Security Web Filter for F5
Installation Guide

Contributors

Content architect:	Rui Maximo
Writers:	Fabian Kunz, Rui Maximo
Editor:	Kelly Fuller Blue
Published:	Feb 15, 2020

Security-Filters.com/Lync-Solutions.com operates under the legal entity "MB Corporation", and is incorporated in the State of Washington.

MB Corporation, by publishing this document, does not guarantee that any information contained herein is and will remain accurate or that use of the information will ensure correct and faultless operation of the relevant service or equipment. MB Corporation, its agents and employees shall not be held liable to or through any user for any loss or damage whatsoever results from relying on the information contained herein.

Nothing in this document is intended to and does not alter the legal obligations, responsibilities, or relationship between you and MB Corporation as set out in the contract existing between you and MB Corporation. MB Corporation will not be liable for any compliance or technical information provided herein.

This document is provided "as-is." The information and views expressed in this document, including URL and other Internet website references, may change without notice.

Information in the examples in this document is fictitious and is only for illustration. No actual association or connection is in any way intended or should be inferred.

Table of contents

1 Security Web Filter

The Security Web Filter is a security solution to protect Skype for Business Server and Exchange from external attacks targeting the HTTPS traffic through the reverse proxy. The enterprise ready Security Filters suite of products is designed for customers who have multiple instances of reverse proxies deployed (used to publish Skype for Business and Exchange Web URLs), and who want to centralize the lockout count across all instances of Security Edge Filter and Security Web Filter or want to block unauthorized Skype for Business Mobile devices. The Security Web Filter for F5 is installed on a separate server that is configured as a member of the virtual ICAP server on the BIG-IP that publishes Skype for Business Server's External Web Services.

2 Security Concern

When customers expose their Skype for Business Server (formerly Lync Server) infrastructure to the Internet by publishing their Skype for Business Web URLs (that is, dial-in, meeting, ABS (Address Book Service), and so on) through their reverse proxy, they expose both their Skype for Business Server environment and their internal corporate network to external attacks. This puts their users and Skype for Business Servers potentially at risk from Denial of Service (DoS), Distributed Denial of Service (DDoS), and brute-force password attacks as shown in Figure 2 1.

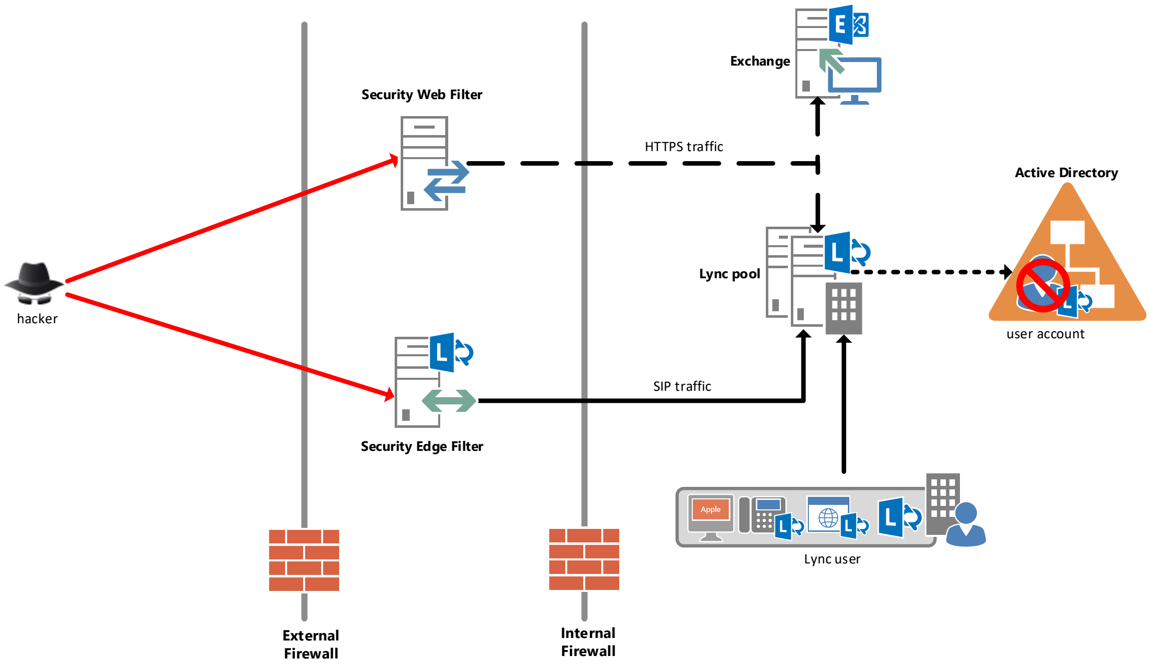


Figure 2.1 Users and Skype for Business Servers that are potentially at risk

3 Solution

The Active Edge Protection solution protects against Active Directory Directory Services account lockout attacks by scanning all incoming unauthenticated traffic. It scans all incoming SIP traffic going through the Edge Server and HTTPS traffic going through the reverse proxy. This solution's architecture consists of the following components:

- Security Edge Filter
- Security Web Filter
- Security Filter Manager

Here's how it all works:

- The Security Web Filter is designed to track denied authentication attempts and block further login attempts before the Active Directory Directory Services lockout limit is reached.
- The lockout gives you one more tier of account security, safely locking the account out of the extranet.
- Security Filters prevent password-guessing on the extranet by blocking authentication attempts for that account after the number of failed authentication attempts reaches a threshold.
- Even when an Active Directory user account is locked out at the network perimeter by the Security Filters, the employee can still log in to their Active Directory account from within the corporate network or through a VPN. The DoS risk is substantially mitigated, without much inconvenience.
- When the Security Filters are configured to block Windows NT LAN Manager (NTLM) authentication and enforce the whitelist, remote users must sign in to Skype for Business Server from a domain-joined computer without preventing Skype for Business Mobile clients from signing in.
- The Security Web Filter filters access to Exchange Web Services, and can block non-Skype for Business clients from connecting to Exchange based on client type.
- The Security Web Filter protects against cross-site scripting (XSS) and SOAP based attacks.

The Security Web Filter track the number of failed login attempts from remote users. When the number of failed login attempts exceeds the administrator's specified threshold, the Security Filters block all further login attempts until the lockout period expires or the administrator unlocks the account. The Security Filter Manager centralizes the number of failed login attempts, configuration settings, and logging information across all instances of the Security Edge Filters and Security Web Filters, and provides an administrative web interface that visualizes metrics captured by the Security Filters.

Figure 3.1 illustrates the architecture of the Active Edge Protection solution.

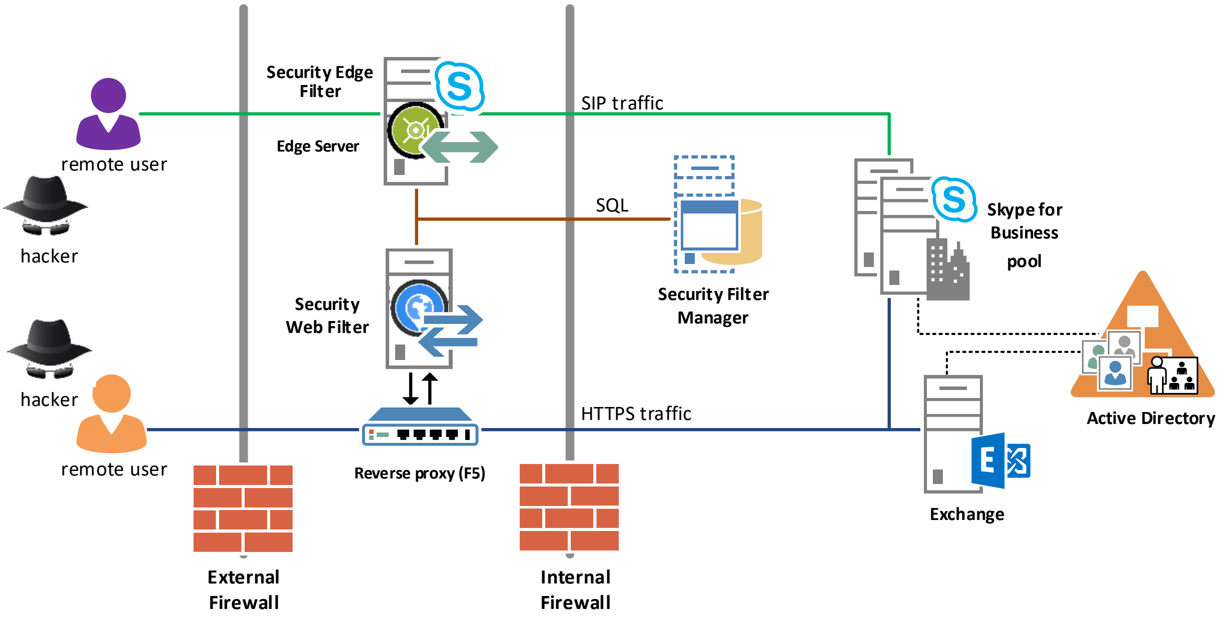


Figure 3.1 Active Edge Protection architecture

4 Security Web Filter

After the Security Filter Manager is installed and configured, you can install the Security Web Filter. The Security Web Filter protects the HTTPS traffic to your Skype for Business web services.

