Building Baselines Visually

"Aka my 10 year quest to help make sense of the flickering bits flashing on and off before my eyes"

Paul Sop, CISSP, CISM, CISA
Chief Strategy Officer, RedWolf Security
Founder, Intellitactics

Presentation Structure

(streetfighter edition)

- Baselining, the Early Years
- Baselining Turbo, Ethereal
- Super Baselining, Graph Visualization
- Super Baselining 2 Turbo, Pivot with Business Labels and Taxonomy
- Baselining 2, Championship Edition, Fuzzy Feature Selection
- Baselining, the retrospective

Baselining

- **Why?**
  - Separate the signal from the noise
  - Determine what's 'normal' in an ever-changing network
  - Be able to see 'abnormal'
  - Make less tedious work for us
  - Help real people make sense of what they're seeing so they can make decisions

In the beginning, TCPDUMP

```
redwolfsecurity:/var/log/apache2# tcpdump | grep -v ph.ph.cox | grep -v CM0012
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
23:15:58.077987 IP redwolfsecurity.com.1995 > ns1.colo4dallas.net.domain:  52297+ PTR? 34.187.15.68.in-addr
23:15:58.079238 IP ns1.colo4dallas.net.domain > redwolfsecurity.com.1995:  52297 1/2/2 (167)
23:15:58.079455 IP redwolfsecurity.com.1995 > ns1.colo4dallas.net.domain:  52298+ PTR? 245.64.123.206.in-ad
23:15:58.080359 IP ns1.colo4dallas.net.domain > redwolfsecurity.com.1995:  52298* 1/1/1 (108)
23:15:58.130377 IP redwolfsecurity.com.1995 > ns1.colo4dallas.net.domain:  52299+ PTR? 62.86.57.72.in-addr.a
23:15:58.131825 IP ns1.colo4dallas.net.domain > redwolfsecurity.com.1995:  52299 1/6/6 PTR[|domain]
23:15:59.452402 802.1d config 8000.00:50:bd:0e:4c:4a.81c6 root 8000.00:30:f2:85:b0:4a pathcost 19 age 1 max
23:16:01.356076 IP 207.210.219.65.colo4dallas.net > OSPF-ALL.MCAST.NET: OSPFv2, Hello (1), length: 44
23:16:01.356281 IP redwolfsecurity.com.1995 > ns1.colo4dallas.net.domain:  52300+ PTR? 5.0.0.224.in-addr.arpa. (40)
23:16:01.357853 IP ns1.colo4dallas.net.domain > redwolfsecurity.com.1995:  52300 1/3/6 PTR[|domain]
