配置ISE 2.0第三方与Aruba无线集成

目录

简介

先决条件

- 要求
- 使用的组件

配置

- 网络图
- 第三方支持的挑战
  - 会话
  - URL重定向
  - CoA
  - ISE解决方案
- 思科ISE
  - 步骤1.将Aruba无线控制器添加到网络设备
  - 步骤2.配置授权配置文件
  - 步骤3.配置授权规则
- Aruba AP
  - 步骤1.强制网络门户配置
  - 步骤2. Radius服务器配置
  - 步骤3. SSID配置

验证

- 步骤1.连接到SSID mgarcarz_arubawith EAP-PEAP
- 步骤2.BYOD的Web浏览器流量重定向
- 步骤3.执行网络设置助理

其他流和CoA支持

- 带CoA的CWA

故障排除

- 具有IPAddress而非FQDN的Aruba强制网络门户
- Aruba强制网络门户访问策略不正确
- Aruba CoA端口号
- 某些Aruba设备上的重定向

相关信息

简介

本文档介绍如何对思科身份服务引擎(ISE)上的第三方集成功能进行故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- Aruba IAP配置
- ISE上的自带设备流
- 密码和证书身份验证的ISE配置

使用的组件

本文档介绍如何对思科身份服务引擎(ISE)上的第三方集成功能进行故障排除。

它可以作为与其他供应商和流程集成的指南。ISE版本2.0支持第三方集成。

本配置示例展示如何将Aruba IAP 204管理的无线网络与ISE集成以实现自带设备(BYOD)服务。

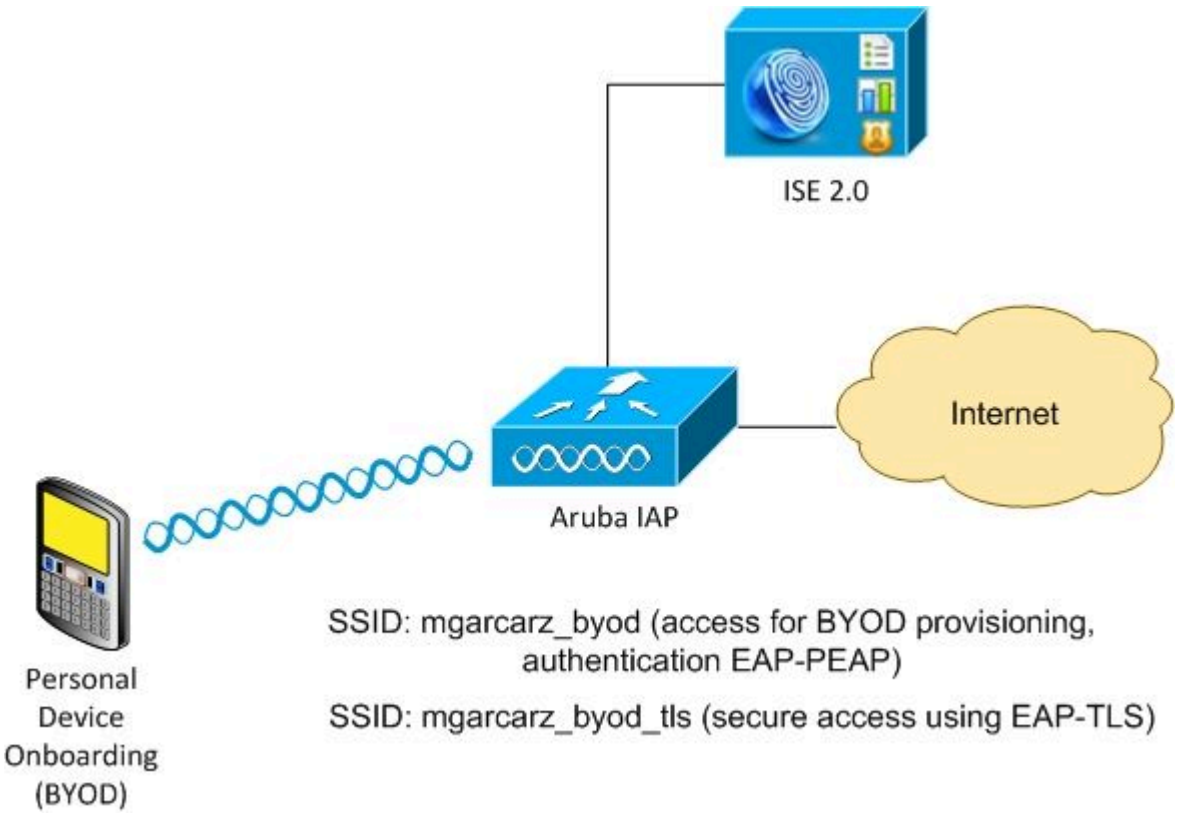
本文档中的信息基于以下软件版本：

- Aruba IAP 204软件6.4.2.3
- 思科ISE版本2.0及更高版本

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图



有两个无线网络由Aruba AP管理。

第一个(mgarcarz_byod)用于802.1x可扩展身份验证协议保护EAP(EAP-PEAP)访问。

身份验证成功后，Aruba控制器必须将用户重定向到ISE BYOD门户 — 本地请求方调配(NSP)流程。

用户被重定向，网络设置助理(NSA)应用被执行，证书被调配并安装在Windows客户端上。

ISE内部CA用于该进程（默认配置）。

NSA还负责为Aruba管理的第二个服务集标识符(SSID)(mgarz_byod_tls)创建无线配置文件 — 该配置文件用于802.1x可扩展身份验证协议 — 传输层安全(EAP-TLS)身份验证。

因此，企业用户可以执行个人设备自注册，并安全地访问企业网络。

本示例可以轻松地针对不同类型的访问进行修改，例如：

- 采用BYOD服务的集中式Web身份验证(CWA)
- 使用状况和BYOD重定向的802.1x身份验证
- 通常，对于EAP-PEAP身份验证，使用Active Directory（为了让本文使用短的内部ISE用户）
- 通常，对于使用证书调配外部简单证书注册协议(SCEP)服务器的证书，通常使用Microsoft网络设备注册服务(NDES)来缩短本文的篇幅，使用内部ISE CA。

第三方支持的挑战

将ISE访客流量(例如BYOD、CWA、NSP、客户端调配门户(CPP))与第三方设备配合使用时存在挑战。

会话

Cisco网络接入设备(NAD)使用名为audit-session-id的Radius cisco-av-pair向身份验证、授权和记帐(AAA)服务器通知会话ID。

ISE使用该值跟踪会话并为每个流提供正确的服务。其他供应商不支持cisco-av对。

ISE必须依赖于在访问请求和记帐请求中收到的IETF属性。

收到访问请求后，ISE会构建综合的思科会话ID（从Calling-Station-ID、NAS-Port、NAS-IP-Address和共享密钥）。 该值仅具有本地意义（不通过网络发送）。

因此，希望每个流(BYOD、CWA、NSP、CPP)都附加正确的属性，因此ISE能够重新计算思科会话ID并执行查找，以便将其与正确的会话关联并继续流。

URL重定向

ISE使用名为url-redirect和url-redirect-acl的Radius cisco-av-pair通知NAD必须重定向特定流量。

其他供应商不支持cisco-av对。通常，这些设备必须使用指向ISE上特定服务（授权配置文件）的静

态重定向URL进行配置。

用户启动HTTP会话后，这些NAD重定向到URL，并附加其他参数（如IP地址或MAC地址），以允许ISE识别特定会话并继续流程。

CoA

ISE使用Radius cisco-av-pair called subscriber:command， subscriber:reauthenticate-type来指示特定会话的NAD必须执行的操作。

其他供应商不支持cisco-av对。因此，这些设备通常使用RFC CoA（3576或5176）和以下两个定义的消息之一：

- 断开连接请求（也称为断开连接数据包） — 用于断开会话（经常用于强制重新连接）
- CoA推送 — 用于透明地更改会话状态而不断开连接（例如VPN会话和应用的新ACL）