The Security Web Filter is installed as a service on Windows Server 2012 R2 64-bit or later with .Net Framework 4.5 installed. The Security Web Filter server should not be joined to Active Directory. The Windows Firewall on the Security Web Filter server must allow TCP traffic on port 1344. The Security Filter Manager can be collocated with the Security Web Filter (see Security Filter Manager Installation Guide for requirements).

Hardware (physical or virtual) requirements:

Hardware component	Recommended
CPU	64-bit dual processor, quad-core, 2.26 gigahertz (GHz) or higher.
Memory	16 gigabytes.
Disk	1 drive (200 GB or more) 10,000 rpm or higher speed
Network	1 dual-port network adapter, 1 Gbps or higher.

The Security Web Filter monitors and filters all login attempts from the following sources:

- Skype for Business desktop clients
- Mobile clients (iPhone, iPad, Android, Windows Phone)
- Dial-in URL
- Meet URL
- Skype for Business Web App
- Hacker tool (DoS Attack available on from Lync-Solutions (http://lync-solutions.com)

4.1 Install Security Web Filter

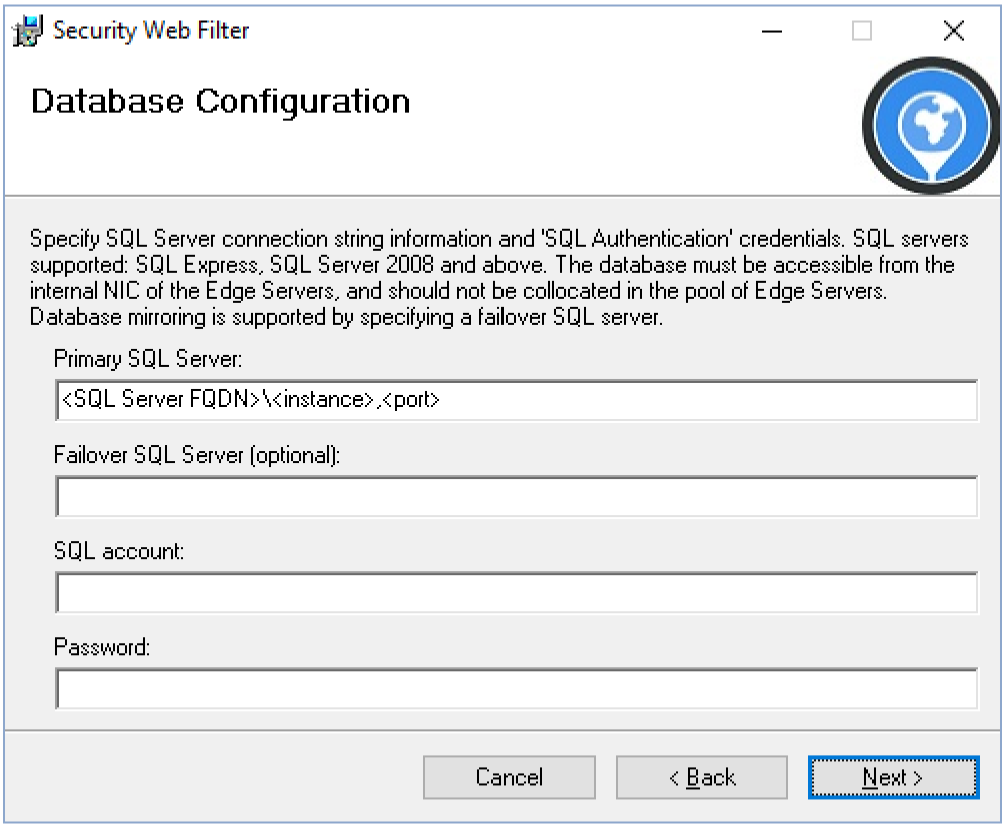
Before installing the Security Web Filter, you must install and configure the Security Filter Manager. Please refer to the Security Filter Manager Installation Guide for details on how to install.

If you plan to control access to only registered mobile device, then you'll need to install and configure the Security Authorization Filter. Once you've configured the Security Authorization Filter by running the PowerShell script, configure.ps1, provide the application endpoint SIP address to MB Corporation so that a version of the Security Web Filter tied to this SIP address is generated for you.

Here are the installation steps for setting up the Security Web Filter:

1. After you have downloaded the Security Web Filter file (that contains SecurityWebFilterSetup.msi and setup.exe), run the setup.exe with local administrator privileges.
2. The Security Web Filter Setup Wizard opens. Click **Next**.
3. On the **License Agreement** page, click **I Agree**, and then click **Next**.
4. On the **Database Configuration** page (see Figure 4.1.1), specify the SQL Server connection string information and the SQL Authentication credentials to connect to the

SecurityFilterManager database.



Database Configuration

Specify SQL Server connection string information and 'SQL Authentication' credentials. SQL servers supported: SQL Express, SQL Server 2008 and above. The database must be accessible from the internal NIC of the Edge Servers, and should not be collocated in the pool of Edge Servers. Database mirroring is supported by specifying a failover SQL server.

Primary SQL Server: <SQL Server FQDN>\<instance>,<port>

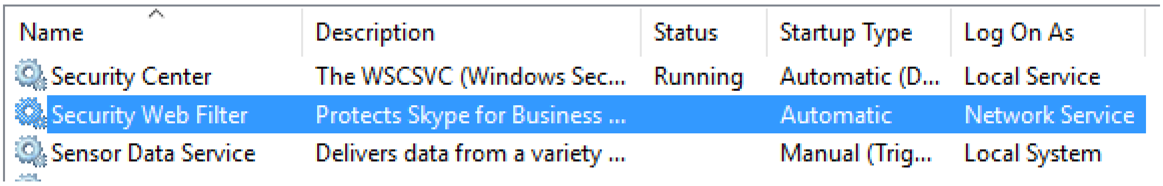
Failover SQL Server (optional):

SQL account:

Password:

Figure 4.1.1 SQL Server connection string and SQL Authentication credentials

7. Click **Next**.
8. Configure the Windows Firewall and any other firewall to allow the BIG-IP to connect to the Security Web Filter over TCP port 1433.
9. Click **Next**.
10. On the **Confirm Installation** page, click **Next** and then **Close** to complete the installation.
11. Open the **Services** console.
12. Search for the **Security Web Filter** service (Figure 4.1.2).



