NetFlow Optimizer™

User Guide

Version 2.4.8 (Build 2.4.8.0.2)

February 2017

Contents

About this Guide 3
How NetFlow Optimizer Works 3
What Are Modules and Converters? 3
How External Data Feeder for NFO Works 5
How to Use this Guide 5
Solutions at a Glance 6
Modules Specifications 9
Network Traffic and Devices Monitoring 9
Top Traffic Monitor (10067 / 20067) 9
Top Pairs Monitor (10064 / 20064) 12
Top Connections Monitor (10063 / 20063) 15
Top Packets Monitor (10068 / 20068) 18
Network Subnets Monitor (10011 / 20011) 20
TCP Health Monitor (10060 / 20060) 22
CBQoS Monitor (10065 / 20065) 24
Autonomous Systems Monitor (10066 / 20066) 26
Enhanced Traffic Monitor 27
Top Traffic Monitor Geo Country (10967 / 20967) 27
Enhanced Traffic Monitor 2 31
Top Traffic Monitor Geo City (10867 / 20867) 31
Network Bandwidth Consumption Monitor by Application for Blue Coat PacketShaper 33
Network Bandwidth Consumption Monitor (10964 / 20964) 33
Security 35
Hosts Geographical Location Monitor (10040 / 20040) 35
Botnet Command and Control Traffic Monitor (10050 / 20050) 38
Host Reputation Monitor (10052 / 20052) 40
Threat Feeds Monitor (10053 / 20053) 42
Email 44
Outbound Mail Spammers Monitor (10025 / 20025) 44
Inbound Mail Spammers Monitor (10026 / 20026) 46
Unauthorized Mail Servers Monitor (10027 / 20027) 49
Rejected Emails Monitor (10028 / 20028) 50
Services Monitor 51
DNS Monitor (10004 / 20004, 20005) 51
Asset Access Monitor (10014 / 20014) 55
Services Performance Monitor (10017 / 20017) 57
Cisco ASA Devices Monitoring 60
Top Bandwidth Consumers for Cisco ASA (10018 / 20018) 60
Top Traffic Destinations for Cisco ASA (10019 / 20019) 62
Top Policy Violators for Cisco ASA (10020 / 20020) 63
Top Hosts with most Connections for Cisco ASA (10021 / 20021) 65
Palo Alto Networks Devices Monitoring 66
Top Bandwidth Consumers for Palo Alto Networks (10030 / 20030) 66
Top Traffic Destinations for Palo Alto Networks (10031 / 20031) 68

Hosts with Most Policy Violations for Palo Alto Networks (10032 / 20032) 70
Most Active Hosts for Palo Alto Networks (10033 / 20033) 71
Bandwidth Consumption per Application for Palo Alto Networks (10034 / 20034) 73
Bandwidth Consumption per Application and Users for Palo Alto Networks (10035 / 20035) 74
VMware 76
Top VM:Host Pairs (10164 / 20164) 76
Top VM Traffic Monitor (10167 / 20167) 78
Utilities 80
Sampling Monitor (10002 / 20002) 80
SNMP Information Monitor (10003 / 20003) 82
Special Converters 84
Original Flow Data (20001) 84
sFlow Data (20800, 20900) 86
FDR Packeteer-2 Flow Data (20010) 88
Appendix 94
NetFlow v5 - NetFlow v9 Field Types Mapping 94

About this Guide

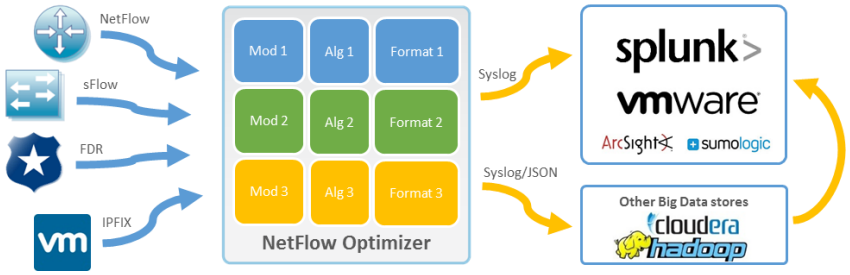
Use this User Guide to learn about NetFlow Optimizer (NFO), its Modules and Converters, their functionality, inputs, outputs, and configuration parameters.

Announcement of product name change

Our core product NetFlow Integrator, or NFI, is now called NetFlow Optimizer (NFO). NFI Updater, or Updater, is now called External Data Feeder for NFO. All references to NetFlow Integrator (NFI) or NFI Updater in this document apply to NetFlow Optimizer or External Data Feeder for NFO.

How NetFlow Optimizer Works

NetFlow Optimizer is a software-only processing engine for network flow data (NetFlow, IPFIX, sFlow, jFlow, etc.). **It is not a NetFlow collector**.



NetFlow Optimizer accepts network flow data from network devices (routers, switches, firewalls), applies map-reduce algorithms to the data to extract the information needed to address desired use cases, converts the processed data to syslog (or other formats such as JSON), then sends that useful information to your visualization platform or SIEM.

By enabling appropriate Modules, you turn on specific functionality within NetFlow Optimizer. For example, you can monitor:

- your network conversations and hosts' behavior
- your network devices
- malicious host (e.g. botnets, scanning hosts) communications to your data center

And many other use cases are expressed via the Modules.

What Are Modules and Converters?

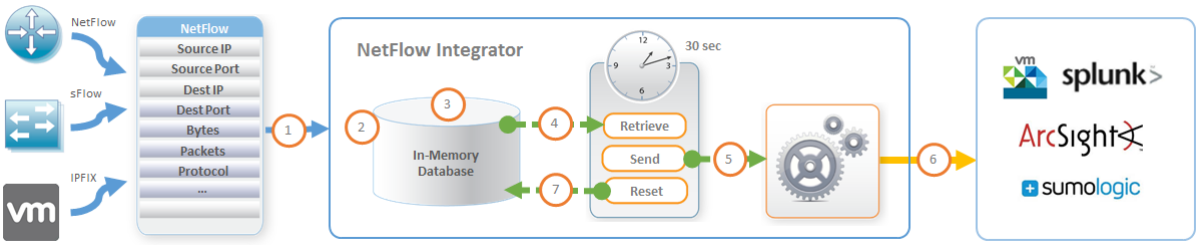
NetFlow data is notoriously voluminous. Traditionally, all NetFlow records generated by network devices are captured and stored for further interpretation. This exact process of capturing all NetFlow records, without understanding the significance of information contained in the records' data, creates tremendous storage and data analysis problems. A mid-range 20 Gb device in a large office can process tens of thousands of network exchanges per second, which results in a hundred thousand NetFlow records per second. Assuming that each NetFlow record is 100 bytes long, storing data at this rate it would take 8.6TB of disk space every day. Even a smaller switch, router or firewall that processes 10 times less network connections produces 860GB of flow data every day.

NetFlow Optimizer Modules and Converters are designed to provide solutions for specific use cases and at the same time reduce the amount of data (without losing information veracity) that needs to be stored by orders of magnitude. The Modules and Converters are packaged into Module Set packages. Each Module consists of one or more content-based rules and one or more time-based triggers (called "Data Collection Interval"). Converters provide

mechanisms for translating information emitted by the Modules into a format suitable for further processing. Please see Solutions at a Glance section below for more details.

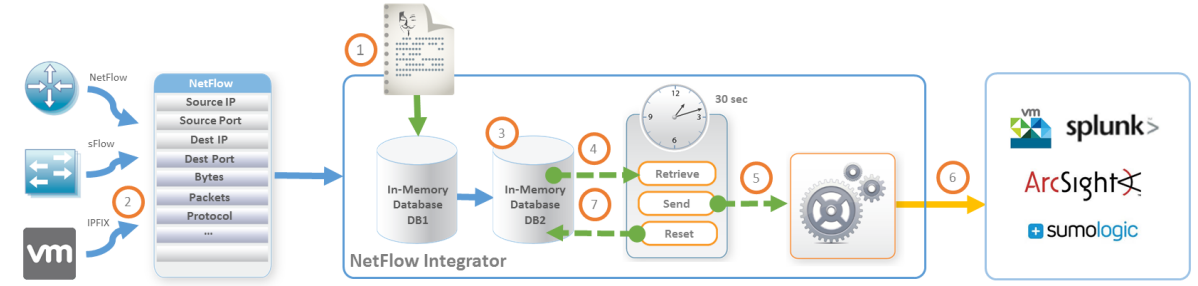
Let us consider a typical example: a network administrator would like to know how the bandwidth of his Cisco ASA firewall is consumed. This is not possible using traditional Cisco ASA logging because setting logging at the Informational level severely impacts device performance. A better approach is to use Cisco ASA NetFlow Secure Event Logging (NSEL) but the sheer volume of NSEL data may overwhelm traditional NetFlow collectors. This is when NetFlow Optimizer's Modules mechanism comes to the rescue.

The diagram below shows how data reduction is implemented in the Top Bandwidth Consumers Module. This Module employs an in-memory Map-Shuffle-Reduce algorithm. To report top 50 bandwidth consumers, the Module sums up bytes by source IP/Port, Destination IP/Port, and Protocol -- processing every single flow record over a short period of time (e.g. 30 seconds) (Map), then the data is sorted by accumulated bytes (Shuffle), and finally the top 50 records are retrieved (Reduce), converted to syslog, and sent to a SIEM system (e.g. Splunk Enterprise). Thus this Module processes thousands of flow records per second, and reports only top 50 bandwidth consumers every 30 seconds, which are typically responsible for 98%-99% of all traffic bandwidth consumtion.



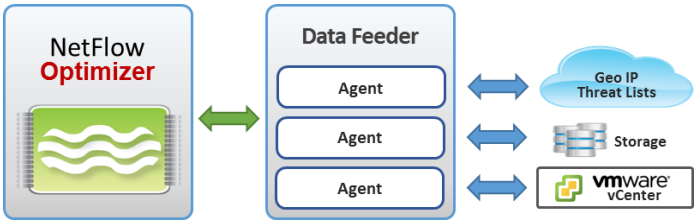
1. NetFlow Integrator receives all NetFlow (sFlow, IPFIX) records from network devices
2. Each record is processed and its bytes and packets are summed up in in-memory database by Source IP/Port, Destination IP/Port, and Protocol over the Data Collection Interval (e.g. every 30 seconds, configurable parameter)
3. At the end of the Data Collection Interval, the records are sorted by bytes
4. Top 50 records are retrieved
5. And sent to the Converter
6. They are translated from binary format to other format (e.g. syslog) and sent to the SIEM
7. In-Memory Database is dropped making room for the next 30 seconds worth of data

NFO Modules' use cases are not limited to NetFlow Consolidation. Another diagram below shows how security NFO Module reports all malicious network conversation based on threat lists.



1. External security threat list is loaded into In-Memory database 1 (DB1) when the module is configured
2. NetFlow Integrator receives all NetFlow (sFlow, IPFIX) records from network devices
3. Each flow's Source and Destination IP addresses are matched against the threat list in DB1, and only those flows that match are stored in In-Memory database DB2
4. At the end of the Data Collection Interval, the records from DB2 are retrieved
5. sent to the Converter, where
6. they are translated from binary format to other format (e.g. syslog) and sent to the SIEM
7. In-Memory Database DB2 is dropped making room for the next 30 seconds worth of data

How External Data Feeder for NFO Works



External Data Feeder for NFO (EDFN) is a remote component which serves as a knowledge base of information outside of the NetFlow domain. Its task is to provide NetFlow Optimizer with information generally unavailable in the data streams supplied by NetFlow/IPFIX exporters.

EDFN is comprised of a Platform and a collection of Agents each of which is designed to obtain information of a certain kind. The Platform provides a common interface for the Agents' configuration and data exchange and serves as a conduit for delivering information collected by the Agents to the NetFlow Optimizer. Typically External Data Feeder for NFO is installed on a separate server with access to the internet.

How to Use this Guide

The Modules Specification section contains detailed descriptions of the Modules. Modules are numbered from 10000. Each Converter produces its' own type of syslog message, identified by a special field: nfc_id. For example, "Top Bandwidth Consumers for Cisco ASA (10018/20018)" Module has the corresponding Converter 20018. The syslog message produced by this Converter-20018 is identified by the field **nfc_id =20018**.

All Modules are configurable. Parameters to specify the granularity and the amount of consolidated flow data to be sent out are described at the end of each Module specification. For example, "Data Collection Interval, sec" sets the interval for the Module time trigger. Top N parameter specifies the number of records (usually per exporter) to be converted and sent out. Other parameters may specify a list of IP addresses, or subnets, or ports, depending on the use case of the Module.

Solutions at a Glance

The table below shows which Modules need to be enabled to turn on NetFlow Optimizer specific solutions and corresponding Splunk application menu.

