"There is nothing more important than our customers"

Network Behavioral Anomaly Detection
Dragon Securtiy Command Console – DSCC

Zdeněk Pala

ECIE certified engineer
ECI certified instructor

26.5.2010

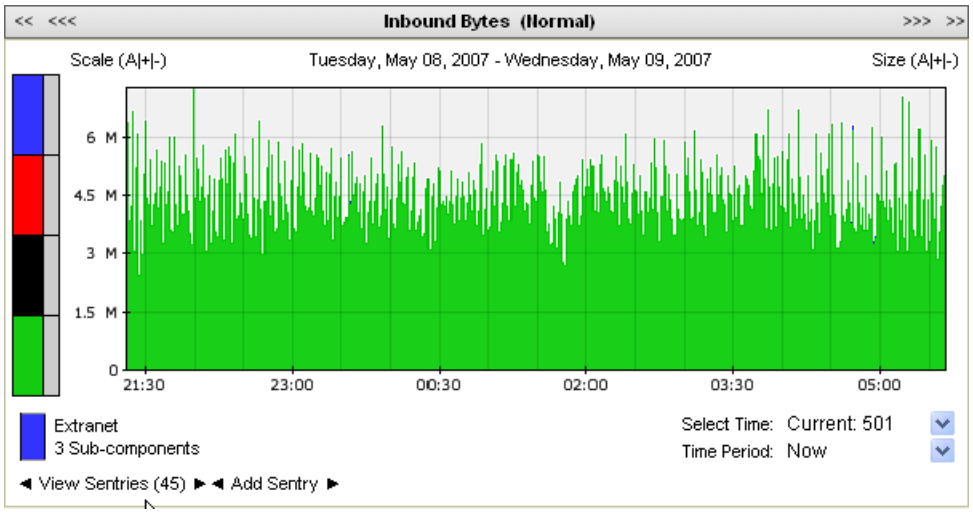
IDS Technologies

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



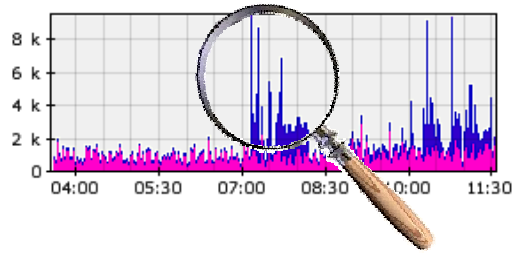
Sentry List

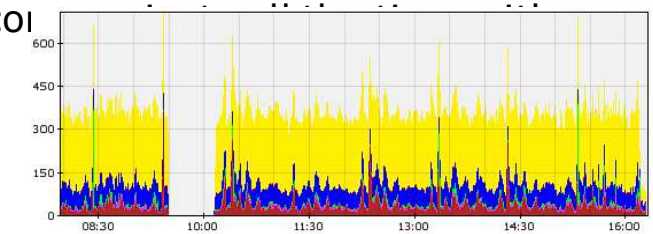
Name	Owner	Actions	Enabled
Behavior - Flow Count Behavior Change	admin		✓
Behavior - Host Count Behavior Change	admin		✓
Behavior - Threat Traffic Packet Rate Behavior Change	admin		✓
Default Suspicious - External - Inbound Unidirectional Flows Threshold	admin		✓
DoS - External - Distributed DoS Attack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

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 repetive amounts of traffic
  - Example: Typically a mail server communicates with 100 hosts in the night, suddenly it starts communicating with 1000 hosts instead

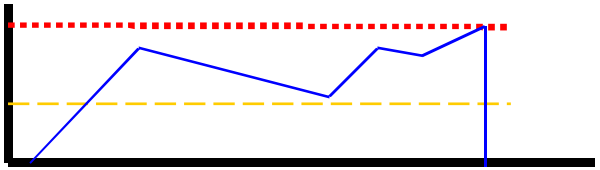
- **Anomaly sentries**
  - Checks for **activity changes** of the entities **inside a view**
  - Detects new or unknown traffic or changes in the amount of **time** a
  - If an anomaly is detected, an alarm will be generated
  - Behavioral sentry -> **volume based**
  - Anomaly sentry -> **activity based**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





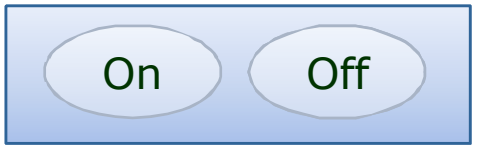
NBAD methods

- **Threshold sentries**
  - Monitors traffic and objects that **exceeds a configured threshold**
  - Useful for monitoring utilized bandwith 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**

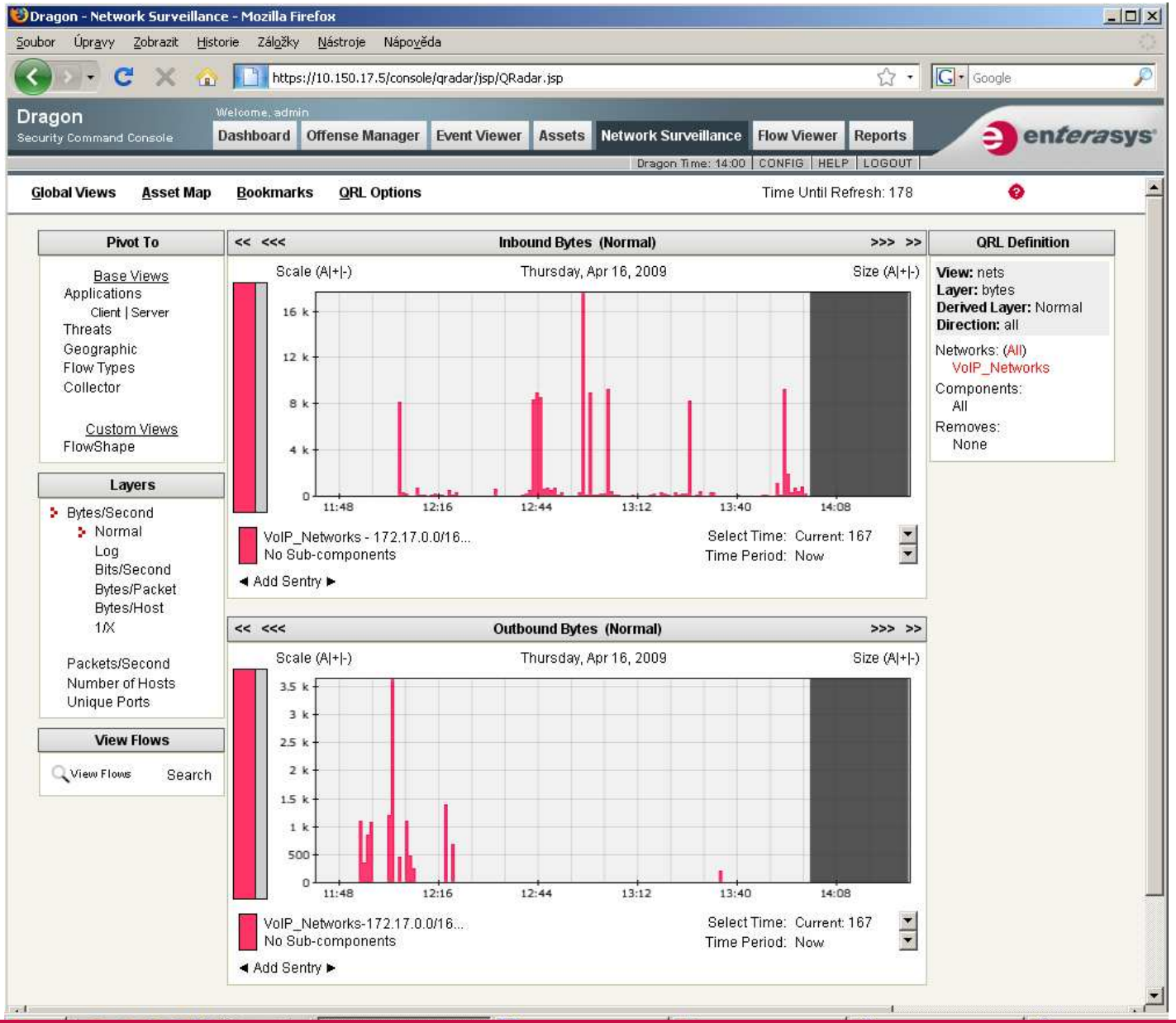


"There is nothing more important than our customers"

Real data

Some examples from customer

VoIP – non local traffic



What applications VoIP talking non local

Flow List - Mozilla Firefox

https://10.150.17.5/console/do/qradar/dataminesearch?dispatch=performSearch&startTimeAbs=1239879270&endTimeAbs=1239879570&rangeStart=1239874539&rangeEnd=1239884559&time=1239879420&aspect=all&interval=5&fullNetworkName=VoIP_Networks&

Search... ▼ Save Search Actions ▼ Display Application

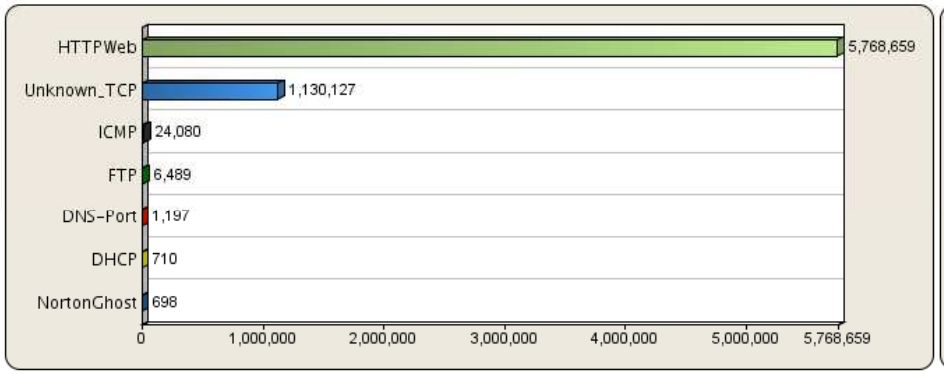
Viewing flows from 2009-04-16 11:35:39 to 2009-04-16 14:22:39 **View:** Specific Interval

