Konfigurieren von SSL AnyConnect mit lokaler Authentifizierung auf von FMC verwaltetem FTD

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurieren Konfigurationen Schritt 1: Lizenzierung überprüfen Schritt 2: AnyConnect-Paket auf FMC hochladen Schritt 3: Erstellen eines selbstsignierten Zertifikats Schritt 4: Lokalen Bereich auf FMC erstellen Schritt 5: Konfigurieren von SSL AnyConnect Überprüfung Fehlerbehebung

Einleitung

In diesem Dokument wird beschrieben, wie Cisco AnyConnect mit lokaler Authentifizierung auf einer Cisco FirePOWER Threat Defense (FTD) konfiguriert wird, die vom Cisco FirePOWER Management Center (FMC) verwaltet wird. Im Beispiel unten wird Secure Sockets Layer (SSL) zum Erstellen eines Virtual Private Network (VPN) zwischen FTD und einem Windows 10-Client verwendet.

Mitarbeiter: Daniel Perez Vertti Vazquez, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- SSL AnyConnect-Konfiguration über FMC
- Konfiguration von FirePOWER-Objekten über FMC
- SSL-Zertifikate für FirePOWER

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco FTD Version 7.0.0 (Build 94)
- Cisco FMC Version 7.0.0 (Build 94)
- Cisco AnyConnect Secure Mobility Client 4.10.01075

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Ab Version 7.0.0 unterstützt von FMC verwaltetes FTD die lokale Authentifizierung für AnyConnect-Clients. Dies kann entweder als primäre Authentifizierungsmethode oder als Fallback definiert werden, falls die primäre Methode fehlschlägt. In diesem Beispiel wird die lokale Authentifizierung als primäre Authentifizierung konfiguriert.

Vor dieser Softwareversion war die lokale AnyConnect-Authentifizierung auf FTD nur auf dem Cisco FirePOWER Device Manager (FDM) verfügbar.

Konfigurieren

Konfigurationen

Schritt 1: Lizenzierung überprüfen

Bevor AnyConnect konfiguriert werden kann, muss das FMC registriert und mit dem Smart Licensing Portal kompatibel sein. AnyConnect kann nicht bereitgestellt werden, wenn FTD keine gültige Plus-, Apex- oder VPN Only-Lizenz besitzt.

Navigieren Sie zu System > Licenses > Smart Licenses (System > Lizenzen > Smart Licenses), um zu überprüfen, ob das FMC registriert ist und dem Smart Licensing Portal entspricht.

| Overview Analysis Policie | es Devices Objects AMP Intellig | gence | | | | | | 🔍 De | ploy System | Help 🔻 d | perezve |
|-----------------------------|--|-----------------|----------------------|-----------------|---------|---------|---------------------------|-----------|-------------|--------------|---------|
| | | Configuration | Users Doma | ins Integration | SecureX | Updates | Licenses • Smart Licenses | Logging • | Health • | Monitoring • | Tools |
| Smart License Status | | <u>Cisco Sn</u> | nart Software Manage | £ 😐 🔁 | | | | | | | |
| Usage Authorization: | Authorized (Last Synchronized On Sep 0 | 04 2021) | | | | | | | | | |
| Product Registration: | Registered (Last Renewed On Sep 04 20 | 021) | | | | | | | | | |
| Assigned Virtual Account: | SEC TAC | | | | | | | | | | |
| Export-Controlled Features: | Enabled | | | | | | | | | | |
| Cisco Success Network: | Enabled () | | | | | | | | | | |
| Cisco Support Diagnostics: | Disabled 🕕 | | | | | | | | | | |
| | | | | | | | | | | | |

Scrollen Sie auf derselben Seite unten im **Smart Licenses-**Diagramm nach unten, um die verschiedenen verfügbaren AnyConnect-Lizenzen und die jeweils abonnierten Geräte anzuzeigen. Validieren Sie, ob die jeweilige FTD in einer dieser Kategorien registriert ist.

