技术白皮书

aruba
a Hewlett Packard Enterprise company

用户角色和基于用户的隧道(UBT)技术白皮书

Aruba动态隔离解决方案

内容

版本历史

更改修订日期的文档版本原因		
1.0	初稿	3/2020
2.0	新模板 语法更正 术语变更 CP6.9增强内容	9/2020

基于用户的隧道（UBT）

概述

基于用户的隧道（UBT）有两个基本的组成部分:

- 用户角色：指Aruba结合ClearPass根据终端接入方式、以及接入时间、终端类型等上下文信息，为有线设备/用户动态分配角色的能力，因此IT人员不再需要为接入端口预先配置VLAN。
- 隧道：指Aruba将流量传输回Aruba移动网关 (以前称为控制器) 的能力。

AOS-CX支持基于用户的隧道，这是Aruba动态隔离解决方案的一部分，该解决方案实现了基于用户或终端对流量进行隧道传输，并将流量发送到Aruba网关的功能。通过ClearPass返回可下载用户角色（Downloadable User-role）,或通过标准RADIUS服务器返回本地用户角色(Local User-role)，策略可以通过用户角色关联到接入终端。 与可下载用户角色相比，本地用户角色是在每个交换机上配置的，并且 “本地” 驻留在配置中。

许多需要以太网供电 (PoE) 和网络访问的设备，如安全摄像机、打印机、支付卡读卡器和医疗设备，没有像台式电脑或笔记本电脑那样内置的安全软件，可能会因为缺少安全性而将网络暴露在风险面前。 基于角色的隧道可以利用ClearPass对这些设备进行身份验证，将终端流量通过隧道传送到Aruba移动网关，并利用高级防火墙和策略功能对终端流量进行控制。它还可以通过ArubaOS 8.x中的网关群集提供高可用性和负载平衡。这可以为园区网内的物联网设备提供安全的访问。

UBT支持的两种网关部署方式：

- 单网关独立部署
- 多网关集群部署

支持UBT的Aruba CX交换机：

- Aruba CX 6200交换机系列
- Aruba CX 6300交换机系列
- Aruba CX 6400交换机系列

建议的交换机固件版本：

- AOS-CX 10.4或更高版本建

议的网关固件版本：

- 单网关独立部署模式 (70xx，72xx): ArubaOS 8.4 或 更高版本
- 多网关集群部署模式 (70xx，72xx): ArubaOS 8.4 或 更高版本

建议的ClearPass策略管理平台版本 （用于分配用户角色）

- Clearpass 6.9 或更高版本

术语

- “无色” 端口: 无色端口的最大好处是，我们不再需要以静态方式为接入端口预配置特定的策略和端口属性。无色端口背后的逻辑是，在过去，为了控制接入终端的权限，传统网络往往需要手动配置端口，从物理上为这些交换机端口分配 “颜色”，从而使特定的权限策略可以被配置并且关联到物理端口上。而特定的终端必须按照相应的“颜色”，插入对应的交换机端口。通过使用无色端口，可以大大减少IT操作周期，从而可以更加有效地对初始部署或者后续变更进行规划，以适应将来的添加，移动或更改。

无色端口表明交换机端口可以自动、实时地将所需的角色分配给接入终端。

最简单的无色端口可以通过在单台交换机中使用本地用户角色和本地MAC身份验证 (LMA)进行演示。在没有外部Radius服务器或隧道的情况下，客户可以观察到同一端口如何根据所连接的设备采取不同的角色策略(QoS/ACL/VLAN)。

- 用户角色:将策略和端口属性组合为 “角色”，并被不同的设备或用户类型引用，提供了简化配置负担的能力。

  可以在交换机上配置本地用户角色 (LUR)，也可以在ClearPass服务器上配置可下载的用户角色 (DUR)。在使用本地用户角色(LUR)时，可以通过任何RADIUS服务器向交换机返回Aruba-User-Role VSA来实现用户角色的分配； 在使用可下载用户角色(DUR)时，需要采用ClearPass服务器想交换机返回Aruba-CPPM-Role VSA，同时利用HTTPS将角色配置下发到交换机。

  最基本的用户角色需要包括给终端分配什么VLAN (中继或非中继)，以及流量是否需要在本地转发，或者通过隧道传输回Aruba移动网关。 此外，作为可选项，用户角色还可以包括权限策略 (ACL/QOS)、身份再验证计时器和强制门户重定向。 无论是在交换机上预先定义本地用户角色(LUR)或在ClearPass上配置可下载用户角色(DUR)，都使用相同的交换机CLI语法。
- 隧道交换机: 具有隧道配置文件并建立隧道到移动网关的交换机。
- 隧道配置文件: 包括需要设置的配置参数集，如主用网关IP、备份网关IP等。用户可以在交换机上启用或禁用隧道配置文件。
- 隧道端口: 配置了隧道的端口。
- 基于用户的隧道（ UBT ）: 基于用户和/或设备角色的隧道
- 客户端设备: 连接到隧道端口的终端主机 (台式机/笔记本电脑/物联网设备)，该端口通过用户名/密码或MAC身份验证等凭据对终端主机进行身份验证。
- 主用网关:作为主用隧道终结端点的Aruba移动网关。
- 备份网关:作为备份隧道终结端点的Aruba移动网关。仅当整个主用集群都失效时才会切换到备份网关。
- MC: Mobility Conductor（ 以前称为Mobilty Master)，采用层次化结构对移动网关的配置进行管理。
- MD: Mobility Device，被Mobility Conductor管理的Aruba移动网关。
- RADIUS server: RADIUS服务器，用于对用户和设备进行身份验证。
- LCS: Local Conductor Server，本地管理服务器
- User Anchor Gateway (UAG): 终结某个用户隧道的主用网关，可以是集群中的任何一台网关。
- Secondary User Anchor Gateway (S-UAG):用户隧道备用网关（ 基于Bucket Map确定），在主用UAG故障时自动接管用户隧道流量。
- Switch Anchor Gateway (SAG): 用于传输交换机控制面流量的移动网关，取决于隧道配置文件中的主用网关IP。
- Secondary Switch Anchor Gateway (S-SAG): 在SAG发生故障的情况下，作为备份SAG自动接管交换机控制面流量传输的网关。

UBT的组件

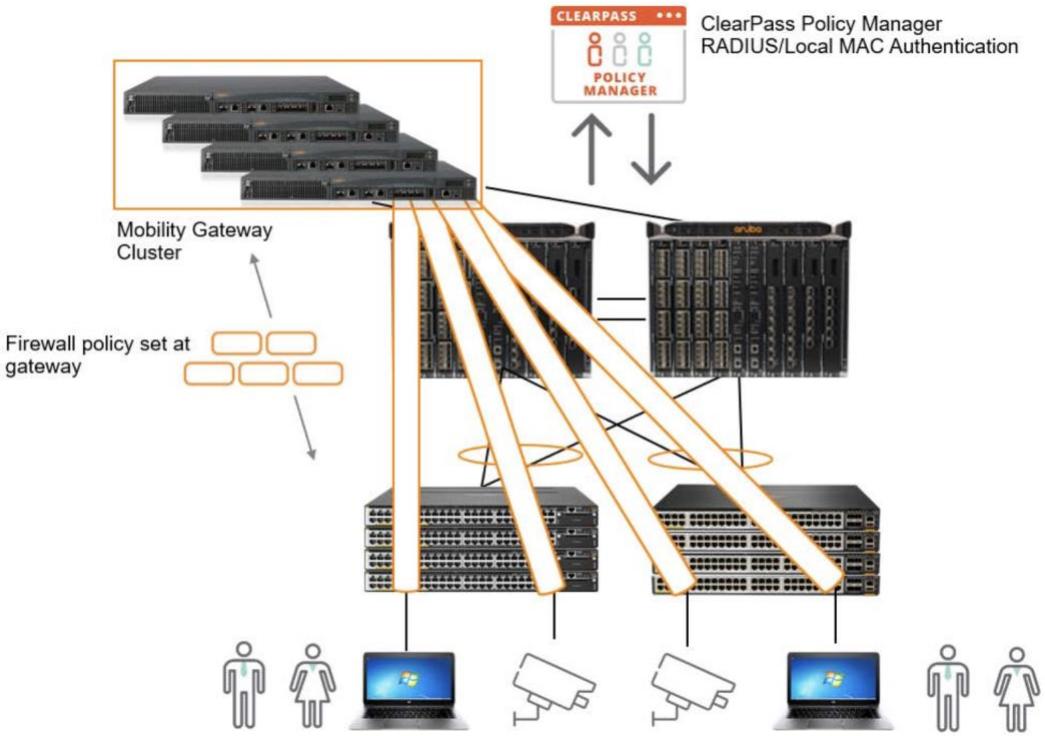

图1: UBT部署示例

客户端和设备

这就是“无色”端口被开发出来的原因。传统上，接入交换机端口都会标上“颜色”，同时特定设备也会被分配特定“颜色”。 采用“无色”端口时，接入交换机上的所有端口都设置为启用802.1X和MAC身份验证。终端接入“无色”端口时，接入交换机通过MAC或802.1X对终端进行身份验证，并触发ClearPass身份验证策略，从而获得包含用户角色配置的强制策略配置文件。

接入交换机

接入交换机对连接到交换机的用户进行身份验证，并在完成设备或用户身份验证后，将角色应用于设备或用户。用户角色是应用于设备或用户的一组属性和策略，可以存在于接入交换机本地，或者作为一个组成部分存在于ClearPass强制策略配置文件中。

移动网关集群

Aruba移动网关具有许多专门针对无线流量定制的内置安全性和应用优化功能，这些功能同样可以扩展到有线流量。这是将流量从Aruba接入交换机通过隧道传输到移动网关的主要原因之一，基于隧道的有线流量因此可以充分利用移动网关内置的防火墙和应用优化功能。

Aruba ClearPass策略管理平台

ClearPass根据识别处的终端类型信息和用户身份验证信息来分发包含用户角色信息的强制策略和配置文件。

深入理解UBT

它是如何工作的

首先在交换机上通过命令“ubt zone”配置 “隧道配置文件”。在这条命令的上下文中，可以配置主用网关IP地址，这个IP地址需要是移动网关集群中某一台的接口IP地址。交换机配置了移动网关信息并启用了UBT服务后，发起与移动网关之间的“握手”，以此来确认移动网关的可达性和版本信息。

当移动网关可达性被确认时，交换机会执行一个交换机“bootstrap”。这时,交换机会向移动网关发送一个bootstrap消息，类似于AP和移动网关之间的“AP Hello”。这个bootstrap消息包含用户角色信息 (网关/辅助角色、GRE密钥等)。在网关收到bootstrap消息后，就会回复一条 “acknowledge”消息。 交换机根据收到的确认消息，会更新本地的 “bucket map”和 “node list”列表，用于将用户映射到网关并实现终端负载均衡。 说得更加详细一些，“bucket map”是一个散列条目的列表，其中包含终端MAC地址与用于终结用户隧道的移动网关 (群集) 的映射关系。 当“bucket map”列表被下载到交换机本地后，交换机和移动网关之间建立隧道并且开始发送GRE“心跳”。其中，根据ubt zone命令中配置的主用移动网关IP地址，交换机会同时与SAG(Switch Anchor Gateway)建立GRE“心跳”。与此同时，交换机也会和S-SAG(Secondary Switch Anchor Gateway)建立GRE “心跳” 。

当用户连接到安全接入端口时，交换机向RADIUS服务器 (例如ClearPass策略管理器) 发送RADIUS请求，RADIUS服务器对用户进行认证后，如果采用交换机本地用户角色的方式，则向交换机返回与用户角色有关的供应商特定属性 (VSA)；如果采用可下载用户角色的方式，则RADIUS服务器将通过VSA把整个角色本身下载到交换机。

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	testrole

图2: 示例ClearPass本地用户角色VSA

交换机接收到VSA后，将本地用户角色或从ClearPass下载的角色应用于用户。 Aruba通过用户角色的概念来定义用户策略以及基于该角色对网络的访问。 用户角色可以包含ACL/QoS策略、Portal认证门户、VLAN信息 (用于本地交换流量) 和设备属性。 如前所述，当交换机从RADIUS服务器接收到用户角色相关的VSA，并将用户角色应用于用户时，用户角色中也可以包括将流量重定向到网关的指令。 这是通过 “gateway zone” 这个命令来定义的。 有了这个命令，当隧道启用时，交换机上的身份验证子系统会向隧道子系统提供gateway role, 又称为secondary role。 gateway role或者secondary role是移动网关上的用户角色，针对隧道用户的策略，特别是防火墙和安全策略。通常都会包含在这个用户角色中。 有些时候，这个用户角色也可以采用与无线用户相同的角色，重新应用到有线用户上。 发送到交换机隧道子系统的gateway role就是告诉移动网关，它必须基于这个角色的策略配置对用户流量施加额外的策略并建立用户隧道。 这个secondary role可以从ClearPass直接下载到移动网关，本文后面将对这一点做进一步的讨论。有关如何在ClearPass中配置强制策略和强制文件的更深入的内容，请参阅《有线策略实施指南》- https://arubapedia.arubanetworks.com/arubapedia/index.php/Clearpass_Solution_Guide:_Wired_Policy_Enforcement。

对于需要把用户通过隧道重定向到移动网关群集的情况，“bucket map” 包含给定的客户端 与主用和备用User Anchor Gateway (UAG) 之间的映射。 当需要把某个用户重定向到移动网关时，交换机会基于客户端MAC地址获得一个值，然后用这个值查找bucket map，并将客户端设备锚定到特定移动网关节点（即UAG）。 在此过程之后，交换机隧道子系统将创建到此UAG的隧道 (如果尚未创建)，并将用户流量通过隧道转发到该UAG。 如果用户角色不包含将流量重定向到移

动网关的属性，则交换机将为用户或设备分配相应的VLAN，并且将流量在本地转发。

一旦到UAG的用户隧道建立，交换机与UAG之间就会开始交换基于PAPI (进程应用程序接口) 的keepalive数据包，以此保持隧道的完整性。

基于角色的隧道建立流程

- 验证用户
- 将用户角色应用于经过身份验证的用户
- 将用户流量重定向到移动网关
- 在移动网关上将Secondary role应用于用户流量

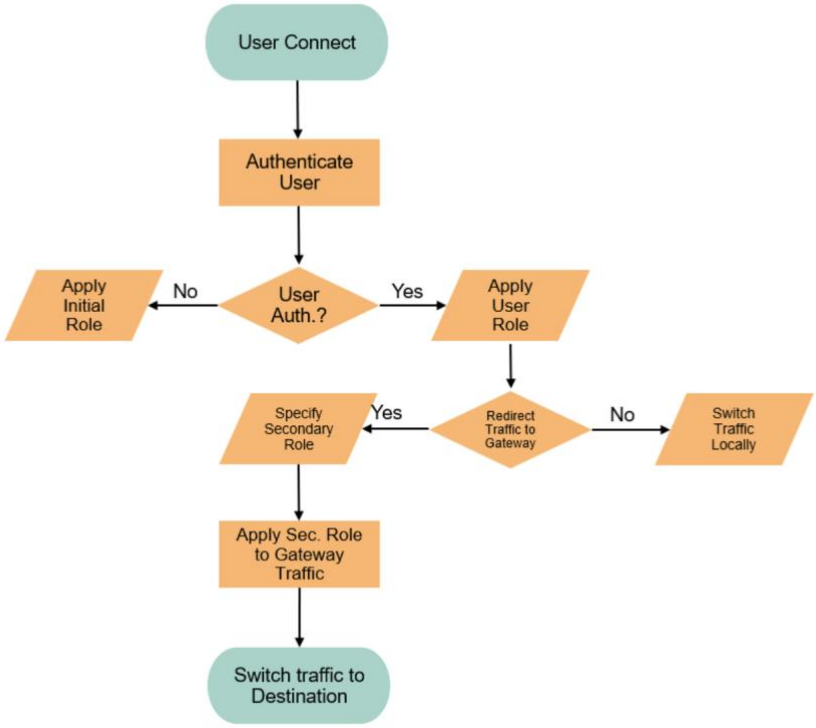

图3: 具有动态细分的用户身份验证流程

所有隧道流量将对reserve VLAN或ubt-client-vlan进行透传，并在移动网关处解封装，然后根据手动创建或下载到移动网关的gateway/secondary role中指定的VLAN，为用户分配vlan。 这个解决方案不再需要在园区网络中所有交换机上配置用户vlan，大大简化了网络运维。

广播/多播流量

所有多播/广播流量都通过reserve VLAN发送到移动网关。 然后，移动网关将为VLAN上的每个用户复制多播/广播数据包，并转换成单播流，再将单播流沿着用户隧道发送回客户端或设备。

请参阅下面对来自隧道用户的多播视频流的抓包，这个报文是从用户侧获取的。 请注意，源地址是移动网关的ip地

址，目标地址是隧道用户所连接的接入交换机的ip地址。 隧道中传输的流量是实时传输协议 (RTP) 视频流。 观察到的流使用的协议是UDP，这表明移动网关正在将多播流量转换为发往隧道客户端的UDP或单向流量。 还要注意，隧道内部报文的源地址是客户端IP，目的地址是多播组IP。

```
> Frame 6: 1412 bytes on wire (11296 bits), 1412 bytes captured (11296 bits) on interface 0
> Ethernet II, Src: ArubaAHe_dd:6c:00 (00:0b:86:dd:6c:00), Dst: ArubaAHe_02:9a:00 (f8:60:f0:02:9a:00)
> Internet Protocol Version 4, Src: 10.5.8.7, Dst: 10.5.8.17
> Generic Routing Encapsulation (Transparent Ethernet bridging)
> Ethernet II, Src: HewlettP_47:1e:6a (10:60:4b:47:1e:6a), Dst: HewlettP_f8:1b:0d (d4:c9:ef:f8:1b:0d)
> Internet Protocol Version 4, Src: 10.15.1.101, Dst: 239.0.0.1
v User Datagram Protocol, Src Port: 58697, Dst Port: 5004
    Source Port: 58697
    Destination Port: 5004
    Length: 1336
    Checksum: 0xc012 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
> Data (1328 bytes)
```

图4: 数据包捕获显示向隧道用户的多播流量转换

下面是描述这是如何工作的过程:

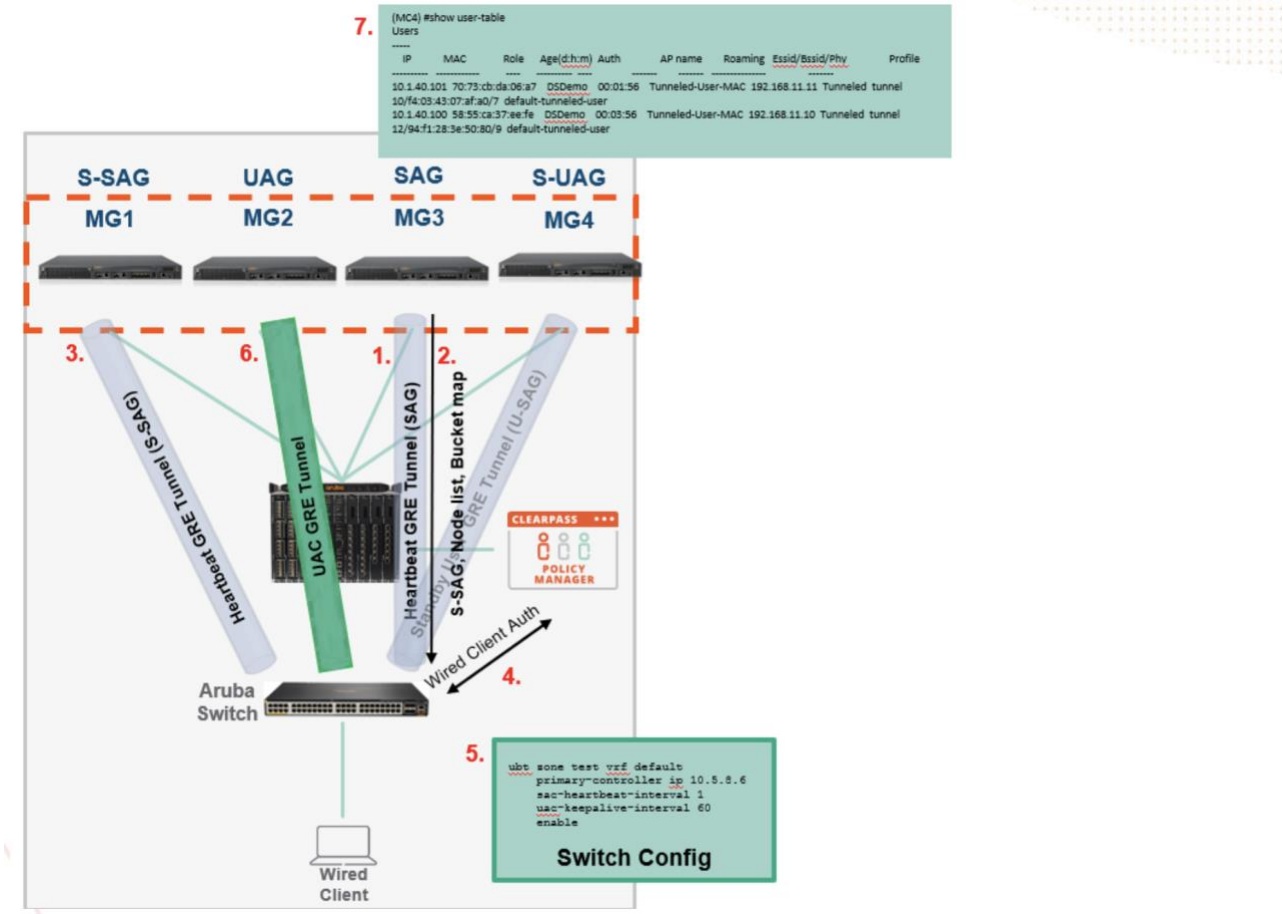

图5: 基于用户的隧道过程

请参阅上面的图，它显示了用户到移动网关集群建立用户隧道的过程。

1. 交换机按照预先配置与移动网关集群的MG3节点建立心跳/多播GRE隧道。
2. MG3向交换机返回Standby Switch Anchor Gateway (S-SAG) 、集群节点列表和Bucket map。
3. 交换机与MG1建立心跳/多播备份隧道 (S-SAG)，该隧道是根据来自bucket map的散列来分配的。
4. 当客户端连接到交换机时，进行用户或设备认证 (802.1x/MAC-Auth)
5. 如果本地或下载的用户角色具有重定向属性以及secondary role，交换机检查bucket map找到UAG = MG2和S-UAG = MG4
6. 交换机使用MG2作为User Anchor Gateway(UAG)建立用户GRE隧道，并发送包含用户VLAN信息的secondary role。
7. UAG (MG2)按照交换机发送的seondary role和VLAN创建用户条目，任何广播或多播流量都将转换为单播，并通过用户/设备隧道发送回去。
8. 在S-UAG上添加一个暂时休眠的用户条目，于此同时，交换机和S-UAG网关之间建立隧道，但是交换机不向S-UAG发送keepalive报文，keepalive报文仅发送到UAG。 如果集群节点列表发生更新，表明某个UAG已关闭，则交换机立即将这个UAG上的所有客户端切换到S-UAG，这将立即启动一个keepalive报文，直到依照bucket map更新确定一个新的S-UAG。

方案用例

基于用户的隧道传输（UBT）常见的使用场景包括提供访客有线接入、利用移动网关内置防火墙为逻辑接入网络提供终端准入控制，以及为有线流量提供隧道传输的能力。

有线接入防火墙

就像基于端口的隧道传输（PBT）一样，通过把用户流量隧道传输到Aruba移动网关之后，IT部门可以借助于Aruba移动网关内置的防火墙和访问策略来限制用户访问，而不需要在网络基础架构中安装昂贵的下一代防火墙。

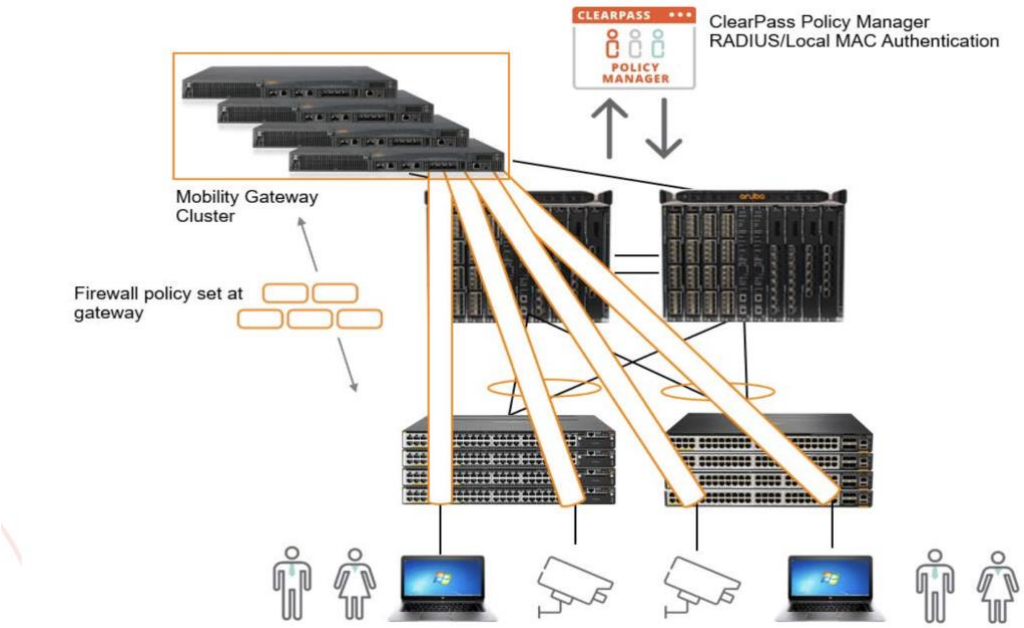

图6: 有线防火墙访问用例图

有线访客/终端隔离

可以使用基于角色的隧道（UBT）在网络上对有线方式接入的访客流量进行隔离。 通过在Aruba移动网关上创建 “secondary role” 作为访客角色，并分配特定的 “访客” VLAN，可以在移动网关上实现访客接入的防火墙策略，以隔离访客对园区网络其余部分的访问。

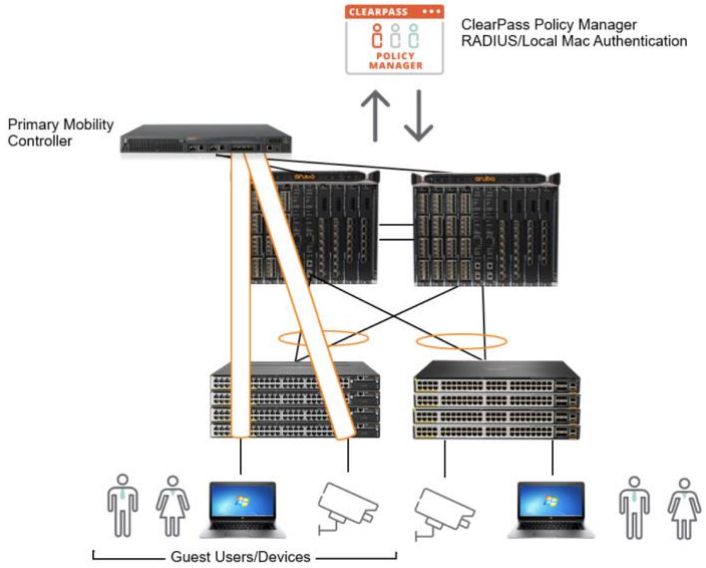

图7: 有线访客隔离用例图

分支部署

在典型的分支场景中，例如在零售行业，可以通过在每个商店部署一个移动网关来实现基于用户的隧道（UBT）。 移动网关可以下挂接入交换机来实现端口扩展，用于连接所有设备和用户。

所有这些设备和用户的流量都被传输回部署在本地的移动网关，通过移动网关内置的防火墙进行策略管控，并将流量通过WAN转发到特定目的地。

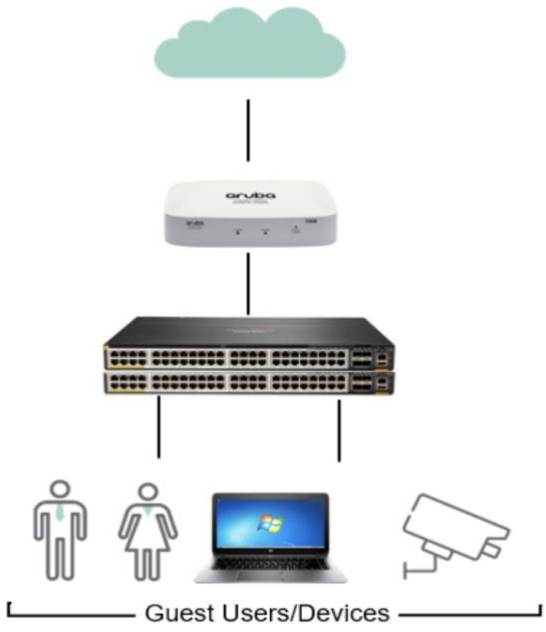

图8: 分支用例图

部署场景

基于用户的隧道-移动网关独立部署

此部署包括单个主用网关和可选的备用网关，在主用网关发生故障时充当备份提供故障切换。

- 在单个交换机端口上，支持多达256个具有不同用户角色的客户端，例如，Aruba交换机作为汇聚设备，通过非托管的2层交换机或者集线器连接各种有线终端。
- 在单个交换机端口上，如果有两个隧道客户端处于同一用户角色，并通过隧道传输到同一个User Anchor Gateway(UAG)，则该交换机端口与移动网关之间建立单个隧道
- 在单个交换机端口上，如果有两个隧道客户端处于不同的用户角色，并通过隧道传输到同一个User Anchor Gateway(UAG)，则该交换机端口与移动网关之间建立两个隧道
- 在单个交换机上，如果有十个隧道客户端连接在十个不同的端口上，则交换机与移动网关之间建立十个隧道。

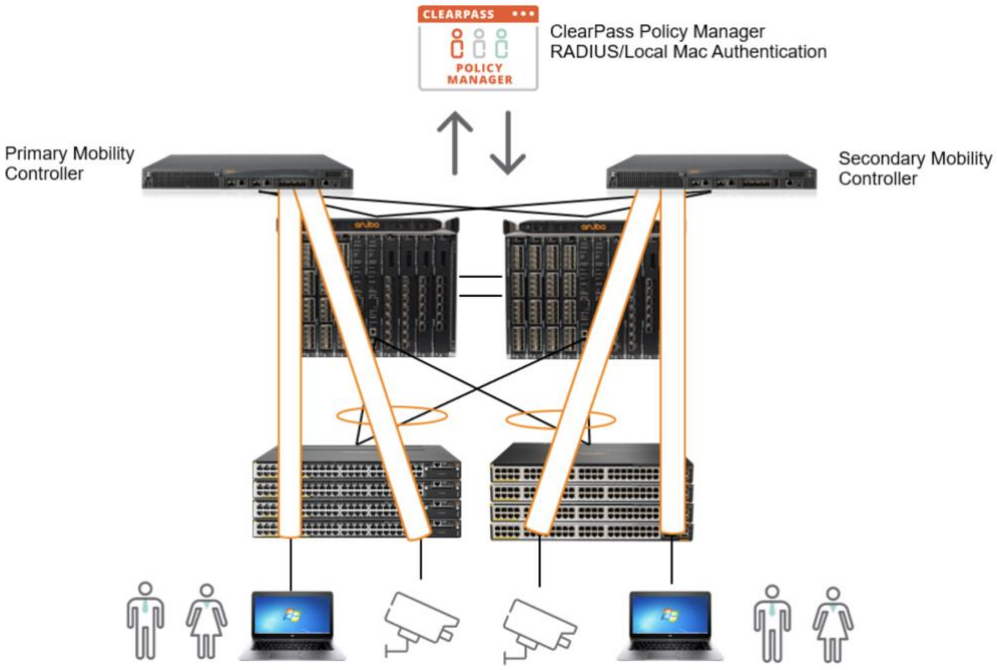

图9: 独立网关部署图

基于用户的隧道-移动网关集群部署 (仅有线接入)

此实现利用了Aruba移动网关的集群特性。

移动网关集群

- 集群的目的是为所有客户端提供高可用性，并通过故障切换确保服务连续性
- 一个集群中最多支持12个72xx网关平台(所有网关都是72XX)。
- 一个集群中最多支持4个70xx网关平台 (所有网关都是70XX)。
- 如果混合使用70xx和72xx网关，则每个集群最多可以支持4个网关。
- 在集群中，用于配置管理其他移动网关的节点被称为Mobility Conductor，其他移动网关节点被称为Managed Devices。

- 如果网络中有大量的有线设备需要采用隧道传输到移动网关以实现中心化控制，可以部署专用的移动网关集群专门处理有线隧道流量，这有利于实现大规模的基于用户的隧道（UBT）部署。 在大规模的有线客户端接入情况下，只要配置了正确的移动网关资源 (移动网关集群、负载均衡等)，每个交换机有线端口都可以启用基于用户的隧道功能，将用户流量通过动态隧道传输回移动网关。
- 在单个交换机端口上，如果有两个具有相同/不同角色的隧道客户端，锚定在两个不同的UAG上，则交换机会与每个UAG分别建立一个隧道。

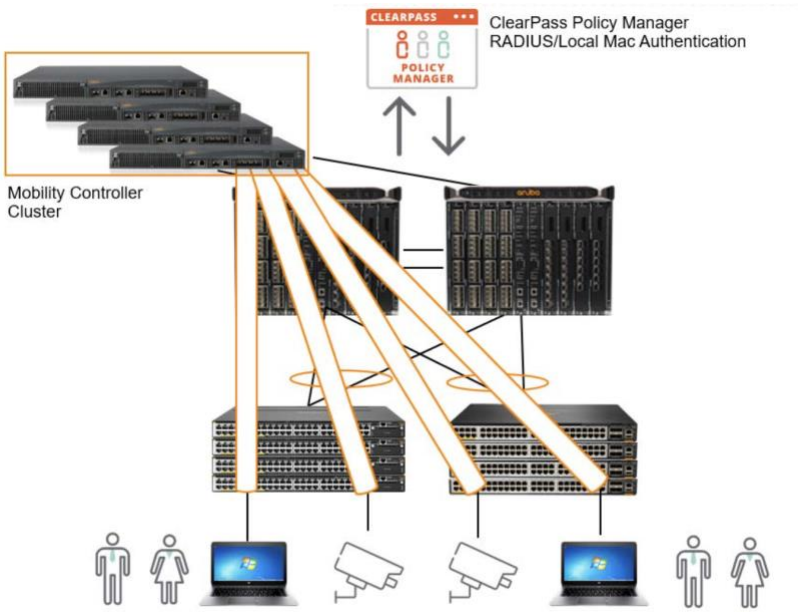

图10: 集群网关部署图

基于用户的隧道-移动网关集群部署 (大规模有线和无线接入)

如果同时存在大规模的有线和无线接入，则可以分别部署用于有线接入和无线接入的移动网关群集。 这将使有线客户端和设备能够采用专用的移动网关集群来建立隧道，同时把用于无线接入的移动网关集群用于专门处理无线流量。

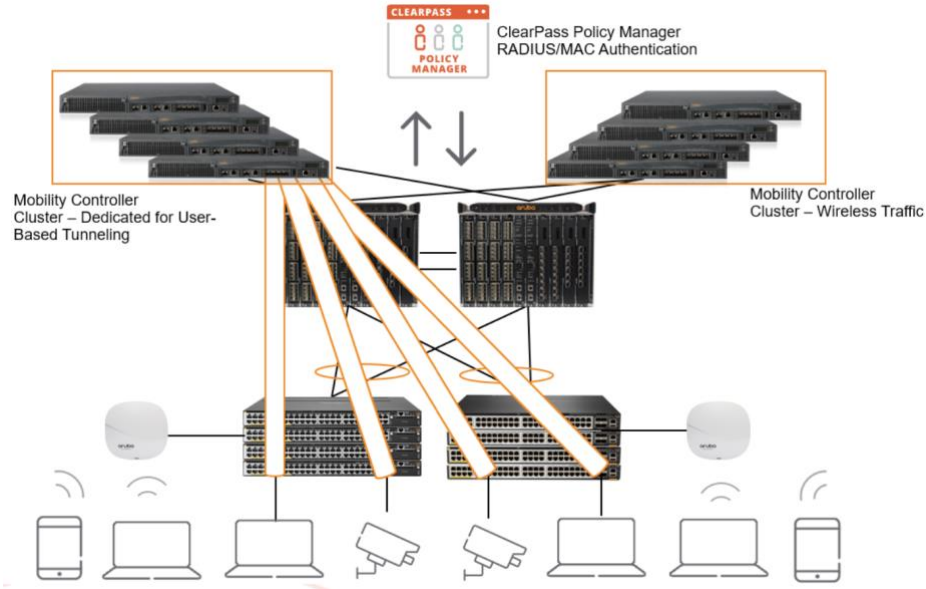

图11: 有线网关集群部署图

配置方法

配置基于用户的隧道 - AOS-CX

AOS-CX的配置与AOS-Switch相比有一些根本的区别，CX是基于接口的，而AOS-Switch是基于VLAN的。 但是，配置基于用户的隧道的概念仍然是相同的。

需要首先定义ubt网关，以便交换机可以形成到移动网关集群的控制隧道。 为此，我们需要输入以下命令:

```
switch(config)#ubt zone default vrf default
```

然后需要定义移动网关集群的IP地址，以便交换机可以指向移动网关并下载集群信息。 这也“打开”了交换机的隧道功能。这是通过primary-controller ip命令完成的。

```
switch(config-ubt-default)# primary-controller ip 10.6.9.6
```
– 注意: 必须使用移动网关的物理IP地址

配置ubt-client-vlan，首先定义VLAN，然后将VLAN指定为ubt-client-vlan。 这是交换机到移动网关的所有隧道流量的保留VLAN。

```
switch(config)#vlan 4000
switch(config)#ubt-client-vlan 4000
```

配置交换机与移动网关通讯需要使用的源地址。

```
switch(config)#ip source-interface ubt interface vlan200
```

可选配置: `switch(config-ubt-default)# sac-heartbeat-interval` –用于更改交换机和SAG（Switch Anchor Gateway）之间的 `keepalive/heartbeat` 数据包间隔时间 `(默认 = 1)`。 通常用于隧道在网络拥塞期间无法建立的情况下进行故障排除，或者在故障时确保更快地切换到备份网关。

可选配置: `switch(config-ubt-default)# UAG-keepalive-interval 60`

```
    Enable
```

以下命令用于验证配置:

```
switch# show ubt

Zone Name               : Aruba
Primary Controller      : 10.6.9.6
Backup Controller       : 10.6.9.5
SAC HeartBeat Interval  : 1
UAG KeepAlive Interval  : 60
VLAN Identifier         : 4000
VRF Name                : default
Admin State             : Enabled
PAPI Security Key       : Disabled

switch# show ubt state

Local Master Server (LMS) State:

LMS Type       IP Address     State                Role
Primary      : 10.6.9.6    ready_for_bootstrap operational_primary
Secondary    : 10.6.9.5    ready_for_bootstrap operational_secondary

Switch Anchor Controller (SAC) State:

Active       : 10.6.9.6
```

