NetFlow-based DDoS Detection

Solution Guide

Build 2.5.1.0

June 2018

Contents

Introduction

Distributed denial-of-service (DDoS) Detection solution developed by NetFlow Logic brings new early warning alerting capabilities allowing to stop DDoS attack before targeted network devices and servers are incapacitated.

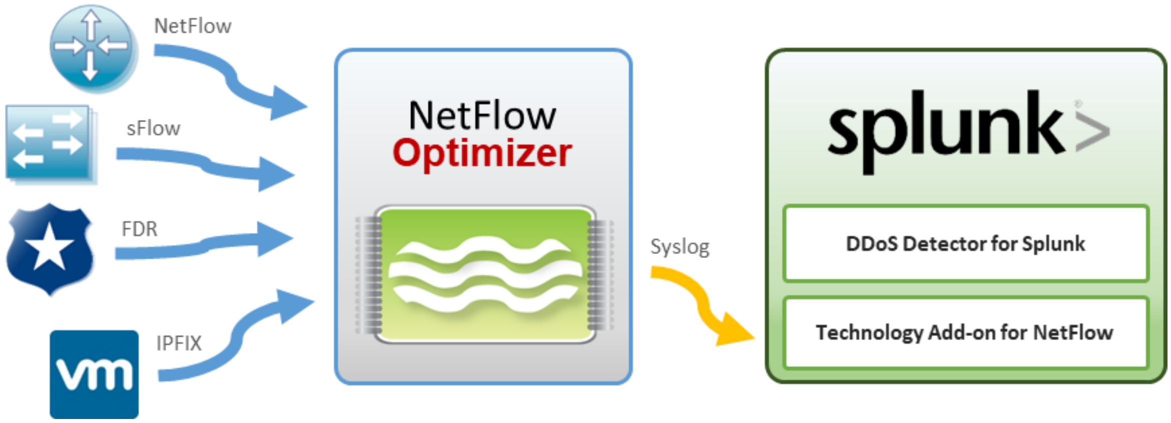
DDoS attacks are notoriously difficult to detect timely and defend against. Traditional perimeter based technologies such as firewalls and intrusion detection systems (IDSs) do not provide comprehensive DDoS protection. Solutions positioned inline must be deployed at each endpoint, and are vulnerable in case of a volumetric attack. Typically, solutions require systems to run in "learning" mode, passively monitoring traffic patterns to understand normal behavior and establish a baseline profile. The baseline is later used to detect anomalous network activity, which could be a DDoS attack. These takes a long time to implement and any change in the infrastructure makes baseline obsolete, and results in lots of false positives.

In contrast to the inline solutions, NetFlow Logic's DDoS Detector is based on the network flow information analysis, thus it is not susceptible to volumetric flood attacks. Also, it does not rely on baseline data collection, which may take days or weeks to establish. Instead, NetFlow Logic's DDoS detection solution uses an innovative approach which makes it operational in 15-20 minutes after deployment.

The NetFlow Logic's solution is based on advanced statistical and machine learning methods and consists of several components each analyzing network metadata from a different perspective. Results of the analysis are combined and a final event reporting decision is made. The objective of such "collective mind" approach is false positives reduction.

The core of NetFlow Logic's solution is NetFlow Optimizer™ (NFO) and DDoS Detector NFO Module.

The core of the solution is NetFlow Optimizer™ (NFO), a processing engine for the network flow data (NetFlow, IPFIX, sFlow, etc.) with enabled DDoS Detector NFO Module.



NetFlow Optimizer accepts network flow data from network devices (routers, switches, firewalls), applies analytical algorithms to the data to address various use cases, converts the processed data to syslog, then sends that processed information to Splunk for visualization and alerting.

Solution Components

Component	Platforms	Description
NetFlow Optimizer (NFO) RLS 2.5.1.0	Linux or Windows	This is a processing engine for various formats of flow data: NetFlow, IPFIX, sFlow, J-Flow, etc. Available for Windows, Linux, or as Virtual Appliance. Downloadable from NetFlow Logic's web site – www.netflowlogic.com/download/
DDoS Detector (NFO Module)	NetFlow Optimizer 2.5.1.0	NetFlow Optimizer Module. This component contains analytics for the solutions. Select Windows or Linux version to match your NFO platform. Upload the zip file **ddos_detector-2.5.1.0.x-<platform>-x86_64** into NFO. Downloadable from NetFlow Logic's web site – www.netflowlogic.com/download/
DDoS Detector for Splunk App	Splunk App (dashboards and alerts)	Download from Splunkbase: https://splunkbase.splunk.com/app/4016/

NetFlow Optimizer

Agentless Deployment

A single instance of NFO, deployed in a data center, is capable of processing and analyzing massive volumes of network metadata. It is easy to deploy and configure and can be operational in 15 minutes after the installation. NFO does not rely on multiple agents as some of its competitors and does not affect other network security tools that you may already have in place.

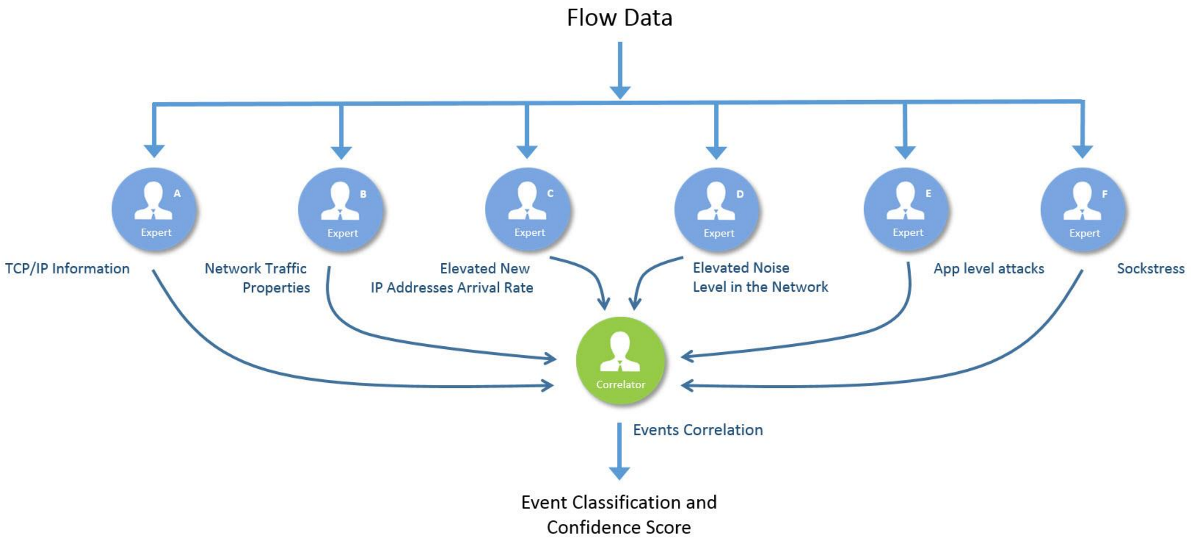
Select and configure your flow-reporting network devices to send NetFlow/sFlow/J-Flow/IPFIX to NetFlow Optimizer.

