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

Version 11.5

Table of Contents

Legal Notices

Publication Date

This document was published on February 13, 2014.

Publication Number

MAN-0504-00

Copyright

Copyright © 2013-2014, F5 Networks, Inc. All rights reserved.

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

AAM, Access Policy Manager, Advanced Client Authentication, Advanced Firewall Manager, Advanced Routing, AFM, APM, Application Acceleration Manager, Application Security Manager, ARX, AskF5, ASM, BIG-IP, BIG-IQ, Cloud Extender, CloudFucious, Cloud Manager, Clustered Multiprocessing, CMP, COHESION, Data Manager, DevCentral, DevCentral [DESIGN], DNS Express, DSC, DSI, Edge Client, Edge Gateway, Edge Portal, ELEVATE, EM, Enterprise Manager, ENGAGE, F5, F5 [DESIGN], F5 Certified [DESIGN], F5 Networks, F5 SalesXchange [DESIGN], F5 Synthesis, f5 Synthesis, F5 Synthesis [DESIGN], F5 TechXchange [DESIGN], Fast Application Proxy, Fast Cache, FirePass, Global Traffic Manager, GTM, GUARDIAN, iApps, IBR, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, L7 Rate Shaping, LC, Link Controller, Local Traffic Manager, LTM, LineRate, LineRate Systems [DESIGN], LROS, LTM, Message Security Manager, MSM, OneConnect, Packet Velocity, PEM, Policy Enforcement Manager, Protocol Security Manager, PSM, Real Traffic Policy Builder, SalesXchange, ScaleN, Signalling Delivery Controller, SDC, SSL Acceleration, software designed applications services, SDAC (except in Japan), StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TechXchange, TMOS, TotALL, Traffic Management Operating System, Traffix Systems, Traffix Systems (DESIGN), Transparent Data Reduction, UNITY, VAULT, vCMP, VE F5 [DESIGN], Versafe, Versafe [DESIGN], VIPRION, Virtual Clustered Multiprocessing, WebSafe, and ZoneRunner, are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent.

All other product and company names herein may be trademarks of their respective owners.

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.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

This product includes software developed by Thomas Williams and Colin Kelley. Copyright ©1986 - 1993, 1998, 2004, 2007

Permission to use, copy, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Permission to modify the software is granted, but not the right to distribute the complete modified source code. Modifications are to be distributed as patches to the released version. Permission to distribute binaries produced by compiling modified sources is granted, provided you

1. distribute the corresponding source modifications from the released version in the form of a patch file along with the binaries,
2. add special version identification to distinguish your version in addition to the base release version number,
3. provide your name and address as the primary contact for the support of your modified version, and
4. retain our contact information in regard to use of the base software.

Permission to distribute the released version of the source code along with corresponding source modifications in the form of a patch file is granted with same provisions 2 through 4 for binary distributions. This software is provided "as is" without express or implied warranty to the extent permitted by applicable law.

This product contains software developed by Google, Inc. Copyright ©2011 Google, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

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. 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 software developed by Jeremy Ashkenas and DocumentCloud, and distributed under the MIT license. Copyright © 2010-2013 Jeremy Ashkenas, DocumentCloud.

This product includes gson software, distributed under the Apache License version 2.0. Copyright © 2008-2011 Google Inc.

This product includes Boost libraries, which are distributed under the Boost license (http://www.boost.org/LICENSE_1_0.txt).

Chapter 1

BIG-IP APM Secure Web Gateway Overview

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).
IF-MAP server	When you configure the BIG-IP system to communicate with the F5 DC 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.
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?

