

Agility 2018 Hands-on Lab Guide

Contents:

1	Welcome	5
2	Class 1: SSL Orchestration	7
2.1	Lab Topology	8
2.2	Module 1: Outbound SSLO	9
2.2.1	Lab 1.1: Deployment Settings	9
2.2.2	Lab 1.2: HTTP Service	12
2.2.3	Lab 1.3: ICAP Service	16
2.2.4	Lab 1.4: L2 Service	17
2.2.5	Lab 1.5: L3 Service	19
2.2.6	Lab 1.6: TAP Service	21
2.2.7	Lab 1.7: Outbound Interception Rules	23
2.2.8	Lab 1.8: Testing	27
2.3	Module 2: Inbound SSLO	29
2.3.1	Lab 2.1: Inbound Interception Rules	29
2.3.2	Lab 2.2: Testing	34
2.4	Module 3: Service Policies	35
2.4.1	Lab 3.1: Reviewing the Policies	35

Welcome

Welcome to F5's SSL Orchestration Training series. The intended audience for these labs are security engineers that would like to leverage the SSL Orchestration tools offered by the F5 platform and gain regulatory visibility into the encrypted traffic on their networks. If you require a pre-built lab environment, please contact your F5 account team and they can provide access to environments on an as-needed basis.

The content contained here adheres to a DevOps methodology and automation pipeline. All content contained here is sourced from the following GitHub repository:

<https://github.com/f5devcentral/f5-agility-labs-sslviz>

Bugs and Requests for enhancements are handled in two ways:

- Fork the Github Repo, fix or enhance as required, and submit a Pull Request
 - <https://help.github.com/articles/creating-a-pull-request-from-a-fork/>
- Open an [Issue](#) within the repository.

Class 1: SSL Orchestration

F5 SSL Orchestrator provides high-performance decryption of inbound and outbound SSL/TLS traffic, enabling security inspection to expose threats and stop attacks. Dynamic service chaining and policy-based traffic steering allow organizations to intelligently manage encrypted traffic flows across the entire security chain with optimal availability.

SSL Orchestrator ensures encrypted traffic can be decrypted, inspected by security controls, then re-encrypted, delivering enhanced visibility to mitigate threats traversing the network. As a result, organizations maximize their security services investment for malware, data loss prevention (DLP), ransomware, and next-generation firewalls (NGFW), thereby preventing inbound and outbound threats, including exploitation, callback, and data exfiltration.

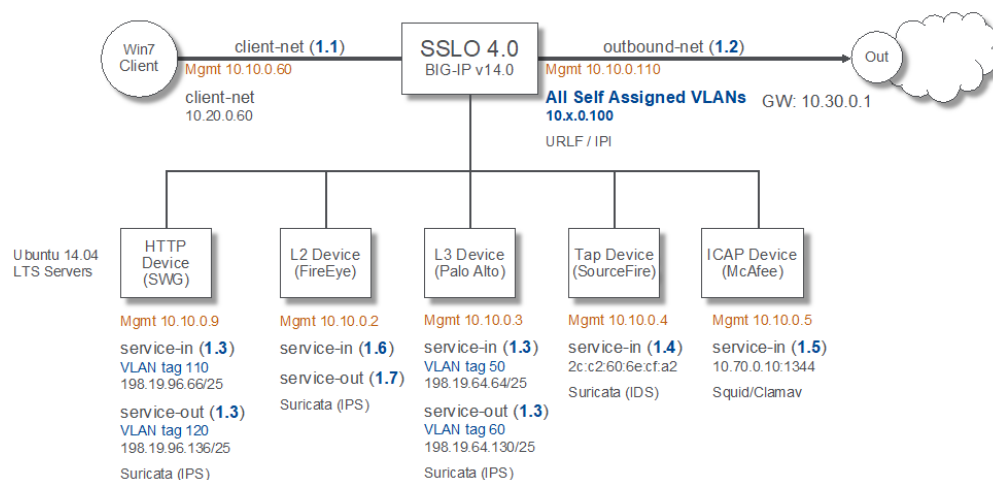
This class covers the following topics:

- SSLO Deployment Settings
- Security Services Creation
- Classification and Interception Rules
- Outbound and Inbound Use cases

Expected time to complete: **4 hours**

To continue please review the information about the Lab Environment.

2.1 Lab Topology



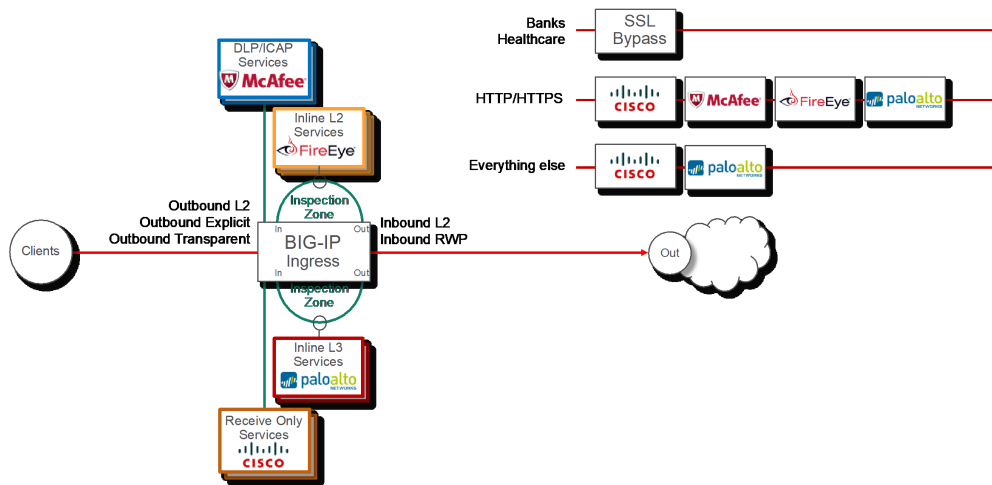
The credentials used to access the resources are:

Environment	Username	Password
Window(s) RDP	student	agility
Ubuntu(s)	student	agility
BIG-IP SSH	root	F5agility!2
BIG-IP GUI	admin	F5agility!2

And the networking information is as follows:

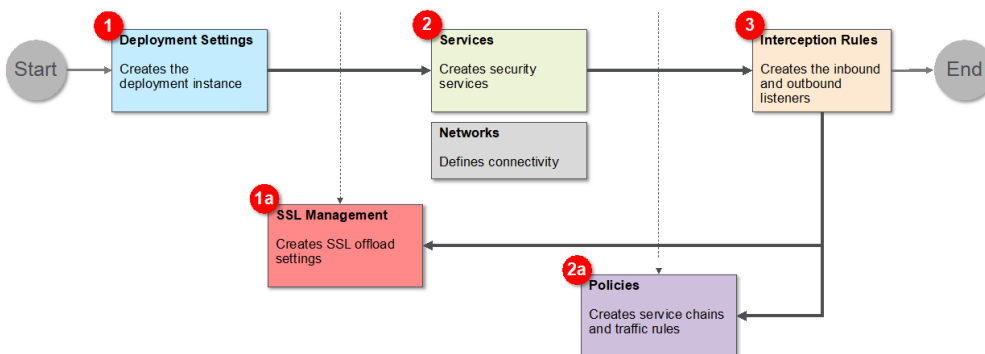
VLAN	Interface (tag)	Self-IP
client-net	1.1	10.20.0.100
HTTP_in	1.3 (110)	SSLO managed
HTTP_out	1.3 (120)	SSLO managed
ICAP	admin	10.70.0.10
L2_in	1.6	SSLO managed
L2_out	1.7	SSLO managed
L3_in	1.3 (50)	SSLO managed
L3_out	1.3 (60)	SSLO managed
Tap	1.4	SSLO managed
outbound-net	1.2	10.30.0.100

2.2 Module 1: Outbound SSLO



In this module we will learn the basic concepts required to deploy Outbound SSLO. Additionally, we will walk through creating services and interception rules. It's important to note that this module will focus on demonstrating an **Outbound** SSLO.

We will be following the workflow in the following diagram for the SSLO configuration:



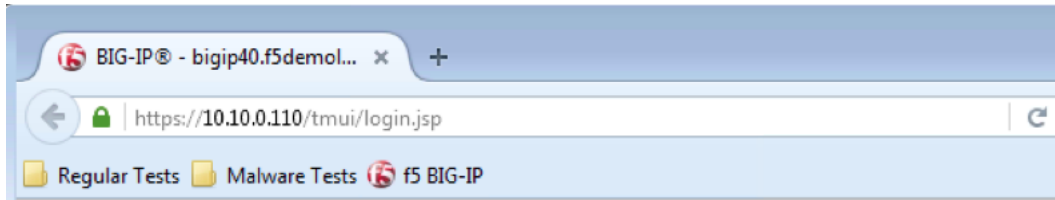
2.2.1 Lab 1.1: Deployment Settings

Task 1 - Create Outbound SSLO Deployment

In this lab, we will explore the settings required to deploy Outbound SSLO. First, we will cover the *General Properties* of the deployment. We will then configure the *Egress*, *DNS*, and *Logging* settings.

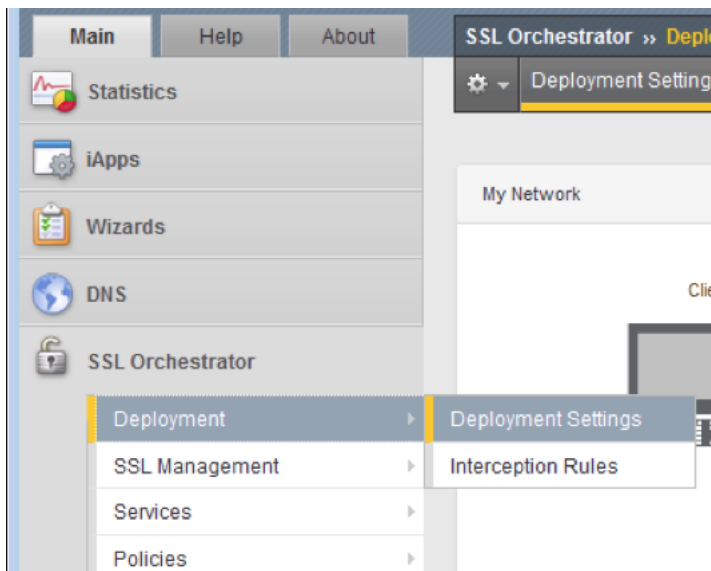
Note: This guide may require you to Copy/Paste information from the guide to your jumphost. To make this easier you can open a copy of the guide by using the **Lab Guide** bookmark in Firefox.

1. Open Firefox and navigate to the following bookmark: *f5 BIG-IP*. Bypass any SSL errors that appear and ensure you see the login screen for each bookmark:



Warning: We are using a self-signed certificate in this lab. In your environment you must make sure that you use certificates issued by your certificate authority for both production and lab equipment. Not doing so would make it possible for an attacker to do a man-in-the-middle attack and allow him the ability to steal passwords and tokens.

2. Authenticate to the interface using the default credentials as defined in the lab topology.
3. Navigate to *SSL Orchestrator* → *Deployment* → *Deployment Settings* and click:



4. In *General Properties* change the *Deployment Name* to *sslo_agility_lab*

General Properties	
Deployment Name	sslo_agility_lab
Description	SSL Orchestrator
Strict Update	<input checked="" type="checkbox"/>
Deployed Network	L3 Network
IP Family	IPv4

5. In the *Egress Configuration* section set the following:
 - (a) *Manage SNAT Settings* → *Auto Map*
 - (b) *Gateways* → *Specific gateways*
 - (c) Add IPv4 gateway address *10.30.0.1*

Egress Configuration	
Manage SNAT Settings	Auto Map ▼
Gateways	Specific gateways ▼
IPv4 Outbound Gateway	<div>Ratio</div> <div>1</div> <div>IPv4 gateway address</div> <div>10.30.0.1</div> <div>+</div> <div>-</div>

6. Leave the *DNS* settings at their defaults.
7. Change *Logging level* → *Debug*

Logging Configuration	
Logging Level	Debug ▼

Note: The *Debug* log level should not be used in production unless recommended by f5 Support.

This completes the *Deployment Settings* setup. When your screen looks like the following, click *Finished*:

General Properties	
Deployment Name	sslo_agility_lab
Description	SSL Orchestrator
Strict Update	<input checked="" type="checkbox"/>
Deployed Network	L3 Network ▼
IP Family	IPv4 ▼

Egress Configuration	
Manage SNAT Settings	Auto Map ▼
Gateways	Specific gateways ▼
IPv4 Outbound Gateway	<div>Ratio</div> <div>1</div> <div>IPv4 gateway address</div> <div>10.30.0.1</div> <div>+</div> <div>-</div>

DNS	
DNS Query Resolution	Internet authoritative Name Server ▼
Local Forwarding Nameserver(s)	
Local/Private Forward Zones	<div>Forward Zones:</div> <div>Nameservers:</div> <div></div> <div>+</div> <div>-</div> <div>Add</div>
DNSSEC Validation	<input type="checkbox"/>

Logging Configuration	
Logging Level	Debug ▼

Finished

Note: The *Strict Updates* option protects against accidental changes to an application service's configuration. The *Strict Updates* setting is *checked* by default.

