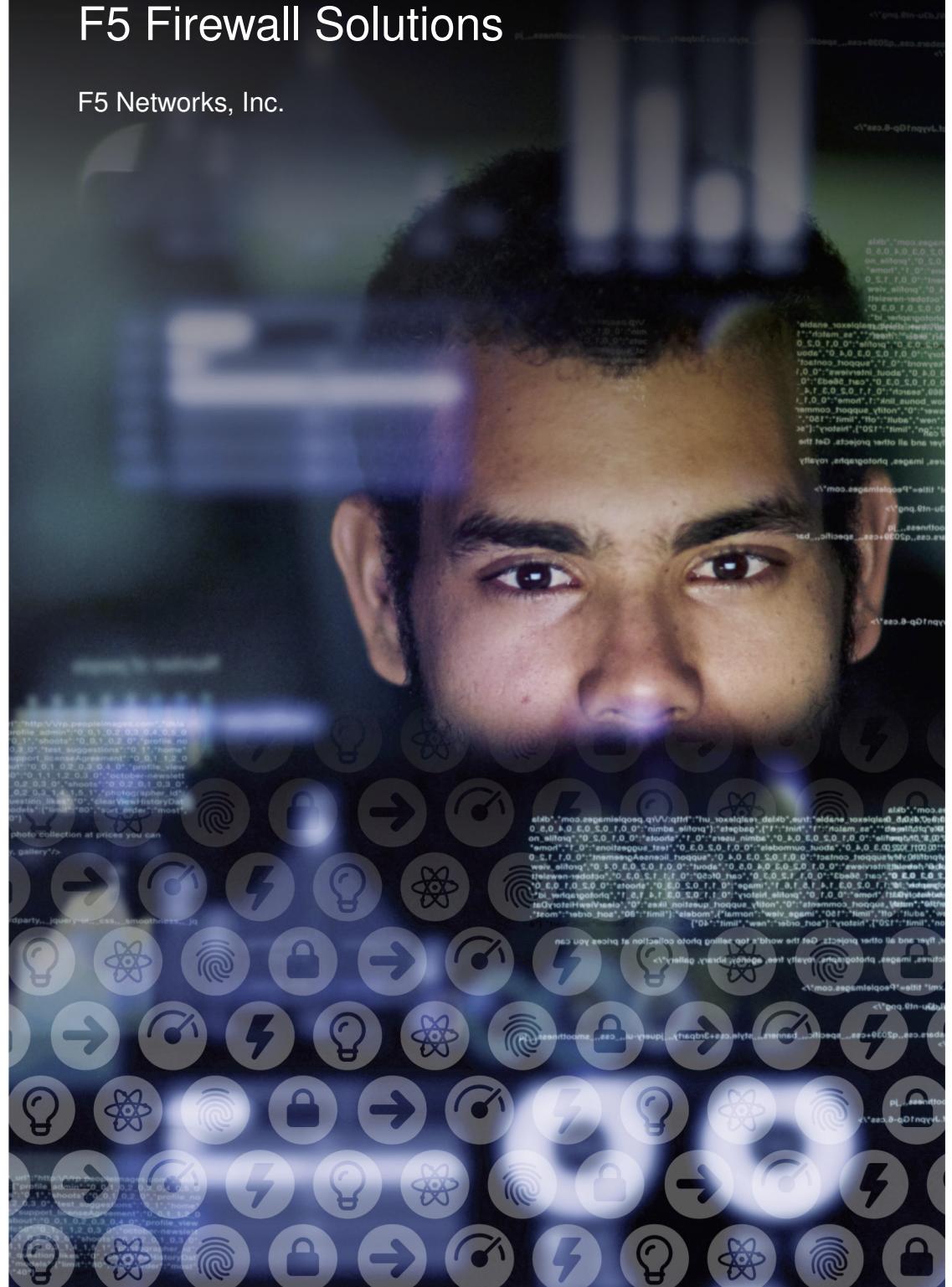




Agility 2017 Hands-on Lab Guide

F5 Firewall Solutions

F5 Networks, Inc.



Contents:

1 Class 2: Advanced Multi-Layer Firewall Protection	5
1.1 Module 1: F5 Multi-layer Firewall Lab	5

Class 2: Advanced Multi-Layer Firewall Protection

Welcome to the F5 Agility 2016 Multilayer Firewall Implementations setup and hands-on exercise series.

1.1 Module 1: F5 Multi-layer Firewall Lab

The purpose of the Lab Setup and Configuration Guide is to walk you through the setup of F5 BIGIP to protect applications at multiple layers of the OSI stack hence providing Application Security Control. This in effect allows F5 BIG-IP to be multiple firewalls within a single platform.

Assumptions/Prerequisites: You have attended the AFM 101 lab sessions either this year or in previous years. Additionally this lab guide assumes that you understand LTM/TMOS basics and are comfortable with the process of creating Nodes, Pools, Virtual Servers, Profiles and Setting up logging and reporting.

There are three labs detailed in this document.

Lab 1

This lab has six steps in configuring an Advanced Multi-layer firewall applicable to many data center environments. Task 7 will demonstrate additional protocol protections.

Tasks 1 - 2 highlights the flexibility of leveraging an application proxy such as the BIG-IP for your perimeter security utilizing common traffic management techniques.

Task 3 & 4 Breaks out applying differing security policies to the multi-tiered application deployment.

Task 5 Highlights the flexibility of the Multi-Layered Firewall to solve common problems for hosting providers.

Task 6 Applies Layer 7 protocol validation and security for HTTP to the existing applications.

Task 7 Highlights protecting the DNS protocol.

Lab 2

This lab highlights Advanced Firewall Security (L2-7) layering on authentication and access control with Access Policy Manager Application Security (L7) for Multi-tenancy using Route Domains and network fire-walling. (LTM+AFM+APM)

Lab 3

This lab introduces iRules Language eXtensions (LX) or iRulesLX which enables node.js on the BIG-IP platform. The lab uses Tcl iRules and JavaScript code to make a MySQL call to look up a client IP address providing access control in the Multi-Layered Firewall.

Lab 4

This lab highlights the Advanced Firewall Manager SSH proxy for securing SSH traffic. You will configure an SSH Profile to control the command users can execute in an SSH channel.

Note: IP addresses in screenshots are examples only. Please read the step-by-step lab instructions to ensure that you use the correct IP addresses.

1.1.1 Lab 1: Advanced Firewall with Protocol Security

In this lab, you will build an extensive perimeter firewall with advanced Layer 7 security mitigations

Estimated completion time: 45 minutes

Objective:

- Create multiple internal pools and virtual servers for different applications
- Create external hosted virtual server
- Configure LTM policy to direct traffic to appropriate virtual server
- Configure local logging; test
- Configure a network firewall policy to protect the external virtual server
- Create a network firewall policy to protect the internal application virtual servers; test
- Apply the XFF-SNAT iRule to the external virtual server; test
- Modify the network firewall policy to block based on XFF; test
- Apply Layer 7 (403 Denied) to respond to firewall drop rules
- Configure HTTP protocol security; test
- Configure Clone Pool; test

Lab Requirements:

- Remote Desktop Protocol (RDP) client utility
 - Windows: Built-in
 - Mac (Microsoft Client): <https://itunes.apple.com/us/app/microsoft-remote-desktop/id715768417?mt=12>
 - Mac (Open Source Client): http://sourceforge.net/projects/cord/files/cord/0.5.7/CoRD_0.5.7.zip/
 - Unix/Linux (Source – Requires Compiling): <http://www.rdesktop.org/>
- Connectivity to the facility provided Internet service
- Unique destination IP address for RDP to your lab

Estimated completion time: 1 Hour

TASK 1 – Configure pools and internal virtual servers

A virtual server is used by BIG-IP to identify specific types of traffic. Other objects such as profiles, policies, pools and iRules are applied to the virtual server to add features and functionality. In the context of security, since BIG-IP is a default-deny device, a virtual server is necessary to accept specific types of traffic.

The pool is a logical group of hosts that is applied to and will receive traffic from a virtual server.

On your personal device

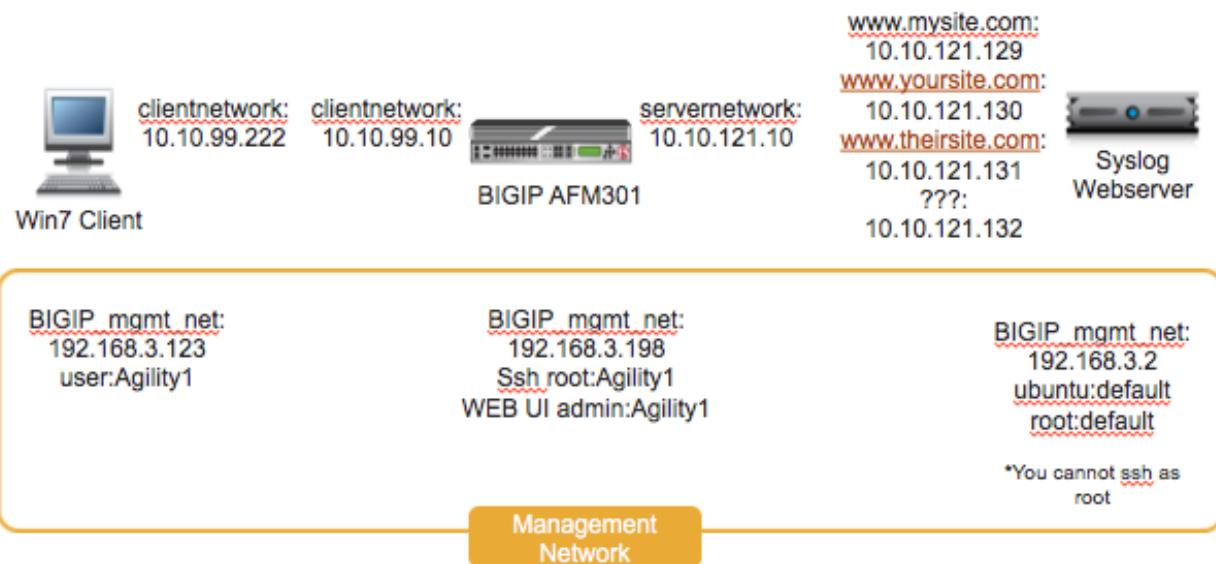
Look at the supplemental login instructions for:

External Hostnames

External IP addressing diagram

Login IDs and Passwords are subject to change as well.

All networks are /24



On BIG-IP

Create a pool using the following information:

Navigation: Local Traffic > Pools > Pool List, then click Create

Name	Health Monitor	Members	Service Port
pool_www.mysite.com	tcp_half_open	10.10.121.129	80
pool_www.mysite.com-api	tcp_half_open	10.10.121.132	80
pool_www.theirsite.com	tcp_half_open	10.10.121.131	80
pool_www.yoursite.com	tcp_half_open	10.10.121.130	80

Configuration: Basic

Name	pool_www.mysite.com						
Description							
Health Monitors	<div style="display: flex; justify-content: space-between;"> <div style="flex: 1;"> Active <input checked="" type="checkbox" value="/Common/tcp_half_open"/> /Common/tcp_half_open </div> <div style="flex: 1;"> Available <input type="checkbox" value="https_head_f5"/> https_head_f5 <input type="checkbox" value="inband"/> inband <input type="checkbox" value="tcp"/> tcp <input type="checkbox" value="udp"/> udp </div> </div>						
Resources <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%;">Load Balancing Method</td> <td>Round Robin</td> </tr> <tr> <td>Priority Group Activation</td> <td>Disabled</td> </tr> <tr> <td>New Members</td> <td> <div style="display: flex; align-items: center;"> <input checked="" type="radio"/> New Node <input type="radio"/> New FQDN Node <input type="radio"/> Node List (Optional) </div> <div style="margin-top: 5px;"> Node Name: <input type="text"/> Address: <input type="text" value="10.10.121.129"/> Service Port: <input type="text" value="80"/> <input type="button" value="HTTP"/> </div> <div style="margin-top: 10px;"> <input type="button" value="Add"/> <pre>R:1 P:0 C:0 10.10.121.129 10.10.121.129 :80</pre> </div> <div style="margin-top: 10px;"> <input type="button" value="Edit"/> <input type="button" value="Delete"/> </div> </td> </tr> </table>		Load Balancing Method	Round Robin	Priority Group Activation	Disabled	New Members	<div style="display: flex; align-items: center;"> <input checked="" type="radio"/> New Node <input type="radio"/> New FQDN Node <input type="radio"/> Node List (Optional) </div> <div style="margin-top: 5px;"> Node Name: <input type="text"/> Address: <input type="text" value="10.10.121.129"/> Service Port: <input type="text" value="80"/> <input type="button" value="HTTP"/> </div> <div style="margin-top: 10px;"> <input type="button" value="Add"/> <pre>R:1 P:0 C:0 10.10.121.129 10.10.121.129 :80</pre> </div> <div style="margin-top: 10px;"> <input type="button" value="Edit"/> <input type="button" value="Delete"/> </div>
Load Balancing Method	Round Robin						
Priority Group Activation	Disabled						
New Members	<div style="display: flex; align-items: center;"> <input checked="" type="radio"/> New Node <input type="radio"/> New FQDN Node <input type="radio"/> Node List (Optional) </div> <div style="margin-top: 5px;"> Node Name: <input type="text"/> Address: <input type="text" value="10.10.121.129"/> Service Port: <input type="text" value="80"/> <input type="button" value="HTTP"/> </div> <div style="margin-top: 10px;"> <input type="button" value="Add"/> <pre>R:1 P:0 C:0 10.10.121.129 10.10.121.129 :80</pre> </div> <div style="margin-top: 10px;"> <input type="button" value="Edit"/> <input type="button" value="Delete"/> </div>						

Note: Leave all other fields using the default values.

Navigation: Click Finished

	Status	Name	Description	Application	Members	Partition / Path
<input type="checkbox"/>	●	pool_www.mysite.com			1	Common
<input type="checkbox"/>	●	pool_www.mysite.com-api			1	Common
<input type="checkbox"/>	●	pool_www.theirsite.com			1	Common
<input type="checkbox"/>	●	pool_www.yoursite.com			1	Common

Note: The pools should now show a green circle for status.

Create the internal virtual servers using the following information:

Navigation: Local Traffic > Virtual Servers > Virtual Server List, then click Create

Name	Dest	Port	HTTP Profile	Enabled on VLAN	SNAT	Default Pool
int_vip_www.mysite.com_1.1.1.1	1.1.1.1	80	YES	loopback	AUTO	pool_www.mysite.com
int_vip_www.mysite.com-api_1.1.1.2	1.1.1.2	80	YES	loopback	AUTO	pool_www.mysite.com-api
int_vip_www.mysite.com-downloads_1.1.1.3	1.1.1.3	80	YES	loopback	AUTO	pool_www.mysite.com
int_vip_www.theirsite.com_2.2.2.2 2.2.2.2	80	YES	loopback	AUTO	pool_www.theirsite.com	
int_vip_www.yoursite.com_3.3.3.3 3.3.3.3	80	YES	loopback	AUTO	pool_www.yoursite.com	

Local Traffic » Virtual Servers : Virtual Server List » New Virtual Server...

