Februari 2008

EXTREME NETWORKS IP SÄKERHET

i EXOS relaterat SSnFs SKA krav

1 Inledning

I detta dokument beskrivs funktioner i Extreme Networks operativsystem EXOS och hur de kan tillämpas för att uppnå de SKA-krav som SSnF begär.

2 SSnFs SKA-krav

Dessa krav är kopierade direkt från sida 12, avsnitt 7.2.3 i SSnFs dokument Kundanslutning till bredbansnät, rev 3.

- Så kallad DHCP-snooping ska finnas på accessportarna, d v s. en kund ska inte kunna vara DHCP-server åt någon annan kund.
- Det ska inte gå att sätta en fast IP-adress och komma vidare från porten som kunden är ansluten i.
- När kunden fått en eller flera adresser via DHCP ska bara den eller de adresserna kunna skicka trafik ut från den porten.
- Om inte adressen förnyas via DHCP-servern ska den adressen stängas av I switchporten.
- Alla typer av spoofing/poisoning ska förhindras för TCP/IP och ARP-protokollen. Dvs. de av DHCP godkända adresserna är de enda adresserna som skaförekomma som sourceaddress i TCP/IP och ARP paket.
- Alla försök till spoofing/poisoning bör kunna loggas till t.ex syslogserver för att trojaner/virus och hackare ska kunna spåras.
- Spårbarhet ska läggas in i DHCP-förfrågningarna i ”L2-läge”, accessswitchen skall inte vara DHCP-relay.
- Det bör finnas filtreringsmöjligheter mellan kundportar så att t.ex godtyckliga TCP/UDP-portar kan filtreras bort mellan kunder
- Om fasta IP-adresser används ska switchporten bara tillåta den för porten definierade IP-adressen som source-adress i TCP/IP och ARP-paket.
- UPnP ska alltid vara spärrat mellan acessportar.
- IPv6 ICMP6 router advertisment och IPv6 DHCP-servrar ska spärras mellankundportar.

3 EXOS SKA-kravs relaterade funktioner

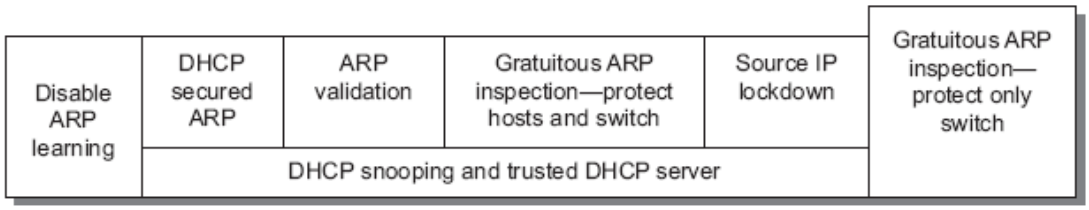
I EXOS finns ett antal IP säkerhetsfunktioner implementerade som erbjuder enkla verktyg till att höja säkerheten i ett nätverk genom att kontrollera vilka resurser som tillåts eller inte tillåts att få åtkomst.

De verktyg som presenteras i följande avsnitt är:

- DHCP Snooping and Trusted DHCP Server
- DHCP Relay Agent Option (Option 82) at Layer 2
- Source IP Lockdown
- DHCP Secured ARP
- ARP Validation
- Gratuitous ARP

Krav på reglering av UPnP och IPv6 trafik hanteras med filtrering i traditionella accesslistor, se exempel i avsnitt 10.

Vissa säkerhetsfunktioner är beroende av varandra. Bild nedan visar beroendet för några funktioner med avseende på SKA-kraven. T.ex. Är ARP validation beroende av att funktionerna DHCP snooping och trusted server är konfigurerade.



4 DHCP Snooping and Trusted DHCP Server

DHCP Snooping höjer säkerheten genom att bygga upp en databas över vilken IP adress som blivit tilldelad till vilken enhet och på vilken port. DHCP databasen innehåller IP adress, MAC adress, VLAN ID och port nummer för accessportar som klienter ansluts till. Många av säkerhetsfunktionerna som beskrivs i detta dokument använder sig av denna databas.

Trusted DHCP server används för att enbart tillåta att enheter blir tilldelade IP adresser från godkända DHCP servrar.

