DAVID PISCITELLO

are commercial firewalls ready for IP version 6?

Dave Piscitello is a Senior Security Technologist for ICANN. A 30-year Internet veteran, Dave currently serves on ICANN's Security and Stability Advisory Committee.

dave.piscitello@icann.org

THE DEPLETION RATE OF THE IP VERsion 4 (IPv4) address space has been the subject of considerable analysis and even greater speculation for nearly 15 years. However, Network Address Translation [1, 2] and classless inter-domain routing (CIDR [3]) have extended the lifespan of the IPv4 address space beyond many projected exhaustion dates. Today, many organizations still choose to dismiss experts who voice IPv4 addressing concerns as modern-day "boys who cry wolf." Whether we are perilously close to the day when ignoring the cries will prove fatal to the flock remains an open question. Assuming that exhaustion of the IPv4 address space is imminent, we consider whether the community will be able to secure networks when we are left with little choice but to deploy IPv4's successor, Internet Protocol version 6.

IPv4 Lifetime Projections

In 2005, Tony Hain of Cisco Systems applied several mathematical models to project IPv4 address lifetime [4] (see Figures 1 and 2) and concludes, "Depending on the model chosen, the nonlinear historical trends . . . covering the last 5- and 10-year data show that the remaining 64 /8s will be allocated somewhere between 2009 and 2016, with no change in policy."

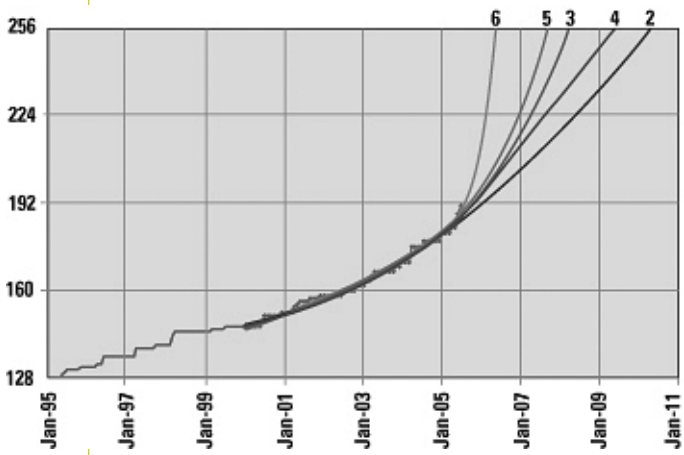


FIGURE 1: IPV4 LIFETIME PROJECTIONS FOR ORDER-N POLYNOMIALS, POST-2000 HISTORY BASIS

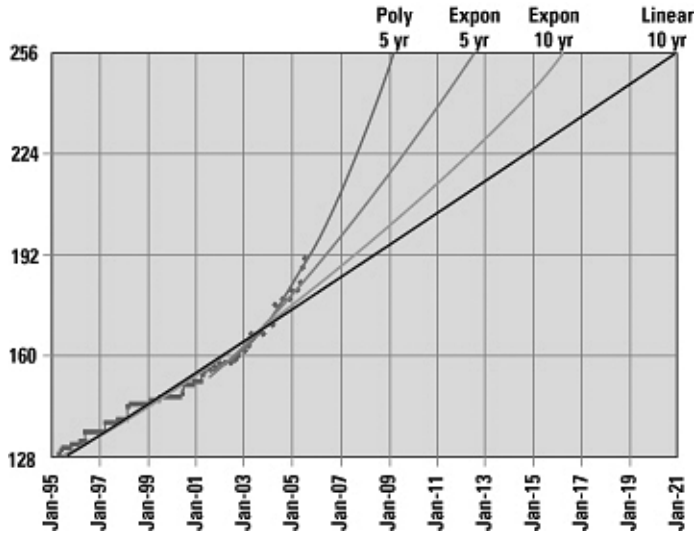


FIGURE 2: IPV4 LIFETIME PROJECTIONS FOR POLYNOMIALS AND EXPONENTIALS

These projections appear to be spot on; in particular, Geoff Huston, a respected authority on IPv4 routing and addressing, offered that "these different predictive approaches yield slightly different outcomes, but not beyond any reasonable error margin for predictions of this nature. Sometime in the forthcoming 5 to 10 years the current address distribution policy framework for IPv4 will no longer be sustainable for the current industry address consumption model because of effective exhaustion of the unallocated address pool." (Bear in mind that his comments were offered in 2005.) The Cooperative Association for Internet Data Analysis (CAIDA) has an equally sobering projection: "If current consumption rates continue unchanged (a wholly unwarranted assumption) and little of the already allocated space is ever reclaimed (a realistic assumption), then Internet Assigned Numbers Authority's (IANA) unallocated IPv4 pool and currently reserved spaces would run dry in March 2009"[5].

