Configuración de la integración de ISE 2.0 de terceros con Aruba Wireless

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Configurar
Diagrama de la red
Dates est la coistencia de terreste
<u>SESIONES</u> Redirección de LIRI
CoA
Solución en ISE
Paso 1 Agregar el controlador inalámbrico de Aruba a los dispositivos de red
Paso 2. Configurar perfil de autorización
Paso 3. Configuración de las reglas de autorización
AP de Aruba
Paso 1. Configuración del portal cautivo
Paso 2. Configuración del servidor de RADIUS
Paso 3. Configuración de SSID
Verificación
Paso 1. Conexión a SSID mgarcarz arubacon EAP-PEAP
Paso 2. Redirección del tráfico del navegador web para BYOD
Paso 3. Ejecución de Network Setup Assistant
<u>Otros flujos y soporte de CoA</u>
CWA con CoA
Troubleshoot
Portal cautivo de Aruba con dirección IP en lugar de EODN
Número de puerto CoA de Aruba
Redirección en algunos dispositivos de Aruba
Información Relacionada

Introducción

Este documento describe cómo resolver problemas de la función de integración de terceros en Cisco Identity Services Engine (ISE).

Nota: Tenga en cuenta que Cisco no se hace responsable de la configuración o el soporte de dispositivos de otros proveedores.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de Aruba IAP
- Flujos de BYOD en ISE
- Configuración de ISE para autenticación de certificados y contraseñas

Componentes Utilizados

Este documento describe cómo resolver problemas de la función de integración de terceros en Cisco Identity Services Engine (ISE).

Se puede utilizar como guía para la integración con otros proveedores y flujos. La versión 2.0 de ISE admite la integración de terceros.

Este es un ejemplo de configuración que presenta cómo integrar una red inalámbrica gestionada por Aruba IAP 2004 con ISE para servicios Bring Your Own Device (BYOD).

La información que contiene este documento se basa en estas versiones de software:

- Software Aruba IAP 204 6.4.2.3
- Cisco ISE, versión 2.0 y posteriores

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red



Hay dos redes inalámbricas administradas por Aruba AP.

El primero (mgarcarz_byod) se utiliza para el acceso EAP protegido por protocolo de autenticación extensible (EAP-PEAP) 802.1x.

Después de una autenticación correcta, el controlador de Aruba debe redirigir al usuario al portal BYOD de ISE: flujo de aprovisionamiento de suplicante nativo (NSP).

Se redirige al usuario, se ejecuta la aplicación Network Setup Assistant (NSA) y se aprovisiona e instala el certificado en el cliente Windows.

La CA interna de ISE se utiliza para ese proceso (configuración predeterminada).

La NSA también es responsable de la creación del perfil inalámbrico para el segundo identificador de conjunto de servicios (SSID) gestionado por Aruba (mgarcarz_byod_tls), que se utiliza para la autenticación de protocolo de autenticación extensible 802.1x con seguridad de capa de transporte (EAP-TLS).

Como resultado, el usuario corporativo puede incorporar dispositivos personales y obtener acceso seguro a la red corporativa.

Este ejemplo se puede modificar fácilmente para diferentes tipos de acceso, por ejemplo:

- Autenticación web central (CWA) con servicio BYOD
- Autenticación 802.1x con redirección de estado y BYOD

- Normalmente, para la autenticación EAP-PEAP se utiliza Active Directory (para abreviar este artículo se utilizan usuarios internos de ISE)
- Normalmente, para el aprovisionamiento de certificados se utiliza un servidor externo de Protocolo simple de inscripción de certificados (SCEP), normalmente el Servicio de inscripción de dispositivos de red (NDES) de Microsoft para que este artículo sea breve, se utiliza una CA ISE interna.

Retos con la asistencia de terceros

Existen algunos retos a la hora de utilizar flujos de invitados de ISE (como BYOD, CWA, NSP, Client Provisioning Portal [CPP]) con dispositivos de terceros.

SESIONES

Los Cisco Network Access Devices (NAD) utilizan Radius cisco-av-pair llamado audit-session-id para informar al servidor de Autenticación, Autorización y Contabilización (AAA) sobre el ID de sesión.

ISE utiliza ese valor para realizar un seguimiento de las sesiones y proporcionar los servicios correctos para cada flujo. Otros proveedores no admiten el par cisco-av.

ISE debe basarse en los atributos IETF recibidos en la solicitud de acceso y la solicitud de cuentas.

Después de recibir la solicitud de acceso, ISE crea una ID de sesión de Cisco sintetizada (a partir de ID de estación de llamada, puerto NAS, dirección IP de NAS y secreto compartido). Ese valor tiene un significado local solamente (no enviado vía red).

Como resultado, se espera que cada flujo (BYOD, CWA, NSP, CPP) adjunte los atributos correctos, por lo que ISE puede volver a calcular la ID de sesión de Cisco y realizar una búsqueda para correlacionarla con la sesión correcta y continuar el flujo.

Redirección de URL

ISE utiliza un par cisco-av de RADIUS llamado url-redirect y url-redirect-acl para informar a NAD de que se debe redirigir el tráfico específico.

Otros proveedores no admiten el par cisco-av. Por lo general, estos dispositivos deben configurarse con una URL de redirección estática que señale a un servicio específico (perfil de autorización) en ISE.

Una vez que el usuario inicia la sesión HTTP, esos NAD se redirigen a la URL y también adjuntan argumentos adicionales (como la dirección IP o la dirección MAC) para permitir que ISE identifique la sesión específica y continúe el flujo.

CoA

ISE utiliza el comando Radius cisco-av-pair called subscriber:command,

subscriber:reauthenticate-type para indicar qué acciones debe realizar NAD para una sesión específica.

Otros proveedores no admiten el par cisco-av. Por lo general, estos dispositivos utilizan RFC CoA (3576 o 5176) y uno de los dos mensajes definidos:

- pedido de desconexión (también llamado paquete de desconexión) que se utiliza para desconectar la sesión (muy a menudo para forzar la reconexión)
- Transferencia CoA: se utiliza para cambiar el estado de la sesión de forma transparente sin desconexión (por ejemplo, sesión VPN y nueva ACL aplicada).

ISE admite tanto Cisco CoA con par av de Cisco como RFC CoA 3576/5176.

Solución en ISE

Con el fin de ofrecer compatibilidad con proveedores externos, ISE 2.0 introdujo un concepto de perfiles de dispositivos de red que describe cómo se comporta un proveedor específico: cómo se admiten sesiones, redirección de URL y CoA.

Los perfiles de autorización son de un tipo específico (perfil de dispositivo de red) y una vez que se produce la autenticación, el comportamiento de ISE se deriva de ese perfil.

Como resultado, ISE puede gestionar fácilmente dispositivos de otros proveedores. Además, la configuración en ISE es flexible y permite ajustar o crear nuevos perfiles de dispositivos de red.

Este artículo presenta el uso del perfil predeterminado para el dispositivo Aruba.

Más información sobre la función:

Perfiles de dispositivos de acceso a la red con Cisco Identity Services Engine

ISE de Cisco

Paso 1. Agregar el controlador inalámbrico de Aruba a los dispositivos de red

Vaya a Administración > Recursos de red > Dispositivos de red. Elija el perfil de dispositivo correcto para el proveedor seleccionado, en este caso: ArubaWireless. Asegúrese de configurar el secreto compartido y el puerto CoA como se muestra en las imágenes.

Network Devices List > aruba

Network Devices

		* Name	aruba		
		Description			
	* IP Addres	s: 10.62.148.118	/ 32		
		* Device Profile	ArubaWireless	•	
		Model Name	•		
		Software Version	.		
	Network De	vice Group			
	Location	All Locations	Set To Defa	11+	
		All Locations			
	evice type	All Device Types	Set To Defa	llt	
✓	▼ RADIUS	Authentication Settings			
		Enable Auth	entication Settings		
			Protocol	RADIUS	
			* Shared Secret	•••••	Show
			Enable KeyWrap	i	
		* к	ey Encryption Key		Show
		* Message Authe	nticator Code Key		Show
			Key Input Format	ASCII HEXADEC	IMAL
			CoA Port	3799	Set To Default

En caso de que no haya un perfil disponible para el proveedor deseado, se puede configurar en Administration > Network Resources > Network Device Profiles.

Paso 2. Configurar perfil de autorización

Vaya a Policy > Policy Elements > Results > Authorization > Authorization Profiles y elija el mismo perfil de dispositivo de red que en el paso 1. ArubaWireless. El perfil configurado es Aruba-redirect-BYOD with BYOD Portal y se muestra en las imágenes.

Authorization Profiles > A	ruba-redirect-BYOD
Authorization Prof	file di la constante di la const
* Name	Aruba-redirect-BYOD
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	Terret ArubaWireless 💌 🕀
Common Tasks Web Redirection (Native Supplicant	CWA, MDM, NSP, CPP) Provisioning Value BYOD Portal (default)
- Advanced Attribute	es Settings
Select an item	
▼ Attributes Details	
Access Type = ACCES	SS_ACCEPT

Falta parte de la configuración de redirección web, donde se genera un enlace estático al perfil de autorización. Aunque Aruba no admite la redirección dinámica al portal de invitados, hay un enlace asignado a cada perfil de autorización, que se configura en Aruba y se muestra en la imagen.

