Sterling Secure Proxy

PeSIT Proxy Scenarios

Version 3.4

Sterling Secure Proxy

PeSIT Proxy Scenarios

Version 3.4

Note

Before using this information and the product it supports, read the information in "Notices" on page 69.

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. Sterling Secure Proxy and PeSIT Overview

Sterling Secure Proxy acts as an application proxy between IBM® Sterling Connect:Express and PeSIT nodes. It provides a high level of data protection between external PeSIT connections and your internal network. Define an inbound node definition for each trading partner connection from outside the company and outbound node definition for every company server to which Sterling Secure Proxy will connect.

Sterling Secure Proxy provides reverse proxy services for Sterling Connect:Express servers when the trading partners initiate sessions to Sterling Connect:Express servers in the trusted zone. Sterling Secure Proxy provides forward proxy services for Sterling Connect:Express servers when the node in the trusted zone initiates a session to a server at a remote trading partner.

Sterling Secure Proxy provides these services for Sterling Connect:Express and PeSIT nodes in a manner similar to the way it provides these services for other protocols.

The PeSIT configuration scenarios describe how to configure PeSIT protocol connections to and from the Sterling Secure Proxy engine using Configuration Manager.

Supported PeSIT Software

The following software is supported for use with the Sterling Secure Proxy PeSIT Proxy Adapter:

- Sterling Connect:Express for z/OS version 4.2.2 or later
- Sterling Connect:Express for UNIX version 1.4.4 or later
- Sterling Connect:Express for Microsoft Windows version 3.0.5 or later

Organization of the PeSIT Configuration Scenarios

The first scenario instructs you how to do a basic setup. Each successive scenario adds an additional security feature to the basic configuration. After you go through each scenario, test the connection to ensure that it is correctly configured. You determine your security needs and configure the security features applicable to your environment.

The scenarios include the following:

- Create a basic PeSIT configuration
- Add SSL/TLS support
- Configure PNODE-based routing
- Add local Logon ID authentication
- Provide outbound credentials using the netmap

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

- Authenticate an inbound certificate or user using Sterling External Authentication Server
- Configure logon ID mapping to the SNODE using Sterling External Authentication Server
- Configure certificate-based routing

Additional procedures are provided to instruct you how to configure the following features:

- Define alternate nodes for failover support
- Enable action based on protocol errors
- Block a PeSIT command from a PNODE

Chapter 2. Complete Scenario Worksheets

Before you perform each PeSIT configuration, gather the information on the provided worksheet. You use this information as you configure each feature. Complete worksheets as follows:

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

Chapter 3. Complete and Test Configuration Scenarios

About this task

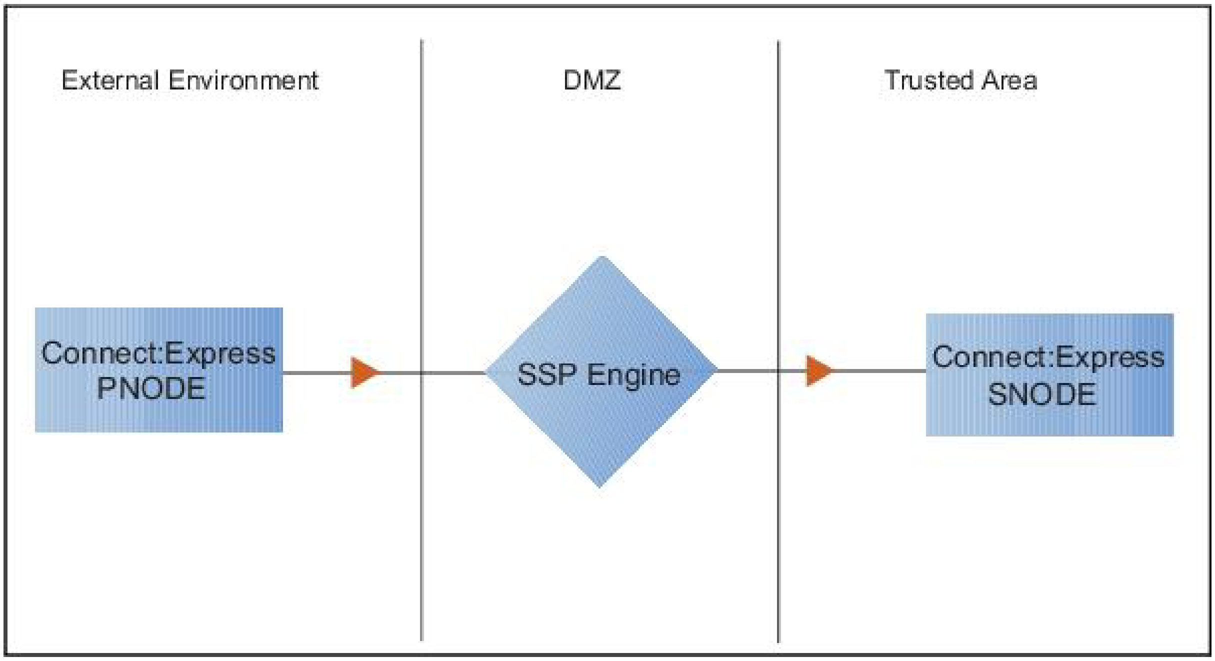
Work through the sequence of PeSIT configuration scenarios in the order in which they are presented to add security features. Be sure to test each feature before you add the next one to the configuration. Before you move Sterling Secure Proxy into production, ensure that you have configured and tested all security features you need 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 PeSIT Configuration

This scenario contains all the information and tools you need to configure Sterling Secure Proxy to establish a basic connection between PeSIT servers. Using default values, the PNODE presents a Logon ID to connect to the SNODE without Sterling External Authentication Server. As a result, no authentication occurs in Sterling Secure Proxy and the logon ID presented by the PNODE is used to connect to the SNODE. This scenario assumes that all nodes are Sterling Connect:Express nodes.

The basic configuration uses standard routing to route connections to the node you define in the adapter. You are instructed on how to configure PNODE routing, mixed routing, and certificate-based routing in later scenarios.



Before you configure a PeSIT connection, make sure that an engine has been configured. Refer to *Install or Upgrade Sterling Secure Proxy on UNIX or Linux* or *Install or Upgrade Sterling Secure Proxy on Microsoft Windows* for instructions.

After you configure Sterling Secure Proxy, validate the configuration by initiating a PeSIT connection from the PNODE. For more information on testing the configuration, see *Test the PeSIT Connections*.