ISE同时支持具有cisco-av-pair的Cisco CoA和RFC CoA 3576/5176。

ISE解决方案

为了支持第三方供应商，ISE 2.0引入了网络设备配置文件的概念，描述了特定供应商的行为方式 — 如何支持会话、URL重定向和CoA。

授权配置文件为特定类型（网络设备配置文件），身份验证发生后，ISE行为会从该配置文件派生。

因此，ISE可以轻松管理其他供应商的设备。ISE上的配置也很灵活，可以调整或创建新的网络设备配置文件。

本文介绍Aruba设备默认配置文件的用法。

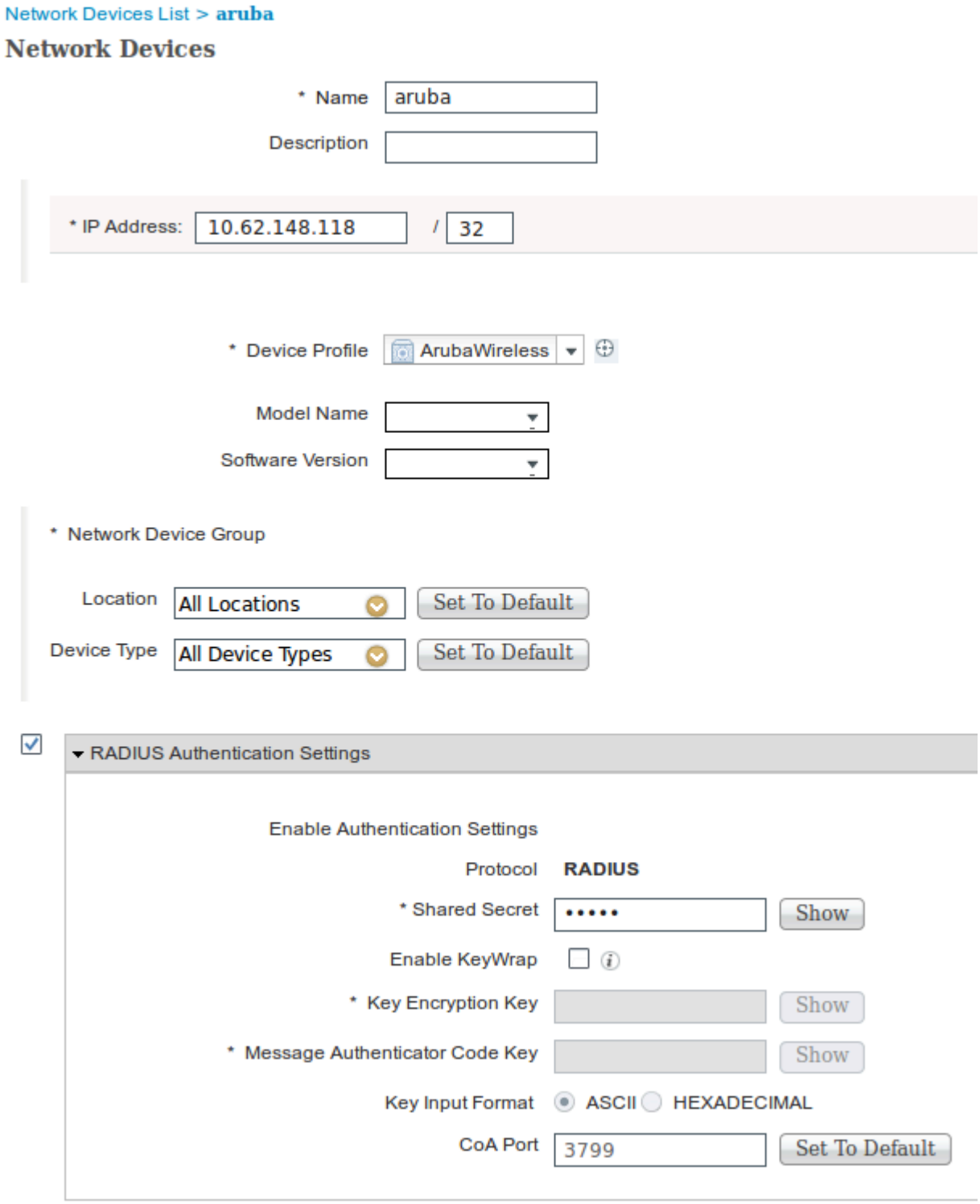
有关功能的详细信息：

使用思科身份服务引擎的网络访问设备配置文件

思科ISE

步骤1.将Aruba无线控制器添加到网络设备

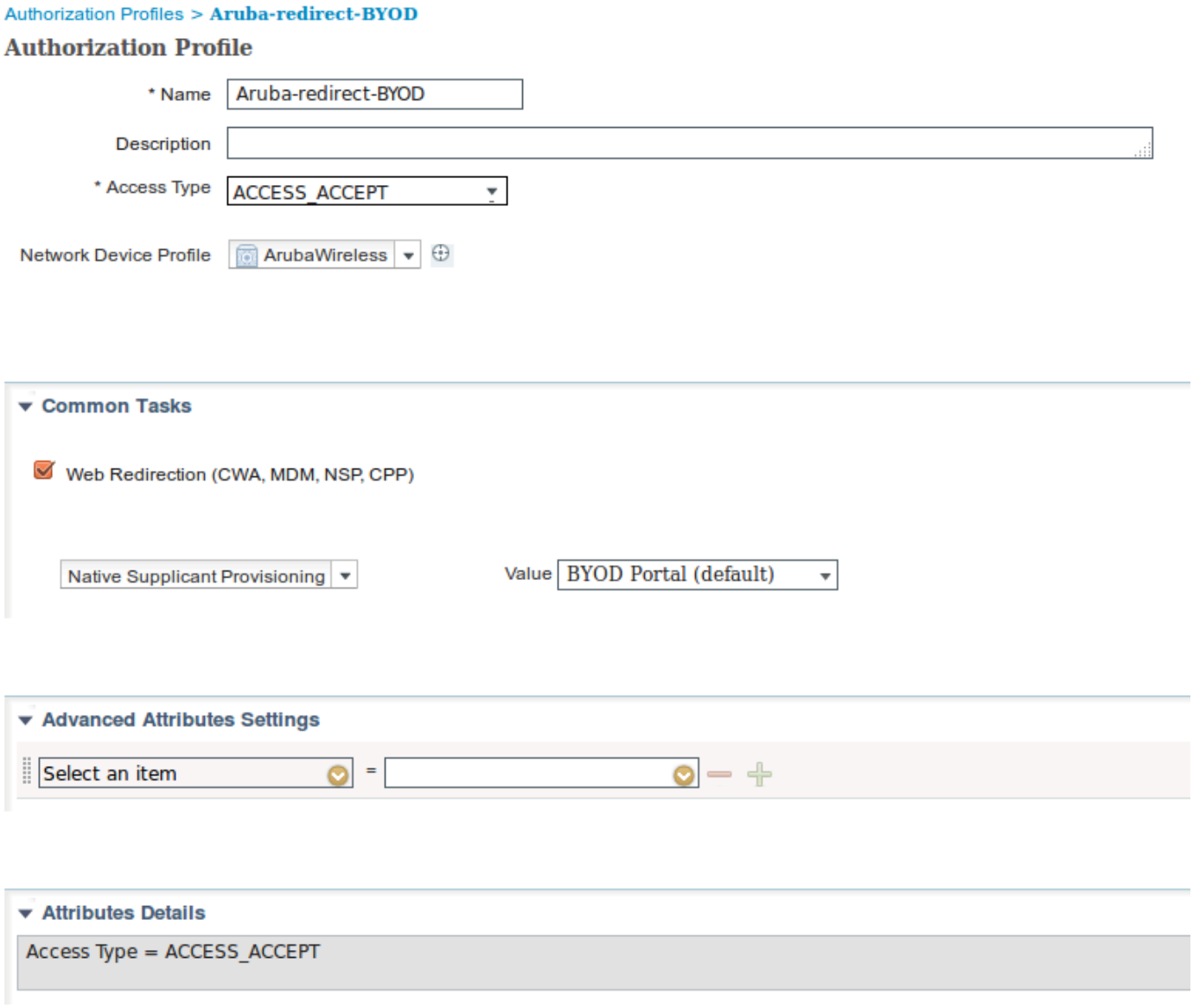
导航到管理>网络资源>网络设备。为所选供应商选择正确的设备配置文件，在这种情况下：ArubaWireless。 确保配置Shared Secret和CoA端口，如图所示。



如果所需供应商没有可用的配置文件，可以在Administration > Network Resources > Network Device Profiles下对其进行配置。

步骤2.配置授权配置文件

导航至策略>策略元素>结果>授权>授权配置文件选择与步骤1中相同的网络设备配置文件。ArubaWireless。配置的配置文件为Aruba-redirect-BYOD with BYOD Portal，如图所示。

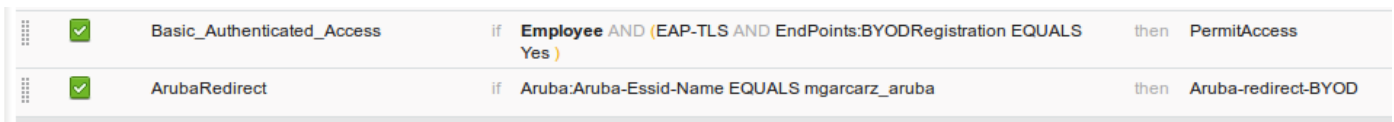


缺少Web重定向配置的一部分，其中生成了到授权配置文件的静态链接。虽然Aruba不支持动态重定向到访客门户，但每个授权配置文件都分配有一个链接，然后在Aruba上配置该链接，如图所示。



步骤3.配置授权规则

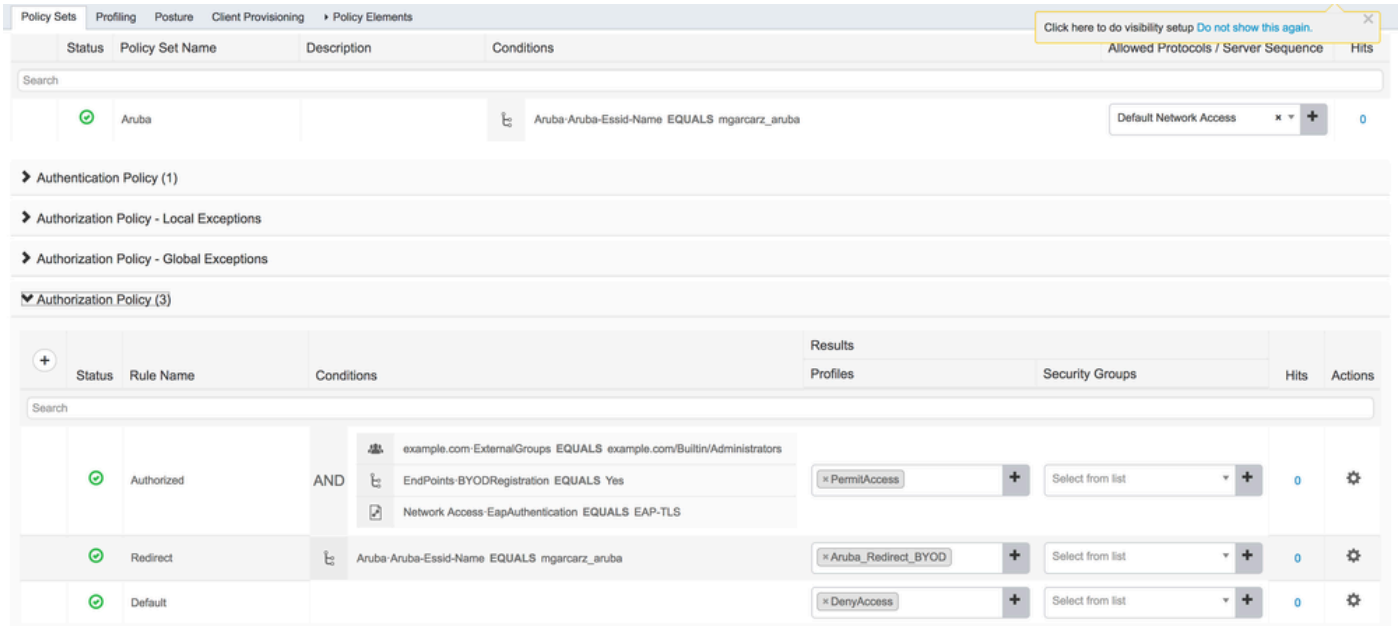
导航到Policy > Authorization Rules，配置如图所示。



首先，用户连接到SSID mgracarz_aruba，ISE返回授权配置文件Aruba-redirect-BYOD，它将客户

端重定向到默认BYOD门户。完成BYOD流程后，客户端将使用EAP-TLS进行连接，并授予对网络的完全访问权限。

在较新版本的ISE中，同一策略如下所示：



Aruba AP

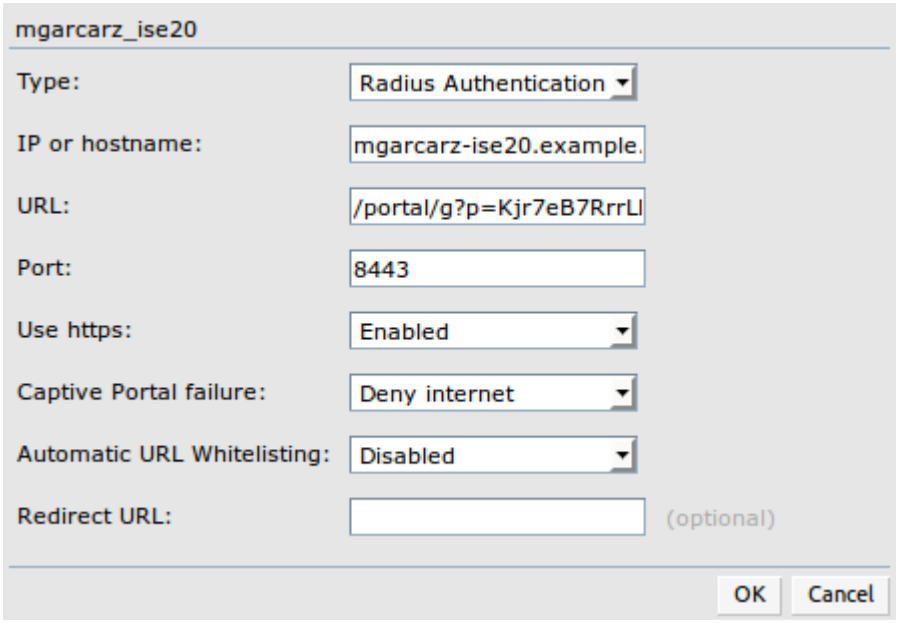
步骤1.强制网络门户配置

要在Aruba 204上配置强制网络门户，请导航到Security > External Captive Portal并添加新的强制网络门户。输入此信息以进行正确的配置，如图所示。

- type：RADIUS 身份验证
- IP或主机名：ISE服务器
- URL:在ISE上根据授权配置文件配置创建的链接；它特定于特定的授权配置文件，可以在此处的Web重定向配置下找到



