Referencia de implementación y rendimiento/escalabilidad de AnyConnect para la preparación de COVID-19

Contenido

Introducción
Instrumentación
Licencias
Guías de inicio rápido de configuración inicial de AnyConnect
Guías de configuración completas
Guías de instalación de certificados
Problemas de rendimiento y escalabilidad
Síntomas e identificación del problema
Utilización alta de la CPU
Número máximo de conexiones VPN
Referencias de la hoja de datos
Mitigaciones potenciales
Habilitación de la tunelización dividida
Implementar equilibrio de carga VPN (solo ASA)
Optimización de la configuración
Selección de protocolo de túnel
Aplicación de QoS por túnel (sólo FTD)
Implementación de la Bia del Acelerador de Crypto Engine (solo ASA)
Preguntas frecuentes
Licencias
Configuración
Control
Resolución de problemas
Obtener ayuda adicional
Referencias

Introducción

A medida que los países de todo el mundo luchan contra la pandemia global COVID-19, cada vez más empresas implementan políticas de trabajo remotas para prevenir la propagación de la enfermedad. Como resultado, existe una mayor demanda de VPN de acceso remoto (RAVPN) para proporcionar a los empleados acceso a los recursos internos de la empresa. En este artículo se proporcionan referencias a las guías de configuración para configurar rápidamente RAVPN dentro de la red o identificar y abordar problemas relacionados con el rendimiento o la ampliación.

Instrumentación

La siguiente sección detalla la configuración de acceso remoto de AnyConnect y las implementaciones en las diversas plataformas de Cisco, así como las guías de instalación de certificados, ya que la implementación de certificados es una parte integral del acceso remoto de Cisco debido a los requisitos de autenticación de certificados para RAVPN.

Licencias

Se requieren licencias para finalizar las conexiones RAVPN en un dispositivo. Las plataformas ASA sólo admitirán 2 puntos de VPN sin licencia. Los FTD no permitirán que la configuración de AnyConnect se implemente en el dispositivo sin licencia. Debido al brote de COVID-19, Cisco ofrece licencias temporales gratuitas para ayudar a los usuarios a implementar RAVPN en sus dispositivos Cisco. Se puede encontrar más información al respecto: Obtención de una licencia AnyConnect de emergencia COVID-19

Guías de inicio rápido de configuración inicial de AnyConnect

Siga estas guías de inicio rápido para implementar AnyConnect Remote Access con las configuraciones más comunes:

- Configuración de AnyConnect Secure Mobility Client con túneles divididos en ASA
- Configuración de VPN de acceso remoto AnyConnect en FTD
- Configuración de AnyConnect inicial para FTD gestionada por FMC (Vídeo)

Para obtener guías completas de configuración de productos, consulte a continuación.

Guías de configuración completas

ASA:

- configuración ASDM de ASA
- Configuración CLI ASA

FTD:

- FTD gestionado por FDM
- FTD gestionado por FMC

IOS/IOS-XE:

- Router IOS para SSLVPN
- Router IOS-XE para SSL VPN (sólo CSR)
- Router IOS/IOS-XE para VPN IKEv2

Guías de instalación de certificados

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

Problemas de rendimiento y escalabilidad

Con el aumento significativo del uso de RAVPN, los usuarios de AnyConnect pueden experimentar problemas de rendimiento. Vea lo siguiente para determinar cómo identificar estos problemas y estrategias de mitigación para abordarlos.

Síntomas e identificación del problema

Utilización alta de la CPU

La utilización de la CPU afecta directamente al rendimiento de los usuarios de VPN. El uso de la CPU aumentará a medida que el dispositivo administre más tráfico cifrado o descifrado. El dispositivo puede experimentar una CPU alta cuando la plataforma se acerca al rendimiento máximo de VPN que puede manejar. Es necesario determinar si la alta utilización de la CPU se debe a la suscripción excesiva del dispositivo o a otro problema.

Para verificar si el dispositivo está experimentando un uso excesivo de la CPU, se sugiere ejecutar los siguientes comandos:

show process cpu-usage non-zero

show cpu usage

Ejemplo de salida:

```
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%
```

En el ejemplo anterior, se observa que DATAPATH-0 y DATAPATH-1 consumen el 87,7% del uso total de la CPU. En este caso, el ASA está sobresuscrito y es necesario para determinar si este síntoma se debe a la gran cantidad de tráfico cifrado y descifrado. Esto se puede comparar con el valor de rendimiento de VPN documentado en la hoja de datos para esa plataforma.