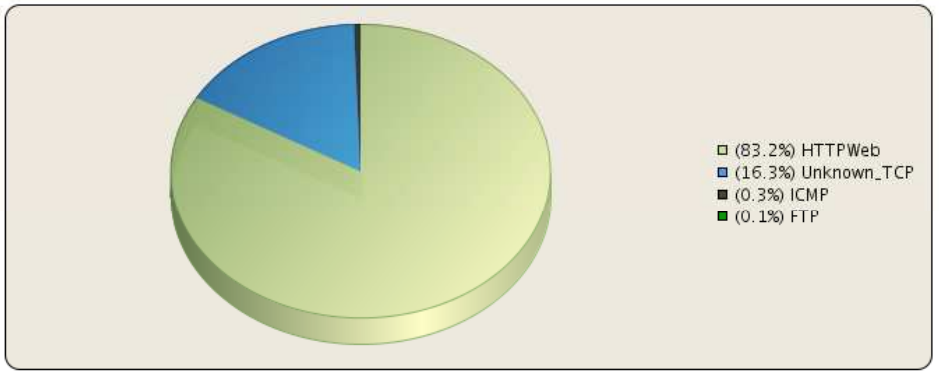
Grouping By:

Application

Current Filters:

Source or Destination Network is any of VoIP_Networks (Clear Filter), Flow Direction is any of [L2R or R2L] (Clear Filter)





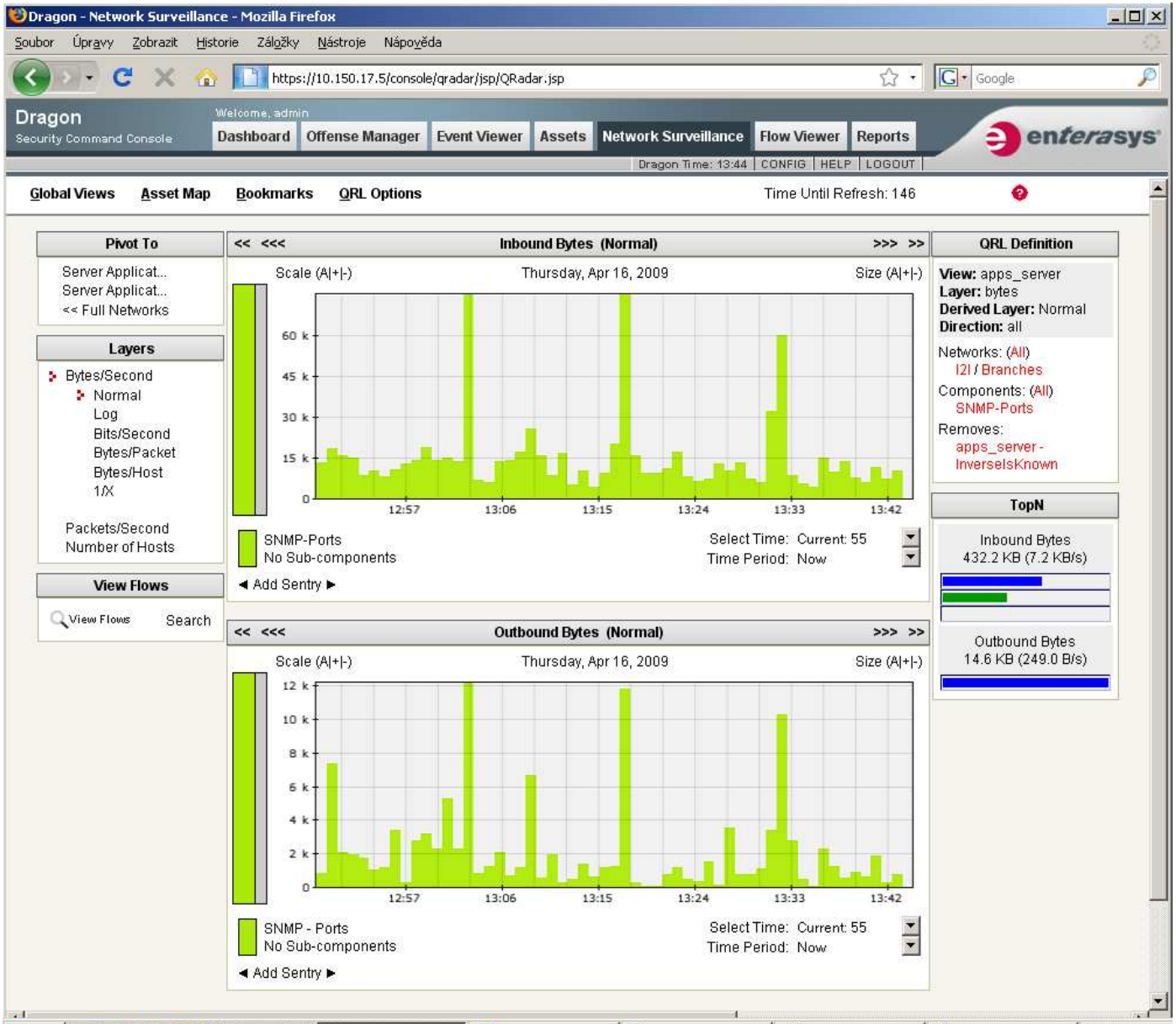
(Hide Charts)

	Application	Source IP	Source Network	Destination IP	Destination Port	Destination Network	Source Bytes	Destination Bytes	Total Bytes	Source Packets	Destination Packets	Total Packets	Count
	HTTPWeb	Multiple (4)	other	Multiple (2)	80	VoIP_Networks	5 768 659	0	5 768 659	15 217	0	15 217	331
	Unknown_TCP	Multiple (5)	Multiple (2)	Multiple (3)	Multiple (36)	Multiple (2)	1 130 127	0	1 130 127	8 057	0	8 057	131
	ICMP	Multiple (11)	other	Multiple (124)	0	VoIP_Networks	24 080	0	24 080	430	0	430	385
	FTP	172.17.8.37	VoIP_Networks	172.133.4.9	21	other	6 489	0	6 489	131	0	131	10
	DNS-Port	Multiple (2)	VoIP_Networks	172.150.14.70	53	other	1 197	0	1 197	18	0	18	9
	DHCP	172.128.1.208	other	Multiple (2)	68	VoIP_Networks	710	0	710	2	0	2	2
	NortonGhost	172.17.1.135	VoIP_Networks	172.137.1.209	Multiple (2)	other	698	0	698	7	0	7	2

Displaying 1 to 7 of 7 items (Elapsed time: 0:00:18.591)

Hotovo 10.150.17.5

Snmp traffic



SNMP talkers

Flow List - Mozilla Firefox

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

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

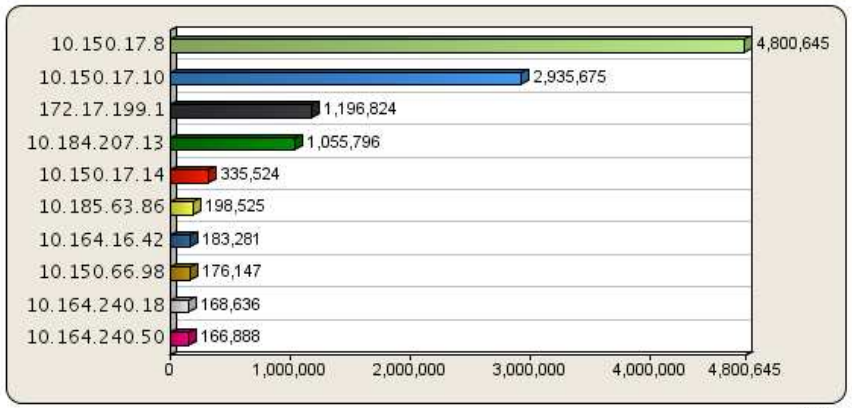
Viewing flows from 2009-04-16 13:13:32 to 2009-04-16 13:18:32 (Slice 2 of 3) (First | Previous | View All | | Next | Last) (Duration is 5m) View: Real Time (auto refresh)

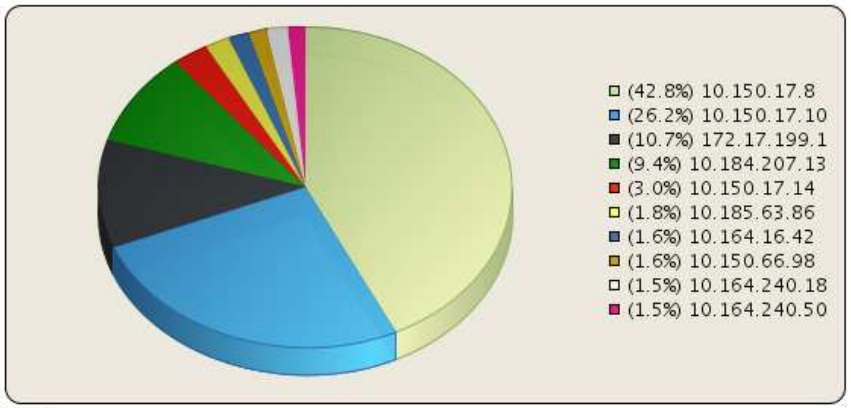
Grouping By:

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)





(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)

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

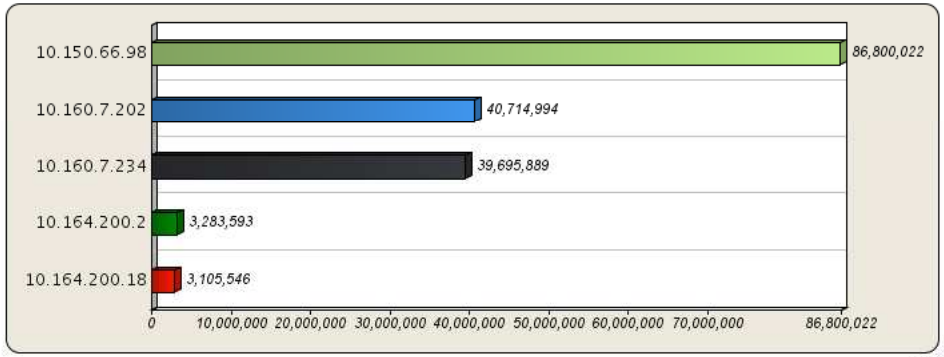
Viewing flows from 2009-04-16 07:48:00 to 2009-04-16 10:48:00 **View:** Last 3 Hours

