Sterling Secure Proxy

Other Configuration Options

Version 34

Sterling Secure Proxy

Other Configuration Options

Version 34

Note
Before using this information and the product it supports, read the information in "Notices" on page 33.

This edition applies to version 3.4 of IBM Sterling Secure Proxy and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Configure Perimeter Servers

Configure Perimeter Servers to Manage Sterling Secure Proxy Communications

A perimeter server is used by Sterling Secure Proxy to manage inbound and outbound TCP communication. This software tool enables you to manage the communications flow between outer layers of your network and the TCP-based transport adapters. Perimeter servers can be used to restrict areas where TCP connections are initiated from more secure areas to less secure areas.

During the Sterling Secure Proxy installation, a perimeter server is installed. This perimeter server is referred to as the local perimeter server. You can use this default local perimeter server to restrict connections or you can install other perimeter server instances as needed. You can install additional perimeter servers on different computers or you can install different instances on the same computer, if you want to use different network cards for inbound and outbound traffic. A perimeter server requires a perimeter server definition in Sterling Secure Proxy.

After you install and configure a remote perimeter server, you need to map how the perimeter server is used:

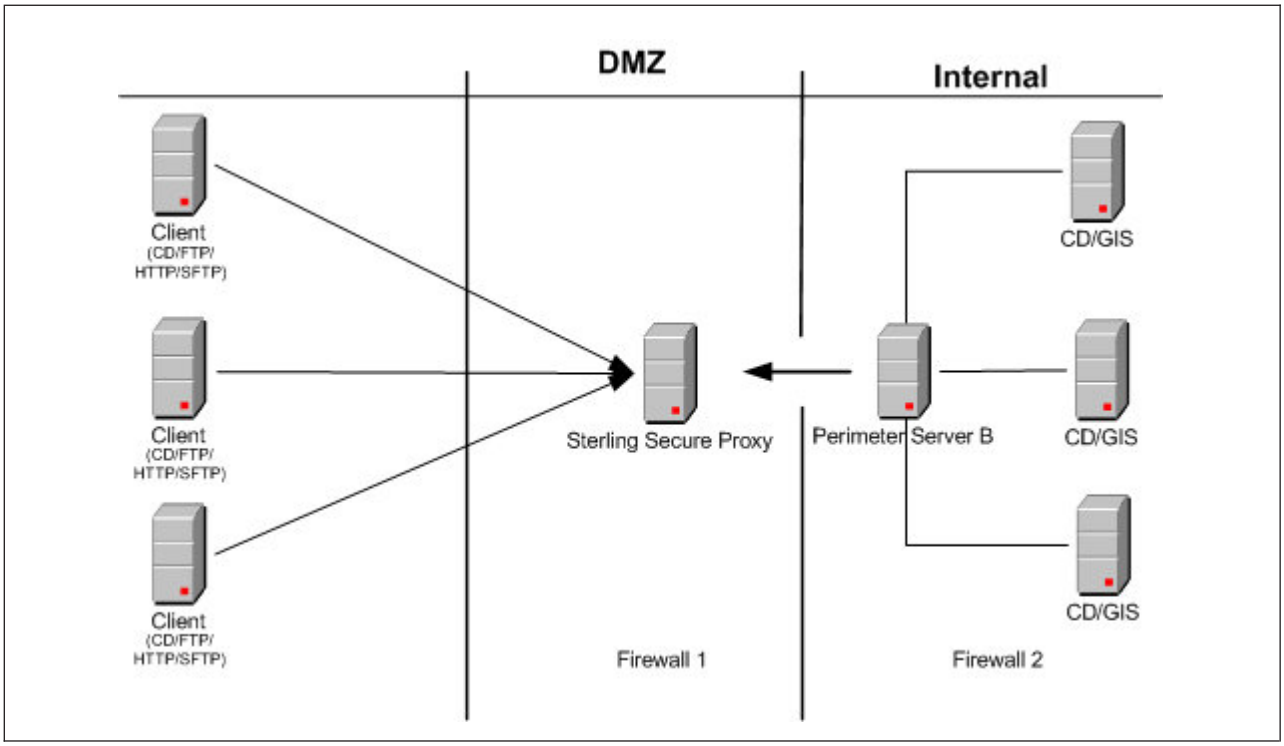
- inbound
- outbound
- External Authentication

Refer to *Map Perimeter Servers.*

Before you configure remote perimeter servers in Sterling Secure Proxy, complete the installation procedures outlined in *Install a Remote Perimeter Server Overview*.

Typical Installation

The following figure illustrates a typical Sterling Secure Proxy installation with perimeter servers:



The preceding figure shows the following:

- The persistent connection is established from the perimeter server in the internal trusted network to Sterling Secure Proxy in the DMZ. This allows for only an outbound hole to be configured in the Firewall 2 (no inbound hole is needed with this configuration)
- Sterling Secure Proxy has an HTTP server adapter configured for two scenarios, one secure HTTP (HTTPS) and the other non-secure HTTP.
- Two trading partners with separate host and port numbers are configured to communicate with Sterling Secure Proxy.

A perimeter server and all adapters that communicate with the local perimeter server must be configured on the same Sterling Secure Proxy engine. An engine can have more then one perimeter server but a perimeter server can be used by only one engine.You can configure a perimeter server for one trading partner with large files and low transaction volume, and another perimeter server on the same engine for a different trading partner with smaller files and high transaction volume. By configuring each perimeter server according to the trading partner, you increase Sterling Secure Proxy performance.

Sample Remote Perimeter Server Configurations

Use remote perimeter servers with Sterling Secure Proxy if you want to:

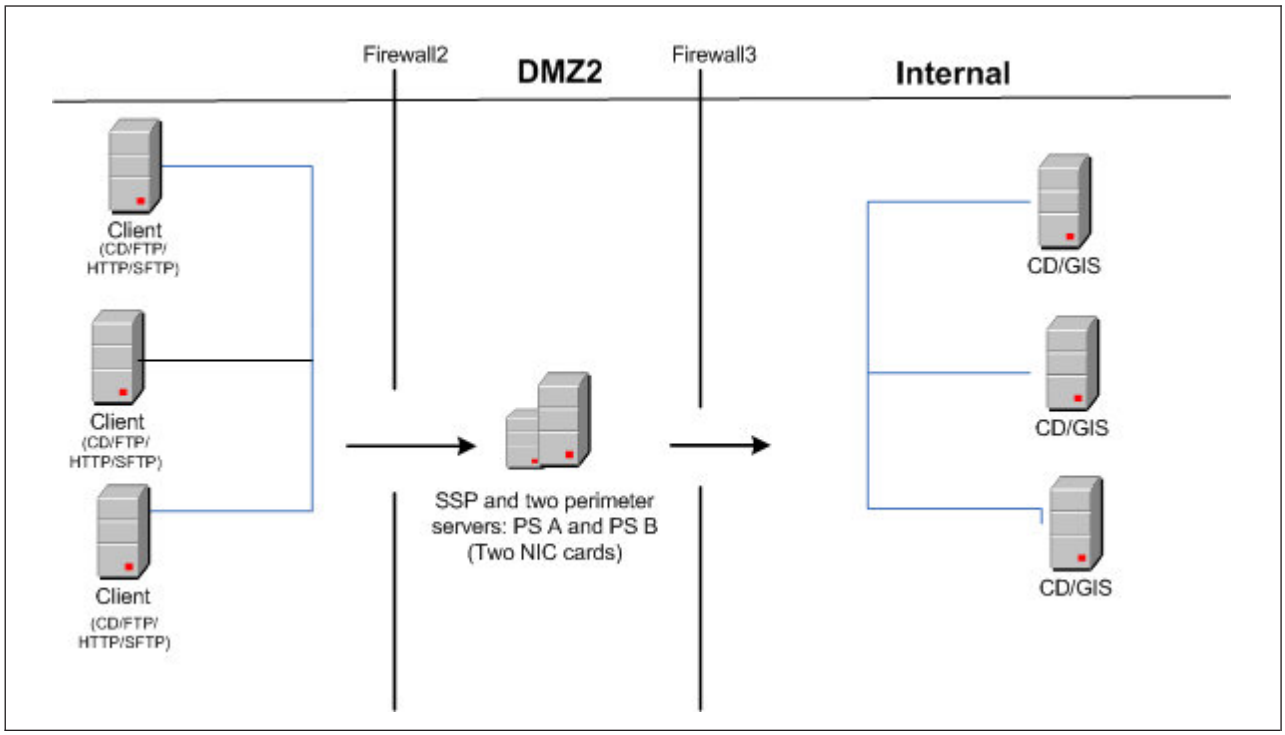
- Eliminate an inbound hole in your firewall to allow connections from less secure to more secure areas.
- Send data to your customers from the perimeter server as the originating IP address.
- Use different network cards for inbound and outbound traffic.
- Implement multiple DMZ scenarios. You can use perimeter servers in your outer DMZ with Sterling Secure Proxy in the internal DMZ.

