SAC 021
Survey of IPv6 Support in Commercial Firewalls

A Report from the ICANN
Security and Stability
Advisory Committee
(SSAC)
October 2007

About the Security and Stability Advisory Committee

The Security and Stability Advisory Committee (SSAC) is an advisory committee to the Internet Corporation for Assigned Names and Numbers (ICANN). The Committee's purpose is to offer independent advice to the ICANN board, the ICANN staff and the various ICANN supporting organizations, councils and committees as well as to the technical community at large on matters relating to the security and integrity of the Internet's naming and address allocation systems. The Committee has no official authority to regulate, enforce or adjudicate. Those functions belong to others. The advice offered by the Committee should be evaluated on its merits, not on the status of the Committee or its members.

About this Report

This report was prepared by the SSAC Fellow, Dave Piscitello, under the direction of Stephen Crocker. The SSAC Fellow designed and executed the survey; the Committee reviewed and approved the work. The report represents output from the committee as a whole. Appendix A contains the current list of members and contributors to this report.

Executive Summary

This report surveys the commercial firewall market for IPv6 security service availability. The report attempts to answer the following questions:

1. How broadly is IP version 6 (IPv6) transport supported by commercial firewalls?

2. Is support for IPv6 transport and security services available from commercial firewalls available for all market segments - home and small office (SOHO), small-to-medium business (SMB), large enterprise and service provider networks (LE/SP) – or is availability lagging in certain segments?

3. Among the security services most commonly used at Internet firewalls to enforce an organization's security policy, which are available when IPv6 transport is used?

4. Can an organization that uses IPv6 transport enforce a security policy at a firewall that is commensurate to a policy supported when IPv4 transport is used?

For this survey, commercial firewall vendors were contacted and asked to complete a survey regarding IPv4 and IPv6 networking and security service support in currently available products. Considerable efforts were made to contact all commercial firewall vendors; however, it is possible that some were inadvertently excluded from the list. Vendor responses were analyzed and key findings are illustrated throughout this report. This report presents all findings and statistics in an aggregated fashion. No individual vendor responses are reported. The survey results suggest that an organization that adopts IPv6 today may not be able duplicate IPv4 security feature support.

Introduction

This report surveys the commercial firewall market for IPv6 security service availability. The report attempts to answer the following questions:

1. How broadly is IP version 6 (IPv6) transport supported by commercial firewalls?

2. Is support for IPv6 transport and security services available from commercial firewalls available for all market segments - home and small office, small-to-medium business, large enterprise and service provider networks – or is availability lagging for certain segments ?

3. Among the security services most commonly used at Internet firewalls to enforce an organization's security policy, which are available when IPv6 transport is used?

4. 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 report presents the results of an industry survey conducted by the SSAC Fellow from June – September 2007. Only commercial firewall products commonly used to enforce a security policy are included; specifically, we do not include personal firewalls for popular commercial operating systems, nor do we include open source firewalls that could be installed on Intel-based computer systems and deployed as Internet firewalls.

Commercial firewall vendors were contacted and asked to complete a survey regarding IPv6 networking and security service support in currently available products. The survey listed security features that are commonly used to enforce security policy in IPv4 networks. The survey asked vendors to state which features are also supported by their products when IPv6 network layer is used.

A complete list of vendors contacted, along with a list of those that responded, is provided as Appendix A of this report. Considerable efforts were made to contact all commercial firewall vendors of which the author was aware; however, it is possible that some were inadvertently excluded from the list. Readers familiar with the commercial firewall market should concur with SSAC's estimation that firewalls representing in excess of 95% of the installed base of commercial firewalls are included in this study.

Vendor responses were analyzed and key findings are illustrated throughout this report. This report presents all findings and statistics in an aggregated fashion. No individual vendor responses are reported. Publication of such responses could be construed as an endorsement or disapproval of a vendor or product, which is outside the scope of SSAC's study.

SSAC bases its findings on what firewall vendors reported in their responses to the survey questions. SSAC has not performed any formal testing to confirm that a firewall performs as its vendor reported. Such testing is beyond SSAC's scope. SSAC did attempt to

corroborate vendor claims by contacting knowledgeable third parties in cases where the committee received multiple, conflicting or incomplete information from a vendor. Where available, the Fellow reviewed administrative and user documentation available for firewall products; in particular, technical specifications and user guides were the primary source for determining security feature support when IPv4 transport is used and for compiling the list of features included in the survey. The efforts to corroborate what vendors reported do not provide the same empirical results that formal testing might; however, they provide the committee with a greater measure of confidence that vendors responded accurately and honestly to the survey questions.

Background: Why perform this study, now?

SSAC elected to study the availability of security services support for IPv6 networks following a presentation during an open session at the July 2007 ICANN Public Meeting in San Juan Puerto Rico. In that presentation, Ray Plzak, CEO of ARIN, described the accelerated depletion rate of IPv4 addresses and the growing difficulties the Regional Internet Registries (RIRs) are experiencing in allocating contiguous address blocks of sufficient size to service providers. Mr. Plzak also described how fragmentation in the IPv4 address space is taxing and stressing the global routing fabric, and how the RIRs will impose more restrictive IPv4 allocation policies and promote a rapid adoption of IPv6 addresses. SSAC members took note of anecdotal observations that organizations may not be able to achieve the same security baseline for IPv6 networks as they are currently able to achieve for IPv4 networks. Noting that no formal study had been recently conducted to assess the availability of security services for IPv6 networks, SSAC determined to fill that void.

Methodology

SSAC composed a list of commercial vendors to survey using search engines, popular security portals that list security products and vendors (e.g., networkintrusion.com), and contact lists compiled by security product certification testing organizations. We collected information to complete the survey using vendor publications (web sites, white papers, product specifications, administrative and user manuals), vendor email responses to a survey email message, telephone conversations with sales, marketing and technical support personnel. In several cases, SSAC corresponded directly with technical staff responsible for product development.

SSAC attempted to corroborate vendor claims by contacting multiple parties in cases where the committee received conflicting or ambiguous responses. In certain cases, we contacted experts at large, colleagues at reputable testing laboratories, or firewall administrators. The SSAC fellow also consulted vendor documentation (e.g., configuration and administration guides that were accessible via a vendor's technical support web portal), where available.

SSAC contacted many vendors using general contact email addresses, e.g., addresses extracted from the general contact information vendors publish at web sites for prospective customers (`info@company.com, sales@company.com, support@company.com,`

prodinfo@company.com). This list was supplemented as often as possible with direct technical contacts. SSAC solicited direct technical contact information for a number of firewall vendors by posting a general inquiry to popular firewall and security mailing lists, (e.g., bugtraq@securityfocus.com, firewall-wizards@listserv.icsalabs.com, pen-test@securityfocus.com).

ICSA Laboratories shared technical contact information for firewall vendors who have participated in its certification programs. In most cases, ICSA staff graciously provided email introductions. These introductions proved to be invaluable in eliciting accurate responses and SSAC is indebted to ICSA for their assistance. SSAC also attempted to contact by telephone vendors who did not respond to email. Calls were initially placed to contact telephone numbers obtained from vendor web sites (general, sales, marketing, or technical support). Through these efforts, SSAC obtained survey responses and gathered complementary information for 42 of 60 products vendors identified.

