Sterling Secure Proxy

Overview

Version 34

Sterling Secure Proxy

Overview

Version 34

Note
Before using this information and the product it supports, read the information in "Notices" on page 43.

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 Overview

IBM® Sterling Secure Proxy acts as an application proxy between IBM Sterling Connect:Direct® nodes or between a client application and a Sterling B2B Integrator server. Sterling Secure Proxy provides a high level of data protection between external connections and your internal network. Define an inbound node definition for each trading partner connection from outside the company and an outbound node definition for every company server to which Sterling Secure Proxy will connect.

Chapter 2. Sterling Secure Proxy Architecture

The components of the Sterling Secure Proxy architecture are:

- Sterling Secure Proxy Engine—the engine resides in the DMZ and contains the minimum components necessary to manage communications sessions. The engine configuration (Sterling Secure Proxy engine properties) is created at Configuration Manager and pushed to the engine. It is stored in active memory and is never stored on disk in the DMZ. No web services or UI ports are open in the DMZ.
- Configuration Manager (Sterling Secure Proxy CM)—Configuration Manager is installed in the trusted zone. Use this tool to configure your environment. When you save a configuration definition (Sterling Secure Proxy configuration store) at CM, it is pushed to an engine, using an SSL session. Configuration files are encrypted and stored on the computer where CM is installed.

  Note: Only one Configuration Manager should update an engine definition.
- Sterling Secure Proxy configuration store—This file is encrypted on disk and contains the following information:
  - The user store with information on user credentials
  - The system certificate store with the certificates used for SSL/TLS sessions
  - The key store with the SSH keys
  - The engine configuration store with all configuration information for the engine
- Sterling Secure Proxy engine properties file—These files are encrypted and contain the following information:
  - The IP and port number to listen on for connections from Configuration Manager
  - SSL key certificate, trusted certificate, and encryption cipher used for the connection from Configuration Manager
- Web server—Configuration Manager is installed with a web server. You open a browser and access CM through a web page to configure Sterling Secure Proxy and monitor the engine activity. The web server is installed when you install Configuration Manager.
- Adapter—an adapter identifies the protocol allowed for connections from trading partners. You can accept connections from clients that use different protocols; however, you must define a different adapter for each protocol. A single engine can run multiple adapters. In an adapter definition, you identify the port on which to listen for connections, the netmap to use with the adapter, the security policy, and the routing method to use. If you are using Sterling External Authentication Server, you identify the Sterling External Authentication Server to use in the adapter definition. If you are using a remote perimeter server, you identify the perimeter server to use in the adapter definition.
- Netmap—define a netmap to identify the trading partners authorized to communicate through Sterling Secure Proxy and the company servers where connections are made.
  - For a Sterling Connect:Direct netmap, create a node definition for all Sterling Connect:Direct nodes that will communicate through Sterling Secure Proxy. The node definition identifies the IP address and port to be used by the node and the policy to associate with the node. If SSL or TLS security is required

for the connection, configure the protocol options in the node definition. You can also enable node-level logging in the node definition.

- For HTTP and FTP netmaps, define an inbound node definition for trading partner connections from outside the company. The inbound node definition identifies the IP address or address pattern to allow for the connection and the policy to associate with the node. If SSL or TLS security is required, configure the protocol options in the node definition. You can also enable node-level logging in the inbound node definition.
- For HTTP and FTP netmaps, define an outbound node for every company server to which Sterling Secure Proxy will connect. An outbound node definition identifies the address and port used to connect to the company server and enables SSL or TLS if this is required. You can also enable node-level logging and failover support in the outbound node definition.
- For SFTP netmaps, define an inbound node definition for trading partner connections from outside the company. The inbound node definition identifies the IP address or address pattern to allow for the connection and the policy to associate with the node.You can also enable node-level logging in the inbound node definition.
- For SFTP netmaps, define an outbound node for every company server to which Sterling Secure Proxy will connect. An outbound node definition identifies the address and port used to connect to the company server, the known host key that is used to authenticate the company server to Sterling Secure Proxy, and the cipher suites and MACs used to secure the connection. You can also enable node-level logging and failover support in the outbound node definition.

- Policy—define a policy to identify the security features to implement for an inbound node definition or a Sterling Connect:Direct node definition.
  - In all protocol policies, you can enable the capability to authenticate the inbound connection and identify what user ID and password to use to connect to the secure company server.
  - For FTP, HTTP, and Sterling Connect:Direct policies, you can enable the capability to authenticate certificate information using Sterling External Authentication Server,
  - In an HTTP policy, you can enable the capability to block commonly occurring HTTP exploits.
  - In a Sterling Connect:Direct policy, you can enable the capability to send a warning message or stop a session if a protocol error occurs, as well as prevent a Sterling Connect:Direct node from performing a runtask, runjob, copystep, or submit step function.
  - In an SFTP policy, you identify the method required to authenticate the inbound connection. Authentication methods supported are key, password, password or key, and password and key.
- Sterling External Authentication Server—a separately installed feature of Sterling Secure Proxy, Sterling External Authentication Server allows you to validate digital certificates passed by the client or trading partner during SSL/TLS session requests. You can also validate certificates against one or more certificate revocation lists (CRLs), and validate certificates based on a valid date range. See the Sterling Secure Proxy documentation library for more information.

  Sterling External Authentication Server can be configured to validate certificates and authenticate users. The functions performed by Sterling External Authentication Server are defined in an Sterling External Authentication Server definition. Sterling External Authentication Server performs one or more of the following functions:

- Certificate Validation
- Certificate Revocation List (CRL)—certificate revocation checking using a certificate revocation list (CRL)
- Multi-factor Authentication
- Certificate Policy Enforcement
- LDAP Authentication
- User ID mapping—remote trading partners can be given IDs and passwords that do not provide access to internal systems. The ID and password presented by the trading partner is mapped to an ID and password that can then access the internal system
- Tivoli Access Manager Authentication
- Generic Authentication

Before you can use Sterling External Authentication Server with Sterling Secure Proxy, you must configure Sterling External Authentication Server definitions in Sterling Secure Proxy. Then, when configuring policies and protocol adapters, you select these server definitions. You can also select security features available in Sterling External Authentication Server such as certificate authentication, user authentication, and user mapping. Refer to the Sterling External Authentication Server documentation library for more information.

Chapter 3. Authenticate Trading Partners in the DMZ

Sterling Secure Proxy allows you to select an authentication method to meet your security requirements. The authentication mechanisms can be used together to enforce multi-factor authentication. Authentication options include certificate authentication, user authentication, and IP address checking.

Chapter 4. Authenticate Sterling Secure Proxy to the Trusted Zone Application

After Sterling Secure Proxy authenticates the remote trading partner, it creates another session to the application in the trusted zone. For this connection, Sterling Secure Proxy is the client and is authenticated by the trusted zone application. Sterling Secure Proxy provides SSL client authentication and user authentication.

- SSL client authentication (recommended)—if you want to secure the session between Sterling Secure Proxy and the application in the trusted zone, you can require that Sterling Secure Proxy present a certificate during SSL client authentication. This certificate is authenticated by the trusted zone application during the SSL handshake. Use this option if you want to enforce the following security features:
  - Secure the connection from Sterling Secure Proxy to the trusted zone application (recommended).
  - You require multiple factors of authentication by the trusted zone application and will authenticate Sterling Secure Proxy, using SSL client and user authentication.
  - You require a single factor of authentication by the trusted zone application, and you will authenticate Sterling Secure Proxy using SSL client authentication only.
- User authentication—Sterling Secure Proxy is required to provide user credentials when logging on to the application in the trusted zone. The following are user authentication options:
  - Pass-through (recommended)—this option sends the user credentials presented by the trading partner to the application in the trusted zone for authentication. This mechanism allows the user identity to be maintained at the trusted zone application.
  - Sterling External Authentication Server Mapped User Credentials—the user credentials are mapped using Sterling External Authentication Server. When Sterling Secure Proxy uses Sterling External Authentication Server for user authentication, it receives the user credentials from the trading partner and sends them to Sterling External Authentication Server for validation. If configured, Sterling External Authentication Server returns the mapped user credentials, and Sterling Secure Proxy uses them to log on to the application in the trusted zone.
  - Netmap—the user credentials are defined in the outbound node of the netmap that is used by Sterling Secure Proxy to establish a session with the application, in the trusted zone. Sterling Secure Proxy logs in to the trusted zone application as the same user for all sessions. This method is not recommended.

Chapter 5. Certificate Authentication Options

You can authenticate a remote trading partner using certificate authentication. Certificate authentication uses SSL client authentication and is optional. Three methods of certificate authentication are available to allow you the flexibility to choose how you want to authenticate trading partners using x.509 certificates. Certificate authentication options include no authentication, local authentication, or authentication using Sterling External Authentication Server. Authentication using Sterling External Authentication Server provides the highest level of security.

Option	Description
Additional Certificate Authentication Using Sterling External Authentication Server (Recommended)	This method provides the most secure method of certificate authentication. Configure SSL client authentication to use Sterling External Authentication Server to perform additional authentication on the certificate. Sterling External Authentication Server can perform the following authentications: • Certificate Revocation List (CRL) checking—validates that the certificate has not been revoked. • Common name check or subject name lookup— validates that the certificate is issued to a trusted trading partner by looking up the name at your LDAP server. • Binary comparison—compares the certificate received to a public certificate. • Bind certificate to an IP address—validates that the certificate and IP address are associated and that the certificate is presented by the IP address identified. • Custom Exit—transmit the certificate to your java program to interface with internal certificate validation routines. Choose this option to enforce the following security policy requirements: • Enforce multiple factors of authentication in the DMZ and authenticate the trading partner connection using SSL client authentication and user authentication. • Enforce a single factor of authentication in the DMZ and you plan to authenticate the trading partner connection using SSL client authentication. • To further authenticate the client certificate using a mechanism external to Sterling Secure Proxy.
Local Certificate Authentication	If SSL client authentication is configured, Sterling Secure Proxy requests a valid certificate from the trading partner. The certificate is validated against the trusted root. Choose this option to enforce the following security policy requirements: • Enforce multiple factors of authentication in the DMZ and authenticate using SSL client authentication and user authentication. • Enforce a single factor of authentication in the DMZ and authenticate using SSL client authentication. • Authenticate using SSL client authentication and do not use Sterling External Authentication Server to provide certificate validation.

Option	Description
No Certificate Authentication	You can configure Sterling Secure Proxy so that the remote trading partner certificate is not authenticated. Either disable SSL security or turn on SSL security but do not enforce SSL client authentication. In both configurations, Sterling Secure Proxy will not require the client to send a certificate for authentication. Choose this option to enforce the following security policy requirements: • Enforce a single factor of authentication in the DMZ and authenticate a trading partner using user authentication. • You require an SSL session break in the DMZ but you do not want to authenticate the trading partner. In this case, you do not enforce SSL client authentication to Sterling Secure Proxy nor do you authenticate the user. • The session with the remote trading partner is not secure and does not use SSL. The trading partner does not present a certificate.

