The Impact of IP Access Control Lists on Firewalls & Routers

A Business Case For Threat Intelligence Gateways

The volume of cyber attacks and threat indicators is massive and continues to grow. As a result, more organizations are leveraging threat intelligence to improve cyber defense. However, there is a significant challenge in putting threat intelligence into action because firewalls and routers were not built to effectively and efficiently handle the massive volume of known threat indicators. This leads organizations to either operate with a subset of threat indicators (i.e. increased attack surface) or suffer performance and management challenges as the threat indicator volumes taxes firewall and router processing and ACL management becomes a nightmare.

At Bandura, we saw this problem years ago leading us to pioneer the threat intelligence gateway (TIG) market with the development of our PoliWall solution. PoliWall is purpose-built to consume hundreds of millions of known threat indicators and to block known threats and unwanted traffic with virtually no latency before it hits the firewall. The 100+ customers that have deployed our PoliWall solution are seeing clear benefits including a significant reduction in attack surface and a significant improvement in the performance of and return on existing security investments, both technology and people.

A simple, but powerful, use case for our PoliWall TIG solution is use of our map-driven, best in class Country Blocking feature (also known as GEO-IP blocking). Country Blocking is about controlling traffic based on the country of origin. For example, if your company only does business in the U.S. then there may be no need to have traffic from China, Russia, etc. entering your network.

Country Blocking represents a subset of the broader IP blocking organizations must do to protect their networks, but it provides an excellent illustration of the challenges of IP blocking in firewalls and routers and the benefits of doing this with a threat intelligence gateway like PoliWall. We have customers who have tried to use the Country Blocking features in their firewalls and have found it to be cumbersome and all or none blocking. The PoliWall TIG offers an easy to use, robust Country Blocking solution, with granular exception capability that many clients are using to offload this from firewall and routers and simplify the process.

> *"By stopping unwanted 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"*
>
> **DAVE MAESTAS • CTO OF BANDURA SYSTEMS**

Challenges of Country Blocking Using Firewalls & Routers

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.

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 TIG offloading the country blocking.
- Only the PoliWall TIG 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.

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. While the U.S. remains a leading source of cyber attacks, the fact is a significant volume of cyber attacks originate from outside the U.S. In Akamai's State of the Internet Security Q4 2017 report, after the U.S., the Netherlands, China, Brazil, and Russia rounded out the top five source countries for web application attacks. 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 to consume and enforce based on the required high volume of indicators to protect your network.

© 2018 Bandura Systems. All rights reserved.

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

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

The testing environment included a typical SMB router and firewall, each with 100Mbit connectivity. These devices were paired with the entry-level PoliWall TIG. The products were chosen to demonstrate the PoliWall TIG'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 TIG added the capability to block threats from IP reputation lists containing millions of entries with threat indicators.

“By stopping unwanted 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 Bandura Systems.

Firewall Test

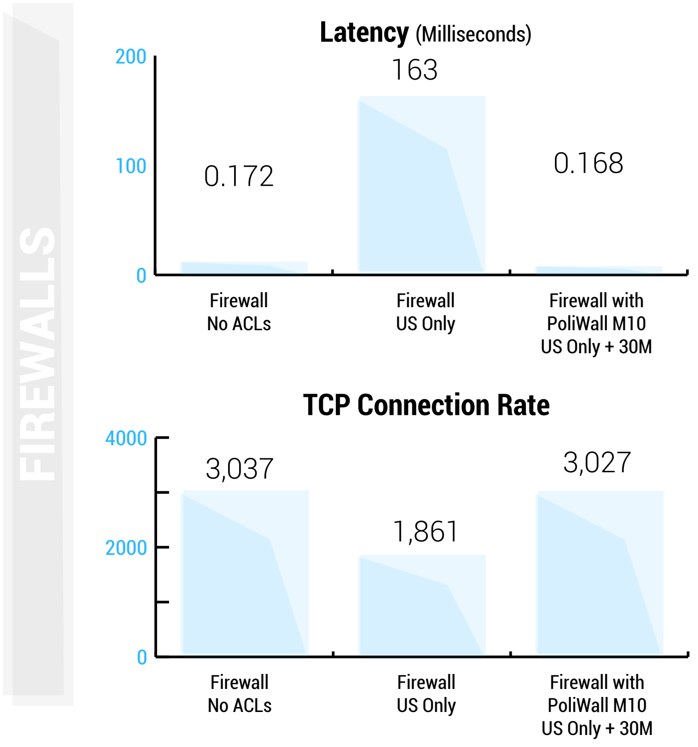
The baseline test used the BreakingPoint Storm device to generate TCP/IP sessions and measure packet latency and connection rate. The session test for the firewall device showed .172 milliseconds of latency with no access list loaded. When the 'US Only' filter rules were added to the firewall, latency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