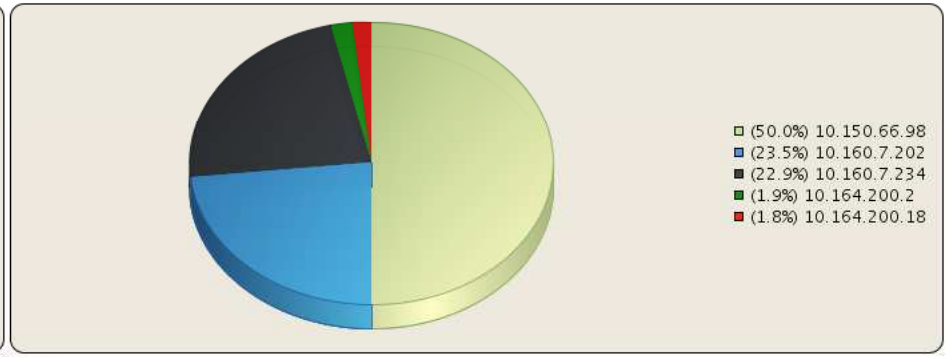
Grouping By:

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)





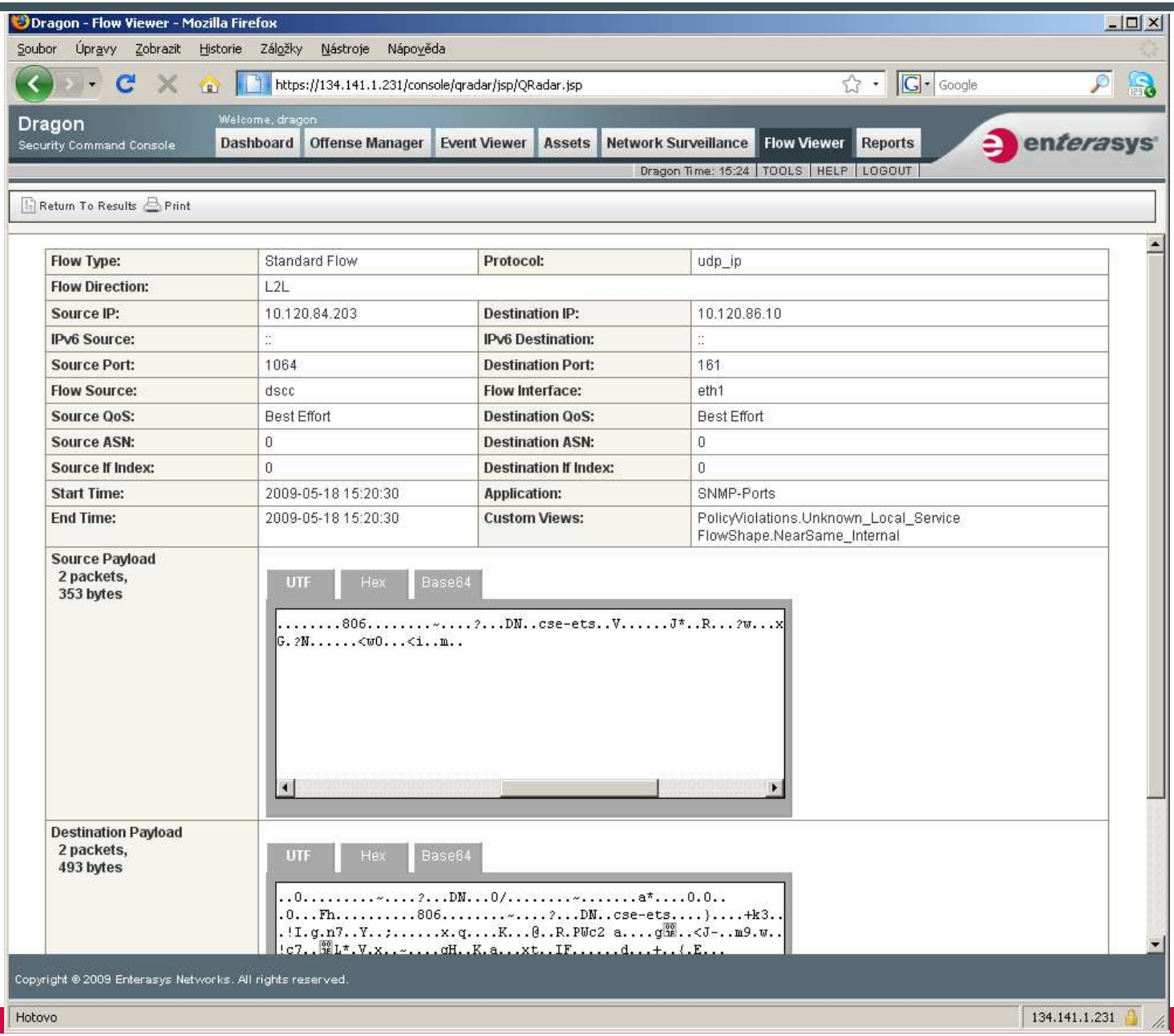
(Hide Charts)

	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

Displaying 1 to 5 of 5 items (Elapsed time: 0:00:00.150)

Hotovo 10.150.17.5

Detail of SNMP communication



SSH

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: 11:09 | CONFIG | HELP | LOGOUT

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

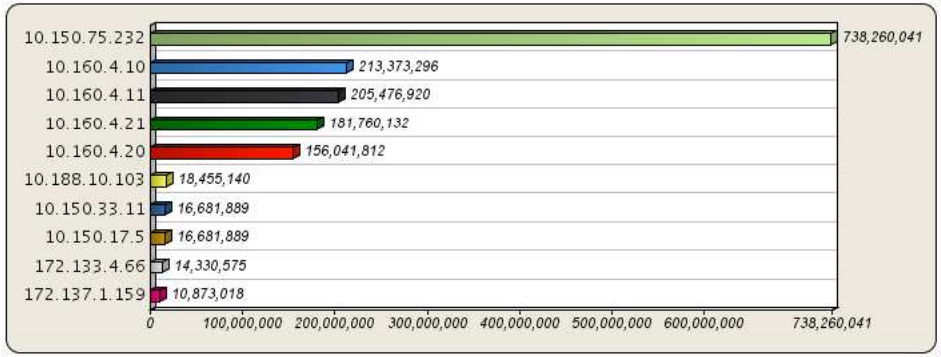
Viewing flows from 2009-04-15 11:06:00 to 2009-04-16 11:06:00 **View:** Last 24 Hours

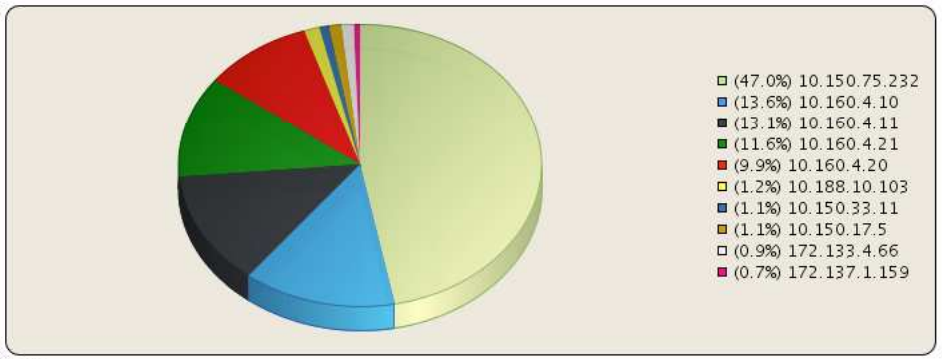
Grouping By:

IP

Current Filters:

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





(Hide Charts)

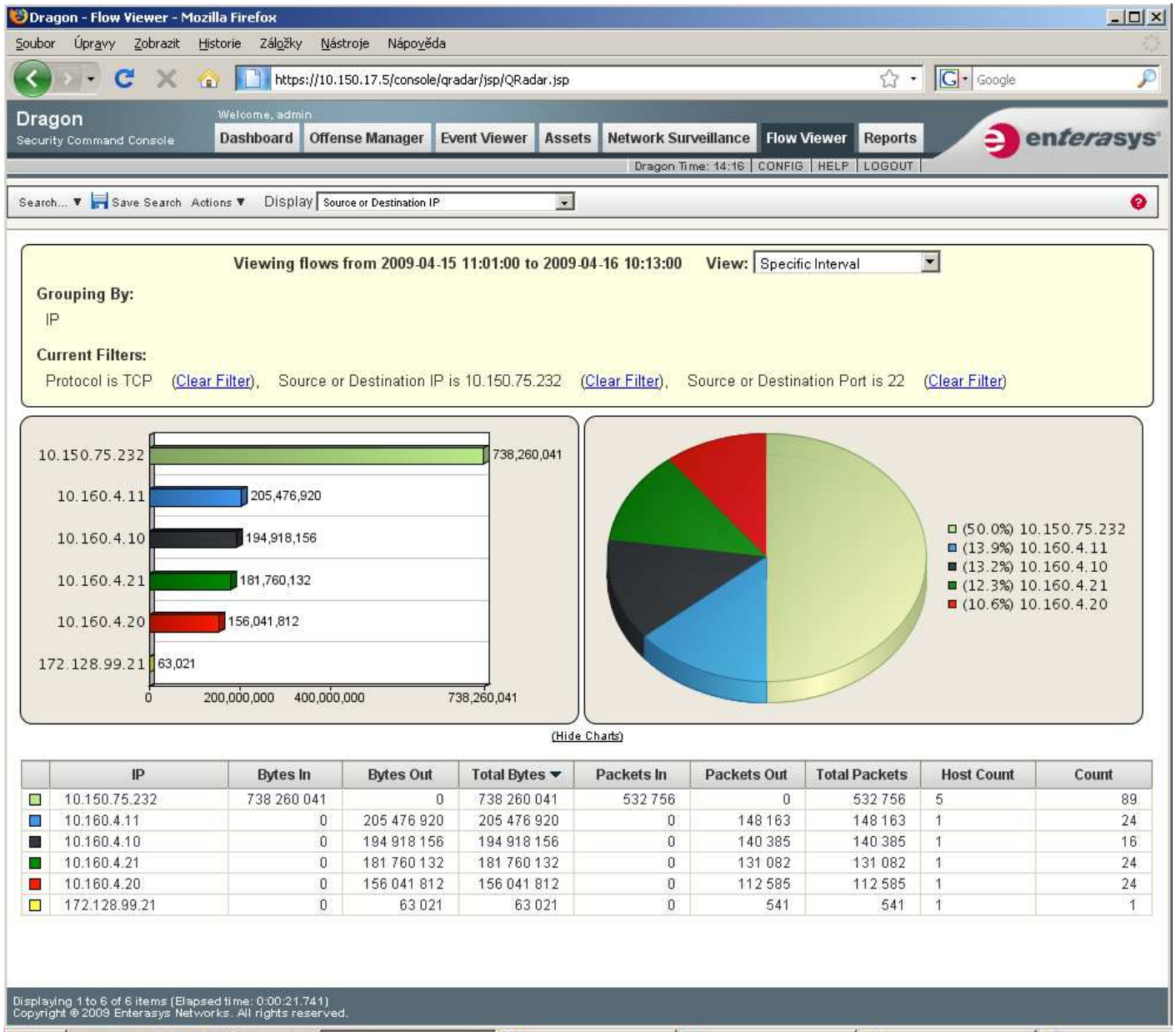
	IP	Bytes In	Bytes Out	Total Bytes	Packets In	Packets Out	Total Packets	Host Count	Count
	10.150.75.232	738 260 041	0	738 260 041	532 756	0	532 756	5	89
	10.160.4.10	0	213 373 296	213 373 296	0	153 891	153 891	2	17
	10.160.4.11	0	205 476 920	205 476 920	0	148 163	148 163	1	24
	10.160.4.21	0	181 760 132	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)

