Extreme Gen2 ACL Enforcement

In order to push ACL enforcement to a user during authentication the below VSA must be configured and used in Clearpass. You can substitute the example for any one policy name you have created to enforce that specific policy.

> Radius:IETF Filter-Id = Data

Below is an example of several one policy configurations. This example below was configured and pushed from Extreme XMC

> configure policy captive-portal web-redirect 1 server 1 url "https://clearpass.designlogic.net:443/guest/cpguestwrd.php" enable
> configure policy profile 1 name "Data" pvid-status "enable" pvid 1280 egress-vlans 100 untagged-vlans 1280
> configure policy profile 2 name "Internet-Only" pvid-status "enable" pvid 1280 untagged-vlans 1280
> configure policy profile 3 name "Device-Profile" pvid-status "enable" pvid 1280 untagged-vlans 1280
> configure policy profile 4 name "Guest-Portal" pvid-status "enable" pvid 1280 untagged-vlans 1280 web-redirect 1
> configure policy profile 5 name "Deny" pvid-status "enable" pvid 0
> configure policy profile 6 name "Voice" pvid-status "enable" pvid 1280 untagged-vlans 1280
> configure policy profile 7 name "test" pvid-status "enable" pvid 20 untagged-vlans 20
> configure policy rule 2 ipdestsocket 10.0.0.0 mask 8 drop
> configure policy rule 2 ipdestsocket 10.21.0.10 mask 32 forward
> configure policy rule 2 ipdestsocket 172.16.0.0 mask 12 drop
> configure policy rule 2 ipdestsocket 192.168.0.0 mask 16 drop
> configure policy rule 2 udpdestportIP 53 mask 16 forward
> configure policy rule 2 udpdestportIP 67 mask 16 forward
> configure policy rule 2 ether 0x0806 mask 16 forward
> configure policy rule 3 udpdestportIP 53 mask 16 forward
> configure policy rule 3 udpdestportIP 67 mask 16 forward
> configure policy rule 3 ether 0x0806 mask 16 forward
> configure policy rule 4 udpdestportIP 53 mask 16 forward
> configure policy rule 4 udpdestportIP 67 mask 16 forward

```
configure policy rule 4 tcpdestportIP 80 mask 16 forward
configure policy rule 4 tcpdestportIP 443 mask 16 forward
configure policy rule 4 ether 0x0806 mask 16 forward
configure policy maptable response both
configure policy captive-portal listening 80
configure policy captive-portal listening 443
configure policy captive-portal listening 8080
enable policy
```

This is another way to push a similar configuration if you're not using XMC.

```
configure policy rule-model access-list
configure policy captive-portal web-redirect 1 server 1 url
"https://clearpass.designlogic.net:443/guest/cpguestwrd.php" enable
configure policy profile 1 name "Data" pvid-status "enable" pvid 1280 egress-
vlans 100 untagged-vlans 1280
configure policy profile 2 name "Internet-Only" access-list "Internet_Only" pvid-
status "enable" pvid 1280 untagged-vlans 1280
configure policy profile 3 name "Device-Profile" access-list "Device_Profile" pvid-
status "enable" pvid 1280 untagged-vlans 1280
configure policy profile 4 name "Guest-Portal" access-list "Guest_Portal" pvid-
status "enable" pvid 1280 untagged-vlans 1280 web-redirect 1
configure policy profile 5 name "Deny" pvid-status "enable" pvid 0
configure policy profile 6 name "Voice" pvid-status "enable" pvid 1280
untagged-vlans 1280
create policy access-list Internet_Only.Allow_DNS matches udpdestportIP 53
mask 16 actions forward
create policy access-list Internet_Only.Allow_DHCP matches udpdestportIP 67
mask 16 actions forward
create policy access-list Internet_Only.Deny_Tens matches ipdestsocket 10.0.0.0
mask 8 actions drop
create policy access-list Internet_Only.Deny_One_Sevens matches ipdestsocket
172.16.0.0 mask 12 actions drop
create policy access-list Internet_Only.Deny_One_Nines matches ipdestsocket
192.168.0.0 mask 16 actions drop
create policy access-list Device_Profile.Allow_DNS matches udpdestportIP 53
mask 16 actions forward
create policy access-list Device_Profile.Allow_DHCP matches udpdestportIP 67
mask 16 actions forward
create policy access-list Guest_Portal.Allow_DNS matches udpdestportIP 53
mask 16 actions forward
create policy access-list Guest_Portal.Allow_DHCP matches udpdestportIP 67
mask 16 actions forward
```

```
create policy access-list Guest_Portal.Allow_HTTP matches tcpdestportIP 80 mask 16 actions forward
create policy access-list Guest_Portal.Allow_HTTPS matches tcpdestportIP 443 mask 16 actions forward
create policy access-list Guest_Portal.Allow_ARP matches ether 0x0806 mask 16 actions forward
configure policy maptable response both
configure policy captive-portal listening 80
configure policy captive-portal listening 443
configure policy captive-portal listening 8080
enable policy
```

Revision #2
Created 7 June 2022 16:58:49 by Tyler
Updated 7 June 2022 17:13:21 by Tyler