PIX/ASA 7.x: CAC - SmartCards Authentication for Cisco VPN Client

Contents

Introduction

This document provides a sample configuration on Cisco Adaptive Security Appliance (ASA) for network remote access with the Common Access Card (CAC) for authentication.

The scope of this document covers the configuration of Cisco ASA with Adaptive Security Device Manager (ASDM), Cisco VPN Client, and Microsoft Active Directory (AD)/Lightweight Directory Access Protocol (LDAP).

The configuration in this guide uses the Microsoft AD/LDAP server. This document also covers advanced features, such as OCSP and LDAP attribute maps.

Prerequisites

Requirements

A basic knowledge of Cisco ASA, Cisco VPN Client, Microsoft AD/LDAP, and Public Key Infrastructure (PKI) is beneficial to understand the complete setup. Familiarity with AD group membership and user properties, as well as LDAP objects helps to correlate the authorization process between the certificate attributes and AD/LDAP objects.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 5500 Series Adaptive Security Appliance (ASA) that runs the Software Version 7.2(2)
- Cisco Adaptive Security Device Manager (ASDM) Version 5.2(1)
- Cisco VPN Client 4.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Cisco ASA Configuration

This section covers the configuration of Cisco ASA through ASDM. It covers the necessary steps to deploy a VPN remote access tunnel through an IPsec connection. The CAC certificate is used for authentication, and the User Principal Name (UPN) attribute in the certificate is populated in active directory for authorization.

Deployment Considerations

- This guide does NOT cover basic configurations such as interfaces, DNS, NTP, routing, device access, or ASDM access, etc. It is assumed that the network operator is familiar with

these configurations.For more information, refer to Multifunction Security Appliances.

- Some sections are mandatory configurations needed for basic VPN access. For example, a VPN tunnel can be setup with the CAC card without OCSP checks, LDAP mappings checks. DoD mandates OCSP checking, but the tunnel works without the OCSP configured.
- The basic ASA/PIX image required is 7.2(2) and ASDM 5.2(1), but this guide uses an interim build of 7.2.2.10 and ASDM 5.2.2.54.
- No LDAP schema change is necessary.
- See Appendix A for LDAP & Dynamic Access Policy mapping examples for additional policy enforcement.
- See Appendix D on how to check LDAP objects in MS.
- See the Related Information