ASA与使用的无客户端访问在移动设备配置示例的Citrix接收方

目录

简介

本文描述如何配置思科可适应安全工具(ASA)作为Citrix接收方的一个代理在移动设备。 此功能为在移动设备运行到XenApp/XenDesktop虚拟桌面基础设施的Citrix接收方应用程序提供安全远程访问(VDI)服务器通过ASA，排除对Citrix接入网关的需要。

先决条件

要求

Cisco 建议您了解以下主题：

- Citrix接收方
- 无客户端WebVPN

基础设施需求：

- ASA必须有由移动设备委托的一有效身份证书。
- 在Citrix XenApp/XenDesktop/Storefront服务器必须启用和配置XML接口。

使用的组件

本文档不限于特定的软件和硬件版本。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

支持的移动设备

这是支持的移动设备的列表：

- iPad - Citrix接收方版本4.x或以上
- IP电话/iTouch - Citrix接收方版本4.x或以上
- 机器人2.x电话- Citrix接收方版本2.x或以上
- 机器人3.x片剂- Citrix接收方版本2.x或以上
- 机器人4.0/4.1电话/片剂- Citrix接收方版本2.x或以上

演示

为了看到此进程的演示，请访问以下网页：

思科ASA 9.0 Citrix移动接收方代理演示

背景信息

Citrix接入网关(CAG)传统上是提供安全远程访问虚拟化Citrix资源的唯一方法(桌面和应用程序)。在一典型的部署，这样设备在防火墙后将查找在非敏感区域(DMZ)。此功能添加ASA功能为了支持对虚拟资源的安全远程连接从移动设备。

传统部署要求CAG的出现，在防火墙后典型地查找：

使用ASA，对内部Citrix资源的连接是可能的没有CAG ：

为了的ASA能对从Citrix接收方的代理连接到Citrix服务器， ASA扮演Citrix访问。

网关：

1. 当您设法连接到Citrix虚拟化的资源时，是否不需要提供Citrix服务器？s地址/凭证;反而您输入ASA的安全套接字协议层(SSL) VPN IP地址和凭证。

2. 一个新的ASA处理程序创建为了处理请求，包括从Citrix接收方(与识别作为Citrix接收方)的代理程序字符串的HTTPS请求的认证请求。

3. 在ASA验证凭证后，接收方客户端开始通过ASA获取标题名为的应用程序。ASA重写和代理XenApp或XenDesktop服务器的？s XML服务接口(XML服务是在Citrix服务器运行服务虚拟化资源涉及的请求)的服务。

4. ASA连接并且验证到有预先配置的凭证的VDI服务器(请参阅配置部分)。当您发送凭证到后端XenApp/XenDesktop服务器时， ASA总是弄暗淡与Citrix CTX1编码的用户密码。

这是支持的ASA认证方法列表用Citrix接收方：

- 本地
- 域
- RSA SecurID使用SDI本地协议。
  也ASA支持挑战模式，包括下标记、New PIN和已到期PIN模式。
- 两个因素的验证(RSA和轻量级目录访问协议(LDAP))

限制

- 证书限制：
  因为这些认证形式在中部，不允许ASA证书/智能卡验证不支持作为自动登录方法。

  在证书的Md5签名不工作由于安全问题并且是在IOS平台的一问题。更多信息可以在iOS Error:的接收方找到连接错误。Citrix接收方不可能建立与远程主机讨论的连接。

  如果主题名称不充分地匹配ASA完全合格的域名(FQDN)，即使ASA身份证书包含附属的代替名称(SAN)，独立计算架构(ICA)会话不会开始(基于版本，验证错误可能显示)。此问题由Cisco Bug ID CSCuj23632修复。

- Citrix接收方访客接入仅一个XenApp/XenDesktop服务器每次。结果，对一个XenApp/XenDesktop的ASA代理请求每VPN会话也。当Citrix接收方客户端连接时， ASA选择配置的第一个XenApp/XenDesktop。

- HTTP重定向，因为Citrix接收方应用程序当前版本不与重定向一起使用，不支持。

- 在CSD (不仅安全穹顶)不支持客户端证书验证、密码到期通知， Cisco Secure Desktop (CSD)和一切，当使用时独立/移动客户端，因为独立/移动虚拟化基础设施客户端不了解这些概念。

