AnyConnect VPN, ASA, and FTD FAQ for Secure Remote Workers

First Published: 2020-03-19

Last Modified: 2020-04-15

AnyConnect VPN, ASA, and FTD FAQ for Secure Remote Workers

Is this document for you?

This document gathers together FAQs, best practices, and other reference information to help you deploy Cisco AnyConnect remote access VPN for a Cisco ASA or Cisco Firepower Threat Defense (FTD) headend for secure remote workers. Also see the following document for more scaling out tips: https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/215331-anyconnect-implementation-and-performanc.html.

AnyConnect Connection Logic

In the simplest configuration, the AnyConnect client will use a specific entry in a connection list. The connection list can contain backup entries, in case the first entry is non-responsive.

```
<ServerList>
 <HostEntry>
  <HostName>ACME VPN headend</HostName>  ! name that in displayed in AnyConnect window list
  <HostAddress>hq.company.com</HostAddress>    ! first entry that will be tried, can be IP
  <BackupServerList>                           ! backup section list
   <HostAddress>warsaw.company.com</HostAddress>     ! second option
   <HostAddress>london.company.com</HostAddress>     ! third option
   <HostAddress>milan.company.com</HostAddress>      ! fourth option
   <HostAddress>berlin.company.com</HostAddress>     ! fifth option
  </BackupServerList>
  </HostEntry>
</ServerList>
```

In a VPN load-balanced configuration, if there are no sessions remaining:

1. The ASA will try to find and disconnect stale clients (clients connected over 8 hours ago and in hibernation).
2. If no stale clients were found, the connection will fail with a message to the user.
3. The AnyConnect client will not automatically try the next connection entry or backup entries. This occurs because the connection failure happened after initial authentication, so the AnyConnect client appears to have successfully connected. This isn't a big problem: the user can select the next entry from the list of available connections, or retry with the same connection.

SSL vs. TLS vs. DTLS: What's the Difference?

- SSL—SSL is generally obsolete, but it's used widely in data sheets and literature because people know the name. See https://tools.ietf.org/html/rfc7568.
- TLS—TLS 1.0, 1.1, 1.2 and 1.3 are current versions. TLS 1.0 and 1.1 are being deprecated by major OS and browser companies by March 2020. ASA, FTD, and AnyConnect supports TLS up to 1.2 for VPN connectivity.
- DTLS—DTLS is UDP-based TLS for VPN connectivity. See https://tools.ietf.org/html/rfc6347.

Why is DTLS Performance Worse than IPsec?

- DTLS bears more complexity in performing high-speed calculations for processing traffic.
- Current generation crypto accelerators were optimized for years to process IPsec traffic.

Can You Rate-Limit Traffic per AnyConnect User?

Question: Can you rate-limit traffic per AnyConnect user?

Answer:

- FTD—Yes. See https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fmc-config-guide-v64/firepower_threat_defense_remote_access_vpns.html#task_rvk_qnl_ngb
- ASA—You can only limit traffic per Tunnel Group. See https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/82310-qos-voip-vpn.html#anc11 and https://www.cisco.com/c/en/us/td/docs/security/asa/asa913/configuration/firewall/asa-913-firewall-config/conns-qos.html#ID-2133-000002dd

Configuration Tips

- Make sure you're using AnyConnect 4.8.x and DTLS v1.2 or IKEv2 for the headend (FTD 6.6/ASA 9.10+) configuration
- (ASA) Verify the optimization setting for crypto hardware. There are two options:
  - **crypto engine accelerator-bias ssl**
  - **crypto engine accelerator-bias ipsec**

Note Changing this setting will cause traffic disruption.

- MTU in the Group Policy—The higher MTU, the better. However, once you cross 1406, you may start having problems.

- (ASA) AnyConnect tunnel optimizations can be enabled on ASA devices to potentially optimize throughput available per client. Apply following customization for the ASA:

```
webvpn
 anyconnect-custom-attr TunnelOptimizationsEnabled description Optimizations Enabled
 anyconnect-custom-data TunnelOptimizationsEnabled False false
 anyconnect-custom-data TunnelOptimizationsEnabled True true
```

Then in the group-policy:

```
group-policy <Group Policy Name> attributes
  anyconnect-custom TunnelOptimizationsEnabled value True
```

Optimizing Your ASAv Deployment

For detailed information to make sure you're getting the most performance from your ASAv, see the following document:

https://www.cisco.com/content/en/us/td/docs/security/asa/misc/asav-optimization/optimizing-your-asav-deployment.html

Does FTDv Support Remote Access VPN?

Question: Does FTDv support remote access VPN?

Answer: Yes!

Cloud Providers

We currently support following cloud providers for FTDv:

- Microsoft Azure cloud (all instances support up to 250 VPN endpoints):
  - Standard D3—4 vCPUs, 14 GB, 4vNICs
  - Standard D3_v2—4 vCPUs, 14 GB, 4vNICs
  - Standard D4_v2—8 vCPUs, 28 GB, 8vNICs (New in Version 6.5)
  - Standard D5_v2—16 vCPUs, 56 GB, 8vNICs (New in Version 6.5)
- Amazon AWS cloud (all instances support up to 250 VPN endpoints):
  - c4.xlarge—4 vCPUs, 7.5 GB, 2 interfaces, 1 management interface
  - c3.xlarge—4 vCPUs, 7.5 GB, 2 interfaces, 1 management interface

See which FTDv version is supported in which cloud: https://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html

Hypervisors

We currently support following hypervisors for FTDv:

- VMware ESXi
  - 4vCPU/8GB (default)
  - 8vCPU/16GB
  - 12vCPU/24GB
- KVM
  - 4vCPU/8GB (default)
  - 8vCPU/16GB
  - 12vCPU/24GB

See which FTDv version is supported in which hypervisor: https://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html

Viewing Information about VPN on the ASA or FTD

How can you see the number of connected VPN clients?

See the following command:

show vpn-sessiondb summary

```
hq-vpn-headend# show vpn-sessiondb summary
----------------------------------------------------------------------------
VPN Session Summary
----------------------------------------------------------------------------
                          Active : Cumulative : Peak Concur : Inactive
                        ----------------------------------------------
AnyConnect Client          :     1 :         1 :          1 :       0
  SSL/TLS/DTLS             :     1 :         1 :          1 :       0
----------------------------------------------------------------------------
Total Active and Inactive    :     1           Total Cumulative :      1
Device Total VPN Capacity    :   300
Device Load                  :     0%
----------------------------------------------------------------------------
```

How can you see licensing and scaling numbers?

See the following command:

show vpn-sessiondb license-summary

```
hq-vpn-headend# show vpn-sessiondb license-summary
----------------------------------------------------------------------------
VPN Licenses and Configured Limits Summary
----------------------------------------------------------------------------
                                Status : Capacity : Installed :  Limit
                               ----------------------------------------
AnyConnect Premium              : ENABLED :      750 :       750 :   NONE
AnyConnect Essentials           : DISABLED :     750 :       750 :   NONE
Other VPN (Available by Default) :  ENABLED :      750 :       750 :   NONE
[...]
----------------------------------------------------------------------------
VPN Licenses Usage Summary
----------------------------------------------------------------------------
                                    All  :   Peak :  Eff.  :
                                   In Use : In Use :  Limit : Usage
                                  ---------------------------------
AnyConnect Premium     :               :     50 :     94 :    750 :    6%
  Anyconnect Client    :               :     50 :     90 :    750 :    6%
Other VPN              :               :      0 :      0 :    750 :    0%
  L2TP Clients
----------------------------------------------------------------------------
```

Can you see traffic statistics per connected client?

