COVID-19 준비를 위한 AnyConnect 구현 및 성능/확장 참조

목차

소개

세계 각국에서 COVID-19 전염병 확산을 막기 위해 원격 근무 정책을 시행하는 기업이 늘고 있다.그 결과, 직원들이 내부 회사 리소스에 액세스할 수 있도록 하는 RAVPN(Remote Access VPN)에 대한 수요가 증가하고 있습니다.이 문서에서는 네트워크 내에서 RAVPN을 신속하게 설정하거나 성능 또는 확장 관련 문제를 파악하고 해결하기 위한 컨피그레이션 가이드에 대한 참조를 제공합니다.

구현

다음 섹션에서는 RAVPN에 대한 인증서 인증 요구 사항 때문에 인증서 구축이 Cisco 원격 액세스에 필수적인 요소이기 때문에 다양한 Cisco 플랫폼에 AnyConnect 원격 액세스 컨피그레이션 및 구축을 자세히 설명합니다.

라이센싱

디바이스에서 RAVPN 연결을 종료하려면 라이센스가 필요합니다.ASA 플랫폼은 라이센스 없이 2개의 VPN 피어만 지원합니다.FTD는 라이센싱 없이 AnyConnect 컨피그레이션을 디바이스에 구축할 수 없습니다.COVID-19 Outbreak로 인해 Cisco는 사용자가 Cisco 장치에 RAVPN을 구현할 수 있도록 무료 임시 라이센스를 제공합니다.자세한 내용은 다음을 참조하십시오.긴급 COVID-19 AnyConnect 라이센스 받기

AnyConnect 초기 컨피그레이션 빠른 시작 가이드

가장 일반적인 컨피그레이션으로 AnyConnect Remote Access를 구현하려면 다음 빠른 시작 가이드를 따르십시오.

- ASA에서 스플릿 터널링을 사용하여 AnyConnect Secure Mobility Client 구성
- FTD의 AnyConnect 원격 액세스 VPN 컨피그레이션
- FMC에서 관리하는 FTD용 초기 AnyConnect 컨피그레이션(비디오)

전체 제품 구성 가이드는 아래를 참조하십시오.

전체 구성 가이드

ASA:

- ASA ASDM 컨피그레이션
- ASA CLI 컨피그레이션

FTD:

- FDM에서 관리하는 FTD
- FMC에서 관리하는 FTD

IOS/IOS-XE:

- SSLVPN용 IOS 라우터
- SSL VPN용 IOS-XE 라우터(CSR에만 해당)
- IKEv2 VPN용 IOS/IOS-XE 라우터

인증서 설치 가이드

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

성능 및 확장 문제

RAVPN 사용이 크게 증가함에 따라 AnyConnect 사용자는 성능 문제를 경험할 수 있습니다.이러한 문제를 식별하고 이를 해결하기 위한 완화 전략을 결정하는 방법은 다음을 참조하십시오.

문제 증상 및 식별

높은 CPU 사용률

CPU 사용률은 VPN 사용자의 성능에 직접적인 영향을 미칩니다.디바이스에서 처리하는 암호화 또는 암호 해독된 트래픽이 증가하면 CPU 사용률이 증가합니다.플랫폼이 처리할 수 있는 최대 VPN 처리량에 도달할 때 디바이스에서 높은 CPU를 경험할 수 있습니다.CPU 사용률이 높은 이유는 장치가 초과 가입되어 있거나 다른 문제로 인한 것인지 확인해야 합니다.

디바이스에서 높은 CPU를 경험하는지 확인하려면 다음 명령을 실행하는 것이 좋습니다.

show process cpu-usage non-zero

CPU 사용량 표시

출력 예:

```
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%
```

위의 예에서는 DATAPATH-0 및 DATAPATH-1이 총 CPU 사용률의 87.7%를 소비하고 있는 것으로 나타났습니다.이 경우 ASA는 초과 가입되어 있으며, 이 증상에 많은 양의 암호화 및 암호 해독된 트래픽이 발생했는지 확인해야 합니다.그런 다음 해당 플랫폼의 데이터시트에 기록된 VPN 처리량 값에 대해 벤치마킹할 수 있습니다.

