BANDURA®
ADVANCED SECURITY FOR *YOUR* WORLD™

POLIWALL: AHEAD OF THE FIREWALL

FIREWALL HISTORY

Since the earliest days of the Internet, when hackers sat in their darkened basements dialing into networks with dial-up modems, both network threats and network defenses have been evolving. Initially, it was sufficient to simply use port-based blocking for non-public resources. But outbound access to the Internet was required, and hackers quickly learned how to take advantage of the non-stateless nature of firewalls to circumvent them. The introduction of stateful filtering firewalls prevented hackers from taking advantage of non-stateless connections, but hackers next learned to find vulnerabilities in the public-facing applications and exploit them to access private protected resources, moving laterally throughout a business network. Intrusion detection systems, with signature-based deep packet inspection, were the next step in the evolution. These devices attempt to match patterns of known attacks against the data entering the network. Unfortunately, this is where the cyber defense evolution drastically slowed. The defenses have increased in quantity and speed, but the quantity and sophistication of the network intrusion attempts has increased faster.

ABOUT THE AUTHOR

DAVID MAESTAS
CO-FOUNDER, CTO

With more than 20 years experience in the software development and cyber-security fields, David is a nationally recognized cyber security innovator, speaker, panelist and thought-leader as the author of more than 40 patents in five patent families related to the adaptive and intelligence-based security systems.

Prior to Co-Founding Bandura Systems, LLC where he currently serves as CTO, David was CTO of TechGuard Security responsible for leading two core divisions of the company including TechGuard's US Defense Research and Development Lab as Principal Investigator and Manager of a $1.45 million NIST Advanced Technology Program and over $3 million in DoD-funded projects developing security solutions for military networks.

ENTER IP THREAT INTELLIGENCE

Fortunately, a new type of cyber defense based on IP threat intelligence is available today to address the shortcomings of firewalls and intrusion detection systems. IP intelligence-gathering systems study current and past behavior associated with IP addresses across the Internet. This behavior is classified in many categories including botnets, command-and-control servers, distributed denial-of-service attacks, and other threat categories. Using threat intelligence for network defense can significantly decrease the attack surface for a protected network. High-risk IP addresses that have been associated with previous malicious activity are simply denied access to network resources.

IP threat intelligence comes from a global network of sensors, which monitor and record malicious activity. These sensors can reside in honeypots, managed firewalls and intrusion detection systems, and endpoint software on both PCs and mobile devices. Today there are many providers of threat intelligence, both commercial and open source. The problem that faces those desiring to use threat intelligence to protect their networks is how to choose which source to use and how to use the data provided by those intelligence sources. Firewalls are not well suited for this task, as they were originally designed to support only a few thousand rules to protect internal network resources. There are currently over 10 million high-risk IP addresses tracked on a daily basis. Even the most robust enterprise firewalls can only handle a few hundred thousand rules. This leaves the network administrator trying to choose

ENTER IP THREAT INTELLIGENCE (cont.)

which of the 10 million known high-risk IP addresses should be blocked. Even after making this decision, there is no way to apply a different set of IP addresses to individual network resources without further reducing the number of chosen IP addresses to block.

Bandura has introduced two new products to help reduce the organizational risk of cyber intrusion and data leakage —while helping network administrators manage this problem and implement IP threat intelligence-based security in their networks.
PoliWall is software which is deployed as an in-line appliance that utilizes GeoIP and IP threat intelligence to stop attacks that could not be prevented by firewalls and intrusion detection systems. ProAct™ is a software application that allows for easy management of multiple IP threat intelligence sources, including private internal data coming from your own firewalls, IPS or IDS, and can deliver aggregated threat intelligence to PoliWall and other network devices.

