websense
ESSENTIAL INFORMATION PROTECTION™

Configuration Guide

F5 BIG-IP Local Traffic Manager and
Websense® Web Security Gateway or Websense TRITON® AP-WEB

F5 BIG-IP Local Traffic Manager and Websense Web Security Gateway or Websense TRITON AP-WEB

Every effort has been made to ensure the accuracy of this manual. Websense, Inc. does not warrant or guarantee the accuracy of the information provided herein. Websense, Inc. makes no warranties with respect to this documentation and disclaims any implied warranties including, without limitation, warranties of merchantability, noninfringement, and fitness for a particular purpose, or those arising from a course of dealing, usage, or trade practice. All information provided in this guide is provided "as is," with all faults, and without warranty of any kind, either expressed or implied or statutory. Websense, Inc. shall not be liable for any error or for damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Third-party product descriptions and related technical details provided in this document are for information purposes only and such products are not supported by Websense, Inc.

Contents

1 Configuration Guide

Introduction

Configuration Guide | F5 BIG-IP Local Traffic Manager and Websense Web Security Gateway or TRITON AP-WEB

This guide provides step-by-step procedures for configuring F5 BIG-IP Local Traffic Manager (LTM) devices with Websense® Web Security Gateway or Websense TRITON® AP-WEB.

✓ **Note**

Websense product names and bundles changed in 8.0.0. See the v8.0.0 Release Notes for TRITON APX Solutions.

Web Security Gateway and TRITON AP-WEB each provide the defenses you need to defend against advanced attacks: real-time threat analysis at web gateways, plus forensic reporting. Combined with BIG-IP LTM, a security gateway infrastructure gains the capability to be:

- Easily scaled to meet the demands for high traffic levels common to eEnterprise deployments.
- Expanded to accommodate new Web Security Gateway or TRITON AP-WEB cluster members with a simple menu-driven configuration update.
- Monitored closely for any conditions that might affect the availability of the eEnterprise gateway, ensuring continuous traffic flow.
- Used for any configurable authentication mechanism (NTLM and Kerberos) transparently.
- Deployed easily in both transparent and explicit proxy modes.

New to BIG-IP version 11, F5 iApp is a powerful new set of features in the BIG-IP system that provides a new way to architect application delivery in the data center, and it includes a holistic, application-centric view of how applications are managed and delivered inside, outside, and beyond the data center. The iApp templates for Websense applications act as the single-point interface for building, managing, and monitoring these servers.

For more information on iApp, see the White Paper “F5 iApp: Moving Application Delivery Beyond the Network”: http://www.f5.com/pdf/white-papers/f5-iapp-wp.pdf.

For more information on Websense Web Security Gateway or TRITON AP-WEB , see http://www.websense.com/.

For more information on the F5 devices described in this guide, see http://www.f5.com/products/big-ip/.

Prerequisites and configuration notes

Configuration Guide | F5 BIG-IP Local Traffic Manager and Websense Web Security Gateway or TRITON AP-WEB

iApp Downloads

Some components need to be downloaded in order to assist you in configuring your environment.

Websense Content Gateway Assistant iApp.

This component will allow you to configure an integrated environment for explicit and transparent proxy in combination with a Websense appliance (e.g., Websense V10000™ appliance). Use this if you want to route traffic through your Websense appliance directly, or if you are managing the traffic configuration of a cluster of Websense appliances.

https://devcentral.f5.com/wiki/iApp.Websense-Content-Gateway-Assistant-iApp.ashx

Generic forward proxy with the Websense Filtering iApp

This app is for configuring a simple, anonymous HTTP or SOCKS4/5 proxy that uses the Websense Filtering Service for blocking threats and enforcing policy. Use this iApp if you want to create a simple blocking proxy without routing traffic through the Websense appliance directly. This functionality is good for providing basic proxy filtering for guest networks.

https://devcentral.f5.com/wiki/iApp.Generic-Forward-Proxy-with-Websense-Filtering-iApp.ashx

Requirements

Configuration Guide | F5 BIG-IP Local Traffic Manager and Websense Web Security Gateway or TRITON AP-WEB

F5 LTM

Software

BIG-IP LTM must be running version 11.3 or later. We recommend using version 11.3 or later in order to be compatible with both Websense iApps.

- Websense Content Gateway Assistant iApp: Supported beginning with version 11.3.
- Generic forward proxy with Websense Filtering iApp: Supported beginning with version 11.3.

Hardware

There are no specific hardware recommendations; these configuration iApps are compatible with all hardware appliances known to run the recommended BIG-IP Traffic Management Operating System (TMOS) versions, including Virtual Edition.

Websense

Software

We recommend using Websense software that is version 7.7.3 or greater. This version contains special health monitoring tools that we can utilize to check the proper operation of your proxy instance that previous versions do not contain.

- **Websense Content Gateway Assistant iApp**: Version 7.7 or above is recommended. For extended health monitoring capabilities, version 7.7.3 or greater is highly desired.
- **Generic forward proxy with Websense Filtering iApp**: Version 7.6 or above is recommended. In order to use extended health monitoring capabilities, version 7.7.3 or greater is highly desired.

Hardware

There are no specific hardware recommendations.

General

The following items are generally recommended before starting your deployment:

- You should have a thorough understanding of your Websense configuration and its relation to your desired network topology before beginning your deployment. In particular, carefully consider your network's traffic routing; it is likely that you will need to make one or more changes in order to complete your task.
- This guide is not intended to replace Websense documentation or best practices, merely to supplement them with enough information to enable you to easily configure this particular integration. You should not begin a new Websense deployment using this document. Refer to http://www.websense.com/content/support/library/deployctr/v81/first.aspx for up-to-date information about your Websense deployment.

- If you use user authentication with your Websense installation, ensure that you pay attention to the configuration instructions related to configuration changes needed on the Websense platform to prevent repeated authentication.

Product versions and revision history

Configuration Guide | F5 BIG-IP Local Traffic Manager and Websense Web Security Gateway or TRITON AP-WEB

Product and versions tested for this guide:

Product Tested	Version Tested
BIG-IP LTM	11.3, 11.4, and 11.5
Websense	7.6, 7.7 or higher (applicable to generic proxy iApp) 7.7 or higher (applicable to Websense Assistant iApp)

Revision history for this document:

Version	Comment	Author
1.0	Initial release	JM

Configuration examples

Configuration Guide | F5 BIG-IP Local Traffic Manager and Websense Web Security Gateway or TRITON AP-WEB

Before continuing, you should select the type of integrated deployment that suits your environment. BIG-IP supports several deployment modes for Websense integration.