Configuration

NetFlow Optimizer installers are available for Windows and Linux, or as a Virtual Appliance. When installed, NFO is automatically configured to listen to flow data on UDP port 9995. You can change this port and/or add additional ports to receive flows from your network flow generating devices. You also need to configure NetFlow Optimizer output to report network traffic anomalies. Specify the IP address and port of your alerting system (e.g. SIEM) which will receive alert messages and supporting information for the detected DDoS attacks. Please refer to **NetFlow Optimizer Installation and Administration Guide** for additional details.

DDoS Detector Module

This Module consists of six independent components, which we call **experts**, each specializing in its own domain of knowledge. All experts process all the flow records received by NetFlow Optimizer, apply their own analytics, and, if an attack is detected, send messages to the **events correlator**, indicating the type of detected attack, confidence level, and a trend of the event characteristics dynamics (increasing, steady, or abating). The event correlator combines the information received from the experts, assigns weight to each reported event, and makes a final determination on reporting and its confidence in event validity.


Flow Data
A
Expert
B
Expert
C
Expert
D
Expert
E
Expert
F
Expert
TCP/IP Information
Network Traffic Properties
Elevated New IP Addresses Arrival Rate
Elevated Noise Level in the Network
App level attacks
Sockstress
Correlator
Events Correlation
Event Classification and Confidence Score

TCP/IP Information Monitor

This expert is designed for detecting types of attacks that abuse the TCP/IP protocol by taking advantage of some of its weaknesses. TCP/IP is a connection-based protocol. The sender must establish a connection with his or her peer before sending any data packets. TCP/IP relies on a three-way handshake mechanism (SYN, SYN-ACK, ACK) where every request creates a half-open connection (SYN), a request for a reply (SYN-ACK), and then an acknowledgement of the reply (ACK). Attacks attempting to abuse the TCP/IP protocol will often send TCP packets in the wrong order or with wrong TCP flags, causing the target server to hold an increasing number of half-open connections and eventually running out computing resources.

This expert assesses flow information for the signs of the SYN flood, the reflected SYN-ACK, ACK flood, and PSH + ACK attacks.

Network Traffic Properties Monitor

This expert is designed to monitor various traffic metrics for each of the major protocols - TCP, UDP, and ICMP. It looks for changes in traffic rate, packet rate, flow rate, and average flow duration. This expert detects and reports abnormal changes in all four traffic characteristics by each protocol.

New IP Addresses Arrival Rate Monitor

Detecting bandwidth attacks could be particularly difficult when the attack is highly distributed, since the attack traffic from each source may be small compared to the normal background traffic. One of a better indicators of a highly distributed attack is increase in the number of external source IP addresses observed on the victim network.

Changes in the network’s IP addresses composition are tracked by a dedicated expert. This expert is capable of distinguishing attack patterns from the “flash mob” events – a significant increase in the network’s IP addresses composition due to a legitimate event such as a sale promotion which attracted an unusually large number of customers.

Noise Level in the Network Monitor

Another indication of a DDoS attack is a sudden appearance of many hosts which send one or two packets and go away. Such hosts’ behavior may be described as noise in the network environment. A dedicated level tracks noise level in a network and raises an alert when the level becomes excessively high.

Application Protocol Level Attack

The application layer attacks usually have nothing to do with overwhelming bandwidth, and are different from common volumetric attacks. Sometimes they are called “low and slow” as they target flaws and limitations of applications. This expert is designed for detecting network hosts which send abnormal number of application level protocol requests to a selected group of servers (e.g. Web Servers, DNS Servers).

Sockstress Attack

Sockstress is an attack that exploits vulnerable feature in the TCP protocol stack implementation. The attacker forces the server to maintain an idle connection by setting the size of the TCP window (TCP window is a buffer that stores the received data before uploading it to the application layer) to 0 bytes soon after a connection is established. This indicates that there is no more room in that buffer on the client side, and it causes the server to send Window Zero Probe (ZWP) packets to the client continually to see when it can accept new information. Because the attacker does not change the window size the connection is kept open indefinitely.

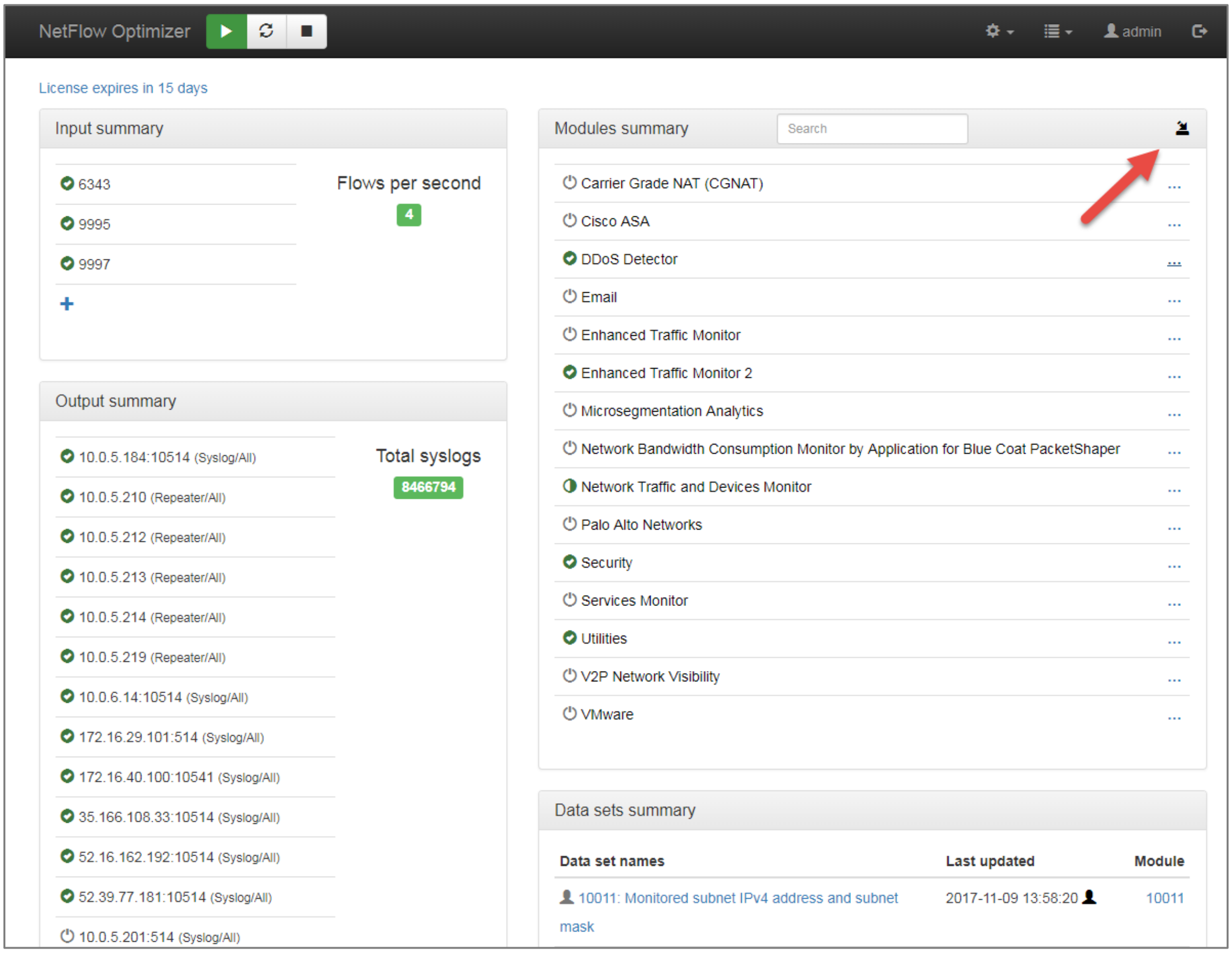
By opening many connections like this to a server, the attacker consumes all of the resources in the server, preventing legitimate users from establishing new connections or causing the server to crash.

