

Sterling Secure Proxy



HTTP Reverse Proxy Scenarios

Version 34

Sterling Secure Proxy



HTTP 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. HTTP Reverse Proxy Configuration	1	Chapter 16. Add Credentials to the Local User Store for an HTTP Connection	35
Chapter 2. Complete Scenario Worksheets	3	Chapter 17. Provide Credentials to the Outbound HTTP Node Using the Netmap	37
Chapter 3. Complete and Test HTTP Configuration Scenarios.	5	Chapter 18. Configure Name and Password to Connect to the Outbound HTTP Server in the Netmap	39
Chapter 4. Create a Basic HTTP Configuration	7	Chapter 19. Strengthen Authentication for an HTTP Connection Using Sterling External Authentication Server	41
Chapter 5. Create an HTTP Policy	11	Chapter 20. Authenticate the Inbound HTTP Node Using Sterling External Authentication Server	43
Chapter 6. Create an HTTP Netmap	13	Chapter 21. Connect to the Outbound HTTP Server Using Sterling External Authentication Server Worksheet	45
Chapter 7. Define the HTTP Adapter Used for the Connection	15	Chapter 22. Connect to the Outbound HTTP Server Using Information Stored in LDAP	47
Chapter 8. What You Defined with the Basic HTTP Configuration Scenario	17	Chapter 23. Test the Inbound and Outbound HTTP Connections	49
Chapter 9. Variations on the Basic HTTP Configuration	19	Chapter 24. Block Common Exploits	51
Chapter 10. Define Inbound HTTP Node Connection Definitions.	21	Chapter 25. Change the Values to Block in a URL String	53
Chapter 11. Add SSL/TLS Support for an HTTP Connection.	23	Chapter 26. Map a URL in HTML Content from the Outbound Server	55
Chapter 12. Secure the Inbound HTTP Connection Using the SSL or TLS Protocol	27	Chapter 27. Configure HTTP Rewrite to Support the Sterling B2B Integrator Dashboard	57
Chapter 13. Secure the Outbound HTTP Connection Using the SSL or TLS Protocol	29	Chapter 28. Configure HTML Rewrite	59
Chapter 14. Add Local User Authentication to the HTTP Connection	31	Chapter 29. Define Alternate Nodes for Failover Support for an Outbound HTTP Connection	61
Chapter 15. Enable Local User Authentication to an HTTP Inbound Connection	33		

Notices 63

Chapter 1. HTTP Reverse Proxy Configuration

The HTTP configuration scenarios describe how to configure HTTP protocol connections to and from the engine.

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

Organization of the HTTP Configuration Scenarios

The first scenario instructs you on how to configure a basic configuration. Each successive scenario adds an additional security feature to the basic configuration. After configuring each scenario, 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 HTTP protocol connections to the Sterling B2B Integrator server:

- Create a basic HTTP 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 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 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

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

- Block common exploits
- Rewrite URLs in HTML content to route inbound connections through Sterling Secure Proxy
- Define alternate nodes for failover support

Chapter 2. Complete Scenario Worksheets

About this task

Before you begin configuring Sterling Secure Proxy for each HTTP connection scenario, 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 in the worksheet.
3. Note the Configuration Manager fields where you will specify the value.

