NETFORT know your network

LANGuardian

Comparison of network traffic analysis protocols.

NetFort LANGuardian analyzes the traffic on your network and uses advanced deep packet inspection techniques to give you a unique level of visibility into everything that's happening on your network, including user activity, file and database monitoring, intrusion detection, bandwidth usage, and Internet access. LANGuardian can analyze full packet data as well as flow data conforming to the NetFlow and sFlow protocols. This document lists the main features of LANGuardian and shows their availability in terms of the traffic information that is provided to the software.

Data	Description	Pcap	NetFlow	sFlow
		Full packet data	Flow data from a Cisco router	Flow data from an sFlow-capable router
Flow data				
IP flow logging	For every IP flow, record: Source IP protocol Destination IP protocol Start time End time TOS Volume sent and received For TCP and UDP flows, the source and destination port numbers are also recorded.	Yes	Yes	Yes
Ethernet flow logging	For every Ethernet flow, record: Source MAC address Destination MAC address Timestamp	Yes	No	No
Proxy flow logging	Proxy traffic is decoded to extract the following information: Machines running HTTP proxies Busiest proxies Sites accessed via a proxy	Yes	No	Partial
TOS logging	The IP Type of Service recorded for each IP flow.	Yes	Yes	Yes
TCP state	Analyzes TCP session	Yes	Yes	Partial

Data	Description	Pcap	NetFlow	sFlow
tracking	establishment to construct a list of all servers and services running on the internal network.			
Alert Data				
Signature-based intrusion detection system (IDS)	Enables real-time detection and alerting of malicious events that occur on your network via a rule-based language.	Yes	No	No
Portscans	Multiple connections from one IP to multiple ports on a single IP address.	Yes	Yes	Yes
Netscans	Multiple connections from one IP to a single (or multiple) port on multiple IP addresses.	Yes	Yes	Yes
Volume overflows	Volume overflow alerts are used to identify, short-lived high data transfer rates. A sample use case is to identify the transfer of more than 100 MB in 60 seconds.	Yes	Yes	Yes
DPI alerts				
Microsoft filename detection	Monitors and records every access to Windows file shares, recording details of: User name Client application Server name Event type File name Data volume	Yes	No	No
New MAC address	Creates an alert if a new MAC address is seen on the network	Yes	No	Partial
Website access logging	Logs all web accesses, whether direct or through proxy servers,	Yes	No	Partial
Domain watchlist	Creates an alert if a user accesses a site that is known to contain malware.	Yes	No	Partial
DNS spam detection	Creates an alert if a system that is not running a mail server generates an excessive number of DNS MX record look ups.	Yes	No	Partial
URI logging	Enables you to see the exact page on a website that a user was visiting.	Yes	No	Partial
Microsoft SQL Server logging	Monitors and records every access to Microsoft SQL Server databases.	Yes	No	Partial
SMTP logging	Decodes incoming and outgoing SMTP traffic to and from the	Yes	No	Partial

Data	Description	Pcap	NetFlow	sFlow
	organization, and extracts the following information from email headers: Sender Recipient Subject			
Web client detection	Enables detection of which web browers are used by systems on the network.	Yes	No	Partial
Network inventory				
Service resolution	Uses passive traffic analysis techniques to identify the applications running on a server.	Yes	No	Partial
Operating system identification	Uses passive traffic analysis techniques to identify the the operating system running on a system.	Yes	No	Partial
DNS hostname resolution	Using passive traffic analysis techniques to identify the hostname associated with an IP address without the system generating look ups itself.	Yes	No	Partial
Misc				
Identify module support	Tracks all events and traffic statistics back to an Active Directory account. This is done by interegrating data from Active Directory logs into the LANGuardian internal database.	Yes	Yes	Yes
Bandwidth quota manager	Identifies bandwidth hogs and monitors their bandwidth consumption,	Yes	Yes	Yes

About NetFort Technologies

NetFort Technologies provides a range of software products to monitor activity on virtual and physical networks. Headquartered in Galway, Ireland, NetFort Technologies was established in 2002 and has built up a global customer base in the enterprise, education, and government sectors.

North America Sales Office
11th Floor
120 Eglinton East
Toronto, ON
M4P IE2
Canada

☎ +1 (647) 947 9154

UK Sales Office
27 Old Gloucester Street
London
WC1N 3XX

☎ +44 (207) 060 2850

Asia-Pacific Sales Office
1B Mincom Central Building
Suite 251
192 Ann Street
Brisbane
Queensland 4000
Australia

☎ +61 (7) 3177 7682

Head Office
Unit 7
IDA Innovation Centre
Upper Newcastle
Galway
Ireland

☎ +353 (91) 520 501

Email: sales@netfort.com