BANDURA CYBER

Position Paper

The Threat Intelligence Challenges with Next-Generation Firewalls

The Threat Intelligence Challenges with Next-Generation Firewalls

Today's networks are transforming at an unprecedented speed. Nation-state events and global crises are challenging every aspect of how business is conducted. Now more than ever, organizations are relying on their network infrastructure to maintain business continuity and support digital business initiatives. Unfortunately, one aspect of the digital economy that remains constant, is the threat to the network by cyber criminals. As they scramble to adopt new network paradigms, organizations continue to rely on their traditional security controls like Next-Generation Firewalls (NGFWs) to secure their businesses.

However, what many organizations are realizing is that their next generation firewalls are having a tough time keeping up with today's threats. To be fair, organizations require a lot from their firewalls, including dealing with increasing network traffic, threat volumes, encrypted traffic, and a never-ending array of functions they're asked to perform. However, there is a more fundamental challenge facing firewalls, that requires our attention, which is their reliance upon proprietary and closed threat intelligence to detect and block threats. Simply put, this means that they operate with too narrow a view of the threat landscape, and therefore struggle to keep up with today's attacks.

In light of this and in an effort to better secure their networks, organizations have increasingly adopted threat intelligence as a means to identify and respond to evolving threats. However, as organizations look to operationalize threat intelligence, they find it challenging to integrate threat intelligence into their next-generation firewalls.

When combined, the limitations of broad-based threat visibility and an inability to integrate threat intelligence at scale, represent two significant challenges for next-generation firewalls. In this whitepaper, we will provide an overview of these challenges, provide real world data, discuss why these challenges exist, and briefly describe how the Bandura Cyber Threat Intelligence Firewall platform eliminates these challenges.

Firewalls Rely On Proprietary & Closed Threat Intelligence

Cyber security vendors, especially mainstay, next-generation firewall vendors, have long advertised threat intelligence expertise as a differentiating value proposition beyond their product technology. It makes sense in an industry whose bread and butter relies on the ever evolving sophistication of cyber attacks. However, with so many different vendors, institutions, and government entities engaged in the pursuit of threat intelligence, its definition has become muddled. This has resulted in confusion around both the definition of what constitutes threat intelligence, as well as its uses.

Next-generation firewalls are powered by threat intelligence. However, the threat intelligence they use is wholly controlled by the vendor, and is typically both proprietary and closed. The threat intelligence they use to detect and block threats is predominantly based on threat activity they see within their own customer base supplemented by analysis from their internal “Intelligence” teams. Make no mistake, this threat intelligence is valuable. However, it alone is insufficient to protect organizations from today’s dynamic threats, because it provides too narrow a view of constantly evolving threat activity. Simply put, it’s just one vendor’s perspective.

Fortunately, the challenges with relying on single source threat intelligence are well known. For this reason, more organizations are supplementing the threat intelligence they get from existing controls with a broad-based view of threat intelligence that spans multiple, diverse sources. These sources include commercial threat intel providers like DomainTools, IntSights, Recorded Future, and others, open source threat intel (OSINT), government providers like DHS, and industry sharing communities like ISACs/ISAOs. This broad-based view of threat intelligence enables organizations to better protect themselves from cyber threats.

Firewalls have Limited Ability to Integrate Third-Party Threat Intelligence

As organizations invest more in threat intelligence, they logically look to maximize its value by making it actionable thereby using that intelligence to detect and block threats. To make threat intelligence actionable, organizations first look to integrate it into existing security controls like firewalls. However, it doesn't take long to realize the significant challenges that exist here.

The fact is, next-generation firewalls don't "play nicely" with third-party threat intelligence. These legacy devices have significant limitations with respect to the volume and ways that third-party threat intelligence can be integrated. Volume limitations can include the total volume of third-party indicators, the size of external blocklists, and/or the number of lists that can be used. Firewalls also have significant limitations in the ways third-party threat feeds can be integrated into them with most firewalls only having the ability to consume text file lists of indicators over HTTPS. While some firewall providers have broadened their integration abilities to support standards like STIX/TAXII, using this capability requires an additional solution.