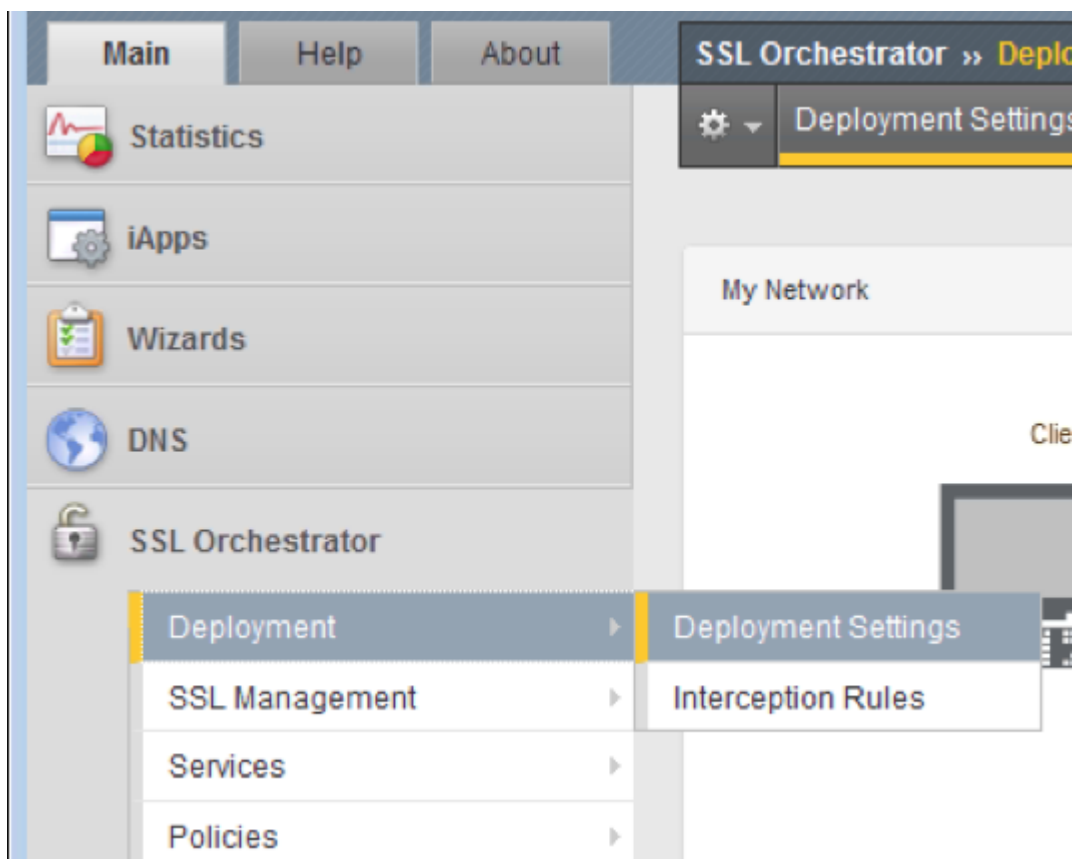
Unless you have a specific reason to turn off strict updates, F5 recommends that you leave the setting enabled.

2.2.2 Lab 1.2: HTTP Service

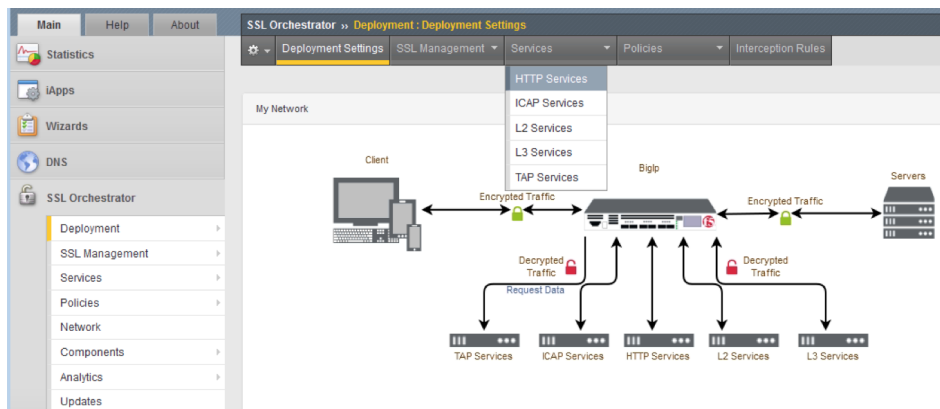
Task 1 - Create SSLO HTTP Service

A service is a collection of security devices that will receive decrypted traffic from the SSLO solution. In this section, the HTTP Service will be created. An HTTP Service would typically be a Secure Web Proxy. The proxy could explicit or transparent.

1. Login to the BIG-IP with Firefox
2. Navigate to *SSL Orchestrator* → *Deployment* → *Deployment Settings* and click:



3. On the menu across the top of the main window pane, navigate to *Services* → *HTTP Services* and click:



4. Click *Create* on the far right:

General Properties					
Name	ssloS_HTTP_service				
Description					
Strict Update	<input checked="" type="checkbox"/>				
IP Family	IPv4 only				
Service Definition					
Auto Manage	<input checked="" type="checkbox"/>				
Proxy Type	Explicit				
To Service	198.19.96.7/25 Create New...				
VLAN	ssloN_HTTP_in.app/ssloN_HTTP_in Create New...				
Node	<table border="1"> <thead> <tr> <th>IP Address</th> <th>Port</th> </tr> </thead> <tbody> <tr> <td>198.19.96.66</td> <td>3128</td> </tr> </tbody> </table> <div> <input type="text"/> 3128 Add </div>	IP Address	Port	198.19.96.66	3128
IP Address	Port				
198.19.96.66	3128				
From Service	198.19.96.245/25 Create New...				
VLAN	ssloN_HTTP_out.app/ssloN_HTTP_out Create New...				
Service Down Action	Ignore				
Authentication Offload	<input type="checkbox"/>				
Resources					
iRules	<div> <div>Selected</div> <div>Filter</div> <div>No available items</div> </div> <div> <div>Available</div> <div> / Common/ / Common/ / Common/ / Common/ / Common/ / Common/ / Common/ / Common/ </div> </div>				
Cancel Finished					

5. Enter the following information:

Property	Value
Name	ssloS_HTTP_service
Proxy Type	Explicit
To Service VLAN	ssloN_HTTP_in.app/ssloN_HTTP_in
Node -> IP Address	198.19.96.66 (click Add)
From Service VLAN	ssloN_HTTP_out.app/ssloN_HTTP_out

Note: For *To Service VLAN* and *From Service VLAN*, use the drop-down menu to select the correct value.

6. Once your settings look like the following screenshot, click *Finish*:

General Properties	
Name	ssloS_HTTP_service
Description	
Strict Update	<input checked="" type="checkbox"/>
IP Family	IPv4 only

Service Definition					
Auto Manage	<input checked="" type="checkbox"/>				
Proxy Type	Explicit				
To Service	198.19.96.7/25 Create New...				
VLAN	ssloN_HTTP_in.app/ssloN_HTTP_in Create New...				
Node	<table border="1"><thead><tr><th>IP Address</th><th>Port</th></tr></thead><tbody><tr><td>198.19.96.66</td><td>3128</td></tr></tbody></table> <div><input type="text"/> 3128 Add</div>	IP Address	Port	198.19.96.66	3128
IP Address	Port				
198.19.96.66	3128				
From Service	198.19.96.245/25 Create New...				
VLAN	ssloN_HTTP_out.app/ssloN_HTTP_out Create New...				
Service Down Action	Ignore				
Authentication Offload	<input type="checkbox"/>				

Resources	
iRules	<div><div>Selected</div><div>Filter</div><div>No available items</div></div> <div><div>Available</div><div>/Common/ /Common/ /Common/ /Common/ /Common/ /Common/ /Common/ /Common/ /Common/</div></div>

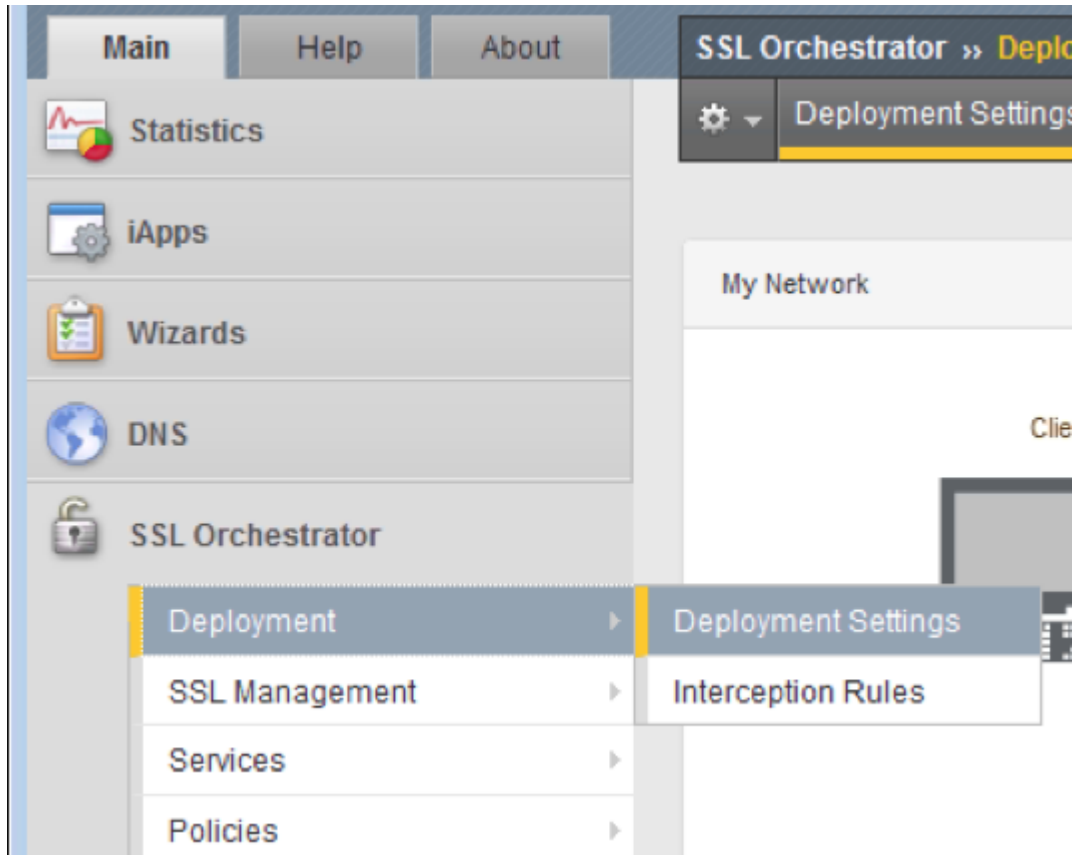
[Cancel](#) [Finished](#)

2.2.3 Lab 1.3: ICAP Service

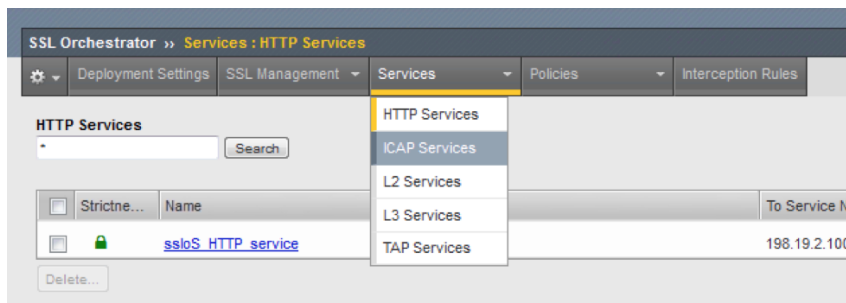
Task 1 - Create SSLO ICAP Service

A *Service* is a collection of security devices that will receive decrypted traffic from the SSLO solution. In this section, an *ICAP Service* will be created. An ICAP Service would typically be an Anti-Virus or DLP solution. It is important to have the correct *Request* and *Response* URIs for the solution and the appropriate *Preview Max Length*.