Module Set (package name) Module Name (AppMod id / syslog id)	Description
Network Traffic and Devices Monitor (network_monitor)	
Network Subnets Monitor (10011 / 20011)	Reports top bandwidth consumers for each monitored subnet
TCP Health Monitor (10060 / 20060)	This Module reports TCP Health by detecting top hosts with the most TCP Resets
Top Connections Monitor (10063 / 20063)	This Module identifies hosts with the most connections
Top Pairs Monitor (10064 / 20064)	This Module reports top Host Pairs network conversations
CBQoS Monitor (10065 / 20065)	This Module reports traffic for all DSCP bits combinations (QoS)
Traffic by Autonomous Systems (10066 / 20066)	This Module reports traffic by all Autonomous Systems (AS)
Top Traffic Monitor (10067 / 20067)	This Module identifies hosts with the most traffic
Top Packets Monitor (10068 / 20068)	This Module identifies hosts with the most packets
Enhanced Traffic Monitor (enhanced_top_traffic_monitor)	
Top Traffic Monitor Geo Country (10967 / 20967)	This Module identifies hosts with the most traffic and reports Reputation and Geo locations of source and destination hosts
Enhanced Traffic Monitor 2 (enhanced_top_traffic_monitor_2)	
Top Traffic Monitor Geo Country (10967 / 20967)	This Module identifies hosts with the most traffic and reports Reputation and Geo locations of source and destination hosts
Network Bandwidth Consumption Monitor by Application for Blue Coat PacketShaper (bc_packetshaper_monitor)	

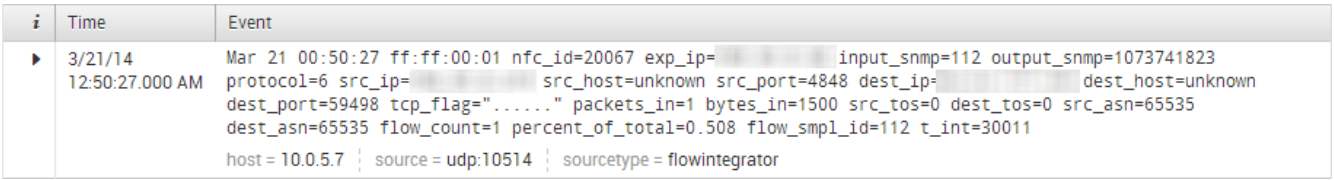
Network Bandwidth Consumption Monitor (10964 / 20964)	This Module reports network bandwidth consumption by pairs of network users per application kind per PacketShaper instance.
Security (security)	
Visitors by country (Hosts GeoIP) (10040 / 20040)	This Module identifies hosts with most traffic, and reports them with their geographical locations
Botnet C&C Traffic Monitor (10050 / 20050)	This Module monitors traffic originated from known Command and Control hosts (C&C) or directed to these hosts
Host Reputation Monitor (10052 / 20052)	This Module uses a host reputation database from Alienvault (www.alienvault.com) to report communications with malicious peers
Threat Feeds Traffic Monitor (10053 / 20053)	This Module monitors traffic originated from known threat lists specified as IP blocks, list of domains, or IP addresses.
Email (email_monitor)	
Outbound Mail Spammers Monitor (10025 / 20025)	This Module detects internal hosts infected with spam malware
Inbound Mail Spammers Monitor (10026 / 20026)	This Module detects external hosts sending excessive email traffic to your organization
Unauthorized Mail Servers Monitor (10027 / 20027)	This Module detects internal hosts running unauthorized mail servers
Rejected Emails Monitor (10028 / 20028)	This Module detects external hosts sending emails rejected by internal mail servers
Services Monitor (services_monitor)	
DNS Monitor (10004 / 20004, 20005)	This Module monitors DNS servers and DNS traffic
Asset Access Monitor (10014 / 20014)	This Module monitors traffic to selected services and matches communications to a list of authorized peers
Services Performance Monitor (10017 / 20017)	This Module monitors services performance characteristics
Cisco ASA (cisco_asa)	

Top Bandwidth Consumers for Cisco ASA (10018 / 20018)	This Module provides a list of top network bandwidth consumers operating on the internal network
Top Traffic Destinations for Cisco ASA (10019 / 20019)	This Module provides a list of most popular destinations measured by the traffic
Top Policy Violators for Cisco ASA (10020 / 20020)	This Module provides a list of firewall policies violators
Top Hosts with most Connections for Cisco ASA (10021 / 20021)	This Module provides top N (by the number of connections) consumers (users)
Palo Alto Networks (panw_monitor)	
Top Bandwidth Consumers for Palo Alto Networks Firewall (10030 / 20030)	This Module provides a list of top network bandwidth consumers operating on the internal network
Top Traffic Destinations for Palo Alto Networks Firewall (10031 / 20031)	This Module provides a list of top network bandwidth destinations
Hosts with Most Policy Violations for Palo Alto Networks Firewall (10032 / 20032)	This Module provides a list of top firewall policies violators
Most Active Hosts for Palo Alto Networks Firewall (10033 / 20033)	This Module provides a list of most active hosts by the number of initiated connections
Bandwidth Consumption per Application for Palo Alto Networks Firewall (10034 / 20034)	This Module provides a list of most active applications by traffic
Bandwidth Consumption per Application and Users for Palo Alto Networks Firewall (10035 / 20035)	This Module provides a list of most active applications and users by traffic
VMware (vmware)	
Top Host VM:Host Pairs (10164 / 20164)	This Module reports top network conversations in VM environment
Top VM:Host Traffic Monitor (10167 / 20167)	This Module identifies VMs with the most traffic
Utilities (service_rules)	
Sampling Monitor (10002 / 20002)	This Module reports NetFlow sampling information
SNMP Information Monitor (10003 / 20003)	This Module reports SNMP information

Modules Specifications

Network Traffic and Devices Monitoring

All Modules report information in syslog key=value pairs format, as shown below.



Top Traffic Monitor (10067 / 20067)

Description

This Module identifies hosts with the most traffic. It consolidates NetFlow records over a period of time (Data Collection Interval) which all have the same combination of the following fields:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol
- Input interface
- Output interface

This information is provided per NetFlow exporter.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 5 sec, max = 600 sec, default = 30 sec
N – number of reported hosts	The number of top hosts reported per NetFlow exporter	min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)

Input

NetFlow v5, v9, IPFIX, Cisco ASA NSEL, and Palo Alto Networks NetFlow v9.

Required NetFlow fields

Information Element (IE)	IE id	IE size, B	Description
IPv4			
sourceIPv4Address	8	4	The IPv4 source address in the IP packet header
destinationIPv4Address	12	4	The IPv4 destination address in the IP packet header
IPv6			
sourceIPv6Address	27	16	The IPv6 source address in the IP packet header
destinationIPv6Address	28	16	The IPv6 destination address in the IP packet header

Syslog message fields

Key	Description	Comments
	NetFlow Optimizer timestamp	Format: Mmm dd hh:mm:ss
	NetFlow Optimizer server IP address	Format: IPv4_address
	NetFlow Optimizer server NetFlow source ID	Configurable.
nfc_id	Message type identifier	“nfc_id=20067”
exp_ip	NetFlow exporter IP address	<IPv4 address>
input_snmp	NetFlow exporter ingress interface SNMP index	<number>
output_snmp	NetFlow exporter egress interface SNMP index	<number>
[protocol] [1]	Transport Protocol (TCP = 6, UDP = 17)	<number>

[1] Protocol field is optional. It is reported only if there is a corresponding field in NetFlow.

Key	Description	Comments
src_ip	Source host IPv4 address	<IPv4_address>
src_ip6	Source host IPv6 address	<IPv6_address>
[src_host][2] [3]	Source host name	<string>, included when FQDN is on
src_port	Source port number	<number>
dest_ip	Destination host IPv4 address	<IPv4_address>
dest_ip6	Destination host IPv6 address	<IPv6_address>
[dest_host]2	Destination host name	<string>, included when FQDN is on
dest_port	Destination port number	<number>
tcp_flag	Cumulative OR of TCP flags	<string>
packets_in	Packets in the flow received by the input interface	<number>
bytes_in	Total number of Layer 3 bytes in the packets of the flow received by the input interface	<number>
src_tos	Inbound IP type of service	<number>
dest_tos	Outbound IP type of service	<number>
src_asn	Source AS	<number>
dest_asn	Destination AS	<number>
flow_count	Number of Flows	<number>

[2] Host name field is optional and included only if FQDN Service is enabled

[3] Optional message fields are enclosed in square brackets

Key	Description	Comments
percent_of_total	Percent of Total (bytes)	<decimal>, e.g. 25.444% is 25.444
[flow_smpl_id]	Flow Sampler ID	<number>
t_int	Observation time interval, msec	<number>

Top Pairs Monitor (10064 / 20064)

Description

This Module reports top Host Pairs network conversations. In contract to Module 10067 which reports consolidated unidirectional flows, this Module stitches client-server request-response flows, reporting bytes and packets server-to-client and client-to-server in separate fields.

Server destination port: Source port of client hosts is not reported, and ignored while consolidating client-server communications. Destination port of server hosts is reported. The Module determines which host is a client and which is a server as follows: a server sends more traffic (bytes) than a client. This logic can be overridden by specifying the list in “List of known server destination port numbers” parameter.

Deduplication: optionally the module can report host pairs only from authoritative router/switch. Authoritative network device is determined as follows. The Module sums up bytes, packets, and connections between two hosts over data collection interval (parameter, default = 30 sec), reported by each flow exporter. An exporter with most connections for each host pair is considered authoritative, and host pair conversations reported by all other exporters are discarded.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 5 sec, max = 600 sec, default = 30 sec
N – number of reported host pairs	The number of top host pairs reported per NetFlow exporter	min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)
List of known server destination port numbers	List of server destination ports to be used to determine which host is a client and which is a server. If the list is empty, the server is the one sending more traffic than receiving	e.g. 53, 80, 443

Parameter Name	Description	Comments
Enable(1) or disable (0) reporting by server port	If set to 1, enable traffic reporting by destination port. If set to 0, dest_port field will be omitted	default = 1
Enable(1) or disable (0) reporting by authoritative exporters only	If set to 1, the Module reports host pairs only from authoritative exporters	default = 0

Input

NetFlow v5, v9, IPFIX, Cisco ASA NSEL, and Palo Alto Networks NetFlow v9.

Required NetFlow fields

Information Element (IE)	IE id	IE size, B	Description
IPv4			
sourceIPv4Address	8	4	The IPv4 source address in the IP packet header
destinationIPv4Address	12	4	The IPv4 destination address in the IP packet header
IPv6			
sourceIPv6Address	27	16	The IPv6 source address in the IP packet header
destinationIPv6Address	28	16	The IPv6 destination address in the IP packet header

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20064”

Key	Field Description	Comments
exp_ip	NetFlow exporter IPv4 address	<IPv4_address>
[protocol] [4]	Transport Protocol (TCP = 6, UDP = 17)	<number>
dest_ip	Server IP address	<IPv4_address>
dest_ip6	Server IPv6 address	<IPv6_address>
[dest_host][5]	Server host name	<string>, included when FQDN is on
[dest_port][6]	Server port number	<number>
src_ip	Client IP address	<IPv4_address>
src_ip6	Client IPv6 address	<IPv6_address>
[src_host]5	Client host name	<string>, included when FQDN is on
packets_in	Packets from client to server	<number>
bytes_in	Layer 3 bytes from client to server	<number>
packets_out	Packets from server to client	<number>
bytes_out	Layer 3 bytes from server to client	<number>
bytes	Layer 3 bytes in both directions	<number>
flow_count	Number of flows	<number>
percent_of_total	Percent of Total (bytes) (Client + Server)	<decimal>, e.g. 25.444% is 25.444

[4] Protocol field is optional. It is reported only if there is a corresponding field in NetFlow.

[5] Host name field is optional and included only if FQDN Service is enabled

[6] Server destination port is optional

Key	Field Description	Comments
[flow_smpl_id]	Flow Sampler ID	<number>
t_int	Observation time interval, msec	<number>

Top Connections Monitor (10063 / 20063)

Description

This Module identifies hosts with the most connections. It consolidates NetFlow records over a period of time (Module execution interval) which all have the same combination of the following fields:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol
- Input interface
- Output interface

This information is provided per NetFlow exporter.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 5 sec, max = 600 sec, default = 30 sec
N – number of reported hosts	The number of top hosts reported per NetFlow exporter	min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)

Input

NetFlow v5, v9, IPFIX, Cisco ASA NSEL, and Palo Alto Networks NetFlow v9.

Required NetFlow fields

Information Element (IE)	IE id	IE size, B	Description
IPv4			
sourceIPv4Address	8	4	The IPv4 source address in the IP packet header

Information Element (IE)	IE id	IE size, B	Description
destinationIPv4Address	12	4	The IPv4 destination address in the IP packet header
IPv6			
sourceIPv6Address	27	16	The IPv6 source address in the IP packet header
destinationIPv6Address	28	16	The IPv6 destination address in the IP packet header

Syslog message fields

Key	Field Description	Comments
	NetFlow Optimizer timestamp	Format: Mmm dd hh:mm:ss
	NetFlow Optimizer server IP address	Format: IPv4_address
	NetFlow Optimizer server NetFlow source ID	Configurable.
nfc_id	Message type identifier	“nfc_id=20063”
exp_ip	NetFlow exporter IP address	<IPv4 address>
input_snmp	NetFlow exporter ingress interface SNMP index	<number>
output_snmp	NetFlow exporter egress interface SNMP index	<number>
[protocol][7]	Transport Protocol (TCP = 6, UDP = 17)	<number>
src_ip	Source host IPv4 address	<IPv4_address>
src_ip6	Source host IPv6 address	<IPv6_address>

[7] Protocol field is optional. It is reported only if there is a corresponding field in NetFlow.

