FortiADC - SSLi Deployment Guide

Version 7.2.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

February 3, 2023
FortiADC 7.2.0 SSLi Deployment Guide
01-540-000000-20200207

TABLE OF CONTENTS

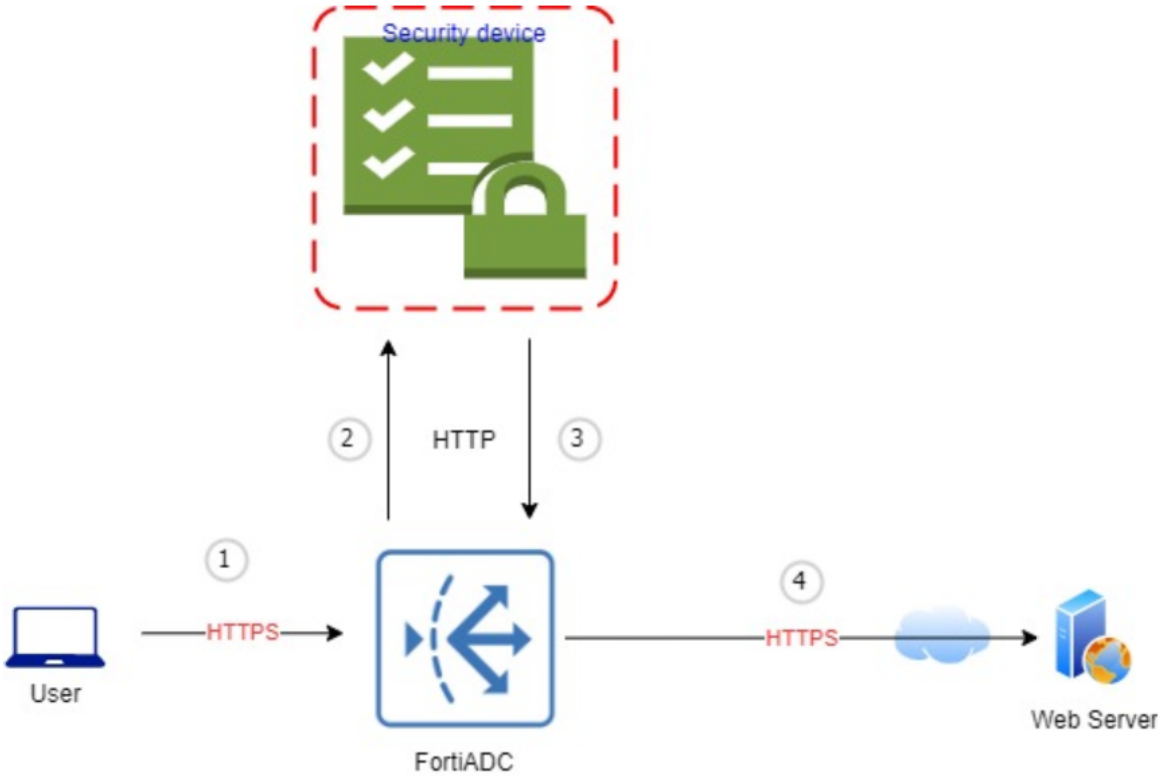
Change Log **4**
Introduction **5**
Deployment **6**
Enabling SSL mode 6
Scenario 1 – Layer 2 Transparent Proxy 7
Scenario 2 – Layer 3 Transparent Proxy 13
Scenario 3 – Layer 7 Reverse Proxy 17
Troubleshooting **21**

Change Log

Date	Change Description
2020-12-22	Initial release.

Introduction

Traditional security devices have the ability to inspect HTTP traffic, however, such devices cannot inspect SSL or encrypted traffic without incurring heavy CPU resources. This limitation raises concerns as the volume of the encrypted traffic is increasing and is expected to surpass the volume of unencrypted traffic. Considering the immense possibility of cyber threats propagating through encrypted traffic, it is essential that organizations configure their security devices to inspect both encrypted and unencrypted traffic.



Deploy FortiADC as an SSLi Proxy in your organization to dedicatedly decrypt SSL traffic, which can then be analyzed by a security device. Since the encryption and decryption functions are performed by the FortiADC, there is minimum latency in the network.

This document will show you how to quickly set up FortiADC as SSLi proxy. Before you begin, you must:

- Have Read-Write permission for System settings.
- Have the CA certificate that added to Local Certificate (optional)
- Have the Security Device connected to FortiADC (SSLi proxy)

Deployment

When FortiADC is configured with SSLi mode, it acts as the SSL proxy to decrypt and encrypt SSL connections between the client and the server.

FortiADC terminates the SSL session from the client and establishes a new SSL session to the server. A certificate authority (CA) certificate and private key need to be installed on FortiADC with the "Forward Proxy" function enabled so that the server certificates can be successfully proxied and re-signed to the client.

FortiADC gets the original certificate from the server, but instead of forwarding the same certificate to the client, it creates a new one with the same CN but with different issuer and public key. This derived certificate is signed by "Local Signing CA" that is trusted by the client, so the client completes its handshake with FortiADC, and FortiADC decrypts the traffic to the security device and encrypts it to the destination.

The SNI (Server Name Indication) is a TLS extension that indicates the hostname of the SSL server that the client wants to connect to. In this version (FortiADC v6.1.0), it's a known issue that the SNI sometimes is unable to be forwarded to the destination web server, which will cause some website to be inaccessible. We will fix this issue soon.

Limitations for the SSLi function:

- DDoS prevention is only supported in L7 Reverse Proxy.
- Bypass function is only supported in L2/L3 transparent proxy.
- RS_pool only supports one member (RS).
- vDOM is not supported.
- IPv6 is only supported in L7 Reverse Proxy.
- Pre-login disclaimer message configuration is not supported.

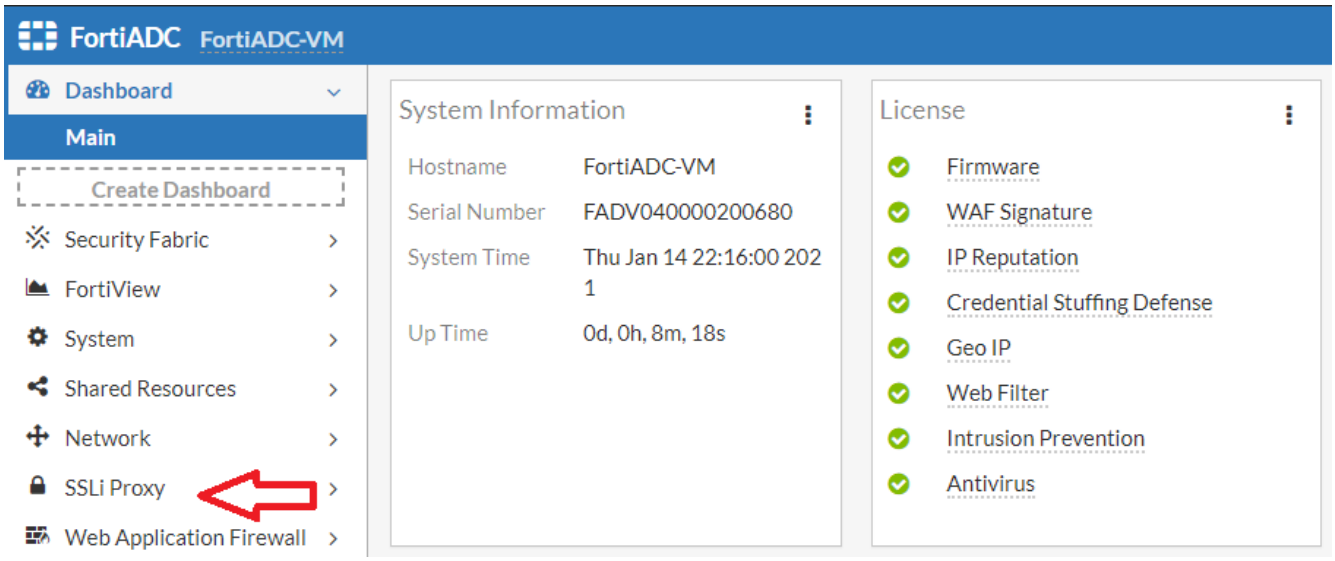
Enabling SSL mode

Before beginning the deployment, you should enable the SSLi mode on FortiADC first. All the settings on the FortiADC will be erased.

```
execute ssli mode enable
```

This operation will change all settings to factory defaults. FortiADC will reboot.

