

Sterling Secure Proxy



FTP Reverse Proxy Scenarios

Version 34

Sterling Secure Proxy



FTP Reverse Proxy Scenarios

Version 34

Note

Before using this information and the product it supports, read the information in "Notices" on page 63.

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.

© **Copyright IBM Corporation 2006, 2012.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Chapter 1. FTP Reverse Proxy Configuration	1	Chapter 15. Enable a Clear Control Channel for an Outbound FTP Node Connection	33
Chapter 2. Complete FTP Scenario Worksheets	3	Chapter 16. Add Local User Authentication to the Inbound FTP Connection	35
Chapter 3. Complete and Test FTP Configuration Scenarios.	5	Chapter 17. Add Local User Authentication to the FTP Inbound Connection	37
Chapter 4. Create a Basic FTP Configuration	7	Chapter 18. Add Credentials to the Local User Store	39
Chapter 5. Basic FTP Configuration Worksheet.	9	Chapter 19. Connect to the Outbound FTP Server Using Credentials from the Netmap	41
Chapter 6. Create an FTP Policy	11	Chapter 20. Strengthen Authentication of an FTP Node Using Sterling External Authentication Server	43
Chapter 7. Create an FTP Netmap	13	Chapter 21. Authenticate the Inbound FTP Node Using Sterling External Authentication Server	45
Chapter 8. Define the FTP Adapter Used for the Connection	15	Chapter 22. Connect to Outbound FTP Server Using Sterling External Authentication Server Worksheet	47
Chapter 9. What You Defined with the Basic FTP Configuration Scenario	17	Chapter 23. Connect to the Outbound Node Using Information Stored in Sterling External Authentication Server.	49
Chapter 10. Variations on the Basic FTP Configuration	19	Chapter 24. Test the Inbound and Outbound FTP Connections	51
Define Connection Requirements Between Sterling Secure Proxy and Inbound FTP Nodes	19	Chapter 25. Route an Outbound FTP Connection to Alternate Sterling B2B Integrator Servers	53
Define Inbound Node Connection Definitions for an FTP Connection	21	Chapter 26. Define a Passive Data Outbound Port Range for an FTP Reverse Proxy Adapter.	55
Chapter 11. Add SSL/TLS Support for an FTP Connection	23		
SSL/TLS Support Worksheet	24		
Chapter 12. Secure the Inbound FTP Connection Using the TLS or SSL Protocol	27		
Enable a Clear Control Channel for an Inbound FTP Node Connection	28		
Chapter 13. Secure the Outbound FTP Connection Using the TLS or SSL Protocol	29		
Chapter 14. Variations on the Add SSL/TLS Support on the Outbound Node	31		

Chapter 27. Define a Passive NAT Address for an FTP Reverse Proxy Adapter 57

Chapter 28. Define an Active Data Outbound Port Range for an FTP Reverse Proxy Adapter. 59

Chapter 29. Use IP Address from a PASV Response For Outbound Data Connections 61

Notices 63

Chapter 1. FTP Reverse Proxy Configuration

The FTP configuration scenarios describe how to configure FTP protocol connections to and from the Sterling Secure Proxy engine.

Note: Configuration information must be available on the engine before communication sessions with Sterling B2B Integrator can be established.

Organization of the FTP Configuration Scenarios

The first scenario instructs you how to configure a basic configuration. Each successive scenario adds a security feature to the basic configuration. After adding a security feature, test the connection to ensure that you have correctly configured it. You determine your security needs and configure the security features applicable for your environment.

The following scenarios help you configure and test Sterling Secure Proxy for FTP protocol connections to the Sterling B2B Integrator server:

- Create a basic FTP configuration
- Add SSL/TLS support
- Perform user authentication using the local user store
- Provide outbound credentials using the netmap

The remaining configuration scenarios require Sterling External Authentication Server, an optional security feature that must be configured independently. After Sterling External Authentication Server is configured, you can update your basic security definitions to enable Sterling Secure Proxy to connect to the Sterling External Authentication Server to enforce the following advanced security features:

- Authenticate an inbound certificate or user using Sterling External Authentication Server
- Manage connection requirements to the outbound server using Sterling External Authentication Server

Other options help you do the following:

- Define alternate nodes for failover support
- Define a passive data outbound port range for an FTP Reverse Proxy adapter
- Define a passive NAT address for an FTP Reverse Proxy adapter
- Define an active data outbound port range for an FTP Reverse Proxy adapter

Chapter 2. Complete FTP Scenario Worksheets

About this task


Before you begin configuring Sterling Secure Proxy for FTP connections, gather the information on the worksheet provided with the scenario. You use this information as you configure each feature. Complete worksheets as follows:

Procedure

1. Provide a value for each Sterling Secure Proxy feature listed. Fields listed in the worksheet are required.
2. Accept default values for fields not listed.
3. The worksheet identifies the Configuration Manager field where you will specify each value.

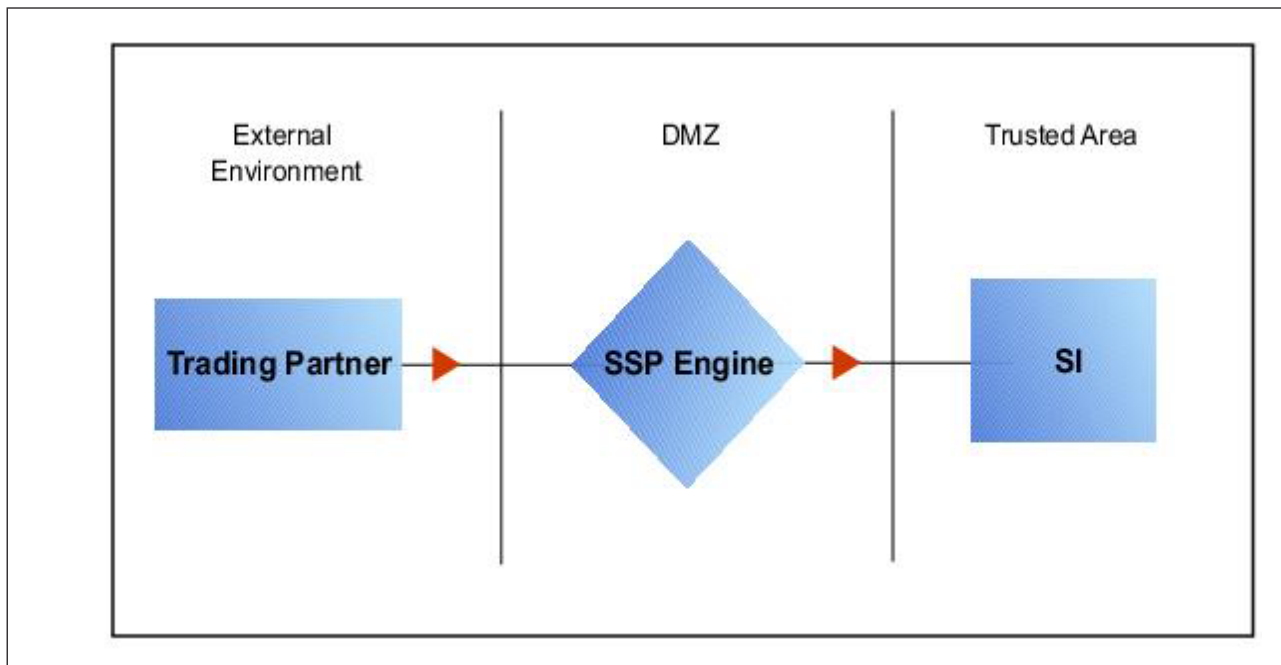
Chapter 3. Complete and Test FTP Configuration Scenarios

