AnyConnect Implementation and Performance/Scaling Reference for COVID-19 Preparation

Contents

Introduction

As countries around the world are battling the COVID-19 global pandemic, more and more companies are implementing remote working policies to prevent the spreading of the disease. As a result, there is an increased demand for Remote Access VPN (RAVPN) to provide employees access to internal company resources. This article provides references to configuration guides for quickly setting up RAVPN within the network or identify and address performance or scaling related issues.

Implementation

The following section details AnyConnect remote access configuration and deployments on the various Cisco platforms, as well as certificate installation guides since certificate deployment is an integral part to Cisco remote access due to the certificate authentication requirements for RAVPN.

Licensing

Licenses are required to terminate RAVPN connections on a device. ASA platforms will only support 2 VPN peers without a license. FTDs will not allow AnyConnect configuration to be deployed to the device without licensing. Due to the COVID-19 outbreak, Cisco is offering free temporary licenses to assist users with implementing RAVPN on their Cisco devices. More information about this can be found: Obtaining an Emergency COVID-19 AnyConnect License

AnyConnect Initial Configuration Quickstart Guides

Follow these quickstart guides to implement AnyConnect Remote Access with the most common configurations:

- Configure AnyConnect Secure Mobility Client with Split Tunneling on an ASA
- AnyConnect Remote Access VPN configuration on FTD
- Initial AnyConnect Configuration for FTD managed by FMC (Video)

For full product configuration guides, see below.

Full Configuration Guides

ASA:

- ASA ASDM configuration
- ASA CLI configuration

FTD:

- FTD managed by FDM
- FTD managed by FMC

IOS/IOS-XE:

- IOS router for SSLVPN
- IOS-XE router for SSL VPN (CSR only)
- IOS/IOS-XE router for IKEv2 VPN

Certificate Installation Guides

- ASA
- FTD FDM
- FTD FMC
- IOS/IOS-XE

Performance and Scaling Issues

With significantly increased RAVPN usage, AnyConnect users may experience performance

issues. See the following to determine how to identify these issues and mitigation strategies to address them.

Problem Symptoms and Identification

High CPU Utilization

CPU utilization directly impacts performance for VPN users. CPU utilization will increase as more encrypted or decrypted traffic handled by the device. The device can experience high CPU when the platform approaches the maximum VPN throughput it can handle. It is necessary to determine if the high CPU utilization is due to the device being oversubscribed or due to another issue.

To check if the device is experiencing high CPU, it is suggested to run the following commands:

show process cpu-usage non-zero

show cpu usage

Example output:

```
asa# show processes cpu-usage non-zero
PC         Thread       5Sec     1Min     5Min   Process
0x00000000019da592   0x00007fffd808b040     0.0%     0.0%     0.5%   Logger
0x0000000000844596   0x00007fffd807bd60     0.0%     0.0%     0.1%   CP Processing
0x0000000000c0dc8c   0x00007fffd8074960     0.1%     0.1%     0.1%   ARP Thread
   -          -        43.8%    43.8%    40.3%   DATAPATH-0-2209
   -          -        43.9%    43.8%    40.3%   DATAPATH-1-2210

asa# show cpu usage
CPU utilization for 5 seconds = 88%; 1 minute: 88%; 5 minutes: 82%
```

In the above example, it is observed that DATAPATH-0 and DATAPATH-1 are consuming 87.7% of the total CPU utilization. In this case, the ASA is oversubscribed and is necessary to determine if this symptom is due the a large amount of encrypted and decrypted traffic. This can then be benchmarked against the VPN throughput value documented in the datasheet for that platform.

To calculate the total amount of VPN traffic going through the device per second, we can add the ***Input bytes*** and ***Output bytes*** within the ***Global Statistics*** section found in the ***show crypto accelerator statistics*** command. On an ASA or FTD, clear the output ***show crypto accelerator statistics*** with the command ***clear crypto accelerator statistics***. Wait for a certain amount of time, then run the command: ***show crypto accelerator statistics*** as shown in the following:

```
asa# show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
[Capability]
   Supports hardware crypto: True
   Supports modular hardware crypto: False
   Max accelerators: 2
   Max crypto throughput: 1000 Mbps
   Max crypto connections: 5000
[Global Statistics]
   Number of active accelerators: 2
   Number of non-operational accelerators: 0
```

```
   Input packets: 257353
   Input bytes: 271730225                          <---------------
   Output packets: 2740
   Output error packets: 0
   Output bytes: 57793                             <---------------
[…]
```

Take a few snapshots at specific intervals and get an average throughput in bytes that can be converted into bits per second (bps). The formula to do this is:

$$\frac{[InputBytes + OutputBytes] * 8}{1,000,000 * seconds} = Mbps$$

In the previous example, a ***clear crypto accelerator statistics*** command is issued at time 0 seconds. 10 seconds later, the ***show crypto accelerator statistics*** command was issued to get the total bytes over the 10 second interval. These values are then used to calculate a bps of 217Mbps that was processed over a 10 second interval. Multiple snapshots may be needed to get a more accurate average.