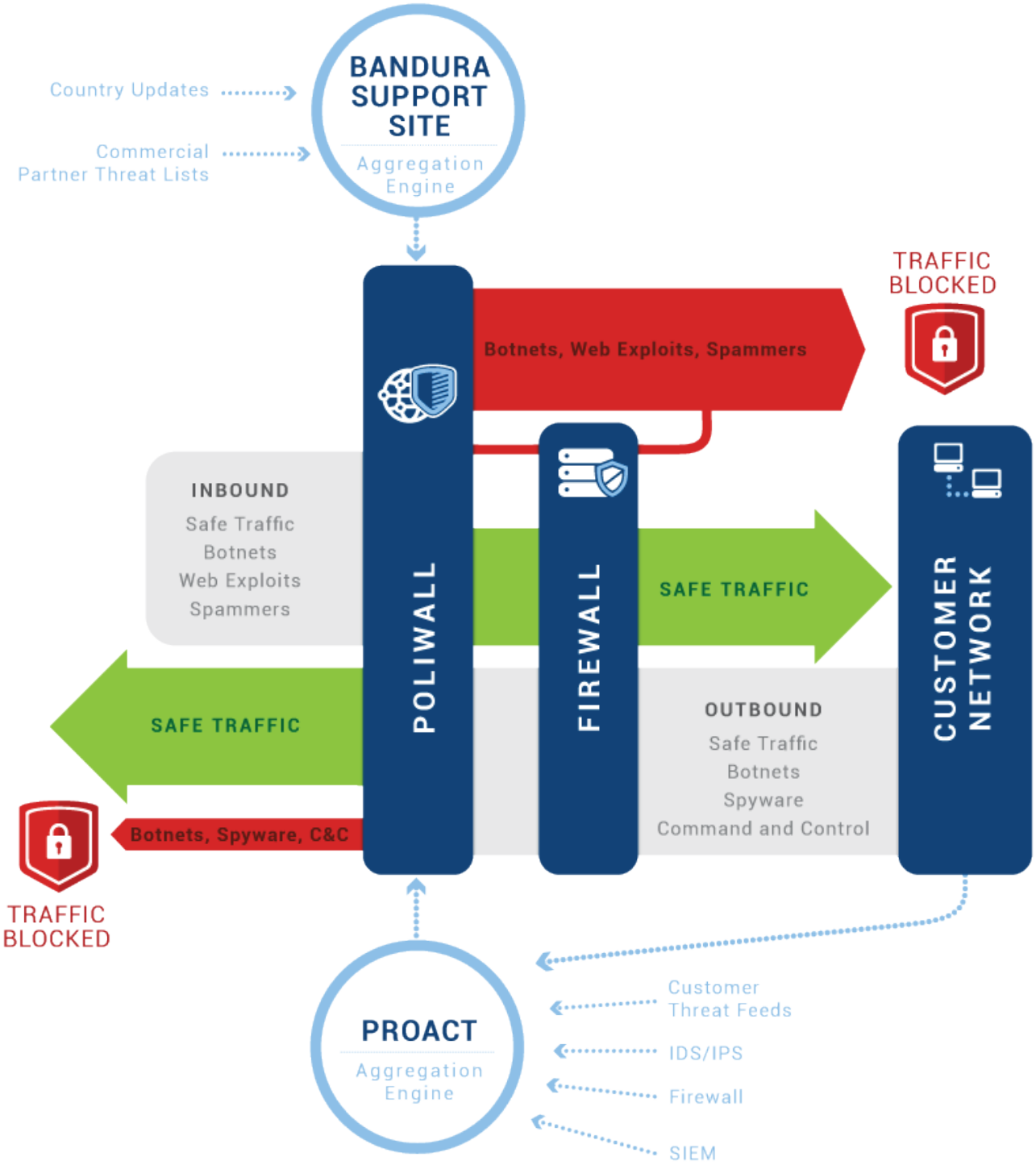
The PoliWall works by consuming IP threat intelligence from multiple providers. Each provider is capable of aggregating threat feeds from multiple sources. With this delivery system, PoliWall is capable of consuming information from hundreds of sources and millions of addresses. PoliWall is currently able to load 100,000,000 high-risk IP addresses into its low-latency lookup engine. Unlike the firewall scenario, Network administrators don't have to choose which ones to block – they can block them all. Additionally, the PoliWall allows the administrator to choose which categories they wish to block and select how aggressively they want to block within each category. Each IP address and the threat intelligence feed has an associated risk score. Blocking all IP addresses within a category can lead to false positives, a common problem when using intelligence base filtering. By using a slider control to adjust the sensitivity of filtering within a category, the administrator can find a proper balance between security and false positives.

PoliWall provides granular security by allowing the creation of resource groups, which are collections of IP assets which share a security policy. Packets inspected by the PoliWall are first assigned to a resource group and then the corresponding policy is examined. The policy may specify which countries are allowed to access network resources, how much bandwidth they are allowed to use to access resources, and which categories of IP threats to block and how aggressively to block them. Resource groups can be defined for both inbound traffic and outbound traffic, enabling protection of internal resources in protecting internal users from accessing malicious sites on the Internet. This also can prevent malware which may currently be embedded in the network from communicating to the Internet for command and control or data exfiltration.

