Still Using Proxies for URL Filtering?
There’s a Better Way

October 2013
The Arrival of Proxies

Firewalls enforce network access via a positive control model, where only specific traffic defined in policies is granted access to the network while all other traffic is denied. Access Control Lists (ACLs) initially performed this functionality, often in routers, but their rudimentary approach gave way to dedicated packet filtering and stateful inspection firewall devices that offered deeper levels of access controls. Unfortunately, these traditional firewalls shared a common shortcoming—an inability to see all of the applications traversing the network across all ports and protocols. The use of proxy-based devices began providing more granular visibility into a small set of applications and protocols where traditional firewalls were blind.

A proxy solution—either in the form of software on a specific server or a dedicated network appliance—acts as a middleman sitting between the source and destination of the traffic. The proxy intercepts and terminates the application session connections for a limited number of applications and protocols, and then re-initializes those connections to the originally targeted destination. This process allows the proxy to forward specific traffic and execute security decisions, like scanning files for viruses or deciding which website a user is permitted to access.

Many organizations deployed proxy-based devices simply to gain a degree of visibility and control over web traffic because their stateful firewalls lacked this critical capability. Those who added dedicated proxies in conjunction with their existing legacy firewalls now had access to security functions such as URL filtering, and web acceleration via proxy caching.

Times Have Changed Though

Over time, proxy-based devices evolved to become part of a growing collection of security “helpers”, just like dedicated intrusion prevention systems (IPS) and antivirus (AV) scanning boxes. Each “helper” has a limited view of network traffic though, and a standalone proxy-based URL filtering device is no exception. Not only is it yet another device to manage, but also when proxies are deployed as URL filtering devices, they are too narrowly focused on specific traffic to identify all of the web traffic and modern applications flowing through the network.

In addition, the historical benefits of implementing a proxy URL filtering solution have become muddied. For example, features on proxy-based devices have expanded to include web caching for performance—but web content has become so dynamic in recent years that caching really only holds a small percentage of a web page’s up-to-date content. Lately, with the dramatic increase of connectivity speeds combined with the dropping prices for Internet bandwidth, the importance of a proxy caching function becomes less relevant too.

The fact is, many organizations still find benefit with their proxies—despite some fundamental problems. With the exploding growth of new web- and network-based applications, coupled with the changing threat landscape, those organizations have an opportunity to reevaluate the reasons they originally implemented proxies. Network security experts consider the following to be several of the primary problems that proxy-based products and standalone URL filtering present.

Problems With Proxies and Standalone URL Filtering

Lack of Context

A standalone, proxy-based URL filtering solution remains to this day an isolated, disconnected tool—partially because it has an incomplete view of all network traffic, and due to its limited role among other security devices on the network. Its primary mission is to receive web traffic from other devices, like a firewall, and classify the requests into defined groupings of websites, or URL categories for policies to either permit or deny user access. Information learned from policy actions taken by this proxy-based device and other security devices lack integration though. For example, administrators are unable to build granular, comprehensive network security policies using a standalone URL filtering device. The URL device simply cannot factor into its policies all of the connection logs on the firewall, malicious files seen by an AV device, nor threats encountered by an IPS box. Without a centralized view of the connections and activities witnessed by each separate device, network and security administrators are left with islands of information that lack context.
In addition, this lack of context comes at a price—literally. Ongoing maintenance support contracts, costly equipment upgrades, and per-user licensing fees eat up precious IT security budgets, however the security team doesn’t gain any additional perspective into what’s happening on their network for that money.

Lack of Visibility Across All Ports and Protocols
The list of applications and protocols supported by most proxies is limited to a handful of applications (e.g. messaging and media streaming) and specific protocols, e.g. HTTP (port 80), HTTPS (port 443), and FTP (port 21). As such, proxy-based devices are unable to differentiate between applications that run across different protocols, plus they cannot identify applications using non-standard ports. Many applications appear web-based by design, using ports 80 or 443, helping ensure successful connectivity through port-based firewalls and delivering an improved user experience. From a security standpoint though, since the proxy-based device lacks visibility across all ports and protocols, it cannot precisely identify—or make policy decisions on—all of the applications traversing those two opened ports. Similarly, some applications, like Skype and BitTorrent, are capable of dynamically seeking out and utilizing any available ports on the network. Implementing port hopping techniques allow these applications to bypass the limited visibility and security capabilities of proxy-based devices.

Not only are proxy-based URL filtering devices blind to applications, they’re also limited in their ability to protect against evasive techniques. End-users have a myriad of tools at their disposal that can allow them to easily bypass traditional URL filtering methods and proxy-based devices. Examples range from public, open proxy servers like PHProxy or CGIproxy, to ProxEasy, Guardster and other anonymizing applications. In addition, traffic encryption has also made it relatively easy for determined end-users to hide their true application usage within Secure Shell (SSH) tunnels, SOCKS proxies, and via applications such as Tor and Hamachi. In fact, a knowledge base article from one security vendor openly admits their proxy-based solution is unable to block the security circumvention tool, Ultrasurf, due to the fact the Ultrasurf client dynamically switches from TCP to UDP traffic while it attempts to connect to the Ultrasurf network.