Complete the following tasks to define a basic PeSIT configuration:

- Create a policy
- Define PeSIT nodes in a netmap
- Define a PeSIT adapter

Basic PeSIT Configuration Worksheet

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

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

Configuration Manager Field	Feature	Value
Policy Name	Name of policy	

Create a netmap that contains connection information for the nodes connecting to and from Sterling Secure Proxy. For each node, associate a policy with the node.

Configuration Manager Field	Feature	Value
Netmap Name	Netmap name	
PeSIT Node Definition		
Node Name	Name to assign to the PeSIT node definition	
PeSIT Server Address	Host name or IP address of the PeSIT server	
PeSIT Port	Listening port number of the PeSIT server	
Policy	Name of policy you create (Select from a pull-down list.)	
Node Name	Name to assign to the PeSIT node definition	
PeSIT Server Address	Host name or IP address of the PeSIT server	
PeSIT Port	Listening port number of the PeSIT server	
Policy	Name of policy you create (Select from a pull-down list.)	
Node Name	Name to assign to the PeSIT node definition	
PeSIT Server Address	Host name or IP address of the PeSIT server	
PeSIT Port	Listening port number of the PeSIT server	
Policy	Name of policy you create (Select from a pull-down list.)	

Create a PeSIT adapter that defines information necessary to establish PeSIT connections to and from Sterling Secure Proxy. When configuring the adapter, select the basic netmap and the PeSIT server where connections are routed and defined in the netmap definition.

Configuration Manager Field	Feature	Value
Name	Adapter name	
Listen Port	Listen port to use for inbound connections	
Netmap	Netmap to associate with the adapter	
SNODE Netmap Entry	Name of PeSIT node where the connection is routed	
Engine	Engine to run the PeSIT adapter on	

Chapter 5. Create a Basic PeSIT Policy

About this task

The policy defines how you impose controls to authenticate a PeSIT PNODE trying to communicate with a PeSIT SNODE over the public Internet. The basic policy does not enforce any controls over the defined node. You add security controls when you define more advanced security settings.

To define a basic policy:

Procedure

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

Chapter 6. Create a PeSIT Netmap

About this task

You define connection information for every PeSIT node that communicates using Sterling Secure Proxy. 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 PeSIT nodes:

Procedure

1. Select **Configuration** from the menu bar.
2. Click **Actions** > **New Netmap** > **PeSIT Netmap**.
3. Type a **Netmap Name**.
4. To define a PeSIT node definition, click **New**.
5. Specify the following values:
   - **Node Name**
   - **PeSIT Server Address or hostname**
   - **PeSIT Server Port (listening port)**
   - **Policy**
6. Click **OK**.
7. Repeat steps 4 through 6 for each node you want to define. Define at least one PNODE and at least one SNODE in order to establish a connection between two PeSIT nodes.
8. Click **Save**.

Chapter 7. Define the PeSIT Adapter Used for the Connection

About this task

A PeSIT adapter definition specifies system-level communications information necessary for PeSIT connections through Sterling Secure Proxy.

Before you begin this procedure, create a netmap and an engine to associate with the adapter.

To define a PeSIT adapter:

Procedure

1. Select **Configuration** from the menu bar.
2. Click **Actions** > **New Adapter** > **PeSIT Proxy**.
3. Specify values for the following:
   - **Name**
   - **Listen Port**
   - **Netmap**
   - **SNODE Netmap Entry**
   - **Engine**
4. Click **Save**.

Chapter 8. What You Defined with the Basic PeSIT Configuration Scenario

Creating connections between PeSIT nodes when routing them through Sterling Secure Proxy requires that you organize information about the PeSIT nodes in a policy, a netmap, and an adapter definition. You created these items when you defined the basic PeSIT configuration. The next step is to test the configuration to ensure that the connections work. Before you test the configuration, be sure that:

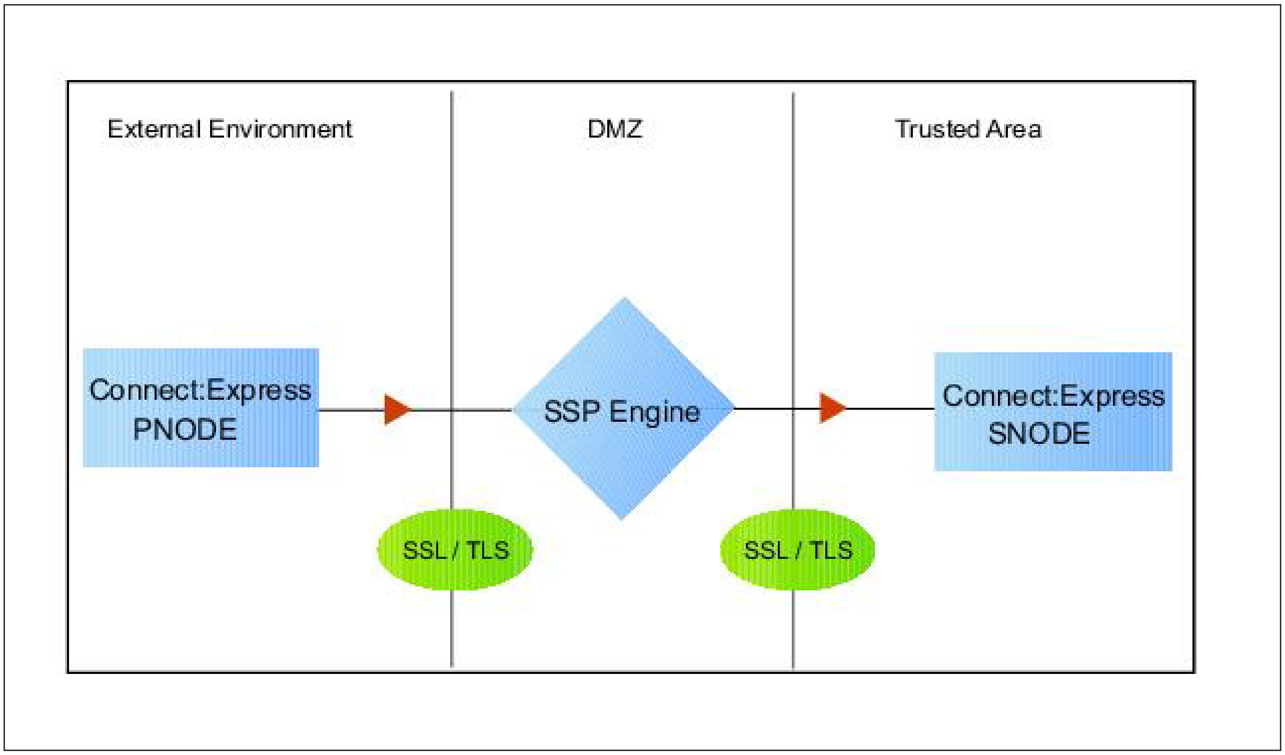
- The Sterling Connect:Express SNODE server has a definition in its partner's directory for the Sterling Connect:Express or PeSIT PNODE. The definition must use the IP address of the Sterling Secure Proxy server. The local name must be the SNODE name.
- The Sterling Connect:Express PNODE server has a definition in its partner's directory for the Sterling Connect:Express or PeSIT SNODE, using the IP address and port of the Sterling Secure Proxy server. The local name must be the PNODE name.

