BIG-IP® Access Policy Manager®: Network Access

Version 11.6

Table of Contents

Legal Notices

Publication Date

This document was published on August 20, 2014.

Publication Number

MAN-0362-07

Copyright

Trademarks

Patents

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

Export Regulation Notice

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

RF Interference Warning

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

FCC Compliance

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

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

Canadian Regulatory Compliance

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

Standards Compliance

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

Acknowledgments

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

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

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

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

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

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

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

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

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

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

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

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

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

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

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

This product includes software developed by Christos Zoulas.

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

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

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

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

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

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

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

This product includes software developed by Jared Minch.

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

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

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

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

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

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

This product includes Hypersonic SQL.

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

This product includes software developed by the Internet Software Consortium.

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

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

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

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

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

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

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

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

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).

This product includes jxrlib software, copyright ©2009 Microsoft Corp. All rights reserved. Distributed under the new BSD license.

This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/).

This product includes libmagic software, copyright © Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995. Software written by Ian F. Darwin and others; maintained 1994- Christos Zoulas.

This product contains OpenLDAP software, which is distributed under the OpenLDAP v2.8 license (BSD3-like).

Chapter 1

About Network Access

What is network access?

The BIG-IP® Access Policy Manager® network access feature provides secure access to corporate applications and data using a standard web browser, or the BIG-IP Edge Client®. Using network access, employees, partners, and customers can have access to corporate resources securely, from any location.

The network access feature provides users with the functionality of a traditional IPsec VPN client. Unlike IPsec, however, network access does not require any pre-installed software or configuration on the remote user's computer. It is also more robust than IPsec VPN against router and firewall incompatibilities.

Network access features

Network access provides connections with the following features.

Full access from any client
Provides Windows®, Macintosh®, Linux®, and Windows Mobile users with access to the complete set of IP-based applications, network resources, and intranet files available, as if they were physically working on the office network.

Split tunneling of traffic
Provides control over exactly what traffic is sent over the network access connection to the internal network, and what is not. This feature provides better client application performance by allowing connections to the public Internet to go directly to their destinations, rather than being routed over the tunnel and then out to the public Internet.

Client checking
Detects operating system and browser versions, antivirus and firewall software, registry settings, and processes, and checks files during the login process to insure that the client configuration meets the organization's security policy for remote access.

Compression of transferred data
Compresses traffic with GZIP before it is encrypted, reducing the number of bytes transferred between the Access Policy Manager and the client system and improving performance.

Routing table monitoring
Monitors changes made in the client's IP routing table during a network access connection. You can configure this feature to stop the connection if the routing table changes, helping prevent possible information leaks. This feature applies to Windows clients only.

Session inactivity detection
Closes network access connections after a period below an inactivity threshold that you can configure. This feature helps prevent security breaches.

Automatic application start
Starts a client application automatically after establishing the network access connection. This feature simplifies user access to specific applications or sites.

Automatic drive mapping
Connects the user to a specific drive on the intranet. This feature simplifies user access to files.

Note: *This feature is available only for Windows clients.*

Connection-based ACLs
Filters network traffic by controlling whether packets are allowed, discarded, or rejected, based on specific criteria. For example, connections can be filtered by Layer 4 properties like source and destination IP address and port, protocol (TCP or UDP), and Layer 7 properties like scheme, host name, and paths. ACLs also support auditing capabilities with logging. ACLs allow groups of users or access policy users to have access to full client-server application support without opening up the entire network to each user.

Dynamic IP address assignment
Assigns client endpoint IP addresses dynamically from a configured pool of addresses. IP addresses can also be assigned with an external AAA server attribute.

Traffic classification, prioritization, and marking
Provides the ability to classify and prioritize traffic to ensure levels of service to users with defined characteristics.

About network access traffic

Network access implements a point-to-point network connection over SSL, which provides a secure solution that works well with firewalls and proxy servers.

Network access settings specify IP address pools, which the Access Policy Manager® then uses to assign IP addresses to a client computer's virtual network adapter. When an end user opens the address of the Access Policy Manager in a web browser, the browser starts an SSL connection to the Access Policy Manager. The user can then log in to the Access Policy Manager.

Network access connection diagram

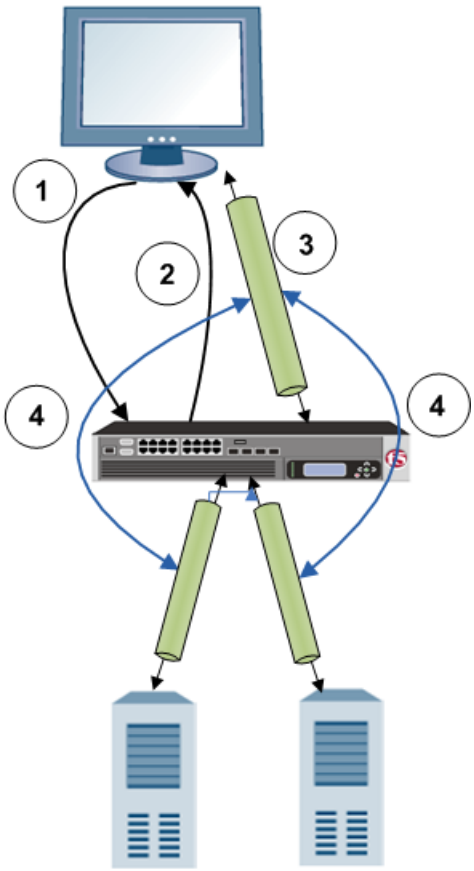
The process flow of a network access connection is depicted in this diagram.

1 The user starts a 443 SSL session with the Access Policy Manager, and logs on.

2 The Access Policy Manager downloads and installs the ActiveX control or browser plugin to the client.

3 The ActiveX control or browser plugin establishes an encrypted network access tunnel with the Access Policy Manager.

4 The user connects to internal servers over the Network Access connection, as if the client is located directly on the internal network.



Network access configuration elements

A network access configuration requires:

- A network access resource
- An access profile, with an access policy that assigns:
  - A network access resource
  - A network access or full webtop
- A lease pool that provides internal network addresses for tunnel clients
- A connectivity profile
- A virtual server that assigns the access profile

Network access elements are summarized in the following diagram.

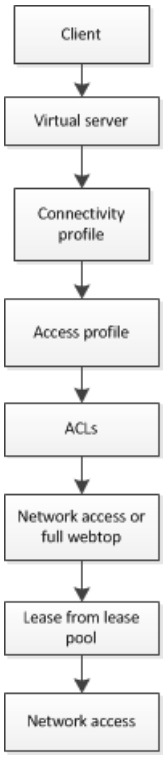


Figure 1: Network access elements

Chapter 2

Configuring Network Access Resources

Creating a network access resource

You configure a network access resource to allow users access to your local network through a secure VPN tunnel.

1. On the Main tab, click **Access Policy** > **Network Access**.
   The Network Access List screen opens.
2. Click the **Create** button.
   The New Resource screen opens.
3. In the **Name** field, type a name for the resource.
4. Type an optional description for the network access resource.
5. For the **Auto launch** setting, only select the **Enable** check box if you want to automatically start this network access resource when the user reaches a full webtop.

   When assigning network access resources to a full webtop, only one network access resource can have auto launch enabled.
6. Click **Finished** to save the network access resource.

The General Properties screen for the network access resource opens.

Configuring properties for a network access resource

You must create a network access resource, or open an existing resource, before you can perform this task.

You can configure the description of a network access resource with network access properties.

1. On the Main tab, click **Access Policy** > **Network Access**.
   The Network Access Resource List screen opens.
2. Click the name to select a network access resource on the Resource List.
   The Network Access editing screen opens.
3. To configure the general properties for the network resource, click **Properties** on the menu bar.
4. Click the **Update** button.
   Your changes are saved and the page refreshes.

Network access resource properties

Use these general properties to update settings for the network access resource.

Property setting	Value	Description
Name	A text string. Avoid using global reserved words in the name, such as all, delete, disable, enable, help, list, none, or show.	Name for the network access resource.
Partition	Typically, **Common**.	Partition under which the network access resource is created. You cannot change this value.
Description	Text.	Text description of the network access resource.

Property setting	Value	Description
Auto launch	**Enable** or **Disable**.	The network access resource starts automatically when the user reaches the full webtop, if this option is enabled. ***Note:*** *When assigning network access resources to a full webtop, only one network access resource can have auto launch enabled.*

Configuring network settings for a network access resource

You must create a network access resource, or open an existing resource, before you can perform this task.

You can use network settings to specify a lease pool for network access clients, and also to configure traffic options, client behavior, DTLS settings, and set up proxy behavior.

1. On the Main tab, click **Access Policy** > **Network Access** > **Network Access List**.
   The Network Access List screen opens.
2. Click the name to select a network access resource on the Resource List.
   The Network Access editing screen opens.
3. To configure the network settings for the network access resource, click **Network Settings** on the menu bar.
4. Click the **Update** button.
   Your changes are saved and the page refreshes.

Proxy ARP considerations

To configure proxy ARP, you must be aware of the following conditions.

- Proxy ARP is not compatible with SNAT pools. You must disable SNAT Automap or a specific SNAT pool to use proxy ARP.
- If you enable split tunneling, you must configure an entry for the server LAN segment in the **LAN Address Space** setting. You must also configure the LAN address spaces for any clients that will send traffic to each other.
- In a high availability configuration, both BIG-IP® systems must have interfaces on the same server LAN segment.
- IP addresses that you reserve for tunnel clients cannot be used for self IPs, NATs, SNATs, or wildcard (port-0) virtual servers.

Network settings for a network access resource

Network settings specify tunnel settings, session settings, and client settings.

Setting	Value	Description
Network Tunnel	Enable	When you enable a network tunnel, you configure the network access tunnel to provide network access. Clear the **Enable** option to hide all network settings and to disable the tunnel.

Setting	Value	Description
Supported IP Version	**IPV4** or **IPV4&IPV6**	Sets the Network Access tunnel to support either an IPv4 lease pool, or both IPv4 and IPv6 lease pools. ***Important:*** *Network access with IPv6 alone is not supported. An IPv6 tunnel requires a simultaneous IPv4 tunnel, which is automatically established when you assign IPv4 and IPv6 lease pools, and set the version to* ***IPv4&IPv6****.*
General Settings	Basic/Advanced	Select **Advanced** to show settings for Proxy ARP, SNAT Pool, and Session Update.
IPv4 Lease Pool	List selection of existing IPv4 lease pools	Assigns internal IP addresses to remote network access clients, using configured lease pools. Select a lease pool from the drop-down list. To create a lease pool within this screen, click the + sign next to **Lease Pool**.
IPv6 Lease Pool	List selection of existing IPv6 lease pools	Assigns internal IP addresses to remote network access clients, using configured lease pools. Select a lease pool from the drop-down list. To create a lease pool within this screen, click the + sign next to **Lease Pool**.
Compression	**No Compression/GZIP Compression**	Select GZIP Compression to compress all traffic between the Network Access client and the Access Policy Manager®, using the GZIP deflate method.
Proxy ARP	Enable	Proxy ARP allows remote clients to use IP addresses from the LAN IP subnet, and no configuration changes are required on other devices such as routers, hosts, or firewalls. IP address ranges on the LAN subnet are configured in a lease pool and assigned to network access tunnel clients. When this setting is enabled, a host on the LAN that sends an ARP query for a client address gets a response from Access Policy Manager with its own MAC address. Traffic is sent to the Access Policy Manager and forwarded to clients over network access tunnels.
SNAT Pool	List selection of **None**, **Auto Map**, or SNAT pool name	Specifies the name of a SNAT pool used for implementing selective and intelligent SNATs. The default is **Auto Map**. If you have defined a SNAT on the system, that SNAT is available as an option on this list. The following two options are always available. • **None** specifies that the system uses no SNAT pool for this network resource. • **Auto Map** specifies that the system uses all of the self IP addresses as the translation addresses for the pool. ***Note:*** *To support CIFS/SMB and VoIP protocols, select* ***None*** *and configure routable IP addresses in the lease pool*
Session Update Threshold	Integer (bytes per second)	Defines the average byte rate that either ingress or egress tunnel traffic must exceed, in order for the tunnel to update a session. If the average byte rate falls below the specified threshold, the system applies the inactivity timeout, which is defined in the Access Profile, to the session.