4.1 Konfigurationskommandon

enable ip-security dhcp-snooping {vlan} <vlan_name> ports [all | <ports>] violationaction [drop-packet {[block-mac | block-port] [duration <duration_in_seconds> | permanently] | none]}] {snmp-trap}

configure trusted-servers {vlan} <vlan_name> add server <ip_address> trust-for dhcpserver

configure trusted-ports [<ports>|all] trust-for dhcp-server

show ip-security dhcp-snooping {vlan} <vlan_name>
show ip-security dhcp-snooping entries {vlan} <vlan_name>

5 DHCP Relay Agent Option (Option 82)

DHCP Option 82 är ett attribut som bifogas med DHCP förfrågan för att öka spårbarheten av vilken användare sitter på vilken port. Genom att switchen bifogar information om vilken port, vlan etc som en enhet sitter på så kan man i DHCP servern spåra vilken IP adress som tilldelats vilken enhet och på vilken port/vlan/switch den enheten sitter. DHCP Option 82 kan bifogas både i L3-mode när switchen är konfigurerad som DHCP-relay eller som är fallet för SKA-kraven i L2-mode där DHCP Snooping lägger på informationen.

5.1 Konfigurationskommandon

```
configure ip-security dhcp-snooping information option
configure ip-security dhcp-snooping information policy [drop | keep
|replace]
```

5.2 Exempel på dhcpd.conf konfiguration och loggfil

DHCPD.CONF KONFIGURATION:

```
ddns-update-style ad-hoc;
subnet 10.0.2.0 netmask 255.255.255.0 {
      range 10.0.2.90 10.0.2.99;
      option routers 10.0.2.1;
}

if exists agent.circuit-id {
      log (info, concat ( "Lease for ", binary-to-ascii (10, 8, ".",
leased-address), " is connected to interface ", suffix (option
agent.circuit-id,2), " VLAN ", substring(option agent.circuit-id,0,4),
" on switch ", binary-to-ascii (16, 8, ":", substring (option
agent.remote-id, 0, 6))));

log (info, concat ( "Lease for ", binary-to-ascii (10,8, ".", leased-
address), " raw option 82 info is CID: ", option agent.circuit-id, "
AID: ", binary-to-ascii(16,8,".",option agent.remote-id)));
}
```

LOGGFIL:

```
Feb 22 15:28:03 (none) dhcpd: Lease for 10.0.2.97 is connected to
interface 05 VLAN 4094 on switch 0:4:96:27:7c:1a
```

```
Feb 22 15:28:03 (none) dhcpd: Lease for 10.0.2.97 raw option 82 info is
CID: 4094-1005 AID: 0.4.96.27.7c.1a

Feb 22 15:28:03 (none) dhcpd: DHCPDISCOVER from 00:0f:1f:ba:6e:8d via
eth0

Feb 22 15:28:04 (none) dhcpd: DHCPOFFER on 10.0.2.97 to
00:0f:1f:ba:6e:8d (SE-NBXP-BPERSS) via eth0

Feb 22 15:28:04 (none) dhcpd: Lease for 10.0.2.97 is connected to
interface 05 VLAN 4094 on switch 0:4:96:27:7c:1a

Feb 22 15:28:04 (none) dhcpd: Lease for 10.0.2.97 raw option 82 info is
CID: 4094-1005 AID: 0.4.96.27.7c.1a

Feb 22 15:28:04 (none) dhcpd: DHCPREQUEST for 10.0.2.97 (10.0.2.10)
from 00:0f:1f:ba:6e:8d (SE-NBXP-BPERSS) via eth0

Feb 22 15:28:04 (none) dhcpd: DHCPACK on 10.0.2.97 to 00:0f:1f:ba:6e:8d
(SE-NBXP-BPERSS) via eth0
```

6 Source IP Lockdown

Med Source IP Lockdown förhindrar man att enheter med statisk IP adress kan kommunicera genom porten.

Funktionen Source IP Lockdown använder sig av dynamiska accesslistor för att låsa ner en port till att enbart tillåta kommunikation till och från en enhet som har fått en IP adress tilldelad via en godkänd DHCP server. Denna funktion baseras sig alltså på att Trusted DHCP och DHCP Snooping är aktiverat.