Chapter 3. Complete and Test HTTP Configuration Scenarios

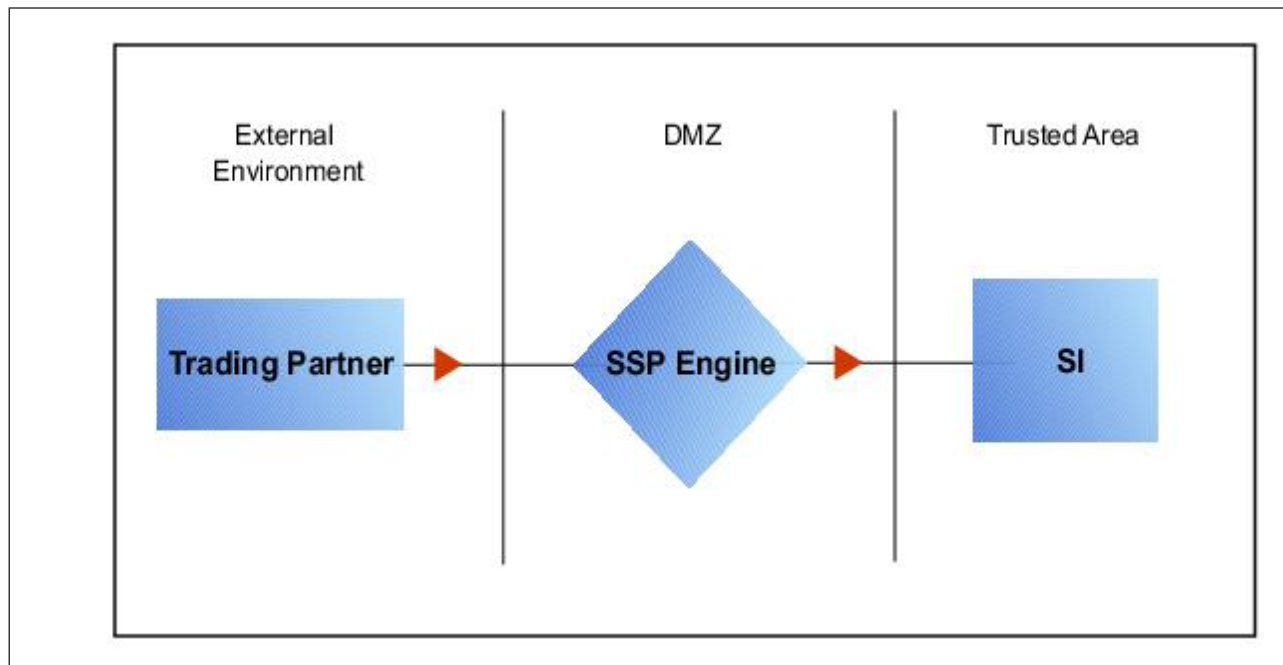
About this task

Work through the sequence of HTTP configuration scenarios in the order they are presented to add additional security features. Be sure to test each feature before you add the next feature to the configuration. Before you move Sterling Secure Proxy into production, ensure that you have configured and tested all of the 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 HTTP 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 shown in the following diagram. 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 HTTP connection from the trading partner. For more information on testing the configuration, see *Test the Inbound and Outbound HTTP Connections*.

Complete the following tasks to define a basic HTTP configuration:

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

Basic HTTP Configuration Worksheet

Before you configure Sterling Secure Proxy for HTTP connections, gather the information on the Basic HTTP Configuration Worksheet. You use this information as you configure a basic HTTP connection for Sterling Secure Proxy. After you configure Sterling Secure Proxy for HTTP connections, validate the configuration by initiating an HTTP connection from the inbound node.

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

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: 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	Netmap name	

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	*
		Specifying * for this value allows all inbound nodes configured on the Sterling B2B Integrator server as trading partners to connect to the Sterling B2B Integrator server. Use this value for testing purposes. To create a more specific node definition, see Define Inbound HTTP Node Connection Definitions.
Policy	Name of policy you create	This value is selected from a pull-down list.

Outbound Sterling B2B Integrator Server Connection

Node Name	Outbound Sterling B2B Integrator server node name.
Primary Destination Address	Host name or IP address to connect to the outbound Sterling B2B Integrator server.
Primary Destination Port	Port number to connect to the outbound Sterling B2B Integrator server.

Create an HTTP adapter that defines information necessary to establish HTTP connections to and from Sterling Secure Proxy. When you are configuring the adapter, select the basic netmap and the outbound Sterling B2B Integrator server you define in the netmap definition.

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	

Configuration Manager Field	Feature	Value
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 5. Create an HTTP Policy

About this task

The HTTP policy defines how you impose controls to authenticate a trading partner trying to access an 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 > HTTP Policy**.
3. Type a **Policy Name**.
4. Click **Save**.

Chapter 6. Create an HTTP Netmap

About this task

You define inbound connection information for your external 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 > HTTP 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 7. Define the HTTP Adapter Used for the Connection

About this task

An HTTP adapter definition specifies system-level communications information necessary for HTTP 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 Windows* for instructions.

To define an HTTP adapter:

Procedure

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

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

Creating 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 HTTP 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 HTTP server adapter configured to listen for the port specified in the outbound node definition
- The user ID and password provided by the inbound node are defined at the Sterling B2B Integrator server

Refer to *Test the Inbound and Outbound HTTP Connections* for information about testing the HTTP 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 9. Variations on the Basic HTTP Configuration

After you confirm that the communications sessions you established using the basic HTTP 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 HTTP 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

Chapter 10. Define Inbound HTTP Node Connection Definitions

About this task

This procedure instructs you how to modify the basic HTTP configuration to add inbound node definitions for a group of nodes with similar information, and definitions that limit access to one specific inbound node. It assumes that you have already configured an adapter. Gather a list of all inbound trading partners, including names and IP addresses.

