

Configuración y resolución de problemas de teléfonos VPN

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Configuración ASA](#)

[Configuración de CUCM](#)

[Troubleshoot](#)

[Datos a recopilar](#)

[Problemas comunes](#)

[Actualización del certificado de identidad autofirmado de ASA](#)

[ASA selecciona el cifrado de curva elíptica \(EC\)](#)

[Falla de conexión DTLS](#)

[El teléfono no se puede conectar al ASA después de la actualización del certificado](#)

[El teléfono no puede resolver la URL de ASA a través de DNS](#)

[El teléfono no habilita VPN](#)

[Registro del teléfono pero no se puede mostrar el historial de llamadas](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar y resolver problemas de la función de teléfono VPN de Cisco IP Phones y Cisco Unified Communications Manager.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Communications Manager (CUCM)
- Dispositivo de seguridad adaptable (ASA) de Cisco
- Red privada virtual (VPN) de AnyConnect
- Teléfonos IP de Cisco

Componentes Utilizados

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El entorno de prueba en este artículo incluye un 8861, ASAv y CUCM 11.5.1, pero hay muchas variaciones diferentes de estos productos que podría utilizar. Debe comprobar la Lista de funciones del teléfono en CUCM para asegurarse de que el modelo del teléfono admite la función VPN. Para utilizar la lista de funciones del teléfono, acceda al editor de CUCM en su navegador y navegue hasta **Cisco Unified Reporting > Unified CM Phone Feature List**. Genere un nuevo informe y, a continuación, seleccione su modelo de teléfono en el menú desplegable. A continuación, debe buscar la sección Funciones de lista para Virtual Private Network Client, como se muestra en la imagen:

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

Configurar

Los teléfonos VPN requieren que tenga la configuración adecuada en su ASA y CUCM. Podría comenzar con cualquiera de los productos primero, pero este documento trata primero la configuración de ASA.

Configuración ASA

Paso 1. Verifique que ASA tenga licencia para admitir AnyConnect para teléfonos VPN. El comando **show version** en el ASA se puede utilizar para verificar que **Anyconnect para Cisco VPN Phone** esté habilitado como se muestra en este fragmento de código:

```
[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
```

Si esta función no está activada, debe trabajar con el equipo de licencias para obtener la licencia adecuada. Ahora que ha confirmado que su ASA admite teléfonos VPN, puede iniciar la configuración.

Nota: Todos los elementos subrayados de la sección de configuración son nombres configurables que se pueden cambiar. La mayoría de estos nombres se mencionan en otros lugares de la configuración, por lo que es importante recordar los nombres que se utilizan en estas secciones (política de grupo, grupo de túnel, etc.) porque los necesita más adelante.

Paso 2. Cree un conjunto de direcciones IP para clientes VPN. Esto es similar a un conjunto DHCP en que cuando un teléfono IP se conecta al ASA recibe una dirección IP de este conjunto. El conjunto se puede crear con este comando en el ASA:

```
ip local pool vpn-phone-pool 10.10.1.1-10.10.1.254 mask 255.255.0
```

Además, si prefiere una red o máscara de subred diferente, también se puede cambiar. Una vez creado el conjunto, debe configurar una política de grupo (un conjunto de parámetros para la conexión entre el ASA y los teléfonos IP):

```
group-policy vpn-phone-policy internal
```

atributos `group-policy` `vpn-phone-policy`

`split-tunnel-policy tunnelall`

`vpn-tunnel-protocol ssl-client`

Paso 3. Debe activar AnyConnect si aún no está habilitado. Para hacer esto, necesita conocer el nombre de la interfaz externa. Normalmente, esta interfaz se denomina **outside** (como se muestra en el fragmento de código), pero es configurable, por lo que asegúrese de confirmar que tiene la interfaz correcta. Ejecute **show ip** para ver la lista de interfaces:

```
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
```

En este entorno, la interfaz exterior se denomina **externa**, por lo que estos comandos habilitan AnyConnect en esa interfaz.