Events Correlator

The events correlator receives messages from the experts containing information about the corresponding events and makes a decision about reporting a DDoS attack based on the latest received expert's message and earlier messages received from same or other experts. When reporting a DDoS attack the events correlator classifies the event according to information received from the contributing experts.

Module Installation

The Module should be uploaded into NFO and enabled. In NetFlow Optimizer Home page click on upload button, and select the package to upload (e.g. ddos_detector-2.5.1.0.40-linux-x86_64.zip).



License expires in 15 days

Input summary

- ✓ 6343
- ✓ 9995
- ✓ 9997
- +

Flows per second 4

Output summary

- ✓ 10.0.5.184:10514 (Syslog/All)
- ✓ 10.0.5.210 (Repeater/All)
- ✓ 10.0.5.212 (Repeater/All)
- ✓ 10.0.5.213 (Repeater/All)
- ✓ 10.0.5.214 (Repeater/All)
- ✓ 10.0.5.219 (Repeater/All)
- ✓ 10.0.6.14:10514 (Syslog/All)
- ✓ 172.16.29.101:514 (Syslog/All)
- ✓ 172.16.40.100:10541 (Syslog/All)
- ✓ 35.166.108.33:10514 (Syslog/All)
- ✓ 52.16.162.192:10514 (Syslog/All)
- ✓ 52.39.77.181:10514 (Syslog/All)
- ⏻ 10.0.5.201:514 (Syslog/All)

Total syslogs 8466794

Modules summary

- ⏻ Carrier Grade NAT (CGNAT) ...
- ⏻ Cisco ASA ...
- ✓ DDoS Detector ...
- ⏻ Email ...
- ⏻ Enhanced Traffic Monitor ...
- ✓ Enhanced Traffic Monitor 2 ...
- ⏻ Microsegmentation Analytics ...
- ⏻ Network Bandwidth Consumption Monitor by Application for Blue Coat PacketShaper ...
- ◑ Network Traffic and Devices Monitor ...
- ⏻ Palo Alto Networks ...
- ✓ Security ...
- ⏻ Services Monitor ...
- ✓ Utilities ...
- ⏻ V2P Network Visibility ...
- ⏻ VMware ...

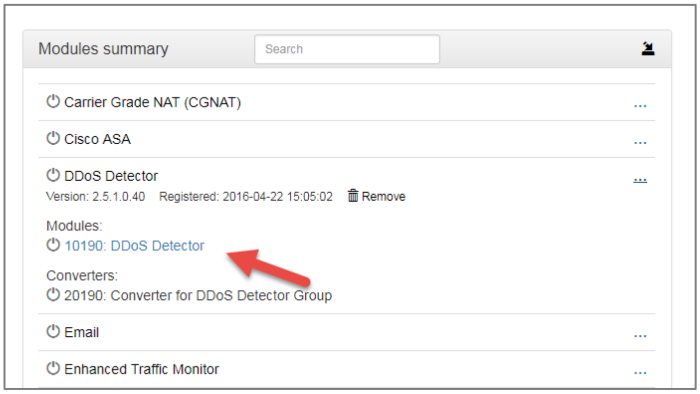
Data sets summary

Data set names	Last updated	Module
10011: Monitored subnet IPv4 address and subnet mask	2017-11-09 13:58:20	10011

Once uploaded, click on ⏻ to enable the DDoS Detector Module. You don't have to restart the server – the Module is operational when enabled.

Module Configuration

The Module is highly configurable. Click on DDoS Detector.



Modules summary

Carrier Grade NAT (CGNAT)

Cisco ASA

DDoS Detector
Version: 2.5.1.0.40 Registered: 2016-04-22 15:05:02 Remove

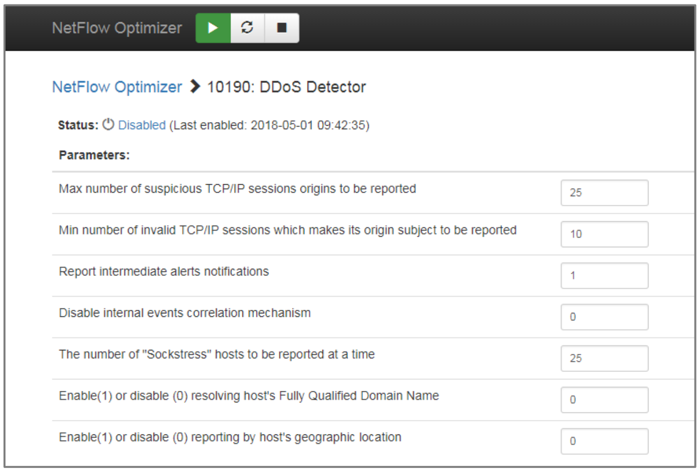
Modules:
10190: DDoS Detector

Converters:
20190: Converter for DDoS Detector Group

Email

Enhanced Traffic Monitor

You will be presented with the following screen.



NetFlow Optimizer > 10190: DDoS Detector

Status: Disabled (Last enabled: 2018-05-01 09:42:35)

Parameters:

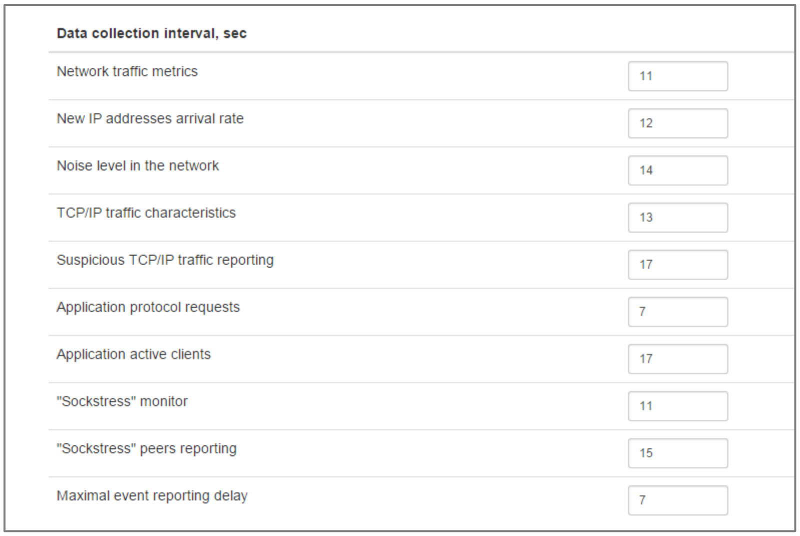
Max number of suspicious TCP/IP sessions origins to be reported	25
Min number of invalid TCP/IP sessions which makes its origin subject to be reported	10
Report intermediate alerts notifications	1
Disable internal events correlation mechanism	0
The number of "Sockstress" hosts to be reported at a time	25
Enable(1) or disable (0) resolving host's Fully Qualified Domain Name	0
Enable(1) or disable (0) reporting by host's geographic location	0

Change configuration parameters as desired and press the <Save> button. You don’t need to restart NetFlow Optimizer nor enable/disable the Module in order for the new parameters to take effect.