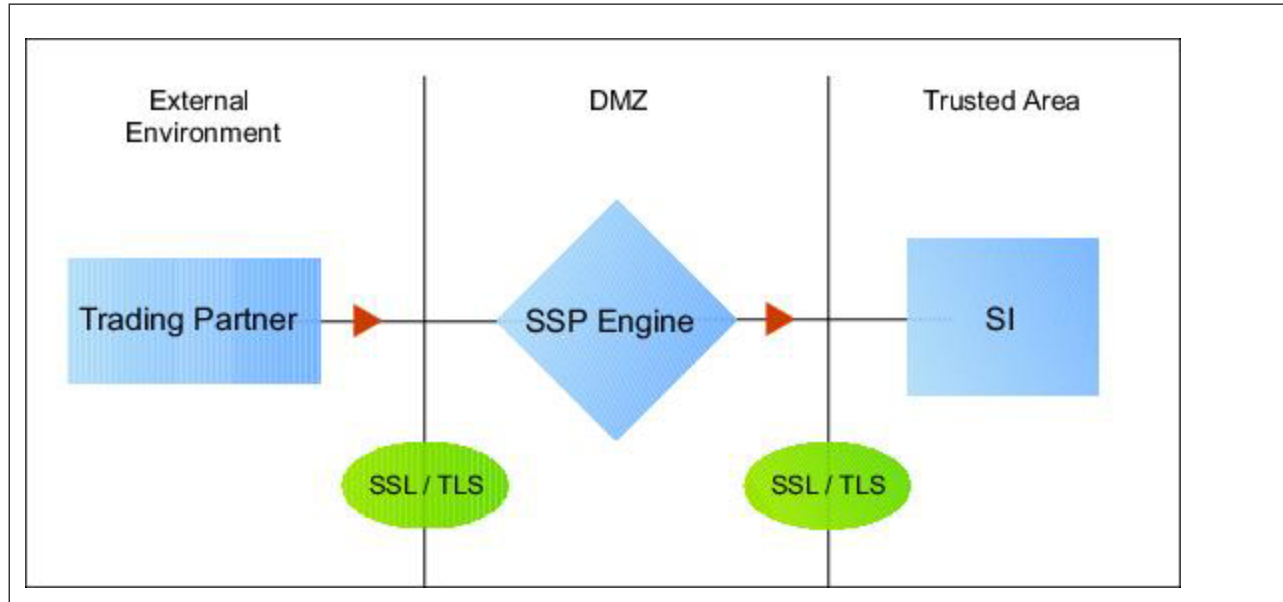
To define inbound connection definitions:

Procedure

1. Identify patterns that can be used to define groups of inbound nodes.
2. Decide if you need to define a trading partner connection for any individual IP addresses.
3. Click **Configuration** from the menu bar.
4. Expand the **Netmaps** tree and select 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 for 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 since 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**.
10. Establish a session initiated by an HTTP client to an Sterling B2B Integrator server to test the configuration.

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

This scenario builds on the Basic HTTP 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 the outbound node connections.



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*.

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

- Protocol
- Cipher suites
- Stores and certificates

To effectively configure and test this scenario:

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

SSL/TLS Support for HTTP Worksheet

Before you add SSL/TLS support to the connection information you created in the Basic HTTP 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	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 • 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 where the certificate is stored.	
CA Certificates/Trusted Root	Name of CA certificate/trusted root (if client authentication is enabled).	
Key Store	The database 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 connection. Select the trusted certificate to use to validate the server certificate. If the server requires client authentication, you must specify a server certificate. If the server requires client authentication, you specify a key/system certificate.

Configuration Manager Field	Feature	Value
Outbound Node Name	Name of outbound node to add security to.	Select a node definition from the list.

Configuration Manager Field	Feature	Value
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 • SSL v3
Trust Store	The trust store where the certificate is stored.	
CA Certificates/ Trusted Root	Identify the certificate to use to secure the outbound connection.	
Key Store	Key store where the Key/System Certificate is stored.	
Key/System Certificate	System certificate used to validate the server.	
Available Ciphers	Cipher suites to enable.	
Selected Ciphers		

Chapter 12. Secure the Inbound HTTP Connection Using the SSL or TLS 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 Cert Stores.

To enable the TLS or SSL protocol:

Procedure

1. Click **Configuration** from the menu bar.
 2. Expand the **Netmaps** tree and select an HTTP 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 Cipher Suites**
 - **Selected Cipher Suites**
 7. To enable client authentication:
 - a. Click **Enable Client Authentication**.
 - b. Select the trust store where the CA certificate or trusted root certificate is stored.
 - c. Select the CA Certificates/Trusted Root certificate to use.
- 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**.
 10. Establish a session initiated by an HTTP client to an Sterling B2B Integrator server to test the configuration.

Chapter 13. Secure the Outbound HTTP Connection Using the SSL or TLS 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 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 cert stores.

