

Configurare TLSv1.3 per Secure Email Gateway

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Componenti usati](#)

[Panoramica](#)

[Configurazione](#)

[Configurazione da WebUI](#)

[Configurazione dalla CLI:](#)

[Verifica](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive la configurazione del protocollo TLS v1.3 per Cisco Secure Email Gateway (SEG).

Prerequisiti

Si desidera una conoscenza generale delle impostazioni e della configurazione di SEG.

Componenti usati

- Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:
 - Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 e versioni successive.
- Impostazioni di configurazione SSL SEG.

"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".

Panoramica

Il SEG ha integrato il protocollo TLS v1.3 per crittografare le comunicazioni per i servizi correlati a SMTP e HTTPS; interfaccia utente classica, NGUI e API Rest.

Il protocollo TLS v1.3 offre una comunicazione più sicura e una negoziazione più rapida, in quanto il settore lavora per renderlo lo standard.

SEG utilizza il metodo di configurazione SSL esistente all'interno di SEG WebUI o CLI di SSL con

alcune impostazioni importanti da evidenziare.

- Consigli cautelativi per la configurazione dei protocolli autorizzati.
- I cifrari non possono essere manipolati.
- TLS v1.3 può essere configurato per GUI HTTPS, Posta in arrivo e Posta in uscita.
- Le opzioni di selezione della casella di controllo del protocollo TLS tra TLS v1.0 e TLS v1.3 utilizzano uno schema illustrato più dettagliatamente all'interno dell'articolo.

Configurazione

Il SEG integra il protocollo TLS v1.3 per HTTPS e SMTP in AsyncOS 15.5. È consigliabile prestare attenzione quando si scelgono le impostazioni del protocollo per evitare errori di ricezione/recapito dei messaggi e-mail e HTTPS.

Le versioni precedenti di Cisco SEG supportano TLS v1.2 nella fascia alta, insieme ad altri provider di posta elettronica come MS O365 che supportano TLS v1.2 al momento in cui l'articolo è stato scritto.

L'implementazione Cisco SEG del protocollo TLS v1.3 supporta 3 cifrari predefiniti che non possono essere modificati o esclusi dalle impostazioni di configurazione della cifratura SEG come gli altri protocolli consentono.

Le impostazioni di configurazione SSL SEG esistenti consentono ancora la modifica di TLS v1.0, v1.1, v1.2 alle suite di cifratura.

Cifre TLS 1.3:

TLS_AES_256_GCM_SHA384

TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

Configurazione da WebUI

Selezionare > Amministrazione sistema > Configurazione SSL

- Dopo l'aggiornamento alla versione 15.5 AsyncOS, la selezione del protocollo TLS predefinito include solo TLS v1.1 e TLS v1.2.
- L'impostazione per "Altri servizi client TLS" utilizza TLS v1.1 e TLS v1.2 con l'opzione di selezione, utilizzare solo TLS v1.0.

SSL Configuration			
GUI HTTPS:	Methods:	TLS v1.2 TLS v1.1	
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!D ES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA! ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:- EXPORT:-IDEA:!DHE-RSA-AES128-CCM:!DHE-RSA- AES256-CCM:!DHE-RSA-AES256-SHA	
	TLS Renegotiation:	Enabled	
Inbound SMTP:	Methods:	TLS v1.2 TLS v1.1	
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!D ES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA! ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:- EXPORT:-IDEA:!DHE-RSA-AES128-CCM:!DHE-RSA- AES256-CCM:!DHE-RSA-AES256-SHA	
	TLS Renegotiation:	Enabled	
Outbound SMTP:	Methods:	TLS v1.2 TLS v1.1	
	SSL Cipher(s) to use:	ECDH+aRSA:ECDH+ECDSA:DHE+DSS+AES:AES128:A ES256:!3DES:!IDEA:!SRP:IAESGCM+DH+aRSA:IAESG CM+RSA:!aNULL:!eNULL:!kRSA:@STRENGTH:- aNULL:-EXPORT:-IDEA:!DHE-RSA-AES128-CCM:!DHE- RSA-AES256-CCM:!ECDHE-ECDSA-CAMELLIA128- SHA256:!ECDHE-RSA-CAMELLIA128-SHA256:!ECDHE- ECDSA-CAMELLIA256-SHA384:!ECDHE-RSA- CAMELLIA256-SHA384:!ECDHE-ECDSA-AES128- CCM:!ECDHE-ECDSA-AES256-CCM:!DHE-RSA-AES256- SHA	
	Other TLS Client Services: ?	Methods: TLS v1.2, TLS v1.1 are being used as default	
Peer Certificate FQDN Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	Disabled	
Peer Certificate X509 Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	Disabled	

Other TLS Client Services ⊞

TLS method is applicable for the following services:

LDAP
Updater Client
SMTP Call-Ahead
Remote Syslog Server

Default TLS Selections

Selezionare "Edit Settings" (Modifica impostazioni) per visualizzare le opzioni di configurazione.