Name	Description	Status	Startup Type	Log On As
Security Center	The WSCSVC (Windows Sec...	Running	Automatic (D...	Local Service
Security Web Filter	Protects Skype for Business ...		Automatic	Network Service
Sensor Data Service	Delivers data from a variety ...		Manual (Trig...	Local System

Figure 4.1.2 Security Web Filter service

13. Start the **Security Web Filter** service.

4.2 Monitor Security Web Filter

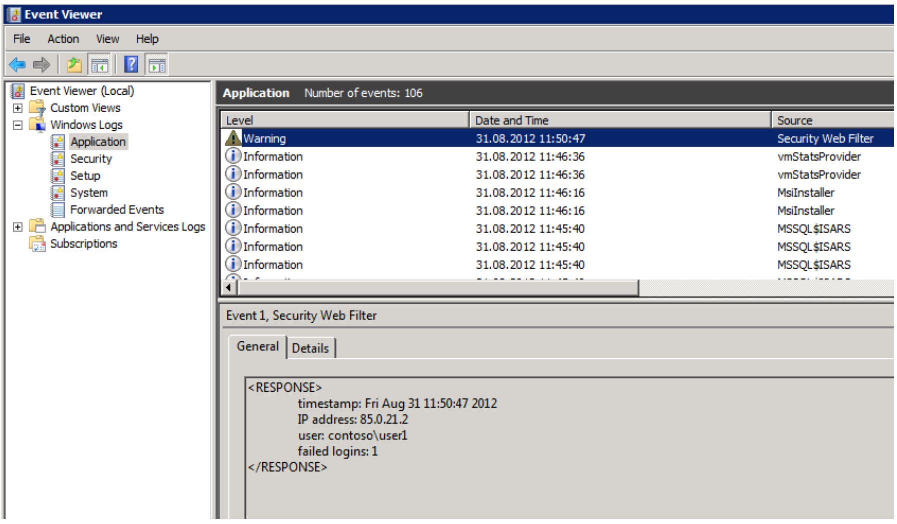
The Security Web Filter does not store any configuration or data locally. Therefore, there is no need to backup the Security Web Filter service. Any events are logged to the Application Event log, and can be viewed in the Event Viewer. When restoring the server, the Security Web Filter can be reinstalled or the VM restored to the last snapshot.

The BIG-IP LTM can be configured to probe the health of the Security Web Filter by defining a Health Monitor in step 5 in section 5.1.2. This allows the BIG-IP LTM to stop routing traffic to an unresponsive Security Web Filter server.

4.3 Security Web Filter in Action

The Security Web Filter logs all bad login attempts and service interactions in the Application Windows Logs. The following screenshots show possible event log entries.

The Event Viewer shows the first bad login attempt as shown in Figure 4.3.1

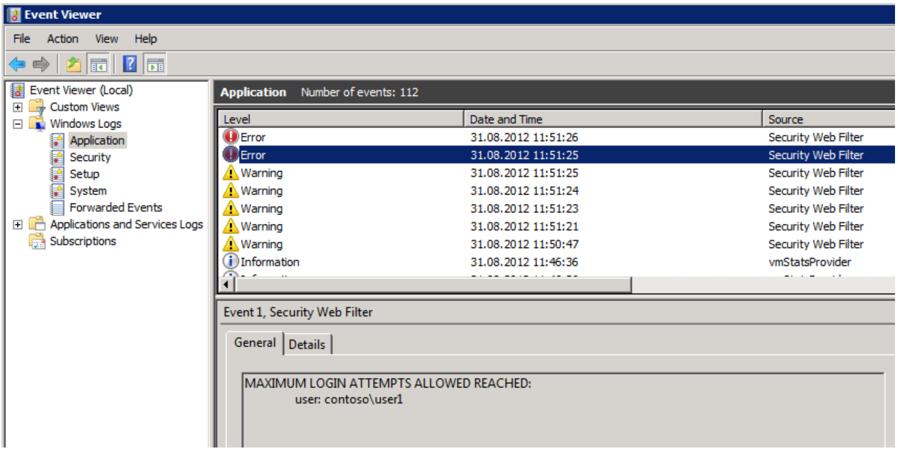


Level	Date and Time	Source
Warning	31.08.2012 11:50:47	Security Web Filter
Information	31.08.2012 11:46:36	vmStatsProvider
Information	31.08.2012 11:46:36	vmStatsProvider
Information	31.08.2012 11:46:16	MsiInstaller
Information	31.08.2012 11:46:16	MsiInstaller
Information	31.08.2012 11:45:40	MSSQL$ISARS
Information	31.08.2012 11:45:40	MSSQL$ISARS
Information	31.08.2012 11:45:40	MSSQL$ISARS

```
<RESPONSE>
        timestamp: Fri Aug 31 11:50:47 2012
        IP address: 85.0.21.2
        user: contoso\user1
        failed logins: 1
</RESPONSE>
```

Figure 4.3.1 First bad login attempt shown in Event Viewer

When the maximum bad login attempt is reached, account lockout is enforced as shown in Figure 4.3.2.

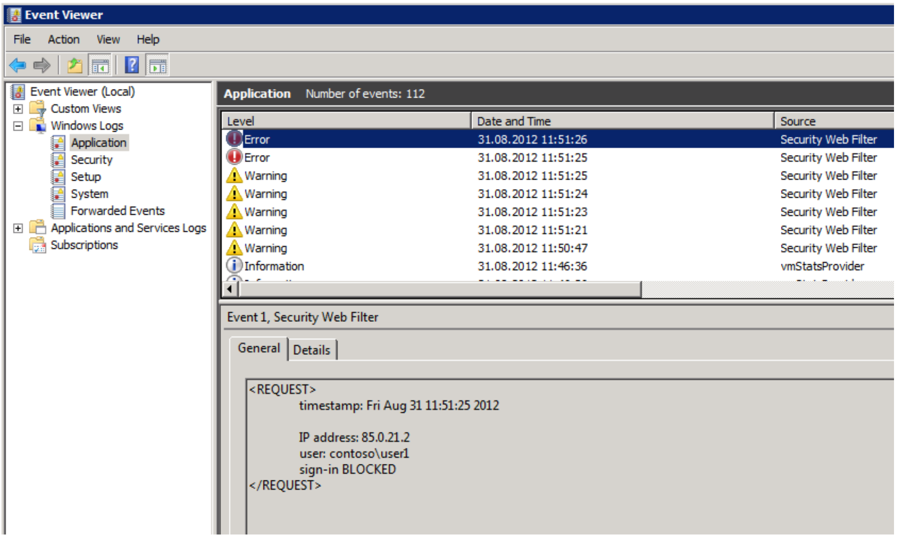


Level	Date and Time	Source
Error	31.08.2012 11:51:26	Security Web Filter
Error	31.08.2012 11:51:25	Security Web Filter
Warning	31.08.2012 11:51:25	Security Web Filter
Warning	31.08.2012 11:51:24	Security Web Filter
Warning	31.08.2012 11:51:23	Security Web Filter
Warning	31.08.2012 11:51:21	Security Web Filter
Warning	31.08.2012 11:50:47	Security Web Filter
Information	31.08.2012 11:46:36	vmStatsProvider

```
MAXIMUM LOGIN ATTEMPTS ALLOWED REACHED:
        user: contoso\user1
```

Figure 4.3.2 Lockout enforced after maximum bad login attempts shown in Event Viewer

Figure 4.3.3 illustrates account lockout still enforced for an already blocked user.



Application Number of events: 112

Level	Date and Time	Source
Error	31.08.2012 11:51:26	Security Web Filter
Error	31.08.2012 11:51:25	Security Web Filter
Warning	31.08.2012 11:51:25	Security Web Filter
Warning	31.08.2012 11:51:24	Security Web Filter
Warning	31.08.2012 11:51:23	Security Web Filter
Warning	31.08.2012 11:51:21	Security Web Filter
Warning	31.08.2012 11:50:47	Security Web Filter
Information	31.08.2012 11:46:36	vmStatsProvider

Event 1, Security Web Filter

```
<REQUEST>
        timestamp: Fri Aug 31 11:51:25 2012

        IP address: 85.0.21.2
        user: contoso\user1
        sign-in BLOCKED
</REQUEST>
```

Figure 4.3.3 Event Viewer showing already blocked user

By default the Security Web Filter only logs failed logins. To view successful logins as well, configure the Security Edge Filter for verbose logging. This requires modifying the configuration file. Locate the config file %programFiles%\MB\Security Web Filter\SecurityWebFilter.exe.config

Open the config file using Notepad or your preferred text editor. Modify the value, "normal", to "verbose" for the key, "logLevel".

```
<add key="logLevel" value="verbose" />
```

4.4 Troubleshooting

Before opening a case, please reproduce your issue with verbose logging enabled. This will provide additional information not available in the Application Event Viewer.

Use the DebugView tool to capture this verbose logging. You can download this free tool from Windows Sysinternals (http://technet.microsoft.com/en-us/sysinternals/bb896647.aspx).

1. Start Dbgview.exe using administrative privileges, and check the **Capture Global Win32** option as shown in Figure 4.4.1.

