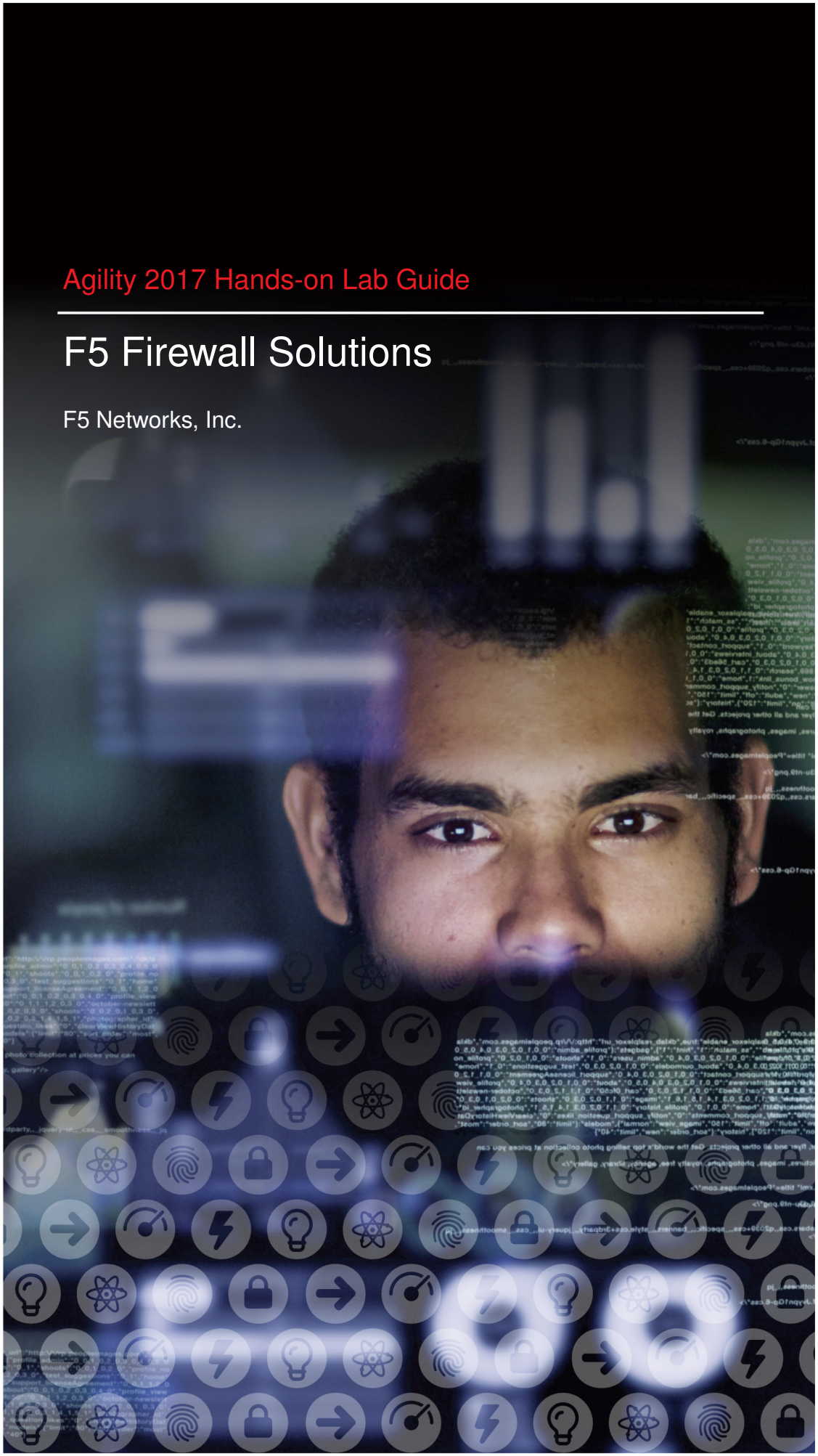


Agility 2017 Hands-on Lab Guide

F5 Firewall Solutions

F5 Networks, Inc.

Contents:

1

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 firewalling. (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/download
  - 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.

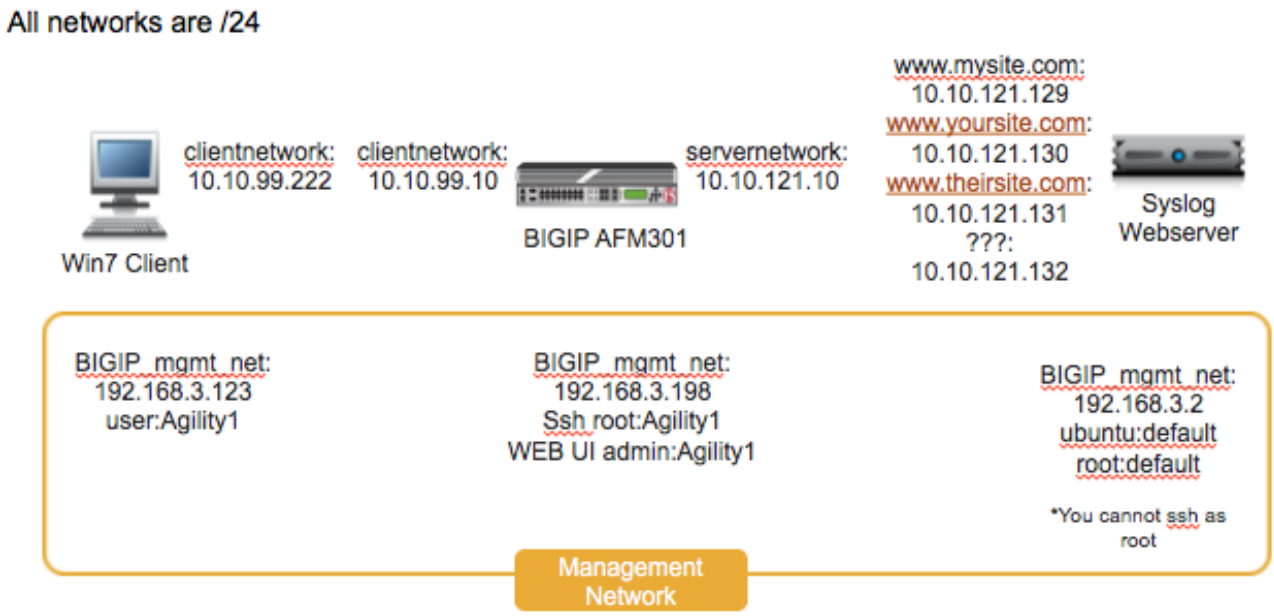
On your personal device

Look at the supplemental login instructions for:

External Hostnames

External IP addressing diagram

Login IDs and Passwords are subject to change as well.

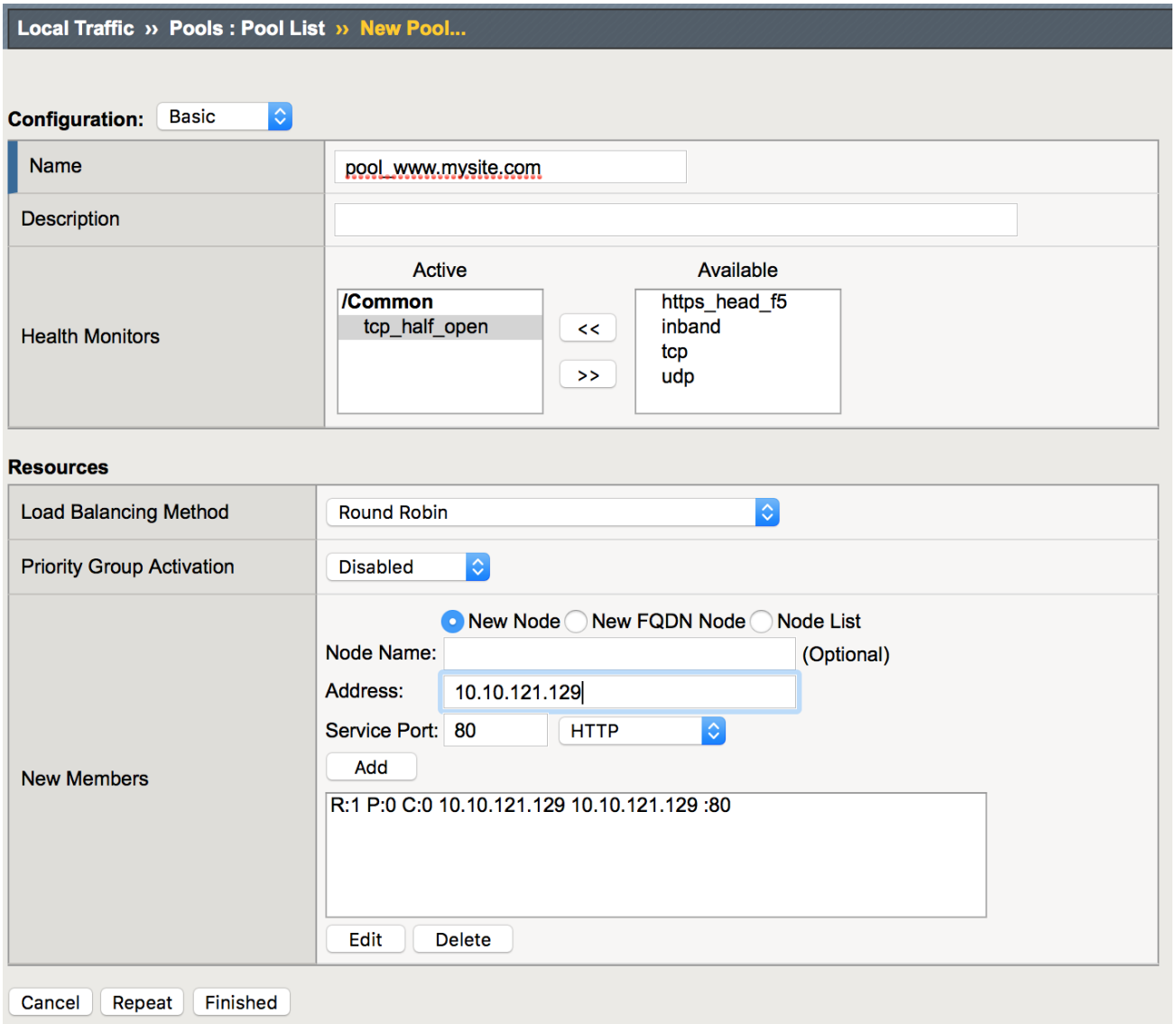


On BIG-IP

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



Note: Leave all other fields using the default values.

Navigation: Click Finished

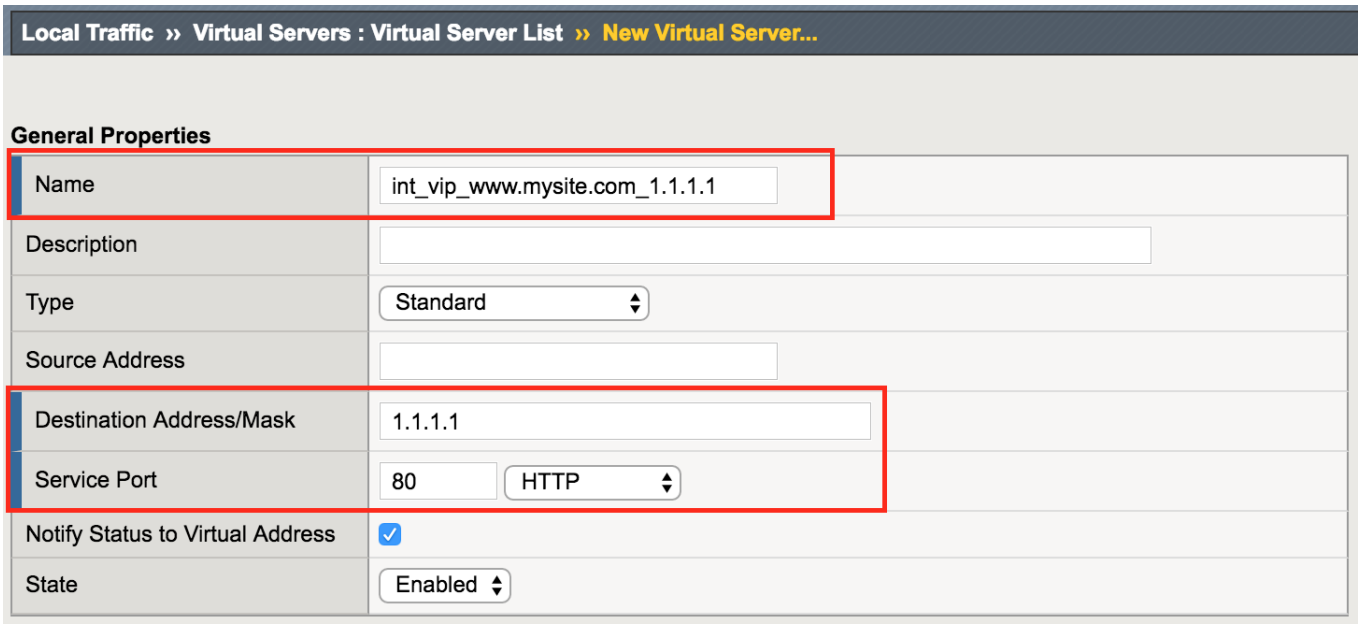
Status	Name	Description	Application	Members	Partition / Path
	pool_www.mysite.com			1	Common
	pool_www.mysite.com-api			1	Common
	pool_www.theirsite.com			1	Common
	pool_www.yoursite.com			1	Common

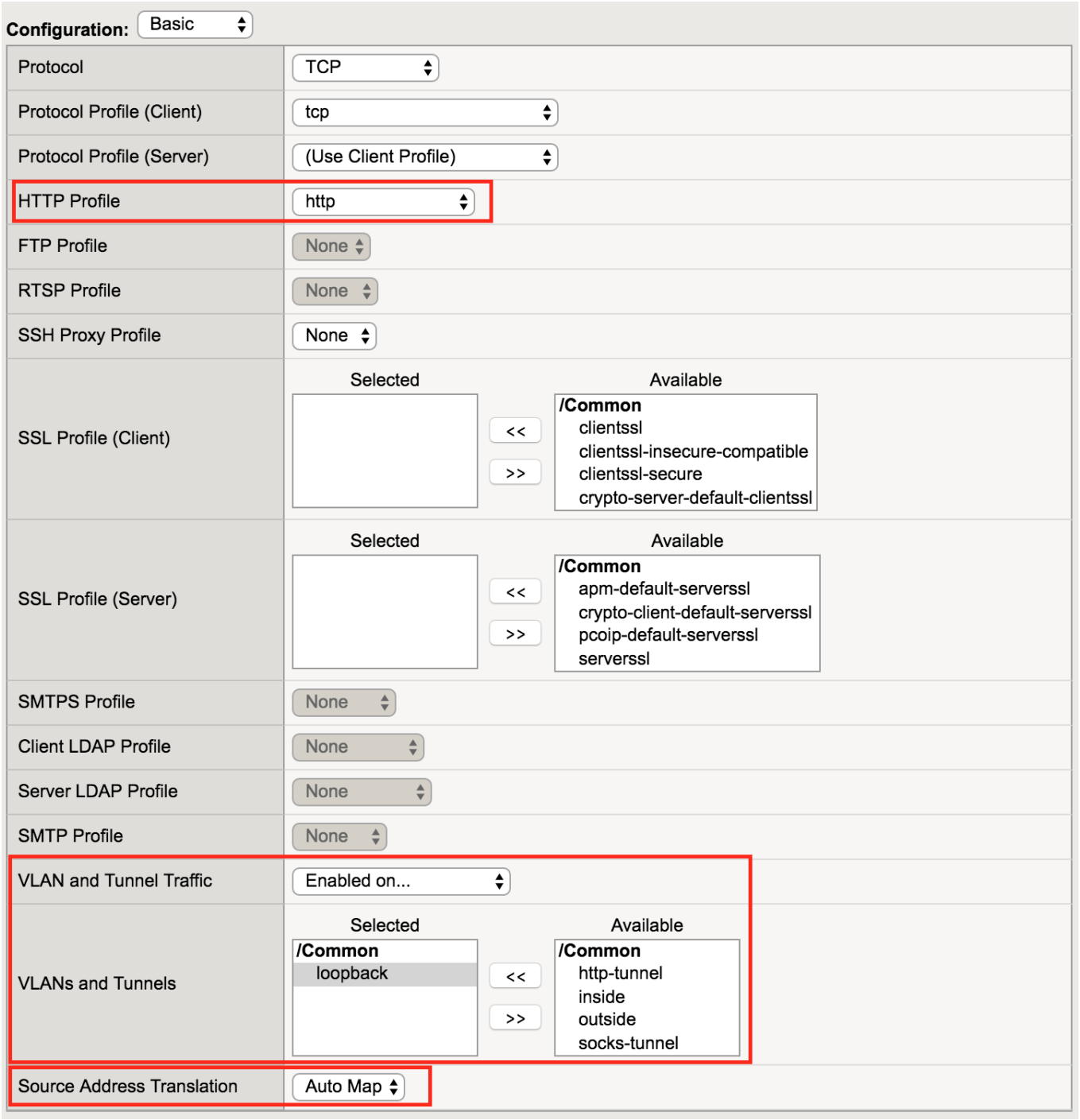
Note: The pools should now show a green circle for status.

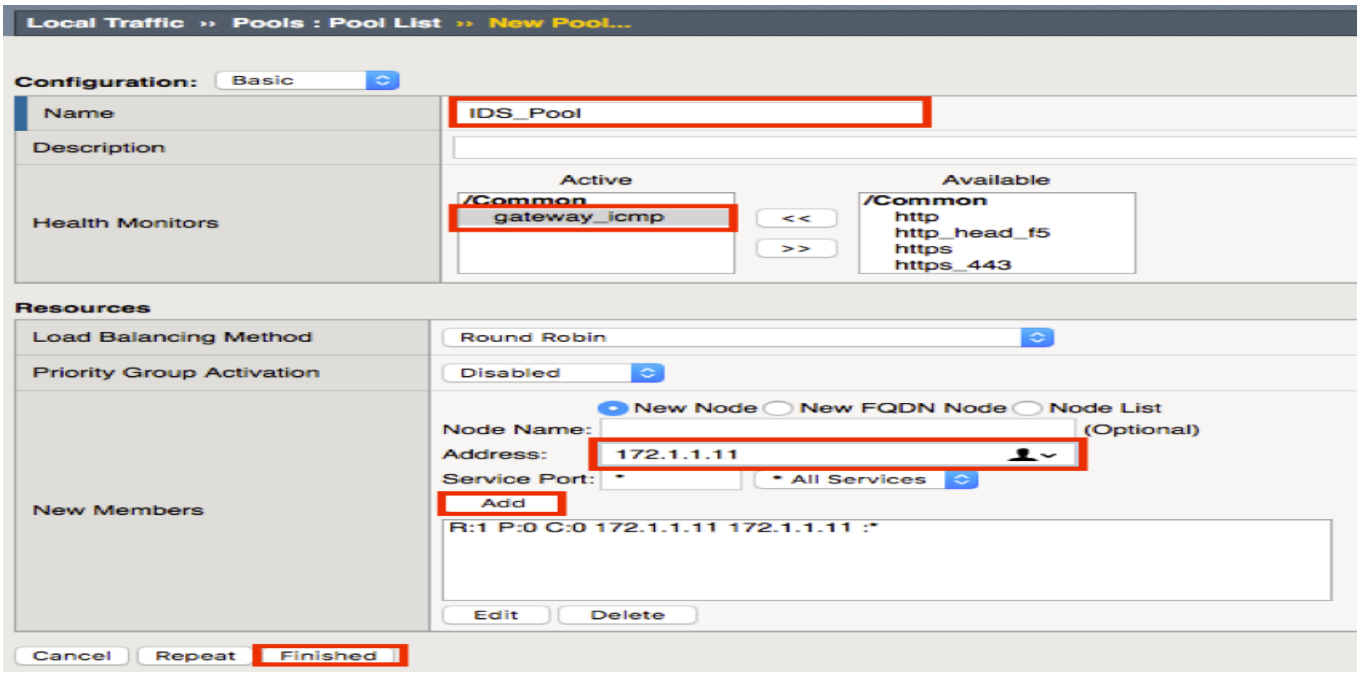
Create the internal virtual servers using the following information:

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

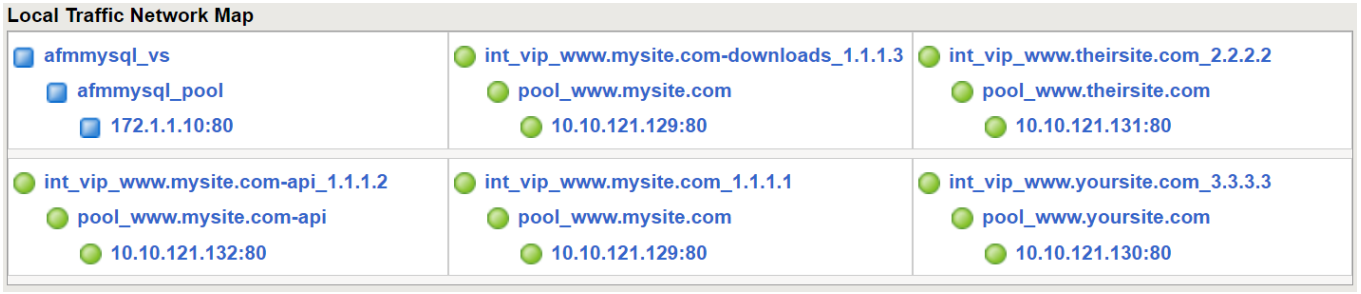



Configuration: Basic
Protocol
TCP
Protocol Profile (Client)
tcp
Protocol Profile (Server)
(Use Client Profile)
HTTP Profile
http
FTP Profile
None
RTSP Profile
None
SSH Proxy Profile
None
SSL Profile (Client)
Selected
Available
/Common
clientssl
clientssl-insecure-compatible
clientssl-secure
crypto-server-default-clientssl
<<
>>
SSL Profile (Server)
Selected
Available
/Common
apm-default-serverssl
crypto-client-default-serverssl
pcoip-default-serverssl
serverssl
<<
>>
SMTPS Profile
None
Client LDAP Profile
None
Server LDAP Profile
None
SMTP Profile
None
VLAN and Tunnel Traffic
Enabled on...
VLANs and Tunnels
Selected
/Common
loopback
Available
/Common
http-tunnel
inside
outside
socks-tunnel
<<
>>
Source Address Translation
Auto Map



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

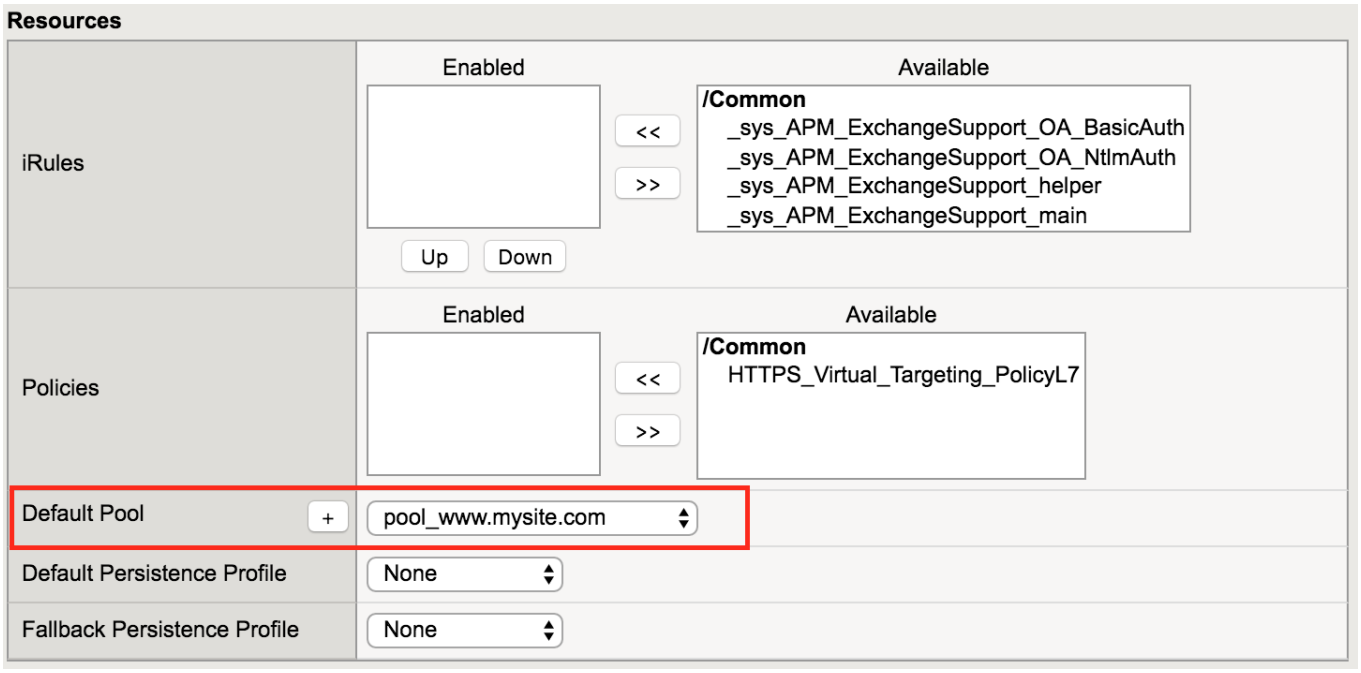
Name	Dest	Port	HTTP Profile	SSL Profile (Client)	Default Pool
EXT_VIP_10.10.99.30	10.10.99.30	443	YES	www.mysite.com www.theirsite.com www.yoursite.com	pool_www.mysite.com

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	☑
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)	Selected: /Common, www.mysite.com, www.theirsite, www.yoursite.com — Available: clientssl, clientssl-insecure-compatible, clientssl-secure, crypto-server-default-clientssl, wom-default-clientssl
SSL Profile (Server)	Selected: — Available: /Common, apm-default-serverssl, crypto-client-default-serverssl, pcoip-default-serverssl, serverssl
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



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

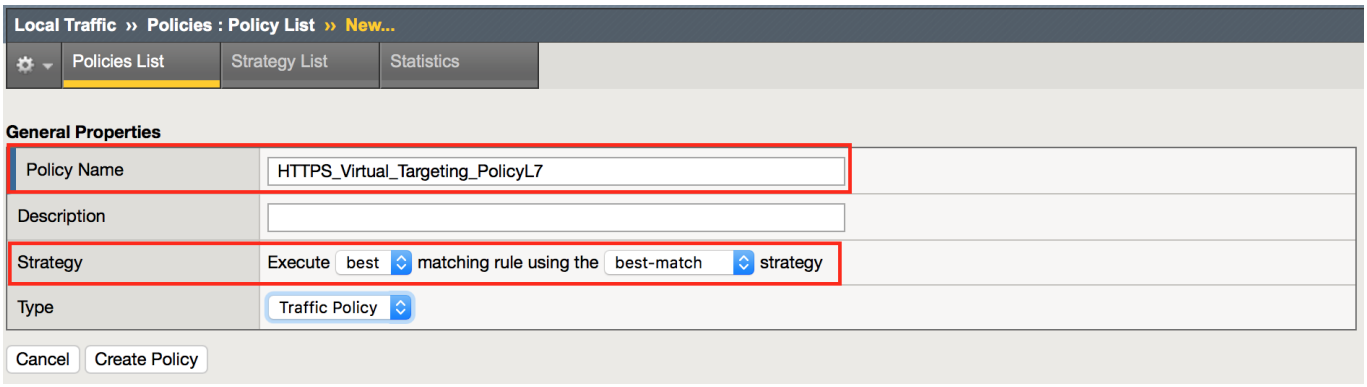
TASK 2 – Configure And Attach The LTM Policy

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.