▼ Common Tasks	
Native Supplicant Provisioning	Value BYOD Portal (default) +
The network device profile selected above re	quires the following redirect URL to be configured manually on the network access device in order to enforce web redirection:
https://iseHost:8443/portal/g?p=10	mawmklieZQhapEvIXPAoELx

Paso 3. Configuración de las reglas de autorización

Navegue hasta Policy > Authorization Rules y la configuración es como se muestra en la imagen.

~	Basic_Authenticated_Access	if	Employee AND (EAP-TLS AND EndPoints:BYODRegistration EQUALS Yes)	then	PermitAccess
~	ArubaRedirect	if	Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba	then	Aruba-redirect-BYOD

En primer lugar, el usuario se conecta al SSID mgracarz_aruba e ISE devuelve el perfil de autorización Aruba-redirect-BYOD, que redirige al cliente al portal BYOD predeterminado. Una vez finalizado el proceso de BYOD, el cliente se conecta con EAP-TLS y se concede acceso completo a la red.

En las versiones más recientes de ISE, la misma política podría parecerse a la siguiente:

	ofiling Posture Client Provi	isioning Polic	cy Elements					Click here to do visibility s	setup Do not show t	his again.	
Status	Policy Set Name	Descript	ion	Conditions				Allowed Pr	otocols / Server	Sequenc	e Hits
Search											
ø	Aruba			្រៃ Aruba-Aruba-Essid-Na	ame EQUALS mgarcarz_arub	a		Default Ne	twork Access	x • +	•
> Authentication	on Policy (1)										
Authorization	Policy - Local Exceptions										
Authorization	Policy - Global Exceptions	1									
 Authorization 	Policy (3)										
Authorization	Policy (3)					Results					
Authorization + Status	Rule Name	Condit	ons			Results Profiles		Security Groups		Hits	Action
Authorization Status Search	Policy (3)	Condit	ons			Results Profiles		Security Groups		Hits	Actions
Authorization Authorization Search	Policy (3)	Condit	ons as example.	om-ExternalGroups EQUALS exampl	le.com/Builtin/Administrators	Results Profiles		Security Groups		Hits	Action
Authorization Authorization Search	Rule Name	Condit	ons ම example. දී EndPoints	om ExternalGroups EQUALS example BYODRegistration EQUALS Yes	le.com/Builtin/Administrators	Results Profiles	•	Security Groups		Hits	Action
Authorization Authorization Search Ø	Rule Name	Condit	example. È: EndPoint: P Network A	om-ExternalGroups EQUALS exampl BYODRegistration EQUALS Yes ccess-EapAuthentication EQUALS Ex	Ne.com/Builtin/Administrators	Results Profiles	*	Security Groups	× #	Hits	Action:
Authorization Authorization Search O	Rule Name Authorized Redirect	Condit AND E	example.o	om ExternalGroups EQUALS exampl •BYODRegistration EQUALS Yes ccess-EapAuthentication EQUALS E Name EQUALS mgarcarz_aruba	ile.com/Builtin/Administrators	Results Profiles ×PermitAccess ×Aruba_Redirect_BYOD	•	Select from list	· #	Hits 0	Action:

AP de Aruba

Paso 1. Configuración del portal cautivo

Para configurar Captive Portal en Aruba 2004, navegue hasta Security > External Captive Portal y agregue uno nuevo. Ingrese esta información para una configuración adecuada y como se muestra en la imagen.

- Tipo: Autenticación Radius
- IP o nombre de host: servidor ISE
- URL: enlace que se crea en ISE en la configuración del perfil de autorización; es específico de un perfil de autorización concreto y se puede encontrar aquí en la configuración de redirección web

Native Supplicant Provisioning	Ŧ	Value	BYOD Portal (default)		•				
The network device profile selected above requires the following redirect URL to be configured manually on the network access device in order to enforce web redirection:									

https://iseHost:8443/portal/g?p=10lmawmklleZQhapEvIXPAoELx

• Puerto: número de puerto en el que el portal seleccionado está alojado en ISE (de forma predeterminada: 8443), como se muestra en la imagen.

mgarcarz_ise20			
Туре:	Radius Authentication -		
IP or hostname:	mgarcarz-ise20.example.		
URL:	/portal/g?p=Kjr7eB7RrrLl		
Port:	8443		
Use https:	Enabled 💌		
Captive Portal failure:	Deny internet		
Automatic URL Whitelisting:	Disabled 💌		
Redirect URL:		(optional)	
		ОК	Cancel

Paso 2. Configuración del servidor de RADIUS

Vaya a Security > Authentication Servers para asegurarse de que el puerto CoA sea el mismo que el configurado en ISE como se muestra en la imagen.

De forma predeterminada, en Aruba 2004, está configurado en 5999, sin embargo, no cumple con RFC 5176 y tampoco funciona con ISE.

Security

Authentication Servers	Users for Interna	l Server	Roles	Blacklisting
Edit				
Name:	mgarcarz_ise20			
IP address:	10.48.17.235			
Auth port:	1812			
Accounting port:	1813			
Shared key:	•••••			
Retype key:	•••••			
Timeout:	5	sec.		
Retry count:	3			
RFC 3576:	Enabled 🗾			
Air Group CoA port:	3799			
NAS IP address:	10.62.148.118	(optiona	1)	
NAS identifier:		(optiona	l)	
Dead time:	5	min.		
DRP IP:				
DRP Mask:				
DRP VLAN:				
DRP Gateway:				

Nota: En la versión 6.5 y posteriores de Aruba, seleccione también la casilla de verificación "Portal cautivo".

Paso 3. Configuración de SSID

• La ficha Seguridad es la que se muestra en la imagen.

it mgarcarz_aruba								
WLAN Settings	2 VLAN	3 Security 4 Ac						
curity Level								
lore	Key management:	WPA-2 Enterprise						
ecure	Termination:	Disabled						
	Authentication server 1:	mgarcarz_ise20 🗾 Edit						
Enterprise	Authentication server 2:	Select Server 💌						
Personal	Reauth interval:	0 hrs. 🔽						
Open	Authentication survivability:	Disabled Perform MAC authentication before 802.1X						
	MAC authentication:							
•		MAC authentication fail-thru						
ess	Accounting:	Use authentication servers						
ecure	Accounting interval:	0 min.						
	Blacklisting:	Disabled						
	Fast Roaming							
	Opportunistic Key Caching(OKC):							
	802.11r:							
	802.11k:							
	802.11v:							
	t mgarcarz_aruba WLAN Settings curity Level fore ecure Personal Open ess ecure	WLAN Settings 2 VLAN Settings 2 VLAN Settings 2 VLAN Settings Authentication server 1: Authentication server 2: Personal Open Authentication survivability: MAC authentication: Accounting: Accounting: Blacklisting: Fast Roaming Opportunistic Key Caching(OKC): 802.11r: 802.11r: 802.11r:						

• Ficha Acceso: seleccione Regla de acceso basada en red para configurar el portal cautivo en SSID.

Utilice el portal cautivo configurado en el paso 1. Haga clic en New, elija Rule type: Captive portal, Splash page type: External como se muestra en la imagen.

1 WLAN Settin	gs	2	VLAN	3	Security	4	Access			
Access Rules										
More Control - Role-based		Acce → Er ● Al ● Al	ss Rules (3) <mark>Iforce captive portal</mark> Iow any to all destinations Iow TCP on ports 1-20000	on server :	10.48.17.235					
A Network-bas	Edit Rule	Enfo	rce captive portal							
- Network-base	Rule typ	e:		Splash page type:			Captive portal profile:			
- Unrestricted	Captive	port	al 🔽	Exte	rnal 👤		mgarcarz_ise20 _			
Less										

Además, permite todo el tráfico al servidor ISE (puertos TCP en el rango 1-20000), mientras que

la regla configurada de forma predeterminada en Aruba: Permitir cualquiera a todos los destinos parece no funcionar correctamente como se muestra en la imagen.