General Properties	
Name	int_vip_www.mysite.com_1.1.1.1
Description	
Type	Standard
Source Address	
Destination Address/Mask	1.1.1.1
Service Port	80 HTTP
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled

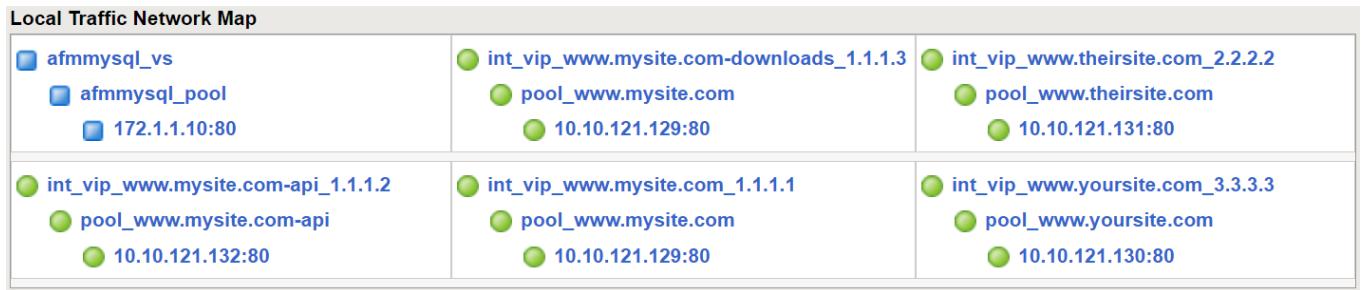
Configuration: Basic	
Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	http
FTP Profile	None
RTSP Profile	None
SSH Proxy Profile	None
SSL Profile (Client)	<div style="display: flex; align-items: center;"> <div style="flex: 1; border: 1px solid #ccc; padding: 5px; margin-right: 10px;">Selected</div> <div style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 10px;"><<</div> <div style="border: 1px solid #ccc; padding: 2px 5px;">>></div> </div> <div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9; margin-top: 5px;"> /Common clientssl clientssl-insecure-compatible clientssl-secure crypto-server-default-clientssl </div>
SSL Profile (Server)	<div style="display: flex; align-items: center;"> <div style="flex: 1; border: 1px solid #ccc; padding: 5px; margin-right: 10px;">Selected</div> <div style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 10px;"><<</div> <div style="border: 1px solid #ccc; padding: 2px 5px;">>></div> </div> <div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9; margin-top: 5px;"> /Common apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl serverssl </div>
SMTPS Profile	None
Client LDAP Profile	None
Server LDAP Profile	None
SMTP Profile	None
VLAN and Tunnel Traffic	Enabled on...
VLANs and Tunnels	<div style="display: flex; align-items: center;"> <div style="flex: 1; border: 1px solid #ccc; padding: 5px; margin-right: 10px;">Selected</div> <div style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 10px;"><<</div> <div style="border: 1px solid #ccc; padding: 2px 5px;">>></div> </div> <div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9; margin-top: 5px;"> /Common loopback </div>
Source Address Translation	Auto Map

Local Traffic > Pools : Pool List > New Pool...

Configuration:	Basic						
Name	IDS_Pool						
Description							
Health Monitors	<div style="display: flex; align-items: center;"> <div style="flex: 1;"> Active /Common gateway_icmp </div> <div style="margin-left: 20px;"> Available /Common http http_head_f5 https https_443 </div> </div>						
Resources <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 10%;">Load Balancing Method</td> <td>Round Robin</td> </tr> <tr> <td>Priority Group Activation</td> <td>Disabled</td> </tr> <tr> <td>New Members</td> <td> <div style="display: flex; align-items: flex-end;"> <div style="flex: 1;"> <input checked="" type="radio"/> New Node <input type="radio"/> New FQDN Node <input type="radio"/> Node List Node Name: <input type="text" value="172.1.1.11"/> Address: <input type="text" value="172.1.1.11"/> Service Port: <input type="text" value="*"/> </div> <div style="margin-left: 20px;"> <small>(Optional)</small> </div> </div> <div style="margin-top: 10px;"> <input type="button" value="Add"/> R:1 P:0 C:0 172.1.1.11 172.1.1.11 :* </div> <div style="margin-top: 10px; border: 1px solid #ccc; padding: 5px; display: flex; justify-content: space-between;"> <input type="button" value="Edit"/> <input type="button" value="Delete"/> </div> </td> </tr> </table>		Load Balancing Method	Round Robin	Priority Group Activation	Disabled	New Members	<div style="display: flex; align-items: flex-end;"> <div style="flex: 1;"> <input checked="" type="radio"/> New Node <input type="radio"/> New FQDN Node <input type="radio"/> Node List Node Name: <input type="text" value="172.1.1.11"/> Address: <input type="text" value="172.1.1.11"/> Service Port: <input type="text" value="*"/> </div> <div style="margin-left: 20px;"> <small>(Optional)</small> </div> </div> <div style="margin-top: 10px;"> <input type="button" value="Add"/> R:1 P:0 C:0 172.1.1.11 172.1.1.11 :* </div> <div style="margin-top: 10px; border: 1px solid #ccc; padding: 5px; display: flex; justify-content: space-between;"> <input type="button" value="Edit"/> <input type="button" value="Delete"/> </div>
Load Balancing Method	Round Robin						
Priority Group Activation	Disabled						
New Members	<div style="display: flex; align-items: flex-end;"> <div style="flex: 1;"> <input checked="" type="radio"/> New Node <input type="radio"/> New FQDN Node <input type="radio"/> Node List Node Name: <input type="text" value="172.1.1.11"/> Address: <input type="text" value="172.1.1.11"/> Service Port: <input type="text" value="*"/> </div> <div style="margin-left: 20px;"> <small>(Optional)</small> </div> </div> <div style="margin-top: 10px;"> <input type="button" value="Add"/> R:1 P:0 C:0 172.1.1.11 172.1.1.11 :* </div> <div style="margin-top: 10px; border: 1px solid #ccc; padding: 5px; display: flex; justify-content: space-between;"> <input type="button" value="Edit"/> <input type="button" value="Delete"/> </div>						
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input checked="" type="button" value="Finished"/>							

Note: Leave all other fields using the default values.

Navigation: Click Finished



Note: The virtual server should now show a green circle for status.

Create the external virtual server using the following information:

Navigation: Local Traffic > Virtual Servers > Virtual Server List, then click Create

Name	Dest	Port	HTTP Profile	SSL Profile (Client)	Default Pool
EXT_VIP_10.10.99.30	10.99.30.43	3043	YES	www.mysite.com www.theirsite.com www.yoursite.com	pool_www.mysite.com

General Properties

Name	EXT_VIP_10.10.99.30
Description	
Type	Standard
Source Address	
Destination Address/Mask	10.10.99.30
Service Port	443 HTTPS
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled

Configuration: Basic

Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	http
FTP Profile	None
RTSP Profile	None
SSH Proxy Profile	None
SSL Profile (Client)	<div style="display: flex; align-items: center;"> <div style="flex: 1;"> Selected /Common www.mysite.com www.theirsite www.yoursite.com </div> <div style="margin: 0 10px;"> << >> </div> <div style="flex: 1;"> Available clientssl clientssl-insecure-compatible clientssl-secure crypto-server-default-clientssl wom-default-clientssl </div> </div>
SSL Profile (Server)	<div style="display: flex; align-items: center;"> <div style="flex: 1;"> Selected /Common </div> <div style="margin: 0 10px;"> << >> </div> <div style="flex: 1;"> Available apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl serverssl </div> </div>
SMTPS Profile	None
Client LDAP Profile	None
Server LDAP Profile	None
SMTP Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	None

Resources

iRules	Enabled	Available
	<input type="button" value="<<"/> <input type="button" value=">>"/> <input type="button" value="Up"/> <input type="button" value="Down"/>	/Common _sys_APM_ExchangeSupport_OA_BasicAuth _sys_APM_ExchangeSupport_OA_NtlmAuth _sys_APM_ExchangeSupport_helper _sys_APM_ExchangeSupport_main
Policies	Enabled	Available
	<input type="button" value="<<"/> <input type="button" value=">>"/>	/Common HTTPS_Virtual_Targeting_PolicyL7
Default Pool <input style="margin-left: 10px;" type="button" value="+"/> pool_www.mysite.com <input style="margin-left: 10px;" type="button" value="▼"/>		
Default Persistence Profile	None <input type="button" value="▼"/>	
Fallback Persistence Profile	None <input type="button" value="▼"/>	

Note: The pool is not necessary and might not be what you want from

a security perspective but it's here as a fallback and to let the virtual server turn green

Note: Please STOP here until after lecture

TASK 2 – Configure And Attach The LTM Policy

The LTM policy is what allows traffic to flow from the external virtual server to the internal virtual servers based on the Layer 7 request. Whether it is based on the hostname or the URI path, the request can be forwarded to a different virtual server or an application pool of servers.

Navigation: Local Traffic > Policies : Policy List > Policy List Page, then click Create

Policy Name	HTTPS_Virtual_Targeting_PolicyL7
Strategy	Execute *best* matching rule using the *best-match* strategy

Navigation: Click Create Policy

Local Traffic > Policies : Policy List > New...

<input type="button" value="Policies List"/>	<input type="button" value="Strategy List"/>	<input type="button" value="Statistics"/>
General Properties		
Policy Name	HTTPS_Virtual_Targeting_PolicyL7	
Description		
Strategy	Execute best matching rule using the best-match strategy	
Type	Traffic Policy	
<input type="button" value="Cancel"/> <input type="button" value="Create Policy"/>		

Navigation: Local Traffic > Policies : Policy List > /Common/HTTPS_Virtual_Targeting_PolicyL7

Local Traffic > Policies : Policy List > /Common/HTTPS_Virtual_Targeting_PolicyL7

<input type="button" value="Published Policy"/>	<input type="button" value="Draft Policy"/>										
General Properties											
Policy Name	HTTPS_Virtual_Targeting_PolicyL7										
Description											
Strategy	Execute best matching rule using the best-match strategy										
Type	Traffic Policy										
<input type="button" value="Cancel"/> <input type="button" value="Save Draft"/> <input type="button" value="Clone"/>											
Rules <table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>ID</th> <th>Name</th> <th>Description</th> <th><input type="button" value="Create"/></th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td></td> <td></td> <td><input type="button" value="Create"/></td> </tr> </tbody> </table>		<input type="checkbox"/>	ID	Name	Description	<input type="button" value="Create"/>	<input checked="" type="checkbox"/>				<input type="button" value="Create"/>
<input type="checkbox"/>	ID	Name	Description	<input type="button" value="Create"/>							
<input checked="" type="checkbox"/>				<input type="button" value="Create"/>							

The policy configuration should now include a Rules section

Navigation: Click Create

You will need to create the following rules within your policy:

Rule Name				
www.mysite.com	HTTP Host	Host	is	www.mysite.com
ACTION	Forward Traffic	Virtual Server		int_vip_www.mysite.com_1.1.1.1
www.yoursite.com	HTTP Host	Host	is	www.yoursite.com
ACTION	Forward Traffic	Virtual Server		int_vip_www.yoursite.com_3.3.3.3
www.theirsite.com	HTTP Host	Host	is	www.theirsite.com
ACTION	Forward Traffic	Virtual Server		int_vip_www.theirsite.com_2.2.2.2
www.mysite.com-api	HTTP Host	host	is	www.mysite.com
	HTTP URI	path	begins with	/api
ACTION	Forward Traffic	Virtual Server		int_vip_www.mysite.com-api_1.1.1.2
	Replace	http uri	path	with /
www.mysite.com-downloads	HTTP Host	host	is	www.mysite.com
	HTTP URI	path	begins with	/downloads
ACTION	Forward Traffic	Virtual Server		int_vip_www.mysite.com-downloads_1.1.1.3

Navigation: Remember to click Add after adding the matching string

The screenshot shows the configuration of a policy named "HTTPS_Virtual_Targeting_PolicyL7:www.mysite.com".

- General Properties:**
 - Policy Name: HTTPS_Virtual_Targeting_PolicyL7
 - Name: www.mysite.com
 - Description: (empty)
- Match all of the following conditions:**
 - HTTP Host host is any of www.mysite.com
- Do the following when the traffic is matched:**
 - Forward traffic to virtual server int_vip_www.mysite.com_1.1.1.1

Navigation: Click Save

Additional Example for /api. The replacement line is required to strip the path from the request for the site to work.

Local Traffic > Policies : Policy List > /Common/HTTPS_Virtual_Targeting_PolicyL7:New Rule...

Properties

General Properties

Policy Name	HTTPS_Virtual_Targeting_PolicyL7
Name	www.mysite.com-api
Description	

Match all of the following conditions:

HTTP Host	host	begins with	any of	www.mysite.com	Options	-	+
<input type="button" value="Add"/>							
HTTP URI	path	begins with	any of	/api	Options	-	+
<input type="button" value="Add"/>							

Do the following when the traffic is matched:

Forward traffic	to	virtual server	int_vip_www.mysite.com-api_1.1.1.2	-	+	
Replace	http uri	path	with value	/	-	+

Complete the additional policies according to the list above.

Once complete publish the policy.

Navigation: Local Traffic > Policies: Policy List > /Common/HTTPS_Virtual_Targeting_PolicyL7

Navigation: Click Publish

Local Traffic > Policies > Policy List Page

Policies List

<input checked="" type="checkbox"/> Name	Last Published	Description	Partition
<input checked="" type="checkbox"/> HTTPS_Virtual_Targeting_PolicyL7	Sun Jul 17 2016 17:51:08 (PDT)		Common

Now apply the policy to the external virtual server

Navigation: Local Traffic > Virtual Servers : Virtual Server List

Local Traffic » Virtual Servers : Virtual Server List								
		Virtual Server List		Virtual Address List		Statistics		
<input checked="" type="checkbox"/>		Status	Name	Description	Application	Destination	Service Port	Type
<input type="checkbox"/>	●	EXT_VIP_10.10.99.30			10.10.99.30	443 (HTTPS)	Standard	Edit...
<input type="checkbox"/>	■	afmmysql_vs			192.168.1.51	80 (HTTP)	Standard	Edit...
<input type="checkbox"/>	●	int_vip_www.mysite.com-api_1.1.1.2			1.1.1.2	80 (HTTP)	Standard	Edit...
<input type="checkbox"/>	●	int_vip_www.mysite.com-downloads_1.1.1.3			1.1.1.3	80 (HTTP)	Standard	Edit...
<input type="checkbox"/>	●	int_vip_www.mysite.com_1.1.1.1			1.1.1.1	80 (HTTP)	Standard	Edit...
<input type="checkbox"/>	●	int_vip_www.theirsite.com_2.2.2.2			2.2.2.2	80 (HTTP)	Standard	Edit...
<input type="checkbox"/>	●	int_vip_www.yoursite.com_3.3.3.3			3.3.3.3	80 (HTTP)	Standard	Edit...

[Enable](#) [Disable](#) [Delete...](#) [Create...](#)

Navigation: Click the EXT_VIP_10.10.90.30

Local Traffic » Virtual Servers : Virtual Server List								
		Virtual Server List		Virtual Address List		Statistics		
<input checked="" type="checkbox"/>		Status	Name	Description	Application	Destination	Service Port	Type
<input type="checkbox"/>	●	EXT_VIP_10.10.99.30			10.10.99.30	443 (HTTPS)	Standard	Edit...
<input type="checkbox"/>	●	int_vip_www.mysite.com-api_1.1.1.2			1.1.1.2	80 (HTTP)	Standard	Edit...
<input type="checkbox"/>	●	int_vip_www.mysite.com-downloads_1.1.1.3			1.1.1.3	80 (HTTP)	Standard	Edit...
<input type="checkbox"/>	●	int_vip_www.mysite.com_1.1.1.1			1.1.1.1	80 (HTTP)	Standard	Edit...
<input type="checkbox"/>	●	int_vip_www.theirsite.com_3.3.3.3			3.3.3.3	80 (HTTP)	Standard	Edit...
<input type="checkbox"/>	●	int_vip_www.yoursite.com_2.2.2.2			2.2.2.2	80 (HTTP)	Standard	Edit...

Navigation: Click the Resources Tab

Local Traffic » Virtual Servers : Virtual Server List » EXT_VIP_10.10.99.30								
		Properties		Resources		Security		Statistics
<input checked="" type="checkbox"/>								

Navigation: Under Policies Click Manage

Local Traffic » Virtual Servers : Virtual Server List » EXT_VIP_10.10.99.30

Properties Resources Security Statistics

Load Balancing

Default Pool	pool_www.mysite.com
Default Persistence Profile	None
Fallback Persistence Profile	None

Update

iRules

Name	Manage...
No records to display.	

Policies

Name	Manage...
No records to display.	

Navigation: Select the HTTPS_Virtual_Targeting_PolicyL7

Local Traffic » Virtual Servers : Virtual Server List » EXT_VIP_10.10.99.30

Properties Resources Security Statistics

Resource Management

Policies	Enabled	Available
		/Common HTTPS_Virtual_Targeting_PolicyL7

<< >>

Cancel Finished

Navigation: Click the Double Arrow to move the policy into the left-hand column and click Finished.

Local Traffic » Virtual Servers : Virtual Server List » EXT_VIP_10.10.99.30

Properties Resources Security Statistics

Resource Management

Policies	Enabled	Available
	/Common HTTPS_Virtual_Targeting_PolicyL7	<< >>

Cancel **Finished**

The result should look like the screenshot below.

Local Traffic » Virtual Servers : Virtual Server List » EXT_VIP_10.10.99.30

Properties Resources Security Statistics

Load Balancing

Default Pool	pool_www.mysite.com
Default Persistence Profile	None
Fallback Persistence Profile	None

Update

iRules

Name

No records to display.