Refer to *Test the PeSIT Connections*for information about testing the PeSIT proxy configuration 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 9. Add SSL/TLS Support

This scenario builds on the basic PeSIT configuration by enabling security for the nodes you defined in the netmap.



Adding SSL/TLS support to the netmap for the nodes involves selecting the following options for the connections:

- SSL or TLS Protocol
- Cipher suites
- Certificate stores and certificates

Add SSL/TLS support to the PNODE and the SNODE definitions. Set up SSL/TLS parameter files at both the SNODE and the PNODE servers. Obtain certificates for both sessions and check them into the certificate store. Then, test the connection.

Note: This procedure assumes you have checked in your certificates. Refer to *Manage Certificates for SSL/TLS Transactions with Trading Partners* for more information.

SSL/TLS Support Worksheet

Before you add SSL/TLS support to the connection information you created in the basic PeSIT 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 require that the certificate common name be validated in a certificate presented, enable this option and identify the common name value to check. Select the key/system certificate to use to validate the connection.

Configuration Manager	**Feature**	**Value**
Node Name	Name of the node to add security to, from the nodes you've already defined.	
Use SSL	Enable this option to enable security checking	Enabled
Verify Common Name	Enable this option to enable common name checking. This is optional.	Enabled/Disabled
Certificate Common Name	Value of common name in certificate presented, if Common Name Checking is enabled.	
Security Setting	Security protocol to use. Options include SSL or TLS.	
Enable Client Authentication	Do you want to require the inbound connection to present its certificate for SSL or TLS client authentication?	
Trust Store	Name of the store for the CA certificate or trusted root certificate	
CA Certificates/Trusted Root	Name of CA certificate/trusted root	
Key Store	Name of the store for the key or system certificate is stored	
Key/System Certificate	Name of the Sterling Secure Proxy system certificate presented to the PeSIT server	
Available Cipher Suites	Select the ciphers to enable by moving them from the Available Cipher Suites to the Selected Cipher Suites field	

Chapter 10. Secure the PeSIT Connection Using the SSL or TLS Protocol

About this task

The first step to strengthen security is to secure the communications channel. This procedure describes how to enable the SSL or TLS protocol for the PeSIT connections to and from Sterling Secure Proxy in a netmap you created in the basic configuration. To require that Sterling Secure Proxy perform common name checking, enable this option and identify the common name in the configuration.

Before you can configure this option, you must obtain the necessary certificates and place them in the Sterling Secure Proxy Cert Store. Refer to *Manage Certificates for SSL/TLS Transactions with Trading Partners* for instructions.

To enable the SSL or TLS protocol:

Procedure

1. Select Configuration from the menu bar.
2. Expand the **Netmaps** tree and select a netmap to modify.
3. Select a node to modify, and click **Edit**.
4. Click the **Security** tab, and then click **Use SSL to enable security**.
5. To enable common name checking:
   a. Click **Verify Common Name**.
   b. Type the certificate common name in the Certificate Common Name field.
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. If only one certificate is displayed in the field, it is not selected until you highlight it.
8. Click **OK**.
9. Click **Save**.
10. Establish a session initiated by a Sterling Connect:Express PNODE to test the configuration.

Chapter 11. Variation on the Add SSL/TLS Support Configuration

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 configuration. After testing the SSL/TLS configuration, you can configure the environment to allow the inbound and outbound sessions to use different levels of encryption.

Allow Different Levels of Encryption for the Inbound and Outbound Node

About this task

In a PeSIT environment where Sterling Secure Proxy is not being used, one session is established between an SNODE and a PNODE. In the Sterling Secure Proxy environment, a session break is created; therefore, two sessions are established: one between the PNODE and Sterling Secure Proxy and another between Sterling Secure Proxy and the SNODE. To use the same protocol on both sessions, use the default settings.

Complete this procedure to define one protocol for the inbound node and a different protocol for the outbound node. This function is useful when you want to secure the inbound connection but allow a nonsecure session between Sterling Secure Proxy and the outbound node.

To enable different levels of encryption for the inbound and the outbound connection:

Procedure

1. Select **Configuration** from the menu bar.
2. Expand the **Adapter** tree, and select the adapter you want to modify.
3. Click the **Advanced** tab.
4. Enable the **Inbound and outbound sessions can have different levels of encryption** option.
5. Click **Save**.

Chapter 12. Configure PNODE-Based Routing Overview

The basic configuration uses standard routing to determine where a connection is routed. If you configure standard routing, all sessions through an adapter are routed to the same connection. To allow a PNODE to determine what SNODE it connects to, configure PNODE-based routing. For PNODE-based routing, you must configure a node definition in the netmap for the PNODE and for all the SNODEs you will route to.

PNODE-based Routing Worksheet

This scenario builds on the basic PeSIT configuration by enabling PNODE-based routing. Before you add PNODE-based routing to the connection information you created in the basic PeSIT configuration scenario, gather the information on the PNODE-based Routing Worksheet. You use this information as you configure PNODE-based routing.

Make sure that you have a node definition for the PNODE and for every node where the connection is routed in the netmap you select.

Configuration Manager Field	Feature	Value
Name	Adapter name	
Routing Type	Routing type to use for this connection	PNODE-specified

Chapter 13. Configure PNODE-based Routing

About this task

To configure a PeSIT adapter to use PNODE-based routing:

Procedure

1. Select **Configuration** from the menu bar.
2. Expand the **Adapter** tree and select the adapter you want to modify.
3. Select **PNODE-specified** in the **Routing Type** field.
4. Click **Save**.

Chapter 14. Configure Mixed Routing

Mixed routing allows a PNODE to determine what SNODE it connects to. If the PNODE does not identify what SNODE to connect to, mixed routing then routes to the SNODE identified in the Sterling Secure Proxy configuration. Before PNODE-based routing can be implemented, you must configure a node definition in the netmap for the PNODE and the SNODE.

Mixed Routing Worksheet

This scenario builds on the basic PeSIT configuration by enabling PNODE-based routing. Before you add PNODE-based routing to the connection information you created in the basic PeSIT configuration scenario, gather the information on the Mixed Routing Worksheet. You use this information as you configure PNODE-based routing.