| Smart Licenses | | Filter Devices | × Edit | Performance Tier Edit License |
|--|----------------|---|---------------------------------|--|
| License Type/Device Name | License Status | Device Type | Domain | Group |
| Firepower Management Center Virtual (2) | ٢ | | | |
| ▷ 💋 Base (2) | 0 | | | |
| ▷ 💋 Malware (2) | 0 | | | |
| > 💋 Threat (2) | 0 | | | |
| > 💋 URL Filtering (2) | 0 | | | |
| a 💋 AnyConnect Apex (2) | 0 | | | |
| ftdv-dperezve 192.168.13.8 - Cisco Firepower Threat Defense for VMWare - v6.7.0 | ٥ | Cisco Firepower Threat Defense for VMWare | Global | N/A |
| ftdvha-dperezve (Performance Tier: FTDv50 - Tiered) 192.168.13.9 - Cisco Firepower Threat Defense for VMware - v7.0.0 | 0 | Cisco Firepower Threat Defense for VMware | Global | N/A |
| AnyConnect Plus (0) | | | | |
| AnyConnect VPN Only (0) | | | | |
| Note: Container Instances of same blade share feature licenses | | | Activate Win Go to System in | dows Control Panel to activate Windows. |
| st login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2 | | | | |

Schritt 2: AnyConnect-Paket auf FMC hochladen

Laden Sie das AnyConnect Headend-Bereitstellungspaket für Windows von cisco.com herunter.

| Application Programming Interface [API] (Windows) anyconnect-win-4.10.01075-vpnapi.zip Advisories | 21-May-2021 | 141.72 MB | <u>+</u> \; |
|---|-------------|-----------|-------------|
| AnyConnect Headend Deployment Package (Windows) anyconnect-win-4.10.01075-webdeploy-k9.pkg Advisories | 21-May-2021 | 77.81 MB | <u>+</u> \; |
| AnyConnect Pre-Deployment Package (Windows 10 ARM64) - includes individual MSI files anyconnect-win-arm64-4.10.01075-predeploy-k9.zip Advisories | 21-May-2021 | 34.78 MB | <u>+</u> ₩ |
| AnyConnect Headend Deployment Package (Windows 10 ARM64) anyconnect-win-arm64-4.10.01075-webdeploy-k9.pkg Advisories | 21-May-2021 | 44.76 MB | <u>+</u> \; |
| Profile Editor (Windows) tools-anyconnect-win-4.10.01075-profileeditor-k9.msi Advisories 📑 | 21-May-2021 | 10.90 MB | ±₩ |
| AnyConnect Installer Transforms (Windows) tools-anyconnect-win-4.10.01075-transforms.zip Advisories | 21-May-2021 | 0.05 MB | ±₩ |

Um das AnyConnect-Image hochzuladen, navigieren Sie zu **Objects > Object Management** und wählen Sie **AnyConnect File** unter der **VPN-**Kategorie im Inhaltsverzeichnis aus.



Wählen Sie die Schaltfläche AnyConnect-Datei hinzufügen aus. Weisen Sie im Fenster AnyConnect-Datei hinzufügen einen Namen für das Objekt zu, und wählen Sie dann Durchsuchen aus. um das AnyConnect-Paket auszuwählen und schließlich AnyConnect Client Image im Dropdown-Menü als Dateityp auszuwählen.

| Overview Analysis Polici | es Devices Objects AMP Intelliger | ce | | . I Deploy System Help ▼ dperezve ▼ |
|---|---|--|---------------------|---|
| Object Management Intro | usion Rules | | | |
| AnyConnect File File objects represent files used in o | configurations, typically for remote access VPN policies. | They can contain AnyConnect Client Profile and AnyConnect | Client Image files. | Add AnyConnect File |
| IPv6 Prefix List | Name | | Value | Туре |
| Ø Route Map | | | | |
| - Security Intelligence | | No re | cords to display | |
| DNS Lists and Feeds | | Add AnyConnect File | ? × | |
| Network Lists and Feeds | | | | |
| URL Lists and Feeds | | Name:* AnyConnect Win 4.10 | | |
| Sinkhole | | induced in the second s | | |
| Ga SLA Monitor | | File Name: anyconnect-win-4.10.01075-web | deploy-k9.pl Browse | |
| Time Range | | | | |
| Time Zone | | File Type:* AnyConnect Client Image | ~ | |
| General zone | | Description | | |
| S Variable Set | | Description: | | |
| VIAN Tao | | | | |
| A BD VPN | | | | |
| M AnyConnect File | | | Save Cancel | |
| R Certificate Map | | | | |
| Custom Attribute | | | | |
| Group Policy | | | | |
| IKEv1 IPsec Proposal | | | | |
| S IKEV1 Policy | | | | |
| IKEv2 IPsec Proposal | | | | |
| B IKEv2 Policy | | | | All No data to display 5 🔣 🔍 Page 🔟 of 1 🗦 🗏 🖒 |
| | | | | Go to System in Control Panel to activate Windows |
| Last login on Friday, 2021-09-03 at 1 | | | | - iliulu cisco |