Policies

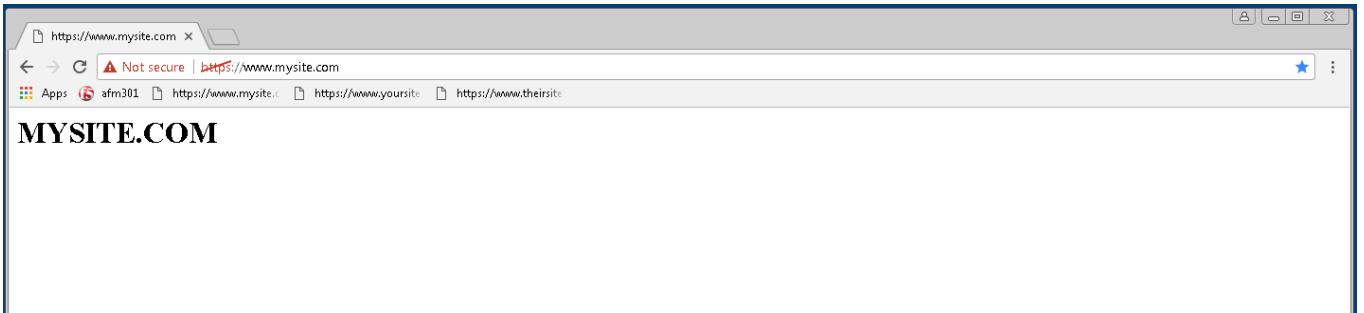
Name

/Common/HTTPS_Virtual_Targeting_PolicyL7

Validation: This lab is using self-signed certificates. You can either open a web browser on the test client or run CURL from the CLI to validate your configuration.

Note: you may have to edit the hosts file on your Win7 Client to add:

```
10.10.99.30 www.mysite.com
10.10.99.30 www.yoursite.com
10.10.99.30 www.theirsite.com
```



From a terminal window (use Cygwin on Win7 Client Desktop). Curl will let us do some of the additional testing in later sections.

```
curl -k https://10.10.99.30 -H 'Host:www.mysite.com' ``

<H1> MYSITE.COM </H1>

curl -k https://10.10.99.30 -H 'Host:www.theirsite.com'

<H1> THEIRSITE.COM </H1>

curl -k https://10.10.99.30 -H 'Host:www.yoursite.com'

<H1> YOURSITE.COM </H1>

curl -k https://10.10.99.30/api -H 'Host:www.mysite.com'
```

A bunch of nonsense JSON should be returned.

```
{
  "web-app": {
    "servlet": [
      {
        "servlet-name": "cofaxCDS",
        "servlet-class": "org.cofax.cds.CDSServlet"
      }
    ...
  }}
```

```
curl -k https://10.10.99.30/downloads/ -H 'Host:www.mysite.com'
```

A larger page with this title should be displayed.

```
<html>
<head>
  <title>Index of /downloads</title>
</head>
<body>
```

→**NOTE:** This is the end of Task 2

TASK 3 – Configure local logging

Security logging needs to be configured separately from LTM logging. In our lab, we will configure a local log publisher and log profile. The log profile will then be applied to the virtual server and tested.

On BIG-IP

Create a log publisher using the following information:

Navigation: System > Logs > Configuration > Log Publishers, then click Create

Name	firewall_log_publisher
Destinations (Selected)	local-db

System » Logs : Configuration : Log Publishers

General Properties

Name	firewall_log_publisher
Description	

Log Destinations

Destinations	<p>Selected</p> <p>/Common local-db</p> <p><< >></p> <p>Available</p> <p>/Common alertd local-syslog</p>
--------------	--

Note: Leave all other fields using the default values.

Navigation: Click Finished

Create a log profile using the following information:

Navigation: Security > Event Logs > Logging Profiles, then click Create

Name	firewall_log_profile
Protocol Security	Checked
Network Firewall	Checked

Edit log profile protocol security tab using the following information:

Navigation: Click on the Protocol Security tab

Publisher	firewall_log_publisher
-----------	------------------------

Security » Event Logs : Logging Profiles » Create New Logging Profile...

Logging Profile Properties

Profile Name	firewall_log_profile
Protocol Security	<input checked="" type="checkbox"/> Enabled
Network Firewall	<input checked="" type="checkbox"/> Enabled
DoS Protection	<input type="checkbox"/> Enabled

Protocol Security Network Firewall

HTTP, FTP, and SMTP Security

Publisher	firewall_log_publisher ▾
-----------	--------------------------

Note: Leave all other fields using the default values.

Edit log profile network firewall tab using the following information:

Navigation: Click on the Network Firewall tab

Network Firewall Publisher	firewall_log_profile
Log Rule Matches	Check Accept Check Drop Check Reject
Log IP Errors	Checked
Log TCP Errors	Checked
Log TCP Events	Checked
Log Translation Fields	Checked
Storage Format	Field-List (Move all to Selected Items)

Security > Event Logs : Logging Profiles > Create New Logging Profile...

Logging Profile Properties

Profile Name	<input type="text" value="firewall_log_profile"/>	<input type="button" value="Cancel"/>	<input type="button" value="Finished"/>
Protocol Security	<input checked="" type="checkbox"/> Enabled		
Network Firewall	<input checked="" type="checkbox"/> Enabled		
DoS Protection	<input type="checkbox"/> Enabled		

Protocol Security Network Firewall

Network Firewall

Publisher	<input type="text" value="firewall_log_publisher"/>
Aggregate Rate Limit	<input type="text" value="Indefinite"/>
Log Rule Matches	<input checked="" type="checkbox"/> Accept <input type="text" value="Rate Limit: Indefinite"/> <input checked="" type="checkbox"/> Drop <input type="text" value="Rate Limit: Indefinite"/> <input checked="" type="checkbox"/> Reject <input type="text" value="Rate Limit: Indefinite"/>
Log IP Errors	<input checked="" type="checkbox"/> Enabled <input type="text" value="Rate Limit: Indefinite"/>
Log TCP Errors	<input checked="" type="checkbox"/> Enabled <input type="text" value="Rate Limit: Indefinite"/>
Log TCP Events	<input checked="" type="checkbox"/> Enabled <input type="text" value="Rate Limit: Indefinite"/>
Log Translation Fields	<input checked="" type="checkbox"/> Enabled
Always Log Region	<input type="checkbox"/> Enabled

Storage Format

Field-List	<input type="text" value="Delimiter: ,"/>
Selected Items:	action acl_policy_name acl_policy_type acl_rule_name bigip_hostname context_name context_type date_time dest_geo dest_ip
Available Items:	<input type="text"/>
	<input type="button" value="<<"/>
	<input type="button" value=">>"/>
Up	<input type="button"/>
Down	<input type="button"/>

Note: Leave all other fields using the default values.

Navigation: Click Finished

Apply the newly created log profile to the external virtual server created in the previous task.

Navigation: Local Traffic > Virtual Servers > Virtual Server List

Navigation: Click on EXT_VIP_10.10.99.30

Navigation: Security tab > Policies

Log Profile

Local Traffic » Virtual Servers : Virtual Server List » EXT_VIP_10.10.99.30

Properties	Resources	Security	Statistics																																				
Policy Settings: Basic ▾ <table border="1"> <tr> <td>Destination</td> <td>10.10.99.30:443</td> </tr> <tr> <td>Service</td> <td>HTTPS</td> </tr> <tr> <td>Application Security Policy</td> <td>Disabled ▾</td> </tr> <tr> <td>Protocol Security</td> <td>Disabled ▾</td> </tr> <tr> <td>Network Firewall</td> <td>Enforcement: Disabled ▾ Staging: Disabled ▾</td> </tr> <tr> <td>Network Address Translation</td> <td><input type="checkbox"/> Use Device Policy <input type="checkbox"/> Use Route Domain Policy Policy <input style="width: 100px; height: 20px;" type="button" value="None"/></td> </tr> <tr> <td>Service Policy</td> <td><input style="width: 100px; height: 20px;" type="button" value="None"/></td> </tr> <tr> <td>IP Intelligence</td> <td>Disabled ▾</td> </tr> <tr> <td>DoS Protection Profile</td> <td>Disabled ▾</td> </tr> <tr> <td>Anti-Fraud Profile</td> <td>Disabled ▾</td> </tr> <tr> <td>Log Profile</td> <td> Selected: <input checked="" type="checkbox"/> /Common <input type="checkbox"/> firewall_log_profile <table border="1" style="margin-left: 20px;"> <tr><td style="text-align: center;"><<</td><td style="text-align: center;">>></td></tr> <tr><td colspan="2" style="text-align: center;">Available</td></tr> <tr><td colspan="2" style="text-align: center;">/Common</td></tr> <tr><td colspan="2" style="text-align: center;">Log all requests</td></tr> <tr><td colspan="2" style="text-align: center;">Log illegal requests</td></tr> <tr><td colspan="2" style="text-align: center;">global-network</td></tr> <tr><td colspan="2" style="text-align: center;">local-dos</td></tr> </table> </td> </tr> </table>				Destination	10.10.99.30:443	Service	HTTPS	Application Security Policy	Disabled ▾	Protocol Security	Disabled ▾	Network Firewall	Enforcement: Disabled ▾ Staging: Disabled ▾	Network Address Translation	<input type="checkbox"/> Use Device Policy <input type="checkbox"/> Use Route Domain Policy Policy <input style="width: 100px; height: 20px;" type="button" value="None"/>	Service Policy	<input style="width: 100px; height: 20px;" type="button" value="None"/>	IP Intelligence	Disabled ▾	DoS Protection Profile	Disabled ▾	Anti-Fraud Profile	Disabled ▾	Log Profile	Selected: <input checked="" type="checkbox"/> /Common <input type="checkbox"/> firewall_log_profile <table border="1" style="margin-left: 20px;"> <tr><td style="text-align: center;"><<</td><td style="text-align: center;">>></td></tr> <tr><td colspan="2" style="text-align: center;">Available</td></tr> <tr><td colspan="2" style="text-align: center;">/Common</td></tr> <tr><td colspan="2" style="text-align: center;">Log all requests</td></tr> <tr><td colspan="2" style="text-align: center;">Log illegal requests</td></tr> <tr><td colspan="2" style="text-align: center;">global-network</td></tr> <tr><td colspan="2" style="text-align: center;">local-dos</td></tr> </table>	<<	>>	Available		/Common		Log all requests		Log illegal requests		global-network		local-dos	
Destination	10.10.99.30:443																																						
Service	HTTPS																																						
Application Security Policy	Disabled ▾																																						
Protocol Security	Disabled ▾																																						
Network Firewall	Enforcement: Disabled ▾ Staging: Disabled ▾																																						
Network Address Translation	<input type="checkbox"/> Use Device Policy <input type="checkbox"/> Use Route Domain Policy Policy <input style="width: 100px; height: 20px;" type="button" value="None"/>																																						
Service Policy	<input style="width: 100px; height: 20px;" type="button" value="None"/>																																						
IP Intelligence	Disabled ▾																																						
DoS Protection Profile	Disabled ▾																																						
Anti-Fraud Profile	Disabled ▾																																						
Log Profile	Selected: <input checked="" type="checkbox"/> /Common <input type="checkbox"/> firewall_log_profile <table border="1" style="margin-left: 20px;"> <tr><td style="text-align: center;"><<</td><td style="text-align: center;">>></td></tr> <tr><td colspan="2" style="text-align: center;">Available</td></tr> <tr><td colspan="2" style="text-align: center;">/Common</td></tr> <tr><td colspan="2" style="text-align: center;">Log all requests</td></tr> <tr><td colspan="2" style="text-align: center;">Log illegal requests</td></tr> <tr><td colspan="2" style="text-align: center;">global-network</td></tr> <tr><td colspan="2" style="text-align: center;">local-dos</td></tr> </table>	<<	>>	Available		/Common		Log all requests		Log illegal requests		global-network		local-dos																									
<<	>>																																						
Available																																							
/Common																																							
Log all requests																																							
Log illegal requests																																							
global-network																																							
local-dos																																							

| | | | |
| * | Policy Type | | Source | | Destination | | |--|------|---|-------------|--|----------| | <input checked="" type="checkbox"/> | Name | <input type="button" value="Rule List"/> | Description | State | Schedule | | <input type="checkbox"/> (Default) | | Enabled | | Any | Any | | | | | | Any | Any | | | | | | Any | Any | | | | | | Action | Accept | | <input type="button" value="Delete..."/> | | <input type="button" value="Search Logs..."/> | | <input type="button" value="Reset Count"/> | | | | | |

Note: Leave all other fields using the default values.

Navigation: Click Update

View empty network firewall logs.

Navigation: Security > Event Logs > Network > Firewall

Security » Event Logs : Network : Firewall

Protocol	Network	DoS	Logging Profiles																				
<input checked="" type="checkbox"/>	<input type="button" value="Time"/>	<input type="button" value="Context"/>	<input type="button" value="Name"/>	<input type="button" value="Policy Type"/>	<input type="button" value="Policy Name"/>	<input type="button" value="Rule"/>	<input type="button" value="User"/>	<input type="button" value="Region"/>	<input type="button" value="Address"/>	<input type="button" value="Port"/>	<input type="button" value="VLAN / Tunnel"/>	<input type="button" value="Region"/>	<input type="button" value="Address"/>	<input type="button" value="Port"/>	<input type="button" value="Route Domain"/>	<input type="button" value="Protocol"/>	<input type="button" value="Action"/>	<input type="button" value="Drop Reason"/>					
Last Hour ▾ <input type="button" value="Search"/> Custom Search... <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 10%;">Source</td> <td style="width: 10%;">Destination</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td colspan="2">No records to display.</td> </tr> <tr> <td colspan="2"><input type="button" value="Create Rule..."/></td> </tr> </table>																Source	Destination	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No records to display.		<input type="button" value="Create Rule..."/>	
Source	Destination																						
<input checked="" type="checkbox"/>	<input type="checkbox"/>																						
No records to display.																							
<input type="button" value="Create Rule..."/>																							

Open a new web browser tab and access the virtual server or repeat the curl statements from the previous sections.

URL: <https://www.mysite.com>

Note: This test creates network firewall log entries.

View new network firewall log entries.

Navigation: Security > Event Logs > Network > Firewall

Source														Destination			
<input checked="" type="checkbox"/>	Time	Context	Name	Policy Type	Policy Name	Rule	User	Region	FQDN	Address	Port	VLAN / Tunnel	Region	FQDN	Address	Port	
<input type="checkbox"/>	2016-07-17 18:12:39	Virtual Server	/Common/EXT_VIP_10.10.99.30	-		No-lookup		10.10.99.222	49528	/Common/outside	No-lookup		10.10.99.30	443	1.1.1.1	80	
<input type="checkbox"/>	2016-07-17 18:09:21	Virtual Server	/Common/EXT_VIP_10.10.99.30	-		No-lookup		10.10.99.222	49478	/Common/outside	No-lookup		10.10.99.30	443	1.1.1.1	80	
<input type="checkbox"/>	2016-07-17 18:08:32	Virtual Server	/Common/EXT_VIP_10.10.99.30	-		No-lookup		10.10.99.10	56453	/Common/outside	No-lookup		10.10.99.30	443	1.1.1.2	80	
<input type="checkbox"/>	2016-07-17 18:08:32	Virtual Server	/Common/EXT_VIP_10.10.99.30	-		No-lookup		10.10.99.10	56453	/Common/outside	No-lookup		10.10.99.30	443	1.1.1.2	80	
<input type="checkbox"/>	2016-07-17 18:07:38	Virtual Server	/Common/EXT_VIP_10.10.99.30	-		No-lookup		10.10.99.222	49478	/Common/outside	No-lookup		10.10.99.30	443			

Note: This is the end of task 3.

TASK 4 – Configure a network firewall policy and rules

A network firewall policy is a collection of network firewall rules that can be applied to a virtual server. In our lab, we will create two policies, each of which includes two rules. This policy will then be applied to the appropriate virtual servers and tested.

On BIG-IP

Create Network Firewall Policy

Navigation: Security > Network Firewall > Policies, then click Create

Name

General Properties

Name	<input type="text" value="downloads_policy"/>
Description	<input type="text"/>
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>	

Note: Leave all other fields using the default values.

Navigation: Click Finished

Create an IP Drop Network Firewall Rule

Navigation: Click Add

The screenshot shows the 'Network Firewall : Policies' section with the policy name 'downloads_policy'. The 'Properties' tab is selected. Under 'General Properties', the 'Name' is set to 'downloads_policy' and 'Partition / Path' is 'Common'. There is a blank 'Description' field. Below are 'Update', 'Clone', and 'Delete' buttons. A table below lists firewall rules, with the 'Add' button highlighted.

