Verificación de CRL en HTTP en un concentrador Cisco VPN 3000

Contenido

Introducción

Este documento describe cómo habilitar la lista de revocación de certificados (CRL) para comprobar los certificados de entidad de certificación (CA) instalados en el Cisco VPN 3000 Concentrator mediante el modo HTTP.

Normalmente se espera que un certificado sea válido durante todo su período de validez. Sin embargo, si un certificado deja de ser válido debido a cosas como el cambio de nombre, el cambio de asociación entre el asunto y la CA y el riesgo de seguridad, la CA revoca el certificado. En X.509, las CA revocan los certificados emitiendo periódicamente una CRL firmada, donde cada certificado revocado se identifica por su número de serie. La habilitación de la verificación de CRL significa que cada vez que el concentrador VPN utiliza el certificado para la autenticación, también verifica la CRL para asegurarse de que el certificado que se verifica no ha sido revocado.

Las CA utilizan bases de datos LDAP/HTTP para almacenar y distribuir CRL. También pueden utilizar otros medios, pero el concentrador VPN depende del acceso LDAP/HTTP.

La verificación HTTP CRL se introduce en la versión 3.6 o posterior del concentrador VPN. Sin embargo, la verificación CRL basada en LDAP se introdujo en las versiones anteriores de 3.x. Este documento sólo trata la comprobación de CRL mediante HTTP.

Nota: El tamaño de caché de CRL de los concentradores de la serie VPN 3000 depende de la

plataforma y no se puede configurar según el deseo del administrador.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Ha establecido correctamente el túnel IPsec desde los clientes de hardware VPN 3.x mediante certificados para la autenticación de Intercambio de claves de Internet (IKE) (sin comprobación de CRL activada).
- El concentrador VPN tiene conectividad con el servidor de la CA en todo momento.
- Si el servidor de la CA está conectado a la interfaz pública, habrá abierto las reglas necesarias en el filtro público (predeterminado).

Componentes Utilizados

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

- VPN 3000 Concentrator versión 4.0.1 C
- Cliente de hardware VPN 3.x
- Servidor de CA de Microsoft para generación de certificados y comprobación de CRL que se ejecuta en un servidor de Windows 2000.

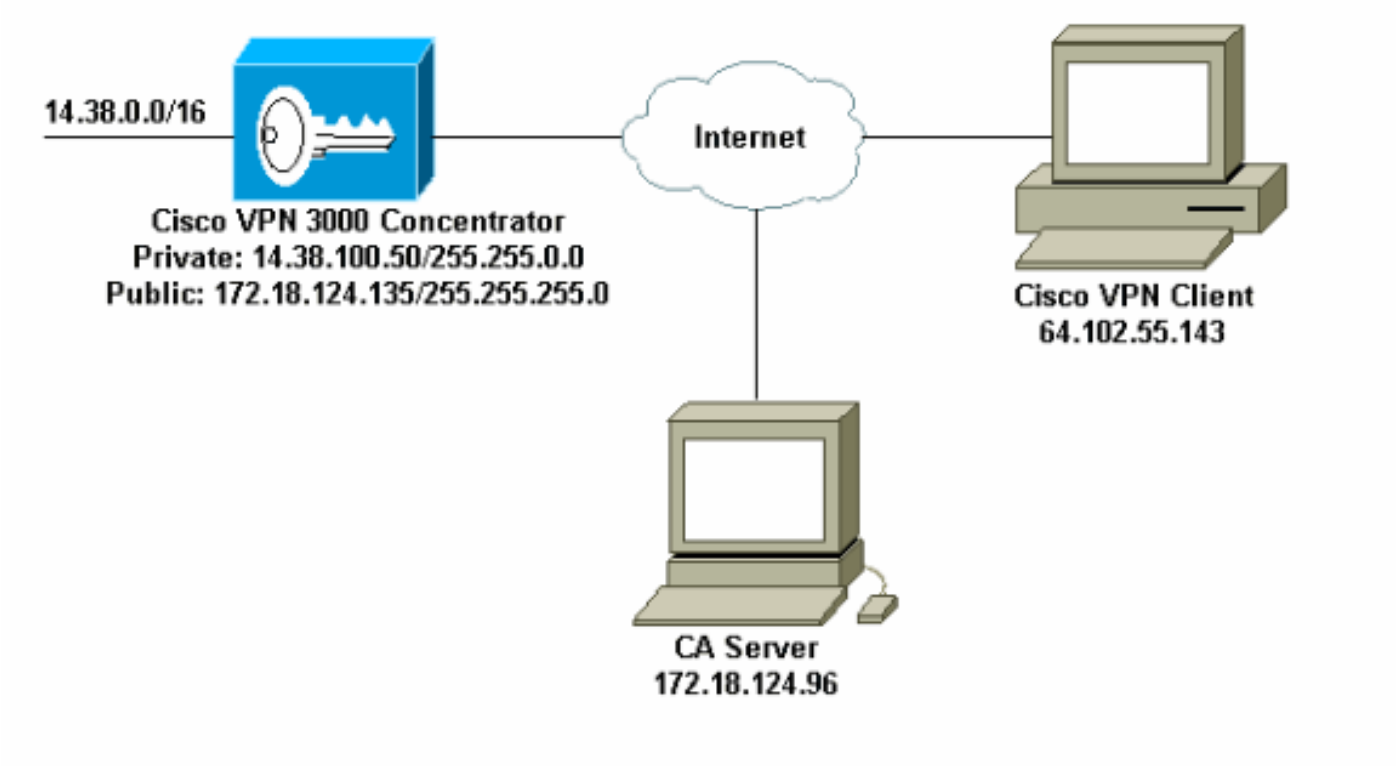
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

