Plugging Network Security Holes using NetFlow

Loopholes in today's network security solutions and how NetFlow can help
ManageEngine is an IT management vendor focused on bringing a complete IT management portfolio to all types of enterprises.
Network Security Concerns
Network Security Concerns

Increasing Network Security Violations

2010: Major DDoS attacks and arrival of STUXNET

2011: HB Gary Federal & Sony PSN Hacked - Emails made public and user data stolen

Since then: Sony Pictures, Nintendo, Fox Networks, Eve’s online, Lockheed Martin, PBS, Honda Canada, Booz Allen Hamilton, C.I.A...The list is growing
Network Security Concerns

Malwares – More Numbers and More Sophisticated

- The start
- 1971
- 1990
- 2011

*Malware*
Malwares – More Numbers and More Sophisticated

More numbers and more sophisticated malwares


Targeted, custom malwares appearing. STUXNET is just the beginning

The era of the zero-day malware and attacks is here
Telecommuting & Erosion of Perimeter

Percentage of US workers Telecommuting

- 1994: 7.5%
- 2004: 17%
- 2014: ??
Telecommuting & Erosion of Perimeter

More number of telecommuters per enterprise

Increasing number of enterprise users have mobile devices like laptops & tablets

Disappearing perimeter – Users connect over VPN, 3G, Public Wi-Fi, etc. from home or mobile devices

Less secure transactions - Susceptible to malwares and Trojans
Telecommuting & Erosion of Perimeter

More number of telecommuters per enterprise
Increasing number of enterprise users have mobile devices like laptops & tablets
Disappearing perimeter – Users connect over VPN, 3G, Public Wi-Fi, etc. from home or mobile devices

Less secure transactions – Susceptible to malwares and Trojans

Network Security Concerns

![Diagram of network security with various devices and connections]

7.5%
17%

<table>
<thead>
<tr>
<th>Year</th>
<th>Percentage of US workers Telecommuting</th>
</tr>
</thead>
<tbody>
<tr>
<td>1994</td>
<td>0%</td>
</tr>
<tr>
<td>2004</td>
<td>5%</td>
</tr>
<tr>
<td>2014</td>
<td>15%</td>
</tr>
<tr>
<td>2015</td>
<td>20%</td>
</tr>
<tr>
<td>2016</td>
<td>25%</td>
</tr>
<tr>
<td>2017</td>
<td>30%</td>
</tr>
<tr>
<td>2018</td>
<td>35%</td>
</tr>
</tbody>
</table>
Faster Networks – More Business Localization

Increasing Network Bandwidth – The fastest Ethernet will soon move from 10 Gigabit to 100 Gigabit Ethernet

Newer applications and services added everyday

Business localization – Increased users and thus higher volume of network traffic

More unknown applications are encountered

Network Security Concerns
Faster Networks – More Business Localization

Increasing Network Bandwidth – The fastest Ethernet will soon move from 10 Gigabit to 100 Gigabit Ethernet

Newer applications and services added everyday

Business localization – Increased users and thus higher volume of network traffic

More unknown applications are encountered
Network Security Concerns

Star Topology
Complex Meshed Networks

Networks are no longer based on the simple STAR topology

Distributed networks in MESH topology

Huge number of devices and nodes interconnected

Traffic moves in multiple directions through different nodes
Complex Meshed Networks

Networks are no longer based on the simple STAR topology.
Distributed networks in MESH topology.
Huge number of devices and nodes interconnected.
Traffic moves in multiple directions through different nodes.

