Hoe TLS 1.2 op verschillende interfaces van CVP VXML Server inschakelen

Inhoud

Inleiding

Dit document beschrijft hoe u Cisco Customer Voice Portal (CVP) Call Server en Voice Extensible Markup Language (VXML) Server Transport Layer Security (TLS) ondersteuning voor HyperText Transfer Protocol (HTTP) kunt configureren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- CVP VXML-server
- Cisco Virtual Voice browser (CVVB)
- VXML-gateways

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

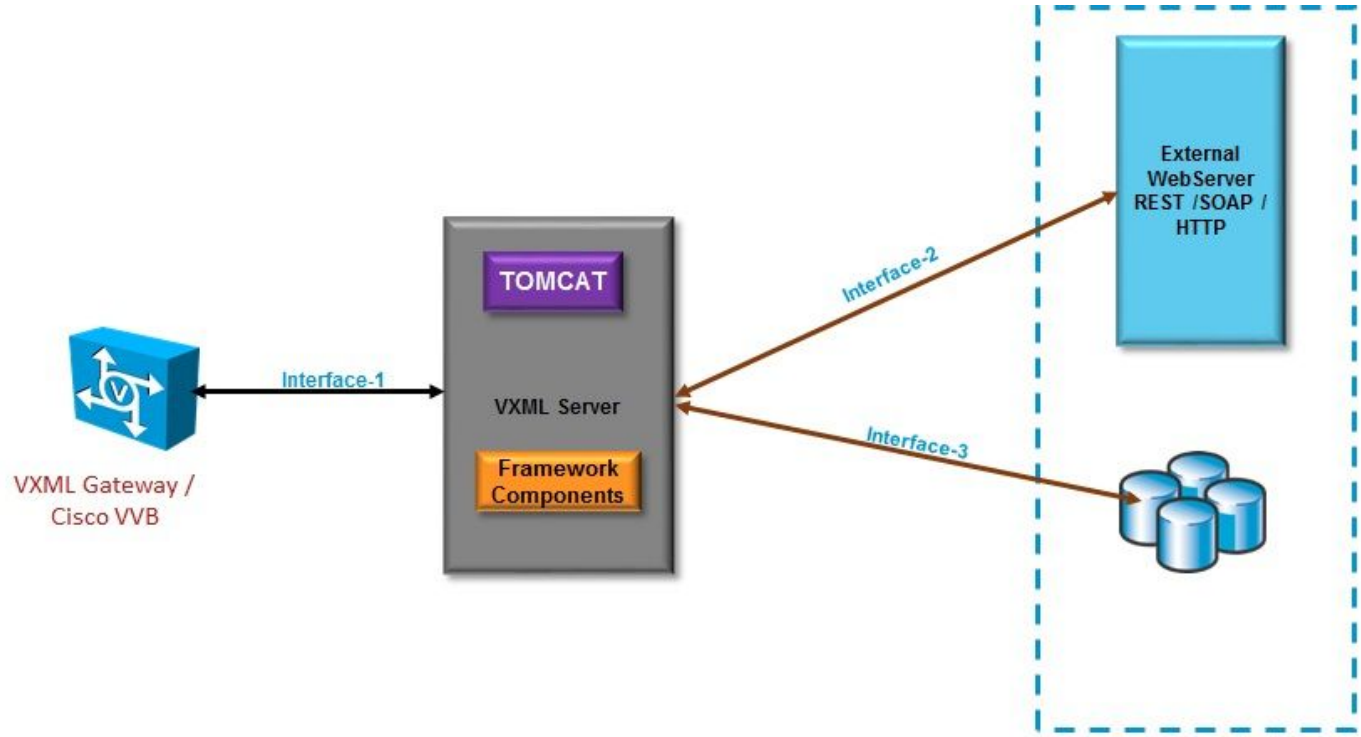
- CVP 11.5(1)
- CVVB 11.5(1)

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 levend is, zorg er dan voor dat u de

mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Op dit moment kan de VXML Server drie veilige interfaces met verschillende componenten hebben, zoals weergegeven in de afbeelding.



