

VPN-telefoons configureren en probleemoplossing

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[ASA-configuratie](#)

[CUCM-configuratie](#)

[Problemen oplossen](#)

[Te verzamelen gegevens](#)

[Veelvoorkomende problemen](#)

[Actualisering van het ASA-identiteitsbewijs](#)

[ASA selecteert een Elliptische curve \(EC\)-algoritme](#)

[TLS-aansluitingsfout](#)

[Kan geen verbinding met ASA maken na update van certificaat](#)

[Kan ASA URL niet via DNS oplossen](#)

[Telefoon schakelt VPN niet in](#)

[Telefoonregisters maar kan gespreksgeschiedenis niet weergeven](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u de VPN-telefoonfunctie van Cisco IP-telefoons en Cisco Unified Communications Manager kunt configureren en oplossen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Unified Communications Manager (CUCM)
- Cisco adaptieve security applicatie (ASA)
- AnyConnect Virtual Private Network (VPN)
- Cisco IP-telefoons

Gebruikte componenten

- 8861 14-0-1-0101-145
- ASAv 9.12(2)9
- UCM 11.5.1.21900-40

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

De testomgeving in dit artikel bevat een 8861, ASAv en CUCM 11.5.1, maar er zijn veel verschillende variaties van deze producten die je kunt gebruiken. U moet de lijst met telefoonfuncties op CUCM controleren om er zeker van te zijn dat uw telefoonmodel de VPN-functie ondersteunt. Om de lijst met telefoonfuncties te gebruiken, hebt u toegang tot uw CUCM-uitgever in uw browser en navigeer naar **Cisco Unified Reporting > Unified CM-telefoonfunctiekaart**. Generate een nieuw rapport en selecteer vervolgens uw telefoonmodel in de uitrollijst. Vervolgens moet u in het gedeelte Lijst-functies naar client voor Virtual Private Network zoeken zoals in de afbeelding:

Unified CM Phone Feature List

Provides a complete list of features available to products supported by Unified CM.
Created on Wed Apr 01 09:41:27 EDT 2020

Product:

Feature:

Unified CM Cluster Name

Cluster Name	Publisher Name/IP
cucm1251	cucm1251

List Features

Product	Protocol	Feature Name
Cisco 7962	SCCP	Security By Default
Cisco 7962	SCCP	Security Encryption
Cisco 7962	SCCP	Shared Line Appearance
Cisco 7962	SCCP	Show Speeddial Labels
Cisco 7962	SCCP	Single Button Barge
Cisco 7962	SCCP	Size Safe on Phone Template
Cisco 7962	SCCP	Support CAPF
Cisco 7962	SCCP	Trusted Device
Cisco 7962	SCCP	Use Generic Icon
Cisco 7962	SCCP	User Hold
Cisco 7962	SCCP	Video
Cisco 7962	SCCP	Virtual Private Network Client
Cisco 7962	SIP	7915 12-Button Line Expansion Module
Cisco 7962	SIP	7915 24-Button Line Expansion Module
Cisco 7962	SIP	7916 12-Button Line Expansion Module

Configureren

VPN-telefoons vereisen dat u de juiste configuratie op uw ASA en CUCM hebt. U kunt eerst met elk product starten, maar dit document heeft eerst betrekking op de ASA-configuratie.

ASA-configuratie

Stap 1. Controleer dat de ASA gelicentieerd is om AnyConnect voor VPN-telefoons te ondersteunen. De opdracht **show** in de ASA kan worden gebruikt om te verifiëren dat **AnyConnect voor Cisco VPN-telefoon** is ingeschakeld zoals in dit fragment wordt getoond:

```
[output omitted]
Licensed features for this platform:
Maximum VLANs : 50
Inside Hosts : Unlimited
Failover : Active/Standby
Encryption-DES : Enabled
Encryption-3DES-AES : Enabled
Security Contexts : 0
Carrier : Enabled
AnyConnect Premium Peers : 250
AnyConnect Essentials : Disabled
Other VPN Peers : 250
Total VPN Peers : 250
AnyConnect for Mobile : Enabled
AnyConnect for Cisco VPN Phone : Enabled
Advanced Endpoint Assessment : Enabled
Shared License : Disabled
Total TLS Proxy Sessions : 500
Botnet Traffic Filter : Enabled
Cluster : Disabled
```

Als deze optie niet is ingeschakeld, moet u met het licentieteam werken om de juiste licentie te krijgen. Nu u hebt bevestigd dat uw ASA VPN-telefoons ondersteunt, kunt u de configuratie starten.

Opmerking: Alle onderstreepte punten in het configuratiegedeelte zijn configureerbare namen die kunnen worden gewijzigd. De meeste van deze namen worden elders in de configuratie genoemd, dus is het belangrijk om de namen te onthouden die u gebruikt in deze secties (groepsbeleid, tunnelgroep, etc.) omdat u ze later nodig hebt.

Stap 2. Maak een IP-adrespool voor VPN-clients. Dit is gelijk aan een DHCP-pool in die zin dat wanneer een IP-telefoon op de ASA aansluit, het een IP-adres uit deze pool ontvangt. De pool kan worden aangemaakt met deze opdracht op de ASA:

ip lokale pool VPN-telefoon-pool 10.10.1.1-10.10.1.254 masker 255.255.255.0

Ook, als u een ander netwerk of SUBNET masker verkiest, kan dat ook worden veranderd. Zodra de pool wordt gecreëerd, moet u een groepsbeleid (een reeks parameters voor de verbinding tussen de ASA en IP telefoons) configureren:

intern vpn-telefoonbeleid met groepsbeleid

Eigenschappen van het vpn-phone-beleid voor groepsbeleid

tunnelbeleid

VPN-tunnelprotocol ssl-client

Stap 3. U dient AnyConnect in te schakelen als dit nog niet is ingeschakeld. Om dit te doen, moet je de naam van de buiteninterface kennen. Meestal wordt deze interface **buiten** genoemd (zoals in het fragment wordt getoond), maar het is configureerbaar, dus controleer of u de juiste interface hebt. Start **ip** om de lijst met interfaces te zien:

```
sckiewer-ASAv# show ip
System IP Addresses:
Interface Name IP address Subnet mask Method
GigabitEthernet0/0 outside 172.16.1.250 255.255.255.0 CONFIG
GigabitEthernet0/1 inside 172.16.100.250 255.255.255.0 CONFIG
Current IP Addresses:
Interface Name IP address Subnet mask Method
GigabitEthernet0/0 outside 172.16.1.250 255.255.255.0 CONFIG
GigabitEthernet0/1 inside 172.16.100.250 255.255.255.0 CONFIG
```

