PIX/ASA 7.x: CAC - Autenticação das carta inteligente para o Cisco VPN Client

Índice

Introdução

Este documento fornece uma configuração de exemplo na ferramenta de segurança adaptável de Cisco (ASA) para o Acesso remoto de rede com o cartão comum do acesso (CAC) para a autenticação.

O espaço do este capas de documento a configuração de Cisco ASA com o Security Device Manager adaptável (ASDM), o Cisco VPN Client, e o Directory Access Protocol do microsoft ative directory (AD) /Lightweight (LDAP).

A configuração neste guia usa o server de Microsoft AD/LDAP. Este documento igualmente cobre recursos avançados, tais como mapas do atributo OCSP e LDAP.

Pré-requisitos

Requisitos

Um conhecimento básico de Cisco ASA, Cisco VPN Client, Microsoft AD/LDAP, e Public Key Infrastructure (PKI) é benéfico compreender a instalação completa. A familiaridade com a membrasia do clube e as propriedades de usuário AD, assim como o LDAP objetam ajudas para correlacionar o processo da autorização entre os atributos do certificado e objetos AD/LDAP.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- A ferramenta de segurança adaptável do Cisco 5500 Series (o ASA) essa executa a versão de software 7.2(2)
- Versão 5.2(1) do Cisco Adaptive Security Device Manager (ASDM)
- Cisco VPN Client 4.x

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configuração ASA Cisco

Esta seção cobre a configuração de Cisco ASA com o ASDM. Cobre as etapas necessárias para distribuir um túnel de acesso remoto VPN através de uma conexão IPSec. O certificado CAC é usado para a autenticação, e o atributo do nome principal do usuário (UPN) no certificado é povoado no diretório ativo para a autorização.

Considerações de desenvolvimento

- Este guia não cobre configurações básicas tais como relações, DNS, NTP, roteamento, acesso de dispositivo, ou acesso ASDM, etc. Supõe-se que o operador de rede é familiar com estas configurações.Para mais informação, refira ferramentas de segurança Multifunction.
- Algumas seções são configurações imperativas necessárias para o acesso básico VPN. Por exemplo, um túnel VPN pode ser setup com o cartão CAC sem verificações OCSP, mapeamentos LDAP verifica. O DoD encarrega de OCSP que verifica, mas dos trabalhos do túnel sem o OCSP configurado.
- A imagem básica ASA/PIX exigida é 7.2(2) e ASDM 5.2(1), mas este guia usa uma configuração temporária de 7.2.2.10 e de ASDM 5.2.2.54.
- Nenhuma mudança do esquema LDAP é necessária.
- Veja o apêndice A para o LDAP & os exemplos do mapeamento da política do acesso dinâmico para o reforço de política adicional.
- Veja o apêndice D em como verificar objetos LDAP no MS.
- Veja a informação relacionada