Network Security Concerns

Meshed Networks
Loopholes in current network security systems
The Loopholes

Internet

IDS

Internal Network

Signature Anomaly Blocked

Non Signature Anomaly Undetected
The Loopholes

More targeted, custom made, STUXNET like malwares

IDS and IPS is based on “signatures”, a known characteristic of some particular attack

Increasing number of zero day attacks whose signatures has not yet been documented

Firewalls are ineffective against zero-day malwares as they block only traffic defined by the user
The Loopholes

Telecommuters – Access the Internet from public Wi-Fi spots & unknown networks

Personal computers are easier to attack and infect

Users carry infected devices into the network or connect via VPN - Malware spreads across the LAN

Packet inspection technologies are impractical for use in LAN due to the number of nodes to be monitored

IDS not feasible for internal network monitoring
The Loopholes

Telecommuters – Access the Internet from public Wi-Fi spots & unknown networks

Personal computers are easier to attack and infect

Users carry infected devices into the network or connect via VPN

Malware spreads across the LAN

Packet inspection technologies are impractical for use in LAN due to the number of nodes to be monitored

IDS not feasible for internal network monitoring
With malwares in your LAN, your network could be the one hosting an attack or sending spam.

STUXNET spread across 100,000 computers and never used Internet as the stream.

Each time STUXNET infected a system, it connected to 2 public domains to report about the infected machines.

Egress traffic accounting can help with early detection.

IDS and IPS does only ingress traffic accounting.
10 Gigabit network is now standard & 100 Gigabit network is around the corner

Organizations now have more traffic and applications

Packet Inspection is rendered ineffective due to the volume of traffic involved

High performance and scalable packet inspection tools are highly expensive
The Loopholes

10 Gigabit network is now standard & 100 Gigabit network is around the corner

Organizations now have more traffic and applications

Packet Inspection is rendered ineffective due to the volume of traffic involved

High performance and scalable packet inspection tools are highly expensive
Localization and branching of enterprises means more users and many services

Firewall rules are used to block any undesired traffic but web service traffic (port 80) is allowed in most networks

Sophisticated attacks use port 80 with the ACK bit set so that traffic appears to be legitimate web transactions

Such traffic surpasses the firewalls and enters your network
The Loopholes

Localization and branching of enterprises means more users and many services. Firewall rules are used to block any undesired traffic but web service traffic (port 80) is allowed in most networks. Sophisticated attacks use port 80 with the ACK bit set so that traffic appears to be legitimate web transactions. Such traffic surpasses the firewalls and enters your network.

TCP Connect Scan
SYN Scan
NULL Scan
FIN Scan
Ack Scan
XMAS-TREE Scan

TCP Traffic
Meshed networks include more nodes than the STAR topologies of the old times.

Traffic between sites choose the best path and do not always traverse through a center node.

Packet analysis / inspection technology not be feasible at all nodes.

Multiple locations and hence data collection for packet inspection at each point is difficult.
Meshed networks include more nodes than the STAR topologies of the old times. Traffic between sites choose the best path and do not always traverse through a center node. Packet analysis/inspection technology at all nodes is not feasible, especially with multiple locations. Data collection for packet inspection at each point is difficult.
The Solution
Technology developed by Cisco Systems - initially used as a switching path

Primary network IP traffic accounting technology

All major vendors now support flow export:
- **NetFlow** - Cisco, Adtran, 3COM
- **sFlow** - Alcatel, HP, Brocade, Enterasys, Dell
- **IPFIX** - Nortel / J-Flow - Juniper
Captures specific information from network IP Traffic and stores to the device’s NetFlow cache

Traffic information exported as UDP packets to the configured destination

7 Key fields defines a flow as one unique conversation in NetFlow
About NetFlow

Source Interface (ifindex)
- Protocol
- Source IP Address
- Destination IP Address
- Source Port
- Destination Port
- ToS
The Solution