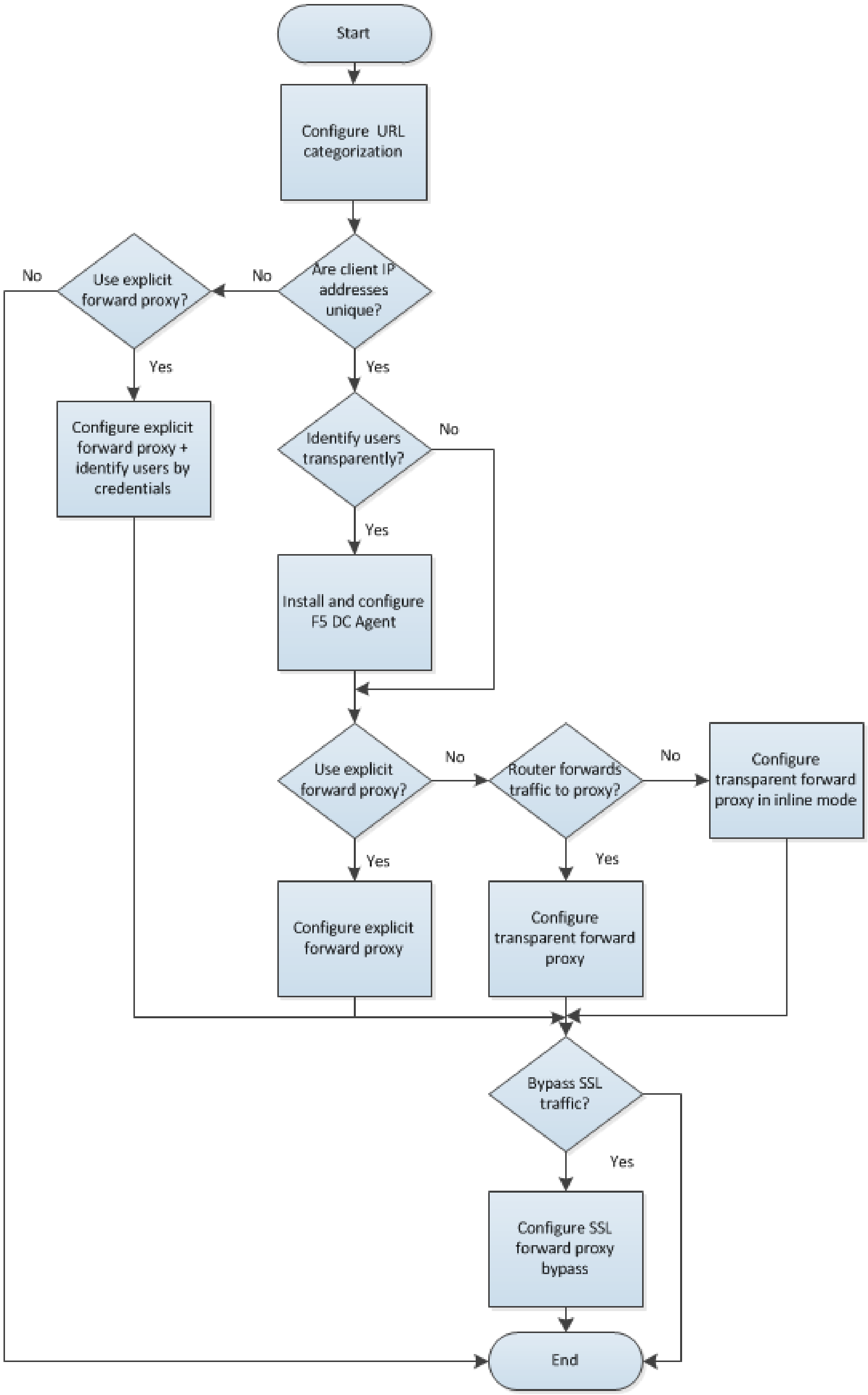
Start
Configure URL categorization
Are client IP addresses unique?
No
Use explicit forward proxy?
No
Yes
Configure explicit forward proxy + identify users by credentials
Yes
Identify users transparently?
No
Yes
Install and configure F5 DC Agent
Use explicit forward proxy?
No
Router forwards traffic to proxy?
No
Configure transparent forward proxy in inline mode
Yes
Configure explicit forward proxy
Yes
Configure transparent forward proxy
Bypass SSL traffic?
Yes
Configure SSL forward proxy bypass
End

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.
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.

Document	Description
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

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 configuring URL filters, you can group them and schedule them into SWG schemes. In an SWG scheme, you select and schedule URL filters so that at any time of day during a week, only one URL filter is actively being enforced. You can configure different schemes for different groups of users. In a scheme, you specify URL filters that you want to apply at specific periods in the day or and on specific days of the week.

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

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
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 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. You can use a custom category, for example, as a blacklist or as a whitelist.

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. 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/***.

5. Add, edit, or delete URLs to make the list.
6. Click **Finished**.
   The URL Categories screen displays.
7. 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.

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 add it to a scheme.

Configuring Secure Web Gateway schemes

You configure schemes to specify and schedule a group of URL filters that you want to apply to users.

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. In the Configuration area from the **SWG Service Failure Action** list, select the filtering action to take in the event that a service failure occurs.
   - **Block**
   - **Allow**

A service failure condition applies when SWG determines that an error occurred while trying to categorize a URL or analyze the response.

5. From the **Content Scanning (Response)** list, select whether and when to scan the content.

   Content scanning inspects the response web page contents for malicious embedded components.

   - **None**. No content scanning occurs.
   - **Recommended**. Content scanning occurs only when the system recommends it.

   If you select **Recommended**, **Max Buffer Size** and **Max Buffer Time** fields display.
6. In the **Max Buffer Size** field, retain the default value or type another value.

   This field 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 data is retained in the buffer.
7. In the **Max Buffer Time** field, retain the default value or type another value.

   This field specifies the maximum amount of time (in seconds) to retain data in the buffer. If the time elapses, SWG allows the response through to the client or sends the client a block page based on the URL category and action that SWG determined before the scan started.
8. From the **Default URL Filter** list, select the URL filter to apply if no other URL filter is scheduled.
9. Click **Finished**.
   The screen redisplays. The Associated Schedules table displays.
10. Add schedules to the scheme:

    Configure schedules that do not overlap one another.

    a) Click **Add**.
    b) From the **URL Filter** list, select a URL filter.
    c) For the fields in the **Time Range** setting, type or select the time to start using this scheme and the time to stop using this scheme.

       The default time range specifies 24 hours.
    d) For the **Days Valid** setting, select the days of the week that this schedule is in effect.
    e) The default settings specify all 7 days.
    f) To add another schedule, click **Repeat**.
    g) Click **Finished**.

    If there are gaps in the schedule, SWG uses the default filter to enforce the scheme.

    The Schemes screen displays.

A scheme goes into effect when an access policy assigns it to a user in a Secure Web Gateway (SWG) explicit forward proxy or transparent forward proxy configuration.

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

Secure Web Gateway (SWG) identifies users and maps them to IP addresses, or to sessions, without using cookies. Based on user identity, SWG assigns the appropriate scheme to each user. A *scheme* categorizes and filters URLs.

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. Based on user identification, you can determine which scheme to assign in the access policy so that Secure Web Gateway (SWG) filters URLs appropriately.

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. It queries domain controllers and stores a mapping of IP addresses to user names in an IF-MAP server.

