smoothwall®
The Web You Want

Smoothwall Secure Global Proxy

Secure Global Proxy Installation and Administration Guide

Smoothwall® Secure Global Proxy, Installation and Administration Guide, September 2014

For more information, contact: docs@smoothwall.net

Trademark notice

Acknowledgements

Smoothwall acknowledges the work, effort and talent of the Smoothwall GPL development team: Lawrence Manning and Gordon Allan, William Anderson, Jan Erik Askildt, Daniel Barron, Emma Bickley, Imran Chaudhry, Alex Collins, Dan Cuthbert, Bob Dunlop, Moira Dunne, Nigel Fenton, Mathew Frank, Dan Goscomb, Pete Guyan, Nick Haddock, Alan Hourihane, Martin Houston, Steve Hughes, Eric S. Johansson, Stephen L. Jones, Toni Kuokkanen, Luc Larochelle, Osmar Lioi, Richard Morrell, Piere-Yves Paulus, John Payne, Martin Pot, Stanford T. Prescott, Ralf Quint, Guy Reynolds, Kieran Reynolds, Paul Richards, Chris Ross, Scott Sanders, Emil Schweickerdt, Paul Tansom, Darren Taylor, Hilton Travis, Jez Tucker, Bill Ward, Rebecca Ward, Lucien Wells, Adam Wilkinson, Simon Wood, Nick Woodruffe, Marc Wormgoor.

Secure Global Proxy contains graphics taken from the Open Icon Library project http://openiconlibrary.sourceforge.net/

Address	Smoothwall Limited 1 John Charles Way Leeds. LS12 6QA United Kingdom	
Email	info@smoothwall.net	
Web	www.smoothwall.net	
Telephone	USA and Canada:	1 800 959 3760
	United Kingdom:	0870 1 999 500
	All other countries:	+44 870 1 999 500
Fax	USA and Canada:	1 888 899 9164
	United Kingdom:	0870 1 991 399
	All other countries:	+44 870 1 991 399

Contents

About This Guide

Smoothwall Secure Global Proxy is a feature of the Smoothwall firewall products.

This manual provides guidance for installing and using Smoothwall Secure Global Proxy.

Audience and Scope

This guide is aimed at system administrators maintaining and deploying Secure Global Proxy.

This guide assumes the following prerequisite knowledge:

- An overall understanding of the functionality of the Smoothwall System application
- An overall understanding of the functionality of the Secure Global Proxy application
- An overall understanding of networking concepts

Organization and Use

This guide is made up of the following chapters and appendices:

Conventions

The following typographical conventions are used in this guide:

Item	**Convention**	**Example**
Key product terms	Initial Capitals	Smoothwall Secure Global Proxy
Cross-references and references to other guides	*Italics*	See *Chapter 1, Introduction to Secure Global Proxy* on page 3
Filenames and paths	`Courier`	The `portal.xml` file
Variables that users replace	***`Courier Italics`***	`http://<`*`my_ip`*`>/portal`
Smoothwall System	This may be one of: • Guardian • Advanced Firewall • Unified Threat Management depending on the license purchased	

This guide is written in such a way as to be printed on both sides of the paper.

1 Introduction to Secure Global Proxy

This chapter provides an overview of Secure Global Proxy, including:

- *About Secure Global Proxy* on page 3
- *Supported Operating Systems* on page 4

About Secure Global Proxy

Secure Global Proxy is a feature of the Smoothwall firewall products allowing direct connection to the Guardian web filter, through external interfaces, for remote devices.

Since this feature allows the web filter to be exposed as a public facing service, there is an additional layer of certificate security to reduce any potential risk from malicious abuse.

Secure Global Proxy uses NTLM authentication, and allows remote access to the web filter for iOS devices (via iOS Global HTTP Proxy), Android tablets, Chromebook, Windows and OSX laptops.

Securing the Web Filter

With Secure Global Proxy, users are expected to be authenticated via NTLM. As an additional layer of security, devices can be required to present a client-side certificate for validation. This ensures only valid devices are permitted through the firewall to the network. The client-side certificate must be deployed to all devices, irrespective of operating system. Devices presenting an invalid certificate, or none, will be blocked.

Note: The home page of the device's browser must be set to the external IP address of your Smoothwall System and port `62444`, using `https` to validate the certificate before web traffic is allowed through, such as: `https://my_external_ip:62444`.

About the Client-Side Certificate

The client-side certificate is downloadable from the Smoothwall System. It has a blank password, and is in `PKCS#12` format which is supported by the majority of browsers.

However, iOS operating systems do require a password on the certificate, which you must configure separately. For more information, see *Uploading the Client-Side Certificate* on page 12.