Name	Description	State	Schedule	Address/Region	Port	VLAN / Tunnel	Address/Region	Port	Protocol	iRule	Action	Logging	Service Policy
<input checked="" type="checkbox"/> Name	Rule List	Description		Source	Destination								
No records to display.													
Remove													

Name	block_export_restricted_countries
Order	First
Protocol	Any
Source	Country/Region: AF,CN,CA
Action	Drop
Logging	Enabled

Rule Properties

Name	block_export_restricted_countries
Description	
Order	First
Type	Rule
State	Enabled
Protocol	Any
Source	Address/Region: <input type="button" value="Specify..."/> <input type="radio"/> Address <input type="radio"/> Address List <input type="radio"/> Address Range <input checked="" type="radio"/> Country/Region Canada (CA) <input type="button" value="Edit"/> <input type="button" value="Delete"/> State: <input type="button" value="Select..."/> <input type="button" value="Add"/> Afghanistan (AF) China (CN) Canada (CA)
VLAN / Tunnel:	Any
Destination	Address/Region: Any
iRule	None
Action	Drop
Logging	Enabled
Service Policy	None
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>	

Note: Leave all other fields using the default values.

Navigation: Click Finished

Name	permit_log
Order	Last
Action	Accept
Logging	Enabled

Create Permit Log Network Firewall Rule

Security » Network Firewall : Policies » downloads_policy : New Rule...

Rule Properties

Name	permit_log
Description	
Order	Last
Type	Rule
State	Enabled
Protocol	Any
Source	Address/Region: Any VLAN / Tunnel: Any
Destination	Address/Region: Any
iRule	None
Action	Accept
Logging	Enabled
Service Policy	None

Note: Leave all other fields using the default values.

Navigation: Click Finished

Security » Network Firewall : Policies » downloads_policy

Properties

General Properties

Name	downloads_policy
Partition / Path	Common
Description	

Name	Description	State	Schedule	Source		Destination		iRule	Action	Logging	Service Policy
				Address/Region	Port	VLAN / Tunnel	Address/Region				
block_export_restricted_countries	Enabled	Enabled		Afghanistan (AF) Canada (CA) China (CN)	Any	Any	Any	Any	Any	Drop	Enabled
permit_log	Enabled	Enabled		Any	Any	Any	Any	Any	Accept	Enabled	

From client machine

URL: <https://www.mysite.com/downloads/>

The screenshot shows a web browser window with the URL <https://www.mysite.com/downloads/>. The page title is "Index of /downloads". The content is a table listing files in the download directory:

	<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
	Parent Directory		-	
	THIS_IS_THE_DOWNLOAD_DIRECTORY.txt	2016-05-22 15:44	0	

Below the table, the text "Apache/2.4.10 (Ubuntu) Server at www.mysite.com Port 80" is displayed.

Note: We want to validate the site is available before and after applying the Network Firewall Policy

On BIG-IP

Apply the Network Firewall Policy to Virtual Server

Virtual Server	int_vip_www.mysite.com-downloads_1.1.1.3
Enforcement	Enabled
Policy	downloads_policy
Log Profile	firewall_log_profile

Local Traffic » Virtual Servers : Virtual Server List » Int_vip_www.mysite.com-downloads_1.1.1.3

Properties	Resources	Security	Statistics
Policy Settings: Basic			
Destination	1.1.1.3:80		
Service	HTTP		
Application Security Policy	Disabled		
Protocol Security	Disabled		
Network Firewall	Enforcement: Enabled... Policy: downloads_policy Staging: Disabled		
Network Address Translation	<input type="checkbox"/> Use Device Policy <input type="checkbox"/> Use Route Domain Policy Policy: None		
Service Policy	None		
IP Intelligence	Disabled		
DoS Protection Profile	Disabled		
Anti-Fraud Profile	Disabled		
Log Profile	Enabled... Selected <input type="checkbox"/> /Common firewall_log_profile	Available <input type="checkbox"/> /Common Log all requests <input type="checkbox"/> Log illegal requests <input type="checkbox"/> global-network <input type="checkbox"/> local-dos	<< >>
<input type="button" value="Update"/>			

Note: Leave all other fields using the default values.

Navigation: Click Update

From client machine

URL: <https://www.mysite.com/downloads/>

The screenshot shows a web browser window with the URL <https://www.mysite.com/downloads/>. The page title is "Index of /downloads". The table lists two items:

	<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
	Parent Directory		-	
	THIS_IS_THE_DOWNLOAD_DIRECTORY.txt	2016-05-22 15:44	0	

Apache/2.4.10 (Ubuntu) Server at www.mysite.com Port 80

Note: We want to ensure the On BIG-IP the site is still available

after applying the policy. We will get into testing the block later.

Now we want to create a second policy for access to the /api/ application

Create Network Firewall Policy

Navigation: Security > Network Firewall > Policies, then click Create

api_policy

The screenshot shows the "Network Firewall : Policies" screen with a "New Policy..." button highlighted. A modal dialog box is open for creating a new policy:

General Properties

Name	api_policy
Description	

Buttons at the bottom: Cancel, Repeat, Finished

Note: Leave all other fields using the default values.

Navigation: Click Finished

Create Allow TCP Port 80 From Host 172.16.99.5 Network Firewall Rule

Navigation: Click Add

Security » Network Firewall : Policies » api_policy

Properties

General Properties

Name	api_policy
Partition / Path	Common
Description	

Update Clone Delete

* Search Source Destination Reorder Add

Name Rule List Description State Schedule Address/Region Port VLAN / Tunnel Address/Region Port Protocol iRule Action Logging Service Policy

No records to display.

Remove

The screenshot shows a network firewall policy configuration interface. At the top, the path is Security » Network Firewall : Policies » api_policy. A 'Properties' tab is selected. Below it, there's a 'General Properties' section with fields for Name (api_policy), Partition / Path (Common), and Description (empty). Below this are buttons for Update, Clone, and Delete. The main area shows a table header with columns: * (empty), Search, Source, Destination, Reorder, and Add. Under Source and Destination, there are dropdown menus for Address/Region, Port, VLAN / Tunnel, and Address/Region, Port, Protocol, iRule, Action, Logging, and Service Policy. A red box highlights the 'Add' button. Below the header, a message says 'No records to display.' There is also a 'Remove' button. At the bottom, there's a table showing a single rule:

Name	allow_api_access
Order	First
Protocol	TCP (6)
Source	Address: 172.16.99.5
Action	Accept
Logging	Enabled

Security » Network Firewall : Policies » api_policy : New Rule...

Rule Properties

Name	allow_api_access	
Description	customer_hosts	
Order	First	
Type	Rule	
State	Enabled	
Protocol	TCP	6
Source	Address/Region: <input type="button" value="Specify..."/> <input checked="" type="radio"/> Address <input type="radio"/> Address List <input type="radio"/> Address Range <input type="radio"/> Country/Region 172.16.99.5 172.16.99.5 <input type="button" value="Edit"/> <input type="button" value="Delete"/> Port: Any VLAN / Tunnel: Any	
Destination	Address/Region: Any Port: Any	
iRule	None	
Action	Accept	
Logging	Enabled	
Service Policy	None	
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>		

Note: Leave all other fields using the default values.

Navigation: Click Finished

As we are deployed in “ADC Mode” where the default action on a virtual server is ‘Accept’ we must also create a default deny rule.

Name	deny_log
Order	Last
Action	Drop
Logging	Enabled

Create Deny Log Network Firewall Rule

Security » Network Firewall : Policies » api_policy : New Rule...

Rule Properties

Name	deny_log
Description	
Order	Last
Type	Rule
State	Enabled
Protocol	Any
Source	Address/Region: Any VLAN / Tunnel: Any
Destination	Address/Region: Any
iRule	None
Action	Drop
Logging	Enabled
Service Policy	None

Note: Leave all other fields using the default values.

Navigation: Click Finished

Apply the Network Firewall Policy to Virtual Server

Virtual Server	int_vip_www.mysite.com-api_1.1.1.2
Enforcement	Enabled
Policy	api_policy
Log Profile	firewall_log_profile

Local Traffic » Virtual Servers : Virtual Server List » Int_vip_www.mysite.com-api_1.1.1.2

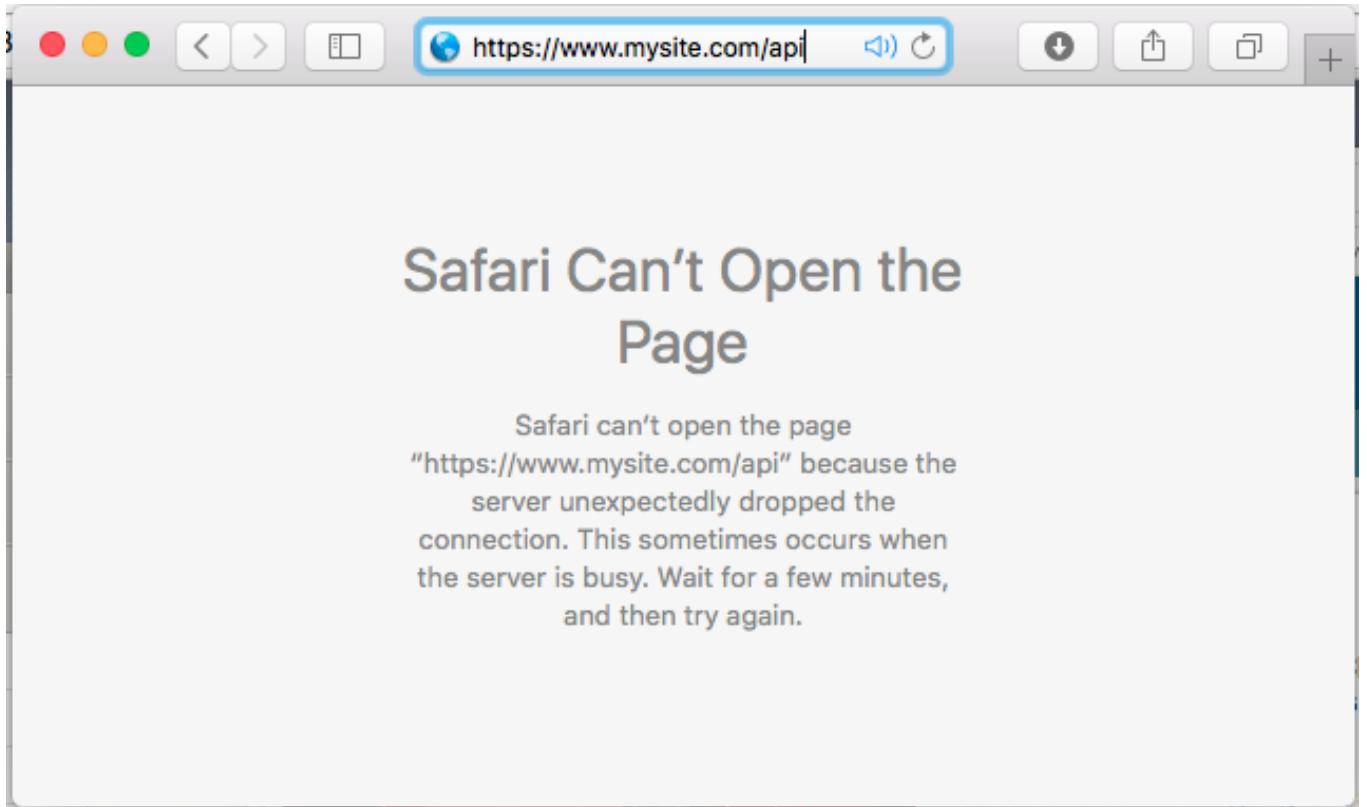
Properties	Resources	Security	Statistics
Policy Settings: Basic			
Destination	1.1.1.2:80		
Service	HTTP		
Application Security Policy	Disabled		
Protocol Security	Disabled		
Network Firewall	Enforcement: Enabled... Policy: api_policy Staging: Disabled		
Network Address Translation	<input type="checkbox"/> Use Device Policy <input type="checkbox"/> Use Route Domain Policy Policy: None		
Service Policy	None		
IP Intelligence	Disabled		
DoS Protection Profile	Disabled		
Anti-Fraud Profile	Disabled		
Log Profile	Enabled... Selected /Common firewall_log_profile Available /Common Log all requests Log illegal requests global-network local-dos << >>		
<input type="button" value="Update"/>			

Note: Leave all other fields using the default values.

Navigation: Click Update

From client machine

URL: <https://www.mysite.com/api>



Note: We can no longer access the /api site because the only allowed address is 172.16.99.5. You can verify this in the logs

Policy Name	Rule	Source					Destination					Protocol	Action	Drop Reason		
		User	Region	FQDN	Address	Port	VLAN / Tunnel	Region	FQDN	Address	Port					
No-lookup		10.10.99.1	51823	/Common/outside	No-lookup	10.10.99.30	443	0	TCP	Closed	10.10.99.1	51823	_loopback	1.1.1.2	80	TCP
/Common/api_policy	deny_log	unknown	No-lookup	No-lookup	10.10.99.1	51823	_loopback	No-lookup	No-lookup	1.1.1.2	80	0	TCP	Drop	Policy	

Note: This concludes Task 4

TASK 5 – Configure SNAT for CDN networks or other proxies

Many enterprise sites have some or all of their content served up by Content Delivery Networks (CDN). This common use case leverages proxies to provide static content closer to the end client machines. Because of this there may only be one or two IP addresses connecting to the origin website. The original IP address of the client in this case is often mapped to a common HTTP header XFF. In this deployment, the BIG-IP can translate the original source of the request in the XFF to the source IP address.

The iRule to accomplish this is already installed on your BIG-IP. We need to apply it to the External Virtual Server. Here is a sample of the iRule.

```
when HTTP_REQUEST {
    if {[HTTP::header exists "X-Forwarded-For"]} {
        snat [HTTP::header X-Forwarded-For]
        log local0. '[HTTP::header X-Forwarded-For]'
```

```
}
```

Apply the iRule to the Virtual Server

Navigation: Click on the EXT_VIP_10.10.99.30 virtual server

Local Traffic » Virtual Servers : Virtual Server List » EXT_VIP_10.10.99.30

Properties Resources Security Statistics

Load Balancing

Default Pool	pool_www.yoursite.com
Default Persistence Profile	None
Fallback Persistence Profile	None

Update

iRules

Name

No records to display.

Manage...

Policies

Name

/Common/HTTPS_Virtual_Targeting_PolicyL7

Navigation: Click Manage under the iRule section

Local Traffic » Virtual Servers : Virtual Server List » EXT_VIP_10.10.99.30

Properties Resources Security Statistics

Resource Management

iRule	<table border="1"><tr><td>Enabled</td><td>Available</td></tr><tr><td>/Common XFF-SNAT</td><td>/Common _sys_APM_ExchangeSupport_OA_BasicAuth _sys_APM_ExchangeSupport_OA_NtlmAuth _sys_APM_ExchangeSupport_helper _sys_APM_ExchangeSupport_main</td></tr></table>	Enabled	Available	/Common XFF-SNAT	/Common _sys_APM_ExchangeSupport_OA_BasicAuth _sys_APM_ExchangeSupport_OA_NtlmAuth _sys_APM_ExchangeSupport_helper _sys_APM_ExchangeSupport_main
Enabled	Available				
/Common XFF-SNAT	/Common _sys_APM_ExchangeSupport_OA_BasicAuth _sys_APM_ExchangeSupport_OA_NtlmAuth _sys_APM_ExchangeSupport_helper _sys_APM_ExchangeSupport_main				

<< >>

Up Down

Cancel Finished

Navigation: Once you have moved the iRule XFF-SNAT over to the Enabled Section, Click Finished

To test functionality, we will need to leverage curl from the CLI to insert the X-Forwarded-For header.

```
curl -k https://10.10.99.30/downloads/ -H 'Host: www.mysite.com'
```

Expected Result:

```
<html>
<head>
<title>Index of /downloads</title>
</head>
<body>
```

Validate that IP addresses sourced from China are blocked:

```
curl -k https://10.10.99.30/downloads/ -H 'Host: www.mysite.com' -H
'X-Forwarded-For: 1.202.2.1'
```

Expected Result: The site should now be blocked

Validate that requests sourced from the X-Forwarded-For IP address of 172.16.99.5 are now allowed.

```
curl -k https://10.10.99.30/api -H 'Host:www.mysite.com' -H 'X-Forwarded-For:
172.16.99.5'
```

Expected Result:

```
{
    "web-app": {
        "servlet": [
            {
                "servlet-name": "cofaxCDS",
                "servlet-class": "org.cofax.cds.CDSServlet"
            }
        ...
    }}
```

The next step is to solve for the TCP connection issue with CDN providers. This is accomplished via AFM iRules. The iRule is already provided for you. We need to apply it to the Network Firewall downloads_policy Policy.