Chapter 6. Configuration Overview

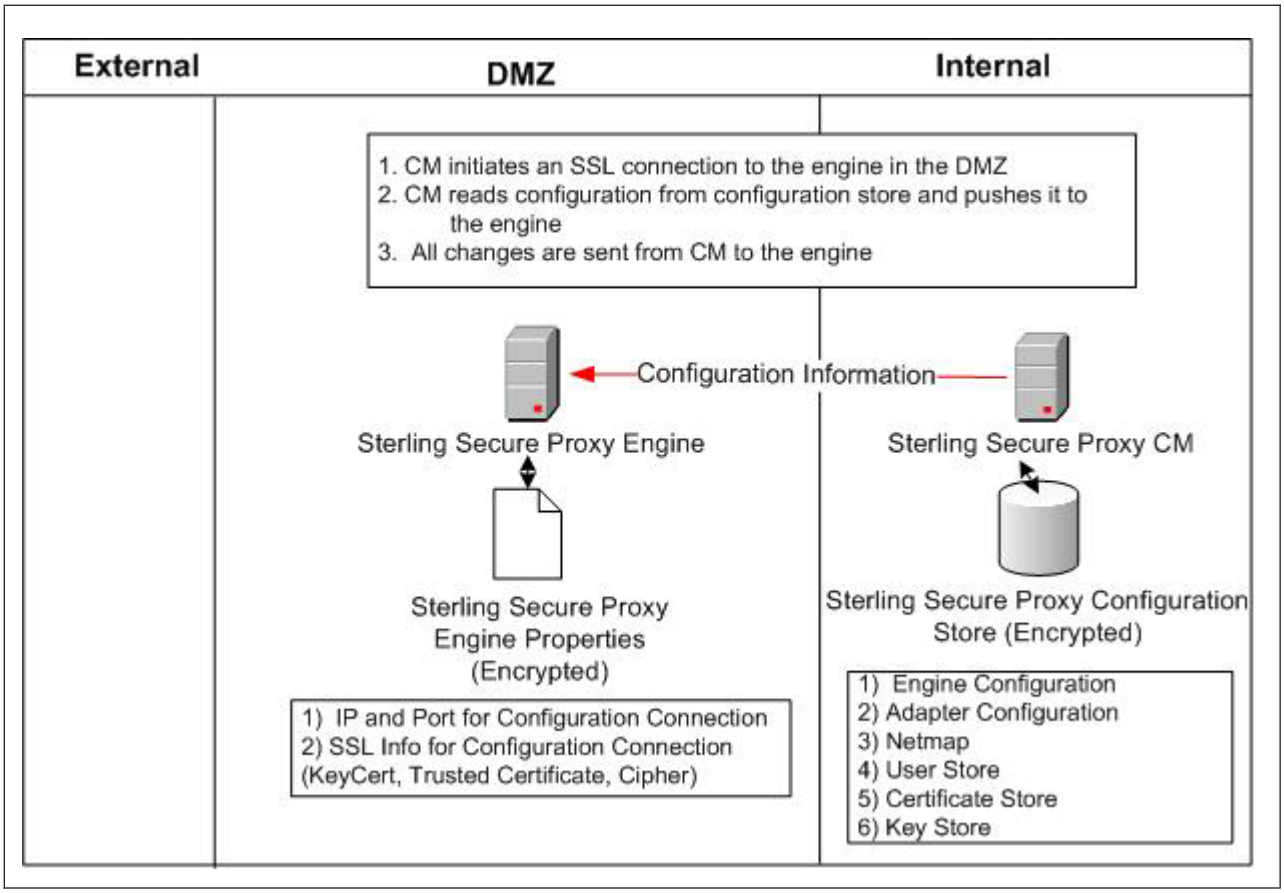
The Sterling Secure Proxy architecture requires that only the minimum amount of configuration information be stored in the DMZ. It includes two components: the Configuration Manager (CM) and an engine. Configuration data is stored at CM, is encrypted, and does not require a database. CM is installed on the internal or trusted network.

The engine resides in the DMZ and receives configuration data from CM. The engine stores engine properties on disk in the DMZ, and the files are encrypted. The engine properties contain the minimum information required to accept and secure a connection from CM. It includes the IP address and port that the Sterling Secure Proxy engine listens on for the CM connection. It also includes the SSL key certificate, trusted certificate, and encryption cipher that will be used to secure the connection with CM.

When the engine is first started, it does not have configuration information. It listens on the configured IP address and port for a connection from CM, which tries to connect to the engine at a configurable interval. When CM connects to the engine, they negotiate an SSL session and secure the connection.

After the channel is secure, CM pushes the configuration to the engine. The engine reads the configuration and starts the appropriate proxy services. When you update a configuration in CM, CM transfers the updates to the engine.

Following is an illustration of the Sterling Secure Proxy flow of a configuration push:


External
DMZ
Internal
1. CM initiates an SSL connection to the engine in the DMZ
2. CM reads configuration from configuration store and pushes it to the engine
3. All changes are sent from CM to the engine
Configuration Information
Sterling Secure Proxy Engine
Sterling Secure Proxy CM
Sterling Secure Proxy Engine Properties (Encrypted)
1) IP and Port for Configuration Connection
2) SSL Info for Configuration Connection
(KeyCert, Trusted Certificate, Cipher)
Sterling Secure Proxy Configuration Store (Encrypted)
1) Engine Configuration
2) Adapter Configuration
3) Netmap
4) User Store
5) Certificate Store
6) Key Store

Chapter 7. Using Digital Certificates

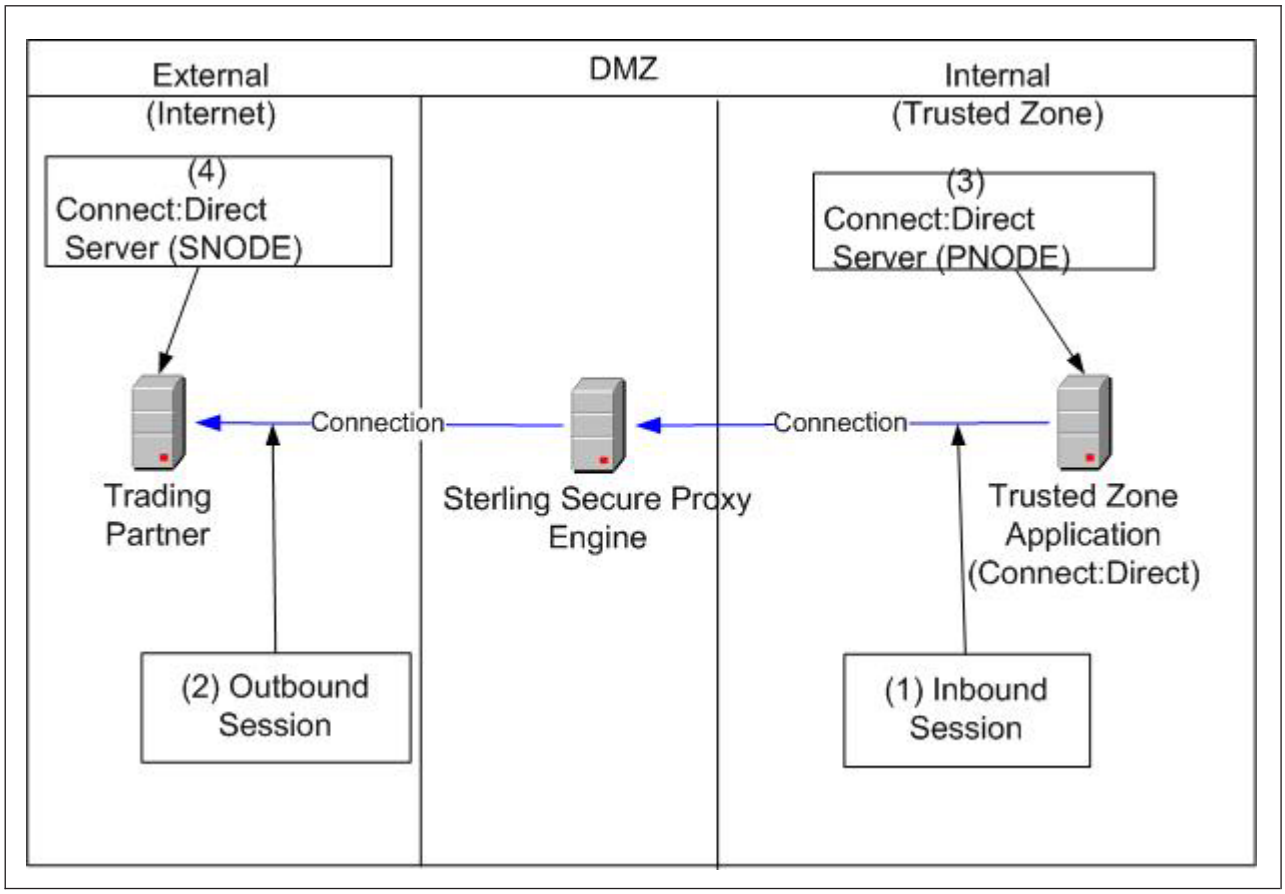
Sterling Secure Proxy uses X.509 digital certificates for secure data transport. Before you set up trading partner information, you must obtain and check in any digital certificates. Certificates can be stored in the Sterling Secure Proxy store or on a Hardware Security Module (HSM). An HSM is a hardware-based security device that generates, stores, and protects cryptographic keys. Sterling Secure Proxy provides support for the Safenet and Thales HSMs.

After you store system certificates on the HSM and import information about the system certificates stored on the HSM to the Sterling Secure Proxy store, all system certificates, including those in the store and on an HSM, are displayed and available when you configure Sterling Secure Proxy.

Chapter 8. About a Forward Proxy

A forward proxy participates in connections that originate from the trusted zone. The client in the trusted zone connects to the forward proxy in the DMZ and the forward proxy sends connection information to the destination application at the remote trading partner. Sterling Secure Proxy provides forward proxy services for Sterling Connect:Direct servers when the node in the trusted zone initiates a session to a server at a remote trading partner.

Following is an illustration of Sterling Secure Proxy, labeled with forward proxy terminology.