"The fact is, next-generation firewalls dont 'play nicely' with third-party threat intelligence."

Real World Data Illustrates the Threat Intelligence Limitations of Firewalls

Third-party threat intelligence limitations within next-generation firewalls is a very real challenge facing organizations. Here at Bandura Cyber, we see it and hear it daily, as we interact with our customers and prospects. We often hear that this fundamental reality is a key reason why organizations purchase and deploy our Threat Intelligence Firewall platform. Importantly, real world data from leading firewall providers validates the limitations. Let's take a look.

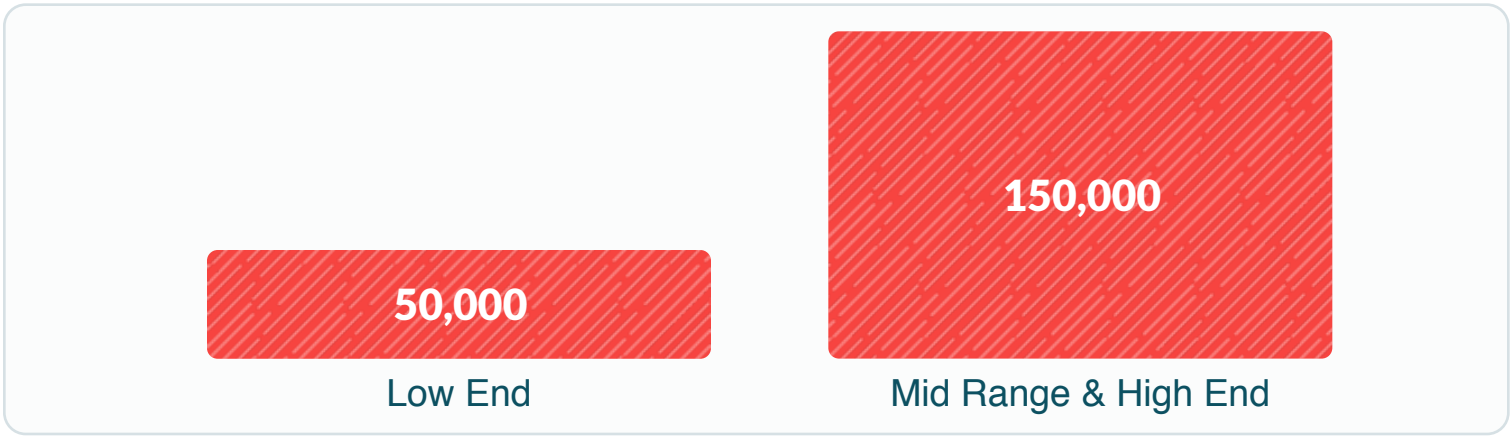
Palo Alto Networks External Dynamic Lists

Palo Alto Networks is arguably, the most popular Next-Generation Firewall on the market today. However, it is not without its own faults. In it's PAN-OS® Administrator's Guide, the company provides information on its External Dynamic Lists, which are defined as text files that are hosted on an external web server. The data clearly illustrates the limitations Palo Alto Networks' next-gen firewalls have with respect to third-party threat indicators.