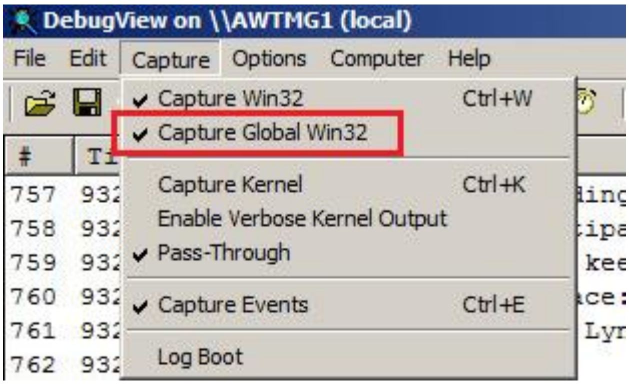
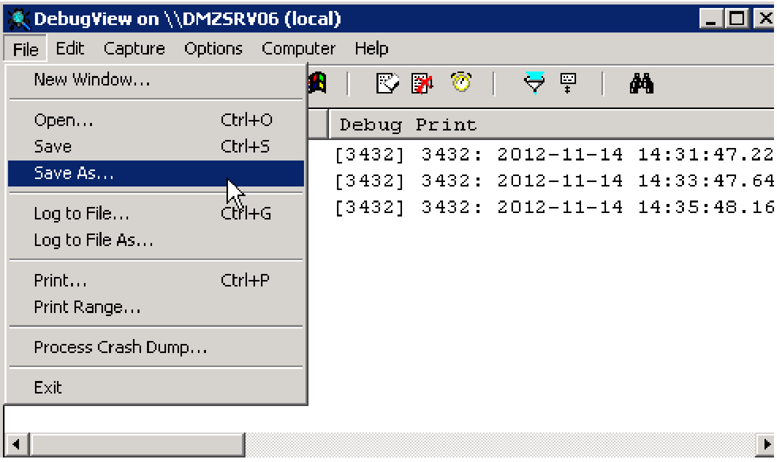


Figure 4.4.1 Options to select for DbgView

2. As soon as you have reproduced the issue, save the output to a text file as shown in Figure 4.4.2.



```
Debug Print
[3432] 3432: 2012-11-14 14:31:47.22
[3432] 3432: 2012-11-14 14:33:47.64
[3432] 3432: 2012-11-14 14:35:48.16
```

Figure 4.4.2 Debug output

5 F5 BIG-IP

It is assumed that you have already configured your F5 BIG-IP LTM as a reverse proxy for Skype for Business (and Exchange) traffic. Configuration of the BIG-IP LTM as a reverse proxy for Skype for Business traffic is out of scope in this document. Please refer to the F5 documentation.

The Security Web Filter acts as an ICAP server and the BIG-IP LTM acts as an ICAP client. BIG-IP LTM version 11.5 and above is supported. The BIG-IP must be configured to forward client requests to the Security Web Filter for inspection. When a Skype for Business server or Exchange servers responds, the outgoing response is forwarded to the Security Web Filter for inspection. This allows the Security Web Filter to inspect, modify and block HTTPS traffic in both directions. The Security Web Filter and BIG-IP LTM communicate using the ICAP protocol over TCP on port 1344. This configuration is illustrated in Figure 4.2.1.

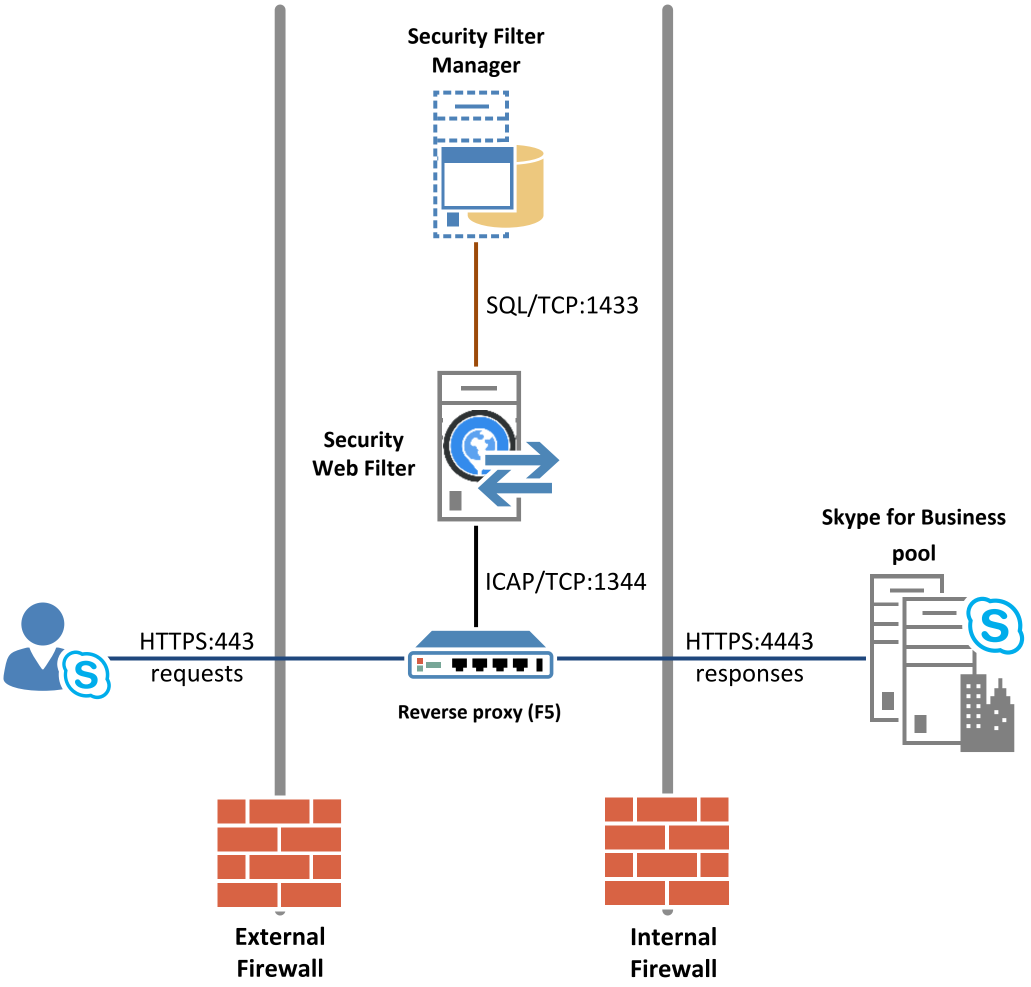


Figure 4.2.1 F5 BIG-IP Configuration

5.1 Configure BIG-IP

The BIG-IP LTM should be configured to forward only Skype for Business (and Exchange if desired) traffic to the Security Web Filter. Other Web traffic does not need to go through the Security Web Filter.

To configure the BIG-IP LTM to forward HTTPS traffic to the Security Web Filter, an internal virtual server must be defined on the BIG-IP LTM. The internal virtual server is defined to forward the request to a pool of Security Web Filters (i.e. ICAP servers) to perform content inspection and modification. When the BIG-IP LTM receives a client's request, the request is forwarded to the internal virtual server (i.e. Security Web Filter). The internal virtual server uses an ICAP profile, so that BIG-IP LTM knows how to forward the HTTP request as an ICAP message.

