



"There is nothing more important
than our customers"

A handwritten signature in black ink, appearing to read 'Zdeněk Pala'.

Network Behavioral Anomaly Detection Dragon Security Command Console – DSCC

Zdeněk Pala



ZÁPADOČESKÁ
UNIVERZITA
V PLZNI

26.5.2010

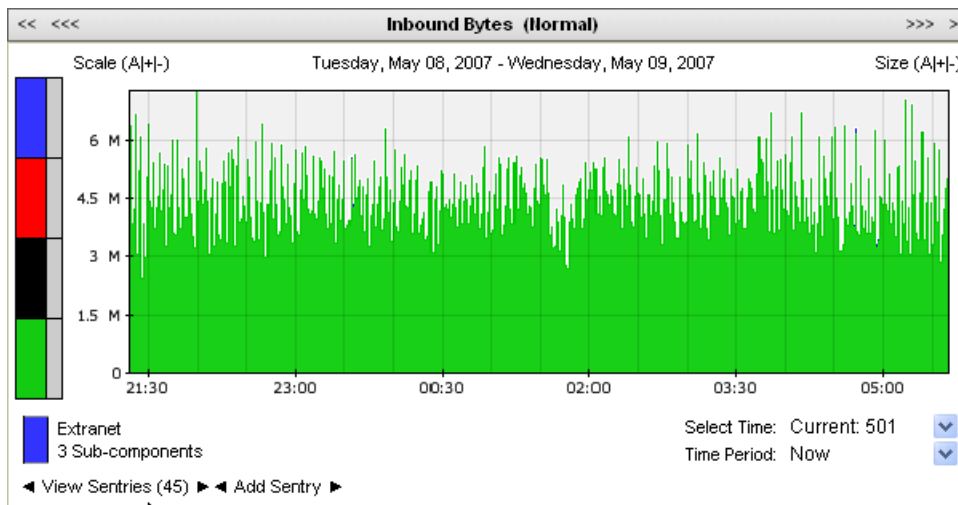
ECIE certified engineer
ECI certified instructor

How can an intrusion be identified?

- Pattern Matching:
 - Look for patterns in the data filed that indicate an attack
 - Signatures
- Protocol Analysis:
 - Look for header values that indicate an attack
 - Do the headers match the RFC
- Behavior Based:
 - Does the current traffic pattern match the normal pattern
 - Flow Based

Network Behavior Anomaly Detection (NBAD)

- Works with flow data
- Constantly monitors traffic to detect changes in network traffic flows
- Optimal for detection of Day-Zero attacks
- Can be adjusted to customers special needs



Sentry List			
Name	Owner	Actions	Enabled
Behavior - Flow Count Behavior Change	admin		<input checked="" type="checkbox"/>
Behavior - Host Count Behavior Change	admin		<input checked="" type="checkbox"/>
Behavior - Threat Traffic Packet Rate Behavior Change	admin		<input checked="" type="checkbox"/>
Default Suspicious - External - Inbound Unidirectional Flows Threshold	admin		<input checked="" type="checkbox"/>
DoS - External - Distributed DoS Attack (High Number of Hosts)	admin		<input checked="" type="checkbox"/>
DoS - External - Distributed DoS Attack (Low Number of Hosts)	admin		<input checked="" type="checkbox"/>
DoS - External - Distributed DoS Attack (Medium Number of Hosts)	admin		<input checked="" type="checkbox"/>
DoS - External - Flood Attack (Low)	admin		<input checked="" type="checkbox"/>
DoS - External - Flood Attack (Medium)	admin		<input checked="" type="checkbox"/>
DoS - External - Potential ICMP DoS	admin		<input checked="" type="checkbox"/>
DoS - External - Potential TCP DoS	admin		<input checked="" type="checkbox"/>
DoS - External - Potential UDP DoS	admin		<input checked="" type="checkbox"/>
DoS - External - Potential Unresponsive Service or Distributed DoS	admin		<input checked="" type="checkbox"/>
DoS - External - IFlood Attack (High)	admin		<input checked="" type="checkbox"/>
Malware - External - Client Based DNS Activity to the Internet	admin		<input checked="" type="checkbox"/>
Malware - External - Communication with BOT Control Channel	admin		<input checked="" type="checkbox"/>
Policy - External - Clear Text Application Usage	admin		<input checked="" type="checkbox"/>
Policy - External - Hidden FTP Server	admin		<input checked="" type="checkbox"/>
Policy - External - IM/Chat	admin		<input checked="" type="checkbox"/>
Policy - External - IRC Connections	admin		<input checked="" type="checkbox"/>
Policy - External - Local P2P Server Detected	admin		<input checked="" type="checkbox"/>
Policy - External - Long Duration Flow Detected	admin		<input checked="" type="checkbox"/>
Policy - External - P2P Communications Detected	admin		<input checked="" type="checkbox"/>
Policy - External - Remote Desktop Access from the Internet	admin		<input checked="" type="checkbox"/>
Policy - External - SMTP Mail Sender	admin		<input checked="" type="checkbox"/>
Policy - External - SSH or Telnet Detected on Non-Standard Port	admin		<input checked="" type="checkbox"/>
Policy - External - Usenet Usage	admin		<input checked="" type="checkbox"/>
Policy - External - VNC Access From the Internet to a Local Host	admin		<input checked="" type="checkbox"/>
Policy - P2P Policy Threshold	admin		<input checked="" type="checkbox"/>
Recon - External - ICMP Scan (High)	admin		<input checked="" type="checkbox"/>
Recon - External - ICMP Scan (Low)	admin		<input checked="" type="checkbox"/>
Recon - External - ICMP Scan (Medium)	admin		<input checked="" type="checkbox"/>
Recon - External - Potential Network Scan	admin		<input checked="" type="checkbox"/>
Recon - External - Scanning Activity (High)	admin		<input checked="" type="checkbox"/>
Recon - External - Scanning Activity (Low)	admin		<input checked="" type="checkbox"/>
Recon - External - Scanning Activity (Medium)	admin		<input checked="" type="checkbox"/>
Suspicious - External - Anomalous ICMP Flows	admin		<input checked="" type="checkbox"/>
Suspicious - External - Invalid TCP Flag Usage	admin		<input checked="" type="checkbox"/>
Suspicious - External - Outbound Unidirectional Flows Threshold	admin		<input checked="" type="checkbox"/>
Suspicious - External - Port 0 Flows Detected	admin		<input checked="" type="checkbox"/>
Suspicious - External - Rejected Communication Attempts	admin		<input checked="" type="checkbox"/>
Suspicious - External - Unidirectional ICMP Detected	admin		<input checked="" type="checkbox"/>
Suspicious - External - Unidirectional ICMP Responses Detected	admin		<input checked="" type="checkbox"/>
Suspicious - External - Unidirectional TCP Flows	admin		<input checked="" type="checkbox"/>
Suspicious - External - Unidirectional UDP or Misc Flows	admin		<input checked="" type="checkbox"/>

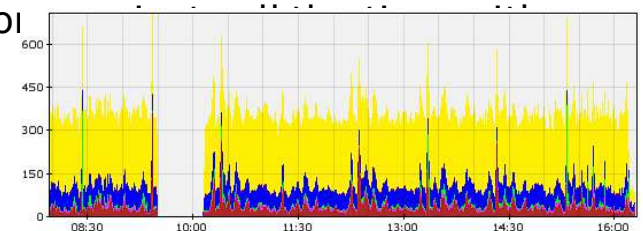
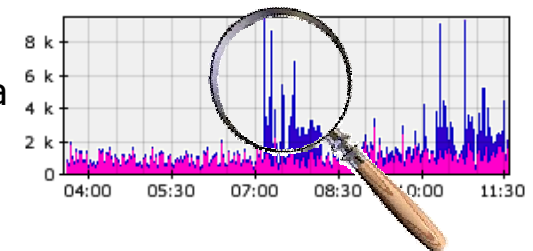
NBAD methods

- **Behavior sentries**

- Checks for **volume changes** in behavior that occurs in **regular seasonal patterns**
- If a behavior change occurs, an alarm will be generated
- Behavioral sentries can be deployed in environments with consistent or repetitive amounts of traffic
- Example: Typically a mail server communicates with 100 hosts in the night, suddenly it starts communicating with 1000 hosts instead

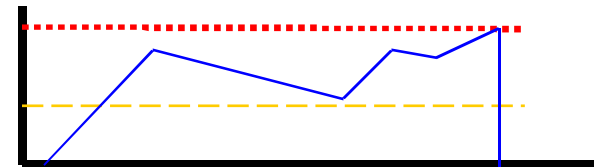
- **Anomaly sentries**

- Checks for **activity changes** of the entities **inside a view**
- Detects new or unknown traffic or changes in the amount of **time a**
- If an anomaly is detected, an alarm will be generated
- Behavioral sentry -> **volume based**
- Anomaly sentry -> **activity based** (% changes)
- Example: A monitored host inside a network would start to connect to external network instead of 16% of its time



- **Threshold sentries**

- Monitors traffic and objects that **exceeds a configured threshold**
- Useful for monitoring utilized bandwidth or number of clients connected to a server
- Example: Create an alert if more than 100 connections are established with a certain server in the network



- **Security/policy sentries**

- Monitors traffic inside a view for **policy violations** at network or application level
- Monitors for violations of usage policies
- If any traffic is detected, that meets the sentry criteria, an alarm will be generated
- The security/policy sentry is a **derivate of the threshold sentry but with a threshold of one**
- Example: A user attempts to make a SSH connection to a server, which he is not entitled to do

- **Custom sentries**





"There is nothing more important
than our customers"

A handwritten signature in black ink, appearing to read 'myself'.

