如何在CVP VXML服务器的不同接口上启用TLS 1.2

目录

简介

本文档介绍如何配置思科客户语音门户(CVP)呼叫服务器和语音可扩展标记语言(VXML)服务器传输层安全(TLS)支持超文本传输协议(HTTP)。

先决条件

要求

Cisco 建议您了解以下主题：

- CVP VXML服务器
- 思科虚拟语音浏览器(CVVB)
- VXML网关

使用的组件

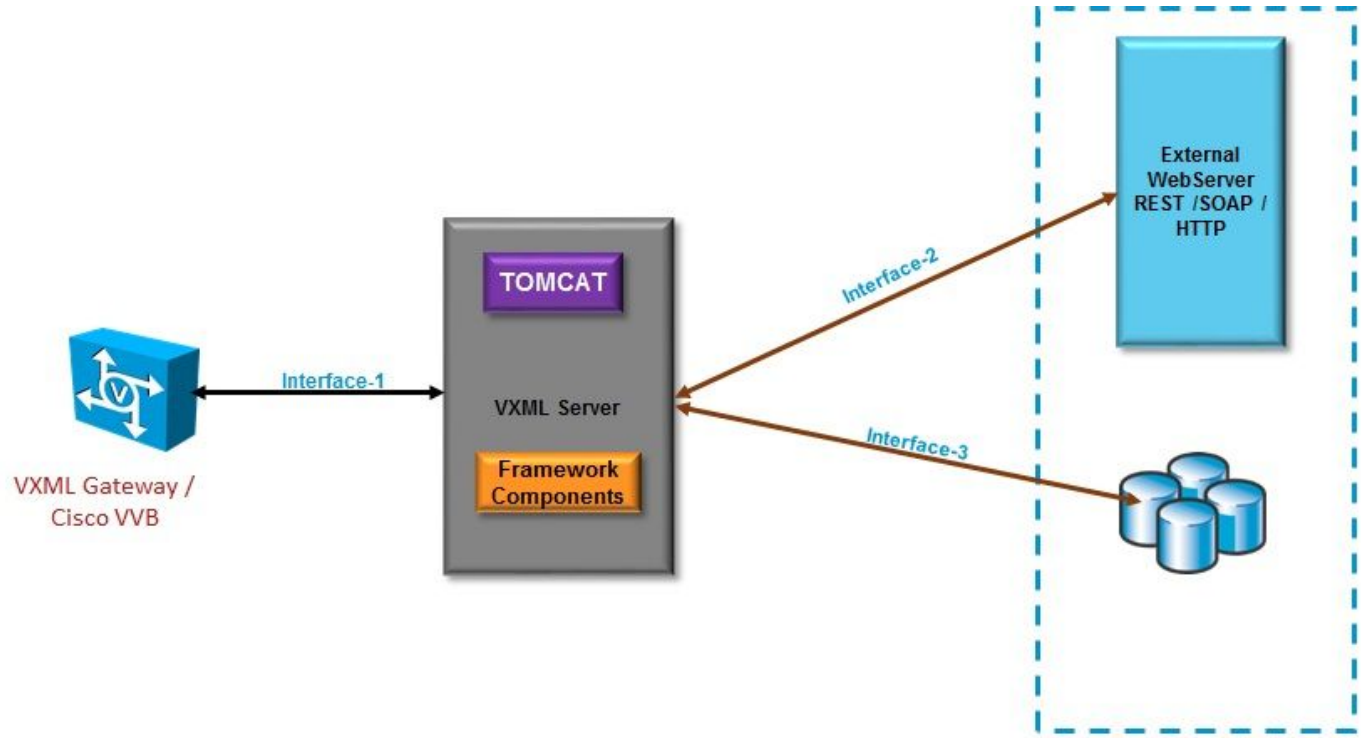
本文档中的信息基于以下软件版本：

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

目前，VXML服务器可以有三个具有不同组件的安全接口，如图所示。



VXML服务器的TLS接口

接口1.这是VXML网关、思科虚拟化语音浏览器(CVVB)和VXML服务器之间的超文本传输协议(HTTP)接口。此处VXML服务器用作服务器。

接口2。这是VXML服务器与使用HTTP/简单对象访问协议(SOAP)接口的外部Web服务器交互的典型HTTP接口。此接口定义为自定义元素、WebService元素或SOAP元素的一部分。

接口3。这是使用内置DB元素接口或自定义元素接口的外部数据库(DB)(Microsoft Structured Query Language(MSSQL)Server和ORACLE DB)。

在此方案中，在接口1.中，VXML服务器充当服务器，在接口2.和3.中，VXML服务器充当安全客户端。

问题：如何在CVP VXML服务器的不同接口上启用TLS 1.2

CVP VXML服务器通过不同的接口与各种设备和服务器通信。必须在所有TLS 1.2上启用，才能达到所需的安全级别。

解决方案

在接口1中启用TLS 1.2的步骤

如前所述，在此接口中，CVP VXML服务器充当服务器。此安全实现由Tomcat完成。此配置由

Tomcat中**的server.xml**控制。

典型连接器配置：

```
<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"/>
```

此示例具有TLS v1.2，因此需要配置的参数(sslEnabledProtocols和证书)具有支持TLS 1.2所需的配置。

使用java **keytool.exe** 以生成TLS 1.2证书。此工具可在Cisco\CVP\jre\bin\中**找到。**

Keytool文档

在接口2中启用TLS 1.2的步骤

这是最常用的接口。此处，VXML服务器充当客户端，需要打开与外部WebServer的安全通信。

有两种不同的方法来处理此问题。

- 使用自定义代码。
- 使用CVP框架。

本章介绍CVP框架的使用。

从11.6开始，默认启用该功能，对于以前的版本，请检查下表：

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	

如果安装了受此缺陷影响的ES版本：CSCvc39129 VXML服务器作为TLS客户端,则需要应用此手动配置：

步骤1.打开注册表编辑器并导航至**HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\VXMLServer\Parameters\Java。**

步骤2.打**开选项**密钥，**并在末尾添加 — Dhttps.client.protocol=**TLSv1.2。

步骤3.重新启动Cisco CVP VXMLServer服务。

以下是不同JAVA版本中默认协议支持的快速列表。

	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.
```

此配置要求VXML服务器在Java SE开发工具包(JDK)7和JDK6中使用TLS 1.2。

> **注意**：默认情况下禁用SSL。

在接口3中启用TLS 1.2的过程

CVP VXML

TLS 1.2TLS 1.2

SQL server 2014Service Pack(SP)2TLS 1.2 TLS 1.2SQL Server

SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

CVP3TLS 1.2

1.**HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\VXMLServer\Parameters\Java**

2. **— Djdk.tls.client.protocols=TLSv1**.2

3.Cisco CVP VXMLServer

> **注意**：有关详细信息，请检查此Bug:CSCvg20831 JNDI数据库连接与CVP11.6 SQL 2014SP2失败。

升级TLS 1.2支持的JRE的过程

CVP支持将Java Runtime Environment(JRE)升级到最新版本，以解决漏洞缺陷。

此表显示JAVA版本。

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版本

按照此链接中描述的步骤操作。

警告：不支持从32位升级到64位，反之亦然

升级Tomcat的步骤

支持Tomcat Minor升级。但是，请确保在执行升级之前检查自定义Jar（AXIS、JDBC等）之间的兼容性问题。

有关详细信息，请参阅此处的步骤。