The Impact of IP Access Control Lists on Firewalls & Routers - A business case for specalized nextgen perimeter security

The overwhelming majority of Spam, Malware, and DDoS attacks come from countries outside the United States and from infected machines in global Botnets. Small and mid size businesses are working to reduce the attack space by blocking IP addresses originating from countries that offer no business value, and by using IP reputation lists to block connections from IP addresses that are tied to malicious activity.

Often, the best place to block unwanted IP traffic is at the network perimeter. This is traditionally done with firewalls or routers by implementing large access control lists (ACLs). This approach has the following problems:

1. IP addresses assigned to countries change daily so they must be kept current to be effective.
2. Access lists often have tens of thousands of entries, taking 15 minutes a day to load.
3. Processing large ACLs can add unacceptable network latency and reduce the device's capacity to handle legitimate connections.

In addition to possible latency issues, labor costs, and the need for continual maintenance of country ACLs, you must contend with malicious actors operating in countries allowed by your policy. According to McAfee, the US was the top source of SQL attacks, and almost half of new botnet controllers reside in the United States[1]. In fact, the US has the greatest number of bot-infected computers of any country in the world[2]. Many of the offending IPs are known and can be blocked using IP reputation lists. The problem is commercial blocklists can contain millions of IP addresses, far exceeding the capacity of most firewalls and routers, and since botnets are globally dispersed, you remain open to attack from countries allowed by your policy.

Now the performance impact and administrative costs of loading ACLs into entry-level routers and firewalls has been quantified.

TechGuard's PoliWall® IP Blocker appliance was tested with the BreakingPoint Storm™ to measure product resiliency in the face of massive scale simulated cyber attacks from millions of users and hundreds of applications. The PoliWall blocks inbound and outbound traffic by country and by IP Reputation Block Lists for both IPV4 and IPV6 traffic at line-speed.

Tested with BreakingPoint Storm™

The testing environment included a typical SMB router and firewall, each with 100Mbit connectivity. These devices were paired with the entry-level PoliWall M10 appliance (MSRP of $3499). The products were chosen to demonstrate the PoliWall's capability to offload blocking of countries and known cyber-threats, while allowing the SMB devices to deliver maximum performance for their intended use. Additionally, the PoliWall added the capability to block threats from IP reputation lists containing millions of entries.

'By stopping needless foreign traffic and malicious IPs at the perimeter, the workload on systems deeper inside the network is decreased, making them more effective at stopping attacks', said Dave Maestas, CTO of TechGuard.

Testing Parameters

- The tests show latency and TCP throughput of the tested router and firewall with no rules for the baseline, and then with 'US Only' filtering rules containing over 12,000 unique IP ranges.
- The 'US Only' tests were then run again with the PoliWall offloading the country blocking.

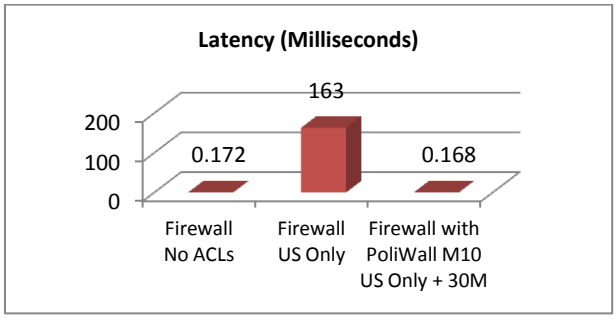
- ❖ Only the PoliWall was tasked with filtering an IP Reputation block list containing 30 million individual IP addresses since the number of entries exceeded the capacity of the router and firewall.

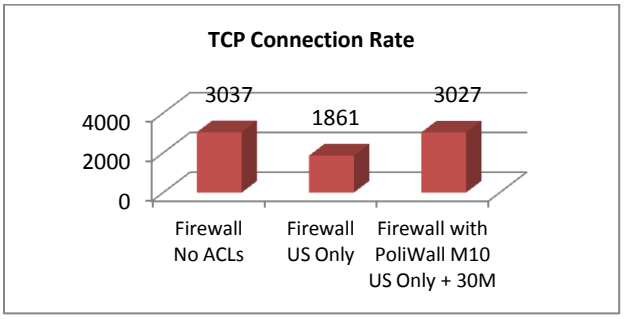
[1] McAfee Q1, 2012 Threat Report
[2] ThreatPost, US Reigns As Most Bot-Infected Country

Firewall Test

The baseline test used the BreakingPoint Storm device to generate TCP/IP sessions and measure packet latency and connection rate. The session test for the firewall device showed .172 milliseconds of latency with no access list loaded. When the 'US Only' filter rules were added to the firewall, latency reached 162.866 milliseconds, an increase of 9,000%, and the TCP connection rate dropped nearly 39%.