Para calcular la cantidad total de tráfico VPN que pasa a través del dispositivo por segundo, podemos agregar los ***bytes de entrada*** y ***bytes de salida*** dentro de la sección ***Estadísticas globales*** que se encuentra en el comando ***show crypto Accelerator statistics***. En un ASA o FTD, borre la salida ***show crypto Accelerator statistics*** con el comando ***clear crypto Accelerator statistics***. Espere una cierta cantidad de tiempo y ejecute el comando: ***mostrar estadísticas del acelerador de criptografía*** como se muestra en lo siguiente:

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

Tome algunas instantáneas a intervalos específicos y obtenga un rendimiento promedio en bytes que se puede convertir en bits por segundo (bps). La fórmula para hacerlo es:

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

En el ejemplo anterior, se ejecuta un comando ***clear crypto Accelerator statistics*** en el tiempo 0 segundos. 10 segundos después, se ejecutó el comando ***show crypto Accelerator statistics*** para obtener los bytes totales durante el intervalo de 10 segundos. Estos valores se utilizan luego para calcular un bps de 217 Mbps que se procesó en un intervalo de 10 segundos. Es posible que se necesiten varias instantáneas para obtener una media más precisa.

Tenga en cuenta que estos valores aumentarán para todo el tráfico cifrado/descifrado (HTTPS, SSL, IPsec, SSH, etc.). Podemos utilizar este valor para determinar el rendimiento promedio de VPN y compararlo con la hoja de datos. Si el rendimiento medio es aproximadamente la misma cantidad que se ve en la hoja de datos de la plataforma, el tráfico cifrado y descifrado está sobresuscrito al dispositivo.

Además, este método no se puede utilizar para determinar el rendimiento de VPN en las plataformas firepower 2100, ya que los contadores no aumentan para el tráfico VPN. Esto se está rastreando en CSCvt46830 .

Número máximo de conexiones VPN

Al alcanzar el número máximo de conexiones VPN, es posible que los usuarios experimenten períodos de interrupción en los que no puedan conectarse. Aunque la activación de la licencia AnyConnect Plus o Apex desbloquea el número máximo de peers VPN, si se alcanza ese máximo, no se permitirá que otros usuarios accedan al dispositivo.

