The Evolution of the Edge

Dynamic Perimeter Defense and the Virtual Minefield Zone™

A PacketViper White Paper

Dated: August 23, 2017

INTRODUCTION

As firewalls (taken here to include firewalls and next-generation firewalls with IDS/IPS) have evolved in their processing of application layer inspections, the epidemic of rising global IP traffic volume has made it less practical and secure to perform these deep packet inspections as a first line of defense. Only legitimate traffic should make it into the firewall inspection process, but efficiently stripping away illegitimate traffic is not the primary purpose of firewalls. Firewalls are simply not built to address the anticipated global IP traffic growth. Many have come to accept the issues with global IP traffic and the unmanageable levels of alerts and logging as a reality of today's business climate.

While we are seeing a proliferation of bots, proxies and DDoS attackers that cultivate malware to expand bot forces and come up with new ways to deceive victims, there is a similar proliferation of network security and cybersecurity tools available today. While some of these tools offer marginal benefit, most increase management time without sufficiently dealing with the root cause issue – the volume of illegitimate traffic. Taking steps to reduce illegitimate IP traffic from the network (inbound and outbound) without taxing the resources of the firewall, NGFW, IDS/IPS is one of the most proactive, cost-effective and impactful network security moves that one can make today. Others feel that log and event managers provide a solution by sorting through traffic, but many of these log consolidators (SIEM, Syslog & Event Manager solutions) become less effective when processing too much traffic with information. It is not uncommon for information to go unseen for days or months.

This paper discusses the evolution of network perimeter defense and proposes a different, far more proactive approach that empowers network security teams by addressing the traffic volume problem head-on while solving previously unsolvable issues with respect to filtering rules complexity. This approach is based on a unique and dynamic security zone/layer called the Virtual Minefield Zone (VMZ)™, containing characteristics unlike any other perimeter defense mechanism. With VMZ methods in place, attackers are repeatedly deceived and confused by rotating access rules. The VMZ also alters the nature of the perimeter from static to dynamic while at the same time increasing transparency into traffic at the perimeter while reducing overall security costs. The result is that 70% of traffic is stripped away before the firewall inspection process and network security teams are better equipped to cost-efficiently improve their cybersecurity posture in the face of growing threats and unprecedented IP traffic volumes.

PERIMETER DEFENSE TECHNOLOGIES: A BRIEF HISTORY

Over time we have seen the evolution of perimeter defense solutions bring about important evolutionary benefits that addressed the more pressing problems of the times. This is reflected in the chart below:

Figure 1

ERA	Problem	Technology	Evolutionary Benefit
Late 1980's	Identified need for basic technical internet security	1st gen packet firewalls	Layer 3 OSI filtering of packets
Early 1990's	Inability to judge the 'state' of the connection	Circuit level gateways	Layer 4 OSI filtering – Stateful Firewalls
Mid 1990's	Inability to understand applications and protocols	Application level firewalls	Application layer filtering
Early 2000's	Disparate networking and security tools	Next Gen Firewalls (NGFW)	Integrated networking and security (FW, IDS, IPS)
Mid 2000's	Traffic volumes and lack of context	Advanced Perimeter Defense	Simplified context based traffic management

While firewalls have evolved to perform very effective application layer inspections, **the epidemic of rising global IP traffic volume has made it less practical and secure to perform these deep packet inspections as a first line of defense.**

Furthermore, there are four serious limitations to firewalls as an edge defense tool in today's networking environment:

1. The need for open ports and services
2. Static fronts and the inability to quickly, easily and frequently change access rules
3. The inability to strip away illegitimate traffic
4. The inability to lessen the flow of unmanageable logs and alerts

The firewall inspection process is not a 'catch-all' and should be reserved for properly vetted traffic. Only traffic that is known to be well aligned with the mission/needs of the enterprise should make it into the firewall inspection process, but efficiently reducing high volumes of potentially harmful illegitimate traffic is not the primary purpose of the firewall. In turn, most firewalls are set to 'over-alert' which puts a tremendous strain on security teams to keep up. This gap in the legitimization process of traffic at the perimeter opens the door for the next phase in the evolution of network perimeter defense.

