High Availability Options

High Availability Options

Distributed VPN Clustering, Load balancing and Failover are high-availability features that function differently and have different requirements. In some circumstances you may use multiple capabilities in your deployment. The following sections describe these features. Refer to the appropriate release of the ASA General Operations CLI Configuration Guide for details on Distributed VPN and Failover. Load Balancing details are included here.

VPN and Clustering on the FXOS Chassis

An ASA FXOS Cluster supports one of two mutually exclusive modes for S2S VPN, centralized or distributed:

- Centralized VPN Mode. The default mode. In centralized mode, VPN connections are established with the control unit of the cluster only.

  VPN functionality is limited to the control unit and does not take advantage of the cluster high availability capabilities. If the control unit fails, all existing VPN connections are lost, and VPN connected users see a disruption in service. When a new control unit is elected, you must reestablish the VPN connections.

  When you connect a VPN tunnel to a Spanned interface address, connections are automatically forwarded to the control unit. VPN-related keys and certificates are replicated to all units.

- Distributed VPN Mode. In this mode, S2S IPsec IKEv2 VPN connections are distributed across members of an ASA cluster providing scalability. Distributing VPN connections across the members of a cluster allows both the capacity and throughput of the cluster to be fully utilized, significantly scaling VPN support beyond Centralized VPN capabilities.

Note Centralized VPN clustering mode supports S2S IKEv1 and S2S IKEv2.

Distributed VPN clustering mode supports S2S IKEv2 only.

Distributed VPN clustering mode is supported on the Firepower 9300 only.

Remote access VPN is not supported in centralized or distributed VPN clustering mode.

VPN Load Balancing

VPN load balancing is a mechanism for equitably distributing remote-access VPN traffic among the devices in a VPN load-balancing group. It is based on simple distribution of traffic without taking into account throughput or other factors. A VPN load-balancing group consists of two or more devices. One device is the director, and the other devices are member devices. Group devices do not need to be of the exact same type, or have identical software versions or configurations.

All active devices in a VPN load-balancing group carry session loads. VPN load balancing directs traffic to the least-loaded device in the group, distributing the load among all devices. It makes efficient use of system resources and provides increased performance and high availability.

Failover

A failover configuration requires two identical ASAs connected to each other through a dedicated failover link and, optionally, a stateful failover link. The health of the active interfaces and units is monitored to determine when specific failover conditions are met. If those conditions occur, failover occurs. Failover supports both VPN and firewall configurations.

The ASA supports two failover configurations: Active/Active failover and Active/Standby failover.

With Active/Active failover, both units can pass network traffic. This is not true load balancing, although it might appear to have the same effect. When failover occurs, the remaining active unit takes over passing the combined traffic, based on the configured parameters. Therefore, when configuring Active/Active failover, you must make sure that the combined traffic for both units is within the capacity of each unit.

With Active/Standby failover, only one unit passes traffic, while the other unit waits in a standby state and does not pass traffic. Active/Standby failover lets you use a second ASA to take over the functions of a failed unit. When the active unit fails, it changes to the standby state, while the standby unit changes to the active state. The unit that becomes active assumes the IP addresses (or, for transparent firewall, the management IP address) and MAC addresses of the failed unit and begins passing traffic. The unit that is now in standby state takes over the standby IP addresses of the active unit. If an active unit fails, the standby takes over without any interruption to the client VPN tunnel.

VPN Load Balancing

About VPN Load Balancing

If you have a remote-client configuration in which you are using two or more ASAs connected to the same network to handle remote sessions, you can configure these devices to share their session load by creating a

VPN load-balancing group. VPN Load balancing directs session traffic to the least loaded device, thus distributing the load among all devices. It makes efficient use of system resources and provides increased performance an availability.

All devices in the VPN load-balancing group carry session loads. One device in the group, the *director*, directs incoming connection requests to the other devices, called *member devices*. The director monitors all devices in the group, keeps track of how busy each is, and distributes the session load accordingly. The role of director is not tied to a physical device; it can shift among devices. For example, if the current director fails, one of the member devices in the group takes over that role and immediately becomes the new director.