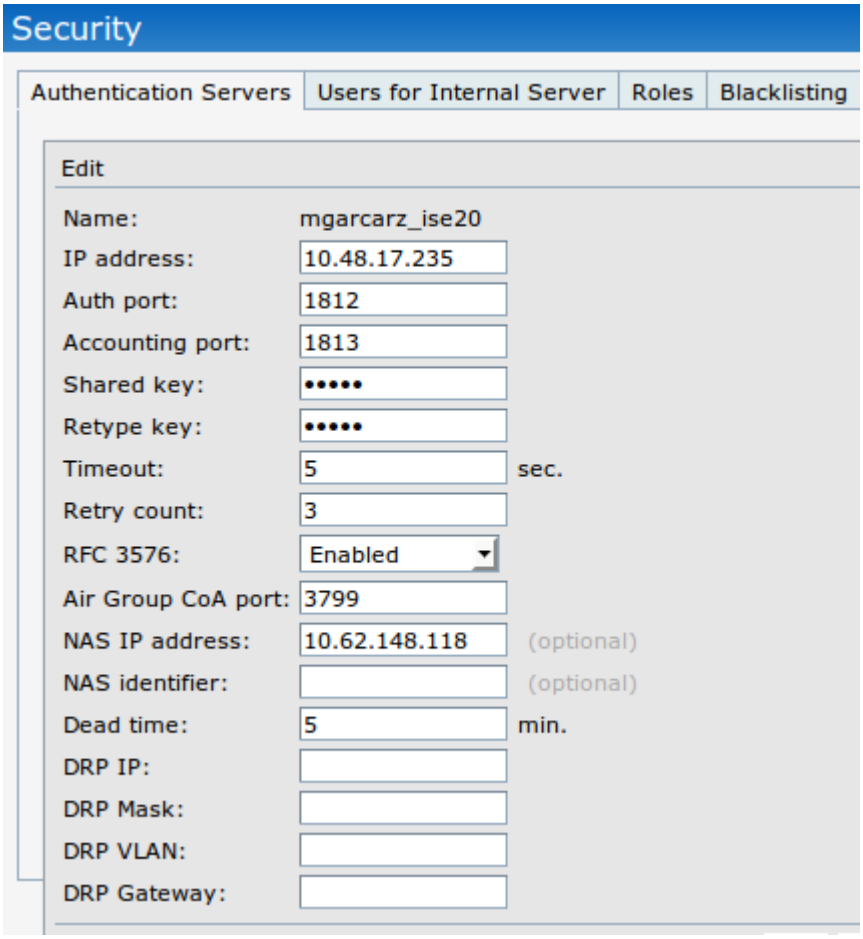
- 端口：在ISE上托管所选门户的端口号(默认情况下：8443)。



步骤2. Radius服务器配置

导航到安全>身份验证服务器，确保CoA端口与ISE上配置的端口相同，如图所示。

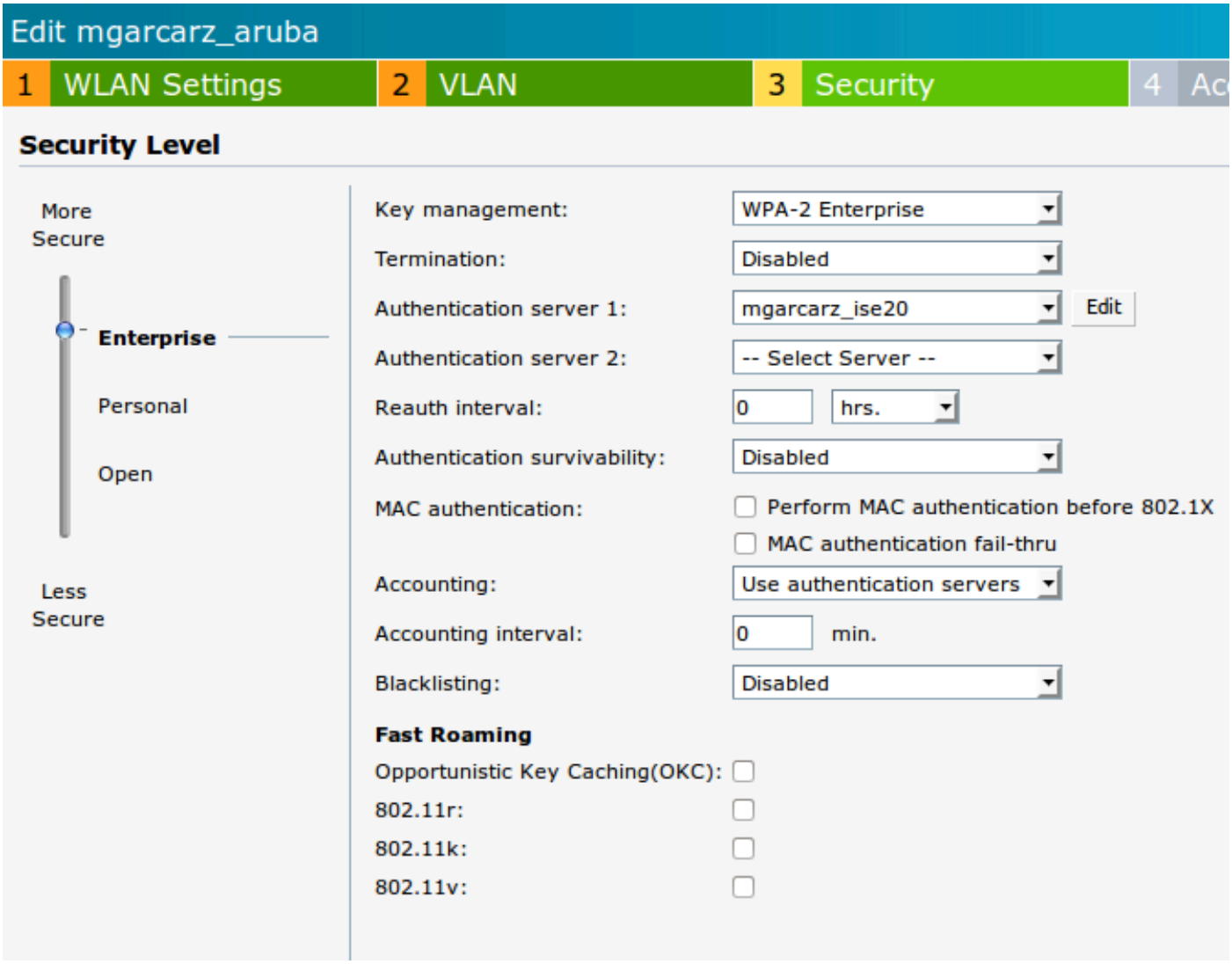
默认情况下，在Aruba 204上，它设置为5999，但这不符合RFC 5176，也不适用于ISE。



注意：在Aruba版本6.5及更高版本中，选中“Captive Portal”复选框。

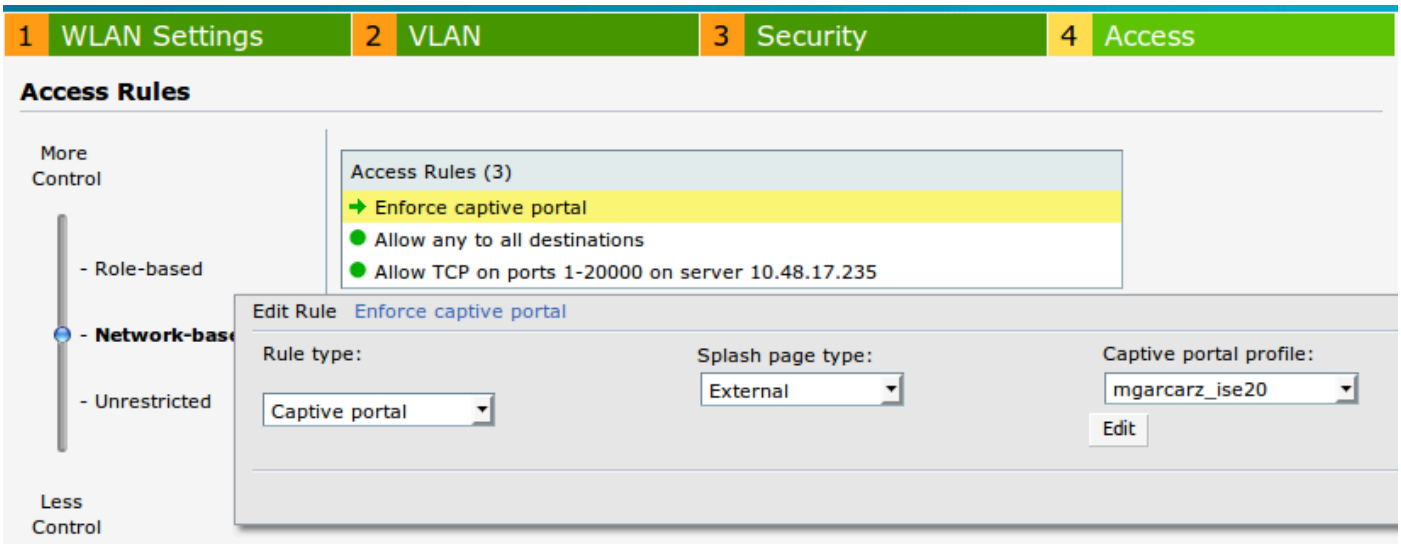
步骤3. SSID配置

- “安全”选项卡如图所示。

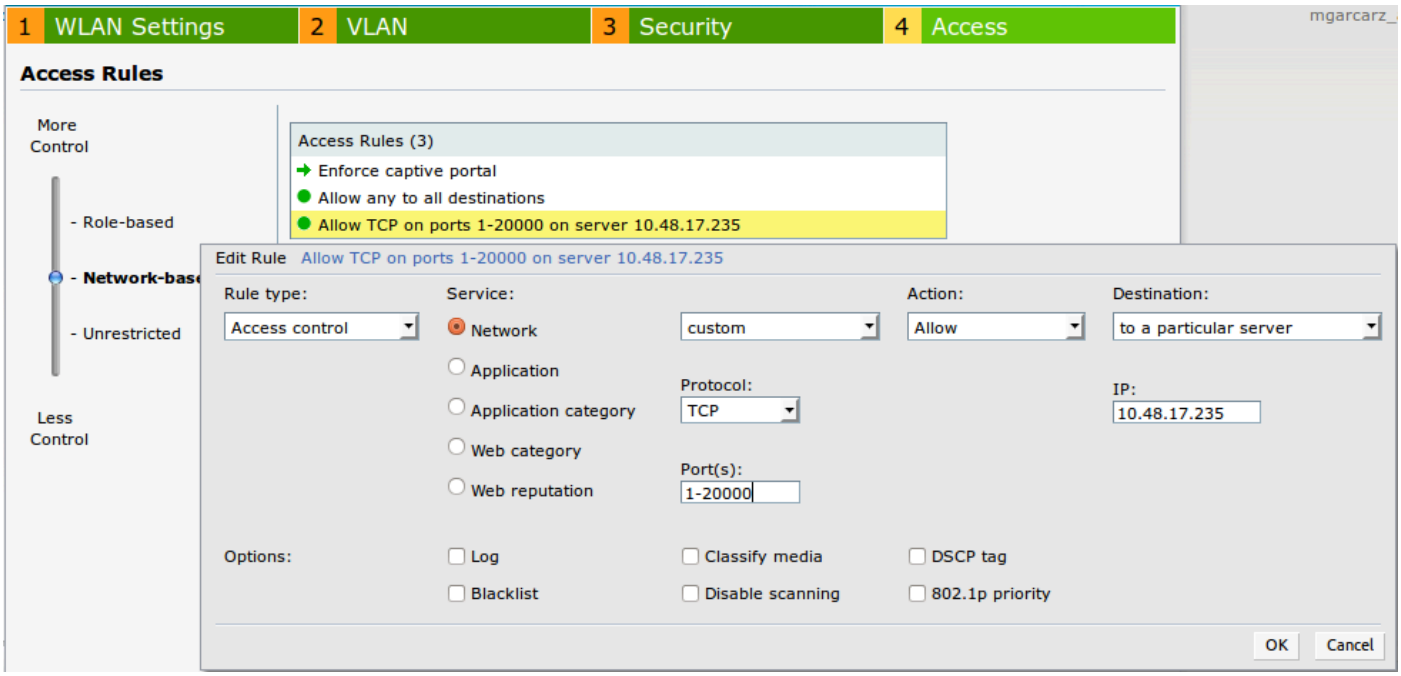


- “访问”选项卡：选择Network-based Access Rule以在SSID上配置强制网络门户。

使用在步骤1中配置的强制网络门户。单击New，依次选择Rule type: Captive portal、Splash page type: External，如图所示。



此外，允许所有流量发送到ISE服务器(范围1-20000中的TCP端口)，同时默认在Aruba上配置规则：Allow any to all destinations似乎无法正常运行（如图所示）。