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

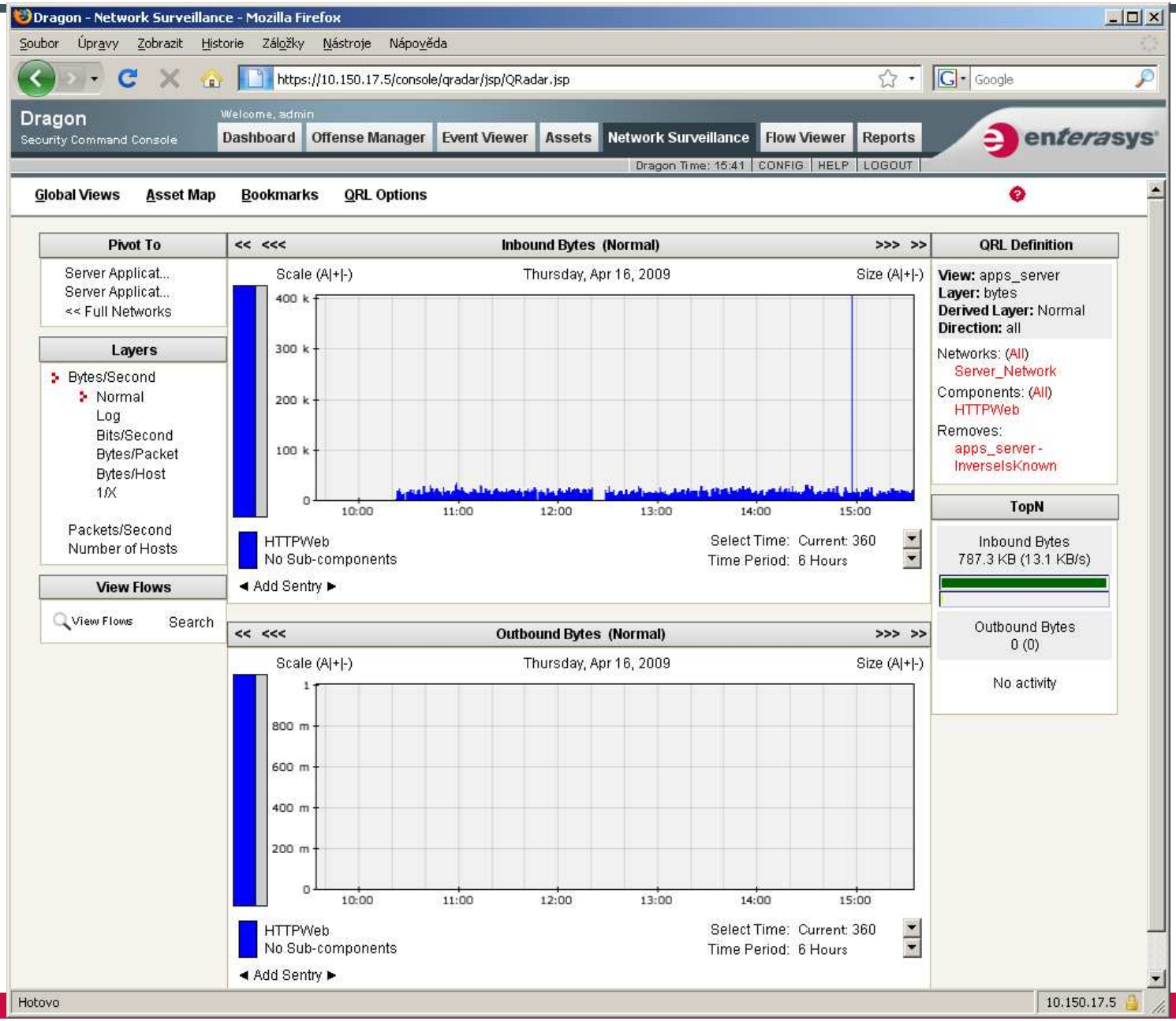
Hotovo 10.150.17.5

Whom was he talking ssh?

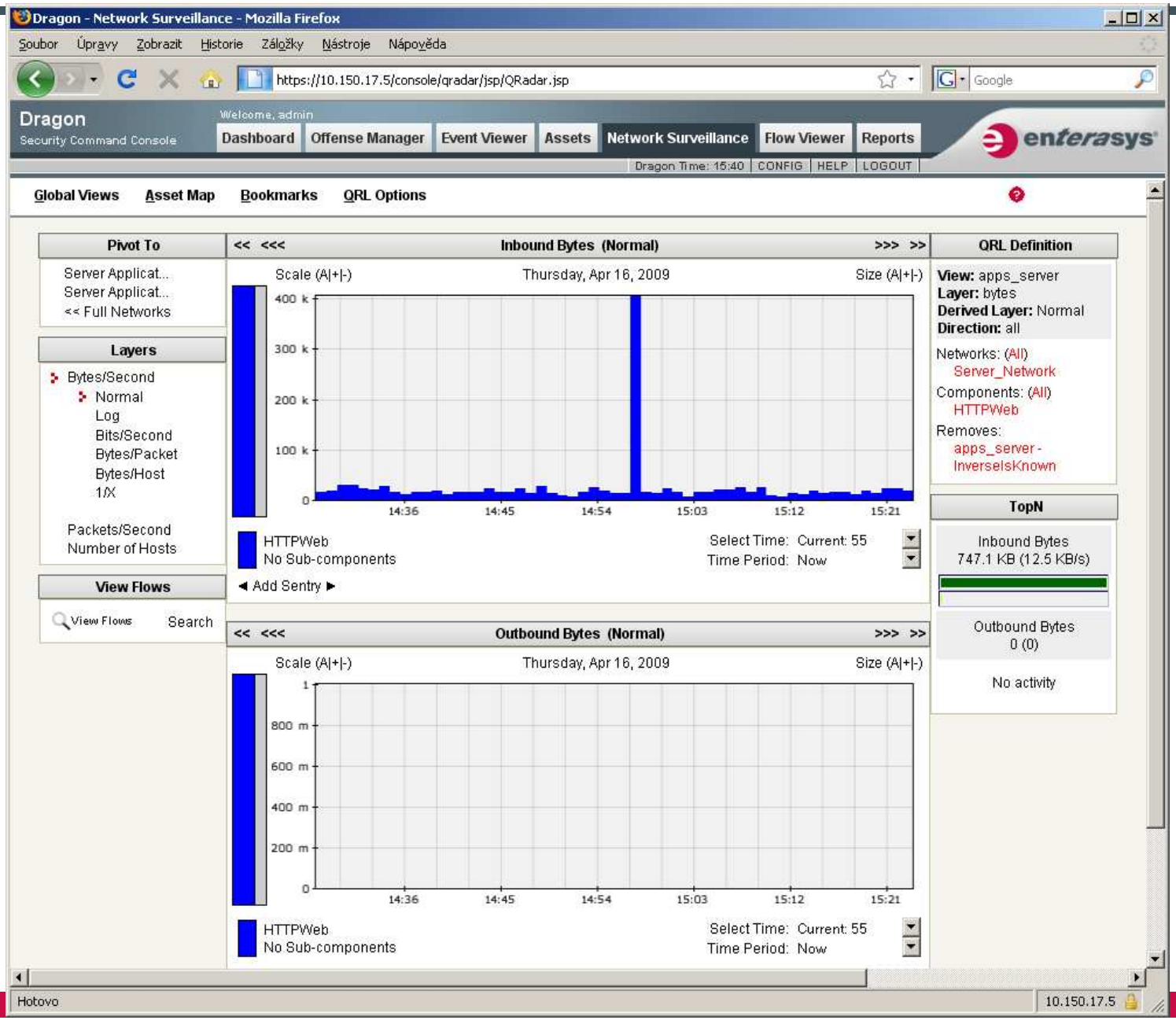


	IP	Bytes In	Bytes Out	Total Bytes	Packets In	Packets Out	Total Packets	Host Count	Count
	10.150.75.232	738 260 041	0	738 260 041	532 756	0	532 756	5	89
	10.160.4.11	0	205 476 920	205 476 920	0	148 163	148 163	1	24
	10.160.4.10	0	194 918 156	194 918 156	0	140 385	140 385	1	16
	10.160.4.21	0	181 760 132	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