To enable the TLS or SSL protocol:

Procedure

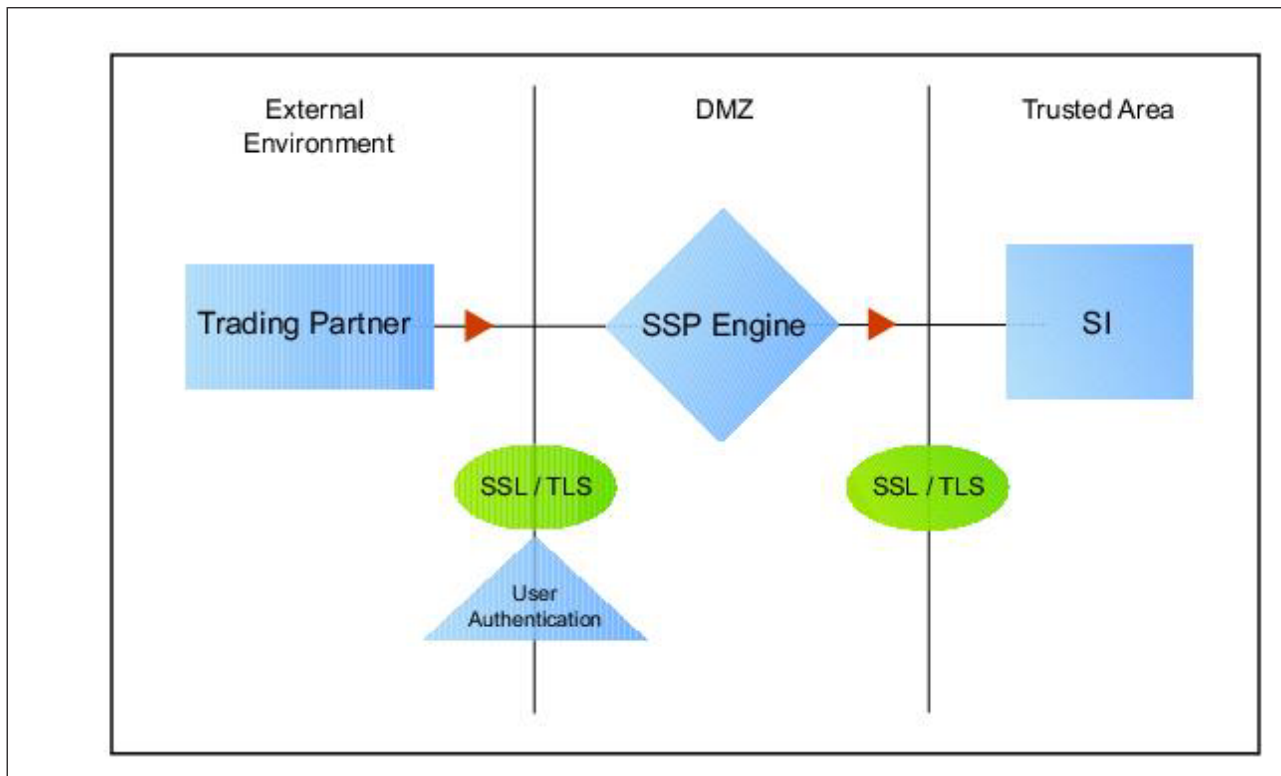
1. Click **Configuration** from the menu bar.
2. Expand the **Netmaps** tree and select an HTTP netmap to modify.
3. Click the **Outbound Nodes** tab.
4. Select an outbound node to modify, and click **Edit**.
5. Click the **Security** tab, and then click **Secure Connection** to enable security.
6. Select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

 - **Available Ciphers**
 - **Selected Ciphers**
7. If the Sterling B2B Integrator server requires client authentication, select the key store and key/system certificate to present to the Sterling B2B Integrator server during the SSL/TLS handshake.
8. Click **OK**.
9. Click **Save**.
10. Establish a session initiated by an HTTP client to an Sterling B2B Integrator server to test the configuration.

Chapter 14. Add Local User Authentication to the HTTP Connection

This scenario builds on the Basic HTTP Configuration by adding user authentication to the inbound connection using information defined in the local user store. Following is an illustration of the security options enabled for this scenario:



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.

Adding user authentication to the inbound connection defined in the Basic HTTP 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 HTTP client to an Sterling B2B Integrator server.

HTTP Inbound Connection (Local User Authentication) Worksheet

Before you add user authentication to the inbound connection you created in the Basic HTTP Configuration scenario, gather the information on the HTTP 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 HTTP 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 15. Enable Local User Authentication to an HTTP Inbound Connection

About this task

You can strengthen the security of inbound connections by enabling local user authentication. This procedure describes how to configure the use of the local user store to validate an inbound connection.

Note: Check the netmap to ensure that the policy you edit 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 the policy you created in the basic configuration.
3. Click the **Advanced** tab.
4. Enable the **User Authentication Through Local User Store** option.
5. Click **Save**.

Chapter 16. Add Credentials to the Local User Store for an HTTP Connection

About this task

If you enable user authentication through the local user store, you have to add user information to the local user store to be validated by Sterling Secure Proxy during an inbound HTTP 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 that contains the user credentials.