Work through the sequence of FTP configuration scenarios in the order in which they are presented to add and test more security features. Be sure to test each feature before you add the next to the configuration. Before you move Sterling Secure Proxy into production, ensure that you have configured and tested the security features needed for your environment.

Note: As you complete each task, provide all required information. If information is not provided or is incorrect, the following error icon is displayed:  To view more information about the error, hover over the icon.

Chapter 4. Create a Basic FTP Configuration

This scenario contains all the information and tools you need to configure Sterling Secure Proxy to establish a basic connection from a trading partner to the Sterling B2B Integrator server as illustrated below. You accept default values when configuring this scenario. As a result, no authentication occurs in Sterling Secure Proxy and credentials presented by the inbound node are passed through to the Sterling B2B Integrator server.



After you configure Sterling Secure Proxy, validate the configuration by initiating an FTP connection from the trading partner. For more information on testing the configuration, see *Test the Inbound and Outbound FTP Connections*.

Complete the following tasks to define a basic FTP configuration:

- Create a policy
- Define inbound and outbound connections in a netmap
- Define an FTP adapter

Chapter 5. Basic FTP Configuration Worksheet

About this task

Before you configure Sterling Secure Proxy for FTP connections, gather the information on the Basic FTP Configuration Worksheet. You use this information as you configure a basic FTP connection.

Procedure

1. Create a basic policy. In a later FTP configuration scenario, you edit this policy to add security features to it.

Configuration Manager Field	Feature	Value
Policy Name	Name of policy.	

2. Create a netmap that contains connection information for the nodes connecting to and from Sterling Secure Proxy: the trading partner (inbound node) and the Sterling B2B Integrator server (outbound node). You will also associate the basic security policy you create with the inbound node.

Configuration Manager Field	Feature	Value
Netmap Name	Name of the netmap.	

Inbound Trading Partner Information

Inbound Node Name	Trading partner name (name to assign to inbound node definition).	
Peer Address Pattern	Host name or IP address pattern.	* (* allows all inbound nodes to connect to the Sterling B2B Integrator server, using this definition. To define a more specific node definition, see <i>Create a Basic FTP Configuration</i> .)
Policy	Name of policy you create.	This value is selected from a pull-down list.

Outbound FTP Server Connection

Node Name	Outbound FTP server node name.
Primary Destination Address	Host name or IP address to connect to the outbound FTP server.
Primary Destination Port	Port number to connect to the outbound FTP server.

3. Create an FTP adapter that defines information necessary to establish FTP connections to and from Sterling Secure Proxy. When you configure the

adapter, select the basic netmap and the outbound FTP server you define in the netmap definition. If the outbound host uses virtual IP address, set the IP address in the PASV response.

Configuration		
Manager Field	Feature	Value
Adapter Name	Adapter name.	
Listen Port	Listen port to use for inbound connections.	
Netmap	Netmap to associate with the adapter.	
Standard Routing Node	Name of the outbound node corresponding to the Sterling B2B Integrator server where inbound connections are routed.	
Engine	Engine to run on.	

Chapter 6. Create an FTP Policy

About this task

The FTP policy defines how you impose controls to authenticate a trading partner trying to access Sterling B2B Integrator server over the public Internet.

To define a policy:

Procedure

1. Click **Configuration** from the menu bar.
2. Click **Actions > New Policy > FTP Policy**.
3. Type a **Policy Name**.
4. Click **Save**.

Chapter 7. Create an FTP Netmap

About this task

You define inbound connection information for your trading partners and outbound connection information for the Sterling B2B Integrator server that Sterling Secure Proxy connects to. These values are stored in a netmap. The netmap is associated with a policy and an adapter.

Before you begin this procedure, create a policy to associate with the netmap.

To create a netmap and define inbound and outbound nodes:

Procedure

1. Click **Configuration** from the menu bar.
2. Click **Actions > New Netmap > FTP Netmap**.
3. Type a **Netmap Name**.
4. To define an inbound node definition, click the **Inbound Nodes** tab and click **New**.
5. Specify the following values:
 - **Inbound Node Name**
 - **Peer Address Pattern**
 - **Policy**

Note: If you have not defined a policy, click the green plus sign to define one.
6. Click **OK**.
7. To define an outbound node definition, click the **Outbound Nodes** tab and click **New**.
8. Specify the following values:
 - **Outbound Node Name**
 - **Primary Destination Address**
 - **Primary Destination Port**
9. Click **OK**.
10. Click **Save**.

Chapter 8. Define the FTP Adapter Used for the Connection

About this task

An FTP adapter definition specifies system-level communications information necessary for FTP connections to and from Sterling Secure Proxy. You can create multiple adapter definitions.

Before you begin this procedure, create the following definitions:

- A netmap to associate with the adapter
- An engine definition to associate with the adapter. Refer to *Install or Upgrade Sterling Secure Proxy on UNIX or Linux* or *Install or Upgrade Sterling Secure Proxy on Microsoft Windows* for instructions.

To define an FTP adapter:

Procedure

1. Click **Configuration** from the menu bar.
2. Click **Actions > New Adapter > FTP Reverse Proxy**.
3. Specify values for the following:
 - **Adapter Name**
 - **Listen Port**
 - **Netmap**
 - **Standard Routing Node**
 - **Engine**
4. Click **Save**.