Note: *To identify users transparently, you must first install and configure the F5® DC 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.

single scheme

You can apply the same scheme to all users. 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

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

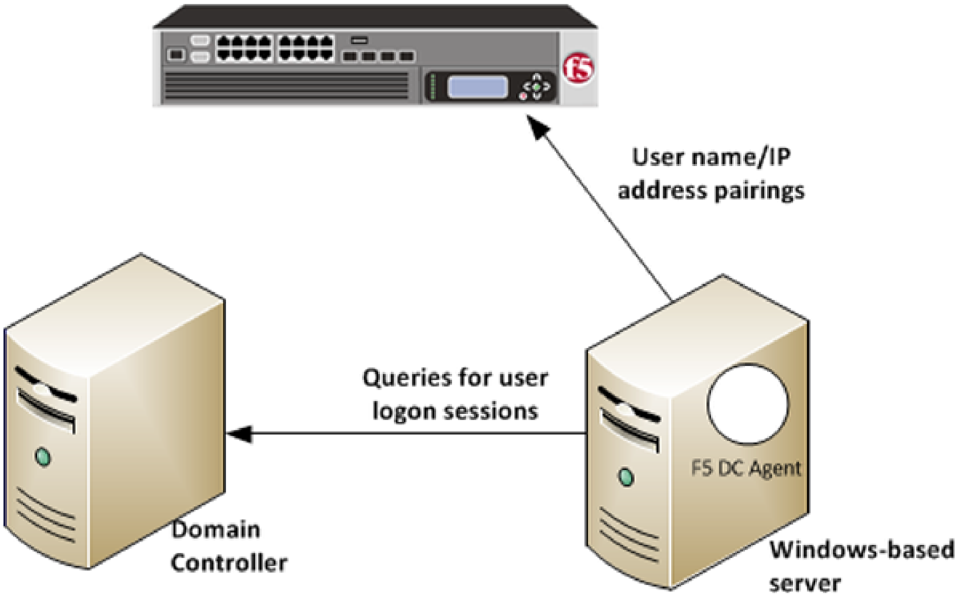
User name/IP address pairings
Queries for user logon sessions
F5 DC Agent
Domain Controller
Windows-based server

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
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**.
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.

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 Secure Web Gateway.

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.
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 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"`.)

Downloading and installing F5 DC Agent

F5® DC Agent is available when Secure Web Gateway (SWG) 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 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 **DC Agent** link.
   A `DC Agent.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 `DC Agent.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.*

   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:** 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 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\bin\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 server.
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, 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\bin\`.

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 `DC Agent.exe` file and follow the instructions to install F5 DC Agent again.

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

Error code	Error message	Possible causes
		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.
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.

Chapter 4

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.

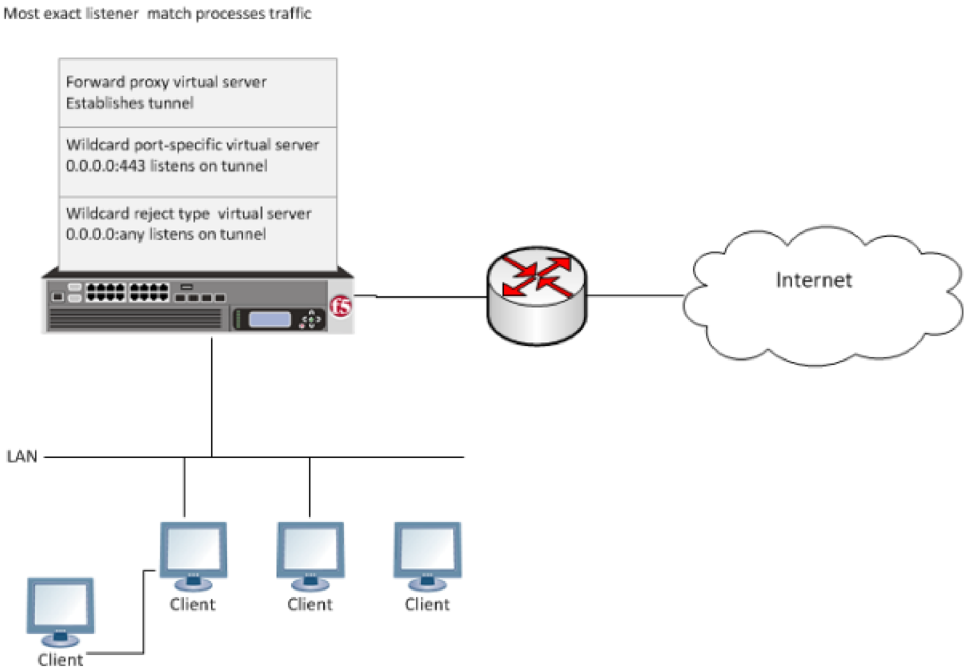
Most exact listener match processes traffic
Forward proxy virtual server
Establishes tunnel
Wildcard port-specific virtual server
0.0.0.0:443 listens on tunnel
Wildcard reject type virtual server
0.0.0.0:any listens on tunnel
Internet
LAN
Client
Client
Client
Client

Figure 3: 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.)

Before you begin

To use 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 the F5® DC 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.

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
Creating a custom Client SSL forward proxy profile
Creating a custom Server SSL profile
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 virtual server for SSL forward proxy traffic
Creating a virtual server to reject traffic

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 (or L4 ACLs that match L7 traffic, like hostname or IP-address only ACLs) work with Secure Web Gateway (SWG) explicit forward proxy.