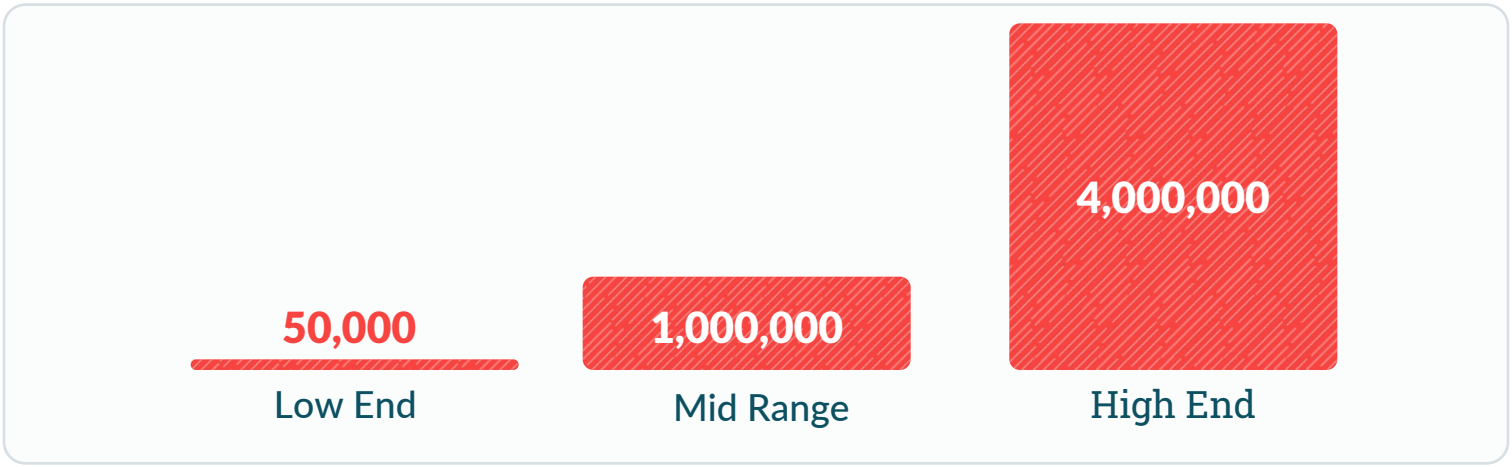
Specifically:

- The PA-5200 Series and the PA-7000 Series firewalls, which are Palo Alto's high-end models, support **a maximum of 150,000 total IP addresses;** all other models support a **maximum of 50,000 total IP addresses.**
- The **maximum number of domains ranges from 50,000 to 4 million** depending on the model. The upper end of the maximum range requires upgraded network processing cards.
- On each firewall model, you can add **a maximum of 30 custom External Dynamic Lists** with unique sources.

Palo Alto Networks NGFW IP Address Limits



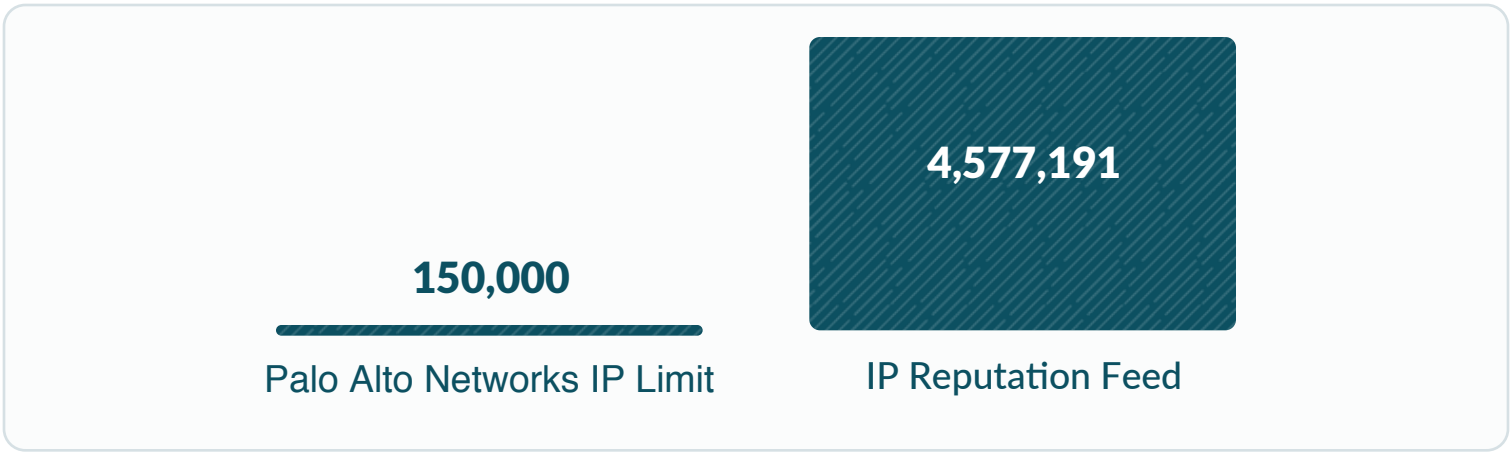
Palo Alto Networks NGFW Domain List Entry Limits



