AnyConnect-Implementierungs- und Leistungs-/Skalierungsreferenz für COVID-19-Vorbereitung

Inhalt

Einführung

Während Länder auf der ganzen Welt gegen die globale Pandemie COVID-19 kämpfen, setzen immer mehr Unternehmen eine Politik der Fernarbeit ein, um die Ausbreitung der Krankheit zu verhindern. Die Nachfrage nach Remote Access VPN (RAVPN), um Mitarbeitern den Zugriff auf interne Unternehmensressourcen zu ermöglichen, steigt. Dieser Artikel enthält Referenzen zu Konfigurationsleitfäden für die schnelle Einrichtung von RAVPN im Netzwerk oder die Identifizierung und Behebung von Leistungs- oder Skalierungsproblemen.

Implementierung

Im folgenden Abschnitt werden die Konfiguration und die Bereitstellungen für den Remote-Zugriff über AnyConnect auf den verschiedenen Cisco Plattformen sowie die Installationsanleitungen für

Zertifikate beschrieben, da die Bereitstellung von Zertifikaten aufgrund der Authentifizierungsanforderungen für RAVPN ein integraler Bestandteil des Remote-Zugriffs von Cisco ist.

Lizenzierung

Lizenzen sind erforderlich, um RAVPN-Verbindungen auf einem Gerät zu terminieren. ASA-Plattformen unterstützen nur 2 VPN-Peers ohne Lizenz. FTDs lassen keine Bereitstellung der AnyConnect-Konfiguration auf dem Gerät ohne Lizenzierung zu. Aufgrund des Ausbruchs von COVID-19 bietet Cisco kostenlose temporäre Lizenzen an, um Benutzer bei der Implementierung von RAVPN auf ihren Cisco Geräten zu unterstützen. Weitere Informationen hierzu finden Sie unter: Erhalt einer COVID-19 AnyConnect-Notlizenz

Kurzanleitungen zur Erstkonfiguration bei AnyConnect

Befolgen Sie diese Kurzanleitungen, um AnyConnect Remote Access mit den gängigsten Konfigurationen zu implementieren:

- Konfigurieren des AnyConnect Secure Mobility Client mit Split Tunneling auf einer ASA
- AnyConnect Remote Access VPN-Konfiguration auf FTD
- Erstmalige AnyConnect-Konfiguration für FTD, verwaltet durch FMC (Video)

Vollständige Leitfäden zur Produktkonfiguration finden Sie unten.

Vollständige Konfigurationsanleitungen

ASA:

- ASA ASDM-Konfiguration
- ASA CLI-Konfiguration

FTD:

- FTD verwaltet von FDM
- FTD verwaltet von FMC

IOS/IOS-XE:

- IOS-Router für SSL VPN
- IOS-XE-Router für SSL VPN (nur CSR)
- IOS/IOS-XE-Router für IKEv2-VPN

Zertifizierungsinstallationsanleitungen

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

Leistungs- und Skalierungsprobleme

Bei deutlich erhöhter RAVPN-Nutzung kann es für AnyConnect-Benutzer zu Leistungsproblemen kommen. Im Folgenden erfahren Sie, wie Sie diese Probleme identifizieren und entsprechende Strategien zur Problembehebung einsetzen können.

Problemsymptome und Identifizierung

Hohe CPU-Auslastung

Die CPU-Auslastung wirkt sich direkt auf die Leistung von VPN-Benutzern aus. Die CPU-Auslastung steigt, wenn mehr verschlüsselter oder entschlüsselter Datenverkehr vom Gerät verarbeitet wird. Das Gerät kann eine hohe CPU erleben, wenn die Plattform dem maximalen VPN-Durchsatz nähert, den es verarbeiten kann. Es muss ermittelt werden, ob die hohe CPU-Auslastung auf eine Überbelegung des Geräts oder auf ein anderes Problem zurückzuführen ist.

Um zu überprüfen, ob das Gerät eine hohe CPU aufweist, werden folgende Befehle empfohlen:

Anzeige der CPU-Nutzung nicht null

CPU-Nutzung anzeigen

Beispielausgabe:

```
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%
```

Im obigen Beispiel wird beobachtet, dass DATAPATH-0 und DATAPATH-1 87,7 % der gesamten CPU-Auslastung ausmachen. In diesem Fall ist die ASA überbelegt und muss ermitteln, ob dieses Symptom auf die große Menge an verschlüsseltem und entschlüsseltem Datenverkehr zurückzuführen ist. Dies kann dann anhand des VPN-Durchsatzwerts verglichen werden, der im Datenblatt für diese Plattform dokumentiert ist.