1	1 WLAN Settings		2 VLAN	3 S	ecurity	4	Access				mgarcarz_
Ac	cess Rules										
M Co	ore ntrol - Role-based		Access Rules (3) + Enforce captiv Allow any to a Allow TCP on p	e portal II destinations ports 1-20000 on server 10.	.48.17.235						
	🔿 - Network-base	Edit Rule	e Allow TCP on po	rts 1-20000 on server 10.48 Service:	8.17.235	Act	ion:		Destinatio	in:	
	- Unrestricted	Acces	s control 🗾	Network	custom 💌	All	ow	•	to a part	icular server	•
Le Co	Less Control Options			 Application Application category Web category Web reputation 	Protocol: TCP Port(s): 1-20000				IP: 10.48.17	.235	
			5:	Log Blacklist	Classify media		DSCP tag 802.1p priority				
										ОК	Cancel

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Paso 1. Conexión a SSID mgarcarz_aruba con EAP-PEAP

Aparece el primer registro de autenticación en ISE. Se ha utilizado la política de autenticación predeterminada; el perfil de autorización de Aruba-redirect-BYOD se ha devuelto tal y como se muestra en la imagen.

cisco Identity Se	ervices Engine	Home	 Operations 	Policy	Guest Access	Administration	Work Centers			
RADIUS Livelog	TACACS Livelog	Reports	▶ Troubleshoot	Adaptive Netw	ork Control					
Mi	isconfigured Supplic 1	ants 🕡		Miso	onfigured Netw 0	vork Devices (i)	RADIUS Drops (i) 12			Client Stopped Respond O
📓 Show Live Sessions 🛛 🤬 Add or Remove Columns 🕶 🍕 Refresh 👔 Reset Repeat Counts										
Time	▼ Status All ▼ Det.	R. [dentity 🕐	Endpoint ID 🛞	Authenticat	ion Policy ()	Authorization Policy	Authorization Profiles	Network Device	Event ()
2015-10-29 22:2	23:37 🕦 🔒	0 0	isco C	0:4A:00:14:6E:3	1 Default >>	Dot1X >> EAP-TLS	Default >> Basic_Authenticated	PermitAccess		Session State is Started
2015-10-29 22:2	3:37 🗹 🛛	c	isco C	0:4A:00:14:6E:3	1 Default >>	Dot1X >> EAP-TLS	Default >> Basic_Authenticated	PermitAccess	aruba	Authentication succeeded
0015 10 00 00 1	0.00	0	isco (0:44:00:14:6E:3	Default >>	Dot1X >> Default	Default >> ArubaRedirect	Anuba-redirect-BVOD	aruba	Authentication succeeded

ISE devuelve el mensaje de aceptación de acceso de RADIUS con EAP correcto. Tenga en cuenta que no se devuelven atributos adicionales (no se devuelve el URL-redirect o el URL-redirect-acl de Cisco av-pair), como se muestra en la imagen.

No.	Source	Destination	Protocol	Length	Info	User-Nam(Acct-Session-Id
133	10.62.148.118	10.48.17.235	RADIUS	681	Access-Request(1) (id=102, l=639)	cisco	
134	10.48.17.235	10.62.148.118	RADIUS	257	Access-Challenge(11) (id=102, l=215)		
135	10.62.148.118	10.48.17.235	RADIUS	349	Access-Request(1) (id=103, l=307)	cisco	
136	10.48.17.235	10.62.148.118	RADIUS	235	Access-Challenge(11) (id=103, l=193)		
137	10.62.148.118	10.48.17.235	RADIUS	386	Access-Request(1) (id=104, l=344)	cisco	
138	10.48.17.235	10.62.148.118	RADIUS	267	Access-Challenge(11) (id=104, l=225)		
139	10.62.148.118	10.48.17.235	RADIUS	450	Access-Request(1) (id=105, l=408)	cisco	
140	10.48.17.235	10.62.148.118	RADIUS	283	Access-Challenge(11) (id=105, l=241)		
141	10.62.148.118	10.48.17.235	RADIUS	386	Access-Request(1) (id=106, l=344)	cisco	
142	10.48.17.235	10.62.148.118	RADIUS	235	Access-Challenge(11) (id=106, l=193)		
143	10.62.148.118	10.48.17.235	RADIUS	386	Access-Request(1) (id=107, l=344)	cisco	
149	10.48.17.235	10.62.148.118	RADIUS	363	Access-Accept(2) (id=107, l=321)	cisco	
150	10.62.148.118	10.48.17.235	RADIUS	337	Accounting-Request(4) (id=108, l=295)	cisco	048D88888142-C04A00146E31-42F8
153	10.48.17.235	10.62.148.118	RADIUS	62	Accounting-Response(5) (id=108, l=20)		
Pack	et identifier: Ox	-, 6h (107)					
Leng	th: 321						
Auth	enticator: 1173a3	d3ea3d0798fe30fdac	-f644f19				
[Thi	s is a response t	o a request in fra	me 143]				
[Tim	e from request: C	038114000 seconds	1				
⇒ ∆ttr	ibute Value Pairs		,				
D AV	P: l=7 t=User-Na	me(l): cisco					
Þ AV	P: 1=67 t=State(24): 5265617574685	3657373696f6	e3a3061	3330313165625862		
Þ AV	P: 1=87 t=Class(25): 434143533a306	133303131656	2586269	7544413379554e6f		
ΔV	P: 1=6	sage(79) Last Segme	ent[1]	2000200	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		
b av	P: 1=18 t=Messar	e.Authenticator(80)	• e0h74092c	acf 8880	3464370326761513		
Þ AV	P: 1=58 t=Vendor	-Specific(26) v=Mi	rosoft(311)				
Þ AV	P: l=58 t=Vendor	-Specific(26) v=Mic	rosoft(311)				

Aruba informa de que se ha establecido la sesión (la identidad EAP-PEAP es cisco) y que la función seleccionada es mgarcarz_aruba, como se muestra en la imagen.



Esa función es responsable de la redirección a ISE (funcionalidad de portal cautivo en Aruba).

En Aruba CLI, es posible confirmar cuál es el estado de autorización actual para esa sesión:

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	Р	1	Ν
10.62.148.71	C0:4A:00:14:6E:31	138/0	0/0	0	0	6/65535		1	в
0.0.0.0	C0:4A:00:14:6E:31	138/0	0/0	0	0	0/65535	Р	1	В
172.31.98.1	04:BD:88:C3:88:14	105/0	0/0	0	1	0/65535	Р	3333	В
0.0.0.0	04:BD:88:C3:88:14	105/0	0/0	0	0	0/65535	Р	1	Ν
04:bd:88:c3:88:	14#								

Y para verificar el ID de ACL 138 para los permisos actuales:

<#root>

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

show datapath acl 138

Datapath ACL 138 Entries

Que coincida con lo que se configuró en la GUI para ese Rol, como se muestra en la imagen.

Security							
Authentication Servers Users for 2	Internal Server Ro	oles Blacklisting	Firewall Settings	Inbound Firewall	Walled Garden		
Roles	Access Rules for	mgarcarz_aruba					
default_wired_port_profile wired-instant ArubaAAA wcecot_BYOD_aruba mgarcarz_aruba	default_wired_port_profile Enforce captive portal Allow any to all destinations Allow TCP on ports 1-20000 on server 10.48.17.235 mgarcarz_aruba Marcarz_aruba						
New Delete	New Edit De	elete 🔒 🖶					

Paso 2. Redirección del tráfico del navegador web para BYOD

Una vez que el usuario abre el navegador web y escribe cualquier dirección, se produce la redirección como se muestra en la imagen.



Al observar las capturas de paquetes, se confirma que Aruba suplanta el destino (5.5.5.5) y devuelve la redirección HTTP a ISE.

Observe que es la misma URL estática configurada en ISE y copiada en Captive Portal en Aruba, pero además se agregan varios argumentos como se muestra a continuación en la imagen:

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

Image: Section Connection (Wireshark:10.3 (SWN Rev SB022 from /tunk:10)) File: <												
Eie Edit Yiew Go Capture Analyze Statistics Telephony Tools Internals Help • • • • • • • • • • • • • • •	📕 *W	ireless Network Connection	[Wireshark 1.10.3 (SVN Rev 530	22 from /tru	nk-1.10)]							
••••••••••••••••••••••••••••••••••••	<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture	Analyze Statistics Telephor	ny <u>T</u> ools	Internals Help							
Filter Intp Peression Clear Apply Save No. Source Destination Protocol Length Info 724 10.62.148.71 S.5.5.5 HTP 335 GET / HTP/1.1 302 752 10.62.148.71 HTP 438 GET / HTP/1.1 302 752 10.62.148.71 HTP 515 GET / HCS1.txt HTP/1.1 302 8 Frame 726: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits), 10.62.148.71 internet virt. Go:4a:00:14:6e:31) 9 Enternet virt.sion 4, social of social ocial o	0 () 🧵 🔳 🔬 🖻 🛅	🗶 🛃 🔍 🔶 🔿 🥥	₹ •	🗐 🗐 (Q, Q, 🖸 🖉 🛛 🥵 % 🧝							
No. Source Detination Protocol Length Info 724 10.62.148.71 5.5.5.5 HTTP 335 GET / HTTP/1.1 302 752 10.62.148.71 23.62.99.25 HTTP 151 GET /ncsi.txt HTTP/1.1 302 # Frame 726: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits) on interface 0 * # Ethernet II, src: 04:bd:88:c3:88:14 (04:bd:88:c3:88:14), DSt: TP-inKt_J4:68:31 (C0:44:00:14:68:31) * # Internet Protocol Protocol, src Port: http (80), DSt Port: 53939 (53939), Seg: 1, Ack: 282, Len: 444 * Hypertext Transfer Protocol server: \n * # HTTP/1.1 302 Vin server: \n * # Hypertext Transfer Protocol, src Port: http (80), DSt Port: 53939 (53939), Seg: 1, Ack: 282, Len: 444 * Hypertext Transfer Protocol * * # Hypertext Transfer Protocol * * # Connection: Close\r\n * * Date: Thu, 01 Jan 1970 05:36:56 GMT/\n * * Connection: Close\r\n * * * * * * * * * * * * * * * *	Filter:	http			Expression Clear Apply Save							
724 10.62.148.71 5.5.5.5 HTTP 335 GET / HTTP/1.1 726 5.5.5.5 10.62.148.71 HTTP 438 HTTP/1.1 302 752 10.62.148.71 23.62.99.25 HTTP 151 GET /ncsi.txt HTTP/1.1 302 Frame 726:498 bytes on wire (3984 bits), 498 bytes captured (3984 bits) on interface 0 Ethernet II, Src: 04:bd:88:c3:88:14 (04:bd:88:c3:88:14), Dst: Tp-LinkT_14:6e:31 (c0:4a:00:14:6e:31) Internet Protocol Version 4, Src: 5.5.5.5 (5.5.5.5), Dst: 10.62.148.71 (10.62.148.71) Internet Protocol Version 4, Src: 5.5.5.5 (0.5.5.5), Dst: 10.62.148.71 (10.62.148.71) Internet Protocol Version 4, Src: 5.5.5 (0.5.5.5), Dst: 10.62.148.71 (10.62.148.71) HTTP/1.1 302/r/n Internet Protocol Version 4, Src: 5.5.5 (0.5.5.5), Dst: 10.62.148.71 (10.62.148.71) Internet Protocol Version 4, Src: 5.5.5 (2.5.5.5) Internet Protocol Version 4, Src: 5.5.5 (2.5.5) BHTP/1.1 302/r/n <tr< td=""><td>No.</td><td>Source</td><td>Destination</td><td>Protocol</td><td>Length Info</td><td></td></tr<>	No.	Source	Destination	Protocol	Length Info							
725 5.5.5.5 10.62.148.71 HTTP 498 HTTP/1.1 302 752 10.62.148.71 23.62.99.25 10.62.148.71 HTTP 515 HTTP/1.1 302 IF FRAME 726: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits) on interface 0 IF Frame 726: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits) on interface 0 Internet II, Src: 04:bd:88:c3:88:14 (04:bd:88:c3:88:14), Dst: TP-LinkT_14:6e:31 (C0:4a:00:14:6e:31) Internet Protocol version 4, Src: 5.5.5.5 (5.5.5.5), Dst: 10.62.148.71 (C0:4a:00:14:6e:31) Internet Transmission Control Protocol, Src Port: http (80), Dst Port: S3939 (S3939), Seq: 1, Ack: 282, Len: 444 Hypertext Transfer Protocol Gache-Control: no-cache, no-store, must-revalidate, post-check=0, pre-check=0\r\n Itrume relevation: https://maarcare-ise20.example.com:843/portal/grp=10/mawnkllez0hapev/XPA0ELx&cmd=login&mac=c0:4a:C Connection: close\r\n Obbo 70 72 65 2d 63 68 56 63 6b 3d 30 0d 0a 8C 6f 63 Obbo 70 72 65 2d 63 68 56 63 6b 3d 30 0d 0a 8C 6f 63 <t< td=""><td>7</td><td>24 10.62.148.71</td><td>5.5.5.5</td><td>HTTP</td><td>335 GET / HTTP/1.1</td><td></td></t<>	7	24 10.62.148.71	5.5.5.5	HTTP	335 GET / HTTP/1.1							
752 10.62.148.71 23.62.99.25 HTTP 151 GET /ncs1.txt HTTP/1.1 755 23.62.99.25 10.62.148.71 HTTP 515 HTTP/1.1 302 # Frame 726: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits) on interface 0 * # Ethernet II, Src: 04:bd:88:c3:88:13+ (04:bd:88:c3:88:13+0, Dst: Tp-Lintr.14:6e:31 (C0:4a:00:14:6e:31) * # Internet Protocol version 4, Src: 5.5.5 (5.5.5.5), Dst: 10.62.148.71 (10.62.148.71) * # Transmission Control Protocol, Src Port: http (80), Dst Port: 53939 (53939), Seq: 1, Ack: 282, Len: 444 * # NTPYL1.1 302/Vn * Server: \r\n Date: Thu, 01 an 1970 05:36:56 GMT\r\n cache-Control: no-cache,no-store,must-revalidate,post-check=0,pre-check=0\r\n [Turtneted] Location: https://mgarcarz-ise20.example.com:8443/portal/g?p=01mawmk11e2Qhaptv1xPA0ELx&cmd=login&mac=c0:4a:0 Connection: close\r\n * "HTTP 1 response 1/11 * # * @ dod 01 c6 65 2e 63 6f 66 3a 38 34 34 32 f 70 64 dito 17 26 36 2f 67 31 7 33 2 f 76 64 dito 17 26 46 16 61 7 74 47 0 73 3a 2 f 76 dito 17 74 74 77 73 36 2 f 6 31 6 7 73 36 9 f 73 35 9 0 73 31 9 4 35 6 0 0 4 dito 17 0 0 0 0 14 7 0 7 2 a 16 2 c 6 7 6 3 7 73 36 9 f 73 36 9 f 6 6 30 31 30 0 0 31 30 2 dito 2 c 7 7 37 7 73 36 9 f 4 31 6 6 f 6 7 7 33 19 4 f 6 5 6 6 7 73 36 9 f 6 6 6 3 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	7.	26 5.5.5.5	10.62.148.71	HTTP	498 HTTP/1.1 302							
75 23.62.99.25 10.62.148.71 HTP StD HTP/1.1 302 Frame 726: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits) on interface 0 Ethernet II, Src: 04:bit88:c138:142 (05:43:00:14:6e:31) (0:4a:00:14:6e:31) Internet Protocol Version 4, Src: 5.5.5 (5.5.5.5), Dst: 10.62.148.71 (10.62.148.71) Internet Protocol Protocol, Src Port: http (80), Dst Port: 53939 (53939), Seq: 1, Ack: 282, Len: 444 Hypertext Transfer Protocol Hypertext Transfer Protocol Hypertext Transfer Protocol Barter, Thu, 01 Jan 1970 05:36:56 GMT/r\n Cache-Control: no-cache, no-store, must-revalidate, post-check=0, pre-check=0\r\n (truncated] Location: https://mgarcar2-ise20.example.com:8443/portal/g?p=10.mawmklleZQhaptv1XPAOELx&cmd=login&mac=c0:4a:0 (r/n truncated] Location: https://mgarcar2-ise20.example.com:8443/portal/g?p=10.mawmklleZQhaptv1XPAOELx&cmd=login&mac=c0:4a:0 (r/n (truncated] Location: https://mgarcar2-ise20.example.com:8443/portal/g?p=10.mawmklleZQhaptv1XPAOELx&cmd=login&mac=c0:4a:0 (r/n	7	52 10.62.148.71	23.62.99.25	HTTP	151 GET /ncsi.txt HTTP/1.1							
