Verificación de CRL en HTTP en un concentrador Cisco VPN 3000

Contenido

Introducción

Este documento describe cómo habilitar el Listas de revocación de certificados (CRL) que marca para saber si hay Certificados del Certification Authority (CA) instalados en el Cisco VPN 3000 Concentrator usando el modo HTTP.

Se espera que un certificado normalmente sea válido para su período de validez entero. Sin embargo, si un certificado vence no válido debido a las cosas tales como un cambio de nombre, cambio de la asociación entre el tema y CA, y compromiso de la Seguridad, CA revoca el certificado. Bajo el X.509, los CA revocan los Certificados periódicamente publicando un CRL firmado, donde cada certificado revocado es identificado por su número de serie. Habilitar la verificación de CRL significa que cada vez que el concentrador VPN utiliza el certificado para la autenticación, también marca el CRL para asegurarse de que el certificado que era verificado no se ha revocado.

Bases de datos del Lightweight Directory Access Protocol (LDAP) /HTTP del uso CA para salvar y para distribuir los CRL. Puede ser que también utilicen los otros medios, pero el concentrador VPN confía en el acceso LDAP/HTTP.

La verificación de CRL HTTP se introduce en la versión 3.6 o posterior del concentrador VPN. Sin embargo, la verificación de CRL LDAP-basada fue introducida en las versiones anteriores 3.x. Este documento discute solamente la verificación de CRL usando el HTTP.

Nota: El tamaño de la memoria caché CRL del VPN 3000 series concentrators depende de la plataforma y no puede ser configurado según el deseo del administrador.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Usted ha establecido con éxito el túnel IPsec de los hardwares cliente VPN 3.x que usaban los Certificados para la autenticación del Internet Key Exchange (IKE) (sin la verificación de CRL habilitada).
- Su concentrador VPN tiene Conectividad al servidor de CA siempre.
- Si su servidor de CA está conectado hacia fuera con la interfaz pública, después usted ha abierto las reglas necesarias en el filtro (predeterminado) público.

Componentes Utilizados

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

- C concentrador VPN 3000 de la versión 4.0.1
- Hardware cliente VPN 3.x
- Microsoft CA server para la generación y la verificación de CRL del certificado que se ejecutan en a Windows 2000 Server.

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.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Configurar el concentrador VPN 3000

Instrucciones Paso a Paso

Complete estos pasos para configurar el concentrador VPN 3000:

1. Seleccione el **Administration (Administración) > Certificate Management (Administración de certificados)** para pedir un certificado si usted no tiene un certificado.Seleccione **hacen clic**