Setting	Value	Description
Session Update Window	Integer (seconds)	Defines the time value in seconds that the system uses to calculate the EMA (Exponential Moving Average) byte rate of ingress and egress tunnel traffic.
Client Settings	Basic/Advanced	Select **Advanced** to configure client proxy, DTLS, domain reconnect settings, and client certificate options.
Force all traffic through tunnel	Enable/disable	Specifies that all traffic (including traffic to or from the local subnet) is forced over the VPN tunnel.
Use split tunneling for traffic	Enable/disable	Specifies that only the traffic targeted to a specified address space is sent over the network access tunnel. With split tunneling, all other traffic bypasses the tunnel. By default, split tunneling is not enabled. When split tunneling is enabled, all traffic passing over the network access connection uses this setting.
IPV4 LAN Address Space	IPv4 IP address, IP address and network mask	Provides a list of addresses or address/mask pairs describing the target LAN. When using split tunneling, only the traffic to these addresses and network segments goes through the tunnel configured for Network Access. You can add multiple address spaces to the list, one at a time. For each address space, type the IP address and the network mask and click **Add**.
IPV6 LAN Address Space	IPv6 IP address, IP address and network mask	Provides a list of IPv6 addresses or address/mask pairs describing the target LAN. When using split tunneling, only the traffic to these addresses and network segments goes through the tunnel configured for Network Access. You can add multiple address spaces to the list, one at a time. For each address space, type the IP address and the network mask and click **Add**. This list appears only when you select **IPV4&IPV6** in the **Supported IP Version** setting.
DNS Address Space	domain names, with or without wildcards	Provides a list of domain names describing the target LAN DNS addresses. This field only appears if you use split tunneling. You can add multiple address spaces to the list, one at a time. For each address space, type the domain name, in the form `site.siterequest.com` or `*.siterequest.com`, and click **Add**.
Exclude Address Space	IP address/network mask pairs	Specifies address spaces whose traffic is not forced through the tunnel. For each address space that you want to exclude, type the IP address and the network mask and click **Add**.
Allow Local Subnet	Enable/disable	Select this option to enable local subnet access and local access to any host or subnet in routes that you have specified in the client routing table. When you enable this setting, the system does not support integrated IP filtering.
Client Side Security > **Prohibit routing table changes during Network Access connection**	Enable/disable	This option closes the network access session if the client's IP routing table is modified during the session.
Client Side Security > **Integrated IP filtering engine**	Enable/disable	Select this option to protect the resource from outside traffic (traffic generated by network devices on the client's LAN),

Setting	Value	Description
		and to ensure that the resource is not leaking traffic to the client's LAN.
Client Side Security > **Allow access to local DHCP server**	Enable/disable	This option appears when the **Integrated IP filtering engine** option is enabled. This option allows the client access to connect through the IP filtering engine, to use a DHCP server local to the client to renew the client DHCP lease locally. This option is not required or available when IP filtering is not enabled, because clients can renew their leases locally. ***Important:*** *This option does not renew the DHCP lease for the IP address assigned from the network access lease pool; this applies only to the local client IP address.*
Client Traffic Classifier	List selection	Specifies a client traffic classifier to use with this network access tunnel, for Windows clients.
Client Options > **Client for Microsoft Networks**	Enable/disable	Select this option to allow the client PC to access remote resources over a VPN connection. This option is enabled by default. This allows the VPN to work like a traditional VPN, so a user can access files and printers from the remote Microsoft network.
Client Options > **File and printer sharing for Microsoft networks**	Enable/disable	Select this option to allow remote hosts to access shared resources on the client computer over the network access connection. This allows the VPN to work in reverse, and a VPN user to share file shares and printers with remote LAN users and other VPN users.
Provide client certificate on Network Access connection when requested	Enable/disable	If client certificates are required to establish an SSL connection, this option must always be enabled. However, you can disable this option if the client certificates are only requested in an SSL connection. In this case, the client is configured not to send client certificates.
Reconnect to Domain > **Synchronize with Active Directory policies on connection establishment**	Enable/disable	When enabled, this option emulates the Windows logon process for a client on an Active Directory domain. Network policies are synchronized when the connection is established, or at logoff. The following items are synchronized: • Logon scripts are started as specified in the user profile. • Drives are mapped as specified in the user profile. • Group policies are synchronized as specified in the user profile. Group Policy logon scripts are started when the connection is established, and Group Policy logoff scripts are run when the network access connection is stopped.
Reconnect to Domain > **Run logoff scripts on connection termination**	Enable/disable	This option appears when **Synchronize with Active Directory policies on connection establishment** is enabled. Enable this option if you want the system to run logoff scripts, as configured on the Active Directory domain, when the connection is stopped.
Client Interface Speed	Integer, bits per second	Specifies the maximum speed of the client interface connection, in bits per second.

Setting	Value	Description
Display connection tray icon	Enable/disable	When enabled, balloon notifications for the network access tray icon (for example, when a connection is made) are displayed. Disable this option to prevent balloon notifications.
Client Power Management	**Ignore**, **Prevent**, or **Terminate**	Specifies how network access handles client power management settings, for example, when the user puts the system in standby, or closes the lid on a laptop. • **Ignore** - ignores the client settings for power management. • **Prevent** - prevents power management events from occurring when the client is enabled. • **Terminate** - terminates the client when a power management event occurs.
DTLS	Enable/disable	Specifies, when enabled, that the network access connection uses Datagram Transport Level Security (DTLS). DTLS uses UDP instead of TCP, to provides better throughput for high-demand applications like VoIP or streaming video, especially with lossy connections.
DTLS Port	Port number	Specifies the port number that the network access resource uses for secure UDP traffic with DTLS. The default is `4433`.
Client Proxy Settings	Enable/disable	When selected, provides configuration settings for client proxy connections for this network access resource. This option requires the client computer to have Internet Explorer 5.0 or later installed. These options are available only when using the Advanced setting, when you select the Client proxy settings option.
Client Proxy Uses HTTP for Proxy Autoconfig Script	Enable/disable	Some applications, like Citrix® MetaFrame, can not use the client proxy autoconfig script when the browser attempts to use the `file://` prefix to locate it. Select this option to specify that the browser uses `http://` to locate the proxy autoconfig file, instead of `file://`.
Client Proxy Autoconfig Script	URL	The URL for a proxy auto-configuration script, if one is used with this connection.
Client Proxy Address	IP address	The IP address for the client proxy server that network access clients use to connect to the Internet.
Client Proxy Port	Port number	The port number of the proxy server that network access clients use to connect to the Internet.
Bypass Proxy For Local Addresses	Enable/disable	Select this option if you want to allow local intranet addresses to bypass the proxy server.
Client Proxy Exclusion List	IP addresses, domain names, with wildcards	Specifies the web addresses that do not need to be accessed through your proxy server. You can use wildcards to match domain and host names, or addresses. For example, `www.*.com`, `128.*`, `240.8`, `8.`, **mygroup.***, `*.*`.

Configuring DNS and hosts for a network access resource

You must create a network access resource, or open an existing resource, before you can perform this task.

You can configure DNS and hosts to configure how a user's tunnel connection resolves addresses.

1. On the Main tab, click **Access Policy** > **Network Access** > **Network Access List**.
   The Network Access List screen opens.
2. Click the name to select a network access resource on the Resource List.
   The Network Access editing screen opens.
3. To configure DNS and hosts settings for the network access resource, click **DNS/Hosts** on the menu bar.
4. Configure DNS and Hosts settings as required.
5. Click the **Update** button.
   Your changes are saved and the page refreshes.

Network access resource DNS and hosts settings

DNS and hosts settings specify lookup information for remote tunnel clients. This table describes and lists these settings and values.

Setting	Value	Description
Primary Name Server	IP address	Type the IP address of the DNS server that network access conveys to the remote access point.
Secondary Name Server	IP address	Type a second IP address for the DNS server that network access conveys to the remote access point.
Primary WINS Server	IP address	Type the IP address of the WINS server in order to communicate to the remote access point. This address is needed for Microsoft Networking to function properly.
Secondary WINS Server	IP address	Type the IP address of the WINS server to be conveyed to the remote access point. This address is needed for Microsoft Networking to function properly.
DNS Default Domain Suffix	domain suffix	Type a DNS suffix to send to the client. If this field is left blank, the controller will send its own DNS suffix. For example, `siterequest.com`. ***Tip:*** *You can specify multiple default domain suffixes separated with commas.*
Register this connection's addresses in DNS	check box	If your DNS server has dynamic update enabled, select this check box to register the address of this connection in the DNS server. This check box is cleared by default.
Use this connection's DNS suffix in DNS registration	check box	If your DNS server has dynamic update enabled, select this check box to register the default domain suffix when you register the connection in the DNS server. This check box is cleared by default.

Setting	Value	Description
Enforce DNS search order	check box	When this setting is enabled, APM continuously checks the DNS order on the network interface and sets the network access-supplied entries first in the list if they change during a session. To use your local DNS settings as primary and the network access-supplied DNS settings as secondary, clear this setting. This might be useful when split tunneling is in use and a client connects remotely. This check box is selected by default.
Static Hosts	host name/IP address pairs	To add host and IP addresses manually to a connection-specific hosts file, type the **Host Name** and the **IP Address** for that host in the provided fields, and click **Add**.

Mapping drives for a network access resource

You must create a network access resource, or open an existing resource, before you can perform this task.

Use drive mappings to map network locations to drive letters on Windows®-based client systems.

1. On the Main tab, click **Access Policy** > **Network Access** > **Network Access List**.
   The Network Access List screen opens.
2. Click the name to select a network access resource on the Resource List.
   The Network Access editing screen opens.
3. To configure the drive mappings for the network access resource, click **Drive Mappings** on the menu bar.
4. Click **Add** to add a new drive mapping.
5. Type the **Path**, select the **Drive** letter, and type an optional **Description** for the drive mapping.
6. Click **Finished**.
   The drive mapping is added to the network access resource.

Network access resource drive mapping settings

The table lists the drive mapping settings for a network access resource.

Setting	Value	Description
Path	A network path, for example `\\networkdrive\users`	Specifies the path to the server network location.
Drive	Drive letter, list selection	Specifies the drive used. **Drive** is set to `D:` by default. Drive mapping is supported for Windows-based clients only.
Description	Text	An optional description of the drive mapping.

Launching applications on a network access connection

You must create a network access resource, or open an existing resource, before you can perform this task.

Use application launching to start applications on network access clients after the tunnel is established.

1. On the Main tab, click **Access Policy** > **Network Access** > **Network Access List**.
   The Network Access List screen opens.
2. Click the name to select a network access resource on the Resource List.
   The Network Access editing screen opens.
3. To configure applications to start for clients that establish a network access connection with this resource, click **Launch Applications** on the menu bar.
4. Click **Add** to add a new application.
5. Type the **Application Path**, type any required **Parameters** letter, and select the **Operating System**.
6. Click **Finished**.
   The application start configuration is added to the Launch Applications list, and the applications appropriate to the client operating system start when a client establishes a tunnel connection.

Network access launch applications settings

Specify launch application settings to control how applications are launched when the network access connection starts.

Setting	Value	Description
Display warning before launching applications	Enable or disable	If you enable this setting, the system displays security warnings before starting applications from network access, regardless of whether the site is considered a Trusted site. If the check box is not selected, the system displays security warnings if the site is not in the Trusted Sites list.
Application Path	An application path	Specifies the path to the application. You can type special application paths here: • `reconnect_to_domain` - Type this application path to specify that the client reconnects to the domain after the network access tunnel starts. Use this if, for example, the network access tunnel is established before the domain controller logon occurs. • `/gpo_logoff_scripts` - Type this in the application path field to run group policy object (GPO) logoff scripts on the client when the network access tunnel is stopped.
Parameters	Text	Parameters that govern the application launch.
Operating System	List selection	From the list, select whether the application launch configuration applies to Windows-based, Unix-based, Macintosh-based, or iOS clients.

About APM ACLs

APM® access control lists (ACLs) restrict user access to host and port combinations that are specified in access control entries (ACEs). An ACE can apply to Layer 4 (the protocol layer), Layer 7 (the application layer), or both. A Layer 4 or Layer 7 ACL is used with network access, application access, or web access connections.

Configuring an ACL

You use access control lists (ACLs) to restrict user access to host and port combinations that you specify in access control entries (ACEs).

1. On the Main tab, click **Access Policy** > **ACLs**.
   The ACLs screen opens.
2. Click **Create**.
   The New ACL screen opens.
3. In the **Name** field, type a name for the access control list.
4. From the **Type** list, select **Static**.
5. (Optional) In the **Description** field, add a description of the access control list.
6. (Optional) From the **ACL Order** list, specify the relative order in which to add the new ACL respective to other ACLs:
   - Select **After** to add the ACL after a specific ACL and select the ACL.
   - Select **Specify** and type the specific order number.
   - Select **Last** to add the ACL at the last position in the list.
7. From the **Match Case for Paths** list, select **Yes** to match case for paths, or **No** to ignore path case.
   This setting specifies whether alphabetic case is considered when matching paths in an access control entry.
8. Click the **Create** button.
   The ACL Properties screen opens.
9. In the Access Control Entries area, click **Add** to add an entry.
   For an ACL to have an effect on traffic, you must configure at least one access control entry.
   The New Access Control Entry screen appears.
10. From the **Type** list, select the layers to which the access control entry applies:
    - **L4** (Layer 4)
    - **L7** (Layer 7)
    - **L4+L7** (Layer 4 and Layer 7)
11. From the **Action** list, select the action for the access control entry:
    - **Allow** Permit the traffic.
    - **Continue** Skip checking against the remaining access control entries in this ACL and continue evaluation at the next ACL.
    - **Discard** Drop the packet silently.
    - **Reject** Drop the packet and send a TCP RST message on TCP flows or proper ICMP messages on UDP flows. Silently drop the packet on other protocols.

    Note: *If HTTP traffic matches a Layer 4 ACL, APM sends a TCP RST message. If traffic matches a Layer 7 ACL and is denied, APM sends the ACL Deny page.*

    To create a default access control list, complete this step, then skip to the last step in this procedure.
12. In the **Source IP Address** field, type the source IP address.
    This specifies the IP address to which the access control entry applies.
13. In the **Source Mask** field, type the network mask for the source IP address.
    This specifies the network mask for the source IP address to which the access control entry applies.

14. For the **Source Port** setting, select **Port** or **Port Range**.

    This setting specifies whether the access control entry applies to a single port or a range of ports.

15. In the **Port** field or the **Start Port** and **End Port** fields, specify the port or port ranges to which the access control entry applies.

    To simplify this choice, you can select from the list of common applications, to the right of the **Port** field, to add the typical port or ports for that protocol.

16. In the **Destination IP Address** field, type the IP address to which the access control entry controls access.
17. In the **Destination Mask** field, type the network mask for the destination IP address.
18. For the **Destination Ports** setting, select **Port** or **Port Range**.

    This setting specifies whether the access control entry applies to a single port or a range of ports.

19. In the **Port** field or the **Start Port** and **End Port** fields, specify the port or port ranges to which the access control entry applies.

    To simplify this choice, you can select from the list of common applications, to the right of the **Port** field, to add the typical port or ports for that protocol.

20. From the **Scheme** list, select the URI scheme for the access control entry:

    - **http**
    - **https**
    - **any**

    The scheme **any** matches either HTTP or HTTPS traffic.

21. In the **Host Name** field, type a host to which the access control entry applies.

    The **Host Name** field supports shell glob matching: you can use the asterisk wildcard (*****) to match match zero or more characters, and the question mark wildcard (?) to match a single character.

    `*.siterequest.com` matches siterequest.com with any prefix, such as www.siterequest.com, mail.siterequest.com, finance.siterequest.com, and any others with the same pattern.
    `n?t.siterequest.com` matches the hosts net.siterequest.com and not.siterequest.com, but not neet.siterequest.com, nt.siterequrest.com, or note.siterequest.com.

