CENTRIPETAL
NETWORKS

Using RuleGate® Network Protection System to Accelerate Cyber Defense

A Technical White Paper
Centripetal Networks, Inc.

Using RuleGate® NPS to Accelerate Cyber Defense

A Technical White Paper
Centripetal Networks, Inc.

Summary:

Conventional cyber defenses – network firewalls, routers, web proxies, and intrusion prevention systems (IPS) – are rapidly losing effectiveness as the size, power, and dynamics of the cyber threat increase at a prodigious rate. Today, there exists asymmetry between cyber defenses and cyber threats. The core problem is these defenses have reached the limits of their scalability. Disruptive technologies are needed to accelerate these defenses past their scale barriers. In particular, the performance of TCP/IP packet filtering technology needs to improve by several orders of magnitude (1000X or more). Packet filters located at network security boundaries – Internet access points, peering points, etc. – need to be able to enforce highly dynamic security policies with millions of rules, but without impacting network performance and users' quality of experience. The RuleGate® packet filter from Centripetal Networks Inc. (CNI) meets these performance specifications. RuleGate devices are readily combined with conventional defenses to accelerate existing cyber security infrastructure. The result is a cyber security arsenal that scales to the size of the threat and reverses the asymmetry to the defenders' advantage.

The Asymmetric Cyber War

Cyber criminals are winning the Internet cyber war. Millions and millions of computers are infected by malware. Small, unfunded teams of attackers can easily disrupt the operations of government, military, utilities and banking/financial organizations. Many experts believe that it is not only possible but also probable that a hostile government or terrorist organization could launch a massive cyber attack, potentially disabling US Internet infrastructure.

Despite large investments in cyber defense, the asymmetry of cyber warfare continues to grow. Although the reasons span legal, political, business and economic domains, the most fundamental reason is that conventional cyber defense technologies simply do not scale nor adapt to the size and dynamics of the threat.

However the cyber threat may be characterized and measured, it is at least 1000X larger than the practical limits of conventional defenses. For example, an intrusion prevention system (IPS) may apply several hundred or a few thousand malware detecting signatures to packet traffic; whereas, several hundred million malware variants are known to exist. Thus, in this case, the size of the threat is approximately one million times larger than the size of the defense. Increasing computational resources to match the scale is obviously impractical. Scale-disruptive cyber technologies are needed to defend against the threat and to reverse the asymmetry of cyber warfare.

Disruptive Scalability of the RuleGate® Network Protection System

A disruption in the scalability of packet filtering technology is the simplest and most effective first step in next-generation cyber defense. A packet filter examines packets traversing a network link and compares the values of certain IP packet header fields – source and destination IP addresses (which computers are communicating), source and destination ports (which application is in use) and transport protocol type – to a database of filtering rules (called a policy). If a packet matches a rule, then the rule's packet handling action is applied, either to BLOCK/drop the packet or ALLOW/forward the packet to its destination. Conventional packet filters have practical limits on policy size of approximately 10,000 rules; when the limit is exceeded, then network performance – as measured by additional latency (delay) and packet loss – degrades to levels that are unacceptable to users. For reference, large e-commerce operations consider an average increase in latency of one millisecond to be too much (one millisecond equals one million dollars in lost business), and live videoconferencing becomes unusable when packet loss rates exceed 1 percent.

The RuleGate packet filter from CNI shatters the scale barriers. Testing (RFC 2544) by US Department of Defense laboratories has shown that the RuleGate can apply million-rule policies to 10Gbps packet traffic while incurring only a few microseconds of latency and no packet loss. The RuleGate readily scales to policies composed of millions of rules. Because the size of the

known threat (known malware servers, spam servers, cyber-crime networks, hostile/ITAR country networks, etc) is several hundred thousand IP addresses, and the estimated size of the suspected threat is 2-5 million, then clearly the RuleGate is able to scale to the size of the threat. By integrating the RuleGate with automated threat intelligence services – such as CNI's Advanced Cyber Threat™ (ACT) service, services available from CNI partners, and/or internal services – the generation, management, maintenance and enforcement of massively scaled, cyber defense policies can be fully automated.

RuleGate NPS Accelerates Cyber Defense Technologies to the Scale and Dynamics of the Threat

RuleGate devices by themselves can provide by far the best network security available, because of their massive scalability and broad coverage of the Internet threat surface. However, current cyber defense systems should not be discarded and replaced with RuleGate devices. Instead, RuleGate devices should be combined with conventional defense systems, not only to further strengthen cyber defense, but also to enable conventional defense systems to dedicate their resources to performing their primary functions. In effect, the RuleGate accelerates conventional cyber defense systems.

Firewall Acceleration

Network firewalls are an essential component of any cyber defense system for enterprise networks. A firewall is typically located at the enterprise's Internet access points, in front of the DMZ where publicly accessible servers (e.g., e-commerce web servers) are located. The primary functions of the firewall is to (1) allow public Internet access to servers/services located in the DMZ while blocking unsolicited attempts from the Internet to access private resources (enterprise user desktops and internal business servers); (2) Allow inbound Internet traffic that was solicited by an internal user (or by malware); and (3) restrict outbound traffic to well-known ports (e.g., port 80 for web, port 53 for DNS, etc.).

