ASA 8.x: Konfigurationsbeispiel für die AnyConnect SCEP-Registrierung

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Hintergrundinformationen Übersicht der erforderlichen Änderungen XML-Einstellungen zum Aktivieren der AnyConnect SCEP-Funktion Konfigurieren der ASA zur Unterstützung des SCEP-Protokolls für AnyConnect AnyConnect SCEP testen Zertifikatsspeicherung in Microsoft Windows nach SCEP-Anforderung Fehlerbehebung Zugehörige Informationen

Einführung

Die SCEP-Anmeldungsfunktion wird in AnyConnect Standalone Client 2.4 eingeführt. Bei diesem Prozess ändern Sie das AnyConnect XML-Profil, um eine SCEP-bezogene Konfiguration einzuschließen, und erstellen eine bestimmte Gruppenrichtlinie und ein bestimmtes Verbindungsprofil für die Zertifikatregistrierung. Wenn ein AnyConnect-Benutzer eine Verbindung zu dieser bestimmten Gruppe herstellt, sendet AnyConnect eine Zertifikatsanmeldungsanfrage an den CA-Server, und der CA-Server akzeptiert oder verweigert die Anforderung automatisch.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Adaptive Security Appliances der Serie ASA 5500 mit Softwareversion 8.x
- Cisco AnyConnect VPN Version 2.4

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten

Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Ziel der automatischen SCEP-Registrierung für AnyConnect ist die sichere und skalierbare Ausstellung eines Zertifikats für den Client. Beispielsweise müssen Benutzer kein Zertifikat von einem CA-Server anfordern. Diese Funktion ist im AnyConnect-Client integriert. Die Zertifikate werden den Clients basierend auf den in der XML-Profildatei erwähnten Zertifikatsparametern ausgestellt.

Übersicht der erforderlichen Änderungen

Für die SCEP-Registrierung bei AnyConnect müssen bestimmte Zertifikatsparameter im XML-Profil definiert werden. Auf der ASA wird eine Gruppenrichtlinie und ein Verbindungsprofil für die Zertifikatsregistrierung erstellt, und das XML-Profil ist dieser Richtlinie zugeordnet. Der AnyConnect-Client stellt eine Verbindung zum Verbindungsprofil her, das diese spezifische Richtlinie verwendet, und sendet eine Anforderung für ein Zertifikat mit den Parametern, die in der XML-Datei definiert sind. Die Zertifizierungsstelle (Certificate Authority, CA) akzeptiert oder verweigert die Anfrage automatisch. Der AnyConnect-Client ruft Zertifikate mit dem SCEP-Protokoll ab, wenn das <CertificateSCEP>-Element in einem Clientprofil definiert ist.

Die Client-Zertifikatsauthentifizierung muss fehlgeschlagen sein, bevor AnyConnect versucht, die neuen Zertifikate automatisch abzurufen. Wenn Sie also bereits ein gültiges Zertifikat installiert haben, erfolgt die Registrierung nicht.

Wenn sich Benutzer bei der bestimmten Gruppe anmelden, werden sie automatisch registriert. Es gibt auch eine manuelle Methode zum Abrufen von Zertifikaten, bei der Benutzern eine Schaltfläche **Zertifikat abrufen** angezeigt wird. Dies funktioniert nur, wenn der Client direkten Zugriff auf den CA-Server hat, nicht über den Tunnel.

Weitere Informationen finden Sie im <u>Administratorhandbuch für den Cisco AnyConnect VPN-Client, Version 2.4</u>.

XML-Einstellungen zum Aktivieren der AnyConnect SCEP-Funktion

Dies sind die wichtigen Elemente, die in der XML-Datei von AnyConnect definiert werden müssen. Weitere Informationen finden Sie im <u>Administratorhandbuch für den Cisco AnyConnect VPN-</u> <u>Client, Version 2.4</u>.

 <AutomaticSCEPHost> - Gibt den ASA-Hostnamen und das Verbindungsprofil (Tunnelgruppe) an, für die der SCEP-Zertifikatsabruf konfiguriert ist. Der Wert muss im Format des vollqualifizierten Domänennamens des ASA\Connection-Profilnamens oder der IP-Adresse des ASA\Connection-Profilnamens sein.

