

Configuring NAT over LAN-to-LAN Between Two Cisco VPN 3000 Concentrators

Document ID: 44402

Introduction

Prerequisites

- Requirements
- Components Used
- Network Diagram
- Conventions

Configure the Cisco VPN 3005-1 Concentrator

- Verify the Configuration
- Troubleshoot the Configuration

Configure the Cisco VPN 3005-2 Concentrator

- Verify the Configuration
- Troubleshoot the Configuration

Related Information

Introduction

This document demonstrates how to configure the Network Address Translation (NAT) over LAN-to-LAN feature as introduced in Cisco VPN 3000 Concentrator 3.6. This feature allows you to configure the IPsec LAN-to-LAN tunnel with overlapping private networks on each side of the VPN tunnel.

With the NAT over LAN-to-LAN feature enabled, packets that come into the private interface of the VPN Concentrator are translated according to the NAT rule defined before they are encrypted. On the other side, the VPN packets that reach the public interface of the VPN Concentrator are translated according the NAT rules defined after they are decrypted.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- You have performed the initial configuration steps for the VPN Concentrators in order to get Internet connectivity.
- Familiarity of standard LAN-to-LAN IPsec tunnel configurations with the use of VPN Concentrators. Refer to *Configuring a Central Cisco VPN 3000 Concentrator to Allow Communication Between Spokes* for further reference.

Components Used

The information in this document is based on these software and hardware versions:

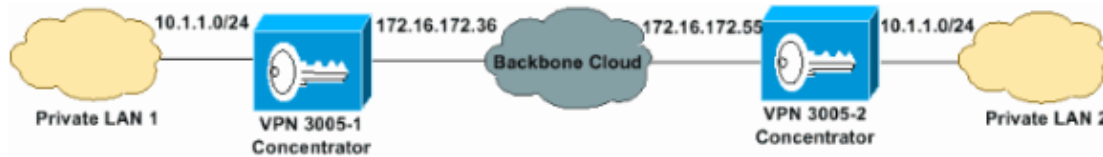
- Cisco VPN 3005 Concentrator version 3.6

Note: This document was recently reviewed with 4.x code on October 4, 2004.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Network Diagram

This document uses this network setup:



This network diagram shows that private LAN 1 and private LAN 2 have overlapping networks of 10.1.1.0/24. The configuration examples in this document demonstrate how to configure the NAT over LAN-to-LAN feature so that the hosts on the two private LANs can communicate easily through the IPsec tunnel between the Cisco VPN 3005-1 and Cisco VPN 3005-2 Concentrators.

This table highlights the translation scheme used in this example to map the overlapping networks on each side to different subnets and corresponding interesting traffic for the IPsec LAN-to-LAN tunnel:

NAT Table			
	Source Network	Translated Network	Remote Network
3005-1	IP Address <input type="text" value="10.1.1.0"/>	:	<input type="text" value="30.1.1.0"/> -> <input type="text" value="20.1.1.0"/>
	Wildcard Mask <input type="text" value="0.0.0.255"/>	:	<input type="text" value="0.0.0.255"/> -> <input type="text" value="0.0.0.255"/>

Note: The IPsec LAN-to-LAN tunnel for the Local Networks is 30.1.1.0/24 and the IPsec LAN-to-LAN tunnel for the Remote Networks is 20.1.1.0/24.

NAT Table			
	Source Network	Translated Network	Remote Network
3005-1	IP Address <input type="text" value="10.1.1.0"/>	:	<input type="text" value="20.1.1.0"/> -> <input type="text" value="30.1.1.0"/>
	Wildcard Mask <input type="text" value="0.0.0.255"/>	:	<input type="text" value="0.0.0.255"/> -> <input type="text" value="0.0.0.255"/>

Note: The IPsec LAN-to-LAN tunnel for the Local Networks is 20.1.1.0/24 and the IPsec LAN-to-LAN tunnel for the Remote Networks is 30.1.1.0/24.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure the Cisco VPN 3005-1 Concentrator

Complete these steps to configure the Cisco VPN 3005-1 Concentrator with an IP address of 172.16.172.36.

1. Select **Configuration > System > Tunneling Protocols > IPSec > LAN-to-LAN > Modify** to define a LAN-to-LAN tunnel with the Cisco VPN 3005-1 Concentrator (172.16.172.36).

