Problema del certificato server Unified Mobility Advantage con ASA

Sommario

Introduzione

In questo documento viene descritto come scambiare certificati autofirmati tra Adaptive Security Appliance (ASA) e il server Cisco Unified Mobility Advantage (CUMA) e viceversa. Viene inoltre illustrato come risolvere i problemi comuni che si verificano durante l'importazione dei certificati.

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
- Cisco Unified Mobility Advantage Server 7

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 Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Scenari di distribuzione

Sono disponibili due scenari di implementazione per il **proxy TLS** utilizzato dalla soluzione **Cisco Mobility Advantage**.

Nota: in entrambi gli scenari, i client si connettono da Internet.

1. L'appliance di sicurezza adattiva funziona sia come firewall che come proxy TLS.
2. L'appliance di sicurezza adattiva funziona solo come proxy TLS.

In entrambi gli scenari è necessario esportare il **certificato server UMA Cisco** e la **coppia di chiavi** in formato **PKCS-12** e importarlo nell'appliance di sicurezza adattiva. Il certificato viene utilizzato durante l'handshake con i client Cisco UMA.

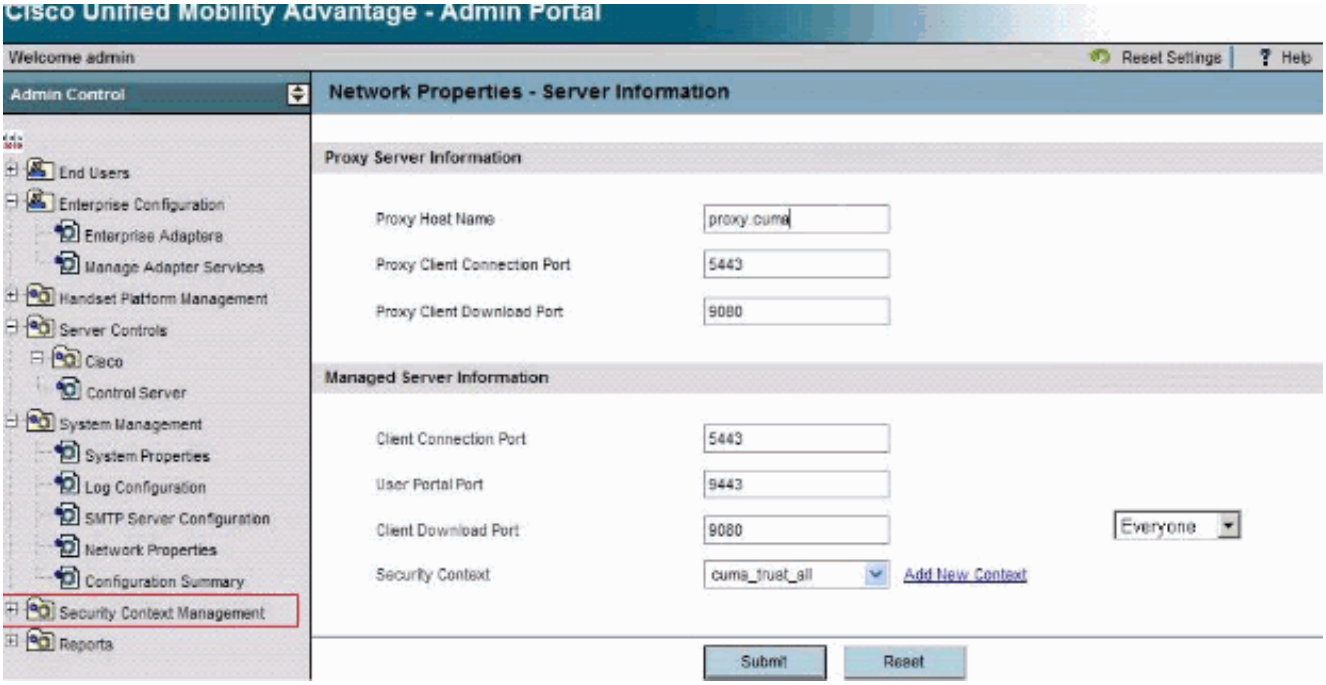
L'installazione del certificato autofirmato del server Cisco UMA nel truststore dell'appliance Adaptive Security è necessaria affinché l'appliance Adaptive Security esegua l'autenticazione del server Cisco UMA durante il handshake tra il proxy dell'appliance Adaptive Security e il server Cisco UMA.

Installa il certificato autofirmato del server Cisco UMA

Operazioni da eseguire sul server CUMA

Queste operazioni devono essere eseguite sul server CUMA. Mediante questa procedura, è possibile creare un certificato autofirmato su una licenza CUMA da scambiare con l'appliance ASA con CN=portal.aipc.com. È necessario installare questo elemento nell'archivio attendibile ASA. Attenersi alla seguente procedura:

1. Creare un certificato autofirmato nel server CUMA.Accedere al portale di amministrazione di Cisco Unified Mobility Advantage.Scegliere **[+]** accanto a Gestione contesto di sicurezza.