NetFlow enabled interface

Core Network

Edge Router

UDP NetFlow

NetFlow Collector
### The Solution

NetFlow enabled interface

**Core Network**

**Edge Router**

**NetFlow Collector**

**UDP NetFlow**

### Data Table

<table>
<thead>
<tr>
<th>Src IP</th>
<th>Dst IP</th>
<th>Application</th>
<th>Port</th>
<th>Dst Port</th>
<th>Protocol</th>
<th>DSCP</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>112.244.182.67</td>
<td>61.16.161.10</td>
<td>ESP_App</td>
<td>20491</td>
<td>24316</td>
<td>ESP</td>
<td>Default</td>
<td>310.93 MB</td>
</tr>
<tr>
<td>112.244.182.67</td>
<td>74.201.154.191</td>
<td>https</td>
<td>53023</td>
<td>443</td>
<td>TCP</td>
<td>111111</td>
<td>125.77 MB</td>
</tr>
<tr>
<td>112.244.182.67</td>
<td>74.201.154.152</td>
<td>https</td>
<td>59500</td>
<td>443</td>
<td>TCP</td>
<td>111111</td>
<td>52.44 MB</td>
</tr>
<tr>
<td>112.244.182.67</td>
<td>74.201.154.191</td>
<td>https</td>
<td>55383</td>
<td>443</td>
<td>TCP</td>
<td>Default</td>
<td>44.72 MB</td>
</tr>
<tr>
<td>112.244.182.70</td>
<td>74.201.113.15</td>
<td>TCP_App</td>
<td>29040</td>
<td>43659</td>
<td>TCP</td>
<td>111111</td>
<td>38.84 MB</td>
</tr>
<tr>
<td>112.244.182.67</td>
<td>61.16.161.61</td>
<td>https</td>
<td>49505</td>
<td>443</td>
<td>TCP</td>
<td>111111</td>
<td>32.51 MB</td>
</tr>
<tr>
<td>112.244.182.76</td>
<td>114.29.195.84</td>
<td>https</td>
<td>32753</td>
<td>443</td>
<td>TCP</td>
<td>111111</td>
<td>19.49 MB</td>
</tr>
<tr>
<td>112.244.182.80</td>
<td>182.19.95.68</td>
<td>http</td>
<td>41064</td>
<td>80</td>
<td>TCP</td>
<td>Default</td>
<td>14.2 MB</td>
</tr>
<tr>
<td>112.244.182.67</td>
<td>80.231.71.29</td>
<td>http</td>
<td>47022</td>
<td>80</td>
<td>TCP</td>
<td>Default</td>
<td>11.5 MB</td>
</tr>
<tr>
<td>112.244.182.67</td>
<td>74.201.113.1</td>
<td>ESP_App</td>
<td>41456</td>
<td>30232</td>
<td>ESP</td>
<td>Default</td>
<td>8.52 MB</td>
</tr>
<tr>
<td>112.244.182.67</td>
<td>74.201.154.150</td>
<td>https</td>
<td>36389</td>
<td>443</td>
<td>TCP</td>
<td>111111</td>
<td>8.44 MB</td>
</tr>
<tr>
<td>112.244.182.80</td>
<td>80.231.71.25</td>
<td>http</td>
<td>51480</td>
<td>80</td>
<td>TCP</td>
<td>Default</td>
<td>7.87 MB</td>
</tr>
<tr>
<td>112.244.182.67</td>
<td>74.201.154.43</td>
<td>https</td>
<td>37654</td>
<td>443</td>
<td>TCP</td>
<td>111111</td>
<td>7.39 MB</td>
</tr>
<tr>
<td>112.244.182.80</td>
<td>84.45.63.43</td>
<td>http</td>
<td>58201</td>
<td>80</td>
<td>TCP</td>
<td>Default</td>
<td>6.0 MB</td>
</tr>
<tr>
<td>112.244.182.67</td>
<td>74.125.236.77</td>
<td>https</td>
<td>83630</td>
<td>443</td>
<td>TCP</td>
<td>111111</td>
<td>5.79 MB</td>
</tr>
<tr>
<td>112.244.182.77</td>
<td>65.220.146.224</td>
<td>https</td>
<td>54053</td>
<td>443</td>
<td>TCP</td>
<td>Default</td>
<td>5.48 MB</td>
</tr>
<tr>
<td>112.244.182.67</td>
<td>74.125.236.66</td>
<td>https</td>
<td>40683</td>
<td>443</td>
<td>TCP</td>
<td>111111</td>
<td>5.44 MB</td>
</tr>
<tr>
<td>112.244.182.67</td>
<td>61.16.161.50</td>
<td>https</td>
<td>58025</td>
<td>443</td>
<td>TCP</td>
<td>111111</td>
<td>4.7 MB</td>
</tr>
<tr>
<td>112.244.182.76</td>
<td>216.115.212.95</td>
<td>https</td>
<td>47569</td>
<td>443</td>
<td>TCP</td>
<td>Default</td>
<td>4.52 MB</td>
</tr>
<tr>
<td>112.244.182.69</td>
<td>61.16.161.10</td>
<td>netmeeting</td>
<td>3309</td>
<td>38260</td>
<td>TCP</td>
<td>111111</td>
<td>4.07 MB</td>
</tr>
</tbody>
</table>
The Solution

