Gentran Integration Suite™

Perimeter Server Guide

Version 4.2

Sterling Commerce
An IBM Company

© Copyright 2006 Sterling Commerce, Inc. All rights reserved.
Additional copyright information is located on the Gentran Integration Suite Documentation Library:
http://www.sterlingcommerce.com/Documentation/GIS42/homepage.htm

Contents

Chapter 1

Introduction to Perimeter Servers

Gentran Integration Suite uses perimeter servers to minimize demilitarized zone (DMZ) issues, enhance scalability, enhance handling of large files, and improve performance.

This section covers the following topics:

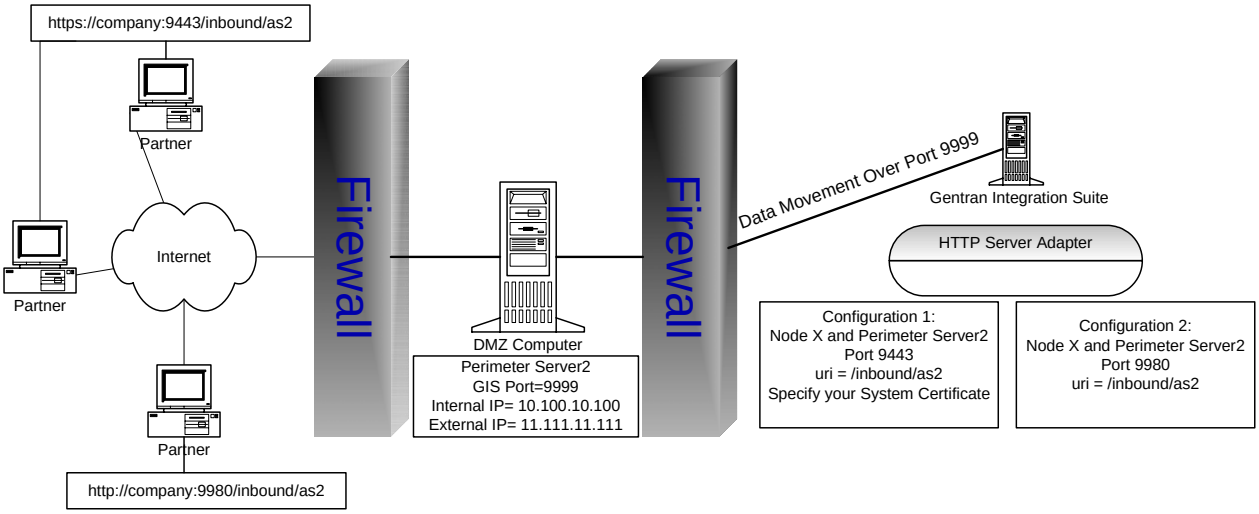
What is a Perimeter Server

A *perimeter server* is communications management software that can be installed in a DMZ and manages communication flows between a perimeter network and Gentran Integration Suite TCP-based transport adapters. 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 Gentran Integration Suite through perimeter services. *Perimeter services* is the Gentran Integration Suite subsystem supporting multihoming and secure perimeter network traversing for Gentran Integration Suite B2B communications protocols.

Perimeter services consist of the following components:

- Perimeter server you install on your DMZ computer (remote perimeter server).
- Perimeter server pre-installed in Gentran Integration Suite (local perimeter server)
- Perimeter services API that communications adapters in Gentran Integration Suite use to use the perimeter servers (local and remote) to use multihoming and perimeter network traversal functionality.
- Perimeter servers configuration management components in the Gentran Integration Suite interface.

The following figure shows a typical Gentran Integration Suite with perimeter servers:



The preceding figure shows the following:

1. The persistent connection is established from the perimeter services API in Gentran Integration Suite to the remote perimeter server on the DMZ computer to communicate through port 9999.
2. Gentran Integration Suite 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 Gentran Integration Suite:
   - https://company:9443./Inbopund/as2 – Communicates securely with the HTTP Server Adapter on Gentran Integration Suite through the initial port of 9443.
   - http://company:9980/Inbound/as2 – Communicates through non-secure http with the HTTP Server Adapter on Gentran Integration Suite through the initial port 9980.

