

# Configuring Load–Balancing on VPN 3000 Concentrators

Document ID: 7602

---

## Introduction

### Prerequisites

Requirements

Components Used

Conventions

### Key Definitions

### Network Diagram

### Addresses

### Restrictions

### Configuration

IP Address Assignment

Filter Configuration

Cluster Configuration

Monitoring

### Test the Load–Balancing Feature

### Troubleshoot

### NetPro Discussion Forums – Featured Conversations

### Related Information

---

## Introduction

Load–balancing is the ability to have Cisco VPN 3000 Clients shared across multiple units without user intervention. It ensures that the public IP address is highly available to users. For example, if the Cisco VPN 3000 Concentrator that services the public IP address fails, another VPN 3000 Concentrator in the cluster assumes the public IP address. It also allows non–IP Security (PPTP and L2TP) and non–Cisco IPsec clients to connect to the VPN 3000 Concentrator in the existing manner, although these VPN Clients are not load–balanced or supported by secure session failover.

**Note:** Virtual Router Redundancy Protocol (VRRP) and load–balancing are mutually exclusive of one another. VRRP cannot be enabled while load–balancing is enabled and vice versa.

## Prerequisites

### Requirements

This document assumes:

- You have assigned IP addresses on your VPN 3000 Concentrators (on both public and private interfaces).
- IPsec is configured on the VPN 3000 Concentrators for the VPN user. Refer to IPsec with VPN Client to VPN 3000 Concentrator Configuration Example for a sample configuration if IPsec is not configured.
- VPN users are able to connect to all the VPN 3000 Concentrators with the use of their individually assigned public IP address.

## Components Used

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

- VPN 3000 Software Client Software Releases 3.0 and later
- VPN 3000 Concentrator Software Releases 3.0 and later

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.

## Conventions

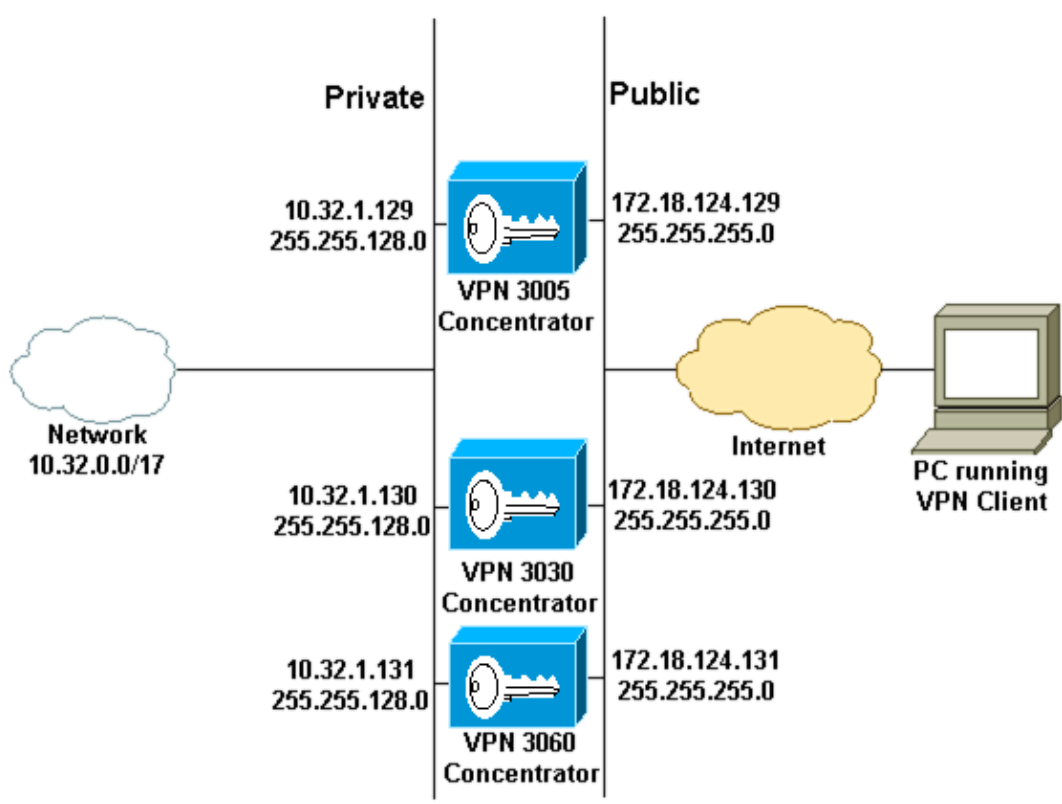
Refer to the Cisco Technical Tips Conventions for more information on document conventions.

