

Got IPv6 Proxy?

Qing Li

Blue Coat Systems, Inc.



A proxy does your organization good, especially the ones with IPv6 capabilities. A proxy by definition is an intermediary that is situated between a requestor and a responder of a transaction. There exist various types of proxies. In Web access a proxy is well-known for its caching capabilities to reduce information access latency and bandwidth consumption. A proxy that is located in front of a group of origin servers, which is known as a reverse proxy or surrogate offers load balancing capability and hides the identities of those servers. In addition to the caching functionality, proxies provide many other types of services

including user authentication, connection acceleration, redirect, request and response filtering, access logging, translation and transcoding, virus scanning and spyware removal. For example, a proxy can accelerate SSL connections by offloading computation intensive cryptographic operations to the built-in crypto hardware; a proxy can translate web page content from one language into another before presenting the information to the user; a proxy can perform compression and decompression over slow or cost sensitive links. Proxies are also known to act as provisioned service access points to traverse firewalls. An intelligent information security proxy is a complex network appliance that is comprised of both hardware and software, which facilitates the construction of intelligent and fine-grained policy rules, and is the ultimate enforcer of those policies. The transition of an intelligent proxy from the IPv4 domain to the IPv6 world is not a straightforward syntactical conversion; rather, the transition requires thorough analysis of the necessary information security policies and the underlying protocols in the context of IPv6 semantically.

In IPv4, when nodes reside behind NAT devices, applying IPSec to traffic in the private realm is problematic for various technical reasons. For example, the IPSec Authentication Header (AH) offers data integrity on all immutable fields of the entire IP packet. The source and destination addresses are considered as the immutable fields. Therefore, modification by NAT or NAPT will result in packet integrity validation failure. The IPSec Encapsulating Security Payload offers both confidentiality and integrity protection for a packet, and differs from AH in that ESP does not cover the outer packet header. Encrypting upper layer payload renders NAPT incapable of extracting port information that is necessary in performing the packet translation. Automatic keying for Security Association (SA) setup and subsequent re-keying either cannot function or would reach incorrect outcome without proper NAT traversal techniques, especially with dynamic NAT. IPv6 expands the perimeter of the edge network to individual nodes when valid global prefixes are distributed throughout the autonomous system. Allowing individual nodes to acquire globally unique IPv6 addresses challenges proxy designers and organizations, which want control over information flow to reconsider many design, implementation and deployment issues that have been either solved or have workaround solutions in IPv4. The ability of an IPv6 node to set up a secure tunnel to the outside world, in which any type of traffic can stream through, is nothing short of a security breach and is an indisputable liability. The problem with encrypted tunnels is not unique to IPv6; however, IPv6 amplifies this problem multifold. Therefore, performing interception at the key exchange phase is a necessary step in tapping the secure tunnels.

Traffic interception is the key to realizing advertised services for any proxy. Transparent interception is not always possible for certain types of traffic flows and largely depends on the

level of sophistication of the deployed proxy. For example, a secure proxy must intercept IKE exchanges in order to intercept and terminate a VPN connection. Interception is possible during the main mode exchange, when the keying material used for authentication, confidentiality protection and Phase-II key generations is derived from either public key signature or public key encryption, but is impossible when a pre-shared key is in force. Another example: during SSL Handshake protocol exchanges a proxy can masquerade as the origin server and hand out a certificate for authentication. Transparent interception is difficult at best because this certificate needs to be either in the list of each client, or such a certificate must be verifiable through a valid CA by the client. The first option is not scalable and the second option defeats transparency. Therefore, some traffic flows must be stopped at the firewall, period. There exist expectations on increased IPSec traffic with the deployment of IPv6. Such predictions, if true, will certainly place demands on secure proxies, which are seldom seen today in operations.

An IPv6 proxy still needs to plug those security holes created by the covert communications channels such as HTTP tunnels and secure port forwarders. For example, a typical firewall tends to open port 80 to allow for HTTP traffic. Spyware and Trojan horses punch through firewalls by exploiting this common default rule. An intelligent IPv6 proxy must examine the HTTP POST and CONNET requests and determine appropriately whether to allow or deny such traffic according to the set policy rules. Designing good filters requires both heuristics and ongoing training through analysis and detailed real-time logging. A proof of concept program has shown that the IPv6 Destination options can be exploited as a covert channel. IPv6 changes the landscape of policy definitions and semantics. For example, with IPv6 automatic address generation the old policy rules that were based on specific IPv4 addresses require rethinking. In nodes that are running dual stacks, new rules need to allow for protocol preference when a proxy terminates connections and reinitiate outgoing connections on behalf of the clients. Similarly, an organization that acquires IPv6 services from multiple ISPs needs to implement address preference rules.

Ultimately, the question is: "Are you prepared to deploy IPv6 without opening doors and giving away keys?" I will continue this discussion in future issues of the 6Sense Newsletter.
