PIX/ASA 7.x:CAC - Cisco VPN 클라이언트에 대한 스마트 카드 인증

목차

소개

이 문서에서는 인증을 위해 CAC(Common Access Card)를 사용하는 네트워크 원격 액세스를 위한 Cisco ASA(Adaptive Security Appliance)의 샘플 컨피그레이션을 제공합니다.

이 문서의 범위는 Cisco ASA with Adaptive Security Device Manager(ASDM), Cisco VPN Client 및 Microsoft AD(Active Directory)/LDAP(Lightweight Directory Access Protocol)의 컨피그레이션을 다룹니다.

이 가이드의 컨피그레이션에서는 Microsoft AD/LDAP 서버를 사용합니다.이 문서에서는 OCSP 및 LDAP 특성 맵과 같은 고급 기능도 다룹니다.

사전 요구 사항

요구 사항

Cisco ASA, Cisco VPN Client, Microsoft AD/LDAP 및 PKI(Public Key Infrastructure)에 대한 기본적인 지식은 전체 설정을 이해하는 데 유용합니다.AD 그룹 멤버십 및 사용자 속성 및 LDAP 객체에 대해 잘 알고 있으면 인증서 특성과 AD/LDAP 객체 간의 권한 부여 프로세스의 상관관계를 파악할 수 있습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 7.2(2)를 실행하는 Cisco 5500 Series ASA(Adaptive Security Appliance)
- Cisco ASDM(Adaptive Security Device Manager) 버전 5.2(1)
- Cisco VPN Client 4.x

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 규칙을 참조하십시오.

Cisco ASA 컨피그레이션

이 섹션에서는 ASDM을 통한 Cisco ASA의 컨피그레이션에 대해 설명합니다.IPsec 연결을 통해 VPN 원격 액세스 터널을 구축하는 데 필요한 단계를 다룹니다.CAC 인증서는 인증에 사용되며 인증서의 UPN(User Principal Name) 특성은 권한 부여를 위해 Active Directory에 채워집니다.

구축 고려 사항

- 이 설명서에서는 인터페이스, DNS, NTP, 라우팅, 디바이스 액세스 또는 ASDM 액세스 등의 기본 컨피그레이션에 대해 다루지 않습니다.네트워크 운영자가 이러한 컨피그레이션에 익숙하다고 가정합니다.자세한 내용은 다기능 보안 어플라이언스를 참조하십시오.
- 일부 섹션은 기본 VPN 액세스에 필요한 필수 컨피그레이션입니다.예를 들어 OCSP 검사, LDAP 매핑 검사 없이 CAC 카드로 VPN 터널을 설정할 수 있습니다.DoD는 OCSP 검사를 지시하지만 터널은 OCSP가 구성되지 않은 상태에서 작동합니다.
- 필요한 기본 ASA/PIX 이미지는 7.2(2) 및 ASDM 5.2(1)이지만 이 설명서에서는 7.2.2.10 및 ASDM 5.2.2.54의 임시 빌드를 사용합니다.
- LDAP 스키마를 변경할 필요가 없습니다.
- 추가 정책 시행을 위한 LDAP 및 동적 액세스 정책 매핑 예는 부록 A를 참조하십시오.
- MS에서 LDAP 객체를 확인하는 방법은 부록 D를 참조하십시오.
- 관련 정보 참조