See the following command:

show vpn-sessiondb anyconnect

```
hq-vpn-headend# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : santaclaus             Index        : 1
Assigned IP  : 192.168.46.5           Public IP    : 10.254.8.19
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 382125                Bytes Rx     : 324015
Group Policy : SCPolicy              Tunnel Group : DefaultWEBVPNGroup
Login Time   : 01:41:18 CEST Mon Mar 9 2020
Duration     : 0h:13m:19s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                   VLAN         : none
Audt Sess ID : c0a80afe000010005e6590ae
Security Grp : none
```

Can you filter traffic statistics per connected client?

See the following command:

show vpn-sessiondb anyconnect filter

```
hq-vpn-headend# show vpn-sessiondb anyconnect filter ?
  a-ipaddress   Assigned IP Address specific session
  a-ipversion   Assigned IP Version specific sessions
  encryption    Encryption Algorithm
  inactive      inactive sessions
  name          Username specific sessions
  p-ipaddress   Public IP Address specific sessions
  p-ipversion   Public IP Version specific sessions
  protocol      Protocol
  tunnel-group  Tunnel-group sessions
```

What details can you show per connected client?

See the following command:

show vpn-sessiondb detail anyconnect

```
hq-vpn-headend# show vpn-sessiondb detail anyconnect
Username     : santaclaus            Index        : 1
Assigned IP  : 192.168.46.5          Public IP    : 144.254.8.19
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 465106                Bytes Rx     : 395293
Pkts Tx      : 3310                  Pkts Rx      : 4115
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
Group Policy : SCPolicy              Tunnel Group : DefaultWEBVPNGroup
Login Time   : 01:41:18 CEST Mon Mar 9 2020
Duration     : 0h:17m:45s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                   VLAN         : none
Audt Sess ID : c0a80afe000010005e6590ae
Security Grp : none

AnyConnect-Parent:
  Tunnel ID    : 1.1
  Public IP    : 144.254.8.19
  Encryption   : none                Hashing      : none
  TCP Src Port : 1026                TCP Dst Port : 443
  Auth Mode    : userPassword
  Idle Time Out: 30 Minutes          Idle TO Left : 12 Minutes
  Client OS    : mac-intel
  Client OS Ver: 10.15.3
  Client Type  : AnyConnect
  Client Ver   : Cisco AnyConnect VPN Agent for Mac OS X 4.8.02042
  Bytes Tx     : 7650                Bytes Rx     : 0
  Pkts Tx      : 6                   Pkts Rx      : 0
  Pkts Tx Drop : 0                   Pkts Rx Drop : 0

SSL-Tunnel:
  Tunnel ID    : 1.2
  Assigned IP  : 192.168.46.5        Public IP    : 144.254.8.19
```

```
 Encryption   : AES-GCM-256          Hashing      : SHA384
 Ciphersuite  : ECDHE-ECDSA-AES256-GCM-SHA384
 Encapsulation: TLSv1.2              TCP Src Port : 1029
 TCP Dst Port : 443                  Auth Mode    : userPassword
 Idle Time Out: 30 Minutes           Idle TO Left : 12 Minutes
 Client OS    : Mac OS X
 Client Type  : SSL VPN Client
 Client Ver   : Cisco AnyConnect VPN Agent for Mac OS X 4.8.02042
 Bytes Tx     : 7874                 Bytes Rx     : 942
 Pkts Tx      : 10                   Pkts Rx      : 7
 Pkts Tx Drop : 0                    Pkts Rx Drop : 0

DTLS-Tunnel:
 Tunnel ID    : 1.3
 Assigned IP  : 192.168.46.5         Public IP    : 144.254.8.19
 Encryption   : AES256               Hashing      : SHA1
 Ciphersuite  : DHE-RSA-AES256-SHA
 Encapsulation: DTLSv1.0             UDP Src Port : 1024
 UDP Dst Port : 443                  Auth Mode    : userPassword
 Idle Time Out: 30 Minutes           Idle TO Left : 30 Minutes
 Client OS    : Mac OS X
 Client Type  : DTLS VPN Client
 Client Ver   : Cisco AnyConnect VPN Agent for Mac OS X 4.8.02042
 Bytes Tx     : 453544               Bytes Rx     : 395493
 Pkts Tx      : 3312                 Pkts Rx      : 4128
 Pkts Tx Drop : 0                    Pkts Rx Drop : 0
```

Scaling Out Remote Access VPNs

ASA VPN Load Balancing

Load balancing is a mechanism for equitably distributing remote access VPN traffic among the devices in a virtual cluster. For more information, see https://www.cisco.com/c/en/us/td/docs/security/asa/asa913/configuration/vpn/asa-913-vpn-config/vpn-ha.html.

This section includes common questions and best practices for VPN load balancing.

VPN Load Balancing on the FTD: Not Supported

Question: Does the FTD support VPN load balancing?

Answer: No. Only the ASA supports VPN load balancing.

.

Clustering and VPN Load Balancing: Not Supported

Question: Can I mix clustering with VPN load balancing?

Answer: No. Clustering (multiple ASAs connected together in a cluster configuration) does not support Remote Access VPN. See the Cisco ASA unsupported clustering features: https://www.cisco.com/c/en/us/td/docs/security/asa/asa913/configuration/general/asa-913-general-config/ha-cluster.html#ID-2170-00000296. Note that the clustering feature is not related to VPN load balancing "clusters", although they use the same terminology.