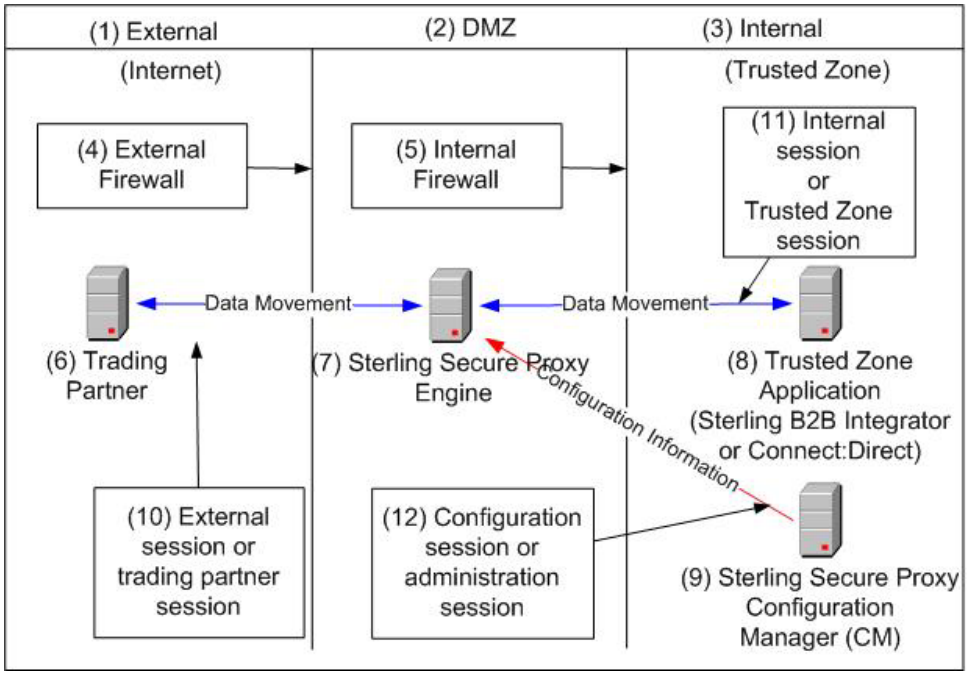
The following table describes forward proxy terminology used in the illustration.

	Term	Description
1	Inbound Session	The session between the Sterling B2B Integrator or Sterling Connect:Direct application in the trusted zone and Sterling Secure Proxy and is inbound to Sterling Secure Proxy.

	Term	Description
2	Outbound Session	The session between Sterling Secure Proxy and the remote trading partner. It is outbound from Sterling Secure Proxy.
3	Sterling Connect:Direct PNODE	The Sterling Connect:Direct node in the trusted zone that initiates the session.
4	Sterling Connect:Direct SNODE	The Sterling Connect:Direct server at the trading partner.

Chapter 9. General Proxy Terminology

Following is an illustration of the Sterling Secure Proxy general proxy environment:



The following table describes the terminology used in the illustration:

#	Term	Description
1	External Network (Internet)	Network providing connectivity for trading partners to your network. This network is usually the Internet and is called the Internet in this documentation. The external network can also be a private network.
2	DMZ	The part of the network that is neither the internal network nor the Internet. It is a network between the two networks. Sterling Secure Proxy is deployed in the DMZ and provides authentication before a trading partner can access information in the trusted zone.
3	Internal Network (Trusted Network or Trusted Zone)	The internal network behind the internal firewall and secure from outside networks.
4	External Firewall (Outer Firewall)	The firewall between the public network (Internet) and DMZ.
5	Internal Firewall (Inner Firewall)	The firewall between the DMZ and trusted zone.

#	Term	Description
6	Trading Partner	The external entity that you do business with. Trading partner may also be referred to as remote trading partner, external trading partner, or remote client.
7	Sterling Secure Proxy Engine	Sterling Secure Proxy includes two parts: an Sterling Secure Proxy engine and Configuration Manager (CM). The engine is deployed in the DMZ. It authenticates trading partners and information that is transmitted between the trading partner and trusted zone.
8	Trusted Zone Application	The application in the trusted zone with which the trading partners exchanges information. It is either Sterling B2B Integrator or a Sterling Connect:Direct server. It is also called the end point, destination node, or internal application.
9	Sterling Secure Proxy Configuration Manager (CM)	Sterling Secure Proxy includes two components: an engine and CM. CM resides in the trusted zone and configures the engine to perform its duties.
10	External Session (Trading Partner session)	The session between the remote trading partner and Sterling Secure Proxy.
11	Internal Session (Trusted Zone session)	The session between Sterling Secure Proxy and the trusted zone application.
12	Configuration Session (Administration session)	The session between CM and the engine that CM is configuring. This session is used by CM to push the configuration to the engine.

Chapter 10. IP Address Checking (Netmap Check)

IP address checking validates the IP address of the trading partner and makes sure that the IP address is an allowed address. You perform IP address checking with Sterling Secure Proxy or through Sterling External Authentication Server, with the following options:

- Inbound Node List for the FTP, HTTP, and SFTP protocols—Use Sterling Secure Proxy to validate the IP address from which a remote trading partner connects. When a trading partner connects to Sterling Secure Proxy, Sterling Secure Proxy looks up the IP address in the inbound node list of the netmap. If the IP address is not found, the session ends.

  You can specify wildcard characters in the inbound node list, to provide the flexibility to be as granular in your check as you require. For example, you can specify an entry of * in the inbound node list. This value allows connections from all IP addresses. If you specify an IP address for each trading partner in the inbound node list, only connections from the client IP addresses identified are allowed. The more specific the IP address is in the inbound node list, the stricter the IP address check is.
- Netmap Check for Sterling Connect:Direct—For Sterling Connect:Direct connections, the netmap contains one node list that is used for both inbound and outbound nodes. Sterling Connect:Direct does not use the IP address to find the netmap entry to use. It uses the node name provided by the initiating node (PNODE). However, a parameter in the Sterling Connect:Direct adapter allows you to check the IP address of the initiating node.
- External Authentication (recommended)—Validate the IP address using Sterling External Authentication Server to perform certificate or user validation. If Sterling Secure Proxy is configured to use Sterling External Authentication Server for user or certificate authentication, it sends the IP address to Sterling External Authentication Server, Sterling External Authentication Server validates the IP address and determines if the IP address is valid for a user or for a certificate subject name, common name, or other specified values in the certificate.

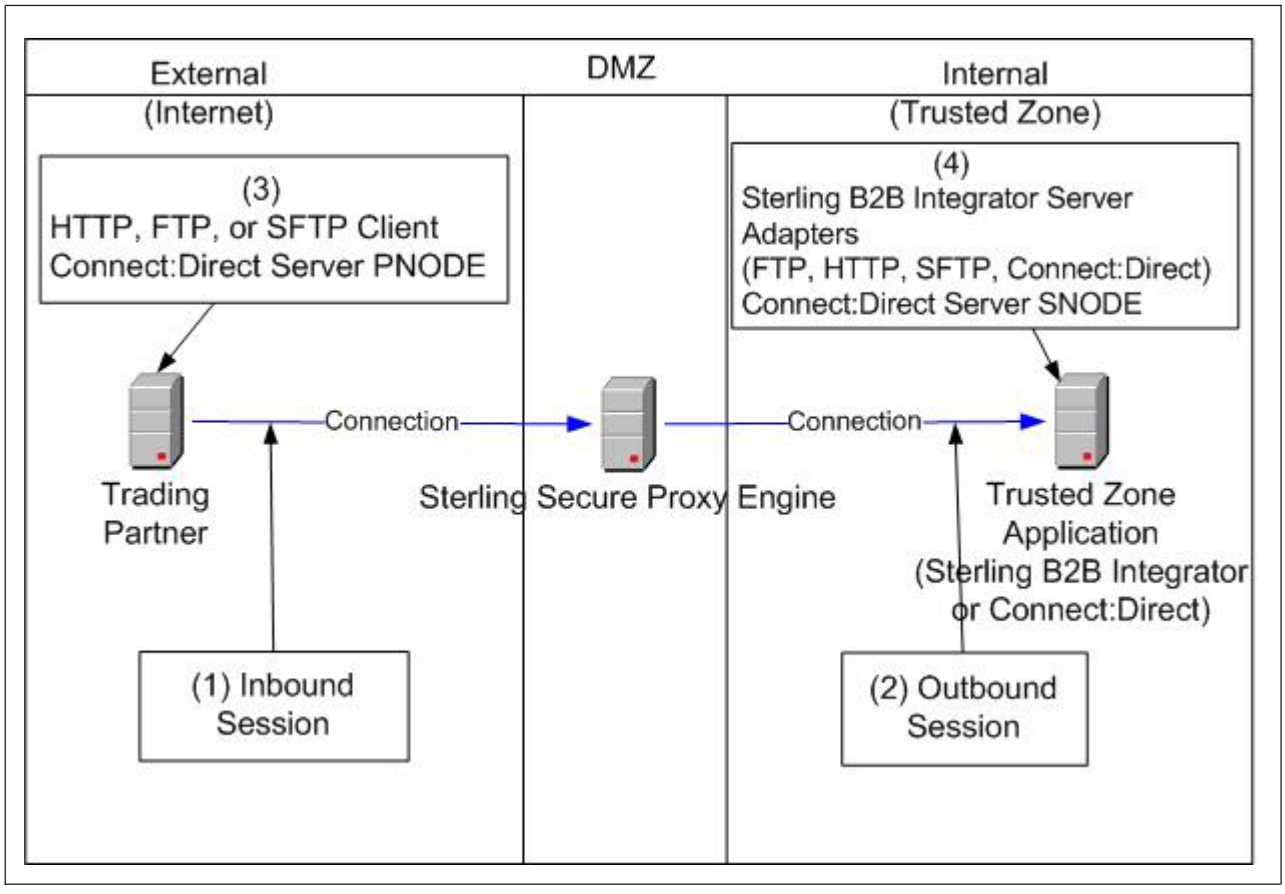
Chapter 11. About a Reverse Proxy

A reverse proxy acts on behalf of a trusted zone application. The trading partner or remote client initiates a connection to a trusted zone application and is connected to a reverse proxy.

Sterling Secure Proxy provides reverse proxy services for Sterling B2B Integrator when the trading partners initiate FTP, HTTP, SFTP, and Sterling Connect:Direct sessions to the Sterling B2B Integrator server in the trusted zone.

Sterling Secure Proxy provides reverse proxy services for Sterling Connect:Direct servers when the trading partners initiate Sterling Connect:Direct sessions to Sterling Connect:Direct servers in the trusted zone.

Following is an illustration of Sterling Secure Proxy, labeled with reverse proxy terminology.



