Web Security Service

Proxy Forwarding Access Method

Version 6.10.2.x/Nov.17.2017

Symantec

Copyrights

Symantec Corporation

350 Ellis Street
Mountain View, CA 94043

www.symantec.com

Web Security Service: Proxy Forward Access Method

The Symantec Web Security Service solutions provide real-time protection against web-borne threats. As a cloud-based product, the Web Security Service leverages Symantec's proven security technology as well as the WebPulse™ cloud community of over 75 million users.

With extensive web application controls and detailed reporting features, IT administrators can use the Web Security Service to create and enforce granular policies that are instantly applied to all covered users, including fixed locations and roaming users.

This document describes how to send logs from an existing Symantec ProxySG or Microsoft appliance (ISA Proxy or Forefront Threat Management Gateway) to the Web Security Service for security scanning and policy checks.

- "Learn..." on page 8
- "Configure..." on page 13
- "References" on page 54

This document contains topics collected from the Web Security Service online documentation. For the complete doc set, see:

Symantec Support Site > WSS Documentation

Table Of Contents

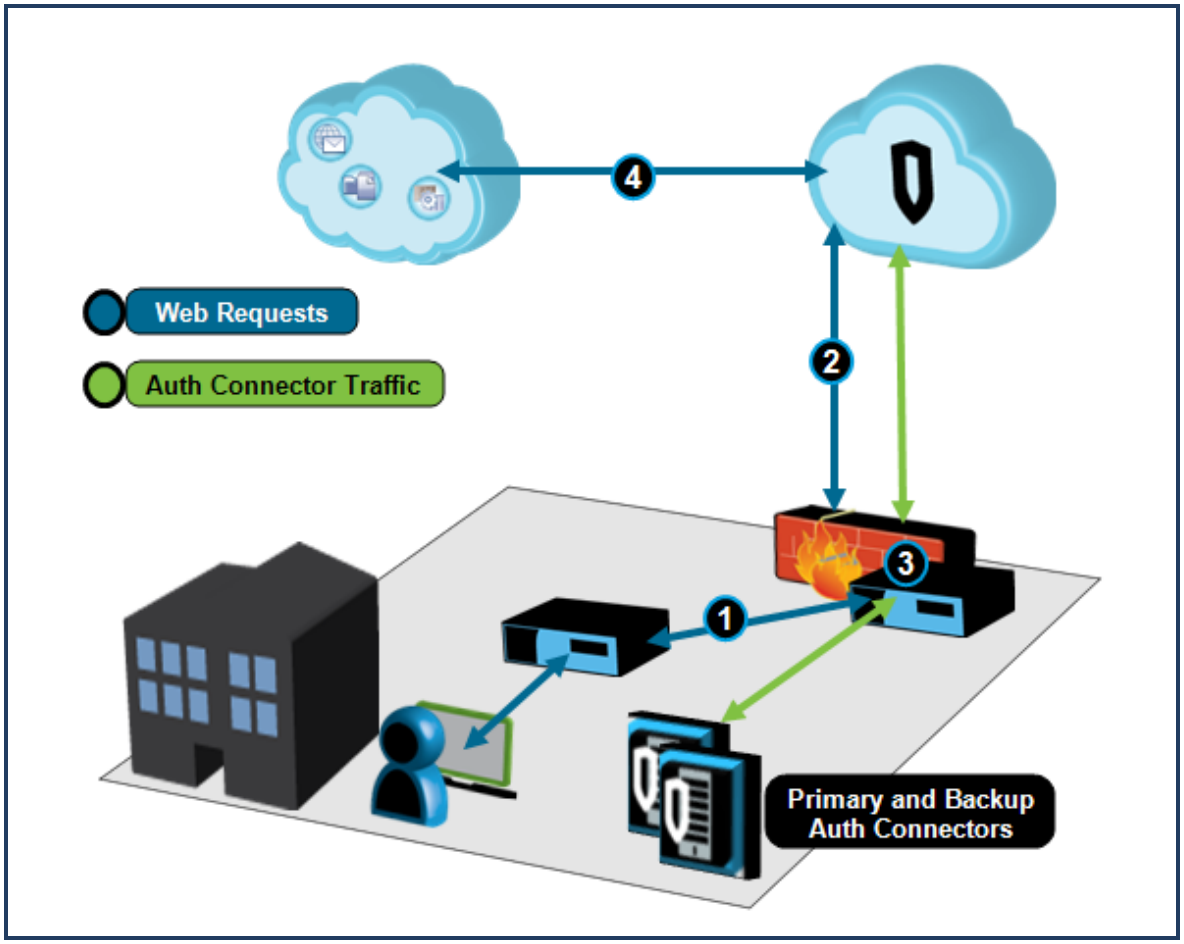
Learn...

This section describes the purpose of the Unified Agent application, which provides security to users who use corporate clients, such as laptops, outside of the corporate network.

About ProxySG Appliance Forwarding

The Proxy Forwarding access method allows you to configure an existing Symantec ProxySG appliance (or other supported proxy) to forward non-internal Web traffic to the Symantec Web Security Service. AES encryption provides central yet secure reporting solution for all locations.

This topic references SymantecProxySG appliances. The Web Security Service also supports Microsoft ISA/TMG proxies. See "About Microsoft ISA/TMG Proxy Forwarding" on page 11.



Data Flow:

1–The gateway ProxySG appliance accepts requests from a downstream proxy or directly from clients.

2–Host forwarding configuration on the gateway ProxySG appliance routes requests to the Web Security Service over ports 8080 (HTTP proxy for HTTPS and SSL traffic) and 8443 (unintercepted SSL traffic plus user/group header information). If the ProxySG appliance is running SGOS 6.4.x or later, you can configure it to intercept some SSL traffic locally; you can then create an additional forwarding host on port 8084.

The gateway ProxySG sends the user identity and group affiliation (added to the request).

The gateway firewall must allow ports 8080, 8443, and 8084 (if configured). See "Reference: Required Locations, Ports, and Protocols" on page 65.

3–The Symantec Auth Connector application allows the Web Security Service to communicate with your Active Directory and provide the user/group information to the service for use in custom policy creation. See Enable User/Group Names Custom Policy (AuthConnector).

If the Primary Active Directory goes down and you have a Backup Active Directory/Auth Connector configuration, seamless failover occurs.

4–The Web Security Service configuration and policy extracts the user information from the request to complete transaction authentication and sends the content request to the Web.

Why Select This Method?

- Your Secure Web Gateway solution already implements proxies.
- Supports using any standard method to route user web traffic: PAC file (explicit proxy), browser settings, WCCP, and inline.
- Enables you to leverage policy-based routing and route selected groups to the Web Security Service.

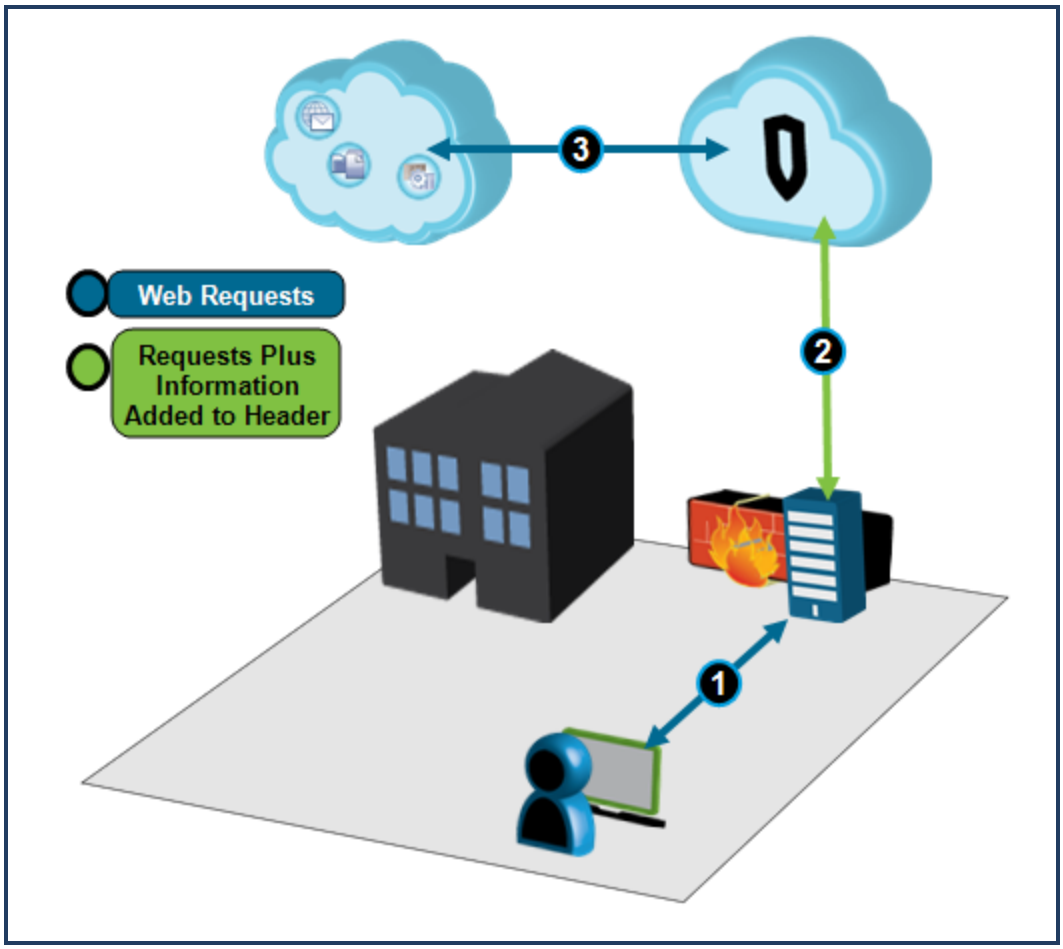
About Microsoft ISA/TMG Proxy Forwarding

The Symantec Web Security Service supports a deployment where Microsoft® Internet Security and Acceleration (ISA)™ 2006 or Microsoft Forefront Threat Management Gateway (TMG)™ proxy servers forward information about authenticated user sessions. To do this, you must install the Symantec Internet Server Application Programming Interface (ISAPI) filter (also known as the Symantec ISA Filter) on the ISA/TMG server. This filter, which is a Dynamic Link Library (DLL), extends the functionality of the ISA/TMG server to add the authenticated user name and client IP address to the HTTP headers in the client requests it forwards to the Web Security Service, which in turn uses this information to perform user-based policy decisions. AES encryption provides central yet secure reporting solution for all locations.

By default, when the Symantec ISA filter is installed, the ISA/TMG adds the following HTTP headers to the requests it sends to the service:

- `X-Forwarded-For`: Used to forward the client IP address.
- `BC_Auth_User` and `BC_Auth_Groups`: Used to forward the authenticated user name (if available). The value in this field is base-64 encoded. If the current session is unauthenticated, the ISA/TMG server will not include a value for this header.

Although these are the only headers that the Symantec ISA filter adds by default, you can edit the `bc-isapifilter.ini` file to include any additional headers that you require by associating a header name with an ISA server variable and an encoding type for the header value. Non-standard HTTP headers typically begin with `X-` and they *must* end with a colon (`:`).



Data Flow

1–The gateway ISA/TMG appliance accepts requests directly from clients (or a downstream proxy) and validates user and group memberships.

2–The installed ISA filter on the ISA/TMG device routes requests to the Web Security Service over ports 8080 (HTTP proxy for HTTPS and SSL traffic) and 8443. The filter adds information to the header: HTTPS server for HTTP traffic plus user/group header information.

3–The Web Security Service extracts the user information from the request to complete transaction authentication. The service processes the web request and returns the content to the user if that content is allowable by policy and is found free of malware.

Why Select This Method?

- Your Secure Web Gateway solution already implements an ISA/TMG proxy.
- Supports using any standard method to route user web traffic: PAC file (explicit proxy), browser settings, WCCP, and inline.
- Enables you to leverage policy-based routing and route selected groups to the Web Security Service.

Configure...

To connect remote users to the Symantec Web Security Service, you must download the Unified Agent application and install it on client systems, then configure various options on the service.

Plan

- Plan the Forwarding Access Method

Install

1. Prerequisite–To make use of user and group names in policy, the Auth Connector application integration with your Active Directory deployment is required. If necessary, consult the Web Security Service documentation relating to this component.
2. If not yet existing, define a Proxy Forward *location* in the Web Security Service. A location instructs the Web Security Service to listen for traffic from specific proxy device IP addresses. "Add a Proxy Forwarding Location" on page 15.
3. Configure proxy device to forward web requests to the Web Security Service.

   Symantec

   - "ProxySG Forwarding Configuration: SGOS 6.x/7.x" on page 17
   - "Reference: Additional Authentication CPL for SGOS MACH 5 Proxy Forwarding" on page 63

   Microsoft

   - "Install the ISA Filter" on page 28 (required for Microsoft proxy deployments).
   - "Forward From Microsoft ISA to the Web Security Service" on page 30
   - "Forward From Microsoft TMG to the Web Security Service" on page 39

Verify

- "Verify Service Connectivity to Locations" on page 49

Reference

- "Reference: Proxy Forwarding Policy" on page 59
- "Reference: Additional Authentication CPL for SGOS MACH 5 Proxy Forwarding" on page 63

Plan The Proxy Forward Access Method

Complete the forms in the following sheet (one per location).

Step 1–Enter Network Information

Network Item	Comments	Values
Web Security Service hostname	Required during hostname configuration.	proxy.threatpulse.net
SGOS Version		☐ 4.3 ☐ 5.5.x/6.1.3.x ☐ 6.4.x/6.5.x/6.6.x
Firewall Ports	Must be opened: SGOS 6.5.x+/inspect some SSL traffic locally:	8080, 8443 8084

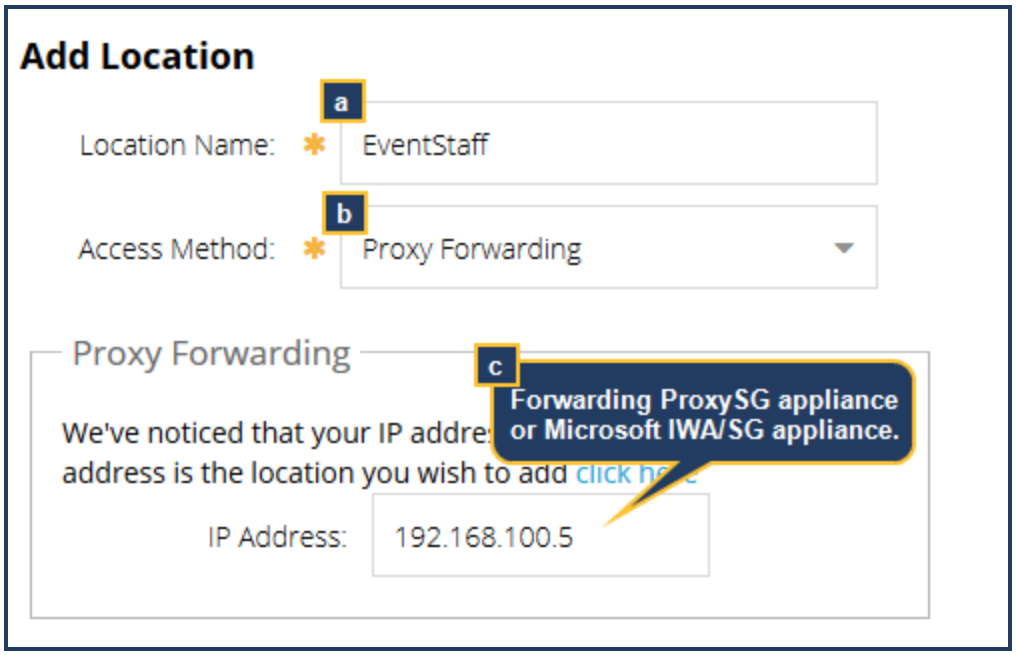
Step 2–Specify Groups of Interest

Item	Comments	Values
Interest Group 1	Group of interest sent to the Web Security Service.	Group Example: HQ-SALES\NAWest User Example: HQ-SALES\Administrator
Interest Group 2		
Interest Group 3		
Interest Group 4		
Interest Group 5		
Interest Group 6		
Interest Group 7		

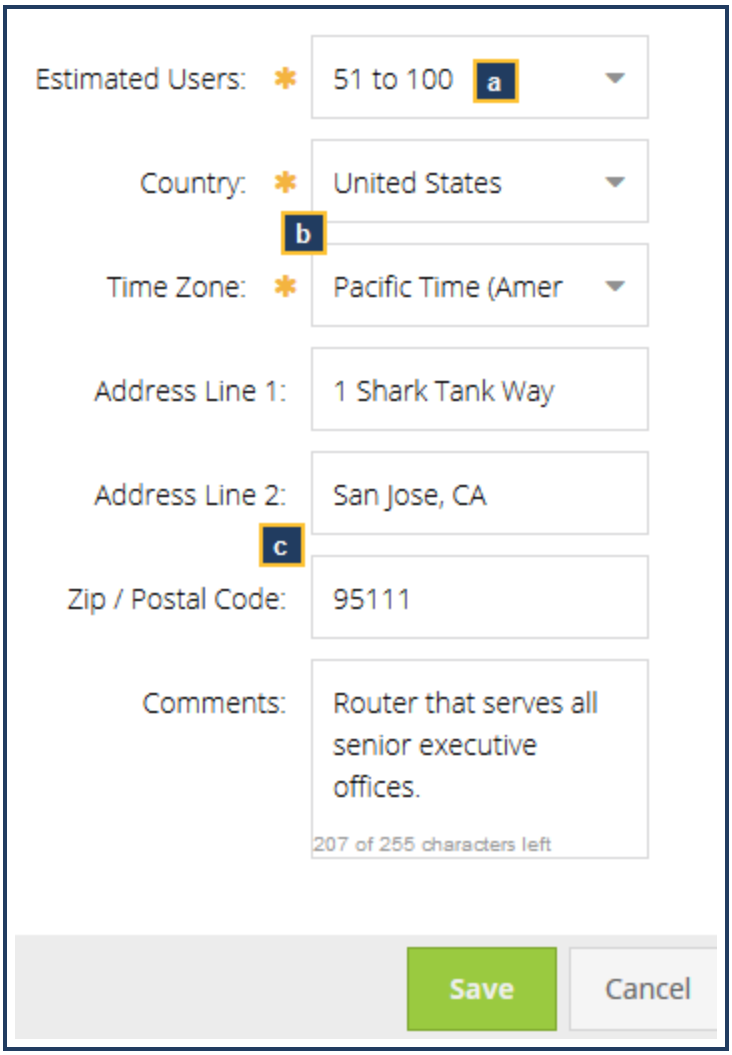
Add a Proxy Forwarding Location

Each forwarding host that is configured to send web traffic to the Symantec Web Security Service requires an equivalent location configuration. The service supports forwarded traffic from SymantecProxySG appliances and Microsoft Internet Security and Acceleration (ISA) 2006 or Microsoft Forefront Threat Management Gateway (TMG) proxy servers.