Real data
Some examples from customer

VoIP – non local traffic

Dragon - Network Surveillance - Mozilla Firefox

https://10.150.17.5/console/qradar/jsp/QRadar.jsp

Dragon Security Command Console

Welcome, admin

Dashboard | Offense Manager | Event Viewer | Assets | Network Surveillance | Flow Viewer | Reports

Dragon Time: 14:00 | CONFIG | HELP | LOGOUT

Global Views | Asset Map | Bookmarks | QRL Options | Time Until Refresh: 178

Pivot To

- Base Views
 - Applications
 - Client | Server
 - Threats
 - Geographic
 - Flow Types
 - Collector
- Custom Views
 - FlowShape

Layers

- Bytes/Second
 - Normal
 - Log
 - Bits/Second
 - Bytes/Packet
 - Bytes/Host
 - 1/X
- Packets/Second
- Number of Hosts
- Unique Ports

View Flows

View Flows Search

Inbound Bytes (Normal)

Scale (A|+)- Thursday, Apr 16, 2009 Size (A|+)-




VoIP_Networks - 172.17.0.0/16...
No Sub-components

Select Time: Current: 167
Time Period: Now

◀ Add Sentry ▶

Outbound Bytes (Normal)

Scale (A|+)- Thursday, Apr 16, 2009 Size (A|+)-



VoIP_Networks-172.17.0.0/16...
No Sub-components

Select Time: Current: 167
Time Period: Now

◀ Add Sentry ▶

QRL Definition

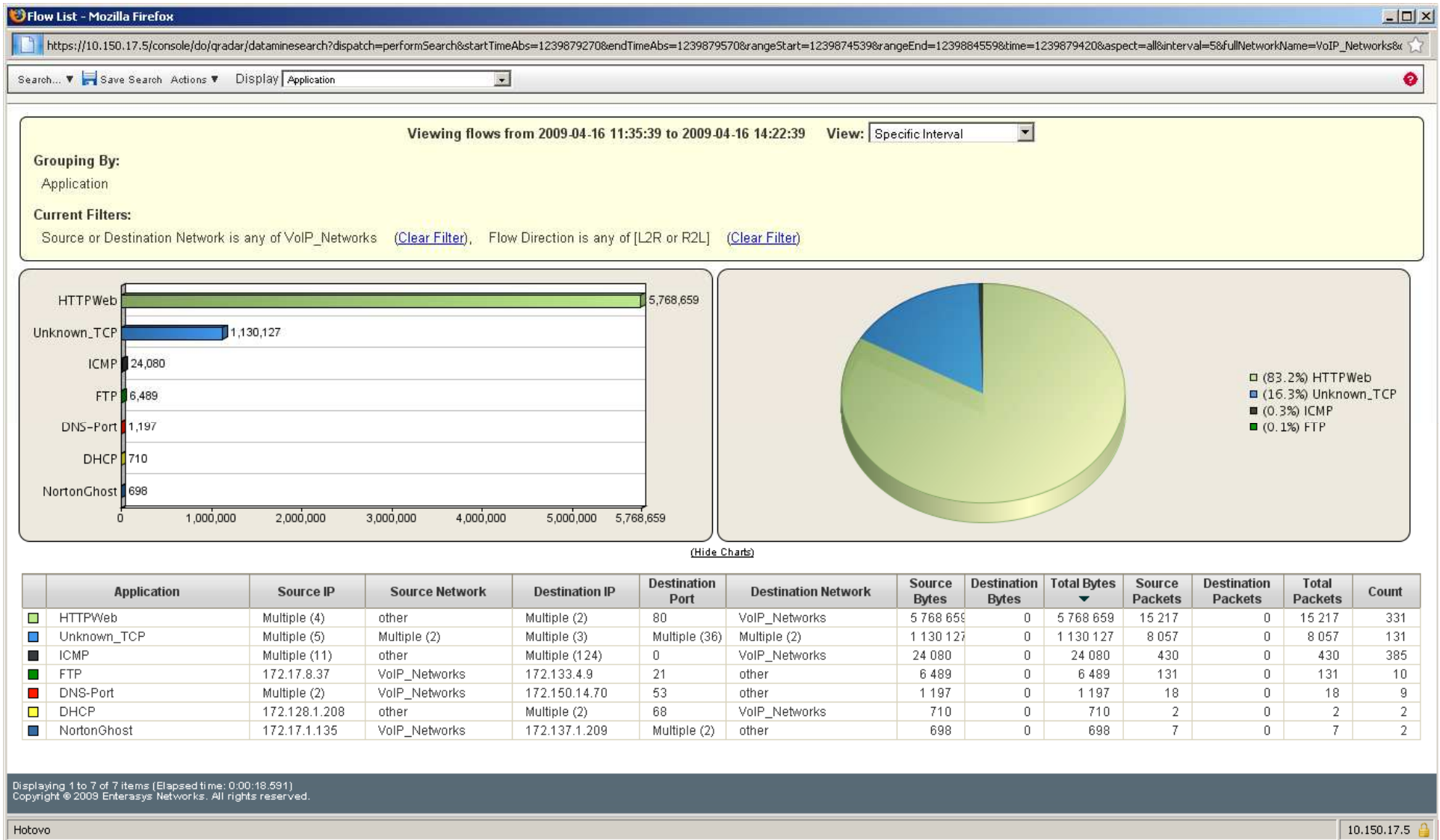
View: nets
Layer: bytes
Derived Layer: Normal
Direction: all

Networks: (All)
VoIP_Networks

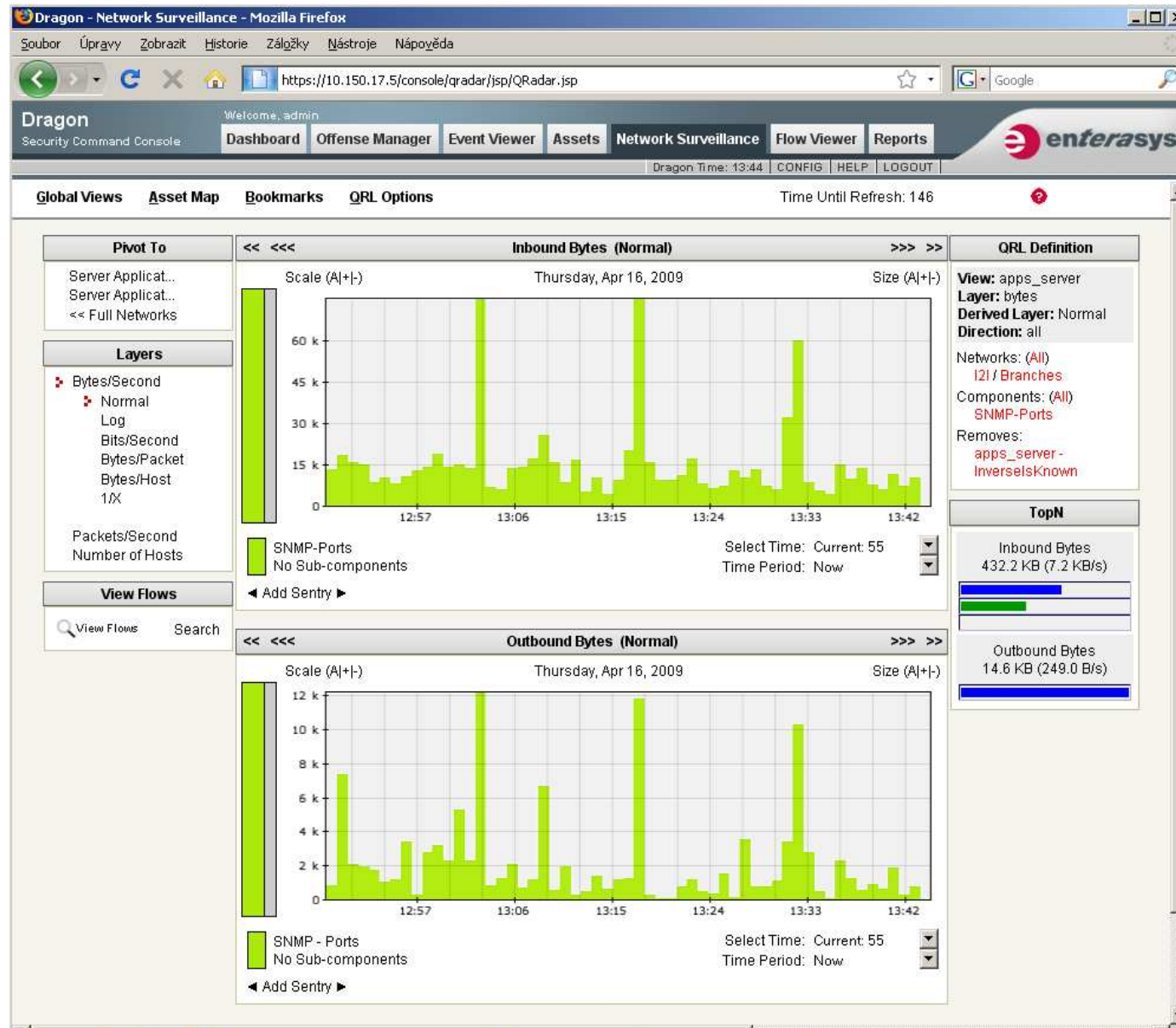
Components:
All

Removes:
None

What applications VoIP talking non local



Snmp traffic



SNMP talkers



Flow List - Mozilla Firefox

https://10.150.17.5/console/do/qadar/dataminesearch?dispatch=performSearch&startTimeAbs=1239880470&endTimeAbs=1239880770&rangeStart=1239880412&rangeEnd=1239880812&time=1239880620&aspect=all&intl

