Unified Mobility Advanced Server-certificatie met ASA

Inhoud

Inleiding

Dit document beschrijft hoe u zelfgetekende certificaten kunt uitwisselen tussen de adaptieve security applicatie (ASA) en de Cisco Unified Mobility Advanced (CUMA) server en vice versa. Het legt ook uit hoe u de gebruikelijke problemen kunt oplossen die zich voordoen bij het importeren van de certificaten.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ASA 5500 Series Next-Generation
- Cisco Unified Mobility Advanced Server 7

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Plaatsingsscenario's

Er zijn twee inzetscenario's voor de **TLS-proxy** die wordt gebruikt door de **Cisco Mobility Advanced-**oplossing.

Opmerking: in beide scenario's verbinden de clients met internet.

1. Het adaptieve security apparaat werkt als zowel de firewall als de TLS-proxy.
2. Het adaptieve security apparaat werkt alleen als de TLS-proxy.

In beide scenario's moet u het **Cisco UMA server certificaat** en **key-pair** in **PKCS-12**-indeling exporteren en deze naar het adaptieve security apparaat importeren. Het certificaat wordt gebruikt tijdens handdruk met de Cisco UMA klanten.

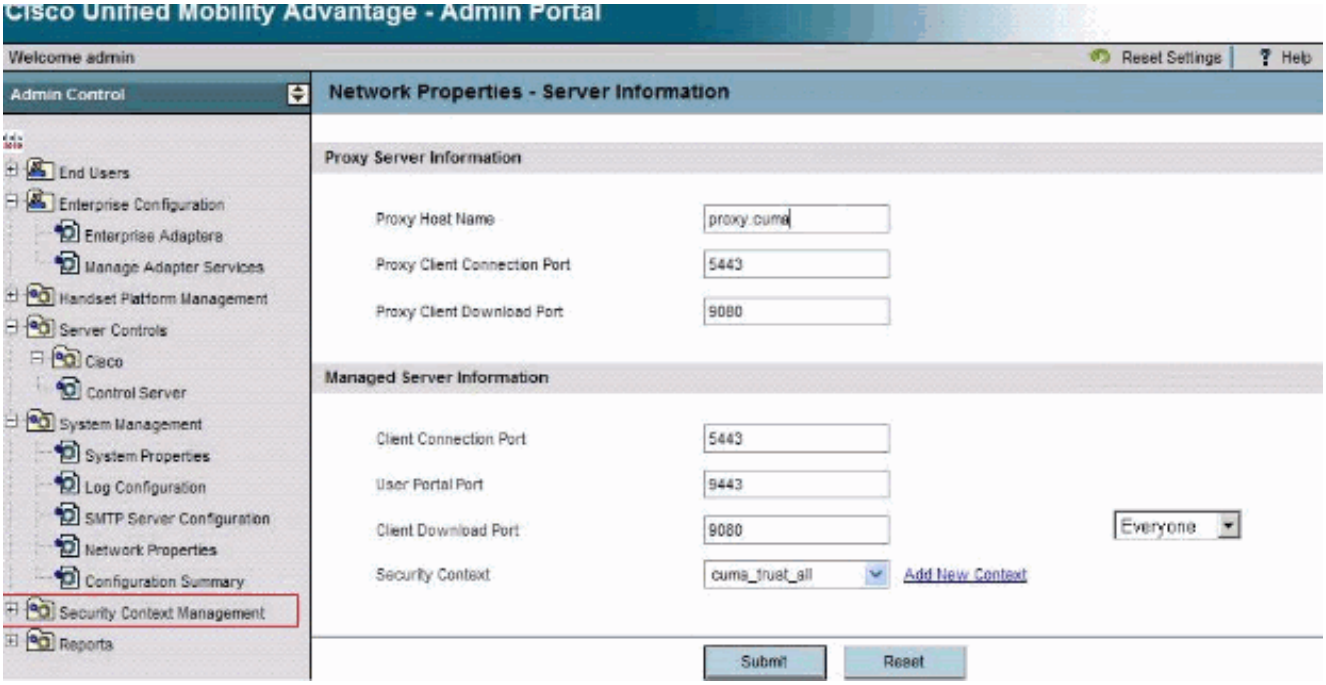
De installatie van het Cisco UMA-server met zelfgetekende certificering in de trustwinkel van het adaptieve security apparaat is nodig voor de verificatie van de Cisco UMA-server tijdens de handdruk tussen de proxy van het adaptieve security apparaat en de Cisco UMA-server.