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, type the name of the default tunnel, **http-tunnel** , or type the name of the tunnel you created previously.

   SWG requires a tunnel with tcp-forward encapsulation to support SSL traffic for explicit forward proxy.
10. Select the **Default Connect Handling** check box.

    Select this check box so that HTTP CONNECTs are allowed and consequently, SSL traffic goes through to SWG. By default, this check box is cleared and CONNECTs are blocked.
11. In the **Hostnames** field, type the name of any host that sends requests to the server that are not forward proxy requests.
12. Populate the message fields in the Explicit Proxy area as needed.

    You can include Tcl expressions, such as `[HTTP::uri]`, in the messages.
13. Click **Finished**.

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

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. From the **SSL Forward Proxy** list, select **Advanced**.
6. Select the **Custom** check box for the SSL Forward Proxy area.
7. Modify the SSL Forward Proxy settings.
   a) 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.
   b) From the **CA Certificate** list, select a certificate.
   c) From the **CA Key** list, select a key.
   d) In the **CA Passphrase** field, type a passphrase.
   e) In the **Confirm CA Passphrase** field, type the passphrase again.
   f) In the **Certificate Lifespan** field, type a lifespan for the SSL forward proxy certificate in days.
   g) (Optional) From the **Certificate Extensions** list, select **Extensions List**.
   h) (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.
   i) 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.
   j) For **Default Bypass Action**, retain the default value **Intercept**.

      You can change this setting, as well as add and update intercept and bypass lists at any time. If you set the value to **Bypass** without specifying lists, you might introduce a security risk to your system. If you set the value to **Intercept** without specifying lists, the system intercepts and examines all SSL traffic.
8. 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**.

   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 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. Type a name for the access profile.
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 the appropriate scheme for filtering URLs. 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.
   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. (Optional) To identify a user transparently, perform these substeps.

   To use transparent user identification, you must have installed and configured the F5[®] DC 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. On the associated branch, you might assign a scheme.

5. (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.

6. (Optional) To assign a scheme that categorizes and filters URLs, perform these substeps:
   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.

7. 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. For the **Destination** setting, select **Host** and in the **Address** field, type the IP address for the virtual server.
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.
11. Click **Finished**.

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

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. For the **Destination** setting, select **Network**, and type `0.0.0.0` in the **Address** field and `0.0.0.0` in the **Mask** field.
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, 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.

8. 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.

9. From the **VLAN and Tunnel Traffic** list, select **Enabled on**.
10. 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.
11. From the **Source Address Translation** list, select **Auto Map**.
12. In the Access Policy area, from the **Access Profile** list, select the access profile.
13. 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** field, type `0.0.0.0/0`.
6. For the **Destination** setting, select **Network**, and type `0.0.0.0` in the **Address** field and `0.0.0.0` in the **Mask** field.
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.

Chapter 5

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.

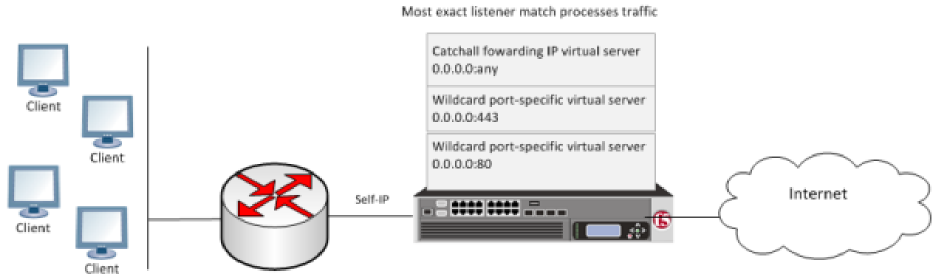
Most exact listener match processes traffic
Catchall fowarding IP virtual server 0.0.0.0:any
Wildcard port-specific virtual server 0.0.0.0:443
Wildcard port-specific virtual server 0.0.0.0:80
Client
Client
Client
Client
Self-IP
Internet

Figure 4: 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.*

Before you begin

To use 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 the F5® DC 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.

Task Summary

Creating a VLAN for transparent forward proxy
Assigning a self IP address to a VLAN
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

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. Based on user identification, you can determine which scheme to assign in the access policy so that Secure Web Gateway (SWG) filters URLs appropriately.

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. It queries domain controllers and stores a mapping of IP addresses to user names in an IF-MAP server.

Note: *To identify users transparently, you must first install and configure the F5® DC 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.

single scheme

You can apply the same scheme to all users. 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, click an interface number from the **Available** list, and use the Move button to add the selected interface to the **Untagged** list. Repeat this step as necessary.
5. Click **Finished**.
   The screen refreshes, and displays the new VLAN from 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**.
   The Self IPs screen opens.
2. Click **Create**.
   The New Self IP screen opens.
3. In the **Name** field, type a unique name for the self IP.
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 network mask for the specified IP address.
6. From the **VLAN/Tunnel** list, select the VLAN.
7. Click **Finished**.
   The screen refreshes, and displays the new self IP address.

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. Type a name for the access profile.
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 a scheme for filtering URLs. 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.
   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
3. (Optional) 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. (Optional) To identify a user transparently, perform these substeps.