Security » Network Firewall : Policies » downloads_policy : block_export_restricted_countries

Properties	
Name	block_export_restricted_countries
Partition / Path	Common
Description	
Type	Rule
State	Enabled
Protocol	Any
Source	Address/Region: <input type="button" value="Specify..."/> <input checked="" type="radio"/> Address <input type="radio"/> Address List <input type="radio"/> Address Range <input type="radio"/> Country/Region <input type="text"/> Afghanistan (AF) Canada (CA) China (CN) <input type="button" value="Edit"/> <input type="button" value="Delete"/> VLAN / Tunnel: Any
Destination	Address/Region: Any
iRule	AFM_403_Downloads
iRule Sampling	Disabled
Action	Drop
Logging	Enabled
Service Policy	None
<input type="button" value="Update"/> <input type="button" value="Delete"/>	

Navigation: iRule select the AFM_403_Downloads

Validate that denied requests are now responded with a Layer 7 403 Error.

```
curl -k https://10.10.99.30/downloads -H 'Host: www.mysite.com' -H 'X-Forwarded-For: 1.202.2.1'
```

Expected Result: Instead of the traffic getting dropped, a 403 error should be returned.

```
<html>
<head>
<title>403 Forbidden</title>
</head>
```

```

<body>
403 Forbidden Download of Cryptographic Software Is Restricted
</body>
</html>

```

TASK 6 – Configure HTTP security

HTTP security profiles are used to apply basic HTTP security to a virtual server. Significantly more advanced HTTP security is available by adding ASM (Application Security Manager).

On BIG-IP

Configure a HTTP security profile.

Navigation: Security > Protocol Security > Security Profiles > HTTP, then click Create.

Profile Name	demo_http_security
Custom	Checked
Profile is case sensitive	Checked
HTTP Protocol Checks	Check All

Security » Protocol Security : Security Profiles : HTTP » New HTTP Security Profile...

Profile Properties		Custom <input type="checkbox"/>																																
Profile Name	demo_http_security																																	
Partition / Path	Common																																	
Parent Profile	http_security ▾																																	
Profile Description																																		
Profile is case sensitive	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/>																																
<input type="radio"/> HTTP Protocol Checks <input type="radio"/> Request Checks <input type="radio"/> Blocking Page																																		
<table border="1"> <tr> <td><input checked="" type="checkbox"/> Header name with no header value</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input checked="" type="checkbox"/> Several Content-Length headers</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input checked="" type="checkbox"/> Chunked request with Content-Length header</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input checked="" type="checkbox"/> Null in request headers</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input checked="" type="checkbox"/> Null in request body</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input checked="" type="checkbox"/> POST request with Content-Length: 0</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input checked="" type="checkbox"/> Body in GET or HEAD requests</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input checked="" type="checkbox"/> Content length should be a positive number</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input checked="" type="checkbox"/> Bad HTTP version</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input checked="" type="checkbox"/> High ASCII characters in headers</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input checked="" type="checkbox"/> Host header contains IP address</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input checked="" type="checkbox"/> Unparseable request content</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input checked="" type="checkbox"/> Bad host header value</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input checked="" type="checkbox"/> Check maximum number of headers <input type="text" value="20"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td colspan="2"> <input checked="" type="checkbox"/> Alarm <input type="checkbox"/> Block </td> </tr> <tr> <td colspan="2"> <input checked="" type="checkbox"/> Alarm <input type="checkbox"/> Block </td> </tr> </table>			<input checked="" type="checkbox"/> Header name with no header value	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Several Content-Length headers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Chunked request with Content-Length header	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Null in request headers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Null in request body	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> POST request with Content-Length: 0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Body in GET or HEAD requests	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Content length should be a positive number	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Bad HTTP version	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> High ASCII characters in headers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Host header contains IP address	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Unparseable request content	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Bad host header value	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Check maximum number of headers <input type="text" value="20"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Alarm <input type="checkbox"/> Block		<input checked="" type="checkbox"/> Alarm <input type="checkbox"/> Block	
<input checked="" type="checkbox"/> Header name with no header value	<input checked="" type="checkbox"/>																																	
<input checked="" type="checkbox"/> Several Content-Length headers	<input checked="" type="checkbox"/>																																	
<input checked="" type="checkbox"/> Chunked request with Content-Length header	<input checked="" type="checkbox"/>																																	
<input checked="" type="checkbox"/> Null in request headers	<input checked="" type="checkbox"/>																																	
<input checked="" type="checkbox"/> Null in request body	<input checked="" type="checkbox"/>																																	
<input checked="" type="checkbox"/> POST request with Content-Length: 0	<input checked="" type="checkbox"/>																																	
<input checked="" type="checkbox"/> Body in GET or HEAD requests	<input checked="" type="checkbox"/>																																	
<input checked="" type="checkbox"/> Content length should be a positive number	<input checked="" type="checkbox"/>																																	
<input checked="" type="checkbox"/> Bad HTTP version	<input checked="" type="checkbox"/>																																	
<input checked="" type="checkbox"/> High ASCII characters in headers	<input checked="" type="checkbox"/>																																	
<input checked="" type="checkbox"/> Host header contains IP address	<input checked="" type="checkbox"/>																																	
<input checked="" type="checkbox"/> Unparseable request content	<input checked="" type="checkbox"/>																																	
<input checked="" type="checkbox"/> Bad host header value	<input checked="" type="checkbox"/>																																	
<input checked="" type="checkbox"/> Check maximum number of headers <input type="text" value="20"/>	<input checked="" type="checkbox"/>																																	
<input checked="" type="checkbox"/> Alarm <input type="checkbox"/> Block																																		
<input checked="" type="checkbox"/> Alarm <input type="checkbox"/> Block																																		

Cancel Create

Note: Leave all other fields using the default values.

Navigation: Click Request Checks Tab.

File Types | **Select All**

Security » Protocol Security : Security Profiles : HTTP » New HTTP Security Profile...

Profile Properties

Profile Name	demo_http_security	Custom <input type="checkbox"/>
Partition / Path	Common	
Parent Profile	http_security	
Profile Description		
Profile is case sensitive	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/>	

HTTP Protocol Checks **Request Checks** **Blocking Page** Custom

Length Checks	URL length	<input type="radio"/> Any <input checked="" type="radio"/> Length: 1024 bytes <input checked="" type="checkbox"/>
	Query String length	<input type="radio"/> Any <input checked="" type="radio"/> Length: 1024 bytes <input checked="" type="checkbox"/>
	Request length	<input type="radio"/> Any <input checked="" type="radio"/> Length: 0 bytes <input checked="" type="checkbox"/>
	POST data length	<input type="radio"/> Any <input checked="" type="radio"/> Length: 0 bytes <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Alarm <input type="checkbox"/> Block		
Methods	Allowed:	Available:
	GET HEAD POST	ACL BCOPY BDELETE BMOVE BPROPFIND
	Method <input type="button" value="Add"/>	<input type="checkbox"/> Alarm <input type="checkbox"/> Block
	<input type="checkbox"/> Define Disallowed <input type="checkbox"/>	
File Types	Selected:	Available:
	asp aspx bmp cgi css	
	File Type <input type="button" value="Add"/>	<input type="checkbox"/> Alarm <input type="checkbox"/> Block
	<input type="checkbox"/> Selected <input type="checkbox"/> Available	
Mandatory Headers	Mandatory:	Available:
		authorization cookie referer
	Mandatory Header <input type="button" value="Add"/>	<input type="checkbox"/> Alarm <input type="checkbox"/> Block
	<input type="checkbox"/> Mandatory <input type="checkbox"/> Available	

Create **Cancel**

The screenshot shows the 'Request Checks' tab of the 'New HTTP Security Profile' dialog. The 'File Types' section is highlighted with a red box. It contains two lists: 'Selected' (containing 'asp', 'aspx', 'bmp', 'cgi', 'css') and 'Available' (empty). Below these lists is a 'File Type' input field and an 'Add' button. To the right of the lists are checkboxes for 'Alarm' and 'Block'.

Note: Leave all other fields using the default values.

Navigation: Click Blocking Page Tab.

Response Type	Custom Response
Response Body	Insert "Please contact the helpdesk at x1234" as noted below

Security » Protocol Security : Security Profiles : HTTP » HTTP Profile Properties

HTTP Profile Properties

Profile Name	demo_http_security
Partition / Path	Common
Parent Profile	http_security ▾
Profile Description	
Profile is case sensitive	Yes

HTTP Protocol Checks Request Checks **Blocking Page** Custom

Response Type	Custom Response ▾	<input checked="" type="checkbox"/>
HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Connection: close		
Response Headers	Paste Default Response Header	
Response Body	<p>Upload File: <input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload"/></p> <pre><html><head><title>Request Rejected</title></head><body>The requested URL was rejected. Please contact the helpdesk at x1234.

Your support ID is: <%TS.request.ID()%></body></html></pre> <p>Paste Default Response Body <input type="button" value="Show..."/></p>	

Note: Leave all other fields using the default values.

Navigation: Click Finished

Apply HTTP security profile to virtual server.

Navigation: Local Traffic > Virtual Servers > Virtual Server List > EXT_VIP_10.10.99.30

Protocol Security	Enabled demo_http_security
--------------------------	-------------------------------

Local Traffic » Virtual Servers : Virtual Server List » EXT_VIP_10.10.99.30

	Properties	Resources	Security	Statistics
--	------------	-----------	----------	------------

Policy Settings: Basic

Destination	10.10.99.30:443														
Service	HTTPS														
Application Security Policy	Disabled														
Protocol Security	Enabled... Profile: demo_http_security														
Network Firewall	Enforcement: Disabled Staging: Disabled														
Network Address Translation	<input type="checkbox"/> Use Device Policy <input type="checkbox"/> Use Route Domain Policy Policy: None														
Service Policy	None														
IP Intelligence	Disabled														
DoS Protection Profile	Disabled														
Anti-Fraud Profile	Disabled														
Log Profile	<table border="1"><tr><td style="text-align: center;">Selected</td><td style="text-align: center;">Available</td></tr><tr><td>/Common firewall_log_profile</td><td><input type="button" value="<<"/> <input type="button" value=">>"/></td></tr><tr><td colspan="2"><table border="1"><tr><td style="text-align: center;">/Common</td><td style="text-align: center;">Log all requests</td></tr><tr><td style="text-align: center;">firewall_log_profile</td><td style="text-align: center;">Log illegal requests</td></tr><tr><td colspan="2" style="text-align: center;">global-network</td></tr><tr><td colspan="2" style="text-align: center;">local-dos</td></tr></table></td></tr></table>	Selected	Available	/Common firewall_log_profile	<input type="button" value="<<"/> <input type="button" value=">>"/>	<table border="1"><tr><td style="text-align: center;">/Common</td><td style="text-align: center;">Log all requests</td></tr><tr><td style="text-align: center;">firewall_log_profile</td><td style="text-align: center;">Log illegal requests</td></tr><tr><td colspan="2" style="text-align: center;">global-network</td></tr><tr><td colspan="2" style="text-align: center;">local-dos</td></tr></table>		/Common	Log all requests	firewall_log_profile	Log illegal requests	global-network		local-dos	
Selected	Available														
/Common firewall_log_profile	<input type="button" value="<<"/> <input type="button" value=">>"/>														
<table border="1"><tr><td style="text-align: center;">/Common</td><td style="text-align: center;">Log all requests</td></tr><tr><td style="text-align: center;">firewall_log_profile</td><td style="text-align: center;">Log illegal requests</td></tr><tr><td colspan="2" style="text-align: center;">global-network</td></tr><tr><td colspan="2" style="text-align: center;">local-dos</td></tr></table>		/Common	Log all requests	firewall_log_profile	Log illegal requests	global-network		local-dos							
/Common	Log all requests														
firewall_log_profile	Log illegal requests														
global-network															
local-dos															

Note: Leave all other fields using the default values.

Navigation: Click Update.

Open a new web browser tab, access the virtual server and log into the application.

URL: <https://www.mysite.com/dvwa>

Credentials: admin/password



Note: This application is accessible, even though there are policy violations, because the “Block” option in the HTTP security policy is not selected.

Browse the application.

Navigation: Click on various links on the sidebar.

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.8

Note: This traffic will generate network firewall log entries because the “Alarm” option in the HTTP security policy is selected.

On BIG-IP

Review the log entries created in the previous step.

Navigation: Security > Event Logs > Protocol > HTTP

Security » Event Logs : Protocol : HTTP																						
Protocol		Network		DoS		Logging Profiles																
Time		Source		Destination		Address		Port		Route Domain		Description		Support ID		Violation		Protocol		Request URI		Action
2015-07-11 16:37:44	/Common/demo_http_vs	/Common/demo_http_security	192.168.1.10	49679	NA	192.168.1.50	80	0				Host header contains IP address	315007152190128139	HTTP protocol compliance failed	HTTP	/idwva/vulnerabilities/sql_inj/	ALARM					
2015-07-11 16:37:43	/Common/demo_http_vs	/Common/demo_http_security	192.168.1.10	49678	NA	192.168.1.50	80	0				Host header contains IP address	315007152190128136	HTTP protocol compliance failed	HTTP	/idwva/vulnerabilities/sql_inj/	ALARM					
2015-07-11 16:37:43	/Common/demo_http_vs	/Common/demo_http_security	192.168.1.10	49677	NA	192.168.1.50	80	0				Host header contains IP address	315007152190128137	HTTP protocol compliance failed	HTTP	/idwva/vulnerabilities/captcha/	ALARM					
2015-07-11 16:37:42	/Common/demo_http_vs	/Common/demo_http_security	192.168.1.10	49674	NA	192.168.1.50	80	0				Host header contains IP address	315007152190128134	HTTP protocol compliance failed	HTTP	/idwva/vulnerabilities/srf/	ALARM					
2015-07-11 16:37:42	/Common/demo_http_vs	/Common/demo_http_security	192.168.1.10	49671	NA	192.168.1.50	80	0				Host header contains IP address	315007152190128135	HTTP protocol compliance failed	HTTP	/idwva/vulnerabilities/srf/	ALARM					
2015-07-11 16:37:41	/Common/demo_http_vs	/Common/demo_http_security	192.168.1.10	49670	NA	192.168.1.50	80	0				Host header contains IP address	315007152190128133	HTTP protocol compliance failed	HTTP	/idwva/vulnerabilities/exec/	ALARM					
2015-07-11 16:37:41	/Common/demo_http_vs	/Common/demo_http_security	192.168.1.10	49669	NA	192.168.1.50	80	0				Host header contains IP address	315007152190128133	HTTP protocol compliance failed	HTTP	/idwva/vulnerabilities/brute/	ALARM					
2015-07-11 16:37:40	/Common/demo_http_vs	/Common/demo_http_security	192.168.1.10	49668	NA	192.168.1.50	80	0				NA	315007152190128134	Illegal file type	HTTP	/idwva/setup.php	ALARM					
2015-07-11 16:37:40	/Common/demo_http_vs	/Common/demo_http_security	192.168.1.10	49667	NA	192.168.1.50	80	0				Host header contains IP address	315007152190128131	HTTP protocol compliance failed	HTTP	/idwva/	ALARM					
2015-07-11 16:37:40	/Common/demo_http_vs	/Common/demo_http_security	192.168.1.10	49668	NA	192.168.1.50	80	0				Host header contains IP address	315007152190128130	HTTP protocol compliance failed	HTTP	/idwva/setup.php	ALARM					

Note: Your log entries may be different than the example shown above.

Edit the demo_http_security HTTP security profile.

Navigation: Security > Protocol Security > Security Profiles > HTTP

HTTP Protocol Checks	Uncheck all except “Host header contains IP address”. Check “Block”
-----------------------------	--

Security » Protocol Security : Security Profiles : HTTP » HTTP Profile Properties

Profile Properties

Profile Name	demo_http_security
Partition / Path	Common
Parent Profile	http_security
Profile Description	
Profile is case sensitive	Yes

HTTP Protocol Checks **Request Checks** **Blocking Page** **Custom**

<input type="checkbox"/> Header name with no header value	<input checked="" type="checkbox"/>
<input type="checkbox"/> Several Content-Length headers	<input checked="" type="checkbox"/>
<input type="checkbox"/> Chunked request with Content-Length header	<input checked="" type="checkbox"/>
<input type="checkbox"/> Null in request headers	<input checked="" type="checkbox"/>
<input type="checkbox"/> Null in request body	<input checked="" type="checkbox"/>
<input type="checkbox"/> POST request with Content-Length: 0	<input checked="" type="checkbox"/>
<input type="checkbox"/> Body in GET or HEAD requests	<input checked="" type="checkbox"/>
<input type="checkbox"/> Content length should be a positive number	<input checked="" type="checkbox"/>
<input type="checkbox"/> Bad HTTP version	<input checked="" type="checkbox"/>
<input type="checkbox"/> High ASCII characters in headers	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Host header contains IP address	<input checked="" type="checkbox"/>
<input type="checkbox"/> Unparseable request content	<input checked="" type="checkbox"/>
<input type="checkbox"/> Bad host header value	<input checked="" type="checkbox"/>
<input type="checkbox"/> Check maximum number of headers <input type="text" value="0"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Alarm	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Block	<input checked="" type="checkbox"/>

Evasion Techniques Checks

<input checked="" type="checkbox"/> Alarm	<input checked="" type="checkbox"/>
<input type="checkbox"/> Block	<input checked="" type="checkbox"/>

Cancel **Finished**

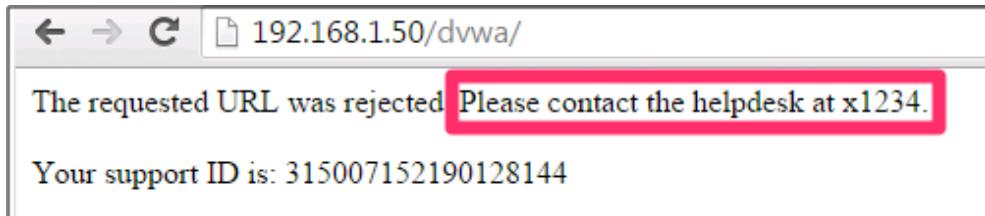
Note: Leave all other fields using the default values.

