Sterling Integrator®

Perimeter Server

Version 5.0

Sterling Commerce
An IBM Company

© Copyright 2009 Sterling Commerce, Inc. All rights reserved.
Additional copyright information is located on the Sterling Integrator Documentation Library:
http://www.sterlingcommerce.com/Documentation/SI50/homepage.htm

Contents

Chapter 1

Overview

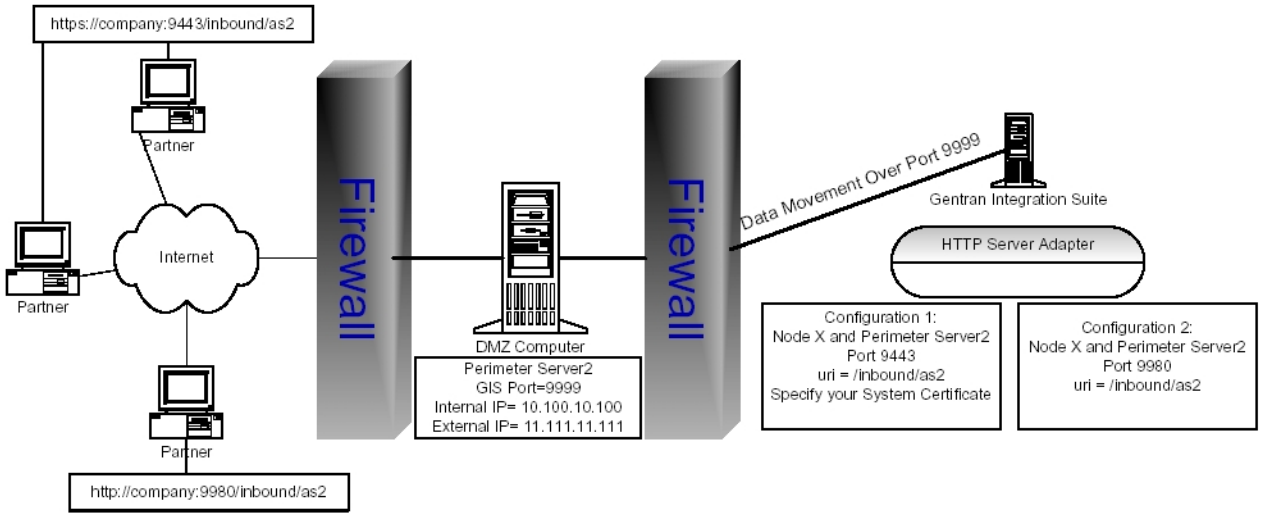
What is a Perimeter Server

A *perimeter server* is a software tool for communications management that can be installed in a DMZ. The perimeter server manages the communications flow between outer layers of your network and the TCP-based transport adapters. A perimeter server can solve problems with network congestion, security, and scalability, especially in high-volume, Internet-gateway environments.
A *perimeter network* is a computer network that is placed between a secure internal network and an unsecure external network to provide an additional layer of security. A perimeter server communicates with through perimeter services. *Perimeter services* is the Sterling Integrator subsystem supporting multihoming and secure perimeter network traversing for Sterling Integrator B2B communications protocols. A perimeter server requires a corresponding perimeter client.

Perimeter services consist of the following components:

- Perimeter server you install on your DMZ computer or in a more secure network (remote perimeter server).
- Perimeter server pre-installed in Sterling Integrator(local perimeter server).
- Perimeter services API that communications adapters in Sterling Integrator use to use the perimeter servers (local and remote) for multihoming and perimeter network traversal functionality.
- Perimeter servers configuration management components in the Sterling Integrator interface.

The following figure shows a typical Sterling Integrator installation with perimeter servers:



The preceding figure shows the following:

1. The persistent connection is established from the perimeter services API in Sterling Integrator to the remote perimeter server on the DMZ computer to communicate through port 9999.
2. Sterling Integrator has an HTTP Server adapter configured for two scenarios, one secure HTTP through port 9443 and the other non-secure HTTP through port 9980.
3. Two trading partners with separate host and port numbers to communicate with Sterling Integrator:

Perimeter servers help reduce network congestion issues and scalability for high volume environments through session and thread management, and enhance security by moving security threats further from your secure network and data.