所有移动网关都应处于“up”和已注册的状态，并且显示为“ready_for_bootstrap”。

在移动网关和集群上配置隧道配置文件

这是在网关上配置secondary role，并移动网关配置为集群模式。

配置secondary role

```
user-role contractor
    vlan 25
    access-list session global-sacl
    access-list session apprf-contractor-sacl
    access-list session blockhttp
```

以下配置适用于移动网关处于集群模式的情况:

Mobility Conductor配置

```
lc-cluster group-profile "aruba2node"
  gateway 10.0.102.6
  gateway 10.0.102.218

(ArubaMC) (config) #show configuration node-hierarchy
       Default-node is not configured. Autopark is disabled.
       Configuration node hierarchy

   Config Node               Type
   -----------               ----
   /                         System
   /md                       System
   /md/00:1a:1e:02:a4:c0     Device
   /md/00:1a:1e:02:a6:40     Device
   /mm                       System
   /mm/mynode                System

(ArubaMC) [mm] (config) #cd /md/00:1a:1e:02:a4:c0
(ArubaMC) [00:1a:1e:02:a4:c0] (config) #lc-cluster group-membership aruba2node
(ArubaMC) [mm] (config) #cd /md/00:1a:1e:02:a6:40
(ArubaMC) [00:1a:1e:02:a6:40] (config) #lc-cluster group-membership aruba2node
```

注意: 配置集群配置文件时需要在集群配置文件中指定移动网关的IP地址。

```
(ARUBAMM-DS) [mynode] #show switches

All Switches
------------
IP Address  IPv6 Address  Name        Location          Type    Model       Version         Status  Configuration State  Config Sync Time (sec)  Config ID
----------  ------------  ----        --------          ----    -----       -------         ------  -------------------  ----------------------  ---------
10.5.8.5    2001::5       ARUBAMM-DS  Building1.floor1  master  ArubaMM-VA  8.4.0.0_68230   up      UPDATE SUCCESSFUL    0                       222
10.5.8.6    None          Aruba7205   Building1.floor1  MD      Aruba7205   8.4.0.0_68230   up      UPDATE SUCCESSFUL    0                       222
10.5.8.7    2001::3       Aruba7010   Building1.floor1  MD      Aruba7010   8.4.0.0_68230   up      UPDATE SUCCESSFUL    0                       222

Total Switches:3
```

图12: “show switches” 命令输出

注意: 验证是否添加了所有移动网关 (md)，并且状态为 “UPDATE SUCCESSFUL”。

交换机上的 Show 命令:

```
#Show ubt
#Show ubt state
#Show ubt statistics
#Show ubt information
#Show ubt users all
#Show ubt users count
```

交换机上的 debug 命令

```
#debug ubt
#debug portaccess (for user roles)
#debug destination console
#debug destination buffer
```

移动网关上用于故障排错的 show 命令:

```
#Show tunneled-node-mgr tunneled-nodes
#Show tunneled-node-mgr tunneled-users
#Show station-table
#Show datapath bridge
#Show datapath tunnel
#show lc-cluster group-membership
#show lc-cluster vlan-probe status
#show tunneled-node-mgr cluster-bucket-map
```

通过NetEdit中配置基于用户的隧道

使用Aruba NetEdit配置编辑工具，现在只需通过NetEdit中的向导即可完成动态隔离配置。

首先从NetEdit的拓扑视图中选择配置ubt的交换机。

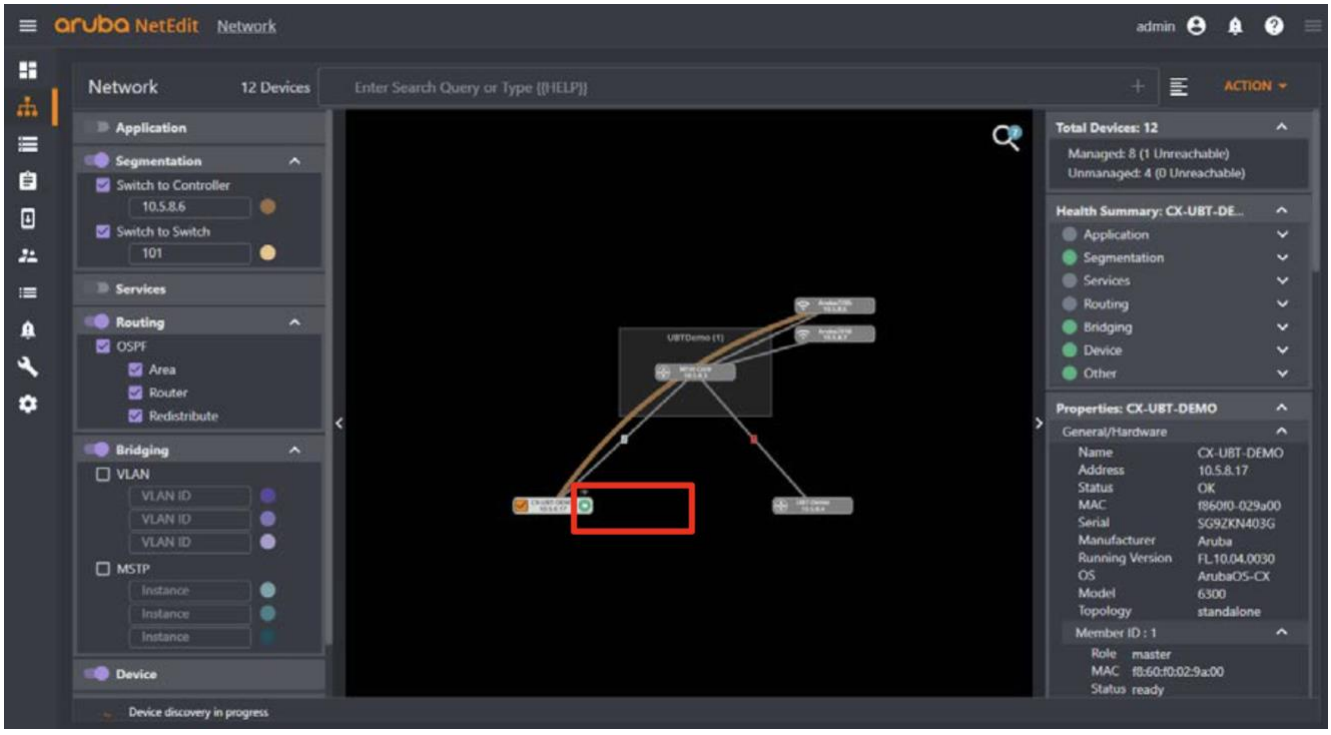

图13: NetEdit拓扑视图

然后，右键单击所需的设备以显示部署解决方案选项:

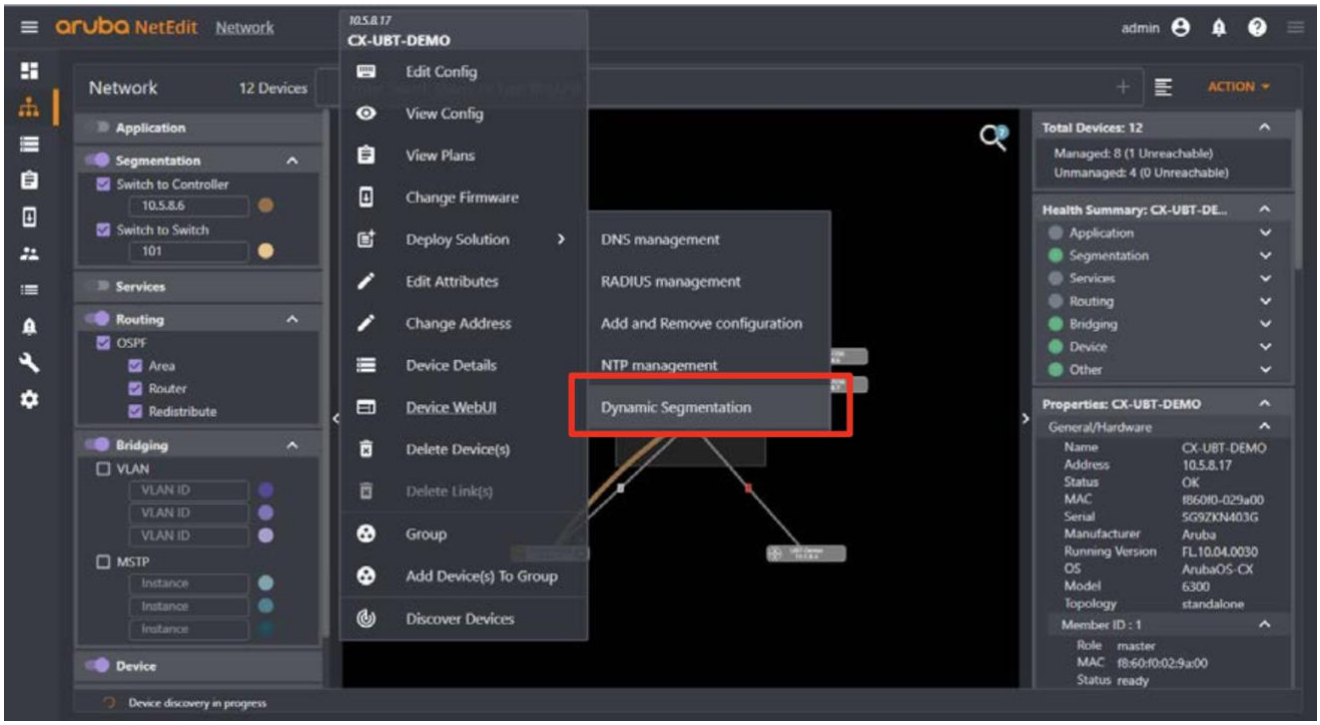

图14: NetEdit-动态隔离解决方案配置菜单

输入ubt配置所需的信息:

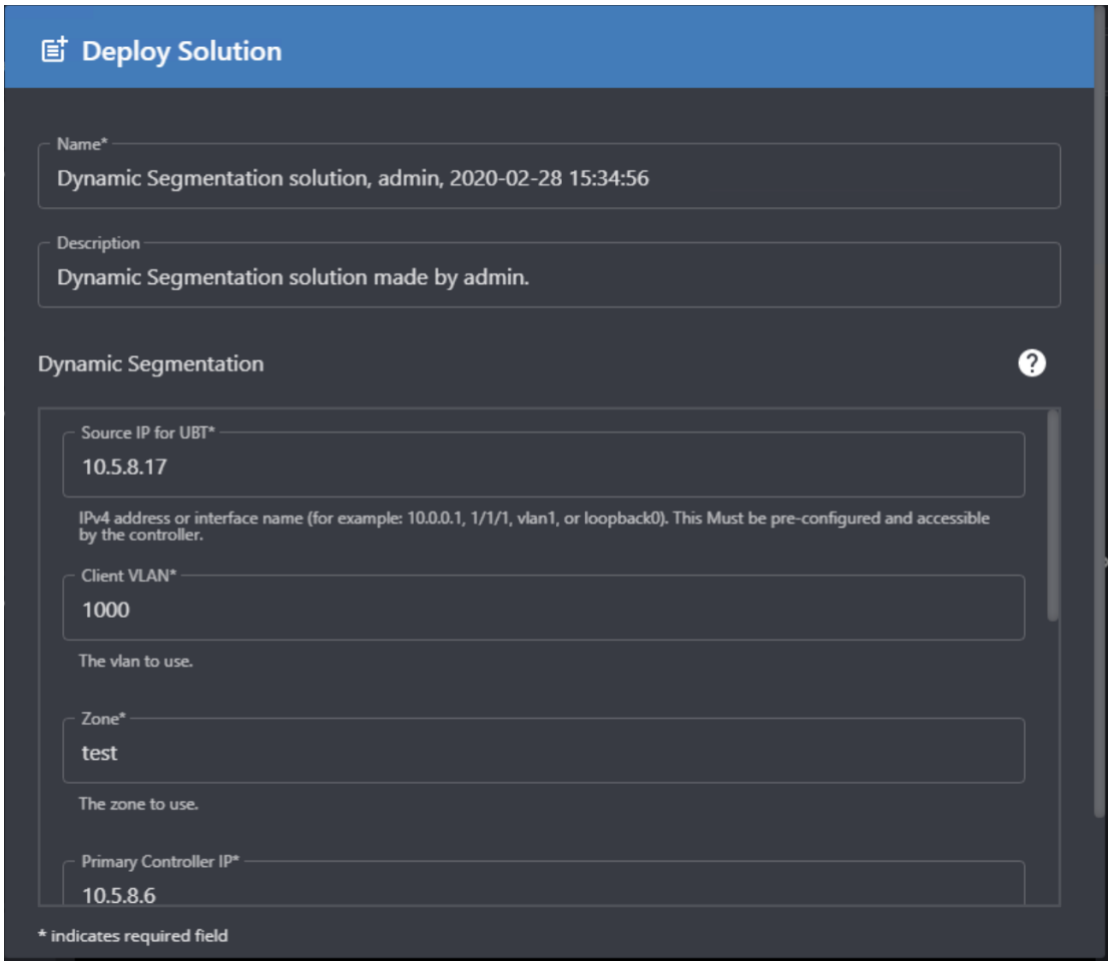

图15: NetEdit-动态细分 “部署解决方案” 菜单详细信息

完成后，可以通过单击预览按钮来预览配置:

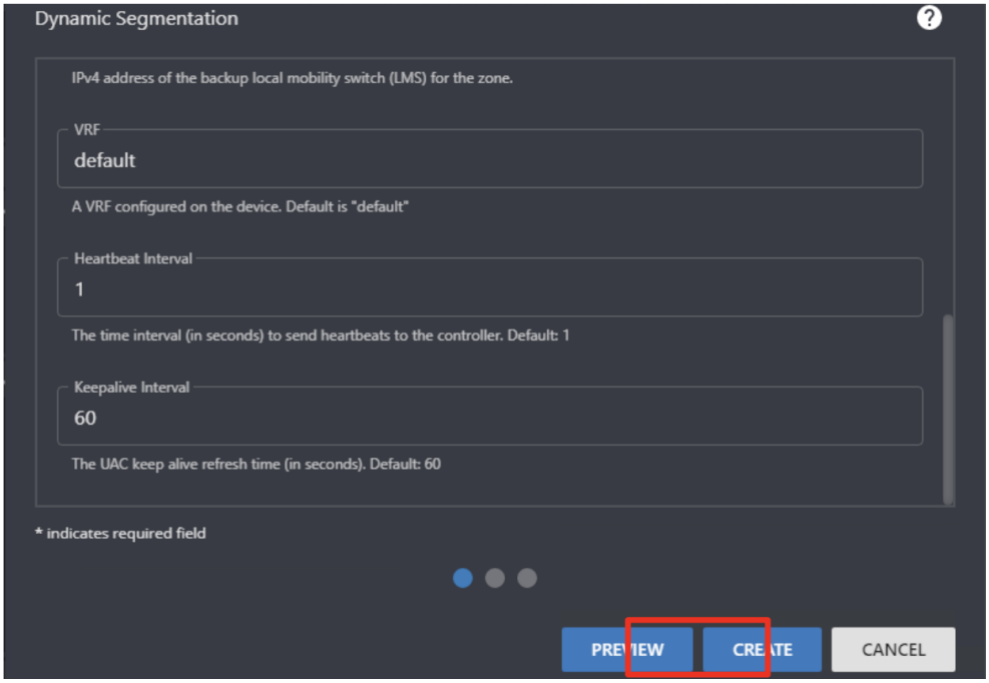

图16: NetEdit-动态细分 “部署解决方案” 预览按钮

在预览窗口中，可以查看添加的配置 (以绿色突出显示)，然后再将其推送到交换机。

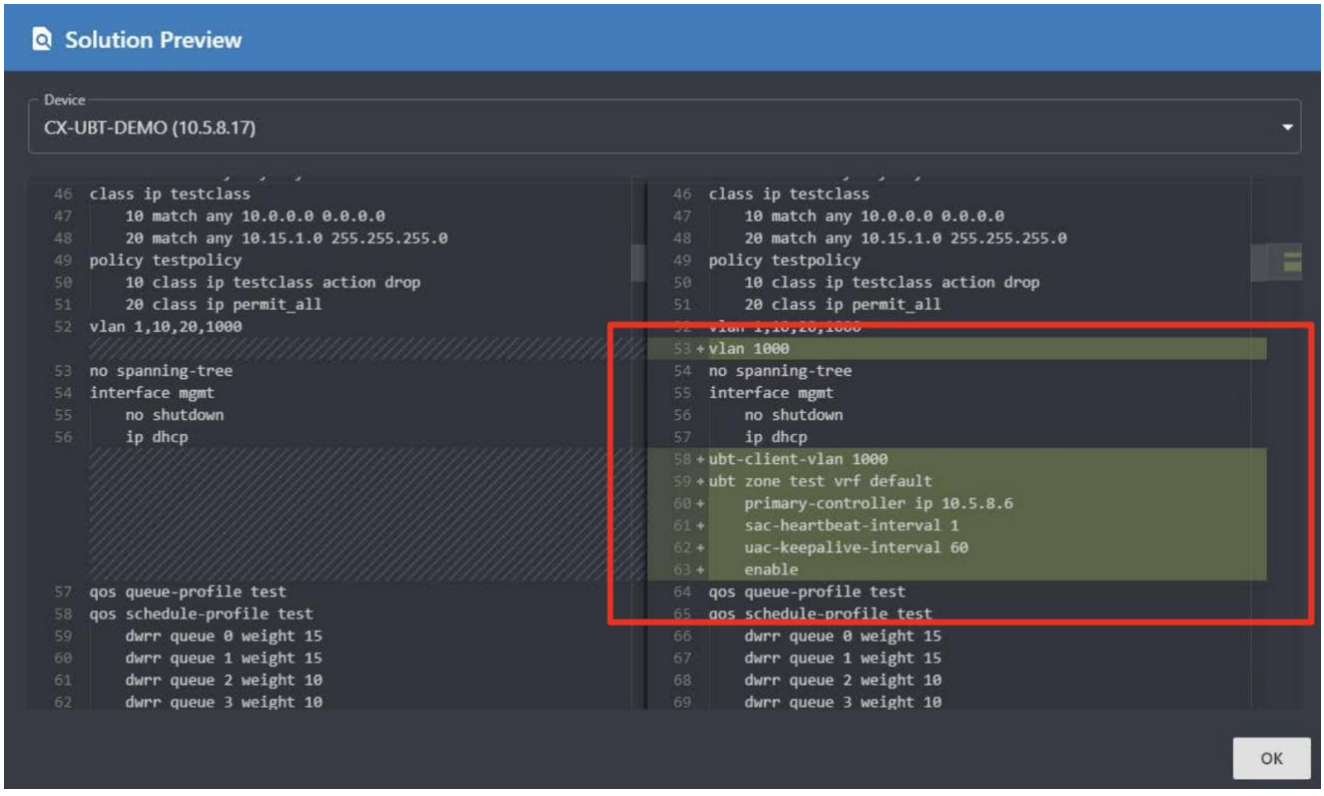

图17: NetEdit-动态细分 “部署解决方案” 配置比较

实现所需的配置后，单击 “确定” 按钮，然后从 “解决方案输入” 窗口中单击 “下一步”。

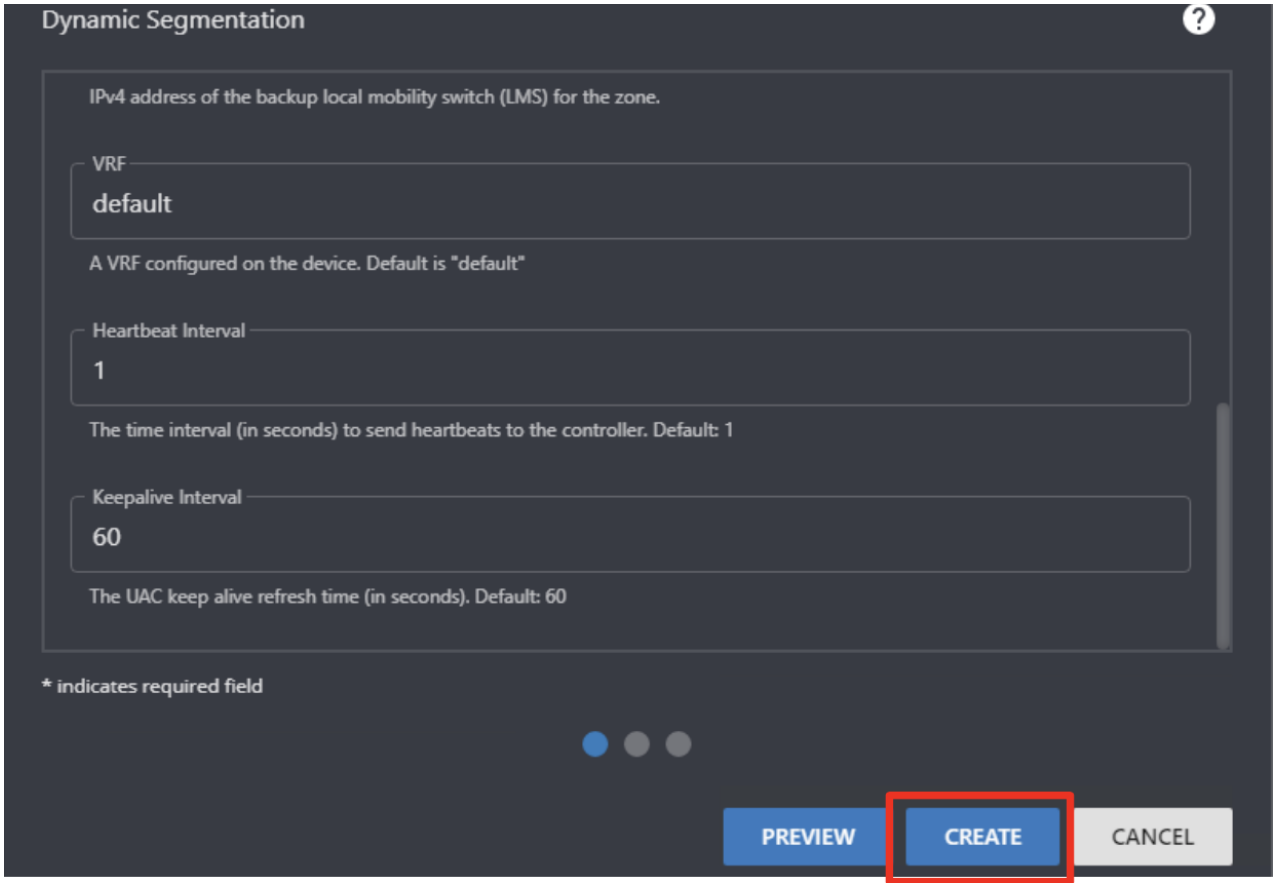

图18: NetEdit-动态细分 “部署解决方案” 创建按钮

这将生成配置并验证解决方案。

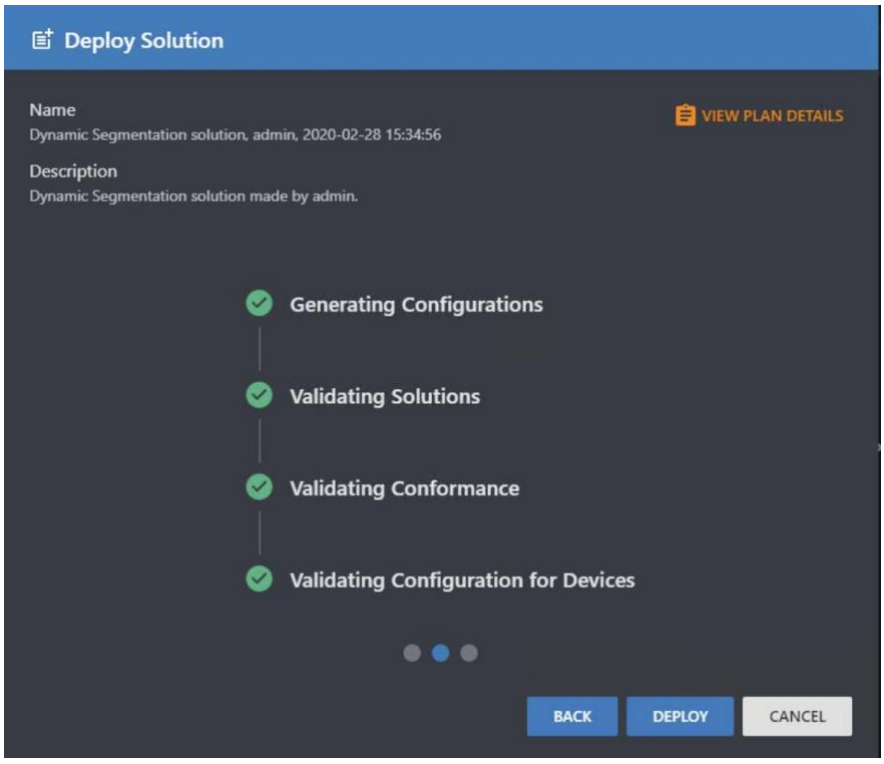

图19: NetEdit-动态细分 “部署解决方案” 配置验证

准备就绪后，单击“Deploy” ，将配置部署到交换机。

如果确定将部署所需的配置，请单击“是”。

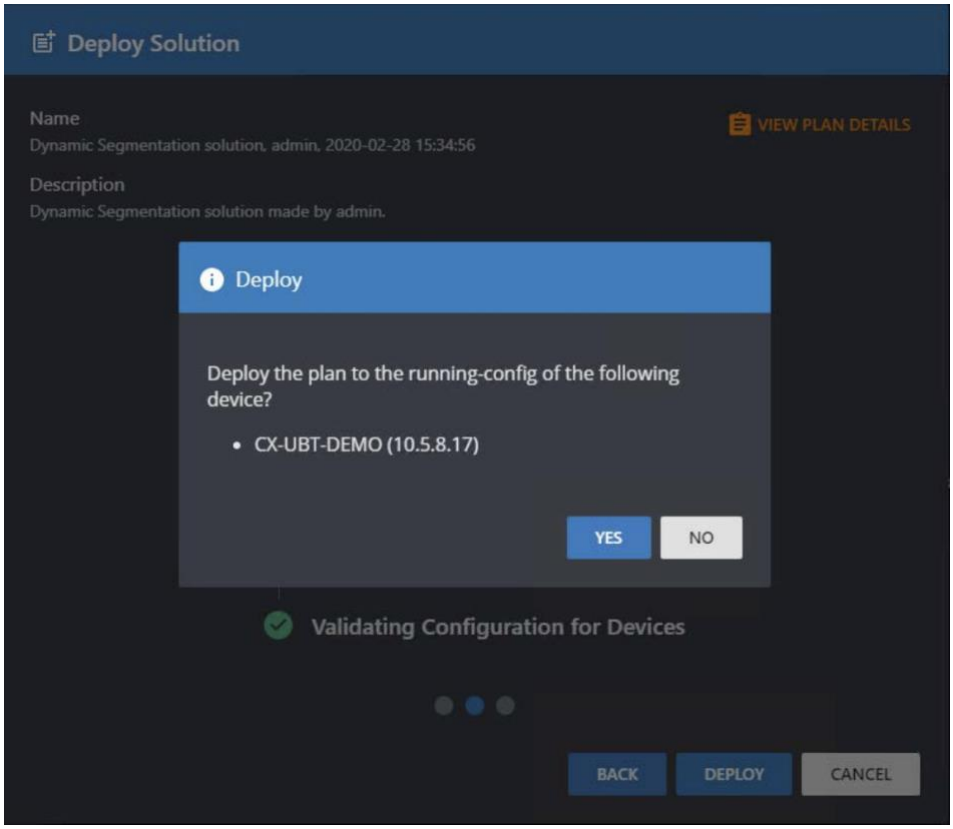

图20: NetEdit-动态细分解决方案部署

然后，NetEdit将配置推送到交换机。

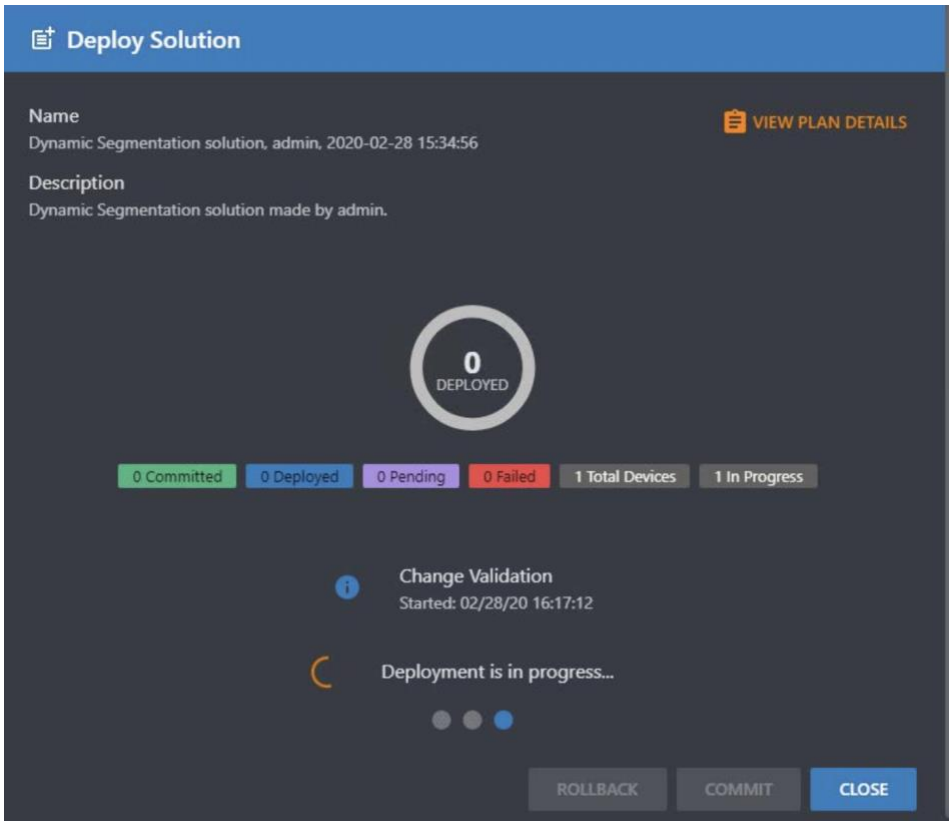

图21: NetEdit-动态细分 “部署解决方案” 部署状态

配置更改后，也可以点击“ROLLBACK”进行回滚。

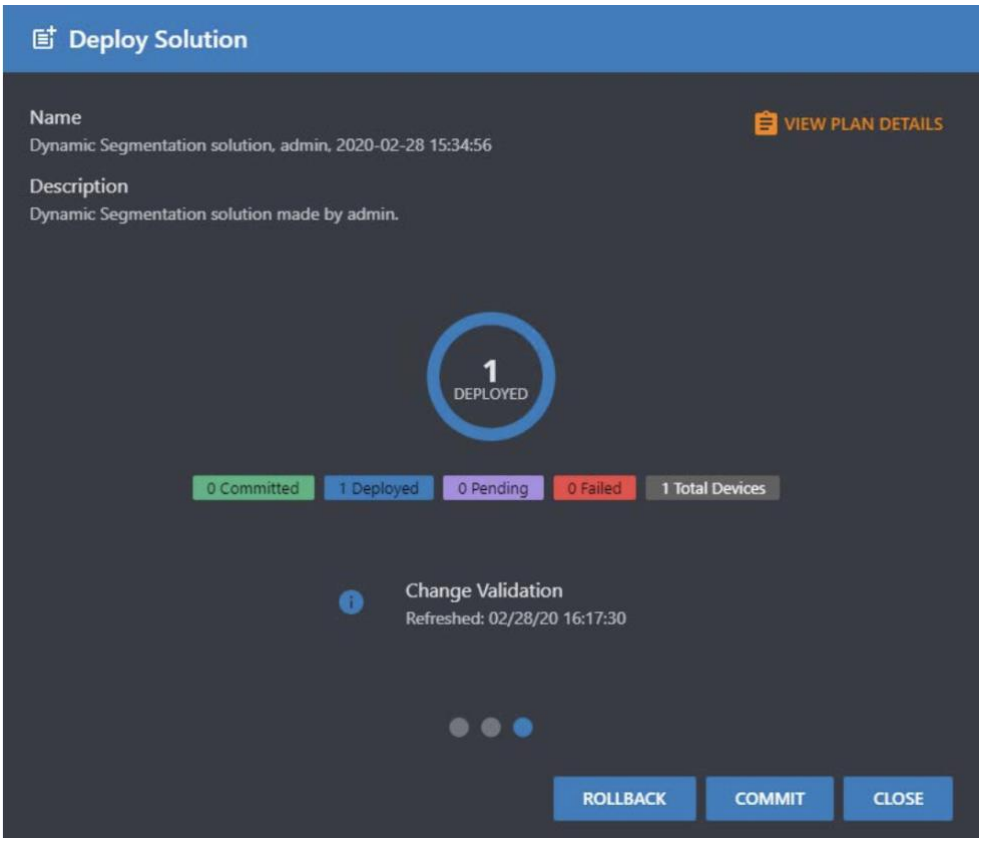

图22: NetEdit-动态分段 “部署解决方案” 回滚或提交。

如果确认更改，点击“COMMIT”将配置更新到交换机启动配置。

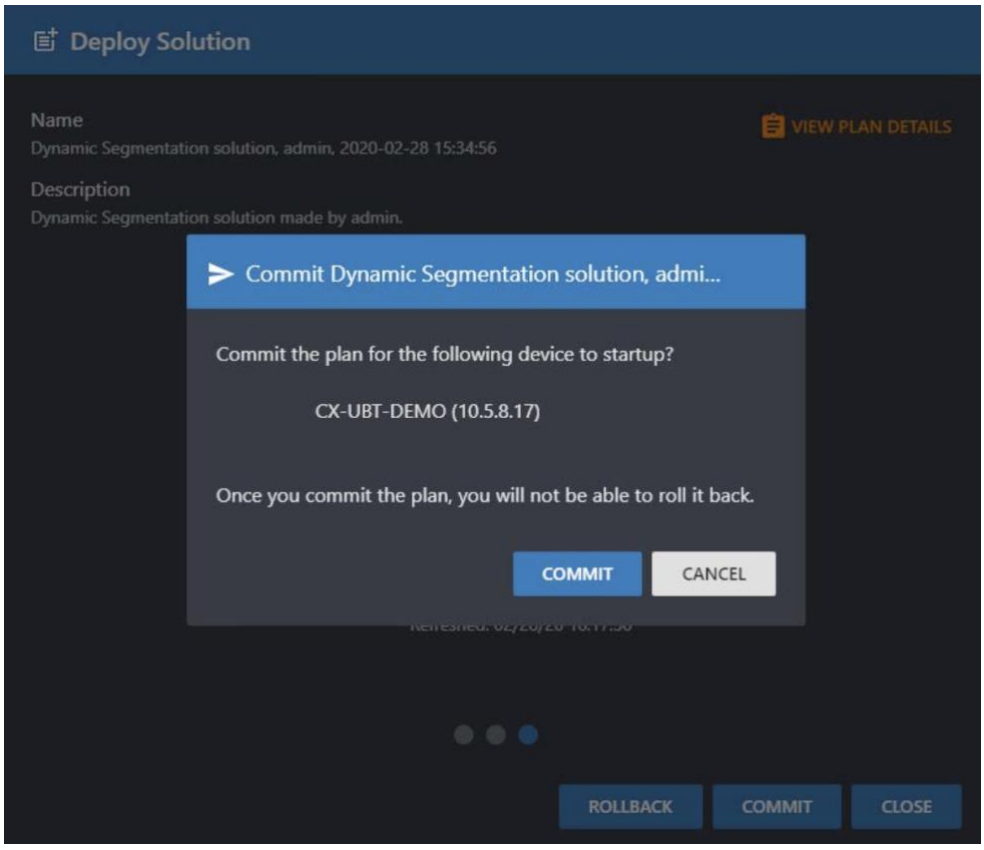

图23: NetEdit-动态隔离 “部署解决方案” 提交。

角色配置

本地用户角色可以与ClearPass或者其他RADIUS服务器配合使用。 任何RADIUS服务器都可以返回Aruba-User-Role VSA，当交换机接收到该VSA时，会依照该VSA为用户分配交换机上本地配置的用户角色。 但是，这种方式要求每台交换机上都必须手工配置所有角色，除非通过自动化部署交换机配置。

用户角色中的属性

多个设备属性可以通过本地配置或者动态下载方式配置在交换机的用户角色中:

- 无标签的 VLAN ID 或 VLAN Name
- 多个带标签的VLAN ID (或者单个带标签的 VLAN Name)
- ACL和QoS策略
- 端口模式
- PoE优先级
- QoS信任
- 重认证时间

流量策略

可以在用户角色中配置流量策略以允许或拒绝流量。 应当注意，每次在客户端或设备的端口处应用用户角色时，该策略中的条目将添加到交换机的TCAM表中。 在部署用户角色时，有必要进行相应的规划，以确保正在使用的交换机型号具有必要数量的TCAM条目，能够支持预期数量的网络客户端。用户角色的流量策略示例如下:

```
class ip BLOCK_VNI101
    match ip any 192.168.101.0/24 count
exit
port-access policy BLOCK_VNI101
    class ip BLOCK_VNI101 action drop
exit
port-access role vxlan102
    associate policy BLOCK_VNI101
    vlan access 102
exit

switch# show port-access policy

Access Policy Details:
======================

Policy Name   : BLOCK_VNI101_VXLAN_102_ACL-3015-3
Policy Type   : Downloaded
Policy Status : Applied

SEQUENCE    CLASS                          TYPE ACTION

10          BLOCK_VNI101_VXLAN_102_AC... ipv4 drop
```

注意: 用户策略中有一个隐含的denyall规则。 任何需要允许的流量都需要具有一个适当的流量类别。

QoS

可以根据用户角色QoS策略中的DSCP或IP优先级对用户流量进行优先级排序。 这使得在网络拥塞的情况下可以对用户或设备的流量优先级进行重新分类。

对于隧道转发的用户或设备流量，则可以根据策略标记隧道外部GRE Header。 有关示例，请参见图24。

	Type	Name		Value
1.	Radius:Aruba	Aruba-CPPM-Role	=	class ip camera-ef 10 match any any any port-access policy camera-ef 10 class ip camera-ef action cir kbps 5000 cbs 1000 exceed drop action dscp EF port-access role camera auth-mode client-mode associate policy camera-ef gateway-zone zone test gateway-role camera

