Crea guida alla configurazione dei certificati per TLS su ESA

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Panoramica funzionale e requisiti](#)
[Acquista il tuo certificato](#)
[Aggiornare un certificato corrente](#)
[Distribuisci certificati autofirmati](#)
[Genera un certificato autofirmato e un CSR](#)
[Fornire il certificato autofirmato a una CA](#)
[Caricare il certificato firmato nell'ESA](#)
[Specificare il certificato da utilizzare con i servizi ESA](#)
[TLS in ingresso](#)
[TLS in uscita](#)
[HTTPS](#)
[LDAP](#)
[Filtro URL](#)
[Eseguire il backup della configurazione e dei certificati dell'accessorio](#)
[Attiva TLS in ingresso](#)
[Attiva TLS in uscita](#)
[Sintomi di configurazione errata dei certificati ESA](#)
[Verifica](#)
[Verifica TLS con un browser Web](#)
[Verifica TLS con strumenti di terze parti](#)
[Risoluzione dei problemi](#)
[Certificati intermedi](#)
[Abilita notifiche per errori di connessione TLS richiesti](#)
[Individua sessioni di comunicazione TLS riuscite nei log di posta](#)
[Informazioni correlate](#)

Introduzione

Questo documento descrive come creare un certificato per l'utilizzo con TLS, attivare TLS in entrata/in uscita e risolvere i problemi relativi all'ESA Cisco.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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.

Premesse

L'implementazione TLS sull'ESA fornisce privacy per la trasmissione point-to-point delle e-mail tramite crittografia. Consente a un amministratore di importare un certificato e una chiave privata da un servizio CA (Certification Authority) oppure di utilizzare un certificato autofirmato.

Cisco AsyncOS for Email Security supporta l'estensione *STARTTLS* al protocollo SMTP (Simple Mail Transfer Protocol) (*Secure SMTP over TLS*).

> **Suggerimento**: per ulteriori informazioni su TLS, consultare la RFC 3207.

> **Nota**: questo documento descrive come installare i certificati a livello di cluster con l'uso della funzione di *gestione centralizzata* sull'ESA. I certificati possono essere applicati anche a livello di computer. Tuttavia, se il computer viene rimosso dal cluster e quindi aggiunto nuovamente, i certificati a livello di computer vengono persi.

Panoramica funzionale e requisiti

Un amministratore desidera creare un certificato autofirmato sull'accessorio per uno dei motivi seguenti:

- Per crittografare le conversazioni SMTP con altri MTA che utilizzano TLS (sia in entrata che in uscita).
- Per abilitare il servizio HTTPS sull'accessorio per l'accesso alla GUI tramite HTTPS.
- Da utilizzare come certificato client per i Lightweight Directory Access Protocol (LDAP), se il server LDAP richiede un certificato client.
- Per garantire una comunicazione sicura tra l'appliance e Rivest-Shamir-Addleman (RSA), Enterprise Manager for Data Loss Protection (DLP).
- Per garantire una comunicazione sicura tra l'accessorio e un'appliance Cisco Advanced Malware Protection (AMP) Threat Grid.

L'ESA è preconfigurata con un certificato dimostrativo che può essere utilizzato per stabilire connessioni TLS.

> **Attenzione**: il certificato dimostrativo è sufficiente per stabilire una connessione TLS sicura, ma non può offrire una connessione verificabile.

Cisco consiglia di ottenere un certificato X.509 o Privacy Enhanced Email (PEM) da una CA. Questo tipo di certificato viene anche denominato certificato *Apache*. Il certificato di un'autorità di certificazione è preferibile al certificato autofirmato, in quanto è simile al certificato di dimostrazione sopra indicato, che non può offrire una connessione verificabile.