초당 디바이스를 통과하는 총 VPN 트래픽의 양을 계산하기 위해 show crypto accelerator statistics 명령에 있는 ***Global Statistics*** 섹션에 있는 ***Input bytes*** 및 ***Output bytes***를 추가할 수 있습니다.ASA 또는 FTD에서 clear crypto accelerator ***statistics*** 명령을 사용하여 ***show crypto accelerator statistics 출력을 지웁니다***.특정 시간을 기다린 다음 명령을 실행합니다.다음***과*** 같이 ***암호화 가속기 통계***를 ***표시합니다***.

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

특정 간격으로 몇 개의 스냅샷을 생성하고 초당 비트(bps)로 변환할 수 있는 평균 처리량을 바이트 단위로 얻습니다. 이 작업을 수행하는 공식은 다음과 같습니다.

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

이전 예에서 clear crypto accelerator ***statistics*** 명령은 0초에 실행됩니다.10초 후에 ***show crypto accelerator statistics*** 명령이 실행되어 10초 간격 동안 총 바이트를 가져왔습니다.그런 다음 이 값은 10초 간격으로 처리된 217Mbps의 bps를 계산하는 데 사용됩니다.보다 정확한 평균을 얻으려면 여러 스냅샷이 필요할 수 있습니다.

이러한 값은 암호화된/해독된 모든 트래픽(HTTPS, SSL, IPsec, SSH 등)에 대해 증가합니다. 이 값을 사용하여 평균 VPN 처리량을 확인하고 데이터시트와 비교할 수 있습니다.평균 처리량이 플랫폼의 데이터시트에서 볼 수 있는 것과 거의 같은 정도라면, 암호화된 트래픽과 해독된 트래픽이 디바이스를 오버서브스크립션하고 있습니다.

또한 카운터가 VPN 트래픽에 대해 증가하지 않으므로 이 방법을 사용하여 Firepower 2100 플랫폼의 VPN 처리량을 확인할 수 없습니다.이는 CSCvt46830에서 추적됩니다. .

최대 VPN 연결 수

최대 VPN 연결 수에 도달하면 사용자가 연결할 수 없는 중단 기간이 발생할 수 있습니다 .AnyConnect Plus 또는 Apex 라이센스를 활성화하면 최대 VPN 피어 수의 잠금이 해제되지만, 최대 수에 도달하면 디바이스에 추가 사용자가 허용되지 않습니다.

디바이스에서 사용 가능한 최대 VPN 연결 수를 확인하려면 ***show vpn-sessiondb***의 출력을 ***확인합니다***.

```
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
```

플랫폼에서 지원하는 총 사용자 수를 확인하려면 아래 위치의 장치에 대한 데이터시트를 확인하십시오.

VPN 사용자가 연결할 수 없고 장치가 최대 VPN 사용자 수에 도달하지 않고 있음을 확인한 경우 TAC에서 추가 지원을 요청하십시오.

데이터시트 참조

다음 데이터시트에서는 플랫폼에서 지원하는 최대 VPN 사용자 수와 테스트를 기반으로 한 최대 VPN 처리량을 모두 보여줍니다.IKEv2 및 DTLS AnyConnect는 각 섹션에 나열된 IPsec VPN 처리량과 비슷한 총(집계) 처리량을 가질 것으로 예상됩니다.