   To use transparent user identification, you must have installed and configured the F5® DC 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. On the associated branch, you might assign a scheme.
5. (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.
6. (Optional) To assign a scheme that categorizes and filters URLs, perform these substeps:
   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.
7. 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. From the **SSL Forward Proxy** list, select **Advanced**.
6. Select the **Custom** check box for the SSL Forward Proxy area.
7. Modify the SSL Forward Proxy settings.
   a) 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.
   b) From the **CA Certificate** list, select a certificate.
   c) From the **CA Key** list, select a key.
   d) In the **CA Passphrase** field, type a passphrase.
   e) In the **Confirm CA Passphrase** field, type the passphrase again.
   f) In the **Certificate Lifespan** field, type a lifespan for the SSL forward proxy certificate in days.
   g) (Optional) From the **Certificate Extensions** list, select **Extensions List**.
   h) (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.
   i) 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.
   j) For **Default Bypass Action**, retain the default value **Intercept**.

      You can change this setting, as well as add and update intercept and bypass lists at any time. If you set the value to **Bypass** without specifying lists, you might introduce a security risk to your system. If you set the value to **Intercept** without specifying lists, the system intercepts and examines all SSL traffic.
8. 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**.

   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. For the **Destination** setting, select **Network**, and type `0.0.0.0` in the **Address** field and `0.0.0.0` in the **Mask** field.
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, 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.
8. 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.

9. For the **VLAN and Tunnel Traffic** setting, retain the default value **All VLANs and Tunnels** list.
10. From the **Source Address Translation** list, select **Auto Map**.
11. 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.
12. 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. For the **Destination** setting, select **Network**, and type `0.0.0.0` in the **Address** field and `0.0.0.0` in the **Mask** field.
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.
10. 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** field, type `0.0.0.0/0`.
6. For the **Destination** setting, select **Network**, and type `0.0.0.0` in the **Address** field and `0.0.0.0` in the **Mask** field.
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. For the **Destination** setting, select **Host** and in the **Address** field, type the IP address for the virtual server.
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. Click **Finished**.

The HTTPS 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.

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.

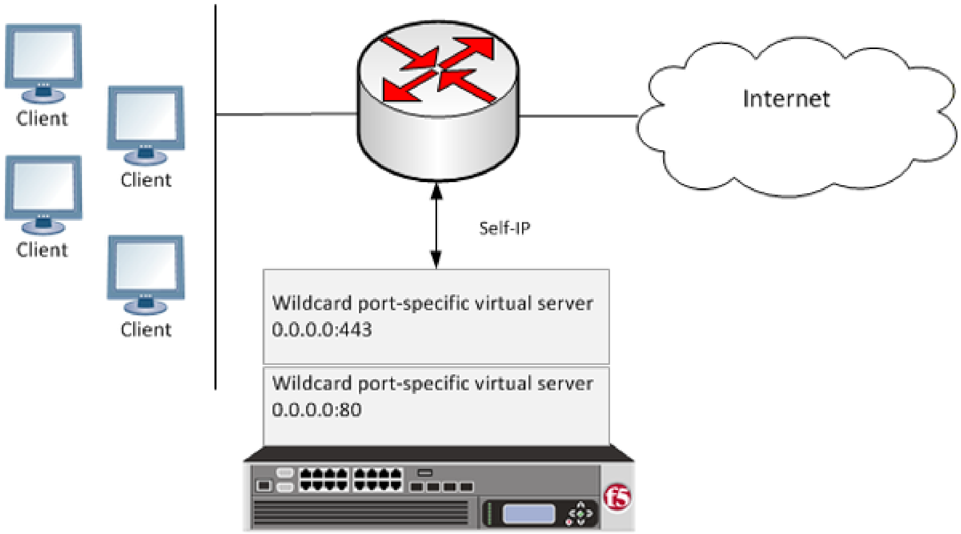
Client
Client
Client
Client
Internet
Self-IP
Wildcard port-specific virtual server
0.0.0.0:443
Wildcard port-specific virtual server
0.0.0.0:80

Figure 5: 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.*

Before you begin

To use 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 the F5® DC 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.

Task Summary

Creating a VLAN for transparent forward proxy
Assigning a self IP address to a VLAN
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

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. Based on user identification, you can determine which scheme to assign in the access policy so that Secure Web Gateway (SWG) filters URLs appropriately.

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. It queries domain controllers and stores a mapping of IP addresses to user names in an IF-MAP server.

***Note:** To identify users transparently, you must first install and configure the F5® DC 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.

single scheme

You can apply the same scheme to all users. 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, click an interface number from the **Available** list, and use the Move button to add the selected interface to the **Untagged** list. Repeat this step as necessary.
5. Click **Finished**.
   The screen refreshes, and displays the new VLAN from 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**.
   The Self IPs screen opens.
2. Click **Create**.
   The New Self IP screen opens.
3. In the **Name** field, type a unique name for the self IP.
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 network mask for the specified IP address.
6. From the **VLAN/Tunnel** list, select the VLAN.
7. Click **Finished**.
   The screen refreshes, and displays the new self IP address.

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. Type a name for the access profile.
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 a scheme for filtering URLs. 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.
   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
3. (Optional) 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. (Optional) To identify a user transparently, perform these substeps.

   To use transparent user identification, you must have installed and configured the F5® DC 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. On the associated branch, you might assign a scheme.

5. (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.

6. (Optional) To assign a scheme that categorizes and filters URLs, perform these substeps:
   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.

7. 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. From the **SSL Forward Proxy** list, select **Advanced**.
6. Select the **Custom** check box for the SSL Forward Proxy area.
7. Modify the SSL Forward Proxy settings.
   a) 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.

   b) From the **CA Certificate** list, select a certificate.
   c) From the **CA Key** list, select a key.
   d) In the **CA Passphrase** field, type a passphrase.
   e) In the **Confirm CA Passphrase** field, type the passphrase again.

f) In the **Certificate Lifespan** field, type a lifespan for the SSL forward proxy certificate in days.

g) (Optional) From the **Certificate Extensions** list, select **Extensions List**.

h) (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.

i) 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.

j) For **Default Bypass Action**, retain the default value **Intercept**.

