DEPLOYMENT GUIDE

DEPLOYING F5 WITH SAP NETWEAVER AND ENTERPRISE SOA

Table of Contents

Introducing the F5 Deployment Guide for SAP NetWeaver and Enterprise SOA

Prerequisites and configuration notes 1-1
Configuring the SAP Enterprise Portal for the BIG-IP LTM system 1-2
Configuring the BIG-IP LTM system for deployment with SAP 1-6
Prerequisites and configuration notes 1-7
Configuring the BIG-IP LTM system for the SAP Enterprise Portal 1-8
Creating the HTTP health monitor 1-8
Creating the pool 1-10
Creating profiles 1-11
Creating the virtual server 1-17
Configuring the BIG-IP LTM system for the SAP ERP Central Component (ECC) 1-20
Creating the TCP health monitor 1-20
Creating the pool 1-21
Creating the profiles 1-22
Creating the virtual server 1-23
Creating a default SNAT 1-25
Configuring the BIG-IP LTM for offloading SSL traffic from the SAP Deployment 1-26
Using SSL certificates and keys 1-26
Creating additional profiles 1-27
Creating the Redirect iRule 1-29
Creating an HTTPS virtual server 1-30
Modifying the SAP Enterprise Portal virtual server 1-33
Appendix A: Backing up and restoring the BIG-IP system configuration 1-35
Saving and restoring the BIG-IP configuration 1-35

Configuring the F5 WebAccelerator module with SAP Enterprise Portal

Prerequisites and configuration notes 2-1
Configuration example 2-2
Configuring the WebAccelerator module 2-2
Connecting to the BIG-IP device 2-2
Creating an HTTP Class profile 2-2
Modifying the Virtual Server to use the Class profile 2-4
Creating an Application 2-5

Deploying the FirePass controller with SAP NetWeaver and Enterprise SOA

Prerequisites and configuration notes 3-1
Configuration scenario 3-2
Configuring the FirePass controller for deployment with SAP 3-2
Connecting to the FirePass controller 3-2
Creating the Resource groups 3-2
Creating the Master groups 3-5
Configuring the Master group for Active Directory authentication 3-6
Limiting access for the Partner group 3-8
Configuring Endpoint security 3-9

1

Deploying F5 with SAP NetWeaver and Enterprise SOA

- Configuring the SAP Enterprise Portal for load balancing with the BIG-IP LTM system
- Configuring the BIG-IP LTM system for the SAP Enterprise Portal
- Configuring the BIG-IP LTM system for the SAP ERP Central Component (ECC)
- Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment

Introducing the F5 Deployment Guide for SAP NetWeaver and Enterprise SOA

Welcome to the F5 - SAP Deployment Guide. By taking advantage of this Application Ready infrastructure for SAP® deployments organizations can achieve a secure, fast and available network infrastructure that reduces the total cost of operation and increases ROI. This guide gives you step-by-step procedures on how to configure the BIG-IP LTM system, WebAccelerator, and FirePass controller for SAP deployments.

The BIG-IP LTM version 9 with WebAccelerator and FirePass controller version 6 have achieved SAP certification for SAP ERP 6.0 based on NetWeaver 7.0. For more information on the certifications, see **http://www.f5.com/solutions/applications/sap/**.

For more information on the BIG-IP system, see **http://www.f5.com/products/**.

For more information on SAP, see **http://www.sap.com/index.epx**.

Prerequisites and configuration notes

The following are prerequisites for this Deployment Guide, each chapter contains its own prerequisites section:

- We recommend using the latest version of SAP NetWeaver and mySAP Business Suite applications. Our testing environment included both SAP ERP 6.0 based on NetWeaver 7.0 and SAP NetWeaver 2004 and mySAP ERP 2005. High availability was configured for Enterprise Portal and Composite Services on the front end along with Exchange Infrastructure (XI), Business Warehouse (BW), and SAP ERP Core Component (ECC).
- This document is written with the assumption that you are familiar with both F5 devices and SAP products. For more information on configuring these devices, consult the appropriate documentation.
- Make a list of the IP addresses and ports used by each SAP application component in your deployment, as these are used in the F5 configuration. Consult the SAP documentation and your SAP administrator for this information.

Configuring the SAP Enterprise Portal for load balancing with the BIG-IP LTM system

This section contains a brief description of how to create a new ***System*** within SAP EP using the load balancing template that allows the BIG-IP LTM system to load balance the SAP devices.

Important

This is just an overview of some of the SAP configuration details related to load balancing. For more detailed instructions on configuring your SAP solution, see the SAP documentation or contact SAP.

To create a new SAP System

1. Log on to the SAP Enterprise Portal (EP).
2. On the Menu bar, click **System Administration**, and then click **System Configuration**.
3. In the Detailed Navigation pane, click **System Landscape**.
4. Expand **Portal Content**, and then the name of your company/portal.
5. Right click **Systems**. From the Systems menu, select **New**, and then **System (from template)**. See Figure 1.1.
   You create a new System for each non EP SAP application type.
   The System Wizard opens.

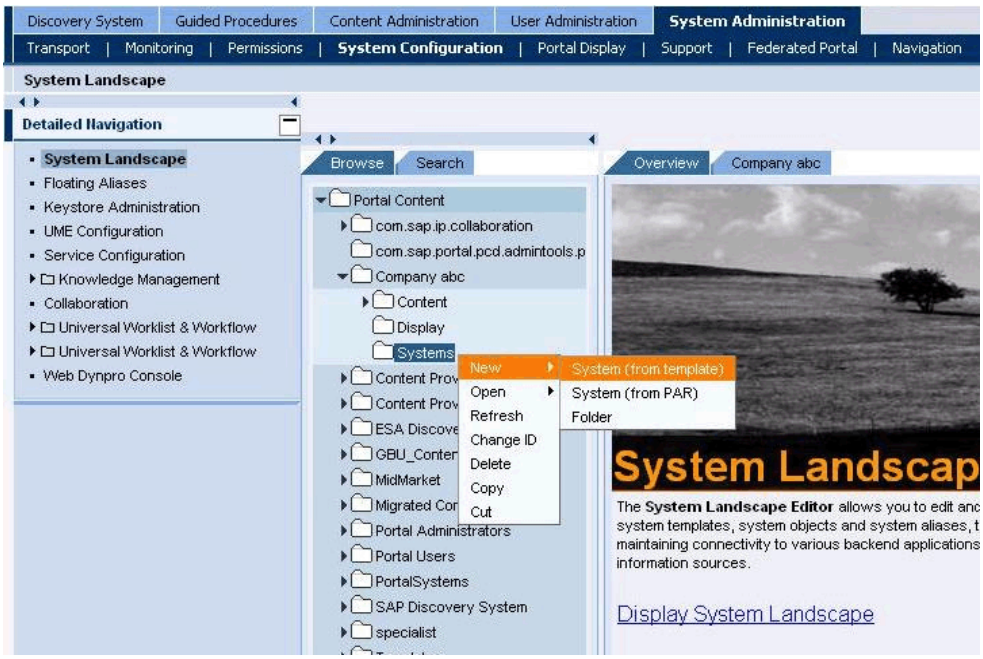

Figure 1.1 *Creating a new System in the SAP Enterprise Portal*

6. From the System Wizard, Template Selection, select **SAP system with load balancing** (you may need to scroll down to see this option depending on your installation). See Figure 1.2.
   Click the **Next** button.

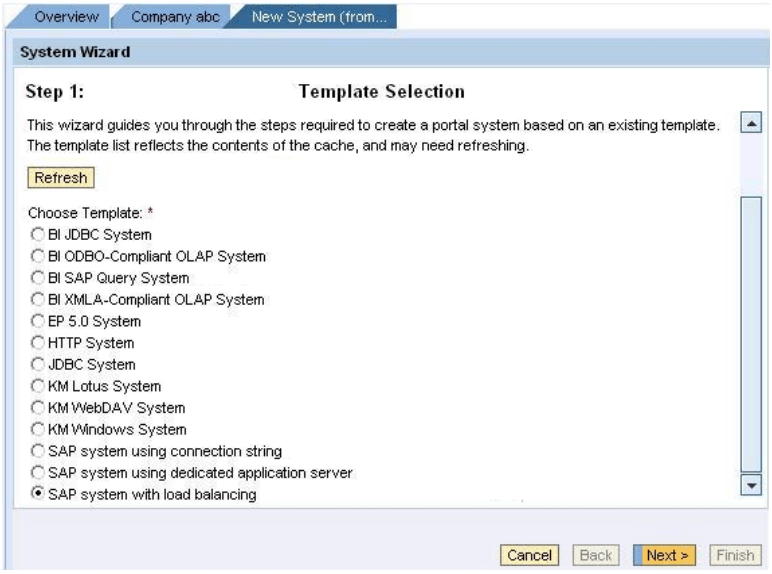

Figure 1.2 *Selecting the load balancing option from the System wizard*

7. In the General Properties step, enter the following information (see Figure 1.3):
   a) In the **System Name** box, type a name for this system, using the following syntax: **SAP <System Type> <System Name>**
      In our example, we type **SAP ECC**.
   b) In the **System ID** box, type a system ID, using the following syntax: **sap_<system id>**
      In our example, we type **sap_ecc**.
   c) In the **System ID** Prefix box, type a system ID using a prefix from the SAP deployment guidelines (**com.<companyname>.erp.ops.sys)**. In our example, we type **com.companyabc.erp.ops.sys**.
   d) From the **Master Language** list, select a language. In our example, we select **English**.
   e) In the **Description** box, you can type an optional description of this system.
8. Click the **Next** button.

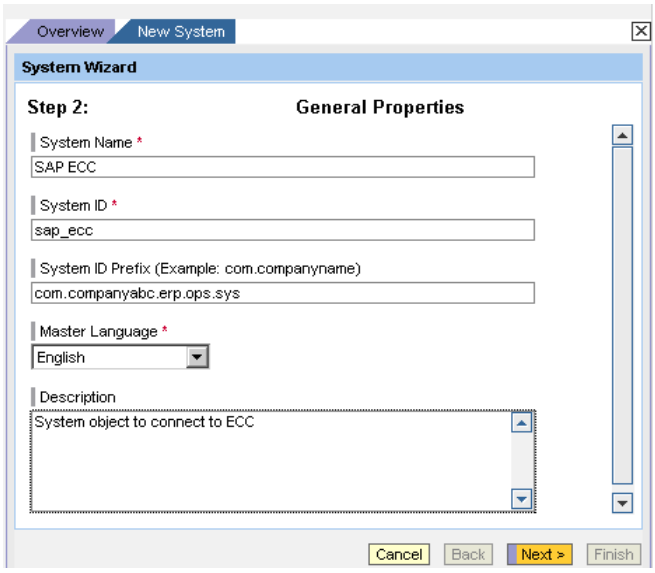

Figure 1.3 *Entering the General properties of the system*

9. Review the Summary screen. To accept your entries, click **Finish**.
10. In the **Choose your next step** menu, select **Open object for editing** and click **OK**.
11. Complete the Property Editor based on the following table:

Property	Value	Example
Group	<Group ID>	ECC_PRD_01
ITS Host Name	<Load-balanced ITS server host name>:**80**<System #>	Gerp.ecc.site.com:8050 ***see warning below**
ITS Path	<Path to ITS home>	/sap/bc/gui/sap/its/
ITS Protocol	“http” or “https”	http
Logical System Name	<System ID>CLNT<System #>	RP1CLNT030
Message Server	<System message server>	usri-pdbx-c01.site.com
SAP Client (*)	<SAP Client>	030
SAP System ID	<System ID>	RP1
Server Port	36<System #>	3650
System Type	<Type of system>	SAP_R3
WAS Host Name	<Load-balanced WAS server host name>:5<System #>00	gerp-rp1-ecc.site.com:55000 ***see note on the following page**
WAS Path	<WAS path>	/webdynpro/dispatcher
WAS Protocol	“http” or “https”	http

Table 1.1 *SAP Property table*

WARNING

** In the preceding examples, some of the entries include the port numbers. It is critical that* ***if you are using the BIG-IP LTM system to terminate SSL traffic, that you do NOT use port numbers as shown in the table****. If the application ports are hard coded, SSL termination will break the application.*

12. From the **Display selection** box, click **System Aliases**. The System Alias Editor opens.
13. In the **Alias** box, type at least one system alias for each object. Every object should have a system alias of the form **SAP_<System Type>_<Environment>** (for example SAP_SRM_QAS).

    Note that certain system aliases are required for the portal business packages to work; these aliases are listed in the following table:

System	Alias	For Bus Pack
ECC	SAP_R3_HumanResources	ESS / MSS
Web Dynpro runtime (ECC)	SAP_WebDynpro_XSS	ESS / MSS
SRM	SAP_EBP, SAP_R3_Procurement	SRM / Supplier Collaboration

Table 1.2 *System Aliases*

It is also important to note that system aliases cannot be transported - they must be assigned manually in each EP environment.

