vehere

WHITEPAPER

NetFlow vs Full Packet Capture Based Detection – A Comparative Analysis

Numerous vulnerabilities, zero-day exploits, ransomware, malware, and other threats persistently impact organizations. To counter these threats, organizations have the option to employ either NetFlow-based detection or full packet capture-based detection. This whitepaper aims to explore the advantages of utilizing full packet capture-based detection, which offers a superior edge compared to traditional NetFlow-based detection.

What is NetFlow?

NetFlow is a feature that was introduced on Cisco routers around 1996 that provides the ability to collect IP network traffic as it enters or exits an interface. NetFlow provides metadata based on the activity over the network. NetFlow can only give a high-level view of what is going on across the network. It can provide metadata like IP Addresses, Ports, Network protocols, number of bytes, number of packets, etc.

Reference:
https://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9.html

NetFlow does not provide details about the protocol header or payload which limits it uses from detection perspective. For example, if a malware file is getting downloaded over the network or if an exploit attempt is being made over the network, it cannot be detected by NetFlow-based detection.

What is DPI or Deep Packet Inspection?

Deep Packet inspection, or full packet capture, enables a thorough inspection of the network traffic. It allows us to reconstruct data, which helps us figure out what is going on over the network. With DPI, we can parse not only network protocols but also various application layer data like headers, payloads, and files.

This enables detecting threats that were not possible with NetFlow, as NetFlow only provides data related to performance monitoring and visibility.

DPI can accurately reconstruct exactly what happened and when it happened, so you can uncover the cause of a security incident quickly and definitively.

Why is DPI better than NetFlow?

NetFlow can only provide data that is related to network performance monitoring/visibility. It cannot parse various

network or application layer protocol fields, which makes NetFlow-based detection limited. For example, with NetFlow-based rules, we cannot get http headers, SMB protocol, or any other protocol-related payload or field.

There are many zero-day vulnerabilities, malware, and ransomware threats that use a variety of tactics to compromise and gain access to organizations; they also use a variety of lateral movement techniques once they get inside an organization.

Some of them involve exploiting vulnerable software or using SMB to spread across networks.

Vehere DPI Technology:

Vehere's products are capable of parsing various network protocols and extracting fields and payloads from them. This enables one to write detections based on them. With DPI, one can easily catch a malicious user agent used by a botnet, an anomalous URL pattern used in an exploitation attempt, or a file being transferred over the SMB for lateral movement.

Here are some examples from the security research team's detection where they have used **full packet capture;** these types of rules cannot be done with **only flow-based** detection (NetFlow):

- **TI08105 SMB Brute force Attempt:** This rule detects multiple login connections to an SMB server to determine the username and password combination to access the system. This could be an internal or external host trying to determine the password.
- **TI01042 High TXT Records Requests Rate:** This rule detects data exfiltration using DNS TXT records.
- **TI10146 High SMB Peer:** This rule indicates one client has connected to many systems using the SMB protocol. This could be a case where a malware connects to several other hosts after infecting one client in a short span of time.
- **TI10114 Executable Upload to ADMIN share using SMBv2 Lateral Movement:** There are various lateral movement activities that happen over SMB. This signature checks for any .exe upload to the ADMIN share. This detection can be easily done with full packet capture, as one gets the entire session and payload, but it will be difficult or impossible to do with only flow-based detection.
- **TI10136 SCMR Enable Remote Registry access service SMBv1 Lateral Movement:** This signature requires checking the SMB named pipe first, then checking the MSRPC UUID, followed by checking the MSPRC operation number, which cannot be done with NetFlow-based detection

Conclusion:

While NetFlow has its own use cases, DPI provides better protection than NetFlow. With the parsing capabilities that come with DPI, it becomes easy to detect various threats over the network, like zero-days, exploits, malware, ransomware, etc. Detecting various tactics like initial access, exfiltration, and lateral movement can be easily detected by DPI-based detection compared to NetFlow-based detection.

