Cisco IOS CA에 자동 재등록을 위한 인증서 만료 및 자동 등록

목차

소개

모든 디지털 인증서는 등록 중에 발급 CA(인증 기관) 서버에서 할당한 인증서에 기본적으로 만료 시간이 있습니다.ISAKMP의 VPN IPSec 인증에 디지털 인증서가 사용되는 경우 통신 디바이스의 인증서 만료 시간 및 디바이스(VPN 엔드포인트)의 시스템 시간을 자동으로 확인합니다. 이렇게 하면 사용된 인증서가 유효하며 만료되지 않습니다.또한 각 VPN 엔드포인트(라우터)에 내부 클록을 설정해야 *합니다*. VPN 암호화 라우터에서 NTP(Network Time Protocol)(또는 SNTP[Simple Network Time Protocol])를 사용할 수 없는 경우 수동 **set clock** 명령을 사용합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 해당 플랫폼에 대해 cXXXX-advsecurityk9-mz.123-5.9.T 이미지를 실행하는 모든 라우터를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

디지털 인증서는 언제 만료되었거나 만료되지 않은 것으로 간주됩

니까?

- 시스템 시간이 인증서 만료 시간 이후이거나 인증서의 발급 시간 이전인 경우 인증서가 만료됨(유효하지 않음)
- 시스템 시간이 인증서의 발급 시간과 인증서의 만료 시간 사이에 있는 경우 인증서가 만료되지 않습니다(유효).

자동 등록 기능의 목적은 CA 관리자에게 현재 등록된 라우터가 라우터 인증서 수명의 구성된 백분율로 CA 서버에 자동으로 재등록할 수 있도록 하는 메커니즘을 제공하는 것입니다.이는 제어 메커니즘으로서 인증서의 관리 용이성/지원 용이성을 위해 중요한 기능입니다.특정 CA를 사용하여 1년 수명(자동 등록 없이)으로 수천 개의 지점 VPN 라우터에 인증서를 발급하면 발급된 시간 중 정확히 1년 이내에 모든 인증서가 만료되고 모든 브랜치는 IPSec을 통해 연결이 끊깁니다.또는 이 예에서와 같이 자동 등록 기능이 "자동 등록 70"으로 설정된 경우 발급된 인증서의 수명(1년)의 70%에서 각 라우터는 신뢰 지점에 나열된 Cisco IOS® CA 서버에 새 등록 요청을 자동으로 발행합니다.

참고: 자동 등록 기능의 한 가지 예외 사항은 자동 등록 기능이 *10보다 작거나 같도록* 설정된 경우 분 단위입니다.*10보다 큰* 경우 인증서 수명의 백분율입니다.

Cisco IOS CA 관리자가 자동 등록을 통해 알아야 할 몇 가지 주의 사항이 있습니다.관리자가 재등록을 성공하려면 다음 작업을 실행해야 합니다.

1. Cisco IOS CA 서버에서 각 재등록 요청을 수동으로 허용하거나 거부합니다(Cisco IOS CA 서버에서 "grant auto"를 사용하지 않는 한).Cisco IOS CA 서버는 이러한 각 요청을 승인하거나 거부해야 합니다(Cisco IOS CA에 "grant auto"가 활성화되지 않았다고 가정). 그러나 재등록 프로세스를 시작하려면 라우터 등록에 대한 관리 작업이 필요하지 않습니다.
2. 필요한 경우 재등록된 새 인증서를 재등록 VPN 라우터에 저장합니다.라우터에 보류 중인 저장되지 않은 컨피그레이션 변경 사항이 없는 경우 새 인증서가 Non-Volatile RAM(NVRAM)에 자동으로 저장됩니다. 새 인증서가 NVRAM에 기록되고 이전 인증서가 제거됩니다.대기 중인 저장되지 않은 컨피그레이션 변경 사항이 있는 경우 컨피그레이션 변경 사항 및 새 재등록된 인증서를 NVRAM에 저장하려면 등록 라우터에서 **copy run start** 명령을 실행해야 합니다 .copy **run start** 명령이 완료되면 새 인증서가 NVRAM에 기록되고 이전 인증서가 제거됩니다 .**참고:** 새 재등록이 성공하면 CA 서버에서 등록된 디바이스에 대한 이전 인증서가 취소되지 *않습니다*.VPN 디바이스가 통신할 때 인증서 일련 번호(고유 번호)를 서로 전송합니다.**참고:** 예를 들어 인증서 수명의 70%에 있고 VPN 분기가 CA에 재등록하는 경우 해당 CA에는 해당 호스트 이름에 대한 두 개의 인증서가 있습니다.그러나 등록된 라우터에는 하나만 있습니다(최신 라우터). 선택 한 경우 관리 적으로 이전 인증서를 취소 하거나 정상적으로 만료 할 수 있습니다.**참고:** 자동 등록 기능의 최신 코드 버전에는 등록에 사용되는 키 쌍을 "재생성"하는 옵션이 있습니다.이 옵션은 키 쌍을 재생성하려면 "not default"입니다.이 옵션을 선택한 경우 Cisco 버그 ID CSCea90136에 유의하십시오. 이 버그 픽스를 사용하면 새 인증서 등록이 기존 IPSec 터널(기존 키 쌍을 사용하는)을 통해 수행되는 동안 새 키 쌍을 임시 파일에 넣을 수 있습니다.자동 등록에는 인증 갱신 시점에 새 키를 생성할 수 있는 옵션이 있습니다.현재 이 경우 새 인증서를 가져오는 데 걸리는 시간 동안 서비스 손실이 발생합니다.이는 새 키가 있지만 일치하는 인증서가 없기 때문입니다.이 기능은 새 인증서를 사용할 수 있을 때까지 이전 키와 인증서를 유지합니다.자동 키 생성도 수동 등록을 위해 구현됩니다.자동 또는 수동 등록을 위해 필요한 경우 키가 생성됩니다.버전 발견 - 12.3PIH03수정될 버전 - 12.3T버전 적용 대상 - 12.3PI03통합 - 없음자세한 내용은 Cisco 기술 지원에 문의하십시오.

관련 정보

- IPSec 지원 페이지
- Technical Support - Cisco Systems