Use Case: Network Security Visibility

Improve your Network Security Visibility using Network Performance Monitoring (NPM)

Business Goals

- Leverage and expand existing tools to increase security footprint and reduce CapEx
- Improve security posture with network level insights and reduce OpEx
- Optimize infrastructure spend on security

cPacket's Benefits

- Security tools cannot be everywhere. NPM solution increases your security footprint; a ‘Two for One’ deal
- Provide network level insights to security tools for better decision making
- More monitoring points means more visibility and a better security footprint
- Seamlessly integrates with security

Today’s enterprises require comprehensive network security tools to safeguard every aspect of their network, data and information. As security concerns in data centers continue to rise, pervasive high-performing security solutions will become a necessity to maintain the integrity of data. Security attacks in a network can be considered minor, with little loss of data or financial resources, but many of them are considered major, or even catastrophic, resulting in data breaches and lost revenue. According to a recent report, Cybersecurity Ventures predicts that cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. In addition, it is estimated that by 2019, a business will fall victim to a ransomware attack every 14 seconds.

Cybersecurity Ventures predicts that cybercrime will cost the world $6 trillion annually by 2021

Achieving pervasive coverage is not possible with just security tools.
These tools need valuable network level insights to make informed decisions. Companies that adopt a security first approach and choose the right network performance monitoring tools (NPM) to protect their networks will gain a competitive edge. cPacket’s NPM tools are designed to increase network visibility, provide end-to-end security, and reduce MTTR for faster threat detection.

Network performance monitoring (NPM) and Network Security Monitoring (NSM) are like two sides of the same coin. While NPM provides valuable KPIs to ensure that your network and applications meet SLAs, NSM looks at the same KPIs to identify anomalies in the network to provide alerts on potential security attacks.

Over the years, some network protocols have earned the notorious distinction as tools to launch cyberattacks, such as DoS, DDoS and Man-in-the-middle (MitM). This document will discuss these protocols in detail and the required actions to effectively monitor and identify anomalous behavior(s).

1. DNS:
   Monitoring DNS activity is essential in identifying early signs of a DDoS attack. There have been many DNS based DDoS attacks reported in the past, and many will continue to occur. On October 21st, 2016, one of the largest cyberattacks occurred which brought down the majority of America's internet. The victim were the servers of Dyn, a company that controls much of the Internet's DNS infrastructure. Dyn estimated that the attack strength occurred at 1.2 terabits (1,200 gigabytes) per second. One preventative measure is to monitor DNS in-depth. DNS protocol uses two types of packets: DNS Request and DNS Response. Both packets need to be independently monitored. In the case of a DNS DoS attack, the ratio of number of DNS Request packets will be considerably higher than the number of DNS Response packets. Therefore, it is essential to monitor these two types of packets separately to obtain the granular view of DNS behavior and to alert SecOps when the ratio goes beyond a rational number.

2. DHCP:
   DHCP monitoring is needed for two specific reasons:

   a. NetOps need to know the time it takes for a device to obtain an IP address via DHCP. For a mobile service provider (SP), this is an essential requirement because of the growing number of people who use their mobile device to browse online. The slightest performance issue in a DHCP server can affect the user experience for a few thousand subscribers. This can be problematic, especially for an SP, when customer retention is a high priority and an important business KPI. Therefore, DHCP monitoring is important in order to troubleshoot issues where performance may have been degraded.

   b. DHCP Starvation is a well-known DDOS and man-in-the-middle (MitM) attack that is designed to deplete the DNS Server's IP address pool by flooding with DHCP requests using spoofed mac addresses. Once the server DHCP IP address pool is depleted, the attacker will launch a rogue DHCP server that replies to any other DHCP request with its own IP address, gateway and DNS. Ultimately, all traffic from the client to the host will flow through this network, creating a MitM attack. The result is a violation of privacy, a compromised network and financial loss. To prevent this situation, monitoring DHCP is essential, and SecOps need to identify DHCP Starvation issue early enough to take immediate action.