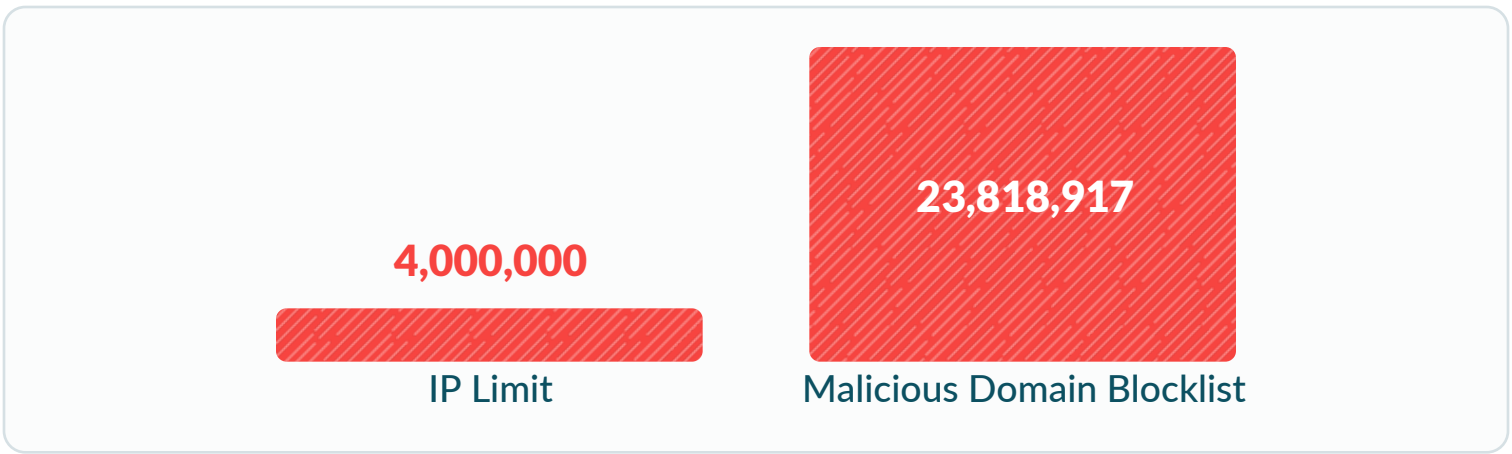
By its own admission, the top-end Palo Alto Networks next-generation firewall, the PA-7080, which is marketed to large enterprises and service providers, can only handle 150,000 total third-party IP indicators and 4 Million total third-party domain indicators.

To put this into perspective, let's compare Palo Alto Networks' External Dynamic List limits with two threat feed examples. The first graphic below shows an IP Reputation feed that typically has over 4.5 Million indicators. The second graphic below shows a Malicious Domain Blocklist that is powered by threat intelligence from DomainTools. This blocklist represents domains with a risk score of 99 and higher (out of 100). As you can see, integrating these threat feeds into a Palo Alto Networks' External Dynamic List is next to impossible.

Third Party IP Reputation Feed Example



Third Party Domain Blocklist Example



Fortinet Threat Feeds (External Dynamic Block Lists)

Another leader in the next-gen firewall market is Fortinet. Similar to Palo Alto Networks, Fortinet has the ability to dynamically import external block list text files from an HTTP server. Text files can contain IP addresses, domain names, and hashes. Fortinet calls these dynamic block lists "Threat Feeds."

Identifying third-party threat intelligence limitations with Fortinet is more challenging than Palo Alto due to limited data. However, one important data point illustrates key limitations. Fortinet indicates that the size of a blocklist file can be 10 MB, or 128,000 lines of text, whichever is most restrictive.

While it's unclear if Fortinet has a total volume limit, what is clear is that integrating a large, third-party threat feed into Fortinet would be cumbersome requiring the separation of one large threat list into many smaller lists. For example, the IP Reputation feed would require over 30 separate lists and the DomainTools threat feed would require over 170 separate lists.