Explicit Proxy - Websense

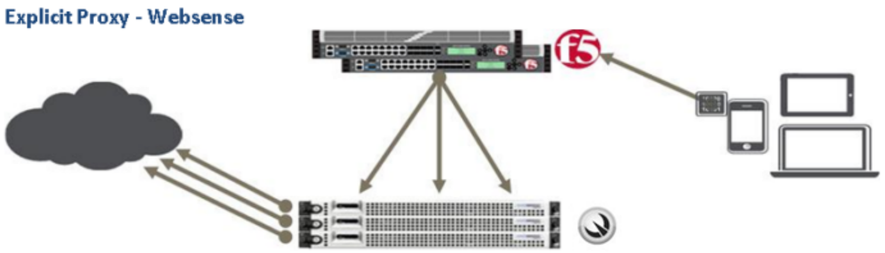


Figure 1. Explicit proxy configuration (Websense-routed)

This mode allows you to configure your network's web browser clients to use the BIG-IP Virtual Server as a direct HTTP proxy, or to define the created virtual address within a proxy auto-configuration that is distributed via DNS or DHCP.

If you use this particular mode, you must ensure that your browser clients are either manually configured or that you have correctly set up an auto-configuration mechanism that will serve them.

This explicit proxy configuration will route traffic **through** the Websense appliance. To begin, turn to the "Configuring using Websense Content Gateway Assistant" configuration section of this document.

Transparent Proxy - Websense

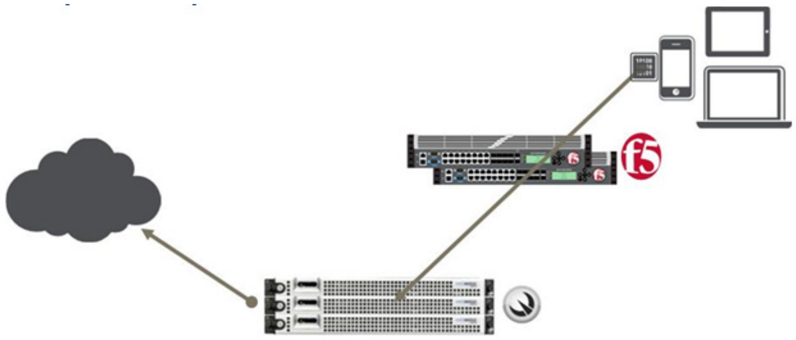


Figure 2. Transparent proxy configuration (Websense-routed)

This mode allows you to redirect select traffic from your network's web browser clients transparently through the Websense appliance cluster.

This mode ensures that you do not need to distribute any configuration changes to your clients, but may require routing changes to your network. To begin, turn to the "Configuring using Websense Content Gateway Assistant" configuration section of this document.

Explicit (or SOCKS) Proxy - BIG-IP

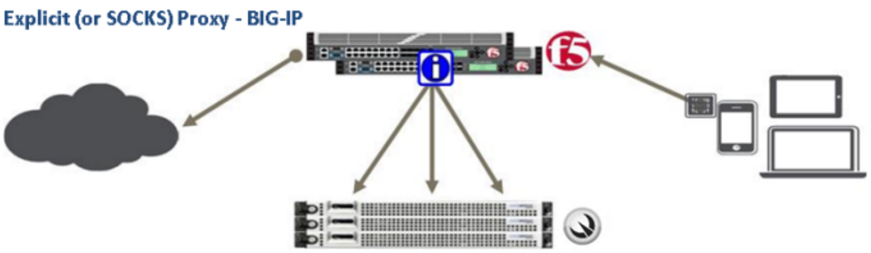


Figure 3. Explicit proxy (BIG-IP-routed)

This mode allows you to configure your network's web browser clients to use the BIG-IP Virtual Server as an HTTP proxy, or to define the created virtual address within a proxy auto-configuration that is distributed via DNS or DHCP.

If you use this particular mode, you must ensure that your browser clients are either manually configured or that you have correctly set up an auto-configuration mechanism that will serve them.

This explicit proxy configuration will route traffic through the BIG-IP, but will ask the Websense appliance for blocking decisions. To begin, turn to the "Configuring using generic proxy with Websense Support" configuration section of this document.

Configuring using Websense Content Gateway Assistant

Configuration Guide | F5 BIG-IP Local Traffic Manager and Websense Web Security Gateway or TRITON AP-WEB

Refer to the following for guidance on how to configure the BIG-IP system for the modes described by Figures 1 and 2 in the section "Configuration examples" using the iApp template described on page 1 of this document.

Getting started with the iApp

To begin using the Websense Content Gateway Assistant iApp, you must import it and then create an application from the template.

1. Unpack the template file from the Zip archive that you downloaded as part of the requirements section. The template file will be named:

   `f5.websense_cg_assistant_<version>_<date>.tmpl`
2. Log on to the BIG-IP system.
3. On the Main tab, expand **iApp**, and then c lick Templates.
4. Click the **Import…** button at the top of the main window.
5. Click **Browse…** and select the template file from your file system in the window provided. If you have previously imported an earlier version of the iApp template, you may also check the box next to **Overwrite Existing Templates** to ensure that the newest version of the template is imported over the old one.
6. Once the template is imported, you can begin using it to create applications. On the main tab, click **Application Services** under the **iApp** tab.
7. Click **Create**. The template selection page will open.
8. In the **Name** box, type in the name you wish to use to describe this deployment (i.e., "websense_datacenter").
9. From the **Template** list, select **f5.websense_content_gateway**.

Advanced options

If you select **Advanced** from the Template Selection list, you see Sync and Failover options for the application. This feature, new to v11, is a part of the Device Management configuration. This functionality extends the existing High Availability infrastructure and allows for clustering, granular control of configuration synchronization, and granular control of failover. For more information on Device Management, see the Online Help or product documentation.