1. In Service Mode, select **Network > Locations**.
2. Click **Add Location**.
3. Complete the **Location** dialog.



   a. **Name** the location. For example, a location designation or employee group identification name.
   b. Select **Proxy Forwarding** as the **Access Method**.
   c. Enter the gateway **IP/Subnet** that you defined in the ProxySG forwarding host configuration dialog or ISA/TWG policy.
4. Enter resource and location information.



a. Select the **Estimated User** range that will be sending web requests through this gateway interface.Symantec uses this information to ensure proper resources.

b. Select a **Country** and **Time Zone**.

c. Fill out location information and enter comments (optional).

5. Click **Save**.

Next Step

- "Verify Service Connectivity to Locations" on page 49.

ProxySG Forwarding Configuration: SGOS 6.x/7.x

To configure an existing gateway ProxySG appliance to forward HTTP/HTTPS traffic from downstream devices/clients up to the Symantec Web Security Service, you must create forwarding hosts that carry HTTP, HTTPS, and SSL traffic. The forwarding policy installed on the ProxySG directs traffic to the correct forwarding host.

- Required: HTTP—Traffic forwarded on port 8443 (encrypted).
- Required: Unintercepted SSL—Traffic forwarded on port 8080.
- Optional: Intercepted SSL—A gateway ProxySG appliance running SGOS 6.4.x or later supports the deployment option where the local proxy performs SSL interception and forwards the user authentication information (in addition to traffic) to the Web Security Service on port 8084. While you will likely configure the ProxySG to intercept some SSL traffic (specific categories), you must create this additional service if you do.

This task assumes that the ProxySG appliance is configured and functioning as a gateway proxy. The procedure demonstrates the SGOS 6.5.x SGOS/Management Console.

If you create hosts with the example names in this procedure, you do not need to edit the installed forwarding policy.

Configure the ProxySG Appliance

Prerequisite—Verify that proper authentication is configured on the ProxySG appliance.

To display user names in reports and make user names and groups available for custom policy, the ProxySG appliance must have authentication configured. For more information about Proxy Edition authentication, refer to the document for your SGOS **Version** (drop-down):

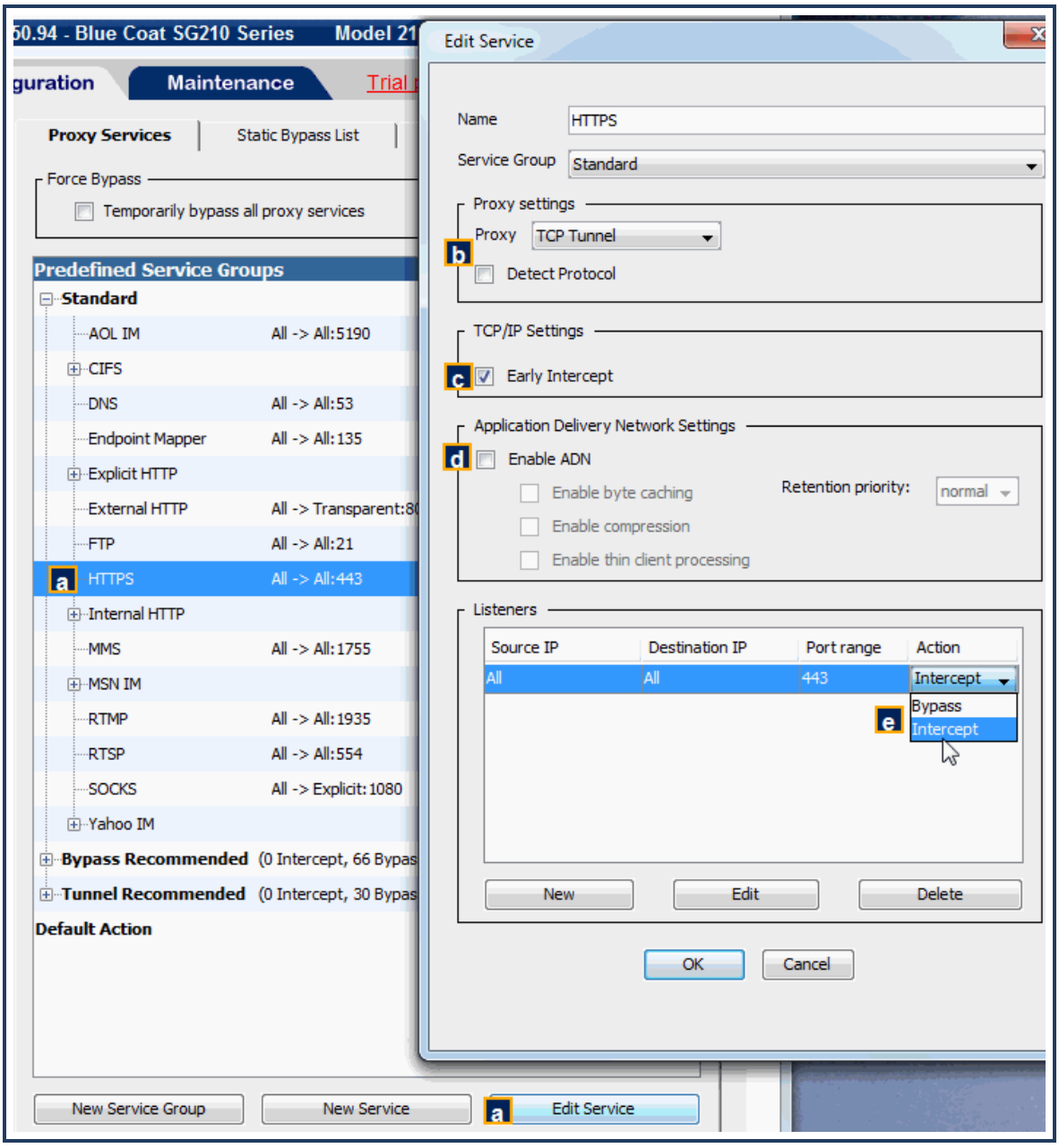
- Symantec ProxySG/SGOS Documentation

For MACH 5 Edition ProxySG appliances, authentication configuration requires adding additional authentication Content Policy Language (CPL) to the Local policy file. See "Reference: Additional Authentication CPL for SGOS MACH 5 Proxy Forwarding" on page 63.

Step 1—Verify that the External/Explicit HTTP proxy services are enabled and set the HTTPS proxy service Proxy Setting to TCP Tunnel.

To avoid connection issues, the **External HTTP** or **Explicit HTTP** proxy services (configured together for ports 80 and 8080) must be enabled and the **HTTPS** proxy service configured use **TCP Tunnel** as the **Proxy Setting**.

1. In the ProxySG appliance Management Console, select **Configuration > Services > Proxy Services**.
2. Verify that either the **Explicit HTTP** or the External HTTP service is enabled (set to **Intercept**); which service depends on your gateway deployment method.
3. Configure the **HTTPS** service to use **TCP_Tunnel**.



a. Select the **Explicit HTTPS** or **External HTTPS** service.

b. In **Proxy Settings**, select **TCP Tunnel**; clear the **Detect Protocol** option.

c. (Recommended) Select **Early Intercept**.

d. Clear the **Enable ADN** option.

e. Set the **Action** to **Intercept**.

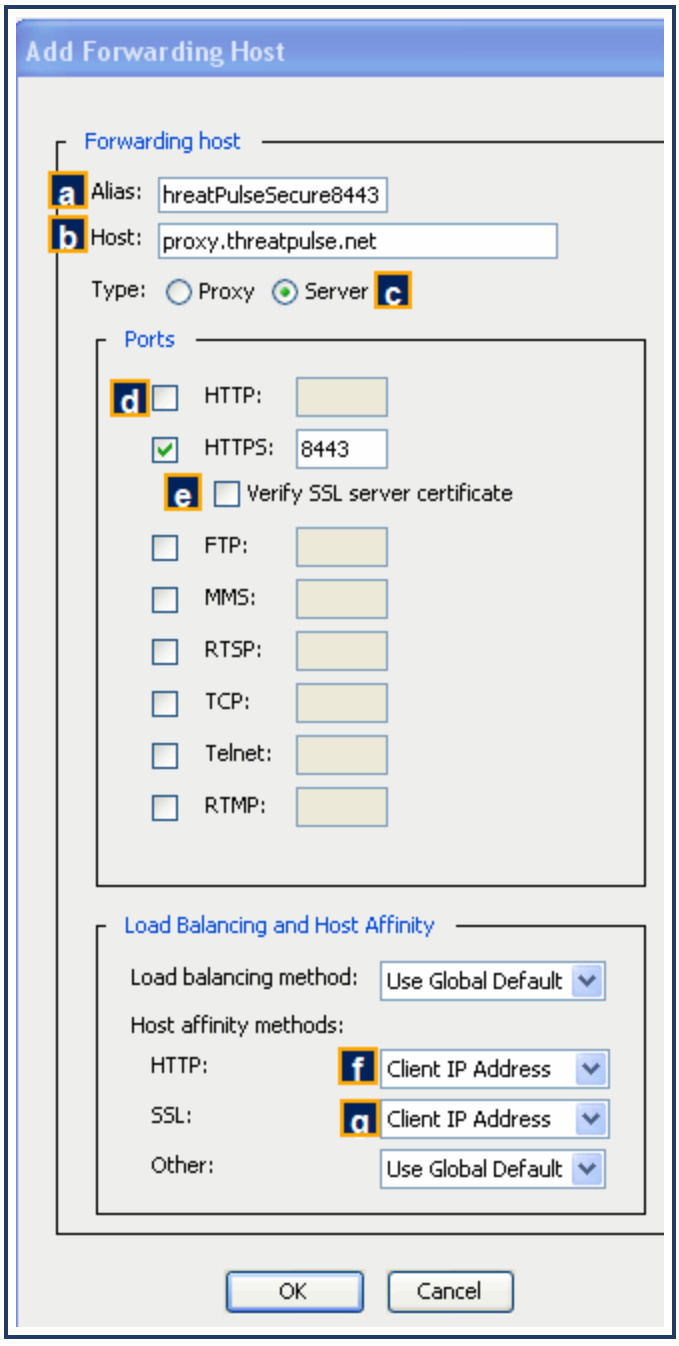
f. Click **OK**.

4. Click **Apply**.

Step 2–Create a Server Forwarding Host for HTTPS (Port 8443).

Forwards HTTP traffic–with an encrypted connection–to the Web Security Service.

1. In the Management Console, select the **Configuration > Forwarding > Forwarding Hosts > Forwarding Hosts** tab.
2. Click **New**. The Management Console displays the Add Forwarding Hosts dialog.
3. Create the Web Security Service host.



a. Enter an **Alias** name the host. For example: **`ThreatPulseSecure8443`**.

b. Enter the Web Security Service**Host** name: **`proxy.threatpulse.net`** (unless you were given another service point name).

c. Select **Server**.

d. Clear the **Ports: HTTP** option.

e. Enter **8443** in the **Ports: HTTPS** field and clear the **Verify SSL server certificate** option.

f. **Host Affinity Methods–HTTP**: Select **Client IP Address**.

g. **Host Affinity Methods–SSL**: Select **Client IP Address**.

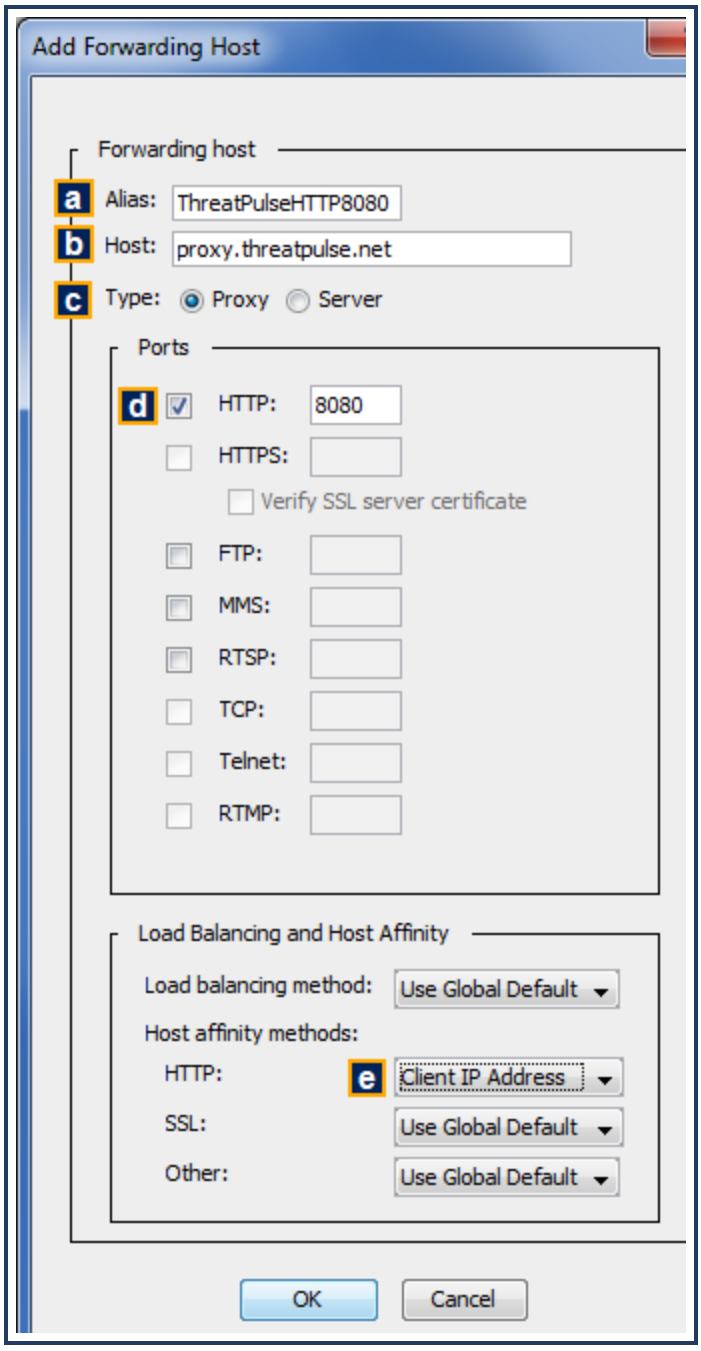
h. Click **OK** to close the dialog.

4. Click **Apply**.

Step 3–Create a Proxy Forwarding Host for Unintercepted SSL (Port 8080)

Forwards HTTPS, SSL, and TCP traffic to the Web Security Service. Installed policy directs the traffic over port 8080 or 443. If configured, the Web Security Service intercepts SSL for policy inspection.

1. In the Management Console, select the **Configuration > Forwarding > Forwarding Hosts > Forwarding Hosts** tab.
2. Click **New**. The Management Console displays the Add Forwarding Hosts dialog.
3. Create the Web Security Service host.



a. Enter an **Alias** name for the host. For example: **`ThreatPulseHTTP8080`**.

b. Enter the Web Security Service**Host** name: **`proxy.threatpulse.net`** (unless you were given another service point name).

c. Select **Proxy**.

d. Enter **`8080`** in the **Ports: HTTP** field.

e. Click **OK** to close the dialog.

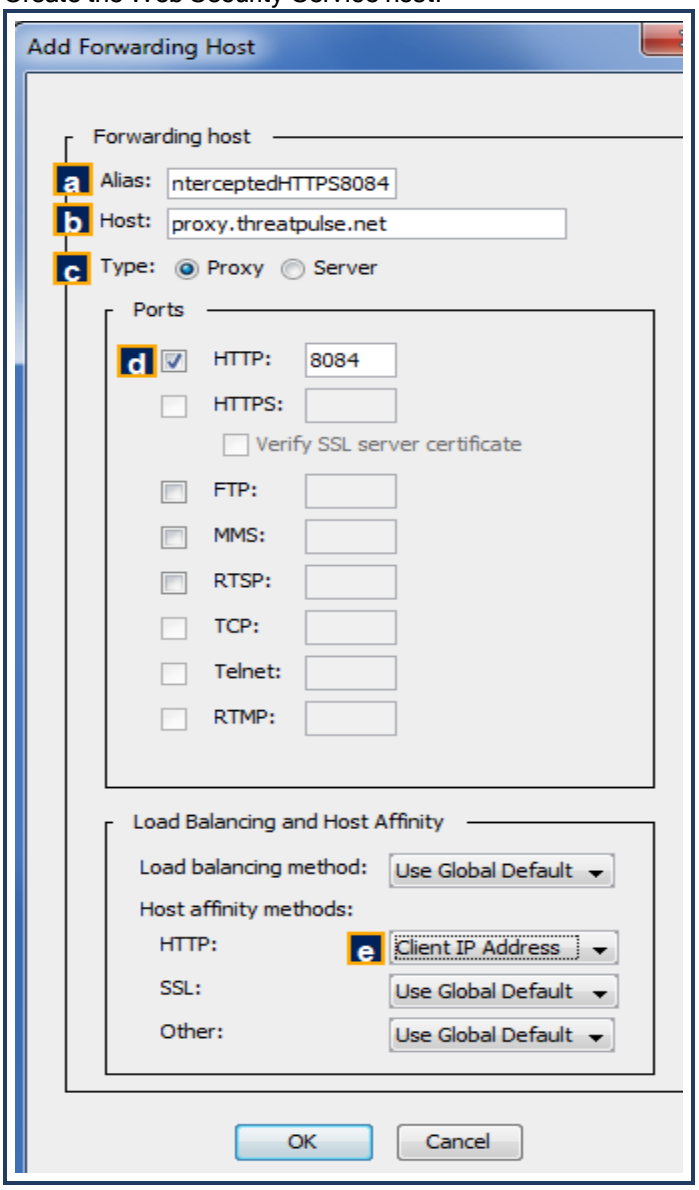
4. Click **Apply**.