22. In the **Paths** field, type the path or paths to which the access control entry applies.

    You can separate multiple paths with spaces, for example, **/news /finance**. The **Paths** field supports shell glob matching. You can use the wildcard characters * and question mark (?) to represent multiple or single characters, respectively. You can also type a specific URI, for example, `/finance/content/earnings.asp`, or a specific extension, for example, `*.jsp`.

23. From the **Protocol** list, select the protocol to which the access control entry applies.
24. From the **Log** list, select the log level for this access control entry:

    - **None** Log nothing.
    - **Packet** Log the matched packet.

    When events occur at the selected log level, the server records a log message.

25. Click **Finished**.

You have configured an ACL with one access control entry. (You can configure additional entries.)

To use the ACL, assign it to a session using an Advanced Resource Assign or ACL Assign action in an access policy.

Example ACE settings: reject all connections to a network

This example access control entry (ACE) rejects all connections to a specific network at 192.168.112.0/24.

Property	Value	Notes
Source IP Address	0.0.0.0	If you leave an IP address entry blank, the result is the same as typing the address 0.0.0.0
Source Mask	0.0.0.0	
Source Ports	All Ports	
Destination IP address	192.168.112.0	
Destination Mask	255.255.255.0	
Destination Ports	All Ports	
Protocol	All Protocols	
Action	Reject	

Example ACE settings: allow SSH to a specific host

This example access control entry (ACE) allows SSH connections to the internal host at 192.168.112.9.

Property	Value	Notes
Source IP Address	0.0.0.0	If you leave an IP address entry blank, the result is the same as typing the address 0.0.0.0
Source Mask	0.0.0.0	
Source Ports	All Ports	
Destination IP address	192.168.112.9	
Destination Mask	255.255.255.0	
Destination Ports	22 (or select SSH)	
Protocol	TCP	
Action	Allow	

Example ACE settings: reject all connections to specific file types

This example access control entry (ACE) rejects all connections that attempt to open files with the extensions `doc`, `exe`, and `txt`.

Property	Value	Notes
Source IP Address	0.0.0.0	If you leave an IP address entry blank, the result is the same as typing the address 0.0.0.0
Source Mask	0.0.0.0	

Property	Value	Notes
Source Ports	All Ports	
Destination IP address	0.0.0.0	
Destination Mask	0.0.0.0	
Destination Ports	All Ports	
Scheme	http	
Paths	*.doc*.exe *.txt	
Protocol	All Protocols	
Action	Reject	

Chapter 3

Using Forward Error Correction with Network Access

Overview: Using FEC on network access tunnels

Forward error correction (FEC) is a technique for controlling data transmission errors over unreliable or noisy communication channels. With FEC, the sender encodes messages with a little extra error-correcting code. FEC enables recovery of lost packets to avoid retransmission and increase throughput on lossy links. FEC is frequently used when retransmission is not possible or is costly.

In Access Policy Manager®, you can use FEC on network access tunnels. You can do this provided that you configure a network access resource for Datagram Transport Level Security (DTLS) and configure two virtual servers with the same IP address. Users connect on a TCP/HTTPS virtual server. Another virtual server handles DTLS for the network access resource.

Note: *FEC is not included on every BIG-IP® system.*

Task summary

Creating a network access resource for DTLS
Adding a FEC profile to a connectivity profile
Configuring a webtop for network access
Creating an access profile
Adding network access to an access policy
Creating an HTTPS virtual server for network access
Configuring a virtual server for DTLS

Creating a network access resource for DTLS

You configure a network access resource to allow users access to your local network through a secure VPN tunnel. You configure the resource to use Datagram Transport Level Security (DTLS) as a prerequisite for using forward error correcting (FEC) on the connection.

1. On the Main tab, click **Access Policy** > **Network Access**.
   The Network Access List screen opens.
2. Click the **Create** button.
   The New Resource screen opens.
3. In the **Name** field, type a name for the resource.
4. Click **Finished** to save the network access resource.
5. On the menu bar, click **Network Settings**.
6. In the Enable Network Tunnel area, for **Network Tunnel**, retain the default setting **Enable**.
7. In the General Settings area from the **Supported IP Version** list, retain the default setting **IPV4**, or select **IPV4 & IPV6**.
   If you select **IPV4 & IPV6**, the **IPV4 Lease Pool** and **IPV6 Lease Pool** lists are displayed. They include existing pools of IPv4 addresses and IPv6 addresses, respectively.
8. Select the appropriate lease pools from the lists.
   APM® assigns IP addresses to a client computer's virtual network from the lease pools that you specify.
9. From the Client Settings list, select **Advanced**.
   Additional settings are displayed.
10. Select the **DTLS** check box.
    A **DTLS Port** field displays with the default port, `4433`.

11. Click **Update**.

Adding a FEC profile to a connectivity profile

You add a forward error correction (FEC) profile to a connectivity profile to apply on a network access tunnel.

Note: *A connectivity profile contains default settings for network access compression. However, compression is not active when a network access connection is configured for DTLS.*

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Select the connectivity profile that you want to update and click **Edit Profile**.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
3. From the **FEC Profile** list, select the default profile, **/Common/fec**.
   A FEC profile is a network tunnel profile. You can configure a custom FEC profile in the Network area on the BIG-IP system.
4. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.

The connectivity profile appears in the list.

To provide functionality with a connectivity profile, you must add the connectivity profile and an access profile to a virtual server.

Configuring a webtop for network access

A webtop allows your users to connect and disconnect from the network access connection.

1. On the Main tab, click **Access Policy** > **Webtops**.
   The Webtop List screen opens.
2. Click **Create** to create a new webtop.
3. Select the type of webtop to create.

Option	Description
Network Access	Select **Network Access** for a webtop to which you will assign only a single network access resource.
Portal Access	Select **Portal Access** for a webtop to which you assign only portal access resources.
Full	Select **Full** for a webtop to which you assign one or more network access resources, multiple portal access resources, and multiple application access app tunnel resources, or any combination of the three types.

The webtop is now configured, and appears in the list. You can edit the webtop further, or assign it to an access policy.

To use this webtop, it must be assigned to an access policy with an advanced resource assign action or with a webtop and links assign action.

Creating an access profile

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

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

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

4. From the **Profile Type** list, select one:
   - **LTM-APM** - Select for a web access management configuration.
   - **SSL-VPN** - Select to configure network access, portal access, or application access. (Most access policy items are available for this type.)
   - **ALL** - Select to support LTM-APM and SSL-VPN access types.
   - **SSO** - Select to configure matching virtual servers for Single Sign-On (SSO).

     Note: *No access policy is associated with this type of access profile*

   - **RDG-RAP** - Select to validate connections to hosts behind APM when APM acts as a gateway for RDP clients.
   - **SWG - Explicit** - Select to configure access using Secure Web Gateway explicit forward proxy.
   - **SWG - Transparent** - Select to configure access using Secure Web Gateway transparent forward proxy.
   - **System Authentication** - Select to configure administrator access to the BIG-IP system (when using APM as a pluggable authentication module).
   - **Identity Service** Used internally to provide identity service for a supported integration. Only APM creates this type of profile.

     Note: *You can edit Identity Service profile properties.*

   Note: *Depending on licensing, you might not see all of these profile types.*

   Additional settings display.
5. In the Language Settings area, add and remove accepted languages, and set the default language.
   A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.
6. Click **Finished**.

This creates an access profile with a default access policy.

Adding network access to an access policy

Before you assign a network access resource to an access policy, you must:

- Create a network access resource
- Create an access profile
- Define a network access webtop or a full webtop

When you assign a network access resource to an access policy branch, a user who successfully completed the branch rule (which includes that access policy item) starts a network access tunnel.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile for which you want to edit the access policy.
   The properties screen opens for the profile you want to edit.
3. On the menu bar, click **Access Policy**.
   The Access Policy screen opens.
4. Click **Edit Access Policy for Profile *profile_name***.
   The visual policy editor opens the access policy in a separate screen.
5. Click the **(+)** icon anywhere in the access policy to add a new action item.

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

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
6. Select one of the following resource assignment actions and click **Add**.

Option	Description
Resource Assign	Select the **Resource Assign** action to add a network access resource only. **Resource Assign** does not allow you to add a webtop or ACLs. If you want to add ACLs, a webtop, or webtop links after you add a Resource Assign action, you can add them with the individual actions **ACL Assign** and **Webtop and Links Assign**.
Advanced Resource Assign	Select the **Advanced Resource Assign** action to add network access resources, and optionally add a webtop, webtop links, and one or more ACLs.

7. Select the resource or resources to add.
   - If you added an **Advanced Resource Assign** action, on the Resource Assignment screen, click **Add New Entry**, then click **Add/Delete**, and select and add resources from the tabs, then click **Update**.
   - If you added a **Resource Assign** action, next to Network Access Resources, click **Add/Delete**.

   If you add a full webtop and multiple network access resources, Auto launch can be enabled for only one network access resource. (With Auto launch enabled, a network access resource starts automatically when the user reaches the webtop.)
8. Click **Save**.
9. Click **Apply Access Policy** to save your configuration.

A network access tunnel is assigned to the access policy. You may also assign a network access or full webtop. On the full webtop, users can click the Network Access link to start the network access tunnel, or one network access tunnel (that is configured with Auto launch enabled) can start automatically.

After you complete the access policy, you must define a connectivity profile. In the virtual server definition, you must select the access policy and connectivity profile.

Creating an HTTPS virtual server for network access

Create a virtual server for HTTPS traffic.

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

   This field accepts an address in CIDR format (IP address/prefix). However, when you type the complete IP address for a host, you do not need to type a prefix after the address.
5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. From the **HTTP Profile** list, select **http**.
7. If you use client SSL, for the **SSL Profile (Client)** setting, select a client SSL profile.
8. If you use server SSL, for the **SSL Profile (Server)** setting, select a server SSL profile.
9. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
10. In the Access Policy area, from the **Connectivity Profile** list, select the connectivity profile.
11. Click **Finished**.

The HTTPS virtual server displays on the list.

Configuring a virtual server for DTLS

To configure DTLS mode for a network access connection, you must configure a virtual server specifically for use with DTLS.

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

   The supported format is address/prefix, where the prefix length is in bits. For example, an IPv4 address/prefix is `10.0.0.1/32` or `10.0.0.0/24`, and an IPv6 address/prefix is `ffe1::0020/64` or `2001:ed8:77b5:2:10:10:100:42/64`.

   Note: *This is the same IP address as the TCP (HTTPS) virtual server to which your users connect.*

   ---
5. In the **Service Port** field, type the port number that you specified in the DTLS Port field in the network access resource configuration.

   By default, the DTLS port is `4433`.
6. From the **Protocol** list, select **UDP**.
7. For the **SSL Profile (Client)** setting, in the **Available** box, select a profile name, and using the Move button, move the name to the **Selected** box.
8. In the Access Policy area, from the **Connectivity Profile** list, select the connectivity profile.

Use the same connectivity profile that you specified for the TCP (HTTPS) virtual server to which your users connect.

9. Click **Finished**.

Network settings for a network access resource

Network settings specify tunnel settings, session settings, and client settings.

Setting	Value	Description
Network Tunnel	Enable	When you enable a network tunnel, you configure the network access tunnel to provide network access. Clear the **Enable** option to hide all network settings and to disable the tunnel.
Supported IP Version	**IPV4** or **IPV4&IPV6**	Sets the Network Access tunnel to support either an IPv4 lease pool, or both IPv4 and IPv6 lease pools. ***Important:*** *Network access with IPv6 alone is not supported. An IPv6 tunnel requires a simultaneous IPv4 tunnel, which is automatically established when you assign IPv4 and IPv6 lease pools, and set the version to* ***IPv4&IPv6****.*
General Settings	Basic/Advanced	Select **Advanced** to show settings for Proxy ARP, SNAT Pool, and Session Update.
IPv4 Lease Pool	List selection of existing IPv4 lease pools	Assigns internal IP addresses to remote network access clients, using configured lease pools. Select a lease pool from the drop-down list. To create a lease pool within this screen, click the + sign next to **Lease Pool**.
IPv6 Lease Pool	List selection of existing IPv6 lease pools	Assigns internal IP addresses to remote network access clients, using configured lease pools. Select a lease pool from the drop-down list. To create a lease pool within this screen, click the + sign next to **Lease Pool**.
Compression	**No Compression**/**GZIP Compression**	Select GZIP Compression to compress all traffic between the Network Access client and the Access Policy Manager®, using the GZIP deflate method.
Proxy ARP	Enable	Proxy ARP allows remote clients to use IP addresses from the LAN IP subnet, and no configuration changes are required on other devices such as routers, hosts, or firewalls. IP address ranges on the LAN subnet are configured in a lease pool and assigned to network access tunnel clients. When this setting is enabled, a host on the LAN that sends an ARP query for a client address gets a response from Access Policy Manager with its own MAC address. Traffic is sent to the Access Policy Manager and forwarded to clients over network access tunnels.
SNAT Pool	List selection of **None**, **Auto Map**, or SNAT pool name	Specifies the name of a SNAT pool used for implementing selective and intelligent SNATs. The default is **Auto Map**. If you have defined a SNAT on the system, that SNAT is available as an option on this list. The following two options are always available. • **None** specifies that the system uses no SNAT pool for this network resource.