Appendix:

Vehere's Full Packet Capture Based rules:

- TI10136 SCMR Enable Remote Registry access service SMBv1 Lateral Movement
- TI08104 Telnet Brute Force Attempt
- TI10119 DLL Upload to ProgramFiles Dir using SMBv1 Lateral Movement
- TI10127 Exe Upload to System32 Dir using SMBv2 Lateral Movement
- TI10134 Executable Upload to Windows Dir using SMBv1 Lateral Movement
- TI08105 SMB Brute force Attempt
- TI10122 Remote Registry System Services Key smbv1 Lateral Movement
- TI10118 DLL Upload to ProgramFiles Dir using SMBv2 Lateral Movement
- TI10115 Executable Upload to ADMIN share using SMBv1 Lateral Movement
- TI10130 User Enumeration using SRVSVC service SMBv1 Lateral movement
- TI10138 Remote Registry RunServices Key smbv1 Lateral Movement
- TI01042 High TXT Records Requests Rate
- TI10112 User Enumeration using SAMR service SMBv2 Lateral movement
- TI10141 Share Enumeration using SRVSVC service SMBv2 Lateral movement
- TI10125 Remote Registry AppInit DLL smbv2 change Lateral Movement
- TI01056 Suspicious DNS Query with Base64 Encoded String
- TI10111 Executable Upload to C share using SMBv2 Lateral Movement
- TI10121 Remote Registry WinLogon Key Shell smbv2 Lateral Movement
- TI10128 User Enumeration using WKSSVC service SMBv1 Lateral movement
- TI10143 Remote Registry Run Key smbv2 Lateral Movement
- TI03036 Empty User Agent
- TI10142 Remote Registry Run Key smbv1 Lateral Movement
- TI10131 User Enumeration using SRVSVC service SMBv2 Lateral movement
- TI03033 Exploit Framework User Agent Seen in Network Traffic
- TI10135 Executable Upload to Windows Dir using SMBv2 Lateral Movement
- TI10137 SCMR Enable Remote Registry access service SMBv2 Lateral Movement
- TI10144 Remote Task Scheduling Lateral Movement
- TI01074 DNS TXT Answer with Possible Execution Strings
- TI01058 High NULL Records Requests Rate
- TI10132 SID enumeration via LSA service SMBv1 Lateral Movement
- TI01107 Large Fragments in a Flow
- TI10139 Remote Registry RunServices Key smbv2 Lateral Movement
- TI10120 Remote Registry WinLogon Key Shell smbv1 Lateral Movement
- TI10123 Remote Registry System Services Key smbv2 Lateral Movement
- TI01108 Small Fragments In a flow
- TI10113 User Enumeration using SAMR service SMBv1 Lateral movement
- TI13095 SSH Reverse Shell
- TI03016 Raw Paste Service Access
- TI01073 Possible DNS Tunneling
- TI03020 Suspicious User Agent in Network Traffic
- TI10114 Executable Upload to ADMIN share using SMBv2 Lateral Movement
- TI01092 ARP Scan
- TI10124 Remote Registry AppInit DLL smbv1 change Lateral Movement
- TI10126 Exe Upload to System32 Dir using SMBv1 Lateral Movement
- TI05504 Remote PowerShell Session
- TI10133 SID enumeration via LSA service SMBv2 Lateral Movement
- TI10140 Share Enumeration using SRVSVC service SMBv1 Lateral movement

- TI01057 Wannacry Killswitch Domain
- TI10129 User Enumeration using WKSSVC service SMBv2 Lateral movement
- TI10146 High SMB Peer
- TI04013 Oracle WebLogic Exploit
- 10007 Blacklisted SSL-fingerprint
- TI08106 FTP Brute force Attempt
- TI10110 Executable Upload to C share using SMBv1 Lateral Movement
- TI03021 Download from unknown TLDs
- 10009 Blacklisted HTTP URL
- 10012 High data transfer to a country

References:

Vehere Netflow Vs DPI Paper:
https://vehere.com/resource/whitepaper-netflowvsdpi/

F5 BIG-IP Vulnerability:
https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-206a

Log4J Vulnerability:
https://www.wsj.com/articles/what-is-the-log4j-vulnerability-11639446180

ProxyShell Vulnerability:
https://www.socinvestigation.com/proxyshell-vulnerability-large-exploitation-of-microsoft-exchange-servers/

Lateral Movement:
https://www.securityweek.com/lateral-movement-when-cyber-attacks-go-sideways/

Authored by:

- Winny Thomas, Principal Security Architect
- Hardik Shah, Principal Security Researcher
- Parin Dedhia, Security Researcher