Para verificar la cantidad máxima de conexiones VPN disponibles en el dispositivo, verifique el resultado de ***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
------------------------------------------------------------------------------
```

Para determinar la cantidad total de usuarios admitidos por la plataforma, verifique la hoja de datos del dispositivo que se encuentra a continuación.

Si los usuarios de VPN no pueden conectarse y ha verificado que el dispositivo no está alcanzando el número máximo de usuarios de VPN, solicite asistencia adicional del TAC.

Referencias de la hoja de datos

Las siguientes fichas técnicas resaltan tanto el número máximo de usuarios de VPN soportados por una plataforma como el rendimiento máximo de VPN basado en pruebas. Se espera que IKEv2 y DTLS AnyConnect tengan un rendimiento total (agregado) similar al rendimiento de VPN IPsec enumerado en cada sección.

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

Mitigaciones potenciales

Habilitación de la tunelización dividida

De forma predeterminada, las políticas de grupo en ASA y FTD implementarán tunnelall. Esto enviará todo el tráfico generado por los clientes RA a través de la VPN para que la cabecera lo procese. Dado que el cifrado y el descifrado de paquetes están directamente relacionados con la utilización de la CPU, es importante asegurarse de que el centro distribuidor de VPN solo gestione el tráfico necesario, tal como permite la política de seguridad de la empresa. Considere la posibilidad de utilizar una política de túnel dividido en lugar de un túnel completo para guardar la cabecera VPN de una carga innecesaria.

- Guía de túnel dividido ASA
- Guía de tunelación dividida de FTD (FMC)

Nota: Tunnel All implementa una política de seguridad de parámetros de toda la empresa, mientras que la tunelización dividida se basa en el dispositivo cliente para ayudar a proteger el tráfico de Internet del usuario. Cisco proporciona una herramienta de seguridad adicional como Umbrella para proteger a los usuarios de VPN cuando se utiliza una política de túnel dividido.

Implementar equilibrio de carga VPN (solo ASA)

El balanceo de carga VPN es una función soportada en las plataformas ASA que permite a dos o más ASA compartir la carga de sesión VPN. Si ambos dispositivos admiten 500 puntos de VPN, al configurar el balanceo de carga VPN entre ellos, los dispositivos admitirán un total de 1000 puntos de VPN entre ellos. Esta función se puede utilizar para aumentar la cantidad de usuarios simultáneos de VPN más allá de lo que puede manejar un único dispositivo. Puede encontrar más información sobre el Balanceo de Carga VPN, incluido el algoritmo de balanceo de carga aquí: Equilibrio de carga VPN

Optimización de la configuración

Los servicios adicionales habilitados en la plataforma aumentarán la cantidad de procesamiento y carga en el dispositivo. Por ejemplo, IPS, descifrado SSL, NAT, etc. Considere la posibilidad de configurar el dispositivo como concentrador VPN que solo finaliza las sesiones VPN.

Selección de protocolo de túnel

De forma predeterminada, las políticas de grupo en los ASA se configuran para intentar establecer un túnel DTLS. Si el tráfico UDP 443 se bloquea entre la cabecera VPN y el cliente AnyConnect, se devolverá automáticamente a TLS. Se recomienda utilizar DTLS o IKEv2 para aumentar el rendimiento máximo de VPN. DTLS ofrece un mejor rendimiento que TLS debido a una menor sobrecarga de protocolo. IKEv2 también ofrece un mejor rendimiento que TLS. Además, el uso de cifrados AES-GCM puede mejorar ligeramente el rendimiento. Estos cifrados están disponibles en TLS 1.2, DTLS 1.2 e IKEv2.

Aplicación de QoS por túnel (sólo FTD)

QoS se puede implementar para limitar la cantidad de tráfico enviado a los usuarios de AnyConnect en la dirección saliente. Al hacer esto, la cabecera VPN puede aplicar cada cliente de acceso remoto obtiene su justa cuota de ancho de banda de egreso. Puede encontrar más información sobre esto aquí: Configuración de FTD

Implementación de la Bia del Acelerador de Crypto Engine (solo ASA)

Crypto Engine Accelerator Bias se utiliza para reasignar los núcleos criptográficos para favorecer un protocolo de cifrado sobre el otro (SSL o IPsec). El propósito de esto es optimizar el rendimiento de AnyConnect si la mayoría de los túneles VPN utilizan IPsec o SSL. La implementación de este comando puede dar lugar a la interrupción del servicio y, por lo tanto, se requiere una ventana de mantenimiento. Además, la mejora del rendimiento (rendimiento de AnyConnect y utilización de la CPU) puede variar en función del perfil de tráfico. Si la cabecera VPN sólo está terminando sesiones SSL o sólo sesiones IPsec, este comando se puede considerar para una mayor optimización del centro distribuidor VPN. La referencia de comandos se puede encontrar aquí: Referencia de Comandos

