COVID-19準備工作中的AnyConnect實施和效能/擴展參考

目錄

簡介

隨著世界各國都在與COVID-19全球大流行病作鬥爭，越來越多的公司正在實施遠端工作政策，以防止該疾病的傳播。因此，對遠端訪問VPN(RAVPN)的需求增加，以使員工能夠訪問公司內部資源。本文提供一些配置指南的參考，用於在網路中快速設定RAVPN，或確定並解決效能或擴展相關問題。

實現

以下部分詳細介紹各種思科平台上的AnyConnect遠端訪問配置和部署，以及證書安裝指南，因為由於RAVPN的證書身份驗證要求，證書部署是思科遠端訪問的一個有機組成部分。

授權

在裝置上終止RAVPN連線需要許可證。ASA平台僅支援2個沒有許可證的VPN對等點。FTD不會允許在未經授權的情況下將AnyConnect配置部署到裝置。由於COVID-19爆發，思科提供免費臨時許可證，以幫助使用者在其思科裝置上實施RAVPN。有關此問題的詳細資訊，請參閱：獲取緊急COVID-19 AnyConnect許可證

AnyConnect初始配置快速入門手冊

按照以下快速入門手冊，使用最常見的配置實施AnyConnect遠端訪問：

- 使用 ASA 上的分割通道設定 AnyConnect Secure Mobility 用戶端
- FTD上的AnyConnect遠端存取VPN組態
- FMC管理的FTD的初始AnyConnect配置（影片）

有關完整的產品配置指南，請參見下文。

完整配置指南

ASA:

- ASA ASDM配置
- ASA CLI配置

FTD:

- FDM管理的FTD
- 由FMC管理的FTD

IOS/IOS-XE:

- 適用於SSLVPN的IOS路由器
- 適用於SSL VPN的IOS-XE路由器（僅限CSR）
- 適用於IKEv2 VPN的IOS/IOS-XE路由器

憑證安裝指南

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

效能和擴展問題

隨著RAVPN使用量的顯著增加，AnyConnect使用者可能會遇到效能問題。請參見以下內容，以確定如何確定這些問題以及解決這些問題的緩解策略。

問題症狀和識別

高CPU利用率

CPU利用率直接影響VPN使用者的效能。CPU利用率將隨著裝置處理更多加密或解密的流量而增加

。當平台接近其可處理的最大VPN吞吐量時，裝置會遇到高CPU使用率。必須確定CPU使用率高是由於裝置超額訂閱還是由於其他問題。

要檢查裝置是否遇到高CPU使用率，建議運行以下命令：

show process cpu-usage non-zero

show cpu usage

輸出示例：

```
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%
```

在上面的示例中，發現DATAPATH-0和DATAPATH-1消耗的CPU總利用率的87.7%。在這種情況下，ASA為超訂用，必須確定此症狀是否由於大量加密和解密流量所致。然後，可以參照該平台資料表中記錄的VPN吞吐量值對此進行基準標籤。

要計算每秒通過裝置的VPN流量總量，可以在*show crypto accelerator statistics*命令中的*Global Statistics*部分新增*Input bytes*和*Output bytes*。在ASA或FTD上，使用命令*clear crypto accelerator statistics*清除輸出*show crypto accelerator statistics*。等待一定的時間，然後運行命令：*show crypto accelerator statistics*，如下所示：

```
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                             <----------------
[…]
```

按特定間隔拍攝幾個快照，獲取可轉換為位/秒(bps)的平均吞吐量（以位元組為單位）。 這樣做的公式為：

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

在上一個示例中，在0秒時發出*clear crypto accelerator statistics*命令。10秒後，發出*show crypto accelerator statistics*命令以獲取10秒間隔內的總位元組數。然後，使用這些值計算在10秒時間間隔內處理的bps(217Mbps)。可能需要多個快照以獲得更準確的平均值。

請注意，所有加密/解密的流量（HTTPS、SSL、IPsec、SSH等）的這些值都會增加。 我們可以使用此值確定VPN的平均吞吐量並將其與資料表進行比較。如果平均吞吐量與平台的資料表上顯示的吞吐量大致相同，則裝置會被加密和解密的流量超額使用。

此外，此方法不能用於確定firepower 2100平台上的VPN吞吐量，因為計數器不會增加VPN流量。CSCvt中正在跟蹤此項46830 .