Supported Operating Systems

Secure Global Proxy supports the following operating systems on devices:

- Android devices:
  - o Running Jellybean (4.3), KitKat (4.4), or above
  - o For more information, see *Chapter 3, Redirecting Android Devices' Web Traffic* on page 9
- iOS devices:
  - o Running iOS 7.1, or above
  - o For more information, see *Chapter 4, Redirecting iOS Devices' Web Traffic* on page 11
- Desktops:
  - o Most mainstream browsers which support NTLM authentication
  - o For more information, see *Chapter 5, Redirecting Computers' Web Traffic* on page 17
- Google Chromebooks
  - o For more information, see *Chapter 6, Redirecting Chromebooks' Web Traffic* on page 19

2 Preparing Your Smoothwall System

Before you can install Secure Global Proxy, the following must be configured on your Smoothwall System:

- *Configuring the Smoothwall System Interfaces* on page 5
- *Configuring an Active Directory Connection* on page 5
- *Configuring an NTLM Authentication Policy* on page 6
- *Using Client-Side Certificates* on page 6
- *Creating Your Own Block Page* on page 8

Configuring the Smoothwall System Interfaces

You must ensure your Smoothwall System has at least one internal, and one external interface configured. For a detailed description of how to do this, refer to your *Smoothwall System's Administration Guide*.

Configuring an Active Directory Connection

Secure Global Proxy requires users to be authenticated via NTLM, therefore you must set up your Smoothwall System to use Active Directory. For a detailed description of how to do this, refer to your *Smoothwall System's Administration Guide*.

Configuring an NTLM Authentication Policy

Users using Secure Global Proxy must be authenticated using NTLM, providing at least one layer of protection between the user, and the proxy server and service. You must set up your Smoothwall System with the correct NTLM authentication policy.

You do this as follows:

1. On the Smoothwall System, browse to **Web proxy > Authentication > Policy wizard**.
2. From the **Step 1: What** panel, configure the following:
   - **Type** — Select **Non-transparent**.

     For more information about non-transparent, and transparent authentication policies, refer to your *Smoothwall System's Administration Guide*.
   - **Method** — From the drop down list, select **Global Proxy using NTLM**.

     You use this authentication method for connections from all remote devices.
   - **Interface** — From the drop down list, select the relevant interface for your Smoothwall System.

     Note that even if your Smoothwall System has multiple internal interfaces, you can only create one **Global Proxy using NTLM** authentication policy. Enabling this policy automatically adds firewall rules to allow external access to the proxy port. If your Smoothwall System uses primary and secondary external connections, Secure Global Proxy will listen on the primary connection.
   - **Port** — From the drop down list, select the relevant port number for your Smoothwall System to listen on for proxy requests.

     Note that the internal port assigned here will also be opened on this external interface.
3. You can either choose to have web traffic from all devices on your network redirect to Secure Global Proxy, or just those from a specific location, or locations.

   Note that the location chosen must include all possible external and internal addresses that the devices might use.

   From the **Step 2: Where** panel, either add the location where this policy will apply to, or recreate and add a new location.
4. From the **Step 3: Options for authenticated requests** panel, tick **Enable policy**.
5. Click **Confirm**.

For more information about configuring authentication policies, refer to your *Smoothwall System's Administration Guide*.

Using Client-Side Certificates

As well as utilizing NTLM authentication to authenticate users, you can use client-side certificates to ensure only approved devices have access to web filter policies. This has the advantage of providing an additional layer of security.

The same certificate is used by all devices. You must download the client certificate from the Smoothwall System licenced for Secure Global Proxy, and install them on the relevant devices.

To download a client certificate, do the following:

1. On the Smoothwall System, browse to **Web proxy > Global Proxy > Settings**.
2. Ensure **Proxy security** is set to **Client certificates**.
3. Click **Save**.
4. From the **Client certificate** panel, click **Download certificate**.
5. Copy this certificate into the relevant devices internal storage, and import it into the browsers, see:
   - *Chapter 3, Redirecting Android Devices' Web Traffic* on page 9
   - *Chapter 4, Redirecting iOS Devices' Web Traffic* on page 11
   - *Chapter 5, Redirecting Computers' Web Traffic* on page 17
   - *Chapter 6, Redirecting Chromebooks' Web Traffic* on page 19

Note: The client-side certificate downloaded from Secure Global Proxy has a blank password.

Using Multiple, Distinct Proxies

You can configure multiple Secure Global Proxy servers in separate locations, which are not part of a centrally managed solution. Each proxy server must have the same Root Certificate Authority (CA) to validate the same client certificates presented to them.

