BIG-IP® Access Policy Manager®: Secure Web Gateway Implementations

Version 11.6

Table of Contents

Legal Notices....9
Acknowledgments....11

Chapter 1: BIG-IP APM Secure Web Gateway Overview....15
Overview: BIG-IP APM Secure Web Gateway....16
BIG-IP APM Secure Web Gateway terminology....16
Flowchart for Secure Web Gateway configuration....17
Additional resources and documentation for BIG-IP Access Policy Manager....18

Chapter 2: URL Categorization....21
Overview: Updating URL categories and specifying web traffic schemes....22
About the Instant Messaging URL category....22
Downloading and updating URL categories....22
Adding custom URL categories....23
Looking up the category for a URL....24
Customizing preconfigured URL categories....24
Configuring URL filters....25
Configuring Secure Web Gateway schemes....26
Implementation result....26
Secure Web Gateway database download log messages....26

Chapter 3: User Identification....27
About user identification....28
About session management cookies and Secure Web Gateway....28
About ways to configure user identification for SWG....28
Overview: Identifying users transparently using F5 DC Agent....29
Configuring the BIG-IP system for the F5 DC Agent....30
Verifying network communication....31
Downloading and installing F5 DC Agent....32
Updating privileges for the F5 DC Agent service....32
Configuring the initialization file....33
Configuring domain controller polling in the dc_agent.txt file....34
Recovering from an unsuccessful installation....35
Enabling debug logging for the F5 DC Agent....35
Troubleshooting when a user is identified incorrectly....36
F5 DC Agent error messages....36
Overview: Identifying users transparently using F5 Logon Agent....37
Configuring the BIG-IP system for the F5 Logon Agent....38
Verifying network communication....39
Downloading and installing F5 Logon Agent....40

Updating privileges for the F5 Logon Agent service....40
Configuring the initialization file....41
Recovering from an unsuccessful installation....42
Enabling debug logging for the F5 Logon Agent....42
Troubleshooting when a user is identified incorrectly....43
Files used by Logon Agent....43
Overview: Creating a script on a Windows system for F5 Logon Agent....43
Creating a logon or logout script....44
Running a logon or logout script on Active Directory....44
Logon and logout script parameters....45

Chapter 4: Per-Request Policy Concepts and Examples....47
Exporting and importing a per-request policy across BIG-IP systems....48
About access and per-request policies....48
About per-request policy configuration....49
About per-request policies and SWG logging and reports....49
About Safe Search and supported search engines....49
Access and per-request policy comparison....50
Category-specific access control example....50
Access for date, time, and user group example....51
URL filter per user group example....51
SSL intercept and bypass set example....51
Response Analytics example....52
Per-flow variables....52
Session variables for use in a per-request policy....53
About per-request policy items....53
About Protocol Lookup....54
About SSL Intercept Set....54
About Category Lookup....54
About Response Analytics....55
About SSL Bypass Set....55
About URL Filter Assign....55
About Dynamic Date Time....55
About AD Group Lookup....56
About LDAP Group Lookup....56
About LocalDB Group Lookup....56
About RADIUS Class Lookup....57
About per-request policy endings....57
Customizing messages for URL filter denied....57

Chapter 5: Explicit Forward Proxy....59
Overview: Configuring SWG explicit forward proxy....60
SWG explicit forward proxy configuration prerequisites....61
About the iApp for Secure Web Gateway configuration....61

About ACLs and SWG explicit forward proxy 61
About ways to configure user identification for SWG....61
Creating a DNS resolver....62
Adding forward zones to a DNS resolver....62
Creating a tunnel for SSL forward proxy traffic....63
Creating a custom HTTP profile for explicit forward proxy....64
Configuring a per-request policy for SWG....64
Creating an access profile for SWG explicit forward proxy....67
Configuring an access policy for SWG explicit forward proxy....68
Creating a virtual server to use as the forward proxy server....70
Creating a custom Client SSL forward proxy profile....71
Creating a custom Server SSL profile....71
Creating a virtual server for SSL forward proxy traffic....72
Creating a virtual server to reject traffic....73
Implementation result....74
Session variables for use in a per-request policy....74

Chapter 6: Transparent Forward Proxy....75
Overview: Configuring transparent forward proxy in inline mode....76
SWG transparent forward proxy configuration prerequisites....76
About the iApp for Secure Web Gateway configuration....77
About ways to configure user identification for SWG....77
Creating a VLAN for transparent forward proxy....78
Assigning a self IP address to a VLAN 78
Configuring a per-request policy for SWG....79
Creating an access profile for SWG transparent forward proxy....81
Configuring an access policy for transparent forward proxy....82
Creating a custom Client SSL forward proxy profile....84
Creating a custom Server SSL profile....85
Creating a virtual server for forward proxy SSL traffic....86
Creating a virtual server for forward proxy traffic....87
Creating a forwarding virtual server....87
Creating a Client SSL profile for a captive portal....88
Creating a virtual server for a captive portal....88
Implementation result....89
Session variables for use in a per-request policy....89
About redirects after access denied by captive portal....89
Overview: Configuring transparent forward proxy....90
SWG transparent forward proxy configuration prerequisites....91
About the iApp for Secure Web Gateway configuration....91
About ways to configure user identification for SWG....91
Creating a VLAN for transparent forward proxy....92
Assigning a self IP address to a VLAN 92
Configuring a per-request policy for SWG....93

Creating an access profile for SWG transparent forward proxy....95
Configuring an access policy for transparent forward proxy....96
Creating a custom Client SSL forward proxy profile....99
Creating a custom Server SSL profile....99
Creating a virtual server for forward proxy SSL traffic....100
Creating a virtual server for forward proxy traffic....101
Creating a Client SSL profile for a captive portal....101
Creating a virtual server for a captive portal....102
Implementation result....102
Session variables for use in a per-request policy....103
About redirects after access denied by captive portal....103

Chapter 7: Remote Access Configuration....105
Overview: Configuring SWG explicit forward proxy for network access....106
Prerequisites for SWG explicit forward proxy for network access....107
Configuration outline for explicit forward proxy for network access....107
Creating a connectivity profile....107
Adding a connectivity profile to a virtual server....108
Creating a DNS resolver....108
Adding forward zones to a DNS resolver....108
Creating a custom HTTP profile for explicit forward proxy....109
Configuring a per-request policy for SWG....110
Creating an access profile for SWG explicit forward proxy....112
Creating a virtual server for network access client forward proxy server....113
Creating a wildcard virtual server for HTTP tunnel traffic....114
Creating a custom Client SSL forward proxy profile....114
Creating a custom Server SSL profile....115
Creating a wildcard virtual server for SSL traffic on the HTTP tunnel....115
Updating the access policy in the remote access configuration....117
Configuring a network access resource to forward traffic 118
Implementation result....119
Session variables for use in a per-request policy....119
Overview: Configuring SWG transparent forward proxy for remote access....119
Prerequisites....120
Configuration outline 120
Creating a connectivity profile....121
Adding a connectivity profile to a virtual server....121
Configuring a per-request policy for SWG....121
Creating an access profile for SWG transparent forward proxy....124
Creating a wildcard virtual server for HTTP traffic on the connectivity interface....125
Creating a custom Client SSL forward proxy profile....125
Creating a custom Server SSL profile....126

Creating a wildcard virtual server for SSL traffic on the connectivity interface....127
Updating the access policy in the remote access configuration....128
Implementation result....129
Session variables for use in a per-request policy....129

Chapter 8: Reports, Logs, and Statistics....131
About SWG data for threat monitoring....132
About per-request policies and SWG logging and reports....132
About Access Policy Manager and Secure Web Gateway logs....132
About local and remote logging for Secure Web Gateway....132
Flowchart for local logging configuration....133
Overview: Monitoring Internet traffic and making adjustments to SWG....134
About the reporting interval for charts and reports....135
Configuring statistics collection for reports....135
Examining Secure Web Gateway statistics....135
Focusing charts and reports on security threats....136
Exporting or emailing Secure Web Gateway statistics....137
Creating an SMTP server configuration....138
Chart and report drilldown paths....138
Overview: Configuring remote high-speed SWG event logging....139
Creating a pool of remote logging servers....141
Creating a remote high-speed log destination....141
Creating a formatted remote high-speed log destination....142
Creating a publisher 142
Creating log settings for Secure Web Gateway events....143
Adding log settings to an access profile....143
Disabling logging 144

Chapter 9: Kerberos Authentication and SWG....145
Overview: Authenticating SWG users with Kerberos....146
About basic authentication and Kerberos end-user logon....146
How does end-user logon work?....146
About Kerberos authentication requirements....148
Joining a Kerberos user account to a domain 148
Configuring an AAA server for Kerberos authentication 148
Kerberos authentication troubleshooting tips....149
Implementation result....149

Chapter 10: NTLM Authentication and SWG....151
Overview: Authenticating SWG users with NTLM....152
Configuring a machine account....152
Creating an NTLM Auth configuration....152
Maintaining a machine account....153

Legal Notices

Publication Date

This document was published on March 4, 2015.

Publication Number

MAN-0504-01

Copyright

Trademarks

Patents

This product may be protected by one or more patents indicated at:
http://www.f5.com/about/guidelines-policies/patents

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Acknowledgments

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by the Politecnico di Torino, and its contributors.

This product includes software developed by the Swedish Institute of Computer Science and its contributors.

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the Computer Systems Engineering Group at the Lawrence Berkeley Laboratory.

This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

This product includes software developed by Jochen Pohl for the NetBSD Project.

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

This product includes software developed by SigmaSoft, Th. Lockert.

This product includes software developed for the NetBSD Project by Jason R. Thorpe.

This product includes software developed by Jason R. Thorpe for And Communications, http://www.and.com.

This product includes software developed for the NetBSD Project by Frank Van der Linden.

This product includes software developed for the NetBSD Project by John M. Vinopal.

This product includes software developed by Christos Zoulas.

This product includes software developed by the University of Vermont and State Agricultural College and Garrett A. Wollman.

This product includes software developed by Balazs Scheidler (bazsi@balabit.hu), which is protected under the GNU Public License.

This product includes software developed by Niels Mueller (nisse@lysator.liu.se), which is protected under the GNU Public License.

In the following statement, "This software" refers to the Mitsumi CD-ROM driver: This software was developed by Holger Veit and Brian Moore for use with 386BSD and similar operating systems. "Similar operating systems" includes mainly non-profit oriented systems for research and education, including but not restricted to NetBSD, FreeBSD, Mach (by CMU).

This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/).

This product includes software licensed from Richard H. Porter under the GNU Library General Public License (© 1998, Red Hat Software), www.gnu.org/copyleft/lgpl.html.

This product includes the standard version of Perl software licensed under the Perl Artistic License (© 1997, 1998 Tom Christiansen and Nathan Torkington). All rights reserved. You may find the most current standard version of Perl at http://www.perl.com.

This product includes software developed by Jared Minch.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product contains software based on oprofile, which is protected under the GNU Public License.

This product includes RRDtool software developed by Tobi Oetiker (http://www.rrdtool.com/index.html) and licensed under the GNU General Public License.

This product contains software licensed from Dr. Brian Gladman under the GNU General Public License (GPL).

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes Hypersonic SQL.

This product contains software developed by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and others.

This product includes software developed by the Internet Software Consortium.

This product includes software developed by Nominum, Inc. (http://www.nominum.com).

This product contains software developed by Broadcom Corporation, which is protected under the GNU Public License.

This product contains software developed by MaxMind LLC, and is protected under the GNU Lesser General Public License, as published by the Free Software Foundation.

This product includes Intel QuickAssist kernel module, library, and headers software licensed under the GNU General Public License (GPL).

This product includes software licensed from Gerald Combs (gerald@wireshark.org) under the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or any later version. Copyright ©1998 Gerald Combs.

This product includes software developed by Daniel Stenberg. Copyright ©1996 - 2012, Daniel Stenberg, (daniel@haxx.se). All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This product includes node-uuid software, copyright © 2010-2012, Robert Kieffer, and distributed under the MIT license.

This product includes opencsv software, which is distributed under the Apache 2.0 license.

This product includes owasp-jave-encoder software, copyright © 2014, Jeff Ichnowski, and distributed under the New BSD license.

Chapter 1

BIG-IP APM Secure Web Gateway Overview

- *Overview: BIG-IP APM Secure Web Gateway*
- *BIG-IP APM Secure Web Gateway terminology*
- *Flowchart for Secure Web Gateway configuration*
- *Additional resources and documentation for BIG-IP Access Policy Manager*

Overview: BIG-IP APM Secure Web Gateway

BIG-IP® Access Policy Manager® Secure Web Gateway (SWG) implements a secure web gateway by adding access control, based on URL categorization, to forward proxy. The access profile supports both transparent and explicit forward proxy modes. The access policy includes support for using a captive portal to collect credentials for transparent forward proxy mode and HTTP 407-based credential capture for explicit forward proxy mode. In addition to user identification by credentials, SWG provides the option to identify users transparently, providing access based on best effort identification. SWG also supports SSL traffic inspection.

The benefits that SWG provides include:

- URL filtering capability for outbound web traffic.
- Identifying malicious content and providing the means to block it.
- Applying web application controls for application types, such as social networking and Internet communication in corporate environments.
- Monitoring and gating outbound traffic to maximize productivity and meet business needs.
- User identification or authentication (or both) tied to monitoring, and access control compliance and accountability.
- Visibility into SSL traffic.

BIG-IP APM Secure Web Gateway terminology

Here are some common terms as defined within the context of BIG-IP®APM Secure Web Gateway (SWG).

Term	Definition
application templates	An application template is a collection of parameters (in the form of F5® iApps® templates) that an administrator defines to create a configuration, such as configuration objects for explicit or transparent forward proxy or for communication between the BIG-IP® system and the F5 DC Agent.
explicit forward proxy	Traffic goes directly from the client browser to the forward proxy server. The forward proxy configuration takes place in the client browser, either manually or using a Proxy Auto-Configuration (PAC) file.
F5 DC Agent	The F5® DC Agent is an optional program that runs on a Windows-based server in your network. As users log on to Windows domains, the agent makes a best effort to map IP addresses to user names and send them to Secure Web Gateway (SWG).
F5 Logon Agent	The F5®Logon Agent is an optional program that runs on a Windows-based server in your network. When clients log on, the agent runs a script to map IP addresses to user names and send them to Secure Web Gateway (SWG).
IF-MAP server	When you configure the BIG-IP system to communicate with a user identity agent (one of F5 DC Agent or F5 Logon Agent), IP address and user name pairs are stored on the BIG-IP system in an IF-MAP server.
transparent forward proxy	The administrator can place the BIG-IP system right in the path of traffic (inline) as the next hop after the gateway, or can use policy-based routing or Web Cache Communication Protocol (WCCP) to send traffic for ports 80 and 443 to Secure Web Gateway.

Term	Definition
transparent user identification	The Transparent Identity Import access policy item obtains the IP-address-to-username-mapping from the IF-MAP server. Alone or by pairing this item with another query to look up the user or validate user information, you can allow access through the proxy without requesting credentials. Transparent user identification is not authentication; use it only when you are comfortable accepting a best effort at identifying a user.

Flowchart for Secure Web Gateway configuration

How you proceed with configuring Secure Web Gateway (SWG) depends on answers to questions such as:

- Are IP addresses unique and trusted in your network? F5® recommends that they should be if you plan to identify users by IP address.
- Do you want to use transparent user identification? It identifies users by a best effort at login.
- Can you and do you want to use policy-based routing or Web Cache Communication Protocol (WCCP) to forward traffic to the proxy?

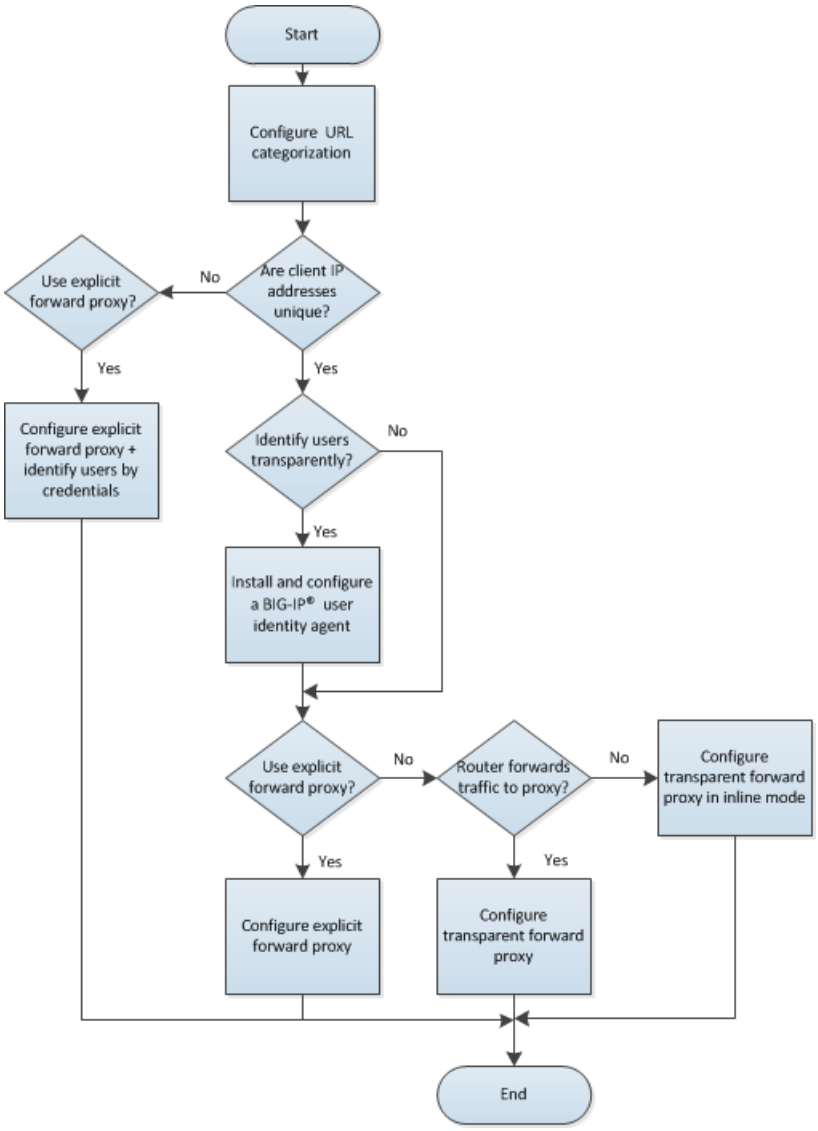

Figure 1: Configuring SWG

Additional resources and documentation for BIG-IP Access Policy Manager

You can access all of the following BIG-IP® system documentation from the AskF5™ Knowledge Base located at `http://support.f5.com/`.

Document	Description
BIG-IP® Access Policy Manager®: Secure Web Gateway Implementations	This guide contains information to help an administrator configure Secure Web Gateway (SWG) explicit or transparent forward proxy and apply URL categorization and filtering to Internet traffic from your enterprise.
BIG-IP® Access Policy Manager®: Third-Party Integration Implementations	This guide contains information about integrating third-party products with Access Policy Manager (APM®). It includes implementations for integration with VMware Horizon View, Oracle Access Manager, Citrix Web Interface site, and so on.

Document	Description
BIG-IP® Access Policy Manager®: Authentication and Single-Sign On	This guide contains information to help an administrator configure APM for single sign-on and for various types of authentication, such as AAA server, SAML, certificate inspection, local user database, and so on.
BIG-IP® Access Policy Manager®: Visual Policy Editor	This guide contains information about how to use the visual policy editor to configure access policies.
BIG-IP® Access Policy Manager®: Implementations	This guide contains implementations for synchronizing access policies across BIG-IP systems, hosting content on a BIG-IP system, maintaining OPSWAT libraries, configuring dynamic ACLs, web access management, and configuring an access policy for routing.
BIG-IP® Access Policy Manager®: Portal Access	This guide contains information about how to configure APM portal access. In portal access, APM communicates with back-end servers, rewrites links in application web pages, and directs additional requests from clients back to APM.
BIG-IP® Access Policy Manager®: Edge Client and Application Configuration	This guide contains information for an administrator to configure the BIG-IP system for these clients: • BIG-IP® Edge Client® for Windows • BIG-IP Edge Client for Mac • BIG-IP Edge Client for Linux • BIG-IP Edge Command-Line Client for Linux It also includes information about how to configure or obtain client packages and install them, as well as configuration details of system security settings on the BIG-IP system for these applications: • BIG-IP Edge Client for iOS • BIG-IP Edge Client for Android • BIG-IP® Edge Portal® for iOS • BIG-IP Edge Portal for Android
BIG-IP® Access Policy Manager®: Application Access	This guide contains information for an administrator to configure application tunnels for secure, application-level TCP/IP connections from the client to the network.
BIG-IP® Access Policy Manager®: Network Access	This guide contains information for an administrator to configure APM network access to provide secure access to corporate applications and data using a standard web browser.
BIG-IP® Access Policy Manager®: Customization	This guide provides information about using the APM customization tool to provide users with a personalized experience for access policy screens, and errors. An administrator can apply your organization's brand images and colors, change messages and errors for local languages, and change the layout of user pages and screens.
Release notes	Release notes contain information about the current software release, including a list of associated documentation, a summary of new features, enhancements, fixes, known issues, and available workarounds.
Solutions and Tech Notes	Solutions are responses and resolutions to known issues. Tech Notes provide additional configuration instructions and how-to information.

Chapter 2

URL Categorization

- *Overview: Updating URL categories and specifying web traffic schemes*

Overview: Updating URL categories and specifying web traffic schemes

With BIG-IP® system Secure Web Gateway (SWG), you can create a configuration to protect your Internet network assets and end users from threats and enforce a rightful use and compliance policy for Internet access. Users that access the Internet from the enterprise go through SWG, which allows or blocks access to certain URL categories. When recommended or configured to do so, SWG analyzes the content in the request and the response to determine whether it represents a threat, and to block access if needed.

SWG supplies over 150 URL categories and identifies over 60 million URLs that fit within these categories. In addition, you can create custom categories if needed and add URLs to any category, custom or otherwise. You can also use custom categories to define blacklists and whitelists.

SWG supplies default URL filters as a starting point for your configuration. For example, the URL filter named default blocks the majority of inappropriate websites. You can use any default filter as a starting point from which to define your own URL filters to reflect your acceptable use policies.

When you are done, you have SWG schemes that you can assign to users when they access the Internet.

Note: *SWG schemes are assigned in an access policy and apply to the whole session. URL filters are assigned in per-request policies as HTTP and HTTPS requests are made throughout a session.*

Task summary

Use these tasks to download URL categories initially, to refresh them over time, and to specify URL filters that support your rightful use and compliance policy. Before you begin, the BIG-IP system must be licensed and provisioned to support URL categorization.

Task list

Downloading and updating URL categories
Adding custom URL categories
Looking up the category for a URL
Customizing preconfigured URL categories
Configuring URL filters
Configuring Secure Web Gateway schemes

About the Instant Messaging URL category

Secure Web Gateway (SWG) supports HTTP and HTTPs-based instant messaging protocols. As a result, when you use the Instant Messaging URL category to block messages, SWG can block messages to ICQ, for example, but cannot block messages from applications that use non-standard ports or tunneling over HTTP, such as, Yahoo Messenger, Skype, Google Talk, and so on.

Similarly, SWG cannot block messages from file-sharing and peer-to-peer protocols that do not use HTTP or HTTPs; most such protocols do not use either HTTP or HTTPs.

Downloading and updating URL categories

For database downloads to work, you must have configured DNS for the BIG-IP® device in the System area of the product.

You must download the URL categories for Secure Web Gateway (SWG) to work. You schedule regular database downloads to update the existing URL categories with new URLs. SWG can then most efficiently protect your network from new threats. Without these updates, SWG uses obsolete security intelligence and as a result, protection of your networks is less effective.

Note: *You must schedule database downloads for a time with very little no user activity so that users are not impacted. Alternatively, you can initiate database downloads on-demand.*

1. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **Database Settings** > **Database Download**.
2. In the Download Settings area from the **Downloads** list, select **Enabled**.
   Additional settings display. **Download Schedule** displays a default schedule for the download.
3. In the **Download Schedule** settings, configure a two-hour window in which to start the download.
   Schedule the download to occur during off-peak hours. The default schedule is between one and three A.M.

   Warning: *After the download completes, database indexing occurs. It consumes a high amount of CPU for approximately 45 minutes.*
4. Click **Update Settings**.
5. To download the database immediately, click **Download Now**.
   A download occurs only when a newer version becomes available.

   Warning: *Database indexing occurs after the download and impacts system performance.*

Adding custom URL categories

You can add a custom category to the existing Secure Web Gateway URL categories to specify a list of URLs that you want to block or to allow.

Note: *The URL categories that you add become subcategories of Custom Categories. Custom Categories take precedence over other categories.*

1. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **URL Categories**.
   The URL Categories table displays. **Custom Categories** displays as the first entry in the table.
2. Click **Create**.
   The Category Properties screen displays.
3. In the **Name** field, type a unique name for the URL category.
4. From the **Default Action** list, retain the default value **Block**; or, select the alternative, **Allow**.
   If no action has been specified in a filter for this category, the default action is taken.
5. Add URLs to the **Associated URLs** list:
   a) In the **URL** field, type a well-formed URL that ends with a backslash (/).
   Here are some examples.
   - `https://www.siterequest.com/`
   - `http://www.siterequest.com:8080/`
   - `http://www.sitequest.com/docs/siterequest.pdf/`
   - `http://www.sitequest.com/products/application-guides/`

b) To specify that the URL is a prefix to be used for matching multiple URLs, click the **Prefix Match** check box.
c) Click **Add**.
The URL displays in the **Associated URLs** list. If the URL is used for prefix matching, an asterisk is appended to the URL; for example, **http://www.sitequest.com/products/application-guides/***.

6. Add, edit, or delete URLs to make the list.
7. Click **Finished**.
The URL Categories screen displays.
8. To view the newly created URL category, expand **Custom Categories**.
The custom URL category displays in the Sub-Category column.

Add or edit a URL filter to specify an action (allow or block) for the custom category.

Looking up the category for a URL

You look up a URL to determine whether it already exists in the master database and, if it exists, to see which categories include it.

1. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **Database Settings** > **URL Category Lookup**.
2. In the **URL** field, type the URL that you want to look up.
Type the complete URL, including the URI scheme.
Type `https://www.google.com`; not `www.google.com` or `https://www.google`.
3. Click **Search**.

Note: *Custom categories are not searched.*

Results display in the URL Category table.

If the URL is not found, you can add it to an existing or a custom category. If the URL is found, you do not need to do anything, but can recategorize it by adding it to another category.

Customizing preconfigured URL categories

You can customize the URL categories that Secure Web Gateway (SWG) supplies by adding URLs to them. You might do this after you run SWG for a while, view logs and reports, and determine that you need to make changes.

Note: *If you add a URL to a URL category, SWG gives precedence to that categorization and database downloads do not overwrite your changes.*

---

1. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **URL Categories**.
The URL Categories table displays.
2. Click the name of any category or subcategory to edit the properties for it.
To view and select a subcategory, expand categories.
The Category Properties screen displays. There are many URLs in a given category; however, any URLs that display on the **Associated URLs** list are entered by the user.
3. Edit or delete any URLs on the **Associated URLs** list.

4. To add URLs to the **Associated URLs** list:
   a) In the **URL** field, type a well-formed URL that ends with a backslash (/).
   Here are some examples.
      - `https://www.siterequest.com/`
      - `http://www.siterequest.com:8080/`
      - `http://www.sitequest.com/docs/siterequest.pdf/`
      - `http://www.sitequest.com/products/application-guides/`

   b) To specify that you want to use the URL as a prefix, for matching multiple URLs, select the **Prefix Match** check box.
   c) Click **Add**.
   The URL displays in the **Associated URLs** list. If the URL is used for prefix matching, an asterisk is appended to the URL; for example, **http://www.sitequest.com/products/application-guides/***.

5. Click **Update**.
   The URL Properties screen refreshes.
6. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **URL Categories**.
   The URL Categories table displays. The screen displays **(recategorized)** next to the URL category that you customized.

URLs are added to the URL category that you selected. When categorizing these URLs, SWG selects the customized URL category regardless of whether the URL is assigned, by default, to the customized URL category or any other URL category.

Configuring URL filters

You configure a URL filter to specify the URL categories that are allowed and those that are blocked. You can configure multiple URL filters.

1. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **URL Filters**.
   You can click the name of any filter to view its settings.

   Note: *Default URL filters, such as block-all and basic-security, are available. You cannot delete default URL filters.*

   The URL Filters screen displays.
2. To configure a new URL filter, click one of these:
   - **Create** button - Click to start with a URL filter that allows all categories.
   - **Copy** link - Click this link for an existing URL filter in the table to start with its settings.

   Another screen opens.
3. In the **Name** field, type a unique name for the URL filter.
4. In the **Description** field, type any descriptive text.
5. Click **Finished**.
   The screen redisplays. An Associated Categories table displays. It includes each URL category and the filtering action that is currently assigned to it. The table includes a Subcategory column.
6. To view filtering actions that are assigned to subcategories, expand the category or categories by clicking the plus button for the category or in the table heading.
7. To block access to particular categories or subcategories, select them and click **Block**.

Important: *When you select a category, you also select the related subcategories. You can expand the category and clear any subcategory selections.*

Note: *To block URLs that SWG cannot categorize, expand the category,* ***Miscellaneous****, and select* ***Uncategorized****.*

8. To allow access to particular categories or subcategories, select them and click **Allow**.

To use a URL filter, you must assign it in a per-request policy. A per-request policy runs each time a URL request is made.

Configuring Secure Web Gateway schemes

A Secure Web Gateway (SWG) scheme is a required component of an SWG configuration.

1. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **Schemes**.
   The Schemes screen displays.
2. Click **Create**.
   The New Scheme screen displays.
3. In the **Name** field, type a unique name for the scheme.
4. Click **Finished**.

A scheme goes into effect when an access policy assigns it to a user in an SWG explicit forward proxy or transparent forward proxy configuration; this assignment must occur in the access policy.

Implementation result

Now you have BIG-IP® Secure Web Gateway (SWG) configured to regularly download updates to URL categories. Schemes are configured and ready to be added to access policies.

Secure Web Gateway database download log messages

When you deploy Secure Web Gateway (SWG), the database downloads output messages to the `/var/log/apm` file. This table lists messages that are available only when you enable debug.

Debug message	Description
`Transfer Status 247`	The file is transferred successfully to the BIG-IP® system. If you see a Transfer Status other than 247, it might indicate an error.
`RTU Type`	The RTU Type is always 1. If you see an RTU Type other than 1, it might indicate an error.
`Expiration Date`	The BIG-IP system does not use the expiration date in this message. Instead, the BIG-IP system enforces the SWG license and the database download works accordingly.

Chapter 3

User Identification

- *About user identification*
- *About session management cookies and Secure Web Gateway*
- *About ways to configure user identification for SWG*
- *Overview: Identifying users transparently using F5 DC Agent*
- *Overview: Identifying users transparently using F5 Logon Agent*
- *Overview: Creating a script on a Windows system for F5 Logon Agent*

About user identification

Secure Web Gateway (SWG) identifies users and maps them to IP addresses, or to sessions, without using cookies.

About session management cookies and Secure Web Gateway

Secure Web Gateway (SWG) does not use Access Policy Manager® (APM®) session management cookies. If presented with an APM session management cookie, SWG ignores it.

About ways to configure user identification for SWG

User identification configuration requires a method setting in the access profile and an access policy configured to support the setting. Depending on the access profile type, you can select one of these user identification methods: by IP address (for SWG-Explicit or SWG-Transparent access profile types) or by credentials (for SWG-Explicit type).

Identification by IP address

When you identify users by IP address, you can employ any of these methods.

Note: *Identify users by IP address only when IP addresses are unique and can be trusted.*

---

transparent user identification

Transparent user identification makes a best effort to identify users without requesting credentials. An agent obtains data and stores a mapping of IP addresses to user names in an IF-MAP server. An F5 DC Agent queries domain controllers. An F5 Logon Agent runs a script when a client logs in and can run a script when the client logs out.

Note: *To identify users transparently, you must first install and configure one BIG-IP user identification agent, either the F5® DC Agent or the F5 Logon Agent.*

---

explicit user identification

You can present a logon page in an access policy to request user credentials and validate them. SWG maintains an internal mapping of IP addresses to user names. (You can present the appropriate logon page for the access policy type. For explicit forward proxy, you can present a 407 page. For transparent forward proxy, you can present a 401 page.)

source IP ranges or subnets

You can forego actually identifying the user and base the choice of which scheme to apply on whether the IP address is in a source IP range or on a subnet. SWG maintains an internal mapping of IP addresses to sessions.

Identification by credentials

When you choose to identify users by credentials, SWG maintains an internal mapping of credentials to sessions. To support this choice, you need an NTLM Auth Configuration object and you should check the result of NTLM authentication in the access policy.

Overview: Identifying users transparently using F5 DC Agent

The F5® DC Agent enables *transparent user identification*, a best effort to identify users without requesting credentials.

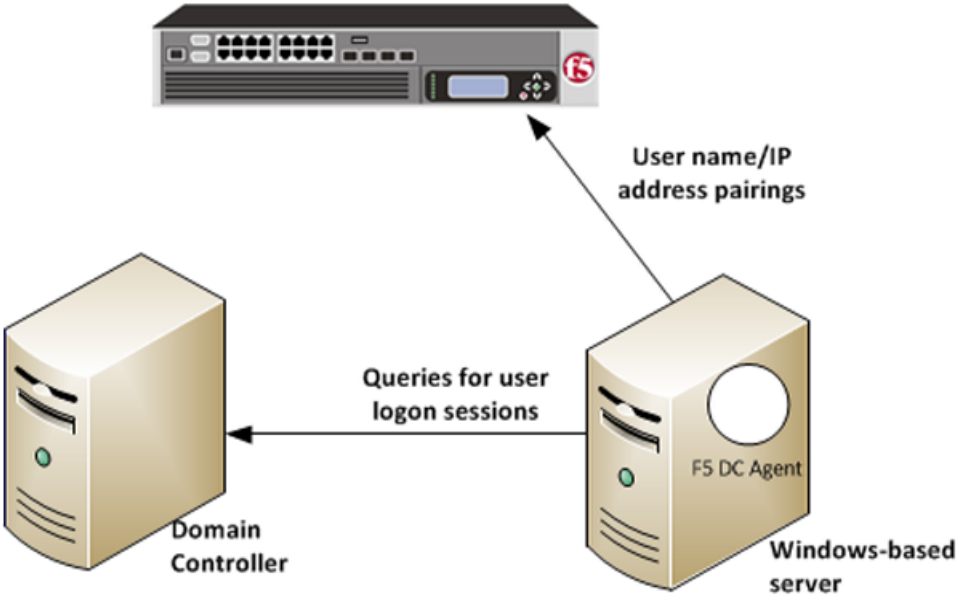

Figure 2: How F5 DC Agent transparently identifies users

You can install the F5® DC Agent on a Windows-based server in any domain in the network. The F5 DC Agent discovers domains and domain controllers, queries the domain controllers for logon sessions, and sends an IP-address-to-user-name mapping to the BIG-IP® system. F5 DC Agent sends only those new user name and IP address pairs recorded since the previous query. The BIG-IP system maintains user identity information in an IF-MAP server and stores only the most recently identified user name for a given IP address.