One important thing to notice is that the IP addresses in Local Network and Remote Network need to

be the translated IP subnets as planned in the translation table.

2. Complete these steps from the Modify window:

- a. Enter the name for your LAN-to-LAN connection in the Name field.
- b. Select the interface for your LAN-to-LAN connection from the Interface drop-down list.
- c. Enter the IP address of the remote peer for your LAN-to-LAN connection in the Peer field.
- d. Select the digital certificate to use from the Digital Certificate drop-down list.
- e. Choose how to send the digital certificate to the IKE peer from Certificate Transmission.
Select either **Entire Certificate chain** or **Identity Certificate only**.
- f. Enter the preshared key for your LAN-to-LAN connection in the Preshared Key field.
- g. Specify the packet authentication mechanism to use from the Authentication drop-down list.
- h. Select the encryption mechanism to use from the Encryption drop-down list.
- i. Select the IKE proposal to use for this LAN-to-LAN connection from the IKE Proposal drop-down list.
- j. Select the filter to apply to the traffic that is tunneled through the LAN-to-LAN connection from the Filter drop-down list.
- k. Select the **NAT-T** check box to allow NAT-T compatible IPsec peers to establish your LAN-to-LAN connection through a NAT device. You must also enable **IPsec over NAT-T** under NAT Transparency.
- l. Choose the bandwidth policy to apply to your LAN-to-LAN connection from the Bandwidth Policy drop-down list.
- m. Select the routing mechanism to use from the Routing drop-down list.

Configuration | System | Tunneling Protocols | IPsec | LAN-to-LAN | Modify

Modify an IPsec LAN-to-LAN connection.

Name	To-172.16.172.55	Enter the name for this LAN-to-LAN connection.
Interface	Ethernet2 (Public) (172.16.172.36)	Select the interface for this LAN-to-LAN connection.
Peer	172.16.172.55	Enter the IP address of the remote peer for this LAN-to-LAN connection.
Digital Certificate	None (Use Preshared Keys)	Select the digital certificate to use.
Certificate Transmission	<input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only	Choose how to send the digital certificate to the IKE peer.
Preshared Key	cisco123	Enter the preshared key for this LAN-to-LAN connection.
Authentication	ESP/MD5/HMAC-128	Specify the packet authentication mechanism to use.
Encryption	3DES-168	Specify the encryption mechanism to use.
IKE Proposal	IKE-3DES-MD5	Select the IKE Proposal to use for this LAN-to-LAN connection.
Filter	-None-	Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.
IPsec NAT-T	<input type="checkbox"/>	Check to let NAT-T compatible IPsec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPsec over NAT-T under NAT Transparency.
Bandwidth Policy	-None-	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
Routing	None	Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.

Note: You do not need to specify these next set of parameters if you choose Network Autodiscovery.

- a. Select the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection from the Network List drop-down field.

- b. Enter the IP address in the IP Address field.
- c. Enter the wildcard mask (reverse of a subnet mask) in the Wildcard Mask field.
- d. Repeat steps a through c for the Remote Network section and click **Apply** to apply the LAN-to-LAN tunnel configuration.

Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.

Network List Use IP Address/Wildcard-mask below Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.

IP Address 30.1.1.0

Wildcard Mask 0.0.0.255

Note: Enter a *wildcard mask*, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.

Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.

Network List Use IP Address/Wildcard-mask below Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.

IP Address 20.1.1.0

Wildcard Mask 0.0.0.255

Note: Enter a *wildcard mask*, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.

Apply Cancel

3. After you apply the LAN-to-LAN tunnel configuration, click on the **LAN-to-LAN NAT Rules** to define the NAT for the NAT-to-LAN tunnel.
4. Click **Add** to add a LAN-to-LAN connection, or select a connection and click either **Modify** or **Delete** from the LAN-to-LAN Connection field.

Configuration | System | Tunneling Protocols | IPSec | LAN-to-LAN Save

This section lets you configure IPSec LAN-to-LAN connections. LAN-to-LAN connections are established with other VPN 3000 Concentrators, PIX firewalls, 7100/4000 series routers and other IPSec-compliant security gateways. To configure a VPN 3002 or other remote access connection, go to [User Management](#) and configure a Group and User. To configure NAT over LAN-to-LAN, go to [LAN-to-LAN NAT Rules](#).

