Esempio di configurazione di SSLVPN con telefoni IP

Sommario

Introduzione

In questo documento viene descritto come configurare i telefoni IP su una VPN SSL (Secure Sockets Layer VPN), nota anche come WebVPN. Con questa soluzione vengono utilizzati due Cisco Unified Communications Manager (CallManager) e tre tipi di certificati. I CallManager sono:

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

I tipi di certificato sono:

- Certificati autofirmati
- Certificati di terze parti, ad esempio Entrust, Thawte e GoDaddy
- Autorità di certificazione (CA) di Cisco IOS®/Adaptive Security Appliance (ASA)

Il concetto chiave da capire è che, una volta completata la configurazione sul gateway VPN SSL e su CallManager, è necessario unirsi ai telefoni IP localmente. In questo modo i telefoni possono unirsi al CUCM e utilizzare le informazioni e i certificati VPN corretti. Se i telefoni non vengono uniti localmente, non potranno trovare il gateway VPN SSL e non disporranno dei certificati corretti per completare l'handshake VPN SSL.

Le configurazioni più comuni sono CUCM/Unified CME con certificati autofirmati ASA e certificati

autofirmati Cisco IOS. Di conseguenza, sono i più semplici da configurare.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Unified Communications Manager (CUCM) o Cisco Unified Communications Manager Express (Cisco Unified CME)
- SSL VPN (WebVPN)
- Cisco Adaptive Security Appliance (ASA)
- Tipi di certificato, ad esempio autofirmato, di terze parti e autorità di certificazione

Componenti usati

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

- Licenza ASA Premium.
- Licenza per telefoni VPN AnyConnect.
  - Per ASA release 8.0.x, la licenza è AnyConnect per Linksys Phone.
  - Per ASA release 8.2.x o successive, la licenza è AnyConnect per Cisco VPN Phone.
- Gateway VPN SSL: ASA versione 8.0 o successive (con una licenza AnyConnect per Cisco VPN Phone) o software Cisco IOS versione 12.4T o successive.
  - Il software Cisco IOS versione 12.4T o successive non è formalmente supportato come documentato nella guida alla configurazione della VPN SSL.
  - Nel software Cisco IOS versione 15.0(1)M, il gateway VPN SSL è una funzionalità di licenza basata sul numero di posti sulle piattaforme Cisco 880, Cisco 890, Cisco 1900, Cisco 2900 e Cisco 3900. Per una sessione VPN SSL riuscita è necessaria una licenza valida.
- CallManager: CUCM 8.0.1 o versione successiva oppure Unified CME 8.5 o versione successiva.

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.

Configurazione

> **Note:**
>
> per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi show. Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

Configurazione VPN SSL ASA di base

La configurazione VPN SSL ASA di base è descritta nei seguenti documenti:

- ASA 8.x: Accesso VPN con il client VPN AnyConnect utilizzando un esempio di configurazione di un certificato autofirmato
- Configurazione delle connessioni client VPN AnyConnect

Al termine della configurazione, un PC di test remoto deve essere in grado di connettersi al gateway VPN SSL, connettersi tramite AnyConnect ed eseguire il ping sul CUCM. Verificare che l'appliance ASA disponga di una licenza AnyConnect per telefoni IP Cisco. Utilizzare il comando **show ver**. Le porte TCP e UDP 443 devono essere entrambe aperte tra il gateway e il client.

Nota: La VPN SSL con carico bilanciato non è supportata per i telefoni VPN.

CUCM Configurazione VPN ASA SSL con certificati autofirmati

Per informazioni più dettagliate, fare riferimento a IP Phone SSL VPN to ASA using AnyConnect.

L'appliance ASA deve avere una licenza per AnyConnect per Cisco VPN Phone. Dopo aver configurato la VPN SSL, configurare il CUCM per la VPN.

1. Per esportare il certificato autofirmato dall'appliance ASA, usare questo comando:

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

   Con questo comando viene visualizzato un certificato di identità con codifica PEM nel terminale.
2. Copiare e incollare il certificato in un editor di testo e salvarlo come file con estensione pem. Assicurarsi di includere le righe BEGIN CERTIFICATE e END CERTIFICATE, altrimenti il certificato non verrà importato correttamente. Non modificare il formato del certificato perché ciò potrebbe causare problemi quando il telefono tenta di autenticarsi all'appliance ASA.
3. Passare a **Cisco Unified Operating System Administration > Security > Certificate Management > Upload Certificate/Certificate Chain** (Amministrazione del sistema operativo unificato Cisco > Sicurezza > Gestione certificati > Carica certificato/catena di certificati) per caricare il file del certificato nella sezione CERTIFICATE MANAGEMENT (GESTIONE CERTIFICATI) di CUCM.
4. Scaricare i certificati CallManager.pem, CAPF.pem e Cisco_Manufacturing_CA.pem dalla stessa area usata per caricare i certificati autofirmati dall'appliance ASA (vedere il passaggio 1) e salvarli sul desktop.
   1. Ad esempio, per importare CallManager.pem sull'appliance ASA, usare questi comandi:

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

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

2. Quando viene richiesto di copiare e incollare il certificato corrispondente per il trust point, aprire il file salvato da CUCM, quindi copiare e incollare il certificato con codifica Base64. Assicurarsi di includere le righe BEGIN CERTIFICATE e END CERTIFICATE (con trattini).
3. Digitare **end**, quindi premere **Invio**.
4. Quando viene richiesto di accettare il certificato, digitare **yes**, quindi premere **Invio**.
5. Ripetere i passaggi da 1 a 4 per gli altri due certificati (CAPF.pem, Cisco_Manufacturing_CA.pem) da CUCM.