最大VPN連線數

達到最大VPN連線數時，使用者可能會在無法連線時經歷中斷。雖然啟用AnyConnect Plus或Apex許可證可以解鎖VPN對等裝置的最大數量，但是如果達到該最大數量，則不允許其他使用者訪問裝置。

要檢查裝置上可用的VPN連線的最大數量，請檢查*show vpn-sessiondb*的輸出：

```
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
----------------------------------------------------------------------------
```

要確定平台支援的使用者總數，請檢視以下裝置的資料表。

如果VPN使用者無法連線，並且您已經驗證裝置未達到最大VPN使用者數，請向TAC尋求其他幫助。

資料表參考

以下資料表突出顯示了平台支援的最大VPN使用者數以及基於測試的最大VPN吞吐量。IKEv2和DTLS AnyConnect的總吞吐量（聚合）預計與每個部分列出的IPsec VPN吞吐量相似。

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

潛在緩解

啟用分割通道

預設情況下，ASA和FTD上的組策略將實施隧道。這將通過VPN傳送RA客戶端生成的所有流量，並由頭端進行處理。由於資料包加密和解密與CPU利用率直接相關，因此確保只有必要流量在公司安全策略允許的情況下由VPN頭端處理非常重要。考慮使用拆分隧道策略而不是全隧道來將VPN頭端從不必要的負載中儲存。

- ASA分割隧道指南
- FTD(FMC)分割通道指南

附註：Tunnel All實施公司範圍引數安全策略，而分割隧道依賴於客戶端裝置來幫助保護使用者的Internet流量。思科提供額外的安全工具（例如Umbrella），以便在使用分割通道原則時保護VPN使用者。

實施VPN負載平衡（僅限ASA）

VPN負載平衡是ASA平台上支援的一項功能，它允許兩個或多個ASA共用VPN會話負載。如果兩台裝置都支援500個VPN對等點，則通過在它們之間配置VPN負載平衡，裝置將支援它們之間的總共1000個VPN對等點。此功能可用於增加同步VPN使用者的數量，使其超過單個裝置所能處理的數量。有關VPN負載均衡的詳細資訊（包括負載均衡演算法），請訪問以下網站：VPN負載平衡

組態最佳化

平台上啟用的其他服務將增加裝置上的處理量和負載。例如，IPS、SSL解密、NAT等。考慮將裝置配置為僅終止VPN會話的VPN集中器。

通道通訊協定選擇

預設情況下，ASA上的組策略配置為嘗試建立DTLS隧道。如果在VPN頭端和AnyConnect客戶端之間阻止了UDP 443流量，它將自動回退到TLS。建議使用DTLS或IKEv2來提高最大VPN吞吐量效能。DTLS比TLS具有更好的效能，因為協定開銷更少。IKEv2提供的吞吐量也比TLS好。此外，使用AES-GCM密碼可能會稍微改善效能。這些密碼可用於TLS 1.2、DTLS 1.2和IKEv2。

依照通道執行QoS（僅限FTD）

可以實施QoS以限制在出站方向傳送到AnyConnect使用者的流量。通過這樣做，VPN前端可以強制每個遠端訪問客戶端獲得其公平份額的出口頻寬。有關這方面的更多資訊，請訪問以下網站

：FTD組態

實施加密引擎加速器偏差（僅限ASA）

加密引擎加速器偏置用於重新分配加密核心，使一個加密協定優先於另一個加密協定（SSL或IPsec）。 如果大多數VPN隧道使用IPsec或SSL，則此操作的目的是最佳化AnyConnect吞吐量。實施此命令可能會導致服務中斷，因此需要維護視窗。此外，效能（AnyConnect吞吐量和CPU利用率）的提高可能因流量配置檔案而異。如果VPN頭端僅終止SSL會話或僅IPsec會話，則可以考慮使用此命令進一步最佳化VPN頭端。命令引用可以在以下位置找到：安裝和升級指南