The survey listed security features that SSAC believes to be commonly used at firewalls to enforce security policy in IPv4 networks. The survey asked vendors to state which features are supported by their products within a given market segment when IPv6 transport is used. The networking and security features requested in the survey are included in Table 1.

Security service or feature	Description
IPv6 transport	
- Forward IPv6 traffic	Can the product forward native IPv6 packets between internal and external (public) interfaces?
- IPv6 routing	Can the product participate in IPv6 neighbor discovery exchanges or act as a peer in IPv6 routing protocol exchanges?
Traffic filtering	
- Static packet filtering	Can the product enforce a security policy by applying a filter on individual IPv6 packets?
- Stateful inspection	Can the product enforce a security policy by applying a filter on all IPv6 packets associated with a given connection or flow?
- Proxies or inspection engines run on top of IPv6 network protocol	Can the product enforce a security policy on protocols encapsulated in IPv6 packets (e.g., ICMP, TCP/UDP, and application protocols such as HTTP, SMTP, DNS…) using either application layer gateway (proxy) or stateful inspection of application protocols and payloads?
IDS/IPS	Can the product provide intrusion detection and intrusion prevention measures on IPv6 traffic?
DDoS Protection	Can the product protect networks from IPv6, ICMP, and TCP flooding and malformed packet attacks?
Network Address Translation and Tunneling	
- IP masquerading	Can the product map IP addresses assigned to endpoints on internal networks to a single IP address on the external (public) interface (and thus prevent the disclosure of the internal network addressing and topology information)?
- 4to6	Can the product encapsulate (tunnel) IPv4 packets in IPv6 packets? This is useful when it is necessary to bridge two or more IPv4-only hosts or networks that do not use IPv6 and the only available transport between those hosts or networks is IPv6.
- 6to4	Can the product encapsulate (tunnel) IPv6 packets in IPv4 packets? This is useful when it is necessary to bridge two or more IPv6-only hosts or networks that do not use IPv4 and the only available transport between those hosts or networks is IPv4.
- Flow monitoring	Can the product monitor flows of traffic, detect and respond to known-to-be malicious or suspicious/anomalous traffic patterns?
- Log IPv6 traffic	Can the product record security events when the transport is IPv6?
- IPsecv6	Can the product support IP Security when the transport is IPv6?
- DHCPv6	Can the product support dynamic address assignment when the transport and addressing scheme is IPv6?
- RADIUS	Can the product support authentication, accounting and auditing (AAA) features in conjunction with a RADIUS-capable server when the transport is IPv6?

Table 1. Network and Security Features Surveyed for this Report

Survey Results

We present the results of the survey using charts accompanied by brief analyses. SSAC obtained survey responses and gathered complementary information for 42 of 60 vendors identified, representing an aggregate of 81 product placements across the three defined market segments analyzed. In the charts, we label the bar representing these respondents with "ALL" and calculate percentages based on a total of 42 responses. Several products were reported as serving multiple market segments (e.g., SOHO/SMB or SMB/LE/SP); specifically, 19 products were classified as serving a SOHO market, 35 as serving a SMB market, and 27 as serving a LE/SP market. In the charts, we calculate percentages for SOHO, SMB, and LE/SP based on the unique totals for each segment (19, 35, and 27, respectively).

Breadth of IPv6 Networking support among commercial firewalls

The first survey question asked was, *How broadly is IPv6 transport supported by commercial firewalls?*

Firewalls must nominally be capable of basic IPv6 traffic forwarding between internal and external interfaces, or able to accept IPv4 datagrams arriving from internal networks and hosts that are IPv4-only, encapsulating these as payloads in IPv6 datagrams, and forwarding these to IPv6 destinations (the latter feature is considered separately, see the section entitled *Availability of NAT and Tunneling*). Chart 1 illustrates the survey results:

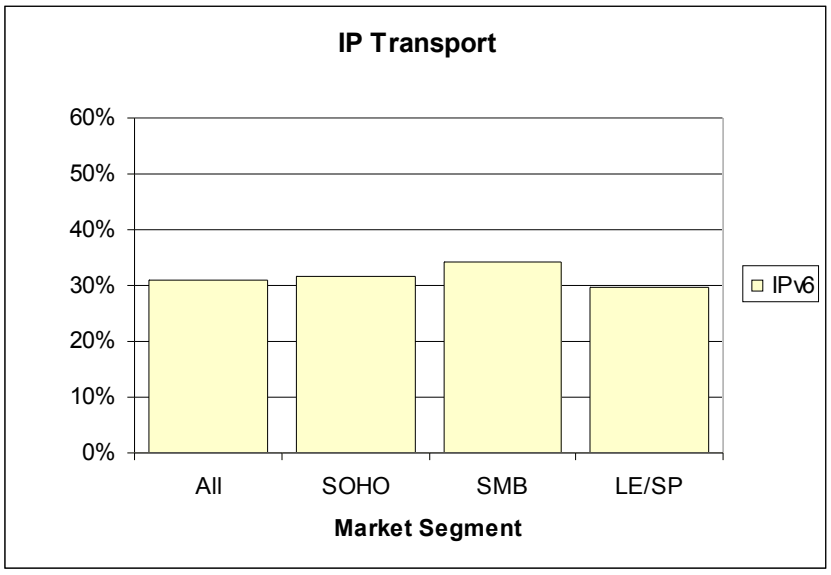


Chart 1. Firewall support, IPv4 and IPv6 transport

All firewalls surveyed support IPV4 transport. All 42 surveyed firewalls support IPv4 transport; among these, 13 (31%) support IPv6 transport. Support among SMB (12 out of 35, or 34%) products is slightly higher than among LE/SP (8 out of 27, or 30%) and SOHO products (6 out of 19, or 32%).

LE/SP firewalls, and to a lesser extent, SMB firewalls are often used in more 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. Chart 2 illustrates support for neighbor discovery and peer routing protocols.