DHCP uses BOOTP as its transport protocol. Figure 1 below shows the four important types of DHCP packets, and the handshake mechanism between a client and a server. The four major packet types are: DHCP Discover, Offer, Request, and Acknowledge. From a security monitoring perspective, monitoring the volume of DHCP Request packets is essential in identifying the early warnings of a DHCP Starvation attack.

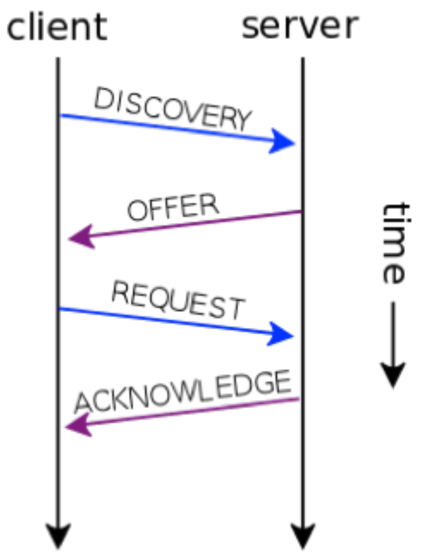

Figure 1: DHCP Protocol handshake

3. ARP:
   Address Resolution Protocol (ARP) monitoring can serve several purposes other than identifying external attacks. Oftentimes, a misconfigured device can start an ARP storm that effectively consumes the bandwidth and causes the network to slow to a crawl. Therefore, monitoring the ARP behavior as a number (count of ARP packets) as well as a percentage of network traffic in that segment can provide very useful metrics. When NetOps are armed with this information, they can effectively monitor, locate, and quickly cease ARP storms in the network.

4. TCP-SYN:
   TCP's SYN packet monitoring provides information regarding an important precursor to a DDoS attack. This type uses a flood of TCP SYN packets to consume enough server resources that renders the system unresponsive to legitimate traffic. SYN packets are the initial packets that the client sends to a server with an intent to establish a session. Every time a server accepts a SYN packet, it allocates server resources (memory buffers, file handles, socket related resources etc.), in anticipation that the connection will get established via a 3-way or a 4-way TCP handshake protocol (SYN-SYNACK-ACK or SYN-ACK-SYN-ACK). According to the protocol, the resources allocated to this session will not be immediately released because the server is anticipating ACKs for its 'half-open' sessions. The repercussion is a depletion of the server's resources, ultimately causing catastrophic results. Therefore, it's essential to continuously monitor for SYN flood.

5. ICMP:
   Monitoring the ICMP protocol is important to prevent both internal and external security attacks. To clarify, internal security breaches are those that originate within an organization's network, while external security breaches are those that originate outside the organization's network perimeter. Monitoring the overall throughput/count of ICMP packets will provide early warning(s) to an ICMP storm. Furthermore, there are a few ICMP subtypes that need to be independently monitored for the same security reasons. These subtypes include the following:

- ICMP Address Mask request
  From a protocol perspective, a gateway receiving an address mask request will reply with the address mask field set to the 32-bit mask of the bits identifying the subnet and network, for the subnet on which the request was received. An attacker can intentionally send an ICMP Type 17 Address Mask Request to gather information about a target's networking configuration. ICMP type 17 message triggers the remote system to respond with a list of its related subnets, as well as its default gateway and broadcast address via an Address Mask Reply (ICMP type 18) message. Armed with this information, the attacker can mount router-based attacks as well as denial-of-service attacks against the broadcast address. Although ICMP Type 17 and 18 are rare and often blocked by border firewalls and gateways, it is still useful to monitor for those intermittent occasions when these messages can pop up. It is also recommended to test whether the gateways and firewalls block them.