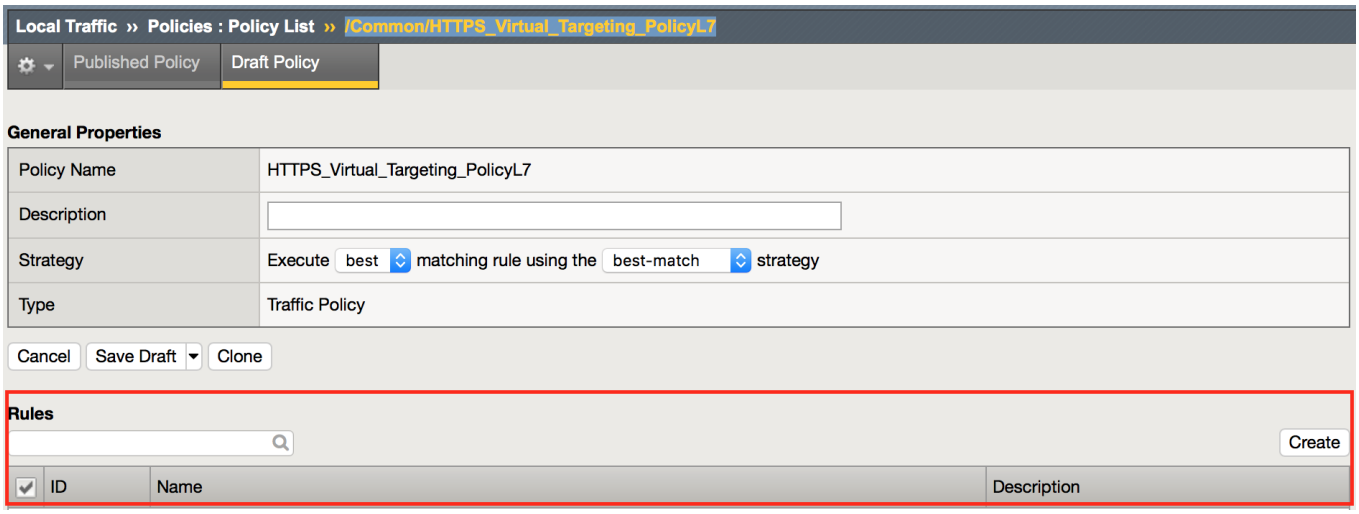
Navigation: Local Traffic > Policies : Policy List > Policy List Page, then click Create

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

Navigation: Click Create Policy



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



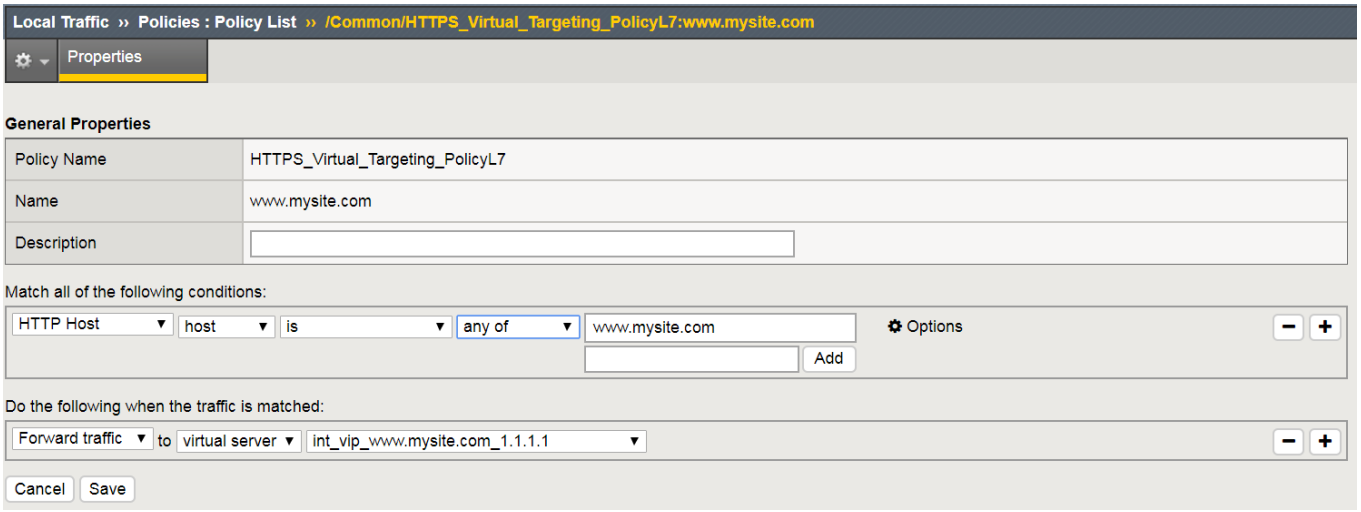
The policy configuration should now include a Rules section

Navigation: Click Create

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

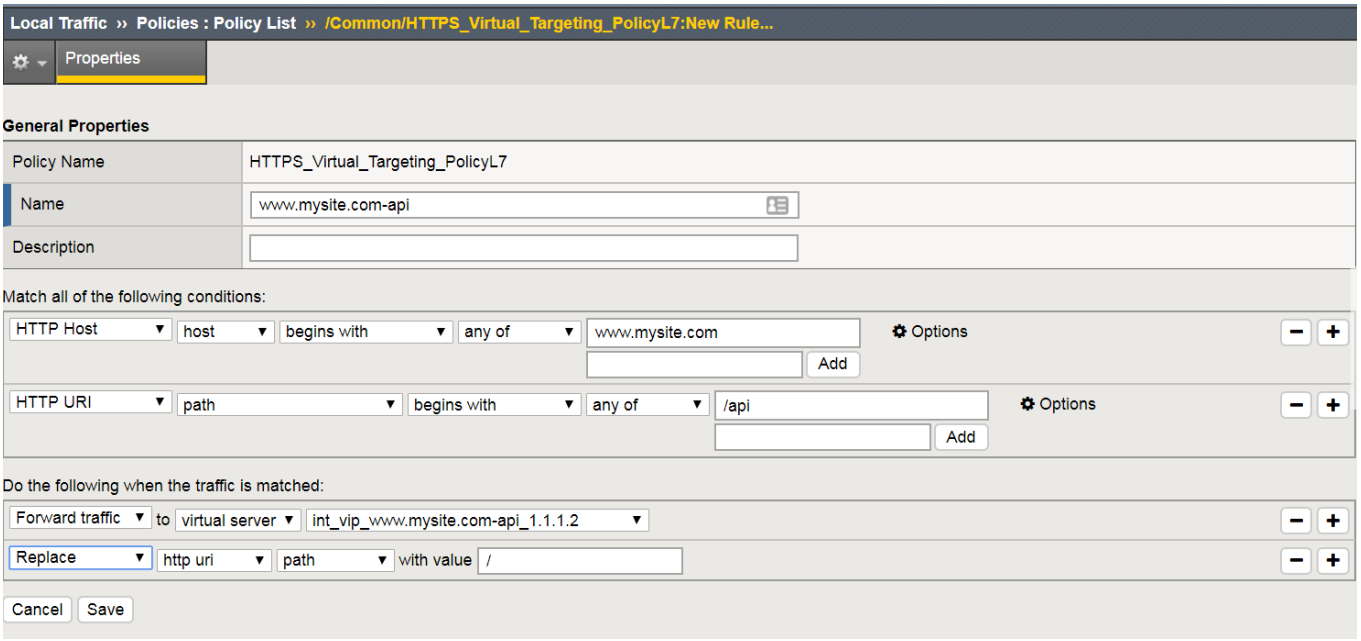
Rule Name				
www.mysite.com	HTTP Host	Host	is	www.mysite.com
ACTION	Forward Traffic	Virtual Server		int_vip_www.mysite.com_1.1.1.1
www.yoursite.com	HTTP Host	Host	is	www.yoursite.com
ACTION	Forward Traffic	Virtual Server		int_vip_www.yoursite.com_3.3.3.3
www.theirsite.com	HTTP Host	Host	is	www.theirsite.com
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



Navigation: Click Save

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

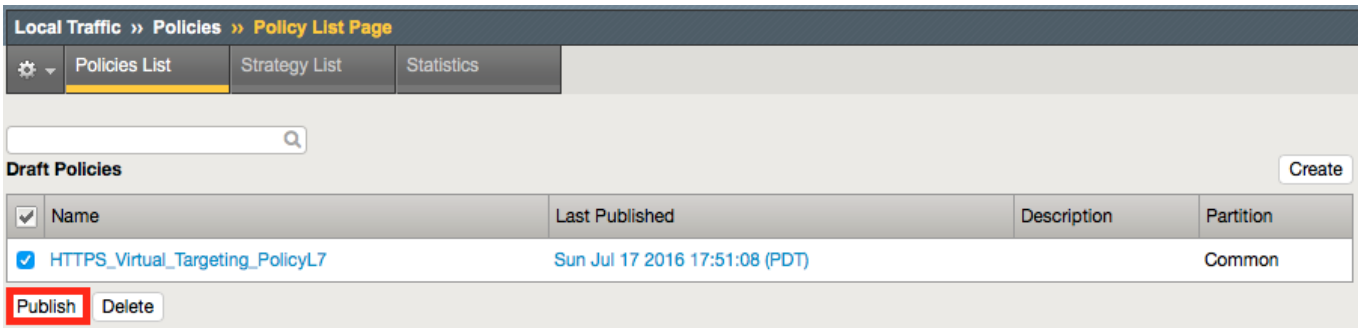


Complete the additional policies according to the list above.

Once complete publish the policy.

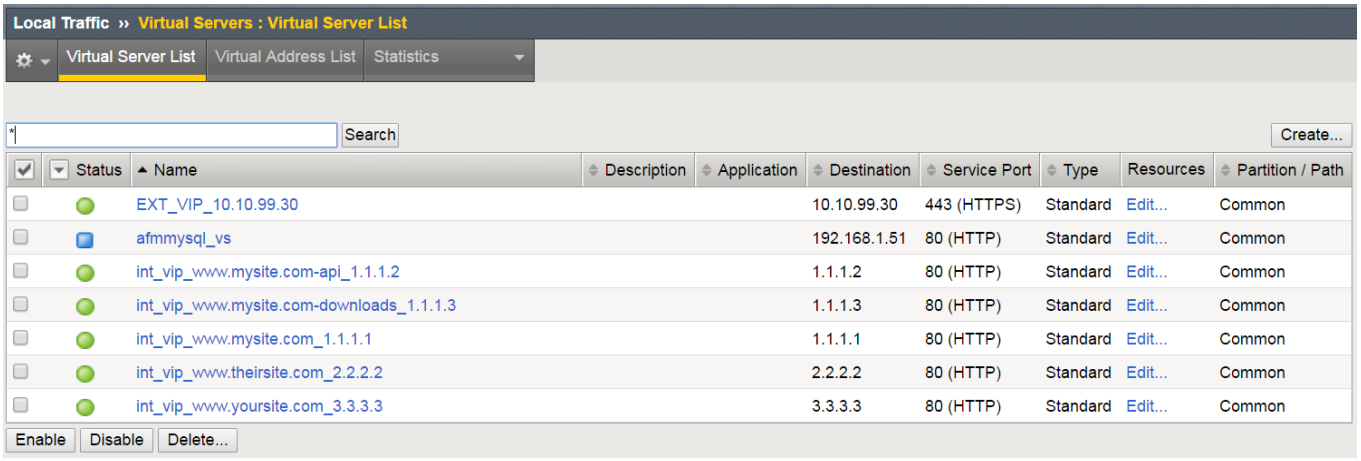
Navigation: Local Traffic > Policies: Policy List > /Common/HTTPS_Virtual_Targeting_PolicyL7

Navigation: Click Publish

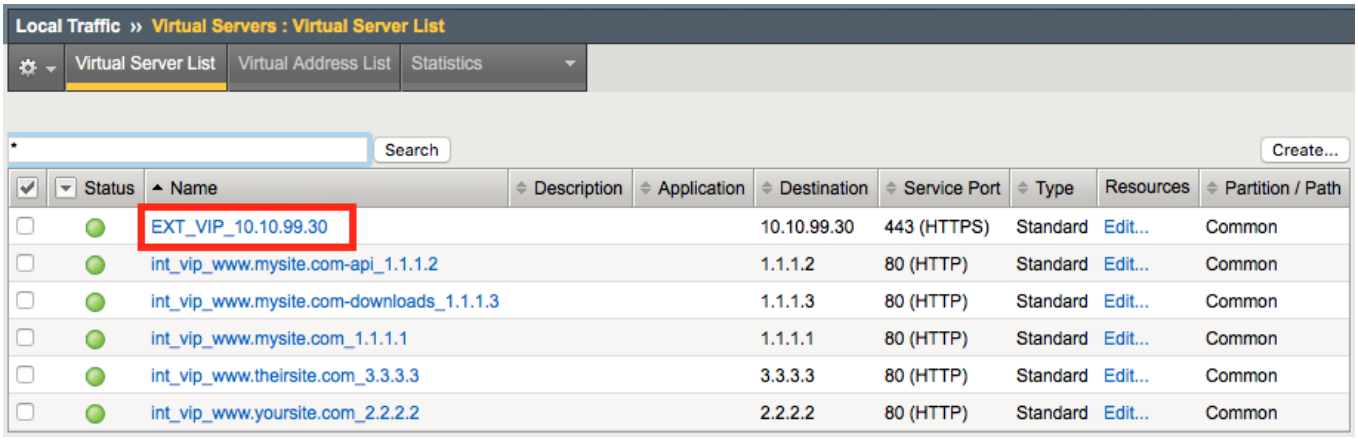


Now apply the policy to the external virtual server

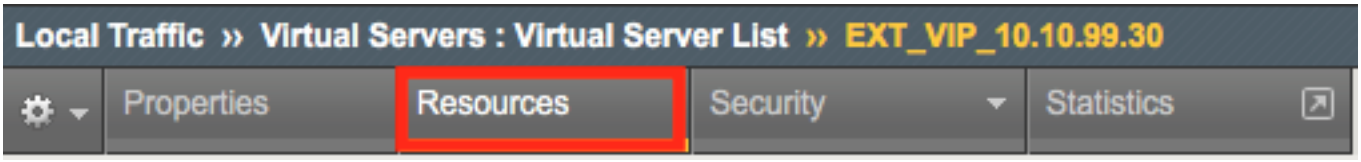
Navigation: Local Traffic > Virtual Servers : Virtual Server List



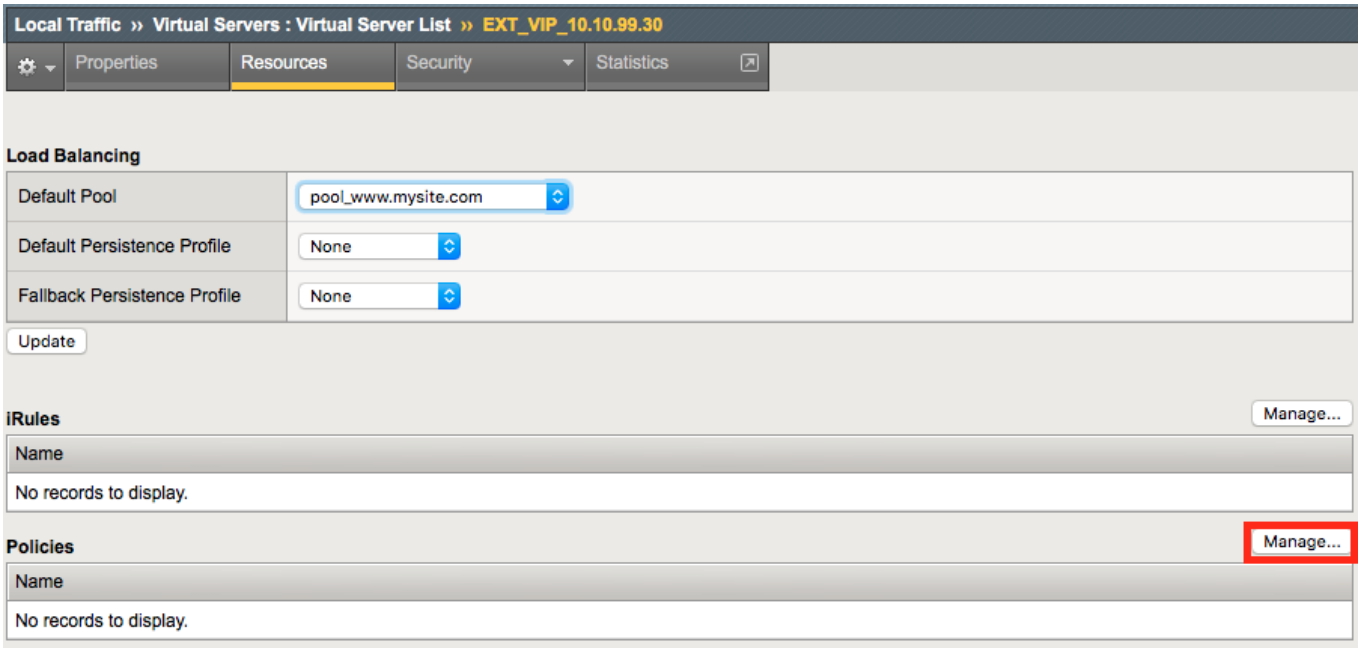
Navigation: Click the EXT_VIP_10.10.90.30



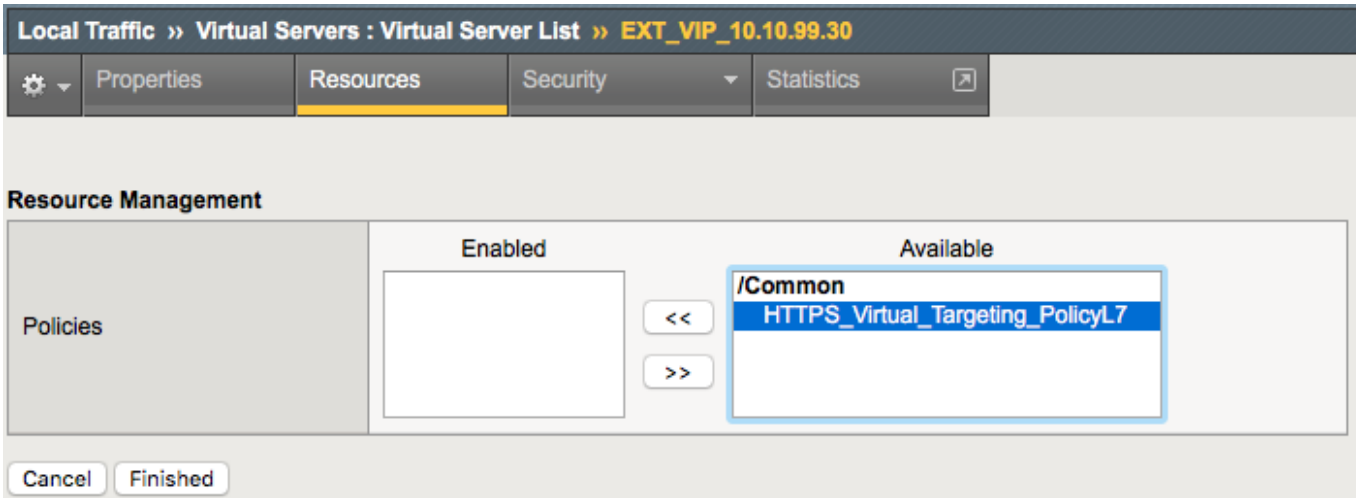
Navigation: Click the Resources Tab



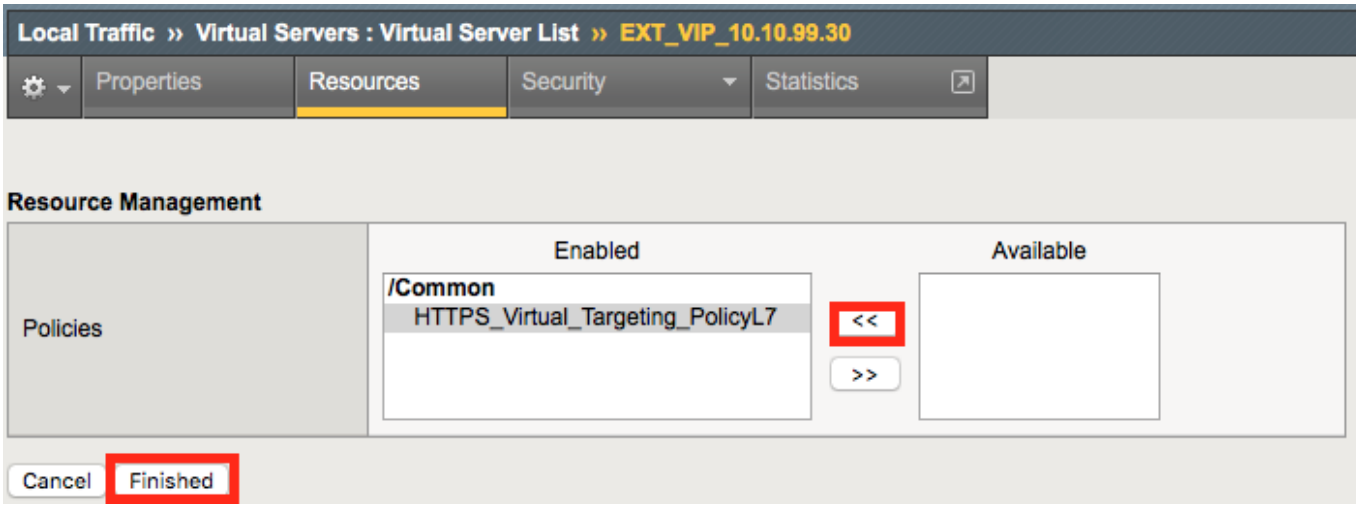
Navigation: Under Policies Click Manage



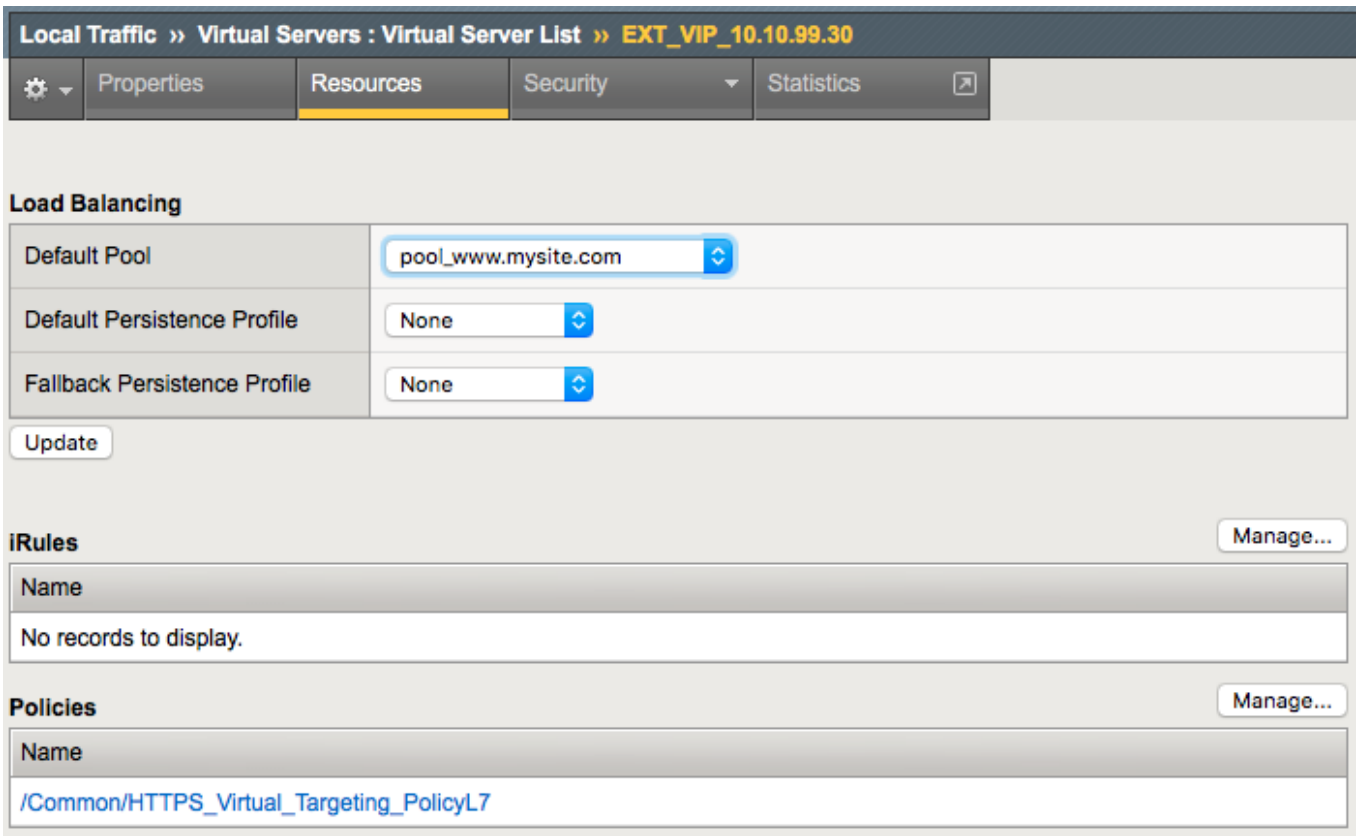
Navigation: Select the HTTPS_Virtual_Targeting_PolicyL7



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



The result should look like the screenshot below.



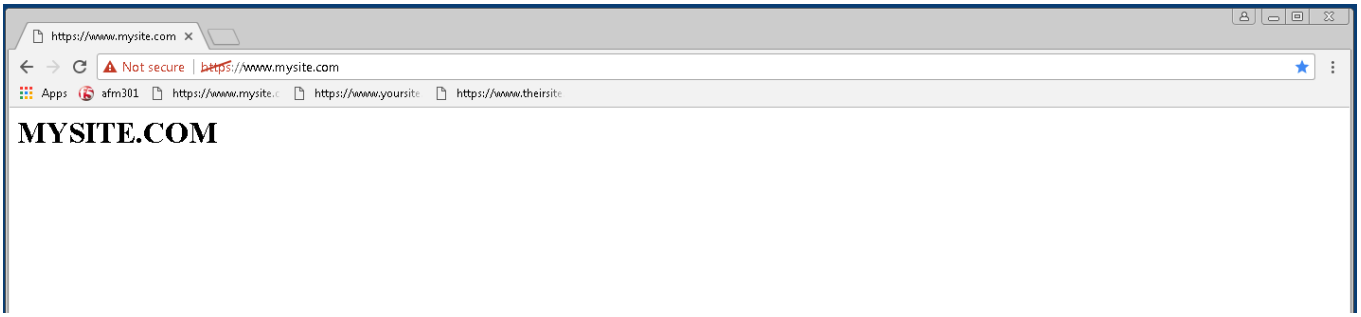
Validation: This lab is using self-signed certificates. You can either open a web browser on the test client or run CURL from the CLI to validate your configuration.

