

DACL'S AND VLAN ASSIGNMENT

CONTENTS

DACL's and Vlan assignment	1
Requirements.....	1
Overview.....	1
Topology.....	2
Adding a Device To ISE.....	3
Adding The User Role VSA to the HP Dictionary.....	6
Using DAACL'S and Vlan Assignment VSA's.....	9
Verification.....	12

REQUIREMENTS

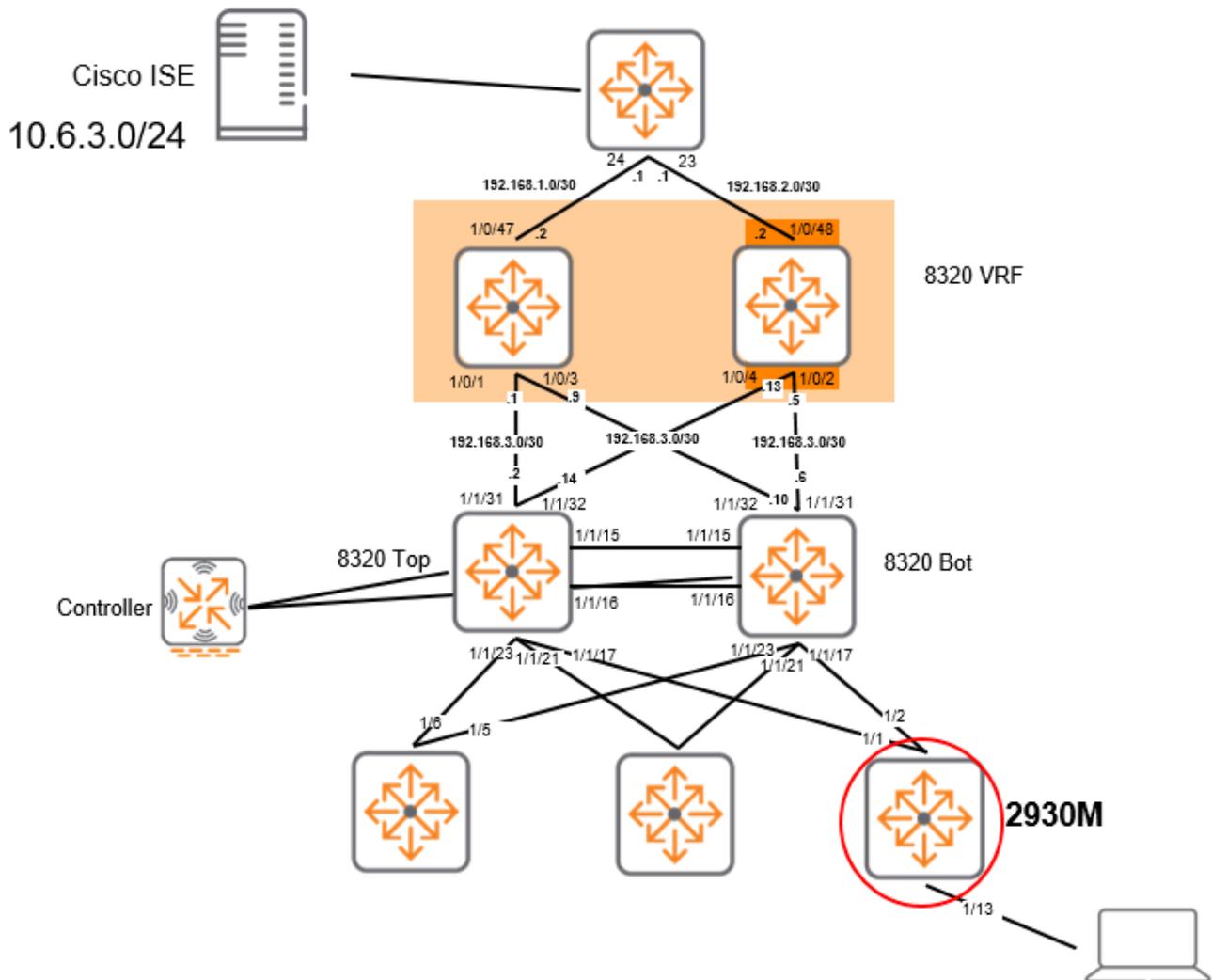
- Aruba Switch (2930M/F, 3810M, 5400)
- Cisco ISE (2.3 And Above)

OVERVIEW

This document will cover downloadable ACL's (DAACL) and VLAN assignment using Cisco ISE and ArubaOS-Switch.

