Aktivierung von TLS 1.2 auf verschiedenen Schnittstellen des CVP VXML-Servers

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Unterstützung von Cisco Customer Voice Portal (CVP) Call Server und Voice Extensible Markup Language (VXML) Server Transport Layer Security (TLS) für HyperText Transfer Protocol (HTTP) konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- CVP VXML-Server
- Cisco Virtual Voice Browser (CVVB)
- VXML-Gateways

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

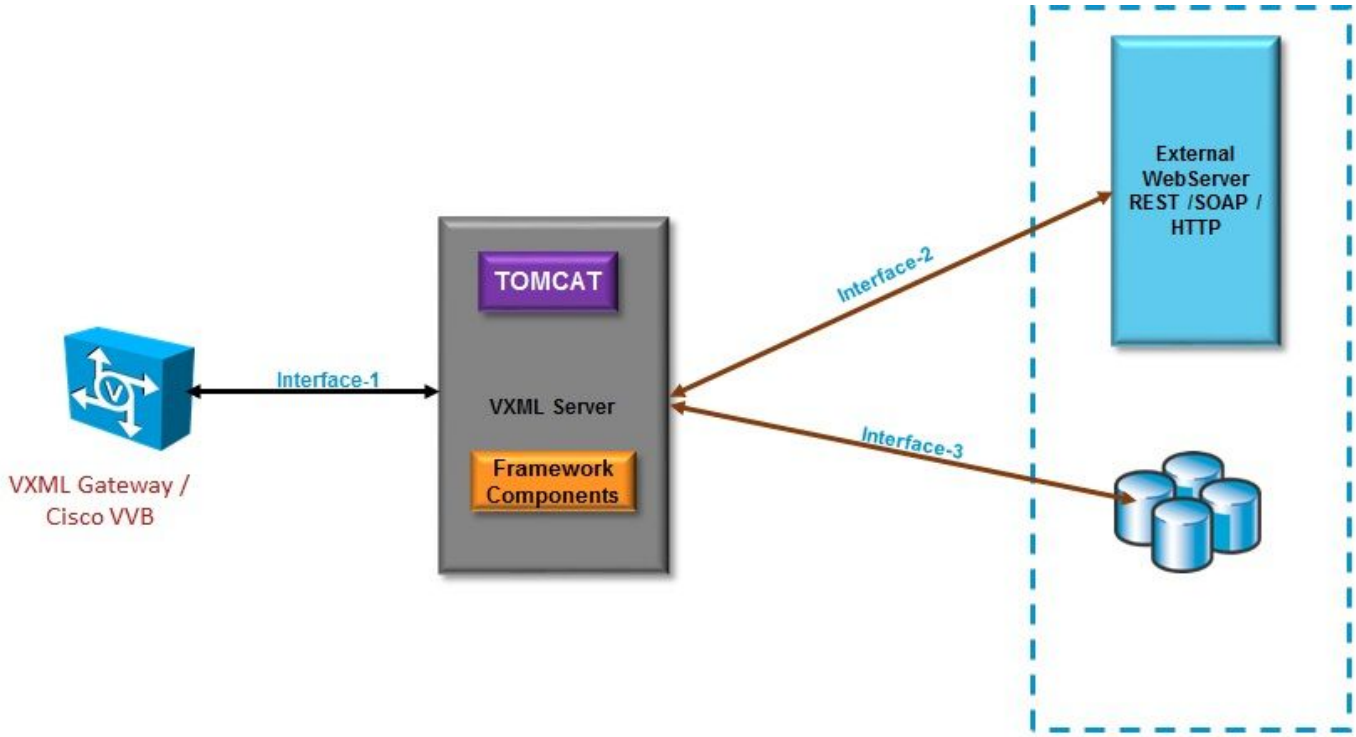
- CVP 11,5(1)
- CVVB 11.5(1)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie

die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Derzeit kann der VXML-Server drei sichere Schnittstellen mit verschiedenen Komponenten aufweisen, wie im Bild gezeigt.



TLS-Schnittstelle des VXML-Servers

Schnittstelle 1. Dies ist die HTTP-Schnittstelle (Hypertext Transfer Protocol) zwischen dem VXML-Gateway, dem Cisco Virtualized Voice Browser (CVVB) und dem VXML-Server. Hier fungiert der VXML-Server als Server.

Schnittstelle 2. Dies ist die typische HTTP-Schnittstelle, bei der der VXML-Server mit einem externen Webserver interagiert, der die SOAP-Schnittstelle (HTTP/Simple Object Access Protocol) verwendet. Diese Schnittstelle wird als Teil des benutzerdefinierten Elements, des WebService-Elements oder des SOAP-Elements definiert.

Schnittstelle 3. Dies ist eine externe Datenbank (DB) (Microsoft Structured Query Language (MSSQL) Server und ORACLE DB), die eine integrierte DB-Element-Schnittstelle oder eine benutzerdefinierte Elementschnittstelle verwendet.

In diesem Szenario agiert der VXML-Server in Schnittstelle 1 als Server und in Schnittstelle 2. und 3. fungiert der VXML-Server als sichere Clients.

