SCEP legacy con esempio di configurazione CLI

Sommario

Introduzione

In questo documento viene descritto l'utilizzo del protocollo SCEP (Simple Certificate Enrollment Protocol) legacy su Cisco Adaptive Security Appliance (ASA).

> **Attenzione:** A partire dalla versione Cisco AnyConnect 3.0, questo metodo non deve essere utilizzato. In precedenza era necessario perché i dispositivi mobili non avevano il client 3.x, ma sia Android che iPhone ora hanno il supporto per il proxy SCEP, che dovrebbe essere utilizzato. Configurare SCEP legacy solo nei casi in cui non è supportato dall'appliance ASA. Tuttavia, anche in questi casi, si consiglia di aggiornare l'appliance ASA.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di SCEP legacy.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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

SCEP è un protocollo progettato per rendere la distribuzione e la revoca dei certificati digitali quanto più possibile scalabili. L'idea è che qualsiasi utente di rete standard dovrebbe essere in grado di richiedere un certificato digitale elettronicamente con un intervento minimo da parte degli amministratori di rete. Per le distribuzioni VPN che richiedono l'autenticazione dei certificati con l'organizzazione, l'autorità di certificazione (CA) o qualsiasi autorità di certificazione di terze parti che supporti SCEP, gli utenti possono ora richiedere certificati firmati dai computer client senza l'intervento degli amministratori di rete.

> **Nota:** Se si desidera configurare l'ASA come server CA, SCEP non è il metodo di protocollo corretto. Fare riferimento alla sezione CA locale del documento Cisco sulla **configurazione dei certificati digitali**.

A partire dalla versione 8.3 di ASA, sono disponibili due metodi supportati per SCEP:

- In questo documento viene illustrato il metodo precedente, denominato Legacy SCEP.
- Il metodo proxy SCEP è l'ultimo dei due metodi, dove l'ASA invia tramite proxy la richiesta di registrazione del certificato per conto del client. Questo processo è più pulito in quanto non richiede un gruppo di tunnel aggiuntivo ed è anche più sicuro. Tuttavia, lo svantaggio è che il proxy SCEP funziona solo con Cisco AnyConnect release 3.x. Ciò significa che la versione corrente del client AnyConnect per dispositivi mobili non supporta il proxy SCEP.

Configurazione

In questa sezione vengono fornite informazioni che è possibile utilizzare per configurare il metodo del protocollo SCEP legacy.

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

Di seguito sono riportate alcune note importanti da tenere presenti quando si utilizza SCEP legacy:

- Dopo che il client riceve il certificato firmato, l'ASA deve riconoscere la CA che ha firmato il certificato prima di poter autenticare il client. Pertanto, è necessario verificare che l'ASA venga registrata anche con il server CA. Il processo di iscrizione all'ASA deve essere il primo passo in quanto garantisce che:

  La CA è configurata correttamente ed è in grado di rilasciare certificati tramite SCEP se si utilizza il metodo di registrazione URL.

L'ASA è in grado di comunicare con la CA. Pertanto, se il client non può farlo, si verifica un problema tra il client e l'ASA.

- Al primo tentativo di connessione, non sarà presente un certificato firmato. Per autenticare il client è necessario utilizzare un'altra opzione.

- Nel processo di registrazione dei certificati, l'ASA non svolge alcun ruolo. Funge solo da aggregatore VPN in modo che il client possa creare un tunnel per ottenere in modo sicuro il certificato firmato. Una volta stabilito il tunnel, il client deve essere in grado di raggiungere il server CA. In caso contrario, non sarà possibile eseguire l'iscrizione.

Registrazione dell'appliance ASA

Il processo di registrazione dell'ASA è relativamente semplice e non richiede nuove informazioni. Per ulteriori informazioni su come registrare l'ASA su una CA di terze parti, consultare il documento Registrazione dell'ASA su una CA con SCEP.

Configurazione di un tunnel per l'utilizzo della registrazione

Come accennato in precedenza, per consentire al client di ottenere un certificato, è necessario creare un tunnel sicuro con l'appliance ASA usando un metodo di autenticazione diverso. A tale scopo, è necessario configurare un gruppo di tunnel utilizzato solo per il primo tentativo di connessione quando viene effettuata una richiesta di certificato. Di seguito è riportata un'istantanea della configurazione utilizzata, che definisce questo gruppo di tunnel (le linee importanti sono mostrate in ***grassetto-corsivo***):

```
rtpvpnoutbound6(config)# show run user
username cisco password ffIRPGpDSOJh9YLq encrypted privilege 0

rtpvpnoutbound6# show run group-policy gp_certenroll
group-policy gp_certenroll internal
group-policy gp_certenroll attributes
wins-server none
dns-server value <dns-server-ip-address>

vpn-tunnel-protocol ikev2 ssl-client ssl-clientless
group-lock value certenroll
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value acl_certenroll
default-domain value cisco.com
webvpn
anyconnect profiles value pro-sceplegacy type user

rtpvpnoutbound6# show run access-l acl_certenroll
access-list acl_certenroll remark to allow access to the CA server
access-list acl_certenroll standard permit host
```

```
rtpvpnoutbound6# show run all tun certenroll
tunnel-group certenroll type remote-access
tunnel-group certenroll general-attributes
```

```
address-pool ap_fw-policy
authentication-server-group LOCAL
secondary-authentication-server-group none
default-group-policy gp_certenroll
tunnel-group certenroll webvpn-attributes
authentication aaa
 group-alias certenroll enable
```