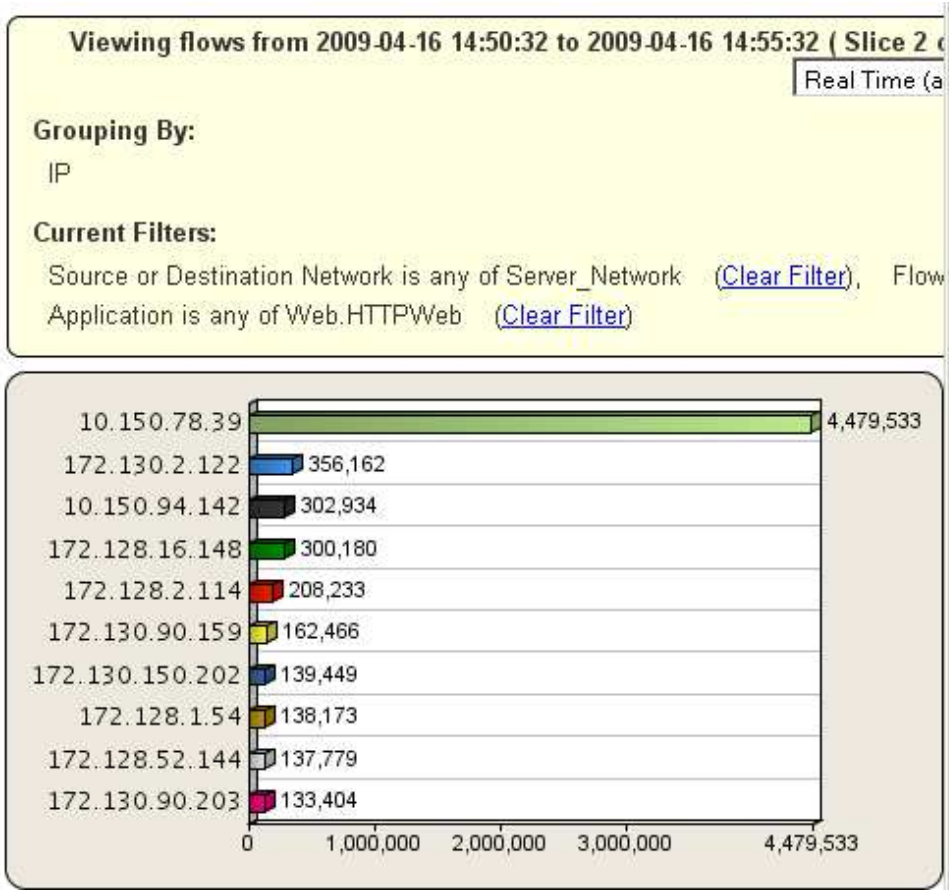
HTTP profile to servers

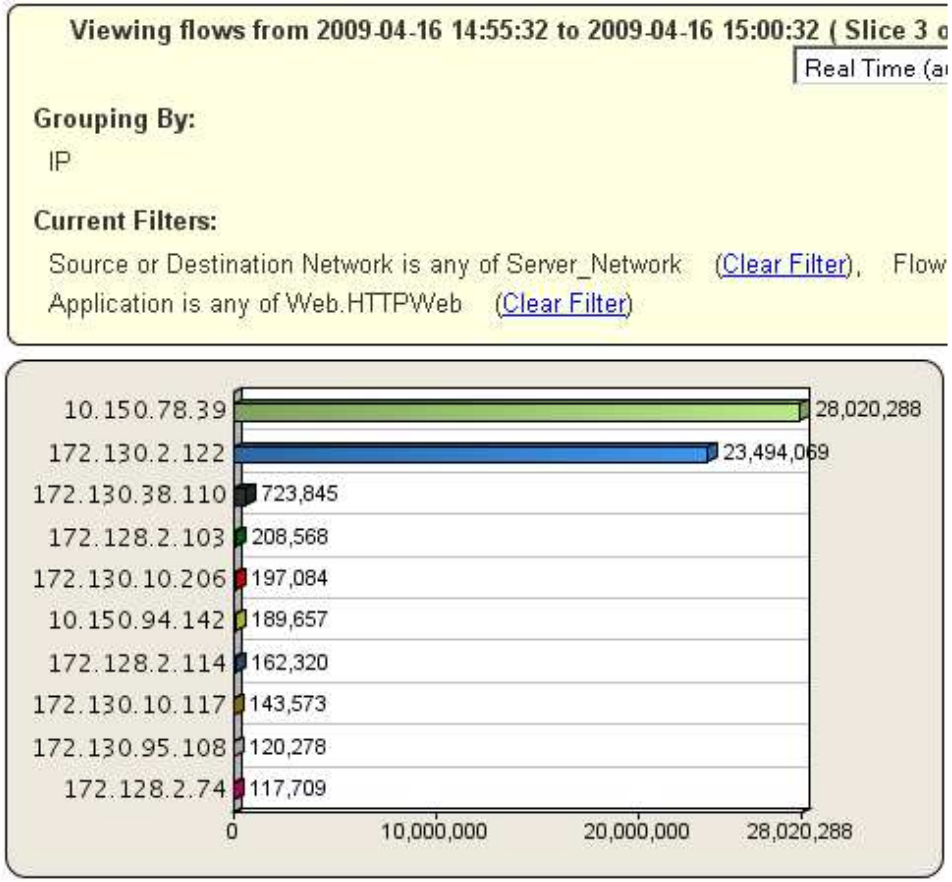


HTTP traffic to servers



Comparison





UDP/TCP port 0

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: 08:02 | CONFIG | HELP | LOGOUT

Global Views | Asset Map | Bookmarks | QRL Options | Time Until Refresh: 148

Pivot To

Threats by Netw...
Threats
<< Full Networks

Layers

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

View Flows

<< <<< **Inbound Bytes (Normal)** >>> >>

Scale (A|+|-) Thursday, Apr 16, 2009 - Friday, Apr 17, 2009 Size (A|+|-)

12
9
6
3
0

00:30 02:00 03:30 05:00 06:30 08:00

Tcp_Udp_Port_0
No Sub-components

Select Time: Current: 501
Time Period: Now

◄ View Sentries (48) ► ◄ Add Sentry ►

QRL Definition

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

Networks:
All

Components: (All)
Tcp_Udp_Port_0

Removes:
Threats - other

TopN

Inbound Bytes
267 B (4.4 B/s)

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%3Bnet

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

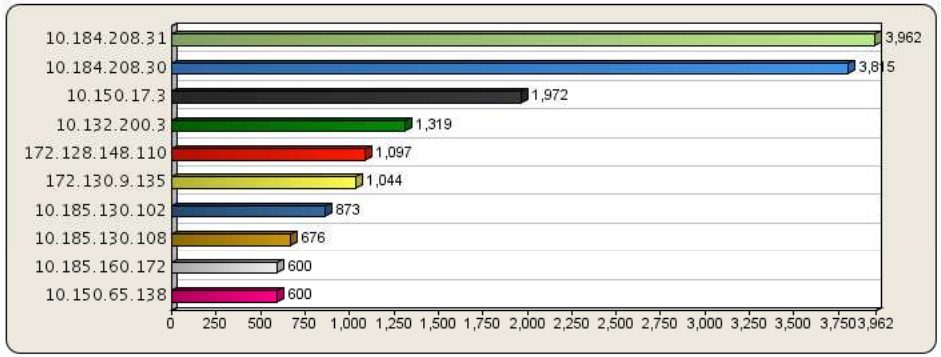
Viewing flows from 2009-04-16 23:43:35 to 2009-04-17 08:04:35 **View:** Specific Interval

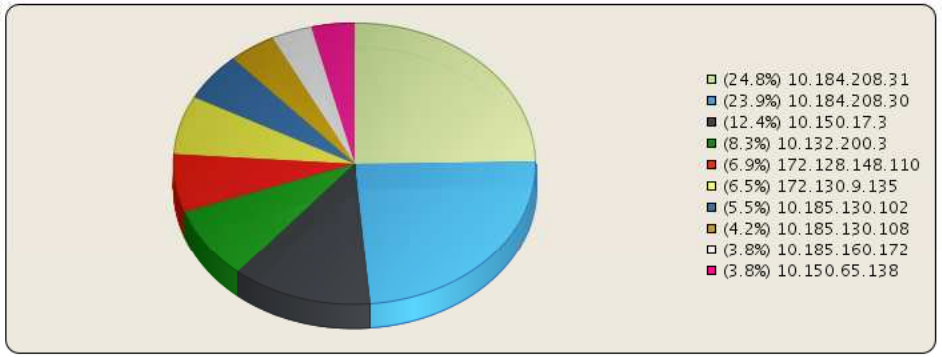
Grouping By:

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)

Page: 1 Go << 1 | 2 >>

Hotovo 10.150.17.5

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

Threats by Netw...
Threats
<< Full Networks

Layers

Bytes/Second
Normal
Log
Bits/Second
Bytes/Packet
Bytes/Host
1/X

Packets/Second
Number of Hosts

View Flows

Inbound Bytes (Normal)

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

3.5 3 2.5 2 1.5 1 500 m 0

06:28 06:56 07:24 07:52 08:20 08:48

Suspicious_ICMP_Type_Code
No Sub-components

Select Time: Current: 167
Time Period: Now

View Sentries (48) Add Sentry

QRL Definition

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

Networks:
All

Components: (All)
Suspicious_ICMP...