ManageEngine NetFlow Analyzer

Without NetFlow Analysis


With NetFlow Analysis

TCP ESP Kazaa HTTP Src IP Cnvrstn IPv4 DSCP Octets 80
UDP GRE Torrent Telnet Dst IP Host IPv6 ToS Time 23
The Solution

ManageEngine NetFlow Analyzer

Leverages on the flow data exported from your network devices

Reports on traffic, applications, hosts, conversations, QoS, etc.

Easy to use GUI and extensive graph options for quick understanding and fast problem drill down
The Solution

Who?
- Source IP Address
- Destination IP Address

What?
- Source Port
- Destination Port
- Protocol

When?
- Flow Start and End time
- Packet Count
- Octet count

Usage?
- ToS
- TCP Flags

Path?
- Protocol
- Input and Output Interface (ifindex)

QoS?
- NextHop
- Source AS Information
- Destination AS Information

Route?
- QoS
Advanced Security Analytics Module

Flow based network behavior analysis tool

Add-On to ManageEngine NetFlow Analyzer and leverages on its agentless data collection capabilities

Uses the NetFlow or sFlow data received by NetFlow Analyzer for internal and external threat detection

Continuous Stream Mining Engine™ detects network anomalies in real-time
Advanced Security Analytics Module

Flow based network behavior analysis tool

Add On to ManageEngine NetFlow Analyzer and leverages on its agentless data collection capabilities

Uses the NetFlow or sFlow data received by NetFlow Analyzer for internal and external threat detection

Continuous Stream Mining Engine (TM) detects network anomalies in real-time

The Solution

![Network Diagram]
The Solution

Advanced Security Analytics Module
Flow based network behavior analysis tool
Add - On to ManageEngine NetFlow Analyzer and leverages on its agentless data collection capabilities
Uses the NetFlow or sFlow data received by NetFlow Analyzer for internal and external threat detection
Continuous Stream Mining Engine
detects network anomalies in real-time

User

NetFlow Data
NetFlow Analyzer
Continuous Stream Mining Engine
Advanced Security Analytics
Events
Plugging Loopholes
Except port scan, all the traffic is detectable as it is using NetFlow data

ASAM analyzes NetFlow data and detect scans – TCP Scans like SYN scan, reverse scan, Xmas-Tree scan
Detect Hacking Attempts

Network Hacking Reconnaissance Methods

- Port Scans
- DNS Lookup
- Ping Sweeps
- Traceroute

Problem / Events / Resources
- Short TCP Rst Ack Diagonal Scan: 926 events, 232 resources
- Short TCP Psh Ack Diagonal Scan: 928 events, 232 resources
- Short TCP Handshake Diagonal Scan: 925 events, 232 resources
- Short TCP Handshake Port Scan: 800 events, 200 resources
- Short TCP Rst Ack Port Scan: 800 events, 200 resources
- TCP Syn Port Scan: 241 events, 120 resources
- ICMP Port Unreachable Host Scan: 196 events, 97 resources
- TCP Urg Port Scan: 194 events, 96 resources
- TCP Rst Port Scan: 149 events, 74 resources
- Empty TCP Diagonal Scan: 47 events, 19 resources
- Others

Time Distribution

Counts

0 50 100 150 200


Events

Resources

Problems
Identify the Top N and baseline your network behavior

Change in traffic patterns can be identified using NetFlow data

Sudden increase in traffic, spike in UDP traffic, etc.