Step 4—(Conditional Option) Create a Proxy Forwarding Host for Locally Intercepted SSL Traffic (Port 8084).

If your gateway ProxySG appliance is running SGOS 6.4.x or later and you have configured it to intercept some SSL traffic

for local inspection and user authentication forwarding, configure a forwarding host for port 8084.

1. In the Management Console, select the **Configuration > Forwarding > Forwarding Hosts > Forwarding Hosts** tab.
2. Click **New**. The Management Console displays the Add Forwarding Hosts dialog.
3. Create the Web Security Service host.



   a. Enter an **Alias** name the host. For example: **`ThreatPulseInterceptedHTTPS8084`**.

   b. Enter the Web Security Service **Host** name: **`proxy.threatpulse.net`** (unless you were given another service point name).

   c. Select **Proxy**.

   d. Enter **`8084`** in the **Ports: HTTP** field.

e. **Host Affinity Methods–HTTP**: Select **Client IP Address**.

f. Click **OK** to close the dialog.

4. Click **Apply**.

Step 5–On the gateway ProxySG appliance, define policy that sends traffic to the forwarding host.

1. In the Management Console, select the **Configuration > Policy > Policy Files** tab.
2. Install the forwarding policy:
   a. In the **Install Policy** area, select **Text Editor** from the **Install Forward File From** drop-down list.
   b. Click **Install**; the interface displays the Edit and Install the Forward File dialog.
   c. Enter the forwarding policy to the *end* of any existing forwarding policy. To copy and paste in a template created by Symantec, see "Reference: Proxy Forwarding Policy" on page 59.
   d. Click **Install** to close the dialog.
3. This step is required if these groups are not currently referenced in the gateway proxy policies or if you want the ability to define Web Security Service policy against these groups.

   Define policy that lists the groups of interest that are allowed access to the Web Security Service. Add this policy to the Forward file or the Central file (if you use one for easier distribution).
   a. In the **Install Policy** area, select **Text Editor** from the **Install Forward File From** or **Install Central File From** drop-down list.
   b. Click **Install**; the interface displays the Edit and Install the File dialog.
   c. Paste in the following policy, which defines the groups of interest that are subject to Web Security Service policy and are visible in reports. Add this at the *end* of any existing central policy:

   ```
   define condition threatpulse_groups
      group = (group_name, group_name, group_name)
   end
   ```

   d. Click **Install** to close the dialog.
4. Click **Apply**.

Step 6–Other Required ProxySG appliance configuration best practices.

Enable port randomization and allow for the full TCP-IP port range.

From the ProxySG CLI (`enable > configure` mode), enter the following commands:

```
#config term
#(config)tcp-ip inet-lowport 16384
#(config)tcp-ip tcp-randomize-port enable
#(config)exit
```

Do not use the **Reflect Client IP** option because this disables port randomization, which forces the use of another, not-recommended port mapping algorithm.

- ProxySG Management Console: Select the **Configuration > Proxy Settings > General > General** tab and clear the **Reflect client's source IP when connecting to servers** option.

- ProxySG CLI (enable > configure mode):

```
SGOS#(config) general
SGOS#(config general) reflect-client-ip disable
```

The Reflect Client IP option is also available in policy. Verify that you do not have any policy actions that enable Reflect Client IP.

Verify Required Open Ports

Configure the gateway firewall device to allow traffic from the gateway ProxySG on ports 8080 and 8443. If you created a forwarding host for port 8084 in **Step 4**, ensure that port is also open.

Next Step

- "Add a Proxy Forwarding Location" on page 15.

Plan the Microsoft Proxy Forwarding Access Method

Complete the forms in the following sheet (one per location).

Step 1–Select your server model and enter network Information

The devices listed here were officially tested. Similar models might have varying configuration interfaces. You can configure any device that supports site-too-site VPN. The company adds more devices after they are tested by QA.You can also search the Symantec Knowledge Base, which occasionally provides documented, yet not-as-yet sanctioned device configuration steps.

Network Item	Comments	Values
Model	☐ ISA (Windows Server, 32-bit) ☐ TMG (Windows 2008 Server, 64-bit)	
ISA/TMG Server Location	Network Information	
	Location (example: region, lab ID):	
	Domain:	
	Server Name:	
	Folder for Symantec filter file:	
Firewall Ports	Required:	8080, 8443
Authentication Filter Present on Proxy	Required; look in System > Web Filters.	☐ Yes ☐ No (must install one)

Step 2–Specify Groups of Interest

You can specify which groups or users from your security directory are forwarded to the Web Security Service.

Item	Comments	Values
Interest Group 1	Group of interest sent to the Web Security Service.	Group Example: HQ-SALES\NAWest User Example: HQ-SALES\Administrator
Interest Group 2		
Interest Group 3		
Interest Group 4		
Interest Group 5		
Interest Group 6		
Interest Group 7		

Step 3–Select a Regional Web Security Service IP Address

Required for the IPsec configuration. Your region dictates which IP address (or set of addresses) to enter. The format is: **Estimated optimal region coverage (Data Center location)**. Select a primary and a secondary (for redundancy) location.

Occasionally, changes occur before documentation is revised. If you encounter a connection issue, refer to this Support Article to reconcile: **https://support.symantec.com/en_US/article.TECH242979.html**.

Americas			
North America: West **(Sunnyvale/Santa Clara, CA, USA)** 199.19.248.164 199.19.248.0/24	**North America: West** **(Seattle, WA, USA)** 199.116.168.164	**North America: Central** **(Denver, CO, USA)** 8.39.233.164 [July 28, 2017] (8.39.233.132 was removed on July 28, 2015)	**North America: Central** **(Chicago, IL, USA)** 198.135.124.164 38.134.125.0/24
North America: South **(Dallas, TX, USA)** 199.116.171.164	**North America: East** **(Ashburn, VA, USA)** 199.19.250.164 **148.64.16.0/24** **[November 22, 2017]**	**North America: North East** **(New York, NY, USA)** 199.116.175.164 48.133.154.0/24	**North America: South East** **(Miami, FL, USA)** 199.19.251.164
North America: North/Canada East **(Toronto, Ontario, Canada)** 38.64.174.164	**North America: North/Canada East** **(Montreal, Quebec, Canada)** 199.19.253.164	**Central America** **(Mexico City, Mexico)** 162.97.9.84	**South America: North** **(Sao Paulo, Brazil)** 189.125.138.212
South America: South **(Buenos Aries, Argentina)** 200.41.18.228			

EMEA			
United Kingdom/Ireland/Scandinavia **(London, England)** Location 1 (West): 46.235.152.164 Location 2 (South): 185.2.196.164	**France** **(Paris, France)** 46.235.153.164	**Switzerland/Italy** **(Zurich, Switzerland)** 154.47.224.36	**Sweden** **(Stockholm, Sweden)** 46.235.155.164
Norway **(Oslo, Norway)** 193.240.54.68	**Finland** **(Helsinki, Finland)** 46.235.157.164	**Eastern Europe** **(Frankfurt, Germany)** 46.235.154.164	**Netherlands** **(Amsterdam, Netherlands)** 149.13.178.164
Spain/Portugal **(Madrid, Spain)** 185.180.48.164 (Available September 21, 2017)	**Italy** (revised) **(Milan, Italy)** 46.235.159.164	**South Africa** **(Johannesburg, South Africa)** 197.96.129.164	**Israel** **(Tel Aviv, Israel)** 81.218.44.68

APAC			
Hong Kong **(Hong Kong)** 103.246.38.164	**Japan/Far East** **(Tokyo, Japan)** 103.246.39.164	**South Korea** **(Seoul, South Korea)** 203.246.168.164	**Singapore** **(Singapore)** 103.246.37.164
India/Western APAC **(Mumbai, India)** 180.179.142.84	**India** **(Chennai, India)** 180.179.40.84	**Dubai** **(UAE)** 46.235.156.164	**Australia** **(Sydney, Australia)** 103.246.36.164
China **(Shanghai, China)** 211.147.76.84	**Taiwan** **(Taipei, Taiwan)** 61.58.46.164	**New Zealand** **(Auckland, New Zealand)** (This location is not presented as a configurable location, as it provides a carrier location for a Symantec partner. However, some devices might detect this geo-location and connect.) 124.157.113.252	

The company continues to add global locations. If you are not in a location specified above, use the following guidelines:

- Southern Europe (Mediterranean): Use Frankfurt or Paris, but not London.
- Middle East and North Africa: Use Frankfurt or Paris, but not London.

Install the ISA Filter

Configuring a Microsoft Internet Security and Acceleration (ISA) 2006 or Forefront Threat Management Gateway (TMG) proxy/firewall server to send web requests plus user identification information to the SymantecWeb Security Service requires two phases. The first phase, described on this page, is install the Symantec ISA filter program on the ISA/TMG device. The installation process copies the appropriate `DLL` and `INI` files to the selected folder and registers the filter with the ISA/TMG server.

Step 1–Download the ISA filter.

1. Save the ISA filter ZIP file to the ISA/TMG server.

   http://portal.threatpulse.com/dl/isa/filter/bcisafilter-setup.zip ~or~

   http://portal.threatpulse.com/docs/am/AccessMethods/deploy/onpremise/proxy/prxy_fwdfilter_ta.htm

2. When prompted, save the `bcisafilter.zip` file to the ISA/TMG server.

Step 2–Unzip the ISA filter file and begin the wizard.

1. Unzip the `bcisafilter.zip` file.
2. Double-click the `bcisafilter.exe` file, which launches the installation wizard.
3. Click **Next** on the first screen.

Step 3–As prompted by the wizard, install the filter file.

1. Specify an **Installation Folder** for the ISA Filter. Accept the default location **(C:\Program Files\Blue Coat Systems\ISAFilter**) or browse to a different location. Click **Next**.
2. Select **Forwarding to the ThreatPulse Cloud Service** and click **Next**.
3. To begin the installation, click **Install**. When the installation completes, click **Next**.

Step 4–Verify that the Symantec ISA filter successfully registered.

On the ISA server:

1. Select **Start > Programs > Microsoft ISA Server > ISA Server Management**.
2. In the **Configuration** section, select **Add-ins**.
3. Select the **Web-filter** tab and verify that the **Blue Coat ISAPI Filter** is there.

On the TMG server:

1. Select **Start > Programs > Microsoft Forefront TMG > Microsoft Forefront TMG Management**
2. In the **System** section, select **Add-in**.
3. Select the **Web-filter** tab and verify that the **Blue Coat ISAPI Filter** is there.

Next Step

To continue the walkthrough, select which Microsoft proxy you have deployed.

- "Forward From Microsoft ISA to the Web Security Service" on the next page
- "Forward From Microsoft TMG to the Web Security Service" on page 39

Forward From Microsoft ISA to the Web Security Service

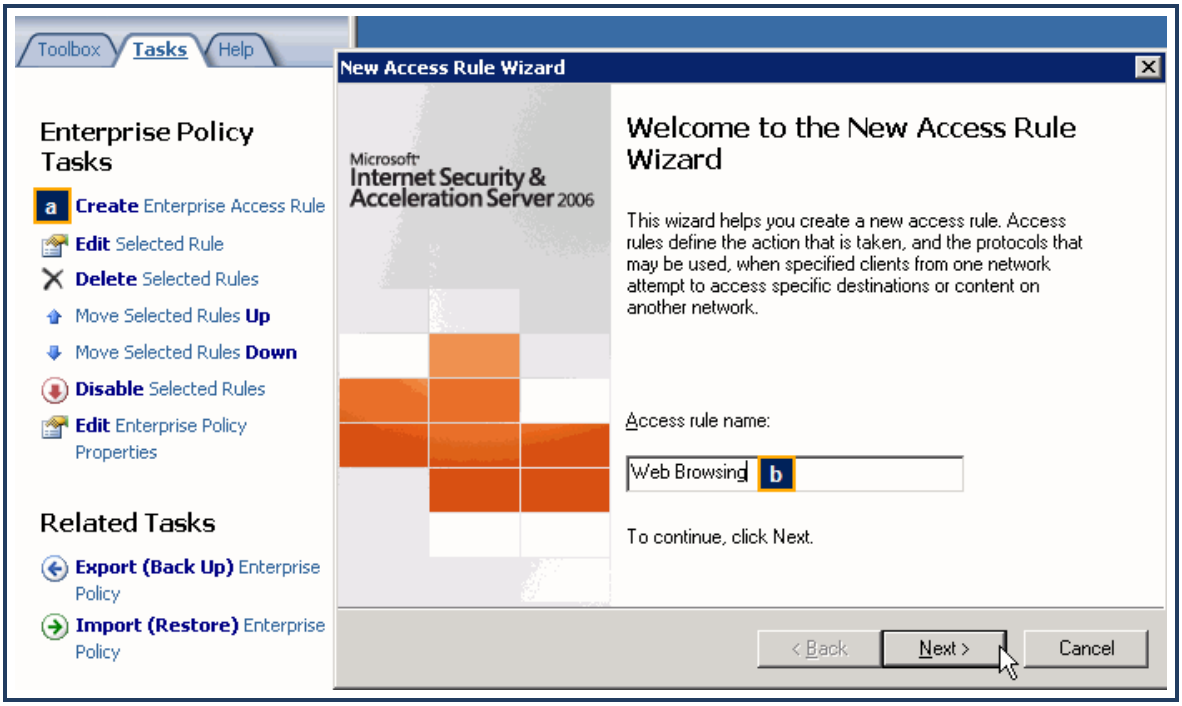
Define policy on the Microsoft ISA server to forward web requests plus user identification information to the Symantec Web Security Service.

Prerequisites.

- The ISA server must be running Windows 2003 Server–32-bit.
- This procedure assumes that the server is already configured and operating.
- Verify existence of authentication filter. An authentication filter that can perform the authentication to the users workstation must be configured. This is usually a Microsoft Web filter and is usually already installed by default. Look in **System > Web Filters**.

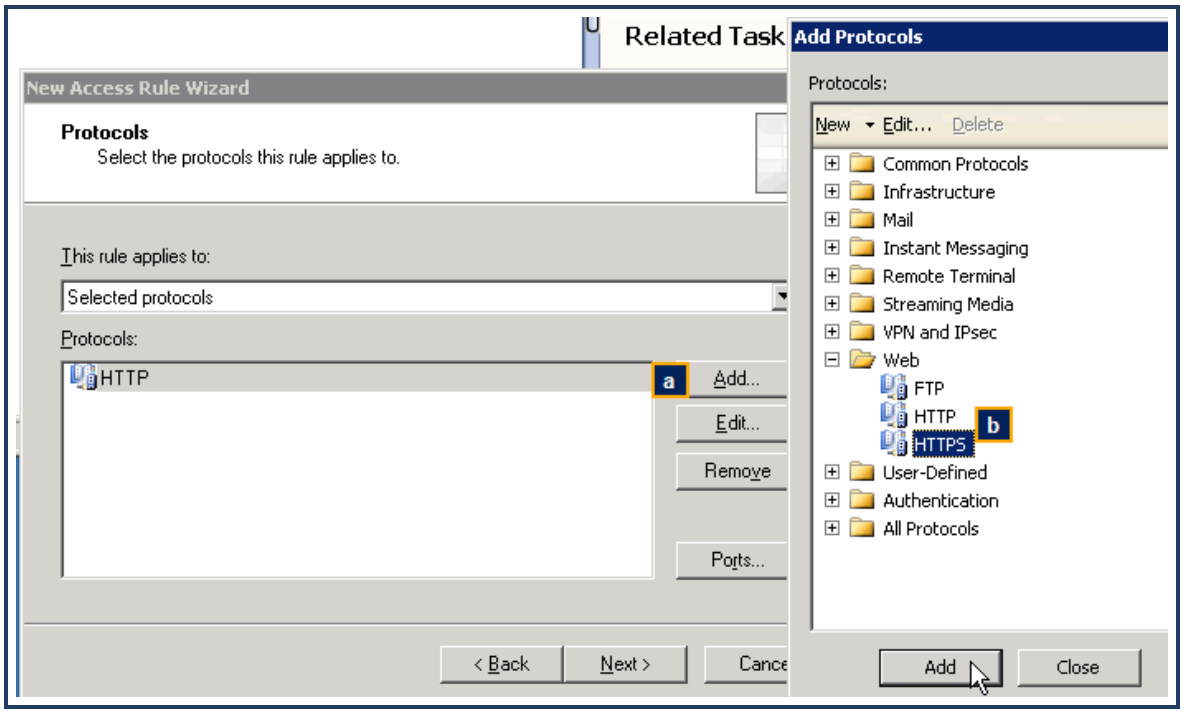
Step 1–Create a Firewall Policy/Access Rule for web traffic (HTTP and HTTPS).

1. If the default location was set during the ISA server installation, select **Start > All Programs > Microsoft ISA Server > ISA Server Management**. The sever management interface displays.
2. From the left-side option tree, select **Arrays > Firewall Policy**.
3. Add a new Access Rule.