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

잠재적 완화

스플릿 터널링 활성화

기본적으로 ASA 및 FTD의 그룹 정책은 터널all을 구현합니다.그러면 헤드엔드에서 처리할 VPN을 통해 RA 클라이언트에서 생성된 모든 트래픽이 전송됩니다.패킷 암호화 및 암호 해독은 CPU 사용률과 직접 관련되어 있으므로 회사의 보안 정책에서 허용하는 대로 VPN 헤드엔드에서 필요한 트래픽만 처리되도록 하는 것이 중요합니다.전체 터널이 아닌 스플릿 터널 정책을 사용하여 불필요한 로드에서 VPN 헤드엔드를 저장하는 것을 고려해 보십시오.

- ASA 스플릿 터널링 가이드
- FTD(FMC) 스플릿 터널링 가이드

참고:Tunnel All은 회사 차원의 매개 변수 보안 정책을 구현하는 반면 스플릿 터널링은 사용자 인터넷 트래픽을 보호하기 위해 클라이언트 디바이스를 사용합니다.Cisco는 스플릿 터널 정책을 사용할 때 VPN 사용자를 보호하기 위해 Umbrella와 같은 추가 보안 툴을 제공합니다.

VPN 로드 밸런싱 구현(ASA에만 해당)

VPN 로드 밸런싱은 ASA 플랫폼에서 지원되는 기능으로, 둘 이상의 ASA에서 VPN 세션 로드를 공유할 수 있습니다.두 디바이스 모두 500개의 VPN 피어를 지원하는 경우, VPN 로드 밸런싱을 구성하면 디바이스 간에 총 1,000개의 VPN 피어가 지원됩니다.이 기능을 사용하면 단일 디바이스에서 처리할 수 있는 범위를 넘어 동시 VPN 사용자의 수를 늘릴 수 있습니다.로드 밸런싱 알고리즘을 포함한 VPN 로드 밸런싱에 대한 자세한 내용은 다음 사이트를 참조하십시오.VPN 로드 밸런싱

구성 최적화

플랫폼에서 활성화된 추가 서비스를 통해 디바이스의 처리 및 로드 양이 증가합니다.예: IPS, SSL

암호 해독, NAT 등디바이스를 VPN 세션만 종료하는 VPN Concentrator로 구성하는 것이 좋습니다.

터널 프로토콜 선택

기본적으로 ASA의 그룹 정책은 DTLS 터널 설정을 시도하도록 구성됩니다.VPN 헤드엔드와 AnyConnect 클라이언트 간에 UDP 443 트래픽이 차단되면 자동으로 TLS로 대체됩니다.DTLS 또는 IKEv2를 사용하여 최대 VPN 처리량 성능을 높이는 것이 좋습니다.DTLS는 프로토콜 오버헤드를 줄여 TLS보다 우수한 성능을 제공합니다.또한 IKEv2는 TLS보다 처리량이 좋습니다.또한 AES-GCM 암호를 사용하면 성능이 약간 향상될 수 있습니다.이러한 암호는 TLS 1.2, DTLS 1.2 및 IKEv2에서 사용할 수 있습니다.

터널당 QoS 적용(FTD에만 해당)

QoS를 구현하여 AnyConnect 사용자에게 보내는 트래픽의 양을 아웃바운드 방향으로 제한할 수 있습니다.이를 통해 VPN 헤드엔드는 각 원격 액세스 클라이언트가 이그레스 대역폭의 균등한 점유율을 얻을 수 있도록 할 수 있습니다.이에 대한 자세한 내용은 여기를 참조하십시오.FTD 컨피그레이션

Crypto Engine Accelerator Bias 구현(ASA에만 해당)

Crypto Engine Accelerator Bias는 암호화 코어를 재할당하여 다른 암호화 프로토콜(SSL 또는 IPsec)을 우선하는 데 사용됩니다. 이는 대부분의 VPN 터널에서 IPsec 또는 SSL을 사용하는 경우 AnyConnect 처리량을 최적화하는 데 사용됩니다.이 명령을 구현하면 서비스가 중단되므로 유지 보수 기간이 필요합니다.또한 성능(AnyConnect 처리량 및 CPU 사용률)은 트래픽 프로필에 따라 달라질 수 있습니다.VPN 헤드엔드가 SSL 세션만 종료하거나 IPsec 세션만 종료하는 경우 VPN 헤드엔드를 추가로 최적화하기 위해 이 명령을 고려할 수 있습니다.명령 참조는 여기에서 찾을 수 있습니다.명령 참조

