

Configuration de TLSv1.3 pour la passerelle de messagerie sécurisée

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Composants utilisés](#)

[Aperçu](#)

[Configurer](#)

[Configuration à partir de WebUI](#)

[Configuration CLI :](#)

[Vérifier](#)

[Informations connexes](#)

Introduction

Ce document décrit la configuration du protocole TLS v1.3 pour Cisco Secure Email Gateway (SEG).

Conditions préalables

Une connaissance générale des paramètres et de la configuration du SEG est souhaitée.

Composants utilisés

- Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :
 - Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 et versions ultérieures.
- Paramètres de configuration SEG SSL.

"Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de comprendre l'impact potentiel de toute commande. »

Aperçu

Le SEG a intégré le protocole TLS v1.3 pour chiffrer les communications pour les services SMTP et HTTPS ; interface utilisateur classique, interface utilisateur nouvelle génération et API de repos.

Le protocole TLS v1.3 offre des communications plus sécurisées et des négociations plus rapides,

car le secteur travaille à en faire la norme.

Le SEG utilise la méthode de configuration SSL existante dans l'interface WebUI ou CLI de SEG de SSL avec quelques paramètres notables à mettre en évidence.

- Conseils de prudence lors de la configuration des protocoles autorisés.
- Les chiffrements ne peuvent pas être manipulés.
- TLS v1.3 peut être configuré pour HTTPS, les messages entrants et les messages sortants de l'interface utilisateur graphique.
- Les options de sélection de la case à cocher du protocole TLS entre TLS v1.0 et TLS v1.3 utilisent un modèle illustré plus en détail dans l'article.

Configurer

Le SEG intègre le protocole TLS v1.3 pour HTTPS et SMTP dans AsyncOS 15.5. Il est recommandé de faire preuve de prudence lors du choix des paramètres de protocole pour éviter les échecs HTTPS et de remise/réception des e-mails.

Les versions précédentes de Cisco SEG prennent en charge TLS v1.2 haut de gamme avec d'autres fournisseurs de messagerie tels que MS O365 prenant en charge TLS v1.2 au moment de la rédaction de l'article.

L'implémentation Cisco SEG du protocole TLS v1.3 prend en charge 3 chiffrements par défaut qui ne peuvent pas être modifiés ou exclus dans les paramètres de configuration du chiffrement SEG comme le permettent les autres protocoles.

Les paramètres de configuration SSL SEG existants autorisent toujours la manipulation des protocoles TLS v1.0, v1.1 et v1.2 vers les suites de chiffrement.

Chiffres TLS 1.3 :

TLS_AES_256_GCM_SHA384

TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

Configuration à partir de WebUI

Accédez à > Administration système > Configuration SSL

- La sélection du protocole TLS par défaut après la mise à niveau vers 15.5 AsyncOS inclut TLS v1.1 et TLS v1.2 uniquement.
- Le paramètre « Autres services client TLS » utilise TLS v1.1 et TLS v1.2 avec l'option de sélection, utilisez uniquement 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: (?)	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

Sélectionnez « Modifier les paramètres » pour présenter les options de configuration.


- Les protocoles TLS v1.1 et TLS v1.2 sont cochés avec des cases actives pour sélectionner les autres protocoles.
- Le point d'interrogation (?) situé en regard de chaque TLS v1.3 est une répétition des options de chiffrement statique.
- L'option « Autres services client TLS : » propose désormais d'utiliser TLS v1.0 uniquement si cette option est sélectionnée.

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:	<div style="border: 1px solid gray; padding: 2px; width: fit-content;"> TLSv1.3 Cipher Info TLSv1.3 uses the default ciphers. You do not need to configure any cipher for TLSv1.3. </div> <p style="color: red; margin-left: 20px;">Informational ? for TLS Default Ciphers</p> 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

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.

Les options de sélection du protocole TLS incluent TLS v1.0, TLS v1.1, TLS v1.2 et TLS v1.3.

- Après la mise à niveau vers AsyncOS 15.5, seuls les protocoles TLS 1.1 et TLS 1.2 sont sélectionnés par défaut.