## Key Definitions

This table defines key words associated with VPN 3000 Concentrators and load-balancing.

Key Word	Definition
Virtual Cluster	In a virtual cluster, VPN 3000 Concentrators work together as a single entity. The cluster is known by one IP address to the outside VPN Client space. This virtual IP address is not tied to a specific device in the VPN cluster but is serviced by the virtual cluster master. The virtual IP address has to be a routable address.
Virtual Cluster Agent (VCA)	VCA is added to the VPN 3000 code in order to control the load-balancing on the VPN 3000 Concentrators. Minimal changes were made to the IPsec code in order to handle the virtual cluster IP address.
Load Information	The master maintains the load information from all secondary VPN 3000 Concentrators in the cluster. Each secondary sends load information in the KeepAlive message exchange to the master. Load is calculated as a percentage of current active sessions divided by the configured maximum-allowed connections.

## Network Diagram



## Addresses

This table shows public and private addresses for VPN 3000 Concentrators.

VPN 3000 Concentrator	Private		Public	
	Interface	Subnet Mask	Interface	Subnet Mask
3005	10.32.1.129	255.255.128.0	172.18.124.129	255.255.255.0
3030	10.32.1.130	255.255.128.0	172.18.124.130	255.255.255.0
3060	10.32.1.131	255.255.128.0	172.18.124.131	255.255.255.0

## Restrictions

These restrictions apply to load-balancing on VPN 3000 Concentrators:

- Load-balancing can only occur with Cisco Release 3.x (or later) IPsec VPN Clients-to-LAN connections. Earlier VPN Clients can still connect to their target Ethernet2 (public) port IP address within the cluster.

**Note:** Load balancing can still work if both VPN Concentrators do not have the same software version loaded on them.

- VPN virtual cluster IP address, User Datagram Protocol (UDP) port, and shared secret must be identical on every device in the virtual cluster.
- All devices in the virtual cluster must be on the same public and private IP subnets.
- A filter has to be applied on both public and private interfaces. The defaults are:
  - ◆ private filter on the private interface
  - ◆ public filter on the public interface

# Configuration

## IP Address Assignment

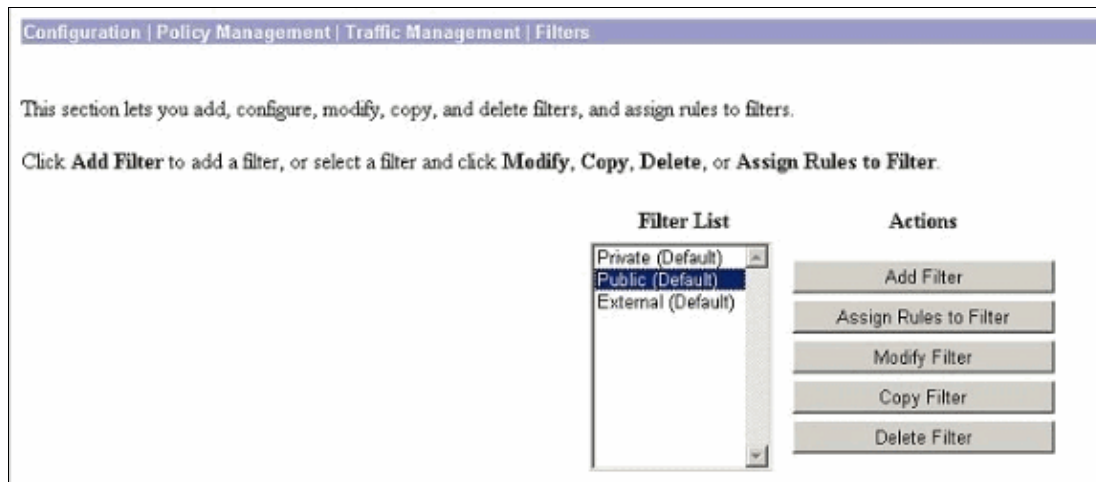
Ensure that the IP addresses are configured on the public and private interfaces and you are able to get to the Internet from your VPN 3000 Concentrator.