14. Click the **Save** button.

Configuring the BIG-IP LTM system for deployment with SAP

In this section, we configure the BIG-IP LTM system for deployment with SAP deployments. The BIG-IP LTM version 9, in conjunction with WebAccelerator, has achieved the following SAP certifications:

- Network Performance Optimization for Enterprise SOA-Based Solutions
- SOA Landscapes Access Reliability and Availability Through Networks
- Network Security for Enterprise SOA-Based Solutions

This section of the Deployment Guide is broken up into three sections:

- *Configuring the BIG-IP LTM system for the SAP Enterprise Portal*, on page 1-8
- *Configuring the BIG-IP LTM system for the SAP ERP Central Component (ECC)*, on page 1-20
- *Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment*, on page 1-26 ***(optional)***.

A SAP deployment can be incredibly large and complex, deployed in infinite variations, with number of different SAP applications and components. In this Deployment Guide, we focus on providing high availability and acceleration for the SAP Enterprise Portal and an example SAP application component: ERP Central Component (ECC). The procedures outlined for the SAP ECC can be repeated for any additional SAP application components you may be running.

Tip

We recommend you save the BIG-IP configuration before you begin this Deployment Guide. To save your BIG-IP configuration, see ***Appendix A: Backing up and restoring the BIG-IP system configuration****, on page 1-35.*

The BIG-IP LTM system offers both web-based and command line configuration tools, so that users can work in the environment that they are most comfortable with. This Deployment Guide contains procedures to configure the BIG-IP system using the BIG-IP web-based Configuration utility only.

Prerequisites and configuration notes

The following are prerequisites for this Chapter:

- The BIG-IP LTM system must be running version 9.0 or later, we strongly recommend running version 9.4 or later. Some of the examples in this guide use profiles introduced in version 9.4. To use these profiles you must either be running LTM version 9.4, or refer to the ***Configuration Guide for BIG-IP Local Traffic Management*** for version 9.4 (available on AskF5), which shows the configuration differences between the base profiles and the optimized profile types.
- If you are using the BIG-IP LTM system for load balancing the SAP services, you **do not** need to use the ***SAP Web Dispatcher*** for load balancing traffic. This allows you to devote the resources that would have been dedicated to Web Dispatcher to servicing other aspects of the application.
- We assume that the BIG-IP LTM device is already installed in the network, and objects like Self IPs and VLANs have already been created. For more information on configuring these objects, see the BIG-IP LTM manuals.
- If you are using the BIG-IP LTM system to offload SSL traffic from the SAP servers, you must already have obtained an SSL Certificate (but not necessarily installed it on the BIG-IP LTM system). For more information about offloading SSL traffic, see *Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment*, on page 1-26.

Connecting to the BIG-IP LTM device

Use the following procedure to access the BIG-IP LTM web-based Configuration utility using a web browser.

To connect to the BIG-IP LTM system using the Configuration utility

1. In a browser, type the following URL:
   https://<administrative IP address of the BIG-IP device>
   A Security Alert dialog box appears, click **Yes**.
   The authorization dialog box appears.
2. Type your user name and password, and click **OK**.
   The Welcome screen opens.

Once you are logged onto the BIG-IP system, the Welcome screen of the new Configuration utility opens. From the Configuration utility, you can configure and monitor the BIG-IP system, as well as access online help, download SNMP MIBs and Plug-ins, and search for specific objects.

Configuring the BIG-IP LTM system for the SAP Enterprise Portal

In this section, we configure the BIG-IP LTM system to manage traffic for the SAP Enterprise Portal.

To configure the BIG-IP LTM system for the SAP Enterprise Portal, you must complete the following procedures:

- *Creating the HTTP health monitor*
- *Creating the pool*
- *Creating profiles*
- *Creating the virtual server*

◆ Note

If you are using the BIG-IP LTM system to offload SSL, there are additional procedures you must follow. After completing this section, go to ***Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment****, on page 26.*

Creating the HTTP health monitor

For this configuration, we create a simple HTTP health monitor. Although the monitor in the following example is quite simple, you can configure optional settings such as Send and Receive Strings to make the monitor much more specific. You can also use one of the other types of monitors available on the BIG-IP LTM system.

To configure the HTTP health monitor

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**.
   The Monitors screen opens.
2. Click the **Create** button. The New Monitor screen opens.
3. In the **Name** box, type a name for the Monitor.
   In our example, we type **sap_http**.
4. From the **Type** list, select **HTTP**.
   The HTTP Monitor configuration options appear.
5. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a 1:3 +1 ratio between the interval and the timeout. In our example, we use an **Interval** of **30** and a **Timeout** of **91.**
6. In the **Send String** and **Receive Rule** boxes, you can add a Send String and Receive Rule specific to the device being checked.

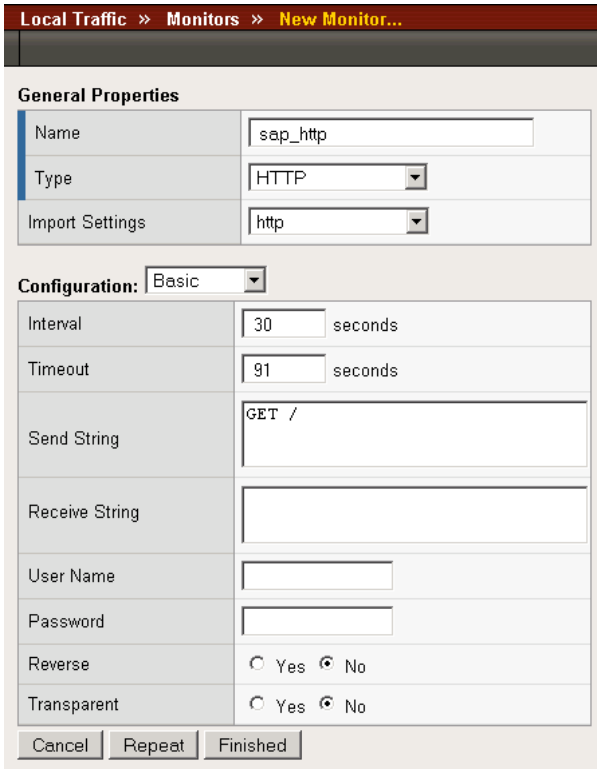

Figure 1.4 *Creating the HTTP Monitor*

7. Click the **Finished** button.
   The new monitor is added to the Monitor list.

Remember that if you configure a Send String and Receive String specific to one of the application components, you should create a new monitor for the other components.

Creating the pool

The next step is to create a pool on the BIG-IP LTM system for the SAP Enterprise Portal nodes.

To create a new pool for the Enterprise portal servers

1. On the Main tab, expand **Local Traffic**, and then click **Pools**.
   The Pool screen opens.
2. In the upper right portion of the screen, click the **Create** button.
   The New Pool screen opens.
   Note: *For more (optional) pool configuration settings, from the Configuration list, select* ***Advanced****. Configure these settings as applicable for your network.*
3. In the **Name** box, type a name for the pool. We use **sap_portal**.
4. In the **Health Monitors** section, select the name of the monitor you created in the *Creating the HTTP health monitor* section, and click the Add (**<<**) button. In our example, we select **sap_http**.
5. From the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).
   In our example, we select **Least Connections**.
6. In the New Members section, make sure the **New Address** option button is selected.
7. In the **Address** box, add the first server to the pool. In our example, we type **10.132.81.1**.
8. In the **Service Port** box, type the appropriate port. In our example, we type **80**. Your SAP Portal services might be running on a different TCP port, such as port **50000**. Type the proper port number here, and the BIG-IP LTM system will properly perform the translation.
   If you are using the BIG-IP LTM system for offloading SSL, see *Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment*, on page 1-26 after completing this section.
9. Click the **Add** button to add the member to the list.
10. Repeat steps 9-11 for each SAP Enterprise Portal server. In our example, we repeat these steps for **10.132.81.2** and **10.132.81.3**.
11. Click the **Finished** button.

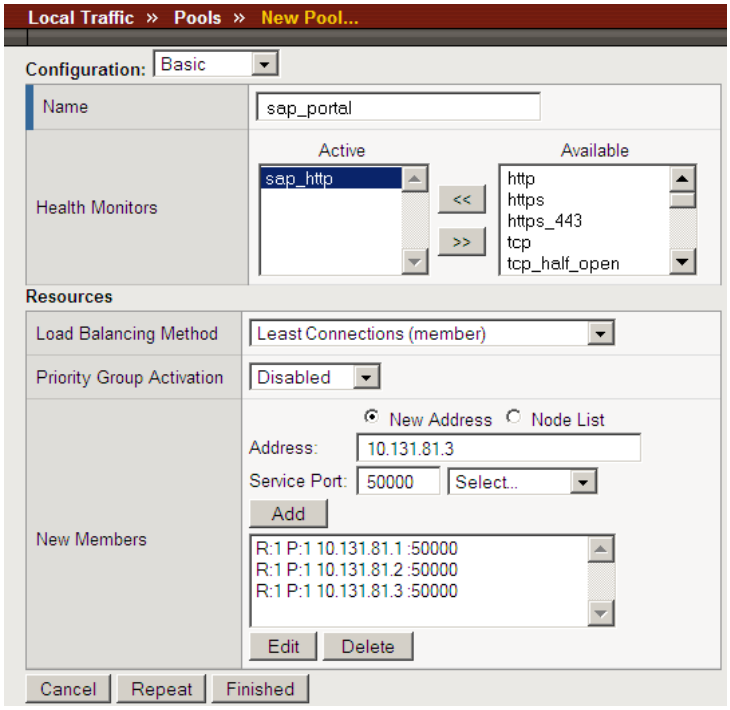

Figure 1.5 *Creating the pool for the Enterprise Portal devices*

Creating profiles

BIG-IP version 9.0 and later use profiles. A ***profile*** is an object that contains user-configurable settings, with default values, for controlling the behavior of a particular type of network traffic, such as HTTP connections. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

Although it is possible to use the default profiles, we strongly recommend you create new profiles based on the default parent profiles, even if you do not change any of the settings initially. Creating new profiles allows you to easily modify the profile settings specific to this deployment, and ensures you do not accidentally overwrite the default profile.

Important

If you are using NTLM authentication instead of SAP Single Sign-on, Kerberos or other SAP default authentication methods for SAP Enterprise Portal, do not use a OneConnect profile on the BIG-IP system for this deployment. Note that a OneConnect profile is part of this configuration in this guide because the default SAP authentication method is not NTLM.

Creating an HTTP profile

The first new profile we create is an HTTP profile. The HTTP profile contains numerous configuration options for how the BIG-IP LTM system handles HTTP traffic. For implementations where the majority of users accessing SAP Enterprise Portal are connecting across a WAN, F5 recommends enabling compression and caching on the BIG-IP LTM by using a profile introduced in BIG-IP version 9.4 called **http-wan-optimized-compression-caching**. This profile uses specific compression and caching (among other) settings to optimize traffic over the WAN. Note that to properly use this profile, you need to have compression and caching licensed on the BIG-IP LTM. For more information on licensing, contact your sales representative.

Tip

*If you are using a version of BIG-IP LTM previous to v9.4, the **Configuration Guide for BIG-IP Local Traffic Management** for version 9.4 (available on **AskF5**) shows the configuration differences between the base HTTP profile and the optimized profile types. Use the Configuration Guide to manually configure the optimization settings.*

Important

*If you are using BIG-IP LTM version 9.4.2 or later with the WebAccelerator module, use the **http-acceleration** parent profile.*

In our example, we also configure the HTTP profile to encrypt the SAP cookie as well as the BIG-IP LTM cookie. This helps prevent cookie tampering attacks by denying malicious users from modifying the otherwise cleartext cookie to gain unauthorized access. Although encrypting cookie is optional, we recommend it. In BIG-IP LTM version 9.4, you simply click a check box for cookie encryption. In versions prior to 9.4, you need to configure an iRule to perform the encryption. See the following post on DevCentral for more information:
http://devcentral.f5.com/weblogs/Joe/archive/2005/11/09/1541.aspx

If you are using the BIG-IP LTM system to offload SSL traffic from the SAP deployment, you need to configure an alternate HTTP profile, among other settings. After completing the Enterprise Portal configuration, be sure to see *Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment*, on page 1-26.

To create a new HTTP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New HTTP Profile screen opens.
3. In the **Name** box, type a name for this profile. In our example, we type **sap_http-opt**.

4. From the **Parent Profile** list, select **http-wan-optimized-compression-caching**. The profile settings appear. If you are using BIG-IP LTM version 9.4.2 with the WebAccelerator module, use the **http-acceleration** parent profile.
5. *Optional:* Click a check in the Custom box in the **Encrypt Cookies** row. Type the name of the cookies you want to encrypt, with a space between each cookie. In our example, we type the name of the SAP cookie (**MYSAPSSO2** by default), and the BIG-IP cookie (**BIGipServer<***Name_of_Pool***>** by default, so in our example, **BIGipServersap_portal**).
   You can either modify the Cookie Passphrase or leave it at the default. In our example, we leave it at the default.
6. Check the Custom box for **Content Compression**, and leave **Content List** selected.
7. In the Content List section, add the following items to the existing entries in the **Content Type** box one at a time, each followed by clicking **Include**:
   - **application/pdf**
   - **application/vnd.ms-powerpoint**
   - **application/vnd.ms-excel**
   - **application/msword**
   - **application/vnd.ms-publisher**

   We add these MIME types to ensure these highly compressible document types are compressed.

