

# IPv6 & IPv4 Threat Review with Dual-Stack Considerations

Troy Lancaster

University of Southampton, Department of Electronics and Computer Science  
tl302@ecs.soton.ac.uk

**Abstract**—The gradual transition from IPv4 to IPv6 requires network administrators to become aware of the next generation protocol and the associated security risks. IPv6 provides many new features, which directly or indirectly improve the security environment for devices connected to both public and private networks. However, the very presence of IPv6 makes networks susceptible to attack. By transitioning to IPv6 without adequate precautions, an adversary can easily bypass a networks security infrastructure. Most administrators are aware of the security considerations with IPv4, however, are lacking such knowledge for IPv6. This paper provides a condensed review of the most common attacks in IPv4 and compares them to IPv6 and its transition mechanisms. Specific emphasis is placed with dual-stack deployment where a modified security model is proposed. Finally, guidelines and recommendations are given to outline the key considerations throughout the deployment process.

**Index Terms**—Dual-stack, IPv6, Network Security.

## I. INTRODUCTION

THE current Internet and all the corporate and private intranets predominately use Internet Protocol version 4 (IPv4) [1], however, with its 32 bit address space being rapidly exhausted [2] alternative solutions are needed [3]. The long-term solution is a transition to IPv6 [4], which is designed to be an evolutionary step from IPv4, where most transport and application-layer protocols need little or no change to work. In addition, IPv6 includes various transition and interoperability mechanisms to allow users to adopt and deploy IPv6 incrementally, whilst maintaining an IPv4 connection. To this extent, network administrators must familiarise themselves with the security considerations and comparisons between IPv4 and IPv6 before a comprehensive transition strategy can be implemented.

The methods of attack remain similar in many aspects between IPv4 and IPv6. The IP layer is only concerned with the transportation of packets, so vulnerabilities in the other layers such as the application layer will continue to exist in IPv6, even with successful deployment.

This paper is intended to provide a review of the most common threats present to IPv4 and determine their relevance to IPv6. This is extended by investigating the additional threats through the deployment of IPv6, including those associated with the various transition mechanisms available with specific emphasis on dual-stack. Where necessary, the current capabilities of IPv6 security products are assessed to highlight how the intrinsic characteristics of the protocol contribute to the nature of a threat. Finally, a general outline of the author's

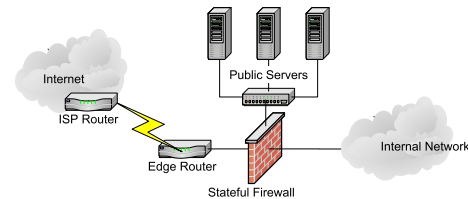


Fig. 1. Simplified IPv4 Edge Security Model

key recommendations and known best practices are delivered, to allow the reader to understand the key security requirements throughout the deployment process.

The reader is assumed to have an understanding of the security considerations of IPv4 and has made the decision to deploy IPv6, but is unaware of the potential threats. An understanding of network security and a general knowledge of IPv6 and its corresponding transition mechanisms are required, for more details refer to [5].

Network security is a very large and dynamic topic that is constantly evolving. For these reasons, Mobile IPv6 (MIPv6) will not be covered in any depth due to the magnitude of the subject, however, the reader will be directed to relevant resources where necessary.

## II. IPV6 AND IPV4 THREAT REVIEW

### A. Overview of the Current IPv4 Security Model

Before investigating IPv6 security and comparing it to IPv4, a general description of the architecture used within a traditional IPv4 security design is required. The basic design, shown in Figure 1, illustrates the point that there are two principle security elements, the firewall and the edge router, which control the traffic in and out of the network. Firewall policies are generally permissive for outbound traffic and restrictive for inbound traffic. Additional security devices/technologies can be incorporated into the network design, counting Intrusion Detection Systems (IDSs), application proxies, and so on. Public servers, which are accessible to the outside world are placed within a demilitarised zone (DMZ) which is isolated from the rest of the network, therefore if a host becomes compromised within the DMZ, other network segments remain unaffected. These three interfaces to the firewall characterise the basic IPv4 security model and its many variants.

For IPv6 to be successful it must be able to blend in with the current security architecture, at least for the period

of transition. This restriction demands that all the current security devices/technologies need to have IPv6 capabilities and be aware of the associated threats.

1) *Perceived Security of IPv4 Network Address Translation:* Many users on the Internet use Network Address Translation (NAT) [6][7] due to its economic use of IPv4 addresses and the perceived security benefits that have been marketed. This comprises of providing a simple mechanism to hide the internal topology of a network and limiting the ability to perform ‘device profiling’ through the monitoring of a specific IP address. Although the serious disadvantages of NAT have been well documented [8][9], including breaking security protocols such as IPSec, many organisations who primarily use the Internet in a client/server fashion feel the advantages outweigh the disadvantages, thereby making it a popular solution. IPv6 Network Architecture Protection (NAP) [10] provides a method for IPv6 to emulate the protection features associated with IPv4 NAT without compromising end-to-end connectivity [11].

Device profiling can be minimised by using IPv6 Privacy Extensions [12] with short lifetimes since a node will not respond to the address once the address is no longer valid. Limited lifetimes only allow a session to be traced back to the subnet it originated from, not directly to the host. This is exactly the same benefit that IPv4 NAT provides, however, due to the large address space of IPv6; a casual ‘snooper’ would find it extremely difficult to determine anything substantial about the network’s internal topology. The disadvantage of constant address changing is that network management tools must start to become aware of which addresses are from the same host, otherwise they may produce false alarms.

