ASA 8.X: Esempio di configurazione della registrazione di AnyConnect SCEP

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Premesse Panoramica delle modifiche richieste Impostazioni XML per abilitare la funzione Anyconnect SCEP Configurazione dell'ASA per il supporto del protocollo SCEP per AnyConnect Test AnyConnect SCEP Archiviazione certificati in Microsoft Windows dopo la richiesta SCEP Risoluzione dei problemi Informazioni correlate

Introduzione

La funzionalità di registrazione di SCEP è stata introdotta nel client standalone AnyConnect 2.4. In questo processo, è possibile modificare il profilo XML di AnyConnect in modo da includere una configurazione relativa a SCEP e creare un criterio di gruppo e un profilo di connessione specifici per la registrazione dei certificati. Quando un utente AnyConnect si connette a questo gruppo specifico, AnyConnect invia una richiesta di registrazione del certificato al server CA, che a sua volta accetta o rifiuta automaticamente la richiesta.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

- Cisco ASA serie 5500 Adaptive Security Appliance con software versione 8.x
- Cisco AnyConnect VPN versione 2.4

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.

Convenzioni

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni</u> <u>dei documenti.</u>

Premesse

L'obiettivo della registrazione SCEP automatica per AnyConnect è quello di rilasciare un certificato a l client in modo sicuro e scalabile. Ad esempio, gli utenti non devono richiedere un certificato a un server CA. Questa funzionalità è integrata nel client AnyConnect. I certificati vengono rilasciati ai client in base ai parametri di certificato indicati nel file di profilo XML.

Panoramica delle modifiche richieste

La funzionalità di registrazione di AnyConnect SCEP richiede la definizione di alcuni parametri di certificato nel profilo XML. Sull'appliance ASA per la registrazione dei certificati viene creato un profilo di connessione e un criterio di gruppo e il profilo XML viene associato a tale criterio. Il client AnyConnect si connette al profilo di connessione che utilizza questo criterio specifico e invia una richiesta di certificato con i parametri definiti nel file XML. L'Autorità di certificazione (CA) accetta o nega automaticamente la richiesta. Il client AnyConnect recupera i certificati con il protocollo SCEP se l'elemento <CertificateSCEP> è definito in un profilo client.

L'autenticazione del certificato client non può essere eseguita prima che AnyConnect tenti di recuperare automaticamente i nuovi certificati, quindi se è già installato un certificato valido, la registrazione non viene eseguita.

Quando gli utenti accedono al gruppo specifico, vengono registrati automaticamente. È inoltre disponibile un metodo manuale per il recupero dei certificati in cui agli utenti viene visualizzato il pulsante **Ottieni certificato**. Questa procedura funziona solo quando il client ha accesso diretto al server CA, non attraverso il tunnel.

Per ulteriori informazioni, consultare la <u>guida all'amministrazione dei client VPN di Cisco</u> <u>AnyConnect, versione 2.4</u>.

Impostazioni XML per abilitare la funzione Anyconnect SCEP

Questi sono gli elementi importanti che devono essere definiti nel file XML di AnyConnect. Per ulteriori informazioni, consultare la <u>guida all'amministrazione dei client VPN di Cisco AnyConnect</u>, <u>versione 2.4</u>.

- <AutomaticSCEPost>: specifica il nome host ASA e il profilo di connessione (gruppo di tunnel) per cui è configurato il recupero del certificato SCEP. Il valore deve essere nel formato del nome di dominio completo dell'ASA\nome del profilo di connessione o dell'indirizzo IP dell'ASA\nome del profilo di connessione.
- <CAURL>: identifica il server CA SCEP.

- <CertificateSCEP> Definisce la modalità di richiesta del contenuto del certificato.
- <DisplayGetCertButton>: determina se nell'interfaccia utente di AnyConnect viene visualizzato il pulsante Ottieni certificato. Consente agli utenti di richiedere manualmente il rinnovo o il provisioning del certificato.