Problem: Aktivierung von TLS 1.2 auf verschiedenen

Schnittstellen des CVP VXML-Servers

Der CVP VXML-Server kommuniziert mithilfe verschiedener Schnittstellen mit verschiedenen Geräten und Servern. TLS 1.2 muss auf allen Geräten aktiviert werden, um die gewünschte Sicherheitsstufe zu erreichen.

Lösung

Verfahren zur Aktivierung von TLS 1.2 in Schnittstelle 1

In dieser Schnittstelle fungiert der CVP VXML-Server wie bereits beschrieben als Server. Diese sichere Implementierung erfolgt durch Tomcat. Diese Konfiguration wird von **server.xml** in Tomcat gesteuert.

Typische Connector-Konfiguration:

```
<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"/>
```

In diesem Beispiel wird TLS v1.2 verwendet, sodass die zu konfigurierenden Parameter (sslEnabledProtocols und Certificate) die erforderliche Konfiguration aufweisen, um die Unterstützung von TLS 1.2 zu erhalten.

Verwenden Sie java **keytool.exe**, um TLS 1.2-Zertifikate zu generieren. Dieses Tool finden Sie unter **Cisco\CVP\jre\bin\.**

Tastaturdokumentation

Verfahren zur Aktivierung von TLS 1.2 in Schnittstelle 2

Dies ist die am häufigsten verwendete Schnittstelle. Hier agiert der VXML-Server als Client und muss eine sichere Kommunikation mit einem externen Web-Server öffnen.

Es gibt zwei verschiedene Möglichkeiten, damit umzugehen.

- Benutzerdefinierten Code verwenden.
- CVP-Framework verwenden

Dies beschreibt die Verwendung des CVP-Frameworks.

Ab 11.6 ist es standardmäßig aktiviert. Überprüfen Sie für vorherige Versionen die folgende Tabelle:

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	

Wenn eine von diesem Fehler betroffene ES-Version installiert ist: CSCvc39129 VXML-Server als TLS-Client, müssen Sie diese manuelle Konfiguration anwenden:

Schritt 1: Öffnen Sie den Registrierungs-Editor, und navigieren Sie zu **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\VXMLServer\Parameters\Java**.

Schritt 2: Öffnen Sie **den Optionsschlüssel**, und fügen Sie am Ende **Dhttps.client.protocol=TLSv1.2 hinzu**.

Schritt 3: Starten Sie den Cisco CVP VXMLServer-Dienst neu.

Hier finden Sie eine kurze Liste mit Standardprotokollunterstützung in verschiedenen JAVA-Versionen.

	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.
```

Für diese Konfiguration muss der VXML-Server das TLS 1.2 im Java SE Development Kit (JDK) 7 und JDK6 verwenden.

Hinweis: SSL ist standardmäßig deaktiviert.

Verfahren zur Aktivierung von TLS 1.2 in Schnittstelle 3

In dieser Schnittstelle agiert der CVP VXML-Server, wie bereits beschrieben, als Client und als Datenbankserver eines Drittanbieters, der als Server fungiert.

Stellen Sie sicher, dass der Datenbankserver eines Drittanbieters TLS 1.2 und TLS 1.2 unterstützt.

Wenn Sie z. B. SQL Server 2014 mit Service Pack (SP) 2 verwenden, wird TLS 1.2 unterstützt, und bestätigen Sie, dass Das TLS 1.2-Protokoll ist unter der Registrierung aktiviert, wie hier auf dem SQL-Server erwähnt:

SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

So aktivieren Sie TLS 1.2 für die Schnittstelle 3 auf der CVP-Seite:

Schritt 1: Öffnen Sie den Registrierungs-Editor, und navigieren Sie zu **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\VXMLServer\Parameters\Java**.

Schritt 2: Öffnen Sie **den Optionsschlüssel**, und fügen Sie **Djdk.tls.client.logs=TLSv1.2** am Ende hinzu.

Schritt 3: Starten Sie den Cisco CVP VXMLServer-Dienst neu.

> **Hinweis**: Lesen Sie diesen Fehler für weitere Informationen: CSCvg20831 JNDI-Datenbankverbindung schlägt mit CVP11.6 SQL 2014SP2 fehl.

Verfahren zum Upgrade von JRE für TLS 1.2-Unterstützung

CVP unterstützt das Upgrade von Java Runtime Environment (JRE) auf die neueste Version für Bug-Defekte.

Diese Tabelle zeigt die JAVA-Versionen.

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-Versionen

Befolgen Sie die in diesem Link beschriebenen Schritte.

> **Vorsicht**: Upgrade von 32 Bit auf 64 Bit und umgekehrt wird nicht unterstützt

Verfahren zum Upgrade von Tomcat

Tomcat Minor Upgrade wird unterstützt. Stellen Sie jedoch sicher, dass Sie die Kompatibilitätsprobleme zwischen Custom Jars (AXIS, JDBC usw.) überprüfen, bevor Sie das Upgrade durchführen.

Weitere Informationen finden Sie hier.