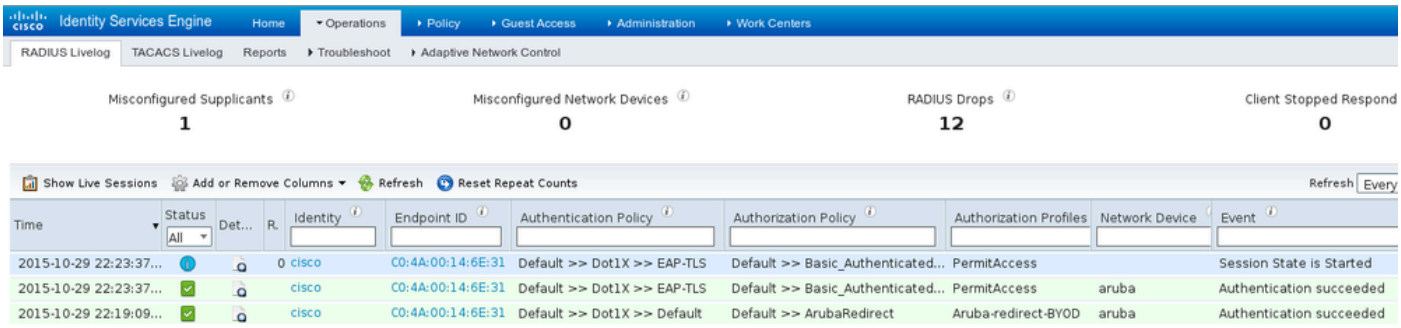


验证

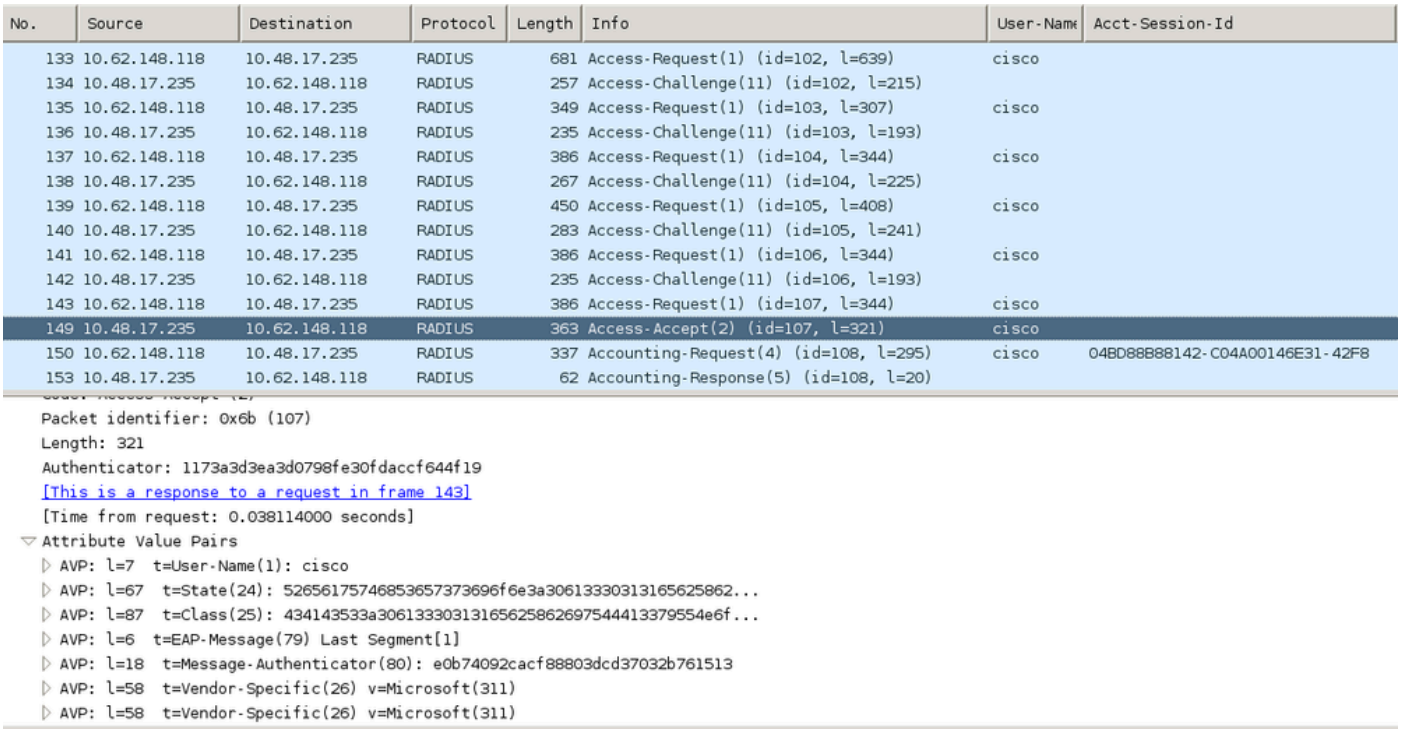
使用本部分可确认配置能否正常运行。

步骤1.使用EAP-PEAP连接到SSID mgarcarz_aruba

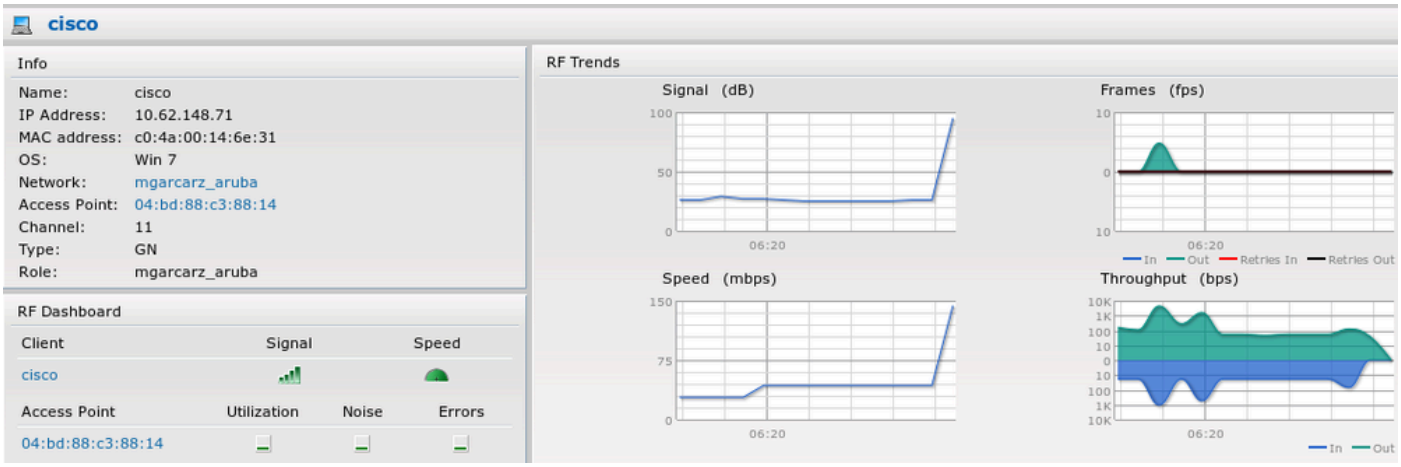
ISE上出现第一个身份验证日志。已使用默认身份验证策略，已返回Aruba-redirect-BYOD授权配置文件，如图所示。



ISE返回EAP成功的RADIUS访问接受消息。请注意，不会返回其他属性（无思科av-pair url-redirect或url-redirect-acl），如图所示。



Aruba报告会话已建立(EAP-PEAP身份为cisco)，并且选定的角色为mgarcarz_aruba，如图所示。



该角色负责重定向至ISE（Aruba上的强制网络门户功能）。

在Aruba CLI中，可以确认该会话的当前授权状态：

<#root>

04:bd:88:c3:88:14#

show datapath user

```
Datapath User Table Entries
---------------------------
Flags: P - Permanent, W - WEP, T- TKIP, A - AESCCM
       R - ProxyARP to User, N - VPN, L - local, I - Intercept, D - Deny local routing
FM(Forward Mode): S - Split, B - Bridge, N - N/A

       IP              MAC            ACLs    Contract   Location  Age    Sessions   Flags     Vlan  FM
---------------  -----------------  -------  ---------  --------  -----  ---------  -----     ----  --
10.62.148.118    04:BD:88:C3:88:14   105/0      0/0      0         1        0/65535  P            1   N

10.62.148.71     C0:4A:00:14:6E:31   138/0      0/0      0         0        6/65535               1   B


0.0.0.0          C0:4A:00:14:6E:31   138/0      0/0      0         0        0/65535  P            1   B
172.31.98.1      04:BD:88:C3:88:14   105/0      0/0      0         1        0/65535  P         3333   B
0.0.0.0          04:BD:88:C3:88:14   105/0      0/0      0         0        0/65535  P            1   N
04:bd:88:c3:88:14#
```

要检查ACL ID 138的当前权限，请执行以下操作：

<#root>

04:bd:88:c3:88:14#

show datapath acl 138

```
Datapath ACL 138 Entries
------------------------
Flags: P - permit, L - log, E - established, M/e - MAC/etype filter
       S - SNAT, D - DNAT, R - redirect, r - reverse redirect m - Mirror
       I - Invert SA, i - Invert DA, H - high prio, O - set prio, C - Classify Media
       A - Disable Scanning, B - black list, T - set TOS, 4 - IPv4, 6 - IPv6
       K - App Throttle, d - Domain DA
-------------------------------------------------------------
 1:  any  any  17 0-65535 8209-8211  P4
 2:  any  172.31.98.1 255.255.255.255  6 0-65535 80-80  PSD4
 3:  any  172.31.98.1 255.255.255.255  6 0-65535 443-443  PSD4
```

4: any mgarcarz-ise20.example.com 6 0-65535 80-80 Pd4

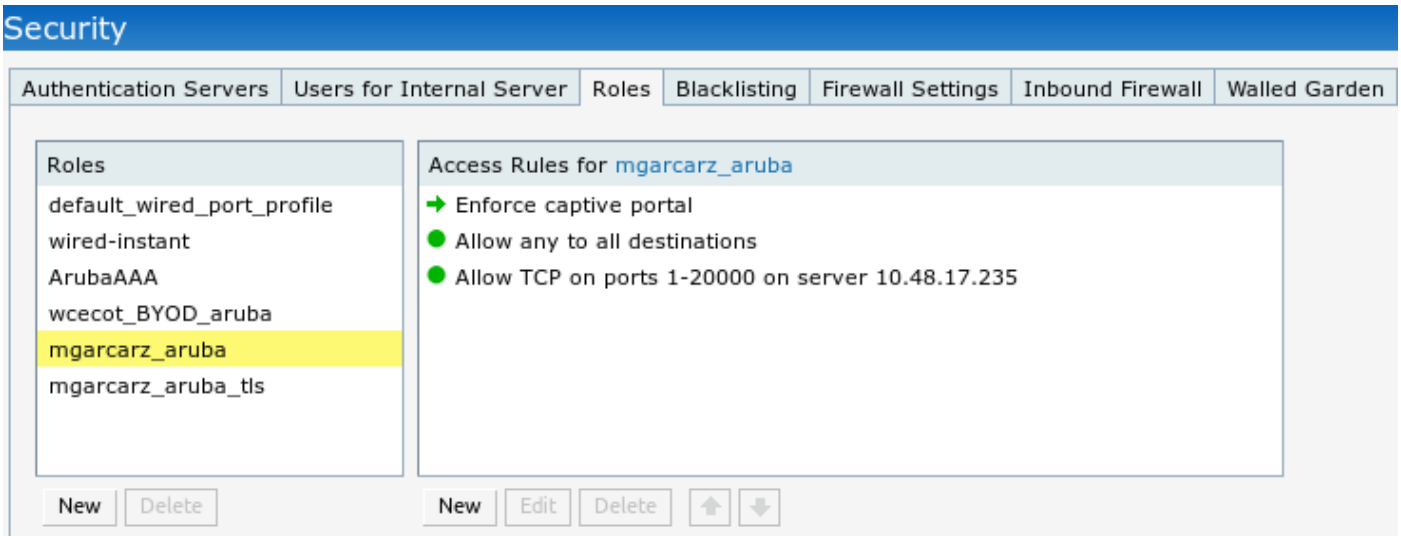
5: any mgarcarz-ise20.example.com 6 0-65535 443-443 Pd4