23:16:01.357992 IP redwolfsecurity.com.1995 > ns1.colo4dallas.net.domain:  52301+ PTR? 65.219.210.207.in-a
23:16:01.358967 IP ns1.colo4dallas.net.domain > redwolfsecurity.com.1995:  52301* 1/2/2 (157)
23:16:01.452294 802.1d config 8000.00:50:bd:0e:4c:4a.81c6 root 8000.00:30:f2:85:b0:4a pathcost 19 age 1 ma
23:16:03.452853 802.1d config 8000.00:50:bd:0e:4c:4a.81c6 root 8000.00:30:f2:85:b0:4a pathcost 19 age 1 ma
23:16:05.452650 802.1d config 8000.00:50:bd:0e:4c:4a.81c6 root 8000.00:30:f2:85:b0:4a pathcost 19 age 1 ma
23:16:07.452779 802.1d config 8000.00:50:bd:0e:4c:4a.81c6 root 8000.00:30:f2:85:b0:4a pathcost 19 age 1 ma
23:16:09.452996 802.1d config 8000.00:50:bd:0e:4c:4a.81c6 root 8000.00:30:f2:85:b0:4a pathcost 19 age 1 ma
23:16:10.795818 arp who-has 207.210.219.65.colo4dallas.net tell VeloceNet.powernoc.net
23:16:10.795999 IP redwolfsecurity.com.1995 > ns1.colo4dallas.net.domain:  52302+ PTR? 105.219.210.207.in
23:16:10.797108 IP ns1.colo4dallas.net.domain > redwolfsecurity.com.1995:  52302* 1/2/2 (162)
23:16:11.356531 IP 207.210.219.65.colo4dallas.net > OSPF-ALL.MCAST.NET: OSPFv2, Hello (1), length: 44
23:16:11.453151 802.1d config 8000.00:50:bd:0e:4c:4a.81c6 root 8000.00:30:f2:85:b0:4a pathcost 19 age 1 ma
23:16:11.755773 CDPv2, ttl: 180s, Device-ID '069054520'[|cdp]
23:16:12.015676 IP redwolfsecurity.com.www > bdhz-1714e.adsl.wanadoo.nl.3182: F 1600181077:1600181077
23:16:12.015830 IP redwolfsecurity.com.1995 > ns1.colo4dallas.net.domain:  52303+ PTR? 78.143.69.81.in-addr.arpa. (43)
23:16:12.141510 IP ns1.colo4dallas.net.domain > redwolfsecurity.com.1995:  52303* 1/2/2 (190)
23:16:12.159868 IP bdhz-1714e.adsl.wanadoo.nl.3182 > redwolfsecurity.com.www: . ack 1 win 65535
23:16:13.453304 802.1d config 8000.00:50:bd:0e:4c:4a.81c6 root 8000.00:30:f2:85:b0:4a pathcost 19 age 1 max 20 hello 2 f
23:16:13.524164 IP bdhz-1714e.adsl.wanadoo.nl.3182 > redwolfsecurity.com.www: R 1:1(0) ack 1 win 0
```