Parameter	Description
Max number of suspicious TCP/IP sessions origins to be reported	Maximum number of TCP/IP sessions reported by the following experts: TCP/IP Information, Network Traffic Properties, Application Protocol Level Attack (min = 0, max = 10000, default: 25)
Min number of invalid TCP/IP sessions which makes its origin subject to be reported	Minimum number of invalid TCP/IP sessions that triggers reporting by TCP/IP Information expert (min = 1, max = 100, default = 10)
Report intermediate alerts notifications	1 – report intermediate alerts notifications, 0 – do not report intermediate alerts notifications (default = 1)

Parameter	Description
Disable internal events correlation mechanism	1 – disable internal event correlator, 0 – enable internal event correlator (default = 0)
The number of "Sockstress" hosts to be reported at a time	The number of "Sockstress" hosts to be reported by Sockstress Attack expert (min = 0, max = 10000, default = 25)
Enable(1) or disable (0) resolving host's Fully Qualified Domain Name	1 – enable DNS host name resolution, 0 – disable DNS host name resolution (default = 0)
Enable(1) or disable (0) reporting by host's geographic location	1 – enable GeoIP enrichment, 0 – disable GeoIP enrichment (default = 0)

This section contains d**ata collection intervals** for various attack type.



Data collection interval, sec

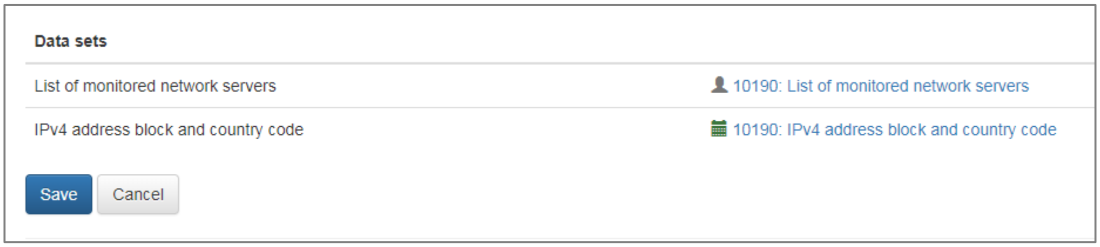
Network traffic metrics	11
New IP addresses arrival rate	12
Noise level in the network	14
TCP/IP traffic characteristics	13
Suspicious TCP/IP traffic reporting	17
Application protocol requests	7
Application active clients	17
"Sockstress" monitor	11
"Sockstress" peers reporting	15
Maximal event reporting delay	7

⚠ Please contact NetFlow Logic support before changing Data collection intervals.

Data Collection Interval	Description
Network traffic metrics	Time interval between two successive invocations of the network traffic analysis mechanism, in seconds
New IP addresses arrival rate	Time interval between two successive invocations of the IP addresses composition mechanism, in seconds
Noise level in the network	Time interval between two successive invocations of the noise level in the network tracker, in seconds
TCP/IP traffic characteristics	Time interval between two successive invocations of the TCP/IP traffic monitor, in seconds

Data Collection Interval	Description
Suspicious TCP/IP traffic reporting	Time interval between two successive invocations of the TCP/IP traffic monitor reporting function, in seconds
Application protocol requests	Time interval between two successive invocations of the Application Protocol Level Attack expert
Application active clients	Time interval between two successive invocations of the reporting of Application Protocol Level Attack sources
"Sockstress" monitor	Time interval between two successive invocations of the Sockstress Attack expert
"Sockstress" peers reporting	Time interval between two successive invocations of the reporting of Sockstress Attack sources
Maximal event reporting delay	Maximal time between event detection and reporting to external system, in seconds

This section contains Module Configuration Data set



Data sets

List of monitored network servers	10190: List of monitored network servers
IPv4 address block and country code	10190: IPv4 address block and country code

Specify the data set parameters.

Data set	Description
List of monitored network servers	This is the list of applications you want to protect against application level attacks. It should be specified in the following format: [IPv4 Address],[Port],[IP Protocol],[Protocol name] For example: 10.10.20.11,80,6,HTTP
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

DDoS Detector for Splunk App

Overview

DDoS Detector for Splunk App (“App”) provides alerting and visualization capabilities for events detected and reported to Splunk by NetFlow Optimizer’s DDoS Detector Module. The operators benefit from being able to address traffic anomalies and DDoS attacks before network devices and servers targeted by DDoS are incapacitated.

Use this App to setup and receive email alerts within minutes after a DDoS attack is detected. Select the detection confidence level for notifications to reduce false positives. View details of the anomaly, and/or browse through the history of detected attacks, searching for common origins and victims.

Installation

The DDoS Detector for Splunk App and Technology Add-on for NetFlow are designed to work together.

Download

- DDoS Detector for Splunk App <link>
- Technology Add-on for NetFlow https://splunkbase.splunk.com/app/1838/

Where to install

Install DDoS Detector Splunk App and Technology Add-on for NetFlow.

Splunk Node	What to install
Search Head	Add-on and App
Indexer	Add-on only
Heavy Forwarder	Add-on only
Universal Forwarder	None

Post Installation Steps

Create a data input

Use the GUI to create a Data Input, or create it in `inputs.conf` using the CLI. Make sure sourcetype is set to `flowintegrator`.

GUI

- In the top right corner, click **Settings -> Data inputs**
- In the row for UDP click **Add new**
- Enter a port number and click **Next**
- Click **Select Sourcetype** and type **flowintegrator**
- Change the App Context to the **Technology Add-on for NetFlow (TA-netflow)**
- Set any other settings such as Method or Index as appropriate for your environment
- Click **Review**, followed by **Submit**

CLI

Create the inputs.conf in the correct directory: $SPLUNK_HOME/etc/apps/TA-netflow/local/inputs.conf

Add the following lines to the inputs.conf file. This examples uses the syslog port UDP 10514. Change the port as needed:

```
    [udp://10514]
    sourcetype = flowintegrator
```

By default NetFlow Optimizer events will be stored in main index. In case you want to use another index, for example `flowintegrator`, please create the $SPLUNK_ROOT/etc/apps/TA-netflow/local/indexes.conf file, and add the following lines to it:

```
   [flowintegrator]
    homePath    = $SPLUNK_DB/flowintegrator/nfi_traffic/db
    coldPath    = $SPLUNK_DB/flowintegrator/nfi_traffic/colddb
    thawedPath  = $SPLUNK_DB/flowintegrator/thaweddb
```

In that case make sure your $SPLUNK_ROOT/etc/apps/TA-netflow/local/inputs.conf file contains the following:

```
    [udp://10514]
    sourcetype = flowintegrator
    index = flowintegrator
```

Verify the configuration

To test that NFO syslogs reached Splunk, go to default Search App, and type:

```
index=flowintegrator sourcetype=flowintegrator
```

If Splunk is getting the syslogs from NFO, then you’ll see events show up here.