All three functions, however, provide only weak protections from determined attackers, even when the IP addresses of attackers' computers are well known. Function 1 allows any (unsolicited) traffic, which is accessing the public servers. This includes traffic from known cyber criminal/hacker networks, and DDoS attacks using, for example, well-known bogon IP addresses DDoS attacks may even attack the firewall itself. Firewalls do not have the scalability to filter these known attacks – but the RuleGate does. By placing a RuleGate in front of the firewall, which filters the hundreds of thousands of known bad IP addresses, these inbound attacks can be highly mitigated. And, the firewall can dedicate its resources to Function 2 (managing users' sessions) to ensure good network performance for enterprise users. Function 3 (restrict outbound traffic well-known ports) in the firewall is the outdated method for preventing criminals from stealing data. It can be made effective only if filtering rules are added which block data transfers to known bad or suspicious destination sites. The RuleGate can provide this capability for firewalls and thus effectively prevent data stealing.

Thus, the RuleGate accelerates network firewalls by significantly enhancing the effectiveness of the firewall, mitigating the adverse impact on network performance, and greatly increasing overall network security.

Router Acceleration

IP routers have packet filters, called Access Control Lists (ACLs), embedded in their network interfaces. Router ACLs are typically used by Internet Service Providers (ISPs) and by large enterprises that operate their own switching centers interconnecting their geographically distributed satellite networks.

Internet Service Providers (ISPs) typically use ACLs to rate-limit traffic and to filter certain types of DDoS attack packets (packets with spoofed, bogon and martian addresses). However, policy size (the number of rules) must be limited (e.g. <10,000 rules) and rule complexity must be restricted to inspecting only source IP addresses so network performance degradation – latency and packet drops – is minimized. Also, because updating router ACL filter policies causes temporary loss-of-service (and loss-of-security), ISPs often filter with static (vs. dynamic) policies and therefore cannot efficiently adapt to changes in the cyber threat. Because of these

severe limitations on size, complexity and adaptability, the cyber security provided by ISPs via router ACLs is also severely limited. For example, many ISPs do not ingress filter for spoofed packets and bogon packets, even though such filtering has been deemed Best Practices by the Internet standards organization (IETF), and even though such filtering would eliminate many DDoS attacks launched against ISPs' subscribers.

Large enterprises typically use router ACLs to enforce corporate communications policies within the enterprise network (e.g., which internal hosts can use which internal servers), and to regulate Internet communications and prevent Internet-borne attacks. Similar to ISPs, however, enterprises must restrict policy size, complexity and adaptability in order to provide acceptable network performance and network availability to their users. Even with these restrictions, it is often quite difficult for enterprises to manage their router ACL policies. The result is that cyber security is limited and expensive, and corporate communications policies cannot be properly enforced and often cause loss of business functionality and continuity.

RuleGate devices support policy sizes, complexity, adaptability and manageability at levels that exceed the requirements for ISPs and enterprises, and without causing degradation in network performance. By accelerating router interfaces with RuleGate filters, ISPs can provide comprehensive cyber security protections to their subscribers. They can even provide revenue-generating managed security services for their subscribers. Similarly, enterprises can provide additional cyber security protections for their networks while properly enforcing corporate communications policies, reducing management and operational costs, and improving business continuity, network performance and users' quality of experience.

Web Proxy Acceleration

Enterprises uses web proxies to enforce corporate policies for web usage, i.e., to prevent users from accessing web sites that are not related to corporate business functions. Web proxies are typically located near enterprises' Internet access points so that all web browser requests can be filtered through a domain or URL blacklist containing domains (e.g., www.facebook.com) or URLs (e.g., www.dropbox.com/file/xyz.zip) for web sites that are not business-related. When cyber criminals began using the web to perpetrate their crimes using malware and phishing techniques, security-conscious enterprises began using their web proxies for cyber defense, simply by adding known cyber criminal web sites to the domain and URL blacklist. Today, however, the size of the web-mediated cyber threat has grown so large, and it evolves so rapidly, that web proxies simply can't keep up without severely degrading performance to unacceptable levels. Additionally, cyber criminals have invented numerous methods to easily subvert web proxies. One adverse effect of this situation is that web proxies cannot effectively provide their original function– enforcing corporate web usage policies – while also providing even low levels of cyber security.

RuleGate devices can accelerate web proxies by assuming all of the web cyber security responsibilities. RuleGate devices scale to the size of the web cyber threat and can immediately adapt in response to cyber threat evolution. Enterprises that accelerate their web proxies with RuleGate devices can focus on managing their corporate web usage policies while receiving vastly improved and fully automated web cyber security.

IPS Acceleration

An enterprise uses an Intrusion Prevention System (IPS) to detect inbound attacks, malware downloads, virus infection attempts, etc. An IPS detects cyber threats by correlating inbound packet traffic with a database of threat signatures. An IPS can be quite effective at detecting some complex attacks, but as with other cyber defenses, current IPS technology cannot scale and adapt to the current cyber threat. Also, the IPS is notorious for adversely affecting network performance. Part of the problem is that an IPS wastes much of its processing resources on detecting simple attacks. An IPS solution often includes a conventional network firewall to filter the simple attacks; however, as described above, firewalls do not scale or adapt to the size and dynamics of even the simple cyber threats.

RuleGate devices can readily accelerate an IPS. By assuming the IPS's firewall function, the RuleGate filters all of the known sources of cyber threats. The IPS's resources can be dedicated to detecting complex attacks, thereby accelerating its primary cyber security function. Furthermore, when the IPS detects an attack, it can provide the attack source information to the RuleGate, which will then block any future attack attempts. In effect, the IPS can self-improve its performance by using a RuleGate accelerator.

Conclusion

Conventional cyber defenses are overwhelmed by the size and dynamics of the current cyber threat. The RuleGate packet filter can scale and adapt to the threat, potentially reversing the current asymmetry in cyber warfare. RuleGate devices can be used to accelerate existing cyber security infrastructure and provide an overwhelming advantage.