NetFlow Optimizer™

Release Notes

Version 2.4.9 (Build 2.4.9.0.3)

May 2017

Contents

What's New in this Release

Build 2.4.9.0.3

Change default URL for Dshield Threat List

Change External Data Feeder agent URLs:

- Threat Feeds addresses to https://secure.dshield.org/feeds/suspiciousdomains_High.txt
- Threat Feeds IP blocks to https://feeds.dshield.org/block.txt

Add certificate into JRE truststore.

Customer Request/Ticket numbers: NFC-7923, ZEN-525

Password Policy

Implement password policy as follows:

- Be at least eight characters in length
- Contain characters from all of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)

Customer Request/Ticket numbers: NFC-7925

Improve Visitors by Country (GeoIP) Module (10040)

Introduce Top N, Set default local subnets, allow to optionally suppress reporting local traffic

Customer Request/Ticket numbers: NFC-7899, ZEN-532

Improve information in NFO internal logs

Add more details in logs such as OS, processor, network, libc version, etc.

Customer Request/Ticket numbers: NFC-7845

Improve accuracy of r_load and r_rate in V2P Network Visibility Module (10180)

V2P Network Visbility is a new name for NFO Logic Module, formerly known as NetOps. It provides complete visibility between the virtual overlay and physical networking layers. In this release we improved the algorithm that calculates network device interfaces health and risk, and report r_load and r_load with 3 decimals.

Customer Request/Ticket numbers: NFC-7897

Build 2.4.8.0.2

Introduce two factor authentication (2FA)

Two Factor Authentication (2FA) functionality enables organizations with certificate policies to restrict access to NetFlow Optimizer GUI for configuration. This functionality, together with AD integration, ensures that only users with valid certificate from a designated user group have access to NFO.

Customer Request/Ticket numbers: NFC-7561

NFv9/IPFIX Template persistence improvements

Several improvements in usability and performance of Template persistence functionality.

Customer Request/Ticket numbers: NFC-7747, NFC-7812

Log enhancements in Windows platform

Implement --StdOutput and –StdError in Windows version of NFO for Tomcat's logging.

Customer Request/Ticket numbers: NFC-7809

NFO virtual appliance enhancements

Implement additional parameters in NFO virtual appliance: Domain and Search Path (Domain Suffix).

Customer Request/Ticket numbers: NFC-7810

Build 2.4.7.0.23

NFv9/IPFIX Template persistence

NFO cannot process incoming NFv9/IPFIX traffic unless it receives required templates from the exporters. As a result the incoming NF records are dropped. This behavior is tolerable at a very first run but it is undesirable after subsequent NFO server restarts.

NFO server collects unique templates along with the templates origins and periodically saves them in configuration DB. Upon a restart NFO reads saved templates, thus enabling processing of relevant flows without waiting for templates to be sent by exporters.

Customer Request/Ticket numbers: NFC-4114

Tomcat 8 migration

Implement NFO and NFO Updater to be based on Tomcat 8. Implement upgrade process from Tomcat 7 to Tomcat 8.

Customer Request/Ticket numbers: NFC-7523

NFO Memory usage

Implement NFO [controller] memory usage improvements.

Customer Request/Ticket numbers: NFC-7563

Add Cisco AVC support to Security Ruleset

Implement support for Cisco AVC IPFIX templates in Module 10040: Visitors by Country, and in Security Modules 10050/52/53.

Customer Request/Ticket numbers: NFC-7578

Implement server.log Rotation

Implement rotation of server.log. New file name has a timestamp, and it is subject to rotation rules.

Customer Request/Ticket numbers: NFC-7617, NFC-7618

Improve java memory usage

Improve java memory usage. Java heap size parameter “-Xmx3g” is sufficient now.

Customer Request/Ticket numbers: NFC-7634, ZEN-465, ZEN-524

Allow non root user accessing Updater log files

Non-root user cat read Server and Controller log files but not the Updater logs. Change permissions so it can be read by non-root user.

Customer Request/Ticket numbers: NFC-7573

What's Been Fixed in this Release

Build 2.4.9.0.3

BUG in reporting snmp_index in NetOps Module (10180)

Intermittent problem in Module 10180 (Network Operations Analytics): reporting wrong snmp_index in syslog with nfc_id=20181.

Customer Request/Ticket numbers: NFC-6866

⚠ Security update: Disable HTML5 Cross-Origin Resource Sharing

Disable CORS (add tomcat filter).

Customer Request/Ticket numbers: NFC-7928

⚠ Security update: Change Server HTTP header name

Change Apache tomcat server http header to "NFOWebServer".

Customer Request/Ticket numbers: NFC-7931

LDAP queries all domain controllers

LDAP queries all domain controllers on failed authentication call to Active Directory. Stop authentication, when invalid credentials or locked account is detected.

Customer Request/Ticket numbers: NFC-7945, ZEN-534

Warning message when Updater reconnects

Description: When connection between Updater and NFO is lost and Updater reconnects, incorrect warning "*WARNING #409: There are 2 updaters connected to the NetFlow Optimizer with the same UID*" is given.

Customer Request/Ticket numbers: NFC-7839

Build 2.4.8.1.3

⚠ Security update: Cross-Site scripting vulnerability

Fixed XSS vulnerability.

Customer Request/Ticket numbers: NFC-7880, ZEN-521

Intermittent Repeater issue: stop output

Intermittent issue – about once a day Repeater stops sending data and NFO is restarted.

Customer Request/Ticket numbers: NFC-7849, ZEN-515

Build 2.4.8.0.2

Unable to load vCenter parameters after upgrading

Failure to load vCenter integration watchlist parameters in Modules 10180 (Network Operations Analytics) and 10264 (Microsegmentation Analytics).

Customer Request/Ticket numbers: NFC-7825

Known Issues

Corrupted password when x509 is edited in two tabs. Unclear message

Affected Platforms: All

Description: When admin edits x509 in two separate browser sessions (tabs), AD service account password could be corrupted. This results in inability of users with 2FA to login to NetFlow Optimizer. Logs (nf2sl.log) and Status page messages have the following message:

```
2017-04-27 12:56:59 WARNING #500 AD ldap://<domain>:389, LDAP error:
user@<domain>.com, javax.naming.NamingException: [LDAP: error code 1 - 000004DC:
LdapErr: DSID-0C090752, comment: In order to perform this operation a successful bind
must be completed on the connect...
```

Customer Request/Ticket numbers: NFC-7971

Workaround: Login as admin and re-enter x509 AD service account password

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.