Click the **Add** button to add a LAN-to-LAN connection, or select a connection and click **Modify** or **Delete**.

LAN-to-LAN Connection	Actions
To-172.16.172.55 (172.16.172.55) on Ethernet2 (Public)	<div style="display: flex; flex-direction: column; gap: 5px;"> <input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> </div>

5. Select **Configuration > Policy Management > Traffic Management > NAT > LAN-to-LAN Rules > Modify** to add a LAN-to-LAN NAT rule based on the NAT plan defined in step 3 and then complete these steps.

Note: In this case, the 10.1.1.0/24 behind the VPN 3005-1 Concentrator is translated to 30.1.1.0/24 when it communicates with the private LAN behind the VPN 3005-2 Concentrator through the IPSec LAN-to-LAN tunnel.

- a. Select either **Static**, **Dynamic**, or **PAT** to modify a LAN-to-LAN NAT rule.
- b. Enter the IP Address and Wildcard Mask in the Source Network, Translated Network, and Remote Network column fields.
- c. Click **Apply**.

Configuration | Policy Management | Traffic Management | NAT | LAN-to-LAN Rules | Modify Save

Modify a LAN-to-LAN NAT rule.

NAT Type

Static **Static:** maps source IP addresses to translated IP addresses on a one-to-one basis. Static mappings apply to both inbound and outbound traffic.

Dynamic **Dynamic:** maps source IP addresses to one of a pool of available translated IP addresses. Dynamic mappings apply to outbound traffic only.

PAT **PAT:** Dynamic mapping with Port Address Translation. PAT applies to outbound traffic only.

Source Network: specifies the source IP address and wildcard mask to be translated.
Translated Network: specifies the translated IP address and wildcard mask for the **Local Network**. It is the local address of the LAN-to-LAN connection.
Remote Network: specifies the destination IP address and wildcard mask for which this rule applies. To allow any remote network, set IP address/wildcard mask to 0.0.0.0/255.255.255.255. It is the remote address of the LAN-to-LAN connection.

	Source Network		Translated Network		Remote Network
IP Address	<input type="text" value="10.1.1.0"/>	:	<input type="text" value="30.1.1.0"/>	->	<input type="text" value="20.1.1.0"/>
Wildcard Mask	<input type="text" value="0.0.0.255"/>	:	<input type="text" value="0.0.0.255"/>	->	<input type="text" value="0.0.0.255"/>

6. Select **Configuration > Policy Management > Traffic Management > NAT > Enable** to enable the LAN-to-LAN NAT rule.
7. Select **Check to enable NAT rules on LAN-to-LAN tunnels** from the Enable window and click **Apply**.

Configuration | Policy Management | Traffic Management | NAT | Enable

This section lets you enable system-wide NAT rules.

Interface NAT Rules Enabled Check to enable NAT rules on interfaces.

LAN-to-LAN Tunnel NAT Rule Enabled Check to enable NAT rules on LAN-to-LAN tunnels.

8. Select **Configuration > System > IP Routing > Static Routes** to verify the routing configuration. In this case, a simple default route is used.

Configuration | System | IP Routing | Static Routes Save Needed

This section lets you configure static routes for IP routing.

Static Routes	Actions
Default -> 172.16.172.33	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>

Verify the Configuration

This section provides information you can use to confirm your configuration works properly.

After you complete this configuration, test the IPsec tunnel by sending traffic between the two private LANs. Note that the hosts on private LAN 1 see the private LAN 2 as 20.1.1.0/24 and the hosts on private LAN 2 see private LAN 1 as 30.1.1.0/24.

The process demonstrates how to verify and monitor the IPsec sessions from the Cisco VPN 3005-1 Concentrator.

1. Select **Administration > Administer Sessions** on the Cisco VPN 3005-1 Concentrator.

Administration | Administer Sessions Tuesday, 13 August 2002 17:15:13
Reset Refresh

This screen shows statistics for sessions. To refresh the statistics, click **Refresh**. Select a **Group** to filter the sessions. For more information on a session, click on that session's name. To log out a session, click **Logout** in the table below. To test the network connection to a session, click **Ping**.