You will see the **SSLi Proxy** menu if the SSLi mode is enabled.



When FortiADC is working in SSLi mode, the following features are not supported and are removed from GUI and CLI.

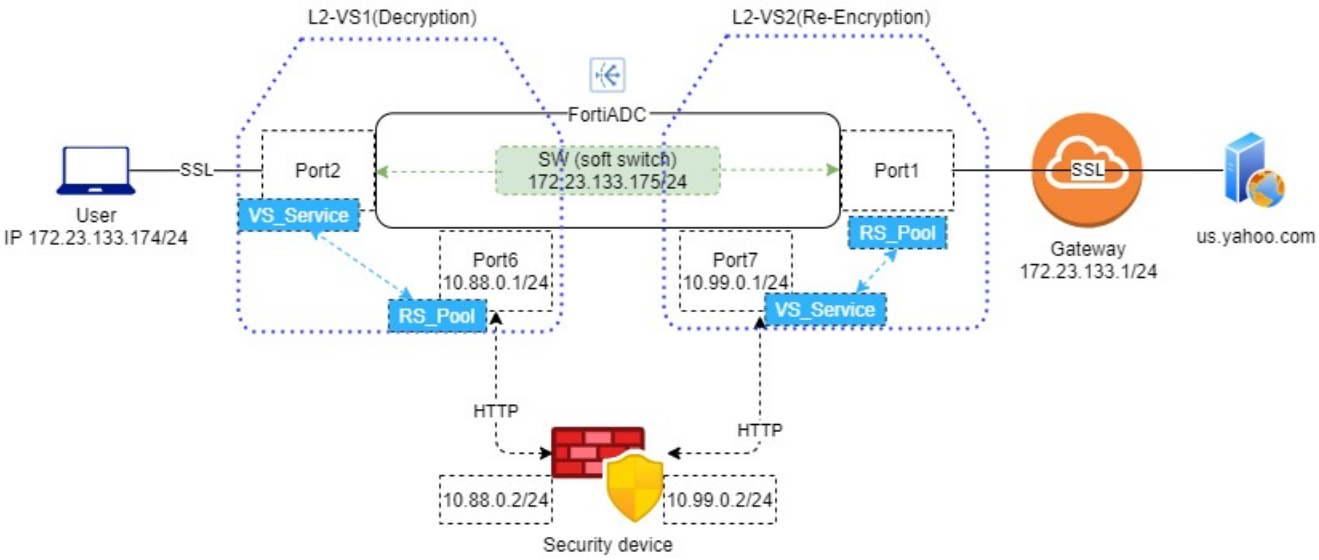
- GLB, LLB
- Intrusion Prevention, IP Reputation, Geo IP Protection
- Central Management, User Authentication

All settings related to SSLi must be configured through the GUI. We do not support configuring this function through CLI, but you can view all the SSLi configurations by CLI.

Scenario 1 – Layer 2 Transparent Proxy

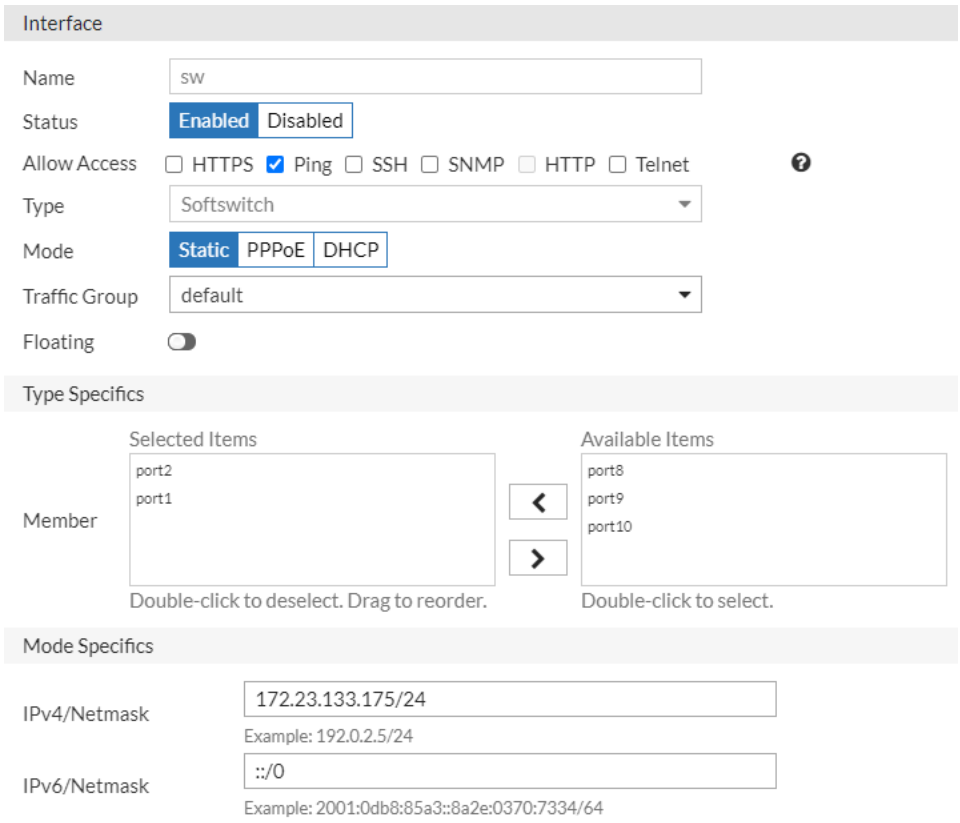
This is the most common deployment type, the client and FortiADC are on the same subnet. They don't need to have IP address changed. This topology is also known as a stealth firewall.

Topology



Creating a Soft-switch

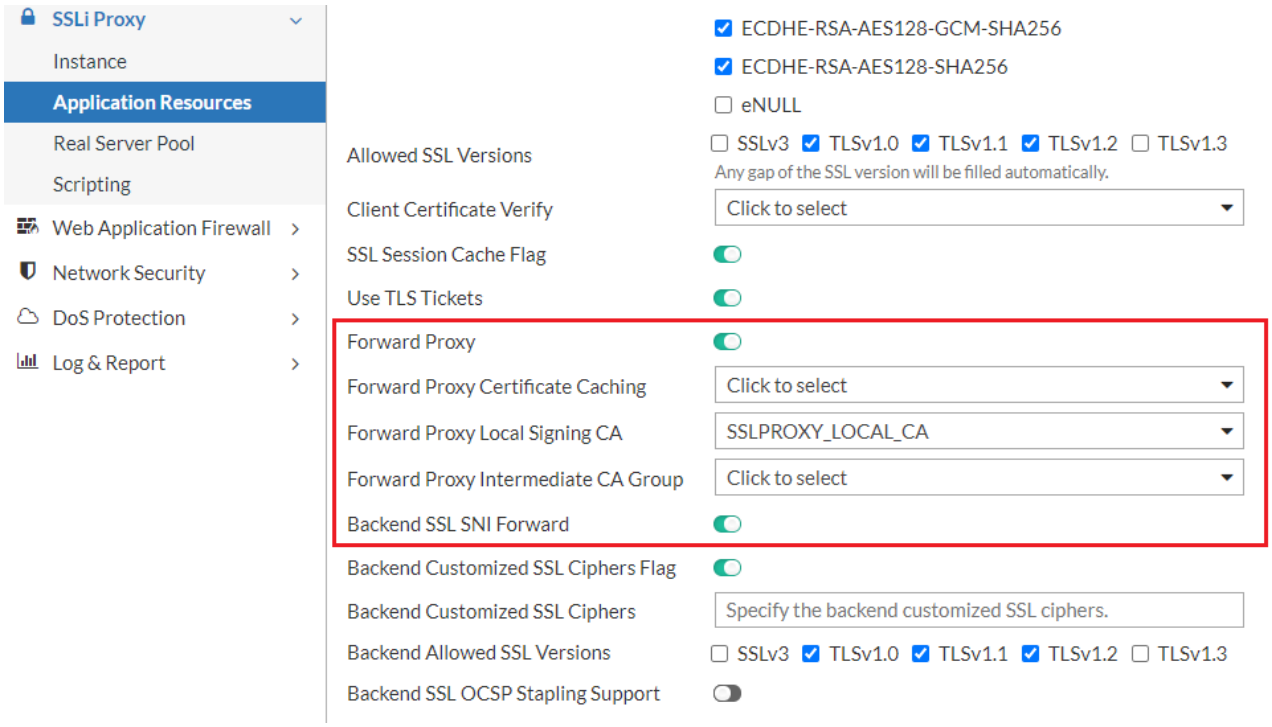
1. Go to Network > Interface, then click the tab Interface.
2. Click Create New to display the configuration editor.
3. Complete the key configuration as shown in the screenshot.
   - **Name:** Enter a unique name for the soft-swtich name
   - **Type:** Select the Softswtich
   - **Member in Type Specifics:** Bind the ports facing the client side and gateway side. In the above topology, that is Port1 and Port2.
   - **IPv4 in Mode Specifics:** Type the address of the softswitch. In the above topology, that is 172.23.133.175/24.