Wählen Sie die Schaltfläche Speichern, das Objekt muss der Objektliste hinzugefügt werden.

| Overview Analysis Policies Devices Objects AMP Intelligence | | . Deploy System Help ▼ | dperezve v |
|--|--|---|------------|
| Object Management Intrusion Rules | | | |
| | | | |
| AnyConnect File | | Add AnyConnect File | |
| File objects represent files used in configurations, typically for remote access VPN policies. They can contain AnyConnect Client Profile and AnyConnect Client Image files. | | | |
| The Policy List | | | |
| A Name | Value | Туре | |
| AnyConnect_Win_4.10 | anyconnect-win-4.10.01075-webdeploy-k9.pkg | AnyConnect Client Image | 2/8 |
| The Ded Deelsy List | | | |
| Prof Prefix List | | | |
| (I) Route Map | | | |
| A REF Security Intelligence | | | |
| DNS Lists and Feeds | | | |
| W Network Lists and Feeds | | | |
| URL Lists and Feeds | | | |
| Sinkhole | | | |
| c SLA Monitor | | | |
| and Time Range | | | |
| @ Time Zone | | | |
| nunel zone | | | |
| I RL | | | |
| \$ Variable Set | | | |
| S VLAN Tag | | | |
| - BIVPN | | | |
| ManyConnect File | | | |
| Certificate Map | | | |
| 6 Custom Attribute | | | |
| ing Group Policy | | | |
| (IKEVI PISEC Proposal | | | |
| 2 IKEVI Policy | | | |
| | | | |
| C INCLU PUNCY | A | Displaying 10 Sof Yrows K < Page 1 | 1 > > C |
| | G | o to System in Control Panel to activate Wind | 7WS. |
| Last Josés on Schurder 1011-00-04 at 14/15/07 BM form 101 158 111 2 | | | սիսիս |

Schritt 3: Erstellen eines selbstsignierten Zertifikats

Für SSL AnyConnect ist die Verwendung eines gültigen Zertifikats im SSL-Handshake zwischen VPN-Headend und Client erforderlich.

Anmerkung: In diesem Beispiel wird zu diesem Zweck ein selbstsigniertes Zertifikat generiert. Neben selbstsignierten Zertifikaten ist es jedoch möglich, ein Zertifikat hochzuladen, das entweder von einer internen Zertifizierungsstelle (Certificate Authority, CA) oder einer bekannten Zertifizierungsstelle signiert wurde.

Um ein selbstsigniertes Zertifikat zu erstellen, navigieren Sie zu **Devices > Certificates (Geräte > Zertifikate)**.

| Overview Analysis | Policies Devi | ces O | bjects | AMP In | ntelligence | | | . ● Deploy System Help ▼ dperezve ▼ |
|-------------------|----------------|-------|--------|--------|-------------------|------------|--------------|-------------------------------------|
| Device Management | Device Upgrade | NAT | VPN • | QoS | Platform Settings | FlexConfig | Certificates | |

Wählen Sie die Schaltfläche **Hinzufügen** und anschließend im Dropdown-Menü **Gerät** im Fenster **Neues Zertifikat hinzufügen die** entsprechende FTD aus.

| Overview Analysis Policies Devices Objects AMP Intel | igence | 🍳 Deploy System Help 🛛 dperezve 🔻 |
|---|--|--|
| Device Planagement Device opgrade INAT VPN V 200 Ph | doini secungs riexconing Certificates | C Add |
| Name Domain | Enrollment Type Status | |
| | No certificates Add Certificates | |
| | | |
| | Add New Certificate ? × | |
| | Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate. | |
| | Device*: ttdvha-dperezve | |
| | Cert Enrollment*: Select a certificate entrollment object | |
| | Add Cancel | |
| | | |
| | | |
| | | |
| | | |
| 4 | | Activate Windows Code Grand Grand Brade and Market Market |
| Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2 | | -iliiilii cisco |

Wählen Sie die Schaltfläche Add Cert Enrollment (grünes + Symbol), um ein neues Anmeldeobjekt zu erstellen. Weisen Sie nun im Fenster Add Cert Enrollment (Registrierung hinzufügen) einen Namen für das Objekt zu, und wählen Sie im Dropdown-Menü Anmeldungstyp die Option Self Signed Certificate (selbstsigniertes Zertifikat) aus.