> **Nota**: il formato del certificato PEM è ulteriormente definito nelle RFC 1421 fino alle RFC 1424. PEM è un formato contenitore che può includere solo il certificato pubblico (ad esempio con installazioni Apache e file di certificati CA */etc/ssl/certs*) o un'intera catena di certificati, per includere la chiave pubblica, la chiave privata e i certificati radice. Il nome *PEM* deriva da un metodo non riuscito per la posta elettronica protetta, ma il formato contenitore utilizzato è ancora attivo ed è una traduzione in base 64 delle chiavi X.509 ASN.1.

Acquista il tuo certificato

L'opzione per l'importazione del proprio certificato è disponibile sull'ESA; tuttavia, il requisito è che il certificato sia in formato *PKCS#12*. Questo formato include la chiave privata. Gli amministratori spesso non dispongono di certificati disponibili in questo formato. Per questo motivo, Cisco consiglia di generare il certificato sull'ESA e di farlo firmare correttamente da una CA.

Aggiornare un certificato corrente

Se un certificato già esistente è scaduto, ignorare la sezione *Distribuzione di certificati autofirmati* di questo documento e firmare nuovamente il certificato esistente.

> **Suggerimento**: per ulteriori informazioni, consultare il documento sul rinnovo di un certificato su Email Security Appliance Cisco.

Distribuisci certificati autofirmati

In questa sezione viene descritto come generare un certificato autofirmato e una richiesta di firma del certificato (CSR), fornire il certificato autofirmato a una CA per la firma, caricare il certificato firmato all'ESA, specificare il certificato da utilizzare con i servizi ESA ed eseguire il backup della configurazione e dei certificati dell'accessorio.

Genera un certificato autofirmato e un CSR

Per creare un certificato autofirmato tramite la CLI, immettere il comando **certconfig**.

Per creare un certificato autofirmato dalla GUI:

1. Selezionare **Rete > Certificati > Aggiungi certificato** dalla GUI dell'accessorio.

2. Fare clic sul menu a discesa **Crea certificato autofirmato**.

   Quando si crea il certificato, verificare che il *nome comune* corrisponda al nome host dell'interfaccia di ascolto o che corrisponda al nome host dell'interfaccia di recapito. L'interfaccia di *ascolto* è l'interfaccia collegata al listener configurato in **Rete > Listener**.L'interfaccia *di recapito* viene selezionata automaticamente, a meno che non sia configurata in modo esplicito dalla CLI con il comando **deliveryconfig**.
3. Per una connessione in ingresso verificabile, verificare che i tre elementi corrispondano:

   Record MX (nome host DNS)

   Nome comune

   Nome host interfaccia

   Nota: il nome host del sistema non influisce sulle connessioni TLS per quanto riguarda la possibilità di verifica. Il nome host del sistema viene visualizzato nell'angolo superiore destro dell'interfaccia utente dell'accessorio o dall'output del comando **sethostname della** CLI.

   Attenzione: **inviare** e **confermare** le modifiche prima di esportare il CSR. Se questi passaggi non vengono completati, non verrà eseguito il commit del nuovo certificato nella configurazione dell'accessorio e il certificato firmato dalla CA non potrà firmare o essere applicato a un certificato già esistente.

Fornire il certificato autofirmato a una CA

Per inviare il certificato autofirmato a una CA per la firma:

1. Salvare il CSR in un computer locale in formato PEM **Rete > Certificati > Nome certificato > Scarica richiesta di firma certificato**.

2. Inviare il certificato generato a una CA riconosciuta per la firma.

3. Richiedere un certificato formattato X.509/PEM/Apache, nonché il certificato intermedio.

La CA genera quindi un certificato in formato PEM.

Nota: per un elenco dei provider CA, fare riferimento all'articolo di Wikipedia Certification Authority.

Caricare il certificato firmato nell'ESA

Dopo che la CA ha restituito il certificato pubblico attendibile firmato da una chiave privata, caricare il certificato firmato nell'ESA.

Il certificato può quindi essere utilizzato con un listener pubblico o privato, un servizio HTTPS

dell'interfaccia IP, l'interfaccia LDAP o tutte le connessioni TLS in uscita ai domini di destinazione.

