Certificaten opstellen Handleiding voor TLS op ESA

Inhoud

Inleiding

Dit document beschrijft hoe u een certificaat maakt voor gebruik met TLS, inkomende/uitgaande TLS activeert en problemen met de Cisco ESA oplost.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De TLS-implementatie op de ESA biedt privacy voor point-to-point transmissie van e-mails via encryptie. Het staat een beheerder toe om een certificaat en privé sleutel van de dienst van de Certificaatautoriteit (CA) in te voeren, of een zelf-ondertekend certificaat te gebruiken.

Cisco AsyncOS voor Email Security ondersteunt de extensie *STARTTLS* naar Simple Mail Transfer Protocol (SMTP) (*Secure SMTP over TLS*).

> **Tip**: raadpleeg RFC 3207 voor meer informatie over TLS.

> **Opmerking**: In dit document wordt beschreven hoe certificaten op clusterniveau kunnen worden geïnstalleerd met behulp van de functie *Gecentraliseerd beheer* op de ESA. Certificaten kunnen ook op machineniveau worden toegepast; als de machine echter ooit uit het cluster wordt verwijderd en vervolgens weer wordt toegevoegd, gaan de machineniveau certificaten verloren.

Functioneel overzicht en vereisten

Een beheerder wil om een van de volgende redenen een zelf-ondertekend certificaat op het apparaat aanmaken:

- Om de SMTP-gesprekken te versleutelen met andere MTA's die TLS gebruiken (zowel inkomende als uitgaande gesprekken).
- Om de HTTPS-service op het apparaat toegang tot de GUI via HTTPS mogelijk te maken.
- Voor gebruik als clientcertificaat voor Lichtgewicht Directory Access Protocols (LDAP's), als de LDAP-server een clientcertificaat vereist.
- Om veilige communicatie tussen het apparaat en de Rivest-Shamir-Addleman (RSA) Enterprise Manager for Data Loss Protection (DLP) mogelijk te maken.
- Om veilige communicatie tussen het apparaat en een Cisco Advanced Malware Protection

(AMP) Threat Grid-applicatie mogelijk te maken.

De ESA wordt geleverd met een demonstratiecertificaat dat kan worden gebruikt om TLS-verbindingen tot stand te brengen.

> **Waarschuwing**: hoewel het demonstratiecertificaat voldoende is voor het opzetten van een beveiligde TLS-verbinding, moet u zich ervan bewust zijn dat er geen verifieerbare verbinding kan worden aangeboden.

Cisco raadt u aan een X.509-certificaat of een PEM-certificaat (Privacy Enhanced Email) te verkrijgen van een CA. Dit wordt ook wel een *Apache*-certificaat genoemd. Het certificaat van een CA is gewenst boven het zelfondertekende certificaat omdat een zelfondertekend certificaat vergelijkbaar is met het eerder genoemde demonstratiecertificaat, dat geen verifieerbare verbinding kan bieden.

> **Opmerking**: Het PEM-certificaatformaat is nader gedefinieerd in RFC 1421 tot en met RFC 1424. De PEM is een containerformaat dat alleen het publieke certificaat kan bevatten (zoals bij Apache-installaties en CA-certificaatbestanden */etc/ssl/certs*) of een volledige certificaatketen, inclusief publieke sleutel-, privé-sleutel- en basiscertificaten. De naam *PEM* is afkomstig van een mislukte methode voor beveiligde e-mail, maar het containerformaat dat wordt gebruikt is nog steeds actief en is een base-64 vertaling van de X.509 ASN.1 toetsen.

Breng uw eigen certificaat mee

De mogelijkheid om uw eigen certificaat in te voeren is beschikbaar op de ESA; het certificaat moet echter in *PKCS#12*-formaat zijn opgesteld. Dit formaat bevat de privé-sleutel. Beheerders hebben vaak geen certificaten die in deze indeling beschikbaar zijn. Om deze reden raadt Cisco u aan het certificaat op de ESA te genereren en het correct door een CA te laten ondertekenen.

