Aggiornamento del certificato ASA su CUCM per VPN telefono con funzione AnyConnect

Sommario

Introduzione

Questo documento descrive il processo corretto per aggiornare il certificato ASA (Adaptive Security Appliance) su Cisco Unified Communications Manager (CUCM) per i telefoni su VPN (Virtual Private Network) con la funzionalità AnyConnect, in modo da evitare l'interruzione del servizio telefonico.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- VPN telefonica con funzione AnyConnect.
- Certificati ASA e CUCM.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Unified Communications Manager 10.5.2.1590-8.
- Software Cisco Adaptive Security Appliance versione 9.8(2)20.
- Cisco IP Phone CP-8841.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

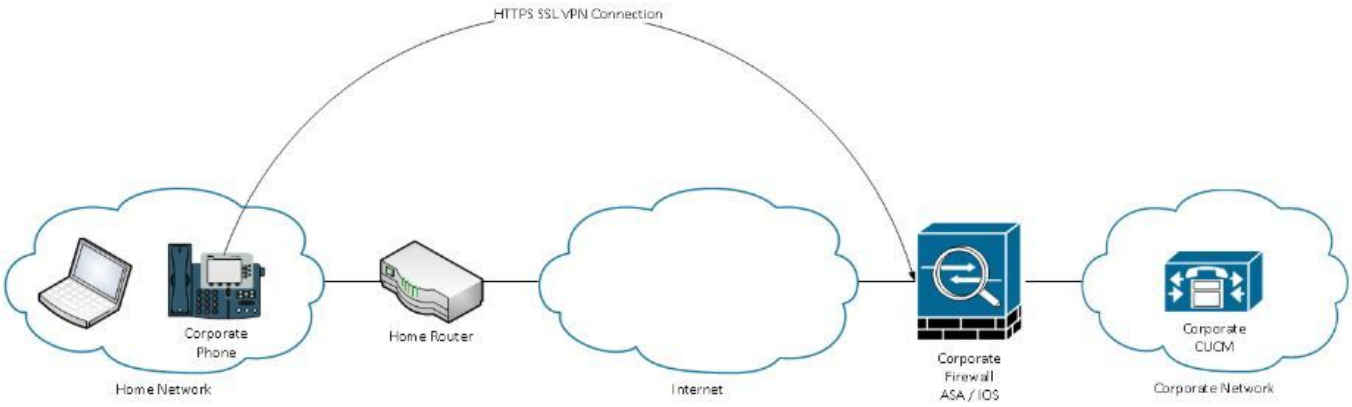
La funzionalità VPN per telefono con AnyConnect consente di fornire il servizio telefonico su una connessione VPN.

Prima che il telefono sia pronto per la VPN, è necessario eseguirne il provisioning nella rete interna. Ciò richiede l'accesso diretto al server CUCM TFTP (Trivial file transfer Protocol).

Il primo passo dopo aver configurato completamente l'ASA, è usare il certificato ASA Hypertext Transfer Protocol Secure (HTTPS) e caricarlo sul server CUCM come Phone-VPN-trust e assegnarlo al gateway VPN corretto in CUCM. In questo modo, il server CUCM può creare un file di configurazione del telefono IP che indica al telefono come raggiungere l'ASA.

È necessario effettuare il provisioning del telefono all'interno della rete prima di poterlo spostare all'esterno della rete e usare la funzionalità VPN. Dopo aver effettuato il provisioning interno, il telefono può essere spostato sulla rete esterna per l'accesso VPN.

Il telefono si connette alla porta TCP 443 sull'HTTPS all'ASA. L'ASA risponde con il certificato configurato e verifica il certificato presentato.



Come aggiornare il certificato ASA senza interrompere i servizi VPN Phone?

Ad un certo punto, il certificato ASA deve essere modificato, ad esempio in seguito a qualsiasi circostanza.

Il certificato sta per scadere

Il certificato è firmato da terze parti e la CA (Certification Authority) viene modificata, ecc

Per evitare l'interruzione del servizio sui telefoni connessi a CUCM tramite VPN con AnyConnect, è necessario seguire alcuni passaggi.

> **Attenzione:** Se i passaggi non vengono seguiti, è necessario effettuare nuovamente il provisioning dei telefoni nella rete interna prima di poterli installare in una rete esterna.

Passaggio 1. Generare il nuovo certificato ASA ma non applicarlo ancora all'interfaccia.

Il certificato potrebbe essere autofirmato o firmato dalla CA.

Nota: Per ulteriori informazioni sui certificati ASA, consultare il documento sulla configurazione dei certificati digitali

Passaggio 2. Caricare il certificato in CUCM come attendibilità della VPN del telefono nell'editore CUCM.