Para revisar la asignación de núcleo crypto actual, ejecute el comando ***show crypto acelerador load-balance***. Este comando no muestra la cantidad total de utilización de crypto que el dispositivo puede manejar - Indica la proporción de tráfico ssl o ipsec que se está asignando a cada núcleo. Para encontrar la cantidad aproximada de utilización en el dispositivo, consulte la sección anterior sobre **Uso Excesivo de CPU** y compare el valor calculado con el valor en la hoja de datos para la plataforma.

En una plataforma ASA que en su mayoría termina el acceso remoto SSLVPN, se recomienda ajustar la asignación de núcleo crypto para favorecer SSL con el comando ***crypto engine Accelerator-bias ssl***.

El siguiente ejemplo muestra la asignación de núcleo en un ASA5555 con el comando ***crypto engine Accelerator-bias ssl*** para favorecer a los clientes 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 distribución de sesiones activas siempre será del 100% independientemente de la utilización de criptografía actual de la plataforma.

Nota: El rebalanceo del núcleo criptográfico está disponible en las siguientes plataformas: ASA 5585, 5580, 5545/5555, 4110, 4120, 4140, 4150, SM-24, SM-36, SM-44 y ASASM.

Preguntas frecuentes

Licencias

A: ¿Por qué no puedo descargar el software de AnyConnect?

R: Debe comprar la licencia AnyConnect Plus o Apex para poder descargar el cliente AnyConnect. Después de esto, debería tener derecho. Si no tiene derecho a ello a pesar de adquirir la licencia AnyConnect Apex o Plus, abra un caso con Entitlement para solucionar este problema.

A: ¿Por qué veo 99999 comprados para la licencia de AnyConnect en mi cuenta de licencias inteligentes?

R: Esto se espera con ciertas licencias de AnyConnect, como las licencias AnyConnect Plus Perpetual o AnyConnect Plus o Apex sin banda.

A: ¿Qué determina cuándo disminuye "En uso"?

R: Este valor disminuye cada vez que se registra un dispositivo que utiliza la licencia de AnyConnect. Por ejemplo, si registra FMC y luego agrega la licencia AnyConnect Plus a un dispositivo, el valor En uso de la licencia AnyConnect Plus disminuirá. Este valor **NO** disminuye en función de las sesiones de usuario actuales. El registro de los dispositivos ASAv **NO** disminuye el número de "En uso". Este es un tema cosmético conocido. No puede registrar más dispositivos que el número de usuarios autorizados que han adquirido.

A: ¿Qué determina el valor adquirido?

R: El valor de compra se determina por el número de usuarios autorizados que se adquirieron con la licencia. Por ejemplo, una licencia AnyConnect Plus de 25 usuarios tendrá un recuento de 25 clientes.

A: ¿Cómo puedo habilitar el cifrado seguro?

R: Para habilitar el cifrado seguro, debe marcar la casilla "Permitir la funcionalidad controlada por exportación en los productos registrados con este token" al crear el token de registro.

A: ¿Cómo puedo pasar de PAK a licencias inteligentes?

R: Se debe abrir un caso con licencia para esto.

A: Si tengo una licencia de usuario "X", ¿qué ocurrirá si "X+1" o más usuarios se conectan al dispositivo?

R: Con la licencia Apex y Plus, se desbloquea la capacidad total de usuario de VPN del dispositivo. Mientras el dispositivo no alcance su límite máximo de usuario vpn, continuará aceptando conexiones. No hay aplicación en el dispositivo para las sesiones de usuario VPN y se basa en el honor. Es su responsabilidad comprar licencias de usuario autorizadas adicionales si es necesario aumentar el uso de la sesión vpn para el dispositivo. Para verificar el número máximo de usuarios soportados por el dispositivo, verifique la hoja de datos del dispositivo en el sitio web de Cisco o ejecute ***show vpn-sessiondb*** y examine la "Capacidad VPN Total del Dispositivo". Para los ASA, también puede ejecutar los comandos ***show version*** o ***show vpn-sessiondb license-summary***.

A: ¿Cómo puedo comprobar que la licencia está activada en mi dispositivo?

R: En los FTD, no podrá implementar la configuración de AnyConnect a menos que se active la licencia. En los ASA, puede verificar la ***versión show*** o ***show vpn-sessiondb license-summary*** para examinar cuántos usuarios se permiten. Sin una licencia activada, el máximo será de 2 usuarios. Tenga en cuenta que en el ASA, los comandos mencionados anteriormente no mostrarán la información de la licencia Plus/Apex. Esto se está rastreando con la solicitud de mejora CSCuw74731.

Configuración

P: ¿Qué plataformas ASA puedo utilizar para el balanceo de carga de VPN? ¿Puedo utilizar

diferentes plataformas de hardware ASA o diferentes versiones de software en un clúster de balanceo de carga VPN?