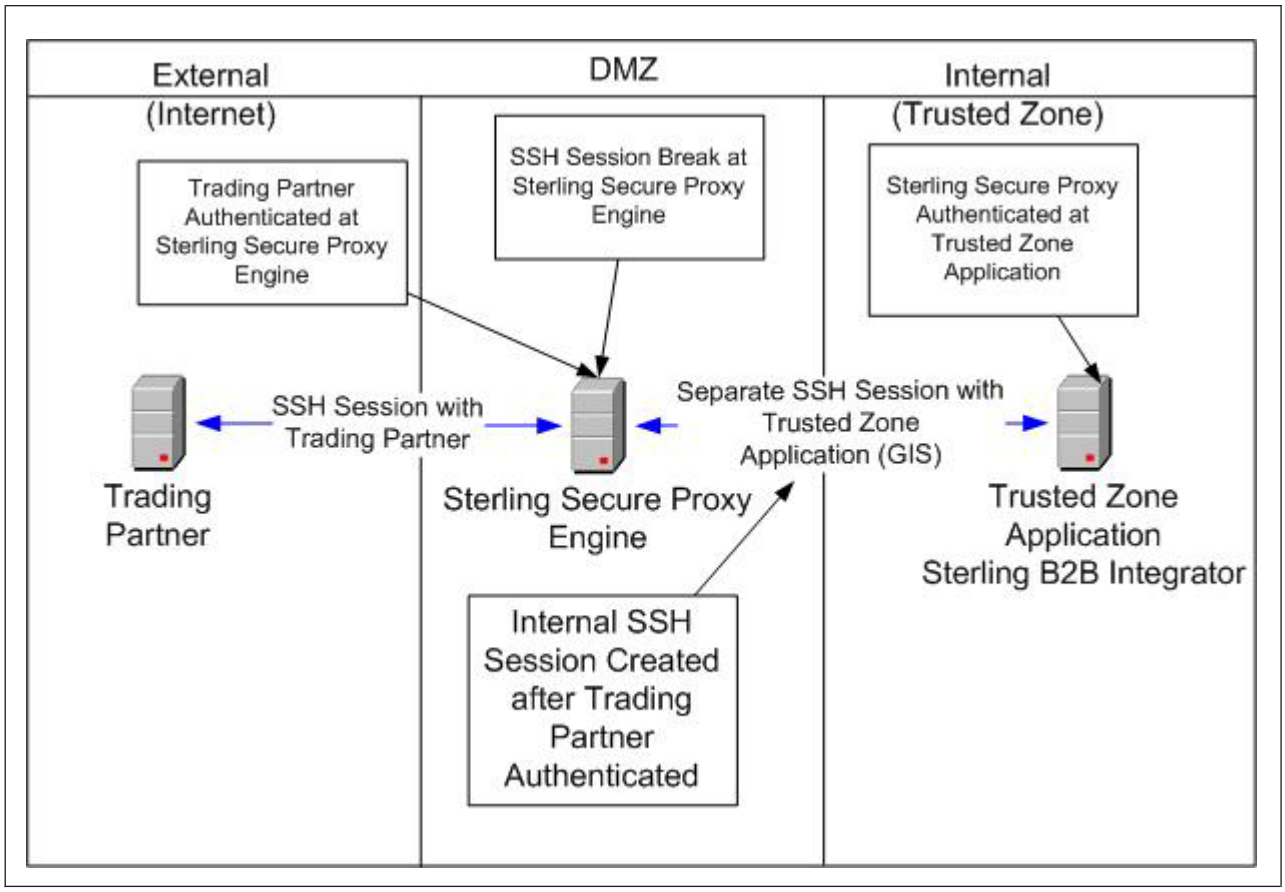
The following table explains the reverse proxy terminology used in the illustration.

#	Term	Description
1	Inbound Session	The session between the remote trading partner and Sterling Secure Proxy. It is inbound to Sterling Secure Proxy.
2	Outbound Session	The session between Sterling Secure Proxy and the Sterling B2B Integrator or Sterling Connect:Direct application in the trusted zone. It is outbound from Sterling Secure Proxy.
3	Client or Sterling Connect:Direct PNODE	The trading partner. It can be an HTTP, FTP, SFTP, or Sterling Connect:Direct client. For Sterling Connect:Direct implementations, the client is the PNODE or the initiating node.
4	Server Adapters or Sterling Connect:Direct SNODE	The Sterling B2B Integrator server in the trusted zone. The adapters at Sterling B2B Integrator are the HTTP server adapter, FTP server adapter, SFTP server adapter, and the Sterling Connect:Direct server adapter (SNODE). For Sterling Connect:Direct implementations, the trusted zone server is the SNODE.

Chapter 12. About SSH Session Break

Just as Sterling Secure Proxy creates an SSL session break for the HTTP, FTP, and Sterling Connect:Direct protocols, it creates an SSH session break when using the SFTP protocol. The SSH session break occurs because the trading partner connects to Sterling Secure Proxy in the DMZ and not to the application in the trusted zone. The trading partner is unaware that Sterling Secure Proxy is deployed and believes it is connecting to your backend system. Sterling Secure Proxy negotiates an SSH session with the remote trading partner and authenticates the trading partner's key and/or password as part of the SSH negotiation. After the SSH session is established, Sterling Secure Proxy initiates a separate SSH session to the application in the trusted zone. After the application in the trusted zone authenticates Sterling Secure Proxy using key and/or password authentication, Sterling Secure Proxy relays messages between the trading partner connection and the trusted zone application connection to allow the remote trading partner to move data into and out of the trusted zone application.

Following is a sample flow of an SSH session break:

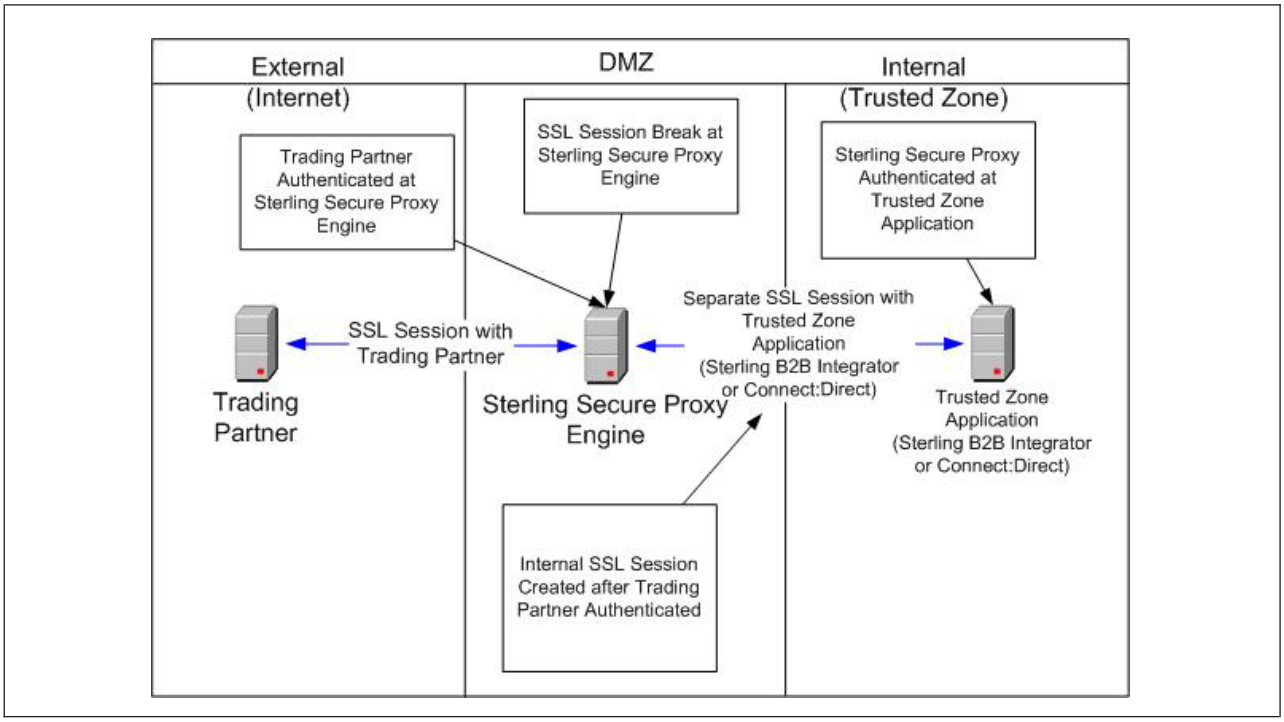


Chapter 13. About SSL Session Break

The SSL session break is a primary Sterling Secure Proxy security feature. Sterling Secure Proxy authenticates a remote trading partner in the DMZ, before creating a separate SSL session into the trusted zone. This allows you to create firewall rules to prevent trading partners from obtaining direct access to your application in the trusted zone. It also allows you to keep sensitive data out of the DMZ.

The SSL session break occurs because the trading partner connects to Sterling Secure Proxy in the DMZ and not to the application in the trusted zone. The trading partner is unaware that Sterling Secure Proxy is deployed and believes it is connecting to your backend system. Sterling Secure Proxy negotiates an SSL session with the remote trading partner and authenticates the trading partner's certificate, if SSL client authentication is configured. Sterling Secure Proxy then enforces user authentication to validate that the trading partner uses a valid user ID and password. After the SSL session is established and the user ID and password is authenticated, Sterling Secure Proxy initiates a separate SSL session to the application in the trusted zone. After the application in the trusted zone authenticates Sterling Secure Proxy using SSL client authentication and user ID and password authentication, Sterling Secure Proxy communicates messages between the trading partner and trusted zone application connection to allow the remote trading partner to move data into and out of the trusted zone application.

Following is a sample SSL session break flow:



Chapter 14. Summary of Authentication

Sterling Secure Proxy provides flexibility in how you authenticate users and connections.

The table below summarizes the options available in Sterling Secure Proxy and the factor of authentication for each. Recommended options are in bold.

	SSL Client Authentication Enforced			**SSL Client Authentication Not Enforced**		
	No User Authentication	**Users Authenticated Locally**	Users Authenticated using Sterling External Authentication Server	**No User Authentication**	**Users Authenticated Locally**	Users Authenticated using Sterling External Authentication Server
Pass Through User Credentials	Single factor authentication in DMZ (SSL client auth only)	Multi-factor authentication in DMZ	**Multi-factor authentication in DMZ** (recommended)	No authentication in DMZ	Single factor authentication in DMZ (user auth only)	Single factor authentication in DMZ (user auth only)
Outbound User Credentials Mapped from Sterling External Authentication Server	N/A	N/A	**Multi-factor authentication in DMZ**	N/A	N/A	Single factor authentication in DMZ (user auth only)
	No User Authentication	Users Authenticated Locally	Users Authenticated using Sterling External Authentication Server	**No User Authentication**	**Users Authenticated Locally**	**Users Authenticated using Sterling External Authentication Server**
Outbound User Credentials from Outbound Node in Netmap	Single factor authentication in DMZ (SSL client auth only.) All users look the same at Sterling B2B Integrator or Sterling Connect:Direct in trusted zone.	Multi-factor authentication in DMZ. All users look the same at Sterling B2B Integrator or Sterling Connect:Direct in trusted zone.	Multi-factor authentication in DMZ. All users look the same at Sterling B2B Integrator or Sterling Connect:Direct in trusted zone.	No authentication in DMZ. All users look the same at Sterling B2B Integrator or Sterling Connect:Direct in trusted zone.	No authentication in DMZ. All users look the same at Sterling B2B Integrator or Sterling Connect:Direct in trusted zone.	Single Factor authentication in DMZ (user authentication only.) All users look the same at Sterling B2B Integrator or Sterling Connect:Direct in trusted zone.