Search... Save Search Actions Display Source or Destination IP

Viewing flows from 2009-04-16 13:13:32 to 2009-04-16 13:18:32 (Slice 2 of 3) (First | Previous | View All | Next | Last) (Duration is 5m) View: Real Time (auto refresh)

Grouping By: IP

Current Filters: Source or Destination Network is any of Branches (Clear Filter), Flow Direction is any of L2L (Clear Filter), Application is any of Misc.SNMP-Ports (Clear Filter)

IP	Total Bytes
10.150.17.8	4,800,645
10.150.17.10	2,935,675
172.17.199.1	1,196,824
10.184.207.13	1,055,796
10.150.17.14	335,524
10.185.63.86	198,525
10.164.16.42	183,281
10.150.66.98	176,147
10.164.240.18	168,636
10.164.240.50	166,888

IP	Percentage
10.150.17.8	42.8%
10.150.17.10	26.2%
172.17.199.1	10.7%
10.184.207.13	9.4%
10.150.17.14	3.0%
10.185.63.86	1.8%
10.164.16.42	1.6%
10.150.66.98	1.6%
10.164.240.18	1.5%
10.164.240.50	1.5%

(Hide Charts)

	IP	Bytes In	Bytes Out	Total Bytes ▼	Packets In	Packets Out	Total Packets	Host Count	Count
	10.150.17.8	653 161	4 147 484	4 800 645	2 107	13 078	15 185	195	195
	10.150.17.10	889 821	2 045 854	2 935 675	6 860	14 142	21 002	457	1 879
	172.17.199.1	569 756	627 068	1 196 824	5 266	5 266	10 532	1	11
	10.184.207.13	260 962	794 834	1 055 796	3 454	10 732	14 186	93	176
	10.150.17.14	0	335 524	335 524	0	941	941	2	2
	10.185.63.86	198 525	0	198 525	1 248	0	1 248	1	11
	10.164.16.42	183 281	0	183 281	1 749	0	1 749	1	23
	10.150.66.98	0	176 147	176 147	0	1 782	1 782	2	10
	10.164.240.18	168 636	0	168 636	473	0	473	1	1
	10.164.240.50	166 888	0	166 888	468	0	468	1	1
	10.184.166.250	64 707	72 486	137 193	636	638	1 274	1	11

Displaying 1 to 40 of 833 items (Elapsed time: 0:00:00.875)
Copyright © 2009 Enterasys Networks. All rights reserved.

Page: 1 Go << 1 | 2 | 3 | ... | 21 >>

Hotovo 10.150.17.5

SNMP anomaly?



Dragon - Flow Viewer - Mozilla Firefox

Soubor Úpravy Zobrazit Historie Záložky Nástroje nápověda

https://10.150.17.5/console/qradar/jsp/QRadar.jsp

Dragon Security Command Console

Welcome, admin

Dashboard Offense Manager Event Viewer Assets Network Surveillance **Flow Viewer** Reports

Dragon Time: 10:57 CONFIG HELP LOGOUT

Search... Save Search Actions Display Source or Destination IP

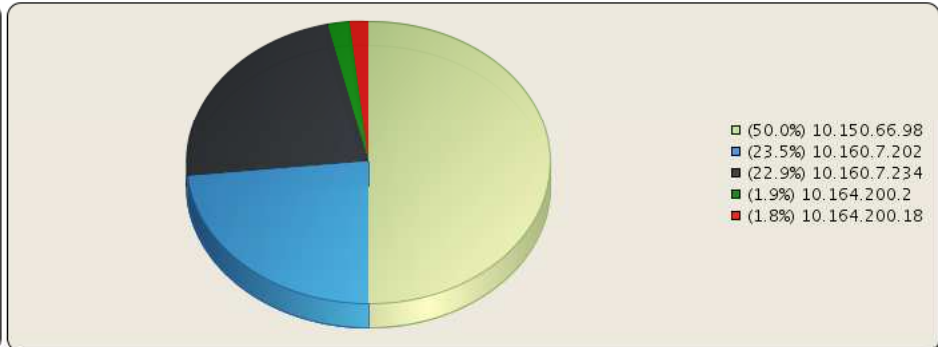
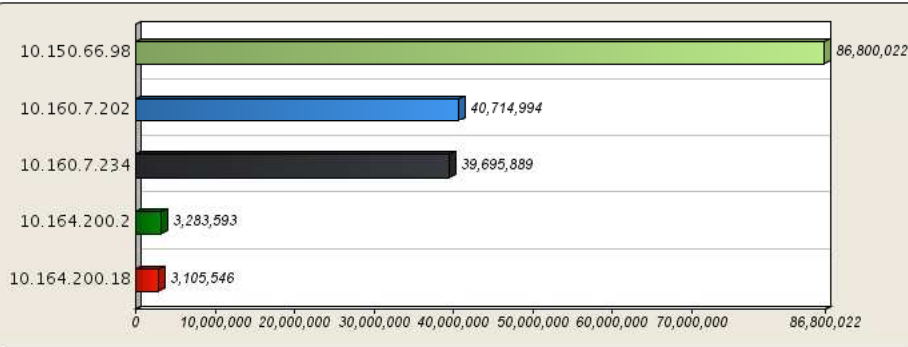
Viewing flows from 2009-04-16 07:48:00 to 2009-04-16 10:48:00 View: Last 3 Hours

Grouping By:

IP

Current Filters:

Protocol is UDP (Clear Filter), Source or Destination IP is 10.150.66.98 (Clear Filter), Source or Destination Port is 161 (Clear Filter)



(Hide Charts)

	IP	Bytes In	Bytes Out	Total Bytes ▼	Packets In	Packets Out	Total Packets	Host Count	Count
■	10.150.66.98	80 410 883	6 389 139	86 800 022	66 059	64 602	130 661	4	723
■	10.160.7.202	0	40 714 994	40 714 994	0	33 566	33 566	1	178
■	10.160.7.234	0	39 695 889	39 695 889	0	32 493	32 493	1	179
■	10.164.200.2	3 283 593	0	3 283 593	33 347	0	33 347	1	183
■	10.164.200.18	3 105 546	0	3 105 546	31 255	0	31 255	1	183

Detail of SNMP communication

Dragon - Flow Viewer - Mozilla Firefox

https://134.141.1.231/console/qradar/jsp/QRadar.jsp

Dragon Security Command Console

Dashboard | Offense Manager | Event Viewer | Assets | Network Surveillance | **Flow Viewer** | Reports

Dragon Time: 15:24 | TOOLS | HELP | LOGOUT

Return To Results | Print

Flow Type:	Standard Flow	Protocol:	udp_ip
Flow Direction:	L2L		
Source IP:	10.120.84.203	Destination IP:	10.120.86.10
IPv6 Source:	::	IPv6 Destination:	::
Source Port:	1064	Destination Port:	161
Flow Source:	dsc	Flow Interface:	eth1
Source QoS:	Best Effort	Destination QoS:	Best Effort
Source ASN:	0	Destination ASN:	0
Source If Index:	0	Destination If Index:	0
Start Time:	2009-05-18 15:20:30	Application:	SNMP-Ports
End Time:	2009-05-18 15:20:30	Custom Views:	PolicyViolations.Unknown_Local_Service FlowShape.NearSame_Internal

Source Payload
2 packets, 353 bytes

UTF | Hex | Base64

```
.....806.....~.....?...DN..cse-ets..V.....J*..R...?w...x
G.?N.....<w0...<i..m..
```

Destination Payload
2 packets, 493 bytes

UTF | Hex | Base64

```
..0.....~.....?...DN...0/.....~.....a*....0.0..
.0...Ph...806.....~.....?...DN..cse-ets...}....+k3..
!I.g.n7..Y..?.....x.q....K...@..R.PWc2 a....g...<J--m9.w..
lc7...L*.V.x...~...gH...K.a...xt..IF.....d...+...E...
```

Copyright © 2009 Enterasys Networks. All rights reserved.

Hotovo | 134.141.1.231

Dragon - Flow Viewer - Mozilla Firefox

https://10.150.17.5/console/qadar/jsp/QRadar.jsp

Dragon Security Command Console

Welcome, admin

Dashboard | **Offense Manager** | Event Viewer | Assets | Network Surveillance | **Flow Viewer** | Reports

Dragon Time: 11:09 | CONFIG | HELP | LOGOUT

Search... Save Search Actions Display Source or Destination IP

Viewing flows from 2009-04-15 11:06:00 to 2009-04-16 11:06:00 View: Last 24 Hours

Grouping By: IP

Current Filters: Protocol is TCP (Clear Filter), Source or Destination Port is 22 (Clear Filter)

IP	Bytes
10.150.75.232	738,260,041
10.160.4.10	213,373,296
10.160.4.11	205,476,920
10.160.4.21	181,760,132
10.160.4.20	156,041,812
10.188.10.103	18,455,140
10.150.33.11	16,681,889
10.150.17.5	16,681,889
172.133.4.66	14,330,575
172.137.1.159	10,873,018

IP	Percentage
10.150.75.232	47.0%
10.160.4.10	13.6%
10.160.4.11	13.1%
10.160.4.21	11.6%
10.160.4.20	9.9%
10.188.10.103	1.2%
10.150.33.11	1.1%
10.150.17.5	1.1%
172.133.4.66	0.9%
172.137.1.159	0.7%

(Hide Charts)

IP	Bytes In	Bytes Out	Total Bytes	Packets In	Packets Out	Total Packets	Host Count	Count
10.150.75.232	738 260 041	0	738 260 041	532 756	0	532 756	5	89
10.160.4.10	0	213 373 296	213 373 296	0	153 891	153 891	2	17
10.160.4.11	0	205 476 920	205 476 920	0	148 163	148 163	1	24
10.160.4.21	0	181 760 132	181 760 132	0	131 082	131 082	1	24
10.160.4.20	0	156 041 812	156 041 812	0	112 585	112 585	1	24
10.188.10.103	18 455 140	0	18 455 140	13 506	0	13 506	1	1
10.150.33.11	16 047 915	633 974	16 681 889	10 255	8 872	19 127	1	5
10.150.17.5	633 974	16 047 915	16 681 889	8 872	10 255	19 127	1	5

Displaying 1 to 40 of 110 items (Elapsed time: 0:01:15.360)
Copyright © 2009 Enterasys Networks. All rights reserved.