配置

注意：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

CLI命令

当您使用Citrix接收方移动客户端为了登录到ASA时， ASA必须连接它到预定义的Citrix XenApp或XenDesktop服务器。为了完成此，管理员配置Citrix服务器？s地址和登录凭证在组策略或用户名下。万一用户名和组政策CLI配置，用户名设置优先于组政策。

```
configure terminal
group-policy DfltGrpPolicy attributes
webvpn
[no] vdi { none | type <vdi_type>url <url> domain <domain> username
<username> password <password>}
```

```
configure terminal
username <username> attributes
webvpn
[no] vdi { none | type <vdi_type>url <url> domain <domain> username
<username> password <password>}
```

注意：
类型- VDI的类型。对于Citrix接收方，类型必须是**citrix**。
URL - XenApp或XenDesktop服务器的全双工URL，包括HTTP或HTTPS、主机名、端口号，以及路径对XML服务。主机名和XML服务路径能包含无客户端宏。如果没有提供XML服务路径，使用**/Citrix/pnagent/**默认路径。
使用为了登录虚拟化基础设施服务器的**用户名用户名**。这可以是无客户端宏。
使用为了登录虚拟化基础设施服务器的**password password**。这可以是无客户端宏。
域-使用为了登录虚拟化基础设施服务器的域。这可以是无客户端宏。

注意：XenAPP服务器通常配置为了听波尔特80，因此应该配置VDI与**HTTP**而不是**HTTPS**。

当他们验证与ASA时， Citrix移动接收方用户能选择隧道组。隧道组基群段允许另外身份验证协议和XenApp/XenDekstop服务器支持VDI访问。管理员能配置隧道组，因为VDI访问的，默认。此配置的隧道组，当用户不做隧道组基群段时，使用：

```
configure terminal
   webvpn
      [no] application-type <application_name> default tunnel-group <tunnel-group-name>
```

- *application_name* -应用程序名称。当前支持的唯一的应用程序是citrix**接收方**。
- *通道组NAME* -作为默认将使用的当前隧道群的名称指定的类型VDI访问。

配置示例

这些是有效VDI配置示例：

```
configure terminal
   webvpn
      [no] application-type <application_name> default tunnel-group <tunnel-group-name>
```

自适应安全设备管理器 (ASDM) 配置

1. 导航对**Asdm > Configuration>远程访问VPN >无客户端SSL VPN访问>组策略**：

2. 导航**编辑>更多选项> VDI访问**：

3. 添加**VDI服务器**：

注意：唯一的支持的模式是单模。

ASA身份证书和证书权限(CA)

- 为了Citrix接收方能与ASA一起使用，**移动设备必须委托发出ASA的身份证书的CA。 必须为完全限定域名**(例如， clientlessvdi.cisco.com)， ASA的而不是IP地址**发出ASA的证书**。如果不是存在移动设备KEY存储的ASA的证书由中间CA发出，中间CA必须也是委托。
- 当Citrix接收方连接对与一不信任证书时的ASA，用户用弹出式警告提示是否继续。
- 因为他们支持证书和CA，直接的导入运行iOS的苹果公司设备可以支持自已签署的ASA证书。
- 在运行iOS的苹果公司移动设备上，接收方允许对ASA的应用列表的连接和检索，如果证书警告忽略。然而，用户也许不能开始其中任一已发布资源，直到一有效ASA证书安装。
- 某些更旧的机器人操作系统(OS)移动设备不提供合法方式导入第三方证书到关键存储。所以，为了在这样机器人设备的一个Citrix接收方与ASA/CAG一起使用， ASA必须有被嵌入了到关键存储，例如， Verisign或者Godaddy CA发出的身份证书。
- 在机器人移动设备上，如果ASA的证书不是存在设备的关键存储， Citrix接收方不允许对ASA的连接。
- 机器人设备用OS版本4.1和以上证书和CA的支持导入，并且应该如上所述与iOS一起使用。