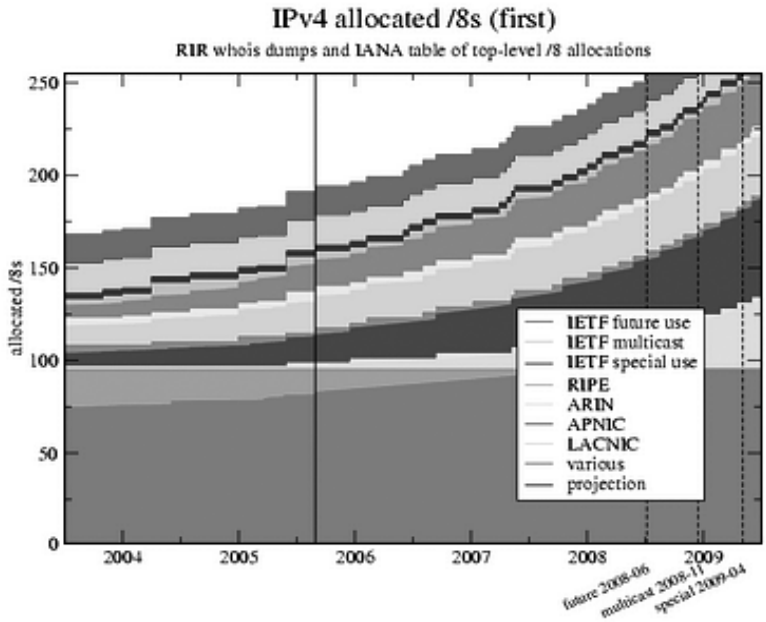


FIGURE 3: ALLOCATED IPV4 ADDRESS SPACE

If you doubt the accuracy of these claims, look at the allocation of IPv4 address space as of 28 October 2007 [6] (see Figure 3). Regional Internet registries (RIRs) are struggling to allocate contiguous address blocks of sufficient size to service providers. Proposals to reclaim unused (or "hoarded," as some claim) IPv4 address space remain nonstarters for operational and legal reasons; for example, attempts to use the RFC 1700 experimental space (known as Class E addresses) will prove problematic for some IPv4 implementations, and there is no legal basis for recovering previously allocated address space. More important, if the projections are accurate, reclamation will not happen fast enough to have an impact.

The only practical way forward is to deploy IP version 6. Claims that IPv6 adds nothing that has not been added to IPv4 notwithstanding, the one indisputable fact about the next-generation Internet Protocol is that it does provide more address space. But at what cost? IPv6 standards and implementations are available, but they are little used, and little is known about the availability of security products and services. Will relieving the addressing problem put organizations in a position where they will not be able to provide the same security baseline for IPv6 networks that they currently are able to do for IPv4 networks?

A security baseline encompasses many policies, practices, operations, and technologies. Any thorough analysis would undoubtedly span multiple studies, involve detailed product testing, and require considerable resources. However, a survey that limits the scope of the question to "Can a commonly deployed security product provide the same breadth of security policy enforcement for IPv6 networks as it does for IPv4 networks?" may provide a useful reference point for the Internet community.

ICANN's Security and Stability Advisory Committee (SSAC) considered candidate security systems for such a study and concluded that Internet firewalls would serve the purpose well. Firewalls are among the oldest and most commonly employed security technologies and are still considered critical components of security deployment. Thus, we should be able to gain meaningful insight into the state of IPv6 readiness of the Internet security industry by studying firewalls.