- <CAURL> Identifiziert den SCEP CA-Server.
- <CertificateSCEP>: Definiert, wie der Inhalt des Zertifikats angefordert wird.
- <DisplayGetCertButton>: Bestimmt, ob die AnyConnect-GUI die Schaltfläche Zertifikat abrufen anzeigt. Benutzer können die Verlängerung oder Bereitstellung des Zertifikats manuell beantragen.

Hier ein Beispielprofil:

```
<?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_O>Cisco</Company_O>
<DisplayGetCertButton>true</DisplayGetCertButton>
</CertificateSCEP>
</CertificateEnrollment>
</ClientInitialization>
<ServerList>
<HostEntrv>
<HostName>asa2.cisco.com</HostName>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

Konfigurieren der ASA zur Unterstützung des SCEP-Protokolls

für AnyConnect

Um den Zugriff auf eine private Registrierungs-Authority (RA) zu ermöglichen, muss der ASA-Administrator einen Alias erstellen, der über eine ACL verfügt, die die private Netzwerkverbindung auf das gewünschte RA beschränkt. Um ein Zertifikat automatisch abzurufen, verbinden sich Benutzer und authentifizieren sich bei diesem Alias.

Gehen Sie wie folgt vor:

- 1. Erstellen Sie einen Alias auf der ASA, um auf die spezifische konfigurierte Gruppe zu zeigen.
- 2. Geben Sie den Alias im <AutomaticSCEPHost>-Element im Clientprofil des Benutzers an.
- 3. Hängen Sie das Clientprofil, das den <CertificateEnrollment>-Abschnitt enthält, an die spezifische konfigurierte Gruppe an.
- 4. Legen Sie eine ACL für die spezifische konfigurierte Gruppe fest, um den Datenverkehr auf die private RA zu beschränken.

Gehen Sie wie folgt vor:

 Laden Sie das XML-Profil auf ASA hoch.Wählen Sie Remote Access VPN > Network (Client) access > Advanced > SSL VPN > Client settings aus.Klicken Sie unter SSL VPN-Clientprofile auf Hinzufügen.Klicken Sie auf Lokale Dateien durchsuchen, um die Profildatei auszuwählen, und klicken Sie auf Flash durchsuchen, um den Namen der Flash-Datei anzugeben.Klicken Sie auf Datei

Remote Access VPN 🗗 4	X Configuration > Remote Access VPN > N	Network (Client) Access > Advanced > SSL VPN > Client Setting		
Introduction Network (Client) Access AnyCornect Connection Profiles IPsec Connection Profiles Advanced Advanced Advanced Advanced Dippass Laterface Access List IPsec ACL Manager Clientless SSL VPN Access Easy VPN Remote AAA\Local Users Certificate Management Language Localization DHCP Server DNS Advanced	Identify AnyConnect Client related files. AnyConnect Client Images The regular expression is used to match th You can also minimize connection setup tim Add I file fait 1 Delete 1	e user-agent of a browser to an image. e by moving the image used by the most commonly encountered operation		
	Image Regular expression to match user-agent disk0:/anyconnect-win-2.4.1012-k9.pkg			
	SSE VPN Clent Profiles	Package		
	Upload a file from local computer the few minutes. Please wait for the or Local File Path: sourcerts Flash File System Path: disk0:/ac Upload	to flash file system on the device. The upload process might take a speration to finish. s and Settings\asimalik\Desktop\ac_scep Browse Local Files scep Browse Flash File Close Help		

 Richten Sie eine certenroll-Gruppenrichtlinie f
ür die Zertifikatsregistrierung ein.W
ählen Sie Remote Access VPN > Network Client Access > Group Policy (Remote-Zugriffs-VPN > Netzwerk-Client-Zugriff > Gruppenrichtlinie) aus, und klicken Sie auf Add

(Hinzufügen).

📴 Edit Internal Group Pol	icy: cert	enroll				
General Portal B-More Options	Name: Banner:	certenroll				
	More	Options				*
	Tunnel	ing Protocols:	📃 Inherit	Clientless SSL VPN	SSL VPN Client	IPsec
