Cisco RES: Hoe TLS te gebruiken om niet-gecodeerde RES-antwoorden te beveiligen

Inhoud

Inleiding

Dit document beschrijft hoe u Transport Layer Security (TLS) kunt gebruiken om antwoorden te beveiligen van de Cisco Registered Service (CRES), die een gebruiker toestaat om ze niet te hoeven decrypteren, in samenhang met de Cisco Email Security Appliance (ESA).

Cisco RES: Hoe TLS te gebruiken om niet-gecodeerde RES-antwoorden te beveiligen

Standaard worden antwoorden op een beveiligde e-mail versleuteld met Cisco RES en verzonden naar uw e-mailgateway. Ze geven dan door naar uw mailservers die versleuteld zijn zodat de eindgebruiker de toegang kan openen met hun Cisco RES-aanmeldingsgegevens.

Om de noodzaak voor de gebruiker te vermijden om zich met Cisco RES te authentiseren om het veilige antwoord te openen, levert Cisco RES in een "niet-versleuteld" formulier om gateways te verzenden die TLS ondersteunen. In de meeste gevallen is de mailgateway het ESA, en dit artikel is van toepassing.

Als er echter een andere e-mailpoort voor de ESA ligt, zoals een extern spamfilter, is de configuratie van de stroom certificaat/TLS/mail op uw ESA niet nodig. In dit geval kunt u stap 1 tot en met 3 overslaan in het gedeelte Oplossing van dit document. Voor niet-versleutelde antwoorden op het werk in deze omgeving is het externe spamfilter (mailgateway) het apparaat dat TLS moet ondersteunen. Als zij TLS ondersteunen, kunt u Cisco RES dit bevestigen en u voor "niet-versleutelde" antwoorden laten instellen om e-mails te beveiligen.

Kader voor Steekproefbeleid

Om de fouten van het Sender Policy Framework (SPF) te voorkomen, moet u mx:res.cisco.com, mxnat1.res.cisco.com en mxat3.res.cisco.com aan uw SPF-record toevoegen. Of je kunt **spfc._spf.cisco.com** 'opnemen' in je SPF-record.

Voorbeeld:

```
 ~ dig txt spfc._spf.cisco.com +short
"v=spf1 mx:res.cisco.com mx:sco.cisco.com ~all"
```

Waar en hoe u Cisco RES aan uw SPF-record toevoegt, is afhankelijk van de manier waarop uw Domain Name System (DNS) met uw netwerktopologie is geïmplementeerd. Zorg ervoor dat u contact opneemt met de DNS-beheerder voor meer informatie.

Als DNS niet is ingesteld om Cisco RES op te nemen, wanneer beveiligde compositie en beveiligde antwoorden worden gegenereerd en geleverd via de Hosted Key servers, komt het uitgaande IP-adres niet overeen met de vermelde IP-adressen aan het einde van de ontvanger, wat resulteert in een verificatiestoornis van het SFP.

Hostnamen en IP-adressen

schuilnaam	IP-adres	Type opname
res.cisco.com	184.94.241.74	A
mxnat1.res.cisco.com	208.90.57.32	A
mxnat2.res.cisco.com	208.90.57.33	A
mxnat3.res.cisco.com	184.94.241.96	A
mxnat4.res.cisco.com	184.94.241.97	A
mxnat5.res.cisco.com	184.94.241.98	A
mxnat6.res.cisco.com	184.94.241.99	A
mxnat7.res.cisco.com	208.90.57.34	A
mxnat8.res.cisco.com	208.90.57.35	A
esa1.cres.iphmx.com	68.232.140.79	MX
esa2.cres.iphmx.com	68.232.140.57	MX
esa3.cres.iphmx.com	68.232.135.234	MX
esa4.cres.iphmx.com	68.232.135.235	MX

> **Opmerking**: Hostname- en IP-adressen zijn aan wijziging onderhevig op basis van service-/netwerkonderhoud of groei van service-/netwerknetwerken. Niet alle hostnamen en IP-adressen worden voor de service gebruikt. Zij worden hier ter referentie verstrekt.

Oplossing

1. Ontvang en plaats een ondertekend certificaat en een tussentijds certificaat op de ESA. **Opmerking**: het is belangrijk dat u het tussentijdse certificaat van uw ondertekenende instantie inschaft, aangezien het demo-certificaat dat op het apparaat is afgegeven, ervoor zorgt dat het CRES-verificatieproces niet verloopt.
2. Een nieuw poststroombeleid maken: Kies in de GUI **het beleid voor e-mail > beleid voor e-mail stromen > Beleid toevoegen...**.Voer een naam in en laat alle andere waarden standaard behouden, behalve *voor beveiligingsfuncties: KNELS.* Stel dit item in op **verplicht**.
3. Een nieuwe sendergroep maken: Kies in de GUI **het postbeleid > HAT - Overzicht > Toevoegen verzendgroep...**.Typ een naam en stel het bestelnummer in op #1. U kunt ook een optionele opmerking opgeven. Kies het poststroombeleid dat u in stap 2 hebt gemaakt. Laat alles leeg.Klik op **Indienen en voeg Senders toe >>**.
4. Voer in het veld Sender deze IP-marges en hostnamen in:
```
.res.cisco.com
.cres.iphmx.com
208.90.57.0/26 (current CRES IP network range)
204.15.81.0/26 (old CRES IP network range)
```
5. Breng de wijzigingen aan en begaan ze.
6. Nadat u ervan overtuigd bent dat de ESA voor TLS is voorbereid van de Cisco RES-servers, volgt u de stappen in How do I test als mijn domein TLS ondersteunt met Cisco RES? om de Cisco RES-servers te vragen TLS te gaan gebruiken.

Gerelateerde informatie

- Cisco RES: IP-adressen en hostnamen voor belangrijke servers
- Cisco e-mail security applicatie - eindgebruikershandleidingen
- Technische ondersteuning en documentatie – Cisco Systems