Setting up Local subnets

The App relies on the list of local subnets to determine inbound / outbound traffic and attackers and victims location. Default **my-subnets.csv** file is located here:

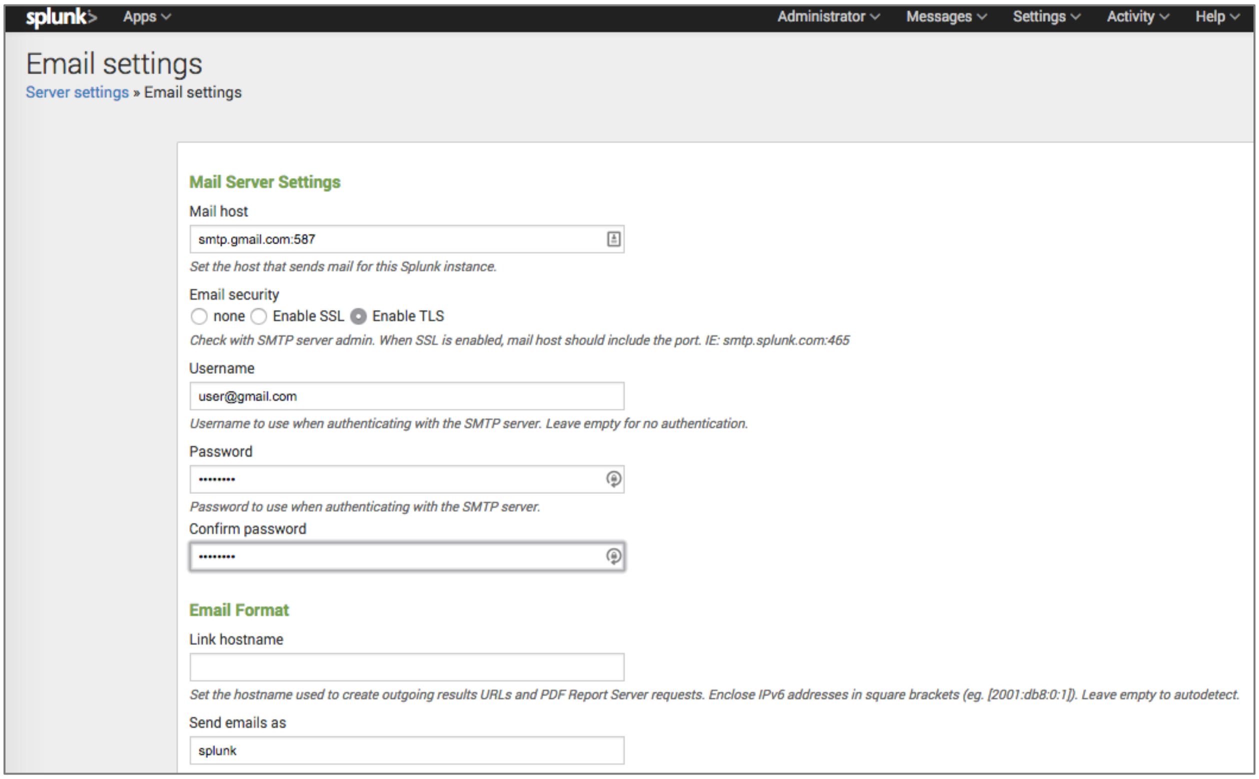
$SPLUNK_ROOT /etc/apps/ddos_detector/lookups

and contains the following:

```
subnet,description
10.0.0.0/8,ClassA
172.16.0.0/12,ClassB
192.168.0.0/16,ClassC
```

Please modify **my-subnets.csv** lookup file to match your environment.

Setting Email Alerting



Email settings

Server settings » Email settings

Mail Server Settings

Mail host

smtp.gmail.com:587

Set the host that sends mail for this Splunk instance.

Email security

○ none ○ Enable SSL ● Enable TLS

Check with SMTP server admin. When SSL is enabled, mail host should include the port. IE: smtp.splunk.com:465

Username

user@gmail.com

Username to use when authenticating with the SMTP server. Leave empty for no authentication.

Password

••••••••

Password to use when authenticating with the SMTP server.

Confirm password

••••••••

Email Format

Link hostname

Set the hostname used to create outgoing results URLs and PDF Report Server requests. Enclose IPv6 addresses in square brackets (eg. [2001:db8:0:1]). Leave empty to autodetect.

Send emails as

splunk

As the first step, if not already done, the outbound email server settings needs to be configured. It could be an internal email server or external mail service (Gmail for example).

Gmail configuration is shown below.

```
Mail host = smtp.gmail.com:587
Email security = TLS
Username = <YOUR_GMAIL_ADDRESS>
Password = <YOUR_GMAIL_PASSWORD>
```

After filling in the details in the “Mail Server Settings”, also the Link hostname should be configured in the “Email format” section.. Use the following format: **https://hostname:port_number** (example: https://mysplunk.com:8000). Don’t leave it blank for autodetect -- it may not work. This value is later used in the email alert to create a clickable link.

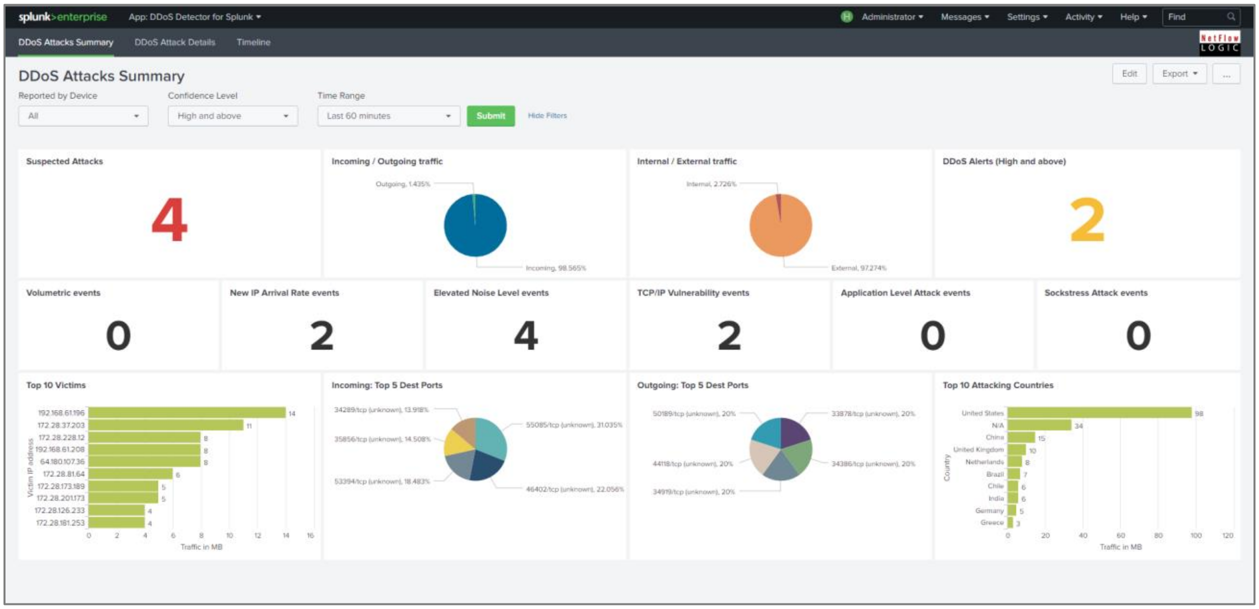
The DDoS email notifications recipients list is empty by default. See Alerts section with details how to set up alerts parameters.