4. Save the configuration.

Creating Client SSL Profile for SSLi instance

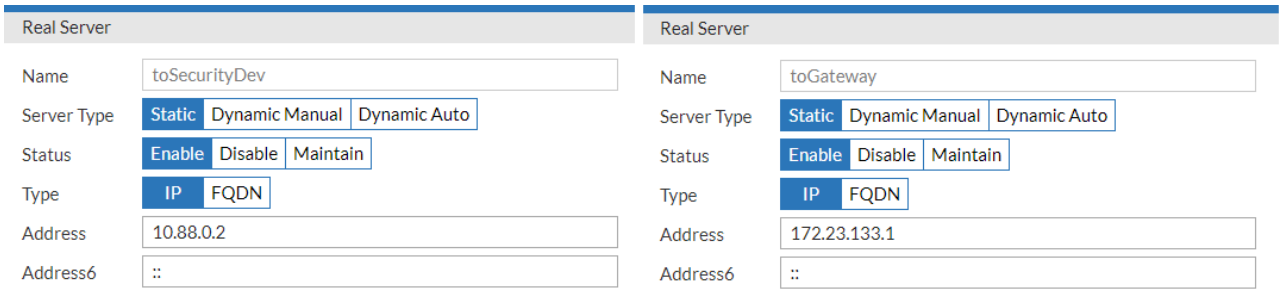
1. Go to SSLi Proxy > Application Resources, then click the tab Client SSL.
2. Click Create New > Advanced Mode to display the configuration editor.
3. Complete the key configuration as shown in the screenshot.
   - **Name:** Enter a unique name for the SSLi instance name.
   - **Forward Proxy:** Enable this option.
   - **Forward Proxy Local Signing CA:** Select a CA certificate that your client trusts it.
   - **Backend SSL SNI Forward:** Enable this option.



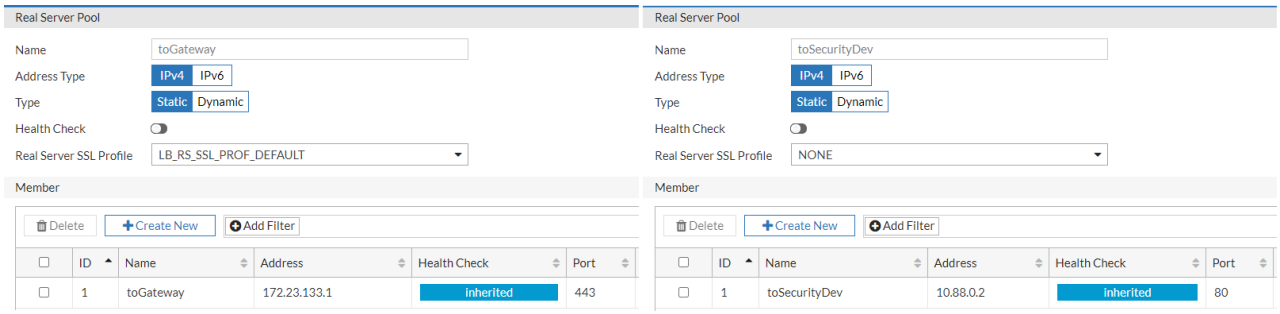
4. Save the configuration.

Creating Real Server Profile for SSLi instance

1. Go to SSLi Proxy > Real Server Pool, then click the tab Real Server.
2. Click Create New to display the configuration editor.
3. Complete the key configuration as shown in the screenshot. Here we need to add two real servers, one connecting with the gateway, and the other connecting with the security device.
   - **Name:** Enter a unique name for the Real Server.
   - **Address:** Enter the correct IP address.



4. Save the configuration.
5. Go to SSLi Proxy > Real Server Pool, then click the tab Real Server Pool. Here we need to create two real server pools containing the above two real servers respectively.
6. Click Create New to display the configuration editor.
7. Complete the key configuration as shown in the screenshot.
   - **Name:** Enter a unique name for the Real Server Pool.
   - **Real Server SSL Profile:** Enable SSL on the real server to the gateway side, and disable SSL on the one to the security device side.
   - **Member:** Select the correct the real server in your topology.

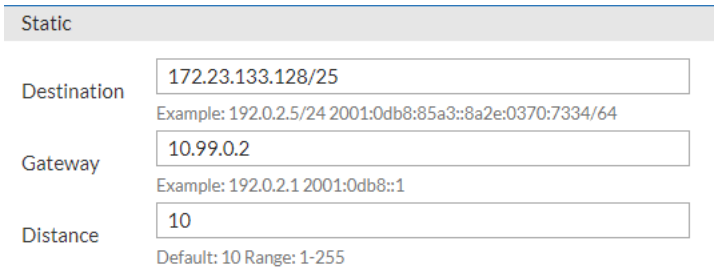


8. Save the configuration.

Configuring Static Routing

1. Go to Network > Routing, then click the tab Static.
2. Click Create New to display the configuration editor.
3. Complete the key configuration as shown in the screenshot.
   - **Destination:** Enter a Client IP address scope.
   - **Gateway:** Enter a Security Device IP address which in the Re-encryption side.
4. Save the configuration.

This static routing forwards the packets whose destination is the client IP to the security device.