最终用户接口/用户体验

添加新帐户

当使用时，使用Citrix接收方访问虚拟资源通过ASA提供用户体验和一样Citrix接入网关。

如果服务器没有配置，您必须配置一种新的虚拟资源。

提供ASA的FQDN IP地址：

检查**接入网关**，**标准版**，并且输入凭证为了连接到ASA。

当用户配置文件保存时，应用程序自动地请求凭证(ASA)并且设法登陆。

当登陆，应用程序显示已发布资源列表。

您能导航文件夹和点击资源为了启动它。

WebVPN会话的注销

Citrix接收方应用程序不提供能力任意终止有已连接ASA或CAG的一WebVPN会话。典型地，当您到达已配置的超时时，这样会话终止。虽然Citrix接收方新版本有一个新的**注销**按钮，不终止有ASA的当前会话。反而它关闭所有开放应用程序并且显示配置的服务器列表。所以，如果ASA只配置使用每个用户一个许可证，使用**注销**按钮的客户端不能再登陆在会话时间之后。

为了允许最终用户任意终止WebVPN会话，并且，结果，发布ASA许可证，新建的功能被添加了对注入**安全注销**资源。

在Citrix接收方拿来已发布资源时候，列表此射入发生。

当您点击**安全注销**应用程序时，在ASA和Citrix接收方之间的会话终止。为了适当地发布ASA许可证，必须用于**安全注销**资源为了终止WebVPN会话而不是本地Citrix接收方注销按钮。

不同的消息显示由于根据移动设备和Citrix接收方版本的会话终止。并且，差异就象Citrix申请写入对另外移动平台的产生一不同的体验，当您注销机器人设备时。

在iPad和IP电话上， Citrix接收方显示**您的对网关会话的访问超时的**消息**，再请登录。** 当您点击OK键时， Citrix接收方显示屏幕用配置的服务器。

机器人设备也显示被注入的**安全注销**资源。

然而，当您点击**安全注销**应用程序，网络连接错误显示。

虽然WebVPN会话现在终止， Citrix接收方应用程序未嵌入消息适当地通知您进一步操作。这是预料之中的现象。当由于终止的会话的此**错误消息**显示，它盼望您点击**Cancel按钮**， **Back按钮**在机器人设备为了退出往来帐，然后**OK，**当询问，如果要留下此帐户。

在您退出往来帐后，您提交与预先配置的服务器列表。

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

调试

> **注意**：使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

您能显示Citrix接收方的调试信息用此命令：

```
debug webvpn citrix <1-255>
```

> **注意**：
> 1级显示异常状况、失败的连接对XenApp/XenDesktop服务器和一般错误。
> 级别50显示关于解析/重写的数据的信息。
> 级别255显示如被添加为Citrix接收方连接的所有调试信息。

新的命令未为Citrix接收方验证被添加。然而，为了查看在客户端和ASA之间的处理，您能使用此调试：

```
debug webvpn transformation request
```

供参考。此输出显示从工作的连接采取的这两调试：

```
debug webvpn transformation request
```

请使用通用的验证调试指令为了debug authentication问题，例如：

```
debug aaa commondebug ldapdebug radiusdebug sdi
```

常见问题(FAQ)

Q.此新特性是否保留在XenServer配置的粒状控制(例如，控制例如客户端推进重定向、客户端打印机重定向，客户端CLIP面板重定向和客户端USB设备重定向)？

A. 这些参数在XenServer定义并且是ICA文件的一部分。ASA不修改这些参数。所以，您有在XenApp的设置或XenDesktop在客户端反射。

Q. ASA是否有例如防止剪贴和控制打印机、驱动、剪贴板或者USB重定向的ICA连接的粒状控制？

A. ASA不修改那些设置。所以，您有在XenApp的设置或XenDesktop在接收方客户端反射。思科知道功能差距，因为其竞争(Citrix CAG) Juniper SA和不管在XenApp的设置能防止剪贴。

Q.店面Citrix服务器与ASA一起使用作为代理？

A. 此功能不支持是。提出增强请求CSCug18734为了添加服务器的这些类型的支持。作为XenDesktop支持一部分，店面版本2.0 SSO支持被添加。店面版本2.0支持所有传统Citrix功能(XenApp和XenDesktop)。APP控制器涉及功能不通过ASA支持。

当您配置Citrix接收方的时ASA，请确保指定完整路径到在店面的XML服务运行，例如，**http://storefront.cisco.com/Citrix/storefrontweb/pnagent/**。

在没有CSCug18734的修正，并且有**citrix enabled调试的WebVPN的**版本中，如果设法访问店面服务器，然后您在调试看到此：

debug aaa commondebug ldapdebug radiusdebug sdi

Q.即使Citrix服务器启用和配置的XML服务，**被捉住的**错误**+++未知例外**继续显示。用于的这工作。会是什么错误?