Group

Logout [All](#) | [PPTP User](#) | [L2TP User](#) | [IPSec User](#) | [IPSec LAN-to-LAN](#)

Session Summary

Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Concurrent Sessions Limit	Total Cumulative Sessions
1	0	1	2	2	1500	10

LAN-to-LAN Sessions

[[Remote Access Sessions](#) | [Management Sessions](#)]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Ix	Bytes Rx	Actions
To-172.16.172.55	172.16.172.55	IPSec/LAN-to-LAN	3DES-168	Aug 13 16:47:59	0:27:14	416	416	[Logout Ping]

Remote Access Sessions

[[LAN-to-LAN Sessions](#) | [Management Sessions](#)]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Ix Bytes Rx	Actions
No Remote Access Sessions							

2. Select **Administration > Administer Sessions > Detail** to view detailed information on the IPsec SAs.

Administration Administer Sessions Detail							
							Tuesday, 13 August 2002 17:16:53
							Reset Refresh
Back to Sessions							
Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
To-172.16.172.55	172.16.172.55	IPSec/LAN-to-LAN	3DES-168	Aug 13 16:47:59	0:28:54	416	416
IKE Sessions: 1							
IPSec Sessions: 1							
IKE Session							
Session ID	1	Encryption Algorithm	3DES-168				
Hashing Algorithm	MD5	Diffie-Hellman Group	Group 2 (1024-bit)				
Authentication Mode	Pre-Shared Keys	IKE Negotiation Mode	Main				
Rekey Time Interval	86400 seconds						
IPSec Session							
Session ID	2	Remote Address	20.1.1.0/0.0.0.255				
Local Address	30.1.1.0/0.0.0.255	Encryption Algorithm	3DES-168				
Hashing Algorithm	MD5	SEP	1				
Encapsulation Mode	Tunnel	Rekey Time Interval	28800 seconds				
Bytes Received	416	Bytes Transmitted	416				

Troubleshoot the Configuration

Refer to Troubleshooting Connection Problems on the Cisco VPN 3000 Concentrator for additional information on troubleshooting Cisco VPN 3000 Concentrator connection issues.

Configure the Cisco VPN 3005–2 Concentrator

Complete these steps to configure the Cisco VPN 3005–2 Concentrator with an IP address of 172.16.172.55.

1. Select **Configuration > System > Tunneling Protocols > IPSec > LAN-to-LAN > Modify** to define a LAN-to-LAN tunnel with Cisco VPN 3005–2 (172.16.172.55). One important thing to notice is that the IP addresses in Local Network and Remote Network should be the translated IP subnets as planned in the NAT tables.
2. Complete these steps from the Modify window:
 - a. Enter the name for your LAN-to-LAN connection in the Name field.
 - b. Select the interface for your LAN-to-LAN connection from the Interface drop-down list.
 - c. Enter the IP address of the remote peer for your LAN-to-LAN connection in the Peer field.
 - d. Select the digital certificate to use from the Digital Certificate drop-down list.
 - e. Choose how to send the digital certificate to the IKE peer by selecting either **Entire Certificate chain** or **Identity Certificate only** from Certificate Transmission.
 - f. Enter the preshared key for your LAN-to-LAN connection in the Preshared Key field.
 - g. Specify the packet authentication mechanism to use from the Authentication drop-down list.
 - h. Select the encryption mechanism to use from the Encryption drop-down list.
 - i. Select the IKE proposal to use for this LAN-to-LAN connection from the IKE Proposal drop-down list.
 - j. Select the filter to apply to the traffic that is tunneled through the LAN-to-LAN connection

- from the Filter drop-down list.
- k. Select the **NAT-T** check box to allow NAT-T compatible IPsec peers to establish your LAN-to-LAN connection through a NAT device. You must also enable **IPSec over NAT-T** under NAT Transparency.
 - l. Choose the bandwidth policy to apply to your LAN-to-LAN connection from the Bandwidth Policy drop-down list.
 - m. Select the routing mechanism to use from the Routing drop-down list.

Configuration | System | Tunneling Protocols | IPsec | LAN-to-LAN | Modify

Modify an IPsec LAN-to-LAN connection.

