IPv6 säkerhet för hem och små företag

Säkerhet genom simpel nätverksutrustning

Högskoleingenjörsexamensarbete
Fredrik Folke
2012-06-18

Agenda

- Inledning
- Bakgrund
- Metod
- Sammanfattning
- Frågor

Inledning

Inledning: Behovet av IPv6

- Ipv4 är idag slut hos världs distributören
  - Europe and Meddle East(RIPE) slut ca: Mars 2013!

    Enligt http://www.ipv4depletion.com
- Återanvändning
- Nya hem, verksamheter eller andra publika enheter kommer inte kunna anslutas

Inledning: Säkerhets problem

- Bristande kunskap
  - Dålig säkerhet i slutet på IPv4, återupprepning med IPv6
  - Små företag blir vanliga måltavlor
- Globalt växande genom ett ökande IPv6 stöd
  - Vanliga OS levereras med IPv6 tillgängligt som standard
  - Vanliga VPN tjänster kan ge IPv6 anslutning som standard
- Skadlig kod har fått fotfäste på IPv6
  - Bank trojanen Zeus samt kontroll trafik för botnät

Inledning: Kommersiella lösningar

- Dyr och svår konfigurerad hårdvarubrandvägg
  - Tester visar att fåtal brandväggar ger ett bra IPv6 skydd

  Enligt http://techworld.idg.se/2.15821/1.431895/6-brandvaggar-for-ipv6
- Tillverkare vill inte se IPv6 tester i media
- Kunskap och tillvägagångssätt saknas
  - Hem och små företag behöver vägledning till IPv6 säkerhet.

Inledning: Projektets problem definition

- Hotbilds analys
  - Vilka hot kan ett IPv6 nätverk utsättas för?
- Kostnadseffektiv implementation
  - Går det att använda simpel nätverks utrustning?
- Strukturerad metod
  - Går det att fastställa ett tillvägagångssätt för normala användare?

Bakgrund

Bakgrund: IPv6 introduktion

- 128 bit adress istället för 32 bit
  - Global scanning blir svårt, DNS ny måltavla
- ICMPv6
  - Viktigt för all IPv6 anslutning både LAN och WAN, kräver finare filtrering.
- IPsec
  - Vanligt missförstånd, kryptering som måste konfigureras mellan dom berörda noderna.

Bakgrund: Hotbild

- Rekognosering/Spaning
- Överbelastningsattack
- Inbrytning/Forcering

- Social Engineering
- Trojaner/skadlig kod
- Inkapslad trafik

Externa Attacker

Interna Attacker

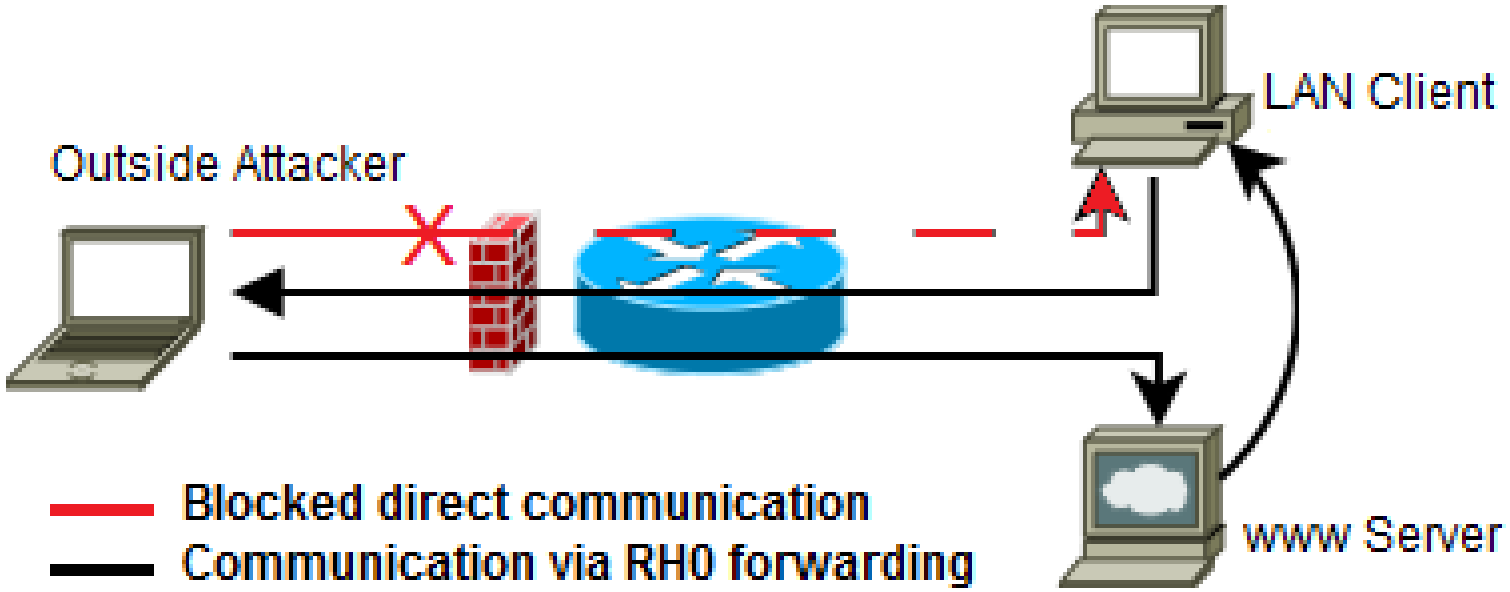
Bakgrund: IPv6 svaghet

- Type 0 Routing Header ”RH0”
  - Innehåller flera IP adresser som måste besökas

Next Header (8 bit)	Hdr Ext Length **Value N**	Routing Type **Value 0**	Segments Left **Value N**
Reserved			
Address[1]			
Address[2]			
Address[N]			