`webvpn`

`habilitar afuera`

`anyconnect enable`

Paso 4. Configure un nuevo grupo de túnel para aplicar la política de grupo creada anteriormente a cualquier cliente que se conecte en una URL específica. Observe la referencia a los nombres del conjunto de direcciones IP y la política de grupo que creó anteriormente en las líneas tercera y cuarta del fragmento de código. Si ha modificado los nombres del conjunto de direcciones IP o de la política de grupo, debe utilizar la opción Reemplazar los valores incorrectos con los nombres modificados:

`tunnel-group vpn-phone-group type remote-access`

`tunnel-group vpn-phone-group general-attribute`

`address-pool vpn-phone-pool`

`default-group-policy vpn-phone-policy`

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

`certificado de autenticación`

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

Puede utilizar una dirección IP en lugar de un nombre para el **grupo url**. Esto suele hacerse si los teléfonos no tienen acceso a un servidor DNS que pueda resolver el nombre de dominio completo (FQDN) del ASA. Además, puede ver que este ejemplo utiliza autenticación basada en certificados. También tiene la opción de utilizar la autenticación de nombre de usuario/contraseña, pero hay más requisitos en el ASA que están fuera del alcance de este documento.

En este ejemplo, el servidor DNS tiene el registro A, **asav.sckiewer.lab - 172.16.1.250** y puede ver en la salida **show ip** que se configura 172.16.1.250 en la interfaz denominada **outside**. Así que la configuración sería:

crypto ca trustpoint asa-identity-cert

propio de inscripción

subject-name CN=asav.sckiewer.lab

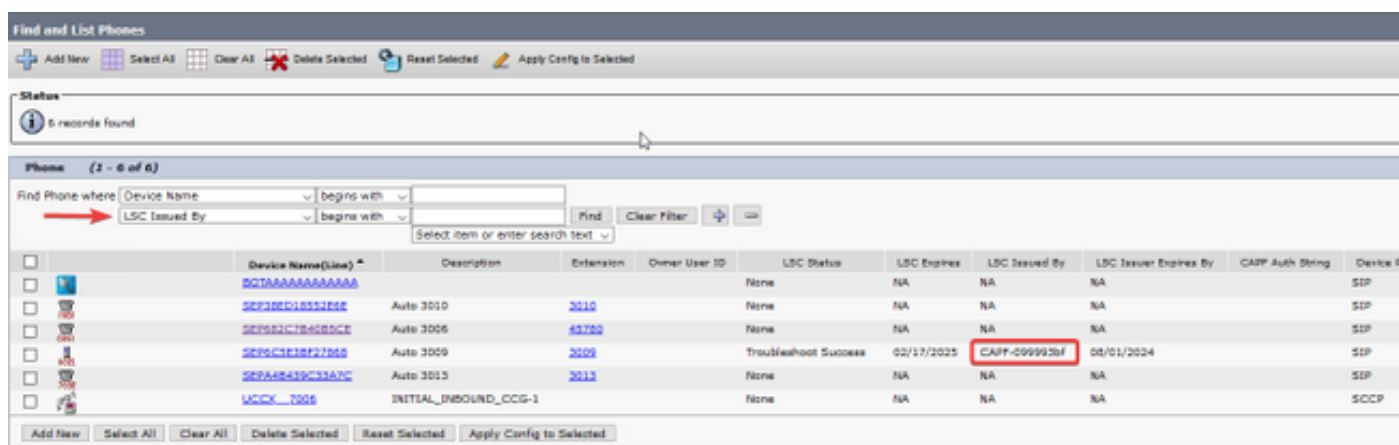
crypto ca enroll asa-identity-cert

ssl trust-point asa-identity-cert afuera

Algunas cosas a tener en cuenta:

1. Se ha creado un nuevo punto de confianza llamado asa-identity-cert y se le ha aplicado un nombre de asunto. Esto hace que el certificado generado desde este punto de confianza utilice el nombre de asunto especificado
2. A continuación, el comando 'crypto ca enroll asa-identity-cert' permite al ASA generar un certificado autofirmado y guardarlo en ese punto de confianza
3. Por último, ASA presenta el certificado en el punto de confianza a cualquier dispositivo que se conecte a la interfaz exterior

Paso 5. Cree los puntos de confianza necesarios para permitir que el ASA confíe en el certificado del teléfono IP. En primer lugar, debe determinar si los teléfonos IP utilizan el certificado instalado por el fabricante (MIC) o el certificado de importancia local (LSC). De forma predeterminada, todos los teléfonos utilizan su MIC para conexiones seguras a menos que se instale un LSC en ellos. En CUCM 11.5.1 y posterior, puede realizar una búsqueda en **Unified CM Administration > Device > Phone** para ver si los LSC están instalados mientras que las versiones anteriores de CUCM requieren que verifique físicamente la configuración de seguridad en cada teléfono. En CUCM 11.5.1, observe que necesita agregar un filtro (o cambiar el filtro predeterminado) a **LSC Emitido por**. Los dispositivos con **NA** en la **columna LSC Emitido por** utilizan el MIC ya que no tienen un LSC instalado.