Slow Performance
Performing security functions has traditionally been computationally intensive work, but proxy-based devices require significantly more computing resources due to the demanding workloads of the additional proxy connections being established between the source client, the proxy device, and the destination server. These processing demands, along with the latency introduced with proxied connections, have relegated proxy-based devices to be deployed where rapid throughput and high scalability are not key requirements. Confining the placement of proxies to a small portion of traffic on the network can help; otherwise the entire organization’s network performance may suffer.

Slow Application Development
Proxy-based products struggle to keep pace with the rapid development of new applications and updates of existing applications or protocols. Creating a new application proxy is a very involved process, requiring development efforts ranging from months to years for some vendors. New protocols or applications must be brought in and analyzed to fully understand how the client and server transactions, along with their responses, are handled. Traditionally the containing protocol requires its own dedicated proxy for the connection; otherwise a vendor faces the difficult challenge to build a proxy that attempts to recreate all possible scenarios. Then after being modeled and re-created in the proxy, the new application proxy must be tested repeatedly to gain a level of confidence that it will not break connections or negatively impact the application it was designed to support. With all of this time and effort, proxies simply can’t scale appropriately to keep pace with the highly dynamic content of the Internet and Web 2.0 applications that continually undergo updates and improvements.
Complex Implementations

To be an effective tool for the purposes of filtering web traffic, all users across the organization must have their traffic and connection requests steered to the proxy-based device. There are two primary methods of performing proxy forwarding, but they both involve complex implementations and include unique challenges.

Explicit Proxies

Explicit proxy deployments require an IT organization to configure the web browsers on every laptop and workstation in their enterprise to ensure that web traffic is pointed to the proxy appliance or security device. Many enterprises deploy proxy auto-configuration (PAC) files using manual methods, system policies enforced by Microsoft Global Policy Object (GPO), or via web proxy auto-discovery (WPAD) protocol. However, a misconfigured WPAD file could allow an attacker to redirect a user’s machine toward a malicious configuration file, while too restrictive of a GPO can result in an increase of IT trouble tickets submitted by frustrated users. Organizations face additional challenges when they don’t own or control an endpoint, like mobile devices, which can be used to bypass corporate proxy policies.

Implicit Proxies

Implicit, or transparent proxy deployments add complexity, latency, and include additional equipment to manage, all for a partial view of traffic on the network. Implicit proxies typically involve IT organizations that reconfigure their switches and routers to use Web Cache Communication Protocol (WCCP) for steering web traffic directly to the proxy appliance. Many proxy appliances pass off certain inspection tasks, e.g. AV scanning, via Internet Content Adaptation Protocol (ICAP) to an additional, separate appliance. Not only does this add to the complexity, it becomes yet another tool that requires another management console. The entire process impacts performance while the proxy device takes time to forward traffic to the AV scanning appliance and holds the connection open awaiting a response on whether to allow or deny that traffic.

Deploying Palo Alto Networks® to Solve Proxy Problems

Organizations shouldn’t employ a security solution that is incapable of seeing all network traffic, lacks context, impacts network performance, is difficult to implement and maintain, and is unable to prevent users from bypassing the intended security enforcements. Fortunately, Palo Alto Networks® focuses on understanding the challenges of network security, for all enterprises, both big and small. Palo Alto Networks built a network security platform from the ground up which tackles the fundamental problems associated with proxy-based security solutions, including standalone URL filtering.

A Comprehensive Platform

The Palo Alto Networks next-generation security platform—a combination of next-generation firewall and threat prevention technologies—delivers visibility into, and control over applications, users, and content for enterprise data networks. Tightly integrated technologies, such as App-ID™ and User-ID, identify the applications in use along with who the user is, while Content-ID and WildFire™ technologies continually look for and block threats inside the application traffic. Security administrators are empowered to create logical, application-based security policies using these technologies to classify all of their traffic by applications, users, and content—exactly where traditional firewalls and “helpers” are blind. Most importantly, the first task executed by Palo Alto Networks security platforms is determining the precise identity of the application regardless of port, protocol, or evasive technique employed; the identity then becomes the basis of the firewall security policy. Palo Alto Networks platforms are continually updated with information on the latest applications and threats, along with malware details collected by the WildFire cloud-based virtual environment.

Deploying network security technology from Palo Alto Networks is easy, and doesn’t require a bunch of different “helper” boxes or standalone devices such as traditional URL filtering. With a single policy, all of Palo Alto Networks security profiles, which provide additional protection and control, can be brought to bear against that policy’s traffic such as URL filtering, antivirus, and vulnerability protection. An administrator simply specifies one or more security profiles within the management console, creating fine-grained security policies.
The Palo Alto Networks platform sees all of the traffic on the network due to its ability to sit in place of a traditional firewall. Palo Alto Networks security platforms offer flexible Layer 1 (Virtual Wire), Layer 2, and Layer 3 deployment modes along with a rich set of networking features (including static and dynamic routing capabilities), allowing network engineers to easily insert the network security platform into any existing network architectural design. Predictable, high-speed performance is achieved through a combination of a single-pass software engine, along with a purpose-built hardware platform that uses function-specific processing for networking, security, threat prevention, and management functions.