Navigation: Click Finished.

On Windows jumpbox

Open a new web browser tab and access the virtual server.

URL: <https://10.10.99.30/dvwa>



Note: This application is not accessible because the "Host header contains IP address" and "Block" options in the HTTP security policy are selected.

Open a new web browser tab and access the virtual server.

URL: <https://www.mysite.com/dvwa>



Note: This application is accessible because we requested a FQDN instead of an IP address.

Note: Do not log into DVWA at this time.

Note: This is the end of task 6.

TASK 7 – Configure Clone Pool for SSL Visibility to IDS Sensors

Since the BIG-IP is terminating SSL on the external virtual server, when we forward the traffic to the secondary virtual server in clear-text we have an opportunity to make an unencrypted copy of the application traffic and send it to an external sensor such as an IDS for further security assessment.

On BIG-IP

Configure a new Pool.

Navigation: Local Traffic > Pools > Pool List > Click Create.

Name	Health Monitor	Members	Service Port
IDS_Pool	gateway_icmp	172.1.1.11	*

DNS » Delivery : Profiles : DNS » New DNS Profile...

General Properties

Name	demo_dns_profile
Parent Profile	dns

Denial of Service Protection

Rapid Response Mode	Disabled	Custom <input checked="" type="checkbox"/>
Rapid Response Last Action	Drop	<input checked="" type="checkbox"/>

Hardware Acceleration

Protocol Validation	Disabled	<input checked="" type="checkbox"/>
Response Cache	Disabled	<input checked="" type="checkbox"/>

DNS Features

DNSSEC	Enabled	<input checked="" type="checkbox"/>
GSLB	Enabled	<input checked="" type="checkbox"/>
DNS Express	Enabled	<input checked="" type="checkbox"/>
DNS Cache	Disabled	<input checked="" type="checkbox"/>
DNS Cache Name	Select...	<input checked="" type="checkbox"/>
DNS IPv6 to IPv4	Disabled	<input checked="" type="checkbox"/>
Unhandled Query Actions	Allow	<input checked="" type="checkbox"/>
Use BIND Server on BIG-IP	Enabled	<input checked="" type="checkbox"/>

DNS Traffic

Zone Transfer	Disabled	<input checked="" type="checkbox"/>
DNS Security	Disabled	<input checked="" type="checkbox"/>
DNS Security Profile Name	Select...	<input checked="" type="checkbox"/>
Process Recursion Desired	Enabled	<input checked="" type="checkbox"/>

Logging and Reporting

Logging	Disabled	<input checked="" type="checkbox"/>
Logging Profile	Select...	<input checked="" type="checkbox"/>
AVR Statistics Sample Rate	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Buttons: Cancel | Repeat | Finished

Note: Leave all other fields using the default values.

Navigation: Click Finished.

Attach the *IDS_Pool* as a clone pool to the server side of the external virtual server

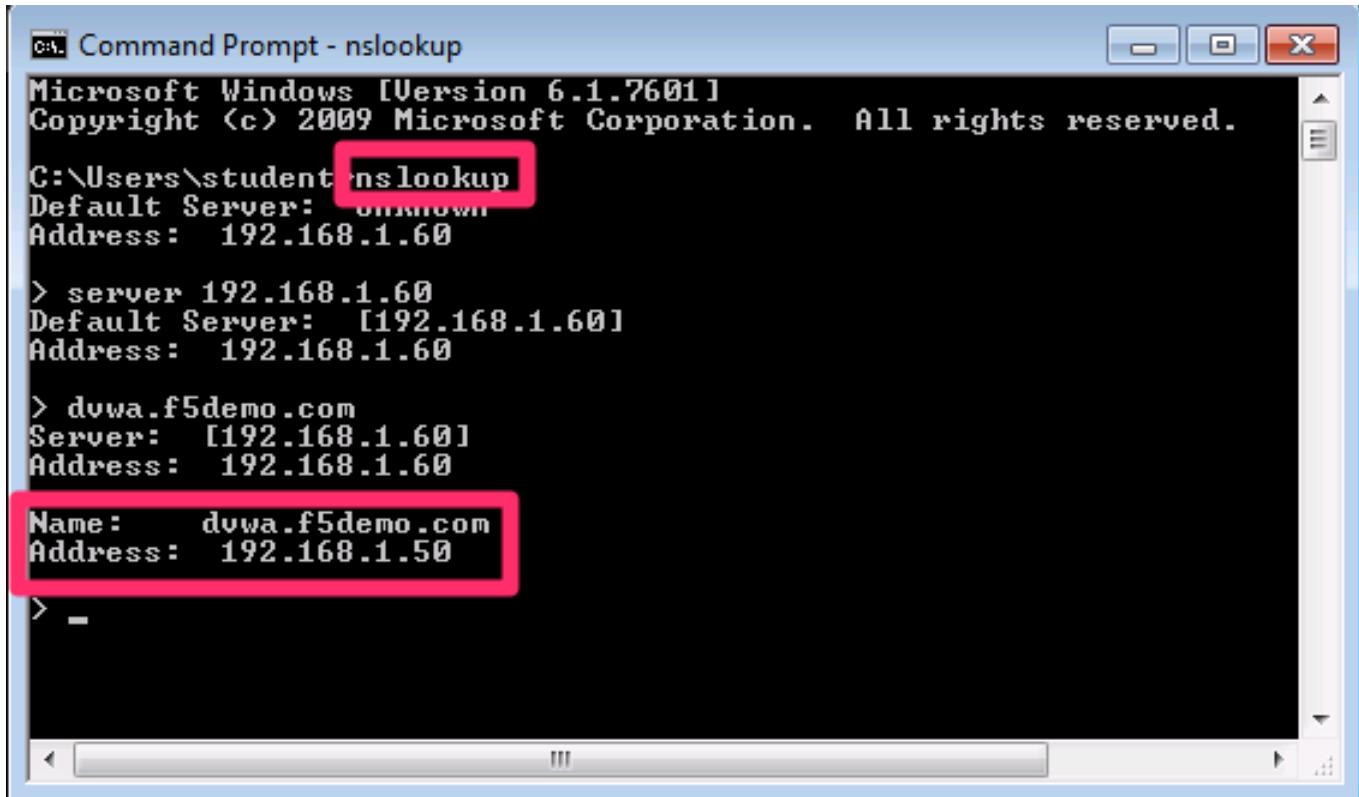
Navigation: Local Traffic > Virtual Servers > Virtual Server List > EXT_VIP_10.10.99.30.

Navigation: Configuration > Advanced.

DNS » Delivery : Listeners : Listener List » New...

General					
Name	demo_dns_listener				
Description					
State	Enabled ▾				
Listener: Basic ▾					
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.10.99.30				
VLAN Traffic	All VLANs ▾				
Service: Basic ▾					
Protocol	UDP ▾				
DNS Profile	demo_dns_profile ▾				
Load Balancing					
Default Pool	None ▾				
Default Persistence Profile	None ▾				
Fallback Persistence Profile	None ▾				
iRules					
Statistics Profile	None ▾				
iRules	<table border="1"> <thead> <tr> <th>Selected</th> <th>Available</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>/Common _sys_APM_ExchangeSupport_OA_BasicAuth _sys_APM_ExchangeSupport_OA_NtlmAuth _sys_APM_ExchangeSupport_helper _sys_APM_ExchangeSupport_main</td> </tr> </tbody> </table> <input type="button" value="<<"/> <input type="button" value=">>"/> <input type="button" value="Up"/> <input type="button" value="Down"/>	Selected	Available	<input type="checkbox"/>	/Common _sys_APM_ExchangeSupport_OA_BasicAuth _sys_APM_ExchangeSupport_OA_NtlmAuth _sys_APM_ExchangeSupport_helper _sys_APM_ExchangeSupport_main
Selected	Available				
<input type="checkbox"/>	/Common _sys_APM_ExchangeSupport_OA_BasicAuth _sys_APM_ExchangeSupport_OA_NtlmAuth _sys_APM_ExchangeSupport_helper _sys_APM_ExchangeSupport_main				
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>					

Navigation: Scroll to the configuration for Clone Pools and select the IDS_Pool



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\student>nslookup
Default Server: unknown
Address: 192.168.1.60

> server 192.168.1.60
Default Server: [192.168.1.60]
Address: 192.168.1.60

> dvwa.f5demo.com
Server: [192.168.1.60]
Address: 192.168.1.60

Name: dvwa.f5demo.com
Address: 192.168.1.50

> -
```

Navigation: Click on update at the bottom of the page.

→**NOTE:** Leave all other fields using the default values.

Navigation: SSH in to the Syslog/Webserver or open the console

Run `tcpdump -i eth2 port 80`

```
root@syslogWebserver:~# tcpdump -i eth2 port 80
```

Initiate another attempt to connect to the website via curl or your web browser on the Windows host.

```
curl -k https://10.10.99.30 -H 'Host:www.mysite.com'
```

```
<H1> MYSITE.COM </H1>
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth2, link-type
EN10MB (Ethernet), capture size 262144 bytes
17:25:42.585675 IP 10.10.99.222.50924 > 1.1.1.1.http:
Flags [S], seq 912073522, win 4380, options [mss 1460,sackOK,eol], length 0
17:25:42.585905 IP 1.1.1.1.http > 10.10.99.222.50924: Flags [S.], seq 1263282834, ack 912073523, win 4380, options [mss 1460,sackOK,eol], length 0
17:25:42.585918 IP 10.10.99.222.50924 > 1.1.1.1.http: Flags [.], ack 1, win 4380, length 0
17:25:42.585926 IP 10.10.99.222.50924 > 1.1.1.1.http: Flags [P.], seq 1:79, ack 1, win 4380, length 78
17:25:42.586750 IP 1.1.1.1.http > 10.10.99.222.50924: Flags [.], ack 79, win 4458, length 0
17:25:42.673178 IP 1.1.1.1.http > 10.10.99.222.50924: Flags [P.], seq 1:252, ack 79, win 4458, length 251
17:25:42.673231 IP 10.10.99.222.50924 > 1.1.1.1.http: Flags [.], ack 252, win 4631, length 0
17:25:42.676360 IP 10.10.99.222.50924 > 1.1.1.1.http: Flags [F.], seq 79, ack 252, win 4631,
```

```
length 0 17:25:42.676972 IP 1.1.1.1.http > 10.10.99.222.50924: Flags [.], ack 80, win 4458, length 0  
17:25:42.688028 IP 1.1.1.1.http > 10.10.99.222.50924: Flags [F.], seq 252, ack 80, win 4458, length 0
```

Note: A copy of the web traffic destined for the internal virtual

server is received by the monitoring device on 172.1.1.11. Alternatively you could attach the clone pool to the client side of the internal virtual server to see traffic destined for a single site.

Note: This is the end of task 7.

1.1.2 Lab 2: APM SSL VPN Multi-tenancy using Route Domains and AFM Policies

Estimated completion time: 45 minutes

TASK 1 – Create APM connectivity profile

These steps guide you through configuring the APM VPN and policy

A connectivity profile is needed in order to establish a layer3 tunnel. The name of the connectivity profile will be the name of the tunnel interface where packets bound for the internal network(s) the vpn is protecting will exit. Tcpdump can be used to see if packets making to and from the tunnel

For example, in this exercise `afm_cp` is the name of the connectivity profile therefore the tcpdump syntax would look like