Setting	Value	Description
		• **Auto Map** specifies that the system uses all of the self IP addresses as the translation addresses for the pool. ***Note:*** *To support CIFS/SMB and VoIP protocols, select* ***None*** *and configure routable IP addresses in the lease pool*
Session Update Threshold	Integer (bytes per second)	Defines the average byte rate that either ingress or egress tunnel traffic must exceed, in order for the tunnel to update a session. If the average byte rate falls below the specified threshold, the system applies the inactivity timeout, which is defined in the Access Profile, to the session.
Session Update Window	Integer (seconds)	Defines the time value in seconds that the system uses to calculate the EMA (Exponential Moving Average) byte rate of ingress and egress tunnel traffic.
Client Settings	Basic/Advanced	Select **Advanced** to configure client proxy, DTLS, domain reconnect settings, and client certificate options.
Force all traffic through tunnel	Enable/disable	Specifies that all traffic (including traffic to or from the local subnet) is forced over the VPN tunnel.
Use split tunneling for traffic	Enable/disable	Specifies that only the traffic targeted to a specified address space is sent over the network access tunnel. With split tunneling, all other traffic bypasses the tunnel. By default, split tunneling is not enabled. When split tunneling is enabled, all traffic passing over the network access connection uses this setting.
IPV4 LAN Address Space	IPv4 IP address, IP address and network mask	Provides a list of addresses or address/mask pairs describing the target LAN. When using split tunneling, only the traffic to these addresses and network segments goes through the tunnel configured for Network Access. You can add multiple address spaces to the list, one at a time. For each address space, type the IP address and the network mask and click **Add**.
IPV6 LAN Address Space	IPv6 IP address, IP address and network mask	Provides a list of IPv6 addresses or address/mask pairs describing the target LAN. When using split tunneling, only the traffic to these addresses and network segments goes through the tunnel configured for Network Access. You can add multiple address spaces to the list, one at a time. For each address space, type the IP address and the network mask and click **Add**. This list appears only when you select **IPV4&IPV6** in the **Supported IP Version** setting.
DNS Address Space	domain names, with or without wildcards	Provides a list of domain names describing the target LAN DNS addresses. This field only appears if you use split tunneling. You can add multiple address spaces to the list, one at a time. For each address space, type the domain name, in the form `site.siterequest.com` or `*.siterequest.com`, and click **Add**.
Exclude Address Space	IP address/network mask pairs	Specifies address spaces whose traffic is not forced through the tunnel. For each address space that you want to exclude, type the IP address and the network mask and click **Add**.
Allow Local Subnet	Enable/disable	Select this option to enable local subnet access and local access to any host or subnet in routes that you have specified

Setting	Value	Description
		in the client routing table. When you enable this setting, the system does not support integrated IP filtering.
Client Side Security > **Prohibit routing table changes during Network Access connection**	Enable/disable	This option closes the network access session if the client's IP routing table is modified during the session.
Client Side Security > **Integrated IP filtering engine**	Enable/disable	Select this option to protect the resource from outside traffic (traffic generated by network devices on the client's LAN), and to ensure that the resource is not leaking traffic to the client's LAN.
Client Side Security > **Allow access to local DHCP server**	Enable/disable	This option appears when the **Integrated IP filtering engine** option is enabled. This option allows the client access to connect through the IP filtering engine, to use a DHCP server local to the client to renew the client DHCP lease locally. This option is not required or available when IP filtering is not enabled, because clients can renew their leases locally. ***Important:*** *This option does not renew the DHCP lease for the IP address assigned from the network access lease pool; this applies only to the local client IP address.*
Client Traffic Classifier	List selection	Specifies a client traffic classifier to use with this network access tunnel, for Windows clients.
Client Options > **Client for Microsoft Networks**	Enable/disable	Select this option to allow the client PC to access remote resources over a VPN connection. This option is enabled by default. This allows the VPN to work like a traditional VPN, so a user can access files and printers from the remote Microsoft network.
Client Options > **File and printer sharing for Microsoft networks**	Enable/disable	Select this option to allow remote hosts to access shared resources on the client computer over the network access connection. This allows the VPN to work in reverse, and a VPN user to share file shares and printers with remote LAN users and other VPN users.
Provide client certificate on Network Access connection when requested	Enable/disable	If client certificates are required to establish an SSL connection, this option must always be enabled. However, you can disable this option if the client certificates are only requested in an SSL connection. In this case, the client is configured not to send client certificates.
Reconnect to Domain > **Synchronize with Active Directory policies on connection establishment**	Enable/disable	When enabled, this option emulates the Windows logon process for a client on an Active Directory domain. Network policies are synchronized when the connection is established, or at logoff. The following items are synchronized: • Logon scripts are started as specified in the user profile. • Drives are mapped as specified in the user profile. • Group policies are synchronized as specified in the user profile. Group Policy logon scripts are started when the connection is established, and Group Policy logoff scripts are run when the network access connection is stopped.

Setting	Value	Description
Reconnect to Domain > **Run logoff scripts on connection termination**	Enable/disable	This option appears when **Synchronize with Active Directory policies on connection establishment** is enabled. Enable this option if you want the system to run logoff scripts, as configured on the Active Directory domain, when the connection is stopped.
Client Interface Speed	Integer, bits per second	Specifies the maximum speed of the client interface connection, in bits per second.
Display connection tray icon	Enable/disable	When enabled, balloon notifications for the network access tray icon (for example, when a connection is made) are displayed. Disable this option to prevent balloon notifications.
Client Power Management	**Ignore**, **Prevent**, or **Terminate**	Specifies how network access handles client power management settings, for example, when the user puts the system in standby, or closes the lid on a laptop. • **Ignore** - ignores the client settings for power management. • **Prevent** - prevents power management events from occurring when the client is enabled. • **Terminate** - terminates the client when a power management event occurs.
DTLS	Enable/disable	Specifies, when enabled, that the network access connection uses Datagram Transport Level Security (DTLS). DTLS uses UDP instead of TCP, to provides better throughput for high-demand applications like VoIP or streaming video, especially with lossy connections.
DTLS Port	Port number	Specifies the port number that the network access resource uses for secure UDP traffic with DTLS. The default is `4433`.
Client Proxy Settings	Enable/disable	When selected, provides configuration settings for client proxy connections for this network access resource. This option requires the client computer to have Internet Explorer 5.0 or later installed. These options are available only when using the Advanced setting, when you select the Client proxy settings option.
Client Proxy Uses HTTP for Proxy Autoconfig Script	Enable/disable	Some applications, like Citrix® MetaFrame, can not use the client proxy autoconfig script when the browser attempts to use the `file://` prefix to locate it. Select this option to specify that the browser uses `http://` to locate the proxy autoconfig file, instead of `file://`.
Client Proxy Autoconfig Script	URL	The URL for a proxy auto-configuration script, if one is used with this connection.
Client Proxy Address	IP address	The IP address for the client proxy server that network access clients use to connect to the Internet.
Client Proxy Port	Port number	The port number of the proxy server that network access clients use to connect to the Internet.
Bypass Proxy For Local Addresses	Enable/disable	Select this option if you want to allow local intranet addresses to bypass the proxy server.
Client Proxy Exclusion List	IP addresses, domain names, with wildcards	Specifies the web addresses that do not need to be accessed through your proxy server. You can use wildcards to match

Setting	Value	Description
		domain and host names, or addresses. For example, `www.*.com`, `128.*`, `240.8`, `8.`, **mygroup.***, `*.*`.

Chapter 4

Creating Optimized Application Tunnels

What is an optimized application?

An *optimized application* is a set of compression characteristics that are applied to traffic flowing from the network access client to a specific IP address, network, or host, on a specified port or range of ports. An optimized tunnel provides a TCP Layer 4 connection to an application. You can configure optimized applications separately from the standard TCP Layer 3 network access tunnel specified on the **Network Settings** page.

Important: *Optimized application tunnels are supported only for Windows client systems, and require administrative rights on the client system to install.*

Optimized application tunnels take precedence over standard network access tunnels, so for specified destinations, an optimized connection is established, whether the network access tunnel is enabled or not. In cases where optimized application tunnels have overlapping addresses or ranges, tunnels are prioritized in the following order:

- An address definition with a more specific network mask takes precedence.
- An address definition with a scope defined by a more specific subnet takes precedence.
- A tunnel defined by a host name takes precedence over a tunnel defined by an IP address.
- A tunnel defined by a host name takes precedence over a tunnel defined by a host name with a wildcard. For example, `web.siterequest.com` takes precedence over `*.siterequest.com`.
- A tunnel defined by a host name with a wildcard takes precedence over a tunnel defined by a network address. For example, `*.siterequest.com` takes precedence over `1.2.3.4/16`.
- For equivalent tunnels with different port ranges, the tunnel with a smaller port range takes precedence. For example, `web.siterequest.com:21-22` takes precedence over `web.siterequest.com:21-30`.

Configuring an optimized application on a network access tunnel

You must create a network access resource, or open an existing resource, before you can perform this task.

You can configure the description of a network access resource with network access properties.

1. On the Main tab, click **Access Policy** > **Network Access** > **Network Access List**.
   The Network Access List screen opens.
2. Click the name to select a network access resource on the Resource List.
   The Network Access editing screen opens.
3. To configure optimization for a host with the network access resource, click **Optimization** on the menu bar.
4. Click **Add** to add a new optimized application configuration.
5. Configure the destination and port settings, and any required optimization characteristics.
6. Click **Finished**.
   The optimized application configuration is added to the network access resource.
7. Click the **Update** button.
   Your changes are saved and the page refreshes.

Optimized application settings

Use the following settings to configure an optimized application.

Setting	Value	Description
Optimized Application	Basic/Advanced	Select **Basic** to show only destination and port settings, and **Advanced** to show optimization settings for the application destination.
Destination Type: Host Name	Fully qualified domain name (FQDN)	Select this option to apply optimization to a specific named host. Specify a fully qualified domain name (FQDN) for the destination.
Destination Type: IP Address	IP Address	Select this option to apply optimization to a host at a specific IP address. Specify an IP address for the destination. This can be an IPv4 or IPv6 address.
Destination Network	Network IP address and network mask	Select this option to apply optimization to a network. Specify a network IP address and subnet mask for the destination. This can be an IPv4 or IPv6 address.
Port(s)	Specific numeric port, list selection, or port range	You can specify a single port on which to optimize traffic, or select **Port Range** to specify an inclusive range. If you optimize traffic on a single port, you can type a port number, or you can select an application from the list of common applications to add the appropriate port, for example, FTP.
Deflate	Enabled/Disabled	Enable or disable Deflate compression. Deflate compression uses the least CPU resources, but compresses the least effectively.
LZO	Enabled/Disabled	Enable or disable LZO compression. LZO compression offers a balance between CPU resources and compression ratio, compressing more than Deflate compression, but with less CPU resources than Bzip2.
Bzip2	Enabled/Disabled	Enable or disable bzip2 compression. Bzip2 compression uses the most CPU resources, but compresses the most effectively.

Chapter 5

Configuring Lease Pools

What is a lease pool?

A *lease pool* specifies a group of IPv4 or IPv6 IP addresses as a single object. You can use a lease pool to associate that group of IP addresses with a network access resource. When you assign a lease pool to a network access resource, network access clients are automatically assigned unallocated IP addresses from the pool during the network access session.

Important: *Network access with IPv6 alone is not supported. An IPv6 tunnel requires a simultaneous IPv4 tunnel, which is automatically established when you assign IPv4 and IPv6 lease pools, and set the version to* ***IPv4&IPv6****.*

Creating an IPv4 lease pool

Create a lease pool to provide internal network addresses for network access tunnel users.

1. On the Main tab, select **Access Policy** > **Network Access** > **Lease Pools** > **IPv4 Lease Pools**. The IPv4 Lease Pools list appears.
2. Click the **Create** button.
3. In the **Name** field, type a name for the resource.
4. Add IPv4 addresses to the lease pool.
   - To add a single IP address, in the Member List area, select **IP Address** for the type. In the **IP Address** field, type the IP address.
   - To add a range of IP addresses, in the Member List area, select **IP Address Range** for the type. In the **Start IP Address** field, type the first IP address, and in the **End IP Address** field, type the last IP address.
5. Click the **Add** button.

A lease pool is created with the IP address or IP address range you specified.

To delete an IP address or IP address range, select the IP address or IP address range in the member list, and click the **Delete** button.

Creating an IPv6 lease pool

Create a lease pool to provide internal network addresses for network access tunnel users.

Important: *Network access with IPv6 alone is not supported. An IPv6 tunnel requires a simultaneous IPv4 tunnel, which is automatically established when you assign IPv4 and IPv6 lease pools, and set the version to* ***IPv4&IPv6****.*

1. On the Main tab, select **Access Policy** > **Network Access** > **Lease Pools** > **IPv6 Lease Pools**. The IPv6 Lease Pools list appears.
2. Click the **Create** button.
3. In the **Name** field, type a name for the resource.
4. Add IPv6 addresses to the lease pool.

- To add a single IP address, in the Member List area, select **IP Address** for the type. In the **IP Address** field, type the IP address.
- To add a range of IP addresses, in the Member List area, select **IP Address Range** for the type. In the **Start IP Address** field, type the first IP address, and in the **End IP Address** field, type the last IP address.

5. Click the **Add** button.

A lease pool is created with the IP address or IP address range you specified.

To delete an IP address or IP address range, select the IP address or IP address range in the member list, and click the **Delete** button.

Chapter 6

Shaping Traffic on the Network Access Client

About Windows client traffic shaping

Used together, client traffic classifiers and client rate classes provide client-side traffic shaping features on Windows® network access client connections. You configure a *client traffic classifier*, which defines source and destination IP addresses or networks, and can also specify a protocol. The client traffic classifier is then associated with a *client rate class*, which defines base and peak rates for traffic to which it applies, and other traffic shaping features. A client traffic classifier is assigned in a network access resource.

Important: *Client traffic classifiers support IPv4 addresses only.*

Configuring client traffic shaping

Client rate shaping allows you to shape client-side traffic from Windows® client systems, based on traffic parameters.

1. Create a client rate class.
2. Create a client traffic classifier.

   When you create the client traffic classifier, you select the previously created client rate class.

Together, the client rate class and client traffic classifier work to provide client-side traffic control to Windows clients to which the traffic control is applied.

Select the client traffic classifier in the **Network Settings** configuration of a network access resource. The client traffic classifier is then applied to Windows clients, for client-side traffic on the VPN tunnels defined by that network access resource.

Creating a client rate class

Create a client rate class to define the traffic shaping rules that you can apply to virtual and physical interfaces on a network access tunnel.

1. On the Main tab, click **Access Policy** > **Network Access** > **Client Traffic Control** > **Client Rate Classes**.
2. Click **Create**.
   The New Client Rate Class screen opens.
3. In the **Name** field, type the name for the new client rate class.
4. Select **Basic** or **Advanced**.

