Deployment Guide

Accelerating SaaS Applications with F5 AAM and SSL Forward Proxy

Welcome to the F5 deployment guide for Software as a Service (SaaS). This guide shows administrators how to configure the BIG-IP Local Traffic Manager (LTM) for and Application Acceleration Manager (AAM) for optimizing and securing SaaS deployments using the SSL Forward Proxy iApp template. There is also an appendix with manual configuration tables for users who prefer to create each individual object.

Why F5?

When used in combination with the SSL forward proxy feature, F5's Web Accelerator/Application Acceleration Manager can improve performance of external SaaS applications for internal clients. Because the BIG-IP system is proxying all of the application traffic, it can store local copies of cacheable resources and serve them to clients, reducing the number of external requests to the application and decreasing page load times.

Products and applicable versions

Product	Version
BIG-IP LTM, AAM	11.3, 11.4.x, 11.5, 11.5.1, 11.6
SaaS applications	Not applicable
Deployment guide version	1.2 (see *Document Revision History on page 14*)

Important: *Make sure you are using the most recent version of this deployment guide, available at http://www.f5.com/pdf/deployment-guides/f5-saas-dg.pdf.*

To provide feedback on this deployment guide or other F5 solution documents, contact us at *solutionsfeedback@f5.com*

Contents

What is F5 iApp?

Introduced in BIG-IP version 11, F5 iApp is a powerful 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 template acts as the single-point interface for building, managing, and monitoring this deployment.

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*.

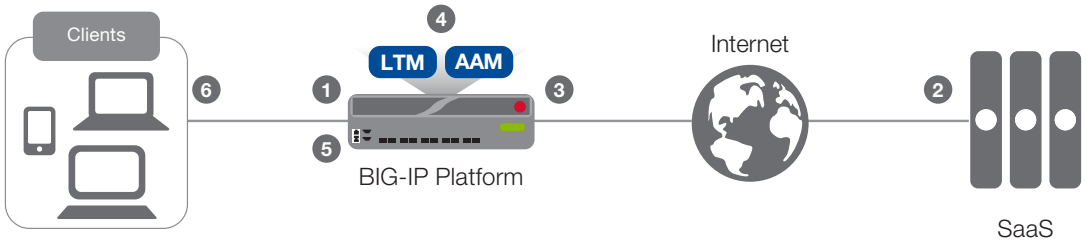
Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide:

- This document provides guidance on using the **downloadable iApp** for SaaS implementations found at *https://devcentral.f5.com/wiki/iApp.SSL-forward-proxy-with-web-acceleration-iApp-template.ashx*, and **not** any previous versions of the iApp. There is a manual configuration guidance at the end of this guide.
- For this guide, the BIG-IP system ***must*** be running version 11.3 or later.
- To use the configuration described in this guide, you must have licensed and provisioned the BIG-IP AAM (in version 11.3.x WebAccelerator) module as well as the SSL Forward Proxy feature. For specific information on licensing, contact your F5 Sales representative.
- You must have imported all the necessary SSL certificates on to the BIG-IP system. This implementation requires a trusted CA certificate and key for client-side connections. If clients use certificates to authenticate to back end services, you need an additional certificate and key. Importing certificates and keys is outside the scope of this document. See **System > File Management > SSL Certificate List** or the BIG-IP documentation for specific instructions.
- If you are using the BIG-IP AAM (or WebAccelerator), you must know the host names for each external resource you want the system to accelerate.

Configuration description

This deployment uses a wildcard virtual server on the BIG-IP system to forward outbound traffic from internal clients to the Internet. Outbound HTTPS traffic to the specific resources terminates on the BIG-IP system, which opens an encrypted connection to the requested external web server. The response is then stored in the cache on the BIG-IP device, but only when the web server has indicated that the content is cacheable. The BIG-IP system, which is configured with a certificate from a Certificate Authority trusted by the client, creates a new certificate for the client side connection and responds with the requested content.