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 perimeter server (local perimeter server) must be configured on the same Gentran Integration Suite node. A *node* is a single installation of Gentran Integration Suite. A single Gentran Integration Suite 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 Gentran Integration Suite.

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

For testing purposes, or when you are running Gentran Integration Suite without the DMZ feature, you can use the local perimeter server that is created during the installation of Gentran Integration Suite.

You should use perimeter servers if you want to:

- Secure communications between the DMZ and Gentran Integration Suite.
- 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 Gentran Integration Suite through session and thread management that includes a large number of connections.
- Use the following adapters or protocols:
  - Connect:Direct Server adapter
  - FTP Client adapter with related services
  - FTP Server adapter
  - HTTP Client adapter with related services
  - HTTP Server adapter
  - Oracle E-Business adapter
  - PeopleSoft adapter
  - Transora adapter
  - SOAP protocol
  - AS2 protocol

Inbound Messages and Perimeter Servers

The following scenario describes how an incoming message is processed in Gentran Integration Suite 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 Gentran Integration Suite to the appropriate adapter in Gentran Integration Suite.

Outbound Messages and Perimeter Servers

The following scenario describes how an outgoing message is processed in Gentran Integration Suite running perimeter services:

1. Gentran Integration Suite sends the message to the local perimeter server in Gentran Integration Suite and the appropriate adapter running in Gentran Integration Suite.
2. The local perimeter server in Gentran Integration Suite sends the message to the remote perimeter server on the DMZ computer through the port established for the persistent connection between the DMZ and Gentran Integration Suite.

3. The remote DMZ perimeter server sends the message to the trading partner through a TCP/IP connection through the port specified in your trading partner agreement.
4. Your trading partner receives the message.

Perimeter Servers and Clustering

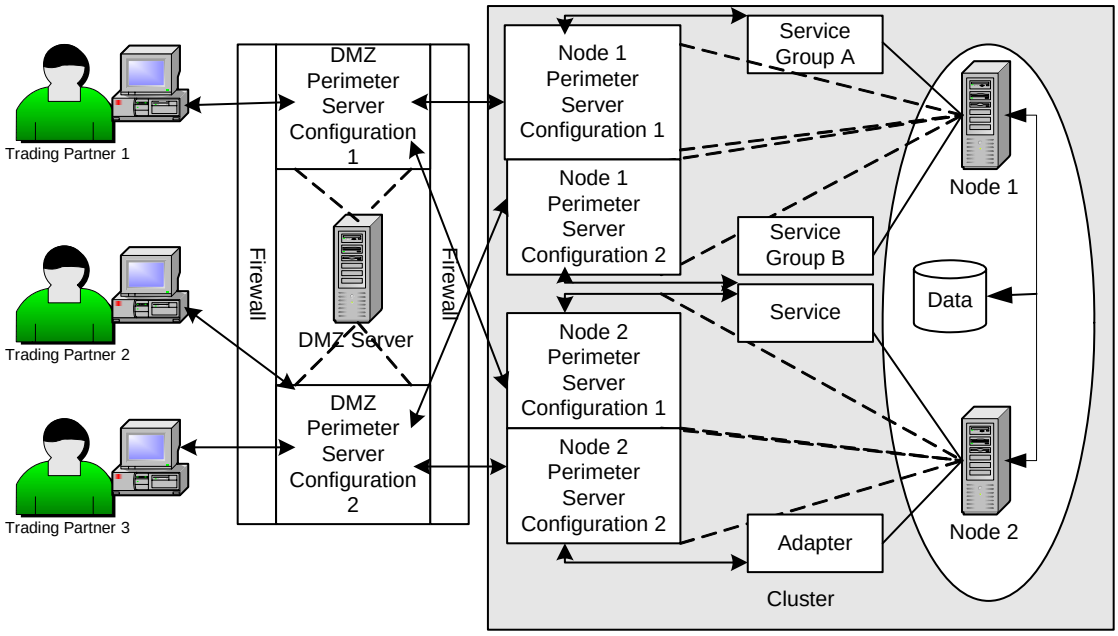
You can use perimeter servers when you install Gentran Integration Suite in a clustered environment. A *cluster* is two or more connected copies of Gentran Integration Suite that share a database. A *node* is one copy of Gentran Integration Suite in the cluster.

