PIX/ASA 7.x: CAC - SmartCards-Authentifizierung für Cisco VPN-Client

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Cisco ASA-Konfiguration
Überlegungen zur Bereitstellung
Konfiguration von Authentifizierung, Autorisierung, Abrechnung (AAA)
LDAP-Server konfigurieren
Trustpoints verwalten
Schlüssel generieren
Installation von CA Trustpoints
Wurzelzertifikate installieren
ASA registrieren und Identitätszertifikat installieren
VPN-Konfiguration
Erstellen von Tunnelgruppen- und Gruppenrichtlinien
Tunnelgruppenschnittstelle und Bildeinstellungen
Konfigurieren der IKE/ISAKMP-Parameter
IPSec-Parameter konfigurieren
Konfigurieren von OCSP
Konfigurieren des OCSP-Responder-Zertifikats
CA zur Verwendung von OCSP konfigurieren
Konfigurieren der OCSP-Regeln
Konfiguration des Cisco VPN-Clients
Cisco VPN-Client starten
Neue Verbindung
Remote-Zugriff starten
Anhang A - LDAP-Zuordnung
Szenario 1: Active Directory-Durchsetzung mit Remote Access Permission Dial-in - Zugriff zulassen/verweigern
Active Directory-Einrichtung
ASA-Konfiguration
Szenario 2: Active Directory-Durchsetzung mit Gruppenmitgliedschaft zum Zulassen/Verweigern des Zugriffs
Active Directory-Einrichtung
ASA-Konfiguration

Anhang B - ASA CLI-Konfiguration
Anhang C: Fehlerbehebung
Fehlerbehebung AAA und LDAP
Beispiel 1: Zulässige Verbindung mit richtiger Attributzuordnung
Beispiel 2: Zulässige Verbindung mit falsch konfigurierter Cisco Attributzuordnung
Fehlerbehebung Zertifizierungsstelle/OCSP
Fehlerbehebung IPSEC
Anhang D Überprüfen von LDAP-Objekten in MS
LDAP-Viewer
Active Directory Services-Schnittstelleneditor
Zugehörige Informationen

Einführung

Dieses Dokument enthält eine Beispielkonfiguration auf der Cisco Adaptive Security Appliance (ASA) für den Remote-Zugriff auf das Netzwerk mit der Common Access Card (CAC) für die Authentifizierung.

Der Umfang dieses Dokuments umfasst die Konfiguration der Cisco ASA mit dem Adaptive Security Device Manager (ASDM), dem Cisco VPN Client und dem Microsoft Active Directory (AD)/Lightweight Directory Access Protocol (LDAP).

Die Konfiguration in diesem Handbuch verwendet den Microsoft AD/LDAP-Server. Dieses Dokument behandelt auch erweiterte Funktionen wie OCSP und LDAP-Attributzuordnungen.

Voraussetzungen

Anforderungen

Grundlegende Informationen über Cisco ASA, Cisco VPN Client, Microsoft AD/LDAP und Public Key Infrastructure (PKI) sind hilfreich, um die vollständige Einrichtung zu verstehen. Die Vertrautheit mit der AD-Gruppenmitgliedschaft und den Benutzereigenschaften sowie mit LDAP-Objekten hilft, den Autorisierungsprozess zwischen den Zertifikatattributen und AD/LDAP-Objekten zu korrelieren.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Adaptive Security Appliance (ASA) der Serie 5500, die die Software Version 7.2(2) ausführt
- Cisco Adaptive Security Device Manager (ASDM) Version 5.2(1)
- Cisco VPN-Client 4.x

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 (Technische Tipps zu Konventionen von Cisco).

Cisco ASA-Konfiguration

Dieser Abschnitt behandelt die Konfiguration von Cisco ASA über ASDM. Es beschreibt die erforderlichen Schritte zur Bereitstellung eines VPN-Remote-Zugriffstunnels über eine IPsec-Verbindung. Das CAC-Zertifikat wird für die Authentifizierung verwendet, und das User Principal Name (UPN)-Attribut im Zertifikat wird zur Autorisierung in das aktive Verzeichnis eingetragen.

Überlegungen zur Bereitstellung

- In diesem Leitfaden werden KEINE Basiskonfigurationen wie Schnittstellen, DNS, NTP, Routing, Gerätezugriff oder ASDM-Zugriff behandelt. Es wird davon ausgegangen, dass der Netzwerkbetreiber mit diesen Konfigurationen vertraut ist.Weitere Informationen finden Sie unter Multifunktions-Sicherheitslösungen.
- Einige Abschnitte sind obligatorische Konfigurationen für den grundlegenden VPN-Zugriff. Beispielsweise kann ein VPN-Tunnel mit der CAC-Karte ohne OCSP-Prüfungen eingerichtet werden, LDAP-Zuordnungsprüfungen. Der DoD erfordert eine OCSP-Überprüfung, aber der Tunnel funktioniert ohne konfiguriertes OCSP.
- Das grundlegende ASA/PIX-Image ist 7.2(2) und ASDM 5.2(1). In diesem Leitfaden wird jedoch eine vorläufige Build 7.2.2.10 und ASDM 5.2.2.54 verwendet.
- Es ist keine LDAP-Schemaänderung erforderlich.
- Siehe Anhang A für Beispiele für die Zuordnung von LDAP- und dynamischen Zugriffsrichtlinien.
- Siehe Anhang D zur Überprüfung von LDAP-Objekten in MS.
- Weitere Informationen