Guida di riferimento all'implementazione e alle prestazioni/alla scalabilità di AnyConnect per la preparazione della COVID-19

Sommario

Introduzione

Mentre i paesi di tutto il mondo stanno combattendo la pandemia di Covid-19, sempre più aziende stanno implementando politiche di lavoro a distanza per prevenire la diffusione della malattia. Di conseguenza, aumenta la domanda di VPN ad accesso remoto (RAVPN) per fornire ai dipendenti l'accesso alle risorse aziendali interne. In questo articolo vengono forniti riferimenti alle guide alla configurazione per configurare rapidamente RAVPN all'interno della rete o per identificare e risolvere i problemi relativi alle prestazioni o alla scalabilità.

Implementazione

La sezione seguente descrive la configurazione dell'accesso remoto AnyConnect e le distribuzioni sulle diverse piattaforme Cisco, nonché le guide all'installazione dei certificati, in quanto la distribuzione dei certificati è parte integrante dell'accesso remoto Cisco a causa dei requisiti di autenticazione dei certificati per RAVPN.

Licenze

Per terminare le connessioni RAVPN su un dispositivo, sono necessarie licenze. Le piattaforme ASA supportano solo 2 peer VPN senza una licenza. I FTD non consentono di distribuire la configurazione AnyConnect sul dispositivo senza licenza. A causa dell'epidemia di COVID-19, Cisco offre licenze temporanee gratuite per assistere gli utenti nell'implementazione di RAVPN sui loro dispositivi Cisco. Ulteriori informazioni su questo argomento sono disponibili: Come ottenere una licenza AnyConnect per Covid-19 di emergenza

Guide introduttive alla configurazione iniziale di AnyConnect

Seguire queste guide introduttive per implementare AnyConnect Remote Access con le configurazioni più comuni:

- Configurazione di AnyConnect Secure Mobility Client con split tunneling su una ASA
- Configurazione VPN ad accesso remoto AnyConnect su FTD
- Configurazione iniziale di AnyConnect per FTD gestita da FMC (video)

Per le guide complete alla configurazione del prodotto, vedere di seguito.

Guide complete alla configurazione

ASA:

- Configurazione ASA ASDM
- Configurazione ASA CLI

FTD

- FTD gestito da FDM
- FTD gestito da FMC

IOS/IOS-XE:

- Router IOS per SSLVPN
- Router IOS-XE per SSL VPN (solo CSR)
- Router IOS/IOS-XE per VPN IKEv2

Guide all'installazione dei certificati

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

Problemi di prestazioni e scalabilità

Con un uso della VPN notevolmente aumentato, gli utenti AnyConnect potrebbero riscontrare problemi di prestazioni. Vedere quanto segue per determinare come identificare questi problemi e le strategie di mitigazione per risolverli.

Sintomi e identificazione dei problemi

Utilizzo CPU elevato

L'utilizzo della CPU influisce direttamente sulle prestazioni per gli utenti VPN. L'utilizzo della CPU aumenterà con l'aumento del traffico crittografato o decrittografato gestito dal dispositivo. Il dispositivo può sperimentare una CPU elevata quando la piattaforma si avvicina al throughput VPN massimo che può gestire. È necessario determinare se l'elevato utilizzo della CPU è dovuto alla sottoscrizione eccessiva del dispositivo o a un altro problema.

Per verificare se la CPU del dispositivo è elevata, si consiglia di eseguire i seguenti comandi:

show process cpu-usage diverso da zero

mostra utilizzo cpu

Output di esempio:

```
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%
```

Nell'esempio precedente, si osserva che DATAPATH-0 e DATAPATH-1 consumano l'87,7% dell'utilizzo totale della CPU. In questo caso, l'ASA ha una sottoscrizione eccessiva ed è necessario per determinare se il problema è dovuto alla grande quantità di traffico crittografato e decrittografato. Questo può quindi essere confrontato con il valore di throughput VPN documentato nel datasheet per quella piattaforma.

