to only listen on the Internal VLAN. This will ensure all other VLANs are not inadvertently allowed. Ensure Source Address Translation is disabled.

Figure 38: Internal BIG-IP HTTPS Virtual Server VLAN and SNAT

Verify Address Translation is Disabled, and for Port Translation, check Enabled.

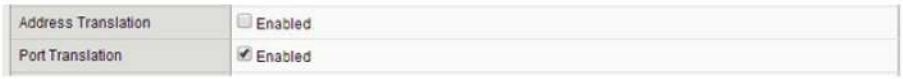

Figure 39: Internal BIG-IP HTTPS Virtual Server Address and Port Translation

Within the resources section, select the ssl intercept iRule and move it to the Enabled column. Define the Default Pool to be the ssl-intercept-pool-ANY previously created.

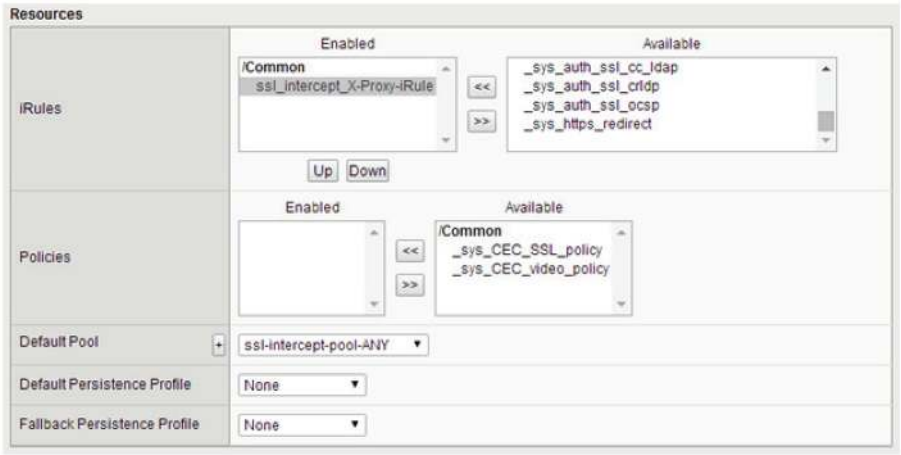

Figure 40: Internal BIG-IP HTTPS Virtual Server iRule and Default Pool

Create a performance layer 4 virtual server with a network destination of 0.0.0.0 and mask of 0.0.0.0, and a server port of 0 (*All Ports). Enable *All Protocols, verify that Address and Port Translation are disabled, and assign the wildcard any port pool. Within the GUI, select Local TrafficgVirtual ServersgVirtual Server List, and then select create.

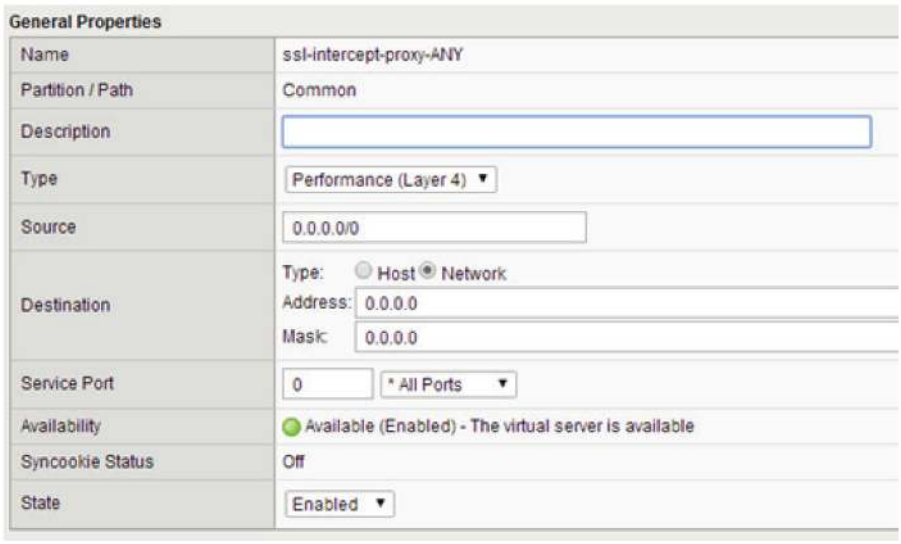

Figure 41: Internal BIG-IP Wildcard Virtual Server General Properties

For the Protocol, select * All Protocols, and for the Profile, select fastL4.

Figure 42: Internal BIG-IP Wildcard Virtual Server Protocol Profile

Enable the VLAN that the Virtual Server is listening on to be the internal VLAN, and for the Source Address Translation, select None.

Figure 43: Internal BIG-IP Wildcard Virtual Server VLAN Assignment

Make sure that Address Translation and Port Translation are not enabled.

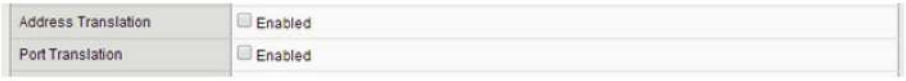

Figure 44: Internal BIG-IP Wildcard Virtual Server Address and Port Translation

For Default Pool, select ssl-intercept-pool-ANY, this was created earlier.

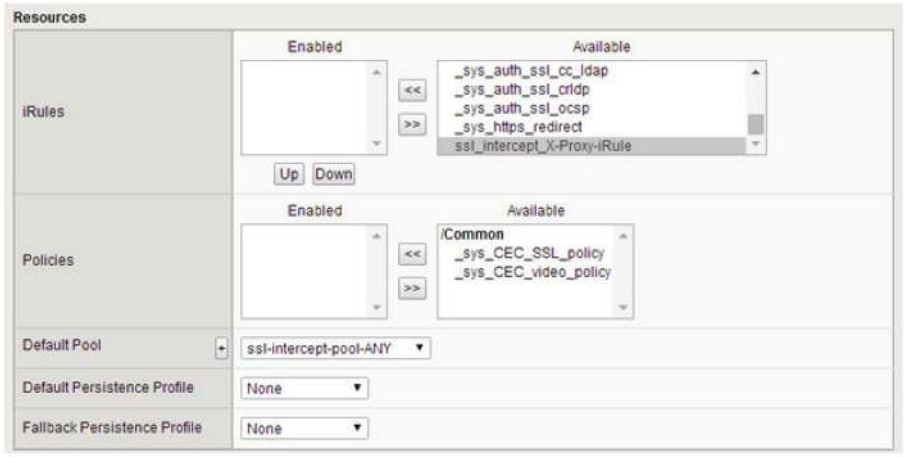

Figure 45: Internal BIG-IP Wildcard Virtual Server Default Pool

The Internal BIG-IP is now configured; the next step is to configure the External BIG-IP.