	Web A	CL:	🗹 Inherit		×.	Manage
	Access	Hours:	🖌 Inherit		×.	Manage
	Simulta	neous Logins:	🖌 Inherit			
	Restric	t access to VLAN:	🗹 Inherit		~	
	Conne	ction Profile (Tunnel Group) Lock:	🗹 Inherit		~	
	Maximu	um Connect Time:	🗹 Inherit	Unlimited	minutes	
	Idle Tir	neout:	🖌 Inherit	Unlimited	minutes	
Find:		Next Previ	ous			
		OK Can	:el	Help		

Fügen Sie einen Split-Tunnel für CA-Server hinzu.Erweitern Sie **Erweitert**, und wählen Sie dann **Getrenntes Tunneling aus**.Wählen Sie **unten** im Menü Richtlinien die Option Tunnel Network List (Tunnel-Netzwerkliste) aus, und klicken Sie auf **Manage (Verwalten)**, um die Zugriffskontrollliste hinzuzufügen.

🖆 Edit Internal Group Po	licy: certenroll			×
General Servers Advanced	Split tunneling network list tunneling. The security ap of addresses on the privat	s distinguish networks that require traffic pliance makes split tunneling decisions on a network.	c to go through the tunnel and those a the basis of a network list, which is	that do not require an ACL that consists of list
Split Tunneling IE Browser Proxy	DNS Names: 🔽 Inherit			
SSL VPN Client Horac Client	Policy: 🔄 Inherit	Tunnel Network List Below		~
	Network List: 🔲 Inherit	scep		Manage
Find:	• • • • • • • • • • • • • • • • • • •	oxt Provious OK Cancel He	lp	
Standard ACL	Extended ACL			
🗣 Add 👻 🗹	Edit 前 Delete	↑ ↓ 👗 🗈 🖬	1 · ·	
No Ad	dress	Action	Description	
Ģ∘scep				
1	10.11.11.0/24	🖌 Permit		
😑 split		A CARLON AND AND A CARLON AND A CARLON AND A CARLON AND A CARLON AND AND A CARLON AND AND AND AND AND AND AND AND AND AN		
1	10.1.1.11	🖌 Permit	1.	
<		Ш		
	ОК	Cancel	Help	

Wählen Sie **SSL VPN Client** aus, und wählen Sie das Profil für die Registrierung im Menü **Client Profile to Download (Client-Profil zu Download)** aus.

🔯 Edit Internal Group Poli	icy: certenroll			
General	Keep Installer on Client System:	🖌 Inherit	🔿 Yes 💫 No	
Advanced	Compression:	🖌 Inherit	🔵 Enable 🕥 Disable	
Spit Tunneing IE Browser Proxy	Datagram TLS:	🖌 Inherit	🔿 Enable 🕜 Disable	
 SSL VPN Client IPsec Client 	Keepalive Messages:	🔽 Inherit	Disable Interval: seconds	
	MTU:	🖌 Inherit		
	Client Profile to Download:	🗌 Inherit	ac_scep 💙 New	5
	Optional Client Modules to Download:	🖌 Inherit		4

3. Erstellen Sie eine weitere Gruppe mit dem Namen **certauth** für die Zertifikatsauthentifizierung.

📴 Edit Internal Group Po	licy: certauth					×
General	Name:	certauth				
Servers ⊕-Advanced	Banner:	🖌 Inherit				
	Address Pools:	🗹 Inherit			Select	
	IPv6 Address Pools:	🖌 Inherit			Select	
	More Options					*
	Tunneling Protocol	5:	🗌 Inherit	Clientless SSL VPN	SSL VPN Clie	ent
	IPv4 Filter:		🖌 Inherit		~	Mé
	IPv6 Filter:		🖌 Inherit		×	Ma
	NAC Policy:		🗸 Inherit		×	Ma
	Access Hours:		🖌 Inherit		×	Ma
	Simultaneous Login	is:	🖌 Inherit			
	Restrict access to	VLAN:	🗸 Inherit		~	
	Connection Profile	(Tunnel Group) Lock:	🗸 Inherit		×.	
	Maximum Connect	Time:	🖌 Inherit	Unlimited	minutes	
Find:		🔵 Next 🛛 🔘 Previ	ous			
	ОК	Cancel	Help			

4. Erstellen Sie ein certenroll-Verbindungsprofil.Wählen Sie Remote Access VPN > Network Client Access > AnyConnect connection connection profiles (Remotezugriffs-VPN > Netzwerkclientzugriff > AnyConnect-Verbindungsprofile) aus, und klicken Sie auf Hinzufügen.Geben Sie im Feld Aliase die Gruppe certenroll ein.Hinweis: Der Aliasname muss mit dem im AnyConnect-Profil unter AutomaticSCEPHost verwendeten Wert übereinstimmen.

🔯 Add SSL VPN Connect	ion Profile		
Basic -Advanced -General -Client Addressing -Authentication -Secondary Authentication -Authorization -Accounting -SSL VPN	Name: Aliases: Authentication t Method: AAA Server Group:	certenroll Certenrol AAA Certificate Both LOCAL Use LOCAL if Server Group fails	Manage
