TLSv1.3 configureren voor beveiligde e-mailgateway

Inhoud

Inleiding

Dit document beschrijft de configuratie van het TLS v1.3-protocol voor Cisco Secure Email Gateway (SEG).

Voorwaarden

Een algemene kennis van de SEG-instellingen en -configuratie is gewenst.

Gebruikte componenten

- De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:
  - Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 en nieuwer.
- SEG SSL-instellingen.

"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, zorg er dan voor dat u de mogelijke impact van elke opdracht begrijpt."

Overzicht

De SEG heeft het TLS v1.3-protocol geïntegreerd om communicatie voor SMTP- en HTTPS-gerelateerde services te versleutelen; Classic UI, NGUI en Rest API.

TLS v1.3 Protocol biedt veiligere communicatie en snellere onderhandeling terwijl de industrie werkt om er de standaard van te maken.

De SEG maakt gebruik van de bestaande SSL Configuration methode binnen de SEG WebUI of CLI van SSL met een paar opmerkelijke instellingen om te markeren.

- Voorzorgsadvies bij het configureren van de toegestane protocollen.
- De codering kan niet worden gemanipuleerd.
- TLS v1.3 kan worden geconfigureerd voor GUI HTTPS, inkomende post en uitgaande post.
- Met de selectieopties voor het TLS-protocol tussen TLS v1.0 en TLS v1.3 wordt een patroon gebruikt dat in het artikel meer in detail wordt weergegeven.

Configureren

De SEG integreert het TLS v1.3-protocol voor HTTPS en SMTP in AsycOS 15.5. Voorzichtigheid wordt aanbevolen bij het kiezen van de protocolinstellingen om te voorkomen dat HTTPS en e-maillevering/ontvangst mislukkingen.

Eerdere releases van Cisco SEG ondersteunen TLS v1.2 aan de top-end samen met andere e-mailproviders zoals MS O365 die TLS v1.2 ondersteunen op het moment dat het artikel werd geschreven.

De Cisco SEG-implementatie van het TLS v1.3 Protocol ondersteunt 3 standaardalgoritmen die niet kunnen worden gewijzigd of uitgesloten binnen de instellingen voor de configuratie van het SEG-algoritme zoals de andere protocollen dat toestaan.

De bestaande SEG SSL Configuration-instellingen maken nog steeds manipulatie van de TLS v1.0, v1.1, v1.2 manipulatie mogelijk om coderingssuites te gebruiken.

TLS 1.3-algoritmen:

TLS_AES_256_GCM_SHA384

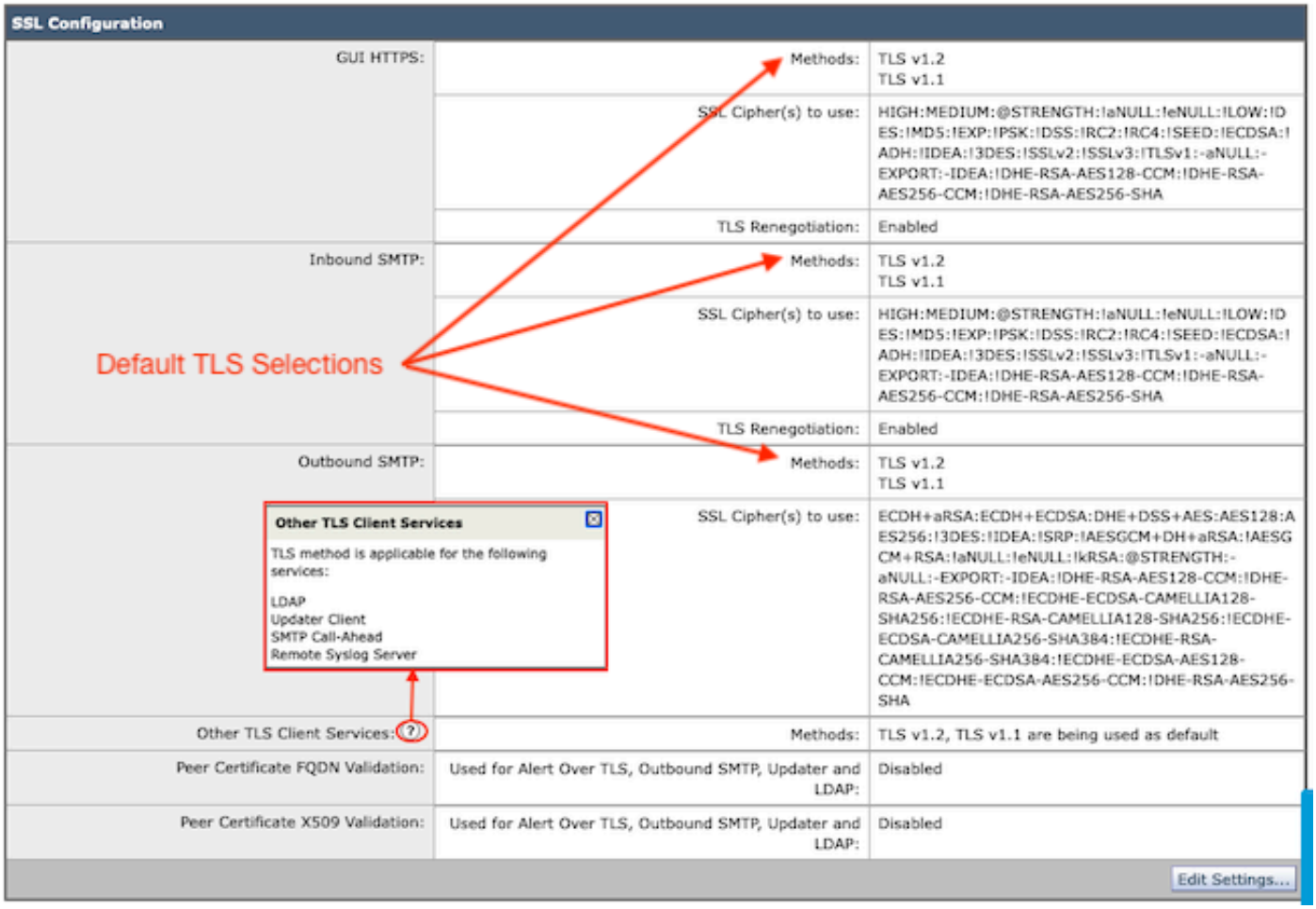
TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

Configuratie via WebUI

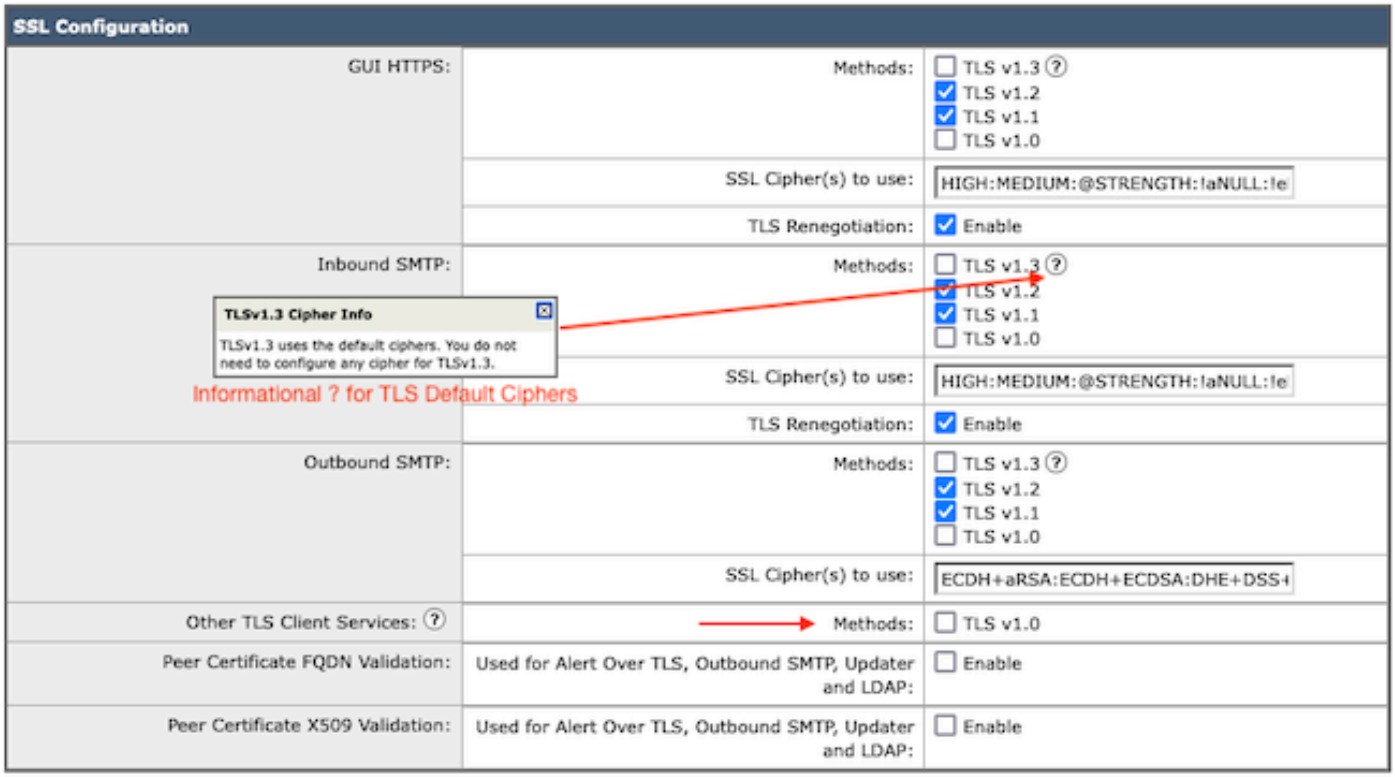
Navigeren naar > Systeembeheer > SSL-configuratie