The BIG-IP LTM configuration consists of the following steps:

1. Define ICAP profiles
2. Define ICAP monitor (optional)
3. Define Security Web Filter pool
4. Define Virtual Servers
5. Define Request Adapt and Response Adapt profile

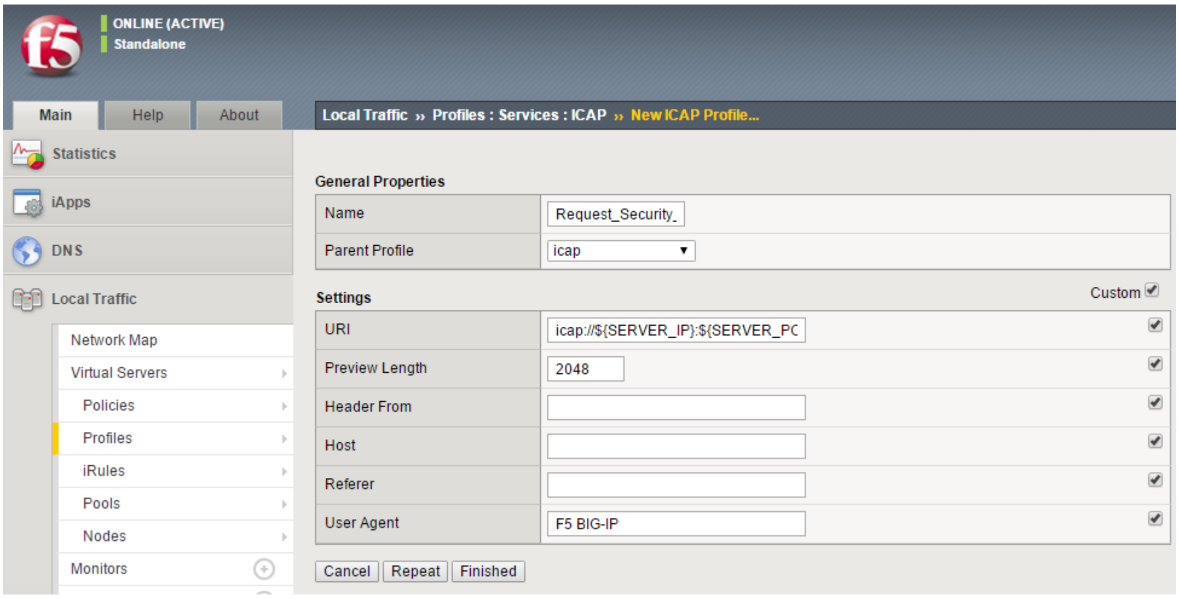
5.1.1 Define ICAP profiles

You'll define two ICAP profiles on the BIG-IP LTM to wrap the HTTP requests or responses into an ICAP message. The request ICAP profile is for client requests. The response ICAP profile is for Skype for Business and Exchange server responses.

From the F5 BIG-IP Configuration Utility, complete the following steps to create an ICAP profile for requests:

1. Navigate to **Local Traffic** -> **Profiles** -> **Services** -> **ICAP**
2. Click **Create** to create a new ICAP profile
3. Specify a unique name for the request profile (i.e. Security_Web_Filter_REQ_Profile)
4. Set **Parent Profile** to icap
5. Check **Custom** on the right side of **Settings**
6. Set the **URI** to icap://${SERVER_IP}:${SERVER_PORT}/security_web_filter_req
7. Set the **Preview Length** to 2048
8. Set the **User Agent** to F5 BIG-IP (optional)
9. Leave the other fields blank, and click **Finished** to save the ICAP profile

This request ICAP profile configuration is illustrated in Figure 5.1.1.1.



General Properties

Name	Request_Security_
Parent Profile	icap

Settings Custom ☑

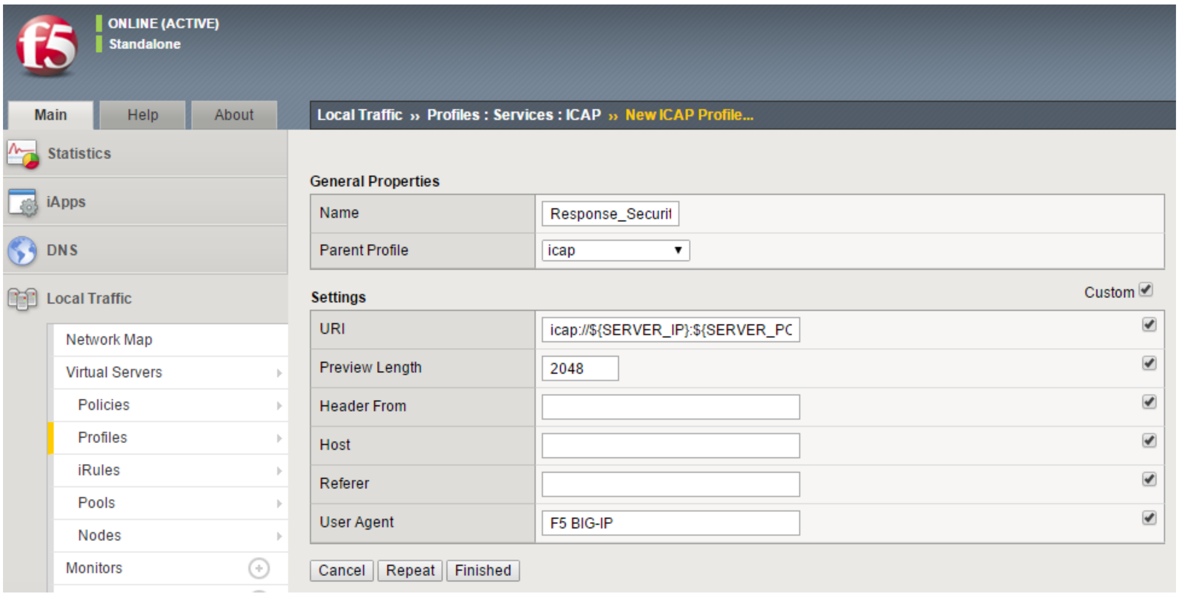
URI	icap://${SERVER_IP}:${SERVER_PC	☑
Preview Length	2048	☑
Header From		☑
Host		☑
Referer		☑
User Agent	F5 BIG-IP	☑

Figure 5.1.1.1 request ICAP Profile

From the F5 BIG-IP Configuration Utility, complete the following steps to create an ICAP profile for responses:

1. Navigate to **Local Traffic** -> **Profiles** -> **Services** -> **ICAP**
2. Click **Create** to create a new ICAP profile
3. Specify a unique name for the request profile (i.e. Security_Web_Filter_RESP_Profile)
4. Set **Parent Profile** to icap
5. Check **Custom** on the right side of **Settings**
6. Set the **URI** to icap://${SERVER_IP}:${SERVER_PORT}/security_web_filter_resp
7. Set the **Preview Length** to 2048
8. Set the **User Agent** to F5 BIG-IP (optional)
9. Leave the other fields blank, and click **Finished** to save the ICAP profile

This response ICAP profile configuration is illustrated in Figure 5.1.1.2.



Local Traffic » Profiles : Services : ICAP » New ICAP Profile...

General Properties

Name	Response_Securit
Parent Profile	icap

Settings

		Custom ☑
URI	icap://${SERVER_IP}:${SERVER_PC	☑
Preview Length	2048	☑
Header From		☑
Host		☑
Referer		☑
User Agent	F5 BIG-IP	☑

