PIX/ASA 7.x: CAC - مصادقة الشهادات الرقمية لعميل Cisco VPN

المحتويات

المقدمة

يقدم هذا المستند نموذجا 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) وعميل Cisco VPN وبروتوكول الوصول إلى الدليل خفيف الوزن (LDAP) Microsoft Active Directory (AD).

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

المتطلبات الأساسية

المتطلبات

من المفيد فهم الإعداد الكامل معرفة أساسية ب Cisco ASA، وعميل 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 التخويل 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 إستخدام شهادة CAC للمصادقة، وسمة اسم المستخدم الأساسي (UPN) في الشهادة يتم ملؤها في خدمة Active Directory للتخويل.

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 تحققات OCSP، تحققات 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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).