To mask the internal structure of the network from the outside world IPv6 addresses need to be ‘untraceable’. This can be achieved by using DHCPv6 and ‘route-injection’ [10] but has the scalability limitation of the Interior Gateway Protocol, as it was not designed to carry large numbers of host routes.

One should note, for IPv6 to substitute NAT, IPv6 security best practices must be followed, whereby the minimum should be the deployment of a dedicated IPv6 firewall. In addition, all security devices must be configured and maintained correctly for full protection to be preserved. For these reasons, IPv6 is unlikely to replace NAT until IPv6 security devices become more mature and easily deployable by home users.

## B. Threat Comparison between IPv4 & IPv6

1) *Scanning:* The first point of attack is reconnaissance, where an adversary performs various operations in an attempt to probe and map a victim’s network. For IPv4, this involves ping sweeps, to find active hosts, port scans, to determine which services are running, and finally correlating this information with known vulnerabilities to optimise an attack. A typical small subnet size of  $2^8$  hosts within IPv4, makes it very easy to perform brute force scanning to find active hosts. In comparison, IPv6 has a typical subnet size of  $2^{64}$  which is (currently) computationally unfeasible [13] provided the

addresses are allocated at random. However, simple reliance on the IPv6 address space for protection against scanning is not a wise defensive strategy as will be illustrated.

An administrator can make scanning significantly easier for an attacker in various ways. This includes conveniently numbering their hosts [prefix>::1 upwards, statelessly auto-configuring [14] hosts using vendor prefixes [13][15], and using techniques that derive the low-order bits of the IPv6 address from the IPv4 address. The latter point also has the disadvantage of an attacker gaining specific knowledge about the hosts within the network [16] (Microsoft’s 6to4 implementation uses the address 2002:V4ADDR::V4ADDR while older Linux and FreeBSD implementations default to 2002:V4ADDR::1).

Privacy extensions for stateless autoconfiguration [12] can facilitate the generation of randomised interface identifiers to exploit the full 64-bit subnet, greatly reducing the need for administrator intervention whilst maintaining randomised addresses. However, if a node’s address has a very short lifetime the frequency of address changing would display the behaviour of a compromised system, which has been the source of a Distributed Denial of Service (DDoS) attack [16].

The implications of larger subnets presents a significant development, which is likely to evolve the reconnaissance process from brute force scanning, to selectively exploiting poorly secured routers and maliciously acquiring web and system logs to harvest a large pool of IP addresses. Attacking routers to obtain the neighbour-discovery cache (equivalent to ARP cache) is one example, which can be used to determine other nodes on a LAN. In addition, many organisations use internal routing protocols such as RIPng [17] (adaptation of RIP for IPv6), which can be manipulated by looking at the routing tables of nodes that are participants of the routing protocol. Using this information, an attacker could determine other valid subnets within the organisation and subsequently target those [18]. Domain Name Servers (DNS) will be more prone to attack by exhaustively searching all words and obtaining valid IP address from the results. This may seem irrational, however, it has been shown in [19] that a DNS worm in IPv6 could spread just as fast as an IPv4 address scanning worm.

IPv6 presents additional security considerations through its addressing architecture [20], the use of specific site-scope multicast addresses can be used to identify key resources on a network for attack. Such addresses consist of, the ‘all routers’ (FF05::2) and ‘all Dynamic Host Configuration Protocol (DHCP) servers’ (FF05::1:3) as defined in RFC 2375. The risk of attack can be minimised by ensuring all firewalls and site boundary routers are configured to drop packets with site scope destination addresses [16][21], however, this does not stop an attack from being performed from within the site. Furthermore, 38-bits of the IPv6 address are dedicated to identifying the site and ISP as explained in RFC 3177, using this knowledge an attacker can considerably reduce the volume of addresses to search through.

The ability to find hosts to attack is highly related to how Internet based worms attempt to spread. So future IPv6 worms will most definitely use the tactics outlined above to reduce

the search space. However, some worms such as the Melissa Worm spread by email, so the adoption of IPv6 will have no affect on these worms as they can consult such things as Microsoft Outlook's address book. A good overview of the strategies that future worms will use for spreading is considered in [15].

To summarise, conventional random address space scanning within IPv6 is not feasible as it would be prohibitively expensive, however, there are many other sources to obtain valid IPv6 addresses. Therefore, it is imperative that network administrators number their network carefully and continue to monitor for scanning activity and do not rely on the IPv6 address space for protection. The most popular port scanner for IPv4, Nmap, now supports IPv6, so it is likely that it will eventually employ some of the techniques explained in this paper, once IPv6 becomes more wide spread.

The author recommends that a nodes address should not be assigned dependent on the MAC address or through the use of IPv6 privacy extensions, but by allocating a unique randomised static IP address for servers and routers and dynamic IP addresses for all other nodes. In both instances, this can be achieved through DHCP. The reader should be aware that reconnaissance cannot be stopped due to the need for open communication channels, however, it can be made harder for an adversary by thoughtfully numbering the network.