- ICMP Type 9 (mobile router advertisement) and ICMP Type 10 (ICMP Router Discovery Protocol –IRDP)
  The name IRDP can be misleading since this is not a routing protocol. ICMP Type 10 only enables hosts to discover the existence of neighboring routers, but can't interpret which router is best suited to reach a destination. The problem with this message is that it doesn't have any form of authentication, therefore, it's impossible for end hosts to know whether the information they receive is valid.
  An attacker can perform a MitM attack where it will act as a middle man for all the communication from the source to the endpoint. Attackers can also spoof ICMP router discovery messages, and remotely add bad route entries into a victim's routing table. Therefore, the victim's system would be forwarding the frames to the wrong address, making it unreachable to other networks. Such attacks can lead to DoS attack and can become quite severe. A preventative measure is to prevent ICMP route discovery and use digital signatures to block all type 9 and type 10 ICMP packets. To identify if your network can handle type 9 and 10 ICMP packets, monitoring the network is a highly recommended approach.

Using cPacket's NPM tools to Improve Network Visibility and Enhance Network Security

Every organization has their unique network environment (physical and/or virtual) and different security profiles that dictate their use for an NPM tool to secure their networks. Below are several use case examples and how cPacket solutions can be implemented to augment the security footprint in the network.

Example 1: Capture Relevant Data in a Single Dashboard

To mitigate security issues faster, NetOps/SecOps must be proactive rather than reactive. A single, easy to use, and highly customizable dashboard is imperative for NetOps and SecOps to have the ability to deep dive further into investigating the security of the network. Accurate and reliable data that can provide valuable metrics and KPIs allows security teams to mitigate any issues in the network before they occur. cPacket's cClear collects and correlates the data from the cStor to provide relevant metrics and KPIs in a single dashboard, and proactively sends alerts whenever anomalous activity is detected. Figure 2 below shows the cClear dashboard and security dashlets in real-time. This dashboard, as well as the dashlets can be easily modified within seconds, to suit the user's business needs.