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

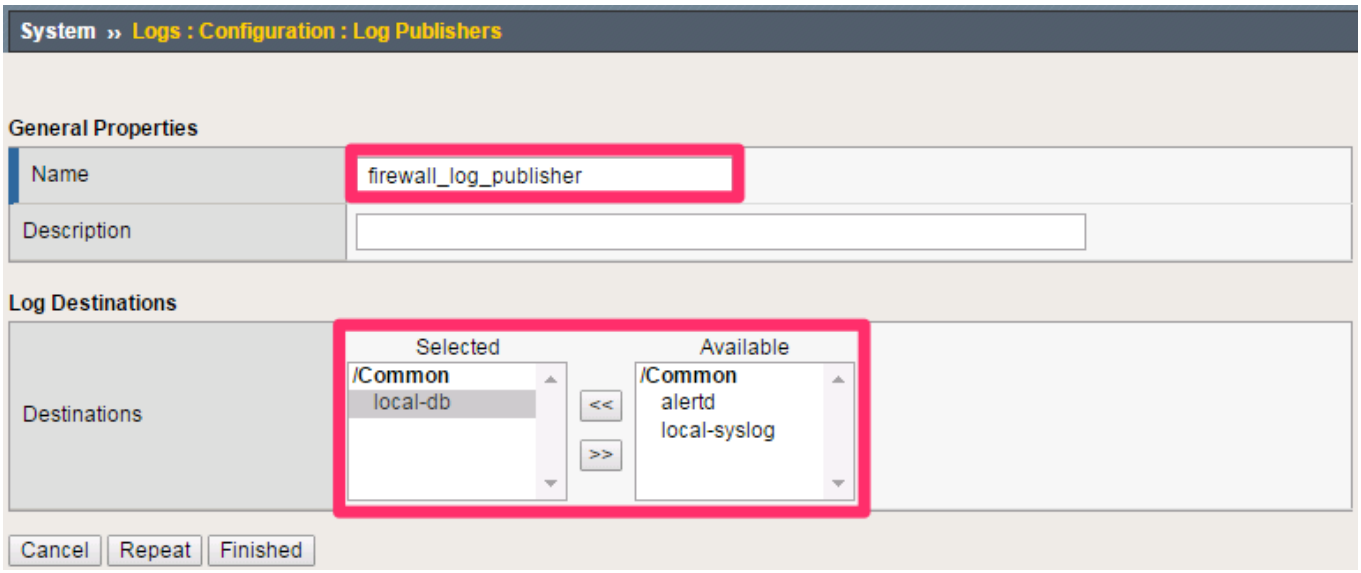
Security logging needs to be configured separately from LTM logging. In our lab, we will configure a local log publisher and log profile. The log profile will then be applied to the virtual server and tested.

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



Note: Leave all other fields using the default values.

Navigation: Click Finished

Create a log profile using the following information:

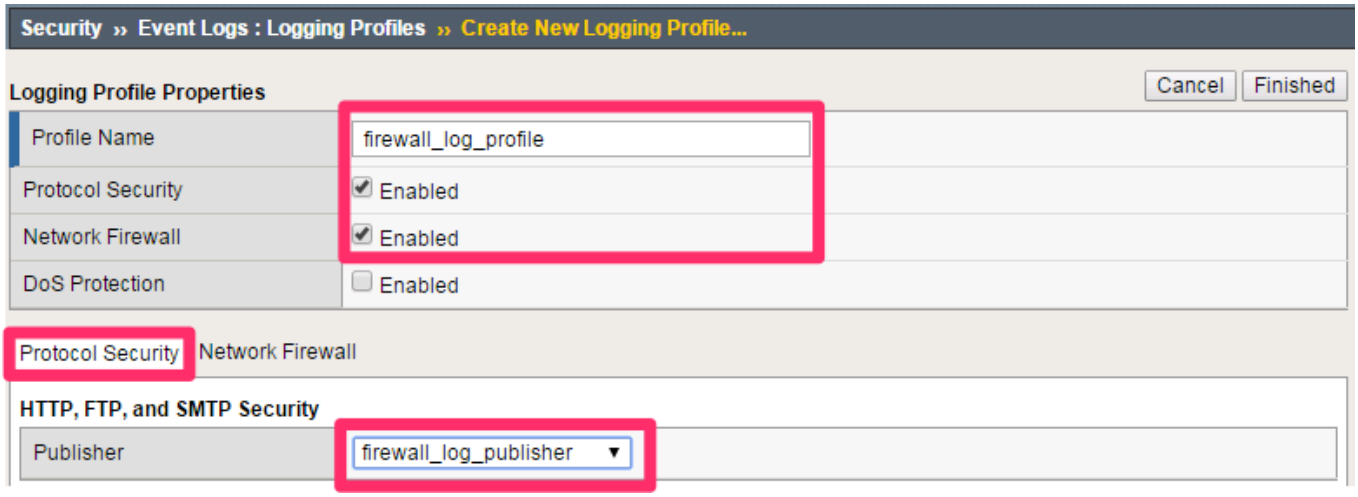
Navigation: Security > Event Logs > Logging Profiles, then click Create

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

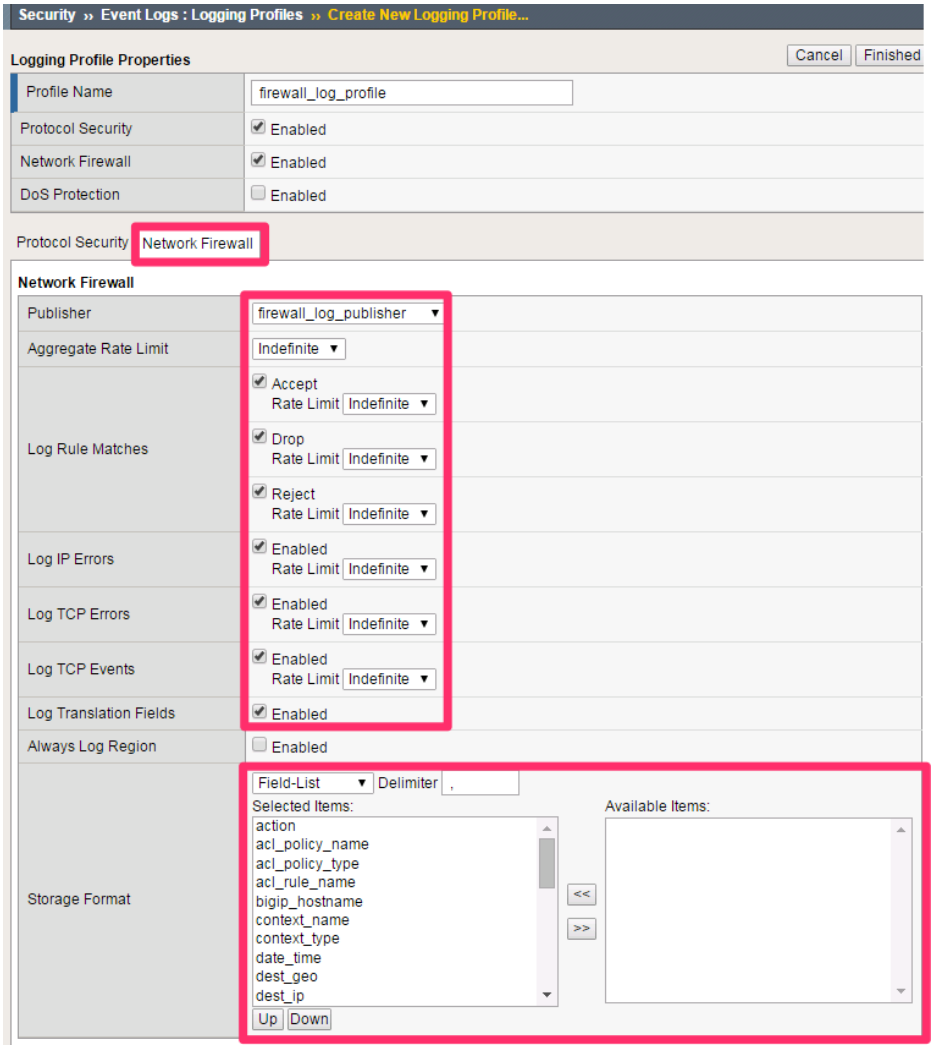


Note: Leave all other fields using the default values.

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)



Note: Leave all other fields using the default values.

Navigation: Click Finished

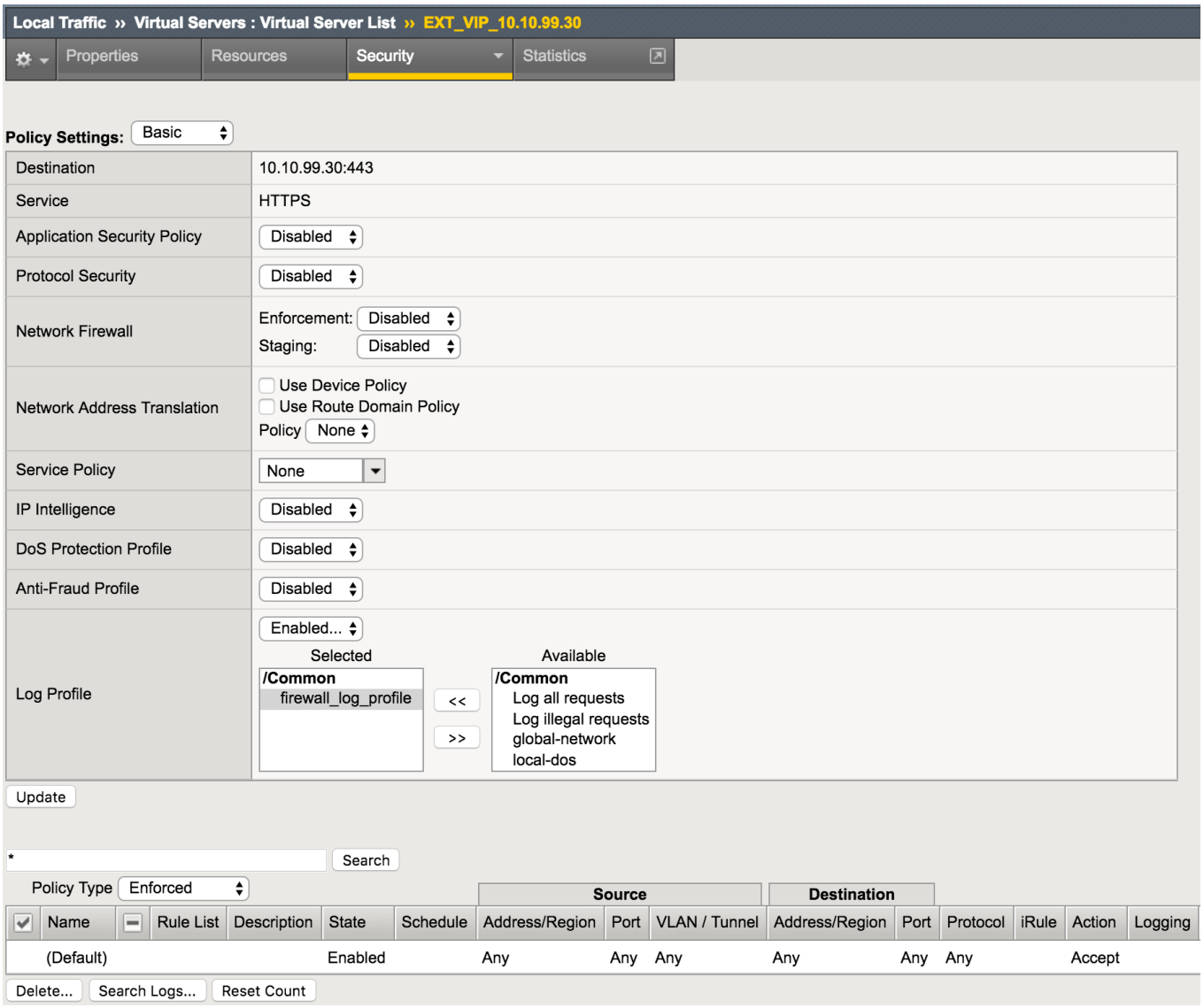
Apply the newly created log profile to the external virtual server created in the previous task.

Navigation: Local Traffic > Virtual Servers > Virtual Server List

Navigation: Click on EXT_VIP_10.10.99.30

Navigation: Security tab > Policies

Log Profile	firewall_log_profile

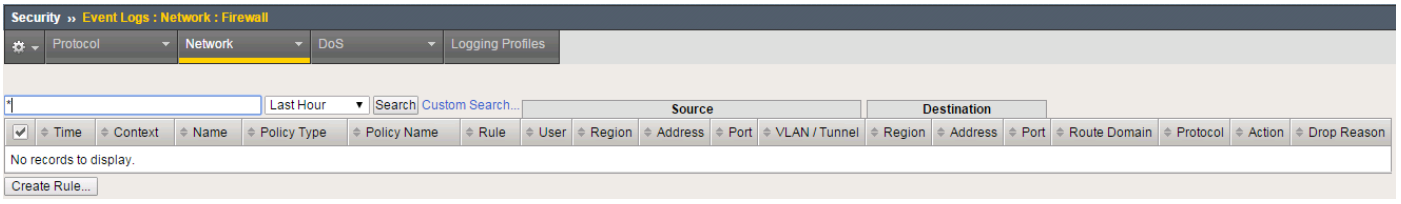


Note: Leave all other fields using the default values.

Navigation: Click Update

View empty network firewall logs.

Navigation: Security > Event Logs > Network > Firewall



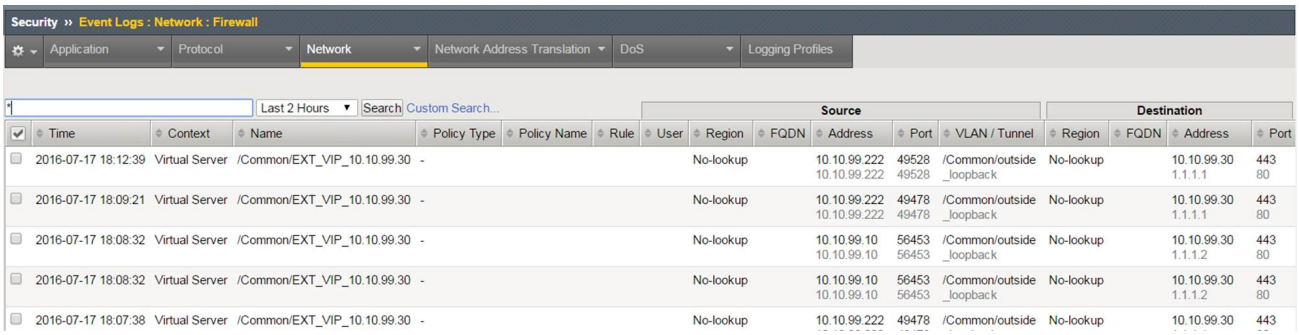
Open a new web browser tab and access the virtual server or repeat the curl statements from the previous sections.

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



Note: This is the end of task 3.

TASK 4 – Configure a network firewall policy and rules

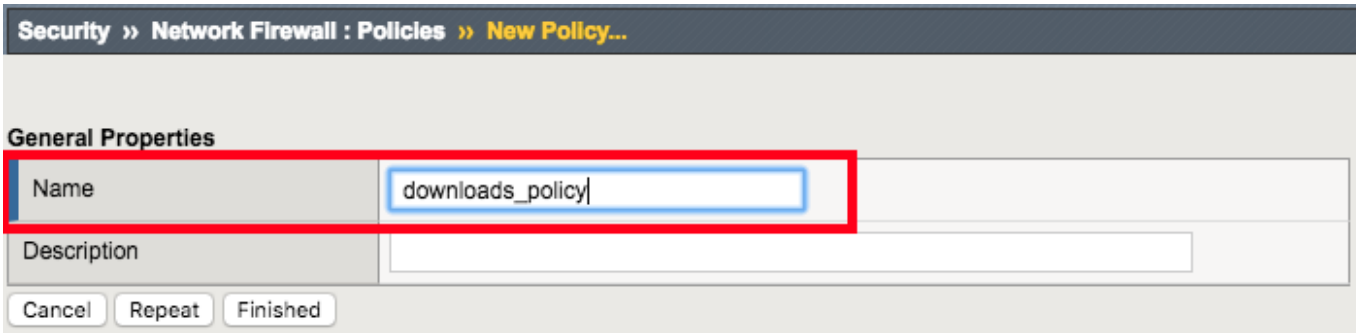
A network firewall policy is a collection of network firewall rules that can be applied to a virtual server. In our lab, we will create two policies, each of which includes two rules. This policy will then be applied to the appropriate virtual servers and tested.

On BIG-IP

Create Network Firewall Policy

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

Name	downloads_policy

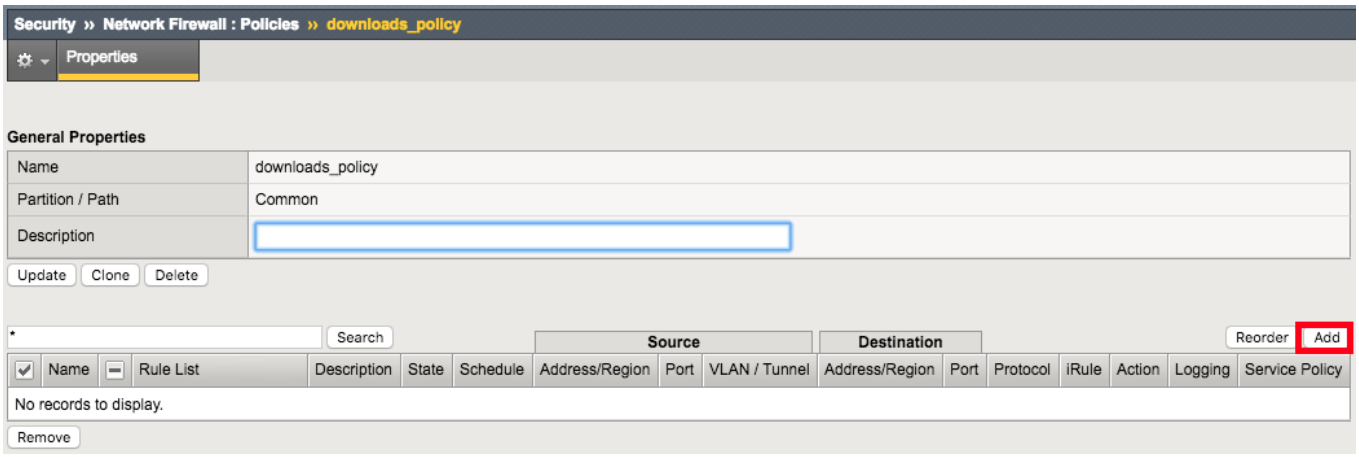


Note: Leave all other fields using the default values.

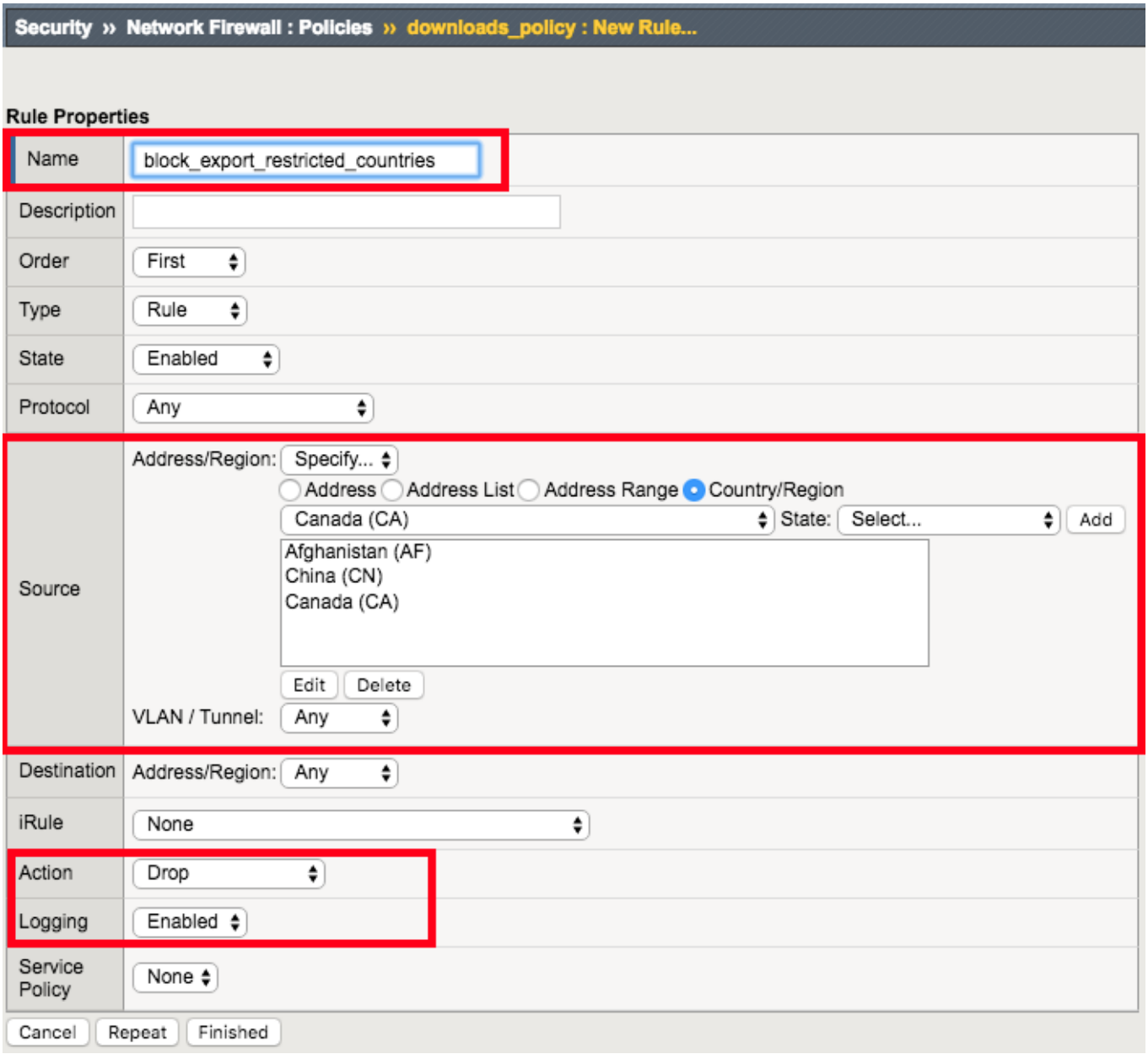
Navigation: Click Finished

Create an IP Drop Network Firewall Rule

Navigation: Click Add



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

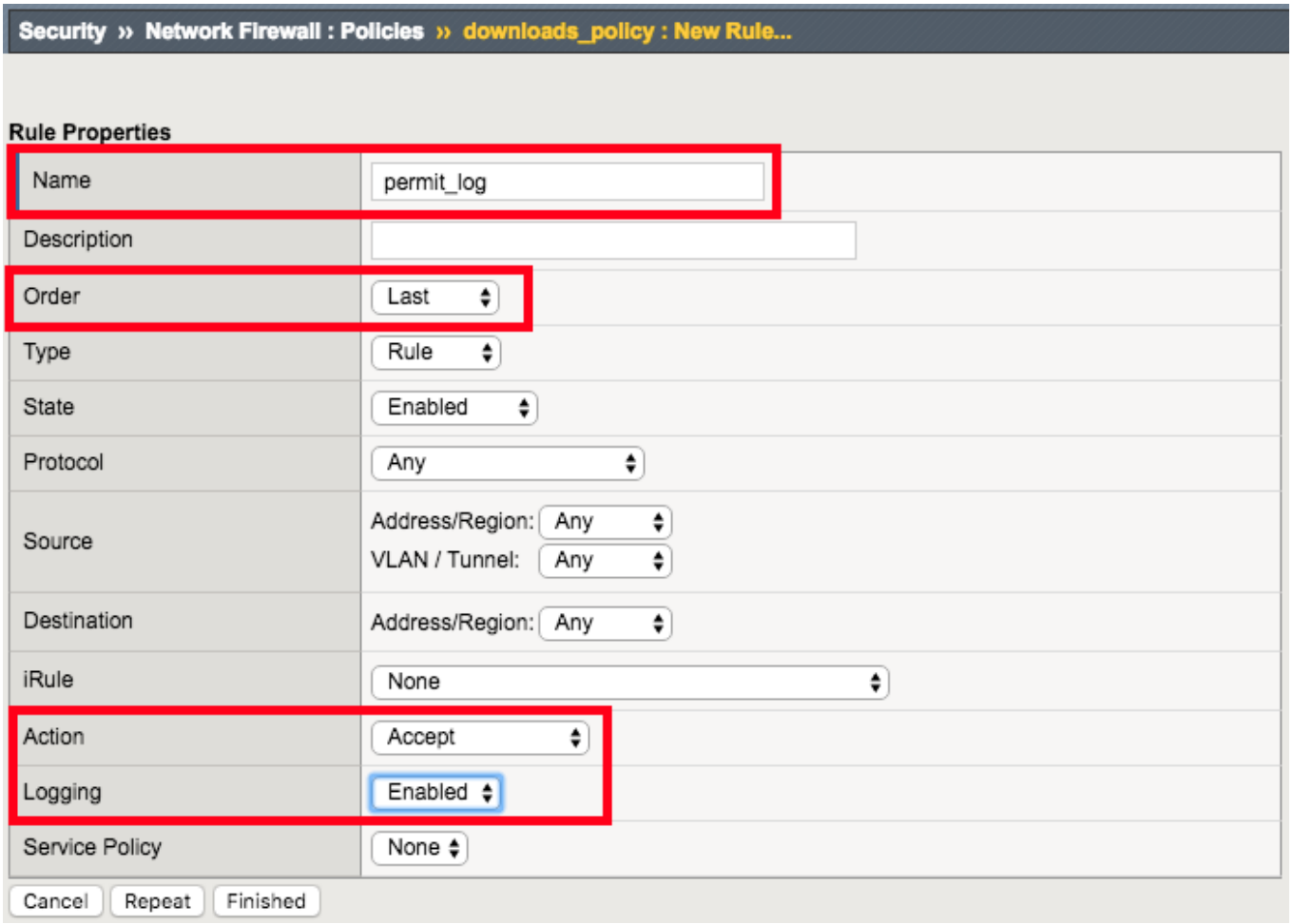


Note: Leave all other fields using the default values.

Navigation: Click Finished

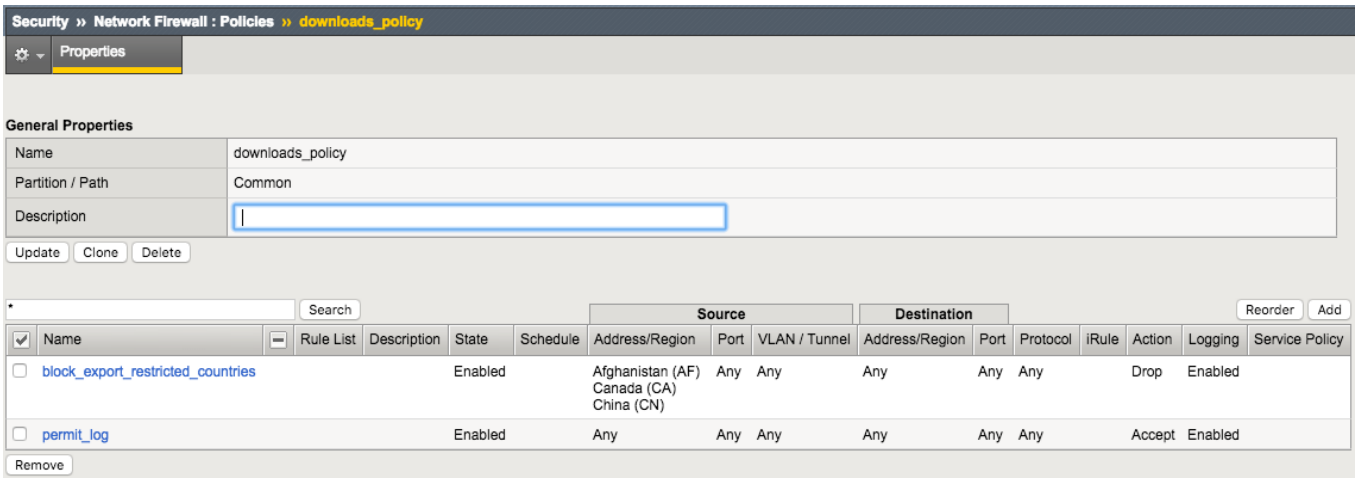
Name	permit_log
Order	Last
Action	Accept
Logging	Enabled

Create Permit Log Network Firewall Rule



Note: Leave all other fields using the default values.