5. Configurare CUCM per le configurazioni VPN corrette, come descritto in CUCM IPphone VPN config.pdf.

Nota: Il gateway VPN configurato nel CUCM deve corrispondere all'URL configurato nel gateway VPN. Se il gateway e l'URL non corrispondono, il telefono non è in grado di risolvere l'indirizzo e non verranno visualizzati debug sul gateway VPN.

- Per il CUCM: L'URL del gateway VPN è https://192.168.1.1/VPNPhone
- Sull'appliance ASA, utilizzare i seguenti comandi:

```
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
```

- Èpossibile utilizzare questi comandi in Adaptive Security Device Manager (ASDM) o nel profilo di connessione.

CUCM Configurazione di ASA SSL VPN con certificati di terze parti

Questa configurazione è molto simile a quella descritta in CUCM: Sezione ASA SSLVPN con configurazione dei certificati autofirmati, con la differenza che si utilizzano certificati di terze parti. Configurare la VPN SSL sull'appliance ASA con certificati di terze parti come descritto nell'esempio di configurazione di WebVPN con l'installazione manuale dei certificati dei fornitori di terze parti per ASA 8.x.

Nota: È necessario copiare l'intera catena di certificati dall'appliance ASA a CUCM e includere tutti i certificati intermedi e radice. Se CUCM non include la catena completa, i telefoni non dispongono dei certificati necessari per l'autenticazione e l'handshake VPN SSL non riuscirà.

Configurazione VPN SSL IOS di base

Nota: I telefoni IP sono indicati come non supportati nella VPN SSL di IOS; Le configurazioni sono a portata di mano.

La configurazione VPN SSL Cisco IOS di base è descritta nei seguenti documenti:

- Esempio di configurazione di SSL VPN Client (SVC) su IOS con SDM
- Esempio di configurazione del firewall per i criteri basati sulla zona IOS con il client VPN AnyConnect su router IOS

Al termine della configurazione, un PC di test remoto deve essere in grado di connettersi al gateway VPN SSL, connettersi tramite AnyConnect ed eseguire il ping sul CUCM. Per completare questa attività, è necessario disporre di una licenza VPN SSL valida in Cisco IOS 15.0 e versioni successive. Le porte TCP e UDP 443 devono essere entrambe aperte tra il gateway e il client.

CUCM Configurazione VPN SSL IOS con certificati autofirmati

Questa configurazione è simile a quella descritta in CUCM: ASA SSLVPN con configurazione dei certificati di terze parti e CUCM: ASA SSLVPN con sezioni di configurazione dei certificati autofirmati. Le differenze sono:

1. Utilizzare questo comando per esportare il certificato autofirmato dal router:

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

2. Utilizzare questi comandi per importare i certificati CUCM:

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

Nella configurazione del contesto WebVPN deve essere visualizzato il seguente testo:

```
gateway webvpn_gateway domain VPNPhone
```

Configurare CUCM come descritto in CUCM: Sezione Configurazione ASA SSLVPN con certificati autofirmati.

CUCM Configurazione VPN IOS SSL con certificati di terze parti

Questa configurazione è simile a quella descritta in CUCM: Sezione Configurazione ASA SSLVPN con certificati autofirmati. Configurare WebVPN con un certificato di terze parti.

> **Nota:** È necessario copiare la catena di certificati WebVPN completa in CUCM e includere tutti i certificati intermedi e radice. Se CUCM non include la catena completa, i telefoni non dispongono dei certificati necessari per l'autenticazione e l'handshake VPN SSL non riuscirà.

CME unificato: Configurazione VPN ASA/Router SSL con certificati autofirmati/certificati di terze parti

La configurazione per l'Unified CME è simile alle configurazioni del CUCM; ad esempio, le configurazioni degli endpoint WebVPN sono le stesse. L'unica differenza significativa riguarda le configurazioni dell'agente di chiamata CME unificato. Configurare il gruppo VPN e il criterio VPN per Unified CME come descritto in Configurazione del client VPN SSL per i telefoni IP SCCP.

Nota: Unified CME supporta solo il protocollo SCCP (Skinny Call Control Protocol) e non supporta il protocollo SIP (Session Initiation Protocol) per i telefoni VPN.

Nota: Non è necessario esportare i certificati da Unified CME all'ASA o al router. È necessario solo esportare i certificati dal gateway ASA o WebVPN del router al CME unificato.

Per esportare i certificati dal gateway WebVPN, fare riferimento alla sezione ASA/router. Se si utilizza un certificato di terze parti, è necessario includere l'intera catena di certificati. Per importare i certificati in Unified CME, utilizzare lo stesso metodo utilizzato per importare i certificati in un router:

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

UC 520 IP Phone con configurazione VPN SSL

Il telefono IP Cisco Unified Communications serie 500 modello UC 520 è abbastanza diverso dalle configurazioni CUCM e CME.

- Poiché il telefono IP UC 520 è sia CallManager che il gateway WebVPN, non è necessario configurare certificati tra i due.
- Configurare WebVPN su un router come se si trattasse di certificati autofirmati o di certificati di terze parti.
- Il telefono IP UC 520 ha un client WebVPN integrato ed è possibile configurarlo come un normale PC per collegarsi a WebVPN. Immettere il gateway, quindi la combinazione di nome utente e password.
- Il telefono IP UC 520 è compatibile con i telefoni IP Phone SPA 525G di Cisco Small Business.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.