6.1 Konfigurationskommandon

enable ip-security source-ip-lockdown ports [all | <ports>]

show ip-security source-ip-lockdown

7 DHCP Secured ARP

Funktionen DHCP secured ARP populerar ARPtabellen enbart när DHCP tilldelar klienter IP adresser. Genom att inaktivera ARP learning för de portar som klienter asnluter sig till och enbart tillåta manuell eller genom DHCP Secured ARP populering av ARPtabellen går det bla att centralt managera och allokera klienters IP adresser och förhindra störningar i nätet på grund av duplicerade IP adresser.

7.1 Konfigurationskommandon

enable ip-security arp learning learn-from-dhcp {vlan} <vlan_name> ports [all | <ports>]

show ip-security arp learning {vlan} <vlan_name>

8 ARP Validation

Funktionen ARP validation är beroende av funktionen DHCP snooping. Den använder sig av samma DHCP relationsdatabas och validerar inkommande ARPs på en port och kan då förhindra försök till att få resurser i nätverket skapa felaktiga ARP tabeller. Bild nedan beskriver vilka optioner som finns

Validation Option	ARP Request Packet Type	ARP Response Packet Type
DHCP		Source IP is not present in the DHCP snooping database OR is present but Source Hardware Address doesn't match the MAC in the DHCP bindings entry.
IP	Source IP == Mcast OR Target IP == Mcast OR Source IP exists in the DHCP bindings database but Source Hardware Address doesn't match the MAC in the DHCP bindings entry.	Source IP == Mcast OR Target IP == Mcast
Source-MAC	Ethernet source MAC does not match the Source Hardware Address.	Ethernet source MAC does not match the Source Hardware Address.
Destination-MAC		Ethernet destination MAC does not match the Target Hardware Address.

8.1 Konfigurationskommandon

enable ip-security arp validation {destination-mac} {source-mac} {ip} {vlan} <vlan_name> [all | <ports>] violation-action [drop-packet {[block-port] [duration <duration_in_seconds> | permanently]}] {snmp-trap}

show ip-security arp validation {vlan} <vlan_name>

9 Gratuitous ARP protection

Klienter kan genom att skicka gratuitous ARP förfrågningar för en routers IP adress aktivera en så kallad man-in-the-middle . Som resulterar att en annan klient skickar sin trafik tänkt att gå mot routern via attackerande klient. Genom funktionen gratuitous ARP protection skyddar switchen sin egen IP adress mot sådana attacker.

9.1 Konfigurationskommandon

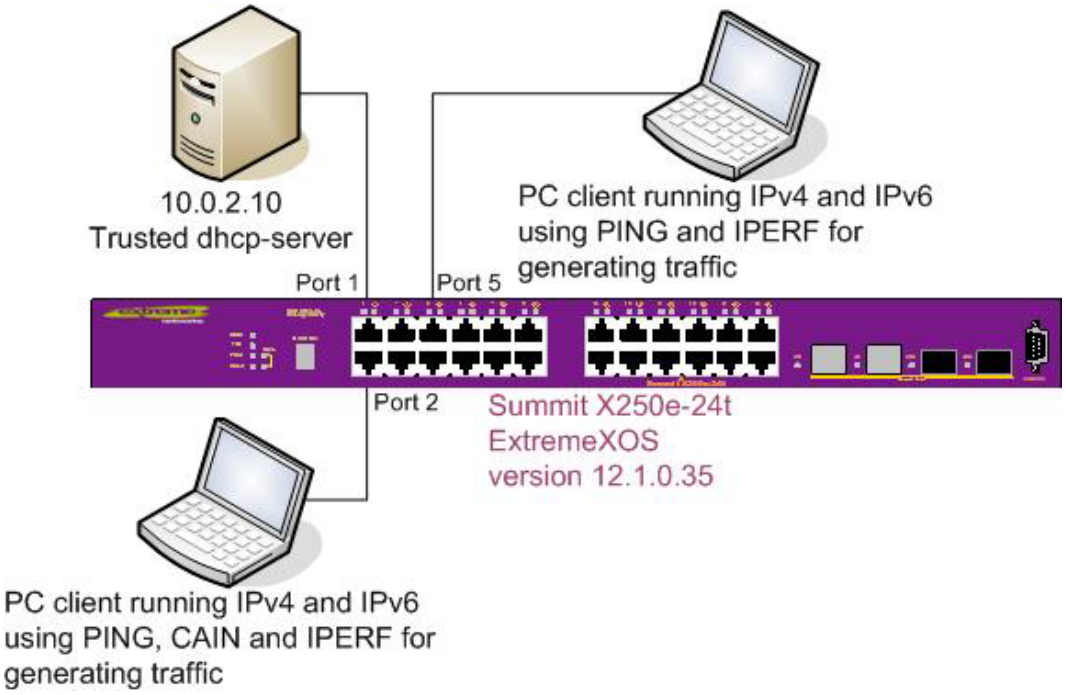
enable ip-security arp gratuitous-protection {vlan} [all | <vlan_name>]