In a Gentran Integration Suite 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 Gentran Integration Suite node. You can also have many different services and adapters using the same perimeter server.

You can use service groups in your Gentran Integration Suite 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 Gentran Integration Suite clustered environment, call Sterling Commerce Customer Support.

The following figure shows a Gentran Integration Suite 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:
   - Service Group A is a group of adapters that are all configured compatibly (identically, except for perimeter server selection) to achieve load balancing and failover support.
   - Service Group B is a group of adapters that are configured differently and cannot be used for load balancing or failover support.
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:
   - Node 1 Perimeter Server Configuration 1 is configured to communicate using Service Group A.
   - Node 1 Perimeter Server Configuration 2 is configured to communicate using Service Group B.
   - Node 2 Perimeter Server Configuration 1 is configured to communicate using a single service configuration.
   - Node 2 Perimeter Server Configuration 2 is configured to communicate using a single adapter configuration.
5. The DMZ Server has two perimeter servers configured:
   - DMZ Server Perimeter Server Configuration 1 is configured to communicate with Node 1 Perimeter Servers 1 and 2.
   - DMZ Server Perimeter Server Configuration 2 is configured to communicate with Node 2 Perimeter Servers 1 and 2.
6. Three trading partners are configured to communicate with the DMZ Server Perimeter Servers:

- Trading Partner 1 communicates with DMZ Server Perimeter Server Configuration 1.
- Trading Partner 2 communicates with DMZ Server Perimeter Server Configuration 2.
- Trading Partner 3 communicates with DMZ Server Perimeter Server Configuration 3.

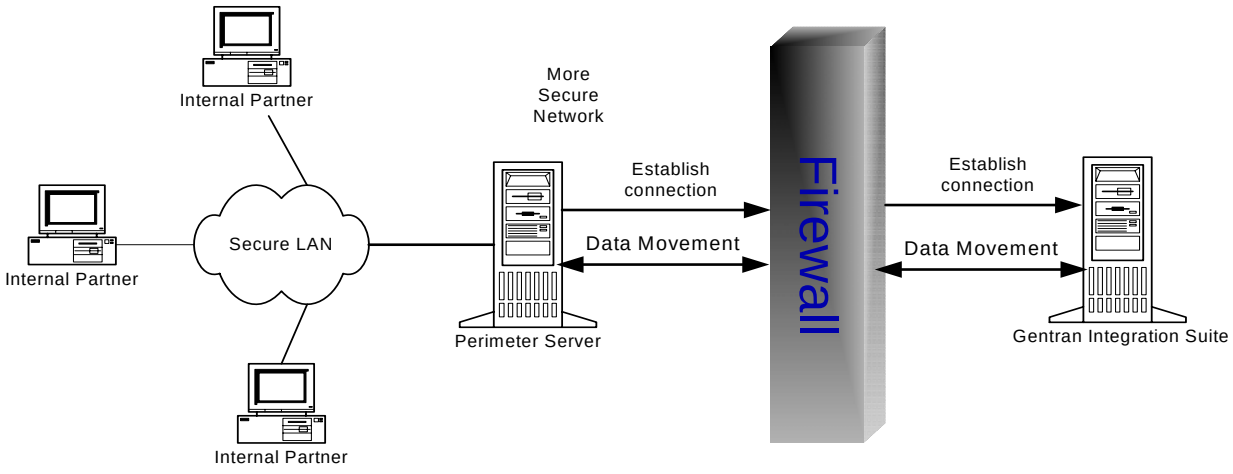
The following is an example of how a business process is routed through the preceding figure. For example, Trading Partner 1 sends a message to your Gentran Integration Suite cluster. The message is sent through the DMZ Perimeter Server Configuration 1, which communicates with the Node 1 Perimeter Server Configuration 1 in your Gentran Integration Suite cluster. 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 Gentran Integration Suite cluster. Because clustering is a way to control load balancing and scale your system, Node 1 is too busy processing other business processes, so Node 2 accepts and processes the business process.