For this scenario, we will be creating a Mac Authentication Fallback policy within Cisco ISE to allow guest devices some network connectivity. To do this, we will also need to assign a VLAN and a DAACL. This allows these guest devices to access the internet and get a DHCP address. We also need to allow the device to connect to one internal address. The 10.6.3.0/24 subnet is an internal subnet with different services sitting within the subnet such as ISE,DHCP,DNS, etc... We are going to allow the client device to access the 10.6.3.12 address on that subnet, which is a web service, for this deployment. To verify connectivity, we will just ping the address, but we will be allowing IP connectivity so web browsing will work as well.

TOPOLOGY



ADDING A DEVICE TO ISE

Description

This section will go over adding a device into Cisco ISE.

Navigate to Administration > Network Devices. Click Add.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Administration' menu is expanded to show 'Network Resources', 'Device Portal Management', 'pxGrid Services', 'Feed Service', and 'Threat Centric NAC'. The 'Network Resources' menu is further expanded to show 'Network Devices', 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', 'RADIUS Server Sequences', 'NAC Managers', 'External MDM', and 'Location Services'. The 'Network Devices' page is active, showing a table with one device entry: '2930M-ISE' with IP/Mask '10.128.1.10/32', Profile Name 'HPWired_copy', Location 'All Locations', and Type 'All Device Types'. The table has columns for Name, IP/Mask, Profile Name, Location, and Type. Above the table are action buttons: Edit, Add, Duplicate, Import, Export, Generate PAC, and Delete.

Name	IP/Mask	Profile Name	Location	Type
<input type="checkbox"/> 2930M-ISE	10.128.1.10/32	HPWired_copy	All Locations	All Device Types

Enter the IP address, RADIUS shared secret, and model of the switch and select the proper switch profile

Note: In this example a copy of the HPWired Profile “HPWired_Copy” is being used, there is no issues using the default HPWired Profile this will work for DACL’s and Vlan Assignment as well.

[Network Devices List > 2930M-ISE](#)

Network Devices

* Name

Description

IP Address /

i IPv6 is supported only for TACACS. At least one IPv4 must be defined when RADIUS is selected

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

CoA Port

RADIUS DTLS Settings (i)

DTLS Required (i)

Shared Secret (i)

CoA Port

Issuer CA of ISE Certificates for CoA (i)

DNS Name

General Settings

Enable KeyWrap (i)

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

Switch Configuration

Pointing the switch to ISE Server

```
radius-server host <Radius-IP> dyn-authorization  
radius-server host <Radius-IP> time-window 0  
radius-server key < KEY-STR>
```

Configuring AAA on the switch for Mac Authentication as a fall back and Configuration for enabling AAA.

```
aaa authentication port-access eap-radius  
aaa port-access authenticator <Ports>  
aaa port-access authenticator <Ports> client-limit <Limit>  
aaa port-access mac-based <Ports> addr-limit <Limit>  
aaa port-access mac-based <Ports>  
aaa port-access <Ports> auth-order authenticator mac-based  
aaa port-access <Ports> auth-priority authenticator mac-based  
aaa port-access authenticator active
```

ADDING THE USER ROLE VSA TO THE HP DICTIONARY

Description

This section will guide you through how to add the HP NAS filter rule to ISE. If it is not already there. To add the VSA, navigate to Policy > Policy Elements then click the "Radius" folder and navigate to the "HP" dictionary within the Radius Vendors Folder.

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes "Home", "Context Visibility", "Operations", "Policy", "Administration", and "Work Centers". The "Policy" menu is expanded, showing "Policy Sets", "Profiling", "Posture", "Client Provisioning", and "Policy Elements". The "Policy Elements" menu is further expanded to show "Dictionaries", "Conditions", and "Results".

The left sidebar shows a tree view of "Dictionaries" with the following structure:

- Network Condition
- NMAP
- NMAPEExtension
- Normalised Radius
- PassiveID
- Posture
- PROFILER
- Radius
 - IETF
 - RADIUS Vendors
 - Airespace
 - Alcatel-Lucent
 - Aruba
 - Aruba_Wired
 - Brocade
 - Cisco
 - Cisco-BBSM
 - Cisco-VPN3000
 - H3C
 - HP
 - Juniper
 - Microsoft

The main content area shows the configuration for the "HP" dictionary. The breadcrumb path is "Dictionaries > ... > RADIUS Vendors > HP". The configuration fields are:

- * Dictionary Name: HP
- Description: Dictionary for Vendor HP
- * Vendor ID: 11
- Vendor Attribute Type Field Length: 1
- Vendor Attribute Size Field Length: 1

At the bottom of the configuration area, there are "Save" and "Reset" buttons.

