Zertifizierungsproblem für Unified Mobility Advantage Server mit ASA

Inhalt

Einleitung

Dieses Dokument beschreibt den Austausch selbstsignierter Zertifikate zwischen der Adaptive Security Appliance (ASA) und dem Cisco Unified Mobility Advantage (CUMA)-Server und umgekehrt. Außerdem wird erklärt, wie die gängigen Probleme behoben werden, die beim Importieren der Zertifikate auftreten.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Serie ASA 5500

- Cisco Unified Mobility Advantage Server 7

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

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

Bereitstellungsszenarien

Es gibt zwei Bereitstellungsszenarien für den **TLS-Proxy**, der von der **Cisco Mobility Advantage**-Lösung verwendet wird.

Hinweis: In beiden Szenarien stellen die Clients eine Verbindung mit dem Internet her.

1. Die Adaptive Security Appliance fungiert als Firewall- und TLS-Proxy.
2. Die Adaptive Security Appliance fungiert nur als TLS-Proxy.

In beiden Szenarien müssen Sie das **Cisco UMA-Serverzertifikat** und das **Schlüsselpaar** im **PKCS-12-**Format exportieren und in die Adaptive Security Appliance importieren. Das Zertifikat wird während des Handshakes mit den Cisco UMA-Clients verwendet.

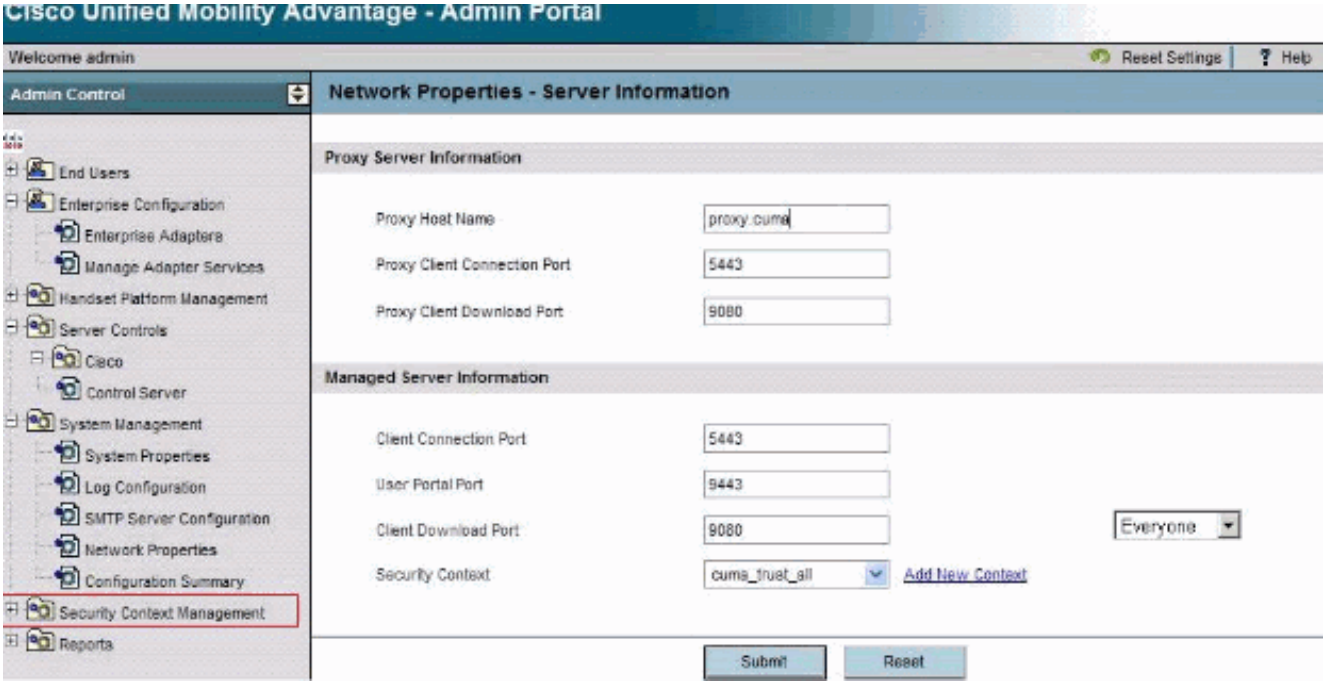
Die Installation des selbstsignierten Cisco UMA-Server-Zertifikats im Truststore der Adaptive Security Appliance ist erforderlich, damit die Adaptive Security Appliance den Cisco UMA-Server beim Handshake zwischen dem Proxy der Adaptive Security Appliance und dem Cisco UMA-Server authentifizieren kann.

Installieren des selbstsignierten Zertifikats des Cisco UMA-Servers

Aufgaben auf dem CUMA-Server

Diese Schritte müssen auf dem CUMA-Server ausgeführt werden. Mit diesen Schritten erstellen Sie ein selbstsigniertes Zertifikat auf CUMA, das Sie mit der ASA mit CN=portal.aipc.com austauschen können. Diese muss im ASA Trust Store installiert werden. Führen Sie diese Schritte aus:

1. Erstellen Sie auf dem CUMA-Server ein selbstsigniertes Zertifikat.Melden Sie sich beim Cisco Unified Mobility Advantage Admin-Portal an.Wählen Sie **[+]** neben der Sicherheitskontextverwaltung
   aus.