```
tcpdump -ni afm_cp
```

The screenshot shows a web-based management interface for a connectivity profile. At the top, there's a navigation bar with 'System > Archives > afmapmbase.ucs'. Below that is a section titled 'General Properties' containing the following table:

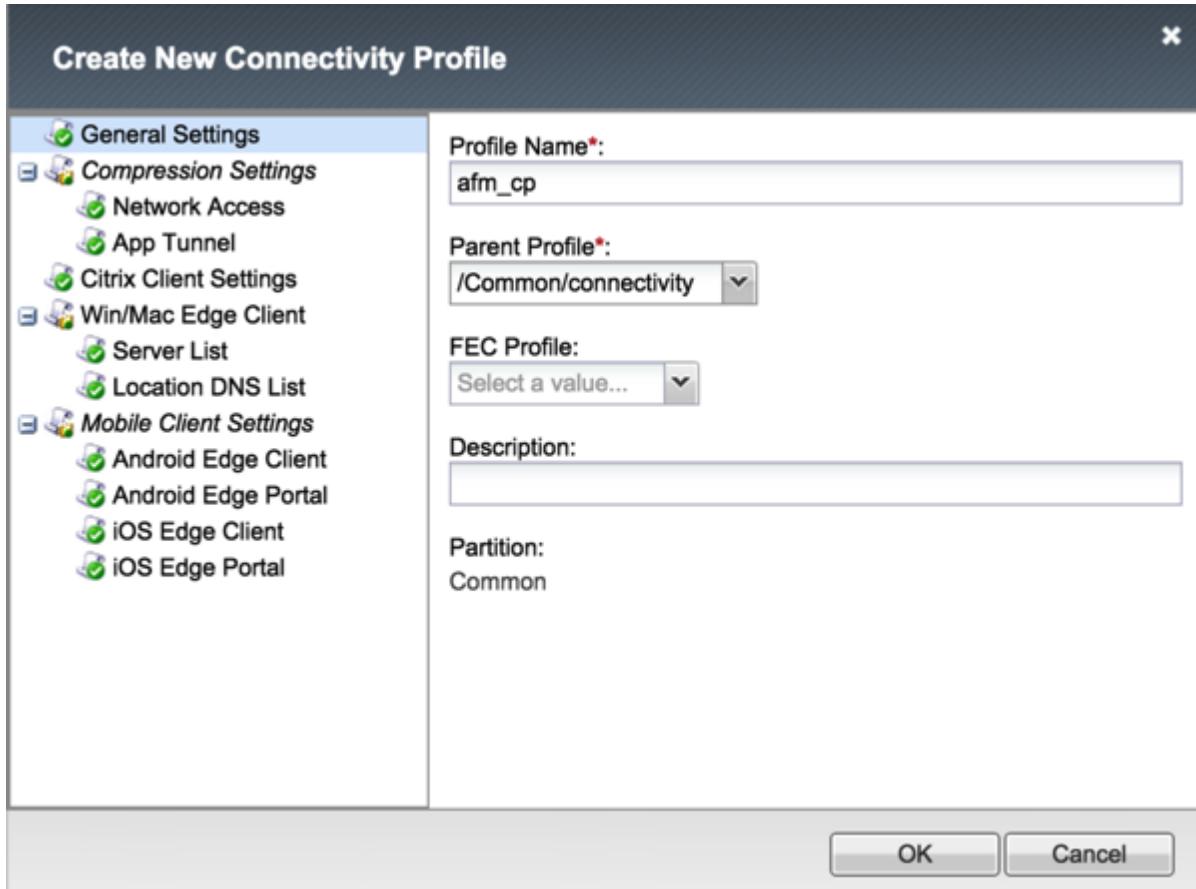
File Name	afmapmbase.ucs
Version	BIG-IP 11.6.0 Build 4.0.420
Encrypted	No
Date	Tue Jul 7 13:25:38 EDT 2015
Size	205888 Kilobytes
Archive File	Download: afmapmbase.ucs

At the bottom of the interface are two buttons: 'Restore' and 'Delete'.

Create a APM connectivity profile

Open the Access > Connectivity/VPN > Profiles, click Add. Use the following values, leave all others at their defaults

- Name: afm_cp
- Parent Profile: /Common/connectivity
- Click **Ok**



TASK 2 – Create APM access profile

Create a APM webtop

Open the Access > Webtops -> page, click Create. Use the following values, leave all others at their defaults

- Name: afm_webtop
- Type: Full
- Click **Finished**

Access Policy » Webtops » New Webtop...

General Properties

Name	afm_webtop	<input type="button" value="x"/>
Type	Full	<input type="button" value="▼"/>

Configuration

Minimize To Tray	<input checked="" type="checkbox"/> Enabled
Show a warning message when the webtop window close	<input checked="" type="checkbox"/> Enabled
Show URL Entry Field	<input checked="" type="checkbox"/> Enabled
Show Resource Search	<input checked="" type="checkbox"/> Enabled

Fallback Section

Initial State	Expanded	<input type="button" value="▼"/>
---------------	----------	----------------------------------

Create a APM lease pool for route domain 0

Open the Access > Connectivity/VPN > Network Access (VPN) > IPV4 Lease Pools page, click Create. Use the following values, leave all others at their defaults

- Name: rd0_leasepool
- Type: IP Address
- IP Address: 172.1.1.50
- Click **Add**
- Click **Finished**

Access Policy » Network Access : Lease Pools : IPV4 Lease Pools » New IPV4 Lease Pool...

General Properties

Name	rd0_leasepool
------	---------------

Configuration

Member List	Type: <input checked="" type="radio"/> IP Address <input type="radio"/> IP Address Range
	IP Address: 172.1.1.50
Add	
172.1.1.50	
Edit Delete	

Buttons: Cancel Repeat Finished

Create a APM connectivity profile for route domain 1

Open the Access > Connectivity/VPN > Network Access (VPN) > IPV4 Lease Pools page, click Create. Use the following values, leave all others at their defaults

- Name: rd1_leasepool
- Type: IP Address
- IP Address: 172.1.2.50
- Click **Add**
- Click **Finished**

Access Policy » Network Access : Lease Pools : IPV4 Lease Pools » New IPV4 Lease Pool...

General Properties	
Name	rd1_leasepool
Configuration	
Member List	Type: <input checked="" type="radio"/> IP Address <input type="radio"/> IP Address Range IP Address: 172.1.2.50 <input type="button" value="x"/> <input type="button" value="Add"/> <div style="border: 1px solid black; padding: 5px; display: inline-block;">172.1.2.50</div> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>	

Create a APM network access configuration for route domain 0

Open the Access > Connectivity/VPN > Network Access Lists page, click Create. Use the following values, leave all others at their defaults

- Name: rd0_networkaccess
- Click **Finished**

Access Policy » Network Access : Network Access List » New Resource...

General Properties	
Name	rd0_networkaccess
Description	<input type="text"/>
Auto launch	<input type="checkbox"/> Enable
Customization Settings for English	
Language	English
Caption	<input type="text"/>
Detailed Description	<input type="text"/>
Image	<input type="button" value="Choose File"/> No file chosen <input type="button" value="View/Hide"/>
<input type="button" value="Cancel"/> <input type="button" value="Finished"/>	

Open the rd0_networkaccess you just created and go to Network Settings. Use the following values,

leave all others at their defaults

- IPV4 Lease Pool: rd0_leasepool
- Traffic Options: Use split tunneling for traffic
- IPV4 LAN Address Space: - IP Address: 172.1.1.0 - Mask: 255.255.255.0
- Click **Add**
- Allow Local Subnet: Enable
- Click **Update**

Access Policy » Network Access : Network Access List » rd0_networkaccess

	Properties	Network Settings	Optimization	DNS/Hosts
Enable Network Tunnel				
Network Tunnel		<input checked="" type="checkbox"/> Enable		
General Settings: Advanced				
Supported IP Version	IPV4			
IPV4 Lease Pool	+	rd0_leasepool		
Compression	No Compression			
Proxy ARP	<input type="checkbox"/> Enable			
SNAT Pool	Auto Map			
Preserve Source Port Strict	<input type="checkbox"/> Enable			
Session Update Threshold	0	Bytes/Second		
Session Update Window	0	Seconds		
Client Settings: Advanced				
Traffic Options	<input type="radio"/> Force all traffic through tunnel <input checked="" type="radio"/> Use split tunneling for traffic			
	IP Address 172.1.1.0			
	Mask 255.255.255.0			
	Add			
IPV4 LAN Address Space	172.1.1.0 / 255.255.255.0			
	Edit Delete			

Allow Local Subnet	<input checked="" type="checkbox"/> Enable
Allow Local DNS Servers	<input type="checkbox"/> Enable
Client Side Security	<input type="checkbox"/> Prohibit routing table changes during Network Access connection

Create a APM network access configuration for route domain 1

Open the Access > Connectivity/VPN > Network Access Lists page, click Create. Use the following values, leave all others at their defaults

- Name: rd1_networkaccess
- Click **Finished**

Access Policy » Network Access : Network Access List » New Resource...

General Properties	
Name	rd1_networkaccess
Description	
Auto launch	<input type="checkbox"/> Enable
Customization Settings for English	
Language	English
Caption	rd1_networkaccess
Detailed Description	
Image	<input type="button" value="Choose File"/> No file chosen <input type="button" value="View/Hide"/>
<input type="button" value="Cancel"/> <input type="button" value="Finished"/>	

Open the rd1_networkaccess you just created and go to Network Settings. Use the following values, leave all others at their defaults

- IPV4 Lease Pool: rd1_leasepool
- Traffic Options: Use split tunneling for traffic
- IPV4 LAN Address Space: - IP Address: 172.1.2.0%1 - Mask: 255.255.255.0
- Click **Add**
- Allow Local Subnet: Enable
- Click **Update**

Access Policy » Network Access : Network Access List » rd1_networkaccess

Properties	Network Settings	Optimization	DNS/Hosts
Enable Network Tunnel			
Network Tunnel	<input checked="" type="checkbox"/> Enable		
General Settings: Advanced ▾			
Supported IP Version	IPV4 ▾		
IPV4 Lease Pool	rd1_leasepool ▾		
Compression	No Compression ▾		
Proxy ARP	<input type="checkbox"/> Enable		
SNAT Pool	Auto Map ▾		
Preserve Source Port Strict	<input type="checkbox"/> Enable		
Session Update Threshold	0	Bytes/Second	
Session Update Window	0	Seconds	
Client Settings: Advanced ▾			
Traffic Options	<input type="radio"/> Force all traffic through tunnel <input checked="" type="radio"/> Use split tunneling for traffic		
	IP Address	172.1.2.0%1	
	Mask	255.255.255.0	
	Add		
IPv4 LAN Address Space	172.1.2.0%1 / 255.255.255.0		
	Edit	Delete	
Allow Local Subnet	<input checked="" type="checkbox"/> Enable		
Allow Local DNS Servers	<input type="checkbox"/> Enable		
Client Side Security	<input type="checkbox"/> Prohibit routing table changes during Network Access connection		

Create a APM access profile

Open the Access >Profiles / Policies (Per-Session Policies) page, click Create. Use the following values,

leave all others at their defaults

- Name: afm_accessprofile
- Profile Type: All
- Accepted Languages: English
- Click **Finished**

The screenshot shows two tabs of a configuration interface:

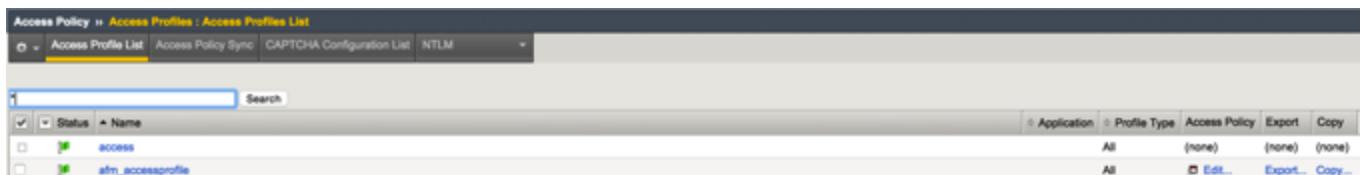
- General Properties**:

Name	afm_accessprofile
Parent Profile	access
Profile Type	All
Profile Scope	Profile
- Language Settings**:

Additional Languages	Afar (aa) <input type="button" value="Add"/>		
Languages	<table border="1"><tr><td>Accepted Languages</td><td>English (en)</td></tr></table>	Accepted Languages	English (en)
Accepted Languages	English (en)		
Default Language	English (en) <input type="button" value=""/>		

On the right, there is a list of "Factory BuiltIn Languages": Japanese (ja), Chinese (Simplified) (zh-cn), Chinese (Traditional) (zh-tw), Korean (ko), Spanish (es), French (fr), German (de). Buttons << and >> are present between the language lists.

Now click **Edit** for the afm_accessprofile



The afm_accessprofile is displayed

Access Policy: /Common/afm_accessprofile



Modify the Visual Policy Editor (VPE) – The VPE is what the client interacts with and is assigned before the approval or denial of access to a resource.

Click on the plus sign after the start block and navigate to Endpoint Security (Client-Side) and select Firewall and click **Add Item**

Endpoint Security (Server-Side)	
<input type="radio"/> Anti-Spyware	Anti-spyware Software Check for Windows and Mac
<input type="radio"/> Antivirus	Antivirus Software Check for Windows, Mac and Linux
<input checked="" type="radio"/> Firewall	Firewall Software Check for Windows, Mac and Linux
<input type="radio"/> Hard Disk Encryption	Hard Disk Encryption Software Check for Windows and Mac

Leave the defaults

Properties Branch Rules

Name: Firewall

Software Check

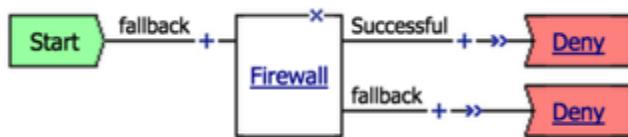
Continuously check the result and end the session if it changes

Add new entry Insert Before: 1

Platform	Vendor ID	Product ID	State	Version	X
1 Any	Any	Any	Enabled		X

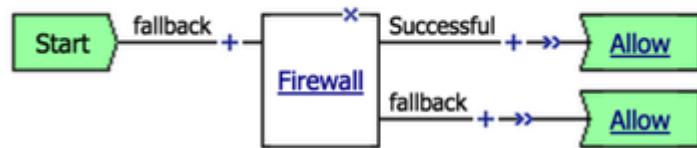
and click **Save**

Change both endings from Deny



to Allow

Access Policy: /Common/afm_accessprofile



In the Successful branch of the Firewall block click the “+” sign and navigate to Assignment->Route Domain and SNAT Selection and click Add Item. Use the following values, leave all others at their defaults

- Name: rd1
- Route Domain: /Common/rd1
- SNAT: none
- Click **Save**

Properties Branch Rules

Name: rd1

Route Domain Selection Agent

Route Domain	/Common/rd1
SNAT	none

After the rd1 block click the “+” sign and navigate to Assignment->Advanced Resource Assign and

- Click **Add Item**
- Click **Add new entry**
- Click **Add/Delete**

Use the following values, leave all others at their defaults

- Network Access: /Common/rd1_networkaccess
- Webtop: /Common/afm_webtop
- Click **Update**

Change the name to rd1 Resource Assign and click Save

Properties* Branch Rules

Name: rd1 Resource Assign

Resource Assignment

Add new entry

Expression: Empty change

1 **Network Access:** /Common/rd1_networkaccess
Webtop: /Common/afm_webtop
[Add/Delete](#)

In the fallback branch of the Firewall block click the “+” sign and navigate to Assignment->Route Domain and SNAT Selection and click Add Item. Use the following values, leave all others at their defaults

- Name: rd0
- Route Domain: /Common/0
- SNAT: none

- Click **Save**

Properties* Branch Rules

Name: rd0

Route Domain Selection Agent

Route Domain	/Common/0
SNAT	none

After the rd0 block click the “+” sign and navigate to Assignment->Advanced Resource Assign and

- Click **Add Item**
- Click **Add new entry**
- Click **Add/Delete**

Use the following values, leave all others at their defaults

- Network Access: /Common/rd0_networkaccess
- Webtop: /Common/afm_webtop
- Click **Update**

Change the name to `rd0 Resource Assign` and click Save

Properties* Branch Rules

