ASA 8.x: Configuração das CAC-carta inteligente de AnyConnect SSL VPN para Windows

Índice

Introdução

Este documento fornece uma configuração de exemplo no Cisco Adaptive Security Appliance (ASA) para o acesso remoto a AnyConnect VPN para Windows com a placa comum do acesso (CAC) para a autenticação.

O espaço deste documento é cobrir a configuração de Cisco ASA com o Directory Access Protocol adaptável do Security Device Manager (ASDM), do Cisco AnyConnect VPN Client e 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 OCSP, mapas do atributo LDAP e o acesso dinâmico policia (DAP).

Pré-requisitos

Requisitos

Uma compreensão básica do cliente de Cisco ASA, de Cisco AnyConnect, do Microsoft AD/LDAP e do Public Key Infrastructure (PKI) é benéfica na compreensão da instalação completa. A familiaridade com a membrasia do clube AD, as propriedades de usuário assim como os objetos LDAP ajudam na correlação do processo da autorização entre 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 (ASA) essa executa a versão de software 8.0(x) e mais atrasada
- Versão 6.x do Cisco Adaptive Security Device Manager (ASDM) para ASA 8.x
- Cisco AnyConnect VPN Client para Windows

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 através do ASDM. Cobre as etapas necessárias a fim distribuir um túnel de acesso remoto VPN através de uma conexão SSL AnyConnect. 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, acesso ASDM e assim por diante. Supõe-se que o operador de rede é familiar com estas configurações.Refira ferramentas de segurança Multifunction para mais informação.
- As seções destacadas no VERMELHO são configurações imperativas necessárias para o acesso básico VPN. Por exemplo, um túnel VPN pode ser setup com o cartão CAC sem fazer verificações OCSP, mapeamentos LDAP e verificações da política do acesso dinâmico (DAP). Os mandatos verificação OCSP do DoD mas o túnel trabalham sem OCSP configurado.
- As seções destacadas no AZUL são os recursos avançados que podem ser incluídos para adicionar mais Segurança ao projeto.
- O ASDM e AnyConnect/SSL VPN não podem usar as mesmas portas na mesma relação. Recomenda-se mudar as portas em uma ou as outro para aceder. Por exemplo, use a porta 445 para o ASDM e deixe 443 para AC/SSL VPN. O acesso ASDM URL mudou em 8.x. Use o `<ip_address> de https://: <port>/admin.html.`
- A imagem ASA exigida é pelo menos 8.0.2.19 e ASDM 6.0.2.
- AnyConnect/CAC é apoiado com vista.
- 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