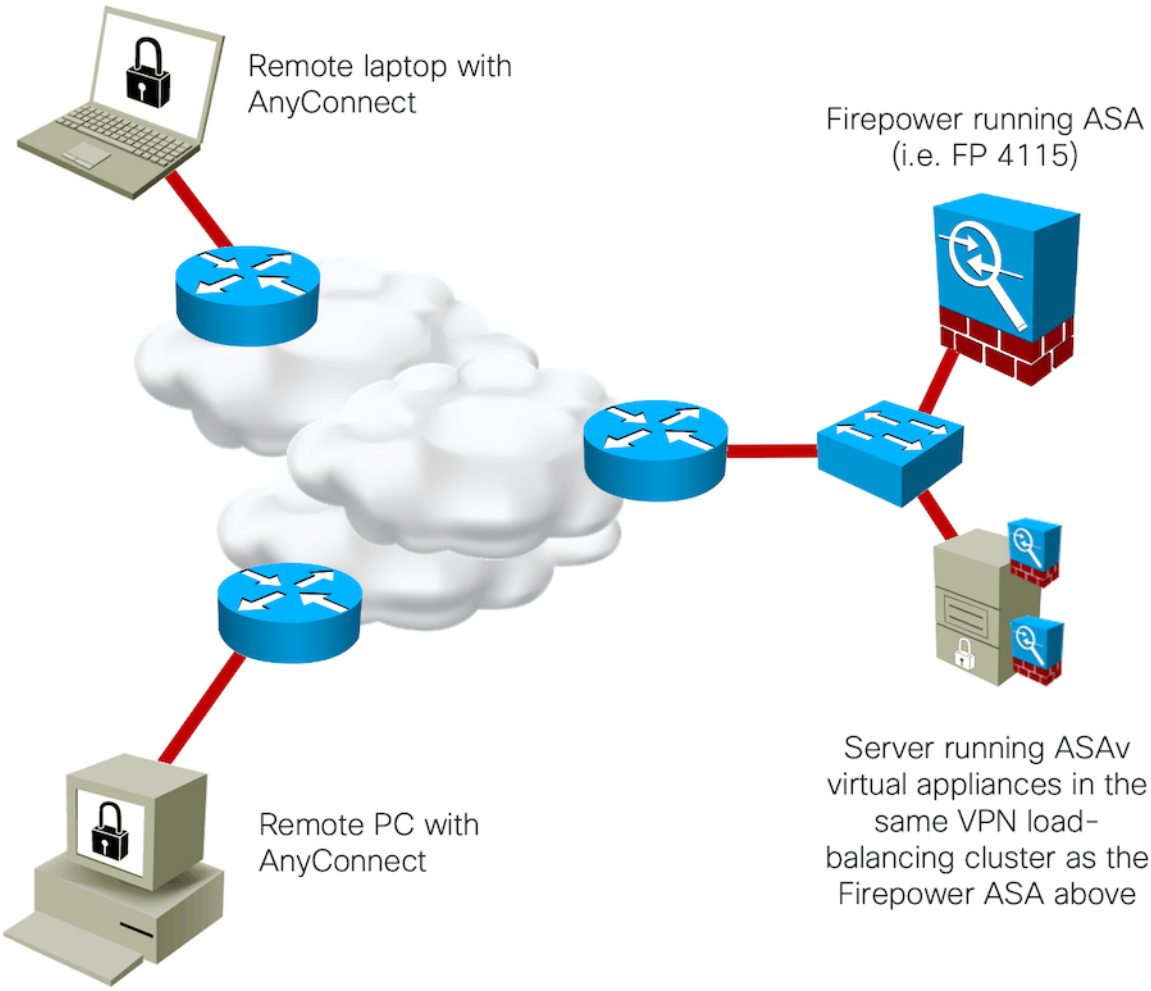
You can use failover with VPN load balancing, however.

Mixing Different Devices in VPN Load Balancing

Question: Can I mix ASA hardware appliances and ASAv virtual appliances for VPN load balancing?

Answer: Yes. But take into account different weighting of devices in the VPN load-balancing algorithm. Also, in Version 9.1 and earlier, different generations of the ASA may not be properly detected and will fail to form a VPN load-balancing group (CSCty54721).

Note that VPN load balancing requires the 3DES/AES license.



Question: How does the VPN load-balancing algorithm work?

Answer: Each VPN load-balancing group member advertises to the director what its maximum number of VPN sessions is. The director then allocates sessions to each member unit equalling 1% the unit's maximum. After balancing sessions to all member units, the director allocates itself 1% of its maximum. The allocation continues in order (each member, and then the director) in 1% increments.

For example, you have three ASAs:

- ASA 5515-X (member) with 250 sessions max.

- ASAv5 (member) with 50 sessions max.
- ASA 5555-X (director) with 5000 sessions max.

See the following VPN session distribution:

1. ASA 5515-X—Allocated the first three sessions (1% of 250).
2. ASAv5—Allocated the next session (1% of 50).
3. ASA 5555-X—Allocated the next 50 sessions (1% of 5000).
4. ASA 5515-X—Allocated the next 3 sessions.
5. ASAv5—Allocated the next session.
6. ASA 5555-X—Allocated the next 50 sessions.
7. And so on...

Mixed-Devices Tips

- In a mixed environment, you can artificially limit supported VPN clients, which will be taken into account by the VPN load balancing director:

```
vpn-cl5# show vpn load-balancing
Total License Load:
 AnyConnect Premium/Essentials       Other VPN        Public IP
  Limit    Used   Load         Limit    Used   Load
    250       0      0%          250       0      0%  100.64.0.15* ! Platform limit of 250 sessions

vpn-cl5(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 30
vpn-cl5(config)# vpn-sessiondb max-other-vpn-limit 30

vpn-cl5# show vpn load-balancing
Total License Load:
 AnyConnect Premium/Essentials       Other VPN        Public IP
  Limit    Used   Load         Limit    Used   Load
     30       0      0%          30       0      0%  100.64.0.15*.   ! adjusted to 30 sessions max
```

- By default, IKE negotiation is setup to accept 100% of incoming connection requests up to current platform limits. For smaller platforms, or a mix of platforms, we suggest that you limit acceptance to a lower amount so you do not overload the device with sudden bursts of traffic:

```
vpn-cl5(config)# crypto ikev2 limit max-in-negotiation-sa 25 ! default is 100 (100%), so for example:
            ! for 250 VPN license, ASA will be accepting only  63 session requests at the same time
            ! for 750 VPN license, ASA will be accepting only 188 session requests at the same time
```

- Another option is to limit the total number of SAs to protect the device from trying to establish too many sessions overall. If the device is in a VPN load balancing group, coordinate this setting with the **vpn-sessiondb max-anyconnect-premium-or-essentials-limit** and **vpn-sessiondb max-other-vpn-limit** commands.

```
vpn-cl5(config)# crypto ikev2 limit max-sa 100 ! good for up to 50 tunnels, 2xSAs each, existing tunnels
                                               ! won't be able to re-negotiate before closing though!

        ! it may make sense to setup this to number higher than
        ! maximum number of VPNs by couple of pairs, for
        ! negotiation and seamless switchover
```

What if VPN Load Balancing Is Not Enough?

In addition to the VPN load balancing feature, you can use these additional networking tools:

- DNS—Use the same A/AAAA record pointing to different IPs
- Anycast—Distribute the same IPs
- Hardware or software load-balancers—Offers VIP per device or a VPN load balanced group

The above options can be mixed and matched. Consider also how you use AnyConnect Connection Logic , on page 1.

Using DNS to Scale Out Your Remote Access VPN Deployment

Use the same A/AAAA record to point to different IP addresses.

Pros:

Very easy to use; you can assign multiple records in your domain zone to the same name like this:

```
asa-vpn     IN A      10.254.220.5
asa-vpn     IN AAAA      2001:420:1::5
asa-vpn     IN A      10.254.220.6
asa-vpn     IN AAAA      2001:420:1::6
asa-vpn     IN A      10.254.220.7
asa-vpn     IN AAAA      2001:420:1::7
```

Cons:

May not give equal load-balancing result. It will depend on the client DNS resolver, the DNS filtering/caching policies of service providers, and so on.