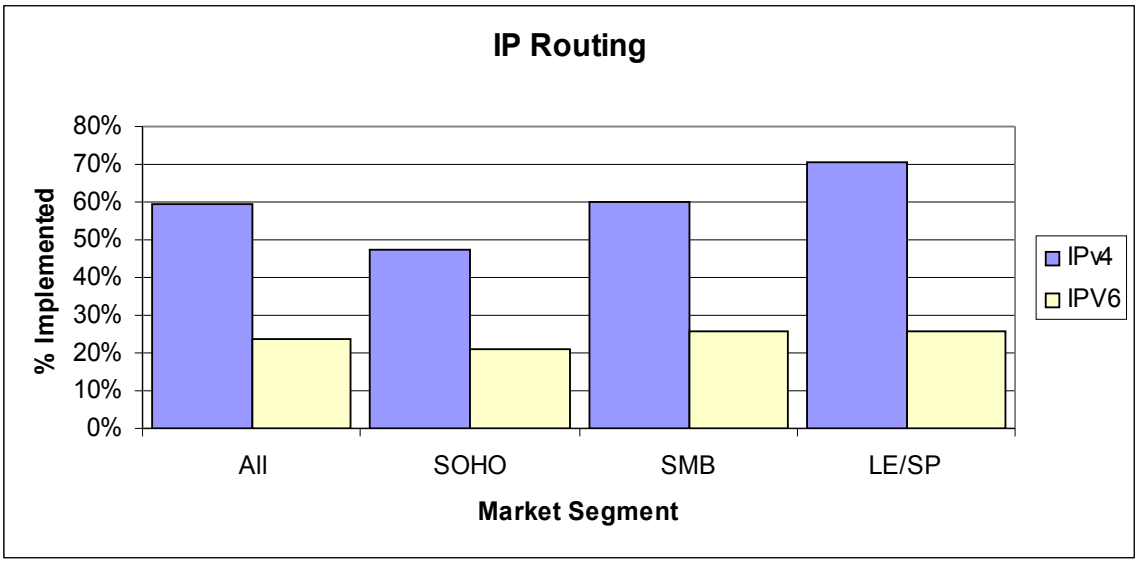


Chart 2. Firewall Support, IPv4 and IPv6 Routing

Sixty percent of all firewall products surveyed (25 of 42) are able to participate as peers in IPv4 routing exchanges or perform neighbor discovery. Only 10 of 42 (24%) are able to do so when IPv6 transport is used. The lowest number of firewalls that support IPv6 routing or neighbor discovery is found in the SOHO segment (4 out of 19, or 21%). This is expected, as most SOHO firewalls are deployed in single and "stub" networking topologies (e.g., a broadband residential or small business access circuit) and thus require minimal routing configuration (e.g., a default gateway). The percentages of firewalls that support IPv6 routing among SMB and LE/SP products surveyed (both at 26%) suggest that certain organizations could not include currently deployed firewalls as peers in IPv6 routing topologies today. These organizations would not be able to implement adaptive recovery from link failure when IPv6 transport is used as they do currently with IPv4. (Note: the survey did not ask about whether products supported high availability and failover features. This feature should be included in future studies.)

Several firewalls included in the study are classified by their vendors as a hybrid of application level firewall and intrusion prevention system for large enterprise and service provider markets. IPv6 transport and routing support is lower among these products. Adaptive routing requirements for SP/LE environments are more extensive than SOHO and SMB networks. The development cost is much higher and this may contribute to the smaller percentage.

Availability of Traffic Inspection Methods

Commercial firewalls are commonly used to enforce a security policy that controls the types of traffic that may pass between an organization's internal networks and public (external) networks. Three forms of traffic inspection are commonly available when IPv4 transport is used: static packet filtering, stateful packet inspection, and application layer inspection.

Static packet filtering is the most basic form of security policy enforcement performed at firewalls. This method examines each packet individually to determine if it complies with a policy. If the packet complies, it is allowed to pass through the firewall; if not, it is typically blocked and discarded. Chart 3 illustrates that 40 of 42 (95%) of all surveyed firewall products provide static packet filtering in all market segments when IPv4 transport is used, whereas only 29% (12 of 42) provide static filtering when IPv6 transport is used. The breakdown according to market segment shows a relatively consistent pattern of availability at this percentage: 6 out of 19 (32%) for SOHO, 11 out of 35 (31%) for SMB, and 8 out of 27 (30%) for LE/SP.

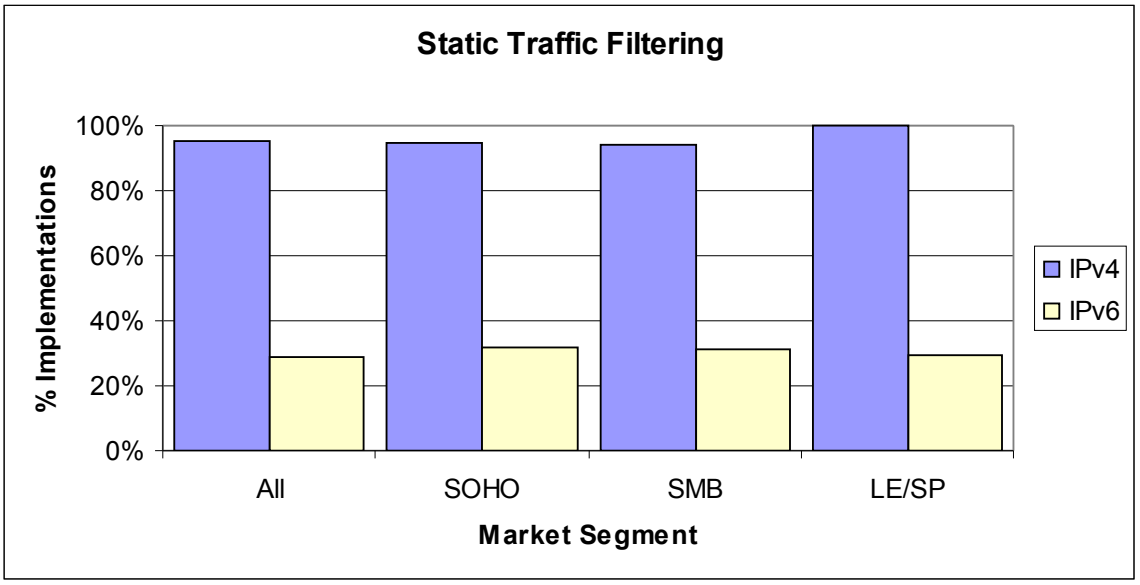


Chart 3. Firewall Support, IPv4 and IPV6 Static Packet Filtering

Stateful inspection of IP layer packets is a more sophisticated, more effective, and hence more desirable form of security policy enforcement. Stateful inspection considers all IP datagram payloads associated with a given TCP connection, UDP stream, etc. and is capable of applying packet filtering policy more accurately onto complete traffic flows. Chart 4 illustrates that 38 of 42 (90%) of all firewall products surveyed provide stateful inspection when IPv4 transport is used, whereas only 10 of 42 (24%) do so when IPv6 transport is used. This is a marked difference and is not strongly biased by any one segment: 4 out of 19 (21%) for SOHO, 8 out of 35 (23%) for SMB, and 7 out of 27 (26%). The limited support for this important firewall feature when IPv6 transport is used is significant; especially when one considers that many vendors extend stateful packet inspection techniques to provide additional application level protection measures.