Accedere a Call Manager e selezionare **Unified OS Administration > Security > Certificate Management > Upload Certificate > Select Phone-VPN-trust.**

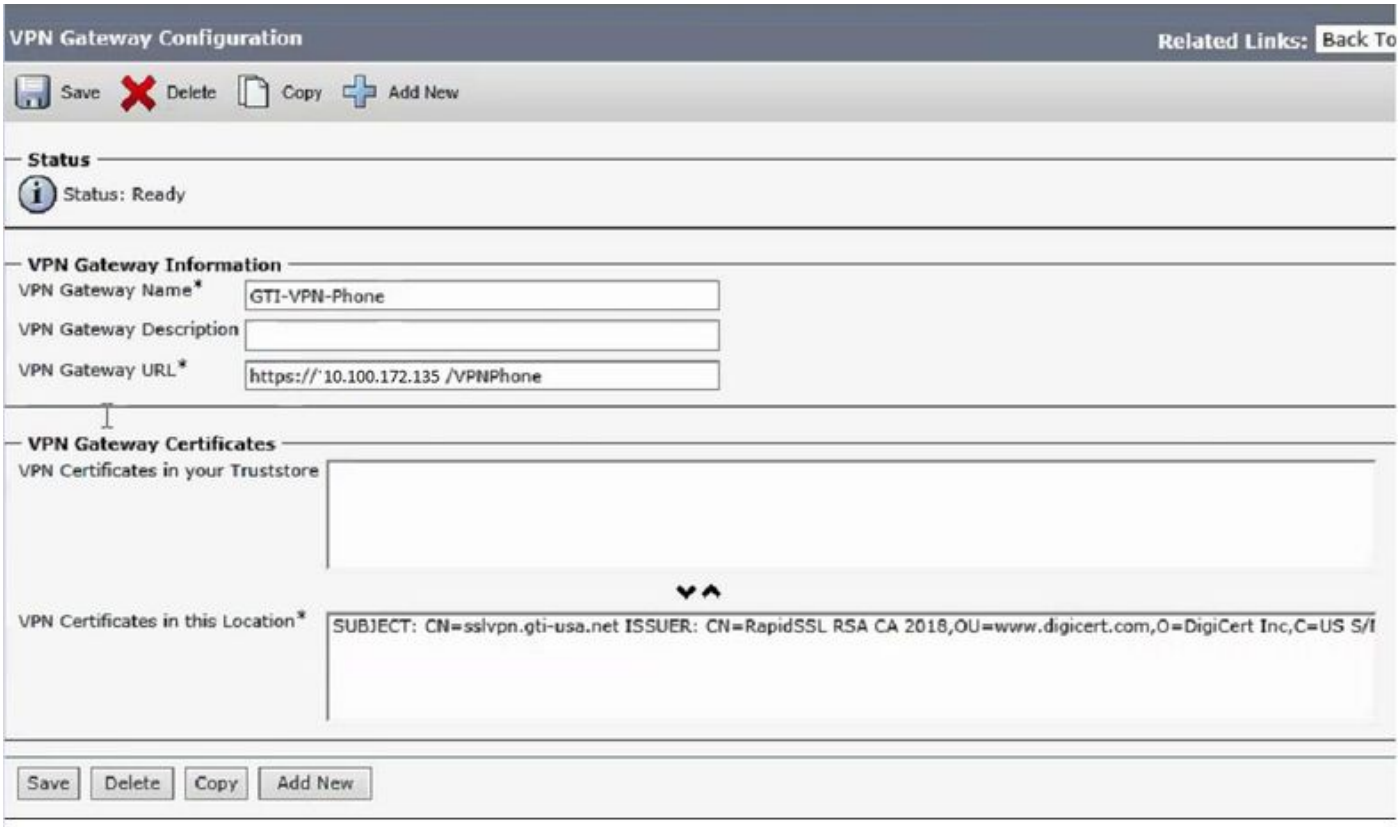
Èconsigliabile caricare la catena di certificati completa. Se i certificati radice e intermedi sono già caricati in CUCM, passare al passaggio successivo.

Attenzione: Ricorda che se il vecchio e il nuovo certificato di identità hanno lo stesso CN (Nome comune), devi seguire la soluzione per il bug CSCuh19734 al fine di evitare che il nuovo certificato sovrascriva quello precedente. In questo modo, il nuovo certificato è presente nel database per la configurazione del gateway VPN per telefono, ma quello precedente non viene sovrascritto.

Passaggio 3. Sul gateway VPN, selezionare entrambi i certificati (il vecchio e il nuovo).

Selezionare **Cisco Unified CM Administration > Advanced Features > VPN > VPN Gateway**.