Chapter 9. What You Defined with the Basic FTP Configuration Scenario

Creating secure connections to Sterling B2B Integrator servers on behalf of nodes external to your trusted zone requires that you organize information about the trading partners and the Sterling B2B Integrator server in a policy, a netmap, and an adapter definition. You created these items when you defined the Basic FTP Configuration. The next step is testing the configuration prior to configuring additional security features. Before you test the configuration, be sure that:

- The Sterling B2B Integrator server has an active FTP server adapter configured to listen for the port specified in the outbound node definition.
- The user ID and password provided by the inbound node is defined at the Sterling B2B Integrator server.

Refer to *Test the Inbound and Outbound FTP Connections* for information about testing the FTP Reverse Proxy configurations outlined in this scenario.

As you add complexity to your security configurations using the procedures in the remaining scenarios, you modify the basic configuration to configure more complex authentication and certificate validation measures.

Chapter 10. Variations on the Basic FTP Configuration

After you confirm that the communications sessions you established using the Basic FTP configuration were successful, you may want to validate sessions using other types of inbound trading partner definitions before you add complexity to the security configuration. To ensure that you can validate and troubleshoot problems, you should test one variation at a time by changing the configuration, initiating a connection, and verifying the result.

Inbound FTP Trading Partner Node Definitions

You can modify the inbound trading partner node definitions as follows:

- Define a specific IP address
- Define a wildcard peer pattern
- Define an IP/subnet pattern

Define Connection Requirements Between Sterling Secure Proxy and Inbound FTP Nodes

You define connection requirements between Sterling Secure Proxy and inbound nodes by defining inbound node definitions. Refer to your company security requirements to determine how tightly to define the parameters an inbound node must provide to allow a connection.

You can define inbound node definitions to allow only one individual inbound connection, or you can identify IP address patterns and create an inbound definition that allows inbound connections that match the pattern to connect to Sterling Secure Proxy. Methods of defining inbound nodes are as follows:

- Create an entry for an individual inbound node and define the inbound node IP address that can connect to Sterling Secure Proxy. Only connections from that IP address are allowed. A single IP address must be specified as a subnet pattern where all bits are matched, such as 11.22.33.44/32. Sterling Secure Proxy also supports individual host names. They must match the value returned by a reverse DNS lookup.
- Define an inbound node entry that allows all nodes that match an IP/subnet address pattern. Patterns include:
 - Matching the first 16 bits of an IP address pattern. For example, 10.20.0.0/16 allows all IP addresses that begin with 10.20.* to connect to Sterling Secure Proxy.
 - Matching the first 8 bits of an IP address pattern. For example, 10.0.0.0/8 allows all IP addresses that begin with 10.* to connect to Sterling Secure Proxy.
- Define an inbound node entry that allows all inbound nodes that match a wildcard host name pattern. When a connection is attempted and you have defined a wildcard host name pattern definition, a reverse DNS lookup is performed on the IP address of the inbound connection. The DNS name is compared to the wildcard pattern. Wildcard patterns include:
 - * matches any number of characters before or after a period. For example, *.a.com allows a connection from b.a.com but not from a.bc.com. A single * allows all inbound nodes to successfully connect to Sterling Secure Proxy.

- ? matches one character. For example, a?.com allows a connection from a.b.com but not from a.bc.com.

You can define more than one inbound node definition and use a combination of the node definition methods. Order the definitions from most specific to least specific. When an inbound node connection is attempted, Sterling Secure Proxy compares the IP address of the inbound node to the first inbound node definition. If it matches, a connection is established. If it does not match, Sterling Secure Proxy checks the next inbound node definition until a match is found. If no match is found, the connection is terminated.

Inbound FTP Connection Definition Worksheet

Use the following worksheet to identify the information needed to configure inbound node definitions for a specific inbound node or for groups of inbound nodes that match a pattern.

Configuration Manager Field	Define Inbound Trading Partner Information	Value
<p>Note: If you define a single node and definitions for multiple nodes using pattern matching, ensure that you order the definitions from most specific to least specific, because Sterling Secure Proxy processes them in the order in which they are listed.</p>		
Inbound Node Name	Trading partner name.	
Policy Name	Policy to associate with the inbound trading partner.	
<p>For a Single Node</p>		
Peer Address Pattern	IP address	
	<p>Create an entry for an individual inbound node and define the inbound node IP address that can connect to Sterling Secure Proxy. Only connections from that IP address will be allowed. Sterling Secure Proxy supports host name. An example definition is a.b.com.</p> <p>A single IP address must be specified as a subnet pattern where all bits are matched, such as 11.22.33.44/32.</p>	
<p>For Multiple IP Addresses Using IP/Subnet Pattern</p>		
Peer Address Pattern	Peer Address IP/Subnet Pattern Options.	
<p>For Multiple Nodes Using Wildcard Peer Address Pattern to Validate Inbound DNS</p>		
Peer Address Pattern	Wildcard Peer Address Pattern.	

Define Inbound Node Connection Definitions for an FTP Connection

About this task

This procedure instructs you how to modify the basic FTP configuration to add inbound node definitions for:

1. a group of nodes with similar information
2. that limit access to one specific inbound node

To perform this procedure, you must have already configured an adapter. Gather a list of all inbound trading partners, including names and IP addresses.

To define inbound connection definitions:

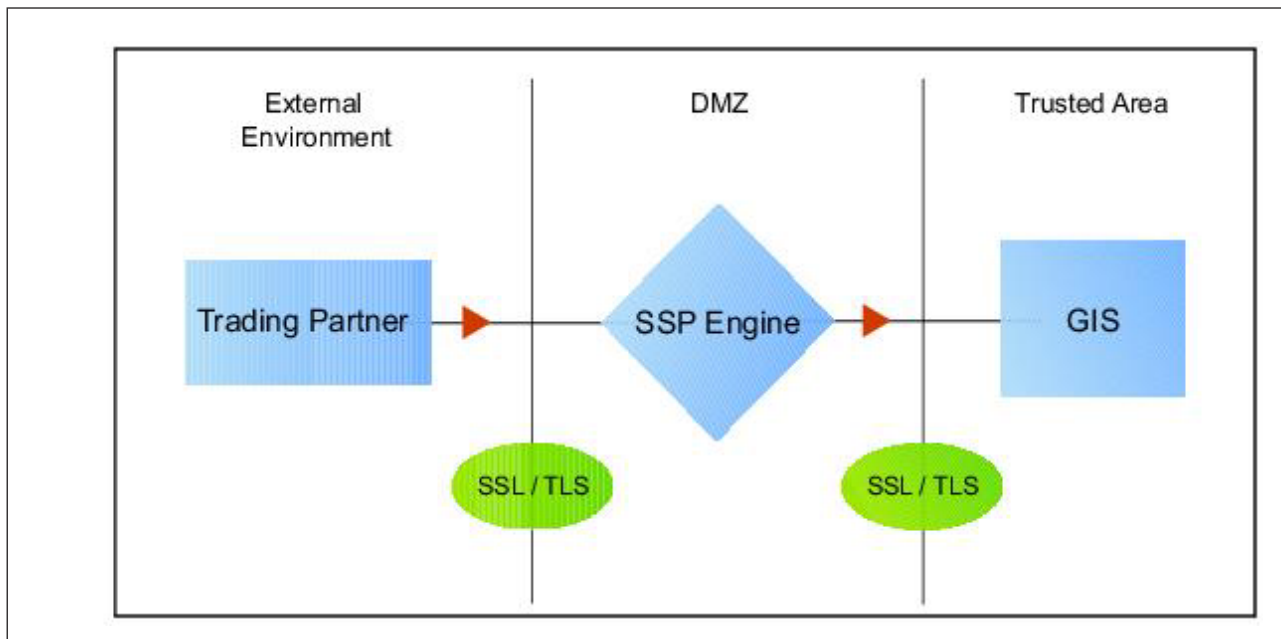
Procedure

1. Identify patterns that can be used to define groups of inbound nodes.
2. To increase security, you need to define a trading partner connection for any individual IP address.
3. Click **Configuration** from the menu bar.
4. Expand the **Netmaps** tree and click the netmap to modify.
5. Click **New** to add a new inbound node definition.
6. Using the information you defined on the Inbound Connection Definition Worksheet, provide the following information, and click **Save**:
 - Inbound Node Name
 - Peer Address Pattern
 - Policy
7. Repeat step 6 for every group of connections and every individual IP address connection you want to define.
8. If necessary, reorder the node definitions in the netmap. Order definitions from most specific to least specific because they will be evaluated in order.
 - a. Click the radio button beside the inbound node definition to move.
 - b. Click **Move Up** or **Move Down** until the node definition is in the correct order.
9. Click **Save**.

Chapter 11. Add SSL/TLS Support for an FTP Connection

About this task

This scenario builds on the Basic FTP Configuration by enabling security for the inbound and outbound nodes you defined in the netmap. Following is a diagram to illustrate the addition of SSL or TLS to the inbound and outbound node connections.



To add SSL/TLS support to the netmap for the inbound and outbound nodes, select the following options for the connections:

- Protocol
- Cipher suites
- Stores and certificates

To effectively configure and test this scenario:

Procedure

1. Add SSL/TLS support to the inbound node definition first and establish a session initiated by an FTP client to an Sterling B2B Integrator server.
2. Add SSL/TLS support to the outbound node definition and establish a session initiated by an FTP client to an Sterling B2B Integrator server.

Note: Before you configure SSL or TLS support, you must check in your certificates. Refer to *Manage Certificates for SSL/TLS Transactions with Trading Partners*.

SSL/TLS Support Worksheet

Before you add SSL/TLS support to the connection information you created in the Basic FTP Configuration scenario, gather the information on the SSL/TLS Support Worksheet. You use this information as you configure the inbound and outbound nodes for SSL/TLS support.

Select the security setting and cipher suites to be used to secure the connection. To configure client authentication, enable this option. Select the key/system certificate to use to validate the connection.

Configuration Manager Field	Feature	Value
Inbound Node Name	Name of inbound node to add security to.	Select an inbound node definition from the list.
Security Setting	Security protocol to use.	<ul style="list-style-type: none"> • SSL v3 or TLS • SSL v2 or v3 with v3 Hello • SSL (any version) or TLS • SSL v2 or v3, TLS, or SSL v3
Enable Client Authentication	Do you want to require that the inbound connection present its certificate for SSL or TLS client authentication?	(Yes or No)
Trust Store	If client authentication is enabled, identify the trust store used to verify the client certificate.	
CA Certificates/Trusted Root	Name of CA certificate/trusted root (if client authentication is enabled).	
Key Store	The location where the keys and system certificates you want to use are stored.	
Key/System Certificate	Name of Sterling Secure Proxy system certificate presented to the inbound connection during the handshake.	
Available Cipher Suites	Select the ciphers to enable by moving them from the Available Ciphers to the Selected Ciphers field.	
Selected Cipher Suites		

Select the security setting and cipher suites to be used to secure the outbound connection. Select the key/system certificate to use to validate the connection.

Configuration Manager Field	Feature	Value
Outbound Node Name	Name of outbound node to add security to.	Select a node definition from the list
Security Setting	Security protocol to use.	<ul style="list-style-type: none"> • SSL v3 or TLS • SSL v2 or v3 with v3 Hello • SSL (any version) or TLS • SSL v2 or v3, TLS, or SSL v3
Trust Store	If client authentication is enabled, identify the trust store where the certificate is stored.	
CA Certificates/Trusted Root	Identify the certificate to use to secure the outbound connection.	
Key Store	The location where the keys and system certificates you want to use are stored.	
Key/System Certificate	Key/System Certificate	
Available Cipher Suites	Cipher suites to enable.	
Selected Cipher Suites		

Chapter 12. Secure the Inbound FTP Connection Using the TLS or SSL Protocol

About this task

The first step in strengthening security is to secure the communications channel. This procedure describes how to enable the TLS or SSL protocol for the inbound connection to authenticate Sterling Secure Proxy to the trading partner initiating the connection. To require that Sterling Secure Proxy authenticate the inbound node, enable client authentication.

Before you can configure this option, you must obtain the necessary certificates and place them in the Sterling Secure Proxy certificate store.

To enable the TLS or SSL protocol on the inbound FTP node:

Procedure

1. Click **Configuration** from the menu bar.
 2. Expand the Netmaps tree and select a netmap to modify.
 3. Click the **Inbound Nodes** tab.
 4. Select an inbound node to modify, and click **Edit**.
 5. Click the **Security** tab, and then click **Secure Connection** to enable security.
 6. Select values for the following:
 - Security Setting
 - Key Store
 - Key/System Certificate
 - Available Ciphers
 - Selected Ciphers
 7. To enable client authentication:
 - a. Click **Enable Client Authentication**.
 - b. Select the Trust Store where the certificate you want to use is located.
 - c. Select the CA Certificates/Trusted Root to use to authenticate the certificate presented by the inbound node.
- Note:** Be sure to highlight the certificate to select it. If only one certificate is displayed in the field, it is not selected until you highlight it.
8. Click **OK**.
 9. Click **Save**.

Results

After you confirm that the communications sessions you established using the basic FTP configuration with SSL/TLS enabled on the inbound node were successful, you may want to enable a clear control channel.

Enable a Clear Control Channel for an Inbound FTP Node Connection

About this task

After you confirm that the communications sessions you established using the basic FTP configuration with SSL/TLS enabled on the inbound node were successful, you may want to enable a clear control channel.

