Configuratievoorbeeld van SSLVPN met IP-telefoons

Inhoud

Inleiding

Dit document beschrijft hoe u IP-telefoons kunt configureren via een Secure Socket Layer VPN (SSL VPN), ook bekend als een WebVPN. Twee Cisco Unified Communications Manager (CallManager) en drie typen certificaten worden met deze oplossing gebruikt. De CallManager is:

- Cisco Unified Communications Manager (CUCM)
- Cisco Unified Communications Manager Express (Cisco Unified CME)

De certificeringstypes zijn:

- Zelfgetekende certificaten
- Certificaten van derden, zoals Entrust, Thawte en GoDaddy
- Cisco IOS/Adaptieve security applicatie (ASA) certificeringsinstantie (CA)

Het belangrijkste concept om te begrijpen is dat, zodra de configuratie op de SSL VPN gateway en CallManager is voltooid, u zich lokaal bij de IP telefoons moet aansluiten. Dit stelt de telefoons in om zich aan te sluiten bij CUCM en de juiste informatie en certificaten van VPN te gebruiken. Als de telefoons niet lokaal worden aangesloten, kunnen zij de SSL VPN gateway niet vinden en hebben niet de juiste certificaten om de SSL VPN handdruk te voltooien.

De meest gebruikelijke configuraties zijn CUCM/Unified CME met ASA zelfgetekende certificaten en Cisco IOS zelfondertekende certificaten. Dientengevolge, zijn zij het makkelijkst te vormen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Unified Communications Manager (CUCM) voor Cisco Unified Communications Manager Express (Cisco Unified Communications Manager Express)
- SSL VPN (WebVPN)
- Cisco adaptieve security applicatie (ASA)
- Certificaattypen, zoals zelfgetekende, derden- en certificeringsinstanties

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ASA Premium licentie.
- AnyConnect VPN-telefoonlicentie
  - Voor ASA release 8.0.x is de licentie AnyConnect voor Linksys-telefoon.
  - Voor ASA release 8.2.x of hoger is de licentie AnyConnect voor Cisco VPN-telefoon.
- SSL VPN-gateway: ASA 8.0 of hoger (met een AnyConnect voor Cisco VPN-telefoonlicentie) of Cisco IOS-softwarerelease 12.4T of hoger.
  - Cisco IOS-softwarerelease 12.4T of hoger wordt niet formeel ondersteund zoals gedocumenteerd in de SSL VPN-configuratiegids.
  - In Cisco IOS-softwarerelease 15.0(1)M, is de SSL VPN-gateway een zittende licentiefunctie voor de Cisco 880-, Cisco 890-, Cisco 1900-, Cisco 2900- en Cisco 3900-platforms. Er is een geldige licentie vereist voor een succesvolle SSL VPN-sessie.
- CallManager: CUCM 8.0.1 of hoger, of Unified CME 8.5 of hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

> Opmerkingen:
>
> Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.
>
> De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met show. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

Basis ASA SSL VPN-configuratie

De basisconfiguratie van ASA SSL VPN wordt in deze documenten beschreven:

- ASA 8.x: VPN-toegang met de AnyConnect VPN-client met zelfgetekende configuratievoorbeeld van certificaat
- AnyConnect VPN-clientverbindingen configureren

Zodra deze configuratie is voltooid, moet een externe testpc in staat zijn om verbinding te maken met de SSL VPN-gateway, verbinding te maken via AnyConnect en de CUCM te typen. Zorg ervoor dat de ASA een AnyConnect heeft voor Cisco IP-telefoonlicentie. (Gebruik de opdracht **tonen**.) Zowel TCP- als UDP-poort 443 moet geopend zijn tussen de poort en de client.

> Opmerking: Laden-gebalanceerde SSL VPN wordt niet ondersteund voor VPN-telefoons.

CUCM: ASA SSL VPN met zelfgetekende certificaten configuratie

Raadpleeg IP-telefoon SSL VPN naar ASA met AnyConnect voor meer informatie.

De ASA moet een licentie hebben voor AnyConnect voor Cisco VPN-telefoon. Nadat u SSL VPN vormt, kunt u vervolgens uw CUCM voor VPN configureren.