Per caricare il certificato firmato nell'ESA:

1. Verificare che il certificato pubblico attendibile ricevuto utilizzi il formato PEM o un formato convertibile in PEM prima di caricarlo nell'accessorio. **Suggerimento**: per convertire il formato è possibile utilizzare il toolkit OpenSSL, un programma software gratuito.
2. Caricare il certificato firmato:

   Passare a **Rete > Certificati**.

   Fare clic sul nome del certificato inviato alla CA per la firma.

   Immettere il percorso del file nel computer locale o nel volume di rete.

   Nota: quando si carica il nuovo certificato, questo sovrascrive il certificato corrente. È inoltre possibile caricare un certificato intermedio correlato al certificato autofirmato.

   Attenzione: ricordarsi di **inviare** e **confermare** le modifiche dopo aver caricato il certificato firmato.

Specificare il certificato da utilizzare con i servizi ESA

Ora che il certificato è stato creato, firmato e caricato sull'ESA, può essere utilizzato per i servizi che richiedono l'utilizzo del certificato.

TLS in ingresso

Per utilizzare il certificato per i servizi TLS in ingresso, completare i seguenti passaggi:

1. Passare a **Rete > Listener**.
2. Fare clic sul nome del listener.
3. Selezionare il nome del certificato dal menu a discesa *Certificato*.
4. Fare clic su **Invia**.
5. Ripetere i passaggi da 1 a 4 in base alle esigenze per ogni listener aggiuntivo.
6. **Eseguire** il **commit** delle modifiche.

TLS in uscita

Per utilizzare il certificato per i servizi TLS in uscita, completare i seguenti passaggi:

1. Selezionare **Mail Policies > Destination Controls** (Policy di posta > Controlli destinazione).

2. Fare clic su **Modifica impostazioni globali...** nella sezione *Impostazioni globali*.
3. Selezionare il nome del certificato dal menu a discesa *Certificato*.
4. Fare clic su **Invia**.
5. **Eseguire** il **commit** delle modifiche.

HTTPS

Completare questi passaggi per utilizzare il certificato per i servizi HTTPS:

1. Selezionare **Rete > Interfacce IP**.
2. Fare clic sul nome dell'interfaccia.
3. Selezionare il nome del certificato dal menu a discesa *Certificato HTTPS*.
4. Fare clic su **Invia**.
5. Ripetere i passaggi da 1 a 4 in base alle esigenze per le interfacce aggiuntive.
6. **Eseguire** il **commit** delle modifiche.

LDAP

Per utilizzare il certificato per gli elenchi LDAP, completare i seguenti passaggi:

1. Passare a **Amministrazione sistema > LDAP**.
2. Fare clic su **Modifica impostazioni...** nella sezione *Impostazioni globali LDAP*.
3. Selezionare il nome del certificato dal menu a discesa *Certificato*.
4. Fare clic su **Invia**.
5. **Eseguire** il **commit** delle modifiche.

Filtro URL

Per utilizzare il certificato per il filtro URL:

1. Immettere il comando **websecurityconfig** nella CLI.
2. Continuare con i prompt dei comandi. Accertarsi di selezionare **Y** quando si raggiunge questo prompt:

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

3. Selezionare il numero associato al certificato.

4. Immettere il comando **commit** per eseguire il commit delle modifiche della configurazione.

Eseguire il backup della configurazione e dei certificati dell'accessorio

Verificare che la configurazione dell'accessorio sia stata salvata in questo momento. La configurazione dell'accessorio contiene il lavoro di certificazione completato che è stato applicato tramite i processi descritti in precedenza.

Per salvare il file di configurazione dell'accessorio, effettuare le seguenti operazioni:

1. Passare a **Amministrazione sistema > File di configurazione > Scarica file nel computer locale per visualizzare o salvare**.