A perimeter server and all adapters that communicate with the local perimeter server must be configured on the same Sterling Integrator node. A *node* is a single installation of Sterling Integrator . A single Sterling Integrator node can have multiple configured perimeter servers (local perimeter servers) associated with it.

You can configure a perimeter server for one trading partner that has large files and low transaction volume, and another perimeter server on the same node for a different trading partner that has smaller files and high transaction volume. By configuring each perimeter server according to the trading partner, you can increase the performance of Sterling Integrator.

All adapters installed on a specific node can use the local perimeter server configurations on the node.

For testing purposes, or when you are running Sterling Integrator without the DMZ feature, you can use the local perimeter server that is installed with Sterling Integrator.

You should use perimeter servers if you want to:

- Secure communications between the DMZ and Sterling Integrator .
- Send data to your customers from the perimeter server as the originating IP address.
- Manage security certificates on your secure network and not in a DMZ.
- Enhance performance and scalability of Sterling Integrator through session and thread management that includes a large number of connections.
- Use the following adapters or protocols:

Inbound Messages and Perimeter Servers

The following scenario describes how an incoming message is processed in Sterling Integrator running perimeter services:

1. Your trading partner sends the message across a TCP/IP connection.
2. The message arrives at the designated listening port on the computer in the DMZ.
3. The remote perimeter server on the DMZ computer sends the message through the port established for the persistent connection to the local perimeter server in Sterling Integrator to the appropriate adapter in Sterling Integrator.

Outbound Messages and Perimeter Servers

The following scenario describes how an outbound message is processed in Sterling Integrator running perimeter services:

1. Sterling Integrator sends the message to the local perimeter server through the appropriate adapter running in Sterling Integrator.
2. The local perimeter server sends the message to the remote perimeter server on the DMZ computer through the port established for the persistent connection between the DMZ and Sterling Integrator.
3. The remote DMZ perimeter server sends the message to the trading partner through a TCP/IP connection using the port specified in your trading partner agreement.
4. Your trading partner receives the message.

Perimeter Servers and Clustering

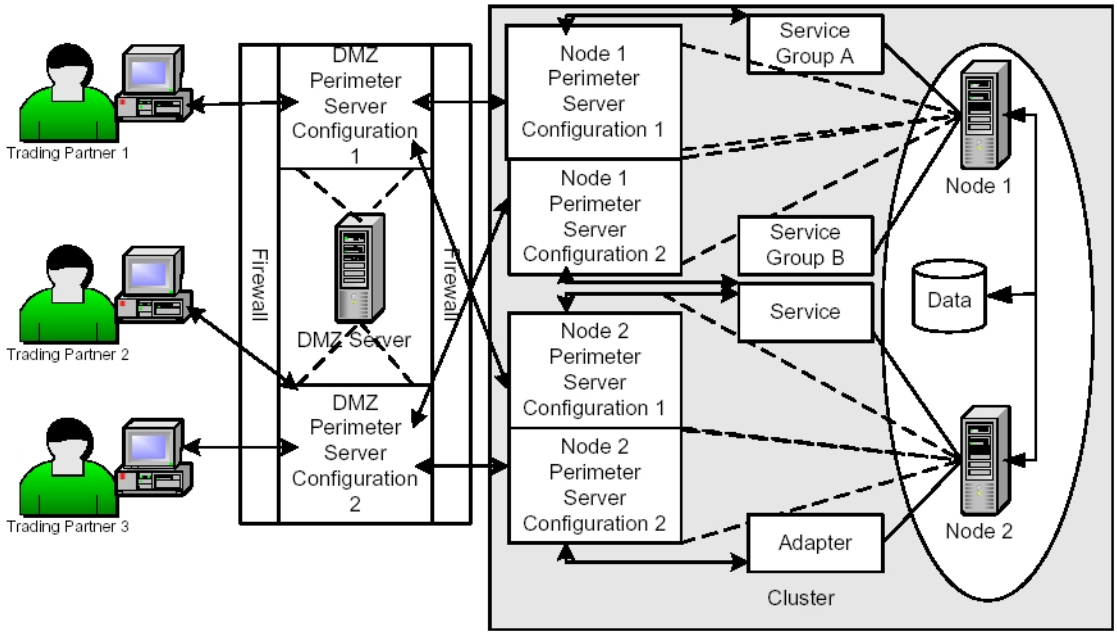
You can use perimeter servers when you install Sterling Integrator in a clustered environment. A *cluster* is two or more connected copies of Sterling Integrator that share a database. A *node* is one copy of Sterling Integrator in the cluster.