The screenshot shows the 'Find and List Phones' interface in CUCM. The search criteria are set to 'LSC Issued By' begins with 'CAPF-099993bf'. The table below shows the results of this search.

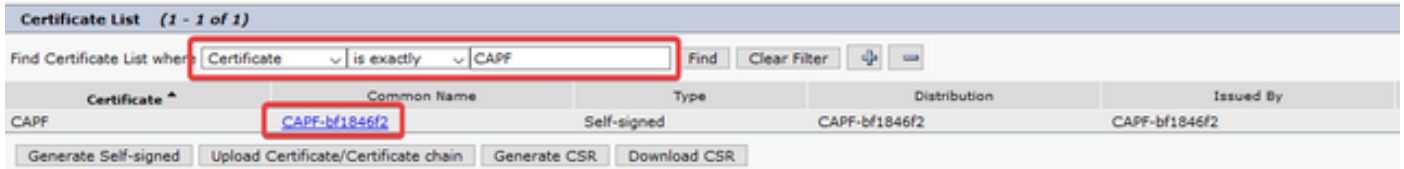
Phone	Device Name(Lines)	Description	Extension	Owner User ID	LSC Status	LSC Expires	LSC Issued By	LSC Issuer Expires By	CAPF Auth String	Device P
<input type="checkbox"/>	SCT6AAAAA				None	NA	NA	NA		SIP
<input type="checkbox"/>	SEP38EC183318E	Auto 3010	3010		None	NA	NA	NA		SIP
<input type="checkbox"/>	SEP381C78608CE	Auto 3006	43780		None	NA	NA	NA		SIP
<input type="checkbox"/>	SEP3C3F3F27860	Auto 3009	3009		Troubleshoot Success	02/17/2025	CAPF-099993bf	05/01/2024		SIP
<input type="checkbox"/>	SEP4A8439C31A7C	Auto 3013	3013		None	NA	NA	NA		SIP
<input type="checkbox"/>	UCCK_7006	INITIAL_INBOUND_CCG-1			None	NA	NA	NA		SCCP

Si el teléfono se parece al que se muestra en la imagen, debe cargar el certificado CAPF del editor de CUCM en el ASA para que el ASA valide el certificado del teléfono para la conexión segura. Si desea utilizar dispositivos sin LSC instalado, deberá cargar los certificados de fabricación de Cisco en el ASA. Estos certificados se pueden encontrar en el editor de CUCM en **Cisco Unified OS Administration > Security > Certificate Management**:

Nota: Puede ver que algunos de estos certificados se encuentran en varios almacenes de confianza (CallManager-trust y CAPF-trust). No importa de qué almacén de confianza descargue los certificados, siempre y cuando se asegure de seleccionar los que tengan

estos nombres exactos.

- Cisco_Root_CA_2048 < Raíz MIC SHA-1
- Cisco_Manufacturing_CA < MIC SHA-1 intermedio
- Cisco_Root_CA_M2 < Raíz MIC SHA-256
- Cisco_Manufacturing_CA_SHA2 < MIC SHA-256 intermedio
- CAPF del editor de CUCM < LSC



En cuanto a la MIC, los modelos de teléfonos antiguos como las series 79xx y 99xx utilizan la cadena de certificados SHA-1, mientras que los modelos de teléfonos más nuevos como la serie 88xx utilizan la cadena de certificados SHA-256. La cadena de certificados que utilizan los teléfonos debe cargarse en el ASA.

