Problema del certificado de servidor del Cisco Unified Mobility Advantage con el ASA

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Escenarios de instrumentación
Instale el certificado autofirmado del servidor de Cisco UMA
Tareas de ser hecho en el servidor CUMA
Problema que agrega el pedido de certificado CUMA a otras autoridades de certificación
Problema 1
Error: Incapaz de conectar
Solución
Algunas páginas en el portal CUMA Admin no son accesibles
Solución
Información Relacionada

Introducción

Este documento describe cómo intercambiar los certificados autofirmados entre el dispositivo de seguridad adaptante (ASA) y el servidor del Cisco Unified Mobility Advantage (CUMA) y vice versa. También explica cómo resolver problemas los problemas frecuentes que ocurre mientras que usted importa los Certificados.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- 5500 Series de Cisco ASA
- Servidor 7 del Cisco Unified Mobility Advantage

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Escenarios de instrumentación

Hay dos escenarios de instrumentación para el **proxy de TLS** usado por la solución de la **ventaja de la movilidad de Cisco**.

Nota: En ambos escenarios, los clientes conectan de Internet.

1. El dispositivo de seguridad adaptante funciona como el Firewall y el proxy de TLS.
2. El dispositivo de seguridad adaptante funciona como el proxy de TLS solamente.

En ambos escenarios, usted necesita exportar el **certificado de servidor** y el **par clave de Cisco UMA** en el formato **PKCS-12** e importarlo al dispositivo de seguridad adaptante. El certificado se utiliza durante el apretón de manos con los clientes de Cisco UMA.

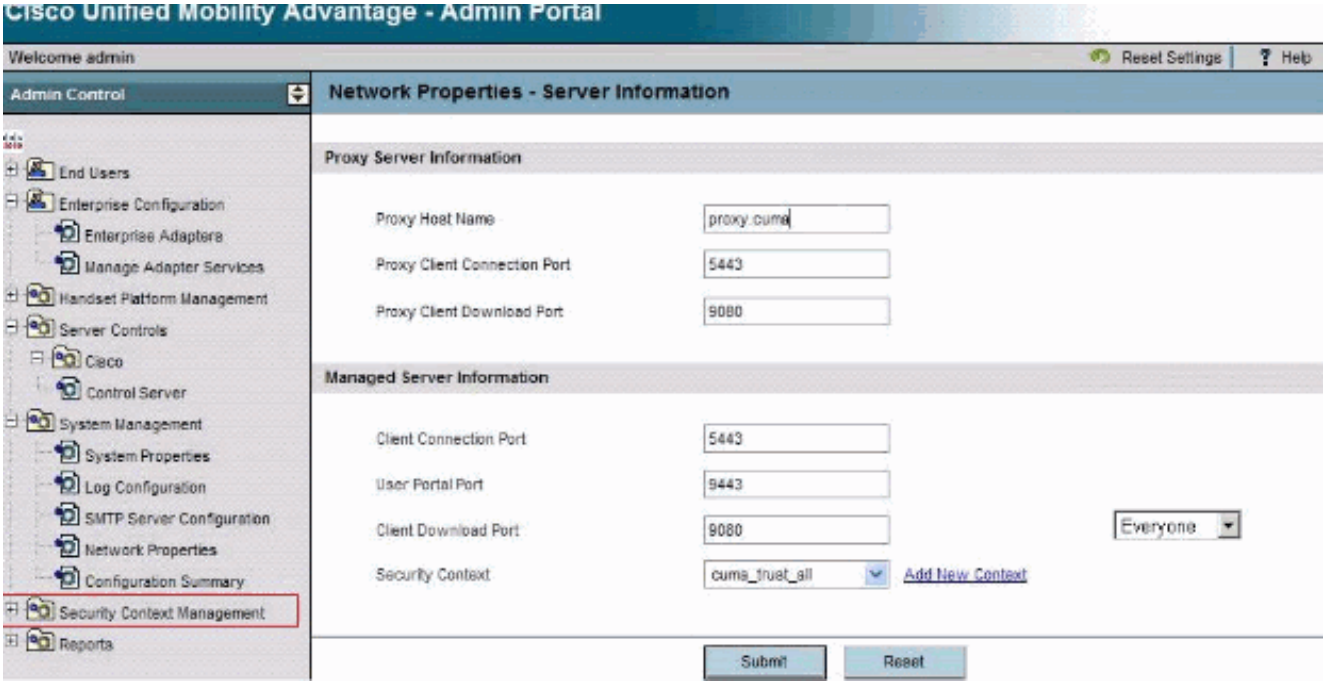
La instalación del certificado autofirmado del servidor de Cisco UMA en el truststore adaptante del dispositivo de seguridad es necesaria para que el dispositivo de seguridad adaptante autentique el servidor de Cisco UMA durante el apretón de manos entre el proxy del dispositivo de seguridad y el servidor adaptantes de Cisco UMA.