Removes:
Threats - other

TopN

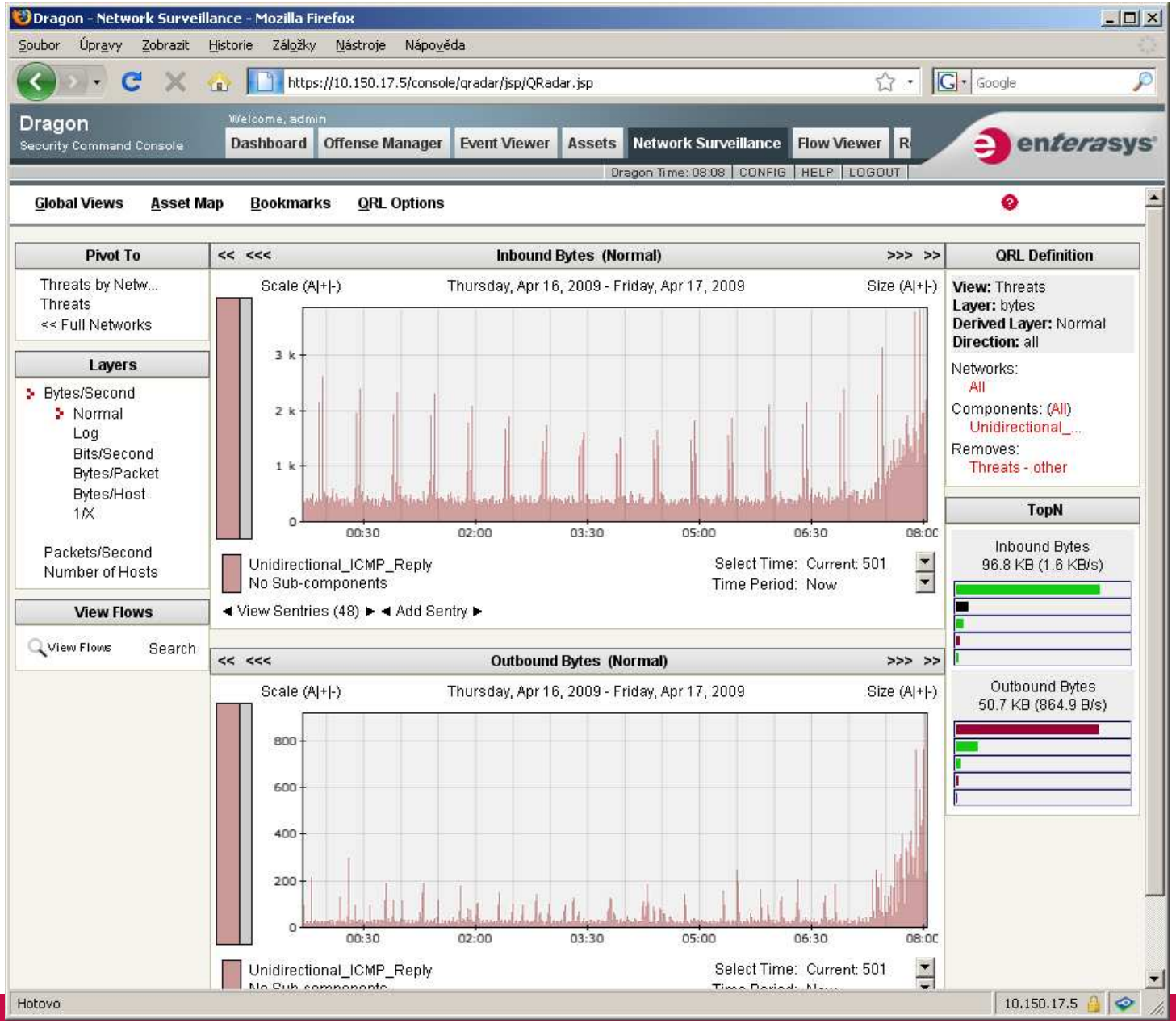
Inbound Bytes
0 (0)