Get alerted when such changes occur
Identify the Top N and baseline your network behavior. Change in traffic patterns can be identified using NetFlow data. Sudden increase in traffic, spike in UDP traffic, etc. Get alerted when such changes occur.

Stopping Zero-Day Malwares

**Daily Average**

<table>
<thead>
<tr>
<th>Category</th>
<th>Total</th>
<th>Max</th>
<th>Min</th>
<th>Avg</th>
<th>Standard Deviation</th>
<th>95th Percentile</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1 min</td>
<td>24Hours</td>
<td>1 min</td>
<td>24Hours</td>
<td></td>
</tr>
<tr>
<td><strong>IN</strong></td>
<td>1.68 TB</td>
<td>9.61 Mbps</td>
<td>4.83 Mbps</td>
<td>0.00</td>
<td>195.33 Kbps</td>
<td>2.47 Mbps</td>
</tr>
<tr>
<td><strong>OUT</strong></td>
<td>1.68 TB</td>
<td>9.85 Mbps</td>
<td>4.84 Mbps</td>
<td>0.00</td>
<td>195.31 Kbps</td>
<td>2.47 Mbps</td>
</tr>
</tbody>
</table>
Session based identification helps track malware

Abnormal traffic to many hosts from single host on a single port can be a worm

Traffic from IANA reserved addresses or over reserved protocols is malicious traffic

ASAM identifies such traffic and creates alerts
### Stopping Zero-Day Malware

Session-based identification helps track malware.

#### Table:

<table>
<thead>
<tr>
<th>ID</th>
<th>Problem / Probes</th>
<th>Offender(s)</th>
<th>Routed via</th>
<th>Target(s)</th>
<th>Time</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>136785</td>
<td>Scans / Probes - Empty TCP Diagonal Scan</td>
<td>NA 1: [192.168.1.160]</td>
<td>1: [192.168.1.16 (ifIndex2)]</td>
<td>NA 16: [192.168.5.145, 192.168.5.146, 192.168.5.147, 192.168.5.148, 192.168....]</td>
<td>2011-07-29 16:37:45</td>
<td>16</td>
</tr>
<tr>
<td>136784</td>
<td>Scans / Probes - Empty TCP Diagonal Scan</td>
<td>NA 1: [192.168.1.132]</td>
<td>1: [192.168.1.16 (ifIndex2)]</td>
<td>NA 16: [192.168.5.144, 192.168.5.145, 192.168.5.146, 192.168.5.147, 192.168.5.152, 192.168....]</td>
<td>2011-07-29 16:37:45</td>
<td>16</td>
</tr>
<tr>
<td>136783</td>
<td>Scans / Probes - Empty TCP Diagonal Scan</td>
<td>NA 1: [192.168.1.160]</td>
<td>1: [192.168.1.16 (ifIndex2)]</td>
<td>NA 16: [192.168.5.145, 192.168.5.146, 192.168.5.147, 192.168.5.148, 192.168....]</td>
<td>2011-07-29 16:30:01</td>
<td>16</td>
</tr>
</tbody>
</table>
Telecommuting brings malwares into the network

An IDS deployment for internal traffic is not feasible

NetFlow is light on the bandwidth and device resources

Most of your devices come with support for NetFlow or similar flow format

Enable flow export and get visibility on both ingress and egress traffic flow
Telecommuting brings malwares into the network.

An IDS deployment for internal traffic is not feasible.

NetFlow is light on the bandwidth and device resources.

Most of your devices come with support for NetFlow or similar flow format.