   Note: *If you are using the WebAccelerator in your deployment, you do not need to add these MIME types.*
8. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
9. Click the **Finished** button.

Creating the TCP profiles

The next profiles we create are the TCP profiles. If most of the Enterprise Portal users are accessing the portal via a Local Area Network, we recommend using the base TCP profile as the parent. If the majority of the Enterprise Portal users are accessing the system from remote or home offices, we recommend using two new profiles available in BIG-IP LTM version 9.4, called **tcp-wan-optimzed** (for client side TCP connections) and

tcp-lan-optimized (for server-side TCP connections). In our example, we leave these profiles at their default levels; you can configure any of the options as applicable for your network.

Tip

*If you are using a version of BIG-IP LTM previous to v9.4, the **Configuration Guide for BIG-IP Local Traffic Management** for version 9.4 (available on **AskF5**) shows the configuration differences between the base TCP profile and the optimized profile types. Use the Configuration Guide to manually configure the optimization settings.*

Creating the WAN optimized TCP profile

First we configure the WAN optimized profile. Remember, if most users are accessing the portal via the LAN, use the base TCP profile instead of this WAN optimized profile.

To create a new TCP WAN optimized profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Protocol** menu, click **tcp**.
3. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **sap_tcp-wan**.
5. From the **Parent Profile** list, select **tcp-wan-optimized**.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating the LAN optimized TCP profile

Now we configure the LAN optimized profile. If you have already created a simple TCP profile, based off the default TCP profile (and not the WAN optimized profile above), you do not need to create another TCP profile, continue with the next procedure.

To create a new TCP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Protocol** menu, click **tcp**.
3. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.

4. In the **Name** box, type a name for this profile. In our example, we type **sap_tcp-lan**.
5. From the **Parent Profile** list, select **tcp-lan-optimized** if you are using BIG-IP LTM version 9.4 or later; otherwise select **tcp**.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating a OneConnect profile

The next profile we create is a OneConnect profile. With OneConnect enabled, client requests can utilize existing, server-side connections, thus reducing the number of server-side connections that a server must open to service those requests. Testing has demonstrated that this can provide significant performance improvements for SAP implementations. For more information on OneConnect, see the BIG-IP LTM documentation.

In our example, we leave all the options at their default settings. You can configure these options as appropriate for your network. Remember, if you are using NTLM authentication instead of SAP Single Sign-on, Kerberos or other SAP default authentication methods, ***do not*** use a OneConnect profile on the BIG-IP system for this deployment.

To create a new OneConnect profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Other** menu, click **OneConnect**. The Persistence Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button. The New HTTP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **sap_oneconnect**.
5. From the **Parent Profile** list, ensure that **oneconnect** is selected.
6. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

For more information on creating or modifying profiles, or applying profiles in general, see the BIG-IP documentation.

Creating persistence profiles

The final profiles we create are Persistence profiles. In this case, we create two persistence profiles; a default and a fallback persistence profile. Because we are using HTTP cookie insert persistence as our default mode, we need the fallback mode in case the user's device does not accept cookies.

Creating the Cookie Persistence profile

The first persistence profile we create is the Cookie Persistence profile. In this profile there are some optional settings you can configure, such as the method of cookie persistence and the expiration. In out experience, SAP expects persistence to be maintained for 8 hours. As a result, we set the time out value in this profile to 8 hours and 1 minute.

To create a new cookie persistence profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
   The HTTP Profiles screen opens.
2. On the Menu bar, click **Persistence**.
   The Persistence Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button.
   The New Persistence Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **sap_cookie**.
5. From the **Persistence Type** list, select **Cookie**.
   The configuration options for cookie persistence appear.
   Make sure the Parent Profile is set to **Cookie**.
6. In the **Expiration** row, click a check in the Custom box. Clear the Session Cookie box, and the Expiration values appear. In the **Hours** box, type **8**, and in the **Minutes** box, type **1**.
7. Modify any of the other settings as applicable for your network.
8. Click the **Finished** button.

Creating the Fallback Persistence profile

Now we configure the fallback persistence profile. In our example, we use Source Address Affinity for the fallback persistence type.

To create a new fallback persistence profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
   The HTTP Profiles screen opens.
2. On the Menu bar, click **Persistence**.
   The Persistence Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button.
   The New Persistence Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **sap_source**.
5. From the **Persistence Type** list, select **Source Address Affinity**.
   The configuration options for Source Address Affinity persistence appear.

6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating the virtual server

Next, we configure a virtual server that uses the profiles and pool you created in the preceding procedures.

To create the virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**.
   The Virtual Servers screen opens.
2. In the upper right portion of the screen, click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** box, type a name for this virtual server. In our example, we type **sap_portal_vs**.
4. In the **Destination** section, click the **Host** button.
5. In the **Address** box, type the IP address of this virtual server. In our example, we use **10.133.21.15**.
6. In the **Service Port** box, type **80**.

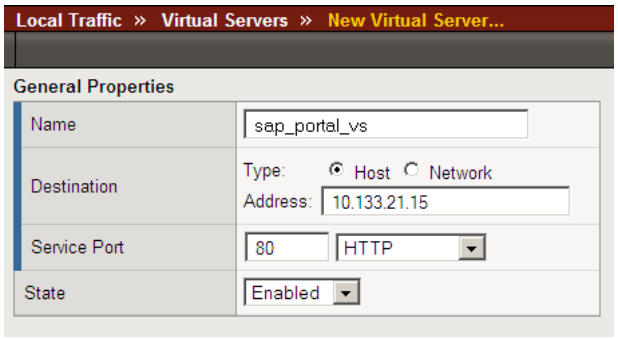

Figure 1.6 *Creating the new virtual server*

7. From the Configuration list, select **Advanced**.
   The Advanced configuration options appear.
8. Leave the **Type** and **Protocol** lists at their default settings: **Standard** and **TCP**.
9. From the **Protocol Profile (Client)** list, select the name of the profile you created in the *Creating the WAN optimized TCP profile* section. In our example, we select **sap_tcp-wan**.

10. From the **Protocol Profile (Server)** list, select the name of the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **sap_tcp-lan**.
11. From the **OneConnect Profile** list, select **sap_oneconnect**.
12. From the HTTP Profile list, select the name of the profile you created in the *Creating an HTTP profile* section. In our example, we select **sap_http-opt** (see Figure 1.7).

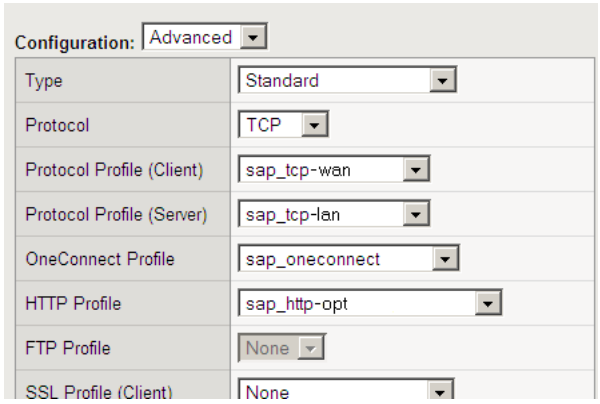

Figure 1.7 *Selecting the profiles for the virtual server*

13. In the Resources section, from the **Default Pool** list, select the pool you created in the *Creating the pool* section. In our example, we select **sap_portal**.
14. From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating persistence profiles* section. In our example, we select **sap_cookie**.

15. From the **Fallback Persistence Profile** list, select the profile you created for the fallback persistence method in the *Creating persistence profiles* section. In our example, we select **sap_source**.

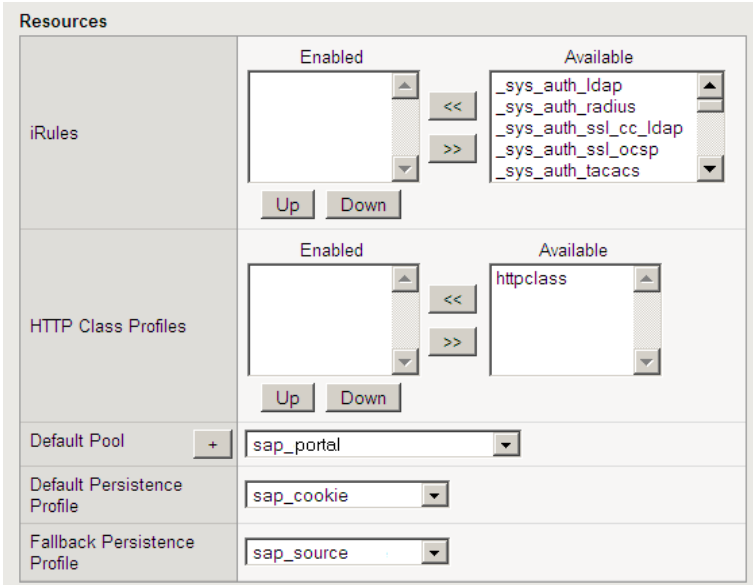

Figure 1.8 *Resources section of the add virtual server page*

16. Click the **Finished** button. The BIG-IP LTM configuration for SAP Enterprise Portal is now complete.

Configuring the BIG-IP LTM system for the SAP ERP Central Component (ECC)

In this section, we configure the BIG-IP LTM system for directing traffic to one of the SAP application components called SAP ERP Central Component (ECC). As mentioned in the introduction, there are a large number of SAP application components available. This Deployment Guide covers the SAP ECC as an example component application. If you have other component applications, such as SAP Exchange Infrastructure, or Business Warehouse, repeat this entire section for each one, replacing names, IP addresses and ports as applicable. In this Deployment Guide, we are configuring high availability for internal services accessed over the Local Area Network.

Creating the TCP health monitor

For ECC, we create a simple TCP health monitor, based off the default TCP monitor. Although the monitor in the following example is quite simple, you can configure optional settings such as Send and Receive Strings to make the monitor much more specific. You can also use one of the other types of monitors available on the BIG-IP LTM system.

To configure a TCP health monitor

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**.
   The Monitors screen opens.
2. Click the **Create** button.
   The New Monitor screen opens.
3. In the **Name** box, type a name for the Monitor.
   In our example, we type **sap_tcp**.
4. From the **Type** list, select **TCP**.
   The TCP Monitor configuration options appear.
5. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a 1:3 +1 ratio between the interval and the timeout. In our example, we use an **Interval** of **30** and a **Timeout** of **91.**
6. In the Send String and Receive Rule sections, you can add an optional Send String and Receive Rule specific to the device being checked.
7. Click the **Finished** button.
   The new monitor is added to the Monitor list.

Remember that if you configure a Send String and Receive String specific to one of the application components, you should create a new monitor for the other components.

Creating the pool

The next step is to create a pool on the BIG-IP LTM system for the application components. In our example, we create a pool containing the IP address and Port for the SAP ECC J2EE instances. For more information on these components, see the SAP documentation.

Our example is based on an Instance Number of 50. As a result, our TCP port for the application service is 55000. Other components will have different Instance Numbers, but you should find the required TCP ports to be in the form of 5NN00 for the HTTP application server traffic.

To create the Internet Connection Manager pool

1. On the Main tab, expand **Local Traffic**, and then click **Pools**.
   The Pool screen opens.
2. In the upper right portion of the screen, click the **Create** button.
   The New Pool screen opens.
   Note: *For more (optional) pool configuration settings, from the Configuration list, select* ***Advanced****. Configure these settings as applicable for your network.*
3. In the **Name** box, enter a name for your pool.
   In our example, we use **sap_ecc_55000**.
4. In the **Health Monitors** section, select the name of the monitor you created in the *Creating the TCP health monitor* section, and click the Add (**<<**) button. In our example, we select **sap_tcp**.
5. From the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).
   In our example, we select **Least Connections (node)**.
6. In the New Members section, make sure the **New Address** option button is selected.
7. In the **Address** box, add the first server to the pool. In our example, we type **10.133.20.1**.
8. In the **Service Port** box, the appropriate port for this component. In our example, we type **55000**. If you modified this port for ECC in the SAP configuration, you need to use that port.
9. Click the **Add** button to add the member to the list.
10. Repeat steps 9-11 for each server you want to add to the pool.
    In our example, we repeat these steps once for **10.133.20.2** and **10.133.20.3**.
11. Click the **Finished** button.