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:

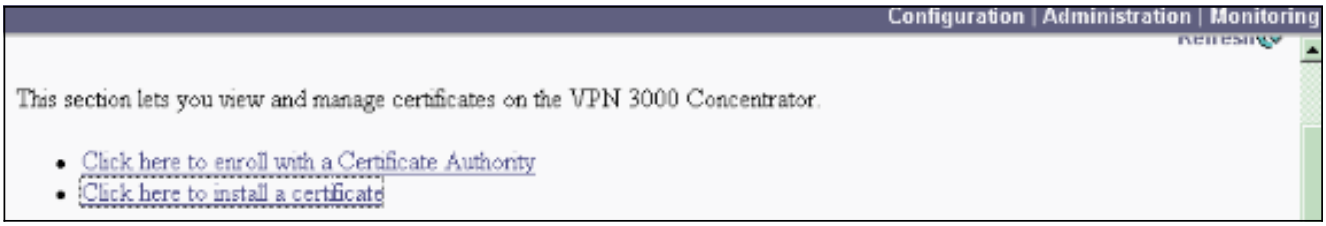


Configurar el concentrador VPN 3000

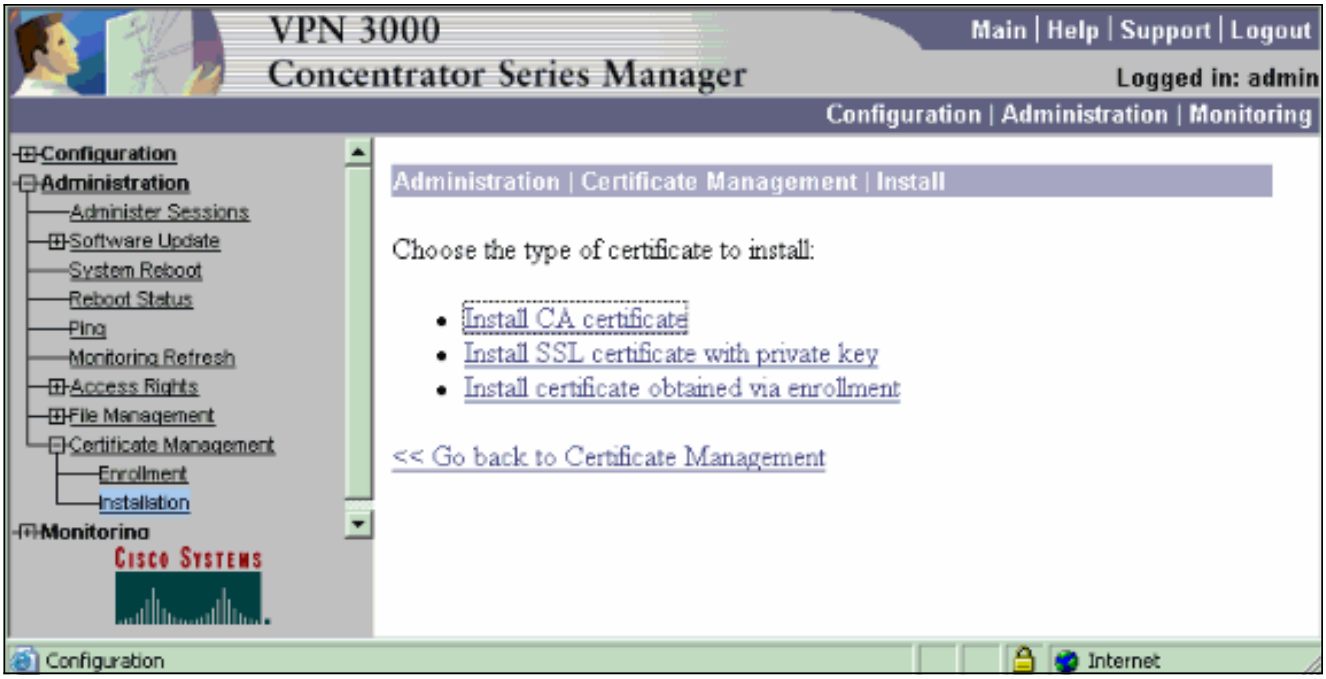
Step-by-Step Instructions

Complete estos pasos para configurar el VPN 3000 Concentrator:

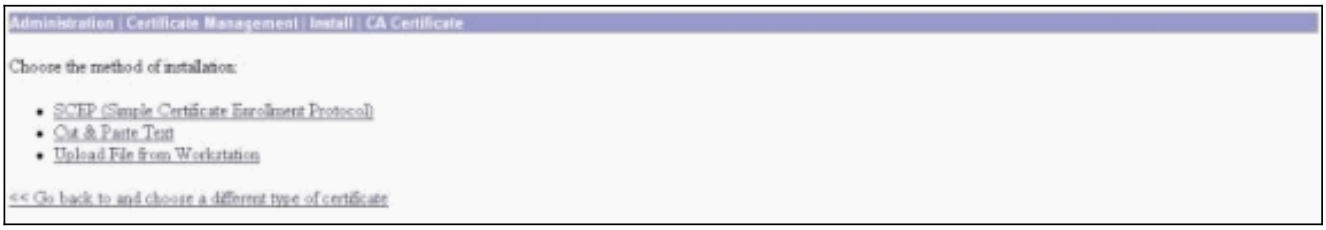
1. Seleccione **Administration > Certificate Management** para solicitar un certificado si no tiene un certificado.Seleccione **Haga clic aquí para instalar un certificado** para instalar el certificado raíz en el concentrador VPN.



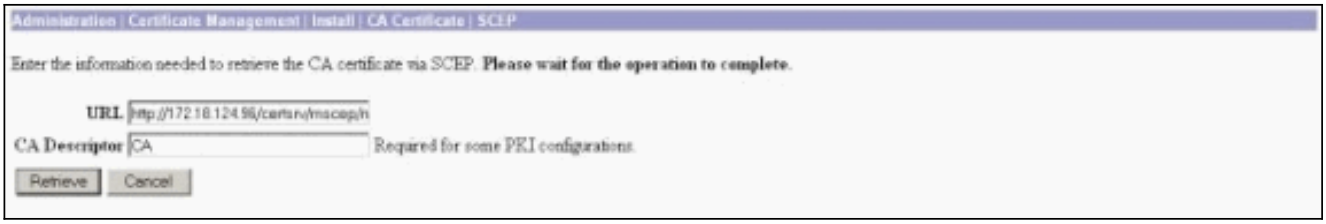
2. Seleccione **Instalar certificado de CA**.