If your environment requires that a firewall be able to see the flow of FTP commands and responses, enable the clear control channel option. Enabling clear control channel for the inbound node requires that the inbound FTP client send the clear control channel command and switch the control channel to an unencrypted channel after user authentication is completed.

To enable a clear control channel for an inbound node:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Netmaps** tree and select a netmap to modify.
3. Click the **Inbound Nodes** tab and select the Inbound Node to modify.
4. Click **Edit**.
5. Click the **Security** tab.
6. Enable **Clear Control Channel**.
7. Click **OK**.
8. Click **Save**.

Chapter 13. Secure the Outbound FTP Connection Using the TLS or SSL Protocol

About this task

If the Sterling B2B Integrator server has enabled the use of SSL or TLS to secure the connection, you must enable the TLS or SSL protocol in the Sterling Secure Proxy outbound node configuration. This procedure describes how to enable the TLS or SSL protocol to authenticate the Sterling B2B Integrator server to Sterling Secure Proxy when establishing an outbound connection.

Before you can configure this option, you must obtain the necessary certificates and place them in the Sterling Secure Proxy certificate store.

To enable the TLS or SSL protocol:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the Netmaps tree and select a netmap to modify.
3. Click the **Outbound Nodes** tab.
4. Select an outbound node to modify, and click **Edit**.
5. Click the **Security** tab, and then click **Secure Connection** to enable security.
6. Select the following security options for the node:
 - Security Setting
 - Trust Store
 - CA Certificates/Trusted Root

Note: Be sure to highlight the certificate to select it. If only one certificate is displayed in the field, it is not selected until you highlight it.

- Key Store
 - Key/System Certificate
 - Available Ciphers Suites
 - Selected Ciphers Suites
7. Click **OK**.
 8. Click **Save**.

Chapter 14. Variations on the Add SSL/TLS Support on the Outbound Node

After you confirm that the communications session you established using the Add SSL/TLS Support scenario was successful, you may want to further modify your inbound and outbound nodes. To ensure that you can validate and troubleshoot problems, you should test one variation at a time by changing the configuration, initiating a connection, and verifying the result.

The following variation applies to this configuration:

Note: You must obtain the necessary certificates and place them in the Sterling Secure Proxy certificate store before you can configure these options.

- Create your own trust store and key store
- Enable a clear control channel for an outbound connection

Chapter 15. Enable a Clear Control Channel for an Outbound FTP Node Connection

About this task

If your environment requires that a firewall be able to see the flow of FTP commands and responses, enable the clear control channel option. If clear control channel is enabled on the outbound node, the FTP reverse proxy adapter sends the clear control channel command and switches the command channel to an unencrypted channel, after user authentication is completed.

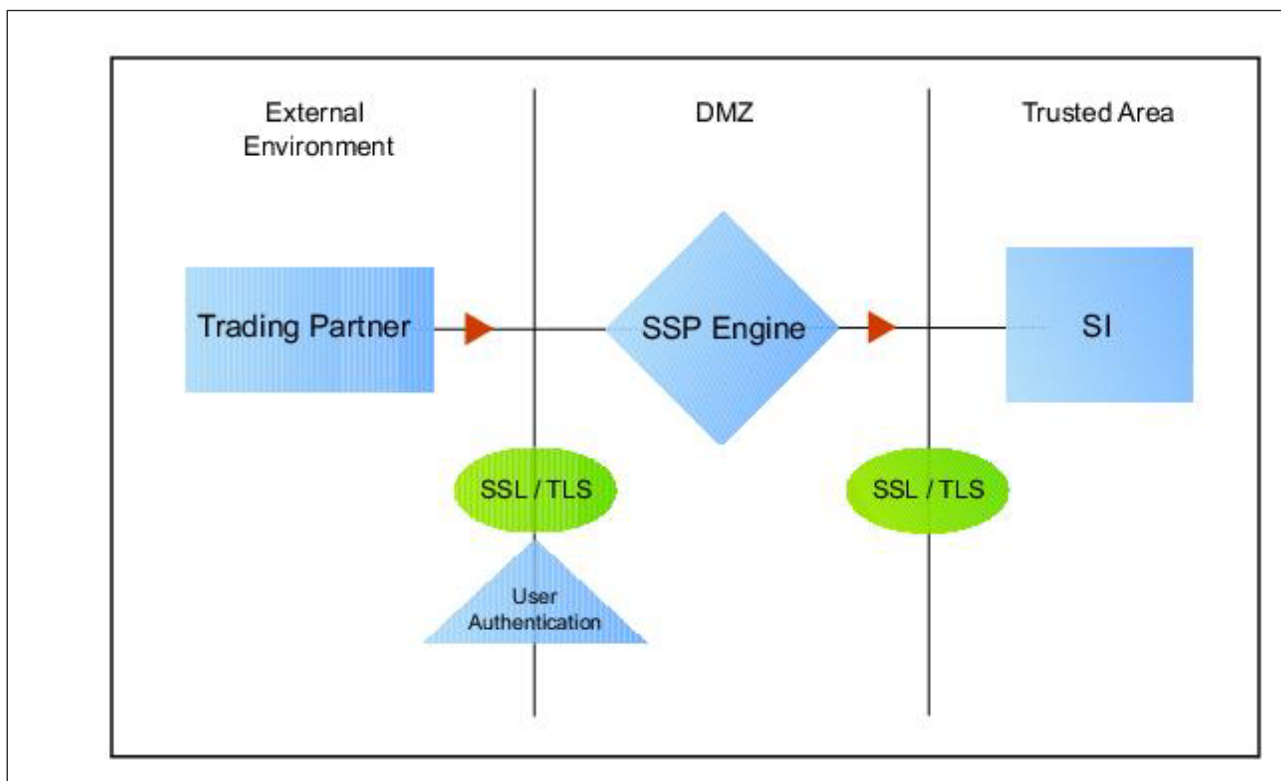
To enable a clear control channel for an outbound node:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the Netmaps tree and select a netmap to modify.
3. Click the **Outbound Nodes** tab and select the Outbound Node to modify.
4. Click **Edit**.
5. Click the **Security** tab.
6. Enable **Clear Control Channel**.
7. Click **OK**.
8. Click **Save**.

Chapter 16. Add Local User Authentication to the Inbound FTP Connection

This scenario builds on the Basic FTP Configuration by adding local user authentication to the inbound connection using information defined in the local user store. The user ID and password presented by the inbound node are authenticated against the information stored in the local user store. The values must match before a connection is established. You must add this information to the local user store before you can test this scenario. Following is an illustration of the secure features supported in this scenario:



Adding user authentication to the inbound connection defined in the Basic FTP Configuration involves enabling user authentication and specifying information about the trading partner.