Please, note, that if you change anything on this configuration page, you must also erase and re-enter the "Password" and "Confirm password" fields. Otherwise the password will be reset and no email notifications will be sent.

DDoS Detector App Dashboards

DDoS Attacks Summary

This dashboard shows detected DDoS attacks summary for the selected confidence level and time range. It breaks down the number of attacks by type, as well as top victims and top attacking countries.



DDoS Attacks Summary

Reported by Device: All

Confidence Level: High and above

Time Range: Last 60 minutes

Suspected Attacks: 4

Incoming / Outgoing traffic

Internal / External traffic

DDoS Alerts (High and above): 2

Volumetric events: 0

New IP Arrival Rate events: 2

Elevated Noise Level events: 4

TCP/IP Vulnerability events: 2

Application Level Attack events: 0

Sockstress Attack events: 0

Top 10 Victims

Incoming: Top 5 Dest Ports

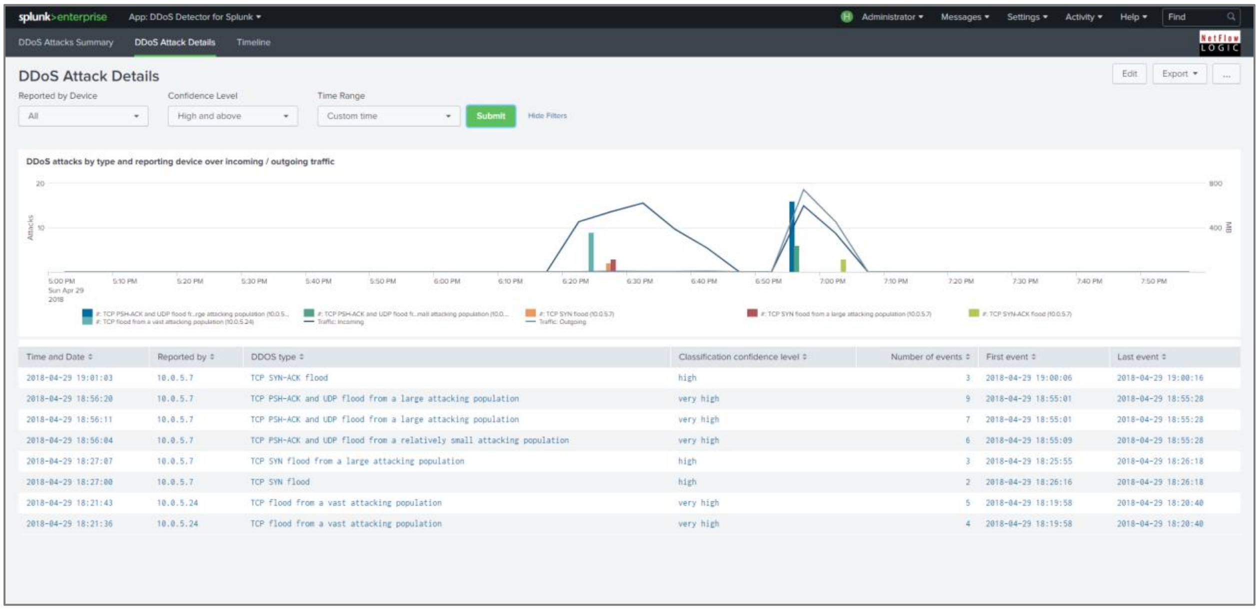
34289/tcp (unknown), 13.918%
35856/tcp (unknown), 14.508%
53394/tcp (unknown), 18.483%
55085/tcp (unknown), 31.035%
46402/tcp (unknown), 22.056%

Outgoing: Top 5 Dest Ports

Top 10 Attacking Countries

DDoS Attacks Details

This dashboard shows detected DDoS attacks details indicating when attacks occurred, traffic in and out of your datacenter before and during the attacks, as well as details on attack types. Attack type is one of 31 basic types, or a combination of them. The list of basic attack types could be found in *Appendix 1 - Basic DDoS Attack* Types on page 15.



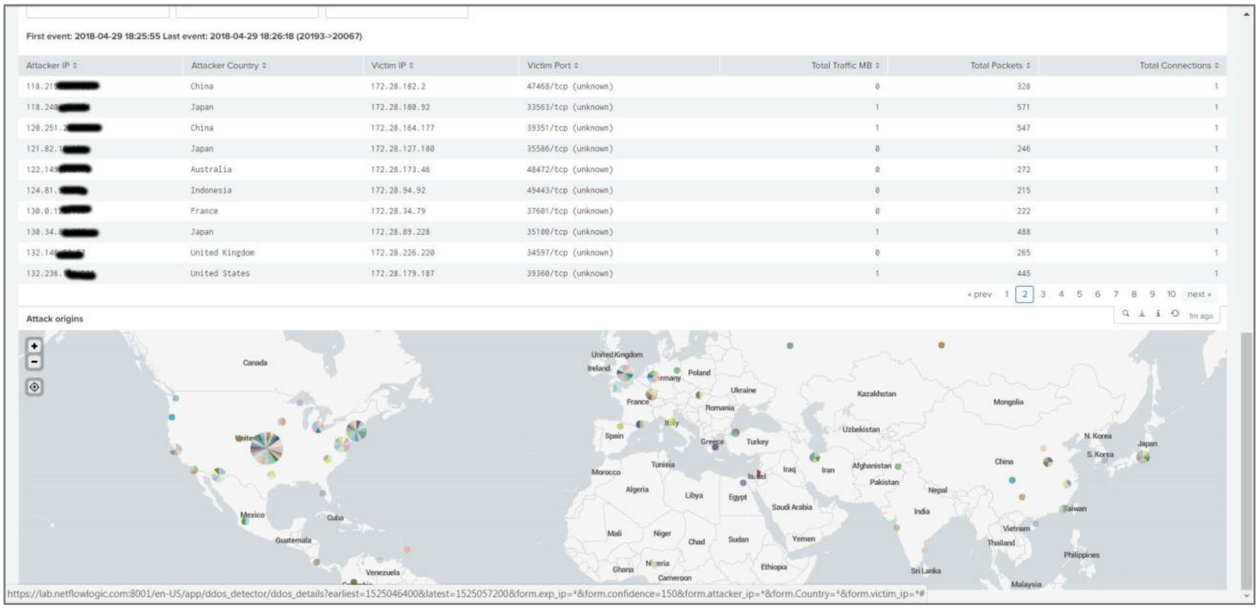
DDoS Attack Details

Reported by Device: All
Confidence Level: High and above
Time Range: Custom time

DDoS attacks by type and reporting device over incoming / outgoing traffic

Time and Date	Reported by	DDOS type	Classification confidence level	Number of events	First event	Last event
2018-04-29 19:01:03	10.0.5.7	TCP SYN-ACK flood	high	3	2018-04-29 19:00:06	2018-04-29 19:00:16
2018-04-29 18:56:20	10.0.5.7	TCP PSH-ACK and UDP flood from a large attacking population	very high	9	2018-04-29 18:55:01	2018-04-29 18:55:28
2018-04-29 18:56:11	10.0.5.7	TCP PSH-ACK and UDP flood from a large attacking population	very high	7	2018-04-29 18:55:01	2018-04-29 18:55:28
2018-04-29 18:56:04	10.0.5.7	TCP PSH-ACK and UDP flood from a relatively small attacking population	very high	6	2018-04-29 18:55:09	2018-04-29 18:55:28
2018-04-29 18:27:07	10.0.5.7	TCP SYN flood from a large attacking population	high	3	2018-04-29 18:25:55	2018-04-29 18:26:18
2018-04-29 18:27:00	10.0.5.7	TCP SYN flood	high	2	2018-04-29 18:26:16	2018-04-29 18:26:18
2018-04-29 18:21:43	10.0.5.24	TCP flood from a vast attacking population	very high	5	2018-04-29 18:19:58	2018-04-29 18:20:40
2018-04-29 18:21:36	10.0.5.24	TCP flood from a vast attacking population	very high	4	2018-04-29 18:19:58	2018-04-29 18:20:40

You can get further details by clicking on a specific attack to open the drilldown panels.



