PIX/ASA 7.x：CAC - Cisco VPN Client的智能卡验证

目录

简介

本文档提供了在 Cisco 自适应安全设备 (ASA) 上针对网络远程访问进行配置的示例，其中使用通用访问卡 (CAC) 进行身份验证。

范围本文用可适应安全设备管理器(ASDM)， Cisco VPN Client和Microsoft Active Directory (AD) /Lightweight目录访问协议(LDAP)包括思科ASA的配置。

本指南中的配置使用 Microsoft AD/LDAP 服务器。本文档还论述了 OCSP 和 LDAP 属性映射等高级功能。

先决条件

要求

思科ASA、Cisco VPN Client， Microsoft AD/LDAP和公共密钥基础设施(PKI)基础知识是有利了解完整设置。熟悉 AD 组成员资格、用户属性以及 LDAP 对象，有助于关联证书属性与 AD/LDAP 对象之间的授权过程。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 该的Cisco ASA 5500系列自适应安全设备(ASA)运行软件版本7.2(2)
- Cisco Adaptive Security Device Manager (ASDM)版本5.2(1)
- Cisco VPN 客户端 4.x

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

Cisco ASA 配置

本部分包括通过 ASDM 配置 Cisco ASA 的内容。其中包含通过 IPsec 连接部署 VPN 远程访问隧道的必要步骤。CAC证书使用验证，并且在证书的用户主体名称(UPN)属性在授权的活动目录填充。

部署注意事项

- 本指南不包含基本配置（例如接口、DNS、NTP、路由、设备访问或 ASDM 访问等）。假定网络操作员已熟悉这些配置。有关详细信息，请参阅多功能安全设备。
- 某些部分是基本 VPN 访问所必需的配置。例如，可以通过 CAC 卡设置 VPN 隧道，而无需进行 OCSP 检查和 LDAP 映射检查。DoD 必须进行 OCSP 检查，但隧道无需配置 OCSP 也可以正常运行。
- 所需的基本 ASA/PIX 映像为 7.2(2) 和 ASDM 5.2(1)，但本指南使用的是 7.2.2.10 和 ASDM 5.2.2.54 的过渡版本。
- 无需更改 LDAP 架构。
- 有关更多策略实施的 LDAP 和动态访问策略映射示例，请参阅附录 A。
- 有关如何在 MS 中检查 LDAP 对象，请参阅附录 D。
- 请参阅相关信息