2. Esportare il certificato:

   Passare a **Rete > Certificati**.

   Fare clic su **Esporta certificato**.

   Selezionare il certificato da esportare.

   Immettere il nome file del certificato.

   Immettere una password per il file di certificato.

   Fare clic su **Esporta**.

   Salvare il file su un computer locale o di rete.

   Èpossibile esportare certificati aggiuntivi in questo momento oppure fare clic su **Annulla** per tornare al percorso **Rete >Certificati**.

   Nota: questa procedura consente di salvare il certificato nel formato PKCS#12, in cui il file viene creato e salvato con una password di protezione.

Attiva TLS in ingresso

Per attivare TLS per tutte le sessioni in entrata, connettersi alla GUI Web, scegliere **Mail Policies > Mail Flow Policies** (Policy di posta) per il listener in entrata configurato, quindi completare i seguenti passaggi:

1. Scegliere un listener per il quale modificare i criteri.

2. Fare clic sul collegamento per il nome del criterio per modificarlo.

3. Nella sezione *Funzioni di sicurezza*, scegliere una delle seguenti opzioni di *crittografia e autenticazione* per impostare il livello di TLS richiesto per il listener e i criteri del flusso di posta:

   Off: quando si seleziona questa opzione, TLS non viene utilizzato.

   Preferenziale: quando si sceglie questa opzione, TLS può negoziare dall'MTA remoto all'ESA. Tuttavia, se l'MTA remoto non esegue la negoziazione (prima della ricezione di una risposta *220*), la transazione SMTP continua *in chiaro* (non crittografata). Non viene effettuato alcun tentativo per verificare se il certificato proviene da un'autorità di certificazione attendibile. Se si verifica un errore dopo la ricezione della risposta 220, la transazione SMTP non ritorna a testo non crittografato.

   Obbligatorio: quando si sceglie questa opzione, è possibile negoziare TLS dall'agente di trasferimento remoto all'ESA. Non viene effettuato alcun tentativo di verificare il certificato del dominio. Se la negoziazione ha esito negativo, non verrà inviato alcun messaggio di posta elettronica tramite la connessione. Se la negoziazione ha esito positivo, la posta viene recapitata tramite una sessione crittografata.
4. Fare clic su **Invia**.

5. Fare clic sul pulsante **Commit modifiche**. Se desiderato, è possibile aggiungere un commento facoltativo in questo momento.

6. Per salvare le modifiche, fare clic su **Commit modifiche**.

Il criterio del flusso di posta per il listener viene ora aggiornato con le impostazioni TLS scelte.

Completare questa procedura per attivare TLS per le sessioni in entrata che arrivano da un set selezionato di domini:

1. Connettersi alla GUI Web e scegliere **Mail Policies > HAT Overview** (Policy di posta > Panoramica HAT).

2. Aggiungere l'indirizzo IP/FQDN del mittente al gruppo di mittenti appropriato.

3. Modificare le impostazioni TLS del criterio flusso di posta associato al gruppo di mittenti modificato nel passaggio precedente.

4. Fare clic su **Invia**.

5. Fare clic sul pulsante **Commit modifiche**. Se desiderato, è possibile aggiungere un commento facoltativo in questo momento.

6. Per salvare le modifiche, fare clic su **Commit modifiche**.

Il criterio del flusso di posta per il gruppo di mittenti è stato aggiornato con le impostazioni TLS scelte.

Suggerimento: fare riferimento a questo articolo per ulteriori informazioni su come l'ESA gestisce la verifica TLS : Qual è l'algoritmo per la verifica dei certificati sull'ESA?

Attiva TLS in uscita

Per attivare TLS per le sessioni in uscita, connettersi alla GUI Web, scegliere **Mail Policies > Destination Controls** (Policy di posta > Controlli destinazione), quindi completare i seguenti passaggi:

1. Fare clic su **Aggiungi destinazione...**.

2. Aggiungere il dominio di destinazione.

3. Nella sezione *Supporto TLS*, fare clic sul menu a discesa e scegliere una delle seguenti opzioni per abilitare il tipo di TLS da configurare:

   Nessuno: quando si sceglie questa opzione, TLS non viene negoziato per le connessioni in uscita dall'interfaccia all'MTA per il dominio.