In deze omgeving wordt de externe interface **buiten** genoemd, zodat deze opdrachten AnyConnect op die interface mogelijk maken.

webvp

buiten inschakelen verbinding maken

Stap 4. Het configureren van een nieuwe tunnelgroep om het groepsbeleid toe te passen dat eerder gemaakt is op elke client die een specifieke URL aansluit. Let op de verwijzing naar de namen van de IP-adrespool en het groepsbeleid dat u eerder maakte in de 3de en 4de regels van het fragment. Als u de namen van de IP-adrespool of het groepsbeleid hebt gewijzigd, moet u de onjuiste waarden door uw aangepaste namen vervangen:

tunnelgroep vpn-telefoon-groep type afstandstoegang
veelzijdige algemene eigenschappen van de tunnelgroep voor VPN-telefoon
Adres-pool VPN-telefoon-pool
vpn-telefoon-beleid met standaardinstellingen
VPN-telefoon-groep webVPN-eigenschappen
echtheidscertificaat
<https://asav.sckiewer.lab/phone> voor groepsgebruik;

U kunt een IP-adres gebruiken in plaats van een naam voor de **groep-URL**. Dit gebeurt meestal als de telefoons geen toegang hebben tot een DNS server die de Full Qualified Domain Name (FQDN) van de ASA kan oplossen. U kunt ook zien dat dit voorbeeld certificatie op certificaat gebruikt. U hebt de optie om ook gebruikersnaam/wachtwoordverificatie te gebruiken, maar er zijn meer vereisten voor de ASA die buiten het toepassingsgebied van dit document vallen.

In dit voorbeeld heeft de DNS-server het A-record, **asav.sckiewer.lab - 172.16.1.250** en u kunt in de **show-ip**-uitgang zien dat 172.16.1.250 is geconfigureerd op de interface die **buiten** is genoemd. De configuratie zou dus zijn:

crypto ca trustpoint als identiteitsbewijs

inschrijving zelf

onderwerp-naam CN=asav.sckiewer.lab

inschrijving van crypto ca als identiteitsbewijs

ssl trust-point asa-Identity-cert buiten

Opmerking:

1. Er was een nieuw 'trustpoint' in het leven geroepen, dat 'asa-Identity-cert' genoemd werd en er is een 'onderwerp-naam' op toegepast. Dit zorgt ervoor dat het certificaat dat uit dit trustpunt is gegenereerd de gespecificeerde naam van de persoon gebruikt
2. Vervolgens stelt de opdracht "crypto kan zich inschrijven als een identiteitsbewijs" de ASA in staat om een zelfgetekend certificaat op te stellen en op dat trustpunt op te slaan
3. Ten slotte presenteert de ASA het certificaat in het trustpoint aan elk apparaat dat zich verbindt met de externe interface

Stap 5. Maak de benodigde trustpoints om de ASA in staat te stellen het certificaat van de IP-telefoon te vertrouwen. Eerst moet u bepalen of uw IP-telefoons gebruik maken van het geïnstalleerde certificaat (MIC) of een lokaal belangrijk certificaat (LSC) van de fabrikant. Standaard gebruiken alle telefoons hun MIC voor beveiligde verbindingen tenzij er een LSC op is geïnstalleerd. In CUCM 11.5.1 en hoger kunt u een zoekopdracht uitvoeren bij **Unified CM-beheer > Apparatuur > Phone** om te zien of LSC's zijn geïnstalleerd terwijl oudere versies van CUCM u fysiek de beveiligingsinstellingen per telefoon moeten controleren. In CUCM 11.5.1 moet u een filter toevoegen (of het standaardfilter wijzigen) aan de **door u afgegeven LSC**. Apparaten met **DNA** in de **LSC afgegeven door** kolom gebruiken de MIC omdat er geen LSC geïnstalleerd is.

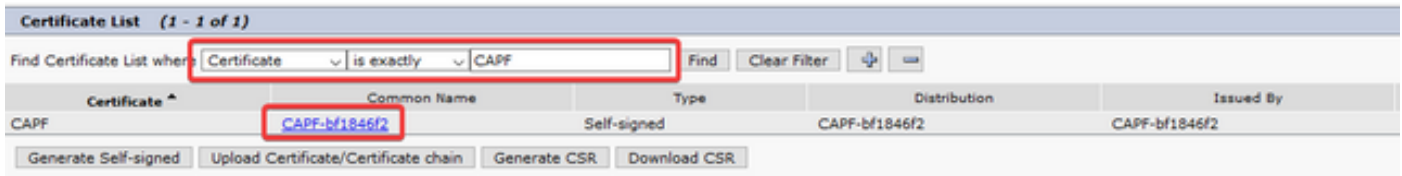
	Device Name(Lines) ^	Description	Extension	Owner User ID	LSC Status	LSC Expires	LSC Issued By	LSC Issuer Expires By	CAPF Auth String	Device P
<input type="checkbox"/>	SC76AAAAAAAAAA				None	NA	NA	NA		SIP
<input type="checkbox"/>	SEP38EC183318E	Auto 3010	3010		None	NA	NA	NA		SIP
<input type="checkbox"/>	SEP381C7840BCE	Auto 3006	43760		None	NA	NA	NA		SIP
<input type="checkbox"/>	SEP3818F27860	Auto 3009	3009		Troubleshoot Success	02/17/2025	CAPF-099993bf	05/01/2024		SIP
<input type="checkbox"/>	SEP448419C31A7C	Auto 3013	3013		None	NA	NA	NA		SIP
<input type="checkbox"/>	UCCK_T006	INITIAL_INBOUND_CCG-1			None	NA	NA	NA		SCCP