图24: 具有QoS配置的可下载用户角色

在上述用户角色中，我们将camera这个角色的所有流量标记为 “EF” 流量。 在客户端连接并建立隧道之后，我们可以在接入交换机和移动网关之间的核心交换机处进行抓包，以查看隧道化的数据包，并GRE数据包中观察到DSCP标记。

```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    Total Length: 1472
    Identification: 0x0000 (0)
  > Flags: 0x4000, Don't fragment
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 100
    Protocol: Generic Routing Encapsulation (47)
    Header checksum: 0xec36 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.5.8.17
    Destination: 10.5.8.6
> Generic Routing Encapsulation (Transparent Ethernet bridging)
> Ethernet II, Src: D-Link_a8:6b:f6 (00:1e:58:a8:6b:f6), Dst: HewlettP_f8:1b:0d (d4:c9:ef:f8:1b:0d)
```

图25: 在GRE报头中显示QoS标记的数据包

设备模式

如果在用户角色中配置了设备模式，当第一个设备被认证并分配该用户角色后，交换机解析到该用户角色为设备模式时，端口被 “打开” 以用于随后的终端接入。 这主要用于Aruba的园区或即时接入点 (IAP)，在IAP被认证后，IAP上的所有后续用户将被允许从该端口访问网络。

在ClearPass中配置设备模式时，用户角色配置如下所示:

	Type	Name		Value
1.	Radius:Aruba	Aruba-CPPM-Role	=	port-access role iap auth-mode device-mode poe-priority high vlan access 10

图26: 具有端口模式配置的可下载用户角色

交换机上应用了该角色以后，可以使用命令 “show port- access role” 查看角色所应用的属性

```
Name   : CX_IAP-3078-1
Type   : clearpass
Status: Completed
-----------------------------------------
    Reauthentication Period                :
    Authentication Mode                    : device-mode
    Session Timeout                        :
    Client Inactivity Timeout              :
    Description                            :
    Gateway Zone                           :
    UBT Gateway Role                       :
    Access VLAN                            : 10
    Native VLAN                            :
    Allowed Trunk VLANs                    :
    MTU                                    :
    QOS Trust Mode                         :
    PoE Priority                           : high
    Captive Portal Profile                 :
    Policy                                 :
```

图27: 交换机中的可下载用户角色

从下面的身份验证输出中，可以看到只有一个MAC地址进行身份验证，这就是IAP。

```
CX-UBT-DEMO(config)# show aaa authentication port-access interface 1/1/6 client-status

Port Access Client Status Details

Client 40:e3:d6:c4:29:64, 40e3d6c42964
==============================
  Session Details
  ---------------
    Port         : 1/1/6
    Session Time : 1478448s

  Authentication Details
  ----------------------
    Status           : mac-auth Authenticated
    Auth Precedence : dot1x - Not attempted, mac-auth - Authenticated

  Authorization Details
  ---------------------
    Role   : CX_IAP-3078-1
    Status : Applied
```

图28: Port-Access 输出，突出显示进行身份验证的客户端设备

但是，通过查看MAC地址表，我们可以看到接口上有多个MAC地址 (1/1/6)。

```
CX-UBT-DEMO(config)# show mac-address-table
MAC age-time                : 300 seconds
Number of MAC addresses : 24

MAC Address              VLAN      Type                                      Port
-----------------------------------------------------------------------------------
a0:36:9f:2a:06:af        1         dynamic                                   1/1/48
e0:9d:31:5a:2c:b4        10        port-access-security                      1/1/6
48:f8:b3:7e:fd:52        10        port-access-security                      1/1/6
40:e3:d6:c4:29:64        10        port-access-security                      1/1/6
24:77:03:c3:df:10        10        port-access-security                      1/1/6
```

图29: MAC地址表的输出，显示了一个即时接入点之外的多个客户端

对照 IAP 用户管理界面，在交换机MAC地址表中显示的3个客户端是 IAP 的无线客户端连接到交换机的。

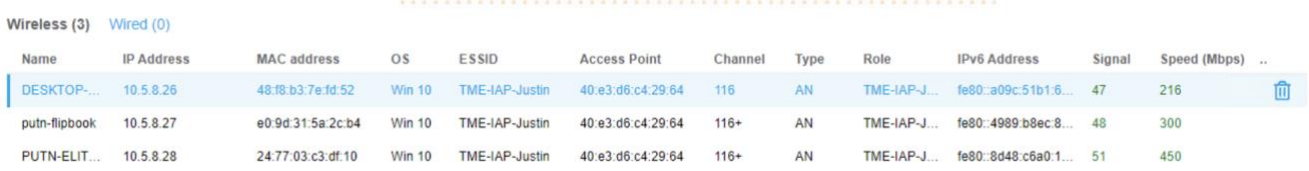

图30: Aruba Instant AP用户管理界面

PoE优先级

可以通过用户角色配置来设置PoE优先级。 这对于需要确保设备具有必要的PoE电源的关键设备很有用。 例如，如果VoIP电

话需要始终通电以确保紧急情况下的关键呼叫，则可以为电话设置更高的PoE优先级，这将确保可以拨打这些电话。

下面的用户角色示例显示PoE优先级和配置以及它们应用在交换机上时显示的信息。

	Type	Name		Value
1.	Radius:Aruba	Aruba-CPPM-Role	=	port-access role iap auth-mode device-mode poe-priority high vlan access 10

图31: 具有PoE优先级设置的可下载用户角色

```
Name   : iap-test
Type   : local
-----------------------------------------------
    Reauthentication Period                 :
    Authentication Mode                     : device-mode
    Session Timeout                         :
    Client Inactivity Timeout               :
    Description                             :
    Gateway Zone                            :
    UBT Gateway Role                        :
    Access VLAN                             : 10
    Native VLAN                             :
    Allowed Trunk VLANs                     :
    MTU                                     :
    QOS Trust Mode                          :
    PoE Priority                            : high
    Captive Portal Profile                  :
    Policy                                  :
```

图32: 交换机上显示的具有PoE分配和优先级设置的可下载用户角色

本地用户角色

本地用户角色允许Aruba交换机在本地配置基于用户的策略。 在用户角色配置中，可以创建ACL和QoS策略，配置设备和端口属性，以及将流量隧道传输到Aruba Mobility gateway的命令，即 “gateway-zone zone <zone> gateway-role <role>”。 当该命令被处理时，交换机将建立用户隧道并在移动网关上应用secondary role（用户角色），secondary role 可以是现有的无线用户角色或自定义的其它用户角色，它驻留在移动网关上。

为了澄清起见，交换机上存在的角色称为 primary role，它是交换机的本地角色，可用于将用户角色属性分配给本地交换的用户或客户端，或是否需要建立隧道将指定客户端或设备流量传输到移动网关。 secondary role 存在于移动网关上，应用于隧道客户端。 例如，如果要将客户端流量通过隧道进行转发，则除了 “gateway-zone” 命令之外，Primary role 还需要包含 secondary role 相关的配置，指示移动网关为该客户端应用何种用户角色。 移动网关在解开隧道封装后，会自动将 secondary role 中的策略和VLAN应用于通过隧道进入的客户端或用户流量。

在RADIUS服务器不是ClearPass的情况下，需要使用本地用户角色。 任何RADIUS服务器都可以返回Aruba-User-Role VSA，当交换机接收到该VSA时，交换机会根据该VSA为用户分配交换机上本地配置的用户角色。 本地角色定义非常灵活和简单，因此也可以用于需要基于位置动态分配vlan (例如建筑楼层) 的场景。

本地用户角色的配置如下所示:

```
class ip camera-ef
     10 match any any any
port-access policy camera-ef
     10 class ip camera-ef action cir kbps 4000 cbs 1000 exceed drop action dscp EF
port-access role camera
     auth-mode client-mode
     associate policy camera-ef
     gateway-zone zone test gateway-role camera
```

注:

- 在上面的示例中，gateway-zone 属性指示交换机将用户所有流量重定向到移动网关，并在移动网关上为用户分配 “camera” 这个用户角色。
- 重定向属性指定的secondary role应预先配置在移动网关上。 在上面的示例中，使用了预定义的角色 “camera”。
- 所有用户策略都包括IPv4和IPv6流量的隐式 “deny all” 规则。 需要创建规则以允许特定端口。 默认情况下，允许在策略中调用未定义任何操作的class。
- 建议在网络中所有需要承载隧道数据包的vlan上使用巨型帧，以避免潜在的分片问题。 如果通过网络发送1518字节的最大标准尺寸的帧，再加上作为GRE报头的46字节，将导致传输的帧超过最大标准帧尺寸。 巨型帧仅在交换机到移动网关的上行链路路径中需要，因为这是用于承载封装数据包 (GRE有效负载) 的链路。 用户VLAN或保留VLAN不需要配置巨型帧。 如果预期客户端会通过隧道发送1518字节的数据包，则巨型帧的建议MTU大小应至少为1564字节。

可下载的用户角色

可下载用户角色允许Aruba交换机直接从ClearPass策略管理器下载用户角色。 这避免了在园区网络中所有交换机配置多个用户角色的工作。 它还使ClearPass成为管理接入交换机用户策略的中心点，同时使交换机上的用户配置最小化。 可下载用户角色通过使用REST API从ClearPass下载与本地用户角色类似的用户属性到交换机上实现用户角色控制功能(请参阅上一节 “本地用户角色”)。 这个过程是基于超文本传输协议安全 (HTTPS) 协议完成的，为了实现安全套接字层 (SSL) 握手，使可下载用户角色正常工作，必须将ClearPass HTTPS证书的签名证书颁发机构 (CA) 添加到交换机并标记为受信任。
在AOS-CX中默认启用了可下载用户角色功能。

创建ClearPass只读管理员账号

建议创建只读管理员账号用于交换机连接Clearpass并下载用户角色。这些账号凭据将用于交换机配置，以创建与Clearpass的安全连接。要创建只读管理员用户，请导航到Clearpass的管理-》用户和权限-》管理员用户-》添加。

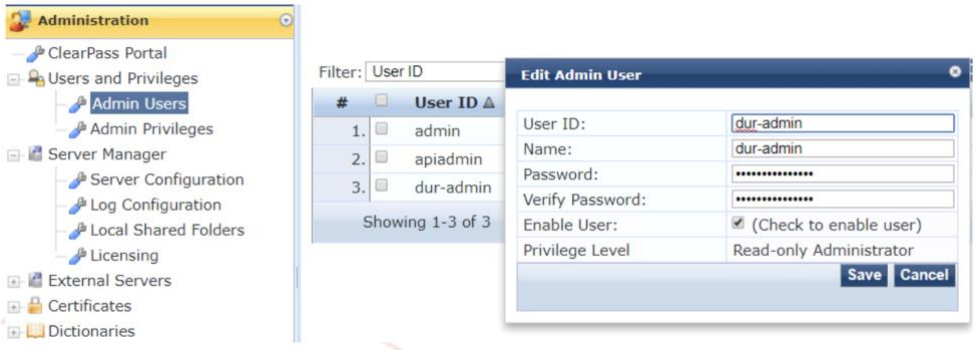

图33: ClearPass只读管理员用户创建

一旦在ClearPass和交换机上创建了凭据，就可以在ClearPass的强制执行配置文件中创建可下载的用户角色。 在ClearPass 6.9和更高版本中，可以通过标准配置模式来创建专门用于AOS-CX交换机的可下载用户角色强制执行配置文件。 而在ClearPass 6.8版本中，则需要使用Mobility Access Switch配置文件和高级配置模式。 要为可下载角色配置强制执行配置文件，请添加新配置文件。 选择 “Aruba Downloadable Role Enforcement” (1)，然后选择 “Standard” (2)，最后选择AOS-CX (3)。 请记住，AOS-CX的标准配置模式仅在ClearPass 6.9及后续版本中支持。

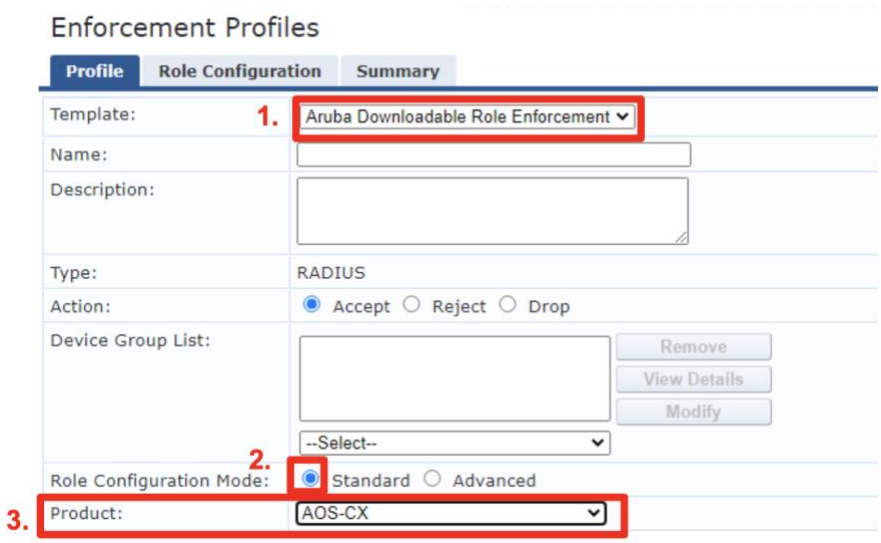

图34: ClearPass强制执行配置文件配置

选择标准配置模式后，可以通过图形化用户界面配置角色，如下所示。

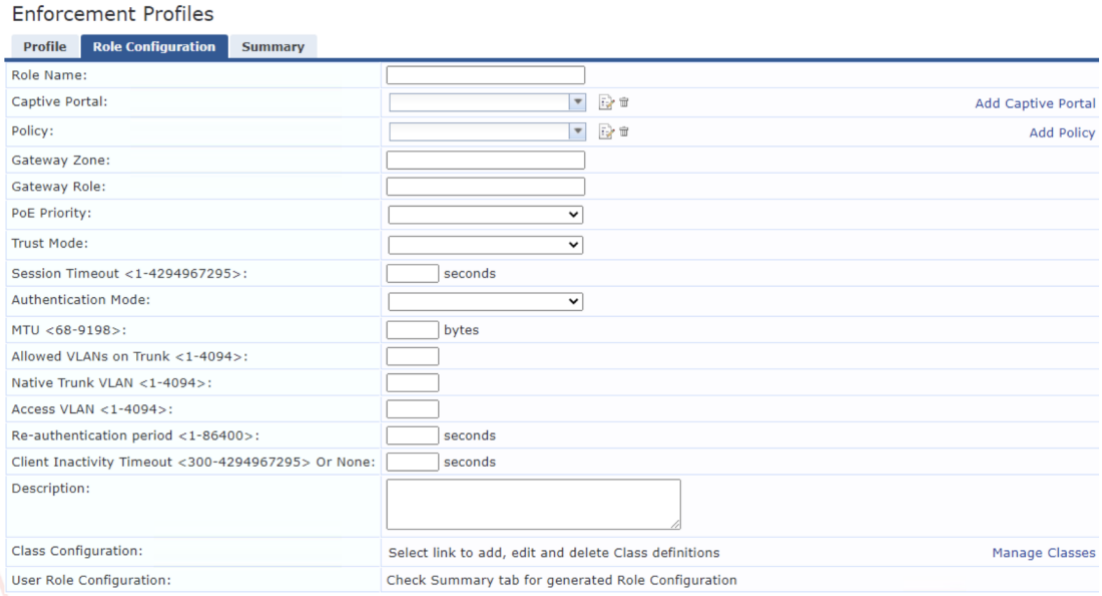

图35: ClearPass标准角色配置-示例

角色的高级配置可以在下面的图中看到。 如先前使用标准配置所做的那样，将使用 “Aruba Downloadable Role Enforcement” 类别 (1) 创建配置文件。 然后，单击 “Advanced” 按钮以配置可下载用户角色 (2)，最后，选择“AOS-CX” (3)。点击 “下一步” 继续。

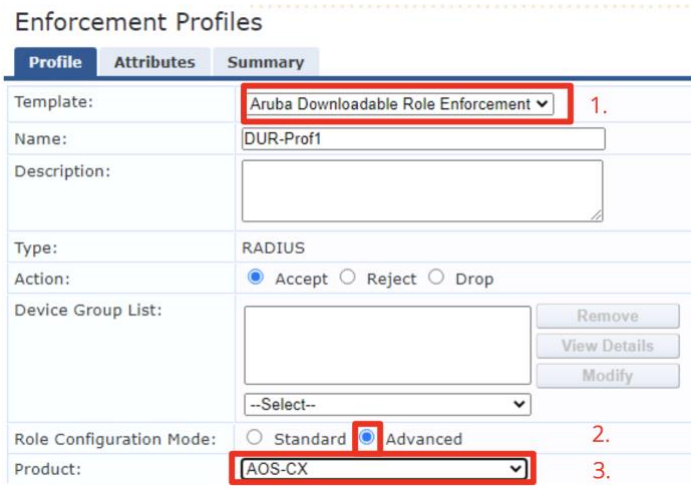

图36: ClearPass可下载用户角色配置文件创建

在图37中，要配置可下载用户角色，请使用RADIUS类型 “Radius: Aruba” (1)。 选择属性名称 “Aruba-CPPM-Role” (2)。 在 “Value” 字段中，输入与AOS-CX 交换机(3)本地用户角色语法完全相同的用户角色配置。 通过单击属性字段右侧的 “软盘” 图标来保存可下载用户角色。

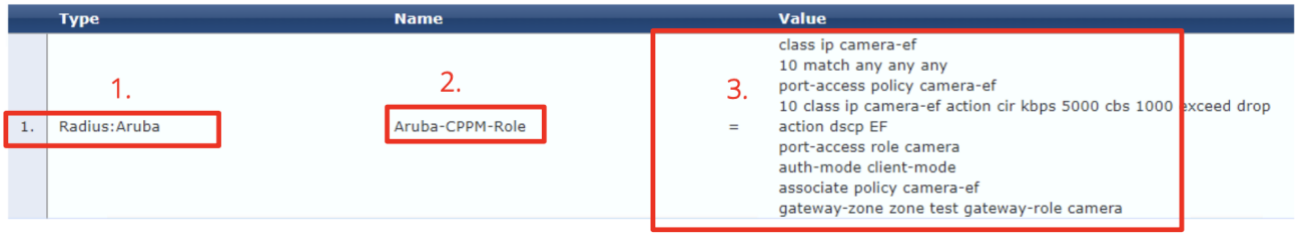

图37: ClearPass可下载用户角色配置文件创建

为了配置交换机以从Clearpass下载用户角色，交换机需要配置以下内容:

- 使用ClearPass FQDN作为证书通用名称 (CN) 签署ClearPass HTTPS证书的根证书 (详细信息如下)。
- 使用Clearpass及其FQDN定义的RADIUS服务器，以及ClearPass的只读管理员登录凭据 (详细信息如下)
- 配置DNS服务器来解析ClearPass FQDN。

交换机配置示例如下：

```
radius-server host aoss-cppm.tmelab.net key ciphertext <encrypted> clearpass-username
admin clearpass-password ciphertext <encrypted> vrf mgmt
```

确认交换机和Clearpass都可以访问到共同的DNS服务器:

```
Switch(config)#ip dns server-address 10.80.2.219
```

注: 也可以使用 “`ip dns host`” 命令。

将根证书复制到Aruba交换机

在交换机中创建受信任的锚配置文件

```
Switch(config)# crypto pki ta-profile <ta profile name>
```

您可以复制并粘贴证书，也可以通过tftp/sftp或USB加载。 首先导航到之前创建的ta配置文件:

```
Switch(config)# crypto pki ta-profile <ta-profile-name>
```