Traffic flow

1. A client establishes a three-way handshake and SSL connection with a wildcard virtual server on the BIG-IP system.
2. The BIG-IP system establishes a three-way handshake and SSL connection with the server
3. The BIG-IP system validates a server certificate, while maintaining the separate connection with the client.
4. Cacheable responses are stored in the BIG-IP AAM cache.
5. The BIG-IP system creates a different server certificate and sends it to the client.
6. Subsequent requests for cacheable content are served from the BIG-IP AAM.

Configuring the BIG-IP system using the iApp template

Use the following guidance to help configure the BIG-IP system for SaaS applications using the BIG-IP iApp template. If you prefer to manually configure the BIG-IP system, see *Manually configuring the BIG-IP system for SaaS implementations on page 11.*

Downloading and importing the iApp

The first task is to download and import the SSL Forward Proxy iApp template.

To download and import the iApp

1. Open a web browser and go to *https://devcentral.f5.com/wiki/iApp.SSL-forward-proxy-with-web-acceleration-iApp-template.ashx*, and then click the link to download the iApp zip file to a location accessible from your BIG-IP system.

   Important

   You must download the file, and not copy and paste the contents. The copy paste operation does not work reliably.

2. Extract (unzip) the **f5.ssl_forward_proxy.v0.1.0.tmpl** file.
3. Log on to the BIG-IP system web-based Configuration utility.
4. On the Main tab, expand **iApp**, and then click **Templates**.
5. Click the **Import** button on the right side of the screen.
6. Click a check in the **Overwrite Existing Templates** box.
7. Click the **Browse** button, and then browse to the location you saved the iApp file.
8. Click the **Upload** button. The iApp is now available for use.

Getting Started with the iApp

To begin the SaaS iApp Template, use the following procedure.

1. Log on to the BIG-IP system.
2. On the Main tab, expand **iApp**, and then click **Application Services**.
3. Click **Create**. The Template Selection page opens.
4. In the **Name** field, type a name.
5. From the **Template** list, select **f5.ssl_forward_proxy.v0.1.0**. The template opens.

Template Options

This section contains general questions about the way you configure the iApp template.

1. ***Do you want to see inline help?***
   Choose whether you want to see informational and help messages inline throughout the template, or if you would rather hide this inline help. If you are unsure, we recommend having the iApp display the inline help.
   Important and critical notes are always shown, no matter which selection you make.
   - **Yes, show inline help text**
     Select this option to see all available inline help text.
   - **No, do not show inline help text**
     If you are familiar with this iApp template, or with the BIG-IP system in general, select this option to hide the inline help text.

Tell us about your deployment

Use this section for guidance on configuring the BIG-IP LTM portion of the iApp template.

1. ***Which trusted CA certificate do you want to use for client-side connections?***
   Select the SSL certificate you imported on to the BIG-IP system for client-side connections. The certificate must already be on the BIG-IP system before you can select it in the iApp template. This certificate must be generated from a Certificate Authority and must be trusted by browser clients; using the BIG-IP default.crt results in an invalid configuration.

2. ***Which trusted CA private key you want to use for client-side connections?***
   Select the SSL private key associated with the certificate you selected in the previous question.

3. ***Will clients use certificates to authenticate to back end services?***
   Choose whether clients are required to authenticate to the back end services behind the BIG-IP system. This determines whether the BIG-IP system presents a certificate to the servers on behalf of the clients.

   - **No, clients will not use certificates**
     If the clients are not required to authenticate to the back end services, leave this selection, and continue with #4.
   - **Yes, clients will use certificates**
     Select this option if the clients require certificates to access the back end resources. In this case, the iApp creates a Server SSL profile and attaches the certificates you specify in the following questions. The Server SSL profile presents the certificate on behalf of the client.

     a. *Which SSL certificate do you want to use for server-side connections?*
        Select the certificate you imported on to the BIG-IP system to use for server-side SSL decryption/re-encryption.

     b. *Which SSL private key do you want to use for server-side connections?*
        Select the associated key from the list.