3. Seleccione **SCEP (protocolo simple de inscripción de certificados)** para recuperar los certificados de
CA.

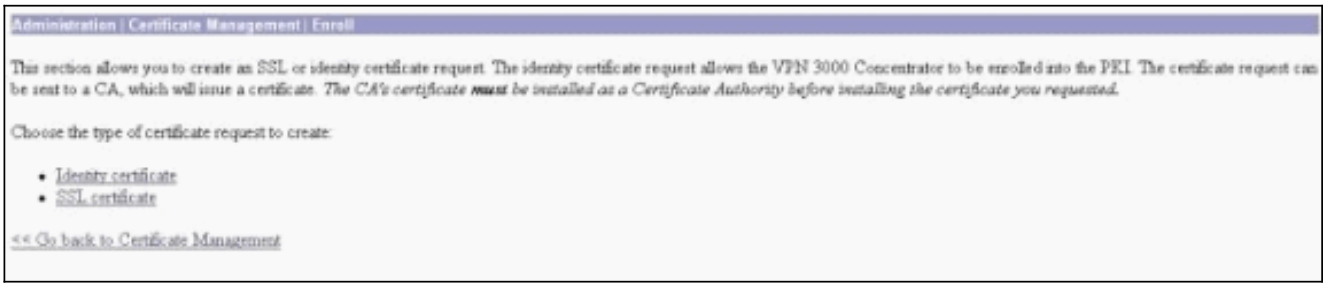


4. En la ventana SCEP, introduzca la URL completa del servidor de la CA en el cuadro de diálogo URL.En este ejemplo, la dirección IP del servidor de la CA es 172.18.124.96. Dado que este ejemplo utiliza el servidor CA de Microsoft, la URL completa es http://172.18.124.96/certsrv/mscep/mscep.dll. A continuación, introduzca un descriptor de una palabra en el cuadro de diálogo Descriptor de la CA. Este ejemplo utiliza
CA.

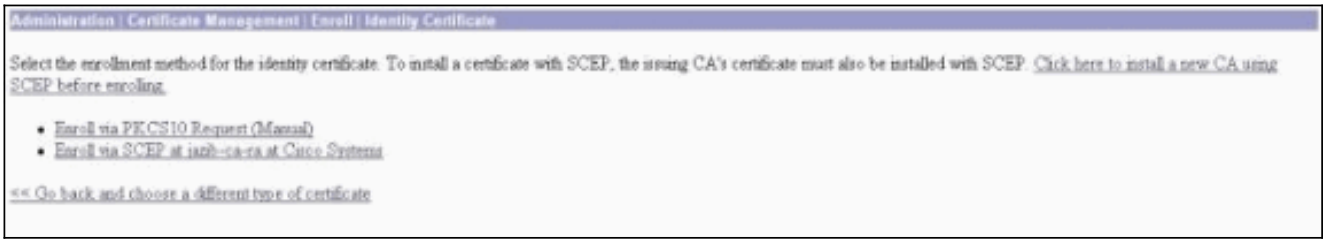


5. Haga clic en **Recuperar**.El certificado de CA debe aparecer en la ventana Administration > Certificate Management . Si no ve ningún certificado, vuelva al paso 1 y siga el procedimiento de
nuevo.