Note: *F5 DC Agent does not transmit passwords or any other confidential information.*

Considerations for installing multiple agents

You can install more than one F5 DC Agent in your network and configure F5 DC Agents to communicate with the same BIG-IP system.

NetBIOS port 139

F5 DC Agent uses NetBIOS port 139 for automatic domain detection. If NetBIOS port 139 is blocked in your network, you can deploy an F5 DC Agent instance for each virtually or physically remote domain.

Multiple subnets

As a best practice, install a separate F5 DC Agent in each subnet to avoid problems gathering logon information from domain controllers.

Network size, disk space, and RAM

If your network is very large (10,000+ users or 30+ domain controllers), you might benefit from installing F5 DC Agent on multiple machines to evenly distribute resource usage. F5 DC Agent uses TCP to transmit data, and transmits roughly 80 bytes per user name and IP address pair.

Number of users	Average amount of data transferred per day
250 users	30 KB
2,000 users	240 KB
10,000 users	1200 KB

Task summary

Configuring the BIG-IP system for the F5 DC Agent
Verifying network communication
Downloading and installing F5 DC Agent
Updating privileges for the F5 DC Agent service
Configuring the initialization file
Configuring domain controller polling in the dc_agent.txt file
Recovering from an unsuccessful installation
Enabling debug logging for the F5 DC Agent
Troubleshooting when a user is identified incorrectly

Configuring the BIG-IP system for the F5 DC Agent

You use an iApps® template to deploy an application service that configures objects that the F5® DC Agent uses to communicate with the IF-MAP server on the BIG-IP® system.

Note: *You can configure the F5 DC Agent to authenticate with the BIG-IP system using certificate inspection or using clientless HTTP basic authentication against a local user database.*

---

1. To support certificate inspection:
   a) Obtain a trusted certificate and key that are valid for all fully qualified domain names (FQDNs) used to access the BIG-IP system.
   b) Import the certificate and key into the BIG-IP system.
      You can import SSL certificates from the System area of the product.

2. Obtain the IFMap iApps template file from F5® DevCentral™ at `http://devcentral.f5.com/wiki/iapp.Codeshare.ashx`.
3. Import the template:
   a) On the Main tab, click **iApps** > **Templates**.
   b) Next, click **Import**.
   c) Select the **Overwrite Existing Templates** check box.
   d) Click **Choose File**, then browse to and choose the template file.
   e) Click **Upload**.

4. Deploy an application service:
   a) On the Main tab, click **iApps Application** > **Services**, and then click **Create**.
   b) In the **Name** field, type a name.

Note: *The application service prefixes this name to the names of configuration objects it creates.*

c) From the **Template** list, select **f5.ifmap**.

Note: *This iApps template displays on the list only when APM is provisioned.*

d) Follow the instructions on the screen to complete the deployment.
A summary displays the configuration objects.

e) Take note of the IP address of the virtual server created by the service. You need to type it into F5 DC Agent initialization file later.

Note: *This virtual server must be accessible by the F5 DC Agent from a routing perspective.*

5. To enable clientless HTTP basic authentication, create a user and password in the local user database.

The purpose of this user account is to authenticate communication between the F5 DC Agent and the BIG-IP system.

a) On the Main tab, click **Access Policy** > **Local User DB** > **Manage Users**.
The Manage Users screen displays.

b) Click **Create New User**.
The Create New Local User screen opens and displays User Information settings.

c) From the **Instance** list, select the instance created when you deployed the application service.

d) In the **User Name** field, type the user name.

Take note of the user name and password. You need to type them again later when you configure the initialization file for F5 DC Agent.

e) In the **Password** and **Confirm Password** fields, type the user's password.

Verifying network communication

You can verify that there are no DNS or NetBIOS or network communications issues on a Windows-based server before you install the F5® DC Agent on it. Alternatively, you can use these steps for troubleshooting if you observe a problem.

1. Open a command prompt on the Windows-based server that hosts, or will host, the F5 DC Agent.

2. To verify that the Windows-based server sees all required domains, use the `net view` command.
For example, type `net view /network`

3. To check for DNS issues, use the `nslookup` command.
For example, to verify that DNS resolves the host name, testmachine1, type this command: `nslookup testmachine1`. If the DNS lookup succeeds, the result is similar to: `Server: testdns.test.example.com Address: 10.56.1.4 Name: testmachine1.test.example.com Address: 10.56.100.15`

4. To verify that F5 DC Agent will be able to use NetBIOS, try to telnet to a domain controller on port `139`.
If the command is successful, the screen remains blank. If unsuccessful, then:

- A router, firewall, or other device might be blocking NetBIOS traffic.
- NetBIOS might not be enabled and the domain controller might not be listening on port `139`.

5. If you could not successfully telnet to a domain controller on port `139`, verify the status of the port using the `netstat` command.

For example, type: `netstat -na | find "139"`

6. To verify that the F5 DC Agent will be able to communicate with the virtual server on the BIG-IP system, telnet to the IP address of the virtual server on port `8096` or on the port that you entered when creating the application service.

   This virtual server was created using an application service based on the f5.ifmap iApps template.

Downloading and installing F5 DC Agent

F5® DC Agent is available when Access Policy Manager® (APM®) is licensed and provisioned on the BIG-IP® system. Before you perform these steps, make sure that the Windows Computer Browser service is running on the Windows server where you plan to install F5 DC Agent.

You perform this task to be able to identify clients transparently by IP address. (Do this only in an environment where IP addresses are trusted and unique.)

1. Go to the BIG-IP® system Configuration utility Welcome screen.

   If you are already logged in, click the F5® logo to open the Welcome screen.

2. In the BIG-IP User Identification Agents area, click the **User Identification Agents** link.
   A `SWGUserIdentificationAgents.exe` file downloads.
3. Copy the downloaded file to a Windows-based server that is joined to a domain controller.

   Important: *Do not install F5 DC Agent on a domain controller because the F5 DC Agent can put a load on the domain controller.*

4. From an account with both local and administrator privileges, click the `SWGUserIdentificationAgents.exe` file to start the installer.

   The installer displays instructions.

5. Follow the instructions to complete the installation.

   Important: *F5® strongly recommends that you use the default destination folder. On the Destination Folder screen, click* ***Next*** *without making any changes.*

   Important: *Install either F5 DC Agent or F5 Logon Agent, but not both. This overwrites the omapd user map every time an update is published.*

   The program installs a Windows service, F5 DC Agent.

Updating privileges for the F5 DC Agent service

The F5® DC Agent service must run from a privileged account. You can create a new user account or use an existing account configured as specified in step 1.

1. On the Windows-based server, create a user account for F5 DC Agent:
   a) Assign the new account domain administrator privileges in all domains.
   b) Assign the same password to this account in all domains.

      Make a note of the password. You must type it again in step 2.

   c) Set the password to never expire.

2. Configure the F5 DC Agent service to log on as the user account you just configured:
   a) Open the Windows Services dialog box.
   From the Control Panel, select **Administrative Tools** > **Services**.
   b) Locate the F5 DC Agent service, right-click the service name, and select **Stop**.
   c) Double-click the service name, and then select the Log On tab.
   d) Select **This account** and type the account name and password for the account you created in step 1.

   Note: *Some domains require that you type the account name in the format domain\username.*

   e) Close the Services dialog box.

Start the F5 DC Agent service again after the initialization file configuration is complete.

Configuring the initialization file

Before you can configure the initialization file, you must have the F5® DC Agent installed on a domain-joined, Windows-based server. You must also have deployed an iApps® application service to configure objects that enable communication between the F5 DC Agent and the BIG-IP® system.

Note: *The following steps require you to enter some values that are available only as a result of completing the prerequisites.*

You configure an initialization file for the F5 DC Agent so that it can send IP address and user name pairs to the BIG-IP system.

1. Log on to the Windows-based server where you installed the F5® DC Agent.
2. Navigate to this directory: `C:\Program Files\F5 Networks\User Identity Agents\config`.
3. Using a text editor, open the `transid.ini` file.
   The file contains one section, [DC Agent].
4. For `IFMapServer`, type the protocol, host address, and port for the server.
   This is the virtual server that was created by the application service. Port `8096` is the default port. You might have specified another port number when you deployed the application service.
   For example, `IFMapServer=https://AA.BB.CC.DD:8096`, where *`AA.BB.CC.DD`* is the IP address of the virtual server created by the application service.
5. To authenticate to the BIG-IP system using clientless HTTP authentication, type values for these parameters.
   a) For `IFMapUsername`, type the name of the user that logs on to the IF-MAP server on behalf of the F5 DC Agent.
   This is the name of a user you created in the local user database on the BIG-IP system.
   b) For `IFMapPassword`, type the password for the user.
   This is the password you typed in the local user database.
6. (Optional) To authenticate using a certificate, for `IFMapCertClient`, type the path to the SSL certificate file to use for authenticating to the BIG-IP system.
   This must match the name of the certificate you specified in the application service on the BIG-IP system. Make sure that this certificate is imported into the certificate store on the BIG-IP system.
7. For the remainder of the parameters, you can retain the default values or change them.

a) For `IFMapLifeTimeType`, retain the default value, *`forever`*.

`IFMapLifeTimeType` specifies whether to keep or purge a user entry from the IF-MAP server when a session ends or times out. The alternative value is *`session`*.

Note: *You can specify an absolute lifetime for a user entry in the* `IPCleanLifetime` *property.*

---

b) For `PurgeOnStart`, retain the default value, *`true`*.

`PurgeOnStart` specifies whether the IF-MAP server should purge user records after the F5 DC Agent restarts.

c) For `IdleUpdate`, you can retain the default value of *`120`* seconds.

`IdleUpdate` specifies the interval between keep-alive pings from the F5 DC Agent to the IF-MAP server.

d) For `DiscoveryInterval`, retain the default value of *`84600`* seconds (24 hours).

`DiscoveryInterval` specifies the interval at which the domain auto-discovery process runs.

e) For `DC AgentEnable`, retain the default value of *`true`*.

`DC AgentEnable` specifies whether domain auto-discovery is enabled (*`true`*) or disabled (*`false`*).

f) For `QueryInterval`, you can retain the default value of *`10`* seconds.

`QueryInterval` specifies the interval at which the F5 DC Agent queries domain controllers in seconds. Valid values are between 5 and 90 seconds.

g) For `IPCleanLifetime`, you can retain the default value of *`7200`* seconds (2 hours).

`IPCleanLifetime` specifies the amount of time a user entry remains in the IF-MAP server before it is removed, in seconds. Valid values are integers greater than 3600; specify 0 to disable.

8. Start or restart the F5 DC Agent service.

The F5 DC Agent discovers domain controllers and starts to send user identity information to the BIG-IP system.

Configuring domain controller polling in the dc_agent.txt file

After the F5® DC Agent starts for the first time, it might take a few minutes to complete domain discovery and to write the list of domains and domain controllers into the `dc_agent.txt` file. If the F5 DC Agent does not create a `dc_agent.txt` file, you can create one manually; refer to the examples in this task.

You configure the list of the domains and domain controllers that F5 DC Agent polls to ensure that the list is accurate and complete. If you installed more than one F5 DC Agent, you edit the `dc_agent.txt` file on each Windows-based server to ensure that each domain controller is queried by one F5 DC Agent only.

1. Log on to the Windows-based server where you installed the F5® DC Agent.

2. Navigate to this directory: `C:\Program Files\F5 Networks\User Identity Agents\`.

3. If the `dc_config.txt` file already exists, make a backup copy in another location.

4. Create or open the `dc_config.txt` file using a text editor.

5. Verify that all domains and controllers are on the list.
This example shows two domain controller entries in each of two domains, WEST_DOMAIN and EAST_DOMAIN; polling is enabled on each domain controller. Note the blank line at the end of the file; it is required.

```
[WEST_DOMAIN]
dcWEST1=on
dcWEST2=on
[EAST_DOMAIN]
dcEAST1=on
dcEAST2=on
```

6. If domains or domain controllers are missing, add them.

   To make sure that F5 DC Agent can see a domain, run the `net view /domain` command before you add the domain.

7. If the list contains domain controllers that F5 DC Agent should not poll, change the entry value from *`on`* to *`off`*.

   If you configure F5 DC Agent to avoid polling an active domain controller, the agent cannot transparently identify the users that log on to it.

   Important: *Rather than deleting a domain controller, change the setting to `off`. Otherwise, F5 DC Agent adds it to the file again after it next discovers domain controllers.*

   In this example, polling is disabled for the `dcEAST2` domain controller.

```
dcEAST2=off
```

8. Make sure that the file includes a carriage return after the last entry, creating a blank line at the end of the file.

   If you do not include the hard return, the last entry in the file get truncated, and an error message is written.

9. Save the changes and close the file.
10. Use the Windows Services dialog box to restart the F5 DC Agent service.

Recovering from an unsuccessful installation

To install F5® DC Agent correctly, first remove any failed installations and then install.

1. Log on to the Windows-based server from a user account with local and domain administrator privilege.
2. From the Windows Programs and Features dialog box, uninstall the F5 Installer application.
3. From Windows Explorer, click the `SWGUserIdentificationAgents.exe` file and follow the instructions to install F5 DC Agent again.

Enabling debug logging for the F5 DC Agent

When you are troubleshooting, you might want debug errors to be logged.

1. Log on to the Windows-based server where you installed the F5® DC Agent.
2. Navigate to this directory: `C:\Program Files\F5 Networks\User Identity Agents\config`.
3. Using a text editor, open the `diagnostics.cfg` file.
4. Look for `log4j.threshold` in Global configuration.
5. Note the value for `log4j.threshold`; you will need it when you complete troubleshooting tasks.
6. Modify the value to `DEBUG`.

7. Restart the DC agent service.
   Debug errors start to be logged.
8. When you are done with troubleshooting, edit the `diagnostics.cfg` file, reset `log4j.threshold` to the previous value, and restart the DC agent service.

Troubleshooting when a user is identified incorrectly

Troubleshooting is critical if you suspect or determine that a user is not being correctly identified.

1. Log on to the client system that belongs to the user.
2. Open a browser and navigate to four or more distinctive web sites.
3. Log on to the Windows-based server where the F5® DC Agent is installed.
4. Look for error messages in the Windows Event Viewer.
5. Proceed based on any error messages that you discover.

F5 DC Agent error messages

Error messages from the F5® DC Agent display in the Event Viewer on the Windows-based server where DC Agent is installed.

Error code	Error message	Possible causes
3	`Could not configure DC Agent (Code 3)`	An attempt was made to install F5 DC Agent using an account that does not have domain and local administrator privileges. As a result, some required files are not installed properly, and F5 DC Agent service cannot run.
5	`ERROR_ACCESS_DENIED`	F5 DC Agent service does not have sufficient permissions to perform required tasks. This error can occur when: • A `NetSessionEnum` call from F5 DC Agent fails due to Local Security Policy or Trust Relationship configurations. • F5 DC Agent uses an anonymous account and the domain controller is configured to not give the list of user logon sessions to an anonymous user.
53	ERROR_BAD_NETPATH	A network problem prevents F5 DC Agent from contacting a domain controller. This error can occur when: • Windows Remote Registry Service is not running on the Windows server with the agent • NetBIOS is not bound to the network adapter on the Windows server • The Windows server and the domain controller use different network protocols for communication • The Windows-based server cannot communicate with the domain controller or with the BIG-IP® system possibly because of a problem with network connection or with placement within the network. • Remote administration is not enabled on the domain controller.

Error code	Error message	Possible causes
71	`System error while enumerating the domain controllers. domain: (****)ecode: 71 : message: No more connections can be made to this remote computer at this time because there are already as many connections as the computer can accept.`	The error results from F5 DC Agent automatic domain discovery process, used to identify new domains and domain controllers. It can also occur when F5 DC Agent tries to connect to a Windows XP-based computer that is broadcasting itself as the master browser for a non-company domain or workgroup. Although the issue might indicate a problem with connectivity to the domain controller, it is more likely that the domain is a workgroup with no domain controllers. This error can be ignored.
997	`Error Code 997`	An attempt was made to install F5 DC Agent using an account that does not have domain and local administrator privileges. As a result, some required files are not installed properly, and F5 DC Agent service cannot run.
1058	`Error Code 1058`	This error is seen on startup. A Local Security Policy on the Windows-based server might have disabled the F5 DC Agent service.

Overview: Identifying users transparently using F5 Logon Agent

The F5® Logon Agent enables *transparent user identification*, a best effort to identify users without requesting credentials.

You can install the F5 Logon Agent on a Windows-based server in any domain in the network. The F5 Logon Agent identifies users in real time when the users log on to domains, which prevents missing a user logon because of a query timing issue. F5 Logon Agent sends up-to-date session information to the BIG-IP® system.

Note: *F5 Logon Agent does not transmit passwords or any other confidential information.*

F5 Logon Agent identification process

1. When users log on to the network, a network logon script invokes the logon application (`LogonApp.exe`).
2. The logon application contacts F5 Logon Agent using HTTP.
3. F5 Logon Agent sends an NTLM authentication challenge, and the logon application provides a user name, hashed password, and IP address to F5 Logon Agent.
4. F5 Logon Agent verifies the username and password combination from the logon application by establishing a session with the domain controller. (F5 Logon Agent contacts User Service to determine which domain controller is the logon source.)
5. After verifying the user name and IP address pair, F5 Logon Agent sends the information to the BIG-IP system and adds an entry to its user map in local memory. The user map is periodically saved to a backup file, `AuthServer.bak`.
6. The BIG-IP system records user name and IP address pairs to the BIG-IP system copy of the user map in local memory. Confidential information (such as user passwords) is not sent to the BIG-IP system.

Considerations for installing multiple agents

You can install more than one F5 Logon Agent in your network, and configure F5 Logon Agents to communicate with the same BIG-IP system. If you have multiple BIG-IP systems, each BIG-IP system must be able to communicate with every F5 Logon Agent in your network.

NetBIOS port 139

F5 Logon Agent uses NetBIOS port 139 for automatic domain detection. If NetBIOS port 139 is blocked in your network, you can deploy an F5 Logon Agent instance for each virtually or physically remote domain.

Multiple subnets

As a best practice, install a separate F5 Logon Agent in each subnet to avoid problems gathering logon information from domain controllers.

Network size, disk space, and RAM

If your network is very large (10,000+ users or 30+ domain controllers), you might benefit from installing F5 Logon Agent on multiple machines to evenly distribute resource usage.

Task summary

Configuring the BIG-IP system for the F5 Logon Agent
Verifying network communication
Downloading and installing F5 Logon Agent
Updating privileges for the F5 Logon Agent service
Configuring the initialization file
Recovering from an unsuccessful installation
Enabling debug logging for the F5 Logon Agent
Troubleshooting when a user is identified incorrectly

Configuring the BIG-IP system for the F5 Logon Agent

You use an iApps® template to deploy an application service that configures objects that the F5® Logon Agent uses to communicate with the IF-MAP server on the BIG-IP® system.

Note: *You can configure the F5 Logon Agent to authenticate with the BIG-IP system using certificate inspection or using clientless HTTP basic authentication against a local user database.*

---

1. Set up to support certificate inspection:
   a) Obtain a trusted certificate and key that are valid for all fully qualified domain names (FQDNs) used to access the BIG-IP system.
   b) Import the certificate and key into the BIG-IP system.
      You can import SSL certificates from the System area of the product.
2. Obtain the IF-Maps iApps template file from F5® DevCentral™at `http://devcentral.f5.com/wiki/iapp.Codeshare.ashx`.
3. Import the template:
   a) On the Main tab, click **iApps** > **Templates**.
   b) Click **Import**.
   c) Select the **Overwrite Existing Templates** check box.
   d) Click **Browse**, then browse to and select the template file.
   e) Click **Upload**.

4. Deploy an application service:
   a) On the Main tab, click **iApps** > **Application Services**, and then click **Create**.
   b) In the **Name** field, type a name.

   Note: *The application service prefixes this name to the names of configuration objects it creates.*

   c) From the **Template** list, select **f5.ifmap**.

   Note: *This iApps template displays on the list only when APM is provisioned.*

   d) Follow the instructions on the screen to complete the deployment.
   A summary displays the configuration objects.
   e) Take note of the IP address of the virtual server created by the service. You need to type it into F5 Logon Agent initialization file later.

   Note: *This virtual server must be accessible by the F5 Logon Agent from a routing perspective.*

5. To enable clientless HTTP basic authentication, create a user and password in the local user database.
   The purpose of this user account is to authenticate communication between the F5 Logon Agent and the BIG-IP system.
   a) On the Main tab, click **Access Policy** > **Local User DB** > **Manage Users**.
   The Manage Users screen displays.
   b) Click **Create New User**.
   The Create New Local User screen opens and displays User Information settings.
   c) From the **Instance** list, select the instance created when you deployed the application service.
   d) In the **User Name** field, type the user name.
   Take note of the user name and password. You need to type them again later when you configure the initialization file for F5 Logon Agent.
   e) In the **Password** and **Confirm Password** fields, type the user's password.

Verifying network communication

You can verify that there are no DNS or NetBIOS or network communications issues on a Windows-based server before you install the F5® Logon Agent on it. Alternatively, you can use these steps for troubleshooting if you observe a problem.

1. Open a command prompt on the Windows-based server that hosts, or will host, the F5 Logon Agent.
2. To verify that the Windows-based server sees all required domains, use the `net view` command.
   For example, type `net view /network`.
3. To check for DNS issues, use the `nslookup` command.
   For example, to verify that DNS resolves the host name, `testmachine1`, type this command: `nslookup testmachine1` . If the DNS lookup succeeds, the result is similar to: `Server: testdns.test.example.com Address: 10.56.1.4 Name: testmachine1.test.example.com Address: 10.56.100.15`
4. To verify that F5 Logon Agent will be able to use NetBIOS, try to open a Telnet session to a domain controller on port `139`.
   If the command is successful, the screen remains blank. If unsuccessful, then:
   - A a router, firewall, or other device might be blocking NetBIOS traffic.

- NetBIOS might not be enabled and the domain controller might not be listening on port `139`.

5. If you could not successfully use a Telnet connection to a domain controller on port `139`, verify the status of the port using the `netstat` command.
   For example, type `netstat -na | find"139"`.)
6. To verify that the F5 Logon Agent will be able to communicate with the virtual server on the BIG-IP system, use a Telnet connection to the IP address of the virtual server on port `8096` or on the port that you entered when creating the application service.
   This virtual server was created using an application service based on the `f5.ifmap` iApps® template.

Downloading and installing F5 Logon Agent

F5® Logon Agent is available when Access Policy Manager® (APM®) is licensed and provisioned on the BIG-IP® system. Before you perform these steps, make sure that the Windows Computer Browser service is running on the Windows server where you plan to install F5 Logon Agent.

You perform this task to be able to identify clients transparently by IP address. (Do this only in an environment where IP addresses are trusted and unique.)

1. Go to the BIG-IP Configuration utility Welcome screen.
   If you are already logged in, click the F5® logo to open the Welcome screen.
2. In the Secure Web Gateway User Identification Agents area, click the **User Identification Agents** link. A `SWGUserIdentificationAgents.exe` file downloads.
3. Copy the downloaded file to a Windows-based server that is joined to a domain controller.

   Important: *Do not install F5 Logon Agent on a domain controller because the F5 Logon Agent can put a load on the domain controller.*

4. From an account with both local and administrator privileges, click the `SWGUserIdentificationAgents.exe` file to start the installer.
   The installer displays instructions.
5. Follow the instructions to complete the installation.

   Important: *F5® strongly recommends that you use the default destination folder. On the Destination Folder screen, click* ***Next*** *without making any changes.*

   Important: *Install either F5 DC Agent or F5 Logon Agent, but not both. This overwrites the omapd user map every time an update is published.*

   The program installs a Windows service, F5 Logon Agent.

Updating privileges for the F5 Logon Agent service

The F5® Logon Agent service must run from a privileged account. You can create a new user account or use an existing account configured as specified in step 1.

1. On the Windows-based server, create a user account for F5 Logon Agent:
   a) Assign the new account domain administrator privileges in all domains.

b) Assign the same password to this account in all domains.
Make a note of the password. You must type it again in step 2.

c) Set the password to never expire.

2. Configure the F5 Logon Agent service to log on as the user account you just configured:
   a) Open the Windows Services dialog box.
   From the Control Panel, select **Administrative Tools** > **Services**.
   b) Locate the F5 Logon Agent service, right-click the service name, and select **Stop**.
   c) Double-click the service name, and then select the Log On tab.
   d) Select **This account** and type the account name and password for the account you created in step 1.

   Note: *Some domains require that you type the account name in the format domain\username.*

   e) Close the Services dialog box.

Start the F5 Logon Agent service again after the initialization file configuration is complete.

Configuring the initialization file

Before you can configure the initialization file, you must have the F5® Logon Agent installed on a domain-joined, Windows-based server. You must also have deployed an iApps® application service to configure objects that enable communication between the F5 Logon Agent and the BIG-IP® system.

Note: *This task requires you to enter some values that are available as a result of completing the prerequisites.*

You configure an initialization file for the F5 Logon Agent so that it can send IP address and user name pairs to the BIG-IP system.

1. Log on to the Windows-based server where you installed the F5® DC Agent.
2. Navigate to this directory: `C:\Program Files\F5 Networks\User Identity Agents\config`.
3. Using a text editor, open the `authserver.ini` file.
   The file contains one section, [Logon Agent].
4. For `IFMapServer`, type the protocol, host address, and port for the server.
   This is the virtual server that was created by the application service. Port `8096` is the default port. You might have specified another port number when you deployed the application service.
   For example, `IFMapServer=https://AA.BB.CC.DD:8096`, where *AA.BB.CC.DD* is the IP address of the virtual server created by the application service.
5. To authenticate to the BIG-IP system using clientless HTTP authentication, type values for these parameters.
   a) For `IFMapUsername`, type the name of the user that logs on to the IF-MAP server on behalf of the F5 Logon Agent.
   This is the name of a user you created in the local user database on the BIG-IP system.
   b) For `IFMapPassword`, type the password for the user.
   This is the password you typed in the local user database.
6. (Optional) To authenticate using a certificate, for `IFMapCertClient`, type the path to the SSL certificate file to use for authenticating to the BIG-IP system.

This must match the name of the certificate you specified in the application service on the BIG-IP system. Make sure that this certificate is imported into the certificate store on the BIG-IP system.

7. For the remainder of the parameters, you can retain the default values or change them.
   a) For `IFMapLifeTimeType`, retain the default value, *`forever`*.

      `IFMapLifeTimeType` specifies whether to keep or purge a user entry from the IF-MAP server when a session ends or times out. The alternative value is *`session`*.

      Note: *You can specify an absolute lifetime for a user entry in the* `IPCleanLifetime` *property.*

   b) For `PurgeOnStart`, retain the default value, *`false`*.

      `PurgeOnStart` specifies whether the IF-MAP server should purge user records after the F5 Logon Agent restarts.

   c) For `IdleUpdate`, you can retain the default value of *`120`* seconds.

      `IdleUpdate` specifies the interval between keep-alive pings from the F5 Logon Agent to the IF-MAP server.

   d) For `QueryInterval`, you can retain the default value of *`900`* seconds.

      `QueryInterval` specifies the interval at which the F5 Logon Agent queries domain controllers in seconds. Valid values are between 5 and 90 seconds.

   e) For `EntryLifetime`, retain the default value of *`86400`* seconds.

      `EntryLifetime` specifies the interval at which the domain auto-discovery process runs.

   f) For `ReconfigPeriod`, you can retain the default value of *`60`* seconds.

      `ReconfigPeriod` specifies the amount of time between agent reconfiguring during an initialization file update.

   g) For `LogonAgentIP`, type the address.

      `LogonAgentIP` specifies the address that the server should bind to.

   h) For `LogonAgentPort`, you can retain the default value of *`15880`* seconds.

      `LogonAgentPort` specifies the TCP/IP Port that the agent should listen on.

8. Start or restart the F5 Logon Agent service.

The F5 Logon Agent discovers domain controllers and starts to send user identity information to the BIG-IP system.

Recovering from an unsuccessful installation

You install F5® Logon Agent correctly by first removing any failed installations, and then installing.

1. Log on to the Windows-based server from a user account with local and domain administrator privilege.
2. From the Windows Programs and Features dialog box, uninstall the F5 Installer application.
3. From Windows Explorer, click the `SWGUserIdentificationAgents.exe` file and follow the instructions to install F5 Logon Agent again.

Enabling debug logging for the F5 Logon Agent

When you are troubleshooting, you might want debug errors to be logged.

1. Log on to the Windows-based server where you installed the F5® DC Agent.
2. Navigate to this directory: `C:\Program Files\F5 Networks\User Identity Agents\`.
3. Using a text editor, open the `diagnostics.cfg` file.
4. Look for `log4j.threshold` in Global configuration.
5. Note the value for `log4j.threshold`; you will need it when you complete troubleshooting tasks.
6. Modify the value to `DEBUG`.
7. Restart the Logon Agent service.
   Debug errors start to be logged.
8. When you are done with troubleshooting, edit the `diagnostics.cfg` file, reset `log4j.threshold` to the previous value, and restart the Logon Agent service.

Troubleshooting when a user is identified incorrectly

Troubleshooting is critical if you suspect or determine that a user is not being correctly identified.

1. Log on to the client system that belongs to the user.
2. Open a browser and navigate to four or more distinctive web sites.
3. Log on to the Windows-based server where the F5® Logon Agent is installed.
4. Look for error messages in the Windows Event Viewer.
5. Proceed based on any error messages that you discover.

Files used by Logon Agent

This table explains the relevant files used by F5 Logon Agent after you install the installation file from the BIG-IP® system Configuration utility Welcome screen.

Filename	File location	Additional information
`LogonApp.exe`	Stored in User Identity Agents > LogonApp > Windows folder.	Sends user information to F5 Logon Agent Captures user logon sessions as they occur. Runs on Windows client machines.
`logon.bat`	Stored in User Identity Agents > LogonApp > Windows folder.	Invokes `LogonApp.exe`, which runs on client machines and captures logon sessions.
`AuthServer.ini`	Stored in User Identity Agents > config folder.	Contains one initialization parameter for Logon Agent.

Overview: Creating a script on a Windows system for F5 Logon Agent

When you install the F5® Logon Agent, you must create a logon script for clients that identify the clients to the BIG-IP system when they log on to a Windows domain. The application, LogonApp.exe, provides a

username and IP address to F5 Logon Agent each time a Windows client connects to a Windows Active Directory or a Windows NT directory service.

When installing F5 Logon Agent, the following files are placed in the F5 Networks folder (by default, `C:\Program Files\F5 Networks\User Identity Agents\LogonApp`):

- LogonApp.exe
- logon.bat

Task summary

Creating a logon or logout script
Running a logon or logout script on Active Directory

Creating a logon or logout script

When you install F5 Logon Agent on a Windows system, the installation stores a batch file, logon.bat, in your local User Identity Agents directory. The batch file contains instructions for using scripting parameters and two sample scripts: a logon script that runs LogonApp.exe, and a logout script that removes user information from the BIG-IP system when a user logs out. You can create a logon or logout script from the logon.bat examples.

1. On your Windows screen, click **Start** > **Accessories** > **Notepad**
2. In the untitled Notepad menu, click **File** > **Open**
3. Navigate to the directory with the logon.bat file. For example:`C:\Program Files\F5 Networks\User Identity Agents\LogonApp\Windows\logon.bat`.
   The .bat file displays logon script examples.
4. Open a new Notepad file.
5. Using the examples in logon.bat, create a script for either F5 Logon Agent logon or logout options.
6. Click **Save** and select .bat as the file extension.

You have created a logon or logout script

Running a logon or logout script on Active Directory

You must create a script before you can run it on Active Directory.

You can configure your logon or logout script to run with a group policy on Active Directory.

1. On the Active Directory machine, click **Control Panel**.
   The Control Panel window displays.
2. From the window, select **Administrative Tools** > **Active Directory Users and Computers**.
3. Right-click the domain and select **Properties**.
4. On the Group Policy tab, click **New**.
5. In the New Group Policy screen, create a new policy.
6. Click **Edit**.
   A window displaying a tree structure displays.
7. Expand **User Configuration**.
8. For Windows Settings option, click **Scripts (Logon/Logoff)**.
9. On the right screen, double-click **Logon**.
10. Click **Show Files**.

The folder that contains the logon script opens in Windows Explorer.

11. Copy the files `logon.bat` and `LogonApp.exe` to the folder.
12. Close the Windows Explorer window.
13. In the Logon Properties dialog box, click **Add**.
14. For the **Script Name** field, type `logon.bat`.
15. Click **OK**.
16. In the domain Properties dialog box, click **OK**.

You have configured your logon or logout script to run with a group policy on Active Directory.

Logon and logout script parameters

This table explains the relevant parameters used by a logon or logout script for F5 Logon Agent.

Parameter	Description
<server>	The IP address of the BIG-IP system F5 Logon Agent.
<port>	The port number used by F5 Logon Agent. The default value is 15880.
/NOPERSIST	Triggers the logon application to send user information to F5 Logon Agent only at logon. The username and IP address are communicated to the server during the logon process and remain in the F5 Logon Agent user map until the user data is automatically cleared at a predefined time interval. The default user entry expiration is 24 hours. If the NOPERSIST parameter is omitted, LogonApp.exe operates in persistent mode, located in the memory of the domain server and updates F5 Logon Agent with the usernames and IP addresses at predefined intervals. The default interval is 15 minutes. The following example logon script sends user information to F5 logon Agent at the logon step only. The information is not updated during the user's session (NOPERSIST). The information is sent to port 15880 on the server identified by IP address 10.2.2.95. `LogonApp.exe http://10.2.2.95:15880 /NOPERSIST`
/COPY	Copies the logon application to the `%USERPROFILE%\Local Settings\Temp` directory on the user machine, where the logon script runs it from the local memory. This optional parameter helps prevent your logon script from hanging. COPY can be used only in persistent mode.
/VERBOSE	A debugging parameter that can be used only with help from technical support.