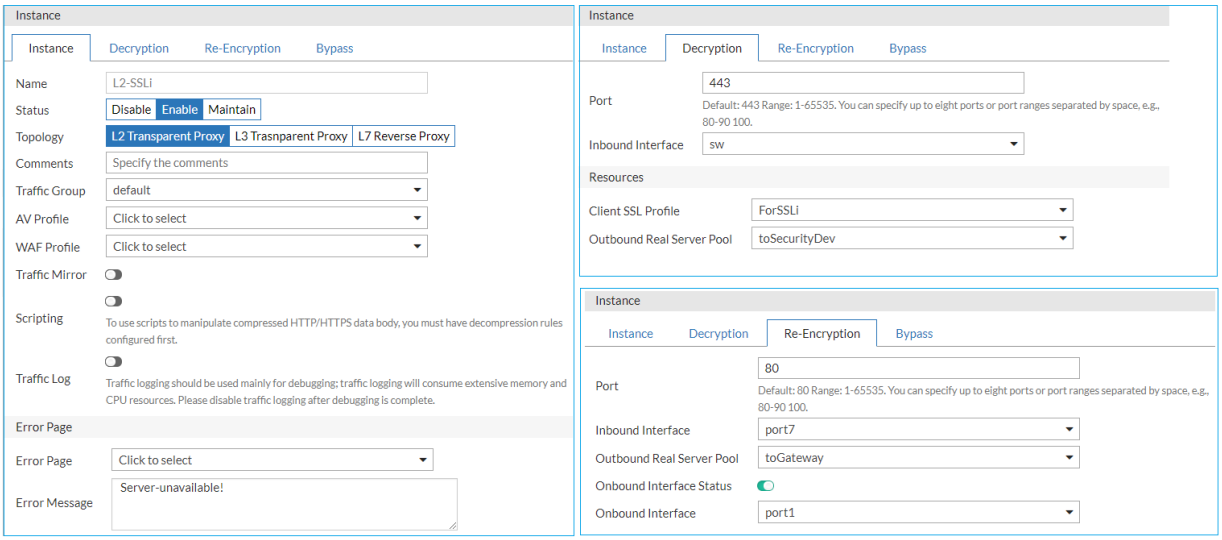


Creating SSLi instance for L2 deploy

1. Go to SSLi Proxy > Instance, then click the tab Instance.
2. Click Create New > Advanced Mode to display the configuration editor.
3. Complete the key configuration as shown in the screenshot.
   - **Name:** Enter a unique name for the SSLi instance.
   - **Topology:** Select the L2 Transparent Proxy.
   - Decryption tab
     - **Inbound Interface:** Select the Softswitch type interface you just created.
     - **Client SSL Profile:** Select the client SSL profile you just created.
     - **Outbound Real Server Pool:** Select the server pool to the security device.
   - Re-encryption tab
     - **Inbound Interface:** Select an interface connected to the security device side.
     - **Outbound Real Server Pool:** Select the server pool to the gateway side.
     - **Onbound Interface Status:** Enable this option.
     - **Onbound Interface:** Select the interface connected to the gateway side.

     If you have configured both L7 and L2/L3 instances for the same security device (attached to the same subnets), their port numbers must not be the same. We will remove this restriction in later releases.

4. Save the configuration.



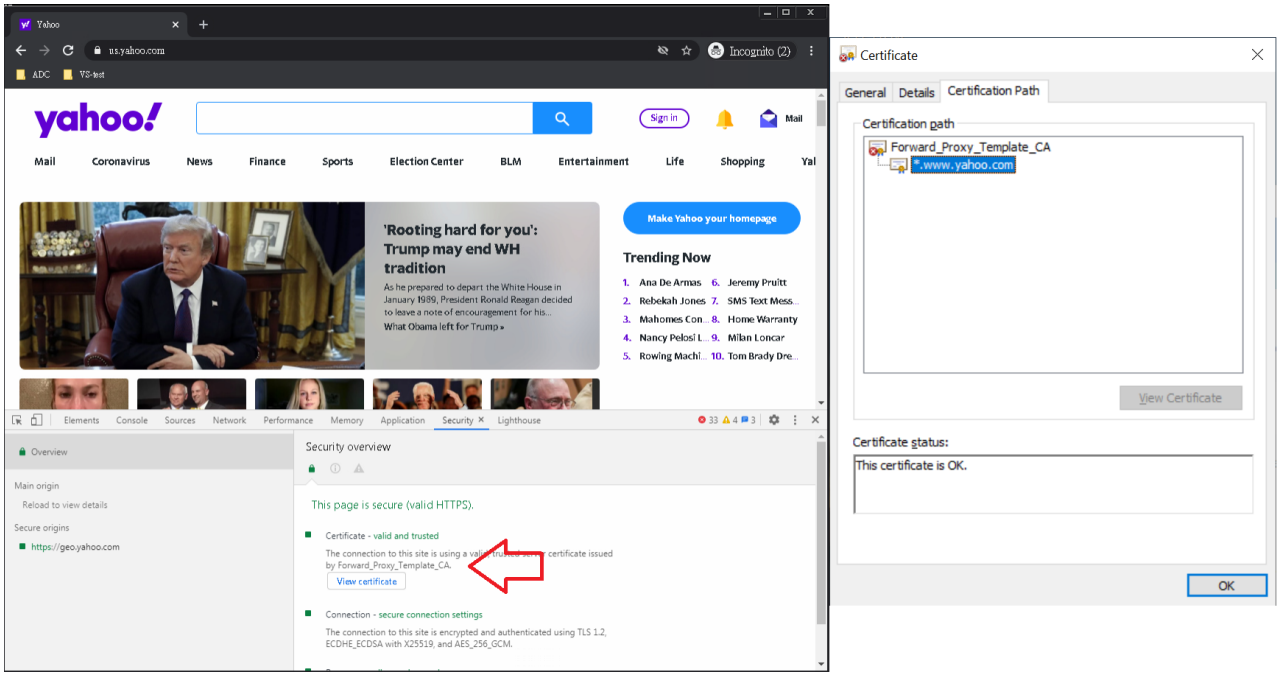
Enabling rt-cache-strict

Run the following command:

```
config router setting
   set rt-cache-strict enable
      config rt-cache-reverse-exception
   end
end
```

Client side: install CA and try the SSLi function

1. Install the Local Signing CA that FortiADC selected.
2. Open the browser and navigate to https://us.yahoo.com, you will see the derived certificate is signed by "Local Signing CA".



Testing SSLi deployment

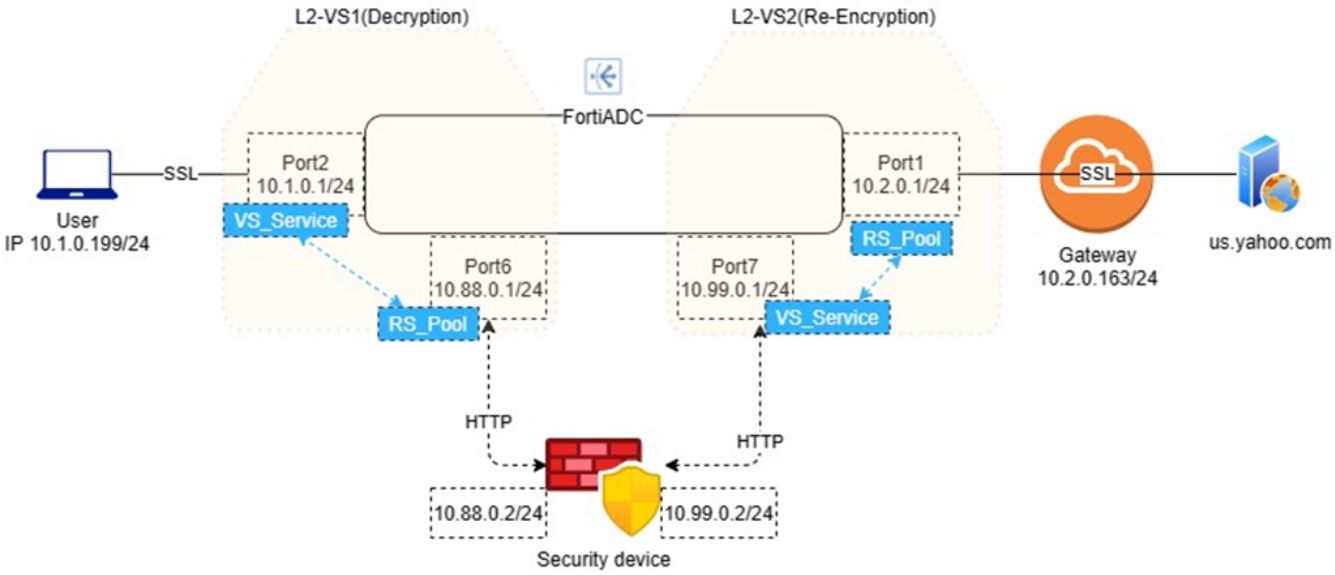
To test the deployment, check if the plain HTTP traffic is logged on the security device.