| Overview Analysis Policies Devices Objects AMP | Intelligence | . ■ Deploy System Help ▼ dperezve ▼ |
|---|--|---|
| Device Management Device Upgrade NAT VPN • Qo | Platform Settings FlexConfig Certificates | |
| | Add Cert Enrollment | ? × |
| Name Domain | Name* SSL_SelfSigned | |
| | Description | |
| | CA Information Certificate Parameters Key Revocation | |
| | Enrollment Type: Self Signed Certificate | |
| | Common Name (CN) is mandatory for self-signed certificate that is used in Remote Access VPN. To configur (N, please navigate to 'Certificate Parameters' tab. | • |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | Allraw Overrides | |
| | | |
| | | |
| | Save Can | Activate Windows |
| Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2 | | Go to System in Control Panel to activate Windows |

Bei selbstsignierten Zertifikaten ist es schließlich erforderlich, einen gemeinsamen Namen (CN) zu haben. Navigieren Sie zur Registerkarte **Zertifikatsparameter**, um einen CN zu definieren.

| Overview Analysis Policies Devices Objects AMP | Intelligence | | | . I Deploy System Help ▼ dperezve ▼ |
|---|----------------------------|-----------------------------------|--------|---|
| Device Management Device Upgrade NAT VPN • Qos | 9 Platform Settings Fl | exConfig Certificates | | |
| | Add Cert Enrollment | | ? × | Add * |
| Name Domain | Name* | SSL_SelfSigned | | |
| | Description | | | |
| | CA Information Cert | ificate Parameters Key Revocation | | |
| | Include FQDN: | Don't use FQDN in certificate | | |
| | Include Device's IP Addres | s: | | |
| | Common Name (CN): | dperezve.local | | |
| | Organization Unit (OU): | | | |
| | Organization (O): | | | |
| | Locality (L): | | | |
| | State (ST): | | | |
| | Country Code (C): | Comma separated country codes | | |
| | Email (E): | | | |
| | Include Device's Serial N | lumber | | |
| | | | | |
| | Allow Overrides | | _ | |
| | | | | |
| | | | | |
| | | Save | Cancel | Activate Windows |
| Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2 | | | | Go to System in Control Panel to activate Windows |

Wählen Sie **die** Schaltflächen **Speichern** und **Hinzufügen**, und nach einigen Sekunden muss das neue Zertifikat der Zertifikatsliste hinzugefügt werden.

| Overview Analysis | Policies Devices | Objects AMP | Intelligence | | 0 ₄ Deploy System Help v dperezve v |
|---------------------|--------------------|-------------|------------------------------|--------------|---|
| Device Management | Device Upgrade NAT | VPN VQoS | Platform Settings FlexConfig | Certificates | |
| | | | | | Add |
| Name | | Domain | Enrollment Type | Status | |
| 4 🇊 ftdvha-dperezve | 1 | | | | ▲ |
| SSL_SelfSigned | | Global | Self-Signed | O CA 🔍 ID | 1 P 🗘 🗄 |
| | | | | | |

Schritt 4: Lokalen Bereich auf FMC erstellen

Die lokale Benutzerdatenbank und die entsprechenden Kennwörter werden in einem lokalen

Bereich gespeichert. Um den lokalen Bereich zu erstellen, navigieren Sie zu **System > Integration > Realms**.



Wählen Sie die Schaltfläche **Bereich hinzufügen aus**. Weisen Sie im Fenster **Neuen Bereich hinzufügen** einen Namen zu, und wählen Sie im Dropdown-Menü **Typ** die Option **LOCAL** aus.

| Overview Analysis Policies Devices Objects AMP | Intelligence | | | | 0 Deploy Sy | item Help 🔻 d | perezve v |
|--|--|------------------|-----|-------------|--|----------------------|----------------|
| | Add New Realm | | ۰× | Licenses 🔻 | Logging • Health | Monitoring | Tools v |
| Cloud Services Realms Identity Sources High A Realms Realm Sequences Sync Results | Name" AnyConnect-Local-Auth Type LOCAL Local User Configuration A New Configuration Username | Description | | Licenses * | Logging • Health | Monitoring | dd Realm |
| Th | Password Add another local user | Confirm Password | | <u>1e</u> . | | | |
| | | Cancel | ave | | Activate Windows Go to System in Control Pa | nel to activate Wind | ws. |
| Last login on Friday, 2021-09-03 at 12:46:00 PM from 192.168.13.2 | | | | | | | cisco |

Benutzerkonten und Kennwörter, die im Abschnitt "Lokale Benutzerkonfiguration" erstellt wurden.

