

PIX/ASA 7.x: CAC - Autenticación de las tarjetas inteligentes para el Cliente Cisco VPN

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configuración de ASA de Cisco](#)

[Consideraciones sobre la instrumentación](#)

[Autenticación, autorización, configuración que considera \(AAA\)](#)

[Servidor LDAP de la configuración](#)

[Maneje el trustpoints](#)

[Genere las claves](#)

[Instale el trustpoints de CA](#)

[Instale los certificados raíz](#)

[Aliste el ASA y instale el certificado de identidad](#)

[Configuración VPN](#)

[Cree la directiva del grupo de túnel y del grupo](#)

[Interfaz y configuraciones de imagen del grupo de túnel](#)

[Parámetros de la configuración IKE/ISAKMP](#)

[Parámetros de IPsec de la configuración](#)

[Configuración OCSP](#)

[Certificado del respondedor de la configuración OCSP](#)

[Configuración CA para utilizar OCSP](#)

[Reglas de la configuración OCSP](#)

[Configuración de Cliente Cisco VPN](#)

[Comience al Cliente Cisco VPN](#)

[Nueva conexión](#)

[Comience el Acceso Remoto](#)

[Apéndice A sincronización LDAP del del del â](#)

[Escenario 1: La aplicación del Active Directory con el del del â del dial-in del Permiso de acceso remoto permite/niega el acceso](#)

[Configuración del Active Directory](#)

[Configuración ASA](#)

[Escenario 2: La aplicación del Active Directory con la membresía del grupo a permitir/niega el acceso](#)

[Configuración del Active Directory](#)

[Configuración ASA](#)

[Configuración CLI del ASA del del â del apéndice B](#)

[Troubleshooting del apéndice c](#)

[Resolver problemas el AAA y el LDAP](#)

[Ejemplo 1: Conexión permitida con la asignación correcta del atributo](#)

[Ejemplo 2: Conexión permitida con la asignación mal configurado del atributo de Cisco](#)

[Resolver problemas el Certificate Authority/OCSP](#)

[Resolver problemas el IPSEC](#)

[El del del â del apéndice D verifica los objetos LDAP en el MS](#)

[Visualizador LDAP](#)

[Editor de la interfaz de los servicios de Active Directory](#)

[Información Relacionada](#)

[Introducción](#)

Este documento proporciona una configuración de muestra en el dispositivo de seguridad adaptante de Cisco (ASA) para el Acceso Remoto de red con el indicador luminoso LED amarillo de la placa muestra gravedad menor común del acceso (CAC) para la autenticación.

El alcance de este documentos abarca la configuración de Cisco ASA con el Administrador de dispositivos de seguridad adaptante (ASDM), el Cliente Cisco VPN, y el Directory Access Protocol del Microsoft Active Directory (AD) /Lightweight (LDAP).

La configuración en esta guía utiliza el servidor de Microsoft AD/LDAP. Este documento también cubre las funciones avanzadas, tales como las correspondencias de atributo OCSP y LDAP.

[prerrequisitos](#)

[Requisitos](#)

Un conocimiento básico de Cisco ASA, Cliente Cisco VPN, Microsoft AD/LDAP, y Public Key Infrastructure (PKI) es beneficioso entender la configuración completa. La familiaridad con la membresía del grupo y las propiedades del usuario AD, así como las ayudas de los objetos LDAP para correlacionar el proceso de la autorización entre los atributos del certificado y el AD/LDAP se opone.

[Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- El dispositivo de seguridad adaptante de las Cisco 5500 Series (el ASA) ese funciona con la versión de software 7.2(2)
- Versión 5.2(1) del Cisco Adaptive Security Device Manager (ASDM)
- Cliente Cisco VPN 4.x

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

[Convenciones](#)

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

[Configuración de ASA de Cisco](#)

Esta sección cubre la configuración de Cisco ASA con el ASDM. Cubre los pasos necesarios para desplegar un túnel de acceso remoto VPN con conexión IPSec. El certificado CAC se utiliza para la autenticación, y el atributo del nombre principal del usuario (UPN) en el certificado se puebla en el Active Directory para la autorización.

[Consideraciones sobre la instrumentación](#)

- Esta guía no cubre las configuraciones básicas tales como interfaces, DNS, NTP, encaminamiento, acceso del dispositivo, o acceso del ASDM, etc. Se asume que el operador de la red es familiar con estas configuraciones. Para más información, refiera a los [dispositivos de seguridad multifuncionales](#).
- Algunas secciones son configuraciones obligatorias necesarias para el acceso básico VPN. Por ejemplo, un túnel VPN se puede poner con el indicador luminoso LED amarillo de la placa muestra gravedad menor CAC sin los controles OCSP, las sincronizaciones LDAP marca. El DoD asigna OCSP que marca, pero los trabajos del túnel por mandato sin el OCSP configurado.
- ASA/PIX la imagen básica requerida es 7.2(2) y el ASDM 5.2(1), pero esta guía utiliza una compilación interina de 7.2.2.10 y del ASDM 5.2.2.54.
- No hay cambio del esquema LDAP necesario.
- Vea el [Apéndice A](#) para el LDAP y los ejemplos de la asignación de la directiva del acceso dinámico para la aplicación de políticas adicional.
- Vea el [apéndice D](#) en cómo marcar los objetos LDAP en el MS.
- Vea la [información relacionada](#)