This allows the connecting client to use an alternative Secure Global Proxy server without having to import a new or additional certificates, with the additional advantage of load-balancing the web traffic from a large number of clients.

Note: Secure Global Proxy servers which are part of a centrally managed solution should have the Root CA bundle uploaded to them via replication. If this does not happen, the following procedure should also be used.

To download a Root CA bundle, do the following:

1. On the Smoothwall System, browse to **Web proxy > Global Proxy > Settings**.
2. Click **Advanced**.
3. From the **Download Root CA Bundle** panel, click **Download certificate**.
4. Manually upload the Root CA certificate (`connect_ca.tgz`) to all other Secure Global Proxy servers as detailed below.

To upload a Root CA bundle, do the following:

1. On the Smoothwall System, browse to **Web proxy > Global Proxy > Settings**.
2. Click **Advanced**.
3. From the **Upload Root CA Bundle** panel, click **Choose File**, and browse to the Root CA bundle (`connect_ca.tgz`).
4. Click **Upload** to make the Root CA available.

Note: Uploading a new Root CA bundle will overwrite the existing Root CA.

Using an Unsecured (Open) Proxy

If you configure Secure Global Proxy as an open proxy, remote clients do not need to present the client-side certificate, although NTLM authentication is still required. Using Secure Global Proxy without certificates may leave your Smoothwall System vulnerable to denial of service (DoS) attack.

To remove the need for client-side certificate checking, do the following:

1. On the Smoothwall System, browse to **Web proxy > Global Proxy > Settings**.
2. Change **Proxy security** to **None (Open proxy)**.
3. Click **Save**.

Creating Your Own Block Page

It should be noted that the block page configured on your Smoothwall System will not be fully accessible to external devices that have been redirected to Secure Global Proxy.

It is recommended that you create an additional plain text block page, and upload it to your Smoothwall System. You can then create a block page policy for users of the **Global Proxy using NTLM** method. For a detailed description of how to do this, refer to your *Smoothwall System's Administration Guide*.

Tip: To use graphics on your Secure Global Proxy policy block page, you must host these on a externally accessible server, using image tags and publicly accessible style sheets. For more information, refer to your Smoothwall representative.

3 Redirecting Android Devices' Web Traffic

This chapter describes how to use Secure Global Proxy on Android devices, including:

- *Configuring the Android Device* on page 9
- *Using Client Certificates with Android Devices* on page 10

Configuring the Android Device

To redirect web traffic from connected Android devices to Secure Global Proxy, you need to configure the relevant access point with the correct proxy details.

You do this as follows:

1. From the Android device, go to the Wi-Fi settings.
2. Do one of the following:
   - o Tap **Add network**.
   - o Press and hold the connected access points' name, and select **Modify network** from the pop-up menu.
3. Tap **Show advanced options**.
4. From the **Proxy settings** drop down menu, select **Manual**.
5. Configure the following proxy settings to redirect back to Secure Global Proxy:
   - o **Proxy hostname** — Enter the external IP address of your Smoothwall System.
   - o **Proxy port** — Enter the port number to send proxy requests to. This is the port number the Smoothwall System is listening on for NTLM authentication requests; see *Configuring an NTLM Authentication Policy* on page 6.
   - o **Bypass proxy for** — Enter the URLs for those domains that do not need proxying, such as `localhost`.

Note: You must enter the IP address of your Smoothwall System as a

6. Leave **IP settings** as DHCP.
7. Tap **Save**.

Note: If the connecting Android device is outside the Active Directory domain configured on the Smoothwall System, users must also provide NTLM authentication credentials when they first open the browser. These credentials must match the ones configured on the Smoothwall System.

Using Client Certificates with Android Devices

If Secure Global Proxy has been configured to use client certificates, you must install the certificate onto the Android device.

You do this as follows:

1. Download the Secure Global Proxy certificate (`client.p12`) from your Smoothwall System, to the Android devices' internal storage. For a detailed description of how to do this, see *Using Client-Side Certificates* on page 6.
2. From the Android device, go to the Security settings.
3. Scroll down to the **Credential storage** panel, and tap **Install from storage**.
4. Locate and select the certificate.
5. Set the home page of your chosen browser to point to:

   `https://<`*`Smoothwall_System_externalIP`*`>:62444.`

   to force certificate validation every time a browsing session is started.

The Android device will use the certificate as an additional layer of security.

Note: If the connecting Android device is outside the Active Directory domain configured on the Smoothwall System, users must also provide NTLM authentication credentials after the certificate has been validated. These credentials must match the ones configured on the Smoothwall System.