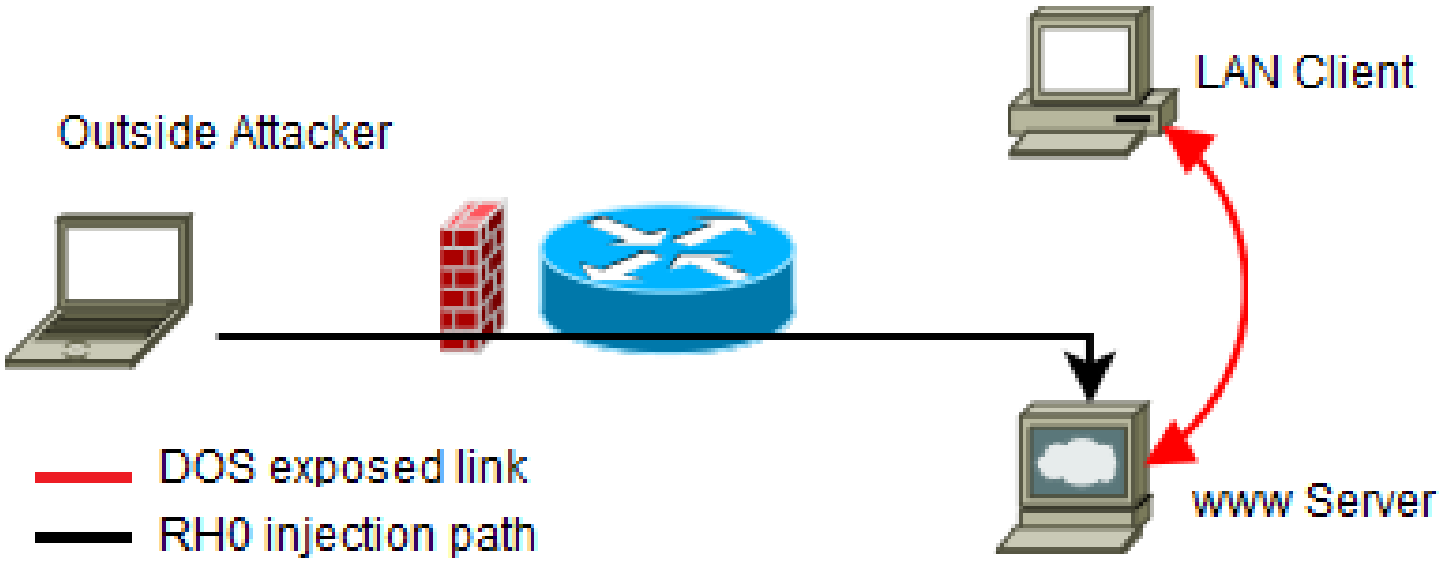
Bakgrund: IPv6 specifika hot

- Type 0 Routing Header ”RH0”
  - Kan tillåta scanning och kommunikation av ej publika adresser



Bakgrund: IPv6 specifika hot, fort.

- Type 0 Routing Header ”RH0”
  - DoS genom flertalet identiska adresser i samma paket