Als uw telefoon lijkt op die welke in het beeld wordt gemarkeerd, moet u het CAPF-certificaat van de CUCM Publisher naar de ASA uploaden om de ASA in staat te stellen het certificaat van de telefoon voor de veilige verbinding te valideren. Als u apparaten wilt gebruiken zonder LSC geïnstalleerd te zijn, moet u de Cisco Fabric Certificates uploaden naar de ASA. Deze certificaten kunnen worden gevonden op de CUCM Publisher bij **Cisco Unified OS-beheer > Security > certificaatbeheer**:

Opmerking: U kunt zien dat sommige van deze certificaten in meerdere trust-winkels (CallManager-vertrouwen en CAPF-vertrouwen) zijn. Het maakt niet uit welke winkel u de certificaten downloaden zolang u ervoor zorgt dat u degene met deze exacte namen selecteert.

- Cisco_Root_CA_2048 < MIC SHA-1 Root

- Cisco_Manufacturing_CA < MIC SHA-1 midden
- Cisco_Root_CA_M2 < MIC SHA-256 Root
- Cisco_Manufacturing_CA_SHA2 < MIC SHA-256 Intermediate
- CAPF van CUCM Publisher < LSC



Wat de MIC betreft, gebruiken oudere telefoons zoals de 79xx en 99xx serie de certificaat ketting van het SHA-1 terwijl nieuwere telefoonmodellen zoals de 88xx serie de certificaat ketting van het SHA-256 gebruiken. De certificeringsketen die uw telefoon(en) gebruikt moet/moeten worden geüpload naar de ASA.

Zodra u de vereiste certificaten heeft, kunt u de vertrouwens-(e)punten maken met:

crypto ca trustpoint cert1

inschrijvingsterminal

crypto om cert echt te maken₁

De eerste opdracht creëert een betrouwbaar punt genaamd **cert1**, en de **crypto kan** opdracht **authenticeren** stelt u in staat om de basis64 gecodeerde certificaat in de CLI te plakken. U kunt deze opdrachten zo vaak uitvoeren als u wilt om de juiste trustpunten op de ASA te hebben, maar vergeet niet bij elk certificaat een nieuwe vertrouwde point naam te gebruiken.

Stap 6. Verkrijg een kopie van het ASA-identiteitsbewijs door deze opdracht uit te geven:

crypto kan exporteren als identiteitsbewijs

Dit exporteert het identiteitsbewijs voor het trustpunt dat bekend staat als een identiteitsbewijs. Zorg ervoor dat u de naam aanpast zodat deze overeenkomt met het vertrouwde punt dat u in stap 4 hebt aangemaakt.

Hier is de volledige labconfiguratie voor de ASA:

```
ip local pool vpn-phone-pool 10.10.1.1-10.10.1.254 mask 255.255.255.0

group-policy vpn-phone-policy internal
group-policy vpn-phone-policy attributes
    split-tunnel-policy tunnelall
    vpn-tunnel-protocol ssl-client

webvpn
    enable outside
    anyconnect enable

tunnel-group vpn-phone-group type remote-access
tunnel-group vpn-phone-group general-attributes
    address-pool vpn-phone-pool
    default-group-policy vpn-phone-policy

tunnel-group vpn-phone-group webvpn-attributes
```

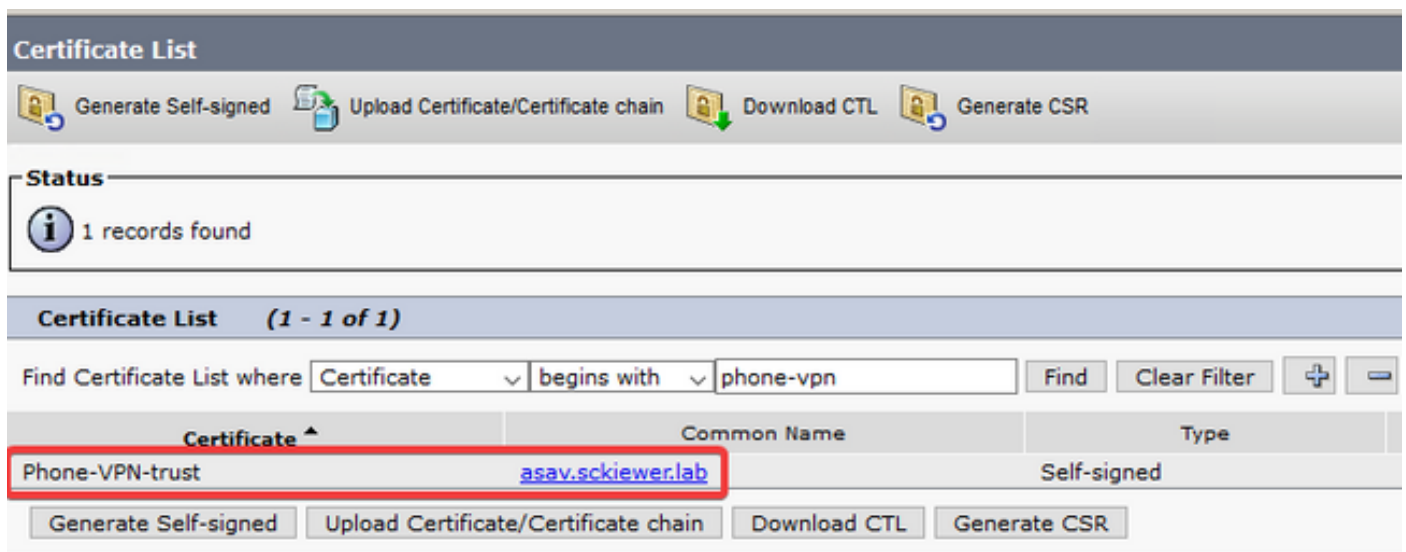
```
authentication certificate
group-url https://asav.sckiewer.lab/phone enable
```

```
ssl trust-point asa-identity-cert outside
```