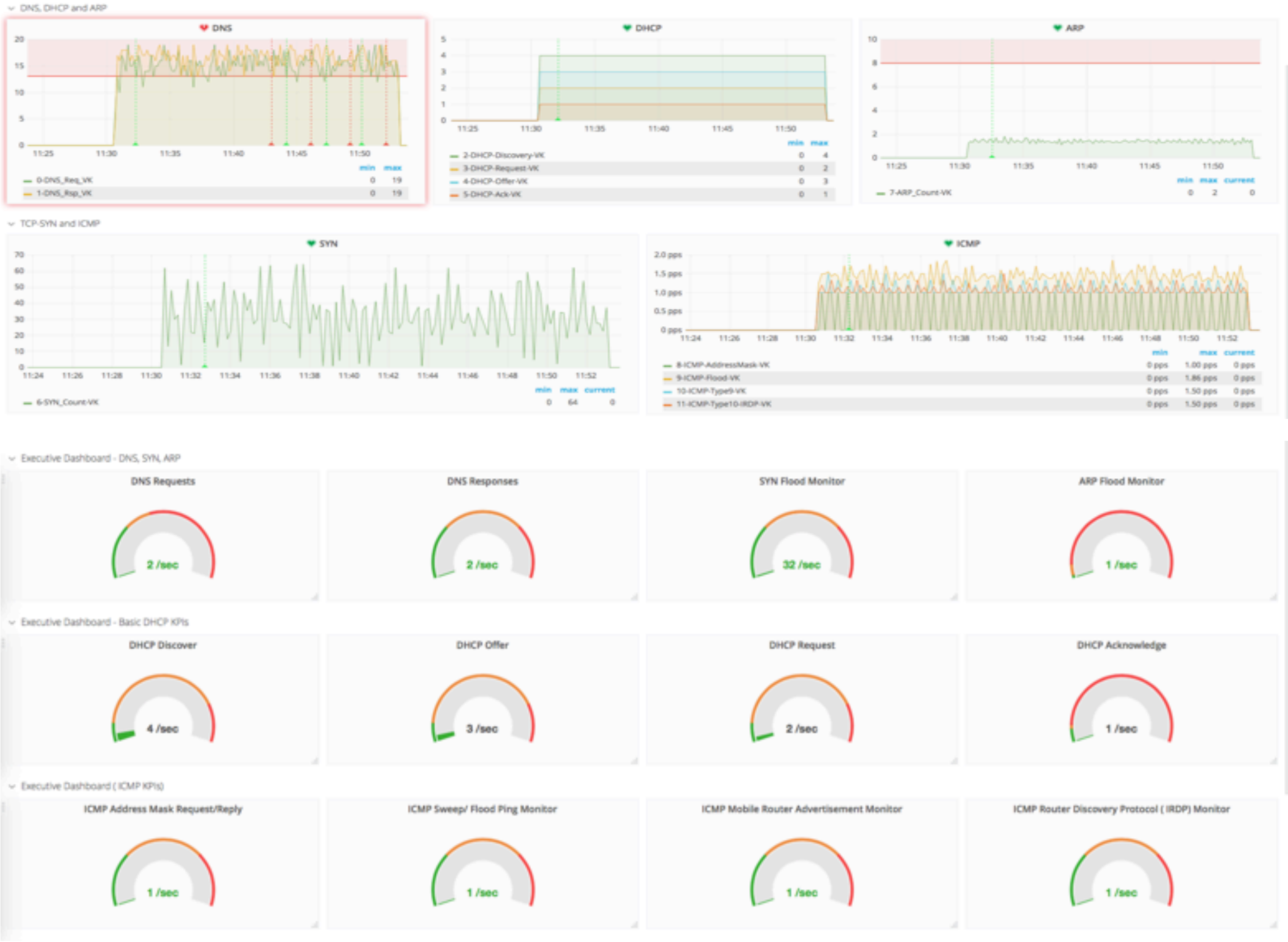
DNS, DHCP and ARP
DNS
0-DNS_Req_VK 0 19
1-DNS_Rsp_VK 0 19
DHCP
2-DHCP-Discovery-VK 0 4
3-DHCP-Request-VK 0 2
4-DHCP-Offer-VK 0 3
5-DHCP-Ack-VK 0 1
ARP
7-ARP_Count-VK 0 2 0
TCP-SYN and ICMP
SYN
6-SYN_Count-VK 0 64 0
ICMP
8-ICMP-AddressMask-VK 0 pps 1.00 pps 0 pps
9-ICMP-Flood-VK 0 pps 1.86 pps 0 pps
10-ICMP-Type9-VK 0 pps 1.50 pps 0 pps
11-ICMP-Type10-IRDP-VK 0 pps 1.50 pps 0 pps
min max current
Executive Dashboard - DNS, SYN, ARP
DNS Requests
2 /sec
DNS Responses
2 /sec
SYN Flood Monitor
32 /sec
ARP Flood Monitor
1 /sec
Executive Dashboard - Basic DHCP KPIs
DHCP Discover
4 /sec
DHCP Offer
3 /sec
DHCP Request
2 /sec
DHCP Acknowledge
1 /sec
Executive Dashboard (ICMP KPIs)
ICMP Address Mask Request/Reply
1 /sec
ICMP Sweep/ Flood Ping Monitor
1 /sec
ICMP Mobile Router Advertisement Monitor
1 /sec
ICMP Router Discovery Protocol (IRDP) Monitor
1 /sec

Figure 2: cClear dashboard displaying Security KPIs

Example 2: Improve Network Visibility with More Monitoring Points

Traditional monitoring architectures are often plagued with bottlenecks, reducing visibility and scalability. The TAP/aggregation solution can be valuable for monitoring live traffic, but can be costly because of the need for higher processing power seen in Figure 3 below. Scalability can also be an issue because such aggregators have a limited ability to filter out unnecessary traffic, and are unable to offload monitoring tools. As network environments evolve, traffic growth and increased port usage can result in reduced visibility because the aggregators become overwhelmed, may slow down, cause packet drops, or even stop working altogether. The result is degradation of the monitoring solutions in place. From a security perspective, the lack of visibility creates problems for NetOps and SecOps because they lack the relevant information needed to identify a problem before it results in a costly service disruption or data breach.