Scegliere **Contesti di protezione**.Scegliere **Aggiungi contesto**.Immettere le informazioni seguenti:

```
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. Scarica i certificati autofirmati da Cisco Unified Mobility Advantage. Per eseguire l'attività, completare i seguenti passaggi:Scegliere **[+]** accanto a Gestione contesto di sicurezza.Scegliere **Contesti di protezione**.Scegliere **Gestisci contesto** accanto al contesto di protezione che contiene il certificato da scaricare.Scegliere **Scarica certificato**.**Nota:** se il certificato è una catena e ad esso sono associati certificati radice o intermedi, verrà scaricato solo il primo certificato della catena. È sufficiente per i certificati autofirmati.Salvare il file.
3. Il passaggio successivo è quello di aggiungere il certificato autofirmato di Cisco Unified Mobility Advantage all'appliance ASA. Completare questi passaggi sull'appliance ASA:Aprire il certificato autofirmato di Cisco Unified Mobility Advantage in un editor di testo.Importare il certificato nell'archivio certificati di Cisco Adaptive Security Appliance:

```
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. Esportare il certificato autofirmato ASA sul server CUMA. È necessario configurare Cisco Unified Mobility Advantage in modo che richieda un certificato da Cisco Adaptive Security Appliance. Completare questi passaggi per fornire il certificato autofirmato richiesto. Questa

procedura deve essere eseguita sull'appliance ASA.Genera una nuova coppia di chiavi:

```
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...
```

Aggiungere un nuovo trust point:

```
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
```

Registrare il trust point:

```
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
```

Esporta il certificato in un file di testo.

```
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. Copiare l'output precedente in un file di testo e aggiungerlo all'archivio di attendibilità del server CUMA e utilizzare la procedura seguente:Scegliere **[+]** accanto a Gestione contesto di sicurezza.Scegliere **Contesti di protezione**.Scegliere **Gestisci contesto** accanto al contesto di sicurezza in cui si importa il certificato firmato.Scegliere **Importa** nella barra dei certificati protetti.Incollare il testo del certificato.Assegnare un nome al certificato.Scegliere **Importa**.**Nota:** per la configurazione Destinazione remota, chiamare il telefono da tavolo per determinare se il telefono cellulare squilla contemporaneamente. Ciò confermerebbe che la connessione mobile funziona e che non vi sono problemi con la configurazione della destinazione remota.

Problema durante l'aggiunta di una richiesta di certificato CUMA ad altre autorità di certificazione

Problema 1

Molte installazioni dimostrative/prototipo in cui è utile che la soluzione CUMC/CUMA funzioni con certificati attendibili sono autofirmate o ottenute da *altre autorità di certificazione*. I certificati Versioni sono costosi e richiedono molto tempo per ottenerli. È consigliabile che la soluzione supporti certificati autofirmati e certificati di altre CA.

I certificati attualmente supportati sono GeoTrust e Verisign. Questa condizione è documentata nell'ID bug Cisco CSCta62971 (solo utenti registrati)

Errore: Impossibile connettersi

Quando si tenta di accedere alla pagina del portale utenti, ad esempio `https://<host>:8443`, viene visualizzato il messaggio di errore `Impossibile connettersi`.

Soluzione

Questo problema è documentato nell'ID bug Cisco CSCsm26730 (solo utenti registrati). Per accedere alla pagina del portale utenti, completare la soluzione seguente:

La causa di questo problema è il carattere del dollaro, quindi eseguire l'escape del carattere del dollaro con un altro carattere del dollaro nel **file server.xml** del server gestito. Ad esempio, modificare /opt/cuma/jboss-4.0.1sp1/server/cuma/deploy/jbossweb-tomcat50.sar/server.xml.

In linea: **keystorePass="pa$word"** maxSpareThreads="15"

Sostituire il carattere `$` con `$$`. È simile a **keystorePass="pa$$word"** maxSpareThreads="15".

Alcune pagine del portale di amministrazione CUMA non sono accessibili

Queste pagine non possono essere visualizzate nel **portale di amministrazione CUMA**:

- attiva/disattiva utente
- ricerca/manutenzione

Se l'utente fa clic su una delle due pagine precedenti nel menu a sinistra, il browser sembra indicare che sta caricando una pagina, ma non accade nulla (è visibile solo la pagina precedente che era nel browser).

Soluzione

Per risolvere il problema relativo alla pagina utente, impostare la porta utilizzata per Active Directory su **3268** e riavviare l'autenticazione cumulativa.

Informazioni correlate

- Configurazione dettagliata del proxy ASA-CUMA
- Introduzione a ASR5000 v1
- Aggiornamento di Cisco Unified Mobility Advantage
- Supporto alla tecnologia vocale
- Supporto ai prodotti voce e Unified Communications
- Documentazione e supporto tecnico – Cisco Systems