2) *Unauthorised Access*: Unauthorised access is restricted through the implementation of a security policy, which usually consists of a firewall to restrict access to and from the network, and an IDS to provide upper-layer inspection. For effective deployment of IPv6, the IPv4 security policy needs to be mirrored wherever possible. IPv4 and IPv6 essentially need to implement the same procedures, however, the maturity of IPv6 security devices are limited in comparison to IPv4. To compensate, each adapter can have multiple IPv6 addresses (link local, site local and global) which can be integrated into the security policy to restrict access to IPv6 end nodes through IPv6 addressing and routing [21].

The filtering of Internet Control Message Protocol (ICMP) messages is vital in IPv4 to maintain security, however, ICMPv6 [22] is a integral part of the inner workings of IPv6 including, Neighbor Discovery [23], Multicast Listener Discovery [24][25], Path Maximum Transmission Unit (PMTU) Discovery [26], and Stateless Address Configuration [14]. Therefore, ICMP filtering cannot simply be mirrored from the IPv4 policy to IPv6. ICMPv6 error messages, (Time Exceeded and Parameter Problem) must be allowed to pass through a firewall in both directions to maintain functionality. This presents the problem that an attacker could create an ICMPv6 tunnel encapsulating malicious traffic to avoid detection from security devices, so careful observation of large amounts of ICMPv6 traffic must be investigated. Current best practices for filtering ICMPv6 messages in firewalls are documented in [27].

IPv6 presents additional threats with IPv6 Extension headers. One in particular is that of the Routing header, which can be used to evade access controls based on the

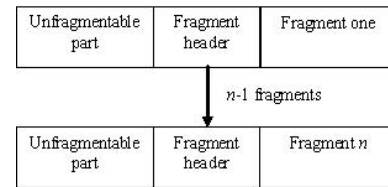


Fig. 2. Fragmentation in IPv6

embedded destination addresses. By sending a packet to a publicly accessible node with a Routing header containing a 'forbidden' destination address the publicly accessible node would forward on the packet to the forbidden address, which would normally be dropped. If the source address can be spoofed then anonymous reflective DoS attacks can be performed [16]. The reader should be aware that some operating systems automatically forward packets with a Routing header where others do not. The author recommends that the security policy should only forward traffic with a Routing header from selected source addresses that can be trusted, however, this is not always feasible to implement.

3) *Fragmentation*: Routers, depending on the MTU perform IPv4 fragmentation. IPv4 fragmentation has caused much controversy due to its associated security problems. This incorporates, DoS attacks through means such as sending large amounts of fragmented packets without a terminating last fragment, in addition to, evading detection tactics through sending out-of-order fragments, overlapping fragments and so on. The proportion of fragmented traffic within a network is generally low, so large amounts of fragmented packets is usually a sign of an intrusion attempt [28]. Most IPv4 firewalls and IDSs reconstruct fragmented traffic to determine the probability of a threat, so fragmentation attacks can generally be detected.

IPv6 eliminates fragmentation in routers [4] and only permits end-to-end fragmentation. A fragmented packet always consists of a unfragmentable part containing an IPv6 header, plus any Extension headers that must be processed by nodes along the path to the destination (Hop-by-hop Options header and the Routing header). The fragmentable part of the original packet consists of any Extension headers that only need to be processed by the destination, plus the upper-layers and the data. The ability to contain Extension headers within the fragmentable part allows an attacker to hide certain attributes from security devices that do not perform stream reassembly correctly. Fragmentation is demonstrated in Figure 2.

The IPv6 specification [4] does not mandate any minimum packet size for the fragments, apart from it must carry the unfragmentable part in all fragments. In addition to this, there is no indication that fragments should not overlap, so many of the threats applicable to IPv4 [29][30] will continue to exist in IPv6. There is no need for packets to overlap, so the author recommends overlapping fragments should be viewed as an attack and discarded. This problem is the same as IPv4, however, it is unlikely that IPv6 devices will be sophisticated enough to perform packet reassembly, consequently making them more vulnerable to attack.

4) *Spoofing*: A key element to the success of most IP attacks is based on the ability for an adversary to construct their own IP packets, often using a modified source IP address to appear to the recipient that the traffic was sent from another location. This so-called “spoofing” attack is made possible by programming a network API allowing packets to be built with customised characteristics, rather than using the kernel to handle all communication flow. The process of creating a basic network API is trivial, so spoofing will continue to cause IPv6 the same problems as with IPv4.

5) *Broadcast Amplification Attacks (Smurf)*: Within IPv6 there are no broadcast addresses, however, the IPv6 equivalent of an IPv4 Smurf attack is still achievable via exploiting the multicast infrastructure. ICMPv6 [22] allows an error notification response to be sent back to the source address when certain packets are sent to multicast addresses. An attacker could construct a suitable packet with a spoofed source address and a multicast destination, which could elicit all responses to be directed to the victim. Furthermore, fragmentation can be used to evade detection for malicious packet types, which incorporate Extension headers that are located in the fragmentable part of a packet. Broadcast amplification attacks using the multicast infrastructure would only be as effective as the number of multicast receivers.

To mitigate against IPv6 amplification attacks the author recommends that RFC 2827 [31] ingress filtering should be implemented to prevent occurrences of various DoS attacks with forged source addresses.