- ”RH0” är inte längre nödvändig för IPv6 implementation

Bakgrund: Hot mot applikationer

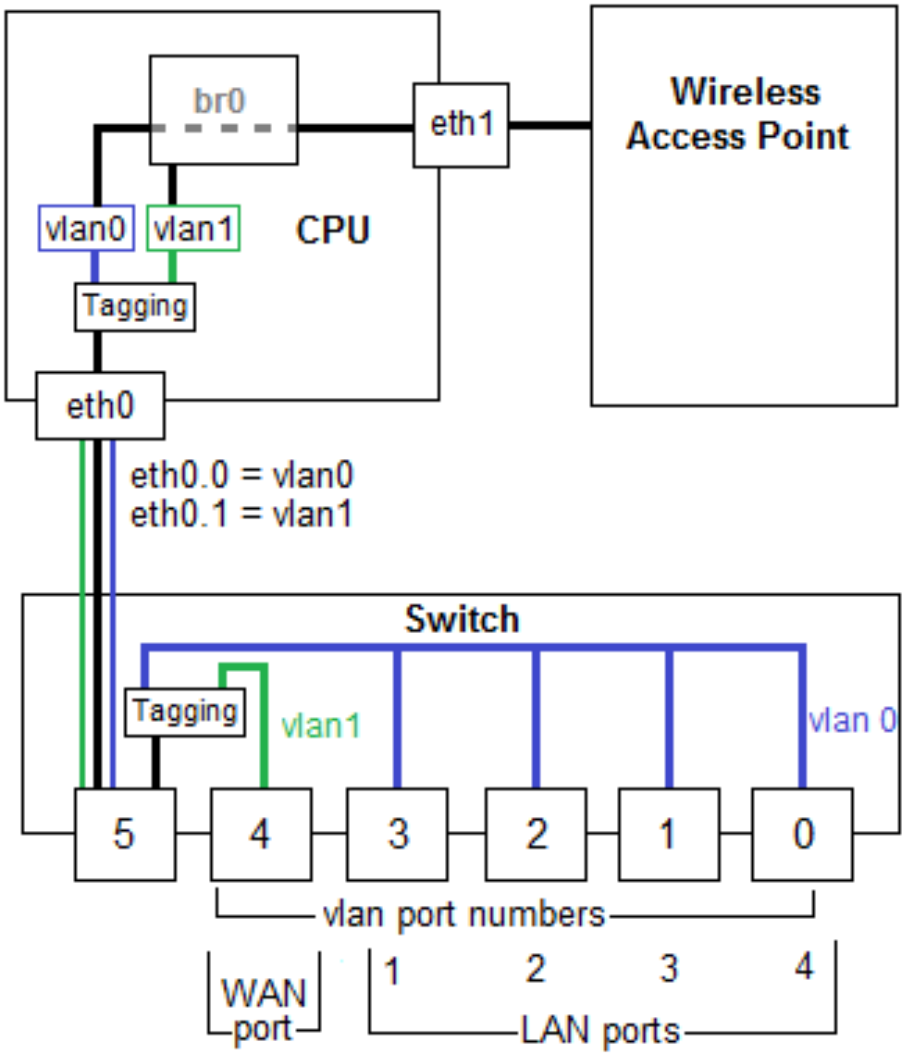
- Inkapslad trafik rakt igenom brandväggen
  - Osynlig utan deep packet inspection

Bakgrund: Hot mot applikationer, fort.

- Anslutningar initierade från LAN sidan
  - Skapar luckor i brandväggen genom att bjuda in trafiken.