Navigation: Click Finished



From client machine

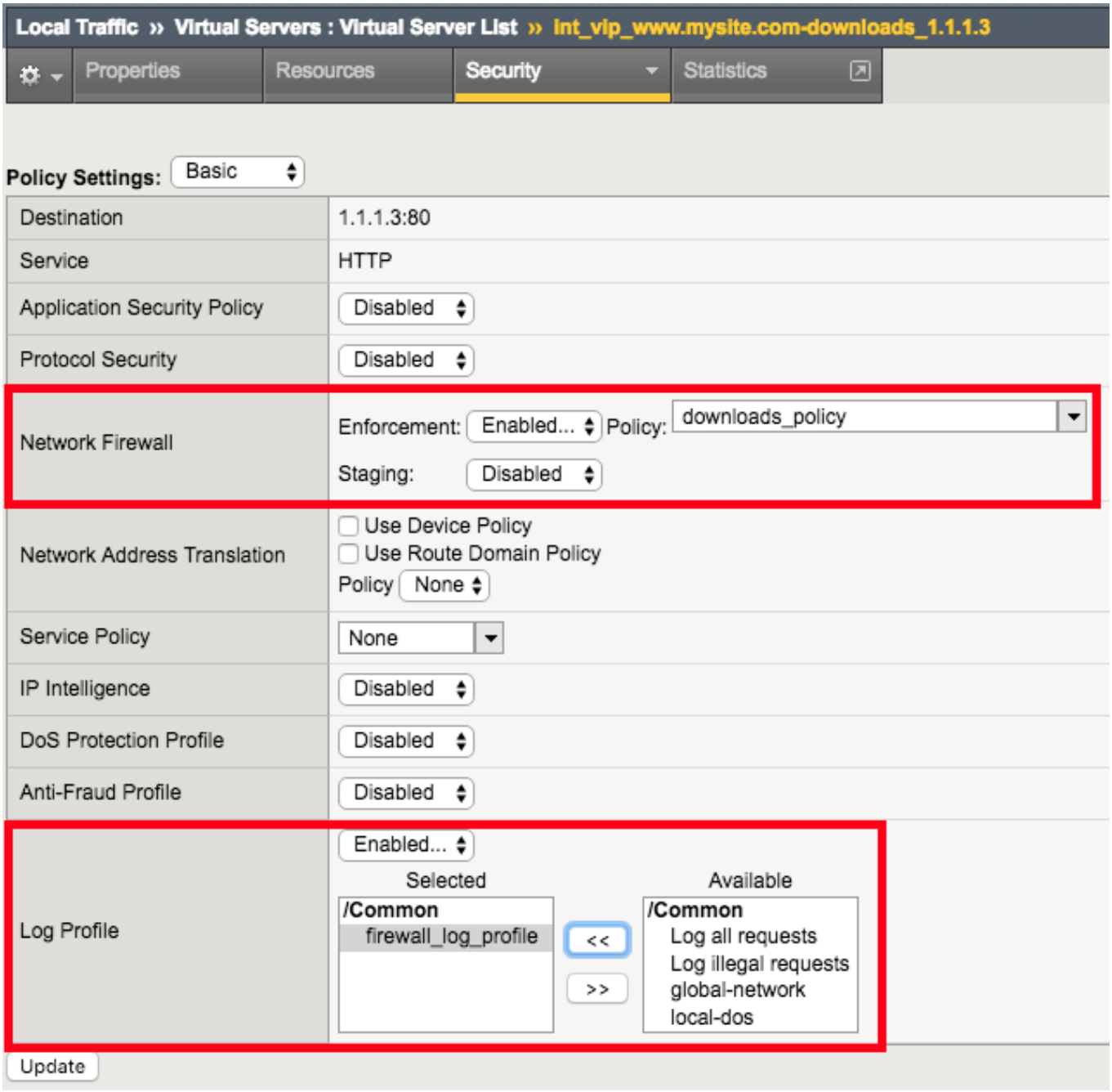
URL: https://www.mysite.com/downloads/

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



Note: Leave all other fields using the default values.

Navigation: Click Update

From client machine

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

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

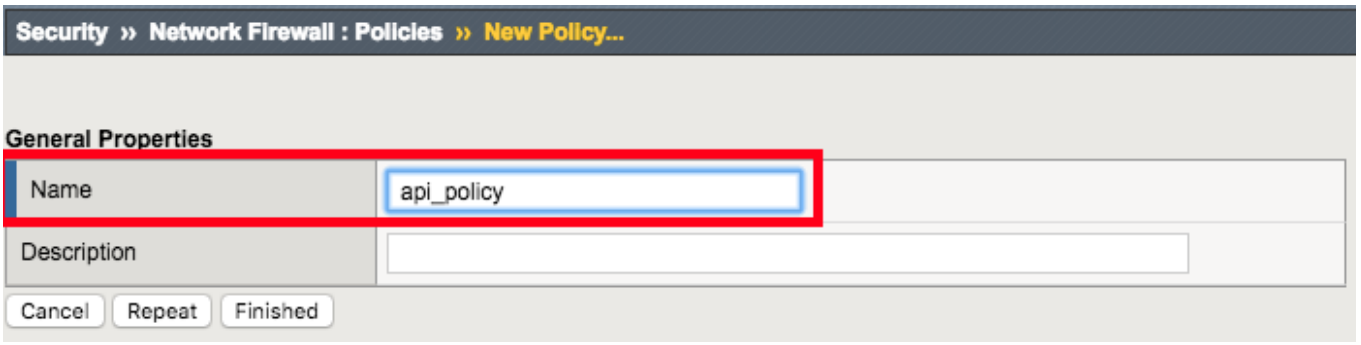
after applying the policy. We will get into testing the block later.

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

Name	api_policy

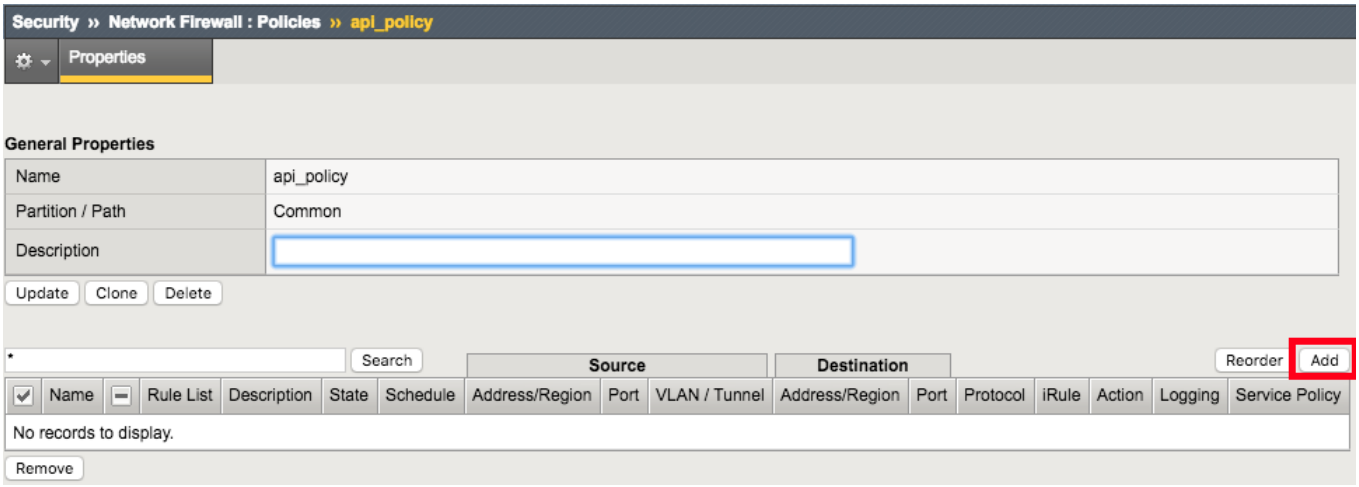


Note: Leave all other fields using the default values.

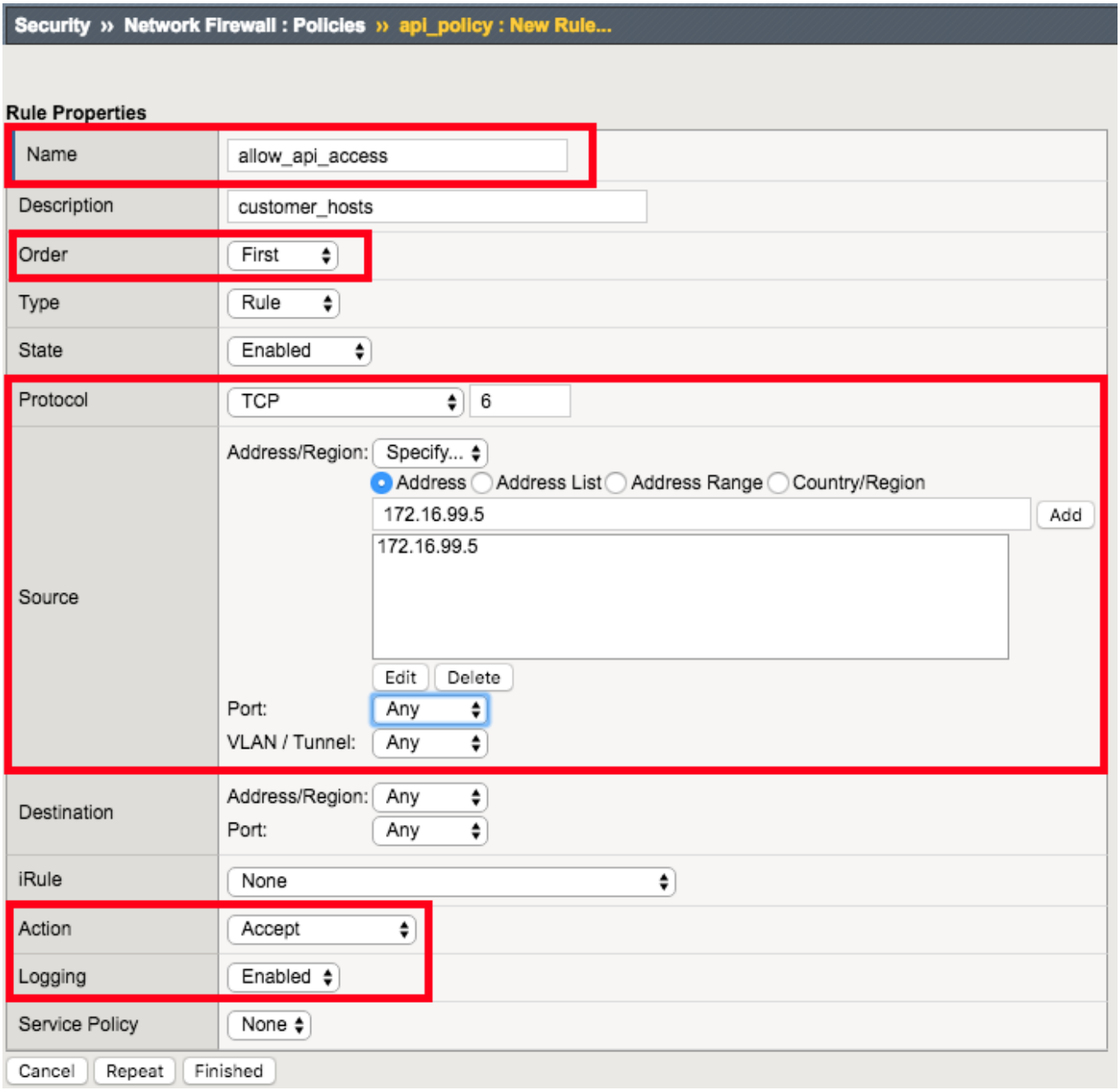
Navigation: Click Finished

Create Allow TCP Port 80 From Host 172.16.99.5 Network Firewall Rule

Navigation: Click Add



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



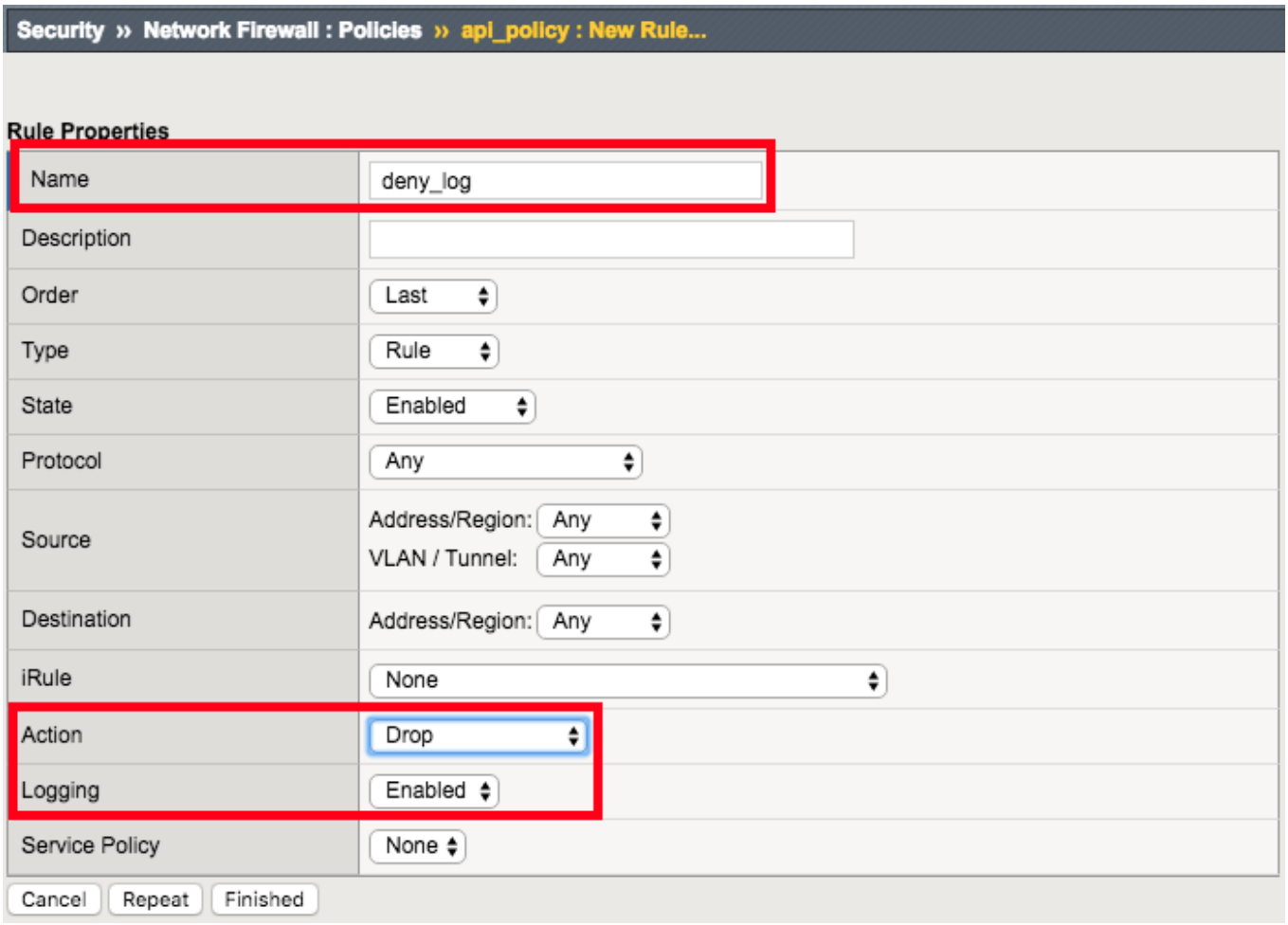
Note: Leave all other fields using the default values.

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

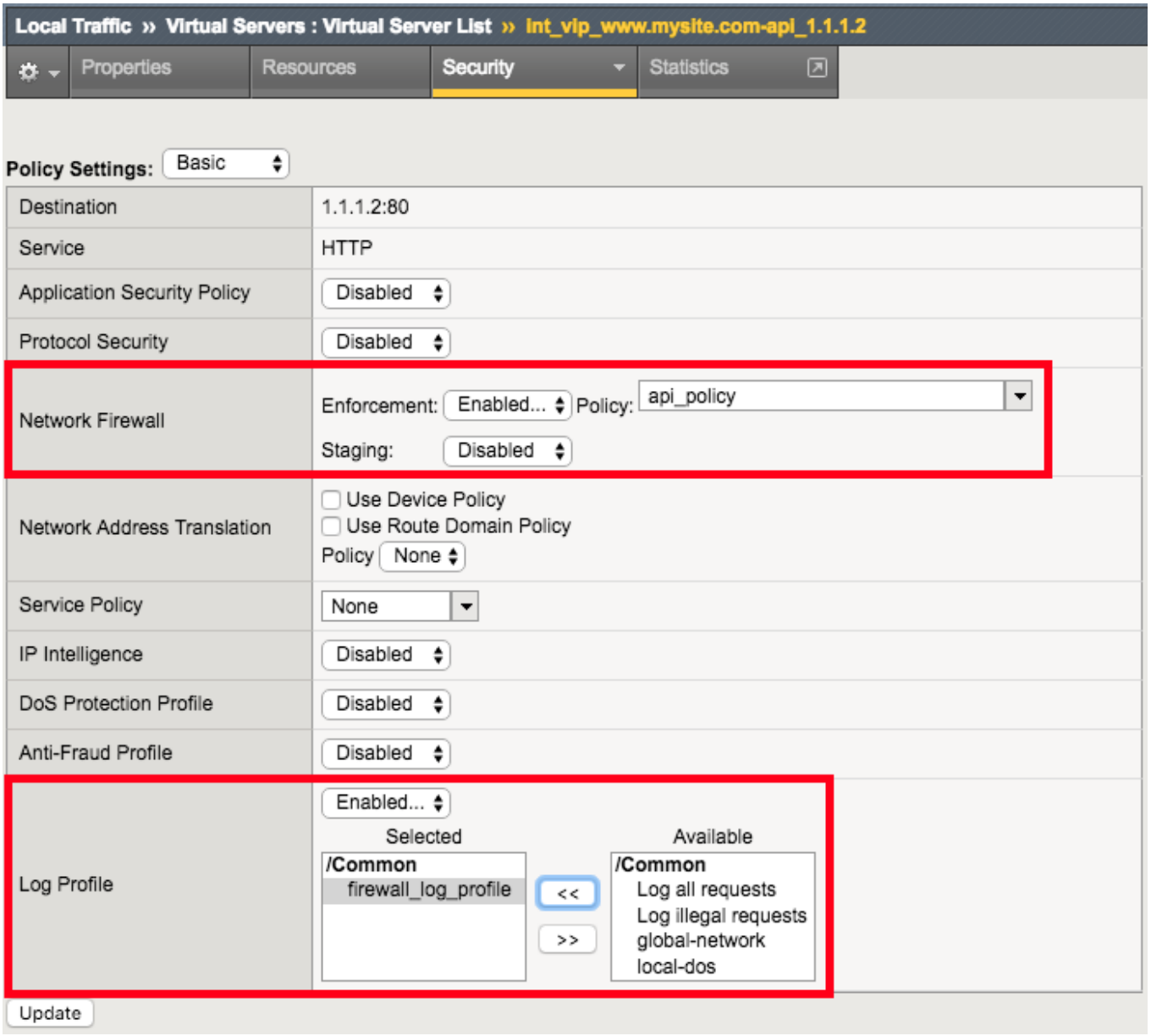


Note: Leave all other fields using the default values.

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

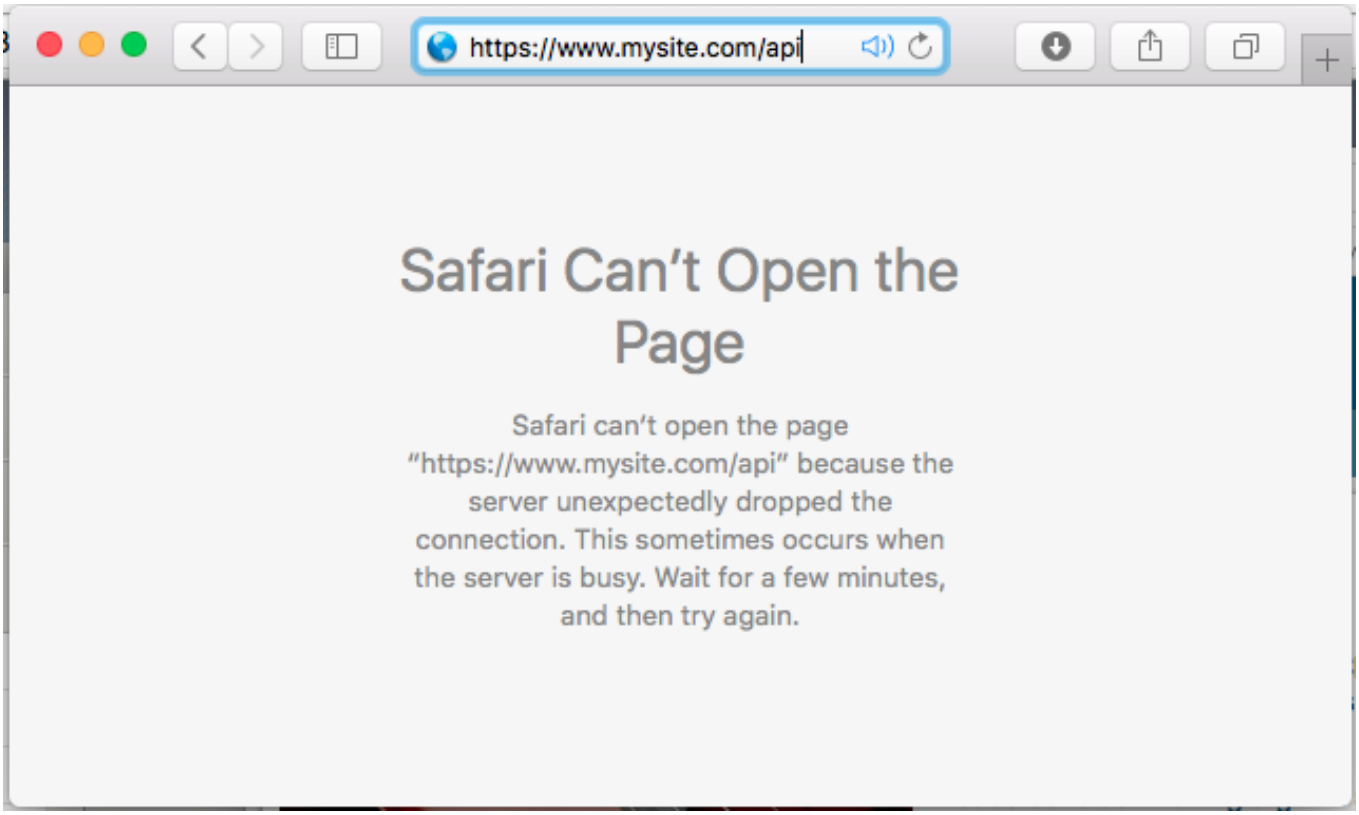


Note: Leave all other fields using the default values.

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

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

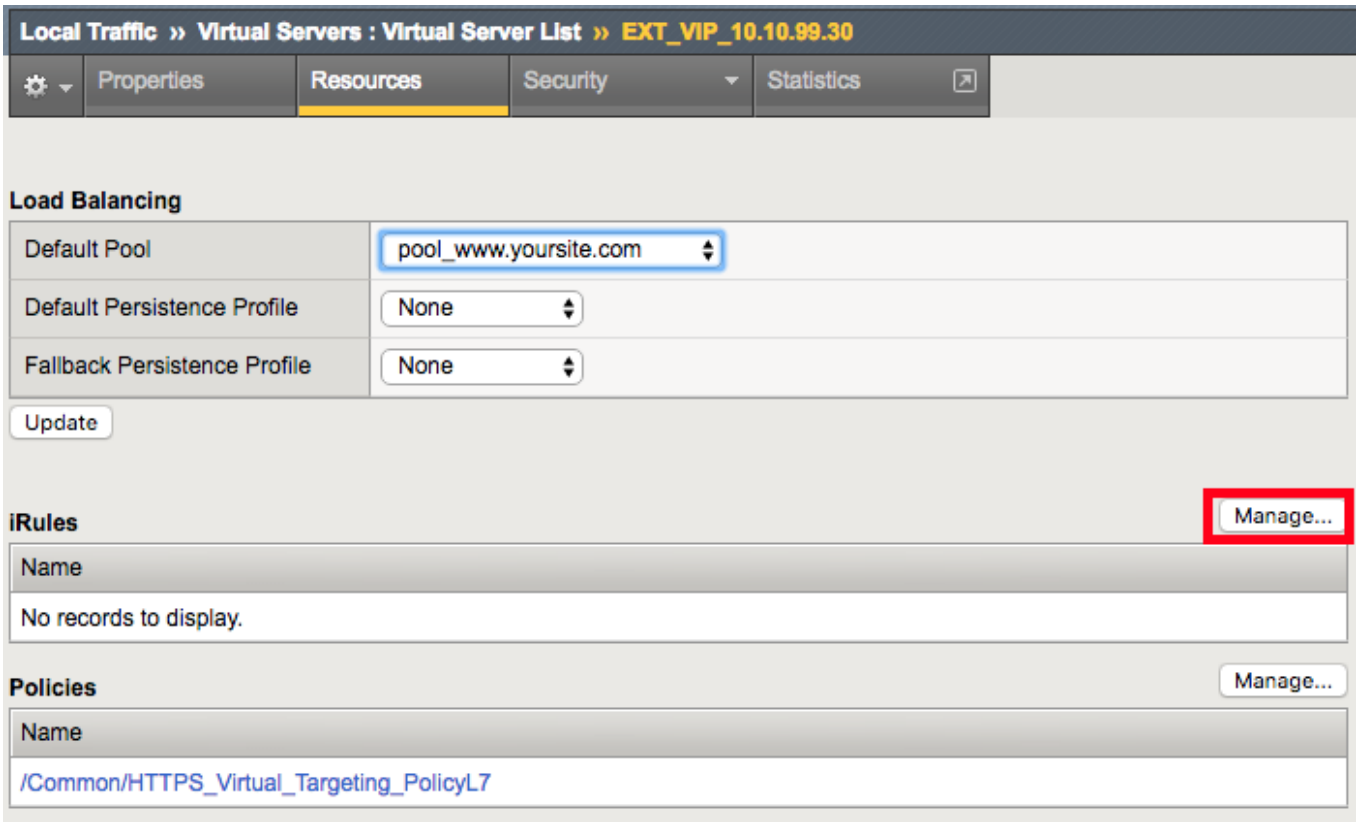
The iRule to accomplish this is already installed on your BIG-IP. We need to apply it the External Virtual Server. Here is a sample of the iRule.