Images copyright Paramount, and 20th Century Fox Respectively

Mat Johnston's Plight

- Hired friend (1996) to create TCPDUMP Filters to filter out and classify all traffic in a little DMZ. (BASELINE IT)
- Figured it would take him a day or two.
- Six weeks later, there were still packets we couldn't classify.
  - Weird packets from Microsoft products.
- Hmm…. I thought. I must be mean.

Then came GUI Sniffers

- Well, GUI is perhaps stretching things a bit (text in boxes).
- We used Network Associates Sniffer
- Later, Ethereal
  - A great, free, network analyzer
- We all stood around the monitor: "Gosh these tools are sure to make short work of figuring out networks!"

The Ethereal GUI

Filters

Frame List

Frame Detail (decoded)

Frame

Compaq WLAN MultiPort W200 (Microsoft's Packet Scheduler) : Capturing - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	rotoco	Info
5165	2186.2313	10.59.1.17	67.19.41.215	HTTP	GET /scrapbook/2005/index.php HTTP/1.1
5166	2186.2914	67.19.41.215	10.59.1.17	TCP	http > 53877 [ACK] Seq=1 Ack=324 Win=6432 Len=0
5167	2186.3383	10.59.1.12	4.79.120.114	TCP	3146 > http [RST, ACK] Seq=431 Ack=9423 Win=0 Len=0
5168	2191.0903	67.19.41.215	10.59.1.17	TCP	[TCP segment of a reassembled PDU]
5169	2191.1043	67.19.41.215	10.59.1.17	TCP	[TCP segment of a reassembled PDU]
5170	2191.1193	10.59.1.17	67.19.41.215	TCP	53877 > http [ACK] Seq=324 Ack=1461 Win=65535 Len=0
5171	2191.1973	67.19.41.215	10.59.1.17	TCP	[TCP segment of a reassembled PDU]
5172	2191.2353	67.19.41.215	10.59.1.17	TCP	[TCP segment of a reassembled PDU]
5173	2191.2593	10.59.1.17	67.19.41.215	TCP	53877 > http [ACK] Seq=324 Ack=5603 Win=65535 Len=0
5174	2191.3204	67.19.41.215	10.59.1.17	HTTP	[TCP Previous segment lost] Continuation or non-HTTP traffic
5175	2191.3204	10.59.1.17	67.19.41.215	TCP	[TCP Dup ACK 5173#1] 53877 > http [ACK] Seq=324 Ack=5603 Win=65535 Len=0
5176	2191.3263	67.19.41.215	10.59.1.17	TCP	[TCP Retransmission] [TCP segment of a reassembled PDU]
5177	2191.3493	10.59.1.17	67.19.41.215	TCP	53877 > http [ACK] Seq=324 Ack=7106 Win=64198 Len=0
5178	2191.3503	10.59.1.17	67.19.41.215	TCP	53877 > http [FIN, ACK] Seq=324 Ack=7106 Win=65535 Len=0
5179	2191.3533	10.59.1.17	67.19.41.215	TCP	53878 > http [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460 WS=0 TSV=905260848 TSER=0
5180	2191.3543	10.59.1.17	67.19.41.215	TCP	53879 > http [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460 WS=0 TSV=905260848 TSER=0
5181	2191.4113	67.19.41.215	10.59.1.17	TCP	http > 53877 [ACK] Seq=7106 Ack=325 Win=6432 Len=0
5182	2191.4173	67.19.41.215	10.59.1.17	TCP	http > 53878 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
5183	2191.4273	67.19.41.215	10.59.1.17	TCP	http > 53879 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460