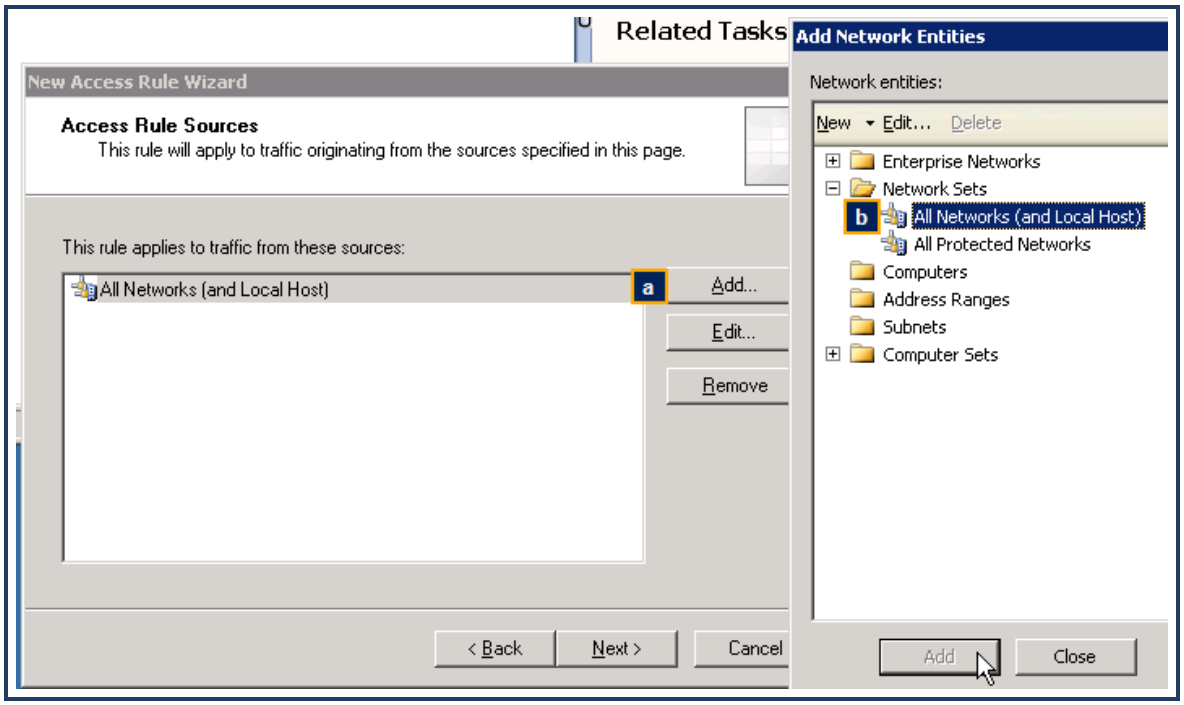
   a. In the **Task** tab, click **Create Access Rule**. The interface displays the New Access Rule Wizard.
   b. **Name** the access rule. For example, **Web Browsing**.
   c. Click **Next**.

4. On the **Rule Action** screen, select **Allow** and click **Next**.
5. Add the **HTTP** and **HTTPS** protocols.



   a. Click **Add**. The interface displays the Add Protocols dialog.
   b. Select **HTTP** and click **Add**.
   c. Repeat for **HTTPS**.
   d. **Close** the dialog.
   e. Click **Next**.

6. This rule applies to all networks and local hosts.



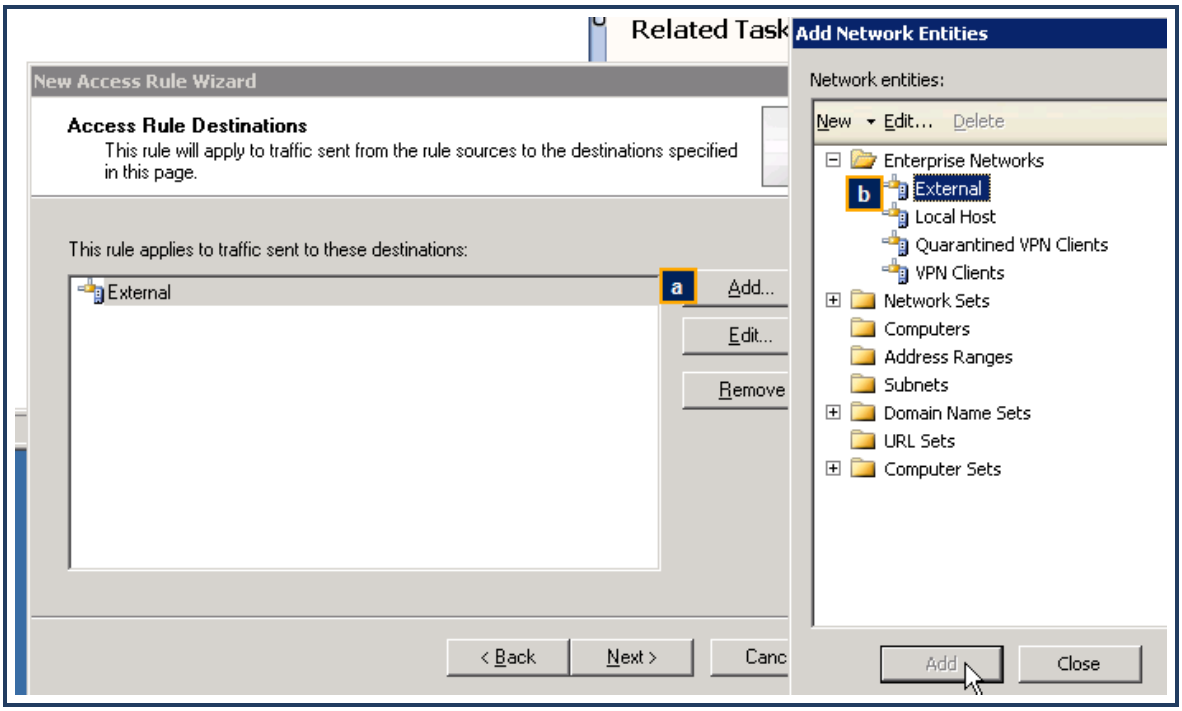
a. Click **Add**. The interface displays the Add Network Entities dialog.

b. Select **Network Sets > All Networks (and Local Host)** and click **Add**.

c. **Close** the dialog.

d. Click **Next**.

7. This rule applies to all external destinations.



a. Click **Add**. The interface displays the Add Network Entities dialog.

b. Select **Enterprise Networks > External** and click **Add**.

c. **Close** the dialog.

d. Click **Next**.

8. This rule applies to authenticated users.

a. The default is **All Users**. Select this object and click **Remove**.

b. Click **Add**. The interface displays the Add Users dialog.

c. Select **All Authenticated Users** and **Close** the dialog.

9. Review the rule summary and click **Finish**.

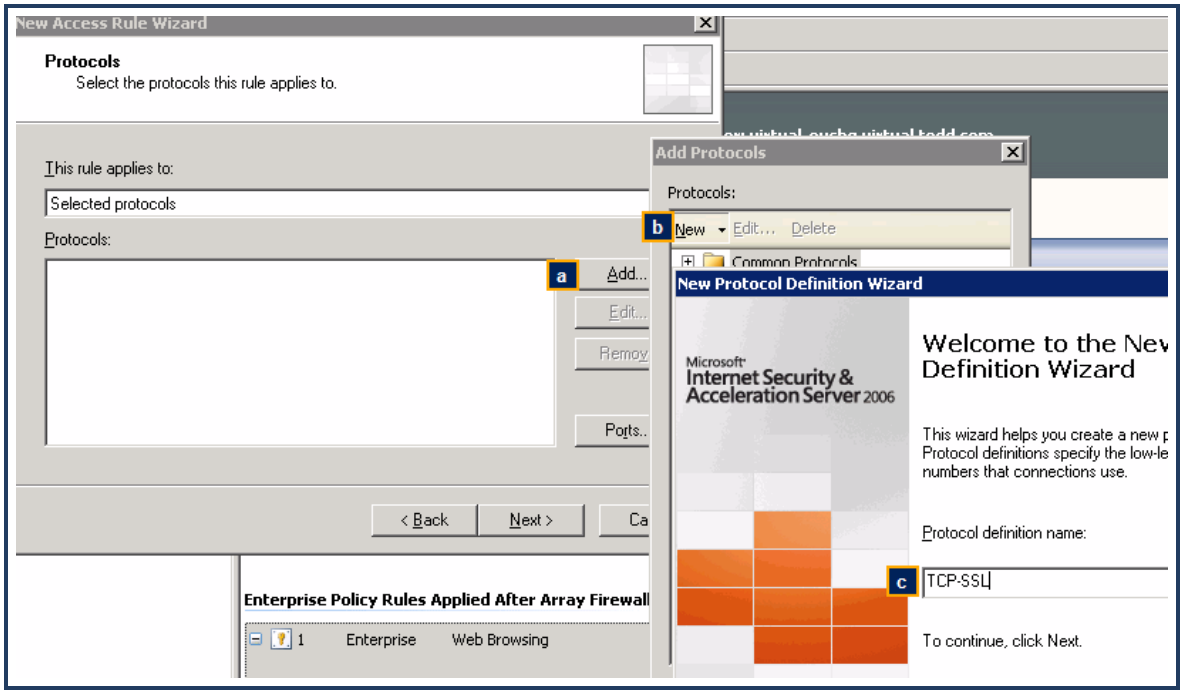
Step 2–Create another access rule for DNS for all users to both internal and external sources.

1. Click **Create Access Rule**. The interface displays the New Access Rule Wizard.

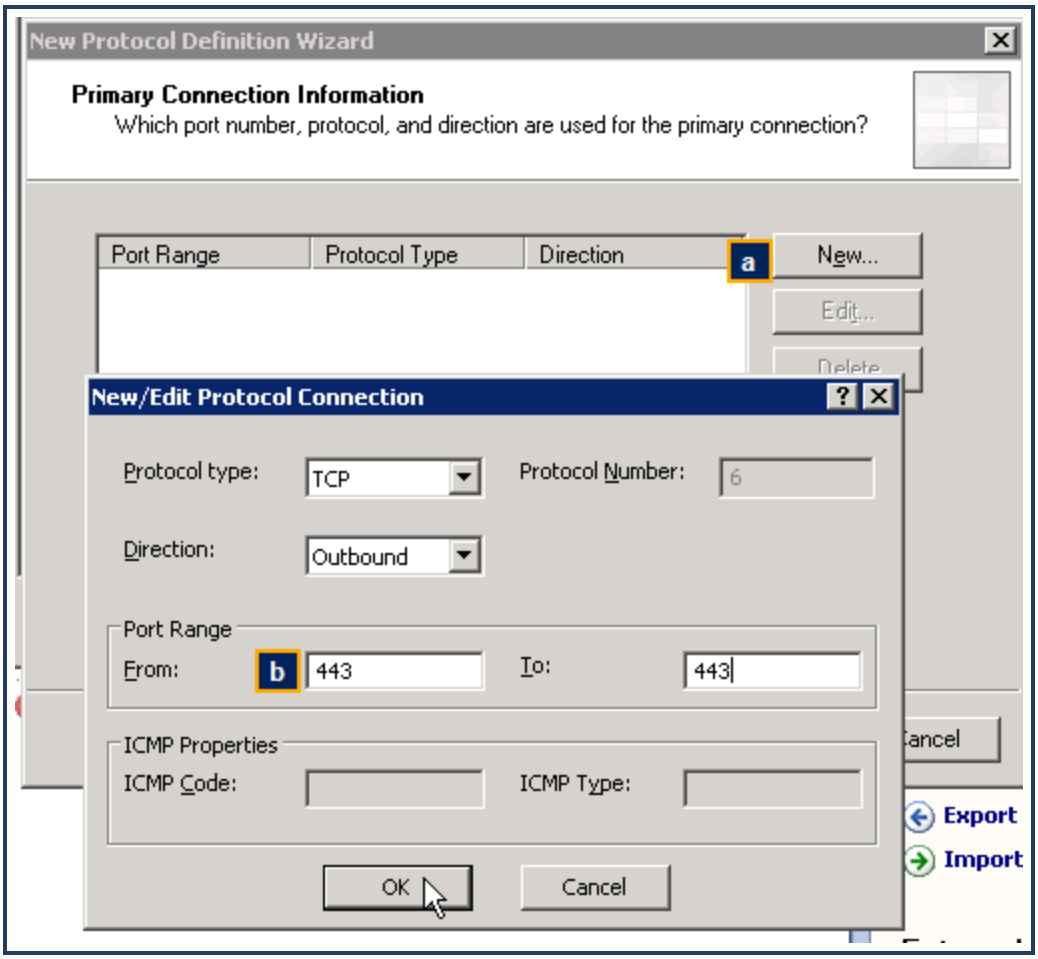
2. Follow the wizard:
    a. **Name**: **DNS Allow**.
    b. **Rule Action**: **Allow**.
    c. **Protocols**: **DNS**.
    d. **Source**: **Internal**.
    e. **Destination**: **Internal** and **External**.
    f. **User Sets**: **All Users** (the default).
    g. Click **Next** and **Finish** to add the rule.

Step 3–Create an access rule to allow for Auth Connector TCP connections on port 443 (SSL) .

1. Click **Create Access Rule**. The interface displays the New Access Rule Wizard.
2. **Name** the rule. For example, **AuthConnector-SSL**. Click **Next**.
3. **Rule Action**: select **Allow**.
4. You must add the SSL protocol with the 443 port.



    a. Select **Add > Protocol**. The interface displays the Add Protocols dialog.
    b. **Name** the new protocol. For example, **TCP-SSL**.
    c. Click **Next**.
5. Add the 443 port.



a. Click **New**. The interface displays the New/Edit Protocol Connection dialog.

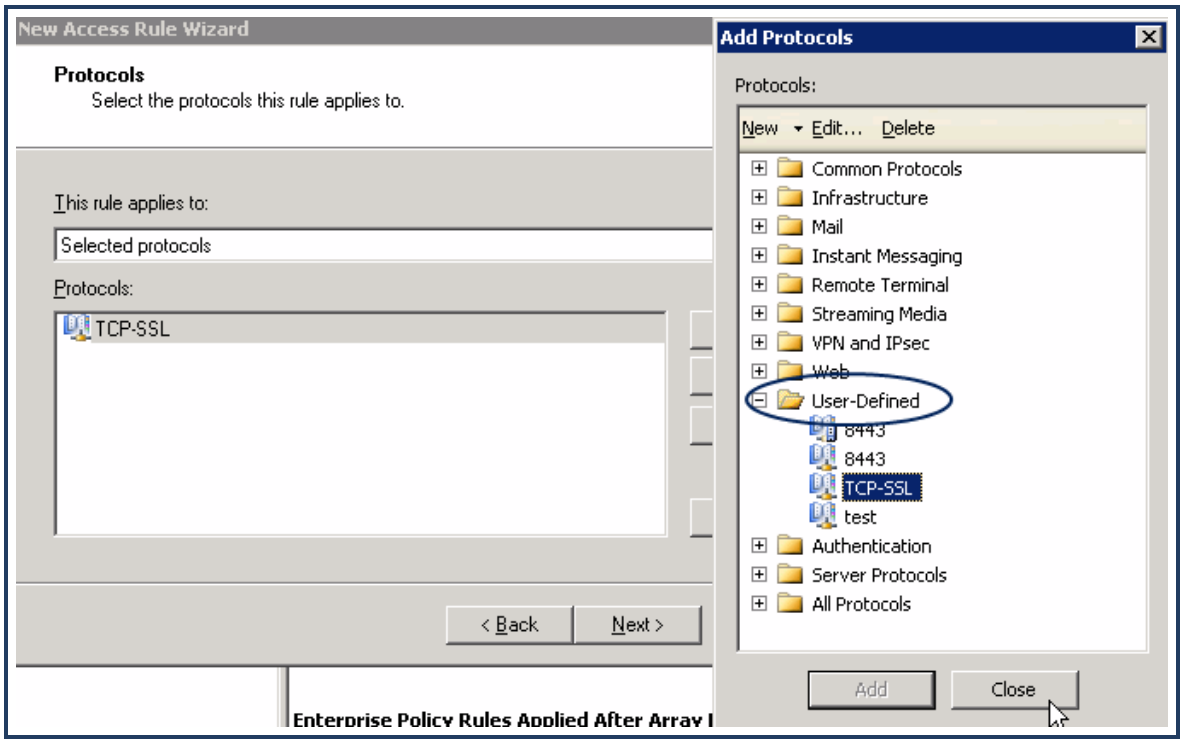
b. **Port Range**: enter **443** in both the **From** and **To** fields.

c. Click **OK**.

d. **Secondary Connections**: **No**.

e. Click **Finish**.

f. Add the protocol.

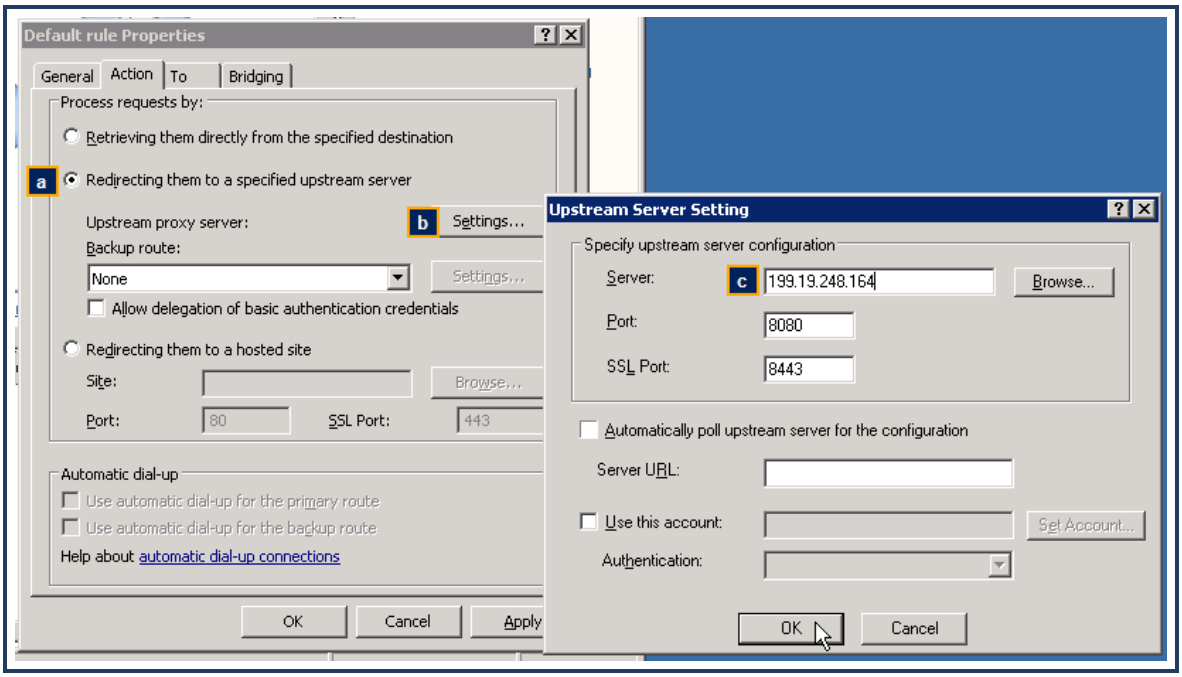


The new object is in the **User-Defined** folder of the Add Protocols dialog. **Add** it and click **Close**.