6) *Autoconfiguration and Neighbor Discovery*: The equivalent to Autoconfiguration and Neighbor Discovery (ND) for IPv4 is a straightforward process through the use of the Address Resolution Protocol (ARP), but limited in security and scope. IPv6 eradicates the need for additional protocols such as ARP through the extensive use of ICMPv6. An IPv6 device can configure automatically and connect to a network without requiring a stateful configuration protocol such as the stateful version of DHCPv6 [32]. Stateless Autoconfiguration involves the exchange of Router Solicitation and Router Advertisement messages to obtain the necessary information to communicate [23]. However, the lack of integrity within these messages makes the procedure vulnerable to attack; any node on the network can maliciously claim to offer routing services which it will not fulfil, through the advertisement of inappropriate prefixes and parameters, threats have been documented in [33][34]. In addition, a malicious node can deny other nodes from obtaining valid IPv6 addresses through manipulating the Duplicate Address Detection procedure, thus provoking a DoS attack to its victims. To combat these problems SEcure Neighbor Discovery (SEND) [35] provides a method for securely associating a cryptographic public key with an IPv6 address, allowing only for authorised routers to offer their services. If a SEND node becomes compromised, the trust model the protocol provides becomes obsolete. Therefore, to further prevent attacks, such as bogus on-link prefixes, IPv6 nodes should adhere to default router preferences outlined in

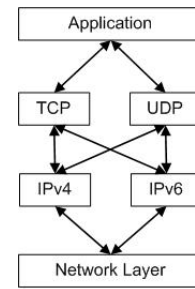


Fig. 3. Dual-Stack Infrastructure for TCP/IP Model

RFC 4191 [36], which will allow hosts to detect unreachable routes and prevent them from being added to their IPv6 routing table.

The added complexity of associating cryptographic public keys with an IPv6 address makes SEND routers/nodes vulnerable to DoS attacks. For example, if a SEND node becomes bombarded with packets, they have to verify each one using asymmetric methods, which consumes time and processing power. Additional attacks to the SEND protocol and possible mitigation methods are further described in Section 23 of RFC 3971.

For configurations that require DNS, stateless autoconfiguration can be substituted by the use of DHCPv6 [32], which can provide a stateful way for nodes to configure. To prevent DoS attacks through the use of bogus DHCP servers, authentication for DHCP message exchanges for IPv6 or IPv4 are possible [37], but are rarely deployed.

### C. Threats Due to Transition Mechanisms

There are a large number of transition mechanisms to deploy IPv6, but can broadly be categorised into, dual stack, tunnelling (manual/automatic), and translation [38].

A dual-stack node has complete support for both IPv6 and IPv4. The two protocol stacks work independently but coexist within the same network, so applications can be subject from attack from both IPv4 and IPv6. Therefore, any security controls, such as firewalls, IDSs, VPN clients and so on, must be mirrored in both protocol deployments to provide full protection.

Tunnelling involves the transportation of IPv6 packets over the existing IPv4 infrastructure. This usually involves encapsulating IPv6 packets within the payload of an IPv4 packet. Such mechanisms as 6to4 tunnelling [39] adopted this procedure, where the security considerations have been well documented in RFC 3964 [40]. Tunnelling can be used to evade security devices, so administrators must ensure they have both an IPv6 and IPv4 firewall where their rules are mirrored for both protocols. The problem is amplified when IPv6 is tunnelled over IPv4 encapsulated in UDP, as UDP is usually allowed to pass through NATs and firewalls [16]. Consequently, allowing an attacker to punch holes within the security infrastructure. The author recommends that if the necessary security measures cannot be taken, tunnelled traffic should be used with caution if not completely blocked. To provide ingress and egress filtering of known IPv6 tunnelled traffic, perimeter firewalls should

block all inbound or outbound IPv4 Protocol 41 traffic. For circumstances where Protocol 41 is not blocked it can easily be detected and monitored by the open-source IPv4 IDS Snort.

### III. SECURE IPV6 DEPLOYMENT FOR DUAL-STACK

The conceptual ease of dual-stack deployment has resulted in it becoming one of the most popular transition methods. The drawback of this mechanism is all processes applied to IPv4 must be duplicated within IPv6. This section presents an overview of the protocols and technologies needed to secure current dual-stack deployment, including basic security models, in addition to investigating and predicting future security models.

#### A. State of Current Security Devices and Technologies

1) *IPv6 Firewalls and Intrusion Detection Systems*: A firewall primarily provides an IP packet filtering capability to enforce a security policy on the traffic flowing through a network. The security policies are usually enforced at the border of a given network, to protect internal hosts from outside attacks and preventing internal users from maliciously attacking external hosts. An IDS on the other hand, passively listens and inspects all inbound and outbound network activity to identify any suspicious patterns that may indicate a network or system attack. Although both devices have different functionalities, they both perform deep packet inspection so rely on the same principles.

The inclusion of IPv6 Extension headers and their sometimes limitless options makes the process of parsing each packet for inspection problematic [41]. Furthermore, the extensive use of ICMPv6 prevents some of the rules implemented in IPv4 to be directly ported over to IPv6. A brief summary of the type of ICMPv6 messages and their functionality is shown in Table I where **bold** represents ICMP features that are essential for the correct operation of IPv6. For further recommendations and best practices on which ICMPv6 messages should be filtered please refer to [27] and Section 9 in [5].