4. ***Do you want to require strict SSL renegotiation for encrypted server-side connections?***
   Choose whether you want to require strict SSL renegotiation for encrypted server-side connections. SSL renegotiation is a process by which the full handshake process takes place over an already existing SSL connection. For more information on SSL renegotiation, see *https://devcentral.f5.com/articles/ssl-profiles-part-6-ssl-renegotiation*.

   - **No, do not require strict SSL renegotiation**
     Select this option if you do not require strict SSL renegotiation for encrypted server-side connections. In this case, the system uses the **Request** setting for SSL renegotiation, which specifies the system requests secure renegotiation of SSL connections, but does not require it.
   - **Yes, require strict SSL renegotiation**
     Select this option if you want the system to require strict SSL renegotiation. With strict renegotiation, the BIG-IP system refuses new SSL connections to insecure servers and terminates existing SSL connections to insecure servers.

5. ***For how many days should the BIG-IP proxy-issued SSL certificate be valid?***
   Specify a number of days the SSL forward proxy certificate issued by the BIG-IP system remains valid. We recommend the default of 30 days.

6. ***On which VLAN(s) should the wildcard virtual server listen for outbound traffic?***
   Specify the VLANs from which the BIG-IP system should allow outbound traffic. This creates a more secure environment, as the BIG-IP virtual server created by the iApp will only listen for traffic on the VLANs you specify, and ignore all other traffic for this deployment. Use the Add (<<) button to move VLANs to the selected list.

   Important

   If you do not specify any VLANs in this section, the system listens on all VLANs configured on the system.

Only VLANs already configured on the BIG-IP system appear in the list. If necessary, you can exit the template and create the necessary VLANs (**Network > VLANs**), or complete the template now, and then reconfigure the iApp after creating necessary VLANs.

2. ***How would you like to route outbound connections from clients?***
Choose whether you want to use an existing route on the BIG-IP system for routing outbound client connections or forward the connections a pool of routers.

   - **Use an existing Route on this BIG-IP system**
   Select this option if you want to use a Route on the BIG-IP system. If you choose a route, it must already exist on the system. See the help tab on the Network > Routes page for more information or help configuring routes.
   - **Forward connections to a pool of routers**
   Select this option if you want to forward outbound client connections to a pool of multiple routers. The system creates a load balancing pool (or you can select an existing pool of routers if applicable) for the router IP addresses you specify.

      a. *Should the iApp create a new pool for the routers?*
      Choose whether you want the iApp to create a new pool of routers using IP addresses you will specify, or if you have already created a load balancing pool for the routers.

         - **No, use an existing pool**
         Select this option if you have already created a Pool on the BIG-IP system for the routers. See the following question for health monitoring requirements.

            i). *Which existing pool do you want to use?*
            Select the existing pool of routers you want to use for this configuration. This pool should have a separate Gateway ICMP monitor for each external resource behind the routers you want to monitor. Each monitor must have 'Transparent' set to 'Yes', and the 'Alias Address' set to the next hop resource behind the router you want to monitor. The pool must have the Health monitor Availability Requirement set to 'At Least...' and '1'.

         - **Yes, create a new pool**
         Select this option if you want the iApp to create a new load balancing pool for the routers. You specify the router IP addresses in the next question.

            i). *Which routers do you want to include?*
            Type the IP address(es) of your routers. Click the Add button to include additional routers.

            ii). *Should the iApp create a new health monitor?*
            Choose whether the iApp should create a new health monitor or if you have created an custom Gateway ICMP monitor for the routers. It is important to note that this health monitor is for monitoring the next hop resources behind the routers, and not the routers themselves.

               - **No, use an existing Gateway ICMP-based monitor**
               Select this option if you have created a Gateway ICMP monitor for the resources behind the routers.

                  1). *Which existing monitor do you want to use?*
                  Select the existing health monitor you want to attach to the pool. Only monitors with a Type of Gateway ICMP appear in the list.

               - **Yes, create a new monitor**
               Select this option if you want the iApp to create a new ICMP health monitor for the resources behind the routers.