   You can change this setting, as well as add and update intercept and bypass lists at any time. If you set the value to **Bypass** without specifying lists, you might introduce a security risk to your system. If you set the value to **Intercept** without specifying lists, the system intercepts and examines all SSL traffic.

8. 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**.

   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. For the **Destination** setting, select **Network**, and type `0.0.0.0` in the **Address** field and `0.0.0.0` in the **Mask** field.
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, 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.

8. 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.

9. For the **VLAN and Tunnel Traffic** setting, retain the default value **All VLANs and Tunnels** list.
10. From the **Source Address Translation** list, select **Auto Map**.
11. 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.
12. 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. For the **Destination** setting, select **Network**, and type `0.0.0.0` in the **Address** field and `0.0.0.0` in the **Mask** field.
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.
10. 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. For the **Destination** setting, select **Host** and in the **Address** field, type the IP address for the virtual server.
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. Click **Finished**.

The HTTPS 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.

Chapter 6

SSL Forward Proxy Bypass

Overview: Configuring exceptions to SSL forward proxy

With BIG-IP® Access Policy Manager®system Secure Web Gateway (SWG), you can create a configuration that enforces your organization's rightful use and compliance policy for Internet access. Users that access the Internet from the enterprise go through SWG forward proxy that allows or blocks access to certain categories of URL. When necessary, for example when a URL is not already categorized, SWG analyzes the content in the request or the response to determine whether it represents a threat and to block access if needed.

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 banking, financial, or government sites.

SSL forward proxy bypass

You enable SSL forward proxy bypass in the client SSL profile. When enabled, SSL forward proxy bypass includes a default action (intercept or bypass) and these lists which you can specify at your option:

- **Destination IP Intercept**
- **Destination IP Bypass**
- **Source IP Intercept**
- **Source IP Bypass**
- **Hostname Intercept**
- **Hostname Bypass**

SSL forward proxy bypass takes the first match found and intercepts a URL if it is found on an intercept list or bypasses a URL if it is found on a bypass list. If no match exists, SSL forward proxy bypass applies the default action to the URL.

The order in which SSL forward proxy bypass searches lists for a matching IP address or hostname depends on whether the default action is intercept or bypass:

Intercept	Bypass
Destination IP Intercept	Destination IP Bypass
Destination IP Bypass	Destination IP Intercept
Source IP Intercept	Source IP Bypass
Source IP Bypass	Source IP Intercept
Hostname Intercept	Hostname Bypass
Hostname Bypass	Hostname Intercept

Note: *When searching for a match in a hostname list, SSL forward proxy bypass first tries to match the Subject Alternative Name (SAN), then the Common Name (CN), and lastly, the Server Name Indication (SNI).*

Task summary

Before you start these tasks, you should have created an SWG explicit or transparent forward proxy configuration that you want to enhance with the addition of SSL forward proxy bypass. To configure SSL forward proxy bypass, first you should determine your strategy, and then configure any lists that you need to implement it.

Task list

Creating a list of IP addresses
Creating a list of hostnames
Configuring a client SSL profile for forward proxy bypass
Enabling SSL forward proxy bypass in a server SSL profile

Creating a list of IP addresses

You create an address data group to specify destination IP addresses or source IP addresses for SSL traffic that you want to be intercepted or to be bypassed by SSL forward proxy bypass.

1. On the Main tab, click **Local Traffic** > **iRules** > **Data Group List**.
   The Data Group List screen opens, displaying a list of data groups on the system.
2. Click **Create**.
   The New Data Group screen opens.
3. In the **Name** field, type a unique name for the data group.
4. From **Type** field, select **Address**.
   A Records area displays.
5. In the Records area, add each IP address that you want to include in the data group:
   a) For the **Type** setting, select **Host** or **Network**.

      To enter a subnet IP address, select **Network**.
   b) In the **Address** field, type an IP address for the host or the subnet.
   c) If the address type is **Network**, type a network mask in the **Mask** field.
   d) Click **Add**.
   e) Repeat these steps for each IP address you want to include in the data group.
6. Click **Finished**.
   The new data group appears in the list of data groups.

Creating a list of hostnames

You create a string data group to specify hostnames for SSL traffic that you want to be intercepted or to be bypassed by SSL forward proxy bypass.

1. On the Main tab, click **Local Traffic** > **iRules** > **Data Group List**.
   The Data Group List screen opens, displaying a list of data groups on the system.
2. Click **Create**.
   The New Data Group screen opens.
3. In the **Name** field, type a unique name for the data group.
4. From the **Type** list, select **String**.
5. In the Records area, create entries that consist of one hostname:
   a) In the **String** field, type a hostname.

      Type any of these names for the host: the common name (CN), the Subject Alternative Name (SAN), or the Server Name Indication (SNI). FQDN and wildcard-matching are supported. The wildcard-matching algorithm matches a single wildcard and only when it is provided as the first character in the name.

If you type the string `*.example.com`, the name store.example.com matches the string, but skis.store.example.com does not match.

b) Click **Add**.

c) Repeat these steps for each host that you want to include in this data group.