## Filter Configuration

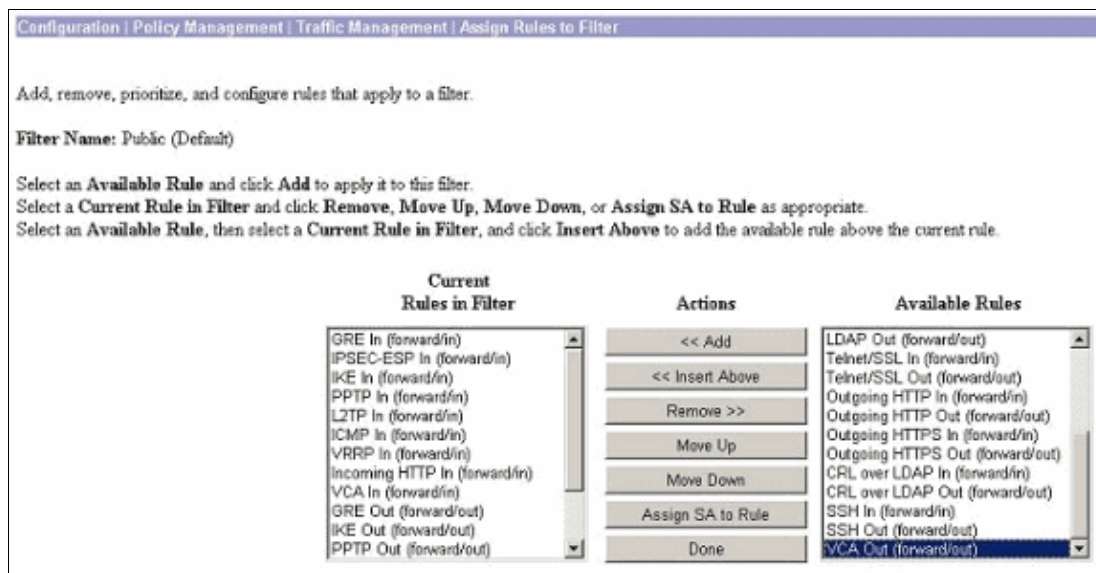
In order for load-balancing to work properly, you need to add a new rule in your current filters for VCA.

**Note:** The private filter by default has a "permit any" rule. Therefore, the addition of the VCA-specific rules to this filter might not be necessary).

In order to add this, select **Configuration > Policy Management > Traffic Management > Assign Rules to filter**.



Then, add **VCA in** and **VCA out** in your filter.



## Cluster Configuration

In order to configure load-balancing, select **Configuration > System > Load Balancing**, and configure these parameters:

- VPN Virtual Cluster IP Address
- VPN Virtual Cluster UDP Port
- Encryption
- IPsec Shared Secret
- Verify Shared Secret
- Load-Balancing Enable
- Priority
- NAT Assigned IP Address

Configuration | System | Load Balancing

Configure Load Balancing. All devices in the cluster must share an identical Cluster Configuration. Note: the public and private filters need to have the VCA In and VCA Out filter rules added. These filter rules may need to be modified if the VPN Virtual Cluster UDP Port is modified.

**Cluster Configuration**

VPN Virtual Cluster IP Address: 172.18.124.254 Enter the cluster's virtual IP address.

VPN Virtual Cluster UDP Port: 9023 Enter the cluster's UDP port.

Encryption:  Check to enable IPsec encryption between cluster devices.

IPSec Shared Secret: \*\*\*\*\* Enter the IPsec Shared secret in the cluster.

Verify Shared Secret: \*\*\*\*\* Re-enter the IPsec Shared secret in the cluster.

**Device Configuration**

Load Balancing Enable:  Check to enable load balancing for this device.

Priority: 1 Enter the priority of this device. The range is from 1 to 10.

NAT Assigned IP Address: 0.0.0.0 Enter the IP address that this device's IP address is translated to by NAT. Enter 0.0.0.0 if NAT is not being used, or the device is not behind a firewall using NAT.

Apply Cancel

### VPN Virtual Cluster IP Address

Enter the single IP address that represents the entire virtual cluster. Choose an IP address that is within the public subnet address range shared by all the VPN 3000 Concentrators in the virtual cluster. In this example, 172.18.124.254 is used as the virtual address. Make sure that you use the same virtual address on all VPN 3000 Concentrators.