Een huidig certificaat bijwerken

Als een certificaat dat al bestaat is verlopen, slaat u het gedeelte *Implementatie-zelfondertekende certificaten* van dit document over en tekent u het bestaande certificaat opnieuw.

> **Tip**: Raadpleeg het certificaat verlengen op een e-mail security applicatie en het Cisco-document voor meer informatie.

Zelfondertekende certificaten implementeren

In dit deel wordt beschreven hoe een zelfondertekend certificaat en verzoek om ondertekening van het certificaat (CSR) moet worden gegenereerd, hoe het zelfondertekende certificaat aan een CA moet worden verstrekt voor ondertekening, hoe het ondertekende certificaat aan de ESA moet worden geüpload, hoe het certificaat moet worden gespecificeerd voor gebruik met de ESA-diensten, en hoe een back-up moet worden gemaakt van de configuratie en het certificaat van het apparaat.

Een zelfondertekend certificaat en MVO genereren

Om een zelf-ondertekend certificaat via CLI te creëren, ga het bevel **certconfig** in.

U maakt als volgt een zelfondertekend certificaat vanuit de GUI:

1. Navigeren naar **netwerk > Certificaten > Certificaat toevoegen** vanuit de GUI van het apparaat.

2. Klik op het vervolgkeuzemenu **Zelfondertekend certificaat maken**.

   Wanneer u het certificaat aanmaakt, zorg er dan voor dat de *algemene naam* overeenkomt met de hostnaam van de luisterinterface of dat het overeenkomt met de hostnaam van de leveringsinterface.
   De *luisterinterface* is de interface die is gekoppeld aan de luisteraar die is geconfigureerd onder **Netwerk > Luisteraars**.De *bezorgingsinterface* wordt automatisch geselecteerd, tenzij deze expliciet vanuit de CLI is geconfigureerd met de opdracht **deliveryConfig**.
3. Voor een verifieerbare inkomende verbinding, bevestig dat deze drie punten aanpassen:

   MX record (Domain Name System (DNS) hostnaam)

   Gebruikelijke naam

   Interface-hostnaam

   Opmerking: het systeem hostname heeft geen invloed op de TLS-verbindingen wat betreft verifieerbaarheid. Het systeem hostname wordt weergegeven in de rechterbovenhoek van de GUI van het apparaat of vanuit de opdrachtoutput van de CLI-**sethostname**.

   Waarschuwing: vergeet niet uw wijzigingen te **verzenden** en **toe** te **leggen** voordat u de MVO exporteert. Als deze stappen niet zijn voltooid, is het nieuwe certificaat niet gecommitteerd aan de configuratie van het apparaat en kan het ondertekende certificaat van de CA geen ondertekenen of worden toegepast op een certificaat dat al bestaat.

Verstrek het zelfondertekende certificaat aan een CA

Het zelfondertekende certificaat indienen bij een CA voor ondertekening:

1. Sla de CSR op op een lokale computer in PEM-formaat **Netwerk > Certificaten > Naam certificaat > Verzoek om certificaatondertekening te downloaden**.

2. Verzend het gegenereerde certificaat naar een herkende CA voor ondertekening.

3. Vraag een X.509/PEM/Apache geformatteerd certificaat aan, evenals het tussentijds certificaat.

CA genereert vervolgens een certificaat in PEM-formaat.

Opmerking: Voor een lijst van CA-providers raadpleegt u het Wikipedia-artikel Certificaatautoriteit.

Upload het ondertekende certificaat naar de ESE

Nadat de CA het vertrouwde openbare certificaat heeft teruggestuurd dat is ondertekend door een privésleutel, kunt u het ondertekende certificaat uploaden naar de ESA.

Het certificaat kan dan worden gebruikt met een openbare of privé-luisteraar, een IP-interface HTTPS-service, de LDAP-interface of alle uitgaande TLS-verbindingen naar de doeldomeinen.