Una vez que tenga los certificados necesarios, puede crear los puntos de confianza con:

crypto ca trustpoint cert1

terminal de inscripción

crypto ca authenticate cert1

El primer comando crea un punto de confianza denominado **cert1**, y el comando **crypto ca authenticate** le permite pegar el certificado codificado base64 en la CLI. Puede ejecutar estos comandos tantas veces como sea necesario para obtener los puntos de confianza apropiados en el ASA, pero asegúrese de utilizar un nuevo nombre de punto de confianza para cada certificado.

Paso 6. Adquiera una copia del certificado de identidad ASA mediante la ejecución de este comando:

crypto ca export asa-identity-cert identity-certificate

Esto exporta el certificado de identidad para el punto de confianza denominado **asa-identity-cert**. Asegúrese de ajustar el nombre para que coincida con el punto de confianza que creó en el paso 4.

Esta es la configuración de laboratorio completa para 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

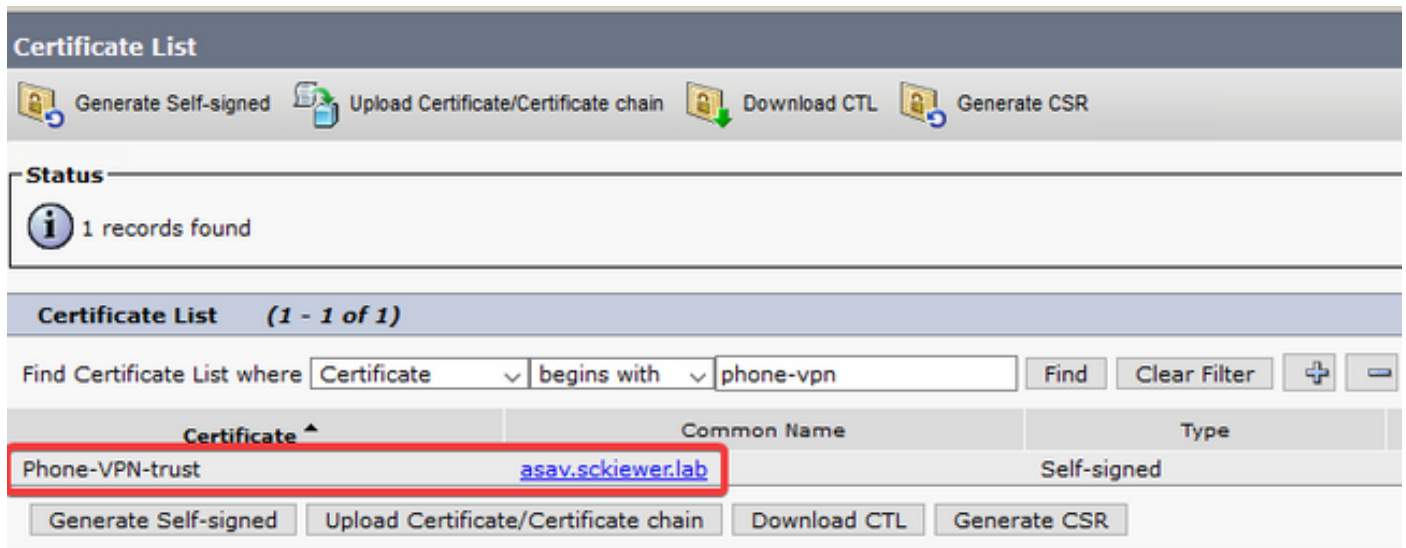
tunnel-group vpn-phone-group webvpn-attributes
  authentication certificate
  group-url https://asav.sckiewer.lab/phone enable

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

En este momento, la configuración de ASA está completa y puede continuar con la configuración de CUCM. Debe tener una copia del certificado ASA que acaba de recopilar y la URL que se configuró en la sección tunnel-group.

Configuración de CUCM

Paso 1. En CUCM, navegue hasta **Cisco Unified OS Administration > Security > Certificate Management** y cargue el certificado ASA como **phone-vpn-trust**.






The screenshot displays the 'Certificate List' interface. At the top, there are buttons for 'Generate Self-signed', 'Upload Certificate/Certificate chain', 'Download CTL', and 'Generate CSR'. Below this is a 'Status' section indicating '1 records found'. The main table has columns for 'Certificate', 'Common Name', and 'Type'. One record is listed: 'Phone-VPN-trust' with a common name of 'asav.sckiewer.lab' and a type of 'Self-signed'. Below the table are buttons for 'Generate Self-signed', 'Upload Certificate/Certificate chain', 'Download CTL', and 'Generate CSR'.