Make sure that you have a node definition for the PNODE and for the node where the connection is routed in the netmap you select.

Configuration Manager Field	Feature	Value
Name	Adapter name	
Routing Type	Routing type to use for this connection	PNODE-specified and then Standard
SNODE Netmap Entry	SNODE to route connections to	

Chapter 15. Configure PNODE Specified and Then Standard (Mixed) Routing

About this task

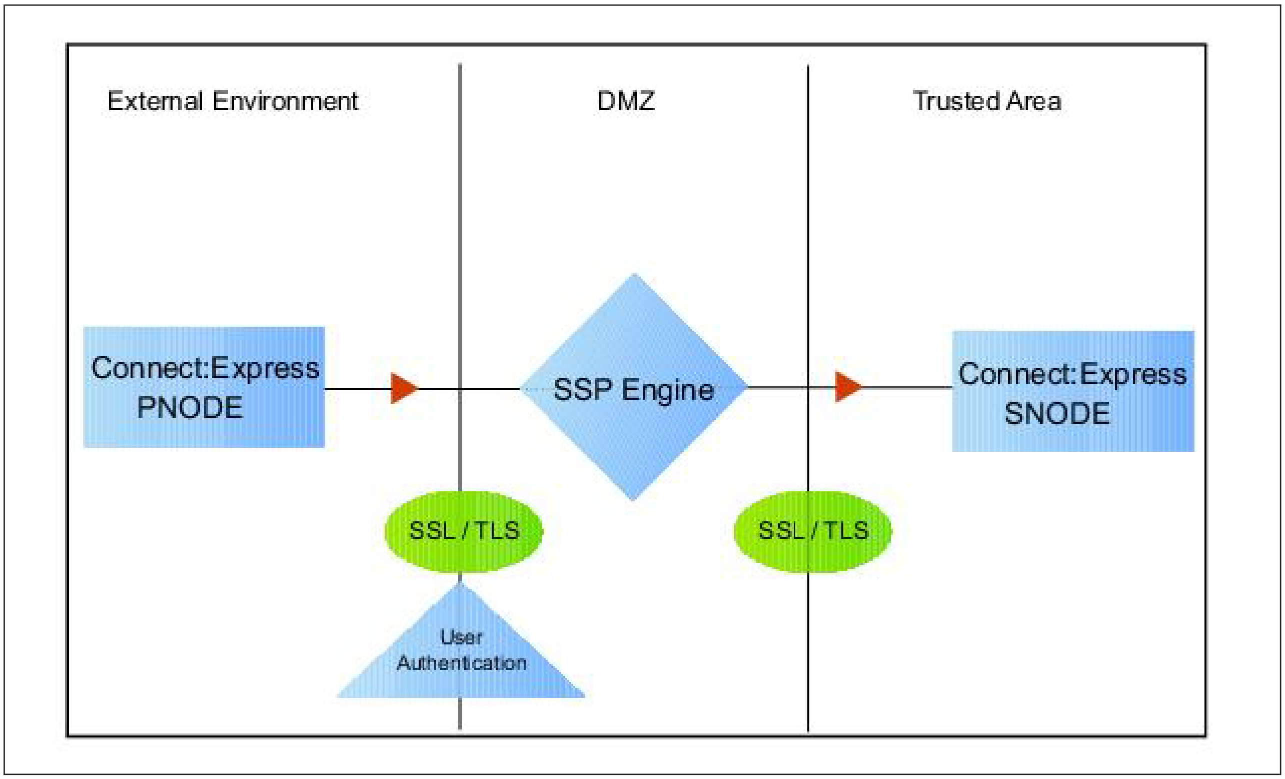
To configure a PeSIT adapter to use PNODE specified and then standard (mixed) routing:

Procedure

1. Select **Configuration** from the menu bar.
2. Expand the **Adapter** tree and select the adapter you want to modify.
3. Select **PNODE-Specified**, then **Standard (mixed)** in the Routing Type field.
4. Select the **SNODE** to route connections to in the SNODE Netmap Entry field.
5. Click **Save**.

Chapter 16. Add Local User Authentication to a PeSIT Connection

This scenario builds on the basic PeSIT configuration by adding local user authentication to the PNODE connection using information defined in the local user store. The logon ID and password presented by the PNODE are authenticated against 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.



Adding logon ID authentication to the PNODE connection defined in the basic PeSIT configuration involves enabling logon ID authentication and specifying information about the PNODE.

After you configure local logon ID authentication, validate the configuration by establishing a session initiated by a Sterling Connect:Express PNODE.

PeSIT PNODE Connection (Local LogonID Authentication) Worksheet

Before you add local logonID authentication to the PNODE connection you created in the basic PeSIT configuration, gather the information on the PeSIT PNODE Connection (Local LogonID Authentication) Worksheet. Use this information as you configure logonID authentication for the PNODE connection.

In this scenario, you edit the policy you created in the PeSIT basic configuration scenario and enable logonID authentication. You also add a logonID and password for the PeSIT PNODE to the default user store.

Configuration Manager Field	Feature	Value
Policy Name	Name of policy associated with the inbound node	
LogonID 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 Confirm Password	The password value to use to validate the inbound connection	

Chapter 17. Add User Authentication to the PeSIT Inbound Connection

About this task

You can strengthen the security of PeSIT PNODE connections by enabling local logonID authentication. This procedure describes how to configure local logonID authentication.

To add local logonID authentication for a PNODE connection:

Procedure

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

Chapter 18. Add Credentials to the Local User Store

About this task

If you enable logonID authentication through the local user store, you also add logonID information to the local user store that is validated by Sterling Secure Proxy during a PeSIT client connection.

Before you begin this procedure:

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

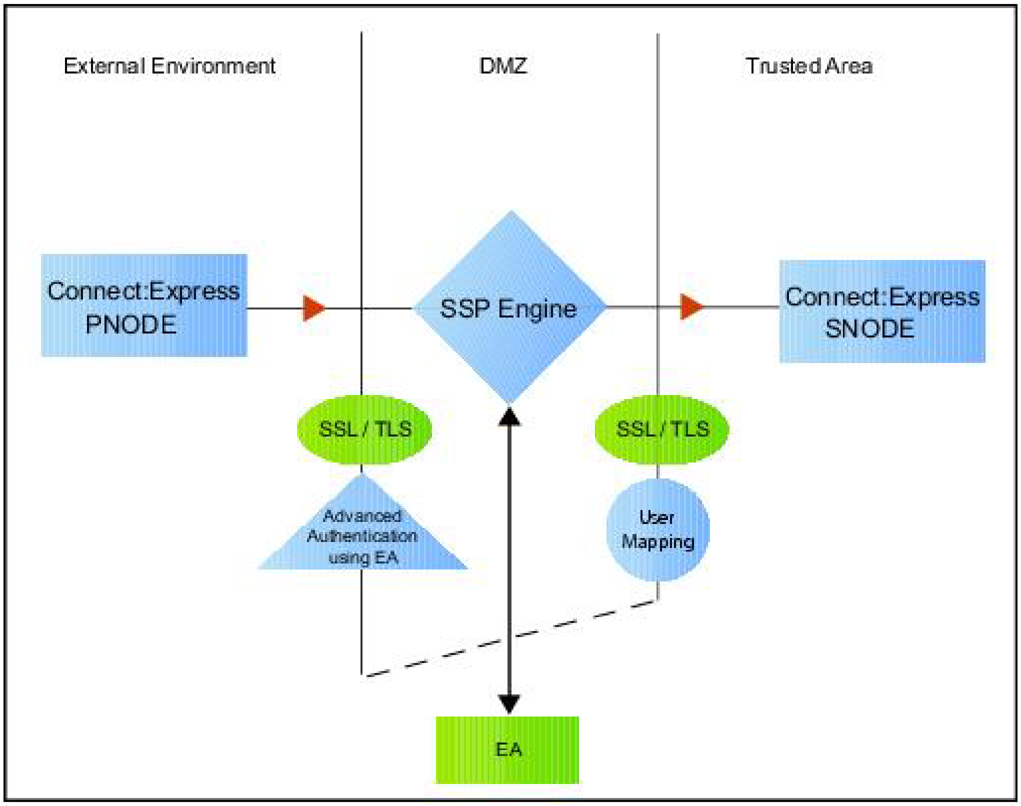
To add user information to the local user store:

Procedure

1. Select **Credentials** from the menu bar.
2. Click **User Stores** to expand the list of user stores.
3. Select the default user store called **defUserStore**.
4. From the User Store Configuration panel, click **New**.
5. Specify values for the following:
   - **User Name**
   - **Password**
   - **Confirm Password**
6. Click **OK**.
7. Click **Save**.

Chapter 19. Strengthen LogonID Authentication Using Sterling External Authentication Server

This scenario builds on the basic PeSIT configuration by adding logonID authentication to the PNODE connection using information defined in Sterling External Authentication Server. To provide a more advanced method of securing a PeSIT connection, use Sterling External Authentication Server to authenticate certificate information or logonID credentials presented by the inbound node or to perform logonID and password mapping.



Authenticate an Inbound Certificate or LogonID Using Sterling External Authentication Server

You can authenticate an inbound connection against information stored in an LDAP database by configuring Sterling External Authentication Server to define how the connection is authenticated. The Sterling External Authentication Server definition determines the options that are enabled. Refer to the Sterling External Authentication Server documentation library for the functions that can be performed in Sterling External Authentication Server.

Authenticate a Certificate or LogonID Using Sterling External Authentication Server - Worksheet

Use the following worksheet to identify the information needed to authenticate a PeSIT connection using information in Sterling External Authentication Server. Update the policy you created in the basic PeSIT configuration for this scenario.

Configuration Manager Field	Information	Value
Certificate Authentication - External Authentication Certificate Validation	Will you validate the certificate presented by the PNODE?	(Yes or No)
Certificate Authentication - External Authentication Profile	If yes, provide the Sterling External Authentication Server certificate validation definition.	
User Authentication - Through Sterling External Authentication Server	Will you validate user information?	(Yes or No)
User Authentication - External Authentication Profile	If yes, provide the Sterling External Authentication Server user validation definition.	

Chapter 20. Authenticate a PeSIT Certificate or LogonID Using Sterling External Authentication Server

About this task

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

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

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

- The public keys for Sterling Secure Proxy have been sent to the Sterling External Authentication Server server and imported into the Sterling External Authentication Server keystore.
- The Sterling External Authentication Server server connection has been configured in Sterling Secure Proxy.

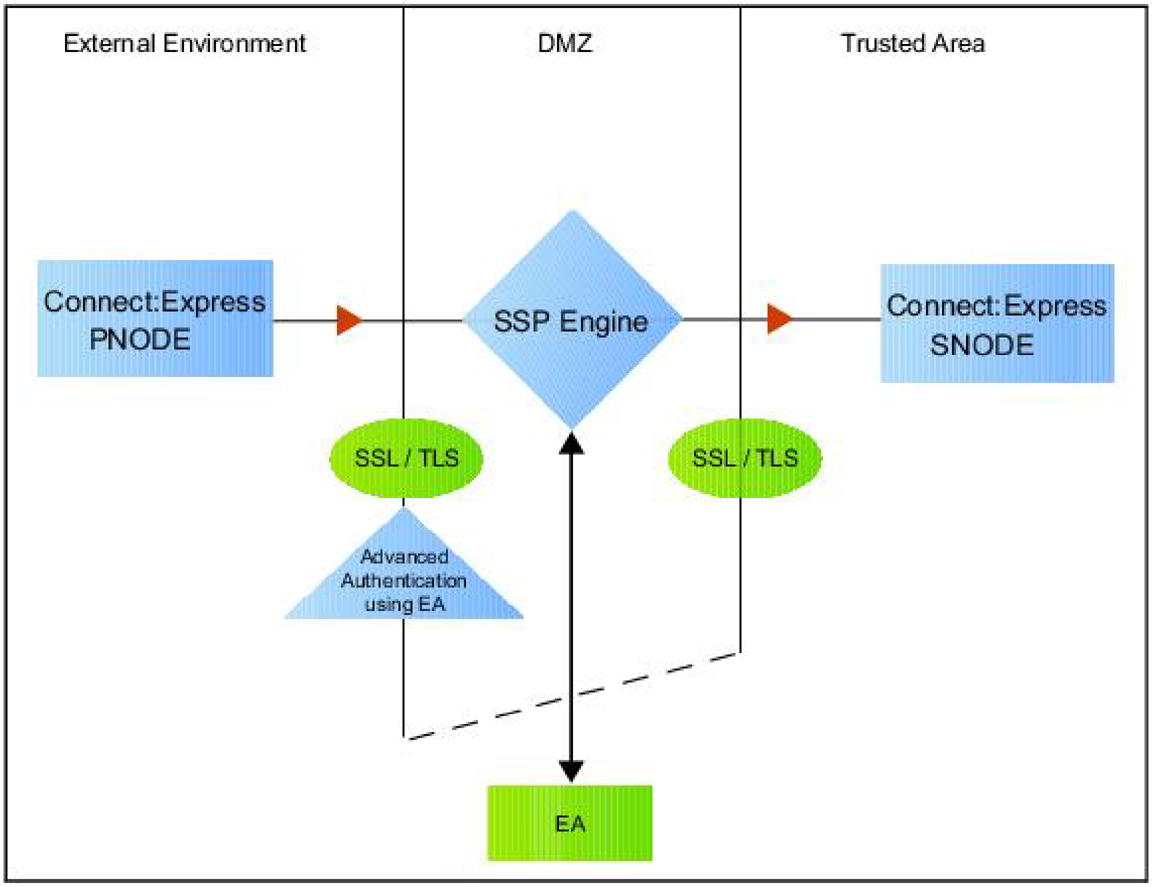
To configure authentication of a PeSIT node using Sterling External Authentication Server:

Procedure

1. Select **Configuration** from the menu bar.
2. Expand the **Policies** tree and click the 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 node against information defined in Sterling External Authentication Server, enable **Certificate Authentication - Sterling External Authentication Certificate Validation** and enter the name of the profile you defined in Sterling External Authentication Server in the Certificate Authentication - Sterling External Authentication Server Profile field.
   - To enable logonID authentication through Sterling External Authentication Server, enable **LogonID Authentication - Through External Authentication** and type the name of the definition you defined in Sterling External Authentication Server in the LogonID Authentication - Sterling External Authentication Server Profile field.
5. Deselect the **Through Local User Store** option.
6. Click **Save**. You can now associate this policy with a PeSIT node where you want to perform logonID authentication using information stored in an LDAP database.

Chapter 21. Strengthen the Connection to the SNODE With LogonID Mapping

This scenario builds on the basic PeSIT configuration by adding logonID mapping using information defined in Sterling External Authentication Server server. To provide a more advanced method of securing a PeSIT connection, use Sterling External Authentication Server to map a PNODE logonID and password to login credentials stored in Sterling External Authentication Server. The mapped login credentials are then used to connect to the SNODE.



Perform LogonID Mapping Using Sterling External Authentication Server - Worksheet

Use this worksheet to identify the logonID mapping method to enable for the SNODE connection with information in Sterling External Authentication Server:

Configuration Manager Field	Feature	Value
Replace LogonID with Userid mapped in External Authentication	The PNODE requires a LogonID to access the SNODE. The LogonID provided is replaced with a value defined in Sterling External Authentication Server.	Enabled
Destination Service Name	Name of the service. If no value is provided, the SNODE is used as the service name.	

Chapter 22. Perform LogonID Mapping Using Information Stored in Sterling External Authentication Server

About this task

If you store user credentials in an LDAP database, use this procedure to map a logonID and password to information stored in Sterling External Authentication Server.

Destination Service Name needs to be selected on the Advanced tab of the Netmap Node screen of the PNODE. If Destination Service Name is not provided, the SNODE name is used.

Before you configure this option:

- Configure a definition in Sterling External Authentication Server.
- Obtain the name of the Sterling External Authentication Server definition.
- Configure a connection between Sterling External Authentication Server and the engine.

To configure logonID mapping:

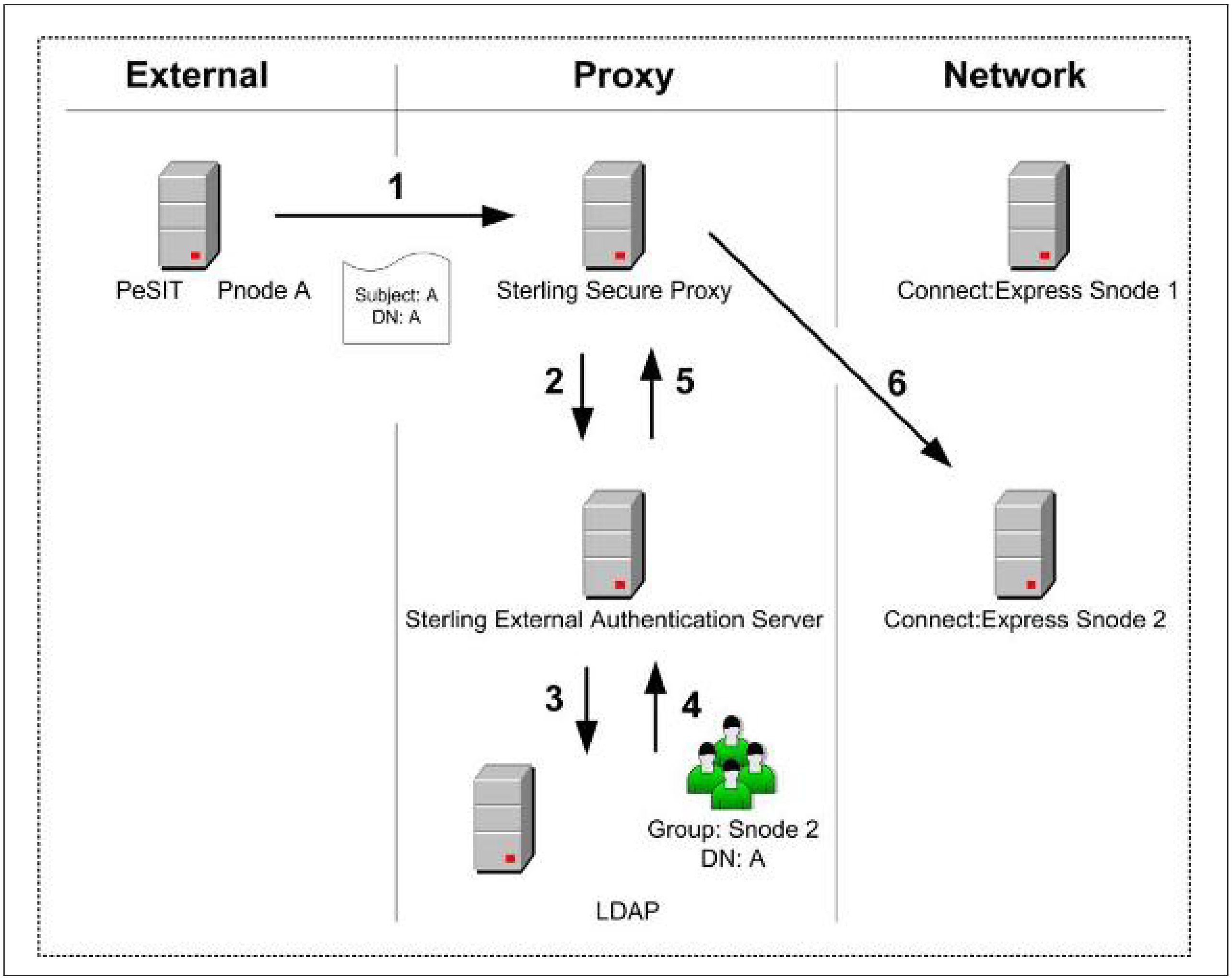
Procedure

1. Select **Configuration** from the menu bar.
2. Expand the **Policies** tree and click the policy to modify.
3. On the Policy Configuration panel, click the **Advanced** tab.
4. To enable logonID authentication through Sterling External Authentication Server, enable the **LogonID Authentication Through External Authentication** option and type the name of the definition you defined in Sterling External Authentication Server in the **External Authentication Profile** field.
5. Select **Replace LogonID with LogonID mapped in External Authentication**.
6. Click **Save**.
7. In the **Configuration** panel, expand the **Netmap** option and click the netmap to modify.
8. Select the PNODE to modify and click **Edit**.
9. Click the **Advanced** tab.
10. Type the name of the service in the **Destination Service Name** field. If no value is provided, the SNODE name is used as the service name.
11. Click **OK**.
12. Click **Save**.