4 Redirecting iOS Devices' Web Traffic

This chapter describes how to use Secure Global Proxy with iOS devices, including:

- *Prerequisites* on page 11
- *Uploading the Client-Side Certificate* on page 12
- *Configuring the Global Proxy* on page 13

Prerequisites

Before you configure the iOS device, you must prepare the following.

Creating the Proxy.pac File

The `proxy.pac` file is an externally resolvable script, hosted on a publicly accessible web server. A basic file contains the hostname and external IP address of the Secure Global Proxy proxy server. You add additional commands, such as whether to bypass the proxy server for local addresses or a defined list of domains. An example `proxy.pac` file may be as follows:

```
function FindProxyForURL(url, host)
{
     /* serverip:  The external IP address of the Smoothwall. */
     var serverip = "1.1.1.1";

     /* smoothwallHostname:  The hostname of the Smoothwall. */
     var smoothwallHostname = "smoothwall.local";

     /* The global proxy policy port. */
     var globalProxyPort = 805;

     /* If the host is the server, or the localhost matches the host name,
      * then return direct; and don't go through the proxy.
      */
     if ((host == serverip)
          || localHostOrDomainIs(host, smoothwallHostname))
     {
          return "DIRECT";
     }

     /* If the host looks like something for an intranet (i.e., contains
      * no dots), then don't proxy these requests.
      */
     if (isPlainHostName(host))
          return "DIRECT";

     /* Everything else is therefore subject to being proxied. */
     return "PROXY " + serverip + ":" + globalProxyPort;
}
```

Using a Landing Page

A landing page presents useful information to the user. You must configure a landing page to be the home page of browsers used on the iOS devices connected to your network.

When a browser is started on the iOS device, the landing page will redirect to the proxy server, allowing the client-side certificate to be validated.

Uploading the Client-Side Certificate

If Secure Global Proxy has been configured to use client certificates, you must install the certificate onto the iOS device.

You do this as follows:

1. Download the Secure Global Proxy certificate (`client.p12`) from your Smoothwall System, to the iOS devices' internal storage. For a detailed description of how to do this, see *Using Client-Side Certificates* on page 6.
2. From a Mac OS X server, open a certificate key management tool, such as XCA.
3. Import the certificate.
4. Export the certificate as a `PKCS12`.

   You will be prompted a password.
5. Configure a meaningful password for the certificate.
6. Save the certificate under a new name for later identification.

Note: If you are manually uploading the client-side certificate to the device (see *Manually Installing the Global Proxy* on page 16), you should store the certificate on a web-hosted server.

Configuring the Global Proxy

To redirect web traffic from connected iOS devices to Secure Global Proxy, you need to provision the devices with the Secure Global Proxy settings.

You can either:

- Install the global proxy settings on a single device, and push it through to all other network-connected devices — see *Deploying the Global Proxy* on page 15
- Install the global proxy manually on single devices — see *Manually Installing the Global Proxy* on page 16

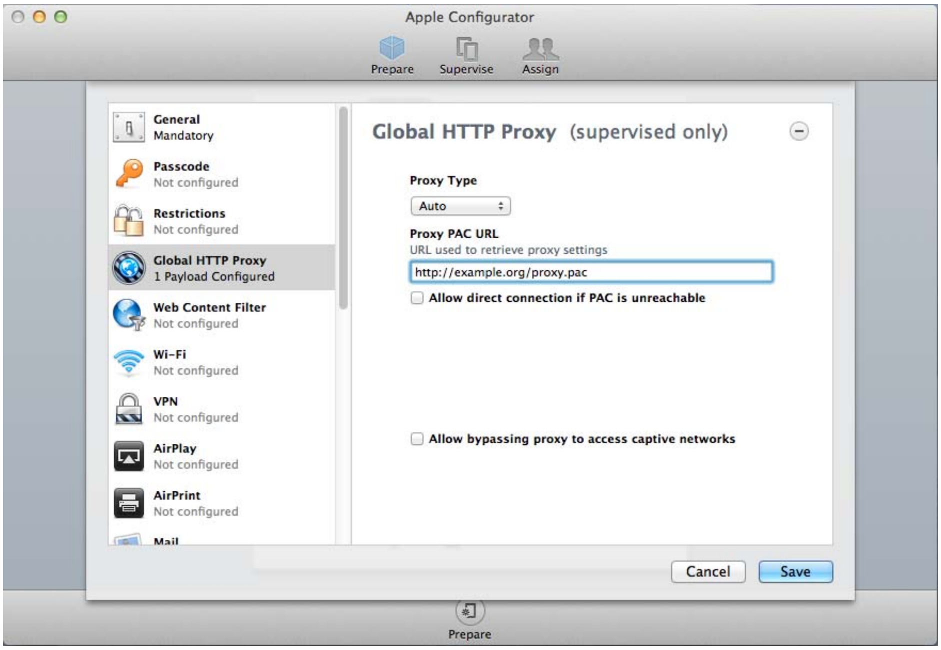
Configuring the global proxy involves configuring a profile on either an Mac OS X server, or desktop, which is then pushed through to all devices. The pre-configured profile includes:

- A certificate
- A web clip — Only used when certificate checking is enabled
- A global proxy setting

Note: To configure the above, you need to download the free Apple Configurator™ app from Apple's App Store. The Apple Configurator app allows mass deployment of profiles to iOS devices suited to corporate or education environments.