Hinweis: Kennwörter müssen aus mindestens einem Großbuchstaben, einem Kleinbuchstaben, einer Zahl und einem Sonderzeichen bestehen.

| Overview Analysis Policies Devices Objects AMP | Intelligence | | | 🍳 Deploy 😽 | stem Help 🔻 | dperezve * |
|--|---|------|-------------------|------------------|-------------|-----------------|
| | Add New Realm | θ× | Licenses * | Logging • Health | Monitoring | ▼ Tools ▼ |
| Cloud Services Realms Identity Sources High A Realms Realm Sequences Sync Results | Add New Realm Name* Description AnyConnect-Local-Auth Type LoCAL Local User Configuration | • × | Licenses • | Logging • Health | Monitoring | Tools |
| | Cancel | Save | | | | |
| Last login on Friday, 2021-09-03 at 12:46:00 PM from 192.168.13.2 | | | | | | 111111 CISCO |

Änderungen speichern und neuer Bereich muss der Liste der vorhandenen Bereiche hinzugefügt werden.

| Overview Analysis | Policies Devices Objects | AMP Intelligence | | | | | | | | | ₿ ₄ De | ploy Syster | Help v d | perezve v |
|---------------------|---------------------------|-----------------------------|-------------------|-------------------|----------|---------|-------------|---------|---------|------------|-------------------|-------------|--------------|-----------|
| | | | | Configuration | Users | Domains | Integration | SecureX | Updates | Licenses • | Logging • | Health • | Monitoring • | Tools • |
| | | | | | | | | | | | | | | |
| Cloud Services | Realms Identity Sources | High Availability eStreamer | Host Input Client | Smart Software Ma | nager On | Prem | | | | | | | | |
| Realms Real | Im Sequences Sync Results | | | | | | | | | | | | | |
| | | | | | | | | | | | | Compa | e Realms Ad | d Realm |
| Name 👻 | Description | Туре | Domain | AD Primary | Domain | | Ba | ise DN | | | | State | | |
| AnyConnect-Local-Au | th | LOCAL | Global | | | | | | | | | ඟ Enable | d 🛓 | n 🖬 |
| | | | | | | | | | | | | | | |

Schritt 5: Konfigurieren von SSL AnyConnect

Um SSL AnyConnect zu konfigurieren, navigieren Sie zu **Devices > VPN > Remote Access**.

| Overview Analysis | Policies Device | ces Ol | ojects AMP Intelligen | ice | | | | e , c | Deploy | System | Help 🔻 | dperezve v |
|-------------------|-----------------|--------|-----------------------|-----|-------------------|------------|--------------|--------------|--------|--------|--------|------------|
| Device Management | Device Upgrade | NAT | VPN ► Remote Access | QoS | Platform Settings | FlexConfig | Certificates | | | | | |

Wählen Sie die Schaltfläche Hinzufügen, um eine neue VPN-Richtlinie zu erstellen. Legen Sie einen Namen für das Verbindungsprofil fest, aktivieren Sie das Kontrollkästchen SSL, und wählen Sie das jeweilige FTD als Zielgerät aus. Im Abschnitt Richtlinienzuweisung im Assistenten für VPN-Remotezugriffsrichtlinien muss alles konfiguriert werden.



Wählen Sie **Weiter**, um zur **Verbindungsprofilkonfiguration** zu wechseln. Definieren Sie einen Namen für das Verbindungsprofil, und wählen Sie **AAA Only** als Authentifizierungsmethode aus. Wählen Sie dann im **Authentication Server-**Dropdown-Menü die Option **LOCAL aus,** und wählen Sie schließlich im Dropdown-Menü Local Realm (Lokaler Bereich) den in Schritt 4 erstellten lokalen Bereich aus.