   The Advanced configuration allows you to configure the burst size, the rate class mode, and override the DSCP code.
5. In the **Base Rate** field, type the base rate for the client rate class. Select the units for the peak rate from the list (**bps**, **Kbps**, **Mbps**, or **Gbps**).
6. In the **Ceiling Rate** field, type the peak rate for the client rate class. Select the units for the ceiling rate from the list (**bps**, **Kbps**, **Mbps**, or **Gbps**).
7. In the **Burst Size** field, type the amount of traffic that is allowed to reach the ceiling rate defined for the traffic rate class. You can select the units for this number from the list (**bytes**, **Kilobytes**, **Megabytes**, or **Gigabytes**).

8. From the **Service Type** list, select the service type.
9. From the **Mode** list, select the traffic shaping mode.
10. (Optional) If you are using a differential services network, you can specify the DSCP value with which to mark this traffic by selecting the DSCP **Override** check box.
    In the field, type the number of the DSCP code with which to mark traffic.
11. Click **Finished**.

The client rate class is created.

Select this client rate class in a client traffic classifier to apply it to Windows® client-side traffic.

Client rate class properties

Client rate class properties specify settings for client traffic control rates.

Setting	Value	Description
Base Rate	Integer in **bps**, **Kbps**, **Mbps**, or **Gbps**	Specifies the base data rate defined for the client rate class.
Ceiling Rate	Integer in **bps**, **Kbps**, **Mbps**, or **Gbps**	Specifies the ceiling data rate defined for the client rate class.
Burst Size	Integer in **bytes**, **Kilobytes**, **Megabytes**, or **Gigabytes**	Specifies the amount of traffic that is allowed to reach the ceiling data rate defined for the client rate class.
Service Type	**Best Effort**, **Controlled Load**, or **Guaranteed**	• **Best Effort** - Specifies that Windows® traffic control creates a flow for this client traffic class, and traffic on the flow is handled with the same priority as other Best Effort traffic. • **Controlled Load** - Specifies that traffic control transmits a very high percentage of packets for this client rate class to its intended receivers. Packet loss for this service type closely approximates the basic packet error rate of the transmission medium. Transmission delay for a very high percentage of the delivered packets does not greatly exceed the minimum transit delay experienced by any successfully delivered packet. • **Guaranteed** - Guarantees that datagrams arrive within the guaranteed delivery time and are not discarded due to queue overflows, provided the flow's traffic stays within its specified traffic parameters. This service type is intended for applications that require guaranteed packet delivery.
Mode	**Shape**, **Discard**, or **Borrow**	• **Shape** - Delays packets submitted for transmission until they conform to the specified traffic profile. • **Discard** - Discards packets that do not conform to the specified traffic control profile. • **Borrow** - Allows traffic on the client rate class to borrow resources from other flows that are temporarily idle. Traffic that borrows resources is marked as nonconforming, and receives a lower priority.
DSCP	Enable/disable, integer for DSCP code	If you select **Override**, you can specify an optional DSCP code for the client rate class. DSCP is a way of classifying traffic for Quality of Service (QoS). Traffic is classified using six-bit values, and then routers on the network interpret the traffic priority based on their configurations and prioritize traffic for QoS accordingly.

Creating a client traffic classifier

You must create at least one client rate class before you create a client traffic classifier. You select client rate classes to define rules in the client traffic classifier.

Create a client traffic classifier to define traffic control rules for the virtual and physical network interfaces on a network access tunnel.

1. On the **Main** tab, click **Access Policy** > **Network Access** > **Client Traffic Control** > **Client Traffic Classifiers**.
2. Click **Create**.
   The New client rate class screen opens.
3. In the **Name** box, type a name for the client traffic classifier, and click **Create**.
   The Client Traffic Classifiers list screen opens.
4. Click the name of the client traffic classifier you just created.
5. Add rules for the appropriate interface.

Rule type	Description
Rules for Virtual Network Access Interface	Add a rule to this section to apply the traffic shaping control only to traffic on the virtual network access interface.
Rules for Local Physical Interfaces	Add a rule to this section to apply the traffic shaping control only to traffic on the client computer's local physical interfaces.
Rules for Virtual Network Access and Local Physical Interfaces	Add a rule to this section to apply the traffic shaping control to traffic on both the virtual Network Access interface and the client's local physical interfaces.

Adding a client traffic classifier entry

You add entries to an existing client traffic classifier. You must first create a client traffic classifier, and at least one client rate class.

Client traffic classifiers define client traffic control for virtual and physical network interfaces on the client systems.

1. On the Main tab, click **Access Policy** > **Network Access** > **Client Traffic Control** > **Client Traffic Classifiers**.
2. Click the name of a client traffic classifier.
3. Under the appropriate interface **Rules** area, click **Add**.
   The New Client Traffic Classifier Entry screen opens.
4. Select **Basic** or **Advanced**.

   Advanced mode allows you to configure a source address and source ports for the client traffic control entry.
5. Select a **Client Rate Class** entry.
6. Specify any settings you require for the client traffic classifier entry.

   Note that currently you can only specify an IPv4 address for a client traffic classifier host entry.
7. When you have finished configuring the client traffic classifier entry, click **Finished**.
   The configuration screen for the client traffic classifier appears again.

The client traffic classifier is updated with the client traffic classifier entry in the **Rules** area you specified.

Client traffic classifier entry properties

Configure properties for the client traffic classifier to determine how traffic is classified for traffic shaping on Windows® clients.

Property	Values	Description
Basic/Advanced	Basic or Advanced (list item)	**Advanced** allows you to configure a source address and source ports.
Client Rate Class	List item	A client rate class defines the client traffic shaping rates and properties for a client traffic control configuration. Because client traffic classifier entries define address pairs and protocols on which client rate classes operate, a client rate class must be created before you can use a client traffic classifier entry.
Protocol	UDP, TCP, or All Protocols.	The protocol to which this client traffic classifier entry applies.
Destination Address	Selection and manual entries	The destination address to which the client traffic classifier entry applies. • **Any** applies the client traffic classifier entry to any destination address. • **Host** applies the client traffic classifier entry to a specific host IP address. Type the IP address in the box that appears. • **Network** applies the client traffic classifier entry to a network address. Type the network address and the network mask in the boxes that appear.
Destination Port	Number or list item	The destination port to which the client traffic classifier entry applies. You can type the port number, or select from the list of predefined application ports.
Source Address	Selection and manual entries	The source address to which the client traffic classifier entry applies. • **Any** applies the client traffic classifier entry to any source address. • **Host** applies the client traffic classifier entry to a specific host IP address. Type the IP address in the box that appears. • **Network** applies the client traffic classifier entry to a network address. Type the network address and the network mask in the boxes that appear.
Source Port	Number or list item	The source port to which the client traffic classifier entry applies. You can type the port number, or select from the list of predefined application ports.

Chapter 7

Configuring Webtops

About webtops

There are three webtop types you can define on Access Policy Manager® (APM®). You can define a network access as only a webtop, a portal access webtop, or a full webtop.

Important: *Do not assign a webtop for a portal access connection configured for minimal patching mode. This configuration does not work.*

- A network access webtop provides a webtop for an access policy branch to which you assign only a network access resource.
- A portal access webtop provides a webtop for an access policy branch to which you assign only portal access resources.
- A full webtop provides an access policy ending for an access policy branch to which you can optionally assign portal access resources, app tunnels, remote desktops, and webtop links, in addition to network access tunnels. Then, the full webtop provides your clients with a web page on which they can choose a network access connection to start.

  Note: *If you add a network access resource with Auto launch enabled to the full webtop, the network access resource starts when the user reaches the webtop. You can add multiple network access resources to a webtop, but only one can have Auto launch enabled.*

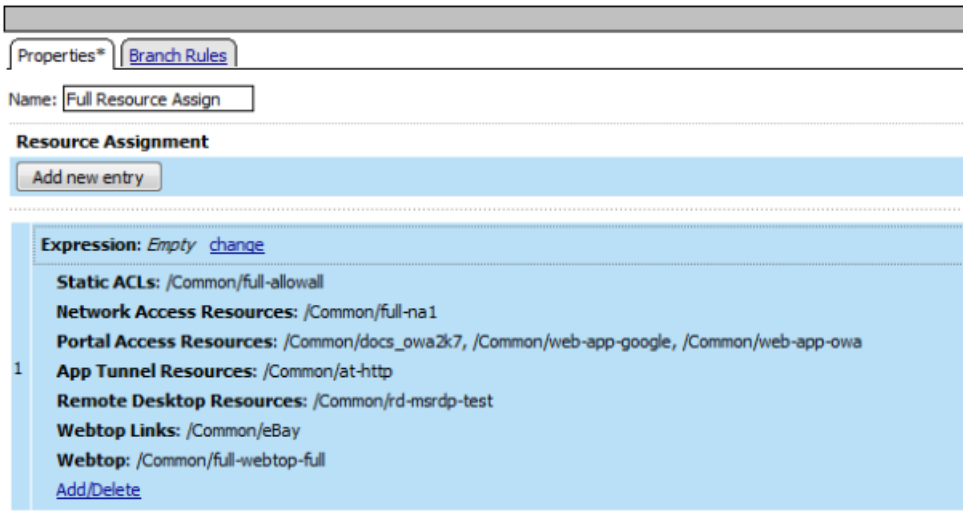


Figure 2: Resource assign action with resources and a webtop assigned

Configuring a webtop for network access

A webtop allows your users to connect and disconnect from the network access connection.

1. On the Main tab, click **Access Policy** > **Webtops**.
   The Webtop List screen opens.
2. Click **Create** to create a new webtop.

3. Select the type of webtop to create.

Option	Description
Network Access	Select **Network Access** for a webtop to which you will assign only a single network access resource.
Portal Access	Select **Portal Access** for a webtop to which you assign only portal access resources.
Full	Select **Full** for a webtop to which you assign one or more network access resources, multiple portal access resources, and multiple application access app tunnel resources, or any combination of the three types.

The webtop is now configured, and appears in the list. You can edit the webtop further, or assign it to an access policy.

To use this webtop, it must be assigned to an access policy with an advanced resource assign action or with a webtop and links assign action.

Configuring a full webtop

A full webtop allows your users to connect and disconnect from a network access connection, portal access resources, SAML resources, app tunnels, remote desktops, and administrator-defined links.

1. On the Main tab, click **Access Policy** > **Webtops**.
2. Click **Create** to create a new webtop.
3. Type a name for the webtop you are creating.
4. From the **Type** list, select **Full**.
5. Click **Finished**.

The webtop is now configured, and appears in the list. You can edit the webtop further, or assign it to an access policy.

To use this webtop, it must be assigned to an access policy with an advanced resource assign action or with a webtop and links assign action. All resources assigned to the full webtop are displayed on the full webtop.

Creating a webtop link

You can create and customize links that you can assign to full webtops. In this context, *links* are defined applications and websites that appear on a webtop, and can be clicked to open a web page or application. You can customize these links with descriptions and icons.

1. On the Main tab, click **Access Policy** > **Webtops** > **Webtop Links**.
2. Click **Create** to create a new webtop link.
3. In the **Name** field, type a name for the new webtop link.
4. From the **Link Type** list, select whether the link is a URI or hosted content.
   - If you selected **Application URI**, in the **Application URI** field, type the application URI.
   - If you selected **Hosted Content**, select the hosted file to use for the webtop link.
5. In the **Caption** field, type a descriptive caption.

The **Caption** field is pre-populated with the text from the **Name** field. Type the link text that you want to appear on the web link.

6. If you want to add a detailed description, type it in the **Detailed Description** field.
7. To specify an icon image for the item on the webtop, click in the **Image** field and choose an image, or click the **Browse** button.

   Click the **View/Hide** link to show or hide the currently selected image.
8. Click **Finished**.

The webtop link is now configured, and appears in the list, and on a full webtop assigned with the same action. You can edit the webtop link further, or assign it to an access policy.

Before you can use this webtop link, it must be assigned to an access policy with a full webtop, using either an advanced resource assign action or a webtop and links assign action.

Customizing a webtop link

You can customize links that you assign to full webtops.

1. On the Main tab, click **Access Policy** > **Webtops** > **Webtop Links**.
2. Click the name of the webtop link you want to customize.
   The properties screen for the webtop link appears.
3. To change the description of the link, in the **Description** field, type a new description.
4. To change the URI of the link, in the **Application URI** field, type the application URI.
5. If you made changes on the properties screen, click **Update**.
6. Click the Customization tab.
7. Select the **Language** to customize, or click the **Create** button to create a new language customization.
8. If you clicked **Create** to create a new language customization, from the **Language** list, select the language to customize.
9. In the **Caption** field, type a descriptive caption.
10. In the **Detailed Description** field, type a detailed description.
11. In the **Image** field, click **Browse** to select an image to show on the webtop to represent the webtop link. Click the **View/Hide** link to show the currently assigned image.

    A webtop link image can be a GIF, BMP, JPG or PNG image up to 32 x 32 pixels in size.
12. Click **Finished**.

The webtop link is now configured, and appears in the list, and on a full webtop assigned with the same action. You can edit the webtop link further, or assign it to an access policy.

Before you can use this webtop link, it must be assigned to an access policy with a full webtop, using either an advanced resource assign action or a webtop and links assign action.

Webtop properties

Use these properties to configure a webtop.

Property setting	Value	Description
Type	**Network Access**, **Portal Access**, or **Full**	• Use **Network Access** for a webtop to which you assign only a single network access resource. • Use **Portal Access** for a webtop to which you assign only portal access resources. • Use **Full** for a webtop to which you assign one or more network access resources, multiple portal access resources, and multiple application access application tunnel resources, or any combination of the three types.
Portal Access Start URI	URI.	Specifies the URI that the web application starts. For full webtops, portal access resources are published on the webtop with the associated URI you define when you select the **Publish on Webtop** option.
Minimize to Tray	**Enable** or **Disable**.	If this check box is selected, the webtop is minimized to the system tray automatically after the network access connection starts. With a network access webtop, the webtop automatically minimizes to the tray. With a full webtop, the webtop minimizes to the system tray only after the network access connection is started.