	Client Address Assignent — DHCP Servers: Client Address Pools: Client IPv6 Address Pools: Default Group Policy Group Policy:	ssl_pool st_certenroll (Following field is an attribute of the group policy selected above.) V Enable SSt VPN Client protocol	Select Select Manage

 Erstellen Sie ein anderes Verbindungsprofil mit dem Namen certauth mit Zertifikatauthentifizierung. Dies ist das tatsächliche Verbindungsprofil, das nach der Registrierung verwendet wird

wiiu.		
📬 Edit SSL VPN Connect	ion Profile: certauth	
-Advanced	Name: Allases: Authentication	certauth
	Method: AAA Server Group:	AAA Certificate Both LOCAL Manage Use LOCAL if Server Group fails
	Client Address Assignent — DHCP Servers: Client Address Pools: Client IPv6 Address Pools: Default Group Policy Group Policy:	ssl_pool Select Select certauth Manage (Following field is an attribute of the group policy selected above.) Following field SSL VPN Client protocol

6. Um sicherzustellen, dass die Verwendung von Alias aktiviert ist, aktivieren Sie auf der Anmeldeseite das Kontrollkästchen Verbindungsprofil, das durch seinen Alias identifiziert wird, zulassen. Andernfalls ist DefaultWebVPNGgroup das Verbindungsprofil.

emote Access VPN	9 6 X	Configuration > Remote A	ccess VPN > Network (Clien	t) Access > AnyConnect Cor	mection Profiles
Introduction Network (Clent) Access AnyConnect Connection Profile Differ Connection Profiles Group Policies Group Policies Group Policies Group Connect Customization/Loc Group Address Assomethed	s alzation	The security appliance auto client deployment requires e Layer Security (DTLS) tunne (More client-related parame	matically deploys the Cisco Any nd-user administrative rights. T ling options. sters, such as client images and	Connect VPN Clent or legacy SS. he Cisco AnyConnect VPN Clent clent profiles, can be found at §	WPN Client to remote users upon connection. The in supports the HTTPS/TCP (SSL) and Datagram Trans Sent Settings.)
Advanced		Enable Cisco AnyConne	ct VPN Client or legacy SSL VPN	Client access on the interfaces s	elected in the table below
B- A Endpoint Security		Interface	Alow Access	Enable DTLS	
Client Settings		outside			
Bypass Interface Acce	is List	inside			
Casy WW Renote AAA(tocal Users AAAA(tocal Users AAAA(tocal Users AAAA(tocal Users AAAA(tocal Users AAAA(tocal Users AAAA(tocal Users AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		Access Port: 443 Click here to <u>Assian Certific</u> Login Page Setting Allow user to select con Connection Profiles	DTLS Port: 443 ate to Interface.	alias, on the login page. Otherwi	se, DefaultWebVFNGroup will be the connection prof
		Connection profile (bunnel g	roup) specifies how user is auth te	enticated and other parameters	·
					for all concentrations and all of
		Name	Enabled	Allases	Authentication Method
		Name certenvoll	Enabled	certenvol	Authentication Method AAA(LOCAL)
		Name certenvoll Sales	Enabled	Certenvol Sales	Addentication Method Add(LoCAL) Add(LoCAL)
		Name certenroll Sales DefaultRAGroup	Enabled	alasies certenvol Sales	Authentication Method AAA(LOCAL) AAA(LOCAL) AAA(LOCAL)
		Name certenroll Sales DefaultRAGroup certauth	Enabled	alloses certenvoll Sales certauth	Authentication Method AAA(LOCAL) AAA(LOCAL) AAA(LOCAL) Certificate

AnyConnect SCEP testen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

1. Starten Sie den AnyConnect-Client, und stellen Sie eine Verbindung zum certenroll-Profil

Connection	1 Statistics 🔒 About
	CISCO