Parameter	Description
/LOGOUT	Used only in an optional logout script, this parameter removes the user's logon information from the F5 Logon Agent user map when the user logs off. If you use Active Directory, this parameter can clear the logon information from the user map before the interval that is defined for F5 Logon Agent has elapsed. Use this optional parameter in a logout script in a batch file that is different than the one containing the logon script. The following example logout script clears the logon information for each user as soon as the user logs out. `LogonApp.exe http://10.2.2.95:15880 /NOPERSIST /LOGOUT`

Chapter 4

Per-Request Policy Concepts and Examples

- *Exporting and importing a per-request policy across BIG-IP systems*
- *About access and per-request policies*
- *Category-specific access control example*
- *Per-flow variables*
- *Session variables for use in a per-request policy*
- *About per-request policy items*
- *About per-request policy endings*
- *Customizing messages for URL filter denied*

Exporting and importing a per-request policy across BIG-IP systems

Export a per-request policy from one BIG-IP® system and import it on another (at the same product version level) to copy a policy across systems.

Note: *Before you import a per-request policy from one BIG-IP system to another BIG-IP system, you must first list any custom categories configured on the source system and make sure you have the same custom categories on the target system. Otherwise, import will fail.*

1. On the Main tab, click **Access Policy** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. Click the link in the **Export** column for the policy that you want to export.
   A file downloads.
3. Note the list of custom categories:
   a) Click **Access Policy** > **Secure Web Gateway** > **URL Categories**.
   b) Expand the Custom Categories list.
4. Log in to the Configuration utility on the BIG-IP system where you want to import the per-request policy.
5. Verify that the custom categories that exist on the other BIG-IP system also exist on this BIG-IP system:
   a) Click **Access Policy** > **Secure Web Gateway** > **URL Categories**.
   b) Expand the Custom Categories list.
   c) Create any additional custom categories needed to match the list on the other BIG-IP system.
6. On the Main tab, click **Access Policy** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
7. Click **Import**.
   An Import Policy screen displays.
8. In **New Policy Name**, type a name.
9. For **Config File Upload**, click **Browse**, locate and select the file downloaded from the other BIG-IP system.
10. To reuse objects already existing on this BIG-IP system, select the **Reuse Existing Objects** check box.
11. Click **Import**.

About access and per-request policies

BIG-IP® Access Policy Manager® Secure Web Gateway (SWG) uses two types of policies.

Access policy

The access policy runs when a client initiates a session. Depending on the actions you include in the access policy, it can authenticate the user and perform group or class queries to populate session variables with data for use throughout the session. It must also specify the SWG scheme to apply to the session.

Per-request policy
After a session starts, a *per-request policy* runs each time the client makes an HTTP or HTTPS request. A per-request policy must provide the logic for determining how to process web-bound traffic. It must determine whether to allow or reject a URL request and control whether or not to bypass SSL traffic.

An access policy and a per-request policy are both specified in a virtual server.

About per-request policy configuration

A per-request policy can be configured with policy items that support these types of branches and actions.

Branch by protocol, date, time, user group or class
Policy items are available for each type of branch. Protocol lookup can branch to HTTP or HTTPS. Group or class lookup items compare strings that you specify against session variables.

Set the SSL bypass action
The SSL Intercept Set and SSL Bypass Set items set the SSL filter to intercept or bypass SSL traffic. This works in a configuration where SSL forward proxy and SSL forward proxy bypass are enabled in client and server SSL profiles on the virtual server.

Look up categories, enable Safe Search
The Category Lookup item does lookups based on URL for an HTTP request or host name for an HTTPS request. It can also enable Safe Search for HTTP requests.

Analyze response content
A Response Analytics item triggers content analysis of the response web page that the Category Lookup item returns.

Apply URL filters
A URL Filter Assign item assigns a URL filter to apply on the categories that the Category Lookup item found.

About per-request policies and SWG logging and reports

Unless a per-request policy includes and executes a Category Lookup item, Secure Web Gateway (SWG) event logging does not occur and there is no data for reports.

About Safe Search and supported search engines

Safe Search is a search engine feature that can prevent offensive content and images from showing up in search results. Safe Search can also protect video searches on Google, Bing, and Yahoo search engines.

Safe Search can be enabled in a per-request policy using the Category Lookup item. Secure Web Gateway (SWG) with Safe Search enabled supports these search engines: Ask, Bing, DuckDuckGo, Google, Lycos, and Yahoo.

Note: *Some search engines, such as Google and Yahoo, use SSL by default. In this case, Safe Search works only when SWG is configured with SSL forward proxy.*

Access and per-request policy comparison

The table summarizes access policy and per-request policy similarities and differences.

Feature	Access policy	Per-request policy
Configuration tool	The visual policy editor.	The visual policy editor.
Macros	Available in visual policy editor.	Not available.
Policy action items	Vary by access profile type.	Small set of items that are unique to a per-request policy.
Apply Access Policy link	Saves the access policy configuration.	Not applicable.
Profile	Access profile.	Not applicable.
Virtual server	Specified in the access profile setting.	Specified in the per-request policy setting.
Access type support	Most.	For use in Secure Web Gateway configurations only.
When run	At session start.	After session is created, on every request.
Policy ending types	Allow, Deny, Redirect; endings apply to the session.	Allow, Reject; endings apply to URL requests processed in the per-request policy. A Reject ending triggers the Deny ending in the access policy.
Session variables	Creates session variables that are available throughout a session.	Reads session variables as specified in policy items.
Per-flow variables	Not applicable.	Creates per-flow variables that are available only while the per-request policy runs.

Category-specific access control example

In this per-request policy example, only recruiters are allowed to access URLs in the job search category. The policy also restricts access to entertainment sites during business hours.

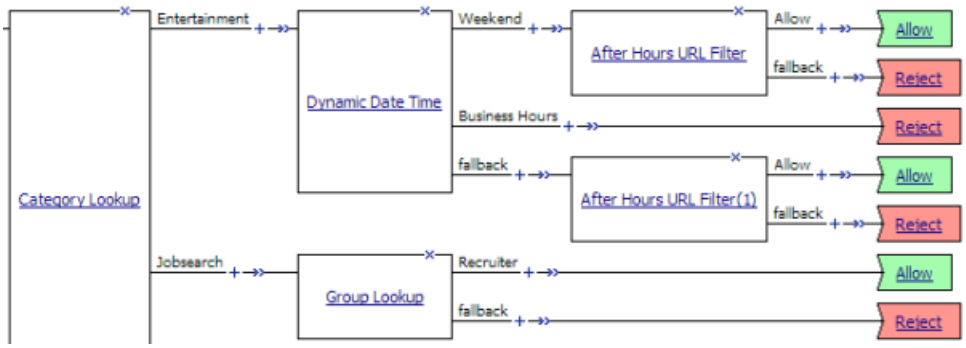

Figure 3: Category-specific access restrictions

Access for date, time, and user group example

This per-group policy example applies specific URL filters for weekends and weeknights, and restricts access during work hours based on user group.

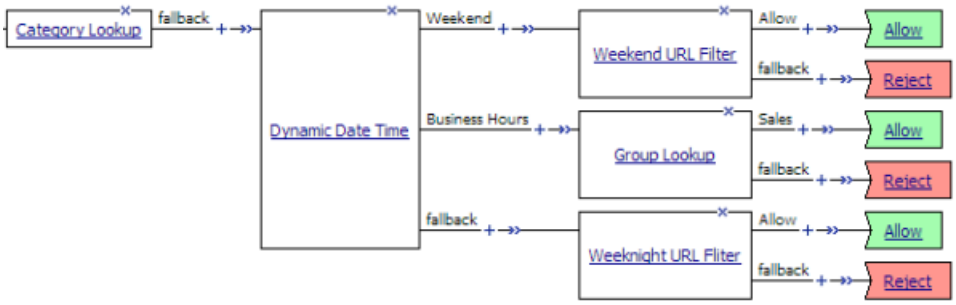

Figure 4: Deny or allow access based on date and time and group membership

URL filter per user group example

Each URL Filter Assign item in this per-request policy example should specify a filter that is applicable to the user group.

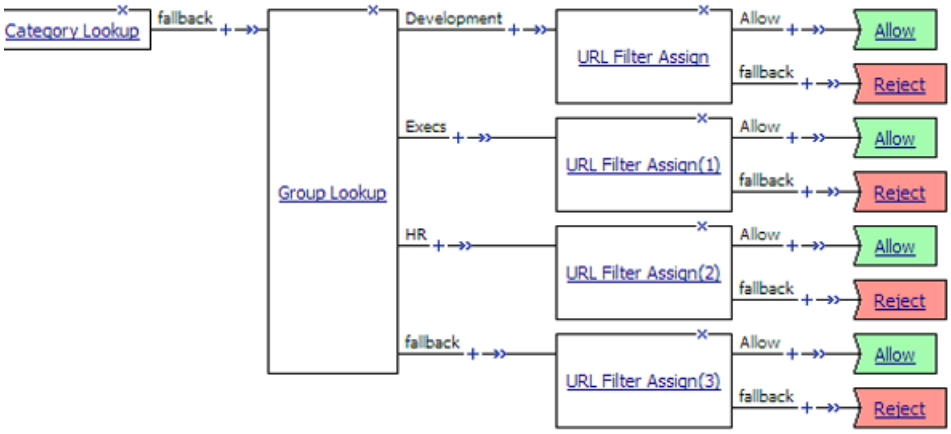

Figure 5: URL filter based on group membership

SSL intercept and bypass set example

In this example per-request policy, some SSL traffic is bypassed in consideration of the user group or the URL category. Other SSL traffic is rejected or allowed after applying a URL filter.

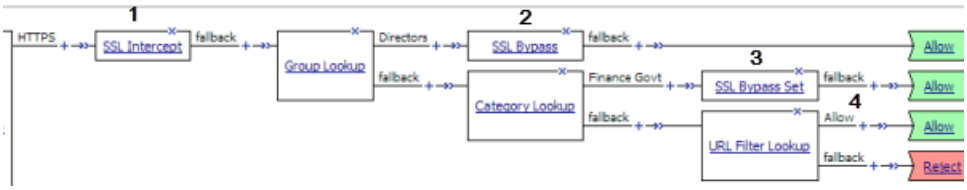

Figure 6: SSL bypass decision based on group membership and URL category

1	On the HTTPS branch after a Protocol Lookup item (not shown), set the SSL bypass action to intercept. Ensuring the SSL bypass action is set to intercept before a category lookup is good practice, particularly if the default SSL bypass action in the client SSL profile is not set to intercept.
2	For directors, do not intercept and inspect any SSL request. The SSL Bypass Set item sets the value of the action to bypass.
3	For others, do not intercept and inspect SSL requests that contain private information. Similarly, the SSL Bypass Set item sets the value of the action to bypass.
4	For SSL requests that do not contain private information, because SSL Intercept Set occurred earlier on the branch, SSL traffic is intercepted. Apply a URL filter to determine whether to allow or reject traffic.

Response Analytics example

In this example per-request policy, after a Category Lookup item obtains a list of categories and a response web page, a Response Analytics item scans the response for malicious embedded content and passes the analysis to the URL filter assign item.

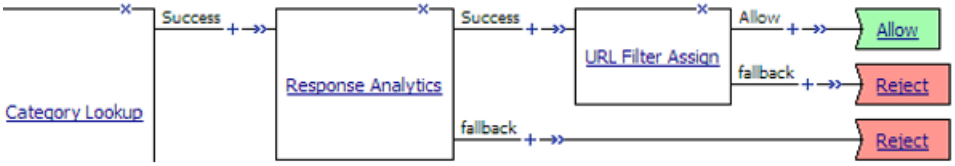

Figure 7: Process of Response Analytics contributing analysis results to URL filter assign

Per-flow variables

Per-flow variables exist only while a per-request policy runs. The table lists per-flow variables and their values.

Name	Value
`perflow.agent_ending.result`	`0` (success) or `1` (failure).
`perflow.category_lookup.failure`	`0` (success) or `1` (server failure).
`perflow.category_lookup.result.categories`	Comma-separated list of categories.
`perflow.category_lookup.result.customcategory`	Unique number that identifies a custom category; used internally.
`perflow.category_lookup.result.effective_category`	Name of the category that is ultimately used.
`perflow.category_lookup.result.filter_name`	Name of the URL filter.

Name	Value
perflow.category_lookup.result.hostname	Host name retrieved from SSL input.
perflow.category_lookup.result.numcategories	Integer. Total number of categories in the comma-separated list of categories.
perflow.category_lookup.result.primarycategory	Name of the category that SWG determines is the primary one. (A URL might fit into more than one category, such as news and sports.)
perflow.category_lookup.result.url	Requested URL.
perflow.protocol_lookup.result	http or https. Defaults to https.
perflow.response_analytics.failure	0 (success) or 1 (server failure).
perflow.session.id	Session id.
perflow.ssl_bypass_set	0 (bypass) or 1 (intercept). SSL Bypass Set and SSL Intercept Set items update this value.
perflow.ssl.bypass_default	0 (bypass) or 1 (intercept). Specified in the client SSL profile, used when SSL Bypass Set and SSL Intercept Set items not included in per-request policy.
perflow.swg_scheme_name	Scheme name as set in access policy.
perflow.urlfilter_lookup.result.action	0 (reject) or 1 (allow).
perflow.username	User name.

Session variables for use in a per-request policy

Per-request policy items that look up the group or class to which a user belongs rely on the access policy to populate these session variables.

Per-request policy item	Session variable	Access policy item
AD Group Lookup	session.ad.last.attr.primaryGroupID	AD Query
LDAP Group Lookup	session.ldap.last.attr.memberOf	LDAP Query
LocalDB Group Lookup	session.localdb.groups ***Note:*** *This session variable is a default in the expression for LocalDB Group Lookup; any session variable in the expression must match the session variable used in the Local Database action in the access policy.*	Local Database
RADIUS Class Lookup	session.radius.last.attr.class	RADIUS Auth

About per-request policy items

When configuring a per-request policy, a few access policy items are available for inclusion in the policy. Most per-request policy items are unique to a per-request policy.

About Protocol Lookup

A Protocol Lookup item determines whether the protocol of the request is HTTP or HTTPS.

About SSL Intercept Set

In a per-request policy, the SSL Intercept Set item sets the SSL bypass action to **Intercept**. Including this item early in the policy ensures that SSL traffic is not bypassed until the policy reaches an SSL Bypass Set item.

A default action for SSL bypass (intercept or bypass) is specified in the client SSL profile.

Important: *F5® recommends that the SSL forward proxy bypass default action be set to intercept SSL traffic.*

The SSL Intercept Set item provides a read-only element, **Action**, that specifies the **Intercept** option.

About Category Lookup

A Category Lookup item looks up URL categories for a request and obtains a web response page.

The Category Lookup item provides these elements and options.

Categorization Input

The list specifies these options:

- **Use HTTP URI (cannot be used for SSL Bypass decisions)**: For HTTP traffic, this option specifies performing a URL-based lookup. When selected, the **SafeSearch Mode** setting displays.
- **Use SNI in Client Hello (if SNI is not available, use Subject.CN)**: For HTTPS traffic, this option specifies performing a host-based lookup.
- **Use Subject.CN in Server Cert**: For HTTPS traffic, this option specifies performing a host-based lookup.

SafeSearch Mode

The options are **Enabled** (default) and **Disabled**. When enabled, SWG enables Safe Search for supported search engines.

Category Lookup Type

Select the category types in which to search for the requested URL. Options are:

- **Select one from Custom categories first, then standard categories if not found**
- **Always process full list of both custom and standard categories**
- **Process standard categories only**

Depending on your selection, the Category Lookup Type item looks through custom categories or standard categories or both, and compiles a list of one or more categories from them. The list is available for subsequent processing by the URL Filter Assign item.

Reset on Failure

When enabled, specifies that SWG send a TCP reset to the client in the event of a server failure.

About Response Analytics

A Response Analytics item inspects a web response page for malicious embedded contents. Response Analytics must be preceded by a Category Lookup item because it obtains a web response page.

Response Analytics provides these elements and options.

Max Buffer Size
Specifies the maximum amount of response data (in bytes) to collect before sending it for content scanning. The system sends the content for analysis when the buffer reaches this size or when the buffer contains all of the response content. Otherwise, the system retains the response data in the buffer.

Max Buffer Time
Specifies the maximum amount of time (in seconds) to retain response data in the buffer. If this time elapses, the system does not send the content for analysis. If the URL is allowed, the system sends the content to the client; otherwise, the system sends a block page or block image to the client.

Exclude Types
Specifies one entry for each type of content to be excluded from content analysis. Images, the **All-Images** type, do not get analyzed.

Reset on Failure
When enabled, specifies that SWG send a TCP reset to the client in the event of a server failure.

About SSL Bypass Set

The SSL Bypass Set item sets the SSL bypass action to **Bypass** in a per-request policy. (A default action, intercept or bypass, for SSL bypass is specified in the client SSL profile.)

The SSL Bypass Set item provides a read-only element, **Action**, that specifies the **Bypass** option.

About URL Filter Assign

A URL Filter Assign item determines whether to block or allow a request. A Category Lookup item must precede URL Filter Assign to provide categories. The URL Filter Assign item looks up the filter action for each category found for the request. If any filter action is set as Block, the request is blocked. The URL filter item also uses the analysis from the Response Analytics item, if used, to determine whether to block or allow the request.

A URL Filter Assign item provides the **URL Filter** element, a list of filters from which to select.

Note: *A Category Lookup item must precede the URL Filter Assign item.*

About Dynamic Date Time

The Dynamic Date Time action enables branching based on the day, date, or time on the server. It provides two default branch rules:

Weekend
Defined as Saturday and Sunday.

Business Hours
Defined as 8:00am to 5:00pm.

The Dynamic Date Time action provides these conditions for defining branch rules.

Time From
Specifies a time of day. The condition is true at or after the specified time.

Time To
Specifies a time of day. This condition is true before or at the specified time.

Date From
Specifies a date. This condition is true at or after the specified date.

Date To
Specifies a date. This condition is true before or at the specified date

Day of Week
Specifies a day. The condition is true for the entire day (local time zone).

Day of Month
Specifies the numeric day of month. This condition is true for this day every month (local time zone).

About AD Group Lookup

An AD Group Lookup item compares a specified string against the `session.ad.last.attr.primaryGroupID` session variable. The specified string is configurable in a branch rule.

The default simple branch rule expression is `User's Primary Group ID is 100`. The specified string, `100`, should be replaced with a group name specific to the Active Directory configuration at the user site.

Note: *An AD Query action is required in the access policy to populate the session variable.*

About LDAP Group Lookup

An LDAP Group Lookup item compares a specified string against the `session.ldap.last.attr.memberOf` session variable. The specified string is configurable in a branch rule. The default simple branch rule expression is `User is a member of CN=MY_GROUP, CN=USERS, CN=MY_DOMAIN` ; the values *`MY_GROUP`*, *`USERS`*, *`MY_DOMAIN`*, must be replaced with values used in the LDAP group configuration at the user site.

Note: *An LDAP Query action is required in the access policy to populate the session variable.*

About LocalDB Group Lookup

A per-request policy LocalDB Group Lookup item compares a specified string against a specified session variable.

The string is specified in a branch rule of the LocalDB Group Lookup item. The default simple branch rule expression is **User is a member of** `MY_GROUP`. The default advanced rule expression is `expression is`

`expr { [mcget {session.localdb.groups}] contains "MY_GROUP" }`. In either the simple or the advanced rule, the variable, *MY_GROUP*, must be replaced with a valid group name.

The session variable must initially be specified and populated by a Local Database action in the access policy. A Local Database action reads groups from a local database instance into a user-specified session variable. It can be `session.localdb.groups` (used by default in the LocalDB Group Lookup advanced rule expression) or any other name. The same session variable name must be used in the Local Database action and the LocalDB Group Lookup advanced rule expression.

About RADIUS Class Lookup

The RADIUS Class Lookup access policy item compares a user-specified class name against the `session.radius.last.attr.class` session variable. The specified class name is configurable in a branch rule.

The default simple branch rule expression is **RADIUS Class attribute contains** `MY_CLASS` . The variable *MY_CLASS* must be replaced with the name of an actual class.

Note: *A RADIUS Acct or RADIUS Auth action is required in the access policy to populate the session variable.*

About per-request policy endings

An ending provides a result for a per-request policy branch. An ending for a per-request policy branch is one of two types.

Allow
Allows the user to continue to the requested URL. Typically, you assign this when the requested URL passes specific checks.

Reject
Blocks the user from continuing to the requested URL. Typically, you assign this when the requested URL fails specific checks. When the per-request policy terminates on a Reject ending, the access policy displays a URL filter denied web page.

Customizing messages for URL filter denied

You need an access profile configured. Before you start, open an access policy for editing.

Customize these messages for display when a user is denied access to a requested URL. When a a per-request policy terminates at a Reject ending, it triggers the access policy Deny ending.

Note: *An access policy displays deny messages any time an access policy reaches a Deny ending. You can customize any Deny ending message using this procedure.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure.

The visual policy editor opens the access policy in a separate screen.

3. Click the **Edit Endings** button.
   A popup screen opens.
4. On the Deny ending that you want to customize, click **+Customization** to expand the customization settings.
   The popup screen displays additional setting options.
5. Customize the text for the URL filter denied settings and for any other settings.

Option	Description
Language	Select the language for which you are configuring Deny messages.
Session ID Title	Specifies the text that precedes the session number when an error occurs.
Error title	Specifies the title for the error message that is displayed when a session cannot be connected.
Error message	Specifies the error message that is displayed when a session cannot be connected.
New session text	Specifies the text that is displayed before the link to start a new session.
New session link	Specifies the link text that is displayed to start a new session.
Session ID title	Specifies the text that precedes the session ID in the Deny message.
ACL denied page retry link message	Specifies the link text that the user can click to retry. This is displayed when a user reaches the ACL denied page.
URL Filter denied page title	Specifies the title for the screen that is displayed when access to a requested URL is blocked.
URL Filter denied page reject message	Specifies the error message that is displayed when access to a requested URL is blocked.
URL Filter denied page return link message	Specifies the link text that the user can click to return to the previous page.
URL Filter denied page retry link message	Specifies the link text that the user can click to retry.
URL Filter denied page category message	Specifies the message to display about the URL category for the blocked URL.
Access not found page title	Specifies the title for the screen that is displayed for access errors.
Access not found page reject message	Specifies the message to display when an access policy is already in progress (in another browser or tab).

6. Click **Save**.
   The popup screen closes.
7. Click **Apply Access Policy** to save your configuration.

You customized messages in one language for use with the Deny ending in this access policy.

Chapter 5

Explicit Forward Proxy

- *Overview: Configuring SWG explicit forward proxy*

Overview: Configuring SWG explicit forward proxy

A Secure Web Gateway (SWG) explicit forward proxy deployment provides an easy way to handle web requests from users. For explicit forward proxy, you configure client browsers to point to a forward proxy server. A forward proxy server establishes a tunnel for SSL traffic. Other virtual servers (wildcard SSL and wildcard forwarding IP virtual servers) listen on the tunnel. The listener that best matches the web traffic directed to the forward proxy server handles the traffic.

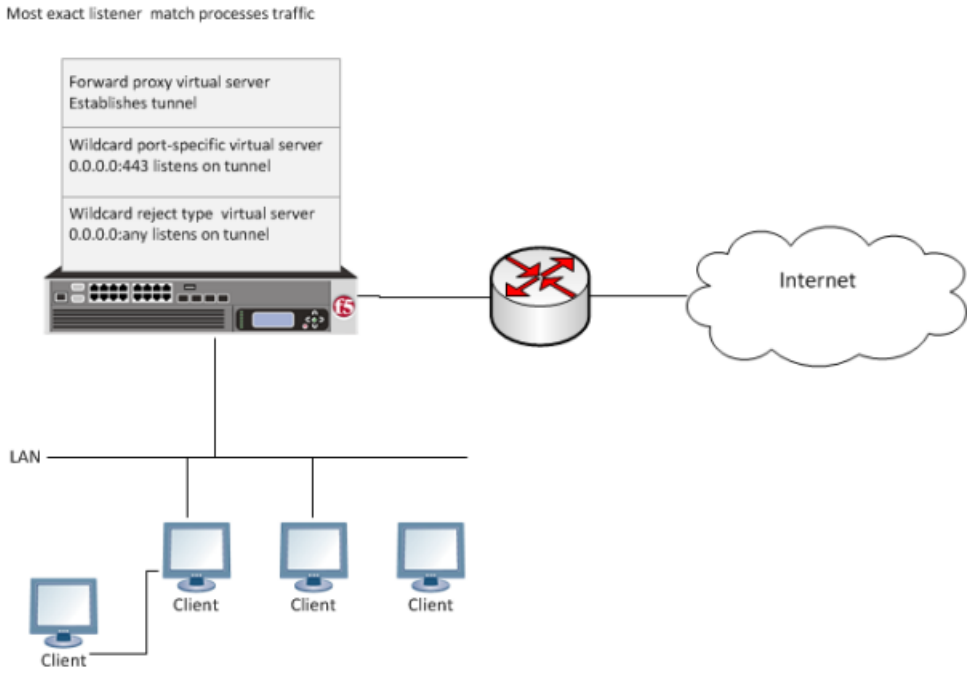

Figure 8: Explicit forward proxy configuration

In any deployment of explicit forward proxy, you must consider how best to configure browsers on client systems to point to the proxy server and how to configure your firewall to prevent users from bypassing the proxy. This implementation does not explain how to do these tasks. However, here are some best practices to consider.

Table 1: Client browser and firewall configuration

Configuration	Recommendation
Client browser	Consider using a group policy that points to a Proxy Auto-Configuration (PAC) file to distribute the configuration to clients and periodically update it.
Firewall	A best practice might be to configure the firewall to trust outbound connections from Secure Web Gateway only. Note that possibly not all applications will work with a firewall configured this way. (Secure Web Gateway uses ports 80 and 443.)

Task summary

Creating a DNS resolver

Adding forward zones to a DNS resolver

Creating a tunnel for SSL forward proxy traffic

Creating a custom HTTP profile for explicit forward proxy
Configuring a per-request policy for SWG
Creating an access profile for SWG explicit forward proxy
Configuring an access policy for SWG explicit forward proxy
Creating a virtual server to use as the forward proxy server
Creating a custom Client SSL forward proxy profile
Creating a custom Server SSL profile
Creating a virtual server for SSL forward proxy traffic
Creating a virtual server to reject traffic

SWG explicit forward proxy configuration prerequisites

To use Secure Web Gateway (SWG), you must configure URL categorization. You might need to configure additional items depending on the other features that you decide to use.

URL categorization
To get a working SWG configuration, you must first download URL categories, configure URL filters, and configure schemes.

Transparent user identification
If you plan to identify users transparently, you must first download, install, and configure a BIG-IP user identification agent, either the F5® DC Agent or the F5 Logon Agent

Authentication
F5 recommends that you use NTLM or Kerberos authentication. If you plan to use authentication, ensure that you have what you need configured.

- For NTLM, you need an NTLM Auth Configuration in Access Policy Manager® (APM®).
- For Kerberos, you need a domain-joined Kerberos user account and a Kerberos AAA server configured in APM.

SSL intercept
To intercept SSL connections that are passing through the proxy, ensure that you have imported a valid subordinate CA certificate and key that is trusted by the endpoints behind the proxy.

About the iApp for Secure Web Gateway configuration

When deployed as an application service, the Secure Web Gateway iApps® template can set up either an explicit or a transparent forward proxy configuration. You can download the template from the F5® DevCentral™ iApp Codeshare wiki at (`http://devcentral.f5.com/wiki/iapp.Codeshare.ashx`).

About ACLs and SWG explicit forward proxy

Only L7 ACLs work with Secure Web Gateway (SWG) explicit forward proxy.

About ways to configure user identification for SWG

User identification configuration requires a method setting in the access profile and an access policy configured to support the setting. Depending on the access profile type, you can select one of these user

identification methods: by IP address (for SWG-Explicit or SWG-Transparent access profile types) or by credentials (for SWG-Explicit type).

Identification by IP address

When you identify users by IP address, you can employ any of these methods.

Note: *Identify users by IP address only when IP addresses are unique and can be trusted.*

---

transparent user identification

Transparent user identification makes a best effort to identify users without requesting credentials. An agent obtains data and stores a mapping of IP addresses to user names in an IF-MAP server. An F5 DC Agent queries domain controllers. An F5 Logon Agent runs a script when a client logs in and can run a script when the client logs out.

Note: *To identify users transparently, you must first install and configure one BIG-IP user identification agent, either the F5® DC Agent or the F5 Logon Agent.*

---

explicit user identification

You can present a logon page in an access policy to request user credentials and validate them. SWG maintains an internal mapping of IP addresses to user names. (You can present the appropriate logon page for the access policy type. For explicit forward proxy, you can present a 407 page. For transparent forward proxy, you can present a 401 page.)

source IP ranges or subnets

You can forego actually identifying the user and base the choice of which scheme to apply on whether the IP address is in a source IP range or on a subnet. SWG maintains an internal mapping of IP addresses to sessions.

Identification by credentials

When you choose to identify users by credentials, SWG maintains an internal mapping of credentials to sessions. To support this choice, you need an NTLM Auth Configuration object and you should check the result of NTLM authentication in the access policy.

Creating a DNS resolver

You configure a DNS resolver on the BIG-IP® system to resolve DNS queries and cache the responses. The next time the system receives a query for a response that exists in the cache, the system returns the response from the cache.

1. On the Main tab, click **Network** > **DNS Resolvers** > **DNS Resolver List**.
   The DNS Resolver List screen opens.
2. Click **Create**.
   The New DNS Resolver screen opens.
3. In the **Name** field, type a name for the resolver.
4. Click **Finished**.

Adding forward zones to a DNS resolver

Before you begin, gather the IP addresses of the nameservers that you want to associate with a forward zone.

Add a forward zone to a DNS resolver when you want the BIG-IP® system to forward queries for particular zones to specific nameservers for resolution in case the resolver does not contain a response to the query.

Note: *Creating a forward zone is optional. Without one, a DNS resolver can still make recursive name queries to the root DNS servers; however, this requires that the virtual servers using the cache have a route to the Internet.*

1. On the Main tab, click **Network** > **DNS Resolvers** > **DNS Resolver List**.
   The DNS Resolver List screen opens.
2. Click the name of the resolver you want to modify.
   The properties screen opens.
3. On the menu bar, click **Forward Zones**.
   The Forward Zones screen displays.
4. Click the **Add** button.

   Note: *You add more than one zone to forward based on the needs of your organization.*

5. In the **Name** field, type the name of a subdomain or type the fully qualified domain name (FQDN) of a forward zone.
   For example, either `example` or `site.example.com` would be valid zone names.
6. Add one or more nameservers:
   a) In the **Address** field, type the IP address of a DNS nameserver that is considered authoritative for this zone.

      Based on your network configuration, add IPv4 or IPv6 addresses, or both.

   b) Click **Add**.
      The address is added to the list.

   Note: *The order of nameservers in the configuration does not impact which nameserver the system selects to forward a query to.*

7. Click **Finished**.

Creating a tunnel for SSL forward proxy traffic

You create a tunnel to support SSL traffic in a Secure Web Gateway (SWG) explicit forward proxy configuration.

Note: *Alternatively, you can use a preconfigured tunnel, http-tunnel.*

1. On the Main tab, click **Network** > **Tunnels** > **Tunnel List**.
   The Tunnel List screen opens.
2. Click **Create**.
3. In the **Name** field, type a name.
4. From the **Encapsulation Type** menu, select **tcp-forward**.
5. Click **Finished**.
   The Tunnel List screen displays the tunnel with tcp-forward in the Profile column.

Creating a custom HTTP profile for explicit forward proxy

An HTTP profile defines the way that you want the BIG-IP® system to manage HTTP traffic.

Note: *Secure Web Gateway (SWG) explicit forward proxy requires a DNS resolver that you select in the HTTP profile.*

1. On the Main tab, click **Local Traffic** > **Profiles** > **Services** > **HTTP**.
   The HTTP profile list screen opens.
2. Click **Create**.
   The New HTTP Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. From the **Proxy Mode** list, select **Explicit**.
5. For **Parent Profile**, retain the **http-explicit** setting.
6. Select the **Custom** check box.
7. Scroll down to the Explicit Proxy area.
8. From the **DNS Resolver** list, select the DNS resolver you configured previously.
9. In the **Tunnel Name** field, you can retain the default value, **http-tunnel**, or type the name of a tunnel if you created one.

   SWG requires a tunnel with tcp-forward encapsulation to support SSL traffic for explicit forward proxy.
10. From the **Default Connect Handling** list, retain the default setting **Deny**.

    Any CONNECT traffic goes through the tunnel to the virtual server that most closely matches the traffic; if there is no match, the traffic is blocked.
11. Click **Finished**.

The custom HTTP profile now appears in the HTTP profile list screen.

Configuring a per-request policy for SWG

Configure a per-request policy to specify the logic that determines how to process web traffic.

Note: *A per-request policy must determine whether to bypass SSL traffic and, otherwise, whether to allow or reject a URL request in a Secure Web Gateway (SWG) forward proxy configuration.*

1. On the Main tab, click **Access Policy** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. Click **Create**.
   The General Properties screen displays.
3. In the **Name** field, type a name for the policy and click **Finished**.

   A per-request policy name must be unique among all per-request policy and access profile names.

   The policy name appears on the Per-Request Policies screen.
4. In the Access Policy column for the per-request policy that you want to update, click the **Edit** link.
   The visual policy editor opens in another tab.
5. To create different branches for processing HTTP and HTTPS traffic, add a **Protocol Lookup** item.
   a) Click the **(+)** icon anywhere in the per-request policy to add a new item.

A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.

b) Type `prot` in the Search field, select **Protocol Lookup**, and click **Add Item**.
A Properties popup screen opens.

c) Click **Save**.
The Properties screen closes. The visual policy editor displays.

6. If you configured SSL forward proxy bypass in the client and server SSL profiles, include an **SSL Intercept Set** item to ensure that SSL traffic is not bypassed until this policy determines that it should be.

   It is important to include SSL Intercept Set when the default SSL bypass action in the client SSL profile is set to Bypass.

7. To retrieve the requested URL and the categories to which it belongs, add a **Category Lookup** item.

   Important: *A Category Lookup item is required to trigger event logging for SWG, to provide a response web page for the Response Analytics item, and to provide categories for the URL Filter Assign item.*

   a) Click the **(+)** icon anywhere in the per-request policy to add a new item.
   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.

   b) Type `cat` in the Search field, select **Category Lookup**, and click **Add Item**.
   A Properties popup screen opens.

   c) From the **Categorization Input** list, select how to obtain the requested URL. For HTTP traffic, select **Use HTTP URI (cannot be used for SSL Bypass decisions)**. For SSL-encrypted traffic, select either **Use SNI in Client Hello (if SNI is not available, use Subject.CN)** or **Use Subject.CN in Server Cert**.
   If you select **Use HTTP URI (cannot be used for SSL Bypass decisions)**, the **SafeSearch Mode** list displays and **Enabled** is selected.

   d) From the **Category Lookup Type** list, select the category types in which to search for the requested URL. Select one from **Custom categories first, then standard categories if not found**, **Always process full list of both custom and standard categories**, or **Process standard categories only**.

