CWA CPPM

vendredi 2 mai 2014

Lessons learned.

Every endpoint is updated with Roles that are valid during 5 minutes. These roles can be used to make posterior decisions.

On each service we need to:

Match the service, define which roles are to be mapped to the endpoint, enforce (return) auth privileges to the endpoind.

Flow is:

Endpoint associates, tries MAC Auth and generates RADIUS request to CPPM - 1st pass on mac auth service (allow all mac)

On CPPM endpoint is unknown - gets returned an access-acept plus an URL redirect

Person using endpoint goes to web browser and gets redirected to CPPM portal and authenticates This authentication is processed in CPPM via a webauth service that will:

Map a role to the endpoint

Generate a coa for the controller to reauthenticate the user (new mac auth - 2nd pass)
This 2nd pass will then be catched by the same mac auth service, but this time (during 5 minutes after accounting start) the endpoint will have roles in its policy cache. These roles will be matched and the appropriate RADIUS attributes will be returned (specific dacl's for instance)

When user disconnects:

Controller will need to time out the endpoint, then send accounting stop to CPPM. CPPM will keep endpoint policy cache in during 5 minutes and then purge it. Next time user associates ---> start all over again.

IN the case of CWA: --

On the mac auth service we need to be able to distinguish between 1st pass (no roles on endpoint) from 2nd pass (already roles assigned to the endpoint) --- we need obviously to enable "use cached results"

Configuration » Services » Edit - S-MACAuth

Services - S-MACAuth

Summary Service	Authentication	Roles Enforcement	
Status:		Enabled	
Monitor Mode:		Disabled	
More Options:		-	
Service Rule			
Match ALL of the following	conditions:		
Туре	Name	Operator	Value
1. Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15), Wireless- 802.11 (19)
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)
3. Connection Client-Mac-Address		EQUALS	%{Radius:IETF:User- Name}
Authentication:			
Authentication Methods:	[Allow All MAC AUTH]		
Authentication Sources:	[Endpoints Repositor	y]	
Strip Username Rules:	-		
Roles:			
Role Mapping Policy:	-		
Enforcement:			
Use Cached Results:	Enabled		
Enforcement Policy:	EPo-MACEnforcement	t	

for this we use an enforcement policy that contains rules to allow us to distinguish between when we need to send a URL redirect versus approve a MAC address through. We are obviously using the values from previous authentications.

Configuration » Enforcement » Policies » Edit - EPo-MACEnforcement

Enforcement Policies - EPo-MACEnforcement

Summary	Enforcement	Rules			
Enforcement	:				
Name:	E	Po-MACEnfo	cement		
Description:					
Enforcement	Type: R	ADIUS			
Default Profil	e: [[Deny Access	Profile]		
Rules:					
Rules Evaluat	tion Algorithm:				First applicable
Conditio	ns			Actions	
1. (T	(Tips:Role <i>EQUALS</i> R_PREGuest)		st)	[Allow Access	Profile]
2. (T	ips:Role <i>EQUALS</i>	[Other])		[Deny Access	Profile]
3. (A	uthentication:Ma	Auth <i>EQUA</i>	LS UnknownClient)	EPr-URLRedir	-WLCACL

The URL redirect needs to be crafted this way - note the usage of variables in the url redirect value (%{Connection:Client-Mac-Address-Colon}):

Configuration » Enforcement » Profiles » Edit Enforcement Profile - EPr-URLRedir-WLCACL

Enforcement Profiles - EPr-URLRedir-WLCACL

Profile	Attributes	
	EPr-URLRed	ir-WLCACL
	Send URL re	edirect + filter ID to WLC
	RADIUS	
	Accept	
List:	-	
	Profile List:	EPr-URLRed Send URL re RADIUS Accept

Туре	Name	Value
1. Radius:Cisco	Cisco-AVPair	url- = redirect=https://10.1.156.142/guest/ciscoguest.php? &mac=%{Connection:Client-Mac-Address-Colon}
2. Radius:Cisco	Cisco-AVPair	= url-redirect-acl=ACL-WEBAUTH-REDIRECT

On the guest auth service we will have:

Configuration » Services » Edit - S_GuestAuth

Services - S_GuestAuth

Summary Service	Authentication	Roles	Enforcement	
Service:				
Name:	S_GuestAuth			
Description:				
Type:	Web-based Authe	entication		
Status:	Enabled			
Monitor Mode:	Disabled			
More Options:	-			
Service Rule				
Match ANY of the followin	g conditions:			
Туре	Name		Operator	Value
1. Host	CheckType		MATCHES_ANY	Authentication
Authentication:				
Authentication Sources:	[Guest User Repo	sitory]		
Strip Username Rules:	-			
Roles:				
Role Mapping Policy:	RMap_2_PREGUE	ST		
Enforcement:				
Use Cached Results:	Disabled			

So basically we're treating every guest authentication on this service and applying the enforcement

policy that will both set the appropriate role to the endpoint as well as trigger a CoA to generate the 2nd pass mac authentication

This part is still a bit shady.... Who populates the guestUser:Role ID variable as well as the TIPS server role...

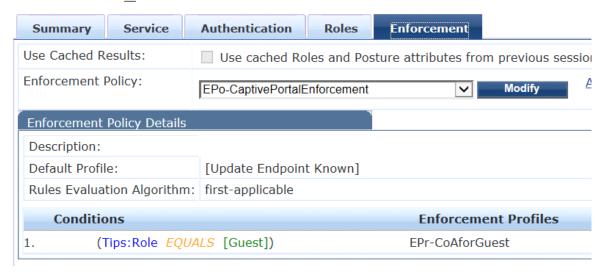
Configuration » Services » Edit - S_GuestAuth

Services - S_GuestAuth



Configuration » Services » Edit - S_GuestAuth

Services - S_GuestAuth



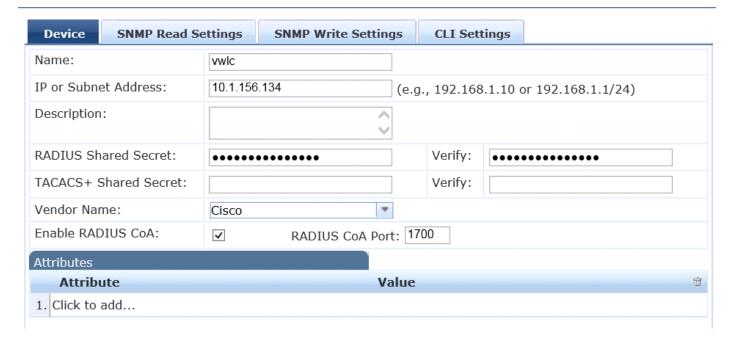
Regarding the way to send the CoA to the WLC. Remember that the web authentication is NOT a radius authentication (so no calling-station-id exists) and in order to trigger a CoA request we need to send the mac-address of the endpoint we want to reauthenticate, so for this we need to tweak the RADIUS CoA Cisco default template:

Configuration » Enforcement » Profiles » Edit Enforcement Profile - EPr-CoAforGuest

Enforcement Profiles - EPr-CoAforGuest



Beware of setting the right CoA port on the WLC NAD - when using the port 3799 towards WLC we were having a lot of "Received CoA request with invalid attributes" -- as soon as we switched the NAD CoA port to 1700 - everything was magically ok.



Regarding the web page configuration we need to go to configuration -> weblogins and make sure we're using Cisco Systems vendor settings as well as server-initiated - CoA sent to Controller

* Vendor Settings:	Cisco Systems Select a predefined group of settings suitable for standard network configurations.
Login Method:	Server-initiated — Change of authorization (RFC 3576) sent to controller Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.
Login Form Options for specifying th	ne behaviour and content of the login form.
Authentication:	Credentials – Require a username and password Select the authentication requirement. Access Code requires a single code (username) to be entered. Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required. Access Code and Anonymous require the account to have the Username Authentication field set.
Prevent CNA:	Enable bypassing the Apple Captive Network Assistant The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented.
Custom Form:	Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
Custom Labels:	Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login form.
Username Suffix:	The suffix is automatically appended to the username before submitting the login form to the NAS.
* Pre-Auth Check:	None — no extra checks will be made Select how the username and password should be checked before proceeding to the NAS authentication.