Zur Berechnung des gesamten VPN-Datenverkehrs, der pro Sekunde durch das Gerät fließt, können die *Eingabe-Bytes* und die *Ausgabe-Bytes* im Abschnitt "*Globale Statistiken"* im Befehl *show crypto accelerator statistics* hinzugefügt werden. Löschen Sie auf einem ASA- oder FTD-Gerät die Ausgabe, um *Krypto-Beschleunigungsstatistiken* mit dem Befehl *Clear Crypto Accelerator-Statistiken anzuzeigen*. Warten Sie eine bestimmte Zeit, und führen Sie dann den Befehl aus: *Zeigt Statistiken zu Krypto-Beschleunigern* an, wie in den folgenden Abschnitten gezeigt:

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

Nehmen Sie einige Snapshots in bestimmten Abständen, um einen durchschnittlichen Durchsatz in Byte zu erhalten, der in Bit pro Sekunde (Bit/s) konvertiert werden kann. Die Formel hierfür lautet:

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

Im vorherigen Beispiel wird ein Befehl ***für eine klare Verschlüsselungsbeschleunigungsstatistik*** mit einer Zeitspanne von 0 Sekunden ausgegeben. 10 Sekunden später wurde der Befehl ***show crypto accelerator*** ausgegeben, um die Gesamtbyte über das 10-Sekunden-Intervall zu erhalten. Diese Werte werden dann zur Berechnung von 217 Mbit/s verwendet, die in einem Intervall von 10 Sekunden verarbeitet wurden. Um einen genaueren Durchschnitt zu erhalten, sind möglicherweise mehrere Snapshots erforderlich.

Beachten Sie, dass sich diese Werte für den gesamten verschlüsselten/entschlüsselten Datenverkehr (HTTPS, SSL, IPsec, SSH usw.) erhöhen. Mit diesem Wert können wir den durchschnittlichen VPN-Durchsatz ermitteln und ihn mit dem Datenblatt vergleichen. Wenn der durchschnittliche Durchsatz etwa der gleiche ist wie im Datenblatt für die Plattform angegeben, wird das Gerät durch verschlüsselten und entschlüsselten Datenverkehr überbelegt.

Darüber hinaus kann diese Methode nicht zur Ermittlung des VPN-Durchsatzes auf 2100-Firewalls verwendet werden, da die Zähler für den VPN-Datenverkehr nicht inkrementell sind. Dies wird im CSCvt46830 nachverfolgt. .

Maximale Anzahl an VPN-Verbindungen

Wenn die maximale Anzahl an VPN-Verbindungen erreicht wird, kann es zu Unterbrechungszeiten kommen, wenn keine Verbindung hergestellt werden kann. Obwohl die Aktivierung der AnyConnect Plus- oder Apex-Lizenz die maximale Anzahl von VPN-Peers freigibt, werden bei Erreichen dieser maximalen Anzahl keine weiteren Benutzer auf das Gerät zugelassen.

Überprüfen Sie die Ausgabe von ***show vpn-sessiondb***, um die maximale Anzahl an VPN-Verbindungen zu überprüfen, die auf dem Gerät verfügbar sind:

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

Um die Gesamtzahl der von der Plattform unterstützten Benutzer zu bestimmen, sehen Sie sich das Datenblatt für Ihr Gerät unten an.

Wenn VPN-Benutzer keine Verbindung herstellen können und Sie überprüft haben, dass das Gerät nicht die maximale Anzahl an VPN-Benutzern erreicht, bitten wir Sie, zusätzliche Unterstützung vom TAC zu erhalten.

Datenblatt-Referenzen

In den folgenden Datenblättern wird sowohl die maximale Anzahl der von einer Plattform unterstützten VPN-Benutzer als auch der maximale VPN-Durchsatz anhand von Tests hervorgehoben. Es wird erwartet, dass IKEv2 und DTLS AnyConnect einen ähnlichen (aggregierten) Gesamtdurchsatz aufweisen wie der in jedem Abschnitt angegebene IPsec-VPN-Durchsatz.