Op dit punt, is de ASA configuratie volledig, en u kunt met de configuratie van CUCM verder gaan. U moet beschikken over een kopie van het ASA-certificaat dat u net hebt verzameld en de URL die is ingesteld in de tunnelgroep sectie.

CUCM-configuratie

Stap 1. Op CUCM, navigeer naar **Cisco Unified OS-beheer > Security > certificaatbeheer** en uploadde het ASA-certificaat als **telefoon-VPN-trust**.



Certificate List

Generate Self-signed Upload Certificate/Certificate chain Download CTL Generate CSR

Status

1 records found

Certificate List (1 - 1 of 1)

Find Certificate List where Certificate begins with phone-vpn Find Clear Filter




Certificate	Common Name	Type
Phone-VPN-trust	asav.sckiewer.lab	Self-signed

Generate Self-signed Upload Certificate/Certificate chain Download CTL Generate CSR


Stap 2. Zodra dit gebeurt, navigeer dan naar **Cisco Unified CM-beheer > Geavanceerde functies > VPN > VPN-profiel** en maak een nieuw profiel. In dit hoofdstuk is er geen recht of fout, het is belangrijk om het doel van elke instelling te begrijpen.

1. **Auto Network Detect inschakelen** - als deze optie is ingeschakeld, pingt de telefoon zijn TFTP-server wanneer deze wordt ingeschakeld. Als het een antwoord op dit pingelen ontvangt, schakelt het VPN niet in. Als de telefoon geen reactie op dit pingelen ontvangt, maakt het VPN mogelijk. Als deze instelling is ingeschakeld, kan VPN niet handmatig worden ingeschakeld.
2. **Host ID Check** - wanneer deze optie is ingeschakeld, controleert de telefoon de VPN-URL uit het configuratiebestand (<https://asav.sckiewer.lab/phone> wordt in dit document gebruikt), en garandeert dat de hostname of FQDN overeenkomt met de Common Name (CN) of een SAN-invoer in het door de ASA gepresenteerde certificaat.
3. **Verificatiemethode** - controleert welk type verificatiemethode wordt gebruikt voor de aansluiting op de ASA. In het configuratievoorbeeld uit dit document wordt op certificaat gebaseerde authenticatie gebruikt.
4. **Wachtwoordpersistentie** - als deze optie is ingeschakeld, wordt het wachtwoord van de klant in de telefoon opgeslagen totdat er een mislukt logbestand wordt uitgevoerd, wordt de client handmatig het wachtwoord gewist of wordt de telefoon opnieuw ingesteld.

VPN Profile Configuration

Save  Delete  Copy  Add New

Status

 Status: Ready

VPN Profile Information

Name*

Description

Enable Auto Network Detect

Tunnel Parameters

MTU*

Fail to Connect*

Enable Host ID Check

Client Authentication

Client Authentication Method*

Enable Password Persistence

Save Delete Copy Add New

Stap 3. Daarna kunt u navigeren naar **Cisco Unified CM-beheer > Geavanceerde functies > VPN > VPN-gateway**. U moet ervoor zorgen dat uw VPN-gateway overeenkomt met de ASA-configuratie en dat u het certificaat van het bovenste vak naar het onderste vak verplaatst zoals in de afbeelding:

VPN Gateway Configuration

Save

Status
 Status: Ready

VPN Gateway Information
 VPN Gateway Name*
 VPN Gateway Description
 VPN Gateway URL*

VPN Gateway Certificates
 VPN Certificates in your Truststore
 VPN Certificates in this Location*

Stap 4. Zodra dit wordt opgeslagen, moet u naar **Cisco Unified CM-beheer > Geavanceerde functies > VPN-groep** navigeren en de gateway verplaatsen die u in het vak 'Geselecteerde VPN-gateways in dit VPN-groepsvak' hebt gemaakt:

VPN Group Configuration

Save

Status
 Status: Ready


VPN Group Information
 VPN Group Name*
 VPN Group Description

VPN Gateway Information
 All Available VPN Gateways
 Selected VPN Gateways in this VPN Group


Stap 5. Nu de VPN-instellingen zijn geconfigureerd, moet u navigeren naar **Cisco Unified CM-beheer > Apparaatinstellingen > Gemeenschappelijk telefoonprofiel**. Hier moet u het profiel kopiëren dat uw gewenste VPN-telefoon gebruikt, het opnieuw noemen en uw VPN-groep en

VPN-profiel selecteren en vervolgens het nieuwe profiel opslaan:

Common Phone Profile Configuration

 Save

Status

 Status: Ready

Common Phone Profile Information

Name*

Description

Local Phone Unlock Password

DND Option*

DND Incoming Call Alert*

Feature Control Policy

Wi-Fi Hotspot Profile [View Details](#)

Enable End User Access to Phone Background Image Setting

Secure Shell Information

Secure Shell User

Secure Shell Password

Phone Personalization Information

Phone Personalization*

Always Use Prime Line*

Always Use Prime Line for Voice Message*

Services Provisioning*

VPN Information

VPN Group

VPN Profile

Stap 6. Ten slotte moet u dit nieuwe profiel op uw telefoon toepassen en de telefoon opnieuw instellen terwijl het op het interne netwerk is. Dit staat de telefoon toe om al deze nieuwe configuratie zoals de ASA certificaathash, en de VPN URL te ontvangen.

