



Configuring Load Balancing

This chapter describes how to configure load balancing using ASDM. It includes the following sections.

- [Introduction, page 11-1](#)
- [Implementing Load Balancing, page 11-2](#)
- [VPN Load-Balancing Cluster Configurations, page 11-3](#)
- [Configuring Load Balancing, page 11-4](#)
- [Configuring VPN Session Limits, page 11-6](#)

Introduction

If you have a remote-access configuration in which you are using two or more security appliances or VPN Concentrators connected on the same network to handle remote sessions, you can configure these devices to share their session load. This feature is called *load balancing*. To implement load balancing, group together logically two or more devices on the same private LAN-to-LAN network, private subnet, and public subnet into a *virtual cluster*.

All devices in the virtual cluster carry session loads. Load balancing directs session traffic to the least loaded device in the cluster, thus distributing the load among all devices. It makes efficient use of system resources and provides increased performance and high availability.

One device in the virtual cluster, the *virtual cluster master*, directs incoming traffic to the other devices, called *secondary devices*. The virtual cluster master monitors all devices in the cluster, keeps track of how busy each is, and distributes the session load accordingly. The role of virtual cluster master is not tied to a physical device; it can shift among devices. For example, if the current virtual cluster master fails, one of the secondary devices in the cluster takes over that role and immediately becomes the new virtual cluster master.

The virtual cluster appears to outside clients as a single *virtual cluster IP address*. This IP address is not tied to a specific physical device. It belongs to the current virtual cluster master; that is, it is a virtual address. A VPN Client attempting to establish a connection connects first to this virtual cluster IP address. The virtual cluster master then sends back to the client the public IP address of the least-loaded available host in the cluster. In a second transaction (transparent to the user), the client connects directly to that host. In this way, the virtual cluster master directs traffic evenly and efficiently across resources.



Note

All clients other than the Cisco VPN Client, Cisco VPN 3002 Hardware Client, or the Cisco ASA model 5505 when configured as a hardware client connect directly to the security appliance as usual; they do not use the virtual cluster IP address.

If a machine in the cluster fails, the terminated sessions can immediately reconnect to the virtual cluster IP address. The virtual cluster master then directs these connections to another active device in the cluster. Should the virtual cluster master itself fail, another device in the cluster immediately and automatically takes over as the new virtual session master. Even if several devices in the cluster fail, users can continue to connect to the cluster as long as any one device in the cluster is up and available.

Implementing Load Balancing

Enabling load balancing involves:

- Configuring the load-balancing cluster by establishing a common virtual cluster IP address, UDP port (if necessary), and IPsec shared secret for the cluster. These values are identical for every device in the cluster.
- Configuring the participating device by enabling load balancing on the device and defining device-specific properties. These values vary from device to device.

**Note**

VPN load balancing requires an active 3DES/AES license. The security appliance checks for the existence of this crypto license before enabling load balancing. If it does not detect an active 3DES or AES license, the security appliance prevents the enabling of load balancing and also prevents internal configuration of 3DES by the load balancing system, unless the license permits this usage.

Prerequisites

Load balancing is disabled by default. You must explicitly enable load balancing.

You must have first configured the public and private interfaces and also have previously configured the interface to which the virtual cluster IP address refers.

All devices that participate in a cluster must share the same cluster-specific values: IP address, encryption settings, encryption key, and port.

Eligible Platforms

A load-balancing cluster can include security appliance models ASA 5520 and higher. You can also include VPN 3000 Series Concentrators in the cluster. While mixed configurations are possible, administration is generally simpler if the cluster is homogeneous.

Eligible Clients

Load balancing is effective only on remote sessions initiated with the following clients:

- Cisco VPN Client (Release 3.0 and later)
- Cisco VPN 3002 Hardware Client (Release 3.5 or later)
- Cisco ASA model 5505 when configured as a hardware client
- Cisco PIX 501/506E when acting as an Easy VPN client.

Load balancing works with both IPSec clients and WebVPN sessions. All other clients, including LAN-to-LAN connections, can connect to a security appliance on which load balancing is enabled, but they cannot participate in load balancing.