First event: 2018-04-29 18:25:55 Last event: 2018-04-29 18:26:18 (20193->20067)

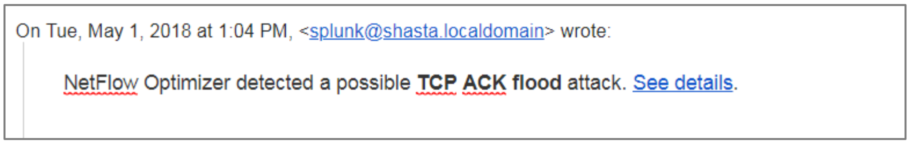
Attacker IP	Attacker Country	Victim IP	Victim Port	Total Traffic MB	Total Packets	Total Connections
118.21[redacted]	China	172.28.182.2	47468/tcp (unknown)	0	328	1
118.24[redacted]	Japan	172.28.180.92	33563/tcp (unknown)	1	571	1
120.251.[redacted]	China	172.28.164.177	39351/tcp (unknown)	1	547	1
121.82.[redacted]	Japan	172.28.127.180	35586/tcp (unknown)	0	246	1
122.14[redacted]	Australia	172.28.173.46	48472/tcp (unknown)	0	272	1
124.81.[redacted]	Indonesia	172.28.94.92	49443/tcp (unknown)	0	215	1
130.0.1[redacted]	France	172.28.34.79	37601/tcp (unknown)	0	222	1
130.34.[redacted]	Japan	172.28.89.228	35100/tcp (unknown)	1	488	1
132.14[redacted]	United Kingdom	172.28.226.220	34597/tcp (unknown)	0	265	1
132.236.[redacted]	United States	172.28.179.187	39360/tcp (unknown)	1	445	1

Attack origins

https://lab.netflowlogic.com:8001/en-US/app/ddos_detector/ddos_details?earliest=1525046400&latest=1525057200&form.exp_ip=*&form.confidence=150&form.attacker_ip=*&form.Country=*&form.victim_ip=*#

Alerts

DDoS Detector Splunk Application has a special alert notification (ddos_alert). The email notifying that a “Possible DDoS attack detected” is sent based on the results of the search and triggers conditions.



On Tue, May 1, 2018 at 1:04 PM, <splunk@shasta.localdomain> wrote:

> NetFlow Optimizer detected a possible **TCP ACK flood** attack. See details.

“See details” link in this email takes the user to the DDoS Attacks Details Splunk application dashboard with reported alert.

Appendix 1 - Basic DDoS Attack Types

Attack Types and Indicators

Attack Type	Textual identifier
Abnormal ICMP traffic	1-ICMP
Abnormal TCP traffic	1-TCP
Abnormal UDP traffic	1-UDP
Abnormal new IP addresses arrival rate	2
Abnormal network traffic entropy value	3
SYN flood	4-SYN
SYN-ACK flood	4-SYN-ACK
ACK flood	4-ACK
PSH - ACK flood	4-PSH-ACK
FIN/RST flood	4-FIN/RST
TCP-based application level protocol (e.g. HTTP) flood	7-TCP-<protocol>
UDP-based application level protocol (e.g. DNS) flood	7- UDP-<protocol>
“Tsunami” SYN flood	7-TSU-<protocol>
“Sockstress” attack	9 - SOCK
TCP SYN flood from a relatively small attacking population	1-TCP:4-SYN
TCP SYN-ACK flood from a relatively small attacking population	1-TCP:4-SYN-ACK

Attack Type	Textual identifier
TCP FIN/RST flood from a relatively small attacking population	1-TCP:4-FIN/RST
TCP SYN flood from a large attacking population	1-TCP:4-SYN:2
TCP SYN-ACK flood from a large attacking population	1-TCP:4-SYN-ACK:2
TCP FIN/RST flood from a large attacking population	1-TCP:4-FIN/RST:2
TCP SYN flood from a vast attacking population	1-TCP:4-SYN:2:3
TCP SYN-ACK flood from a vast attacking population	1-TCP:4-SYN-ACK:2:3
TCP FIN/RST flood from a vast attacking population	1-TCP:4-FIN/RST:2:3
UDP flood from a large attacking population	1-UDP:2
UDP flood from a vast attacking population	1-UDP:2:3
ICMP flood from a large attacking population	1-ICMP:2
ICMP flood from a vast attacking population	1-ICMP:2:3
Application level TCP flood attack	7-TCP-<protocol>:1-TCP
Application level UDP flood attack	7-UDP-<protocol>:1-UDP
Application level TCP “Tsunami” flood attack	7-TSU-<protocol>:1-TCP

Appendix 2 - Syslog Formats

Events Correlator

Key	Field Description	Comments
	NFO timestamp	Format: Mmm dd hh:mm:ss
	NFO server IP address	Format: IPv4_address
	NFO server NetFlow source ID	Configurable.
nfc_id	Message type identifier	“nfc_id=20196”
exp_ip	Network device (exporter) IP address	<IPv4 address>
t_last	NFO time of event	<number>, unix sec. NFO time of a most recent event which contributed to this report.
t_first	NFO time of report	<number>, unix sec. NFO time of an oldest event which contributed to this report
event_count	Event count	<number>, The number of indicators which contributed to this report
indicator	Indicator	<string>, Textual representation of the indicators which contributed to this report. See table in Appendix 1 for details
confidence	Confidence score	<number/number>, Cumulative confidence score and reporting threshold confidence value
confidence_bonus	Confidence bonus	<number>, Bonus confidence score included in the cumulative confidence score

Abnormal Traffic

Key	Field Description	Comments
	NFO timestamp	Format: Mmm dd hh:mm:ss
	NFO server IP address	Format: IPv4_address
	NFO server NetFlow source ID	Configurable.
nfc_id	Message type identifier	“nfc_id=20191”
exp_ip	Network device (exporter) IP address	<IPv4 address>
cause	Message type	<string> “cont” indicates that this message is a follow up report on the event
t_event	NFO time of event	<number>, unix sec. NFO time at the end of the time interval when the event was identified.
t_report	NFO time of report	<number>, unix sec. NFO time to which this message pertains
confidence	Confidence score	<number>, A value ≥ 90 indicating confidence in the event detection
trend	Trend	<string>, increasing, steady, abating
t_int	Observation time interval, msec	<number>