Opmerking: Voordat u de telefoon gaat testen, moet u ervoor zorgen dat de telefoons een 'Alternate TFTP' server hebben geconfigureerd. Aangezien de ASA optie 150 niet aan de telefoons biedt, moet TFTP IP handmatig op de telefoons worden ingesteld.

Stap 7. Test de VPN-telefoon en controleer of deze met succes kan verbinden met de ASA en registreer. U kunt verifiëren dat de tunnel op de ASA staat met, **vpn-sessiondb om het even welke verbinding tonen**:

```
sckiewer-ASAv# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username      : CP-8841-SEP682C7B40B5CE
Index        : 3
Assigned IP   : 10.10.1.131      Public IP    : 192.168.1.52
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium, AnyConnect for Cisco VPN Phone
Encryption    : AnyConnect-Parent: (1)AES256 SSL-Tunnel: (1)AES256 DTLS-Tunnel: (1)AES256
Hashing       : AnyConnect-Parent: (1)SHA1 SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx      : 4275771          Bytes Rx     : 32476192
Group Policy  : VPN-Phone        Tunnel Group : VPN-Phone
Login Time    : 01:07:39 UTC Fri Mar 27 2020
Duration      : 4d 1h:56m:42s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A              VLAN         : none
Audt Sess ID  : 0e3051fa000030005e7d51db
Security Grp  : none
```

Problemen oplossen

Te verzamelen gegevens

Om een probleem met VPN-telefoon op te lossen, worden deze gegevens aanbevolen:

- ASA-debug: kapstokloggendebg crypto ca transactions 255debug crypto ca messages 255debug crypto ca 255debug van webversie 25debug van webversie 25
- Logbestanden van de telefoonconsole (of een PRT als de telefoon het ondersteunt - [hier](#) meer informatie)

Nadat u het probleem hebt gereproduceerd met de enabled-apparaten, kunt u de uitvoer met deze opdracht bekijken aangezien debug-uitvoer altijd 711001 bevat:

toonlogboek | i 711001

Veelvoorkomende problemen

Opmerking: Voor de doeleinden van deze sectie, zijn de logfragmenten van een 8861 telefoon aangezien dat één van de meer algemene telefoonreeksen is die als VPN-telefoon worden ingezet. Houd in gedachten dat andere modellen verschillende berichten in de logs kunnen schrijven.

Actualisering van het ASA-identiteitsbewijs

Voordat het ASA-identiteitsbewijs afloopt, moet er een nieuw certificaat gegenereerd worden en naar de telefoons worden uitgeduwd. Om dit te doen zonder de VPN telefoons te beïnvloeden, gebruik dit proces:

Stap 1. Maak een nieuw betrouwbaar punt voor het nieuwe identiteitsbewijs:

crypto ca trustpoint asa-identity-cert-2

inschrijving zelf

onderwerp-naam CN=asav.sckiewer.lab

inschrijving van crypto ca als identiteitsbewijs 2

Stap 2. Op dit punt zou u een nieuw identiteitsbewijs voor de ASA hebben, maar het wordt nog niet op enige interface gebruikt. U moet dit nieuwe certificaat exporteren en uploaden naar CUCM:

cryptoomexport als identiteitsbewijs

Stap 3. Zodra u het nieuwe identiteitsbewijs hebt, uploadt u het naar een van uw CUCM-knooppunten als telefoon-VPN-vertrouwen bij **Cisco Unified OS-beheer > Security > certificaatbeheer > Upload**.

Opmerking: Het huidige telefoon-VPN-trust certificaat zou alleen aanwezig zijn op het CUCM-knooppunt waarnaar het oorspronkelijk geüpload is. (Het wordt niet automatisch verspreid naar andere knooppunten zoals sommige certificaten). Als uw CUCM-versie wordt beïnvloed door [CSCuo58506](#), moet u het nieuwe ASA-certificaat naar een ander knooppunt uploaden.

Stap 4. Zodra het nieuwe certificaat aan een van de knooppunten in de cluster is geüpload, navigeer dan naar **Cisco Unified CM-beheer > Geavanceerde functies > VPN > VPN-gateway** op de CUCM-uitgever

Stap 5. Selecteer de juiste gateway.

Stap 6. Selecteer het certificaat in het bovenste vakje (dit is het certificaat dat u zojuist geüpload hebt) en selecteer de pijl omlaag om het naar de onderkant te verplaatsen (dit maakt het TFTP mogelijk om dat certificaat toe te voegen aan de configuratiebestanden van uw VPN-telefoon) en selecteer Opslaan.

Stap 7. Zodra dat is gebeurd, stelt u alle VPN-telefoons opnieuw in. Op dit punt in het proces presenteert de ASA nog steeds het oude certificaat, zodat de telefoons verbinding kunnen maken. Maar ze kopen een nieuw configuratiebestand dat zowel het nieuwe certificaat als het oude certificaat bevat.

Stap 8. U kunt het nieuwe certificaat nu op de ASA toepassen. Om dit te doen, hebt u de naam van het nieuwe trustpoint en de naam van de externe interface nodig, en voer dan deze opdracht met die informatie uit:

ssl trust-point asa-Identity-cert-2 buiten

Opmerking: U kunt in uw browser navigeren naar de website URL om te verifiëren dat de ASA het nieuwe certificaat presenteert. Aangezien dat adres publiekelijk bereikbaar moet zijn voor externe telefoons om het te bereiken, kan uw PC het ook bereiken. U kunt dan het certificaat controleren dat de ASA aan uw browser presenteert en bevestigen dat het de nieuwe is.