Di seguito è riportato un esempio di profilo:

```
<?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">true</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AutoConnectOnStart UserControllable="true">true</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">
     ReconnectAfterResume
   </AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">
   Automatic
 </RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Automatic
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<CertificateEnrollment>
<AutomaticSCEPHost>asa2.cisco.com/certenroll</AutomaticSCEPHost>
<CAURL PromptForChallengePW="false">
    http://10.11.11.1/certsrv/mscep/mscep.dll
   </CAURL>
<CertificateSCEP>
<Name CN>cisco</Name CN>
<Company_0>Cisco</Company_0>
<DisplayGetCertButton>true</DisplayGetCertButton>
</CertificateSCEP>
</CertificateEnrollment>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>asa2.cisco.com</HostName>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

Configurazione dell'ASA per il supporto del protocollo SCEP per AnyConnect

Per consentire l'accesso a un'Autorità di registrazione privata (RA), l'amministratore ASA deve

creare un alias con un ACL che limiti la connettività della rete lato privato all'RA desiderata. Per recuperare automaticamente un certificato, gli utenti si connettono e eseguono l'autenticazione a questo alias.

Attenersi alla seguente procedura:

- 1. Creare un alias sull'appliance ASA che punti al gruppo configurato specifico.
- 2. Specificare l'alias nell'elemento <AutomaticSCEPHost> nel profilo client dell'utente.
- 3. Allegare il profilo client contenente la sezione <CertificateEnrollment> al gruppo configurato specifico.
- 4. Impostare un ACL per il gruppo configurato specifico per limitare il traffico all'Autorità registrazione integrità del lato privato.

Attenersi alla seguente procedura:

 Caricare il profilo XML sull'appliance ASA.Scegliere VPN ad accesso remoto > Accesso di rete (client) > Avanzate > VPN SSL > Impostazioni client.In Profili client VPN SSL fare clic su Aggiungi.Fare clic su Sfoglia file locali per selezionare il file del profilo, quindi fare clic su Sfoglia Flash per specificare il nome del file flash.Fare clic su Upload File.

Remote Access VPN 🗗 🖗 🗙	Configuration > Remote Access VPN > Net	twork (Client) Access > Advanced > SSL VPN > Client Settin
 Introduction Network (Client) Access AnyConnect Connection Profiles IPsec Connection Profiles Group Policies Group Policies AnyConnect Customization/Localization 	Identify AnyConnect Client related files. AnyConnect Client Images The regular expression is used to match the u You can also minimize connection setup time b Add C Edit Delete T 4	iser-agent of a browser to an image. ay moving the image used by the most commonly encountered operation
Address Assignment Advaced	Image	Regular expression to match user-agent
Clent Bettings SSL VPN Clent Settings Clent Settings	SSL VPN Clent Profiles Add C Date Delete Name	Package
Certificate Management Language Localization DHCP Server DHCP Server Advanced	Upload Package Upload a file from local computer to f few minutes. Please wait for the ope Local File Path: scuments ar Flash File System Path: disk0:/ac_si Upload Fil	Iash file system on the device. The upload process might take a ration to finish. nd Settings\asimalik\Desktop\ac_scep Browse Local Files tep Browse Flash e Close Help

 Impostare un criterio di gruppo di registrazione certificati per la registrazione dei certificati.Scegliere VPN ad accesso remoto > Accesso client di rete > Criteri di gruppo, quindi fare clic su Aggiungi.