Page: 1 Go << 1 | 2 | 3 >>

Hotovo 10.150.17.5

Whom was he talking ssh?

Dragon - Flow Viewer - Mozilla Firefox

https://10.150.17.5/console/qradar/jsp/QRadar.jsp

Welcome, admin

Dragon Security Command Console

Dashboard | **Offense Manager** | Event Viewer | Assets | Network Surveillance | Flow Viewer | Reports

Dragon Time: 14:16 | CONFIG | HELP | LOGOUT

Search... Save Search Actions Display Source or Destination IP

Viewing flows from 2009-04-15 11:01:00 to 2009-04-16 10:13:00 View: Specific Interval

Grouping By: IP

Current Filters: Protocol is TCP (Clear Filter), Source or Destination IP is 10.150.75.232 (Clear Filter), Source or Destination Port is 22 (Clear Filter)

(Hide Charts)

	IP	Bytes In	Bytes Out	Total Bytes	Packets In	Packets Out	Total Packets	Host Count	Count
	10.150.75.232	738 260 041	0	738 260 041	532 756	0	532 756	5	89
	10.160.4.11	0	205 476 920	205 476 920	0	148 163	148 163	1	24
	10.160.4.10	0	194 918 156	194 918 156	0	140 385	140 385	1	16
	10.160.4.21	0	181 760 132	181 760 132	0	131 082	131 082	1	24
	10.160.4.20	0	156 041 812	156 041 812	0	112 585	112 585	1	24
	172.128.99.21	0	63 021	63 021	0	541	541	1	1

Displaying 1 to 6 of 6 items (Elapsed time: 0:00:21.741)
Copyright © 2009 Enterasys Networks. All rights reserved.

HTTP profile to servers

Dragon - Network Surveillance - Mozilla Firefox

Soubor Úpravy Zobrazit Historie Záložky Nástroje nápověda

https://10.150.17.5/console/qradar/jsp/QRadar.jsp

Dragon Security Command Console

Welcome, admin

Dashboard Offense Manager Event Viewer Assets Network Surveillance Flow Viewer Reports

Dragon Time: 15:41 CONFIG HELP LOGOUT

Global Views Asset Map Bookmarks QRL Options

Pivot To

- Server Applicat...
- Server Applicat...
- << Full Networks

Layers

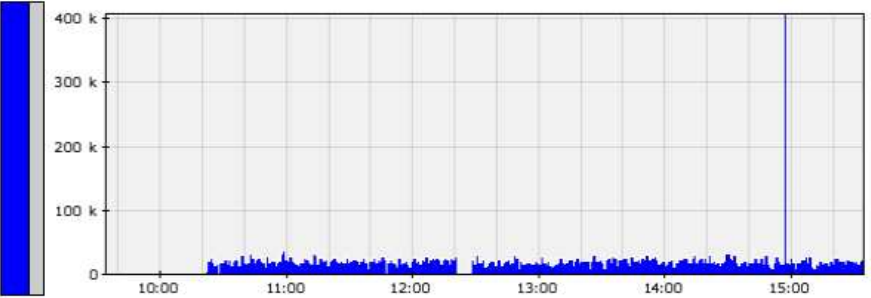
- Bytes/Second
 - Normal
 - Log
 - Bits/Second
 - Bytes/Packet
 - Bytes/Host
 - 1/X
- Packets/Second
- Number of Hosts

View Flows

View Flows Search

Inbound Bytes (Normal)

Scale (A|+)- Thursday, Apr 16, 2009 Size (A|+)-



400 k
300 k
200 k
100 k
0

10:00 11:00 12:00 13:00 14:00 15:00

HTTPWeb
No Sub-components

Select Time: Current: 360
Time Period: 6 Hours

QRL Definition

View: apps_server
Layer: bytes
Derived Layer: Normal
Direction: all

Networks: (All)
Server_Network

Components: (All)
HTTPWeb

Removes:
apps_server -
InverselsKnown

TopN

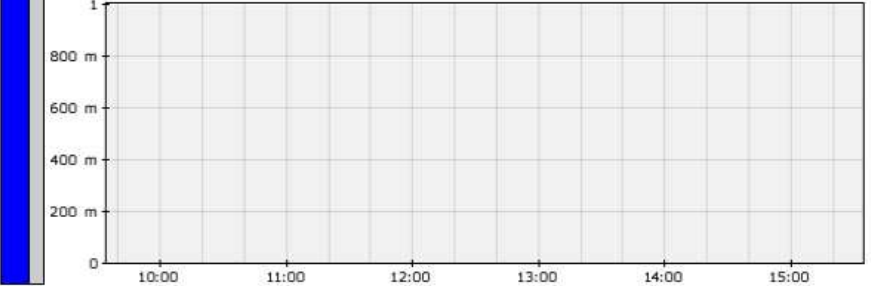
Inbound Bytes
787.3 KB (13.1 KB/s)

Outbound Bytes
0 (0)

No activity

Outbound Bytes (Normal)

Scale (A|+)- Thursday, Apr 16, 2009 Size (A|+)-



1
800 m
600 m
400 m
200 m
0

10:00 11:00 12:00 13:00 14:00 15:00

HTTPWeb
No Sub-components

Select Time: Current: 360
Time Period: 6 Hours

HTTP traffic to servers

Dragon - Network Surveillance - Mozilla Firefox

Soubor Úpravy Zobrazit Historie Záložky Nástroje nápověda

https://10.150.17.5/console/qradar/jsp/QRadar.jsp

Dragon Security Command Console

Welcome, admin

Dashboard Offense Manager Event Viewer Assets Network Surveillance Flow Viewer Reports

Dragon Time: 15:40 CONFIG HELP LOGOUT

Global Views Asset Map Bookmarks QRL Options

Pivot To

- Server Applicat...
- Server Applicat...
- << Full Networks

Layers


- Bytes/Second
 - Normal
 - Log
 - Bits/Second
 - Bytes/Packet
 - Bytes/Host
 - 1/X
- Packets/Second
- Number of Hosts

View Flows

View Flows Search

Inbound Bytes (Normal)

Scale (A|+)- Thursday, Apr 16, 2009 Size (A|+)-



400 k
300 k
200 k
100 k
0

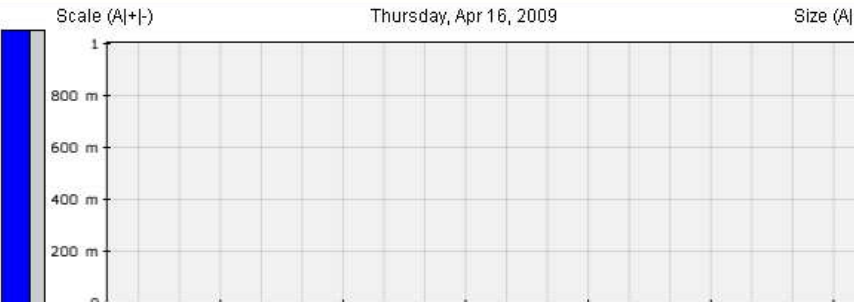
14:36 14:45 14:54 15:03 15:12 15:21

HTTPWeb
No Sub-components

Select Time: Current: 55
Time Period: Now

Outbound Bytes (Normal)

Scale (A|+)- Thursday, Apr 16, 2009 Size (A|+)-



1
800 m
600 m
400 m
200 m
0

14:36 14:45 14:54 15:03 15:12 15:21

HTTPWeb
No Sub-components

Select Time: Current: 55
Time Period: Now

QRL Definition

View: apps_server
Layer: bytes
Derived Layer: Normal
Direction: all

Networks: (All)
Server_Network

Components: (All)
HTTPWeb

Removes:
apps_server -
InverselsKnown

TopN

Inbound Bytes
747.1 kB (12.5 KB/s)

Outbound Bytes
0 (0)

No activity

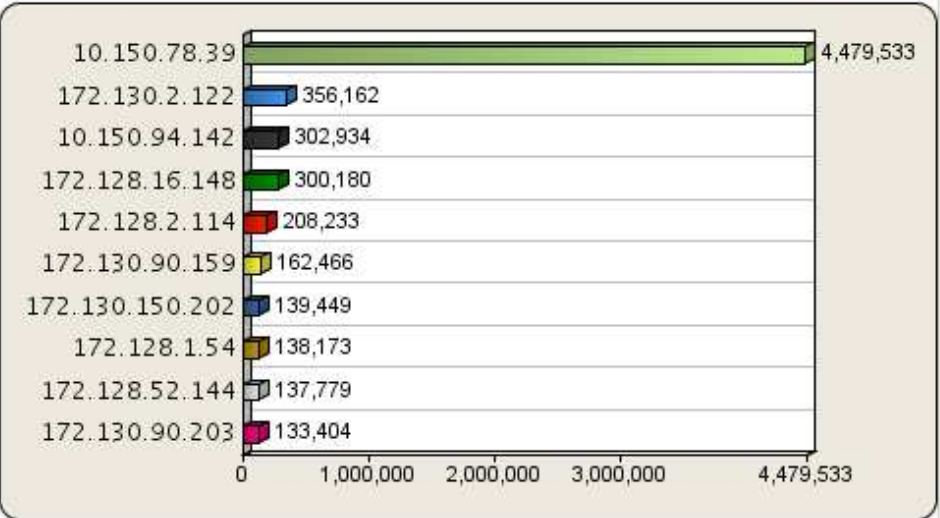
Hotovo 10.150.17.5 16

Comparison

Viewing flows from 2009-04-16 14:50:32 to 2009-04-16 14:55:32 (Slice 2 of 2) Real Time (a)