VPN Load-Balancing Cluster Configurations

A load-balancing cluster can consist of all ASA Release 7.0(x) security appliances, all ASA Release 7.1(1) security appliances or higher, all VPN 3000 Concentrators, or a mixture of these, subject to the following restrictions:

- Load-balancing clusters that consist of all ASA 7.0(x) security appliances, all ASA 7.1(1) security appliances or higher, or all VPN 3000 Concentrators can run load balancing for a mixture of IPSec and WebVPN sessions.
- Load-balancing clusters that consist of a both of ASA 7.0(x) security appliances and VPN 3000 Concentrators can run load balancing for a mixture of IPSec and WebVPN sessions.
- Load-balancing clusters that include ASA 7.1(1) security appliances or higher and either ASA 7.0(x) or VPN 3000 Concentrators or both can support only IPSec sessions. In such a configuration, however, the ASA 7.1(1) or higher security appliances might not reach their full IPSec capacity. [Scenario 1: Mixed Cluster with No WebVPN Connections, page 11-4](#), illustrates this situation.

With Release 7.1(1) and higher, IPSec and WebVPN sessions count or weigh equally in determining the load that each device in the cluster carries. This represents a departure from the load balancing calculation for the ASA Release 7.0(x) software and the VPN 3000 Concentrator, in that these platforms both use a weighting algorithm that calculates 1 WebVPN session as equivalent in load to 10 IPSec sessions.

The virtual master of the cluster assigns session loads to the members of the cluster. An ASA Release 7.1(1) or higher security appliance regards all sessions, WebVPN or IPSec, as equal and assigns them accordingly. An ASA Release 7.0(x) security appliance or a VPN 3000 Concentrator performs the 10:1 weighting calculations in assigning session loads.

If you have a mixed configuration—that is, if your load-balancing cluster includes devices running a mixture of ASA software releases or at least one security appliance running ASA Release 7.1(1) or higher and a VPN 3000 Concentrator—the difference in weighting algorithms becomes an issue if the initial cluster master fails and another device takes over as master.

Suppose, for example, a security appliance running ASA Release 7.1(1) software is the initial cluster master. Then that device fails. Another device in the cluster takes over automatically as master and applies its own load-balancing algorithm to determine processor loads within the cluster. A cluster master running ASA Release 7.1(1) software cannot weight session loads in any way other than what that software provides. Therefore, it cannot assign a combination of IPSec and WebVPN session loads properly to ASA devices running earlier versions nor to VPN 3000 Concentrators. Conversely, a VPN 3000 Concentrator acting as the cluster master cannot assign loads properly to an ASA Release 7.1(1) security appliance. [Scenario 2: Mixed Cluster Handling WebVPN Connections, page 11-4](#), illustrates this dilemma.



Note

You can configure the number of IPSec and WebVPN sessions to allow, up to the maximum allowed by your configuration and license. See [Configuring VPN Session Limits, page 11-6](#) for a description of how to set these limits.

Mixed Cluster Scenarios

The following scenarios illustrate the use of VPN load balancing in clusters consisting of a mixture of security appliances running ASA Release 7.1(1) or higher and ASA Release 7.0(x) software, as well as VPN 3000 Series Concentrators.

Scenario 1: Mixed Cluster with No WebVPN Connections

In this scenario, the cluster consists of a mixture of security appliances and VPN 3000 Concentrators. Some of the security appliance cluster peers are running ASA Release 7.0(x), and some are running Release 7.1(1) or higher. The pre-7.1(1) and VPN 3000 peers do not have any SSL VPN connections, and the 7.1(1) or higher cluster peers have only the base SSL VPN license, which allows two WebVPN sessions, but there are no SSL VPN connections. In this case, all the connections are IPsec, and load balancing works fine.

The two WebVPN licenses have a very small effect on the user's taking advantage of the maximum IPsec session limit, and then only when a VPN 3000 Concentrator is the cluster master. In general, the smaller the number of WebVPN licenses is on a security appliance in a mixed cluster, the smaller the effect on the ASA 7.1(1) or higher device being able to reach its IPsec session limit in a scenario where there are only IPsec sessions.