Cancel | Repeat | Finished

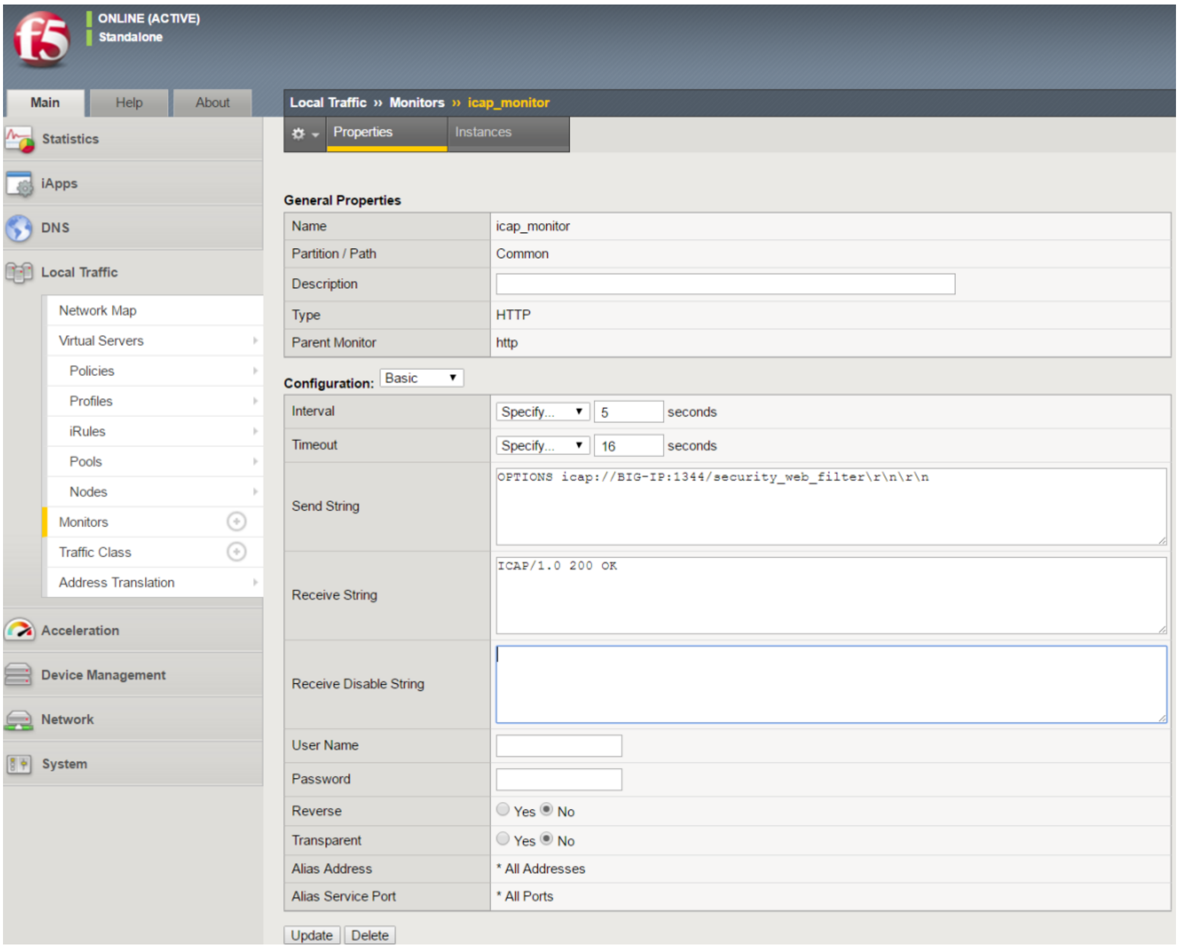
Figure 5.1.1.2 response ICAP Profile

5.1.2 Define ICAP monitor

You can specify a monitor to check the state of the Security Web Filters. This monitor uses the ICAP standard “OPTIONS” method to query the status of the Security Web Filters. Once you’ve defined this monitor, you’ll configure the Security Web Filter pool to use this monitor. Configuring a monitor is optional, but recommended.

1. Navigate to **Local Traffic** -> **Monitors**
2. Select Create
3. Specify a name for your monitor (i.e. icap_monitor)
4. Specify a **Description** of your choosing
5. Specify the string “OPTIONS icap://BIG-IP:1344/security_web_filter\r\n\r\n” for the **Send String**
6. Specify the string “ICAP/1.0 200 OK” for the **Receive String**
7. Click **Finished**

This monitor configuration for the Security Web Filter servers is illustrated in Figure 5.1.2.1.



Local Traffic » Monitors » icap_monitor

General Properties

Name	icap_monitor
Partition / Path	Common
Description	
Type	HTTP
Parent Monitor	http

Configuration: Basic

Interval	Specify... 5 seconds
Timeout	Specify... 16 seconds
Send String	`OPTIONS icap://BIG-IP:1344/security_web_filter\r\n\r\n`
Receive String	`ICAP/1.0 200 OK`
Receive Disable String	
User Name	
Password	
Reverse	○ Yes ● No
Transparent	○ Yes ● No
Alias Address	* All Addresses
Alias Service Port	* All Ports

Figure 5.1.2.1 Security Web Filter pool

5.1.3 Define Security Web Filter pool

You'll define a pool of available Security Web Filter servers (i.e. ICAP servers). The same pool of Security Web Filter servers will inspect both HTTP requests and responses between clients and Skype for Business and Exchange servers.

From the F5 BIG-IP Configuration Utility, complete the following steps to create a pool:

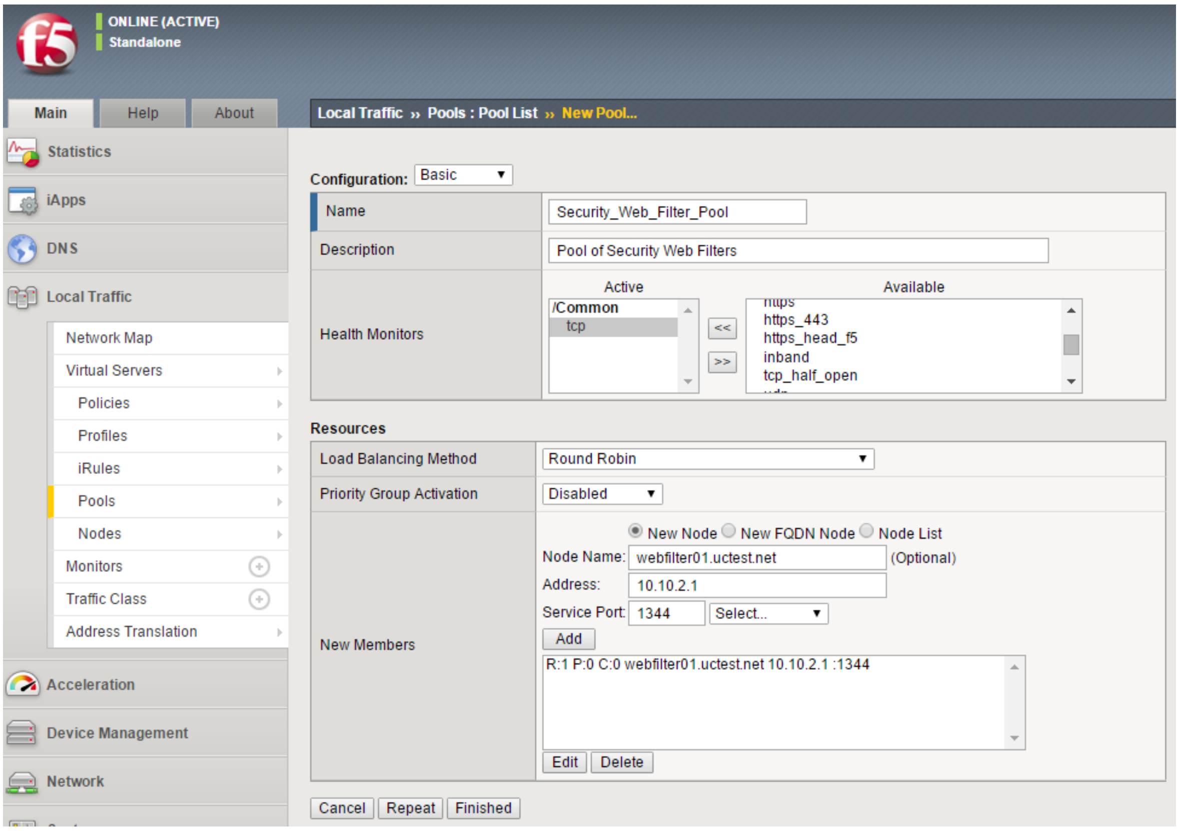
1. Navigate to **Local Traffic** -> **Pools** -> **Pool List**
2. Click **Create** to create a new pool
3. Specify a unique **Name** of your choosing for the pool (i.e. Security_Web_Filter_Pool)
4. Specify a **Description** of your choosing (i.e. "Pool of Security Web Filters")
5. Select the icap_monitor (created in section 5.1.2) for the **Health Monitor** from the list of available monitors
6. Select Round Robin for the **Load Balancing Method**
7. Select Disabled for the **Priority Group Activation**
8. For each of your Security Web Filter servers, specify the server's:
    a. FQDN or name in **Node Name**
    b. IP address in **Address**

   c. 1344 in **Service Port**

   d. Click **Add**

9. Click **Finished**

This pool configuration of Security Web Filter servers is illustrated in Figure 5.1.3.1.



