Survey of IPv6 Support in Commercial Firewalls

David Piscitello
Fellow to the ICANN SSAC
Purpose of Study

• Determine IPv6 transport support and security service availability among commercial firewall products
• Survey only, no product testing
• Did not include
  – Personal firewall software
  – Commodity broadband access device that only "block ports and such" (would skew results)
Objectives

- How broadly is IP version 6 (IPv6) transport supported by commercial firewalls?
- Is support for IPv6 transport and security services available for all market segments?
- Are security services commonly used at Internet firewalls available when IPv6 transport is used?
- Can an organization use IPv6 today and enforce a security policy at a firewall that's comparable to one it would enforce using IPv4?
Methodology

• Compile a list of commercial firewall products
  – Various resources yielded approximately 60 products
  – Identify target market segments for products:
    • Small office, home office (SOHO)
    • Small and medium business (SMB)
    • Large Enterprise, service provider (LE/SP)

• Survey commonly available security services
  – List based on vendor technical specifications and input from firewall administrator community
Features included in survey

• IPv6 transport
  – Forward native IPv6 traffic between internal/external hosts
  – Participate in IPv6 routing or neighbor discovery

• Traffic filtering
  – Static packet filtering
  – Stateful inspection
  – Application level traffic inspection engines run on top of IPv6

• Advanced security features
  – IDS/IPS?
  – DDoS Protection?
Features included in survey (cont'd)

• Network Address Translation
  – IP masquerading

• Tunneling
  – Tunnel IPv4 traffic in IPv6 packets (4to6)
  – Tunnel IPv6 traffic in IPv4 packets (6in4)

• Addition features supported
  – Flow monitoring
  – Log IPv6 traffic
  – IPsecv6
  – DHCPv6
  – RADIUS
Information Gathering: Beyond Survey Data...

• Direct vendor contact by email and telephone
  – Technical support, sales, marketing, general inquiries
  – Technical staff identified by colleagues and ICSA Labs

• 3rd party corroboration
  – Discussion with firewall administrators familiar with product
  – Discussion on firewall mailing lists

• Other corroboration
  – Review technical specifications, user and administration guides when made available

• Ultimately, 42 of 60 products included in report
IPv6 Transport

Overall
• All firewalls surveyed support IPv4 transport
• 31% of firewalls surveyed support IPv6 transport (13 of 42)

Breakdown (IPv6)
• SOHO: 32% (6 of 19)
• SMB: 34% (12 of 35)
• LE/SP: 30% (8 of 27)
IPv6 Routing

60% of firewalls surveyed participate as peers in IPv4 routing or perform neighbor discovery (35 of 42)

24% participate in IPv6 routing

Breakdown (IPv6)
- SOHO: 21% (4 of 19)
- SMB: 26% (9 of 35)
- LE/SP: 30% (8 of 27)
Static Packet Filtering

95% of firewalls surveyed provide static filtering when IPv4 is used (40 of 42)

29% provide static filtering when IPv6 is used (12 of 42)

Breakdown (IPv6)
- SOHO: 32% (6 of 19)
- SMB: 31% (11 of 35)
- LE/SP: 30% (8 of 27)
Stateful traffic inspection

90% of firewalls surveyed offer stateful inspection when IPv4 is used (38 of 42)

24% of products do so when IPv6 is used

Breakdown (IPv6)
- SOHO: 21% (4 of 19)
- SMB: 23%, (8 of 35)
- LE/SP: 26% (7 of 27)
Application Level Inspection

81% products across all market segments offer Application Level inspection when IPv4 is used (34 of 42)

17% when IPv6 is used

Breakdown (IPv6)
- SOHO: 3 out of 19 (16%)
- SMB: 6 out of 35 (17%)
- LE/SP: 5 out of 27 (19%)

[Note: This question covers a broad swath of features. Subsequent studies should inquire about specific features]
76% of surveyed firewalls provide IDS/IPS when IPv4 is used (32 of 42)

14% of products provide IDS/IPS when IPv6 is used (6 of 42)

Breakdown (IPv6)
- SOHO: 1 out of 19 (5%)
- SMB: 5 out of 35 (14%)
- LE/SP: 2 out of 27 (22%)

5% availability of IDS/IPS among SOHO products when IPv6 transport is used biases result
This result does not include commercial appliances that are "IDS/IPS only".
DDoS Protection

76% of surveyed firewalls provide IDS/IPS when IPv4 is used (34 of 42)

21% of products provide IDS/IPS when IPv6 is used (9 of 42)

Breakdown (IPv6)
- SOHO: 4 out of 19 (21%)
- SMB: 8 out of 35 (23%)
- LE/SP: 7 out of 27 (26%)
14% of products surveyed are able to tunnel IPv4 traffic in IPv6 transport

29% of products are able to encapsulate IPv6 traffic in IPv4 tunnels
IPv6 Transport support (Market Leaders)

- Commercial firewall market dominated by small number of vendors

- Availability of IPv6 transport support improves when consumer choice is narrowed to the market leaders

- Sophisticated traffic inspection and advanced security features are still not prevalent
Additional Observations

• Generally, if a product supports IP transport and traffic inspection, that product
  – logs IP level events (true for IPv4 and IPv6 transport).
  – supports IPsec (true for IPv4 and IPv6 transport).

• Few firewall products support DHCPv6, RADIUS, and flow monitoring when IPv6 transport is used.
  – Inconsistent reporting on these features
Observations from Vendor Comments

• IPsecv6 support is not as fully-featured as IPv4
  – some vendors support fewer Internet Key Exchange (IKE) peer
    authentication options, or only support manual keying

• User Interfaces are not as robust
  – IPV6 transport can only be configured using a command line
    interface.

• IDS and DDoS support not as robust
  – Signature sets for IDS/IPS inspection engines for IPv6 not as
    extensive as sets for IPv4.
  – Number and kinds of DoS attacks they can detect and block
    are fewer when IPv6 transport is used.
"Why no support?"

• Vendors who responded that they had no IPv6 support typically claimed that they have received few if any requests for products that support IPv6.
Conclusions

• Support for IPv6 transport and security services is available from commercial firewalls for all market segments

• Firewall products that support IPv6 transport generally provide (some form of traffic inspection), event logging, and IP Security (IPsecv6)

• Availability of advanced security features is lagging in SOHO and SMB segments and strongest in the LE/SP segment.
Conclusions

- IP version 6 (IPv6) transport is not broadly supported by commercial firewalls.
- Across all market segments, less than one in three products support IPv6 transport and security features.
  - Support among the firewall market share leaders improves this figure somewhat
- Can we extrapolate from these results? "Are we prepared to deploy IPv6"?