Het ondertekende certificaat uploaden naar de ESA:

1. Zorg ervoor dat het vertrouwde openbare certificaat dat wordt ontvangen, gebruikmaakt van het PEM-formaat of een formaat dat naar PEM kan worden geconverteerd voordat u het naar het apparaat uploadt. **Tip**: U kunt de OpenSSL toolkit gebruiken, een gratis softwareprogramma, om het formaat te converteren.
2. Upload het ondertekende certificaat:

   Navigeer naar **Netwerk > Certificaten**.

   Klik op de naam van het certificaat dat naar de CA is verzonden voor ondertekening.

   Voer het pad naar het bestand op het lokale apparaat of netwerkvolume in.

   Opmerking: wanneer u het nieuwe certificaat uploadt, wordt het huidige certificaat overschreven. Een tussentijds certificaat dat verband houdt met het zelfondertekende certificaat kan ook worden geüpload.

   Waarschuwing: vergeet niet om de wijzigingen te **verzenden** en **toe** te **leggen** nadat u het ondertekende certificaat hebt geüpload.

Certificaat voor gebruik met ESA Services specificeren

Nu het certificaat wordt gecreëerd, ondertekend en geüpload naar de ESA, kan het worden gebruikt voor de diensten die gebruik van het certificaat vereisen.

Inkomende TLS

Voltooi deze stappen om het certificaat voor de inkomende TLS-diensten te gebruiken:

1. Navigeer naar **Netwerk > Luisteraars**.
2. Klik op de naam van de luisteraar.
3. Selecteer de certificaatnaam in het vervolgkeuzemenu *Certificaat*.
4. Klik op **Verzenden**.
5. Herhaal stappen 1 tot en met 4 zoals nodig voor extra luisteraars.

6. **Breng** de wijzigingen aan.

Uitgaande TLS

Voltooi deze stappen om het certificaat voor de uitgaande TLS-diensten te gebruiken:

1. Navigeer naar **mailbeleid > Bestemmingscontroles**.
2. Klik op **Globale instellingen bewerken...** in het gedeelte *Globale instellingen*.
3. Selecteer de certificaatnaam in het vervolgkeuzemenu *Certificaat*.
4. Klik op **Verzenden**.
5. **Breng** de wijzigingen aan.

HTTPS

Voltooi deze stappen om het certificaat voor de HTTPS-diensten te gebruiken:

1. Navigeer naar **Netwerk > IP-interfaces**.
2. Klik op de interfacenaam.
3. Selecteer de certificaatnaam in het vervolgkeuzemenu *HTTPS*-certificaat.
4. Klik op **Verzenden**.
5. Herhaal stappen 1 tot en met 4 zoals nodig voor extra interfaces.
6. **Breng** de wijzigingen aan.

LDAP's

Voltooi deze stappen om het certificaat voor de LDAP's te gebruiken:

1. Ga naar **Systeembeheer > LDAP**.
2. Klik op **Instellingen bewerken...** in het gedeelte *Globale instellingen LDAP*.
3. Selecteer de certificaatnaam in het vervolgkeuzemenu *Certificaat*.
4. Klik op **Verzenden**.
5. **Breng** de wijzigingen aan.

URL-filtering

U kunt het certificaat als volgt gebruiken voor URL-filtering:

1. Voer de opdracht **websecurity**config in de CLI in.

2. Ga door de opdrachtaanwijzingen. Zorg ervoor dat u **Y** selecteert wanneer u op deze prompt komt:

```
Do you want to set client certificate for Cisco Web Security Services Authentication?
```

3. Selecteer het nummer dat aan het certificaat is gekoppeld.

4. Voer de opdracht **commit** in om de configuratiewijzigingen vast te leggen.

Back-ups maken van de configuratie en certificaten van het apparaat

Zorg ervoor dat de configuratie van het apparaat op dit moment wordt opgeslagen. De configuratie van het apparaat bevat het voltooide certificeringswerk dat via de eerder beschreven processen is toegepast.

Voltooi de volgende stappen om het configuratiebestand van het apparaat op te slaan:

1. Ga naar **Systeembeheer > Configuratiebestand > Downloadbestand naar lokale computer om het bestand te bekijken of op te slaan**.

2. Het certificaat uitvoeren:

   Navigeer naar **Netwerk > Certificaten**.