No activity

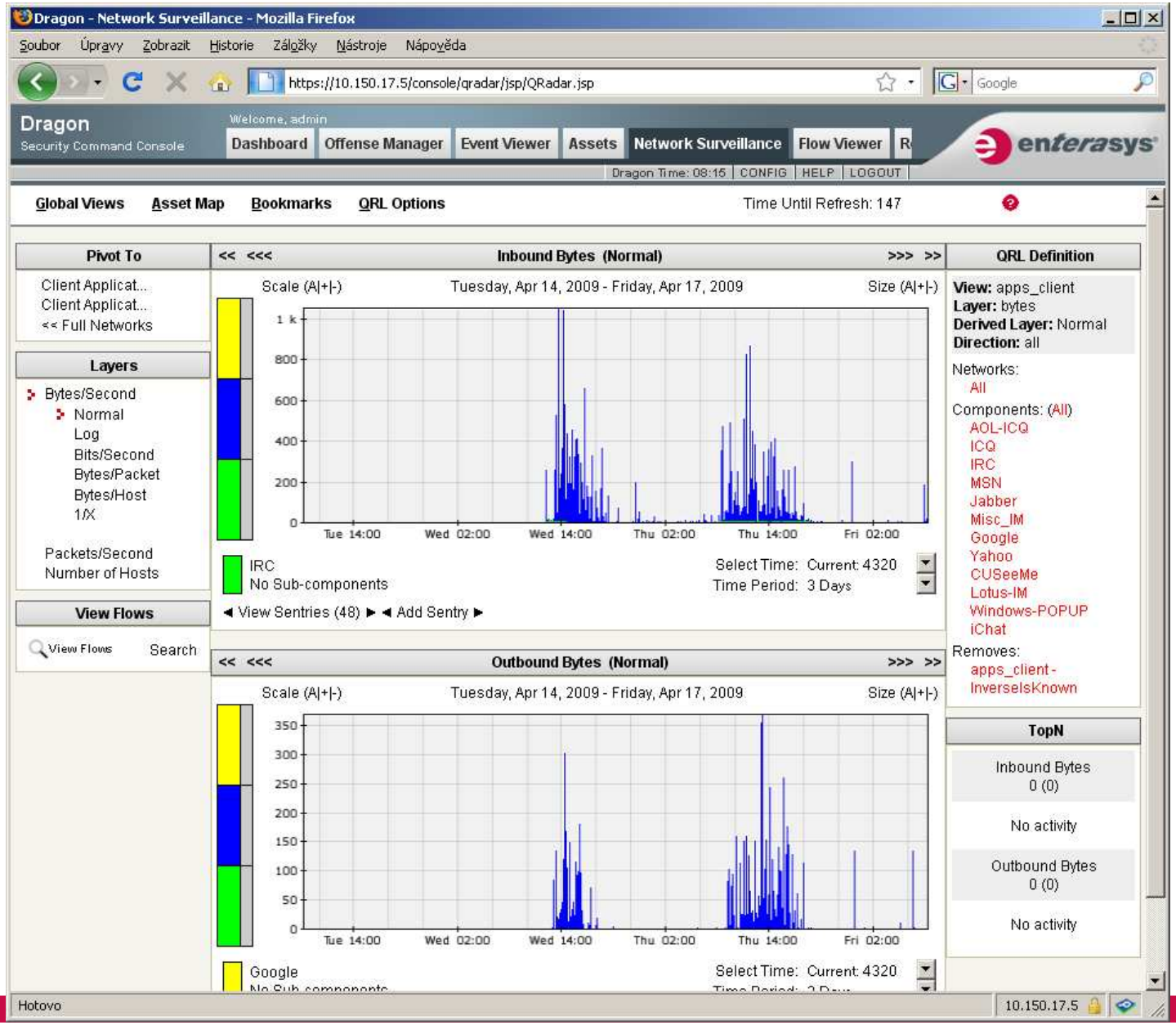
Outbound Bytes

Hotovo | 10.150.17.5

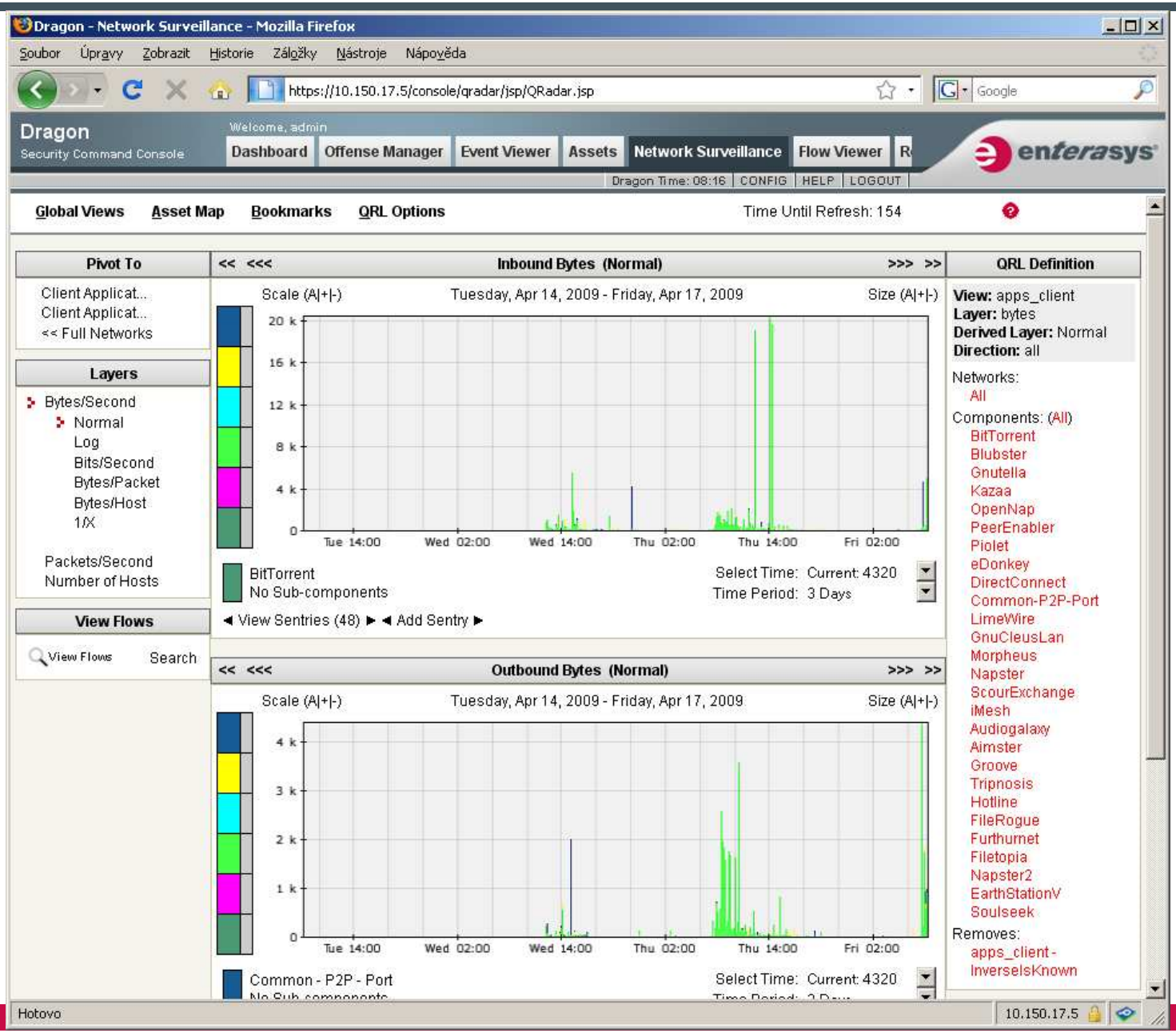
ICMP replies without request



Chatting applications



P2P applications



P2P applications used

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

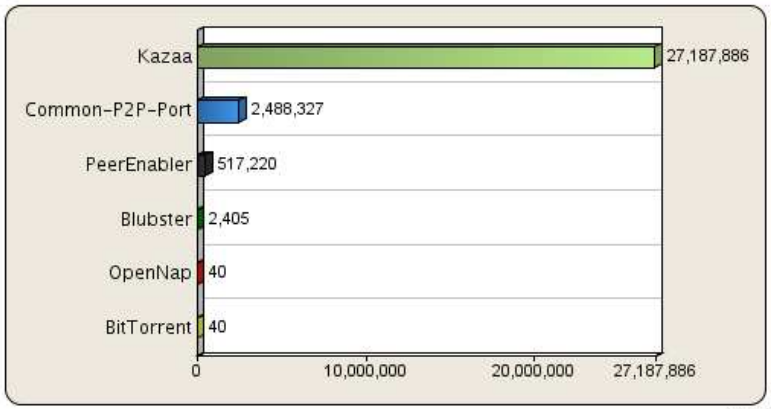
Dragon Time: 08:31 | CONFIG | HELP | LOGOUT

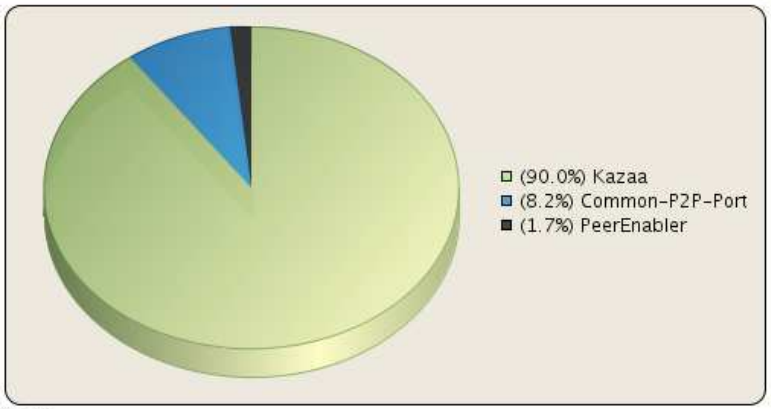
Search... Save Search Actions Display Application

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)





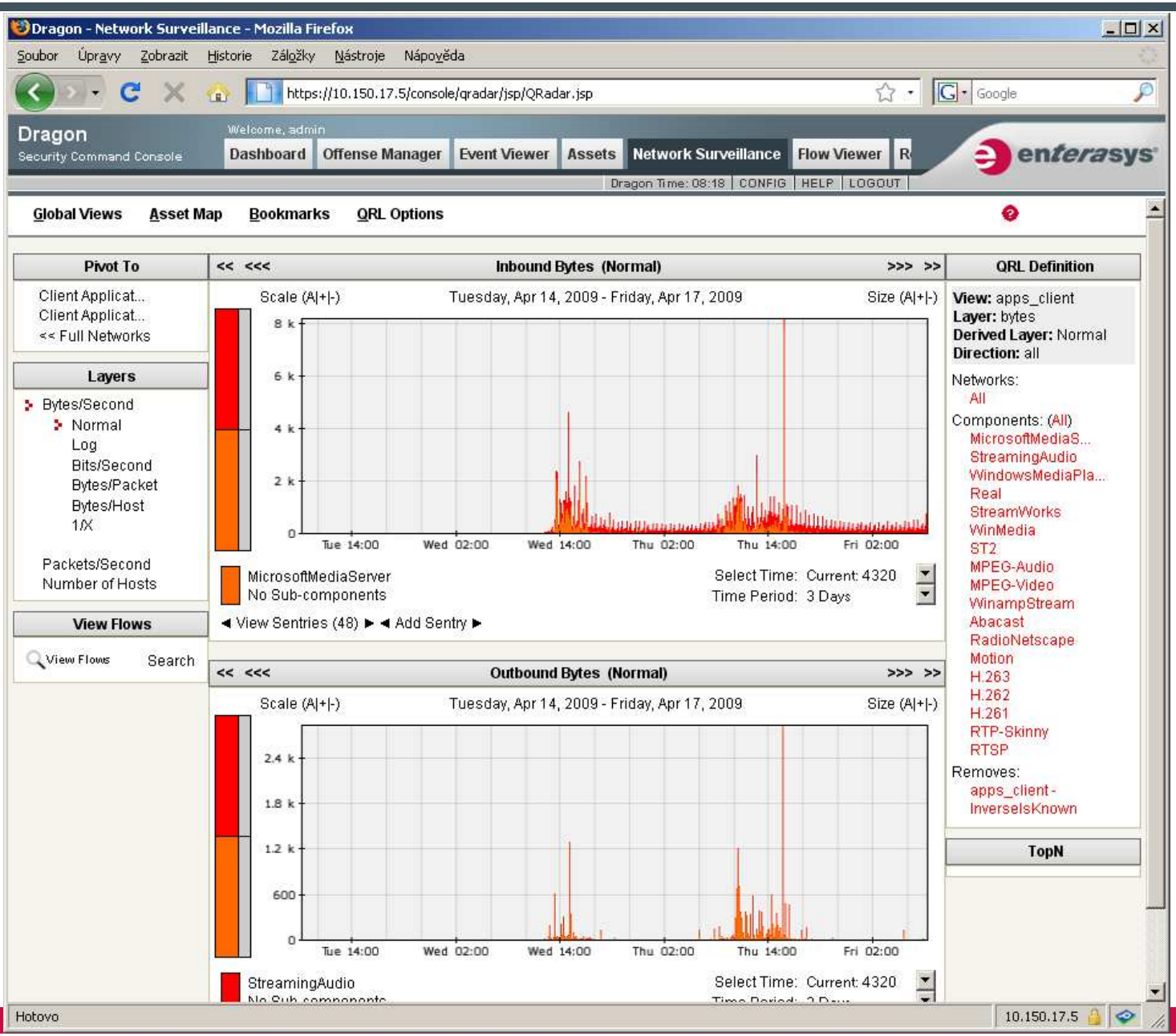
(Hide Charts)

	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)

Hotovo 10.150.17.5

Streaming


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
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|+|-)
8 k
6 k
4 k
2 k
0
Tue 14:00
Wed 02:00
Wed 14:00
Thu 02:00
Thu 14:00
Fri 02:00
MicrosoftMediaServer
No Sub-components
Select Time: Current: 4320
Time Period: 3 Days
View Sentries (48)
Add Sentry
Outbound Bytes (Normal)
Scale (A|+|-)
Tuesday, Apr 14, 2009 - Friday, Apr 17, 2009
Size (A|+|-)
2.4 k
1.8 k
1.2 k
600
0
Tue 14:00
Wed 02:00
Wed 14:00
Thu 02:00
Thu 14:00
Fri 02:00
StreamingAudio
Select Time: Current: 4320
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 -
InverseIsKnown
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

enterasys® Secure Networks™

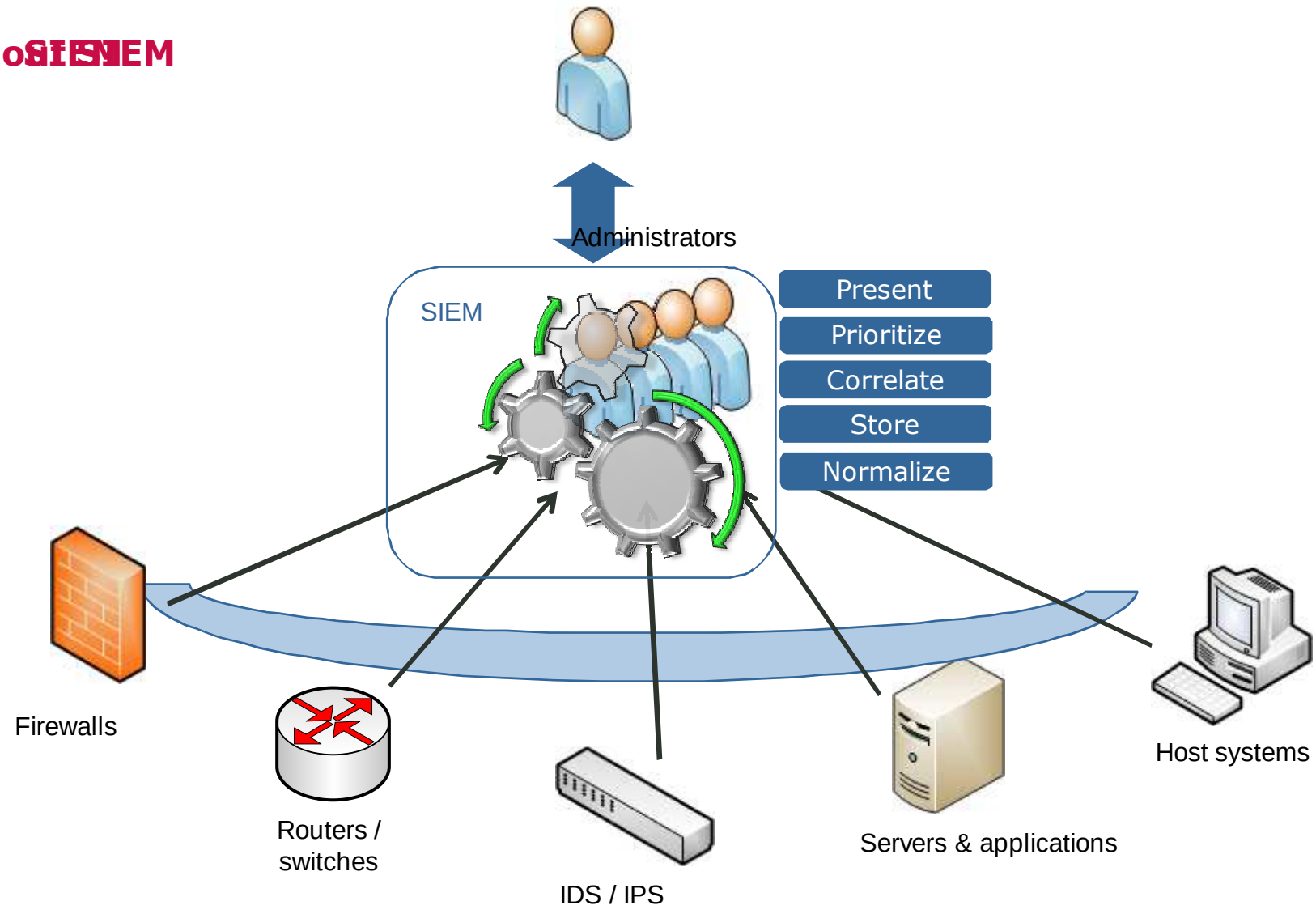
"There is nothing more important than our customers"