- De standaard TLS Protocol selectie post upgrade naar 15.5 AsyncOS bevat alleen TLS v1.1 en TLS v1.2.
- De instelling voor "Overige TLS-clientservices" gebruikt TLS v1.1 en TLS v1.2 met de optie om alleen TLS v1.0 te selecteren.



Selecteer "Instellingen bewerken" om de configuratieopties weer te geven.

- TLS v1.1 en TLS v1.2 worden ingeschakeld met actieve selectievakjes om de andere protocollen te selecteren.
- ? naast elke TLS v1.3 is een herhaling van de statische opties voor het coderen.
- De "Overige TLS-clientservices:" presenteert nu de optie om TLS v1.0 alleen te gebruiken indien geselecteerd.



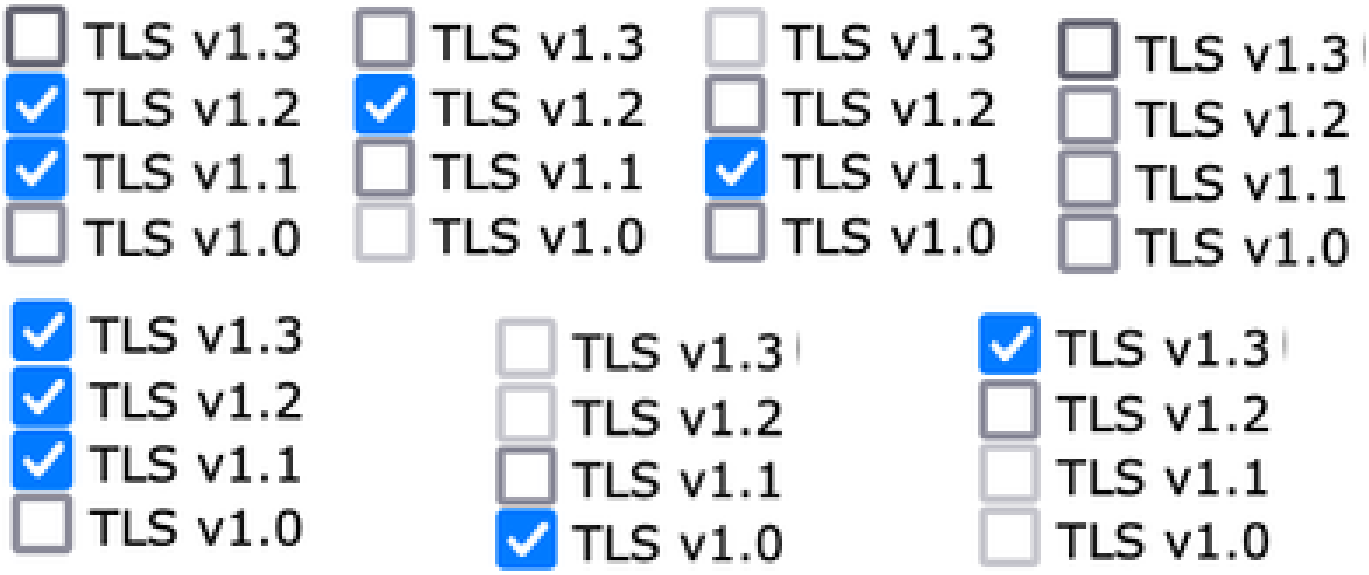
Note:
TLS protocols can be enabled only in sequence.
The configured SSL Cipher(s) do not apply to TLS 1.3. The TLS 1.3 protocol uses default ciphers.