No.	Time	Source	Destination	Protocol	Length	Info
…	4.392964	172.23.133.174	173.222.182.94	HTTP	1425	GET /pixel.gif?e=9&q=5&hp=1&vb=-1&kq=1&lo=0&uk=null&pk=0&
…	4.425905	173.222.182.94	172.23.133.174	HTTP	451	HTTP/1.1 200 OK (GIF89a)
…	4.848770	172.23.133.174	180.222.102.201	HTTP	1366	GET / HTTP/1.1
…	4.850785	172.23.133.174	180.222.102.201	HTTP	679	GET /sdarla/php/fc.php?tID=2&d=0&f=2023538075&l=MON&rn=16
…	4.851458	172.23.133.174	180.222.102.158	HTTP	299	POST /p?s=2023538075&t=NNnjWui33z45T0mv,0.276391910965359
…	4.851740	172.23.133.174	180.222.102.158	HTTP	292	POST /p?s=2023538075&t=t2Gh8plJToY7Rc4Q,0.145864410714454
…	4.913655	180.222.102.158	172.23.133.174	HTTP	808	HTTP/1.1 200 OK (GIF89a)
…	4.915833	180.222.102.158	172.23.133.174	HTTP	808	HTTP/1.1 200 OK (GIF89a)
…	5.093994	180.222.102.201	172.23.133.174	HTTP	168	HTTP/1.1 200 OK (text/html)
…	5.114021	172.23.133.174	180.222.102.158	HTTP	293	POST /p?s=2023538075&t=mSU8ddXKECJ0oRtR,0.578281165718429
…	5.120993	172.23.133.174	180.222.102.158	HTTP	284	POST /p?s=2023538075&t=PEihQpozTz221IbQ,0.745714460510599
…	5.131241	180.222.102.158	172.23.133.174	HTTP	808	HTTP/1.1 200 OK (GIF89a)
…	5.135141	180.222.102.158	172.23.133.174	HTTP	808	HTTP/1.1 200 OK (GIF89a)
…	5.258583	172.23.133.174	104.254.149.68	HTTP	603	POST /vevent?an_audit=0&referrer=https%3A%2F%2Fus.yahoo.c
…	5.593961	180.222.102.201	172.23.133.174	HTTP	810	HTTP/1.1 200 OK (text/html)
…	5.663040	172.23.133.174	69.147.88.7	HTTP	785	GET /p?t=0.9057407623512466&_V=V&type=vod%20short&ss=vod&
…	5.664167	172.23.133.174	69.147.88.7	HTTP	619	GET /p?t=0.42872753225809523&_V=V&type=streamurl&ss=vod&v
…	5.755027	172.23.133.174	69.147.80.12	HTTP	619	GET /nn/lib/metro/g/myy/video_styles_0.0.72.css HTTP/1.1
…	5.755292	172.23.133.174	69.147.80.12	HTTP	611	GET /nn/lib/metro/g/myy/grid_0.0.36.css HTTP/1.1
…	5.755799	172.23.133.174	69.147.80.12	HTTP	621	GET /nn/lib/metro/g/myy/font_yahoosans_0.0.45.css HTTP/1.

Scenario 2 – Layer 3 Transparent Proxy

In this scenario, FortiADC becomes a routed hop between client and gateway.

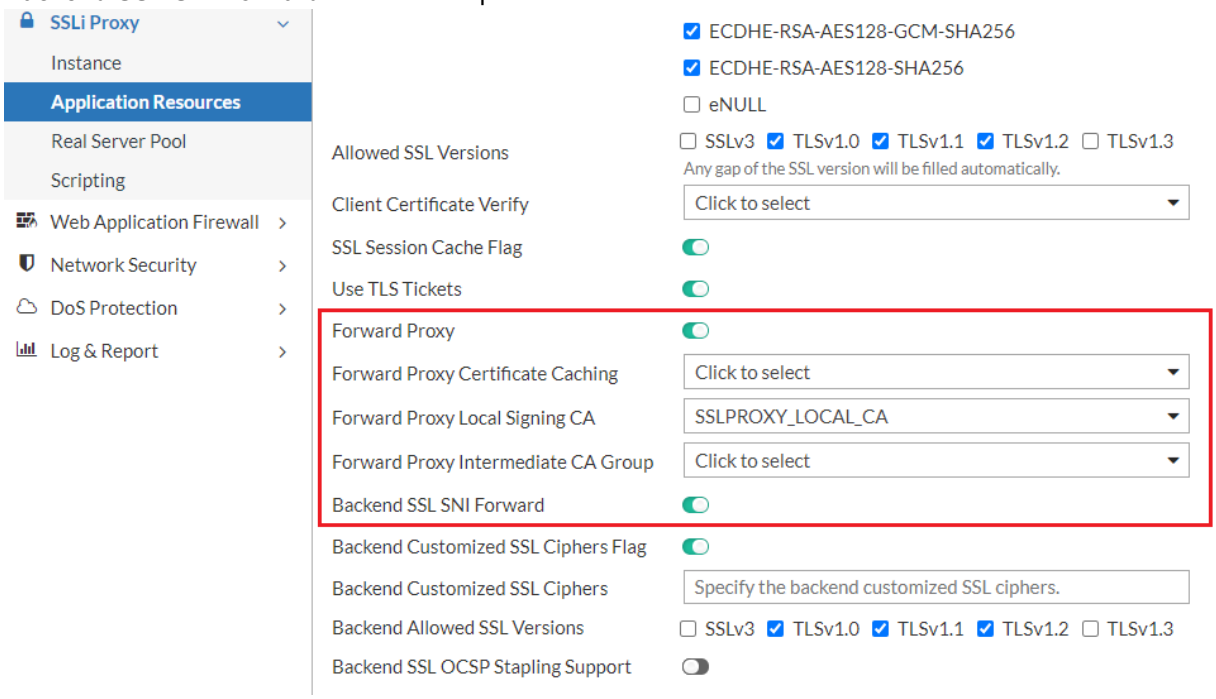
Topology



Creating Client SSL Profile for SSLi instance

1. Go to SSLi Proxy > Application Resources, then click the tab Client SSL.
2. Click Create New > Advanced Mode to display the configuration editor.

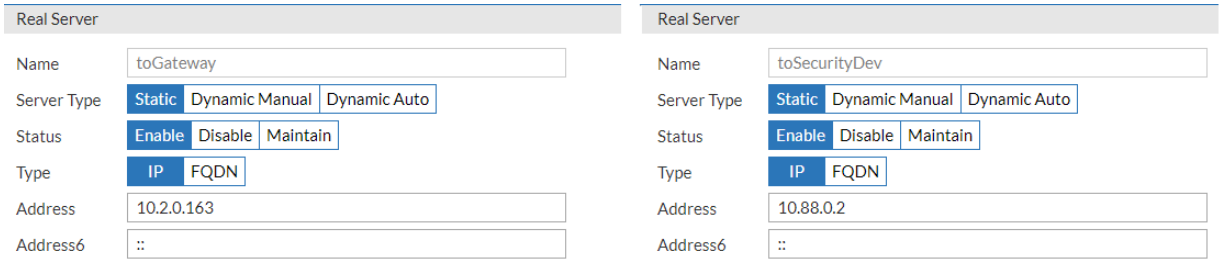
3. Complete the key configuration as shown in the screenshot.
   - **Name:** Enter a unique name for the SSLi instance name.
   - **Forward Proxy:** Enable this option.
   - **Forward Proxy Local Signing CA:** Select a CA certificate that your client trusts it.
   - **Backend SSL SNI Forward:** Enable this option.



4. Save the configuration.

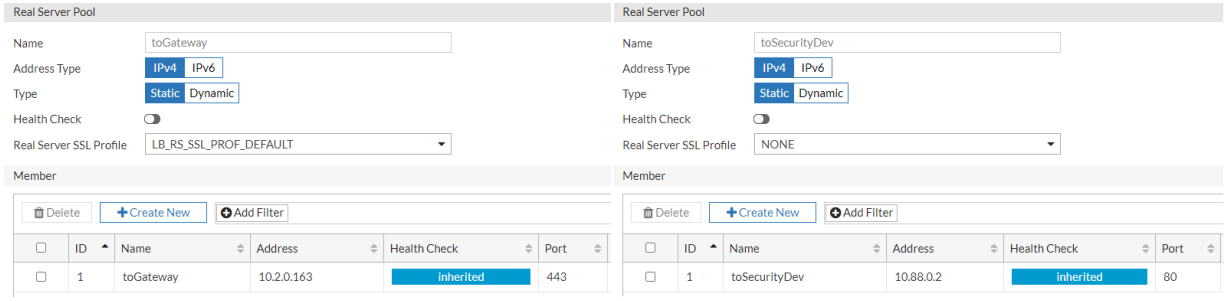
Creating Real Server Profile for SSLi instance

1. Go to SSLi Proxy > Real Server Pool then click the tab Real Server.
2. Click Create New to display the configuration editor. Here we need to add two real servers, one connecting with the gateway, and the other connecting with the security device.
3. Complete the key configuration as shown in the screenshot.
   - **Name:** Enter a unique name for the Real Server name
   - **Address:** Enter the correct IP address.