   Klik op **Certificaat exporteren**.

   Selecteer het certificaat dat u wilt exporteren.

   Voer de bestandsnaam van het certificaat in.

   Voer een wachtwoord in voor het certificaatbestand.

   Klik op **Exporteren**.

   Sla het bestand op een lokale computer of netwerkcomputer op.

   Op dit moment kunnen extra certificaten worden geëxporteerd of klik op **Annuleren** om terug te keren naar de locatie **Network > Certificates**.

   Opmerking: tijdens dit proces wordt het certificaat opgeslagen in de PKCS#12-indeling. Hierdoor wordt het bestand gemaakt en opgeslagen met wachtwoordbeveiliging.

Inkomende TLS activeren

Als u TLS voor alle inkomende sessies wilt activeren, maakt u verbinding met de web GUI, kiest u **Mail Policies > Mail Flow Policies** voor de geconfigureerde inkomende luisteraar en voltooit u vervolgens de volgende stappen:

1. Kies een luisteraar waarvoor het beleid moet worden aangepast.

2. Klik op de link voor de naam van het beleid om het te bewerken.

3. In de sectie *Beveiligingsfuncties* kiest u een van deze opties voor *Encryptie en verificatie* om het niveau van TLS in te stellen dat vereist is voor dat luisteraar- en e-mailstroombeleid:

   Uit - Als u deze optie selecteert, wordt TLS niet gebruikt.

   Voorkeursoptie - Wanneer deze optie wordt gekozen, kan TLS onderhandelen van de MTA op afstand naar de ESA. Als de MTA op afstand echter niet onderhandelt (voorafgaand aan de ontvangst van een *220*-reactie), gaat de SMTP-transactie door *in de duidelijke* (niet-versleutelde) versie. Er wordt geen poging ondernomen om na te gaan of het certificaat afkomstig is van een vertrouwde certificeringsautoriteit. Als er een fout optreedt nadat de 220-reactie is ontvangen, dan valt de SMTP-transactie niet terug naar duidelijke tekst.

   Vereist - Wanneer voor deze optie wordt gekozen, kan over TLS worden onderhandeld vanaf de MTA op afstand tot de ESA. Er wordt geen poging gedaan om het certificaat van het domein te verifiëren. Als de onderhandeling mislukt, wordt er geen e-mail verzonden via de verbinding. Als de onderhandeling slaagt, dan wordt de post geleverd via een versleutelde sessie.
4. Klik op **Verzenden**.

5. Klik op de knop **Wijzigingen vastleggen**. Je kunt op dit moment desgewenst een optioneel commentaar toevoegen.

6. Klik op **Wijzigingen vastleggen** om de wijzigingen op te slaan.

Het e-mailstroombeleid voor de luisteraar wordt nu bijgewerkt met de TLS-instellingen die u hebt gekozen.

Voltooi deze stappen om TLS voor binnenkomende sessies te activeren die uit een geselecteerde reeks domeinen komen:

1. Maak verbinding met de web GUI en kies **Mail Policies > HAT Overzicht**.

2. Voeg de afzender(s) IP/FQDN toe aan de juiste afzendergroep.

3. Bewerk de TLS-instellingen van het e-mailstroombeleid dat is gekoppeld aan de afzendergroep die u in de vorige stap hebt gewijzigd.

4. Klik op **Verzenden**.

5. Klik op de knop **Wijzigingen vastleggen**. Je kunt op dit moment desgewenst een optioneel commentaar toevoegen.

6. Klik op **Wijzigingen vastleggen** om de wijzigingen op te slaan.

Het e-mailstroombeleid voor de afzendergroep wordt nu bijgewerkt met de TLS-instellingen die u hebt gekozen.

> **Tip**: Raadpleeg dit artikel voor meer informatie over de manier waarop de ESE met TLS-verificatie omgaat: Wat is het algoritme voor certificatie-verificatie op de ESA?