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

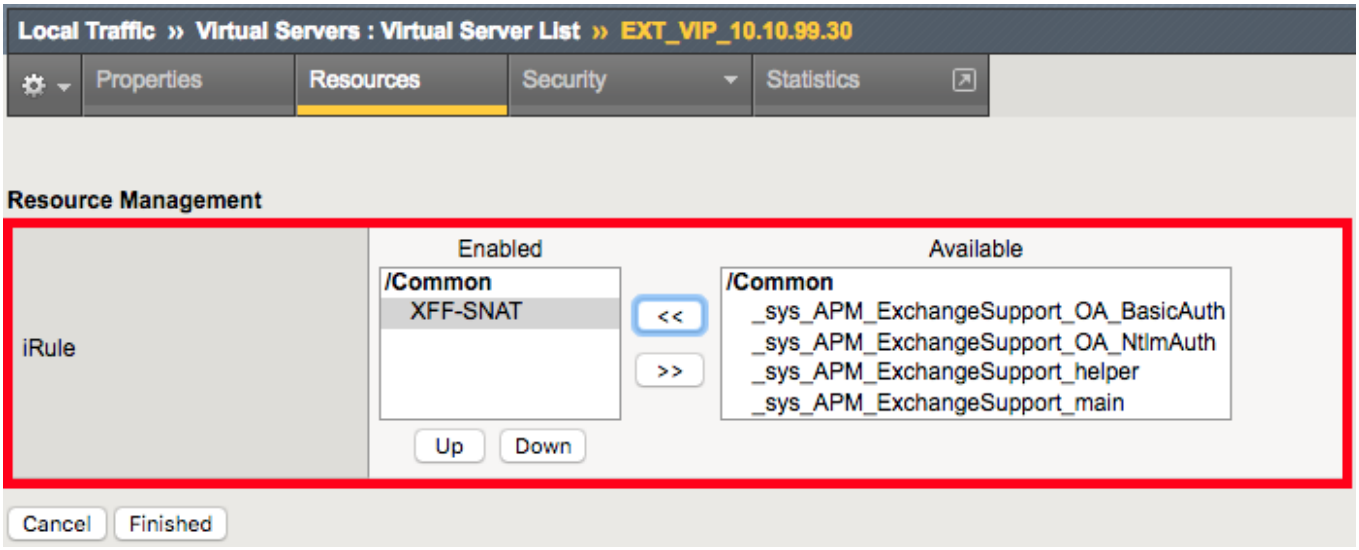
```
    }
}
```

Apply the iRule to the Virtual Server

Navigation: *Click on the* EXT_VIP_10.10.99.30 *virtual server*



Navigation: Click Manage under the iRule section



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

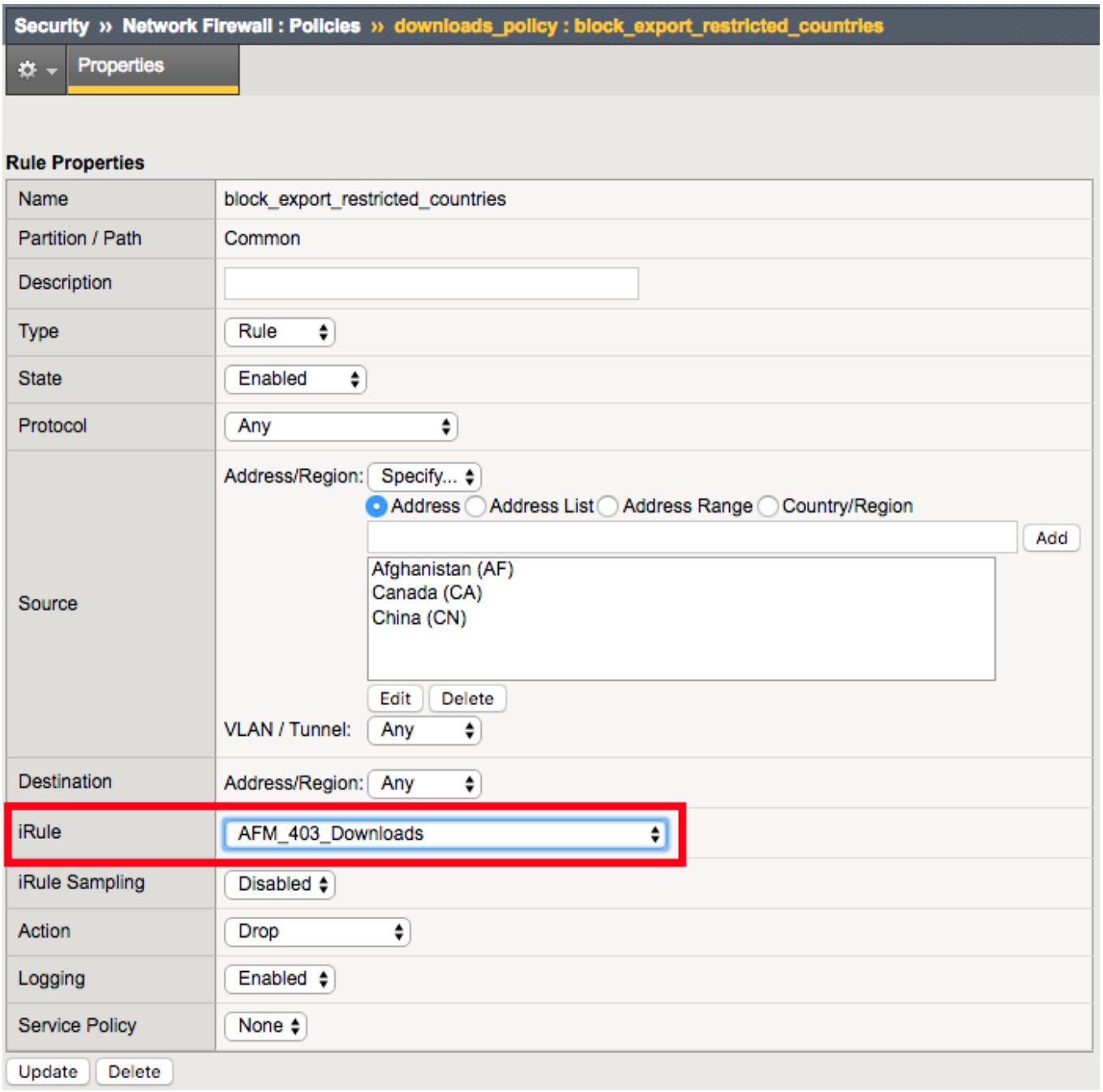
Validate that requests sourced from the X-Forwarded-For IP address of 172.16.99.5 are now allowed.

```
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.



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

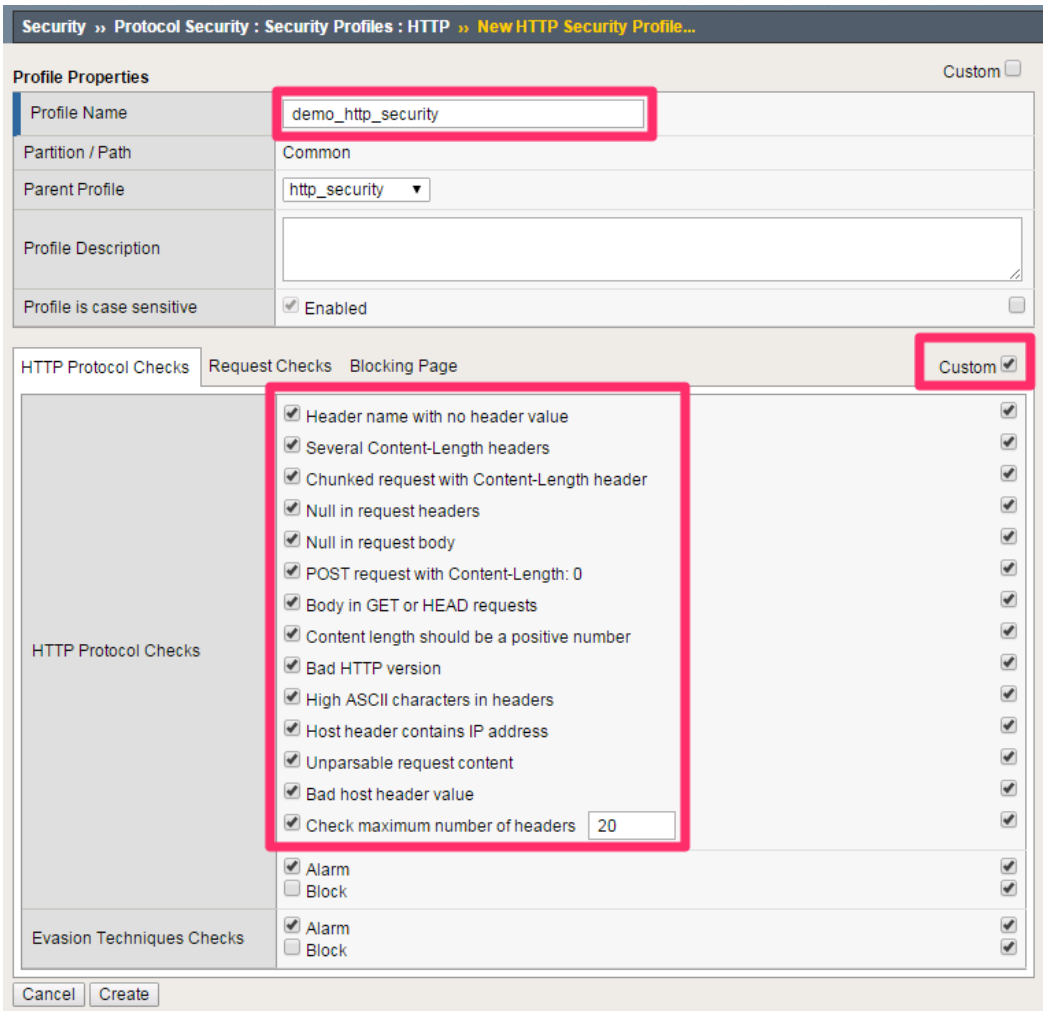
HTTP security profiles are used to apply basic HTTP security to a virtual server. Significantly more advanced HTTP security is available by adding ASM (Application Security Manager).

On BIG-IP

Configure a HTTP security profile.

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

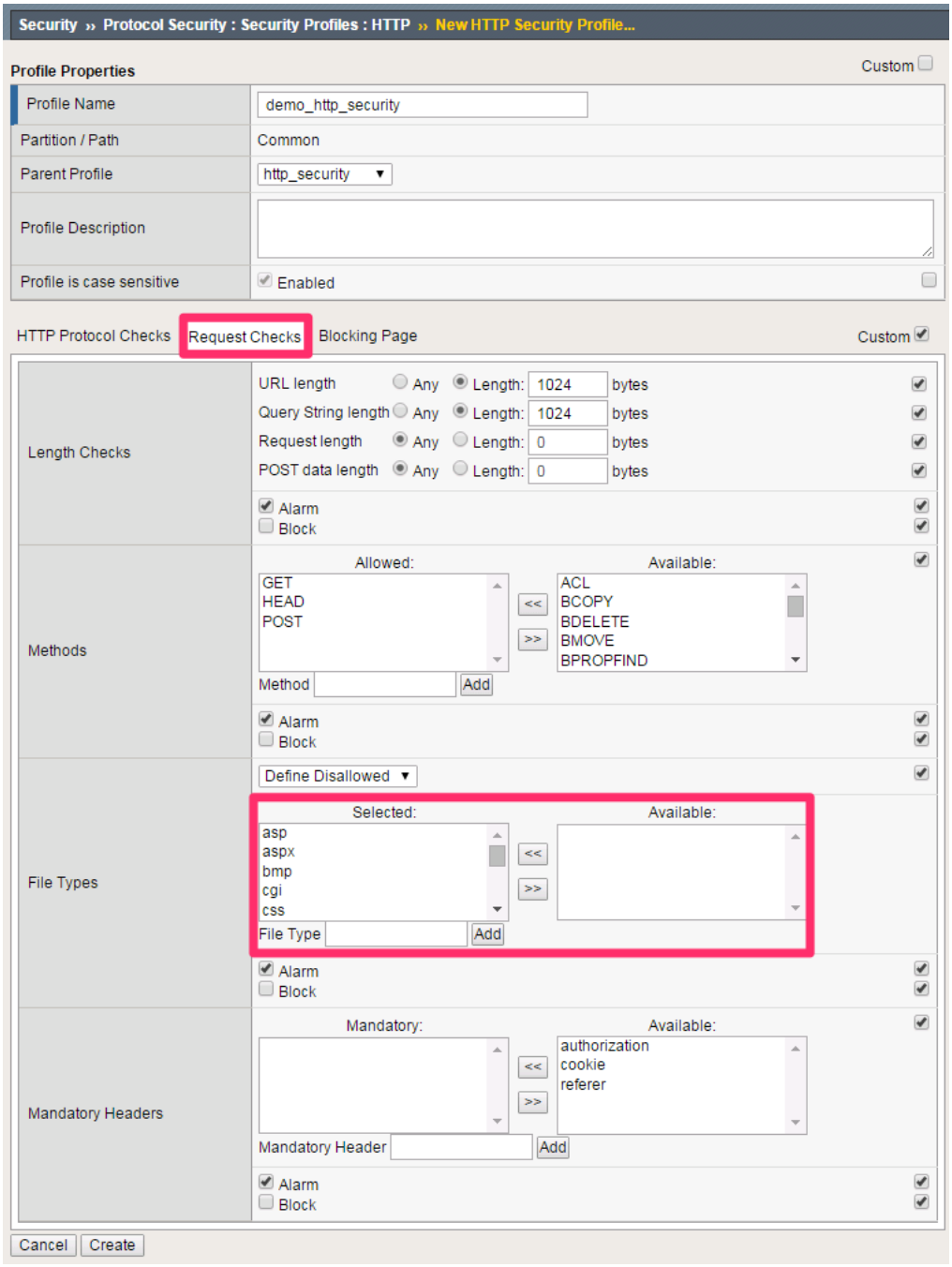
Profile Name	demo_http_security
Custom	Checked
Profile is case sensitive	Checked
HTTP Protocol Checks	Check All



Note: Leave all other fields using the default values.

Navigation: Click Request Checks Tab.

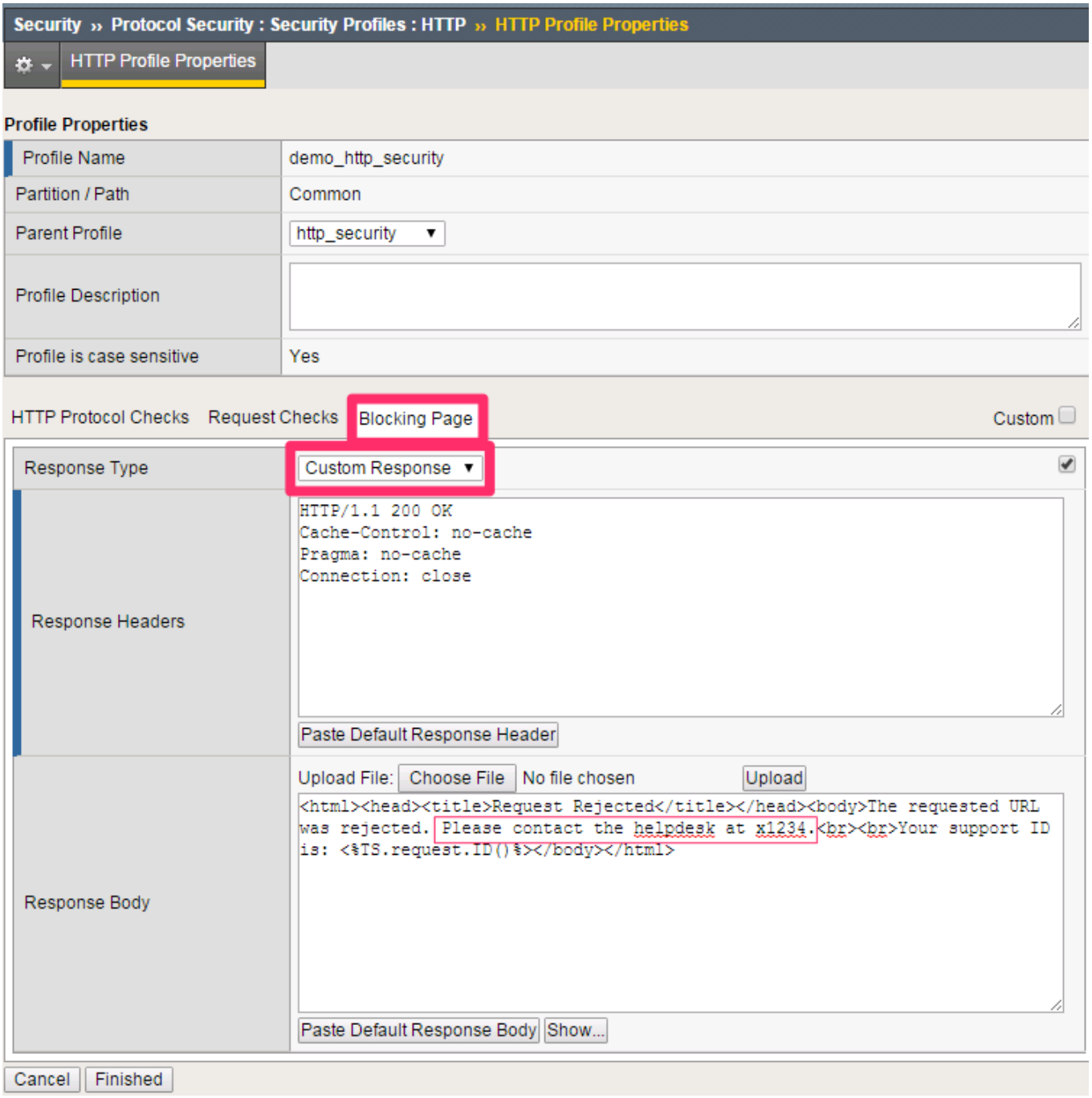
File Types	Select All



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



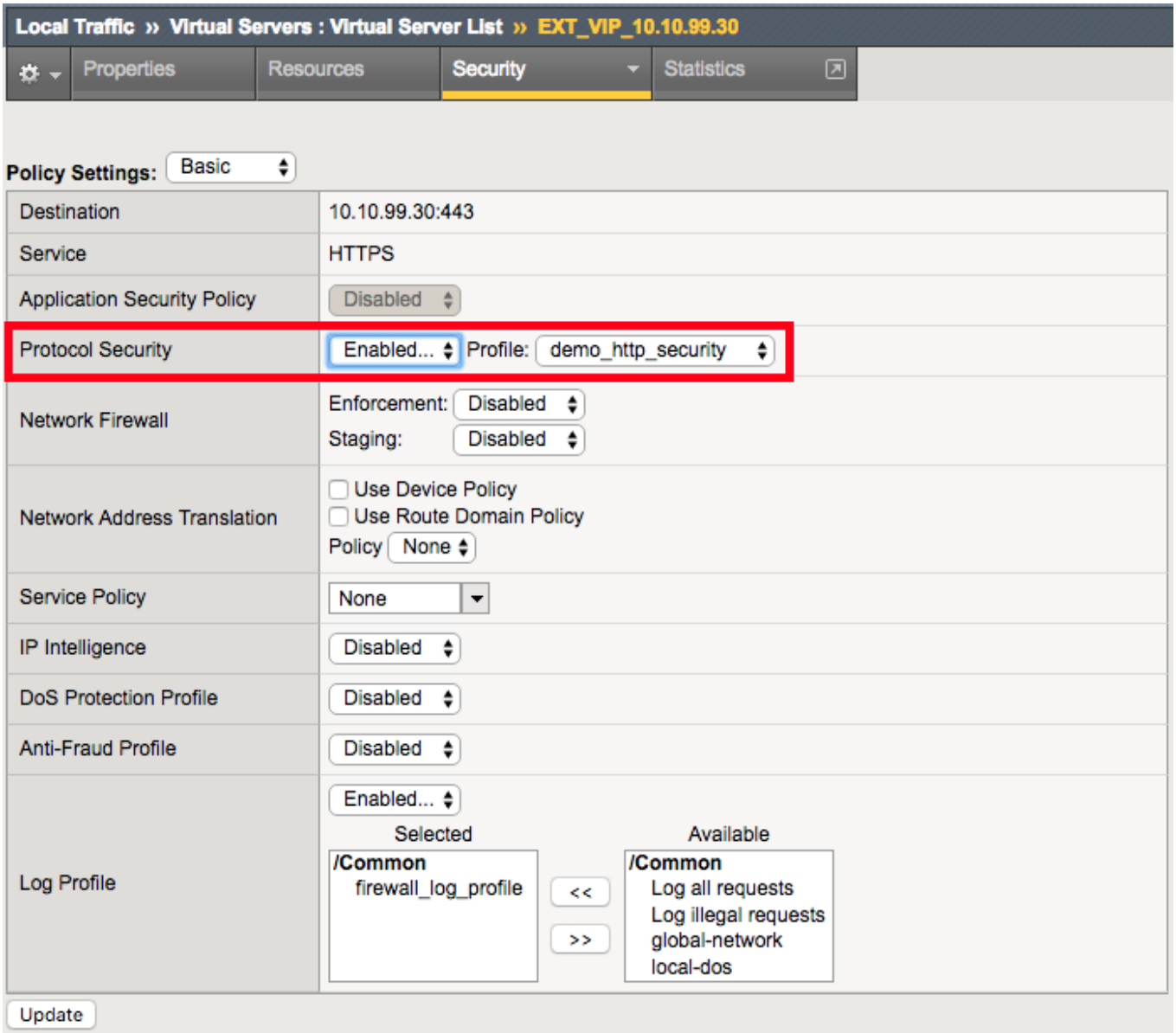
Note: Leave all other fields using the default values.

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



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.

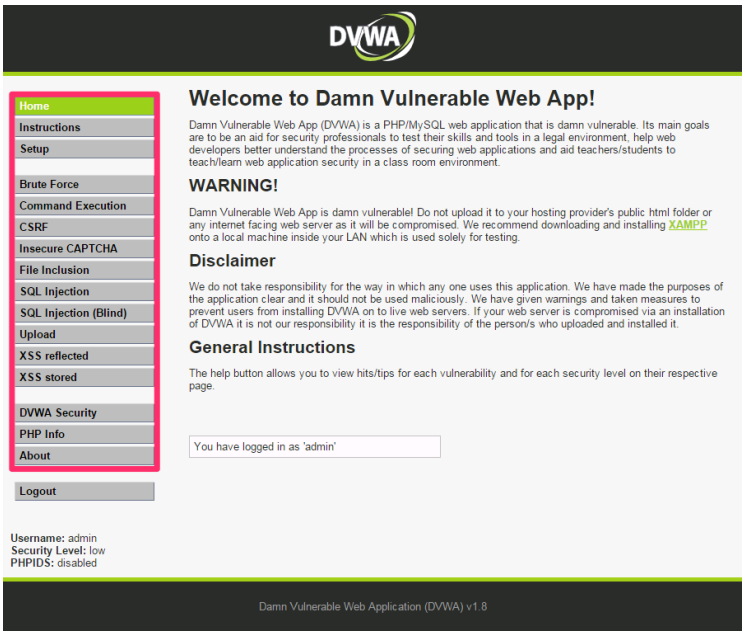
URL: https://www.mysite.com/dvwa

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.

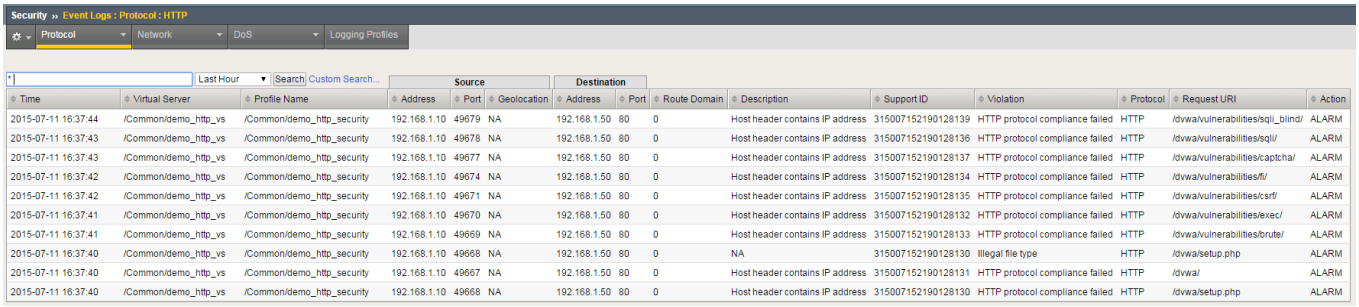


Note: This traffic will generate network firewall log entries because the “Alarm” option in the HTTP security policy is selected.

On BIG-IP

Review the log entries created in the previous step.

Navigation: Security > Event Logs > Protocol > HTTP

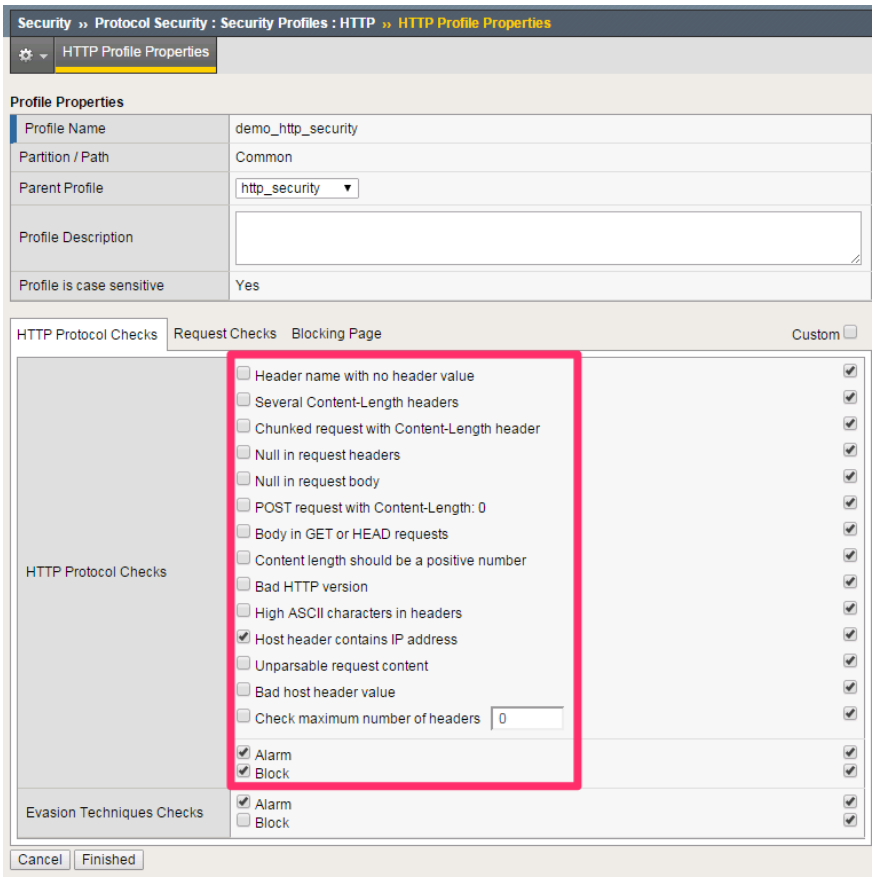


Note: Your log entries may be different than the example shown above.

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”



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

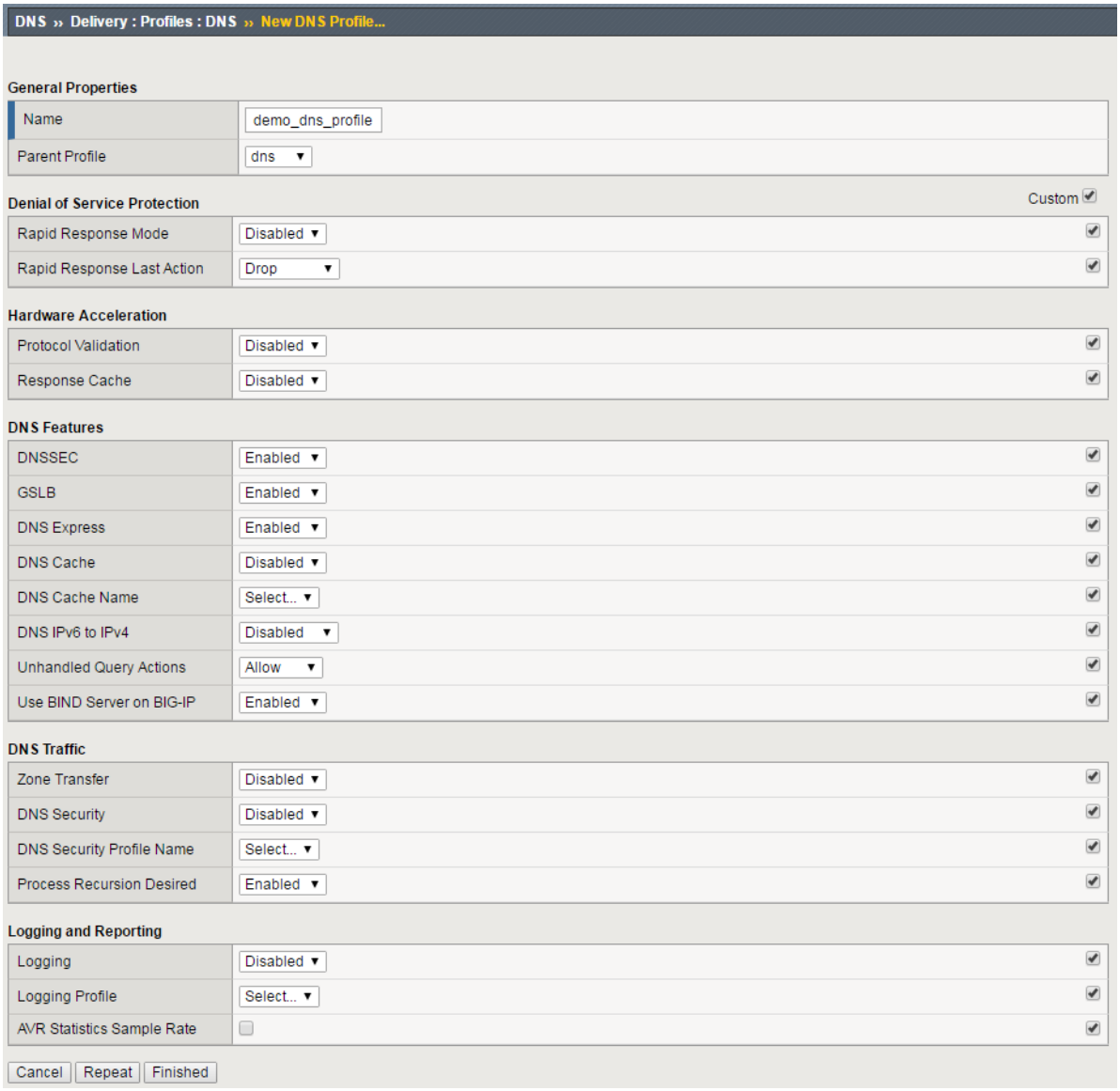