6: any mgarcarz-ise20.example.com 6 0-65535 8443-8443 Pd4 hits 37

7: any 10.48.17.235 255.255.255.255 6 0-65535 1-20000 P4 hits 18

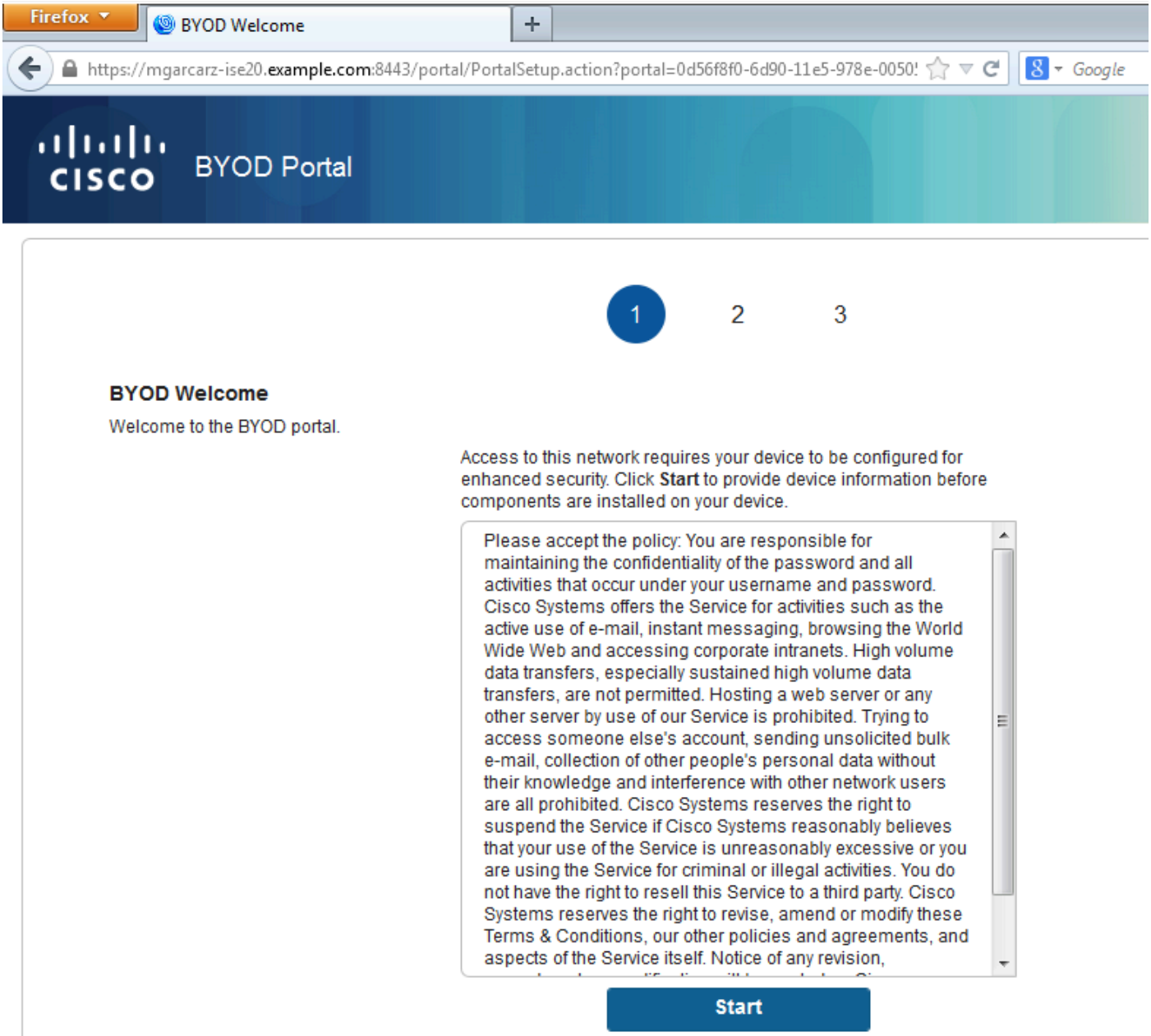
<....some output removed for clarity ... >

该配置与GUI中为该角色配置的内容匹配，如图所示。



步骤2.BYOD的Web浏览器流量重定向

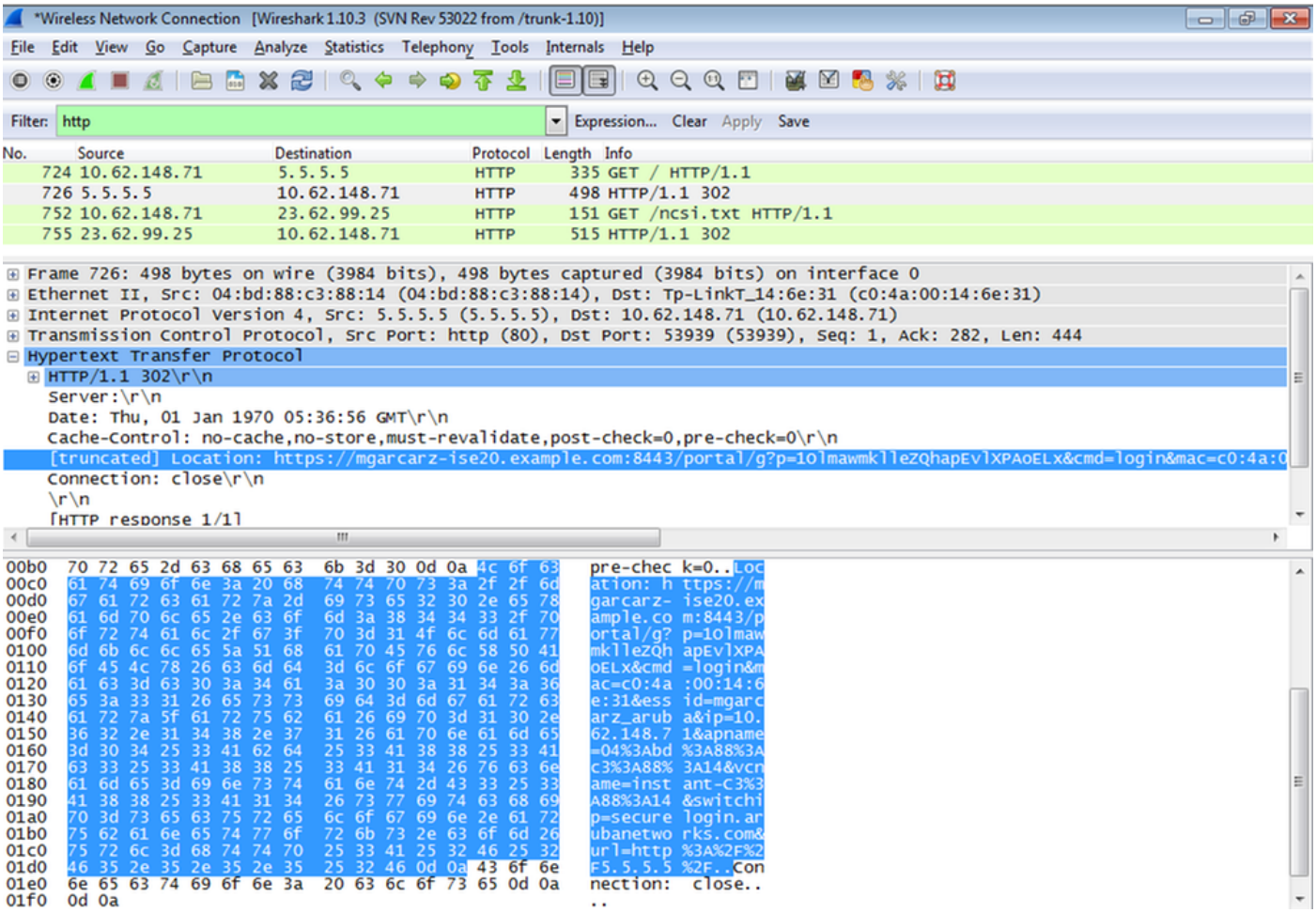
用户打开Web浏览器并键入任何地址后，就会发生重定向，如图所示。



查看数据包捕获，确认Aruba欺骗目标(5.5.5.5)并返回HTTP重定向到ISE。

请注意，它与ISE中配置的静态URL相同，并复制到Aruba上的强制网络门户 — 但还会添加多个参数，如图所示：

- cmd =登录
- mac = c0:4a:00:14:6e:31
- essid = mgarcarz_aruba
- ip = 10.62.148.7
- apname = 4bd88c38814(mac)
- url = http://5.5.5.5



由于这些参数，ISE能够重新创建思科会话ID，在ISE上查找相应的会话并继续执行BYOD（或任何其他已配置的）流程。

对于思科设备，通常使用audit_session_id，但其他供应商不支持此功能。

为了确认从ISE调试，可以看到生成audit-session-id值（从不通过网络发送）：

<#root>

AcsLogs,2015-10-29 23:25:48,538,DEBUG,0x7fc0b39a4700,cntx=0000032947,CallingStationID=
c04a00146e31,FramedIPAddress=10.62.148.71,MessageFormatter::appendValue() attrName:
cisco-av-pair appending value:

audit-session-id=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7G1HXj1M

然后，在BYOD第2页中注册设备后进行关联：

<#root>

AcsLogs,2015-10-29 23:25:48,538,DEBUG,0x7fc0b39a4700,cntx=0000032947,CallingStationID=
c04a00146e31,FramedIPAddress=10.62.148.71,Log_Message=[2015-10-29 23:25:48.533 +01:00
0000011874 88010 INFO

MyDevices: Successfully registered/provisioned the device

(endpoint), ConfigVersionId=145, UserName=cisco, MacAddress=c0:4a:00:14:6e:31,
IpAddress=10.62.148.71, AuthenticationIdentityStore=Internal Users,
PortalName=BYOD Portal (default), PsnHostName=mgarcarz-ise20.example.com,
GuestUserName=cisco, EPMacAddress=C0:4A:00:14:6E:31, EPIdentityGroup=RegisteredDevices
Staticassignment=true, EndPointProfiler=mgarcarz-ise20.example.com, EndPointPolicy=
Unknown, NADAddress=10.62.148.118, DeviceName=ttt, DeviceRegistrationStatus=Registered
AuditSessionId=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7G1HXj1M,
cisco-av-pair=