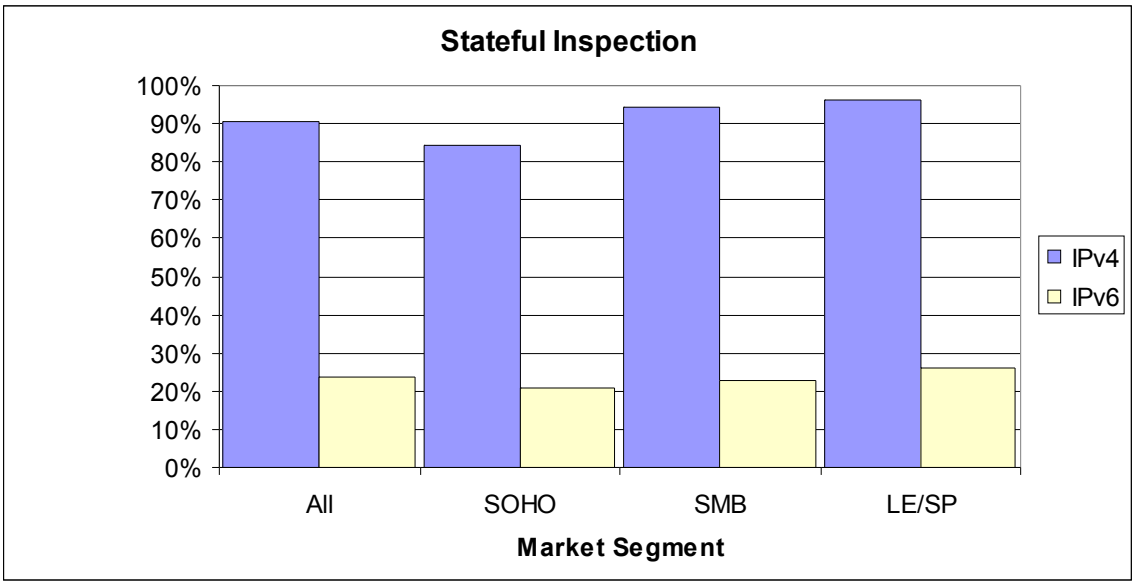


Chart 4. Firewall Support, IPv4 and IPv6 Stateful Inspection

The third form of traffic inspection, *application level protection*, merits additional discussion and context for readers unfamiliar with firewall evolution. Historically, attackers focused on vulnerabilities of commercial operating system and server applications. OS and server application software vendors have, over time, learned to mitigate vulnerabilities and distribute patches in an arguably reasonable time frame following disclosure of the problem or actual exploitation of the vulnerability. In parallel, organizations became more proficient in defending networks against the IP and transport level attacks that were commonly attempted against commercial OSs.

In response, and in no small part due to the adoption of the World Wide Web, attackers devote considerable attention to web-based applications that support messaging services and streaming media, and that provide access to databases, mission critical business applications, and infrastructure servers (e.g., DNS and mail). Attackers also target end users more aggressively today than ever before, and devise attacks that apply social engineering techniques via content delivered to client applications (e.g., phishing, worm, and spyware delivered via email, browser, and instant messaging applications).

Organizations have responded by deploying firewalls that offer *application layer inspection features* that protect web, email, DNS, and other Internet servers and clients from exploitation attacks. Certain firewall vendors provide application layer security features using application layer gateways (also called proxies). Other vendors extend stateful inspection to encompass application protocols and payloads as well as network and transport level protocols. In the survey, SSAC asked whether vendors provide either capability. Chart 5 illustrates the results.

Chart 5 illustrates that support for application layer gateway or stateful inspection of application level traffic is found in approximately 34 of 42 (81%) products across all

market segments when IPv4 transport is used, but in only 7 out of 42 (17%) when IPv6 transport is used. This is again a marked difference and is not strongly biased by any one segment: 3 out of 19 (16%) for SOHO, 6 out of 35 (17%) for SMB, and 5 out of 27 (19%) for LE/SP.

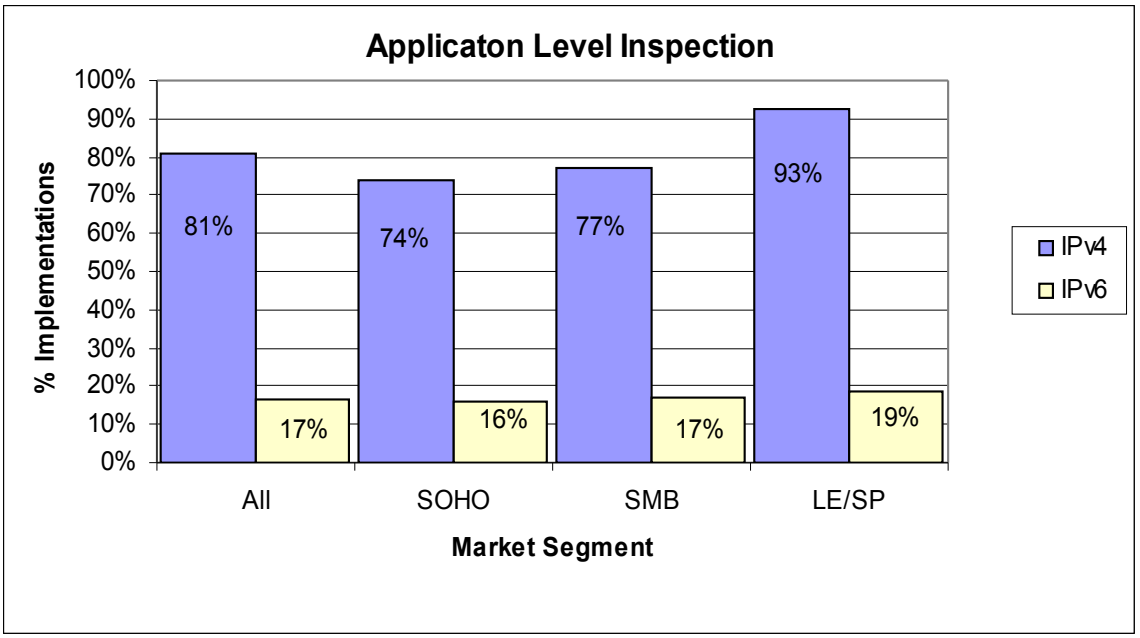


Chart 5. Firewall Support, IPv4 and IPv6 Application Level Inspection

This survey result merits additional comment. Application level protection is a terribly overloaded term. Without enumerating a particular set of application level security requirements, vendors of SOHO may have responded affirmatively based on the presence of a single feature such as content blocking based on a URL blacklist, whereas LE/SP vendors may have interpreted the question as a request for sophisticated application attack detection features intended to protect web and other application servers. The latter features are atypical requirements for SOHO networks, where hosting services is the exception rather than the norm. The survey results for LE/SP products are perhaps a more accurate measure of the availability of products that provide application level protection for organizations that require such features. But even in this segment, support when IPv6 transport is used is low.

Advanced Security Features: Intrusion and DoS Protection

Commercial firewalls are also used to protect an organization from network, transport, and application level exploitation and flooding attacks. *Exploitation attacks* use maliciously crafted packets and traffic streams to identify an exploit a flaw in the programming logic of a targeted application and cause the application to fail (cease operation) or respond in an unintended manner; in particular, attackers use exploitation attacks with the expectation that the application will somehow provide them with a means to take administrative control of the attacked system. Such attacks are called *escalated privilege attacks*. Once an attacker gains administrative control of a system, the attacker may install malicious executables that can communicate back to an attacker's *command and control system* (C&C). The C&C can order remotely controlled systems to perform virtually any service (host a web server, send

spam, etc.). Exploitation and attacks resulting from "gaining root" on exploited or compromised systems are examples of host and network intrusions. Firewalls that provide Intrusion Detection and Prevention Systems (IDS/IPS) are able to detect and block many kinds of exploitation attacks.