Chapter 8

Defining Connectivity Options

About connectivity profiles and network access

In BIG-IP® Access Policy Manager®, a connectivity profile is the profile that you select in a virtual server definition to define connectivity and client settings for a network access session.

The connectivity profile contains:

- Compression settings for network access connections and application tunnels
- Citrix client settings
- Virtual servers and DNS-location awareness settings for BIG-IP Edge Client® for Windows and Mac
- Password caching settings for BIG-IP Edge Client for Windows, Mac, and mobile clients
- Security settings, in addition to password caching, for mobile clients

A connectivity profile is also associated with client download packages that you can customize.

Creating a connectivity profile

You create a connectivity profile to configure client connections for a network access tunnel, application access tunnel, and clients.

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Click **Add**.
   The Create New Connectivity Profile popup screen opens and displays General Settings.
3. Type a **Profile Name** for the connectivity profile.
4. Select a **Parent Profile** from the list.
   APM® provides a default profile, **connectivity**.
5. From the Compression Settings folder, click **Network Access** and make changes to the network access compression settings.
   The settings specify available compression codecs for server-to-client connections.
   The default settings are displayed in the right pane.
6. From the Compression Settings folder, click **App Tunnel** and make changes to the application tunnel compression settings.
   The settings specify available compression codecs for server-to-client connections. By default, compression is enabled, but no codecs are selected in the Available Codecs area.
   The default settings are displayed in the right pane.
7. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.

The connectivity profile appears in the list.

To provide functionality with a connectivity profile, you must add the connectivity profile and an access profile to a virtual server.

About connectivity profile compression settings

Compression settings specify the available compression codecs for server-to-client connections. The server compares the available compression types configured in the connectivity profile with the available compression types on the client, and chooses the most effective mutual compression setting.

Connectivity profile general settings

You can configure the following general settings in a connectivity profile.

Profile setting	Value	Description
Profile Name	Text.	Text specifying name of the connectivity profile.
Parent Profile	A connectivity profile, selected from a list.	A profile inherits settings from its parent profile.
FEC Profile	A forward error correcting (FEC) profile, selected from a list.	A FEC profile applies to a network access tunnel. ***Note:*** *FEC profiles might not be available on all BIG-IP® systems.*
Description	Text.	Text description of the connectivity profile.

Connectivity profile network access compression settings

You can configure the following network access compression settings in a connectivity profile.

Setting	Value	Description
Compression Buffer Size	Number of bytes. The default is `4096`.	Specifies the size of the output buffers containing compressed data.
gzip Compression Level	A preset, or a value between `1` and `9`.	Specifies the degree to which the system compresses the content. Higher compression levels cause the compression process to be slower and the result to be more compressed. The default compression level is **6 - Optimal Compression (Recommended)**, which provides a balance between level of compression and CPU processing time. You can also select compression level **1 - Least Compression (Fastest)**, the lowest amount of compression, which requires the least processing time, or **9 - Most Compression (Slowest)**, the highest level of compression, which requires the most processing time. You can also select a number between `1` and `9`.
gzip Memory Level	`1-256` kb.	Specifies the number of kilobytes of memory that the system uses for internal compression buffers when compressing data. You can select a value between `1` and `256`.
gzip Window Size	`1-128` kb.	Specifies the number of kilobytes in the window size that the system uses when compressing data. You can select a value between `1` and `128`.

Setting	Value	Description
CPU Saver	Selected or cleared.	Specifies, when enabled, that the system monitors the percentage of CPU usage and adjusts compression rates automatically when the CPU usage reaches either the **High** value or the **Low** Value.
High	Percentage	Specifies the percentage of CPU usage at which the system starts automatically decreasing the amount of content being compressed, as well as the amount of compression which the system is applying.
Low	Percentage	Specifies the percentage of CPU usage at which the system resumes content compression at the user-defined rates.

Connectivity profile application tunnel compression settings

You can configure the following application tunnel compression settings in a connectivity profile.

Setting	Value	Description
Compression	**Enable** or **Disable**	Specifies the available compression codecs for server-to-client connections. The server compares the available compression types configured here, with the available compression types on the client, and chooses the most effective mutual compression setting.
Adaptive Compression	**Enable** or **Disable**	Specifies whether to enable to disable adaptive compression between the client and the server.
Deflate Level	From 1 to 9	Specifies a compression level for deflate compression. Higher numbers compress more, at the cost of more processing time.
lzo	**Enable** or **Disable**	Specifies LZO compression. LZO compression offers a balance between CPU resources and compression ratio, compressing more than Deflate compression, but with less CPU resources than Bzip2.
deflate	**Enable** or **Disable**	Specifies deflate compression. Deflate compression uses the least CPU resources, but compresses the least effectively.
bzip2	**Enable** or **Disable**	Specifies Bzip2 compression. Bzip2 compression uses the most CPU resources, but compresses the most effectively.

Chapter 9

Creating an Access Policy for Network Access

About access profiles

In the BIG-IP® Access Policy Manager®, an access profile is the profile that you select in a virtual server definition to establish a secured session. You can also configure an access profile to provide access control and security features to a local traffic virtual server hosting web applications.

The access profile contains:

- Access policy timeout and concurrent user settings
- Accepted language and default language settings
- Single Sign-On information and domain cookie information for the session
- Customization settings for the access profile
- The access policy for the profile

About access policies for network access

Define an access policy for network access in order to provide access control conditions that you want users to satisfy, before they can connect to internal resources. For a network access policy, you need to configure a minimum of a resource assign action that assigns a network access resource.

Creating an access profile

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

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

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

4. From the **Profile Type** list, select **SSL-VPN**.
   Additional settings display.
5. To configure timeout and session settings, select the **Custom** check box.
6. In the **Inactivity Timeout** field, type the number of seconds that should pass before the access policy times out. Type `0` to set no timeout.

   If there is no activity (defined by the **Session Update Threshold** and **Session Update Window** settings in the Network Access configuration) between the client and server within the specified threshold time, the system closes the current session.
7. In the **Access Policy Timeout** field, type the number of seconds that should pass before the access profile times out because of inactivity.

   Type `0` to set no timeout.
8. In the **Maximum Session Timeout** field, type the maximum number of seconds the session can exist.

Type 0 to set no timeout.

9. In the **Max Concurrent Users** field, type the maximum number of users that can use this access profile at the same time.

   Type 0 to set no maximum.

10. In the **Max Sessions Per User** field, type the maximum number of concurrent sessions that one user can start.

    Type 0 to set no maximum.

11. In the **Max In Progress Sessions Per Client IP** field, type the maximum number of concurrent sessions that one client IP address can support.

    Type 0 to set no maximum.

12. Select the **Restrict to Single Client IP** check box to restrict the current session to a single IP address.

    This setting associates the session ID with the IP address.

    Upon a request to the session, if the IP address has changed the request is redirected to a logout page, the session ID is deleted, and a log entry is written to indicate that a session hijacking attempt was detected. If such a redirect is not possible, the request is denied and the same events occur.

13. To configure logout URIs, in the Configurations area, type each logout URI in the **URI** field, and then click **Add**.

14. In the **Logout URI Timeout** field, type the delay in seconds before logout occurs for the customized logout URIs defined in the **Logout URI Include** list.

15. To configure SSO:

    - For users to log in to multiple domains using one SSO configuration, skip the settings in the SSO Across Authentication Domains (Single Domain mode) area. You can configure SSO for multiple domains only after you finish the initial access profile configuration.
    - For users to log in to a single domain using an SSO configuration, configure settings in the SSO Across Authentication Domains (Single Domain mode) area, or you can configure SSO settings after you finish the initial access profile configuration.

16. In the **Domain Cookie** field, specify a domain cookie, if the application access control connection uses a cookie.

17. In the **Cookie Options** setting, specify whether to use a secure cookie.

    - If the policy requires a secure cookie, select the **Secure** check box to add the **secure** keyword to the session cookie.
    - If you are configuring an LTM access scenario that uses an HTTPS virtual server to authenticate the user and then sends the user to an existing HTTP virtual server to use applications, clear this check box.

18. If the access policy requires a persistent cookie, in the **Cookie Options** setting, select the **Persistent** check box.

    This sets cookies if the session does not have a webtop. When the session is first established, session cookies are not marked as persistent; but when the first response is sent to the client after the access policy completes successfully, the cookies are marked persistent. Persistent cookies are updated for the expiration timeout every 60 seconds. The timeout is equal to session inactivity timeout. If the session inactivity timeout is overwritten in the access policy, the overwritten value will be used to set the persistent cookie expiration.

19. From the **SSO Configurations** list, select an SSO configuration.

20. 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.

21. Click **Finished**.

The access profile appears in the Access Profiles List.

To add an SSO configuration for multiple domains, click **SSO / Auth Domains** on the menu bar. To provide functionality with an access profile, you must configure the access policy. The default access policy for a profile denies all traffic and contains no actions. Click **Edit** in the **Access Policy** column to edit the access policy.

Access profile settings

You can configure the following settings in an access profile.

Setting	Value	Description and defaults
Name	Text	Specifies the name of the access profile.
Inactivity Timeout	Number of seconds, or `0`	Specifies the inactivity timeout for the connection. If there is no activity between the client and server within the specified threshold time, the system closes the current session. By default, the threshold is `0`, which specifies that as long as a connection is established, the inactivity timeout is inactive. However, if an inactivity timeout value is set, when server traffic exceeds the specified threshold, the inactivity timeout is reset.
Access Policy Timeout	Number of seconds, or `0`	Designed to keep malicious users from creating a denial-of-service (DoS) attack on your server. The timeout requires that a user, who has followed through on a redirect, must reach the webtop before the timeout expires. The default value is `300` seconds.
Maximum Session Timeout	Number of seconds, or `0`	The maximum lifetime is from the time a session is created, to when the session terminates. By default, it is set to `0`, which means no limit. When you configure a maximum session timeout setting other than `0`, there is no way to extend the session lifetime, and the user must log out and then log back in to the server when the session expires.
Max Concurrent Users	Number of users, or `0`	The number of sessions allowed at one time for this access profile. The default value is `0` which specifies unlimited sessions.
Max Sessions Per User	Number between `1` and `1000`, or `0`	Specifies the number of sessions for one user that can be active concurrently. The default value is `0`, which specifies unlimited sessions. You can set a limit from `1-1000`. Values higher than `1000` cause the access profile to fail. ***Note:*** *Only superAdmins and application editors have access to this field. No other admin roles can modify this field.*
Max In Progress Sessions Per Client IP	Number `0` or greater	Specifies the maximum number of sessions that can be in progress for a client IP address. When setting this value, take into account whether users will come from a NAT-ed or proxied client address and, if so, consider increasing the value accordingly. The default value is **0** which represents unlimited sessions. ***Note:*** *Only superAdmins and application editors have access to this field. No other admin roles can modify this field.*

Setting	Value	Description and defaults
Restrict to Single Client IP	Selected or cleared	When selected, limits a session to a single IP address. ***Note:*** *Only superAdmins and application editors have access to this field. No other admin roles can modify this field.*
Logout URI Include	One or more URIs	Specifies a list of URIs to include in the access profile to initiate session logout.
Logout URI Timeout	Logout delay URI in seconds	Specifies the time delay before the logout occurs, using the logout URIs defined in the logout URI include list.
SSO Authentication Across Domains (Single Domain mode) or SSO / Auth Domains: **Domain Cookie**	A domain cookie	If you specify a domain cookie, then the line `domain=specified_domain` is added to the `MRHsession` cookie.
SSO / Auth Domains: **Domain Mode**	**Single Domain** or **Multiple Domains**	Select **Single Domain** to apply your SSO configuration to a single domain. Select **Multiple Domain** to apply your SSO configuration across multiple domains. This is useful in cases where you want to allow your users a single Access Policy Manager® (APM®) login session and apply it across multiple Local Traffic Manager™ or APM virtual servers, front-ending different domains. ***Important:*** *All virtual servers must be on one single BIG-IP® system in order to apply SSO configurations across multiple domains.*
SSO / Auth Domains: **Primary Authentication URI**	URI	The URI of your primary authentication server, for example `https://logon.siterequest.com`. This is required if you use SSO across multiple domains. You provide this URI so your users can access multiple back-end applications from multiple domains and hosts without requiring them to re-enter their credentials, because the user session is stored on the primary domain.
Cookie Options: **Secure**	Enable or disable check box	Enabled, this setting specifies to add the **secure** keyword to the session cookie. If you are configuring an application access control scenario where you are using an HTTPS virtual server to authenticate the user, and then sending the user to an existing HTTP virtual server to use applications, clear this check box.
Cookie Options: **Persistent**	Enable or disable check box	Enabled, this setting specifies to set cookies if the session does not have a webtop. When the session is first established, session cookies are not marked as persistent, but when the first response is sent to the client after the access policy completes successfully, the cookies are marked persistent. ***Note:*** *Persistent cookies are updated for the expiration timeout every 60 seconds. The timeout is equal to the session inactivity timeout. If the session inactivity timeout is overwritten in the access policy, the overwritten value is used to set the persistent cookie expiration.*

Setting	Value	Description and defaults
Cookie Options: **HTTP only**		HttpOnly is an additional flag included in a Set-Cookie HTTP response header. Use the HttpOnly flag when generating a cookie to help mitigate the risk of a client-side script accessing the protected cookie, if the browser supports HttpOnly. When this option is enabled, only the web access management type of access (an LTM virtual server with an access policy) is supported.
SSO Authentication Across Domains (Single Domain mode) or SSO / Auth Domains **SSO Configuration**	Predefined SSO configuration	SSO configurations contain settings to configure single sign-on with an access profile. Select the SSO configuration from the list that you want applied to your domain.
SSO / Auth Domains: Authentication Domains	Multiple	If you specify multiple domains, populate this area with hosts or domains. Each host or domain can have a separate SSO config, and you can set persistent or secure cookies. Click **Add** to add each host you configure.
Accepted Languages	Language strings	Adds a built-in or customized language to the list of accepted languages. Accepted languages can be customized separately and can present customized messages and screens to users, if the user's default browser language is one of the accepted languages. Select a language from the **Factory Builtin Languages** list and click the Move button (<<) to add it to the **Accepted Languages** list. Select a language from the **Additional Languages** list and click **Add** to add it to the **Accepted Languages** list.
Factory Builtin Languages	Languages in a predefined list	Lists the predefined languages on the Access Policy Manager system, which can be added to the **Accepted Languages** list. Predefined languages include customized messages and fields for common appearance items, as opposed to **Additional Languages**, which must be separately customized.
Additional Languages	Languages in a predefined list	Lists additional languages that can be added to the **Accepted Languages** list, and customized on the Access Policy Manager system. These languages are populated with English messages and fields and must be individually customized using the Customization menu, as opposed to **Factory Builtin Languages**, which are already customized.