The positioning of the firewall at the perimeter of a network affects the additional functionality that it must support. The variations consist of, Internet-router-firewall, Internet-firewall-router and Internet-firewall/router combined. The first has to support Stateless Address Autoconfiguration [14] as the firewall is directly connected to the internal network. Router Advertisements and Router Solicitation messages must be allowed for the firewall to operate transparently to other hosts. The firewall in the second situation is directly visible to the Internet, so it must support the necessary dynamic routing protocols to provide the router access to the Internet Service Provider (ISP). Finally, where the router and firewall are combined they must support both dynamic routing and Router Advertisement/Solicitation messages, as it is a combination of the previous two architectures.

At present, there is a limitation on the amount of commercial IPv6 firewalls that are available, to the author's knowledge they include, CheckPoint Firewall-1, the Nokia IP range and NetScreen. All of which are working towards full functionality but have a long way to go. In addition,

TABLE I

SUMMARY OF ICMPv6 RECOMMENDATIONS (ADAPTED FROM [5])

| ICMPv6                  | Usage                                   | Protocol    |
|-------------------------|---|-------------|
| Echo request/reply      | Debugging                               | IPv4 & IPv6 |
| Destination unreachable | Debugging - better indicators           | IPv4 & IPv6 |
| TTL Exceeded            | Error report                            | IPv4 & IPv6 |
| Parameter problem       | Error report                            | IPv6 only   |
| <b>NS / NA</b>          | Important for IPv6 Neighbour Discovery  | IPv6 only   |
| <b>RS / RA</b>          | For Stateless Address Autoconfiguration | IPv6 only   |
| <b>Packet too big</b>   | Important for PATH MTU discovery        | IPv4 & IPv6 |
| MLD messages            | Required for Multicast operations       | IPv6 only   |

there are various open-source IPv6 firewalls that have been tested [42], which are mostly orientated around Linux or BSD such as IPfilter, IP6fw, and Netfilter; their functionality is not complete but allows for various customisations. Windows XP and Windows Server 2003 both can provide an IPv6 firewall, but under test conditions it has proved not to be as effective as its Linux counterparts [42]. Future versions of Windows such as Vista will have a single, unified dual-layer stack instead two IP stacks working independently, which will provide a more comprehensive and configurable IPv6 firewall. Unfortunately, there are no commercial IDSs that the author is aware of. Work is rumoured to be undergoing for the most popular open source IDS, Snort, but nothing has been provided to the community. The author recommends to administrators that have not yet deployed IPv6, to use their current IPv4 IDS to detect Protocol 41. Otherwise, the network is liable to becoming compromised by tunnelled IPv6 traffic to evade detection. This can be seen in an instance of 6to4 tunnelling from the HoneyNet Project [43].

2) *IP Security*: IP Security (IPsec) [44] is a framework of open standards, which provides a mechanism for securing the transmission of sensitive information over a hostile environment. The network security services that IPsec provides are packet confidentiality, packet integrity, packet origin authentication and protection against replay. These mechanisms can be considered generic as they can be applied both to IPv4 and IPv6. However, IPv6 should implement IPsec capabilities in all conforming nodes as stated in Section 8.3 of RFC 4294 [45], whereas there are no formal requirements in IPv4. It should be noted that IPsec could easily be integrated into the existing IPv4 software if it were to become the de facto standard for IP communication.

IPsec needs to be distributed through a policy, which defines a definite goal, course, or method of action to guide and determine present and future decisions that an IPsec node must adhere to. Before IPsec nodes can comply with a policy they need to facilitate the secure exchange of information to establish a Security Association. This is done using the

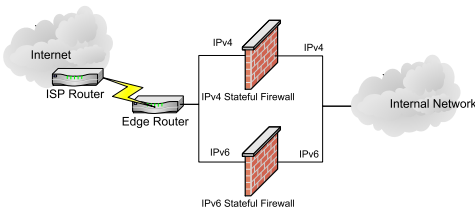


Fig. 4. Basic Security Model for Dual-Stack

Internet Key Exchange (IKE) [46], which describes a protocol to authenticate peers, exchange symmetric keys and to manage Security Associations. For large-scale IPsec policy deployment, a common Public Key Infrastructure (PKI) or Key Distribution Centre (KDC) would be required as it would be impractical to do each network element by hand. However, this is subject to trust considerations and political debates. If the key distribution problem was solved, edge based firewalls would decrease in significance as they only provide access control, whereas, IPsec provides the additional benefits discussed.

### B. Specifics of IPv6 Dual-Stack Deployment

Considering the issues surrounding IPv6 firewalls, Figure 4 demonstrates how all traffic originating from the Internet must be split up into its corresponding protocols. Each protocol must then be inspected and filtered independently based on a consistent policy before being forwarded to their respective destinations. Under most circumstances, the deployment model will be much more complex and will probably consist of some hybrid deployment structure, which may include some element of tunnelling. For these situations, the principle should remain the same but the model should be adapted accordingly.

### C. Large Scale Dynamic IPv6 Deployment

Secure and effective deployment of IPv6 is only possible if it can be integrated into the existing network architectures of IPv4. This mainly orientates around secure dynamic IP address allocation, which incorporates some element of authentication and authorisation. One such protocol, which is widely deployed within IPv4 is Remote Authentication Dial-In User Service (RADIUS) [47] enabling centralised authentication, authorisation, and accounting (AAA) for network access. RADIUS is a central protocol for large-scale dynamic secure address allocation and is now supported by virtual private network (VPN) servers, wireless access points, authenticating Ethernet switches, Digital Subscriber Line (DSL) access, and other network access types. It is possible to implement RADIUS with free open source tools in IPv6 using a DHCPv6 server and RADIUS enabled clients as demonstrated in [48]. This provides the ability for instances such as automated IPv6 wireless connectivity through the IEEE 802.1X standard. In addition to this, ISPs could supply connectivity to another ISP that provides IPv6 access to end-users enabling cross network wide spread IP allocation.