You have flexible deployment options for using perimeter servers with Sterling Secure Proxy: from a simple IP break to no inbound holes in the firewall. Following are sample deployment options:

- Deployment Option Example—Two Remote Perimeter Servers on a Computer with Two NIC Cards
- Deployment Option Example—From More Secure to Less Secure
- Deployment Option Example—From Less Secure to More Secure
- Deployment Option Example —External Authentication Perimeter Server

Deployment Option Example - Two Remote Perimeter Servers on a Computer with Two NIC Cards

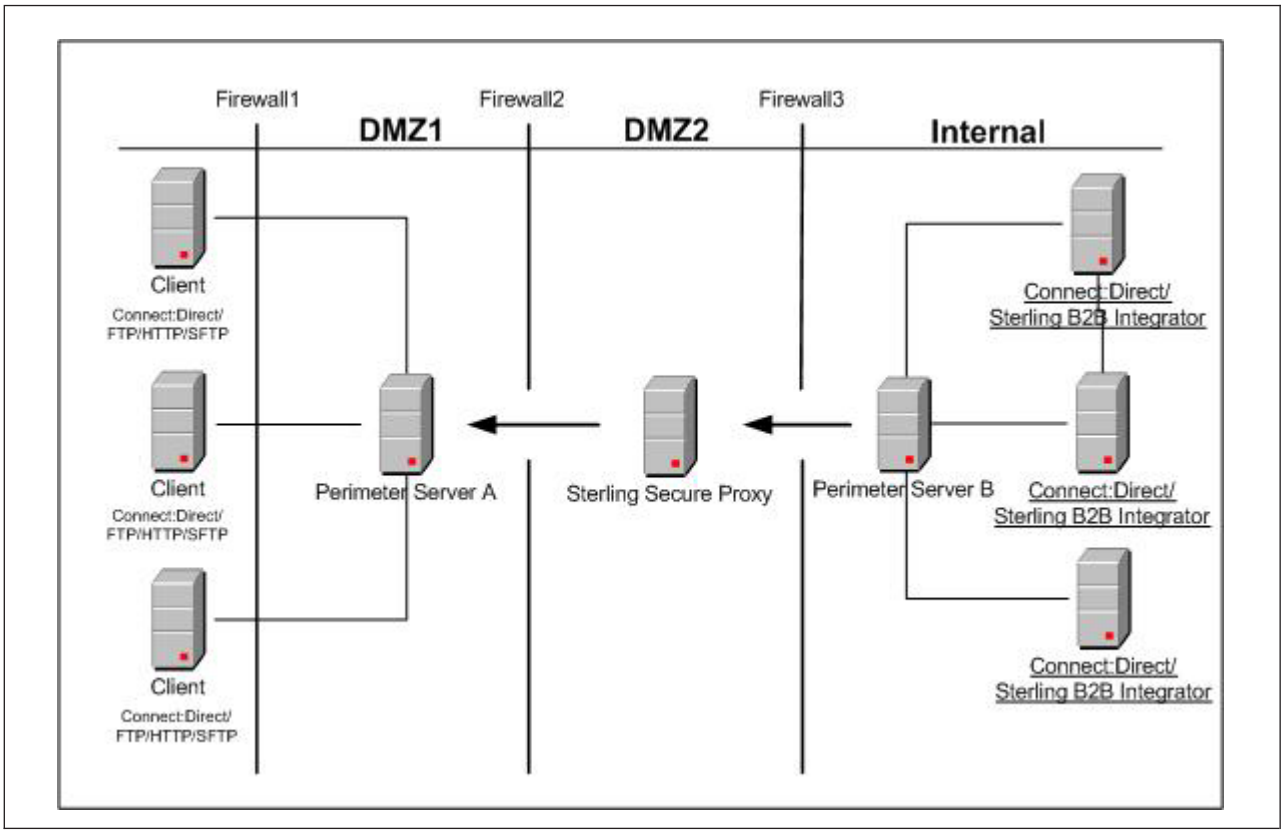
The following sample illustrates a configuration where two remote perimeter servers are installed. One remote perimeter server manages inbound traffic and the other manages outbound traffic.



In this configuration, the firewall is configured to allow connections from trading partners to the remote perimeter server A (PS A). PS A then routes traffic to Sterling Secure Proxy. Outbound traffic is routed from Sterling Secure Proxy through perimeter server B (PS B) to the Sterling B2B Integrator or Sterling Connect:Direct® server.

Deployment Option Example - From More Secure to Less Secure

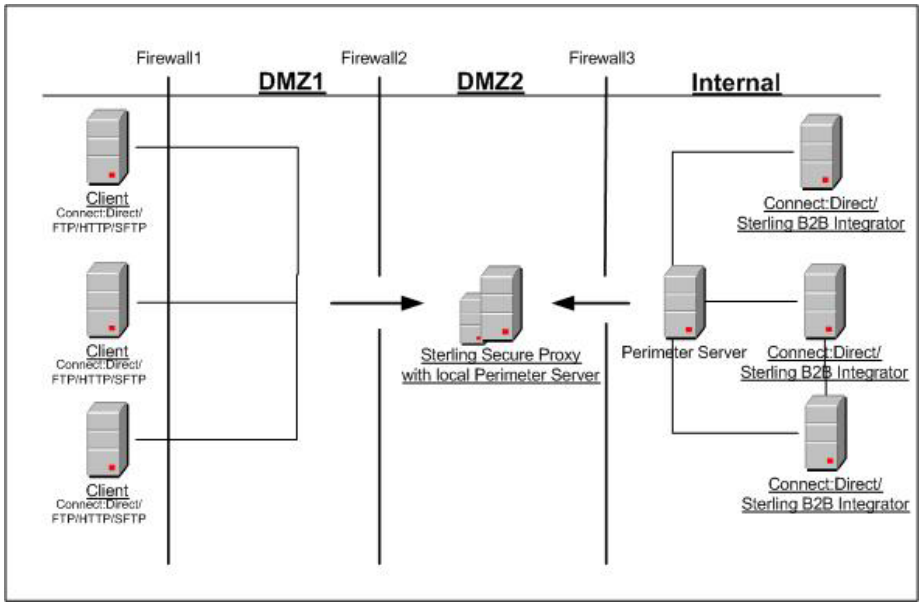
For additional firewall security, you can install a perimeter server in a more secure area than Sterling Secure Proxy and set up your firewall to allow only connections initiated from a more secure area to a less secure area. The following diagram demonstrates a configuration with two perimeter servers:



In this example, Sterling Secure Proxy is configured to use two perimeter servers that reside on remote computers: one on an external network (Perimeter Server A), and one in the internal network (Perimeter Server B). The firewalls are configured to allow only connections initiated from inside a more secure area (only an outbound hole in the firewall). When Sterling Secure Proxy is started, a connection is established from Perimeter Server B to Sterling Secure Proxy and from Sterling Secure Proxy to Perimeter Server A. Through these communication lines, SSL/TLS sessions can be established between clients and Sterling Secure Proxy, and between Sterling Secure Proxy and Sterling Connect:Direct or Sterling B2B Integrator.