Scenario 2: Mixed Cluster Handling WebVPN Connections

This scenario is similar to the previous one, in that the cluster consists of a mixture of security appliances and VPN 3000 Concentrators. Some of the security appliance cluster peers are running ASA Release 7.0(x) and some are running Release 7.1(1) or higher. In this case, however, the cluster is handling SSL VPN connections as well as IPsec connections.

If a device that is running software earlier than ASA Release 7.1(1) is the cluster master, the master applies the protocol and logic in effect prior to Release 7.1(1). That is, sessions might be directed to load-balancing peers that have exceeded their session limit. In that case, the user is denied access.

If the cluster master is a device running ASA Release 7.0(x) software, the old session-weighting algorithm applies only to the pre-7.1(1) peers in the cluster. No one should be denied access in this case. Because the pre-7.1(1) peers use the session-weighting algorithm, they are more lightly loaded.

An issue arises, however, because you cannot guarantee that the 7.1(1) or higher peer is always the cluster master. If the cluster master fails, another peer assumes the role of master. The new master might be any of the eligible peers. Because of the innately unpredictability of the results, we recommend that you avoid configuring this type of cluster.

Configuring Load Balancing

To configure load balancing on a security appliance running ASA Release 7.1(1) or higher software, configure the following elements for each device that participates in the cluster.

- Public and private interfaces
- VPN load-balancing cluster attributes

**Note**

All participants in the cluster must have an identical cluster configuration, except for the device priority within the cluster.

Configuring the Public and Private Interfaces for Load Balancing

To configure a load-balancing cluster, select **Configuration > VPN > Load Balancing** (Figure 11-1).

Figure 11-1 Load Balancing Window

To configure load balancing, do the following steps:

- Step 1** Check the Participate in Load Balancing check box.
- Step 2** Configure the attributes in the VPN Cluster Configuration area, as follows:



Note All servers in the cluster must have an identical cluster configuration.

- a. Enter the **Cluster IP Address**. This is 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 security appliances in the virtual cluster.
- b. Specify the **UDP Port** for the virtual cluster in which this device participates. The default value is 9023. If another application is using this port, enter the UDP destination port number you want to use for load balancing.

- c. Optionally, enable IPsec encryption for the cluster by checking the check box for **Enable IPsec Encryption**. The default is no encryption. This attribute enables or disables IPsec encryption. If you configure this attribute, you must also specify and verify a shared secret. The security appliances in the virtual cluster communicate via LAN-to-LAN tunnels using IPsec. To ensure that all load-balancing information communicated between the devices is encrypted, enable this attribute.

**Note**

When using encryption, you must have previously configured the load-balancing inside interface. If that interface is not enabled, an error message appears when you try to configure cluster encryption.

If the load-balancing inside interface was enabled when you configured cluster encryption, but was disabled before you configured the participation of the device in the virtual cluster, you get an error message when you select the Participate in Load Balancing Cluster check box, and encryption is not enabled for the cluster.

- d. If you enable cluster encryption, you must also specify the IPsec shared secret by entering a value in the **IPsec Shared Secret** field, then entering the same value in the **Verify Secret** field. These fields must match. This command specifies the shared secret to between IPsec peers when you have enabled IPsec encryption. The value you enter in the field appears as consecutive asterisk characters

Step 3 Configure the attributes in the VPN Server Configuration area, as follows:

- a. Select the **Public** interface on the security appliance. This command specifies the name or IP address of the public interface for load balancing for this device. The default value is outside.
- b. Select the **Private** interface on the security appliance. This command specifies the name or IP address of the private interface for load balancing for this device. The default value is inside.
- c. Set the priority to assign to this device within the cluster. The range is from 1 to 10. The priority indicates the likelihood of this device becoming the virtual cluster master, either at start-up or when an existing master fails. The higher you set the priority (for example, 10), the more likely it is that this device becomes the virtual cluster master.
- d. If you want to apply network address translation for this device, enter the NAT Assigned IP Address for the device.