A. 当AnyConnect精华在ASA启用如显示此处时，这能发生：

debug aaa commondebug ldapdebug radiusdebug sdi

AnyConnect精华用于为了启用在ASA的仅最大的客户端支持，并且这禁用ASA的能力处理无客户端连接尝试。当这发生时，如果有**调试WebVPN转换请求**并且**调试citrix enabled的WebVPN**，然后您看到此：

```
Received config.xml request
DBG:29:4089679874:74100d20:9902: Finished with hooks
(aware.c:aware_dispatch_request:389)
DBG:30:4089679886:74100d20:9902: => handoff (AWARE_HOOK_INTERNAL_HANDOFF)
(aware.c:aware_dispatch_request:508)
DBG:31:4089679900:74100d20:9902: in process request
(proxy.c:process_request:239)
DBG:32:4089679950:74100d20:9902: Load proxy settings
(ucte_policy.c:ucte_get_ctx_settings:690)
DBG:33:4089679965:74100d20:9902: Load proxy settings
(ucte_policy.c:ucte_get_ctx_settings:720)
DBG:34:4089680019:74100d20:9902: parse_req_headers(client_fd, p_req) ;
(proxy.c:process_request:275)
DBG:35:4089680038:74100d20:9902: # req
(parse_req_headers.re2c:parse_req_headers:1269)
DBG:36:4089680049:74100d20:9902: # ver: cursor = 0x747e5a9e; lim = 0x747e5d0f
(parse_req_headers.re2c:parse_req_headers:1383)
DBG:37:4089680064:74100d20:9902: # ver: cursor = 0x747e5a9f; lim = 0x747e5d0f
(parse_req_headers.re2c:parse_req_headers:1383)
DBG:38:4089680077:74100d20:9902: Request: [GET /Citrix/pnagent/config.xml HTTP/1.1]:
39 (parse_req_headers.re2c:parse_req_headers:1399)
.
.
.
DBG:96:4089680705:74100d20:9902: Clientless WebVPN is not enabled.
(proxy.c:process_request:384)
.
.
.
DBG:31:4089681295:74100d20:9902: fwrite(0 ? -=> 90): [Connection:
close%0d%0aCache-Control: no-store%0d%0aContent-Type: text/html%0d%0aContent-Length:
0%0d%0a%0d%0a]: 90 (SAL/sal-stdio.c:sal_fwrite:92)
+++ UNKNOWN EXCEPTION CAUGHT
Terminating session for user [test.user]
```

问。 如果接收此错误消息**SSL Error 4 ：错误编号：183**，应该执行什么？

A. 此错误被看到，当对XML经纪(XenDesktop服务器)时的连接允许，但是实际XenDesktop池的端口1494和2598阻塞。如果启用所有端口然后缩小需要的端口，您能调试。

为了XenDesktop能工作通过无客户端，如果有在ASA (里面)和XenDesktop服务器之间的任何半成品防火墙，请确保端口443， 1494， 2598和80是开放的在该防火墙。并且，请保证端口为XenDesktop服务器和XenDesktops的池是开放的。

Q. ASA是否支持起源于从的一个独立Citrix接收方客户端Microsoft Windows/麦金塔OSX平台，正如您使用AnyConnect或Cisco VPN Client的SSL连接？
A. 目前，从桌面的独立Citrix接收方通过仅巧妙的通道支持(w.r.t无客户端)。
CSCum85649 ENH ：对ASA的支持桌面独立Citrix接收方
这是支持对ASA的一独立Citrix接收方连接的增强bug没有对巧妙的通道的需要或标注姓名起首字母

门户登录，类似那里是为有ASA的移动Citrix接收方作为接入网关。目前， ASA发送重置，在最初的握手到一个独立Citrix接收方后(与使用最新4.1 Windows的，和有在其他平台的同一种行为)。