In a clustered environment, each node may have a perimeter server configured. You can have more than one perimeter server for each node, which enables you to increase the number of connections and improve processing times. However, each perimeter server can serve only one Sterling Integrator node. You can also have many different services and adapters using the same perimeter server.

You can use service groups in your Sterling Integrator cluster to enhance load balancing and failover activities. A *service group* is a group of the same service or adapter type that acts as peers. If all of the services or adapters in a service group are configured compatibly (identically, except for perimeter server selection), and one of the services in the service group is busy, another service configuration can pick up the business process and begin processing. This is load balancing. If one of the services in the service group is disabled, another service in the service group can pick up a business process and begin processing. This is failover support.

For more information about setting up a Sterling Integrator clustered environment, call Sterling Commerce Customer Support.

The following figure shows a clustered environment running perimeter servers:



The following explains the preceding figure:

1. Node 1 and Node 2 share a database in a clustered environment.
2. Node 1 includes Service Group A and Service Group B configured for use with a perimeter server:
3. Node 2 includes a service and an adapter configured for use with a perimeter server.
4. Node 1 and 2 both have two perimeter servers configured:
5. The DMZ Server has two perimeter servers configured:
6. Three trading partners are configured to communicate with the DMZ Server Perimeter Servers:

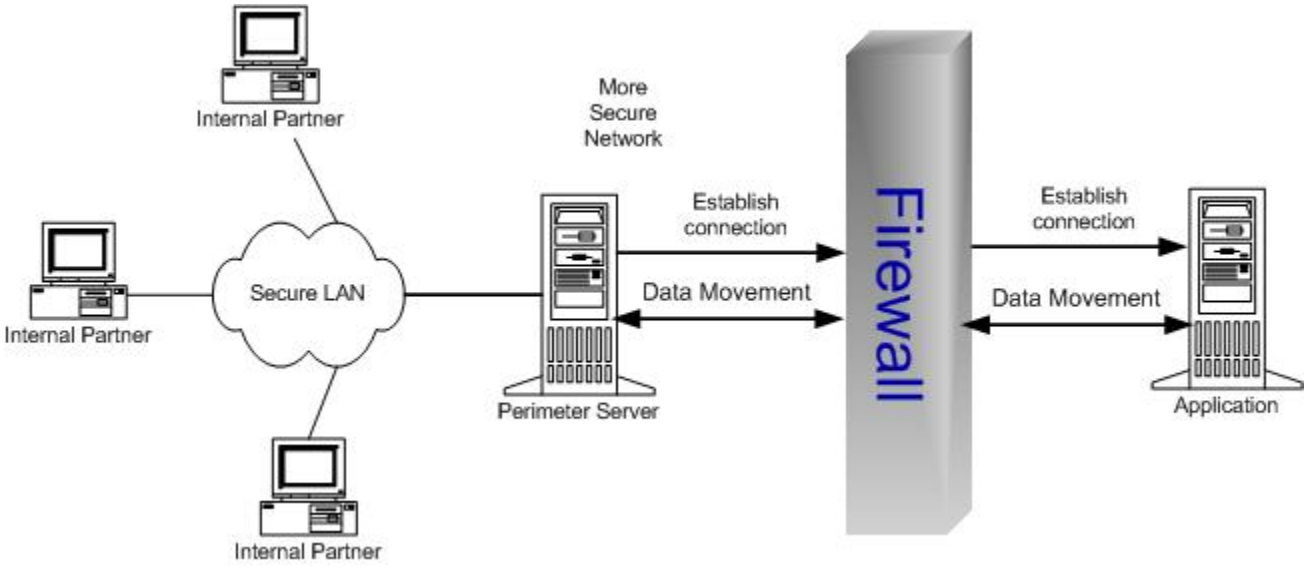
The following is an example of how a business process is routed through the preceding figure:

1. Trading Partner 1 sends a message to your cluster.
2. The message is sent through the DMZ Perimeter Server Configuration 1, which communicates with the Node 1 Perimeter Server Configuration 1 in your cluster.
3. The Node 1 Perimeter Server Configuration 1 is configured for Service Group A, which allows for load balancing and failover support. The first service configuration in Service Group A is disabled, so the second configuration receives the message and begins the processing on Node 1 in your cluster.
4. Because clustering is a way to control load balancing and scale your system, if Node 1 is too busy processing other business processes, Node 2 accepts and processes the business process.

Perimeter Servers and More Secure Networks

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

In some cases, it is desirable for Sterling Integrator to communicate to a more secure network zone. In this case you will want to establish the network connection from the perimeter server to Sterling Integrator. The following figure shows this configuration:



Perimeter Server Property Settings

Many of the property settings for perimeter servers are stored in the Properties directory of your Sterling Integrator installation.
The following properties files affect perimeter servers:

- perimeter.properties
- log.properties

For remote perimeter servers, the following property file is stored in the install directory of perimeter server:

- remote_perimeter.properties

Chapter 2

Using Perimeter Server

Add a Perimeter Server to Sterling Integrator

Before you can add a perimeter server to Sterling Integrator, you must:

- Install a perimeter server.
- Know the host name and port number of the installed perimeter server.

To add a perimeter server in Sterling Integrator:

1. From the **Administration** menu, select **Operations** > **Perimeter Servers**.
2. On the Perimeter Servers page, next to New Perimeter Server, click **add**.
3. On the Perimeter Server Configuration page, complete the following fields and click **Next**.

Field	Description
Name	Name you provided of the perimeter server to connect to.
Near End Configuration **Note** The Near End Configuration fields are useful in environments involving firewalls with rules designed to only allow specific IP addresses, ports, or both to create outbound connections. However, this is not permitted in iSeries (OS/400) environments, and an ephemeral port is chosen to make the connection instead. Consider this when configuring firewall rules in iSeries environments by not restraining the outbound connections to a port number.	
Interface Or IP	DNS name or IP address of the computer that you typed when you installed the perimeter server. Type***** (wildcard) to allow Sterling Integrator to establish this value. This interface will be used for the near end of the persistent connection to the perimeter server. Specify it only if your machine has multiple interfaces and not all are able to connect to your DMZ. **Note** Do not use in iSeries (OS/400) environments.
Local Port	Port number that you chose when you installed the perimeter server. Type **0** (zero) to allow Sterling Integrator to establish this value. This port will be used for the near end of the persistent connection to the perimeter server. Specify a port other than **0** (zero) only if your firewall controls access to the DMZ based on the originating port. Specifying **0** (zero) allows Sterling Integrator to choose any available port. **Note** Do not use in iSeries (OS/400) environments.

Field	Description
Perimeter Server (far-end) is in less secure network zone	Check this to enable the connection from Sterling Integrator to the perimeter server. To connect in the opposite direction, clear the checkbox.
Perimeter Server Host	DNS name or TCP/IP address of the computer that the remote perimeter server is installed on. If you specified an internal interface during your perimeter server installation, use that address here.
Perimeter Server Port	Port number that the remote perimeter server monitors for connections. This is the port number you specified when installing your remote perimeter server.
Cluster Node	Node that is to be used with this perimeter server, if you are running in a clustered environment. If you are running in a clustered environment. If you are not running in a clustered environment, you must select the local node (node1) from the list.