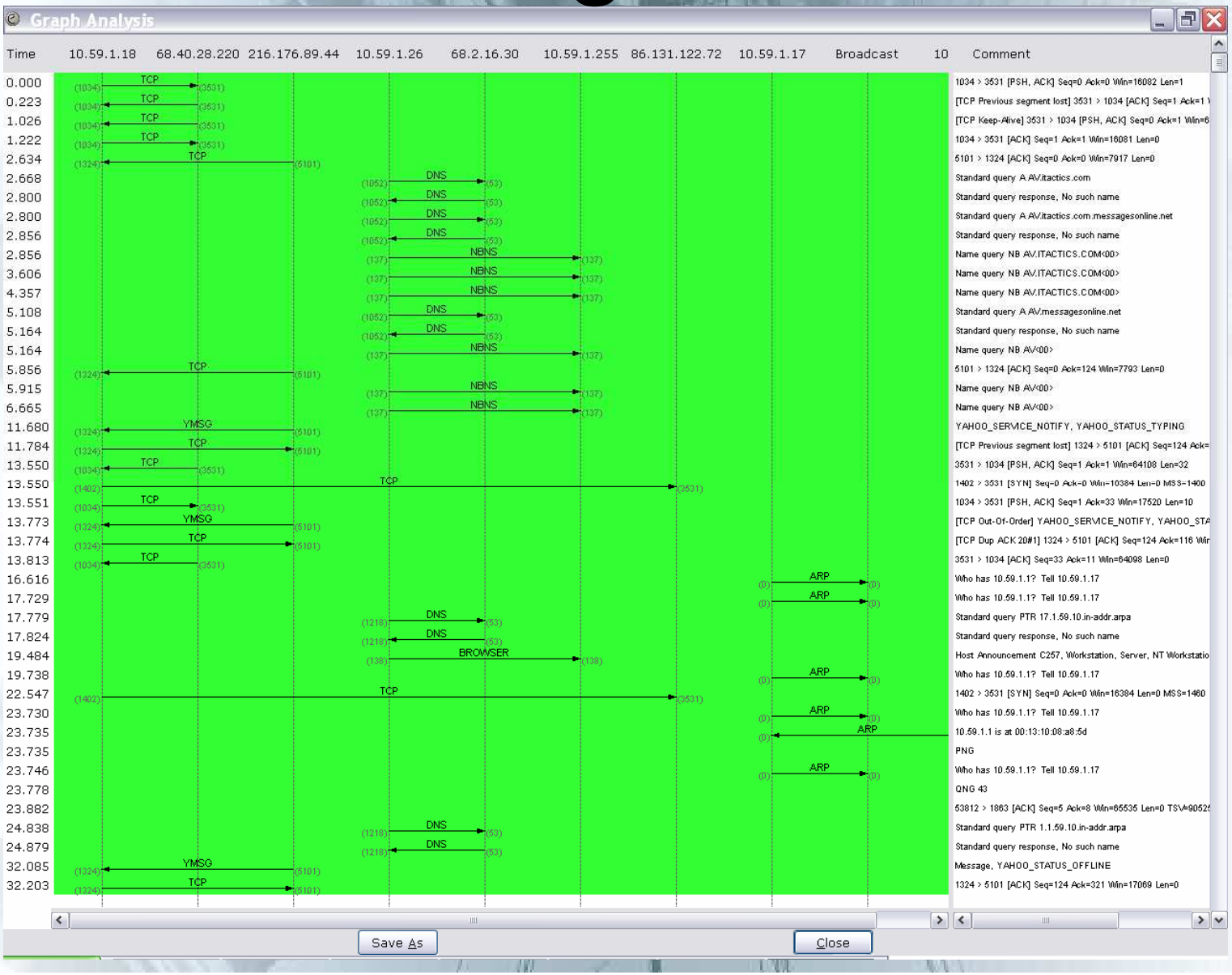
```
⊞ Frame 3238 (477 bytes on wire, 477 bytes captured)
⊞ Ethernet II, Src: 10.59.1.1 (00:13:10:08:a8:5d), Dst: 10.59.1.12 (00:02:6f:34:4a:c7)
⊞ Internet Protocol, Src: 66.94.234.72 (66.94.234.72), Dst: 10.59.1.12 (10.59.1.12)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 3087 (3087), Seq: 1, Ack: 2823, Len: 423
⊟ Hypertext Transfer Protocol
  ⊞ HTTP/1.1 200 OK\r\n
    Date: Mon, 05 Dec 2005 22:39:34 GMT\r\n
    P3P: policyref="http://p3p.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi PUBi IND PHY ON
    Cache-Control: no-cache\r\n
    Connection: close\r\n
    Transfer-Encoding: chunked\r\n
    Content-Type: image/gif\r\n
    \r\n
  ⊞ HTTP chunked response
⊞ Compuserve GIF, Version: GIF89a
```

