ASA 8.x：适用于 Windows 的 AnyConnect SSL VPN CAC 智能卡配置

目录

[相关信息](#)

简介

本文档提供在 Windows 环境下，在 Cisco 自适应安全设备 (ASA) 上针对 AnyConnect VPN 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。

范围本文是用可适应安全设备管理器(ASDM)， Cisco AnyConnect VPN客户和Microsoft Active Directory (AD) /Lightweight目录访问协议(LDAP)报道思科ASA的配置。

本指南中的配置使用 Microsoft AD/LDAP 服务器。本文也包括高级特性例如OCSP， LDAP属性地图，并且动态访问修正(DAP)。

先决条件

要求

思科ASA、思科AnyConnect客户端， Microsoft AD/LDAP和公共密钥基础设施(PKI)基本的了解是有利的在完整设置的领悟。熟悉 AD 组成员、用户属性以及 LDAP 对象有助于了解证书属性和 AD/LDAP 对象的授权过程之间的相互关系。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 以后Cisco 5500系列可适应的安全工具(ASA)该运行软件版本8.0(x)和
- ASA的8.x Cisco Adaptive Security Device Manager (ASDM) 6.x版
- 适用于 Windows 的 Cisco AnyConnect VPN 客户端

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。其中介绍了用于部署使用 SSL AnyConnect 连接的 VPN 远程访问隧道所需的步骤。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

- 本指南不讨论基本配置内容，例如接口、DNS、NTP、路由、设备访问、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。
- 红色突出显示的部分为基本 VPN 访问所必需的配置。例如， VPN通道可以设置CAC卡，无需进行OCSP检查、LDAP映射和动态访问策略(DAP)检查。DoD 需要执行 OCSP 检查，但是隧

道无需配置 OCSP 也可工作。

- 蓝色突出显示的部分是可选的高级功能，此功能可以增强设计的安全性。
- ASDM 和 AnyConnect/SSL VPN 不能使用相同接口上的相同端口。建议更改任意一个接口上的端口以便可以进行访问。例如，将端口 445 用于 ASDM，而将 443 用于 AC/SSL VPN。在 8.x. 版本中，ASDM URL 访问已发生变化。请使用 https:// **<**ip_address**>**:`<port>/admin.html`
- 所需的 ASA 映像的版本至少为 8.0.2.19，并且需要 ASDM 6.0.2。
- AnyConnect/CAC 受 Vista 支持。
- 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