4. On the High/Low Watermarks page, complete the following fields and click **Next**.

Field	Description
Note	You can set specific watermark parameters for each trading partner, by adding a perimeter server for each trading partner and configuring the perimeter server to match the trading volume and document size for each trading partner. This enables you to allocate more system memory to your trading partners with which you trade larger volumes and larger files. By allocating more or less memory to a trading partner, you can increase performance.
Inbound Connection	
High	Highest inbound connection buffer size. This is the high watermark. When a trading partner sends data faster than Sterling Integrator can process it, the excess data accumulates inside perimeter services in the inbound connection buffer. When the buffer size reaches the **High Inbound Connection** value, perimeter services stops receiving data for that connection until enough of the excess data has been processed that the inbound connection buffer size drops to the **Low Inbound Connection** value. For example, if you set the **High Inbound Connection** value to 500 KB and the **Low Inbound Connection** value to 250 KB, perimeter services will stop receiving data when the inbound connection buffer size reaches 500 KB and will resume receiving data when the inbound connection buffer size drops to 250 KB.
Low	Lowest inbound connection buffer size. This is the low watermark. When a trading partner sends data faster than Sterling Integrator can process it, the excess data accumulates inside perimeter services in the inbound connection buffer. When the buffer size reaches the **High Inbound Connection** value, perimeter services stops receiving data for that connection until enough of the excess data has been processed that the inbound connection buffer size drops to the **Low Inbound Connection** value. For example, if you set the **High Inbound Connection** value to 500 KB and the **Low Inbound Connection** value to 250 KB, perimeter services will stop receiving data when the inbound connection buffer size reaches 500 KB and will resume receiving data when the inbound connection buffer size drops to 250 KB.
Outbound Connection	

Field	Description
High	Highest outbound connection buffer size. This is the high watermark. When Sterling Integrator sends data to a trading partner faster than the trading partner can receive it, the excess data accumulates inside perimeter services in the outbound connection buffer. When the buffer size reaches the **High Outbound Connection** value, perimeter services stops sending data through that connection until enough of the excess data has been sent that the outbound connection buffer size drops to the **Low Outbound Connection** value. For example, if you set the **High Outbound Connection** value to 500 KB and the **Low Outbound Connection** value to 250 KB, perimeter services will stop sending data when the outbound connection buffer size reaches 500 KB and will resume sending data when the outbound connection buffer size drops to 250 KB.
Low	Lowest outbound connection buffer size. This is the low watermark. When Sterling Integrator sends data to a trading partner faster than the trading partner can receive it, the excess data accumulates inside perimeter services in the outbound connection buffer. When the buffer size reaches the **High Outbound Connection** value, perimeter services stops sending data through that connection until enough of the excess data has been sent that the outbound connection buffer size drops to the **Low Outbound Connection** value. For example, if you set the **High Outbound Connection** value to 500 KB and the **Low Outbound Connection** value to 250 KB, perimeter services will stop sending data when the outbound connection buffer size reaches 500 KB and will resume sending data when the outbound connection buffer size drops to 250 KB.

5. On the Confirm page, verify your selections and click **Finish**.

   The perimeter server is added to Sterling Integrator. You can now monitor the perimeter server using the Troubleshooter page. View the perimeter server log using the System Logs page. Monitor the remote perimeter server using the perimeter server log on the remote server.

Edit a Perimeter Server Configuration in Sterling Integrator

After you add a perimeter server configuration to Sterling Integrator, you can edit the configuration to meet your changing business needs. You may need to edit a perimeter server if the host name or port number that the perimeter server is installed on changes.

To edit a perimeter server configuration:

1. From the **Administration** menu, select **Operations > Perimeter Servers**.
2. On the Perimeter Servers page, next to the perimeter server you want to edit, click **edit**.
3. On the Perimeter Server Configuration page, make the appropriate changes to the **Far End Configuration** and **Near End Configuration** fields and click **Next**.
4. On the High/Low Watermarks page, make the appropriate changes to the **Inbound Connection**and **Outbound Connection**watermark fields and click **Next**.
5. On the Confirm page, verify the configuration changes and click **Finish**.

Edit a Remote Perimeter Server in a UNIX Environment

You may need to change the IP addresses or the port number that you entered when you installed the remote perimeter server configuration.

To edit a remote perimeter server configuration:

1. On the remote computer, in the *install_dir* , run **stopPs.sh** to stop the perimeter server.
2. Locate the *install_dir* /**remote_perimeter.properties** file.
3. Open **remote_perimeter.properties** in a text editor and make the appropriate changes to the script:
4. Save **remote_perimeter.properties** without changing the name of the file.
5. In *install_dir* ,run **startupPs.sh** to start the perimeter server.