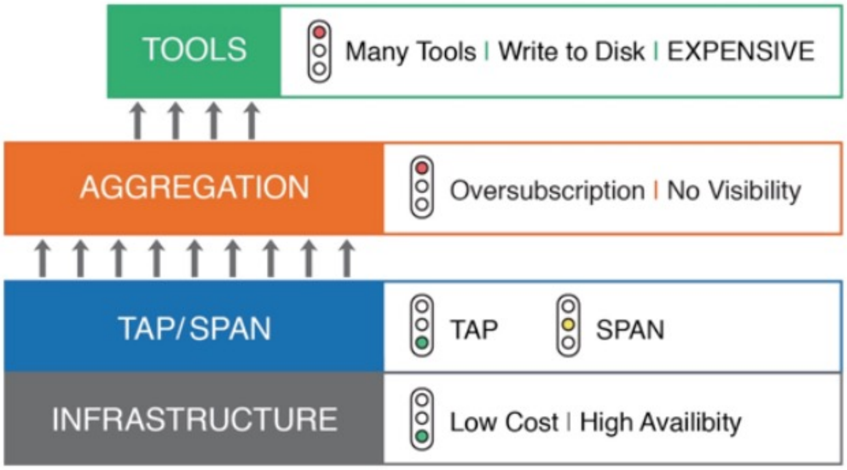
TOOLS
Many Tools | Write to Disk | EXPENSIVE
AGGREGATION
Oversubscription | No Visibility
TAP/SPAN
TAP
SPAN
INFRASTRUCTURE
Low Cost | High Availibity

Figure 3: Scalability of Network Monitoring Stack

cPacket's solutions are equipped with more monitoring points which effectively remove blind spots and allow for improved network visibility and security. cPacket's solution consist of cVu network probes (1G-100G, 24/32 ports) and cStor (64TB storage and analysis) devices that are deployed at critical monitoring points in the network, and managed by a cClear device that collects and correlates valuable KPIs seen in Figure 4 below. The cVu network probes can process KPI metrics as network traffic is carried off the wire from passive optical taps or SPAN ports, without the need to transport traffic to a central analyzer.