I	🛓 Edit Internal Group Pol	icy: cert	enroll					
	General Portal Æ-More Options	Name: Banner:	certenroll					
		More	Options					* 1
		Tunne	ing Protocols:	0	Inherit	Clientless SSL VPN	SSL VPN Client	IPsec
		Web A	CL:	ē	🗸 Inherit		× 1	Manage
		Acces:	Hours:	C	🗸 Inherit		×. 1	Manage
		Simult	aneous Logins:	E	🖌 Inherit			
		Restri	t access to VLAN:	E	🖌 Inherit		Ý	
		Conne	ction Profile (Tunnel G	iroup) Lock: [🖌 Inherit		×.	
		Maxim	um Connect Time:	E	🖌 Inherit	Unlimited	minutes	
		Idle Ti	neout:	E	🖌 Inherit	Unlimited	minutes	
	Find:		S Next	Previou	15			
			ОК	Cancel		Help		

Aggiungere un tunnel suddiviso per il server CA.Espandere **Advanced** (Avanzate), quindi selezionare **Split Tunneling**.Scegliere **Elenco reti tunnel** dal menu Criteri e fare clic su **Gestisci** per aggiungere l'elenco di controllo di accesso.

🖆 Edit Internal Group Po	licy: certenro	u						X
General Servers Advanced	Split tunneling tunneling. The of addresses (network lists security appli on the private	distinguish net iance makes sp network.	works that require olit tunneling decis	e traffic to ions on the	go through the tunn e basis of a network l	el and those that do ist, which is an ACL I	not require hat consists of list
Split Tunneling IE Browser Proxy	DNS Names:	🔽 Inherit						1
SSL VPN Client Dent	Policy:	Inherit	Tunnel Netwo	rk List Below			~	1
U I M Chin	Network List:	Inherit	scep				~	Manage
Find:	Intercept I	OHEP Config	t Provid	sage from Micro	soft Clier	nts		\$
ACL Manage	r		ок	Cancel	Help			
Standard ACL	Extended	ACL	1	li iv aids	200	11		
🔂 🕈 Add	Edit 🛅 I	Delete	+ ↓	X 🖻	-	*		
No Ad	ldress		Į	Action	Į.	Description		
Grscep								
1	10.11.11.	0/24		🖌 Permit	n (
🖻 split								
1 🛄	10.1.1.11			🌳 Permit				
<								>
		ОК		Cancel		Help	(

Selezionare SSL VPN Client, quindi scegliere il profilo per il ciclo di certificazione dal menu Profilo client da scaricare.

🔯 Edit Internal Group Pot	icy: certenroll				
General	Keep Installer on Client System:	🖌 Inherit	🔿 Yes 💫 No		
Servers Advanced	Compression:	🔽 Inherit	🔿 Enable 🛛 Disa	ble	
Split Tunneling IE Browser Proxy	Datagram TLS:	🖌 Inherit	🔿 Enable 🛛 Disa	ble	
SSL VPN Client Prec Client	Keepalive Messages:	🖌 Inherit	Disable Interval	seconds	
	MTU:	🔽 Inherit			
	Client Profile to Download:	🗌 Inherit	ac_scep		V New
	Optional Client Modules to Download:	🖌 Inherit			 v.

3. Creare un altro gruppo denominato **certauth** per l'autenticazione dei certificati.

I	🖆 Edit Internal Group Policy: certauth 🛛 🔀									
	General	Name:	certauth							
	iServers ⊛-Advanced	Banner:	🖌 Inherit							
		Address Pools:	🗸 Inherit			Sele	ct			
		IPv6 Address Pools:	🖌 Inherit			Sele	ct			
		More Options					*			
		Tunneling Protocol	5:	🗌 Inherit	Clientless SSL VPN	SSL VPN C	lient			
		IPv4 Filter:		🖌 Inherit		Ý	Mé			
		IPv6 Filter:		🗹 Inherit		~	Ma			
		NAC Policy:		🗸 Inherit		×.	Me			
		Access Hours:		🗸 Inherit		*	Ma			
		Simultaneous Login	ns:	🖌 Inherit						
		Restrict access to	VLAN:	🗸 Inherit		*				
		Connection Profile	(Tunnel Group) Lock:	🖌 Inherit		×.				
		Maximum Connect	Time:	🗸 Inherit	Unlimited	minutes				
	Find:		🔘 Next 🛛 🔘 Previ	045						
		ОК	Cancel	Help						

4. Creare un profilo di connessione Certenroll.Scegliere VPN ad accesso remoto > Accesso client di rete > Profili di connessione AnyConnect, quindi fare clic su Aggiungi.Immettere il gruppo Certenroll nel campo Alias.Nota: il nome alias deve corrispondere al valore utilizzato nel profilo AnyConnect in