Configuring SSL Intercept on the External BIG-IP

This section will step through the configuration settings to be applied to the External BIG-IP. This is the BIG-IP#1, which is the BIG-IP closest to the Internet-facing router.

Create a new node that is the self IP address of the Internet-facing router. This node will be added to two new pools in the next section. Within the GUI, select **Local Traffic→Nodes→Node List**, and then select **create**. For the Name, enter Internet Router, and for the Address, enter the address of the Internet-facing router.

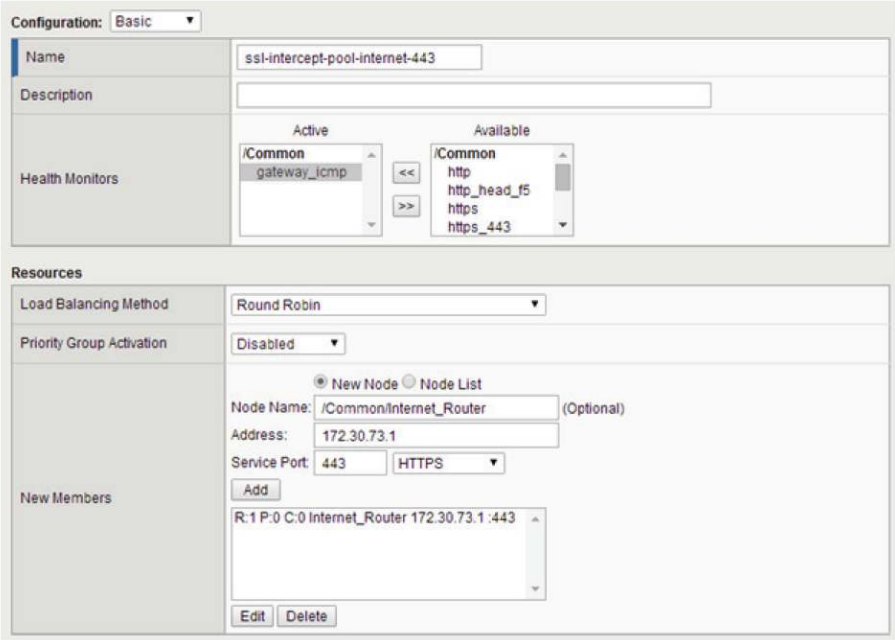

Figure 46: BIG-IP Node

Next, create two new pools. These pools will be for port 443 traffic and for wildcard any traffic. Within the GUI, select **Local Traffic→Pools→Pool List**, and then select **create**. Specify names for the pools. in the following example, we called them **ssl-intercept-pool-internet-443** and **ssl-intercept-poolinternet- ANY** respectively. Specify a health monitor that is appropriate for the deployment, in this example we chose **gateway_icmp**. Add a new member by selecting the Node list button. Choose the node name from the previous step, specify the port to be 443 and then click **Add**.

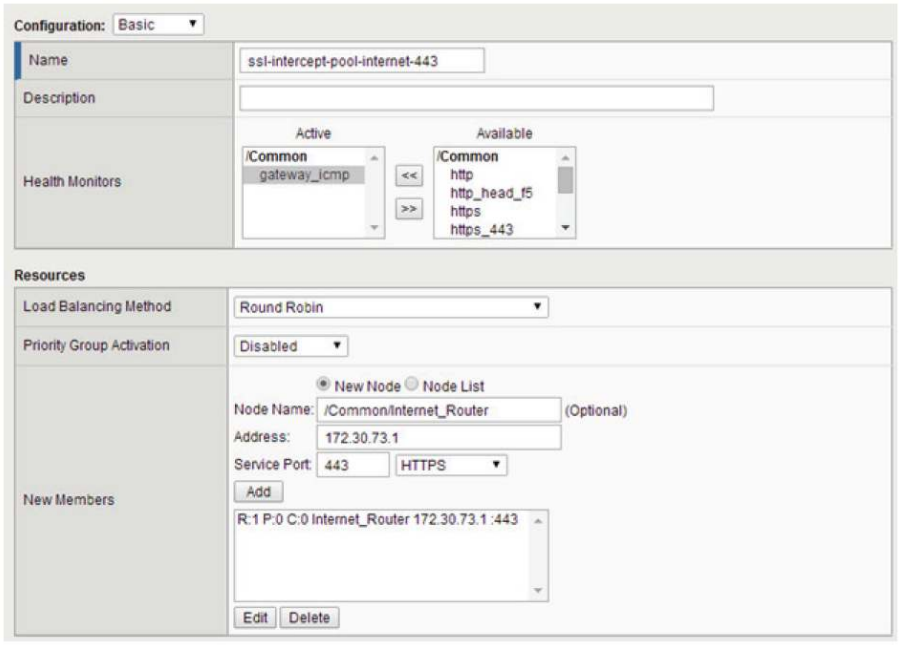

Figure 47: SSL Intercept External BIG-IP port 443 pool

Repeat the previous steps to create a second pool to service all ports.