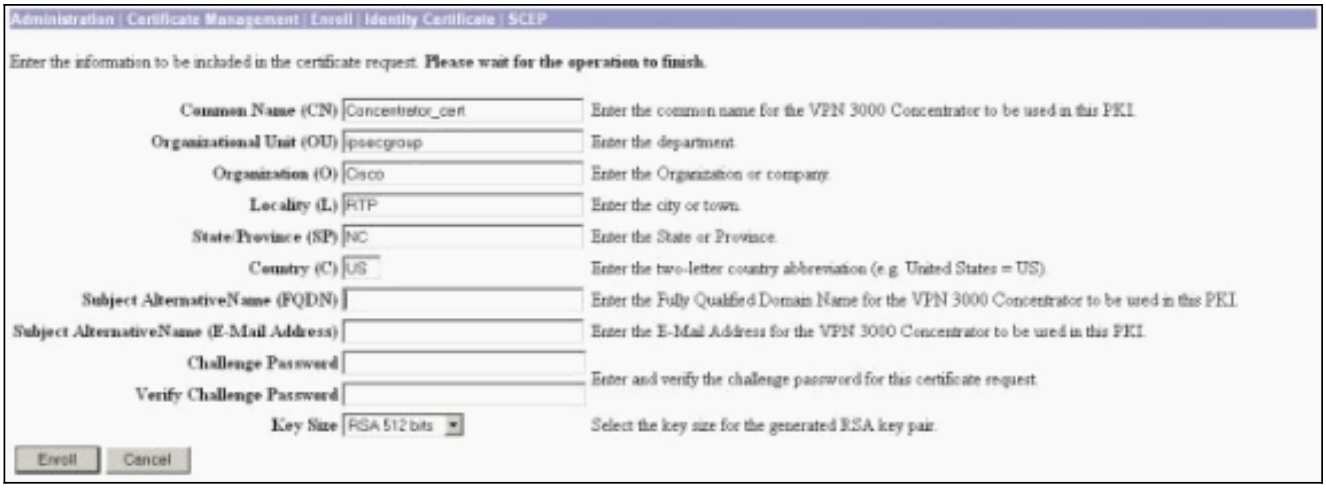
6. Una vez que tenga el certificado de CA, seleccione **Administration > Certificate Management > Enroll** y haga clic en **Identity certificate**.



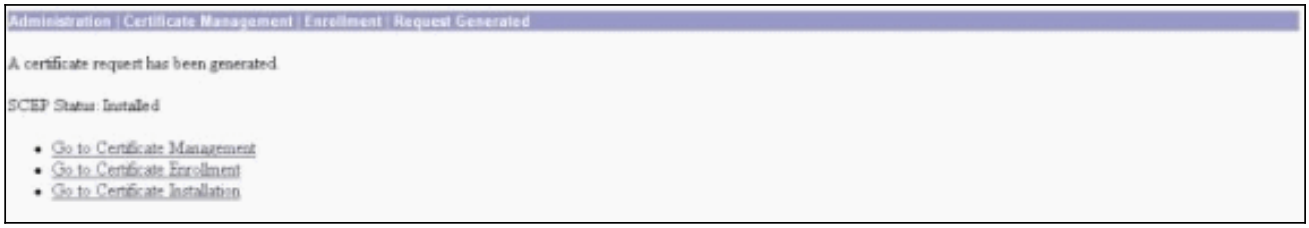
7. Haga clic en **Inscribirse a través de SCEP en ...** para solicitar el certificado de identidad.