AutomaticSCEPHost.

🔄 Add SSL VPN Connecti	on Profile		
Basic	Name:	certenroll	
General	Aliases:	certenrol	
	Authentication		
Secondary Authenticat	Method:	AAA Certificate Both	
Accounting	AAA Server Group:		Manage
SSL VPN		Use LOCAL if Server Group fails	
	Client Address Assignent —		
	DHCP Servers:		
	Client Address Pools:	ssl_pool	Select
	Client IPv6 Address Pools:		Select
	Default Group Policy		
	Group Policy:	Contennol	Manage
		Enable 55t: VPN Client protocol	

 Creare un altro profilo di connessione denominato certauth con autenticazione del certificato. Profilo di connessione effettivo utilizzato dopo la registrazione.

🔁 Edit SSL VPN Connecti	on Profile: certauth		×
-Advanced	Name: Aliases: Authentication Method: AAA Server Group:	certauth certauth O AAA O Certificate Both LOCAL Manage	-
	Client Address Assignent — DHCP Servers: Client Address Pools: Client IPv6 Address Pools: Default Group Policy — Group Policy:	Use LOCAL if Server Group Fails ssl_pool ssl_pool Certauth (Following field is an attribute of the group policy selected above.) Image: I	_

6. Per assicurarsi che l'uso dell'alias sia abilitato, selezionare Consenti all'utente di selezionare il profilo di connessione, identificato dall'alias, nella pagina di accesso. In caso contrario, DefaultWebVPNGroup è il profilo di connessione.

Remote Access VPN	2 0 X	Configuration > Reporte A	ccess VPN > Network (Clien	t) Access > AnyConnect Co	operation Profiles	
Introduction Network (Clent) Access AnyConnect Connection Profiles Prec Connection Profiles Group Policies Dynamic Access Policies AnyConnect Customization/Local	zation	The security appliance autor client deployment requires e Layer Security (DTLS) tunne (More client-related parame	matically deploys the Cisco Any ind-user administrative rights. T ling options. sters, such as client images and	Connect VPN Client or legacy 55 the Cisco Any-Connect VPN Clien client profiles, can be found at	L VFN Clent to remote users upon connect supports the HTTPS/TCP (SSL) and Data Clent Settings.)	ction. The initial agram Transport
Advanced Endpoint Security		Enable Cisco AnyConner	ct VPN Client or legacy SSL VPN	Client access on the interfaces	selected in the table below	
B-1 SSL VPN		Interface	Allow Access	Enable DTLS		
Client Settings		outside	Image: A start and a start	2		
Bypass incertace Access Bypass Psec	use	inside				
Easy VMN Renote Easy VMN Renote AAA(Local Users AaA(Local Users Language Localization DHCP Server DNS Advanced		Access Port: 443 Click here to <u>Assian Certific</u> Allow user to select com Allow user to select com Connection Profiles Connection profile (tunnel g Add C Edit Dele Name certenroll Sales DefaultRAGroup certauth DefaultWEEV/PNGroup	DTLS Port: 443 ate to Interface. nection profile, identified by its roup) specifies how user is auth te Enabled V V V V	alias, on the login page. Otherw enticated and other parameters Aliases certennol Sales certauth default	ise, DefaultWebVPIVGroup will be the con	nection profile.

Test AnyConnect SCEP

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

1. Avviare il client AnyConnect e connettersi al profilo del rotolo del

	ababa		
	cisco		
Connect to:	asa2.cisco.com	v 📀	
Group:	certenroll	~	
Username:	cisco		
Password:	****		
	Coppect		

richiesta di registrazione al server CA tramite



SCEP. AnyConnect passa direttamente la richiesta di registrazione e non attraversa il tunnel, se viene utilizzato il pulsante **Get Certificate** (Ottieni