1. **Configure Sync/Failover?**

   If you want to configure the Application for Sync or failover groups, select **Yes** from the list.

   a. **Device Group**

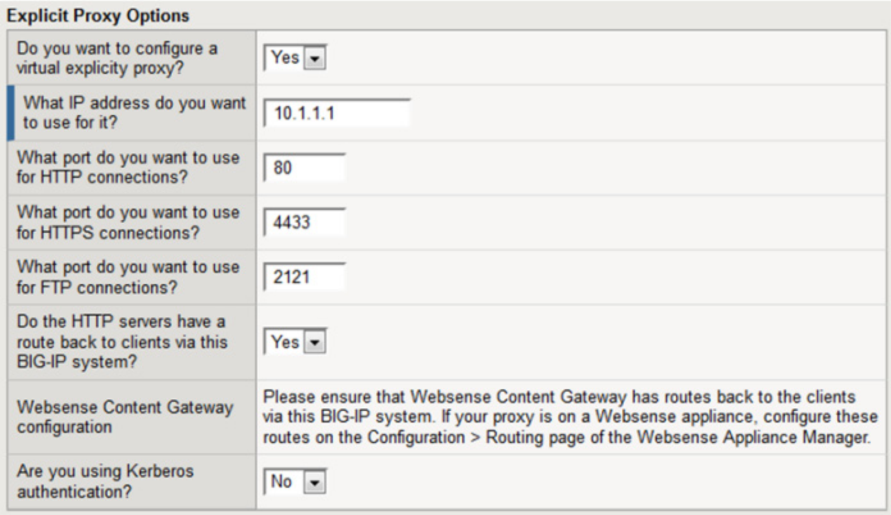
   If you select **Yes** from the question above, the Device Group and Traffic Group options appear. If necessary, uncheck the **Device Group** box and then select the appropriate Device Group from the list.

   b. **Traffic Group**

   If necessary, uncheck the **Traffic Group** box and then select the appropriate Traffic Group from the list.

Explicit Proxy Options

The next section allows you to select whether you wish to configure the explicit proxy mode for your Websense deployment. This mode creates a set of virtual servers with which your browser clients will interact for Internet access. A virtual server is a traffic-management object on the BIG-IP system that is represented by an IP address and a service. Clients can send application traffic to a virtual server, which then directs the traffic according to your configuration instructions.



Explicit Proxy Options

Do you want to configure a virtual explicity proxy?	Yes
What IP address do you want to use for it?	10.1.1.1
What port do you want to use for HTTP connections?	80
What port do you want to use for HTTPS connections?	4433
What port do you want to use for FTP connections?	2121
Do the HTTP servers have a route back to clients via this BIG-IP system?	Yes
Websense Content Gateway configuration	Please ensure that Websense Content Gateway has routes back to the clients via this BIG-IP system. If your proxy is on a Websense appliance, configure these routes on the Configuration > Routing page of the Websense Appliance Manager.
Are you using Kerberos authentication?	No

Figure 4: Explicit proxy options

If you do not wish to configure this functionality answer **No** to the first question in this section, and proceed to the section "Transparent Proxy Options."

1. **IP Address Configuration**: This is the address clients use to access this explicit TRITON AP-WEB proxy (or a FQDN will resolve to this address). You need an available IP address to use here.
2. **Port Configuration**: You can configure the explicit proxy to listen on different ports for certain services. Under normal conditions, most services will be available on the port assigned to HTTP; however, you may find it convenient to assign alternate ports per service (for HTTPS and FTP, for example).
3. **Routing Configuration**: If the Websense servers do not have a route back for clients through the BIG-IP, i.e., if they do not use the BIG-IP as the default gateway, the BIG-IP uses Secure Network Address Translation (SNAT) Automap to translate the client's source address to an address configured on the BIG-IP. The Websense servers then use this new source address as the destination address when responding to traffic originating through the BIG-IP.

   If you indicate the servers do have a route back to the clients through the BIG-IP, the BIG-IP does not translate the client's source address; in this case, you must make sure the BIG-IP is configured as the gateway to the client networks (usually the default gateway) on the servers. Please ensure that Websense Web Security Gateway or TRITON AP-WEB has routes back to the clients via this BIG-IP system. If your proxy is on a Websense appliance, configure these routes on the **Configuration** > **Routing** page of the Websense appliance manager.

   We recommend choosing **No** from the list because it is secure and does not require you to configure routing manually.
4. **Large-Scale Connections (Routing Configuration)**: If you have selected **No** to the option to translate the source of the connection using SNAT, then you have the option to configure for supporting larger connection pools if you need to do so.

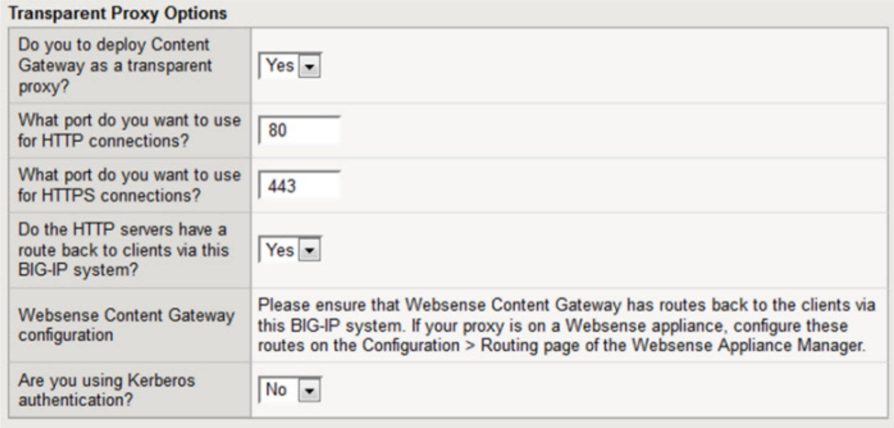
   If you do not expect more than 64,000 simultaneous connections, leave this answer set to No and continue with #5. If you have a large deployment and expect more than 64,000 connections at one time, the iApp creates a SNAT Pool instead of using SNAT Automap. With a SNAT Pool, you need one IP address for each 64,000 connections you expect.

   Select **Yes** from the list. A new row appears with an IP address field. In the **Address** box, type an IP address and then click **Add**. Repeat for any additional IP addresses.
5. **Kerberos Authentication**: If Websense Web Security Gateway or TRITON AP-WEB is configured to authenticate users using Kerberos, you must apply a special configuration to your gateway cluster so that it can be seen with a common name to your authentication server infrastructure. If you need this configuration, you should contact Websense Support for assistance.

Transparent proxy options

This section allows you to select whether you wish to configure transparent proxy mode for your Websense deployment. This mode creates a set of "wildcard" virtual servers that will take traffic that comes into a specified VLAN and redirect it to

Websense transparently. Clients do not need to be configured to connect directly to the proxy in this scenario.