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

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

VPN Load-Balancing Algorithm

The VPN load-balancing group director maintains a sorted list of group members in ascending IP address order. The load of each member is computed as an integer percentage (the number of active sessions). AnyConnect inactive sessions do not count towards the SSL VPN load for VPN load balancing. The director redirects the IPsec and SSL VPN tunnel to the device with the lowest load until it is 1 percent higher than the rest. When all members are 1% higher than the director, the director redirects traffic to itself.

For example, if you have one director and two members, the following cycle applies:

Note All nodes start with 0%, and all percentages are rounded half-up.

1. The director takes the connection if all members have a load at 1% higher than the director.
2. If the director does not take the connection, the session is taken by whichever member device has the lowest load percentage.
3. If all members have the same percentage load, the member with the least number of sessions gets the session.
4. If all members have the same percentage load and the same number of sessions, the member with the lowest IP address gets the session.

VPN Load-Balancing Group Configurations

A VPN load-balancing group can consist of ASAs of the same release or of mixed releases subject to the following restrictions:

- VPN load-balancing groups that consist of both same release ASAs can run VPN load balancing for a mixture of IPsec, AnyConnect, and clientless SSL VPN client and clientless sessions.

- VPN load-balancing groups that include mixed release ASAs or same release ASAs can support IPsec and clientless SSL sessions. In such a configuration, however, the ASAs might not reach their full IPsec capacity.

The director of the group assigns session requests to the members of the group. The ASA regards all sessions, SSL VPN or IPsec, as equal, and assigns them accordingly. You can configure the number of IPsec and SSL VPN sessions to allow, up to the maximum allowed by your configuration and license.

We have tested up to ten nodes in a VPN load-balancing group. Larger groups might work, but we do not officially support such topologies.

Frequently Asked Questions About VPN Load Balancing

Multiple Context Mode

Q. Is VPN load balancing supported in multiple context mode?

A. Neither VPN load balancing nor stateful failover is supported in multiple context mode.

IP Address Pool Exhaustion

Q. Does the ASA consider IP address pool exhaustion as part of its VPN load-balancing method?

A. No. If the remote access VPN session is directed to a device that has exhausted its IP address pools, the session does not establish. The load-balancing algorithm is based on load, and is computed as an integer percentage (number of active and maximum sessions) that each member supplies.

Unique IP Address Pools

Q. To implement VPN load balancing, must the IP address pools for AnyConnect clients or IPsec clients on different ASAs be unique?

A. Yes. IP address pools must be unique for each device.

Using VPN Load Balancing and Failover on the Same Device

Q. Can a single device use both VPN load balancing and failover?

A. Yes. In this configuration, the client connects to the IP address of the group and is redirected to the least-loaded ASA in the group. If that device fails, the standby unit takes over immediately, and there is no impact to the VPN tunnel.

VPN Load Balancing on Multiple Interfaces

Q. If we enable SSL VPN on multiple interfaces, is it possible to implement VPN load balancing for both of the interfaces?

A. You can define only one interface to participate in the VPN load-balancing group as the public interface. The idea is to balance the CPU loads. Multiple interfaces converge on the same CPU, so the concept of VPN load balancing on multiple interfaces does not improve performance.

Maximum Simultaneous Sessions for VPN Load-Balancing Groups

Q. Consider a deployment of two ASA 5525-Xs, each with a 100-user SSL VPN license. In a VPN load-balancing group, does the maximum total number of users allow 200 simultaneous sessions, or only 100? If we add a third device later with a 100-user license, can we now support 300 simultaneous sessions?

A. With VPN load balancing, all devices are active, so the maximum number of sessions that your group can support is the total of the number of sessions for each of the devices in the group, in this case 300.

Licensing for VPN Load Balancing

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

Prerequisites for VPN Load Balancing

Also refer to the Guidelines and Limitations for VPN Load Balancing, on page 6.

- VPN load balancing is disabled by default. You must explicitly enable VPN load balancing.
- You must have first configured the public (outside) and private (inside) interfaces. Subsequent references in this section use the names outside and inside.