Key	Field Description	Comments
[src_host][8]	Source host name	<string>, included when FQDN is on
src_port	Source port number	<number>
dest_ip	Destination host IPv4 address	<IPv4_address>
dest_ip6	Destination host IPv6 address	<IPv6_address>
[dest_host]8	Destination host name	<string>, included when FQDN is on
dest_port	Destination port number	<number>
tcp_flag	Cumulative OR of TCP flags	
packets_in	Packets in the flow received by the input interface	<number>
bytes_in	Total number of Layer 3 bytes in the packets of the flow received by the input interface	<number>
src_tos	Inbound IP type of service	<number>
dest_tos	Outbound IP type of service	<number>
src_asn	Source AS	<number>
dest_asn	Destination AS	<number>
flow_count	Number of Flows	<number>
percent_of_total	Percent of Total (flow_count)	<decimal>, e.g. 25.444% is 25.444
[flow_smpl_id]	Flow Sampler ID	<number>
t_int	Observation time interval, msec	<number>

[8] Host name field is optional and included only if FQDN Service is enabled

Top Packets Monitor (10068 / 20068)

Description

This Module identifies hosts with the most packets. It consolidates NetFlow records over a period of time (Data Collection Interval) which all have the same combination of the following fields:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol
- Input interface
- Output interface

This information is provided per NetFlow exporter.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 5 sec, max = 600 sec, default = 30 sec
N – number of reported hosts	The number of top hosts reported per NetFlow exporter	min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)

Input

NetFlow v5, v9, IPFIX, Cisco ASA NSEL, and Palo Alto Networks NetFlow v9.

Required NetFlow fields

Information Element (IE)	IE id	IE size, B	Description
IPv4			
sourceIPv4Address	8	4	The IPv4 source address in the IP packet header
destinationIPv4Address	12	4	The IPv4 destination address in the IP packet header
IPv6			
sourceIPv6Address	27	16	The IPv6 source address in the IP packet header

Information Element (IE)	IE id	IE size, B	Description
destinationIPv6Address	28	16	The IPv6 destination address in the IP packet header

Syslog message fields

Key	Field Description	Comments
	NetFlow Optimizer timestamp	Format: Mmm dd hh:mm:ss
	NetFlow Optimizer server IP address	Format: IPv4_address
	NetFlow Optimizer server NetFlow source ID	Configurable.
nfc_id	Message type identifier	“nfc_id=20068”
exp_ip	NetFlow exporter IP address	<IPv4 address>
input_snmp	NetFlow exporter ingress interface SNMP index	<number>
output_snmp	NetFlow exporter egress interface SNMP index	<number>
[protocol] [9]	Transport Protocol (TCP = 6, UDP = 17)	<number>
src_ip	Source host IPv4 address	<IPv4_address>
src_ip6	Source host IPv6 address	<IPv6_address>
[src_host][10]	Source host name	<string>, included when FQDN is on
src_port	Source port number	<number>
dest_ip	Destination host IPv4 address	<IPv4_address>

[9] Protocol field is optional. It is reported only if there is a corresponding field in NetFlow.

[10] Host name field is optional and included only if FQDN Service is enabled

Key	Field Description	Comments
dest_ip6	Destination host IPv6 address	<IPv6_address>
[dest_host]10	Destination host name	<string>, included when FQDN is on
dest_port	Destination port number	<number>
tcp_flag	Cumulative OR of TCP flags	
packets_in	Packets in the flow received by the input interface	<number>
bytes_in	Total number of Layer 3 bytes in the packets of the flow received by the input interface	<number>
src_tos	Inbound IP type of service	<number>
dest_tos	Outbound IP type of service	<number>
src_asn	Source AS	<number>
dest_asn	Destination AS	<number>
flow_count	Number of Flows	<number>
percent_of_total	Percent of Total (packets)	<decimal>, e.g. 25.444% is 25.444
[flow_smpl_id]	Flow Sampler ID	<number>
t_int	Observation time interval, msec	<number>

Network Subnets Monitor (10011 / 20011)

Description

This Module reports top bandwidth consumers for each monitored subnet. This information is provided per NetFlow exporter and monitored subnet.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 10 sec, max = 600 sec, default = 30 sec
Monitored subnet IPv4 address and subnet mask	List of the watched subnets' IPv4 addresses and masks (CIDR notation)	e.g. 67.202.0.0 / 18; 72.44.32.0 / 24
Monitored subnet IPv6 address and subnet mask	List of the watched subnets' IPv6 addresses and masks (CIDR notation)	e.g. 2620:0:2d0:200::7/24
N – number of reported hosts	Top N (number of reported hosts per subnet)	min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)

Input

NetFlow v5, v9, IPFIX, and Cisco ASA NSEL.

Required NetFlow fields

Information Element (IE)	IE id	IE size, B	Description
sourceIPv4Address or sourceIPv6Address	8 or 27	4 or 16	The IPv4 or IPv6 source address in the IP packet header
destinationIPv4Address or destinationIPv6Address	12 or 28	4 or 16	The IPv4 or IPv6 destination address in the IP packet header
protocolIdentifier	4	1	The value of the protocol number in the IP packet header. The protocol number identifies the IP packet payload type. Protocol numbers are defined in the IANA Protocol Numbers registry.

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address

Key	Field Description	Comments
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20011”
exp_ip	NetFlow exporter IP address	<IPv4 address>
subnet	Subnet IPv4	<IPv4_address>
subnet	Subnet IPv6	<IPv6_address>
mask	Mask	<number>
src_ip	Source host IPv4 address	<IPv4_address>
src_ip6	Source host IPv6 address	<IPv6_address>
protocol	Transport Protocol (TCP = 6, UDP = 17)	<number>
bytes_out	Bytes Out (Traffic)	<number>
bytes_in	Bytes In (Traffic)	<number>
packets_out	Packets Out count	<number>
packets_in	Packets In count	<number>
flow_count	Number of flows	< number>
percent_of_total	Percent of Total Traffic of the Source Host within Subnet	<decimal>, e.g. 25.444% is 25.444
t_int	Observation time interval, msec	<number>

TCP Health Monitor (10060 / 20060)

Description

This Module reports TCP Health by detecting top hosts with the most TCP Resets.

Top hosts are defined by percent of TCP resets to the total number of Resets for definitive NetFlow exporter or by percent of TCP resets to the total number of host's connections.

This information is provided by a definitive NetFlow exporter.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 5 sec, max = 600 sec, default = 30 sec
N - reporting threshold in percent of total resets number	% of Total Resets	min = 0 %, max = 100 %, default = 10 %
N - reporting threshold in percent of resets to the number of host connections	% of Resets to local host connections	min = 0 %, max = 100 %, default = 50 %

Input

NetFlow v5, v9, IPFIX, and Palo Alto Networks NetFlow v9. sFlow and sampled NetFlow are specifically excluded from processing by this Module. Cisco ASA NSEL is not supported by this Module as it does not have TCP flags.

Syslog message fields - Hosts

Key	Field Description	Comments
	NetFlow Optimizer timestamp	Format: Mmm dd hh:mm:ss
	NetFlow Optimizer server IP address	Format: IPv4_address
	NetFlow Optimizer server NetFlow source ID	Configurable.
nfc_id	Message type identifier	"nfc_id=20060"
src_ip	Source host IPv4 address	<IPv4_address>
src_ip6	Source host IPv6 address	<IPv6_address>

Key	Field Description	Comments
[src_host][11]	Source host name	<string>, included when FQDN is on
reset_count	Count of Resets	<number>
total_share	Percent of the total number of resets sent by source host	<number>
local_share	Percent of the resets to the total number of the source host connections	<number>
t_int	Observation time interval, msec	<number>

CBQoS Monitor (10065 / 20065)

Description

This Module reports traffic for all DSCP bits combinations (QoS). This information is provided per NetFlow exporter.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 5 sec, max = 600 sec, default = 30 sec

Input

NetFlow v5, v9, IPFIX, Palo Alto Networks NetFlow v9.

Required NetFlow fields

Information Element (IE)	IE id	IE size, B	Description
octetDeltaCount	1	4 or 8	The number of octets since the previous report (if any) in incoming packets for this Flow at the Observation Point. The number of octets includes IP header(s) and IP payload.

[11] Host name field is optional and included only if FQDN Service is enabled

Information Element (IE)	IE id	IE size, B	Description
packetDeltaCount	2	4 or 8	The number of incoming packets since the previous report (if any) for this Flow at the Observation Point.

Syslog message fields

Key	Field Description	Comments
	NetFlow Optimizer timestamp	Format: Mmm dd hh:mm:ss
	NetFlow Optimizer server IP address	Format: IPv4_address
	NetFlow Optimizer server NetFlow source ID	Configurable.
nfc_id	Message type identifier	“nfc_id=20065”
exp_ip	NetFlow exporter IP address	<IPv4 address>
[protocol] [12]	Transport Protocol (TCP = 6, UDP = 17)	<number>
src_tos	Inbound IP type of service	<number>
dest_tos	Outbound IP type of service	<number>
packets_in	Packets received in the QoS class flows	<number>
bytes_in	Total number of Layer 3 bytes received in the QoS class flows	<number>
flow_count	Number of flows received in the QoS class flows	<number>
percent_of_total	Percent of Total (bytes) of all bytes received by the exporter	<decimal>, e.g. 25.444% is 25.444
[flow_smpl_id]	Flow Sampler ID	<number>

[12] Protocol field is optional. It is reported only if there is a corresponding field in NetFlow.

Key	Field Description	Comments
t_int	Observation time interval, msec	<number>

Autonomous Systems Monitor (10066 / 20066)

Description

This Module reports traffic by all Autonomous Systems (AS). This information is provided per NetFlow exporter.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 5 sec, max = 600 sec, default = 30 sec
N – number of reported hosts	The number of top ASN pairs reported per NetFlow exporter	min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)

Input

NetFlow v5, v9, IPFIX.

Required NetFlow fields

Information Element (IE)	IE id	IE size, B	Description
octetDeltaCount	1	4 or 8	The number of octets since the previous report (if any) in incoming packets for this Flow at the Observation Point. The number of octets includes IP header(s) and IP payload.
packetDeltaCount	2	4 or 8	The number of incoming packets since the previous report (if any) for this Flow at the Observation Point.

Syslog message fields

Key	Field Description	Comments
	NetFlow Optimizer timestamp	Format: Mmm dd hh:mm:ss

Key	Field Description	Comments
	NetFlow Optimizer server IP address	Format: IPv4_address
	NetFlow Optimizer server NetFlow source ID	Configurable.
nfc_id	Message type identifier	“nfc_id=20066”
exp_ip	NetFlow exporter IP address	<IPv4 address>
src_asn	Source AS	<number>
dest_asn	Destination AS	<number>
bytes	Total number of Layer 3 bytes in the packets of the flow received (IPv4)	<number>
bytes6	Total number of Layer 3 bytes in the packets of the flow received (IPv6)	<number>
packets	Packets in the flow received (IPv4)	<number>
packets6	Packets in the flow received (IPv6)	<number>
flow_count	Number of Flows	<number>
percent_of_total	Percent of Total (bytes)	<decimal>
[flow_smpl_id]	Flow Sampler ID	<number>
t_int	Observation time interval, msec	<number>

Enhanced Traffic Monitor

This package contains an enhanced version of Top Traffic Monitor Module 10067. It reports Reputation and Geo locations of source and destination hosts.

Top Traffic Monitor Geo Country (10967 / 20967)

Description

This Module identifies hosts with the most traffic. It consolidates NetFlow records over a period of time (Data Collection Interval) which all have the same combination of the following fields:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol
- Input interface
- Output interface

This information is provided per NetFlow exporter.

Reputation field is provided as follows:

Watch list parameter “Known malicious hosts list” must be specified. The Module checks if destination IP is in this watch list; if yes, the reputation value is provided, and the rep_ip field is populated with destination IP address. If not, the source IP is checked, the reputation value is populated, and rep_ip field is populated with the source IP.

Country codes for both source IP and destination IP are provided based on “IPv4 address block and country code” watch list.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 5 sec, max = 600 sec, default = 30 sec
N – number of reported hosts	The number of top hosts reported per NetFlow exporter	min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)
Known malicious hosts list	List of known malicious peers	AlienVault Reputation database (OTX)
IPv4 address block and country code	Mapping of country codes to IP addresses blocks	This list is updated by External Data Feeder for NFO, which uses the MaxMind GeoLite Country database as a source

Input

NetFlow v5, v9, IPFIX, Cisco ASA NSEL, and Palo Alto Networks NetFlow v9.

Required NetFlow fields

Information Element (IE)	IE id	IE size, B	Description
IPv4			

Information Element (IE)	IE id	IE size, B	Description
sourceIPv4Address	8	4	The IPv4 source address in the IP packet header
destinationIPv4Address	12	4	The IPv4 destination address in the IP packet header
IPv6			
sourceIPv6Address	27	16	The IPv6 source address in the IP packet header
destinationIPv6Address	28	16	The IPv6 destination address in the IP packet header

Syslog message fields

Key	Field Description	Comments
	NetFlow Optimizer timestamp	Format: Mmm dd hh:mm:ss
	NetFlow Optimizer server IP address	Format: IPv4_address
	NetFlow Optimizer server NetFlow source ID	Configurable.
nfc_id	Message type identifier	“nfc_id=20967”
exp_ip	NetFlow exporter IP address	<IPv4 address>
input_snmp	NetFlow exporter ingress interface SNMP index	<number>
output_snmp	NetFlow exporter egress interface SNMP index	<number>
[protocol] [13]	Transport Protocol (TCP = 6, UDP = 17)	<number>
src_ip	Source host IPv4 address	<IPv4_address>

[13] Protocol field is optional. It is reported only if there is a corresponding field in NetFlow.