Per calcolare la quantità totale di traffico VPN che attraversa il dispositivo al secondo, è possibile aggiungere i ***byte di input*** e di ***output*** nella sezione ***Global Statistics*** trovata nel comando ***show crypto accelerator statistics***. Su un'ASA o un FTD, cancellare l'output ***show crypto accelerator statistics*** con il comando ***clear crypto accelerator statistics***. Attendere qualche istante, quindi eseguire il comando: ***visualizzare le statistiche dell'acceleratore di crittografia***, come mostrato di seguito:

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

Eseguite alcune istantanee a intervalli specifici e ottenete un throughput medio in byte che può essere convertito in bit al secondo (bps). La formula per eseguire questa operazione è:

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

Nell'esempio precedente, un comando ***clear crypto accelerator statistics*** viene emesso alla data e all'ora di 0 secondi. 10 secondi dopo, è stato emesso il comando ***show crypto accelerator statistics*** per ottenere il totale dei byte nell'intervallo di 10 secondi. Questi valori vengono quindi utilizzati per calcolare un bps di 217Mbps elaborato in un intervallo di 10 secondi. Per ottenere una media più accurata potrebbero essere necessarie più istantanee.

Tenere presente che questi valori aumenteranno per tutto il traffico crittografato/decrittografato (HTTPS, SSL, IPsec, SSH, ecc.). Possiamo usare questo valore per determinare il throughput VPN medio e confrontarlo con il foglio dati. Se il throughput medio è all'incirca uguale a quello visualizzato sul foglio dati della piattaforma, il dispositivo viene sovrascritto dal traffico crittografato e decrittografato.

Inoltre, questo metodo non può essere utilizzato per determinare il throughput VPN sulle piattaforme firepower 2100 poiché i contatori non vengono incrementati per il traffico VPN. Questa condizione viene rilevata in CSCvt46830 .

Numero massimo di connessioni VPN

Quando si raggiunge il numero massimo di connessioni VPN, gli utenti possono riscontrare periodi di interruzione delle attività in cui non sono in grado di connettersi. Anche se l'attivazione della licenza AnyConnect Plus o Apex sblocca il numero massimo di peer VPN, se si raggiunge questo numero massimo, non sarà possibile aggiungere altri utenti al dispositivo.