### VPN Virtual Cluster UDP Port

The VPN virtual cluster UDP port is the UDP port number that VCA uses for its communication between VPN 3000 Concentrators. If another application uses this port, enter the UDP destination port number you want to use for load-balancing. The default port is 9023. Make sure that you use the same UDP port on all the VPN 3000 Concentrators.

### Encryption

You can encrypt VCA communication in the load-balancing environment. The VPN 3000 Concentrators in the virtual cluster can communicate via LAN-to-LAN tunnels with the use of IPsec. In order to ensure that all load-balancing information communicated between the VPN 3000 Concentrators is encrypted, check **Encryption**. Note that this parameter is optional. However, if enabled, it improves the load-balancing on the VPN 3000 Concentrators. If you use this option, ensure that all VPN 3000 Concentrators use Encryption in your environment.

### IPsec Shared Secret

The IPsec Shared Secret option is available only if you check the Encryption option. Enter the IPsec Shared Secret for the virtual cluster. The Shared Secret is a common password that authenticates members of the

virtual cluster. IPsec uses the Shared Secret as a pre-shared key in order to establish secure tunnels between virtual cluster peers. In the example in this document, "cisco123" is used as the pre-shared key. Make sure that you enter the same key on all the VPN 3000 Concentrators.

### Verify Shared Secret

Reenter the IPsec Shared Secret.

### Load-Balancing Enable

Check the **Load-Balancing Enable** box to include the VPN 3000 Concentrator in the virtual cluster. If you disable this parameter, then load-balancing is disabled on this particular VPN 3000 Concentrator.

### Priority

Enter a priority for the VPN 3000 Concentrator within the virtual cluster. The priority is a number from 1 to 10 that indicates the likelihood of this device becoming the virtual cluster master either at startup or if an existing master fails. The higher you set the priority (10), the more likely this device becomes the virtual cluster master. If your virtual cluster includes different models of VPN 3000 Concentrators, it is recommended that you choose the device with the greatest load capacity to be the virtual cluster master. For this reason, priority defaults are hardware dependent (see this table).

VPN Concentrator Model	Priority
3005	1
3015	3
3030	5
3060	7
3080	9

If your virtual cluster is made up of identical devices (for example, if all the devices in the virtual cluster are VPN Concentrator 3060s), set the priority of every device to **10**. When all identical devices are set to the highest priority, it shortens the length of time you need in order to select the virtual cluster master.

If the devices in the virtual cluster are powered up at different times, the first device to be powered up assumes the role of virtual cluster master. Because every virtual cluster requires a master, each device in the virtual cluster checks at power-up in order to ensure that the cluster has a virtual master. If none exists, that device takes on the role. Devices powered up and added to the cluster later become secondary devices.

If all the devices in the virtual cluster are powered up simultaneously, the device with the highest priority setting becomes the virtual cluster master. If two or more devices in the virtual cluster are powered up simultaneously and both have the highest priority setting, the one with the lowest IP address becomes the virtual cluster master.

Once the virtual cluster is established and operates, if the VPN 3000 Concentrator that holds the role of the virtual cluster master fails, the secondary device with the highest priority setting takes over. If two or more devices in the virtual cluster both have the highest priority setting, the one with the lowest IP address becomes the virtual cluster master.

## NAT Assigned IP Address

If the VPN 3000 Concentrators are behind a firewall that uses Network Address Translation (NAT), then specify the NAT IP address here. In this example, the VPN 3000 Concentrators are not behind any NAT device. If this is the case, then enter **0.0.0.0**. (default setting).

This screen shot is taken from the 172.18.124.130 VPN Concentrator.

Configuration | System | Load Balancing

Configure Load Balancing. All devices in the cluster must share an identical Cluster Configuration. Note: the public and private filters need to have the *PCA In* and *PCA Out* filter rules added. These filter rules may need to be modified if the *VPN Virtual Cluster UDP Port* is modified.

**Cluster Configuration**

VPN Virtual Cluster IP Address: 172.18.124.254 Enter the cluster's virtual IP address.

VPN Virtual Cluster UDP Port: 5023 Enter the cluster's UDP port.

Encryption:  Check to enable IPSec encryption between cluster devices.

IPSec Shared Secret: \*\*\*\*\* Enter the IPSec Shared secret in the cluster.