   Depending on your selection, the Category Lookup Type item looks through custom categories or standard categories or both, and compiles a list of one or more categories from them. The list is available for subsequent processing by the URL Filter Assign item.

   e) Click **Save**.
   The Properties screen closes. The visual policy editor displays.

8. To enable Safe Search for SSL-encrypted traffic, add an additional Category Lookup item, specify **Use HTTP URI (cannot be used for SSL Bypass decisions)** as the **Category Lookup Type**, and retain the default setting (**Enabled**) for **SafeSearch Mode**.
9. At any point in the policy where a decision to bypass SSL traffic is made, add an **SSL Bypass Set** item.
10. Add any of these items to the policy.

Item	Description
Dynamic Date Time	Branch by day of week or time of day.
AD Group Lookup	Branch by user group. Requires branch rule configuration.
LDAP Group Lookup	Branch by user group. Requires branch rule configuration.
LocalDB Group Lookup	Branch by user group. Requires branch rule configuration.

Item	Description
RADIUS Class Lookup	Branch by the class attribute. Requires branch rule configuration.

11. To configure a branch rule for a LocalDB Group Lookup item:

a) In the visual policy editor, click the name of the item.
A Properties popup screen opens.
b) Click the Branch Rules tab.
c) To edit an expression, click the **change** link.
An additional popup screen opens, displaying the Simple tab.
d) If the Local Database action in the access policy was configured to read groups into the `session.localdb.groups` session variable, edit the default simple expression, **User is a member of** `MY_GROUP`, replacing MY_GROUP with a relevant group.
e) If the Local Database action in the access policy was configured to read groups into a session variable other than `session.localdb.groups`, click the Advanced tab; edit the default advanced expression, `expression is expr { [mcget {session.localdb.groups}] contains "`*`MY_GROUP`*`" }`, replacing MY_GROUP with a relevant group and `session.localdb.groups` with the session variable specified in the Local Database action.
f) Click **Finished**.
The popup screen closes.
g) Click **Save**.
The popup screen closes. The visual policy editor displays.

12. To configure a branch rule for AD, LDAP, or RADIUS group or class lookups:

a) In the visual policy editor, click the name of the policy item.
A Properties popup screen opens.
b) Click the Branch Rules tab.
c) To edit an expression, click the **change** link.
An additional popup screen opens, displaying the Simple tab.
d) Edit the default simple expression to specify group or class that is used in your environment.
In an LDAP Group Lookup item, the default simple expression is **User is a member of** `CN=MY_GROUP, CN=USERS, CN=MY_DOMAIN`. You can use the simple expression editor to replace the default values.
e) Click **Finished**.
The popup screen closes.
f) Click **Save**.
The popup screen closes. The visual policy editor displays.

13. To trigger inspection of the response web page contents, add a Response Analytics item.

A Category Lookup item must precede this item.

a) In the **Max Buffer Size** field, type the number of bytes to buffer.
b) In the **Max Buffer time** field, type the number of seconds to retain response data in the buffer.
c) For the **Reset on Failure** field, retain the default value **Enabled** to send a TCP reset if the server fails.
d) For each type of content that you want to exclude from analysis, click **Add new entry** and then select a type from the list.

The **All-Images** type is on the list by default because images are not scanned.

e) Click **Finished**.
The popup screen closes.
f) Click **Save**.

The fallback branch after this item indicates that a failure occurred during content analysis. The Success branch indicates that content analysis completed.

The popup screen closes. The visual policy editor displays.

14. Add a URL Filter Assign item after the Response Analytics item, if included on the branch; otherwise, add it anywhere on a branch after a Category Lookup item.

    In this item, you must specify a URL filter to apply to the URL categories that the Category Lookup item returned. If any URL category specifies the Block filtering action, this item blocks the request. This item also blocks the request if the Response Analytics item identified malicious content.

To put the per-request policy into effect, add it to the virtual server.

Creating an access profile for SWG explicit forward proxy

Create an access profile to provide the access policy configuration for a virtual server that establishes a secured session.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click **Create**.
   The New Profile screen opens.
3. In the **Name** field, type a name for the access profile.

   Note: *An access profile name must be unique among all access profile and per-request policy names.*

4. From the **Profile Type** list, select **SWG-Explicit**.

   Selecting this type ensures that only access policy items that are valid for Secure Web Gateway (SWG) explicit forward proxy are available in the visual policy editor when you configure an access policy.
5. In the Configurations area for the **User Identification Method** list, select one of these methods:
   - IP address - Select this method only in an environment where a client IP address is unique and can be trusted.
   - Credentials - Select this method to identify users using NTLM authentication.
6. If you selected **Credentials** for the **User Identification Method**, you must select an entry from the **NTLM Auth Configuration** list.
7. If you selected **IP Address** for the **User Identification Method**, you can also select an entry from the **NTLM Auth Configuration** list to use NTLM authentication before a session starts.

   In the case of a shared machine, an IP address might already be associated with a user or a session. Using NTLM authentication ensures that the system can associate the IP address with the correct session (new or existing) or with a new user each time a user logs on to a shared machine.
8. In the Language Settings area, add and remove accepted languages, and set the default language.

   A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.
9. Click **Finished**.
   The Access Profiles list screen displays.
10. To enable Secure Web Gateway event logging for this access profile, add log settings.
    a) Click the name of the access profile that you just created.
       The Properties screen displays.

b) On the menu bar, click **Logs**.
The General Properties screen displays.
c) In the Log Settings area, move log settings from the **Available** list to the **Selected** list.

You can configure log settings in the Access Policy Event Logs area of the product.

This creates an access profile with a default access policy.

Configuring an access policy for SWG explicit forward proxy

You configure an access policy for Secure Web Gateway (SWG) explicit forward proxy to assign an SWG scheme to the policy and to populate session variables with group or class attribute information for use in the per-request policy. You can also add access policy items to collect credentials and to authenticate a user or add access policy items to identify the user transparently.

Note: *If you include authentication in your access policy and the first site that a user accesses uses HTTP instead of secure HTTP, passwords are passed as clear text. To prevent this from happening, F5® recommends using Kerberos or NTLM authentication.*

---

1. On the Main tab, click **Access Policy** > **Access Profiles**.
The Access Profiles List screen opens.
2. Click the **(+)** icon anywhere in the access policy to add a new action item.

   Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
3. If you specified an NTLM Auth configuration in the access profile, verify that authentication succeeded.
   a) Type `NTLM` in the search field.
   b) Select **NTLM Auth Result** from the results list.
   c) Click **Add Item**.
   A properties popup screen opens.
   d) Click **Save**.
   The Properties screen closes. The visual policy editor displays.
4. Assign an SWG scheme to the access policy:

   Scheme assignment is mandatory.
   a) Click the **(+)** icon anywhere in the access policy to add a new action item.
   b) On the Assignment tab, select **SWG Scheme Assign** and click **Add Item**.
   A Properties screen opens.

   a) To display the available schemes, click the **Add/Delete** link.
   b) Select one scheme and click **Save**.
   The Properties screen closes and the visual policy editor displays.
5. To supply LDAP group information for use in the per-request policy, add an LDAP Query item anywhere in the access policy and configure its properties:
   a) From the **Server** list, select an AAA LDAP server.

An LDAP Query uses SSL connections when you select an LDAP AAA server that is configured for LDAPS.

b) Specify the **SearchDN**, and **SearchFilter** settings.

SearchDN is the base DN from which the search is done.

c) Click **Save**.

This item populates the `session.ldap.last.attr.memberOf` session variable.

6. To supply Active Directory groups for use in the per-request policy, add an AD Query item anywhere in the access policy and configure its properties:
   a) From the **Server** list, select an AAA AD server.
   b) Select the **Fetch Primary Group** check box.

      The value of the primary user group populates the `session.ad.last.attr.primaryGroupID` session variable.

   c) Click **Save**.

7. To supply RADIUS class attributes for use in the per-request policy, add a RADIUS Auth item anywhere in the access policy and configure its properties:
   a) From the **Server** list, select an AAA RADIUS server.
   b) Click **Save**.

   This item populates the `session.radius.last.attr.class` session variable.

8. To supply local database groups for use in the per-request policy, add a Local Database item anywhere in the access policy and configure its properties:
   a) From the **LocalDB Instance** list, select a local user database.
   b) In the **User Name** field, retain the default session variable.
   c) Click **Add new entry**
      A new line is added to the list of entries with the Action set to **Read** and other default settings.
   d) In the Destination column **Session Variable** field, type `session.localdb.groups`.

      If you type a name other than `session.localdb.groups`, note it. You will need it when you configure the per-request access policy.

   e) In the Source column from the **DB Property** list, select **groups**.
   f) Click **Save**.

   This item populates the `session.localdb.groups` session variable.

9. (Optional) To identify a user transparently, perform these substeps.

   To use transparent user identification, you must have installed and configured a BIG-IP® user identification agent, either the F5® DC Agent or the F5 Logon Agent.
   a) On an access policy branch, click the plus symbol **(+)** to add an item to the access policy.
   b) From the Authentication tab, select **Transparent Identity Import** and click **Add Item**.

      The transparent identity import access policy item searches the database in the IF-MAP server for the client source IP address. By default, this access policy item has two branches: associated and fallback.

      A properties screen opens.
   c) Click **Save**.
      The visual policy editor displays.
   d) Add any additional access policy items to the fallback or associated branches.
      You might add Kerberos authentication on the fallback branch.

10. (Optional) To add Kerberos authentication to the access policy, perform these substeps:

a) On an access policy branch, click the plus symbol **(+)** to add an item to the access policy.
b) On the Logon tab, select **HTTP 407 Response** and click **Add Item**.
A properties screen opens.
c) From the **HTTP Auth Level** list, select **negotiate** and click **Save**.
The properties screen closes.
d) Click the **(+)** icon on the **negotiate** branch.
A popup screen opens.
e) Type `ker` in the search field, select **Kerberos Auth** from the results, and click **Add Item**.
A properties screen opens.
f) From the **AAA Server** list, select an existing server.
g) From the **Request Based Auth** list, select **Disabled**.
h) Click **Save**.
The properties screen closes and the visual policy editor is displayed.

Note: *The **Max Logon Attempts Allowed** setting specifies attempts by an external client without a Kerberos ticket to authenticate on SWG forward proxy.*

---

11. Click the **Apply Access Policy** link to apply and activate the changes to the access policy.

To put an access policy into effect, you must assign it to a virtual server.

Creating a virtual server to use as the forward proxy server

You specify a virtual server to handle forward proxy traffic with Secure Web Gateway (SWG). In an explicit proxy configuration, client browser configurations specify this virtual server as the proxy server.

Note: *Use this virtual server for forward proxy traffic only. You should not try to use it for reverse proxy too; do not add a pool to it. This virtual server is, in effect, a bastion host.*

---

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
The Virtual Server List screen opens.
2. Click the **Create** button.
The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type the IP address for a host virtual server.
This field accepts an address in CIDR format (IP address/prefix). However, when you type the complete IP address for a host, you do not need to type a prefix after the address.
Type a destination address in this format: `162.160.15.20`.
5. In the **Service Port** field, type the port number to use for forward proxy traffic.
Typically, the port number is `3128` or `8080`.
6. From the **HTTP Profile** list, select the HTTP profile you configured earlier.
7. From the **VLAN and Tunnel Traffic** list, select **Enabled on**.
8. For the **VLANs and Tunnels** setting, move the VLAN on the BIG-IP® system that connects to the internal networks to the **Selected** list.
9. From the **Source Address Translation** list, select **Auto Map**.
10. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
11. From the **Per-Request Policy** list, select the per-request policy that you configured earlier.

12. Click **Finished**.

Creating a custom Client SSL forward proxy profile

Creating a Client SSL forward proxy profile makes it possible for client and server authentication, while still allowing the BIG-IP® system to perform data optimization, such as decryption and encryption. This profile applies to client-side SSL forward proxy traffic only.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.
   The Client profile list screen opens.
2. Click **Create**.
   The New Client SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. From the **Parent Profile** list, select **clientssl**.
5. To avoid issues with privacy concerns, you might need to enable SSL forward proxy bypass for URLs that expose personal user information, such as those for financial or government sites.
   a) Scroll down to the **SSL Forward Proxy** list, and select **Advanced**.
   b) Select the **Custom** check box for the SSL Forward Proxy area.
   c) From the **SSL Forward Proxy** list, select **Enabled**.
      You can update this setting later but only while the profile is not assigned to a virtual server.
   d) From the **CA Certificate** list, select a certificate.
   e) From the **CA Key** list, select a key.
   f) In the **CA Passphrase** field, type a passphrase.
   g) In the **Confirm CA Passphrase** field, type the passphrase again.
   h) In the **Certificate Lifespan** field, type a lifespan for the SSL forward proxy certificate in days.
   i) (Optional) From the **Certificate Extensions** list, select **Extensions List**.
   j) (Optional) For the **Certificate Extensions List** setting, select the extensions that you want in the **Available extensions** field, and move them to the **Enabled Extensions** field using the **Enable** button.
   k) From the **SSL Forward Proxy Bypass** list, select **Enabled**.
      You can update this setting later but only while the profile is not assigned to a virtual server.
      Additional settings display.
   l) For **Default Bypass Action**, retain the default value **Intercept**.
      You can override the value of this action on a case-by-case basis in the per-request policy for the virtual server.

   Note: *Bypass and intercept lists do not work with per-request policies. Retain the setting* ***None*** *for the remainder of the fields.*

6. Click **Finished**.

The custom Client SSL forward proxy profile now appears in the Client SSL profile list screen.

Creating a custom Server SSL profile

Create a custom server SSL profile to support SSL forward proxy.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Server**.

The SSL Server profile list screen opens.

2. Click **Create**.
   The New Server SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. For **Parent Profile**, retain the default selection, **serverssl**.
5. From the **Configuration** list, select **Advanced**.
6. Select the **Custom** check box.
   The settings become available for change.
7. From the **SSL Forward Proxy** list, select **Enabled**.
   You can update this setting later, but only while the profile is not assigned to a virtual server.
8. From the **SSL Forward Proxy Bypass** list, select **Enabled** (or retain the default value **Disabled**).
   The values of the **SSL Forward Proxy Bypass** settings in the server SSL and the client SSL profiles specified in a virtual server must match. You can update this setting later but only while the profile is not assigned to a virtual server.
9. Scroll down to the **Secure Renegotiation** list and select **Request**.
10. Click **Finished**.

The custom Server SSL profile is now listed in the SSL Server profile list.

Creating a virtual server for SSL forward proxy traffic

You specify a port-specific wildcard virtual server to handle SSL traffic. This virtual server listens on the tunnel that the forward proxy server establishes.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. From the **HTTP Profile** list, select **http**.
7. From the **Configuration** list, select **Advanced**.
8. For the **SSL Profile (Client)** setting, from the **Available** list, select the name of the custom Client SSL proxy profile you previously created, and using the Move button, move the name to the **Selected** list.

   Important: *To enable proxy SSL functionality, you can either:*

   - Disassociate existing Client SSL and Server SSL profiles from a virtual server and configure the Proxy SSL settings.
   - Create new Client SSL and Server SSL profiles and configure the Proxy SSL settings.

   Then with either option, select the Client SSL and Server SSL profiles on a virtual server. You cannot modify existing Client SSL and Server SSL profiles while they are selected on a virtual server to enable proxy SSL functionality.

   ---

9. For the **SSL Profile (Server)** setting, from the **Available** list, select the name of the custom Server SSL proxy profile you previously created, and using the Move button, move the name to the **Selected** list.

Important: *To enable SSL proxy functionality, you can either:*

- Disassociate existing Client SSL and Server SSL profiles from a virtual server and configure the Proxy SSL settings.
- Create new Client SSL and Server SSL profiles and configure the Proxy SSL settings.

Then with either option, select the Client SSL and Server SSL profiles on a virtual server. You cannot modify existing Client SSL and Server SSL profiles while they are selected on a virtual server to enable SSL proxy functionality.

10. For the **Address Translation** setting, clear the **Enabled** check box.
11. From the **VLAN and Tunnel Traffic** list, select **Enabled on**.
12. For the **VLANs and Tunnels** setting, move either the tunnel you configured earlier or the default tunnel, **http-tunnel**, to the **Selected** list.

    This must be the same tunnel that you specified in the HTTP profile for the virtual server for forward proxy.
13. From the **Source Address Translation** list, select **Auto Map**.
14. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
15. From the **Per-Request Policy** list, select the per-request policy that you configured earlier.
16. Click **Finished**.

The virtual server now appears in the Virtual Server List screen.

Creating a virtual server to reject traffic

You create a reject type virtual server to reject any IP traffic with URLs that are incomplete, or otherwise misconfigured for use with forward proxy. This virtual server listens on the tunnel that the forward proxy server establishes.

Note: *Secure Web Gateway does not support application access and network access tunnels.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. From the **Type** list, select **Reject**.
5. In the **Source Address** field, type `0.0.0.0/0`.
6. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
7. From the **Service Port** list, select ***All Ports**.
8. From the **Protocol** list, select **TCP**.
9. From the **VLAN and Tunnel Traffic** list, select **Enabled on**.
10. For the **VLANs and Tunnels** setting, select the tunnel you configured earlier, or select the default tunnel, **http-tunnel**, and move it to the **Selected** list.

    This must be the same tunnel that is specified in the virtual server for the forward proxy server.
11. Click **Finished**.

Implementation result

Web traffic that originates from your enterprise networks is now inspected and controlled by F5® Secure Web Gateway forward proxy.

Session variables for use in a per-request policy

Per-request policy items that look up the group or class to which a user belongs rely on the access policy to populate these session variables.

Per-request policy item	Session variable	Access policy item
AD Group Lookup	`session.ad.last.attr.primaryGroupID`	AD Query
LDAP Group Lookup	`session.ldap.last.attr.memberOf`	LDAP Query
LocalDB Group Lookup	`session.localdb.groups` ***Note:*** *This session variable is a default in the expression for LocalDB Group Lookup; any session variable in the expression must match the session variable used in the Local Database action in the access policy.*	Local Database
RADIUS Class Lookup	`session.radius.last.attr.class`	RADIUS Auth

Chapter 6

Transparent Forward Proxy

- *Overview: Configuring transparent forward proxy in inline mode*
- *Overview: Configuring transparent forward proxy*

Overview: Configuring transparent forward proxy in inline mode

In transparent forward proxy, you configure your internal network to forward web traffic to the BIG-IP® system with Secure Web Gateway (SWG). This implementation describes an *inline deployment*. You place the BIG-IP system directly in the path of traffic, or inline, as the next hop after the gateway.

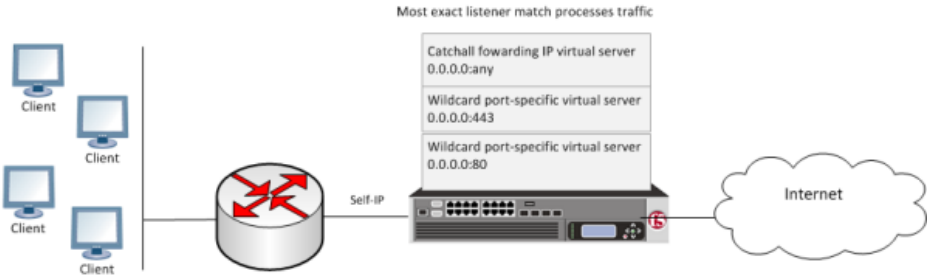

Figure 9: Secure Web Gateway transparent forward proxy inline deployment

The gateway sends traffic to the self-ip address of a VLAN configured on the BIG-IP system. *Wildcard* virtual servers listen on the VLAN and process the traffic that most closely matches the virtual server address. A wildcard virtual server is a special type of network virtual server designed to manage network traffic that is targeted to transparent network devices. SWG identifies users without using session management cookies, and applies a scheme that categorizes and filters URLs, controlling access.

Note: *Transparent forward proxy provides the option to use a captive portal. To use this option, you need an additional virtual server, not shown in the figure, for the captive portal primary authentication server.*

Task Summary

Creating a VLAN for transparent forward proxy
Assigning a self IP address to a VLAN
Configuring a per-request policy for SWG
Creating an access profile for SWG transparent forward proxy
Configuring an access policy for transparent forward proxy
Creating a custom Client SSL forward proxy profile
Creating a custom Server SSL profile
Creating a virtual server for forward proxy SSL traffic
Creating a virtual server for forward proxy traffic
Creating a forwarding virtual server
Creating a Client SSL profile for a captive portal
Creating a virtual server for a captive portal

SWG transparent forward proxy configuration prerequisites

To use Secure Web Gateway (SWG), you must configure URL categorization. You might need to configure additional items depending on the other features that you decide to use.

URL categorization

To get a working SWG configuration, you must first download URL categories, configure URL filters, and configure schemes.

Transparent user identification

If you plan to identify users transparently, you must first download, install, and configure a BIG-IP user identification agent, either the F5® DC Agent or the F5 Logon Agent.

Authentication

F5 recommends that you use NTLM or Kerberos authentication. If you plan to use authentication, ensure that you have what you need configured.

- For NTLM, you need an NTLM Auth Configuration in Access Policy Manager® (APM®).
- For Kerberos, you need a domain-joined Kerberos user account and a Kerberos AAA server configured in APM.

SSL intercept

To intercept SSL connections that are passing through the proxy, ensure that you have imported a valid subordinate CA certificate and key that is trusted by the endpoints behind the proxy.

Captive portal

If you plan to use the captive portal feature, make sure that a certificate and key with the proper common name is imported for use.

About the iApp for Secure Web Gateway configuration

When deployed as an application service, the Secure Web Gateway iApps® template can set up either an explicit or a transparent forward proxy configuration. You can download the template from the F5® DevCentral™ iApp Codeshare wiki at (`http://devcentral.f5.com/wiki/iapp.Codeshare.ashx`).

About ways to configure user identification for SWG

User identification configuration requires a method setting in the access profile and an access policy configured to support the setting. Depending on the access profile type, you can select one of these user identification methods: by IP address (for SWG-Explicit or SWG-Transparent access profile types) or by credentials (for SWG-Explicit type).

Identification by IP address

When you identify users by IP address, you can employ any of these methods.

Note: *Identify users by IP address only when IP addresses are unique and can be trusted.*

---

transparent user identification

Transparent user identification makes a best effort to identify users without requesting credentials. An agent obtains data and stores a mapping of IP addresses to user names in an IF-MAP server. An F5 DC Agent queries domain controllers. An F5 Logon Agent runs a script when a client logs in and can run a script when the client logs out.

Note: *To identify users transparently, you must first install and configure one BIG-IP user identification agent, either the F5® DC Agent or the F5 Logon Agent.*

---

explicit user identification

You can present a logon page in an access policy to request user credentials and validate them. SWG maintains an internal mapping of IP addresses to user names. (You can present the appropriate logon page for the access policy type. For explicit forward proxy, you can present a 407 page. For transparent forward proxy, you can present a 401 page.)

source IP ranges or subnets

You can forego actually identifying the user and base the choice of which scheme to apply on whether the IP address is in a source IP range or on a subnet. SWG maintains an internal mapping of IP addresses to sessions.

Identification by credentials

When you choose to identify users by credentials, SWG maintains an internal mapping of credentials to sessions. To support this choice, you need an NTLM Auth Configuration object and you should check the result of NTLM authentication in the access policy.

Creating a VLAN for transparent forward proxy

You need a VLAN on which the forward proxy can listen. For increased security, the VLAN should directly face your clients.

1. On the Main tab, click **Network** > **VLANs**.
   The VLAN List screen opens.
2. Click **Create**.
   The New VLAN screen opens.
3. In the **Name** field, type a unique name for the VLAN.
4. For the **Interfaces** setting,
   a) From the **Interface** list, select an interface number.
   b) From the **Tagging** list, select **Untagged**.
   c) Click **Add**.
5. Click **Finished**.
   The screen refreshes, and displays the new VLAN in the list.

The new VLAN appears in the VLAN list.

Assigning a self IP address to a VLAN

Assign a self IP address to a VLAN on which the forward proxy listens.

1. On the Main tab, click **Network** > **Self IPs**.
2. Click **Create**.
   The New Self IP screen opens.
3. In the **Name** field, type a unique name for the self IP address.
4. In the **IP Address** field, type the IP address of the VLAN.
   The system accepts IPv4 and IPv6 addresses.
5. In the **Netmask** field, type the full network mask for the specified IP address.
   For example, you can type `ffff:ffff:ffff:ffff:0000:0000:0000:0000` or `ffff:ffff:ffff:ffff::`.
6. From the **VLAN/Tunnel** list, select the VLAN.
7. Click **Finished**.
   The screen refreshes, and displays the new self IP address.

Configuring a per-request policy for SWG

Configure a per-request policy to specify the logic that determines how to process web traffic.

Note: *A per-request policy must determine whether to bypass SSL traffic and, otherwise, whether to allow or reject a URL request in a Secure Web Gateway (SWG) forward proxy configuration.*

1. On the Main tab, click **Access Policy** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. Click **Create**.
   The General Properties screen displays.
3. In the **Name** field, type a name for the policy and click **Finished**.

   A per-request policy name must be unique among all per-request policy and access profile names.

   The policy name appears on the Per-Request Policies screen.
4. In the Access Policy column for the per-request policy that you want to update, click the **Edit** link.
   The visual policy editor opens in another tab.
5. To create different branches for processing HTTP and HTTPS traffic, add a **Protocol Lookup** item.
   a) Click the **(+)** icon anywhere in the per-request policy to add a new item.
      A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
   b) Type `prot` in the Search field, select **Protocol Lookup**, and click **Add Item**.
      A Properties popup screen opens.
   c) Click **Save**.
      The Properties screen closes. The visual policy editor displays.
6. If you configured SSL forward proxy bypass in the client and server SSL profiles, include an **SSL Intercept Set** item to ensure that SSL traffic is not bypassed until this policy determines that it should be.

   It is important to include SSL Intercept Set when the default SSL bypass action in the client SSL profile is set to Bypass.
7. To retrieve the requested URL and the categories to which it belongs, add a **Category Lookup** item.

   Important: *A Category Lookup item is required to trigger event logging for SWG, to provide a response web page for the Response Analytics item, and to provide categories for the URL Filter Assign item.*

   a) Click the **(+)** icon anywhere in the per-request policy to add a new item.
      A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
   b) Type `cat` in the Search field, select **Category Lookup**, and click **Add Item**.
      A Properties popup screen opens.
   c) From the **Categorization Input** list, select how to obtain the requested URL. For HTTP traffic, select **Use HTTP URI (cannot be used for SSL Bypass decisions)**. For SSL-encrypted traffic, select either **Use SNI in Client Hello (if SNI is not available, use Subject.CN)** or **Use Subject.CN in Server Cert**.
      If you select **Use HTTP URI (cannot be used for SSL Bypass decisions)**, the **SafeSearch Mode** list displays and **Enabled** is selected.
   d) From the **Category Lookup Type** list, select the category types in which to search for the requested URL. Select one from **Custom categories first, then standard categories if not found**, **Always process full list of both custom and standard categories**, or **Process standard categories only**.

Depending on your selection, the Category Lookup Type item looks through custom categories or standard categories or both, and compiles a list of one or more categories from them. The list is available for subsequent processing by the URL Filter Assign item.

e) Click **Save**.
The Properties screen closes. The visual policy editor displays.

8. To enable Safe Search for SSL-encrypted traffic, add an additional Category Lookup item, specify **Use HTTP URI (cannot be used for SSL Bypass decisions)** as the **Category Lookup Type**, and retain the default setting (**Enabled**) for **SafeSearch Mode**.

9. At any point in the policy where a decision to bypass SSL traffic is made, add an **SSL Bypass Set** item.

10. Add any of these items to the policy.

Item	Description
Dynamic Date Time	Branch by day of week or time of day.
AD Group Lookup	Branch by user group. Requires branch rule configuration.
LDAP Group Lookup	Branch by user group. Requires branch rule configuration.
LocalDB Group Lookup	Branch by user group. Requires branch rule configuration.
RADIUS Class Lookup	Branch by the class attribute. Requires branch rule configuration.

11. To configure a branch rule for a LocalDB Group Lookup item:

a) In the visual policy editor, click the name of the item.
A Properties popup screen opens.
b) Click the Branch Rules tab.
c) To edit an expression, click the **change** link.
An additional popup screen opens, displaying the Simple tab.
d) If the Local Database action in the access policy was configured to read groups into the `session.localdb.groups` session variable, edit the default simple expression, **User is a member of** `MY_GROUP`, replacing MY_GROUP with a relevant group.
e) If the Local Database action in the access policy was configured to read groups into a session variable other than `session.localdb.groups`, click the Advanced tab; edit the default advanced expression, `expression is expr { [mcget {session.localdb.groups}] contains "`*`MY_GROUP`*`" }`, replacing MY_GROUP with a relevant group and `session.localdb.groups` with the session variable specified in the Local Database action.
f) Click **Finished**.
The popup screen closes.
g) Click **Save**.
The popup screen closes. The visual policy editor displays.

12. To configure a branch rule for AD, LDAP, or RADIUS group or class lookups:

a) In the visual policy editor, click the name of the policy item.
A Properties popup screen opens.
b) Click the Branch Rules tab.
c) To edit an expression, click the **change** link.
An additional popup screen opens, displaying the Simple tab.
d) Edit the default simple expression to specify group or class that is used in your environment.

In an LDAP Group Lookup item, the default simple expression is **User is a member of** `CN=MY_GROUP, CN=USERS, CN=MY_DOMAIN`. You can use the simple expression editor to replace the default values.

e) Click **Finished**.
The popup screen closes.

f) Click **Save**.
The popup screen closes. The visual policy editor displays.

13. To trigger inspection of the response web page contents, add a Response Analytics item.

A Category Lookup item must precede this item.

a) In the **Max Buffer Size** field, type the number of bytes to buffer.

b) In the **Max Buffer time** field, type the number of seconds to retain response data in the buffer.

c) For the **Reset on Failure** field, retain the default value **Enabled** to send a TCP reset if the server fails.

d) For each type of content that you want to exclude from analysis, click **Add new entry** and then select a type from the list.

The **All-Images** type is on the list by default because images are not scanned.

e) Click **Finished**.
The popup screen closes.

f) Click **Save**.

The fallback branch after this item indicates that a failure occurred during content analysis. The Success branch indicates that content analysis completed.

The popup screen closes. The visual policy editor displays.

14. Add a URL Filter Assign item after the Response Analytics item, if included on the branch; otherwise, add it anywhere on a branch after a Category Lookup item.

In this item, you must specify a URL filter to apply to the URL categories that the Category Lookup item returned. If any URL category specifies the Block filtering action, this item blocks the request. This item also blocks the request if the Response Analytics item identified malicious content.

To put the per-request policy into effect, add it to the virtual server.

Creating an access profile for SWG transparent forward proxy

You create an access profile to provide the access policy configuration for a virtual server that establishes a secured session.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
The Access Profiles List screen opens.

2. Click **Create**.
The New Profile screen opens.

3. In the **Name** field, type a name for the access profile.

Note: *An access profile name must be unique among all access profile and per-request policy names.*

4. From the **Profile Type** list, select **SWG-Transparent**.

With this type, only the access policy items that are valid for Secure Web Gateway (SWG) transparent forward proxy are available in the visual policy editor.

5. Select the **Custom** check box for **Settings**.

The settings become available.

6. (Optional) To use NTLM authentication before a session starts, from the **NTLM Auth Configuration** list select a configuration.

   In the case of a shared machine, an IP address might already be associated with a user or a session. Using NTLM authentication ensures that the system can associate the IP address with the correct session (new or existing) or with a new user each time a user logs on to the shared machine.

7. (Optional) To direct users to a captive portal, for **Captive Portal** select **Enabled** and, in the **Primary Authentication URI** field, type the URI.

   You might specify the URI of your primary authentication server if you use single sign-on across multiple domains. Users can then access multiple back-end applications from multiple domains and hosts without needing to re-enter their credentials, because the user session is stored on the primary domain.

   For example, you might type `https://logon.siterequest.com` in the field.

8. In the Language Settings area, add and remove accepted languages, and set the default language.

   A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.

9. Click **Finished**.
   The Access Profiles list screen displays.

10. To enable Secure Web Gateway event logging for this access profile, add log settings.
    a) Click the name of the access profile that you just created.
       The Properties screen displays.
    b) On the menu bar, click **Logs**.
       The General Properties screen displays.
    c) In the Log Settings area, move log settings from the **Available** list to the **Selected** list.

    You can configure log settings in the Access Policy Event Logs area of the product.

This creates an access profile with a default access policy.

Configuring an access policy for transparent forward proxy

You configure an access policy for Secure Web Gateway (SWG) transparent forward proxy to assign an SWG scheme to the policy and to populate session variables with group or class attribute information for use in the per-request policy. You can also add access policy items to collect credentials and to authenticate a user or you can add items to transparently identify the user without requesting credentials.

Note: *If you include authentication in your access policy and the first site that a user accesses uses HTTP instead of secure HTTP, passwords are passed as clear text. To prevent this from happening, F5® recommends using Kerberos or NTLM authentication.*

---

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the **(+)** icon anywhere in the access policy to add a new action item.

   Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
3. If you specified an NTLM Auth configuration in the access profile, verify that authentication succeeded.

a) Type `NTLM` in the search field.
b) Select **NTLM Auth Result** from the results list.
c) Click **Add Item**.
A properties popup screen opens.
d) Click **Save**.
The Properties screen closes. The visual policy editor displays.

4. Assign an SWG scheme to the access policy:

Scheme assignment is mandatory.

a) Click the **(+)** icon anywhere in the access policy to add a new action item.
b) On the Assignment tab, select **SWG Scheme Assign** and click **Add Item**.
A Properties screen opens.

a) To display the available schemes, click the **Add/Delete** link.
b) Select one scheme and click **Save**.
The Properties screen closes and the visual policy editor displays.

5. To supply LDAP group information for use in the per-request policy, add an LDAP Query item anywhere in the access policy and configure its properties:

a) From the **Server** list, select an AAA LDAP server.

An LDAP Query uses SSL connections when you select an LDAP AAA server that is configured for LDAPS.

b) Specify the **SearchDN**, and **SearchFilter** settings.

