



IPv6-stöd i brandväggar

Internetdagarna 2009

hakan.lindberg@b3it.se

Agenda

- **Varför?**
- **Testupplägg**
- **Resultat**
- **Q & A**

Varför IPv6?

- IPv4 blir en bristvara
- NAT etc. inga långsiktiga lösningar för ett större Internet där alla och allt sitter ihop.

• Varför testa brandväggar?

- Går att få IPv6 från operatörer
- Windows Vista, Windows Server 2008, Mac OS X m.fl har IPv6
 - Kan finnas i ditt nät utan att du planerat för det
- Brandväggar en central punkt för säkerhet.
 - Krävs ibland (PCI, policy)
 - Ofta en god idé
 - Enkel stateful IPv6 brandvägg som ersätter NAT skulle ge fördelar kommunikation host-host
 - Bort från NAT i NAT och carrier-NAT
 - VPN koncentrator

Vad är en brandvägg?



IPv6 ready?

Över 350 produkter har en “IPv6-ready” logotyp

D-link DI-524 and DIR-615. Men levererar ej IPv6 i Europa.

IPv6 är inte inne i värmen...

 IPv6 Ready Logo Phase-1

Certificated appliance search

You can ascertain the information of certificated appliance from Logo ID

Fill Logo ID in the textbox (Ex. 01-000xxxx) : DIR-615

Item	Content
IPv6 Ready Logo Phase	Phase-1
Logo ID	01-000322
Vendor Name	D-Link Corporation/D-Link Systems, Inc. and CAMEO Communications, Inc.
Country Name	TW
Product Name (Original)	DI-524 D
Product version (Original)	v6.4.01

SSAC rapporten 2008...