Verificare di disporre di entrambi i certificati nel campo Certificati VPN in questa posizione.



Passaggio 4. Verificare che il gruppo VPN, il profilo e il profilo telefonico comune siano impostati correttamente.

Passaggio 5. Reimpostare i telefoni.

Questo passaggio consente ai telefoni di scaricare le nuove impostazioni di configurazione e garantisce che i telefoni abbiano entrambi i certificati e gli hash, in modo che possano fidarsi del vecchio e del nuovo certificato.

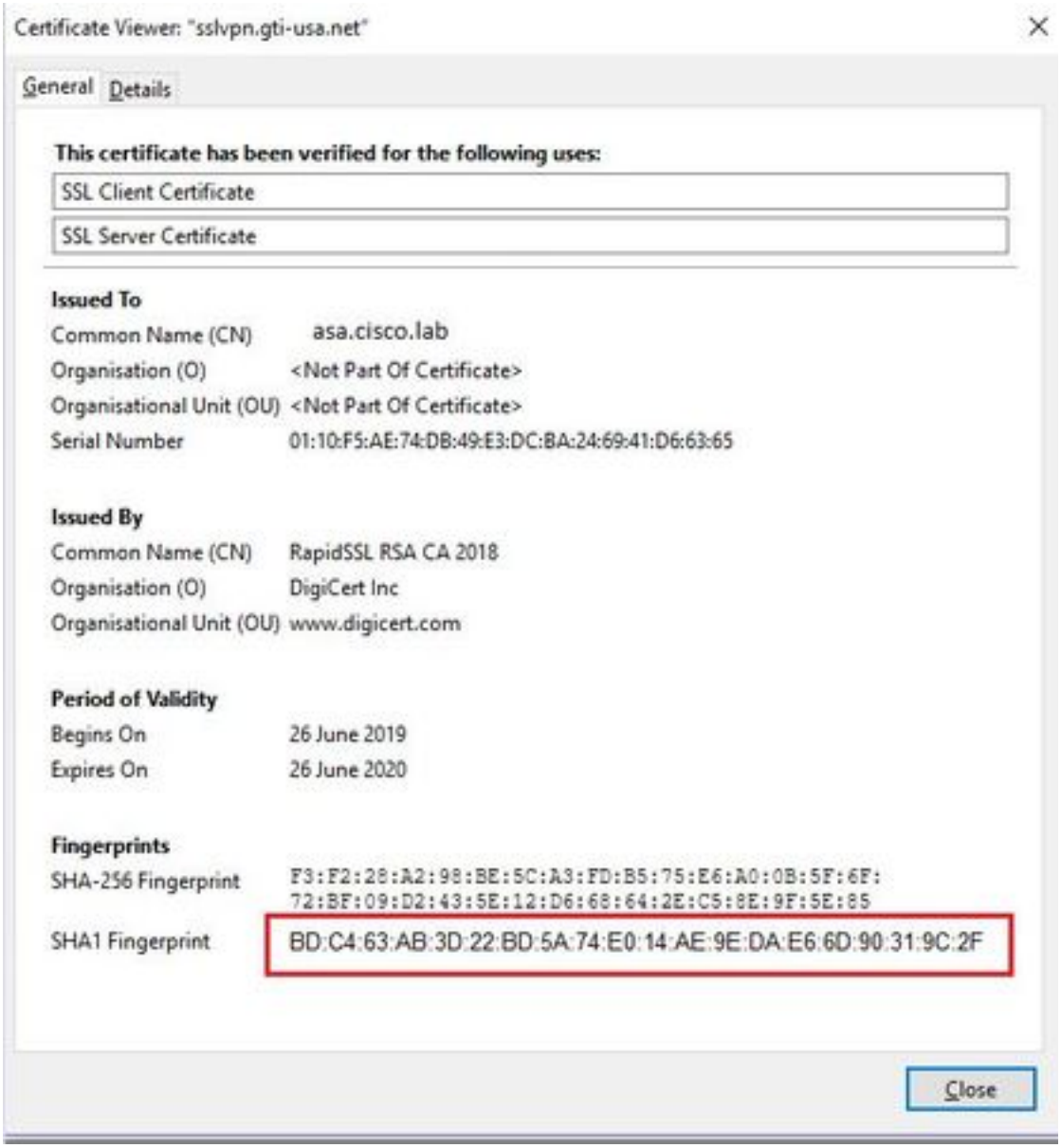
Passaggio 6. Applicare il nuovo certificato sull'interfaccia ASA.

Dopo aver applicato il certificato sull'interfaccia ASA, i telefoni devono avere fiducia nel nuovo certificato perché hanno entrambi gli hash del certificato del passaggio precedente.