Methodology

We compiled a list of commercial firewall vendors to survey using search engines, portals that list security products and vendors (e.g., network intrusion [7] and Rik Farrow's firewall product selector [8]), and contact lists compiled by ICSA Labs [9]. This survey only includes commercial firewall products and in particular does not include personal firewall software or open source firewall libraries that could be installed and configured on PC and server platforms. The survey also excludes broadband access routers that only provide rudimentary firewall features. We collected information to identify the features we would survey using vendor publications (Web sites, white papers, product specifications, and administrative and user manuals). To further shape the survey, we consulted with firewall administrators and security experts for additional input. Ultimately, we chose to include both networking and security features that we believe to be commonly used at firewalls to enforce security policy in IPv4 networks, and we agreed that it would be useful to study security feature availability according to three market segments: small office/home office (SOHO), small and medium business (SMB), and large enterprise/service provider (LE/SP). Finally, we chose to

keep the number of survey questions small and the degree of technical specificity low, with the expectation that this would increase our response rate.

We contacted firewall vendors using general contact email addresses and telephone numbers. We also solicited direct technical contact information from firewall vendors by posting a general inquiry to popular firewall and security mailing lists (e.g., bugtraq@securityfocus.com, pen-test@securityfocus.com, firewall-wizards@listserv.icsalabs.com). We corroborated vendor responses by contacting multiple parties within each company, experts at large, colleagues at reputable testing laboratories, or firewall administrators. Whenever available, we consulted vendor documentation (e.g., configuration and administration guides that were accessible via a vendor's technical support Web portal).

It is important to note that we did not conduct formal testing of any product included in this survey. Our objective was to gauge feature availability, not to qualify or certify any product as being IPv6 "security capable." We relied on the accuracy of available documentation, the expertise of administrators we consulted, and, ultimately, on vendor contacts acting in good faith. We have no reason to believe that any party contacted misrepresented IPv6 feature availability to us; in fact, the majority of correspondence was earnest and involved numerous dialogues beyond the initial survey query and response: Overall, vendors were eager for input that helps prioritize product development or shapes an opportunity for expanding market share and were eager to cooperate.

Survey Results

We obtained survey responses and compiled complementary information for 42 of 60 products from commercial firewall vendors. Several vendors identified a single product as satisfying multiple market segments, resulting in 81 product placements across the three defined market segments. Specifically, 19 results were collected for SOHO products, 35 for SMB products, and 27 for the LE/SP market. In this article, we present a subset of the results. Complete details are available in SAC 021, "Survey of IPv6 Support in Commercial Firewalls" [10].

[Note: In the charts, we label the bars representing these respondents with ALL, SOHO, SMB, and LE/SP based on the unique totals for each segment (i.e., percentages are based on 42, 19, 35, and 27, respectively).]

How broadly are IPv6 transport and routing supported by commercial firewalls?

Many organizations will be able to obtain ample IPv6 address space [11] and will want to take advantage of autoconfiguration and other IPv6 addressing features. Firewalls in such deployments must be able to forward IPv6 traffic between internal and external interfaces. (Note that the ability to encapsulate IPv4 datagrams arriving from internal networks as payloads in IPv6 datagrams and forward these to IPv6 destinations is considered separately in the full report; see [10].) All firewalls surveyed support IPv4 transport. Figure 4 illustrates that IPv6 transport is supported in fewer than one in three of the firewalls surveyed.