Note that these values will increase for all encrypted/decrypted traffic (HTTPS, SSL, IPsec, SSH, etc.). We can use this value to determine the average VPN throughput and compare it to the datasheet. If the average throughput is approximately the same amount as what is seen on the datasheet for the platform, the device is being oversubscribed by encrypted and decrypted traffic.

Additionally, this method can not be used to determine VPN throughput on firepower 2100 platforms since the counters do not increment for VPN traffic. This is being tracked in CSCvt46830 .

Maximum VPN Connections

When hitting the maximum number of VPN connections, users may experience periods of disruption where they are not able to connect. Although activating the AnyConnect Plus or Apex license unlocks the maximum number of VPN peers, if that maximum is reached no additional users will be allowed onto the device.

To check the maximum amount of VPN connections available on the device, check the output of ***show vpn-sessiondb***:

```
asa# show vpn-sessiondb
----------------------------------------------------------------------------
VPN Session Summary
----------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
                           ----------------------------------------------
AnyConnect Client            :     10 :        218 :          11 :        0
  SSL/TLS/DTLS               :     10 :        218 :          11 :        0
Clientless VPN               :      0 :         73 :           4
  Browser                    :      0 :         73 :           4
----------------------------------------------------------------------------
Total Active and Inactive    :     10             Total Cumulative :    291
Device Total VPN Capacity    :    250
Device Load                  :     4%
----------------------------------------------------------------------------

----------------------------------------------------------------------------
Tunnels Summary
```

```
-------------------------------------------------------------------------
                              Active : Cumulative : Peak Concurrent
                            -----------------------------------------
Clientless                  :      0 :         73 :               4
AnyConnect-Parent           :     10 :        218 :              11
SSL-Tunnel                  :     10 :         77 :              10
DTLS-Tunnel                 :     10 :         65 :              10
-------------------------------------------------------------------------
Totals                      :     30 :        433
-------------------------------------------------------------------------
```

To determine the total supported amount of users supported by the platform, check the datasheet for your device located below.

If VPN users are not able to connect and you've verified that the device is not hitting the maximum number of VPN users, please seek additional assistance from TAC.

Datasheet References

The following datasheets highlight both the maximum number of VPN users supported by a platform and the maximum VPN throughput based on testing. IKEv2 and DTLS AnyConnect are expected to have similar total (aggregated) throughput as the IPsec VPN Throughput listed in each section.

- ASAv
- ASA 5500
- ASA 5585
- Firepower 1000
- Firepower 2100
- Firepower 4100
- Firepower 9300

Potential Mitigations

Enabling Split Tunneling

By default, group policies on the ASA and FTD will implement tunnelall. This will send all traffic generated by RA clients over the VPN to be processed by the headend. Since packet encryption and decryption is directly related to CPU utilization, it is important to make sure only necessary traffic is handled by the VPN headend as permitted by the company's security policy. Consider using a split tunnel policy rather than full tunnel to save the VPN headend from unnecessary load.

- ASA Split Tunneling Guide
- FTD (FMC) Split Tunneling Guide

Note: Tunnel All implements a company wide parameter security policy whereas split tunneling relies on the client device to help protect the user's Internet traffic. Cisco provides additional security tool like Umbrella in order to protect VPN users when a split tunnel policy is used.

Implement VPN Load Balancing (ASA Only)

VPN Load Balancing is a feature supported on ASA platforms that allows two or more ASAs the

ability to share VPN session load. If both devices support 500 VPN peers, by configuring VPN load balancing between them, the devices will support a total of 1000 VPN peers between them. This feature can be used to increase the amount of simultaneous VPN users beyond what a single device can handled. More information about VPN Load Balancing including the load balancing algorithm can be found here: VPN Load Balancing

Configuration Optimization

Additional services enabled on the platform will increase the amount of processing and load on the device. For example, IPS, SSL decryption, NAT, etc. Consider configuring the device as a VPN concentrator that only terminates VPN sessions.