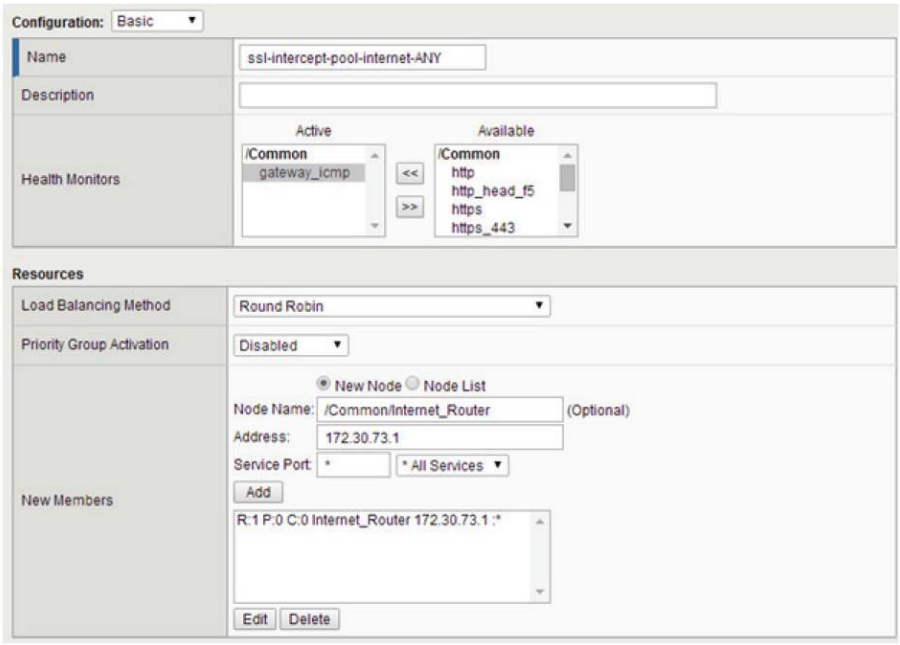

Figure 48: SSL intercept External BIG-IP port ANY pool

Create the following iRule. Within the GUI, select **Local Traffic→iRules→iRule List**, and then select create. Specify a name and copy the code in the following graphic. Rename the pool accordingly. It should be the name of the port ANY pool: **ssl-intercept-pool-internet-ANY**.

```
when HTTP _ REQUEST {
  if { not ( [HTTP::header exists X-Proxy-HTTPS] ) } {
    pool ssl-intercept-pool-internet-ANY
    SSL::disable serverside
  }
}
```

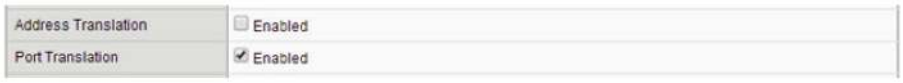

Figure 49: X-Proxy-HTTPS iRule

Create a standard virtual server with a network destination of 0.0.0.0 and a mask of 0.0.0.0, and for Service Port, enter **80**. Assign the **serverssl-insecure-compatible** server SSL profile and disable Address Translation. Be sure that Port Translation is **enabled**. Assign the wildcard port 443 pool and the iRule.

Figure 50: External BIG-IP HTTP Virtual Server General Properties

For Protocol, select TCP, and for HTTP Profile, select http.

Figure 51: External BIG-IP HTTP Virtual Server Advanced Properties

Within the SSL Profile section, select the serverssl-insecure-compatible profile.

Figure 52: External BIG-IP HTTP Virtual Server SSL Profiles

Enable this virtual server to only listen on the Internal VLAN. This will ensure all other VLANs are not inadvertently allowed. Ensure Source Address Translation is disabled by selecting **None**.

Note: If the deployment scenario is using private addressing space inside the protected network. You may want to consider enabling Source Address translation according to your network environment.

Figure 53: External BIG-IP HTTP Virtual Server VLAN and SNAT

For Address Translation, leave the Enabled box unchecked, and for Port Translation, check Enabled.

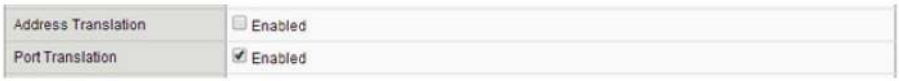

Figure 54: External BIG-IP HTTP Virtual Server Address and Port Translation

Within the resources section, select the ssl intercept iRule **ssl-intercept-Internet-iRule** and move it to the Enabled column. For Default Pool, select **ssl-intercept-pool-internet-443**, which is the name of the previously created ssl intercept 443 pool.

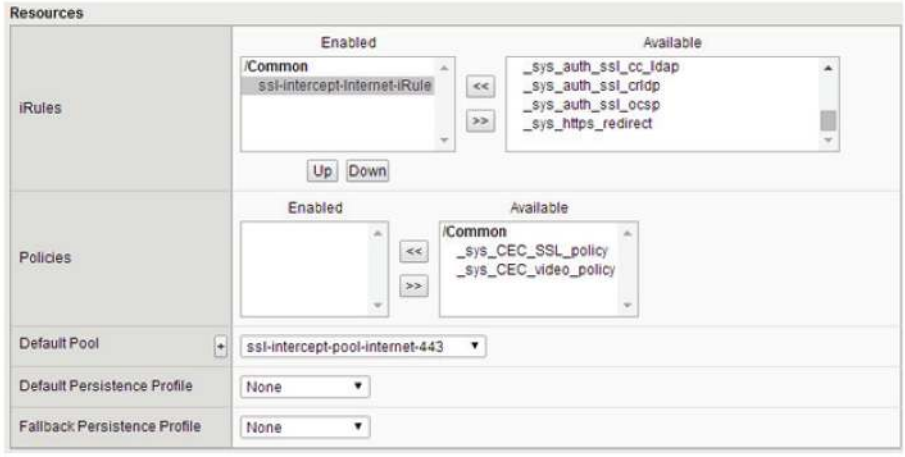

Figure 55: External BIG-IP HTTP Virtual Server iRule and Default Pool

Repeat the previous steps to create a Performance (Layer 4) virtual server with a network destination of **0.0.0.0**, a mask of **0.0.0.0**, and a server port of **0 (*All Ports)**. Enable *All Protocols; verify that Address and Port Translation are disabled, and assign the wildcard any port pool. Within the GUI, select **Local Traffic→Virtual Servers→Virtual Server List**, and then select **create**.

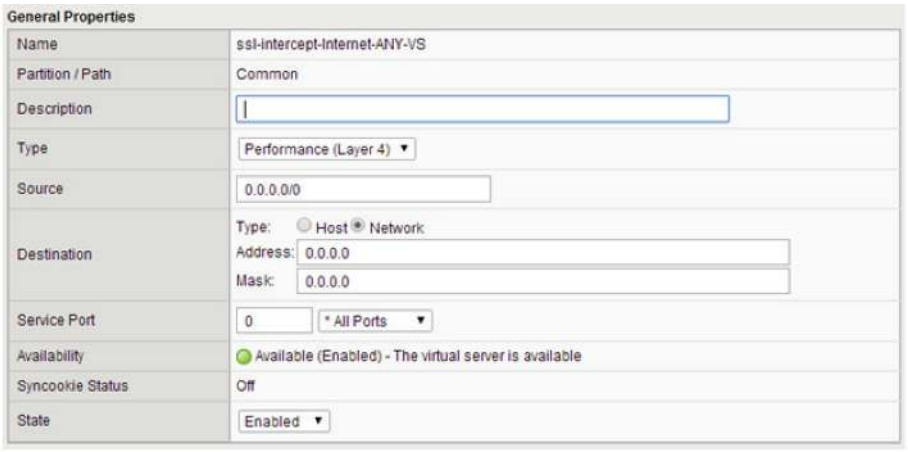

Figure 56: External BIG-IP Wildcard Virtual Server General Properties

For Protocol, select *** All Protocols**, and for Profile, select **fastL4**.