- TLS v1.1 e TLS v1.2 sono selezionate con caselle attive per selezionare gli altri protocolli.
- L'? accanto a ogni TLS v1.3 è una ripetizione delle opzioni di crittografia statica.
- In "Altri servizi client TLS:" è ora possibile utilizzare TLS v1.0 solo se questa opzione è selezionata.

SSL Configuration		
GUI HTTPS:	Methods:	<input type="checkbox"/> TLS v1.3 [?] <input checked="" type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!e
	TLS Renegotiation:	<input checked="" type="checkbox"/> Enable
Inbound SMTP:	Methods:	<input type="checkbox"/> TLS v1.3 [?] <input checked="" type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!e
	TLS Renegotiation:	<input checked="" type="checkbox"/> Enable
Outbound SMTP:	Methods:	<input type="checkbox"/> TLS v1.3 [?] <input checked="" type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0
	SSL Cipher(s) to use:	ECDH+aRSA:ECDH+ECDSA:DHE+DSS+
Other TLS Client Services: [?]	Methods:	<input type="checkbox"/> TLS v1.0
Peer Certificate FQDN Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	<input type="checkbox"/> Enable
Peer Certificate X509 Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	<input type="checkbox"/> Enable

TLSv1.3 Cipher Info
 TLSv1.3 uses the default ciphers. You do not need to configure any cipher for TLSv1.3.

Informational ? for TLS Default Ciphers

Note:

TLS protocols can be enabled only in sequence.

The configured SSL Cipher(s) do not apply to TLS 1.3. The TLS 1.3 protocol uses default ciphers.

Le opzioni di selezione del protocollo TLS includono TLS v1.0, TLS v1.1, TLS v1.2, TLS v1.3.

- Dopo l'aggiornamento ad AsyncOS 15.5, per impostazione predefinita vengono selezionati solo i protocolli TLS v1.1 e TLS v1.2.



Nota: TLS1.0 è deprecato e quindi disabilitato per impostazione predefinita. TLS v1.0 è ancora disponibile se il proprietario sceglie di attivarlo.


- Le opzioni della casella di controllo si illuminano con caselle in grassetto che presentano le caselle Protocolli disponibili e In grigio per le opzioni non compatibili.
- Le opzioni di esempio nell'immagine illustrano le opzioni della casella di controllo.

<input type="checkbox"/> TLS v1.3	<input type="checkbox"/> TLS v1.3	<input type="checkbox"/> TLS v1.3	<input type="checkbox"/> TLS v1.3
<input checked="" type="checkbox"/> TLS v1.2	<input checked="" type="checkbox"/> TLS v1.2	<input type="checkbox"/> TLS v1.2	<input type="checkbox"/> TLS v1.2
<input checked="" type="checkbox"/> TLS v1.1	<input type="checkbox"/> TLS v1.1	<input checked="" type="checkbox"/> TLS v1.1	<input type="checkbox"/> TLS v1.1
<input type="checkbox"/> TLS v1.0	<input type="checkbox"/> TLS v1.0	<input type="checkbox"/> TLS v1.0	<input type="checkbox"/> TLS v1.0

<input checked="" type="checkbox"/> TLS v1.3	<input type="checkbox"/> TLS v1.3	<input checked="" type="checkbox"/> TLS v1.3
<input checked="" type="checkbox"/> TLS v1.2	<input type="checkbox"/> TLS v1.2	<input type="checkbox"/> TLS v1.2
<input checked="" type="checkbox"/> TLS v1.1	<input type="checkbox"/> TLS v1.1	<input type="checkbox"/> TLS v1.1
<input type="checkbox"/> TLS v1.0	<input checked="" type="checkbox"/> TLS v1.0	<input type="checkbox"/> TLS v1.0

Visualizzazione di esempio post-commit dei protocolli TLS selezionati.

SSL Configuration		
GUI HTTPS:	Methods:	TLS v1.3 [?] TLS v1.2
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!D ES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA! ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:!aNULL! EXPORT:!IDEA:!DHE-RSA-AES256-SHA:!DHE-RSA- AES128-CCM:!DHE-RSA-AES256-CCM
	TLS Renegotiation:	Enabled
Inbound SMTP:	Methods:	TLS v1.3 [?] TLS v1.2 TLS v1.1 TLS v1.0
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!D ES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA! ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:!aNULL! EXPORT:!IDEA:!DHE-RSA-AES256-SHA:!DHE-RSA- AES128-CCM:!DHE-RSA-AES256-CCM
	TLS Renegotiation:	Enabled
Outbound SMTP:	Methods:	TLS v1.3 [?] TLS v1.2 TLS v1.1
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!D ES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA! ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:!aNULL! EXPORT:!IDEA:!DHE-RSA-AES256-SHA:!DHE-RSA- AES128-CCM:!DHE-RSA-AES256-CCM:!ECDHE-ECDSA- CAMELLIA128-SHA256:!ECDHE-RSA-CAMELLIA128- SHA256:!ECDHE-ECDSA-CAMELLIA256- SHA384:!ECDHE-RSA-CAMELLIA256-SHA384! ECDHE-ECDSA-AES128-CCM:!ECDHE-ECDSA-AES256-CCM
Other TLS Client Services: [?]	Methods:	TLS v1.2, TLS v1.1 are being used as default
Peer Certificate FQDN Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	Disabled
Peer Certificate X509 Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	Disabled

 Nota: le modifiche al protocollo TLS HTTPS della GUI provocano una breve disconnessione da WebUI a causa della reimpostazione del servizio HTTPS.