- Egress filtrering på applikations nivå

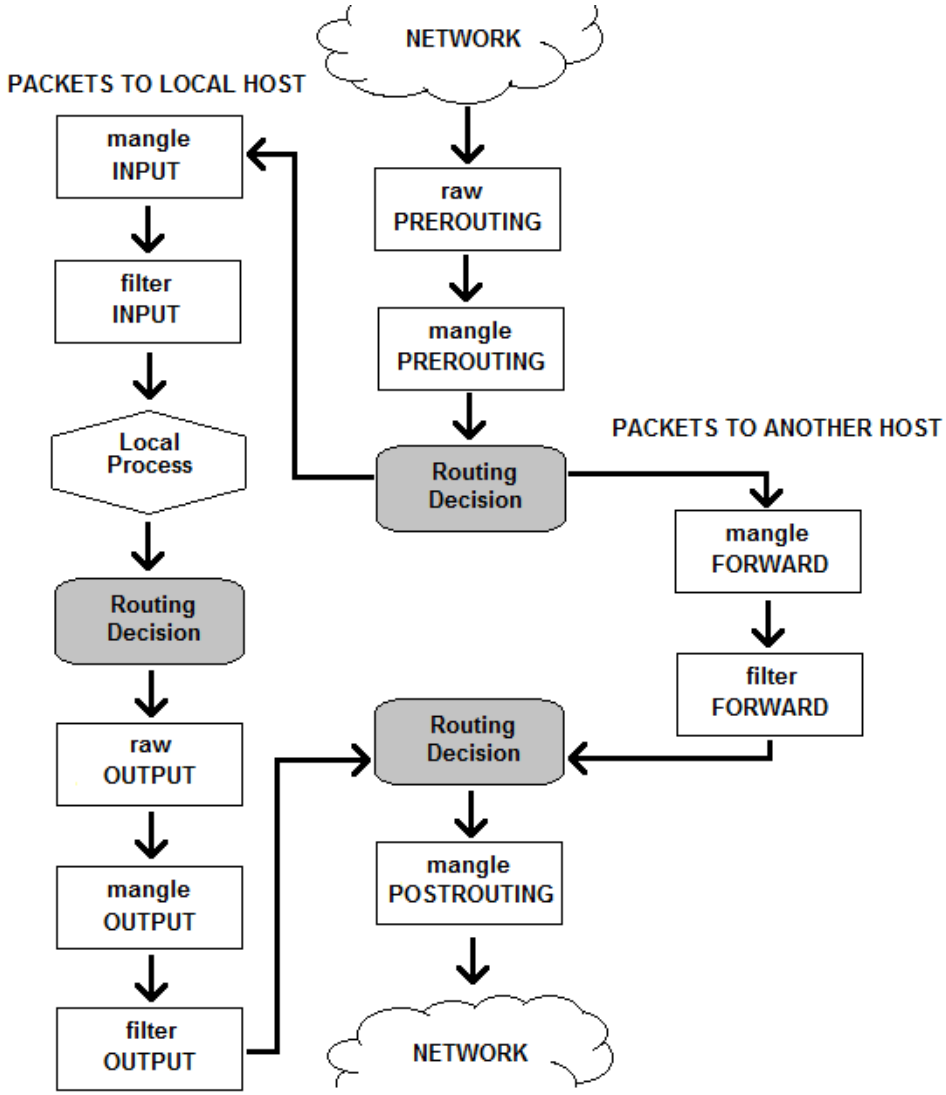
Bakgrund: Routern



Bakgrund: Paket filtrering

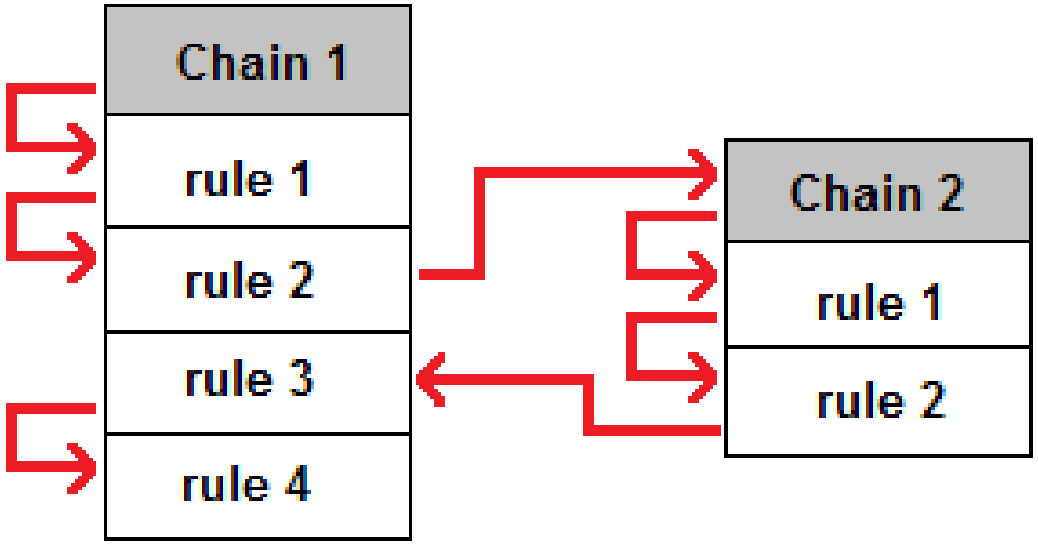
- Access Control Lists (ACL)
  - Begränsa tillgängligheten genom ex. adresser
- Begränsningar
  - Stoppar endast kända trafik mönster
  - Saknar beteende analys
  - Tittar inte i paketets data fält
- Kedjor
  - Forward, trafik destinerat till andra noder(LAN)
  - Input, trafik till den egna kärnan
  - Output, trafik som lämnar den egna kärnan
- Regler
  - Sekventiella listor av regler som matchas mot paket huvudet
  - Måste regleras på både Forward och Input kedjorna

Bakgrund: Filtrerings mekanismen



Bakgrund: Filtrerings mekanismen, fort.

- Regel kedjor
  - Genom hoppregler kan man öka prestanda och skapa egna kedjor



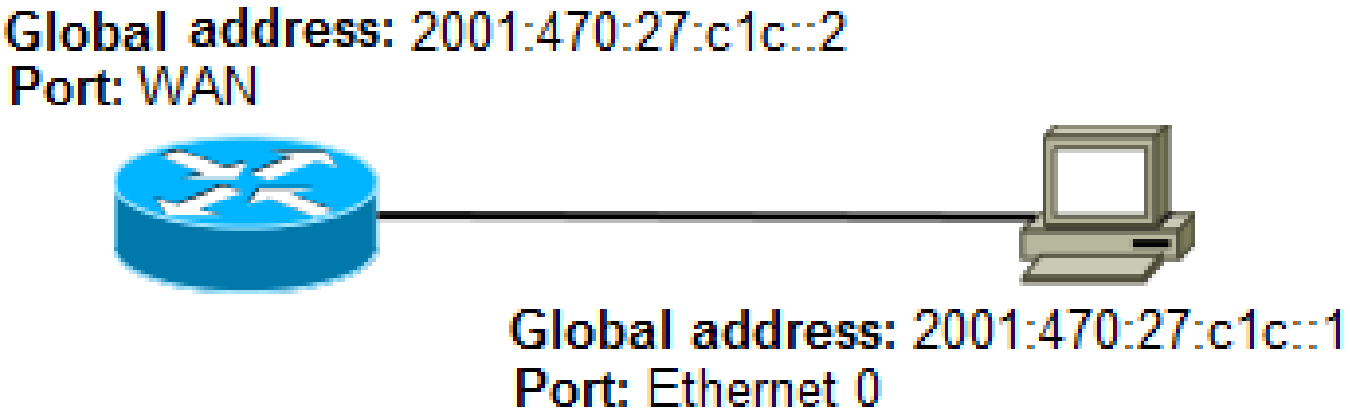
Metod

Metod: Implementering

- Experiment miljö
  - Isolerad och ej exponerad
  - Starta SSH server eller övriga tjänster för granskning
- Debug och paket analysering
  - Tcpdump, spara på router och analysera på klient

Metod: Implementering

- Simulera WAN trafik
  - Isolerat och kontrollerat



Metod: Test av standard konfiguration

- Standard IPv4 Brandvägg

Coding 3.5: Output of iptables, IPv4 firewall at the Asus.

```
root@DD-WRT:~# iptables -vL
Chain INPUT (Policy ACCEPT)
target  prot  opt  source     destination
ACCEPT  0     --   anywhere   anywhere      state RELATED,ESTABLISHED
...
DROP    icmp  --   anywhere    anywhere
...
DROP    0     --   anywhere    anywhere

Chain FORWARD (Policy ACCEPT)
...
```

  - Accept policy, stateful, droppa ICMP, droppa allt.