Deployment Option Example - From Less Secure to More Secure

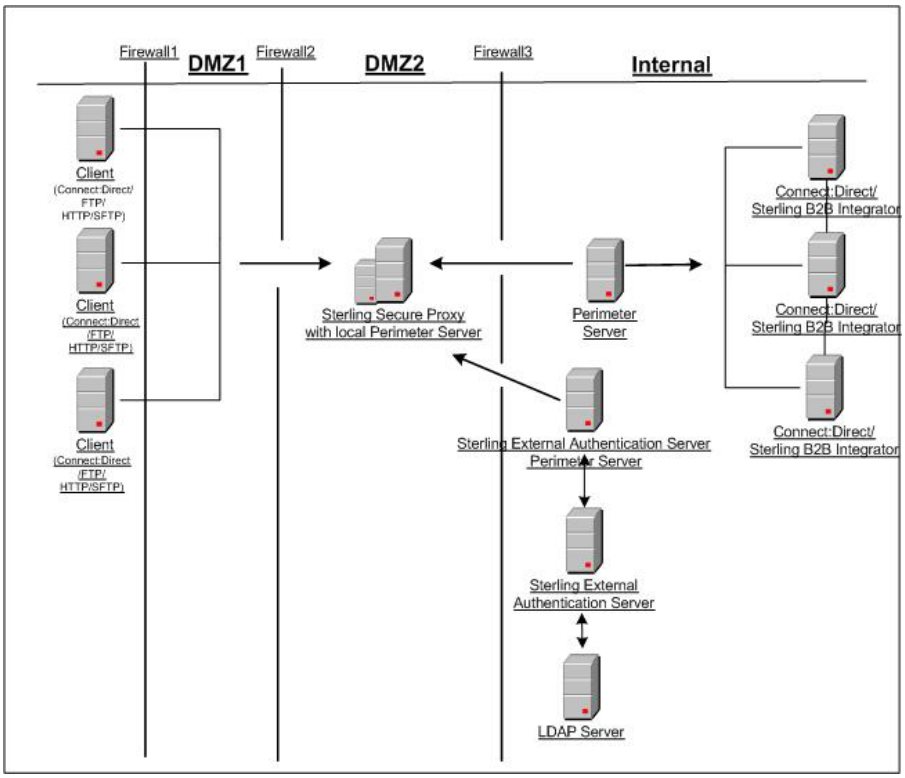
The following sample illustrates a configuration where the remote perimeter server is installed in a more secure location than Sterling Secure Proxy:



In this configuration, the firewall is configured to allow connections from external trading partners to Sterling Secure Proxy and from the internal perimeter server to Sterling Secure Proxy. In this configuration, traffic is moving from a less secure to a more secure location. To restrict unauthorized access, you can limit the perimeter server to perform only those activities required for Sterling Secure Proxy operations. Refer to *Install a Remote Perimeter Server Overview* for more information.

Deployment Option Example - External Authentication Perimeter Server

The following sample illustrates a configuration where the remote perimeter server in the trusted zone is used to connect to Sterling External Authentication Server:



In this example, Sterling Secure Proxy is configured to use two remote perimeter servers and the local perimeter server. When Sterling Secure Proxy is started, a connection is established from Sterling Secure Proxy to the remote perimeter server. Through this communication line, SSL/TLS sessions can be established between clients and Sterling Secure Proxy. Another remote perimeter server is used to communicate between Sterling External Authentication Server and Sterling Secure Proxy.

Define a Remote Perimeter Server for a Less Secure Environment

A common network configuration pattern is for Sterling Secure Proxy to reside in the innermost, secure network zone and the perimeter server to reside in the DMZ. In this case the connection should be established from Sterling Secure Proxy to the perimeter server-that is, from the more secure towards the less secure network zone.

This section contains the following procedures:

- *Configure a Remote Perimeter Server in a Less Secure Zone*
- *Edit a Remote Perimeter Server in a Less Secure Zone Definition*
- *Modify the Water Mark Values and Local Host Information of a Remote Perimeter Server in a Less Secure Zone*

Configure a Remote Perimeter Server in a Less Secure Zone

About this task

To configure a perimeter server in a less secure zone:

Procedure

1. Select **Advanced** from the menu bar.
2. Select **Actions** > **New Perimeter Server** > **Less Secure Zone**.
3. Specify the following values:
   - **Perimeter Server Name**
   - **Perimeter Server Host**
   - **Perimeter Server Port**
4. Click **Save**.

Edit a Remote Perimeter Server in a Less Secure Zone Definition

About this task

To edit the definition of a perimeter server in a less secure zone:

Procedure

1. Select **Advanced** from the menu bar.
2. Expand the **Perimeter Servers** tree and expand the **Less Secure Zone** tree.
3. Click the perimeter server definition you want to edit.
4. Edit the values as needed.
5. Click **Save**.

Modify the Water Mark Values and Local Host Information of a Remote Perimeter Server in a Less Secure Zone

About this task

To modify the water mark values and local host information of a perimeter server in a less secure zone:

Procedure

1. Select **Advanced** from the menu bar.
2. Expand the **Perimeter Server** tree and expand the **Less Secure Zone** tree.
3. Select the perimeter server to edit.
4. Click the **Advanced** Tab.
5. Change the following values as needed:
   - **Perimeter Server Outbound Low Water Mark**
   - **Perimeter Server Outbound High Water Mark**
   - **Perimeter Server Inbound Low Water Mark**
   - **Perimeter Server Inbound High Water Mark**
   - **Proxy Local Interface**
   - **Proxy Local Port**
6. From the **Perform DNS Resolution** list, select the place where DNS resolution occurs.
7. Click **Save**.

Configure a Remote Perimeter Server in a More Secure Zone

About this task

In some cases, it is desirable for Sterling Secure Proxy to communicate with a perimeter server installed in a more secure network zone. In this case establish the network connection from the perimeter server to Sterling Secure Proxy.

To configure a perimeter server in a more secure zone:

Procedure

1. Select **Advanced** from the menu bar.
2. Select **Actions** > **New Perimeter Server** > **More Secure Zone**.
3. Specify the following values:
   - **Perimeter Server Name**
   - **Proxy Local Listen Port**
4. Click **Save**.

Configure a Remote Perimeter Server in a More Secure Zone

About this task

In some cases, it is desirable for Sterling Secure Proxy to communicate with a perimeter server installed in a more secure network zone. In this case establish the network connection from the perimeter server to Sterling Secure Proxy.

To configure a perimeter server in a more secure zone:

Procedure

1. Select **Advanced** from the menu bar.
2. Select **Actions** > **New Perimeter Server** > **More Secure Zone**.
3. Specify the following values:
   - **Perimeter Server Name**
   - **Proxy Local Listen Port**
4. Click **Save**.

Edit A More Secure Zone Remote Perimeter Server Definition

About this task

To edit a more secure zone perimeter server definition:

Procedure

1. Select **Advanced** from the menu bar.
2. Expand the **Perimeter Servers** tree and expand the **More Secure Zone** tree.
3. Click the perimeter server definition to edit.
4. Edit the values as needed.
5. Click **Save**.

Modify Water Mark Values and Local Host Information of a Remote Perimeter Server Installed in a More Secure Zone

About this task

To modify water mark values and local host information of a perimeter server in a more secure zone:

Procedure

1. Select **Advanced** from the menu bar.
2. Expand the **Perimeter Server** tree and expand the **More Secure Zone** tree.
3. Select the perimeter server to edit.
4. Click the **Advanced** Tab.
5. Change the following values as needed:
   - **Perimeter Server Outbound Low Water Mark**
   - **Perimeter Server Outbound High Water Mark**
   - **Perimeter Server Inbound Low Water Mark**
   - **Perimeter Server Inbound High Water Mark**
   - **Proxy Local Interface**
6. From the **Perform DNS Resolution** list, select the place where DNS resolution occurs.
7. Click **Save**.

Map Perimeter Servers

About this task

After you configure perimeter servers, map how they are used by each adapter: inbound perimeter server, outbound perimeter server, or External Authentication perimeter server.

To map perimeter servers:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Adapters** tree and select the adapter you want to edit.
3. Click the **Advanced** tab.
4. Select a perimeter server for each of the following as needed. The default is local.
   - **Inbound Perimeter Server**
   - **Outbound Perimeter Server**
   - **External Authentication Perimeter Server**

   Note: The session limit for inbound perimeter server connections is 4096.
5. Click **Save**.
6. Repeat this process for each adapter that uses a remote perimeter server.

   Note: If you change the perimeter server mapped to an adapter, you must restart the adapter and the perimeter server before the change is enabled.

Modify Perimeter Server Properties

Two property values are defined in the perimeter.properties file located in the *install_dir*/bin folder. These properties determine SSL Session caching. Modify the following properties as necessary:

Parameter	Description
SslSessionDatabaseTimeoutSeconds	How long a cached SSL session is valid. The valid range is 30 seconds to 24 hours (60*60*24 = 86400 seconds). Default=1 hour or 3600 seconds.
SslSessionDatabaseSize	Maximum number of sessions to cache. This parameter is used by FTP and HTTP reverse proxy adapters. SSL sessions are not cached for Sterling Connect:Direct proxy adapters. Valid range is 1024 to 16384. Default=4096.