1. Gebruik deze opdracht om het zelf-ondertekende certificaat van de ASA te exporteren:

   ```
   ciscoasa(config)# crypto ca export trustpoint name identity-certificate
   ```

   Deze opdracht geeft een pem-gecodeerd identiteitsbewijs aan de terminal weer.
2. Kopieer en plak het certificaat naar een teksteditor en bewaar het als een .pem-bestand. Zorg ervoor dat u de BEGIN-CERTIFICAAT- en EINDCERTIFICAATregels opneemt, of dat het certificaat niet correct importeert. Wijzig het formaat van het certificaat niet omdat dit problemen zal veroorzaken wanneer de telefoon aan authentiek ASA probeert te verklaren.
3. Navigeer naar **Cisco Unified Operating System Management > Security > certificaatbeheer > Upload certificaatketen** om het certificaatbestand te laden naar het vak CERTIFICATE MANAGEMENT van het CUCM.
4. Download de certificaten CallManager.pem, CAPF.pem, en Cisco_Manufacturing_CA.pem van het zelfde gebied dat wordt gebruikt om de zelf getekende certificaten van de ASA te laden (zie Stap 1), en bewaar deze aan uw desktop.
   1. Om bijvoorbeeld CallManager.pem in de ASA te importeren, gebruikt u deze opdrachten:

      ```
      ciscoasa(config)# crypto ca trustpoint certificate-name
      ciscoasa(config-ca-trustpoint)# enrollment terminal
      ciscoasa(config)# crypto ca authenticate certificate-name
      ```

   2. Wanneer u wordt gevraagd het corresponderende certificaat voor het vertrouwde punt te kopiëren en te plakken, opent u het bestand dat u met de CUCM hebt opgeslagen, en kopieert u het Base64-gecodeerde certificaat en voegt u het vervolgens op. Zorg ervoor dat u de BEGIN-CERTIFICAAT- en EINDCERTIFICAATregels (met koppeltekens) opneemt.
   3. Typ **het einde** en druk vervolgens op **Terug**.

4. Typ **na** ontvangst van het certificaat **ja** en druk op **ENTER**.
5. Herhaal stap 1 tot en met 4 voor de andere twee certificaten (CAPF.pem, Cisco_Manufacturing_CA.pem) van CUCM.

5. Configureer de CUCM voor de juiste VPN-configuraties, zoals beschreven in CUCM IPphone VPN.pdf.

   Opmerking: De VPN gateway die op CUCM is ingesteld moet overeenkomen met de URL die op de VPN-gateway is ingesteld. Als de gateway en URL niet overeenkomen, kan de telefoon het adres niet oplossen, en u zult geen tekorten op de VPN gateway zien.

- Op het UCM: De VPN gateway URL is https://192.168.1.1/VPNPhone
- Gebruik in de ASA deze opdrachten:

```
ciscoasa# configure terminal
ciscoasa(config)# tunnel-group VPNPhones webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url https://192.168.1.1/VPNPhone
enable
ciscoasa(config-tunnel-webvpn)# exit
```

- U kunt deze opdrachten gebruiken in het Adaptieve Security Apparaat Manager (ASDM) of onder het verbindingsprofiel.

CUCM: ASA SSL VPN met configuratie van derden-certificaten

Deze configuratie lijkt erg op de configuratie die in CUCM is beschreven: ASA SSLVPN met de sectie zelfgetekende Certificaten Configuration, behalve dat u certificaten van derden gebruikt. Het configureren van SSL VPN op de ASA met certificaten van derden zoals beschreven in ASA 8.x Installeer handmatig 3-partijverkopers Certificaten voor gebruik met WebVPN Configuratievoorbeeld.

Opmerking: U moet de volledige certificeringsketen van de ASA naar de CUCM kopiëren en alle intermediaire en wortelcertificaten omvatten. Als CUCM niet de volledige keten bevat, hebben de telefoons niet de benodigde certificaten om te authentiseren en zullen de SSL VPN handdruk niet uitvoeren.

Basis IOS SSL VPN-configuratie

Opmerking: IP-telefoons worden aangeduid als niet ondersteund in IOS SSL VPN; configuraties zijn alleen de best mogelijke moeite .