For more information about configuring perimeter servers, see *Configuring Perimeter Servers* on page 14.

Perimeter Servers and More Secure Networks

The more common network configuration pattern is for Gentran Integration Suite 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 Gentran Integration Suite to the Perimeter server – that is, from the more secure towards the less secure network zone.

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



For more information, see *Adding a Perimeter Server to Gentran Integration Suite* on page 11.

Perimeter Server Property Settings

Many of the property settings for perimeter servers are stored in the perimeter.properties file in the Properties directory of your Gentran Integration Suite installation.

Adding a Perimeter Server to Gentran Integration Suite

Before you can add a perimeter server to Gentran Integration Suite, you must:

- ✦ Install a perimeter server in a demilitarized zone (DMZ).
- ✦ Know the host name and port number of the installed DMZ perimeter server.

To add a perimeter server in Gentran Integration Suite:

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 in Gentran Integration Suite. Type ***** (wildcard) to allow Gentran Integration Suite 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 Gentran Integration Suite 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 in Gentran Integration Suite. Type **0** (zero) to allow Gentran Integration Suite 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 Gentran Integration Suite to choose any available port. **Note:** Do not use in iSeries (OS/400) environments.
Perimeter Server (far-end) is in less secure network zone	Check this to enable the connection from Gentran Integration Suite 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 DMZ perimeter server is installed on. If you specified an internal interface during your perimeter server installation, use that address here.

Field	Description
Perimeter Server Port	Port number that the DMZ perimeter server monitors for connections. This is the port number you specified when installing your perimeter server in the DMZ.
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. For more information about clustered environments, see Perimeter Servers and Clustering.

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 the performance of Gentran Integration Suite.
Inbound Connection	
High	Highest inbound connection buffer size. This is the high watermark. When a trading partner sends data faster than Gentran Integration Suite 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 Gentran Integration Suite 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 Gentran Integration Suite 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 Gentran Integration Suite 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 Gentran Integration Suite. You can now monitor the perimeter server using the Troubleshooter page and you can view the perimeter server log using the System Logs page and monitor the DMZ perimeter server using the perimeter server log on the DMZ server.

Chapter 2

Configuring Perimeter Servers

Gentran Integration Suite uses perimeter servers to minimize demilitarized zone (DMZ) issues, enhance scalability, enhance handling of large files, and improve performance.

This section covers the following topics:

Configuring Perimeter Servers for SSL

If you decide to use SSL with your perimeter server configuration, you must complete the following actions:

1. Create an SSL certificate or import the certificate from your certificate authority in Gentran Integration Suite.

   For additional information about creating an SSL certificate, see *Editing a Perimeter Server Configuration in a DMZ in a Windows Environment* on page 16.

2. Set the **Use SSL** field in the appropriate adapter configuration to **Must**.

Editing a Perimeter Server Configuration in Gentran Integration Suite

After you add a perimeter server configuration to Gentran Integration Suite, 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**.

Editing a Perimeter Server Configuration in a DMZ 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 in your DMZ.

To edit a remote perimeter server configuration in your DMZ:

1. On the DMZ computer, in the *install_dir*, run **stopPs.sh** to stop the perimeter server.
2. Locate the *install_dir*/startupPs.sh file.
3. Open **startupPs.sh** in a text editor and make the appropriate changes to the script:

Parameter	Description
PS_DEBUG	Sets the logging level. Valid values are 1 through 8 with the larger numbers providing more detailed logging information.
PS_PORT	Sets the port for the specific perimeter server to listen to for a connection from Gentran Integration Suite.
INTERNAL_INTERFACE	Sets the network interface for the specific perimeter server to use to communicate with Gentran Integration Suite.
EXTERNAL_INTERFACE	Sets the network interface for the specific perimeter server to use to communicate with your trading partners.
MAX_HEAP_SIZE	Sets the maximum heap size the Java Virtual Machine (JVM) that is running the specific perimeter server uses.