Transparent Proxy Options

Do you to deploy Content Gateway as a transparent proxy?	Yes
What port do you want to use for HTTP connections?	80
What port do you want to use for HTTPS connections?	443
Do the HTTP servers have a route back to clients via this BIG-IP system?	Yes
Websense Content Gateway configuration	Please ensure that Websense Content Gateway has routes back to the clients via this BIG-IP system. If your proxy is on a Websense appliance, configure these routes on the Configuration > Routing page of the Websense Appliance Manager.
Are you using Kerberos authentication?	No

Figure 5: Transparent proxy options

If you do not wish to configure this functionality answer **No** to the first question in this section, and proceed to the section “Websense Server Pool, Load Balancing, and Service Monitor.”

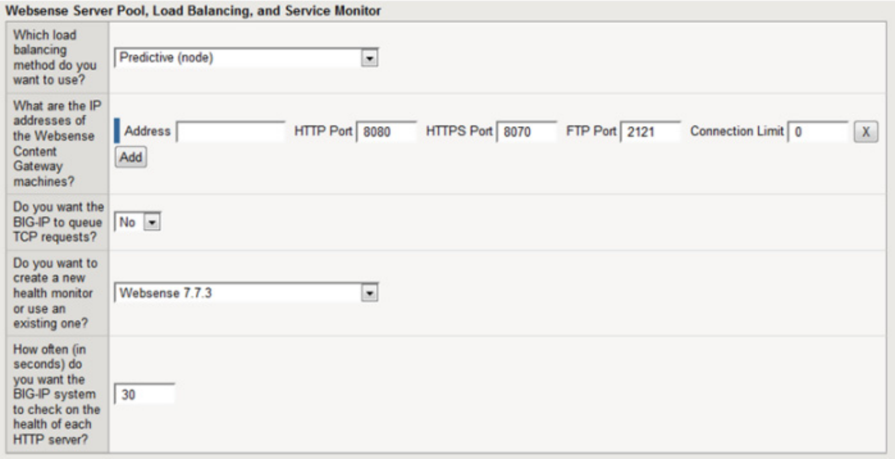
1. **Port Configuration**: You can configure the transparent proxy to listen on different ports for certain services. We recommend this not be changed from the default settings for each listed service (80 for HTTP, 443 for HTTPS). However, if you wish to support outgoing connections on alternate ports, you may change these here.
2. **Large-Scale Connections (Routing Configuration)**: If you have selected **No** to the option to translate the source of the connection using SNAT, then you have the option to configure for supporting larger connection pools if you need to do so.

   If you do not expect more than 64,000 simultaneous connections, leave this answer set to **No,** and continue with #5. If you have a large deployment and expect more than 64,000 connections at one time, the iApp creates a SNAT Pool instead of using SNAT Automap. With a SNAT Pool, you need one IP address for each 64,000 connections you expect.

   Select **Yes** from the list. A new row appears with an IP address field. In the Address box, type an IP address and then click **Add**. Repeat for any additional IP addresses.
3. **Kerberos Authentication**: If Websense Web Security Gateway or TRITON AP-WEB is configured to authenticate users using Kerberos, clients must be able to connect to the gateway using their configured hostnames. If necessary, select **Yes** to create the individual virtual servers.

Websense server pool, load balancing, and service monitor

In this section, we will configure the Websense Web Security Gateway or TRITON AP-WEB cluster pool that the BIG-IP will manage, as well as define how we determine server health and distribute the load across the cluster.



Websense Server Pool, Load Balancing, and Service Monitor

Which load balancing method do you want to use?	Predictive (node)
What are the IP addresses of the Websense Content Gateway machines?	Address HTTP Port 8080 HTTPS Port 8070 FTP Port 2121 Connection Limit 0
Do you want the BIG-IP to queue TCP requests?	No
Do you want to create a new health monitor or use an existing one?	Websense 7.7.3
How often (in seconds) do you want the BIG-IP system to check on the health of each HTTP server?	30

Figure 6: Websense server pool setup

Please note that the default settings are the **Recommended** settings for a Websense Web Security Gateway or TRITON AP-WEB server deployment. If you wish to change from the default settings, please ensure that the matching configuration exists in your Websense server configuration before you apply it.

1. **Load Balancing**: While you can choose any of the load balancing methods BIG-IP supports from the list, we recommend the default, Predictive (node). Note that although all methods are available, any method that is not “node” based may result in higher server workload if transparent mode proxy is selected.
2. **Pool Configuration**: Type in the IP address and port configuration for each Websense server. The default port configuration is:
    a. **HTTP** port 8080
    b. **HTTPS** port 8070
    c. **FTP** port 2121

    Please note that these are Websense defaults and should not be changed unless your Websense configuration has been customized.

    By default, we do not configure a connection limit for any pool member (by default, the connection limit is “0”, which means this functionality is disabled). You can specify a connection limit for this pool member if you wish. Enter the number of concurrent connections to which you wish to limit the individual pool member. If you choose to use TCP request queuing features (below), you must set a connection limit for each pool member.
3. **TCP Request Queuing**: TCP request queuing provides the ability to queue connection requests that exceed the capacity of connections for a pool as determined by the connection limit. Consequently, instead of dropping connection requests that exceed the capacity of a pool, TCP request queuing enables those connection requests to reside within a queue in accordance with defined conditions until capacity becomes available. For more information on TCP request queuing, see the “New Features Guide for BIG-IP Version 11,” available on Ask F5, the F5 knowledge base.

By default, TCP request queuing is disabled.

If you want the BIG-IP to queue TCP requests, select **Yes** from the list. Additional options appear.

a. Type a queue length in the box. Leave the default of 0 for unlimited.

b. Type a number of milliseconds for the timeout value.

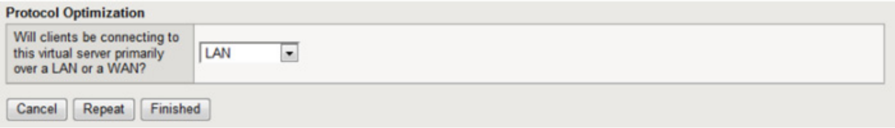
4. **Health Monitor**: Each Websense Content Gateway will be monitored by a custom health monitor on a scheduled basis. To configure this monitoring, select the version of Websense Content Gateway software that your cluster members are running from the list.

