Edgecore SKA 3.1 certifiering

8 augusti

2008

Dokumetet beskriver hur Edgecore's ES3528 segement skall sättas upp för att klara SSNf's SKA 3.1 certifiering

1 Innehållsförteckning

1.1 SSnFs krav för SKA 3.1

Kraven nedan är kopierade från SSNF's SKA v3.1 rapport och dokumentet beskriver sedan hur testen utförts och hur switcharna konfigureras.

1 *Så kallad DHCP-snooping ska finnas på accessportarna, d v s. en kund ska inte kunna vara DHCP-server åt någon annan kund.*
2 *Det ska inte gå att sätta en fast IP-adress och komma vidare från porten som kunden är ansluten i.*
3 *När kunden fått en eller flera adresser via DHCP ska bara den eller de adresserna kunna skicka trafik ut från den porten.*
4 *Om inte adressen förnyas via DHCP-servern ska den adressen stängas av I switchporten.*
5 *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.*
6 *Alla försök till spoofing/poisoning bör kunna loggas till t.ex syslogserver för att trojaner/virus och hackare ska kunna spåras.*
7 *Spårbarhet ska läggas in i DHCP-förfrågningarna i "L2-läge", accessswitchen skall inte vara DHCP-relay.*
8 *Det bör finnas filtreringsmöjligheter mellan kundportar så att t.ex godtyckliga TCP/UDP-portar kan filtreras bort mellan kunder*
9 *Om fasta IP-adresser används ska switchporten bara tillåta den för porten definierade IP-adressen som source-adress i TCP/IP och ARP-paket.*
10 *UPnP ska alltid vara spärrat mellan acessportar.*
11 *IPv6 ICMP6 router advertisment och IPv6 DHCP-servrar ska spärras mellankundportar.*

1.2 Edgecore's säkerhetsfunktioner

I Edgecores ES3528 finns ett antal säkerhetsfunktioner som gör att switcharna uppnår SKA 3.1 och på så sätt ger kunderna som ansluts en säker och trygg anslutning. Funktionerna nedan är det som används för att nå SKA version 3.1 certifiering.

- DHCP snooping
- DHCP snooping option 82
- Ip source guard
- Ip arp inspection
- Private vlan

1.2.1 DHCP snooping

DHCP snooping används för att inte slutkunder skall kunna sätta upp en DHCP-server och dela ut IP-adresser åt andra kunder.

1.2.1.1 Konfigurering av DHCP snooping

DHCP-snooping ställs in globalt per vlan.

```
ip dhcp snooping
ip dhcp snooping vlan 1
```

Uplinkporten mot DHCP-server måste sättas i läget trust så att DHCP-förfrågningar kan passera till/från servern.

```
interface ethernet 1/28
 ip dhcp snooping trust
```

1.2.2 DHCP snooping option 82

DHCP snooping option 82 används för att DHCP-servern skall kunna logga vilka IP-adresser som tilldelats på respektive port och switch.

1.2.2.1 Konfigurering av DHCP option 82

Option 82 ställs in globalt i switchen.

```
ip dhcp snooping information option
```

1.2.3 Ip source guard och ip arp inspection

ip source guard och *ip source guard* garanterar att kundens MAC-adress och IP-adressen som tilldelats av DHCP-servern i är source adresserna i IP och ARP-paket för att förhindra ARP och IP Spoofing.

1.2.3.1 Konfigurering av IP source guard och ip arp inspection

Ip arp inspection ställs in global och per vlan och tillåten IP och MAC-adress registreras på respektive port efter att en IP-adress tilldelats via DHCP.

```
ip arp inspection
ip arp inspection vlan 1
```

Ställ sedan in *ip source-guard*/interface

```
interface ethernet 1/2
 ip source-guard sip-mac
```

Uplinkporten mot DHCP-server ställs i läge trust för *arp inspection*

```
interface ethernet 1/28
ip arp inspection trust
```

1.2.3.2 Ip Source guard med fast IP-adress

Om man använder fast IP-adress måste man ställa in vilken IP och MAC-adress som skall finnas på respective port.

```
Ip source guard binding 00-11-22-44-44-55 vlan 1 192.168.187.187
interface Ethernet 1/13
```

1.2.4 Private vlan

Private VLAN används för att filtrera bort UPNP och Ipv6-trafik mellan slutkundsportar.

1.2.4.1 Uppsättning av Private VLAN

Portarna 1/1-10 kan inte prata direkt med varandra utan de måste upp via uplinkporten 1/28 för att nå varandra. Default gateway bör proxy-arpa mellan kunderna på port 1-10 för att de ska kunna kommunicera med varandra.

```
PVLAN
pvlan up-link ethernet 1/28 down-link ethernet 1/1-10
```

1.3 Exempel på switch och DHCP-konfigurering

1.3.1 Switchkonfigurering

```
ip dhcp snooping
ip dhcp snooping vlan 1
ip dhcp snooping information option
!
ip arp inspection
ip arp inspection vlan 1
!
interface ethernet 1/1
 ip source-guard sip-mac
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
!
interface ethernet 1/2
 ip source-guard sip-mac
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
!
!
interface ethernet 1/28
 ip dhcp snooping trust
 ip arp inspection trust
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
!
!
PVLAN
pvlan up-link ethernet 1/28 down-link ethernet 1/1-10
```

1.3.2 DHCP-server

ISC's dhcp-sevrer version 4.1.0a1 använder vid testen.

Utdrag ur /etc/dhcpd.conf

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

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

I loggen produceras följande.

Jun 13 05:53:57 skaserver dhcpd: DHCPACK on 192.168.50.98 to
00:12:cf:73:6e:e0 via eth1
Jun 13 05:55:29 skaserver dhcpd: DHCPREQUEST for 192.168.50.98 from
00:12:cf:73:6e:e0 via eth1
Jun 13 05:55:29 skaserver dhcpd: DHCPACK on 192.168.50.98 to
00:12:cf:73:6e:e0 via eth1
Jun 13 05:55:59 skaserver dhcpd: Lease for 192.168.50.96 is connected
to interface 1/2 VLAN 1 on switch 0:12:cf:73:6e:e0
Jun 13 05:55:59 skaserver dhcpd: Lease for 192.168.50.96 raw option-
82 info is CID: 4.1.258 AID: 0.6.0.12.cf.73.6e.e0
Jun 13 05:55:59 skaserver dhcpd: DHCPREQUEST for 192.168.50.96 from
00:0c:29:52:7e:7d (ska3.ssnf.org) via eth1
Jun 13 05:55:59 skaserver dhcpd: DHCPACK on 192.168.50.96 to
00:0c:29:52:7e:7d (ska3.ssnf.org) via eth1
```