Grouping By:
IP

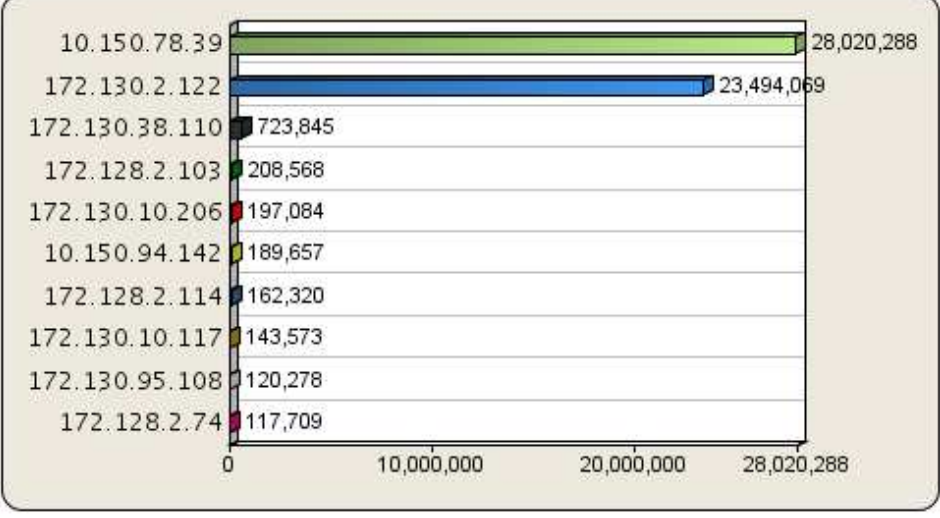
Current Filters:
Source or Destination Network is any of Server_Network [\(Clear Filter\)](#), Flow Application is any of Web.HTTPWeb [\(Clear Filter\)](#)



Viewing flows from 2009-04-16 14:55:32 to 2009-04-16 15:00:32 (Slice 3 of 3) Real Time (a)

Grouping By:
IP

Current Filters:
Source or Destination Network is any of Server_Network [\(Clear Filter\)](#), Flow Application is any of Web.HTTPWeb [\(Clear Filter\)](#)



UDP/TCP port 0



Dragon - Network Surveillance - Mozilla Firefox

https://10.150.17.5/console/qradar/jsp/QRadar.jsp

Dragon Security Command Console

Welcome, admin

Dashboard | Offense Manager | Event Viewer | Assets | Network Surveillance | Flow Viewer | Reports

Dragon Time: 08:02 | CONFIG | HELP | LOGOUT

Global Views | Asset Map | Bookmarks | QRL Options

Time Until Refresh: 148

Pivot To	Inbound Bytes (Normal)	QRL Definition
Threats by Network Threats << Full Networks	Scale (A +/-) Thursday, Apr 16, 2009 - Friday, Apr 17, 2009 Size (A +/-)	View: Threats Layer: bytes Derived Layer: Normal Direction: all
Layers Bytes/Second Normal Log Bits/Second Bytes/Packet Bytes/Host 1/x		Networks: All Components: (All) Tcp_Udp_Port_0 Removes: Threats - other
Packets/Second Number of Hosts	Select Time: Current: 501 Time Period: Now	TopN Inbound Bytes 267 B (4.4 B/s)
View Flows	◀ View Sentries (48) ▶ ▶ Add Sentry ▶	Outbound Bytes 0 (0)

Hotovo

10.150.17.5

UDP/TCP port 0 top talkers

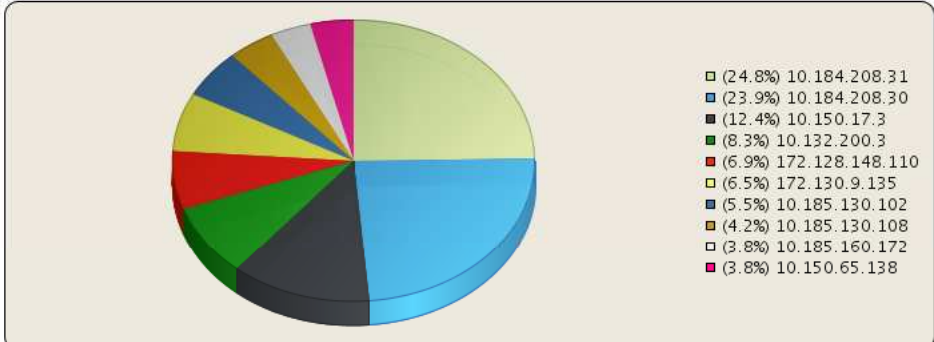
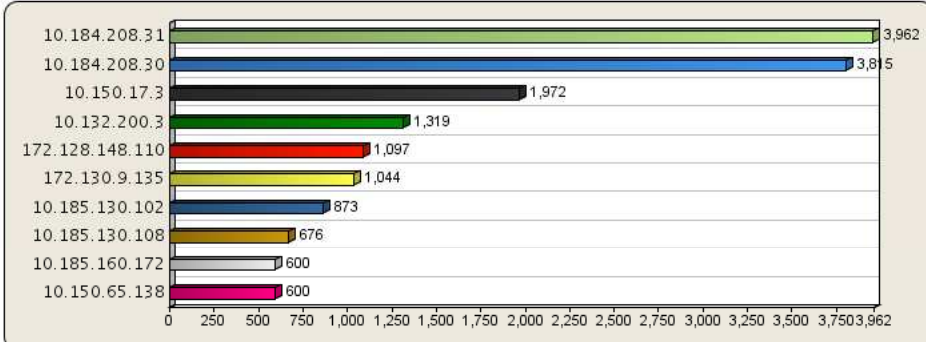
Flow List - Mozilla Firefox
 https://10.150.17.5/console/do/qradar/dataminesearch?dispatch=performSearch&startTimeAbs=1239946710&endTimeAbs=1239947010&rangeStart=1239918215&rangeEnd=1239948275&time=1239946860&aspect=all&interval=5&fullNetworkName=all&qrl=network%3Dall%3Bnets

Search... Save Search Actions Display Source or Destination IP

Viewing flows from 2009-04-16 23:43:35 to 2009-04-17 08:04:35 View: Specific Interval

Grouping By: IP

Current Filters: Matches custom view is any of Threats - Suspicious_IP_Protocol_Usage.Tcp_Udp_Port_0 (Clear Filter), Does not match custom view is Threats - other (Clear Filter)



(Hide Charts)

IP	Bytes In	Bytes Out	Total Bytes	Packets In	Packets Out	Total Packets	Host Count	Count
10.184.208.31	3 962	0	3 962	81	0	81	14	37
10.184.208.30	3 815	0	3 815	101	0	101	18	50
10.150.17.3	1 972	0	1 972	17	0	17	5	5
10.132.200.3	1 319	0	1 319	16	0	16	2	9
172.128.148.110	0	1 097	1 097	0	10	10	1	5
172.130.9.135	0	1 044	1 044	0	9	9	1	1
10.185.130.102	0	873	873	0	8	8	1	3
10.185.130.108	0	676	676	0	6	6	1	1
10.185.160.172	0	600	600	0	5	5	1	5
10.150.65.138	600	0	600	5	0	5	1	5
10.184.170.24	0	518	518	0	13	13	2	3
172.130.9.33	0	464	464	0	4	4	1	1
10.185.162.228	0	455	455	0	13	13	1	5

Displaying 1 to 40 of 52 items (Elapsed time: 0:00:04.770)
 Copyright © 2009 Enterasys Networks. All rights reserved.

Suspicious ICMP



Dragon - Network Surveillance - Mozilla Firefox

Soubor Úpravy Zobrazit Historie Záložky Nástroje nápověda

https://10.150.17.5/console/qradar/jsp/QRadar.jsp

Dragon Security Command Console

Welcome, admin

Dashboard Offense Manager Event Viewer Assets Network Surveillance Flow Viewer Re