Scrollen Sie auf derselben Seite nach unten, und wählen Sie dann das Bleistiftsymbol im Abschnitt **IPv4-Adresspool aus**, um den von AnyConnect-Clients verwendeten IP-Pool zu definieren.

| Overview Analysis Policies Devices Objects AMP Inte | lligence | 🍳 Deploy System Help 🔻 dperezve 🔻 |
|---|---|--|
| Device Management Device Upgrade NAT VPN > Remote Acc | ess QoS Platform Settings FlexConfig Certificates | |
| Remote Access VPN Policy Wizard | | |
| Policy Assignment Onnection Profile 3 Any | Connect > ④ Access & Certificate > ⑤ Summary | |
| Authent | ication Server:* LOCAL V (LOCAL or Realm or RADIUS) | |
| | Address Pools ? × | |
| Author | Available IPv4 Pools C Selected IPv4 Pools | |
| Client Addre: | search ftdv-dperezve-pool | |
| Client IP addre assignment is | tdress ddress | |
| Use | | |
| □ Use ☑ Use | Add | |
| | | |
| | | |
| Group Policy | | |
| A group policy or create a Gr | ed. Select | |
| Group | OK Cancel | |
| | | |
| | | |
| | | |
| | | Back Next Cancel |
| | | Go to system recent of water to scande emissions |
| Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2 | | -dhalla cusco |

Wählen Sie **Weiter**, um zum Abschnitt **AnyConnect** zu wechseln. Wählen Sie jetzt das in Schritt 2 hochgeladene AnyConnect-Image aus.

| Overview Analysis Policies Devices Objects AMP Intelligence | 0, Deploy S | System Help 🔻 | dperezve v |
|--|----------------|---------------|------------|
| Device Management Device Upgrade NAT VPN > Remote Access QoS Platform Settings FlexConfig Certificates | | | |
| Remote Access VPN Policy Wizard | | | |
| 1 Policy Assignment 2 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 S Summary | | | |
| Remote User AnyConnect Client Outside User Corporate Resources | | | ĺ |
| | | | |
| AnyConnect Client Image | | | |
| The VMV gateway Can automatically download the latest Anyconnect package to the client device when the VMV connection is initiated. Himiting connection setup time by choosing the appropriate CS for the selected package. | | | |
| Download AnyConnect Client packages from <u>Cisco Software Download Center</u> . Show Bundler buttons | | | |
| AnyConnect File Object Name AnyConnect Client Package Name Operating System | | | |
| AnyConnect_Win_4.10 anyconnect-win-4.10.01075-webdeploy-k9.pkg Windows | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | to system como | Next | Cancel |
| Last Jooin on Saturday. 2021-00-04 at 14:26:07 PM from 192.168.13.2 | | | aludo |

Wählen Sie **Weiter**, um zum Abschnitt **"Zugriff und Zertifikat"** zu wechseln. Wählen Sie im Dropdown-Menü **Schnittstellengruppe/Sicherheitszone** die Schnittstelle aus, für die AnyConnect aktiviert werden soll. Wählen Sie anschließend im Dropdown-Menü **Zertifikatregistrierung** das in Schritt 3 erstellte Zertifikat aus.

| Overview Analysis Policies Devices Objects AMP Intelligence | 🔒 Deploy | System Help 🔻 | dperezve v |
|--|--------------------|---------------|-------------------|
| Device Management Device Upgrade NAT VPN > Remote Access QoS Platform Settings FlexConfig Certificates | | | |
| Remote Access VPN Policy Wizard | | | |
| 1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary | | | |
| Remote User AnyConnect Client Outside User Inside Corporate Resources | | | ĺ |
| Network Interface for Incoming VPN Access | | | |
| Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections. | | | |
| Interface group/Security Zone:* VLAN232 | | | |
| Enable DTLS on member interfaces All the devices must have interfaces as part of the Interface Group/Security Zone selected. | | | |
| Device Certificates Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway. Certificate Enrollment:* SSL_SelfSigned | | | |
| | | | |
| | Activate Back down | Next | Cancel |
| Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2 | | | alialia cisco |

Wählen Sie abschließend **Weiter**, um eine Zusammenfassung der AnyConnect-Konfiguration anzuzeigen.