然后，可以通过复制/粘贴导入证书。

```
   Switch(config-ta-cppm)# ta-certificate import
     REMOTE_URL     URL of syntax
                    {tftp://|sftp://USER@}{IP|HOST}[:PORT][;blocksize=VAL]/FILE
     STORAGE_URL    URL of syntax usb:/file
     terminal       Read from the current CLI terminal
     <cr>
```

注意: 如果复制和粘贴，请确保完成后运行命令 Ctrl D 以保存证书。 然后验证证书是否复制正确:

```
Switch(config-ta-cppm)# show crypto pki ta-profile cppm

  TA Profile Name      : cppm
  Revocation Check     : disabled
    OCSP Primary URL: Not Configured OCSP
    Secondary URL: Not Configured OCSP
    Enforcement-level: strict OCSP Disable
    Nonce: false
    OCSP VRF             : mgmt
  TA Certificate       : Installed and valid
   Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            66:20:c0:74:f8:56:42:a3:44:dc:fa:4c:0c:17:13:06
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=net, DC=tmelab, CN=tmelab-AD-CA
        Validity
            Not Before: Mar 29 01:13:08 2017 GMT
            Not After : Mar 29 01:23:08 2022 GMT
        Subject: DC=net, DC=tmelab, CN=tmelab-AD-CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:eb:76:a7:51:d9:04:26:e0:ba:37:8b:f5:fd:6e:
                    f4:ee:e3:57:1f:de:c5:45:cc:f1:67:ef:6e:f3:96:
                    0a:d8:c9:25:d6:b7:2b:d6:33:72:73:7f:a3:f7:16:
                    ca:90:ce:bb:1a:3f:e4:21:94:db:18:31:3a:d8:d9:
                    88:9c:72:6e:c2:f6:03:6c:86:9c:7d:e5:e9:73:5e:
                    c6:76:4c:13:fc:f2:aa:14:3c:3f:45:8c:7e:36:62:
                    09:ea:00:de:b5:fa:8a:66:72:df:1a:46:04:89:85:
                    3b:4a:bf:e5:84:a2:55:6d:2e:02:fd:fc:22:f7:ce:
                    6b:e6:6e:9c:f7:a3:26:23:17:d5:b7:95:eb:29:0f:
                    9d:81:78:46:cf:aa:c0:6b:00:b6:d8:43:2a:71:24:
                    92:e8:9d:9b:ae:78:ce:de:3e:14:98:6c:f9:db:ac:
                    6b:95:f0:cf:41:88:3c:84:c9:0f:3b:39:46:06:82:
                    ae:c9:92:bc:23:ad:ea:fe:04:a6:05:23:1a:89:40:
                    31:db:63:de:a8:cd:b6:94:49:cb:fc:9c:ec:a5:a5:
                    4a:c7:e7:aa:f7:8d:3e:57:9f:4e:49:0d:d3:88:26:
                    f0:4a:9e:26:0a:67:12:0a:fa:6e:0c:bf:65:d2:d3:
```

```
                    3c:6e:64:11:b5:17:56:03:97:f6:dc:43:7e:77:8d:
                    ac:db
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage:
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                2E:06:33:B3:D0:BA:42:00:BC:64:83:2F:5B:59:BC:E2:57:ED:43:50
            1.3.6.1.4.1.311.21.1:
                ...
    Signature Algorithm: sha256WithRSAEncryption
         c9:d5:51:f3:a6:19:7b:3f:4d:b8:8b:c9:39:fb:4b:73:3b:b4:
         cb:76:1f:1a:80:39:3c:af:3c:62:fd:d3:48:cb:fe:83:12:b9:
         ca:27:1e:53:61:e4:57:73:ef:55:e0:97:c8:df:4d:9f:d1:14:
         28:b2:7c:f3:bf:c1:a8:34:ec:34:a2:83:db:46:b1:1c:d9:3f:
         c3:6a:79:23:c2:d8:ea:0f:d8:f2:dd:cd:f3:88:17:c7:7e:37:
         f7:e1:9e:cc:17:65:c7:39:c4:99:60:21:79:b0:10:fc:93:27:
         a7:e6:83:f5:78:70:f6:d8:06:78:35:cc:07:f1:88:87:1d:0f:
         08:ad:b6:55:b4:54:a0:37:99:3f:7a:3e:2e:67:41:d9:f3:9d:
         aa:17:cd:f3:e7:b6:38:ca:73:00:6b:01:18:61:09:25:6a:8e:
         29:25:24:1c:2d:b9:26:49:74:45:fc:b2:99:dc:6e:58:47:e5:
         1e:87:db:17:60:e3:49:68:5e:47:4d:b7:03:97:40:e9:ae:56:
         93:14:d5:ed:6c:70:0b:c7:a4:8a:d9:e5:63:90:53:d9:91:d5:
         d4:b5:cb:52:c8:2f:b8:dd:e3:f0:6d:be:ca:f6:22:4b:a6:7f:
         75:ad:ce:45:be:86:ae:6e:fd:b2:a6:69:ce:52:99:5d:68:d4:
         ff:35:71:05
```

使用Windows Server签署ClearPass签名请求

注意: 为了使用此过程，假定已在Windows Server上配置并安装了证书服务。

使用Microsoft Windows Server 2016标准测试了以下过程。 这可能适用于其他版本的Windows Server，并在步骤中有所不同。此过程利用已安装在Windows Server中的根证书。

步骤1: 从ClearPass策略管理器生成证书签名请求 (CSR)

- 导航到ClearPass策略管理器中的 “管理” 和 “服务器证书”
- 单击 “选择类型”，然后选择 “HTTPS服务器证书” (1.)，然后单击 “创建证书签名请求” (2.)

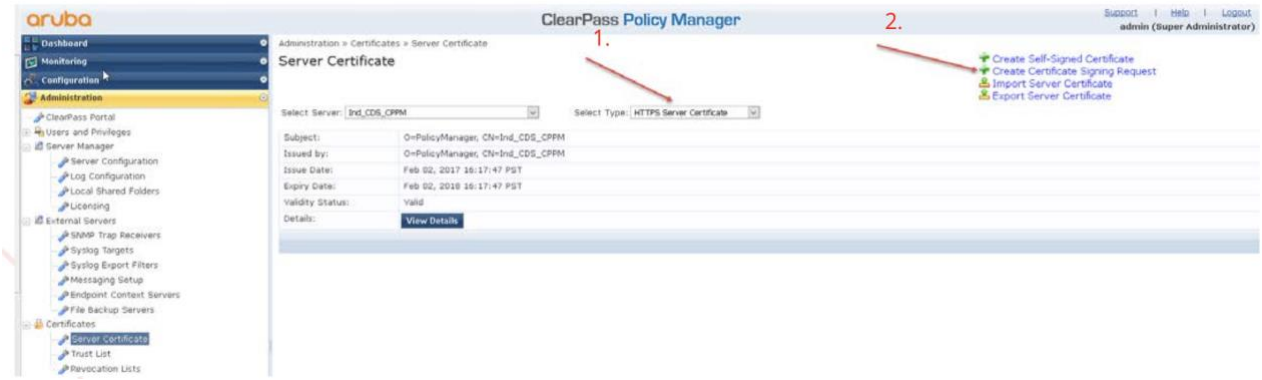

图38: CPPM HTTPS服务器证书和证书签名请求创建

步骤2: 在签名请求中添加适当的信息 (通用名称、组织单位、私钥等)，然后单击提交

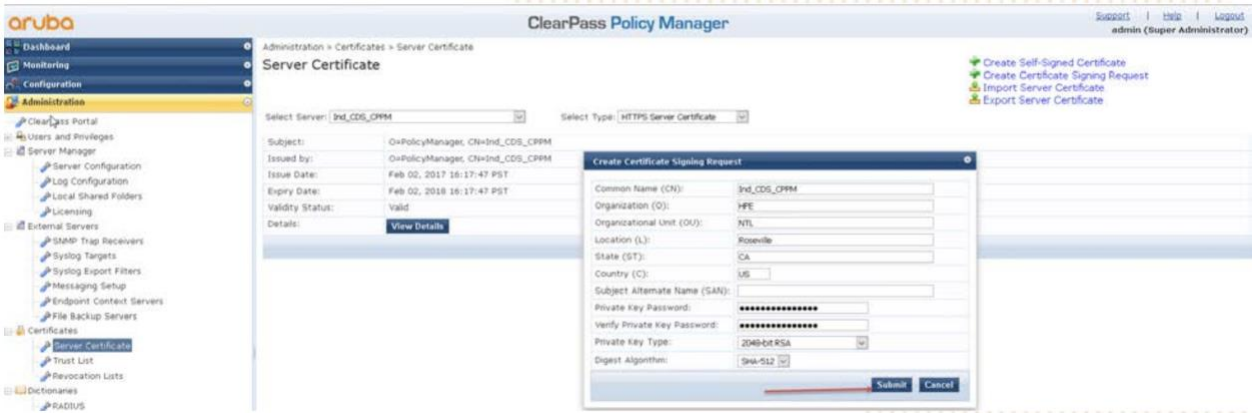

图39: CPPM证书签名请求向导

步骤3： 选择 “Download CSR and Private Key File” 后，可以得到由ClearPass生成的两个文件 CertSignRequest.CSR 和 CertPrivKey.pkey - 可能取决于浏览器

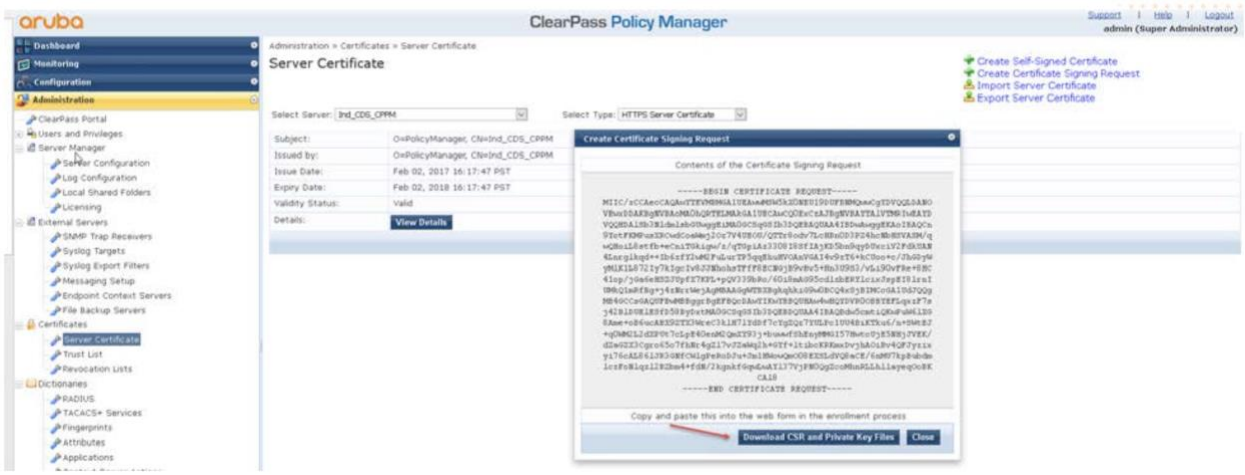

图40: CPPM证书签名请求向导

步骤4: 使用Windows Server 2016标准版签署证书

在Windows Server中打开web浏览器，导航到https:// localhost/certsrv/,然后点击 “申请证书”。

图41: Windows Server证书管理页面

步骤5: 点击 “高级证书申请”

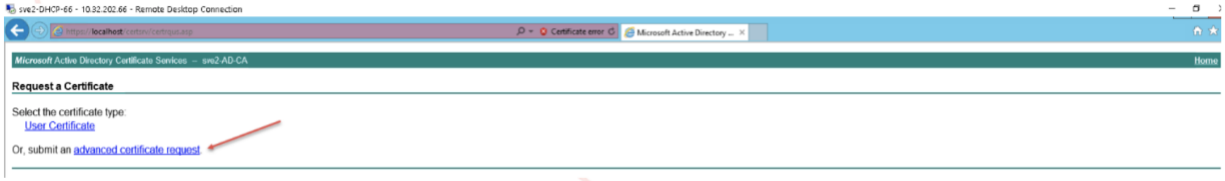

图42: Windows Server高级证书请求

步骤6: 点击 “使用基于64编码的CMC或PKCS #10文件提交证书请求，或者使用基于64编码的PKCS #7文件提交续订请求。”

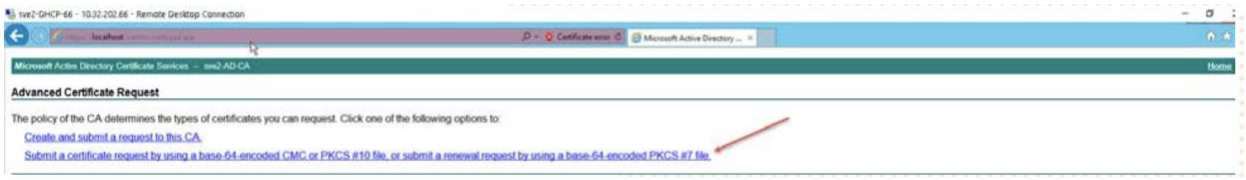

图43: Windows Server提交base-64证书请求向导

步骤7: 复制步骤3中ClearPass生成的CSR请求，然后单击提交

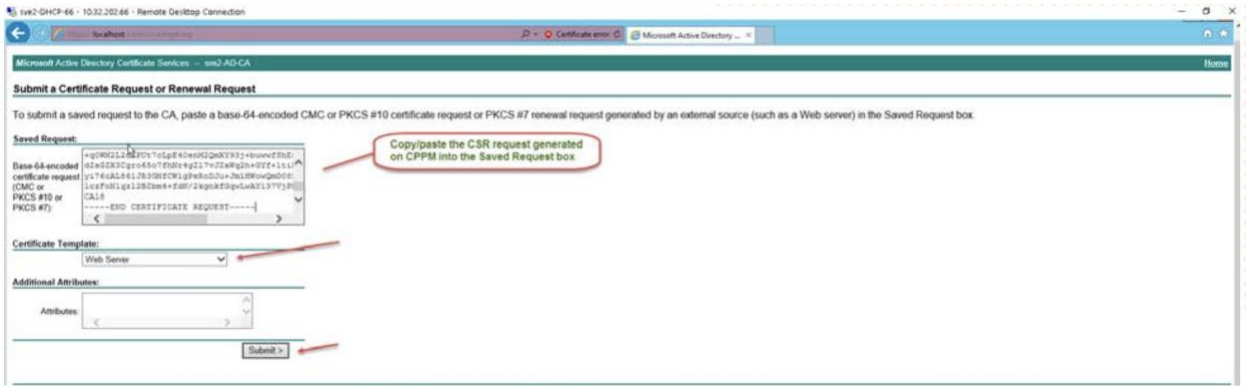

图44: Windows Server将证书签名请求 (CSR) 复制到证书请求向导中

步骤8: 点击 “Base 64编码” 和 “下载证书链”

