NetFlow Optimizer™

Release Notes

Version 2.5.1.4 (Build 2.5.1.4.10)

January 2019

Contents

What’s New in this Release

Build 2.5.1.4.10

This is a maintenance release. It contains all hot fixes delivered in 2018. Several minor features have been implemented as well.

⚠ Security update: Remove SHA-1 ciphers

Disable SHA-1 ciphers: add ciphers="HIGH:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!kRSA:!SHA1" attribute in server.xml

Customer Request/Ticket numbers: NFC-8751, ZEN-607

Added VDS Port group name to Module Microsegmentation output

Implement adding VDS port group name to External Data Feeder Agent for vCenter integration in Microsegmentation Module. Optionally add VDS port group to Module syslog output.

Customer Request/Ticket numbers: NFC-8755

Added "Report denied flows" parameter to Security Modules (1005x)

By default denied flows are reported by Security Modules. Added this parameter to optionally exclude denied flows from being reported.

Customer Request/Ticket numbers: NFC-8756

Implement retries in keep-alive algorithm

When NFO server goes down, NFO controller (keep-alive task) restarts it only once. If restart fails NFO needs to be restarted manually. In this fix the following is implemented: If restart fails, NFO controller attempts to start NFO server several times: in 0s, 30s, 60s, 2m, 4m, and finally in 8m.

Customer Request/Ticket numbers: NFC-8780, ZEN-610

Build 2.5.1.0.43

Added support for SNMP Traps

NFO SNMP service supports SNMP Traps now.

Customer Request/Ticket numbers: NFC-8334

Improved SNMP Polling performance

Implement GetBulk request for Table OIDs.

Customer Request/Ticket numbers: NFC-8415

Added support for sFlow extensions in Original Flow data

NFO sFlow support includes sFlow extended structures as of February 2018 (https://sflow.org/developers/structures.php).

Customer Request/Ticket numbers: NFC-8429

Added support for GeoIP enrichment using IP2Location databases

NFO Geo IP enrichment now has a choice: use MaxMind (GeoLite2-Country or GeoLite2-City) or IP2Location (DB1LITE for country level or DB5LITE for city level).

Customer Request/Ticket numbers: NFC-8397

Added Cisco ASA support in V2P Module

Virtual to Physical (V2P) Network Visibility Module now is able to process Cisco ASA NSEL.

Customer Request/Ticket numbers: (NFC-8436)

Improved health score reporting in V2P Module

Report low traffic / low packet rate interfaces as having health score of 100.

Customer Request/Ticket numbers: NFC-8456

Improved SYN-flood DDoS Attack detection

A number of enhancements were implemented in DDoS detection Module to improve reduction of false positives and increase the number of variations of DDoS attacks.

Customer Request/Ticket numbers: NFC-8320

Improved SSDP Reflection DDoS Attack detection

A number of enhancements were implemented in DDoS detection Module to improve reduction of false positives and increase the number of variations of DDoS attacks.

Customer Request/Ticket numbers: NFC-8381

Improved Visitors by Country Module

Use list of local subnets to determine internal IP addresses and exclude reporting local-to-local traffic.

Customer Request/Ticket numbers: NFC-8264

Added support for IPFIX Private Enterprise Information Elements

NFO IPFIX Original Flow Data processing now has the ability to add and edit key names for any IPFIX field.

Customer Request/Ticket numbers: NFC-8244

Improved usability of Module: SNMP Custom OID Sets Monitor

Customer Request/Ticket numbers: NFC-8092, NFC-8110, NFC-8179, NFC-8202, NFC-8203

Added support for Windows Server 2016

Customer Request/Ticket numbers: NFC-8162

Improve internal process.log format

NFO internal process.log format has been changed: remove units from numeric values.