要檢視當前的加密核心分配，請運行***show crypto accelerator load-balance***命令。此命令不顯示裝置能夠處理的加密使用總量 — 它表示正在將ssl或ipsec流量比率分配給每個核心。要瞭解裝置上的近似使用量，請參閱上面的**CPU使用率高**部分，並將計算出的值與平台資料表中的值進行比較。

在主要終止遠端訪問SSLVPN的ASA平台上，建議使用***crypto engine accelerator-bias ssl***命令調整加密核心分配以偏向SSL。

以下示例顯示使用***crypto engine accelerator-bias ssl*** 命令以支援AnyConnect SSL客戶端的ASA5555上的核心分配：

```
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%
[..]
```

無論平台的當前加密使用率如何，活動會話分佈始終是100%。

附註：加密核心再平衡在以下平台上可用：ASA 5585、5580、5545/555、4110、4120、4140、4150、SM-24、SM-36、SM-44和ASASM。

常見問題

授權

Q:為什麼我無法下載AnyConnect軟體？

A:您必須購買AnyConnect Plus或Apex許可證才能下載AnyConnect客戶端。之後，您就有權了。如果您儘管購買了AnyConnect Apex或Plus許可證，但仍未獲得授權，請開啟包含授權的案例以解決此問題。

Q:為什麼我的智99999許可帳戶中會看到為AnyConnect許可證購買的許可證？

A:某些AnyConnect許可證（例如AnyConnect Plus永久許可證或非帶帶AnyConnect Plus或Apex許

可證）需要這樣做。

Q:什麼決定了何時減少「使用中」？

A:只要註冊使用AnyConnect許可證的裝置，此值就會減少。例如，如果您註冊FMC，然後將AnyConnect Plus許可證新增到裝置，則AnyConnect Plus許可證的使用中值將遞減。該值不**會基於當**前使用者會話遞減。註冊ASAv設**備不會**減少「正在使用」計數。這是一個已知的美容問題。註冊的裝置不能超過已購買的授權使用者數量。

Q:什麼決定了購買價值？

A:購買價值取決於使用許可證購買的授權使用者數量。例如，25位使用者的AnyConnect Plus許可證將具有25個購買計數。

Q:如何啟用強加密？

A:為了啟用強加密，在建立註冊令牌時，必須選中「允許使用此令牌註冊的產品上的匯出控制功能」框。

Q:如何從PAK轉換為智慧許可？

A:應為此使用許可證開啟案例。

Q:如果我擁有「X」使用者許可證，如果「X+1」或更多使用者連線到裝置會發生什麼情況？

A:使用Apex和Plus許可證，裝置的全部VPN使用者容量將被解鎖。只要裝置未達到其最大vpn使用者限制，裝置就會繼續接受連線。裝置上沒有針對VPN使用者會話的強制措施，而是基於榮譽。如果需要增加裝置的VPN會話使用率，則您有責任購買額外的授權使用者許可證。要檢查裝置支援的最大使用者數，請在思科網站上檢查裝置的資料表，或運行***show vpn-sessiondb***並檢查「裝置總VPN容量」。對於ASA，您還可以運行***show version***或***show vpn-sessiondb license-summary***命令。

Q:如何檢查我的裝置上是否已啟用許可證？

A:在FTD上，除非啟用許可證，否則您將無法部署AnyConnect配置。在ASA上，可以檢查***show version***或***show vpn-sessiondb license-summary***，以檢查允許的使用者數。如果沒有啟用的許可證，最多將有2個使用者。請注意，在ASA上，上述命令不會顯示Plus/Apex許可證資訊。正在用增強功能請求CSCuw74731對此進行跟蹤。