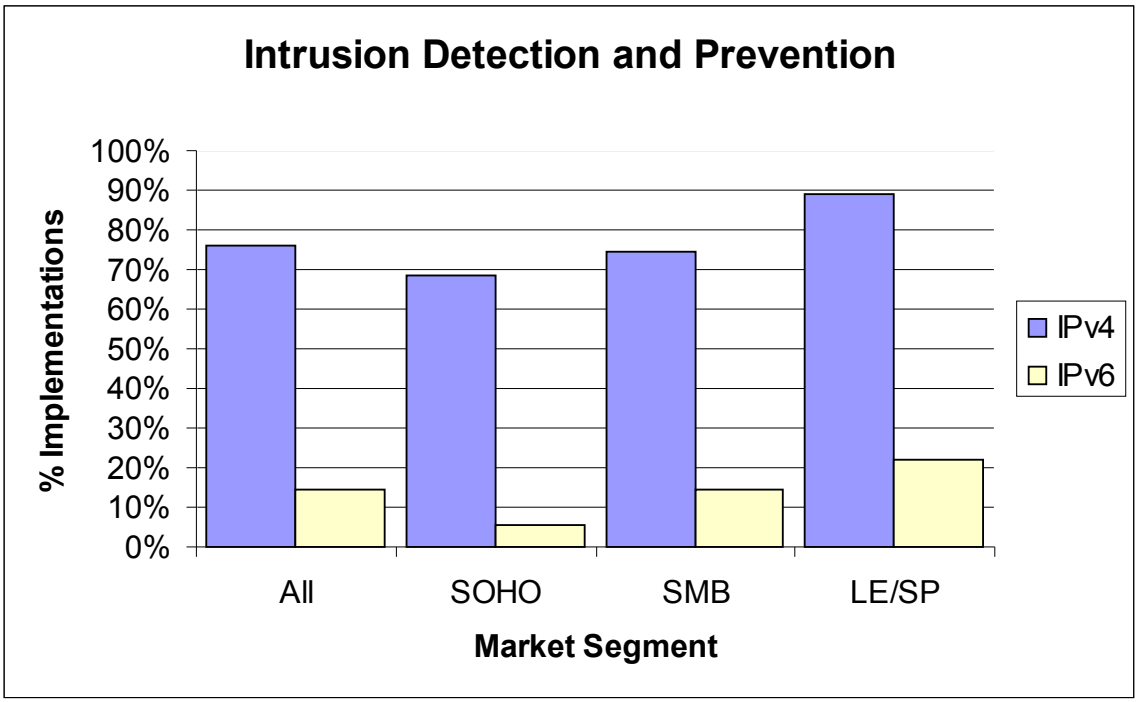


Chart 6. Intrusion Detection and Prevention Services

Chart 6 illustrates that 32 out of 42 (76%) of all firewall products surveyed provide IDS/IPS when IPv4 transport is used, compared to 14% of products when IPv6 transport is used. This survey result is significantly biased by the availability of IDS/IPS among SOHO products when IPv6 transport is used (1 out of 19, or 5%). IDS/IPS features are not commonly available on SOHO products even when IPv4 transport is used (although this market segment is growing in response to the continued increase in viruses, worms, spyware and other malicious code incidents). The survey results for SMB and LE/SP products – 5 out of 35 (14%) and 6 out of 27 (22%), respectively – are more accurate measure of the availability of products that provide IDS/IPS when IPv6 transport is used for organizations that require such features.

SSAC notes that this survey only considers firewalls that offer IDS/IPS functionality and does not include the broader IDS/IPS market. The survey results may not accurately represent the state of IPv6 readiness for the broader IDS/IPS market and should not be interpreted as doing so.

Flooding attacks are designed to exhaust the resources (processing, memory, or bandwidth capacity) of a targeted application, system or network, and thus deny service to users. Flooding attacks are the most commonly recognized forms of denial of service attacks and vendors call specific attention to a product's ability to block the popular variants of denial

and distributed denial of service (DDoS) attacks. Chart 7 illustrates that a higher percentage of products across all market segments offer some form of rate-limiting when DoS and DDoS attacks are detected than offer IDS/IPS protection when IPv6 transport is used: 9 out of 42 overall (21%), 4 out of 19 (21%) for SOHO, 8 out of 35 (23%) for SMB, and 7 out of 27 (26%) for LE/SP. We speculate that this is because the methods vendors use to detect and rate limit TCP and UDP-based DoS attacks instigated using IPv4 transport can be applied when IPv6 transport is used as well.

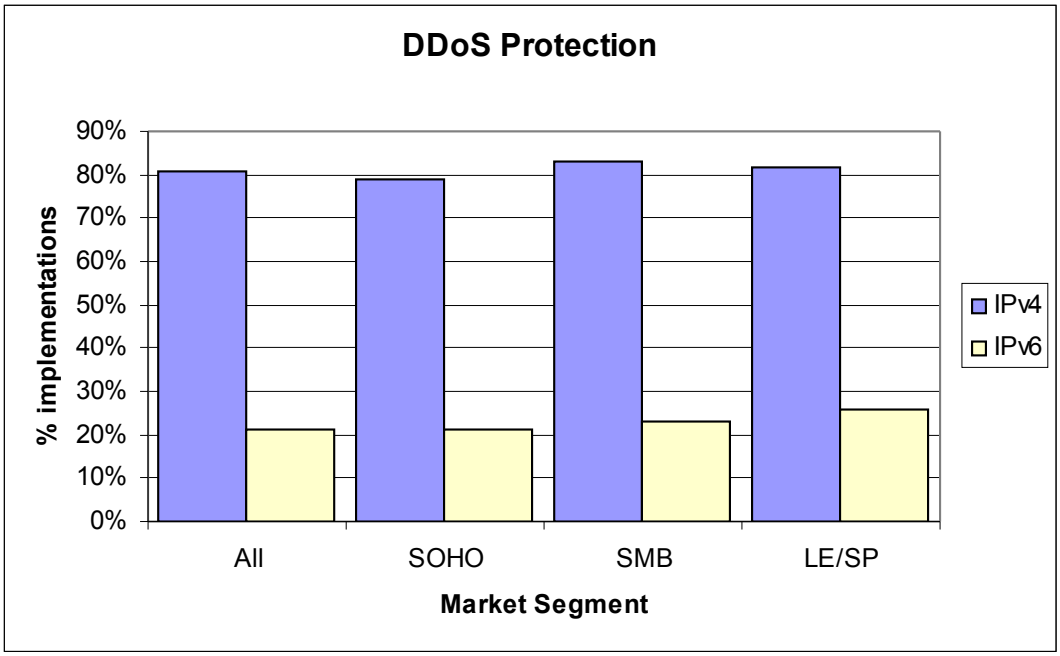


Chart 7: DDoS Protection

Tunneling Capabilities

IPv6 implementation will be incremental; in particular, it is very likely that many systems will not be upgraded to support IPv6 and thus "legacy" IPv4 transport implementations will co-exist or operate in "islands" for many years if not decades. Many organizations will require products that encapsulate (tunnel) IPv4 packets in IPv6 packets to interconnect two or more IPv4-only hosts or networks when the only available transport between those hosts or networks is IPv6.