Metod: Test av standard konfiguration

- Nmap granskning av IPv4 brandvägg via IPv4

Coding 3.6: Nmap scan output using IPv4 address with IPv4 firewall.

```
root@PC/# nmap 10.10.1.2
root@PC/# ...
root@PC/# Nmap scan report for 10.10.1.2
root@PC/# Host is up (0.00029s latency).
root@PC/# All 1000 scanned ports on 10.10.1.2 are filtered (1000)
root@PC/# MAC Address: BC:AC:C5:C4:CA:8F (Unknown)

Nmap done: 1 IP adress (1 host up) scanned in 21.30 secounds
```

  - Bra resultat

Metod: Test av standard konfiguration

- Nmap granskning av IPv4 brandvägg via IPv6

Coding 3.7: Nmap scan output using IPv6 address with IPv4 firewall.

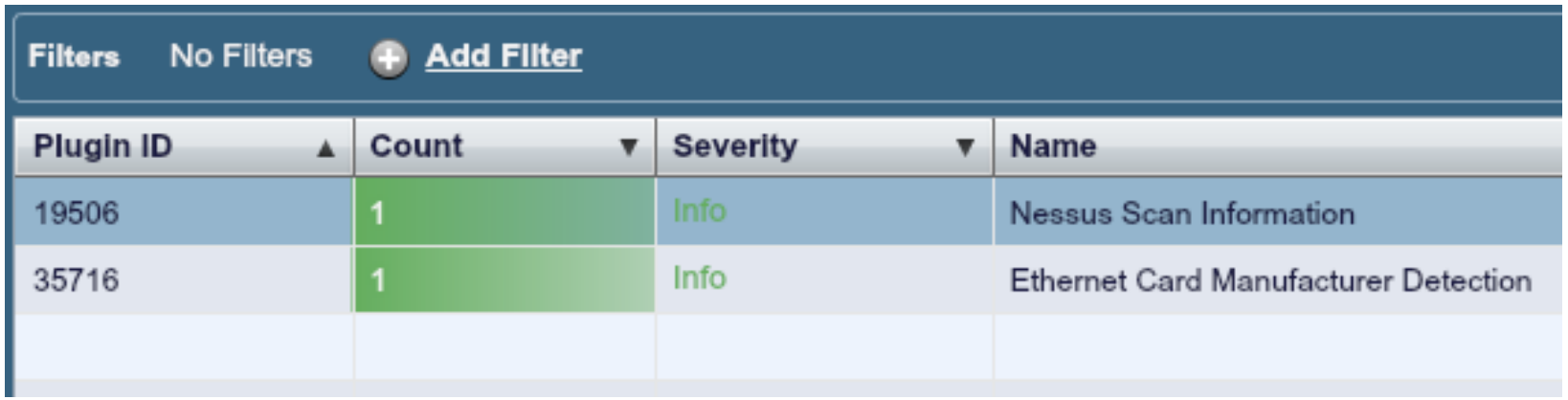
```
root@PC/# nmap -6 2001:470:27:c1c::2
...
Nmap scan report for 2001:470:27:c1c::2
Host is up (0.00088s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 1.14 seconds
```

  - Inte godkänt, SSH samt DNS porten öppen

Metod: Test av standard konfiguration

- Nessus granskning av IPv4 brandvägg via IPv4



  - Godkänt, MAC adressen avslöjar tillverkare i test lab.

Metod: Test av standard konfiguration

- Nessus granskning av IPv4 brandvägg via IPv6

Filters No Filters Add Filter

Plugin ID	Count	Severity	Name
11255	1	Critical	Default Password (root) for 'root' Account
58183	1	High	Dropbear SSH Server Channel Concurrency Use-after-free Remote Code Execution
11219	2	Info	Nessus SYN scanner
22964	2	Info	Service Detection
10267	1	Info	SSH Server Type and Version Information
10881	1	Info	SSH Protocol Versions Supported
19506	1	Info	Nessus Scan Information

  - IPv4 brandväggen får underkänt att hantera IPv6 trafik

Metod: Test av standard konfiguration

- Slutsats av standard konfigurationen
  - Totalt underkänt att använda IPv4 brandvägg
  - Känner inte igen trafiken, accepterar allt
  - Okunskap kan göra mycket skada vid IPv6 migrering
- Lösning, Ip6tables?
  - Implementation
  - Konfiguration

Metod: ip6tables

- Hämta ip6tables, med tillhörande moduler
  - Färdiga paket lösningar
  - Moduler för olika filtrerings funktioner bl.a. ”RH0” samt ”conntrack”
- Startupp skript för IPv6 brandväggs regler
  - Service eller säkerhet, standard policy = Drop

Metod: Regler

- Tillåta LAN och viss WAN trafik

```
# allow all traffic to loopback
ip6tables -A INPUT -i lo -j ACCEPT

# allow all traffic from LAN to local host
ip6tables -A INPUT -i br0 -j ACCEPT
# allow specific traffic from WAN to local host
ip6tables -A INPUT -I vlan2 -m state --state ESTABLISHED,RELATED -j ACCEPT

# allow all traffic from LAN to LAN/WAN
ip6tables -A FORWARD -i br0 -j ACCEPT
# allow traffic from WAN related or est. to LAN connections
ip6tables -A FORWARD -i vlan2 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Metod: Test av IPv6 konfiguration

- Nmap jämförelse med tidigare IPv6 resultat

Coding 3.7: Nmap scan output using IPv6 address with IPv4 firewall.