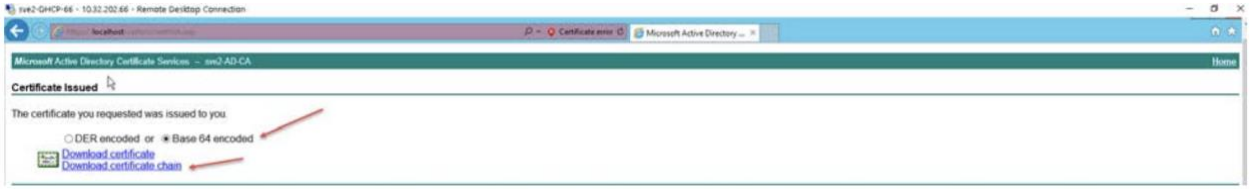

图45: Windows Server完整证书请求和下载证书链

步骤9: 证书应该在 “证书管理器” 中自动打开 -- 根证书和服务器证书都应该出现

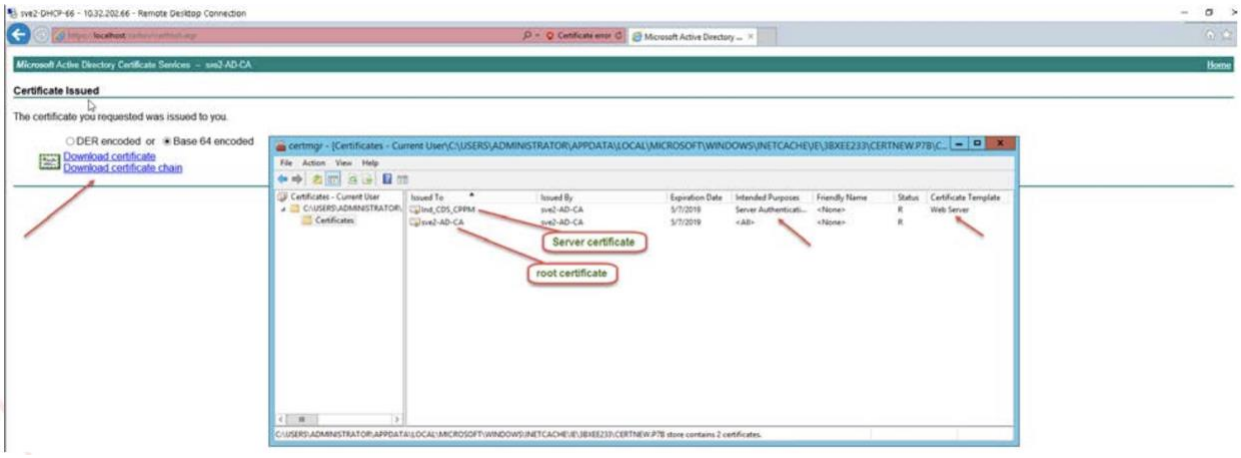

图46: Windows Server证书管理器

步骤10: 鼠标右键单击服务器证书 (顶部)，鼠标左键单击导出，将出现证书导出向导。 单击下一步

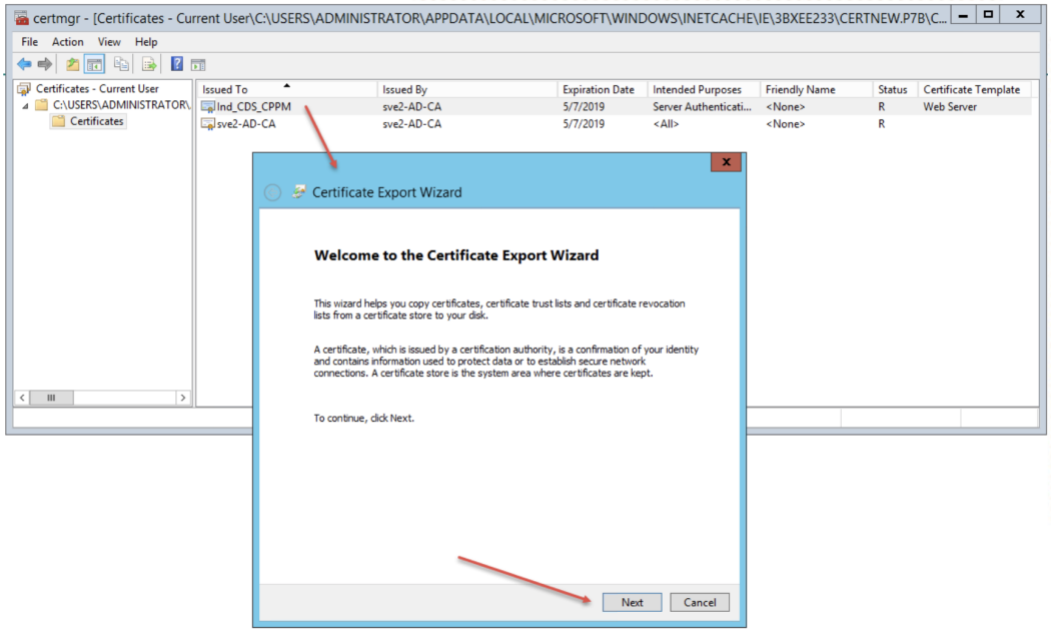

图47: Windows Server证书导出向导

步骤11: 选中 “Base-64编码的X.509 (.CER)，然后单击“ 下一步 ”。

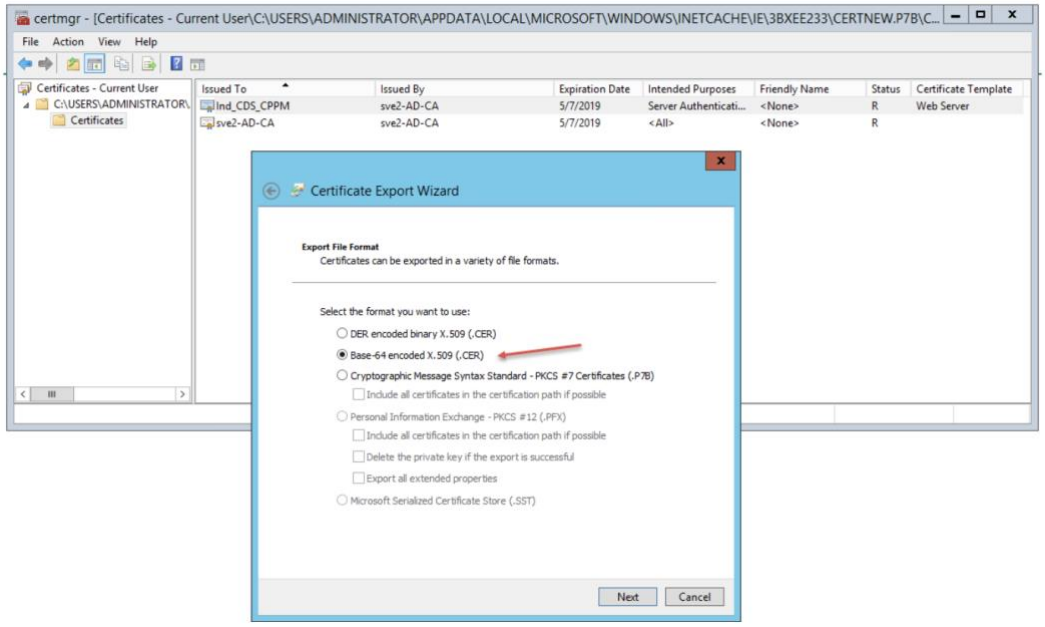

图48: Windows Server证书导出向导-Base 64编码选择

33

步骤12: 浏览到要存储的HTTPS服务器证书的目的地。 单击 “下一步”。

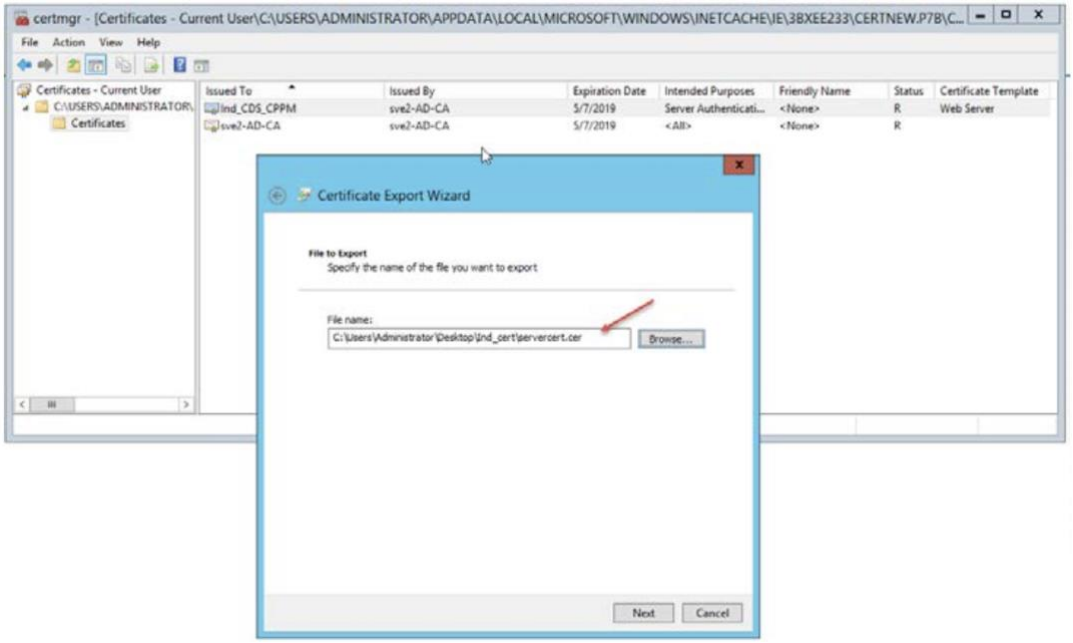

图49: Windows Server证书导出向导文件目标

步骤13: 单击Finish退出证书导出向导

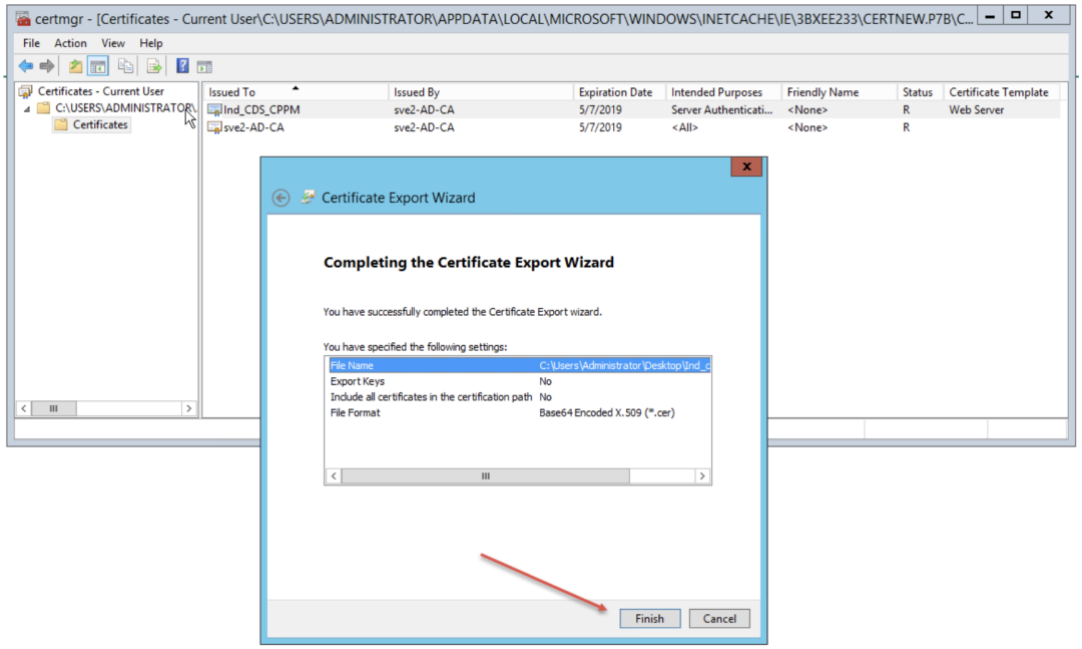

图50: Windows Server证书导出向导完成

步骤14: 重复步骤10-13导出根证书。

步骤15: 将根证书复制到ClearPass信任列表

注意: 可能需要使用FTP或SCP复制文件，以便ClearPass可以从远程访问它们。 复制/粘贴适用于微软的远程桌面连接。

选择管理-》信任列表-》添加

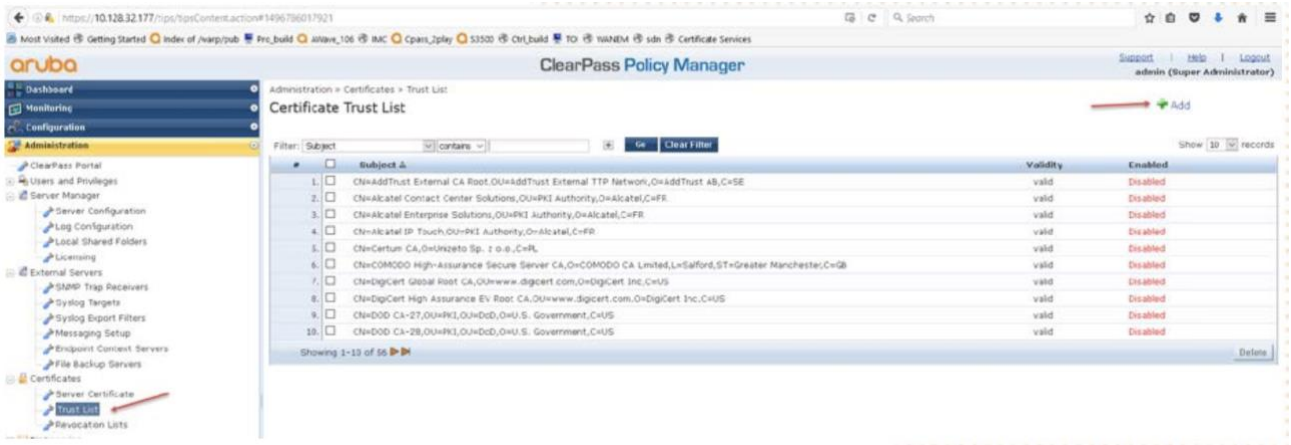

图51: CPPM将根证书添加到信任列表

- 要将根证书添加到信任列表中，请选择 “添加” (1)，然后选择 “浏览” (2) 以从本地选择要安装的证书，并选择 “添加证书” 以将根证书安装到信任列表中 (3)。

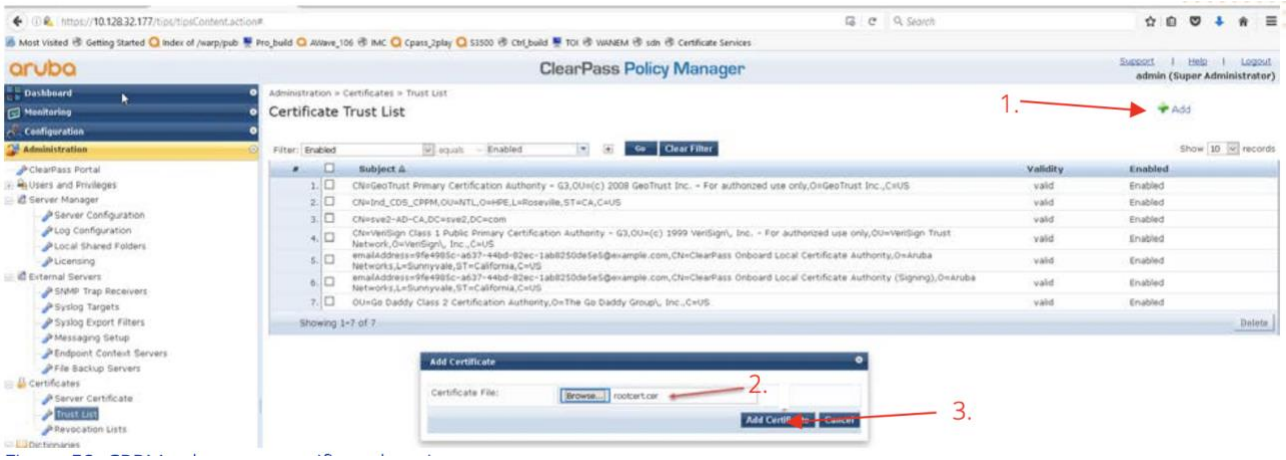

图52: CPPM选择根证书位置

步骤4: 将HTTPS服务器证书添加到ClearPass

1. 导航到管理-》服务器证书-》选择“HTTPS服务器证书”
2. 选择 “导入服务器证书”
3. 找到在步骤10-13中创建的服务器证书 - 可能需要从Windows服务器中复制
4. 找到在步骤3中创建的私钥文件
5. 输入私钥密码

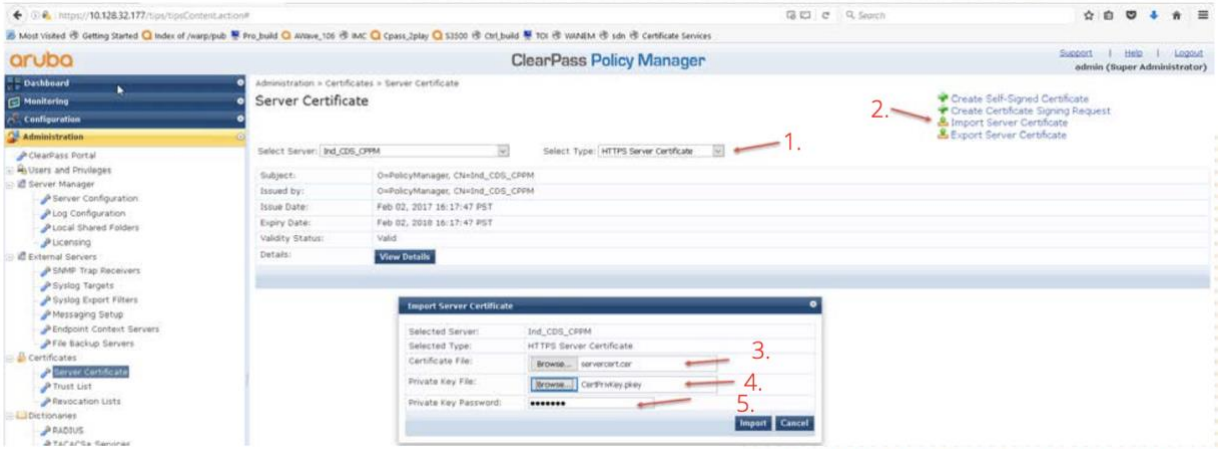

图53: CPPM添加HTTPS服务器证书和私钥文件

使用OpenSSL签署ClearPass证书签名请求

*注意:本节仅用于演示。应始终在生产环境中使用受信任的证书。有关证书和ClearPass的更多信息，请参阅《ClearPass用户指南》-*https://www.arubanetworks.com/techdocs/ClearPass/ 6.8/PolicyManager/index.htm

步骤1: 从ClearPass策略管理器生成证书签名请求 (CSR)

- 导航到ClearPass策略管理器中的 “管理” 和 “服务器证书”
- 单击 “选择类型”，然后选择 “HTTPS服务器证书” (1.)，然后单击 “创建证书签名请求” (2.)

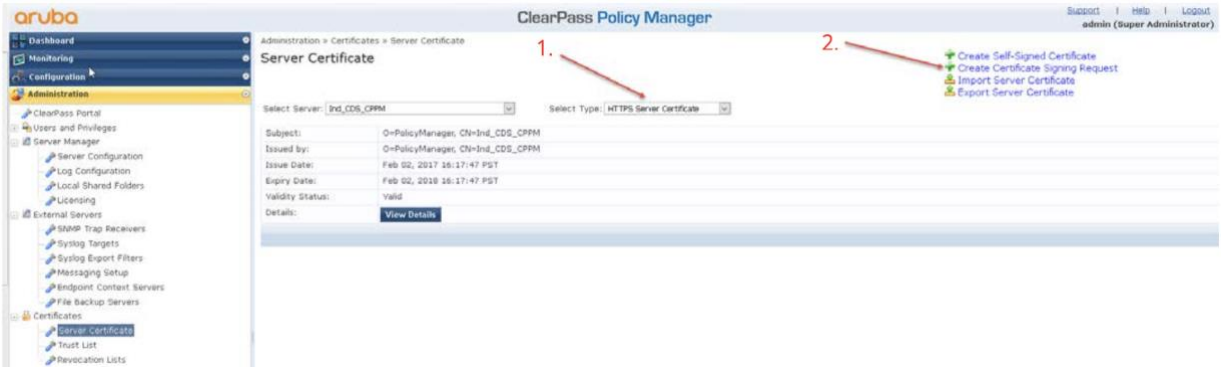

图54: CPPM HTTPS服务器证书和证书签名请求创建

- 在签名请求中添加适当的信息 (通用名称、组织单位、私钥等等;)

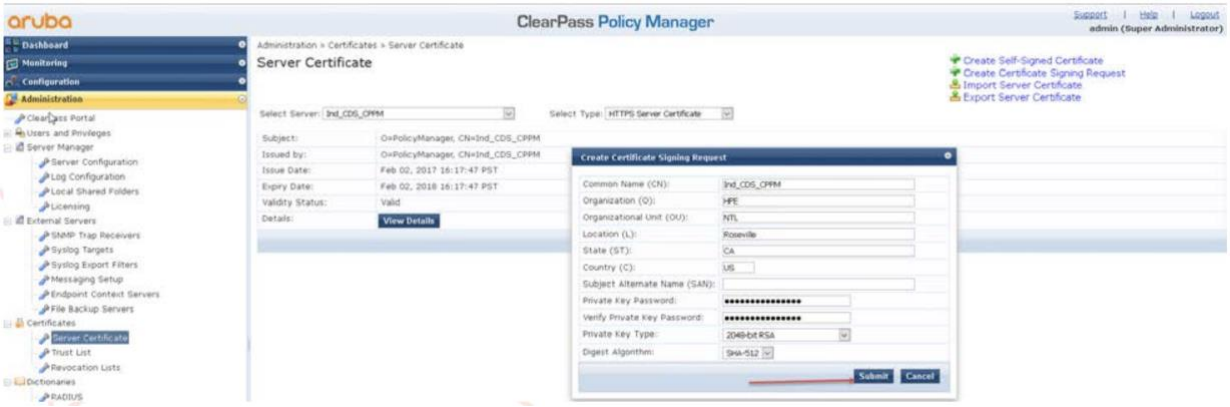

图55: CPPM创建证书签名请求向导

- 然后，选择 “Download CSR and Private Key File ”，可以获得由ClearPass生成的两个文件，

CertSignRequest.CSR 和 CertPrivKey.pkey - 可能取决于浏览器

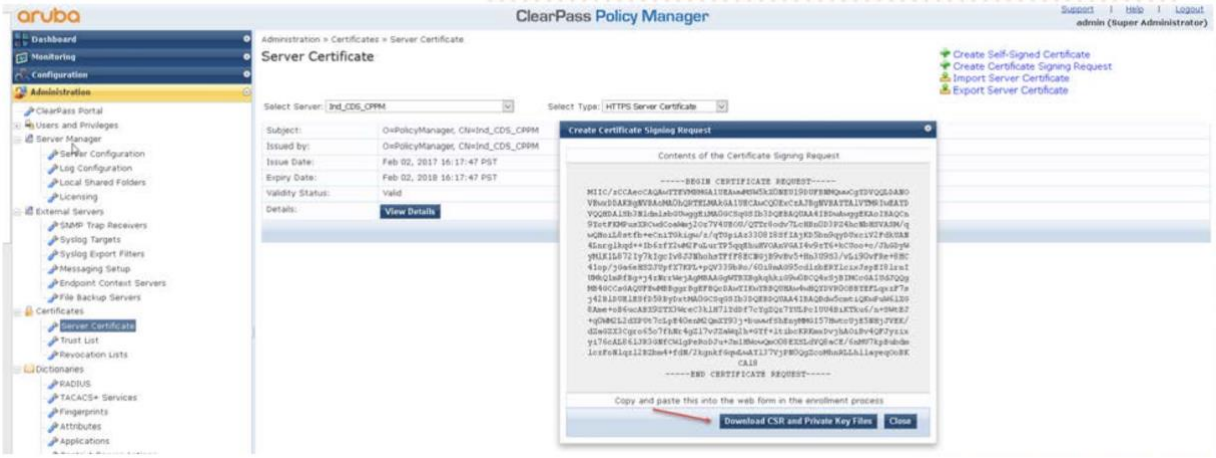

图56: CPPM证书签名请求内容

步骤2: 在CentOS中通过OpenSSL签署ClearPass签名请求 (.csr)