Paso 2. Una vez hecho esto, navegue hasta **Cisco Unified CM Administration > Advanced Features > VPN > VPN Profile** y cree un nuevo perfil. En esta sección no hay nada bueno o malo, sólo es importante entender el propósito de cada configuración.

1. **Enable Auto Network Detect (Activar detección automática de red)**: cuando se habilita, el teléfono hace ping a su servidor TFTP cuando se enciende. Si recibe una respuesta a este ping, no habilita VPN. Si el teléfono no recibe una respuesta a este ping, habilita VPN. Cuando se habilita esta configuración, VPN no se puede habilitar manualmente.
2. **Comprobación de ID de host**: cuando está activada, el teléfono inspecciona la URL de VPN de su archivo de configuración (<https://asav.sckiewer.lab/phone> se utiliza en este documento) y se asegura de que el nombre de host o FQDN coincide con el nombre común (CN) o una entrada SAN en el certificado presentado por el ASA.
3. **Método de autenticación** - controla qué tipo de método de autenticación se utiliza para la conexión al ASA. En el ejemplo de configuración de este documento, se utiliza la autenticación basada en certificados.
4. **Persistencia de contraseña**: si está activada, la contraseña del cliente se almacena en el teléfono hasta que se produce un intento de inicio de sesión fallido, el cliente borra manualmente la contraseña o el teléfono se restablece.

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

Paso 3. A continuación, vaya a **Cisco Unified CM Administration > Advanced Features > VPN > VPN Gateway**. Debe asegurarse de que la URL de su gateway VPN coincida con la configuración de ASA y de que mueva el certificado del cuadro superior al cuadro inferior, como se muestra en la imagen:

VPN Gateway Configuration

Save

Status
Status: Ready

VPN Gateway Information
VPN Gateway Name* asav.sckiewer.lab
VPN Gateway Description
VPN Gateway URL* https://asav.sckiewer.lab/phone

VPN Gateway Certificates
VPN Certificates in your Truststore
VPN Certificates in this Location* SUBJECT: 2.5.4.5=#130b394144563639334c50454c+1.2.840.113549.1.9.2=#160d73636b69657765722d4153417

Paso 4. Una vez guardado, debe navegar hasta **Cisco Unified CM Administration > Advanced Features > VPN > VPN Group** y mover el gateway que creó al cuadro 'Selected VPN Gateways in this VPN Group':

VPN Group Configuration

Save

Status
Status: Ready


VPN Group Information
VPN Group Name* asav.sckiewer.lab
VPN Group Description

VPN Gateway Information
All Available VPN Gateways
Selected VPN Gateways in this VPN Group: asav.sckiewer.lab


Paso 5. Ahora que se han configurado los parámetros de VPN, debe navegar hasta **Cisco Unified CM Administration > Device > Device Settings > Common Phone Profile**. Aquí, debe copiar el perfil que utiliza el teléfono VPN deseado, cambiarle el nombre y seleccionar el grupo VPN y el

perfil VPN y, a continuación, guardar el nuevo perfil:

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

Paso 6. Por último, debe aplicar este nuevo perfil al teléfono y, a continuación, restablecer el teléfono mientras se encuentra en la red interna. Esto permite al teléfono recibir toda esta nueva configuración, como el hash del certificado ASA y la URL VPN.

Nota: Antes de probar el teléfono, debe asegurarse de que los teléfonos tengan un servidor TFTP alternativo configurado. Dado que ASA no proporciona una opción 150 a los teléfonos, la IP TFTP debe configurarse manualmente en los teléfonos.

Paso 7. Pruebe el teléfono VPN y verifique que pueda conectarse correctamente al ASA y registrarse. Puede verificar que el túnel esté activo en el ASA con, **show vpn-sessiondb anyconnect**:

```
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
```

Troubleshoot

Datos a recopilar

Para resolver un problema de teléfono VPN, se recomienda estos datos:

- Depuraciones de ASA: logging buffered debuglogging debug-tracedebug crypto ca Transactions 255debug crypto ca messages 255debug crypto ca 255debug webvpn 255debug webvpn anyconnect 255
- Registros de la consola del teléfono (o un PRT si el teléfono lo admite - más información [aquí](#))

Una vez que haya reproducido el problema con las depuraciones activadas, puede ver el resultado con este comando ya que la salida de depuración siempre contiene 711001:

```
show log | i 711001
```

Problemas comunes

Nota: A los efectos de esta sección, los fragmentos de registro proceden de un teléfono 8861, ya que es una de las series telefónicas más comunes implementadas como teléfono VPN. Tenga en cuenta que otros modelos pueden escribir mensajes diferentes en los registros.