Since the BIG-IP is terminating SSL on the external virtual server, when we forward the traffic to the secondary virtual server in clear-text we have an opportunity to make an unencrypted copy of the application traffic and send it to an external sensor such as an IDS for further security assessment.

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	*



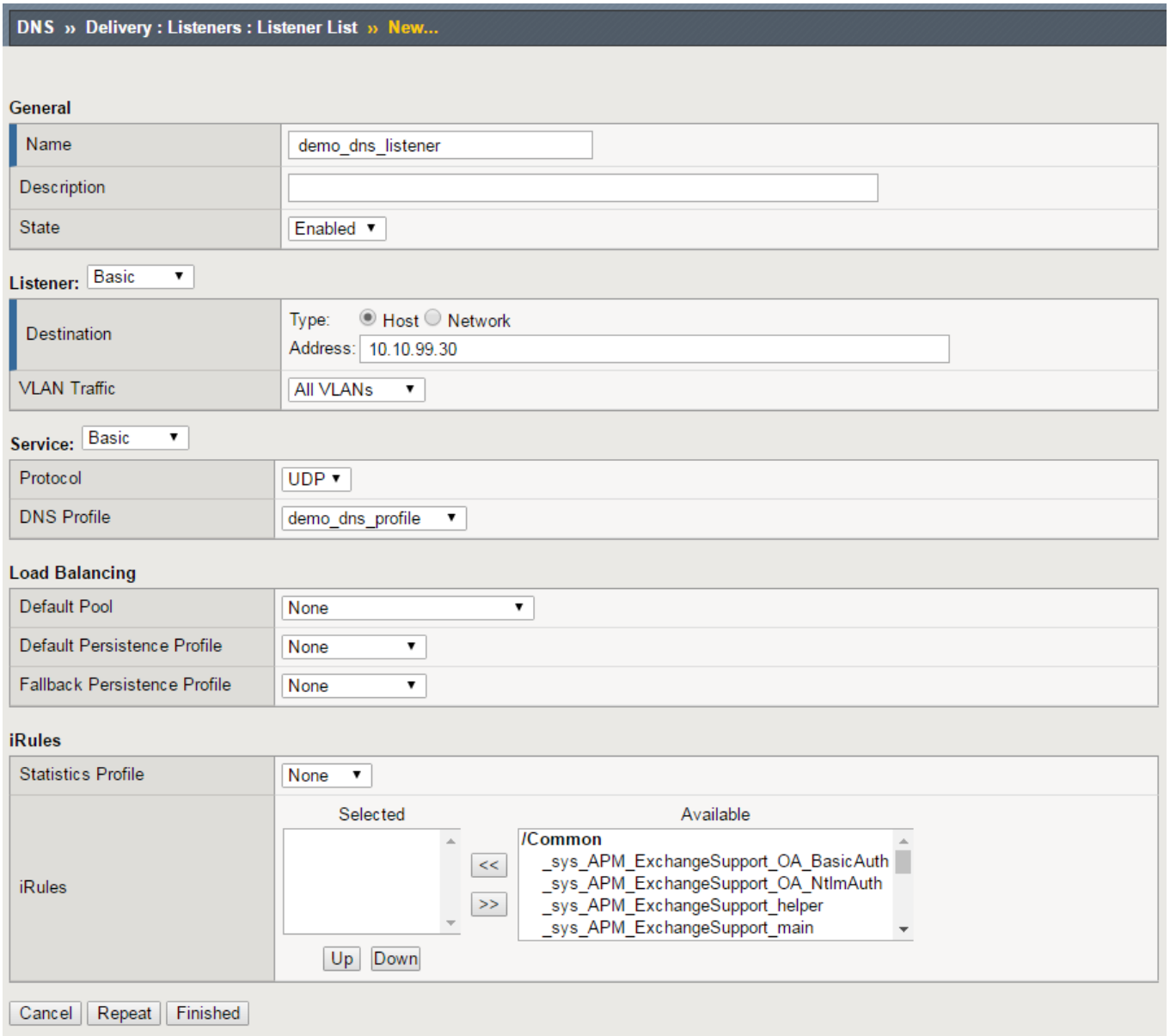
Note: Leave all other fields using the default values.

Navigation: Click Finished.

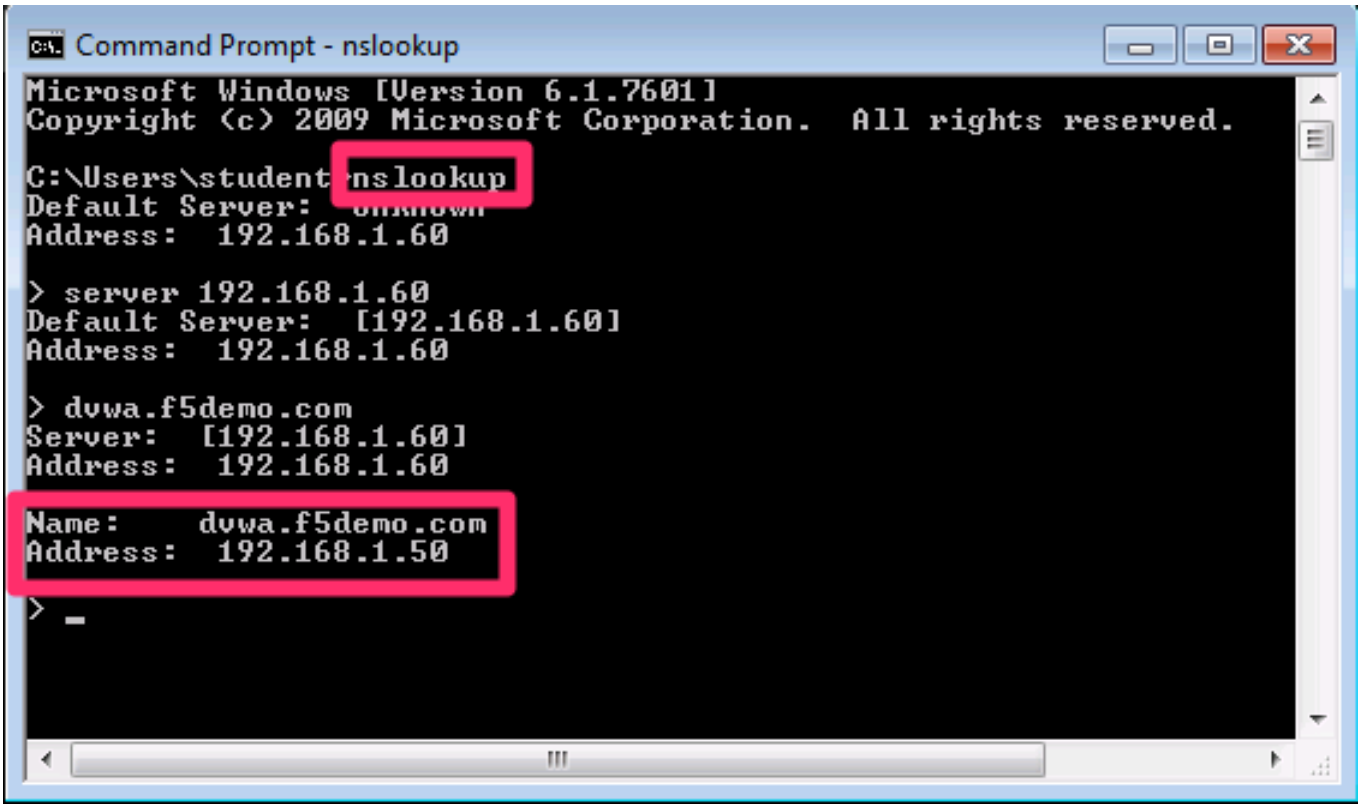
Attach the *IDS_Pool* as a clone pool to the server side of the external virtual server

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

Navigation: Configuration > Advanced.



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



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

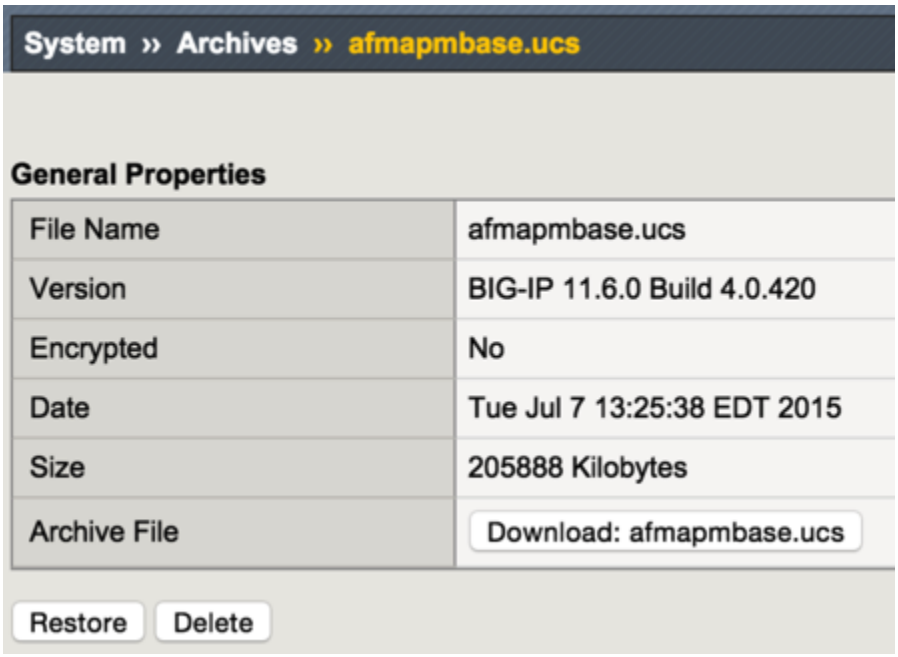
TASK 1 – Create APM connectivity profile

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

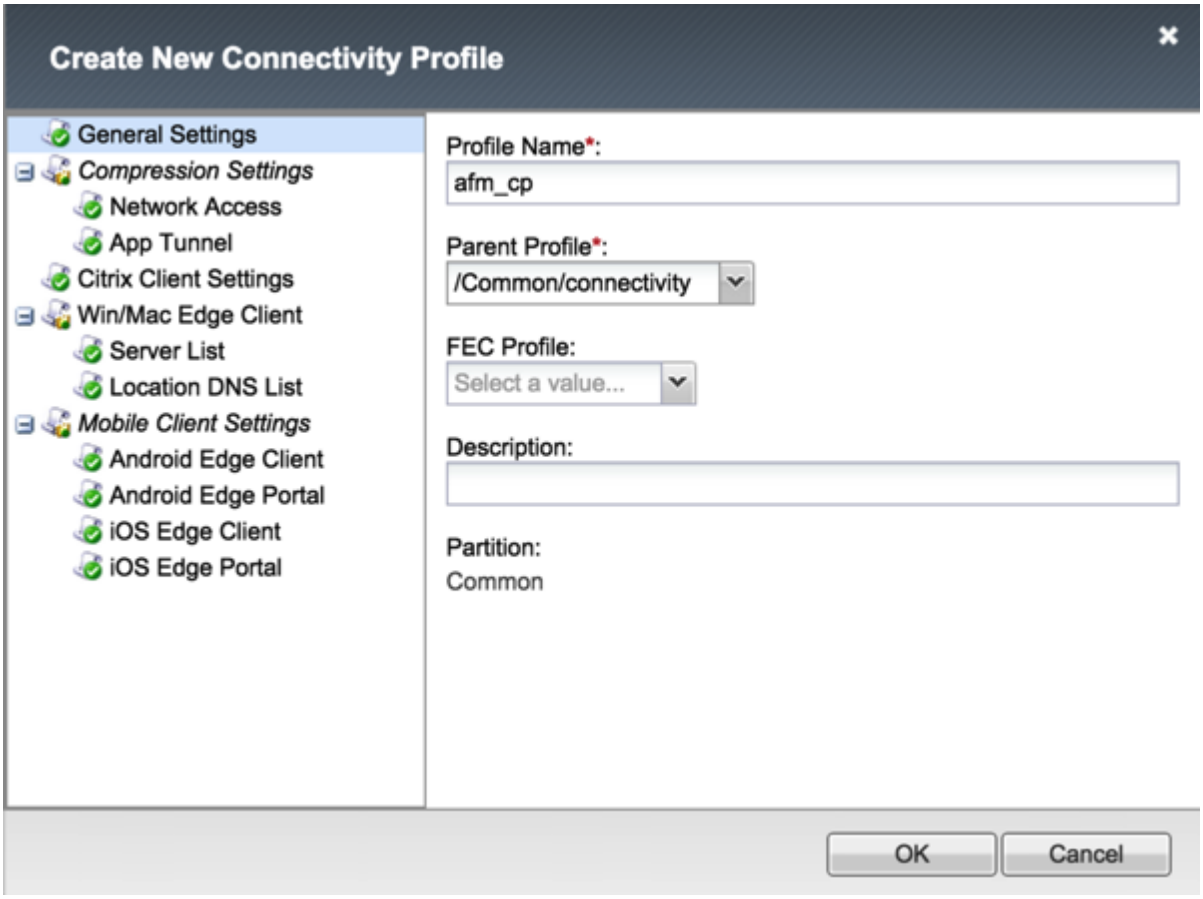
```
tcpdump -ni afm_cp
```



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**

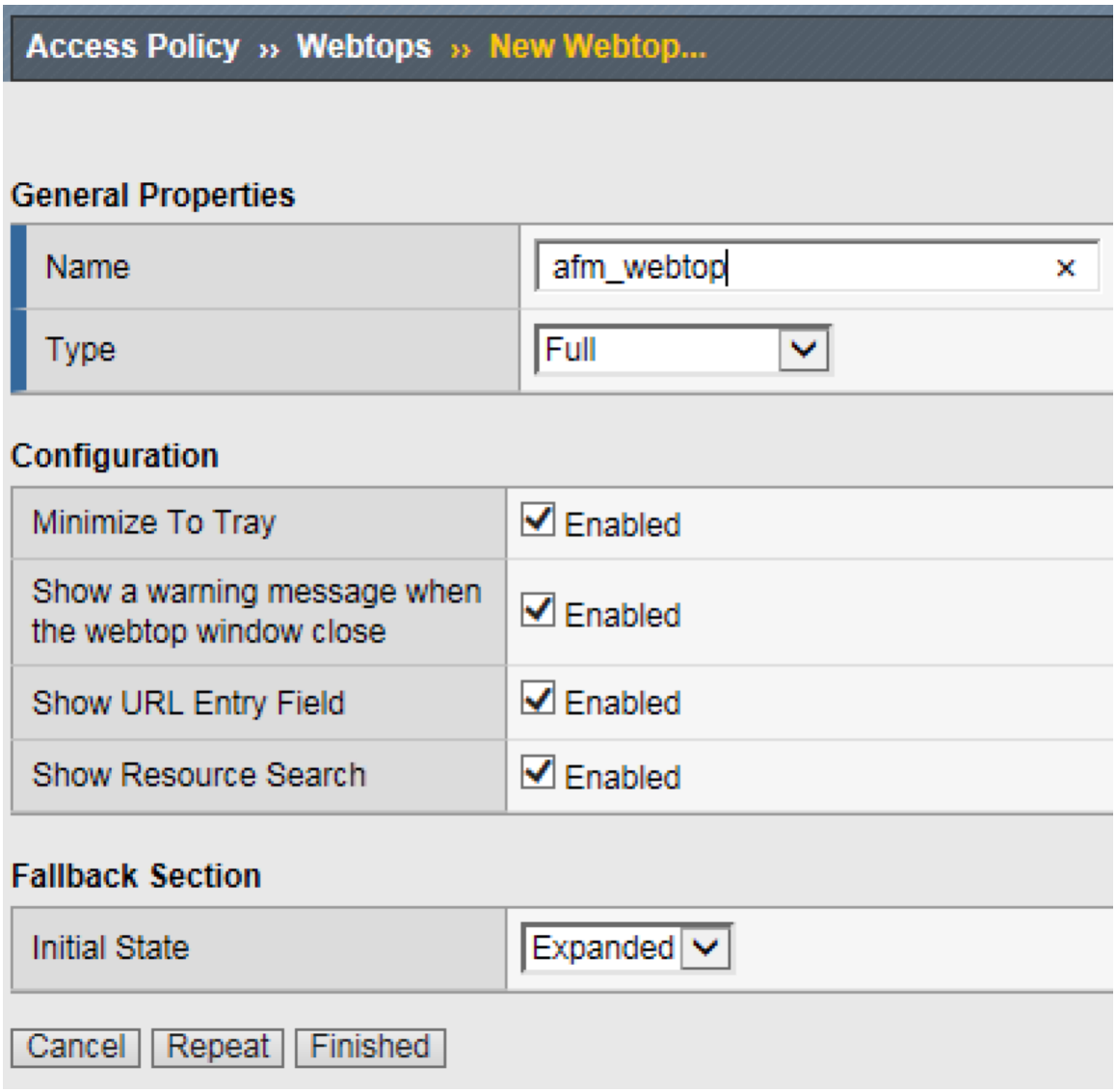


TASK 2 – Create APM access profile

Create a APM webtop

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

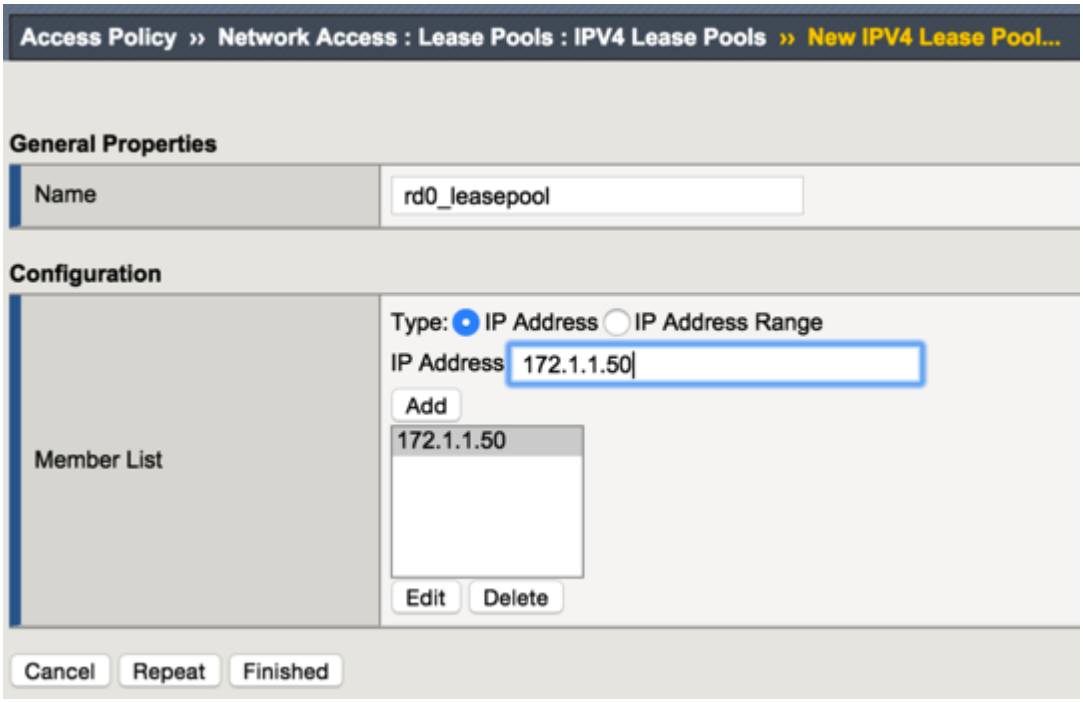
- Name: `afm_webtop`
- Type: `Full`
- Click **Finished**



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

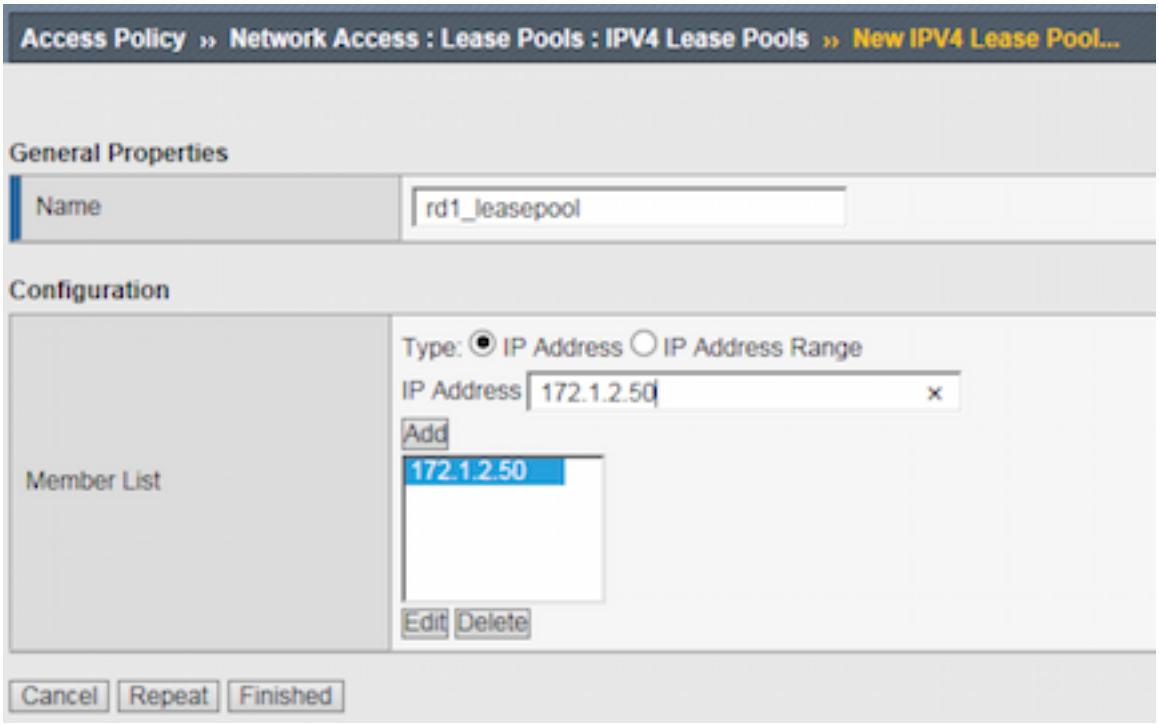
- Name: `rd0_leasepool`
- Type: `IP Address`
- IP Address: `172.1.1.50`
- Click **Add**
- Click **Finished**



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

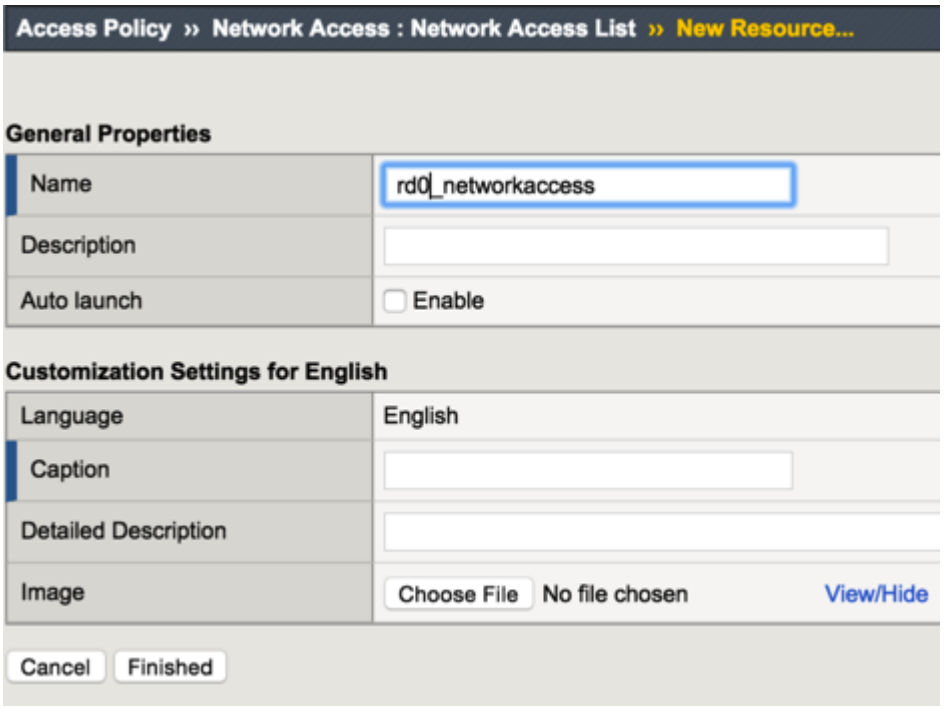
- Name: `rd1_leasepool`
- Type: `IP Address`
- IP Address: `172.1.2.50`
- Click **Add**
- Click **Finished**



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

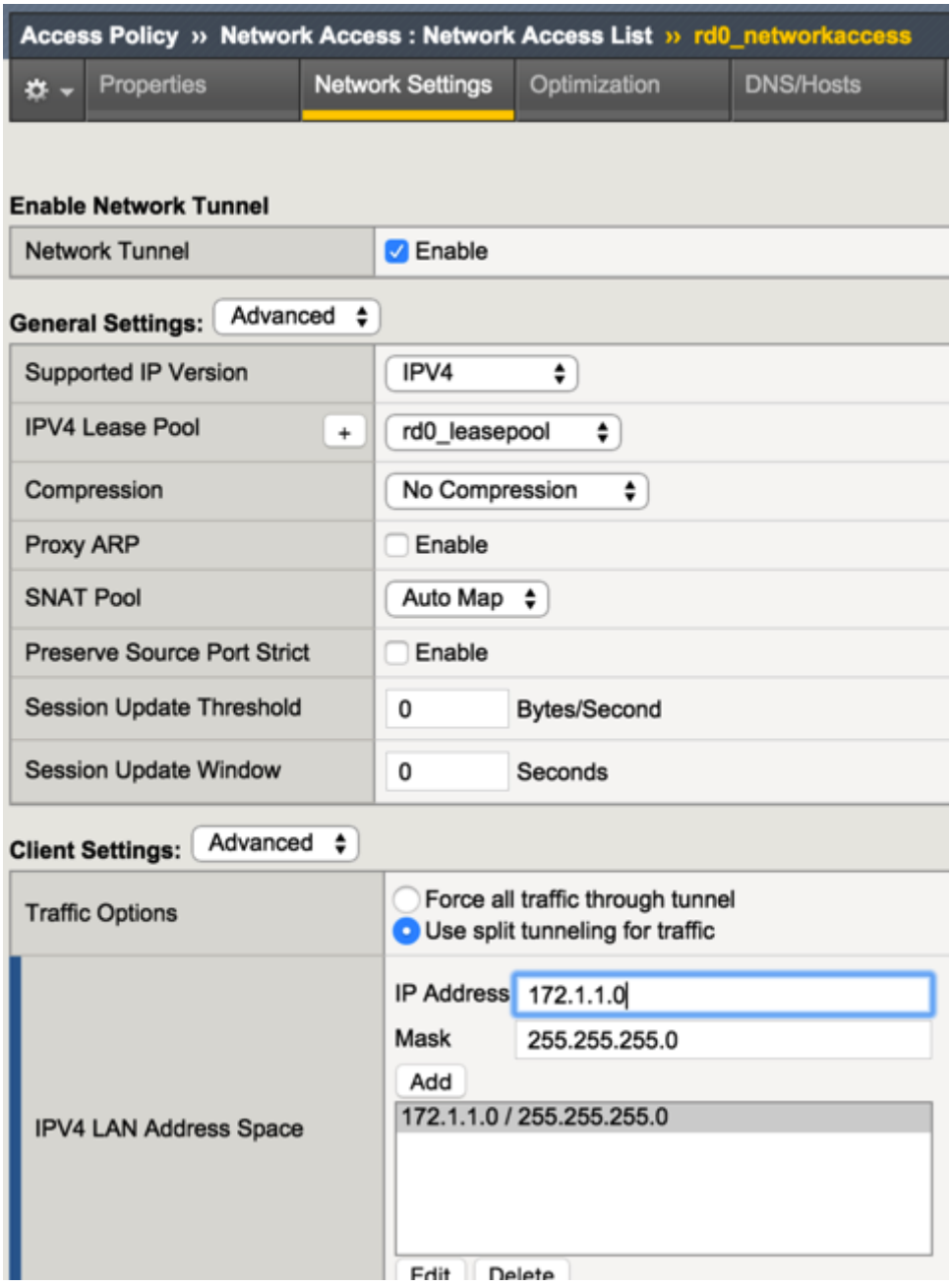
- Name: `rd0_networkaccess`
- Click **Finished**

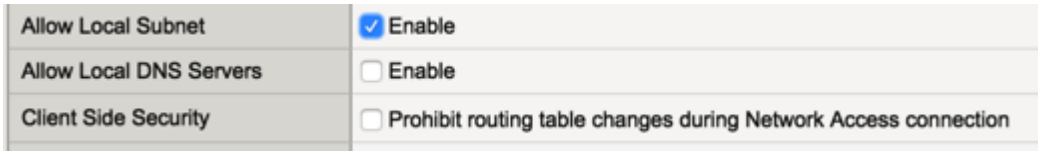


Open the `rd0_networkaccess` you just created and go to Network Settings. Use the following values,

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**

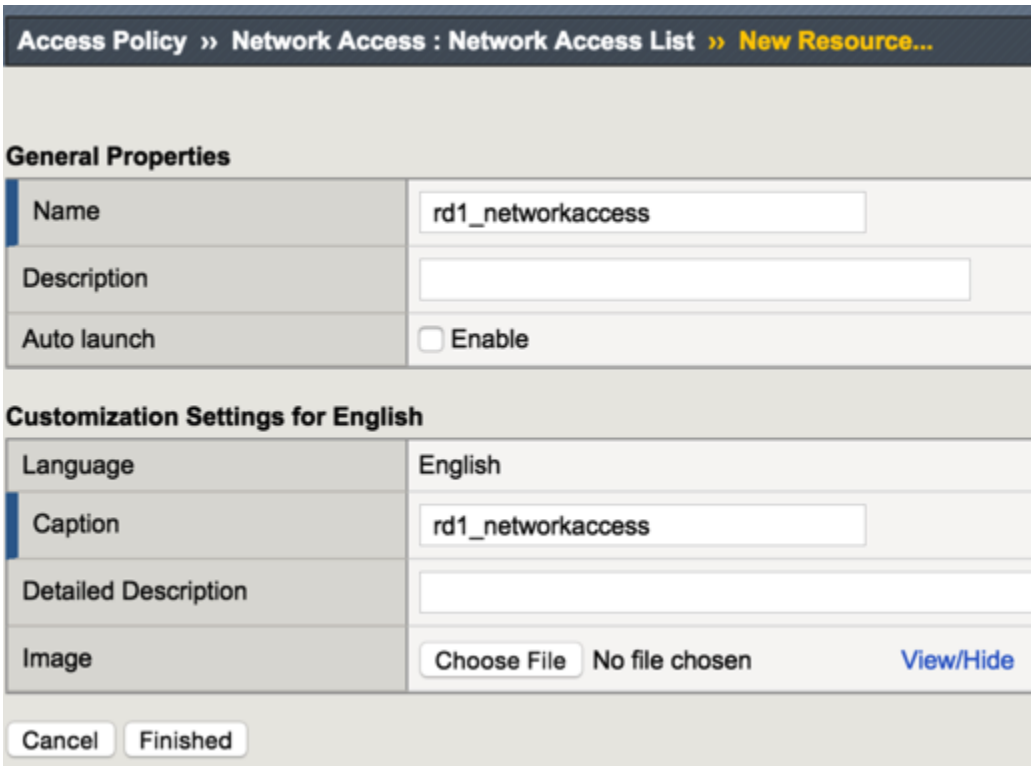