It is very unlikely that all service providers will adopt and provide ubiquitous IPv6 transport over access circuits. This means that some networks that use IPv6 transport will be unable to connect to other IPv6-enabled networks without traversing an IPv4 network. Users and organizations that adopt and prefer IPv6 transport may require products that tunnel IPv6 packets in IPv4 packets to connect to IPV6-enabled destinations when the only available transport is IPv4.

Chart 8 illustrates the availability of IPv4-to-IPv6 (4to6) and IPv6-to-IPv4 (6to4) tunnels on commercial firewalls. The *4to6* survey results illustrate that 6 out of 42 (14%) of all firewall products surveyed are able to tunnel IPv4 traffic in IPv6 transport. The breakdown

according to market segment is: 3 out of 19 (16%) for SOHO, 6 out of 35 for SMB (17%), and 4 out of 27 (15%) for LE/SP. This figure is lower than expected when compared against the availability of IPv6 forwarding (see Chart 1). We cannot offer any explanation based on the information collected from the survey.

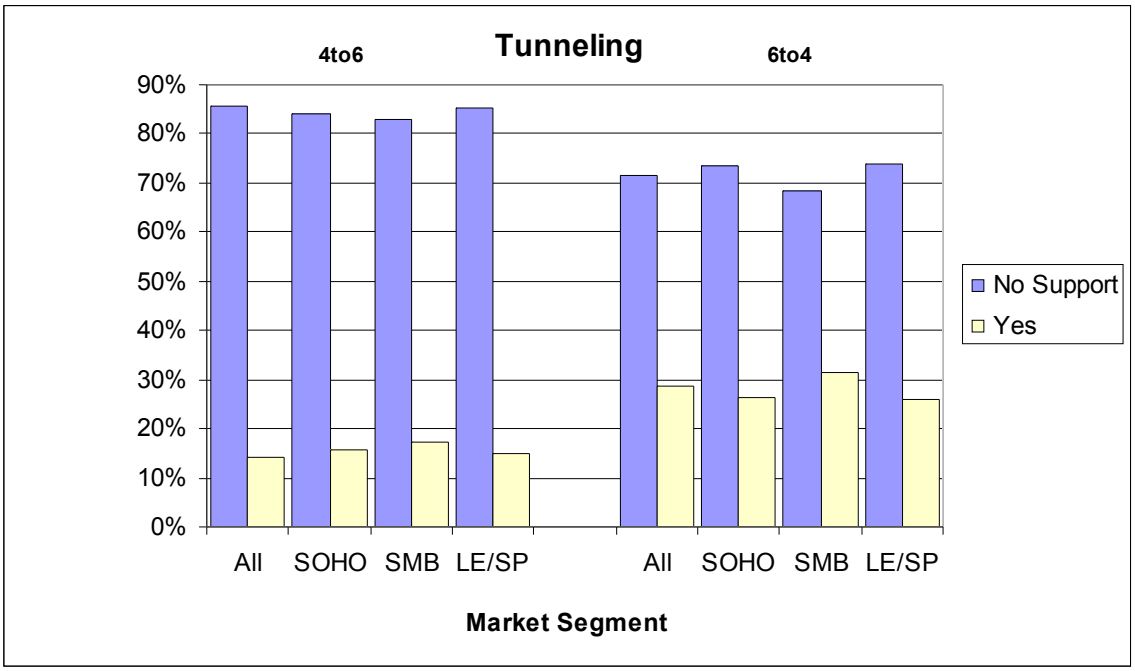


Chart 8. Tunneling Capabilities

A higher percentage of all firewalls surveyed are able to encapsulate IPv6 traffic in IPv4 tunnels (12 out of 42, 29%). The breakdown according to market segment is: 5 out of 19 (26%) for SOHO, 11 out of 35 for SMB (31%), and 7 out of 27 (26%) for LE/SP. This is arguably an easier tunneling implementation, and allows organizations to continue to make use of security features available when IPv4 transport is used when they connect "islands" of IPv6 hosts and networks. Some vendors indicated that they were able to perform IDS/IPS on 6to4 tunneled traffic but the number of vendors providing this additional information was insufficient to draw any conclusions regarding availability of this feature.

IPv6 availability among firewall market share leaders

The commercial firewall market is dominated by a very small number of network and security vendors. SSAC identified the companies it believes comprise the top ten market share holders. Conveniently, all these companies responded to this survey. SSAC then analyzed the survey results using only these sets of data.

Charts 9-12 illustrate the survey results from these vendors. Several vendors in this survey have multiple firewall product lines, and we requested that vendors provide a separate survey response for each product line. All of the product lines reported by vendors that we identify as market leaders are included in Charts 9-12. For these charts, "ALL" represents 13 products, SOHO includes 5 products, SMB includes 11 products, and LE/SP includes 10 products.

Chart 9 illustrates that support for IPv6 transport is stronger among the market leaders, with 7 of 13 (53%) of all product lines providing IPv6 transport. The percentages of products providing IPv6 transport support hover around 50% across market segments, with a slightly higher percentage (60%) among LE/SP products and slightly smaller (40%) among SOHO products. Since several large router and firewall vendors expanded their product lines through acquisitions of companies who targeted the SOHO market, the small drop in support among SOHO products is perhaps attributed to market consolidation.

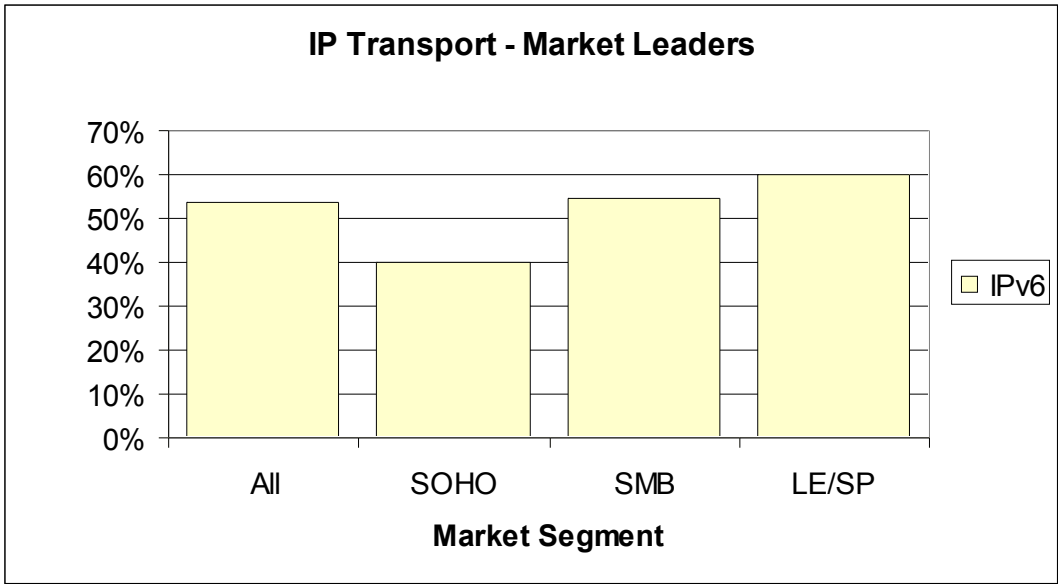


Chart 9. IPv6 transport support (Market Leaders)

Chart 10 illustrates that the availability of all forms of traffic inspection for IPv6 transport improves when only market leader products are considered (Compare to Charts 3, 4, and 5). The availability of static packet inspection across all market segments improves from 29% to 54%. The availability of stateful packet inspection across all market segments improves from 21% to 38%, and the availability of application level protection across all market segments improves from 17% to 27%.