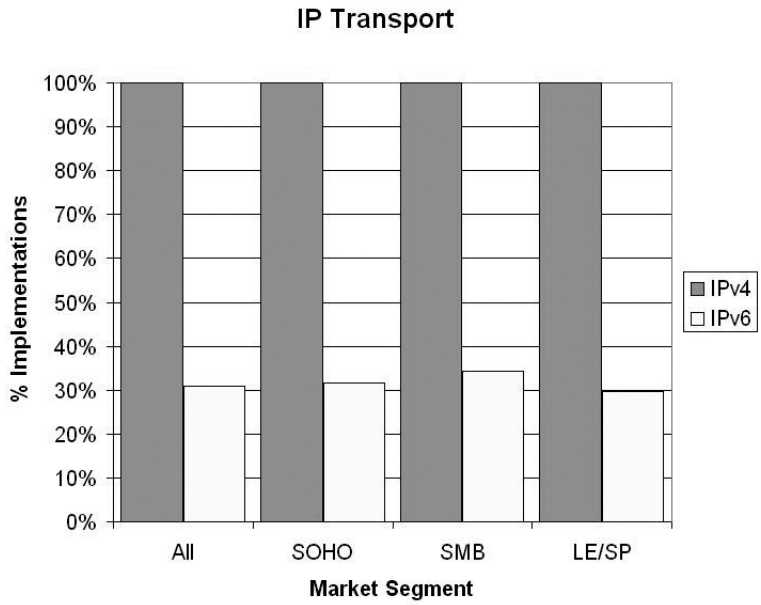


FIGURE 4. FIREWALL SUPPORT FOR IPV4 AND IPV6 TRANSPORT

Firewall systems (as opposed to routers that support certain firewall features) are often used in complex topologies that are designed to satisfy an organization's redundancy, failover, and high-availability needs. Such organizations may run firewalls in transparent or bridging mode, or they may choose to have the firewall participate as a peer in an adaptive routing or neighbor discovery protocol. Figure 5 illustrates support for neighbor discovery and peer routing protocols.

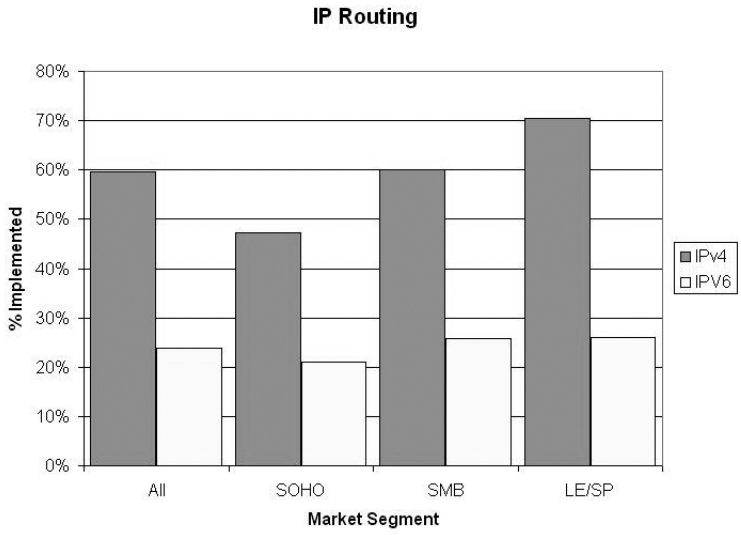


FIGURE 5. FIREWALL SUPPORT FOR IPV4 AND IPV6 ROUTING

Sixty percent of the 42 firewall products surveyed can peer in IPv4 routing exchanges or perform neighbor discovery, but only 24% can peer when IPv6 is used. The results suggest that an organization would have limited choices if it intended to include a firewall in a topology where adaptive recovery from link failure is required. As one might expect, little support exists among SOHO products that are typically deployed in single and "stub" networking topologies.

What types of IPv6 traffic inspection and policy enforcement are available on commercial firewalls?

Commercial firewalls are commonly used to enforce a security policy on traffic that passes between an organization's internal networks and external networks. Three forms of traffic inspection are available when IPv4 transport is used: static packet filtering, stateful packet inspection, and application-layer inspection. We surveyed these individually.

Static packet filtering is the most basic form of security policy enforcement firewalls provide; it is used even when more advanced inspection methods are available (e.g., to enforce a policy on a new protocol or application). This method inspects each arriving IP packet individually. If the packet complies with the security policy, it is allowed to pass through the firewall; if not, it is typically blocked and (silently) discarded.

Ninety-five percent of the commercial firewalls surveyed provide static packet filtering in all market segments when IPv4 transport is used. Twenty-nine percent provide static filtering when IPv6 transport is used (see Figure 6).