                  1). *What external IP address(es) do you want to monitor?*
                  Type the IP address(es) of the external resources behind the routers you want to monitor. The iApp creates a Gateway ICMP monitor for each IP address you enter and attaches all of the monitors to the pool. On the pool, the minimum number of healthy monitors is be set to one to ensure as long as one route exists, the configuration will function properly.

3. ***Which type of SNAT should the system for outbound source IP addresses translation?***
Choose the type of SNAT (Secure Network Address Translation) the iApp should use to translate outbound source IP addresses. Unless you have a large configuration and expect more than 64,000 concurrent connections per SNAT address, we recommend using SNAT Auto Map.

- **Use SNAT Auto Map**
  Select this option if you want the system to apply SNAT Auto Map. With SNAT Auto Map, the BIG-IP system replaces the source IP address of an incoming connection with its local self IP address.
- **Use a SNAT Pool**
  Select this option if you want the iApp to attach a SNAT pool of translation addresses you specify.

  a. *Do you want to create a new SNAT pool, or using an existing one?*
  Select whether you want the iApp to create a new SNAT pool or if you have already created a SNAT pool you want to use for this configuration.

  - **Create a new SNAT Pool**
    Select this option if you want the iApp to create a new SNAT pool. You specify the IP addresses in the following question.

    i). *What IP addresses do you want to use for the SNAT pool?*
    Specify otherwise unused IP addresses to use in the SNAT Pool. SNAT Pool addresses must not include any of the self IP address(es) of the BIG-IP system.
  - **Use an existing SNAT pool**
    Select this option if you have already created a SNAT pool to use in this configuration.

    i). *Which SNAT pool do you want to use?*
    Select the existing SNAT pool you created for this configuration.

4. ***Do you want to allow unencrypted traffic through this BIG-IP virtual server?***
   Choose whether you want the BIG-IP system to allow unencrypted traffic, or if all unencrypted traffic should be ignored.
   - **Yes, allow unencrypted traffic**
     Select this option if you want to allow unencrypted traffic through the BIG-IP system. If you select to allow unencrypted traffic, the iApp includes an iRule to disable SSL to allow unencrypted traffic to pass through the BIG-IP virtual server.
   - **No, do not allow unencrypted traffic**
     Select this option if you do not want the system to allow unencrypted traffic. If you select this option, the system denies all traffic that is not encrypted.

5. ***Do you want to add any custom iRules to this configuration?***
   iRules are a scripting language that allows an administrator to instruct the system to intercept, inspect, transform, direct and track inbound or outbound application traffic. An iRule contains the set of instructions the system uses to process data flowing through it, either in the header or payload of a packet.

   Select if have preexisting iRules you want to add to your implementation.

   Warning

   While iRules can provide additional functionality not present in the iApp, iRules are an advanced feature and should be used only if you understand how each iRule will affect your deployment, including application behavior and BIG-IP system performance.

   If you do not want to add any iRules to the configuration, continue with the following section.

   If you have iRules you want to attach to the virtual server the iApp creates, from the **Options** box, click the name of the applicable iRule(s) and then click the Add (**<<**) button to move them to the **Selected** box.

Web Acceleration and Optimization

1. ***Do you want to use AAM to accelerate server responses?***
   Choose whether you want to use BIG-IP AAM in this configuration. BIG-IP AAM can accelerate server responses to improve performance of external SaaS applications for internal clients.

2. ***Which Web Acceleration profile do you want to use?***
   Choose whether you want the iApp to create a new Web Acceleration profile, or if you have already created an Acceleration profile for this deployment.

3. ***Which application FQDNs do you want to accelerate?***
   Type the fully qualified domain name(s) of the applications you want to accelerate. Click Add to include more FQDNs.

4. ***Which BIG-IP AAM Acceleration policy do you want to use?***
   Choose whether you want the iApp to create a Acceleration policy, or if you have already created an AAM Acceleration policy for this deployment. Unless you have specific needs, we recommend you allow the iApp to create the Acceleration policy.

