PIX/ASA 7.x: CAC - Smart Cards verificatie voor Cisco VPN-client

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor Cisco adaptieve security applicatie (ASA) voor netwerk externe toegang met de Common Access Card (CAC) voor verificatie.

Het toepassingsgebied van dit document bestrijkt de configuratie van Cisco ASA met Adaptieve Security Devices Manager (ASDM), Cisco VPN-client en Microsoft Active Directory (AD)/Light Directory Access Protocol (LDAP).

De configuratie in deze handleiding gebruikt de Microsoft AD/LDAP server. Dit document heeft ook betrekking op geavanceerde functies, zoals OCSP- en LDAP-attributiekaarten.

Voorwaarden

Vereisten

Een basiskennis van Cisco ASA, Cisco VPN-client, Microsoft AD/LDAP en PKI-infrastructuur (Public Key Infrastructure) is gunstig om de volledige setup te begrijpen. Bekendheid met AD-groeplidmaatschap en gebruikerseigenschappen, alsook met LDAP-objecten, helpt het vergunningsproces tussen de certificaareigenschappen en AD/LDAP-objecten te correleren.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 5500 Series adaptieve security applicatie (ASA) die draait op softwareversie 7.2(2)
- Cisco Adaptieve Security Devices Manager (ASDM) versie 5.2(1)
- Cisco VPN-client 4.x

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Cisco ASA-configuratie

Deze sectie bestrijkt de configuratie van Cisco ASA via ASDM. Het omvat de noodzakelijke stappen om een VPN externe toegangstunnel door een IPsec-verbinding in te stellen. Het CAC-certificaat wordt gebruikt voor echtheidscontrole en de gebruikersbenaming (UPN) in het certificaat wordt in een actieve map voor autorisatie ingevuld.

Invoeringsoverwegingen

- Deze gids heeft GEEN betrekking op basisconfiguraties zoals interfaces, DNS, NTP, routing, apparaattoegang of ASDM-toegang, enzovoort. Verondersteld wordt dat de netwerkexploitant bekend is met deze configuraties.Raadpleeg voor meer informatie multifunctionele security applicaties.
- Sommige secties zijn verplichte configuraties nodig voor basisVPN-toegang. Een VPN-tunnel kan bijvoorbeeld worden ingesteld met de CAC-kaart zonder OCSP-controles, en dus zonder lidaf-controles. DoD verplicht om OCSP te controleren, maar de tunnel werkt zonder de OCSP ingesteld.
- Het vereiste basisbeeld ASA/PIX is 7.2(2) en ASDM 5.2(1), maar deze handleiding maakt gebruik van een interimgebouw van 7.2.2.10 en ASDM 5.2.2.54.
- Er is geen wijziging van het LGO-schema nodig.
- Zie Bijlage A voor LDAP & Dynamic Access Policy mapping voorbeelden voor extra beleidshandhaving.
- Zie Bijlage D over de controle van LGO-objecten in MS.
- Zie de verwante informatie