Actualización del certificado de identidad autofirmado de ASA

Antes de que caduque el certificado de identidad ASA, es necesario generar y enviar un nuevo certificado a los teléfonos. Para hacer esto sin un impacto en los teléfonos VPN, utilice este proceso:

Paso 1. Cree un nuevo punto de confianza para el nuevo certificado de identidad:

```
crypto ca trustpoint asa-identity-cert-2
```

propio de inscripción

subject-name CN=asav.sckiewer.lab

crypto ca enroll asa-identity-cert-2

Paso 2. En este momento, tendría un nuevo certificado de identidad para el ASA, pero todavía no se utiliza en ninguna interfaz. Debe exportar este nuevo certificado y cargarlo en CUCM:

crypto ca export asa-identity-cert-2 identity-certificate

Paso 3. Una vez que tenga el nuevo certificado de identidad, cárguelo en uno de sus nodos CUCM como phone-VPN-trust en **Cisco Unified OS Administration > Security > Certificate Management > Upload**.

Nota: El certificado Phone-VPN-trust actual sólo estaría presente en el nodo CUCM al que se cargó originalmente (no se propaga automáticamente a otros nodos como algunos certificados). Si su versión de CUCM se ve afectada por [CSCuo58506](#), debe cargar el nuevo certificado ASA en un nodo diferente.

Paso 4. Una vez que el nuevo certificado se carga en cualquiera de los nodos del clúster, navegue hasta **Administración de Cisco Unified CM > Funciones avanzadas > VPN > Gateway VPN** en el editor de CUCM

Paso 5. Seleccione la puerta de enlace adecuada.

Paso 6. Seleccione el certificado en el cuadro superior (éste es el que acaba de cargar) y seleccione la flecha hacia abajo para moverlo a la parte inferior (esto permite que TFTP agregue ese certificado a los archivos de configuración del teléfono VPN) y seleccione Guardar.

Paso 7. Una vez hecho esto, reinicie todos los teléfonos VPN. En este punto del proceso, el ASA todavía presenta el certificado antiguo, por lo que los teléfonos pueden conectarse, sin embargo, adquieren un nuevo archivo de configuración que contiene tanto el certificado nuevo como el certificado antiguo.

Paso 8. Ahora puede aplicar el nuevo certificado al ASA. Para hacer esto, necesita el nombre del nuevo punto de confianza y el nombre de la interfaz externa, luego ejecute este comando con esa información:

ssl trust-point asa-identity-cert-2 externa

Nota: Puede navegar hasta la URL de webvpn en su navegador para verificar que ASA presenta el nuevo certificado. Puesto que para que los teléfonos externos puedan acceder a ella, la dirección debe estar accesible públicamente, el PC también puede alcanzarla. A continuación, puede comprobar el certificado que el ASA presenta a su navegador y confirmar que es el nuevo.

Paso 9. Una vez que el ASA esté configurado para utilizar el nuevo certificado, reinicie un teléfono de prueba y verifique que pueda conectarse al ASA y registrarse. Si el teléfono se registra correctamente, puede restablecer todos los teléfonos y comprobar que pueden conectarse al ASA y registrarse. Este es el proceso recomendado porque los teléfonos conectados al ASA

permanecen conectados después del cambio del certificado. Si primero prueba la actualización del certificado en un teléfono, se reduce el riesgo de que se produzca un problema de configuración en un gran número de teléfonos. Si el primer teléfono VPN no se puede conectar al ASA, puede recopilar registros del teléfono y/o ASA para resolver problemas mientras los otros teléfonos permanecen conectados.

Paso 10. Una vez que haya verificado que los teléfonos pueden conectarse y registrarse con el nuevo certificado, el certificado antiguo se puede quitar de CUCM.