Chapter 15. User Authentication Options

Three methods of user authentication allow the flexibility to choose how to authenticate users:

- No user authentication
- Authenticate users locally
- Authenticate users using Sterling External Authentication Server

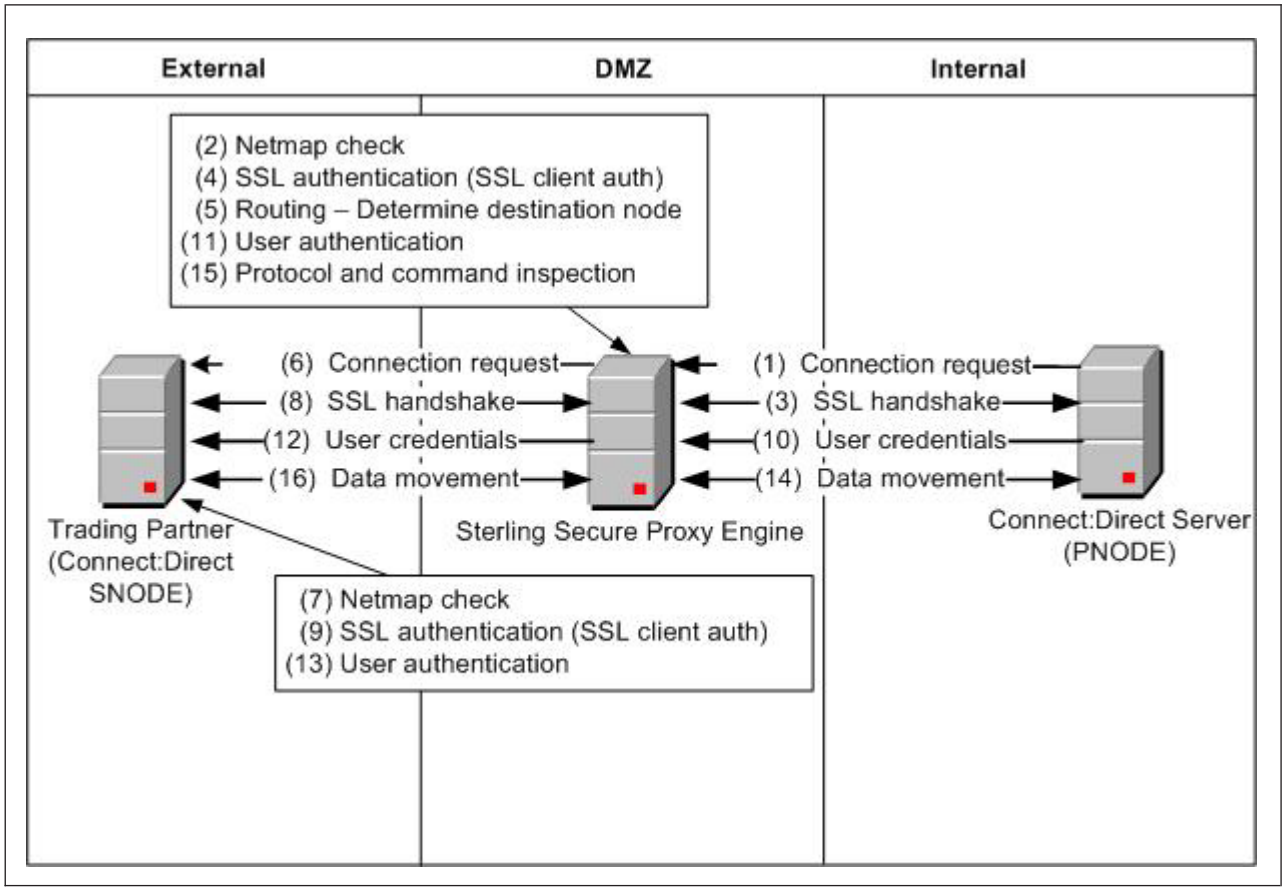
Authenticate using Sterling External Authentication Server is the most secure option. Following is a description of the user authentication methods:

Option	Description
Authenticate Users With Sterling External Authentication Server (Recommended)	Select this option to perform external user authentication, using Sterling External Authentication Server, This option sends the user credentials presented by the client to Sterling External Authentication Server for authentication. Sample user authentication validations that Sterling External Authentication Server can perform include: • Through LDAP to bind to user in LDAP • Through Tivoli Access Manager • Through a customer java exit Choose this option to enforce the following security policy requirements: • To maintain users in an application that is external to Sterling Secure Proxy • You have an existing infrastructure to validate users against • To use the user mapping provided by Sterling External Authentication Server, refer to the Sterling Secure Proxy documentation library • To implement multi-factor authentication and bind the factors together in the LDAP infrastructure
Authenticate Users Locally	Select this option to authenticate users using information in the Sterling Secure Proxy local user store. This option requires you to maintain the users in the Sterling Secure Proxy configuration. Select this option for the following security requirements: • To store and maintain users in the Sterling Secure Proxy user store. • No external infrastructure exists for user authentication to interface with.

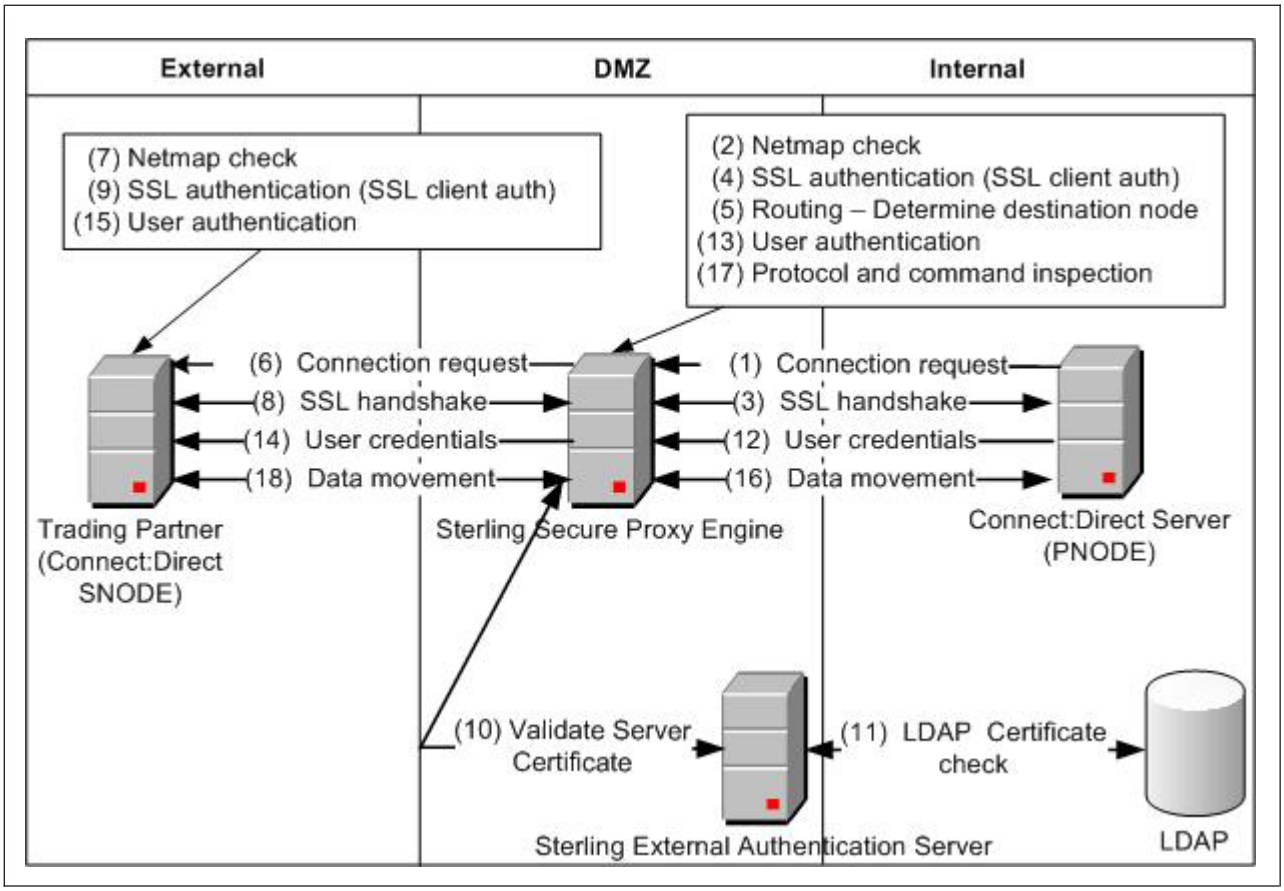
Option	Description
No User Authentication	Select this option if you do not want to validate trading partner credentials in the DMZ. If you select this method, we recommend that you enforce SSL client authentication to provide at least one factor of authentication in the DMZ. If you select no user authentication, you may pass the user credentials through to the destination node in the internal network and validate the user credentials at the internal network. Choose this option to enforce the following security policy requirements: • Enforce single factor authentication in the DMZ and authenticate the trading partner using SSL client authentication. Pass the user credentials to Sterling B2B Integrator or Sterling Connect:Direct trusted zone application so it will authenticate the user and differentiate between users accessing the system. • Use an SSL session break or IP break in the DMZ but do not authenticate the trading partner. Do not enforce SSL client authentication or authenticate the user. Pass the user credentials to the external network in order Sterling B2B Integrator or Sterling Connect:Direct to differentiate between users accessing the system. • You implement a bulletin board type system, where user credentials are not important. This option is not a typical implementation. Carefully evaluate your environment before using this configuration.