THE SILENT KILLER OF NETWORK SECURITY: GLOBAL IP TRAFFIC

While firewalls were evolving to provide much needed comprehensive filtering across the entire OSI stack, a new problem was brewing on the attacker front. Cyber-attacks have become a global phenomenon. Today anyone with a computer or a smart phone and an internet connection can launch an attack on a target victim anywhere in the world. Due to the ease with which attackers can cultivate a botnet and illicit services that rent the use of botnets, the cost to attack is cheap, getting cheaper, and more readily available. Rented and/or newly built botnets can be used to distribute spam and phishing emails, steal money, steal identities and propagate new malware. Cost is no longer a consideration as villains seek to aim high volume attacks at organizations.

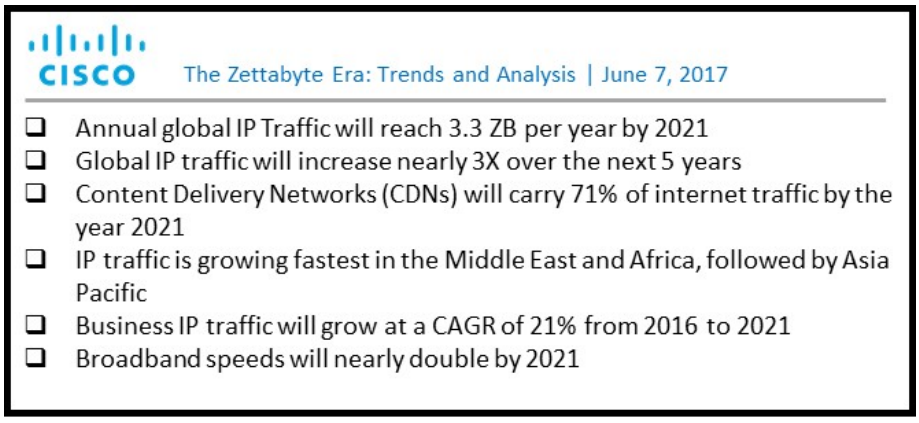
This is all exacerbated by the cultural need to be 'constantly connected'. People's desire to maintain real-time, constant connection to the internet results in a proliferation of devices which provide countless amounts of bot configuration options.

The fluid nature of this expanding and contracting attacker landscape is impossible to address with firewalls and logging systems. Attackers leverage this advantage to distract network managers and constantly keep security teams on their heels in a reactive state. These attackers have countless resources and methods at their disposal and start with a simple reconnaissance scan, probe or some other simple test of service limits. They hide these within everyday traffic patterns to distract administrators and gain intelligence to penetrate, incapacitate and/or extract data from a network.

A ROOT CAUSE PROBLEM

All of these increasing global IP traffic trends represent a root cause problem for network security managers, as evidenced in these excerpts from a recent CISCO report on IP traffic trends:

Figure 2



UNMANAGEABLE LOG AND ALERT VOLUMES

These global IP traffic volumes are resulting in a problematic amount of logging and alerting, which quickly becomes overwhelming for organizations of all size.

ESG Research cites the volume of security alerts as the #1 operational challenge in security operations today. This is equally true of MSP, MSSP and SOC teams as it is for in-house network security teams.

Figure 3

While larger enterprises are increasingly investing in security information and event manager (SIEM) applications, the value of these solutions is compromised by the traffic volume problem. The increases in traffic correspondingly drives up the number of alerts, time required to check and time it takes to remediate.

Also, some popular SIEM solutions have volume based pricing schemes, so the illegitimate traffic can increase SIEM fees and security costs.