```
root@PC/# nmap -6 2001:470:27:c1c::2
...
Nmap scan report for 2001:470:27:c1c::2
Host is up (0.00088s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 1.14 seconds
```

Coding 3.14: Nmap scan output try nr.1 using IPv6 address with IPv6 firewall.

```
root@PC/# nmap -6 2001:470:27:c1c::2
...
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.05 seconds
```

- Den nya IPv6 brandväggen klarar första testet

Metod: Test av IPv6 konfiguration

- Nmap jämförelse med tidigare IPv6 resultat

Coding 3.7: Nmap scan output using IPv6 address with IPv4 firewall.

```
root@PC/# nmap -6 2001:470:27:c1c::2
...
Nmap scan report for 2001:470:27:c1c::2
Host is up (0.00088s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 1.14 seconds
```

Coding 3.14: Nmap scan output try nr.1 using IPv6 address with IPv6 firewall.

```
root@PC/# nmap -6 2001:470:27:c1c::2
...
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.05 seconds
```

- Den nya IPv6 brandväggen klarar första testet

Metod: Test av IPv6 konfiguration

- Nmap försök nr.2

Coding 3.15: Nmap scan output try nr.2 using IPv6 address with IPv6 firewall.

```
root@PC/# nmap –6 -Pn 2001:470:27:c1c::2
...
Nmap scan report for 2001:470:27:c1c::2
Host is up.
All 1000 scanned ports on 2001:470:27:c1c::2 are filtered

Nmap done: 1 IP address (1 host up) scanned in 201.35 seconds
```

Metod: Test av IPv6 konfiguration

- Nmap försök nr.2

Coding 3.15: Nmap scan output try nr.2 using IPv6 address with IPv6 firewall.

```
root@PC/# nmap –6 -Pn 2001:470:27:c1c::2
...
Nmap scan report for 2001:470:27:c1c::2
Host is up.
All 1000 scanned ports on 2001:470:27:c1c::2 are filtered

Nmap done: 1 IP address (1 host up) scanned in 201.35 seconds
```

Metod: Test av IPv6 konfiguration

- Tidigare Nessus granskning av IPv4 brandväggen

Filters No Filters Add Filter

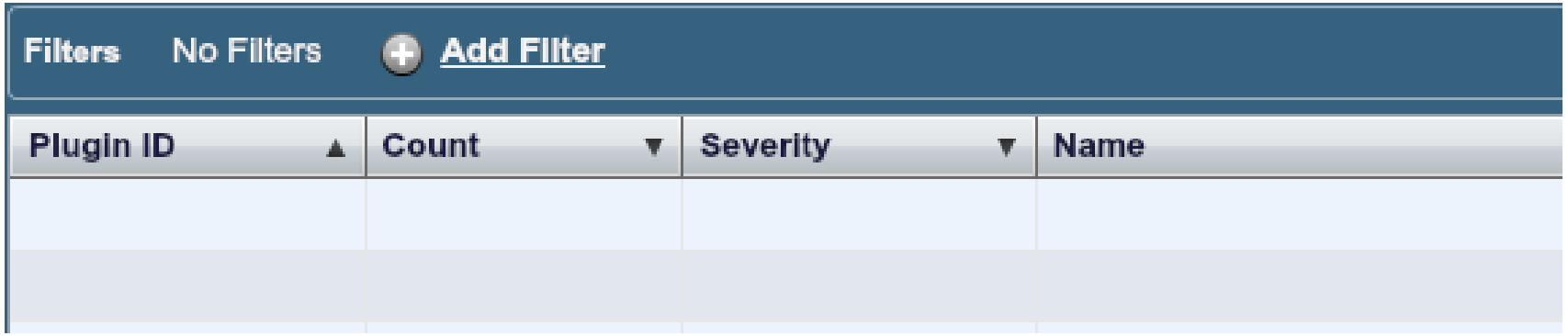
Plugin ID	Count	Severity	Name
11255	1	Critical	Default Password (root) for 'root' Account
58183	1	High	Dropbear SSH Server Channel Concurrency Use-after-free Remote Code Execution
11219	2	Info	Nessus SYN scanner
22964	2	Info	Service Detection
10267	1	Info	SSH Server Type and Version Information
10881	1	Info	SSH Protocol Versions Supported
19506	1	Info	Nessus Scan Information

IPv4

  - Skräck exempel

Metod: Test av IPv6 konfiguration

- Nessus granskning av IPv6 brandväggen
  - Hot analysen visar ett tomt resultat



  - IPv6 brandväggen, klart godkänd

Metod: Test av IPv6 konfiguration

- Test av Rate-limiting
  - Ping flod genom att definiera intervallet till 0

Coding 3.16: Ping output, flood experiment.