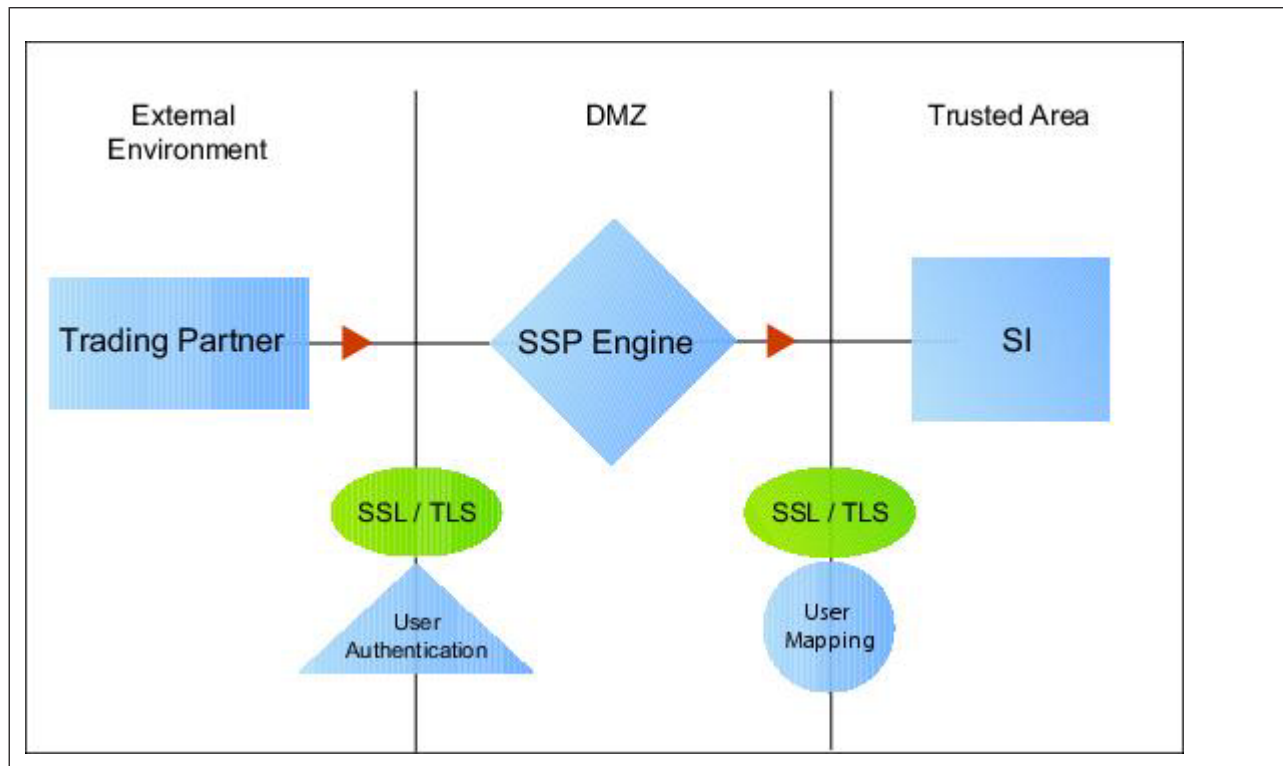
To add user information to the local user store:

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 **OK**.
6. Click **Save**.
7. Establish a session initiated by an HTTP client to an Sterling B2B Integrator server to test the configuration.

Chapter 17. Provide Credentials to the Outbound HTTP Node Using the Netmap

This scenario builds on the Basic HTTP Configuration by enabling the use of user credentials from the netmap to connect to the outbound Sterling B2B Integrator connection. Following is an illustration of the security features supported in this scenario:



If you configure user mapping using the netmap, an inbound trading partner connects to Sterling Secure Proxy and provides one set of credentials. Its credentials are replaced with credentials stored in the netmap. The replacement credentials are then used to connect to the outbound secure server. This method uses Sterling Secure Proxy security features to prevent trading partners from knowing the credentials used to connect to the outbound Sterling B2B Integrator server. The outbound Sterling B2B Integrator server must have a user definition that accepts the user ID and password provided.

After you configure the environment to use credentials defined in the netmap, test the configuration by establishing a session initiated by an HTTP client to an Sterling B2B Integrator server. Refer to *Test the Inbound and Outbound HTTP Connections* for more information on testing the configuration described in this scenario.

Connect to the Outbound HTTP Server Using Credentials from the Netmap Worksheet

In this scenario, edit the netmap and the policy you created in the Basic HTTP Configuration to provide user credentials stored in Sterling Secure Proxy to connect to the outbound Sterling B2B Integrator connection.

Collect the following information so you can match the Sterling Secure Proxy configuration with the Sterling B2B Integrator server configuration. Use the information on this worksheet as you edit the outbound node definition, and be sure to select the netmap and policy you created in the Basic HTTP Configuration.

