PIX/ASA 7.x:CAC — 思科VPN客戶端的智慧卡身份驗證

目錄

簡介

本文檔提供思科自適應安全裝置(ASA)上用於網路遠端訪問的配置示例，使用通用訪問卡(CAC)進行身份驗證。

本文檔的範圍包括配置帶有自適應安全裝置管理器(ASDM)的Cisco ASA、Cisco VPN客戶端和Microsoft Active Directory(AD)/輕量級目錄訪問協定(LDAP)。

本指南中的配置使用Microsoft AD/LDAP伺服器。本文檔還包括高級功能，例如OCSP和LDAP屬性對映。

必要條件

需求

瞭解Cisco ASA、Cisco VPN Client、Microsoft AD/LDAP和公鑰基礎設施(PKI)的基本知識有助於瞭解完整的設定。熟悉AD組成員資格和使用者屬性以及LDAP對象有助於將證書屬性和AD/LDAP對象之間的授權過程相關聯。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行軟體版本7.2(2)的Cisco 5500系列調適型安全裝置(ASA)
- 思科調適型安全裝置管理員(ASDM)版本5.2(1)
- Cisco VPN使用者端4.x

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

Cisco ASA配置

本節介紹通過ASDM配置Cisco ASA。它包括通過IPsec連線部署VPN遠端訪問隧道所需的步驟。CAC證書用於身份驗證，證書中的使用者主體名稱(UPN)屬性填充在active directory中以進行授權

。

部署注意事項

- 本指南不包括基本配置，如介面、DNS、NTP、路由、裝置訪問或ASDM訪問等。假設網路操作員熟悉這些配置。如需詳細資訊，請參閱多功能資安裝置。
- 某些部分是基本VPN訪問所需的必要配置。例如，可以使用CAC卡設定VPN隧道而不進行OCSP檢查、LDAP對映檢查。DoD強制進行OCSP檢查，但隧道在沒有配置OCSP的情況下工作。
- 所需的基本ASA/PIX映像是7.2(2)和ASDM 5.2(1)，但本指南使用7.2.2.10和ASDM 5.2.2.54的過渡版本。
- 無需更改LDAP架構。
- 有關其他策略實施，請參閱附錄A（針對LDAP和動態訪問策略對映示例）。
- 有關如何檢查MS中的LDAP對象的資訊，請參閱附錄D。
- 請參閱相關資訊