Enable flow export and get visibility on both ingress and egress traffic flow.

Internal Network Threat Detection
Packet inspection software capable of handling 10G network traffic are few and expensive.

NetFlow data captures just the important information from actual traffic.

Do traffic analytics using NetFlow information.

Use packet capture only where absolutely necessary.

Brings down cost and helps in faster troubleshooting.
Packet inspection software capable of handling 10G network traffic are few and expensive. NetFlow data captures just the important information from actual traffic. Do traffic analytics using NetFlow information. Use packet capture only where absolutely necessary. Brings down cost and helps in faster troubleshooting.
The star (hub and spoke) networks are a thing of past

Meshed networks today allow traffic to pass through all nodes depending on best path

An IDS or packet inspection at each node is not feasible

Utilize the already available NetFlow from your network devices in locations like branches
The star (hub and spoke) networks are a thing of the past. Meshed networks today allow traffic to pass through all nodes depending on the best path. An IDS or packet inspection at each node is not feasible. Utilize the already available NetFlow from your network devices in locations like branches. Solution for Meshed Networks.
ManageEngine NetFlow Analyzer
An all software solution for bandwidth monitoring, traffic analytics and anomaly detection

Supports all flow formats as well as most of Cisco’s performance monitoring technologies

Cisco NBAR, CBQoS, IPSLA and WAAS reports

Additional features include AS reporting, capacity planning, support for Cisco ASA NSEL, usage alerts, etc.
What else is NetFlow Analyzer

Highly granular traffic reports based on speed, volume, utilization and packets updated in real-time. Conversations details for each minute thus helping with the quick troubleshooting of network incidents.
What else is NetFlow Analyzer

- Highly granular traffic reports based on speed, volume, utilization and packets updated in real-time.
- Conversations details for each minute thus helping with quick troubleshooting of network incidents.
- Details on protocol distribution, application usage & custom application monitoring.
- Future ready with IPv6 conversation reports.
What else is NetFlow Analyzer

Highly granular traffic reports based on speed, volume, utilization and packets updated in real-time.

Conversations details for each minute thus helping with the quick troubleshooting of network incidents.

Details on protocol distribution, application usage & custom application monitoring.

Future ready with IPv6 conversation reports.

<table>
<thead>
<tr>
<th>Application</th>
<th>Traffic (Total: 21.82 GB)</th>
<th>% of total traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>http</td>
<td>15.15 GB</td>
<td>69%</td>
</tr>
<tr>
<td>pop3</td>
<td>4.18 GB</td>
<td>19%</td>
</tr>
<tr>
<td>https</td>
<td>1.71 GB</td>
<td>8%</td>
</tr>
<tr>
<td>sql-net</td>
<td>144.78 MB</td>
<td>1%</td>
</tr>
<tr>
<td>domain</td>
<td>14.77 MB</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>smtp</td>
<td>5.16 MB</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>compressnet</td>
<td>4.07 MB</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>HTTP-Proxy</td>
<td>1.7 MB</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>ssh</td>
<td>993.5 KB</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>tacacs</td>
<td>721.15 KB</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>snmp</td>
<td>110.79 KB</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>icmp</td>
<td>100.3 KB</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>ipx</td>
<td>59.93 KB</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>sip</td>
<td>23.16 KB</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>echo</td>
<td>16.2 KB</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>microsoft-ds</td>
<td>13.16 KB</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>ms-sql-s</td>
<td>6.44 KB</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>ntp</td>
<td>5.22 KB</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>hosta2-na</td>
<td>2.85 KB</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>rpmmap</td>
<td>2.12 KB</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>ldap</td>
<td>1.97 KB</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>netbios-na</td>
<td>1.09 KB</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>wins</td>
<td>390.00 Bytes</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>ftp</td>
<td>60.00 Bytes</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>unaccounted</td>
<td>539.02 MB</td>
<td>3%</td>
</tr>
</tbody>
</table>

Others | 45.29 KB | 3% |
What else is NetFlow Analyzer

- Highly granular traffic reports based on speed, volume, utilization and packets updated in real-time.
- Conversations details for each minute thus helping with the quick troubleshooting of network incidents.
- Details on protocol distribution, application usage & custom application monitoring.
- Future ready with IPv6 conversation reports.
What else is NetFlow Analyzer

Highly granular traffic reports based on speed, volume, utilization and packets updated in real-time.

