Problema de certificado do Unified Mobility Advantage Server com o ASA

Contents

Introduction

Este documento descreve como trocar certificados autoassinados entre o Adaptive Security Appliance (ASA) e o servidor Cisco Unified Mobility Advantage (CUMA) e vice-versa. Ele também explica como solucionar problemas comuns que ocorrem enquanto você importa os certificados.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ASA série 5500
- Cisco Unified Mobility Advantage Server 7

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is

live, make sure that you understand the potential impact of any command.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Cenários de implantação

Há dois cenários de implantação para o **proxy TLS** usado pela solução **Cisco Mobility Advantage**.

Observação: em ambos os cenários, os clientes se conectam da Internet.

1. O aplicativo de segurança adaptável funciona como firewall e proxy TLS.
2. O aplicativo de segurança adaptável funciona somente como proxy TLS.

Em ambos os cenários, você precisa exportar o **certificado do servidor Cisco UMA** e o **par de chaves** no formato **PKCS-12** e importá-lo para o aplicativo de segurança adaptável. O certificado é usado durante o handshake com os clientes Cisco UMA.

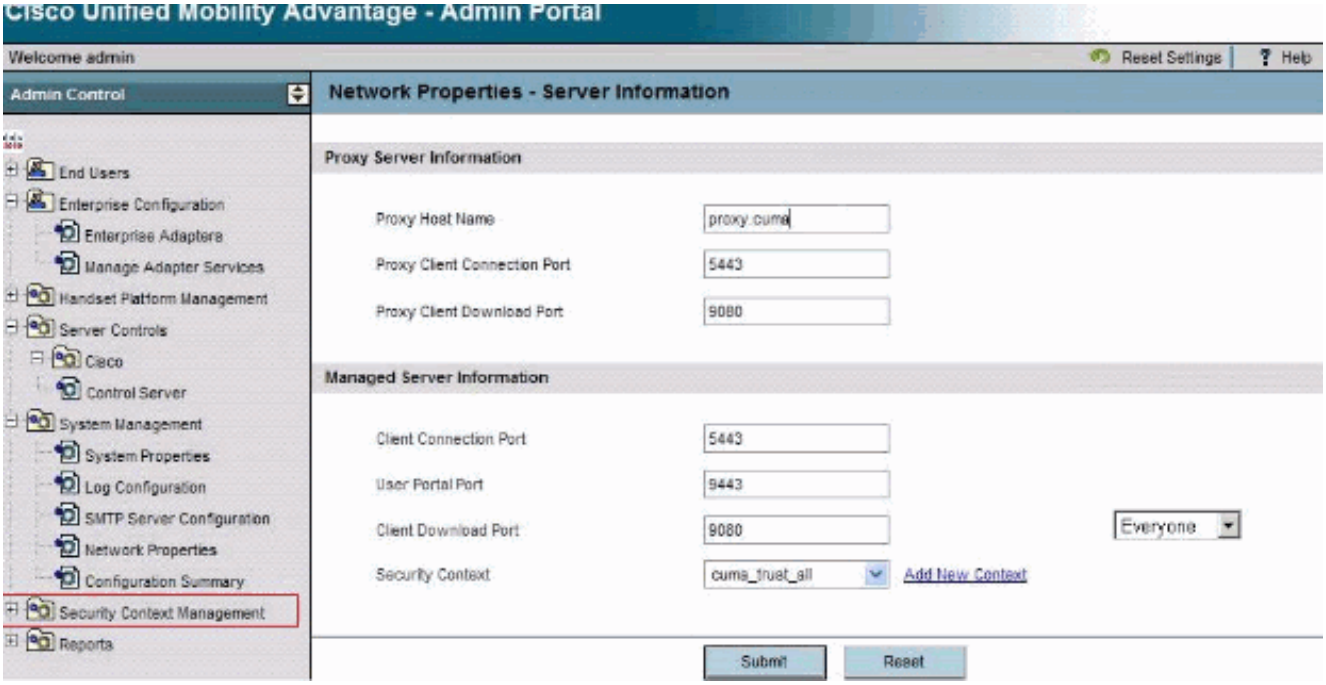
A instalação do certificado autoassinado do servidor Cisco UMA no repositório de confiabilidade do aplicativo de segurança adaptável é necessária para que o aplicativo de segurança adaptável autentique o servidor Cisco UMA durante o handshake entre o proxy do dispositivo de segurança adaptável e o servidor Cisco UMA.

Instalar o certificado autoassinado do servidor Cisco UMA

Tarefas a serem feitas no servidor CUMA

Essas etapas precisam ser feitas no servidor CUMA. Com essas etapas, você cria um certificado autoassinado no CUMA para troca com o ASA com CN=portal.aipc.com. Isso precisa ser instalado no repositório confiável do ASA. Conclua estes passos:

1. Crie um certificado autoassinado no servidor CUMA.Entre no portal do Cisco Unified Mobility Advantage Admin.Escolha o **[+]** ao lado de Gerenciamento de contexto de segurança.