Create a APM network access configuration for route domain 1

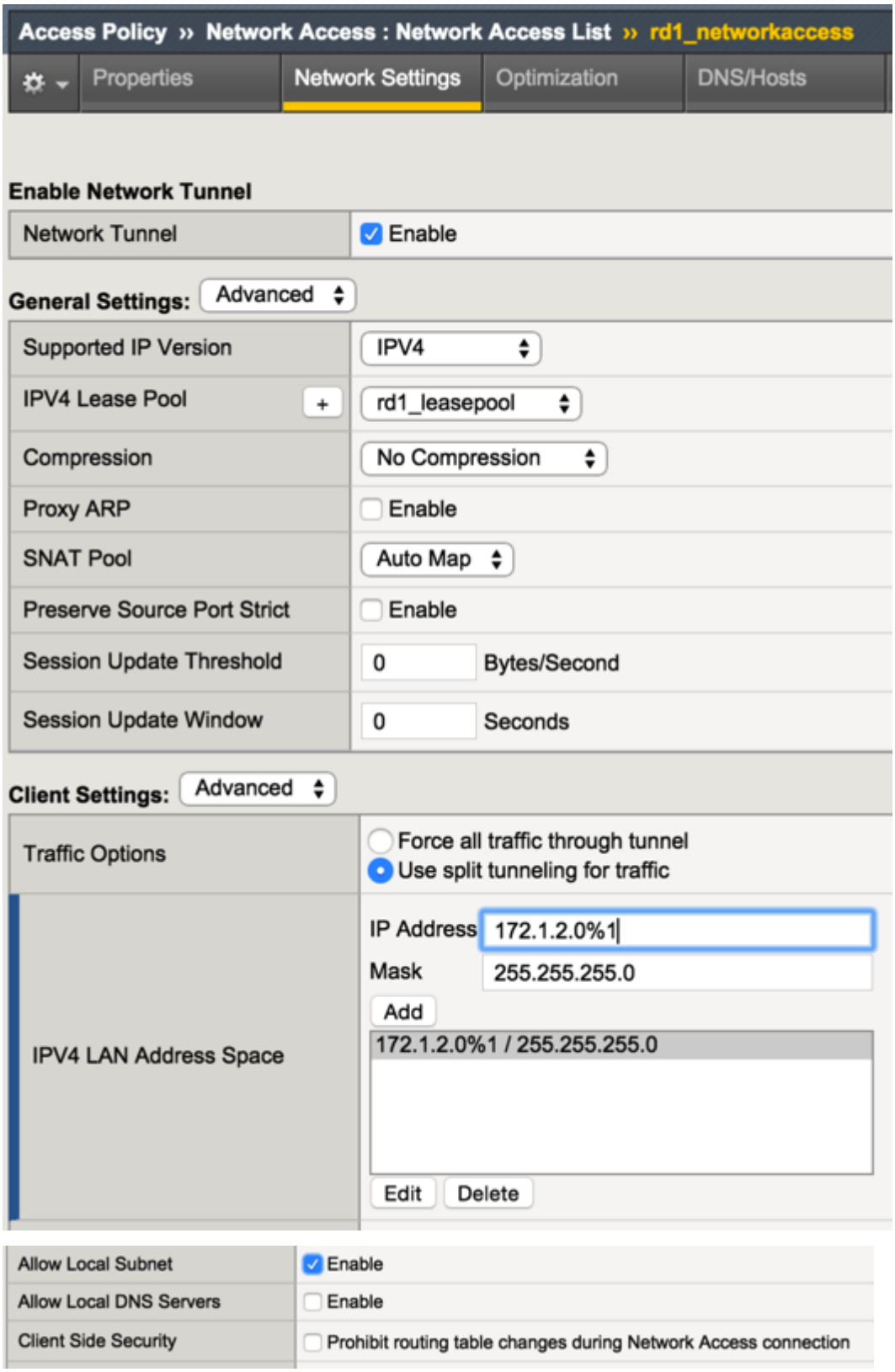
Open the Access > Connectivity/VPN > Network Access Lists page, click Create. Use the following values, leave all others at their defaults

- Name: `rd1_networkaccess`
- Click **Finished**



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**

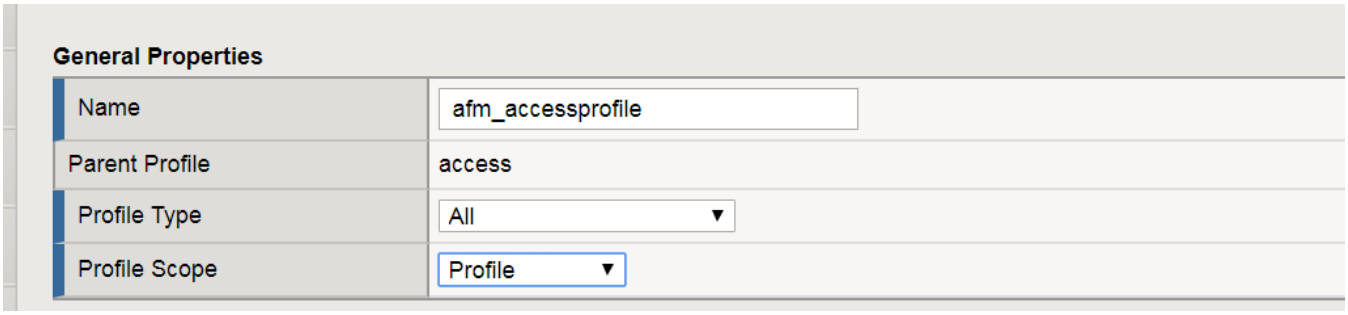


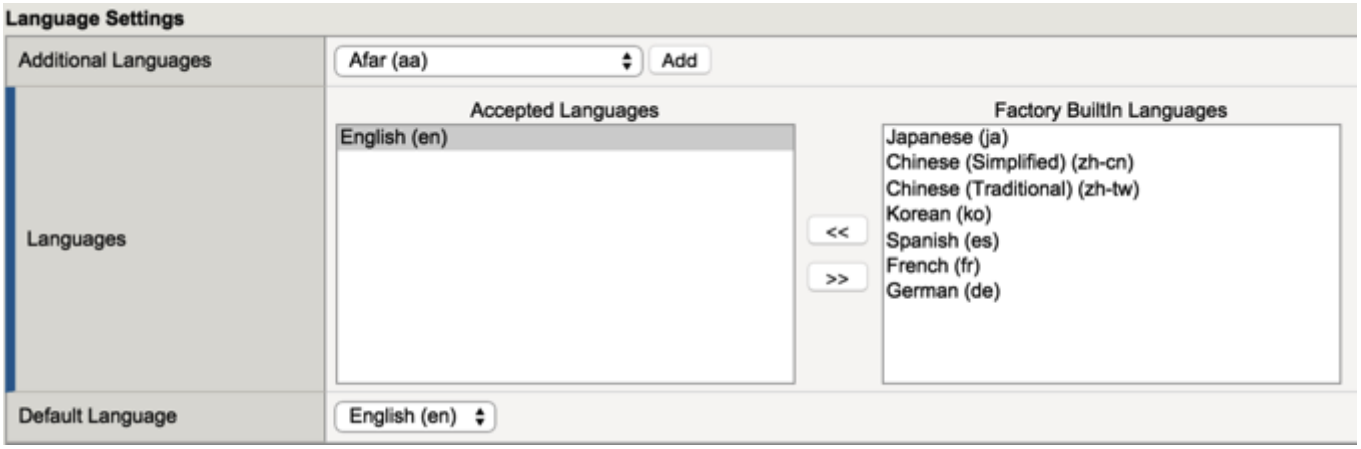
Create a APM access profile

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

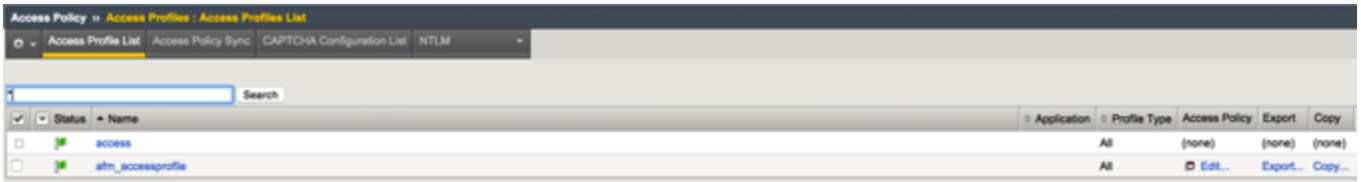
leave all others at their defaults

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





Now the click Edit for the `afm_accessprofile`



The `afm_accessprofile` is displayed

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.

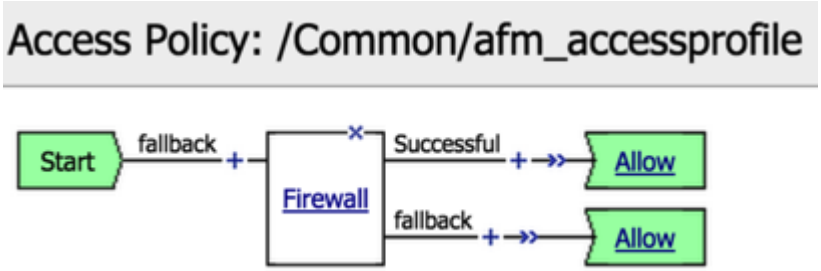
Click on the plus sign after the start block and navigate to Endpoint Security (Client-Side) and select Firewall and click **Add Item**

Leave the defaults

and click **Save**

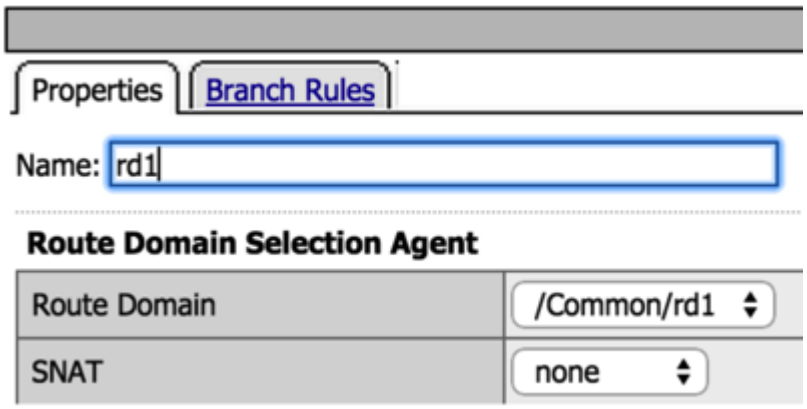
Change both endings from Deny

to Allow



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**



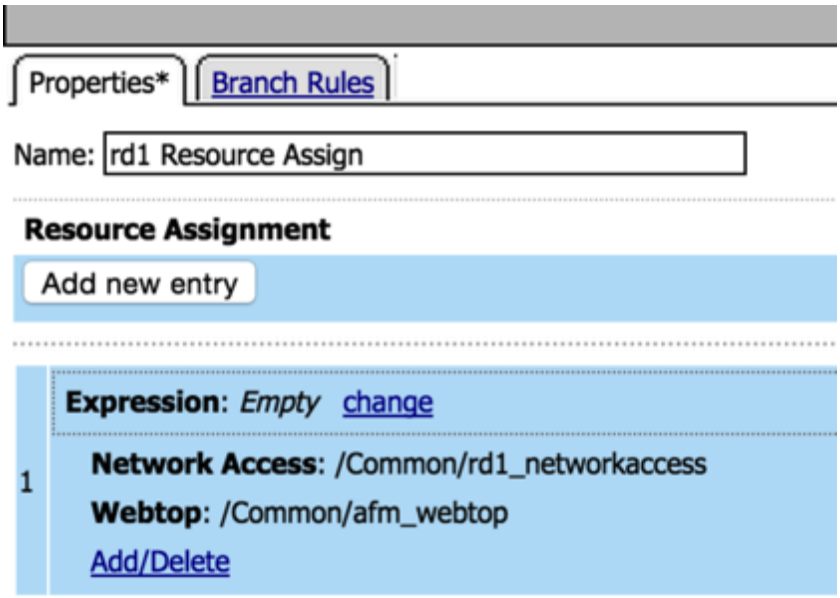
After the rd1 block click the “+” sign and navigate to Assignment->Advanced Resource Assign and

- 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**

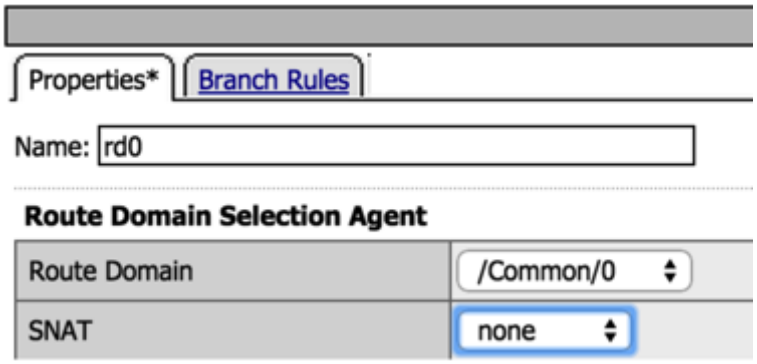
Change the name to `rd1` Resource Assign and click Save



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**



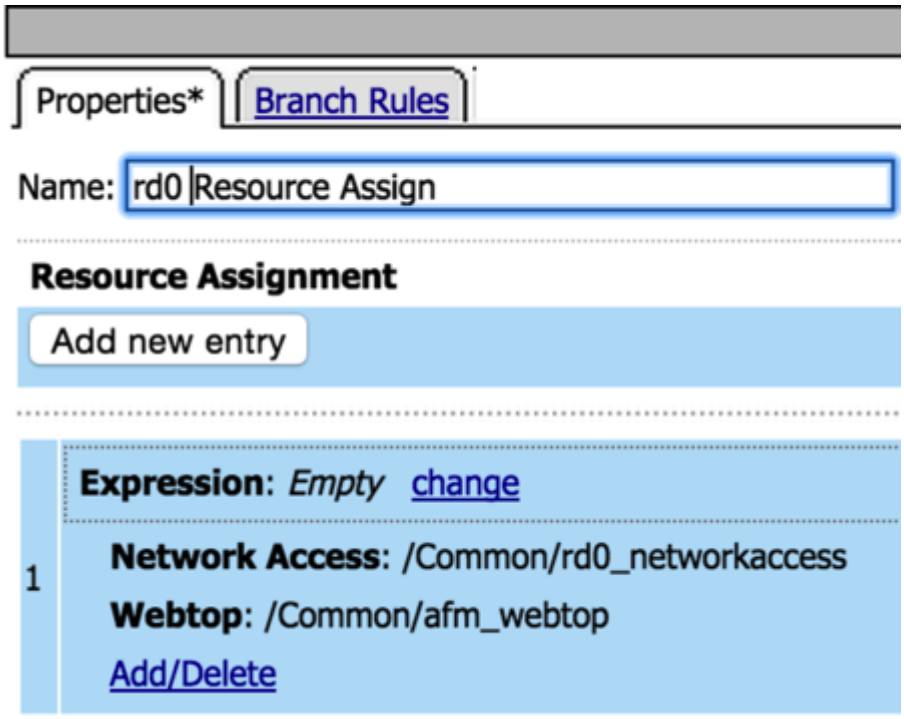
After the rd0 block click the “+” sign and navigate to Assignment->Advanced Resource Assign and

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

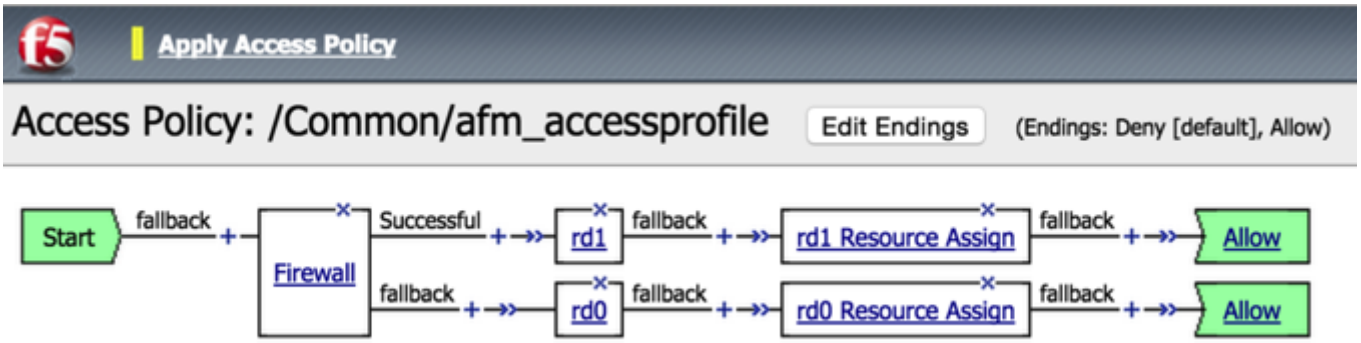
Use the following values, leave all others at their defaults

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

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



The final access policy should look like



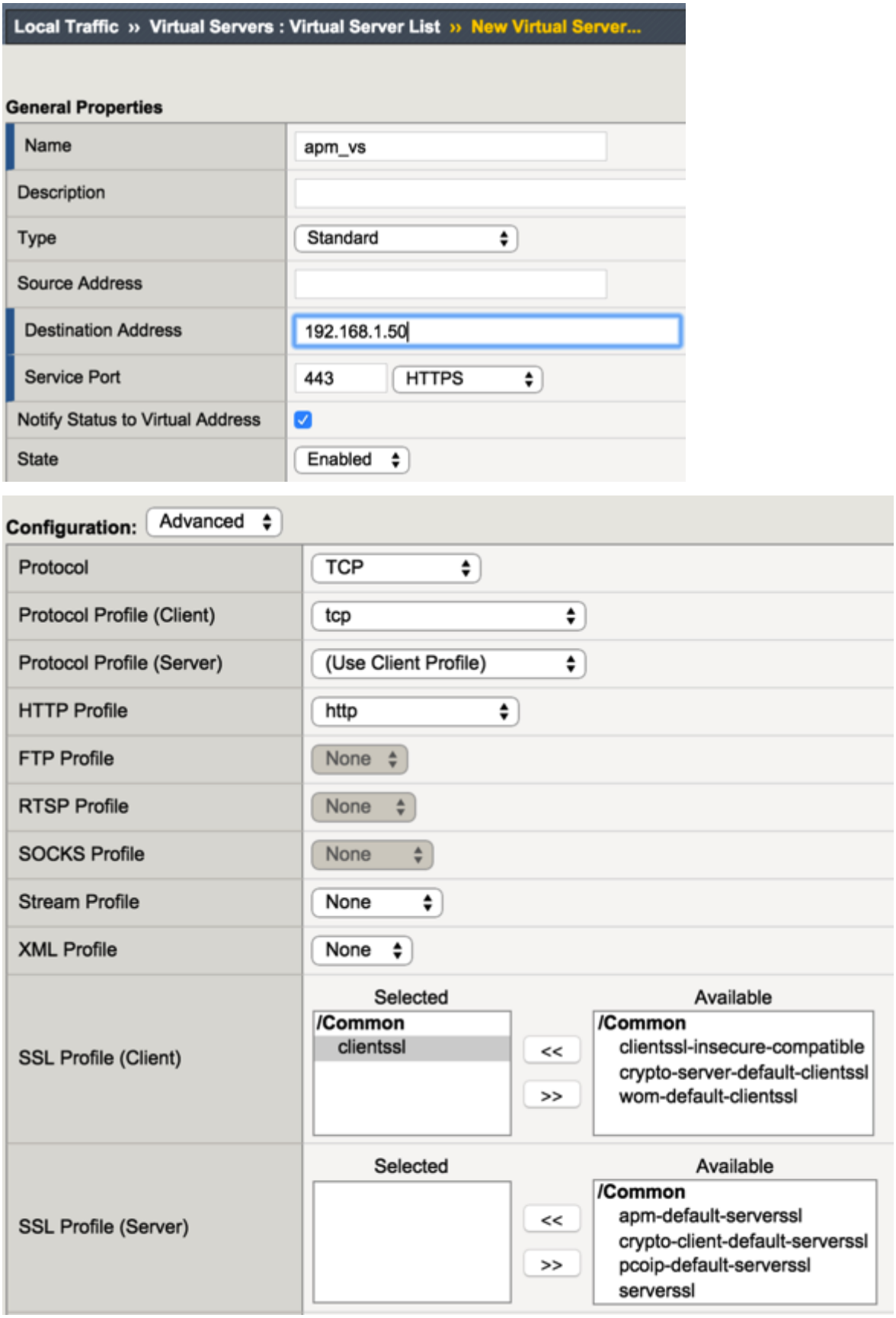
Click Apply Access Policy

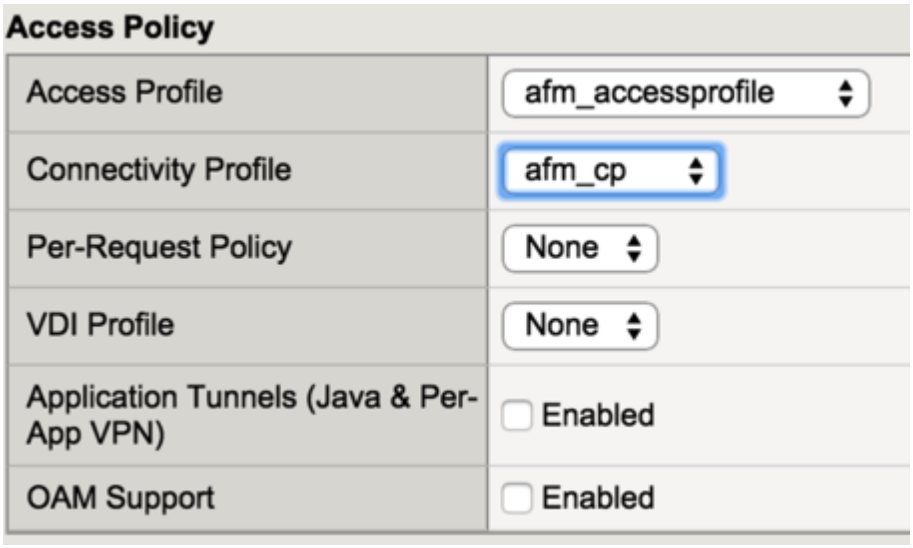
TASK 3 – Create new virtual server for the APM L3 SSL VPN