Key	Field Description	Comments
src_ip6	Source host IPv6 address	<IPv6_address>
[src_host][14]	Source host name	<string>, included when FQDN is on
src_port	Source port number	<number>
dest_ip	Destination host IPv4 address	<IPv4_address>
dest_ip6	Destination host IPv6 address	<IPv6_address>
[dest_host][14]	Destination host name	<string>, included when FQDN is on
dest_port	Destination port number	<number>
tcp_flag	Cumulative OR of TCP flags	
packets_in	Packets in the flow received by the input interface	<number>
bytes_in	Total number of Layer 3 bytes in the packets of the flow received by the input interface	<number>
src_tos	Inbound IP type of service	<number>
dest_tos	Outbound IP type of service	<number>
src_asn	Source AS	<number>
dest_asn	Destination AS	<number>
flow_count	Number of Flows	<number>
percent_of_total	Percent of Total (bytes)	<decimal>, e.g. 25.444% is 25.444
[flow_smpl_id]	Flow Sampler ID	<number>

[14] Host name field is optional and included only if FQDN Service is enabled

Key	Field Description	Comments
[reputation][15]	Reputation:	<string>: "Unexpected Host Reputation Classifier", "Scanning Host", "Malware Domain" "Malware IP", "Spamming" "C&C", "Malicious Host", "Malware distribution", "APT"
[rep_ip][15]	Reputation IP	Actual IP address (source or destination) found in Reputation database
[src_cc][16]	Source IP country code	ISO-3166-1 Alpha 2 country code (a two-character country designation, e.g. US)
[dest_cc][16]	Destination IP country code	ISO-3166-1 Alpha 2 country code (a two-character country designation, e.g. US)
t_int	Observation time interval, msec	<number>

Enhanced Traffic Monitor 2

This package contains Top Traffic Monitor Module with Reputation, Geo locations of source and destination hosts resolved at City level, and TCP flow duration.

 This package is only available on request. Please contact sales@netflowlogic.com.

 To use this Module you need to increase maximum Java heap size:

1. Open file /opt/flowintegrator/tomcat/bin/setenv.sh
2. Change -Xmx3g parameter to -Xmx6g
3. Restart NFO Tomcat: /etc/init.d/tomcat_nfo restart

Top Traffic Monitor Geo City (10867 / 20867)

Description

This Module identifies and reports hosts with the most traffic (optionally all hosts). It consolidates NetFlow records over a period of time (Data Collection Interval) which all have the same combination of the following fields:

- Source IP address
- Destination IP address
- Source port number

[15] This field is omitted if no match of source or destination IP is found in Reputation database

[16] This field is omitted if no MaxMind database is setup

- Destination port number
- Layer 3 protocol

For bidirectional flows the Module stitches request-reply flows inverting source and destination for flows in the opposite direction. It reports consolidated flows separating bytes/packets sent and bytes/packets received.

This information is provided per NetFlow exporter.

Reputation

Watch list parameter “Known malicious hosts list” must be specified for the Module to report reputation of communicating peers. The Module checks if destination IP is in this watch list; if yes, the reputation value is provided, and the rep_ip field is populated with destination IP address. If not, the source IP is checked, the reputation value is populated, and rep_ip field is populated with the source IP.

This list is obtained from Alienvault IP Reputation Database http://reputation.alienvault.com/reputation.snort. It is updated once a day.

If you have your private list in snort format, and/or you want NetFlow Optimizer to get the list from disk (e.g. /opt directory), change the URL from http://reputation.alienvault.com/reputation.snort to file:///opt/reputation.snort.

Geo IP

Country codes, region, city, and other geo information for both source IP and destination IP are provided based on “IPv4 address block and city location” watch list.

This list is obtained from http://geolite.maxmind.com/download/geoip/database/GeoLite2-City-CSV.zip

The free version of MaxMind GeoLite2 City database is updated once a month.

TCP session duration

TCP session duration is calculated as follows:

TCP session duration - `tcp_duration` - is reported in syslogs when the session is terminated. It is calculated as the time between source SYN[17] and first FIN/RST.

"Update" flows reported by network devices triggered by inactive/active timeouts will not have tcp_duration field in corresponding syslogs as the session is not terminated at the time of reporting. These flows will be consolidated for the same session if more than one flow is sent to NFO within the same data collection interval (DCI).

Flows that belong to the same session (requests-replies) will be reported in a single syslog within DCI, with bytes and packets reported separately for each direction (bytes_in and bytes_out, packets_in and packets_out).

[17] The Module takes the first NetFlow record it receives as TCP session start in case SYN flow is lost.

Network Bandwidth Consumption Monitor by Application for Blue Coat PacketShaper

This package contains a Module for Blue Coat PacketShaper-2 Flow Data.

Network Bandwidth Consumption Monitor (10964 / 20964)

Description

This Module reports network bandwidth consumption by pairs of network users per application kind per PacketShaper instance. The Module consolidates per application kind information based on network conversations, where a network conversation is a series of network traffic exchanges between two network hosts executing that application.

Network conversation attributes are user configurable and may include source and destination IP addresses and source and destination transport layer ports. Optionally, the user may provide a list of known ports by which the server side of a network conversation may be determined. In a case when a list of ports is not provided or when the ports are not present in the provided list the Module makes a best effort determination of the server side by assuming that a party which sent most traffic is the server.

The Module classifies applications by the PacketShaper ClassId field found in the Packeteer-2 messages. The Module determines a corresponding application name by dereferencing a list of application names distinguished by the respective ClassId values.

The user has the ability to control Module's output by specifying treatment of the input Packeteer-2 records which ClassId is not present in the PacketShaper ClassId - Application Name mapping table. Unclassified records may either be discarded or processed normally and supplied a default application name such as "unknown".

Input

Flow records in the Blue Coat PacketShaper Packeteer-2 format.

Parameters

Parameter Name	Description	Comments
Module reporting interval	Time-based Rule invocation interval, sec	min = 5 sec, max = 600 sec, default = 30 sec
N - The number of unique host pairs per application kind to report	A number of unique communicating host pairs reported per application per PacketShaper instance. The host pairs are reported in the descending order by traffic volume.	min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)
List of known server destination port numbers	A list of server destination ports to be used to determine which host is a client and which is a server. If the list is empty, the server is the one sending more traffic than receiving	e.g. 53, 80, 443

Parameter Name	Description	Comments
Enable(1) or disable (0) reporting by the server port	If set to 1, enable traffic reporting by destination port. If set to 0, dest_port field in the output syslog message is omitted. Turning this parameter on or off does not affect the number of unique host pairs output by the module.	default = 0
Enable(1) or disable (0) reporting by the client port	If set to 1, enable traffic reporting by source port. If set to 0, src_port field the output syslog message is omitted. Turning this parameter on or off does not affect the number of unique host pairs output by the module.	default = 0
List of PacketShaper ClassId values and corresponding Application names	A list of PacketShaper ClassId and Application name	e.g. 2525, /Outbound/AOL-AIM-ICQ
Report information for a user-defined subset of applications (1) or for all applications (0)	If set to 1, drop Packeteer-2 records with unknown ClassId. Report all network conversations otherwise.	default = 0

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20964”
exp_ip	PacketShaper instance IPv4 address	<IPv4_address>
class_id	PacketShaper application ClassId	<number>
application	PacketShaper application name	<string>
dest_ip	Server IPv4 address	<IPv4_address>

Key	Field Description	Comments
[dest_host]	Server host name	<string>, included when NFO FQDN service is enabled
[dest_port]	Server transport layer port number	<number>
src_ip	Client IPv4 address	<IPv4_address>
[src_host]	Client host name	<string>, included when NFO FQDN service is enabled
[src_port]	Client transport layer port number	<number>
packets_in	Packets sent from the client to the server	<number>
bytes_in	Layer 3 bytes from the client to the server	<number>
packets_out	Packets from the server to the client	<number>
bytes_out	Layer 3 bytes from the server to the client	<number>
flow_count	Number of observed flows	<number>
percent_of_total	Percent of total traffic produced by this host pair per application during current data collection interval	<floating point decimal>
t_int	Observation time interval, msec	<number>

Security

Hosts Geographical Location Monitor (10040 / 20040)

Description

This Module identifies hosts with most traffic, and reports them with their geographical locations.

This Module uses an IPv4 address blocks to geographical locations mapping database provided by MaxMind – GeoLite Country - to find geographical locations of the connecting hosts. The GeoIP database contains approximately

100K entries. The GeoLite Country database update frequency is ones a month. A commercial version of the MaxMind GeoIP database is updated every other day.

Use Updater feature of NetFlow Optimizer for initial load and periodic updates of this list.

Besides a GeoIP database the Module has two other optional watch lists:

- List of monitored localities: Alpha-2 codes per ISO (https://www.iso.org/obp/ui/)
- List of watched local subnets: CIDR notation

The Module is using local subnets list to resolve inbound and outbound traffic, and reports it separately (field direction=ingress or direction=egress in syslog).

In **inbound** traffic report the source IPv4 address is an IPv4 address of a host with most traffic in a geographic locality, and the destination IPv4 address is an IPv4 address of an internal host.

In **outbound** traffic report the source IPv4 address is an IPv4 address of an internal host, and the destination IPv4 address is an IPv4 address of a host with most traffic in an outbound geographic locality.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 10 sec, max = 600 sec, default = 30 sec
List of monitored localities	List of two letter country codes	e.g. AQ, US, GB
List of watched local subnets and hosts	List of the watched subnets' IPv4 addresses and masks (CIDR notation)	e.g. 67.202.0.0 / 18; 72.44.32.0 / 24 default = 0.0.0.0 / 0
IPv4 address block and country code	Mapping of country codes to IP addresses blocks	This list is updated by External Data Feeder for NFO, which uses the MaxMind GeoLite Country database as a source

Input

NetFlow v5, v9, IPFIX, Cisco ASA NSEL, and Palo Alto Networks NetFlow v9

Required NetFlow fields

Information Element (IE)	IE id	IE size, B	Description
sourceIPv4Address	8	4	The IPv4 source address in the IP packet header

Information Element (IE)	IE id	IE size, B	Description
destinationIPv4Address	12	4	The IPv4 destination address in the IP packet header

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20040”
exp_ip	NetFlow exporter IPv4 address	<IPv4_address>
src_ip	Source host IPV4 address	<IPv4_address>
dest_ip	Destination host IPv4 address	<IPv4_address>
direction	Traffic direction	<string>: egress | ingress
cc	Country code	ISO-3166-1 Alpha 2 country code (a two-character country designation, e.g. US)
flow_count	Number of flows	< number>
bytes	Bytes total (Traffic)	<number>
t_int	Observation time interval, msec	<number>

Botnet Command and Control Traffic Monitor (10050 / 20050)

Description

This Module monitors traffic originated from known Command and Control hosts (C&C) or directed to these hosts. The list of IP addresses of C&C hosts is obtained from the list published by Emerging Threats (http://www.emergingthreats.net/) company:

- List of known C&C servers: https://rules.emergingthreats.net/blockrules/emerging-botcc.rules

The Module reports all communications of internal hosts with C&C list, and provides consolidated information about these communications over a time interval. The observation interval (T, sec) is configurable.

Use Updater feature of NetFlow Optimizer for initial load and periodic updates of this threat list.[18]

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 10 sec, max = 300 sec, default = 30 sec
Known C&C hosts (ipv4_dst_addr) list	List of C&C IPv4 addresses	'Shadowserver C&C list' from Emerging Threats. This list is updated by External Data Feeder for NFO

Input

NetFlow v5, v9, IPFIX, Cisco ASA NSEL, and Palo Alto Networks NetFlow v9.

Required NetFlow fields

Information Element (IE)	IE id	IE size, B	Description
sourceIPv4Address	8	4	The IPv4 source address in the IP packet header
destinationIPv4Address	12	4	The IPv4 destination address in the IP packet header
sourceTransportPort	7	2	The source port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the source port number given in the respective header.

[18] Please contact support@netflowlogic.com if you want to use your own feeds.

Information Element (IE)	IE id	IE size, B	Description
destinationTransportPort	11	2	The destination port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the destination port number given in the respective header.
octetDeltaCount	1	4 or 8	The number of octets since the previous report (if any) in incoming packets for this Flow at the Observation Point. The number of octets includes IP header(s) and IP payload.

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20050”
exp_ip	NetFlow exporter IPv4 address	<IPv4_address>
src_ip	Source host IPV4 address	<IPv4_address>
src_port	Source port	<number>
dest_ip	Destination host IPv4 address	<IPv4_address>
dest_port	Destination port	<number>
flow_count	Number of flows	< number>
bytes	Bytes total (Traffic)	<number>
min_bytes	Minimum bytes count of flows	<number>

Key	Field Description	Comments
max_bytes	Maximum bytes count of flows	<number>
direction	Flow direction	<string>: “ingress” or “egress”
t_int	Observation time interval, msec	<number>

Host Reputation Monitor (10052 / 20052)

Description

This Module uses a host reputation database from Alienvault (www.alienvault.com) to report communications with malicious peers. The reputation table provides a suspicious host IPv4 address and one or more host classifications (e.g. Scanning Host, Malicious Host, Malware Domain). The host reputation database size is approximately 260K entries.