**Using Dynamic, Contextual Policies—It’s Not Just About URL Filtering**

Complete visibility and control over applications, users and content arm security administrators with meaningful data points to use in creating dynamic, contextual policies. In contrast, standalone traditional URL filtering devices only see a small portion of network traffic and focus solely on classifying websites into defined URL categories. They lack the shared intelligence which Palo Alto Networks technologies provide IT organizations.

The Palo Alto Networks URL filtering security profile works alongside all other integrated technologies and available security profiles, thereby creating a complete threat protection framework, using context gained from the network traffic. For example, Palo Alto Networks App-ID technology perfectly complements the URL filtering security profile to enforce control of network activity, while preventing the use of URL filtering avoidance tools. Identifying the application, who the user is and where they’re coming from is a powerful capability in policy enforcement, especially when combined with URL filtering and threat prevention security profiles. Ultimately, this liberates security administrators to create policies that safely enable traffic, versus simply blocking or allowing traffic for a specific URL category.

**Real-World Policy Examples**

The following are several policy examples using next-generation security technologies already designed into the Palo Alto Networks next-generation security platform. Going far beyond simply “blocking” or “allowing” web requests, these granular policies enable businesses to protect their network and conduct work safely.

- Authorize Internet access, for specific individuals or groups via App-ID and User-ID, except connections to servers in certain geographical regions or “Malware” categorized websites—preventing user devices from connecting to known malware and phishing download sites
- Implement SSL decryption policies with URL filtering security profiles so that all websites categorized as “Financial Services” remain encrypted, yet traffic to known malware sites is decrypted—preserving a reasonable sense of privacy for users’ banking information while securing traffic
- Grant certain users with access to online storage tools through a URL category, but apply file blocking security profiles to prevent the upload of Microsoft documents or the download of executable files—controlling sensitive company information and potential malware
- Allow media streaming per the URL category, but explicitly block Netflix or BBC iPlayer application usage via App-ID—saving bandwidth and preventing misuse of employee time
- Throttle access during peak times of popular, momentary occasions, e.g. Olympic events or FIFA World Cup matches, for certain users or groups via User-ID, quality of service (QoS), and customized App-ID signatures—balancing business-related usage with workplace culture
Customer Stories

No Longer Needed Their Proxies

A top technology provider for a global consulting firm currently protects approximately 8,000 users via a High Availability (HA) pair of Palo Alto Networks PA-5020 security platforms at their network perimeter. These appliances integrated smoothly with the customer’s existing high-speed switching gear, and were placed in front of their standalone, proxy-based URL filtering devices. Seven months after having deployed their Palo Alto Networks security platforms, the network design consultant realized that their proxy appliances hadn’t been logging any security alerts. Upon investigation they realized the Palo Alto Networks equipment were catching all of the malware and continued to protect their network against threats.

The customer carefully considered the situation and then decided to disconnect their proxy-based appliances (see Diagram 1) and de-commissioned them. This decision simplified their network architecture by eliminating the devices with the proxy technology, but also saved the company operational and capital expenses by avoiding pending support renewal costs along with future upgrades of unnecessary proxy hardware.

Diagram 1: Palo Alto Networks deployed in front of existing proxy solution on a customer network.

A True Solution Shouldn’t Take Forever

A Canadian organization with one thousand employees in the energy industry struggled with implementing their proxy devices into their network environment. They spent an entire year toiling with their proxies using a WCCP implementation, but couldn’t get it to work to their satisfaction—resulting in six to seven use cases they never fully solved. Palo Alto Networks approached this oil and gas company and offered an evaluation platform as a solution. Installing the equipment using a Layer 1 (Virtual Wire) deployment mode, the Palo Alto Networks engineer was able to solve all of the company’s proxy problems they spent a year wrestling with—in just half a day. This compelling demonstration convinced the customer to purchase several Palo Alto Networks hardware platforms for each of their office locations, and they opted to manage them with a Palo Alto Networks Panorama central management console.
Reevaluate Your Original Proxy Requirements

As applications and threats continue to evolve, it becomes increasingly difficult for some organizations to secure their networks without getting in the way of their employees conducting business. Challenges unfold as diverse users roam the network with an assortment of company-owned and personal devices, accessing new types of applications that communicate across many different network ports and protocols. Although proxy-based devices provide support to the original capabilities of traditional firewalls with an added degree of visibility and control over web traffic, that visibility is restricted to a limited number of protocols such as HTTP (port 80) and HTTPS (port 443). Palo Alto Networks delivers a next-generation network security platform to secure enterprise networks, utilizing dynamic policies that take advantage of the context shared between applications, users and content gleaned from the platform’s central location within the network. The platform provides complete network visibility to apply fine-grained security over an organization’s users and safe enablement of their applications—regardless of ports, protocols, or evasive techniques. Implementing next-generation security and threat prevention technologies from Palo Alto Networks can give IT organizations the confidence to reevaluate their original requirements for utilizing proxy-based devices, like standalone URL filtering solutions. Contact your Palo Alto Networks authorized reseller to learn more information and arrange an online or in-person demonstration.