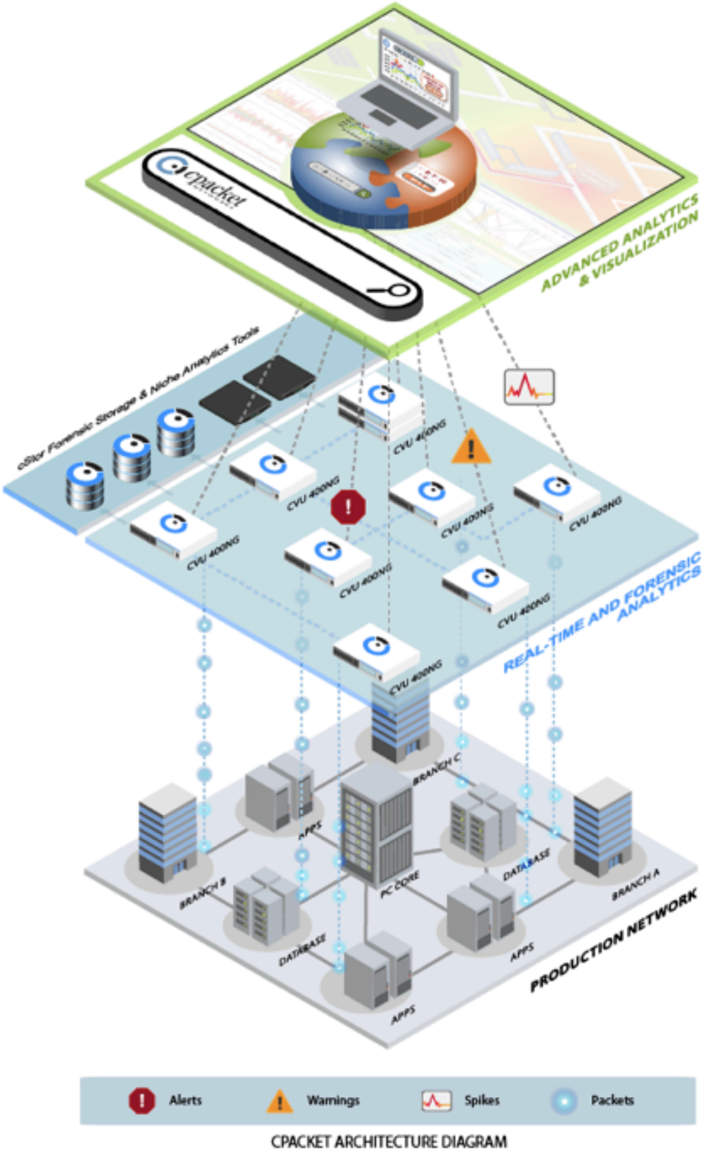

Figure 4: cPacket's Network Layer Diagram

Example 3: Reduce Mean Time to Resolution for Faster Threat Detection

The key to faster threat detection is having the ability to capture relevant data and respond to security issues in the network before they occur. With cPacket's scalable monitoring architecture and visibility fabric approach, NetOps and SecOps can respond faster to any security threats in the network. Furthermore, a visibility fabric can help eliminate issues associated with oversubscription and scale. As applications and networks grow over time, the amount of traffic can exceed the existing capabilities of security devices and reporting tools which can reduce network visibility as seen in Figure 5 below. With cPacket's scalable architecture and ability to process at line rate, security teams can access network traffic with greater flexibility. This allows them to allocate the right tools at the right time in order increase response time. Figure 6 below shows cPacket's architecture which eliminates oversubscription and bottlenecks by removing the aggregation layer from the monitoring stack.

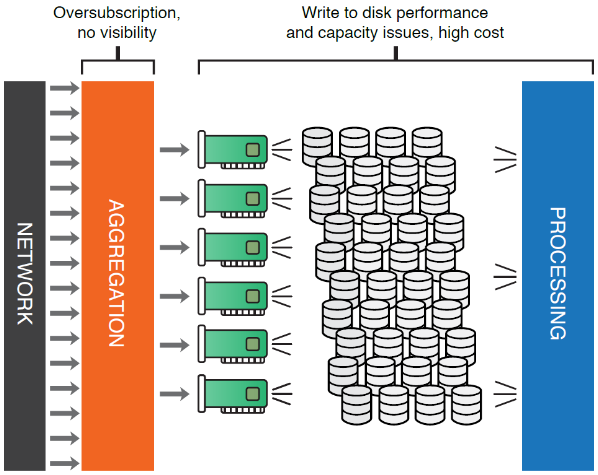
Oversubscription, no visibility
Write to disk performance and capacity issues, high cost
NETWORK
AGGREGATION
PROCESSING

Figure 5: Traditional Monitoring Stack

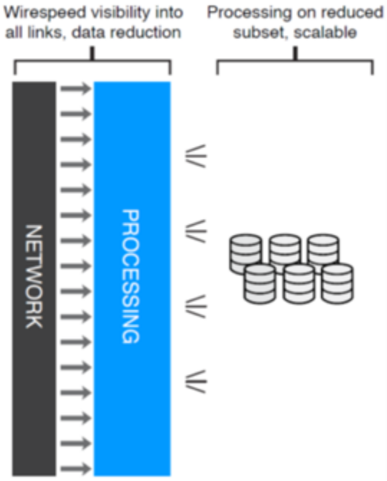
Wirespeed visibility into all links, data reduction
Processing on reduced subset, scalable
NETWORK
PROCESSING

Figure 6: Processing at the wire removes bottlenecks and improves

Conclusion

Having a secure network infrastructure that can prevent and mitigate security threats is important to ensuring smooth business operations. When networks are not adequately secured, they become vulnerable to data breaches, and in some cases, find it impossible to fully recover from the financial repercussions. Organizations need to implement the right NPM tools, so they can be agile enough to address potential issues before their business becomes the target of an attacker and a costly breach. cPacket's always on network monitoring solutions offer the foundation of a strong and cost-effective strategy that can provide a positive ROI for organizations looking to improve the security of their networks.

Contact Us

To learn more about our products and solutions, please visit www.cpacket.com