   Preferenziale: quando si sceglie questa opzione, il TLS viene negoziato dall'interfaccia ESA agli MTA del dominio. Tuttavia, se la negoziazione TLS non riesce (prima della ricezione di una risposta 220), la transazione SMTP continua *in chiaro* (non crittografata). Non viene eseguito alcun tentativo per verificare se il certificato proviene da una CA attendibile. Se si verifica un errore dopo la ricezione della risposta 220, la transazione SMTP non ritorna a testo non crittografato.

   Obbligatorio: quando si sceglie questa opzione, il TLS viene negoziato dall'interfaccia ESA agli MTA per il dominio. Non viene effettuato alcun tentativo di verificare il certificato del dominio. Se la negoziazione ha esito negativo, non verrà inviato alcun messaggio di posta elettronica tramite la connessione. Se la negoziazione ha esito positivo, la posta viene recapitata tramite una sessione crittografata.

   Preferred-Verify: quando si sceglie questa opzione, il TLS viene negoziato dall'ESA agli MTA del dominio e l'accessorio tenta di verificare il certificato di dominio. In questo caso, sono possibili i seguenti tre risultati:

   Il TLS viene negoziato e il certificato verificato. La posta viene recapitata tramite una sessione crittografata.

   Il TLS viene negoziato, ma il certificato non viene verificato. La posta viene recapitata tramite una sessione crittografata.

   Non viene stabilita alcuna connessione TLS e il certificato non viene verificato. Il messaggio e-mail viene recapitato in formato testo normale.**Required-Verify**: quando si sceglie questa opzione, il TLS viene negoziato dall'ESA agli MTA per il dominio ed è necessaria la verifica del certificato di dominio. In questo caso, sono possibili i seguenti tre risultati:

   Una connessione TLS viene negoziata e il certificato viene verificato. Il messaggio e-mail viene recapitato tramite una sessione crittografata.

Una connessione TLS viene negoziata, ma il certificato non viene verificato da una CA attendibile. La posta non viene recapitata.

Una connessione TLS non viene negoziata, ma la posta non viene recapitata.

4. Apportare le ulteriori modifiche necessarie ai *controlli di destinazione* per il dominio di destinazione.

5. Fare clic su **Invia**.

6. Fare clic sul pulsante **Commit modifiche**. Se desiderato, è possibile aggiungere un commento facoltativo in questo momento.

7. Per salvare le modifiche, fare clic su **Commit modifiche**.

Sintomi di configurazione errata dei certificati ESA

TLS funziona con un certificato autofirmato, tuttavia se la verifica TLS è richiesta dal mittente, è necessario installare un certificato firmato dall'autorità di certificazione.

La verifica TLS può avere esito negativo anche se sull'ESA è stato installato un certificato firmato dalla CA.

In questi casi, si consiglia di verificare il certificato eseguendo la procedura descritta nella sezione Verifica.

Verifica

Verifica TLS con un browser Web

Per verificare il certificato firmato dalla CA, applicare il certificato al servizio HTTPS GUI ESA.

Quindi, accedere alla GUI dell'ESA nel browser Web. Se vengono visualizzati avvisi quando si passa a https://youresa, è probabile che il certificato sia concatenato in modo non corretto, ad esempio che non sia presente un certificato intermedio.

