

Detecting Threats & Anomalies Then Taking Action

Securing the internal network requires the ability to see the issues when they occur, understand the nature of the problem, and respond with the appropriate action. The action should be surgically precise and affect only the “bad” traffic without penalizing performance. The following examples demonstrate how cVu appliances can help network managers detect problems and take proactive steps to secure their networks.

Dark IPs – Worm Behavior

The presence of network traffic with unused destination addresses (“dark IPs”) is often indicative of a possible worm infestation. The worm tries to scan the network to find vulnerable machines to infect. Therefore, monitoring network traffic to “dark IPs” can be used to identify infected hosts.

Solution:

cVu is configured to alert if network traffic to “dark IPs” is detected. It can also be configured to selectively block the bad traffic if deemed harmful or capture it for further investigation and forensics.

Request to Reply Ratios – Scanning for Anomalies

Healthy networks exhibit balanced behavior such as requests being matched by replies. For example, the number of ICMP echo requests should have a matching number of replies. Similarly, each ARP request should have a reply. Unbalanced behavior usually indicates host scans or network misconfiguration.

Solution:

cVu is configured to alert if the ICMP echo request/reply ratio or ARP query/response ratio deviates from a healthy level (ideally equal to one). Traffic from infected hosts can be selectively controlled to contain infections.

Detecting Evasion – ICMP/SSH Encapsulation

A good example of a connection hiding technique is the Ping Tunnel (Ptunnel) open source utility, where TCP connections are tunneled over ICMP with encrypted payload (SSH) and appear as innocent ping packets. Users can use Ptunnel to send and receive unauthorized traffic that evades detection by firewalls or content inspection tools.

Solution:

cVu is configured to trigger on ICMP packets with payload that establishes a Ptunnel connection and to block such connection attempts.

Application Traffic – “normal” vs. “others”

Traffic over TCP or UDP ports which are not used by standard applications might indicate port scanning or use of unauthorized applications.

Solution:

cVu is configured to alert if network traffic over non-standard ports exceeds some specified threshold. Traffic can be selectively blocked if deemed harmful or captured for further investigation and forensics.

Keep Alive

Hosts that become inactive and stop sending traffic may indicate a server crash, security issue, or load balancer failure.

Solution:

cVu is configured to trigger if there is no network traffic from a host or set of hosts for some period of time. For example, if there is not at least one packet per n seconds from the host the administrator is alerted.

Virtual E-Patching of Servers

Software applications need to be continuously patched against newly discovered vulnerabilities. Often servers can be patched only during pre-scheduled service intervals in order to minimize business disruptions. Until the right software patch can be verified and installed, a virtual network E-patch can prevent the particular vulnerability from spreading over the network.

Solution:

cVu is configured to block the SQL slammer (Sapphire) worm. On the fly payload inspection and pattern matching identify packets with the worm code and the “bad” packets are dropped to prevent propagation and protect vulnerable hosts until they can be patched.

Non-standard ports – Encapsulation Masquerading and Evasion

Users can evade corporate firewall policies by using open ports such as 53 and 80 for “banned” applications (e.g. rogue mail server, file sharing, etc.). Deep packet inspection of the payload of every packet is required to detect such evasion techniques.

Solution:

cVu is configured to trigger if SMTP (send-mail) connections are made over a port that is not the standard TCP port 25.

Error Messages – Destination Unreachable

Malicious port scans from outside or inside the firewall perimeter might be reconnaissance prior to an attack. Large numbers of “destination unreachable ICMP error messages” might indicate that a scan is in progress. When the number of destination unreachable error messages is “unusual”, it is indicative of potential issues.

Solution:

cVu is configured to trigger if the number of destination unreachable ICMP error packets exceeds some threshold. cVu can selectively duplicate those packets, allowing drill down and root cause analysis.

Summary

cPacket brings granular network behavioral information and surgical response capabilities to the LAN. This document describes several cVu 1000 use cases for identifying and containing threats. With cVu, network managers spend less time on tedious reactive troubleshooting and more time on enhancing network performance and reliability.



2061 Landings Drive
Mountain View, CA 94043
650.969.9500 **T**
650.969.4900 **F**
www.cpacket.com