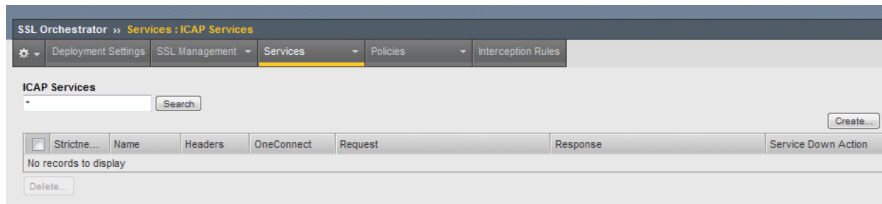
1. Login to the BIG-IP with Firefox
2. Navigate to *SSL Orchestrator* → *Deployment* → *Deployment Settings* and click:



3. On the menu across the top of the main window pane, navigate to *Services* → *ICAP Services* and click:



4. Click *Create* on the far right



5. Enter the following values:

Property	Value
Name	ssloS_ICAP_service
ICAP Devices → IP Address	10.70.0.10 (click <i>Add</i>)
Request	Replace <i>/req</i> with <i>/squidclamav</i>
Response	Replace <i>/res</i> with <i>/squidclamav</i>
Preview Max Length	1048576

6. Once your settings look like the following screenshot, click *Finish*:

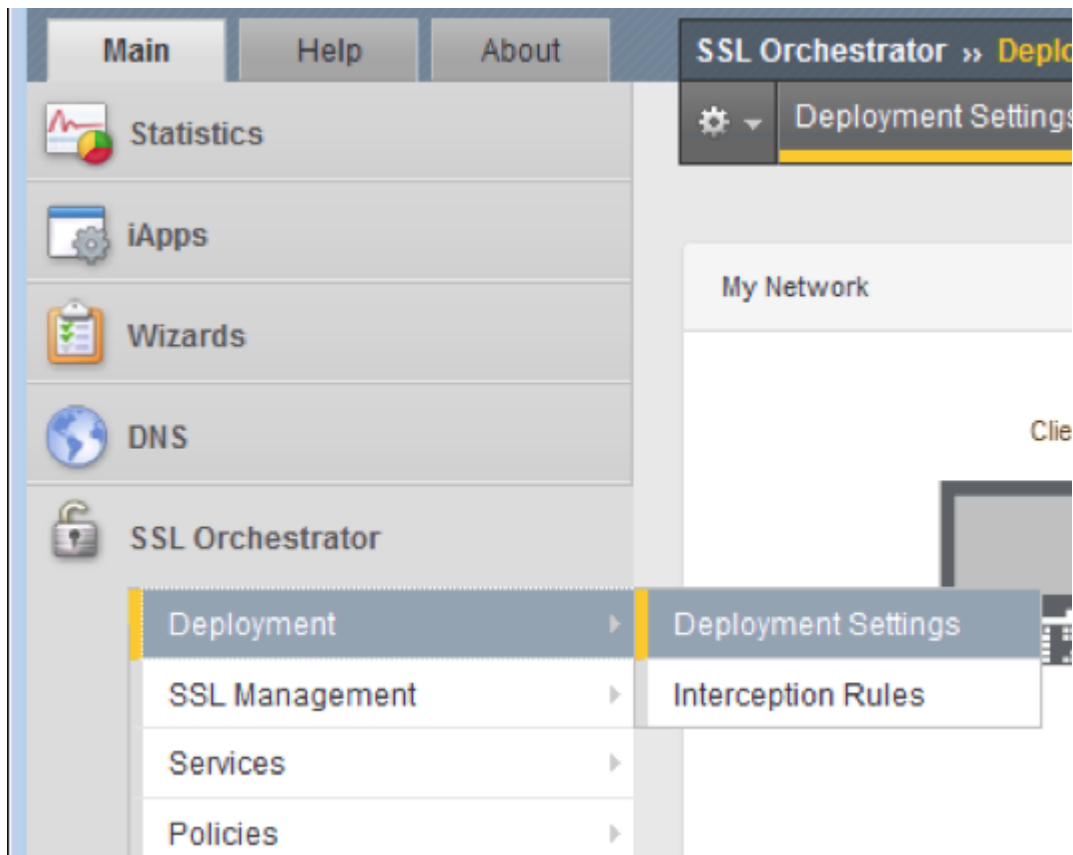
2.2.4 Lab 1.4: L2 Service

Task 1 - Create SSLO L2 Service

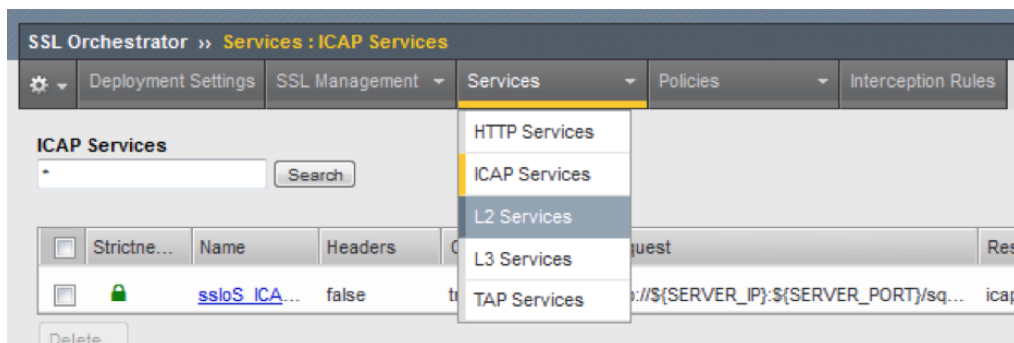
A *Service* is a collection of security devices that will receive decrypted traffic from the SSLO solution. In this section an *L2 Service* will be created. An L2 Service could be an IDS/IPS or DLP solution. Some refer

to this as a “Bump in the Wire.”

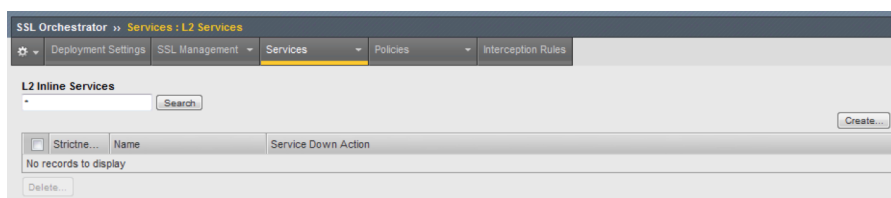
1. Login to the BIG-IP with Firefox
2. Navigate to *SSL Orchestrator* → *Deployment* → *Deployment Settings* and click:



3. On the menu across the top of the main window pane, navigate to *Services* → *L2 Services* and click:



4. Click *Create* on the far right:



5. Enter the following values:

Property	Value
Name	ssloS_L2_service
Paths -> From BIGIP VLAN	ssloN_L2_in.app/ssloN_L2_in
Paths -> To BIGIP VLAN	ssloN_L2_out.app/ssloN_L2_out (click <i>Add</i>)

6. Once your settings look like the following screenshot, click *Finished*:

General Properties

Name: ssloS_L2_service

Description:

Strict Update: ☒

IP Family: IPv4 only

Service Subnet: 198.19.32.0 ⚠ The L2-service's internally assigned IP Address out on the VLAN where the L2-service resides.

L2 Service

Paths:

Ratio	From BIGIP VLAN	To BIGIP VLAN
1	-- choose option	-- choose option
1	ssloN_L2_in.app/ssloN_L2_in	ssloN_L2_out.app/ssloN_L2_out

Service Down Action: Ignore

Port Remap: ☒ Enabled

Resources

iRules:

Selected:

Filter:

No available items

Available:

- /Common/_sys_Af
- /Common/_sys_Af
- /Common/_sys_Af
- /Common/_sys_Af
- /Common/_sys_Af
- /Common/_sys_Af
- /Common/_sys_Au
- /Common/_sys_Au

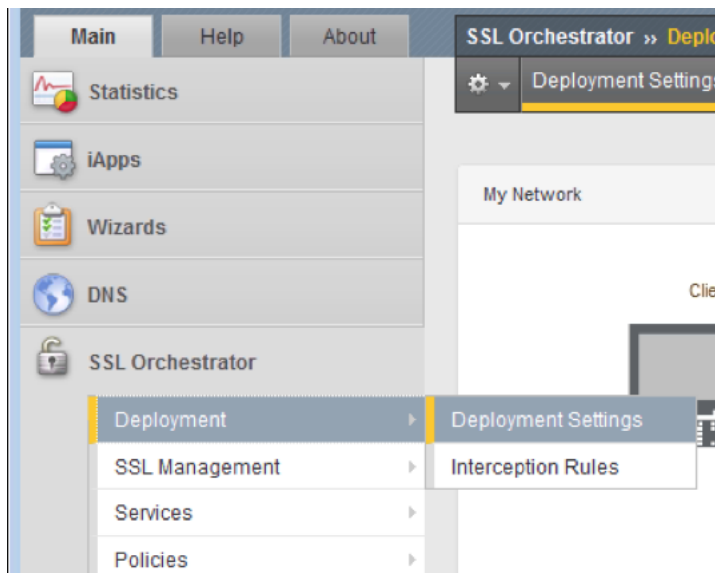
Cancel Finished

2.2.5 Lab 1.5: L3 Service

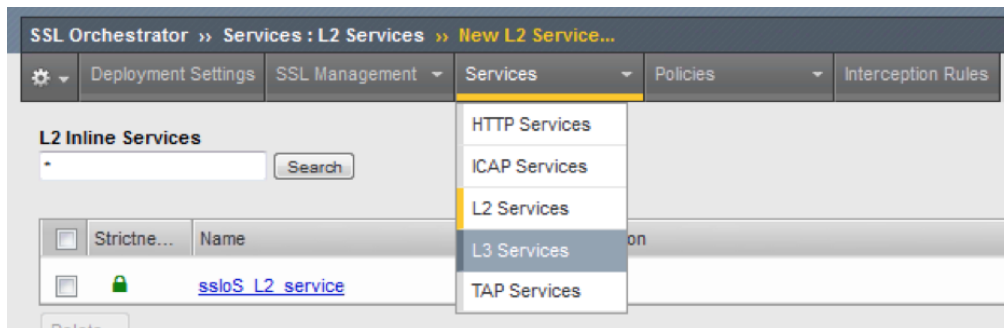
Task 1 - Create SSLO L3 Service

A *Service* is a collection of security devices that will receive decrypted traffic from the SSLO solution. In this section, an *L3 Service* will be created. An L3 Service would typically be an IDS/IPS, DLP, or Next-Gen Firewall (NGFW).

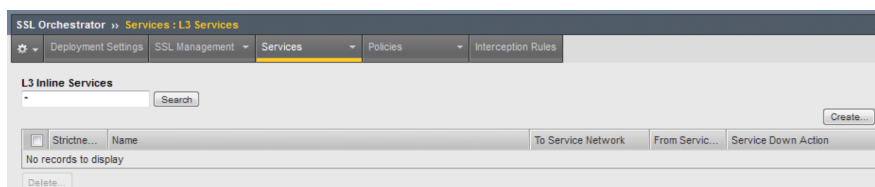
1. Login to the BIG-IP with Firefox
2. Navigate to *SSL Orchestrator* → *Deployment* → *Deployment Settings* and click:



- On the menu across the top of the main window pane navigate to *Services* → *L3 Services* and click:



- Click *Create* on the far right:



- Enter the following values:

Property	Value
Name	ssloS_L3_service
To Service VLAN	ssloN_L3_in.app/ssloN_L3_in
Node → IP Address	198.19.64.64 (click <i>Add</i>)
From Service VLAN	ssloN_L3_out.app/ssloN_L3_out

Note: For *To Service VLAN* and *From Service VLAN*, use the drop-down menu to select the correct value.