Figure 57: External BIG-IP Wildcard Virtual Server Protocol Profile

Enable the VLAN that the Virtual Server is listening on to be the **internal** VLAN. And set the Source Address Translation field to **None**.

Note: If the deployment scenario is using private addressing space inside the protected network, you may want to consider enabling Source Address Translation according to your network environment.

Figure 58: External BIG-IP Wildcard Virtual Server VLAN Assignment

Make sure that Address Translation and Port Translation are not enabled.

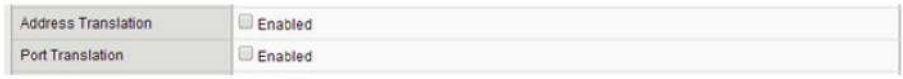

Figure 59: External BIG-IP Wildcard Virtual Server Address and Port Translation

For Default Pool, select **ssl-intercept-pool-internet-ANY**, the name of the pool that was created earlier.

Figure 60: External BIG-IP Wildcard Virtual Server Default Pool

The External BIG-IP is configured. The next step is to configure the client Default Gateway and Browser certificate.

Modifying the client host configuration

These steps are client O.S. - And browser-specific. First set the Client default gateway to be the Internal BIG-IP (BIG-IP#2) Internal Client VLAN self IP address. Then install the certificate into the client browser as a trusted intermediate CA. Refer to the Client O.S. and Browser documentation for specific detailed steps. Sourcefire NGIPS Setup and Configuration.

Sourcefire NGIPS Setup and Configuration

To configure and set up Sourcefire NGIPS–managed devices, you must define blocking rules, set up the IPS to capture traffic, and, if necessary, block untrusted IP addresses. Sourcefire NGIPS is widely deployed in many enterprise environments that help protect the perimeter from intrusions.

Review the Sourcefire Installation Guides to set up a Defense Center and managed devices. The appliance will be configured as a Next Generation firewall.

Log in to the Sourcefire management interface and select the device you have configured.

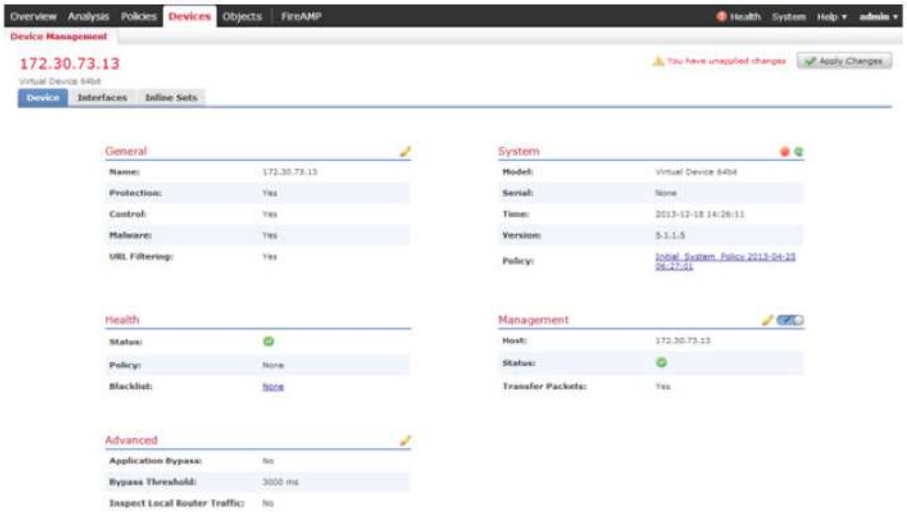

Figure 61: Sourcefire NGIPS Interfaces Tab

Enter the specific details within the Device section. Click the pencil icon to edit the device-specific details.

Figure 62: Sourcefire Managed Device Setup

We have two separate security zones created on this device: the BIG-IP load balanced security zone, which is the zone for all the IPS-managed device interfaces, and the VLAN-35 security zone, which is the network for all the application server nodes (i.e., FTP, HTTPS, WEB). The Sourcefire NGIPS– managed device will inspect network flows coming from the BIG-IP appliance and then connect to the back-end server pools.

Figure 63: Sourcefire Interfaces

Create Inline Bridge

On the Sourcefire device, we created an inline bridge to simulate a routed network setup. This ensures that network flows routed through the Sourcefire NGIPS will in turn be sent back through the BIG-IP device. As described above, network flows route through the Sourcefire NGIPS via the forwarding IP virtual server, and then through the NGIPS protect virtual server hosted on the F5 BIG-IP device.

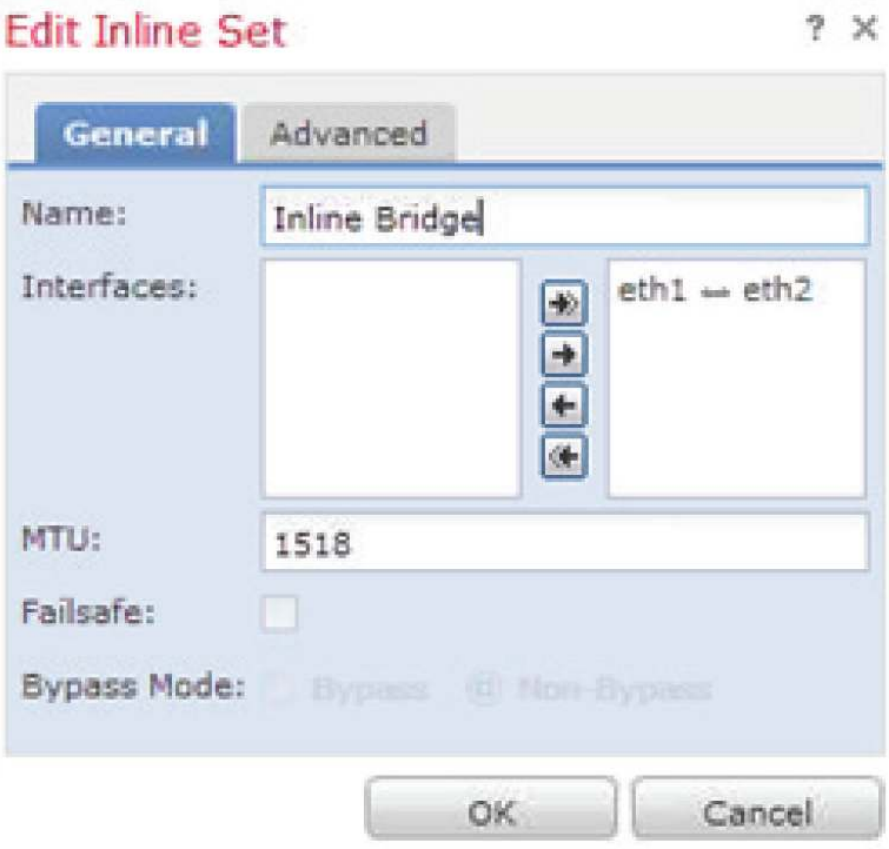

Figure 64: Inline Bridge

After the inline bridge is configured, we will create the inline settings. In this case we will set up the Transparent Inline Mode.