Elevated New IP Addresses Arrival Rate

Key	Field Description	Comments
	NFO timestamp	Format: Mmm dd hh:mm:ss
	NFO server IP address	Format: IPv4_address
	NFO server NetFlow source ID	Configurable.
nfc_id	Message type identifier	“nfc_id=20192”
exp_ip	Network device (exporter) IP address	<IPv4 address>
cause	Message type	<string> “cont” indicates that this message is a follow up report on the event
t_event	NFO time of event	<number>, unix sec. NFO time at the end of the time interval when the event was identified.
t_report	NFO time of report	<number>, unix sec. NFO time to which this message pertains
confidence	Confidence score	<number>, A value ≥ 90 indicating confidence in the event detection
trend	Trend	<string>, increasing, steady, abating
t_int	Observation time interval, msec	<number>

Elevated Noise Level in the Network

Key	Field Description	Comments
	NFO timestamp	Format: Mmm dd hh:mm:ss
	NFO server IP address	Format: IPv4_address
	NFO server NetFlow source ID	Configurable.
nfc_id	Message type identifier	“nfc_id=20193”
exp_ip	Network device (exporter) IP address	<IPv4 address>
cause	Message type	<string> “cont” indicates that this message is a follow up report on the event
t_event	NFO time of event	<number>, unix sec. NFO time at the end of the time interval when the event was identified.
t_report	NFO time of report	<number>, unix sec. NFO time to which this message pertains
confidence	Confidence score	<number>, A value ≥ 90 indicating confidence in the event detection
trend	Trend	<string>, increasing, steady, abating
t_int	Observation time interval, msec	<number>

TCP/IP Vulnerability

Key	Field Description	Comments
	NFO timestamp	Format: Mmm dd hh:mm:ss
	NFO server IP address	Format: IPv4_address
	NFO server NetFlow source ID	Configurable.
nfc_id	Message type identifier	“nfc_id=20194”
exp_ip	Network device (exporter) IP address	<IPv4 address>
cause	Message type	<string> “cont” indicates that this message is a follow up report on the event
t_event	NFO time of event	<number>, unix sec. NFO time at the end of the time interval when the event was identified.
t_report	NFO time of report	<number>, unix sec. NFO time to which this message pertains
flood_type	Flood type	<string>, Flood type, “SYN”, “SYN-ACK”
confidence	Confidence score	<number>, A value ≥ 90 indicating confidence in the event detection
trend	Trend	<string>, increasing, steady, abating
t_int	Observation time interval, msec	<number>

TCP/IP Information Details

Key	Field Description	Comments
	NFO timestamp	Format: Mmm dd hh:mm:ss
	NFO server IP address	Format: IPv4_address
	NFO server NetFlow source ID	Configurable.
nfc_id	Message type identifier	“nfc_id=20195”
exp_ip	Network device (exporter) IP address	<IPv4 address>
src_ip	Source IP address	<IPv4_address>
dest_ip	Destination IP address	<IPv4_address>
dest_port	Destination port number	<number>
first_seen	First time seen	<number> Time when a first invalid TCP/IP session between the hosts was observed
last_seen	Last time seen	<number> Time when a last invalid TCP/IP session between the hosts was observed
syn_count	SYN count	<number>, The number of observed invalid TCP/IP sessions between the hosts which correspond to the SYN-flood attack pattern
syn_ack_count	SYN-ACK count	<number>, The number of observed invalid TCP/IP sessions between the hosts which correspond to the SYN-ACK (“reflection”) flood attack pattern
ack_count	ACK count	<number>, The number of observed invalid TCP/IP sessions between the hosts which correspond to the ACK flood attack pattern
fin_count	FIN count	<number>, The number of observed invalid TCP/IP sessions between the hosts which correspond to the FIN flood attack pattern

Key	Field Description	Comments
psh_count_sd	PSH count from source to destination	<number>, The number of PSH requests from the source host to the destination host
psh_count_ds	PSH count from destination to source	<number>, The number of PSH requests from the destination host to the source host

Application Protocol Level Attack

Key	Field Description	Comments
	NFO timestamp	Format: Mmm dd hh:mm:ss
	NFO server IP address	Format: IPv4_address
	NFO server NetFlow source ID	Configurable.
nfc_id	Message type identifier	“nfc_id=20197”
exp_ip	Network device (exporter) IP address	<IPv4 address>
cause	Message type	<string> “cont” indicates that this message is a follow up report on the event
dest_ip	Monitored server IP address	<IPv4_address>
dest_port	Monitored server port number	<number>
protocol	Transport Protocol (TCP = 6, UDP = 17)	<number>
t_event	NFO time of event	<number>, unix sec. NFO time at the end of the time interval when the event was identified.
t_report	NFO time of report	<number>, unix sec. NFO time to which this message pertains
confidence	Confidence score	<number>, A value ≥ 90 indicating confidence in the event detection
trend	Trend	<string>, increasing, steady, abating
t_int	Observation time interval, msec	<number>

Application Protocol Level Attack - Active Clients

Key	Field Description	Comments
	NFO timestamp	Format: Mmm dd hh:mm:ss
	NFO server IP address	Format: IPv4_address
	NFO server NetFlow source ID	Configurable.
nfc_id	Message type identifier	“nfc_id=20198”
exp_ip	Network device (exporter) IP address	<IPv4 address>
dest_ip	Monitored server IP address	<IPv4_address>
dest_port	Monitored server port number	<number>
protocol	Transport Protocol (TCP = 6, UDP = 17)	<number>
src_ip	Client IPv4 address	<IPv4_address>
percent_of_total	Percent of total connections to the server made by the client during the observation interval	<decimal>, e.g. 25.444% is 25.444
t_int	Observation time interval, msec	<number>

Sockstress Attack

Key	Field Description	Comments
	NFO timestamp	Format: Mmm dd hh:mm:ss
	NFO server IP address	Format: IPv4_address
	NFO server NetFlow source ID	Configurable.
nfc_id	Message type identifier	“nfc_id=20199”
exp_ip	Network device (exporter) IP address	N/A, reported as 255.255.255.255
cause	Message type	<string> “cont” indicates that this message is a follow up report on the event
dest_ip	Monitored server IP address	<IPv4_address>
dest_port	Monitored server port number	<number>
count	The number of anomalously behaving network peers	<number>
t_event	NFO time of event	<number>, unix sec. NFO time at the end of the time interval when the event was identified.
t_report	NFO time of report	<number>, unix sec. NFO time to which this message pertains
confidence	Confidence score	<number>, A value ≥ 90 indicating confidence in the event detection
trend	Trend	<string>, increasing, steady, abating
t_int	Observation time interval, msec	<number>

Sockstress Attack – Network Peers

Key	Field Description	Comments
	NFO timestamp	Format: Mmm dd hh:mm:ss
	NFO server IP address	Format: IPv4_address
	NFO server NetFlow source ID	Configurable.
nfc_id	Message type identifier	“nfc_id=20200”
exp_ip	Network device (exporter) IP address	N/A, reported as 255.255.255.255
cause	Message type	<string> “cont” indicates that this message is a follow up report on the event
dest_ip	Monitored server IP address	<IPv4_address>
dest_port	Monitored server port number	<number>
src_ip	“Sockstress” client IPv4 address	<IPv4_address>
src_port	“Sockstress” client port number	<number>
first_seen	Time when first ZWP request was sent, unix seconds	<number>, unix sec
last_seen	Time when latest ZWP request was sent, unix seconds	<number>, unix sec
last_zwp_interval	Time interval between two last ZWP requests, sec	<number>, unix sec
zwp_count	Total number of ZWP requests sent	<number>, unix sec