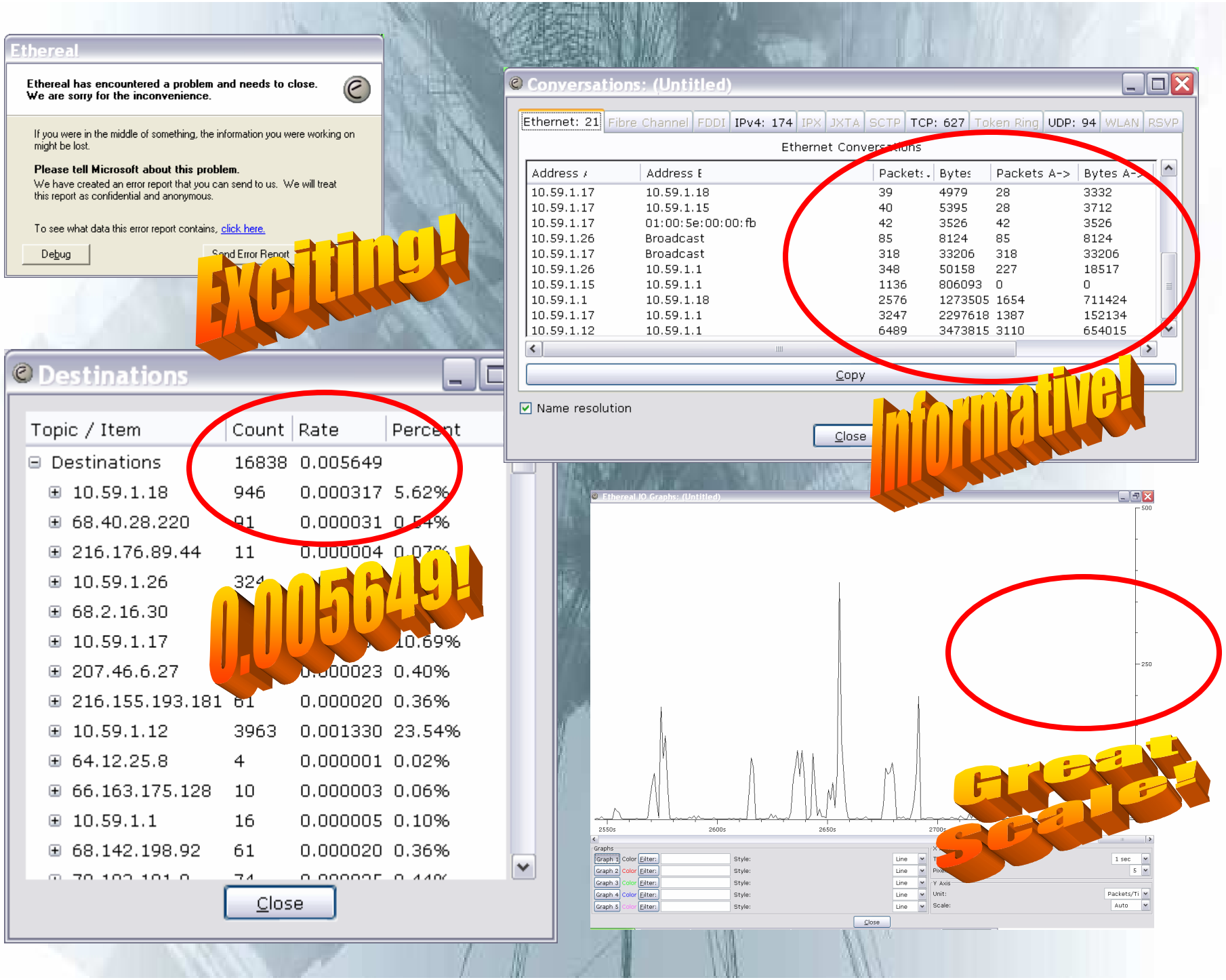
```
0000  00 02 6f 34 4a c7 00 13  10 08 a8 5d 08 00 45 00   ..o4J... ...]..E.
0010  01 cf 6e e0 40 00 32 06  a0 5b 42 5e ea 48 0a 3b   ..n.@.2. .[B^.H.;
0020  01 0c 00 50 0c 0f 2f 40  d2 40 a4 2c a2 eb 50 18   ...P../@ .@.,..P.
0030  ff ff f2 e2 00 00 48 54  54 50 2f 31 2e 31 20 32   ......HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 4d 6f 6e   00 OK..D ate: Mon
0050  2c 20 30 35 20 44 65 63  20 32 30 30 35 20 32 32   , 05 Dec  2005 22
0060  3a 33 39 3a 33 34 20 47  4d 54 0d 0a 50 33 50 3a   :39:34 G MT..P3P:
0070  20 70 6f 6c 69 63 79 72  65 66 3d 22 68 74 74 70    policyr ef="http
0080  3a 2f 2f 70 33 70 2e 79  61 68 6f 6f 2e 63 6f 6d   ://p3p.y ahoo.com
0090  2f 77 33 63 2f 70 33 70  2e 78 6d 6c 22 2c 20 43   /w3c/p3p .xml", C
00a0  50 3d 22 43 41 4f 20 44  53 50 20 43 4f 52 20 43   P="CAO D SP COR C
00b0  55 52 20 41 44 4d 20 44  45 56 20 54 41 49 20 50   UR ADM D EV TAI P
```