audit-session-id=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7G1HXj1M

在后续请求中，客户端被重定向到BYOD第3页，在该页中下载并执行NSA。

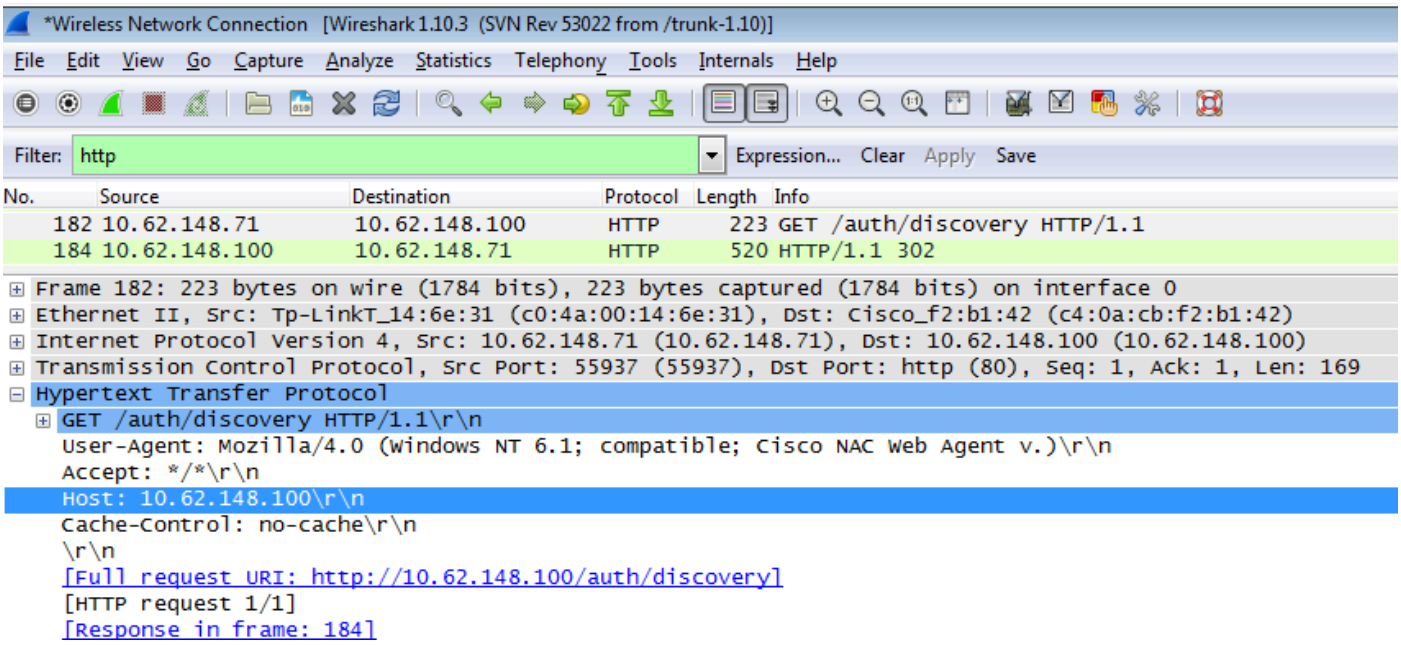
步骤3.执行网络设置助理



NSA的任务与Web浏览器相同。首先，它需要检测ISE的IP地址。这是通过HTTP重定向实现的。

由于这次用户无法键入IP地址（如在Web浏览器中），因此该流量会自动生成。

使用默认网关(也可使用enroll.cisco.com)，如图所示。



响应与Web浏览器的响应完全相同。

这样，NSA可以连接到ISE，通过配置获取xml配置文件，生成SCEP请求，将其发送到ISE，获取签名证书（由ISE内部CA签名），配置无线配置文件，最后连接到配置的SSID。

从客户端收集日志(在Windows上%temp%/spwProfile.log中)。 为清楚起见，省略了部分输出：

<#root>

```
Logging started
SPW Version: 1.0.0.46
System locale is [en]
Loading messages for english...
Initializing profile
SPW is running as High integrity Process - 12288
GetProfilePath: searched path = C:\Users\ADMINI~1.EXA\AppData\Local\Temp\ for file name = spwProfile.xm
GetProfilePath: searched path = C:\Users\ADMINI~1.EXA\AppData\Local\Temp\Low for file name = spwProfile

Profile xml not found Downloading profile configuration...


Downloading profile configuration...

Discovering ISE using default gateway


Identifying wired and wireless network interfaces, total active interfaces: 1
Network interface - mac:C0-4A-00-14-6E-31, name: Wireless Network Connection, type: wireless
Identified default gateway: 10.62.148.100

Identified default gateway: 10.62.148.100, mac address: C0-4A-00-14-6E-31



redirect attempt to discover ISE with the response url


DiscoverISE - start
Discovered ISE - : [mgarcarz-ise20.example.com, sessionId: 0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7
```

DiscoverISE - end

Successfully Discovered ISE: mgarcarz-ise20.example.com, session id: 0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7

GetProfile - start
GetProfile - end

Successfully retrieved profile xml

using V2 xml version
parsing wireless connection setting

Certificate template: [keysize:2048, subject:OU=Example unit,O=Company name,L=City,ST=State,C=US, SAN:MA

set ChallengePwd

creating certificate with subject = cisco and subjectSuffix = OU=Example unit,O=Company name,L=City,ST=
Installed [LAB CA, hash: fd 72 9a 3b b5 33 72 6f f8 45 03 58 a2 f7 eb 27^M
ec 8a 11 78^M
] as rootCA

Installed CA cert for authMode machineOrUser - Success

HttpWrapper::SendScepRequest

 - Retrying: [1] time, after: [2] secs , Error: [0], msg: [Pending]
creating response file name C:\Users\ADMINI~1.EXA\AppData\Local\Temp\response.cer

Certificate issued - successfully

ScepWrapper::InstallCert start

ScepWrapper::InstallCert: Reading scep response file

  [C:\Users\ADMINI~1.EXA\AppData\Local\Temp\response.cer].
ScepWrapper::InstallCert GetCertHash -- return val 1
ScepWrapper::InstallCert end

Configuring wireless profiles...

Configuring ssid [mgarcarz_aruba_tls]

WirelessProfile::SetWirelessProfile - Start

Wireless profile: [mgarcarz_aruba_tls] configured successfully

Connect to SSID

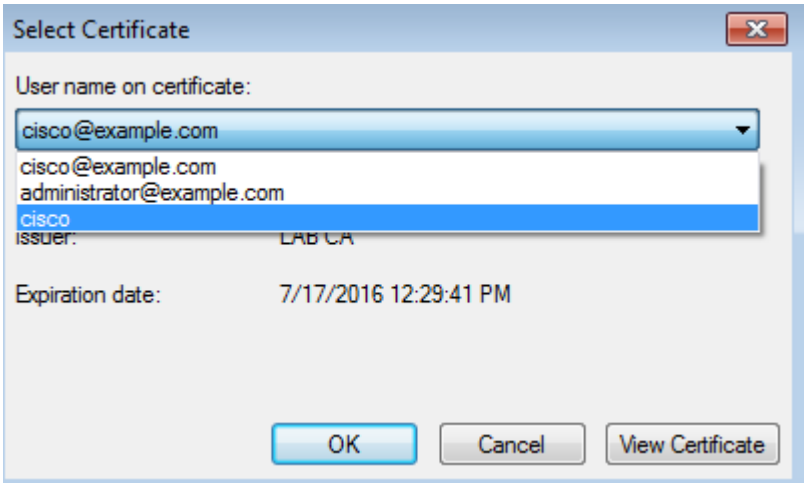
Successfully connected profile: [mgarcarz_aruba_tls]

```
WirelessProfile::SetWirelessProfile. - End
```

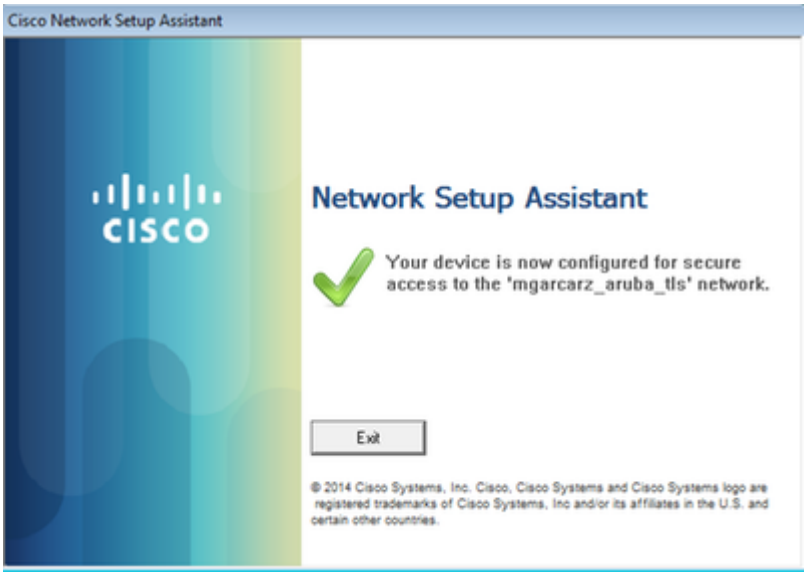
这些日志与使用思科设备的BYOD流程完全相同。

注意：此处不需要Radius CoA。它是强制重新连接到新配置的SSID的应用程序(NSA)。

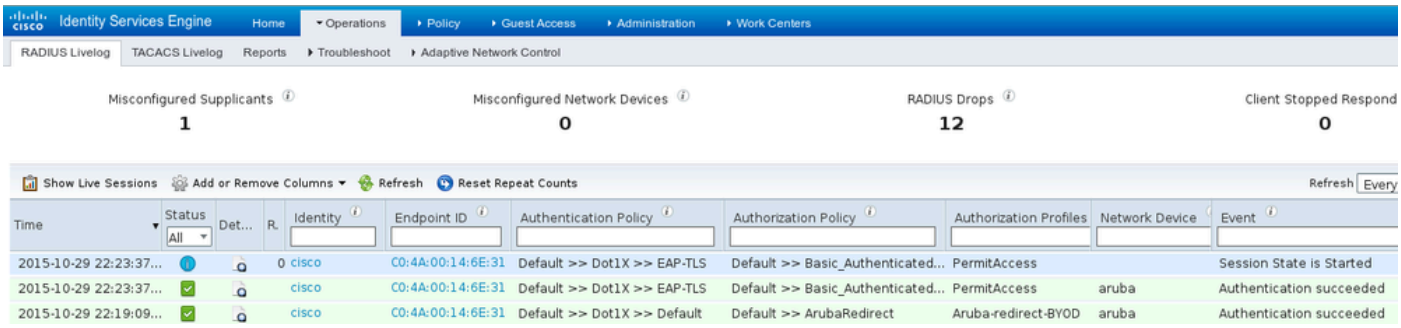
在此阶段，用户可以看到系统尝试与最终SSID关联。如果您有多个用户证书，则必须选择正确的证书（如下所示）。



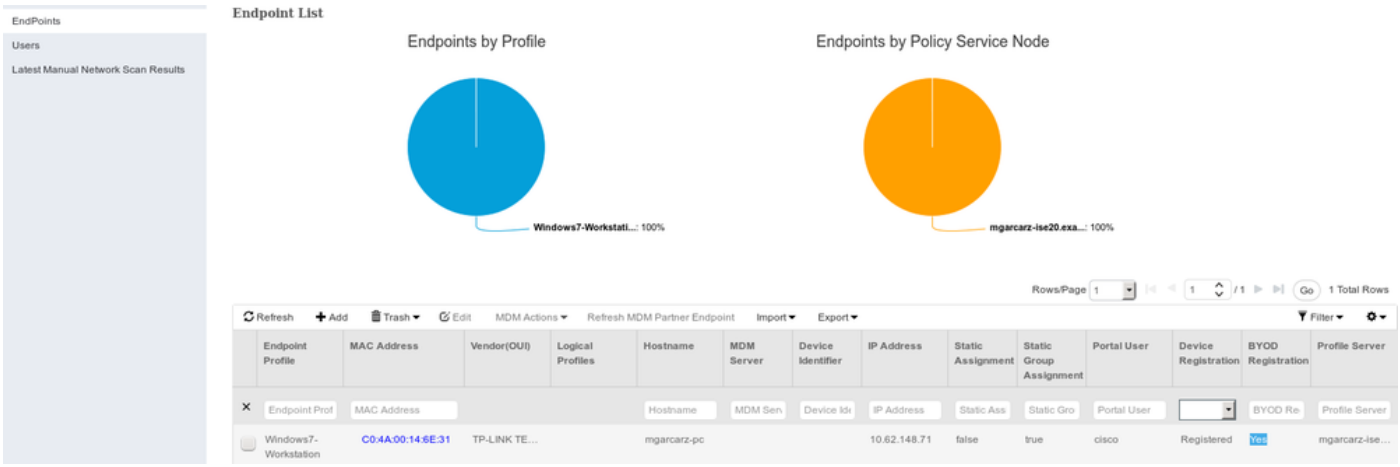
连接成功后，NSA报告如图所示。



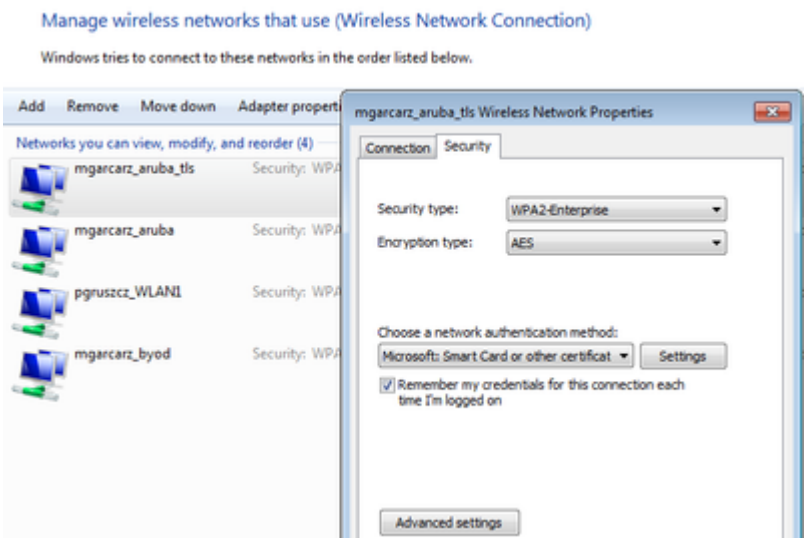
可以在ISE上确认 — 第二个日志命中EAP-TLS身份验证，该身份验证匹配Basic_Authenticated_Access的所有条件（EAP-TLS、Employee和BYOD Registered true）。