Uitgaande TLS activeren

Als u TLS voor uitgaande sessies wilt activeren, maakt u verbinding met de web GUI, kiest u **Mail Policies > Bestemmingscontroles** en voltooit u vervolgens de volgende stappen:

1. Klik op **Bestemming toevoegen...**.

2. Voeg het doeldomein toe.

3. In de sectie *TLS-ondersteuning* klikt u op het vervolgkeuzemenu en kiest u een van deze opties om het type TLS in te schakelen dat moet worden geconfigureerd:

   Geen - Wanneer deze optie wordt gekozen, wordt TLS niet besproken voor uitgaande verbindingen van de interface naar MTA voor het domein.

   Voorkeursoptie - Wanneer voor deze optie wordt gekozen, wordt TLS overeengekomen van de ESA-interface naar de MTA(s) voor het domein. Als de TLS-onderhandeling echter mislukt (voorafgaand aan de ontvangst van een 220-reactie), gaat de SMTP-transactie *in de duidelijke* (niet-versleutelde) versie verder. Er wordt geen poging ondernomen om te verifiëren of het certificaat afkomstig is van een vertrouwde certificeringsinstantie. Als er een fout optreedt nadat de 220-reactie is ontvangen, dan valt de SMTP-transactie niet terug naar duidelijke tekst.

   Vereist - Wanneer voor deze optie is gekozen, wordt TLS via de ESA-interface tot MTA(s) voor het domein overeengekomen. Er wordt geen poging gedaan om het certificaat van het domein te verifiëren. Als de onderhandeling mislukt, wordt er geen e-mail verzonden via de verbinding. Als de onderhandeling slaagt, dan wordt de post geleverd via een versleutelde sessie.

   Preferred-verify - wanneer deze optie is gekozen, wordt TLS overeengekomen van de ESA naar de MTA(s) voor het domein en het apparaat probeert het domeincertificaat te controleren. In dit geval zijn deze drie resultaten mogelijk:

   Over het TLS wordt onderhandeld en het certificaat wordt geverifieerd. De mail wordt geleverd via een versleutelde sessie.

   Over het TLS wordt onderhandeld, maar het certificaat wordt niet geverifieerd. De mail wordt geleverd via een versleutelde sessie.

Er wordt geen TLS-verbinding gemaakt en het certificaat wordt niet geverifieerd. Het e-mailbericht wordt in onbewerkte tekst verzonden.**Vereist-verify** - wanneer deze optie is gekozen, wordt TLS door de ESA aan de MTA(s) voor het domein overeengekomen en is verificatie van het domeincertificaat vereist. In dit geval zijn deze drie resultaten mogelijk:

Er wordt onderhandeld over een TLS-verbinding en het certificaat wordt geverifieerd. Het e-mailbericht wordt geleverd via een versleutelde sessie.

Er wordt onderhandeld over een TLS-verbinding, maar het certificaat wordt niet geverifieerd door een vertrouwde certificeringsinstantie. De post wordt niet afgeleverd.

Een TLS-verbinding wordt niet tot stand gebracht, maar de post wordt niet afgeleverd.

4. Breng om het even welke verdere veranderingen aan die aan de *Bestemmingscontroles* voor het bestemmingsdomein nodig zijn.

5. Klik op **Verzenden**.

6. Klik op de knop **Wijzigingen vastleggen**. Je kunt op dit moment desgewenst een optioneel commentaar toevoegen.

7. Klik op **Wijzigingen vastleggen** om de wijzigingen op te slaan.

ESA-certificaat: foutconfiguratiesymptomen

TLS werkt met een zelfondertekend certificaat, maar als TLS-verificatie vereist is door de afzender, zou een CA-ondertekend certificaat moeten worden geïnstalleerd.

TLS-verificatie kan mislukken, ook al is er een CA-ondertekend certificaat geïnstalleerd op de ESA.

In deze gevallen wordt aangeraden het certificaat te controleren via de stappen in het vak Verifiëren.

Verifiëren

Controleer TLS met een webbrowser

Om het door de CA ondertekende certificaat te verifiëren, dient u het certificaat toe te passen op de ESA GUI HTTPS-dienst.