Chapter 16. Diagram of a Finished Sterling Connect:Direct Forward Proxy Configuration

The following illustration describes the steps in a Sterling Connect:Direct forward proxy authentication:

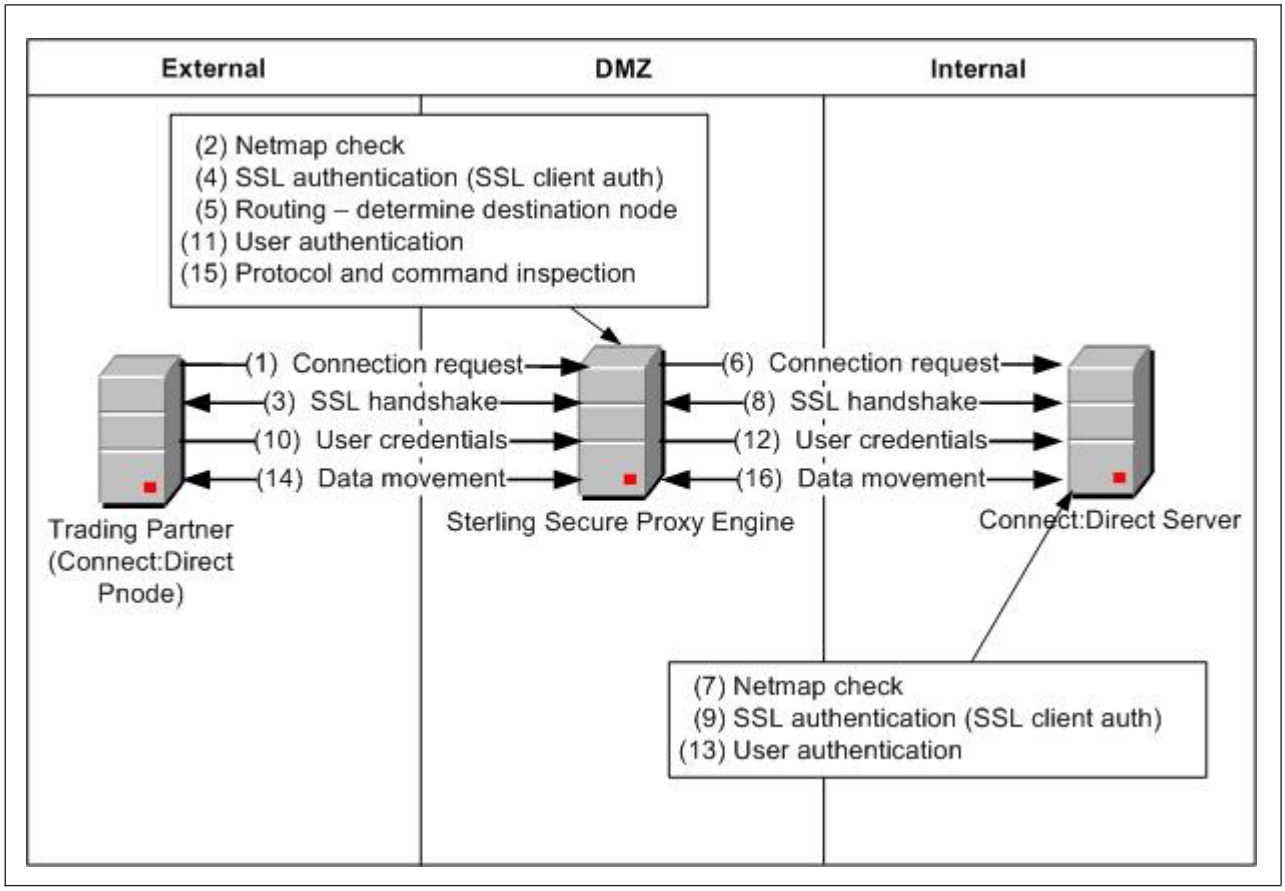


The following illustration describes the steps in a Sterling Connect:Direct forward proxy authentication using Sterling External Authentication Server:

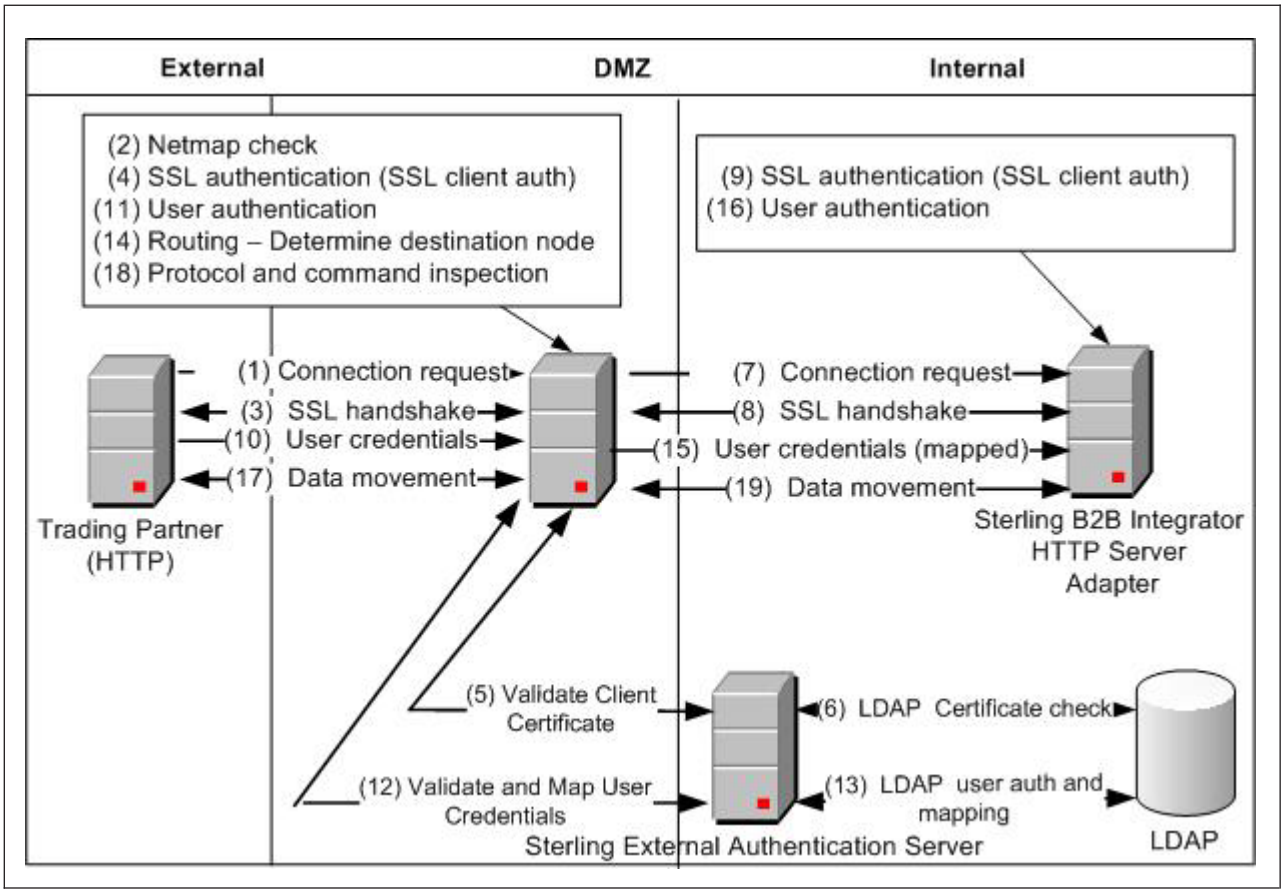

External
DMZ
Internal
(7) Netmap check
(9) SSL authentication (SSL client auth)
(15) User authentication
(2) Netmap check
(4) SSL authentication (SSL client auth)
(5) Routing – Determine destination node
(13) User authentication
(17) Protocol and command inspection
(6) Connection request
(8) SSL handshake
(14) User credentials
(18) Data movement
(1) Connection request
(3) SSL handshake
(12) User credentials
(16) Data movement
Trading Partner (Connect:Direct SNODE)
Sterling Secure Proxy Engine
Connect:Direct Server (PNODE)
(10) Validate Server Certificate
(11) LDAP Certificate check
Sterling External Authentication Server
LDAP

Chapter 17. Diagram of a Finished Sterling Connect:Direct Reverse Proxy Configuration

The following illustration describes the Sterling Connect:Direct reverse proxy authentication steps:

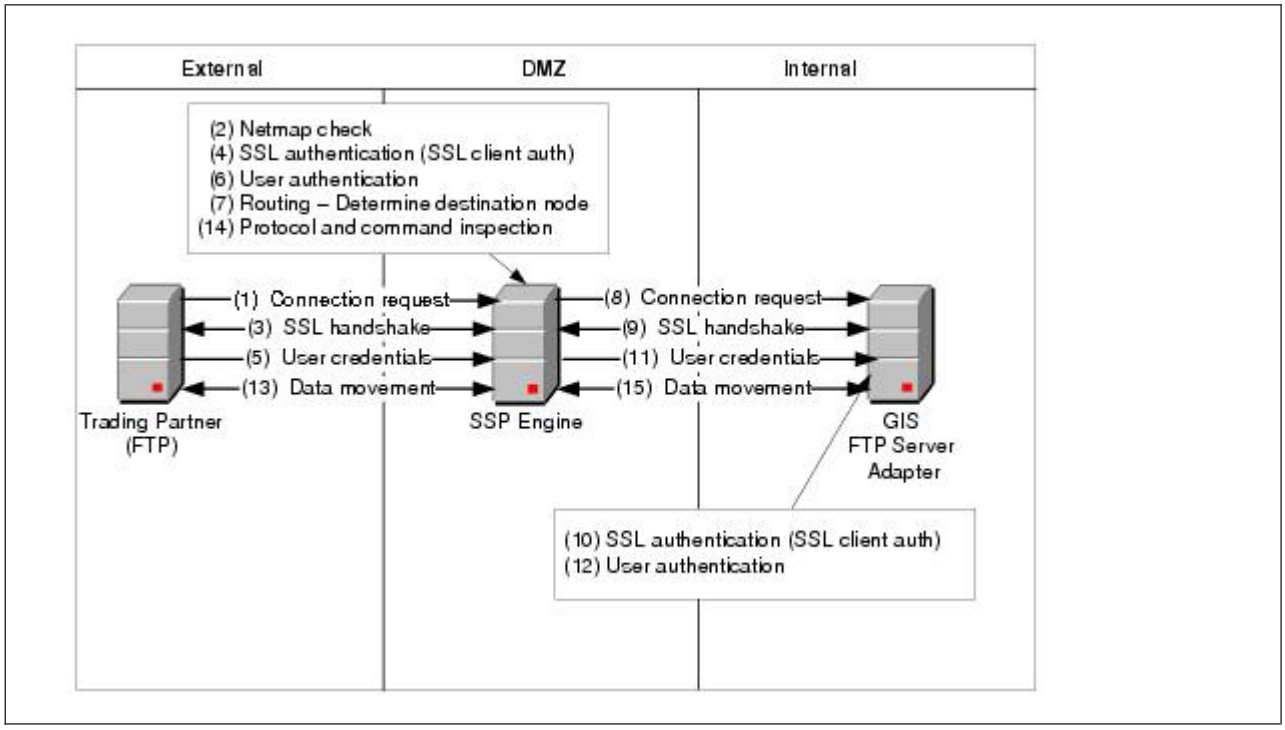


The following illustration describes a Sterling Connect:Direct reverse proxy authentication using Sterling External Authentication Server:

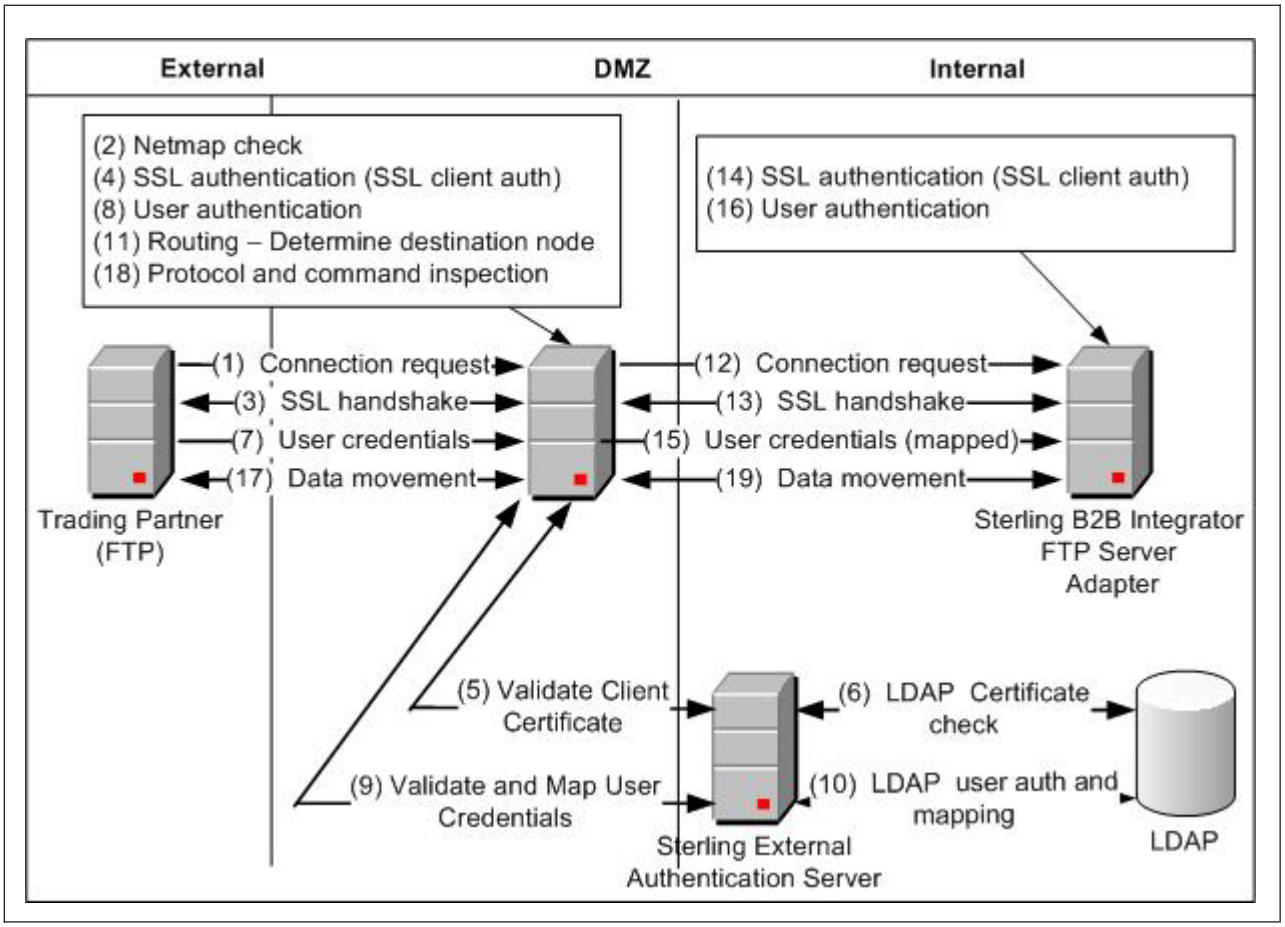

External
DMZ
Internal
(2) Netmap check
(4) SSL authentication (SSL client auth)
(11) User authentication
(14) Routing – Determine destination node
(18) Protocol and command inspection
(9) SSL authentication (SSL client auth)
(16) User authentication
(1) Connection request
(3) SSL handshake
(10) User credentials
(17) Data movement
(7) Connection request
(8) SSL handshake
(15) User credentials (mapped)
(19) Data movement
Trading Partner
(HTTP)
Sterling B2B Integrator
HTTP Server
Adapter
(5) Validate Client
Certificate
(6) LDAP Certificate check
(12) Validate and Map User
Credentials
(13) LDAP user auth and
mapping
Sterling External Authentication Server
LDAP

Chapter 18. Diagram of a Finished FTP Reverse Proxy Configuration

The following illustration describes the steps in an FTP reverse proxy authentication:

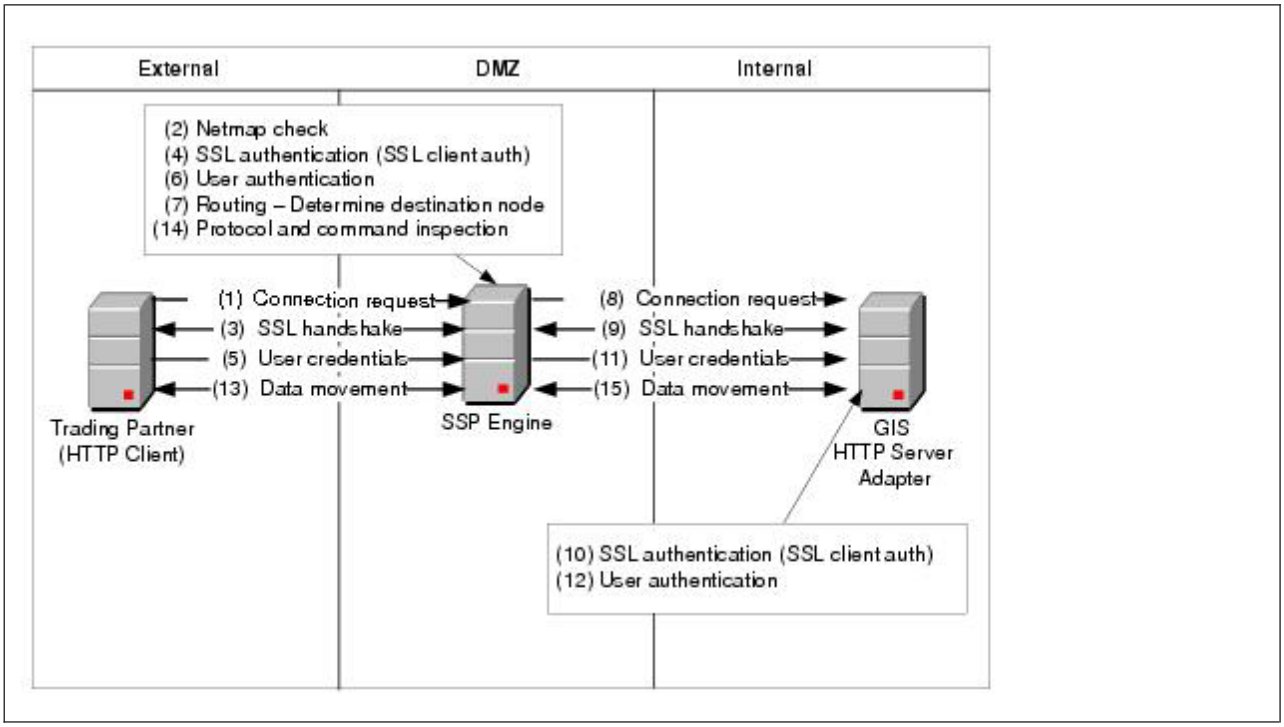


The following illustration describes the steps in an FTP reverse proxy authentication using Sterling External Authentication Server:

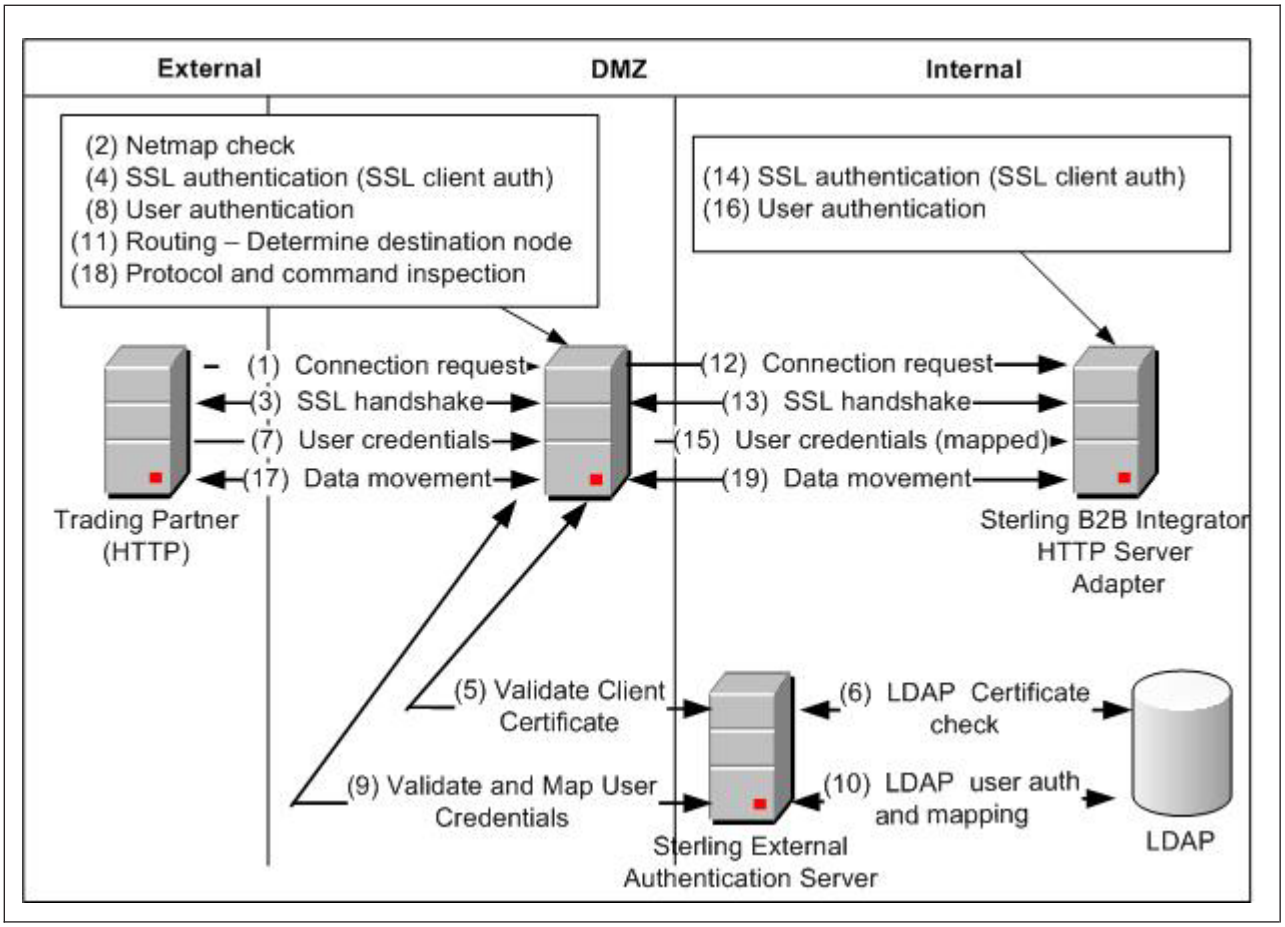

External
DMZ
Internal
(2) Netmap check
(4) SSL authentication (SSL client auth)
(8) User authentication
(11) Routing – Determine destination node
(18) Protocol and command inspection
(14) SSL authentication (SSL client auth)
(16) User authentication
(1) Connection request
(3) SSL handshake
(7) User credentials
(17) Data movement
(12) Connection request
(13) SSL handshake
(15) User credentials (mapped)
(19) Data movement
Trading Partner (FTP)
Sterling B2B Integrator FTP Server Adapter
(5) Validate Client Certificate
(6) LDAP Certificate check
(9) Validate and Map User Credentials
(10) LDAP user auth and mapping
Sterling External Authentication Server
LDAP