   - *Select an existing Acceleration policy from the list*
     If you already created an Acceleration policy for this implementation, select it from the list.
   - **Create a new Web Acceleration policy**
     Select this option for the iApp to create a new Web Acceleration policy.

5. ***Do you want to insert the standard AAM debugging header?***
   By default, the AAM X-WA-info header is not included in the response from the BIG-IP system. This header is useful for debugging AAM behavior. If you choose to enable this header, you have two options, Standard and Debug. In Standard mode, the BIG-IP system inserts an HTTP header that includes numeric codes which indicate if and how each object was cached. In Debug mode, the BIG-IP system includes additional information which may help for extended troubleshooting.

6. ***Allow requests for unaccelerated resources through this virtual server?***
   Choose whether you want the BIG-IP system to allow requests for unaccelerated resources through the BIG-IP virtual server. If you select to allow unaccelerated traffic, the iApp includes an iRule to allow this traffic to pass through the BIG-IP virtual server.

7. ***Which TCP profile do you want to use for client-side connections?***
   Select the client-side TCP profile you created for this configuration. To select a profile from the list, it must already be present on the BIG-IP system. Creating a custom profile is not a part of this template. To select any new profiles you create, you need to restart or reconfigure this template.

8. ***Which TCP profile do you want to use for server-side connections?***
   Select the server-side TCP profile you created for this configuration. To select a profile from the list, it must already be present on the BIG-IP system. Creating a custom profile is not a part of this template. To select any new profiles you create, you need to restart or reconfigure this template.

9. ***Which HTTP profile do you want to use?***
   The HTTP profile contains settings for instructing the BIG-IP system how to handle HTTP traffic. Choose whether you want the iApp to create a new HTTP profile or if you have previously created an HTTP profile for this deployment.

   Unless you have requirements for configuring specific HTTP settings, we recommend allowing the iApp to create a new profile. To select a profile from the list, it must already be present on the BIG-IP system. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Services : HTTP** to create a HTTP profile. To select any new profiles you create, you need to restart or reconfigure this template.

   - *Select an existing HTTP profile from the list*
     If you already created an HTTP profile for this implementation, select it from the list.
   - **Create a new HTTP profile**
     Select this option for the iApp to create a new HTTP profile.

10. ***Do you want to enable OneConnect?***
    OneConnect (connection pooling or multiplexing) can improve server scalability by reducing load associated with concurrent connections and connection rate to the servers. When enabled, the BIG-IP system maintains one connection to each server which is used to send requests from multiple clients. Select whether you want the iApp to apply a OneConnect profile to the configuration.

- **Do not use OneConnect**
  Select this option if you do not want to use OneConnect.
- *Select an existing OneConnect profile from the list*
  If you want to use OneConnect, select the default oneconnect profile, or select the OneConnect profile you created for this implementation.

11. ***Do you want to enable HTTP compression for server responses?***
    Compression improves performance and end user experience for Web applications that suffer from WAN latency and throughput bottlenecks. Compression reduces the amount of traffic sent to the client to complete a transaction. Select whether you want to enable HTTP compression for server responses in this configuration.
    - **Do not use HTTP Compression**
      Select this option if you do not want to use HTTP Compression.
    - *Select an existing HTTP Compression profile from the list*
      If you want to use HTTP Compression, select the default **httpcompression** profile, or select the profile you created for this implementation.

Finished

Review the answers to your questions. When you are satisfied, click the **Finished** button. The BIG-IP system creates the relevant objects for the SaaS application.

Troubleshooting

Use this section for common issues and troubleshooting steps.

➤ **SSL connection attempts fail with a bad signature error message when using OpenSSL s_client**

There is a known issue that causes SSL connection attempts to fail with an error when using **s_client**. ECDHE_ECDSA and DHE_DSS ciphers do not work with OpenSSL 1.0.1k and later.