Name: rd0 Resource Assign

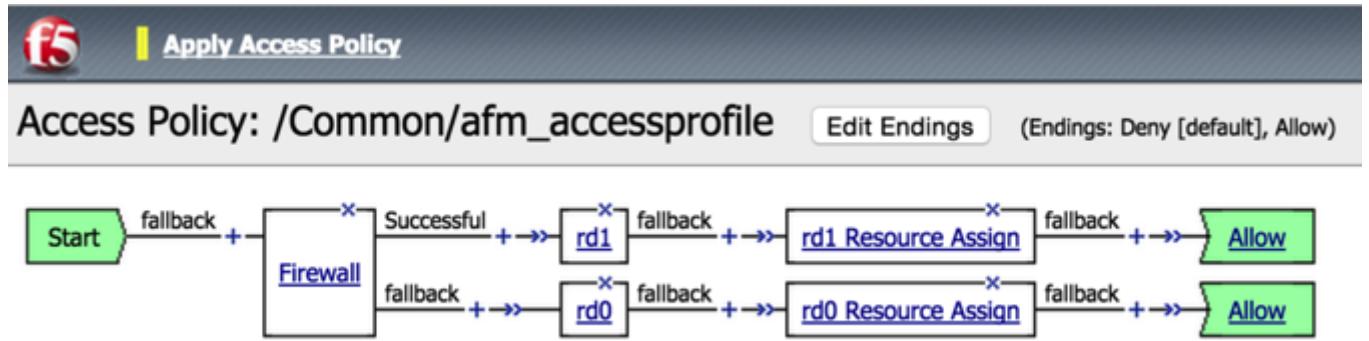
Resource Assignment

Add new entry

Expression: Empty change

1 **Network Access:** /Common/rd0_networkaccess
Webtop: /Common/afm_webtop
[Add/Delete](#)

The final access policy should look like



Click Apply Access Policy

TASK 3 – Create new virtual server for the APM L3 SSL VPN

Create a new virtual server for the APM L3 SSL VPN. This is the virtual where the APM policy will be assigned and where sslvpn traffic will be terminated.

Open the Local Traffic -> Virtual Servers page, click Create. Use the following values, leave all others at their defaults

- Name: `apm_vs`
- Type: standard
- Destination Address: `192.168.1.50`
- Service Port: `443`
- HTTP Profile: `HTTP`
- SSL Profile (Client): `clientssl`
- Access Profile: `afm_accessprofile`
- Connectivity Profile: `afm_cp`
- Click **Finished**

General Properties

Name	apm_vs
Description	
Type	Standard
Source Address	
Destination Address	192.168.1.50
Service Port	443 HTTPS
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled

Configuration: Advanced

Protocol	TCP						
Protocol Profile (Client)	tcp						
Protocol Profile (Server)	(Use Client Profile)						
HTTP Profile	http						
FTP Profile	None						
RTSP Profile	None						
SOCKS Profile	None						
Stream Profile	None						
XML Profile	None						
SSL Profile (Client)	<table border="1"> <tr> <th>Selected</th> <th>Available</th> </tr> <tr> <td>/Common clientssl</td> <td> <input type="button" value="<<"/> <input type="button" value=">>"/> </td> </tr> <tr> <td colspan="2"> <input type="button" value="<<"/> <input type="button" value=">>"/> </td> </tr> </table>	Selected	Available	/Common clientssl	<input type="button" value="<<"/> <input type="button" value=">>"/>	<input type="button" value="<<"/> <input type="button" value=">>"/>	
Selected	Available						
/Common clientssl	<input type="button" value="<<"/> <input type="button" value=">>"/>						
<input type="button" value="<<"/> <input type="button" value=">>"/>							
SSL Profile (Server)	<table border="1"> <tr> <th>Selected</th> <th>Available</th> </tr> <tr> <td></td> <td> <input type="button" value="<<"/> <input type="button" value=">>"/> </td> </tr> <tr> <td colspan="2"> <input type="button" value="<<"/> <input type="button" value=">>"/> </td> </tr> </table>	Selected	Available		<input type="button" value="<<"/> <input type="button" value=">>"/>	<input type="button" value="<<"/> <input type="button" value=">>"/>	
Selected	Available						
	<input type="button" value="<<"/> <input type="button" value=">>"/>						
<input type="button" value="<<"/> <input type="button" value=">>"/>							

Access Policy	
Access Profile	afm_accessprofile ▾
Connectivity Profile	afm_cp ▾
Per-Request Policy	None ▾
VDI Profile	None ▾
Application Tunnels (Java & Per-App VPN)	<input type="checkbox"/> Enabled
OAM Support	<input type="checkbox"/> Enabled

TASK 4 – Create APM policies

Create a new virtual server. Two new virtual servers need to be created that control traffic coming out of the vpn tunnel to resources protected by the tunnel. In addition the virtual servers provide a place to apply afm policies to control traffic.

Create a new virtual server for route domain 0 traffic

Open the Local Traffic -> Virtual Servers page, click Create. Use the following values, leave all others at their defaults

- Name: rd0_vs
- Type: Forwarding (IP)
- Destination Address: 172.1.1.0/24
- Service Port: * All Ports
- Protocols: * All Protocols
- VLANS and Tunnels: afm_cp
- Click **Finished**

Local Traffic » Virtual Servers : Virtual Server List » New Virtual Server...

General Properties	
Name	rd0_vs
Description	
Type	Forwarding (IP)
Source Address	
Destination Address	172.1.1.0/24
Service Port	* All Ports
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled

Configuration: Advanced

Protocol	* All Protocols						
Protocol Profile (Client)	fastL4						
Statistics Profile	None						
VLAN and Tunnel Traffic	Enabled on...						
VLANS and Tunnels	<table border="1"> <thead> <tr> <th>Selected</th> <th>Available</th> </tr> </thead> <tbody> <tr> <td>/Common afm_cp</td> <td>/Common clientlan_vlan http-tunnel serverlan1_vlan serverlan2_vlan</td> </tr> <tr> <td><<</td> <td>>></td> </tr> </tbody> </table>	Selected	Available	/Common afm_cp	/Common clientlan_vlan http-tunnel serverlan1_vlan serverlan2_vlan	<<	>>
Selected	Available						
/Common afm_cp	/Common clientlan_vlan http-tunnel serverlan1_vlan serverlan2_vlan						
<<	>>						

Create a new virtual server for route domain 1 traffic

Open the Local Traffic -> Virtual Servers page, click Create. Use the following values, leave all others at their defaults

- Name: rd1_vs
- Type: Forwarding (IP)
- Source Address: 0.0.0.0%1/0
- Destination Address: 172.1.2.0%1/24
- Service Port: * All Ports
- Protocols: * All Protocols
- VLANS and Tunnels: afm_cp
- Click **Finished**

Local Traffic » Virtual Servers : Virtual Server List » rd1_vs

	Properties	Resources	Security	Statistics
General Properties				
Name	rd1_vs			
Partition / Path	Common			
Description				
Type	Forwarding (IP) ▾			
Source Address	0.0.0.0%1/0			
Destination Address	172.1.2.0%1/24			
Service Port	0	* All Ports	▼	
Notify Status to Virtual Address	<input checked="" type="checkbox"/>			
Availability	<input type="checkbox"/> Unknown (Enabled) - The children pool member(s) either			
Syncookie Status	Off			
State	Enabled ▾			
Configuration:	Advanced ▾			
Protocol	* All Protocols ▾			
Protocol Profile (Client)	fastL4 ▾			
Statistics Profile	None ▾			
VLAN and Tunnel Traffic	Enabled on... ▾			
VLANs and Tunnels	<p style="text-align: center;">Selected</p> <div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> /Common afm_cp </div> <div style="display: flex; justify-content: space-around; margin-top: 10px;"> << >> </div>	<p style="text-align: center;">Available</p> <div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> /Common clientlan_vlan http-tunnel serverlan1_vlan serverlan2_vlan </div>		

Create the AFM policy for route domain 0 traffic. This limits traffic through sslvpn to the internal subnet in route domain 0.

Open the Security -> Network Firewall->Active Rules page, click Add. Use the following values, leave all others at their defaults

- Context: Virtual Server, rd0
- Policy New, Name: rd0_afmpolicy
- Name: rd0_denyall_rule
- Action: Reject
- Logging: Enabled

- Click **Finished**

Security » Network Firewall : Active Rules » New Rule...

General Properties	
Context	Virtual Server... <input type="button" value="rd0_vs"/>
Policy Type	Enforced <input type="button"/>
Policy	New... <input type="button"/> Name: rd0_afmpolicy

Rule Properties	
Name	rd0_denyall_rule
Description	
Order	Last <input type="button"/>
Type	Rule <input type="button"/>
State	Enabled <input type="button"/>
Protocol	Any <input type="button"/>
Source	Address/Region: Any <input type="button"/> Port: Any <input type="button"/> VLAN / Tunnel: Any <input type="button"/>
Destination	Address/Region: Any <input type="button"/> Port: Any <input type="button"/>
iRule	None
Action	Reject <input type="button"/>
Logging	Enabled <input type="button"/>

Cancel **Repeat** **Finished**

Create the AFM policy for route domain 1 traffic. This limits traffic through sslvpn to the internal subnet in route domain 1.

Open the Security -> Network Firewall->Active Rules page, click Add. Use the following values, leave all others at their defaults

- Context: Virtual Server, rd1
- Policy New, Name: rd1_afmpolicy

- Name: rd1_denyall_rule
- Action: Reject
- Logging: Enabled
- Click **Finished**

Security » Network Firewall : Active Rules » New Rule...

General Properties	
Context	Virtual Server... <input type="button" value="rd1_vs"/>
Policy Type	Enforced <input type="button"/>
Policy	New... <input type="button"/> Name: <input type="text" value="rd1_afmpolicy"/>

Rule Properties	
Name	<input type="text" value="rd1_denyall_rule"/>
Description	<input type="text"/>
Order	Last <input type="button"/>
Type	Rule <input type="button"/>
State	Enabled <input type="button"/>
Protocol	Any <input type="button"/>
Source	Address/Region: Any <input type="button"/> Port: Any <input type="button"/> VLAN / Tunnel: Any <input type="button"/>
Destination	Address/Region: Any <input type="button"/> Port: Any <input type="button"/>
iRule	<input type="text" value="None"/>
Action	Reject <input type="button"/>
Logging	Enabled <input type="button"/>

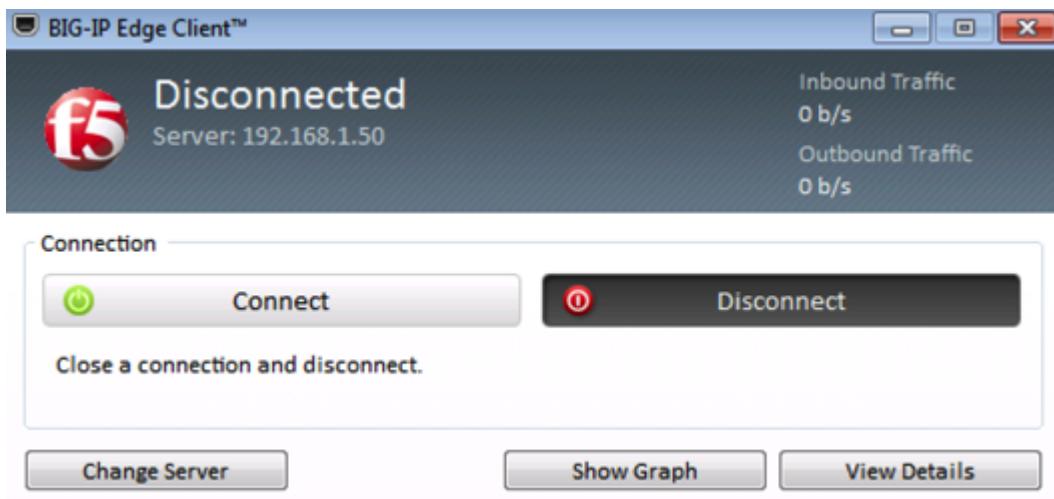
TASK 5 – Test

Now its time to test the vpn.

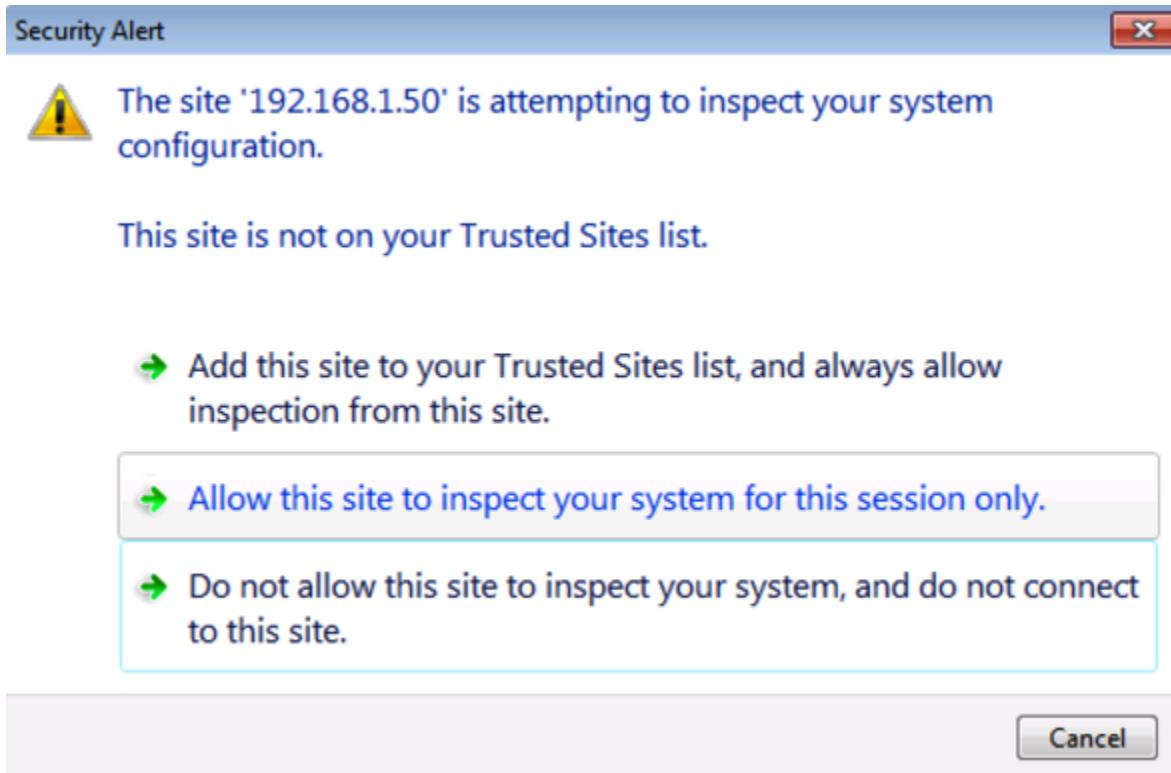
On your jumpstation start the BIG-IP Edge Client which is the grey ethernet port at the bottom of the desktop.



Ensure the Edge Client is using server 192.168.1.50, the APM vip, if not use Change Server to select it and Click Connect



The Edge Client will inspect your jumpstation to determine the firewall status, select “Allow this site to inspect for this session only”



Once the Edge Client is connected, go to View Details, which route domain are you in?

Why?

This completes Lab2

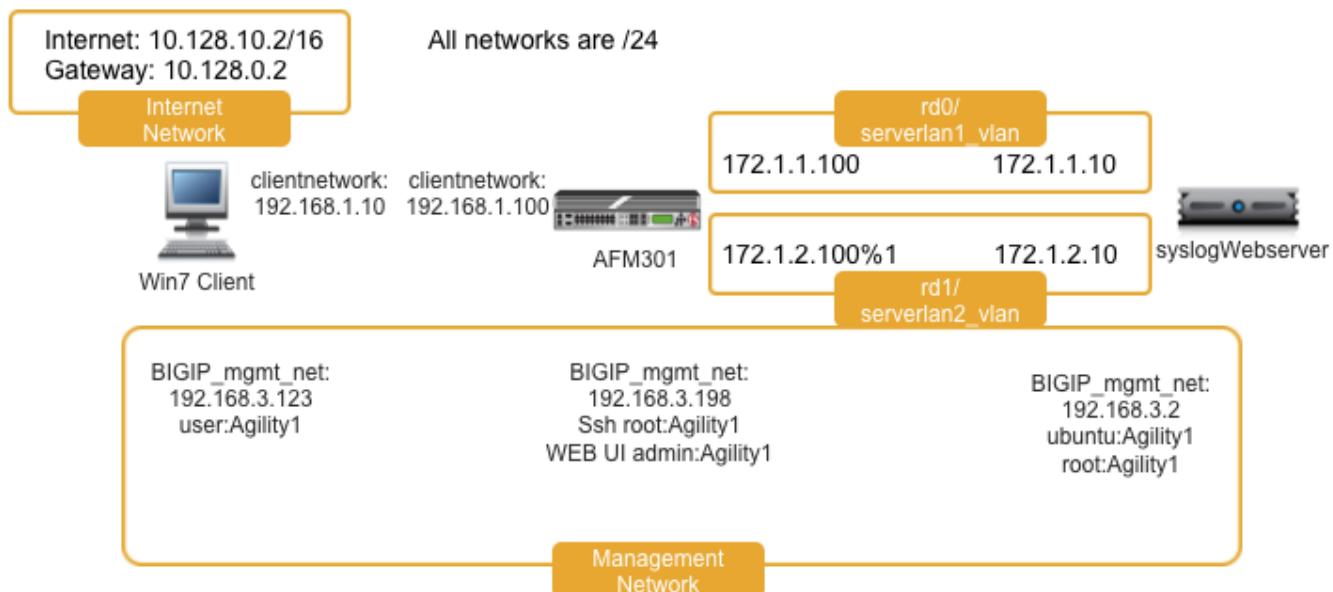
1.1.3 Lab 3: AFM with iRules LX

Estimated completion time: 15 minutes

Overview

Beginning in TMOS 12.1 BIGIP offers iRules LX which is a node.js extension to iRules. iRules LX does not replace iRules, rather allows iRules to offer additional functionality. In this lab you see how iRules LX can be used to look up client ip addresses that should be disallowed by AFM.

Use the following network diagram



TASK 1 – Copy LX Code and Test

On the Win7 client, open the index.js file located in the Desktop folder, copy its entire contents.

On the AFM301 webgui, navigate to Local Traffic->iRules-> LX Workspaces-> irules_lx_mysql_workspace

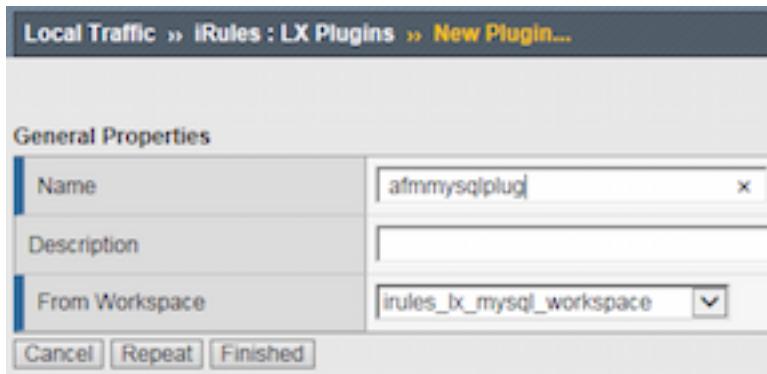
And replace the contents of mysql_extension/index.js with the contents of the index.js on the Win7 client.

Click “Save File”

Next click on rules->mysql_irulelx

On the Win7 client, open the mysql_iRulesLx.txt file located in the Desktop folder, copy its entire contents and paste the contents into the “mysql_irulelx”. Click “Save File”

On the AFM301 webgui, navigate to Local Traffic->iRules-> LX Plugins and create a new LX Plugin named “afmmysqlplug” using the workspace (From Workspace dropdown) irules_lx_mysql_workspace. Click “Finished”



Navigate to Security->Network Firewall->Policies->afmmysql_pol->afmmysql_rule (this rule already exists) and click iRule to assign the “mysql_irulelx” iRule. Click “Update”

Security > Network Firewall : Policies > afmmysql_pol : afmmysql_rule

Properties	
Name	afmmysql_rule
Partition / Path	Common
Description	
Type	Rule
State	Enabled
Protocol	Any
Source	Address/Region: Any VLAN / Tunnel: Any
Destination	Address/Region: Any
iRule	mysql_irulelx
iRule Sampling	Disabled
Action	Accept
Logging	Disabled
Service Policy	None
<input type="button" value="Update"/> <input type="button" value="Delete"/>	

This policy is already enforced on the afmmysql_vs (192.168.1.51)

On the Win7 client, use curl in the cygwin cli to test that the client is being blocked, as the Win7 client's ip is in the mysql database.

```
curl http://192.168.1.51 --connect-timeout 5
```

this should timeout.

Ensure that the Irule is working properly, by going back to the AFM rule and setting the iRule back to None.

Also look at /var/log/ltm on the AFM301 BIG-IP.

WE MAKE APPS



FASTER.
SMARTER.
SAFER.



F5 Networks, Inc. | f5.com