Installeer het Cisco UMA-server met zelfgetekend certificaat

Taken die op de CUMA-server moeten worden uitgevoerd

Deze stappen moeten worden uitgevoerd op de CUMA server. Met deze stappen, creëer u een zelf-ondertekend certificaat op CUMA om met de ASA te ruilen met CN=portal.aipc.com. Dit moet op de ASA trustwinkel geïnstalleerd worden. Voer de volgende stappen uit:

1. Maak een zelf-ondertekend cert op de CUMA server.Aanmelden bij de Cisco Unified Mobility Advanced Admin-portal.Kies de **[+]** naast Security Context Management.



Kies **beveiligingscontexten**.Kies **Context toevoegen**.Voer deze informatie in:

```
Do you want to create/upload a new certificate? create
Context Name "cuma"
Description "cuma"
Trust Policy "Trusted Certificates"
Client Authentication Policy "none"
Client Password "changeme"
Server Name cuma.ciscodom.com
Department Name "vsec"
Company Name "cisco"
City "san jose"
State "ca"
Country "US"
```

2. Download de zelfgetekende certificaten van Cisco Unified Mobility Advanced. Voltooi deze stappen om de taak te volbrengen:Kies de **[+]** naast Security Context Management.Kies **beveiligingscontexten**.Kies **Context beheren** naast de beveiligingscontext waarin het certificaat moet worden gedownload.Kies **Downloadcertificaat**.**Opmerking:** Als het certificaat een ketting is en de bijbehorende wortel- of intermediaire certificaten heeft, wordt alleen het eerste certificaat in de keten gedownload. Dit is voldoende voor zelfondertekende certificaten.Sla het bestand op.
3. De volgende stap is het zelf-ondertekende certificaat van Cisco Unified Mobility Advanced aan de ASA toe te voegen. Voltooi deze stappen op de ASA:Open het zelf-ondertekende certificaat van Cisco Unified Mobility Advanced in een teksteditor.Importeer het certificaat in de Cisco adaptieve security applicatie winkel:

```
cuma-asa(config)# crypto ca trustpoint cuma-server-id-cert
cuma-asa(config-ca-trustpoint)# enrollment terminal
cuma-asa(config-ca-trustpoint)# crypto ca authenticate
cuma-server-id-cert
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

----BEGIN CERTIFICATE----
** paste the contents from wordpad **
----END CERTIFICATE----
```

4. Exporteren ASA zelf-ondertekend certificaat op CUMA server. U moet Cisco Unified Mobility Advanced configureren om een certificaat te vereisen van de Cisco adaptieve security applicatie. Voltooi deze stappen om het vereiste zelf-ondertekende certificaat te verstrekken.

Deze stappen moeten worden ondernomen op het ASA-systeem.Generate een nieuw sleutelpaar:

```
cuma-asa(config)# crypto key generate rsa label asa-id-key mod 1024

INFO: The name for the keys will be: asa-id-key

Keypair generation process begin. Please wait...
```

Voeg een nieuw betrouwbaar punt toe:

```
cuma-asa(config)# crypto ca trustpoint asa-self-signed-id-cert

cuma-asa(config-ca-trustpoint)# keypair asa-id-key

cuma-asa(config-ca-trustpoint)# enrollment self
```

Geef het trustpunt op:

```
cuma-asa(config-ca-trustpoint)# crypto ca enroll asa-self-signed-id-cert
% The fully-qualified domain name in the certificate will be:
cuma-asa.cisco.com
% Include the device serial number in the subject name? [yes/no]: n
Generate Self-Signed Certificate? [yes/no]: y
```