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

Potenzielle Risikominderungen

Aktivieren von Split Tunneling

Standardmäßig implementieren Gruppenrichtlinien auf ASA und FTD Tunnelverbindungen. Dadurch wird der gesamte von RA-Clients über das VPN generierte Datenverkehr zur Verarbeitung durch das Headend gesendet. Da die Paketverschlüsselung und -entschlüsselung direkt mit der CPU-Auslastung zusammenhängt, ist es wichtig, sicherzustellen, dass nur der erforderliche Datenverkehr vom VPN-Headend verarbeitet wird, wie es die Sicherheitsrichtlinien des Unternehmens zulassen. Verwenden Sie eine Split-Tunnel-Richtlinie statt eines Full-Tunnels,

um das VPN-Headend vor unnötiger Belastung zu schützen.

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

Hinweis: Tunnel All implementiert eine unternehmensweite Parametersicherheitsrichtlinie, während Split-Tunneling zum Schutz des Internetdatenverkehrs des Benutzers auf das Client-Gerät angewiesen ist. Cisco stellt zusätzliche Sicherheitstools wie Umbrella zur Verfügung, um VPN-Benutzer bei Verwendung einer Split-Tunnel-Richtlinie zu schützen.

VPN-Lastenausgleich implementieren (nur ASA)

VPN-Lastenausgleich ist eine Funktion, die von ASA-Plattformen unterstützt wird und zwei oder mehr ASAs die gemeinsame Nutzung der VPN-Sitzungslast ermöglicht. Wenn beide Geräte 500 VPN-Peers unterstützen, unterstützen die Geräte durch die Konfiguration des VPN-Lastenausgleichs zwischen ihnen insgesamt 1.000 VPN-Peers. Diese Funktion kann verwendet werden, um die Anzahl der gleichzeitigen VPN-Benutzer zu erhöhen, die über die Möglichkeiten hinausgehen, die ein einzelnes Gerät bietet. Weitere Informationen zum VPN Load Balancing einschließlich des Load Balancing-Algorithmus finden Sie hier: VPN-Lastenausgleich

Konfigurationsoptimierung

Zusätzliche Dienste, die auf der Plattform aktiviert sind, erhöhen die Verarbeitungsleistung und die Last auf dem Gerät. Beispielsweise IPS, SSL-Entschlüsselung, NAT usw. Ziehen Sie in Betracht, das Gerät als VPN-Konzentrator zu konfigurieren, der nur VPN-Sitzungen beendet.

Tunnelprotokollauswahl

Standardmäßig werden Gruppenrichtlinien auf ASAs so konfiguriert, dass versucht wird, einen DTLS-Tunnel einzurichten. Wenn UDP 443-Datenverkehr zwischen dem VPN-Headend und dem AnyConnect-Client blockiert wird, wird automatisch ein Fallback auf TLS durchgeführt. Es wird empfohlen, DTLS oder IKEv2 zu verwenden, um die maximale VPN-Durchsatzleistung zu erhöhen. DTLS bietet aufgrund des geringeren Protokoll-Overhead eine bessere Leistung als TLS. IKEv2 bietet auch einen besseren Durchsatz als TLS. Darüber hinaus kann die Verwendung von AES-GCM-Chiffren die Leistung leicht verbessern. Diese Chiffren sind in TLS 1.2, DTLS 1.2 und IKEv2 verfügbar.

QoS pro Tunnel durchsetzen (nur FTD)

QoS kann implementiert werden, um die an AnyConnect-Benutzer in ausgehende Richtung gesendete Datenverkehrsmenge zu begrenzen. Auf diese Weise kann das VPN-Headend jedem Client mit Remote-Zugriff den angemessenen Anteil an der Ausgangsbandbreite zuweisen. Weitere Informationen hierzu finden Sie hier: FTD-Konfiguration

Implementierung von Crypto Engine Accelerator-BIOS (nur ASA)

Crypto Engine Accelerator Bias wird verwendet, um die Kryptokerne neu zuzuweisen, um ein Verschlüsselungsprotokoll gegenüber dem anderen (SSL oder IPsec) zu bevorzugen. Dies dient der Optimierung des AnyConnect-Durchsatzes, wenn die Mehrzahl der VPN-Tunnel entweder IPsec oder SSL verwendet. Die Implementierung dieses Befehls kann zu Serviceunterbrechungen führen, sodass ein Wartungsfenster erforderlich ist. Darüber hinaus kann die Leistungssteigerung