ASA selecciona el cifrado de curva elíptica (EC)

Los ASA admiten criptografía de curva elíptica (EC) a partir de la 9.4(x), por lo que es común ver que los teléfonos VPN que funcionaban anteriormente fallan después de una actualización de ASA a la 9.4(x) o superior. Esto ocurre porque el ASA ahora selecciona un cifrado EC durante el intercambio de señales TLS con modelos de teléfono más nuevos. Normalmente, hay un certificado RSA asociado a la interfaz a la que se conecta el teléfono, ya que la versión anterior de ASA no admitía EC. En este punto, dado que el ASA ha seleccionado un cifrado EC, no puede utilizar un certificado RSA para la conexión, por lo que genera y envía al teléfono un certificado temporal autofirmado que crea con el algoritmo EC en lugar de RSA. Dado que el teléfono no reconoce este certificado temporal, la conexión falla. Puede verificar esto en los registros del teléfono 88xx es bastante sencillo.

```
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
```

Los registros del teléfono muestran que el ASA seleccionó un cifrado EC para esta conexión, ya que la línea 'nuevo cifrado' contiene cifrados EC, lo que hace que la conexión falle.

En un escenario en el que se seleccionó AES, verá lo siguiente:

```
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
```

Puede encontrar más información sobre esto aquí, [CSCuu02848](#).

La solución para esto sería inhabilitar los cifrados EC en el ASA para la versión TLS que utiliza el teléfono. Puede encontrar más información sobre qué versión de TLS admite cada modelo de teléfono aquí:

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>

Una vez que sepa qué versiones de TLS son relevantes en su entorno, puede ejecutar estos comandos en el ASA para inhabilitar los cifrados EC para esas versiones:

```
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"
```

Tenga en cuenta que los teléfonos IP utilizan DTLS (seguridad de la capa de transporte del datagrama) de forma predeterminada, por lo que debe ejecutar la instrucción cipher para DTLS y la versión correspondiente de TLS para los teléfonos. Además, es importante comprender que estos cambios son cambios globales en el ASA, por lo que evitan que los códigos EC sean negociados por cualquier otro cliente de AnyConnect que utilice esas versiones de TLS.

Falla de conexión DTLS

En algunos casos, los teléfonos VPN no pueden establecer una conexión al ASA con DTLS. Si el teléfono intenta utilizar DTLS pero falla, el teléfono continúa probando DTLS una y otra vez, sin éxito, porque sabe que DTLS está habilitado. Verá esto en los registros del teléfono 88xx:

```
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

```

Esto puede ser causado por el mismo problema mencionado en la sección [Selección de Cifrado de Curva Elíptica \(EC\)](#) de ASA, por lo que debe asegurarse de que tiene los cifrados EC desactivados para DTLS. Aparte de eso, puede inhabilitar por completo DTLS, lo que obliga a los teléfonos VPN a utilizar TLS en su lugar. Esto no sería ideal, ya que significaría que todo el tráfico utilizaría TCP en lugar de UDP, lo que agrega cierta sobrecarga. Sin embargo, en algunos escenarios esta es una buena prueba ya que al menos confirma que la mayor parte de la configuración está bien y el problema es específico de DTLS. Si desea probar esto, es mejor hacerlo a nivel de política de grupo porque los administradores suelen utilizar una política de grupo única para los teléfonos VPN, por lo que esto nos permite probar un cambio sin afectar a otros clientes.

```

atributos group-policy vpn-phone-policy
webvpn
anyconnect ssl dtls none

```

Otro problema de configuración común que puede impedir una conexión DTLS exitosa es si el teléfono no puede establecer la conexión TLS y DTLS con el mismo cifrado. Ejemplo de extracto de registro:

```

%%%% 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

```

Puede ver los cifrados TLS ofrecidos en la primera línea desde el fragmento. Se selecciona la opción más segura compatible con ambos lados (los registros no muestran la selección; sin embargo, puede deducir que al menos es AES-256 del fragmento de registro). También puede ver que el único cifrado DTLS ofrecido es AES128. Dado que el cifrado TLS seleccionado no está disponible para DTLS, la conexión falla. La solución en este escenario sería asegurarse de que la configuración ASA permita que se utilicen los mismos cifrados para TLS y DTLS.