Chapter 23. Configure Certificate-Based Routing

This scenario builds on the basic PeSIT configuration by configuring certificate-based routing. Certificate-based routing uses a routing name returned by Sterling External Authentication Server. It is associated with the subject distinguished name found in the PNODE certificate. Sterling Secure Proxy uses this routing name to determine the SNODE where the incoming Sterling Secure Proxy connection is routed. To perform certificate-based routing, modify an adapter you defined in the basic PeSIT configuration.

The following diagram illustrates the certificate-based routing function:



Summary of Certificate-Based Routing

Following are the steps performed during certificate-based routing:

1. The PNODE passes a certificate chain during an SSL/TLS session. This certificate includes several attributes, such as subject and distinguished name (DN).

2. Sterling Secure Proxy passes the certificate chain to Sterling External Authentication Server.
3. Using the configuration parameters in a certificate validation request, Sterling External Authentication Server attempts to match PNODE certificate attributes to the LDAP server and requests the associated routing value.
4. LDAP returns the routing value to Sterling External Authentication Server.
5. Sterling External Authentication Server passes the routing value to the Sterling Secure Proxy engine.
6. Sterling Secure Proxy routes the PNODE request to the SNODE using the routing value.

Chapter 24. Configure Certificate-Based Routing in Sterling Secure Proxy

About this task

Before you test certificate-based routing, you must create a certificate validation request in Sterling External Authentication Server that includes an attribute query definition called Routing Names. This attribute query definition is created to retrieve a routing name value using certificate attributes as search criteria. You must also configure a connection between Sterling Secure Proxy and Sterling External Authentication Server.

Refer to *Configure Sterling Secure Proxy for Sterling External Authentication Server* for instructions.

To configure certificate-based routing:

Procedure

1. Select **Configuration** from the menu bar.
2. Expand the **Adapters** tree and select the adapter you want to modify.
3. Select **Certificate-based** in the Routing Type field.
4. Click **Save**.
5. Click the **Netmap** navigation panel, expand the **Netmap** tree, and select the PeSIT adapter that contains the SNODE where the connections are routed.
6. Select the node to modify and click **Edit**.
7. Type the routing value to be returned from the LDAP server in the **Routing Name** field. The routing name must exactly match the routing value returned from the LDAP server. This routing name identifies the SNODE for routing the PNODE request.
8. Click **OK**.
9. Click **Save**.
10. Configure Sterling Secure Proxy to enable certificate authentication using Sterling External Authentication Server. Refer to *Authenticate an Inbound Certificate or LogonID Using Sterling External Authentication Server*.

Chapter 25. Test the PeSIT Connections

About this task

To verify that the engine can receive and initiate communications sessions, you have to establish a connection between a Sterling Connect:Express PNODE and the engine, initiate a session from the engine to the Sterling Connect:Express SNODE in the trusted zone, and review the Sterling Secure Proxy log for the results.

This procedure enables you to verify that the engine can:

- Establish a Sterling Connect:Express session between a PNODE and Sterling Secure Proxy
- Initiate a session to a Sterling Connect:Express SNODE on behalf of the Sterling Connect:Express PNODE connection

To verify the communications sessions:

Procedure

1. View the secureproxy.log.
2. Confirm that the sessions were established, as shown in the following example.

   ```
   23 avr. 2010 13:39:37,459 INFO  [ProxyNearScheduler-Thread-9]
   sys.ADAPTER.PeSITClearAdapter - protocol=pesit sessid=124048677744407
   SSP103I Session started from Peer Address: PNODE1.company/10.20.10.80
   23 avr. 2010 13:39:37,459 INFO  [ProxyNearScheduler-Thread-9]
   sys.ADAPTER.PeSITClearAdapter - protocol=pesit sessid=120000000007
   SSP104I Session Proceeding after Node match: INSERVER
   23 avr. 2010 13:39:37,459 INFO  [ProxyNearScheduler-Thread-9]
   sys.ADAPTER.PeSITClearAdapter - protocol=pesit sessid=120000000007
   SSE1831I Authentication mechanism: no authentication.
   23 avr. 2010 13:39:37,475 INFO  [ProxyNearScheduler-Thread-3]
   sys.ADAPTER.PeSITClearAdapter - protocol=pesit sessid=120000000007
   SSE0103I Connecting to server.
   23 avr. 2010 13:39:37,475 INFO  [ProxyNearScheduler-Thread-3]
   sys.ADAPTER.PeSITClearAdapter - protocol=pesit sessid=120000000007
   SSP0237I Attempting outbound connection with
   10.20.129.3/InetSocketAddress-host:/10.20.129.3-port:4004 ...
   23 avr. 2010 13:39:37,631 INFO  [ProxyFarScheduler-Thread-12]
   >  :  Bytes Received: 646 [at:  7.398711524695777E-4 MBPS]
   >  Bytes Sent: 402 [at:  4.604151753758053E-4 MBPS]
   >
   >  :  Bytes Received: 402 [at:  4.710017574692443E-4 MBPS]
   >  Bytes Sent: 646 [at:  7.568834212067955E-4 MBPS]
   >  23 avr. 2010 13:39:44,459 INFO  [ProxyFarScheduler-Thread-14]
   sys.ADAPTER.PeSITClearAdapter - protocol=pesit sessid=12400000000744407
   SSE0112I Session ended.
   ```

   If your session was unsuccessful, review the log information to determine the likely cause of the failure and the corrective action to take.

   Additional PeSIT configuration options support the following features:

   - Define alternate nodes for failover support
   - Record an error message or shutdown a connection based on protocol errors
   - Block PeSIT command from a PNODE

Chapter 26. Define Alternate Nodes for Failover Support

About this task

If you are using standard routing to connect to a Sterling Connect:Express server in the secure zone, you identify a primary server to connect to in the adapter. The primary nodes are defined in the netmap. For each PNODE definition in the netmap, you can identify up to three alternate outbound nodes to connect to if the primary Sterling Connect:Express server is not available.