aquí para instalar un certificado para instalar el certificado raíz en el concentrador VPN.
2. Selecto **instale el certificado de CA**.
3. Seleccione **SCEP (protocolo simple certificate enrollment)** para extraer los Certificados de CA.
4. De la ventana SCEP, ingrese el URL completo del servidor CA en el cuadro de diálogo URL.En este ejemplo, la dirección IP del servidor de CA es 172.18.124.96. Puesto que este ejemplo utiliza el servidor de CA de Microsoft, el URL completo es http://172.18.124.96/certsrv/mscep/mscep.dll. Después, ingrese a un descriptor de una palabra en el cuadro de diálogo del descriptor CA. Este ejemplo utiliza CA.
5. El tecleo **extrae**.Su certificado de CA debe aparecer bajo la ventana del Administration (Administración) > Certificate Management (Administración de certificados). Si usted no ve un certificado, vuelva al paso 1 y siga el procedimiento otra vez.
6. Una vez que usted tiene el certificado de CA, el **Administration (Administración) > Certificate Management (Administración de certificados) > Enroll (Registrar)** selecto, y el **certificado de identidad del** tecleo.
7. El tecleo **alista vía el SCEP en…** para solicitar el certificado de identidad.
8. Complete estos pasos para rellenar el impreso de la inscripción:Ingrese el Common Name para que el concentrador VPN sea utilizado en el Public Key Infrastructure (PKI) en el campo del Common Name (CN).Ingrese su departamento en el campo de la unidad organizativa (OU). El OU debe hacer juego el nombre del grupo IPSec configurado.Ingrese su organización o compañía en el campo de la organización (o).Ingrese su ciudad o pueblo en el campo del lugar (l).Ingrese su estado o provincia en el campo del estado/de la provincia (SP).Ingrese su país en el campo del país (c).Ingrese el Nombre de dominio totalmente calificado (FQDN) (FQDN) para que el concentrador VPN sea utilizado en el PKI en el campo del Nombre de dominio totalmente calificado (FQDN) (FQDN).Ingrese la dirección email para que el concentrador VPN sea utilizado en el PKI en el campo alternativo sujeto del nombre (dirección email).Ingrese la contraseña de impugnación para el pedido de certificado en el campo de contraseña de impugnación.Entre la contraseña de impugnación de nuevo en el campo de contraseña de impugnación del verificar.Seleccione el tamaño de clave para el par clave generado RSA de la lista desplegable del tamaño de clave.
9. Selecto **aliste** y vea el estado SCEP en el estado de consulta.
10. Vaya a su servidor de CA a aprobar el certificado de identidad. Una vez que se aprueba en el servidor de CA, su estado SCEP debe ser instalado.
11. Bajo administración de certificados, usted debe ver su certificado de identidad.Si usted no hace, marcar abre una sesión su servidor de CA para más troubleshooting.
12. Seleccione la **opinión** sobre su certificado recibido para ver si su certificado tiene un CRL Distribution Point (CDP).El CDP enumera todas las puntas de la distribución CRL del emisor de este certificado. Si usted tiene CDP en su certificado, y usted utiliza un nombre DNS para enviar una interrogación al servidor de CA, aseegurese que usted tiene los servidores DNS definidos en su concentrador VPN para resolver el nombre de host con una dirección IP. En este caso, el nombre del host del ejemplo del servidor de CA es la jazib-PC que resuelve a una dirección IP de 172.18.124.96 en el servidor DNS.
13. Haga clic la **configuración** en su certificado de CA para habilitar la verificación de CRL en los Certificados recibidos.Si usted tiene CDP en su certificado recibido y usted quisiera utilizarlo, después seleccione las **puntas de la distribución CRL del uso del certificado que es marcado**.Puesto que el sistema tiene que extraer y examinar el CRL de un punto de distribución de la red, habilitar la verificación de CRL pudo reducir los tiempos de respuesta del sistema. También, si la red es lenta o congestionada, la verificación de CRL pudo fallar.

Permiso CRL que oculta para atenuar estos problemas potenciales. Esto salva los CRL extraídos en memoria volátil local y por lo tanto permite que el concentrador VPN verifique el estado de anulación de Certificados más rápidamente.Con el almacenamiento en memoria inmediata CRL habilitado, las en primer lugar controles del concentrador VPN si el CRL requerido existe en el caché y marca el número de serie del certificado contra la lista de números de serie en el CRL cuando necesita marcar el estado de anulación de un certificado. El certificado se considera revocado si se encuentra su número de serie. El concentrador VPN extrae un CRL de un servidor externo cualquiera cuando no encuentra el CRL requerido en el caché, cuando ha expirado el período de validez del CRL ocultado, o cuando ha transcurrido el tiempo de actualización configurado. Cuando el concentrador VPN recibe un nuevo CRL de un servidor externo, pone al día el caché con el nuevo CRL. El caché puede contener hasta 64 CRL.**Nota:** El caché CRL existe en la memoria. Por lo tanto, el reiniciar el Concentrador VPN borra el caché CRL. El concentrador VPN repuebla el caché del CRL con CRLs actualizado como él procesa los pedidos de autenticación del peer nuevos.Si usted selecciona las **puntas estáticas de la distribución CRL del uso**, después usted puede utilizar hasta cinco puntas estáticas de la distribución CRL, según lo especificado en esta ventana. Si usted elige esta opción, usted debe ingresar por lo menos un URL.Usted puede también seleccionar las **puntas de la distribución CRL del uso del certificado que es marcado**, o seleccionar las **puntas estáticas de la distribución CRL del uso**. Si el concentrador VPN no puede encontrar cinco puntas de la distribución CRL en el certificado, equivale las puntas estáticas de la distribución CRL, hasta un límite de cinco. Si usted elige esta opción, habilite por lo menos un protocolo del CRL Distribution Point. Usted también debe ingresar por lo menos las puntas estáticas de una (y no más que cinco) distribución CRL.No seleccione **ninguna verificación de CRL** si usted quiere inhabilitar la verificación de CRL.Bajo el CRL que oculta, seleccione el cuadro **habilitado** para permitir que el concentrador VPN oculte los CRL extraídos. El valor por defecto no es habilitar el almacenamiento en memoria inmediata CRL. Cuando usted inhabilita el CRL que oculta (unselect el cuadro), se borra el caché CRL.Si usted configuró una política de recuperación de CRL que utiliza las puntas de la distribución CRL del certificado que es marcado, elija un protocolo del punto de distribución para utilizar para extraer el CRL. Elija el **HTTP** en este caso para extraer el CRL. Asigne las reglas HTTP al filtro de la interfaz pública si su servidor de CA está hacia la interfaz pública.