Configuring VPN Session Limits

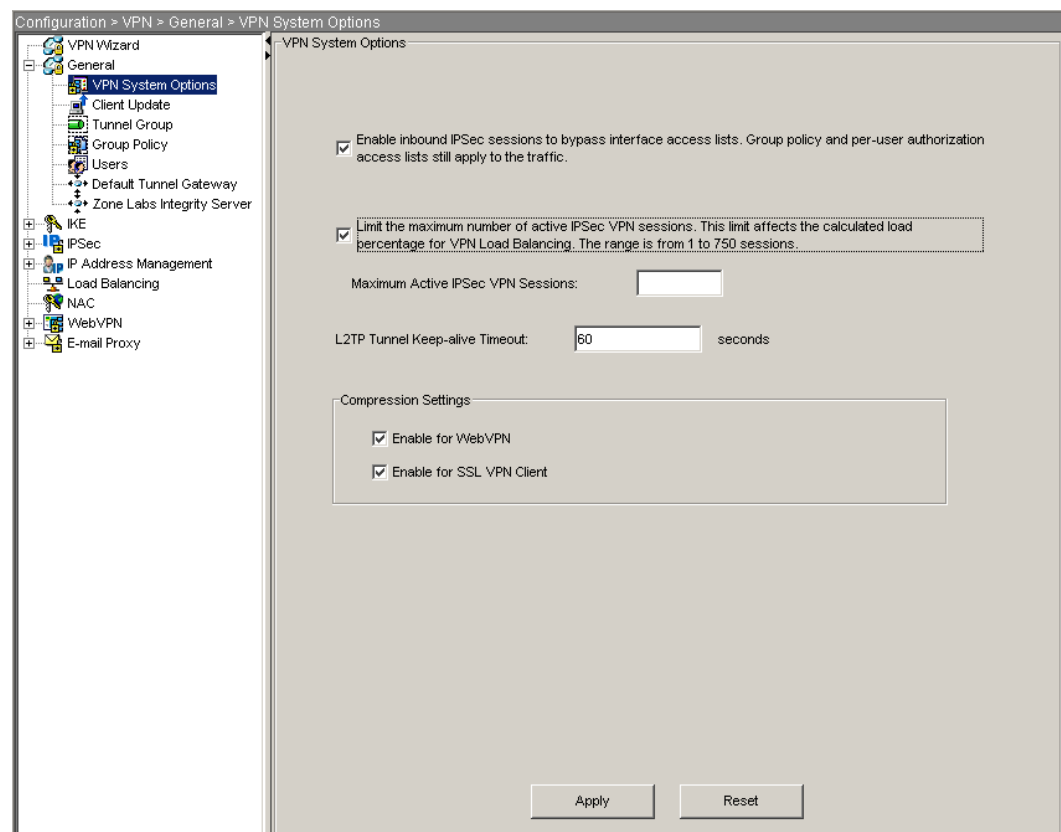
You can run as many IPsec and WebVPN sessions as your platform and license for the security appliance supports. To view the licensing information for your security appliance, select the Home icon at the top of the opening window for ASDM and select the License tab (Figure 11-2).

Figure 11-2 License Information



To limit the maximum number of active IPsec VPN sessions to a lower value than the security appliance allows, select **Configuration > VPN > General > VPN System Options** (Figure 11-3).

Figure 11-3 VPN System Options Window



Specify the limit that you want to apply in the **Maximum Active IPsec VPN Sessions** field. The maximum number of sessions depends on your license. This limit affects the calculated load percentage for VPN Load Balancing.

For example, if the security appliance license allows 750 IPsec sessions, and you want to limit the number of IPsec sessions to 500, enter 500 in the **Maximum Active IPsec VPN Sessions** field.

To remove the session limit, clear the **Limit the maximum number of active IPsec VPN sessions** check box.

For a complete description of the features available with each license, see *Cisco Security Appliance Command Line Configuration Guide*, Appendix A, “Feature Licenses and Specifications.”