1. Click Dictionary Attributes then click add

The screenshot shows the Aruba configuration interface. On the left is a navigation tree under 'Dictionaries' with 'RADIUS Vendors' expanded to 'HP'. The main area shows the 'Dictionary Attributes' table for the HP vendor.

Dictionary Attributes

<input type="checkbox"/>	Name	Number	Type	Direction	Description	Predefined
<input type="checkbox"/>	HP-User-Role	25	STRING	BOTH		NO
<input type="checkbox"/>	HP-CPPM-Role	27	STRING	BOTH		NO
<input type="checkbox"/>	HP-CPPM-Secondary...	28	STRING	BOTH		NO
<input type="checkbox"/>	HP-Captive-Portal-URL	24	STRING	BOTH		NO
<input type="checkbox"/>	HP-Bandwidth-Max-Egr...	48	UINT32	BOTH	Attribute HP-Bandwidth-Max-Egr...	NO
<input type="checkbox"/>	HP-Bandwidth-Max-Ingr...	46	UINT32	BOTH	Attribute HP-Bandwidth-Max-Ingr...	NO
<input type="checkbox"/>	HP-Capability-Advert	255	OCTET_STRING	BOTH	Attribute HP-Capability-Advert	NO
<input type="checkbox"/>	HP-Command-Exception	3	UINT32	BOTH	Attribute HP-Command-Exception	NO
<input type="checkbox"/>	HP-Command-String	2	STRING	BOTH	Attribute HP-Command-String	NO
<input type="checkbox"/>	HP-Cos	40	STRING	BOTH	Attribute HP-Cos	NO
<input type="checkbox"/>	HP-Egress-VLAN-Name	65	STRING	BOTH	Attribute HP-Egress-VLAN-Name	NO
<input type="checkbox"/>	HP-Egress-VLANID	64	UINT32	BOTH	Attribute HP-Egress-VLANID	NO
<input type="checkbox"/>	HP-Management-Proto...	26	UINT32	BOTH	Attribute HP-Management-Protocol	NO
<input type="checkbox"/>	HP-Nas-Rules-IPv6	63	UINT32	BOTH	Attribute HP-Nas-Rules-IPv6	NO
<input type="checkbox"/>	HP-Port-Auth-Mode-Dot...	13	UINT32	BOTH	Attribute HP-Port-Auth-Mode-Dot1x	NO
<input type="checkbox"/>	HP-Port-Client-Limit-Do...	10	UINT32	BOTH	Attribute HP-Port-Client-Limit-Dot...	NO
<input type="checkbox"/>	HP-Port-Client-Limit-MA	11	UINT32	BOTH	Attribute HP-Port-Client-Limit-MA	NO
<input type="checkbox"/>	HP-Port-Client-Limit-WA	12	UINT32	BOTH	Attribute HP-Port-Client-Limit-WA	NO
<input type="checkbox"/>	HP-Privilege-Level	1	UINT32	BOTH	Attribute HP-Privilege-Level	NO

2. After clicking the “add dictionary attribute”, enter the information below then click Submit.
Attribute name: “HP-Nas-Filter-Rule”
Data type: “String”
Direction: “Both”
ID: “61”
Be sure to have the “Allow Multiple Instances of this in a Profile” Box checked.

Dictionaries > ... > HP > HP-Nas-Filter-Rule

* Attribute Name: HP-Nas-Filter-Rule

Description: Attribute HP-Nas-Filter-Rule

* Data Type: STRING Enable MAC option

* Direction: BOTH

* ID: 61 (0-255)

Allow Tagging

Allow multiple instances of this attribute in a profile

Save Reset

USING DACL'S AND VLAN ASSIGNMENT VSA'S

Description

This section will go over how to use the VSA in a Policy Set in ISE, however this will not cover how to create a policy set in ISE.