Adding network access to an access policy

Before you assign a network access resource to an access policy, you must:

- Create a network access resource
- Create an access profile
- Define a network access webtop or a full webtop

When you assign a network access resource to an access policy branch, a user who successfully completed the branch rule (which includes that access policy item) starts a network access tunnel.

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

2. Click the name of the access profile for which you want to edit the access policy.
   The properties screen opens for the profile you want to edit.
3. On the menu bar, click **Access Policy**.
   The Access Policy screen opens.
4. Click **Edit Access Policy for Profile** ***profile_name***.
   The visual policy editor opens the access policy in a separate screen.
5. Click the **(+)** icon anywhere in the access policy to add a new action item.

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

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
6. Select one of the following resource assignment actions and click **Add**.

Option	Description
Resource Assign	Select the **Resource Assign** action to add a network access resource only. **Resource Assign** does not allow you to add a webtop or ACLs. If you want to add ACLs, a webtop, or webtop links after you add a Resource Assign action, you can add them with the individual actions **ACL Assign** and **Webtop and Links Assign**.
Advanced Resource Assign	Select the **Advanced Resource Assign** action to add network access resources, and optionally add a webtop, webtop links, and one or more ACLs.

7. Select the resource or resources to add.
   - If you added an **Advanced Resource Assign** action, on the Resource Assignment screen, click **Add New Entry**, then click **Add/Delete**, and select and add resources from the tabs, then click **Update**.
   - If you added a **Resource Assign** action, next to Network Access Resources, click **Add/Delete**.

   If you add a full webtop and multiple network access resources, Auto launch can be enabled for only one network access resource. (With Auto launch enabled, a network access resource starts automatically when the user reaches the webtop.)
8. Click **Save**.
9. Click **Apply Access Policy** to save your configuration.

A network access tunnel is assigned to the access policy. You may also assign a network access or full webtop. On the full webtop, users can click the Network Access link to start the network access tunnel, or one network access tunnel (that is configured with Auto launch enabled) can start automatically.

After you complete the access policy, you must define a connectivity profile. In the virtual server definition, you must select the access policy and connectivity profile.

Chapter 10

Configuring Virtual Servers for Network Access

Associating a virtual server with network access

When creating a virtual server for an access policy, specify an IP address for a single host as the destination address.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. In the **Destination Address** field, type the IP address for a host virtual server.

   This field accepts an address in CIDR format (IP address/prefix). However, when you type the complete IP address for a host, you do not need to type a prefix after the address.
4. From the **HTTP Profile** list, select **http**.
5. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
6. From the **Connectivity Profile** list, select the connectivity profile.
7. If you are creating a virtual server to use with portal access resources in addition to remote desktops, from the **Rewrite Profile** list, select the default **rewrite** profile, or another rewrite profile you created.
8. If you use server SSL for this connection, from the **SSL Profile (Server)** list, select a server SSL profile.
9. If you use client SSL for this profile, from the **SSL Profile (Client)** list, select a client SSL profile.
10. If you want to provide connections to Java RDP clients for application access, allow Java rewriting for portal access, or support a per-app VPN connection that is configured on a mobile device, select the **Application Tunnels (Java & Per-App VPN)** check box.

    You must enable this setting to make socket connections from a patched Java applet. If your applet doesn't require socket connections, or only uses HTTP to request resources, this setting is not required.
11. If you want to provide native integration with an OAM server for authentication and authorization, select the **OAM Support** check box.

    You must have an OAM server configured in order to enable OAM support.
12. Click **Update**.

Your access policy is now associated with the virtual server.

Chapter 11

Integrating Network Access and Secure Web Gateway

About SWG remote access

With proper configuration, Secure Web Gateway (SWG) can support these types of remote access:

Network access
SWG supports explicit forward proxy or transparent forward proxy for network access connections.

Portal access
SWG supports transparent forward proxy for portal access.

Application access
SWG supports transparent forward proxy for application access.

Overview: Configuring SWG explicit forward proxy for network access

You can configure Secure Web Gateway (SWG) explicit forward proxy and network access configurations so that SWG processes the Internet traffic from a network access client in the same way that it processes such traffic from a client in the enterprise.

Note: *Using a distinct SWG explicit forward proxy configuration to process traffic from remote clients separately from an SWG configuration used for processing traffic from internal clients provides an important measure of network security.*

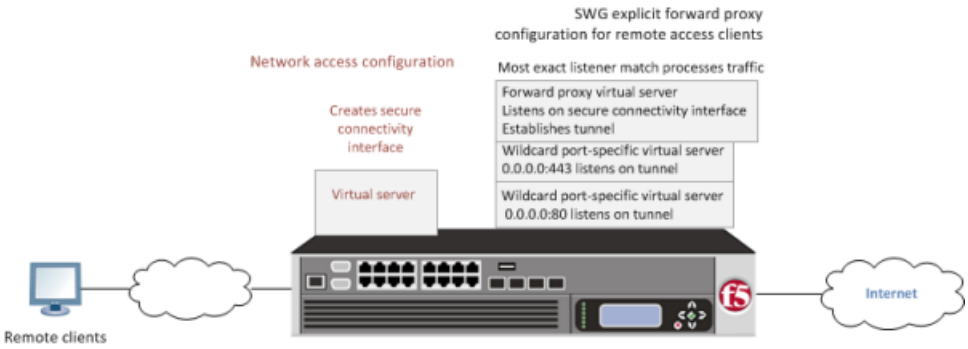


Figure 3: Explicit forward proxy for network access

You should understand how these configuration objects fit into the overall configuration.

Secure connectivity interface
In a network access configuration, a connectivity profile on the virtual server specifies a secure connectivity interface for traffic from the client. In the SWG configuration, an SWG explicit forward proxy server must listen on the secure connectivity interface for traffic from network access clients.

Tunnel
In the SWG configuration, an HTTP profile on the explicit forward proxy server specifies the name of a tunnel of tcp-forward encapsulation type. You can use the default tunnel, http-tunnel, or create another tunnel and use it.

Per-request policy

In any SWG configuration, the determination of whether a user can access a URL must be made in a per-request policy. A per-request policy determines whether to block or allow access to a request based on time or date or group membership or other criteria that you configure.

Access policies

The access policy in the network access configuration continues to authenticate users, assign resources, and evaluate ACLs, if any. In addition, this access policy must assign an SWG scheme for the network access session and populate any session variables used in the per-request policy. An access profile of the SWG-Explicit type is required in the SWG configuration; however, it is not necessary to include any items in the access policy.

Task summary

Creating a connectivity profile
Adding a connectivity profile to a virtual server
Creating a DNS resolver
Adding forward zones to a DNS resolver
Creating a custom HTTP profile for explicit forward proxy
Configuring a per-request policy for SWG
Creating an access profile for SWG explicit forward proxy
Creating a virtual server for network access client forward proxy server
Creating a wildcard virtual server for HTTP tunnel traffic
Creating a custom Client SSL forward proxy profile
Creating a custom Server SSL profile
Creating a wildcard virtual server for SSL traffic on the HTTP tunnel
Updating the access policy in the remote access configuration
Configuring a network access resource to forward traffic

Prerequisites for SWG explicit forward proxy for network access

Before you start to create a Secure Web Gateway (SWG) explicit forward proxy configuration to support network access clients, you must have completed these tasks.

- You need to have configured a working network access configuration.
- If you have not already done so, you must ensure that the URL database is downloaded.
- You need to have configured at least one SWG scheme and any URL filters that you want to use in addition to or instead of the default URL filters.

Configuration outline for explicit forward proxy for network access

Tasks for integrating an Access Policy Manager® (APM®) network access configuration with a Secure Web Gateway (SWG) explicit forward proxy configuration follow this order.

- First, if your network access configuration does not include a connectivity profile, create one and add it to the virtual server.
- Next, create an SWG explicit forward proxy configuration. This configuration includes the per-request policy.
- Finally, in the network access configuration, update the access policy (so that it assigns an SWG scheme and populates any session variables required for successful execution of the per-request policy) and update the network access resource for client proxy.

Creating a connectivity profile

You create a connectivity profile to configure client connections.

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Click **Add**.
   The Create New Connectivity Profile popup screen opens and displays General Settings.
3. Type a **Profile Name** for the connectivity profile.
4. Select a **Parent Profile** from the list.
   APM® provides a default profile, **connectivity**.
5. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.

The connectivity profile appears in the list.

To provide functionality with a connectivity profile, you must add the connectivity profile to a virtual server.

Adding a connectivity profile to a virtual server

Update a virtual server that is part of an Access Policy Manager® application access, network access, or portal access configuration to enable a secure connectivity interface for traffic from the client.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. Scroll down to the Access Policy area.
4. From the **Connectivity Profile** list, select the connectivity profile.
5. Click **Update** to save the changes.

Creating a DNS resolver

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

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

Adding forward zones to a DNS resolver

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

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

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

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

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

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

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

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

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

7. Click **Finished**.

Creating a custom HTTP profile for explicit forward proxy

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

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

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

3. In the **Name** field, type a unique name for the profile.
4. From the **Proxy Mode** list, select **Explicit**.
5. For **Parent Profile**, retain the **http-explicit** setting.
6. Select the **Custom** check box.
7. Scroll down to the Explicit Proxy area.
8. From the **DNS Resolver** list, select the DNS resolver you configured previously.
9. In the **Tunnel Name** field, you can retain the default value, **http-tunnel**, or type the name of a tunnel if you created one.

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

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

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

Configuring a per-request policy for SWG

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

10. Add any of these items to the policy.

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

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

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

b) Click the Branch Rules tab.

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

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

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

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

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

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

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

b) Click the Branch Rules tab.

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

d) Edit the default simple expression to specify group or class that is used in your environment.
In an LDAP Group Lookup item, the default simple expression is **User is a member of** `CN=MY_GROUP, CN=USERS, CN=MY_DOMAIN`. You can use the simple expression editor to replace the default values.

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

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

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

A Category Lookup item must precede this item.

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

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

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

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

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

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

f) Click **Save**.

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

The popup screen closes. The visual policy editor displays.

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

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

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

Creating an access profile for SWG explicit forward proxy

You create an access profile to specify any access policy configuration for a virtual server that serves in a Secure Web Gateway (SWG) explicit forward proxy configuration.

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

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

4. From the **Profile Type** list, select **SWG-Explicit**.
   Additional fields display set to default values.
5. In the Language Settings area, add and remove accepted languages, and set the default language.

   A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.
6. Click **Finished**.
   The Access Profiles list screen displays.
7. To enable Secure Web Gateway event logging for this access profile, add log settings.
   a) Click the name of the access profile that you just created.
      The Properties screen displays.
   b) On the menu bar, click **Logs**.
      The General Properties screen displays.
   c) In the Log Settings area, move log settings from the **Available** list to the **Selected** list.

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

This creates an access profile with a default access policy that contains a **Start** and a **Deny** ending.

You do not need to add any actions or make any changes to the access policy.

Creating a virtual server for network access client forward proxy server

Before you begin, you need to know the name of the connectivity profile specified in the virtual server for the network access configuration that you want to protect using Secure Web Gateway (SWG).

You specify a virtual server to process forward proxy traffic with Secure Web Gateway (SWG). This virtual server must listen on the secure connectivity interface that is specified on the virtual server through which network access clients connect. This virtual server is also the one that network access resources must specify as the client proxy server.

Note: *Use this virtual server for forward proxy traffic only. You should not try to use it for reverse proxy, or add a pool to it.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.

3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type the IP address for a host virtual server.

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

   Type a destination address in this format: `162.160.15.20`.
5. In the **Service Port** field, type the port number to use for forward proxy traffic.

   Typically, the port number is `3128` or `8080`.
6. From the **HTTP Profile** list, select the HTTP profile you configured earlier.
7. Scroll down to the **VLAN and Tunnel Traffic** setting and select **Enabled on**.
8. For the **VLANs and Tunnels** setting, move the secure connectivity interface to the **Selected** list.
9. From the **Source Address Translation** list, select **Auto Map**.
10. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
11. In the Access Policy area, from the **Per-Request Policy** list, select the policy that you configured earlier.
12. Click **Finished**.

Creating a wildcard virtual server for HTTP tunnel traffic

You configure a virtual server to process web traffic coming in on the HTTP tunnel from the explicit forward-proxy virtual server.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
5. In the **Service Port** field, type `80`, or select **HTTP** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.
8. Scroll down to the **VLAN and Tunnel Traffic** setting and select **Enabled on**.
9. For the **VLANs and Tunnels** setting, move the tunnel to the **Selected** list.

   The tunnel name must match the tunnel specified in the HTTP profile for the forward proxy virtual server. The default tunnel is **http-tunnel**.
10. From the **Source Address Translation** list, select **Auto Map**.
11. Scroll down to the **Port Translation** setting and clear the **Enabled** check box.
12. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
13. In the Access Policy area, from the **Per-Request Policy** list, select the policy that you configured earlier.
14. Click **Finished**.

Creating a custom Client SSL forward proxy profile

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

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

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

6. Click **Finished**.

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

Creating a custom Server SSL profile

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

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

3. In the **Name** field, type a unique name for the profile.
4. For **Parent Profile**, retain the default selection, **serverssl**.
5. From the **Configuration** list, select **Advanced**.
6. Select the **Custom** check box.
   The settings become available for change.
7. From the **SSL Forward Proxy** list, select **Enabled**.