To configure the Global Proxy settings, do the following:

1. From the Mac OS X server, open the Apple Configurator.
2. Open **Global HTTP Proxy**.



Global HTTP Proxy (supervised only)

Proxy Type
Auto

Proxy PAC URL
URL used to retrieve proxy settings
http://example.org/proxy.pac

□ Allow direct connection if PAC is unreachable

□ Allow bypassing proxy to access captive networks

3. From the drop down list, set **Proxy Type** to **Auto**.

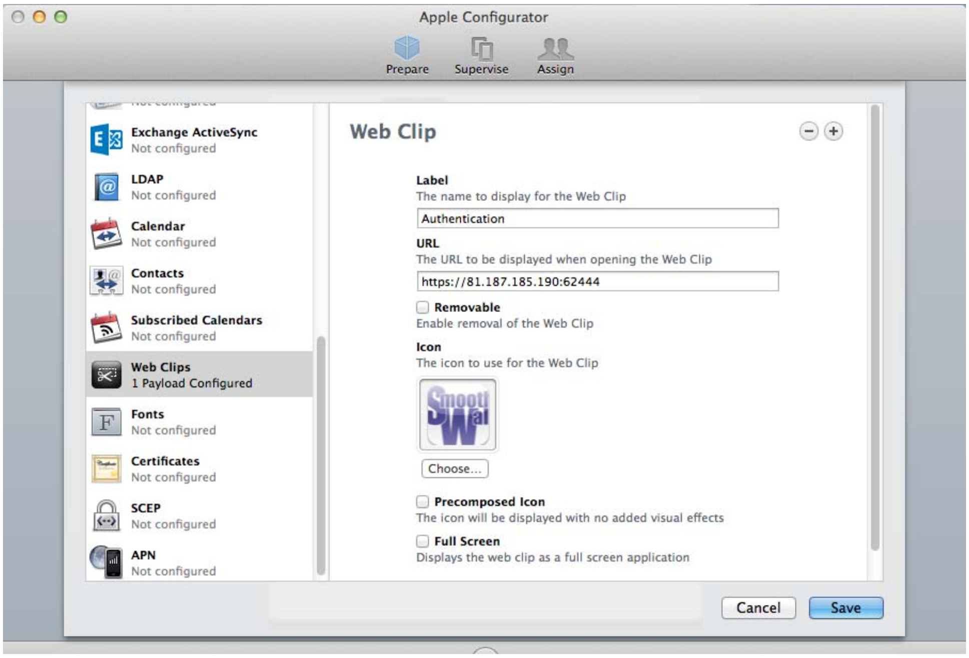
   This forces the iOS device to use the `proxy.pac` file it is presented.

4. In **Proxy PAC URL**, enter the URL that the iOS device will use to retrieve the `proxy.pac` file. For more information about creating the `proxy.pac` file, see *Creating the Proxy.pac File* on page 11.
5. Leave **Allow direct connection if PAC is unreachable** unticked.
6. If users are expected to authenticate via a captive portal, tick **Allow bypassing proxy to access captive networks**.
7. Click **Save**.

You must create a link to the landing page of your Smoothwall System (see *Using a Landing Page* on page 12) to validate the client-side certificate. This link must be used on the iOS device before attempting to use the Safari browser for authentication. This is done in the **Web Clips** page of the Apple Configurator.

To create the link to the landing page, do the following:

1. From the Mac OS X server, open the Apple Configurator.
2. Open **Web Clips**.



Label
The name to display for the Web Clip
Authentication

URL
The URL to be displayed when opening the Web Clip
https://81.187.185.190:62444