The need for correlation

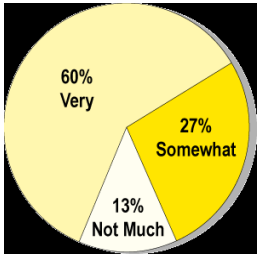
NBAD is one of the information sources

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 in increased

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

Main Features

- Network Survaillance
- 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			
Description			
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		

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,AUTH		HOD=802_1X

Save Changes 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

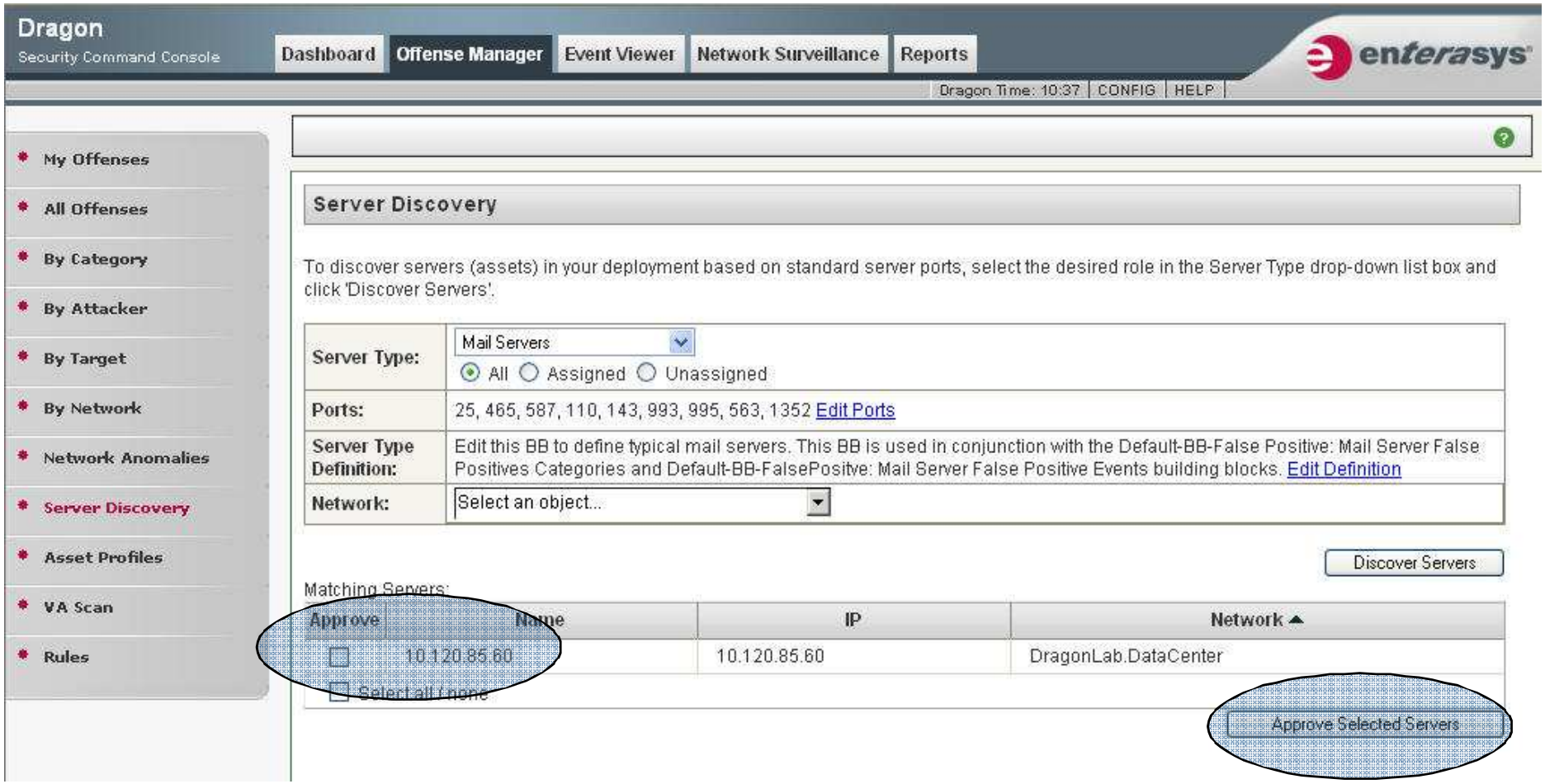
Ports History

Name			
Description			
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		

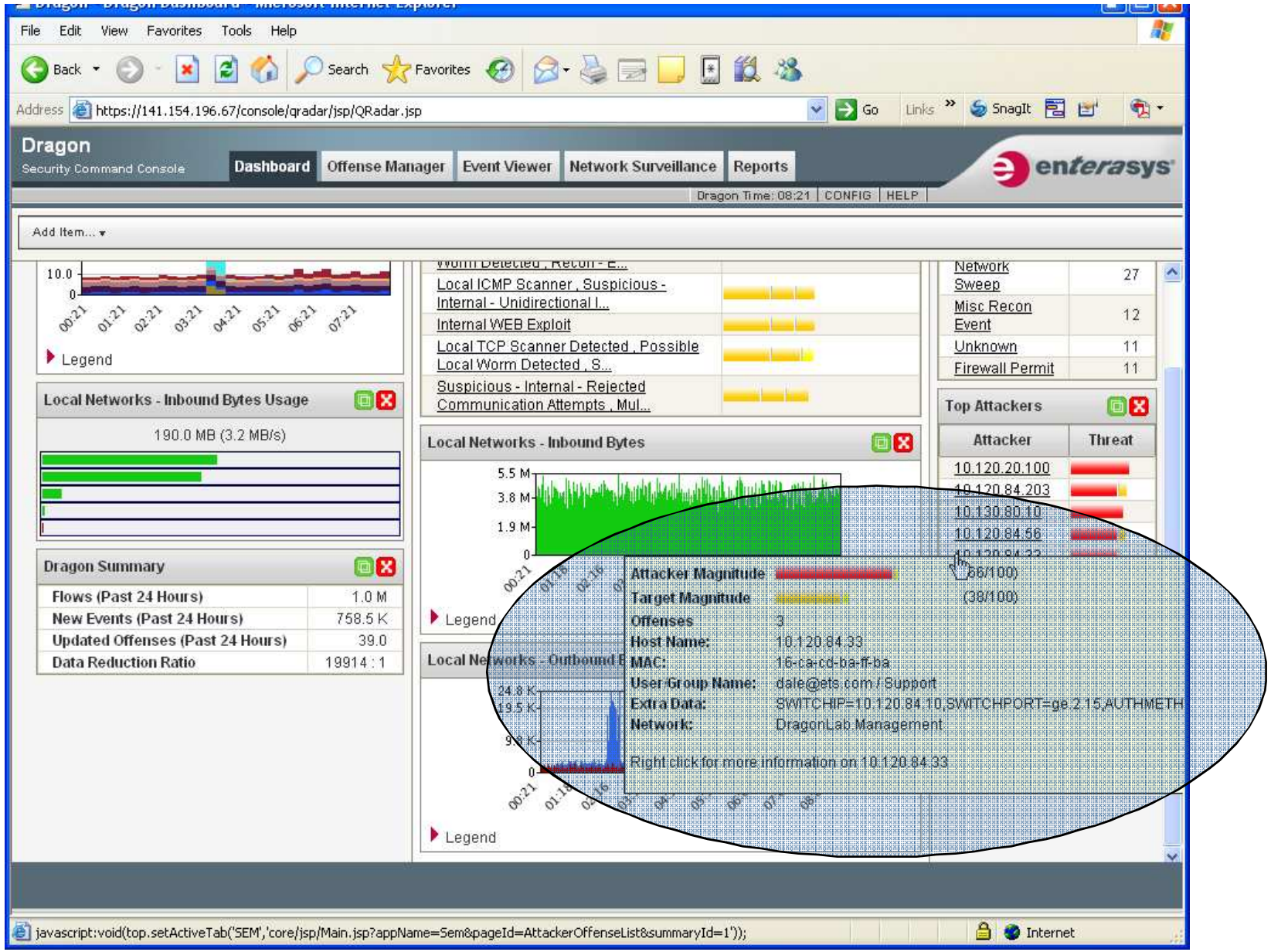
Save Changes Cancel Close Window

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	2100	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)

Approve Servers



Attackers Identity Information



"There is nothing more important than our customers"

Time for real-time demo

Questions?

enterasys®
Secure Networks™

"There is nothing more important than our customers"