De opties voor de selectie van TLS-protocollen omvatten TLS v1.0, TLS v1.1, TLS v1.2 en TLS v1.3.

- Na de upgrade naar AsyncOS 15.5 worden standaard alleen TLS v1.1- en TLS v1.2-protocollen geselecteerd.

Opmerking: TLS1.0 wordt standaard afgekeurd en uitgeschakeld. TLS v1.0 is nog steeds beschikbaar als de eigenaar ervoor kiest deze in te schakelen.

- De opties voor het aanvinkvakje worden weergegeven met vetgedrukte vakken waarin de beschikbare protocollen en de grijswaarden voor niet-compatibele opties worden weergegeven.
- De voorbeeldopties in de afbeelding illustreren de opties voor het selectievakje.



Verplaats de voorbeeldweergave van de geselecteerde TLS-protocollen.

SSL Configuration

GUI HTTPS:	Methods:	TLS v1.3 TLS v1.2
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!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:!DES:!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:!DES:!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

Edit Settings...

Opmerking: wijzigingen in het GUI HTTPS TLS-protocol veroorzaakt een korte verbreking van de verbinding met de WebUI als gevolg van het resetten van de https-service.

CLI-configuratie:

De SEG staat TLS v1.3 toe op drie diensten:

- GUI HTTPS
- Inkomende SMTP
- Uitgaande SMTP

Het uitvoeren van het bevel **>** sslconfig, output de momenteel gevormde Protocollen en de algoritmen voor GUI HTTPS, Inkomende SMTP, Uitgaande SMTP

- GUI HTTPS-methode: tlsv1_0tlsv1_1tlsv1_2tlsv1_3
- Inkomende SMTP-methode: tlsv1_0tlsv1_1tlsv1_2tlsv1_3
- Uitgaande SMTP-methode: tlsv1_1tlsv1_2tlsv1_3

Kies de bewerking die u wilt uitvoeren:

- GUI - GUI HTTPS-SSL-instellingen bewerken.
- INKOMEND - Bewerk de instellingen van inkomende SMTP ssl.
- UITGAAND - Bewerk uitgaande SMTP ssl-instellingen.

[]> inkomend

Voer de inkomende SSL-methode in die u wilt gebruiken.

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

[2-4]> 1-3

Opmerking: het SEG-selectieproces kan één menunummer omvatten, zoals 2, een menubereik van menunummers zoals 1-4 of menunummers gescheiden door komma's 1,2,3.

De volgende CLI slconfig-prompt accepteert de bestaande waarde door op ‘enter’ te drukken of de instelling naar wens aan te passen.

Voltooi de wijziging met de opdracht **>** commit **>>** Voer indien gewenst een optionele opmerking in **>** druk op "Enter" om de wijzigingen te voltooien.

Verifiëren

Deze sectie bevat een aantal basistestscenario's en fouten die kunnen optreden als gevolg van niet-overeenkomende TLS-protocolversies of syntaxisfouten.

Het logboekingang van de steekproef van een SEG uitgaande onderhandeling SMTP die een

verwerping toe te schrijven aan bestemming niet ondersteunde TLS v1.3 veroorzaakt:

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

Logboekregistratie van voorbeeldgegevens van een verzendende SEG die een met succes onderhandelde TLS v1.3 ontvangt:

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

Log voorbeeldinvoer van een ontvangende SEG zonder TLS v1.3 ingeschakeld.