   Although it is not recommended, if you do not want to use the preconfigured monitors, then select **Custom** or **Use Monitor…** from the dropdown and choose the monitor you want to employ.

5. **Monitor Interval**: Enter the number of **Seconds** that will elapse between each check of a single Websense cluster member. We recommend a default of no greater than 30 seconds.

Protocol Optimization

In this last section, we will configure the communication between the browser client and the BIG-IP so that it will be fully optimized for the network it serves.



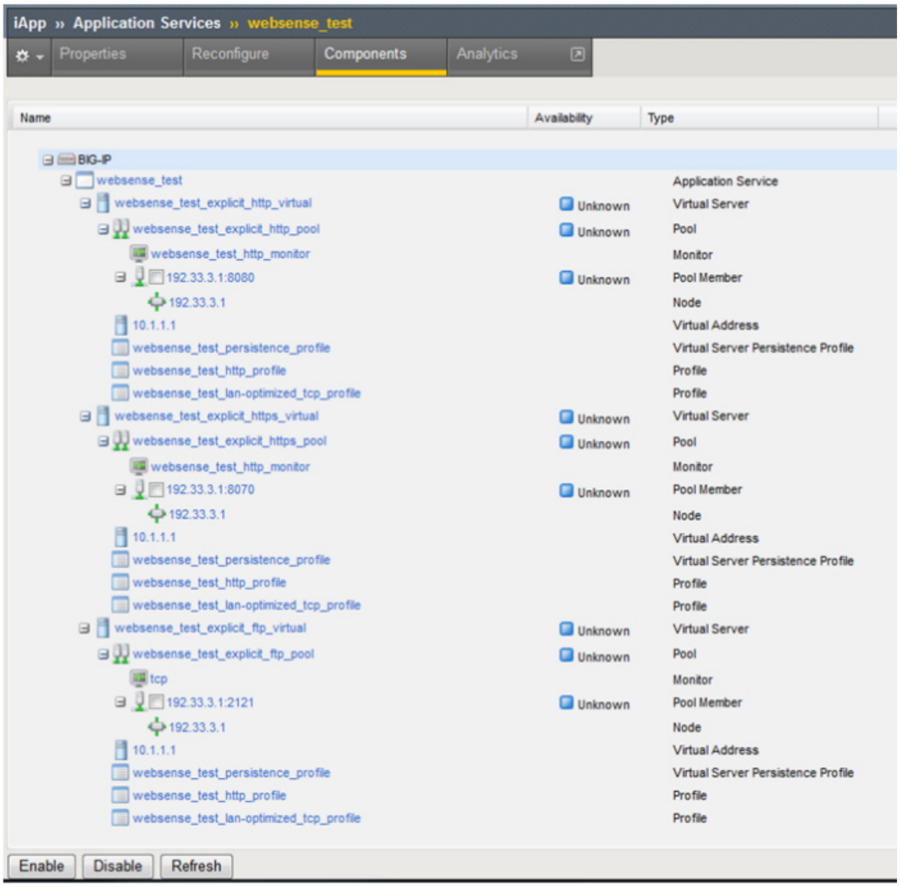
Protocol Optimization

Will clients be connecting to this virtual server primarily over a LAN or a WAN? LAN

Figure 7: Protocol optimization settings

Select either **WAN** or **LAN** from the dropdown menu. If most of your browser clients are accessing via a LAN, then configuring this will apply special optimizations that will make the connection work better over a shorter network distance. If your network involves any longer-distance routing, choose **WAN**.

When you click **Finished**, the iApp will then build your configuration as seen in Figure 8.



Name	Availability	Type
BIG-IP		
websense_test		Application Service
websense_test_explicit_http_virtual	Unknown	Virtual Server
websense_test_explicit_http_pool	Unknown	Pool
websense_test_http_monitor		Monitor
192.33.3.1:8080	Unknown	Pool Member
192.33.3.1		Node
10.1.1.1		Virtual Address
websense_test_persistence_profile		Virtual Server Persistence Profile
websense_test_http_profile		Profile
websense_test_lan-optimized_tcp_profile		Profile
websense_test_explicit_https_virtual	Unknown	Virtual Server
websense_test_explicit_https_pool	Unknown	Pool
websense_test_http_monitor		Monitor
192.33.3.1:8070	Unknown	Pool Member
192.33.3.1		Node
10.1.1.1		Virtual Address
websense_test_persistence_profile		Virtual Server Persistence Profile
websense_test_http_profile		Profile
websense_test_lan-optimized_tcp_profile		Profile
websense_test_explicit_ftp_virtual	Unknown	Virtual Server
websense_test_explicit_ftp_pool	Unknown	Pool
tcp		Monitor
192.33.3.1:2121	Unknown	Pool Member
192.33.3.1		Node
10.1.1.1		Virtual Address
websense_test_persistence_profile		Virtual Server Persistence Profile
websense_test_http_profile		Profile
websense_test_lan-optimized_tcp_profile		Profile

Figure 8: A completed Websense Web Security Gateway or TRITON AP-WEB configuration

Configuring using generic proxy with Websense Support

Configuration Guide | F5 BIG-IP Local Traffic Manager and Websense Web Security Gateway or TRITON AP-WEB

Refer to the following for guidance on how to configure the BIG-IP system for the modes described by Figures 1 and 2 in the section “Configuration examples” using the iApp template described on page 1 of this document.

Features

This iApp implements a simple anonymous HTTP (CONNECT) or SOCKS 4/4a/5 foward proxy virtual server, and has the following features:

- Support for Websense Web Security and Web Filtering
- Menu-driven proxy autoconfiguration file generation
- Simple network-based restriction of proxy use
- Control of allowed ports-per-protocol

- Support for dynamic FTP PASV (passive move) mapping
- Simple name resolution caching from a pool of configured DNS resolvers
- Informative error pages
- Extended enforcement of SSL blocking through confirmation of Server Name Indication

Limitations

This implementation of a forward proxy uses a set of iRules to create a proxy directly on the BIG-IP LTM. There are some limitations to this particular proxy implementation that you should understand before configuring it.

- This proxy does not support user authentication at this time. All proxy operations (HTTP or SOCKS) are anonymous in nature.
- The SOCKS proxy does not support user datagram protocol (UDP) association mode.
- This proxy is intended for limited use (i.e., limited guest access requiring filtering, test lab functionality, development environments).

Getting started with the iApp

To begin using the Websense Content Gateway Assistant iApp, you must import it and then create an application using the iApp template.