Chapter 2. Sterling External Authentication Server Configuration

Configure Sterling Secure Proxy for Sterling External Authentication Server

To provide a more advanced method of securing an inbound or outbound connection to Sterling Secure Proxy, use Sterling External Authentication Server. Sterling External Authentication Server allows you to authenticate certificate information or user credentials presented by the inbound node or to perform user ID and password mapping for the credentials used to attach to the outbound node.

Sterling External Authentication Server Configuration - Worksheet

Before you begin configuring Sterling Secure Proxy for authentication options using Sterling External Authentication Server, gather the information on this worksheet from the Sterling External Authentication Server administrator. Collect this information for each Sterling External Authentication Server you will configure.

Configuration Manager Field	Value
EA Server Name	
EA Server Address	
EA Server Port	
Outbound Port Range	
Security Setting	(SSL or TLS)
Trust Store	
CA/Trusted Certificates	
Key Store	
Key/System Certificate	
Cipher Suites	

Configure a Sterling External Authentication Server Connection

About this task

You can use Sterling External Authentication Server to increase the security of your Sterling Secure Proxy environment. Sterling External Authentication Server can be used to validate certificates from an inbound node, authenticate inbound users, and provide more secure credentials to the outbound node.

Before you can configure Sterling Secure Proxy to use Sterling External Authentication Server, you must configure an Sterling External Authentication Server definition.

To configure an Sterling External Authentication Server definition:

Procedure

1. Click **Advanced** from the menu bar.
2. Select **Actions** > **New External Authentication Server**.
3. Specify values for the following fields:
   - **EA Server Name**
   - **EA Server Address**
   - **EA Server Port**
   - **Outbound Port Range**
4. To enable SSL or TLS for the Sterling External Authentication Server connection, click the **Security** tab and enable **Use Secure Connection**.
5. Set the following values:
   - **Security Setting**
   - **Trust Store**
   - **CA/Trusted Certificates**
   - **Key Store**
   - **Key/System Certificate**
   - **Cipher Suites**
6. Click **Save**.

Specify Alternate Sterling External Authentication Servers for Failover Support

About this task

You can specify alternate Sterling External Authentication Servers that Sterling Secure Proxy connects to if a connection to the primary Sterling External Authentication Server cannot be made. Up to three alternate Sterling External Authentication Servers can be defined for each Sterling External Authentication Server.

You must first configure an Sterling External Authentication Server connection for each Sterling External Authentication Server you want to identify for failover support. Then you can identify alternate Sterling External Authentication Servers to use if a Sterling External Authentication Server is not available by selecting an Sterling External Authentication Server definition from the list.

To specify an alternate Sterling External Authentication Server for failover support:

Procedure

1. Click **Advanced** from the menu bar.
2. Expand the **External Authentication Servers** tree and select the Sterling External Authentication Server you want to edit.
3. Click the **Advanced** tab.
4. Select an alternate server from the **Alternate External Authentication Server #1** list.
5. Select additional servers as needed from the remaining lists. Connection attempts will be made to the alternate servers in the order in which they are specified.
6. Click **Save**.

Use a Perimeter Server to Connect to Sterling External Authentication Server

You can configure Sterling External Authentication Server to use a remote perimeter server in the trusted zone to manage connections to and from Sterling External Authentication Server, This configuration enables you to have one outbound opening in your more trusted firewall. For more information on configuring and mapping perimeter servers, refer to *Configure Perimeter Servers to Manage Sterling Secure Proxy Communications*.

Chapter 3. Failover Support

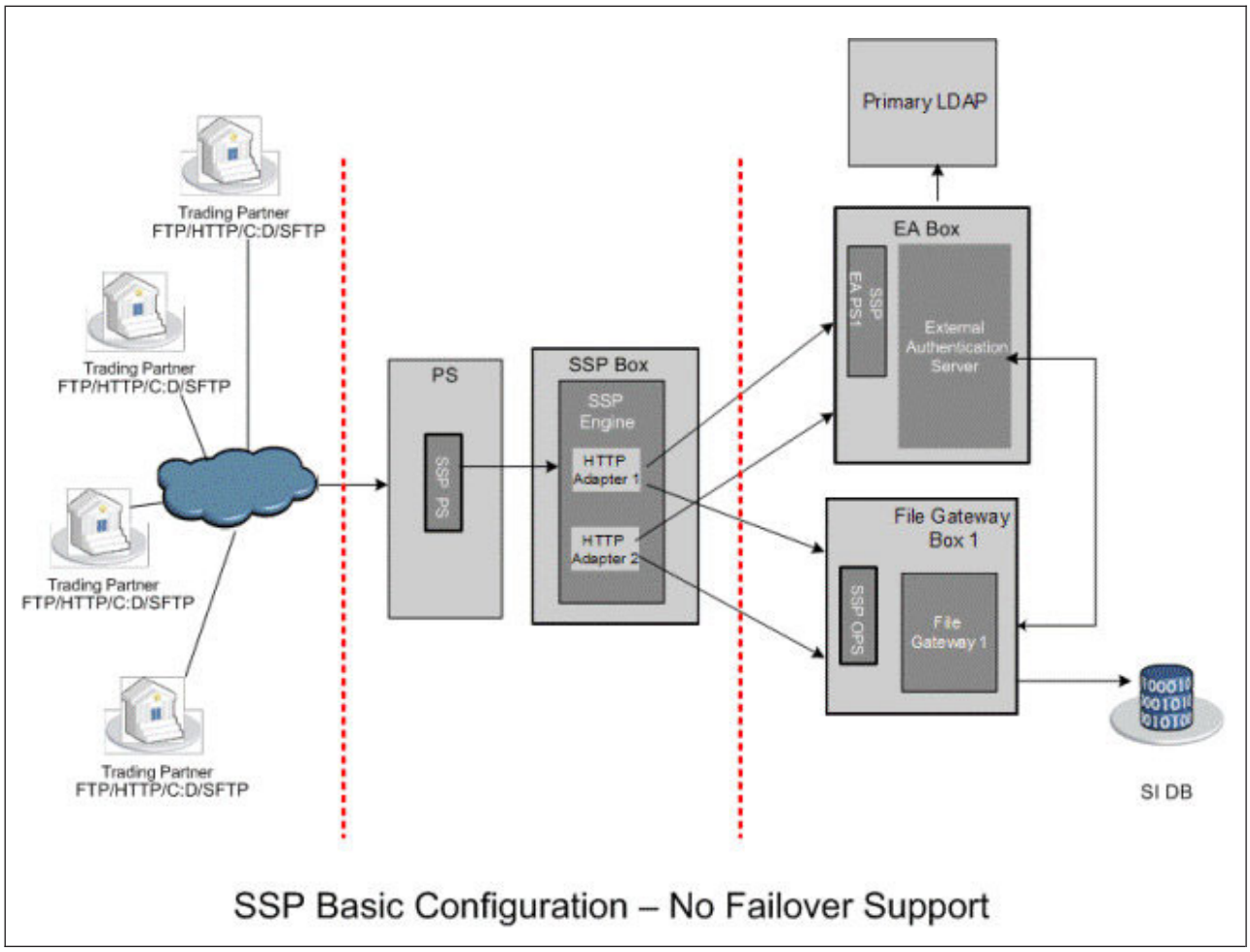
Overview of Failover Support

You can configure failover support in Sterling Secure Proxy to manage connections from a trading partner to a company server and ensure that your operation functions even when a component such as a perimeter server, Sterling Secure Proxy engine, Sterling External Authentication Server, or Sterling B2B Integrator server in the configuration is not operational.

