Contenido

[Introducción](#)
[Requisito previo](#)
[Procedimiento](#)

Introducción

Usted puede configurar un centro de administración de FireSIGHT para permitir que los usuarios externos del Active Directory LDAP autentiquen el acceso a la interfaz del Web User y al CLI. Este artículo discute cómo configurar, probar, resolver problemas el objeto de la autenticación para la autenticación de Microsoft AD sobre el SSL/TLS.

Requisito previo

Cisco recomienda que usted tiene el conocimiento encendido User Management (Administración de usuario) y sistema de autenticación externa en el centro de administración de FireSIGHT.

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.

Procedimiento

Paso 1. Objeto de la autenticación de la configuración sin el cifrado SSL/TLS.

1. Configure el objeto de la autenticación como usted normalmente. Los pasos de configuración básicos para la autenticación cifrada y unencrypted son lo mismo.
2. Confirme que el objeto de la autenticación está trabajando y los usuarios AD LDAP puede autenticar unencrypted.

Paso 2. Pruebe el objeto de la autenticación sobre el SSL y TLS sin el certificado de CA.

Pruebe el objeto de la autenticación sobre el SSL y TLS sin el CERT de CA. Si usted encuentra un problema, consulte por favor con su System Admin para resolver este problema en el servidor AD LD. Si un certificado ha estado cargado previamente al objeto de la autenticación, seleccione por favor el “**certificado se ha cargado (selecto borrar el certificado cargado)**” para borrar el CERT y para probar el AO otra vez.

Si el objeto de la autenticación falla, satisfaga consultan su System Admin para verificar la configuración AD LD SSL/TLS antes de que usted se traslade encendido al siguiente paso. Sin embargo, no dude en continuar por favor a los pasos siguientes probando el objeto de la autenticación más lejos con el certificado de CA.

Paso 3. CERT de CA del **base64 de la** descarga.

1. Login al AD LD.
2. Abra a un buscador Web y conecte con `http://localhost/certsrv`
3. Haga clic en la "**descarga un certificado de CA, una Cadena de certificados, o un CRL**"
4. Elija el CERT de CA del "**certificado de CA**" lista y el "**Base64"** "del **método de codificación**"
5. Haga clic en "el link del **certificado de CA de la descarga**" para descargar el archivo de `certnew.cer`.

Paso 4. Verifique el valor **sujeto** en el CERT.

1. Haga clic con el botón derecho del ratón en `certnew.cer` y seleccione **abierto**.
2. Haga clic en los **detalles** lengueta y seleccione el **<All> de las** opciones del descenso-abajo de la **demostración**
3. Verifique el valor para cada campo. Particularmente, verifique que el valor **sujeto** haga juego el **nombre del host del servidor primario del** objeto de la autenticación.

Paso 5. Pruebe el CERT en una máquina de Microsoft Windows. Usted puede realizar esta prueba en un grupo de trabajo o una máquina unida dominio de Windows.

> Consejo: Este paso se puede utilizar para probar el certificado de CA en un Sistema Windows antes de crear el objeto de la autenticación en un centro de administración de FireSIGHT.

1. Copie el CERT de CA a `C:\Certficate` o a cualquier directorio preferido.
2. Funcione con la línea de comando de Windows, `cmd.exe como` administrador
3. Pruebe el certificado de CA con el comando de Certutil

```
cd c:\Certificate

certutil -v -urlfetch -verify certnew.cer >cacert.test.txt
```

Si la máquina de Windows ya se une al dominio, el certificado de CA debe estar en el almacén de certificados y no debe haber error en `cacert.test.txt`. Sin embargo, si la máquina de Windows está en un grupo de trabajo, usted puede ver uno de los dos mensajes dependiendo de la existencia del CERT de CA en la lista de confianza de CA.

a. Se confía en CA pero ningún CRL encontró para CA:

```
ERROR: Verifying leaf certificate revocation status returned The revocation function
was unable to check revocation because the revocation server was offline. 0x80092013
(-2146885613)

CertUtil: The revocation function was unable to check revocation because the
revocation server was offline.
```

b. CA no se confía en:

```
Verifies against UNTRUSTED root
Cert is a CA certificate
Cannot check leaf certificate revocation status
CertUtil: -verify command completed successfully.
```

Si usted consigue cualesquiera otros mensajes de error como debajo, consulte por favor con su System Admin para resolver el problema en el AD LD y CA intermedio. Estos mensajes de error son indicativos del CERT incorrecto, del tema en el CERT de CA, de la Cadena de certificados que falta, del etc.

```
Verifies against UNTRUSTED root
Cert is a CA certificate
Cannot check leaf certificate revocation status
CertUtil: -verify command completed successfully.
```

Paso 6. Una vez que usted confirma el CERT de CA es válido y ha pasado la prueba en el paso 5, carga el CERT al objeto de la autenticación y funciona con la prueba.

Paso 7. Salve el objeto de la autenticación y reaplique la política del sistema.