Stap 9. Zodra de ASA is geconfigureerd om het nieuwe certificaat te gebruiken, stelt u een

testtelefoon in en controleert u of er verbinding is met de ASA en het register. Als de telefoon succesvol registreert kunt u alle telefoons dan herstellen en verifiëren dat zij aan de ASA kunnen verbinden en registreren. Dit is het aanbevolen proces omdat de telefoons die op de ASA zijn aangesloten, verbonden blijven na de certificaatverandering. Als u eerst uw certificaatupdate op één telefoon test, verlaagt u het risico van een configuratieprobleem dat een groot aantal telefoons beïnvloedt. Als de eerste VPN-telefoon niet in staat is om verbinding te maken met de ASA, dan kunt u logbestanden van de telefoon en/of ASA verzamelen om problemen op te lossen terwijl de andere telefoons aangesloten blijven.

Stap 10. Zodra u hebt geverifieerd dat de telefoons met het nieuwe certificaat kunnen verbinden en registreren, kan het oude certificaat worden verwijderd van CUCM.

ASA selecteert een Elliptische curve (EC)-algoritme

ASA's ondersteunen cryptografie van de Elliptic Curve (EC) vanaf 9.4(x), zodat het algemeen voorkomt dat eerder werkende VPN-telefoons falen na een ASA upgrade naar 9.4(x) of hoger. Dit gebeurt omdat de ASA nu een EC-algoritme selecteert tijdens de TLS-handdruk met nieuwere telefoonmodellen. Meestal is er een RSA-certificaat gekoppeld aan de interface waartoe de telefoon aansluit aangezien de vorige ASA-versie de EC niet ondersteunde. Aangezien de ASA een EC-algoritme heeft geselecteerd, kan zij op dit punt geen RSA-certificaat voor de verbinding gebruiken, genereert en stuurt zij de telefoon een tijdelijk zelf-ondertekend certificaat dat zij met het EC-algoritme maakt in plaats van RSA. Aangezien dit tijdelijke certificaat niet door de telefoon wordt herkend, wordt de verbinding verbroken. Je kunt dit verifiëren in de 88xx-telefoonlogs is vrij eenvoudig.

```
2101 NOT Mar 30 12:23:21.331861 (393:393) VPNC: -protocol_handler: current cipher -> ECDHE-RSA-  
AES256-GCM-SHA384: ECDHE-RSA-AES128-GCM-SHA256: AES256-SHA: AES128-SHA  
2102 NOT Mar 30 12:23:21.331871 (393:393) VPNC: -protocol_handler: new cipher -> ECDHE-RSA-  
AES256-GCM-SHA384: ECDHE-RSA-AES128-GCM-SHA256: AES256-SHA: AES128-SHA
```

De telefoonlogs tonen aan dat de ASA een EG-algoritme voor deze verbinding heeft geselecteerd, aangezien de "nieuwe algoritme" EG-ciphers bevat, waardoor de verbinding mislukt.

In een scenario waarin AES werd geselecteerd, ziet u het volgende:

```
2691 NOT Mar 30 12:18:19.016923 (907:907) VPNC: -protocol_handler: current cipher -> ECDHE-RSA-  
AES256-GCM-SHA384: ECDHE-RSA-AES128-GCM-SHA256: AES256-SHA: AES128-SHA  
2690 NOT Mar 30 12:18:19.016943 (907:907) VPNC: -protocol_handler: new cipher -> AES256-  
SHA: AES128-SHA
```

Klik hier voor meer informatie hierover, [CSCuu02848](#).

De oplossing hiervoor zou zijn om EG-telefoons uit te schakelen op de ASA-versie voor de TLS-versie die uw telefoon gebruikt. Klik hier voor meer informatie over de TLS-versie van elk telefoonmodel:

Table 6 lists the TLS versions supported by the Cisco IP phones.

Table 6. TLS version support

Version	Phone Models			
	7900	6900, 8900, 9900	7811, 7821, 7841, 7861	8811, 8821, 8841, 8845, 8851, 8861, 8865
TLS 1.0	Yes	Yes	Yes	Yes
TLS 1.2	No	No	Yes	Yes
Disable TLS 1.0 and TLS 1.1 with https for web access*	No	No	Yes	Yes
Selectively Disable TLS cipher suites used by TLS connection or handshake**	No	No	Yes	Yes

* With 12.1 firmware

** With 12.5 firmware

<https://www.cisco.com/c/dam/en/us/products/collateral/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-c11-739097.pdf>

Zodra u weet welke TLS versies relevant zijn in uw omgeving, kunt u deze opdrachten in de ASA uitvoeren om EC-printers voor deze versies uit te schakelen:

```
ssl cipher tlsv1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-SHA256:AES128-SHA256:AES256-SHA"
ssl cipher tlsv1.1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-SHA256:AES128-SHA256:AES256-SHA"
ssl cipher tlsv1.2 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-SHA256:AES128-SHA256:AES256-SHA"
ssl cipher dtlsv1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-SHA256:AES128-SHA256:AES256-SHA"
```

Bedenk dat IP-telefoons standaard DTLS (Datagram Transport Layer Security) gebruiken, dus u moet de algoritmische verklaring voor DTLS en de relevante TLS-versie voor uw telefoons uitvoeren. Het is ook belangrijk om te begrijpen dat deze wereldwijde veranderingen op de ASA zijn, zodat ze voorkomen dat EG-ciphers worden onderhandeld door een andere AnyConnect-client die deze TLS-versies gebruikt.