□ Removable
Enable removal of the Web Clip

Icon
The icon to use for the Web Clip

□ Precomposed Icon
The icon will be displayed with no added visual effects

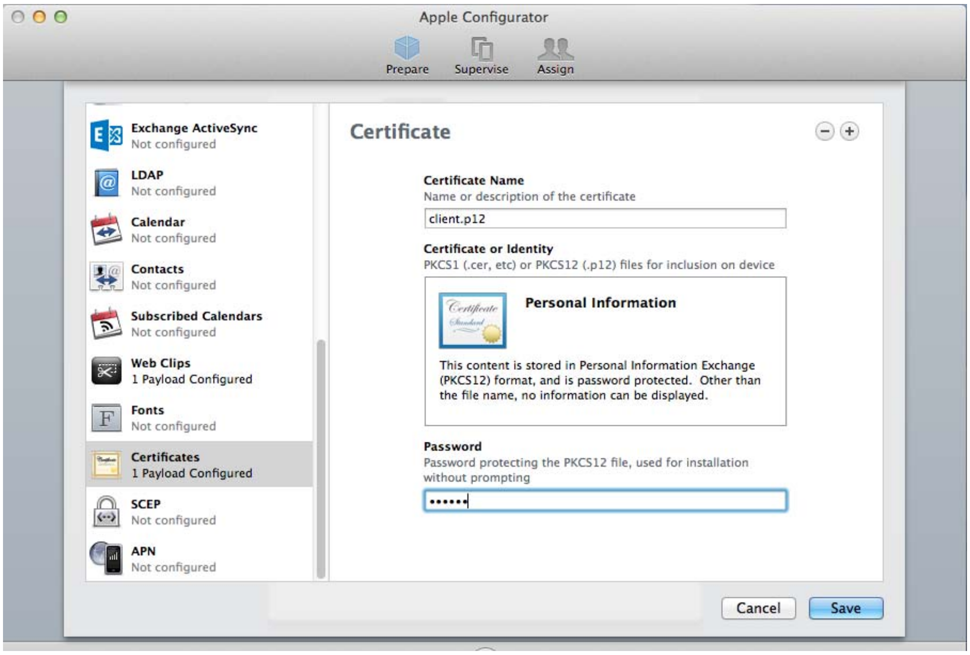
□ Full Screen
Displays the web clip as a full screen application

3. Configure the following settings:
   - **Label** — Enter a meaningful name for the Web Clip
   - **URL** — Enter the URL to display when the Web Clip is opened, using the format: `http://<`*`Smoothwall_System_externalIP`*`>:62444`.
   - **Icon** — If you wish, you can provide an icon for the configured Web Clip.
4. Click **Save**.

You now need to add the password that was previously configured for the uploaded client-side certificate (see *Uploading the Client-Side Certificate* on page 12).

You do this as follows:

1. From the Mac OS X server, open the Apple Configurator.
2. Open **Certificates**.



Certificate

Certificate Name
Name or description of the certificate
client.p12

Certificate or Identity
PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device

Personal Information

This content is stored in Personal Information Exchange (PKCS12) format, and is password protected. Other than the file name, no information can be displayed.

Password
Password protecting the PKCS12 file, used for installation without prompting
••••••

3. The client-side certificate you previously uploaded should appear in the **Certificate Name** box. If it does not, enter `client.p12`.
4. Enter the assigned password for the `PKCS12` file in the **Password** text box.
5. Click **Save**.

Note: If the connecting iOS device is outside the Active Directory domain configured on the Smoothwall System, users will be required to provide NTLM authentication credentials after the certificate has been validated. These credentials must match the ones configured on the Smoothwall System.

Deploying the Global Proxy

You must push the configured global proxy settings out to relevant iOS devices on your network. You do this by either:

- Connecting the iOS device to the Mac OS X server, and copying the global proxy settings over.
- Using the Push wireless service to push the global proxy settings from the Max OS X server out to the iOS devices.

  For a detailed description of how to use the Push wireless service, refer to your Apple® documentation.

Manually Installing the Global Proxy

The following procedure describes how to configure the Secure Global Proxy settings on a single iOS device.

To manually install the global proxy settings, do the following:

1. Download the Secure Global Proxy certificate (`client.p12`) from your Smoothwall System, to a web-hosted location. For a detailed description of how to do this, see *Uploading the Client-Side Certificate* on page 12.
2. Using a Safari browser, browse to the web-hosted `client.p12` certificate.

   The **Install Profile** page will display the identity certificate.
3. Click **Install**.
4. If prompted, enter the device's passcode.
5. Enter the password you configured for the `client.p12` certificate to confirm the installation of the profile.
6. When completed, go to the Wi-Fi settings of the iOS device.
7. Scroll down to, and open, **HTTP Proxy**.
8. Tick **Auto**.
9. In the **Proxy PAC URL** box, enter the URL that the iOS device will use to retrieve the `proxy.pac` file. For more information about creating the `proxy.pac` file, see *Creating the Proxy.pac File* on page 11.
10. Click **Save** and exit out of the application.
11. Open a Safari browser, and browse to:
    `https://<Smoothwall_System_externalIP>:62444.`

    This validates the installed certificate.