ENHANCING, NOT REPLACING, THE FIREWALL

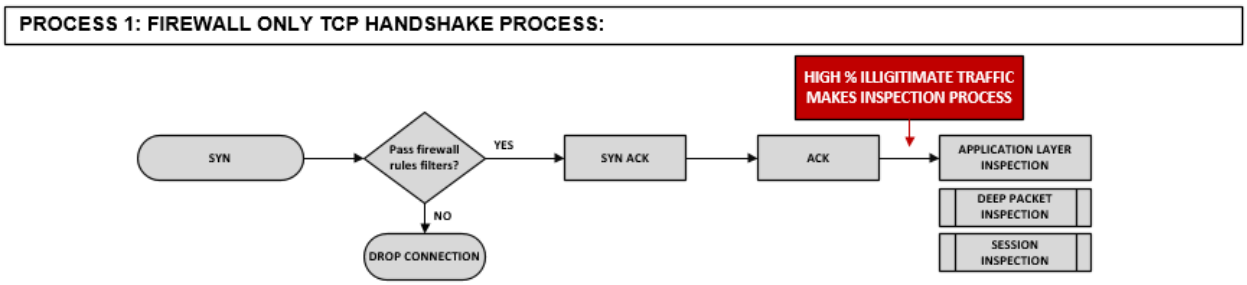
None of this is to suggest displacing firewalls. However, given the trends in global IP traffic, this is suggesting an alternate place for the firewall in the perimeter hierarchy, which would be behind the advanced perimeter defense application.

Firewalls perform critical inspection duties and will perform these tasks optimally and most accurately when less inundated with traffic that a business or enterprise has no purpose for.

Furthermore, firewalls would experience serious latency if they even attempted to tackle the traffic problem with the levels of control, transparency and granularity that PacketViper does.

Figure 3 below shows the process flow of a firewall only TCP handshake process. This results in a high percentage of illegitimate traffic making it into the inspection process, hinders firewall performance and compromises other essential security tools such as the IDS/IPS and SIEM.

Figure 3



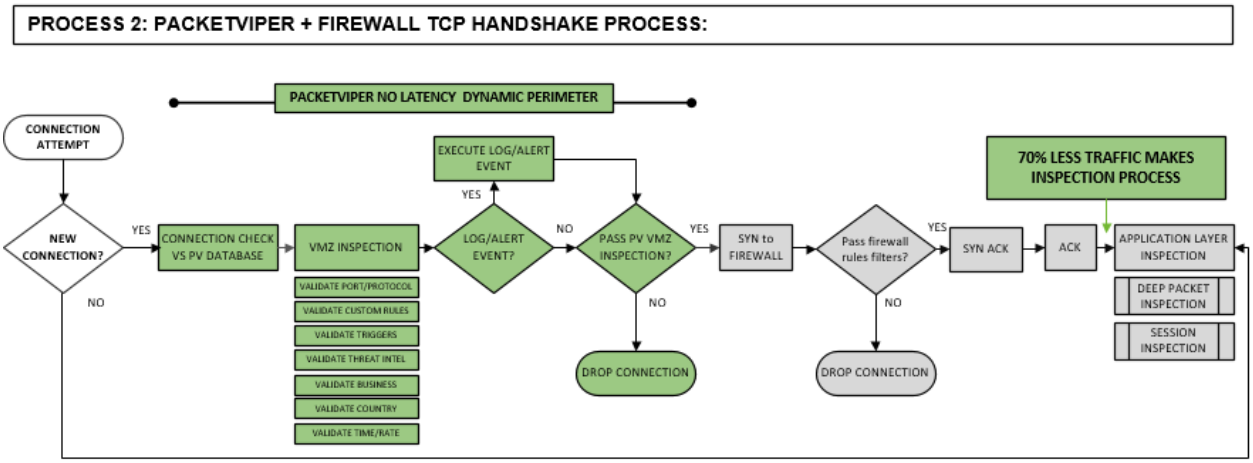
Alternatively, Figure 4 below shows the process flow of a perimeter that includes both PacketViper advanced perimeter defense software and the firewall. In this scenario, PacketViper sits in front of the firewall as an undetectable in-line bridge, checking new connections.

PacketViper checks new connections and collects the network information, aligning it against a robust and proprietary database that is tightly integrated with the logging, reporting and rules dashboard and engines. PacketViper then uses a unique and configurable array of sensors, triggers and redirection/decoy techniques to create a dynamically changing, virtually impenetrable perimeter around essential services.