Parameter	Description
MAX_ALLOCATION	Sets the maximum amount of data the specific perimeter server buffers in MB.

4. Save **startupPs.sh** without changing the name of the file.
5. In *install_dir*, run **startupPs.sh** to start the perimeter server.

Editing a Perimeter Server Configuration in a DMZ 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 in your DMZ.

To edit a remote perimeter server configuration in your DMZ 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*\installPS.cmd file.
3. Open **installPS.cmd** in a text editor and make the appropriate changes to the script:

Parameter	Description
set PS_DEBUG	Sets the logging level. Valid values are 1 through 8 with the larger numbers providing more detailed logging information.
set PS_PORT	Sets the port for the specific perimeter server to listen to for a connection from Gentran Integration Suite.
set INTERNAL_INTERFACE	Sets the network interface for the specific perimeter server to use to communicate with Gentran Integration Suite.
set EXTERNAL_INTERFACE	Sets the network interface for the specific perimeter server to use to communicate with your trading partners.
set MAX_HEAP_SIZE	Sets the maximum heap size the Java Virtual Machine (JVM) that is running the specific perimeter server uses.
set MAX_ALLOCATION	Sets the maximum amount of data the specific perimeter server buffers in MB.

4. Save **installPS.cmd** 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.

Viewing 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.

   The perimeter server configuration displays.
3. Click **Close Window**.

Enabling a Perimeter Server Configuration in Gentran Integration Suite

You may find that you have disabled a perimeter server configuration for some reason and need to enable the perimeter server configuration.

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.

Disabling a Perimeter Server Configuration in Gentran Integration Suite

You may find that you need to disable a perimeter server configuration in Gentran Integration Suite to edit the perimeter server configuration or to remove the perimeter server from use, but retain the configuration in case you want to enable the perimeter server at a later time.

If you disable the perimeter server configuration in Gentran Integration Suite, you do not need to disable the remote DMZ perimeter server as the perimeter server in Gentran Integration Suite does not attempt to contact the remote DMZ perimeter server.

To disable a perimeter server configuration in Gentran Integration Suite:

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.

Disabling a DMZ Perimeter Server Configuration in a UNIX Environment

After you install a remote perimeter server in a DMZ, you may need to disable the perimeter server configuration for maintenance of the DMZ computer. If you disable the DMZ perimeter server configuration and the perimeter server configuration in Gentran Integration Suite is enabled, the perimeter server configuration in Gentran Integration Suite continues trying to connect to the DMZ perimeter server configuration until a successful connection is made.

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

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

Disabling a DMZ Perimeter Server Configuration in a Windows Environment

After you install a remote perimeter server in a DMZ, you may need to disable the perimeter server configuration for maintenance of the DMZ computer. If you disable the DMZ perimeter server configuration and the perimeter server configuration in Gentran Integration Suite is enabled, the perimeter server configuration in Gentran Integration Suite continues trying to connect to the remote DMZ perimeter server configuration until a successful connection is made.

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

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

Deleting a Perimeter Server Configuration from Gentran Integration Suite

After you add a perimeter server configuration to Gentran Integration Suite, 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 Gentran Integration Suite. You may need to reconfigure specific adapters and services to work properly without a specific perimeter server configuration.

To delete 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 delete, click **Delete**.
3. On the Confirm page, verify that the perimeter server is the perimeter server you want to delete. Is this the perimeter server you want to delete?
   - If Yes, click **Delete**. The perimeter server configuration is deleted from Gentran Integration Suite.
   - If No, click **Cancel** to return to the Perimeter Servers page.

Removing a DMZ Perimeter Server Configuration in a UNIX Environment

After you install a remote perimeter server configuration in a DMZ, you may need to remove the remote perimeter server configuration for maintenance of the DMZ computer or to install a replacement perimeter server configuration.

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

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

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

Removing a DMZ Perimeter Server Configuration from a Windows Environment

After you install a perimeter server configuration in a DMZ, you may need to remove the perimeter server configuration for maintenance of the DMZ computer or to install a replacement perimeter server configuration.

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

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

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

Index