Het certificaat exporteren naar een tekstbestand.

```
cuma-asa(config)# crypto ca export asa-self-signed-id-cert
identity-certificate
The PEM encoded identity certificate follows:

-----BEGIN CERTIFICATE-----

Certificate data omitted

-----END CERTIFICATE-----
```

5. Kopieert de vorige uitvoer naar een tekstbestand en voegt deze toe aan de CUMA server trust store en gebruikt deze procedure:Kies de **[+]** naast Security Context Management.Kies **beveiligingscontexten**.Kies **Context beheren** naast de beveiligingscontext waarin u het ondertekende certificaat importeert.Kies **Importeren** in de balk Betrouwbare certificaten.Plakt de certificaattekst.Geef het certificaat een naam.Kies **Importeren**.**Opmerking:** Voor de configuratie van de afstandsbediening, bel dan naar de tafeltelefoon om te bepalen of de mobiele telefoon op hetzelfde moment draait. Dit zou bevestigen dat de mobiele verbinding werkt en dat er geen probleem is met de configuratie van de afstandsbediening.

Problemen bij het toevoegen van het CUMA-certificaatverzoek aan andere certificeringsinstanties

Probleem 1

Veel demo-/prototype-installaties waar deze helpen als de CUMC/CUMA-oplossing met vertrouwde certificaten werkt, zelf-ondertekend zijn of van *andere certificeringsinstanties* worden verkregen. Goedkeuringscertificaten zijn duur en het duurt lang voordat ze worden afgegeven. Het is goed als de oplossing zelfgetekende certificaten en certificaten van andere CA's ondersteunt.

De huidige ondersteunde certificaten zijn GeoTrust en Versizing. Dit is gedocumenteerd in Cisco bug-ID CSCta62971 (alleen geregistreerde klanten)

Fout: Kan geen verbinding maken

Wanneer u probeert om de pagina van het gebruikersportal te openen, bijvoorbeeld `https://<host>:8443`, `verschijnt` de foutmelding `Kan geen verbinding maken.`

Oplossing

Dit probleem is gedocumenteerd in Cisco bug-ID CSCsm26730 (alleen geregistreerde klanten). Voltooi de volgende bewerking om de pagina met een gebruikersportal te openen:

De oorzaak van deze kwestie is het dollarteken, zodat kunt u het dollarteken met een ander dollarteken in het **bestand server.xml** van de beheerde server **ontvluchten**. Bijvoorbeeld, bewerk/opt/cuma/jbaas-4.0.1sp1/server/cuma/deploy/jbossweb-tomcat50.sar/server.xml.

In de regel: **keystorePass="pa$woord"** maxSpareThreads="15"

Vervang het `$` teken met `$$`. Het lijkt op **keystorePass="pa$$woord"** maxSpareThreads="15".

Sommige pagina's in CUMA Admin Portal zijn niet toegankelijk

Deze pagina's kunnen niet in het **CUMA Admin Portal** worden bekeken:

- gebruiker in- en uitschakelen
- opsporing/onderhoud

Als de gebruiker op een van de twee bovengenoemde pagina's in het menu links klikt, lijkt de browser aan te geven dat de pagina een pagina laadt, maar er gebeurt niets (alleen de vorige pagina die in de browser was, is zichtbaar).

Oplossing

Om deze kwestie met betrekking tot gebruikerspagina op te lossen, wijzigt u de poort die voor Active Directory wordt gebruikt in **3268** en start u CUMA opnieuw.

Gerelateerde informatie

- ASA 5000-CUMA proxy voor stapsgewijze configuratie
- Inleiding over al ASR 5000 v1
- Verbetering in Cisco Unified Mobility Advanced
- Ondersteuning voor spraaktechnologie
- Productondersteuning voor spraak en Unified Communications
- Technische ondersteuning en documentatie – Cisco Systems