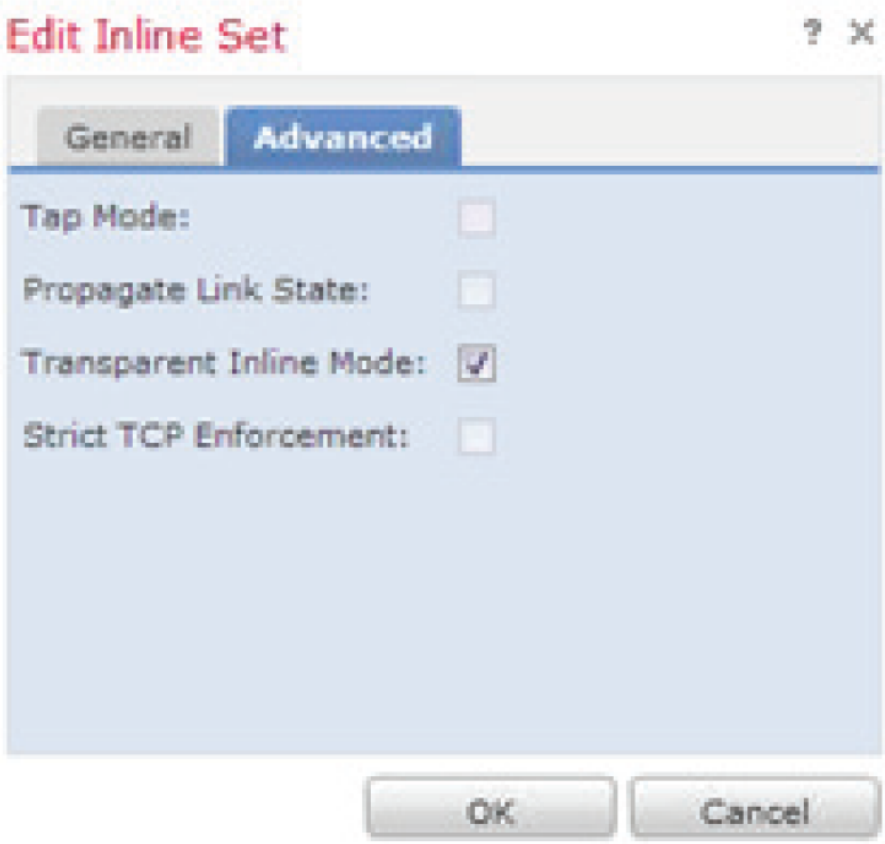

Figure 65: Transparent Inline Mode

Network flows from the BIG-IP will be sent through to the Sourcefire-managed device and will be blocked if necessary. The External Security Zone needs to be associated with this inline bridge.

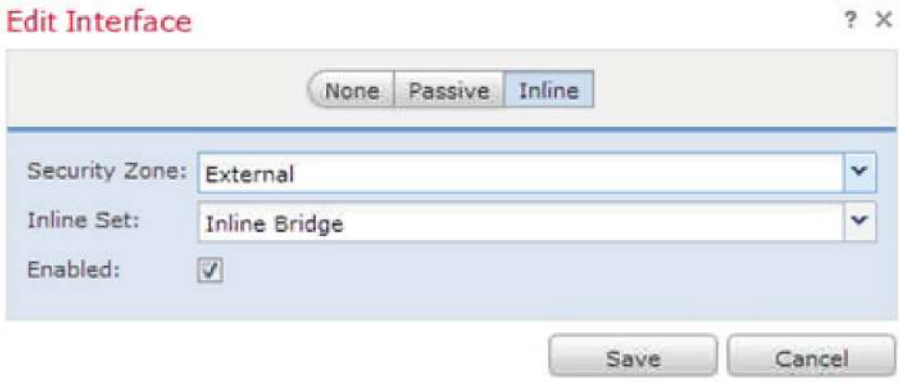

Figure 66: Associate an Inline Bridge with the External Security Zone

The Internal Security Zone also needs to be associated with this inline bridge.

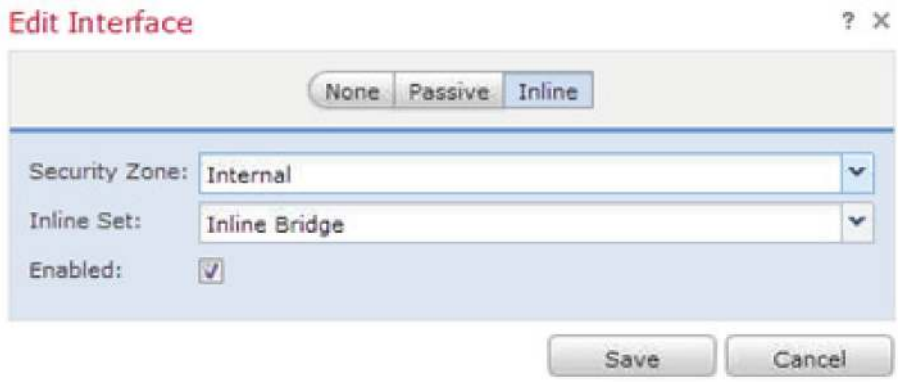

Figure 67: Associate an Inline Bridge with the Internal Security Zone

Configure VLANS

Once we have configured the inline bridge, we will configure the VLAN setup. One VLAN (VLAN35) will be configured for the F5 BIG-IP client, and another will be configured for back-end connection to the protected virtual server on the F5 BIG-IP. The VLAN configuration and networks should correlate to those of the BIG-IP.