TLS-interface van VXML-server

Interface 1. Dit is de Hypertext Transfer Protocol (HTTP)-interface tussen VXML Gateway, Cisco Gevirtualiseerde Voice browser (CVVB) en VXML Server. Hier werkt de VXML-server als een server.

Interface 2. Dit is de typische HTTP-interface waar de VXML-server interageert met een externe webserver die HTTP/Simple Object Access Protocol (SOAP)-interface gebruikt. Deze interface is gedefinieerd als een deel van het aangepaste element of een WebService-element of een SOAP-element.

Interface 3. Dit is externe Database (DB) (Microsoft Structured Search Query Language (MSSQL) Server en ORACLE DB), die ingebouwde DB Element interface of aangepaste interface gebruikt.

In dit scenario, in Interface 1., werkt VXML Server als server, en in Interface 2. en 3., werkt VXML Server als veilige cliënten.

Probleem: Hoe TLS 1.2 op verschillende interfaces van CVP VXML Server inschakelen

CVP VXML Server communiceert met verschillende apparaten en servers met behulp van verschillende interfaces. TLS 1.2 moet op alle systemen worden ingeschakeld om het gewenste veiligheidsniveau te bereiken.

Oplossing

Procedure om TLS 1.2 in interface 1 in te schakelen

In deze interface, zoals eerder beschreven, werkt CVP VXML Server als een server. Deze veilige implementatie wordt uitgevoerd door Tomcat. Deze configuratie wordt gecontroleerd door de **server.xml** in Tomcat.

Configuratie typische connector:

```
<Connector SSLCertificateFile="C:\Cisco\CVP\conf\security\vxml.crt"
SSLCertificateKeyFile="C:\Cisco\CVP\conf\security\vxml.key" SSLEnabled="true" acceptCount="1500"
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_W
ITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256"
clientAuth="false" disableUploadTimeout="true" enableLookups="false" executor="tomcatThreadPool"
keyAlias="vxml_certificate"
keystoreFile="C:\Cisco\CVP\conf\security\.keystore"
keystorePass="3WJ~RH0WjKgyq3CKl$x?7f0?JU*7R3}WW0jE,I*_RC8w2Lf" keystoreType="JCEKS"
maxHttpHeaderSize="8192" port="7443"
protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https" secure="true"
sslEnabledProtocols="TLSv1, TLSv1.1, TLSv1.2" sslProtocol="TLS"/>
```

Dit voorbeeld heeft TLS v1.2, zodat de parameters die moeten worden geconfigureerd (SSLEnabledProtocols en certificaat) de vereiste configuratie hebben om de ondersteuning van TLS 1.2 te hebben.

Gebruik java **keytool.exe** om TLS 1.2-certificaten te genereren. U vindt dit gereedschap in **Cisco\CVP\jre\bin\.**

Documentatie voor gereedschap

Procedure om TLS 1.2 in interface 2 in te schakelen

Dit is de meest gebruikte interface. Hier werkt de VXML Server op een client en moet de beveiligde communicatie naar een externe WebServer worden geopend.

Er zijn twee verschillende manieren om dit aan te pakken.

- Gebruik aangepaste code.
- Gebruik het CVP-kader.

Hierin wordt het gebruik van CVP-framework beschreven.

Vanaf 11.6 is deze standaard ingeschakeld. Bij eerdere versies wordt deze tabel gecontroleerd:

CVP Version	ES release	JAVA Version	Support
9.0	NA	JRE 1.6	Upgrade JAVA to 111 and above for 1.2 support and customer has to implement custom java code to handle TLS1.2 (Refer to the example)
10.0	NA	JRE 1.6	Customer has to implement TLS 1.2 in Customer code (Refer to the example).Upgrade to JRE111 or upgrade to 1.7.
10.5	ES-26	JAVA 1.7 32 bit	JAVA In built support for TLS1.2, no update of JAVA required
11.0	ES-23	JAVA 1.7 32 Bit	JAVA In built support for TLS1.2, no update of JAVA required
11.5	ES-12	JAVA 1.7 64 Bit	JAVA In built support for TLS1.2, no update of JAVA required
11.6	NA	JRE 1.7 64 bit	

Als er een ES release is geïnstalleerd die door dit defect wordt beïnvloed: CSCvc39129 VXML Server als TLS-client, moet u deze handmatige configuratie toepassen:

Stap 1. Open de registereditor en navigeer naar **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\VXMLServer\Parameters\Java**.