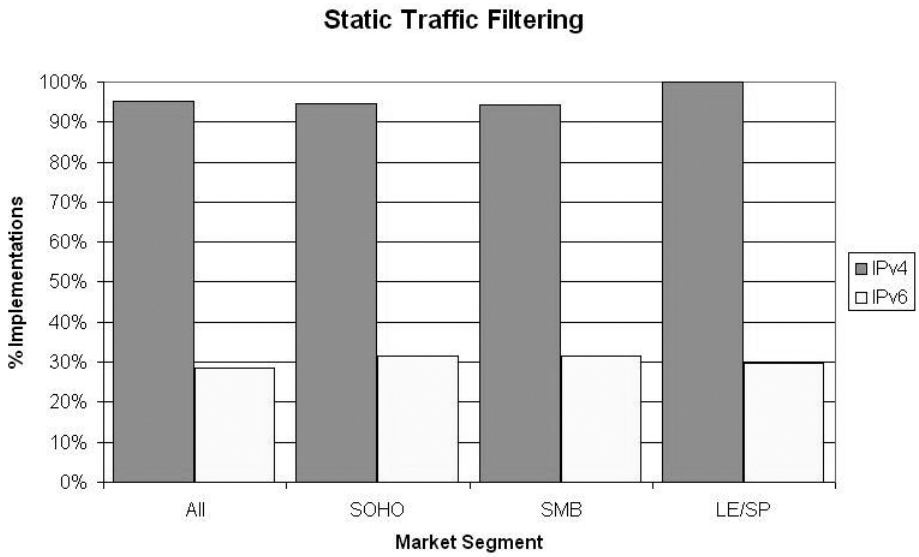


FIGURE 6. FIREWALL SUPPORT FOR IPV4 AND IPV6 STATIC PACKET FILTERING

Stateful inspection of IP layer packets is a more advanced form of security policy enforcement. Stateful inspection considers all IP datagram payloads associated with a given TCP connection, UDP stream, or application datum and enforces a policy on multipacket and complete traffic flows. Ninety percent of commercial firewall products surveyed provide stateful inspection when IPv4 transport is used, whereas only 23% do so when IPv6 transport is used (see Figure 7). (Note that firewalls capable of supporting stateful packet inspection typically support static packet filtering, and this appears to be true for both IPv4 and IPv6. We also observed from the results that if a product supports IP transport and one or more forms of traffic inspection, that product supports IPsec for IPv4 and IPv6 transport. These observations are discussed in some detail in [10].)

FIGURE 7. FIREWALL SUPPORT FOR IPV4 AND IPV6 STATEFUL INSPECTION

Increasingly, organizations expect firewalls to protect Web, email, DNS, and other Internet servers and clients from exploitation and privilege escalation attacks. Firewall vendors use application-layer gateways (proxies) or stateful traffic inspection techniques to detect and block malicious traffic that can cause an application or system to fail, respond incorrectly, disclose sensitive data, or allow unauthorized parties to gain administrative control over a system. In the survey, we were agnostic about the method used and simply asked whether vendors provide application-level inspection.

Eighty-one percent of commercial firewalls surveyed can apply stateful inspection or proxy techniques to application -level traffic when IPv4 transport is used, but only 17% are able to do so when IPv6 transport is used (see Figure 8).

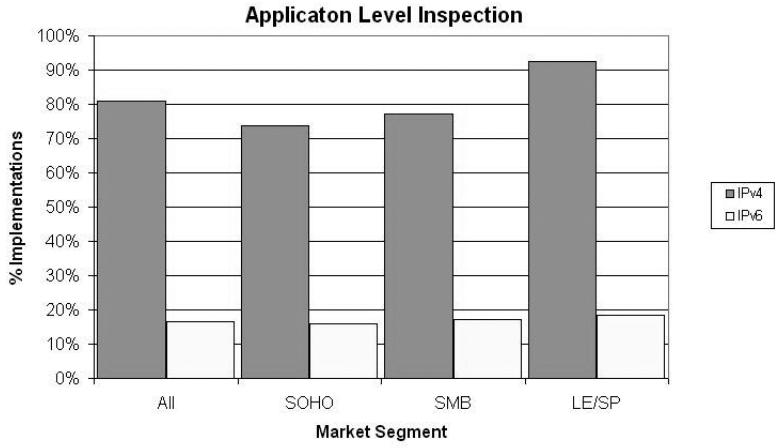
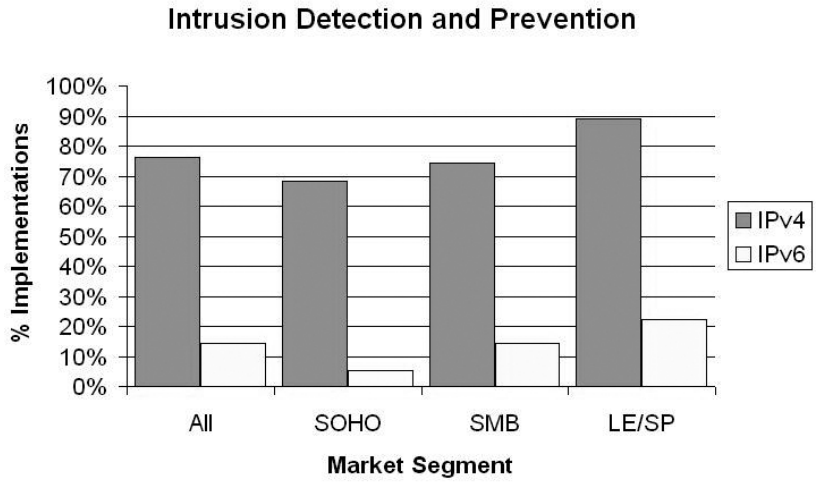