Di seguito è riportato il profilo client che può essere incollato in un file del Blocco note e importato sull'appliance ASA oppure può essere configurato direttamente con Adaptive Security Device Manager (ASDM):

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">ReconnectAfterResume
</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Disable
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
```

```
<EnableAutomaticServerSelection UserControllable="false">false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false</RetainVpnOnLogoff>
</ClientInitialization>
```

```
</AnyConnectProfile>
```

> **Nota:** Per questo gruppo di tunnel non è configurato un URL di gruppo. Questa operazione è importante perché il protocollo SCEP legacy non funziona con l'URL. È necessario selezionare il gruppo di tunnel con il relativo alias. Questo problema è causato dall'ID bug Cisco CSCtq74054. Se si verificano problemi a causa dell'URL del gruppo, potrebbe essere necessario intervenire su questo bug.

Configurare un tunnel per l'autenticazione dei certificati utente

Quando si riceve il certificato ID firmato, è possibile connettersi con l'autenticazione del certificato. Tuttavia, il gruppo di tunnel effettivo utilizzato per la connessione non è ancora stato configurato. Questa configurazione è simile a quella di qualsiasi altro profilo di connessione. Questo termine è sinonimo di gruppo tunnel e non deve essere confuso con il profilo client, che utilizza

l'autenticazione del certificato.

Di seguito è riportata un'istantanea della configurazione utilizzata per il tunnel:

```
rtpvpnoutbound6(config)# show run access-l acl_fw-policy

access-list acl_fw-policy standard permit 192.168.1.0 255.255.255.0

rtpvpnoutbound6(config)# show run group-p gp_legacyscep
group-policy gp_legacyscep internal
group-policy gp_legacyscep attributes
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value acl_fw-policy
default-domain value cisco.com
webvpn
anyconnect modules value dart

rtpvpnoutbound6(config)# show run tunnel tg_legacyscep
tunnel-group tg_legacyscep type remote-access
tunnel-group tg_legacyscep general-attributes
address-pool ap_fw-policy
 default-group-policy gp_legacyscep
tunnel-group tg_legacyscep webvpn-attributes
 authentication certificate
group-alias legacyscep enable
group-url https://rtpvpnoutbound6.cisco.com/legacyscep enable
```

Rinnova il certificato utente

Quando il certificato utente scade o viene revocato, Cisco AnyConnect non esegue l'autenticazione del certificato. L'unica opzione consiste nel riconnettersi al gruppo di tunnel di registrazione dei certificati per attivare di nuovo la registrazione SCEP.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare le informazioni contenute in questa sezione.

> **Nota:** Poiché il metodo SCEP legacy deve essere implementato solo con l'utilizzo di dispositivi mobili, in questa sezione vengono trattati solo i client mobili.

Per verificare la configurazione, effettuare i seguenti passaggi:

1. Quando si tenta di connettersi per la prima volta, immettere il nome host o l'indirizzo IP dell'appliance ASA.

2. Selezionare **certenroll** o l'alias del gruppo configurato nella sezione Configurazione di un tunnel per l'utilizzo della registrazione in questo documento. Vengono quindi richiesti nome utente e password e viene visualizzato il pulsante **get certificate** (Ottieni certificato).

3. Fare clic sul pulsante **Ottieni certificato**.

Se si controllano i log del client, questo output dovrebbe visualizzare:

```
[06-22-12 11:23:45:121] <Information> - Contacting https://rtpvpnoutbound6.cisco.com.
[06-22-12 11:23:45:324] <Warning> - No valid certificates available for authentication.
[06-22-12 11:23:51:767] <Information> - Establishing VPN session...
[06-22-12 11:23:51:879] <Information> - Establishing VPN session...
[06-22-12 11:23:51:884] <Information> - Establishing VPN - Initiating connection...
[06-22-12 11:23:52:066] <Information> - Establishing VPN - Examining system...
[06-22-12 11:23:52:069] <Information> - Establishing VPN - Activating VPN adapter...
[06-22-12 11:23:52:594] <Information> - Establishing VPN - Configuring system...
[06-22-12 11:23:52:627] <Information> - Establishing VPN...
[06-22-12 11:23:52:734]




[06-22-12 11:23:52:764]




[06-22-12 11:23:52:771]




[06-22-12 11:23:55:642]




[06-22-12 11:24:02:756]
```

Anche se nell'ultimo messaggio viene visualizzato un **errore**, è sufficiente informare l'utente che questo passaggio è necessario affinché il client venga utilizzato per il successivo tentativo di connessione, ovvero il secondo profilo di connessione configurato nella sezione Configurazione tunnel per autenticazione certificato utente di questo documento.

Informazioni correlate

- CSCtq74054 SCEP non viene avviato quando si utilizza un URL (alias asa-IP/tunnel-group)
- Documentazione e supporto tecnico