Ga vervolgens naar de GUI van uw ESA in uw webbrowser. Als er waarschuwingen zijn wanneer u naar https://youresa navigeert, dan is het certificaat waarschijnlijk onjuist geketend, zoals het missen van een tussentijds certificaat.

Controleer TLS met tools van derden

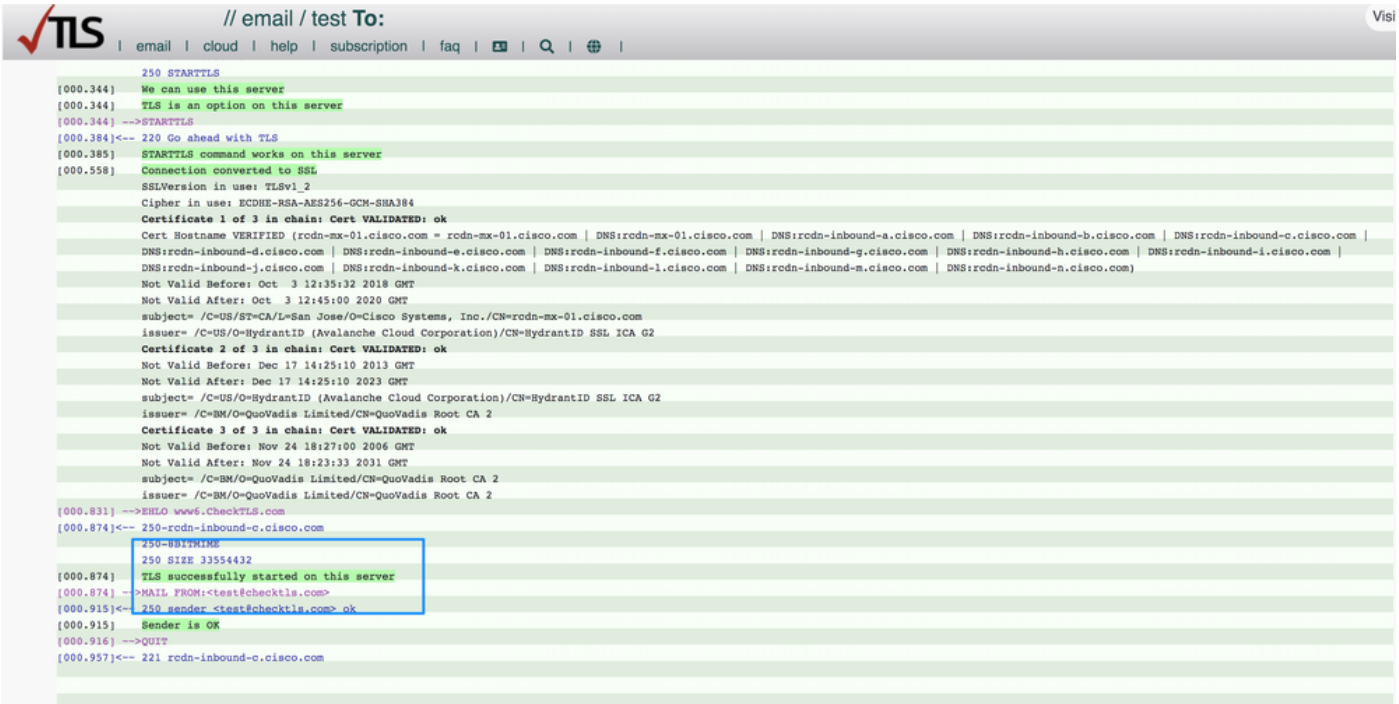
Zorg er vóór de test voor dat het te testen certificaat wordt aangevraagd bij de luisteraar waar uw apparaat inkomende mail ontvangt.

Gereedschappen van derden zoals CheckTLS.com en SSL-Tools.net kunnen worden gebruikt om de juiste koppeling van het certificaat te controleren.