<p>Name <input type="text" value="To-172.16.172.36"/></p> <p>Interface <input type="text" value="Ethernet2 (Public) (172.16.172.55)"/></p> <p>Peer <input type="text" value="172.16.172.36"/></p> <p>Digital Certificate <input type="text" value="None (Use Preshared Keys)"/></p> <p>Certificate Transmission <input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only</p> <p>Preshared Key <input type="text" value="cisco123"/></p> <p>Authentication <input type="text" value="ESP/MD5/HMAC-128"/></p> <p>Encryption <input type="text" value="3DES-168"/></p> <p>IKE Proposal <input type="text" value="IKE-3DES-MD5"/></p> <p>Filter <input type="text" value="-None-"/></p> <p>IPsec NAT-T <input type="checkbox"/></p> <p>Bandwidth Policy <input type="text" value="-None-"/></p> <p>Routing <input type="text" value="None"/></p>	<p>Enter the name for this LAN-to-LAN connection.</p> <p>Select the interface for this LAN-to-LAN connection.</p> <p>Enter the IP address of the remote peer for this LAN-to-LAN connection.</p> <p>Select the digital certificate to use.</p> <p>Choose how to send the digital certificate to the IKE peer.</p> <p>Enter the preshared key for this LAN-to-LAN connection.</p> <p>Specify the packet authentication mechanism to use.</p> <p>Specify the encryption mechanism to use.</p> <p>Select the IKE Proposal to use for this LAN-to-LAN connection.</p> <p>Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.</p> <p>Check to let NAT-T compatible IPsec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over NAT-T under NAT Transparency.</p> <p>Choose the bandwidth policy to apply to this LAN-to-LAN connection.</p> <p>Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.</p>
--	--

Note: You do not need to specify the next set of parameters if you choose Network Autodiscovery.

- a. Select the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection from the Network List drop-down field.
- b. Enter the IP address in the IP Address field.
- c. Enter the wildcard mask (reverse of a subnet mask) in the Wildcard Mask field.
- d. Repeat steps a through c for the Remote Network section and click **Apply** to apply the LAN-to-LAN tunnel configuration.

Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.

Network List Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.

IP Address

Wildcard Mask

Note: Enter a *wildcard mask*, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.

Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.

Network List Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.

IP Address

Wildcard Mask

Note: Enter a *wildcard mask*, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.

3. Select **Configuration > Policy Management > Traffic Management > NAT > LAN-to-LAN Rules > Modify** to add a LAN-to-LAN NAT rule based on the NAT plan you defined earlier in this document and complete these steps.

Note: In this case, the 10.1.1.0/24 behind the Cisco VPN 3005-2 Concentrator is translated to 20.1.1.0/24 when they communicate with the private LAN behind the Cisco VPN 3005-1 Concentrator through the IPsec LAN-to-LAN tunnel.

- a. Select either **Static**, **Dynamic**, or **PAT** to modify a LAN-to-LAN NAT.
- b. Enter the IP Address and Wildcard Mask in the Source Network, Translated Network, and Remote Network column fields.
- c. Click **Apply**.

Configuration | Policy Management | Traffic Management | NAT | LAN-to-LAN Rules | Modify

Modify a LAN-to-LAN NAT rule.

Static **Static:** maps source IP addresses to translated IP addresses on a one-to-one basis. Static mappings apply to both inbound and outbound traffic.

NAT Type **Dynamic** **Dynamic:** maps source IP addresses to one of a pool of available translated IP addresses. Dynamic mappings apply to outbound traffic only.

PAT **PAT:** Dynamic mapping with Port Address Translation. PAT applies to outbound traffic only.

Source Network: specifies the source IP address and wildcard mask to be translated.
Translated Network: specifies the translated IP address and wildcard mask for the **Local Network**. It is the local address of the LAN-to-LAN connection.
Remote Network: specifies the destination IP address and wildcard mask for which this rule applies. To allow any remote network, set IP address/wildcard mask to 0.0.0.0/255.255.255.255. It is the remote address of the LAN-to-LAN connection.