FIGURE 8. FIREWALL SUPPORT FOR IPV4 AND IPV6 APPLICATION-LEVEL INSPECTION

Do commercial firewalls provide intrusion detection or intrusion prevention when IPv6 transport is used?

Firewalls are in-line devices and are designed to detect and prevent attacks by blocking traffic or stripping objectionable content prior to forwarding traffic to a destination. Certain commercial firewalls incorporate detection and mitigation techniques to protect an organization from sophisticated



network, transport, and application attacks ("intrusions"). These firewalls may provide one or combinations of signature- and anomaly-based detection methods as adjunct services to the three forms of traffic inspection described earlier.

FIGURE 9. INTRUSION DETECTION AND PREVENTION SERVICES

Figure 9 shows that 76% of commercial firewall products surveyed provide some form of intrusion detection or prevention when IPv4 transport is used. Only 14% offer IDS/IPS when IPv6 transport is used. We note that some vendors commented that the signature sets for IDS/IPS inspection engines for IPv6 were not as extensive as the signature sets for IPv4. (The very low availability of IDS/IPS among SOHO products biases this result. The survey result for LE/SP products is perhaps a more accurate representation of IDS/IPS availability when IPv6 transport is used for organizations that require such features.)

Do commercial firewalls provide (distributed) denial-of-service protection when IPv6 transport is used?

Flooding forms of denial-of-service (DoS) attacks attempt to exhaust the resources of a targeted application, system, or network and thus deny service to users. Whereas exploitation attacks can deny service to users, flooding attacks are familiar to most Internet users and thus represent a marketing opportunity. For this reason, we chose to survey protection against flooding separately from IDS/IPS. A higher percentage of commercial firewalls offer some form of rate-limiting when DoS and DDoS attacks are detected than offer IDS/IPS protection when IPv6 transport is used, but generally support is still relatively weak (see Figure 10). We note that some vendors indicated that DoS protection is not as comprehensive when IPv6 transport was used (i.e., fewer kinds of DoS attacks are mitigated or reduced).