Configuration: Basic

Name	Security_Web_Filter_Pool
Description	Pool of Security Web Filters
Health Monitors	Active: /Common tcp Available: https_443 https_head_f5 inband tcp_half_open

Resources

Load Balancing Method	Round Robin
Priority Group Activation	Disabled
New Members	● New Node ○ New FQDN Node ○ Node List Node Name: webfilter01.uctest.net (Optional) Address: 10.10.2.1 Service Port: 1344 Select... R:1 P:0 C:0 webfilter01.uctest.net 10.10.2.1 :1344

Figure 5.1.3.1 Security Web Filter pool

5.1.4 Define Virtual Servers

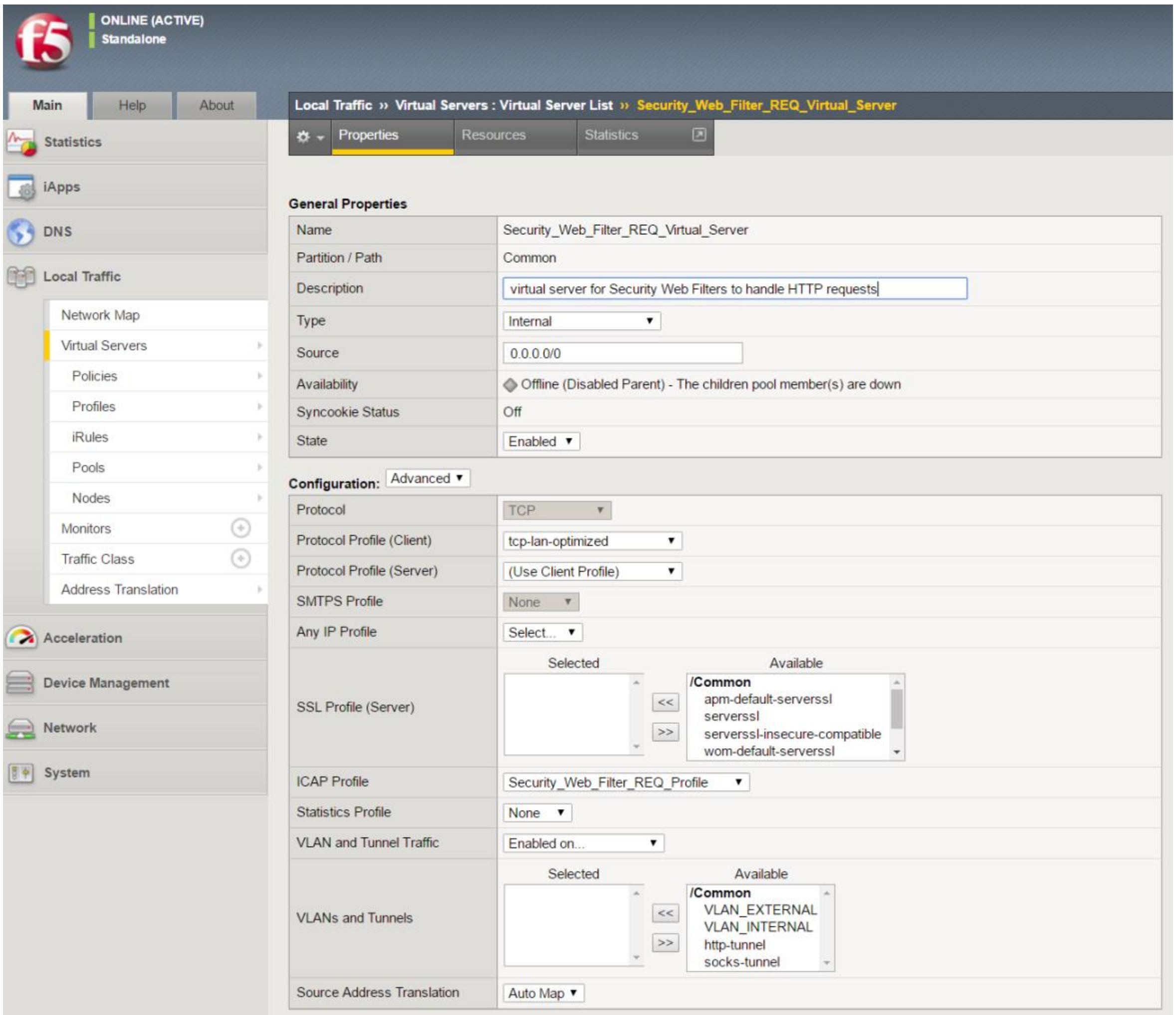
You'll define two virtual servers to forward requests and responses to the pool of Security Web Filter servers (created in section 5.1.3). A separate virtual server is defined for each type of adaptation (requests and responses).

From the F5 BIG-IP Configuration Utility, complete the following steps to create a virtual server for requests:

1. Navigate to **Local Traffic** -> **Virtual Servers** -> **Virtual Server List**
2. Click **Create** to create a virtual server
3. Specify a unique **Name** of your choosing for the virtual server (i.e. Security_Web_Filter_REQ_Virtual_Server)
4. Specify a **Description** of your choosing (i.e. "virtual server for Security Web Filters to handle HTTP requests")
5. Select internal for **Type**

6. Select Enabled for **State**
7. Select Advanced from the **Configuration** drop-down
8. Select TCP for **Protocol**
9. Select tcp-lan-optimized for **Protocol Profile (Client)**
10. Select the request ICAP profile (i.e. Security_Web_Filter_REQ_Profile) created in section 5.1.1 for the **ICAP Profile**
11. Select Auto Map for **Source Address Translation**
12. Select the pool (i.e. Security_Web_Filter_Pool) created in section 5.1.3 for the **Default Pool**
13. Select the **Resources** tab
14. Select *source_addr* for **Default Persistence Profile** to enable source address affinity
15. Click **Finished**

This virtual server configuration for requests is illustrated in Figure 5.1.4.1.



Local Traffic » Virtual Servers : Virtual Server List » Security_Web_Filter_REQ_Virtual_Server

General Properties

Name	Security_Web_Filter_REQ_Virtual_Server
Partition / Path	Common
Description	virtual server for Security Web Filters to handle HTTP requests
Type	Internal
Source	0.0.0.0/0
Availability	Offline (Disabled Parent) - The children pool member(s) are down
Syncookie Status	Off
State	Enabled

Configuration: Advanced

Protocol	TCP
Protocol Profile (Client)	tcp-lan-optimized
Protocol Profile (Server)	(Use Client Profile)
SMTPS Profile	None
Any IP Profile	Select...
SSL Profile (Server)	Selected: Available: /Common apm-default-serverssl serverssl serverssl-insecure-compatible wom-default-serverssl
ICAP Profile	Security_Web_Filter_REQ_Profile
Statistics Profile	None
VLAN and Tunnel Traffic	Enabled on...
VLANs and Tunnels	Selected: Available: /Common VLAN_EXTERNAL VLAN_INTERNAL http-tunnel socks-tunnel
Source Address Translation	Auto Map

Figure 5.1.4.1 virtual server for requests

This virtual server configuration for responses is similar to the virtual server configuration for requests. From the F5 BIG-IP Configuration Utility, complete the following steps to create a virtual server for responses:

1. Navigate to **Local Traffic** -> **Virtual Servers** -> **Virtual Server List**
2. Click **Create** to create a virtual server
3. Specify a unique **Name** of your choosing for the virtual server (i.e. Security_Web_Filter_RESP_Virtual_Server)
4. Specify a **Description** of your choosing (i.e. “virtual server for Security Web Filters to handle HTTP responses”)
5. Select internal for **Type**
6. Select Enabled for **State**
7. Select Advanced from the **Configuration** drop-down
8. Select TCP for **Protocol**
9. Select tcp-lan-optimized for **Protocol Profile (Client)**
10. Select the response ICAP profile (i.e. Security_Web_Filter_RESP_Profile) created in section 5.1.1 for the **ICAP Profile**
11. Select Auto Map for the **Source Address Translation**
12. Select the pool (i.e. Security_Web_Filter_Pool) created in section 5.1.3 for the **Default Pool**
13. Select the **Resources** tab
14. Select *source_addr* for **Default Persistence Profile** to enable source address affinity
15. Click **Finished**