Using IP Anycast to Scale Out Your Remote Access VPN Deployment

Use the same IPv4/v6 as the VPN load balancer virtual IP address.

For more about IP Anycast best practices, see https://lukasz.bromirski.net/docs/prezos/plnog2011/ip_anycast.pdf.

Pros:

- Works across many devices or VPN load-balancer groups in different sites or in different segments at the same site (depending on requirements/resources).
- Uses normal IP routing mechanisms to reach the nearest advertised instance of service.

Cons:

IP Anycast needs to be monitored, and a failed site needs to be removed from IP routing so you do not blackhole connection requests.

Using Load Balancers to Scale Out Your Remote Access VPN Deployment

You can use a regular traffic load balancer in front of multiple ASAs and FTDs.

Pros:

- Numerous hardware (i.e. Nexus 9000 ITD feature, F5, A10) and software (i.e. HAProxy, Traefik) or even cloud-specific (AWS/Azure/GCP) load balancers are readily available and offer very high performance.
- Most load balancers offer additional tests, features, and protection.

Cons:

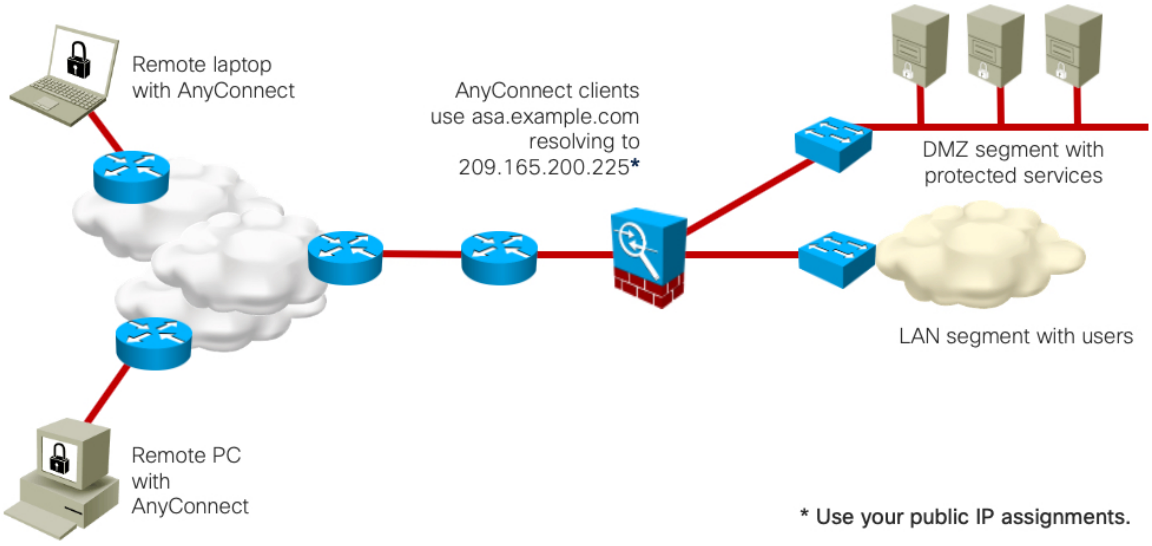
You don't have visibility in the front-end layer (the ASA or FTD).

Design Choices for VPN Deployments

ASA: Single Site Scenarios

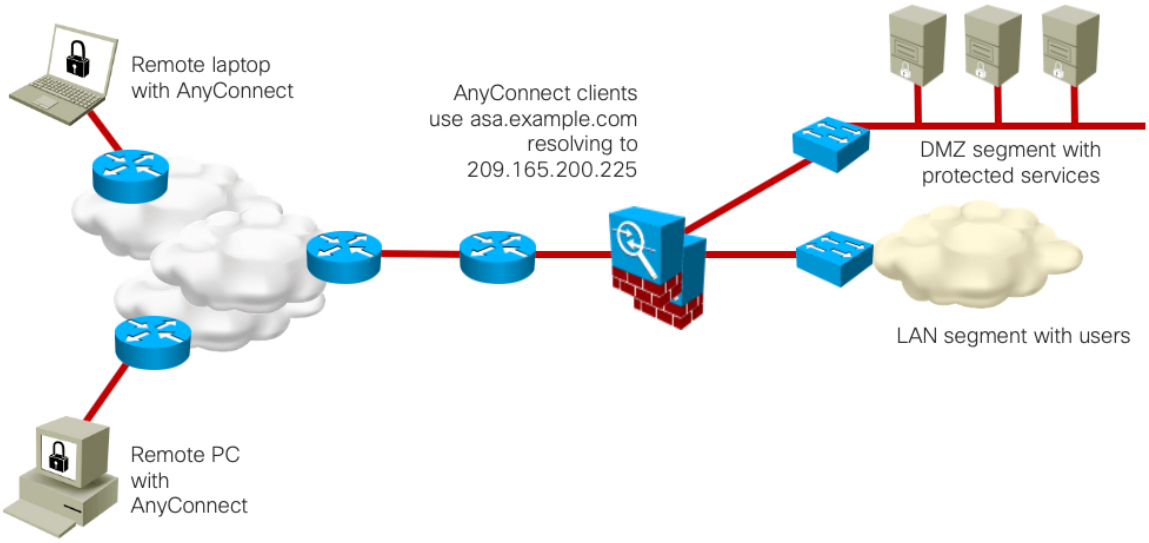
Option 1a: : Single ASA (not recommended because of lack of redundancy)

Scaling: Up to the maximum VPN peers in the data sheet, with session setup at data sheet rate.



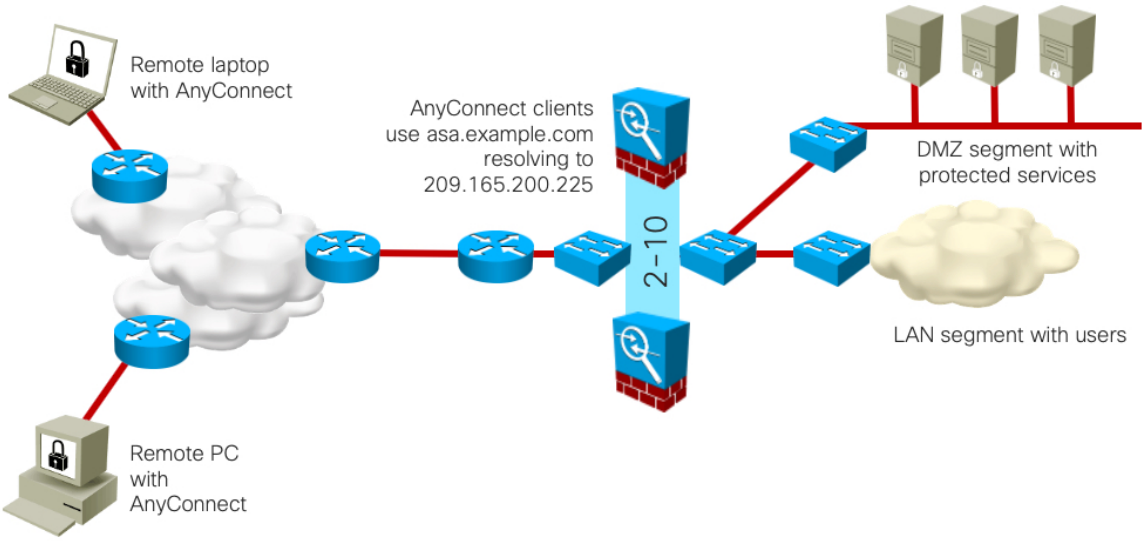
Option 1b: Two ASAs in Active/Standby

Scaling: Up to the maximum VPN peers in the data sheet, with session setup at data sheet rate. (The second ASA gracefully continues established VPN connections).