The Module reports all communications of internal hosts with the hosts included in the reputation database and provides consolidated information about these communications over a time interval. The observation interval (T, sec) is configurable.

Use Updater feature of NetFlow Optimizer for initial load and periodic updates of this threat list from https://reputation.alienvault.com/reputation.snort.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 10 sec, max = 300 sec, default = 30 sec
Known malicious hosts list	List of known malicious peers	This list is loaded and updated by External Data Feeder for NFO

Input

NetFlow v5, v9, IPFIX, Cisco ASA NSEL, and Palo Alto Networks NetFlow v9.

Required NetFlow fields

Information Element (IE)	IE id	IE size, B	Description
sourceIPv4Address	8	4	The IPv4 source address in the IP packet header

Information Element (IE)	IE id	IE size, B	Description
destinationIPv4Address	12	4	The IPv4 destination address in the IP packet header
sourceTransportPort	7	2	The source port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the source port number given in the respective header.
destinationTransportPort	11	2	The destination port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the destination port number given in the respective header.
octetDeltaCount	1	4 or 8	The number of octets since the previous report (if any) in incoming packets for this Flow at the Observation Point. The number of octets includes IP header(s) and IP payload.

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20052”
exp_ip	NetFlow exporter IPv4 address	<IPv4_address>
src_ip	Source host IPV4 address	<IPv4_address>
src_port	Source port	<number>
dest_ip	Destination host IPv4 address	<IPv4_address>
dest_port	Destination port	<number>
flow_count	Number of flows	< number>

Key	Field Description	Comments
bytes	Bytes total (Traffic)	<number>
min_bytes	Minimum bytes count of flows	<number>
max_bytes	Maximum bytes count of flows	<number>
direction	Flow direction	<string>: “ingress” or “egress”
reputation	Reputation	<string>: "Unexpected Host Reputation Classifier" "Scanning Host" "Malware Domain" "Malware IP" "Spamming" "C&C" "Malicious Host" "Malware distribution" "APT"
t_int	Observation time interval, msec	<number>

Threat Feeds Monitor (10053 / 20053)

Description

This Module monitors traffic originated from known threat feeds:[19]

- List of attacking IP address ranges: http://feeds.dshield.org/block.txt
- List of suspicious domains: http://www.dshield.org/feeds/suspiciousdomains_High.txt

The Module reports all communications of internal hosts with known suspicious domains (IP addresses are resolved from the list of domain names using your DNS) and IP addresses blocks, and provides consolidated information about these communications over a time interval. The observation interval (T, sec) is configurable.

Use Updater feature of NetFlow Optimizer for initial load and periodic updates of watch list parameters.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 10 sec, max = 300 sec, default = 30 sec

[19] Please contact support@netflowlogic.com if you want to use your own feeds.

Parameter Name	Description	Comments
Known Threat Feeds hosts (ipv4_dst_addr) list	List of known Threat Feeds addresses resolved using DNS	This list is loaded and updated by External Data Feeder for NFO
Known Threat Feeds IPv4 address ranges list	List of known Threat Feeds address ranges	This list is loaded and updated by External Data Feeder for NFO

Input

NetFlow v5, v9, IPFIX, Cisco ASA NSEL, and Palo Alto Networks NetFlow v9.

Required NetFlow fields

Information Element (IE)	IE id	IE size, B	Description
sourceIPv4Address	8	4	The IPv4 source address in the IP packet header
destinationIPv4Address	12	4	The IPv4 destination address in the IP packet header
sourceTransportPort	7	2	The source port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the source port number given in the respective header.
destinationTransportPort	11	2	The destination port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the destination port number given in the respective header.
octetDeltaCount	1	4 or 8	The number of octets since the previous report (if any) in incoming packets for this Flow at the Observation Point. The number of octets includes IP header(s) and IP payload.

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable

Key	Field Description	Comments
nfc_id	Message type identifier	“nfc_id=20053”
exp_ip	NetFlow exporter IPv4 address	<IPv4_address>
src_ip	Source host IPV4 address	<IPv4_address>
src_port	Source port	<number>
dest_ip	Destination host IPv4 address	<IPv4_address>
dest_port	Destination port	<number>
origin	Communication origin	<string> = host | block
flow_count	Number of flows	< number>
bytes	Bytes total (Traffic)	<number>
min_bytes	Minimum bytes count of flows	<number>
max_bytes	Maximum bytes count of flows	<number>
direction	Flow direction	<string>: “ingress” or “egress”
t_int	Observation time interval, msec	<number>

Email

Outbound Mail Spammers Monitor (10025 / 20025)

Description

This Module detects internal hosts infected with spam malware. It monitors egress traffic over TCP protocol and destination ports 25 or 465, excluding known authorized mail servers. This Module reports top email senders and provides consolidated information over a time interval.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 10 sec, max = 3600 sec, default = 600 sec
N - number of reported outbound spammers	Top N (number of reported spammers)	min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)
Known local mail servers (ipv4_src_addr) list	List of IP addresses of known mail servers to be **excluded from reporting**	

Input

NetFlow v5, v9, IPFIX, Cisco ASA NSEL, and Palo Alto Networks NetFlow v9.

Required NetFlow fields

Information Element (IE)	IE id	IE size, B	Description
sourceIPv4Address	8	4	The IPv4 source address in the IP packet header
protocolIdentifier	4	1	The value of the protocol number in the IP packet header. The protocol number identifies the IP packet payload type. Protocol numbers are defined in the IANA Protocol Numbers registry.
destinationTransportPort	11	2	The destination port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the destination port number given in the respective header.
octetDeltaCount	1	4 or 8	The number of octets since the previous report (if any) in incoming packets for this Flow at the Observation Point. The number of octets includes IP header(s) and IP payload.
packetDeltaCount	2	4 or 8	The number of incoming packets since the previous report (if any) for this Flow at the Observation Point.

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20025”
exp_ip	NetFlow exporter IPv4 address	<IPv4_address>
src_ip	Source host IPv4 address	<IPv4_address>
bytes_out	Bytes total (Traffic)	<number>
packets_out	Packets	<number>
num_conn	Number of flows initiated by the source host	<number>
min_bytes	Minimum bytes count of flows	<number>
max_bytes	Maximum bytes count of flows	<number>
t_int	Observation time interval, msec	<number>

Inbound Mail Spammers Monitor (10026 / 20026)

Description

This Module detects external hosts sending excessive email traffic to your organization. It monitors ingress traffic over TCP protocol and destination ports 25 or 465 sent to designated mail servers. The Module reports top email senders and provides consolidated information over a time interval.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 10 sec, max = 3600 sec, default = 600 sec
N - number of reported inbound spammers	Top N (number of reported spammers)	min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)
Known local mail servers (ipv4_dst_addr) list	List of IP addresses of known mail servers **to be monitored**	

Input

NetFlow v5, v9, IPFIX, Cisco ASA NSEL, and Palo Alto Networks NetFlow v9.

Required NetFlow fields

Information Element (IE)	IE id	IE size, B	Description
sourceIPv4Address	8	4	The IPv4 source address in the IP packet header
destinationIPv4Address	12	4	The IPv4 destination address in the IP packet header
protocolIdentifier	4	1	The value of the protocol number in the IP packet header. The protocol number identifies the IP packet payload type. Protocol numbers are defined in the IANA Protocol Numbers registry.
destinationTransportPort	11	2	The destination port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the destination port number given in the respective header.
octetDeltaCount	1	4 or 8	The number of octets since the previous report (if any) in incoming packets for this Flow at the Observation Point. The number of octets includes IP header(s) and IP payload.
packetDeltaCount	2	4 or 8	The number of incoming packets since the previous report (if any) for this Flow at the Observation Point.

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20026”
exp_ip	NetFlow exporter IPv4 address	<IPv4_address>
src_ip	Source host IPv4 address	<IPv4_address>
bytes_out	Bytes total (Traffic)	<number>
packets_out	Packets	<number>
num_conn	Number of flows initiated by the source host	<number>
min_bytes	Minimum bytes count of flows	<number>
max_bytes	Maximum bytes count of flows	<number>
t_int	Observation time interval, msec	<number>

Unauthorized Mail Servers Monitor (10027 / 20027)

Description

This Module detects internal hosts running unauthorized mail servers. It monitors ingress traffic over TCP protocol and destination ports 25 or 465 sent to hosts which are not designated mail servers. The Module reports all detected unauthorized email servers.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 10 sec, max = 3600 sec, default = 600 sec
Known local mail servers (ipv4_dst_addr) list	List of IP addresses of known mail servers to be excluded from reporting	

Input

NetFlow v5, v9, IPFIX, Cisco ASA NSEL, and Palo Alto Networks NetFlow v9.

Required NetFlow fields

Information Element (IE)	IE id	IE size, B	Description
destinationIPv4Address	12	4	The IPv4 destination address in the IP packet header
protocolIdentifier	4	1	The value of the protocol number in the IP packet header. The protocol number identifies the IP packet payload type. Protocol numbers are defined in the IANA Protocol Numbers registry.
destinationTransportPort	11	2	The destination port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the destination port number given in the respective header.
octetDeltaCount	1	4 or 8	The number of octets since the previous report (if any) in incoming packets for this Flow at the Observation Point. The number of octets includes IP header(s) and IP payload.

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20027”
exp_ip	NetFlow exporter IPv4 address	<IPv4_address>
dest_ip	Destination host IPv4 address	<IPv4_address>
bytes_out	Bytes total (Traffic)	<number>
num_conn	Number of flows initiated by the source host	<number>
min_bytes	Minimal bytes number in a flow	<number>
max_bytes	Maximal bytes number in a flow	<number>
t_int	Observation time interval, msec	<number>

Rejected Emails Monitor (10028 / 20028)

Description

This Module detects external hosts sending emails rejected by internal mail servers. It monitors ingress traffic over TCP protocol and destination ports 25 or 465. The Module reports all email senders and provides consolidated information (Source IP and the number of rejected emails) over a time interval.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 10 sec, max = 300 sec, default = 30 sec

Input

Cisco ASA NSEL flow denied template and Palo Alto Networks Ipv4 Traffic Templates IPv4 Standard (Template ID 256) and IPv4 Enterprise (Template ID 257)

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20028”
exp_ip	NetFlow exporter IPv4 address	<IPv4_address>
src_ip	Source host IPv4 address	<IPv4_address>
dest_ip	Destination host IPv4 address	<IPv4_address>
denied_count	Number of rejected emails	< number>
t_int	Observation time interval, msec	< number>

Services Monitor

DNS Monitor (10004 / 20004, 20005)

Description

This Module monitors DNS servers and DNS traffic as follows:

- It calculates an average DNS servers’ response time over a specified time interval and reports it for all observed DNS servers
- It calculates an average DNS servers’ packet size (both in and out). DNS attacks are characterized by suspiciously large messages (packet size over 512 bytes)
- It reports top DNS users

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 30 sec, max = 600 sec, default = 60 sec
How many most active DNS requestors do you want to report?	Top N (number of reported hosts)	min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)

Input

NetFlow v5, v9, and IPFIX. Cisco ASA NSEL is not fully supported by this Module. Please contact support@netflowlogic.com for more information.

Required NetFlow fields

Information Element (IE)	IE id	IE size, B	Description
sourceIPv4Address	8	4	The IPv4 source address in the IP packet header
destinationIPv4Address	12	4	The IPv4 destination address in the IP packet header
protocolIdentifier	4	1	The value of the protocol number in the IP packet header. The protocol number identifies the IP packet payload type. Protocol numbers are defined in the IANA Protocol Numbers registry.
sourceTransportPort	7	2	The source port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the source port number given in the respective header.
destinationTransportPort	11	2	The destination port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the destination port number given in the respective header.
octetDeltaCount	1	4 or 8	The number of octets since the previous report (if any) in incoming packets for this Flow at the Observation Point. The number of octets includes IP header(s) and IP payload.
packetDeltaCount	2	4 or 8	The number of incoming packets since the previous report (if any) for this Flow at the Observation Point.

Information Element (IE)	IE id	IE size, B	Description
flowStartSysUpTime	22	4	The relative timestamp of the first packet of this Flow. It indicates the number of milliseconds since the last (re-)initialization of the IPFIX Device (sysUpTime). sysUpTime can be calculated from systemInitTimeMilliseconds.
flowEndSysUpTime	21	4	The relative timestamp of the last packet of this Flow. It indicates the number of milliseconds since the last (re-)initialization of the IPFIX Device (sysUpTime). sysUpTime can be calculated from systemInitTimeMilliseconds.