Frame (477 bytes) | De-chunked entity body (43 bytes)

Compaq WLAN MultiPort W200 (Micros | P: 13763 D: 13763 M: 0

Ethereal gets visual




Ethereal
Ethereal has encountered a problem and needs to close.
We are sorry for the inconvenience.
If you were in the middle of something, the information you were working on might be lost.
Please tell Microsoft about this problem.
We have created an error report that you can send to us. We will treat this report as confidential and anonymous.
To see what data this error report contains, click here.
Debug
Send Error Report
Exciting!
Conversations: (Untitled)
Ethernet: 21
Fibre Channel
FDDI
IPv4: 174
IPX
JXTA
SCTP
TCP: 627
Token Ring
UDP: 94
WLAN
RSVP
Ethernet Conversations
Address A
Address B
Packets
Bytes
Packets A->
Bytes A->
10.59.1.17 10.59.1.18 39 4979 28 3332
10.59.1.17 10.59.1.15 40 5395 28 3712
10.59.1.17 01:00:5e:00:00:fb 42 3526 42 3526
10.59.1.26 Broadcast 85 8124 85 8124
10.59.1.17 Broadcast 318 33206 318 33206
10.59.1.26 10.59.1.1 348 50158 227 18517
10.59.1.15 10.59.1.1 1136 806093 0 0
10.59.1.1 10.59.1.18 2576 1273505 1654 711424
10.59.1.17 10.59.1.1 3247 2297618 1387 152134
10.59.1.12 10.59.1.1 6489 3473815 3110 654015
Copy
Name resolution
Close
Informative!
Destinations
Topic / Item
Count
Rate
Percent
Destinations 16838 0.005649
10.59.1.18 946 0.000317 5.62%
68.40.28.220 91 0.000031 0.54%
216.176.89.44 11 0.000004
10.59.1.26
68.2.16.30
10.59.1.17 10.69%
207.46.6.27 0.000023 0.40%
216.155.193.181 61 0.000020 0.36%
10.59.1.12 3963 0.001330 23.54%
64.12.25.8 4 0.000001 0.02%
66.163.175.128 10 0.000003 0.06%
10.59.1.1 16 0.000005 0.10%
68.142.198.92 61 0.000020 0.36%
0.005649!
Close
Ethereal IO Graphs: (Untitled)
500
250
2550s
2600s
2650s
2700s
Graphs
Graph 1
Graph 2
Graph 3
Graph 4
Graph 5
Color
Filter:
Style:
Line
Y Axis
Unit:
Packets/Ti
Scale:
Auto
1 sec
Close
Great Scale!

Ethereal

- I don't wanna pick on it:
  - Great (fantastic even?) **DIAGNOSTIC** tool
  - GREAT if you want to move from MICRO FOCUS and gradually expand into HYPER CRYSTAL CLARITY
- But
  - Not so great to determine policy violations made by people
  - Not so great for security planning
  - Not so great to get baselines of big networks
    - Why? Hard to see features over long periods of time
  - <u>I want the outer limits: to change the focus to a soft blur, or sharpen it to crystal clarity.</u>

So I started dreaming

- How do you describe a representation or a feature you want to see?
  - In English first, then in some precise representation?
  - Relevance is not a true/false bivalent concept
- Translate this into SQL
  - “Usually” and “Occasionally”
  - “about as often as”
  - Network is **very** quiet
  - Traffic between two hosts is **very** heavy
  - Server has **many** ports open
  - Host communicates over the internet **most** of the time

