Utilizzo certificato WSA per decrittografia HTTPS

Sommario

Introduzione

In questo documento viene descritto il tipo di certificato da utilizzare per la decrittografia HTTPS in un Cisco Web Security Appliance (WSA).

Panoramica certificato

WSA può utilizzare un certificato e una chiave privata correnti per la decrittografia HTTPS. Tuttavia, potrebbe esserci confusione sul tipo di certificato da utilizzare, poiché non tutti i certificati x.509 funzionano.

Esistono due tipi principali di certificati: **Certificati server** e **certificati radice**. Tutti i certificati x.509 contengono un campo Vincoli di base che identifica il tipo di certificato:

- **Subject Type=Entità finale** - Certificato server
- **Subject Type=CA** - Certificato radice

> **Nota:** Per la decrittografia HTTPS in WSA, è necessario utilizzare un certificato radice, denominato anche certificato di firma dell'Autorità di certificazione (CA).

Certificati radice

Per firmare i certificati server viene creato un certificato radice. È possibile creare e utilizzare la propria CA e firmare i propri certificati server.

> **Nota:** Poiché un certificato radice firma solo altri certificati, non può essere utilizzato su un server Web per eseguire la crittografia e la decrittografia HTTPS.

Per generare attivamente certificati server per la decrittografia HTTPS, WSA deve utilizzare un certificato radice. Per l'utilizzo del certificato radice sono disponibili due opzioni:

- Generare un certificato radice sul server WSA. WSA crea il proprio certificato radice e la propria chiave privata e utilizza questa coppia di chiavi per firmare i certificati del server.
- Èpossibile caricare un certificato radice corrente e la relativa chiave privata nel WSA. Il campo Nome comune (CN) in un certificato radice identifica l'entità, in genere un nome di società, che considera attendibili tutti i certificati server contenenti la relativa firma.

  Nota: Prima di poter considerare attendibile un certificato server, è necessario firmarlo con un certificato radice che disponga di una chiave pubblica presente nel browser Web.

Certificati server

Un certificato server viene creato specificamente per essere utilizzato nella crittografia e decrittografia HTTPS e per verificare l'autenticità di un server specifico. I certificati server sono firmati da una CA che utilizza il certificato radice CA. Un esempio comune di CA è VeriSign o Thawte.

> **Nota:** Impossibile utilizzare un certificato server per firmare altri certificati. pertanto, la decrittografia HTTPS non funziona se un certificato server è installato nel server di distribuzione Windows.

Il campo CN in un certificato server specifica l'host per il quale si desidera utilizzare il certificato. Ad esempio, **https://www.verisign.com** utilizza un certificato Server con un CN di **www.verisign.com**.

Informazioni correlate

- Utilizzo certificato Web Security Appliance (WSA) (decrittografia HTTPS, accesso GUI, crittografia credenziali)
- Passaggi per abilitare il proxy HTTPS sull'opzione WSA e richiesta di firma del certificato (CSR)
- Procedura per abilitare il proxy HTTPS su (WSA) e caricare l'opzione di certificato radice/intermedio
- Documentazione e supporto tecnico – Cisco Systems