B Frame 726: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits) on interface 0 B Ethernet II, Src: 04:bd:88:c3:88:14 (04:bd:88:c3:88:14), Dst: Tp-LinkT_14:6e:31 (c0:4a:00:14:6e:31) B Internet Protocol Version 4, Src: 55.5 (55.5 5), Dst: 10.62.148.71 (10.62.148.71) B Transmission Control Protocol, Src Port: http (80), Dst Port: 53939 (53939), Seq: 1, Ack: 282, Len: 444 B Wypertext Transfer Protocol B HTTP/L.1 302\r\n B Cache-Control: no-cache, no-store, must-revalidate, post-check=0, pre-check=0\r\n C frameAted Location: https://mgarcanz-ise20.example.com:8443/portal/g?p=10lmaxmkllezQhapEvlXPAGELx&cmd=login&mace=c0:4a:0 C connection: close\r\n r\n P frame 726 65 2d 63 68 65 63 6b 3d 30 0d 0a 4c 6f 63 D re-check=0, IDC C dot 70 72 65 2d 63 68 65 63 6b 3d 30 0d 0a 4c 6f 63 D re-check =0, IDC M ortal if transfer 1/1 W m P ortal if transfer 1/1 C method for the form of the	1	55 23.62.99.25	10.62.148./1	нттр	515 HTTP/1.1 302							
B Impartext: naising in rotocol B Impartext: naising in rotocol B Impartext: naising in rotocol Server: \r\n Date: Thu, 01 Jan 1970 05::36:56 GMT\r\n Cache-Control: no-cache,no-store,must-revalidate,post-check=0,pre-check=0\r\n Connection: close\r\n (r\n Introp resoonse 1/11 * (r\n (r\n)	 Fra Eth Int Tra 	<pre>Frame 726: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits) on interface 0 Ethernet II, Src: 04:bd:88:c3:88:14 (04:bd:88:c3:88:14), Dst: Tp-LinkT_14:6e:31 (c0:4a:00:14:6e:31) Internet Protocol Version 4, Src: 5.5.5 (5.5.5.5), Dst: 10.62.148.71 (10.62.148.71) Transmission Control Protocol, Src Port: http (80), Dst Port: 53939 (53939), Seq: 1, Ack: 282, Len: 444 Hypertext Transfer Protocol</pre>										
Server::r\n Date: Thu, 01 Jan 1970 05:36:56 GMT\r\n Cache-Control::no-cache,no-store,must-revalidate,post-check=0,pre-check=0\r\n [truncated] Location: https://mgarcarz-ise20.example.com:8443/portal/g?p=101mawmk11eZQhapEv1XPAOELx&cmd=login&mac=c0:4a:0 Connection: close\r\n \r\n HHTTP response 1/11 * @ 00b0 70 72 65 2d 63 68 65 63 6b 3d 30 0d 0a 4c 6f 63 00c0 61 74 69 6f 6e 3a 20 08 74 74 70 73 3a 2f 2f 6d ation: h ttps://m garcarz-ise20.example.com:8443/portal/g?p=101mawmk11eZQhapEv1XPAOELx&cmd=login&mac=c0:4a:0 00c0 6f 72 74 63 66 76 6e 3a 20 68 74 74 70 73 3a 2f 2f 64 ation: h ttps://m garcarz-ise20.exa 00c0 6f 72 74 61 6c 2f 67 3f 70 3d 31 4f 6c 6d 61 77 00f0 6f 05 2e 63 6d 6d 43 d6 cf 6f 76 96 6e 26 6d 0100 6f 06 5c 6c 17 72 73 69 64 3d 6d 67 61 72 63 0120 6f 03 3d 63 30 3a 34 13 30 2a 31 34 3a 36 0130 65 3a 33 31 26 65 73 73 69 64 3d 66 76 67 62 76 63 6e 0140 6f 72 74 61 72 75 61 72 76 61 70 6e 61 6d 65 0130 63 3d 63 30 3a 34 13 32 25 73 31 12 66 61 70 6e 61 6d 65 0130 65 3a 33 31 26 67 77 73 26 63 66 76 76 96 6e 26 6d 72 74 63 32 53 34 11 31 32 26 76 63 66		$\frac{1}{1} \frac{1}{1} \frac{302}{r}n$	0001									
Date: Thu, 01 Jan 1970 05:36:56 GMT\r\n Cache-Control: no-cache,no-store,must-revalidate,post-check=0,pre-check=0\r\n [truncated] Location: https://mgarcarz-ise20.example.com:8443/portal/g?p=10]maxmklleZQhapEvlXPAOELx&cmd=login&mac=c0:4a:0 Connection: close\r\n \r\n [HTTP response 1/1] 00b0 70 72 65 2d 63 68 65 63 6b 3d 30 0d 0a 4c 6f 63 00c0 61 74 69 6f 6e 3a 20 68 74 74 70 73 3a 2f 2f 6d 00c0 61 74 69 6f 6e 3a 20 68 74 74 70 73 3a 2f 2f 6d 00c0 61 67 72 66 17 72 ad 69 73 65 32 30 2e 65 78 00e0 61 6d 70 6c 65 2e 63 6f 6d 3a 38 34 34 33 2f 70 00f0 6f 72 74 61 6c 2f 67 7 70 3d 14 f6 c6 d6 17 7 0010 6d 6b 6c 6c 65 5a 51 68 61 70 45 76 6c 28 50 41 multicache approximation approxi		Server:\r\n										
Cache-Control: no-cache,no-store,must-revalidate,post-check=0,pre-check=0\r\n [truncated] Location: https://mgarcarz-ise20.example.com:8443/portal/g?p=101mawmklleZQhapEv1XPAOELx&cmd=login&mac=c0:4a:0 [vr\n [HTTP resonse 1/1] [truncated] Location: https://mgarcarz-ise20.example.com:8443/portal/g?p=101mawmklleZQhapEv1XPAOELx&cmd=login&mac=c0:4a:0 [vr\n [HTTP resonse 1/1] [truncated] Location: https://mgarcarz-ise20.example.com:8443/portal/g?p=101mawmklleZQhapEv1XPAOELx&cmd=login&mac=c0:4a:0 [vr\n [HTTP resonse 1/1] [truncated] Location: https://mgarcarz-ise20.example.com:8443/p [truncated] Location: https://mgarcarz-ise20.example.co		Date: Thu, 01 Jan 19	70 05:36:56 GMT\r\n									
[truncated] Location: https://mgarcarz-ise20.example.com:8443/portal/g?p=101mawmk11eZQhapEv1XPAOELx&cmd=login&mac=c0:4a:G Connection: close/r\n (r\n [HTTP resoonse 1/1] Image: com:8443/portal/g?p=101mawmk11eZQhapEv1XPAOELx&cmd=login&mac=c0:4a:G (r\n [HTTP resoonse 1/1] Image: com:8443/portal/g?p=101mawmk11eZQhapEv1XPAOELx&cmd=login&mac=c0:4a:G (r\n [ImtTP resoonse 1/1] Image: com:8443/portal/g?p=101maw (r\n) 00b0 70 72 65 2d 63 68 65 63 6b 3d 30 0d 0a 4C 6f 6 00c0 61 74 69 6f 6e 3a 20 68 74 74 70 73 3a 2f 2f 6d ation: h ttps://m 00c0 61 67 72 63 61 72 7a 2d 69 73 65 32 30 2e 65 78 garcarz-ise20.ex 00c0 61 67 27 74 61 6c 2f 67 3f 70 3d 31 4f 6c 6d 61 70 ortal/g? p=101maw 0100 6d 65 45 2e 63 6d 64 3d 6c 6f 67 69 6e 2e 6 com:8443/portal/g? 0100 6f 45 4c 78 2f 73 69 64 3d 6d 6f 6f 7 61 2e 6 com:extal/portal/g? 0120 61 63 3d 63 30 3a 34 61 3a 30 30 3a 31 34 3a 36 ac=c0:4A :00:14:6 0130 65 3a 33 12 66 57 77 36 96 43 d6 6f 66 7 6 63 6e com:ax_antb akip=10. 0140 61 72 74 5f 61 72 75 62 61 26 69 70 3d 31 30 2e ar_x_antb akip=10.	c	ache-Control: no-ca	che, no-store, must-re	validate,	,post-check=0,pre-check=0\r\n							
Connection: close\r\n \r\n IHTP resonse 1/11		[truncated] Location	: https://mgarcarz-i	se20.exar	mple.com:8443/portal/g?p=10lmawmklleZQhapEvlXPAoELx&cmd=login&ma	c=c0:4a:0						
IHTTP response 1/11 * *	C C	Connection: close\r\	n									
Intro r 12500156 1/11 Image: State Sta		r\n HTTP response 1/1]				-						
OOb0 70 72 65 2d 63 68 65 63 d8 30 0d 0a 4c 6f 63 ation: http://m O0c0 61 74 69 6f 6a 3a 20 68 74 74 70 73 3a 2f 2f 6d ation: http://m O0c0 61 72 63 61 72 7a 2d 69 73 65 32 30 2e 65 78 garcarz- ise20.ex 00e0 61 64 6c 2f 6f 6d 31 4f 6c 6d 177 ortal/g? p=10/maw 0100 6d 6b 6c 65 5a 51 6a 6d 6d 6f 76 9c 6d 6d 6f 76 76 6c 8a 36 ac=c0:4a 100:14:6 6d ation: ation: atian; ation; atian; ation; atian; atian; ation;	<	ITTP TESDONSE 1/11	III			F.						
00c0 61 74 69 67 67 73 3a 25 76 67 73 3a 22 76 77 3a 32 27 67 3ample.com:8443/p 00 60 66 73 67 73 3a 31 47 66 62 66 67 67 66 62 66 61 77 01 74 74 74 74 74 74 74 74 74 74 74 74 73 3a 22 77 3a 32 72 72 73 33 32 26 67 74 74 74 74 74 74 74 74 74 74 74 74 74 74 74	00b0	70 72 65 2d 63 68	65 63 6b 3d 30 0d 0	4 C 6F 6	nre-chec k=0 loc							