SearchDN is the base DN from which the search is done.

c) Click **Save**.

This item populates the `session.ldap.last.attr.memberOf` session variable.

6. To supply Active Directory groups for use in the per-request policy, add an AD Query item anywhere in the access policy and configure its properties:

a) From the **Server** list, select an AAA AD server.
b) Select the **Fetch Primary Group** check box.

The value of the primary user group populates the `session.ad.last.attr.primaryGroupID` session variable.

c) Click **Save**.

7. To supply RADIUS class attributes for use in the per-request policy, add a RADIUS Auth item anywhere in the access policy and configure its properties:

a) From the **Server** list, select an AAA RADIUS server.
b) Click **Save**.

This item populates the `session.radius.last.attr.class` session variable.

8. To supply local database groups for use in the per-request policy, add a Local Database item anywhere in the access policy and configure its properties:

a) From the **LocalDB Instance** list, select a local user database.
b) In the **User Name** field, retain the default session variable.
c) Click **Add new entry**
A new line is added to the list of entries with the Action set to **Read** and other default settings.
d) In the Destination column **Session Variable** field, type `session.localdb.groups`.

If you type a name other than `session.localdb.groups`, note it. You will need it when you configure the per-request access policy.

e) In the Source column from the **DB Property** list, select **groups**.
f) Click **Save**.

This item populates the `session.localdb.groups` session variable.

9. (Optional) To identify a user transparently, perform these substeps.

To use transparent user identification, you must have installed and configured a BIG-IP® user identification agent, either the F5® DC Agent or the F5 Logon Agent.

a) On an access policy branch, click the plus symbol **(+)** to add an item to the access policy.
b) From the Authentication tab, select **Transparent Identity Import** and click **Add Item**.

The transparent identity import access policy item searches the database in the IF-MAP server for the client source IP address. By default, this access policy item has two branches: associated and fallback.

A properties screen opens.

c) Click **Save**.
The visual policy editor displays.
d) Add any additional access policy items to the fallback or associated branches.
You might add Kerberos authentication on the fallback branch.

10. (Optional) To add Kerberos authentication to the access policy, perform these substeps:

a) On an access policy branch, click the plus symbol **(+)** to add an item to the access policy.
b) On the Logon tab, select **HTTP 401 Response** and click **Add Item**.
A Properties screen opens.
c) From the **HTTP Auth Level** list, select **negotiate** and click **Save**.
The properties screen closes.
d) Click the **(+)** icon on the **negotiate** branch.
A popup screen opens.
e) Type `ker` in the search field, select **Kerberos Auth** from the results, and click **Add Item**.
A properties screen opens.
f) From the **AAA Server** list, select an existing server.
g) From the **Request Based Auth** list, select **Disabled**.
h) Click **Save**.
The properties screen closes and the visual policy editor is displayed.

Note: *The **Max Logon Attempts Allowed** setting specifies attempts by an external client without a Kerberos ticket to authenticate on SWG forward proxy.*

---

11. Click the **Apply Access Policy** link to apply and activate the changes to the access policy.

To put an access policy into effect, you must assign it to a virtual server.

Creating a custom Client SSL forward proxy profile

Creating a Client SSL forward proxy profile makes it possible for client and server authentication, while still allowing the BIG-IP® system to perform data optimization, such as decryption and encryption. This profile applies to client-side SSL forward proxy traffic only.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.
The Client profile list screen opens.

2. Click **Create**.
   The New Client SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. From the **Parent Profile** list, select **clientssl**.
5. To avoid issues with privacy concerns, you might need to enable SSL forward proxy bypass for URLs that expose personal user information, such as those for financial or government sites.
   a) Scroll down to the **SSL Forward Proxy** list, and select **Advanced**.
   b) Select the **Custom** check box for the SSL Forward Proxy area.
   c) From the **SSL Forward Proxy** list, select **Enabled**.
      You can update this setting later but only while the profile is not assigned to a virtual server.
   d) From the **CA Certificate** list, select a certificate.
   e) From the **CA Key** list, select a key.
   f) In the **CA Passphrase** field, type a passphrase.
   g) In the **Confirm CA Passphrase** field, type the passphrase again.
   h) In the **Certificate Lifespan** field, type a lifespan for the SSL forward proxy certificate in days.
   i) (Optional) From the **Certificate Extensions** list, select **Extensions List**.
   j) (Optional) For the **Certificate Extensions List** setting, select the extensions that you want in the **Available extensions** field, and move them to the **Enabled Extensions** field using the **Enable** button.
   k) From the **SSL Forward Proxy Bypass** list, select **Enabled**.
      You can update this setting later but only while the profile is not assigned to a virtual server.
      Additional settings display.
   l) For **Default Bypass Action**, retain the default value **Intercept**.
      You can override the value of this action on a case-by-case basis in the per-request policy for the virtual server.

   Note: *Bypass and intercept lists do not work with per-request policies. Retain the setting* ***None*** *for the remainder of the fields.*

6. Click **Finished**.

The custom Client SSL forward proxy profile now appears in the Client SSL profile list screen.

Creating a custom Server SSL profile

Create a custom server SSL profile to support SSL forward proxy.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Server**.
   The SSL Server profile list screen opens.
2. Click **Create**.
   The New Server SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. For **Parent Profile**, retain the default selection, **serverssl**.
5. From the **Configuration** list, select **Advanced**.
6. Select the **Custom** check box.
   The settings become available for change.
7. From the **SSL Forward Proxy** list, select **Enabled**.
   You can update this setting later, but only while the profile is not assigned to a virtual server.

8. From the **SSL Forward Proxy Bypass** list, select **Enabled** (or retain the default value **Disabled**).
   The values of the **SSL Forward Proxy Bypass** settings in the server SSL and the client SSL profiles specified in a virtual server must match. You can update this setting later but only while the profile is not assigned to a virtual server.
9. Scroll down to the **Secure Renegotiation** list and select **Request**.
10. Click **Finished**.

The custom Server SSL profile is now listed in the SSL Server profile list.

Creating a virtual server for forward proxy SSL traffic

You configure a virtual server to handle SSL web traffic.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.
8. For the **SSL Profile (Client)** setting, from the **Available** list, select the name of the Client SSL forward proxy profile you previously created, and using the Move button, move the name to the **Selected** list.

   Important: *To enable SSL forward proxy functionality, you can either:*

   - Disassociate existing Client SSL and Server SSL profiles from a virtual server and configure the SSL Forward Proxy settings.
   - Create new Client SSL and Server SSL profiles and configure the SSL Forward Proxy settings.

   Then with either option, select the Client SSL and Server SSL profiles on a virtual server. You cannot modify existing Client SSL and Server SSL profiles while they are selected on a virtual server to enable SSL forward proxy functionality.

9. For the **SSL Profile (Server)** setting, from the **Available** list, select the name of the Server SSL forward proxy profile you previously created, and using the Move button, move the name to the **Selected** list.

   Important: *To enable SSL forward proxy functionality, you can either:*

   - Disassociate existing Client SSL and Server SSL profiles from a virtual server and configure the SSL Forward Proxy settings.
   - Create new Client SSL and Server SSL profiles and configure the SSL Forward Proxy settings.

   Then with either option, select the Client SSL and Server SSL profiles on a virtual server. You cannot modify existing Client SSL and Server SSL profiles while they are selected on a virtual server to enable SSL forward proxy functionality.

10. For the **Address Translation** setting, clear the **Enabled** check box.
11. For the **VLAN and Tunnel Traffic** setting, retain the default value **All VLANs and Tunnels** list.
12. From the **Source Address Translation** list, select **Auto Map**.

13. If you are using a captive portal, in the Access Policy area from the **Access Profile** list, select the access profile that you configured for transparent forward proxy, and from the **Per-Request Policy** list, select the per-request policy you configured earlier.
14. Click **Finished**.

The virtual server now appears in the Virtual Server List screen.

Creating a virtual server for forward proxy traffic

You configure a virtual server to handle web traffic going to port 80.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
5. In the **Service Port** field, type `80`, or select **HTTP** from the list.
6. From the **HTTP Profile** list, select **http**.
7. For the **VLAN and Tunnel Traffic** setting, retain the default value **All VLANs and Tunnels** list.
8. From the **Source Address Translation** list, select **Auto Map**.
9. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
10. From the **Per-Request Policy** list, select the per-request policy that you configured earlier.
11. Click **Finished**.

The virtual server now appears in the Virtual Server List screen.

Creating a forwarding virtual server

For Secure Web Gateway transparent forward proxy in inline mode, you create a forwarding virtual server to intercept IP traffic that is not going to ports 80 or 443.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. From the **Type** list, select **Forwarding (IP)**.
5. In the **Source Address** field, type `0.0.0.0/0`.
6. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
7. In the **Service Port** field, type `*` or select *** All Ports** from the list.
8. From the **Protocol** list, select *** All Protocols**.
9. From the **VLAN and Tunnel Traffic** list, retain the default selection, **All VLANs and Tunnels**.
10. From the **Source Address Translation** list, select **Auto Map**.
11. Click **Finished**.

Creating a Client SSL profile for a captive portal

You create a Client SSL profile when you want the BIG-IP® system to authenticate and decrypt/encrypt client-side application traffic. You create this profile if you enabled Captive Portals in the access profile and if you want to use SSL.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.
   The Client profile list screen opens.
2. Click **Create**.
   The New Client SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. For the **Parent Profile** list, retain the default value, **clientssl**.
5. Select the **Custom** check box.
6. In the Certificate Key Chain area, select a certificate and key combination to use for SSL encryption for the captive portal.

   This certificate should match the FQDN configured in the SWG-Transparent access profile to avoid security warnings, and should be generated by a certificate authority that your browser clients trust.

   Note: *If the key is encrypted, type a passphrase. Otherwise, leave the* ***Passphrase*** *field blank.*
7. Click **Finished**.

After creating the Client SSL profile and assigning the profile to a virtual server, the BIG-IP system can apply SSL security to the type of application traffic for which the virtual server is configured to listen.

Creating a virtual server for a captive portal

You configure a virtual server to use as a captive portal if you enabled the **Captive Portals** setting in the access profile.

Note: *If you do not plan to use client-side SSL, select a service port other than 443 and do not select a SSL (Client) profile.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type the IP address for a host virtual server.

   This field accepts an address in CIDR format (IP address/prefix). However, when you type the complete IP address for a host, you do not need to type a prefix after the address.

   Type a destination address in this format: `162.160.15.20`.
5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. From the **HTTP Profile** list, select **http**.
7. For the **SSL Profile (Client)** setting, move the profile you configured previously from the **Available** list to the **Selected** list.
8. Scroll down to the Access Policy area.
9. From the **Access Profile** list, select the access profile you configured previously.

10. From the **Per-Request Policy** list, select the per-request policy that you configured earlier.
11. Click **Finished**.

The virtual server appears in the Virtual Server List screen.

Implementation result

Web traffic that originates from your enterprise networks is now inspected and controlled by F5® Secure Web Gateway forward proxy.

Session variables for use in a per-request policy

Per-request policy items that look up the group or class to which a user belongs rely on the access policy to populate these session variables.

Per-request policy item	Session variable	Access policy item
AD Group Lookup	`session.ad.last.attr.primaryGroupID`	AD Query
LDAP Group Lookup	`session.ldap.last.attr.memberOf`	LDAP Query
LocalDB Group Lookup	`session.localdb.groups` ***Note:*** *This session variable is a default in the expression for LocalDB Group Lookup; any session variable in the expression must match the session variable used in the Local Database action in the access policy.*	Local Database
RADIUS Class Lookup	`session.radius.last.attr.class`	RADIUS Auth

About redirects after access denied by captive portal

A tool that captures HTTP traffic can reveal what appears to be an extra redirect after a user attempts to gain access using a captive portal but fails, and the access policy goes to a Deny ending. Instead of immediately redirecting the user to the logout page, the user is first redirected to the landing URI, and then a request to the landing URI is redirected to the logout page.

This sample output shows both redirects: the 302 to the landing page `http://berkeley.edu/index.html` and the 302 to the logout page `http://berkeley.edu/vdesk/hangup.php3`.

```
POST  https://bigip-master.com/my.policy?ORIG_URI=http://berkeley.edu/index.html
302   http://berkeley.edu/index.html

GET   http://berkeley.edu/index.html
302   http://berkeley.edu/vdesk/hangup.php3
```

Although the 302 to the landing page might seem to be an extra redirect, it is not. When a request is made, a subordinate virtual server transfers the request to the dominant virtual server to complete the access policy. When the dominant virtual completes the access policy, it transfers the user back to the subordinate virtual server, on the same original request. The subordinate virtual server then enforces the result of the access policy.

Overview: Configuring transparent forward proxy

In transparent forward proxy, you configure your internal network to forward web traffic to the BIG-IP® system with Secure Web Gateway (SWG). Use this implementation when your topology includes a router on which you can configure policy-based routing or Web Cache Communication Protocol (WCCP) to send any traffic for ports 80 and 443 to the BIG-IP system.

This implementation describes only the configuration required on the BIG-IP system.

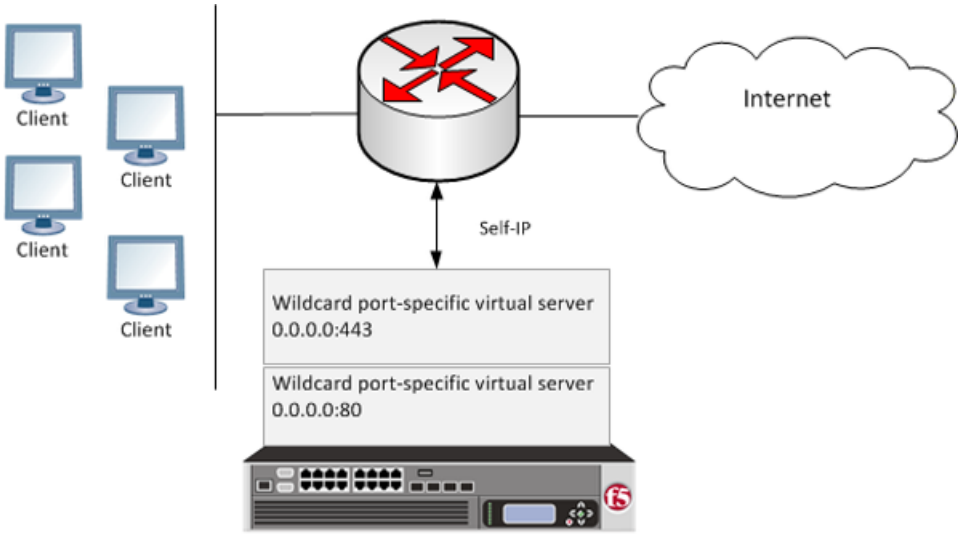

Figure 10: Secure Web Gateway transparent forward proxy deployment

The router sends traffic to the self-ip address of a VLAN configured on the BIG-IP system. Virtual servers listen on the VLAN and process the traffic that most closely matches the virtual server address. Secure Web Gateway identifies users without using session management cookies, and applies a scheme that categorizes and filters URLs, controlling access.

Note: *Transparent forward proxy provides the option to use a captive portal. To use this option, you need an additional virtual server, not shown in the figure, for the captive portal primary authentication server.*

Task Summary

Creating a VLAN for transparent forward proxy
Assigning a self IP address to a VLAN
Configuring a per-request policy for SWG
Creating an access profile for SWG transparent forward proxy
Configuring an access policy for transparent forward proxy
Creating a custom Client SSL forward proxy profile
Creating a custom Server SSL profile
Creating a virtual server for forward proxy SSL traffic
Creating a virtual server for forward proxy traffic
Creating a Client SSL profile for a captive portal
Creating a virtual server for a captive portal

SWG transparent forward proxy configuration prerequisites

To use Secure Web Gateway (SWG), you must configure URL categorization. You might need to configure additional items depending on the other features that you decide to use.

URL categorization

To get a working SWG configuration, you must first download URL categories, configure URL filters, and configure schemes.

Transparent user identification

If you plan to identify users transparently, you must first download, install, and configure a BIG-IP user identification agent, either the F5® DC Agent or the F5 Logon Agent.

Authentication

F5 recommends that you use NTLM or Kerberos authentication. If you plan to use authentication, ensure that you have what you need configured.

- For NTLM, you need an NTLM Auth Configuration in Access Policy Manager® (APM®).
- For Kerberos, you need a domain-joined Kerberos user account and a Kerberos AAA server configured in APM.

SSL intercept

To intercept SSL connections that are passing through the proxy, ensure that you have imported a valid subordinate CA certificate and key that is trusted by the endpoints behind the proxy.

Captive portal

If you plan to use the captive portal feature, make sure that a certificate and key with the proper common name is imported for use.

About the iApp for Secure Web Gateway configuration

When deployed as an application service, the Secure Web Gateway iApps® template can set up either an explicit or a transparent forward proxy configuration. You can download the template from the F5® DevCentral™ iApp Codeshare wiki at (`http://devcentral.f5.com/wiki/iapp.Codeshare.ashx`).

About ways to configure user identification for SWG

User identification configuration requires a method setting in the access profile and an access policy configured to support the setting. Depending on the access profile type, you can select one of these user identification methods: by IP address (for SWG-Explicit or SWG-Transparent access profile types) or by credentials (for SWG-Explicit type).

Identification by IP address

When you identify users by IP address, you can employ any of these methods.

Note: *Identify users by IP address only when IP addresses are unique and can be trusted.*

---

transparent user identification

Transparent user identification makes a best effort to identify users without requesting credentials. An agent obtains data and stores a mapping of IP addresses to user names in an IF-MAP server. An F5 DC

Agent queries domain controllers. An F5 Logon Agent runs a script when a client logs in and can run a script when the client logs out.

Note: *To identify users transparently, you must first install and configure one BIG-IP user identification agent, either the F5® DC Agent or the F5 Logon Agent.*

---

explicit user identification

You can present a logon page in an access policy to request user credentials and validate them. SWG maintains an internal mapping of IP addresses to user names. (You can present the appropriate logon page for the access policy type. For explicit forward proxy, you can present a 407 page. For transparent forward proxy, you can present a 401 page.)

source IP ranges or subnets

You can forego actually identifying the user and base the choice of which scheme to apply on whether the IP address is in a source IP range or on a subnet. SWG maintains an internal mapping of IP addresses to sessions.

Identification by credentials

When you choose to identify users by credentials, SWG maintains an internal mapping of credentials to sessions. To support this choice, you need an NTLM Auth Configuration object and you should check the result of NTLM authentication in the access policy.

Creating a VLAN for transparent forward proxy

You need a VLAN on which the forward proxy can listen. For increased security, the VLAN should directly face your clients.

1. On the Main tab, click **Network** > **VLANs**.
   The VLAN List screen opens.
2. Click **Create**.
   The New VLAN screen opens.
3. In the **Name** field, type a unique name for the VLAN.
4. For the **Interfaces** setting,
   a) From the **Interface** list, select an interface number.
   b) From the **Tagging** list, select **Untagged**.
   c) Click **Add**.
5. Click **Finished**.
   The screen refreshes, and displays the new VLAN in the list.

The new VLAN appears in the VLAN list.

Assigning a self IP address to a VLAN

Assign a self IP address to a VLAN on which the forward proxy listens.

1. On the Main tab, click **Network** > **Self IPs**.
2. Click **Create**.
   The New Self IP screen opens.
3. In the **Name** field, type a unique name for the self IP address.

4. In the **IP Address** field, type the IP address of the VLAN.
   The system accepts IPv4 and IPv6 addresses.
5. In the **Netmask** field, type the full network mask for the specified IP address.
   For example, you can type `ffff:ffff:ffff:ffff:0000:0000:0000:0000` or `ffff:ffff:ffff:ffff::`.
6. From the **VLAN/Tunnel** list, select the VLAN.
7. Click **Finished**.
   The screen refreshes, and displays the new self IP address.

Configuring a per-request policy for SWG

Configure a per-request policy to specify the logic that determines how to process web traffic.

Note: *A per-request policy must determine whether to bypass SSL traffic and, otherwise, whether to allow or reject a URL request in a Secure Web Gateway (SWG) forward proxy configuration.*

1. On the Main tab, click **Access Policy** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. Click **Create**.
   The General Properties screen displays.
3. In the **Name** field, type a name for the policy and click **Finished**.
   A per-request policy name must be unique among all per-request policy and access profile names.
   The policy name appears on the Per-Request Policies screen.
4. In the Access Policy column for the per-request policy that you want to update, click the **Edit** link.
   The visual policy editor opens in another tab.
5. To create different branches for processing HTTP and HTTPS traffic, add a **Protocol Lookup** item.
   a) Click the **(+)** icon anywhere in the per-request policy to add a new item.
      A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
   b) Type `prot` in the Search field, select **Protocol Lookup**, and click **Add Item**.
      A Properties popup screen opens.
   c) Click **Save**.
      The Properties screen closes. The visual policy editor displays.
6. If you configured SSL forward proxy bypass in the client and server SSL profiles, include an **SSL Intercept Set** item to ensure that SSL traffic is not bypassed until this policy determines that it should be.
   It is important to include SSL Intercept Set when the default SSL bypass action in the client SSL profile is set to Bypass.
7. To retrieve the requested URL and the categories to which it belongs, add a **Category Lookup** item.

   Important: *A Category Lookup item is required to trigger event logging for SWG, to provide a response web page for the Response Analytics item, and to provide categories for the URL Filter Assign item.*

   a) Click the **(+)** icon anywhere in the per-request policy to add a new item.
      A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
   b) Type `cat` in the Search field, select **Category Lookup**, and click **Add Item**.

A Properties popup screen opens.

c) From the **Categorization Input** list, select how to obtain the requested URL. For HTTP traffic, select **Use HTTP URI (cannot be used for SSL Bypass decisions)**. For SSL-encrypted traffic, select either **Use SNI in Client Hello (if SNI is not available, use Subject.CN)** or **Use Subject.CN in Server Cert**.
If you select **Use HTTP URI (cannot be used for SSL Bypass decisions)**, the **SafeSearch Mode** list displays and **Enabled** is selected.

d) From the **Category Lookup Type** list, select the category types in which to search for the requested URL. Select one from **Custom categories first, then standard categories if not found**, **Always process full list of both custom and standard categories**, or **Process standard categories only**.
Depending on your selection, the Category Lookup Type item looks through custom categories or standard categories or both, and compiles a list of one or more categories from them. The list is available for subsequent processing by the URL Filter Assign item.

e) Click **Save**.
The Properties screen closes. The visual policy editor displays.

8. To enable Safe Search for SSL-encrypted traffic, add an additional Category Lookup item, specify **Use HTTP URI (cannot be used for SSL Bypass decisions)** as the **Category Lookup Type**, and retain the default setting (**Enabled**) for **SafeSearch Mode**.

9. At any point in the policy where a decision to bypass SSL traffic is made, add an **SSL Bypass Set** item.

10. Add any of these items to the policy.

Item	Description
Dynamic Date Time	Branch by day of week or time of day.
AD Group Lookup	Branch by user group. Requires branch rule configuration.
LDAP Group Lookup	Branch by user group. Requires branch rule configuration.
LocalDB Group Lookup	Branch by user group. Requires branch rule configuration.
RADIUS Class Lookup	Branch by the class attribute. Requires branch rule configuration.

11. To configure a branch rule for a LocalDB Group Lookup item:

a) In the visual policy editor, click the name of the item.
A Properties popup screen opens.

b) Click the Branch Rules tab.

c) To edit an expression, click the **change** link.
An additional popup screen opens, displaying the Simple tab.

d) If the Local Database action in the access policy was configured to read groups into the `session.localdb.groups` session variable, edit the default simple expression, **User is a member of** `MY_GROUP`, replacing MY_GROUP with a relevant group.

e) If the Local Database action in the access policy was configured to read groups into a session variable other than `session.localdb.groups`, click the Advanced tab; edit the default advanced expression, `expression is expr { [mcget {session.localdb.groups}] contains "`*`MY_GROUP`*`" }`, replacing MY_GROUP with a relevant group and `session.localdb.groups` with the session variable specified in the Local Database action.

f) Click **Finished**.
The popup screen closes.

g) Click **Save**.
The popup screen closes. The visual policy editor displays.

12. To configure a branch rule for AD, LDAP, or RADIUS group or class lookups:

a) In the visual policy editor, click the name of the policy item.
A Properties popup screen opens.
b) Click the Branch Rules tab.
c) To edit an expression, click the **change** link.
An additional popup screen opens, displaying the Simple tab.
d) Edit the default simple expression to specify group or class that is used in your environment.
In an LDAP Group Lookup item, the default simple expression is **User is a member of** `CN=MY_GROUP, CN=USERS, CN=MY_DOMAIN`. You can use the simple expression editor to replace the default values.
e) Click **Finished**.
The popup screen closes.
f) Click **Save**.
The popup screen closes. The visual policy editor displays.

13. To trigger inspection of the response web page contents, add a Response Analytics item.

A Category Lookup item must precede this item.

a) In the **Max Buffer Size** field, type the number of bytes to buffer.
b) In the **Max Buffer time** field, type the number of seconds to retain response data in the buffer.
c) For the **Reset on Failure** field, retain the default value **Enabled** to send a TCP reset if the server fails.
d) For each type of content that you want to exclude from analysis, click **Add new entry** and then select a type from the list.

The **All-Images** type is on the list by default because images are not scanned.

e) Click **Finished**.
The popup screen closes.
f) Click **Save**.

The fallback branch after this item indicates that a failure occurred during content analysis. The Success branch indicates that content analysis completed.

The popup screen closes. The visual policy editor displays.

14. Add a URL Filter Assign item after the Response Analytics item, if included on the branch; otherwise, add it anywhere on a branch after a Category Lookup item.

In this item, you must specify a URL filter to apply to the URL categories that the Category Lookup item returned. If any URL category specifies the Block filtering action, this item blocks the request. This item also blocks the request if the Response Analytics item identified malicious content.

To put the per-request policy into effect, add it to the virtual server.

Creating an access profile for SWG transparent forward proxy

You create an access profile to provide the access policy configuration for a virtual server that establishes a secured session.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
The Access Profiles List screen opens.

2. Click **Create**.

The New Profile screen opens.

3. In the **Name** field, type a name for the access profile.

   Note: *An access profile name must be unique among all access profile and per-request policy names.*

4. From the **Profile Type** list, select **SWG-Transparent**.

   With this type, only the access policy items that are valid for Secure Web Gateway (SWG) transparent forward proxy are available in the visual policy editor.

5. Select the **Custom** check box for **Settings**.
   The settings become available.
6. (Optional) To use NTLM authentication before a session starts, from the **NTLM Auth Configuration** list select a configuration.

   In the case of a shared machine, an IP address might already be associated with a user or a session. Using NTLM authentication ensures that the system can associate the IP address with the correct session (new or existing) or with a new user each time a user logs on to the shared machine.

7. (Optional) To direct users to a captive portal, for **Captive Portal** select **Enabled** and, in the **Primary Authentication URI** field, type the URI.

   You might specify the URI of your primary authentication server if you use single sign-on across multiple domains. Users can then access multiple back-end applications from multiple domains and hosts without needing to re-enter their credentials, because the user session is stored on the primary domain.

   For example, you might type `https://logon.siterequest.com` in the field.

8. In the Language Settings area, add and remove accepted languages, and set the default language.

   A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.

9. Click **Finished**.
   The Access Profiles list screen displays.
10. To enable Secure Web Gateway event logging for this access profile, add log settings.
    a) Click the name of the access profile that you just created.
       The Properties screen displays.
    b) On the menu bar, click **Logs**.
       The General Properties screen displays.
    c) In the Log Settings area, move log settings from the **Available** list to the **Selected** list.

    You can configure log settings in the Access Policy Event Logs area of the product.

This creates an access profile with a default access policy.

Configuring an access policy for transparent forward proxy

You configure an access policy for Secure Web Gateway (SWG) transparent forward proxy to assign an SWG scheme to the policy and to populate session variables with group or class attribute information for use in the per-request policy. You can also add access policy items to collect credentials and to authenticate a user or you can add items to transparently identify the user without requesting credentials.

Note: *If you include authentication in your access policy and the first site that a user accesses uses HTTP instead of secure HTTP, passwords are passed as clear text. To prevent this from happening, F5® recommends using Kerberos or NTLM authentication.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.

The Access Profiles List screen opens.

2. Click the **(+)** icon anywhere in the access policy to add a new action item.

Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.

3. If you specified an NTLM Auth configuration in the access profile, verify that authentication succeeded.
   a) Type `NTLM` in the search field.
   b) Select **NTLM Auth Result** from the results list.
   c) Click **Add Item**.
   A properties popup screen opens.
   d) Click **Save**.
   The Properties screen closes. The visual policy editor displays.

4. Assign an SWG scheme to the access policy:

   Scheme assignment is mandatory.
   a) Click the **(+)** icon anywhere in the access policy to add a new action item.
   b) On the Assignment tab, select **SWG Scheme Assign** and click **Add Item**.
   A Properties screen opens.

   a) To display the available schemes, click the **Add/Delete** link.
   b) Select one scheme and click **Save**.
   The Properties screen closes and the visual policy editor displays.

5. To supply LDAP group information for use in the per-request policy, add an LDAP Query item anywhere in the access policy and configure its properties:
   a) From the **Server** list, select an AAA LDAP server.

      An LDAP Query uses SSL connections when you select an LDAP AAA server that is configured for LDAPS.
   b) Specify the **SearchDN**, and **SearchFilter** settings.

      SearchDN is the base DN from which the search is done.
   c) Click **Save**.

   This item populates the `session.ldap.last.attr.memberOf` session variable.

6. To supply Active Directory groups for use in the per-request policy, add an AD Query item anywhere in the access policy and configure its properties:
   a) From the **Server** list, select an AAA AD server.
   b) Select the **Fetch Primary Group** check box.

      The value of the primary user group populates the `session.ad.last.attr.primaryGroupID` session variable.
   c) Click **Save**.

7. To supply RADIUS class attributes for use in the per-request policy, add a RADIUS Auth item anywhere in the access policy and configure its properties:
   a) From the **Server** list, select an AAA RADIUS server.
   b) Click **Save**.

   This item populates the `session.radius.last.attr.class` session variable.

8. To supply local database groups for use in the per-request policy, add a Local Database item anywhere in the access policy and configure its properties:
   a) From the **LocalDB Instance** list, select a local user database.
   b) In the **User Name** field, retain the default session variable.
   c) Click **Add new entry**
      A new line is added to the list of entries with the Action set to **Read** and other default settings.
   d) In the Destination column **Session Variable** field, type `session.localdb.groups`.
      If you type a name other than `session.localdb.groups`, note it. You will need it when you configure the per-request access policy.
   e) In the Source column from the **DB Property** list, select **groups**.
   f) Click **Save**.

   This item populates the `session.localdb.groups` session variable.

9. (Optional) To identify a user transparently, perform these substeps.
   To use transparent user identification, you must have installed and configured a BIG-IP® user identification agent, either the F5® DC Agent or the F5 Logon Agent.
   a) On an access policy branch, click the plus symbol **(+)** to add an item to the access policy.
   b) From the Authentication tab, select **Transparent Identity Import** and click **Add Item**.
      The transparent identity import access policy item searches the database in the IF-MAP server for the client source IP address. By default, this access policy item has two branches: associated and fallback.
      A properties screen opens.
   c) Click **Save**.
      The visual policy editor displays.
   d) Add any additional access policy items to the fallback or associated branches.
      You might add Kerberos authentication on the fallback branch.

10. (Optional) To add Kerberos authentication to the access policy, perform these substeps:
    a) On an access policy branch, click the plus symbol **(+)** to add an item to the access policy.
    b) On the Logon tab, select **HTTP 401 Response** and click **Add Item**.
       A Properties screen opens.
    c) From the **HTTP Auth Level** list, select **negotiate** and click **Save**.
       The properties screen closes.
    d) Click the **(+)** icon on the **negotiate** branch.
       A popup screen opens.
    e) Type `ker` in the search field, select **Kerberos Auth** from the results, and click **Add Item**.
       A properties screen opens.
    f) From the **AAA Server** list, select an existing server.
    g) From the **Request Based Auth** list, select **Disabled**.
    h) Click **Save**.
       The properties screen closes and the visual policy editor is displayed.

    Note: *The **Max Logon Attempts Allowed** setting specifies attempts by an external client without a Kerberos ticket to authenticate on SWG forward proxy.*

    ---

11. Click the **Apply Access Policy** link to apply and activate the changes to the access policy.

To put an access policy into effect, you must assign it to a virtual server.

Creating a custom Client SSL forward proxy profile

Creating a Client SSL forward proxy profile makes it possible for client and server authentication, while still allowing the BIG-IP® system to perform data optimization, such as decryption and encryption. This profile applies to client-side SSL forward proxy traffic only.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.
   The Client profile list screen opens.
2. Click **Create**.
   The New Client SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. From the **Parent Profile** list, select **clientssl**.
5. To avoid issues with privacy concerns, you might need to enable SSL forward proxy bypass for URLs that expose personal user information, such as those for financial or government sites.
   a) Scroll down to the **SSL Forward Proxy** list, and select **Advanced**.
   b) Select the **Custom** check box for the SSL Forward Proxy area.
   c) From the **SSL Forward Proxy** list, select **Enabled**.
      You can update this setting later but only while the profile is not assigned to a virtual server.
   d) From the **CA Certificate** list, select a certificate.
   e) From the **CA Key** list, select a key.
   f) In the **CA Passphrase** field, type a passphrase.
   g) In the **Confirm CA Passphrase** field, type the passphrase again.
   h) In the **Certificate Lifespan** field, type a lifespan for the SSL forward proxy certificate in days.
   i) (Optional) From the **Certificate Extensions** list, select **Extensions List**.
   j) (Optional) For the **Certificate Extensions List** setting, select the extensions that you want in the **Available extensions** field, and move them to the **Enabled Extensions** field using the **Enable** button.
   k) From the **SSL Forward Proxy Bypass** list, select **Enabled**.
      You can update this setting later but only while the profile is not assigned to a virtual server.
      Additional settings display.
   l) For **Default Bypass Action**, retain the default value **Intercept**.
      You can override the value of this action on a case-by-case basis in the per-request policy for the virtual server.

   Note: *Bypass and intercept lists do not work with per-request policies. Retain the setting* ***None*** *for the remainder of the fields.*

6. Click **Finished**.

The custom Client SSL forward proxy profile now appears in the Client SSL profile list screen.

Creating a custom Server SSL profile

Create a custom server SSL profile to support SSL forward proxy.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Server**.
   The SSL Server profile list screen opens.
2. Click **Create**.
   The New Server SSL Profile screen opens.