(AnyConnect-Durchsatz und CPU-Auslastung) je nach Datenverkehrsprofil variieren. Wenn das VPN-Headend nur SSL-Sitzungen oder nur IPsec-Sitzungen terminiert, kann dieser Befehl zur weiteren Optimierung des VPN-Headends in Betracht gezogen werden. Die Befehlsreferenz finden Sie hier: Befehlsreferenz

Um die aktuelle Crypto Core-Zuweisung zu überprüfen, führen Sie den Befehl ***show crypto accelerator Load Balancing aus***. Dieser Befehl zeigt nicht die gesamte Kryptoauslastung an, die das Gerät verarbeiten kann. Er zeigt an, dass jedem Kern das Verhältnis von SSL- oder IPSec-Datenverkehr zugewiesen wird. Um die ungefähre Auslastung auf dem Gerät zu finden, lesen Sie den Abschnitt oben zur **Hochleistungs-CPU-Auslastung** und vergleichen Sie den berechneten Wert mit dem Wert im Datenblatt für die Plattform.

Auf einer ASA-Plattform, die SSL VPN für den Remote-Zugriff hauptsächlich terminiert, wird empfohlen, die Verschlüsselungskernzuweisung so anzupassen, dass SSL mithilfe des Befehls ***crypto engine accelerator-bias ssl*** bevorzugt wird.

Das folgende Beispiel zeigt die Kernzuweisung auf einem ASA555 mit dem ***Befehl crypto engine accelerator-bias ssl,*** um AnyConnect SSL-Clients zu bevorzugen:

```
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%
[..]
```

Die aktive Sitzungsverteilung wird immer 100 % betragen, unabhängig von der aktuellen Verschlüsselungsauslastung der Plattform.

Hinweis: Der kryptografische Core-Ausgleich ist auf den folgenden Plattformen verfügbar: ASA 5585, 5580, 5545/555, 4110, 4120, 4140, 4150, SM-24, SM-36, SM-44 und ASASM.

Häufig gestellte Fragen

Lizenzierung

Frage: Warum kann ich die AnyConnect-Software nicht herunterladen?

Antwort: Sie müssen die AnyConnect Plus- oder Apex-Lizenz erwerben, um den AnyConnect Client herunterladen zu können. Danach sollten Sie ein Recht haben. Wenn Sie trotz des Erwerbs der AnyConnect Apex- oder Plus-Lizenz keinen Anspruch darauf haben, erstellen Sie ein Ticket bei Entitlement, um dieses Problem zu beheben.

Frage: Warum wird 99999 für die AnyConnect-Lizenz in meinem Smart-Lizenzkonto gekauft?

Antwort: Dies ist bei bestimmten AnyConnect-Lizenzen wie den unbefristeten oder nicht

bandbasierten AnyConnect Plus- oder Apex-Lizenzen zu erwarten.

Frage: Was bestimmt, wann "In Use" dekreiert?

Antwort: Dieser Wert nimmt ab, wenn ein Gerät, das die AnyConnect-Lizenz verwendet, registriert wird. Wenn Sie beispielsweise FMC registrieren und dann die AnyConnect Plus-Lizenz zu einem Gerät hinzufügen, wird der Wert für "In Use" (In Verwendung) für die AnyConnect Plus-Lizenz verringert. Dieser Wert **WIRD NICHT** aufgrund der aktuellen Benutzersitzungen herabgesetzt. Bei der Registrierung von ASAv-Geräten **wird** die Anzahl "In Use" (In Verwendung) NICHT verringert. Dies ist ein bekanntes kosmetisches Problem. Sie können nicht mehr Geräte registrieren als die Anzahl der autorisierten Benutzer, die gekauft haben.

Frage: Was bestimmt den gekauften Wert?

Antwort: Der Kaufwert richtet sich nach der Anzahl der autorisierten Benutzer, die zusammen mit der Lizenz erworben wurden. Beispielsweise beträgt die Anzahl der erworbenen AnyConnect Plus-Lizenzen für 25 Benutzer 25.

Frage: Wie aktiviere ich eine starke Verschlüsselung?

Antwort: Um eine starke Verschlüsselung zu aktivieren, müssen Sie beim Erstellen des Registrierungstokens das Kontrollkästchen "Exportgesteuerte Funktionen für die mit diesem Token registrierten Produkte zulassen" aktivieren.