 Remarque : TLS1.0 est déconseillé et donc désactivé par défaut. TLS v1.0 est toujours disponible si le propriétaire choisit de l'activer.


- Les options de case à cocher s'affichent avec des cases en gras présentant les protocoles disponibles et les cases grisées pour les options non compatibles.
- Les exemples d'options de l'image illustrent les options de case à cocher.

<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

Exemple de vue Post-commit des protocoles TLS sélectionnés.

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

 Remarque : les modifications apportées au protocole HTTPS TLS de l'interface utilisateur graphique entraînent une courte déconnexion de l'interface WebUI en raison de la réinitialisation du service HTTPS.

Configuration CLI :

Le SEG autorise les services TLS v1.3 sur 3 :

- HTTPS GUI
- SMTP entrant
- SMTP sortant

L'exécution de la commande > sslconfig, affiche les protocoles et les chiffrements actuellement configurés pour l'interface graphique HTTPS, le protocole SMTP entrant et le protocole SMTP sortant

- Méthode HTTPS de l'interface utilisateur graphique : tlv1_0tlv1_1tlv1_2tlv1_3
- Méthode SMTP entrante : tlv1_0tlv1_1tlv1_2tlv1_3
- Méthode SMTP sortante : tlv1_1tlv1_2tlv1_3

Sélectionnez l'opération que vous souhaitez effectuer :


- GUI - Modifiez les paramètres SSL HTTPS de l'interface utilisateur graphique.
- INBOUND - Modifiez les paramètres ssl SMTP entrants.
- OUTBOUND - Modifiez les paramètres SSL SMTP sortants.

[> entrant

Entrez la méthode SMTP SSL entrante que vous souhaitez utiliser.

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

[2-4]> 1-3

 Remarque : le processus de sélection SEG peut inclure un numéro de menu unique tel que 2, une plage de numéros de menu tels que 1-4 ou des numéros de menu séparés par des virgules 1,2,3.

Les invites suivantes de la commande CLI sslconfig acceptent la valeur existante en appuyant sur Entrée ou en modifiant le paramètre comme vous le souhaitez.

Complétez la modification à l'aide de la commande > commit >> saisissez un commentaire facultatif si vous le souhaitez >> appuyez sur « Entrée » pour compléter les modifications.

Vérifier

Cette section présente quelques scénarios de test de base et les erreurs pouvant se produire en raison de versions de protocole TLS non concordantes ou d'erreurs de syntaxe.

Exemple d'entrée de journal d'une négociation SMTP sortante SEG générant un rejet dû à une destination TLS v1.3 non prise en charge :

```
Wed Jan 17 20:41:18 2024 Info: DCID 485171 TLS deferring: (336151598, 'error:1409442E:SSL routines:ss13
```

Exemple d'entrée de journal d'un SEG émetteur recevant un TLS v1.3 négocié avec succès :

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

Exemple d'entrée de journal d'un SEG récepteur sans TLS v1.3 activé.

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

Réception de TLS v1.3 pris en charge par SEG

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

Pour vérifier la fonctionnalité de votre navigateur, ouvrez simplement une session de navigateur Web sur la SEG WebUI ou NGUI configurée avec TLSv1.3.

 Remarque : tous les navigateurs Web testés sont déjà configurés pour accepter TLS v1.3.

- Test : la configuration du paramètre de navigateur sur Firefox désactivant la prise en charge de TLS v1.3 produit des erreurs sur l'interface ClassicUI et l'interface NGUI de l'appliance.
- Interface utilisateur classique utilisant Firefox configurée pour exclure TLS v1.3, comme test.
- NGUI reçoit la même erreur, à la seule exception du numéro de port 4431 (par défaut) dans l'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?

- Pour garantir la communication, vérifiez les paramètres du navigateur pour vous assurer que TLSv1.3 est inclus. (Cet exemple provient de Firefox et utilise les numéros 1 à 4

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

Informations connexes

- [Cisco Secure Email Gateway - Guide de configuration](#)
- [Guides d'assistance de la page de lancement de Cisco Secure Email Gateway](#)
- [Cisco Secure Email Gateway - Notes de version](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.