```
root@PC/# ping6 -i 0 2001:470:27:c1c::2
PING 2001:470:27:c1c::2(2001:470:27:c1c::2) 56 data bytes
64 byte from 2001:470:27:c1c::2: icmp_seq=1 ttl=64 time=9.80 ms
64 byte from 2001:470:27:c1c::2: icmp_seq=2 ttl=64 time=0.336 ms
...
64 byte from 2001:470:27:c1c::2: icmp_seq=214 ttl=64 time=0.342 ms
--- 2001:470:27:c1c::2 ping statistics ---
221 packets transmitted, 25 received, 88% packet loss, time 3119ms
...
```

    - Icmp_seq=1… 214, 221 skickade paket och 25 mottagna

Metod: Test av IPv6 konfiguration

- Test av Rate-limiting
  - IPv6 brandväggen har registrerat paketen

```
Chain ICMPfilter (2 references)
 pkts bytes target     prot opt in   out  source   destination
    0     0 ACCEPT     icmpv6     *    *    ::/0     ::/0       ipv6-icmp type 1
    0     0 ACCEPT     icmpv6     *    *    ::/0     ::/0       ipv6-icmp type 2
    0     0 ACCEPT     icmpv6     *    *    ::/0     ::/0       ipv6-icmp type 3
    0     0 ACCEPT     icmpv6     *    *    ::/0     ::/0       ipv6-icmp type 4
    0     0 ACCEPT     icmpv6     *    *    ::/0     ::/0       ipv6-icmp type 133
    0     0 ACCEPT     icmpv6     *    *    ::/0     ::/0       ipv6-icmp type 134
    1    72 ACCEPT     icmpv6     *    *    ::/0     ::/0       ipv6-icmp type 135
    1    64 ACCEPT     icmpv6     *    *    ::/0     ::/0       ipv6-icmp type 136
   25  2600 ACCEPT     icmpv6     *    *    ::/0     ::/0       ipv6-icmp type 128 limit: avg 5/sec burst 10
    0     0 ACCEPT     icmpv6     *    *    ::/0     ::/0       ipv6-icmp type 129
```

  - Endast accepterat 25 av 221 packet skickade.

Metod: Test av IPv6 konfiguration

No.	Time	Source	Destination	Protocol	Info
1	0.000000	2001:470:27:c1c::1	ff02::1:ff00:2	ICMPv6	Neighbor solicitation for 2001:470:27:c1c::2
2	0.000235	2001:470:27:c1c::2	2001:470:27:c1c::1	ICMPv6	Neighbor advertisement 2001:470:27:c1c::2 (rt
3	0.000452	2001:470:27:c1c::1	2001:470:27:c1c::2	ICMPv6	Echo (ping) request id=0x0a5c, seq=1
4	0.000690	2001:470:27:c1c::2	2001:470:27:c1c::1	ICMPv6	Echo (ping) reply id=0x0a5c, seq=1
5	0.001089	2001:470:27:c1c::1	2001:470:27:c1c::2	ICMPv6	Echo (ping) request id=0x0a5c, seq=2
6	0.001280	2001:470:27:c1c::2	2001:470:27:c1c::1	ICMPv6	Echo (ping) reply id=0x0a5c, seq=2
7	0.001550	2001:470:27:c1c::1	2001:470:27:c1c::2	ICMPv6	Echo (ping) request id=0x0a5c, seq=3
8	0.001732	2001:470:27:c1c::2	2001:470:27:c1c::1	ICMPv6	Echo (ping) reply id=0x0a5c, seq=3
9	0.001988	2001:470:27:c1c::1	2001:470:27:c1c::2	ICMPv6	Echo (ping) request id=0x0a5c, seq=4
10	0.002167	2001:470:27:c1c::2	2001:470:27:c1c::1	ICMPv6	Echo (ping) reply id=0x0a5c, seq=4