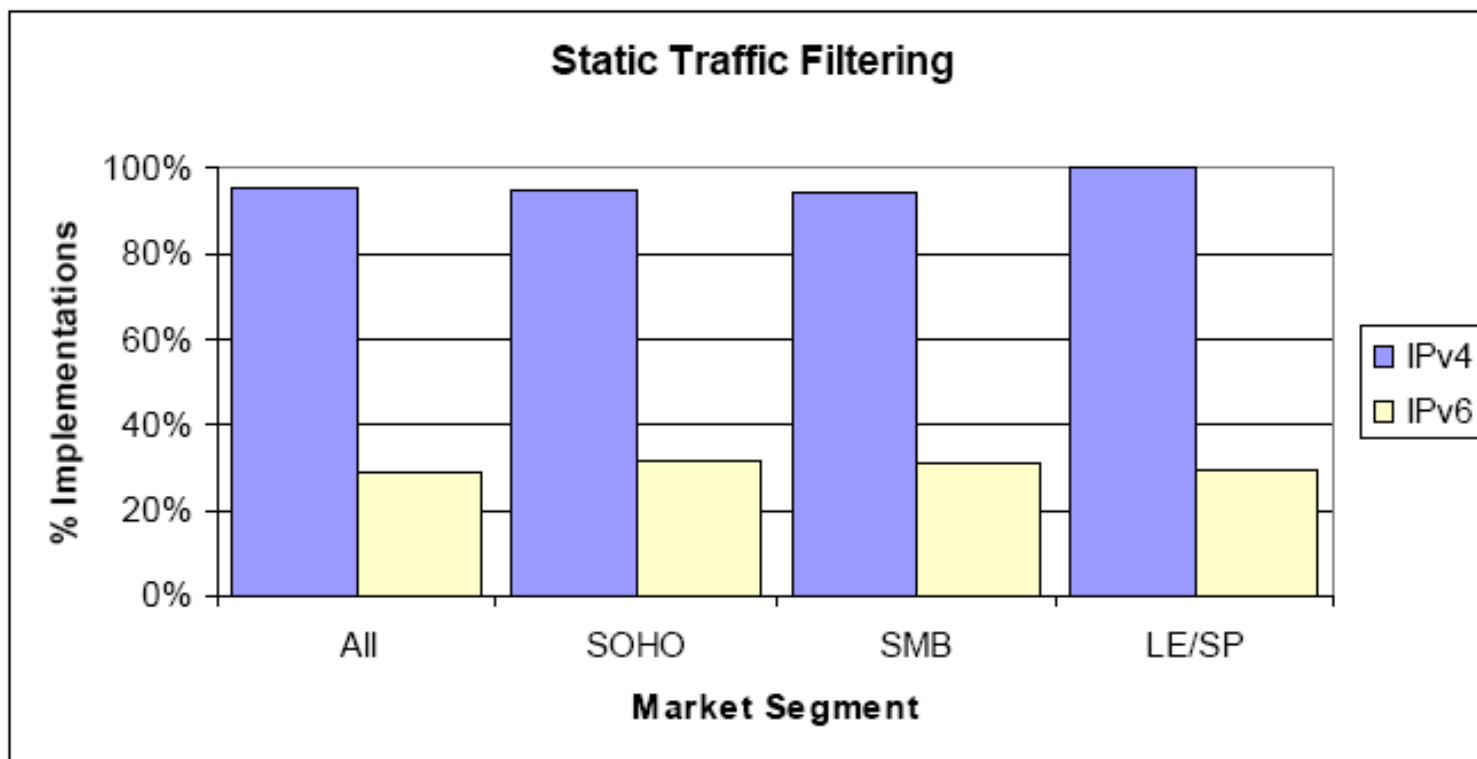
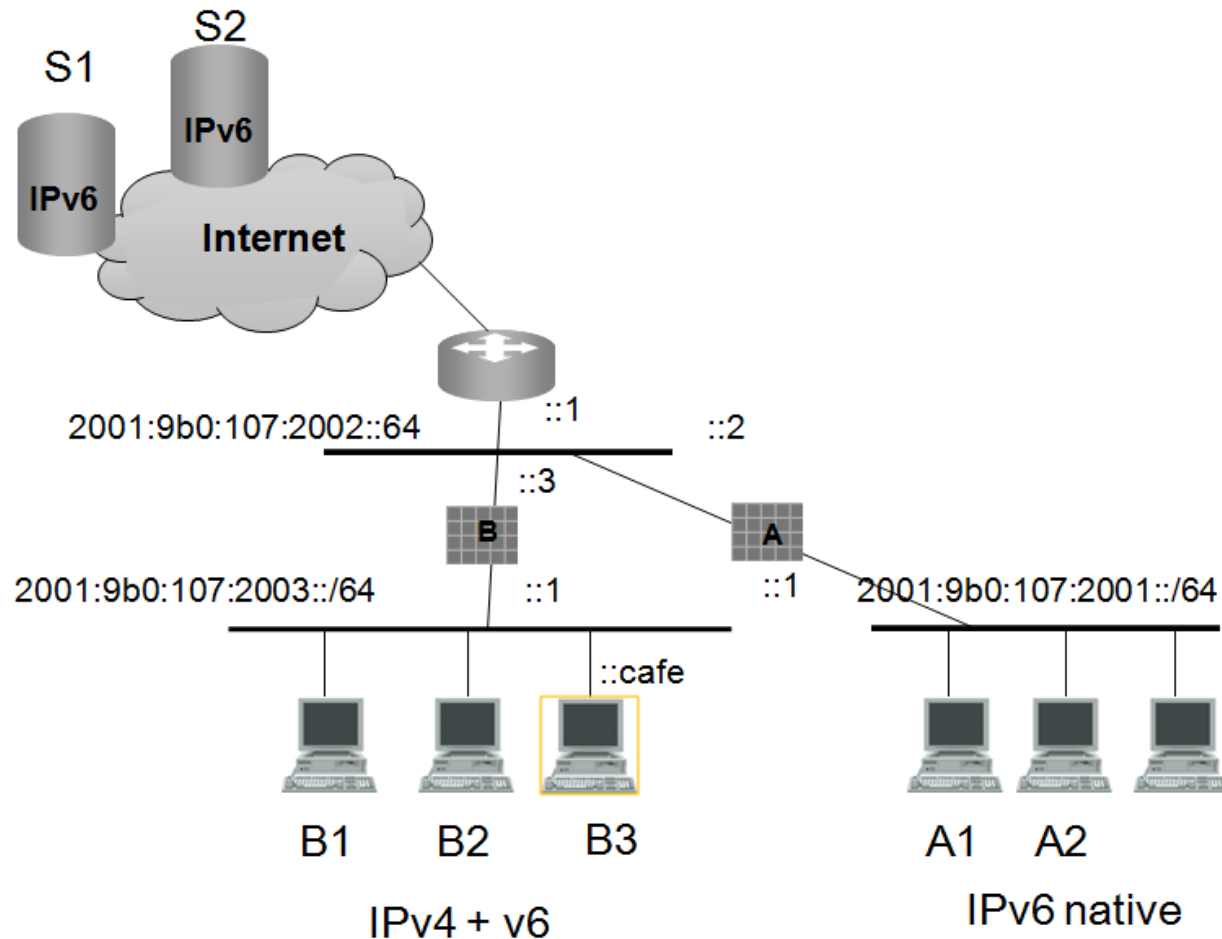


