

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

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione di Cisco ASA](#)

[Considerazioni sulla distribuzione](#)

[Configurazione di autenticazione, autorizzazione e accounting \(AAA\)](#)

[Configura server LDAP](#)

[Gestisci trust point](#)

[Genera chiavi](#)

[Installa trust tra CA](#)

[Installa certificati radice](#)

[Registra ASA e installa certificato di identità](#)

[Configurazione VPN](#)

[Crea gruppo tunnel e Criteri di gruppo](#)

[Impostazioni interfaccia e immagine tunnel Group](#)

[Configurazione parametri IKE/ISAKMP](#)

[Configurazione dei parametri IPsec](#)

[Configura OCSP](#)

[Configura certificato risponditore OCSP](#)

[Configura CA per l'utilizzo di OCSP](#)

[Configura regole OCSP](#)

[Configurazione client VPN Cisco](#)

[Avvia Cisco VPN Client](#)

[Nuova connessione](#)

[Avvia Accesso remoto](#)

[Appendice A â Mappatura LDAP](#)

[Scenario 1: Applicazione di Active Directory con Autorizzazione di accesso remoto Chiamata in ingresso â Consenti/Nega accesso](#)

[Installazione di Active Directory](#)

[Configurazione ASA](#)

[Scenario 2: Applicazione di Active Directory con appartenenza a gruppi per consentire/negare l'accesso](#)

[Installazione di Active Directory](#)

[Configurazione ASA](#)

[Appendice B â Configurazione ASA CLI](#)

[Appendice C - Risoluzione dei problemi](#)

[Risoluzione dei problemi relativi a AAA e LDAP](#)

[Esempio 1: Connessione consentita con mapping attributi corretto](#)

[Esempio 2: Connessione consentita con mapping di attributi Cisco non configurati correttamente](#)

[Risoluzione dei problemi di Autorità di certificazione/OCSP](#)

[Risoluzione dei problemi di IPSEC](#)

[Appendice D â Verifica degli oggetti LDAP in MS](#)

[Visualizzatore LDAP](#)

[Editor interfaccia servizi Active Directory](#)

[Informazioni correlate](#)

[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](#)