Verifica TLS con strumenti di terze parti

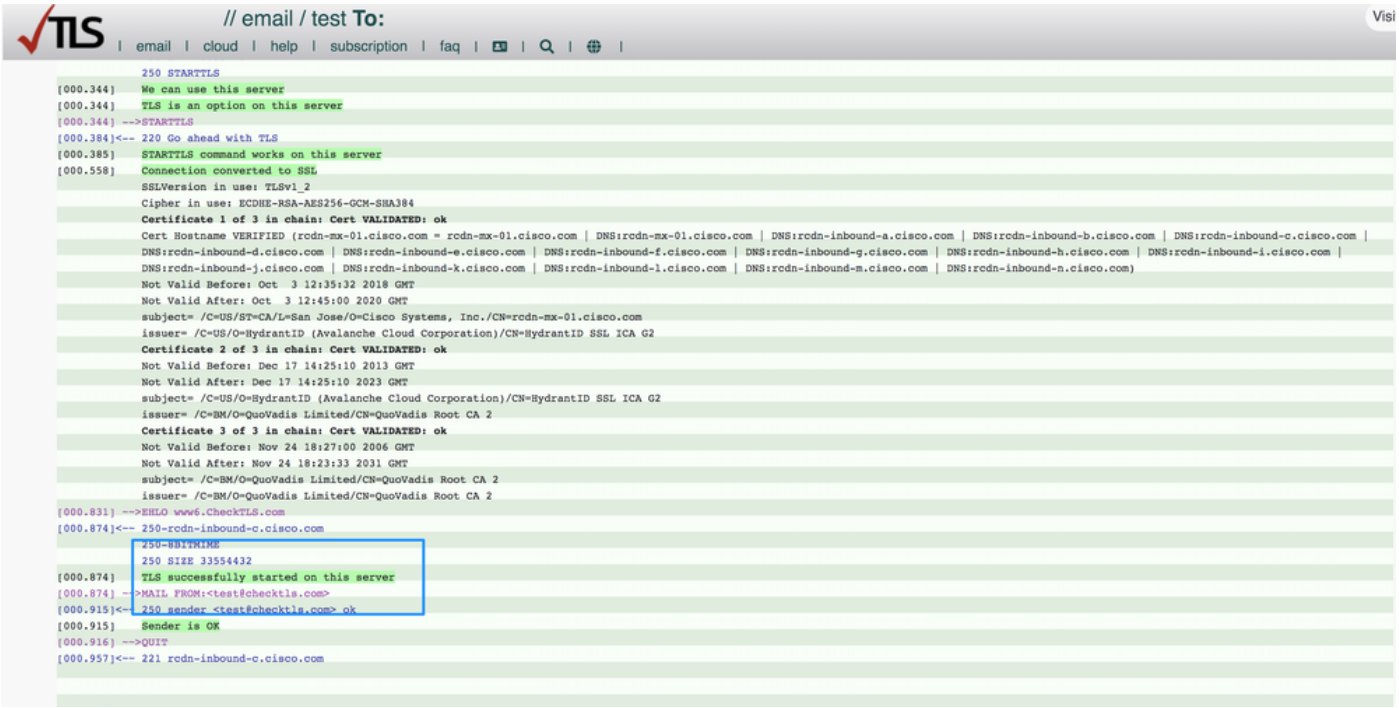
Prima di eseguire il test, verificare che il certificato da testare venga applicato al listener in cui l'accessorio riceve la posta in entrata.

Èpossibile utilizzare strumenti di terze parti, ad esempio CheckTLS.com e SSL-Tools.net, per verificare il corretto concatenamento del certificato.

Esempio di output CheckTLS.com per la verifica TLS riuscita

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%



Esempio di output CheckTLS.com per errore di verifica TLS

TestReceiver

CheckTLS Confidence Factor for "[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%

Il nome host del certificato NON VIENE VERIFICATO (mailC.example.com != gvsvipa006.example.com)

Risoluzione

> **Nota:** se è in uso un certificato autofirmato, il risultato previsto nella colonna "Cert OK" è "FAIL".