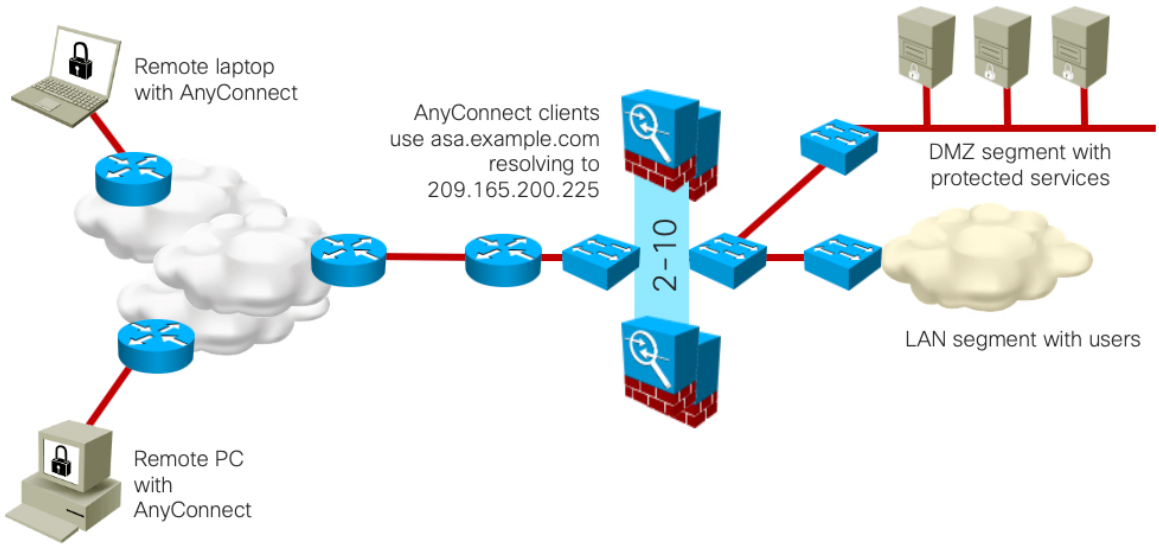
Option 2a: Two to Ten ASAs with VPN load balancing enabled

Scaling: Up to the maximum VPN peers in the data sheet for *each* ASA in a VPN load-balancing setup (different ASA models allowed), with session setup at data sheet rate for the terminating ASA. Cisco has tested up to ten ASAs in a VPN load-balancing group.



Option 2b: Two to Ten ASAs in Active/Standby with VPN load balancing enabled

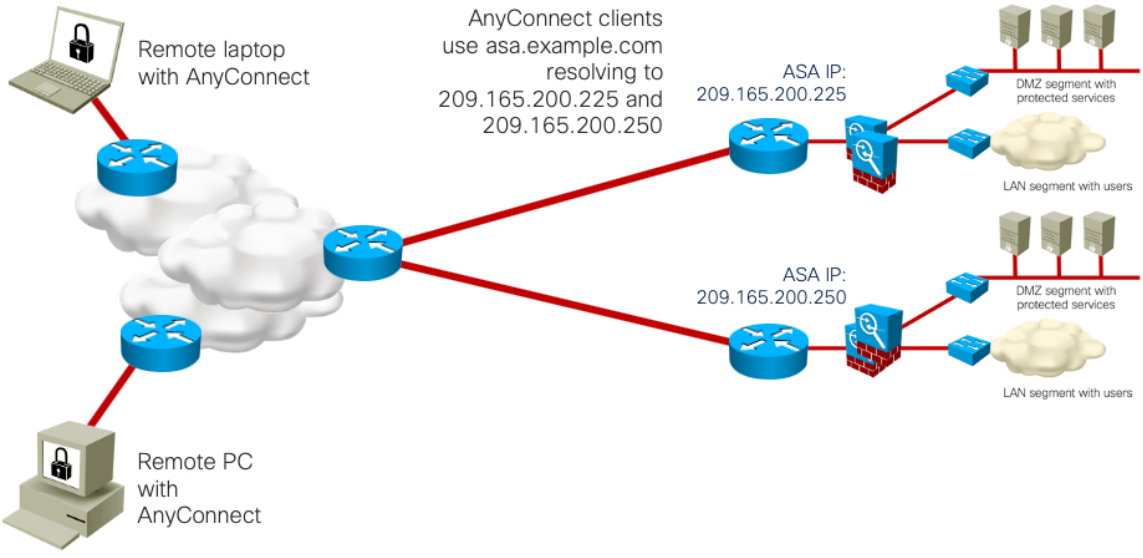
Scaling: Up to the maximum VPN peers in the data sheet for *each* ASA in a VPN load-balancing setup (different ASA models allowed), with session setup at data sheet rate for the terminating ASA. Cisco has tested up to ten ASAs in a VPN load-balancing group. (The second ASA of each pair gracefully continues established VPN connections)



ASA: Dual Site Scenarios

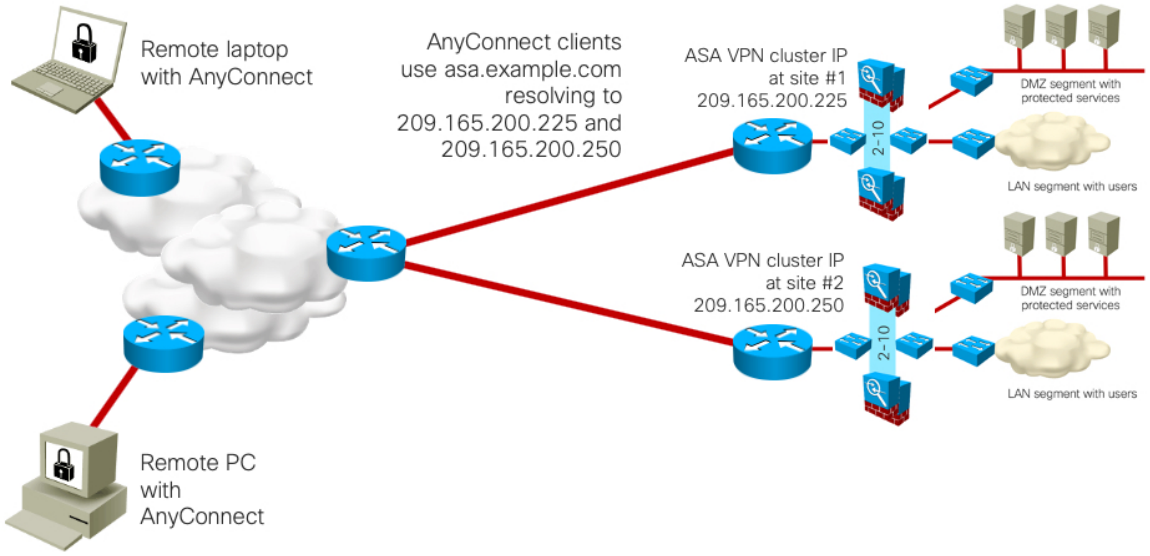
Option 3a: Two ASAs in Active/Standby per Site, with DNS Load Balancing

Scaling: Up to the maximum VPN peers in the data sheet for each ASA pair, with session setup at data sheet rate per site. DNS is responsible for load balancing. Note that load balancing may not be equal to each site.