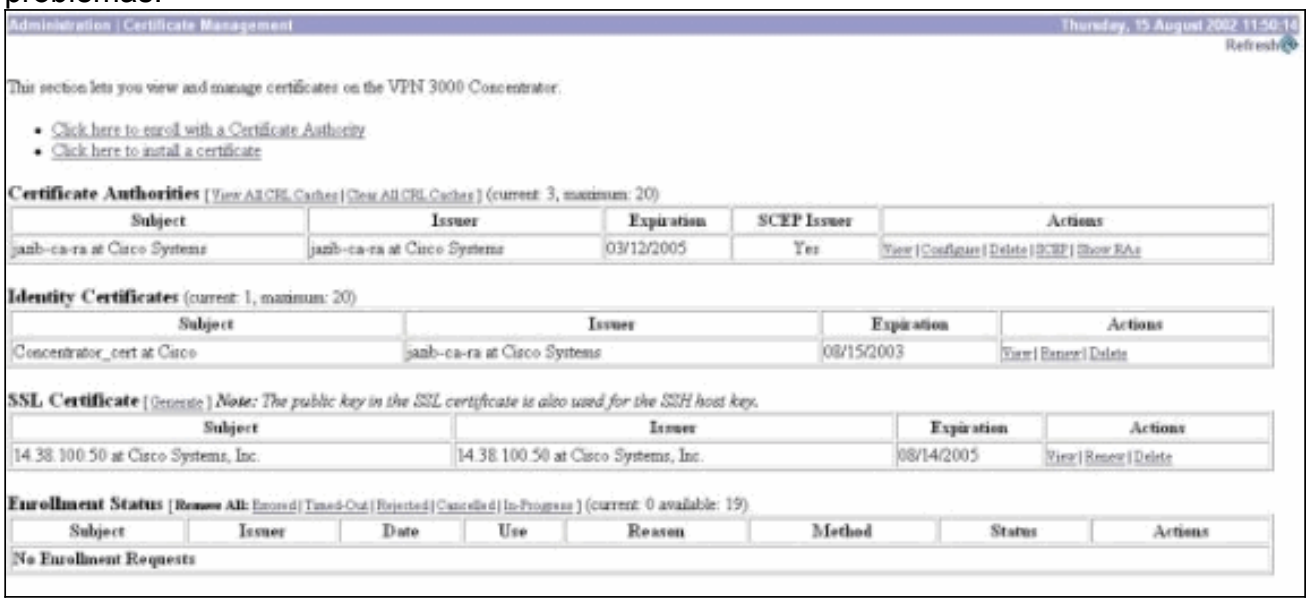
8. Complete estos pasos para completar el formulario de inscripción:Introduzca el nombre común del concentrador VPN que se utilizará en la infraestructura de clave pública (PKI) en el campo Nombre común (CN).Introduzca su departamento en el campo Unidad organizativa (OU). El OU debe coincidir con el nombre de grupo IPSec configurado.Introduzca su organización o empresa en el campo Organización (O).Introduzca su ciudad en el campo Localidad (L).Introduzca su estado o provincia en el campo Estado o provincia (SP).Introduzca su país en el campo País (C).Introduzca el nombre de dominio completo (FQDN) del concentrador VPN que se utilizará en la PKI en el campo Nombre de dominio completo (FQDN).Introduzca la dirección de correo electrónico del concentrador VPN que se utilizará en la PKI en el campo Nombre alternativo del asunto (dirección de correo electrónico).Introduzca la contraseña de desafío para la solicitud de certificado en el campo Contraseña de desafío.Vuelva a introducir la contraseña de desafío en el campo Verify Challenge Password (Verificar contraseña de desafío).Seleccione el tamaño de clave para el par de claves RSA generado en la lista desplegable Tamaño de clave.



9. Seleccione **Inscribirse** y vea el estado SCEP en el estado de sondeo.
10. Vaya al servidor de la CA para aprobar el certificado de identidad. Una vez que se haya aprobado en el servidor de la CA, se debe instalar el estado de SCEP.



