Ablauf von Zertifikaten und automatische Anmeldung zur automatischen Neuregistrierung bei Cisco IOS CA

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Wann gilt ein digitales Zertifikat als abgelaufen oder nicht abgelaufen?
Zugehörige Informationen

Einführung

Alle digitalen Zertifikate verfügen über eine integrierte Ablaufzeit im Zertifikat, das vom Server der ausstellenden Zertifizierungsstelle (Certificate Authority, CA) bei der Registrierung zugewiesen wird. Wenn ein digitales Zertifikat für die VPN IPSec-Authentifizierung von ISAKMP verwendet wird, werden die Ablaufzeit des Zertifikats des kommunizierenden Geräts und die Systemzeit auf dem Gerät (VPN-Endpunkt) automatisch überprüft. Dadurch wird sichergestellt, dass ein verwendetes Zertifikat gültig ist und nicht abgelaufen ist. Aus diesem Grund *müssen* Sie die interne Uhr auf jedem VPN-Endpunkt (Router) festlegen. Wenn das Network Time Protocol (NTP) (oder Simple Network Time Protocol (SNTP)) auf den VPN-Krypto-Routern nicht möglich ist, verwenden Sie den Befehl **set clock**.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf allen Routern, die das cXXXX-advancek9-mz.123-5.9.T-Image für die jeweilige Plattform ausführen.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Wann gilt ein digitales Zertifikat als abgelaufen oder nicht abgelaufen?

- Ein Zertifikat ist abgelaufen (ungültig), wenn die Systemzeit nach Ablauf des Zertifikats oder vor der Ausstellung des Zertifikats liegt.
- Ein Zertifikat ist nicht abgelaufen (gültig), wenn die Systemzeit zu oder zwischen der Ausgabe des Zertifikats und der abgelaufenen Zeit des Zertifikats liegt.

Die Funktion zur automatischen Registrierung bietet dem CA-Administrator einen Mechanismus, mit dem sich ein aktuell angemeldeter Router automatisch für einen konfigurierten Prozentsatz der Lebensdauer des Router-Zertifikats bei seinem CA-Server neu anmelden kann. Dies ist eine wichtige Funktion für die Verwaltbarkeit/Unterstützung der Zertifikate als Kontrollmechanismus. Wenn Sie eine bestimmte Zertifizierungsstelle für die Ausstellung von Zertifikaten an potenziell Tausende von VPN-Routern in Zweigstellen mit einer Lebensdauer von einem Jahr (ohne automatische Anmeldung) verwendet haben, laufen in genau einem Jahr nach der Ausstellung alle Zertifikate ab, und alle Zweigstellen verlieren die Verbindungen durch IPSec. Wenn die Funktion für die automatische Anmeldung wie in diesem Beispiel auf "auto-enroll 70" (automatische Anmeldung 70) festgelegt ist, gibt jeder Router in 70 % der Lebensdauer des ausgestellten Zertifikats (1 Jahr) automatisch eine neue Registrierungsanfrage für den im Trustpoint aufgeführten Cisco IOS® CA-Server aus.

Hinweis: Eine Ausnahme von der Funktion für die automatische Anmeldung ist, dass es in Minuten ist, wenn sie auf *maximal 10* festgelegt ist. Wenn es *größer als 10* ist, ist dies ein Prozentsatz der Lebensdauer des Zertifikats.

Bei der automatischen Registrierung muss der Cisco IOS CA-Administrator einige Vorbehalte beachten. Der Administrator muss diese Schritte ausführen, damit die erneute Anmeldung erfolgreich ist:

1. Gewähren oder Ablehnen jeder erneuten Registrierungsanfrage auf dem Cisco IOS CA-Server manuell (es sei denn, auf dem Cisco IOS CA-Server wird "Allow auto" verwendet).Der Cisco IOS CA-Server muss weiterhin jede dieser Anfragen entweder unterstützen oder ablehnen (unter der Annahme, dass die Cisco IOS CA die Funktion "auto" nicht aktiviert hat). Der Registrierungsprozess für den Router muss jedoch nicht von der Administration gestartet werden.
2. Speichern Sie das neue neu angemeldete Zertifikat ggf. im neu angemeldeten VPN-Router.Wenn im Router keine ungespeicherten Konfigurationsänderungen ausstehen, wird das neue Zertifikat automatisch im Non-Volatile RAM (NVRAM) gespeichert. Das neue Zertifikat wird im NVRAM geschrieben, und das vorherige Zertifikat wird entfernt.Wenn ungespeicherte Konfigurationsänderungen ausstehen, müssen Sie den Befehl **copy run start** auf dem registrierenden Router ausführen, um die Konfigurationsänderungen und das neu angemeldete Zertifikat im NVRAM zu speichern. Wenn der Befehl **copy run start** abgeschlossen ist, wird das neue Zertifikat im NVRAM geschrieben und das vorherige Zertifikat entfernt.**Hinweis:** Wenn eine erneute Anmeldung erfolgreich ist, wird das vorherige Zertifikat für das registrierte Gerät auf dem CA-Server *nicht* widerrufen. Wenn VPN-Geräte

kommunizieren, senden sie einander die Seriennummer des Zertifikats (eine eindeutige Nummer).**Hinweis:** Wenn Sie sich beispielsweise zu 70 % der Lebensdauer des Zertifikats befinden und eine VPN-Zweigstelle die erneute Anmeldung bei der Zertifizierungsstelle vornehmen sollte, verfügt die Zertifizierungsstelle über zwei Zertifikate für diesen Hostnamen. Der Router, der die Registrierung vornimmt, hat jedoch nur einen (den neueren). Wenn Sie dies wünschen, können Sie das alte Zertifikat administrativ widerrufen oder zulassen, dass es normal abläuft.**Hinweis:** Die neueren Codeversionen der automatischen Registrierung bieten die Möglichkeit, die für die Registrierung verwendeten Schlüsselpaare neu zu erstellen.Diese Option ist "not default", um Schlüsselpaare neu zu generieren.Wenn diese Option ausgewählt wurde, beachten Sie die Cisco Bug-ID CSCea90136. Diese Fehlerbehebung ermöglicht es, das neue Schlüsselpaar in temporären Dateien zu speichern, während die neue Zertifikatregistrierung über einen vorhandenen IPSec-Tunnel erfolgt (d. h. über das alte Schlüsselpaar).Bei der automatischen Anmeldung können Sie bei der Erneuerung der Zertifizierung neue Schlüssel erstellen. Derzeit führt dies zu einem Service-Verlust während der Zeit, die für den Erhalt eines neuen Zertifikats erforderlich ist. Der Grund hierfür ist, dass ein neuer Schlüssel vorhanden ist, aber kein Zertifikat, das ihm entspricht.Diese Funktion behält den alten Schlüssel und das alte Zertifikat bei, bis das neue Zertifikat verfügbar ist.Die automatische Schlüsselgenerierung wird auch für die manuelle Registrierung implementiert. Schlüssel werden (je nach Bedarf) für die automatische oder manuelle Registrierung generiert.Version gefunden - 12.3PIH03Version zu reparieren in - 12.3TVersion angewendet auf - 12.3PI03Integriert in - KeineWeitere Informationen erhalten Sie vom technischen Support von Cisco.

Zugehörige Informationen

- IPSec-Support-Seite
- Technischer Support - Cisco Systems