1. Unpack the template file from the Zip archive that you downloaded as part of the requirements section. The template file will be named:

   `f5.forward_proxy_<version>_<date>.tmpl`
2. Log onto the BIG-IP system.
3. On the Main tab, expand **iApp**, and then c lick **Templates**.
4. Click the **Import…** button at the top of the main window.
5. Click **Browse…** and select the template file from your file system in the window provided. If you have previously imported an earlier version of the iApp template, you may also check the box next to **Overwrite Existing Templates** to ensure that the newest version of the template is imported over the old one.
6. Once the template is imported, you can begin using it to create applications. On the main tab, click **Application Services** under the **iApp** tab.
7. Click **Create**. The template selection page will open.
8. In the **Name** box, type in the name you wish to use to describe this deployment (i.e., “websense_datacenter”).
9. From the **Template** list, select **f5.forward_proxy**.

Advanced options

If you select **Advanced** from the Template Selection list, you see Sync and Failover options for the application. This feature, new to v11, is a part of the Device Management configuration. This functionality extends the existing High Availability infrastructure and allows for clustering, granular control of configuration synchronization, and granular control of failover. For more information on Device Management, see the Online Help or product documentation.

1. **Configure Sync/Failover?**

   If you want to configure the Application for Sync or failover groups, select **Yes** from the list.

   a. **Device Group**

   If you select **Yes** from the question above, the Device Group and Traffic Group options appear. If necessary, uncheck the Device Group box and then select the appropriate Device Group from the list.

   b. **Traffic Group**

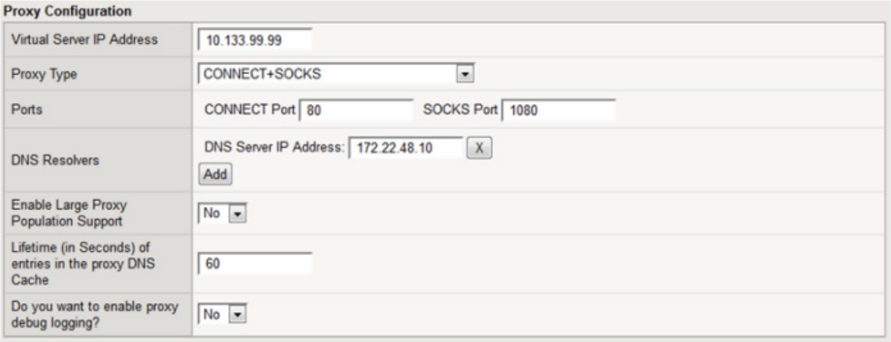
   If necessary, uncheck the Traffic Group box and then select the appropriate Traffic Group from the list.

Inside the iApp, you can also enable advanced options specific to the proxy deployment. If you wish to do so, select **Yes** to the Advanced Options question below the iApp description. This will show the following optional features:

- Large Proxy Population Support (SNAT Pool)
- Proxy Debug Logging

Proxy configuration

In this section, you will configure your BIG-IP proxy's type, address, and ports.



Proxy Configuration

Virtual Server IP Address	10.133.99.99
Proxy Type	CONNECT+SOCKS
Ports	CONNECT Port 80 SOCKS Port 1080
DNS Resolvers	DNS Server IP Address: 172.22.48.10 X Add
Enable Large Proxy Population Support	No
Lifetime (in Seconds) of entries in the proxy DNS Cache	60
Do you want to enable proxy debug logging?	No

Figure 9: Main proxy configuration options

You will need to select the type of proxy you wish to deploy – SOCKS or CONNECT (HTTP). You can configure both simultaneously should you wish to accommodate both types of clients on your network.

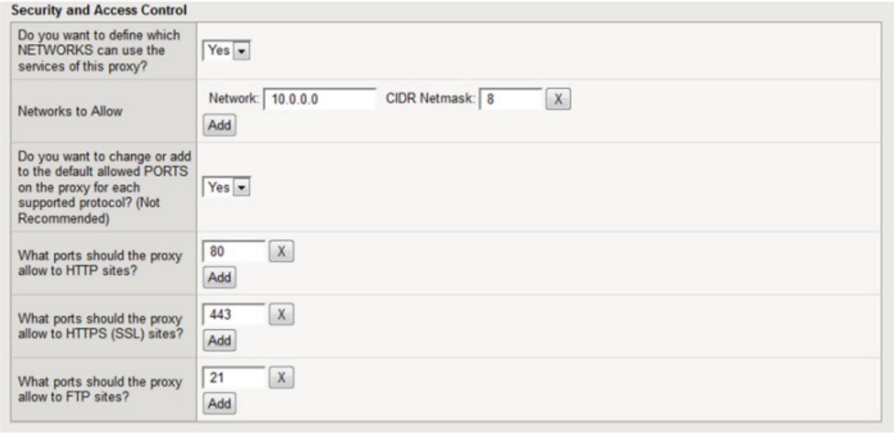
1. **Virtual Server IP Address**: This is the address clients use to access this explicit proxy (or a FQDN will resolve to this address). You need an available IP address to use here.
2. **Proxy Type**: If you wish to enable both HTTP and SOCKS proxies, select **CONNECT+SOCKS** from the dropdown menu. Otherwise you can select **CONNECT Only** or **SOCKS Only** for a single-type configuration.
3. **Port Configuration**: You can configure the explicit proxy to listen on different ports for each type of proxy being performed. If you've selected **CONNECT+SOCKS** in the above step, then you can configure one port per proxy type. By default, CONNECT proxy traffic will use port **80** and SOCKS proxy traffic will use port **1080.** You may assign different ports if you wish.
4. **DNS Resolvers**: Because explicit proxies are typically deployed in environments with little or no access to resolve names external to the network, we must resolve all hostnames that are sent to the proxy. To do this, we will create a pool of external-facing resolvers and send all hostname lookups to them. Enter a DNS Server IP address in the box; if multiple resolvers are desired, click **Add** and enter another IP address in the resulting box. Continue until you've added the desired number of resolvers.
5. **Large Proxy Population Support (Advanced Mode Only)**: The BIG-IP uses Secure Network Address Translation (SNAT) Automap to translate the client's source address to an address configured on the BIG-IP when sending the connection to an external network.

   If you do not expect more than 64,000 simultaneous connections, leave this answer set to No and continue with #6. If you have a large deployment and expect more than 64,000 connections at one time, the iApp creates a SNAT Pool instead of using SNAT Automap. With a SNAT Pool, you need one IP address for each 64,000 connections you expect.