	Source Network		Translated Network		Remote Network
IP Address	<input type="text" value="10.1.1.0"/>	:	<input type="text" value="20.1.1.0"/>	->	<input type="text" value="30.1.1.0"/>
Wildcard Mask	<input type="text" value="0.0.0.255"/>	:	<input type="text" value="0.0.0.255"/>	->	<input type="text" value="0.0.0.255"/>

4. Select **Configuration > Policy Management > Traffic Management > NAT > Enable** to enable the LAN-to-LAN NAT rule.
5. Select **Check to enable NAT rules on LAN-to-LAN tunnels** from the Enable window and click **Apply**.

Configuration | Policy Management | Traffic Management | NAT | Enable

This section lets you enable system-wide NAT rules.

Interface NAT Rules Enabled Check to enable NAT rules on interfaces.

LAN-to-LAN Tunnel NAT Rule Enabled Check to enable NAT rules on LAN-to-LAN tunnels.

Apply Cancel

Verify the Configuration

This section provides information you can use to confirm your configuration works properly.

After you complete this configuration, test the IPsec tunnel by sending traffic between the two private LANs. Note that the hosts on private LAN 1 see the private LAN 2 as 20.1.1.0/24 and the hosts on private LAN 2 see private LAN 1 as 30.1.1.0/24.

This process demonstrates how to verify and monitor the IPsec sessions from the Cisco VPN 3005-2 Concentrator.

1. Select **Administration > Administer Sessions** on the Cisco VPN 3005-2 Concentrator.

Administration | Administer Sessions Friday, 13 September 2002 17:22:06

[Reset](#) [Refresh](#)

This screen shows statistics for sessions. To refresh the statistics, click **Refresh**. Select a **Group** to filter the sessions. For more information on a session, click on that session's name. To log out a session, click **Logout** in the table below. To test the network connection to a session, click **Ping**.

Group:

Logout All: [PPTP User](#) | [L2TP User](#) | [IPSec User](#) | [IPSec LAN-to-LAN](#)

Session Summary

Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Concurrent Sessions Limit	Total Cumulative Sessions
1	0	1	2	2	100	20

LAN-to-LAN Sessions [[Remote Access Sessions](#) | [Management Sessions](#)]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx	Actions
To-172.16.172.36	172.16.172.36	IPSec/LAN-to-LAN	3DES-168	Sep 13 15:49:23	0:32:43	416	416	[Logout Ping]

Remote Access Sessions [[LAN-to-LAN Sessions](#) | [Management Sessions](#)]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	Actions
No Remote Access Sessions							

2. Select **Administration > Administer Sessions > Detail** to view detailed information of the IPsec SAs.

Administration Administer Sessions Detail				Friday, 13 September 2002 17:22:22			
				Reset Refresh			
Back to Sessions							
Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
To-172.16.172.36	172.16.172.36	IPSec/LAN-to-LAN	3DES-168	Sep 13 16:49:23	0:32:59	416	416
IKE Sessions: 1							
IPSec Sessions: 1							
IKE Session							
Session ID	1	Encryption Algorithm	3DES-168				
Hashing Algorithm	MD5	Diffie-Hellman Group	Group 2 (1024-bit)				
Authentication Mode	Pre-Shared Keys	IKE Negotiation Mode	Main				
Rekey Time Interval	86400 seconds						
IPSec Session							
Session ID	2	Remote Address	30.1.1.0/0.0.0.255				
Local Address	20.1.1.0/0.0.0.255	Encryption Algorithm	3DES-168				
Hashing Algorithm	MD5	Encapsulation Mode	Tunnel				
Rekey Time Interval	28800 seconds						
Bytes Received	416	Bytes Transmitted	416				

3. Select **Monitoring > Statistics > NAT** in this tab to verify whether the NAT rule is working or not. You can view the NAT translations, packet details (source IP, destination IP, and so forth). This allows you to see the translated entries for the interesting and non interesting traffic (depends on network lists) of the VPN Concentrator so that you can trace out the outgoing translated packets.

Troubleshoot the Configuration

Refer to Troubleshooting Connection Problems on the Cisco VPN 3000 Concentrator for additional information on troubleshooting Cisco VPN 3000 Concentrator connection issues.

Related Information

- [Cisco VPN 3000 Series Concentrator Support Page](#)
- [Cisco VPN 3000 Series Client Support Page](#)
- [IPSec Negotiation/IKE Protocols Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Feb 02, 2006

Document ID: 44402