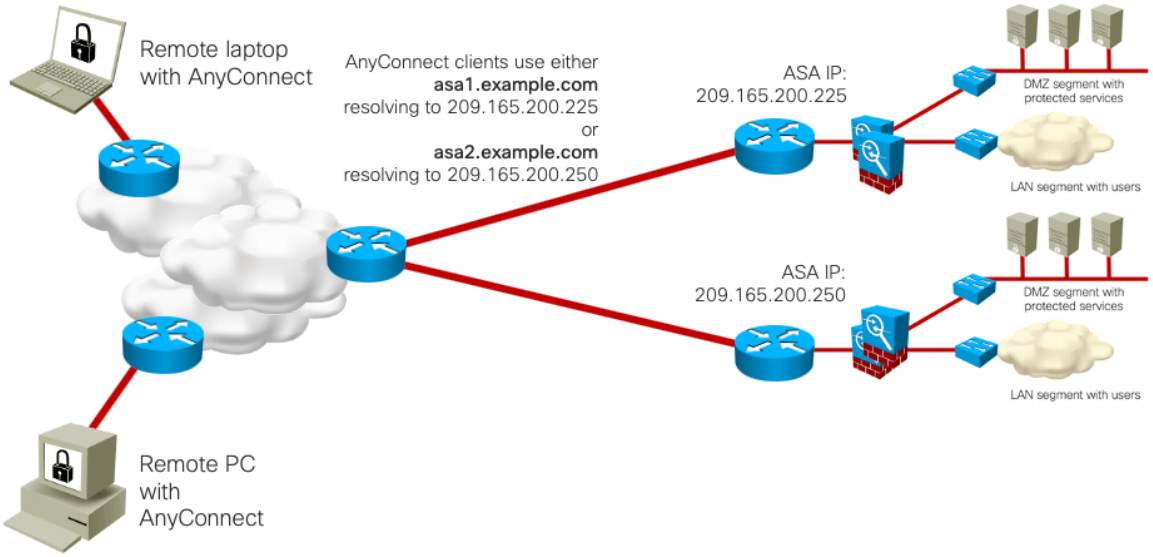
Option 3b: Two to Ten ASAs in Active/Standby, with DNS and VPN load balancing

Scaling: Up to the maximum VPN peers in the data sheet for each ASA pair, with session setup at data sheet rate per site. DNS is responsible for initial load balancing. Note that load balancing may not be equal to each site. Within each site, ASA VPN load balancing distributes traffic to the site ASAs. Cisco has tested up to ten ASAs in a VPN load-balancing cluster.



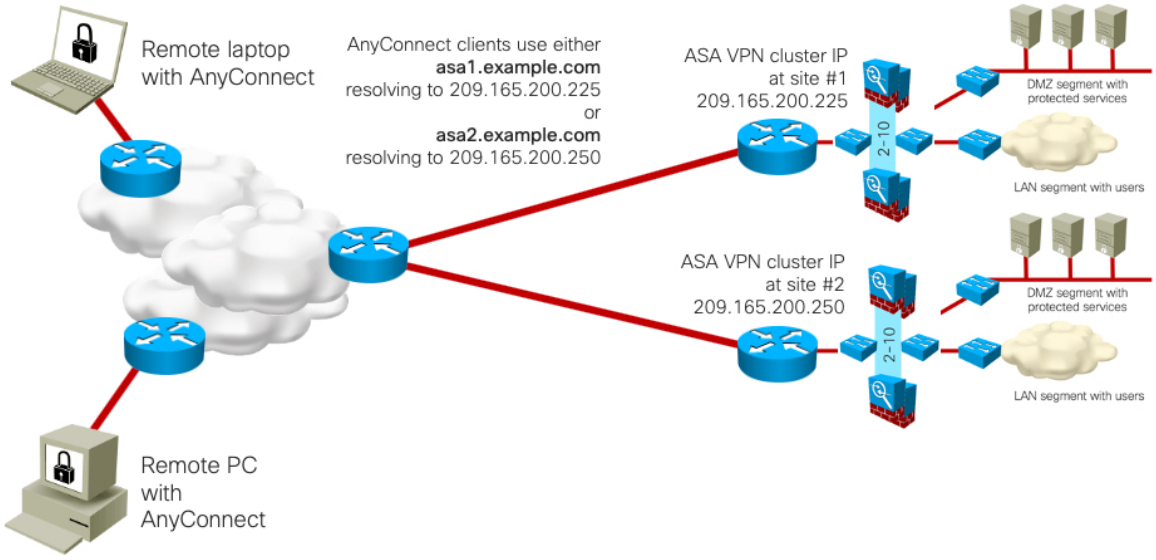
Option 4a: Two ASAs in Active/Standby per Site, User-Selected Site with Backup

Scaling: Up to the maximum VPN peers in the data sheet for each ASA pair, with session setup at data sheet rate per site. The user selects a specific site name, with a backup entry in case the first site is unavailable.



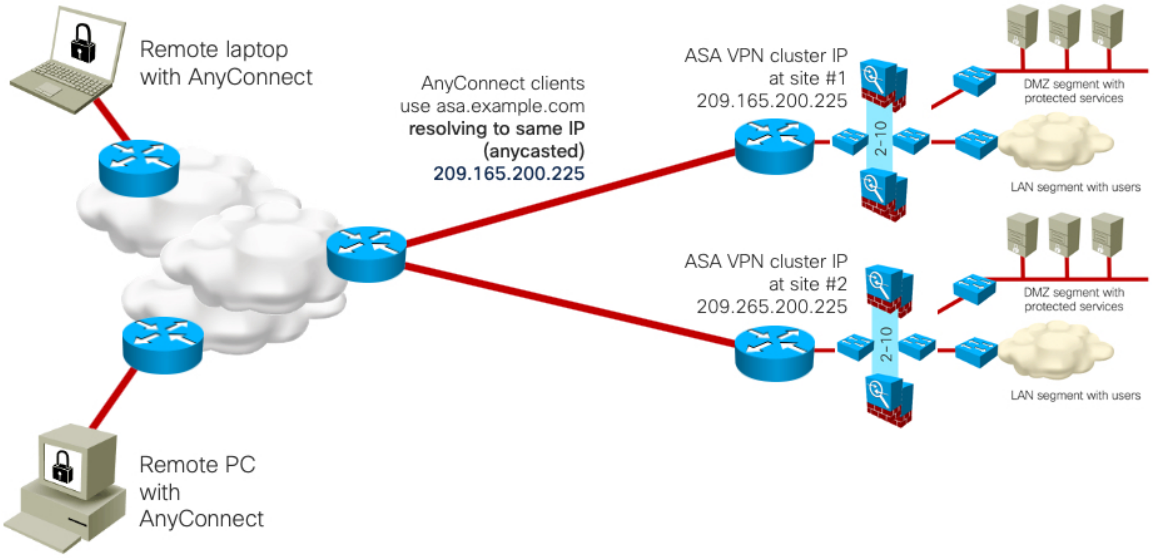
Option 4b: Two to Ten ASAs in Active/Standby, with User-Selected Site with Backup, VPN load balancing