After you configure user authentication using the local user store information, validate the configuration by establishing a session initiated by an FTP client to an Sterling B2B Integrator server.

FTP Inbound Connection (Local User Authentication) - Worksheet

Before you add user authentication to the inbound connection you created in the Basic FTP Configuration scenario, gather the information on the FTP Inbound Connection (Local User Authentication) - Worksheet. Use this information as you configure user authentication for the inbound connection.

In this scenario, you edit the policy you created in the FTP Basic Configuration scenario and enable user authentication. You also add a user ID and password for the trading partner to the default user store.

Configuration Manager Field	Feature	Value
Policy Name	Name of policy associated with the inbound node.	
User Authentication	Method to use to authenticate the inbound node.	Through Local User Store
User Store	Name of the user store you create.	
User Name	Name of the user you define in the User Store.	
Password	The password value to use to validate the inbound connection.	
Confirm Password		

Chapter 17. Add Local User Authentication to the FTP Inbound Connection

About this task

You can strengthen the security of inbound connections by enabling user authentication. This procedure describes how to add user information to the local user store to be validated by the engine during an inbound FTP client connection.

Note: Check the netmap to ensure that the policy you select is associated with the inbound nodes you want to authenticate.

To add user authentication for an inbound connection:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Policies** tree and select a policy to modify.
3. Click the **Advanced** tab.
4. Enable the **User Authentication Through Local User Store** option.
5. Click **OK**.
6. Click **Save**.

Chapter 18. Add Credentials to the Local User Store

About this task

If you enable user authentication through the local user store, you have to add user information to the local user store for validation by Sterling Secure Proxy during an inbound FTP client connection.

Before you begin this procedure:

- Enable user authentication for the inbound connection.
- Ensure that the engine is configured to use the user store containing the user credentials.

To add user information to the local user store:

Procedure

1. Click **Credentials** from the menu bar.
2. Expand the **User Stores** tree and select a user store to modify.
3. From the **User Store Configuration** panel, click **New**.
4. Specify values for the following:
 - **User Name**
 - **Password**
 - **Confirm Password**
5. Click **Save**.

Chapter 19. Connect to the Outbound FTP Server Using Credentials from the Netmap

About this task

To increase security for connections to the server in the trusted zone, you can use the netmap to store the user ID and password to connect to the outbound Sterling B2B Integrator server. If you configure this option, the inbound node uses one set of credentials to connect to Sterling Secure Proxy and Sterling Secure Proxy uses information stored in the netmap to connect to the outbound FTP server.

Before you configure this option:

- Ensure the user ID and password are defined on the Sterling B2B Integrator server.
- Obtain the user ID and password.

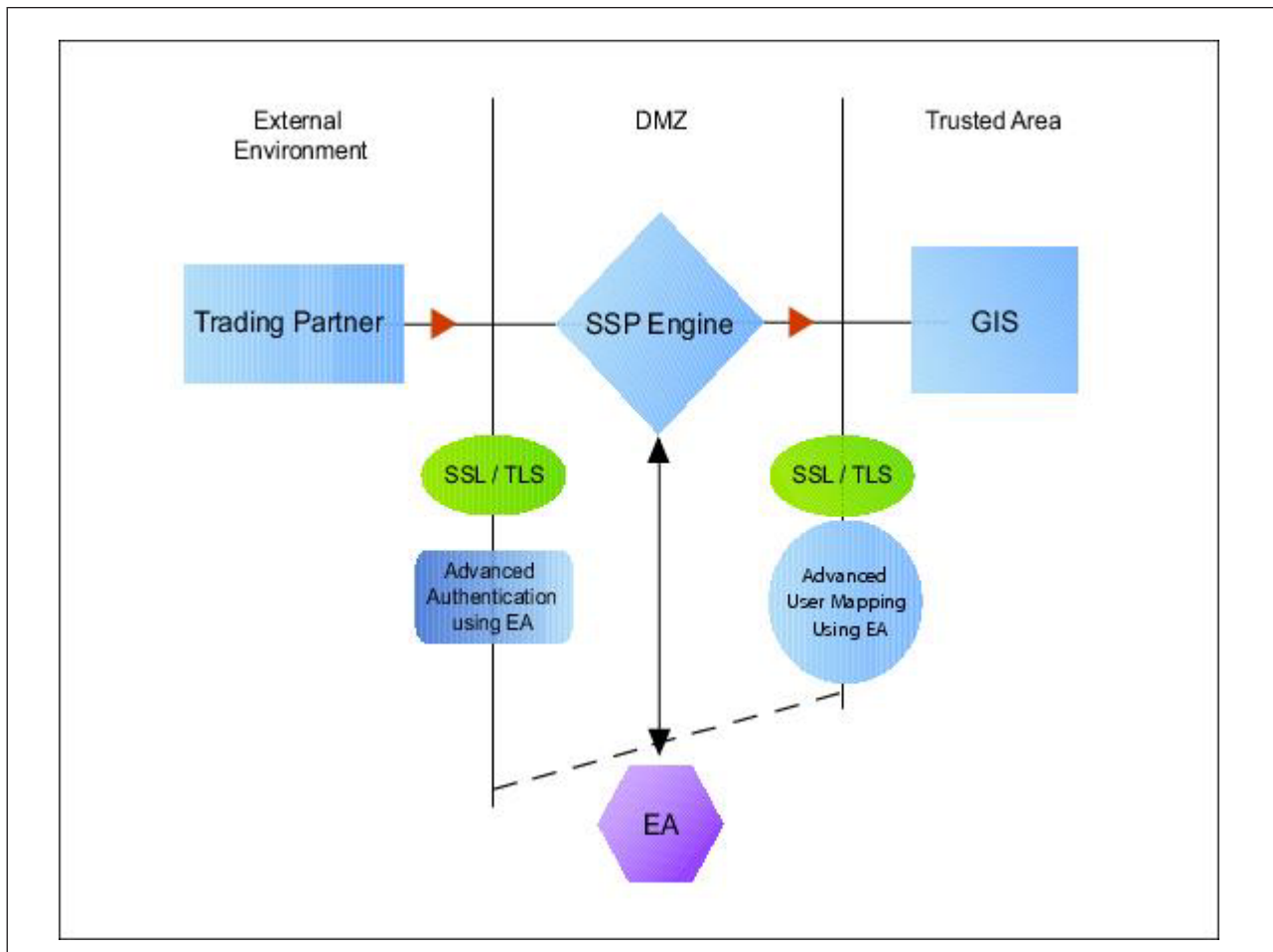
To configure validation for the outbound connection using credentials stored in the netmap:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Netmaps** tree and select the FTP netmap to modify.
3. Click the **Outbound Nodes** tab.
4. Select the outbound node to modify and click **Edit**.
5. Click the **Advanced** tab.
6. Type values in the following fields for connecting to the Sterling B2B Integrator server:
 - **User ID**
 - **Password**
7. Click **Save**.
8. Expand the **Policies** tree and select the policy to modify.
9. On the FTP Policy Configuration panel, click the **Advanced** tab.
10. From the **User Mapping: Internal User ID** list, select **From Netmap**.
11. Click **Save**.
12. Test the configuration to ensure that this feature is working.