- 将步骤1中生成的CSR文件复制到CentOS目录/etc/pki/tls/misc中 （可能需要使用SCP或FTP）
- 使用以下命令在OpenSSL中签署证书:

```
sudo openssl x509 -req -days 900 -in CertSignRequest.csr -CA rootcert.pem -CAkey
../../CA/private/cakey.pem -CAcreateserial -out servercert.pem
```

注意:

- “-days” 参数将确定证书的到期时间
- 确保与根证书存在于同一目录中 （例如/etc/pki/tls/misc）
- ../../CA/private/cakey.pem指的是在步骤1中创建的私钥
- servercert.pem指的是将创建的新的HTTPS签名证书

步骤3: 将根证书复制到ClearPass信任列表

注意: 可能需要使用FTP或SCP复制文件，以便ClearPass可以从远程访问它们。

- 选择管理-》信任列表-》添加

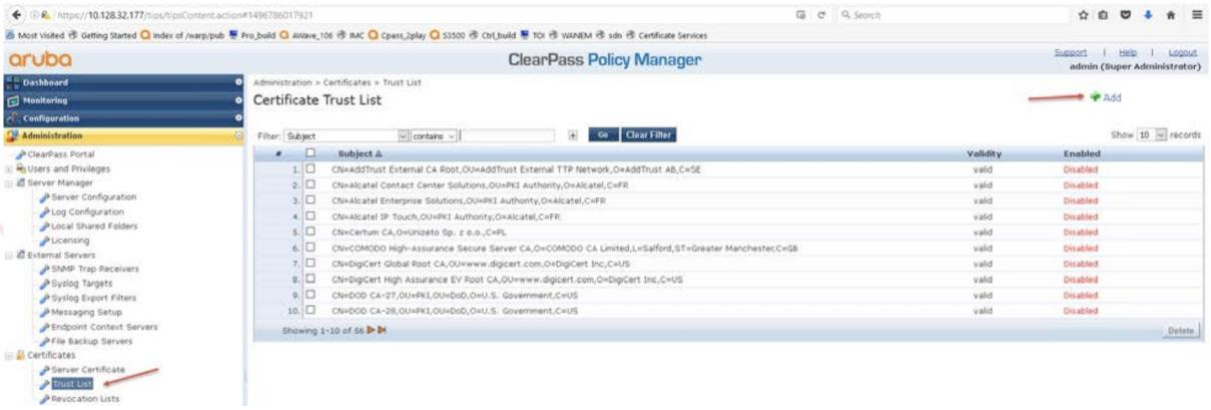

图57: CPPM信任列表

- 要将根证书添加到信任列表中，请选择 “添加” (1)，然后选择 “浏览” (2) 以获取要安装的证书，并选择 “添加证书” 以将根证书安装到信任列表中 (3)。

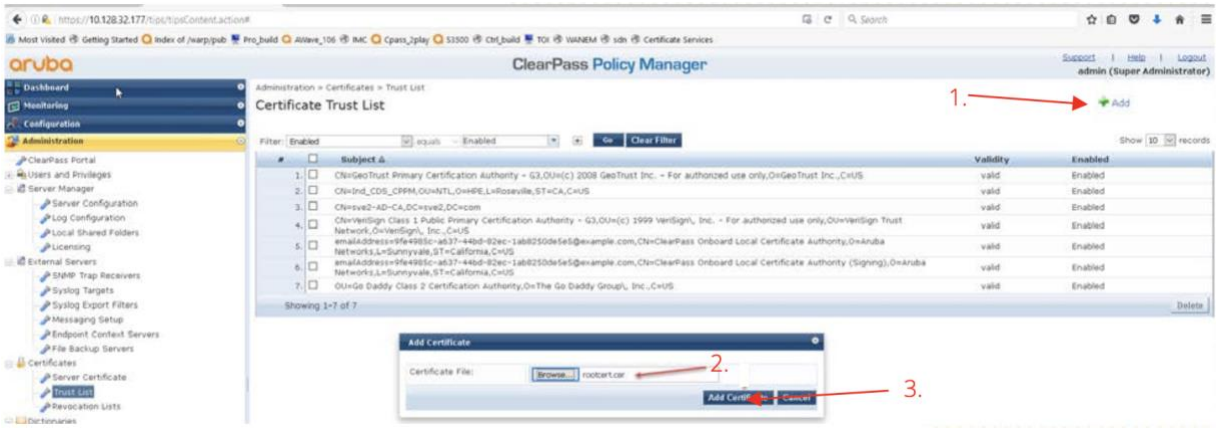

图58: CPPM将根证书添加到信任列表

步骤4: 将HTTPS服务器证书添加到ClearPass

1. 导航到管理-》服务器证书-》选择“HTTPS服务器证书”
2. 选择 “导入服务器证书”
3. 找到在步骤2中创建的服务器证书-可能需要从CentOS复制
4. 浏览到在步骤1中创建的私钥文件
5. 输入私钥密码

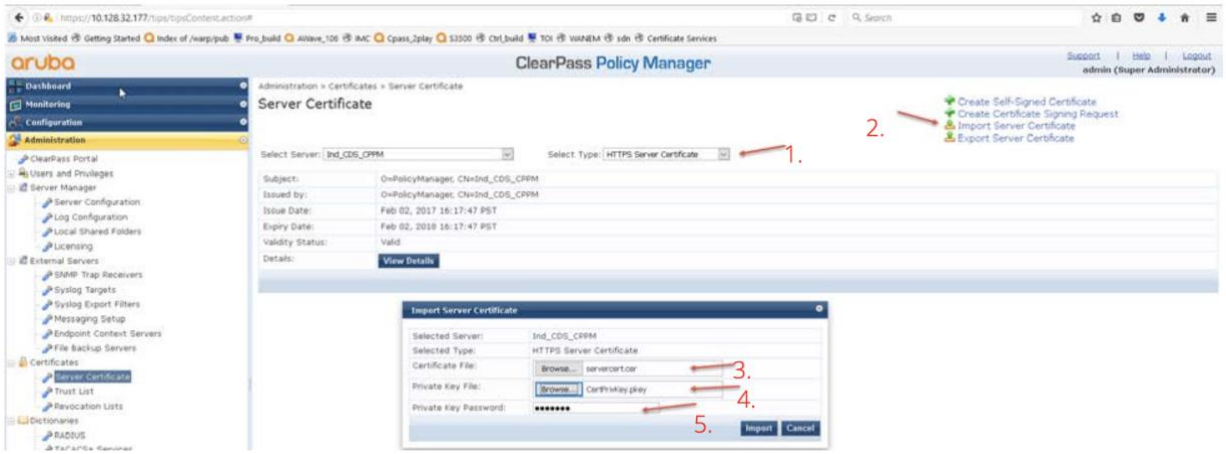

图59: CPPM添加HTTPS服务器证书

注意: 这是最不安全的方法，它是没有证书颁发机构签署证书时的一种解决方法，建议仅用于演示目的。

从CentOS中的OpenSSL创建根证书

这些步骤已通过CentOS 7虚拟机进行了验证。 这个经过测试的CentOS 7版本带有默认的OpenSSL版本1.0.k-fips (2017年1月26日)。 这些步骤可能会因Linux/Unix或MacOS X的发行而异。

步骤1: 确保您有一个运行CentOS的电脑。

步骤2:在 “Terminal”中，使用以下命令更改到/etc/pki/tls/misc目录 （可能会因所使用的Linux操作系统而异）:

```
cd /etc/pki/tls/misc - OpenSSL的默认路径
```

步骤3: 从 “misc” 目录中输入以下命令以创建证书文件并设置权限:

```
touch ../../CA/serial
```

```
chmod 777 ../../CA/serial
touch ../../CA/cacert.pem
chmod 777 ../../CA/cacert.pem
touch ../../CA/private/cakey.pem
chmod 777 ../../CA/private/cakey.pem
touch ../../CA/index.txt
chmod 777 ../../CA/index.txt
echo 1000 > /etc/pki/CA/serial
chmod 600 ../../CA/index.txt /etc/pki/CA/serial /etc/pki/tls/openssl.cnf
```

步骤4: 生成新的根证书。

```
./CA -newcert
```

步骤5： 将newcert.pem （在步骤4中生成的证书） 文件复制到cacert.pem

cp newcert.pem ../../CA/cacert.pem

cp: overwrite `../../CA/cacert.pem'? y - 如果文件已经存在

步骤6: 将newkey.pem (在步骤4中生成的私钥) 复制到cakey.pem中

```
cp newkey.pem ../../CA/private/cakey.pem
```

cp: overwrite `../../CA/private/cakey.pem'? y - 如果文件已经存在

步骤7: 使用文本编辑器 (vi，vim，emacs，gedit ……)，将cacert.pem的内容复制到新文件中，并另存为pem文件 (例如 rootcert.pem)

图60: Gedit示例: 将cacert.pem内容粘贴到新的PEM文件中

用户角色故障排除

常用的用户角色故障诊断命令:

- Debug portaccess role
- Debug destination buffer (or console)
- Show debug buffer

常见的用户角色错误代码:

- 错误代码35 - 此错误显示在debug日志中，并指示交换机和ClearPass之间的时间存在偏差，或者证书下载/安装存在问题。
- Parsing the XML for the cprole <role name> failed - 检查交换机上配置的Clearpass只读帐户和密码是否正确

可扩展性

移动网关

表3 - 移动网关扩展能力

移动网关	最大支持隧道数
7280	32768
7240 /7240XM	32768
7220	16384
7210	8192
7205	4096
7030	1024
7024	512
7010	512
7008	256
7005	256

交换机

表4 - 交换机扩展能力

交换机/堆叠	每个交换机或堆栈支持的最大用户隧道数	每个端口支持的最大用户隧道数
6200	1024	32
6300F/M	1024	256
6400	1024	256

性能（每个交换机1024个隧道用户）

表5 - 1024隧道用户时的性能

数据包尺寸(字节)	每个端口隧道用户	交换机中的隧道用户总数	32端口Tx/Rx Rx吞吐量平均值 (Gbps)	平均延迟(ms)
256	32	1024	13.195	1.071
512	32	1024	26.447	0.982
1024	32	1024	31.387	0.031
1280	32	1024	31.508	0.035
1518	32	1024	31.584	0.038

常见问题

1) 在移动网关集群中，交换机如何确定将用户流量发送到哪个网关？
   a. 在交换机引导过程中，SAG将bucket map发送到交换机。 此映射是256条目的数组，每个条目都包含要使用的主用网关和备用网关。 用户的mac地址被散列到此表中，以获取将用户流量隧道到的移动网关地址。
2) 交换机从什么时候开始发送与SAG和S-SAG之间的心跳？
   a. 心跳在具有特定GRE key (0xDEED) 的GRE隧道上传输。 交换机完成引导后会立即发起SAG和S-SAG心跳。
3) 与SAG心跳失败时会发生什么？
   a. 心跳失败会触发交换机采取以下动作:

i. 移除锚定到SAG的用户

ii. 故障切换到S-SAG (例如: S-SAG现在成为新的SAG)

4) 当UAG的keepalive失败时会发生什么？

a. 锚定到UAG的用户将被删除，并在事件日志中进行消息记录。

5) 是否应该在交换机上启用巨型帧？

a. 建议在隧道数据包的数据路径上启用巨型帧。 当分组大小达到1468字节时，加上GRE报头具有的46字节报头，将使分组接近标准MTU最大值。 如果不希望在网络中设置巨型帧，则Aruba移动网关可以对TCP流量进行tcp-mss重写。 但是，如果在其他类型的流量中看到更大的数据包，则可能会看到数据包丢失。 如果期望客户端发送大于1518字节的数据包，则推荐的MTU不小于1564字节。

b. 巨型帧TCP MSS重写场景 (移动网关上的TCP重写)

表6-巨型帧TCP MSS重写方案

位于交换机和网关之间的基础设施	移动网关	交换机客户端VLAN	Windows客户端MTU	移动网关TCP mss重写	ICMP
Jumbo	Jumbo	Jumbo	9014字节	没有发生重写，因为客户端发送的mss不超过隧道->mtu-114	在更大的数据包中没有观察到任何问题
Jumbo	No Jumbo	Jumbo	9014字节	没有发生重写，因为移动网关上隧道mtu设置为9198	ICMP直到1706字节 (ping 1664字节)之前工作正常，之后不通过网关转发报文
Jumbo	Jumbo	No Jumbo	默认	没有发生重写，因为移动网关上隧道mtu设置为9198	没有观察到任何问题
Jumbo	No Jumbo	No Jumbo	默认	没有发生重写，因为移动网关上隧道mtu设置为9198	没有观察到任何问题
No Jumbo	Jumbo	Jumbo	9014字节	当客户端发送的mss大于隧道->mtu-114时，网关重写发生	由于隧道开销为46字节，报文超过1468字节时发生丢包
No Jumbo	No Jumbo	Jumbo	9014字节	当客户端发送的mss大于隧道->mtu-114时，网关重写发生	由于隧道开销为46字节，报文超过1468字节时发生丢包
No Jumbo	Jumbo	No Jumbo	默认	当客户端发送的mss大于隧道->mtu-114时，网关重写发生	由于隧道开销为46字节，报文超过1468字节时发生丢包
No Jumbo	No Jumbo	No Jumbo	默认	当客户端发送的mss大于隧道->mtu-114时，网关重写发生	由于隧道开销为46字节，报文超过1468字节时发生丢包

6) 当UAG网关不可达时会发生什么？

a. SAG将节点列表更新发送到交换机，以通知UAG网关已关闭。 锚定到该网关的所有用户都将被删除。一段时间后，SAG网关会向交换机发送bucket map更新。 然后，交换机处理bucket map更新，并根据bucket

map将用户锚定到相应的网关 (备用)。

注意: 重要的是要验证交换机和网关上的bucket map是否相同。 另外，应验证用户是否已锚定到正确的网关，如交换机和网关上的bucket map所示。

7) 当SAG网关不可达时会发生什么？

   a. 节点列表更新由S-SAG发送给switch。 由于节点列表是从S-SAG而不是SAG接收的，因此交换机认为SAG已停止服务并启动到S-SAG的故障切换。 此外，该交换机会删除锚定到SAG的所有用户。 一旦S-SAG确认故障切换请求，S-SAG就成为新的主用SAG。 然后，新的主用SAG发送节点列表更新和bucket map更新。 在节点列表更新中，将提供新的S-SAG。 然后，交换机将引导并与新的S-SAG建立心跳。 之后，交换机处理bucket map更新，并将用户锚定到相应的网关。

   注意: 重要的是要验证交换机和网关上的bucket map是否相同。 另外，应验证用户是否锚定在交换机和网关上的bucket map中标识的正确网关。

8) 当S-SAG网关不可达时会发生什么？

   a. 节点列表更新由SAG发送到交换机。 该交换机停止与S-SAG之间的心跳，并删除锚定在其上的所有用户。 然后，交换机将启动引导到节点列表更新中提供的新S-SAG。 一旦收到引导确认，交换机就会开始与新的S-SAG建立心跳。 一段时间后，SAG将发送bucket map更新。 然后，交换机处理更新并将用户锚定到其各自的网关。

   注意: 重要的是要验证交换机和网关上的bucket map是否相同。 另外，应根据交换机和网关上的bucket map验证用户是否已锚定到适当的网关。

9) “`show ubt state`” 中的状态是什么意思？

   a. 正在注册 - Bootstrapping

   b. 已注册 - Bootstrapped

   c. 未注册 – Un-Bootstrapping

10) 当用户角色属性改变时会发生什么？

   a. 为应用了该角色的用户启动重新引导，该角色包含引导数据包中更新的角色属性。 这些用户状态变更为“正在注册” 状态。 一旦从移动网关接收到确认消息，用户状态再次变更为 “已注册” 状态。 这仅适用于VLAN和secondary role的更改。

11) 客户端 “MAC地址移动” 会发生什么？

   a. 为客户端启动重新引导。 仅在收到来自移动网关的确认后，客户端流量才开始隧道传输。

12) 隧道客户端VLAN配置的建议是什么？

   a. 使用保留的VLAN，无需在用户角色中专门添加VLAN配置，所有隧道化的流量将通过保留VLAN发送。 VLAN分配将通过网关用户角色在网关进行

13) 如何使用QoS对隧道数据包进行优先级排序？

   a. 参见第23页。

14) “我看到交换机上用户状态是 '已注册' ，但对ping没有反应。 如何调试？”

a. 检查交换机和网关是否正确配置了用户角色和vlan。

检查从隧道交换机到移动网关的路径中的所有交换机的IP MTU设置为> = (1500 + 46)。

由于解决方案有两个部分，因此我们需要确切地知道哪个部分的行为不正确。 要确定交换机是否正在隧道传输流量，请使用 “show ubt statistics” 命令检查是否正在接收和传输用户流量。 如果计数器没有增加，则需要分析交换机配置。

在移动网关: 检查 “show datapath tunnel”，以查看 “Encaps” 和 “Decaps” 计数器是否增加。

对交换机到移动网关的上行链路上发送和接收到网关的流量进行数据包跟踪也是有帮助的，GRE封装的数据包将会有所帮助。

15) 需要打开哪些防火墙端口才能启用基于用户的隧道？

a. 确保Aruba交换机和移动网关之间的网络允许PAPI (UDP 8211)，GRE (协议47) 和ICMP (Echo-Request/Echo-Reply)。

16) 备份网关IP是干什么用的？

a. 如果主用网关(交换机锚网关) 由于各种原因碰巧 “脱机”，则备用交换机锚网关将自动接管作为主用网关，并且选择新的移动网关作为备用网关 (如果可用)，直至整个集群所有移动网关都不可达。 在ubt-zone配置中看到的备份网关IP命令用于在整个集群处于脱机状态的情况下为交换机提供额外的备份网关或集群，用于故障切换。

17) 每个隧道使用多少个TCAM条目？

a. 每个用户隧道一个TCAM条目:

```
Switch(config-if)# show resources
Resource Usage:
Mod  Description
         Resource                                      Used     Free

1/1  L2 Tunnel Lookup
         Ingress TCAM Entries                           4     1013
     Total
         Ingress Lookups                                1        4
         Egress Lookups                                 0        4
Switch(config-if)# sho ubt state

Local Master Server (LMS) State:
LMS Type      IP Address    State
Primary     : 10.5.8.6   ready_for_bootstrap


Switch Anchor Gateway (SAC) State:

              IP Address      MAC Address          State

Active      : 10.5.8.6        00:0b:86:b7:6a:7f    Registered
Standby     : 10.5.8.7        00:0b:86:dd:6c:00    Registered

User Anchor Gateway(UAG): 10.5.8.7
User               Port    State                          Bucket ID  Gre Key

d4:c9:ef:f8:1b:0d   1/1/4  registered                      238        4

User Anchor Gateway(UAG): 10.5.8.6
```

```
User                Port     State                        Bucket ID  Gre Key

2c:41:38:7f:51:45   1/1/3    registered                   107          3
10:60:4b:47:1e:6a   1/1/3    registered                   51           3
00:1e:58:a8:6b:f6   1/1/2    registered                   53     2
```

a Hewlett Packard Enterprise company

www.arubanetworks.com

斯科特大道3333号 圣克拉拉，CA 95054

1.844.472.2782 | 电话: 1.408.227.4500 | 传真: 1.408.227.4550 |info@arubanetworks.com