Edit a Remote Perimeter Server in a Windows Environment

You may need to change the IP addresses or the port number that you entered when you installed the remote perimeter server configuration.

To edit a remote perimeter server configuration in a Windows environment:

1. On the DMZ computer, in the *install_dir* , run **stopPs.cmd** to stop the perimeter server.
2. Locate the *install_dir* **remote_perimeter.properties** file.
3. Open **remote_perimeter.properties** in a text editor and make the appropriate changes to the script:
4. Save **remote_perimeter.properties** without changing the name of the file.
5. In the *install_dir* , run **uninstallPSService.cmd** to uninstall the perimeter server service.
6. In the *install_dir* , run **installPS.cmd** to install the perimeter server service.
7. In the *install_dir* , run **startPSService.cmd** to start the perimeter server.

View a Perimeter Server Configuration

You may need to verify that a specific perimeter server is configured to monitor a specific port, or is configured for a specific host.

To view a perimeter server configuration:

1. From the **Administration** menu, select **Operations** > **Perimeter Servers** .
2. On the Perimeter Servers page, click the name of the perimeter server you want to view.

Enable a Perimeter Server Configuration in Sterling Integrator

You may have disabled a perimeter server configuration, and need to enable it.

To enable a perimeter server configuration:

1. From the **Administration** menu, select **Operations System** > **Troubleshooter** .
2. On the System Troubleshooting page, locate **Perimeter Servers**.
3. In the Perimeter Servers area, in the On/Off column, select the check box next to the perimeter server you want to enable.

   The perimeter server is enabled.

Disable a Perimeter Server in Sterling Integrator

You may need to disable a perimeter server configuration in Sterling Integrator to edit it or to remove the perimeter server from use, but retain the configuration to enable the perimeter server later.

If you disable the perimeter server configuration in Sterling Integrator, you do not need to disable the remote perimeter server, because once disabled, the perimeter server will not contact it.

To disable a perimeter server:

1. From the **Administration** menu, select **Operations System** > **Troubleshooter** .
2. On the System Troubleshooting page, locate **Perimeter Servers** .
3. In the Perimeter Servers area, in the On/Off column, clear the check box next to the perimeter server you want to disable.

Disable a Remote Perimeter Server in a UNIX Environment

After you install a remote perimeter server, you may need to disable it for maintenance. If you disable the remote perimeter server configuration and the perimeter server configuration in Sterling Integrator is enabled, the perimeter server configuration in Sterling Integrator continues trying to connect to the remote perimeter server configuration until a successful connection is made.

Caution: Disabling a remote perimeter server configuration may cause errors in some features of Sterling Integrator. You may need to reconfigure specific adapters and services to work properly without a specific perimeter server configuration.

To disable a remote perimeter server configuration in a UNIX environment, run **stopPs.sh** to stop the perimeter server on the remote computer in the *install_dir* directory.

Disable a Remote Perimeter Server Configuration in a Windows Environment

After you install a remote perimeter server, you may need to disable it for maintenance. If you disable the remote perimeter server configuration and the perimeter server configuration in Sterling Integrator is enabled, the perimeter server configuration in Sterling Integrator continues trying to connect to the remote perimeter server configuration until a successful connection is made.

Caution: Disabling a remote perimeter server configuration may cause errors in some features of Sterling Integrator. You may need to reconfigure specific adapters and services to work properly without a specific perimeter server configuration.

To disable a remote perimeter server configuration in a Windows environment, run **stopPs.cmd** to stop the perimeter server configuration on the remote computer in the *install_dir* .

Delete a Perimeter Server Configuration from Sterling Integrator

After you add a perimeter server configuration to Sterling Integrator, you may find you need to delete the perimeter server configuration because you no longer need it, or you make a mistake in the name and need to start over.

Caution: Deleting a perimeter server configuration may cause errors in some features of Sterling Integrator. You may need to reconfigure specific adapters and services to work properly without a specific perimeter server configuration.

To delete a perimeter server configuration:

Remove a Remote Perimeter Server in a UNIX Environment

After you install a remote perimeter server, you may need to remove it for maintenance or replacement.