This issue occurs when all of the following conditions are met:

- You are using BIG-IP v11.5.1, 11.5.2, or 11.6
- You have configured the BIG-IP system to process Secure Socket Layer (SSL) traffic using a Client SSL profile.
- You attempt to create a new SSL connection using OpenSSL version 1.0.1k or later **s_client** utility.
- The new SSL connections attempt to negotiate any of the ECDHE_ECDSA or DHE_DSS ciphers.

This issue has been fixed in 11.5.3 and in 11.6.0 HF5. If you are experiencing this issue, upgrade to one of those versions. For more information, see *https://support.f5.com/kb/en-us/solutions/public/16000/400/sol16461.html*.

Manually configuring the BIG-IP system for SaaS implementations

While recommend using the iApp template to configure the BIG-IP system, users familiar with the BIG-IP system can use the following table to manually configure the system. The table contains a list of configuration objects along with any non-default settings you should configure as a part of this deployment. Settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

BIG-IP object	Non-default settings/Notes		
If you want to use multiple routers for outbound connections from clients			
Health Monitor (*Local Traffic-->Monitors*) ***OPTIONAL***: Health monitors are optional and are for monitoring the next hop resources behind the routers, not the routers themselves	***Name***	Type a unique name.	
	Type	**Gateway ICMP**	
	Interval	**30**	
	Timeout	**91**	
	Transparent	**Yes**	
	Alias Address	Type the IP address the external resource (behind the router) you want to monitor	
	Best Practice: Repeat this section to create a health check for each external resource you want to monitor in this configuration		
Pool (*Local Traffic -->Pools*)	***Name***	Type a unique name.	
	Health monitor	Add health monitor(s) you created	
	Availability Requirement	**At Least... 1**	
	Load Balancing Method	**Least Connections (member)** recommended	
	Address	Type the IP address of one of the routers	
	Service Port	*** All Ports**	
If you want to a single route on the BIG-IP system for outbound connections from clients			
Routes (*Network -->Routes*)	To create a route on the BIG-IP system, click **Network > Routes > Create**. Details on creating a route on the BIG-IP system is outside the scope of this guide. See the Online help tab on the Routes page, or the BIG-IP TMOS: IP Routing Administration guide for your version (for example, for 11.4: *http://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-ip-routing-administration-11-4-0.html*)		
BIG-IP AAM Acceleration (optional)	***Web Acceleration Policy***	To configure the Web Acceleration policy follow the procedure in *Creating the Acceleration policy on page 13*	
	Web Acceleration Application (*Acceleration--> Web Application--> Applications*)	Name	Type a unique name.
		Requested Hosts	Type the FQDN of a host you want to accelerate using AAM. Click Add to include additional hosts.
Profiles (*Local Traffic-->Profiles*)	***HTTP*** (*Profiles-->Services*)	Name	Type a unique name.
		Parent Profile	**http**
	TCP WAN (*Profiles-->Protocol*)	Name	Type a unique name.
		Parent Profile	**tcp-wan-optimized**
	TCP LAN (*Profiles-->Protocol*)	Name	Type a unique name.
		Parent Profile	**tcp-lan-optimized**
	Client SSL *(Profiles > SSL)*	Name	Type a unique name
		Parent Profile	**clientssl**
		SSL Forward Proxy	**Enabled**
		CA Certificate and Key	In the SSL Forward Proxy section, select the Certificate and Key you imported from a Certificate Authority that is trusted by all internal clients
		Certificate Lifespan	Optional: Specify a lifespan for the SSL forward proxy certificate.
	Server SSL *(Profiles > Other)*	Name	Type a unique name
		Parent Profile	**serverssl**
		SSL Forward Proxy	**Enabled** (for basic functionality)
		Secure Renegotiation	**Request** (recommended)
		Certificate and Key	Optional: For clients using certificate authentication, you must specify a valid cert/key pair matching those offered by the external resource. If clients are doing certificate authentication to multiple resources with different certificates, a separate serverssl profile is required for each certificate offered by the resources