4. Save the configuration.
5. Go to SSLi Proxy > Real Server Pool, then click the tab Real Server Pool. Here we need to create two real server pools containing the above two real servers respectively.
6. Click Create New to display the configuration editor.

7. Complete the key configuration as shown in the screenshot.
   - **Name:** Enter a unique name for the Real Server Pool.
   - **Real Server SSL Profile:** Enable SSL on the real server to the gateway side, and disable SSL on the one to the security device side.
   - **Member:** Select the correct real server in your topology.

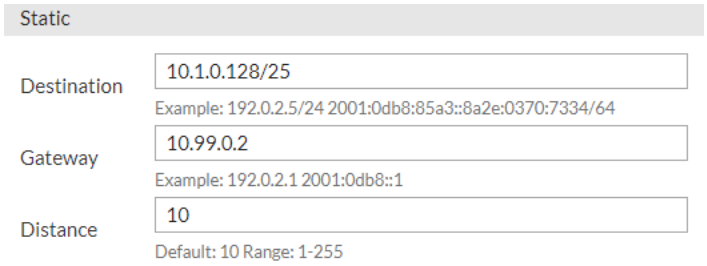


8. Save the configuration.

Configuring Static Routing

1. Go to Network > Routing, then click the tab Static.
2. Click Create New to display the configuration editor.
3. Complete the key configuration as shown in the screenshot.
   - **Destination:** Enter a Client IP address scope.
   - **Gateway:** Enter a Security Device IP address which in the Re-encryption side.
4. Save the configuration.

This static routing forwards the packets whose destination is the client IP to the security device.

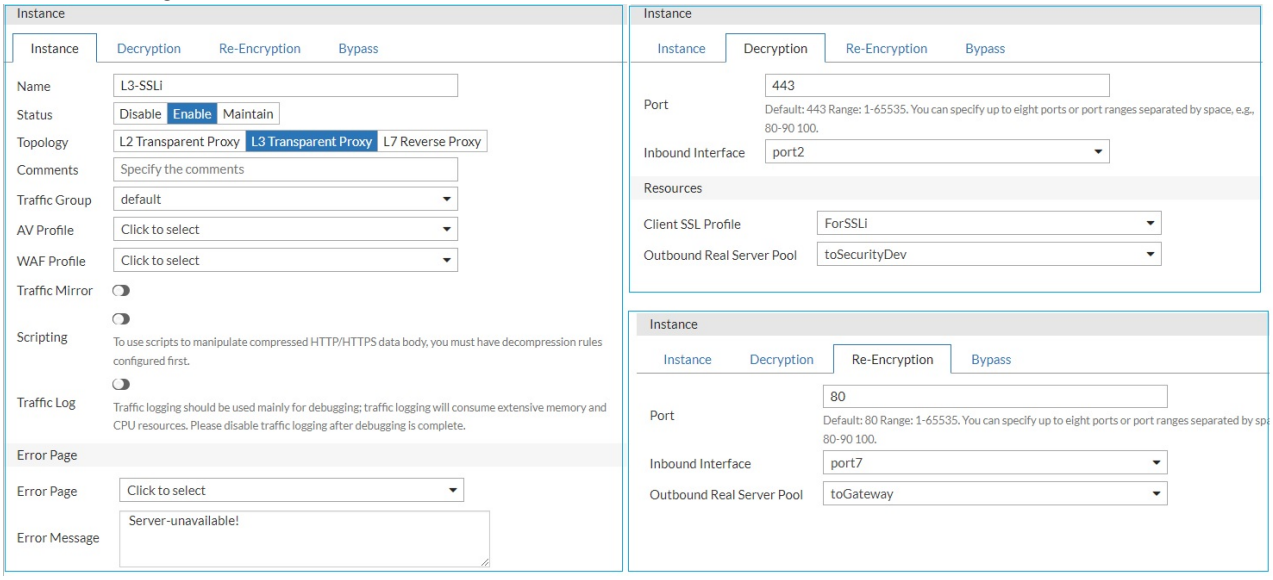


Creating SSLi instance for L3 deploy

1. Go to SSLi Proxy > Instance, then click the tab Instance.
2. Click Create New > Advanced Mode to display the configuration editor.
3. Complete the key configuration as shown in the screenshot.
   - **Name:** Enter a unique name for the SSLi instance.
   - **Topology:** Select the L3 Transparent Proxy.
   - Decryption tab
     - **Inbound Interface:** Selected an interface connected to the client side.
     - **Client SSL Profile:** Select the client SSL profile you just created.
     - **Outbound Real Server Pool:** Select the server pool to the security device.
   - Re-encryption tab
     - **Inbound Interface:** Select an interface connected to the security device side.
     - **Outbound Real Server Pool:** Select the server pool to the gateway side.

If you have configured both L7 and L2/L3 instances for the same security device (attached to the same subnets), their port numbers must not be the same. We will remove this restriction in later releases.

4. Save the configuration.



Enabling rt-cache-strict

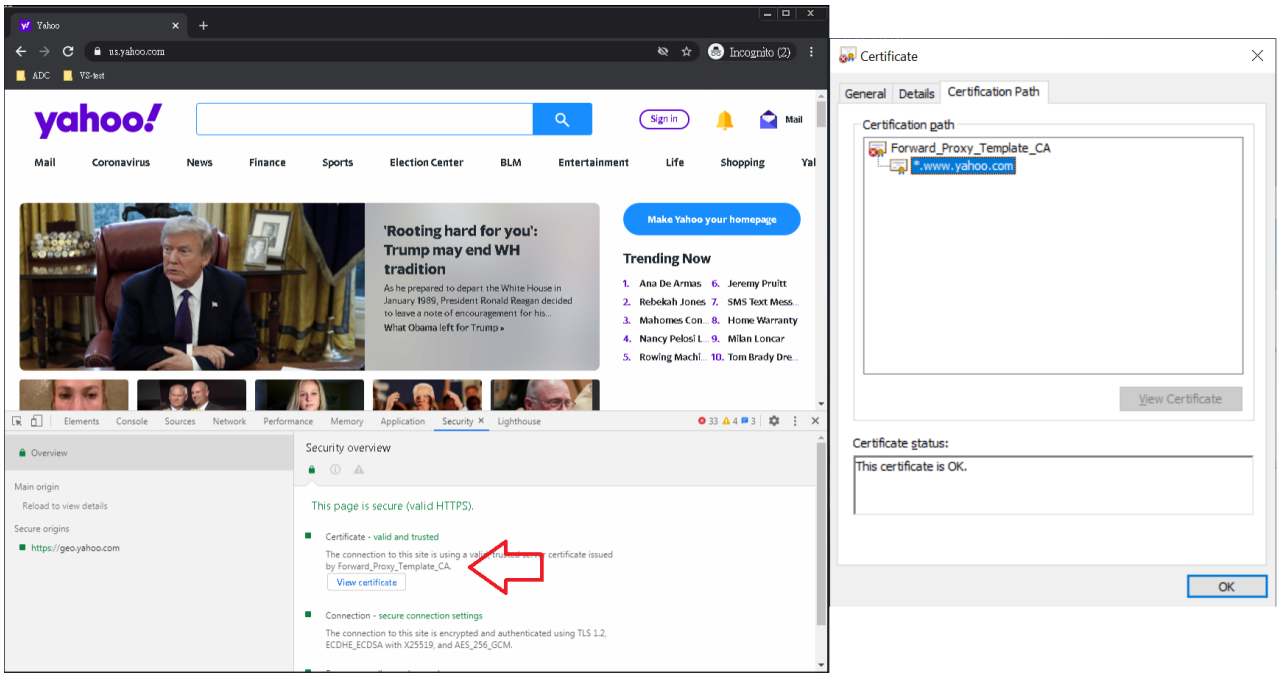
Run the following command:

```
config router setting
   set rt-cache-strict enable
      config rt-cache-reverse-exception
   end
end
```

Client side: install CA and try the SSLi function

1. Install the Local Signing CA that FortiADC selected.
2. Configure the ADC's Port2 as default gateway.
3. Open the browser and navigate to https://us.yahoo.com, you will see the derived certificate is signed by "Local

Signing CA".