  You can use the **interface** and **nameif** commands to configure different names for these interfaces.
- You must have previously configured the interface to which the virtual IP address refers. Establish a common virtual IP address, UDP port (if necessary), and IPsec shared secret for the group.
- All devices that participate in a group must share the same cluster-specific values: IP address, encryption settings, encryption key, and port.
- To use VPN load-balancing group encryption, first enable IKEv1 on the inside interface using the **crypto ikev1 enable** command, with the inside interface specified; otherwise you will get an error message when you try to configure VPN load-balancing group encryption.
- The Local CA feature is not supported if you use Active/Active stateful failover or VPN load-balancing. The Local CA cannot be subordinate to another CA; it can act only as the Root CA.
- If a load balancing unit is also configured for failover, you must configure standby IP addresses for the inside and outside interfaces. Otherwise, the VPN load balancing configuration will not synchronize properly to the secondary node and after failover, the secondary unit will not join the VPN load balancing group.

Guidelines and Limitations for VPN Load Balancing

Eligible Clients

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

- AnyConnect Secure Mobility Client (Release 3.0 and later)
- ASA 5505 (when acting as an Easy VPN client)
- Firepower 1010 (when acting as an Easy VPN client)
- IOS EZVPN Client devices supporting IKE-redirect (IOS 831/871)
- Clientless SSL VPN

Client Considerations

VPN load balancing works with IPsec clients and SSL VPN client and clientless sessions. All other VPN connection types (L2TP, PPTP, L2TP/IPsec), including LAN-to-LAN, can connect to an ASA on which VPN load balancing is enabled, but they cannot participate in VPN load balancing.

When multiple ASA nodes are grouped for load balancing, and using Group URLs is desired for AnyConnect client connections, the individual ASA nodes must:

- Configure each remote access connection profile with a Group URL for each VPN load-balancing virtual address (IPv4 and IPv6).

- Configure a Group URL for this node's VPN load-balancing public address.

Context Mode

VPN load balancing is not supported in multiple context mode.

Certificate Verification

When performing certificate verification for VPN load balancing with AnyConnect, and the connection is redirected by an IP address, the client does all of its name checking through this IP address. Make sure the redirection IP address is listed in the certificates common name or the subject alt name. If the IP address is not present in these fields, then the certificate will be deemed untrusted.

Following the guidelines defined in RFC 2818, if a **subject alt name** is included in the certificate, we only use the **subject alt name** for name checks, and we ignore the common name. Make sure that the IP address of the server presenting the certificate is defined in the **subject alt name** of the certificate.

For a standalone ASA, the IP address is the IP of that ASA. In a VPN load-balancing group situation, it depends on the certificate configuration. If the group uses one certificate, then the certificate should have SAN extensions for the virtual IP address and group FQDN and should contain Subject Alternative Name extensions that have each ASA's IP and FQDN. If the group uses multiple certificates, then the certificate for each ASA should have SAN extensions for the virtual IP, group FQDN, and the individual ASA's IP address and FQDN.

Geographical VPN Load Balancing

In a VPN load balancing environment where the DNS resolutions are being changed at regular intervals, you must carefully consider how to set the time to live (TTL) value. For the DNS load balance configuration to work successfully with AnyConnect, the ASA name-to-address mapping must remain the same from the time the ASA is selected until the tunnel is fully established. If too much time passes before the credentials are entered, the lookup restarts and a different IP address may become the resolved address. If the DNS mapping changes to a different ASA before the credentials are entered, the VPN tunnel fails.

Geographical load balancing for VPN often uses a Cisco Global Site Selector (GSS). The GSS uses DNS for the load balancing, and the time to live (TTL) value for DNS resolution is defaulted to 20 seconds. You can significantly decrease the likelihood of connection failures if you increase the TTL value on the GSS. Increasing to a much higher value allows ample time for the authentication phase when the user is entering credentials and establishing the tunnel.

To increase the time for entering credentials, you may also consider disabling Connect on Start Up.

Configuring VPN Load Balancing

If you have a remote-client configuration in which you are using two or more ASAs connected to the same network to handle remote sessions, you can configure these devices to share their session load. This feature is called VPN load balancing, which directs session traffic to the least loaded device, thereby distributing the load among all devices. VPN load balancing makes efficient use of system resources and provides increased performance and system availability.