Caution: Removing a remote perimeter server configuration may cause errors in some features of Sterling Integrator. You may need to reconfigure specific adapters and services to work properly without a specific perimeter server configuration.

To remove a remote perimeter server configuration in a UNIX environment:

1. On the remote computer, in the *install_dir* , run **stopPs.sh** to stop the perimeter server.
2. Remove the perimeter server *install_dir* from the remote computer.

Remove a Remote Perimeter Server from a Windows Environment

After you install a remote perimeter server, you may need to remove it for maintenance or replacement.

Caution: Removing a perimeter server configuration may cause errors in some features of Sterling Integrator. You may need to reconfigure specific adapters and services to work properly without a specific perimeter server configuration.

To remove a remote perimeter server configuration in a Windows environment:

1. On the remote computer, in the *install_dir* , run **stopPs.cmd** to stop the perimeter server configuration.
2. Remove the perimeter server *install_dir* from the remote computer.

Use Local Perimeter Server Logs to Troubleshoot Problems

If you encounter a problem, first check the logs. An error may have been logged that provides the information to resolve the problem.

To access the Perimeter Services logs:

1. From the Administration menu, select **Operations > System > Logs** >.
2. Under Perimeter Services, select a log file.

   The interface displays only the last 2500 lines of a current log file. To view the entire log, you must have Read permission for the file system where the application is located. Open the log file (located at the installation path on your hard drive), with a text editor in read-only mode.
3. If the error is not in the logs, change the logging level. To change the settings, click on the icon next to Perimeter Services. There are four levels of logging information:
   - Error - shows errors only (default)
   - Info - adds information about persistent connections
   - Commtrace - adds information about customer connections
   - All - shows full detail, including developer-only bugs
4. Attempt to recreate the problem.
5. View the logs again to see the additional entries.

Use Remote Perimeter Server Logs to Troubleshoot Problems

Each remote perimeter server writes log files in its installation directory. You should examine these for information needed to diagnose a problem.

If you need more information, the logging level of a remote perimeter server can be changed by editing its remote_perimeter.properties file.

Verify Software Versions

Verify that you have the supported JVM on the computer running Sterling Integrator and on the DMZ computer where you are running perimeter servers.

Both JVM versions must match the requirements for your version of Sterling Integrator. The build date and lower release numbers of your Sterling Integrator and the remote perimeter server must also match.

Call Customer Support

If you cannot pinpoint the cause of the problem you are experiencing, call Sterling Commerce Customer Support for assistance.

Create a Perimeter Server System Internal State Dump

If necessary, Customer Support may request that you create an internal state dump to facilitate problem resolution.

To create an internal state dump for a local perimeter server:

1. Access the computer on which Sterling Integrator is installed.
2. Locate the command script (psDumpMaster.sh or psDumpMaster.cmd) from the main Sterling Integrator bin directory:

   ```
   psDumpMaster.sh [-nNODE] [PserverName]
   ```

   with the following values:

   - -nNODE specifies the cluster node to request a dump on. If not specified a reasonable default will be selected.
   - PserverName specifies an optional perimeter server to restrict the dump. If PserverName is not specified, a dump for all servers configured on the specified cluster node is created.

Create a Remote Perimeter Server System Internal State Dump

If necessary, Customer Support may request that you create an internal state dump from a remote perimeter server to facilitate problem resolution.

To request a dump of a remote perimeter server:

1. Access the computer on which the remote perimeter server is installed.
2. Locate the command script (psDumpSlave.sh or psDumpSlave.cmd) in the remoter perimeter server install directory:

   psDumpSlave.sh

   The dump files are written to the log file directory, named PSDump.<timestamp>, using the log file timestamp format.

Establish a Connection if a Perimeter Server Shows as Disconnected

If you cannot establish a connection between Sterling Integrator and a perimeter server:

1. Use the netstat command to verify that the perimeter server is listening on the expected port.
2. Verify that the firewall betweenSterling Integrator and the perimeter server is configured to allow this connection.
3. Verify that only one Sterling Integrator is configured to use this perimeter server.

Index