11	0.002417	2001:470:27:c1c::1	2001:470:27:c1c::2	ICMPv6	Echo (ping) request id=0x0a5c, seq=5
12	0.002598	2001:470:27:c1c::2	2001:470:27:c1c::1	ICMPv6	Echo (ping) reply id=0x0a5c, seq=5
13	0.002854	2001:470:27:c1c::1	2001:470:27:c1c::2	ICMPv6	Echo (ping) request id=0x0a5c, seq=6
14	0.003033	2001:470:27:c1c::2	2001:470:27:c1c::1	ICMPv6	Echo (ping) reply id=0x0a5c, seq=6
15	0.003287	2001:470:27:c1c::1	2001:470:27:c1c::2	ICMPv6	Echo (ping) request id=0x0a5c, seq=7
16	0.003466	2001:470:27:c1c::2	2001:470:27:c1c::1	ICMPv6	Echo (ping) reply id=0x0a5c, seq=7
17	0.003720	2001:470:27:c1c::1	2001:470:27:c1c::2	ICMPv6	Echo (ping) request id=0x0a5c, seq=8
18	0.003899	2001:470:27:c1c::2	2001:470:27:c1c::1	ICMPv6	Echo (ping) reply id=0x0a5c, seq=8
19	0.004154	2001:470:27:c1c::1	2001:470:27:c1c::2	ICMPv6	Echo (ping) request id=0x0a5c, seq=9
20	0.004332	2001:470:27:c1c::2	2001:470:27:c1c::1	ICMPv6	Echo (ping) reply id=0x0a5c, seq=9
21	0.004583	2001:470:27:c1c::1	2001:470:27:c1c::2	ICMPv6	Echo (ping) request id=0x0a5c, seq=10
22	0.004763	2001:470:27:c1c::2	2001:470:27:c1c::1	ICMPv6	Echo (ping) reply id=0x0a5c, seq=10
23	0.005018	2001:470:27:c1c::1	2001:470:27:c1c::2	ICMPv6	Echo (ping) request id=0x0a5c, seq=11
24	0.019962	2001:470:27:c1c::1	2001:470:27:c1c::2	ICMPv6	Echo (ping) request id=0x0a5c, seq=12
25	0.039871	2001:470:27:c1c::1	2001:470:27:c1c::2	ICMPv6	Echo (ping) request id=0x0a5c, seq=13
26	0.049862	2001:470:27:c1c::1	2001:470:27:c1c::2	ICMPv6	Echo (ping) request id=0x0a5c, seq=14

Metod: Brandväggs alternativ

- Nyckeln till topologin
  - Behovet existerar
- Endast ett skydd
  - Skydda allt eller inget
- Centraliserad admin
  - Bekvämt

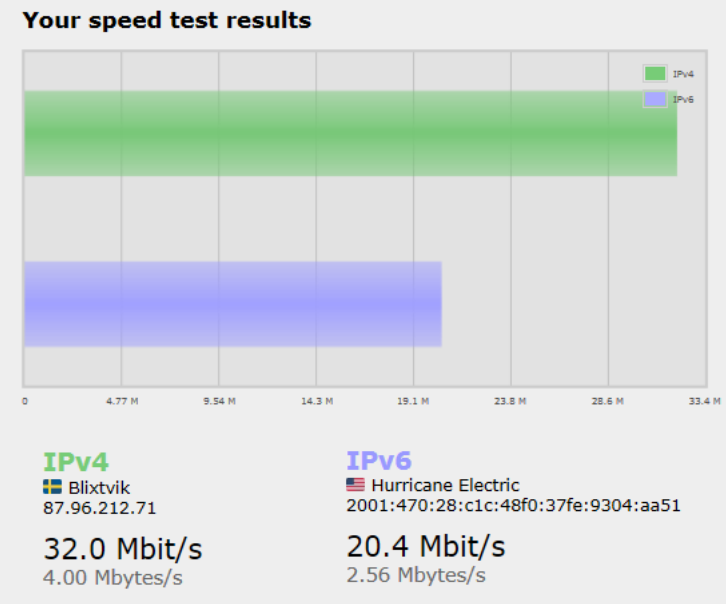
- Lättare utan firmware
  - Mer kapacitet på PC
- Fler stegs skydd
  - Ingen ensam punkt
- Svårt för andra enheter
  - NAS/TV apparater

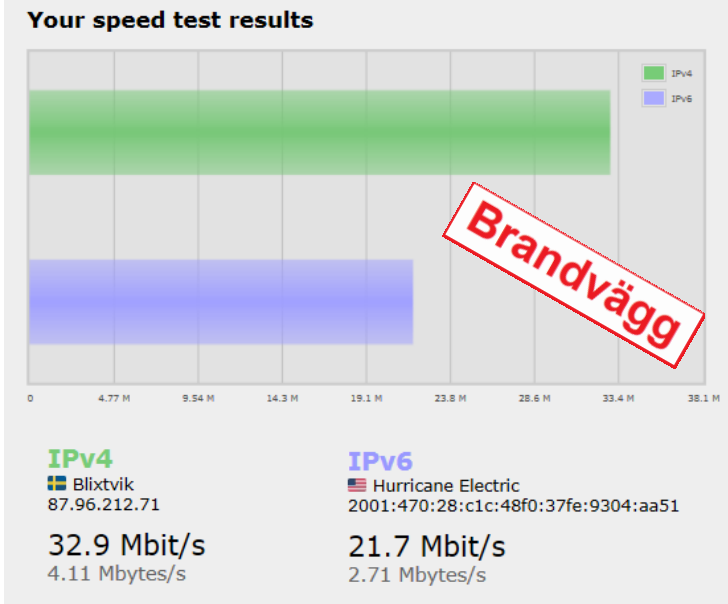
Router metoden

Klient metoden

Metod: Prestanda

- Hastighets test från Klient genom ipv6-test.com





- Ingen förändring för den vanliga användaren

Sammanfattning

- IPv6 migrering kan innebära stora säkerhets risker
  - Bristande kunskap gör situationen ett skräck exempel
  - ICMP spelar en större roll och behöver special behandling
- Det går inte att förlita sig på IPv4 brandväggen
  - Revidera dom befintliga tjänsterna noga
- Konceptet med simpla konsument routrar fungerar
  - Det går att öka IPv6 säkerheten både billigt och effektivt.
  - Prestandan är den samma för den vanliga användaren
  - Router eller Klient metoden är en behovs fråga

Frågor / Questions