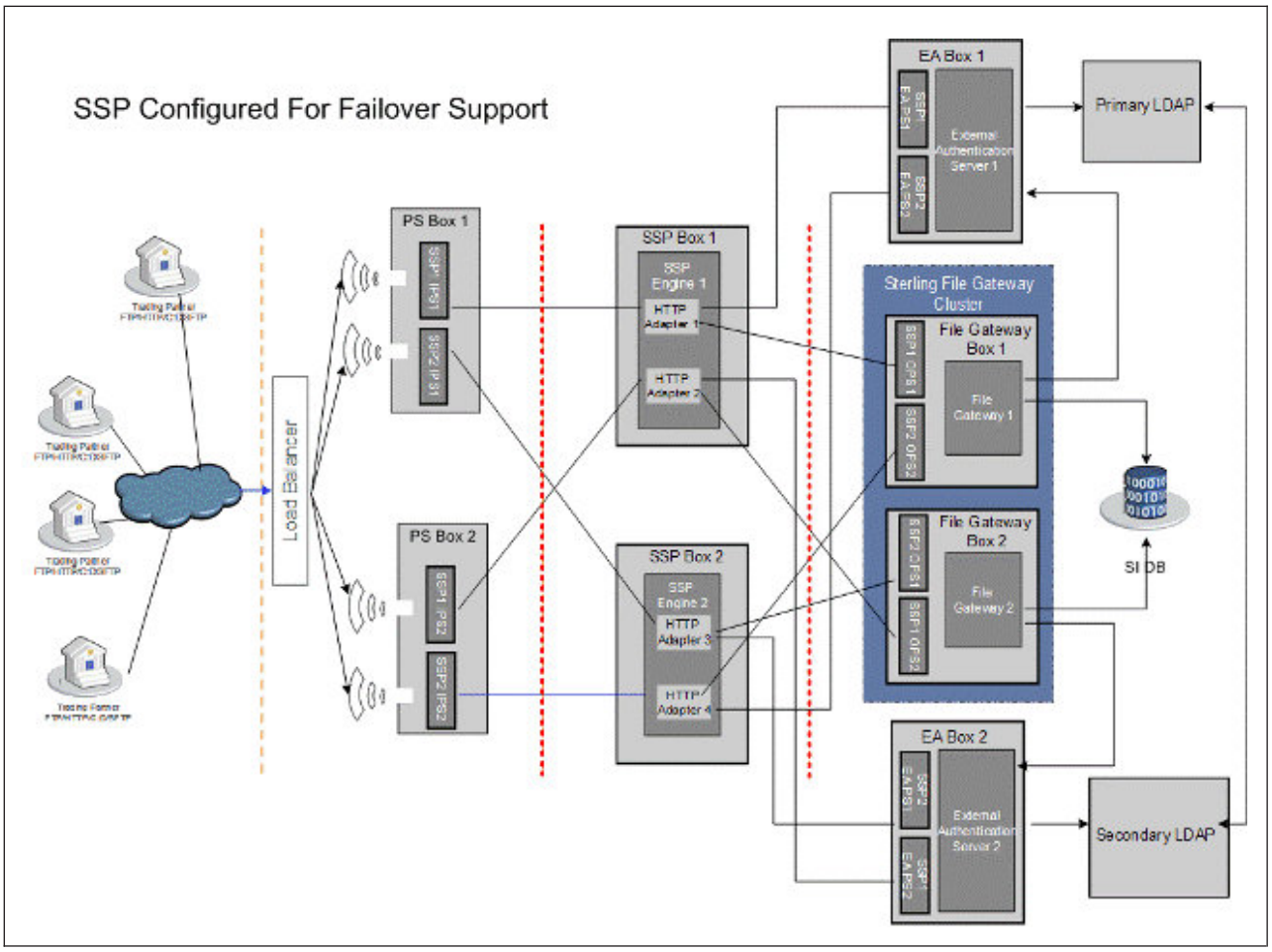
This document provides overview information about a failover environment and instructions on how to configure failover. It assumes that you have configured a basic Sterling Secure Proxy engine and defined adapters.

Illustration of Failover Support in Sterling Secure Proxy

Following is an illustration of a basic Sterling Secure Proxy configuration. This illustration does not include any components to support failover.



The following illustration builds on the basic Sterling Secure Proxy configuration and illustrates one way to configure failover support:

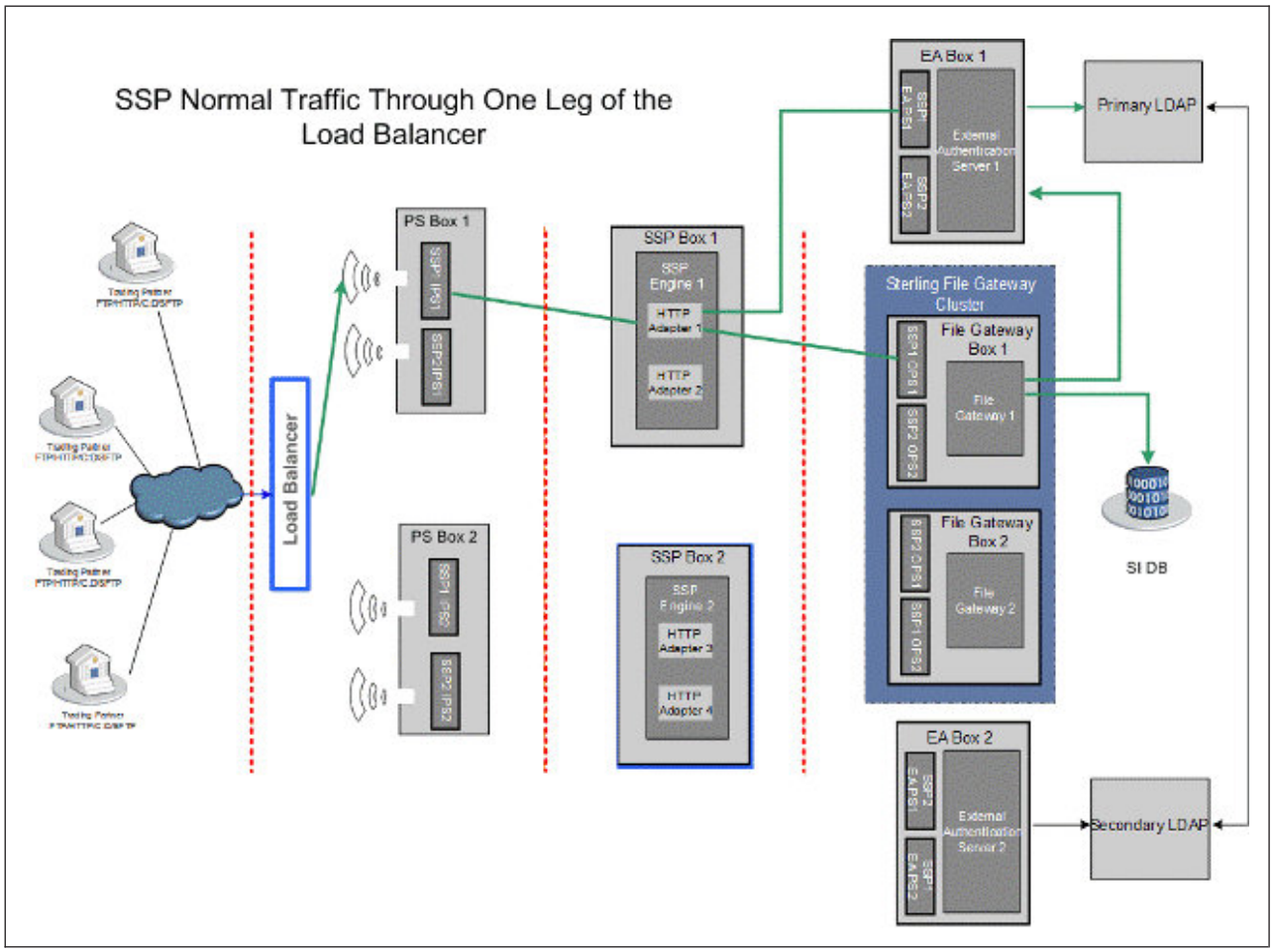


To set up the sample failover environment illustrated above, add the following components to the basic configuration:

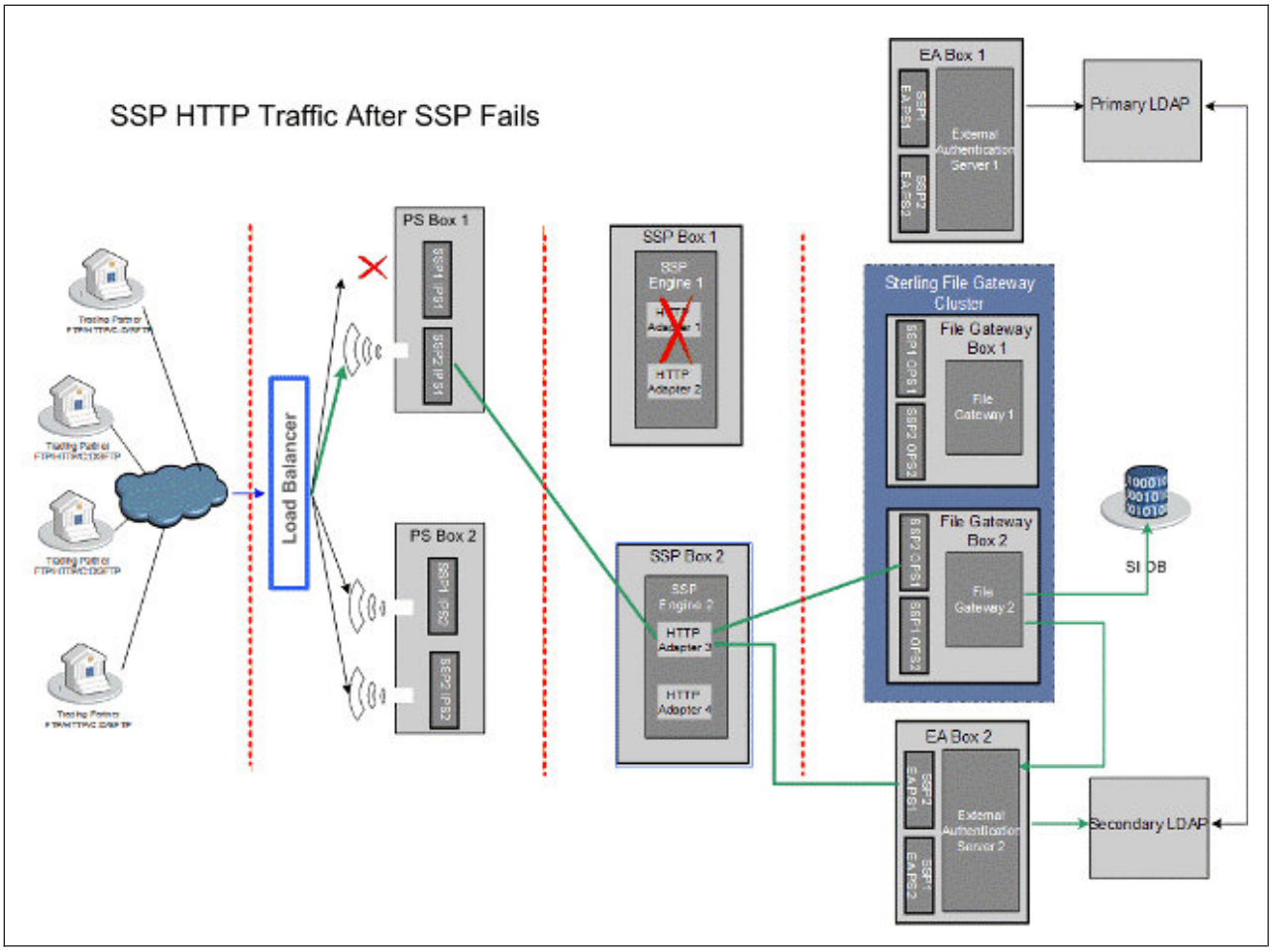
- A second external inbound perimeter server computer (PS Box 2) with two perimeter server instances
- A second perimeter server instance on the initial inbound PS computer (PS Box 1)
- A second Sterling Secure Proxy engine (SSP Box 2)
- A second Sterling External Authentication Server with two perimeter server instances (EA Box 2)
- A second perimeter server instance on Sterling External Authentication Server 1 (EA Box 1)
- A second Sterling File Gateway, configured as part of a two-node cluster (File Gateway Box 2)
- A second LDAP server (Secondary LDAP)

This sample configuration illustrates one way to set up Sterling Secure Proxy for failover support. Your failover setup depends upon your hardware configuration and security requirements.

The following diagram illustrates the flow of traffic through one leg of an Sterling Secure Proxy setup when failover support is configured and all components are operating. Traffic is allowed through the first leg of the setup and moves through the Sterling Secure Proxy engine 1.



The following diagram illustrates the flow of traffic when Sterling Secure Proxy engine 1 is not available and failover support is enabled:



Components to Configure for Failover Support

To configure a failover environment, you must add one or more of the following components to your setup:

- Internal perimeter server—If you configure a perimeter server between the trading partners and Sterling Secure Proxy, configure a second perimeter server to enable failover for the perimeter server.
- Sterling Secure Proxy engine—Install and configure a second engine in your Sterling Secure Proxy setup for failover support. You duplicate the setup of engine 1 in engine 2. However, the adapters for each engine must have unique names.
- Sterling File Gateway—Configure two instances of Sterling File Gateway as a cluster. The instances share a database.
- External Authentication server and LDAP server—For each Sterling File Gateway installation, install an Sterling External Authentication Server and LDAP.

About Failover Support

When failover detection is enabled, the adapter periodically polls the status of the outbound perimeter server and the Sterling External Authentication Server

perimeter server. If one of the perimeter servers is down, the adapter stops the listener. When both perimeter servers are back online, the adapter restarts the listener.

If Sterling Secure Proxy tries to connect to an Sterling External Authentication Server and fails, the adapter stops the listener but continues to poll for the status of the Sterling External Authentication Server connection. When the Sterling External Authentication Server or any alternates are back online and the outbound and Sterling External Authentication Server perimeter servers are connected, the listener is restarted.

If the connection to the standard outbound node and all alternate outbound nodes fail, the adapter stops the listener.

When the outbound node or any alternate nodes are back online and the outbound and Sterling External Authentication Server perimeter servers are connected, the listener is restarted.

You can configure failover support for the HTTP, FTP, SFTP, and Sterling Connect:Direct protocols.

Failover for a Back-end Server

After you configure failover for a back-end server, Sterling Secure Proxy functions as follows:

1. The trading partner connects to Adapter 1 through the load balancer.
2. Sterling Secure Proxy authenticates the user against information stored on the External Authentication Server 1 and connects to the back-end server.
3. If the internal perimeter server (SSP1 OPS1) or the back-end server (File Gateway 1) is not available, the session fails.
4. Sterling Secure Proxy does the following:
   a. Disconnects the listen port for Adapter 1.
   b. Begins a background health check agent to determine when the internal perimeter server and the back-end server are available.
   c. Performs an SSL handshake if SSL is configured between Sterling Secure Proxy and the back-end server.
5. The load balancer recognizes that the adapter is not connected and no longer sends traffic to it.
6. After the internal perimeter server (SSP1 OPS1) and the back-end server (File Gateway 1) are back online, Sterling Secure Proxy enables the adapter 1 listen port and the load balancer makes it available for traffic.
7. The health check agent is stopped.

Overview of Failover Configuration

To configure failover support:

- Configure the load balancer.
- Configure additional perimeter servers.
- Modify a basic Sterling Secure Proxy configuration to add support for failover.
- Configure failover components for Sterling File Gateway and Sterling External Authentication Server.

Configure the Load Balancer

Configure the load balancer so that for each protocol service port, incoming traffic is routed to the corresponding listen port on the pool of destination inbound perimeter servers. After a client connection for a service is routed to a destination IP address, subsequent connections from the same client IP address for that service should be routed to the same destination IP address and port that the first connection was initially routed to (IP stickiness).

Summary of Steps to Set Up a Load Balancer for an HTTP Connection

About this task

To set up a load balancer for an HTTP connection:

Procedure

1. Set up an HTTP monitor to monitor the HTTP adapter ports.
2. Match the value in the **Send String/Receive String** in the load balancer with the values in the Adapter HTTP Ping response and Ping URI fields in the adapter definition.
3. In the **Send String** field, type the following text:

   ```
   GET pingURI HTTP/1.1
   ```

   Following is a sample entry:

   ```
   GET /pingResponse HTTP/1.1
   ```
4. In the **Receive String** field, type the value of the HTTP ping response. Following is a example entry:

   ```
   pingResponse
   ```
5. Provide a dummy user name and password. This information is not used to authenticate the user. It is used so the load balancer sends HTTP headers to Sterling Secure Proxy. You can use any dummy user ID and password.