Se è in uso un certificato firmato da un'autorità di certificazione e la verifica TLS ha comunque esito negativo, verificare che i seguenti elementi corrispondano:

- Nome comune del certificato.
- Hostname (su GUI > Rete > Interfaccia).
- Nome host record MX: colonna del server MX nella tabella TestReceiver.

Se è stato installato un certificato firmato dall'autorità di certificazione e vengono visualizzati errori, passare alla sezione successiva per informazioni sulla risoluzione del problema.

Risoluzione dei problemi

Questa sezione descrive come risolvere i problemi relativi al TLS di base sull'ESA.

Certificati intermedi

Cercare i certificati intermedi duplicati, in particolare quando i certificati correnti vengono aggiornati anziché essere creati. È possibile che i certificati intermedi siano stati modificati o che siano stati concatenati in modo non corretto e che il certificato abbia caricato più certificati intermedi. Ciò può introdurre problemi di concatenamento e verifica dei certificati.

Abilita notifiche per errori di connessione TLS richiesti

Èpossibile configurare l'ESA in modo da inviare un avviso se la negoziazione TLS non riesce quando i messaggi vengono recapitati a un dominio che richiede una connessione TLS. Il messaggio di avviso contiene il nome del dominio di destinazione per la negoziazione TLS non riuscita. L'ESA invia il messaggio di allarme a tutti i destinatari impostati per ricevere gli allarmi del livello di gravità dell'allarme per i tipi di allarme *del sistema*.

> **Nota**: questa è un'impostazione globale, quindi non può essere impostata per i singoli domini.

Per abilitare gli avvisi di connessione TLS, completare i seguenti passaggi:

1. Selezionare **Mail Policies > Destination Controls** (Policy di posta > Controlli destinazione).
2. Fare clic su **Modifica impostazioni globali**.
3. Selezionare la casella di controllo **Invia un avviso quando una connessione TLS necessaria non riesce**.

> **Suggerimento**: è possibile configurare questa impostazione anche con il comando **destconfig > setup** CLI.

L'ESA registra inoltre le istanze per le quali è richiesto TLS per un dominio, ma non è stato possibile utilizzarlo nei log di posta dell'accessorio. Questo si verifica quando viene soddisfatta una delle seguenti condizioni:

- L'MTA remoto non supporta ESMTP (ad esempio, non ha compreso il comando *EHLO* dell'ESA).
- L'agente di trasferimento messaggi remoto supporta ESMTP, ma il comando *STARTTLS* non è incluso nell'elenco delle estensioni annunciate nella risposta *EHLO*.
- L'agente di trasferimento messaggi remoto ha annunciato l'estensione *STARTTLS*, ma ha risposto con un errore quando l'ESA ha inviato il comando *STARTTLS*.

Individua sessioni di comunicazione TLS riuscite nei log di posta

Le connessioni TLS vengono registrate nei log di posta, insieme ad altre azioni significative correlate ai messaggi, come le operazioni filtro, i verdetti antivirus e antispam e i tentativi di recapito. Se la connessione TLS ha esito positivo, nei log di posta risulta una voce TLS *success*. Analogamente, una connessione TLS non riuscita genera una voce TLS *non riuscita*. Se a un messaggio non è associata una voce TLS nel file di log, il messaggio non è stato recapitato tramite una connessione TLS.

> **Suggerimento**: per ulteriori informazioni sui log di posta, consultare il documento Cisco ESA Message Disposition Determination.

Di seguito è riportato un esempio di una connessione TLS riuscita dall'host remoto (ricezione):

```
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
```

Di seguito è riportato un esempio di connessione TLS non riuscita dall'host remoto (ricezione):

```
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
```

Di seguito è riportato un esempio di una connessione TLS all'host remoto (recapito) riuscita:

```
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]
```

Di seguito è riportato un esempio di connessione TLS all'host remoto (recapito) non riuscita:

```
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
```

Informazioni correlate

- Cisco Email Security Appliance - Guide per l'utente
- Cisco Content Security Management Appliance - Guide per l'utente
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).