The application of these techniques turns the normally static front associated with firewall based perimeters into a dynamic perimeter. Based on the changing nature of the dynamic perimeter, attackers find it difficult to understand a potential victim's network capabilities.

Upon complete implementation, customers have their own Virtual Minefield Zone or VMZ™ and the result is typically 70% less traffic making it into the firewall inspection process.

Figure 4



THE VIRTUAL MINEFIELD ZONE & DYNAMIC PERIMETER DEFENSE

Attackers have historically leveraged many advantages to gain cyber supremacy. These include anonymity, knowledge of security solutions, poorly designed software and a keen manipulation of the borderless space between their targets and their bots.

On the other hand, the network administrator has one large advantage, that being knowledge of the network. Leveraging this advantage together with attacker blindness can put administrators in a position of strength. In order for attackers to test the perimeter defense, they typically use readily available tools to scan networks for responses. Attackers starts this process 'blind' to network terrain, but they alter and adjust their attack plans based on their discoveries at the perimeter. Over time their attempts and persistence pays off and they work their way in with unrelenting scans including but not limited to; high volume floods, low and slow scans, probes, attack dry-runs, distractions and other techniques that distract administrators, gauge capabilities, identify service limits and ultimately wear away at firewall based perimeters. Ultimately the firewall based static front and open ports intended to protect an enterprise is used as a focal point or beacon for attackers to refine and perfect their attack plan.

To effectively defend against these ever changing, discrete and relentless malicious efforts, network administrators need to be nimble. Ideally, they could change the nature of the perimeter with frequency to continuously trip up attackers. However, constant rule changing within firewalls is prohibitive.

The answer to these challenges is the PacketViper Virtual Minefield Zone (VMZ).

THE DYNAMIC PERIMETER

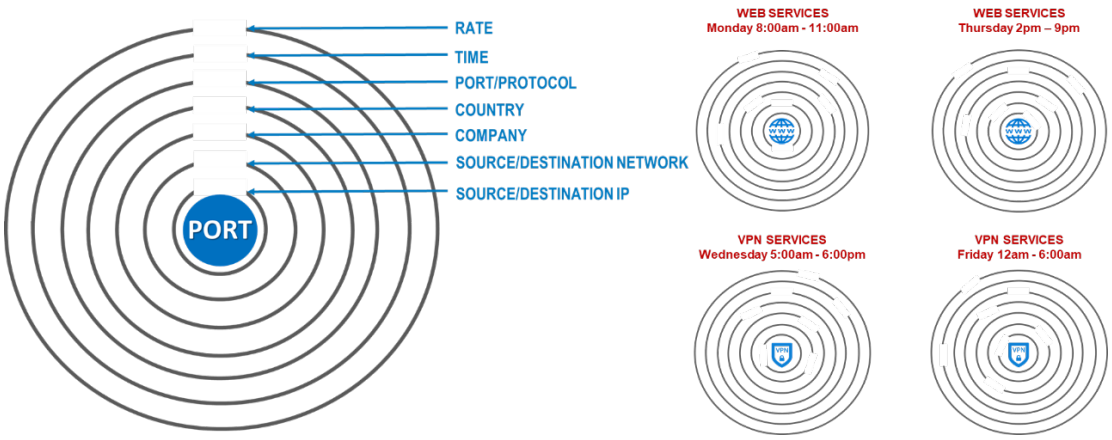
The PacketViper VMZ creates a dynamic perimeter and extends the perimeter using features and techniques that are unique to PacketViper. These features allow you to rotate sensor settings and confuse attackers by deploying decoys and traffic redirection. The VMZ triggers can be configured around each port/service to change themselves around to never provide a static front. Each scan/probe is met with a different set of access rules and parameters.

With 'point & click' simplicity, rules can be altered and set to automatically rotate/change, on a per-port basis based on the following parameters:

- Rate | Time | Port/protocol | Country | Company | Source/destination network | Source/destination IP

Figure 5 depicts the variety of levels that triggers that can be configured 'around' each port and how those triggers can be rotated over time.