Syslog message fields – Average DNS response time

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20004”
exp_ip	NetFlow exporter IP address	<IPv4 address>
protocol	Transport Protocol (TCP = 6, UDP = 17)	<number>
dest_ip	DNS server IPv4 address	<IPv4_address>
min_time	Min DNS server response time, msec	<number>
max_time	Max DNS server response time, msec	<number>
avg_time	DNS server average response time, msec	<number>
flow_count	Number of flows	< number>

Key	Field Description	Comments
bytes_in	Average packet size received by the host from DNS server	<number>
packets_in	Packets received by the host from DNS server	<number>
bytes_out	Average packet size sent by the source host to DNS server	<number>
packets_out	Packets sent by the source host DNS server, packets	<number>
t_int	Observation time interval, msec	<number>

Syslog message fields – Top DNS users

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20005”
exp_ip	NetFlow exporter IP address	<IPv4 address>
src_ip	Source host IPv4 address	<IPv4_address>
flow_count	Number of flows	< number>
t_int	Observation time interval, msec	<number>

Asset Access Monitor (10014 / 20014)

Description

This Module monitors traffic to selected services characterized by an IP address, destination port number and an IP protocol (services) and matches communications to a list of authorized peers. The list of authorized peers may include IP address ranges or IP addresses of individual hosts. For each of the services the Module reports communications with the hosts outside of the authorized peers list.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 5 sec, max = 600 sec, default = 30 sec
List of protected IPv4 address, destination port number and IP protocol	Monitored Services List	e.g. 67.202.0.0,80,6; 72.44.32.0,53,17
List of protected IPv6 address, destination port number and IP protocol	Monitored Services List	e.g. 2620:0:2d0:200::7,80,6
Authorized Peers (IPv4 addresses and masks)	List of IPv4 addresses and masks (CIDR notation) (potentially IP addresses ranges)	e.g. 67.202.0.0,18; 72.44.32.0,24
Authorized Peers (IPv6 addresses and masks)	List of IPv6 addresses and masks (CIDR notation) (potentially IP addresses ranges)	e.g. 2620:0:2d0:200::7,64

Input

NetFlow v5 and v9, Cisco ASA NSEL, Palo Alto Networks NFv9, and IPFIX.

Required NetFlow fields

Information Element (IE)	IE id	IE size, B	Description
sourceIPv4Address or sourceIPv6Address	8 or 27	4 or 16	The IPv4 or IPv6 source address in the IP packet header
destinationIPv4Address or destinationIPv6Address	12 or 28	4 or 16	The IPv4 or IPv6 destination address in the IP packet header

Information Element (IE)	IE id	IE size, B	Description
protocolIdentifier	4	1	The value of the protocol number in the IP packet header. The protocol number identifies the IP packet payload type. Protocol numbers are defined in the IANA Protocol Numbers registry.
sourceTransportPort	7	2	The source port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the source port number given in the respective header.
destinationTransportPort	11	2	The destination port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the destination port number given in the respective header.

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20014”
exp_ip	NetFlow exporter IP address	<IPv4 address>
src_ip	Peer IPv4 address	<IPv4_address>
src_ip6	Peer IPv6 address	<IPv6_address>
[src_host]	Peer host name	<string>
dest_ip	Service IPv4 address	<IPv4_address>
dest_ip6	Service IPv6 address	<IPv6_address>
[dest_host]	Service host name	<string>

Key	Field Description	Comments
dest_port	Service transport port number	<number>
protocol	IP protocol (TCP = 6, UDP = 17)	<number>
flow_count	Number of observed flows	<number>
bytes_in	Traffic received, bytes	<number>
bytes_out	Traffic sent, bytes	<number>
t_int	Observation time interval, msec	<number>

Services Performance Monitor (10017 / 20017)

Description

This Module monitors services performance characteristics. A service is defined as a combination of a host IP address, a destination port number and an IP protocol. The Module calculates average response time over a specified Data Collection Interval and reports it for each of the listed servers. A special port number value (0) indicates that response time should be calculated over all ports serviced by that server (e.g. an FTP server in the passive mode). Along with response time measurements the Module also provides traffic volume in each direction and the number of flows.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 5 sec, max = 600 sec, default = 30 sec
List of monitored IPv4 address, destination port number and IP protocol tuples	List of the watched services (IPv4 address, destination port number and IP protocol)	e.g. 67.202.0.200 / 80/6; 72.44.32.1 / 53/ 17
List of monitored IPv6 address, destination port number and IP protocol tuples	List of the watched services (IPv6 address, destination port number and IP protocol)	e.g. 2620:0:2d0:200::7/ 53/ 17

Input

NetFlow v5 and v9, Cisco ASA NSEL, Palo Alto Networks NFv9.

Required NetFlow fields

Information Element (IE)	IE id	IE size, B	Description
sourceIPv4Address or sourceIPv6Address	8 or 27	4 or 16	The IPv4 or IPv6 source address in the IP packet header
destinationIPv4Address or destinationIPv6Address	12 or 28	4 or 16	The IPv4 or IPv6 destination address in the IP packet header
protocolIdentifier	4	1	The value of the protocol number in the IP packet header. The protocol number identifies the IP packet payload type. Protocol numbers are defined in the IANA Protocol Numbers registry.
sourceTransportPort	7	2	The source port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the source port number given in the respective header.
destinationTransportPort	11	2	The destination port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the destination port number given in the respective header.
octetDeltaCount	1	4 or 8	The number of octets since the previous report (if any) in incoming packets for this Flow at the Observation Point. The number of octets includes IP header(s) and IP payload.
flowStartSysUpTime	22	4	The relative timestamp of the first packet of this Flow. It indicates the number of milliseconds since the last (re-)initialization of the IPFIX Device (sysUpTime). sysUpTime can be calculated from systemInitTimeMilliseconds.
flowEndSysUpTime	21	4	The relative timestamp of the last packet of this Flow. It indicates the number of milliseconds since the last (re-)initialization of the IPFIX Device (sysUpTime). sysUpTime can be calculated from systemInitTimeMilliseconds.

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss

Key	Field Description	Comments
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20017”
exp_ip	NetFlow exporter IP address	<IPv4 address>
dest_ip	Service IPv4 address	<IPv4_address>
dest_ip6	Service IPv6 address	<IPv6_address>
dest_port	Service transport port number	<number>
protocol	IP protocol (TCP = 6, UDP = 17)	<number>
min_time	Min service response time, msec	<number>
max_time	Max service response time, msec	<number>
avg_time	Average service response time, msec	<number>
flow_count	Number of observed flows	<number>
bytes_in	Traffic received, bytes	<number>
bytes_out	Traffic sent, bytes	<number>
t_int	Observation time interval, msec	<number>

Cisco ASA Devices Monitoring

Top Bandwidth Consumers for Cisco ASA (10018 / 20018)

Description

This Module utilizes Cisco ASA NSEL data and provides a list of top network bandwidth consumers operating on the internal network. Top bandwidth consumers are reported **by Network Device and by Destination Port** over a time interval T. Only TCP/IP and UDP traffic is accounted for. The number of reported top consumers (N) and the observation interval (T, sec) are configurable.

This information is provided per NetFlow exporter.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 10 sec, max = 600 sec, default = 30 sec
Application protocol (l4_dst_port) list	List of watched layer 4 destination ports. If specified, the traffic is reported by specified ports, and all other traffic is summed up under dest_port=0. If the list is empty, the traffic is reported by all actual destination ports.	e.g. 80, 443
N – number of reported hosts	Top N (number of reported destinations)	min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)
Enable(1) or disable (0) reporting by destination port	If set to 1, enable network traffic monitoring by destination port. If set to 0, report total network traffic as destination port 0 (dest_port=0)	default = 0

Inputs

Cisco ASA NSEL.

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss

Key	Field Description	Comments
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20018”
exp_ip	NetFlow exporter IPv4 address	<IPv4_address>
src_ip	Source host IPv4 address	<IPv4_address>
src_ip6	Source host IPv6 address	<IPv6_address>
dest_port	Destination port number (e.g. 80 for http)	<number>
user	Username (up to 20 bytes)	<string> (“na” if not available)
created_count	Created flows count	<number>
denied_count	Denied flows count	<number>
bytes	Bytes total (Traffic)	<number>
percent_of_total	Percent of Total (Traffic)	<decimal>, e.g. 25.444% is 25.444
t_int	Observation time interval, msec	<number>

Top Traffic Destinations for Cisco ASA (10019 / 20019)

Description

This Module utilizes Cisco ASA NSEL data and provides a list of most popular destinations measured by the traffic. Top destinations are reported by Network Device and by Destination Port over a time interval T. Only TCP/IP and UDP traffic is accounted for. The number of reported top destinations (N) and the observation interval (T, sec) are configurable.

This information is provided per NetFlow exporter.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 10 sec, max = 600 sec, default = 30 sec
Application protocol (l4_dst_port) list	List of watched layer 4 destination ports. If specified, the traffic is reported by specified ports, and all other traffic is summed up under dest_port=0. If the list is empty, the traffic is reported by all actual destination ports.	e.g. 80, 443
N – number of reported hosts	Top N (number of reported destinations)	min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)
Enable(1) or disable (0) reporting by destination port	If set to 1, enable network traffic monitoring by destination port. If set to 0, report total network traffic as destination port 0 (dest_port=0)	default = 0

Inputs

Cisco ASA NSEL.

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address

Key	Field Description	Comments
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20019”
exp_ip	NetFlow exporter IPv4 address	<IPv4_address>
dest_ip	Destination host IPv4 address	<IPv4_address>
dest_ip6	Destination host IPv6 address	<IPv6_address>
dest_port	Destination port number (e.g. 80 for http)	<number>
created_count	Created flows count	<number>
denied_count	Denied flows count	<number>
bytes	Bytes total (Traffic)	<number>
percent_of_total	Percent of Total (Traffic)	<decimal>, e.g. 25.444% is 25.444
t_int	Observation time interval, msec	<number>

Top Policy Violators for Cisco ASA (10020 / 20020)

Description

This Module utilizes Cisco ASA NSEL data and provides a list of firewall policies violators. Top violators are reported by Network Device and by Destination Port over a time interval T. Only TCP/IP and UDP traffic is accounted for. The number of reported top violators (N) and the observation interval (T, sec) are configurable.

This information is provided per NetFlow exporter.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 10 sec, max = 600 sec, default = 30 sec
Application protocol (l4_dst_port) list	List of watched layer 4 destination ports. If specified, the traffic is reported by specified ports, and all other traffic is summed up under dest_port=0. If the list is empty, the traffic is reported by all actual destination ports.	e.g. 80, 443
N – number of reported hosts	Top N (number of reported destinations)	min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)
Enable(1) or disable (0) reporting by destination port	If set to 1, enable network traffic monitoring by destination port. If set to 0, report total network traffic as destination port 0 (dest_port=0)	default = 0

Inputs

Cisco ASA NSEL.

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20020”
exp_ip	NetFlow exporter IPv4 address	<IPv4_address>
src_ip	Source host IPv4 address	<IPv4_address>
src_ip6	Source host IPv6 address	<IPv6_address>

Key	Field Description	Comments
dest_ip	Destination host IPv4 address	<IPv4_address>
dest_ip6	Destination host IPv6 address	<IPv6_address>
dest_port	Destination port number (e.g. 80 for http)	<number>
denied_count	Denied flows count	<number>
t_int	Observation time interval, msec	<number>

Top Hosts with most Connections for Cisco ASA (10021 / 20021)

Description

This Module handles Cisco ASA NSEL. It provides top N (by the number of connections) consumers (users) by Network Device by Protocol (Destination Port) over a time interval T. Cisco ASA customers may turn on NSEL at the highest reporting level, and still receive consolidated data (several syslog messages) every T seconds.

This information is provided per NetFlow exporter.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 10 sec, max = 600 sec, default = 30 sec
Application protocol (l4_dst_port) list	List of watched layer 4 destination ports. If specified, the traffic is reported by specified ports, and all other traffic is summed up under dest_port=0. If the list is empty, the traffic is reported by all actual destination ports.	e.g. 80, 443
N – number of reported hosts	Top N (number of reported destinations)	min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)
Enable(1) or disable (0) reporting by destination port	If set to 1, enable network traffic monitoring by destination port. If set to 0, report total network traffic as destination port 0 (dest_port=0)	default = 0

Inputs

Cisco ASA NSEL.

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20021”
exp_ip	NetFlow exporter IPv4 address	<IPv4_address>
src_ip	Source host IPv4 address	<IPv4_address>
src_ip6	Source host IPv6 address	<IPv6_address>
dest_port	Destination port number (e.g. 80 for http)	<number>
user	Username (up to 20 bytes)	<string> (“na” if not available)
created_count	Created flows count	<number>
t_int	Observation time interval, msec	<number>

Palo Alto Networks Devices Monitoring

Top Bandwidth Consumers for Palo Alto Networks (10030 / 20030)

Description

This Module utilizes Palo Alto Networks NetFlow v9 reporting and provides a list of top network bandwidth consumers operating on the internal network. Top bandwidth consumers are reported **by Network Device and by Destination Port** over a time interval. Only TCP/IP and UDP traffic is accounted for. The number of reported top consumers (N) and the observation interval (T, sec) are configurable.

This information is provided per NetFlow exporter.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 10 sec, max = 600 sec, default = 30 sec
N - number of reported bandwidth consumers	Top N (number of reported consumers)	min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)

Inputs

Palo Alto Networks NetFlow v9.

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20030”
exp_ip	NetFlow exporter IPv4 address	<IPv4_address>
src_ip	Source host IPv4 address	<IPv4_address>
src_ip6	Source host IPv6 address	<IPv6_address>
user	User-ID	<string> (“na” if not available)
created_count	Created flows count	<number>
denied_count	Denied flows count	<number>

Key	Field Description	Comments
bytes	Bytes total (Traffic)	<number>
percent_of_total	Percent of Total (Traffic)	<decimal>, e.g. 25.444% is 25.444
t_int	Observation time interval, msec	<number>

Top Traffic Destinations for Palo Alto Networks (10031 / 20031)

Description

This Module utilizes Palo Alto Networks NetFlow v9 reporting and provides a list of top network bandwidth destinations. Top bandwidth destinations are reported **by Network Device and by Destination Port** over a time interval. Only TCP/IP and UDP traffic is accounted for. The number of reported top consumers (N) and the observation interval (T, sec) are configurable.

