Aruba Clearpass

Wired Authentication

Extreme Gen1 ACL Enforcement

In order to push ACL enforcement to a user during authentication the below VSA must be configured and used in Clearpass

> Radius:Extreme Extreme-Security-Profile = Internet-Only-5M

Below is an example script that can be used to provide internet only access with a limit of 5mbps bandwidth limit.

```
create upm profile Internet-Only-5M
enable cli scripting
set var namedPortId $TCL(regsub ":" ${EVENT.USER_PORT} "")
set var macv $TCL(string range ${EVENT.USER_MAC} 6 end)
set var namedMACId $TCL(regsub -all ":" ${macv} "")
if (!$match($EVENT.NAME,USER-AUTHENTICATED) then
configure cli mode non-persistent
create meter NLM-P$namedPortId
configure meter NLM-P$namedPortId committed-rate 5 Mbps
configure ports $EVENT.USER_PORT rate-limit egress 5 Mbps max-burst-size 128
Kb
create access-list $(namedMACId)_allow "ethernet-source-address
$(EVENT.USER_MAC); destination-address 0.0.0.0/0" "permit;meter NLM-
P$(namedPortId)"
create access-list $(namedMACId)_10_0 "ethernet-source-address
$(EVENT.USER_MAC); destination-address 10.0.0.0/8" "deny"
create access-list $(namedMACId)_172_16 "ethernet-source-address
$(EVENT.USER_MAC); destination-address 172.16.0.0/12" "deny"
create access-list $(namedMACId)_192_168 "ethernet-source-address
$(EVENT.USER_MAC); destination-address 192.168.0.0/16" "deny"
create access-list $(namedMACId)_dhcp "protocol udp; destination-port 67"
"permit"
create access-list $(namedMACId)_dns "protocol udp; destination-port 53"
"permit"
create access-list $(namedMACId)_ntp "protocol udp; destination-port 123"
"permit"
create access-list $(namedMACId)_deny "ethernet-source-address
```

```
$(EVENT.USER_MAC); destination-address 0.0.0.0/0" "deny"
configure access-list add $(namedMACId)_allow first port $EVENT.USER_PORT
configure access-list add $(namedMACId)_10_0 first port $EVENT.USER_PORT
configure access-list add $(namedMACId)_172_16 first port $EVENT.USER_PORT
configure access-list add $(namedMACId)_192_168 first port $EVENT.USER_PORT
configure access-list add $(namedMACId)_dhcp first port $EVENT.USER_PORT
configure access-list add $(namedMACId)_dns first port $EVENT.USER_PORT
configure access-list add $(namedMACId)_ntp first port $EVENT.USER_PORT
configure access-list add $(namedMACId)_deny last port $EVENT.USER_PORT
endif
if (!$match($EVENT.NAME,USER-UNAUTHENTICATED)) then
configure access-list delete $(namedMACId)_allow ports $EVENT.USER_PORT
configure access-list delete $(namedMACId)_10_0 ports $EVENT.USER_PORT
configure access-list delete $(namedMACId)_172_16 ports $EVENT.USER_PORT
configure access-list delete $(namedMACId)_192_168 ports $EVENT.USER_PORT
configure access-list delete $(namedMACId)_dhcp ports $EVENT.USER_PORT
configure access-list delete $(namedMACId)_dns ports $EVENT.USER_PORT
configure access-list delete $(namedMACId)_ntp ports $EVENT.USER_PORT
configure access-list delete $(namedMACId)_deny ports $EVENT.USER_PORT
delete access-list $(namedMACId)_allow
delete access-list $(namedMACId)_10_0
delete access-list $(namedMACId)_172_16
delete access-list $(namedMACId)_192_168
delete access-list $(namedMACId)_dhcp
delete access-list $(namedMACId)_dns
delete access-list $(namedMACId)_ntp
delete access-list $(namedMACId)_deny
delete meter NLM-P$namedPortId
configure ports $EVENT.USER_PORT rate-limit egress no-limit
endif
.

configure upm event user-authenticate profile "Internet-Only-5M" ports 1:1-24
configure upm event user-unauthenticated profile "Internet-Only-5M" ports 1:1-
24
```