Figure 5



A dynamic and automatically changing perimeter with the PacketViper VMZ creates a treacherous path for connections working outside of normal operating ranges.

ACHIEVE 100% SECURITY ALERT REVIEW

Most organizations in both the public and private sector are understaffed with respect to FTE resources to check network security alerts. In another recent report, CISCO identified that on average 44% of network security alerts go unexplored[1]. What is especially troublesome here is the lack of understanding of what lurks in unchecked alerts. The '80/20 Rule' doesn't work for network security. One can't believe they have 80% of their major threats covered by checking only 20% of alerts.

Another challenge here is that resources and expertise along these lines are scarce and expensive. The answer is for organizations to get closer to 100% security alert review with the team they have. The best way to do this is to radically alter the number of alerts, and the best way to do that is by getting out in front of the global IP traffic volume problem.

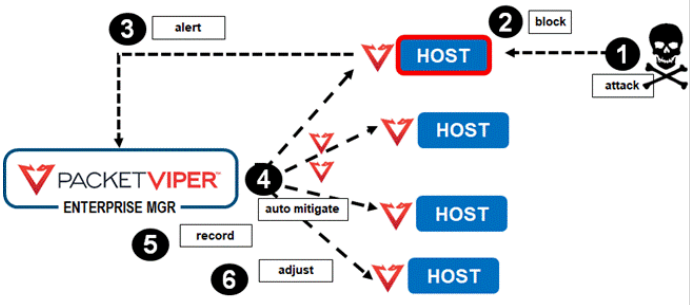
Reducing traffic with PacketViper gives the existing team a chance to review more alerts and provides significant cost savings as opposed to hiring more network security analysts.

THE VMZ AND ENTERPRISE MANAGEMENT

Enterprise Management can be deployed across an enterprise to create a dynamic, self-mitigating perimeter across an organization with multiple gateway connections. In this environment, each PacketViper unit works as one so that when one PacketViper is attacked the enterprise automatically self-protects all systems to defend against the source of the original threat. With this model, attacks and threats are remediated in real-time while threat intelligence is gathered and stored.

Figure 6 below shows the workflow that ensues when a connection attempt violates a VMZ trigger or rule:

Figure 6



1. An attack, probe or scan violates a VMZ trigger/rule
2. The violated host is protected by PacketViper
3. Enterprise manager is alerted to violation
4. Automatic mitigation ensues across all hosts
5. Intelligence on violation is captured & recorded for diagnostics
6. Triggers adjust to ensure perimeter presents differently

[1] CISCO 2017 Annual Cybersecurity Report: The Hidden Danger of Uninvestigated Threats | February 6, 2017

CONCLUSION

The epidemic of increasing global IP traffic creates the need for the next phase in the evolution of network perimeter defense. While firewalls have evolved in their processing of application layer inspections, rising global IP traffic volumes renders the firewall a suboptimal first line of defense.

Advanced perimeter defense software from PacketViper focusing on the root cause problem of global IP traffic volumes brings a new level of dynamic protection to network perimeter defense. This results in important benefits to network security managers, including but not limited to:

- Reducing overall network traffic up to 70%
- Easily capturing, filtering and analyzing source traffic in real-time
- Increasing defense against both known and unknown threats
- Improving performance of firewall and SIEM solutions
- Easily tripping up scanners, attackers and probers
- Redirecting unwanted access attempts to phony services
- Extending the useful life of legacy systems
- Improving transparency into perimeter traffic patterns (inbound and outbound)
- Reducing security costs and SIEM fees
- Generating real-time threat intelligence based on actual perimeter based network traffic activity
- Unifying & hardening enterprise-wide perimeter defense

ABOUT PACKETVIPER

Based in Pittsburgh, PA PacketViper develops advanced perimeter defense cybersecurity software. Deployed either on-premise or in a virtual environment it sits in-line at the edge of the network with the primary functions of reducing illegitimate global IP traffic, increasing transparency and security while generating custom threat intelligence.

For more please visit www.packetviper.com.