Instale el certificado autofirmado del servidor de Cisco UMA

Tareas de ser hecho en el servidor CUMA

Estos pasos necesitan ser hechos en el servidor CUMA. Con estos pasos, usted crea un certificado autofirmado en CUMA para intercambiar por el ASA con CN=portal.aipc.com. Esto necesita ser instalada en el almacén de la confianza ASA. Complete estos pasos:

1. Cree un CERT uno mismo-firmado en el servidor CUMA.Ingrese al portal Admin del Cisco Unified Mobility Advantage.Elija el **[+]** al lado de la Administración de los contextos de seguridad.



Elija los **contextos de seguridad**.Elija **agregan el contexto**.Ingresar esta información`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. Descargue los certificados autofirmados del Cisco Unified Mobility Advantage. Complete estos pasos para lograr la tarea:Elija el **[+]** al lado de la Administración de los contextos de seguridad.Elija los **contextos de seguridad**.Elija **manejan el contexto** al lado de los contextos de seguridad que sostienen el certificado para descargar.Elija el **certificado de la descarga**.**Nota:** Si el certificado es un encadenamiento, y ha asociado los Certificados de la raíz o del intermedio, sólo el primer certificado en el encadenamiento se descarga. Esto es suficiente para los certificados autofirmados.Guarde el archivo.
3. El siguiente paso es agregar el certificado autofirmado del Cisco Unified Mobility Advantage sobre el ASA. Complete estos pasos en el ASA:Abra el certificado autofirmado del Cisco Unified Mobility Advantage en un editor de textos.Importe el certificado en el almacén adaptante de la confianza del dispositivo de seguridad de Cisco:`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. Exporte el certificado autofirmado ASA en el servidor CUMA. Usted necesita configurar el Cisco Unified Mobility Advantage para requerir un certificado del dispositivo de seguridad adaptante de Cisco. Complete estos pasos para proporcionar el certificado autofirmado requerido. Estos pasos necesitan ser hechos en el ASA.Genere un nuevo par clave:`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...`Agregue un nuevo trustpoint:`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` Aliste el

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`Exporte el certificado a un archivo 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 la salida anterior a un archivo de texto y agreguela al almacén de la confianza del servidor CUMA y utilice este procedimiento:Elija el **[+]** al lado de la Administración de los contextos de seguridad.Elija los **contextos de seguridad**.Elija **manejan el contexto** al lado de los contextos de seguridad en las cuales usted importa el certificado firmado.Elija la **importación** en la barra de los certificados confiables.Pegue el texto del certificado.Nombre el certificado.Elija la **importación**.**Nota:** Para la configuración del destino remoto, llamada en el teléfono de escritorio para determinar si el teléfono celular suena en la misma hora. Esto confirmaría que el móvil conecta los trabajos y que no hay problema con la configuración del destino remoto.

Problema que agrega el pedido de certificado CUMA a otras autoridades de certificación

Problema 1

Mucho instalaciones de la versión parcial de programa/del prototipo en donde ayuda si los trabajos de la solución CUMC/CUMA con los certificados confiables uno mismo-se firman o se obtienen de *otras autoridades de certificación*. Los certificados de Verisign son costosos y tarda un tiempo prolongado para conseguir estos Certificados. Es bueno si la solución soporta los certificados autofirmados y los Certificados de otros CA.

Los Certificados actuales soportados son GeoTrust y Verisign. Esto se documenta en el Id. de bug Cisco CSCta62971 (el clientes registrados solamente)

Error: Incapaz de conectar

Cuando usted intenta acceder la página porta del usuario, por ejemplo, `https://<host>:8443`, el `incapaz de conectar el` mensaje de error aparece.

Solución

Este problema se documenta en el Id. de bug Cisco CSCsm26730 (clientes registrados solamente). Para acceder la página porta del usuario, complete esta solución alternativa:

La causa de este problema es el carácter del dólar, así que escape el carácter del dólar con otro carácter del dólar en el **archivo server.xml del** servidor manejado**. Por ejemplo**, edite /opt/cuma/jboss-4.0.1sp1/server/cuma/deploy/jbossweb-tomcat50.sar/server.xml.

En la línea: **keystorePass= " pa$word" el** maxSpareThreads="15"

Substituya el carácter `$` por `$$`. Parece el **keystorePass= " pa$$word" el** maxSpareThreads="15".

Algunas páginas en el portal CUMA Admin no son accesibles

Estas páginas no se pueden ver en el **portal CUMA Admin**:

- active/desactive al usuario
- búsqueda/mantenimiento

Si el usuario hace clic en una de las dos páginas antedichas en el menú a la izquierda, el hojeador parece indicar que está cargando una página, pero sucede nada (solamente la página previa que estaba en el hojeador es visible).

Solución

Para resolver este problema se relacionó con la página del usuario, cambia el puerto usado para el Active Directory a **3268** y recomienza el CUMA.

Información Relacionada

- Configuración gradual del proxy ASA-CUMA
- V1 del al ASR5000 de Introduccion
- Actualizar el Cisco Unified Mobility Advantage
- Soporte de tecnología de voz
- Soporte de Productos de Voice and Unified Communications
- Soporte Técnico y Documentación - Cisco Systems