Chapter 20. Strengthen Authentication of an FTP Node Using Sterling External Authentication Server

Use Sterling External Authentication Server to provide a more advanced method of securing the inbound or the outbound connection, such as, authenticating certificate information or user credentials presented by the inbound node, or performing user ID and password mapping for the internal credentials. The following illustrates the security features enabled in this scenario:



Chapter 21. Authenticate the Inbound FTP Node Using Sterling External Authentication Server

About this task

To authenticate certificate information or user information about the inbound node against information stored in an external database, you must configure Sterling External Authentication Server. After you configure Sterling External Authentication Server to enable certificate validation or user authentication, use this procedure to configure Sterling Secure Proxy to use the authentication method you defined in Sterling External Authentication Server.

Before you configure Sterling Secure Proxy to use Sterling External Authentication Server to authenticate an inbound node authentication, obtain the name of the Sterling External Authentication Server definition.

In addition, ensure that the following procedures have been performed:

- The policy associated with the inbound node has enabled client authentication.
- The public keys for Sterling Secure Proxy have been sent to the Sterling External Authentication Server and imported into the Sterling External Authentication Server key store.
- The Sterling External Authentication Server server connection has been configured in Sterling Secure Proxy.

To configure authentication of an inbound node using Sterling External Authentication Server:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Policies** tree and select a policy to modify.
3. On the **Policy Configuration** panel, click the **Advanced** tab.
4. Configure one or more of the following options:
 - To validate the certificate presented by the inbound node against information defined in Sterling External Authentication Server, enable **Certificate Authentication - External Authentication Certificate Validation** and identify the name of the profile you defined in Sterling External Authentication Server in the **Certificate Authentication - External Authentication Profile** field.
 - To validate the user, enable **Through External Authentication** and identify the name of the profile defined in Sterling External Authentication Server in the **External Authentication Profile** field.
5. Click **Save**.

Results

You can now associate this policy with the inbound node on which you want to perform user authentication using information stored in an LDAP server.

Chapter 22. Connect to Outbound FTP Server Using Sterling External Authentication Server Worksheet

Use this worksheet to configure a stronger outbound connection using information from an LDAP database.

Configuration Manager Field	Feature	Value
User Certification Through External Authentication	Will you validate user information?	Yes
External Authentication Profile	If yes, identify the Sterling External Authentication Server user validation definition	
Destination Service Name	Identify the destination server that can be accessed by the outbound node, when using Sterling External Authentication Server to map a user ID and password. Valid values are 1-255 alphanumeric characters and certain special characters. The following characters are not allowed: ! @ # % ^ * () + ? , < > { } [] ; " ' & #	

Chapter 23. Connect to the Outbound Node Using Information Stored in Sterling External Authentication Server

About this task

If you store user credentials in an external database accessed by Sterling External Authentication Server, use this procedure to configure Sterling Secure Proxy to use these credentials to connect to the secure outbound server.

Before you configure this option:

- Configure a user validation definition in Sterling External Authentication Server.
- Obtain the name of the Sterling External Authentication Server definition.
- Configure the Sterling External Authentication Server to allow connections from Sterling Secure Proxy.
- Ensure that the policy associated with the inbound node has enabled client authentication.
- Ensure that the public keys for Sterling Secure Proxy have been sent to the Sterling External Authentication Server and imported into the Sterling External Authentication Server key store.

To configure the use of credentials from Sterling External Authentication Server:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Policies** tree and select a policy to modify.
3. On the **Policy Configuration** panel, click the **Advanced** tab.
4. Enable the **User Authentication Through External Authentication** option.
5. Type the name of the definition you defined in Sterling External Authentication Server in the **External Authentication Profile** field.
6. Deselect the **Local User Store** option.
7. From the **Internal User ID field**, select **From External Authentication**.
8. Click **Save**.
9. Expand the **Netmaps** tree and click the HTTP netmap to modify.
10. On the HTTP Netmap panel, click the **Outbound Nodes** tab.
11. Select the node to edit and click **Edit**.
12. Click the **Advanced** tab.
13. Identify the destination service name to use to connect the outbound node when using Sterling External Authentication Server in the **Destination Service Name** field.
14. Click **OK** and click **Save**.

Chapter 24. Test the Inbound and Outbound FTP Connections

About this task

To verify that the engine can receive and initiate communication sessions, you have to establish a connection between an FTP client and the engine, initiate a session from the engine to the Sterling B2B Integrator server in the trusted zone, and review the Sterling Secure Proxy audit log for the results.

Note: Configuration files must be available at the engine for communication sessions to be established.

This procedure enables you to verify that the engine can:

- Establish an FTP session initiated by a trading partner using an FTP client
- Initiate an outbound session to an Sterling B2B Integrator server on behalf of the FTP client connection

Sample Inbound Node Log

```
11 Sep 2010 11:38:28,914 [ProxyNearScheduler-Thread-2]
INFO sys.SESSION_NODE.HTTP_Netmap_Any - protocol=http Sterling IntegratorD=1
SNAME=user.company.com SIP=10.20.200.100 SPORT=40134 Sterling Secure Proxy104I Session:
1 - Session Proceeding after Node match: Any11 Sep 2010 11:38:31,557
[ProxyFarScheduler-Thread-4] INFO sys.SESSION_NODE.HTTP_Netmap_Any
- protocol=http SID=1 SNAME=user.company.com SIP=10.20.200.100 SPORT=40134
DNAME=lunar.company.com DIP=10.20.246.42 DPORT=10054 SUID=admin
DUID=admin Sterling Secure Proxy102I Session: 1 - Control:ServerAgent Connection closed
(CloseCode.EOF): Elapsed Time: 2.13 (s): Bytes Received: 194 [at:
7.286384976525821E-4 MBPS]Bytes Sent: 20480595 [at: 76.92242253521127
MBPS]
```