Per controllare la quantità massima di connessioni VPN disponibili sul dispositivo, controllare l'output di ***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
------------------------------------------------------------------------------
```

Per determinare il numero totale supportato di utenti supportati dalla piattaforma, controllare il foglio dati del dispositivo riportato di seguito.

Se gli utenti VPN non sono in grado di connettersi e si è verificato che il dispositivo non sta raggiungendo il numero massimo di utenti VPN, richiedere ulteriore assistenza a TAC.

Riferimenti al foglio dati

Le seguenti schede tecniche evidenziano sia il numero massimo di utenti VPN supportati da una piattaforma sia il throughput VPN massimo basato su test. Ci si aspetta che IKEv2 e DTLS AnyConnect abbiano un throughput totale (aggregato) simile a quello della VPN IPsec elencata in ciascuna sezione.

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

Potenziali mitigazioni

Abilitazione del tunneling ripartito

Per impostazione predefinita, i criteri di gruppo sull'ASA e sull'FTD implementano il tunneling all. In questo modo, tutto il traffico generato dai client RSA sulla VPN verrà elaborato dall'headend. Poiché la crittografia e la decrittografia dei pacchetti sono direttamente correlate all'utilizzo della CPU, è importante assicurarsi che solo il traffico necessario venga gestito dall'headend VPN, come consentito dalla policy di sicurezza aziendale. Prendere in considerazione l'uso di un criterio di suddivisione del tunnel anziché di un tunnel completo per salvare l'headend VPN da carichi non necessari.

- Guida al tunneling diviso ASA
- Guida al tunneling ripartito FTD (FMC)

Nota: Tunnel All implementa un criterio di sicurezza dei parametri a livello aziendale, mentre il tunneling suddiviso si basa sul dispositivo client per proteggere il traffico Internet dell'utente. Cisco fornisce uno strumento di sicurezza aggiuntivo, come Umbrella, per proteggere gli utenti VPN quando si usa un criterio di separazione del tunnel.

Implementazione del bilanciamento del carico VPN (solo ASA)

Il bilanciamento del carico VPN è una funzione supportata sulle piattaforme ASA che consente a due o più appliance ASA di condividere il carico delle sessioni VPN. Se entrambi i dispositivi supportano 500 peer VPN, configurando il bilanciamento del carico VPN tra di essi, i dispositivi supporteranno un totale di 1000 peer VPN tra di essi. Questa funzione può essere utilizzata per aumentare la quantità di utenti VPN simultanei oltre il limite gestibile da un singolo dispositivo. Per ulteriori informazioni sul bilanciamento del carico VPN, incluso l'algoritmo di bilanciamento del carico, vedere: Load balancing VPN

Ottimizzazione della configurazione

I servizi aggiuntivi abilitati sulla piattaforma aumentano la quantità di elaborazione e il carico sul dispositivo. Ad esempio IPS, decrittografia SSL, NAT e così via. Si consiglia di configurare il dispositivo come concentratore VPN che interrompe solo le sessioni VPN.

Selezione protocollo tunnel

Per impostazione predefinita, i criteri di gruppo sulle appliance ASA sono configurati per tentare di stabilire un tunnel DTLS. Se il traffico UDP 443 tra l'headend VPN e il client AnyConnect è bloccato, verrà automaticamente eseguito il fallback a TLS. Si consiglia di utilizzare DTLS o IKEv2 per aumentare le prestazioni di throughput VPN massime. Il protocollo DTLS offre prestazioni migliori rispetto al protocollo TLS grazie a un minore sovraccarico del protocollo. Inoltre, IKEv2 offre una velocità effettiva superiore rispetto a TLS. Inoltre, l'uso dei cifrari AES-GCM può migliorare leggermente le prestazioni. Queste cifrature sono disponibili in TLS 1.2, DTLS 1.2 e IKEv2.

Applica QoS per tunnel (solo FTD)

Èpossibile implementare QoS per limitare la quantità di traffico inviato agli utenti AnyConnect nella direzione di uscita. In questo modo, l'headend VPN può imporre a ogni client di accesso remoto di ottenere la giusta quota di larghezza di banda in uscita. Per ulteriori informazioni su questo argomento, fare clic qui: Configurazione FTD

Implementa differenza acceleratore motore di crittografia (solo ASA)

La polarizzazione dell'acceleratore del motore di crittografia viene utilizzata per riallocare i core di crittografia in modo da favorire un protocollo di crittografia rispetto all'altro (SSL o IPsec). Lo scopo di questa operazione è l'ottimizzazione del throughput di AnyConnect se la maggior parte dei tunnel VPN usa IPsec o SSL. L'implementazione di questo comando può causare l'interruzione del servizio ed è quindi necessaria una finestra di manutenzione. Inoltre, il miglioramento delle prestazioni (velocità effettiva e utilizzo della CPU di AnyConnect) può variare a seconda del profilo di traffico. Se l'headend VPN termina solo sessioni SSL o solo sessioni IPsec, è possibile prendere in considerazione questo comando per ottimizzare ulteriormente l'headend VPN. Il riferimento al comando è disponibile qui: Riferimento per i comandi

Per rivedere l'allocazione corrente dei core di crittografia, eseguire il comando ***show crypto accelerator load-balance***. Questo comando non mostra la quantità totale di utilizzo della crittografia che il dispositivo è in grado di gestire. Indica la percentuale di traffico ssl o ipsec allocato a ciascun core. Per calcolare la quantità approssimativa di utilizzo sul dispositivo, consultare la sezione precedente relativa all'**utilizzo elevato della CPU** e confrontare il valore calcolato con il valore del foglio dati per la piattaforma.

Su una piattaforma ASA che termina principalmente la VPN ad accesso remoto, è consigliabile modificare l'allocazione del core di crittografia in modo da preferire SSL con il comando ***crypto engine accelerator-bias ssl***.

L'esempio seguente mostra l'allocazione di base su un'appliance ASA5555 con il comando ***crypto engine accelerator-bias ssl*** per favorire i client AnyConnect SSL:

```
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%
[..]
```

La distribuzione della sessione attiva sarà sempre 100%, indipendentemente dall'utilizzo della crittografia della piattaforma.

Nota: Il ribilanciamento del core di crittografia è disponibile sulle seguenti piattaforme: ASA 5585, 5580, 5545/5555, 4110, 4120, 4140, 4150, SM-24, SM-36, SM-44 e ASASM.

Domande frequenti

Licenze

D: Perché non posso scaricare il software AnyConnect?

A: Per scaricare il client AnyConnect, è necessario acquistare la licenza AnyConnect Plus o Apex. Dopo questo, dovresti avere diritto. Se non si ha diritto a usare la licenza AnyConnect Apex o Plus nonostante l'acquisto, aprire una richiesta di assistenza in modo da poter risolvere il problema.

D: Perché lo switch 99999 è stato acquistato per la licenza AnyConnect nel mio account di licenza Smart?

A: Questa procedura è prevista per alcune licenze AnyConnect, ad esempio le licenze AnyConnect Plus Perpetual o le licenze AnyConnect Plus o Apex non basate sul volume.

D: Cosa determina quando "In uso" decrementa?

A: Questo valore diminuisce quando viene registrata una periferica che usa la licenza AnyConnect. Ad esempio, se si registra un FMC e si aggiunge la licenza AnyConnect Plus a un dispositivo, il valore in uso della licenza AnyConnect Plus diminuirà. Questo valore **NON** diminuisce in base alle sessioni utente correnti. La registrazione delle periferiche ASAv **NON** riduce il numero di dispositivi in uso. Si tratta di un problema noto di natura estetica. Non è possibile registrare un numero di dispositivi superiore al numero di utenti autorizzati acquistati.

D: Cosa determina il valore Acquistato?

A: Il valore di acquisto è determinato dal numero di utenti autorizzati acquistati con la licenza. Ad esempio, per una licenza AnyConnect Plus di 25 utenti, conteggio degli utenti acquistati: 25.

D: Come attivare la crittografia avanzata

A: Per abilitare la crittografia avanzata, è necessario selezionare la casella "Consenti funzionalità di controllo dell'esportazione sui prodotti registrati con questo token" durante la creazione del token di registrazione.

D: Come si esegue la conversione da PAK a Smart Licensing?

A: Per questa richiesta, aprire una richiesta di assistenza in Licensing.

D: Se si dispone di una licenza utente "X", cosa succede se "X+1" o più utenti si connettono al dispositivo?

A: Con la licenza Apex e Plus, la capacità utente VPN completa del dispositivo viene sbloccata. Finché il dispositivo non raggiunge il limite massimo di utenti VPN, continuerà ad accettare connessioni. Sul dispositivo non è presente alcuna imposizione per le sessioni utente VPN ed è basato sul onore. Se è necessario aumentare l'uso della sessione vpn per il dispositivo, è responsabilità del cliente acquistare altre licenze utente autorizzate. Per verificare il numero massimo di utenti supportati dal dispositivo, controllare la scheda tecnica del dispositivo sul sito Web di Cisco o eseguire ***show vpn-sessiondb*** ed esaminare "Device Total VPN Capacity". Sulle appliance ASA, è possibile eseguire anche i comandi ***show version*** o ***show vpn-sessiondb license-summary***.

D: Come verificare che la licenza sia attivata sul dispositivo?

A: Sugli FTD, non sarà possibile distribuire la configurazione AnyConnect a meno che la licenza non sia attivata. Sulle appliance ASA, è possibile controllare il valore ***show version*** o ***show vpn-sessiondb license-summary*** per esaminare il numero di utenti consentiti. Senza una licenza attivata, il massimo sarà di 2 utenti. Nota: sull'appliance ASA, i comandi menzionati non visualizzano le informazioni sulle licenze Plus/Apex. La richiesta di miglioramento CSCuw74731 viene rilevata.

Configurazione

D: Quali piattaforme ASA posso utilizzare per il bilanciamento del carico VPN? È possibile

utilizzare piattaforme hardware ASA o versioni software diverse in un cluster di bilanciamento del carico VPN?

R: Sì, un cluster di bilanciamento del carico VPN può essere composto da diversi modelli ASA fisici o virtuali, incluso ASAv. Tuttavia, è generalmente consigliabile che il cluster sia omogeneo. Se in un cluster di bilanciamento del carico vpn vengono utilizzate versioni software diverse, sono supportate solo le sessioni IPSec. Per ulteriori informazioni, vedere: Linee guida e limitazioni per il bilanciamento del carico della VPN.