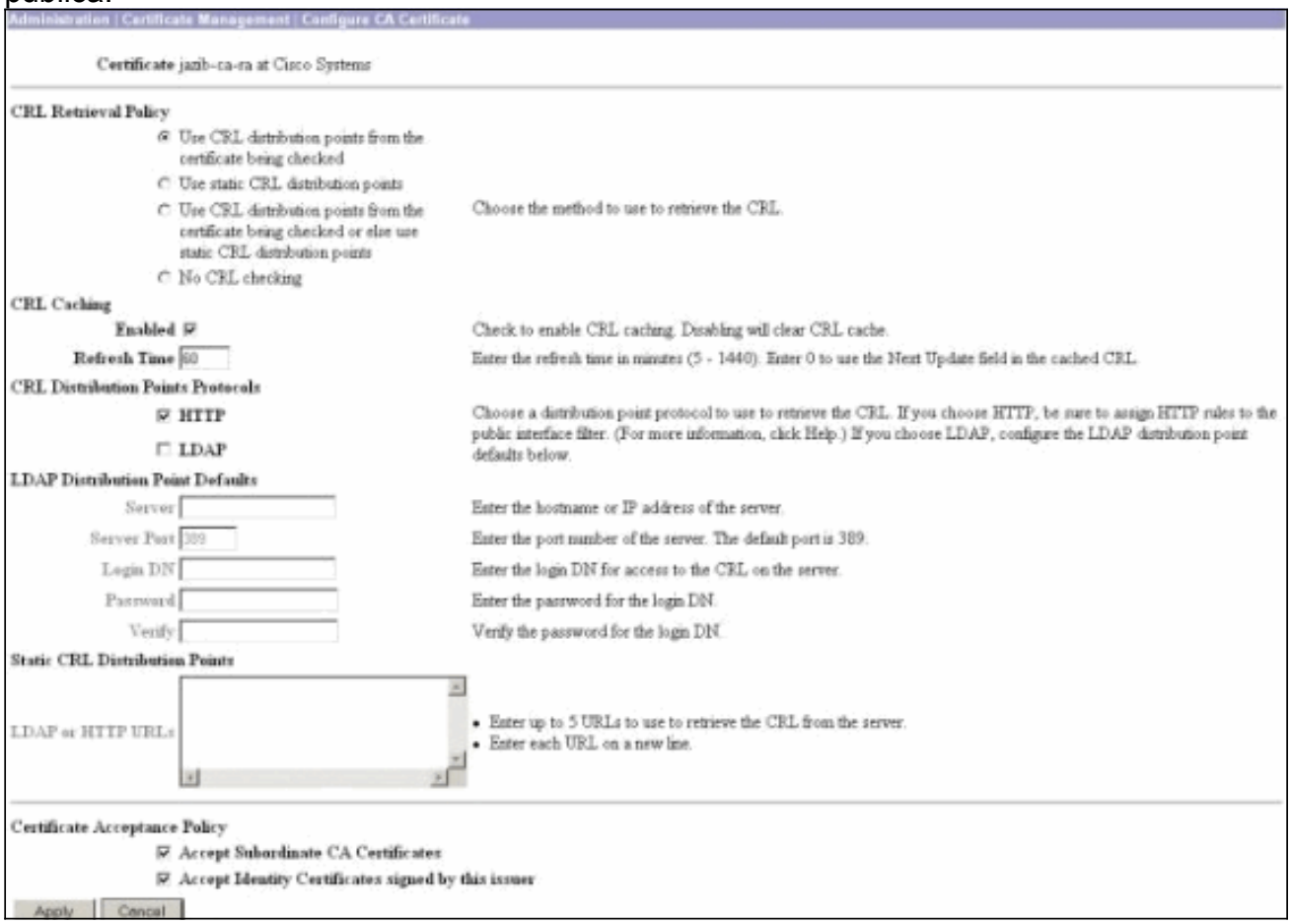
11. En Administración de certificados, debe ver su certificado de identidad.Si no lo hace, verifique los registros en su servidor de la CA para obtener más información sobre la resolución de problemas.



12. Seleccione **Ver** en el certificado recibido para ver si el certificado tiene un punto de distribución de CRL (CDP).CDP enumera todos los puntos de distribución de CRL del emisor de este certificado. Si tiene CDP en el certificado y utiliza un nombre DNS para enviar una consulta al servidor CA, asegúrese de que tiene servidores DNS definidos en el concentrador VPN para resolver el nombre de host con una dirección IP. En este caso, el nombre de host del servidor de la CA de ejemplo es jazib-pc que se resuelve en una dirección IP de 172.18.124.96 en el servidor DNS.

