# Como permitir TLS 1.2 em relações diferentes do server CVP VXML

## Índice



## Introdução

Este documento descreve como configurar o server portal do atendimento da Voz de cliente Cisco (CVP) e exprimir o apoio do Transport Layer Security do server do linguagem de marcação extensível (VXML) (TLS) para o Hypertext Transfer Protocol (HTTP).

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Server CVP VXML
- Navegador de voz virtual de Cisco (CVVB)
- Gateways VXML

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

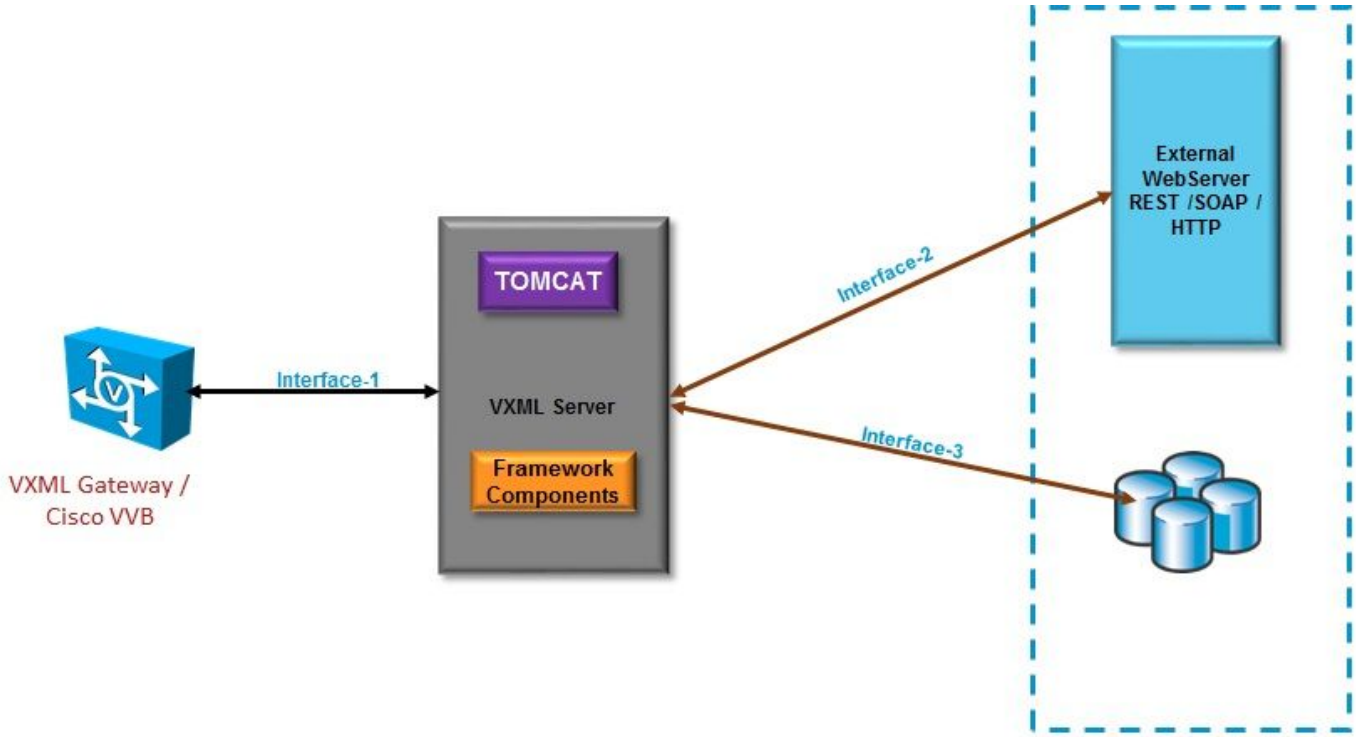
- CVP 11.5(1)
- CVVB 11.5(1)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

# Informações de Apoio

Presentemente, o server VXML pode ter três interfaces seguras com os componentes diferentes, segundo as indicações da imagem.




## Relação TLS do server VXML

Relação 1. Esta é a relação do Hypertext Transfer Protocol (HTTP) entre o gateway VXML, Cisco virtualizou o navegador de voz (CVVB) e o server VXML. Aqui o server VXML atua como um server.

Relação 2. Esta é a relação típica HTTP onde o server VXML interage com um servidor de Web externo que use a relação do protocolo de acesso do objeto HTTP/Simple (SABÃO). Esta relação é definida como parte do elemento feito sob encomenda ou elemento de WebService ou elemento do SABÃO.