- Once your settings look like the following screenshot, click *Finished*:

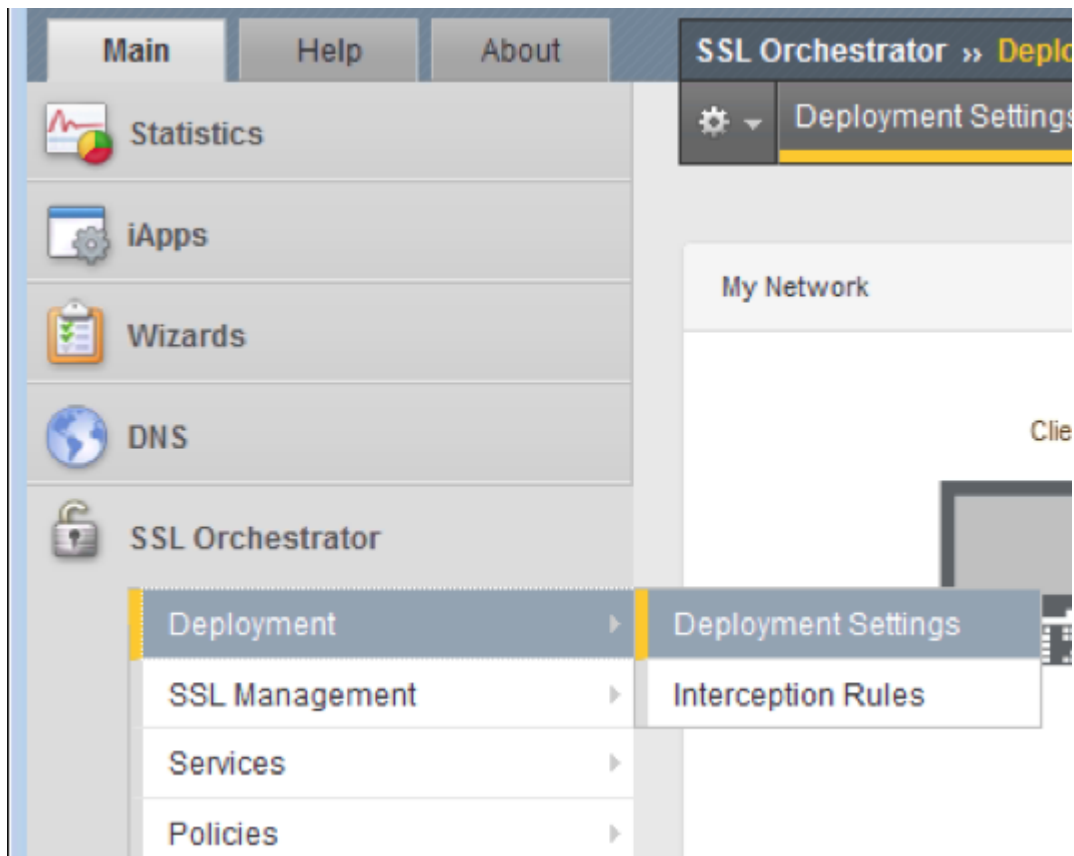
General Properties	
Name	ssloS_L3_service
Description	
IP Family	IPv4 only
Strict Update	<input checked="" type="checkbox"/>
Service Definition	
Auto Manage	<input checked="" type="checkbox"/>
To Service	198.19.64.7/25 Create New...
VLAN	ssloN_L3_in.app/ssloN_L3_in Create New...
Node	<div> <div>IP Address</div> <div>198.19.64.64</div> <div><input type="text"/></div> <div>Add</div> </div>
From Service	198.19.64.245/25 Create New...
VLAN	ssloN_L3_out.app/ssloN_L3_out Create New...
Service Down Action	Ignore
Port Remap	<input type="checkbox"/> Enabled
Resources	
iRules	<div> <div>Selected</div> <div>Filter</div> <div>No available items</div> <div>Available</div> <div> <div><<</div> <div>>></div> <div>▲</div> <div>▼</div> <div>⋮</div> </div> <div> <div>/Common/</div> <div>/Common/</div> <div>/Common/</div> <div>/Common/</div> <div>/Common/</div> <div>/Common/</div> <div>/Common/</div> <div>/Common/</div> </div> </div>
<div> <div>Cancel</div> <div>Finished</div> </div>	

2.2.6 Lab 1.6: TAP Service

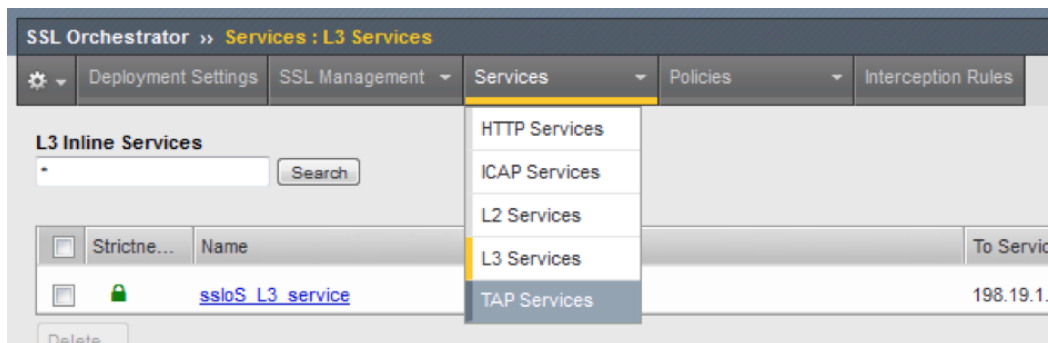
Task 1 - Create SSLO TAP Service

A *Service* is a collection of security devices that will receive decrypted traffic from the SSLO solution. In this section, a *TAP Service* will be created. A TAP Service would typically be an IDS/IPS.

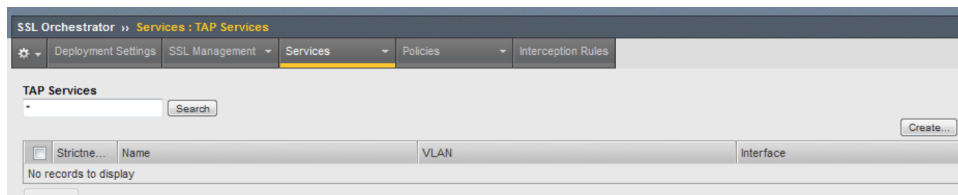
1. Login to the BIG-IP with Firefox
2. Navigate to *SSL Orchestrator* → *Deployment* → *Deployment Settings* and click:



- On the menu across the top of the main window pane navigate to *Services* → *TAP Services* and click:



- Click *Create* on the far right:



- Enter the following values:

Property	Value
Name	ssloS_TAP_service
MAC Address	2c:c2:60:22:e4:23
VLAN	ssloN_TAP_in.app/ssloN_TAP_in
Interface	1.4

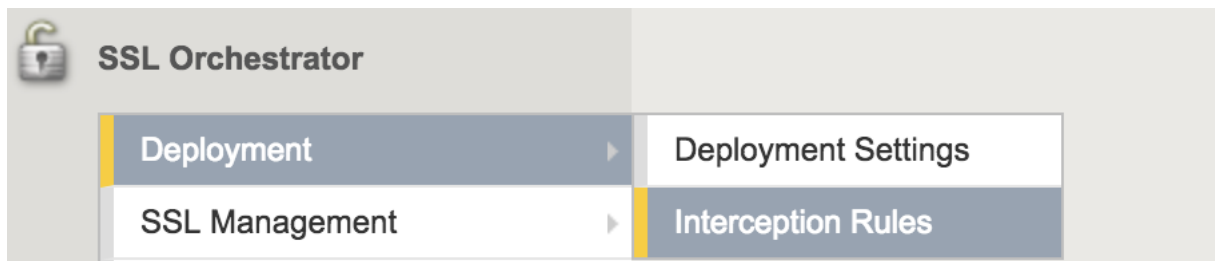
Note: For *VLAN*, use the drop-down menu to select the correct value.

- Once your settings look like the following screenshot, click *Finished*:

2.2.7 Lab 1.7: Outbound Interception Rules

Task 1 - Interception Rules

- Login to the BIG-IP with Firefox
- Navigate to *SSL Orchestrator* → *Deployment* → *Interception Rules* and click:



- Click *Install Default Rules...*

Interception Rules							
<div style="text-align: right;"> Install Default Rules... Create Outbound Rule... Create Inbound Rule... </div>							
Destination Address...	Service Port	Protocol	VLAN	Partition	Policy	SSL	

4. Under *Proxy Settings*, configure these options:

Property	Value
Proxy Scheme	Transparent and Explicit
Proxy Server : Port	10.20.0.150 : 3128

Proxy Settings	
IP Family	IPv4
Proxy Scheme	Transparent and Explicit Proxies
Proxy Server	IPV4 Address : 10.20.0.150 Port : 3128
Classify UDP	<input checked="" type="checkbox"/>
Allow non-UDP/non-TCP	<input checked="" type="checkbox"/>

5. Under *Security* → *SSL*, select *Create New*. This will redirect to a separate page for configuring SSL settings.

Security	
SSL	<div> --choose option Create New... </div>
Per Request Policy	<div> -- choose option </div>

6. Name the configuration *ssloT_ob_ssl*

General Properties	
Name	ssloT_ob_ssl
Description	
Strict Update	<input checked="" type="checkbox"/>

Proxy Section	
---------------	--

7. In the *Client* section, for *Certificate Key Chains*, select *default.crt* and *default.key*, and then click *Add*

Client											
Cipher Type	<input type="radio"/> Cipher Group <input checked="" type="radio"/> Cipher String										
Ciphers	DEFAULT										
Certificate Key Chains	<table border="1"> <thead> <tr> <th>Certificate</th> <th>Key</th> <th>Chain</th> <th>PassPhrase</th> </tr> </thead> <tbody> <tr> <td>/Common/default.crt</td> <td>/Common/default.key</td> <td></td> <td></td> </tr> </tbody> </table> <div style="text-align: right;">Add</div>			Certificate	Key	Chain	PassPhrase	/Common/default.crt	/Common/default.key		
Certificate	Key	Chain	PassPhrase								
/Common/default.crt	/Common/default.key										
	<div> <input type="text" value="/Common/default.crt"/> <input type="text" value="/Common/default.key"/> <input type="text" value="None"/> <input type="text"/> </div> <div style="text-align: right;">Add</div>										

8. Under *CA Certificate Key Chains*, select *subca.f5demolabs.com.cer* and *subca.f5demolabs.com.key*, and then click *Add*.

Certificate Key Chains	<table border="1"> <thead> <tr> <th>Certificate</th> <th>Key</th> <th>Chain</th> <th>PassPhrase</th> </tr> </thead> <tbody> <tr> <td>/Common/default.crt</td> <td>/Common/default.key</td> <td></td> <td></td> </tr> </tbody> </table> <div style="text-align: right;">Add</div>				Certificate	Key	Chain	PassPhrase	/Common/default.crt	/Common/default.key		
Certificate	Key	Chain	PassPhrase									
/Common/default.crt	/Common/default.key											
	<div> <input type="text" value="/Common/default.crt"/> <input type="text" value="/Common/default.key"/> <input type="text" value="None"/> <input type="text"/> </div> <div style="text-align: right;">Add</div>											
CA Certificate Key Chains	<table border="1"> <thead> <tr> <th>Certificate</th> <th>Key</th> <th>Chain</th> <th>PassPhrase</th> </tr> </thead> <tbody> <tr> <td>/Common/subca.f5demolabs.com</td> <td>/Common/subca.f5demolabs.com</td> <td></td> <td></td> </tr> </tbody> </table> <div style="text-align: right;">Add</div>				Certificate	Key	Chain	PassPhrase	/Common/subca.f5demolabs.com	/Common/subca.f5demolabs.com		
Certificate	Key	Chain	PassPhrase									
/Common/subca.f5demolabs.com	/Common/subca.f5demolabs.com											
	<div> <input type="text" value="/Common/subca.f5demolabs.com"/> <input type="text" value="/Common/subca.f5demolabs.com"/> <input type="text" value="None"/> <input type="text"/> </div> <div style="text-align: right;">Add</div>											

9. In the *Server* section, select *ca-bundle.crt* for *Trusted Certificate Authority*. Leave all other settings at the defaults. Click *Finished*.

Server	
Cipher Type	<input type="radio"/> Cipher Group <input checked="" type="radio"/> Cipher String
Ciphers	DEFAULT
Trusted Certificate Authority	<input type="text" value="/Common/ca-bundle.crt"/>
Expire Certificate Response Control	drop
Untrusted Certificate Response Control	drop
OCSP	--choose option
CRL	<input type="text" value="--choose option"/> <input type="button" value="Create New..."/>

10. The screen should have returned to the original *Install Default Rules* page. Under the *Security* section, from the *Per Request Policy* drop-down select *Create New*

Security	
SSL	ssloT_outbound_ssl Create New...
Per Request Policy	-- choose option ▼
Ingress Network	
VLANs	<div> <div>Create New</div> <div> <div>Selected</div> <div>Availab</div> </div> </div>

11. Name the policy *ssloP_ob_pol*

General Properties	
Name	ssloP_ob_pol
TCP Service Chain	

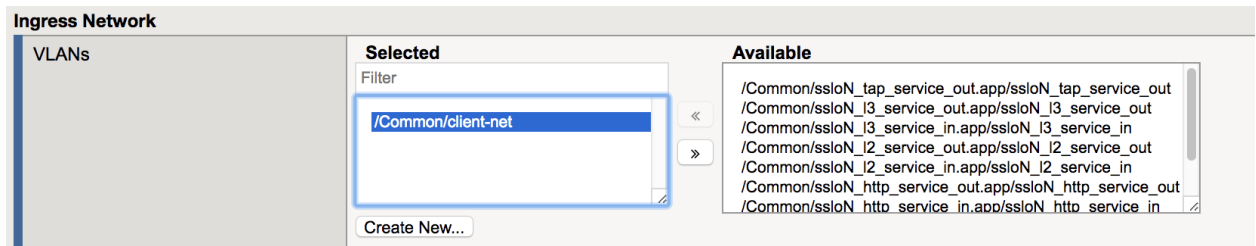
12. Under *TCP Service Chain*, add and order the available services to both the *Intercept Chain* and *Non Intercept Chain*:

TCP Service Chain		
Non Intercept Chain	Selected Filter ssloS_ICAP_service ssloS_HTTP_service ssloS_L3_service ssloS_L2_service ssloS_Tap_service	Available <div></div>
Intercept Chain	Selected Filter ssloS_ICAP_service ssloS_HTTP_service ssloS_L3_service ssloS_L2_service ssloS_Tap_service	Available <div></div>
UDP Service Chain		
Service Chain Sequence	Selected Filter ssloS_L3_service ssloS_L2_service ssloS_Tap_service	Available <div></div>

13. Repeat step (12) for *UDP Service Chain*

14. Click *Finish*.

15. Under *Ingress Network* → *VLANs*, choose */Common/client-net* from the *Available VLANs* and add to the *Selected* section.