show ip-security arp gratuitous-protection

10 KONFIGURATIONSEXEMPEL

Nedan visar utdrag ur en konfigurationsfil och visar på hur kommandon i en switch från Extreme Networks med EXOS, version 12.1 eller senare kan användas för att aktivera funktioner som tillhandahåller de krav som ställs på SKA-certifierad switch.

Ett vlan, kallat uservlan med portar 1-2,5,24-25 är skapat och har fått ovanstående beskrivna funktioner aktiverade. DHCP server ansluts till port 1, se bild nedan:




```
#X250e-24t.11 # sh conf "vlan"
#
# Module vlan configuration.
#
enable iparp gratuitous inspection vlan Default
create vlan "uservlan"
enable iparp gratuitous inspection vlan uservlan
configure vlan Default delete ports all
configure vlan uservlan add ports 1-2, 5, 24-25 untagged
configure qosscheduler strict-priority
disable iparp learning vlan uservlan port 2
disable iparp learning vlan uservlan port 5
disable iparp learning vlan uservlan port 24
disable iparp learning vlan uservlan port 25
```

```
X250e-24t.12 # sh conf "ipSecurity"
#
# Module ipSecurity configuration.
#
enable ip-security dhcp-snooping vlan uservlan port 1 violation-action drop-packet
enable ip-security dhcp-snooping vlan uservlan port 2 violation-action drop-packet
enable ip-security dhcp-snooping vlan uservlan port 5 violation-action drop-packet
enable ip-security dhcp-snooping vlan uservlan port 24 violation-action drop-packet
enable ip-security dhcp-snooping vlan uservlan port 25 violation-action drop-packet
configure trusted-ports 1 trust-for dhcp-server
configure trusted-servers vlan uservlan add server 10.0.2.10 trust-for dhcp-server
enable ip-security source-ip-lockdown ports 2-12, 16-24
enable ip-security arp learning learn-from-arp vlan uservlan ports 1
enable ip-security arp learning learn-from-dhcp vlan uservlan ports 1
enable ip-security arp learning learn-from-dhcp vlan uservlan ports 2
enable ip-security arp learning learn-from-dhcp vlan uservlan ports 5
enable ip-security arp learning learn-from-dhcp vlan uservlan ports 24
enable ip-security arp learning learn-from-dhcp vlan uservlan ports 25
enable ip-security arp validation ip vlan uservlan ports 2 violation-action drop-packet
enable ip-security arp validation ip vlan uservlan ports 5 violation-action drop-packet
enable ip-security arp validation ip vlan uservlan ports 24 violation-action drop-packet
enable ip-security arp validation vlan uservlan ports 25 violation-action drop-packet
enable ip-security arp gratuitous-protection vlan Default
enable ip-security arp gratuitous-protection vlan uservlan
configure ip-security dhcp-snooping information policy replace

X250e-24t.13 # sh conf "acl"
#
# Module acl configuration.
#
create access-list NoIPv6ICMP " protocol icmpv6 ;" " deny  ;" application "Cli"
create access-list NoMCAST " destination-address 224.0.0.0/4 ;" " deny  ;" application
"Cli"

configure access-list zone SYSTEM application NetLogin application-priority 3
configure access-list zone SECURITY application GenericXml application-priority 2
configure access-list add NoMCAST last priority 0 zone SYSTEM ports 2 application
"Cli" ingress
configure access-list add NoMCAST last priority 0 zone SYSTEM ports 5 application
"Cli" ingress
configure access-list add NoMCAST last priority 0 zone SYSTEM ports 24 application
"Cli" ingress
configure access-list add NoIPv6ICMP last priority 0 zone SYSTEM vlan uservlan
application "Cli" ingress
```