The iOS device will use the certificate as an additional layer of security.

Note: If the connecting iOS device is outside the Active Directory domain configured on the Smoothwall System, users will be required to provide NTLM authentication credentials when they first open the browser. These credentials must match the ones configured on the Smoothwall System.

5 Redirecting Computers' Web Traffic

This chapter describes how to use Secure Global Proxy with other browsers.

Configuring Internet Options

To redirect web traffic from connected computers, you must configure the proxy settings of the web browser to point to the public IP address of your Smoothwall System. The browser used must also support client-side certificates.

Example Configuration for Windows 7 Computers

You may not be using a Windows 7 computer. You must refer to your own documentation accompanying the computer for a description of how to set this up accordingly. The following is only relevant for Windows 7 computers.

To redirect web traffic to Secure Global Proxy from a Windows 7 computer, do the following:

1. Log into your Windows computer, and open **Control Panel**.
2. Click **Internet Options** to open the **Internet Properties** dialog.
3. Open the **Connections** tab.
4. From the **Local Area Network (LAN) settings** panel, click **LAN settings**.
5. Tick **Use a proxy server for your LAN**, and configure the following proxy settings:
   - **Address** — Either the external IP address of your Smoothwall System, or hostname if it's a publicly resolvable domain name.
   - **Port** — The port number to send proxy requests to. This is the port number the Smoothwall System is listening on for NTLM authentication requests; see *Configuring an NTLM Authentication Policy* on page 6.
6. Ensure **Bypass proxy server for local addresses** is ticked.

7. Click **OK**.

Note: If the connecting Windows machine is outside the Active Directory domain configured on the Smoothwall System, users will be required to provide NTLM authentication credentials when they first open the browser. These credentials must match the ones configured on the Smoothwall System. However, you may notice a performance hit when browsing. This is because Windows will respond to every `407:Proxy authentication required` request from Secure Global Proxy with the local Windows credentials first before using the NTLM credentials provided. For optimal performance, the computer should be a member of the Active Directory domain that the Smoothwall System uses for authentication.

Using Client Certificates with Windows 7 Computers

If Secure Global Proxy has been configured to use client certificates, you must install the certificate onto the Windows 7 computer.

You do this as follows:

1. Download the Secure Global Proxy certificate (`client.p12`) from your Smoothwall System, to your Windows computer. For a detailed description of how to do this, see *Using Client-Side Certificates* on page 6.
2. Open **Control Panel**.
3. Click **Internet Options** to open the **Internet Properties** dialog.
4. Open the **Content** tab.
5. From the **Certificates** panel, click **Certificates**.
6. From the **Intended purpose** drop down list, select **<All>**.
7. Click **Import** to start the **Certificate Import Wizard**. Click **Next**.
8. Locate and open the certificate downloaded from your Smoothwall System. Click **Next**.
9. Leave the certificate in the Personal certificate store. Click **Next**.

   The default client certificate downloaded from your Smoothwall System has a blank password. If the certificate has been manually manipulated to have a password, you will be prompted to enter it now.
10. Confirm your changes, and click **Finish** to load the certificate.
11. You must add a proxy exception for the external address of your Smoothwall System to the proxy server details configured in *Example Configuration for Windows 7 Computers* on page 17.
12. Set the home page of your chosen browser to point to:

    `https://<Smoothwall System_externalIP>:62444.`

    to force certificate validation every time a browsing session is started.

The Windows 7 computer will use the certificate as an additional layer of security.

Note: Some browsers, such as Mozilla Firefox®, do not use the central proxy configuration on Windows computers, and must be configured separately. For a detailed description of how to set this up, refer to the browsers’ own documentation.

6 Redirecting Chromebooks' Web Traffic

This chapter describes how to use Secure Global Proxy with Google Chromebooks, including:

- *Configuring the Chromebook* on page 19
- *Using Client Certificates with Chromebooks* on page 20

Configuring the Chromebook

To redirect web traffic from connected Chromebooks to Secure Global Proxy, you need to configure the relevant access point with the correct proxy details.

You do this as follows:

1. Log into the Chromebook.
2. Click on the **Network** icon in the bottom right of the screen.
3. Select **Settings** from the pop-up dialog.
4. Click the access point the Chromebook is connected to, and click **Network Options** from the pop-up dialog.
5. Open the **Proxy** tab.
6. Configure the following:
    - Select **Manual proxy configuration**
    - **HTTP Proxy** — Either the external IP address or hostname of your Smoothwall System.
    - **Port** — The port number to send proxy requests to. This is the port number the Smoothwall System is listening on for NTLM authentication requests; see *Configuring an NTLM Authentication Policy* on page 6.