Frage: Wie wandle ich von PAK zu Smart Licensing um?

Antwort: Hierfür sollte ein Ticket mit Lizenzierung geöffnet werden.

Frage: Wenn ich eine "X"-Benutzerlizenz habe, was geschieht, wenn "X+1" oder mehr Benutzer eine Verbindung zum Gerät herstellen?

Antwort: Mit der Apex- und Plus-Lizenz wird die volle VPN-Benutzerkapazität des Geräts entsperrt. Solange das Gerät die maximale VPN-Benutzergrenze nicht erreicht, akzeptiert das Gerät weiterhin Verbindungen. Auf dem Gerät gibt es keine Durchsetzung für VPN-Benutzersitzungen, und es ist ehrenbasiert. Es liegt in Ihrer Verantwortung, zusätzliche autorisierte Benutzerlizenzen zu erwerben, wenn die Nutzung der VPN-Sitzung für das Gerät erhöht werden muss. Um die maximale Anzahl von Benutzern zu überprüfen, die vom Gerät unterstützt werden, überprüfen Sie das Datenblatt für das Gerät auf der Cisco Website, oder führen Sie ***show vpn-sessiondb aus***, und prüfen Sie die "Geräte-Total VPN-Kapazität". Für ASAs können Sie auch die Befehle ***show version*** oder ***show vpn-sessiondb license-summary*** ausführen.

Frage: Wie kann ich überprüfen, ob die Lizenz auf meinem Gerät aktiviert ist?

Antwort: Bei FTDs können Sie die AnyConnect-Konfiguration nur dann bereitstellen, wenn die Lizenz aktiviert ist. Auf ASAs können Sie die ***show version*** oder ***show vpn-sessiondb license summary*** überprüfen, um zu überprüfen, wie viele Benutzer zugelassen sind. Ohne aktivierte Lizenz sind maximal 2 Benutzer möglich. Auf der ASA-ASA werden die oben genannten Befehle

keine Plus-/Apex-Lizenzinformationen anzeigen. Diese wird mit der Erweiterungsanfrage CSCuw74731 verfolgt.

Konfiguration

Frage: Welche ASA-Plattformen kann ich für den VPN-Lastenausgleich verwenden? Kann ich in einem VPN-Lastenausgleichs-Cluster verschiedene ASA-Hardwareplattformen oder verschiedene Softwareversionen verwenden?

A: Ja, ein VPN-Lastenausgleichs-Cluster kann aus verschiedenen physischen oder virtuellen ASA-Modellen bestehen, einschließlich der ASAv. Es wird jedoch generell empfohlen, dass der Cluster homogen ist. Wenn in einem VPN-Lastenausgleichs-Cluster verschiedene Softwareversionen verwendet werden, werden nur IPsec-Sitzungen unterstützt. Weitere Informationen finden Sie unter: Richtlinien und Einschränkungen für VPN-Lastenausgleich.

Frage: Wie konfiguriere ich Split-Tunneling? Können Sie verhindern, dass bestimmte Typen von Anwendungsdatenverkehr, wie Office 365, in einer Split-Tunnel-Konfiguration getunnelt werden?

Antwort: Konfigurationsbeispiele zu verschiedenen Anwendungsfällen finden Sie im Cisco Community-Artikel AnyConnect Split Tunneling. Sie können auch eine Kombination aus Split-Tunneling und dynamischem Split-Tunneling verwenden, um anwendungsbasiertes Split-Tunneling zu erreichen. Ein Beispiel zur Optimierung des AnyConnect-Split-Tunneling für Office 365 und WebEx finden Sie unter Optimieren von AnyConnect für Microsoft Office 365- und Cisco WebEx-Verbindungen.

Frage: Beim Herstellen einer Verbindung mit einem ASA-Headend mit AnyConnect wird der Fehler "Untrusted Certificate Warning" (Warnung bei nicht vertrauenswürdigem Zertifikat) angezeigt. Warum geschieht das?

Antwort: Dies liegt wahrscheinlich daran, dass das Headend ein selbstsigniertes Zertifikat verwendet. Um dies zu beheben, kann ein SSL-Zertifikat von einer Zertifizierungsstelle erworben und auf der Headend-ASA installiert werden. Ausführliche Informationen zu den Implementierungsschritten finden Sie unter: Konfigurieren der ASA: Installation und Verlängerung digitaler SSL-Zertifikate.