0000 67 61 72 63 61 72 74 2d 69 73 65 32 30 2e 65 78 garcarz- ise20.ex 0000 61 6d 70 6c 65 2e 63 6f 6d 3a 38 34 34 33 2f 70 ample.co m:8443/p 0010 6f 72 74 61 6c 2f 67 3f 70 3d 31 4f 6c 6d 61 77 ortal/9? p=101maw 0100 6f 45 4c 78 26 63 6d 64 3d 6c 6f 67 69 6e 26 6d 0120 61 63 3d 63 30 3a 34 61 3a 30 30 3a 31 34 3a 36 ac=c0:4a :00:14:6 0130 65 3a 33 31 26 65 73 73 69 64 3d 6d 67 61 72 63 e:31&ess id=mgarc 0140 61 72 7a 5f 61 72 75 62 61 26 69 70 3d 31 30 2e arz_arub a&ip=10. 0150 36 32 2e 31 34 38 2e 37 31 26 61 70 6e 61 6d 65 0160 3d 30 34 25 33 41 62 64 25 33 41 38 38 25 33 41 =04%3Abd %3A88%3A 0170 63 33 25 33 41 38 38 25 33 41 31 34 26 76 63 6e c3%3A88% 3A14&evcn 0180 61 6d 65 3d 69 6e 73 74 61 6e 74 2d 43 33 25 33 0190 41 38 38 25 33 41 31 34 26 73 77 69 74 63 68 69 A88%3A14 &switchi 01a0 70 3d 73 65 63 75 72 65 6c 6f 67 69 74 63 68 69 A88%3A14 &switchi 01a0 70 3d 73 65 63 75 72 65 72 6b 73 2e 63 6f 62 61 72 p=secure login.ar 01b0 75 62 61 6e 65 74 77 6f 72 6b 73 2e 63 6f 62 62 di 72 p=secure login.ar 01b0 75 62 61 6e 65 74 77 6f 72 6b 73 2e 63 6f 62 53 22 url hevor rks.com& 01c0 76 72 63 67 74 67 66 63 ac 20 63 6c 6f 73 65 0d 0a 43 6f 6e rest.com and rest.com a	00c0	61 74 69 6f 6e 3a	20 68 74 74 70 73 3	a 2f 2f 6	5d ation: h ttps://m	<u>^</u>						
0000 01 00 06 05 22 03 03 33 34 33 27 70 ample.co mis443/p 00100 6d 66 62 67 37 70 3d 31 46 6d 6d 177 ortal/gr p=lolmaw 01100 6f 45 4c 78 26 63 6d 6d 6d 177 ortal/gr p=lolmaw 0120 61 63 30 33 14 6c 6d 717 6d 6d 6d 717 717 6d 6d 6d 717	00d0	67 61 72 63 61 72	7a 2d 69 73 65 32 3) 2e 65 7	78 garcarz- ise20.ex							
0100 6d 6b 6c 65 5a 51 6a 61 70 76 6c 58 50 41 mklle20h apev1xpA 0110 6f 45 4c 78 26 63 6d 3d 6a 30 3a 31 34 3a 36 oet_x&cmd = login&m 0120 61 63 30 3a 34 3a 36 ac=c0:4a :00:14:6 0130 65 3a 31 126 61 70 61 72 63 61 70 34 3a 22 arz_arub akip=10. 0140 61 72 73 56 61 70 66 65 62 148.7 1&apname 0160 3d 30 42 33 41 38 38 25 33 41 =04%3Abd %3A88%3A 0170 63 33 25 33 41 38 38 25 33 41 =04%3Abd %3A88%3A <t< td=""><td>00e0</td><td>6f 72 74 61 6c 2f</td><td>67 3F 70 3d 31 4F 6</td><td>+ 33 2T / 5 6d 61 7</td><td>70 ampie.com:8443/p 77 ortal/02 p=101maw</td><td></td></t<>	00e0	6f 72 74 61 6c 2f	67 3F 70 3d 31 4F 6	+ 33 2T / 5 6d 61 7	70 ampie.com:8443/p 77 ortal/02 p=101maw							
0110 6f 45 4c 78 26 63 6d 64 3d 6c 6f 67 69 6e 26 6d oct.x&cmd =login&m 0120 61 63 3d 63 30 3a 34 61 3a 30 30 3a 31 34 3a 36 ac=c0:4a :00:14:6 0130 65 3a 33 31 26 65 73 73 69 64 3d 6d 67 61 72 63 e:31&ess id=mgarc 0140 61 72 7a 5f 61 72 75 62 61 26 69 70 3d 31 30 2e arz_arub $a\&ip=10$. 0150 36 32 2e 31 34 38 2e 37 31 26 61 70 6e 61 6d 65 62.148.7 1&apname 0160 3d 30 34 25 33 41 32 64 170 6e 61 6d 65 66 cc 3&3A88% 3A 14&xvcn 0180 61 6d 65 3d 69 6e 73 74 61 6e 74 2d 43 33 25 33 41 =04&3Abd &3A88&3A 14&vccn 0180 61 6d 65 3d 69 6e 73 74 61 6e 74 2d 43 33 25 33 an=inst ant-c3% 30 0190 41 38 38 25 33 41 31 34 26 76 63 66 66 72 p=secure login.ar 01b0 75 62 61 66 65 74 77 6f 72 6b 73 2e 63 6f 6d 26 ubanetwo rks.com& 01c0 75 72 6c 3d 68 74 74 70 25 33 41 25 32 46 25 32 4r 1=hy $3A82FX2$ 01d0 46 35 2e	0100	6d 6b 6c 6c 65 5a	51 68 61 70 45 76 6	58 50 4	41 mkllezQh apEvlXPA							
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	0110	6f 45 4c 78 26 63	6d 64 3d 6c 6f 67 6	9 6e 26 6	5d OELx&cmd =login&m							
0140 61 72 73 51 61 76 97 93 93 13 02 a arz_arub a&hg=10. 0150 36 32 2 231 34 38 28 37 31 26 61 70 66 66 65 .148.7 1&apname 0160 36 32 25 33 41 38 38 25 33 41 =04%3Abd %3A88%3A 0170 63 33 25 33 41 31 34 26 76 63 6e c3%3A88% 3A14&/vcn 0180 61 66 66 74 2d 43 32 25 33 ame=inst ant-c3%3 0190 41 38 38 25 32 41 63 86 69 A88%3A14 & & & & & & & & & & & & & & & & & & &	0120	61 63 30 63 30 3a 65 3a 33 31 26 65	34 61 3a 30 30 3a 3. 73 73 69 64 3d 6d 6	L 34 3a 3 7 61 72 6	30 aC=CU:4a :00:14:0 53 e:31&ess id=moarc							
0150 36 32 2e 31 34 38 2e 37 31 26 61 70 6e 61 6d 65 62.148.7 1&apname 0160 3d 30 34 25 33 41 62 64 25 33 41 38 38 25 33 41 =-04%3Abd %3A88%3A 0170 63 33 25 33 41 38 38 25 33 41 31 34 26 76 63 6e 0180 61 6d 65 3d 69 6e 73 74 61 6e 74 2d 43 33 25 33 0190 41 38 38 25 33 41 31 34 26 73 77 69 74 63 68 69 A88%3A14 &switchi 01a0 70 3d 73 65 63 75 72 65 6c 6f 67 69 6e 2e 61 72 p=secure login.ar 01b0 75 62 61 6e 65 74 77 6f 72 6b 73 2e 63 6f 6d 26 ubanetwo rks.com& 01c0 75 72 6c 3d 68 74 74 70 25 33 41 25 32 46 25 32 01d0 46 35 2e 35 2e 35 2e 35 25 32 46 0d 0a 43 6f 6e 01e0 6e 65 63 74 69 6f 6e 3a 20 63 6c 6f 73 65 0d 0a 01f0 0d 0a	0140	61 72 7a 5f 61 72	75 62 61 26 69 70 3	d 31 30 2	2e arz_arub a&ip=10.							
0160 30 30 34 25 33 41 62 64 25 33 41 38 38 25 33 41 0170 63 33 25 33 41 38 38 25 33 41 31 34 26 76 63 6e 0180 61 6d 65 3d 69 6e 73 74 61 6e 74 2d 43 33 25 33 0190 41 38 38 25 33 41 31 34 26 73 77 69 74 63 68 69 01a0 70 3d 73 65 63 75 72 65 6c 6f 67 69 6e 2e 61 72 p=secure login.ar 01b0 75 62 61 6e 65 74 77 6f 72 6b 73 2e 63 6f 6d 26 01c0 75 72 6c 3d 68 74 74 70 25 33 41 25 32 46 25 32 01d0 46 35 2e 35 2e 35 2e 35 25 32 46 0d 0a 43 6f 6e 01e0 6e 65 63 74 69 6f 6e 3a 20 63 6c 6f 73 65 0d 0a 01f0 0d 0a T	0150	36 32 2e 31 34 38	2e 37 31 26 61 70 6	e 61 6d 6	65 62.148.7 1&apname							
0180 61 66 53 69 62 74 2d 43 33 25 33 ame=inst ant-c3%3 0190 41 38 38 25 33 41 31 34 26 73 77 69 74 63 68 69 A88%3A14 &switchi 0100 75 72 65 66 67 79 69 62 26 17 p=secure login.ar 0100 75 72 62 34 73 27 23 41 25 32 46 26 61 72 p=secure login.ar 010a 010 75 72 67 74 70 25 33 41 25 32 46 25 32 ulanetwor ks.com& ulanetwor ks.com ulanetwor ks.com 010 016 66 65 67 74 70 25 33 41 25 32 46 25 32 ulanetwor ks.com 010 014 36 66 66 66 66 66 66 <	0170	30 30 34 25 33 41 63 33 25 33 41 38	02 04 20 33 41 38 30 38 25 33 41 31 34 20	5 20 33 4 5 76 63 6	41 == 04%3AD0 %3A88%3A 5e c3%3A88% 3A1 <i>48</i> vcn							
0190 41 38 38 25 33 41 31 34 26 73 77 69 74 63 68 69 A88%3A14 &switchi 01a0 70 3d 73 65 63 75 72 65 6c 6f 67 69 6e 2e 61 72 p=secure login.ar 01b0 75 62 61 6e 65 74 77 6f 72 6b 73 2e 63 6f 6d 26 ubanetwo rks.com& 01c0 75 72 6c 3d 68 74 74 70 25 33 41 25 32 46 25 32 url=http %3A%2F%2 01d0 46 35 2e 35 2e 35 2e 35 25 32 46 0d 0a 43 6f 6e F5.5.5.5 %2FCon 01e0 6e 65 63 74 69 6f 6e 3a 20 63 6c 6f 73 65 0d 0a critical control	0180	61 6d 65 3d 69 6e	73 74 61 6e 74 2d 4	3 33 25 3	33 ame=inst ant-C3%3	=						
01a0 70 30 73 65 63 75 72 65 66 67 67 69 66 26 61 72 p=secure login.ar 01b0 75 62 61 66 65 74 77 6f 72 6b 73 2e 63 6f 6d 26 ubanetwo rks. com& 01c0 75 72 6c 3d 68 74 74 70 25 33 41 25 32 46 25 32 01d0 46 35 2e 35 2e 35 2e 35 25 32 46 0d 0a 43 6f 6e 01e0 6e 65 63 74 69 6f 6e 3a 20 63 6c 6f 73 65 0d 0a 01f0 0d 0a 	0190	41 38 38 25 33 41	31 34 26 73 77 69 74	4 63 68 6	59 A88%3A14 &switchi							
01c0 75 72 6c 3d 68 74 74 70 25 33 41 25 32 46 25 32 01d0 46 35 2e 35 2e 35 2e 35 25 32 46 0d 0a 43 6f 6e 01e0 6e 65 63 74 69 6f 6e 3a 20 63 6c 6f 73 65 0d 0a o1f0 0d 0a	01b0	70 30 73 65 63 75 75 62 61 6e 65 74	72 65 6C 6T 67 69 6	e 2e 61 / 3 6f 6d 2	26 ubapetwo_rks.com&							
01d0 <u>46 35 2e 35 </u>	01c0	75 72 6c 3d 6 <u>8</u> 74	74 70 25 33 41 25 3	2 46 25 3	32 url=http %3A%2F%2							
01f0 0d 0a	01d0	46 35 2e 35 2e 35	2e 35 25 32 46 0d 0	43 6f 6	5e F5. 5. 5. 5 %2F Con							
	01f0	0e 05 03 74 09 6T Od 0a	0e 5a 20 03 0C 6T 7	5 65 00 0	Ja nection: close	-						