Scaling: Up to the maximum VPN peers in the data sheet for each ASA pair, with session setup at data sheet rate per site. The user selects a specific site name, with a backup entry in case the first site is unavailable. Within each site, ASA VPN load balancing distributes traffic to the site ASAs. Cisco has tested up to ten ASAs in a VPN load-balancing cluster.



Option 5: Two to Ten ASAs in Active/Standby, with IP Anycast and VPN load balancing

Scaling: Up to the maximum VPN peers in the data sheet for each ASA pair, with session setup at data sheet rate per site. IP Anycast is responsible for initial load balancing, directing traffic to the nearest IP instance topology-wise (depending on SP-level routing, policies, etc.). Within each site, ASA VPN load balancing distributes traffic to the site ASAs. Cisco has tested up to ten ASAs in a VPN load-balancing cluster.

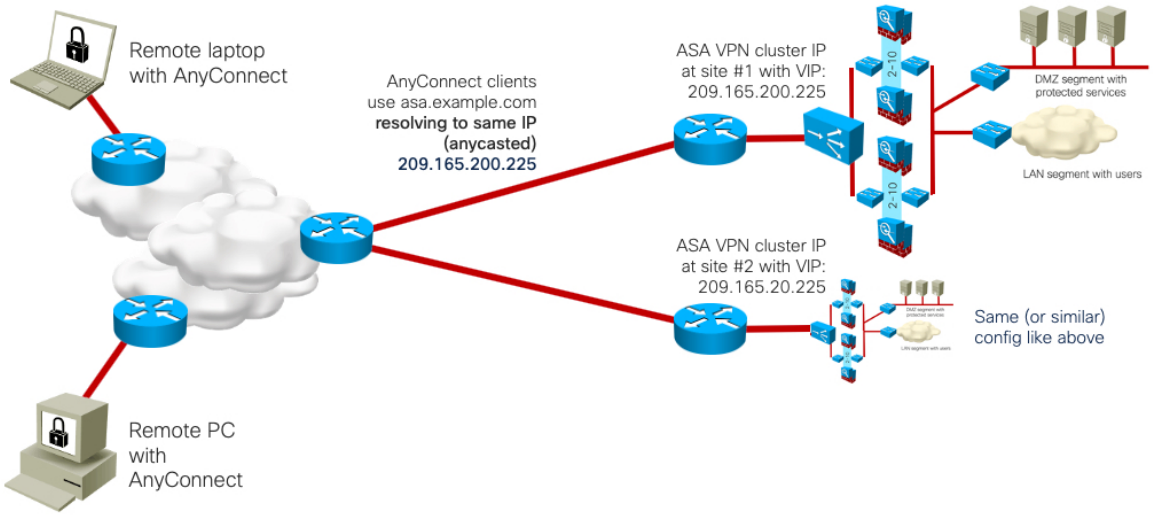


Option 6: Two to Ten ASAs in Active/Standby, with IP Anycast, Traffic Load Balancers, and VPN load balancing

Option 6: from two up to ten (tested) ASA+Active/Standby HA (failover) per VPN load-balancer cluster in each site, times number of VPN load-balanced clusters at site

Scaling: Up to the maximum VPN peers in the data sheet for each ASA pair, with session setup at data sheet rate per site. IP Anycast is responsible for initial load balancing, directing traffic to the nearest IP instance topology-wise (depending on SP-level routing, policies, etc.). Within each site, VIP load balancers (Nexus

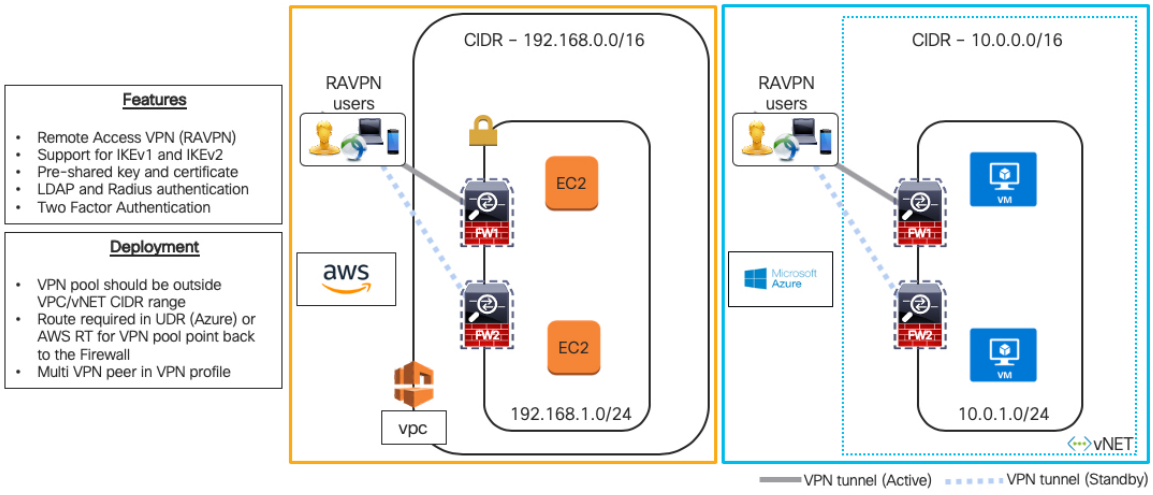
ITD, F5, etc) distribute traffic to the ASAs. Finally, ASA VPN load balancing redistributes traffic as necessary. Cisco has tested up to ten ASAs in a VPN load-balancing cluster. ASA IP assignments will be local or NATted.