Voorbeeld van CheckTLS.com Output voor TLS-verify-succes

CheckTLS Confidence Factor for "postmaster@cisco.com": 100

MX Server	Pref	Answer	Connect	HELO	TLS	Cert	Secure	From
alln-mx-01.cisco.com [173.37.147.230:25]	10	OK (41ms)	OK (422ms)	OK (50ms)	OK (48ms)	OK (450ms)	OK (58ms)	OK (41ms)
rcdn-mx-01.cisco.com [72.163.7.166:25]	20	OK (41ms)	OK (260ms)	OK (42ms)	OK (41ms)	OK (446ms)	OK (43ms)	OK (42ms)
aer-mx-01.cisco.com [173.38.212.150:25]	30	OK (80ms)	OK (484ms)	OK (81ms)	OK (79ms)	OK (548ms)	OK (80ms)	OK (81ms)
Average		100%	100%	100%	100%	100%	100%	100%



Voorbeeld van CheckTLS.com Output voor TLS-verify-fout

TestReceiver

CheckTLS Confidence Factor for "i[redacted]": 90

MX Server	Pref	Con-nect	All-owed	Can Use	TLS Adv	Cert OK	TLS Neg	Sndr OK	Rcvr OK
[redacted]	5	OK (121ms)	OK (683ms)	OK (407ms)	OK (236ms)	FAIL	OK (2,122ms)	OK (122ms)	OK (122ms)
[redacted]	5	OK (125ms)	OK (715ms)	OK (130ms)	OK (125ms)	FAIL	OK (1,608ms)	OK (125ms)	OK (127ms)
Average		100%	100%	100%	100%	0%	100%	100%	100%

Cert Hostname CONTROLEERT NIET (mailC.example.com != gvsvipa006.example.com)

Resolutie

> **Opmerking:** als een zelfondertekend certificaat wordt gebruikt, is het verwachte resultaat in de kolom "OK branden" "FAIL".

Als een CA ondertekend certificaat in gebruik is en TLS-verify nog steeds mislukt, controleert u of deze items overeenkomen:

- Algemene naam certificaat.
- Hostname (bij GUI > Network > Interface).
- MX record hostnaam: dit is de MX Server kolom in de TestReceiver tabel.

Als een CA ondertekend certificaat is geïnstalleerd en u ziet fouten, gaat u verder naar de volgende sectie voor informatie over het oplossen van problemen bij het probleem.

Problemen oplossen

In deze paragraaf wordt beschreven hoe u problemen met de TLS-basisproblemen op de ESA kunt oplossen.

Tussentijdse certificaten

Zoek dubbele tussenliggende certificaten, vooral wanneer de huidige certificaten worden bijgewerkt in plaats van een nieuw certificaat aanmaken. De tussenliggende certificaten zijn mogelijk gewijzigd of onjuist geketend en het certificaat is mogelijk geüpload op meerdere tussenliggende certificaten. Dit kan certificatie ketenen en verificatiekwesties introduceren.

Meldingen voor vereiste TLS-verbindingsfouten inschakelen

U kunt de ESA configureren om een waarschuwing te verzenden als de TLS-onderhandeling mislukt wanneer berichten worden geleverd aan een domein waarvoor een TLS-verbinding vereist is. Het waarschuwingsbericht bevat de naam van het doeldomein voor de mislukte TLS-onderhandeling. De ESA stuurt het waarschuwingsbericht naar alle ontvangers die zijn ingesteld

om waarschuwingen te ontvangen met betrekking tot de ernst van de waarschuwing voor types *systeemwaarschuwingen*.

> **Opmerking**: dit is een algemene instelling, dus het kan niet per domein worden ingesteld.

Voltooi de volgende stappen om TLS-verbindingswaarschuwingen in te schakelen:

1. Navigeer naar **mailbeleid > Bestemmingscontroles**.
2. Klik op **Globale instellingen bewerken**.
3. Schakel het aanvinkvakje **Verzend een waarschuwing in als een vereiste TLS-verbinding mislukt**.

   Tip: u kunt deze instelling ook configureren met de opdracht **destconfig > Setup** CLI.