### D. Predicted Security Models for Dual-Stack

Research is pushing the way towards reducing the restrictions that are preventing widespread deployment of IPsec. Advances in the development of a PKI solution [49] to offer basic and advanced certification services, supplies a solution to allow client systems or end entities in one administrative domain to communicate securely with client systems or end users in another administrative domain. This can be extended to support multi-domain IPv6 scenarios through the deployment of cross-certification modules, thus reducing the key management problems. In addition to this, policy-based management systems are being implemented to solve the challenges presented by large-scale IPsec policy deployment across many network elements through the use of a centralised policy server which controls policy targets [50]. These advances are in their preliminary stages but demonstrate the options available to start solving the limitations of widespread IPsec deployment within IPv6.

If IPsec deployment dramatically increases, it is likely that a large portion of traffic will become encrypted. Therefore, the traditional perimeter based firewalls will decrease in their effectiveness to provide a high degree of security due to its inability to perform deep packet inspection. As discussed in [41] there is no real solution to prevent this problem. This will force the security model to move from an edge based firewall infrastructure to a distributed firewall system, where a security policy is still centrally defined, but enforcement is left to up to the individual endpoint [51]. From a dual-stack perspective, this would require all nodes to have host-based firewalls running both protocol stacks (IPv4 and IPv6), where the policy would be obtained from a central server. Therefore, future emphasis must be placed on comprehensive development of host-based firewalls for both IPv4 and IPv6.

## IV. RECOMMENDATIONS

This section helps to summarise all the key recommendations made throughout the paper. In addition to this, a general guideline is presented for a network administrator to take through each stage of deployment.

### A. Immediate Actions to take before IPv6 Deployment

1) *Prevent unknown IPv6 Attacks:* Administrators who have not deployed IPv6 must first ensure that it is not being maliciously used without their knowledge. Filtering all traffic with Protocol 41 set in an IPv4 header will prevent known IPv6 traffic from being tunnelled within IPv4, thus preventing any back doors from being created within the network. However, tunnels can also be set up over UDP, HTTP (port 80) and so on, so the author recommends to use an IDS to carefully detect and monitor all tunnelled traffic for instances of IPv6 traffic.

2) *Firewall Research:* The fundamental element within the current and foreseeable security model is the firewall. To prevent holes from appearing within the security model by introducing IPv6, adequate investigation into how best to mirror current IPv4 firewall settings over to IPv6 is essential. This

can be ambiguous due to the modifications within the protocol, such as the extensive use of ICMPv6 and the inclusion of Extension headers. To this extent, the administrator must make themselves aware of ICMPv6 best practices, shown in [27], and selectively apply them to their security policy. In addition, the author recommends the policy should be extended by using RFC 2827 like filtering, to verify all outgoing traffic is from a valid internal IP address within the subnet. Rules to filter site scope IPv6 destination addresses at the boundary must not be omitted.

Once sufficiently aware of how best to mirror the security policy, this information should be correlated with the functionality available in commercial and open-source based firewalls, so the best firewall can be selected for the purpose of the policy. To facilitate the incomplete support for some IPv6 Extension headers and their associated attacks, the administrator must carefully choose whether to permit or deny the use of some Extension headers such as the Routing header; otherwise, they may find themselves susceptible to attack.

3) *Other Considerations:* Whilst testing and debugging networks a deeper understanding of the protocol is needed to verify there is no abnormal activity. This includes having a general knowledge of which packets are associated with specific applications of the protocol.

To exploit the address space of IPv6 and make conventional scanning techniques harder, correct addressing is essential. As previously mentioned the author recommends using a unique randomised static IP address for servers and routers but using DHCPv6 for all other nodes. This method utilises the full address space for important nodes whilst maintaining scalability for address allocation of all other nodes without requiring complex network tools to maintain their addresses.

Finally, different operating systems can respond to the same messages inconsistently. This problem cannot be rectified, but administrators should be aware that under extreme circumstances these discrepancies could create holes within their security policy. Furthermore, all unnecessary IPv6 services should be blocked at the edge firewall, in addition to being disabled within the operating system to prevent vulnerabilities within applications from being exploited.

### B. Immediate Actions to take on IPv6 Deployment

The initial introduction of IPv6 is likely to result in some hosts not being secured properly, so it is essential to maintain security at the application level within all hosts via regular updates.

1) *Testing Firewall & Securing IPv6 Hosts:* Following the implementation of the IPv6 security policy, it is essential to probe the network to verify there are no “backdoors”. This process involves methodically breaking down the policy into its constituent rules and systematically testing that they work. Depending on whether the rule is providing ingress or egress filtering capabilities will depend on whether the test needs to be performed internally or externally from

the network. Testing should be performed with the mindset of an attacker, by starting with reconnaissance and then moving onto vulnerability scans and so on. If at any point weaknesses/vulnerabilities are found, they should be logged and fixed immediately.

2) *Evolve:* As IPv6 matures and attackers become more advanced, gaps will begin to appear within the initial security policies devised. Therefore, administrators must re-evaluate and evolve their security policies over time.

