Contenido

Introducción

Todos los Certificados digitales tienen construidos en el vencimiento en el certificado que es asignado por el servidor de publicación del Certificate Authority (CA) durante la inscripción. Cuando un certificado digital se utiliza para VPN IPSec la autenticación del ISAKMP, hay una verificación automática del tiempo del vencimiento del certificado del dispositivo de comunicación y del Tiempo del sistema en el dispositivo (punto final de VPN). De esta forma se garantiza que el certificado que se utiliza es válido y no ha vencido. Es también porqué usted *debe* fijar el reloj interno en cada punto final de VPN (router). Si [SNTP] del Network Time Protocol (NTP) (o del protocolo de tiempo de la red sencillo) no es posible en los VPN Crypto Router, después utilice el **comando set clock** manual.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en todo el Routers que funcione con la imagen para esa plataforma correspondiente.

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

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

¿Cuándo un certificado digital considerado no expiró ni se

expira?

- Se expira un certificado (inválido) si el Tiempo del sistema es después del tiempo del vencimiento del certificado o antes de la época publicada del certificado.
- Un certificado no se expira (válido) si el Tiempo del sistema está en o entre el certificado publicado tiempo y el tiempo expirado del certificado.

El propósito de la característica del Auto-alistar es proporcionar al administrador de CA con un mecanismo para permitir que un router actualmente alistado re-aliste automáticamente con su servidor de CA en un por ciento configurado del curso de la vida del certificado del router. Esto es una característica importante para la manejabilidad/la posibilidad de entretenimiento de los Certificados como mecanismo de control. Si usted utilizó CA determinado para publicar los Certificados potencialmente a miles de routers VPN de rama con un un año de por vida (sin Auto-aliste), después en exactamente un año del tiempo publicado, todos los Certificados expiran y todas las bifurcaciones pierden la Conectividad con el IPSec. Alternativamente, si se fija la característica del Auto-alistar “auto-aliste el 70", como en este ejemplo, después en el 70% del curso de la vida del certificado publicado (1 año), cada router publica automáticamente una nueva petición de la inscripción al servidor de Cisco IOS® CA enumerado en el trustpoint.

Nota: Una excepción a la característica del Auto-alistar es que si se fija a *inferior o igual 10*, después es en los minutos. Si es *mayor de 10*, después es un porcentaje del curso de la vida del certificado.

Hay algunas advertencias que el administrador de CA del Cisco IOS necesita ser consciente de con Auto-alista. El administrador necesita ejecutar estas acciones para que la reinscripción sea acertado:

1. Conceda o rechace manualmente cada petición de la reinscripción en el servidor de CA del Cisco IOS (a menos que el “auto de la concesión” se utiliza en el servidor de CA del Cisco IOS).El servidor de CA del Cisco IOS todavía necesita conceder o rechazar cada uno de éstos las peticiones (con la suposición que el Cisco IOS CA no tiene “auto de la concesión” habilitado). Sin embargo, no se requiere ninguna acción administrativa en el router que alista para comenzar el proceso de la reinscripción.
2. Salve el nuevo certificado re-alistado en el VPN Router re-que alista, si es apropiado.Si no hay cambios de configuración unsaved pendientes en el router, después el nuevo certificado se guarda automáticamente al RAM no volátil (NVRAM). El nuevo certificado se escribe en el NVRAM y se quita el certificado anterior.Si hay cambios de configuración unsaved pendientes, después usted debe publicar el **comando copy run start** en el router que alista para salvar los cambios de configuración y el nuevo certificado re-alistado en el NVRAM. Una vez que completan al **comando copy run start**, después el nuevo certificado se escribe en el NVRAM y se quita el certificado anterior.**Nota:** Cuando una nueva reinscripción es acertada, ésa no revoca el certificado anterior para eso dispositivo alistado en el servidor de CA. Cuando los dispositivos VPN comunican, se envían el número de serie del certificado (un número único).**Nota:** Por ejemplo, si usted está en el 70% del curso de la vida del certificado y una bifurcación VPN era re-alistar con CA, ese CA tiene dos Certificados para ese nombre de host. Sin embargo, el router que alista tiene solamente uno (el más nuevo). Si usted elige a, usted puede administrativo revocar el certificado viejo, o permita que expire normalmente.**Nota:** Las más nuevas versiones del código de la característica del Auto-alistar tienen una opción “para regenerar” los pares de claves usados para la inscripción.Esta opción es “no predeterminada” regenerar los pares de claves.Si esta opción fue elegida, sea

consciente del Id. de bug Cisco CSCea90136. Este arreglo del bug permite para que el nuevo par clave sea puesto en los archivos temporales mientras que la nueva inscripción del certificado ocurre sobre un túnel IPsec existente (que esté utilizando el viejo par clave).Auto-aliste tiene la opción para generar las nuevas claves en el tiempo de renovación de la certificación. Esto causa actualmente una pérdida de servicio durante el tiempo que toma para obtener un nuevo certificado. Esto es porque hay una nueva clave pero ningún certificado que la hace juego.Este featurette conserva la clave y el certificado viejos hasta que el nuevo certificado esté disponible.La generación de claves automática también se implementa para el Registro manual. Las claves se generan (según las necesidades) para automático o el Registro manual.Versión encontrada - 12.3PIH03Versión a ser adentro reparado - 12.3TVersión aplicada a - 12.3PI03Integrado adentro - NingunosPara la información adicional, Soporte técnico de Cisco del contacto.

Información Relacionada

- Página de soporte de IPSec
- Soporte Técnico - Cisco Systems