Tunnel Protocol Selection

By default, group policies on ASAs are configured to attempt establishing a DTLS tunnel. If UDP 443 traffic is blocked between the VPN headend and the AnyConnect client, it will automatically fallback to TLS. It is recommended to use DTLS or IKEv2 to increase maximum VPN throughput performance. DTLS offers better performance than TLS due to less protocol overhead. IKEv2 also offers better throughput than TLS. Additionally, using AES-GCM ciphers may slightly improve performance. These ciphers are available in TLS 1.2, DTLS 1.2 and IKEv2.

Enforce per tunnel QoS (FTD Only)

QoS can be implemented to limit the amount of traffic sent to AnyConnect users in the outbound direction. By doing this, the VPN headend can enforce each remote access client gets its fair share of egress bandwidth. More information about this can be found here: FTD Configuration

Implement Crypto Engine Accelerator Bias (ASA Only)

Crypto Engine Accelerator Bias is used to reallocate the crypto cores to favor one encryption protocol over the other (SSL or IPsec). The purpose of this is optimization of AnyConnect throughput if the majority of VPN tunnels use either IPsec or SSL. Implementing this command can result in service interruption and so a maintenance window is required. Additionally, performance (AnyConnect throughput and CPU utilization) improvement may vary depending on the traffic profile. If the VPN headend is only terminating SSL sessions or only IPsec sessions, this command can be considered for further optimization of the VPN headend. The command reference can be found here: Command Reference

To review the current crypto core allocation, run the command ***show crypto accelerator load-balance***. This command does not show the total amount of crypto utilization the device is capable of handling - It indicates the ratio of ssl or ipsec traffic is being allocated to each core. To find the approximate amount of utilization on the device refer to the section above on **High CPU Utilization** and compare the calculated value to the value in the datasheet for the platform.

On an ASA platform that mostly terminates remote access SSLVPN, it is recommended that the crypto core allocation is adjusted to favor SSL with the command ***crypto engine accelerator-bias ssl***.

The following example shows the core allocation on an ASA5555 with the ***crypto engine accelerator-bias ssl*** command to favor AnyConnect SSL clients:

```
asa# sh run all crypto engine
crypto engine accelerator-bias ssl
asa# show crypto accelerator load-balance

[..]
                  Crypto SSL Load Balancing Stats:
                  ================================

Engine      Crypto Cores             SSL Sessions            Active Session
                                                             Distribution (%)
======     ==============      ============================   ================
  0        IPSEC 1, SSL 7      Total: 166714  Active:   205         100.0%
[..]
```

The Active Session Distribution will always be 100% regardless of the platform's current crypto utilization.

Note: Cryptographic core rebalancing is available on the following platforms: ASA 5585, 5580, 5545/5555, 4110, 4120, 4140, 4150, SM-24, SM-36, SM-44 and ASASM.

FAQ

Licensing

Q: Why can I not download AnyConnect software?

A: You must purchase the AnyConnect Plus or Apex license in order to be able to download the AnyConnect client. After this, you should be entitled. If you are not entitled despite purchasing the AnyConnect Apex or Plus license, open a case with Entitlement to fix this issue.

Q: Why do I see 99999 Purchased for the AnyConnect license in my smart licensing account?

A: This is expected with certain AnyConnect licenses, such as the AnyConnect Plus Perpetual or non-banded AnyConnect Plus or Apex licenses.

Q: What determines when “In Use” decrements?

A: This value decrements whenever a device using the AnyConnect license is registered. For example, if you register FMC then add the AnyConnect Plus license to a device, the In Use value for the AnyConnect Plus license will decrement. This value **DOES NOT** decrement based on current user sessions. Registering ASAv devices **DOES NOT** decrement the “In Use” count. This is a known cosmetic issue. You can not register more devices than the number of authorized users that have purchased.

Q: What determines the Purchased value?

A: The purchase value is determined by the number of authorized users purchased with the license. For example, a 25 user AnyConnect Plus license will have a 25 Purchased count.

Q: How do I enable strong encryption?

A: In order to enable strong encryption, you must check the box “Allow export-controlled functionality on the products registered with this token” when creating the registration token.

Q: How do I convert from PAK to smart licensing?

A: A case should be opened with Licensing for this.

Q: If I have a "X" user license, what will happen if "X+1" or more users connect to the device?