6. Click **Finished**.
   The new data group appears in the list of data groups.

Configuring a client SSL profile for forward proxy bypass

You perform this task to update a client SSL profile that is already configured for SSL forward proxy. You enable SSL forward proxy bypass in cases where you need to make exceptions, such as to mitigate privacy concerns.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.
   The Client profile list screen opens.
2. Click the name of a profile.
3. In the SSL Forward Proxy area, select the **Custom** check box.
4. From the **SSL Forward Proxy Bypass** list, select **Enabled**.

   When assigned to a virtual server, a client SSL profile and a server SSL profile both must specify the same value for this setting. You cannot change this setting in either profile while assigned to a virtual server. To change the **SSL Forward Proxy Bypass** setting, you can create new profiles and add them to the virtual server, or detach the profiles from the virtual server, update them, and assign them to the virtual server again.

   Additional settings display.
5. From the **Bypass Default Action** list, select **Intercept** or **Bypass**.

   The default action applies to addresses and hostnames that do not match any entry specified in the lists that you specify. The system matches traffic first against destination IP address lists, then source IP address lists, and lastly, hostname lists. Within these, the default action also specifies whether to search the intercept list or the bypass list first.

   ***Note:** If you select **Bypass** and do not specify any additional settings, you introduce a security risk to your system.*
6. Select a data group for any of these settings that you want to apply:
   a) From the **Destination IP Intercept** list, select a data group that specifies destination IP addresses to intercept.
   b) From the **Destination IP Bypass** list, select a data group that specifies destination IP addresses to bypass.
   c) From the **Source IP Intercept** list, select a data group that specifies source IP addresses to intercept.
   d) From the **Source IP Bypass** list, select a data group that specifies source IP addresses to bypass.
   e) From the **Hostname Intercept** list, select a data group that specifies hostnames to intercept.
   f) From the **Hostname Bypass** list, select a data group that specifies hostnames to bypass.
7. Click **Finished**.

The custom Client SSL forward proxy profile now supports forward proxy bypass.

You must also enable SSL forward proxy bypass on the server SSL profile.

Enabling SSL forward proxy bypass in a server SSL profile

You perform this task to update a server SSL profile that is already configured for SSL forward proxy. You must enable SSL forward proxy bypass in a server SSL profile when SSL forward proxy bypass is enabled in the corresponding client SSL profile in your configuration.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Server**.
   The SSL Server profile list screen opens.
2. Click the name of a profile.
3. Select the **Custom** check box for the SSL Forward Proxy area.
4. From the **SSL Forward Proxy Bypass** list, select **Enabled**.

   When assigned to a virtual server, a client SSL profile and a server SSL profile both must specify the same value for this setting. You cannot change this setting in either profile while assigned to a virtual server. To change the **SSL Forward Proxy Bypass** setting, you can create new profiles and add them to the virtual server, or detach the profiles from the virtual server, update them, and assign them to the virtual server again.

   Additional settings display.
5. Click **Finished**.

The custom server SSL forward proxy profile now supports SSL forward proxy bypass.

Chapter 7

Reports, Logs, and Statistics

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 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.*

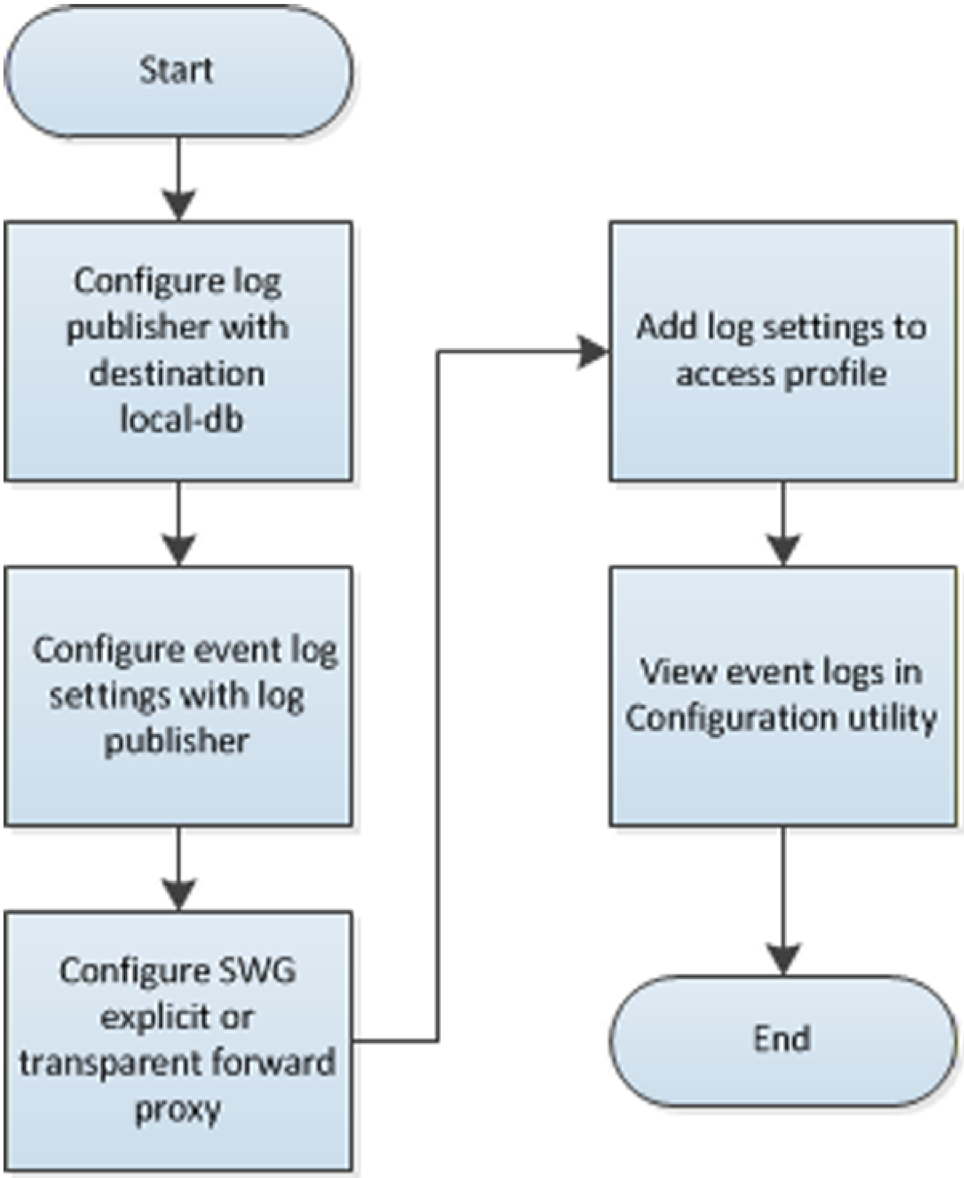
Start
Configure log publisher with destination local-db
Configure event log settings with log publisher
Configure SWG explicit or transparent forward proxy
Add log settings to access profile
View event logs in Configuration utility
End