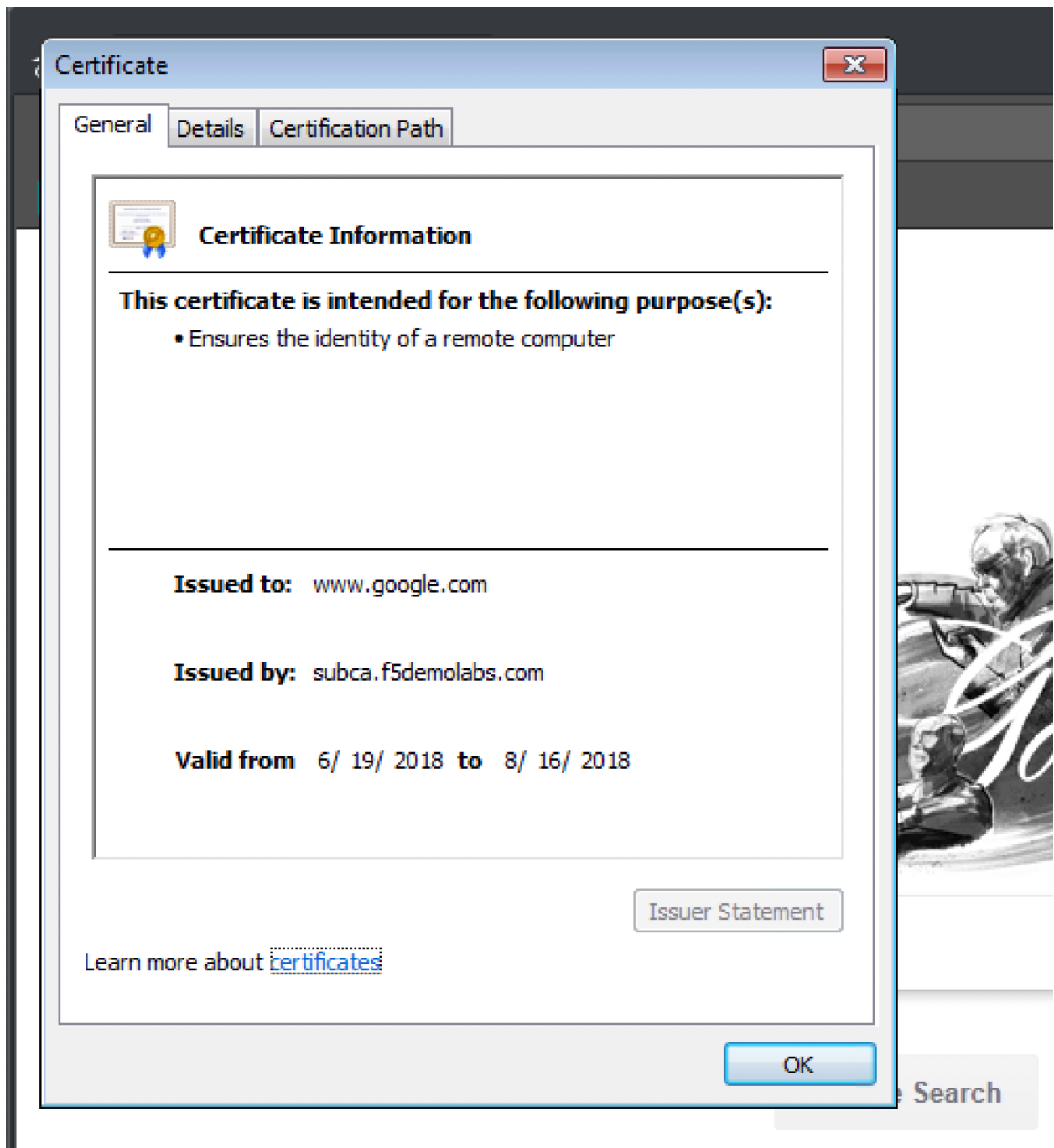
16. Click *Finish*.

2.2.8 Lab 1.8: Testing

In order to test the configuration, we will open an HTTPS website and observe plain text traffic within the inspection zone.

Task 1 - Issuing Requests

1. Open a remote desktop (RDP) session to the Windows 7 Outbound Client and log in with the credentials referenced in the lab topology.
2. Open a web browser and navigate to some HTTPS URLs.
3. Observe the resigned certificate. (Pay attention to the Issued By line.)



4. SSH into the Layer 3 Security device with the credentials in the topology. Run a *tcpdump* with the following parameters:

```
sudo tcpdump -i eth5.60 -X
```

Observe the plain text HTTP traffic.

```

0x0040:  2f3f 7069 643d 3638 3833 2673 3d31 267b  /?pid=6883&s=1&u
0x0050:  726c 3d68 7474 7073 2533 4125 3246 2532  rl=https%3A%2F%2
0x0060:  4666 352e 636f 6d25 3246 2670 6167 6555  Ff5.com%2F&pageU
0x0070:  726c 3d68 7474 7073 2533 4125 3246 2532  rl=https%3A%2F%2
0x0080:  4666 352e 636f 6d25 3246 2672 6566 3d26  Ff5.com%2F&ref=&
0x0090:  636f 6f6b 6965 7354 6573 743d 7472 7565  cookiesTest=true
0x00a0:  266f 7069 643d 3831 3632 2666 6d74 3d6a  &opid=8162&fmt=j
0x00b0:  7326 7469 6d65 3d31 3533 3139 3032 3736  s&time=153190276
0x00c0:  3938 3334 2048 5454 502f 312e 310d 0a55  9834.HTTP/1.1..U
0x00d0:  7365 722d 4167 656e 743a 204d 6f7a 696c  ser-Agent:.Mozil
0x00e0:  6c61 2f35 2e30 2028 5769 6e64 6f77 7320  la/5.0.(Windows.
0x00f0:  4e54 2036 2e31 2920 4170 706c 6557 6562  NT.6.1).AppleWeb
0x0100:  4b69 742f 3533 372e 3336 2028 4b48 544d  Kit/537.36.(KHTM
0x0110:  4c2c 206c 696b 6520 4765 636b 6f29 2043  L,.like.Gecko).C

```

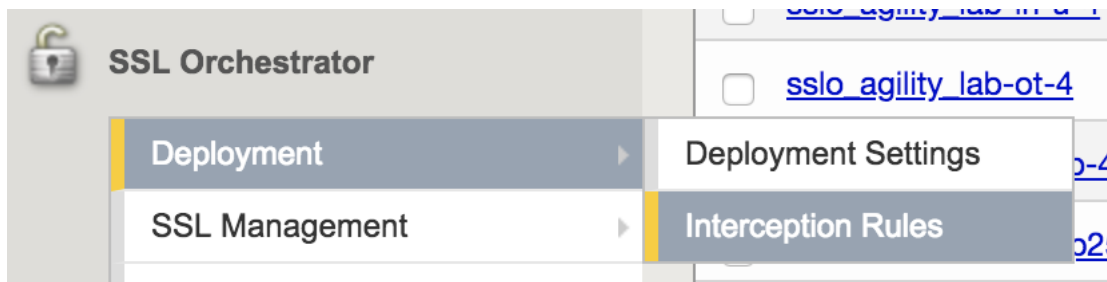
2.3 Module 2: Inbound SSLO

In this lab, we will explore the settings required to deploy **Inbound SSLO**. We will be deploying SSLO in *Transparent Proxy* mode. This single rule will provide visibility for all SSL sites behind the SSLO solution.

2.3.1 Lab 2.1: Inbound Interception Rules

Task 1 - Create a new Interception Rule

1. Navigate to *SSL Orchestrator* → *Deployment* → *Interception Rules*



2. In the top, right hand corner, click *Create Inbound Rule...*

Edit Default Outbound Rules... Create Outbound Rule... Create Inbound Rule...	
Policy	SSL
ssloP_outbound_ssl_prpTcp	ssloT_ob_ssl
ssloP_outbound_ssl_prpTcp	

Task 2 - Create Wildcard Listener

In this step we will create a listener to intercept all inbound HTTPS traffic. After the configuration steps, this will be saved as a wildcard virtual server listening on port 443.

1. Under the *General Properties* section, configure the following values:

Property	Value
Name	ssl_inbound_listener
Destination Address/Mask	0.0.0.0/0
Service Port	443

General Properties	
Name	ssl_inbound_listener
Description	
Configuration	Basic
Label	Inbound
Protocol	TCP
Source Address	0.0.0.0/0
Destination Address/Mask	0.0.0.0/0
Service Port	443

2. Under the *Security Policy* section, select *Create New*.

Security Policy	
SSL settings	None Create New...
L7 Profile Type	None

The configuration GUI will redirect to the SSL settings configuration page.

3. In the *General Settings* section of the Security Policy, set the name to *ssloT_inbound_ssl*.

Note: For **Inbound** configurations the *Forward Proxy* option should be *disabled*

General Properties	
Name	<input type="text" value="ssloT_inbound_ssl"/>
Description	<input type="text"/>
Strict Update	<input checked="" type="checkbox"/>

Proxy Section	
Forward Proxy	<input type="checkbox"/> Enabled

4. Under the *Client-side SSL* section, choose *wildcard.f5demolabs.com.crt* and *wildcard.f5demolabs.com.key* from the respective drop-down menus and click *Add*.

Client-side SSL													
Cipher Type	<input type="radio"/> Cipher Group <input checked="" type="radio"/> Cipher String												
Ciphers	<input type="text" value="DEFAULT"/>												
Certificate Key Chains	<table><thead><tr><th>Certificate</th><th>Key</th><th>Chain</th><th>PassPhrase</th></tr></thead><tbody><tr><td colspan="4"><input type="text" value="/Common/wildcard.f5demolabs.com /Common/wildcard.f5demolabs.com"/></td></tr><tr><td><input type="text" value="/Common/wildcard.f5demolabs.com"/></td><td><input type="text" value="/Common/wildcard.f5demolabs.com"/></td><td><input type="text" value="None"/></td><td><input type="text"/></td></tr></tbody></table> <div><input type="button" value="Add"/></div>	Certificate	Key	Chain	PassPhrase	<input type="text" value="/Common/wildcard.f5demolabs.com /Common/wildcard.f5demolabs.com"/>				<input type="text" value="/Common/wildcard.f5demolabs.com"/>	<input type="text" value="/Common/wildcard.f5demolabs.com"/>	<input type="text" value="None"/>	<input type="text"/>
Certificate	Key	Chain	PassPhrase										
<input type="text" value="/Common/wildcard.f5demolabs.com /Common/wildcard.f5demolabs.com"/>													
<input type="text" value="/Common/wildcard.f5demolabs.com"/>	<input type="text" value="/Common/wildcard.f5demolabs.com"/>	<input type="text" value="None"/>	<input type="text"/>										

5. Under the section *Server-side SSL*, configure the following values:

Property	Value
Expire Certificate Response Control	ignore
Untrusted Certificate Response Control	ignore

The screenshot shows the SSL configuration interface with several sections and fields. Red arrows point to the following elements:

- General Properties:**
 - Name: `ssloT_inbound_ssl`
 - Strict Update: ☒
- Proxy Section:**
 - Forward Proxy: ☐ Enabled
- Client-side SSL:**
 - Cipher Type: ☒ Cipher String
 - Ciphers: `DEFAULT`
 - Certificate Key Chains table:
 - Certificate: `/Common/wildcard.f5demolabs.com`
 - Key: `/Common/wildcard.f5demolabs.com`
 - Chain: `/Common/wildcard.f5demolabs.com`
 - PassPhrase: `None`
- Server-side SSL:**
 - Cipher Type: ☒ Cipher String
 - Ciphers: `DEFAULT`
 - Trusted Certificate Authority: `/Common/ca-bundle.crt`
 - Expire Certificate Response Control: `ignore`
 - Untrusted Certificate Response Control: `ignore`
 - OCSP: `--choose option`
 - CRL: `--choose option` `Create New...`

- Review the settings and click *Finished*. This will redirect back to the original *Inbound Listener* configuration screen.

Task 3 - Configure VLAN Settings

In this step, we will define which VLAN interface that our listener will accept connections.

Note: Since we are configuring only for inbound traffic, it is important that the wildcard listener only accept connections on the incoming interface. In this case, the VLAN labeled *outbound*.

- In the *VLANs* section, choose the `/Common/outbound` VLAN from the *Available List* and click the left arrow to move it into *Selected*.