Verify Shared Secret: \*\*\*\*\* Re-enter the IPSec Shared secret in the cluster.

**Device Configuration**

Load Balancing Enable:  Check to enable load balancing for this device.

Priority: 7 Enter the priority of this device. The range is from 1 to 10.

NAT Assigned IP Address: 0.0.0.0 Enter the IP address that this device's IP address is translated to by NAT. Enter 0.0.0.0 if NAT is not being used, or the device is not behind a firewall using NAT.

Apply Cancel

This screen shot is taken from the 172.18.124.131 VPN Concentrator.

Configuration | System | Load Balancing

Configure Load Balancing. All devices in the cluster must share an identical Cluster Configuration. Note: the public and private filters need to have the *PCA In* and *PCA Out* filter rules added. These filter rules may need to be modified if the *VPN Virtual Cluster UDP Port* is modified.

**Cluster Configuration**

VPN Virtual Cluster IP Address: 172.18.124.254 Enter the cluster's virtual IP address.

VPN Virtual Cluster UDP Port: 5023 Enter the cluster's UDP port.

Encryption:  Check to enable IPSec encryption between cluster devices.

IPSec Shared Secret: \*\*\*\*\* Enter the IPSec Shared secret in the cluster.

Verify Shared Secret: \*\*\*\*\* Re-enter the IPSec Shared secret in the cluster.

**Device Configuration**

Load Balancing Enable:  Check to enable load balancing for this device.

Priority: 7 Enter the priority of this device. The range is from 1 to 10.

NAT Assigned IP Address: 0.0.0.0 Enter the IP address that this device's IP address is translated to by NAT. Enter 0.0.0.0 if NAT is not being used, or the device is not behind a firewall using NAT.

Apply Cancel

## Monitoring

In order to monitor the load-balancing feature on the VPN 3000 Concentrator side, select **Monitoring > Statistics > Load Balancing**, and make sure that all the participating VPN 3000 Concentrators are listed as peers. On the 172.18.124.129 VPN Concentrator, you see 172.18.124.130 and 172.18.124.131 as the peers. Note that 172.18.124.131 is the master VPN Concentrator.

Private IP Address	Public IP Address	Mapped IP Address	Role	Device Type	Load	Sessions	Priority	Duration
10.32.1.130	172.18.124.130	0.0.0.0	Secondary	VPN3030	N/A	N/A	7	0:18:27
10.32.1.131	172.18.124.131	0.0.0.0	Master	VPN3060	N/A	N/A	7	0:18:36

On the 172.18.124.130 VPN Concentrator, you see 172.18.124.129 and 172.18.124.131 as the peers.

Private IP Address	Public IP Address	Mapped IP Address	Role	Device Type	Load	Sessions	Priority	Duration
10.32.1.129	172.18.124.129	0.0.0.0	Secondary	VPN3005	N/A	N/A	1	0:18:50
10.32.1.131	172.18.124.131	0.0.0.0	Master	VPN3060	N/A	N/A	7	2:07:52

On the 172.18.124.131 VPN Concentrator, you see 172.18.124.129 and 172.18.124.130 as the peers. Role is listed as Master for the 172.18.124.131 VPN Concentrator.

Private IP Address	Public IP Address	Mapped IP Address	Role	Device Type	Load	Sessions	Priority	Duration
10.32.1.129	172.18.124.129	0.0.0.0	Secondary	VPN3005	0%	0	1	0:18:49
10.32.1.130	172.18.124.130	0.0.0.0	Secondary	VPN3030	0%	1	7	2:07:50

If you enable **Encryption** under the Load Balancing configuration window, you see the VCA/IPsec tunnels with your peer when you select **Monitoring > Sessions**.

This screen shot is taken from the 172.18.124.129 VPN Concentrator.

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.

Group:

**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
0	0	4	4	5	100	14

**LAN-to-LAN Sessions**

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

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
No LAN-to-LAN Sessions							

**Remote Access Sessions**

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

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

**Management Sessions**

[\[ LAN-to-LAN Sessions \]](#) [\[ Remote Access Sessions \]](#)

Administrator	IP Address	Protocol	Encryption	Login Time	Duration
admin	172.18.124.104	HTTP	None	Oct 16 12:30:10	0:16:03
admin	64.102.55.142	HTTP	None	Oct 16 12:43:56	0:02:17
10.32.1.131	10.32.1.131	VCA/IPSec	3DES-168	Oct 16 12:28:29	0:17:43
10.32.1.130	10.32.1.130	VCA/IPSec	3DES-168	Oct 16 12:28:57	0:17:16

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.