Wenn alle Einstellungen korrekt sind, wählen Sie **Fertig stellen** und geben Sie die Änderungen an FTD weiter.

| Overview | Analysis Policies Devices Objects | AMP Intelligence | | | | | Deploy System Help | operezve + |
|---------------|---|------------------|----------------------|------------|---------------------|----------------------------|--|--------------------|
| | | | | | | | 1 device select Deploy time: Estim | ed Deploy |
| T (| Search using device name, user name, type, g | group or status | | | | | | |
| ۲ | Device | Modified by | Inspect Interruption | Type Group | Last Deploy Time | Preview | Status | |
| > 🛛 | ftdvha-dperezve | dperezve | | FTD | Sep 7, 2021 2:44 PM | 8 | Pending | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | Activate W Go to System | findows in Control Panel to activate Wi | ndows. |
| Last login on | Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13 | 3.2 | | | | | | -ili.ili. cisco |

Überprüfung

Sobald die Bereitstellung erfolgreich war, starten Sie eine AnyConnect-Verbindung vom Windows-Client zu FTD. Der Benutzername und das Kennwort, die bei der Authentifizierungsaufforderung verwendet werden, müssen mit denen übereinstimmen, die in Schritt 4 erstellt wurden.

| | VPN: |
|--------------|-------------------------------------|
| | S Cisco AnyConnect 10.31.124.25 X |
| | |
| | Group: SSL_AnyConnect_LocalAuth ~ |
| ¢ (i) | Username: dperezve |
| | Password: ******** |
| | |
| | |

Sobald die Anmeldeinformationen von FTD genehmigt wurden, muss die AnyConnect-App den Status "Verbunden" anzeigen.

| y Cisco AnyC | onnect Secure Mobility Client | | - | | × |
|--------------|--|---|---|-----------|-------|
| | VPN: Connected to 10.31.124.25. 10.31.124.25 | ~ | D | isconnect | t |
| 00:00:49 | | | | I | IPv4 |
| Ö (i) | | | | | ahaha |

Von FTD aus können Sie den Befehl **show vpn-sessiondb anyconnect** ausführen, um die derzeit aktiven AnyConnect-Sitzungen auf der Firewall anzuzeigen.

Assigned IP : 172.16.13.1 Public IP : 10.31.124.34 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384 Bytes Tx : 15756 Bytes Rx : 14606 Group Policy : DfltGrpPolicy Tunnel Group : SSL_AnyConnect_LocalAuth Login Time : 21:42:33 UTC Tue Sep 7 2021 Duration : 0h:00m:30s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0000000000000000000137dcc9 Security Grp : none Tunnel Zone : 0

Fehlerbehebung

Führen Sie den Befehl **debug webvpn anyconnect** 255 auf FTD aus, um den SSL-Verbindungsfluss bei FTD anzuzeigen.

firepower# debug webvpn anyconnect 255

Neben den AnyConnect-Debuggen kann der Verbindungsfluss auch bei der TCP-Paketerfassung beobachtet werden. Unten sehen Sie ein Beispiel für eine erfolgreiche Verbindung. Ein regulärer Drei-Handshake zwischen Windows-Client und FTD ist abgeschlossen, gefolgt von einem SSL-Handshake, der verwendet wird, um Verschlüsselungen zu akzeptieren.