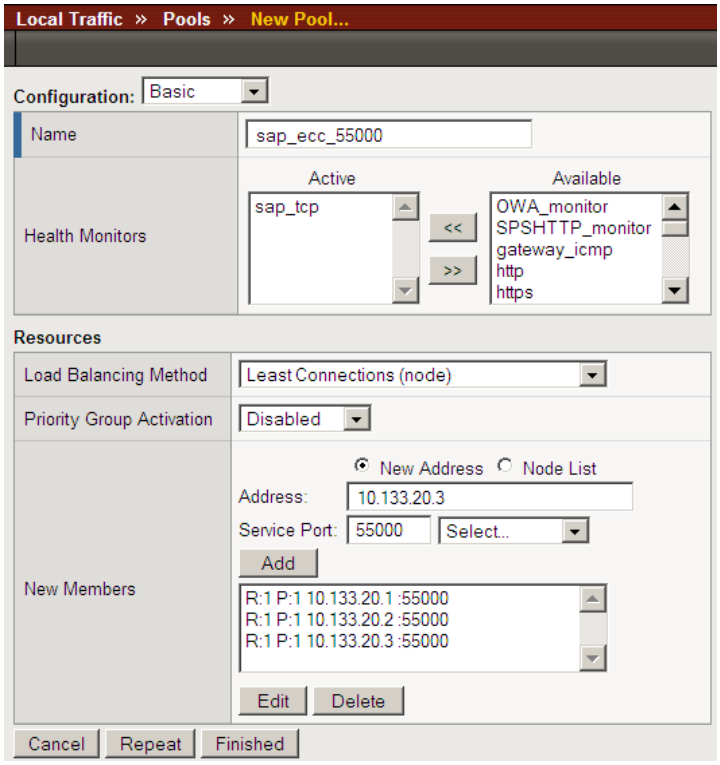

Figure 1.9 *Creating the pool for the ECC devices*

Creating the profiles

In our example, we use the same profiles for the ECC that we created for the SAP Portal in *Creating profiles*, on page 1-11, with the exception of the HTTP profile, and possibly the TCP profile.

If you need to change other BIG-IP profiles you created earlier for individual SAP application components, we recommend creating new profiles using the previous profiles as the parent.

Important

If you are using NTLM authentication instead of SAP Single Sign-on, Kerberos or other SAP default authentication methods for SAP Enterprise Portal, do not use a OneConnect profile on the BIG-IP system for this deployment. Note that a OneConnect profile is part of this configuration in this guide because the default SAP authentication method is not NTLM.

Creating the HTTP profile

In this procedure, we create a new HTTP profile. If you are using the BIG-IP LTM system to offload SSL traffic, there are additional modifications to this profile you need to make. See *Creating the new HTTP profile*, on page 1-28.

To create a new HTTP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New HTTP Profile screen opens.
3. In the **Name** box, type a name for this profile. In our example, we type **sap_http-ecc**.
4. From the **Parent Profile** list, select **http**. The profile settings appear.
5. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
6. Click the **Finished** button.

Creating the TCP profile

Next is the TCP profile. In our example, we use the same LAN optimized TCP profile we configured for the Enterprise Portal (see *Creating the LAN optimized TCP profile*, on page 1-14). If there are specific settings you want to change for the particular component application, we recommend you configure a new TCP profile, based on the **tcp-lan-optimized** profile.

Creating the virtual server

Next, we configure a virtual server that reference the profiles and pool you created in the preceding procedures. In our testing with SAP, we found that persistence was not required for the application server connections. As a result, no persistence is configured for this virtual server. If you find that your implementation requires persistence, refer to the persistence and virtual server configuration for the Enterprise Portal servers discussed earlier in this guide.

To create the virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**.
   The Virtual Servers screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New Virtual Server screen opens.

3. In the **Name** box, type a name for this virtual server. In our example, we type **sap_ecc_55000**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type the IP address of this virtual server. In our example, we use **10.133.21.15**.
6. In the **Service Port** box, type **55000**. Note that this port should match the port number of the pool you created, so if you are using a different port for ECC, use this port here (see Figure 1.10).

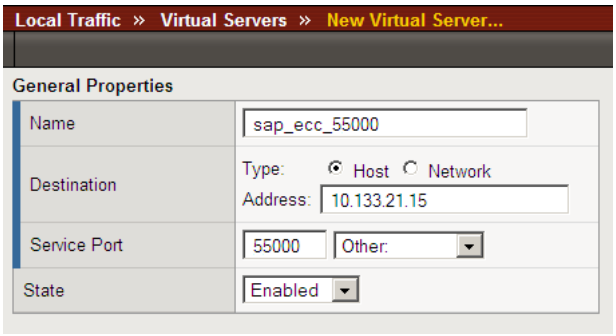

Figure 1.10 *Creating the SAP ECC virtual server*

7. From the Configuration list, select **Advanced**.
   The Advanced configuration options appear.
8. Leave the **Type** list at the default setting: **Standard**.
9. From the **Protocol Profile (Client)** list select the name of the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **sap_tcp-lan**.
10. Leave the **Protocol Profile (Server)** option at the default setting, or you can select **sap_tcp-lan** from the list.
11. From the **OneConnect Profile** list, select **sap_oneconnect**.
12. From the HTTP Profile list, select the name of the profile you created in the *Creating the HTTP profile* section. In our example, we select **sap_http-ecc** (see Figure 1.11).

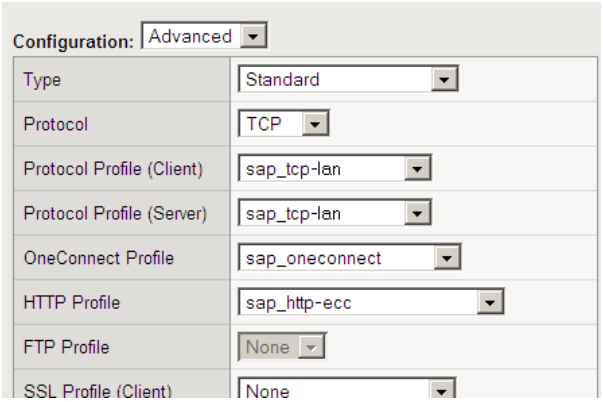

Figure 1.11 *Selecting the profiles for the virtual server*

13. In the Resources section, from the **Default Pool** list, select the pool you created in the *Creating the pool* section. In our example, we select **sap_ecc_55000**.

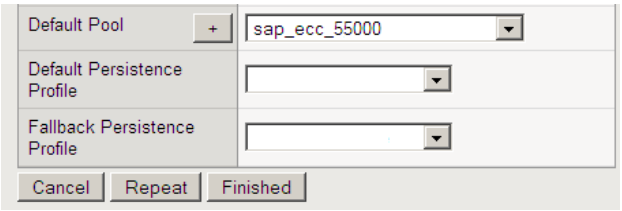

Figure 1.12 *Resources section of the add virtual server page*

14. Click the **Finished** button.

Creating a default SNAT

This SNAT is in place to ensure that the inter-application traffic is routed back to the BIG-IP LTM system.

To create a default SNAT

1. On the Main tab, expand **Local Traffic**, and then click **SNATs**. The SNATs screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New SNAT screen opens.
3. In the **Name** box, type a name for this SNAT. In our example, we type **sapSNAT**.

4. In the **Translation** list, select **Automap**. With Automap, the BIG-IP LTM system maps one or more client IP addresses using all system self IP addresses as the translation addresses. For more information on SNAT or SNAT Automap, see the BIG-IP LTM manuals.
5. ***Optional:*** If you to disable (or enable) the default SNAT for specific VLANs, from the VLAN Traffic list, select either **Enabled on** or **Disabled on** from the list. From the Available list, select the appropriate VLAN and click the Add (<<) button to move it to the Selected list.
6. Click the **Finished** button.

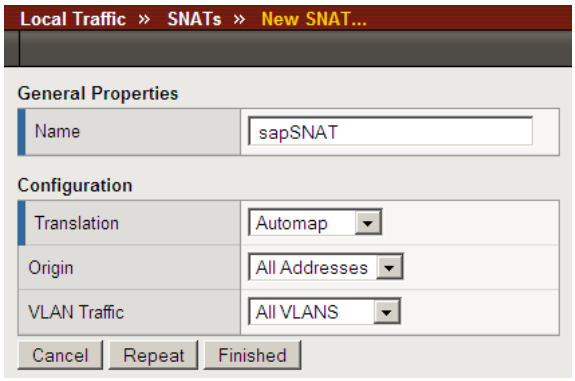

Figure 1.13 *Creating a Default SNAT*

The configuration for the SAP ECC is now complete. Repeat this section for any additional SAP application components you may be using.

Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment

The BIG-IP LTM device can be configured as an SSL proxy, offloading the SSL duties from the servers. F5's testing, performed in conjunction with SAP, demonstrated significant increases in efficiency for the Enterprise Portal and component application servers when SSL processing was offloaded to the F5 BIG-IP LTM. If you want to use this functionality, you must complete the following procedures.

Important

This section is optional, and only necessary if you are using the BIG-IP LTM system for offloading SSL.

Using SSL certificates and keys

Before you can enable the BIG-IP system to act as an SSL proxy, you must install a SSL certificate on the virtual server that you wish to use for SAP connections on the BIG-IP device. For this Deployment Guide, we assume that you already have obtained an SSL certificate, but it is not yet installed on the BIG-IP system. For information on generating certificates, or using the BIG-IP system to generate a request for a new certificate and key from a certificate authority, see the Managing SSL Traffic chapter in the ***Configuration Guide for Local Traffic Management***.

Importing keys and certificates

Once you have obtained a certificate, you can import this certificate into the BIG-IP system using the Configuration utility. By importing a certificate or archive into the Configuration utility, you ease the task of managing that certificate or archive. You can use the Import SSL Certificates and Keys screen only when the certificate you are importing is in Privacy Enhanced Mail (PEM) format.

To import a key or certificate

1. On the Main tab, expand Local Traffic.
2. Click **SSL Certificates**.
   This displays the list of existing certificates.
3. In the upper right corner of the screen, click **Import**.
4. From the **Import** list, select the type of import (**Key** or **Certificate**).
5. Select the import method (text or file).
6. Type the name of the key or certificate.
7. Click **Import**.

If you imported the certificate in the preceding procedure, repeat the entire procedure for the key.

Creating additional profiles

When using the BIG-IP LTM system to offload SSL traffic, you need to create two additional profiles. The first is a new Client SSL profile, and the second is a slightly modified HTTP profile that instructs the SAP server to respond with the appropriate content, and directs the BIG-IP LTM system to rewrite the URI in all HTTP redirect responses.

The following profiles can be created whether you are configuring the BIG-IP LTM for the Enterprise Portal or application component servers.

Creating a Client SSL profile

The first profile is the SSL profile. This profile contains the SSL certificate and Key information for offloading the SSL traffic.

To create a new Client SSL profile based on the default profile

1. On the Main tab, expand **Local Traffic**.
2. Click **Profiles**.
   The HTTP Profiles screen opens.
3. On the Menu bar, from the **SSL** menu, select **Client**.
   The Client SSL Profiles screen opens.
4. In the upper right portion of the screen, click the **Create** button.
   The New Client SSL Profile screen opens.
5. In the **Name** box, type a name for this profile. In our example, we type **sap_clientssl**.
6. In the Configuration section, click a check in the **Certificate** and **Key** Custom boxes.
7. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section.
8. From the **Key** list, select the key you imported in the *Importing keys and certificates* section.
9. Click the **Finished** button.

For more information on creating or modifying profiles, or SSL Certificates, see the BIG-IP documentation.

Creating the new HTTP profile

The next profile is a new HTTP profile that contains the necessary client header, along with the rewrite/redirect setting. You must have an HTTP profile with the settings in the following procedure for each SAP virtual server that will be offloading SSL.

If you have already created an HTTP profile as described earlier in this guide, you can modify that profile with the modifications found in the following procedure.

To create a new HTTP profile for SSL

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
   The HTTP Profiles screen opens.
2. In the upper right portion of the screen, click the **Create** button.
   The New HTTP Profile screen opens.
3. In the **Name** box, type a name for this profile. In our example, we type **sap_ssl**.

4. From the **Parent Profile** list, ensure that **HTTP** is selected.
5. In the **Request Header Insert** row, click a check in the Custom box. In the box, type: **clientprotocol: https**.
6. In the **Redirect Rewrite** row, click a check in the Custom box. From the list, select **Matching**.
7. *Optional for virtual servers requiring Cookie Persistence:* In the **Encrypt Cookies** row, click a check in the Custom box. Type the name of the cookies you want to encrypt, with a space between each cookie. In our example, we type the name of the SAP cookie (**MYSAPSSO2** by default), and the BIG-IP cookie (**BIGipServer<***Name_of_Pool***>** by default, so in our example, **BIGipServersap_portal**).

   You can either modify the Cookie Passphrase or leave it at the default. In our example, we leave it at the default level.
8. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
9. Click the **Finished** button (see Figure 1.14).