This information is provided per NetFlow exporter.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 10 sec, max = 600 sec, default = 30 sec
Application protocol (l4_dst_port) list	List of watched layer 4 destination ports. If specified, the traffic is reported by specified ports, and all other traffic is summed up under dest_port=0. If the list is empty, the traffic is reported by all actual destination ports.	e.g. 80, 443
N – number of reported hosts	Top N (number of reported destinations)	min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)
Enable(1) or disable (0) reporting by destination port	If set to 1, enable network traffic monitoring by destination port. If set to 0, report total network traffic as destination port 0 (dest_port=0)	default = 0
M – maximum number of destination ports to report	Top number of ports to report	min = 1, max = 50, default = 10

Inputs

Palo Alto Networks NetFlow v9.

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20031”
exp_ip	NetFlow exporter IPv4 address	<IPv4_address>
dest_ip	Destination host IPv4 address	<IPv4_address>
dest_ip6	Destination host IPv6 address	<IPv6_address>
dest_port	Destination port number (e.g. 80 for http)	<number>
created_count	Created flows count	<number>
denied_count	Denied flows count	<number>
bytes	Bytes total (Traffic)	<number>
percent_of_total	Percent of Total (Traffic)	<number> (if < 1% reported as zero)
t_int	Observation time interval, msec	<number>

Hosts with Most Policy Violations for Palo Alto Networks (10032 / 20032)

Description

This Module utilizes Palo Alto Networks NetFlow v9 reporting and provides a list of top firewall policies violators. Top violators are reported **by Network Device and by Destination Port** over a time interval. The number of reported top violators (N) and the observation interval (T, sec) are configurable.

This information is provided per NetFlow exporter.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 10 sec, max = 600 sec, default = 30 sec
Application protocol (l4_dst_port) list	List of watched layer 4 destination ports. If specified, the traffic is reported by specified ports, and all other traffic is summed up under dest_port=0. If the list is empty, the traffic is reported by all actual destination ports.	e.g. 80, 443
N – number of reported hosts	Top N (number of reported destinations)	min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)
Enable(1) or disable (0) reporting by destination port	If set to 1, enable network traffic monitoring by destination port. If set to 0, report total network traffic as destination port 0 (dest_port=0)	default = 0
M – maximum number of destination ports to report	Top number of ports to report	min = 1, max = 50, default = 10

Inputs

Palo Alto Networks NetFlow v9.

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss

Key	Field Description	Comments
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20032”
exp_ip	NetFlow exporter IPv4 address	<IPv4_address>
src_ip	Source host IPv4 address	<IPv4_address>
src_ip6	Source host IPv6 address	<IPv6_address>
dest_ip	Destination host IPv4 address	<IPv4_address>
dest_ip6	Destination host IPv6 address	<IPv6_address>
dest_port	Destination port number (e.g. 80 for http)	<number>
user	User-ID	<string> (“na” if not available)
denied_count	Denied flows count	<number>
t_int	Observation time interval, msec	<number>

Most Active Hosts for Palo Alto Networks (10033 / 20033)

Description

This Module utilizes Palo Alto Networks NetFlow v9 reporting and provides a list of most active hosts by the number of initiated connections. Most active hosts are reported **by Network Device and by Destination Port** over a time interval. The number of reported top most active hosts (N) and the observation interval (T, sec) are configurable.

This information is provided per NetFlow exporter.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 10 sec, max = 600 sec, default = 30 sec
Application protocol (l4_dst_port) list	List of watched layer 4 destination ports. If specified, the traffic is reported by specified ports, and all other traffic is summed up under dest_port=0. If the list is empty, the traffic is reported by all actual destination ports.	e.g. 80, 443
N – number of reported hosts	Top N (number of reported destinations)	min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)
Enable(1) or disable (0) reporting by destination port	If set to 1, enable network traffic monitoring by destination port. If set to 0, report total network traffic as destination port 0 (dest_port=0)	default = 0
M – maximum number of destination ports to report	Top number of ports to report	min = 1, max = 50, default = 10

Inputs

Palo Alto Networks NetFlow v9.

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20033”
exp_ip	NetFlow exporter IPv4 address	<IPv4_address>
src_ip	Source host IPv4 address	<IPv4_address>

Key	Field Description	Comments
src_ip6	Source host IPv6 address	<IPv6_address>
dest_port	Destination port number (e.g. 80 for http)	<number>
user	User-ID	<string> (“na” if not available)
created_count	Created flows count	<number>
t_int	Observation time interval, msec	<number>

Bandwidth Consumption per Application for Palo Alto Networks (10034 / 20034)

Description

This Module utilizes Palo Alto Networks NetFlow v9 reporting and provides a list of most active applications by traffic. Most active applications are reported **by Network Device** over a time interval. The number of reported top most active applications (N) and the observation interval (T, sec) are configurable.

This information is provided per NetFlow exporter.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 10 sec, max = 600 sec, default = 30 sec
Application id list	A list of watched applications. If specified, the traffic is reported by specified applications, and all other traffic is summed up under app=other. If the list is empty, the traffic is reported by all applications.	
N - number of reported consumers	Top N (number of reported applications)	min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)
Report selected applications only (1)	Enable/Disable reporting selected apps only (1 - report only apps in the list, 0 - report all apps)	default = 0

Inputs

Palo Alto Networks NetFlow v9.

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20034”
exp_ip	NetFlow exporter IPv4 address	<IPv4_address>
app	Application	<string>
created_count	Created flows count	<number>
bytes	Bytes total (Traffic)	<number>
percent_of_total	Percent of Total (Traffic)	<decimal>, e.g. 25.444% is 25.444
t_int	Observation time interval, msec	<number>

Bandwidth Consumption per Application and Users for Palo Alto Networks (10035 / 20035)

Description

This Module utilizes Palo Alto Networks NetFlow v9 reporting and provides a list of most active applications and users by traffic. Most active applications and users are reported **by Network Device** over a time interval. The number of reported top most active applications and users (N) and the observation interval (T, sec) are configurable.

This information is provided per NetFlow exporter.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 10 sec, max = 600 sec, default = 30 sec
Application id list	A list of watched applications. If specified, the traffic is reported by specified applications, and all other traffic is summed up under app=other. If the list is empty, the traffic is reported by all applications.	
Share of total traffic reported, %	Reported percent of total traffic by application by user	e.g. 50 - indicates that all application/user entries consuming 50% of traffic are reported; min = 1%, max = 100%, default = 80%
Report selected applications only (1)	Enable/Disable reporting selected apps only (1 - report only apps in the list, 0 - report all apps)	default = 0

Inputs

Palo Alto Networks NetFlow v9.

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20035”
exp_ip	NetFlow exporter IPv4 address	<IPv4_address>
app	Application	<string>
user	User-ID	<string> (“na” if not available)

Key	Field Description	Comments
created_count	Created flows count	<number>
bytes	Bytes total (Traffic)	<number>
percent_of_total	Percent of Total (Traffic)	<decimal>, e.g. 25.444% is 25.444
t_int	Observation time interval, msec	<number>

VMware

Top VM:Host Pairs (10164 / 20164)

Description

This Module reports top network conversations in VM environment. A network conversion is a series of data exchanges between two VM:Hosts (VM source IP:Host source IP and VM destination IP:Host destination IP), over the same protocol (TCP or UDP), and going through the same vSphere Distributed switch (VDS) (VxLAN ID). The number of exchanged bytes and packets are summed up.

The Module determines which VM:Host is a client and which is a server as follows: a server sends more traffic (bytes) than a client.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 5 sec, max = 600 sec, default = 30 sec
N - number of reported host:vm pairs	The number of top hosts reported per NetFlow exporter	min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)

Input

VMware IPv4 VXLAN Template.

Syslog message fields

Key	Field Description	Comments
	NetFlow Optimizer timestamp	Format: Mmm dd hh:mm:ss
	NetFlow Optimizer server IP address	Format: IPv4_address
	NetFlow Optimizer server NetFlow source ID	Configurable.
nfc_id	Message type identifier	“nfc_id=200164”
exp_ip	NetFlow exporter IP address	<IPv4 address>
vxlanId	VxLAN ID	<number>
sourceIPv4Address	Source host IPv4 address	<IPv4 address>
destinationIPv4Address	Destination host IPv4 address	<IPv4 address>
packetDeltaCount_in	Packets from client to server	<number>
octetDeltaCount_in	Layer 3 bytes from client to server	<number>
packetDeltaCount_out	Packets from server to client	<number>
octetDeltaCount_out	Layer 3 bytes from server to client	<number>
packetDeltaCount	Total Packets in the flow received by the input interface	<number>
octetDeltaCount	Total number of Layer 3 bytes in the packets of the flow received by the input interface	<number>
tenantSourceIPv4	Source VM IPv4 address	<IPv4 address>
tenantDestIPv4	Destination VM IPv4 address	<IPv4 address>

Key	Field Description	Comments
vm_adjacency	VM adjacency indicator. If equal “Y”, VMs are residing on the same host.	<string> “Y” or “N”
flow_count	Number of Flows	<number>
percent_of_total	Percent of Total (bytes) VXLAN traffic	<decimal>
t_int	Observation time interval, msec	<number>

Top VM Traffic Monitor (10167 / 20167)

Description

This Module identifies VMs with the most traffic. It consolidates NetFlow records over a period of time (Data Collection Interval) which all have the same combination of the following fields:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol
- Input interface
- Output interface
- VxLAN ID
- Source VM IPv4 address
- Destination VM IPv4 address
- Source VM port number
- Destination VM port number
- VM protocol
- VM ingress interface SNMP index
- VM egress interface SNMP index

This information is provided per NetFlow exporter.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 5 sec, max = 600 sec, default = 30 sec
N – number of reported hosts	The number of top hosts reported per NetFlow exporter	min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)

Input

VMware IPv4 VXLAN Template.

Syslog message fields

Key	Field Description	Comments
	NetFlow Optimizer timestamp	Format: Mmm dd hh:mm:ss
	NetFlow Optimizer server IP address	Format: IPv4_address
	NetFlow Optimizer server NetFlow source ID	Configurable.
nfc_id	Message type identifier	“nfc_id=200167”
exp_ip	NetFlow exporter IP address	<IPv4 address>
vxlanId	VxLAN ID	<string>
sourceIPv4Address	Source host IPv4 address	<IPv4 address>
destinationIPv4Address	Destination host IPv4 address	<IPv4 address>
octetDeltaCount	Total number of Layer 3 bytes in the packets of the flow received by the input interface	<number>
packetDeltaCount	Packets in the flow received by the input interface	<number>
sourceTransportPort	Source host port number	<number>
destinationTransportPort	Destination host port number	<number>
ingressInterface	Exporter ingress interface SNMP index	<number>
egressInterface	Exporter egress interface SNMP index	<number>
protocolIdentifier	Transport Protocol (TCP = 6, UDP = 17)	<number>

Key	Field Description	Comments
tcpFlags	Cumulative OR of TCP flags	
IPv4TOS	IP type of service (ToS)	<number>
tenantSourceIPv4	Source VM IPv4 address	<IPv4 address>
tenantDestIPv4	Destination VM IPv4 address	<IPv4 address>
tenantSourcePort	Source VM port number	<number>
tenantDestPort	Destination VM port number	<number>
tenantProtocol	VM protocol	<number>
vm_adjacency	VM adjacency indicator. If equal “Y”, VMs are residing on the same host.	<string> “Y” or “N”
flow_count	Number of Flows	<number>
percent_of_total	Percent of Total (bytes) VXLAN traffic	<decimal>
t_int	Observation time interval, msec	<number>

Utilities

Sampling Monitor (10002 / 20002)

Description

This utility reports NetFlow sampling information. For NFv5 sampling interval is taken from the header. For NFv9 sampling interval and other fields are taken from NetFlow options.

Parameters

Parameter Name	Description	Comments
Data Collection Interval, sec	Module logic execution interval	min = 10 sec, max = 600 sec, default = 60 sec
Default sampling interval	Sampling interval used in case no NFv9 options are available	min = 1, max = 100000, default = 1
Sampling info expiration time	Stop sending sampling information after this time of not seeing any traffic from the network device	min = 1 sec, max = 100000 sec, default = 300 sec

Input

NetFlow v5, v9, sFlow

Required NetFlow fields

Information Element (IE)	IE id	IE size, B	Description
samplerId	48	1	The unique identifier associated with samplerName. **Attention**: this IE is deprecated in favor of selectorId (302)

Syslog message fields

Key	Field Description	Comments
	NetFlow Optimizer timestamp	Format: Mmm dd hh:mm:ss
	NetFlow Optimizer server IP address	Format: IPv4_address
	NetFlow Optimizer server NetFlow source ID	Configurable.
nfc_id	Message type identifier	“nfc_id=20002”
exp_ip	NetFlow exporter IP address	<IPv4 address>
flow_smpl_id	Flow Sampler ID	<number>

Key	Field Description	Comments
smpl_int	Sampling interval	<number>
smpl_algo	Sampling algorithm	<string>
t_int	Observation time interval, msec	<number>

SNMP Information Monitor (10003 / 20003)

Description

This utility reports SNMP information. This information is provided per exporter-interface (exp_ip-ifIndex) pair.