TLS-aansluitingsfout

In sommige gevallen kunnen VPN-telefoons geen verbinding maken met de ASA met DTLS. Als de telefoon probeert om DTLS te gebruiken maar het faalt, blijft de telefoon DTLS over en heen proberen, zonder succes, omdat het weet dat DTLS is toegelaten U zou dit in de 88xx telefoonlogboeken zien:

```
3249 ERR Mar 29 15:22:38.949354 (385:385) VPNC: -dtls_state_cb: DTLSv0.9: write: alert: fatal:illegal parameter
3250 NOT Mar 29 15:22:38.951428 (385:385) VPNC: -vpnc_set_notify_netsd : cmd: 0x5 event: 0x40000 status: 0x0 error: 0x0
3251 ERR Mar 29 15:22:38.951462 (385:385) VPNC: -alert_err: DTLS write alert: code 47, illegal parameter
3252 ERR Mar 29 15:22:38.951489 (385:385) VPNC: -create_dtls_connection: SSL_connect ret -1, error 1
```

```

3253 ERR Mar 29 15:22:38.951506 (385:385) VPNC: -DTLS: SSL_connect: SSL_ERROR_SSL (error 1)
3254 ERR Mar 29 15:22:38.951552 (385:385) VPNC: -DTLS: SSL_connect: error:140920C5:SSL
routines:ssl3_get_server_hello:old session cipher not returned
3255 ERR Mar 29 15:22:38.951570 (385:385) VPNC: -create_dtls_connection: DTLS setup failure,
cleanup
3256 WRN Mar 29 15:22:38.951591 (385:385) VPNC: -dtls_state_cb: DTLSv0.9: write: alert:
warning:close notify
3257 ERR Mar 29 15:22:38.951661 (385:385) VPNC: -do_dtls_connect: create_dtls_connection failed
3258 ERR Mar 29 15:22:38.951722 (385:385) VPNC: -protocol_handler: connect: do_dtls_connect
failed
3259 WRN Mar 29 15:22:38.951739 (385:385) VPNC: -protocol_handler: connect : err: SSL success
DTLS fail

```

Dit kan worden veroorzaakt door hetzelfde probleem dat in het gedeelte [ASA Selecting Elliptic Curve \(EC\) Cipher](#) wordt genoemd, dus u moet ervoor zorgen dat EG-ciphers uitgeschakeld zijn voor DTLS. Afgezien daarvan kunt u DTLS in zijn geheel uitschakelen, waardoor VPN-telefoons worden gedwongen om TLS te gebruiken. Dit zou niet ideaal zijn omdat het zou betekenen dat al het verkeer TCP in plaats van UDP zou gebruiken dat wat overhead toevoegt. In sommige scenario's is dit echter een goede test, omdat het tenminste bevestigt dat het grootste deel van de configuratie prima is en het probleem specifiek is voor DTLS. Als u dit wilt testen, is het best om het op een niveau van het groepsbeleid te doen omdat beheerders normaal een uniek groep-beleid voor VPN telefoons gebruiken, dus laat dit ons een verandering testen zonder andere cliënten te beïnvloeden.

Eigenschappen van het vpn-phone-beleid voor groepsbeleid

webvp
; geen ssl dtls

Een ander gemeenschappelijk configuratieprobleem dat een succesvolle verbinding van DTLS kan verhinderen is als de telefoon de verbinding van TLS en DTLS met het zelfde algoritme niet kan vestigen. Voorbeeld logfragment:

```

##### TLS Ciphers Offered
3905 NOT Apr 01 20:14:22.741838 (362:362) VPNC: -protocol_handler: new cipher -> ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA

##### DTLS Ciphers Offered
4455 NOT Apr 01 20:14:23.405417 (362:362) VPNC: -process_connect: x-dtls-ciphersuite: AES128-SHA
4487 NOT Apr 01 20:14:23.523994 (362:362) VPNC: -create_dtls_connection: cipher list: AES128-SHA

##### DTLS connection failure
4496 WRN Apr 01 20:14:53.547046 (362:474) VPNC: -vpnc_control: conn timer expired at:1585772093,
to abort connect
4497 NOT Apr 01 20:14:53.547104 (362:474) VPNC: -abort_connect: in dtls setup phase

```

Je kunt de TLS-ciphers zien die in de eerste regel van het fragment worden aangeboden. De best beveiligde optie die door beide partijen wordt ondersteund, is geselecteerd (de logbestanden tonen de selectie niet, maar u kunt toch concluderen dat het ten minste AES-256 is van het logfragment). U kunt ook zien dat het enige DTLS-algoritme dat u hebt aangeboden, AES128 is. Aangezien het geselecteerde TLS-algoritme niet beschikbaar is voor DTLS, wordt de verbinding verbroken. De oplossing in dit scenario zou zijn om te verzekeren dat de ASA-configuratie het gebruik van dezelfde telefoons voor TLS en DTLS mogelijk maakt.

Kan geen verbinding met ASA maken na update van certificaat

Het is heel belangrijk dat u het nieuwe ASA-identiteitsbewijs als telefoon-VPN-trust op CUCM uploadt, zodat de telefoons de hash voor dit nieuwe certificaat kunnen verkrijgen. Als dit proces

niet wordt gevolgd, na de update en de volgende keer dat een VPN-telefoon probeert verbinding te maken met de ASA, wordt de telefoon aangeboden met een certificaat dat het geen vertrouwen heeft, dus de verbinding faalt. Dit kan soms dagen of weken na de ASA certificaat update voorkomen omdat de telefoons niet losgekoppeld zijn wanneer het certificaat verandert. Zolang de ASA keepalives van de telefoon blijft ontvangen, blijft de VPN-tunnel omhoog. Dus als u hebt bevestigd dat het ASA-certificaat is bijgewerkt, maar dat het nieuwe certificaat niet eerst op CUCM is aangebracht, hebt u twee opties:

1. Als het oude ASA-identiteitsbewijs nog steeds geldig is, dient u de ASA terug te draaien naar het oude certificaat en vervolgens het in dit document beschreven proces te volgen om het certificaat bij te werken. U kunt het gedeelte gegenereerd certificaat overslaan als u al een nieuw certificaat hebt gegenereerd.
2. Als het oude ASA-identiteitsbewijs is verlopen, moet u de nieuwe ASA cert naar CUCM uploaden en de telefoons terug naar het interne netwerk brengen om het bijgewerkte configuratiebestand te ontvangen met de nieuwe certificaathash.