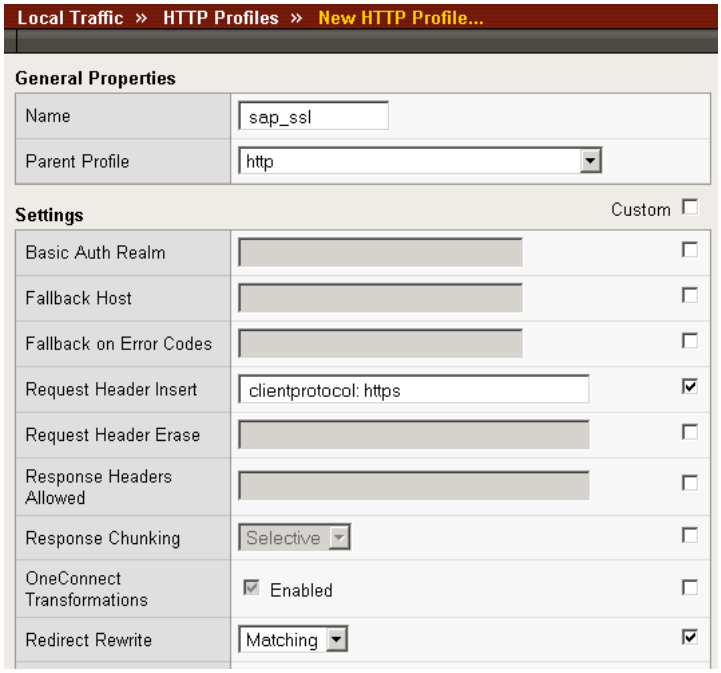

Figure 1.14 *Creating the HTTP profile for SSL deployments*

For more information on creating or modifying profiles, or applying profiles in general, see the BIG-IP documentation.

Creating the Redirect iRule

The next step is to create an iRule that redirects all traffic to same hostname (stripping port if it exists), same URI over HTTPS. This iRule catches the traffic that incorrectly comes in on HTTP and redirects it to HTTPS. This ensures that SSL traffic remains on the virtual server that supports the traffic. The iRule will be applied to an HTTP Virtual Server where required.

To create the redirect iRule

1. On the Main tab, expand **Local Traffic**, and then click **iRules**.
2. In the upper right portion of the screen, click the **Create** button. The New iRule screen opens.
3. In the **Name** box, enter a name for your iRule. In our example, we use **sap_httptohttps**.
4. In the Definition section, copy and paste the following iRule:

```
when HTTP_REQUEST {
  HTTP::redirect https://[getfield [HTTP::host] ":" 1][HTTP::uri]
}
```

5. Click the **Finished** button.

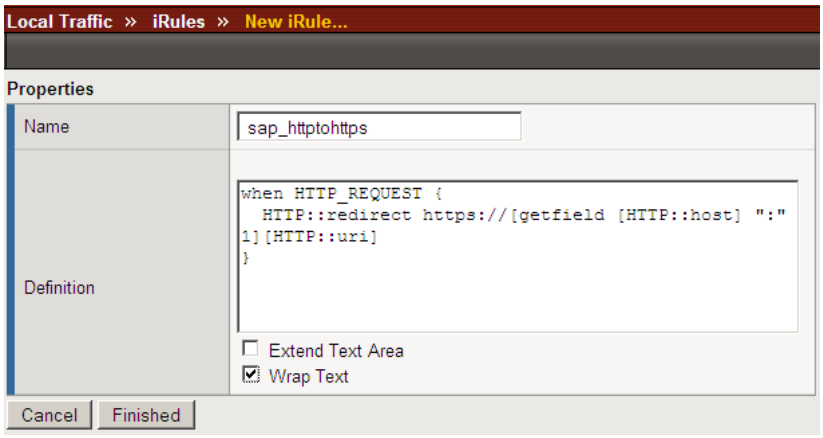

Figure 1.15 *Creating the redirect iRule*

The iRule is now complete. You use this iRule when you modify the existing SAP Enterprise Portal virtual server on port 80 in *Modifying the SAP Enterprise Portal virtual server*, on page 1-33.

Creating an HTTPS virtual server

The next step is to create a virtual server for the SSL offload that will use the Client SSL profile you just created. The example virtual server is for SAP Enterprise Portal. As a result, TCP WAN and LAN optimized profiles

are used along with a Cookie Persistence profile. These settings would not necessarily apply if this were a virtual server dedicated to managing traffic between SAP application components.

To create a new HTTPS virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**.
   The Virtual Servers screen opens.
2. In the upper right portion of the screen, click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** box, type a name for this virtual server. In our example, we type **sap_erp_ssl**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type the IP address of this virtual server. In our example, we use **10.133.21.15**.
6. In the **Service Port** box, type **443**, or select **HTTPS** from the list.

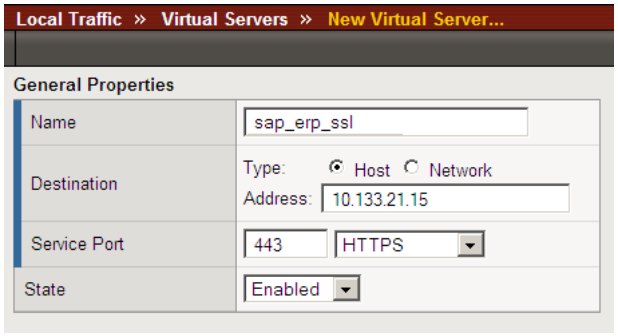

Figure 1.16 *Creating the HTTPS virtual server*

7. From the Configuration list, select **Advanced**.
   The Advanced configuration options appear.
8. Leave the **Type** list at the default setting: **Standard**.
9. From the **Protocol Profile (Client)** list, select a tcp profile. If you are configuring this virtual server for Enterprise Portal, select the tcp profile you created in *Creating the WAN optimized TCP profile*. If this is for a component application, select the profile you created in *Creating the TCP profile*.
10. From the **Protocol Profile (Server)** select the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **sap_tcp-lan** from the list.
11. From the **OneConnect Profile** list, select **sap_oneconnect**.

12. From the **HTTP Profile** list, select the name of the profile you created in the *Creating the new HTTP profile* section. In our example, we select **sap_ssl**.
13. From **SSL Profile (Client)** list, select the name of the profile you created in the *Creating a Client SSL profile* section. In our example we select **sap_clientssl** (see Figure 1.17).

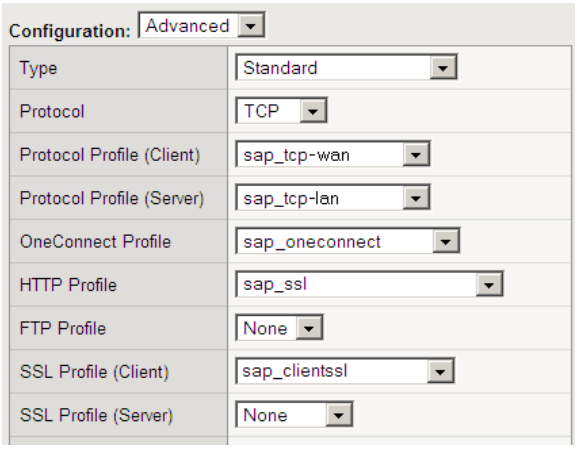

Figure 1.17 *Selecting the profiles for the HTTPS virtual server*

14. In the Resources section, from the **Default Pool** list, select the pool you created for your SAP Portal nodes in the *Creating the pool* section. In our example, we select **sap_portal**.
15. From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating persistence profiles* section. In our example, we select **sap_cookie**.
16. From the **Fallback Persistence Profile** list, select the profile you created for the fallback persistence method in the *Creating persistence profiles* section. In our example, we select **sap_source**.

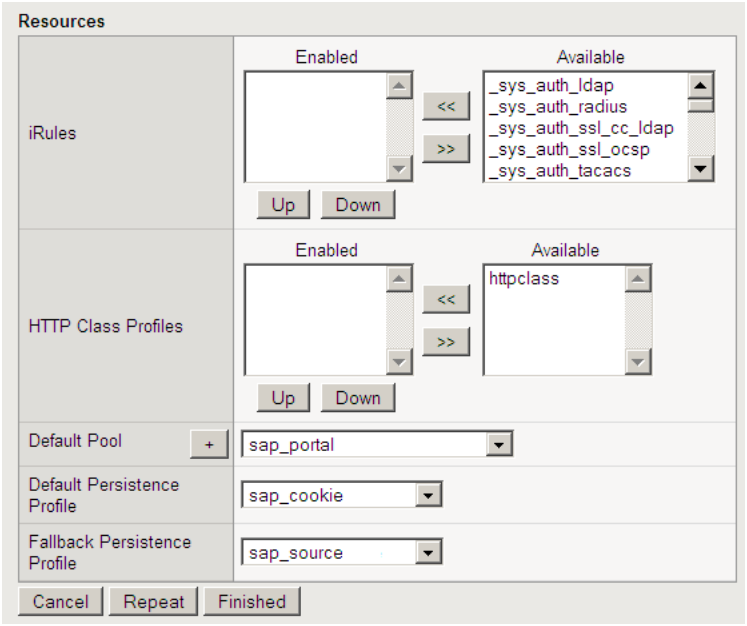

Figure 1.18 *Resources section of the add virtual server page*

17. Click the **Finished** button.

Modifying the SAP Enterprise Portal virtual server

In this procedure, we modify the portal virtual server on port 80 that you created in the *Creating the pool*, on page 1-10, to use the iRule instead of the pool. This iRule is in place to ensure that any accidental requests to port 80 are redirected to the SSL virtual server.

To modify the Enterprise Portal virtual server to use the iRule

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. From the list, click the virtual server you created in *Creating the virtual server*, on page 1-17. In our example, we click **sap_portal_vs**. The Virtual Server properties page opens.
3. On the Menu bar, click **Resources**.
4. In the iRules section, click the **Manage** button.
   The iRules Resource Management screen opens.
5. From the **Available** list, select the iRule you created in the *Creating the Redirect iRule* section, and click the Add (<<) button.
   In our example, we select **sap_httptohttps**.

6. Click the **Finished** button.
   You return to the Resources page.
7. From the Default Pool list, select **None**.
8. Click the **Update** button.

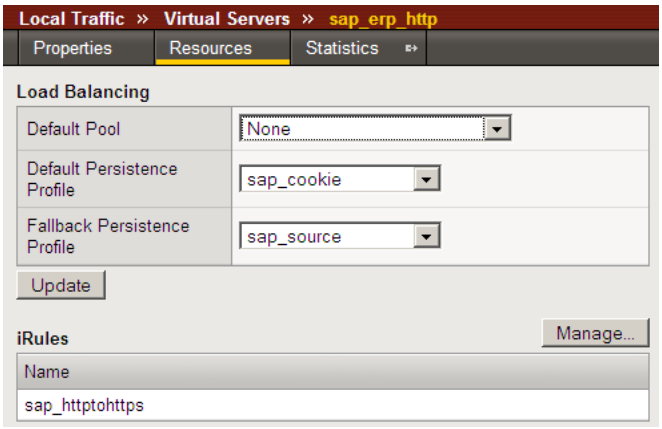

Figure 1.19 *Modifying the virtual server to use the iRule and not the pool.*

This concludes the steps necessary to use the BIG-IP LTM system to offload SSL traffic.

Appendix A: Backing up and restoring the BIG-IP system configuration

We recommend saving your BIG-IP configuration before you begin this configuration. When you save the BIG-IP configuration, it collects the following critical data and compress it into a single User Configuration Set (UCS) file:

- BIG-IP configuration files
- BIG-IP license and passwords
- SSL certificates
- SSH keys

Saving and restoring the BIG-IP configuration

The Configuration Management screen allows you to save and restore all configuration files that you may edit to configure a BIG-IP system. These configuration files are called a User Configuration Set (UCS). The Configuration Management screen contains sections for saving and restoring a configuration. The list boxes in these sections display only files in the **/usr/local/ucs** directory. If you want to save or restore files from another directory, you must type the full path in the box.

To save the BIG-IP configuration using the Configuration utility

1. In the navigation pane, click **System Admin**.
   The User Administration screen displays.
2. Click the Configuration Management tab.
   The Configuration Management screen displays.
3. In the **Save Current Configuration** section, type the path where you want your configuration file saved or choose a path from the list box. If no path is specified, the BIG-IP saves files to **/usr/local/ucs**. The BIG-IP appends the extension.ucs to file names without it.
   In our example, we type **pre_sap_backup.ucs.**
4. Click the **Save** button to save the configuration file.

To restore a BIG-IP configuration

1. In the navigation pane, click **System Admin**.
   The User Administration screen displays.
2. Click the Configuration Management tab.
   The Configuration Management screen displays.

3. In the **Restore a Configuration** section, choose the configuration file you want to restore from the list box, or type the path where your configuration files were saved.
4. Click the **Restore** button.
   To check the status of the restoration, click the **View Log** button. You should wait a few moments for the log file to start generating before you click **View Log**. Repeated clicking of this button will update your screen with the most current log file information until the restoration is complete.