### C. Preparation for the Future

1) *Familiarisation with Technologies:* To be one-step above the attacker, administrators must be familiar with current and future technologies. The author recommends learning emerging technologies such as IPsec because this could have a radical effect on the future of security models, in addition to being able to prevent malicious usage of the standard by attackers.

2) *Implementation of Decentralised Security Structure:* The edge router and firewall security model is already starting to blur within larger networks. The advent of large-scale deployment of IPsec could further reduce its effectiveness. To future proof against this problem, research of how to manage and decentralise the security policy should be considered.

## V. FUTURE WORK

This paper has not considered Mobile IPv6, which is another large and complex topic within IPv6 security. To provide a complete overview of IPv6 security this paper should be used in conjunction with a paper on MIPv6 security.

The most important area to move forward within IPv6 security is the extension of current IPv6 firewalls and network tools to test them (IPv6 packet constructors, IDSs and so on). This will allow more users to adopt IPv6 without being paranoid about their openness to attack. Luckily, the U.S. Department of Defence aims to complete its transition to IPv6 by 2008 [52], which should result in a more serious attitude to IPv6 security and the corresponding number of tools available.

## VI. CONCLUSION

This paper has shown IPv6 has both benefits and drawbacks from a security perspective. Many of the attacks applicable to IPv4 remain the same in principle to IPv6, but different in the way that they are applied. Knowledge of the presence of IPv6 and its corresponding transition methods is often enough to arm network administrators with enough information to thwart common attacks.

Any deployment strategy should include a firewall to improve protection. The security considerations of dual-stack have been investigated, whereby success is determined on how well the IPv4 security policy can be mirrored to IPv6. Differences in the protocol architecture have prevented complete firewall coverage, but by using firewall best practices, comprehensive protection is possible.

The future of the traditional IPv4 security model is debatable depending on the uptake of IPsec. However, it is clear the firewall will remain a fundamental element within both IPv4 and IPv6 security.

#### ACKNOWLEDGMENT

The author would like to thank Dr. T Chown, University of Southampton, for his guidance and helpful comments throughout the writing of this paper.