BIG-IP object	Non-default settings/Notes		
Profiles (*Local Traffic-->Profiles*)	***Web Acceleration*** *Optional: Create if you configured BIG-IP AAM (Profiles > Services)*	Name Parent Profile WA Applications[2]	Type a unique name **webacceleration** Enable the AAM Application you created
iRules (*Local Traffic--> iRules*	***iRule to disable SSL to allow unencrypted traffic to pass through the BIG-IP virtual server***		
	Name	Type a unique name	

	Definition	Copy and paste the following code in the definition section.
		`when CLIENT_ACCEPTED {`
		`  set ssl_disabled 0`
		`  if { [TCP::local_port] != 443 } {`
		`  SSL::disable`
		`  set ssl_disabled 1`
		`  }`
		`}`
		
		`when HTTP_REQUEST {`
		`  if { $ssl_disabled == 1 } {`
		`  SSL::disable serverside`
		`  }`
		`}`	

	iRule to disable AAM for host names that should not be accelerated		
	Name	Type a unique name	

	Definition	Copy and paste the following code. Change the host names (and add/delete line items) as appropriate
		`when HTTP_REQUEST  {`
		`  switch -glob [string tolower [HTTP::host]] {`
		`  www.example1.com -`
		`  www.example2.com -`
		`  www.example3.com`
		`  {`
		`  WAM::enable`
		`  }`
		`  default WAM::disable`
		`  }`
		`}`	

Virtual Server (*Local Traffic-->Virtual Servers*)	***Name***	Type a unique name.	
	Destination	**Type: Network** **Address: 0.0.0.0** **Mask: 0.0.0.0**	
	Service Port	***All Ports**	
	Protocol Profile (Client)[1]	Select the TCP LAN profile you created	
	Protocol Profile (Server)[1]	Select the TCP WAN profile you created	
	HTTP Profile	Select the HTTP profile you created	
	SSL Profile (Client)	Enable the Client SSL profile you created	
	SSL Profile (Server)	Enable the Server SSL profile you created	
	Web Acceleration Profile	If you created a Web Acceleration profile, select if from the list.	
	SNAT Pool	**Auto Map** (SNAT is recommended. If you expect more than 64,000 concurrent connections per server, use a SNAT Pool[2] instead of Auto Map)	
	iRules	Enable any optional iRules you created	
	Default Pool	If you created a pool of routers, select it here. If you did not create a pool, leave this at None.	

[1] *You must select* **Advanced** *from the* **Configuration** *list for these options to appear.*
[2] *For more information on SNAT Pools, see the BIG-IP documentation*

Creating the Acceleration policy

If you want to use the BIG-IP AAM to accelerate responses from the server, you must create a new Acceleration policy.

To create the Acceleration Policy

1. From the Configuration utility, click **Acceleration > Web Application > Policies**.
2. In the Predefined Policies section, in the **Generic Policy - Fundamental** row, click the **Copy** link.
3. In the **Name** field, type a name, and then click the **Copy** button.
4. In the User-defined Acceleration Policies section, click the Policy you just created. The Editing Policy page opens.
5. On the menu bar, click **Matching Rules > Acceleration Rules**.
6. On the menu bar, click **Proxying**.
    a. Ensure that **Configure and use Proxy Rules for this node** is checked.
    a. Click **Save**.
7. On the menu bar, click **Lifetime**.
    a. Check the **Honor Headers from Origin Web Server** box.
    b. In the **Origin Web Server Headers** section, from the Available list, select **all**, and then click the Add (<<) button.
    c. Ensure that **Preserve Origin Web Server headers/directives to downstream devices** is checked.
    d. In the **Origin Web Server Headers** section, from the Available list, select **all**, and then click the Add (<<) button.
    e. Click **Save**.
8. Click **Publish**.

Document Revision History

Version	Description	Date
1.0	New guide	06-18-2013
1.1	Added support for BIG-IP v11.6	08-25-2014
1.2	Added *Troubleshooting on page 10*, with an entry regarding SSL connection failures when using OpenSSL s_client.	07-29-2015

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com