Figure 6: 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:

Client IP address
IP address from which the request for the URL originated.

URL 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.

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
Exporting or emailing Secure Web Gateway statistics

Creating an SMTP server configuration

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.

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

Option	Action
	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.

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 to create in implementation	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.
Virtual server	In a SWG configuration, an access profile is associated with the virtual server that handles the forward proxy traffic.

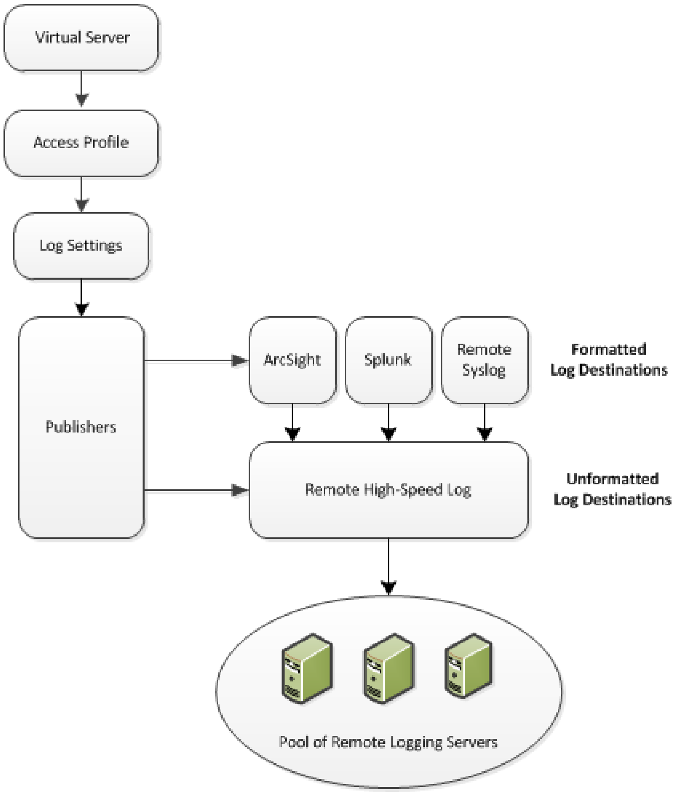

Figure 7: Association of remote high-speed logging configuration objects

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 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.
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.
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, 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 8

Kerberos Authentication and SWG

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.

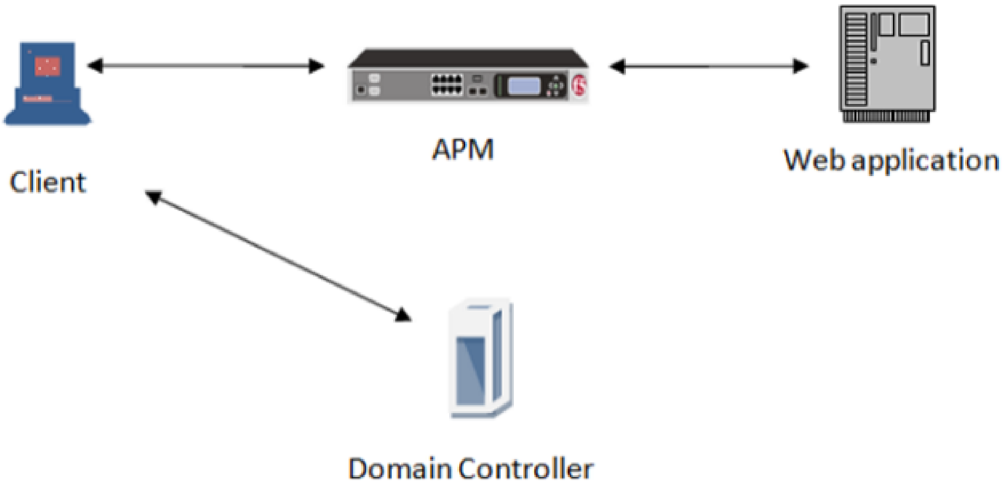

Figure 8: How SPNEGO/Kerberos end-user login works

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 9

NTLM Authentication and SWG

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