2

Configuring the F5 WebAccelerator module with SAP Enterprise Portal

- Configuring the WebAccelerator module
- Creating an HTTP Class profile
- Modifying the Virtual Server to use the Class profile
- Creating an Application

Configuring the F5 WebAccelerator module with SAP Enterprise Portal

In this section, we configure the WebAccelerator module for the SAP Enterprise Portal (EP) devices to increase performance for end users. The F5 WebAccelerator is an advanced web application delivery solution that provides a series of intelligent technologies designed to overcome problems with browsers, web application platforms and WAN latency issues which impact user performance.

As mentioned in the previous chapter, the BIG-IP LTM version 9, in conjunction with WebAccelerator, has achieved the following SAP certifications:

- Network Performance Optimization for Enterprise SOA-Based Solutions
- SOA Landscapes Access Reliability and Availability Through Networks
- Network Security for Enterprise SOA-Based Solutions

For more information on the F5 WebAccelerator, see **http://www.f5.com/products/WebAccelerator/**.

Prerequisites and configuration notes

The following are prerequisites for this section:

- We assume that you have already configured the BIG-IP LTM system for directing traffic to the SAP deployment as described in this Deployment Guide.
- You must have purchased and licensed the WebAccelerator module on the BIG-IP LTM system, version 9.4 or later.
- If you are using the BIG-IP LTM version 9.4.2 or later, you must have created an HTTP profile on the BIG-IP LTM system that has RAM Cache enabled. In our example (*Creating an HTTP profile*, on page 1-12) we use a parent profile that includes RAM Cache. If you did not create an HTTP profile with RAM Cache enabled, you must create a new HTTP profile, based on a parent profile that uses RAM Cache (we recommend HTTP Acceleration) and associate it with the virtual server. This is only required for BIG-IP LTM version 9.4.2 and later.
- This document is written with the assumption that you are familiar with the BIG-IP LTM system, WebAccelerator and SAP Enterprise Portal. Consult the appropriate documentation for detailed information.

Configuration example

Using the configuration in this section, the BIG-IP LTM system with WebAccelerator module is optimally configured to accelerate traffic to SAP Enterprise Portal servers. The BIG-IP LTM with WebAccelerator module both increases end user performance as well as offloads the servers from serving repetitive and duplicate content.

In this configuration, a remote client with WAN latency logs onto the SAP portal via the WebAccelerator. The user's request is accelerated on repeat visits by the WebAccelerator instructing the browser to use the dynamic or static object that is stored in its local cache. Additionally, dynamic and static objects are cached at the WebAccelerator so that they can be served quickly without requiring the server to re-serve the same objects.

Configuring the WebAccelerator module

Configuring the WebAccelerator module requires creating an HTTP class profile and creating an Application. The WebAccelerator device has a large number of other features and options for fine tuning performance gains, see the ***WebAccelerator Administrator Guide*** for more information.

Connecting to the BIG-IP device

Use the following procedure to access the BIG-IP system's web-based Configuration utility using a web browser.

To connect to the BIG-IP system using the Configuration utility

1. In a browser, type the following URL:
   https://<administrative IP address of the BIG-IP device>
   A Security Alert dialog box appears, click **Yes**.
   The authorization dialog box appears.
2. Type your user name and password, and click **OK**.
   The Welcome screen opens.

Creating an HTTP Class profile

The first procedure is to create an HTTP class profile. When incoming HTTP traffic matches the criteria you specify in the WebAccelerator class, the system diverts the traffic through this class. In the following example, we create a new HTTP class profile, based on the default profile.

To create a new HTTP class profile

1. On the Main tab, expand **WebAccelerator**, and then click **Classes**.
   The HTTP Class Profiles screen opens.

2. Click the **Create** button.
3. In the **Name** box, type a name for this Class. In our example, we type **SAP_class**.
4. From the Parent Profile list, make sure **httpclass** is selected.
5. In the Configuration section, from the **WebAccelerator** row, make sure **Enabled** is selected.
6. In the Hosts row, click the Custom box, and then from the list select **Match Only**. The Host List options appear.
   a) In the **Host** box, type the host name that your end users use to access the SAP Enterprise Portal. In our example, we type **myportal.companyxyz.com** (see Figure 2.1).
   b) Leave the Entry Type at **Pattern String**.
   c) Click the **Add** button.
   d) Repeat these sub-steps for any other host names users might use to access the SAP deployment.
7. The rest of the settings are optional, configure them as applicable for your deployment.
8. Click the **Finished** button. The new HTTP class is added to the list.

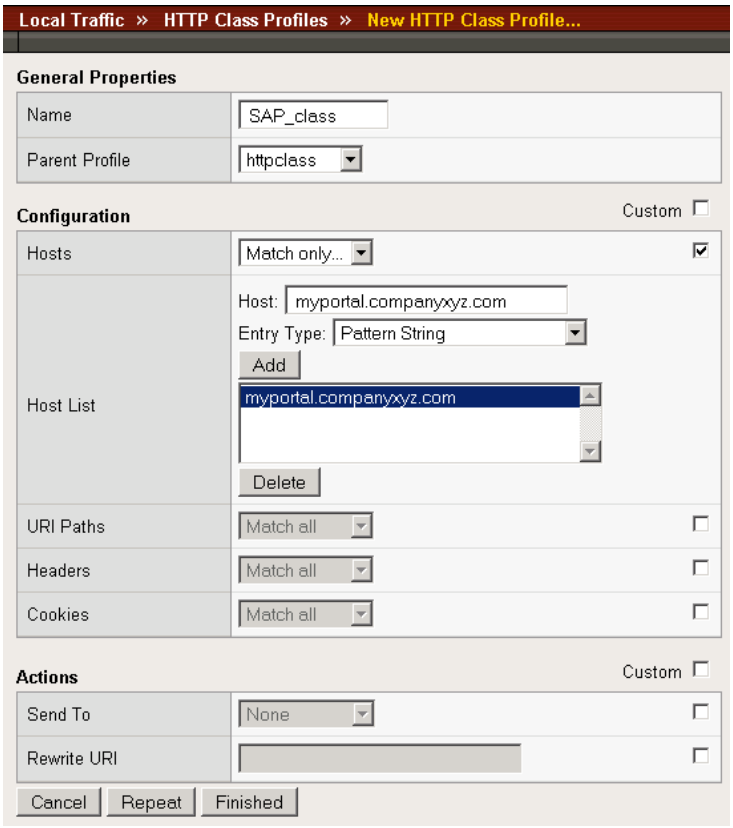

Figure 2.1 *Creating a new HTTP Class profile*

Modifying the Virtual Server to use the Class profile

The next step is to modify the virtual server for your SAP deployment on the BIG-IP LTM system to use the HTTP Class profile you just created.

To modify the Virtual Server to use the Class profile

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. From the **Virtual Server** list, click the name of the virtual server you created for the SAP Enterprise Portal. In our example, we click **sap_portal_vs**.
   The General Properties screen for the Virtual Server opens.
3. On the Menu bar, click **Resources**.
   The Resources screen for the Virtual Server opens.
4. In the HTTP Class Profiles section, click the **Manage** button.
5. From the **Available** list, select the name of the HTTP Class Profile you created in the preceding procedure, and click the Add (**<<**) button to move it to the Enabled box. In our example, we select **SAP_class** (see Figure 2.2).
6. Click the **Finished** button. The HTTP Class Profile is now associated with the Virtual Server.

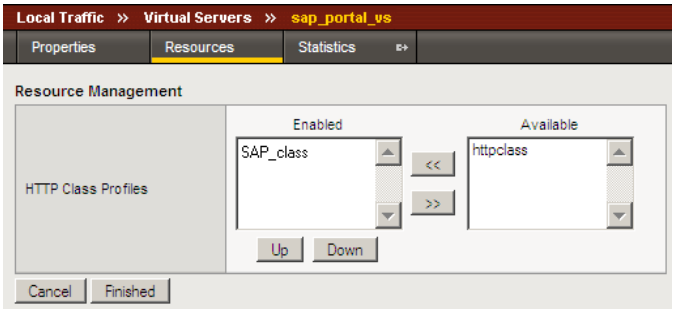

Figure 2.2 *Adding the HTTP Class Profile to the Virtual Server*

Important

*If you are using the BIG-IP LTM version 9.4.2 or later, you must have created an HTTP profile on the BIG-IP LTM system that has RAM Cache enabled. In our example (**Creating an HTTP profile**, on page 1-12) we use a parent profile that includes RAM Cache. If you did not create an HTTP profile with RAM Cache enabled, you must create a new HTTP profile, based on a parent profile that uses RAM Cache (such as HTTP Acceleration), and modify the virtual server to use this new profile. This is only required for BIG-IP LTM version 9.4.2 and later.*

*To create the HTTP profile, use **Creating an HTTP profile**, on page 1-12, selecting the HTTP Acceleration parent profile. You must leave RAM Cache*

enabled; all other settings are optional. To modify the virtual server, follow Steps 1 and 2 from the preceding procedure to access the virtual server, and then from the HTTP Profile list, select the name of the new profile you just created and click Update.

Creating an Application

The next procedure is to create a WebAccelerator Application. The Application provides key information to the WebAccelerator so that it can handle requests to your application appropriately.

To create a new Application

1. On the Main tab, expand **WebAccelerator**, and then click **Applications**.
   The Application screen of the WebAccelerator UI opens in a new window.
2. Click the **Create** button.
3. In the Application Name box, type a name for your application.
   In our example, we type **SAP EP**.
4. In the **Description** box, you can optionally type a description for this application.
5. From the **Central Policies** list, select **SAP Portal**. This is a pre-defined policy created specifically for SAP Enterprise Portal devices (see Figure 2.3).
6. If you are deploying WebAccelerator in a symmetrical deployment, from the **Remote Policy** list, select **SAP Portal**.
   If you not deploying a remote unit, leave this option unselected.
7. In the **Requested Host** box, type the host name that your end users use to access the SAP deployment. This should be the same host name you used in Step 6a in the preceding procedure. In our example, we type **myportal.companyxyz.com**
   If you have additional host names, click the **Add Host** button and enter the host name(s).
8. Click the **Save** button.

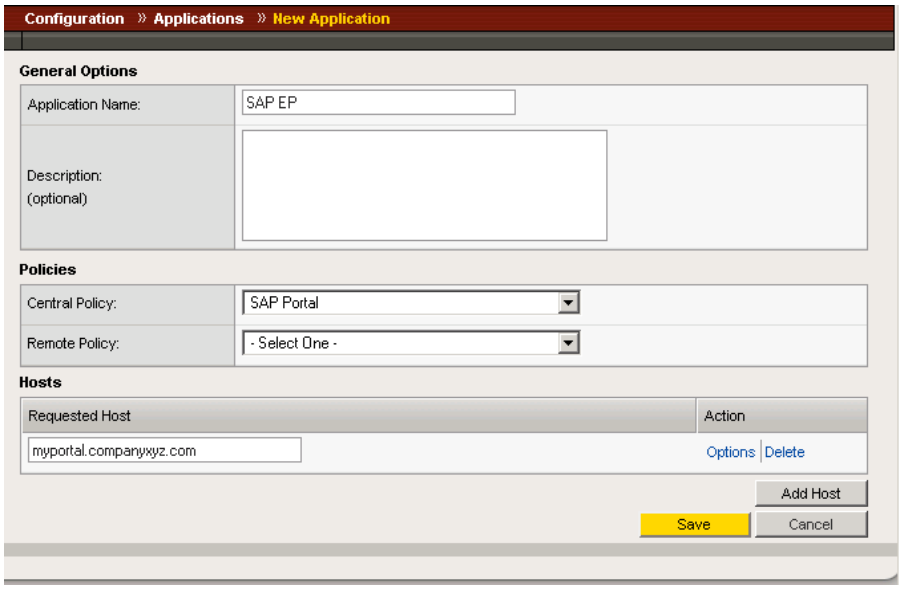

Figure 2.3 *Configuring an Application on the WebAccelerator (not a symmetrical deployment)*

The rest of the configuration options on the WebAccelerator are optional, configure these as applicable for your network. With this base configuration, your end users will notice an marked improvement in performance after their first visit.

3

Deploying the FirePass controller with SAP NetWeaver and Enterprise SOA

- Configuring the FirePass controller for deployment with SAP
- Creating the Resource groups
- Creating the Master groups
- Limiting access for the Partner group
- Configuring Endpoint security

Deploying the FirePass controller with SAP NetWeaver and Enterprise SOA

This section of the Deployment Guide shows you how to configure F5's FirePass controller for secure remote access to SAP deployments.

F5's FirePass® controller is the industry leading SSL VPN solution that enables organizations of any size to provide ubiquitous secure access for employees, partners and customers to SAP applications while significantly lowering support costs associated with legacy client-based VPN solutions.

The FirePass controller version 6 has achieved SAP certification for Network Security for Enterprise SOA-Based Solutions, based on SAP ERP 6.0 based on NetWeaver 7.0. Note that the Endpoint security features of this deployment guide were not a part of this certification.