Configurazione dalla CLI:

Il SEG permette a TLS v1.3 di offrire 3 servizi:

- GUI HTTPS
- SMTP in ingresso
- SMTP in uscita

Eseguendo il comando `> sslconfig`, vengono restituiti i protocolli e le cifrature attualmente configurati per HTTPS GUI, SMTP in entrata, SMTP in uscita

- Metodo HTTPS GUI: `tlsv1_0tlsv1_1tlsv1_2tlsv1_3`
- Metodo SMTP in ingresso: `tlsv1_0tlsv1_1tlsv1_2tlsv1_3`
- Metodo SMTP in uscita: `tlsv1_1tlsv1_2tlsv1_3`

Scegliere l'operazione da eseguire:


- GUI - Modifica impostazioni ssl HTTPS GUI.
- IN ENTRATA - Consente di modificare le impostazioni SSL SMTP in entrata.
- IN USCITA - Consente di modificare le impostazioni SSL SMTP in uscita.

`[]>` in entrata

Immettere il metodo SSL SMTP in ingresso che si desidera utilizzare.

1. TLS v1.3
2. TLS v1.2
3. TLS v1.1
4. TLS v1.0

`[2-4]>` 1-3

 Nota: il processo di selezione SEG può includere un singolo numero di menu, ad esempio 2, un intervallo di numeri di menu, ad esempio da 1 a 4, o numeri di menu separati da virgole 1,2,3.

Nelle successive richieste di CLI `sslconfig`, il valore esistente viene accettato premendo "invio" o modificando l'impostazione come desiderato.

Completare la modifica con il comando `> commit >>` immettere un commento facoltativo, se desiderato `>>` premere "Invio" per completare le modifiche.

Verifica

In questa sezione sono inclusi alcuni scenari di test di base ed errori che possono verificarsi a causa di versioni del protocollo TLS non corrispondenti o di errori di sintassi.

Voce di log di esempio di una negoziazione SMTP in uscita SEG che genera un rifiuto a causa di

una destinazione TLS v1.3 non supportata:

```
Wed Jan 17 20:41:18 2024 Info: DCID 485171 TLS deferring: (336151598, 'error:1409442E:SSL routines:ssl3
```

Esempio di voce nel log di un SEG di invio che riceve un TLS v1.3 negoziato correttamente:

```
Wed Jan 17 21:09:12 2024 Info: DCID 485206 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384
```

Voce di log di esempio di un SEG ricevente senza TLS v1.3 abilitato.

```
Wed Jan 17 20:11:06 2024 Info: ICID 1020004 TLS failed: (337678594, 'error:14209102:SSL routines:tls_ea
```

Ricezione di TLS supportate da SEG v1.3

```
Wed Jan 17 21:09:12 2024 Info: ICID 1020089 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384
```

Per verificare la funzionalità del browser, è sufficiente aprire una sessione del browser Web in SEG WebUI o NGUI configurata con TLSv1.3.



Nota: tutti i browser Web testati sono già configurati per accettare TLS v1.3.

- Test: la configurazione dell'impostazione del browser in Firefox per disattivare il supporto di TLS v1.3 genera errori sia nell'interfaccia utente classica che nell'interfaccia NGUI dell'accessorio.
- Interfaccia utente classica che utilizza Firefox configurata per escludere TLS v1.3 come test.
- NGUI riceverà lo stesso errore con l'unica eccezione del numero di porta 4431 (predefinito) all'interno dell'URL.

Secure Connection Failed

An error occurred during a connection to dh6062-esa1.iphmx.com. Peer reports incompatible or unsupported protocol version.

Error code: SSL_ERROR_PROTOCOL_VERSION_ALERT

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

This website might not support the TLS 1.2 protocol, which is the minimum version supported by Firefox.

[Learn more...](#)

It looks like your network security settings might be causing this. Do you want the default settings to be restored?

- Verificare le impostazioni del browser per assicurarsi che TLSv1.3 sia incluso. (Questo esempio è da Firefox e utilizza i numeri 1-4)

security.tls.version.fallback-limit	4
security.tls.version.max	4
security.tls.version.min	3

Informazioni correlate

- [Cisco Secure Email Gateway - Guida alla configurazione](#)
- [Pagina di avvio di Cisco Secure Email Gateway per il supporto delle guide](#)
- [Cisco Secure Email Gateway - Note sulla release](#)

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).