Optimizing SIEM & Network Environments

The Challenge to SIEM Success: Complexity

Successfully deploying a SIEM is a complex task and the complexity is further amplified by the unmanageably high amounts of noise from within the network and from the skyrocketing volumes of global IP traffic constantly hitting the network.

Furthermore, with some SIEM vendors, depending on their pricing structure, the inability to control complexity and IP traffic volumes can drastically increase subscription/license related costs. The inability to keep up is plaguing security operations in organizations of all sizes, across all industries **(Figure 1).**

Figure 1:

Removing the Noise

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. The country blocking capabilities of firewalls also insufficiency address the global nature of essential contend delivery network (CDN) providers and other commonly dealt with businesses. The deep packet inspection process within the firewall cannot afford to be cluttered with illegitimate traffic that a business has no use for.

With 'point & click' simplicity and patented features, PacketViper can very precisely reduce IP traffic volumes. This is done with a layered filtering approach that includes the ability to geo-target and perform precise filtering based on business intelligence, threat intelligence and customer rules, both inbound and outbound, at the port level.

Our Virtual Minefield Zone (VMZ)™ solves the challenges of static perimeters in firewalls and creates a dynamic perimeter that can automatically change the access rules around any port or service and rotate when they are turned on or off. The VMZ also attracts threats, deceives them and gains new intelligence.

All of this improves the IDS/IPS threat identification process, lowers false positives and reduces alerting to security teams and SIEM related costs.

How it Works

PacketViper's dynamic threat defense platform allows users to continually deceive attackers, gather intelligence on threats and apply that intelligence to strengthen defense in a consistent and automated fashion. This greatly improves the performance of firewalls, IDS/IPS and SIEM solutions. Deploying PacketViper's integrated deception, defense and intelligence plan into a layered security approach provides a practical and cost-effective means to proactively strengthen cybersecurity.

Deployment options include on-premise or in the cloud. PacketViper sits inline as an undetectable bridge at the perimeter of the network, as well as at other key network transition points throughout the network. On inbound IP traffic, PacketViper looks at new connections and is inherently stateful.

PacketViper competencies include Deception, Intelligence, and Defense. Each complimenting the other to harden network defenses in real-time while providing simple, and intuitive interfaces to make fast and impactful operational decisions.

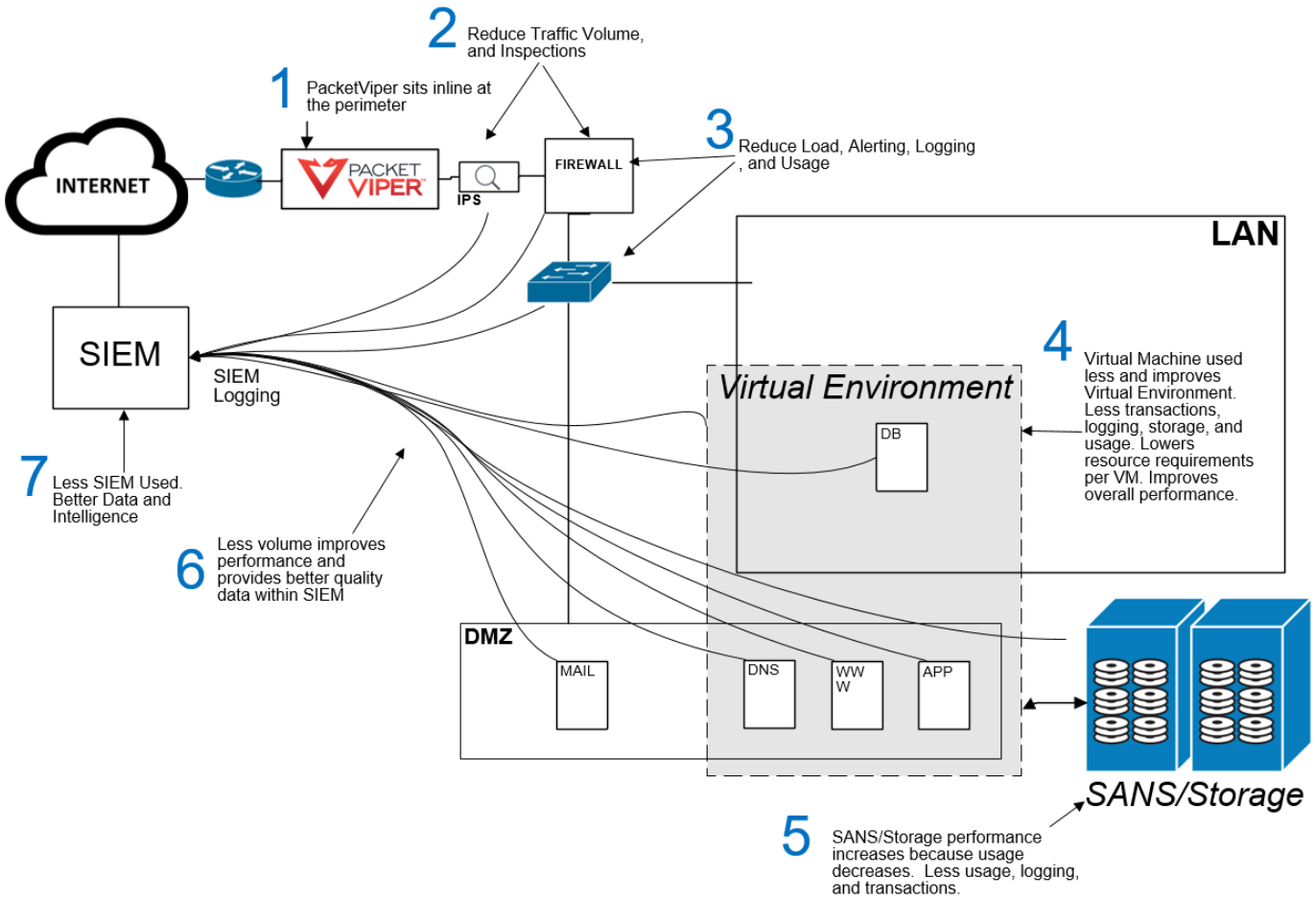
With 'point & click' simplicity, rules can be altered and set to automatically rotate/change, on a per-port basis based on the following parameters: rate, time, port/protocol, country, company, source/destination network, source/destination IP.

Measurable Benefits

Removing illegitimate IP traffic from the network 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 **(Figure 2).** Measurable benefits include:

- Reduction in IP traffic
- Reduction in logs and alerts
- Reduced SIEM licensing costs
- Labor savings
- Reduction in SPAM messaging
- Savings from deferred upgrades
- Bandwidth savings
- Storage savings

Figure 2: This shows how PacketViper benefits the overall network environment, including the SIEM. Once illegitimate IP traffic volumes are reduced, network transparency is greatly improved and logs, alerts and usage is streamlined across the network. Virtual machines are used less which greatly lowers resource requirements. Data quality is greatly improved within the SIEM and network security teams can check and remediate a much higher percentage of alerts.



About PacketViper

PacketViper is a leading provider of integrated cybersecurity deception, defense and intelligence solutions. Our threat defense platform & integrated approach to deception, defense and intelligence helps customers do more with existing resources while reducing cybersecurity related risks and costs. PacketViper customers are in both the public and private sector and cover multiple industries.