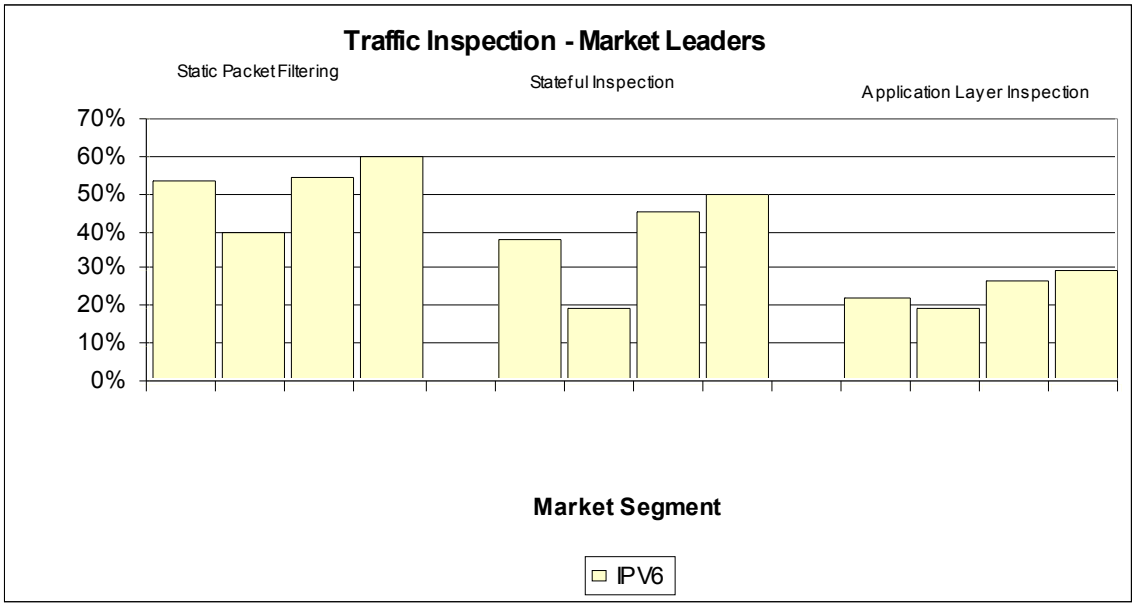


Chart 10. Traffic Inspection (Market Leaders)

Comparing Charts 6 and 7 to Chart 11, we see the availability of IDS/IPS increases from 14% overall to 38% overall when only products from market leaders are considered, and that the availability of DDoS protection increases from 21% to 38%.

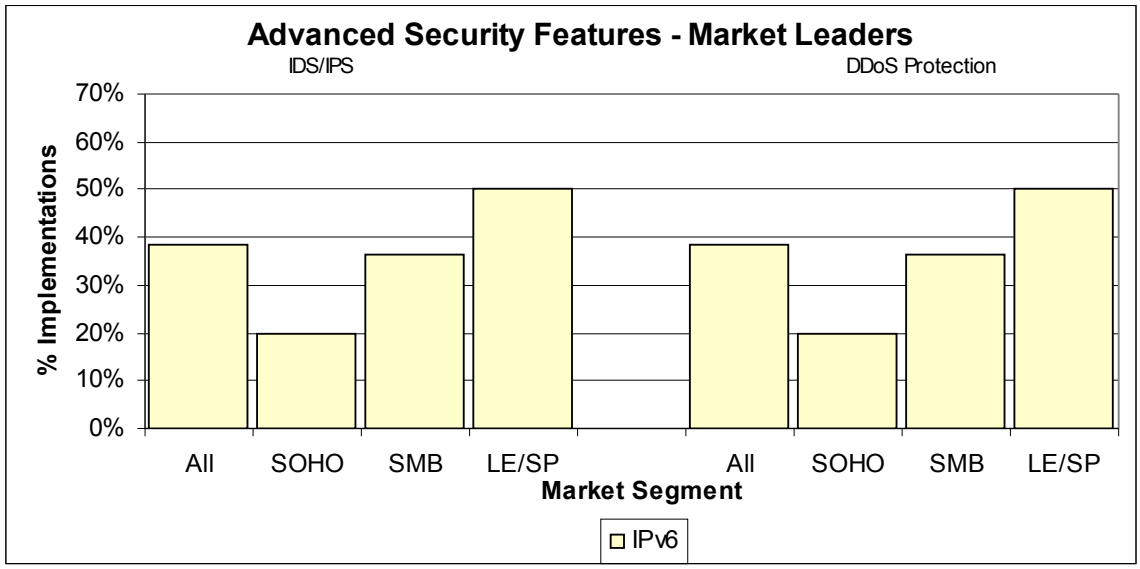
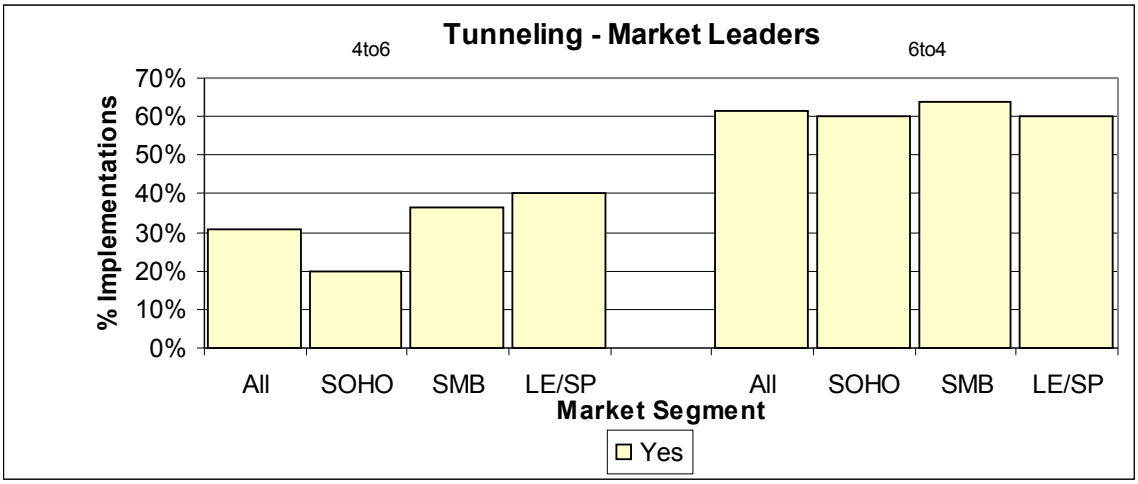


Chart 11. Advanced Security Features (Market Leaders)

Comparing Chart 12 to Chart 8 we see that the availability of tunneling improves when we only consider product lines of market leaders; specifically, if an organization has or intends to purchase and deploy a market leader firewall, the likelihood of finding tunneling support increases to 31% for *4to6* and 62% for *6to4* .



hart 12. Tunneling Capabilities

Collectively, charts 9-12 illustrate that the availability of IPv6 transport and security feature support improves when consumer choice is narrowed to the market leaders but that the availability of more sophisticated traffic inspection and advanced security features are improved but still not prevalent.