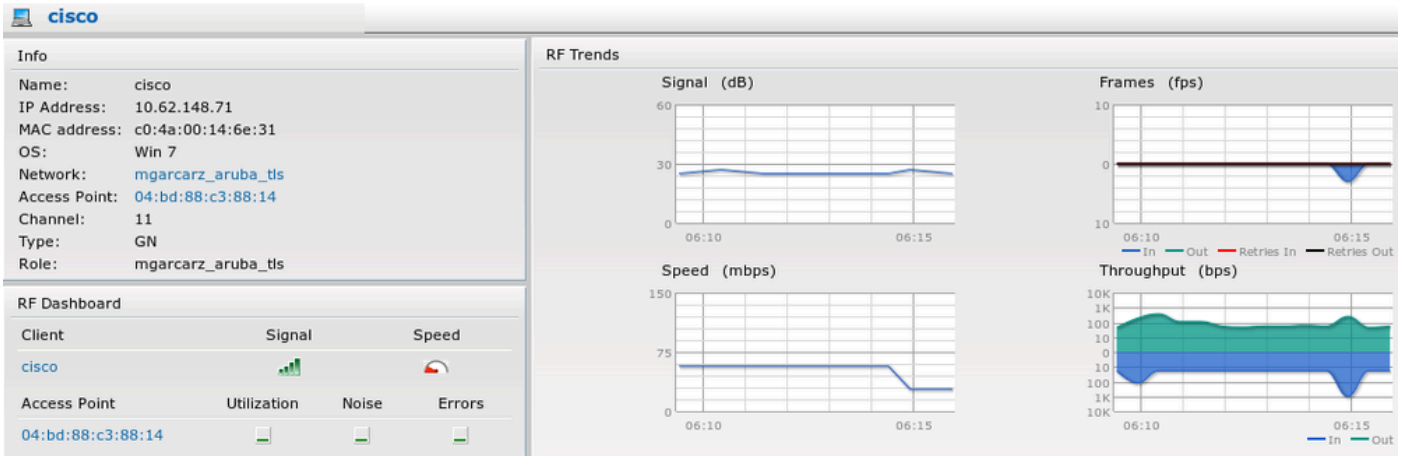
此外，终端身份视图可以确认终端的BYOD注册标志设置为true，如图所示。



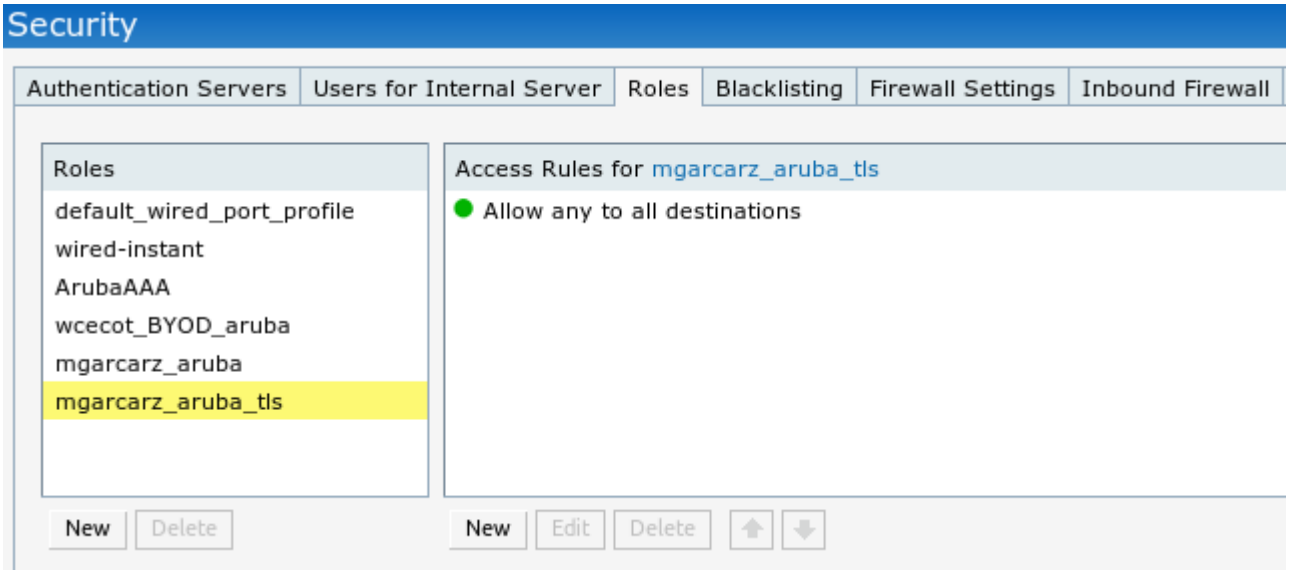
在Windows PC上，新的无线配置文件已自动创建为首选（并配置为EAP-TLS），如下所示。



在此阶段，Aruba确认用户已连接到最终SSID。



自动创建并命名为“与网络相同”的角色提供完整的网络访问。

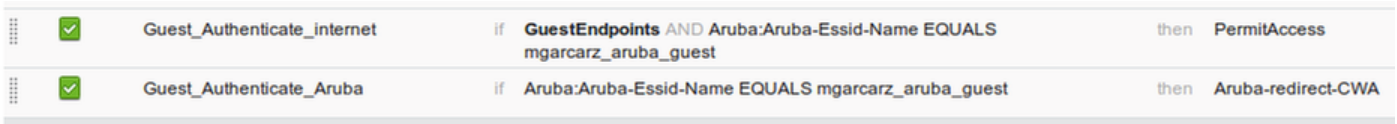


其他流和CoA支持

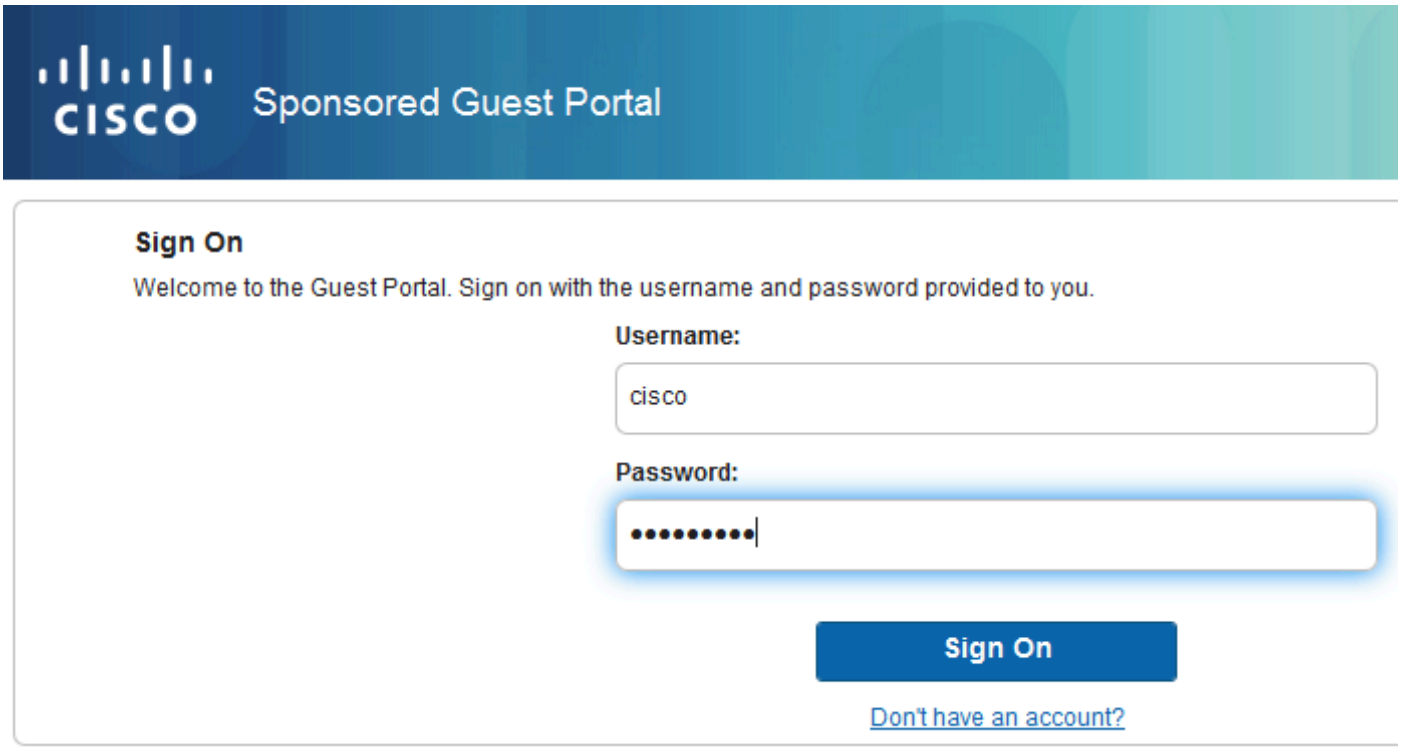
带CoA的CWA

虽然在BYOD流程中没有CoA消息，但具有自助注册访客门户的CWA流程显示如下：

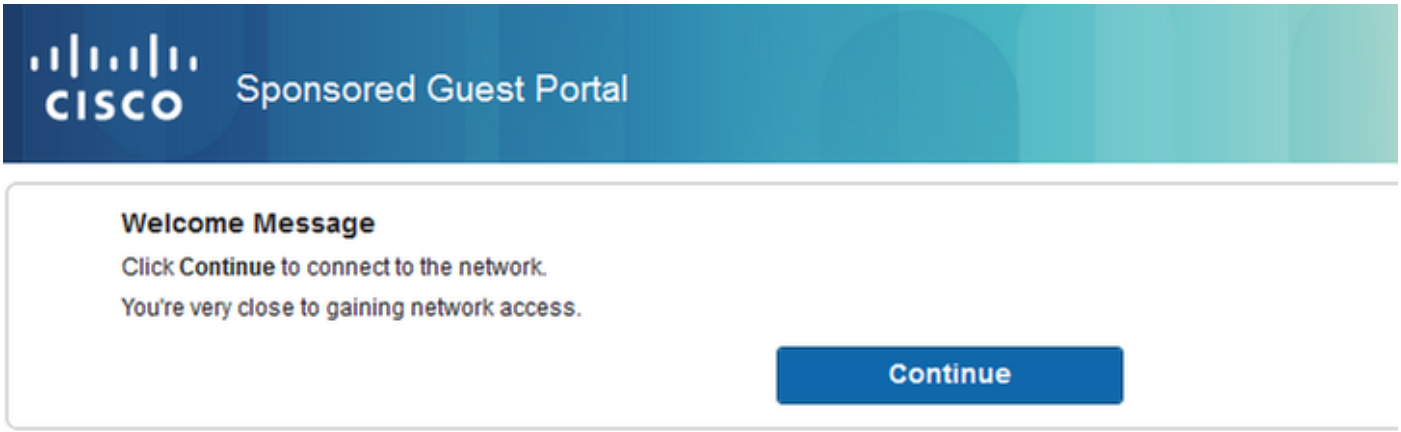
配置的授权规则如图所示。



用户通过MAB身份验证连接到SSID，一旦尝试连接到某个网页，就会重定向到自助注册访客门户，访客可以在其中创建新帐户或使用当前帐户。



成功连接访客后，CoA消息将从ISE发送到网络设备，以更改授权状态。



可以在操作>身份验证下验证，如图所示。

cisco	C0:4A:00:15:76:34	Windows7-Workstat...	Default >> MAB	Default >> Guest_Authenticate_internet	Authorize-Only succeeded	PermitAccess
	C0:4A:00:15:76:34				Dynamic Authorization succe...	
cisco	C0:4A:00:15:76:34				Guest Authentication Passed	
C0:4A:00:15:76	C0:4A:00:15:76:34		Default >> MAB >> ...	Default >> Guest_Authenticate_Aruba	Authentication succeeded	Aruba-redirect-CWA