POLIWALL SIMPLIFIES OUTBOUND (EGRESS) FILTERING

It is difficult to implement a solid egress filtering policy using firewalls. Firewalls were designed to protect internal resources whose numbers and locations are known. Outbound filtering with firewalls can restrict which applications may be accessed by using port filtering, but provides no protection against HTTP access to a malicious server delivering malware. Blocking HTTP is most likely not an option. Using PoliWall with threat intelligence and egress filtering alleviates this problem.

- Egress filtering prevents leakage of sensitive data—credit cards, customer's personal information—by using PoliWall's IP threat intelligence aggregation and auto-blocking service which identifies and prevents malicious IP's from connecting up to receive data leaking out of the network.


Country Updates
Commercial Partner Threat Lists
BANDURA SUPPORT SITE
Aggregation Engine
TRAFFIC BLOCKED
Botnets, Web Exploits, Spammers
INBOUND
Safe Traffic
Botnets
Web Exploits
Spammers
POLIWALL
FIREWALL
SAFE TRAFFIC
CUSTOMER NETWORK
SAFE TRAFFIC
OUTBOUND
Safe Traffic
Botnets
Spyware
Command and Control
Botnets, Spyware, C&C
TRAFFIC BLOCKED
PROACT
Aggregation Engine
Customer Threat Feeds
IDS/IPS
Firewall
SIEM

POLIWALL SIMPLIFIES OUTBOUND (EGRESS) FILTERING (cont.)

- Retailers have experienced massive data compromise because they don't know there data is leaking out for weeks/months. PoliWall's IP threat intelligence updates in near-real time to minimize data loss time to micro-seconds.

- PoliWall's intuitive outbound filtering process eases PCI 3.0 audit compliance and time with easy-to understand maps, graphs and charts showing what countries and IP's are blocked in compliance with the Office of Foreign Asset Control.

PROCESSING SPEED AND VOLUME ENHANCES FIREWALLS

Many firewalls today have implemented deep packet inspection to provide intrusion detection support to look for signatures of known attacks, and some provide application level inspection to search for malicious activity. These are computationally intensive processes, which significantly reduce the throughput and increase the latency for network connections. Using PoliWall with threat intelligence filtering in front of these devices can stop many connections before they even reach the firewall. By blocking connections to or from countries that do not require access to the network resource, the firewall or intrusion detection system does not need to do stream reassembly and packet inspection for that attempted connection. Blocking high-risk connections to or from IP addresses associated with malicious activity prevents these connections from being presented to the firewall or IDS at all. A significant reduction in connection rate by eliminating high-risk connections can allow firewalls and IDS devices to operate more efficiently, and may allow network administrators to turn on functionality and those devices that were performance prohibitive before. PoliWall customers report up to a 60% reduction in manpower needed to manage the security architecture.

REDUCING THE ATTACK SPACE OUTSIDE THE FIREWALL

Reducing the attack space with GeoIP filtering and threat intelligence filtering can save both time and money while providing a more robust network defense. All PoliWall users have reported a significant reduction in network traffic after installation, with one reporting a 90% reduction in network connections. Using egress filtering to protect outbound Internet connections can reduce the number of help desk tickets for compromised PCs. Some users have reported over a 50% reduction in helpdesk tickets since implementing PoliWall.

PoliWall threat intelligence feed delivered by the Bandura support network is constantly updated in near real-time. When malicious actors are detected on the Internet, their IP address is added to PoliWall threat engine within seconds. When risk scores for IP addresses change, whether increasing or decreasing, the information is also updated in the engine within seconds. This eliminates the problem of having stale information in the security policy, or having to manually update this policy on a timely basis. With tens of millions of IP addresses in play at any time, this is a difficult if not impossible task without a device like the PoliWall.

Bandura's new ProAct™ server provides threat intelligence aggregation and delivery based on a publisher-subscriber model. Threat intelligence data may be published by uploading it to the ProAct™ server via the web interface, or can be published to the server using a REST API. The API interface allows real-time publishing of threat information as it is detected by firewalls, intrusion detection systems, or security event managers. PoliWall devices can subscribe to

REDUCING THE ATTACK SPACE OUTSIDE THE FIREWALL (cont.)

the information from the ProAct™ server and integrate that data into their threat filtering engines. This will allow the use of open source and customer-licensed threat intelligence, as well is data that is derived from customer-owned security devices.

PoliWall makes it possible, and also easy, to implement IP threat intelligence filtering as part of an overall security architecture. PoliWall adds capabilities that address the shortcomings of firewalls and intrusion detection systems, while also consuming information from those devices to provide a continually evolving security implementation. In doing so, PoliWall actually makes existing enterprise security assets more effective, and staff more productive, stopping cyber threats as they emerge.