| *Ethernet1 | | | | | | - 0 | × |
|-----------------------|----------------------|---------------------------|----------------|--|---|----------|-----|
| File Edit View Go | Capture Analyze St | atistics Telephony Wirele | ss Tools Help | | | | |
| 🛋 🔳 🔬 🛞 📙 🖴 | X 🖸 🤇 🗢 👳 🕯 | a e 🕂 🗖 🗖 🗹 e | | | | | |
| p.addr == 10.31.124.2 | 25 | | | | | \times | - + |
| | Carnes | Contraction (| Octaval 1 | ngh tala | | | ^ |
| 13 3.331622 | 10.31.124.34 | 10.31.124.25 | TCP | 66 51300 + 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 | | | |
| 14 3.332733 | 10.31.124.25 | 10.31.124.34 | TCP | 60 443 + 51300 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460 | | | |
| 15 3.332833 | 10.31.124.34 | 10.31.124.25 | TCP | 54 51300 + 443 [ACK] Seg=1 Ack=1 Win=64240 Len=0 | | | |
| 16 3.338665 | 10.31.124.34 | 10.31.124.25 | TLSv1.2 | 247 Client Hello | | | |
| 17 3.341963 | 10.31.124.25 | 10.31.124.34 | TCP | 60 443 + 51300 [ACK] Seq=1 Ack=194 Win=32768 Len=0 | | | |
| 18 3.341963 | 10.31.124.25 | 10.31.124.34 | TLSV1.2 | 1171 Server Hello, Certificate, Server Key Exchange, Server Hello Done | | | |
| 21 3.390864 | 10.31.124.34 | 10.31.124.25 | TIGHT | 54 51300 + 443 [ALK] Seq=194 ACK=1118 Win=63123 Len=0 | | | |
| 29 5.494978 | 10.31.124.34 | 10.31.124.25 | TLSV1.2 | 147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Hessage | | | |
| 31 5 497482 | 10.31.124.34 | 10.31.124.25 | TI Sv1.2 | 1299 Application Data | 4 | | |
| 32 5.498069 | 10.31.124.25 | 10.31.124.34 | TCP | 60 443 + 51300 [ACK] Sen=1169 Ack=1532 Win=32768 Len=0 | | | |
| 33 5, 500054 | 10.31.124.25 | 10.31.124.34 | TI Sv1.2 | 594 Application Data | | | |
| 34 5,500054 | 10.31.124.25 | 10.31.124.34 | TLSv1.2 | 797 Application Data | | | |
| 35 5.500054 | 10.31.124.25 | 10.31.124.34 | TLSv1.2 | 90 Application Data | | | |
| 36 5.500158 | 10.31.124.34 | 10.31.124.25 | TCP | 54 51300 + 443 [ACK] Seg=1532 Ack=2488 Win=64240 Len=0 | | | |
| 66 12.255091 | 10.31.124.34 | 10.31.124.25 | TLSv1.2 | 1524 Application Data | | | |
| 67 12.269297 | 10.31.124.25 | 10.31.124.34 | TCP | 60 443 + 51300 [ACK] Seq=2488 Ack=2992 Win=32768 Len=0 | | | |
| 68 12.269297 | 10.31.124.25 | 10.31.124.34 | TCP | 60 443 + 51300 [ACK] Seq=2488 Ack=3002 Win=32768 Len=0 | | | |
| 69 12.269297 | 10.31.124.25 | 10.31.124.34 | TLSv1.2 | 594 Application Data | | | |
| 70 12.269297 | 10.31.124.25 | 10.31.124.34 | TLSv1.2 | 1431 Application Data | | | |
| 71 12.269297 | 10.31.124.25 | 10.31.124.34 | TLSv1.2 | 1433 Application Data | | | |
| 72 12.269518 | 10.31.124.34 | 10.31.124.25 | TCP | 54 51300 + 443 [ACK] Seq+3002 Ack+5784 Win+64240 Len+0 | | | |
| 73 12.278473 | 10.31.124.25 | 10.31.124.34 | TLSv1.2 | 1514 Application Data | | | |
| 74 12.278473 | 10.31.124.25 | 10.31.124.34 | TLSv1.2 | 1514 Application Data [TCP segment of a reassembled PDU] | | | |
| 75 12.278473 | 10.31.124.25 | 10.31.124.34 | TLSv1.2 | 1271 Application Data | | | |
| > Frame 13: 66 byte | es on wire (528 bits |), 66 bytes captured (| 528 bits) on : | interface \Device\NPF_{@C14AC43-8A81-4ACC-A85E-84CFC2FFC8C9}, id @ | | | |
| > Ethernet II, Src: | : Where_96:c6:e8 (0 | 0:50:56:96:c6:e8), Dst | : Where_b3:84 | 4:a7 (00:50:56:b3:84:a7) | | | |
| > Internet Protocol | 1 Version 4, Src: 10 | .31.124.34, Dst: 10.31 | .124.25 | | | | |
| > Transmission Cont | trol Protocol, Src P | ort: 51300, Dst Port: | 443, Seq: 0, 1 | len: 0 | | | |
| | | | | | | | |
| 0000 00 50 56 53 8 | 54 a7 00 50 56 96 ci | 5 e8 08 00 45 00 ·PV | P VE | | | | |
| 0020 7c 19 c8 64 0 | 1 hh 94 5h 21 h4 m | 0 00 00 00 00 00 02 | 1 1 | | | | |
| 0030 fa f0 0c a0 0 | 00 00 02 04 05 b4 0 | 03 03 08 01 01 | | | | | |
| 0040 04 02 | | | | | | | |
| | | | | | | | |

Nach dem Handshakes des Protokolls muss FTD Anmeldeinformationen mit Informationen validieren, die im lokalen Bereich gespeichert sind.

Sammeln Sie ein DART-Paket, und wenden Sie sich für weitere Recherchen an das Cisco TAC.