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
```

Wired RADIUS Authentication

Exstreme Gen1 RADIUS Authentication

The example configuration below shows how to configure RADIUS for both Management and Port authentication. The server, client-ip and secrets will be unique to your environment. This example also configures and enables RADIUS accounting.

> configure radius mgmt-access primary server 10.21.0.10 1812 client-ip 172.16.5.20 vr VR-Default
> configure radius mgmt-access primary shared-secret encrypted "#$sLBECeI3y+vi56D+JsXsSaWmuvynCERCHNm1lyy21cwRTssjdoE="
> configure radius mgmt-access secondary server 10.21.0.12 1812 client-ip 172.16.5.20 vr VR-Default
> configure radius mgmt-access secondary shared-secret encrypted "#$aV4JSbB7qYJIrkN+xyFpkm8C3VhEMCvmeXg+CHuFmWCPuo9/BjA="
> configure radius netlogin primary server 10.21.0.10 1812 client-ip 172.16.5.20 vr VR-Default
> configure radius netlogin primary shared-secret encrypted "#$E1KQvrolmf3rZESnOuZCzgHvxuOncnJsRCrlsGkg9URvSuQAOQ8="
> configure radius netlogin secondary server 10.21.0.12 1812 client-ip 172.16.5.20 vr VR-Default
> configure radius netlogin secondary shared-secret encrypted "#$25naJ++VqZmHWFE3p940NH+BMkvA4BL2GYj1HB1WaY1AFrIt4rQ="
> configure radius-accounting netlogin primary server 10.21.0.10 1813 client-ip 172.16.5.20 vr VR-Default
> configure radius-accounting netlogin primary shared-secret encrypted "#$5f6QnmG9LhNB1pb1WQB3T+F8LIIhnl5n83AzKewrEGHPtlQkLTI="
> configure radius-accounting netlogin secondary server 10.21.0.12 1813 client-ip 172.16.5.20 vr VR-Default
> configure radius-accounting netlogin secondary shared-secret encrypted "#$2vpSd5mMYX46JQvXCLYqFjRnfH4AVawx57QYAm+QufLMbiRc/Do="
> enable radius
> enable radius mgmt-access
> enable radius netlogin
> enable radius-accounting netlogin

The example configuration below will enable both dot1x user and MAC authentication on a port by port basis. Note that you must create a dedicated netlogin pre-authentication vlan, in this case it's called net-login.

> create vlan "net-login"
> configure vlan net-login tag 2000

> configure netlogin vlan net-login
> enable netlogin dot1x mac
> configure netlogin mac authentication database-order radius
> enable netlogin ports 1:12-46 dot1x
> enable netlogin ports 1:12-46 mac
> configure netlogin ports 1:12 mode mac-based-vlans
> configure netlogin ports 1:12 restart
> configure netlogin add mac-list ff:ff:ff:ff:ff:ff 48

Exstreme Gen2 RADIUS Authentication

The example configuration below shows how to configure RADIUS for both Management and Port authentication. The server, client-ip and secrets will be unique to your environment. This example also configures and enables RADIUS accounting and dynamic authorization. Note that dynamic authorizaton (CoA) will not work unless One Policy is enabled.

> configure radius mgmt-access primary server 10.21.0.10 1812 client-ip 10.128.0.65 vr VR-Default
> configure radius mgmt-access primary shared-secret encrypted "#$BAlozLg2AgB4+Mj2p7/CduXt1k+zLA=="
> configure radius netlogin primary server 10.21.0.10 1812 client-ip 10.128.0.65 vr VR-Default
> configure radius netlogin primary shared-secret encrypted "#$DZrZ1cXlNut7x4NyiOZBQ9YsmzHsVg=="
> configure radius-accounting netlogin primary server 10.21.0.10 1813 client-ip 10.128.0.65 vr VR-Default
> configure radius-accounting netlogin primary shared-secret encrypted "#$kH9eGGJX164H6H4jeIpO5wtd6dfrfg=="
> configure radius dynamic-authorization 1 server 10.21.0.10 client-ip 10.128.0.65 vr VR-Default shared-secret encrypted "#$n9pZ5gRfh8dafMk7hbWYnXPXbNCRFQ=="
> enable radius mgmt-access
> enable radius netlogin
> enable radius-accounting netlogin
> enable radius dynamic-authorization

The example configuration below will enable both dot1x user and MAC authentication on a port by port basis. Note that you must create a dedicated netlogin pre-authentication vlan, in this case it's called net-login.

> create vlan "Net-Login"
> configure vlan Net-Login tag 4000

> enable netlogin dot1x mac
> configure netlogin mac authentication database-order radius
> enable netlogin ports 1-21 dot1x
> enable netlogin ports 1-21 mac
> configure netlogin add mac-list ff:ff:ff:ff:ff:ff 48

In my testing I needed to configure an authentication delay to give Clearpass enough time to create the guest user in the database. The example command below shows how to configure a delay on a per port basis.

> configure netlogin mac ports 1 timers delay 5