To use VPN load balancing, do the following on each device in the group:

- Configure the VPN load-balancing group by establishing common VPN load-balancing group attributes. This includes a virtual IP address, UDP port (if necessary), and IPsec shared secret for the group. All

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

- Configure the participating device by enabling VPN load balancing on the device and defining device-specific properties, such as its public and private addresses. These values vary from device to device.

Configure the Public and Private Interfaces for VPN Load Balancing

To configure the public (outside) and private (inside) interfaces for the VPN load-balancing group devices, do the following steps.

Procedure

Step 1 Configure the public interface on the ASA by entering the **interface** command with the **lbpublic** keyword in vpn-load-balancing configuration mode. This command specifies the name or IP address of the public interface for VPN load balancing for this device:

Example:

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic outside
hostname(config-load-balancing)#
```

Step 2 Configure the private interface on the ASA by entering the **interface** command with the **lbprivate** keyword in vpn-load-balancing configuration mode. This command specifies the name or IP address of the private interface for VPN load balancing for this device:

Example:

```
hostname(config-load-balancing)# interface lbprivate inside
hostname(config-load-balancing)#
```

Step 3 Set the priority to assign to this device within the group. The range is from 1 to 10. The priority indicates the likelihood of this device becoming the group director, either at the startup of the device or when an existing director fails. The higher you set the priority (for example, 10), the more likely it is that this device becomes the group director.

Example:

For example, to assign this device a priority of 6 within the group, enter the following command:

```
hostname(config-load-balancing)# priority 6
hostname(config-load-balancing)#
```

Step 4 If you want to apply network address translation for this device, enter the **nat** command with the NAT assigned address for the device. You can define an IPv4 and an IPv6 address or specify the device's hostname.

Example:

For example, to assign this device a NAT address of 192.168.30.3 and 2001:DB8::1, enter the following command:

```
hostname(config-load-balancing)# nat 192.168.30.3 2001:DB8::1
hostname(config-load-balancing)#
```

Configure the VPN Load Balancing Group Attributes

To configure the VPN load-balancing group attributes for each device in the group, do the following steps:

Procedure

Step 1 Set up VPN load balancing by entering the **vpn load-balancing** command in global configuration mode:

Example:

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)#
```

This enters vpn-load-balancing configuration mode, in which you can configure the remaining load-balancing attributes.

Step 2 Configure the IP address or the fully qualified domain name of the group to which this device belongs. This command specifies the single IP address or FQDN that represents the entire VPN load-balancing group. Choose an IP address that is within the public subnet address range shared by all the ASAs in the group. You can specify an IPv4 or IPv6 address.

Example:

For example, to set the virtual IP address to IPv6 address, 2001:DB8::1, enter the following command:

```
hostname(config-load-balancing)# cluster ip address 2001:DB8::1
hostname(config-load-balancing)#
```

Step 3 Configure the group port. This command specifies the UDP port for the VPN load-balancing group in which this device is participating. The default value is 9023. If another application is using this port, enter the UDP destination port number that you want to use for load balancing.

Example:

For example, to set the group port to 4444, enter the following command:

```
hostname(config-load-balancing)# cluster port 4444
hostname(config-load-balancing)#
```

Step 4 (Optional) Enable IPsec encryption for the VPN load-balancing group.

The default is no encryption. This command enables or disables IPsec encryption. If you configure this check attribute, you must first specify and verify a shared secret.The ASAs in the VPN load-balancing group 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 To use VPN load-balancing group encryption, first enable IKEv1 on the inside interface using the **crypto ikev1 enable** command, with the inside interface specified; otherwise, you will get an error message when you try to configure VPN load-balancing group encryption.

If IKEv1 was enabled when you configured group encryption, but was disabled before you configured the participation of the device in the group, you get an error message when you enter the **participate** command, and encryption is not enabled for the group.