Customer Request/Ticket numbers: NFC-8414

Added client_ip to login success/fail messages in nf2sl.log

Customer Request/Ticket numbers: NFC-8507/ZEN-572

Build 2.5.0.0.858

Added support for SNMP v3

NFO SNMP service supports now both SNMP v2c and v3. Added ability to create a list of credentials, specifying appropriate authentication information, and allow customers to choose corresponding credential for each network device for SNMP polling.

Customer Request/Ticket numbers: NFC-8023

New Module: SNMP Custom OID Sets

Extended functionality of SNMP Service by allowing users to specify custom OID sets for SNMP polling.

Customer Request/Ticket numbers: NFC-7723, NFC-8050, NFC-5308, NFC-8190, NFC-8201

Added support for IPv6 in DNS service

NFO now supports IPv6 in the FQDN service

Customer Request/Ticket numbers: NFC-5393

Enhance DNS service

Implemented IP-Name mapping list in FQDN Service. Enable customers to create IPv4 and IPv6 known host name lists. These lists are used by NFO prior to calling DNS service allowing to override (or set) customer specific name resolutions.

Customer Request/Ticket numbers: NFC-5766

Enhance NFO output throttling

Added support for throttling rate parameter to server.cfg file.

Customer Request/Ticket numbers: NFC-7424

New Module: Custom Threat List Monitor

This Module enables NFO administrator to setup unlimited number of Custom Security Threat lists. These lists could be public as well as private.

Customer Request/Ticket numbers: NFC-8026, NFC-8165, NFC-8172, and NFC-8205

Added support for NFv9 and IPFIX in Network Health Monitor Module

Added support for new fields for TCP flags in NFv9 and IPFIX.

Customer Request/Ticket numbers: NFC-8019

Added “Clone AD entry” function when setting X509 Authentication

Customer Request/Ticket numbers: NFC-8039

Added support for Linux with systemd

NFO installation package now supports Linux systemd.

Customer Request/Ticket numbers: NFC-6026

Added support for Oracle Enterprise Linux

Customer Request/Ticket numbers: NFC-8226

Implement New IPFIX Entities (Element ID: 430 through 470)

Implement the latest IPFIX standard Entities - See https://www.iana.org/assignments/ipfix/ipfix.xhtml for details.

Customer Request/Ticket numbers: NFC-7986

Enhanced NFO watchlist maintenance

Added support for comments in CSV files. Added support for 'Comment' column in watchlist parameters

Customer Request/Ticket numbers: NFC-6744, NFC-8017

Implemented NetFlow deduplication

Implemented deduplication in Top Traffic Monitor Modules: 10063 – Top Connections Monitor, 10067 – Top Traffic Monitor, and 10068 – Top Packets Monitor

Customer Request/Ticket numbers: NFC-8025

Make TCP flags field Splunk CIM compliant

Customer Request/Ticket numbers: NFC-8005

Implement New Cisco ASA NSEL Templates

Implement support for new Cisco ASA NSEL templates in all Modules, including Cisco ASA Modules.

Customer Request/Ticket numbers: NFC-8057

Module: V2P Network Visibility – Enhancements and bug fixes

This Module correlates virtual overlay network and underlying physical network and virtual network operators to identify physical network devices impacting VM Applications performance. In this release we improved integration with VMware vCenter.

Customer Request/Ticket numbers: NFC-7980

Enhanced DDoS detection algorithms

A number of enhancements were implemented in DDoS detection Module to improve reduction of false positives and increase the number of variations of DDoS attacks.

Customer Request/Ticket numbers: NFC-8035

What's Been Fixed in this Release

Build 2.5.1.4.10

NetFlow/IPFIX Template conflict after network device reconfiguration

This issue occurs in case when NetFlow device sends one template and then later sends another template with the same ID and fingerprint. This could happen after network device reconfiguration.

Customer Request/Ticket numbers: NFC-8166

Some Citrix Netscaler enterprise IPFIX fields lead to server crash on Windows platform

This issue occurs only on Windows.