6. Complete the rule wizard:
    a. **Source**: **Internal**.
    b. **Destination**: **External**.
    c. **User Sets**: **All Users**.
    d. Click **Finish** to complete the rule.

Step 4—Create a Network/Web Chaining rule that sends Web traffic to the Web Security Service.

1. Modify the existing default Web Chaining rule:
    a. From the left-side option tree, select **Arrays > Configuration > Networks**.
    b. Click the **Web Chaining** tab.
    c. Double-click the default **Last Default Rule**. The interface displays the Default Rule Properties dialog.
2. Add the Web Security Service IP address for your region.



a. Select the **Redirecting them to a specified upstream server** option.

b. Click **Settings**. The interface displays the Upstream Server Setting dialog.

c. Enter the **Server** address, which is the Web Security Service IP address for your region. Refer to your planning sheet.

d. Click **OK** in each dialog to add the rule.

3. If your region requires a second Web Security Service IP address, repeat **Step 4** and add it.

Step 5-Verify that the Microsoft Firewall service is running.

1. In Windows, select **Start > Run**. The interface displays the Run dialog.
2. Enter **services.msc** and click **OK**.
3. Scroll down to the **Microsoft** services and verify that the **Status** column **for Microsoft Firewall** displays **Started**.

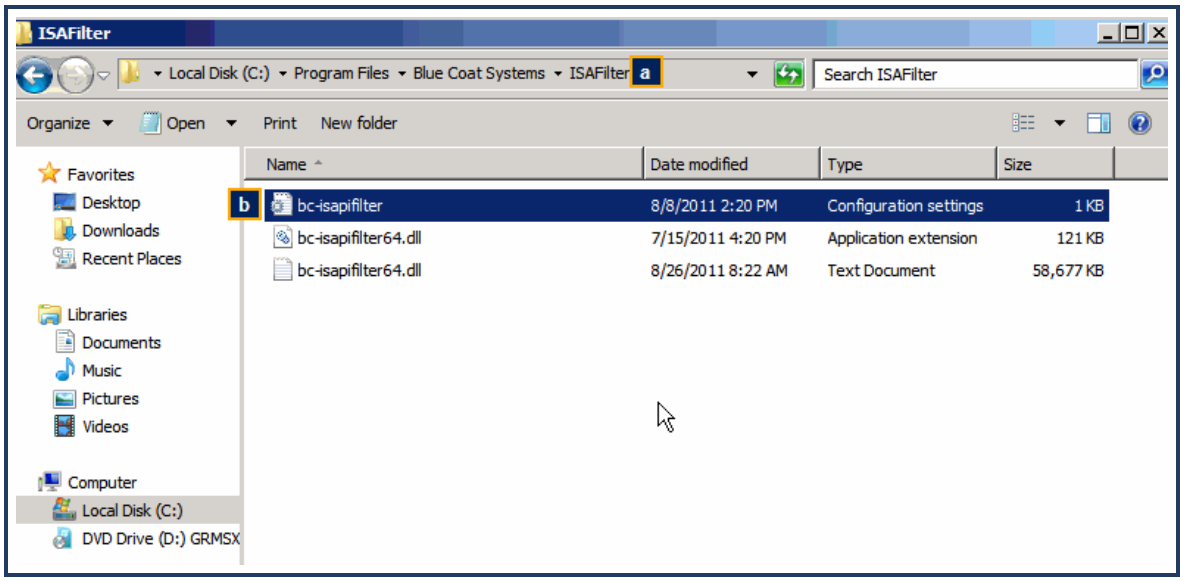
If it is not, right-click the line and select **Start**.

Step 6-Add AD groups of interest to the bc-isapifilter.ini file.

To forward credentials from the Active Directory to the Web Security Service, you must add those groups to the bc-

`isapifilter.ini` file. Symantec recommends adding all groups of interest. If a group is not added, the Web Security Service still generates the Web traffic from those clients; however, the user names are not available for policy.

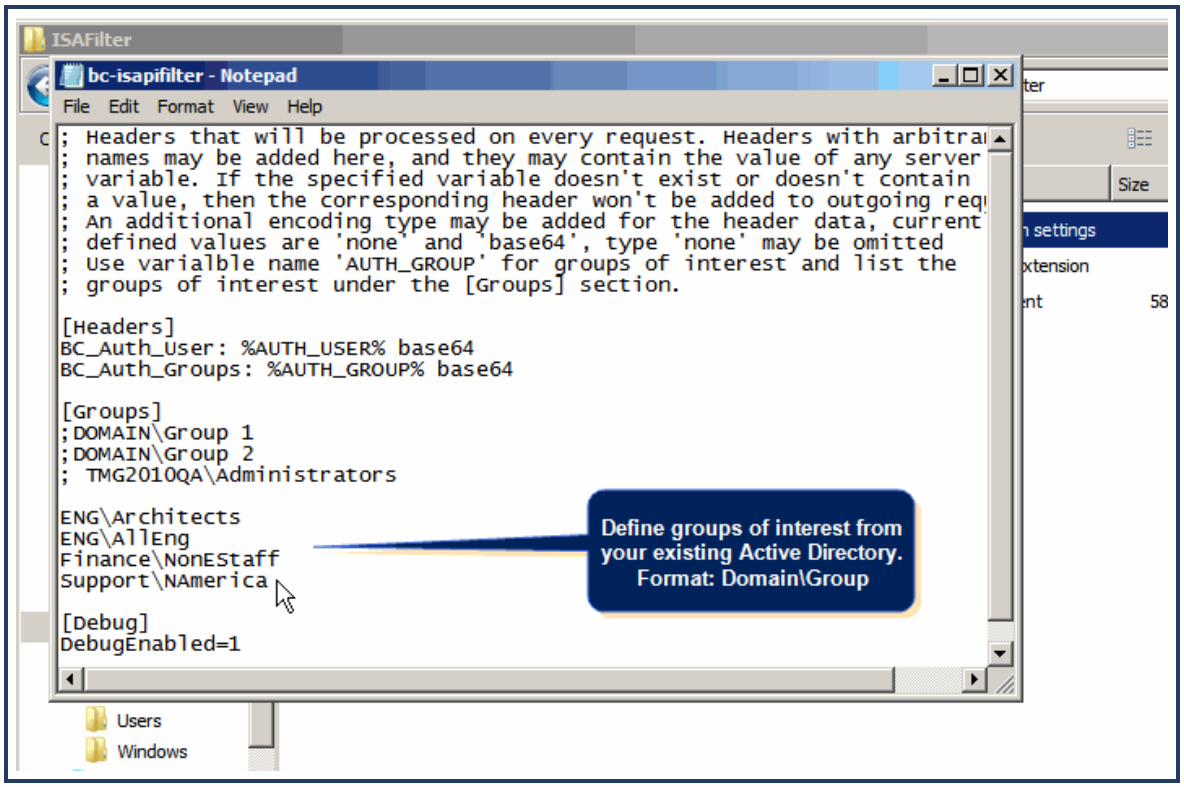
1. In Windows Explorer, navigate to where the **bc-isapifilter.ini** files resides.



   a. By default, the location is **C:/Program Files/Blue Coat Systems/ISAFilter**.

   b. Double-click the **bc-isapifilter text** file (not the **.dll** file).

2. Add the groups of interest.



The format for each group of interest is: ***Domain\Group_Name***. Ensure that they precisely match the Active Directory entries.

Paste or define groups of interest in a separate file, validate them, and paste them into this file.

3. Save and close the file.

Verify Required Open Ports

Configure the gateway firewall device to allow traffic from the gateway ProxySG on ports `8080` and `8443`.

Next Step

- "Add a Proxy Forwarding Location" on page 15.

Forward From Microsoft TMG to the Web Security Service

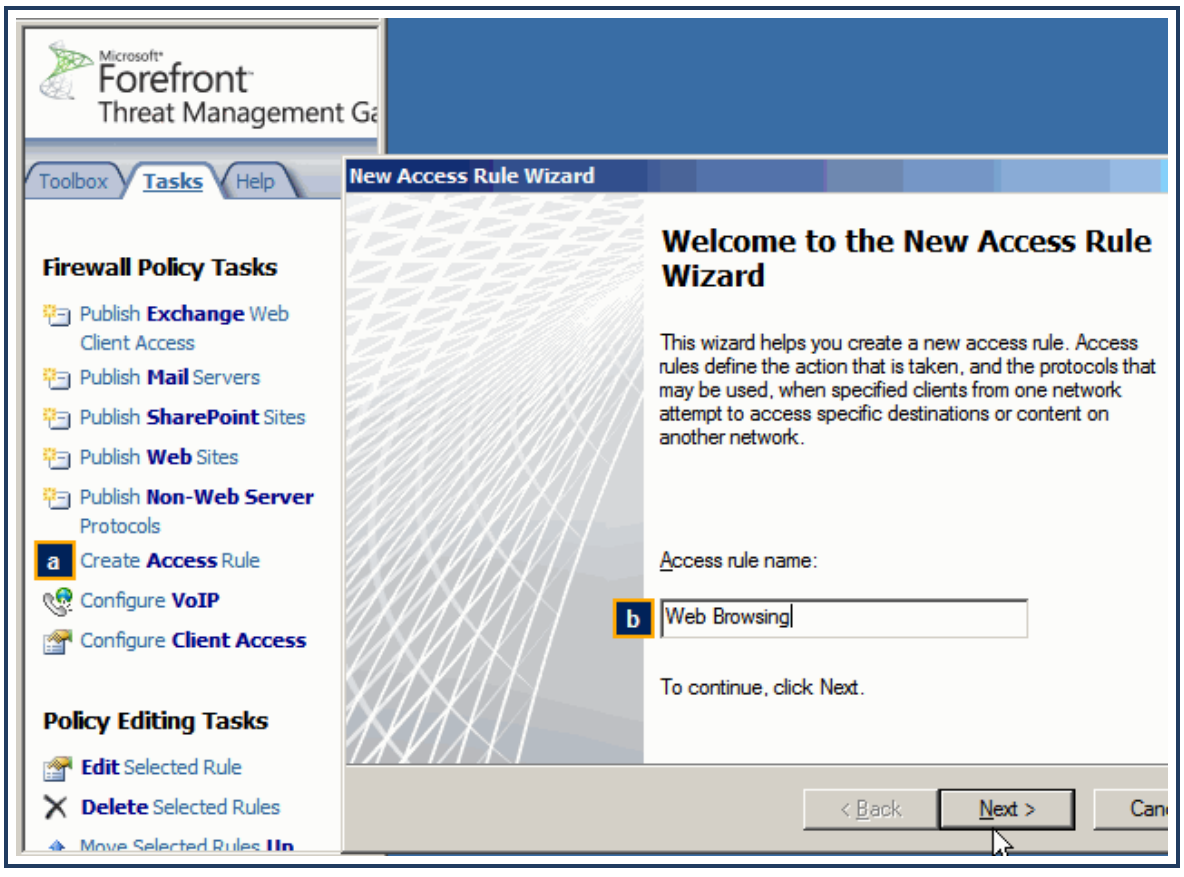
Define policy on the Microsoft TMG server to forward web requests plus user identification information to the Symantec Web Security Service.

Prerequisites

- The TMG server must be running Windows 2008 Server–64-bit.
- This procedure assumes that the server is already configured and operating.
- Verify existence of authentication filter. An authentication filter that can perform the authentication to the users workstation must be configured. This is usually a Microsoft Web filter and is usually already installed by default. Look in **System > Web Filters**. If it is not, work with your Microsoft account.

Step 1–Create a Firewall Policy/Access Rule for Web traffic (HTTP and HTTPS).

1. If the default location was set during the ISA server installation, select **Start > All Programs > Microsoft Forefront TMG> Forefront TMG Management**. The device displays the server management interface.
2. From the left-side option tree, select **Forefront TMG> Firewall Policy**.
3. Add a new Access Rule.

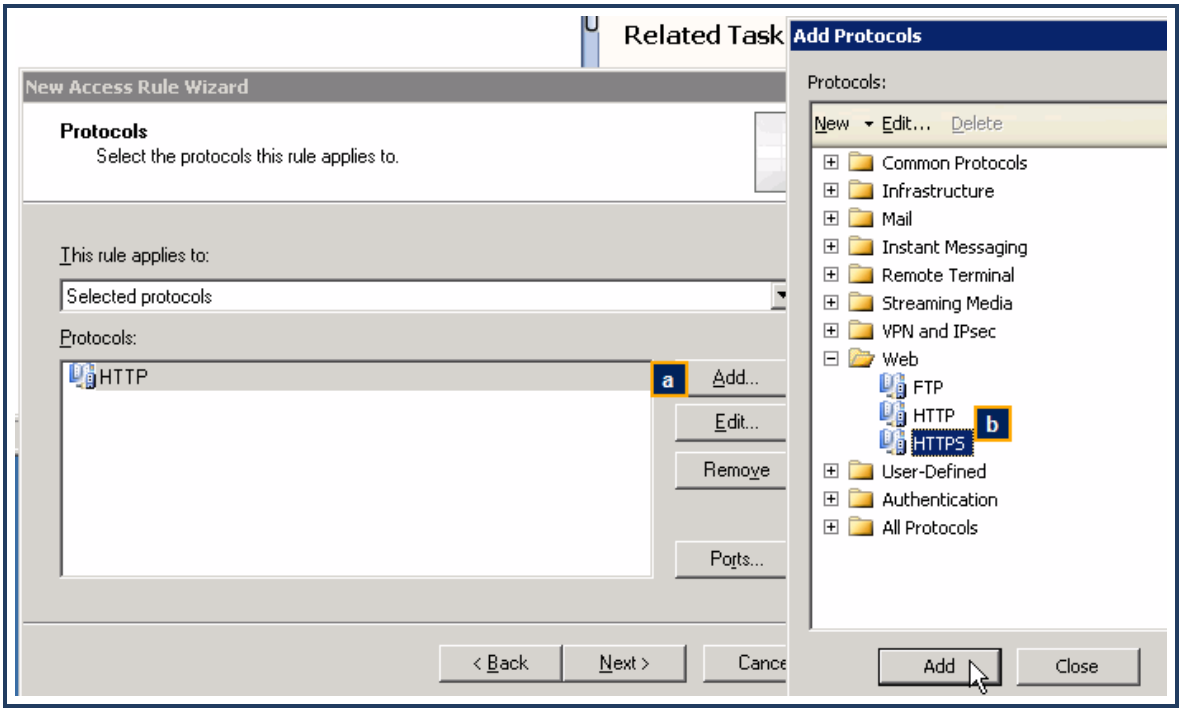


   a. In the **Task** tab, click **Create Access Rule**. The interface displays the New Access Rule Wizard.

   b. **Name** the access rule. For example, **Web Browsing**.

c. Click **Next**.

4. On the **Rule Action** screen, select **Allow** and click **Next**.
5. Add the HTTP and HTTPS protocols.



a. Click **Add**. The interface displays the Add Protocols dialog.

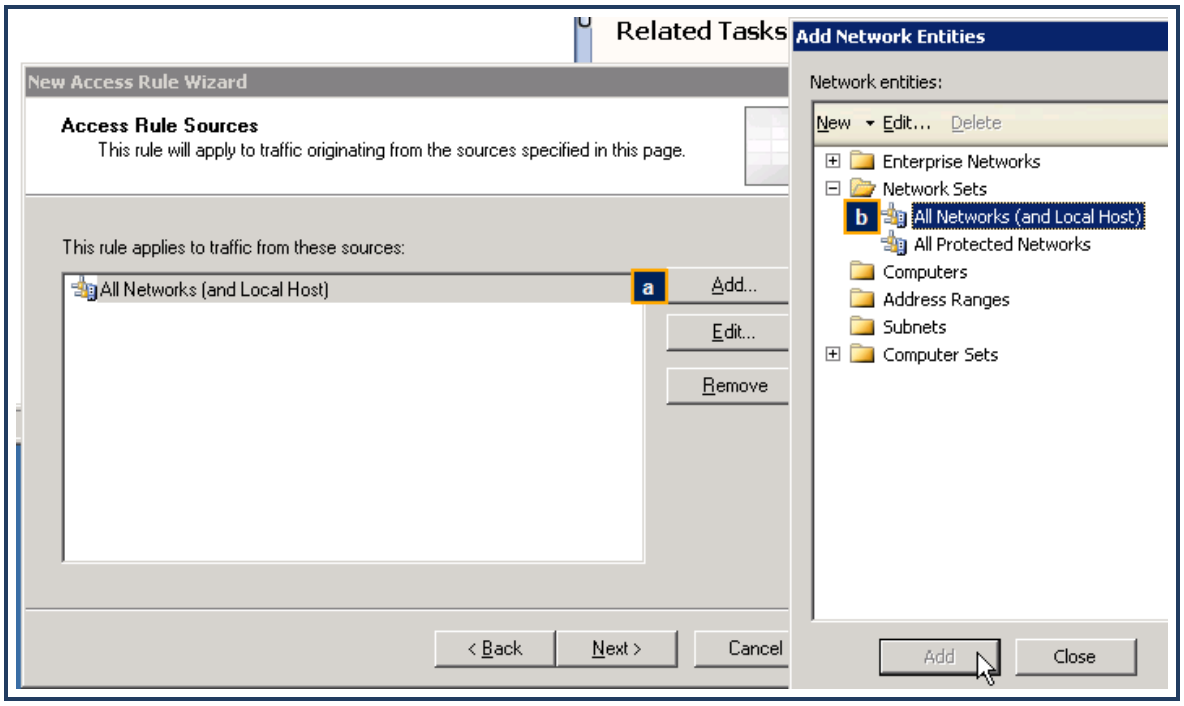
b. Select **HTTP** and click **Add**.

c. Repeat for **HTTPS**.

d. **Close** the dialog.

e. Click **Next**.

6. Select **Do not enable malware inspection for this rule** and click **Next**.
7. This rule applies to all networks and local hosts.