Conversations details for each minute thus helping with quick troubleshooting of network incidents.

Details on protocol distribution, application usage & custom application monitoring.

Future ready with IPv6 conversation reports.
Advanced Security Analytics Module
Security Posture page to list all detected anomalies grouped under problem classes

Drill down on each problem for problem analysis or resource analysis

In-depth details on each event, source, destination and route

Helps you take quick decisions to block IP’s or take action on the device level
ASAM – An Overview

Security Posture page to list all detected anomalies grouped under problem classes. Drill down on each problem for problem analysis or resource analysis. In-depth details on each event, source, destination, and route. Helps you take quick decisions to block IP’s or take action on the device level.
## Event Details

**Show DNS**

### Event Details

**Event Id:** 305677  
**Problem:** Short TCP Rst_Ack Port Scan

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume</td>
<td>3.57 KB</td>
</tr>
<tr>
<td>Packets</td>
<td>85</td>
</tr>
<tr>
<td>Hits</td>
<td>85</td>
</tr>
<tr>
<td>Unique Destination IPs</td>
<td>1: [192.168.6.93]</td>
</tr>
<tr>
<td>Unique Source Networks</td>
<td>1: [192.168.4.0/24]</td>
</tr>
<tr>
<td>Unique Destination Networks</td>
<td>1: [192.168.6.0/24]</td>
</tr>
<tr>
<td>Unique Source Ports</td>
<td>85: [11, 12, 13, 14, 15, 16, 18, 19, 20, 22, 23, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 38, 39, 41, 42, 43, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 56, 57, 59, 60, 61, 62, 63, 64, 65, 68, 69, 70, 72, 73, 74, 75, 77, 78, 79, 80, 81, 82, 83, 85...]</td>
</tr>
<tr>
<td>Unique Applications</td>
<td>79: [sysstat, daytime, msp, chargen, ftp-data, ssh, telnet, smtp, now-fe, msg-ico, msg-auth, dsp, raf, rlp, graphics, name, nicname, mpm, mpm-snd, ni-ftp, auditd, taracs, re-mail-ok, la-maint, xns-time, domain, xns-ch, xns-auth, ni-mail, acas, whois++,...]</td>
</tr>
<tr>
<td>Unique TCP Flags</td>
<td>1: [A_R_]</td>
</tr>
<tr>
<td>Unique Protocols</td>
<td>1: [TCP]</td>
</tr>
<tr>
<td>Unique ToS Values</td>
<td>1: [2]</td>
</tr>
<tr>
<td>Unique In Interfaces (Routed Via)</td>
<td>1: [Cisco ASR (ifIndex2)]</td>
</tr>
<tr>
<td>Unique Out Interfaces</td>
<td>1: [Cisco ASR (ifIndex4)]</td>
</tr>
<tr>
<td>Unique Router IPs</td>
<td>1 Router(s)</td>
</tr>
</tbody>
</table>

- Cisco ASR[127.0.0.1]
An IDS and firewall only system is a thing of the past

New age networks face more sophisticated problems

A combination of well set firewall rules, an effective IDS/IPS system and NetFlow analysis is the answer
Conclusion

Intrusion Detection System

Network Behavior Analysis

Firewall

Comprehensive Enterprise Network Security
Questions?

ManageEngine NetFlow Analyzer is used by over 4000 customers worldwide. Visit our website for details:

www.manageengine.com
www.netflowanalyzer.com
sales@manageengine.com
nfs@manageengine.com