A: With the Apex and Plus license, the full VPN user capacity of the device is unlocked. As long as the device does not reach its maximum vpn user limit, the device will continue to accept connections. There is no enforcement on the device for VPN user sessions and it is honor based. It is your responsibility to purchase additional authorized user licenses if the vpn session usage for the device needs to be increased. To check the maximum number of users supported by the device, check the data sheet for the device on the Cisco Website or run ***show vpn-sessiondb*** and examining the “Device Total VPN Capacity”. For ASAs, you can also run the ***show version*** or ***show vpn-sessiondb license-summary*** commands.

Q: How can I check that the license is activated on my device?

A: On FTDs, you will not be able to deploy AnyConnect configuration unless the license is activated. On ASAs, you can check the ***show version*** or ***show vpn-sessiondb license-summary*** to examine how many users are allowed. Without an activated license, the maximum will be 2 users. Note on the ASA, the above mentioned commands will not display Plus/Apex license information. This is being tracked with the enhancement request CSCuw74731.

Configuration

Q: What ASA platforms can I use for VPN load balancing? Can I use different ASA hardware platforms or different software versions in a VPN load balancing cluster?

A: Yes a VPN load balancing cluster can consists of different physical or virtual ASA models, including the ASAv. However, it is generally recommended for the cluster to be homogeneous. If different software versions are used in a vpn load balancing cluster, then only IPsec sessions are supported. For a details please refer to: Guidelines and Limitations for VPN Load Balancing.

Q: How do I configure split-tunneling? And can you exclude certain type of application traffic, such as Office 365, from being tunneled in a split-tunnel configuration?

A: See Cisco Community article AnyConnect Split Tunneling for configuration examples of various use cases. You can also use a combination of split-tunneling and dynamic split-tunneling to achieve application based split-tunneling. For an example on how to optimize AnyConnect split-tunneling for Office 365 and WebEx, see How to optimize Anyconnect for Microsoft Office365 and Cisco Webex connections.

Q: I'm seeing the error "Untrusted certificate warning" when connecting to an ASA headend with AnyConnect. Why is this happening?

A: This is likely because the headend is using a self-signed certificate. To fix this, an SSL

certificate can be purchased from a Certificate Authority and installed on the headend ASA. For detailed implementation steps, please refer to: Configure ASA: SSL Digital Certificate Installation and Renewal.

Q: Are wildcard certificates supported on Cisco RAVPN headends?

A: Yes wildcard and certificates with DNS subject alternate names (SANs) are supported.

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

A: Active/Standby failover is supported with VPN load balancing. The standby device will take over immediately with no impact to the VPN tunnel if the active unit fails. VPN Load balancing is not supported with an Active/Active failover configuration.

Monitoring

Q: Which SNMP MIB can I use to monitor the ASA CPU usage?

A: The CISCO-PROCESS-MIB can be used to monitor the ASA CPU usage. For a complete list of supported MIBs, please refer to: Adaptive Security Appliance MIB Support List. Also to obtain a list of the supported SNMP MIBs and OIDs for a specific ASA, one can issue the following command: ***show snmp-server oidlist.***

Q: How do I monitor the number of users currently connected to a VPN headend?

A: Use ***show vpn-sessiondb*** from the CLI to check the current number of users on an ASA or FTD, or SNMP MIB

CISCO-REMOTE-ACCESS-MONITOR-MIB.

Troubleshooting

Q: Some of our AnyConnect VPN users seem to experience frequent disconnects. How do I troubleshoot such issues:

A: For troubleshooting VPN disconnect and other common AnyConnect issues, please refer to: AnyConnect VPN Client Troubleshooting Guide - Common Problems.

Q: When a certain amount of users connects to the VPN headend, no more users are able to connect. The license is activated on the device and ***show vpn-sessiondb*** shows that the device can handle more users. What could be the issue?

A: Check the VPN local address pool for those users to make sure that the number of users connecting does not exceed the amount of addresses available. You can verify with the command ***show ip local pool [pool-name]***. Another potential cause on older platforms is that the ***vpn-sessiondb max-anyconnect-premium-or-essentials-limit*** command is set to a low value. You can verify this with the command ***show run all vpn-sessiondb***. If this is the case, the value can be increased or the command can be removed to prevent this limit.

Getting Additional Help

For additional assistance, please contact TAC. A valid support contract will be required: Cisco Worldwide Support Contacts

You can also visit the Cisco VPN Community here.

Additionally, you can check out the TAC Security Show Podcasts

References

Please find below additional links to other resources useful for AnyConnect deployments and the handling of COVOD-19 related issues in general.

- Cisco Security Responds to Increase in Remote Workers - Cisco Community
- AnyConnect Ordering Guide
- AnyConnect Licensing FAQ
- AnyConnect VPN, ASA, and FTD FAQ for Secure Remote Workers