현재 암호화 코어 할당을 검토하려면 show crypto accelerator load-balance 명령을 ***실행합니다***.이 명령은 디바이스가 처리할 수 있는 총 암호화 사용률을 표시하지 않습니다. 즉, 각 코어에 SSL 또는 ipsec 트래픽이 할당되고 있음을 나타냅니다.디바이스에서 대략적인 사용률을 찾으려면 **CPU 사용률이 높은** 위 섹션을 참조하고 계산된 값을 플랫폼의 데이터시트와 비교합니다.

대부분 원격 액세스 SSLVPN을 종료하는 ASA 플랫폼에서 crypto core 할당은 crypto ***engine accelerator-bias ssl*** 명령을 사용하여 SSL을 지원하도록 조정하는 것이 좋습니다.

다음 예는 AnyConnect SSL 클라이언트를 선호하는 crypto ***engine accelerator-bias ssl*** 명령을 사용하여 ASA5555에 대한 코어 할당을 보여줍니다.

```
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%
[..]
```

플랫폼의 현재 암호화 사용률에 관계없이 활성 세션 배포는 항상 100%입니다.

참고:암호화 코어 리밸런싱은 다음 플랫폼에서 사용할 수 있습니다.ASA 5585, 5580, 5545/555, 4110, 4120, 4140, 4150, SM-24, SM-36, SM-44 및 ASASM.

FAQ

라이센싱

Q:AnyConnect 소프트웨어를 다운로드할 수 없는 이유는 무엇입니까?

A:AnyConnect 클라이언트를 다운로드하려면 AnyConnect Plus 또는 Apex 라이센스를 구매해야 합니다.그 후에는 자격이 있어야 합니다.AnyConnect Apex 또는 Plus 라이센스를 구매하더라도 자격이 없는 경우, Entitlement로 케이스를 열어 이 문제를 해결하십시오.

Q:Smart Licensing 어카운트에서 AnyConnect 라이센스로 9999를 구매한 이유는 무엇입니까?

A:이는 AnyConnect Plus Persistent 또는 비 Branded AnyConnect Plus 또는 Apex 라이센스와 같은 특정 AnyConnect 라이센스와 함께 필요합니다.

Q:"사용 중"이 감소되는 시기를 결정하는 요소는 무엇입니까?

A:이 값은 AnyConnect 라이센스를 사용하는 디바이스가 등록될 때마다 감소합니다.예를 들어, FMC를 등록한 다음 AnyConnect Plus 라이센스를 디바이스에 추가하면 AnyConnect Plus 라이센스의 사용 중 값이 감소됩니다.이 값**은** 현재 사용자 세션을 기준으로 감소되지 **않습니다**.ASAv 디바이스를 **등록해도** "사용 중" 수는 감소되지 않습니다.이것은 알려진 화장품 문제입니다.구매한 인증된 사용자 수보다 많은 장치를 등록할 수 없습니다.

Q:구매 가치를 결정하는 요소는 무엇입니까?

A:구매 값은 라이센스와 함께 구매한 승인된 사용자 수에 따라 결정됩니다.예를 들어 사용자 25명 AnyConnect Plus 라이센스에는 25개의 구매 횟수가 포함됩니다.

Q:강력한 암호화를 사용하려면 어떻게 해야 합니까?

A:강력한 암호화를 활성화하려면 등록 토큰을 만들 때 "이 토큰에 등록된 제품에 대해 내보내기 제어 기능 허용" 확인란을 선택해야 합니다.

Q:PAK에서 스마트 라이센싱으로 전환하려면 어떻게 해야 합니까?