Control

Seleccione el **Administration (Administración) > Certificate Management (Administración de certificados)** y haga clic en la **visión todos los cachés del CRL** para ver si su concentrador VPN ha ocultado cualquier CRLs del servidor CA.

Verificación

En esta sección encontrará información que puede utilizar para comprobar que su configuración funcione correctamente.

Registros del concentrador

Permita a estos eventos en el concentrador VPN para aseegurarse que la verificación de CRL

trabaja.

1. Seleccione el **Configuration (Configuración) > System (Sistema) > Events (Eventos) > Classes (Clases)** para fijar los niveles de registro.
2. Bajo nombre de la clase seleccione el **IKE**, el **IKEDBG**, el **IPSEC**, el **IPSECDBG**, o el **CERT**.
3. Haga clic **agregan** o **modifican**, y eligen la **gravedad para registrar la opción 1-13**.
4. El tecleo **se aplica** si usted quiere modificarse, o **agrega** si usted quiere agregar una nueva entrada.

Registros de concentradores exitosos

Si su verificación de CRL es acertada, estos mensajes se consideran en los registros de eventos filtrables.

```
1315 08/15/2002 13:11:23.520 SEV=7 CERT/117 RPT=1
The requested CRL was found in cache.
The CRL Distribution point is: http://jazib-pc/CertEnroll/jazib-ca-ra.crl

1317 08/15/2002 13:11:23.520 SEV=8 CERT/46 RPT=1
CERT_CheckCrl(62f56e8, 0, 0)

1318 08/15/2002 13:11:23.520 SEV=7 CERT/2 RPT=1 Certificate has not been revoked: session = 2
1319 08/15/2002 13:11:23.530 SEV=8 CERT/50 RPT=1 CERT_Callback(62f56e8, 0, 0) 1320 08/15/2002
13:11:23.530 SEV=5 IKE/79 RPT=2 64.102.60.53 Group [ipsecgroup] Validation of certificate
successful (CN=client_cert, SN=61521511000000000086)
```

Refiera a los registros acertados del concentrador para el resultado completo de un registro acertado del concentrador.

Registros fallados

Si su verificación de CRL en no acertado, estos mensajes se considera en los registros de eventos filtrables.

```
1332 08/15/2002 18:00:36.730 SEV=7 CERT/6 RPT=2 Failed to retrieve revocation list: session = 5
1333 08/15/2002 18:00:36.730 SEV=7 CERT/114 RPT=2 CRL retrieval over HTTP has failed. Please
make sure that proper filter rules have been configured. 1335 08/15/2002 18:00:36.730 SEV=7
CERT/8 RPT=2 Error processing revocation list: session = 5, reason = Failed to retrieve CRL from
the server.
```

Refiera a los Registros concentradores caducados para el resultado completo de un registro fallado del concentrador.

Refiera a los registros acertados del cliente para el resultado completo de un registro acertado del cliente.

Refiera a los registros de cliente caducado para el resultado completo de un registro fallado del cliente.

Troubleshooting

Refiera a los Problemas de conexión del troubleshooting en el concentrador VPN 3000 para más información de Troubleshooting.

Información Relacionada

- Página de soporte del Concentradores Cisco VPN de la serie 3000
- Página de soporte del VPN 3000 Client de Cisco
- Negociación IPSec/Protocolos IKE
- Soporte Técnico y Documentación - Cisco Systems