PACKETVIPER®

Deceptive Boundary Defense

Active Threat Detection, Response and Network Obfuscation

A PacketViper White Paper

Updated March, 2021

INTRODUCTION

The static nature of common firewall-based network configurations has made it increasingly easy to scan, attack and breach a network. Leveraging their advantages of time and anonymity, attackers repeatedly and continuously conduct reconnaissance and NMAP scans to determine vulnerabilities and formulate an attack plan.

Furthermore, 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. 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.

'When 99% of external boundary traffic is at best unwanted, or worse, malicious, we call that a DDoS attack. When it's more like 70-80% we call that Tuesday"

Don Gray – PacketViper CTO

Taking steps to reduce illegitimate IP traffic from the network (inbound and outbound) without taxing existing resources is one of the most proactive, cost-effective and impactful network security moves that one can make today.

This paper discusses the evolution of network boundary defense to include increasingly popular deception tactics and techniques to address threats and the traffic volume problem head-on. This is a different, far more proactive approach that empowers network security teams. This approach is based on a deceptive and dynamic approach to boundary defense unlike anything else. This applies to not only external facing boundaries, but also to IT/OT boundaries.

PERIMETER DEFENSE TECHNOLOGIES: A BRIEF HISTORY

Over time we have seen the evolution of boundary defense solutions bring about important evolutionary benefits that addressed the more pressing problems of the times. 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 serious limitations to having firewalls as the only boundary defense tool:

1. The need for open ports and services
2. Static fronts and the inability to create the appearance of a moving target
3. The inability to effectively deceive threats, harvest intelligence and block them at the network edge
4. The inability to strip away illegitimate traffic and 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 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

The fluid nature of the expanding attacker landscape is impossible to address with only firewalls and logging systems. Attackers leverage their advantages of anonymity and unlimited time to scan networks while distracting network managers and constantly keeping security teams on their heels in a reactive state. These attackers have countless resources and methods at their disposal. They typically start with a seemingly innocent 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. Increasing global IP traffic trends represent a root cause problem for network security managers.

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

DECEPTION TO COMPLEMENT, NOT REPLACE, THE FIREWALL

None of this is to suggest displacing firewalls. 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 deception techniques and levels of control, transparency and granularity that PacketViper does.

The typical TCP handshake process 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.

Alternatively, a perimeter that includes both PacketViper deception decoys and a firewall creates a far more dynamic network defense and the appearance of a moving target. In this scenario, PacketViper sits in front of the firewall as an undetectable in-line bridge, interacting with new connections using rotating decoys and decoy responses.

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 customized decoys and decoy responses within their new dynamic, deceptive perimeter, and the result is typically 70% less traffic making it into the firewall inspection process.

DECEPTION & 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.

To effectively defend against these ever changing, discrete and relentless malicious efforts, network administrators need to make their networks harder to detect, reduce attack vectors and block threats before they get to the firewall. Ideally, they could change the nature of the perimeter with frequency to continuously trip up attackers and create the appearance of a moving target. However, constant rule changing within firewalls is prohibitive.

The answer to these challenges is PacketViper's lightweight, agentless decoys and deception responses with Deception360.

THE DYNAMIC AND DECEPTIVE BOUNDARY

PacketViper Deception360 uses deception to create a dynamic boundary that extends the perimeter using proprietary features and techniques. These features allow you to rotate decoys and decoy responses to confuse attackers. Decoys can be

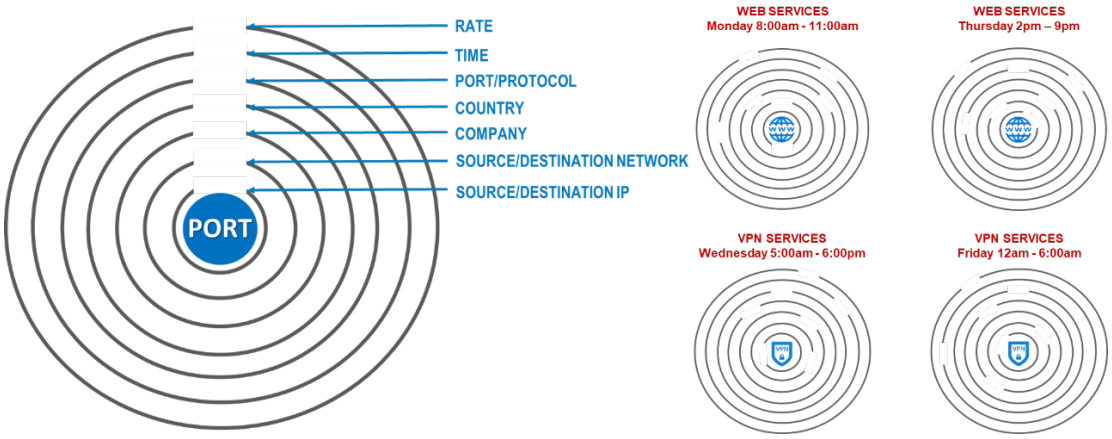
configured around each port/service to change themselves around to never provide a static front. Each scan/probe is met with a different set of decoys, access rules and parameters.

With Deception360 decoys and decoy responses 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 decoys that can be configured 'around' each port and how those decoys can be rotated over time.

Figure 5



A dynamic, deception-based, and automatically changing perimeter with the PacketViper Deception360 creates a treacherous path for connections working outside of normal operating ranges.

SMALLER HAYSTACK, SHINIER NEEDLES

Most organizations in both the public and private sector are understaffed with respect to FTE resources to check network security 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.

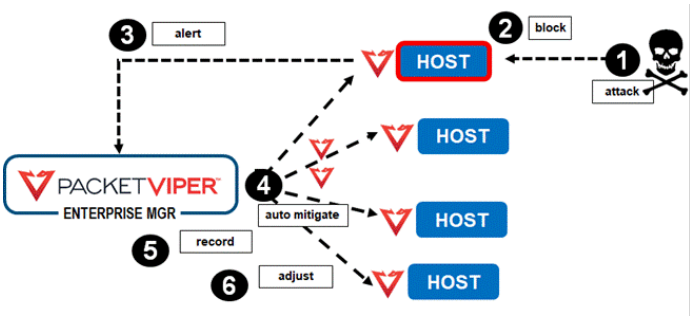
Reducing traffic with PacketViper's deceptive technology gives the existing team a chance to review more alerts and provides significant cost savings as opposed to hiring more network security analysts.

ENTERPRISE MANAGEMENT

Enterprise Management can be deployed across an enterprise to create a deceptive, dynamic, self-mitigating perimeter across an organization with multiple gateway connections. In this environment, each PacketViper unit works as one so that when decoys on one PacketViper are touched, 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 touches a decoy or sensor:

Figure 6



1. An attacker scans and touches a decoy
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 and recorded for diagnostics
6. Decoys are adjusted to ensure dynamic presentation of perimeter

CONCLUSION

Lightweight, agentless deception software from PacketViper focusing on the root cause problem of global IP traffic volumes and brings a new level of dynamic protection to network perimeter defense. This results in important benefits and measurable outcomes for network security managers.

- 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

PacketViper has transformative and trusted cybersecurity solutions for organizations seeking better security performance, reliability and results across their converging OT & IT networks. Deception360 solution automates deception-based attack prevention from both external and internal threats. PacketViper customers cover multiple public and private sector industries.

For more information visit www.packetviper.com.