13. Haga clic en **Configurar** en su certificado de CA para habilitar la verificación CRL en los certificados recibidos.Si tiene CDP en el certificado recibido y desea utilizarlo, seleccione **Usar puntos de distribución CRL del certificado que se está comprobando**.Dado que el sistema tiene que recuperar y examinar la CRL desde un punto de distribución de red, habilitar la comprobación de CRL puede ralentizar los tiempos de respuesta del sistema. Además, si la red es lenta o está congestionada, la comprobación de CRL podría fallar. Habilite el almacenamiento en caché de CRL para mitigar estos problemas potenciales. Esto almacena las CRL recuperadas en la memoria volátil local y, por lo tanto, permite que el concentrador VPN verifique el estado de revocación de los certificados más rápidamente.Con el almacenamiento en caché de CRL habilitado, el VPN Concentrator verifica primero si la CRL requerida existe en la memoria caché y verifica el número de serie del certificado con la lista de números de serie en la CRL cuando necesita verificar el estado de revocación de un certificado. El certificado se considera revocado si se encuentra su número de serie. El concentrador VPN recupera una CRL de un servidor externo cuando no encuentra la CRL necesaria en la memoria caché, cuando el período de validez de la CRL almacenada en la memoria caché ha caducado o cuando ha transcurrido el tiempo de actualización configurado. Cuando el concentrador VPN recibe una nueva CRL de un servidor externo, actualiza la memoria caché con la nueva CRL. La caché puede contener hasta 64 CRL.**Nota:** La caché CRL existe en la memoria. Por lo tanto, al reiniciar el concentrador VPN se borra la memoria caché de CRL. El concentrador VPN vuelve a llenar la caché de CRL con CRL actualizadas a medida que procesa nuevas solicitudes de autenticación de peer.Si selecciona **Usar puntos de distribución CRL estáticos**, puede utilizar hasta cinco puntos de distribución CRL estáticos, como se especifica en esta ventana. Si elige esta opción, debe introducir al menos una dirección URL.También puede seleccionar **Usar puntos de distribución CRL del certificado que se está comprobando**, o **Usar puntos de distribución CRL estáticos**. Si el concentrador VPN no puede encontrar cinco puntos de distribución CRL en el certificado, agrega puntos de distribución CRL estáticos, hasta un límite de cinco. Si elige esta opción, active al menos un protocolo de punto de distribución CRL. También debe introducir al menos uno (y no más de cinco) puntos de distribución CRL estáticos.Seleccione **No CRL Check** si desea inhabilitar la verificación CRL.En CRL Caching, seleccione el cuadro **Enabled** para permitir que el concentrador VPN almacene en caché las CRL recuperadas. El valor predeterminado no es habilitar el almacenamiento en caché de CRL. Cuando desactiva el almacenamiento en caché de CRL (deseleccione el cuadro), se borra la caché de CRL.Si ha configurado una política de recuperación de CRL que utiliza puntos de distribución de CRL del certificado que se está comprobando, elija un protocolo de punto de distribución

que se utilice para recuperar la CRL. Elija **HTTP** en este caso para recuperar la CRL. Asigne reglas HTTP al filtro de interfaz pública si el servidor de la CA se dirige a la interfaz pública.



Control

Seleccione **Administration > Certificate Management** y haga clic en **View All CRL caches** para ver si su concentrador VPN ha almacenado en caché alguna CRL del servidor de la CA.

Verificación

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

Registros del concentrador

Habilite estos eventos en el concentrador VPN para asegurarse de que la verificación CRL funcione.

1. Seleccione **Configuration > System > Events > Classes** para establecer los niveles de registro.
2. En Nombre de clase, seleccione IKE, **IKEDBG**, **IPSEC**, **IPSECDBG** o **CERT**.
3. Haga clic en **Agregar** o **Modificar**, y elija la opción **Gravedad para registrar 1-13**.
4. Haga clic en **Aplicar** si desea modificar o **Agregar** si desea agregar una nueva entrada.

Registros de concentradores exitosos

Si la comprobación de CRL se realiza correctamente, estos mensajes se muestran en 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)
```

Refiérase a Registros de Concentrador Exitosos para obtener el resultado completo de un registro de concentrador exitoso.

Registros fallidos

Si la protección CRL no se realiza correctamente, estos mensajes se muestran 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.
```

Consulte Registros del concentrador revocado para obtener la salida completa de un registro del concentrador fallido.

Refiérase a Registros de Cliente Exitosos para obtener el resultado completo de un registro de cliente exitoso.

Consulte Registros de Cliente Revocados para obtener el resultado completo de un registro de cliente fallido.

Troubleshoot

Consulte Resolución de Problemas de Conexión en el VPN 3000 Concentrator para obtener más información de troubleshooting.

Información Relacionada

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