Design Choices for the Public Cloud

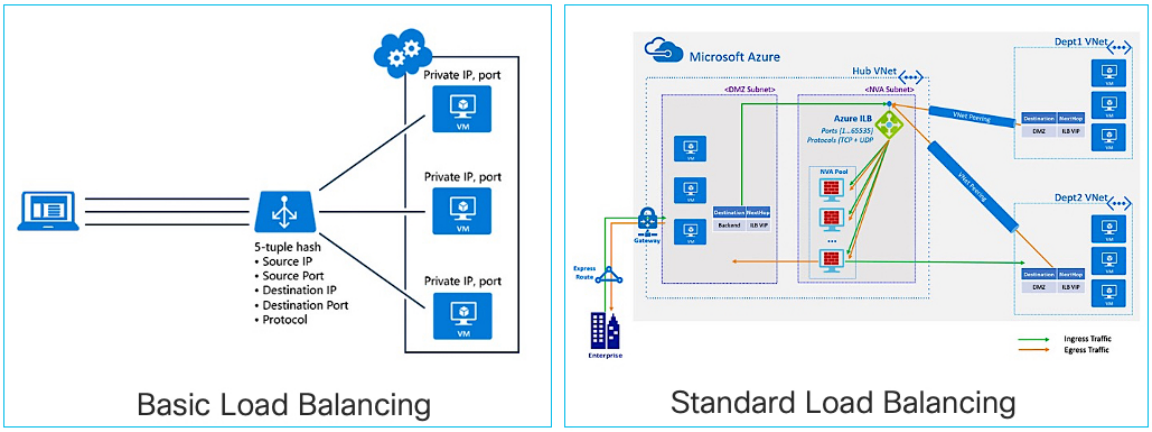
What are design choices for the Public Cloud?

Figure 1: Amazon AWS and Microsoft Azure



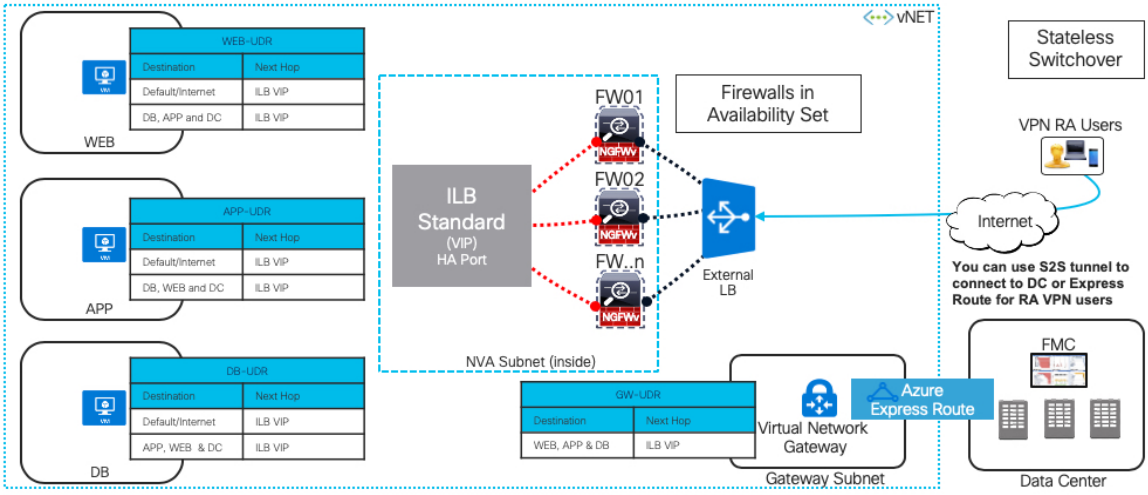
Design Choices for Microsoft Azure Load Balancing

Figure 2: Basic and Standard (Internal and External)



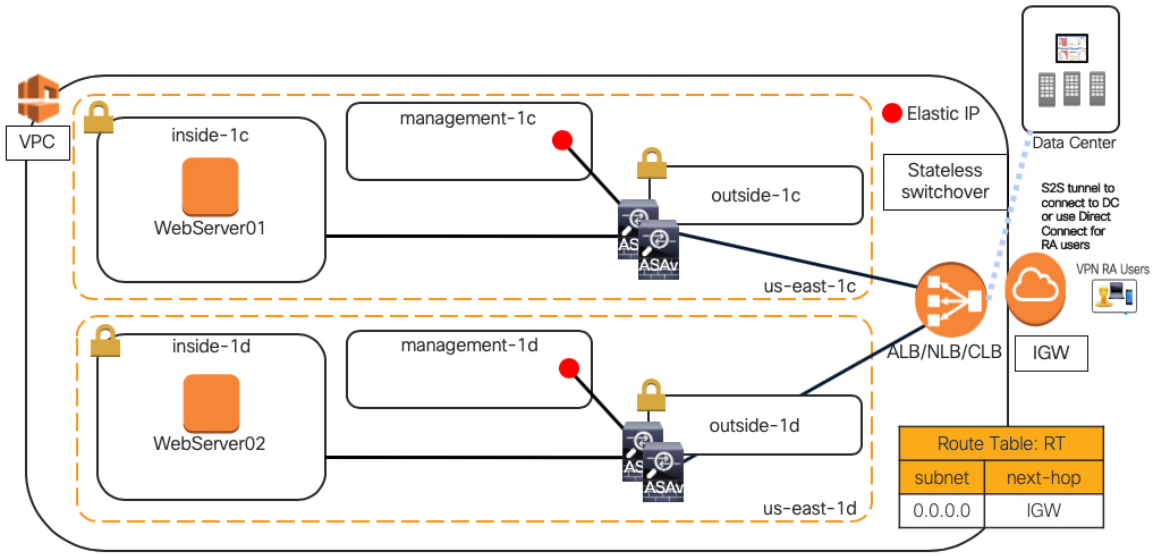
FTDv and ASAv Scalable Design

Figure 3: Azure internal load balancer (ILB) standard & external load balancer



ASAv Scalable Design Using AWS Load Balancing

Figure 4: NLB, ALB, and CLB



Where to Find Remote Access VPN Design Guides

- Cisco Support AnyConnect Examples & Troubleshooting notes—https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client-v4-x/model.html
- Remote Access VPN Design Guide, August 2014—https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-RemoteAccessVPNDesignGuide-AUG14.pdf
- Cisco SAFE Remote Access VPN and DDoS, September 2016 – also covers Firepower 9300 running ASA—https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-RemoteAccessVPNDesignGuide-AUG14.pdf

Where to find more information

- NGFWv RAVPN in AWS—https://youtu.be/2GtK_T9bCAY
- Deploying AnyConnect SSL VPN with ASA (and Firepower Threat Defense) - BRKSEC-2501, CiscoLive!2018 Barcelona
- Deploying AnyConnect with Firepower Threat Defense with posture and MFA - BRKSEC-2348, CiscoLive!2020 Barcelona
- Firepower NGFW Clustering Deep Dive - BRKSEC-3032, CiscoLive!2020 Barcelona
- Firepower Platforms Deep Dive - BRKSEC-3035, CiscoLive!2020 Barcelona
- NGFWv and ASAv in Public Cloud (AWS and Azure) - BRKSEC-2064, CiscoLive!2019 Barcelona
- NGFWv and ASAv in Public Cloud (AWS and Azure) – BRKSEC-2064
- Deploying NGFWv & ASAv in Public Cloud (AWS and Azure) – LTRSEC-3052

- Optimizing Your Firepower/FTD Deployment - BRKSEC-2066
- Best Practices for the Cisco Firepower NGFW - TECSEC-2002
- Firepower Platform Deep Dive - BRKSEC-3035
- Dissecting FTD: architecture and troubleshooting - BRKSEC-3455
- Advanced Firepower IPS deployment - BRKSEC-3300
- Firepower Migration Tools - PSOSEC-2005