Parameters

Parameter Name	Description	Comments
Report SNMP information	Module reporting interval	min = 60 sec, max = 86400 sec, default = 300 sec
Refresh SNMP information	SNMP information time of life	min = 300 sec, max = 86400 sec, default = 3600 sec

Required NetFlow fields

Information Element (IE)	IE id	IE size, B	Description
ingressInterface	10	4	The index of the IP interface where packets of this Flow are being received.[20]
egressInterface	14	4	The index of the IP interface where packets of this Flow are being sent.

[20] The value matches the value of managed SNMP object 'ifIndex'

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable.
nfc_id	Message type identifier	“nfc_id=20003”
exp_ip	NetFlow exporter IP address	<IPv4 address>
mgmt_ip	Device Management IP address	<IPv4 address>
sysName	NetFlow exporter resolved name	<string>
ifIndex	NetFlow exporter interface SNMP index	<number>
ifName	NetFlow exporter interface resolved name	<string>
ifDescr	NetFlow exporter interface resolved description	<string>
ifType	NetFlow exporter interface type	<number>
ifMtu	NetFlow exporter interface MTU	<number>
ifSpeed	NetFlow exporter interface bandwidth in bits/sec	<number>
ifPhysAddress	NetFlow exporter interface physical address	<MAC address>
ifIPAddress	NetFlow exporter interface IP address	<IPv4 address>

Special Converters

Original Flow Data (20001)

Description

Original Flow Data Converter translates NetFlow v5, v9, and IPFIX (including Cisco ASA NSEL, Cisco High-Speed Logging (HSL), Cisco Application Visibility and Control (AVC), and Palo Alto Networks NetFlow) records into syslog messages 1-to-1. Each NetFlow record is converted into a syslog message in the “key=value” format. The table below shows a **partial** list of key values.

Field Type	Value	Length (bytes)	Description	Key
IN_BYTES	1	N (default is 4)	Incoming counter with length N x 8 bits for number of bytes associated with an IP Flow.	bytes_in
IN_PKTS	2	N (default is 4)	Incoming counter with length N x 8 bits for the number of packets associated with an IP Flow	packets_in
FLOWS	3	N	Number of flows that were aggregated; default for N is 4	flow_count
PROTOCOL	4	1	IP protocol byte	protocol
SRC_TOS	5	1	Type of Service byte setting when entering incoming interface	src_tos
TCP_FLAGS	6	1	Cumulative of all the TCP flags seen for this flow	tcp_flag
L4_SRC_PORT	7	2	TCP/UDP source port number i.e.: FTP, Telnet, or equivalent	src_port
IPV4_SRC_ADDR	8	4	IPv4 source address	src_ip

Field Type	Value	Length (bytes)	Description	Key
SRC_MASK	9	1	The number of contiguous bits in the source address subnet mask i.e.: the submask in slash notation	src_mask
INPUT_SNMP	10	N	Input interface index; default for N is 2 but higher values could be used	input_snmp
L4_DST_PORT	11	2	TCP/UDP destination port number i.e.: FTP, Telnet, or equivalent	dest_port
IPV4_DST_ADDR	12	4	IPv4 destination address	dest_ip
DST_MASK	13	1	The number of contiguous bits in the destination address subnet mask i.e.: the submask in slash notation	dest_mask
OUTPUT_SNMP	14	N	Output interface index; default for N is 2 but higher values could be used	output_snmp
IPV4_NEXT_HOP	15	4	IPv4 address of next-hop router	next_hop
SRC_AS	16	N (default is 2)	Source BGP autonomous system number where N could be 2 or 4	src_asn
DST_AS	17	N (default is 2)	Destination BGP autonomous system number where N could be 2 or 4	dest_asn
BGP_IPV4_NEXT_HOP	18	4	Next-hop router's IP in the BGP domain	bgp_next_hop
MUL_DST_PKTS	19	N (default is 4)	IP multicast outgoing packet counter with length N x 8 bits for packets associated with the IP Flow	mul_dest_packets
MUL_DST_BYTES	20	N (default is 4)	IP multicast outgoing byte counter with length N x 8 bits for bytes associated with the IP Flow	mul_dest_bytes

Field Type	Value	Length (bytes)	Description	Key
LAST_SWITCHED	21	4	System uptime at which the last packet of this flow was switched	last_time
FIRST_SWITCHED	22	4	System uptime at which the first packet of this flow was switched	first_time
OUT_BYTES	23	N (default is 4)	Outgoing counter with length N x 8 bits for the number of bytes associated with an IP Flow	bytes_out
OUT_PKTS	24	N (default is 4)	Outgoing counter with length N x 8 bits for the number of packets associated with an IP Flow.	packets_out

Input

NetFlow v5, NetFlow v9, Cisco ASA NSEL, Cisco HSL, Cisco AVC, Palo Alto Networks.

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20001”
…	[Varies depending on the template]	…

sFlow Data (20800, 20900)

Description

sFlow Data Converter translates sFlow records into syslog messages 1-to-1. Each sFlow record is converted into a syslog message in the “key=value” format. sFlow Counter syslogs are identified by nfc_id=20800. sFlow Data records have nfc_id=20900.

The following configuration is available in NetFlow Optimizer:

- Include sFlow Counter records (default is not to include)
- Included headerLen and headerBytes fields in the syslog output (default is not to include)

Additional information on sFlow specifications could be found here:

http://www.sflow.org/developers/specifications.php

The table below shows a **partial** list of key values.

Input

sFlow

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20800” or “nfc_id=20900”
ent	Enterprise ID	<number>
fmt	Format	<number>
exp_ip	sFlow exporter IP address	<IPv4 address>
samplingRate	Sampling rate	<number>
inputPort	SNMP index of input interface	<number>
outputPort	SNMP index of output interface	<number>
[headerLen][21]	Length of Header included in the sample	<number>

[21] This field is optional, and should be enabled in NetFlow Integrator to be included in the syslog.

Key	Field Description	Comments
[headerBytes][21]	Header bytes included in the sample	<string>
srcIP	Source IP address	<IPv4 address>
dstIP	Destination IP address	<IPv4 address>
IPProtocol	Transport Protocol (TCP = 6, UDP = 17)	<number>
IPTOS	IP type of service	<number>
TCPSrcPort	Source port number	<number>
TCPDstPort	Destination port number	<number>
…	[Varies depending on the record type]	…

FDR Packeteer-2 Flow Data (20010)

Description

FDR Packeteer-2 Flow Data Converter translates Blue Coat's PacketShaper flows into syslog messages 1-to-1. Each flow record is converted into a syslog message in the "key=value" format. The tables below describe the mapping between Packeteer-2 Flow Data and key values.

FDR Packeteer-2 Header

This table describes the header present in each Packeteer-2 protocol packet.

Name	Bytes	NetFlow Logic field
Version	2	
Flow records in this PDU	1	
Shaper Serial Number	5	device

Name	Bytes	NetFlow Logic field
Unix Time in sec	4	
Residual nanoseconds	4	
Total flows seen	4	
PacketeerFlowRecordsID	4	flow_id
SysUpTime in millisec	4	

FDR Packeteer-2 Records

This table describes the data records present in each Packeteer-2 packet. The number of bytes used and any additional information is given for each data i`tem included in the FDR packet.

Name	Bytes	Description	NetFlow Logic field
Source IPaddr	4	The IP address from which a flow was sent	src_ip
Destination IPaddr	4	The IP address to which a flow was sent	dest_ip
Packeteer ClassID	4	A numeric descriptor for a PacketShaper-identified traffic class	class_id
Inbound IFindex	2	The PacketShaper interface through which the flow entered	ifindex_in
Outbound IFindex	2	The PacketShaper interface through which the flow exited	ifindex_out
Packet Count	4	The total number of packets in the flow	packets
Byte Count	4	The total number of bytes in the flow	bytes
Time at Start of Flow	4	SysUpTime when first packet seen	first_time
Time at End of Flow	4	SysUpTime when last packet seen	last_time

Name	Bytes	Description	NetFlow Logic field
Source Port	2	The port on which the flow was sent	src_port
Destination Port	2	The port to which the flow was sent	dest_port
Packeteer Policy	1	priority=1, rate=2, uncontrolled=8, discard=16 or never-admit=32	policy
TCP flags	1	The logical sum (AND) of all TCP flags seen during the flow	tcp_flag
Layer 4 protocol	1	The type of layer 4 protocol for the flow. Common IP protocol values are: 1 ICMP 2 IGMP 6 TCP 9 IGRP 17 UDP 41 IPv6 46 RSVP 47 GRE 50 IPSec 51 IPSec 108 IPComp	protocol
IP ToS/DiffServ Byte (DSCP)	1	The value of any Type of Service or DiffServ (DSCP) for the flow, if present	tos
Packeteer Service Type	2	The type of service (TOS)	service_id
Server at Source or Dest.	1	The location of the server for this flow, may not apply to some protocols: s = source of the flow d = destination of the flow 0 = unknown (may not be a client/server based protocol)	srv_loc
Packeteer Policy Priority	1	Priority for this flow (0-7), either the priority assigned by a priority policy, or the priority assigned to excess rate with a rate policy	priority
Retransmitted Bytes	4	The number of bytes requiring retransmission for this flow	r_bytes
VLanID	2	The ID number of any 802.1q VLAN associated with the flow	vlan_id

Name	Bytes	Description	NetFlow Logic field
TTL	1	Time to Live of the flow's last packet	ttl
Measurements Type	1	'p'=Ping 'v'=RTCP 'a'=RTM 't'=TCP 0=none	m_type
Measurement 1	4	The first measurement in this FDR packet (see below)	m1
Measurement 2	4	The second measurement in this FDR packet (see below)	m2
Measurement 3	4	The third measurement in this FDR packet (see below)	m3

Input

FDR Packeteer-2

Syslog message fields

Key	Field Description	Comments
	NetFlowIntegrator timestamp	Format: Mmm dd hh:mm:ss
	NetFlowIntegrator server IP address	Format: IPv4_address
	NetFlowIntegrator server NetFlow source ID	Configurable
nfc_id	Message type identifier	“nfc_id=20010”
device	PacketShaper Serial Number[22]	<string>
flow_id	PacketShaper flow identifier	<number>
src_ip	The IP address from which a flow was sent	<IPv4_address>
dest_ip	The IP address to which a flow was sent	<IPv4_address>

[22] This field is taken from Packeteer-2 Header

Key	Field Description	Comments
class_id	PacketShaper traffic class ID	<number>
application	Application (class ID name)[23]	<string>
ifindex_in	Inbound Interface	<number>
ifindex_out	Outbound Interface	<number>
packets	Packet Count	<number>
bytes	Byte Count	<number>
first_time	Time at Start of Flow	<number>
last_time	Time at End of Flow	<number>
src_port	Source Port	<number>
dest_port	Destination Port	<number>
policy	Packeteer Policy	<number>
tcp_flag	TCP flags	<number>
protocol	Transport Protocol (TCP = 6, UDP = 17)	<number>
tos	IP ToS/DiffServ Byte (DSCP)	<number>
service_id	Packeteer Service Type	<number>
srv_loc	Server Location	<number>
priority	Packeteer Policy Priority	<number>

[23] This field is populated from a lookup CSV file that maps class ID to Application name.

Key	Field Description	Comments
r_bytes	Retransmitted Bytes	<number>
vlan_id	VLanID	<number>
ttl	TTL	<number>
m_type	Measurements Type	<number>
m1	Measurement 1	<number>
m2	Measurement 2	<number>
m3	Measurement 3	<number>

Appendix

NetFlow v5 - NetFlow v9 Field Types Mapping

NetFlow v5 Fields		NetFlow v9 Representation		
Contents	**Description**	**Contents**	**Description**	**Contents**
srcaddr	Source IP address	IPV4_SRC_ADDR	8	4
dstaddr	Destination IP address	IPV4_DST_ADDR	12	4
nexthop	IP address of next hop router	IPV4_NEXT_HOP	15	4
input	SNMP index of input interface	INPUT_SNMP	10	4
output	SNMP index of output interface	OUTPUT_SNMP	14	4
dPkts	Packets in the flow	IN_PKTS	2	4
dOctets	Total number of Layer 3 bytes in the packets of the flow	IN_BYTES	1	4
first	SysUptime at start of flow	FIRST_SWITCHED	22	4
last	SysUptime at the time the last packet of the flow was received	LAST_SWITCHED	21	4
srcport	TCP/UDP source port number or equivalent	L4_SRC_PORT	7	2
dstport	TCP/UDP destination port number or equivalent	L4_DST_PORT	11	2
pad1	Unused (zero) bytes	Not converted	N/A	N/A
tcp_flags	Cumulative OR of TCP flags	TCP_FLAGS	6	1

prot	IP protocol type (for example, TCP = 6; UDP = 17)	PROTOCOL	4	1
tos	IP type of service (ToS)	SRC_TOS	5	1
src_as	Autonomous system number of the source, either origin or peer	SRC_AS	16	2
dst_as	Autonomous system number of the destination, either origin or peer	DST_AS	17	2
src_mask	Source address prefix mask bits	SRC_MASK	9	1
dst_mask	Destination address prefix mask bits	DST_MASK	13	1
pad2	Unused (zero) bytes	Not converted	N/A	N/A