Example:

```
hostname(config)# crypto ikev1 enable inside
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)#
```

Step 5 If you enable group encryption, you must also specify the IPsec shared secret by entering the **cluster key** command. This command specifies the shared secret between IPsec peers when you have enabled IPsec encryption. The value you enter in the box appears as consecutive asterisk characters. If you need to enter an already encrypted key (for example, you copied it from another configuration), enter the **cluster key 8** *key* command.

Example:

For example, to set the shared secret to 123456789, enter the following command:

```
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)#
```

Step 6 Enable this device's participation in the group by entering the **participate** command:

Example:

```
hostname(config-load-balancing)# participate
hostname(config-load-balancing)#
```

What to do next

When multiple ASA nodes are grouped for load balancing, and using Group URLs is desired for AnyConnect client connections, on the individual ASA nodes you must:

- Configure each remote access connection profile with a Group URL for each load balancing virtual address (IPv4 and IPv6).
- Configure a Group URL for this node's VPN Load Balancing public address.

Use the **tunnel-group**, **general-attributes**, **group-url** command to configure these Group URLs.

Enable Redirection Using a Fully Qualified Domain Name

By default, the ASA sends only IP addresses in VPN load-balancing redirection to a client. If certificates are in use that are based on DNS names, the certificates will be invalid when redirected to a member device.

As a VPN load-balancing director, this ASA can send a fully qualified domain name (FQDN), using reverse DNS lookup, of a member device (another ASA in the group) instead of its outside IP address when redirecting VPN client connections to that member device.

To enable or disable redirection using a fully qualified domain name in vpn load-balancing mode, use the **redirect-fqdn enable** command in global configuration mode. This behavior is disabled by default.

Before you begin

All of the outside and inside network interfaces on the VPN load-balancing devices in a group must be on the same IP network.

Procedure

Step 1 Enable the use of FQDNs for VPN load balancing.

redirect-fqdn {**enable** | **disable**}

Example:

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# redirect-fqdn enable
hostname(config-load-balancing)#
```

Step 2 Add an entry for each of your ASA outside interfaces into your DNS server if such entries are not already present. Each ASA outside IP address should have a DNS entry associated with it for lookups. These DNS entries must also be enabled for reverse lookup.

Step 3 Enable DNS lookups on your ASA with the **dns domain-lookup inside** command or whichever interface has a route to your DNS server.

Step 4 Define your DNS server IP address on the ASA. for example: **dns name-server 10.2.3.4** (IP address of your DNS server).

Configuration Examples for VPN Load Balancing

Basic VPN Load Balancing CLI Configuration

The following is an example of a VPN load balancing command sequence that includes an interface command that enables redirection for a fully qualified domain name, specifies the public interface of the group as **test** and the private interface of the group as **foo**”

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
```

```
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# redirect-fqdn enable
hostname(config-load-balancing)# participate
```

Viewing VPN Load Balancing Information

The VPN load-balancing group director receives a periodic message from each ASA in the group with the number of active AnyConnect and clientless sessions, as well as the maximum allowed sessions based on the configured or license limits. If an ASA in the group shows 100 percent full capacity, the group director cannot redirect more connections to it. Although the ASA may show as full, some users may be in inactive/wait-to-resume state, wasting the licenses. As a workaround, each ASA provides the total number of sessions minus the sessions in inactive state, instead of the total number of sessions. Refer to the **-sessiondb summary** command in the ASA command reference. In other words, the inactive sessions are not reported to the group director. Even if the ASA is full (with some inactive sessions), the group director still redirects connections to it if necessary. When the ASA receives the new connection, the session that has been inactive the longest is logged off, allowing new connections to take its license.

The following example shows 100 SSL sessions (active only) and a 2 percent SSL load. These numbers do not include the inactive sessions. In other words, inactive sessions do not count towards the load for VPN load balancing.

```
hostname# show vpn load-balancing
 Status :    enabled
 Role :    Master
 Failover :    Active
 Encryption :    enabled
 Cluster IP :    192.168.1.100
 Peers :    1

 Load %
Sessions
 Public IP     Role   Pri Model    IPsec SSL IPsec SSL
 192.168.1.9   Master 7   ASA-5540 4     2   216   100
 192.168.1.19  Backup 9   ASA-5520 0     0   0     0
```