For more information on the FirePass controller, see **http://www.f5.com/products/FirePass/**.

Prerequisites and configuration notes

The following are prerequisites for this deployment:

- The FirePass controller should be running version 6.0 or later.
- This deployment was tested using SAP ERP 6.0 based on NetWeaver 7.0, load balanced by a BIG-IP LTM system as described in this Deployment Guide.
- All of the configuration procedures in this document are performed on the FirePass device. For information on how to configure SAP devices, consult the appropriate SAP documentation.
- Our configuration scenario uses previously defined Active Directory groups to provide authentication and simple user maintenance. For information on how to configure Active Directory groups, consult the proper documentation.

  This Deployment Guide contains procedures for configuring the FirePass controller with Active Directory authentication only. There are many different authentication methods you can use with the FirePass controller; choose the one most applicable to your configuration.
- In our configuration, we use the FirePass controller to restrict remote access for a trusted partner group to a specific top level domain dedicated to serving partner related SAP content. This document assumes you have configured your SAP deployment in such a way that the all of the partner-accessible content is under one directory, and available via its own top level domain (i.e. http://sappartners.f5.com/).
- This Deployment Guide is written to the scenario outlined in the following section. It is meant as a template; modify the configuration as necessary for your deployment.

Configuration scenario

For the scenario used in this Deployment Guide, the SAP deployment, along with an Active Directory instance, resides behind a BIG-IP LTM system. There is a requirement to allow employees remote access to all internal resources using the FirePass device. There is also a requirement for trusted partners to access SAP applications, although only to a limited subset of the SAP deployment, with no other access.

This Deployment Guide describes how to configure the FirePass controller to allow secure remote access to the SAP deployment, using Active Directory for authentication and how to configure the FirePass to give one group of users full access, and restrict users in the partner group to a certain directory. In our deployment, the FirePass device and the SAP deployment use a common Active Directory Domain Controller. This guide also contains procedures on configuring some endpoint security features, including antivirus checks.

Configuring the FirePass controller for deployment with SAP

To configure the FirePass controller for allowing secure remote access to the SAP deployment, you need to complete the following procedures:

- *Connecting to the FirePass controller*
- *Creating the Resource groups*
- *Limiting access for the Partner group*
- *Configuring Endpoint security*

Connecting to the FirePass controller

To perform the procedures in this Deployment Guide you must have administrative access to the FirePass controller.

To access the Administrative console, in a browser, type the URL of the FirePass controller followed by **/admin/**, and log in with the administrator's user name and password.

Once you are logged on as an administrator, the Device Management screen of the Configuration utility opens. From here, you can configure and monitor the FirePass controller.

Creating the Resource groups

Resource groups allow you to preconfigure specific applications and access by group, and assign the group to a master group or an individual user. For this configuration, we create two resource groups, one for employees and one for partners, in order to create different Favorite links to the SAP deployment.

To configure resource groups

1. From the navigation pane, click **Users**, expand **Groups**, and then click **Resource Groups**.
2. Click the **Create new group** button.
   The Group Management - Create New Group screen opens.
3. In the **New group name** box, type a name for your group and click the **Create** button. In our example we type **SAP-Employee**. The new group appears on the Resource Groups table.
4. Repeat steps 2 and 3 for the Partner group. In our example, we name the group **SAP-partner**.

Configuring Application Access for the Partner group

In this section, we configure an Application Access Web Application Tunnel on the FirePass controller to allow the Partner group specific access to the SAP deployment. In this example, we assume you have already configured the SAP deployment and DNS with a URL that is specific to the applicable partner-specific portion of the SAP deployment.

To configure the Partner resource group

1. From the navigation pane, click **Users**, expand **Groups**, and then click **Resource Groups**.
2. From the Resource Groups table, find the row with the name of the *Partner* group you just created. In this row, from the **Application access** column, click **Edit** (see Figure 3.1). The Application Tunnel section of the Resource Group page opens.

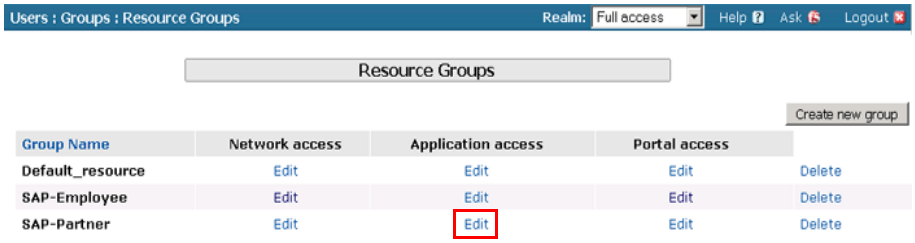

Figure 3.1 *The Resource groups table*

3. Click the Web Applications Tunnel tab.
4. Under Web Application Tunnels, click **Add New Favorite**. The Favorite options display.

5. Type a name for the Favorite. In our example, we type **SAP Partner Access**. This Favorite link only displays for members of the Partner group.
6. In the **URL** box, type the URL used to access the portion of the SAP deployment for Partners. For example **http://sappartners.f5.com.**
7. Click the **Add to allow list** link to the right of the URL box. This adds the URL to the list of URLs the users are allowed to access.
8. Click the **Locked Browser** box. This presents a browser to the user that prohibits typing URLs, and saving and printing web pages.
9. Configure the rest of the settings as applicable to your deployment.
10. Click the **Add New** button.

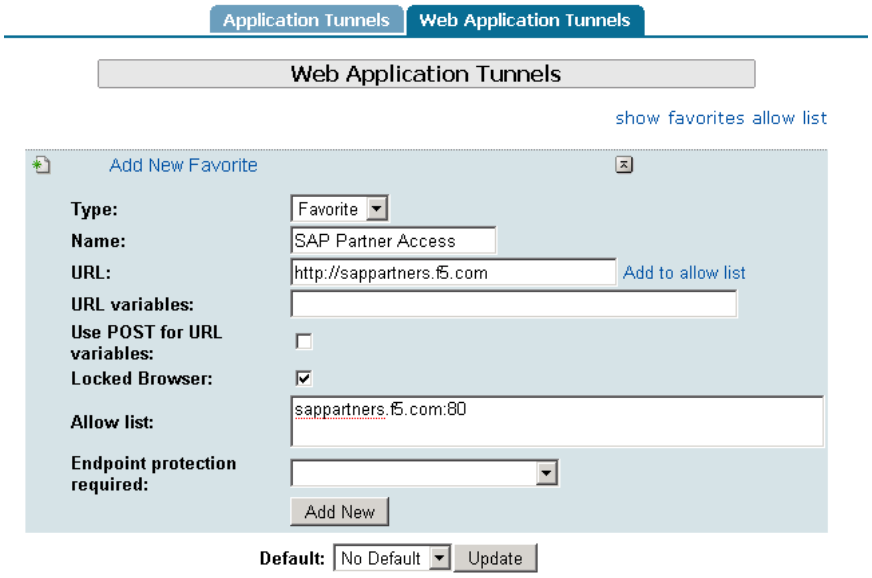

Figure 3.2 *Adding a Web Application Favorite for the Partner group*

Configuring Application Access for the Employee group

In our scenario, the next step is to configure Application Access to the SAP deployment for the employee group.

Tip

You could also configure Network Access for the employee group to allow employees full access to the entire internal network rather than just the SAP deployment. For more information on configuring Network Access, see Chapter 5, ***Configuring Network Access*** *in the* ***FirePass Controller Administrator Guide****.*

To configure Application Access for the Employee group

1. From the navigation pane, click **Users**, expand **Groups**, and then click **Resource Groups**.
2. From the Resource Groups table, find the row with the name of the *Employee* group you just created. In this row, from the **Application access** column, click **Edit** (see Figure 3.1). The Application Tunnel section of the Resource Group page opens.
3. Click the Web Applications Tunnel tab.
4. Under Web Application Tunnels, click **Add New Favorite**. The Favorite options display.
5. Type a name for the Favorite. In our example, we type **SAP Employee Access**. This Favorite link only displays for members of the Employee group.
6. In the **URL** box, type the URL used to access the portion of the SAP deployment for Partners. For example **http://sapportal.f5.com.**
7. Click the **Add to allow list** link to the right of the URL box. This adds the URL to the list of URLs the users are allowed to access.
8. Click the **Locked Browser** box. This presents a browser to the user that prohibits typing URLs, and saving and printing web pages.
9. Configure the rest of the settings as applicable to your deployment.
10. Click the **Add New** button.

Creating the Master groups

FirePass controller master groups are composed of users, authentication methods, and security and policy information. The next task is to create Master groups that will use the resource groups we just created.

To create a new Master Group

1. From the navigation pane, click **Users**, and expand **Groups**.
   The Master Groups list screen opens.
2. Click the **Create new group** button.
   The Group Management Create New Group screen opens.
3. In the **New group name** box, type the name of your group. In our example we type **SAP-Employee-AD**.
4. In the **Users in group** box, select **External.**
5. From the Authentication method list, select **Active Directory**.
6. In the **Copy settings from** list, make sure **Do not copy** is selected (see Figure 3.3).

7. Click the **Create** button.
   The General tab of the new Master Group displays.

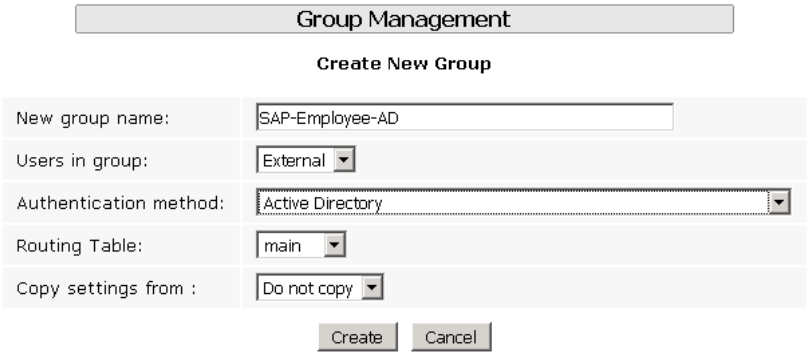

Figure 3.3 *Creating a new Master Group*

8. Click the Resource Groups tab.
   The Resource Groups screen opens.
9. From the **Available** box, select the name of the Resource group you created for employees in the *Creating the Resource groups* section. In our example, we select **SAP-employee**.
10. Click the **Add** button to move the group to the **Selected** box, and click the **Update** button. The Resource group is now associated with the Master group.

Repeat this procedure for the Partners group, using a unique name and selecting the SAP-Partners in step 9.

Configuring the Master group for Active Directory authentication

The next procedure is configuring the Master group to use Active Directory authentication.

Important

The FirePass controller has a number of different authentication methods to choose from; use the method applicable to your configuration. However, this guide only contains instructions on configuration Active Directory authentication. See the online help or FirePass documentation for more information on configuring other authentication methods.

To configure the FirePass Master group to use Active Directory authentication

1. From the navigation pane, click **Users**, expand **Groups**, and then click **Master Groups**.
2. Click the name of the Master group you created in the *Creating the Master groups* section (**SAP-Employee-AD** in our example).
3. Click the Authentication tab.
4. In the **Configure Active Directory Settings** section, configure the appropriate settings for your Active Directory deployment. Type the fully qualified domain name in the **Domain** name box, and IP addresses or DNS names for the Kerberos (Domain Controller) and WINS servers in their respective boxes.
5. Click the **Save Settings** button.

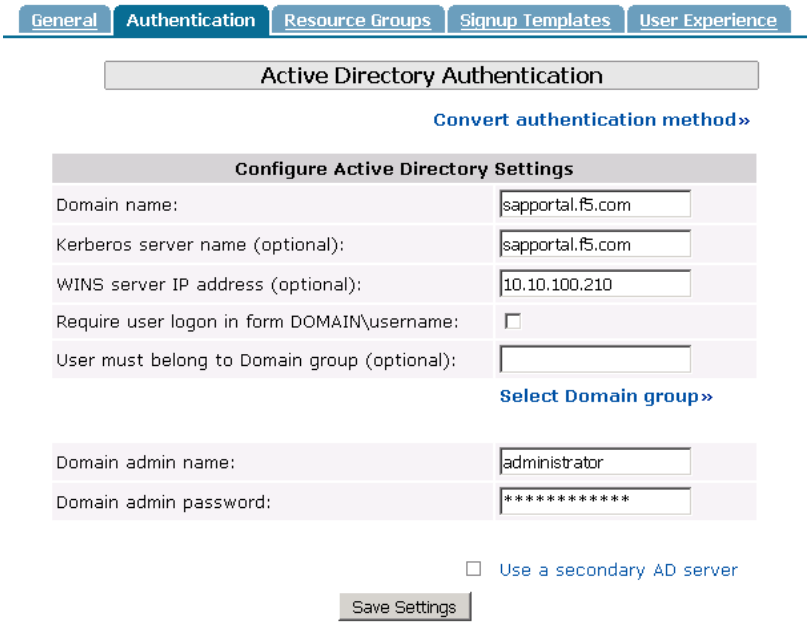

Figure 3.4 *Active Directory Authentication settings*

6. You can optionally click **Test Saved Settings** to test the Active Directory authentication.
7. Click the **Select Domain Group** link.
   The Active Directory Authentication screen opens.
   Important: *Be sure you have entered the* ***Domain admin name and password*** *and saved the settings before clicking Select Domain Group.*
8. From the list, select the Active Directory Domain group the user must belong to in order to authenticate, and click the **Select Group** button (see Figure 3.5).