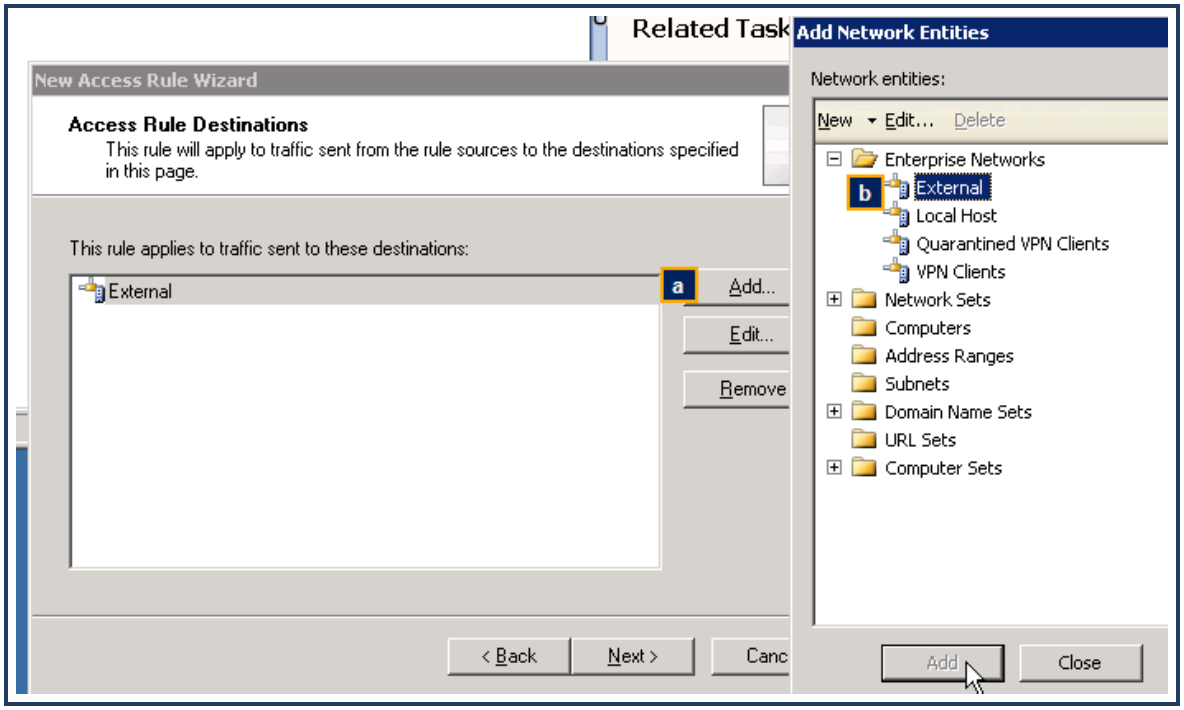
a. Click **Add**. The interface displays the Add Network Entities dialog.

b. Select **Network Sets > All Networks (and Local Host)** and click **Add**.

c. **Close** the dialog.

d. Click **Next**.

8. This rule applies to all external destinations.



a. Click **Add**. The interface displays the Add Network Entities dialog.

b. Select **Enterprise Networks > External** and click **Add**.

c. **Close** the dialog.

d. Click **Next**.

9. This rule applies to authenticated users.

a. The default is **All Users**. Select this object and click **Remove**.

b. Click **Add**. The interface displays the Add Users dialog.

c. Select **All Authenticated Users** and **Close** the dialog.

10. Review the rule summary and click **Finish**.

Step 2–Create another access rule for DNS for all users to both internal and external sources.

1. Click **Create Access Rule**. The interface displays the New Access Rule Wizard.
2. Follow the wizard:

a. **Name**: **DNS Allow**.

b. **Rule Action**: **Allow**.

c. **Protocols**: **DNS**.

d. **Source**: **Internal**.

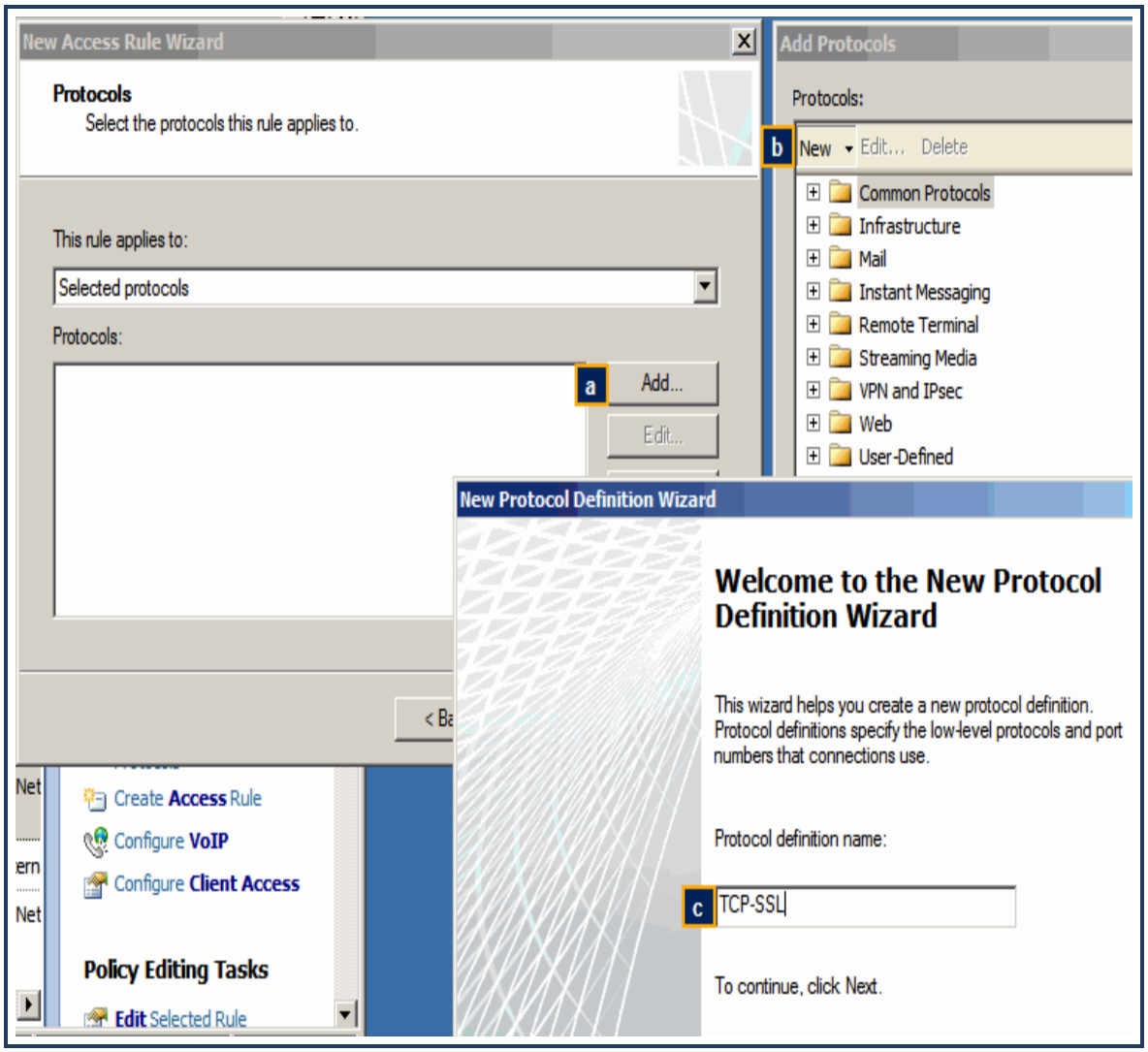
e. **Destination**: **Internal** and **External**.

f. **User Sets**: **All Users** (the default).

g. Click **Next** and **Finish** to add the rule.

Step 3–Create an access rule to allow for Auth Connector TCP connections on port 443 (SSL).

1. Click **Create Access Rule**. The interface displays the New Access Rule Wizard.
2. **Name** the rule. For example, **AuthConnector-SSL**. Click **Next**.
3. **Rule Action**: select **Allow**.
4. You must create the SSL protocol with the 443 port.

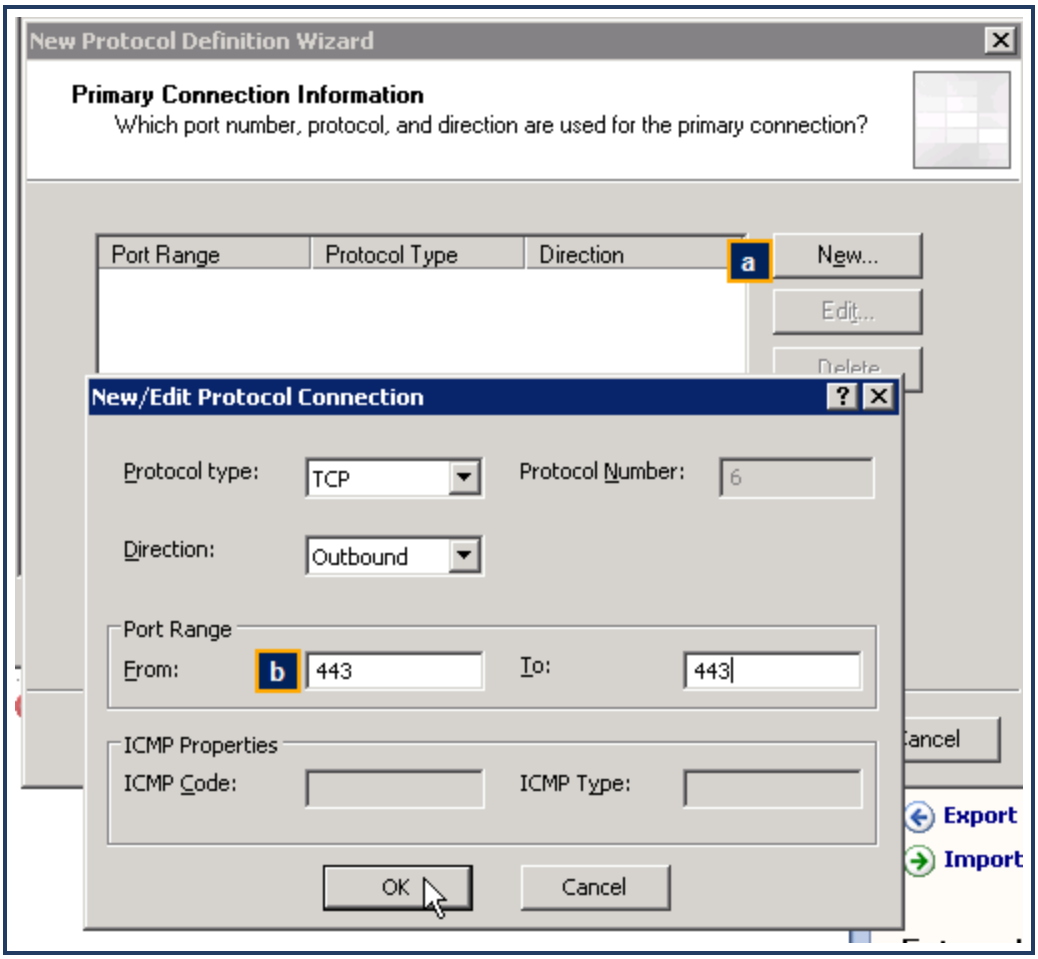


a. Click **Add > Protocol**. The interface displays the Add Protocols dialog.

b. **Name** the new protocol. For example, **TCP-SSL**.

c. Click **Next**.

5. Add the 443 port.



a. Click **New**. The interface displays the New/Edit Protocol Connection dialog.

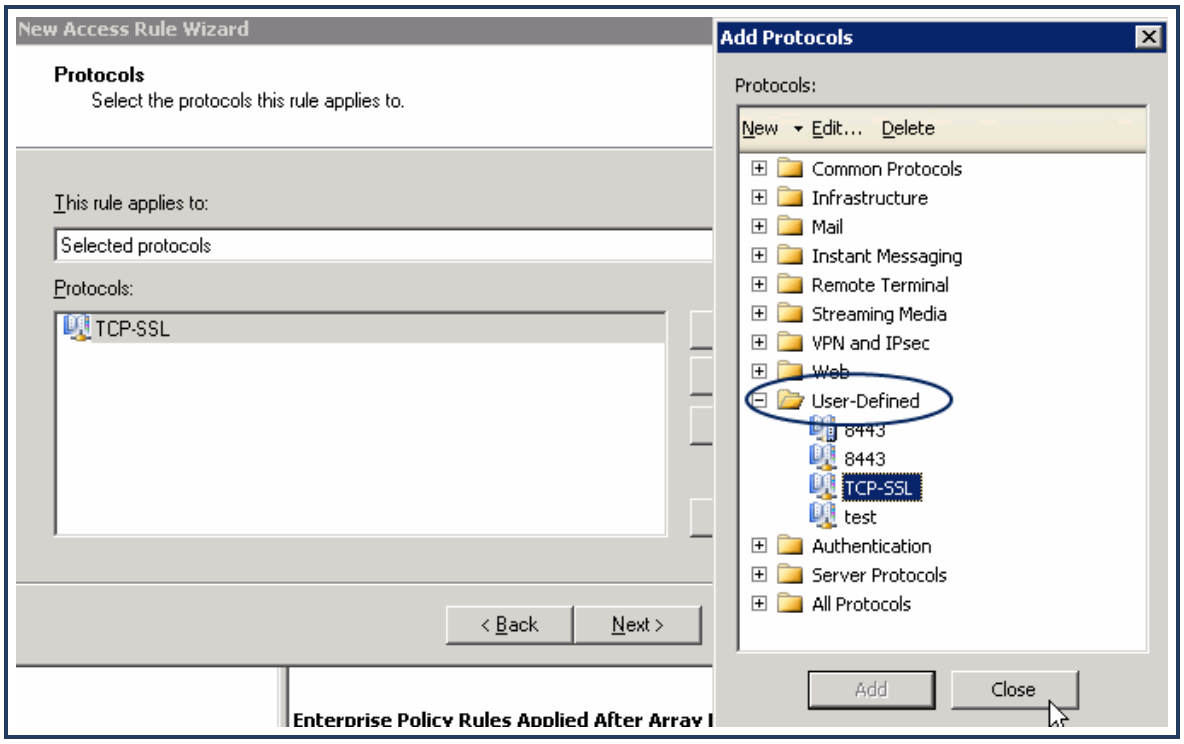
b. **Port Range**: enter **443** in both the **From** and **To** fields.

c. Click **OK**.

d. **Secondary Connections**: **No**.

e. Click **Finish**.

f. Add the protocol.

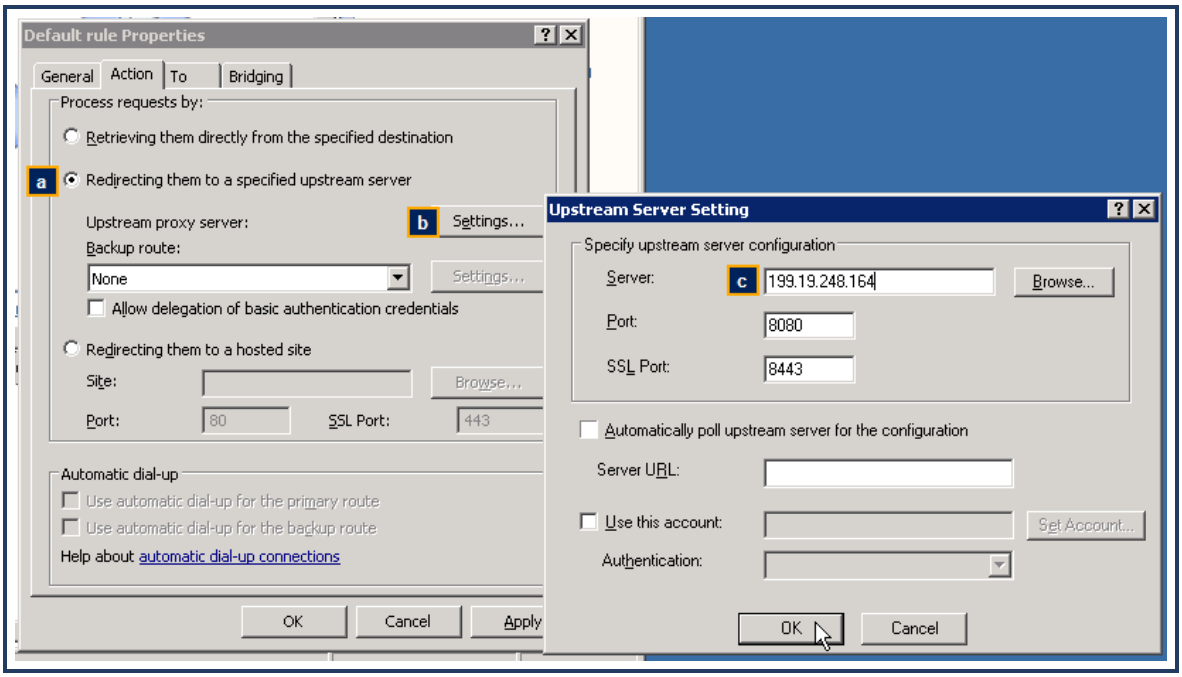


The new object is in the **User-Defined** folder of the Add Protocols dialog. **Add** it and click **Close**.

6. Complete the rule wizard:
    a. **Source**: **Internal**.
    b. **Destination**: **External**.
    c. **User Sets**: **All Users**.
    d. Click **Finish** to complete the rule.

Step 4—Create a Network/Web Chaining rule that sends web traffic to the Web Security Service.

1. Modify the existing default Web Chaining rule:
    a. From the left-side option tree, select **Networking**.
    b. Click the **Web Chaining** link.
    c. Double-click the default **Last Default Rule**. The interface displays the Default Rule Properties dialog.
2. Add the Web Security Service IP address for your region.



a. Select the **Redirecting them to a specified upstream server** option.

b. Click **Settings**. The interface displays the Upstream Server Setting dialog.

c. Enter the **Server** address, which is the Web Security Service IP address for your region. Refer to your planning sheet .

d. Click **OK** in each dialog to add the rule.