Configure the Health Check Monitor for FTP

About this task

To configure the health check monitor for FTP:

Procedure

1. Set up a TCP monitor to monitor the FTP adapter ports.
2. Leave the **Send String** field blank.
3. In the **Receive string** field, type the following text:

   ```
   220 Server greeting banner text for FTP adapter.
   ```

   Following is a sample entry:

   ```
   220 FTP Server ready.
   ```

   Note: If the server greeting banner is defined in the FTP adapter, the default value is `FTP server ready.`

Configure the Health Check Monitor for SFTP

About this task

To configure the health check monitor for SFTP:

Procedure

1. Set up a TCP monitor to monitor the SFTP adapter ports.
2. In the **Send string** field, type the following text:

   `SSH-2.0-`*`text string of your choice`*

   Following is a sample entry:

   `SSH-2.0-BigIP`
3. In the **Receive string** field, type the following text:

   `SSH-2.0-`*`pre auth banner for the SFTP adapter`*

   Following is a sample entry:

   `SSH-2.0-Maverick_SSHD`

   Note: If no SSH Server Identification Text is defined in the SFTP adapter, the default value is `Maverick_SSHD.`

Configure the Health Check Monitor for Sterling Connect:Direct

About this task

To configure the health check monitor for Sterling Connect:Direct,

Procedure

1. Set up an HTTP monitor to monitor the Sterling Connect:Direct adapter ports.
2. In the **Send string** field, type the following text:

   `GET / HTTP/1.1`

   Note: Type the **Send string** field exactly as identified above in order for the health check monitor to work.
3. In the **Receive string** field, type the following text:

   `HTTP/1.0 202 Will be ignored`

   Note: Type the **Receive** string field exactly as identified above, including the string Will be ignored, in order for the health check monitor to work.

   The request is a ping request and Sterling Secure Proxy does not allow it to go to the back-end server.

Configure Failover Support for an HTTP Environment

About this task

To configure failover support for an HTTP adapter:

Procedure

1. Install and create two Sterling Secure Proxy engines, two inbound perimeter servers, two outbound perimeter servers, two Sterling External Authentication Servers, and a perimeter server to manage each Sterling External Authentication Server.
2. Configure the components for each Sterling Secure Proxy engine as described in the table below.

Sterling Secure Proxy Engine 1 Configuration for HTTP

About this task

Configure the following components for Engine 1 in an HTTP environment:

Component	Field to Define	Value
HTTP Adapter 1	Adapter Name HTTP Ping Response	HTTPAdapter1 pingResponse
	HTTP Ping URI	/pingResponse
	External Authentication Server	External Authentication Server 1
	Inbound Perimeter Server	SSP1 IPS1
	Outbound Perimeter Server	SSP1 OPS1
	External Authentication Perimeter Server	SSP1 EA PS1
HTTP Netmap	Netmap Name	HTTPNetmap1
	Inbound Node Name	TPNode1
	Policy	PolicyEA
	Outbound Node Name	FileGateway 1
HTTP Adapter 2	Adapter Name	HTTPAdapter2
	HTTP Ping Response	pingResponse
	HTTP Ping URI	/pingResponse
	Inbound Perimeter Server	SSP1 IPS2
	Outbound Perimeter Server	SSP1 OPS2
	External Authentication Perimeter Server	SSP1 EA PS2
	External Authentication Server	External Authentication Server 2
HTTP Netmap	Netmap Name	HTTPNetmap1
	Inbound Node Name	TPNode1
	Policy	PolicyEA
	Outbound Node Name	FileGateway2

Sterling Secure Proxy Engine 2 Configuration for HTTP

About this task

Configure the following components for Engine 2:

Component	Field to Define	Value
HTTP Adapter 3	Adapter Name	HTTPAdapter3
	HTTP Ping Response	pingResponse
	HTTP Ping URI	/pingResponse
	External Authentication Server 2	External Authentication Server 2
	Inbound Perimeter Server	SSP1 IPS1
	Outbound Perimeter Server	SSP1 OPS1
	External Authentication Perimeter Server	SSP1 EA PS1
HTTP Netmap	Netmap Name	HTTPNetmap1
	Inbound Node Name	TPNode1
	Policy	PolicyEA
	Outbound Node Name	FileGateway 2
HTTP Adapter 4	Adapter Name	HTTPAdapter4
	HTTP Ping Response	pingResponse
	HTTP Ping URI	/pingResponse
	External Authentication Server 1	External Authentication Server 2
	Inbound Perimeter Server	SSP1 IPS2
	Outbound Perimeter Server	SSP1 OPS2
	External Authentication Perimeter Server	SSP1 EA PS2
HTTP Netmap	Netmap Name	HTTPNetmap1
	Inbound Node Name	TPNode1
	Policy	PolicyEA
	Outbound Node Name	FileGateway1

Configure Failover Support for an FTP Environment

About this task

To configure failover support for an FTP adapter:

Procedure

1. Install and create two Sterling Secure Proxy engines, two inbound perimeter servers, two outbound perimeter servers, two Sterling External Authentication Servers, and a perimeter server to manage each Sterling External Authentication Server.

2. Configure the components each Sterling Secure Proxy engine as described in the table below. To configure failover support, configure the following components in Sterling Secure Proxy

Sterling Secure Proxy Engine 1 Configuration for FTP

About this task

Configure the following components for Engine 1:

Component	Field to Define	Value
FTP Adapter 1	Adapter Name	FTPAdapter1
	Inbound Perimeter Server	SSP1 IPS1
	Outbound Perimeter Server	SSP1 OPS1
	External Authentication Perimeter Server	SSP1 EA PS1
External Authentication Server	External Authentication Server Name	External Authentication Server 1
	Alternate External Authentication Server 1	External Authentication Server 2
FTP Netmap	Netmap Name	FTPNetmap1
	Inbound Node Name	TPNode1
	Policy	PolicyEA
	Outbound Node Name	SI1
	Alternate Outbound Node Name	SI2
FTP Adapter 2	Adapter Name	FTPAdapter2
	Inbound Perimeter Server	SSP1 IPS2
	Outbound Perimeter Server	SSP1 OPS2
	External Authentication Perimeter Server	SSP1 EA PS2
FTP Netmap	Netmap Name	FTPNetmap1
	Inbound Node Name	TPNode1
	Policy	PolicyEA
	Outbound Node Name	SI 2
	Alternate Outbound Node (SI2)	SI 1
External Authentication Server	External Authentication Server Name	External Authentication Server 1
	Alternate External Authentication Server 1	External Authentication Server 2

Sterling Secure Proxy Engine 2 Configuration for FTP

About this task

Configure the following components for Engine 2:

Component	Field to Define	Value
FTP Adapter 3	Adapter Name	FTPAdapter3
	Inbound Perimeter Server	SSP2 IPS1
	Outbound Perimeter Server	SSP2 OPS1
	External Authentication Perimeter Server	SSP2 EA PS1
External Authentication Server	External Authentication Server Name	External Authentication Server 2
FTP Netmap	Netmap Name	FTPNetmap1
	Inbound Node Name	TPNode1
	Policy	PolicyEA
	Outbound Node Name	SI 2
	Alternate Outbound Node (SI 2)	SI 1
FTP Adapter 4	Adapter Name	FTPAdapter4
	Inbound Perimeter Server	SSP2 IPS2
	Outbound Perimeter Server	SSP2 OPS2
	External Authentication Perimeter Server	SSP2 EA PS2
External Authentication Server	External Authentication Server Name	External Authentication Server 1
FTP Netmap	Netmap Name	FTPNetmap2
	Inbound Node Name	TPNode1
	Policy	PolicyEA
	Outbound Node Name	SI1
	Alternate Outbound Node Name	SI2

Configure Failover Support for an Sterling Connect:Direct Environment

About this task

To configure failover support for a Sterling Connect:Direct adapter:

Procedure

1. Install and create two Sterling Secure Proxy engines, two inbound perimeter servers, two outbound perimeter servers, two Sterling External Authentication Servers, and a perimeter server to manage each Sterling External Authentication Server.

2. Configure the components for each Sterling Secure Proxy engine as described in the table below. To configure failover support, define the following components in Sterling Secure Proxy.