   Select **Ye**s from the list. A new row appears with an IP address field. In the **Address** box, type an IP address and then click **Add**. Repeat for any additional IP addresses.
6. **Proxy DNS Cache Lifetime (Advanced Mode Only)**: By default, the BIG-IP iApp proxy will cache hostname lookup results for a short amount of time (30 seconds) to reduce the number of lookups that need to go to the DNS resolvers. You may modify this setting if you wish, although this is not recommended.
7. **Debug Logging (Advanced Mode Only)**: If you are experiencing any issues with a particular website through the BIG-IP iApp proxy, you can enable debug logging to get additional details for community support purposes. Do NOT enable this debug logging in a busy environment, as it will quickly fill up the local BIG-IP log.

Security and access control

This section allows you to configure the networks that can access the proxy and the ports that the explicit proxy will allow through for each supported service.



Security and Access Control

Do you want to define which NETWORKS can use the services of this proxy?	Yes ▾
Networks to Allow	Network: 10.0.0.0 CIDR Netmask: 8 X Add
Do you want to change or add to the default allowed PORTS on the proxy for each supported protocol? (Not Recommended)	Yes ▾
What ports should the proxy allow to HTTP sites?	80 X Add
What ports should the proxy allow to HTTPS (SSL) sites?	443 X Add
What ports should the proxy allow to FTP sites?	21 X Add

Figure 10: Security and access control section

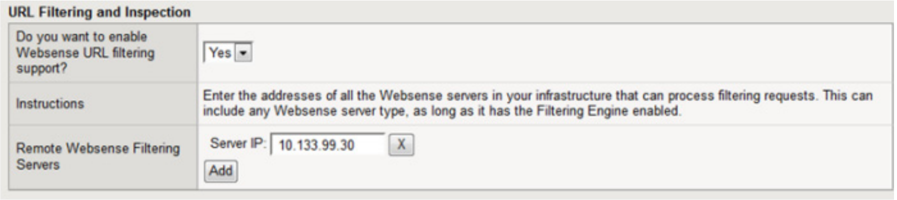
1. **Network Access Control**: If you wish to define the networks allowed to use this proxy instance, then select Yes from the dropdown list.
2. Under **Networks to Allow**, enter the network and CIDR netmask of each network that can use the proxy instance. If you need more than one, click **Add** and enter an additional network; repeat if needed.
3. **Port Access Control**: An explicit proxy may find that browser clients need to handle non-standard ports for certain protocols. For example, although most websites use port 80 for data, there are some websites that use alternate ports like 8000 or 8080. Alternate ports are somewhat uncommon; if you want to support them, please note that there may be security implications to your decision.

   You can configure your proxy instance to allow alternate ports for each supported service. Simply click **Add** under the port entry for the service, and fill in a new port number; repeat if multiple entries are desired.

   Each supported service (HTTP/HTTPS/FTP) can have an alternate port list.

URL filtering and inspection

This section allows you to configure a group of Websense Web Security servers that are able to make blocking decisions for your BIG-IP iApp proxy instance. It is not necessary for these Websense hosts to be running Websense Web Security Gateway or TRITON AP-WEB ; they simply need to be running the Filter Service. Consult your Websense documentation to see if this is the case for your deployment.



URL Filtering and Inspection

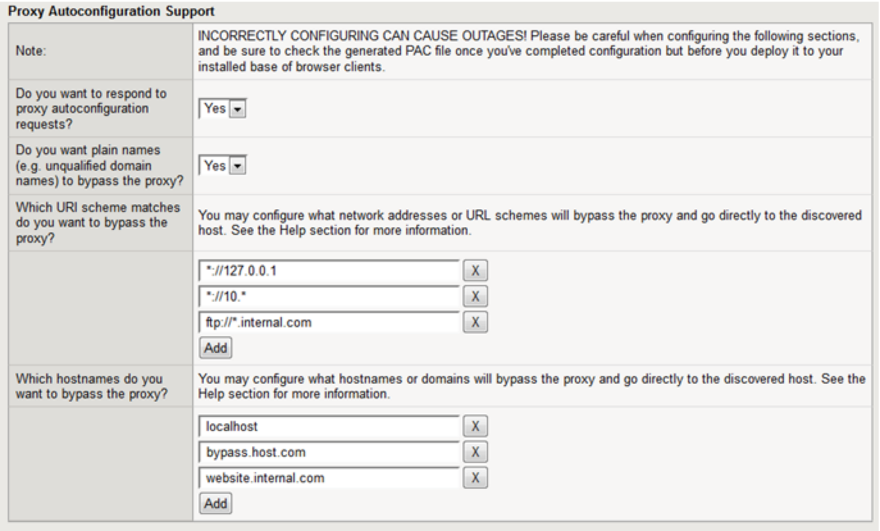
Do you want to enable Websense URL filtering support?	Yes ▾
Instructions	Enter the addresses of all the Websense servers in your infrastructure that can process filtering requests. This can include any Websense server type, as long as it has the Filtering Engine enabled.
Remote Websense Filtering Servers	Server IP: 10.133.99.30 X Add

Figure 11: URL filtering and inspection

If you wish to enable this feature, select **Yes** from the dropdown list, and then enter the IP address of your servers running a Websense Filter Service instance. If you need more than one, click **Add** and enter an additional address; repeat if needed.

Proxy autoconfiguration support

In this final section, you can configure your BIG-IP proxy instance to host a proxy autoconfiguration file (also known as a PAC file). The iApp will construct your PAC file based on your instructions and attach it to the virtual IP you configured earlier.



Proxy Autoconfiguration Support

Note:	INCORRECTLY CONFIGURING CAN CAUSE OUTAGES! Please be careful when configuring the following sections, and be sure to check the generated PAC file once you've completed configuration but before you deploy it to your installed base of browser clients.
Do you want to respond to proxy autoconfiguration requests?	Yes
Do you want plain names (e.g. unqualified domain names) to bypass the proxy?	Yes
Which URI scheme matches do you want to bypass the proxy?	You may configure what network addresses or URL schemes will bypass the proxy and go directly to the discovered host. See the Help section for more information.
	*://127.0.0.1 *://10.* ftp://*.internal.com
Which hostnames do you want to bypass the proxy?	You may configure what hostnames or domains will bypass the proxy and go directly to the discovered host. See the Help section for more information.
	localhost bypass.host.com website.internal.com

Figure 12: Proxy autoconfiguration support

Important

Incorrectly configuring a proxy autoconfiguration file can cause outages for browser clients! Be careful when configuring this section, and always check the generated PAC file before deploying it to your production environment.

