WSA-certificaatgebruik voor HTTPS-decryptie

Inhoud

Inleiding

Dit document beschrijft het type certificaat dat moet worden gebruikt voor HTTPS-decryptie op een Cisco Web Security Appliance (WSA).

Overzicht van certificaten

De WSA heeft de mogelijkheid om een huidige certificaat en privé sleutel te gebruiken voor gebruik met HTTPS-decryptie. Er kan echter verwarring ontstaan over het soort certificaat dat moet worden gebruikt, aangezien niet alle x.509-certificaten werken.

Er zijn twee belangrijke typen certificaten: **Server certificaten** en **wortelcertificaten**. Alle x.509-certificaten bevatten een veld Basisbeperkingen, dat het type certificaat identificeert:

- **Onderwerp Type=eindentiteit** - servercertificaat
- **Onderwerp Type=CA** - Root-certificaat

> Opmerking: U moet een basiscertificaat gebruiken, ook bekend als een certificaat van certificeringsinstantie (CA), voor HTTPS-decryptie op de WSA.

Root-certificaten

Er wordt een Root-certificaat aangemaakt voor het ondertekenen van servercertificaten. U kunt uw eigen CA maken en gebruiken en uw eigen servercertificaten ondertekenen.

> Opmerking: Aangezien een wortelcertificaat alleen andere certificaten ondertekent, kan het niet op een webserver worden gebruikt om HTTPS-encryptie en decryptie uit te voeren.

De WSA moet een certificaat Root gebruiken om actief servercertificaten voor HTTPS-decryptie te genereren. Er zijn twee opties beschikbaar voor gebruik van een wortelcertificaat:

- genereren een basiscertificaat op de WSA. WSA creëert zijn eigen Root certificaat en privé sleutel, en het gebruikt dit sleutelpaar om servercertificaten te ondertekenen.

- U kunt een huidige Root-certificaat en de bijbehorende privésleutel naar het WSA uploaden. Het veld Common Name (CN) in een wortelcertificaat identificeert de entiteit (gewoonlijk een bedrijfsnaam) die alle servercertificaten met zijn handtekening beheert.

  Opmerking: Voordat een servercertificaat kan worden vertrouwd, moet het worden ondertekend door een Root-certificaat met een openbare sleutel in de webbrowser.

Server-certificaten

Er wordt een servercertificaat gecreëerd om te worden gebruikt in HTTPS-encryptie en decryptie en om de authenticiteit van een specifieke server te controleren. De servercertificaten worden ondertekend door een CA met gebruik van het CA Root-certificaat. Een veel voorkomend voorbeeld van een CA is VeriSign of Thawte.

Opmerking: Een servercertificaat kan niet worden gebruikt om andere certificaten te ondertekenen; HTTPS-decryptie werkt niet als er een servercertificaat op de WSA is geïnstalleerd.

In het GN-veld in een servercertificaat wordt de gastheer vermeld waarvoor het certificaat bestemd is. **https://www.verisign.com** bijvoorbeeld gebruikt een servercertificaat met een GN van **www.verisign.com**.

Gerelateerde informatie

- Web security applicatie (WSA) certificaatgebruik (HTTPS-decryptie, GUI-inloggen, Credentiële encryptie)
- Stappen om HTTPS-proxy op WSA- en certificaataanvraag (CSR) in te schakelen
- Stappen om HTTPS proxy op (WSA) en Upload Root/Intermediate certificaatoptie in te schakelen
- Technische ondersteuning en documentatie – Cisco Systems