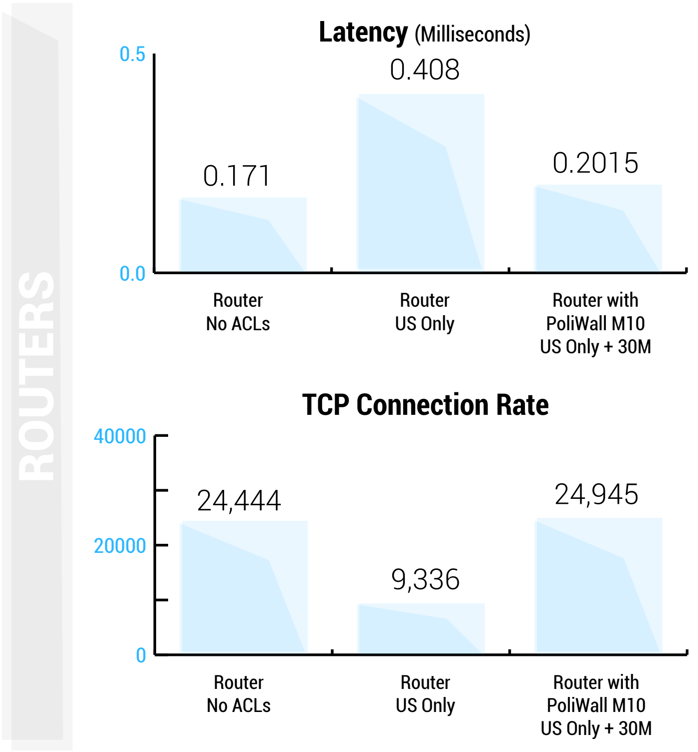
The PoliWall TIG was then configured with a policy to allow only US traffic and block an additional 30 million IP addresses. After placing the PoliWall TIG in front of the firewall, the packet latency impact was near zero (within ± 3% margin of error), and TCP connections remained at 99.6% of the baseline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

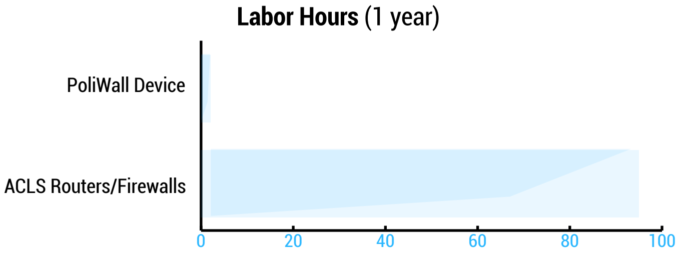




© 2018 Bandura Systems. All rights reserved.

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 TIG performs the daily update tasks automatically.

Specialized Perimeter Protection

PoliWall TIG'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 TIG belongs to a class of specialized threat intelligence gateways designed to work with existing routers and firewalls–adding new capabilities and increased performance.

PoliWall TIG'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.

© 2018 Bandura Systems. All rights reserved.