3. In the **Name** field, type a unique name for the profile.
4. For **Parent Profile**, retain the default selection, **serverssl**.
5. From the **Configuration** list, select **Advanced**.
6. Select the **Custom** check box.
   The settings become available for change.
7. From the **SSL Forward Proxy** list, select **Enabled**.
   You can update this setting later, but only while the profile is not assigned to a virtual server.
8. From the **SSL Forward Proxy Bypass** list, select **Enabled** (or retain the default value **Disabled**).
   The values of the **SSL Forward Proxy Bypass** settings in the server SSL and the client SSL profiles specified in a virtual server must match. You can update this setting later but only while the profile is not assigned to a virtual server.
9. Scroll down to the **Secure Renegotiation** list and select **Request**.
10. Click **Finished**.

The custom Server SSL profile is now listed in the SSL Server profile list.

Creating a virtual server for forward proxy SSL traffic

You configure a virtual server to handle SSL web traffic.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.
8. For the **SSL Profile (Client)** setting, from the **Available** list, select the name of the Client SSL forward proxy profile you previously created, and using the Move button, move the name to the **Selected** list.

   Important: *To enable SSL forward proxy functionality, you can either:*

   - Disassociate existing Client SSL and Server SSL profiles from a virtual server and configure the SSL Forward Proxy settings.
   - Create new Client SSL and Server SSL profiles and configure the SSL Forward Proxy settings.

   Then with either option, select the Client SSL and Server SSL profiles on a virtual server. You cannot modify existing Client SSL and Server SSL profiles while they are selected on a virtual server to enable SSL forward proxy functionality.

   ---

9. For the **SSL Profile (Server)** setting, from the **Available** list, select the name of the Server SSL forward proxy profile you previously created, and using the Move button, move the name to the **Selected** list.

   Important: *To enable SSL forward proxy functionality, you can either:*

   - Disassociate existing Client SSL and Server SSL profiles from a virtual server and configure the SSL Forward Proxy settings.
   - Create new Client SSL and Server SSL profiles and configure the SSL Forward Proxy settings.

Then with either option, select the Client SSL and Server SSL profiles on a virtual server. You cannot modify existing Client SSL and Server SSL profiles while they are selected on a virtual server to enable SSL forward proxy functionality.

10. For the **Address Translation** setting, clear the **Enabled** check box.
11. For the **VLAN and Tunnel Traffic** setting, retain the default value **All VLANs and Tunnels** list.
12. From the **Source Address Translation** list, select **Auto Map**.
13. If you are using a captive portal, in the Access Policy area from the **Access Profile** list, select the access profile that you configured for transparent forward proxy, and from the **Per-Request Policy** list, select the per-request policy you configured earlier.
14. Click **Finished**.

The virtual server now appears in the Virtual Server List screen.

Creating a virtual server for forward proxy traffic

You configure a virtual server to handle web traffic going to port 80.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
5. In the **Service Port** field, type `80`, or select **HTTP** from the list.
6. From the **HTTP Profile** list, select **http**.
7. For the **VLAN and Tunnel Traffic** setting, retain the default value **All VLANs and Tunnels** list.
8. From the **Source Address Translation** list, select **Auto Map**.
9. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
10. From the **Per-Request Policy** list, select the per-request policy that you configured earlier.
11. Click **Finished**.

The virtual server now appears in the Virtual Server List screen.

Creating a Client SSL profile for a captive portal

You create a Client SSL profile when you want the BIG-IP® system to authenticate and decrypt/encrypt client-side application traffic. You create this profile if you enabled Captive Portals in the access profile and if you want to use SSL.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.
   The Client profile list screen opens.
2. Click **Create**.
   The New Client SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. For the **Parent Profile** list, retain the default value, **clientssl**.

5. Select the **Custom** check box.
6. In the Certificate Key Chain area, select a certificate and key combination to use for SSL encryption for the captive portal.

   This certificate should match the FQDN configured in the SWG-Transparent access profile to avoid security warnings, and should be generated by a certificate authority that your browser clients trust.

   Note: *If the key is encrypted, type a passphrase. Otherwise, leave the* ***Passphrase*** *field blank.*
7. Click **Finished**.

After creating the Client SSL profile and assigning the profile to a virtual server, the BIG-IP system can apply SSL security to the type of application traffic for which the virtual server is configured to listen.

Creating a virtual server for a captive portal

You configure a virtual server to use as a captive portal if you enabled the **Captive Portals** setting in the access profile.

Note: *If you do not plan to use client-side SSL, select a service port other than 443 and do not select a SSL (Client) profile.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type the IP address for a host virtual server.

   This field accepts an address in CIDR format (IP address/prefix). However, when you type the complete IP address for a host, you do not need to type a prefix after the address.

   Type a destination address in this format: `162.160.15.20`.
5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. From the **HTTP Profile** list, select **http**.
7. For the **SSL Profile (Client)** setting, move the profile you configured previously from the **Available** list to the **Selected** list.
8. Scroll down to the Access Policy area.
9. From the **Access Profile** list, select the access profile you configured previously.
10. From the **Per-Request Policy** list, select the per-request policy that you configured earlier.
11. Click **Finished**.

The virtual server appears in the Virtual Server List screen.

Implementation result

Web traffic that originates from your enterprise networks is now inspected and controlled by F5® Secure Web Gateway forward proxy.

Session variables for use in a per-request policy

Per-request policy items that look up the group or class to which a user belongs rely on the access policy to populate these session variables.

Per-request policy item	Session variable	Access policy item
AD Group Lookup	`session.ad.last.attr.primaryGroupID`	AD Query
LDAP Group Lookup	`session.ldap.last.attr.memberOf`	LDAP Query
LocalDB Group Lookup	`session.localdb.groups` ***Note:*** *This session variable is a default in the expression for LocalDB Group Lookup; any session variable in the expression must match the session variable used in the Local Database action in the access policy.*	Local Database
RADIUS Class Lookup	`session.radius.last.attr.class`	RADIUS Auth

About redirects after access denied by captive portal

A tool that captures HTTP traffic can reveal what appears to be an extra redirect after a user attempts to gain access using a captive portal but fails, and the access policy goes to a Deny ending. Instead of immediately redirecting the user to the logout page, the user is first redirected to the landing URI, and then a request to the landing URI is redirected to the logout page.

This sample output shows both redirects: the 302 to the landing page `http://berkeley.edu/index.html` and the 302 to the logout page `http://berkeley.edu/vdesk/hangup.php3`.

```
POST  https://bigip-master.com/my.policy?ORIG_URI=http://berkeley.edu/index.html
302   http://berkeley.edu/index.html

GET   http://berkeley.edu/index.html
302   http://berkeley.edu/vdesk/hangup.php3
```

Although the 302 to the landing page might seem to be an extra redirect, it is not. When a request is made, a subordinate virtual server transfers the request to the dominant virtual server to complete the access policy. When the dominant virtual completes the access policy, it transfers the user back to the subordinate virtual server, on the same original request. The subordinate virtual server then enforces the result of the access policy.

Chapter 7

Remote Access Configuration

- *Overview: Configuring SWG explicit forward proxy for network access*
- *Overview: Configuring SWG transparent forward proxy for remote access*

Overview: Configuring SWG explicit forward proxy for network access

You can configure Secure Web Gateway (SWG) explicit forward proxy and network access configurations so that SWG processes the Internet traffic from a network access client in the same way that it processes such traffic from a client in the enterprise.

Note: *Using a distinct SWG explicit forward proxy configuration to process traffic from remote clients separately from an SWG configuration used for processing traffic from internal clients provides an important measure of network security.*

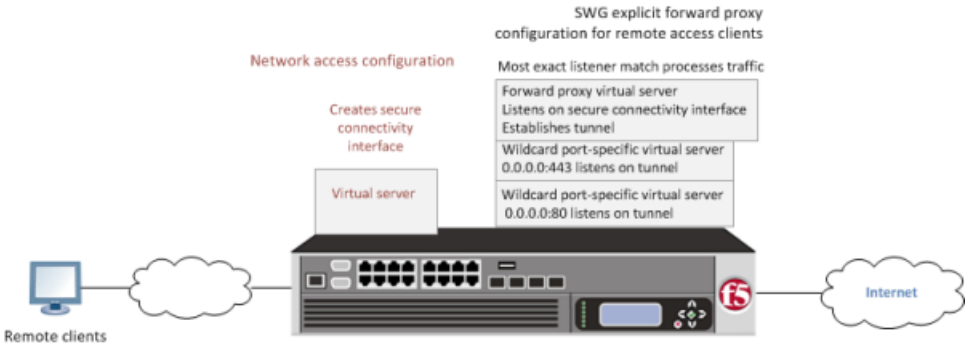

Figure 11: Explicit forward proxy for network access

You should understand how these configuration objects fit into the overall configuration.

Secure connectivity interface

In a network access configuration, a connectivity profile on the virtual server specifies a secure connectivity interface for traffic from the client. In the SWG configuration, an SWG explicit forward proxy server must listen on the secure connectivity interface for traffic from network access clients.

Tunnel

In the SWG configuration, an HTTP profile on the explicit forward proxy server specifies the name of a tunnel of tcp-forward encapsulation type. You can use the default tunnel, http-tunnel, or create another tunnel and use it.

Per-request policy

In any SWG configuration, the determination of whether a user can access a URL must be made in a per-request policy. A per-request policy determines whether to block or allow access to a request based on time or date or group membership or other criteria that you configure.

Access policies

The access policy in the network access configuration continues to authenticate users, assign resources, and evaluate ACLs, if any. In addition, this access policy must assign an SWG scheme for the network access session and populate any session variables used in the per-request policy. An access profile of the SWG-Explicit type is required in the SWG configuration; however, it is not necessary to include any items in the access policy.

Task summary

Creating a connectivity profile
Adding a connectivity profile to a virtual server
Creating a DNS resolver
Adding forward zones to a DNS resolver

Creating a custom HTTP profile for explicit forward proxy
Configuring a per-request policy for SWG
Creating an access profile for SWG explicit forward proxy
Creating a virtual server for network access client forward proxy server
Creating a wildcard virtual server for HTTP tunnel traffic
Creating a custom Client SSL forward proxy profile
Creating a custom Server SSL profile
Creating a wildcard virtual server for SSL traffic on the HTTP tunnel
Updating the access policy in the remote access configuration
Configuring a network access resource to forward traffic

Prerequisites for SWG explicit forward proxy for network access

Before you start to create a Secure Web Gateway (SWG) explicit forward proxy configuration to support network access clients, you must have completed these tasks.

- You need to have configured a working network access configuration.
- If you have not already done so, you must ensure that the URL database is downloaded.
- You need to have configured at least one SWG scheme and any URL filters that you want to use in addition to or instead of the default URL filters.

Configuration outline for explicit forward proxy for network access

Tasks for integrating an Access Policy Manager® (APM®) network access configuration with a Secure Web Gateway (SWG) explicit forward proxy configuration follow this order.

- First, if your network access configuration does not include a connectivity profile, create one and add it to the virtual server.
- Next, create an SWG explicit forward proxy configuration. This configuration includes the per-request policy.
- Finally, in the network access configuration, update the access policy (so that it assigns an SWG scheme and populates any session variables required for successful execution of the per-request policy) and update the network access resource for client proxy.

Creating a connectivity profile

You create a connectivity profile to configure client connections.

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Click **Add**.
   The Create New Connectivity Profile popup screen opens and displays General Settings.
3. Type a **Profile Name** for the connectivity profile.
4. Select a **Parent Profile** from the list.
   APM® provides a default profile, **connectivity**.
5. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.

The connectivity profile appears in the list.

To provide functionality with a connectivity profile, you must add the connectivity profile to a virtual server.

Adding a connectivity profile to a virtual server

Update a virtual server that is part of an Access Policy Manager® application access, network access, or portal access configuration to enable a secure connectivity interface for traffic from the client.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. Scroll down to the Access Policy area.
4. From the **Connectivity Profile** list, select the connectivity profile.
5. Click **Update** to save the changes.

Creating a DNS resolver

You configure a DNS resolver on the BIG-IP® system to resolve DNS queries and cache the responses. The next time the system receives a query for a response that exists in the cache, the system returns the response from the cache.

1. On the Main tab, click **Network** > **DNS Resolvers** > **DNS Resolver List**.
   The DNS Resolver List screen opens.
2. Click **Create**.
   The New DNS Resolver screen opens.
3. In the **Name** field, type a name for the resolver.
4. Click **Finished**.

Adding forward zones to a DNS resolver

Before you begin, gather the IP addresses of the nameservers that you want to associate with a forward zone.

Add a forward zone to a DNS resolver when you want the BIG-IP® system to forward queries for particular zones to specific nameservers for resolution in case the resolver does not contain a response to the query.

Note: *Creating a forward zone is optional. Without one, a DNS resolver can still make recursive name queries to the root DNS servers; however, this requires that the virtual servers using the cache have a route to the Internet.*

---

1. On the Main tab, click **Network** > **DNS Resolvers** > **DNS Resolver List**.
   The DNS Resolver List screen opens.
2. Click the name of the resolver you want to modify.
   The properties screen opens.
3. On the menu bar, click **Forward Zones**.
   The Forward Zones screen displays.
4. Click the **Add** button.

Note: *You add more than one zone to forward based on the needs of your organization.*

5. In the **Name** field, type the name of a subdomain or type the fully qualified domain name (FQDN) of a forward zone.
   For example, either `example` or `site.example.com` would be valid zone names.
6. Add one or more nameservers:
   a) In the **Address** field, type the IP address of a DNS nameserver that is considered authoritative for this zone.
      Based on your network configuration, add IPv4 or IPv6 addresses, or both.
   b) Click **Add**.
      The address is added to the list.

Note: *The order of nameservers in the configuration does not impact which nameserver the system selects to forward a query to.*

7. Click **Finished**.

Creating a custom HTTP profile for explicit forward proxy

An HTTP profile defines the way that you want the BIG-IP®system to manage HTTP traffic.

Note: *Secure Web Gateway (SWG) explicit forward proxy requires a DNS resolver that you select in the HTTP profile.*

1. On the Main tab, click **Local Traffic** > **Profiles** > **Services** > **HTTP**.
   The HTTP profile list screen opens.
2. Click **Create**.
   The New HTTP Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. From the **Proxy Mode** list, select **Explicit**.
5. For **Parent Profile**, retain the **http-explicit** setting.
6. Select the **Custom** check box.
7. Scroll down to the Explicit Proxy area.
8. From the **DNS Resolver** list, select the DNS resolver you configured previously.
9. In the **Tunnel Name** field, you can retain the default value, **http-tunnel**, or type the name of a tunnel if you created one.
   SWG requires a tunnel with tcp-forward encapsulation to support SSL traffic for explicit forward proxy.
10. From the **Default Connect Handling** list, retain the default setting **Deny**.
    Any CONNECT traffic goes through the tunnel to the virtual server that most closely matches the traffic; if there is no match, the traffic is blocked.
11. Click **Finished**.

The custom HTTP profile now appears in the HTTP profile list screen.

Configuring a per-request policy for SWG

Configure a per-request policy to specify the logic that determines how to process web traffic.

Note: *A per-request policy must determine whether to bypass SSL traffic and, otherwise, whether to allow or reject a URL request in a Secure Web Gateway (SWG) forward proxy configuration.*

1. On the Main tab, click **Access Policy** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. Click **Create**.
   The General Properties screen displays.
3. In the **Name** field, type a name for the policy and click **Finished**.

   A per-request policy name must be unique among all per-request policy and access profile names.

   The policy name appears on the Per-Request Policies screen.
4. In the Access Policy column for the per-request policy that you want to update, click the **Edit** link.
   The visual policy editor opens in another tab.
5. To create different branches for processing HTTP and HTTPS traffic, add a **Protocol Lookup** item.
   a) Click the **(+)** icon anywhere in the per-request policy to add a new item.
      A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
   b) Type `prot` in the Search field, select **Protocol Lookup**, and click **Add Item**.
      A Properties popup screen opens.
   c) Click **Save**.
      The Properties screen closes. The visual policy editor displays.
6. If you configured SSL forward proxy bypass in the client and server SSL profiles, include an **SSL Intercept Set** item to ensure that SSL traffic is not bypassed until this policy determines that it should be.

   It is important to include SSL Intercept Set when the default SSL bypass action in the client SSL profile is set to Bypass.
7. To retrieve the requested URL and the categories to which it belongs, add a **Category Lookup** item.

   Important: *A Category Lookup item is required to trigger event logging for SWG, to provide a response web page for the Response Analytics item, and to provide categories for the URL Filter Assign item.*

   a) Click the **(+)** icon anywhere in the per-request policy to add a new item.
      A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
   b) Type `cat` in the Search field, select **Category Lookup**, and click **Add Item**.
      A Properties popup screen opens.
   c) From the **Categorization Input** list, select how to obtain the requested URL. For HTTP traffic, select **Use HTTP URI (cannot be used for SSL Bypass decisions)**. For SSL-encrypted traffic, select either **Use SNI in Client Hello (if SNI is not available, use Subject.CN)** or **Use Subject.CN in Server Cert**.
      If you select **Use HTTP URI (cannot be used for SSL Bypass decisions)**, the **SafeSearch Mode** list displays and **Enabled** is selected.
   d) From the **Category Lookup Type** list, select the category types in which to search for the requested URL. Select one from **Custom categories first, then standard categories if not found**, **Always process full list of both custom and standard categories**, or **Process standard categories only**.

Depending on your selection, the Category Lookup Type item looks through custom categories or standard categories or both, and compiles a list of one or more categories from them. The list is available for subsequent processing by the URL Filter Assign item.

e) Click **Save**.
The Properties screen closes. The visual policy editor displays.

8. To enable Safe Search for SSL-encrypted traffic, add an additional Category Lookup item, specify **Use HTTP URI (cannot be used for SSL Bypass decisions)** as the **Category Lookup Type**, and retain the default setting (**Enabled**) for **SafeSearch Mode**.
9. At any point in the policy where a decision to bypass SSL traffic is made, add an **SSL Bypass Set** item.
10. Add any of these items to the policy.

Item	Description
Dynamic Date Time	Branch by day of week or time of day.
AD Group Lookup	Branch by user group. Requires branch rule configuration.
LDAP Group Lookup	Branch by user group. Requires branch rule configuration.
LocalDB Group Lookup	Branch by user group. Requires branch rule configuration.
RADIUS Class Lookup	Branch by the class attribute. Requires branch rule configuration.

11. To configure a branch rule for a LocalDB Group Lookup item:
    a) In the visual policy editor, click the name of the item.
    A Properties popup screen opens.
    b) Click the Branch Rules tab.
    c) To edit an expression, click the **change** link.
    An additional popup screen opens, displaying the Simple tab.
    d) If the Local Database action in the access policy was configured to read groups into the `session.localdb.groups` session variable, edit the default simple expression, **User is a member of** `MY_GROUP`, replacing MY_GROUP with a relevant group.
    e) If the Local Database action in the access policy was configured to read groups into a session variable other than `session.localdb.groups`, click the Advanced tab; edit the default advanced expression, `expression is expr { [mcget {session.localdb.groups}] contains "MY_GROUP" }`, replacing MY_GROUP with a relevant group and `session.localdb.groups` with the session variable specified in the Local Database action.
    f) Click **Finished**.
    The popup screen closes.
    g) Click **Save**.
    The popup screen closes. The visual policy editor displays.
12. To configure a branch rule for AD, LDAP, or RADIUS group or class lookups:
    a) In the visual policy editor, click the name of the policy item.
    A Properties popup screen opens.
    b) Click the Branch Rules tab.
    c) To edit an expression, click the **change** link.
    An additional popup screen opens, displaying the Simple tab.
    d) Edit the default simple expression to specify group or class that is used in your environment.

In an LDAP Group Lookup item, the default simple expression is **User is a member of** `CN=MY_GROUP, CN=USERS, CN=MY_DOMAIN`. You can use the simple expression editor to replace the default values.

e) Click **Finished**.
The popup screen closes.

f) Click **Save**.
The popup screen closes. The visual policy editor displays.

13. To trigger inspection of the response web page contents, add a Response Analytics item.

A Category Lookup item must precede this item.

a) In the **Max Buffer Size** field, type the number of bytes to buffer.

b) In the **Max Buffer time** field, type the number of seconds to retain response data in the buffer.

c) For the **Reset on Failure** field, retain the default value **Enabled** to send a TCP reset if the server fails.

d) For each type of content that you want to exclude from analysis, click **Add new entry** and then select a type from the list.

The **All-Images** type is on the list by default because images are not scanned.

e) Click **Finished**.
The popup screen closes.

f) Click **Save**.

The fallback branch after this item indicates that a failure occurred during content analysis. The Success branch indicates that content analysis completed.

The popup screen closes. The visual policy editor displays.

14. Add a URL Filter Assign item after the Response Analytics item, if included on the branch; otherwise, add it anywhere on a branch after a Category Lookup item.

In this item, you must specify a URL filter to apply to the URL categories that the Category Lookup item returned. If any URL category specifies the Block filtering action, this item blocks the request. This item also blocks the request if the Response Analytics item identified malicious content.

To put the per-request policy into effect, add it to the virtual server.

Creating an access profile for SWG explicit forward proxy

You create an access profile to specify any access policy configuration for a virtual server that serves in a Secure Web Gateway (SWG) explicit forward proxy configuration.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
The Access Profiles List screen opens.

2. Click **Create**.
The New Profile screen opens.

3. In the **Name** field, type a name for the access profile.

Note: *An access profile name must be unique among all access profile and per-request policy names.*

4. From the **Profile Type** list, select **SWG-Explicit**.
Additional fields display set to default values.

5. In the Language Settings area, add and remove accepted languages, and set the default language.

A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.

6. Click **Finished**.
   The Access Profiles list screen displays.
7. To enable Secure Web Gateway event logging for this access profile, add log settings.
   a) Click the name of the access profile that you just created.
      The Properties screen displays.
   b) On the menu bar, click **Logs**.
      The General Properties screen displays.
   c) In the Log Settings area, move log settings from the **Available** list to the **Selected** list.

   You can configure log settings in the Access Policy Event Logs area of the product.

This creates an access profile with a default access policy that contains a **Start** and a **Deny** ending.

You do not need to add any actions or make any changes to the access policy.

Creating a virtual server for network access client forward proxy server

Before you begin, you need to know the name of the connectivity profile specified in the virtual server for the network access configuration that you want to protect using Secure Web Gateway (SWG).

You specify a virtual server to process forward proxy traffic with Secure Web Gateway (SWG). This virtual server must listen on the secure connectivity interface that is specified on the virtual server through which network access clients connect. This virtual server is also the one that network access resources must specify as the client proxy server.

Note: *Use this virtual server for forward proxy traffic only. You should not try to use it for reverse proxy, or add a pool to it.*

---

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type the IP address for a host virtual server.

   This field accepts an address in CIDR format (IP address/prefix). However, when you type the complete IP address for a host, you do not need to type a prefix after the address.

   Type a destination address in this format: `162.160.15.20`.
5. In the **Service Port** field, type the port number to use for forward proxy traffic.

   Typically, the port number is `3128` or `8080`.
6. From the **HTTP Profile** list, select the HTTP profile you configured earlier.
7. Scroll down to the **VLAN and Tunnel Traffic** setting and select **Enabled on**.
8. For the **VLANs and Tunnels** setting, move the secure connectivity interface to the **Selected** list.
9. From the **Source Address Translation** list, select **Auto Map**.
10. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
11. In the Access Policy area, from the **Per-Request Policy** list, select the policy that you configured earlier.
12. Click **Finished**.

Creating a wildcard virtual server for HTTP tunnel traffic

You configure a virtual server to process web traffic coming in on the HTTP tunnel from the explicit forward-proxy virtual server.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
5. In the **Service Port** field, type `80`, or select **HTTP** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.
8. Scroll down to the **VLAN and Tunnel Traffic** setting and select **Enabled on**.
9. For the **VLANs and Tunnels** setting, move the tunnel to the **Selected** list.

   The tunnel name must match the tunnel specified in the HTTP profile for the forward proxy virtual server. The default tunnel is **http-tunnel**.
10. From the **Source Address Translation** list, select **Auto Map**.
11. Scroll down to the **Port Translation** setting and clear the **Enabled** check box.
12. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
13. In the Access Policy area, from the **Per-Request Policy** list, select the policy that you configured earlier.
14. Click **Finished**.

Creating a custom Client SSL forward proxy profile

Creating a Client SSL forward proxy profile makes it possible for client and server authentication, while still allowing the BIG-IP® system to perform data optimization, such as decryption and encryption. This profile applies to client-side SSL forward proxy traffic only.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.
   The Client profile list screen opens.
2. Click **Create**.
   The New Client SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. From the **Parent Profile** list, select **clientssl**.
5. To avoid issues with privacy concerns, you might need to enable SSL forward proxy bypass for URLs that expose personal user information, such as those for financial or government sites.
   a) Scroll down to the **SSL Forward Proxy** list, and select **Advanced**.
   b) Select the **Custom** check box for the SSL Forward Proxy area.
   c) From the **SSL Forward Proxy** list, select **Enabled**.

      You can update this setting later but only while the profile is not assigned to a virtual server.
   d) From the **CA Certificate** list, select a certificate.
   e) From the **CA Key** list, select a key.
   f) In the **CA Passphrase** field, type a passphrase.

g) In the **Confirm CA Passphrase** field, type the passphrase again.
h) In the **Certificate Lifespan** field, type a lifespan for the SSL forward proxy certificate in days.
i) (Optional) From the **Certificate Extensions** list, select **Extensions List**.
j) (Optional) For the **Certificate Extensions List** setting, select the extensions that you want in the **Available extensions** field, and move them to the **Enabled Extensions** field using the **Enable** button.
k) From the **SSL Forward Proxy Bypass** list, select **Enabled**.
   You can update this setting later but only while the profile is not assigned to a virtual server.
   Additional settings display.
l) For **Default Bypass Action**, retain the default value **Intercept**.
   You can override the value of this action on a case-by-case basis in the per-request policy for the virtual server.

Note: *Bypass and intercept lists do not work with per-request policies. Retain the setting* ***None*** *for the remainder of the fields.*

6. Click **Finished**.

The custom Client SSL forward proxy profile now appears in the Client SSL profile list screen.

Creating a custom Server SSL profile

Create a custom server SSL profile to support SSL forward proxy.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Server**.
   The SSL Server profile list screen opens.
2. Click **Create**.
   The New Server SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. For **Parent Profile**, retain the default selection, **serverssl**.
5. From the **Configuration** list, select **Advanced**.
6. Select the **Custom** check box.
   The settings become available for change.
7. From the **SSL Forward Proxy** list, select **Enabled**.
   You can update this setting later, but only while the profile is not assigned to a virtual server.
8. From the **SSL Forward Proxy Bypass** list, select **Enabled** (or retain the default value **Disabled**).
   The values of the **SSL Forward Proxy Bypass** settings in the server SSL and the client SSL profiles specified in a virtual server must match. You can update this setting later but only while the profile is not assigned to a virtual server.
9. Scroll down to the **Secure Renegotiation** list and select **Request**.
10. Click **Finished**.

The custom Server SSL profile is now listed in the SSL Server profile list.

Creating a wildcard virtual server for SSL traffic on the HTTP tunnel

If you do not have existing client SSL and server SSL profiles that you want to use, configure them before you start.

You configure a virtual server to process SSL web traffic coming in on the HTTP tunnel from the forward proxy virtual server.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.
8. For the **SSL Profile (Client)** setting, from the **Available** list, select the name of the Client SSL forward proxy profile you previously created, and using the Move button, move the name to the **Selected** list.

   Important: *To enable SSL forward proxy functionality, you can either:*

   - Disassociate existing Client SSL and Server SSL profiles from a virtual server and configure the SSL Forward Proxy settings.
   - Create new Client SSL and Server SSL profiles and configure the SSL Forward Proxy settings.

   Then with either option, select the Client SSL and Server SSL profiles on a virtual server. You cannot modify existing Client SSL and Server SSL profiles while they are selected on a virtual server to enable SSL forward proxy functionality.

9. For the **SSL Profile (Server)** setting, from the **Available** list, select the name of the Server SSL forward proxy profile you previously created, and using the Move button, move the name to the **Selected** list.

   Important: *To enable SSL forward proxy functionality, you can either:*

   - Disassociate existing Client SSL and Server SSL profiles from a virtual server and configure the SSL Forward Proxy settings.
   - Create new Client SSL and Server SSL profiles and configure the SSL Forward Proxy settings.

   Then with either option, select the Client SSL and Server SSL profiles on a virtual server. You cannot modify existing Client SSL and Server SSL profiles while they are selected on a virtual server to enable SSL forward proxy functionality.

10. Scroll down to the **VLAN and Tunnel Traffic** setting and select **Enabled on**.
11. For the **VLANs and Tunnels** setting, move the tunnel to the **Selected** list.

    The tunnel name must match the tunnel specified in the HTTP profile for the forward proxy virtual server. The default tunnel is **http-tunnel**.
12. From the **Source Address Translation** list, select **Auto Map**.
13. Scroll down to the **Port Translation** setting and clear the **Enabled** check box.
14. For the **Address Translation** setting, clear the **Enabled** check box.
15. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
16. In the Access Policy area, from the **Per-Request Policy** list, select the policy that you configured earlier.
17. Click **Finished**.

Updating the access policy in the remote access configuration

Add an SWG Scheme Assign item to an access policy to assign a Secure Web Gateway (SWG) scheme to a client session. Add queries to populate any session variables that are required for successful execution of the per-request policy.

Note: *Class lookup or group lookup items in a per-request policy rely on session variables that are populated in this access policy.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile that you want to edit. The properties screen opens.
3. Click **Edit Access Policy for Profile** ***profile_name***.
   The visual policy editor opens the access policy in a separate screen.
4. Click the **(+)** icon anywhere in the access policy to add a new action item.

   Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
5. On the Assignment tab, select **SWG Scheme Assign** and click **Add Item**.
   A properties screen opens.
6. To display the available schemes, click the **Add/Delete** link.
7. Select one scheme and click **Save**.
   The Properties screen closes and the visual policy editor screen displays.
8. To supply LDAP group information for use in the per-request policy, add an LDAP Query item anywhere in the access policy and configure its properties:
   a) From the **Server** list, select an AAA LDAP server.

      An LDAP Query uses SSL connections when you select an LDAP AAA server that is configured for LDAPS.

   b) Specify the **SearchDN**, and **SearchFilter** settings.

      SearchDN is the base DN from which the search is done.

   c) Click **Save**.

   This item populates the `session.ldap.last.attr.memberOf` session variable.
9. To supply Active Directory groups for use in the per-request policy, add an AD Query item anywhere in the access policy and configure its properties:
   a) From the **Server** list, select an AAA AD server.
   b) Select the **Fetch Primary Group** check box.

      The value of the primary user group populates the `session.ad.last.attr.primaryGroupID` session variable.

   c) Click **Save**.
10. To supply RADIUS class attributes for use in the per-request policy, add a RADIUS Auth item anywhere in the access policy and configure its properties:
    a) From the **Server** list, select an AAA RADIUS server.
    b) Click **Save**.

This item populates the `session.radius.last.attr.class` session variable.

11. To supply local database groups for use in the per-request policy, add a Local Database item anywhere in the access policy and configure its properties:
    a) From the **LocalDB Instance** list, select a local user database.
    b) In the **User Name** field, retain the default session variable.
    c) Click **Add new entry**
    A new line is added to the list of entries with the Action set to **Read** and other default settings.
    d) In the Destination column **Session Variable** field, type `session.localdb.groups`.
    If you type a name other than `session.localdb.groups`, note it. You will need it when you configure the per-request access policy.
    e) In the Source column from the **DB Property** list, select **groups**.
    f) Click **Save**.

    This item populates the `session.localdb.groups` session variable.

The access policy is configured to assign an SWG scheme and to support the per-request policy.

Click the **Apply Access Policy** link to apply and activate your changes to this access policy.

Configuring a network access resource to forward traffic

You must create a network access resource, or open an existing resource, before you can perform this task.

Configure a network access resource to forward traffic to the Secure Web Gateway (SWG) explicit forward proxy virtual server so that SWG can filter Internet traffic and analyze content, protecting the client from malware.

1. On the Main tab, click **Access Policy** > **Network Access** > **Network Access List**.
   The Network Access List screen opens.
2. In the Name column, click the name of the network access resource you want to edit.
3. On the menu bar, click **Network Settings**.
4. For **Client Settings**, select **Advanced**.
5. Scroll down and select **Client Proxy Settings**.
   Additional settings display.
6. If the **Traffic Options** setting specifies **Force all traffic through tunnel**, configure these additional settings:
   a) In the **Client Proxy Address** field, type the IP address of the SWG explicit forward proxy virtual server.
   b) In the **Client Proxy Port** field, type the port number of the SWG explicit forward proxy virtual server.
   Typically, the port number is `3128` or `8080`; it might be different in your configuration.
7. If the **Traffic Options** setting specifies **Use split tunneling for traffic**, in the **Client Proxy Autoconfig Script** field, type the URL for a proxy auto-configuration script.
8. Click the **Update** button.
   Your changes are saved and the page refreshes.

The network access resource forwards traffic to the SWG explicit forward proxy server.

Implementation result

The Secure Web Gateway (SWG) explicit forward proxy configuration is ready to process web traffic from network access clients.

Session variables for use in a per-request policy

Per-request policy items that look up the group or class to which a user belongs rely on the access policy to populate these session variables.

Per-request policy item	Session variable	Access policy item
AD Group Lookup	`session.ad.last.attr.primaryGroupID`	AD Query
LDAP Group Lookup	`session.ldap.last.attr.memberOf`	LDAP Query
LocalDB Group Lookup	`session.localdb.groups` ***Note:*** *This session variable is a default in the expression for LocalDB Group Lookup; any session variable in the expression must match the session variable used in the Local Database action in the access policy.*	Local Database
RADIUS Class Lookup	`session.radius.last.attr.class`	RADIUS Auth

Overview: Configuring SWG transparent forward proxy for remote access

Secure Web Gateway (SWG) can be configured to support remote clients that connect using application access, network access, or portal access.

Note: *Using a distinct SWG transparent forward proxy configuration to process traffic from remote clients separately from an SWG configuration used for processing traffic from internal clients provides an important measure of network security.*

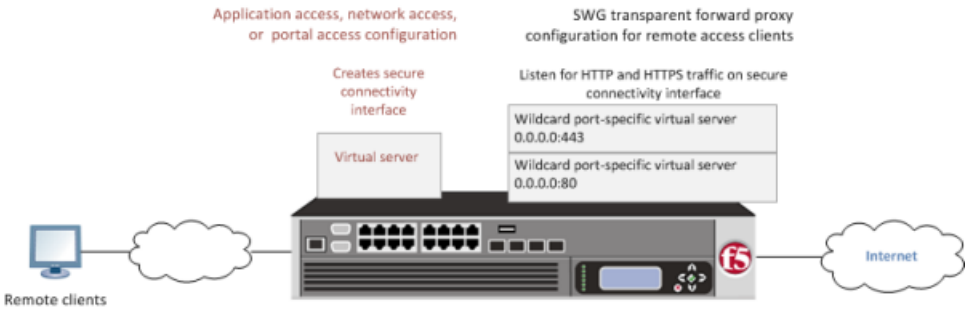

Figure 12: SWG transparent forward proxy for remote access

You should understand how these configuration objects fit into the overall configuration.