Relação 3. Este é o base de dados externo (DB) (server da língua de consulta estruturada de Microsoft (MSSQL) e ORACLE DB), esse usa a relação incorporado do elemento DB ou a relação do elemento feito sob encomenda.

Nesta encenação, na relação 1., o server VXML atua como um server, e na relação 2. e 3., o server VXML atua como clientes seguros.

# Problema: Como permitir TLS 1.2 em relações diferentes do

# server CVP VXML

O server CVP VXML comunica-se aos vários dispositivos e server com a ajuda de relações diferentes. O TLS 1.2 tem que ser permitido em todo de conseguir o nível de segurança desejado.

# Solução

## Procedimento para permitir TLS 1.2 na relação 1

Nesta relação, como descrita mais cedo, o server CVP VXML atua como um server. Esta aplicação segura é feita por Tomcat. Esta configuração é controlada pelo **server.xml em** Tomcat.

Configuração típica do conector:

```
<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"/>
```

Este exemplo tem o v1.2 TLS, assim que os parâmetros necessários ser configurado (sslEnabledProtocols e certificado) têm a configuração requerida para ter o apoio de TLS 1.2.

Use as Javas **keytool.exe a fim** gerar Certificados TLS 1.2. **Esta ferramenta pode ser encontrada em Cisco \ CVP \ jre \ escaninho \.**

Documentação de Keytool

## Procedimento para permitir TLS 1.2 na relação 2

Esta é a relação a mais comum usada. Aqui o server VXML atua um cliente e precisa de abrir uma comunicação segura a um web server externo.

Há duas maneiras diferentes de segurar isto.

- Use o código feito sob encomenda.
- Use a estrutura CVP.

Isto descreve o uso da estrutura CVP.

De 11.6 é permitido à revelia, porque as versões anterior verificam esta tabela:

| 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 | |

Se você tem uma liberação ES instalada que esteja afetada por este defeito: Server CSCvc39129 VXML como o cliente TLS, você precisa de aplicar esta configuração manual:

Etapa 1. Abra o editor de registro e navegue à **fundação do software HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache \ Procrun 2.0\VXMLServer\Parameters\Java**.

Etapa 2. Abrem a **chave das opções** e adicionar-la **- Dhttps.client.protocol=TLSv1.2 na** extremidade.

Etapa 3. Serviço de Cisco CVP VXMLServer do reinício.

Está aqui a lista rápida de suporte de protocolo do padrão em versões de JAVA diferentes.

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

```
<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"/>
```

Esta configuração encarrega do uso do server VXML o TLS 1.2 no jogo do desenvolvimento das Javas SE (JDK) 7 e JDK6.

Nota: O SSL é desabilitado à revelia.

## Procedimento para permitir TLS 1.2 na relação 3

Nesta relação, como descrita mais cedo, o server CVP VXML atua como um cliente e um servidor de base de dados da terceira parte que atue como o server.

Assegure-se de que o servidor de base de dados da terceira parte apoie TLS 1.2 e o TLS 1.2 esteja permitido nele.

Exemplo, se você usa o servidor SQL 2014 com pacote de serviços (SP) 2, apoia TLS 1.2 e confirma que o protocolo TLS 1.2 está permitido sob o registro como mencionado aqui no servidor SQL:

**SISTEMA \ CurrentControlSet \ controle \ SecurityProviders \ SCHANNEL \ protocolos**

A fim permitir TLS 1.2 para a relação 3 no lado CVP:

Etapa 1. Abra o editor de registro e navegue à **fundação do software HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache \ Procrun 2.0\VXMLServer\Parameters\Java**.

Etapa 2. Abrem a **chave das opções** e adicionar-la **- Djdk.tls.client.protocols=TLSv1.2 na** extremidade.

Etapa 3. Serviço de Cisco CVP VXMLServer do reinício.

> Nota: Verifique este erro para ver se há mais detalhe: A Conexão ao base de dados CSCvg20831 JNDI falha com CVP11.6 SQL 2014SP2.

## Procedimento para promover o JRE para o apoio TLS 1.2

O CVP apoia o ambiente de tempo de execução de java (JRE) da elevação à versão a mais atrasada para defeitos do erro.

Esta tabela mostra versões de JAVA.

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

Versões de JAVA

Siga o procedimento descrito neste link.

Cuidado: A elevação do bit 32 a 64 mordido e vice-versa não é apoiada

## Procedimento para promover Tomcat

A elevação menor de Tomcat é apoiada. Contudo, assegure-se de que você checkc as edições compatibilty entre os frascos feitos sob encomenda (AXIS, JDBC etc…) antes que você execute a elevação.

Verifique para mais detalhes o procedimento aqui.