De basisconfiguratie van Cisco IOS SSL VPN wordt in deze documenten beschreven:

- SSL VPN-client (SVC) op IOS met Configuratievoorbeeld
- AnyConnect VPN-client op IOS-router met IOS Zone-gebaseerde beleidsfirewall

Zodra deze configuratie is voltooid, moet een externe testpc in staat zijn om verbinding te maken met de SSL VPN-gateway, verbinding te maken via AnyConnect en de CUCM te typen. In Cisco IOS 15.0 en hoger moet u een geldige SSL VPN-licentie hebben om deze taak te voltooien. Zowel TCP- als UDP-poort 443 moet geopend zijn tussen de poort en de client.

CUCM: IOS SSL VPN met zelfgetekende certificaten

Deze configuratie is vergelijkbaar met de configuratie die in CUCM is beschreven: ASA LVPN met configuratie en CUCM van derden voor certificaten: ASA SSLVPN met zelfgetekende delen van de configuratie van certificaten. De verschillen zijn:

1. Gebruik deze opdracht om het zelf-ondertekende certificaat van de router te exporteren:

```
R1(config)# crypto pki export trustpoint-name pem terminal
```

2. Gebruik deze opdrachten om de CUCM-certificaten te importeren:

```
R1(config)# crypto pki trustpoint certificate-name
R1(config-ca-trustpoint)# enrollment terminal
R1(config)# crypto ca authenticate certificate-name
```

De WebVPN context configuratie zou deze tekst moeten tonen:

```
gateway webvpn_gateway domain VPNPhone
```

Het CUCM configureren zoals in CUCM beschreven wordt: ASA SSLVPN met zelfgetekende sectie van de configuratie van certificaten.

CUCM: IOS SSL VPN met configuratie van derden voor certificaten

Deze configuratie is vergelijkbaar met de configuratie die in CUCM is beschreven: ASA SSLVPN met zelfgetekende sectie van de configuratie van certificaten. Configureer uw Webex met een certificaat van een derde.

> Opmerking: U moet de volledige WebVPN certificaatketen naar CUCM kopiëren en alle intermediaire en wortelcertificaten omvatten. Als CUCM niet de volledige keten bevat, hebben de telefoons niet de benodigde certificaten om te authentiseren en zullen de SSL VPN handdruk niet uitvoeren.

Unified CME: ASA/Router SSL VPN met zelfgetekende certificaten/configuratie van derden

De configuratie van het Unified CME is vergelijkbaar met de configuraties van het CUCM; De WebVPN eindpuntconfiguraties zijn bijvoorbeeld hetzelfde. Het enige significante verschil is de configuraties van de Unified CME call agent. Configureer de VPN-groep en het VPN-beleid voor Unified CME zoals beschreven in SSL VPN-client configureren voor SCCP IP-telefoons.

> Opmerking: Unified CME ondersteunt alleen Skinny Call Control Protocol (SCCP) en ondersteunt Session Initiation Protocol (SIP) niet voor VPN-telefoons.

> Opmerking: Er is geen behoefte om de certificaten van het Unified CME naar de ASA of

router uit te voeren. U hoeft de certificaten alleen te exporteren vanuit de ASA of router WebVPN-gateway naar Unified CME.

Om de certificaten van de gateway WebVPN uit te voeren, verwijs naar de ASA/routersectie. Als u een certificaat van een derde gebruikt, moet u de volledige certificaatketen vermelden. Als u de certificaten aan het Unified CME wilt importeren, gebruikt u dezelfde methode als die gebruikt wordt om certificaten in een router in te voeren:

```
CME(config)# crypto pki trustpoint certificate-name
CME(config-ca-trustpoint)# enrollment terminal
CME(config)# crypto ca authenticate certificate-name
```

UC 520 IP-telefoons met SSL VPN-configuratie

De Cisco Unified Communications 500 Series Model UC 520 IP-telefoon is aanzienlijk anders dan de CUCM- en CME-configuraties.

- Aangezien de UC 520 IP-telefoon zowel de CallManager als de WebVPN-gateway is, hoeft u geen certificaten tussen de twee apparaten te configureren.
- Configureer de WebexVPN op een router zoals u normaal gesproken zou doen met zelfgetekende certificaten of certificaten van derden.
- UC 520 IP-telefoon heeft een ingebouwde WebVPN-client en u kunt de client configureren op dezelfde manier als een normale PC om verbinding te maken met WebVPN. Voer de poort in en dan de gebruikersnaam/wachtwoordcombinatie.
- De UC 520 IP-telefoon is compatibel met de Cisco Small Business IP-telefoon SPA525G.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.