Frage: Werden Platzhalterzertifikate auf Cisco RAVPN-Headends unterstützt?

Antwort: Ja, Platzhalter und Zertifikate mit alternativen DNS-Namen (SANs) werden unterstützt.

Frage: Kann ein einzelnes Gerät sowohl Lastenausgleich als auch Failover verwenden?

Antwort: Active/Standby-Failover wird mit VPN-Lastenausgleich unterstützt. Bei Ausfall der aktiven Einheit übernimmt das Standby-Gerät sofort und ohne Beeinträchtigung des VPN-Tunnels. Der VPN-Lastenausgleich wird bei einer Aktiv/Aktiv-Failover-Konfiguration nicht unterstützt.

Überwachung

F: Welche SNMP MIB kann ich verwenden, um die ASA-CPU-Nutzung zu überwachen?

A: Die CISCO-PROCESS-MIB kann zur Überwachung der ASA-CPU-Auslastung verwendet werden. Eine vollständige Liste der unterstützten MIBs finden Sie unter: Adaptive Security Appliance MIB Support List. Außerdem kann der folgende Befehl ausgegeben werden, um eine

Liste der unterstützten SNMP MIBs und OIDs für eine bestimmte ASA abzurufen: ***show snmp-server oidlist.***

Frage: Wie kann ich die Anzahl der Benutzer überwachen, die derzeit mit einem VPN-Headend verbunden sind?

Antwort: Verwenden Sie ***show vpn-sessiondb*** von der CLI, um die aktuelle Anzahl der Benutzer auf einer ASA oder FTD oder SNMP MIB zu überprüfen.

CISCO-REMOTE-ACCESS-MONITOR-MIB.

Fehlerbehebung

Frage: Einige unserer AnyConnect VPN-Benutzer scheinen häufig getrennt zu sein. Wie kann ich derartige Probleme beheben:

Antwort: Informationen zur Fehlerbehebung bei VPN-Trends und anderen gängigen AnyConnect-Problemen finden Sie im Leitfaden zur Fehlerbehebung bei AnyConnect VPN-Clients - Häufige Probleme.

Frage: Wenn eine bestimmte Anzahl von Benutzern eine Verbindung zum VPN-Headend herstellt, können keine Benutzer mehr eine Verbindung herstellen. Die Lizenz wird auf dem Gerät aktiviert, und ***show vpn-sessiondb*** zeigt, dass das Gerät mehr Benutzer bearbeiten kann. Was könnte das Problem sein?

Antwort: Überprüfen Sie den lokalen VPN-Adresspool für diese Benutzer, um sicherzustellen, dass die Anzahl der Benutzer, die eine Verbindung herstellen, die Anzahl der verfügbaren Adressen nicht überschreitet. Mit dem Befehl ***show ip local pool [pool-name]*** können Sie überprüfen. Ein weiterer potenzieller Grund für ältere Plattformen ist, dass der ***Befehl vpn-sessiondb max-anyconnect-Premium-or-essentials-limit*** auf einen niedrigen Wert festgelegt wird. Sie können dies mit dem Befehl ***show run all vpn-sessiondb*** überprüfen. In diesem Fall kann der Wert erhöht oder der Befehl entfernt werden, um diesen Grenzwert zu verhindern.

Weitere Hilfe erhalten

Für weitere Unterstützung wenden Sie sich bitte an das TAC. Ein gültiger Support-Vertrag ist erforderlich: Weltweite Kontaktpersonen für den Cisco Support

Sie können hier auch die Cisco VPN Community besuchen.

Darüber hinaus können Sie sich auch die TAC Security Show Podcasts ansehen.

Referenzen

Im Folgenden finden Sie weitere Links zu anderen Ressourcen, die für AnyConnect-Bereitstellungen und die allgemeine Behandlung von Problemen im Zusammenhang mit COVOD-19 nützlich sind.

- Cisco Security reagiert auf wachsende Anzahl an Remote-Mitarbeitern - Cisco Community
- AnyConnect-Bestellanleitung

- Häufig gestellte Fragen zu AnyConnect-Lizenzen
- Häufig gestellte Fragen zu AnyConnect VPN, ASA und FTD für sichere Remote-Mitarbeiter