Verifica

Utilizzare questa sezione per verificare di aver eseguito correttamente i passaggi.

Passaggio 1. Aprire i certificati ASA vecchi e nuovi e annotare l'impronta digitale SHA-1.



Passaggio 2. Scegliere un telefono da connettere tramite VPN e raccogliere il relativo file di configurazione.

Nota: Per ulteriori informazioni su come raccogliere il file di configurazione del telefono,

consultare Due modi per ottenere il file di configurazione di un telefono da CUCM

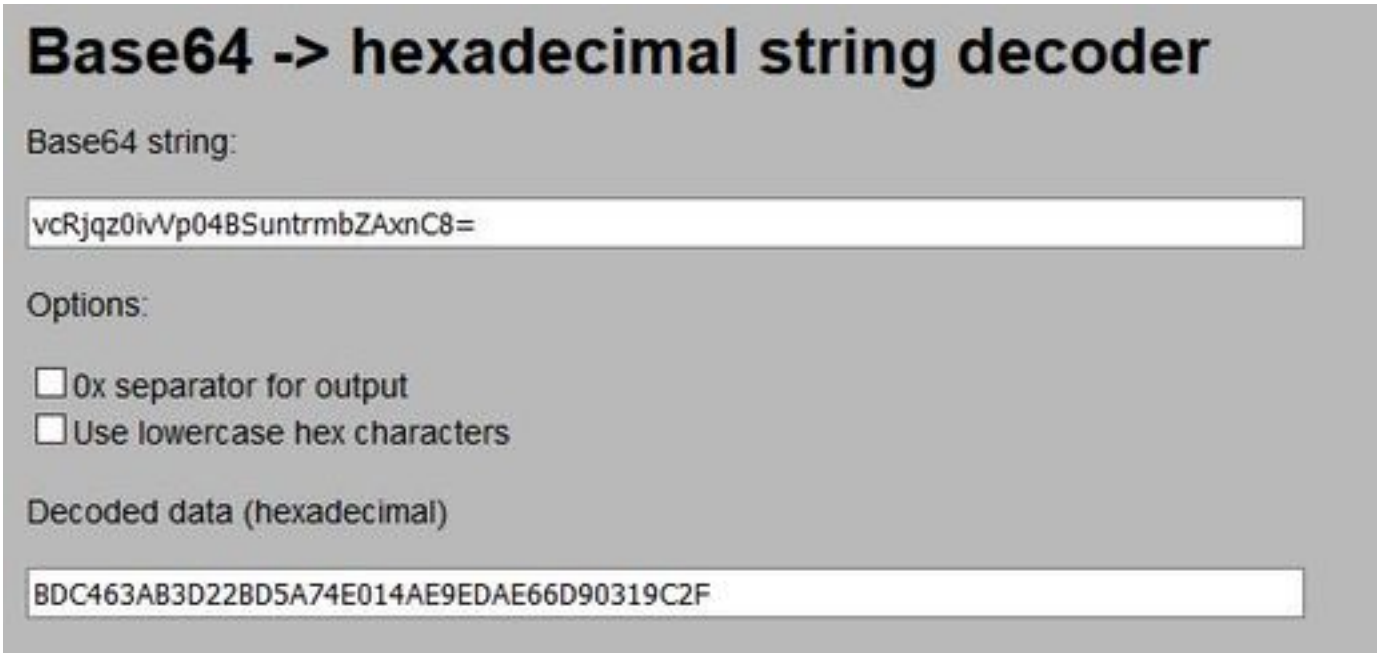
Passaggio 3. Dopo aver ottenuto il file di configurazione, cercare la sezione:

```
<vpnGroup>
<mtu>1290</mtu>
<failConnectTime>30</failConnectTime>
<authMethod>2</authMethod>
<pswdPersistent>0</pswdPersistent>
<autoNetDetect>1</autoNetDetect>
<enableHostIDCheck>0</enableHostIDCheck>
<addresses>
<url1> https://radc.cgsinc.com/Cisco_VOIP_VPN</url1>;
</addresses>
<credentials>
<hashAlg>0</hashAlg>




        </credentials>
</vpnGroup>
```

Passaggio 4. L'hash nel file di configurazione viene stampato nel formato Base 64 e nel certificato ASA viene stampato in formato esadecimale, quindi è possibile utilizzare un decodificatore da Base 64 a Esadecimale per verificare che l'hash (telefono e ASA) corrisponda.



Informazioni correlate

Per ulteriori informazioni sulla funzione AnyConnect VPN Phone:

- **Configurare i telefoni VPN AnyConnect con l'autenticazione dei certificati su un'ASA.**

https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/115785-anyconnect-vpn-00.html