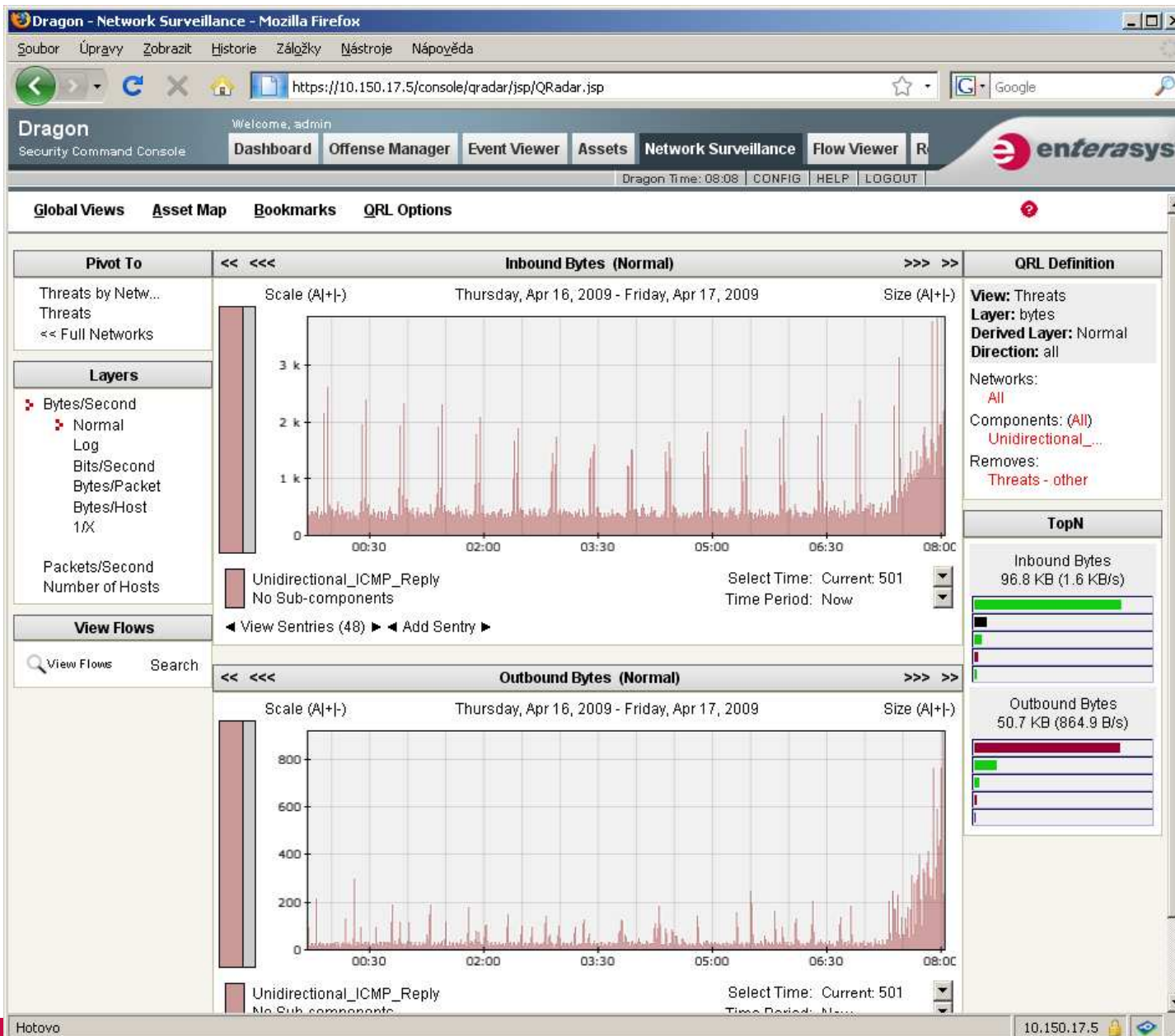
Dragon Time: 08:06 CONFIG HELP LOGOUT

Global Views Asset Map Bookmarks QRL Options Time Until Refresh: 175

Pivot To	<< <<<	Inbound Bytes (Normal)	>>> >>	QRL Definition
Threats by Netw... Threats << Full Networks		Scale (A +)- Friday, Apr 17, 2009 Size (A +)-		View: Threats Layer: bytes Derived Layer: Normal Direction: all Networks: All Components: (All) Suspicious_ICMP... Removes: Threats - other
Layers Bytes/Second Normal Log Bits/Second Bytes/Packet Bytes/Host 1/X				TopN Inbound Bytes 0 (0) No activity
Packets/Second Number of Hosts		◀ View Sentries (48) ▶ ◀ Add Sentry ▶	Select Time: Current: 167 Time Period: Now	Outbound Bytes

Hotovo 10.150.17.5

ICMP replies without request



The screenshot displays the Dragon Network Surveillance interface in Mozilla Firefox. The browser address bar shows the URL `https://10.150.17.5/console/qradar/jsp/QRadar.jsp`. The interface includes a navigation menu with options like Dashboard, Offense Manager, Event Viewer, Assets, Network Surveillance, and Flow Viewer. The main content area is divided into several sections:

- Pivot To:** Threats by Network, Threats, Full Networks.
- Layers:** Bytes/Second (selected), Normal, Log, Bits/Second, Bytes/Packet, Bytes/Host, 1/X, Packets/Second, Number of Hosts.
- View Flows:** View Flows, Search.

The central part of the interface features two line graphs:

- Inbound Bytes (Normal):** A line graph showing traffic volume from Thursday, Apr 16, 2009, to Friday, Apr 17, 2009. The Y-axis is labeled 'Scale (A|+)' and ranges from 0 to 3k. The X-axis shows time intervals from 00:30 to 08:00. The graph shows a series of sharp peaks, indicating periodic traffic bursts. A legend below the graph identifies the data as 'Unidirectional_ICMP_Reply' with 'No Sub-components'. Below the graph, it says 'View Sentries (48)' and 'Add Sentry'.
- Outbound Bytes (Normal):** A similar line graph showing outbound traffic volume for the same period. The Y-axis is labeled 'Scale (A|+)' and ranges from 0 to 800. It also shows periodic peaks and is identified as 'Unidirectional_ICMP_Reply'.

On the right side, there is a 'QRL Definition' panel with the following details:

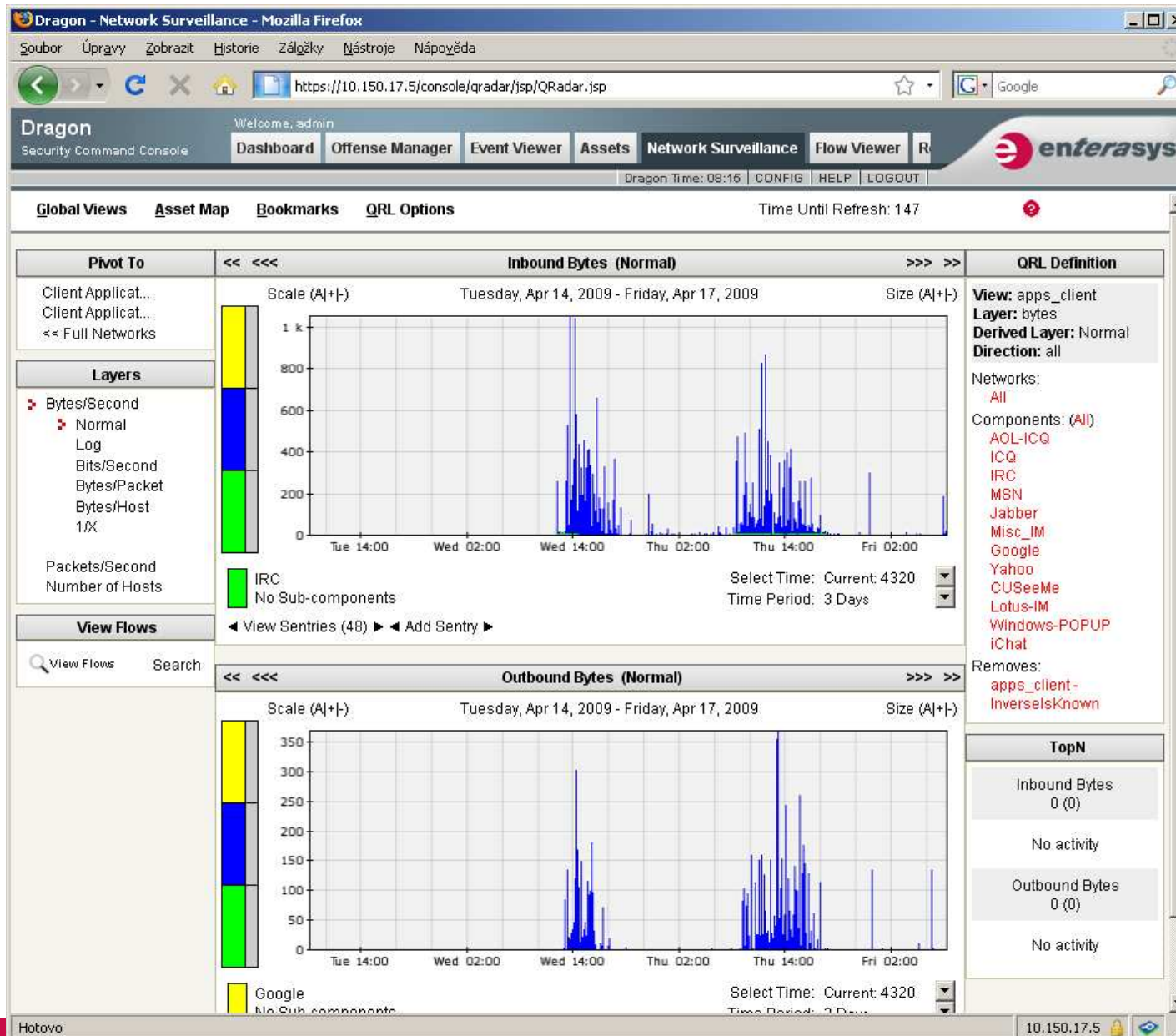
- View:** Threats
- Layer:** bytes
- Derived Layer:** Normal
- Direction:** all
- Networks:** All
- Components:** (All), Unidirectional_...
- Removes:** Threats - other

Below the QRL Definition is a 'TopN' section with two bar charts:

- Inbound Bytes:** 96.8 KB (1.6 KB/s)
- Outbound Bytes:** 50.7 KB (864.9 B/s)

The bottom status bar of the browser shows 'Hotovo' on the left and '10.150.17.5' on the right.

Chatting applications



The screenshot displays the Dragon Network Surveillance interface in Mozilla Firefox. The main content area is divided into two sections: "Inbound Bytes (Normal)" and "Outbound Bytes (Normal)". Both sections show line graphs for the period from Tuesday, Apr 14, 2009, to Friday, Apr 17, 2009. The Inbound Bytes graph has a scale of 0 to 1000, while the Outbound Bytes graph has a scale of 0 to 350. Both graphs show significant activity spikes around 14:00 on Wednesday and Thursday. The interface includes a left sidebar with "Layers" (Bytes/Second, Normal, Log, etc.) and "View Flows" (View Flows, Search). The right sidebar shows "QRL Definition" (View: apps_client, Layer: bytes, etc.) and "TopN" (Inbound Bytes 0 (0), Outbound Bytes 0 (0)). The bottom status bar shows "Hotovo" and the IP address "10.150.17.5".