Sterling Secure Proxy Engine 1 Configuration for Sterling Connect:Direct

About this task

Configure the following components for Engine 1 in a Sterling Connect:Direct environment:

Component	Field to Define	Value
Connect Adapter 1	Adapter Name	ConnectAdapter1
	Http Ping Response	pingResponse
	Inbound Perimeter Server	SSP1 IPS1
	Outbound Perimeter Server	SSP1 OPS1
	External Authentication Perimeter Server	SSP1 EA PS1
External Authentication Server	External Authentication Server Name	External Authentication Server 1
	Alternate External Authentication Server 1	External Authentication Server 2
Connect Netmap	Netmap Name	ConnectNetmap1
	Node Name	TPNode1
	Policy	PolicyEA
	Node Name	ConnectServer1
	Destination Service Name	EAServer1
	Alternate Destinations	Connect2
Connect Adapter 2	Adapter Name	ConnectAdapter2
	Http Ping Response	pingResponse
	External Authentication Server	External Authentication Server 2
	Inbound Perimeter Server	SSP1 IPS2
	Outbound Perimeter Server	SSP1 OPS2
	External Authentication Perimeter Server	SSP1 EA PS2
Connect Netmap	Netmap Name	ConnectNetmap1
	Node Name	TPNode1
	Destination Service Name	EAServer1
	Policy	PolicyEA
	Node Name	Connect2

Component	Field to Define	Value
External Authentication Server	External Authentication Server Name	External Authentication Server 1
	Alternate External Authentication Server 1	External Authentication Server 2

Sterling Secure Proxy Engine 2 Configuration for Sterling Connect:Direct

About this task

Configure the following components for Engine 2:

Component	Field to Define	Value
Connect Adapter 3	Adapter Name	ConnectAdapter3
	Http Ping Response	pingResponse
	Inbound Perimeter Server	SSP2 IPS1
	Outbound Perimeter Server	SSP2 OPS1
	External Authentication Perimeter Server	SSP2 EA PS1
External Authentication Server	External Authentication Server Name	ExternalAuthenticationServer2
	Alternate External Authentication Server 1	ExternalAuthenticationServer1
Connect Netmap	Netmap Name	ConnectNetmap1
	Node Name	TPNode1
	Policy	PolicyEA
	Node Name	Connect 2
Connect Adapter 4	Adapter Name	ConnectAdapter4
	Http Ping Response	pingResponse
	Inbound Perimeter Server	SSP2 IPS2
	Outbound Perimeter Server	SSP2 OPS2
	External Authentication Perimeter Server	SSP2 EA PS2
External Authentication Server	External Authentication Server Name	ExternalAuthenticationServer2
	Alternate External Authentication Server 1	ExternalAuthenticationServer1
Connect Netmap	Netmap Name	ConnectNetmap1
	Node Name	TPNode1
	Policy	PolicyEA
	Node Name	FileGateway1

Configure Failover Support for an SFTP Environment

About this task

To configure failover support for an SFTP adapter:

Procedure

1. Install and create two Sterling Secure Proxy engines, two inbound perimeter servers, two outbound perimeter servers, two Sterling External Authentication Servers, and a perimeter server to manage each Sterling External Authentication Server.
2. Configure the components each Sterling Secure Proxy engine as described in the table below.

Engine 1 Configuration for SFTP

About this task

Configure the following components for Engine 1:

Component	Field to Define	Value
SFTP Adapter 1	Adapter Name	SFTPAdapter1
	Inbound Perimeter Server	SSP1 IPS1
	Outbound Perimeter Server	SSP1 OPS1
	External Authentication Perimeter Server	SSP1 EA PS1
External Authentication Server	External Authentication Server Name	External Authentication Server 1
	Alternate External Authentication Server 1	External Authentication Server 2
SFTP Netmap	Netmap Name	SFTPNetmap1
	Inbound Node Name	TPNode1
	Policy	PolicyEA
	Outbound Node Name	SI 1
	Alternate Outbound Node Name	SI 2
	Alternate External Authentication Server 1	External Authentication Server 2
SFTP Adapter 2	Adapter Name	SFTPAdapter2
	SSH Server Identification Text	Maverick_SSHD
	Inbound Perimeter Server	SSP1 IPS2
	Outbound Perimeter Server	SSP1 OPS2
	External Authentication Perimeter Server	SSP1 EA PS2

Component	Field to Define	Value
SFTP Netmap	Netmap Name	SFTPNetmap1
	Inbound Node Name	TPNode1
	Policy	PolicyEA
	Outbound Node Name	SI 2
	Alternate Outbound Node (SI2)	SI 1
External Authentication Server	External Authentication Server Name	External Authentication Server 1
	Alternate External Authentication Server 1	External Authentication Server 2

Sterling Secure Proxy Engine 2 Configuration for SFTP

About this task

Configure the following components for Engine 2:

Component	Field to Define	Value
SFTP Adapter 3	Adapter Name	SFTPAdapter3
	SSH Server Identification Text	Maverick_SSHD
	Inbound Perimeter Server	SSP2 IPS1
	Outbound Perimeter Server	SSP2 OPS1
	External Authentication Perimeter Server	SSP2 EA PS1
EA Server	External Authentication Server Name	External Authentication Server 2
STTP Netmap	Netmap Name	SFTPNetmap1
	Inbound Node Name	TPNode1
	Policy	PolicyEA
	Outbound Node Name	SI 2
	Alternate Outbound Node (SI 2)	SI 1
SFTP Adapter 4	Adapter Name	SFTPAdapter4
	Inbound Perimeter Server	SSP2 IPS2
	Outbound Perimeter Server	SSP2 OPS2
	External Authentication Perimeter Server	SSP2 EA PS2
EA Server	External Authentication Server Name	External Authentication Server 1

Component	Field to Define	Value
SFTP Netmap	Netmap Name	SFTPNetmap1
	Inbound Node Name	TPNode1
	Policy	PolicyEA
	Outbound Node Name	SI1
	Alternate Outbound Node Name	SI2

Failover Support Properties

Modify the default settings for one or more of the following reasons:

- Enable failover detection
- Modify the polling frequency
- Modify how long a connection can be tried, before the connection fails
- Change the name of the profile sent to Sterling External Authentication Server to request user authentication
- Enable the debug log for failover
- Prevent load balance ping requests from being writing to the debug log

Change Failover Support Properties

About this task

To change a failover support property setting:

Procedure

1. From the Sterling Secure Proxy menu, select **Configuration**.
2. Expand the **Adapters** selection in the navigation panel on the left.
3. Highlight the **Adapter** to modify.
4. Click the **Properties** tab.
5. Modify one or more of the following properties:
   - failover.detection.mode—Determines the mode used to poll the Sterling External Authentication Server and outbound nodes. Set this property to continuous to poll the Sterling External Authentication Server and outbound nodes at the same interval defined in the outbound and Sterling External Authentication Server perimeter servers. Set the property to `standard` to detect that outbound or Sterling External Authentication Server nodes are down only when a connection is attempted. Default=standard.
   - failover.detection.enabled—Enables failover detection. Set this property to `true` to enable failover detection. Default=false.
   - failover.poll.interval—To configure polling frequency, in seconds. Default=5.
   - failover.conn.timeout—To identify how much time is allowed to make a connection, before the connection fails. Default=15.
   - failover.ea.ping.profile —Name of the profile sent to Sterling External Authentication Server to detect if LDAP is available. By default, a profile called sspDUMMYprofile is sent. Change this property to use an actual profile name to extend healthcheck to the LDAP server. Define a profile with this name in Sterling External Authentication Server.

- failover.debug—To enable debug logging for failover. By default, debug logging is disabled. To enable debug logging for failover, set this property to `true`. Output is written to the file called failover.log in the /logs directory.
- load.balancer.addr—Internal IP of load balancer. When this property is defined, all log messages generated by inbound traffic for this address are suppressed.

6. Click **Save**.

Notices

This information was developed for products and services offered in the U.S.A.

IBM® may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

1623-14, Shimotsuruma, Yamato-shi

Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be

incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

J46A/G4

555 Bailey Avenue

San Jose, CA 95141-1003

U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© IBM 2012. Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2012.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Connect Control Center®, Connect:Direct®, Connect:Enterprise®, Gentran®, Gentran®:Basic®, Gentran:Control®, Gentran:Director®, Gentran:Plus®, Gentran:Realtime®, Gentran:Server®, Gentran:Viewpoint®, Sterling Commerce™, Sterling Information Broker®, and Sterling Integrator® are trademarks or registered trademarks of Sterling Commerce®, Inc., an IBM Company.

Other company, product, and service names may be trademarks or service marks of others.

Printed in USA