Configuration Manager Field	Feature	Value
User ID	User ID used to connect to the Sterling B2B Integrator server. (Must also be defined at the Sterling B2B Integrator server)	
Password	Password to connect to the server. (Must also be defined at the Sterling B2B Integrator server)	

Chapter 18. Configure Name and Password to Connect to the Outbound HTTP Server in 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 HTTP 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

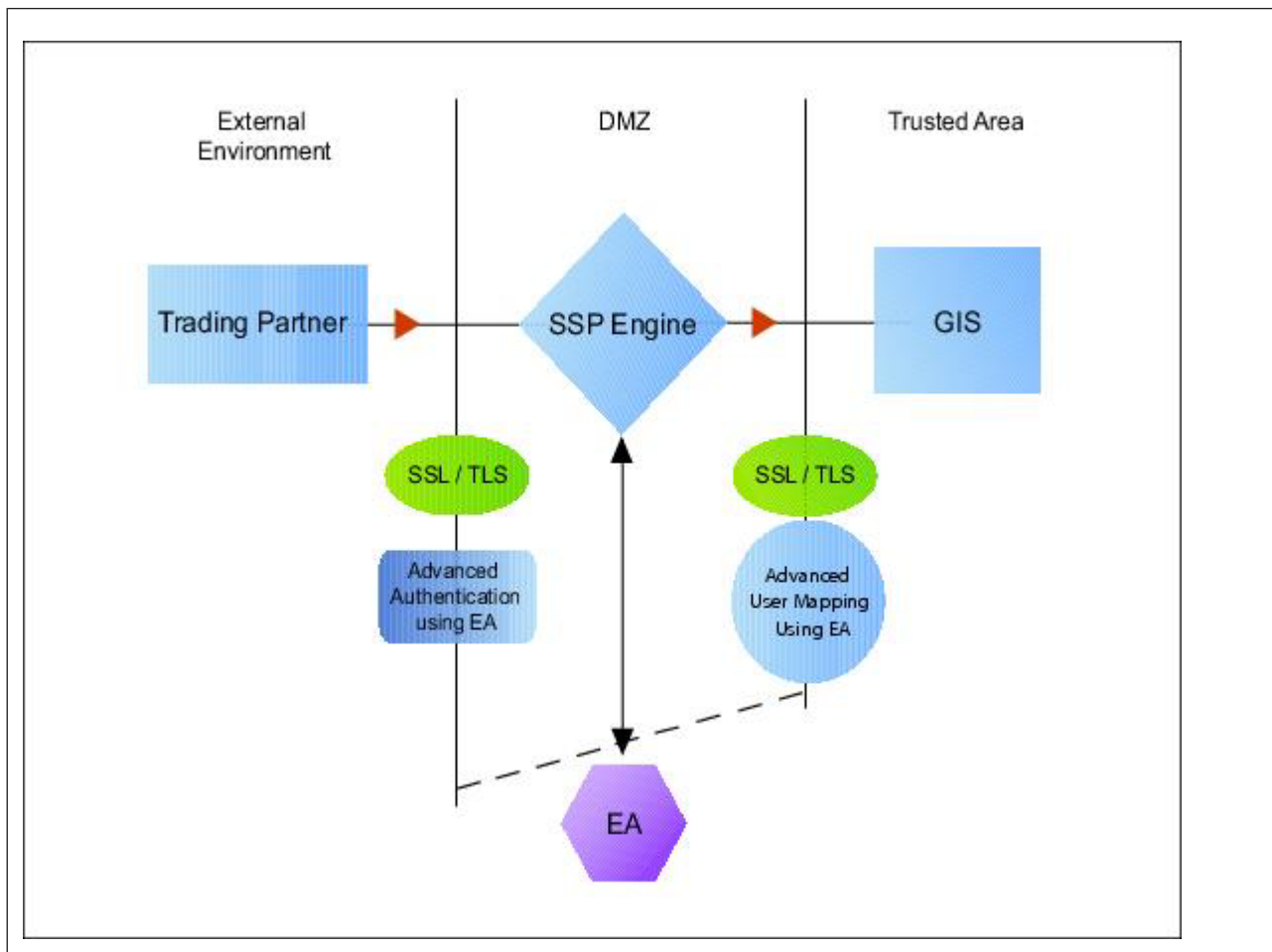
To configure validation for the outbound connection using credentials stored in the netmap:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Netmaps** tree and select an HTTP 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 the following values to be used to connect to the Sterling B2B Integrator server:
 - **User ID**
 - **Password**
7. Click **OK**.
8. Click **Save**.
9. Expand the **Policies** tree and select the policy to modify.
10. On the **Policy Configuration** panel, click the **Advanced** tab.
11. From the **User Mapping: Internal User ID** list, select **From Netmap**.
12. Click **Save**.
13. Test the configuration to ensure that the updated configuration is working.