Wählen Sie **Sicherheitskontexte aus**.Wählen Sie **Kontext hinzufügen aus**.Geben Sie folgende Informationen ein:

```
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. Laden Sie die selbstsignierten Zertifikate von Cisco Unified Mobility Advantage herunter. Gehen Sie wie folgt vor, um die Aufgabe durchzuführen:Wählen Sie **[+]** neben der Sicherheitskontextverwaltung aus.Wählen Sie **Sicherheitskontexte aus**.Wählen Sie **Manage Context (Kontext verwalten)** neben dem Sicherheitskontext aus, der das herunterzuladende Zertifikat enthält.Wählen Sie **Zertifikat herunterladen aus**.**Hinweis:** Wenn das Zertifikat eine Kette ist und mit Stamm- oder Zwischenzertifikaten verknüpft ist, wird nur das erste Zertifikat in der Kette heruntergeladen. Dies reicht für selbstsignierte Zertifikate aus.Speichern Sie die Datei.
3. Im nächsten Schritt wird das selbstsignierte Zertifikat von Cisco Unified Mobility Advantage zur ASA hinzugefügt. Gehen Sie wie folgt vor:Öffnen Sie das selbstsignierte Zertifikat von Cisco Unified Mobility Advantage in einem Text-Editor.Importieren Sie das Zertifikat in den Cisco Adaptive Security Appliance Trust Store:

```
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. Exportieren Sie das selbstsignierte ASA-Zertifikat auf dem CUMA-Server. Sie müssen Cisco

Unified Mobility Advantage konfigurieren, um ein Zertifikat der Cisco Adaptive Security Appliance zu benötigen. Führen Sie diese Schritte aus, um das erforderliche selbstsignierte Zertifikat bereitzustellen. Diese Schritte müssen auf der ASA durchgeführt werden.Erstellen Sie ein neues Schlüsselpaar:

```
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...
```

Hinzufügen eines neuen Trustpoints:

```
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
```

Registrieren Sie den Trustpoint:

```
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
```

Exportieren des Zertifikats in eine Textdatei

```
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. Kopieren Sie die vorherige Ausgabe in eine Textdatei, fügen Sie sie dem CUMA-Serververtrauenswürdigkeitsspeicher hinzu, und führen Sie folgende Schritte aus:Wählen Sie **[+]** neben der Sicherheitskontextverwaltung aus.Wählen Sie **Sicherheitskontexte aus**.Wählen Sie **Kontext verwalten** neben dem Sicherheitskontext aus, in den Sie das signierte Zertifikat importieren.Wählen Sie **Importieren** in der Leiste Vertrauenswürdige Zertifikate aus.Fügen Sie den Zertifikattext ein.Benennen Sie das Zertifikat.Wählen Sie **Importieren aus**.**Hinweis:** Rufen Sie bei der Remote-Zielkonfiguration das Schreibtischtelefon an, um festzustellen, ob das Mobiltelefon gleichzeitig klingelt. Dadurch wird bestätigt, dass die mobile Verbindung funktioniert und dass keine Probleme mit der Konfiguration des Remote-Ziels auftreten.

Schwierigkeiten beim Hinzufügen einer CUMA-Zertifikatsanforderung zu anderen Zertifizierungsstellen

Problem 1

Viele Installationen von Demos/Prototypen, bei denen es hilfreich ist, wenn die CUMC/CUMA-Lösung mit vertrauenswürdigen Zertifikaten funktioniert, sind selbstsigniert oder von *anderen Zertifizierungsstellen* bezogen. Verisign-Zertifikate sind teuer und es dauert lange, diese Zertifikate zu erhalten. Es ist gut, wenn die Lösung selbstsignierte Zertifikate und Zertifikate anderer Zertifizierungsstellen unterstützt.

Die aktuell unterstützten Zertifikate sind GeoTrust und Verisign. Dies wird in der Cisco Bug-ID CSCta62971 dokumentiert (nur registrierte Kunden)

Fehler: Verbindung konnte nicht hergestellt werden

Wenn Sie beispielsweise versuchen, auf die Benutzerportal-Seite `https://<host>:8443` zuzugreifen, wird die Fehlermeldung `Keine Verbindung` möglich angezeigt.

Lösung

Dieses Problem ist in der Cisco Bug ID CSCsm26730 dokumentiert (nur registrierte Kunden). Gehen Sie wie folgt vor, um auf die Benutzerportal-Seite zuzugreifen:

Die Ursache für dieses Problem ist das Dollarzeichen, sodass das Dollarzeichen mit einem anderen Dollarzeichen in der **Datei Server.xml** des verwalteten Servers entfernt wird. Bearbeiten Sie z. B. /opt/cuma/jboss-4.0.1sp1/server/cuma/deploy/jbossweb-tomcat50.sar/server.xml.

Inline: **keystorePass="pa$word"** maxSpareThreads="15"

Ersetzen Sie das `$`-Zeichen durch `$$`. Es sieht aus wie **keystorePass="pa$$word"** maxSpareThreads="15".

Einige Seiten im CUMA-Admin-Portal sind nicht zugänglich.

Diese Seiten können nicht im **CUMA-Administratorportal** angezeigt werden:

- Benutzer aktivieren/deaktivieren
- Suche/Wartung

Wenn der Benutzer auf eine der beiden oben genannten Seiten im Menü links klickt, scheint der Browser anzuzeigen, dass eine Seite geladen wird, aber nichts passiert (nur die vorherige Seite im Browser ist sichtbar).

Lösung

Um dieses Problem bezüglich der Benutzerseite zu beheben, ändern Sie den für Active Directory verwendeten Port in **3268** und starten Sie CUMA neu.

Zugehörige Informationen

- Schrittweise Konfiguration des ASA-CUMA-Proxys
- Einführung: ASR 5000 v1
- Upgrade von Cisco Unified Mobility Advantage
- Unterstützung von Sprachtechnologie
- Produkt-Support für Sprach- und Unified Communications
- Technischer Support und Dokumentation für Cisco Systeme