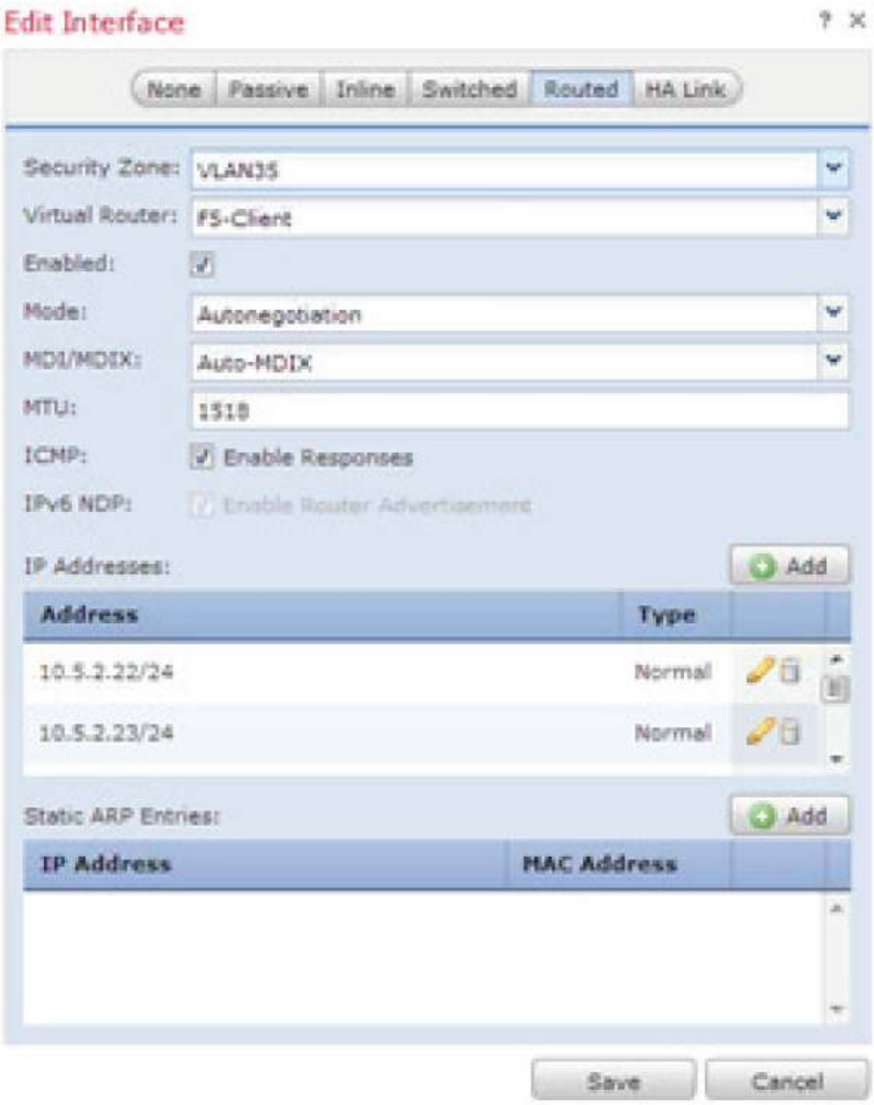

Figure 68: VLAN 35 Configuration

Create Security Zones

After the VLAN configuration is complete, create security zones tied to each IP address that are applied a policy. This will allow for granular configuration of traffic.

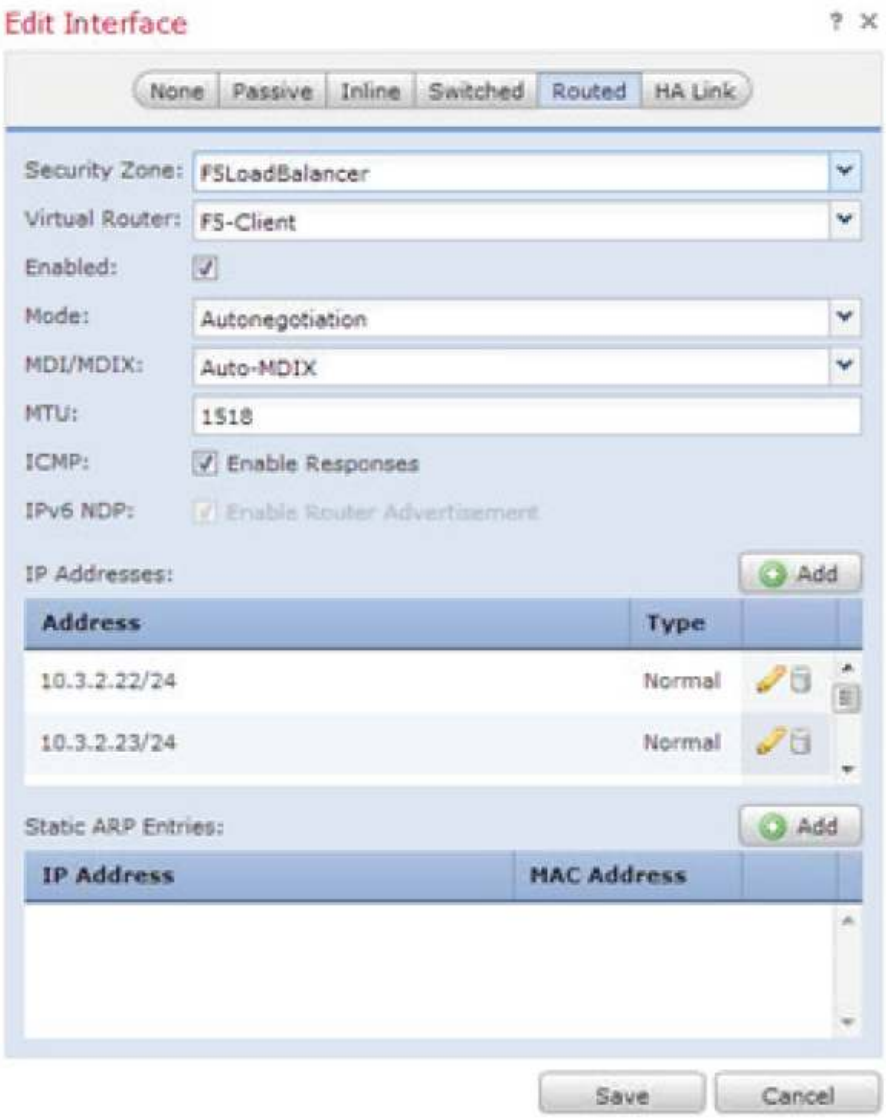

Figure 69: F5 Load-Balancer Security Zone

The Sourcefire NGIPS needs a virtual router configured in order to associate an IP address to the managed device interfaces. To configure a virtual router, select the **Virtual Routers** tab.