The screenshot shows the VLAN configuration interface. The **Selected** list contains the entry `/Common/outbound`. The **Available** list contains the following entries:

- `/Common/ssloN_L3_out.app/ssloN_L3_out`
- `/Common/ssloN_L3_in.app/ssloN_L3_in`
- `/Common/ssloN_L2_out.app/ssloN_L2_out`
- `/Common/ssloN_L2_in.app/ssloN_L2_in`
- `/Common/ssloN_HTTP_out.app/ssloN_HTTP_out`
- `/Common/ssloN_HTTP_in.app/ssloN_HTTP_in`
- `/Common/dlp-net`

- Under the *Security Policy* section, configure these values:

Property	Value
L7 Profile Type	HTTP
L7 Profile	/Common/http
Access Profile	/Common/ssloP_outbound_ssl.app/ssloP_outbound_ssl_accessP
Per Request Policy	Create New

Security Policy

SSL settings	ssloT_inbound_ssl ⬇ Create New...
L7 Profile Type	HTTP ⬆ ⬇
L7 Profile	/Common/http ⬆ ⬇
Access Profile	/Common/ssloP_outbound_ssl.app/ssloP_outbound_ssl_accessProfile ⬆ ⬇
Per Request Policy	None ⬇ Edit...

Ingress Network

VLANs

None

/Common/ssloP_inbound_pol.app/ssloP_inbound_pol_prpTcp

/Common/ssloP_outbound_ssl.app/ssloP_outbound_ssl_prpTcp

/Common/ssloP_outbound_ssl.app/ssloP_outbound_ssl_prpUdp

Create New

3. Once redirected to the *New Inbound Rule* configuration:
 - (a) Create a name for the rule
 - (b) Add ICAP, TAP, and L2 services to the *Intercept Chain* section
 - (c) Repeat step (ii) for the *Non Intercept Chain*
 - (d) Click *Finished*

General Properties

Name: ssloP_inbound_pol

TCP Service Chain

Intercept Chain	<p>Selected Services</p> <p>Filter</p> <p>ssloS_ICAP_service ssloS_TAP_service ssloS_L2_service</p>	<p>Available Services</p> <p>ssloS_HTTP_service ssloS_L3_service</p>
Non Intercept Chain	<p>Selected Services</p> <p>Filter</p> <p>ssloS_ICAP_service ssloS_TAP_service ssloS_L2_service</p>	<p>Available Services</p> <p>ssloS_HTTP_service ssloS_L3_service</p>

Cancel Finished

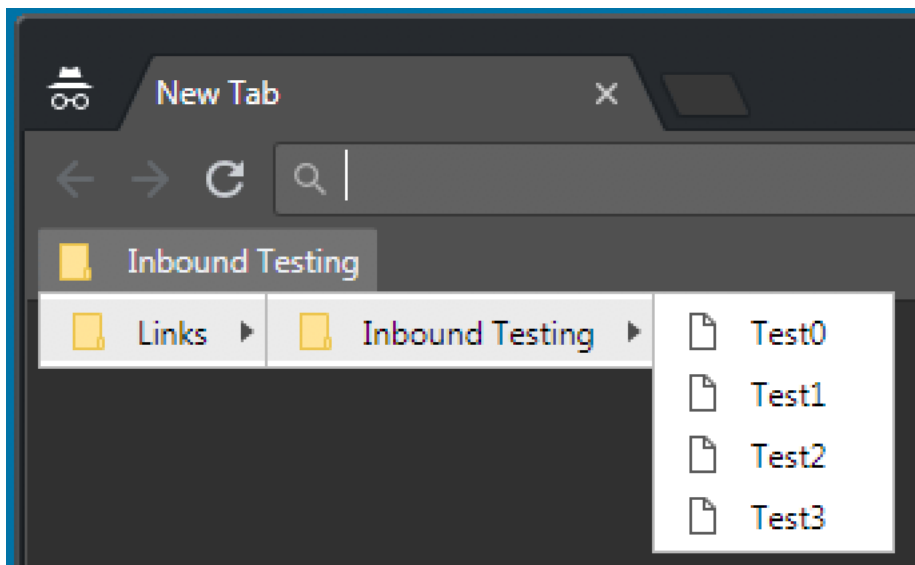
4. Verify the settings under *Security Policy*.

Security Policy	
SSL settings	ssloT_inbound_ssl <input type="button" value="Create New..."/>
L7 Profile Type	HTTP
L7 Profile	/Common/http <input type="button" value="Create New..."/>
Access Profile	/Common/ssloP_outbound_ssl.app/ssloP_outbound_ssl_accessProfile
Per Request Policy	/Common/ssloP_inbound_pol.app/ssloP_inbound_pol_prpTop <input type="button" value="Edit..."/>

5. Click *Finish*

2.3.2 Lab 2.2: Testing

1. Open up a RDP session to the Inbound Win7 Client and log using the documented credentials.
2. Launch Firefox and expand the *Inbound Testing* Bookmarks
3. Use SSH or the console to the Layer 2 Security device and log in using the documented credentials.



4. Choose one of the Test websites and open the page.
5. Run a *tcpdump* with the following parameters:

```
sudo tcpdump -i eth5.60 -X
```

Refresh the web page in the browser and observe the plain text HTTP traffic in the Layer 2 Security device console.

```

0x0040:  2f3f 7069 643d 3638 3833 2673 3d31 2675  /?pid=6883&s=1&u
0x0050:  726c 3d68 7474 7073 2533 4125 3246 2532  rl=https%3A%2F%2
0x0060:  4666 352e 636f 6d25 3246 2670 6167 6555  Ff5.com%2F&pageU
0x0070:  726c 3d68 7474 7073 2533 4125 3246 2532  rl=https%3A%2F%2
0x0080:  4666 352e 636f 6d25 3246 2672 6566 3d26  Ff5.com%2F&ref=&
0x0090:  636f 6f6b 6965 7354 6573 743d 7472 7565  cookiesTest=true
0x00a0:  266f 7069 643d 3831 3632 2666 6d74 3d6a  &opid=8162&fmt=j
0x00b0:  7326 7469 6d65 3d31 3533 3139 3032 3736  s&time=153190276
0x00c0:  3938 3334 2048 5454 502f 312e 310d 0a55  9834.HTTP/1.1..U
0x00d0:  7365 722d 4167 656e 743a 204d 6f7a 696c  ser-Agent:.Mozil
0x00e0:  6c61 2f35 2e30 2028 5769 6e64 6f77 7320  la/5.0.(Windows.
0x00f0:  4e54 2036 2e31 2920 4170 706c 6557 6562  NT.6.1).AppleWeb
0x0100:  4b69 742f 3533 372e 3336 2028 4b48 544d  Kit/537.36.(KHTM
0x0110:  4c2c 206c 696b 6520 4765 636b 6f29 2043  L,.like.Gecko).C

```

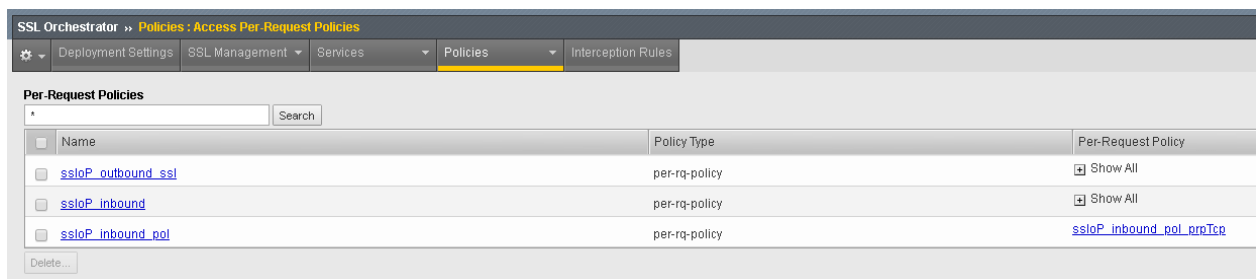
2.4 Module 3: Service Policies

In this lab, we will review and modify the *Service Policies* that are created by the **Inbound** and **Outbound** SSLO templates. Service Policies provide the classification to provide Dynamic Service chaining.

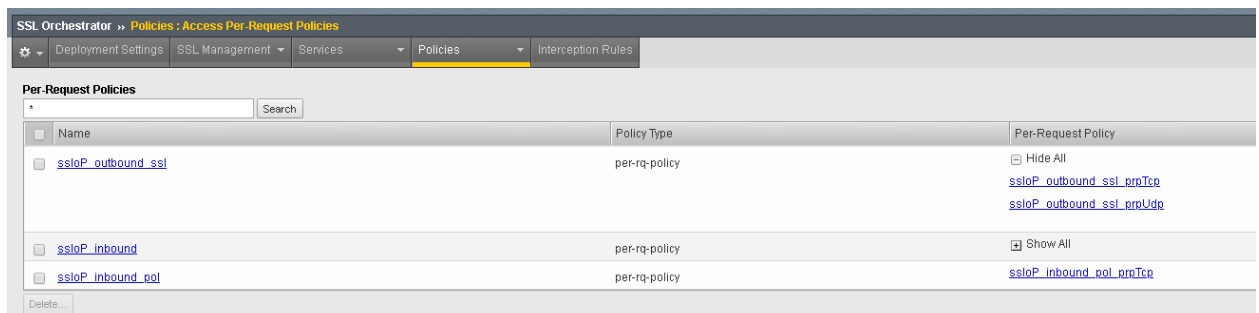
2.4.1 Lab 3.1: Reviewing the Policies

Task 1 - View the Per-Request Policies

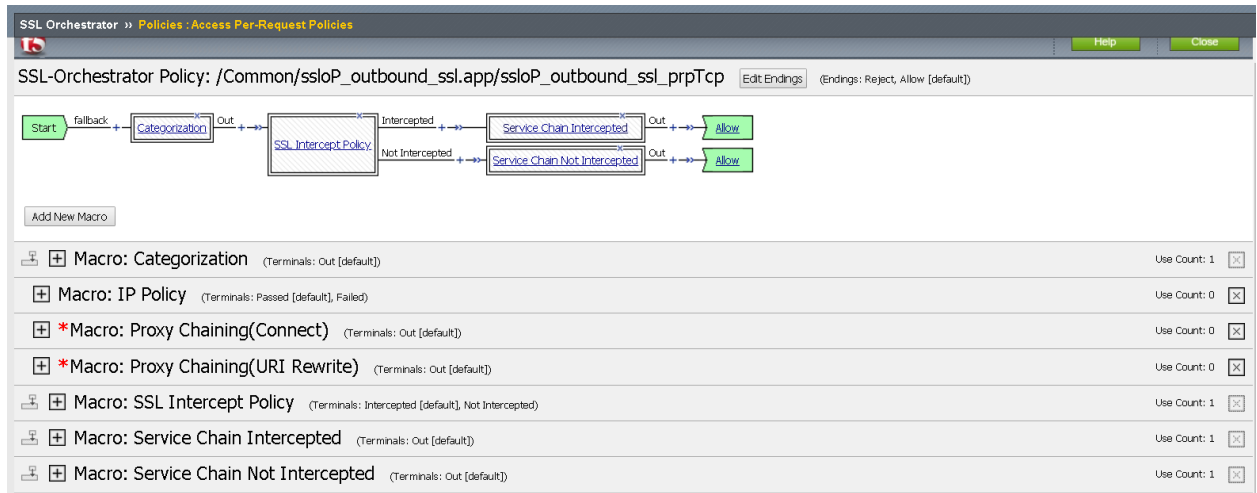
1. Login to the BIG-IP with Firefox
2. Navigate to *SSL Orchestrator* → *Policies* → *Access Per-Request Policies*



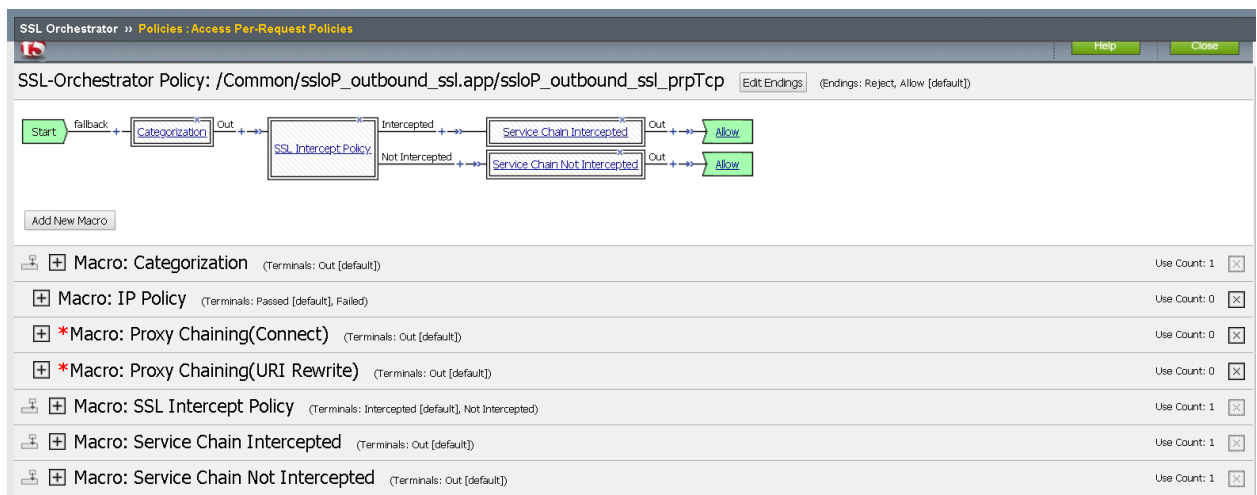
3. Click the plus sign next to *Show all* for the *ssloP_outbound_ssl* row
4. Select the *ssloP_outbound_ssl_prpTcp* Per-Request policy