Secure connectivity interface

In a remote access configuration, a connectivity profile is required on the virtual server to specify a secure connectivity interface for traffic from the client. In the SWG configuration, SWG wildcard virtual servers must listen on the secure connectivity interface for traffic from remote access clients.

Per-request policy

In any SWG configuration, the determination of whether a user can access a URL must be made in a per-request access policy. A per-request access policy determines whether to block or allow access to a request based on time or date or group membership or other criteria that you configure.

Access policies

The access policy in the remote access configuration continues to authenticate users, assign resources, and evaluate ACLs, if any. In addition, this access policy must assign an SWG scheme for the network access session and populate any session variables used in the per-request policy. An access profile of the SWG-Transparent type is required in the SWG configuration; however, it is not necessary to include any items in the access policy.

Task summary

Creating a connectivity profile
Adding a connectivity profile to a virtual server
Configuring a per-request policy for SWG
Creating an access profile for SWG transparent forward proxy
Creating a wildcard virtual server for HTTP traffic on the connectivity interface
Creating a custom Client SSL forward proxy profile
Creating a custom Server SSL profile
Creating a wildcard virtual server for SSL traffic on the connectivity interface
Updating the access policy in the remote access configuration

Prerequisites

Before you start to create a Secure Web Gateway (SWG) transparent forward proxy configuration to support remote access clients, you must have completed these tasks.

- You need to have configured a working application access, network access, or portal access configuration, depending on which type of remote client you want to support.
- If you have not already done so, you must ensure that the URL database is downloaded.
- You need to have configured at least one SWG scheme and any URL filters that you want to use in addition to or instead of the default URL filters.

Configuration outline

Tasks for integrating an Access Policy Manager® (APM®) remote access configuration with a Secure Web Gateway (SWG) transparent forward proxy configuration follow this order.

- First, update the existing application access, network access, or portal access configuration to add a secure connectivity profile to the virtual server if one is not already specified.
- Next, create an SWG transparent forward proxy configuration. The per-request policy is part of this configuration.
- Finally, update the access policy in the existing application access, network access, or portal access configuration. An SWG scheme assignment is required in this access policy. If the per-request policy uses group or class lookup items, add queries to populate the session variables on which the lookup items rely.

Creating a connectivity profile

You create a connectivity profile to configure client connections.

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Click **Add**.
   The Create New Connectivity Profile popup screen opens and displays General Settings.
3. Type a **Profile Name** for the connectivity profile.
4. Select a **Parent Profile** from the list.
   APM® provides a default profile, **connectivity**.
5. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.

The connectivity profile appears in the list.

To provide functionality with a connectivity profile, you must add the connectivity profile to a virtual server.

Adding a connectivity profile to a virtual server

Update a virtual server that is part of an Access Policy Manager® application access, network access, or portal access configuration to enable a secure connectivity interface for traffic from the client.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. Scroll down to the Access Policy area.
4. From the **Connectivity Profile** list, select the connectivity profile.
5. Click **Update** to save the changes.

Configuring a per-request policy for SWG

Configure a per-request policy to specify the logic that determines how to process web traffic.

Note: *A per-request policy must determine whether to bypass SSL traffic and, otherwise, whether to allow or reject a URL request in a Secure Web Gateway (SWG) forward proxy configuration.*

---

1. On the Main tab, click **Access Policy** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. Click **Create**.
   The General Properties screen displays.
3. In the **Name** field, type a name for the policy and click **Finished**.
   A per-request policy name must be unique among all per-request policy and access profile names.
   The policy name appears on the Per-Request Policies screen.
4. In the Access Policy column for the per-request policy that you want to update, click the **Edit** link.
   The visual policy editor opens in another tab.
5. To create different branches for processing HTTP and HTTPS traffic, add a **Protocol Lookup** item.

a) Click the **(+)** icon anywhere in the per-request policy to add a new item.
A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
b) Type `prot` in the Search field, select **Protocol Lookup**, and click **Add Item**.
A Properties popup screen opens.
c) Click **Save**.
The Properties screen closes. The visual policy editor displays.

6. If you configured SSL forward proxy bypass in the client and server SSL profiles, include an **SSL Intercept Set** item to ensure that SSL traffic is not bypassed until this policy determines that it should be.

It is important to include SSL Intercept Set when the default SSL bypass action in the client SSL profile is set to Bypass.

7. To retrieve the requested URL and the categories to which it belongs, add a **Category Lookup** item.

Important: *A Category Lookup item is required to trigger event logging for SWG, to provide a response web page for the Response Analytics item, and to provide categories for the URL Filter Assign item.*

---

a) Click the **(+)** icon anywhere in the per-request policy to add a new item.
A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
b) Type `cat` in the Search field, select **Category Lookup**, and click **Add Item**.
A Properties popup screen opens.
c) From the **Categorization Input** list, select how to obtain the requested URL. For HTTP traffic, select **Use HTTP URI (cannot be used for SSL Bypass decisions)**. For SSL-encrypted traffic, select either **Use SNI in Client Hello (if SNI is not available, use Subject.CN)** or **Use Subject.CN in Server Cert**.
If you select **Use HTTP URI (cannot be used for SSL Bypass decisions)**, the **SafeSearch Mode** list displays and **Enabled** is selected.
d) From the **Category Lookup Type** list, select the category types in which to search for the requested URL. Select one from **Custom categories first, then standard categories if not found**, **Always process full list of both custom and standard categories**, or **Process standard categories only**.
Depending on your selection, the Category Lookup Type item looks through custom categories or standard categories or both, and compiles a list of one or more categories from them. The list is available for subsequent processing by the URL Filter Assign item.
e) Click **Save**.
The Properties screen closes. The visual policy editor displays.

8. To enable Safe Search for SSL-encrypted traffic, add an additional Category Lookup item, specify **Use HTTP URI (cannot be used for SSL Bypass decisions)** as the **Category Lookup Type**, and retain the default setting (**Enabled**) for **SafeSearch Mode**.

9. At any point in the policy where a decision to bypass SSL traffic is made, add an **SSL Bypass Set** item.

10. Add any of these items to the policy.

Item	Description
Dynamic Date Time	Branch by day of week or time of day.
AD Group Lookup	Branch by user group. Requires branch rule configuration.
LDAP Group Lookup	Branch by user group. Requires branch rule configuration.

Item	Description
LocalDB Group Lookup	Branch by user group. Requires branch rule configuration.
RADIUS Class Lookup	Branch by the class attribute. Requires branch rule configuration.

11. To configure a branch rule for a LocalDB Group Lookup item:

a) In the visual policy editor, click the name of the item.
A Properties popup screen opens.
b) Click the Branch Rules tab.
c) To edit an expression, click the **change** link.
An additional popup screen opens, displaying the Simple tab.
d) If the Local Database action in the access policy was configured to read groups into the `session.localdb.groups` session variable, edit the default simple expression, **User is a member of** `MY_GROUP`, replacing MY_GROUP with a relevant group.
e) If the Local Database action in the access policy was configured to read groups into a session variable other than `session.localdb.groups`, click the Advanced tab; edit the default advanced expression, `expression is expr { [mcget {session.localdb.groups}] contains "`*`MY_GROUP`*`" }`, replacing MY_GROUP with a relevant group and `session.localdb.groups` with the session variable specified in the Local Database action.
f) Click **Finished**.
The popup screen closes.
g) Click **Save**.
The popup screen closes. The visual policy editor displays.

12. To configure a branch rule for AD, LDAP, or RADIUS group or class lookups:

a) In the visual policy editor, click the name of the policy item.
A Properties popup screen opens.
b) Click the Branch Rules tab.
c) To edit an expression, click the **change** link.
An additional popup screen opens, displaying the Simple tab.
d) Edit the default simple expression to specify group or class that is used in your environment.
In an LDAP Group Lookup item, the default simple expression is **User is a member of** `CN=MY_GROUP, CN=USERS, CN=MY_DOMAIN`. You can use the simple expression editor to replace the default values.
e) Click **Finished**.
The popup screen closes.
f) Click **Save**.
The popup screen closes. The visual policy editor displays.

13. To trigger inspection of the response web page contents, add a Response Analytics item.

A Category Lookup item must precede this item.

a) In the **Max Buffer Size** field, type the number of bytes to buffer.
b) In the **Max Buffer time** field, type the number of seconds to retain response data in the buffer.
c) For the **Reset on Failure** field, retain the default value **Enabled** to send a TCP reset if the server fails.
d) For each type of content that you want to exclude from analysis, click **Add new entry** and then select a type from the list.

The **All-Images** type is on the list by default because images are not scanned.

e) Click **Finished**.

The popup screen closes.

f) Click **Save**.

The fallback branch after this item indicates that a failure occurred during content analysis. The Success branch indicates that content analysis completed.

The popup screen closes. The visual policy editor displays.

14. Add a URL Filter Assign item after the Response Analytics item, if included on the branch; otherwise, add it anywhere on a branch after a Category Lookup item.

In this item, you must specify a URL filter to apply to the URL categories that the Category Lookup item returned. If any URL category specifies the Block filtering action, this item blocks the request. This item also blocks the request if the Response Analytics item identified malicious content.

To put the per-request policy into effect, add it to the virtual server.

Creating an access profile for SWG transparent forward proxy

You create an access profile to supply an access policy.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
The Access Profiles List screen opens.

2. Click **Create**.
The New Profile screen opens.

3. In the **Name** field, type a name for the access profile.

Note: *An access profile name must be unique among all access profile and per-request policy names.*

---

4. From the **Profile Type** list, select **SWG-Transparent**.
Additional fields display set to default values.

5. In the Language Settings area, add and remove accepted languages, and set the default language.

A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.

6. Click **Finished**.
The Access Profiles list screen displays.

7. To enable Secure Web Gateway event logging for this access profile, add log settings.

a) Click the name of the access profile that you just created.
The Properties screen displays.

b) On the menu bar, click **Logs**.
The General Properties screen displays.

c) In the Log Settings area, move log settings from the **Available** list to the **Selected** list.

You can configure log settings in the Access Policy Event Logs area of the product.

This creates an access profile with a default access policy that contains a **Start** and a **Deny** ending.

You do not need to add any actions or make any changes to the access policy.

Creating a wildcard virtual server for HTTP traffic on the connectivity interface

Before you begin, you need to know the name of the connectivity profile specified in the virtual server for the remote access configuration that you want Secure Web Gateway (SWG) to protect.

You configure a virtual server to process web traffic on the secure connectivity interface for a remote access client.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
5. In the **Service Port** field, type `80`, or select **HTTP** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.
8. Scroll down to the **VLAN and Tunnel Traffic** setting and select **Enabled on**.
9. For the **VLANs and Tunnels** setting, move the secure connectivity interface to the **Selected** list.
10. From the **Source Address Translation** list, select **Auto Map**.
11. Scroll down to the **Port Translation** setting and clear the **Enabled** check box.
12. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
13. In the Access Policy area, from the **Per-Request Policy** list, select the policy that you configured earlier.
14. Click **Finished**.

Creating a custom Client SSL forward proxy profile

Creating a Client SSL forward proxy profile makes it possible for client and server authentication, while still allowing the BIG-IP® system to perform data optimization, such as decryption and encryption. This profile applies to client-side SSL forward proxy traffic only.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.
   The Client profile list screen opens.
2. Click **Create**.
   The New Client SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. From the **Parent Profile** list, select **clientssl**.
5. To avoid issues with privacy concerns, you might need to enable SSL forward proxy bypass for URLs that expose personal user information, such as those for financial or government sites.
   a) Scroll down to the **SSL Forward Proxy** list, and select **Advanced**.
   b) Select the **Custom** check box for the SSL Forward Proxy area.
   c) From the **SSL Forward Proxy** list, select **Enabled**.
      You can update this setting later but only while the profile is not assigned to a virtual server.
   d) From the **CA Certificate** list, select a certificate.
   e) From the **CA Key** list, select a key.
   f) In the **CA Passphrase** field, type a passphrase.

g) In the **Confirm CA Passphrase** field, type the passphrase again.
h) In the **Certificate Lifespan** field, type a lifespan for the SSL forward proxy certificate in days.
i) (Optional) From the **Certificate Extensions** list, select **Extensions List**.
j) (Optional) For the **Certificate Extensions List** setting, select the extensions that you want in the **Available extensions** field, and move them to the **Enabled Extensions** field using the **Enable** button.
k) From the **SSL Forward Proxy Bypass** list, select **Enabled**.

   You can update this setting later but only while the profile is not assigned to a virtual server.

   Additional settings display.
l) For **Default Bypass Action**, retain the default value **Intercept**.

   You can override the value of this action on a case-by-case basis in the per-request policy for the virtual server.

Note: *Bypass and intercept lists do not work with per-request policies. Retain the setting* ***None*** *for the remainder of the fields.*

---

6. Click **Finished**.

The custom Client SSL forward proxy profile now appears in the Client SSL profile list screen.

Creating a custom Server SSL profile

Create a custom server SSL profile to support SSL forward proxy.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Server**.
   The SSL Server profile list screen opens.
2. Click **Create**.
   The New Server SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. For **Parent Profile**, retain the default selection, **serverssl**.
5. From the **Configuration** list, select **Advanced**.
6. Select the **Custom** check box.
   The settings become available for change.
7. From the **SSL Forward Proxy** list, select **Enabled**.

   You can update this setting later, but only while the profile is not assigned to a virtual server.
8. From the **SSL Forward Proxy Bypass** list, select **Enabled** (or retain the default value **Disabled**).

   The values of the **SSL Forward Proxy Bypass** settings in the server SSL and the client SSL profiles specified in a virtual server must match. You can update this setting later but only while the profile is not assigned to a virtual server.
9. Scroll down to the **Secure Renegotiation** list and select **Request**.
10. Click **Finished**.

The custom Server SSL profile is now listed in the SSL Server profile list.

Creating a wildcard virtual server for SSL traffic on the connectivity interface

Before you begin, you need to know the name of the connectivity profile specified in the virtual server for the remote access configuration that you want Secure Web Gateway (SWG) to protect. Also, if you do not have existing client SSL and server SSL profiles that you want to use, configure them before you start.

You configure a virtual server to process SSL web traffic coming in on the secure connectivity interface for a remote access client.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.
8. For the **SSL Profile (Client)** setting, from the **Available** list, select the name of the Client SSL forward proxy profile you previously created, and using the Move button, move the name to the **Selected** list.

   Important: *To enable SSL forward proxy functionality, you can either:*

   - Disassociate existing Client SSL and Server SSL profiles from a virtual server and configure the SSL Forward Proxy settings.
   - Create new Client SSL and Server SSL profiles and configure the SSL Forward Proxy settings.

   Then with either option, select the Client SSL and Server SSL profiles on a virtual server. You cannot modify existing Client SSL and Server SSL profiles while they are selected on a virtual server to enable SSL forward proxy functionality.

9. For the **SSL Profile (Server)** setting, from the **Available** list, select the name of the Server SSL forward proxy profile you previously created, and using the Move button, move the name to the **Selected** list.

   Important: *To enable SSL forward proxy functionality, you can either:*

   - Disassociate existing Client SSL and Server SSL profiles from a virtual server and configure the SSL Forward Proxy settings.
   - Create new Client SSL and Server SSL profiles and configure the SSL Forward Proxy settings.

   Then with either option, select the Client SSL and Server SSL profiles on a virtual server. You cannot modify existing Client SSL and Server SSL profiles while they are selected on a virtual server to enable SSL forward proxy functionality.

10. Scroll down to the **VLAN and Tunnel Traffic** setting and select **Enabled on**.
11. For the **VLANs and Tunnels** setting, move the secure connectivity interface to the **Selected** list.
12. From the **Source Address Translation** list, select **Auto Map**.
13. Scroll down to the **Port Translation** setting and clear the **Enabled** check box.
14. For the **Address Translation** setting, clear the **Enabled** check box.
15. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
16. In the Access Policy area, from the **Per-Request Policy** list, select the policy that you configured earlier.
17. Click **Finished**.

Updating the access policy in the remote access configuration

Add an SWG Scheme Assign item to an access policy to assign a Secure Web Gateway (SWG) scheme to a client session. Add queries to populate any session variables that are required for successful execution of the per-request policy.

Note: *Class lookup or group lookup items in a per-request policy rely on session variables that are populated in this access policy.*

---

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile that you want to edit. The properties screen opens.
3. Click **Edit Access Policy for Profile** ***profile_name***.
   The visual policy editor opens the access policy in a separate screen.
4. Click the **(+)** icon anywhere in the access policy to add a new action item.

   Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
5. On the Assignment tab, select **SWG Scheme Assign** and click **Add Item**.
   A properties screen opens.
6. To display the available schemes, click the **Add/Delete** link.
7. Select one scheme and click **Save**.
   The Properties screen closes and the visual policy editor screen displays.
8. To supply LDAP group information for use in the per-request policy, add an LDAP Query item anywhere in the access policy and configure its properties:
   a) From the **Server** list, select an AAA LDAP server.

      An LDAP Query uses SSL connections when you select an LDAP AAA server that is configured for LDAPS.

   b) Specify the **SearchDN**, and **SearchFilter** settings.

      SearchDN is the base DN from which the search is done.

   c) Click **Save**.

   This item populates the `session.ldap.last.attr.memberOf` session variable.
9. To supply Active Directory groups for use in the per-request policy, add an AD Query item anywhere in the access policy and configure its properties:
   a) From the **Server** list, select an AAA AD server.
   b) Select the **Fetch Primary Group** check box.

      The value of the primary user group populates the `session.ad.last.attr.primaryGroupID` session variable.

   c) Click **Save**.
10. To supply RADIUS class attributes for use in the per-request policy, add a RADIUS Auth item anywhere in the access policy and configure its properties:
    a) From the **Server** list, select an AAA RADIUS server.
    b) Click **Save**.

This item populates the `session.radius.last.attr.class` session variable.

11. To supply local database groups for use in the per-request policy, add a Local Database item anywhere in the access policy and configure its properties:
    a) From the **LocalDB Instance** list, select a local user database.
    b) In the **User Name** field, retain the default session variable.
    c) Click **Add new entry**
    A new line is added to the list of entries with the Action set to **Read** and other default settings.
    d) In the Destination column **Session Variable** field, type `session.localdb.groups`.
    If you type a name other than `session.localdb.groups`, note it. You will need it when you configure the per-request access policy.
    e) In the Source column from the **DB Property** list, select **groups**.
    f) Click **Save**.

    This item populates the `session.localdb.groups` session variable.

The access policy is configured to assign an SWG scheme and to support the per-request policy.

Click the **Apply Access Policy** link to apply and activate your changes to this access policy.

Implementation result

The Secure Web Gateway (SWG) transparent proxy configuration is ready to process web traffic from remote access clients.

Session variables for use in a per-request policy

Per-request policy items that look up the group or class to which a user belongs rely on the access policy to populate these session variables.

Per-request policy item	Session variable	Access policy item
AD Group Lookup	`session.ad.last.attr.primaryGroupID`	AD Query
LDAP Group Lookup	`session.ldap.last.attr.memberOf`	LDAP Query
LocalDB Group Lookup	`session.localdb.groups` ***Note:*** *This session variable is a default in the expression for LocalDB Group Lookup; any session variable in the expression must match the session variable used in the Local Database action in the access policy.*	Local Database
RADIUS Class Lookup	`session.radius.last.attr.class`	RADIUS Auth

Chapter 8

Reports, Logs, and Statistics

- *About SWG data for threat monitoring*
- *About per-request policies and SWG logging and reports*
- *About Access Policy Manager and Secure Web Gateway logs*
- *About local and remote logging for Secure Web Gateway*
- *Flowchart for local logging configuration*
- *Overview: Monitoring Internet traffic and making adjustments to SWG*
- *Overview: Configuring remote high-speed SWG event logging*

About SWG data for threat monitoring

After Secure Web Gateway (SWG) starts proxying web access, it provides information that you can use to monitor threats and to fine-tune URL filters and schemes. SWG provides reports, statistics, and logs. If you configure high-speed remote event logging, you have data on a remote system from which you can create your own reports.

About per-request policies and SWG logging and reports

Unless a per-request policy includes and executes a Category Lookup item, Secure Web Gateway (SWG) event logging does not occur and there is no data for reports.

About Access Policy Manager and Secure Web Gateway logs

Secure Web Gateway (SWG) supports high-speed logging and can store event logs in a local database or on a pool of remote servers (recommended). SWG event logging occurs separately from Access Policy Manager® (APM®) logging and from BIG-IP® system logging as well.

Logs for the access policies that are part of an SWG configuration depend on APM report preference settings. Access policy logs might be in the `/var/log/apm` file or in a local database that APM reports uses.

About local and remote logging for Secure Web Gateway

You can log Secure Web Gateway (SWG) events either locally on the BIG-IP® system or remotely, using the BIG-IP system's high-speed logging mechanism. For remote logging, the high-speed logging mechanism sends log messages to a pool of logging servers that you define. Remote logging is the recommended configuration.

Note: *When you configure remote logging, logs are not available for display in the Configuration utility.*

For local logging, the high-speed logging mechanism stores the logs in either the Syslog or the MySQL database on the BIG-IP system, depending on a destination that you specify. The available local destinations are:

local-db
Causes the system to store log messages in the local MySQL database. When you choose **local-db**, you can view log messages in the Configuration utility.

local-syslog
Causes the system to store log messages in the local Syslog database. When you choose **local-syslog**, log messages are not available for display in the Configuration utility.

Although local logging is not recommended, you can store log messages locally on the BIG-IP system instead of or in addition to storing logs remotely.

Note: *The BIG-IP system is not a logging server and has limited capacity for storing, archiving, and analyzing logs. For this reason a dedicated logging server is recommended.*

Flowchart for local logging configuration

F5® recommends remote high-speed logging. However, you can configure local logging instead of or in addition to remote logging if you want to do so.

Note: *The BIG-IP® system is not a logging server and has limited capacity for storing, archiving, and analyzing logs.*

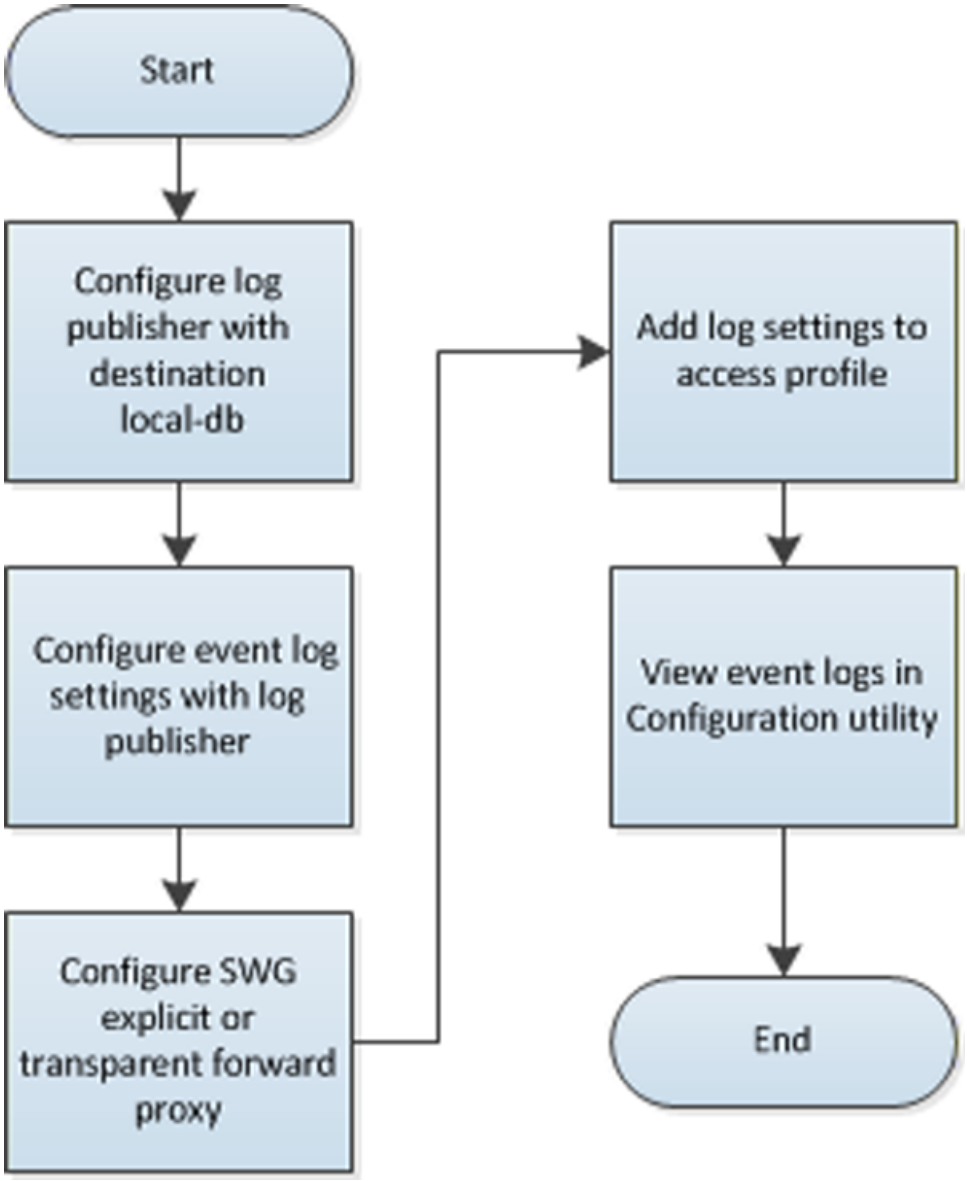

Figure 13: Secure Web Gateway local logging configuration

Overview: Monitoring Internet traffic and making adjustments to SWG

You can view Secure Web Gateway (SWG) statistics on the BIG-IP® system and adjust SWG based on the information that you gather from reports. Charts display statistical information about web traffic on your system, including the following details:

Actions
Action (allowed or blocked) taken on the URL request.

Client IP address
IP address from which the request for the URL originated.

Host Name
When available, host name from which the request for the URL originated.

Categories
Name of the preconfigured or custom URL category into which a requested URL falls.

URLs
Requested URL.

Schemes
Name of the scheme that SWG applied to the request based on your access policy configuration.

URL filters
Name of the URL filter SWG applied to the request based on the schedule in the scheme.

Security categories
The security category of the URL if it was blocked, because it matched a security category.

Users
Name of the user that made the request, if available.

Note: *Configuring your system to identify users is optional.*

SSL bypass
Whether the request was bypassed (yes or no).

Note: *Configuring your system to omit certain SSL traffic from inspection is optional.*

The system updates the statistics every five minutes; you can refresh the charts periodically to see the updates. SWG provides overview charts and report charts.

Note: *You can access statistics when SWG is provisioned and when you enable data collection for SWG reports.*

Overview
The Secure Web Gateway overview charts summarize the top requests, such as top URLs, top categories by blocked request count, top users by permitted request count or by blocked request count, and so on. You can customize the Overview so that it shows the specific type of data you are interested in.

Reports
Secure Web Gateway provides two reports: All Requests and Blocked Requests. You can filter the reports to show the information that you want to see.

From the Overview or Reports, you can export data to a PDF or CSV file, or send the reports to one or more email addresses.

Task summary

Configuring statistics collection for reports
Examining Secure Web Gateway statistics
Focusing charts and reports on security threats
Exporting or emailing Secure Web Gateway statistics
Creating an SMTP server configuration
Chart and report drilldown paths
When drilling down to get more details from a chart or report, the data that displays depends on the starting point and the selections made while drilling down.

About the reporting interval for charts and reports

The system updates the statistics for charts and reports at five minute intervals: at five minutes after the hour, ten minutes after the hour, and so on.

Charts and data that you export from charts reflect the publishing interval of five minutes. For example, if you request data for the time period 12:40-13:40, the data in the chart or in the file that you export is for the time period 12:35-13:35. By default, the BIG-IP® system displays one hour of data.

Configuring statistics collection for reports

You configure report settings to specify whether to gather statistics for Secure Web Gateway (SWG) reports and whether to use data sampling.

1. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **Reports** > **Settings**.
   The Report Settings screen displays.
2. To enable statistics gathering, select the **Collect Data** check box.
   If you clear the check box, data collection stops.
3. To enable dynamic data sampling, select the **Sample Data** check box.
   In exchange for a performance gain, data sampling might provide slightly inaccurate statistics. If statistics must be more accurate, then disable data sampling.

Examining Secure Web Gateway statistics

Note: *Newer browsers (Internet Explorer 9 or later, Firefox 3.6 or later, or Chrome 14 or later) support viewing charts with no additional plug-in. If using older browsers (Internet Explorer 8 or earlier), Adobe® Flash® Player (version 8 or later) must be installed on the computer where you plan to view charts.*

You can review charts that show statistical information about traffic from your enterprise to the Internet. The charts provide visibility into the top requests for URL categories, blocked URL categories, top users, and so on.

1. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **Overview**.
   The Overview screen displays charts for each widget.

2. From the **Override time range to** list, select a new time frame to apply to all of the widgets in the overview.

   Tip: *Within each widget you can override the default time range, as needed.*

3. For each widget, select the data format and the time range to display, as needed.
4. To focus on the specific details you want more information about, click the chart or the **View Details** link.
   The system refreshes the charts and displays information about the item.
5. From the **View By** list, select the specific network object type for which you want to display statistics.
   You can also click **Expand Advanced Filters** to filter the information that displays.
6. On the screen, the system displays the path you followed to reach the current display, including the items you clicked. For example, to review details for the top categories, follow these steps:
   a) In the Top categories by Request Count chart, click the category that interests you.
      Assume that your URL filters allow access to some news and media sites and that **News and Media** is among the top categories. Click **News and Media**.
      Charts display the request count per action over time and the request count per action. A details table lists the request count for allowed actions.
   b) In the **View By** list, select **URLs**.
      Assume that one of the URLs concerns you and you want to know which URL filter or scheme allowed access to it.
      Charts update and a list of URLs displays in the details table. These are the top news and media URLs.
   c) To see which filter allowed this URL, from here you can continue to drill down successively by clicking a link in each details table that displays. These links should first display statistics for URL filter and then for scheme. As an alternative to drilling down, you can select any of the statistics displayed on the **View By** list; for example you can select **URL Filter** or **Scheme** directly.

   The Overview charts display summarized data. You might notice as you drill down that details display on the Reports screen.

You can review the access policy to ensure that you use the optimal strategy for applying a scheme a user. You can update URL filters to block or allow particular URL categories. You can update URL categories to include new URLs that you have seen in statistics details, or to recategorize existing URLs to fit your policies. You can continue to review the collected metrics and troubleshoot the system as needed.

Focusing charts and reports on security threats

You can display attempted access to sites that pose a security risk by adding the security category widget to the Secure Web Gateway Overview screen and by filtering a Blocked Request report using the security categories filter.

1. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **Overview**.
   The Overview screen displays charts for each widget.
2. Click the **Add Widget** link near the bottom of the screen.
   The Add New Widget screen displays.
3. From the **Modules** list, select **Secure Web Gateway (Blocked)**.
   The security categories widget includes data requests that were blocked.
4. From the **View by** list, select **Security Categories**.

Requests that were blocked for URLs because they are included in the Security category or any of its subcategories are included in the data.

5. Move a measurement from **Available measurements** to the **Select up to 6 measurements to display** list.
6. For **Data visualization**, select one of the options.

   Details Table is the default option.
7. Click **Done**.
   The Add New Widget screen closes.

The Overview screen displays the Security Categories chart.

You can also filter a Blocked Requests report to view this data by selecting **Security Categories** from the **View by** list.

Overview: Monitoring Internet traffic and making adjustments to SWG

Examining Secure Web Gateway statistics

Exporting or emailing Secure Web Gateway statistics

Exporting or emailing Secure Web Gateway statistics

You can export or email charts that show Secure Web Gateway (SWG) statistics.

1. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **Overview**.
   The Overview screen displays charts for each widget.
2. Display the charts that show the information you want, clicking any of the options and adjusting the content as needed.
3. On the upper right of the charts screen, click **Export**.

Tip: *You can also export any single report widget from the Overview screen. Click the widget configuration icon for the report and select* ***Export****.*

The Choose Export Options popup screen opens.

4. Choose the appropriate options.

Option	Action
Export the data in *option* format	Specify the export format: • Select **PDF** to save the information in a graphical format to a PDF file. • Select **CSV (Time Series)** to export the information to a text file including specific information for time increments. • Select **CSV (Details Table)** to export the information to a text file providing summary details. If exporting the entire Overview screen, the information is saved only in PDF format (no export format options are available). When exporting widgets, the format options are **PDF** or **CSV** (only one CSV format is provided).
Save the report file on your computer	Select this option to save or open the file containing the report.
Send the report file as an attachment to the following E-mail address(es)	Type one or more email addresses (separated by comma or semicolon) to which to send the report.

5. Click **Export**.
   The system saves the report to a file, or emails the file to the specified recipients. If SMTP is not configured (when sending reports by email), you receive a message that SMTP must be set up before you can send the reports.

Creating an SMTP server configuration

You specify the SMTP server configuration so that you can send emails through an SMTP server.

1. On the Main tab, click **System** > **Configuration** > **Device** > **SMTP**.
2. Click the **Create** button.
   The New SMTP Configuration screen opens.
3. In the **Name** field, type a name for the SMTP server that you are creating.
4. In the **SMTP Server Host Name** field, type the fully qualified domain name for the SMTP server host.
5. In the **SMTP Server Port Number** field, type a port number.
   For no encryption or TLS encryption, the default is `25`. For SSL encryption, the default is `465`.
6. In the **Local Host Name** field, type the host name used in the SMTP headers in the form of a fully qualified domain name.
   This host name is not the same as the BIG-IP system's host name.
7. In the **From Address** field, type the email address that you want displayed as the reply-to address for the email.
8. From the **Encrypted Connection** list, select the encryption level required for the SMTP server.
9. To require that the SMTP server validates users before allowing them to send email, select the **Use Authentication** check box, and type the user name and password required to validate the user.
10. Click the **Finish** button.

You can now configure the system to use this SMTP server to send emails. For the SMTP mailer to work, you must make sure the SMTP server is on the DNS lookup server list, and configure the DNS server on the BIG-IP® system.