De ESA registreert ook de instanties waarvoor TLS vereist is voor een domein, maar kon niet worden gebruikt in de maillogboeken van het apparaat. Dit gebeurt wanneer aan een van deze voorwaarden wordt voldaan:

- De externe MTA ondersteunt ESMTP niet (bijvoorbeeld, hij begreep de *EHLO*-opdracht niet van de ESA).
- De externe MTA ondersteunt ESMTP, maar de opdracht *STARTTLS* stond niet in de lijst met extensies die in de *EHLO*-respons werd geadverteerd.
- De externe MTA adverteerde voor de *STARTTLS*-extensie, maar reageerde met een fout toen de ESA de *STARTTLS*-opdracht verstuurde.

Succesvolle TLS-communicatiesessies vinden in de maillogboeken

De TLS-verbindingen worden in de e-maillogboeken opgenomen, samen met andere belangrijke handelingen die verband houden met berichten, zoals filterhandelingen, antivirus- en antispamvonnissen en leveringspogingen. Als er een succesvolle TLS-verbinding is, wordt er een resulterende TLS-*succesvermelding* ingevoerd in de e-maillogbestanden. Op dezelfde manier produceert een mislukte TLS-verbinding een *mislukte* TLS-ingang. Als een bericht geen gekoppelde TLS-ingang in het logbestand heeft, is dat bericht niet via een TLS-verbinding geleverd.

> **Tip**: raadpleeg het ESR-document Message Disposition Determination Cisco om de e-maillogbestanden te begrijpen.

Hier is een voorbeeld van een succesvolle TLS-verbinding van de externe host (receptie):

```
Tue Apr 17 00:57:53 2018 Info: New SMTP ICID 590125205 interface Data 1 (192.168.1.1) address
10.0.0.1 reverse dns host mail.example.com verified yes
Tue Apr 17 00:57:53 2018 Info: ICID 590125205 ACCEPT SG SUSPECTLIST match sbrs[-1.4:2.0] SBRS -
1.1
```

```
Tue Apr 17 00:57:54 2018 Info: ICID 590125205 TLS success protocol TLSv1 cipher DHE-RSA-AES256-
SHA
Tue Apr 17 00:57:55 2018 Info: Start MID 179701980 ICID 590125205
```

Hier is een voorbeeld van een mislukte TLS-verbinding van de externe host (receptie):

```
Mon Apr 16 18:59:13 2018 Info: New SMTP ICID 590052584 interface Data 1 (192.168.1.1) address
10.0.0.1 reverse dns host mail.example.com verified yes
Mon Apr 16 18:59:13 2018 Info: ICID 590052584 ACCEPT SG UNKNOWNLIST match sbrs[2.1:10.0] SBRS
2.7
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 TLS failed: (336109761, 'error:1408A0C1:SSL
routines:SSL3_GET_CLIENT_HELLO:no shared cipher')
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 lost
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 close
```

Hier is een voorbeeld van een succesvolle TLS-verbinding met de externe host (levering):

```
Tue Apr 17 00:58:02 2018 Info: New SMTP DCID 41014367 interface 192.168.1.1 address 10.0.0.1
port 25
Tue Apr 17 00:58:02 2018 Info: DCID 41014367 TLS success protocol TLSv1.2 cipher ECDHE-RSA-
AES256-GCM-SHA384
Tue Apr 17 00:58:03 2018 Info: Delivery start DCID 41014367 MID 179701982 to RID [0]
```

Hier is een voorbeeld van een mislukte TLS-verbinding met de externe host (levering):

```
Mon Apr 16 00:01:34 2018 Info: New SMTP DCID 40986669 interface 192.168.1.1 address 10.0.0.1
port 25
Mon Apr 16 00:01:35 2018 Info: Connection Error: DCID 40986669 domain: domain IP:10.0.0.1 port:
25 details: 454-'TLS not available due to
temporary reason' interface: 192.168.1.1 reason: unexpected SMTP response
Mon Apr 16 00:01:35 2018 Info: DCID 40986669 TLS failed: STARTTLS unexpected response
```

Gerelateerde informatie

- Cisco e-mail security applicatie – eindgebruikershandleiding
- Cisco Content Security Management-applicatie - eindgebruikershandleidingen
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.