🗞 Connection	🚯 Statistics 🛛 🍰 About
	alada
	CISCO
Connect to:	asa2.cisco.com
Group:	certenroll
Username:	cisco
Password:	
<u>.</u>	
	Connect Get Cert

2. Viene visualizzato questo avviso. Fare clic su Sì per installare il certificato utente e radice



3. Una volta registrato il certificato, connettersi al profilo di certificazione.

Archiviazione certificati in Microsoft Windows dopo la richiesta SCEP

Attenersi alla seguente procedura:

- 1. Fare clic su **Start > Esegui > mmc**.
- 2. Fare clic su Aggiungi/rimuovi snap-in.
- 3. Fare clic su Aggiungi e scegliere certificati.
- 4. Aggiungere i certificati **Account utente** e **Account computer**.Nell'immagine è illustrato il certificato utente installato nell'archivio certificati di Windows:

📸 Console Root\Certificates - Current User\Personal\Certificates 📃 🗖								
Console Root	^	Issued To 🖉	Issued By					
🖻 💋 Certificates - Current User		Cisco .	CA2003					
(🗄 🚞 Personal)			0.12000					
Certificates								
Trusted Root Certification Authorities								
🗄 🚞 Enterprise Trust								
🖅 🚞 Intermediate Certification Authorities								
Active Directory User Object								
🗄 🚞 Trusted Publishers								
🗄 💼 Untrusted Certificates	=							
Third-Party Root Certification Authorities								
🗄 🚞 Trusted People								
🖅 💼 Other People								
🗈 🧰 Other								
🗄 🚞 Certificate Enrollment Requests								
🗄 🧰 _NMSTR								
🗄 🧰 券								
∃								
Certificates (Local Computer)								
(🖻 📋 Personal)								
Certificates								
Trusted Root Certification Authorities								
🗄 🧰 Enterprise Trust								
🗉 🧰 Intermediate Certification Authorities								
Trusted Publishers	*	<		>				
*ersonal store contains 1 certificate.								

Nell'immagine è illustrato il certificato CA installato nell'archivio certificati di Windows:



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

- La registrazione SCEP di AnyConnect funziona solo quando l'autenticazione dei certificati non riesce. In caso contrario, controllare l'archivio certificati. Se i certificati sono già installati, eliminarli e provare di nuovo.
- La registrazione SCEP non funziona a meno che non si utilizzi il comando ssl certificateauthentication interface outside port 443.Per ulteriori informazioni, fare riferimento agli ID dei bug Cisco seguenti:Cisco Bug ID <u>CSCtf06778</u> (solo utenti <u>registrati</u>) —La registrazione AnyConnect SCEP non funziona con il certificato per gruppo Auth 2Cisco Bug ID <u>CSCtf06844</u> (solo utenti <u>registrati</u>) —Iscrizione AnyConnect SCEP non funzionante con ASA Per Group Cert Auth
- Se il server CA è all'esterno dell'appliance ASA, accertarsi di usare il comando **intra-interface** per bloccare il traffico di **sicurezza**. Aggiungere anche i comandi nat outside e access-list, come mostrato nell'esempio:

```
nat (outside) 1
access-list natoutside extended permit ip 172.16.1.0 255.255.255.0 host 171.69.89.87
Dove 172.16.1.0 è il pool AnyConnect e 171.69.89.87 è l'indirizzo IP del server CA.
```

 Se il server CA si trova all'interno, assicurarsi di includerlo nell'elenco degli accessi al tunnel suddiviso per certenroll Criteri di gruppo. In questo documento si presume che il server CA si trovi all'interno.

group-policy certenroll attributes
split-tunnel-policy tunnelspecified
split-tunnel-network-list value scep

Informazioni correlate

- Guida all'amministrazione dei client VPN di Cisco AnyConnect, versione 2.4
- Documentazione e supporto tecnico Cisco Systems