P2P applications

Dragon - Network Surveillance - Mozilla Firefox

Soubor Úpravy Zobrazit Historie Záložky Nástroje Nápověda

https://10.150.17.5/console/qradar/jsp/QRadar.jsp

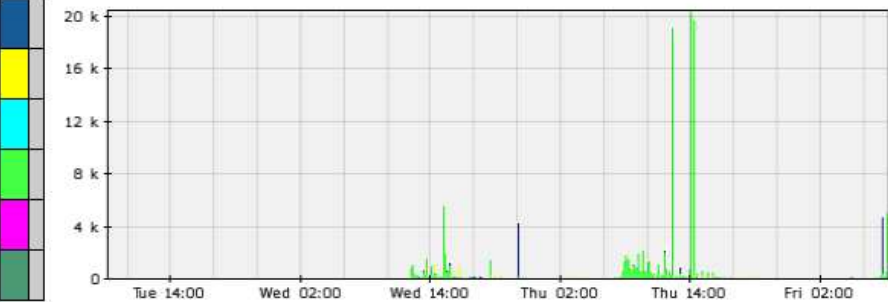
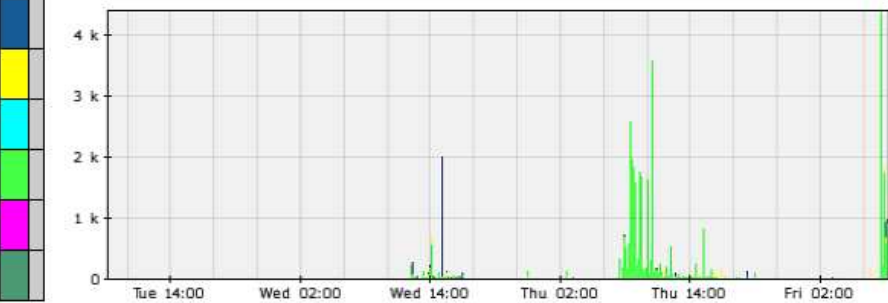
Welcome, admin

Dragon Security Command Console

Dashboard Offense Manager Event Viewer Assets Network Surveillance Flow Viewer R

Dragon Time: 08:16 CONFIG HELP LOGOUT

Global Views Asset Map Bookmarks QRL Options Time Until Refresh: 154

Pivot To	<< <<<	Inbound Bytes (Normal)	>>> >>	QRL Definition
Client Applicat... Client Applicat... << Full Networks		Scale (A +)- Tuesday, Apr 14, 2009 - Friday, Apr 17, 2009 Size (A +)-		View: apps_client Layer: bytes Derived Layer: Normal Direction: all Networks: All Components: (All) BitTorrent Blubster Gnutella Kazaa OpenNap PeerEnabler Piolet eDonkey DirectConnect Common-P2P-Port LimeWire GnuCieusLan Morpheus Napster ScourExchange iMesh Audiogalaxy Aimster Groove Tripnosis Hotline FileRogue Furthurmet Filetopia Napster2 EarthStationV Soulseek Removes: apps_client - InverselsKnown
Layers Bytes/Second Normal Log Bits/Second Bytes/Packet Bytes/Host 1/X Packets/Second Number of Hosts				
View Flows View Flows Search		Outbound Bytes (Normal) Scale (A +)- Tuesday, Apr 14, 2009 - Friday, Apr 17, 2009 Size (A +)-		
				

Hotovo

10.150.17.5

P2P applications used

Dragon - Flow Viewer - Mozilla Firefox

https://10.150.17.5/console/qradar/jsp/QRadar.jsp

Dragon Security Command Console

Dashboard | Offense Manager | Event Viewer | Assets | Network Surveillance | **Flow Viewer** | Reports

Dragon Time: 08:31 | CONFIG | HELP | LOGOUT

Search... Save Search Actions Display Application

Viewing flows from 2009-04-17 02:31:00 to 2009-04-17 08:31:00 View: Last 6 Hours

Grouping By: Application

Current Filters: Application is any of P2P (Clear Filter)

Application	Bytes
Kazaa	27,187,886
Common-P2P-Port	2,488,327
PeerEnabler	517,220
Blubster	2,405
OpenNap	40
BitTorrent	40

(Hide Charts)

Application	Source IP	Source Network	Destination IP	Destination Port	Destination Network	Source Bytes	Destination Bytes	Total B
Kazaa	Multiple (104)	Multiple (17)	Multiple (767)	1214	Multiple (7)	26 898 29	289 590	27 18
Common-P2P-Port	Multiple (22)	Multiple (9)	Multiple (28)	4662	Multiple (8)	305 884	2 182 443	2 488
PeerEnabler	Multiple (17)	Multiple (10)	Multiple (30)	3531	Multiple (7)	517 220	0	517
Blubster	Multiple (3)	Multiple (2)	Multiple (3)	41170	Multiple (2)	2 405	0	2

Displaying 1 to 6 of 6 items (Elapsed time: 0:00:09.624)
Copyright © 2009 Enterasys Networks. All rights reserved.

Hotovo 10.150.17.5

Streaming

Dragon - Network Surveillance - Mozilla Firefox

https://10.150.17.5/console/qradar/jsp/QRadar.jsp

Dragon Security Command Console

Welcome, admin

Dashboard | Offense Manager | Event Viewer | Assets | Network Surveillance | Flow Viewer | R

Dragon Time: 08:18 | CONFIG | HELP | LOGOUT

Global Views | Asset Map | Bookmarks | QRL Options

Pivot To

- Client Applicat...
- Client Applicat...
- << Full Networks

Layers

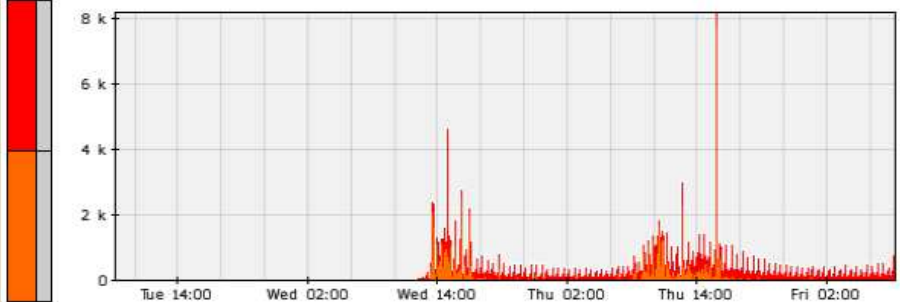
- Bytes/Second
 - Normal
 - Log
 - Bits/Second
 - Bytes/Packet
 - Bytes/Host
 - 1/X
- Packets/Second
- Number of Hosts

View Flows

View Flows Search

Inbound Bytes (Normal)

Scale (A|+)- Tuesday, Apr 14, 2009 - Friday, Apr 17, 2009 Size (A|+)-

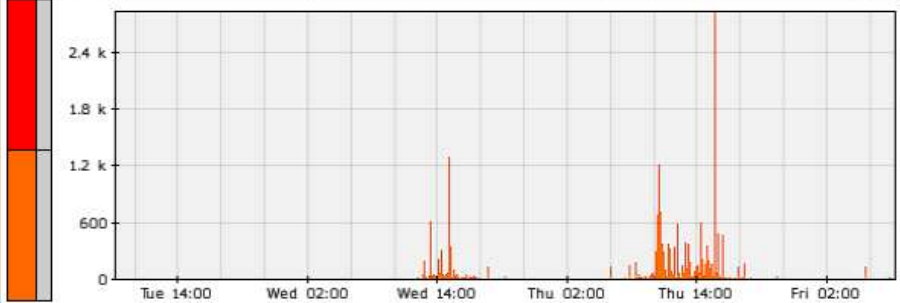


MicrosoftMediaServer
No Sub-components

Select Time: Current: 4320
Time Period: 3 Days

Outbound Bytes (Normal)

Scale (A|+)- Tuesday, Apr 14, 2009 - Friday, Apr 17, 2009 Size (A|+)-



StreamingAudio
No Sub-components

Select Time: Current: 4320
Time Period: 3 Days

QRL Definition

View: apps_client
Layer: bytes
Derived Layer: Normal
Direction: all

Networks:
All

Components: (All)

- MicrosoftMediaS...
- StreamingAudio
- WindowsMediaPla...
- Real
- StreamWorks
- WinMedia
- ST2
- MPEG-Audio
- MPEG-Video
- WinampStream
- Abacast
- RadioNetscape
- Motion
- H.263
- H.262
- H.261
- RTP-Skinny
- RTSP

Removes:
apps_client -
InverselsKnown

TopN

Hotovo

10.150.17.5

Others default detected anomalies

- HostScans
- TCPPortScan
- UDPPortScan
- Suspicious_ICMP_Type_Code
- Tcp_Udp_Port_0
- Large_DNS_Packets
- Long_Duration_Flow
- Zero_Payload_Bidirectional_Flows
- Unidirectional_UDP_and_misc_Flows
- Unidirectional_ICMP_Flows
- Unidirectional_ICMP_Reply
- Unidirectional_TCP_Flows
- Illegal_TCP_Flag_Combination
- Large_ICMP_Packets



