

ةي كذلا تا قاطبلا ةق داصم - PIX/ASA 7.x: CAC ل Cisco VPN ليم عمل

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [تكوين ASA من Cisco](#)
- [اعتبارات النشر](#)
- [تكوين المصادقة والتفويض والمحاسبة \(AAA\)](#)
- [تكوين خادم LDAP](#)
- [إدارة نقاط الثقة](#)
- [إنشاء المفاتيح](#)
- [تثبيت جهات توثيق CA](#)
- [تثبيت الشهادات الجذر](#)
- [تسجيل ASA وتثبيت شهادة الهوية](#)
- [تكوين VPN](#)
- [إنشاء مجموعة النفق ونهج المجموعة](#)
- [واجهة مجموعة النفق وإعدادات الصورة](#)
- [تكوين معلمات IKE/ISAKMP](#)
- [تكوين معلمات IPSec](#)
- [تكوين OCSP](#)
- [تكوين شهادة المستجيب OCSP](#)
- [تكوين CA لاستخدام OCSP](#)
- [تكوين قواعد OCSP](#)
- [تكوين عمل شبكة VPN من Cisco](#)
- [بدء تشغيل عمل شبكة VPN من Cisco](#)
- [اتصال جديد](#)
- [بدء الوصول عن بعد](#)
- [الملحق أ تخطيط LDAP](#)
- [السيناريو 1: تطبيق Active Directory مع طلب إذن الوصول عن بعد السماح/رفض الوصول](#)
- [إعداد Active Directory](#)
- [تكوين ASA](#)
- [السيناريو 2: تطبيق Active Directory مع عضوية المجموعة للسماح بالوصول/رفضه](#)
- [إعداد Active Directory](#)
- [تكوين ASA](#)
- [الملحق تكوين ASA CLI](#)
- [الملحق ج- أستكشاف الأخطاء وإصلاحها](#)

[أستكشاف أخطاء AAA و LDAP وإصلاحها](#)
[المثال 1: الاتصال المسموح به مع تعيين السمة الصحيحة](#)
[المثال 2: الاتصال المسموح به بتعيين سمة Cisco التي تم تكوينها بشكل غير صحيح](#)
[هيئة شهادة أستكشاف الأخطاء وإصلاحها / OCSP](#)
[أستكشاف أخطاء IPsec وإصلاحها](#)
[الملحق D التحقق من كائنات LDAP في MS](#)
[عارض LDAP](#)
[محرر واجهة خدمات Active Directory](#)
[معلومات ذات صلة](#)

[المقدمة](#)

يقدم هذا المستند نموذجاً لتكوين على جهاز الأمان القابل للتكيف (ASA) من Cisco للوصول عن بعد للشبكة باستخدام بطاقة الوصول المشترك (CAC) للمصادقة.

يغطي نطاق هذا المستند تكوين Cisco ASA باستخدام مدير أجهزة الأمان القابل للتكيف (ASDM) و عميل Cisco VPN وبروتوكول الوصول إلى الدليل خفيف الوزن (AD) Microsoft Active Directory (LDAP).

يستخدم التكوين الموجود في هذا الدليل خادم Microsoft AD/LDAP. يغطي هذا المستند أيضاً الميزات المتقدمة، مثل خرائط سمات OCSP و LDAP.

[المتطلبات الأساسية](#)

[المتطلبات](#)

من المفيد فهم الإعداد الكامل معرفة أساسية ب Cisco ASA، و عميل شبكة VPN من Cisco، و Microsoft AD/LDAP، والبنية الأساسية للمفتاح العام (PKI). تساعد المعرفة بعضوية مجموعة AD وخصائص المستخدم، بالإضافة إلى كائنات LDAP على ربط عملية التحويل بين سمات الترخيص وكائنات AD/LDAP.

[المكونات المستخدمة](#)

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- جهاز الأمان القابل للتكيف (ASA) من Cisco 5500 Series الذي يشغل إصدار البرنامج 7.2(2)
 - Cisco Adaptive Security Device Manager (ASDM)، الإصدار 5.2(1)
 - عميل شبكة VPN 4.x من Cisco
- تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

[الاصطلاحات](#)

راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

[تكوين ASA من Cisco](#)

يغطي هذا القسم تكوين Cisco ASA من خلال ASDM. وهو يغطي الخطوات الضرورية لنشر نفق وصول عن بعد

لشبكة VPN من خلال اتصال IPsec. يتم استخدام شهادة CAC للمصادقة، وسمة اسم المستخدم الأساسي (UPN) في الشهادة يتم ملؤها في خدمة Active Directory للتحويل.

اعتبارات النشر

- لا يغطي هذا الدليل التكوينات الأساسية مثل الواجهات أو DNS أو NTP أو التوجيه أو الوصول إلى الجهاز أو الوصول إلى ASDM، وما إلى ذلك. من المفترض أن مشغل الشبكة على دراية بهذه التكوينات. لمزيد من المعلومات، راجع [أجهزة الأمان متعددة الوظائف](#).
- بعض الأقسام هي تكوينات إلزامية مطلوبة للوصول الأساسي إلى شبكة VPN. على سبيل المثال، يمكن إعداد نفق VPN باستخدام بطاقة CAC بدون تحقق OCSP، تحقيقات تعيينات LDAP. تقوم DoD بتفويض فحص OCSP، ولكن يعمل النفق بدون تكوين OCSP.
- الصورة الأساسية ل ASA/PIX المطلوبة هي 7.2(2) و 5.2(1) ASDM، ولكن هذا الدليل يستخدم بنية مؤقتة من 7.2.2.10 و 5.2.2.54 ASDM.
- لا يلزم تغيير مخطط LDAP.
- راجع [الملحق \(أ\)](#) للحصول على أمثلة لرسم خرائط سياسة الوصول الديناميكي و LDAP لتنفيذ السياسات الإضافية.
- راجع [الملحق \(د\)](#) حول كيفية التحقق من كائنات LDAP في MS.
- الاطلاع على [المعلومات ذات الصلة](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ م ف ن م دخت س م ل م عد و ت م م م دقت ل ة م ش ب ل و
م ك ة ق م ق د ن و ك ت ن ل ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م م چ ر م . ة ص ا خ ل م ه ت غ ل ب
Cisco مچرت م ا م د ق م م ا ت ل ا ة م ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه
ل ا ا م ا د ا د ع و چ ر ل ا ب م ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت م ل و ئ س م
Systems (ر ف و ت م ط ب ا ر ل ا) م ل ص ا ل ا م ل م چ ر ت ل ا د ن ت س م ل ا