Connect to:	asa2.cisco.com 💌 🧬
Group:	certenroll
Username:	cisco
Password:	****

Registrierungsanfrage über SCEP an den CA-Server



weiter. Certificate Enrollment - Request forwarded. AnyConnect durchläuft die Registrierungsanfrage direkt und nicht über den Tunnel, wenn die Schaltfläche Zertifikat

Connection	🕄 Statistics 🛛 🍰 About
	CISCO
Connect to:	asa2.cisco.com 💉 🔗
Group:	certenroll
Username:	cisco
Password:	n na standar en
<u>X - 1857 - 185</u> E at uE at ui	

14

abrufen verwendet wird. Please enter your username and password.

2. Diese Warnung wird angezeigt. Klicken Sie auf **Ja**, um den Benutzer und das Stammzertifikat zu



3. Wenn das Zertifikat registriert ist, stellen Sie eine Verbindung zum sicheren Profil her.

Zertifikatsspeicherung in Microsoft Windows nach SCEP-Anforderung

Gehen Sie wie folgt vor:

- 1. Klicken Sie auf Start > Ausführen > MMC.
- 2. Klicken Sie auf Snap-In hinzufügen/entfernen.
- 3. Klicken Sie auf Hinzufügen, und wählen Sie Zertifikate aus.
- 4. Fügen Sie die Zertifikate **Mein Benutzerkonto** und **Computerkonto hinzu**.Dieses Bild zeigt das im Windows-Zertifikatsspeicher installierte Benutzerzertifikat:

🛍 Console Root\Certificates - Current User\Personal\Certificates 📃						
Console Root	^	Issued To 🖉	Issued By			
🖻 🝘 Certificates - Current User		Cisco	CA2003			
(🖻 🧰 Personal 🛛 🔹 🔪						
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						
	_					
⊡ 課給激口湯k						
Certificates (Local Computer)						
Personal						
Certificates						
Trusted Root Certification Authorities						
🗉 🔚 Enterprise Trust						
🕀 🚞 Intermediate Certification Authorities						
F Trusted Publishers	¥			>		
Personal store contains 1 certificate.						

Dieses Bild zeigt das im Windows-Zertifikatsspeicher installierte CA-Zertifikat:



Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

- Die SCEP-Registrierung für AnyConnect funktioniert nur, wenn die Zertifikatsauthentifizierung fehlschlägt. Wenn sie sich nicht anmeldet, überprüfen Sie den Zertifikatsspeicher. Wenn Zertifikate bereits installiert sind, löschen Sie sie und testen Sie sie erneut.
- Die SCEP-Registrierung funktioniert nur, wenn der Befehl SSL Certificate-Authentication Interface außerhalb des Ports 443 verwendet wird.Weitere Informationen finden Sie unter den folgenden Cisco Bug-IDs:Cisco Bug-ID <u>CSCtf06778</u> (nur <u>registrierte</u> Kunden) - Die Anmeldung für AnyConnect SCEP funktioniert nicht mit Auth 2 des Zertifikats pro Gruppe.Cisco Bug-ID <u>CSCtf06844</u> (nur <u>registrierte</u> Kunden) - AnyConnect SCEP-Registrierung funktioniert nicht mit ASA Pro-Group-Zertifizierung
- Wenn sich der CA-Server außerhalb von ASA befindet, stellen Sie sicher, dass das Hairpinning mit dem Befehl für den Datenverkehr mit derselben Sicherheit (permit intrainterface) zugelassen wird. Fügen Sie außerdem die Befehle nat outside und access list hinzu, wie in diesem Beispiel gezeigt:

nat (outside) 1 access-list natoutside extended permit ip 172.16.1.0 255.255.255.0 host 171.69.89.87 Dabei steht 172.16.1.0 für den AnyConnect-Pool und 171.69.89.87 für die IP-Adresse des CA-Servers.

• Wenn sich der CA-Server im Inneren befindet, stellen Sie sicher, dass dieser in die Split-Tunnel-Zugriffsliste für die **certenroll-**Gruppenrichtlinie aufgenommen wird. In diesem Dokument wird davon ausgegangen, dass sich der CA-Server im Inneren befindet.

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

Zugehörige Informationen

- Administratorhandbuch für den Cisco AnyConnect VPN-Client, Version 2.4
- <u>Technischer Support und Dokumentation Cisco Systems</u>