Gracias a estos argumentos, ISE puede recrear la ID de sesión de Cisco, averiguar la sesión correspondiente en ISE y continuar con el flujo de BYOD (o cualquier otro flujo configurado).

Para los dispositivos Cisco, audit_session_id se utilizaría normalmente, pero no es compatible con otros proveedores.

Para confirmar que a partir de las depuraciones de ISE, es posible ver la generación del valor audit-session-id (que nunca se envía a través de la red):

<#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

Y luego, la correlación de eso después del registro del dispositivo en BYOD Página 2:

<#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 INF0
```

```
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=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06fo0Z7G1HXj1M,
cisco-av-pair=
```

```
audit-session-id=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7G1HXj1M
```

En las solicitudes posteriores, el cliente se redirige a la página 3 de BYOD, donde se descarga y ejecuta la NSA.





La NSA tiene la misma tarea que el navegador web. En primer lugar, debe detectar cuál es la dirección IP de ISE. Esto se logra a través de la redirección HTTP.

Debido a que este usuario de tiempo no tiene la posibilidad de escribir la dirección IP (como en el navegador web), ese tráfico se genera automáticamente.

Se utiliza la puerta de enlace predeterminada (también se puede utilizar enroll.cisco.com), como se muestra en la imagen.

*Wireless Network Connection [Wireshark 1.10.3 (SVN Rev 53022 from /trunk-1.10)]
<u>File Edit View Go Capture Analyze Statistics Telephony Tools Internals H</u> elp
◉ ◉ ∡ ■ ∅ ⊨ ҧ ೫ ⊉ < ⇔ ⇔ ♀ ∓ ⊻ ⊟ ⊟ € < ∞ ⊡ ₩ ⊠ 畅 % ⊠
Filter: http Expression Clear Apply Save
No. Source Destination Protocol Length Info
182 10.62.148.71 10.62.148.100 HTTP 223 GET /auth/discovery HTTP/1.1
184 10.62.148.100 10.62.148.71 HTTP 520 HTTP/1.1 302
⊕ Frame 182: 223 bytes on wire (1784 bits), 223 bytes captured (1784 bits) on interface 0
Ethernet II, Src: Tp-LinkT_14:6e:31 (c0:4a:00:14:6e:31), Dst: Cisco_f2:b1:42 (c4:0a:cb:f2:b1:42)
⊞ Internet Protocol Version 4, Src: 10.62.148.71 (10.62.148.71), Dst: 10.62.148.100 (10.62.148.100)
⊞ Transmission Control Protocol, Src Port: 55937 (55937), Dst Port: http (80), Seq: 1, Ack: 1, Len: 169
Hypertext Transfer Protocol
GET /auth/discovery HTTP/1.1\r\n
User-Agent: Mozilla/4.0 (Windows NT 6.1; compatible; Cisco NAC Web Agent v.)\r\n
Accept: */*\r\n
Host: 10.62.148.100\r\n
Cache-Control: no-cache\r\n
\r\n
[Full request URI: http://10.62.148.100/auth/discovery]
[HTTP request 1/1]
[Response in frame: 184]

La respuesta es exactamente la misma que para el navegador web.

De esta manera, la NSA puede conectarse a ISE, obtener un perfil xml con la configuración, generar una solicitud SCEP, enviarla a ISE, obtener un certificado firmado (firmado por una CA interna de ISE), configurar un perfil inalámbrico y, finalmente, conectarse al SSID configurado.

Recopile registros del cliente (en Windows están en %temp%/spwProfile.log). Algunos resultados se omiten para mayor claridad:

<#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:CO-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: CO-4A-00-14-6E-31
```

redirect attempt to discover ISE with the response url

DiscoverISE - start Discovered ISE - : [mgarcarz-ise20.example.com, sessionId: 0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06fo0Z7 DiscoverISE - end

Successfully Discovered ISE: mgarcarz-ise20.example.com, session id: 0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ

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:M2

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
```

Estos registros son exactamente los mismos que para el proceso BYOD con dispositivos Cisco.

Nota: Radius CoA no es necesario aquí. Es la aplicación (NSA) la que fuerza la reconexión a un SSID recién configurado.

En ese momento, el usuario puede ver que el sistema intenta asociarse a un SSID final. Si tiene más de un certificado de usuario, debe seleccionar el correcto (como se muestra en la imagen).

Select Certificate		×
User name on certificate:		
cisco@example.com		-
cisco@example.com administrator@example.com	າ	
issuer:	LAB CA	_
Expiration date:	7/17/2016 12:29:41 PM	
	OK Cancel View Certifi	cate

Después de una conexión exitosa, los informes de la NSA son como se muestra en la imagen.



Esto se puede confirmar en ISE: el segundo registro accede a la autenticación EAP-TLS, que cumple todas las condiciones de Basic_Authenticated_Access (EAP-TLS, Employee y BYOD Registered true).

cisco Identity	Services Engine	Home	▼ Operations	Policy	Guest Access	Administration	Work Centers					
RADIUS Livelog	TACACS Livelog	Reports	Troubleshoot	Adaptive Net	twork Control							
	Misconfigured Supplicants ⁽²⁾ Misconfigured Network Devices ⁽²⁾ RADIUS Drops ⁽²⁾ 1 0 12									Client Stopped Respond O		
Show Live S	📓 Show Live Sessions 🙀 Add or Remove Columns 🔻 🏀 Refresh 😰 Reset Repeat Counts Refresh 💽											
Time	▼ Status De	t R. [Identity ()	Endpoint ID 🛞	Authenticati	ion Policy 🛞	Authorization Policy ①	Authorization Profiles	Network Device	Event (
2015-10-29 22	:23:37 🕦	<u>0</u> 0 0	isco (0:4A:00:14:6E:	31 Default >> 0	Dot1X >> EAP-TLS	Default >> Basic_Authenticated	PermitAccess		Session State is Started		
2015-10-29 22	:23:37 🔽	à c	isco (0:4A:00:14:6E:	31 Default >> [Dot1X >> EAP-TLS	Default >> Basic_Authenticated	. PermitAccess	aruba	Authentication succeeded		
2015-10-29 22	:19:09 🔽	0 0	isco (0:4A:00:14:6E:	31 Default >> [Dot1X >> Default	Default >> ArubaRedirect	Aruba-redirect-BYOD	aruba	Authentication succeeded		

Además, la vista de identidad del terminal puede confirmar que el terminal tiene el indicador BYOD Registered establecido en true, como se muestra en la imagen.

EndPoints	End	lpoint List													
Users			Endpoin	ts by Profile				Endpo	Endpoints by Policy Service Node						
Latest Manual Network Scan Results				W	ndows7-Workstati.	:: 100%				mgan	carz-ise20.exa	: 100%			
	0												. _		-
	0	Refresh 🕈 Ad	id ∎ Trash ♥ 🖸 Eo	Sit MDM Action	ns 👻 Refresh M	IDM Partner Endp	pint Import	Export						,	Filter V Q V
		Endpoint Profile	MAC Address	Vendor(OUI)	Logical Profiles	Hostname	MDM Server	Device Identifier	IP Address	Static Assignment	Static Group Assignment	Portal User	Device Registration	BYOD Registration	Profile Server
	×	Endpoint Prof	MAC Address			Hostname	MDM Sen	Device Ide	IP Address	Static Ass	Static Gro	Portal User		BYOD Re	Profile Server
		Windows7- Workstation	C0:4A:00:14:6E:31	TP-LINK TE		mgarcarz-pc			10.62.148.71	false	true	cisco	Registered	Yes	mgarcarz-ise

En el PC con Windows, el nuevo perfil inalámbrico se ha creado automáticamente como se prefiere (y se ha configurado para EAP-TLS) y como se muestra.

Manage wireless networks that use (Wireless Network Connection)

Windows tries to connect to these networks in the order listed below.

Add Remove Move down	Adapter propert	mgarcarz_aruba_tls Wir	eless Network Properties	×
Networks you can view, modify, an mgarcarz_aruba_tis	d reorder (4) — Security: WPA	Connection Security		
		Security type:	WPA2-Enterprise	
mgarcarz_aruba	Security: WPA	Encryption type:	AES 👻	
pgruszcz_WLANI	Security: WPA	Choose a network au	thentication method:	
mgarcarz_byod	Security: WPA	Microsoft: Smart Car Remember my cre time I'm logged or	d or other certificat Settings dentials for this connection each	
		Advanced settings	•	

En ese momento, Aruba confirma que el usuario está conectado al SSID final.



La función que se crea automáticamente y se denomina igual que Red proporciona acceso completo a la red.

Security					
Authentication Servers Users for	Internal Server	Roles	Blacklisting	Firewall Settings	Inbound Firewall
Roles	Access Rules	for mga	rcarz_aruba_t	tis	
default_wired_port_profile wired-instant ArubaAAA wcecot_BYOD_aruba mgarcarz_aruba	Allow any t	o all des	tinations		
mgarcarz_aruba_tls					
New Delete	New Edit	Delete	•		

Otros flujos y soporte de CoA

CWA con CoA

Aunque en el flujo de BYOD no hay mensajes de CoA, el flujo de CWA con el portal de invitados registrados automáticamente se muestra aquí:

Las reglas de autorización configuradas son las que se muestran en la imagen.

~	Guest_Authenticate_internet	if	GuestEndpoints AND Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba_guest	then	PermitAccess
~	Guest_Authenticate_Aruba	if	Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba_guest	then	Aruba-redirect-CWA

El usuario se conecta al SSID con autenticación MAB y una vez que intenta conectarse a alguna página web, se redirige al portal de invitados registrados automáticamente, donde el invitado puede crear una nueva cuenta o utilizar la actual.

CISCO Sponsored Guest Portal

Sign On

Welcome to the Guest Portal. Sign on with the username and password provided to you.

Username:		
cisco		
Password:		
••••••		
	Sign On	
	Don't have an account?	

Una vez que el invitado se ha conectado correctamente, se envía un mensaje CoA desde ISE al dispositivo de red para cambiar el estado de autorización.

cisco	Sponsored Guest Portal		
Welcon	ne Message		
Click Con	ntinue to connect to the network.		
You're ver	ry close to gaining network access.		
		Continue	

Se puede verificar en Operaciones > Autenticaciones y como se muestra en la imagen.

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:00:15:7	6 C0:4A:00:15:76:34	Default >> MAB >> .	. Default >> Guest_Authenticate_Aruba	Authentication succeeded	Aruba-redirect-CWA

Mensaje CoA en depuraciones de ISE:

<#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
```

```
۰,
```

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=0a3011ebisZXyp0DwqjB6j64GeFiF7RwvyocneEia17ckjtU1HI.,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

y Disconnect-ACK que proviene de Aruba:

<#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

Las capturas de paquetes con CoA, solicitud de desconexión (40) y desconexión-ACK (41) son como se muestra.

⊗ 🗇 💷 aruba_Endpoint_CWA.pcap [Wireshark 1.10.6 (v1.10.6 from master-1.10)]													
•) 🔟 📕 🙍	🗎 🗎 🗶 🄇	, Q	< > <	• •	<u>↓</u> [1		1	* 0	
Filter:	udp.port==3799			- Expre	ession	Clear Ap	ply Save						
No.	Time	Source	Destinat	ion	Proto	ocol	Ler	ngth		1	Enfo		
14	4 17:47:49.654868	10.48.17.235	10.62.148	3.118	RADIU	JS				100 D	isconnect	-Request(40	<pre>0) (id=1, l=58)</pre>
14	7 17:47:49.707216	10.62.148.118	10.48.17.	235	RADIU	JS				74 D	isconnect	-ACK(41) (i	id=1, l=32)
<pre>>Ethernet II, Src: Vmware_99:6d:34 (00:50:56:99:6d:34), Dst: Cisco_1c:e8:00 (00:07:4f:1c:e8:00) >Internet Protocol Version 4, Src: 10.48.17.235 (10.48.17.235), Dst: 10.62.148.118 (10.62.148.118) >User Datagram Protocol, Src Port: 16573 (16573), Dst Port: radius-dynauth (3799) vRadius Protocol Code: Disconnect-Request (40)</pre>													
Pack	Packet identifier: 0x1 (1)												
Length: 58 Authenticator: 517f99c301100cb16f157562784666cb [The response to this request is in frame 147] ▼Attribute Value Pairs ►AVP: l=6 t=NAS-IP-Address(4): 10.62.148.118 ►AVP: l=14 t=Calling-Station-Id(31): c04a00157634 ►AVP: l=18 t=Message-Authenticator(80): d00e10060c68b99da3146b8592c873be													

Nota: RFC CoA se ha utilizado para la autenticación relacionada con Device Profile Aruba (parámetros predeterminados). Para la autenticación relacionada con el dispositivo de Cisco, habría sido Cisco CoA type reauthenticate.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Portal cautivo de Aruba con dirección IP en lugar de FQDN

Si Captive Portal en Aruba se configura con la dirección IP en lugar del FQDN de ISE, PSN NSA falla:

<#root>

Warning - [HTTPConnection]

```
Abort the HTTP connection due to invalid certificate
```

CN

El motivo es la validación estricta de certificados cuando se conecta a ISE. Cuando utiliza una dirección IP para conectarse a ISE (como resultado de una URL de redirección con una dirección IP en lugar de FQDN) y se le presenta un certificado de ISE con el nombre del sujeto = la validación de FQDN falla.

Nota: el navegador web continúa con el portal BYOD (con una advertencia que debe aprobar el usuario).

Política de acceso incorrecta del portal cautivo de Aruba

De forma predeterminada, Aruba Access-Policy configurado con Captive Portal permite los puertos TCP 80, 443 y 8080.

La NSA no puede conectarse al puerto tcp 8905 para obtener el perfil xml de ISE. Se informa de este error:

```
<#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=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06fo0Z7G1HXj1M&os=Windows All]
- http Error: [2]
HTTP response code: 0
]
GetProfile - end
Failed to get profile. Error: 2
```

Número de puerto CoA de Aruba

De forma predeterminada, Aruba proporciona el número de puerto para el puerto CoA Air Group CoA 5999. Lamentablemente, Aruba 2004 no respondió a esas solicitudes (como se indica).

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 (0 Step latency=10009 ms)

11213 No response received from Network Access Device after sending a Dynamic Authorization request

La captura de paquetes es como se muestra en la imagen.



► AVP: l=18 t=Message-Authenticator(80): 1959020d15fe2b0584b3a887c1e3c366

La mejor opción para utilizar aquí puede ser el puerto CoA 3977 como se describe en RFC 5176.

Redirección en algunos dispositivos de Aruba

En Aruba 3600 con v6.3 se observa que la redirección funciona ligeramente diferente que en otros controladores. La captura y explicación de paquetes se puede encontrar aquí.

770 09:29:40.5119110 10.75.94.213	173.194.124.52	HTTP	1373 GET / HTTP/1.1
772 09:29:40.5210656 173.194.124.52	10.75.94.213	HTTP	416 HTTP/1.1 200 Ok (text/html)
794 09:29:41.6982570 10.75.94.213	173.194.124.52	HTTP	63 GET /&arubalp=6b0512fc-f699-45c6-b5cb-e62b3260e5 HTTP/1.1
797 09:29:41.7563060 173.194.124.52	10.75.94.213	HTTP	485 HTTP/1.1 302 Temporarily Moved

<#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/</pre>

&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%2Fwatered approximate the state of the state of

Información Relacionada

- Guía del administrador de Cisco Identity Services Engine, versión 2.0
- Perfiles de dispositivos de acceso a la red con Cisco Identity Services Engine
- Soporte Técnico y Documentación Cisco Systems

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).