3. If your region requires a second Web Security Service IP address, repeat **Step 4** and add it.

Step 5-Verify that the Microsoft Firewall service is running.

1. In Windows, select **Start > Run**. The interface displays the Run dialog.
2. Enter **services.msc** and click **OK**.
3. Scroll down to the **Microsoft** services and verify that the **Status** column **for Microsoft Firewall** displays **Started**.

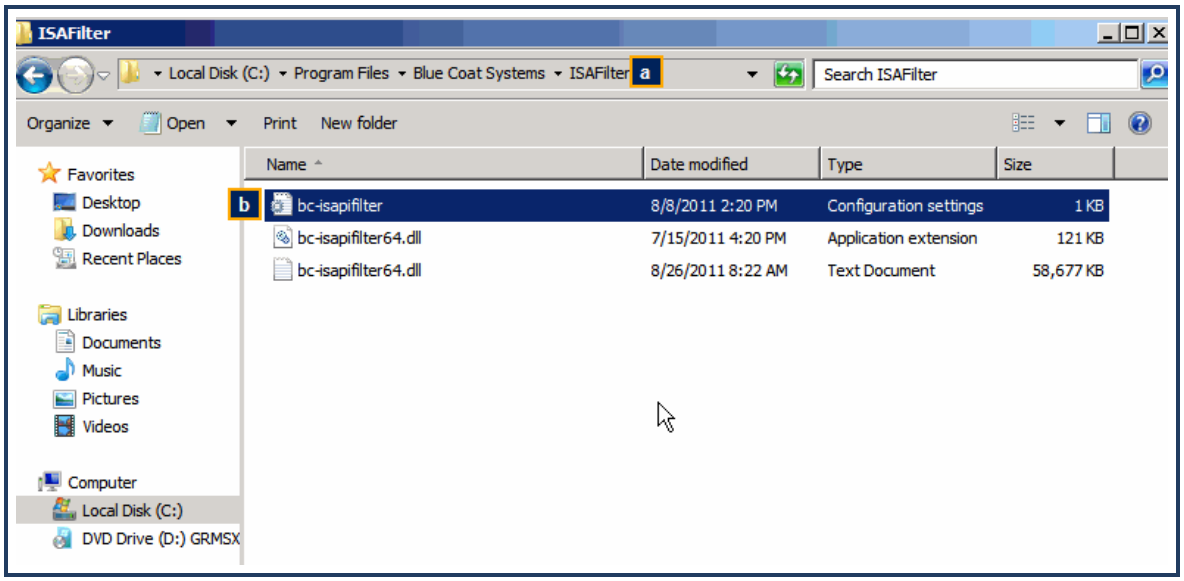
If it is not, right-click the line and select **Start**.

Step 6-Add AD groups of interest to the bc-isapifilter.ini file.

To forward credentials from the Active Directory to the Web Security Service, you must add those groups to the bc-

`isapifilter.ini` file. Symantec recommends adding all groups of interest. If a group is not added, the Web Security Service still generates the web traffic from those clients; however, the user names are not available for policy.

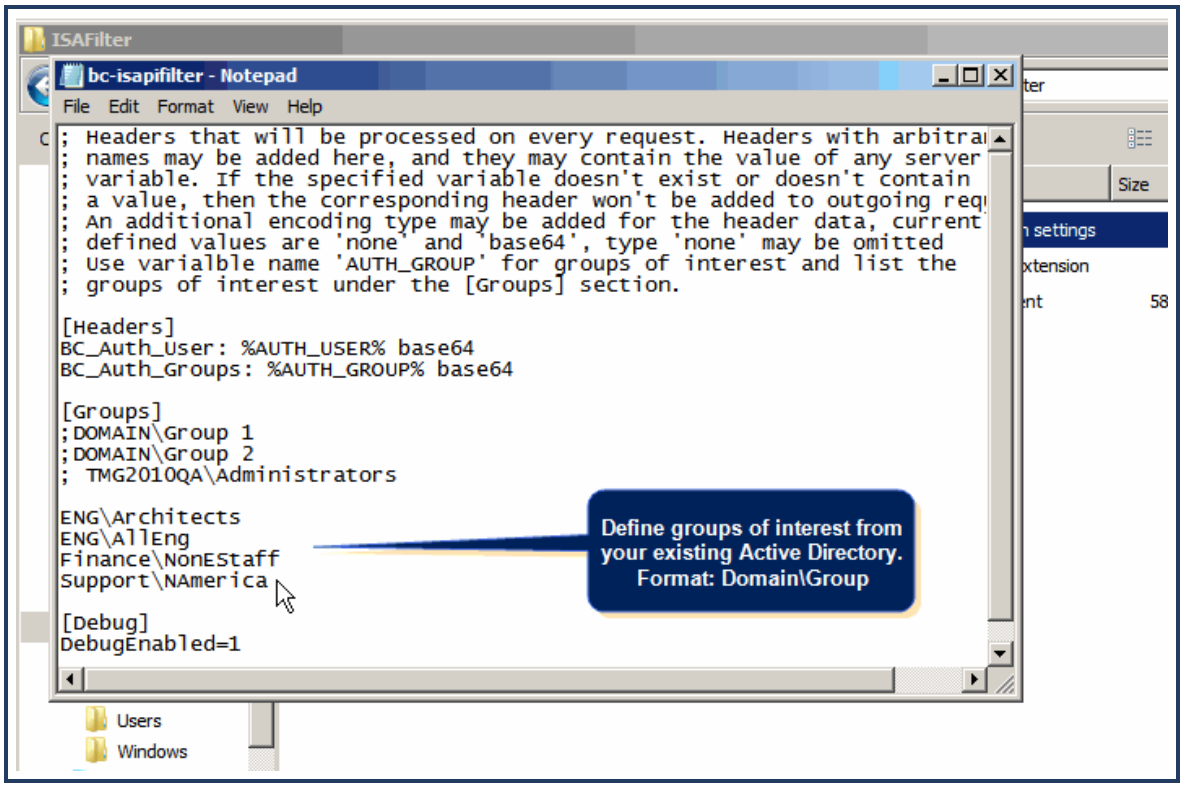
1. In Windows Explorer, navigate to where the **bc-isapifilter.ini** files reside.



   a. By default, the location is **C:/Program Files/Blue Coat Systems/ISAFilter**.

   b. Double-click the **bc-isapifilter text** file (not the **.dll** file).

2. Add the groups of interest.



The format for each group of interest is: ***Domain\Group_Name***. Ensure that they precisely match the Active Directory entries.

Paste or define groups of interest in a separate file, validate them, and paste them into this file.

3. Save and close the file.

Verify Required Open Ports

Configure the gateway firewall device to allow traffic from the gateway ProxySG on ports `8080` and `8443`.

Next Step

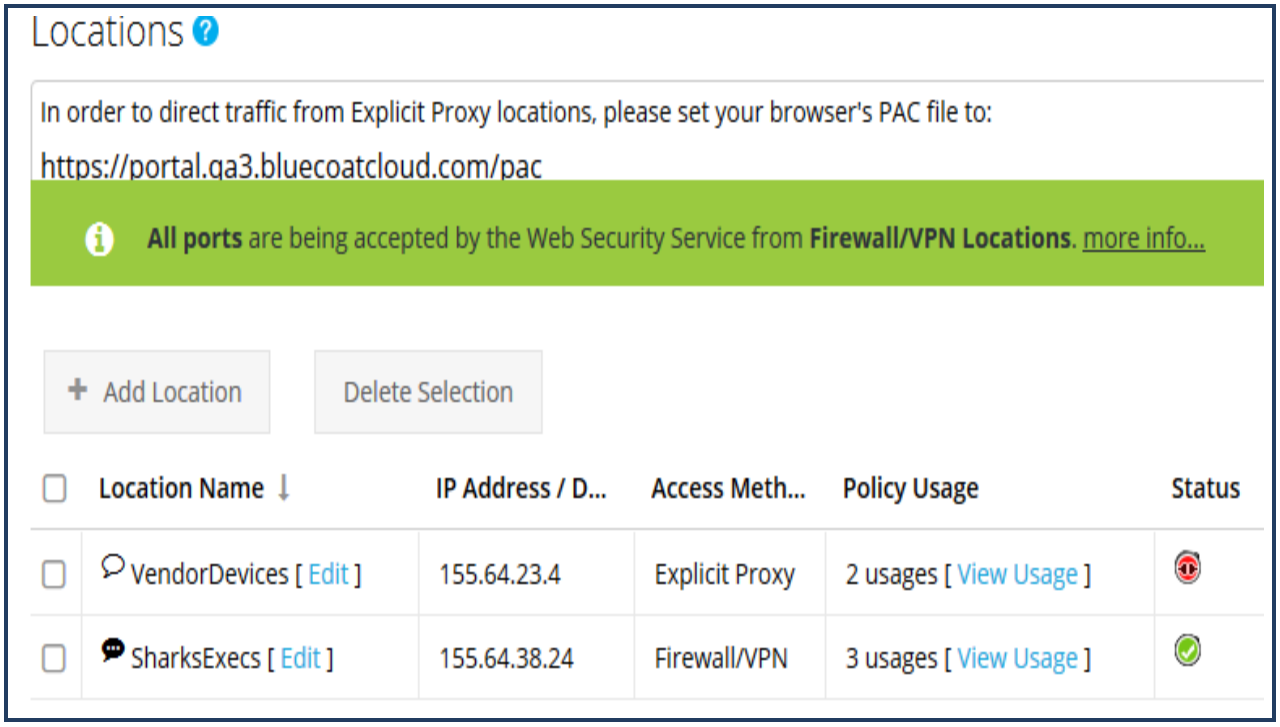
- "Add a Proxy Forwarding Location" on page 15.

Verify Service Connectivity to Locations

After configuring access to the SymantecWeb Security Service, verify that the service is receiving and processing content requests.

All Locations

1. Click the **Service** link (upper-right corner).
2. Select **Network > Locations**.
3. Verify the status of each location.



Various icons represent the connection status.

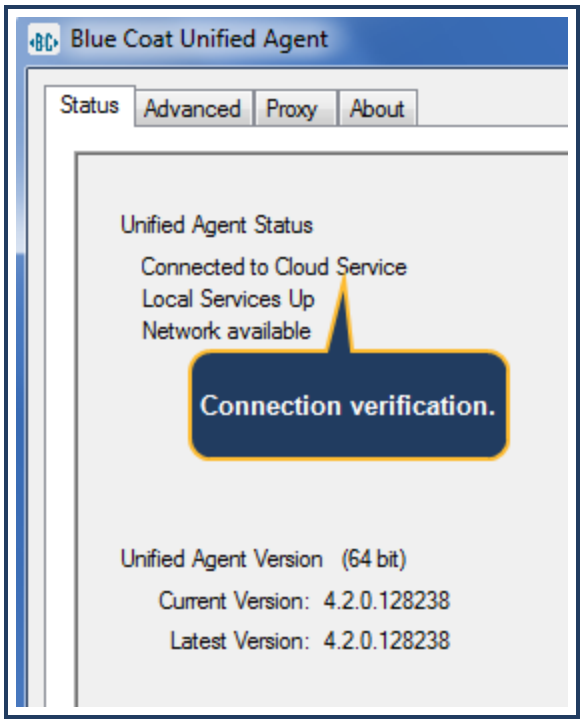
Icon	Connection Status Description
	The Web Security Service recognizes the location and accepts web traffic.
	A location has been configured, but the Web Security Service cannot connect. Verify that the web gateway device is properly configured to route traffic.

Icon	Connection Status Description
	A previously successful web gateway to Web Security Service configuration is currently not connected. ■ Firewall/VPN ■■ Verify your firewall's public gateway address. ■■ Verify the Preshared Key (PSK) in the portal matches that of your firewall configuration. ■■ Verify that the server authentication mode is set to PSK. ■ Explicit Proxy ■■ Verify the PAC file installation and deployment. ■■ Verify that your network allows outbound requests on port `8080`. ■■ Do not attempt to use Explicit Proxy in conjunction with the Unified Agent- the client will detect that a proxy is in effect, assume a man-in-the-middle attack, and fail (open or closed depending on the settings). ■ Proxy Forwarding–Verify the gateway address in the forwarding host is correct. ■ Remote Users–Verify the Unified Agent/Client Connector installation. See the section below for more information.

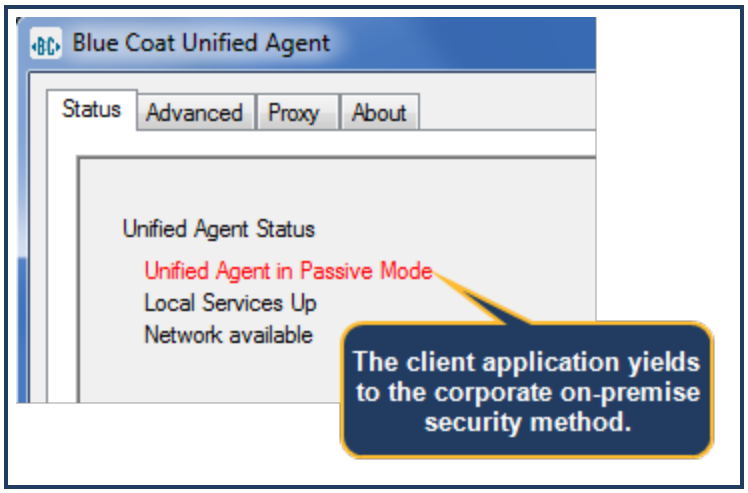
Additional Step For Remote Users

To further verify that Unified Agent running on remote clients is communicating with the Web Security Service, click (or double-click) the application icon in the menu bar and click **Status**.

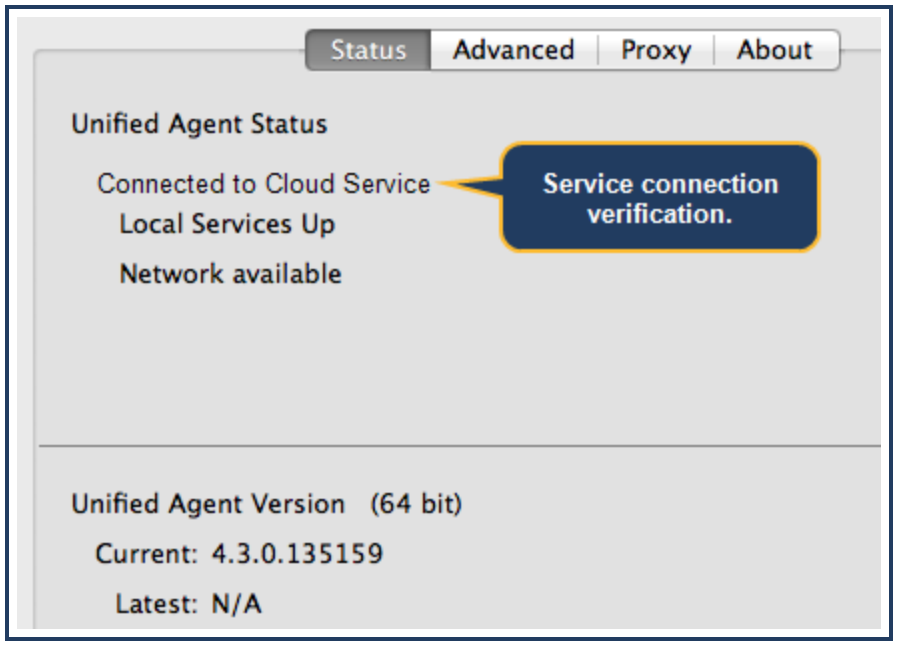
Windows



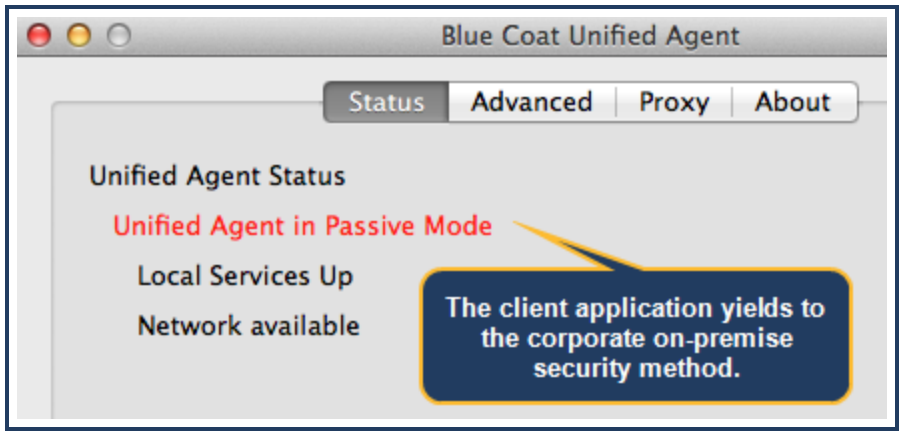
If the system detects a corporate network that provides web access and security, the Unified Agent enters into passive mode.



Mac



If the system detects a corporate network that provides web access and security, the Unified Agent enters into passive mode.

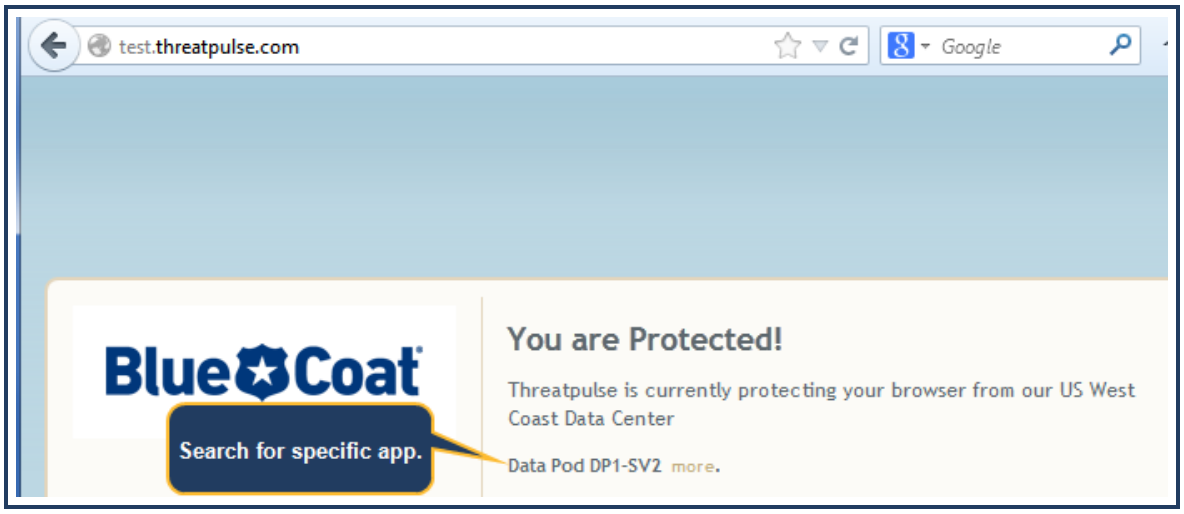


Verify Client Protection

From a client system that has web access (or the specific test client if so configured), browse to the following site:

`test.threatpulse.com`

The test is successful if you see the following webpage.