Customer Request/Ticket numbers: NFC-8689

Build 2.5.1.0.43

Fix syslog format to meet RFC-3164

NFO syslogs do not meet RFC-3164 requirements. Implement HOSTNAME field to follow TIMESTAMP field.

Customer Request/Ticket numbers: NFC-3494

Remove unwanted error logs when External Data Feeder is restarted

When External Data Feeder is restarted, the following ERROR appears in nf2sl.log file:
2018-01-05 13:07:59,380 ERROR [JSR356Endpoint]
NFO and External Data Feeder are working just fine. This error is removed to avoid unnecessary warnings.

Customer Request/Ticket numbers: NFC-8362, ZEN-560

Top Traffic Monitor Module (10067) produces no output when Top N is set to 0 and deduplication is enabled

Customer Request/Ticket numbers: NFC-8325

Various bug fixes

Customer Request/Ticket numbers: NFC-3349, NFC-3604, NFC-4863, NFC-5332, NFC-5871, NFC-6058, NFC-6315, NFC-6540, NFC-7076, NFC-7836, NFC-7863, NFC-7879, NFC-7882, NFC-7886, NFC-7978, NFC-8014, NFC-8299, NFC-8357, NFC-8422, NFC-8439, NFC-8486

Build 2.5.0.0.858

NFO crashes when over 500 devices send flows to a single NFO instance

NFC crashes when over 500 network devices were configured to send NFv9 with multiple templates each.

Customer Request/Ticket numbers: NFC-8143

NFO drops UDP packets when padded with zeros

When NFO validates flows and determines that packet is padded with zeros after the last record it drops the entire packet. The fix is to ignore padding zeros and process good flow records.

Customer Request/Ticket numbers: NFC-8231

V2P Network Visibility Module – vCenter integration bug

V2P Network Visibility Module is unable to build watchlist when two VMs with the same IP address are present in two different vCenters.

Customer Request/Ticket numbers: NFC-8058

Fix bug in processing Viptela IPFIX templates

Customer Request/Ticket numbers: NFC-7992

V2P Network Visibility Module – memory leak

Customer Request/Ticket numbers: NFC-8103

Memory leak when processing Cisco ASA 9.1(7) NSEL templates

Customer Request/Ticket numbers: NFC-8077

Known Issues

Memory Leak after Known malicious hosts list has been updated

Affected Platforms: All

Description: When known malicious hosts list is updated manually or via Updater, about 19MB of memory is not released.

Customer Request/Ticket numbers: NFC-7023

Workaround: NFI should restart automatically. Restart manually if unexpected behavior is observed.

Dashboard: statistics logging interval not displayed

Affected Platforms: All

Description: Changing statistics logging interval, when changing the statistics-logging interval the statistics may not display based on the new value.

Customer Request/Ticket numbers: NFC-2092

Workaround: Reset the statistics to the default of 10 seconds using the reset option.

[Module 10103] Output produces separate syslog with non-table values when module is polling table data and scalar (non-table) data configured in the same OID set

Affected Platforms: All

Customer Request/Ticket numbers: NFC-8466

Workaround: None

The Windows Filtering Platform prevents NFO Controller from a bind to a local port at some point on Windows Server 2016 platform

Affected Platforms: Windows 7/10, Windows Server 2012/2016

Description: When a block of a bind to a local port happens, NFO Controller warns on Status page that NFO Sever is unavailable and restarts it

Customer Request/Ticket numbers: NFC-8505

Workaround: Client port ranges can be changed: https://support.microsoft.com/en-us/help/929851/the-default-dynamic-port-range-for-tcp-ip-has-changed-in-windows-vista.

Use the following commands:

```
netsh int ipv4 show dynamicport tcp
```
It should display default values: start port 49152 and the number of ports 16384.

```
netsh int ipv4 set dynamicport tcp start=49152 num=12000
```
The number of ports should be changed to 12000. To make sure of it, repeat the first command once again.