SonicWall Threat API

Data from SonicWall, a well established provider of firewall solutions to small and mid-sized businesses, also validates threat intelligence limitations. SonicWall's Threat API "allows administrators to send lists of URLs or IP addresses to be blocked via command line." Based on this, it appears there is no automated way to integrate third-party threat intelligence into SonicWall firewalls. SonicWall also indicates that the list is limited to 5,000 entries for all product versions.

Why Do Firewalls Have These Limitations?

Understanding the limitations firewalls have with respect to using third-party threat intelligence is the first step. Next, we must ask, why do these limitations exist? We believe there are two motivating factors: (1) lack of incentives; and (2) resource constraints.

Lack of Incentives

Firewall providers are in the business of providing solutions that protect networks. As mentioned earlier, their solutions are powered by their own proprietary threat intelligence. In fact, one of the key ways firewall providers compete against one another is based on their ability to detect and block threats. This is evidenced in annual firewall tests conducted by organizations like NSS Labs. This fuels a virtuous circle where firewall providers focus on improving their own detection capabilities. The focus on proprietary threat intelligence leads to a natural lack of incentive to use threat intelligence from other sources or to share threat intelligence with other systems.

Resource Constraints

The other major factor that we believe inhibits firewalls' ability to work with third-party threat intelligence are resource constraints. Simply put, today's firewalls perform multiple functions many of which are resource intensive. These functions include deep packet inspection in order to provide services like intrusion detection and prevention (IDS/IPS), URL filtering, and malware detection. The resource intensity of deep packet inspection is evident in the significant decrease in firewall throughput that occurs when these features are used. This decrease is typically in the area of 50%.

Adding further burden to resource requirements is that an increasing amount of traffic is encrypted. This means that firewalls need to decrypt the traffic in order to inspect the traffic for threats. This decryption requires significant additional resources. Many firewalls are now adding SD-WAN capabilities so the list of functions being added keeps growing.

Simply put, the more functions a firewall performs, the more resources this requires. With firewalls being challenged already to provide their own services, this leaves few resources to divert to process third-party threat intelligence feeds.

A Quick Look at the Bandura Cyber Threat Intelligence Firewall Platform

Over the last several years, Bandura Cyber has been at the forefront of driving a new category of cyber security technology that makes threat intelligence actionable. The Bandura Cyber Threat Intelligence Firewall platform aggregates and integrates threat intelligence in the cloud and makes it actionable by blocking known bad traffic before it hits your network.

Compared to traditional firewalls, the Bandura Cyber Threat Intelligence Firewall platform is:

- Purpose-built to detect and block threats based on massive volumes of threat intelligence. It can block up to 150 million unique IP and domain threat indicators at line speed before they hit your network and security controls far exceeding the capabilities of next-generation firewalls. There are also no limitations on the number of lists or list sizes.
- An open platform that can work with IP and domain threat intelligence from any source. The platform provides a broad array of “out of the box” threat feeds from commercial, open source, government, and industry and has the ability to integrate IP and domain threat intelligence from any source. This includes native support for standards like STIX/TAXII, open APIs, and “out of the box” connectors for Threat Intelligence Platforms, SIEMs, SOARs, and other systems.
- Easy to deploy and manage with simple and intuitive policy management capabilities.

The Bandura Cyber Threat Intelligence Firewall Platform Complements Next-Generation Firewalls

A critical point is that the Threat Intelligence Firewall complements next-generation firewalls by providing organizations with another layer of protection. Threat Intelligence Firewalls eliminate the threat intelligence challenges facing next generation firewalls. However, you can also see that it's complementary because next-generation firewalls have capabilities like deep packet inspection, that the Threat Intelligence Firewall does not have.

Importantly, the Bandura Cyber Threat Intelligence Firewall platform not only provides another layer of network protection but it also improves the efficiency of firewalls enabling precious resources to focus on deep packet inspection, decryption, and other important functions.

Conclusion

Next-generation firewalls remain an important foundational component of network security. However, a reliance on proprietary and closed threat intelligence and an inability to integrate threat intelligence at scale are resulting in firewalls having a tough time keeping up with today's threats. The Bandura Cyber Threat Intelligence Firewall platform is helping organizations to overcome these challenges and to make threat intelligence actionable in an easy, open, automated, and scalable way.