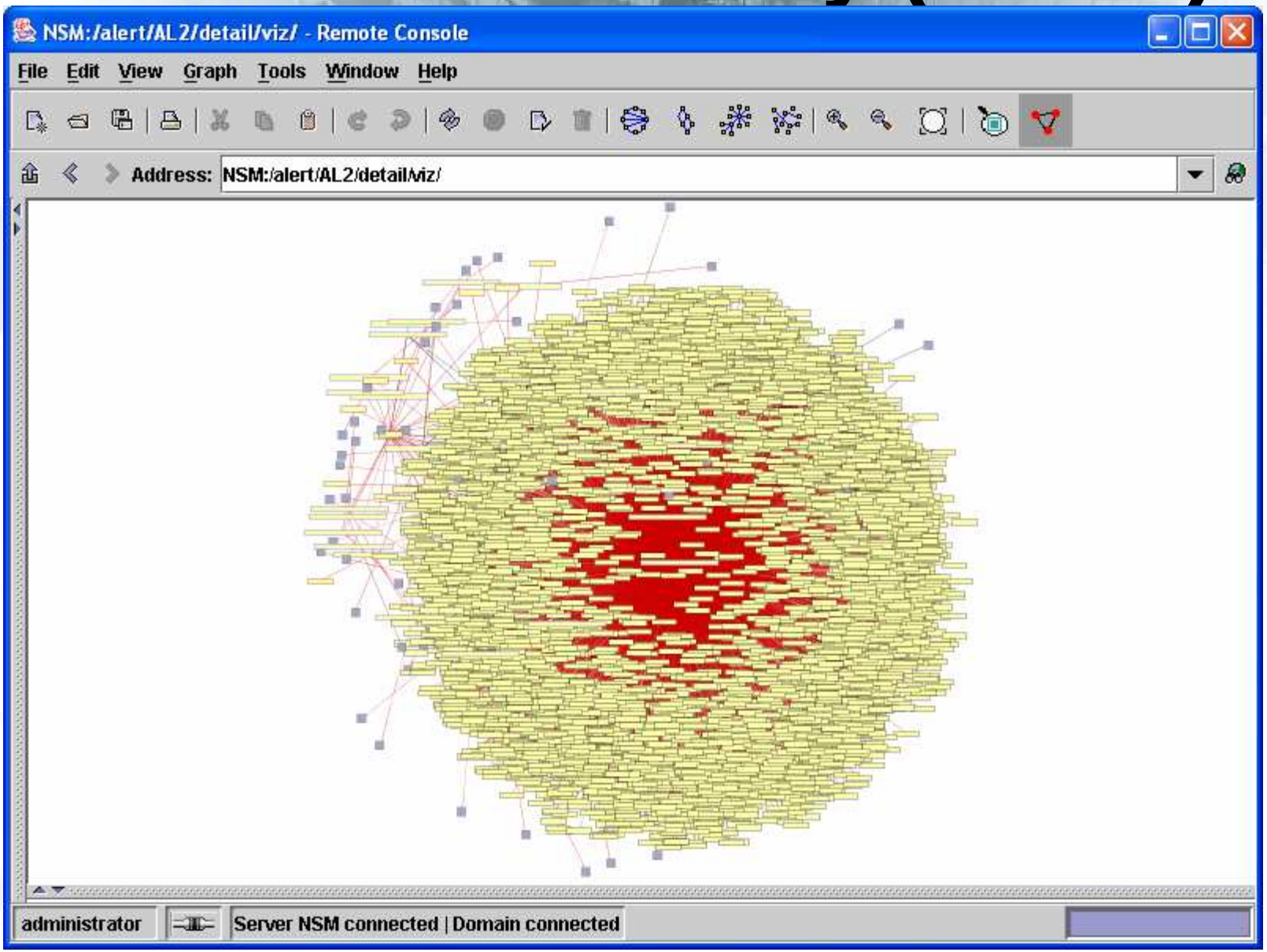
At this point I determined

NEW, MORE SCIENTIFIC WAYS WERE NEEDED

So I set some big goals

- I set some goals
  - How to filter out big amounts of noise from certain kinds of attacks
  - How to see what I need to protect
  - How to see ‘mysterious’ traffic separated from normal traffic

A bad network day (SNOT)