Group:

**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
0	1	4	5	5	1500	13

**LAN-to-LAN Sessions**

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

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
No LAN-to-LAN Sessions							

**Remote Access Sessions**

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

Username	Group	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
3002	3002group	172.18.124.218	172.16.1.1	IPSec/NAT	3DES-168	Oct 16 09:42:30	0:04:06	0	0

**Management Sessions**

[\[ LAN-to-LAN Sessions \]](#) [\[ Remote Access Sessions \]](#)

Administrator	IP Address	Protocol	Encryption	Login Time	Duration
10.32.1.129	10.32.1.129	VCA/IPSec	3DES-168	Oct 16 09:30:39	0:15:57
10.32.1.131	10.32.1.131	VCA/IPSec	3DES-168	Oct 16 07:41:13	2:05:22
admin	172.18.124.104	HTTP	None	Oct 16 09:29:18	0:17:17
admin	64.102.55.142	HTTP	None	Oct 16 09:45:28	0:01:08

Monitoring   Sessions							Tuesday, 16 October 2011 12:58:13		
This screen shows statistics for sessions. To refresh the statistics, click <b>Refresh</b> . Select a <b>Group</b> to filter the sessions. For more information on a session, click on that session's name.							Refresh		
Group: <input type="text" value="-All-"/>									
<b>Session Summary</b>									
Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Concurrent Sessions Limit	Total Cumulative Sessions			
0	0	3	3	4	5000	13			
<b>LAN-to-LAN Sessions</b>			[ Remote Access Sessions   Management Sessions ]						
Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx		
No LAN-to-LAN Sessions									
<b>Remote Access Sessions</b>			[ LAN-to-LAN Sessions   Management Sessions ]						
Username	Group	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
No Remote Access Sessions									
<b>Management Sessions</b>			[ LAN-to-LAN Sessions   Remote Access Sessions ]						
Administrator	IP Address	Protocol	Encryption	Login Time	Duration				
admin	64.102.55.142	HTTP	None	Oct 16 12:49:13	0:01:00				
10.32.1.130	10.32.1.130	VCA/IPSec	3DES-168	Oct 16 10:44:42	2:05:31				
10.32.1.129	10.32.1.129	VCA/IPSec	3DES-168	Oct 16 12:53:39	0:16:33				

## Test the Load-Balancing Feature

**Note:** Virtual addresses are not pingable.

The master always attempts to have the least load as it is burdened with an additional, inherent load. The master maintains all of the administrative LAN-to-LAN sessions, calculates all other cluster member loading, and handles all VPN Client redirects.

In a freshly configured, functioning cluster, the master has about a 1 percent load before any connections are established. Therefore, the master redirects connections to backup VPN 3000 Concentrators until their percentage of load is higher than the percentage of load on the master. For example, if you have two 3030 devices in an "idle" state, the master has a 1 percent load, and the secondary is given 30 connections (2 percent load) before the master accepts connections.

In order to verify that the master accepts connections, you can lower the maximum number of connections (**Configuration > System > General > Sessions**) to an artificially low number in order to quickly increase the load placed on the backup VPN 3000 Concentrator.

In order to test the load-balancing feature, configure the VPN Client to connect to the virtual IP address (172.18.124.254 in this case). The master diverts the IPsec tunnel to one of the secondary VPN 3000 Concentrators that it knows about. If you monitor the Session on the 172.18.124.129 VPN Concentrator, it has accepted the VPN Client tunnel.