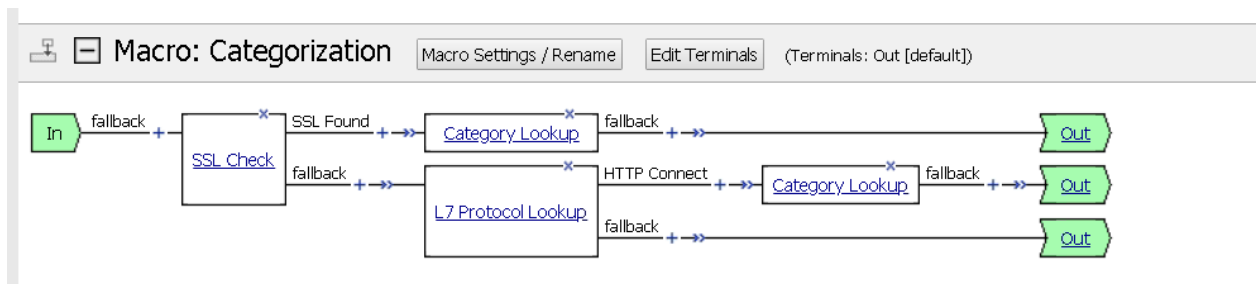
5. Review the general flow from categorization through Intercept policy to Service Chain

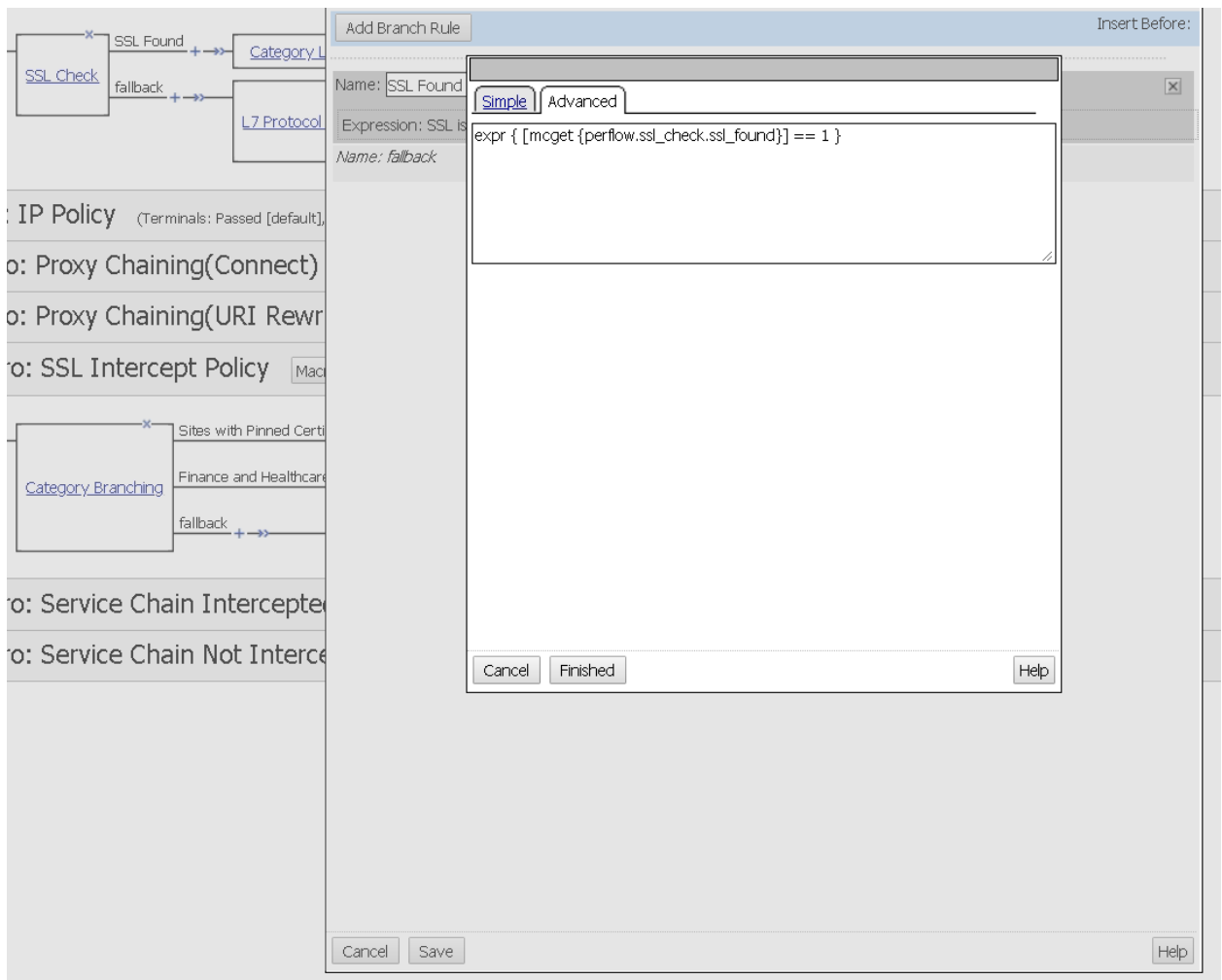


6. Expand the *Macro: Categorization* macro by clicking on *Categorization* in the boxed area or the plus symbol in the macro section.

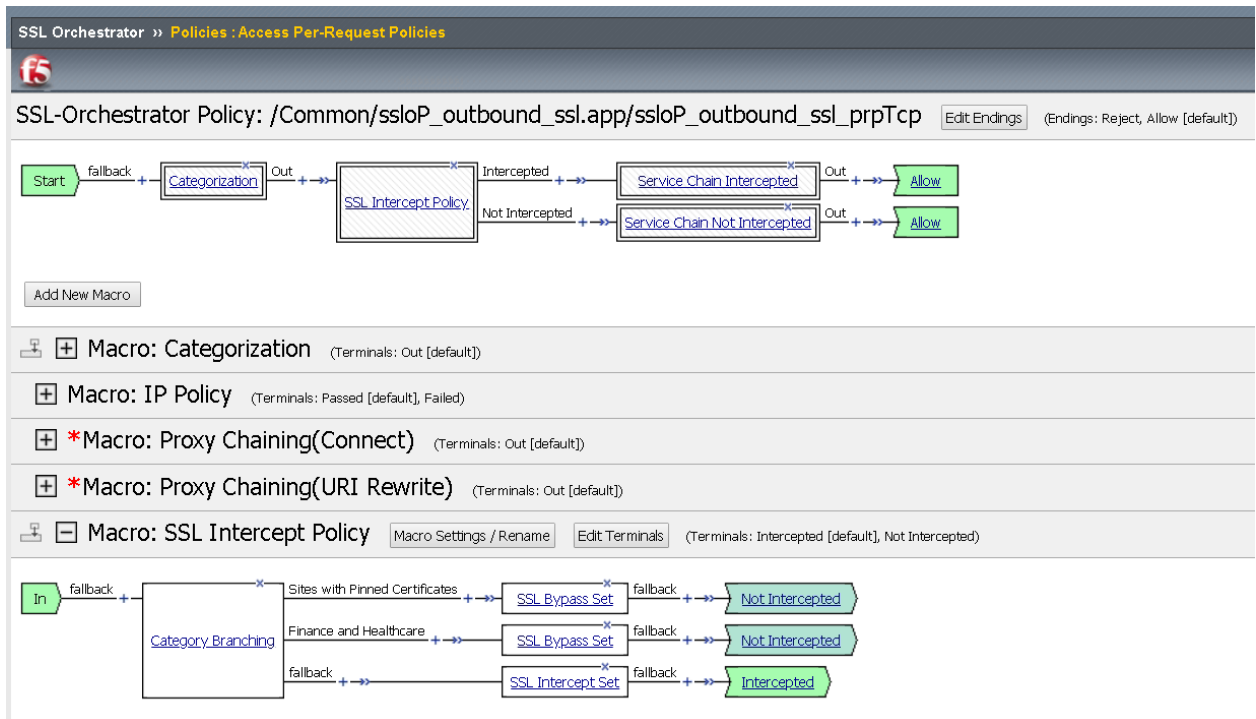


7. Explore the *SSL Check* advanced Action Properties





8. Expand the *SSL Intercept Policy* macro. Notice that the *Not Intercepted* and *Intercepted* terminal endings differ based on the category and setting interception.



9. Explore the *Category Branching* Action Property

SSL Orchestrator » Policies : Access Per-Request Policies

SSL-Orchestrator Policy: /Common/ssloP_outbound_ssl.app/ssloP_outbound_ssl_prpTcp [Edit Endings](#) (Endings: Reject, Allow [default])

Add New Macro

- Macro: Categorization (Terminals: Out [default])
- Macro: IP Policy (Terminals: Passed [default], Failed)
- *Macro: Proxy Chaining(Connect) (Terminals: Out [default])
- *Macro: Proxy Chaining(URI Rewrite) (Terminals: Out [default])
- Macro: SSL Intercept Policy [Macro Settings / Rename](#) [Edit Terminals](#) (Terminals: Intercepted [default], Not Intercepted)

Properties Branch Rules

Add Branch Rule Insert Before: 1: Sites with Pinned Certificates

Name: Sites with Pinned Certificates

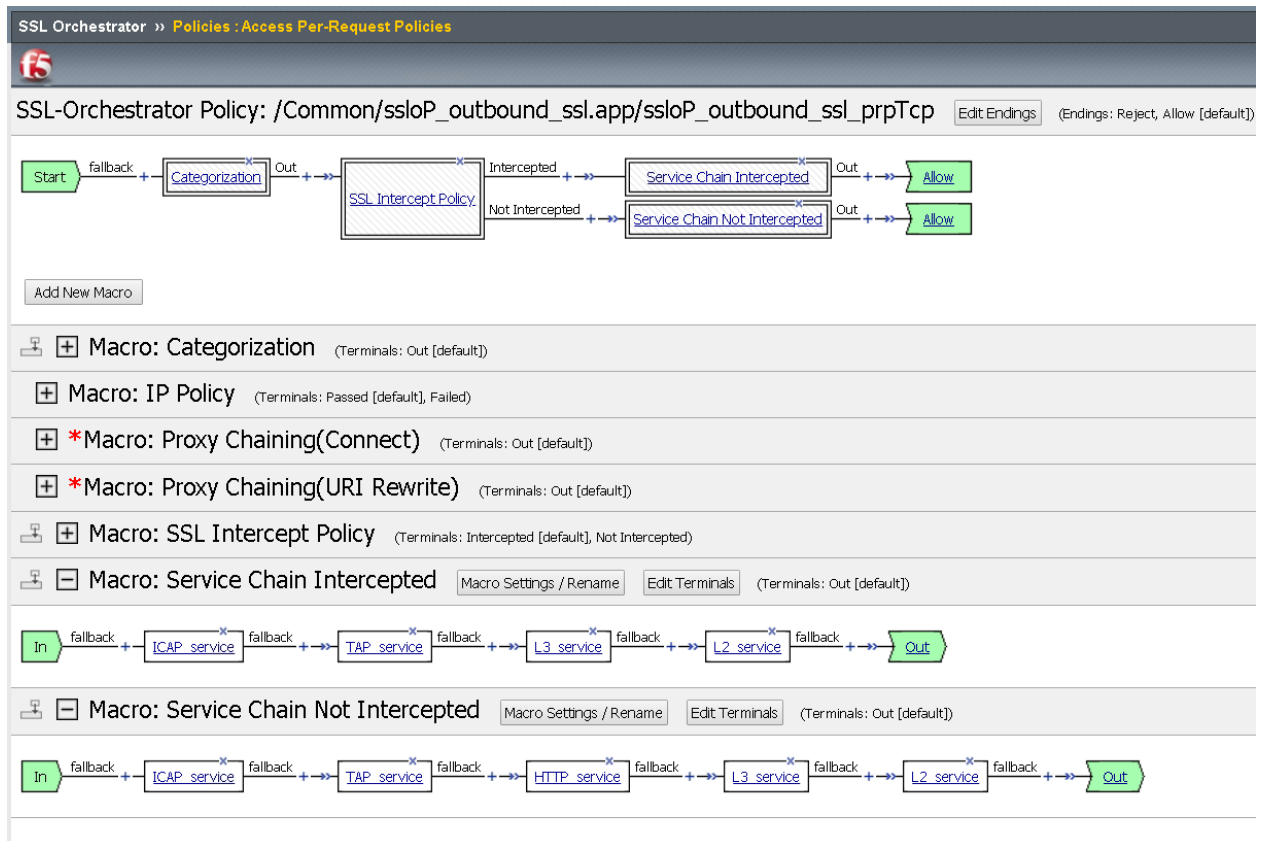
Expression: Category is -Custom- Pinners [change](#)