Testing SSLi deployment

To test the deployment, check if the plain HTTP traffic is logged on the security device.

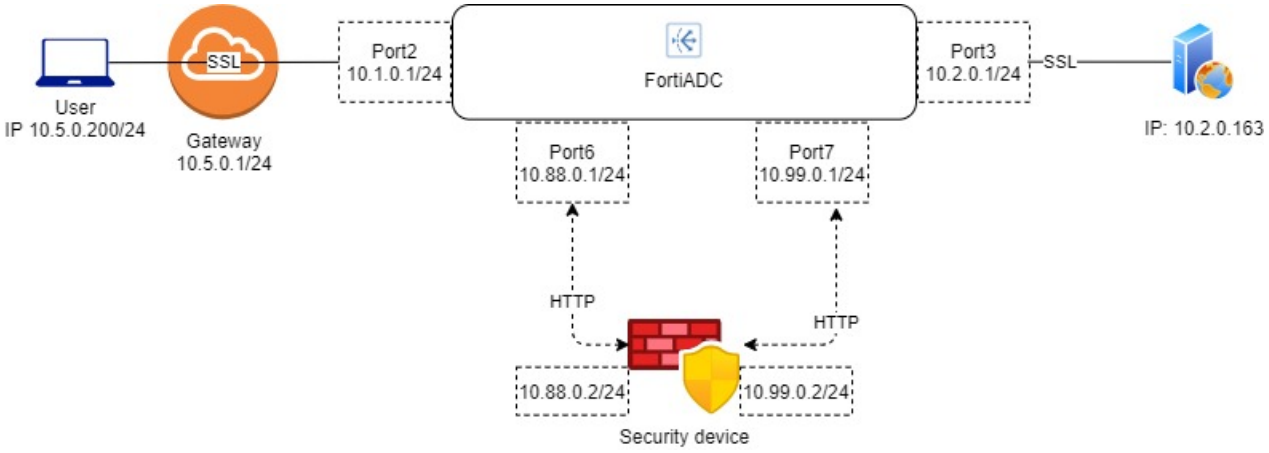
No.	Time	Source	Destination	Protocol	Length	Info
…	6.268216	10.1.0.199	180.222.102.158	HTTP	1773	POST /p?s=2023538075&t=NYooZeHqWJCHOpRr,0.660851121048905
…	6.995122	180.222.102.158	10.1.0.199	HTTP	808	HTTP/1.1 200 OK (GIF89a)
…	7.468141	10.1.0.199	180.222.102.158	HTTP	1767	POST /p?s=2023538075&t=oafy5MLEhzj4R4MG,0.509183716340872
…	7.478694	180.222.102.158	10.1.0.199	HTTP	808	HTTP/1.1 200 OK (GIF89a)
…	7.484775	10.1.0.199	180.222.102.158	HTTP	1761	POST /p?s=2023538075&t=gPkt17gK21kYwFWX,0.127257602591019
…	7.493523	180.222.102.158	10.1.0.199	HTTP	808	HTTP/1.1 200 OK (GIF89a)
…	7.642548	10.1.0.199	180.222.102.202	HTTP	1365	GET / HTTP/1.1
…	7.861377	10.1.0.199	180.222.102.158	HTTP	1762	POST /p?s=2023538075&t=7ruqGcjgUwzhHLsS,0.719540259421653
…	7.868193	10.1.0.199	180.222.102.158	HTTP	1753	POST /p?s=2023538075&t=CcUcYhCuZopJsnWe,0.661113088690134
…	7.871132	180.222.102.158	10.1.0.199	HTTP	808	HTTP/1.1 200 OK (GIF89a)
…	7.900644	180.222.102.158	10.1.0.199	HTTP	808	HTTP/1.1 200 OK (GIF89a)
…	8.057187	10.1.0.199	119.161.16.12	HTTP	611	GET /nn/lib/metro/g/myy/grid_0.0.36.css HTTP/1.1
…	8.081184	10.1.0.199	119.161.16.12	HTTP	619	GET /nn/lib/metro/g/myy/video_styles_0.0.72.css HTTP/1.1
…	8.081459	10.1.0.199	119.161.16.12	HTTP	621	GET /nn/lib/metro/g/myy/font_yahoosans_0.0.45.css HTTP/1.
…	8.081490	10.1.0.199	119.161.16.12	HTTP	615	GET /nn/lib/metro/g/sda/sda_flex_0.0.42.css HTTP/1.1
…	8.081756	10.1.0.199	119.161.16.12	HTTP	619	GET /nn/lib/metro/g/myy/wafertooltip_0.0.15.css HTTP/1.1
…	8.081976	10.1.0.199	119.161.16.12	HTTP	606	GET /os/yc/css/bundle.c60a6d54.css HTTP/1.1
…	8.127449	119.161.16.12	10.1.0.199	HTTP	971	HTTP/1.1 200 OK (text/css)
…	8.129952	10.1.0.199	119.161.16.12	HTTP	671	GET /aaq/fp/css/tdv2-applet-native-ads.PencilAd.atomic.lt
…	8.139815	119.161.16.12	10.1.0.199	HTTP	1393	HTTP/1.1 200 OK (text/css)

Scenario 3 – Layer 7 Reverse Proxy

In this scenario, FortiADC becomes a proxy server for the client, and the security device must be a real server.

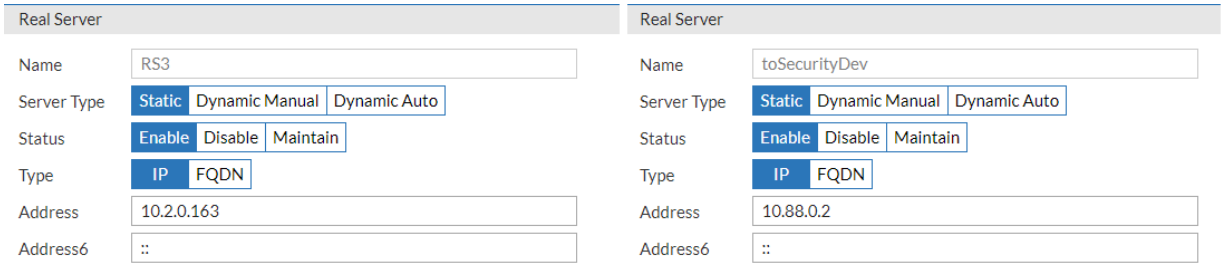
As shown in the following graphic, when traffic comes out of FortiADC from port6, its source IP will be 10.88.0.1, and destination IP 10.88.0.2. For the traffic coming out from port3, its source IP will be 10.2.0.1, and destination IP 10.2.0.163.