Chapter 19. Strengthen Authentication for an HTTP Connection Using Sterling External Authentication Server

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



Authenticate an Inbound HTTP Certificate or User 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. Following are some of the options Sterling External Authentication Server can perform:

- Validate certificates, including dates and signatures
- Verify the presence of X.509 v3 extensions

- Enforce minimum key length requirements
- Check certificates against certificate revocation lists (CRLs)
- Perform LDAP queries

The Sterling External Authentication Server definition determines which options are enabled.

Manage Connection Requirements to the Outbound HTTP Server Using Sterling External Authentication Server

For a higher level of security when connecting to the outbound server, use information stored in an LDAP database to connect to the outbound server. To use information in an LDAP database, you configure Sterling External Authentication Server. Sterling External Authentication Server can map a user ID and password provided by an inbound connection to a user ID and password that is not exposed to the external node.

Authenticate an Inbound HTTP Certificate or User Using Sterling External Authentication Server Worksheet

Use the following worksheet to specify the information needed to authenticate a trading partner with information in Sterling External Authentication Server. Update the policy you created in the Basic HTTP Configuration for this scenario.

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

Chapter 20. Authenticate the Inbound HTTP 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 LDAP 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, 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 keystore.
- The Sterling External Authentication Server connection has been configured in Sterling Secure Proxy. Refer to *Configure Sterling Secure Proxy for Sterling External Authentication Server*.

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 **HTTP Policy Configuration** panel, click the **Advanced** tab.
4. 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.
5. To validate a user from Sterling External Authentication Server:
 - a. Enable **User Authentication Through External Authentication** field.
 - b. Type the name of the definition you defined in Sterling External Authentication Server in the **User Authentication External Authentication Profile** field.
 - c. Deselect the **Through Local User Store** option.
 - d. Select **From External Authentication** in the **User Mapping:Internal User ID** field.
6. Click **Save**.
7. You can now associate this policy with the inbound node on which you want to perform user authentication using Sterling External Authentication Server.

Chapter 21. Connect to the Outbound HTTP Server Using Sterling External Authentication Server Worksheet

Use this worksheet to identify information required to configure a stronger outbound connection using information in an LDAP database:

Configuration Manager Field	Feature	Value
User Certification Through External Authentication	Will you validate user information against LDAP?	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 22. Connect to the Outbound HTTP Server Using Information Stored in LDAP

About this task

If you store user credentials in an LDAP database, 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 definition in Sterling External Authentication Server and 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 trust store.

To configure the use of credentials from an LDAP database:

Procedure

1. Click **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. Enable the **User Authentication Through External Authentication** field.
5. Type the name of the definition you defined in Sterling External Authentication Server in the **User Authentication External Authentication Profile** field.
6. Deselect the **Local User Store** option.
7. Select **User ID/Password from External Authentication** in the **User Mapping:Internal User ID** field.
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 23. Test the Inbound and Outbound HTTP Connections

About this task

To verify that the engine can receive and initiate communications sessions, you have to establish a connection between an HTTP 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 on the engine for communication sessions to be established.

This procedure enables you to verify that the engine can:

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

To verify the communications sessions:

Procedure

1. Make sure the engine is running.
2. Initiate an HTTP 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 shown in the following sample audit log output.

Sample Inbound 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=10.20.200.100 SPORT=40134
SSP104I Session: 1 - Session Proceeding after Node match: Any11
Sep 2009 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=dname.company.com DIP=10.20.246.42 DPORT=10054 SUID=admin
DUID=admin SSP102I 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=10.20.200.100 SPORT=40134
SSP104I Session: 1 - Session Proceeding after Node match: Any11
Sep 2009 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=dname.company.com DIP=10.20.200.40 DPORT=10054 SUID=admin
DUID=admin SSP102I 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]
```

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

The following additional HTTP configuration options are available:

- Block common exploits
- Change the commands that are allowed or blocked
- Rewrite URLs in HTML content to route inbound connections through proxy
- Define alternate nodes for failover support

Chapter 24. Block Common Exploits

About this task

When a connection from an inbound HTTP node to Sterling Secure Proxy is attempted, you can enable the ability to scan the URL requested and look for commonly occurring exploits.

If block common exploits is enabled, HTTP requests cannot contain the following characters or strings, which are commonly used on attacks on HTTP servers:

```
--  
|  
|  
\  
<?  
\u0000
```

You can change the values that are blocked in the policy.

To enable the capability to block common exploits:

Procedure

1. Click **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. Enable the **Block Common Exploit Strings** field.
5. Click **Save**.

Chapter 25. Change the Values to Block in a URL String

About this task

When a connection from an inbound HTTP node to Sterling Secure Proxy is attempted, you can enable the ability to scan the URL requested and look for commonly occurring exploits.

If block common exploits is enabled, HTTP requests cannot contain the characters or strings, identified in the graphic above. You can change the characters that are blocked. To change the blocked strings:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Policy** tree and click the HTTP policy to modify.
3. On the **HTTP Policy Configuration** panel, click the **Advanced** tab.
4. Add a new value, or delete or edit an existing value, by changing the values in the **Block Common Exploit Strings** field.
5. Click **Save**.

Chapter 26. Map a URL in HTML Content from the Outbound Server

About this task

HTTP Reverse Proxy HTML rewriting allows you to replace the URL links submitted by an HTTP client to the HTTP server with URL links to Sterling Secure Proxy. If the HTTP server has web pages with links to other web pages on the same host, you must map all URL connections in order for the links to work.

Before you configure this option, create a netmap definition. Create an outbound node definition for each URL containing a host and port.

Chapter 27. Configure HTTP Rewrite to Support the Sterling B2B Integrator Dashboard

About this task

To communicate with the Sterling B2B Integrator dashboard, two connections must be established to the outbound Sterling B2B Integrator server: one connection to the Sterling B2B Integrator base port and one to the Sterling B2B Integrator base port + 33.

To configure this environment:

Procedure

1. Define two outbound nodes in the netmap: Definition 1 configures a connection to the Sterling B2B Integrator host and base port. Definition 2 configures a connection to the Sterling B2B Integrator host and base port + 33.
2. Add mapping values to the netmap definition for both URL connections.
3. Configure two HTTP Reverse Proxy adapters: one to route connections to the Sterling B2B Integrator host and base port (Definition 1) and another to the Sterling B2B Integrator host and base port + 33 (Definition 2). Use the same netmap with both adapter definitions. For each adapter, select a different outbound node to route connections to in the Standard Routing Node field.

For example, assume Sterling Secure Proxy is installed and running on the host, proxy_host and HTTP Reverse Proxy adapter 1 is configured to listen on the port, adapter1_port. It uses the outbound node defined as Sterling B2B Integrator base port on a host called si_host. HTTP Reverse Proxy adapter 2 listens on the port, adapter2_port and uses an outbound node defined as Sterling B2B Integrator base port + 33 (the dashboard default port).

To configure this environment, define the following URL rewrite values in the netmap definition:

Server URL	Proxy URL
http://<si_host>:<baseport>	http://<proxy_host>:<adapter1_port>
http://<si_host>:<baseport+33>	http://<proxy_host>:<adapter2_port>

Chapter 28. Configure HTML Rewrite

About this task

To configure HTML rewrite:

Procedure

1. Click **Configuration** from the menu bar.
2. Expand the **Netmaps** tree and select an HTTP netmap to modify.
3. Make sure you have two outbound node definitions: one for the Sterling B2B Integrator server and its base port and another for Sterling B2B Integrator base port + 33. To define an outbound node definition:
 - a. Click the **Outbound Nodes** tab and click **New**.
 - b. Specify the following values:
 - **Outbound Node Name**
 - **Primary Destination Address**
 - **Primary Destination Port**
4. Click **OK**.
5. On the **HTTP Netmap Nodes** panel, click the **HTML Rewrite** tab.
6. Click **New**.
7. Enable the **Support HTML Rewrite** field.
8. Type the URL path for the outbound server in the **Server URL** field.
9. Type the URL path for the proxy in the **Proxy URL** field. Refer to *Configure HTTP Rewrite to Support the Sterling Secure Proxy Dashboard* and the table of values for instructions on the URL values to define for the Sterling B2B Integrator dashboard.
10. Click **Save**.
11. Repeat steps 3 through 10 for all HTML Rewrite options you want to configure.
12. To reorder the HTML rewrite definitions:
 - a. Click the radio button beside the URL routing definition to reorder.
 - b. Click **Move Up** or **Move Down** until the item is in the correct order.
13. Click **Save**.
14. Expand the **Adapters** tree and click the adapter to modify.
15. Enable **Support HTML Rewrite**.
16. Click **Save**.
17. Test the configuration to ensure that the HTML rewrite is configured correctly.

Note: If the following message is written to the secureproxy.log file, correct your URL definition:

```
HTML Rewrite proxy URL Map entry is not a valid URI.
```

Chapter 29. Define Alternate Nodes for Failover Support for an Outbound HTTP Connection

About this task

If you are using standard routing to connect to an Sterling B2B Integrator server in the secure zone, you define a primary Sterling B2B Integrator server to connect to in the adapter. For each outbound node definition, you can identify up to three alternate outbound nodes to connect to when the primary Sterling B2B Integrator server is not available.

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

- Select a previously defined outbound node from the drop-down list on the **Advanced** tab. To configure 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 other settings defined for that outbound node in the netmap.
- Select IP address/port from the drop-down 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 other 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 an HTTP 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. To identify an alternate node 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.
7. 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.

8. Click **OK**.
9. 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.

Licenses 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