ISE调试中的CoA消息：

<#root>

```
2015-11-02 18:47:49,553 DEBUG  [Thread-137][] cisco.cpm.prrt.impl.PrRTLoggerImpl -::::-
DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationFlow::createCoACmd]
Processing incoming attribute vendor , name
```

NAS-IP-Address, value=10.62.148.118

.,
DynamicAuthorizationFlow.cpp:708
2015-11-02 18:47:49,567 DEBUG [Thread-137][] cisco.cpm.prrt.impl.PrRTLoggerImpl -:::::-
 DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationFlow::createCoACmd]
 Processing incoming attribute vendor , name

**Acct-Session-Id, value=04BD88B88144-
C04A00157634-7AD**

.,DynamicAuthorizationFlow.cpp:708
2015-11-02 18:47:49,573 DEBUG [Thread-137][] cisco.cpm.prrt.impl.PrRTLoggerImpl -:::::-
 DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationFlow::createCoACmd]
Processing incoming attribute vendor , name cisco-av-pair, v
alue=audit-session-id=0a3011ebisZXypODwqjB6j64GeFiF7RwvyocneEia17ckjtU1HI.,DynamicAuthorizationFlow.cpp
2015-11-02 18:47:49,584 DEBUG [Thread-137][] cisco.cpm.prrt.impl.PrRTLoggerImpl -:::::-
 DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationRequestHelper::
setConnectionParams]

defaults from nad profile : NAS=10.62.148.118, port=3799, timeout=5,

retries=2

 ,DynamicAuthorizationRequestHelper.cpp:59
2015-11-02 18:47:49,592 DEBUG [Thread-137][] cisco.cpm.prrt.impl.PrRTLoggerImpl -:::::-
 DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationRequestHelper::set
ConnectionParams] NAS=10.62.148.118, port=3799, timeout=5, retries=1,
DynamicAuthorizationRequestHelper.cpp:86
2015-11-02 18:47:49,615 DEBUG [Thread-137][] cisco.cpm.prrt.impl.PrRTLoggerImpl -:::::-
 DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationFlow::onLocalHttpEvent]:

invoking DynamicAuthorization,DynamicAuthorizationFlow.cpp:246

和来自Aruba的Disconnect-ACK:

<#root>

2015-11-02 18:47:49,737 DEBUG [Thread-147][] cisco.cpm.prrt.impl.PrRTLoggerImpl -:::::-
DynamicAuthorizationFlow,DEBUG,0x7fc0e9eb4700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b
-44549024315e,

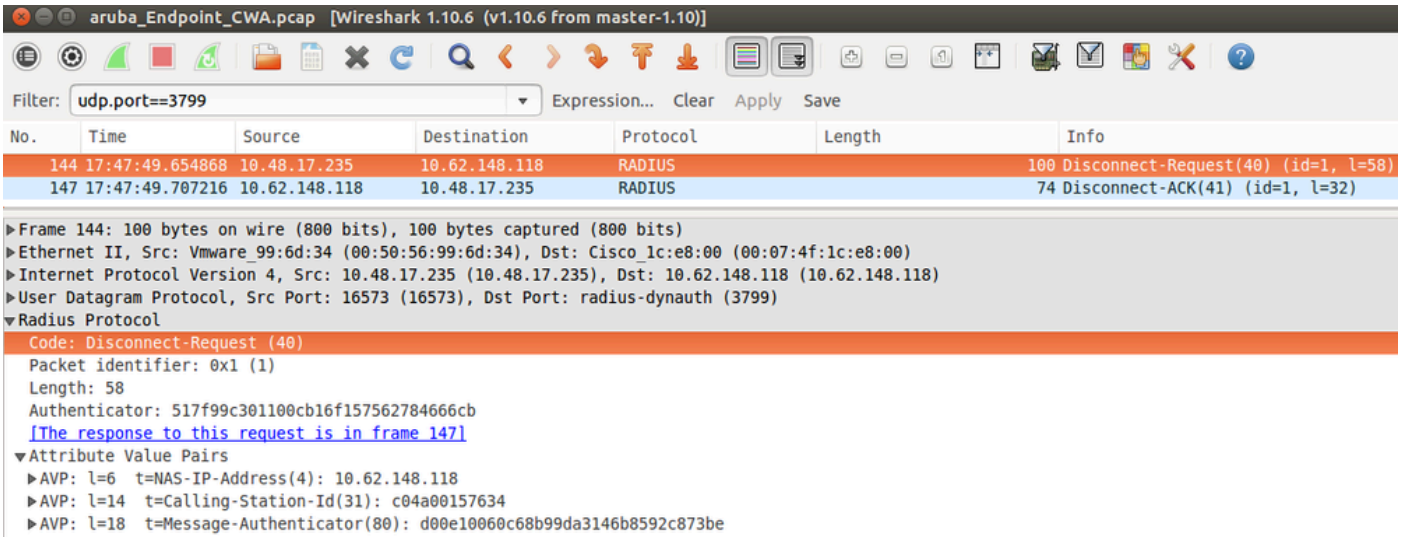
CallingStationID=c04a00157634

,[DynamicAuthorizationFlow::
onResponseDynamicAuthorizationEvent] Handling response
ID c59aa41a-e029-4ba0-a31b-44549024315e, error cause 0,

Packet type 41(DisconnectACK).

,
DynamicAuthorizationFlow.cpp:303

图中所示为CoA Diconnect-Request(40)和Diconnect-ACK(41)数据包捕获。



注意：RFC CoA已用于与设备配置文件Aruba（默认设置）相关的身份验证。 对于与思科设备相关的身份验证，应该是Cisco CoA类型重新进行身份验证。

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。

Aruba强制网络门户，具有IP地址而不是FQDN

如果Aruba上的强制网络门户配置了IP地址而不是ISE的FQDN，则PSN NSA失败：

<#root>

```
Warning - [HTTPConnection]
Abort the HTTP connection due to invalid certificate

CN
```

原因是在连接到ISE时进行严格的证书验证。当您使用IP地址连接到ISE时（由于重定向URL使用IP地址而非FQDN），并且向ISE证书提供主题名称= FQDN验证失败。

注意：Web浏览器继续BYOD门户（带有需要用户批准的警告）。

Aruba强制网络门户访问策略不正确

默认情况下，使用强制网络门户配置的Aruba访问策略允许tcp端口80、443和8080。

NSA无法连接到tcp端口8905以从ISE获取xml配置文件。报告此错误：

<#root>

Failed to get spw profile url using - url

[

https://mgarcarz-ise20.example.com:8905

/auth/provisioning/evaluate?
typeHint=SPWConfig&referrer=Windows&mac_address=C0-4A-00-14-6E-31&spw_version=
1.0.0.46&session=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7G1HXj1M&os=Windows All]
- http Error: [2]

HTTP response code: 0

]
GetProfile - end
Failed to get profile. Error: 2

Aruba CoA端口号

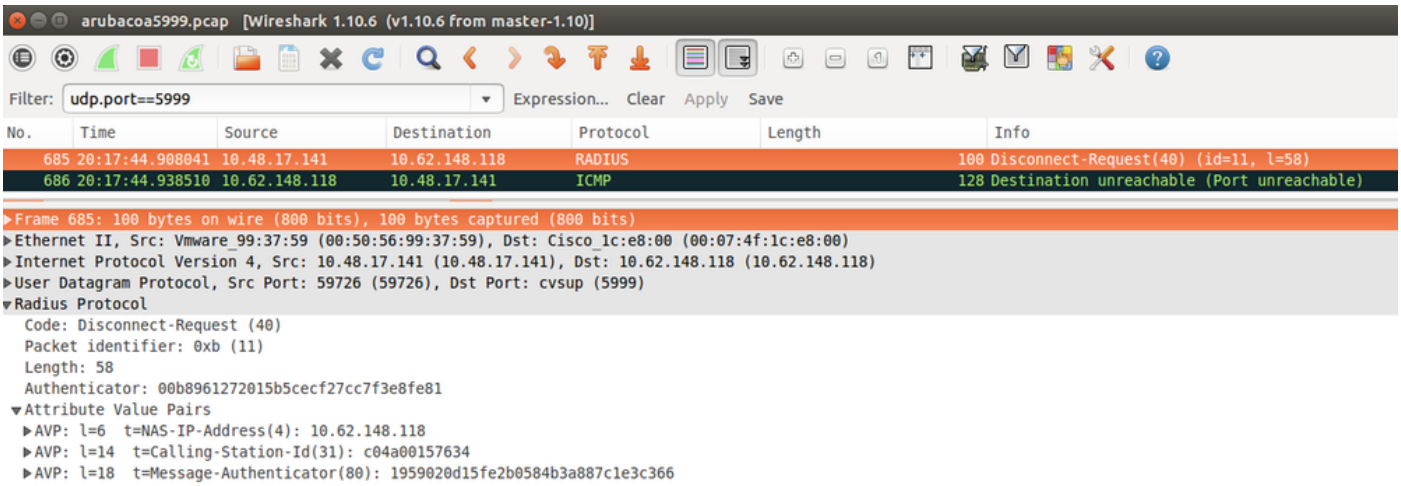
默认情况下，Aruba为CoA Air Group CoA端口5999提供端口号。遗憾的是，Aruba 204没有响应此类请求（如图所示）。

Event	5417 Dynamic Authorization failed
Failure Reason	11213 No response received from Network Access Device after sending a Dynamic Authorization request

Steps

11201	Received disconnect dynamic authorization request
11220	Prepared the reauthenticate request
11100	RADIUS-Client about to send request - (port = 5999 , type = RFC 5176)
11104	RADIUS-Client request timeout expired (Step latency=10009 ms)
11213	No response received from Network Access Device after sending a Dynamic Authorization request

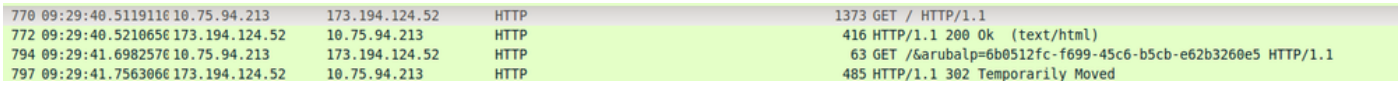
数据包捕获如图所示。



此处使用的最佳选项可以是CoA端口3977，如RFC 5176中所述。

某些Aruba设备上的重定向

在使用v6.3的Aruba 3600上，我们注意到重定向的工作方式与其他控制器略有不同。数据包捕获和解释可以在此处找到。



<#root>

packet 1: PC is sending GET request to google.com
packet 2: Aruba is returning HTTP 200 OK with following content:
<meta http-equiv='refresh' content='1; url=http://www.google.com/

&arubalp=6b0512fc-f699-45c6-b5cb-e62b3260e5

'>\n
packet 3: PC is going to link with Aruba attribute returned in packet 2:
http://www.google.com/

&arubalp=6b0512fc-f699-45c6-b5cb-e62b3260e5

packet 4: Aruba is redirecting to the ISE (302 code):
https://10.75.89.197:8443/portal/g?p=4voD8q6W5Lxr8hpab77gL8VdaQ&cmd=login&

mac=80:86:f2:59:d9:db&ip=10.75.94.213&essid=SC%2DWiFi&apname=LRC-006&apgroup=default&url=http%3A%2F%2Fww

相关信息

- 思科身份服务引擎管理员指南，版本2.0
- 使用思科身份服务引擎的网络访问设备配置文件
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。