#### REFERENCES

- [1] J. Postel, "Internet Protocol, DARPA Internet Program Protocol Specification," RFC 791, Sept. 1981.
- [2] T. Hain, "A Pragmatic Report on IPv4 Address Space Consumption," *The Internet Protocol Journal*, vol. 8, no. 3, pp. 2–19, Sept. 2005. [Online]. Available: [http://www.cisco.com/web/about/ac123/ac147/archived\\_issues/ipj.8-3/ipj.8-3.pdf](http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj.8-3/ipj.8-3.pdf)
- [3] D. Waddington and F. Chang, "Realizing the Transition to IPv6," *IEEE Communications Magazine*, vol. 40, no. 6, pp. 138–147, June 2002.
- [4] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460, Dec. 1998.
- [5] 6NET Deliverable, *An IPv6 Deployment Guide*, Oct. 2005. [Online]. Available: <http://www.6net.org/book/deployment-guide.pdf>
- [6] Y. Rekhter *et al.*, "Address Allocation for Private Internets," RFC 1918, Feb. 1996.
- [7] P. Srisuresh and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)," RFC 3022, Jan. 2001.
- [8] T. Hain, "Architectural Implications of NAT," RFC 2993, Apr. 2000.
- [9] M. Holdrege and P. Srisuresh, "Protocol Complications with the IP Network Address Translator," RFC 3027, Jan. 2001.
- [10] G. V. de Velde *et al.* (2005, Oct.) IPv6 Network Architecture Protection. IETF Internet draft. [Online]. Available: <http://www.ietf.org/internet-drafts/draft-ietf-v6ops-nap-02.txt>
- [11] B. Carpenter, "Internet Transparency," RFC 2775, Feb. 2000.
- [12] T. Narten and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6," RFC 3041, Jan. 2001.
- [13] T. Chown. (2005, Oct.) IPv6 Implications for TCP/UDP Port Scanning. IETF Internet draft. [Online]. Available: <http://www.ietf.org/internet-drafts/draft-chown-v6ops-port-scanning-implications-02.txt>
- [14] S. Thomson and T. Narten, "IPv6 Stateless Address Autoconfiguration," RFC 2462, Dec. 1998.
- [15] B. C. Steven M. Bellovin, Angelos Keromytis, "Worm Propagation Strategies in an IPv6 Internet," *LOGIN*, vol. 31, no. 1, pp. 70–76, Feb. 2006. [Online]. Available: <http://www.cs.columbia.edu/~smb/papers/v6worms.pdf>
- [16] P. S. E. Davies, S. Krishnan. (2006, Mar.) IPv6 Transition/Co-existence Security Considerations. IETF Internet draft. [Online]. Available: <http://www.ietf.org/internet-drafts/draft-ietf-v6ops-security-overview-04.txt>
- [17] G. Malkin and R. Minnear, "RIPng for IPv6," RFC 2080, Jan. 1997.
- [18] C. Zou *et al.*, "Routing Worm: A Fast Selective Attack Worm Based on IP Address," in *Proceedings of the 19th ACM/IEEE/SCS Workshop on Principles of Advanced and Distributed Simulation (PADS'05)*, June 2005, pp. 199–206.
- [19] A. Kamra *et al.*, "The effect of DNS delays on worm propagation in an IPv6 Internet," in *Proc. IEEE of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 4, Mar. 2005, pp. 2405–2414.
- [20] R. Hinden and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture," RFC 3513, Apr. 2003.
- [21] S. Convery and D. Miller. (2004, Mar.) IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0). Cisco Systems. [Online]. Available: <http://seanconvery.com/v6-v4-threats.pdf>
- [22] A. Conta and S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification," RFC 2463, Dec. 1998.
- [23] W. S. T. Narten, E. Nordmark, "Neighbor Discovery for IP Version 6 (IPv6)," RFC 2461, Dec. 1998.
- [24] B. H. S. Deering, W. Fenner, "Multicast Listener Discovery (MLD) for IPv6," RFC 2710, Oct. 1999.
- [25] R. Vida and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6," RFC 3810, June 2004.
- [26] S. D. J. McCann and J. Mogul, "Path MTU Discovery for IP version 6," RFC 1981, Aug. 1996.
- [27] E. Davies and J. Mohacsi. (2006, Mar.) Best Current Practice for Filtering ICMPv6 Messages in Firewalls. IETF Internet draft. [Online]. Available: <http://www.ietf.org/internet-drafts/draft-ietf-v6ops-icmpv6-filtering-bcp-01.txt>
- [28] K. C. Colleen Shannon, David Moore, "Beyond Folklore: Observations on Fragmented Traffic," *IEEE/ACM Transactions on Networking*, vol. 10, no. 6, pp. 709–720, Dec. 2002.
- [29] P. T. G. Ziemba, D. Reed, "Security Considerations for IP Fragment Filtering," RFC 1858, Oct. 1995.
- [30] I. Miller, "Protection Against a Variant of the Tiny Fragment Attack," RFC 3128, June 2001.
- [31] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," RFC 2827, May 2000.
- [32] R. Droms *et al.*, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," RFC 3315, July 2003.
- [33] E. N. P. Nikander, J. Kempf, "IPv6 Neighbor Discovery (ND) Trust Models and Threats," RFC 3756, May 2004.
- [34] M.-E. Kim and D. il Seo, "The Study on Secure Auto-configuration Technology in IPv6," in *Proc. IEEE of the 7th International Conference on Advanced Communication Technology, 2005. ICACT 2005.*, vol. 1, Feb. 2005, pp. 85–88.
- [35] B. Z. P. N. J. Arkko, J. Kempf, "SEcure Neighbor Discovery (SEND)," RFC 3971, Mar. 2005.
- [36] R. Draves and D. Thaler, "Default Router Preferences and More-Specific Routes," RFC 4191, Nov. 2005.
- [37] R. Droms and W. A. (Ed.), "Authentication for DHCP Messages," RFC 3118, June 2001.
- [38] S. Hagen, *IPv6 Essentials*. 1005 Gravenstein Highway North, Sebastopol: O'Reilly & Associates, 2002.
- [39] B. Carpenter and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds," RFC 3056, Feb. 2001.
- [40] P. Savola and C. Patel, "Security Considerations for 6to4," RFC 3964, Dec. 2004.
- [41] P. Savola. (2003, Mar.) Firewalling Considerations for IPv6. IETF Internet draft (Expired). [Online]. Available: <http://www.watersprings.org/pub/id/draft-savola-v6ops-firewalling-01.txt>
- [42] Zagar and D. Vidakovic, "IPv6 Security: Improvements and Implementation Aspects," in *Proc. IEEE of the 8th International Conference on Telecommunications, 2005. ConTEL 2005.*, vol. 1, June 2005, pp. 29–34.
- [43] R. Garcia, "SotM Scan28 - IPv6 Tunneling on a Solaris Sparc," May 2003, unpublished. [Online]. Available: <http://www.honeynet.org/scans/scan28/sol/official/index.html>
- [44] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, Nov. 1998.
- [45] J. Loughney, "IPv6 Node Requirements," RFC 4294, Apr. 2006.
- [46] D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)," RFC 2409, Nov. 1998.
- [47] C. Rigney *et al.*, "Remote Authentication Dial In User Service (RADIUS)," RFC 2865, June 2000.
- [48] A. G. S. R.M. Lopez, G.M. Perez, "Implementing RADIUS and diameter AAA systems in IPv6-based scenarios," in *Proc. IEEE of the 19th International Conference on Advanced Information Networking and Applications, 2005. AINA 2005.*, vol. 2, Mar. 2005, pp. 851–855.
- [49] G. L. Millan *et al.*, "Deploying Secure Cryptographic Services in Multi-domain IPv6 Networks," in *Proc. IEEE of the 19th International Conference on Advanced Information Networking and Applications, 2005. AINA 2005.*, vol. 2, Mar. 2005, pp. 785–789.
- [50] M. Li, "Policy-based IPsec management," *IEEE Network*, vol. 17, no. 6, pp. 36–43, Dec. 2003.
- [51] S. Ioannidis *et al.*, "Implementing a Distributed Firewall," in *ACM Conference on Computer and Communications Security*, Athens, Greece, Nov. 2000.
- [52] J. P. Stenbit. (2003, June) Memorandum for Secretaries of the Military Departments: Subject: IPv6. US Department of Defense. [Online]. Available: <http://www.dod.gov/news/Jun2003/d20030609nii.pdf>