Chart 3. Firewall Support, IPv4 and IPV6 Static Packet Filtering

Set-up



Klientsimulering

- **Programvaran Curl-loader**
 - **Test 1: 5 clients, 3 URLs, 5 cycles**
 - **Test 2: 10 clients, 3 URLs, 10 cycles**
 - **Test 3: 30 sessioner, 3 URLs, 10 cycles**
 - **Vi provade med 100 sessioner och 16 Mbyte på en Apache server men...**

Testat:

- Checkpoint model UTM-1, model 130. Software r70.1
 - Uppsatt av Certezza, Checkpoint ville inte vara med
- Cisco model ASA5505, software 8.2
- Fortinet Fortigate 111C, software v4.0MR1
- H3C, Secpath F1000E, 5.20 feature 3167
- Halon SX-150, software 1.4.0
- Juniper modelSSG320M, sw 6.1.0r2

- 2008: 3Com MSR 50, Cisco 2800 with IOS 12.4, Monowall 1.3b14 (Soekris hardware), (SnapGear SG650), (D-link DIR-615, 524)

Resultat

	IPv6 native	SPI setup ("diode")	IPv6 in log	IPv6 filter	Session test (secs)	Session Failures
Checkpoint	Ok	Ok	Ok	Ok	35 116 342	0
Cisco	Ok	Ok	Ok	Ok	36 170 380	0
Fortinet	Ok	Ok	Ok	Ok	35 102 337	0
H3C	Ok	Ok	Not verified in CLI-interface	Ok	32 95 323	0

Resultat (2)

	IPv6 native	SPI setup ("diode")	IPv6 in log	IPv6 filter	Session test (secs)	Session Failures
Halon	OK	Ok	Ok	Ok	34 107 306	0
Juniper	Ok	Ok	Ok	Ok	No problems with 30 session.	0
No firewall	-	-	-	-	35 108 338	-

Kommentarer

- **Checkpoint model UTM-1, model 130. Software r70.1**
 - Inget webbgränssnitt via IPv6, men enligt uppgift SSH över IPv6
- **Cisco model ASA5505, software 8.2**
 - Har i år även GUI-stöd för IPv6, förra året bara CLI
- **H3C, Secpath F1000E, 5.20 feature 3167**
 - IPv6 genom CLI, inget webbaserat gränssnitt (en tidig releae)

Hands-on är nyttigt!

- **Förra året**
 - DNS problem
 - RA problem
 - ICMP lurigt och lite knepigt
- **2009**
 - RA, Router Advertisement. En brandvägg är ofta en router (och tvärtom) och annonserar att de finns. De blir default gateways men sedan skickar de inte trafiken vidare!
 - Behov av "RA snooping"?
 - ICMP: fungerar annorlunda i IPv6
 - Behövs för "Neighbor Discovery"
 - Får inte stängas av helt (jfr med IPv4)

Extra test: IPsec (ESP och AH)

- **Inbyggd i IPv6**
- **Vi fick det att funka mellan Cisco och Fortinet**
- **Mer info i rapporten**

- **Tack för mig!**