Figure 70: Virtual Router Configuration Tab

Virtual Router Configuration

To route traffic through multiple managed devices to the BIG-IP–protected HTTPS/FTP virtual servers, you will need to create a virtual router on the Sourcefire device. Provide a name, select the available interfaces, and then move them to the selected interface table. For additional information on configuration of the Sourcefire-managed device, please consult the Sourcefire managed-device documentation.

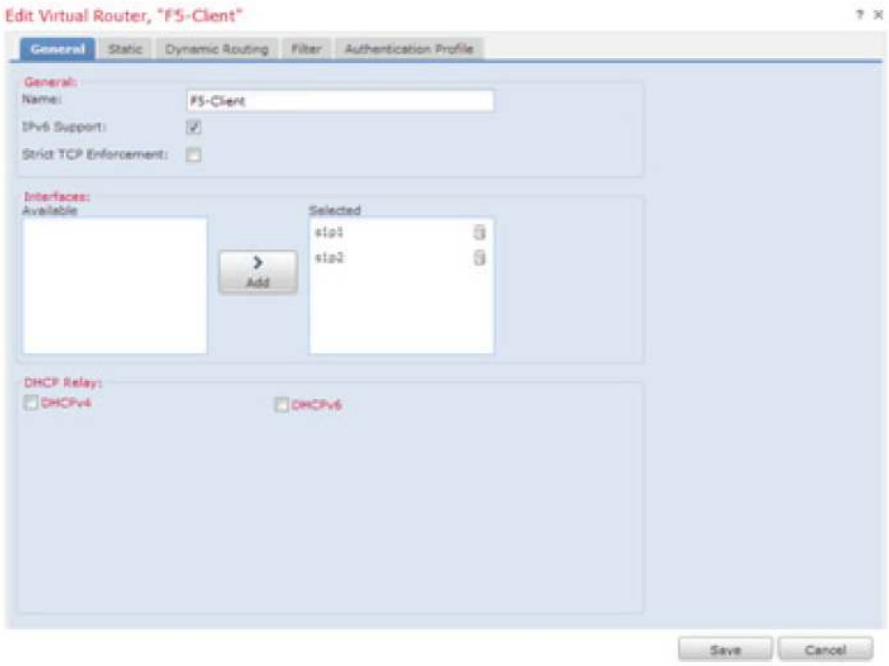

Figure 71: Add Interfaces to Virtual Router

Select the **Static** tab to create a static route. Enter a name and leave the preference and type settings at default. For Destination, enter **0.0.0.0/0;** and for Gateway, enter **10.3.2.16 (The BIG-IP self IP address)**.

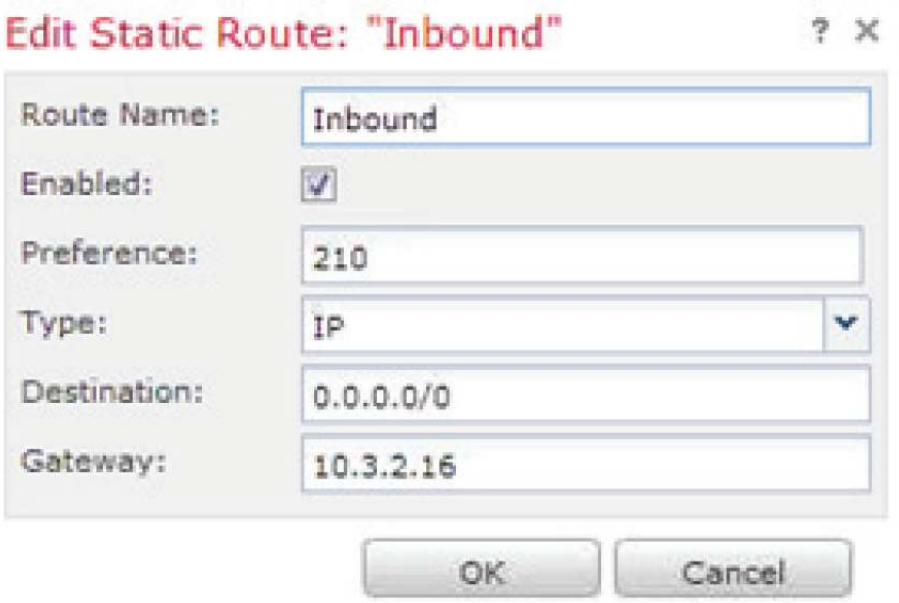

Figure 72: Edit Static Route

Create Intrusion Policy

After the configuration of the necessary networking components, you will need to create an intrusion policy to ensure that IP addresses are properly blocked for bad requests. In this example, we created a request aptly titled **bad**, which if triggered would initiate blocking.

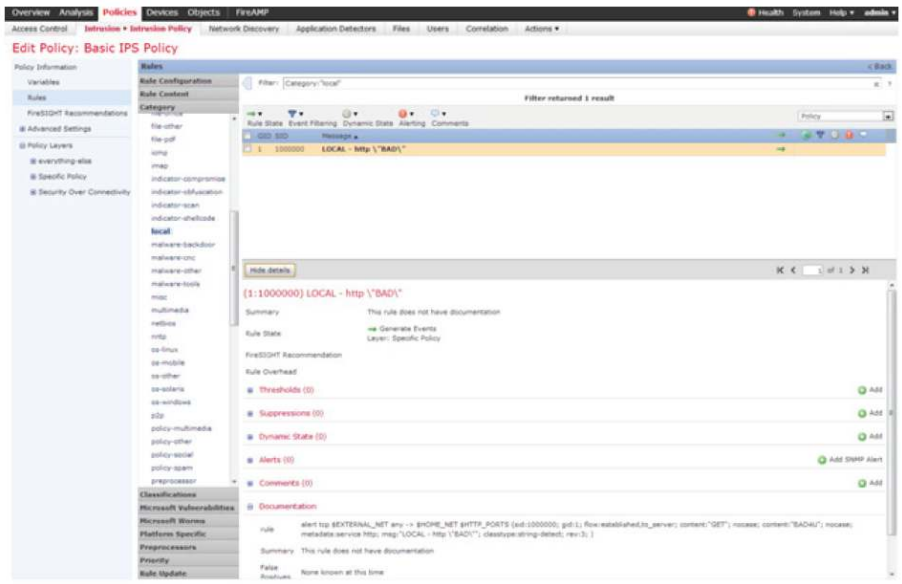

Figure 73: Create Basic Intrusion Policy

Select the **Access Control** tab. Within the default action value, verify that the Basic Intrusion Policy, as shown in Figure 71 is selected. Click the **Save and Apply** button in order to commit the policy settings.