The PoliWall was then configured with a policy to allow only US traffic and block an additional 30 million IP addresses. After placing the PoliWall before the firewall, the packet latency impact was near zero (within ± 3% margin of error), and TCP connections remained at 99.6% of the baseline test. Under load, the PoliWall added effective IP blocking with virtually no latency and no negative impact on network performance, allowing the firewall to utilize its resources for other functions.

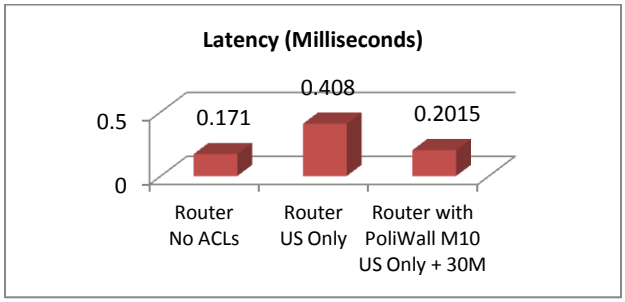


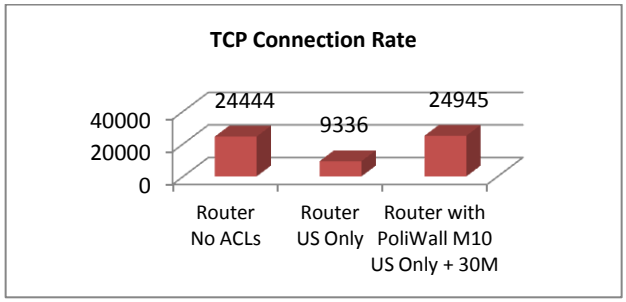


Router Test

The baseline router test also used the BreakingPoint Storm device to generate TCP/IP sessions and measure packet latency and connection rate. The session test for the router device showed .171 milliseconds of latency with no access list loaded. When the 'US Only' filter rules were added to the router, latency reached .408 milliseconds, an increase of 138%, and the TCP connection rate dropped 62%.

The PoliWall was then configured with a policy to allow only US traffic and block an additional 30 million IP addresses. After placing the PoliWall in the network, the packet latency increased by only .03 milliseconds, and TCP connections remained at 98% of the baseline test. Under load, the PoliWall added effective IP blocking with minimal latency and no negative impact on network performance.

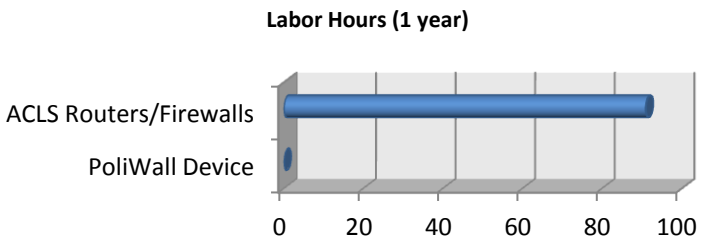




The Labor Factor

Additionally, there are labor costs involved in the configuration and maintenance of thousands of ACLs. Scripts must be run daily to download the address ranges assigned to countries and the IP reputation lists. This data must be converted into access lists for the router or firewall. Network administrators must manually apply the ACLs to the device–a process that can take 15 minutes a day. At $75 per hour, this can mean a savings of $6,800 a year.

Configuring and loading ACLs in a firewall/router will take an admin approximately 15 minutes each day. The PoliWall performs the daily update tasks automatically.



Specialized Perimeter Protection

PoliWall's High-Speed IP Packet Inspection Engine (HIPPIE®) filters stateful traffic to achieve near zero latency while maintaining high throughput and TCP connection rates for both inbound and outbound IPV4 and IPV6 traffic. The PoliWall belongs to a class of specialized security devices designed to work with existing routers and firewalls–adding new capabilities and increased performance.

PoliWall's automatic updating of IP ranges and block lists obviates the high labor costs associated with manually updating ACLs, makes blocking a country as simple as clicking on a geographic map, and keeps device configurations simple. For more information on the performance of all PoliWall devices tested with the BreakingPoint Storm visit the testing page on TechGuard's website.

PoliWall M10 by TechGuard

About TechGuard

TechGuard Security, LLC was founded in February 2000 to address National Cyber Defense initiatives and US Critical Infrastructure Security. TechGuard provides trusted and award-winning Cyber Security Solutions for the DoD, DHS, Federal, Financial, Energy and Healthcare communities. www.techguard.com | sales.636.489.2230