Kan ASA URL niet via DNS oplossen

In sommige scenario's, vormt de beheerder de VPN URL met een hostname in plaats van IP adres. Wanneer dit wordt gedaan, moet de telefoon een DNS server hebben om de naam aan een IP adres te kunnen oplossen. In het fragment kunt u zien dat de telefoon probeert de naam op te lossen met zijn twee DNS-servers, 192.168.1.1 en 192.168.1.2, maar geen respons ontvangt. Na 30 seconden drukt de telefoon een 'DnsLookupErr:'

```
3816 NOT Mar 3 15:38:03.819168 VPNC: -do_login: URL -> https://asav.sckiewer.lab/phone
...
3828 INF Mar 3 15:38:03.834915 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3829 INF Mar 3 15:38:03.835004 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3830 INF Mar 3 15:38:03.835030 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3831 INF Mar 3 15:38:17.845305 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3832 INF Mar 3 15:38:17.845352 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3833 INF Mar 3 15:38:17.845373 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.2
3834 INF Mar 3 15:38:31.854834 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3835 INF Mar 3 15:38:31.854893 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3836 INF Mar 3 15:38:31.855213 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.2
3837 ERR Mar 3 15:38:32.864376 VPNC: -parse_url: gethostbyname failed <asav.sckiewer.lab>
3838 NOT Mar 3 15:38:32.864435 VPNC: -vpnc_set_notify_netsd : cmd: 0x5 event: 0x40000 status:
0x0 error: 0x0
3839 ERR Mar 3 15:38:32.864464 VPNC: -do_login: parse URL failed ->
https://asav.sckiewer.lab/phone
3840 NOT Mar 3 15:38:32.864482 VPNC: -vpn_stop: de-activating vpn
3841 NOT Mar 3 15:38:32.864496 VPNC: -vpn_set_auto: auto -> auto
3842 NOT Mar 3 15:38:32.864509 VPNC: -vpn_set_active: activated -> de-activated
3843 NOT Mar 3 15:38:32.864523 VPNC: -set_login_state: LOGIN: 1 (TRYING) --> 3 (FAILED)
3844 NOT Mar 3 15:38:32.864538 VPNC: -set_login_state: VPNC : 1 (LoggingIn) --> 3 (LoginFailed)
3845 NOT Mar 3 15:38:32.864561 VPNC: -vpnc_send_notify: notify type: 1 [LoginFailed]
3846 NOT Mar 3 15:38:32.864580 VPNC: -vpnc_send_notify: notify code: 32 [DnsLookupErr]
3847 NOT Mar 3 15:38:32.864611 VPNC: -vpnc_send_notify: notify desc: [url hostname lookup err]
```

Dit duidt meestal op een van de volgende factoren:

1. De telefoon heeft een ongeldige DNS-server
2. De telefoon heeft geen DNS-server via DHCP ontvangen of is niet handmatig ingesteld

Om dit probleem op te lossen zijn er twee opties:

1. Controleer de configuratie op de telefoon om er zeker van te zijn dat deze een DNS-server van de DHCP-server ontvangt wanneer deze extern is en/of controleer of de DNS-server van de telefoon de naam die in de ASA-configuratie gebruikt wordt kan oplossen
2. Verandert de URL in de ASA configuratie en CUCM in een IP-adres zodat DNS niet nodig is

Telefoon schakelt VPN niet in

Zoals eerder in dit document vermeld, veroorzaakt Auto Network Detect de telefoon om de TFTP-server te pingelen en om te controleren of er een reactie is. Als de telefoon op het interne netwerk is, dan is de TFTP server bereikbaar zonder VPN, dus wanneer de telefoon reacties op de pings ontvangt, schakelt het VPN niet in. Wanneer de telefoon NIET op het interne netwerk is, ontbreken de pings, zodat de telefoon dan VPN in staat zou stellen en verbinding met de ASA zou maken. Houd in gedachten dat het thuisnetwerk van een client waarschijnlijk niet is geconfigureerd om de telefoon een optie 150 te bieden via DHCP en de ASA kan ook geen optie 150 bieden, dus 'Alternate TFTP' is een vereiste voor VPN-telefoons.

In de blogs wilt u een paar dingen controleren:

1. Is de telefoon het CUCM TFTP server IP?
2. Ontvang de telefoon een reactie op de pings?
3. Maakt de telefoon VPN mogelijk nadat het geen antwoord op de pings ontvangt?

Het is belangrijk om deze items in deze volgorde te bekijken. In een scenario waar de telefoon het verkeerde IP indrukt en een reactie ontvangt, zou het zinloos zijn om Debugs in de ASA toe te laten omdat de telefoon VPN niet zal toelaten. Bevestig deze 3 dingen in deze volgorde zodat u onnodige loganalyse kunt voorkomen. U ziet dit in de 88xx-telefonische logbestanden als ping mislukt en VPN daarna wordt ingeschakeld:

```
5645 NOT Mar 27 11:32:34.630109 (574:769) JAVA-vpnAutoDetect: ping time out
5647 DEB Mar 27 11:32:34.630776 (710:863) JAVA-configmgr MQThread|cip.vpn.VpnStateHandler:? -
VpnStateHandler: handleVPN_ENABLED_STATE()
```

Telefoonregisters maar kan gespreksgeschiedenis niet weergeven

Controleer dat de telefoon Alternatief TFTP en de juiste TFTP IP ingesteld heeft. Alternatieve TFTP is een vereiste voor VPN-telefoons omdat de ASA optie 150 niet kan leveren.

Gerelateerde informatie

- [Technische ondersteuning en documentatie – Cisco Systems](#)