R: Sí, un clúster de balanceo de carga VPN puede estar formado por diferentes modelos de ASA físicos o virtuales, incluido ASAv. Sin embargo, generalmente se recomienda que el clúster sea homogéneo. Si se utilizan diferentes versiones de software en un clúster de balanceo de carga vpn, sólo se soportan las sesiones IPsec. Para obtener más información, consulte: Pautas y limitaciones para el Balanceo de Carga VPN.

P: ¿Cómo configuro la tunelización dividida? ¿Y puede excluir cierto tipo de tráfico de aplicaciones, como Office 365, de ser tunelizado en una configuración de túnel dividido?

R: Consulte el artículo de la comunidad de Cisco AnyConnect Split Tunneling para ver ejemplos de configuración de varios casos prácticos. También puede utilizar una combinación de tunelización dividida y tunelización dividida dinámica para lograr la tunelización dividida basada en aplicaciones. Para obtener un ejemplo sobre cómo optimizar la tunelización dividida de AnyConnect para Office 365 y WebEx, vea Cómo optimizar Anyconnect para las conexiones de Microsoft Office365 y Cisco Webex.

A: Veo el error "Advertencia de certificado no fiable" al conectarse a una cabecera ASA con AnyConnect. ¿Por qué ocurre esto?

R: Esto probablemente se deba a que la cabecera está utilizando un certificado autofirmado. Para corregir esto, se puede comprar un certificado SSL a una Autoridad de Certificación e instalarlo en el ASA de cabecera. Para ver los pasos de implementación detallados, consulte: Configuración de ASA: Instalación y renovación del certificado digital de SSL.

A: ¿Los certificados comodín son compatibles con las cabeceras de Cisco RAVPN?

R: Sí, se admiten caracteres comodín y certificados con nombres alternativos de asunto (SAN) DNS.

P: ¿Puede un solo dispositivo utilizar el balanceo de carga y la conmutación por fallas?

R: La conmutación por fallas activa/en espera se soporta con el balanceo de carga VPN. El dispositivo en espera se hará cargo inmediatamente sin que se produzca ningún impacto en el túnel VPN si la unidad activa falla. El balanceo de carga VPN no se soporta con una configuración de failover Activo/Activo.

Control

P: ¿Qué MIB SNMP puedo utilizar para monitorear el uso de la CPU de ASA?

R: CISCO-PROCESS-MIB se puede utilizar para monitorear el uso de la CPU de ASA. Para obtener una lista completa de MIBs soportadas, consulte: Lista de Soporte de MIB de Adaptive Security Appliance. También para obtener una lista de MIBs y OIDs SNMP soportados para un ASA específico, se puede ejecutar el siguiente comando: ***show snmp-server oidlist.***

A: ¿Cómo superviso el número de usuarios conectados actualmente a una cabecera VPN?

R: Utilice *show vpn-sessiondb* de la CLI para verificar el número actual de usuarios en un ASA o FTD, o SNMP MIB

CISCO-REMOTE-ACCESS-MONITOR-MIB.

Resolución de problemas

A: Algunos de nuestros usuarios de AnyConnect VPN parecen experimentar frecuentes desconexiones. ¿Cómo soluciono estos problemas?:

R: Para resolver problemas de desconexión de VPN y otros problemas comunes de AnyConnect, consulte: Guía de Troubleshooting de AnyConnect VPN Client - Problemas Comunes.

A: Cuando una cierta cantidad de usuarios se conecta a la cabecera VPN, ya no se pueden conectar más usuarios. La licencia se activa en el dispositivo y ***show vpn-sessiondb*** muestra que el dispositivo puede manejar más usuarios. ¿Cuál podría ser el problema?

R: Verifique el conjunto de direcciones locales VPN para esos usuarios para asegurarse de que el número de usuarios que se conectan no exceda la cantidad de direcciones disponibles. Puede verificar con el comando ***show ip local pool [pool-name]***. Otra causa potencial en las plataformas más antiguas es que el comando ***vpn-sessiondb max-anyconnect-premium-or-essentials-limit*** se establece en un valor bajo. Puede verificar esto con el comando ***show run all vpn-sessiondb***. Si este es el caso, el valor se puede aumentar o se puede quitar el comando para evitar este límite.

Obtener ayuda adicional

Para obtener asistencia adicional, póngase en contacto con el TAC. Se requerirá un contrato de soporte válido: Contactos de soporte global de Cisco

También puede visitar la Comunidad Cisco VPN aquí.

Además, puede consultar los podcasts del programa de seguridad del TAC

Referencias

A continuación, encontrará enlaces adicionales a otros recursos útiles para implementaciones de AnyConnect y la gestión de problemas relacionados con COVOD-19 en general.

- La seguridad de Cisco responde al aumento del número de trabajadores remotos - Comunidad de Cisco
- Guía de pedidos de AnyConnect
- Preguntas frecuentes sobre licencias de AnyConnect
- Preguntas frecuentes sobre AnyConnect VPN, ASA y FTD para trabajadores remotos seguros