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

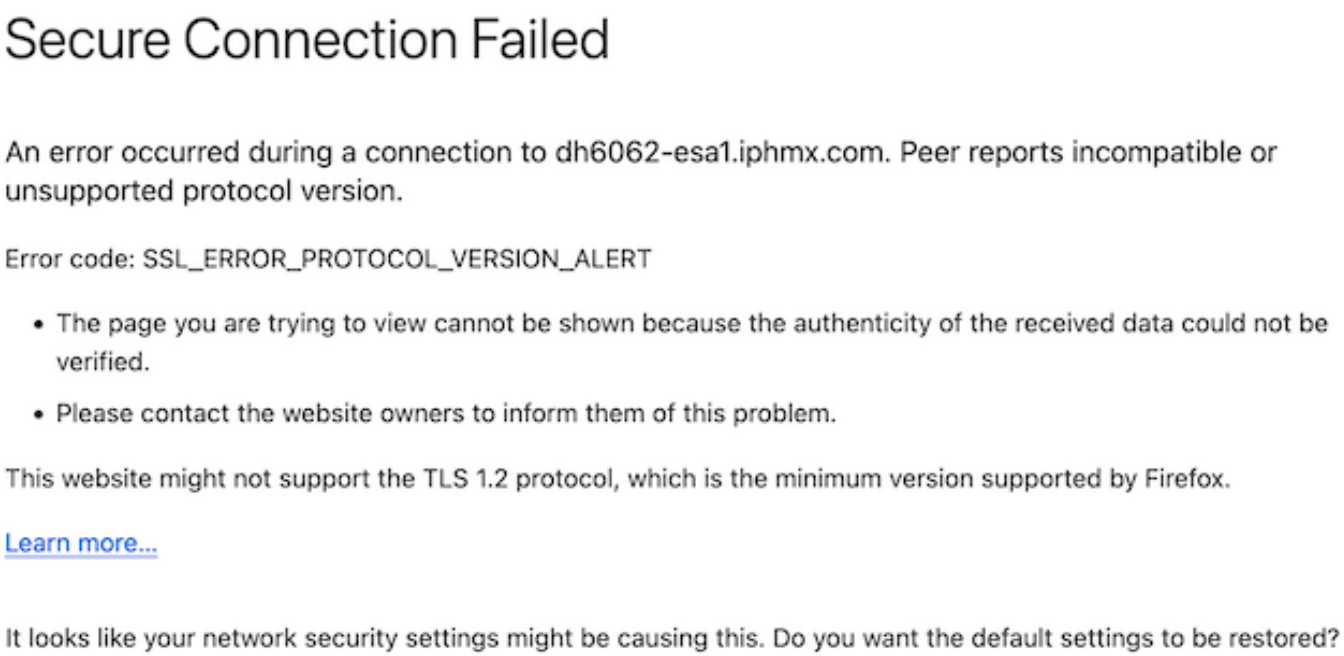
Door SEG ondersteunde TLS v1.3 ontvangen

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

Om de functionaliteit van uw browser te verifiëren, opent u eenvoudig een webbrowsersessie naar de SEG WebUI of NGUI die is geconfigureerd met TLSv1.3.

 Opmerking: alle webbrowsers die we hebben getest, zijn al geconfigureerd om TLS v1.3 te accepteren.

- Test: Configureer de browserinstelling in Firefox die TLS v1.3 ondersteunt en schakelt fouten uit op zowel de Classic UI als de NGUI van het apparaat.
- Classic UI met Firefox geconfigureerd om TLS v1.3 uit te sluiten als test.
- NGUI zou dezelfde fout ontvangen met als enige uitzondering het poortnummer 4431 (standaard) binnen de URL.



- Om de communicatie te verzekeren Controleer de instellingen van de browser om te verzekeren dat TLSv1.3 is opgenomen. (Deze steekproef is van Firefox en gebruikt aantallen 1-4

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

Gerelateerde informatie

- Cisco Secure Email Gateway - installatiegids
- Cisco Secure Email Gateway-startpagina voor ondersteuningshandleidingen
- Cisco Secure Email Gateway - Releaseopmerkingen

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.