A:케이스는 Licensing(라이센싱)으로 열어야 합니다.

Q:"X" 사용자 라이센스가 있는 경우, "X+1" 이상의 사용자가 장치에 연결하면 어떻게 됩니까?

A:Apex 및 Plus 라이센스를 사용하면 디바이스의 전체 VPN 사용자 용량이 잠금 해제됩니다.디바이

스가 최대 vpn 사용자 제한에 도달하지 않으면 디바이스가 연결을 계속 수락합니다.VPN 사용자 세션에 대해서는 디바이스에 대한 시행이 없으며 이를 기반으로 합니다.디바이스에 대한 vpn 세션 사용량을 늘려야 하는 경우 추가 인증된 사용자 라이센스를 구매해야 합니다.디바이스에서 지원되는 최대 사용자 수를 확인하려면 Cisco 웹 사이트에서 디바이스의 데이터 시트를 확인하거나 show vpn-sessiondb를 실행하여 "Device Total VPN Capacity"를 확인하십시오.ASA의 경우 ***show version*** 또는 ***show vpn-sessiondb license-summary*** 명령을 실행할 수도 있습니다.

Q:내 디바이스에서 라이센스가 활성화되었는지 확인하려면 어떻게 해야 합니까?

A:FTD에서는 라이센스가 활성화되지 않으면 AnyConnect 컨피그레이션을 구축할 수 없습니다.ASA에서 ***show version*** 또는 ***show vpn-sessiondb license-summary***를 확인하여 허용되는 사용자 수를 검사할 수 있습니다.활성화된 라이센스가 없으면 최대 사용자 2명이 됩니다.ASA에서 위에서 언급한 명령은 Plus/Apex 라이센스 정보를 표시하지 않습니다.이는 개선 요청 CSCuw74731을 사용하여 추적됩니다.

구성

Q: VPN 로드 밸런싱에 사용할 수 있는 ASA 플랫폼은 무엇입니까?VPN 로드 밸런싱 클러스터에서 서로 다른 ASA 하드웨어 플랫폼 또는 다른 소프트웨어 버전을 사용할 수 있습니까?

A: 예 VPN 로드 밸런싱 클러스터는 ASAv를 비롯한 여러 물리적 또는 가상 ASA 모델로 구성될 수 있습니다.그러나 클러스터는 일반적으로 균일화되어야 합니다.vpn 로드 밸런싱 클러스터에서 서로 다른 소프트웨어 버전을 사용하는 경우 IPsec 세션만 지원됩니다.자세한 내용은 VPN 로드 밸런싱 지침 및 제한을 참조하십시오.

Q: 스플릿 터널링을 구성하려면 어떻게 해야 합니까?또한 Office 365와 같은 특정 유형의 애플리케이션 트래픽이 스플릿 터널 구성에서 터널링되지 않도록 제외할 수 있습니까?

A:다양한 활용 사례의 컨피그레이션 예는 Cisco 커뮤니티 문서 AnyConnect Split Tunneling을 참조하십시오.또한 스플릿 터널링과 동적 스플릿 터널링을 함께 사용하여 애플리케이션 기반 스플릿 터널링을 달성할 수 있습니다.Office 365 및 WebEx용 AnyConnect 스플릿 터널링을 최적화하는 방법에 대한 예는 Microsoft Office365 및 Cisco Webex 연결을 위한 AnyConnect 최적화 방법을 참조하십시오.

Q:AnyConnect를 사용하여 ASA 헤드엔드에 연결할 때 "신뢰할 수 없는 인증서 경고" 오류가 표시됩니다.왜 이런 일이 일어나는가?

A:헤드엔드에서 자체 서명 인증서를 사용하기 때문일 수 있습니다.이 문제를 해결하려면 SSL 인증서를 인증 기관에서 구매하고 헤드엔드 ASA에 설치할 수 있습니다.자세한 구현 단계는 다음을 참조하십시오. ASA 구성:SSL 디지털 인증서 설치 및 갱신.