9. Click the **Save Settings** button again. You can also click the **Test Saved Settings** button to test the configuration.

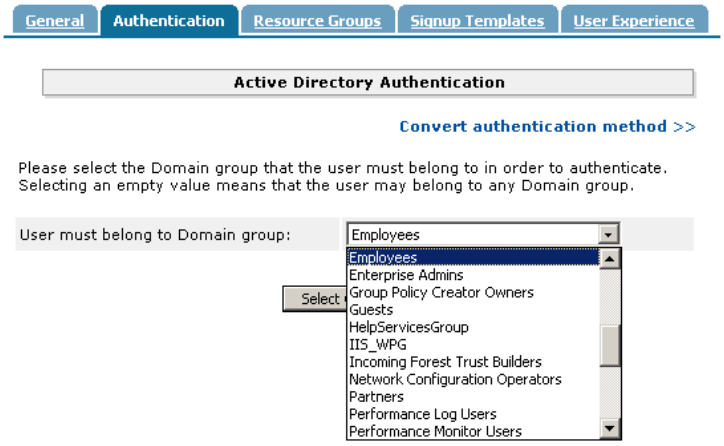

Figure 3.5 *Selecting the Active Directory Domain Group*

Repeat this procedure to configure the Master group for the Partners. In our example, we name the group **Sap-Partners-AD**. Be sure to select the appropriate Active Directory Domain group in step 8.

Limiting access for the Partner group

The FirePass controller allows you to limit access for specific groups on a very granular level. In this scenario, we limit access for the Partner group to only the Favorite we configured earlier, as well as restricting the areas of the SAP deployment they can access by URL.

To limit access for the Partner group

1. From the navigation pane, click **Application Access**.
2. Under Web Applications, click **Master Group Settings**.
3. From the **Master Group** list at the top of the page, select the Master Group you created in the *Creating the Master groups* section. In our example, we select **SAP-Partners-AD**.
   The configuration settings for the Master group open.
4. In the **Access limitation** section, make sure there is a check in the **Show administrator-defined favorites only** box.
5. In the Access Control List section, in the **Allow List** box, type a host name or URL. In our example, we type **sapparnters.f5.com:80,443**.

   For more information on configuring the Access Control section, see the online help.

6. Click the **Update** button. The new settings take effect after any users currently logged onto the FirePass controller log out.

Configuring Endpoint security

One of the strong security features of the FirePass controller is the ability to set endpoint security on a extremely granular level.

In the following procedures, we configure a pre-logon check for anti-virus software on Windows machines. The FirePass controller uses this information to deny SAP access for members of the Partner Resource group if they do not have the appropriate software. In this configuration example, the FirePass device also denies access to *any* client that is determined to have a virus.

For more information on endpoint security, see the online help.

Creating a pre-logon sequence

The pre-logon sequence allows administrators to create one or more sequences of inspections for items such as installed antivirus programs or OS patch levels.

To configure a pre-logon sequence

1. From the navigation pane, click **Users**, expand **Endpoint Security**, and click **Pre-Logon Sequence**.
2. In the New Sequence section at the bottom of the page, type a name for the sequence in the **Create New Sequence** box. In our example, we type **SapBasic**.
3. From the **Based on** list, select **template: Collect information with no pre-logon actions**.
4. Click the **Create** button.
   The new sequence appears in the Select Sequence to Use table.
5. In the row of the sequence you just created, click the **Edit** button.
   Warning *- Do not click the radio button next to the sequence yet. If you click the radio button, the* ***Edit*** *link will be replaced with the* ***View*** *link, and you are not able to edit the sequence.*

   The Pre-Logon Sequence Editor opens.
6. Move the curser between **Sequence Start** and the box. A small add **[+]** link appears on the arrow (see the circle marked **1** in Figure 3.6). Click **Add**.
   The Change Sequence panel appears on the right.
7. Click the **Check for Antiviruses** option button, and click the **Apply Changes** button.
   The Edit Action panel opens.

Note: *The Check for Antiviruses is an optional feature on the FirePass controller. If your device does not have this license, you will not see this option.*

8. Under **Inspectors**, click **Windows Antivirus Checker**.
The Endpoint Inspector Details page opens in a new window.
9. Configure these options as applicable for your deployment. For more information, click **Help**.
10. Click the **Update** button.
11. In the Sequence pane, find **AV installed**, and click the associated Logon Denied Page link (see the circle marked **2** in Figure 3.6).
The End Page Properties pane appears on the right.
12. From the Type box, select **Logon Allowed Page**. This allows a user to logon if they have an antivirus checker installed. You can optionally type a message for failed logons.
13. Repeat steps 11 and 12 for the **Fallback** option.
14. ***Optional:*** You can click the Logon Allowed Page or Logon Denied Page links for the other options to produce a custom message when a user is denied access. You can also change the actions taken as a result of the virus checker's findings. For example, you might still want to allow a user to login if there is virus checking software installed, but not currently running.

    In our example, we click **Logon Denied Page** next to **Virus Detected**, and type a message informing the user there is a virus on their computer.
15. When you are finished, click **Back to Console** in the upper right corner of the screen (see the circle marked 3 in the following figure). You return to the Pre-Logon Sequence main page.

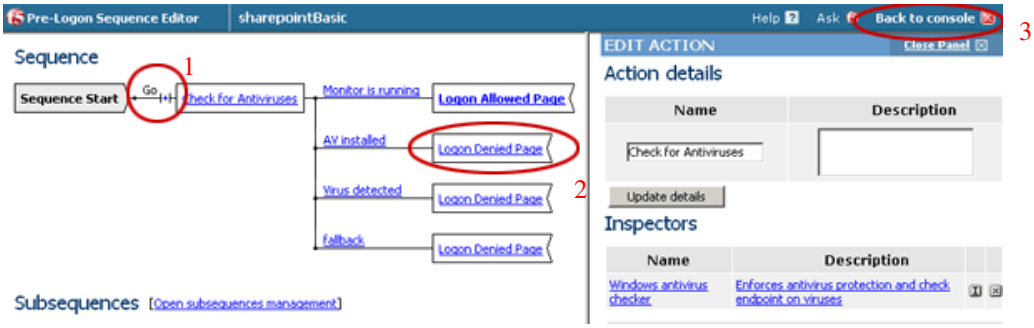

Figure 3.6 *The Pre-Logon Sequence Editor*

16. From the **Select Sequence to Use** section, click the option button next to the sequence you just created. In our example, we click **SapBasic**.
17. Click the **Apply** button.

Protected Configurations

Protected Configurations allow administrators to specify the criteria the endpoint systems must meet to enable access to the various resources. In this procedure, we create a protected configuration for the partner group in order make additional security requirements for that group.

To configure Protected Configurations

1. From the navigation pane, click **Users**, expand **Endpoint Security**, and click **Protected Configurations**.
2. Click **New Protection Configuration**.
3. In the Protected configuration ID box, type a name for this configuration. In our example, we type **Partner_config**. You can optionally type a description.
4. Leave the Mode list at the default setting, **Check endpoint protection, grant access if check passed** (see Figure 3.7).

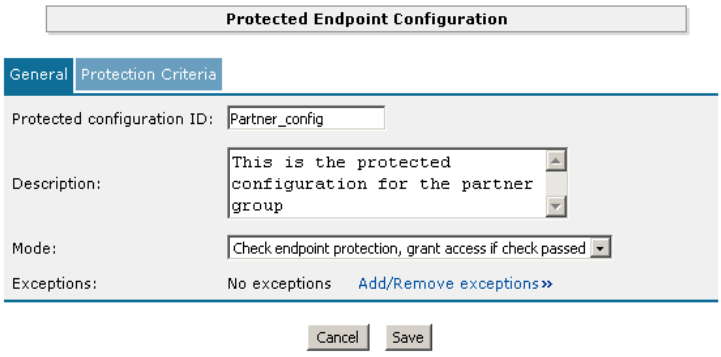

Figure 3.7 *The General tab of the Protected Endpoint Configuration screen*

5. Click the Protected Criteria tab.
6. On the menu bar, click **Information Leaks**.

7. From the Required safety measures or checks list, select **Cache Cleaner** and click the **Add** button. This will remove content from the cache when a user logs off.

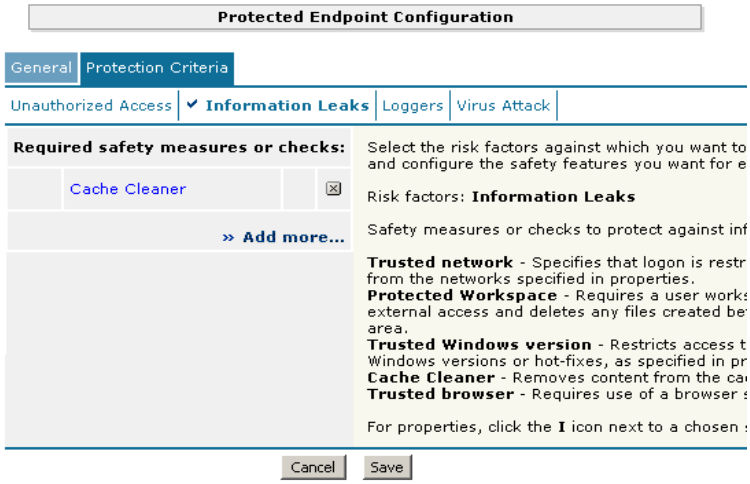

Figure 3.8 *The Protection Criteria tab of the Protected Endpoint Configuration screen*

Important: *The Cache Cleaner feature is currently Windows only. It does not work with Apple Macintosh or Linux systems.*

8. On the menu bar, click **Virus Attack**
9. From the list, select **Antivirus** and click the **Add** button.
10. Click the **I** icon next to Antivirus to configure the antivirus properties (see Figure 3.9). The Select trusted anti-viruses screen opens. Configure these properties as applicable for your configuration, and click the **Save** button.

    You return to the Protection Criteria tab of the Protected Endpoint Configuration page.
11. Click the **Save** button.

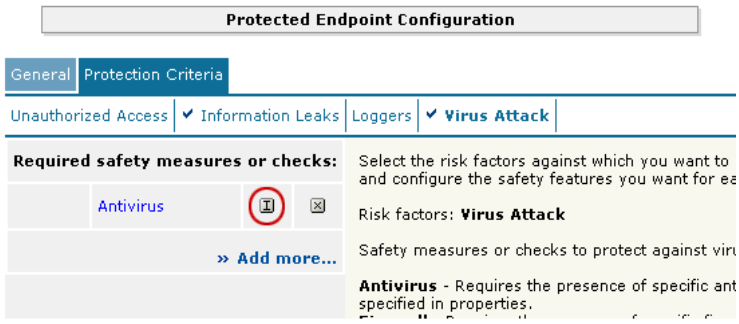

Figure 3.9 *The Edit button for Antivirus properties*

Protecting the Resources

The next step is to associate the protected configuration you just created with a resource.

To protect the resources

1. From the navigation pane, click **Users**, expand **Endpoint Security**, and click **Protect Resources**.
2. From the Resource Table, expand **Web Applications**.
3. Find the **Partners** resource group (in our example, **SAP-Partner**), and click the **Select** link next to the Favorite you configured.
4. From the **Configuration to protect selected resources** list, select the name of the configuration you created in the preceding procedure. In our example, we select **Partner_config**.
5. Click the box next to the Favorite name, and click the **Select** button. A shield image appears in the row.

Resource group		Required protection	
Default_resource			Select
SAP-Employee			Select
SAP-Partner		Partner_config	Select

Figure 3.10 *Adding the Protected Configuration to the Resource*

Configuring post-logon actions

The final step is to configure a post-logon action in which the FirePass device injects an Active X control or plug-in to clean the client browser's web cache.

To configure the post-logon action

1. From the navigation pane, click **Users**, expand **Endpoint Security**, and click **Post-Logon Actions**.
2. Click a check in the **Inject ActiveX/Plugin to clean-up client browser web cache** box. A list of options displays.
3. Configure these options as applicable for your deployment. In our example, we leave these options at their default settings.

Conclusion

The FirePass controller is now configured to allow secure remote access to the SAP deployment. Remember that the procedures in this Deployment Guide are specific to the scenario described in *Configuration scenario*, on page 3-2. Use this guide as a template, and modify the configuration as applicable to your deployment.