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**


Local Traffic » Virtual Servers : Virtual Server List » New Virtual Server...
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
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)
Selected
/Common
clientssl
<<
>>
Available
/Common
clientssl-insecure-compatible
crypto-server-default-clientssl
wom-default-clientssl
SSL Profile (Server)
Selected
<<
>>
Available
/Common
apm-default-serverssl
crypto-client-default-serverssl
pcoip-default-serverssl
serverssl



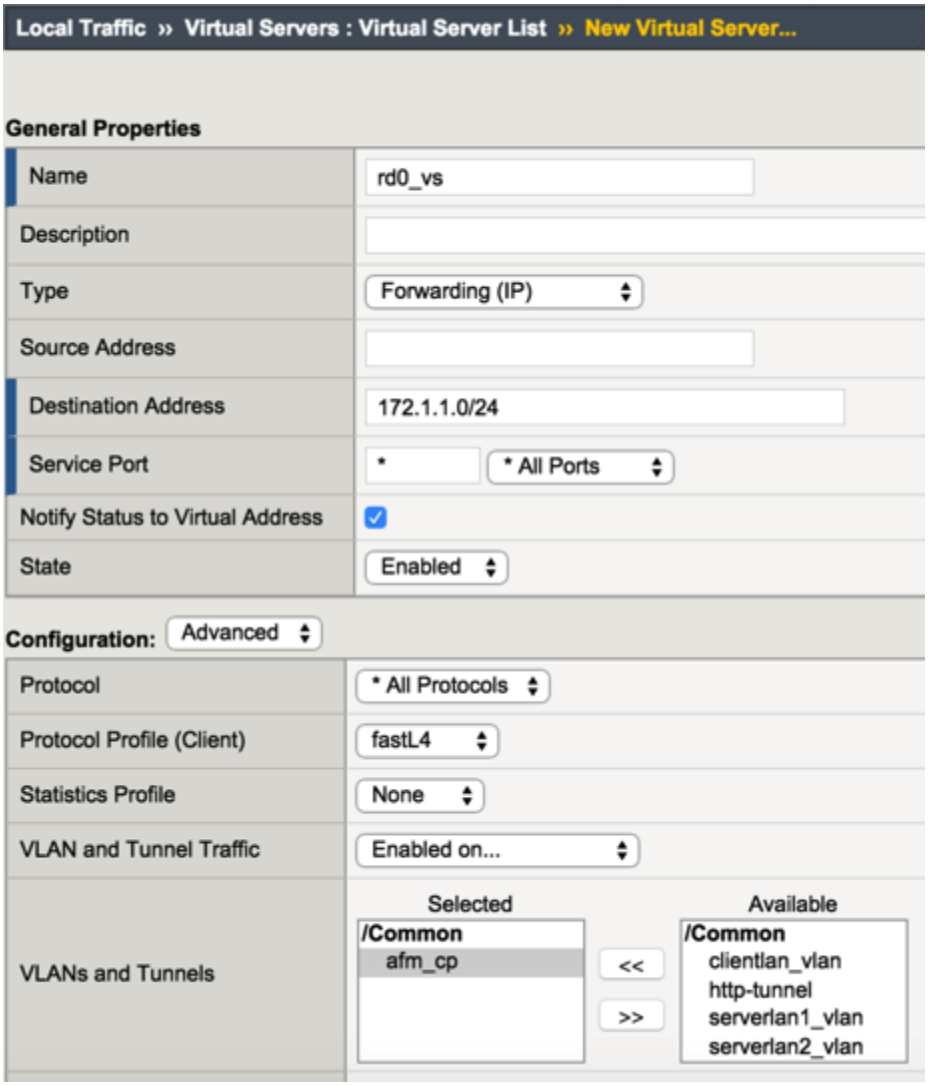
TASK 4 – Create APM policies

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

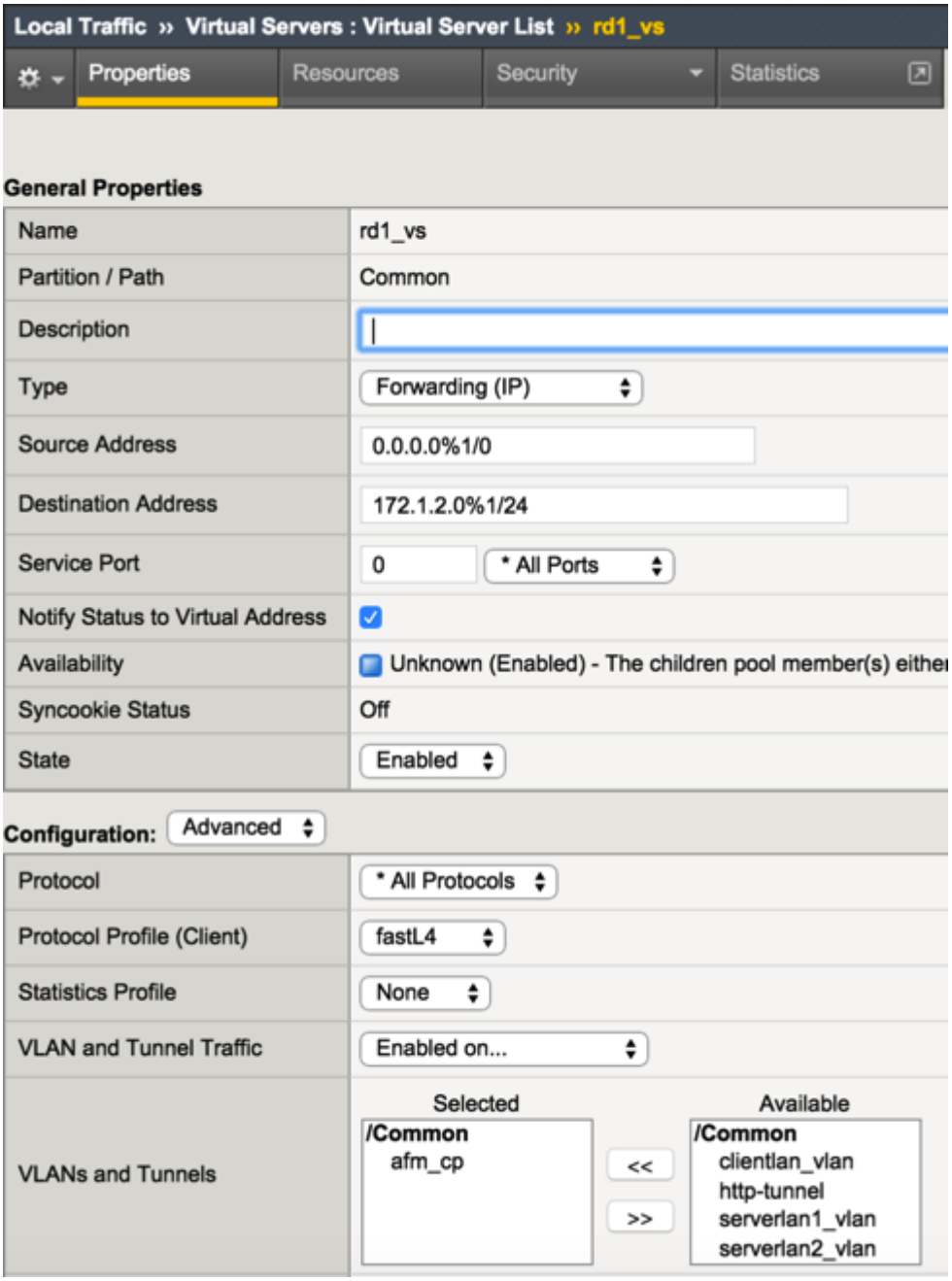
- Name: `rd0_vs`
- Type: `Forwarding (IP)`
- Destination Address: `172.1.1.0/24`
- Service Port: `* All Ports`
- Protocols: `* All Protocols`
- VLANS and Tunnels: `afm_cp`
- Click **Finished**



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**

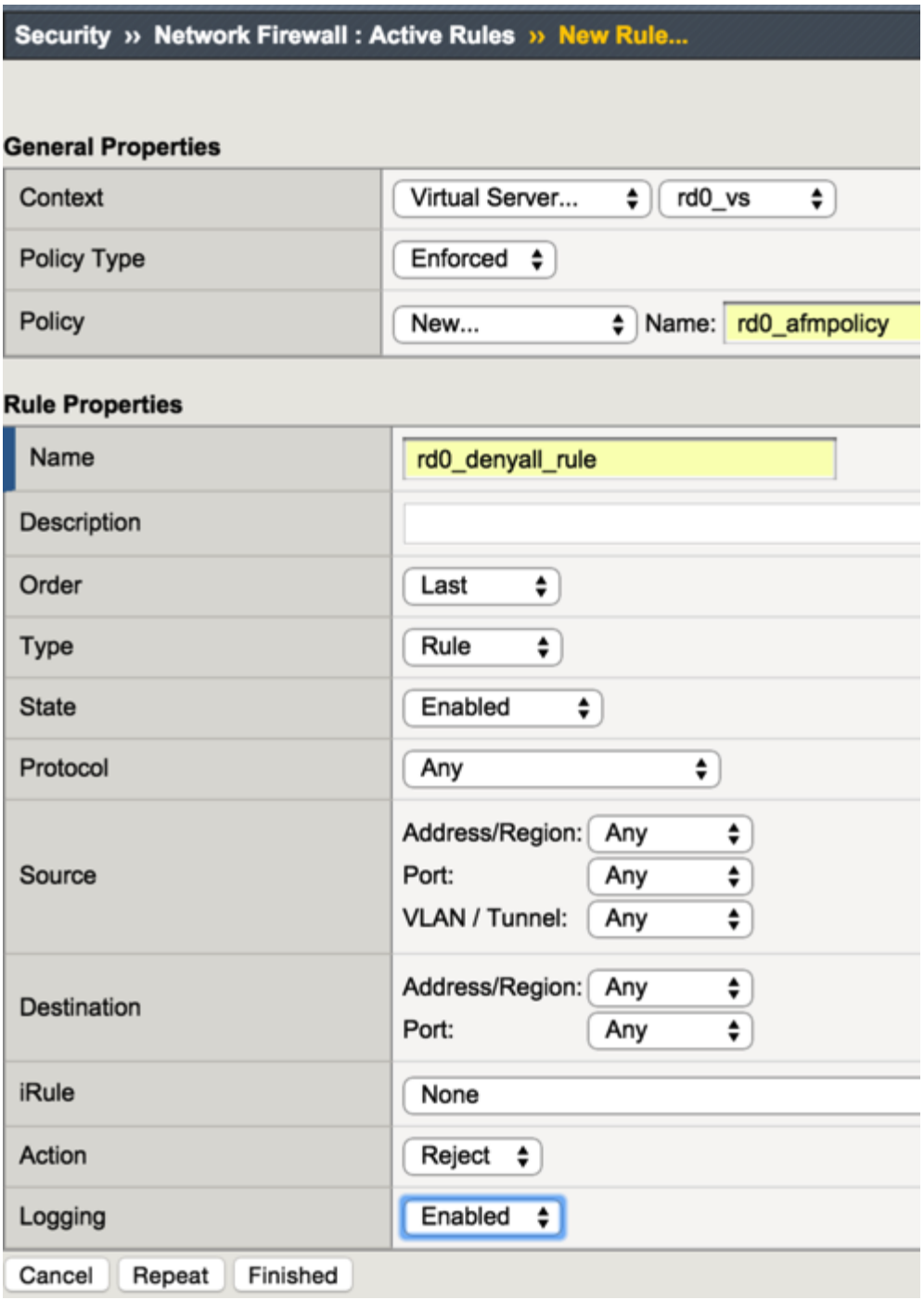


Create the AFM policy for route domain 0 traffic. This limits traffic through sslvpn to the internal subnet in route domain 0.

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**

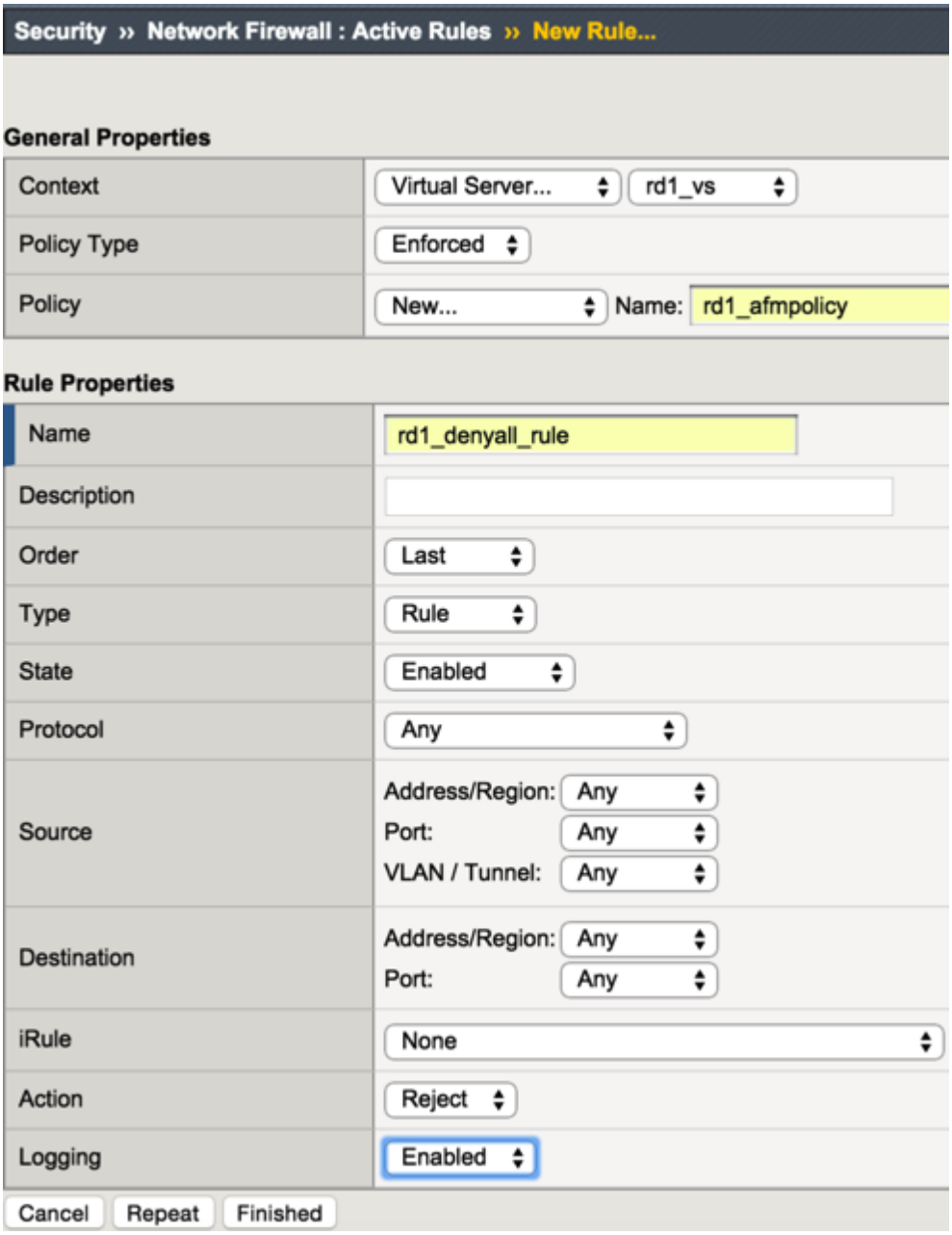


Create the AFM policy for route domain 1 traffic. This limits traffic through sslvpn to the internal subnet in route domain 1.

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**

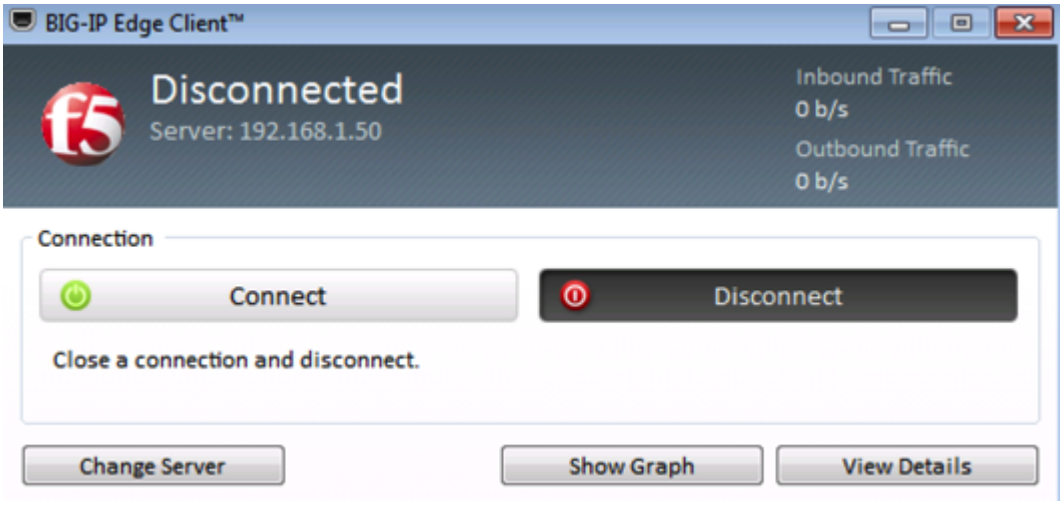


TASK 5 – Test

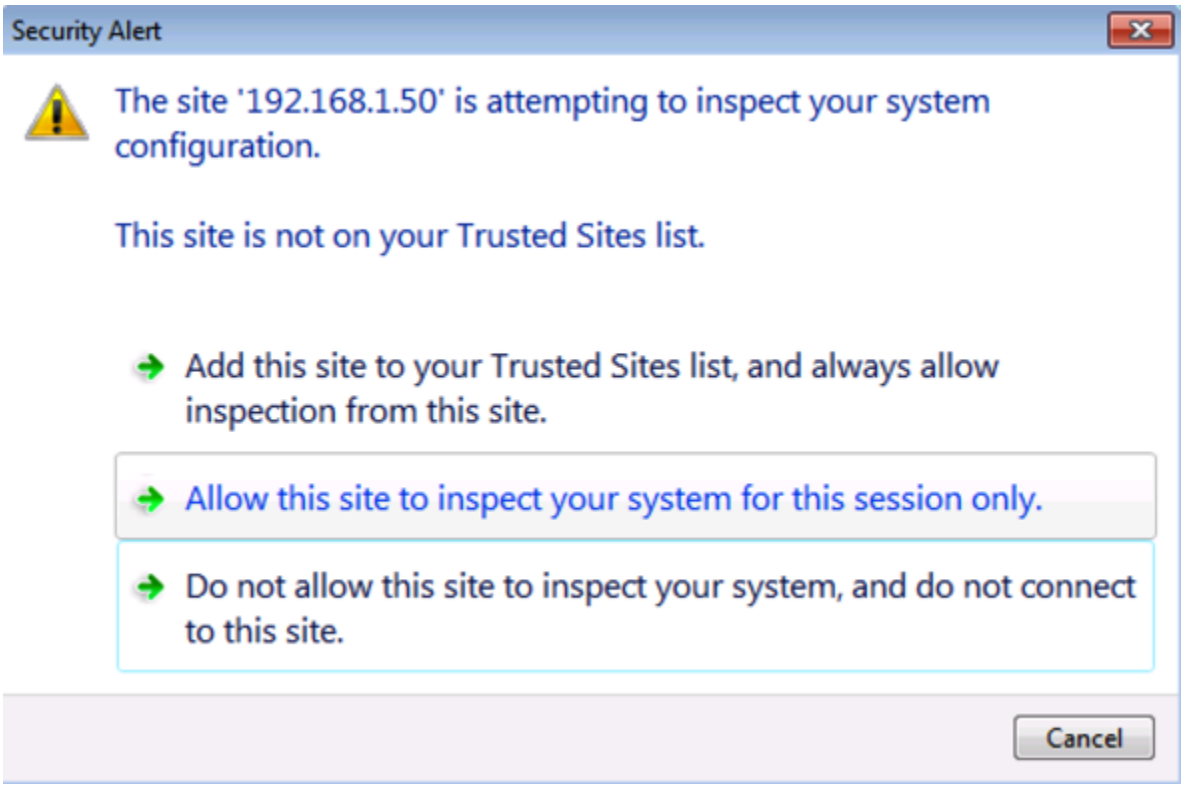
Now its time to test the vpn.

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

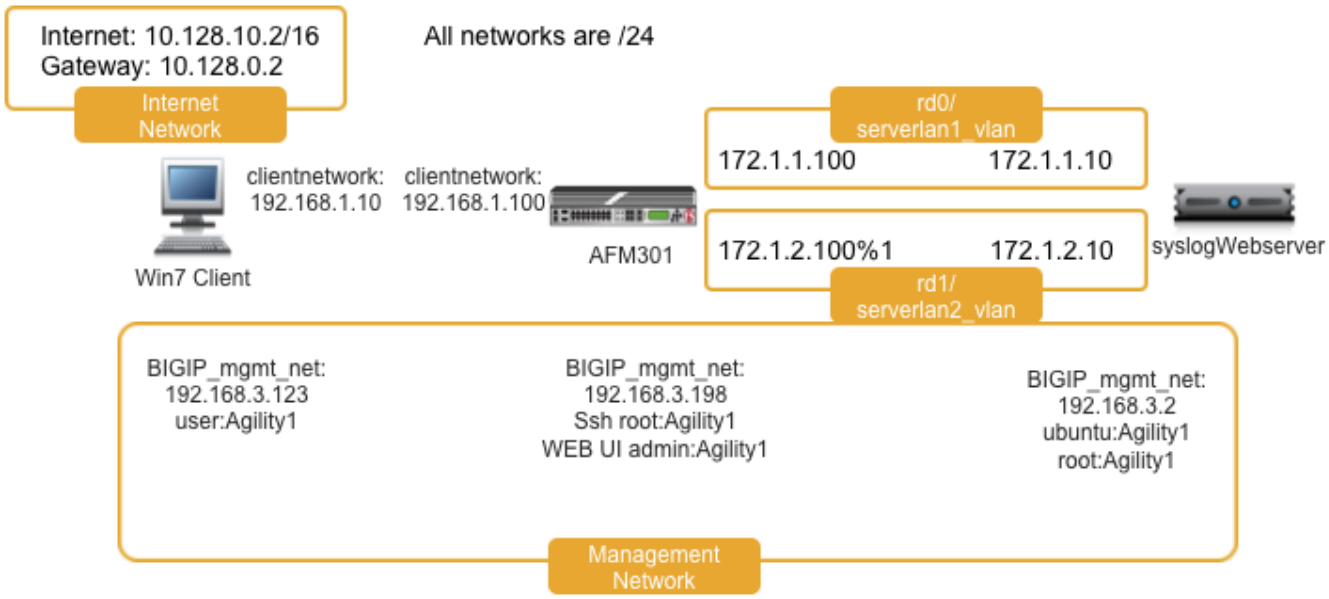
1.1.3 Lab 3: AFM with iRules LX

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

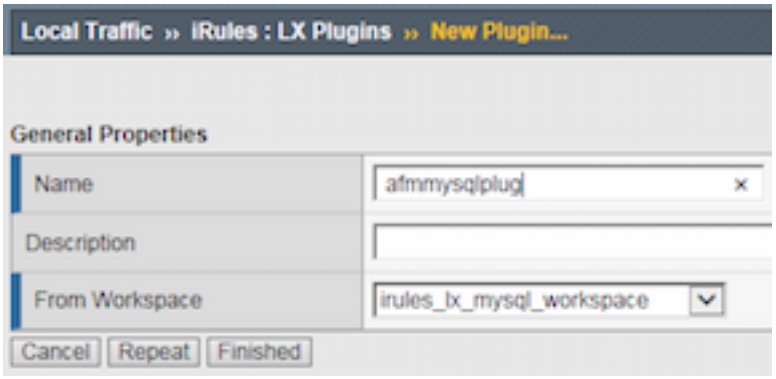
And replace the contents of mysql_extension/index.js with the contents of the index.js on the Win7 client.

Click “Save File”

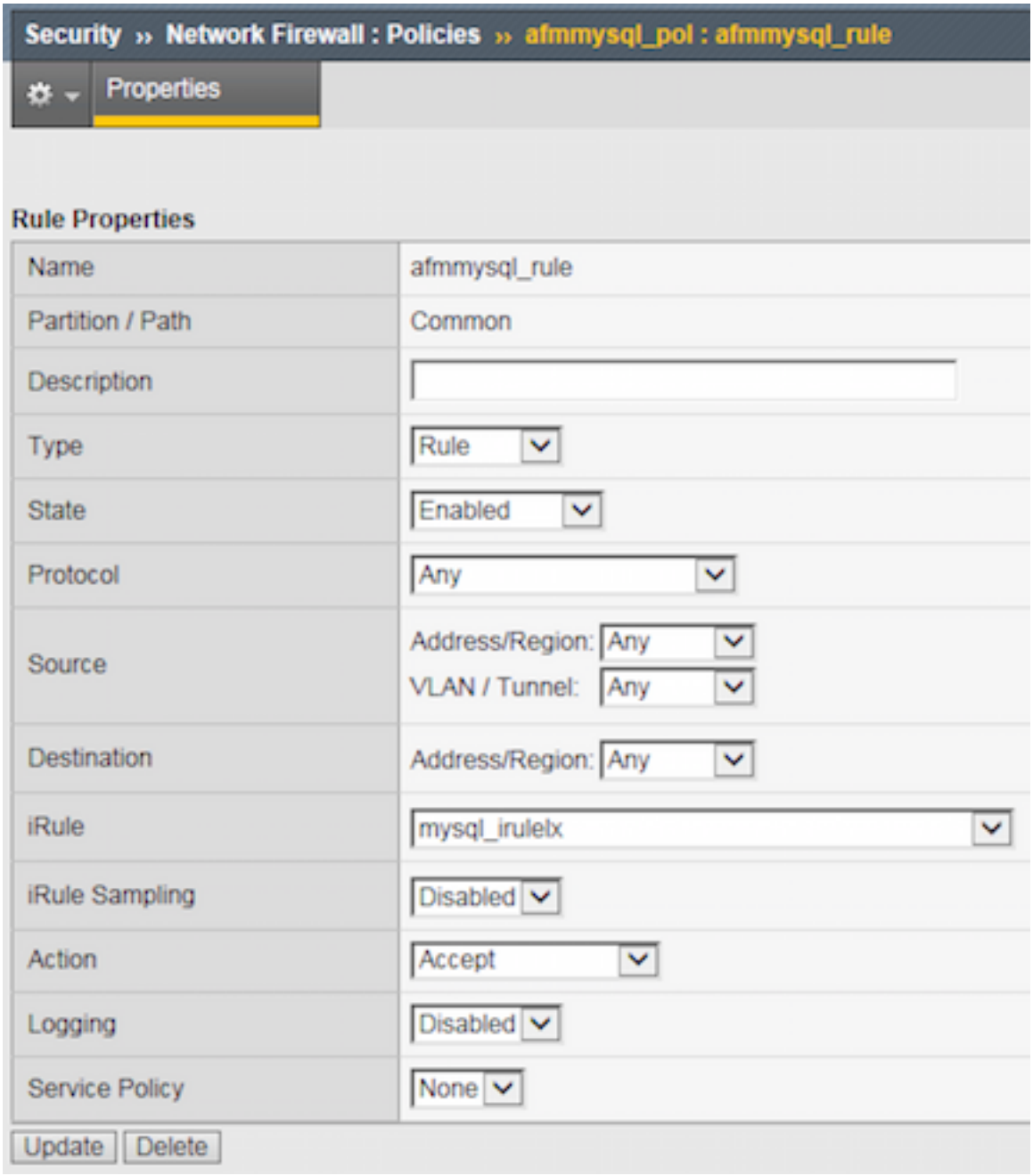
Next click on rules->mysql_irulelx

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_lrulelx” iRule. Click “Update”



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.

F5 Networks, Inc. | f5.com

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com