Escolha **Contextos de segurança**.Escolha **Adicionar contexto**.Insira esta informação:

```
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. Faça o download dos certificados autoassinados do Cisco Unified Mobility Advantage. Conclua estes passos para realizar a tarefa:Escolha o **[+]** ao lado de Gerenciamento de contexto de segurança.Escolha **Contextos de segurança**.Escolha **Gerenciar contexto** ao lado do contexto de segurança que contém o certificado para download.Escolha **Download Certificate**.**Observação:** se o certificado for uma cadeia e tiver certificados raiz ou intermediários associados, somente o primeiro certificado na cadeia será baixado. Isso é suficiente para certificados autoassinados.Salve o arquivo.
3. A próxima etapa é adicionar o certificado autoassinado do Cisco Unified Mobility Advantage ao ASA. Conclua estes passos no ASA:Abra o certificado autoassinado do Cisco Unified Mobility Advantage em um editor de texto.Importar o certificado para o arquivo de confiança do 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. Exportar certificado autoassinado do ASA no servidor CUMA. Você precisa configurar o Cisco Unified Mobility Advantage para exigir um certificado do Cisco Adaptive Security Appliance. Conclua estes passos para fornecer o certificado autoassinado necessário. Essas

etapas precisam ser feitas no ASA.Gerar um novo par de chaves:

```
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...
```

Adicionar um novo ponto de confiança:

```
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
```

Inscreva o ponto de confiança:

```
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
```

Exportar o certificado para um arquivo de texto.

```
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. Copie a saída anterior em um arquivo de texto e adicione-a ao repositório de confiança do servidor CUMA e use este procedimento:Escolha o **[+]** ao lado de Gerenciamento de contexto de segurança.Escolha **Contextos de segurança**.Escolha **Gerenciar Contexto** ao lado do Contexto de Segurança no qual você importa o certificado assinado.Escolha **Importar** na barra Certificados Confiáveis.Cole o texto do certificado.Nomeie o certificado.Escolha **Importar**.**Observação:** para a configuração de Destino Remoto, ligue para o telefone de mesa para determinar se o telefone celular toca ao mesmo tempo. Isso confirmaria que a conexão móvel funciona e que não há nenhum problema com a configuração de Destino Remoto.

Problema ao adicionar a solicitação de certificado CUMA a outras autoridades de certificado

Problema 1

Muitas instalações de demonstração/protótipo em que ajuda se a solução CUMC/CUMA funcionar com certificados confiáveis forem autoassinados ou obtidos de *outras autoridades de certificação*. Os certificados de verificação são caros e leva muito tempo para obter esses certificados. É bom que a solução ofereça suporte a certificados autoassinados e certificados de outras CAs.

Os certificados atuais suportados são GeoTrust e Verisign. Isso está documentado na ID de bug da Cisco CSCta62971 (somente clientes registrados)

Erro: Não é possível conectar

Quando você tenta acessar a página do portal do usuário, por exemplo, `https://<host>:8443`, a mensagem de erro `Unable to connect` é exibida.

Solução

Esse problema está documentado na ID de bug da Cisco CSCsm26730 (somente clientes registrados) . Para acessar a página do portal do usuário, faça esta solução:

A causa deste problema é o caractere dólar, portanto, escape do caractere dólar com outro caractere dólar no **arquivo server.xml** do servidor gerenciado. Por exemplo, edite /opt/cuma/jpatrão-4.0.1sp1/server/cuma/deploy/jbossweb-tomcat50.sar/server.xml.

Em linha: **keystorePass="pa$word"** maxSpareThreads="15"

Substitua o `$` caractere por `$$`. Parece **keystorePass="pa$$word"** maxSpareThreads="15".

Algumas páginas do CUMA Admin Portal não estão acessíveis

Estas páginas não podem ser visualizadas no **Portal de Administração CUMA**:

- ativar/desativar usuário
- pesquisa/manutenção

Se o usuário clicar em uma das duas páginas acima no menu à esquerda, o navegador parece indicar que está carregando uma página, mas nada acontece (somente a página anterior que estava no navegador está visível).

Solução

Para resolver esse problema relacionado à página do usuário, altere a porta usada para o Ative Diretory para **3268** e reinicie o CUMA.

Informações Relacionadas

- Configuração passo a passo do proxy ASA-CUMA
- Introdução a ASR5000 v1
- Atualizando o Cisco Unified Mobility Advantage
- Suporte à Tecnologia de Voz
- Suporte aos produtos de Voz e Comunicações Unificadas
- Suporte Técnico e Documentação - Cisco Systems