The generated PAC file will always be available using two distinct filenames from the main proxy virtual server IP address. You can find it at:

```
http://<proxyipaddress>/proxy.pac
```

or

```
http://<proxyipaddress>/wpad.dat
```

The latter name is used when supplying an autoconfiguration file via DNS or DHCP's WPAD (Web Proxy Autodiscovery Protocol). See http://findproxyforurl.com/deploying-wpad/ for more information on configuring WPAD.

1. If you wish to use a proxy autoconfiguration file generated locally to this proxy instance, select **Yes** from the dropdown menu for **Do you want to respond to proxy autoconfiguration requests**.
2. **Unqualified Host Bypass**: Consider the hosts you wish to connect via your proxy. If your browser clients access any internal sites using unqualified domain names (or “shortnames”), you may want to allow these hosts to bypass the proxy. Select **Yes** from the dropdown list to inform browser clients that these types of sites should not be forwarded to the proxy.
3. **URI Scheme Bypass**: You can configure your generated autoconfiguration file to allow certain wildcard matches against the entire uniform resource identifier (URI) to bypass the proxy. This is useful in cases where you either want to allow an entire protocol to bypass:

   ```
   ftp://*
   ```

   Or you want to allow all connections on any protocol to bypass if they’re found to include an internal IP address:

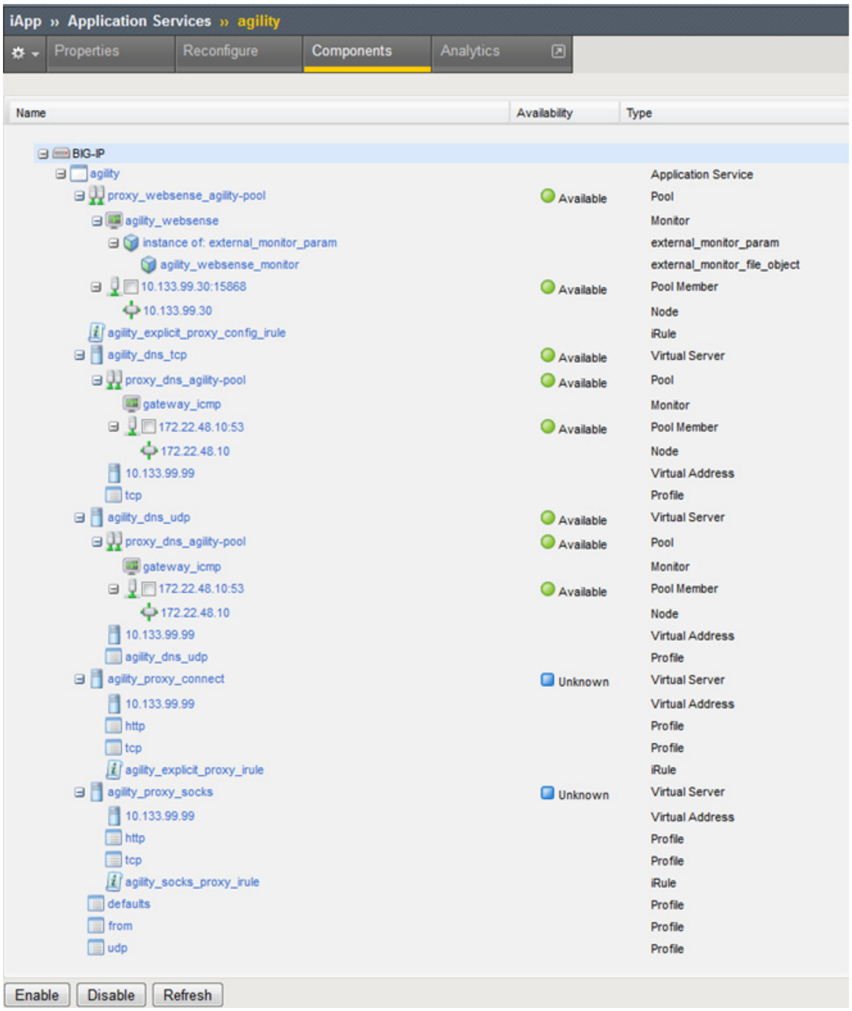
   ```
   *://10.*
   ```

   Or you want to specifically allow connections to localhost from the browser client to bypass the proxy (this is actually recommended and included by default):

   ```
   *://127.0.0.1
   ```

4. **Hostname Bypass**: You can configure your generated autoconfiguration file to bypass a list of configured FQDN hostnames. This is useful when you want to bypass specific hosts in favor of internally resolved hosts (i.e., “localhost,” “specific.host.com,” “internal.portal.com”).

When you have completed the configuration of all the sections above, click **Finished** at the bottom of the screen. The iApp will then build your configuration as seen in Figure 13.



Name	Availability	Type
BIG-IP		
agility		Application Service
proxy_websense_agility-pool	● Available	Pool
agility_websense		Monitor
instance of: external_monitor_param		external_monitor_param
agility_websense_monitor		external_monitor_file_object
10.133.99.30:15868	● Available	Pool Member
10.133.99.30		Node
agility_explicit_proxy_config_irule		iRule
agility_dns_tcp	● Available	Virtual Server
proxy_dns_agility-pool	● Available	Pool
gateway_icmp		Monitor
172.22.48.10:53	● Available	Pool Member
172.22.48.10		Node
10.133.99.99		Virtual Address
tcp		Profile
agility_dns_udp	● Available	Virtual Server
proxy_dns_agility-pool	● Available	Pool
gateway_icmp		Monitor
172.22.48.10:53	● Available	Pool Member
172.22.48.10		Node
10.133.99.99		Virtual Address
agility_dns_udp		Profile
agility_proxy_connect	■ Unknown	Virtual Server
10.133.99.99		Virtual Address
http		Profile
tcp		Profile
agility_explicit_proxy_irule		iRule
agility_proxy_socks	■ Unknown	Virtual Server
10.133.99.99		Virtual Address
http		Profile
tcp		Profile
agility_socks_proxy_irule		iRule
defaults		Profile
from		Profile
udp		Profile

Figure 13: A completed generic proxy with Websense Support configuration