PIX/ASA 7.x: CAC - Autenticazione SmartCard per client VPN Cisco

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio su Cisco Adaptive Security Appliance (ASA) per l'accesso remoto di rete con la scheda CAC (Common Access Card) per l'autenticazione.

L'ambito di questo documento copre la configurazione di Cisco ASA con Adaptive Security Device Manager (ASDM), Cisco VPN Client e Microsoft Active Directory (AD)/Lightweight Directory Access Protocol (LDAP).

La configurazione di questa guida utilizza il server AD/LDAP Microsoft. Nel documento vengono inoltre descritte funzionalità avanzate, ad esempio le mappe di attributi OCSP e LDAP.

Prerequisiti

Requisiti

Una conoscenza base di Cisco ASA, Cisco VPN Client, Microsoft AD/LDAP e Public Key Infrastructure (PKI) è utile per comprendere l'installazione completa. La familiarità con l'appartenenza ai gruppi AD e le proprietà utente, nonché con gli oggetti LDAP, consente di correlare il processo di autorizzazione tra gli attributi del certificato e gli oggetti AD/LDAP.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 5500 Adaptive Security Appliance (ASA) con software versione 7.2(2)
- Cisco Adaptive Security Device Manager (ASDM) versione 5.2(1)
- Cisco VPN Client 4.x

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione di Cisco ASA

In questa sezione viene descritta la configurazione di Cisco ASA tramite ASDM. Illustra la procedura necessaria per distribuire un tunnel di accesso remoto VPN tramite una connessione IPsec. Il certificato CAC viene utilizzato per l'autenticazione e l'attributo UPN (User Principal Name) nel certificato viene inserito in Active Directory per l'autorizzazione.

Considerazioni sulla distribuzione

- Questa guida NON riguarda le configurazioni di base come interfacce, DNS, NTP, routing, accesso ai dispositivi o accesso ASDM, ecc. Si presume che l'operatore di rete abbia familiarità con queste configurazioni.Per ulteriori informazioni, consultare il documento sulle appliance di sicurezza multifunzione.
- Alcune sezioni sono configurazioni obbligatorie necessarie per l'accesso VPN di base. Ad esempio, è possibile configurare un tunnel VPN con scheda CAC senza controlli OCSP e controlli di mapping LDAP. DoD impone il controllo OCSP, ma il tunnel funziona senza OCSP configurato.
- L'immagine ASA/PIX di base richiesta è 7.2(2) e ASDM 5.2(1), ma questa guida usa una build provvisoria di 7.2.2.10 e ASDM 5.2.2.54.
- Non è necessario modificare lo schema LDAP.
- Vedere Appendice A per esempi di mappatura dei criteri di accesso dinamico e LDAP per ulteriori informazioni sull'applicazione dei criteri.
- Vedere Appendice D su come controllare gli oggetti LDAP in MS.
- Vedere le informazioni correlate