

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 $(namedMACId)_deny
delete meter NLM-P$namePortId
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

```

Revision #1

Created 7 June 2022 14:50:14 by Tyler

Updated 7 June 2022 14:55:22 by Tyler