D: Come configurare lo split-tunneling? È possibile escludere determinati tipi di traffico delle applicazioni, ad esempio Office 365, dal tunneling in una configurazione a tunnel separato?

A: Per esempi di configurazione di diversi scenari, vedere l'articolo della Cisco Community AnyConnect Split Tunneling. Per ottenere lo split-tunneling basato sulle applicazioni, è possibile anche utilizzare una combinazione di split-tunneling e split-tunneling dinamico. Per un esempio su come ottimizzare lo split-tunneling AnyConnect per Office 365 e WebEx, vedere Come ottimizzare Anyconnect per le connessioni Microsoft Office 365 e Cisco Webex.

D: Quando si collega un headend ASA con AnyConnect, viene visualizzato l'errore "Avviso certificato non attendibile". Perché sta succedendo questo?

A: È probabile che l'headend utilizzi un certificato autofirmato. Per risolvere questo problema, è possibile acquistare un certificato SSL da un'autorità di certificazione e installarlo sull'appliance ASA dell'headend. Per una procedura di implementazione dettagliata, consultare: Configurazione dell'ASA: installazione e rinnovo del certificato digitale SSL.

D: Gli headend Cisco RAVPN supportano i certificati con caratteri jolly?

A: Sì sono supportati i caratteri jolly e i certificati con nomi alternativi soggetto DNS (SAN).

D: Un singolo dispositivo può utilizzare sia il bilanciamento del carico che il failover?

A: Il failover attivo/standby è supportato con il bilanciamento del carico della VPN. In caso di guasto dell'unità attiva, il dispositivo di standby subentra immediatamente senza alcun impatto sul tunnel VPN. Il bilanciamento del carico della VPN non è supportato con una configurazione di failover attivo/attivo.

Monitoraggio

D: Quale MIB SNMP è possibile utilizzare per monitorare l'utilizzo della CPU dell'ASA?

R: CISCO-PROCESS-MIB può essere usato per monitorare l'uso della CPU dell'ASA. Per un elenco completo dei MIB supportati, consultare: Elenco del supporto MIB per Adaptive Security Appliance. Anche per ottenere un elenco dei MIB e degli OID SNMP supportati per una appliance ASA specifica, è possibile usare il comando seguente: ***show snmp-server oidlist.***

D: Come monitorare il numero di utenti attualmente connessi a un headend VPN?

A: Usare ***show vpn-sessiondb*** dalla CLI per controllare il numero corrente di utenti su un'ASA o un FTD o un MIB SNMP

CISCO-REMOTE-ACCESS-MONITOR-MIB.

Risoluzione dei problemi

D: Alcuni dei nostri utenti VPN AnyConnect sembrano sperimentare disconnessioni frequenti. Come posso risolvere questi problemi:

A: Per la risoluzione dei problemi di disconnessione VPN e di altri problemi comuni di AnyConnect, consultare: Guida alla risoluzione dei problemi dei client VPN di AnyConnect - Problemi comuni.

D: Quando un certo numero di utenti si connette all'headend VPN, non è più possibile connettersi. La licenza viene attivata sul dispositivo e ***show vpn-sessiondb*** mostra che il dispositivo può gestire più utenti. Quale potrebbe essere il problema?

A: Controllare il pool di indirizzi locali VPN per gli utenti in questione per verificare che il numero di utenti che si connettono non superi la quantità di indirizzi disponibili. Per verificarlo, usare il comando ***show ip local pool [pool-name]***. Un'altra possibile causa sulle piattaforme precedenti è l'impostazione del comando ***vpn-sessiondb max-anyconnect-premium-or-essentials-limit*** su un valore basso. Per verificare questa condizione, usare il comando ***show run all vpn-sessiondb***. In questo caso, è possibile aumentare il valore o rimuovere il comando per evitare questo limite.

Ulteriori informazioni

Per ulteriore assistenza, contattare TAC. È necessario un contratto di assistenza valido: Contatti del supporto Cisco internazionali

Qui è possibile visitare la Cisco VPN Community.

Inoltre, è possibile controllare i podcast di TAC Security Show

Riferimenti

Di seguito sono riportati altri collegamenti ad altre risorse utili per le distribuzioni AnyConnect e la gestione dei problemi relativi alla COVOD-19 in generale.

- Cisco Security risponde all'aumento dei lavoratori remoti - Cisco Community
- Guida agli ordini di AnyConnect
- Domande frequenti sulle licenze AnyConnect
- Domande frequenti su AnyConnect VPN, ASA e FTD per dipendenti remoti sicuri