Chart and report drilldown paths

When drilling down to get more details from a chart or report, the data that displays depends on the starting point and the selections made while drilling down.

Table 2: Charts and reports for all requests

Drilldown path	Alternative drilldown path
1. Actions 2. SSL Bypass 3. Users 4. Client IP Addresses 5. Host Names 6. URLs 7. Categories 8. URL Filters 9. Schemes	1. Actions 2. SSL Bypass 3. Host Names 4. URLs 5. Categories 6. URL Filters 7. Schemes

Table 3: Charts and reports for blocked requests

Path
1. SSL Bypass **2.** Users **3.** Client IP Addresses **4.** Host Names **5.** URLs **6.** Categories **7.** URL Filters **8.** Schemes **9.** Security Categories

Overview: Monitoring Internet traffic and making adjustments to SWG
Creating an SMTP server configuration
Overview: Configuring remote high-speed SWG event logging

Overview: Configuring remote high-speed SWG event logging

You can configure the BIG-IP® system to log information about Secure Web Gateway (SWG) events and send the log messages to remote high-speed log servers.

Important: *SWG must be licensed and provisioned before you can configure event logging for it.*

When configuring remote high-speed logging of SWG events, it is helpful to understand the objects you need to create and why, as described here:

Object	Reason
Pool of remote log servers	Create a pool of remote log servers to which the BIG-IP system can send log messages.
Destination (unformatted)	Create a log destination of Remote High-Speed Log type that specifies a pool of remote log servers.
Destination (formatted)	If your remote log servers are the ArcSight, Splunk, or Remote Syslog type, create an additional log destination to format the logs in the required format and forward the logs to a remote high-speed log destination.
Publisher	Create a log publisher to send logs to a set of specified log destinations.
Log Setting	Create event log settings to enable logging of user-specified data, and associate a log publisher with the log settings.
SWG configuration	Create a configuration for SWG explicit forward proxy or transparent forward proxy.
Access profile	Add log settings to the access profile in the explicit forward proxy or transparent forward configuration.

Object	Reason
Virtual server	In a SWG configuration, an access profile is associated with the virtual server that handles the forward proxy traffic.

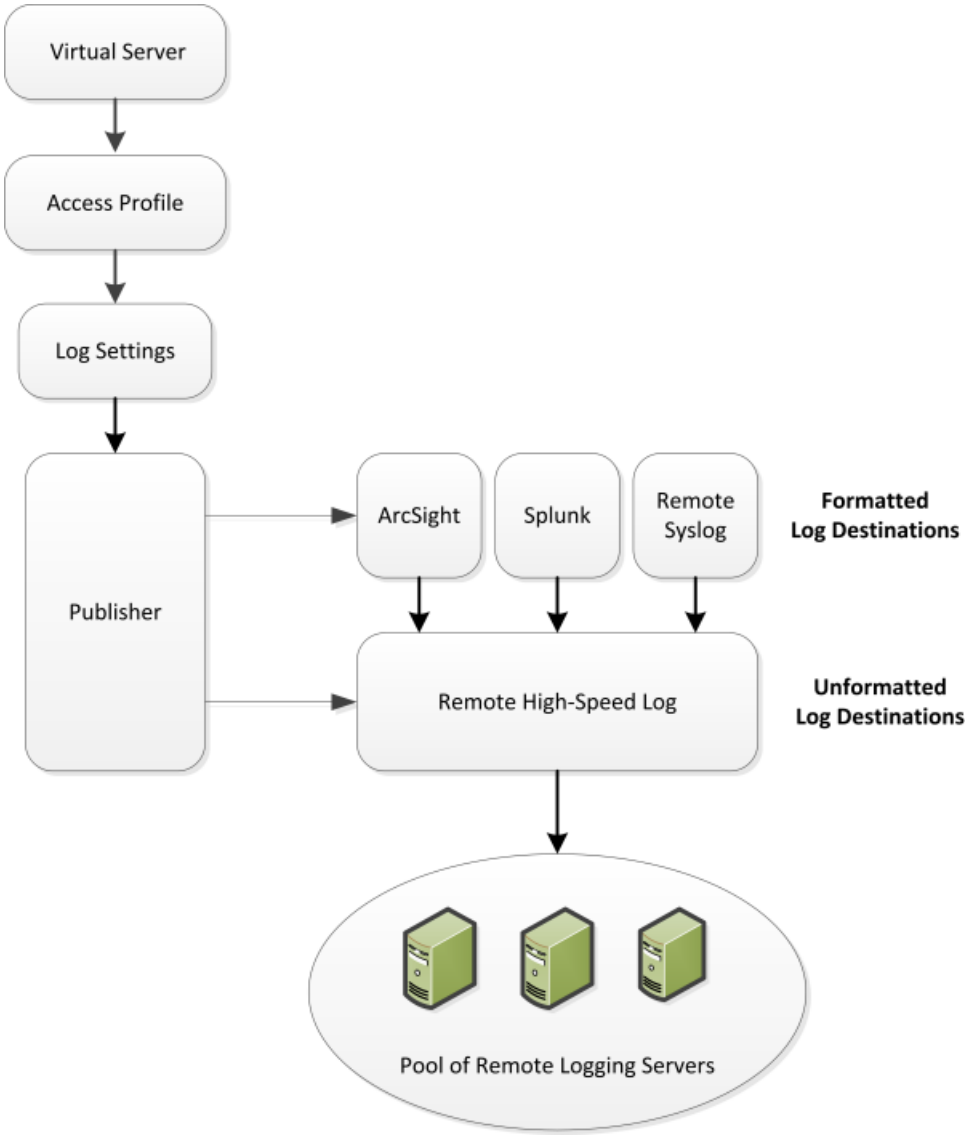

Figure 14: Association of remote high-speed logging configuration objects

Task summary

Perform these tasks to configure remote high-speed SWG event logging on the BIG-IP system.

Note: *Enabling remote high-speed logging impacts BIG-IP system performance.*

Task list

Creating a pool of remote logging servers
Creating a remote high-speed log destination
Creating a formatted remote high-speed log destination
Creating a publisher

Creating log settings for Secure Web Gateway events
Adding log settings to an access profile
Disabling logging

Creating a pool of remote logging servers

Before creating a pool of log servers, gather the IP addresses of the servers that you want to include in the pool. Ensure that the remote log servers are configured to listen to and receive log messages from the BIG-IP® system.

Create a pool of remote log servers to which the BIG-IP system can send log messages.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. Using the **New Members** setting, add the IP address for each remote logging server that you want to include in the pool:
   a) Type an IP address in the **Address** field, or select a node address from the **Node List**.
   b) Type a service number in the **Service Port** field, or select a service name from the list.

   Note: *Typical remote logging servers require port* `514`.

   c) Click **Add**.
5. Click **Finished**.

Creating a remote high-speed log destination

Before creating a remote high-speed log destination, ensure that at least one pool of remote log servers exists on the BIG-IP® system.

Create a log destination of the **Remote High-Speed Log** type to specify that log messages are sent to a pool of remote log servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **Remote High-Speed Log**.

   Important: *If you use log servers such as Remote Syslog, Splunk, or ArcSight, which require data be sent to the servers in a specific format, you must create an additional log destination of the required type, and associate it with a log destination of the* ***Remote High-Speed Log*** *type. With this configuration, the BIG-IP system can send data to the servers in the required format.*

   The BIG-IP system is configured to send an unformatted string of text to the log servers.
5. From the **Pool Name** list, select the pool of remote log servers to which you want the BIG-IP system to send log messages.

6. From the **Protocol** list, select the protocol used by the high-speed logging pool members.
7. Click **Finished**.

Creating a formatted remote high-speed log destination

Ensure that at least one remote high-speed log destination exists on the BIG-IP® system.

Create a formatted logging destination to specify that log messages are sent to a pool of remote log servers, such as Remote Syslog, Splunk, or ArcSight servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select a formatted logging destination, such as **Remote Syslog**, **Splunk**, or **ArcSight**.
   The Splunk format is a predefined format of key value pairs.
   The BIG-IP system is configured to send a formatted string of text to the log servers.
5. If you selected **Remote Syslog**, from the **Syslog Format** list, select a format for the logs, and then from the **High-Speed Log Destination** list, select the destination that points to a pool of remote Syslog servers to which you want the BIG-IP system to send log messages.

   Important: *For logs coming from Access Policy Manager® (APM®), only the BSD Syslog format is supported.*

6. If you selected **Splunk** from the **Forward To** list, select the destination that points to a pool of high-speed log servers to which you want the BIG-IP system to send log messages.
   The Splunk format is a predefined format of key value pairs.
7. Click **Finished**.

Creating a publisher

Ensure that at least one destination associated with a pool of remote log servers exists on the BIG-IP® system.

Create a publisher to specify where the BIG-IP system sends log messages for specific resources.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this publisher.
4. For the **Destinations** setting, select a destination from the **Available** list, and click **<<** to move the destination to the **Selected** list.

   Note: *If you are using a formatted destination, select the destination that matches your log servers, such as Remote Syslog, Splunk, or ArcSight.*

5. Click **Finished**.

Creating log settings for Secure Web Gateway events

Create log settings to specify event logging for Secure Web Gateway (SWG) events.

1. On the Main tab, click **Access Policy** > **Event Logs** > **Log Settings**.
   A list displays.
2. Click **Create**.
   A popup screen opens with General Information selected in the left pane.
3. Fill in the fields.

   The **Log for Secure Web Gateway** check box is selected by default. If you clear this check box, logging is disabled in these settings.

   Note: *You can create multiple log settings for Secure Web Gateway (SWG) and attach multiple log settings to an access profile.*

4. To select a publisher for a high-speed log destination or to change the types of events to log, from the left pane, select **Secure Web Gateway**.
   Settings in the right pane change.
5. From the **Log Publisher** list, select the log publisher of your choice.

   The default log publisher publishes to a destination on the BIG-IP® system.
6. To log events, you must select at least one check box:

   - **Log Allowed Events**: When selected, user requests for allowed URLs are logged.
   - **Log Blocked Events**: When selected, user requests for blocked URLs are logged.

   Whether a URL is allowed or blocked depends on the URL category into which it falls and on URL filter that is applicable at the time of the request.
7. Click **OK**.
   The popup screen closes. The new log setting displays on the list.

To put a log setting into effect, you must assign it to an access profile.

Adding log settings to an access profile

You add log settings to an access profile to log events on the traffic that passes through the virtual server to which the access profile is assigned.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile that you want to edit. The properties screen opens.
3. On the menu bar, click **Logs**.
   The access profile log settings display.
4. Move log settings between the **Available** and **Selected** lists.

   You can assign multiple log settings to an access profile. Logging is disabled when the **Selected** list is empty.

   Note: *Logging can also be disabled in the log setting itself. To check the status, view Log Settings in the Event Logs area of the user interface.*

5. Click **Update**.

An access profile is in effect when it is assigned to a virtual server.

Disabling logging

Disable event logging for Secure Web Gateway (SWG) when you need to suspend logging for a period or time or you no longer want the BIG-IP® system to log specific events.

Note: *Logging is enabled by adding log settings to the access profile.*

1. To clear log settings from access profiles, on the Main tab, click **Access Policy** > **Access Profiles**.
2. Click the name of the access profile.
   Access profile properties display.
3. On the menu bar, click **Logs**.
4. Move log settings from the **Selected** list to the **Available** list.
5. Click **Update**.

Chapter 9

Kerberos Authentication and SWG

- *Overview: Authenticating SWG users with Kerberos*

Overview: Authenticating SWG users with Kerberos

You can include authentication in the access policy in a Secure Web Gateway (SWG) explicit or transparent forward proxy configuration. When you do so if the first site that a user accesses uses HTTP instead of secure HTTP, passwords are passed as clear text. To prevent this from happening, F5® recommends using Kerberos or NTLM authentication.

Kerberos authentication relies on these access policy actions:

- HTTP 407 response and Kerberos authentication for SWG explicit forward proxy
- HTTP 401 response and Kerberos authentication for SWG transparent forward proxy

These access policy items require an AAA Kerberos server object configured in Access Policy Manager®.

Kerberos authentication also requires a domain-joined, Windows-based user account.

This implementation includes steps for configuring and troubleshooting Kerberos authentication, so that you have what you need in place and working before you configure SWG access policies.

Task summary

Joining a Kerberos user account to a domain
Configuring an AAA server for Kerberos authentication

About basic authentication and Kerberos end-user logon

Access Policy Manager® (APM®) provides an alternative to the form-based login authentication method. Instead, an HTTP 401 (unauthorized) or HTTP 407 (proxy authentication required) response triggers a browser login screen to collect credentials.

This option is useful when a user is already logged in to the local domain and you want to avoid submitting an APM HTTP form for collecting user credentials. The browser automatically submits credentials to the server and bypasses the login box to collect the credentials again.

Note: *Because SPNEGO/Kerberos is a request-based authentication feature, the authentication process is different from other authentication methods, which run at session creation time. SPNEGO/Kerberos authentication can occur at any time during the session.*

The benefits of this feature include:

- Provides flexible login mechanism instead of restricting you to use only the form-based login method.
- Eliminates the need for domain users to explicitly type login information again to log in to APM.
- Eliminates the need for user password transmission with Kerberos method.

Important: *Administrators should not turn off the* ***KeepAlive*** *setting on the web server because turning that setting off might interfere with Kerberos authentication.*

How does end-user logon work?

To retrieve user credentials for end-user logon, you can use the basic authentication method, or the SPNEGO/Kerberos method (which is recommended), or both.

Basic authentication

Use this method to retrieve user credentials (user name and password) from a browser. You can think of this method as a replacement for form-based authentication used by the standard login screen. If you use basic authentication, Access Policy Manager® (APM®) populates the user name and password session variables, which can then be used by any other authentication actions, such as Active Directory or RADIUS.

Note: *When using basic authentication, passwords are passed as clear text.*

SPNEGO/Kerberos

Use this method to retrieve user credentials through the SPNEGO/Kerberos authentication header. With the Kerberos method, the client system must first join a domain. A Kerberos action does not run immediately; it runs only when the server requests SPNEGO/Kerberos authentication. By default, Kerberos authentication runs not only on the first request, but also on subsequent requests where authentication is needed, such as for new connections. APM validates the request by confirming that a valid ticket is present.

Note: *You can disable Kerberos per request-based authentication in the AAA Kerberos authentication access policy item configuration in APM. If you disable it, authentication occurs while the access policy runs and subsequent authentications do not occur.*

Both methods require that either an HTTP 401 Response (unauthorized) or an HTTP 407 Response (proxy authentication required) action item be configured in the access policy, and that the authentication method (basic, negotiate, or basic + negotiate) be specified in the action item.

In cases where both methods (basic + negotiate) are selected, the browser determines which method to perform based on whether the system has joined a domain. The HTTP 401 Response and HTTP 407 Response actions each have two default branches to indicate whether basic authentication or Kerberos method is performed.

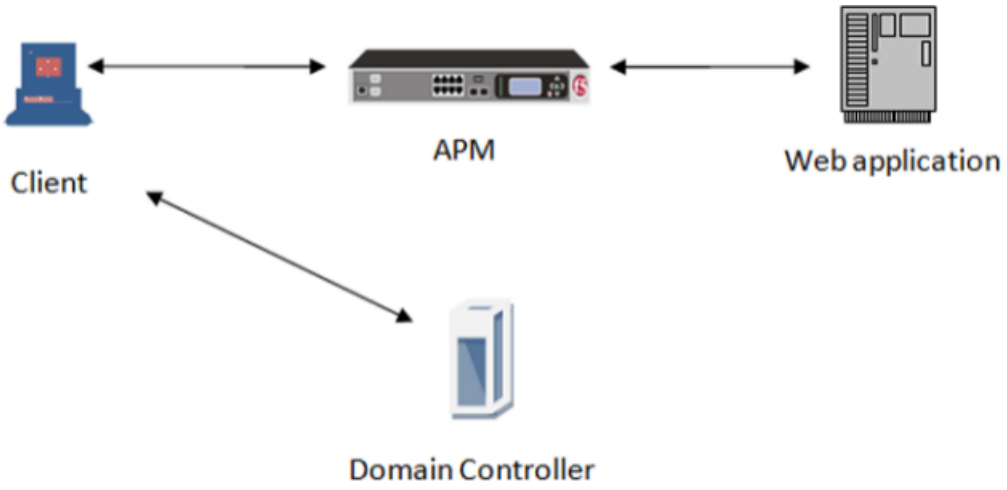

Figure 15: How SPNEGO/Kerberos end-user login works

The end-user logon works with events happening in this order:

- The client becomes a member and connects to the domain.
- The client connects to a virtual server on the BIG-IP® system.
- The access policy runs and issues a 401 or 407 HTTP response.
- If a Kerberos ticket is present or can be obtained, the browser forwards the Kerberos ticket along with the request when it receives the 401 or 407 response.
- APM validates the Kerberos ticket after the request is received, and determines whether or not to permit the request.

About Kerberos authentication requirements

To configure Kerberos authentication, you must meet specific configuration requirements as described here.

Virtual server
The virtual server IP address and host name are necessary to configure DNS.

DNS configuration
Make sure you have the zone file and PTR record for the virtual server IP address. For example:

```
testbed.lab.companynet 10.10.4.100
```

Browser configuration
Configure the browser to use Kerberos. Typically, Internet Explorer is already configured for Kerberos; however, you might need to configure it for trusted sites. To use Firefox, you must configure it for negotiate authentication.

Joining a Kerberos user account to a domain

To use Kerberos authentication, you need the client joined and connected to a domain and you need a keytab file.

1. Create a surrogate user in the domain.

   In this example, the hostname of the virtual server on the BIG-IP system is testbed.lab.companynet and the user name is john.

   ```
   setspn -U -A HTTP/testbed.lab.companynet john
   ```

2. Map the user account to the service account and generate a keytab file for the service.

   You can use the ktpass utility to do this. In this example, LAB.COMPANYNET specifies the Kerberos authentication realm.

   ```
   c:>ktpass -princ HTTP/testbed.lab.companynet.com@LAB.COMPANYNET -mapuser
   john@LAB.COMPANYNET -crypto rc4-hmac-nt -ptype KRB5_NT_SRV_HST -pass password
   -out c:\temp\john.keytab
   ```

Configuring an AAA server for Kerberos authentication

Configure a Kerberos AAA server so that you can add it to a Kerberos authentication action in an access policy.

1. On the Main tab, click **Access Policy** > **AAA Servers** > **Kerberos**.
   The Kerberos Servers list screen opens.
2. Click **Create**.
   The New Server properties screen opens.
3. In the **Name** field, type a unique name for the authentication server.
4. In the **Auth Realm** field, type a Kerberos authentication realm name (administrative name), such as `LAB.COMANYNET`.

   Type the realm name all uppercase; it is case-sensitive.
5. In the **Service Name** field, type a service name; for example, `HTTP`.
6. In the **Keytab File** area, click **Choose File** to locate and upload the keytab file.

A keytab file contains Kerberos encryption keys (these are derived from the Kerberos password).

7. Click **Finished**.
   The new server displays on the list.

Kerberos authentication troubleshooting tips

You might choose to verify Kerberos authentication configurations in some instances. Use these troubleshooting tips to help resolve any issues you might encounter.

Verify the keytab file

From the command line, use the `klist` command as shown in this example.

Important: *The command must be typed on one line.*

```
klist -ke
WRFILE:/config/filestore/files_d/Common_d/kerberos_keytab_file_d/\:Common\:SUN-SPNEGO-APM106_key_file_2
```

The output for the example contains information like this.

```
Keytab name:
FILE:/config/filestore/files_d/Common_d/kerberos_keytab_file_d/:Common:SUN-SPNEGO-APM106_key_file_2
KVNO Principal
3    HTTP/apm106.labt.companynet.com@labt.companynet.com(arcfour-hmac)
```

Verify Kerberos delegation

From the command line, use the `kinit` command, as shown in this example.

```
kinit HTTP/apm106.labt.companynet.com@labt.companynet.com
```

You are prompted for a password and should receive a ticket (no output, no error).

Verify ticket

From the command line, type `klist`. Here is sample output: `/etc/krb5.conf`

Capture a TCP dump

Make sure the client sends the ticket to the BIG-IP® system; this verifies that the client setup is successful.

Implementation result

You should have a domain-joined user account for Kerberos and an AAA Kerberos server configured in Access Policy Manager®.

Chapter 10

NTLM Authentication and SWG

- *Overview: Authenticating SWG users with NTLM*

Overview: Authenticating SWG users with NTLM

You can include authentication in the access policy in a Secure Web Gateway (SWG) explicit or transparent forward proxy configuration. When you do so if the first site that a user accesses uses HTTP instead of secure HTTP, passwords are passed as clear text. To prevent this from happening, F5® recommends using Kerberos or NTLM authentication.

This implementation includes steps for configuring the NTLM authentication objects that you need to have in place before you configure NTLM authentication in an SWG explicit or transparent forward proxy access policy.

Task summary

Configuring a machine account
Creating an NTLM Auth configuration
Maintaining a machine account

Configuring a machine account

You need to configure a machine account so that Access Policy Manager® (APM®) can establish a secure channel to a domain controller.

1. On the Main tab, click **Access Policy** > **Access Profiles** > **NTLM** > **Machine Account**.
   A new Machine Account screen opens.
2. In the Configuration area, in the **Machine Account Name** field, type a name.
3. In the **Domain FQDN** field, type the fully qualified domain name (FQDN) for the domain that you want the machine account to join.
4. (Optional) In the **Domain Controller FQDN** field, type the FQDN for a domain controller.
5. In the **Admin User** field, type the name of a user who has administrator privilege.
6. In the **Admin Password** field, type the password for the admin user.

   APM uses these credentials to create the machine account on the domain controller. However, APM does not store the credentials and you do not need them to update an existing machine account configuration later.
7. Click **Join**.

This creates a machine account and joins it to the specified domain.

Creating an NTLM Auth configuration

Create an NTLM Auth configuration to specify the domain controllers that a machine account can use to log in.

1. On the Main tab, click **Access Policy** > **Access Profiles** > **NTLM** > **NTLM Auth Configuration**.
   A new NTLM Auth Configuration screen opens.
2. In the **Name** field, type a name.
3. From the **Machine Account Name** list, select the machine account configuration to which this NTLM Auth configuration applies.

   You can assign the same machine account to multiple NTLM authentication configurations.

4. For each domain controller, type a fully qualified domain name (FQDN) and click **Add**.

   Note: *You should add only domain controllers that belong to one domain.*

   By specifying more than one domain controller, you enable high availability. If the first domain controller on the list is not available, Access Policy Manager® tries the next domain controller on the list, successively.

5. Click **Finished**.

This specifies the domain controllers that a machine account can use to log in.

Maintaining a machine account

In some networks, administrators run scripts to find and delete outdated machine accounts on the domain controllers. To keep the machine account up-to-date, you can renew the password periodically.

1. On the Main tab, click **Access Policy** > **Access Profiles** > **NTLM** > **Machine Account**.
   The Machine Account screen opens.
2. Click the name of a machine account.
   The properties screen opens and displays the date and time of the last update to the machine account password.
3. Click the **Renew Machine Password** button.
   The screen refreshes and displays the updated date and time.

This changes the machine account last modified time.

Index

A

access policy
    configuring a Deny ending *57*
    per-request policy compared *48*
access profile
    creating *67*, *81*, *95*
    for SWG explicit forward proxy *112*
    for SWG transparent forward proxy *124*
    specifying log settings *143*
ACL
    support with SWG explicit forward proxy *61*
AD group lookup
    dependence on access policy *56*
    per-request policy item *56*
application access
    and SWG configuration *119–120*
application service
    deploying for IF-MAP *30*, *38*
application templates
    defined *16*
    for Secure Web Gateway configuration *61*, *77*, *91*

B

basic authentication and Kerberos end-user logon
    about *146*
blacklist
    using a custom category *23*

C

captive portalsredirects
    after captive portal access denied *89*, *103*
    and redirects after access denied *89*, *103*
category filter lookup
    and response analytics *52*
    per-request policy example *52*
category lookup
    configuring Safe Search *54*
    per-request policy example *50–51*
    per-request policy item *54*
    providing content for response analytics *54*
category lookupdynamic date timegroup lookupURL filter
        assign
    per-request policy example *50–51*
chart
    drilldown path *138*
    drilling down for details *138*
charts
    reporting interval *135*
client proxy
    network access resource *118*
Client SSL forward proxy profiles
    creating *71*, *84*, *99*, *114*, *125*
Client SSL profiles
    creating *88*, *101*
connectivity profile
    creating *107*, *121*
    for secure connectivity interface *108*, *121*
cookies
    APM session management *28*
Custom Categories *23*

D

database download
    debug logs *26*
    scheduling *22*
    warning *22*
database downloads
    and customization *24*
day-based access
    configuring *51*
dc_agent.txt file
    configuring *34*
    location *34*
    purpose *34*
debug logging
    enabling for F5 Logon Agent *42*
    for F5 DC Agent *35*
destinations
    for local logging *132*
    for logging *142*
    for remote high-speed logging *141*
DNS resolver
    adding forward zones *62*, *108*
    creating *62*, *108*
documentation, finding *18*
domain controllers
    disabling polling *34*
    enabling polling *34*
domain join *152*
dynamic date time
    per-request policy example *51*
    per-request policy item *55*

E

emails
    sending Secure Web Gateway reports *137*
    sending through SMTP server *138*
endings
    for per-request policy branches *57*
end-user logon
    about *146*
event logging
    adding to an access profile *143*
    overview *139*
explicit forward proxy
    ACL support with SWG *61*
    configuration using an iApp template *61*, *77*, *91*
    configuring *60–61*, *76*, *91*
    recommendation for authentication *68*

F

F5 DC Agent
  and subnets *29*
  defined *16*
  downloading *32*
  enabling authentication for *30*
  initialization file, configuring *33*
  installation, best practice *29*
  installing *32*
  licensing requirement *32*
  logging debug messages *35*
  ports used *29*
  provisioning requirement *32*
  reinstalling *35*
  service logon *32*
  troubleshooting *36*
  uninstalling *35*
  using *32*
  verifying DNS for *31*
  verifying NetBIOS for *31*
  viewing error messages *36*
  Windows user account *32*
F5 Logon Agent
    43, *45*
  Active Directory *44*
  and licensing requirement *40*
  and ports used *37*
  and provisioning requirement *40*
  and service logon *40*
  and subnets *37*
  and Windows user account *40*
  configuring initialization file *41*
  downloading *40*
  enabling authentication for *38*
  installing *40*
  logging debug messages *42*, *44*
  overview *37*
  reinstalling *42*
  troubleshooting *43*
  uninstalling *42*
  verifying DNS for *39*
  verifying NetBIOS for *39*
  when to use *40*
F5 Logon Agent initialization file
  configuring *41*
F5 Logon Agent installation
  and best practice *37*
F5 Logon Agent installation files
  described *43*
flowchart
  configuring local logging *133*
  configuring Secure Web Gateway *17*
forward proxy statistics
  exporting *137*
forward zones
  adding to DNS resolver *62*, *108*

G

glossary *16*
group-based access
  example per-request policy *51*
group lookup
  per-request policy example *51*
guides, finding *18*

H

high-speed logging
  and server pools *141*
HTTP profiles
  creating *64*, *109*

I

iApps template
  for configuring F5 DC Agent communication *30*
  for configuring F5 Logon Agent communication *38*
  for SWG configuration *61*, *77*, *91*
identifying users by IP address
  explicitly *28*, *61*, *77*, *91*
  transparently *28*, *61*, *77*, *91*
  using subnets *28*, *61*, *77*, *91*
IF-MAP server
  and transparent user identification *29*
  defined *16*
  specifying IP address *33*, *41*
initialization file
  and BIG-IP system address *41*
  and location *41*
  authentication, specifying *33*
  BIG-IP system address *33*
  specifying authentication *41*
  where located *33*
Instant Messaging category
  supported messaging protocols *22*

K

Kerberos authentication requirements
  about *148*
Kerberos authentication troubleshooting tips *149*
Kerberos configuration
  domain, joining a *148*
  user account, creating *148*

L

LDAP group lookup
  dependence on access policy *56*
  per-request policy item *56*
licensing requirement
  for F5 Logon Agent *40*
LocalDB group lookup
  dependence on access policy *56*
  per-request policy item *56*
localization
  customizing the Deny ending *57*
local logging
  configuration flowchart *133*

local user database
account for F5 DC Agent *30*
and account for F5 Logon Agent *38*
log files
access policy *132*
logging
access policy *132*
and destinations *141–142*
and pools *141*
and publishers *142*
and Secure Web Gateway events *143*
disabling for Secure Web Gateway *144*
local *132*
remote *132*
Secure Web Gateway event *132*
logon script
44
parameter *45*
logout script
44
parameter *45*

M

machine account
renewing password for *153*
machine trust account
configuring in Access Policy Manager *152*
manuals, finding *18*
messaging protocols
supported *22*

N

name resolution
using the BIG-IP system *62*, *108*
network access
and explicit forward proxy *106–107*, *120*
and SWG configuration *106–107*, *119–120*
and transparent forward proxy *119–120*
SWG explicit forward proxy configuration *119*
network access resource
client proxy settings *118*
NTLM authentication
accessing domain-joined Microsoft Exchange clients *152*

P

per-request policy
access policy compared *48*
and Secure Web Gateway *48*
branches for *49*
configuring for SWG *48*, *64*, *79*, *93*, *110*, *121*
Empty access policy action *53*
items for *49*
logging, enabling *49*, *132*
reporting *49*, *132*
unique items for *53*
per-request policy endings
about *57*
per-request policylogging report
per-flow variable *52*
pools
for high-speed logging *141*
portal access
and SWG configuration *119–120*
profiles
creating for client-side SSL forward proxy *71*, *84*, *99*, *114*, *125*
creating for HTTP *64*, *109*
creating server SSL *71*, *85*, *99*, *115*, *126*
protocol lookup
per-request policy example *51*
per-request policy item *54*
provisioning requirement
for F5 Logon Agent *40*
proxy server
explicit forward proxy *70*, *113*
publishers
creating for logging *142*

R

RADIUS class lookup
in an access policy *57*
release notes, finding *18*
remote servers
and destinations for log messages *141–142*
for high-speed logging *141*
report
drilldown path *138*
drilling down for details *138*
reports
enabling statistics collection *135*
publishing interval *135*
using data sampling *135*
response analytics
contribution to URL filter assign *52*
dependence on category lookup *52*
per-request policy example *52*
per-request policy item *55*
providing web response page for *54*

S

Safe Search
enabling *54*
Safe Search search engines
about *49*
and Safe Search support *49*
search engines, supported *49*
scheme
assigning to a session *68*
scrip
creating *43*
running *43*
secure renegotiation
not strict *71*, *85*, *99*, *115*, *126*
Secure Web Gateway
about *16*
and event logging *143*
and per-request policy *48*
configuring explicit forward proxy *60–61*, *76*, *91*, *119*, *129*
configuring remote high-speed logging *139*

Secure Web Gateway *(continued)*
disabling logging *144*
emailing reports *137*
exporting forward proxy statistics *137*
fine-tuning URL filters *132*
initial configuration *22*
Safe Search support *49*
supporting network access clients *106–107*, *120*
supporting remote access clients *119*
threat monitoring *132*
URL categories *22*
URL filters *22*
web access schemes *22*
Secure Web Gateway statistics
examining *135*
security category widget
adding *136*
self IP addresses
creating for VLANs *78*, *92*
servers
and destinations for log messages *141–142*
and publishers for log messages *142*
for high-speed logging *141*
SMTP server
configuring *138*
SSL bypass set
per-request policy example *51*
SSL bypass setbypassSSL forward proxy traffic
bypassing in per-request policy *55*
per-request policy item *55*
SSL forward proxy traffic *55*
SSL forward proxy bypass
enabling *71*, *84*, *99*, *114*, *125*
SSL intercept setinterceptSSL forward proxy traffic
intercepting in per-request policy *54*
per-request policy item *54*
SSL forward proxy traffic *54*
SSL profiles
creating *88*, *101*
statistics
examining Secure Web Gateway *135*
exporting application *137*
reporting interval *135*
SWG-Explicit
access profile type *67*
SWG explicit forward proxy
and access profile type *112*
result *74*, *89*, *102*
SWG scheme
assigning from access policy *26*
assigning to a session *117*, *128*
SWG Scheme Assign
adding to access policy *117*, *128*
SWG statistics
overview *134*
SWG transparent forward proxy
and access profile type *124*
SWG URL category configuration
result *26*

T

tcp-forward
encapsulation type *63*
tunnel *63*
terminology *16*
threat monitoring *132*
time-based access
configuring *51*
transparent forward proxy
and remote access clients *129*
configuration using an iApp template *61*, *77*, *91*
configuring *76*, *119*
configuring an access policy *82*, *96*
forwarding virtual server, use for *87*
inline, defined *76*
policy-based routing *90*
WCCP *90*
transparent user identification *43*
about *37*
about how it works *29*
defined *16*
storing IDs *29*, *37*
troubleshooting
F5 DC Agent *36*
F5 Logon Agent *43*
user identification *43*
using error messages *36*
troubleshooting tips
for Kerberos authentication *149*
tunnel
tcp-forward *63*

U

URL
categorizing *24*
determining category for *24*
URL access
allowing *25*
blocking *25*
URL categories *22*
adding URLs *24*
allowing *25*
blocking *25*
customization, precedence of *24*
customizing *23*
downloading *22*
recategorized *24*
using as blacklists *23*
using as whitelists *23*
URL category
lookup *24*
URL filter
applying based on group *51*
URL filter assign
and response analytics *52*
per-request policy example *51–52*
URL filtering *22*

URL filter lookup
per-request policy item *55*
URL filters
25
adjusting to prevent threats *132*
URLs
prefix matching *23*
recategorizing *24*
user group-based access
configuring *51*
user identification
by credentials *28*, *61*, *77*, *91*
by IP address *28*, *61*, *77*, *91*
troubleshooting *43*

V

variable
per-flow *52–53*, *74*, *89*, *103*, *119*, *129*
session *53*, *74*, *89*, *103*, *119*, *129*
virtual servers
and secure connectivity interface *108*, *121*
virtual servers *(continued)*
creating for application traffic *86–87*, *100–101*, *114–115*, *125*, *127*
creating for HTTPS traffic *88*, *102*
creating for SSL forward proxy traffic *72*
explicit forward proxy server *70*, *113*
forwarding virtual servers *87*
reject type *73*
visual policy editor
and access policy *50*
and per-request policy *50*
VLANs
and self IP addresses *78*, *92*
creating *78*, *92*

W

whitelist
using a custom category *23*
Windows user account
for F5 DC Agent *32*
for F5 Logon Agent *40*