Monitoring   Sessions							Thursday, 18 October 2001 16:02:23		
This screen shows statistics for sessions. To refresh the statistics, click <b>Refresh</b> . Select a <b>Group</b> to filter the sessions. For more information on a session, click on that session's name.							Refresh		
Group: <input type="text" value="--All--"/>									
<b>Session Summary</b>									
Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Concurrent Sessions Limit	Total Cumulative Sessions			
0	1	3	4	5	100	20			
<b>LAN-to-LAN Sessions</b>			[ Remote Access Sessions   Management Sessions ]						
Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx		
No LAN-to-LAN Sessions									
<b>Remote Access Sessions</b>			[ LAN-to-LAN Sessions   Management Sessions ]						
Username	Group	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
ipsecuser	ipsecgroup	172.18.124.96	10.1.2.1	IPSec/NAT	3DES-168	Oct 18 09:49:17	0:13:05	280	16112
<b>Management Sessions</b>			[ LAN-to-LAN Sessions   Remote Access Sessions ]						
Administrator	IP Address	Protocol	Encryption	Login Time	Duration				
10.32.1.130	10.32.1.130	VCA/IPSec	3DES-168	Oct 17 15:27:33	18:34:49				
admin	64.102.55.142	HTTP	None	Oct 18 10:00:08	0:02:14				
10.32.1.131	10.32.1.131	VCA/IPSec	3DES-168	Oct 16 12:28:29	45:33:53				

This screen shot is taken from the 172.18.124.129 VPN Concentrator. The load on this VPN 3000 Concentrator is 1 percent (current connections/maximum connection = 1/100 = 1%).

Monitoring   Statistics   Load Balancing										Thursday, 18 October 2001 10:36:33
Refresh										
Enabled?		Yes								
Role		Secondary								
Load		1%								
Number of Peers		2								
<b>Peers</b>										
Private IP Address	Public IP Address	Mapped IP Address	Role	Device Type	Load	Sessions	Priority	Duration		
10.32.1.130	172.18.124.130	0.0.0.0	Secondary	VPN3030	N/A	N/A	7	18:38:48		
10.32.1.131	172.18.124.131	0.0.0.0	Master	VPN3060	N/A	N/A	7	45:37:43		

In this screen shot, the load on the master VPN Concentrator (172.18.124.131) is 0 percent, the load on 172.18.124.129 is 1 percent, and the load for 172.18.124.130 is 0 percent.

Monitoring   Statistics   Load Balancing										Thursday, 18 October 2001 10:11:58
Refresh										
Enabled?		Yes								
Role		Master								
Load		0%								
Number of Peers		2								
<b>Peers</b>										
Private IP Address	Public IP Address	Mapped IP Address	Role	Device Type	Load	Sessions	Priority	Duration		
10.32.1.129	172.18.124.129	0.0.0.0	Secondary	VPN3005	1%	1	1	45:57:32		
10.32.1.130	172.18.124.130	0.0.0.0	Secondary	VPN3030	0%	1	7	18:38:13		

## Troubleshoot

Problem	Solution
Encryption is enabled, but you	Make sure that <b>Encryption</b> is enabled on all the VPN 3000 Concentrators that participate in load-balancing. Also make sure

do not see anything under <b>Monitoring &gt; Sessions</b> for IPsec/VCA tunnels.	that IPsec shared secret is correct on all the VPN 3000 Concentrators.
Load-balancing is enabled, but you do not see any peers under <b>Monitoring &gt; Statistics &gt; Load-Balancing.</b>	<p>Ensure you can ping the other VPN 3000 Concentrators (public and private interfaces). If you are able to ping, check your filters and make sure that <b>VCA in</b> and <b>VCA out</b> rules are enabled on the filters. In order to verify that, if you enable the <b>LBSSF</b> class on the VPN 3000 Concentrator with severity to log set to 1–8, you should see these messages in your logs:</p> <pre> 32198 10/19/2001 10:08:05.260 SEV=8 LBSSF/25 RPT=42577 LBSSF received KEEPALIVE request from [10.32.1.130]  32199 10/19/2001 10:08:05.260 SEV=8 LBSSF/24 RPT=42573 LBSSF sent KEEPALIVE response to [10.32.1.130]  32200 10/19/2001 10:08:05.890 SEV=8 LBSSF/25 RPT=42578 LBSSF received KEEPALIVE request from [10.32.1.129]  32201 10/19/2001 10:08:05.890 SEV=8 LBSSF/24 RPT=42574 LBSSF sent KEEPALIVE response to [10.32.1.129]  32202 10/19/2001 10:08:06.260 SEV=8 LBSSF/25 RPT=42579 LBSSF received KEEPALIVE request from [10.32.1.130]  32203 10/19/2001 10:08:06.260 SEV=8 LBSSF/24 RPT=42575 LBSSF sent KEEPALIVE response to [10.32.1.130]</pre>

## NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for VPN
Service Providers: VPN Service Architectures
Service Providers: Network Management
Virtual Private Networks: General

## 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](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