   You can update this setting later, but only while the profile is not assigned to a virtual server.
8. From the **SSL Forward Proxy Bypass** list, select **Enabled** (or retain the default value **Disabled**).

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

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

Creating a wildcard virtual server for SSL traffic on the HTTP tunnel

If you do not have existing client SSL and server SSL profiles that you want to use, configure them before you start.

You configure a virtual server to process SSL web traffic coming in on the HTTP tunnel from the forward proxy virtual server.

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

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

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

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

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

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

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

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

10. Scroll down to the **VLAN and Tunnel Traffic** setting and select **Enabled on**.
11. For the **VLANs and Tunnels** setting, move the tunnel to the **Selected** list.

    The tunnel name must match the tunnel specified in the HTTP profile for the forward proxy virtual server. The default tunnel is **http-tunnel**.
12. From the **Source Address Translation** list, select **Auto Map**.
13. Scroll down to the **Port Translation** setting and clear the **Enabled** check box.
14. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
15. In the Access Policy area, from the **Per-Request Policy** list, select the policy that you configured earlier.
16. Click **Finished**.

Overview: Configuring SWG explicit forward proxy for network access
Creating a custom Server SSL profile
Updating the access policy in the remote access configuration

Updating the access policy in the remote access configuration

Add an SWG Scheme Assign item to an access policy to assign a Secure Web Gateway (SWG) scheme to a client session. Add queries to populate any session variables that are required for successful execution of the per-request policy.

Note: *Class lookup or group lookup items in a per-request policy rely on session variables that are populated in this access policy.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile that you want to edit. The properties screen opens.
3. Click **Edit Access Policy for Profile** ***profile_name***.
   The visual policy editor opens the access policy in a separate screen.
4. Click the **(+)** icon anywhere in the access policy to add a new action item.

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

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
5. On the Assignment tab, select **SWG Scheme Assign** and click **Add Item**.
   A properties screen opens.
6. To display the available schemes, click the **Add/Delete** link.
7. Select one scheme and click **Save**.
   The Properties screen closes and the visual policy editor screen displays.

8. To supply LDAP group information for use in the per-request policy, add an LDAP Query item anywhere in the access policy and configure its properties:
   a) From the **Server** list, select an AAA LDAP server.
      An LDAP Query uses SSL connections when you select an LDAP AAA server that is configured for LDAPS.
   b) Specify the **SearchDN**, and **SearchFilter** settings.
      SearchDN is the base DN from which the search is done.
   c) Click **Save**.

   This item populates the `session.ldap.last.attr.memberOf` session variable.
9. To supply Active Directory groups for use in the per-request policy, add an AD Query item anywhere in the access policy and configure its properties:
   a) From the **Server** list, select an AAA AD server.
   b) Select the **Fetch Primary Group** check box.
      The value of the primary user group populates the `session.ad.last.attr.primaryGroupID` session variable.
   c) Click **Save**.
10. To supply RADIUS class attributes for use in the per-request policy, add a RADIUS Auth item anywhere in the access policy and configure its properties:
    a) From the **Server** list, select an AAA RADIUS server.
    b) Click **Save**.

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

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

The access policy is configured to assign an SWG scheme and to support the per-request policy.

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

Configuring a network access resource to forward traffic

You must create a network access resource, or open an existing resource, before you can perform this task.

Configure a network access resource to forward traffic to the Secure Web Gateway (SWG) explicit forward proxy virtual server so that SWG can filter Internet traffic and analyze content, protecting the client from malware.

1. On the Main tab, click **Access Policy** > **Network Access** > **Network Access List**.
   The Network Access List screen opens.
2. In the Name column, click the name of the network access resource you want to edit.
3. On the menu bar, click **Network Settings**.
4. For **Client Settings**, select **Advanced**.
5. Scroll down and select **Client Proxy Settings**.
   Additional settings display.
6. If the **Traffic Options** setting specifies **Force all traffic through tunnel**, configure these additional settings:
   a) In the **Client Proxy Address** field, type the IP address of the SWG explicit forward proxy virtual server.
   b) In the **Client Proxy Port** field, type the port number of the SWG explicit forward proxy virtual server.
      Typically, the port number is `3128` or `8080`; it might be different in your configuration.
7. If the **Traffic Options** setting specifies **Use split tunneling for traffic**, in the **Client Proxy Autoconfig Script** field, type the URL for a proxy auto-configuration script.
8. Click the **Update** button.
   Your changes are saved and the page refreshes.

The network access resource forwards traffic to the SWG explicit forward proxy server.

Implementation result

The Secure Web Gateway (SWG) explicit forward proxy configuration is ready to process web traffic from network access clients.

Session variables for use in a per-request policy

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

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

Overview: Configuring SWG transparent forward proxy for remote access

Secure Web Gateway (SWG) can be configured to support remote clients that connect using application access, network access, or portal access.

Note: *Using a distinct SWG transparent forward proxy configuration to process traffic from remote clients separately from an SWG configuration used for processing traffic from internal clients provides an important measure of network security.*

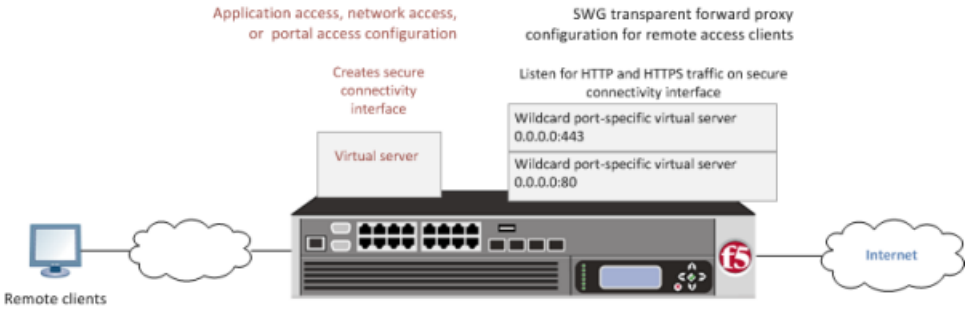


Figure 4: SWG transparent forward proxy for remote access

You should understand how these configuration objects fit into the overall configuration.

Secure connectivity interface

In a remote access configuration, a connectivity profile is required on the virtual server to specify a secure connectivity interface for traffic from the client. In the SWG configuration, SWG wildcard virtual servers must listen on the secure connectivity interface for traffic from remote access clients.

Per-request policy

In any SWG configuration, the determination of whether a user can access a URL must be made in a per-request access policy. A per-request access policy determines whether to block or allow access to a request based on time or date or group membership or other criteria that you configure.

Access policies

The access policy in the remote access configuration continues to authenticate users, assign resources, and evaluate ACLs, if any. In addition, this access policy must assign an SWG scheme for the network access session and populate any session variables used in the per-request policy. An access profile of the SWG-Transparent type is required in the SWG configuration; however, it is not necessary to include any items in the access policy.

Task summary

Creating a connectivity profile
Adding a connectivity profile to a virtual server
Configuring a per-request policy for SWG
Creating an access profile for SWG transparent forward proxy
Creating a wildcard virtual server for HTTP traffic on the connectivity interface
Creating a custom Client SSL forward proxy profile
Creating a custom Server SSL profile
Creating a wildcard virtual server for SSL traffic on the connectivity interface
Updating the access policy in the remote access configuration

Prerequisites

Before you start to create a Secure Web Gateway (SWG) transparent forward proxy configuration to support remote access clients, you must have completed these tasks.

- You need to have configured a working application access, network access, or portal access configuration, depending on which type of remote client you want to support.
- If you have not already done so, you must ensure that the URL database is downloaded.
- You need to have configured at least one SWG scheme and any URL filters that you want to use in addition to or instead of the default URL filters.

Configuration outline

Tasks for integrating an Access Policy Manager® (APM®) remote access configuration with a Secure Web Gateway (SWG) transparent forward proxy configuration follow this order.

- First, update the existing application access, network access, or portal access configuration to add a secure connectivity profile to the virtual server if one is not already specified.
- Next, create an SWG transparent forward proxy configuration. The per-request policy is part of this configuration.
- Finally, update the access policy in the existing application access, network access, or portal access configuration. An SWG scheme assignment is required in this access policy. If the per-request policy uses group or class lookup items, add queries to populate the session variables on which the lookup items rely.

Creating a connectivity profile

You create a connectivity profile to configure client connections.

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Click **Add**.
   The Create New Connectivity Profile popup screen opens and displays General Settings.
3. Type a **Profile Name** for the connectivity profile.
4. Select a **Parent Profile** from the list.
   APM® provides a default profile, **connectivity**.
5. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.

The connectivity profile appears in the list.

To provide functionality with a connectivity profile, you must add the connectivity profile to a virtual server.

Adding a connectivity profile to a virtual server

Update a virtual server that is part of an Access Policy Manager® application access, network access, or portal access configuration to enable a secure connectivity interface for traffic from the client.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.

The Virtual Server List screen opens.

2. Click the name of the virtual server you want to modify.
3. Scroll down to the Access Policy area.
4. From the **Connectivity Profile** list, select the connectivity profile.
5. Click **Update** to save the changes.

Configuring a per-request policy for SWG

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

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

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

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

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

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

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

   a) Click the **(+)** icon anywhere in the per-request policy to add a new item.
      A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
   b) Type `cat` in the Search field, select **Category Lookup**, and click **Add Item**.
      A Properties popup screen opens.
   c) From the **Categorization Input** list, select how to obtain the requested URL. For HTTP traffic, select **Use HTTP URI (cannot be used for SSL Bypass decisions)**. For SSL-encrypted traffic,

select either **Use SNI in Client Hello (if SNI is not available, use Subject.CN)** or **Use Subject.CN in Server Cert**.
If you select **Use HTTP URI (cannot be used for SSL Bypass decisions)**, the **SafeSearch Mode** list displays and **Enabled** is selected.

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

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

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

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

10. Add any of these items to the policy.

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

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

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

b) Click the Branch Rules tab.

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

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

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

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

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

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

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

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

A Category Lookup item must precede this item.

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

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

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

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

The popup screen closes. The visual policy editor displays.

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

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

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

Creating an access profile for SWG transparent forward proxy

You create an access profile to supply an access policy.

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

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

4. From the **Profile Type** list, select **SWG-Transparent**.
   Additional fields display set to default values.
5. In the Language Settings area, add and remove accepted languages, and set the default language.

   A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.
6. Click **Finished**.
   The Access Profiles list screen displays.
7. To enable Secure Web Gateway event logging for this access profile, add log settings.
   a) Click the name of the access profile that you just created.
      The Properties screen displays.
   b) On the menu bar, click **Logs**.
      The General Properties screen displays.
   c) In the Log Settings area, move log settings from the **Available** list to the **Selected** list.

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

This creates an access profile with a default access policy that contains a **Start** and a **Deny** ending.

You do not need to add any actions or make any changes to the access policy.

Creating a wildcard virtual server for HTTP traffic on the connectivity interface

Before you begin, you need to know the name of the connectivity profile specified in the virtual server for the remote access configuration that you want Secure Web Gateway (SWG) to protect.

You configure a virtual server to process web traffic on the secure connectivity interface for a remote access client.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
5. In the **Service Port** field, type `80`, or select **HTTP** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.
8. Scroll down to the **VLAN and Tunnel Traffic** setting and select **Enabled on**.
9. For the **VLANs and Tunnels** setting, move the secure connectivity interface to the **Selected** list.
10. From the **Source Address Translation** list, select **Auto Map**.
11. Scroll down to the **Port Translation** setting and clear the **Enabled** check box.
12. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
13. In the Access Policy area, from the **Per-Request Policy** list, select the policy that you configured earlier.
14. Click **Finished**.

Creating a custom Client SSL forward proxy profile

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

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

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

6. Click **Finished**.

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

Creating a custom Server SSL profile

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

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

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

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

Creating a wildcard virtual server for SSL traffic on the connectivity interface

Before you begin, you need to know the name of the connectivity profile specified in the virtual server for the remote access configuration that you want Secure Web Gateway (SWG) to protect. Also, if you do not have existing client SSL and server SSL profiles that you want to use, configure them before you start.

You configure a virtual server to process SSL web traffic coming in on the secure connectivity interface for a remote access client.

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

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

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

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

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

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

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

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

10. Scroll down to the **VLAN and Tunnel Traffic** setting and select **Enabled on**.
11. For the **VLANs and Tunnels** setting, move the secure connectivity interface to the **Selected** list.
12. From the **Source Address Translation** list, select **Auto Map**.
13. Scroll down to the **Port Translation** setting and clear the **Enabled** check box.
14. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
15. In the Access Policy area, from the **Per-Request Policy** list, select the policy that you configured earlier.
16. Click **Finished**.

Updating the access policy in the remote access configuration

Add an SWG Scheme Assign item to an access policy to assign a Secure Web Gateway (SWG) scheme to a client session. Add queries to populate any session variables that are required for successful execution of the per-request policy.

Note: *Class lookup or group lookup items in a per-request policy rely on session variables that are populated in this access policy.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile that you want to edit. The properties screen opens.
3. Click **Edit Access Policy for Profile** ***profile_name***.
   The visual policy editor opens the access policy in a separate screen.
4. Click the **(+)** icon anywhere in the access policy to add a new action item.

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

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
5. On the Assignment tab, select **SWG Scheme Assign** and click **Add Item**.
   A properties screen opens.
6. To display the available schemes, click the **Add/Delete** link.
7. Select one scheme and click **Save**.
   The Properties screen closes and the visual policy editor screen displays.
8. To supply LDAP group information for use in the per-request policy, add an LDAP Query item anywhere in the access policy and configure its properties:
   a) From the **Server** list, select an AAA LDAP server.

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

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

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

c) Click **Save**.

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

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

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

   c) Click **Save**.

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

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

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

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

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

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

The access policy is configured to assign an SWG scheme and to support the per-request policy.

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

Implementation result

The Secure Web Gateway (SWG) transparent proxy configuration is ready to process web traffic from remote access clients.

Session variables for use in a per-request policy

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

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

Index

L

N

O

P

S

T

V

W