5.1.5 Define Request Adapt profile and Response Adapt profile

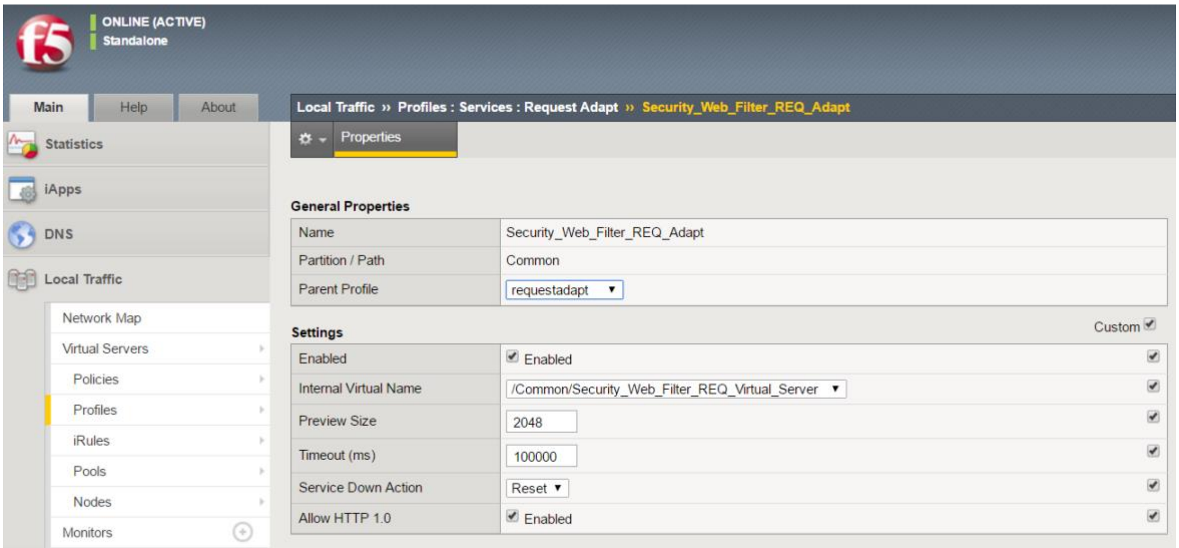
The Adapt profiles forward requests or responses to the corresponding virtual servers. You’ll define a Request Adapt profile to forward requests to the virtual server created to handle requests (see section 5.1.4), and a Response Adapt profile to forwards responses to the virtual server created to handle responses (see section 5.1.4).

From the F5 BIG-IP Configuration Utility, complete the following steps to create a Request Adapt profile:

1. Navigate to **Local Traffic** -> **Profiles** -> **Services** -> **Request Adapt**
2. Click **Create** to create a Request Adapt profile
3. Specify a unique **Name** of your choosing for the Request Adapt profile (i.e. Security_Web_Filter_REQ_Adapt)
4. Select requestadapt for the **Parent Profile**
5. Check **Custom** on the right side of **Settings**

6. Check **Enabled**
7. Select the virtual server (i.e. Security_Web_Filter_REQ_Virtual_Server) created in section 5.1.4 to handle requests for **Internal Virtual Name**
8. Specify 2048 for the **Preview Size**
9. Specify 100000 for the **Timeout (ms)**
10. Select Reset for the **Service Down Action**
11. Check Enabled for **Allow HTTP 1.0**
12. Click **Finished**

This Request Adapt profile configuration is illustrated in Figure 5.1.5.1.



Local Traffic » Profiles : Services : Request Adapt » Security_Web_Filter_REQ_Adapt

General Properties

Name	Security_Web_Filter_REQ_Adapt
Partition / Path	Common
Parent Profile	requestadapt ▼

Settings Custom ☑

Enabled	☑ Enabled	☑
Internal Virtual Name	/Common/Security_Web_Filter_REQ_Virtual_Server ▼	☑
Preview Size	2048	☑
Timeout (ms)	100000	☑
Service Down Action	Reset ▼	☑
Allow HTTP 1.0	☑ Enabled	☑

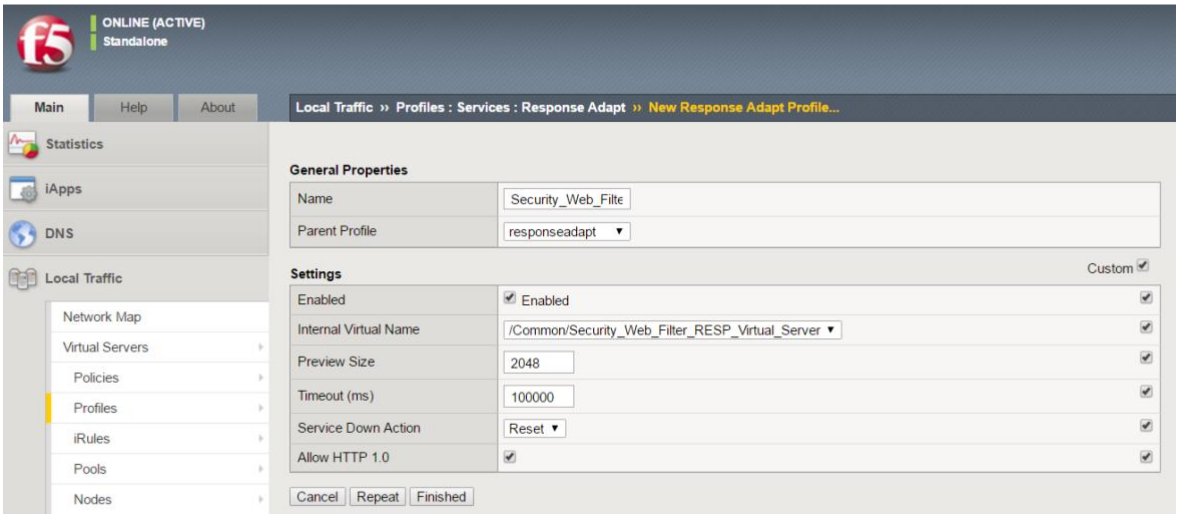
Figure 5.1.5.1 Request Adapt profile

From the F5 BIG-IP Configuration Utility, complete the following steps to create a Response Adapt profile:

1. Navigate to **Local Traffic** -> **Profiles** -> **Services** -> **Response Adapt**
2. Click **Create** to create a Response Adapt profile
3. Specify a unique **Name** of your choosing for the Response Adapt profile (i.e. Security_Web_Filter_RESP_Adapt)
4. Select responseadapt for the **Parent Profile**
5. Check **Custom** on the right side of **Settings**
6. Check **Enabled**
7. Select the virtual server (i.e. Security_Web_Filter_RESP_Virtual_Server) created in section 5.1.4 to handle requests for **Internal Virtual Name**
8. Specify 2048 for the **Preview Size**
9. Specify 100000 for the **Timeout (ms)**

10. Select Reset for the **Service Down Action**
11. Check Enabled for **Allow HTTP 1.0**
12. Click **Finished**

This Response Adapt profile configuration is illustrated in Figure 5.1.5.2.



Local Traffic » Profiles : Services : Response Adapt » New Response Adapt Profile...

General Properties

Name	Security_Web_Filte
Parent Profile	responseadapt ▾

Settings — Custom ☑

Enabled	☑ Enabled	☑
Internal Virtual Name	/Common/Security_Web_Filter_RESP_Virtual_Server ▾	☑
Preview Size	2048	☑
Timeout (ms)	100000	☑
Service Down Action	Reset ▾	☑
Allow HTTP 1.0	☑	☑

Figure 5.1.5.2 Response Adapt profile

5.1.6 Configure HTTP Virtual Server

To route HTTPS traffic to your Skype for Business Servers, you should already have an HTTP virtual server defined otherwise your BIG-IP LTM will not proxy Web traffic to your Skype for Business pools. Configure this HTTP virtual server to use the Request Adapt profile defined in section 5.1.5. This will configure the BIG-IP LTM to send HTTPS requests for content inspection by the Security Web Filter. Configure this HTTP virtual server to use the Response Adapt profile defined in section 5.1.5. This will configure the BIG-IP LTM to send HTTPS responses for content inspection/adaptation by the Security Web Filter.

From the F5 BIG-IP Configuration Utility, complete the following steps to configure your HTTP virtual server to use the created Request Adapt profile and Response Adapt profile:

1. Navigate to **Local Traffic** -> **Virtual Servers** -> **Virtual Server List**
2. Click to open the HTTP virtual server defined to route traffic to your Skype for Business pools.
3. Select Advanced from the **Configuration** drop-down
4. Select the request adapt profile created in section 5.1.5 (i.e. Security_Web_Filter_REQ_Adapt) for **Request Adapt Profile**
5. Select the response adapt profile created in section 5.1.5 (i.e. Security_Web_Filter_RESP_Adapt) for **Response Adapt Profile**
6. Select Auto Map for the **Source Address Translation**

7. Click **Update**

6 References

ICAP standard (RFC 3507):

https://tools.ietf.org/html/rfc3507

Configuring Content Adaptation for HTTP Requests:

https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-implementations-11-3-0/12.html