Two methods of configuring alternate server routing are available.

- Select a previously defined outbound node from the drop-down list on the Netmap - Advanced tab. To configure this method, you first configure an outbound node definition in the netmap for each alternate node you want to use. Each connection uses the security and Sterling External Authentication Server settings defined for that outbound node in the netmap.
- Select IP address/port from the drop-down Node list on the Advanced tab 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 shares the security and Sterling External Authentication Server settings defined in the primary node definition.

If you configure alternate server definitions in the PNODE 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 and then to the third alternate, Node 3. If all are unsuccessful, the inbound connection fails.

To configure alternate outbound connections:

Procedure

1. Select **Configuration** from the menu bar.
2. Expand the **Netmaps** tree and click the netmap to modify.
3. Select the node to modify and click **Edit**.
4. Click the **Advanced** tab.
5. Do one of the following:
6. To identify an alternate node that is defined in the netmap and use its security settings, 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:
   a. Select Address/Port from the drop-down list in the **Alternate Destinations Node** field.
   b. Provide the IP Address and Port number for the alternate outbound node.
7. Click **OK**.
8. Click **Save**.

Chapter 27. Record an Error Message or Shut Down a Connection Based on Protocol Errors

About this task

To write a warning message to the log file or shut down a connection when a protocol violation occurs during a file transfer, enable this function in the Policy definition.

To enable an action based on a protocol error:

Procedure

1. Select **Configuration** from the menu bar.
2. Expand the **Policies** tree and select the policy to modify.
3. Select the action to take on a protocol error in the **Protocol Error Action** field.
4. Click **Save**.

Chapter 28. Block PeSIT Command from a PNODE

About this task

This scenario builds on the basic PeSIT configuration by adding the capability to prevent a PeSIT command from being executed.

To prevent a PeSIT command from being executed:

Procedure

1. Select **Configuration** from the menu bar.
2. Expand the **Policies** tree and click the policy to modify.
3. On the **Policy Configuration** panel, click the **Transfer Directions** tab.
4. Click on one of the following commands to disable the command:
   - **Receive a File Allowed (SELECT)**
   - **Send a File Allowed (CREATE)**
   - **Send a Message Allowed (MSG)**
5. Click **Save**.

Chapter 29. Change the Logging Levels

The following configuration events are written to the engine audit log:

- All fields from an initial engine configuration received from the Configuration Manager
- Changed fields from an engine configuration update from the Configuration Manager
- Inbound connections received for all protocols
- Inbound handshakes completed for the FTP, HTTP, PeSIT, and Sterling Connect:Direct® protocols
- Inbound login successes and failures for the FTP, HTTP, and SFTP protocols
- Outbound connections established for all protocols
- Outbound handshakes completed for the FTP, HTTP, PeSIT, and Sterling Connect:Direct protocols
- Outbound login successes and failures for the FTP, HTTP, and SFTP protocols

When you configure a PeSIT node, the logging level for the node is set to None and no log is created. You can change the logging level to one of the following options:

- ERROR to write error messages
- WARN to write error and warning messages
- INFO to write error, warning, and informational messages
- DEBUG to write all messages to the log including debugging messages

Chapter 30. Use Perimeter Servers to Manage PeSIT Communications

You can use a perimeter server with Sterling Secure Proxy to manage inbound and outbound PeSIT and Sterling Connect:Express communications. Configure perimeter servers for PeSIT and Sterling Connect:Express nodes the same way you configure perimeter servers for Sterling Connect:Direct nodes. Refer to *Configure Perimeter Servers to Manage Sterling Secure Proxy Communications*.

After you set up your Sterling Secure Proxy configuration, refer to *Manage Your Sterling Secure Proxy Configuration*.

Chapter 31. Modify Properties in an Adapter Definition

About this task

Adapters are configured with default settings. Use this procedure to modify a property. For FTP and HTTP adapters, the properties and default values are displayed. To change a property, type a new value for the property key. For SFTP, Sterling Connect:Direct, and PeSIT adapters, the properties are not displayed.

Refer to the field level help for a description of the properties. To change a property, type the property name and its key value.

To modify an adapter property:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Adapters** tree and click the adapter to modify.
3. Click the **Properties** tab.
4. Click **New** to add a new property definition.
5. For each property, specify values for the following:
   - **Key**
   - **Value**
6. Click **Save**.

Chapter 32. Provide Credentials to the Outbound PeSIT Node Using the Netmap

This scenario builds on the Basic PeSIT Configuration by enabling the use of Logon credentials from the netmap to connect to the outbound PeSIT connection. Following is a description of the security features supported in this scenario:

When an inbound trading partner connects to Sterling Secure Proxy, its credentials are replaced with credentials stored in the netmap. The replacement credentials are then used to connect to the outbound PeSIT server. This method uses Sterling Secure Proxy security features to prevent trading partners from knowing the credentials used to connect to the outbound Sterling Connect:Express. The outbound Sterling Connect:Express must have a partner definition that accepts the LogonID and password provided.

After you configure the environment to use credentials defined in the netmap, test the configuration by establishing a session initiated by a Sterling Connect:Express client to a Sterling Connect:Express server. Refer to *Test the PeSIT Connections* for more information on testing the configuration defined in this scenario.

Provide Credentials for the Outbound PeSIT Node Using the Netmap - Worksheet

In this scenario, edit the netmap and policy you created in the Basic PeSIT Configuration to provide user credentials stored in Sterling Secure Proxy to connect to the outbound PeSIT connection.

Collect the following information so that you can match the Sterling Secure Proxy configuration with the Sterling Connect:Express server configuration. Use the information on this worksheet as you edit the outbound node definition. Select the netmap and policy you created in the Basic PeSIT Configuration.

Configuration Manager Field	**Feature**	**Value**
Logon ID	Partner ID to use to connect to the Sterling Connect:Express server. (Must also be defined at the Sterling Connect:Express server.)	
Password	Password to use to connect to the Sterling Connect:Express server. (Must also be defined at the Sterling Connect:Express server.)	

Chapter 33. Copy a PeSIT Node

About this task

To quickly create a PeSIT node definition, you can copy an existing definition and make the changes necessary to create a new item.

To copy a PeSIT node:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Netmap** tree and click the PeSIT netmap where the node is defined.
3. Click the radio button beside the node to copy and click **Copy**.

   A new node is created and renamed to Copyof*ItemName* where *ItemName* is the name of the original node you created.
4. Modify the node definition as necessary.
5. Click **OK**.
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