Name: Finance and Healthcare

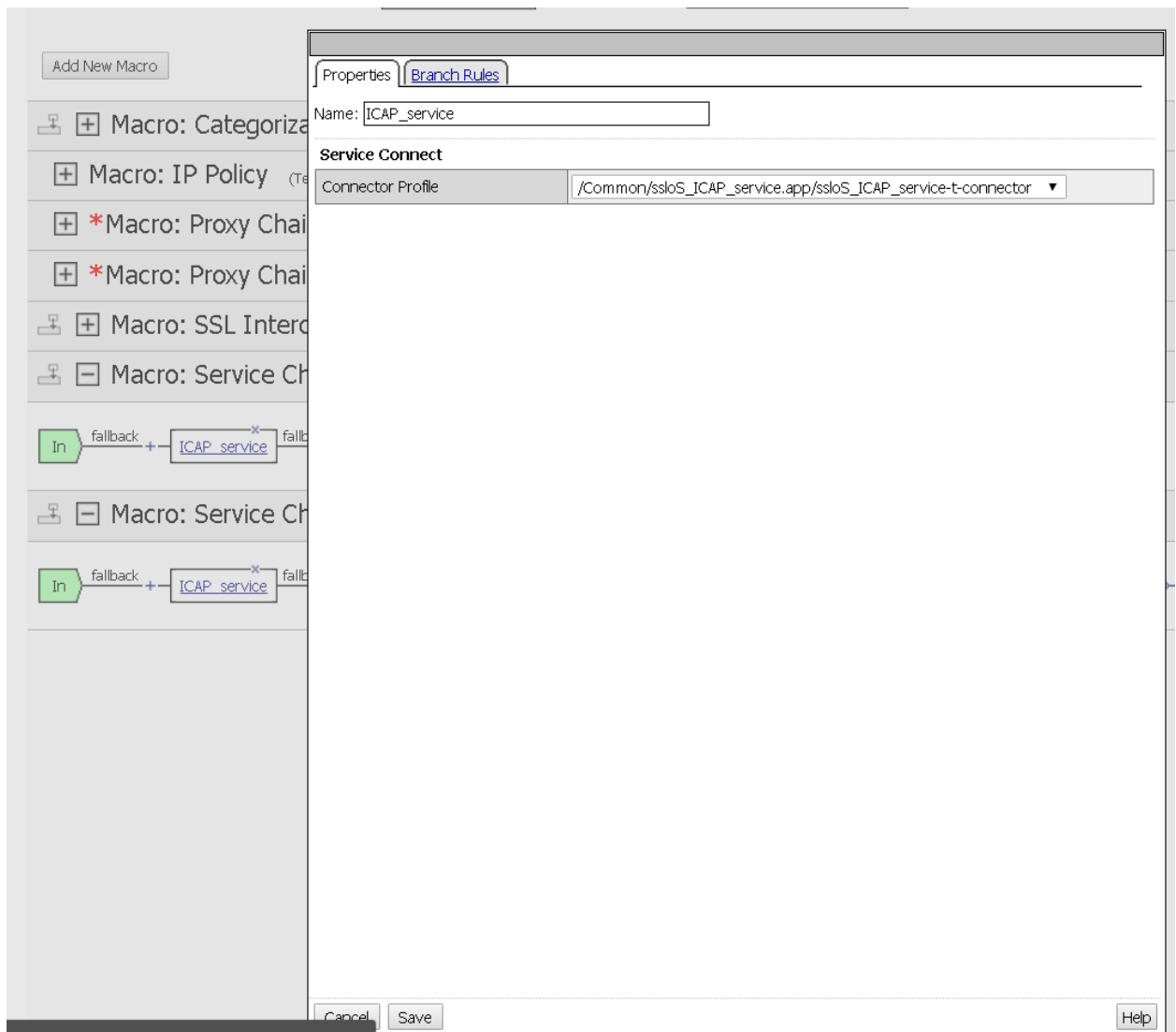
Expression: Category is Financial Data and Services
OR Category is Health and Medicine [change](#)

Name: fallback

10. Expand the macros *Service Chain Intercepted* and *Service Chain Not Intercepted*

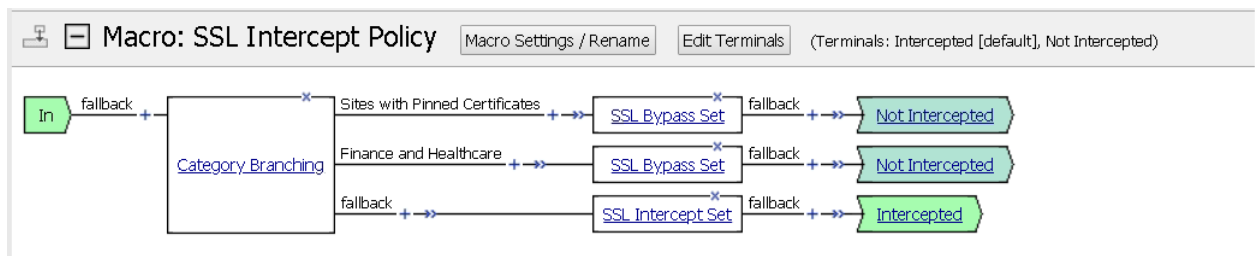


11. Explore the Action Properties in the Service Chains and notice the *Connector Profiles*




Task 2 - Modify the Intercept Policy


1. Expand the macro *SSL Intercept Policy* and click the *Intercepted* terminal ending



2. Select the *Not Intercepted* radio button, then *Save*

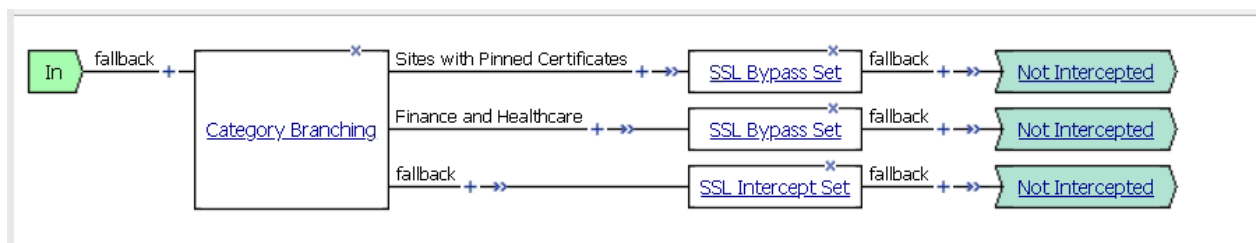
Select Terminal:

☒ Intercepted 

☐ Not Intercepted 

Cancel Save Help

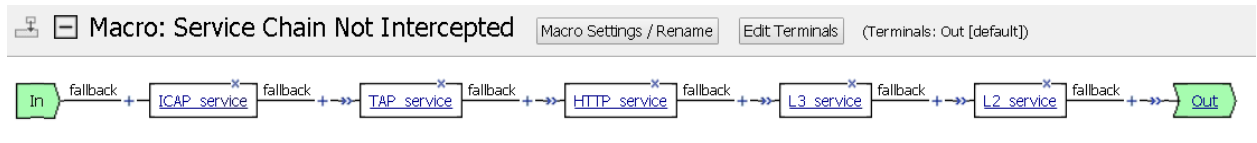
Note: Notice that now all traffic is bypassed and therefore **not** decrypted



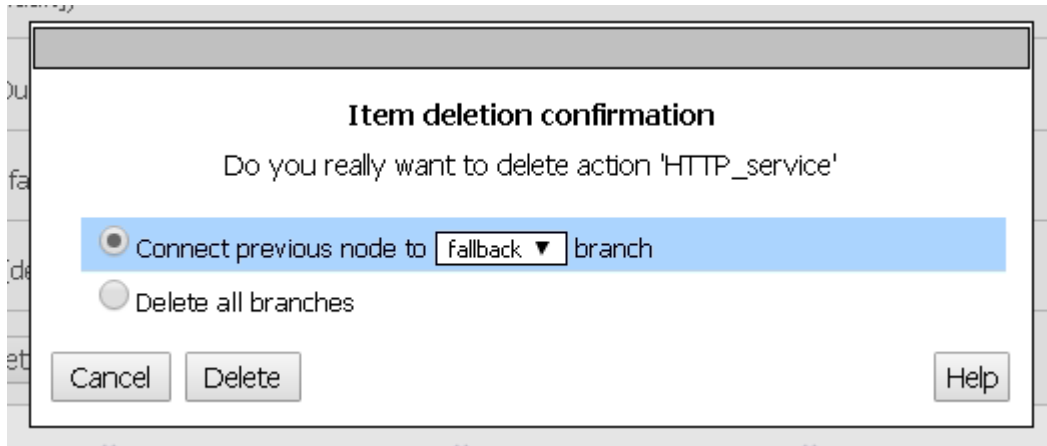
3. Repeat the test from [Lab 1.8](#) and notice that traffic is not decrypted. Notice that this had the impact of all traffic bypassing inspection zone.
4. Undo the change by setting the terminal ending back to *Intercepted* and repeat test.

Task 3 - Modify Service Chain

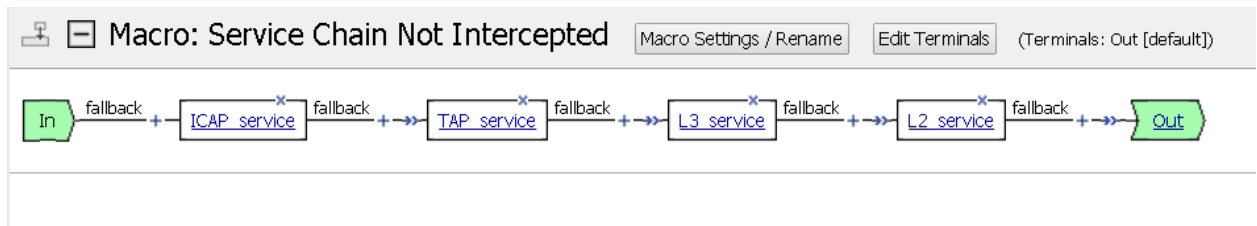
1. Expand the macro named *Service Chain Not Intercepted* and remove the *HTTP Service* node by selecting the X in the corner. The X will turn red when you hover over it.



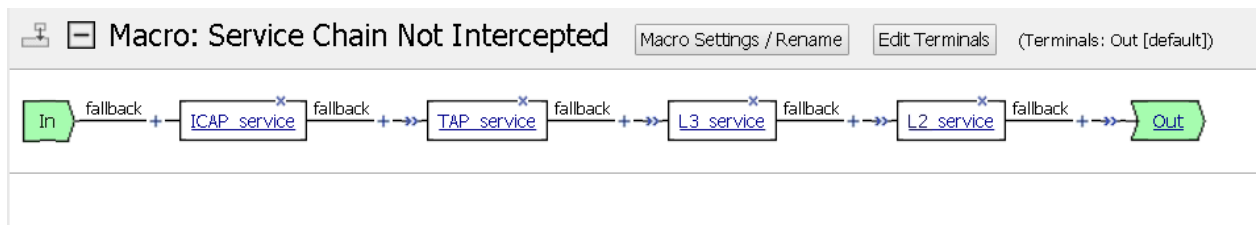
2. Click the *Delete* button in the Item delete confirmation dialogue box



3. View your results



4. Add the *HTTP Service* node back by selecting the plus key between *TAP* and *L3* services



5. Select the *Traffic Management* tab, then the *Service Connect* item and click *Add Item*

Begin typing to search

Assignment

Endpoint Security (Server-Side)

Classification

General Purpose

Traffic Management

SSLO Macros

<input type="radio"/>	Proxy Select	Proxy Select
<input checked="" type="radio"/>	Service Connect	Service Connect
<input type="radio"/>	Session Check	Session Check

Cancel

Add Item

Help

6. Change the *Name* to *HTTP Service*, choose the HTTP Service item from the *Connector Profile* drop down menu named */Common/ssloS_HTTP_server.app/ssloS_HTTP_service-t-connector* and then click *Save* at the bottom

Properties*

Branch Rules

Name: HTTP Service

Service Connect

Connector Profile	
	<div><div>/Common/ssloS_HTTP_service.app/ssloS_HTTP_service-t-connector ▾</div><div>None</div><div>/Common/connector</div><div>/Common/ssloS_ICAP_service.app/ssloS_ICAP_service-t-connector</div><div>/Common/ssloS_TAP_service.app/ssloS_TAP_service-u-connector</div><div>/Common/ssloS_TAP_service.app/ssloS_TAP_service-t-connector</div><div>/Common/ssloS_HTTP_service.app/ssloS_HTTP_service-t-connector</div><div>/Common/ssloS_L3_service.app/ssloS_L3_service-t-connector</div><div>/Common/ssloS_L3_service.app/ssloS_L3_service-u-connector</div><div>/Common/ssloS_L2_service.app/ssloS_L2_service-u-connector</div><div>/Common/ssloS_L2_service.app/ssloS_L2_service-t-connector</div></div>

Cancel

Save

(*Data in tab has been changed, please don't forget to save)

Help