Topology



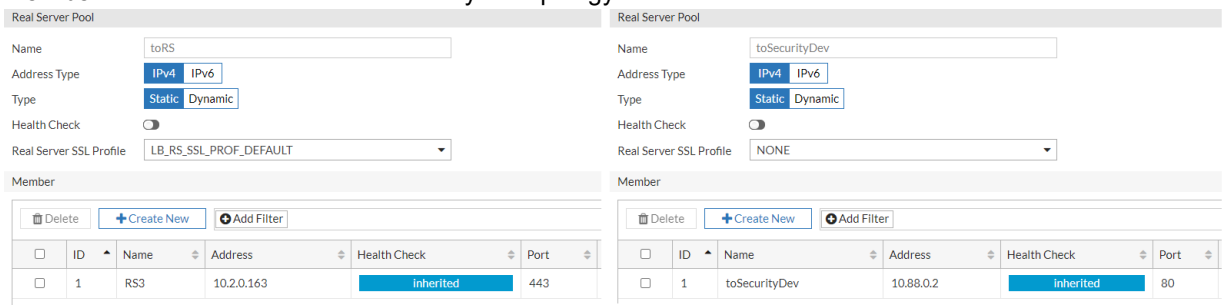
Creating Real Server Profile for SSLi instance

1. Go to SSLi Proxy > Real Server Pool then click the tab Real Server.
2. Click Create New to display the configuration editor. Here we need to add two real servers, one connecting with the gateway, and the other connecting with the security device.
3. Complete the key configuration as shown in the screenshot.
   - **Name:** Enter a unique name for the Real Server name.
   - **Address:** Enter the correct IP address.



4. Save the configuration.
5. Go to SSLi Proxy > Real Server Pool, then click the tab Real Server Pool. Here we need to create two real server pools containing the above two real servers respectively.
6. Click Create New to display the configuration editor.
7. Complete the key configuration as shown in the screenshot.
   - **Name:** Enter a unique name for the Real Server Pool.
   - **Real Server SSL Profile:** Enable SSL on the real server to the gateway side, and disable SSL on the one to the security device side.

- **Member:** Select the correct real server in your topology.



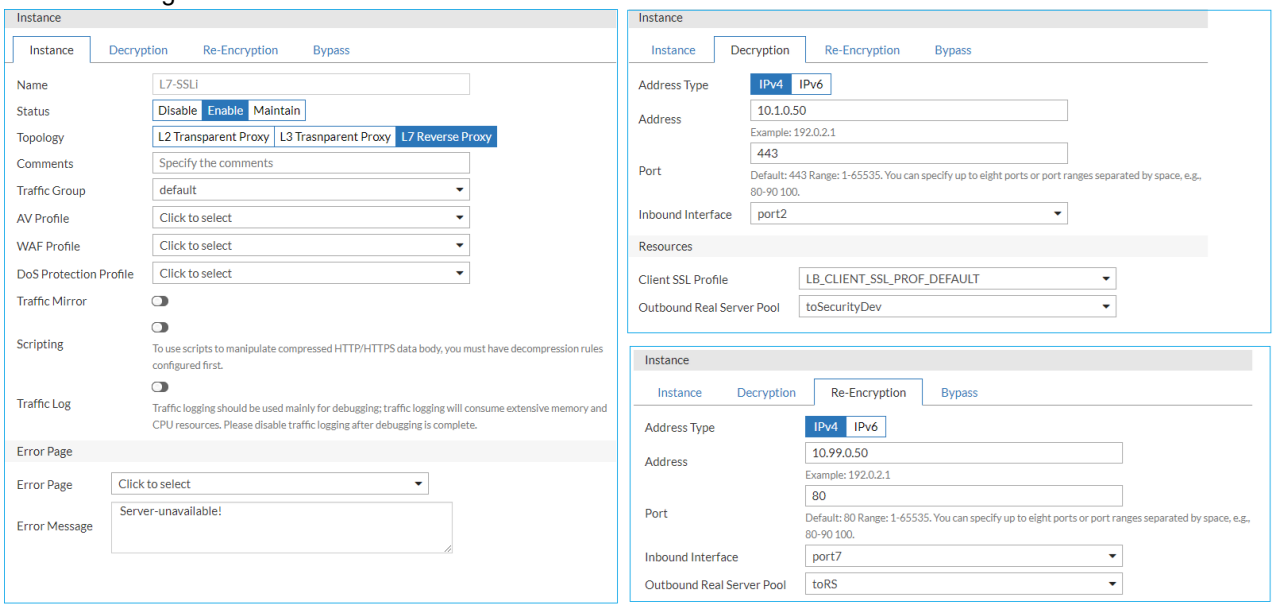
8. Save the configuration.

Creating SSLi instance for L7 deploy

1. Go to SSLi Proxy > Instance, then click the tab Instance.
2. Click Create New > Advanced Mode to display the configuration editor.
3. Complete the key configuration as shown in the screenshot.
   - **Name:** Enter a unique name for the SSLi instance.
   - **Topology:** Select the L7 Transparent Proxy.
   - Decryption tab
     - **Address:** Specify the IP address for the client to access.
     - **Port**: Enter the port (number) for the client to access.
     - **Inbound Interface:** Select an interface connected to Internet side.
     - **Outbound Real Server Pool:** Select the server pool to the security device.
   - Re-encryption tab
     - **Address:** Specify the IP address for FortiADC to listen to traffic from the security device.
     - **Port**: Enter the listening port (number).
     - **Inbound Interface:** Select an interface connected to the security device side.
     - **Outbound Real Server Pool:** Select the server pool to the gateway side.

     If you have configured both L7 and L2/L3 instances for the same security device (attached to the same subnets), their port numbers must not be the same. We will remove this restriction in later releases.

4. Save the configuration.



Client side: install CA and try the SSLi function

Open the browser and navigate to https://10.1.0.50 (the address you configured in SSLi Instance > Decryption tab for the client to access), you will see the derived certificate is signed by Local Certificate (Factory).

Testing SSLi deployment

To test the deployment, check if the plain HTTP traffic is logged on the security device.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000304	10.88.0.1	10.88.0.2	HTTP	742	GET / HTTP/1.1
4	0.005261	10.88.0.2	10.88.0.1	HTTP	1315	HTTP/1.1 200 OK (text/html)

Troubleshooting

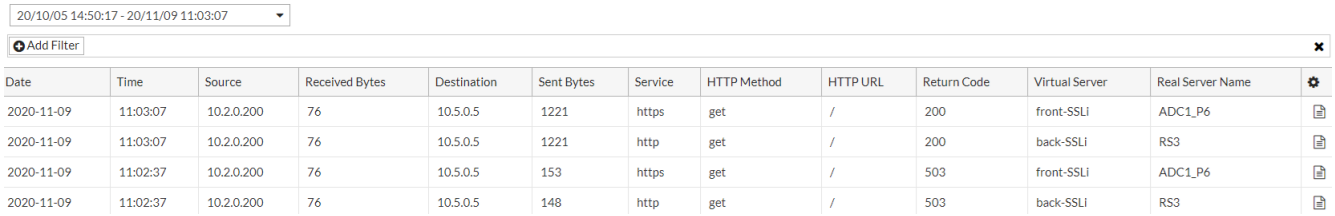
If there is any problem with SSLi Proxy, you can use the console to print out the diagnose debug message or enable traffic log to see what's going on.

To set the diagnose debug print out level in the console:

1. Connect your management computer to the FortiADC.
2. Enable the diagnose debug output for httproxy and ssl-of-httproxy.
   ```
   diagnose debug module httproxy all
   diagnose debug module ssl-of-httproxy all
   diagnose debug enable
   ```
   You will see the SSLi related information printed.

To check the traffic log:

Go to Log & Report > Log Access > Traffic Logs to display the traffic log.


20/10/05 14:50:17 - 20/11/09 11:03:07

Add Filter

Date	Time	Source	Received Bytes	Destination	Sent Bytes	Service	HTTP Method	HTTP URL	Return Code	Virtual Server	Real Server Name
2020-11-09	11:03:07	10.2.0.200	76	10.5.0.5	1221	https	get	/	200	front-SSLi	ADC1_P6
2020-11-09	11:03:07	10.2.0.200	76	10.5.0.5	1221	http	get	/	200	back-SSLi	RS3
2020-11-09	11:02:37	10.2.0.200	76	10.5.0.5	153	https	get	/	503	front-SSLi	ADC1_P6
2020-11-09	11:02:37	10.2.0.200	76	10.5.0.5	148	http	get	/	503	back-SSLi	RS3