Chapter 19. Diagram of a Finished HTTP Reverse Proxy Configuration

The following illustration details the steps in an HTTP reverse proxy authentication:

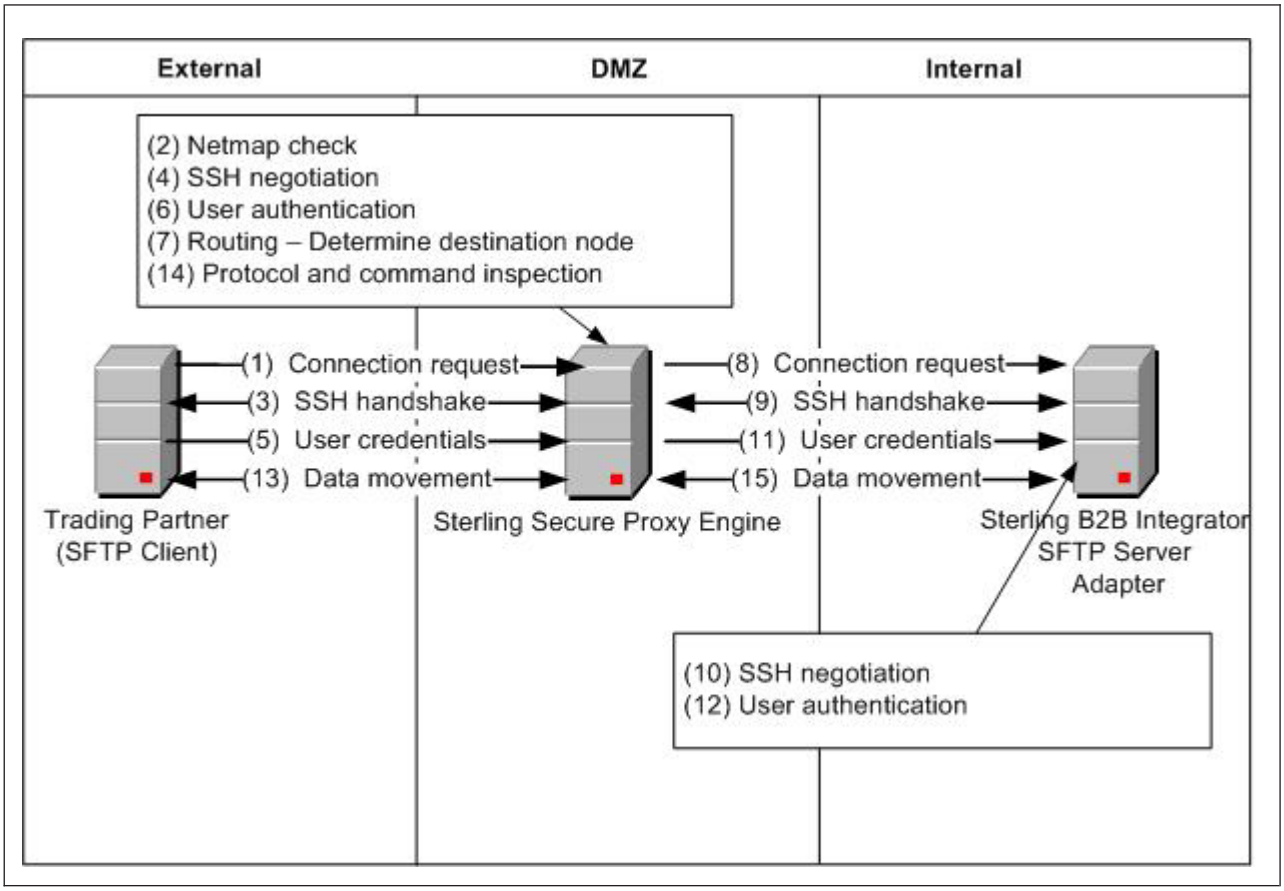


The following illustration details the steps of an HTTP reverse proxy authentication using Sterling External Authentication Server:

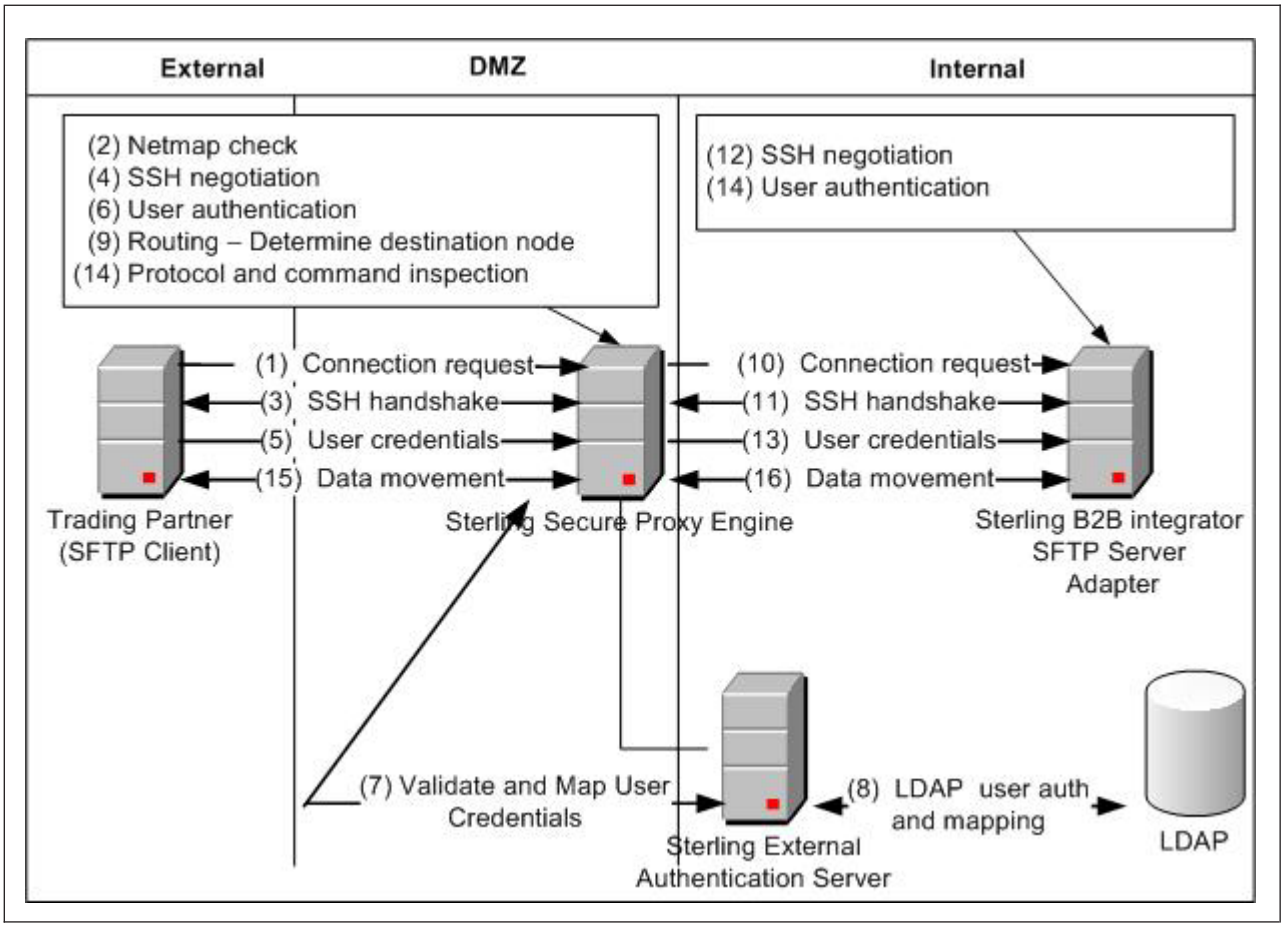

External
DMZ
Internal
(2) Netmap check
(4) SSL authentication (SSL client auth)
(8) User authentication
(11) Routing – Determine destination node
(18) Protocol and command inspection
(14) SSL authentication (SSL client auth)
(16) User authentication
(1) Connection request
(3) SSL handshake
(7) User credentials
(17) Data movement
(12) Connection request
(13) SSL handshake
(15) User credentials (mapped)
(19) Data movement
Trading Partner (HTTP)
Sterling B2B Integrator HTTP Server Adapter
(5) Validate Client Certificate
(6) LDAP Certificate check
(9) Validate and Map User Credentials
(10) LDAP user auth and mapping
Sterling External Authentication Server
LDAP

Chapter 20. Diagram of a Finished SFTP Reverse Proxy Configuration

The following illustration details the steps of an SFTP reverse proxy authentication:



The following illustration describes the steps in an SFTP reverse proxy authentication with Sterling External Authentication Server:


External
DMZ
Internal
(2) Netmap check
(4) SSH negotiation
(6) User authentication
(9) Routing – Determine destination node
(14) Protocol and command inspection
(12) SSH negotiation
(14) User authentication
(1) Connection request
(3) SSH handshake
(5) User credentials
(15) Data movement
(10) Connection request
(11) SSH handshake
(13) User credentials
(16) Data movement
Trading Partner
(SFTP Client)
Sterling Secure Proxy Engine
Sterling B2B integrator
SFTP Server
Adapter
(7) Validate and Map User
Credentials
(8) LDAP user auth
and mapping
Sterling External
Authentication Server
LDAP

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