1. Now that the NAS Filter VSA is defined in ISE, it can now be used. Navigate to Policy > Policy Sets and edit a policy for your environment. Click the Arrow ">" to go into the policy set.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
On	Wired Authentication		Wired_802.1X OR Wired_MAB	Default Network Access	1	Settings	View
On	Default	Default policy set		Default Network Access	0	Settings	View

2. Under the "Policy Set", in this example, there is a "MAB Fall Through" configured. This allows devices that are not in the ISE Authentication databases sources to have some level of network connectivity. This is done by allowing devices that have failed to authenticate against any of the data bases to continue to an authorization policy

Status	Rule Name	Conditions	Use	Hits	Actions
On	Dot1x Fall Through	Wired_802.1X	Internal Users	0	Settings
On	Mab Fall through	Wired_MAB	Guest Portal Sequence Options If Auth fail: CONTINUE If User not found: CONTINUE If Process fail: CONTINUE	1	Settings
On	Default		All_User_ID_Stores	0	Settings

- Next, there needs to be an “Authorization Rule” configured that matches based on MAB. We will specify a profile for the Authorization rule, to do this ,click the “+” button to create a new authorization profile.

The screenshot displays the Aruba Identity Services Engine (ISE) configuration page for an Authorization Policy. The interface includes a navigation menu at the top with options like 'Policy Sets', 'Profiling', 'Posture', 'Client Provisioning', and 'Policy Elements'. A search bar is present at the top left of the main content area.

The main configuration area is divided into two sections:

- Default Policy:** Shows a 'Default' rule with a status of 'On'. It includes configuration options for 'If User not found' (set to CONTINUE), 'If Process fail' (set to CONTINUE), and 'All_User_ID_Stores' (set to All_User_ID_Stores). The 'Hits' column shows 0.
- Authorization Policy - Local Exceptions (5):** A table listing five local exception rules. The table has columns for Status, Rule Name, Conditions, Profiles, Security Groups, Hits, and Actions.

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
On	Guest Registration	Self Register Guest	x Guest_Vlan_100	Select from list	0	Settings
On	Local Exceptions Rule 1	Sponsor Guest Identity Group	x Guest_Vlan_100	Select from list	0	Settings
On	Local Role	InternalUser Name EQUALS user01	x Web_Auth	Select from list	0	Settings
On	Local Exceptions Rule 2	Wired_MAB	Select from list	Select from list	1	Settings

In the 'Local Exceptions' table, the '+' button next to the 'Profiles' column for the 'Local Exceptions Rule 2' row is circled in red, indicating the action to be taken to create a new authorization profile.

4. A pop up should appear and here the authorization rule can be configured. Below is the configuration of the Authorization profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Common Tasks

VLAN Tag ID **1** ID/Name

Web Redirection (CWA, MDM, NSP, CPP)

Advanced Attributes Settings

HP:HP-Nas-Filter-Rule	=	permit in udp from any to any 67,	
HP:HP-Nas-Filter-Rule	=	permit in ip from any to 10.6.3...	
HP:HP-Nas-Filter-Rule	=	deny in ip from any to 192.168...	
HP:HP-Nas-Filter-Rule	=	deny in ip from any to 10.0.0.0/8	
HP:HP-Nas-Filter-Rule	=	deny in ip from any to 172.16.0...	
HP:HP-Nas-Filter-Rule	=	permit in ip from any to any	

Attributes Details

Access Type = ACCESS_ACCEPT
 Tunnel-Private-Group-ID = 1:505
 Tunnel-Type = 1:13
 Tunnel-Medium-Type = 1:6
 HP-Nas-Filter-Rule = permit in udp from any to any 67,53
 HP-Nas-Filter-Rule = permit in ip from any to 10.6.3.12/32
 HP-Nas-Filter-Rule = deny in ip from any to 192.168.0.0/24
 HP-Nas-Filter-Rule = deny in ip from any to 10.0.0.0/8
 HP-Nas-Filter-Rule = deny in ip from any to 172.16.0.0/12
 HP-Nas-Filter-Rule = permit in ip from any to any

- Once the profile is configured, it can be selected in the “Authorization Rule” as a profile. After this is complete, the policy configuration is ready to test

▼ Authorization Policy - Local Exceptions (4)

+	Status	Rule Name	Conditions	Results			Hits	Actions	
				Profiles	Security Groups				
	✔	Guest Registration	Self Register Guest	x Guest Vlan 100	+	Select from list	+	0	⚙
	✔	Local Exceptions Rule 1	Sponsor Guest Identity Group	x Guest Vlan 100	+	Select from list	+	0	⚙
	👁	Local Role	InternalUser Name EQUALS user01	x Web_Auth	+	Select from list	+	0	⚙
	✔	Local Exceptions Rule 2	Wired_MAB	x Unknown_Devices	+	Select from list	+	21	⚙

VERIFICATION

- Using the “Show Port-Access Clients Detail” command the switch will display the details of a session, it will also display the DACL that was configured in ISE.