El teléfono no se puede conectar al ASA después de la actualización del certificado

Es muy importante que cargue un nuevo certificado de identidad ASA como phone-vpn-trust en CUCM para que los teléfonos puedan adquirir el hash para este nuevo certificado. Si no se sigue este proceso, después de la actualización y la próxima vez que un teléfono VPN intente conectarse al ASA, se le presentará al teléfono un certificado en el que no confía, por lo que la

conexión falla. Esto puede ocurrir a veces días o semanas después de la actualización del certificado ASA porque los teléfonos no se desconectan cuando cambia el certificado. Mientras el ASA siga recibiendo señales de mantenimiento del teléfono, el túnel VPN permanecerá activo. Por lo tanto, si ha confirmado que el certificado ASA se ha actualizado, pero el nuevo certificado no se puso primero en CUCM, tiene dos opciones:

1. Si el certificado de identidad ASA antiguo sigue siendo válido, vuelva al ASA al certificado antiguo y siga el proceso proporcionado en este documento para actualizar el certificado. Puede omitir la sección de generación de certificados si ya ha generado un nuevo certificado.
2. Si el certificado de identidad ASA antiguo ha caducado, deberá cargar el certificado ASA nuevo en CUCM y volver a colocar los teléfonos en la red interna para recibir el archivo de configuración actualizado con el nuevo hash de certificado.

El teléfono no puede resolver la URL de ASA a través de DNS

En algunos casos, el administrador configura la URL VPN con un nombre de host en lugar de una dirección IP. Cuando se hace esto, el teléfono necesita tener un servidor DNS para poder resolver el nombre en una dirección IP. En el fragmento de código, puede ver que el teléfono intenta resolver el nombre con sus dos servidores DNS, 192.168.1.1 y 192.168.1.2, pero no recibe respuesta. Después de 30 segundos, el teléfono imprime un '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]
```

Esto generalmente indica una de las siguientes:

1. El teléfono tiene un servidor DNS no válido
2. El teléfono no recibió un servidor DNS a través de DHCP o no se configuró manualmente

Para solucionar este problema hay dos opciones:

1. Verifique la configuración en el teléfono para asegurarse de que recibe un servidor DNS del servidor DHCP cuando es externo y/o verifique que el servidor DNS del teléfono pueda

resolver el nombre usado en la configuración ASA

2. Cambie la URL de la configuración ASA y CUCM a una dirección IP para que no se requiera DNS

El teléfono no habilita VPN

Como se mencionó anteriormente en este documento, Auto Network Detect hace que el teléfono haga ping al servidor TFTP y verifique si hay respuesta. Si el teléfono está en la red interna, entonces el servidor TFTP es accesible sin VPN, de modo que cuando el teléfono recibe respuestas a los pings, no habilita VPN. Cuando el teléfono NO está en la red interna, los pings fallan, por lo que el teléfono entonces habilitaría VPN y se conectaría al ASA. Tenga en cuenta que es probable que la red doméstica de un cliente no se configure para proporcionar al teléfono una opción 150 a través de DHCP, y el ASA tampoco puede proporcionar una opción 150, por lo que 'TFTP alternativo' es un requisito para los teléfonos VPN.

En los registros, desea comprobar algunas cosas:

1. ¿El teléfono hace ping a la IP del servidor TFTP de CUCM?
2. ¿El teléfono recibe una respuesta a los pings?
3. ¿El teléfono habilita VPN después de no recibir una respuesta a los pings?

Es importante ver estos elementos en este orden. En un escenario en el que el teléfono hace un ping a la IP incorrecta y recibe una respuesta, no tendría sentido habilitar los debugs en el ASA porque el teléfono no habilitará la VPN. Valide estas 3 cosas en este orden para evitar el análisis innecesario del registro. Verá esto en los registros del teléfono 88xx si el ping falla y la VPN se habilita después:

```
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()
```

Registro del teléfono pero no se puede mostrar el historial de llamadas

Verifique que el teléfono tenga el TFTP alternativo habilitado y la IP TFTP correcta configurada. TFTP alternativo es un requisito para los teléfonos VPN porque el ASA no puede proporcionar una opción 150.

Información Relacionada

- [Soporte Técnico y Documentación - Cisco Systems](#)