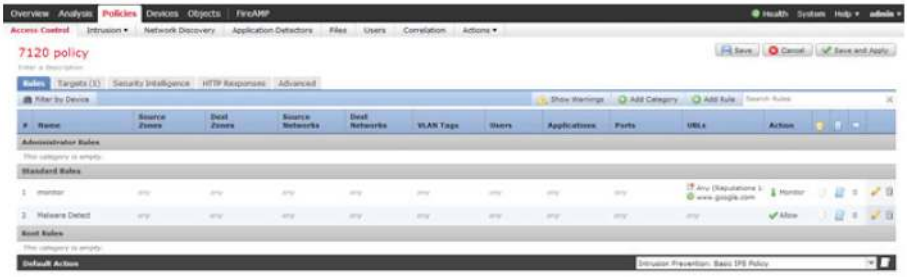

Figure 74: Access Control Policy Rules

Egress Policy Management

If the deployment scenario is providing client egress access traffic enforcement, then modify the Action setting to not just monitor, but also to drop traffic when the policy is detected.

Figure 75: Rule State Selection

Create Remediation Policies

After you have created your intrusion policy, we will need to create a policy for remediation. This will protect against potential IP threats to your applications. As described in the first section of this document, you will have network flows traverse the Sourcefire NGIPS via the virtual server on the BIG-IP, and policies will then be applied to block or allow traffic based upon preset criteria.

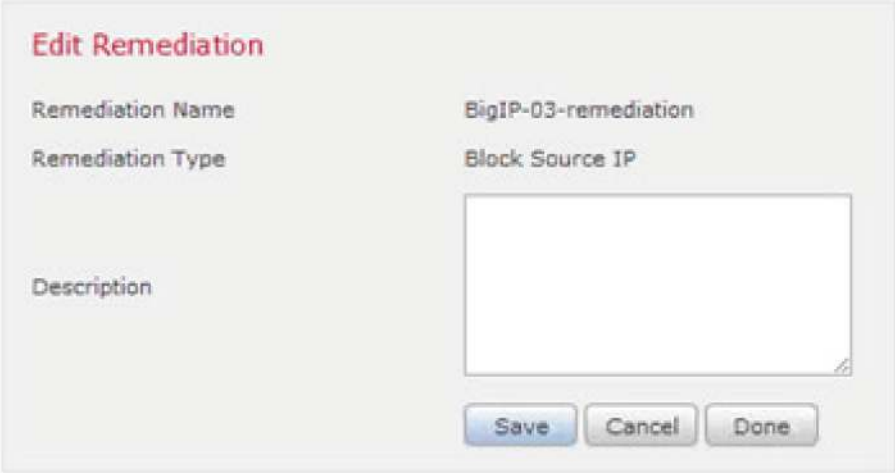

Figure 76: Block Source IP Remediation

Figure 77: Policies for Remediation

Remediated Policy Reporting

As traffic is sent through the NGIPS system that matches the policy rules, the remediation and correlation charts will report traffic hits. The remediation and correlation event counts in Figure 76 report 14,879 hits.

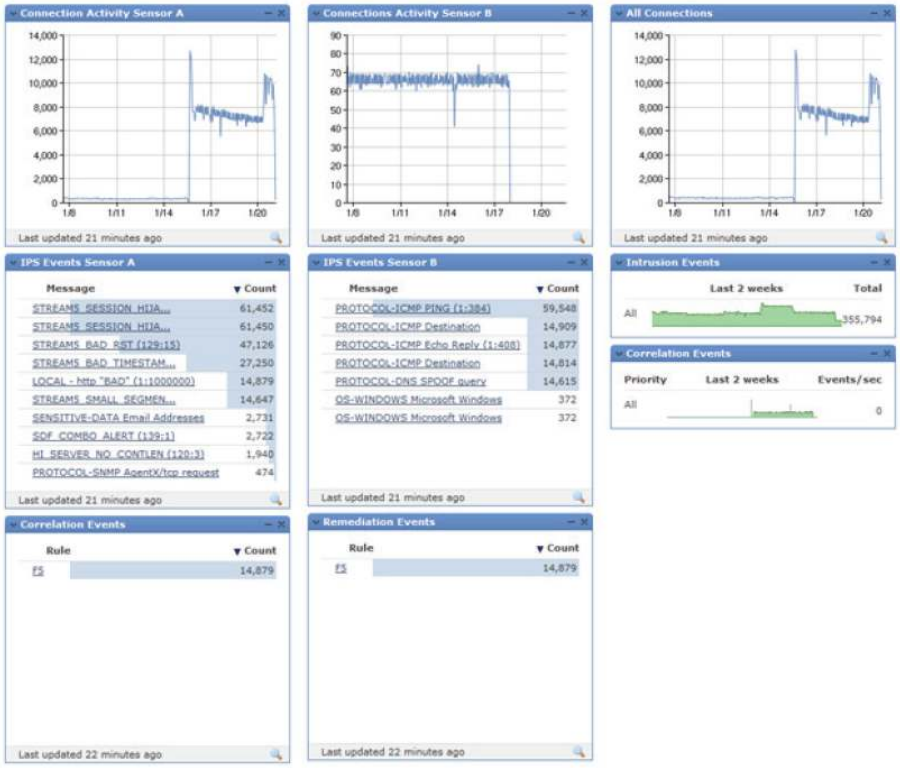

Figure 78: Sourcefire Dashboard Example

Conclusion

This concludes the recommended practices for configuring F5 BIG-IP with the Sourcefire NGIPS. The Air Gap architecture has been demonstrated to address both the SSL visibility and control and IPS Policy Based Traffic Steering and Blocking user scenarios. With the termination of SSL on the BIG-IP LTM, NGIPS sensors are provided visibility into both ingress and egress traffic to adapt and protect an organization's applications, servers and other resources. By leveraging the IPS Policy Based Traffic Steering, an organization can leverage this configuration and can continue to scale through the addition of more Sourcefire NGIPS managed devices in order to provide more traffic capacity for the protected networks and applications. This policy based flexibility which can be provided by the BIG-IP LTM, can also be leveraged to selectively direct traffic to different pools of resources based on business, security or compliance requirements.

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 www.f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com