組態

問：我可以使用哪些ASA平台進行VPN負載平衡？是否可在VPN負載平衡群集中使用不同的ASA硬體平台或不同的軟體版本？

答：是:VPN負載平衡集群可以由不同的物理或虛擬ASA模型組成，包括ASAv。然而，通常建議群集是同構的。如果vpn負載平衡集群中使用了不同的軟體版本，則僅支援IPsec會話。有關詳細資訊

，請參閱VPN負載平衡的准則和限制。

問：如何配置分割隧道？此外，您能否排除某些型別的應用流量（例如Office 365）在拆分隧道配置中通過隧道傳輸？

A:有關各種使用案例的配置示例，請參閱Cisco社群文章 AnyConnect Split Tunneling。還可以使用分割隧道和動態分割隧道的組合來實現基於應用的分割隧道。有關如何最佳化Office 365和WebEx的AnyConnect拆分隧道的示例，請參閱如何最佳化Microsoft Office365和Cisco Webex連線的Anyconnect。

Q:在使用AnyConnect連線到ASA頭端時，我看到「Untrusted certificate warning」（不受信任的證書警告）錯誤。為什麼會這樣？

A:這可能是因為頭端使用自簽名證書。要解決此問題，可以從證書頒發機構購買SSL證書並將其安裝在頭端ASA上。有關實施步驟的詳細資訊，請參閱配置ASA:安裝和更新 SSL 數位憑證.

Q:Cisco RAVPN頭端是否支援萬用字元證書？

A:支援萬用字元和具有DNS使用者替代名稱(SAN)的證書。

問：一個裝置是否可以使用負載平衡和故障切換？

A:VPN負載平衡支援主用/備用故障切換。如果主用裝置發生故障，備用裝置將立即接管，不會影響VPN隧道。主用/主用故障切換配置不支援VPN負載平衡。

監控

問：我可以使用哪個SNMP MIB監控ASA CPU使用情況？

答：CISCO-PROCESS-MIB可用於監控ASA CPU使用情況。有關支援的MIB的完整清單，請參閱自適應安全裝置MIB支援清單。另外，要獲取特定ASA支援的SNMP MIB和OID的清單，可以發出以下命令：***show snmp-server oidlist。***

Q:如何監控當前連線到VPN頭端的使用者數量？

A:從CLI使用*show vpn-sessiondb*檢查ASA或FTD或SNMP MIB上的當前使用者數

CISCO-REMOTE-ACCESS-MONITOR-MIB。

疑難排解

Q:我們的一些AnyConnect VPN使用者似乎經常遇到斷開的情況。如何解決此類問題：

A:有關VPN斷開連線和其它常見AnyConnect問題的故障排除，請參閱：AnyConnect VPN客戶端故障排除指南 — 常見問題。

Q:當一定數量的使用者連線到VPN頭端時，沒有更多的使用者能夠連線。許可證在裝置上啟用，***show vpn-sessiondb***表明裝置可以處理更多使用者。可能是什麼問題？

A:檢查這些使用者的VPN本地地址池，確保連線的使用者數量不超過可用地址數量。您可以使用***show ip local pool [pool-name]***命令進行驗證。在較舊平台上的另一個潛在原因是***vpn-sessiondb max-anyconnect-premium-or-essentials-limit***命令設定為低值。可以使用***show run all vpn-***

*sessiondb*命令驗證此*情況。*如果是這種情況，可以增加值或刪除命令來防止此限制。

獲取其他幫助

如需其他協助，請聯絡TAC。需要有效的支援合約：思科全球支援聯絡人

您還可以在此處訪問Cisco VPN社群。

此外，您還可以檢視TAC Security Show Podcast

參考資料

請找到下列其他資源的連結，這些資源可用於AnyConnect部署以及通常處理COVOD-19相關問題。

- 思科安全解決方案應對遠端員工增加 — 思科社群
- AnyConnect訂購指南
- AnyConnect許可常見問題
- 安全遠端工作人員的AnyConnect VPN、ASA和FTD常見問題解答