Alternatively, if you have a configured URL that contains the Secure Global Proxy settings, configure the following:

- Select **Automatic proxy configuration**
- **Auto-configuration URL** — Enter the proxy settings URL

7. In the **Advanced Configuration** box, enter the URLs for those domains that do not need proxying, such as `localhost`.
8. Click **Close**.

Note: If the connecting Chromebook is outside the Active Directory domain configured on the Smoothwall System, users will be required to provide NTLM authentication credentials when they first open the browser. These credentials must match the ones configured on the Smoothwall System.

Using Client Certificates with Chromebooks

If Secure Global Proxy has been configured to use client certificates, you must install the certificate onto the Chromebook.

You do this as follows:

1. Download the Secure Global Proxy certificate (`client.p12`) from your Smoothwall System, to the Chromebooks' internal storage. For a detailed description of how to do this, see *Using Client-Side Certificates* on page 6.
2. From your Chromebook, open a Chrome browser, and go to `chrome://settings/certificates`.
3. From the **Certificate manager** dialog, click the **Authorities** tab.
4. Click **Import...**.
5. Locate the certificate and click **Open**.

Tip: If the certificate doesn't show in the **Select a file to open** dialog, change the file type filter to **All files**.

6. From the **Certificate authority** dialog, tick the following:
   - **Trust this certificate for identifying websites**
7. Click **OK**.
8. Set the home page of the Chrome browser to point to:

   `https://<`*`Smoothwall System_externalIP`*`>:62444.`

   to force certificate validation every time a browsing session is started.

Chromebook will use the certificate as an additional layer of security.

Note: If the connecting Chromebook is outside the Active Directory domain configured on the Smoothwall System, users will be required to provide NTLM authentication credentials after the certificate has been validated. These credentials must match the ones configured on the Smoothwall System.

7 Using Secure Global Proxy Alerts, and Viewer

This chapter describes how to use Secure Global Proxy alerts, and logs.

About Alerts

Alerts are generated when certain trigger conditions are met. Trigger conditions can be individual events, for example, an administrator login failure, or a series of events occurring over a particular time period, for example, a sustained high level of traffic over a five minute period.

The following sections assumes you have configured your Smoothwall System alerts. For a detailed description of how to do this, refer to your *Smoothwall System's Operations Guide*.

About the Secure Global Proxy Alert

The Secure Global Proxy alert continuously monitors for activity. Alerts are triggered when client misconfiguration, or potential abuse is detected.

The Secure Global Proxy comes pre-defined upon installation. You access alerts on your Smoothwall System, from the **Logs and reports > Alerts > Alerts** page.

Adjust the alert parameters as follows:

- **Monitor for incorrect certificates** — Cancel the selection to disable alerting when a client fails to present the correct certificate.

  This is either due to the client having the wrong certificate.
- **Monitor for DoS attempts** — Cancel the selection to disable alerting when a client, with a valid certificate, repeatedly attempts a connection. Repeated connections from a client are assumed to be a Denial of Service (DoS) attempt.

Enabling Instantaneous Alerts

You can choose to have Secure Global Proxy alerts delivered via SMS or email. By default, the Smoothwall System queues alerts in two minute intervals, and then distributes a merged notification of all configured alerts.

The Smoothwall System can be configured to process instantaneous alerts as soon as they were triggered.

To enable instantaneous alerts, do the following:

1. From the Smoothwall System, browse to **Logs and reports > Alerts > Alerts**.
2. Configure the following settings:
   - From the **Groups** panel, select the group of recipients from the **Group name** drop down list. For a detailed description of how to configure groups, refer to your *Smoothwall System's Administration Guide*.
   - From the **Alert options** panel, select **Enable instantaneous alerts**.
3. Scroll down to the **Global Proxy** alert.
4. Select the delivery method or either SMS 📱 or email ✉
5. Click **Save**.

Looking up Previous Alerts by Reference

You can also look up the content of a Secure Global Proxy alert status that has been sent.

To view the content of an alert that has already been sent, do the following:

1. From the **Lookup alert details** panel, enter the Global Proxy alert's unique ID into the **Alert ID** field, that is, `G8`.
2. Click **Show**.

The content of the alert will be displayed in the **Alert details** panel at the top.

Using the Secure Global Proxy Viewer

The Secure Global Proxy viewer displays information about the users logged into your network using certificates, via Secure Global Proxy, and the length of time left on their session.

To view the Secure Global Proxy activity, do the following:

- From the Smoothwall System, browse to **Web Proxy > Global Proxy > Certificate Activity**.

Index

smoothwall®

The Web You Want