配置CVP和IOS设备之间的安全通信

Contents

Introduction

本文描述进程配置思科统一客户语音门户(CVP)服务器和Cisco互联网操作系统(IOS)设备之间的安全通信。

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.如果您的网络实际，请保证您了解所有命令的潜在影响。

Configure

为了配置CVP服务器与Cisco IOS设备安全地联络类似入口网关和语音扩展标记语言(VXML)网关，您必须完成也是在CVP安全指南的参考的这些步骤

步骤1.使用.security keystore和文件夹备份位于**%CVP_HOME% \ conf。**

步骤2.导入根、中间和Intermediate2 (若有)证书在证书存储。

步骤3.导入CA签署了呼叫服务器和VXML证书。

步骤4.重命名呼叫服务器和VXML .pem文件对callserver.crt和VXML.crt文件。

步骤5.重新启动呼叫服务器和VXML服务。

步骤6.访问呼叫服务器和VXML服务器证明。 他们必须反射当前认证日期。

https://ip_address_of_callserver:8443

https://ip_address_of_vxmlserver:7443

为了进一步配置在Cisco网关和呼叫服务器和VXML服务器之间的HTTPS到HTTPS的网关，请导入呼叫服务器证明和\或在IOS网关的VXML服务器证明。

步骤1.送进**https://ip_address_of_callserver:8443**在Web浏览器的地址栏访问安全的呼叫服务器证明或**https://ip_address_of_vxmlserver:7443**访问安全的VXML服务器证明。安全性预警对话框出现。

步骤2.点击**查看证书**。

步骤3.选择**Details选项**。

步骤4.点击**"Copy"对文件**。认证Export向导对话出现。

步骤5.选择**Base-64编码的X.509 (.CER)**，**其次**然后点击。

步骤6.指定文件名在**文件到Export对话框**，**其次**然后点击。

步骤7.**点击完成**。消息表明导出是成功的。

步骤8.**点击OK键**，并且关闭安全性预警对话框。

步骤9.打开在出现在之间的Notepad的被导出的文件并且复制CVP服务器证书信息---开始认证--并且--END认证--标记。这在程序以后使用。

步骤10.访问在IOS网关的全局配置模式。

步骤11.创建并且登记trustpoints由这些命令：

```
crypto pki trustpoint xxxx
  en terminal
  revocation-check none
  exit
```

那里xxxx是信任点名字。

例如：

crypto pki trustpoint ROOT

登记终端

撤销检查无

crypto pki trustpoint中间

登记终端

撤销检查无

crypto pki trustpoint INTERMEDIATE2

登记终端

撤销检查无

crypto pki trustpoint cvpcallservernew

登记终端

撤销检查无

crypto pki trustpoint cvpvxmlnew

登记终端

撤销检查无

步骤12。在IOS网关的进口证明书签名

从第9步和开放Certificate Authority (CA)证书获得certifiate签名为了获得他们的认证签名和导入在IOS。

返回到在IOS网关的privileged EXEC模式。

1. 输入xxxx是在上一步的信任点指定的名称的**crypto pki auth <xxxx>**。(所有信任点)
2. 粘贴从Notepad剪贴板的认证。(仅内容)
3. 进入离开。

运行这些命令：

```
crypto pki auth ROOT

crypto pki auth INTERMEDIATE

crypto pki auth INTERMEDIATE2

crypto pki auth cvpcallservernew

crypto pki auth cvpvxmlnew
```

信息显示，描述认证属性和确认提示出现。

是进入，并且您能看到表明的消息成功导入认证

Verify

您能做测试通话和运行这些调试验证握手和测试configuraton。

debug crypto pki transactions

debug crypto pki messages

Troubleshoot

目前没有针对此配置的故障排除信息。

Related Information

- CVP安全指南
- Technical Support & Documentation - Cisco Systems