Stap 2. Open de **toets Opties** en voeg **Dhttps.client.protocol=TLSv1.2** aan het eind toe.

Stap 3. Start Cisco CVP-service voor VXServer opnieuw.

Hier is de snelle lijst van standaard protocolondersteuning in verschillende JAVA versies.

	JDK 8 (March 2014 to present)	JDK 7 (July 2011 to present)	JDK 6 (2006 to end of public updates 2013)
TLS Protocols	TLSv1.2 (default) TLSv1.1 TLSv1 SSLv3	TLSv1.2 TLSv1.1 TLSv1 (default) SSLv3	TLS v1.1, TLS v1.2 (JDK 6 update 111 and above) TLSv1 (default) SSLv3

```
-Djdk.tls.client.protocols=TLSv1.2.
```

Deze configuratie machtigt de VXML Server om TLS 1.2 in Java SE Development Kit (JDK) 7 en JDK6 te gebruiken.

> **Opmerking**: SSL is standaard uitgeschakeld.

Procedure om TLS 1.2 in interface 3 in te schakelen

In deze interface, zoals eerder beschreven, werkt CVP VXML Server als een client en een derdendatabank server die als server fungeert.

Zorg ervoor dat de database server van derden TLS 1.2 ondersteunt en TLS 1.2 is ingeschakeld.

Bijvoorbeeld, als u SQL server 2014 met Service Pack (SP) 2 gebruikt, steunt het TLS 1.2 en bevestig dat TLS 1.2 protocol is ingeschakeld onder het register zoals hier op een SQL-server vermeld:

SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

Zo kan TLS 1.2 voor interface 3 aan CVP-zijde worden ingeschakeld:

Stap 1. Open de registereditor en navigeer naar **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\VXMLServer\Parameters\Java**.

Stap 2. Open de **sleutel** van **Opties** en voeg **-Djdk.tls.client.protocols=TLSv1.2** aan het eind toe.

Stap 3. Start Cisco CVP-service voor VXServer opnieuw.

> Opmerking: Controleer dit bug voor meer details: CSCvg20831 JNDI Database verbinding mislukt bij CVP11.6 SQL 2014SP2.

Ondersteuning van procedure voor upgrade JRE voor TLS 1.2

CVP Ondersteunt de upgrade Java Runtime Environment (JRE) tot de nieuwste versie voor defecten van bug.

In deze tabel worden JAVA-versies weergegeven.

CVP Version	JRE	TOMCAT
9.0	java version "1.6.0_67" 32 –Bit Server	Apache Tomcat/6.0
10.0	java version "1.6.0_67" 32 –Bit Server	Apache Tomcat/7.0
10.5	java version "1.7.0_45" 32 –Bit Server	Apache Tomcat/7.0
11.0	java version "1.7.0_67" 32 –Bit Server	Apache Tomcat/7.0
11.5	java version "1.7.0_67" 64 –Bit Server	Apache Tomcat/8.0
11.6	java version "1.8.0_67" 64 –Bit Server	Apache Tomcat/8.0

JAVA-versies

Volg de procedure die in deze link is beschreven.

> **Voorzichtig:** upgrade van 32-bits naar 64-bits en omgekeerd wordt niet ondersteund

Procedure voor upgrade van de computer

Tomcat Minor upgrade wordt ondersteund. Zorg er echter voor dat u de compatibiliteitsproblemen tussen Aangepaste Jars (AXIS, JDBC enzovoort) controleert voordat u de upgrade uitvoert.

Kijk hier voor meer informatie naar de procedure.