🖥 172.16.8.5 - PuTTYNG

```

URL      :

Client Base Details :
Port      : 1/13           Authentication Type : mac-based
Client Status : authenticated   Session Time      : 322 seconds
Client Name  : 00-50-B6-79-BD-AC Session Timeout   : 0 seconds
MAC Address  : 0050b6-79bdac
IP          : n/a

Access Policy Details :
COS Map     : Not Defined      In Limit Kbps     : Not Set
Untagged VLAN : 505           Out Limit Kbps    : Not Set
Tagged VLANs : No Tagged VLANs
Port Mode   : 100FDx
RADIUS ACL List :
  permit in udp from any to any 67,53
  permit in ip from any to 10.6.3.12/32
  deny in ip from any to 192.168.0.0/24
  deny in ip from any to 10.0.0.0/8
  deny in ip from any to 172.16.0.0/12
  permit in ip from any to any
Auth Order  : 8021x, Mac-Auth
Auth Priority : 8021x, Mac-Auth
LMA Fallback : Disabled
  
```

- The Client will not be able to ping the devices we would like as well.

```

CA: Command Prompt

Connection-specific DNS Suffix . : compserver.lab
Link-local IPv6 Address . . . . . : fe80::11ce:2ae:535c:688%18
IPv4 Address. . . . . : 10.96.55.12
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.96.55.254

Tunnel adapter isatap.{D71274A1-E2B8-4E69-B602-9AE3DFDB8799}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Tunnel adapter isatap.{62B03CFE-59FA-4DF6-B32A-51CE484D1C41}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Tunnel adapter isatap.compserver.lab:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : compserver.lab

C:\Users\Admin>ping 10.96.55.254

Pinging 10.96.55.254 with 32 bytes of data:
Request timed out.

Ping statistics for 10.96.55.254:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
Control-C
^C
C:\Users\Admin>ping 10.6.3.12

Pinging 10.6.3.12 with 32 bytes of data:
Reply from 10.6.3.12: bytes=32 time<1ms TTL=124
Reply from 10.6.3.12: bytes=32 time<1ms TTL=124

Ping statistics for 10.6.3.12:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

- In ISE Navigate to Operations>Radius> Live logs and you will be able to see the client's authentication. To see more detail, click the magnifying glass on one of the entries

Mar 11, 2019 08:05:15.818 PM			3	00:50:B6:79:BD:AC	00:50:B6:79:BD:AC	Unknown	Wired Authentication >> Mab ...	Wired Authentication >> Local Exc...	Unknown_Devices	
Mar 11, 2019 08:00:27.807 PM				00:50:B6:79:BD:AC	00:50:B6:79:BD:AC	Unknown	Wired Authentication >> Mab ...	Wired Authentication >> Local Exc...	Unknown_Devices	2930M-ISE
Mar 11, 2019 07:55:15.982 PM				user01	A0:CE:C8:02:A9:48	Unknown	Wired Authentication >> Dot1...	Wired Authentication >> Default	DenyAccess	2930M-ISE
Mar 11, 2019 07:45:15.815 PM				user01	A0:CE:C8:02:A9:48	Unknown	Wired Authentication >> Dot1...	Wired Authentication >> Default	DenyAccess	2930M-ISE

After clicking the magnifying glass, the results of the Radius authentication will display.

Name	Endpoint Identity Groups:Unknown
RADIUS Username	00:50:B6:79:BD:AC
NAS-Identifier	2930M-ISE
Device IP Address	10.128.1.10
Called-Station-ID	F4:03:43:DE:47:73

Result	
User-Name	00-50-B6-79-BD-AC
State	ReauthSession:0a06030fujvrkNNpxXHRed7Hj_mJGPZbiamPLdyo0gx8fici15w
Class	CACS:0a06030fujvrkNNpxXHRed7Hj_mJGPZbiamPLdyo0gx8fici15w:ISE-Comp/341383157/30
Tunnel-Type	(tag=1) VLAN
Tunnel-Medium-Type	(tag=1) 802
Tunnel-Private-Group-ID	(tag=1) 505
LicenseTypes	Base license consumed
HP-Nas-Filter-Rule	permit in ip from any to any 53,67
HP-Nas-Filter-Rule	permit in ip from any to 10.6.3.12/32
HP-Nas-Filter-Rule	deny in ip from any to 192.168.0.0/24
HP-Nas-Filter-Rule	deny in ip from any to 10.0.0.0/8
HP-Nas-Filter-Rule	deny in ip from any to 172.16.0.0/12
HP-Nas-Filter-Rule	permit in ip from any to any