Sample Outbound Node Log

```
11
Sep 2010 11:38:28,914 [ProxyNearScheduler-Thread-2] INFO sys.SESSION_NODE.HTTP_Netmap_Any
- protocol=http SID=1 SNAME=user.company.com SIP=10.20.246.121 SPORT=40134
SSP104I Session: 1 - Session Proceeding after Node match: Any11
Sep 2010 11:38:31,557 [ProxyFarScheduler-Thread-4] INFO sys.SESSION_NODE.HTTP_Netmap_Any
- protocol=http SID=1 SNAME=user.company.com SIP=10.20.200.100 SPORT=40134
DNAME=lunar.csg.stercomm.com DIP=10.20.200.40 DPORT=10054 SUID=admin
DUID=admin Sterling Secure Proxy102I Session: 1 - Control:ServerAgent Connection closed
(CloseCode.EOF): Elapsed Time: 2.13 (s): Bytes Received: 194 [at:
7.286384976525821E-4 MBPS]Bytes Sent: 20480595 [at: 76.92242253521127
MBPS]
```

To verify the communications sessions:

Procedure

1. Make sure the engine is running.
2. Initiate an FTP client session to the Sterling B2B Integrator server in your trusted zone.
3. View the Inbound Node Log and the Outbound Node Log.
4. Confirm that the data transfer was successful, as illustrated in the sample log below: If your session was unsuccessful, review the log information to determine the likely cause of the failure and the corrective action to take.

Chapter 25. Route an Outbound FTP Connection to Alternate Sterling B2B Integrator Servers

About this task

When you configured the adapter, you identified the Sterling B2B Integrator server to connect to by selecting one of the outbound node connections defined in the netmap. For each outbound node definition, you can identify up to three alternate outbound nodes to connect to if the primary Sterling B2B Integrator server is not available.

Two methods of configuring alternate Sterling B2B Integrator server routing are available.

- Select an Sterling B2B Integrator server from the drop-down list. Using this method, you first configure an outbound node definition in the netmap for each alternate Sterling B2B Integrator server you want to use. Each connection uses the security and Sterling External Authentication Server settings defined in the outbound node definition.
- Select IP address/port from the drop-down list and enter values for the IP address and port. If you use this method, you do not have to define the alternate outbound nodes in the netmap, and each alternate connection uses the security and Sterling External Authentication Server settings defined in the primary node definition.

If you configure alternate Sterling B2B Integrator server definitions in the outbound node definition, when a connection to the primary outbound node is unsuccessful Sterling Secure Proxy tries to connect to the alternate node you defined as Node 1. If the connection to the first alternate node is unsuccessful, Sterling Secure Proxy tries to connect to the second alternate node, Node 2. If this connection is unsuccessful, Sterling Secure Proxy tries to connect to the third alternate, Node 3. If the connection to this node is unsuccessful, the inbound connection fails.

To configure alternate outbound connections:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Netmaps** tree and select a netmap to modify.
3. Click the **Outbound Node** tab and select the node to modify.
4. Click the **Advanced** tab.
5. Do one of the following:
 - To identify an alternate node that is defined in the netmap and use the security settings defined in the alternate node definition, select the outbound node name from the drop-down list.
 - To configure an alternate node that is not in the netmap and use the security settings defined in the primary node definition, select Address/Port in the Alternate Destinations Node field and provide the IP address and port number for the alternate outbound node.
6. Click **OK**.
7. Click **Save**.

Chapter 26. Define a Passive Data Outbound Port Range for an FTP Reverse Proxy Adapter

About this task

Two modes can be used to open the FTP data channel: active mode and passive mode. The mode used on the inbound connection is determined by the client. Sterling Secure Proxy always uses passive mode for the outbound connection.

In active mode, the inbound FTP node sends a port command identifying the data channel listen port on which Sterling Secure Proxy needs to connect. You identify the port numbers to use for an active data connection in the Active Data Outbound Port Range field.

In passive mode, the FTP client sends a PASV command and Sterling Secure Proxy starts a listener to receive the data connections from the client. You identify a port number range to use to start the listener that receives connections.

To define a passive data outbound port range:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the Adapters tree and select the adapter to modify.
3. Click the **Advanced** tab.
4. Type a value to use for the passive data outbound port range in the **Passive Data Listening Port Range** field.
5. Click **Save**.

Chapter 27. Define a Passive NAT Address for an FTP Reverse Proxy Adapter

About this task

When a PASV command is sent to Sterling Secure Proxy from an inbound FTP client, the host and port number to which the inbound FTP client needs to connect for the data channel is returned. When Sterling Secure Proxy is behind a firewall, the host address of Sterling Secure Proxy is not visible to the inbound FTP client. To ensure that the client can obtain this information, define the passive network address translation (NAT) address.

Define this value if the client cannot directly connect to the proxy, such as when using a static NAT.

If you are using a remote external perimeter server with the FTP reverse proxy adapter and the perimeter server is also behind a firewall using static network address translation, identify the name or IP address of the computer running the external perimeter server.

To define a passive NAT address:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Adapters** tree and select the adapter to modify.
3. Click the **Advanced** tab.
4. Type a value to use for the passive NAT address in the **Passive NAT Address** field.
5. Click **Save**.

Chapter 28. Define an Active Data Outbound Port Range for an FTP Reverse Proxy Adapter

About this task

Two modes are available to open the FTP data channel: active mode and passive mode. The mode used on the inbound connection is determined by the client. Sterling Secure Proxy always uses passive mode for the outbound connection.

In active mode, the inbound FTP node sends a port command identifying the data channel listen port on which the proxy needs to connect. You identify the port numbers to use for an active data connection in the Active Data Outbound Port Range field.

In passive mode, the FTP client sends a PASV command to Sterling Secure Proxy and Sterling Secure Proxy starts a listener to receive the data connections from the client. You identify a port number range that can be used to start the listener to receive connections.

To define an active data outbound port range for an FTP reverse proxy adapter:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Adapters** tree and select the adapter to modify.
3. Click the **Advanced** tab.
4. Type a value to use for the active data outbound port range in the **Active Data Outbound Port Range** field.
5. Click **Save**.

Chapter 29. Use IP Address from a PASV Response For Outbound Data Connections

About this task

As a security measure, Sterling Secure Proxy ignores PASV response and uses the same IP address as the initial control channel for all data channel connections. If virtual IP address (VIPI) is used by the outbound server, the data connections may be a different IP address than the original connection. Complete this procedure to allow data channel connections to use different IP addresses.

To allow Sterling Secure Proxy to use an IP address from a PASV response:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Adapters** tree and select the adapter to modify.
3. Click the **Advanced** tab.
4. Enable the field **Use IP from PASV Response**.
5. 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](http://www.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