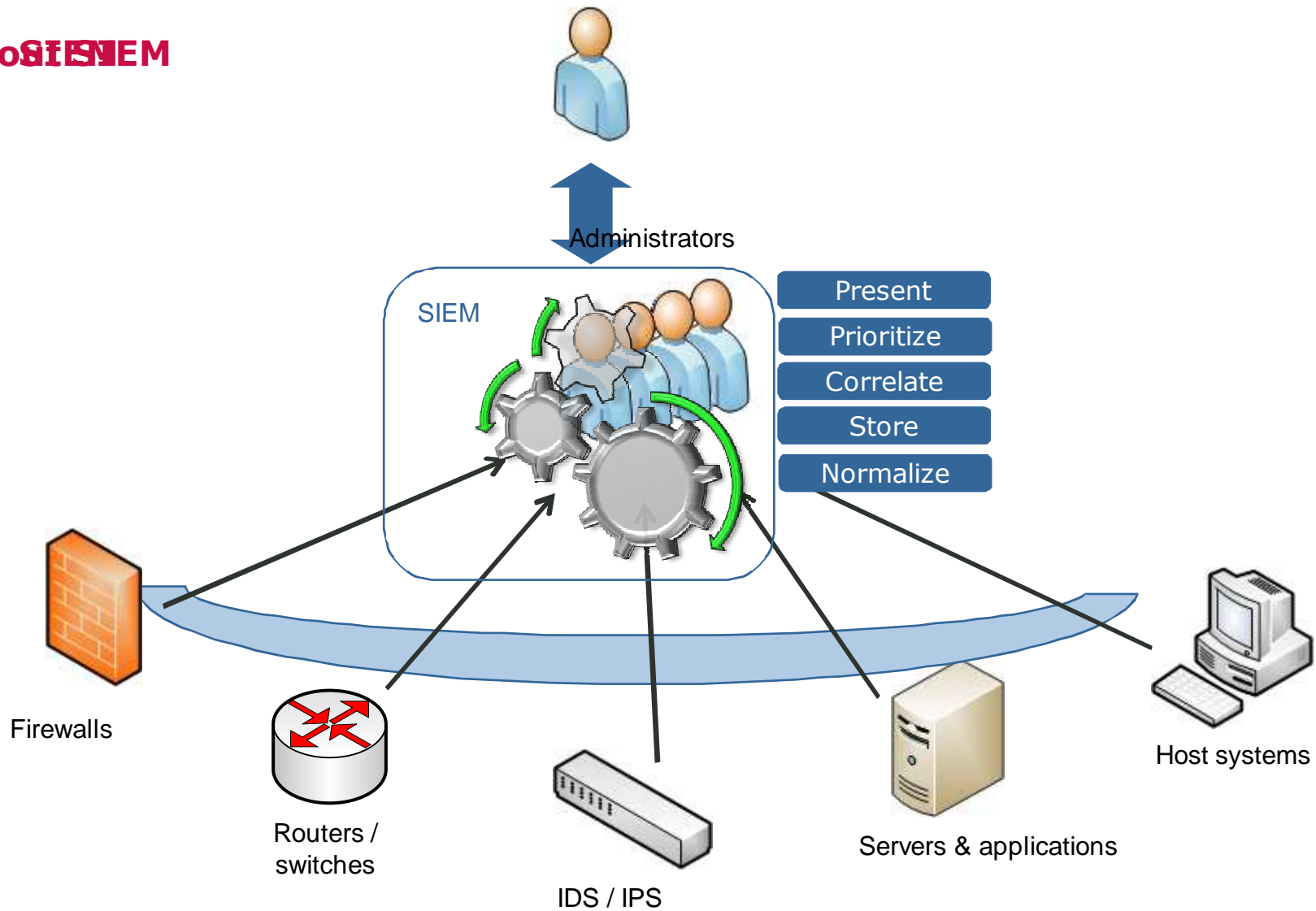
"There is nothing more important
than our customers"

A handwritten signature in black ink, appearing to read 'myself'.

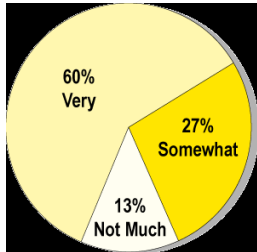
The need for correlation
NBAD is one of the information sources

The need for SIEM

Without SIEM



Building the Magnitude



- Relevance: Based on the weight of Networks and Assets, how relevant is this offense or violation to you. Is it occurring in areas of the network that are not as important to you.



- Credibility: How credible is the evidence. Credibility of the witnesses, if multiple witnesses report same attack, credibility of overall offenses is increased



- Severity: How much of a threat is the attacker, network, offenseto my enterprise. Affected by object weights, asset values, category (type) of attacks, actual vulnerability of targets, and number of targets

Main Features



- Network Surveillance
- Assets
- Offenses
- Events
- Flows
- Reporting
- Administration Configuration

Integrate additional external data

Integration & inline view of identity mapping data:

- User name
- User group
- Switch / port location
- Used authentication mechanism: 802.1x, MAC,...
- Connection type(s): wired / wireless / VPN...
- Assessment server information (i.e. Nessus..)

- Whatever you got that can be related to the system...

Asset Profile			
Name	<input type="text"/>		
Description	<input type="text"/>		
IP Address	10.120.84.56	VA Risk Level	0
Operating System		How Threatening	10
Host Name (DNS Name)	10.120.84.56	How Threatened	2
Asset Weight	0 - Not Important <input type="button" value="v"/>		
MAC	00:02:B3:23:24:BC	Host Name	10.120.84.56
Machine Name			
User Name	BOB1@ets.com	User Group	management
Extra Data	SWITCHIP=10.120.84.1,SWITCHPORT=ge.2.10,AUTHMODE=802_1X		
		<input type="button" value="Save Changes"/>	<input type="button" value="Cancel"/>

Port	OSVDB ID	Name	Description	Risk / Severity	Last Seen
135				1	2008-03-25 12:15:02 (Passive)
445				1	2008-02-19 10:30:01 (Passive)



The Attacker's Identity

Asset Profile
Ports History

Name	<input type="text"/>		
Description	<input type="text"/>		
IP Address	10.120.84.56	VA Risk Level	4
Operating System	unknown	How Threatening	8
Host Name (DNS Name)	10.120.84.56	How Threatened	6
Asset Weight	0 - Not Important		
MAC	14-ac-dc-ba-ee-ab	Host Name	10.120.84.56
Machine Name			
User	bob@ets.com	User Group	Accounting
Extra Data	SWITCHIP=10.120.84.10,SWITCHPORT=ge.1.13,AUTHMETHOD=802_1X		

Close Window

Save Changes Cancel

Port	OSVDB ID	Name	Description	Risk / Severity	Last Seen	First Seen
123				1	2007-07-27 01:52:12 (Active)	2007-07-25 08:45:30 (Active)
135	<u>2100</u>	Microsoft Windows RPC DCOM Interface Overflow	Microsoft Windows platforms contain a flaw that may allow a remote attacker to execute arbitrary code. The issue is due to a flaw in the Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) interface that does not properly sanitize remote requests. If an attacker sends a specially crafted message to the server, they may be able to crash the service or execute	9	2007-07-27 02:00:00 (Passive)	2007-07-25 08:45:00 (Passive)

Copyright © 2007 Enterasys Networks. All rights reserved.

Approve Servers

Dragon Security Command Console

Dashboard **Offense Manager** Event Viewer Network Surveillance Reports

Dragon Time: 10:37 | CONFIG | HELP

- My Offenses
- All Offenses
- By Category
- By Attacker
- By Target
- By Network
- Network Anomalies
- Server Discovery**
- Asset Profiles
- VA Scan
- Rules

Server Discovery

To discover servers (assets) in your deployment based on standard server ports, select the desired role in the Server Type drop-down list box and click 'Discover Servers'.

Server Type: Mail Servers
 All Assigned Unassigned

Ports: 25, 465, 587, 110, 143, 993, 995, 563, 1352 [Edit Ports](#)

Server Type Definition: Edit this BB to define typical mail servers. This BB is used in conjunction with the Default-BB-False Positive: Mail Server False Positives Categories and Default-BB-FalsePositive: Mail Server False Positive Events building blocks. [Edit Definition](#)

Network: Select an object...

Matching Servers:

Approve	Name	IP	Network ▲
<input type="checkbox"/>	10.120.85.60	10.120.85.60	DragonLab.DataCenter
<input type="checkbox"/> Select all items			

Attackers Identity Information

The screenshot displays the Dragon Security Command Console interface. The main content area is divided into several sections:

- Local Networks - Inbound Bytes Usage:** Shows a bar chart with 190.0 MB (3.2 MB/s) of usage.
- Dragon Summary:**

Flows (Past 24 Hours)	1.0 M
New Events (Past 24 Hours)	758.5 K
Updated Offenses (Past 24 Hours)	39.0
Data Reduction Ratio	19914 : 1
- Local Networks - Inbound Bytes:** A green bar chart showing traffic volume over time.
- Local Networks - Outbound Bytes:** A blue bar chart showing outgoing traffic volume over time.
- Attacker Offense List:** A table listing various offenses such as "Local ICMP Scanner", "Internal WEB Exploit", and "Local Worm Detected".
- Top Attackers:** A table listing IP addresses and their associated threat levels.

Attacker	Threat
10.120.20.100	27
Misc Recon Event	12
Unknown	11
Firewall Permit	11

A detailed tooltip for the attacker IP 10.120.84.33 is shown, containing the following information:

- Attacker Magnitude:** 66/100
- Target Magnitude:** 38/100
- Offenses:** 3
- Host Name:** 10.120.84.33
- MAC:** 16-ca-cd-ba-f-f-ba
- User Group Name:** dale@ets.com / Support
- Extra Data:** SWITCHIP=10.120.84.10, SWITCHPORT=ge-2.15, AUTHMETH=...
- Network:** DragonLab Management



"There is nothing more important
than our customers"

A handwritten signature in black ink, appearing to read 'myself'.

Time for real-time demo

Questions?





"There is nothing more important
than our customers"

my kuf