Additional Survey Results and Anecdotal Information

During the collection and processing of the survey, several additional results and information shared anecdotally by vendors provide additional insight into the present state of security feature availability as well as the market attitude.

Generally, if a product supports IP transport and one or more forms of traffic inspection, that product logs IP level events. This holds true for both IPv4 and IPv6 transport. Future studies might compare the breadth and depth of IPv6 logging against IPv4 logging. For example, it might be useful to ask whether logging can be enabled for each of the features and services surveyed, and whether logging facilities accommodate accounting, exception handling and external notification (e.g., pager, email).

While many firewall products support DHCPv6, RADIUS, and flow monitoring when IPv4 transport is used, few of the vendors who responded to survey questions concerning these services indicated that they provide support when IPv6 transport is used.

Generally, if a product supports IP transport and one or more forms of traffic inspection, that product supports IPsec (true for IPv4 and IPv6). Several vendors commented that IPsecv6 support was limited; for example, some vendors support fewer Internet Key Exchange (IKE) peer authentication options, or only support manual keys for IKE, or support IPsecv6 only through a command line interface.

Several vendors commented that IPv6 transport can only be configured using a command line interface (as opposed to the vendor's graphical user interface, i.e., a Microsoft Windows application or HTTPS- or Java-enabled web interface.

Some vendors commented that the signature sets for IDS/IPS inspection engines for IPv6 were not as extensive as the signature sets for IPv4. Similarly, some vendors indicated that the number and kinds of denial of service attacks they can detect and block were fewer when IPv6 transport was used instead of IPv4.

Vendors who commented that they had no IPv6 support typically claimed that they have received few if any requests for products that support IPv6. Some vendors indicated that IPv6 implementation was underway and that product support would appear mid-to-late 2008, whereas others admitted that IPV6 support was not included in product development time tables in their survey response.

Conclusions

Based on the results of this survey, SSAC answers the questions posed at the beginning of this survey report:

How broadly is IP version 6 (IPv6) transport supported by commercial firewalls?

IP version 6 (IPv6) transport is not broadly supported by commercial firewalls. On average, less than one in three products support IPv6 transport and security features. Support among the firewall market share leaders improves this figure somewhat.

Is support for IPv6 transport and security services available from commercial firewalls available for all market segments - home and small office, small-to-medium business, large enterprise and service provider networks – or is availability lagging for certain segments ?

Support for IPv6 transport and security services is available from commercial firewalls for all market segments, however, availability of advanced security features is lagging in SOHO and SMB segments and strongest in the LE/SP segment.

Among the security services most commonly used at Internet firewalls to enforce an organization's security policy, which are available when IPv6 transport is used?

Overall, relatively little support for IPv6 transport and security features exists. However, some form of traffic inspection, event logging, and IP Security (IPsecv6) are commonly available among products that support IPv6 transport and security services.

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?

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 duplicate IPv4 security feature and policy support.

The observations and conclusions in this report are based on collected survey results. Future studies should consider additional and deeper analyses of security technology availability for IPv6. Such analyses are best performed by certification laboratories and security assessment teams. Before attempting further testing and analysis, the community must alter the perception among technology vendors in general (and security vendors specifically) that the market is too small to justify IPv6 product development.

Acknowledgments

SSAC wishes to express its gratitude to all vendors who willingly participated in this survey. The full list of participating vendors is provided in Appendix A. SSAC wishes to express particular thanks to Brian Monkman and David Archer of ICSA Laboratories, who facilitated contact and introduced us to technical staff familiar with IPv6 product development and availability at many vendors who participated in this study.

Appendix A. Vendors Surveyed for this Report

Vendor	Response	Vendor	Response
2-Wire, Inc	Yes	iPolicy Networks	Yes
3Com	No	Jungo	No
Amaranten	No	Juniper/Netscreen	Yes
Arkoon	Yes	Kerio	Yes
ASCE Networks	Yes	Lucidata	Yes
Astaro	Yes	Mako Networks	Yes
Barbedwire Technologies	No	Microsoft	Yes
BlackBox	Yes	MultiTech	Yes
Cecurux	No	Netbox Blue	No
Celestix	No	NetContinuum	Yes
Check Point Software	Yes	Netgear	Yes
Cisco Linksys	Yes	Netopia	No
Cisco (IOS firewall)	Yes	NetSentron	Yes
Cisco (PIX)	Yes	NetSoft	Yes
Clavister	Yes	NetStealth	No
Crossbeam Systems	Yes	Network-1	Yes
Cybernet Linux Firewall	Yes	Nortel Networks (1000, 3000 series)	Yes
D-Link	Yes	PresiNet Systems	No
DrayTek	Yes	Secure-Computing (CyberGuard)	Yes
Eland Systems	Yes	Secure Computing (Sidewinder)	Yes
EliteCore Cyberoam	No	Secure Computing (SnapGear)	Yes
eSoft	No	Sepehrs	Yes
Evidian Networks	No	SonicWall	Yes
Fortinet	Yes	Stonesoft	No
Forum Systems	No	Symantec (7100)	Yes
GajShield	Yes	Telco-Tech	No
GateProtect	No	Tipping Point	Yes
Global Technology Assoc.	Yes	US Robotics	No
Green Computer	No	VarioSecure	No
HotBrick	Yes	Vortech	No
IBM ISS	Yes	WatchGuard Technologies	Yes
inGate	Yes	Zyxel	Yes
Internet-Security (ProxySentinel)	Yes		

Appendix B. SSAC Membership

Members
Alain Aina, Consultant
Jaap Akkerhuis, NLnetLabs
Steve Crocker, Shinkuro (SSAC Chairman)
Mark Kosters, ARIN
Ram Mohan, Afilias
Russ Mundy, SPARTA, Inc.
Frederico A C Neves, NIC Brasil
Dave Piscitello, ICANN (SSAC Fellow)
Ray Plzak, ARIN
Doron Shikmoni, ForeScout, Inc.
Bruce Tonkin, Melbourne IT
Paul A Vixie, ISC
Johan Ihren, Autonomica
James M. Galvin, Elistx
Paul Twomey, ICANN
Jon Peterson, Neustar
Rodney Joffe, Neustar
Suzanne Woolf, ISC
Mike St Johns, Nominum, Inc.
K. C. Claffy, CAIDA

Invited Guests
Daniel Karrenberg, RIPE
David Conrad, ICANN
Steve Conte, ICANN
Lyman Chapin, Interisle
Patrik Fältström, Cisco Systems
Ramaraj Rajashekhar
Jeffrey Bedser, ICG
Rick Wesson, Alice's Registry
Mark Seiden, Yahoo!
Danny McPherson, Arbor Networks, Inc.
Shinta Sato, JPRS

Liaison to the GAC
Stefano Trumpy

Liaison to the IAB
Olaf M. Kolkman

Liaison to the ALAC
Robert Guerra