Q:와일드카드 인증서는 Cisco RAVPN 헤드엔드에서 지원됩니까?

A:예. 와일드카드 및 DNS 주체 대체 이름(SAN)이 있는 인증서가 지원됩니다.

Q: 단일 디바이스에서 로드 밸런싱과 장애 조치를 모두 사용할 수 있습니까?

A:액티브/스탠바이 장애 조치는 VPN 로드 밸런싱에서 지원됩니다.액티브 유닛에 장애가 발생할 경우 스탠바이 디바이스는 VPN 터널에 영향을 주지 않고 즉시 인계됩니다.VPN 로드 밸런싱은 액티브/액티브 장애 조치 컨피그레이션에서 지원되지 않습니다.

모니터링

Q: ASA CPU 사용량을 모니터링하는 데 사용할 수 있는 SNMP MIB는 무엇입니까?

A: CISCO-PROCESS-MIB를 사용하여 ASA CPU 사용량을 모니터링할 수 있습니다.지원되는 MIB의 전체 목록은 Adaptive Security Appliance MIB 지원 목록을 참조하십시오.또한 특정 ASA에 대해 지원되는 SNMP MIB 및 OID 목록을 가져오려면 다음 명령을 실행할 수 있습니다.***show snmp-server oidlist.***

Q:현재 VPN 헤드엔드에 연결된 사용자 수를 모니터링하려면 어떻게 해야 합니까?

A:CLI에서 show vpn-sessiondb를 사용하여 ASA, FTD 또는 SNMP MIB의 현재 사용자 수를 확인합니다.

CISCO-REMOTE-ACCESS-MONITOR-MIB.

문제 해결

Q:AnyConnect VPN 사용자 중 일부는 자주 연결을 끊습니다.이러한 문제를 어떻게 해결합니까?

A:VPN 연결 끊기 및 기타 일반적인 AnyConnect 문제의 트러블슈팅은 AnyConnect VPN 클라이언트 트러블슈팅 가이드 - 일반적인 문제를 참조하십시오.

Q:특정 양의 사용자가 VPN 헤드엔드에 연결되면 더 이상 사용자가 연결할 수 없습니다.디바이스에서 라이센스가 활성화되고 ***show vpn-sessiondb는*** 디바이스에서 더 많은 사용자를 처리할 수 있음을 보여줍니다.무엇이 문제일까요?

A:해당 사용자의 VPN 로컬 주소 풀을 확인하여 연결하는 사용자 수가 사용 가능한 주소 양을 초과하지 않는지 확인합니다.***show ip local pool [pool-name]*** 명령으로 확인할 수 있습니다.이전 플랫폼에서 발생할 수 있는 또 다른 원인은 ***vpn-sessiondb max-anyconnect-premium-or-essentials-limit*** 명령***이*** 낮은 값으로 설정되었기 때문입니다.show run all vpn***-sessiondb*** 명령을 사용하여 이를 확인할 수 ***있습니다***.이 경우 값을 늘리거나 명령을 제거하여 이 제한을 방지할 수 있습니다.

추가 도움말 보기

추가 지원이 필요한 경우 TAC에 문의하십시오.유효한 지원 계약이 필요합니다.Cisco 전 세계 지원 문의처

여기서 Cisco VPN 커뮤니티를 방문할 수도 있습니다.

또한 TAC Security Show PodCast를 확인할 수 있습니다.

참조

AnyConnect 구축 및 COVOD-19 관련 문제 처리에 유용한 기타 리소스에 대한 추가 링크는 일반적으로 아래 링크를 참조하십시오.

- 원격 근무자 증가에 대응한 Cisco 보안 - Cisco 커뮤니티
- AnyConnect 주문 가이드
- AnyConnect 라이센싱 FAQ

- 보안 원격 근무자를 위한 AnyConnect VPN, ASA 및 FTD FAQ