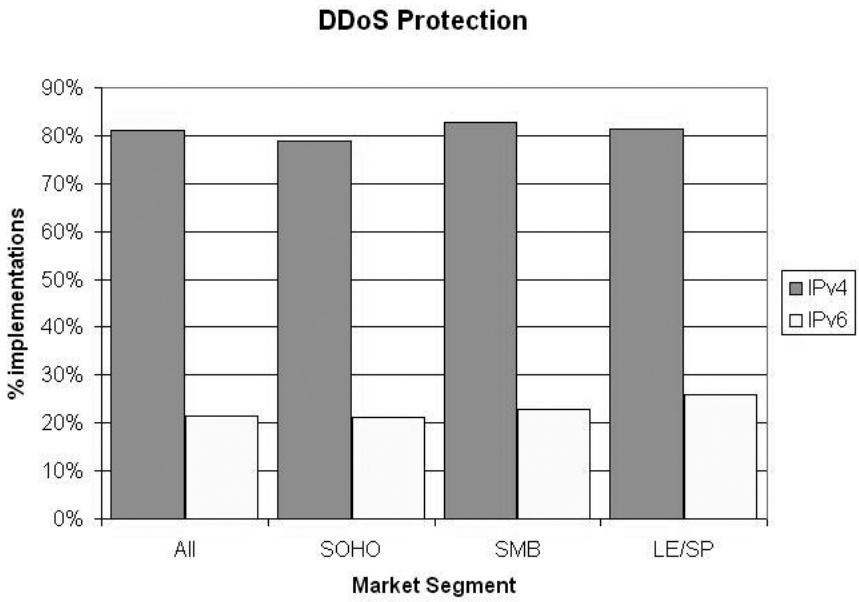


FIGURE 10: DDOS PROTECTION

Conclusions

IP version 6 transport is not broadly supported by commercial firewalls. If organizations attempt to "go native IPv6" today, they will be limited to choosing among the 31% of the firewall products surveyed that support IPv6 transport. We do note, however, that although fewer than one in three products support IPv6 transport and a desirable set of security features, support among the firewall market share leaders improves this figure somewhat. This observation is consistent with recent *Network World* product testing conducted by Dr. Joel Snyder [12].

We find the limited support for IPv6 stateful packet inspection across the commercial firewall product sector quite worrisome. Many vendors extend stateful packet inspection techniques to provide additional application-level protection measures. We also find another cause for concern in the limited availability of IPv6 support at the "periphery" of the Internet. Support for advanced security features is weakest in SOHO and SMB segments, although we did not include broadband access devices that claim firewall capabilities in our survey. Such devices have very little, if any, firewall capability beyond static packet filtering. We speculate that support is no stronger in the broadband market than in SOHO, and we speculate further that if we had included such devices, the overall results of IPv6 support among commercial firewall and "router/firewall" products would have been even more discouraging.

We conclude by quoting from our report:

> Internet firewalls are the most widely employed infrastructure security technology today. With nearly two decades of deployment and evolution, firewalls are also the most mature security technology used in the Internet. They are, however, one of many security technologies commonly used by Internet-enabled and security-aware organizations to mitigate Internet attacks and threats. This survey cannot definitively answer the question, "Can an organization that uses IPv6 transport enforce a security policy at a firewall that is commensurate to a policy currently supported when IPv4 transport is used?" The survey results do suggest that an organization that

adopts IPv6 today may not be able to duplicate IPv4 security feature and policy support.

A comment we heard all too frequently and from altogether too many commercial firewall vendors during our study was, "No one's asking for IPv6." Markets can turn quickly, but not overnight. If we begin asking commercial firewall vendors *soon* we might expect the availability of IPv6 support to improve within the next 9–18 months. If the available IPv4 address pool evaporates faster, some organizations may experience difficulties satisfying security policies with the commercial firewalls they currently employ.

REFERENCES

[1] RFC 1631, The IP Network Address Translator (NAT), K. Egevang and P. Francis: http://www.faqs.org/rfcs/rfc1631.html.

[2] RFC 2663, NAT Terminology and Considerations, P. Srisuresh and M. Holdrege: http://www.faqs.org/rfcs/rfc2663.html.

[3] RFC 1519, Classless Inter-Domain Routing (CIDR), V. Fuller, T. Li, J. Yu, and K. Varadhan: http://www.faqs.org/rfcs/rfc1519.html.

[4] Reprinted from T. Hain, "A Pragmatic Report on IPv4 Address Space Consumption," *The Internet Protocol Journal*, 8, 3. *IPJ* is a quarterly technical journal published by Cisco Systems. See http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_8-3/ipv4.html.

[5] IPv4 Consumption: http://www.caida.org/research/id-consumption/ipv4/.

[6] Internet Protocol v4 Address Space: http://www.iana.org/assignments/ipv4-address-space.

[7] Computer Network Defense, Ltd., Talisker firewalls overview page: http://networkintrusion.co.uk/firewall.htm.

[8] Rik Farrow's firewall product tester page: http://www.spirit.com/cgi-new/report.pl?dbase=fw&function=view.

[9] ICSA Labs certified firewalls list: http://www.icsalabs.com/icsa/product.php?tid=fghhf456fgh.

[10] SAC 021, Survey of IPv6 Support in Commercial Firewalls: http://www.icann.org/committees/security/sac021.pdf.

[11] Guidelines—Initial IPv6 Allocation from ARIN: http://www.arin.net/registration/guidelines/ipv6_initial_alloc.html.

[12] UTM and IPv6: Do they mix? J. Snyder: http://www.networkworld.com/reviews/2007/111207-utm-firewall-test-ipv6.html?nwwpkg=utm.