PIX/ASA 7.x : CAC - Authentification de cartes à puce pour le Client VPN Cisco

Contenu

Introduction

Ce document fournit une configuration d'échantillon sur l'appliance de sécurité adaptable Cisco (ASA) pour l'Accès à distance de réseau en carte d'accès commune (CAC) pour l'authentification.

La portée de ce document couvre la configuration de Cisco ASA d'Adaptive Security Device Manager (ASDM), de Client VPN Cisco, et de Directory Access Protocol de Microsoft Active Directory (AD) /Lightweight (LDAP).

La configuration de ce guide utilise le serveur de Microsoft AD/LDAP. Ce document couvre également la fonctionnalité avancée, des cartes telle qu'OCSP et de LDAP attribut.

Conditions préalables

Conditions requises

Une connaissance de base de Cisco ASA, Client VPN Cisco, Microsoft AD/LDAP, et Infrastructure à clés publiques (PKI) est salutaire pour comprendre l'installation complète. La connaissance des propriétés d'adhésion à des associations et d'utilisateur d'AD, aussi bien que le LDAP objecte des aides pour corréler le processus d'autorisation entre les attributs de certificat et les objets AD/LDAP.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- L'appliance de sécurité adaptable de gamme Cisco 5500 (l'ASA) cette exécute la version de logiciel 7.2(2)
- Version 5.2(1) du Cisco Adaptive Security Device Manager (ASDM)
- Client VPN Cisco 4.x

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configuration de Cisco ASA

Cette section couvre la configuration de Cisco ASA par l'ASDM. Il couvre les étapes nécessaires pour déployer un tunnel d'Accès à distance VPN par une connexion d'IPsec. Le certificat CAC est utilisé pour l'authentification, et l'attribut du nom principal d'utilisateur (UPN) dans le certificat est rempli dans le répertoire actif pour l'autorisation.

Considérations de déploiement

- Ce guide ne couvre pas des configurations de base telles que des interfaces, des DN, NTP, routage, accès au périphérique, ou accès ASDM, etc. On le suppose que l'opérateur réseau est au courant de ces configurations.Le pour en savoir plus, se rapportent aux dispositifs de sécurité multifonctions.
- Quelques sections sont des configurations obligatoires requises pour l'accès VPN de base. Par exemple, un tunnel VPN peut être installé avec la carte CAC sans contrôles OCSP, des mappages de LDAP vérifie. Le DoD exige OCSP vérifiant, mais les travaux de tunnel sans OCSP configuré.
- L'image de base ASA/PIX exigée est 7.2(2) et ASDM 5.2(1), mais ce guide utilise une version intermédiaire de 7.2.2.10 et d'ASDM 5.2.2.54.
- Aucune modification de schéma de LDAP n'est nécessaire.
- Voir l'annexe A pour des exemples de mappage de stratégie de LDAP et d'accès dynamique pour l'application supplémentaire de stratégie.
- Voir l'annexe D sur la façon dont vérifier des objets de LDAP dans le MS.
- Voyez les informations relatives