Next Steps

- Remote Users and Explicit Proxy Access Method–initial Configuration is complete.

  Symantec also recommends adding private IP subnets to the IP bypass list to prevent internal traffic from routing to the Web Security Service service. For more information, see the **How Do I? > Prevent IP/Subnet From Routing to the Service** topic in Symantec Web Security Service WebGuide: Solutions

References

This section provides proxy forwarding reference material.

- Reference: Proxy Forwarding Policy
- Reference: Additional Authentication CPL for SGOS MACH 5 Proxy Forwarding

Reference: Authentication Modes

Before the ProxySG appliance can authenticate intercepted connections, you must create the authentication policy that tells the appliance when and how to authenticate client requests. One of the policy settings you must define is the authentication mode. The authentication mode specifies the type of authentication challenge to use to obtain the client credentials and the type of surrogate credential to use, if any. You define the authentication mode when you create your policy. When creating policy using Content Policy Language (CPL), you set the authentication mode using the `authenticate.mode()` statement. When creating policy using the Visual Policy Manager (VPM), you set the authentication mode when creating the **Authenticate** object.

The appliance automatically overrides the configured mode if the client cannot support the requested mode. For example, if you set the authentication mode to `Origin-Cookie-Redirect`, but the client does not support cookies, the appliance automatically downgrades to `Origin-IP-Redirect` mode.

If you do not set an authentication mode, the appliance uses the default mode, `Auto`. In `Auto` mode the appliance automatically determines which mode to use. However, in most cases it is best to explicitly set the mode.

The following table lists the authentication modes and when to use them.

Authentication Mode	Challenge Type	Surrogate Credential	Use With
Proxy	The ProxySG appliance issues a proxy challenge (HTTP 407) for every new connection.	None	Explicit proxy
Proxy IP	The ProxySG appliance issues a proxy challenge (HTTP 407) for the first connection request from an unauthenticated client. It only reissues the challenge when the IP surrogate expires.	IP address	Explicit proxy, Windows SSO, or Novell SSO
Origin	The ProxySG appliance issues an OCS-style challenge (HTTP 401) for every new connection.	None	Reverse proxy

Authentication Mode	Challenge Type	Surrogate Credential	Use With
Origin IP	The ProxySG appliance issues an OCS-style challenge (HTTP 401) for the first connection request from an unauthenticated client. It only reissues the challenge when the IP surrogate expires.	IP address	Reverse proxy
Origin IP Redirect	Redirects the client to the virtual URL and then issues an OCS-style challenge (HTTP 401). It only reissues the challenge when the client's IP surrogate expires.	IP address	Transparent proxy
Origin Cookie	The ProxySG appliance issues an OCS-style challenge (HTTP 401) for the first connection request for each new OCS domain per client. It only reissues the challenge when the client's cookie surrogate for the domain expires.	cookie	Reverse proxy

Authentication Mode	Challenge Type	Surrogate Credential	Use With
Origin Cookie Redirect	Redirects the client to the virtual URL and then issues an OCS-style challenge (HTTP 401) for the first connection request for each new OCS domain per client. It only reissues the challenge when the client's cookie surrogate for the domain expires.	cookie	Transparent proxy
Form IP	The ProxySG appliance returns a form to the client to request credentials. It only reissues the challenge form when the client's IP surrogate expires.	IP address	Reverse proxy
Form IP Redirect	Redirects the client to the virtual URL and then returns a form to the client to request credentials. It only reissues the challenge when the client's IP surrogate expires.	IP address	Transparent proxy

Authentication Mode	Challenge Type	Surrogate Credential	Use With
Form Cookie	The ProxySG appliance returns a form to the client to request credentials for the first connection for each new OCS domain requested. After the client successfully authenticates to a domain, the ProxySG appliance will only present the form when the client's cookie surrogate for that domain expires.	Cookie	Reverse proxy
Form Cookie Redirect	Redirects the client to the virtual URL and then returns a form to the client to request credentials for the first connection for each new OCS domain requested. After the client successfully authenticates to a domain, the ProxySG appliance will only present the form when the client's cookie surrogate for that domain expires.	Cookie	Transparent proxy

Reference: Proxy Forwarding Policy

The Symantec Web Security Service Proxy Forwarding Access Method requires policy that routes web traffic to service. Specifically, the policy achieves the following:

- To protect credential information in the headers, the policy forwards HTTP traffic over a secure service.
- The policy forwards HTTPS and SSL traffic over the standard proxy service.
- The policy ignores all other traffic.

The following is the Content Policy Language (CPL) template that Symantec recommends appending to the existing ProxySG appliance Local policy file.

Notes

- The lines that being with a semi-colon (;) are CPL comments that provide commentary regarding the purpose of each policy construct.
- The forwarding host names are examples; you must enter hosts that you defined in the Proxy Forwarding configuration topic.

```
;;; $module=proxy_forwarding.cpl; $version=1

;

;

; Template for the Blue Coat Web Security Service Proxy Forwarding access method

; Version Date: 20130423

;

; IMPORTANT: This template contains sample policy. You might need

; customize it for your location.

;

; The purpose of this policy is to decide what traffic is sent to
; the Blue Coat Web Security Service(the Cloud), and how that traffic
; gets forwarded.
; In most cases, it's easier to specify what not to route, such as:
;    - Internal traffic.
; - Blue Coat Web Security Service Service management portal traffic.
; While it is difficult to inadvertently lock yourself
; out of administrative access, you can safely bypass it.

;

; Because of the restrictions on the type of condition referenced from
; CPL layers, define the bypass list twice--once for use in
```

```
; <Proxy> and <Cache> layers and once for use in <Forward> layers.
; These conditions unavoidably identify the same traffic.

;

; SGOS 5.4 supports a configuration definition for the internal
; network that can be directly tested. Previous versions must test
; against the internal network addresses explicitly.

;

#if release.version=5.4..
define condition BC_Cloud_Proxy_Bypass_List
    url.host.is_private=yes ; internal traffic
    ; Add any other public IPs that are not to route to the Web Security Service
    url.domain=portal.threatpulse.com ; threatpulse portal
    url.domain=bluecoat.com ; style sheets
end

define condition BC_Cloud_Forward_Bypass_List
    server_url.host.is_private=yes ; internal traffic
    health_check=yes ; Normally, don't forward health checks
    ; And any other additions required to keep it in line
    ; with the above BC_Cloud_Proxy_Bypass_List
    server_url.domain=portal.threatpulse.com ; threatpulse portal

end

#endif

#if release.version=..5.3
define subnet BC_Internal_subnets
    0.0.0.0/8
    10.0.0.0/8
    127.0.0.0/8

    172.16.0.0/12
    169.254.0.0/16
    192.168.0.0/16
    224.0.0.0/3
    ; Add any other subnets that are treated as internal
end

define condition BC_Cloud_Proxy_Bypass_List
    ; internal traffic
    url.address=BC_Internal_subnets
    ; Add any other public IPs that are not to route to the Web Security Service.
    url.domain=portal.threatpulse.com ; threatpulse portal
end



define condition BC_Cloud_Forward_Bypass_List
    ; internal traffic
    server_url.address=BC_Internal_subnets
    ; Add any other entries required to keep it in line
```

```
    ; with the above BC_Cloud_Proxy_Bypass_List
    server_url.domain=portal.threatpulse.com ; threatpulse portal
end
#endif

; Upon user authentication,
; pass the user-name and groups to the Web Security Service.
;
<Proxy Cloud_Auth> condition=!BC_Cloud_Proxy_Bypass_List
    authenticated=yes action.Auth_Cloud(yes)

; User and Group information are passed to the Web Security Service in
; special headers added to the request.
;
define action Auth_Cloud
    set( request.x_header.BC_Auth_User, "$(user:encode_base64)" )
    set( request.x_header.BC_Auth_Groups, "$(groups:encode_base64)" )
end

; If you plan to use the the Web Security Service to enforce
; appropriate use policies (content filtering and application control),
; then you must either disable caching or ensure that you always
; verify access requests with the Web Security Service.
;
; Blue Coat recommends leaving caching on, and using always_verify().
;
<Cache Cloud_Verify_Cached_Authorization> condition=!BC_Cloud_Proxy_Bypass_List
    always_verify(yes) ; check for authorization

; In SGOS 6.1, has_client= is available in <Cache> layers,
; which provides the ability to mark the system (mostly refresh traffic) with
; a specific userID. This feature is not available in
; previous releases of SGOS (such as 5.x).
; This template marks the traffic with the userID "Refresh User"
; by setting the BC_Auth_User header to the base-64
; encoded version of that string.
;
#if release.version=6.1..
    <Cache Cloud_Tag_System_traffic> condition=!BC_Cloud_Proxy_Bypass_List
    ; it is a system request (mostly refresh?)
    has_client=false action.Cloud_Auth_Refresh_Traffic(yes)
    define action Cloud_Auth_Refresh_Traffic
    set( request.x_header.BC_Auth_User, "UmVmcmVzaCBVc2Vy" )
end
#endif

; Forward the desired traffic to the cloud.
; - Do not forward traffic on the bypass list.
; - Generally, do not forward health checks.
```

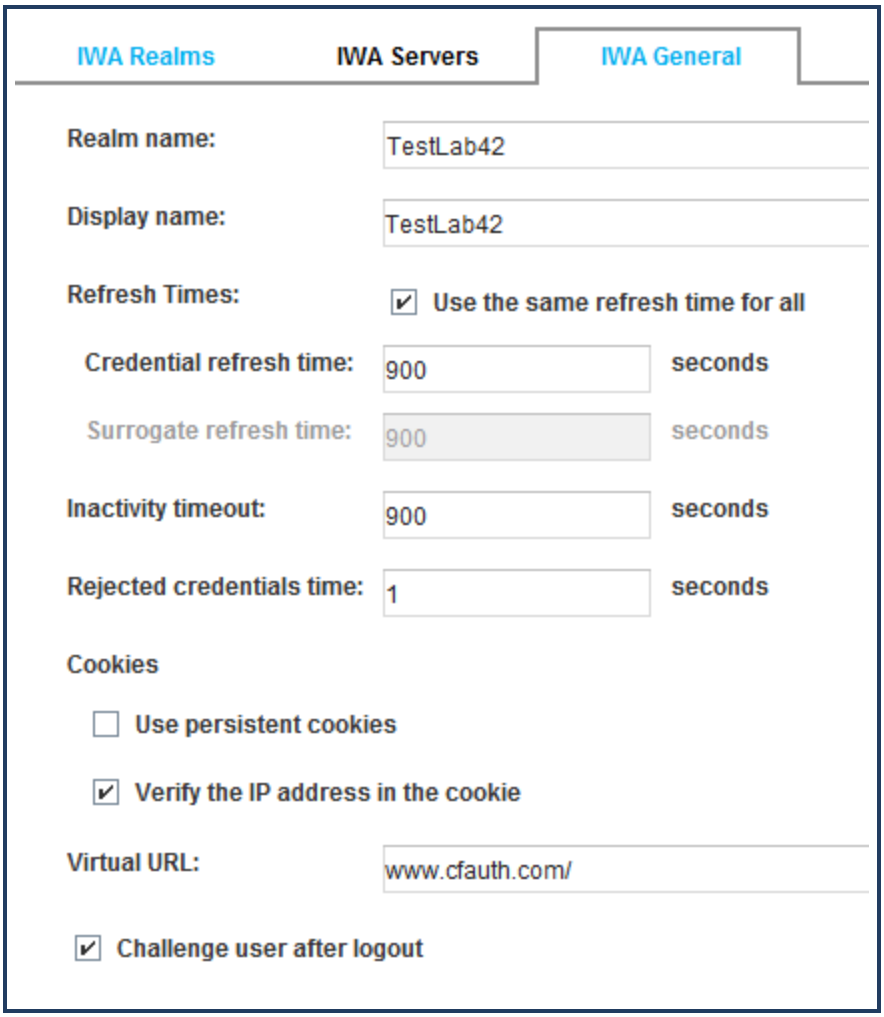
```
; - Because HTTP traffic has user and group information added, it is sent
; over a secure tunnel.
; - Unintercepted HTTPS traffic is forwarded directly (however, no user auth is avail-
able).
;
; In SGOS 6.4.x, forwarding can be based on the server_url.category
; and this provides an opportunity to separate unintercepted SSL from
; intercepted SSL, which can be authenticated to the cloud service.
;
#if release.version=6.4..
    define condition SSL_Unintercepted_category
      ; this is a typical unintercepted category list
      ; it should be modified to match your local interception policy
      ;
      server_url.category=(Brokerage/Trading, "Financial Services", Health)
      ;
      ; exempt this to get the style sheets for exception pages

      server_url.domain=portal.threatpulse.com
    end
    <Forward Cloud> condition=!BC_Cloud_Forward_Bypass_List
       [Rule] proxy.port=(443, 8080) url.scheme=https,ssl,tcp
         condition=SSL_Unintercepted_category forward(ThreatPulseHTTP8080) ; existing
         forward(ThreatPulseInterceptedHTTPS8084) ; new
       [Rule]
         url.scheme=http forward(ThreatPulseSecure8443)
#endif

#if release.version=..6.3
<Forward Cloud> condition=!BC_Cloud_Forward_Bypass_List
    proxy.port=(443, 8080) url.scheme=https,ssl,tcp forward(ThreatPulseHTTP8080)
    url.scheme=http forward(ThreatPulseSecure8443)
#endif

; For reporting purposes, forward the client IP addresses rather than the ProxySG
; appliance IP address.
;
<Proxy Forwarding_Client_IP>
    action.Forwarding_Client_IP(yes)

define action Forwarding_Client_IP
    set( request.header.Client-IP, "$(client.address)" )
end
```

The forwarding host names are examples; you must enter hosts that you defined in the Proxy Forwarding configuration topic.

Reference: Additional Authentication CPL for SGOS MACH 5 Proxy Forwarding

Configuring a Blue Coat ProxySG MACH 5 appliance to forward authenticated web requests through the Symantec Web Security Service requires creating an authentication realm configuring additional CPL added to the Local policy file.

1. Verify the ProxySG appliance is running the correct version of the Symantec Authentication and Authorization Agent (BCAAA).
2. Access the **Advanced Configuration** page in the Management Console.
3. Create an authentication realm. Symantec has tested and recommends an IWA realm.



4. Add the following policy to the Local policy file (**Configuration > Policy**):

```
define condition __CondList1port80and443
url.port=443
url.port=80
```

```
end

<Proxy>

condition=__CondList1port80and443 authenticate(realm_name) authenticate.force(no)
authenticate.mode(auth_mode)
```

Where *realm_name* is the name of the authentication realm you created and *auth_mode* is the authentication mode appropriate for your deployment. See "Reference: Authentication Modes" on page 55.

5. Add the other forwarding policy, as described in "ProxySG Forwarding Configuration: SGOS 6.x/7.x" on page 17.

Reference: Required Locations, Ports, and Protocols

Depending on your configured Symantec Web Security Service Access Methods, some ports, protocols, and locations must be opened on your firewalls to allow connectivity to the various cloud service components and data centers.

Symantec Resource

support.symantec.com	Support site links to support tools and documentation.

Access Methods

Access Method	Port(s)	Protocol	Resolves To
Web Security Service IP addresses			199.19.250.192 199.116.168.192
Firewall/VPN (IPsec)	80/443 UDP 500 (ISAKMP)	IPsec/ESP	
Proxy Forwarding	8080/8443 8084*	HTTP/HTTPS	Port 8080 to proxy.threatpulse.net Port 8443 to proxy.threatpulse.net *Port 8084 to proxy.threatpulse.net *If this forwarding host is configured for local SSL interception.
Explicit Proxy	8080		To proxy.threatpulse.net https://portal.threatpulse.com/pac
Trans-Proxy	8080 (VPN Tunnel)		ep.threatpulse.net resolves to the following pseudo address. 199.19.250.205
Unified Agent	443	UDP (v4.9.1+), TCP, SSL	Port 443 to ctc.threatpulse.com Port 443 to proxy.threatpulse.com Port 443 to portal.threatpulse.com (199.19.250.192)
MDM (registered iOS and Android devices)	UDP 500 (ISAKMP) UDP 4500 (NAT-T)	IPSec/ESP	

Access Method	Port(s)	Protocol	Resolves To
Hybrid Policy			8.28.16.231 (expires July 21, 2017) 199.19.250.195 199.116.168.195 (available July 21, 2017) If connectivity to the Web Security Service is behind stringent firewall rules, adjust the rules to allow traffic to pass to these IP addresses on port 443.

Authentication

Auth Method	Port(s)	Protocol	Resolves To
Auth Connector	443	SSL	to auth.threatpulse.com: 199.19.250.193 199.116.168.193 portal.threatpulse.com: 199.19.250.192 **Additional Required Information:** Reference: Authentication IP Addresses.
Auth Connector to Active Directory	139,445	TCP	
	389	LDAP	
	3268	ADSI LDAP	
	135	Location Services	
	88	Kerberos	
	49152-65535	TCP	If installed on a new Windows Server 2012 Member rather than a Domain Controller.
AC-Logon App	80		Port 80 from all clients to the server.
SAML	8443	Explicit and IPSec	
Roaming Captive Portal	8080		

Cloud-to-Premises DLP

- XMPP port 5222 to `comm.threatpulse.com`