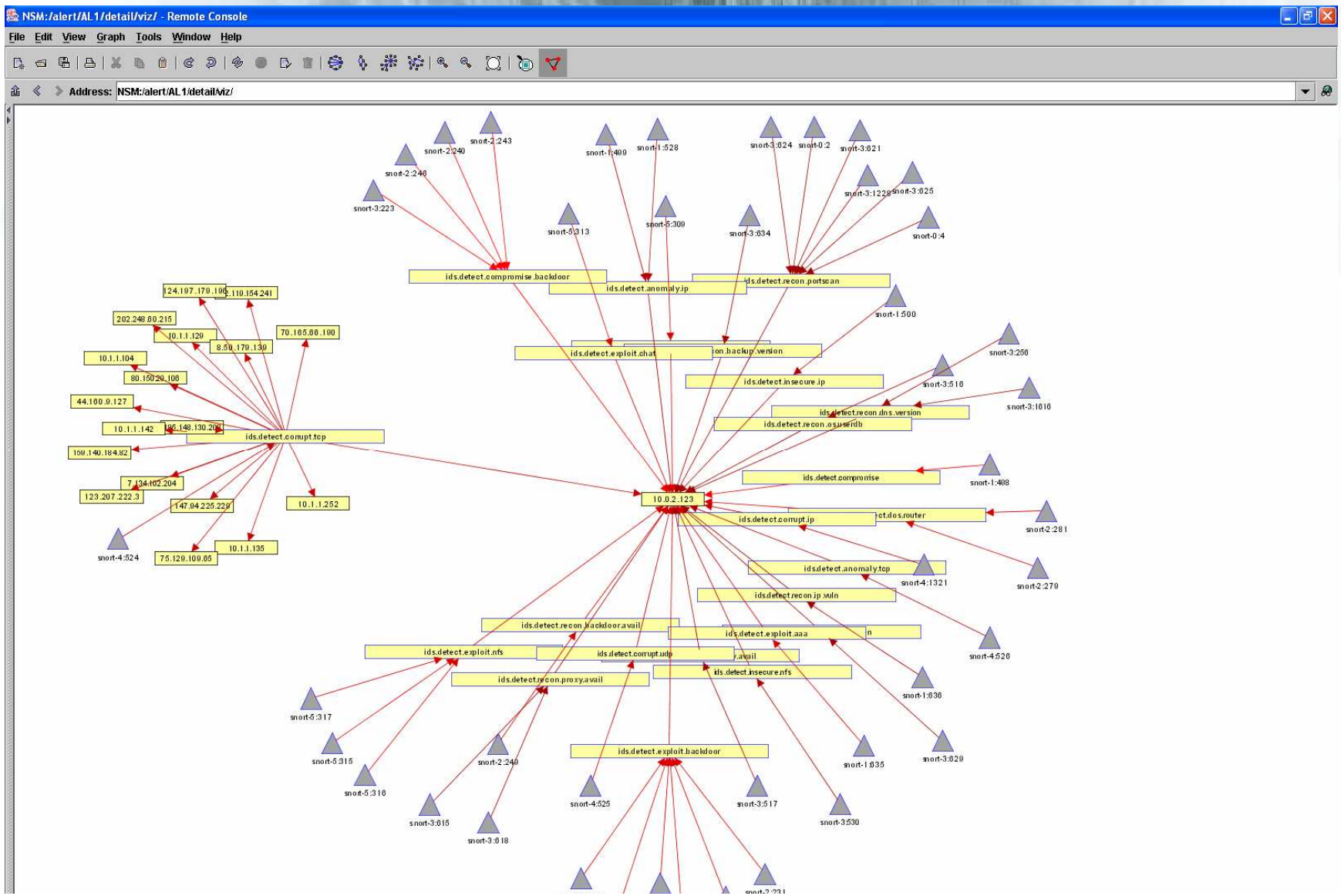


Show me the attack signature, attack type, and target where target is **real** host.

BDL:

Event_id –priority> taxonomy_type –priority> t_ip.isa(real_host)

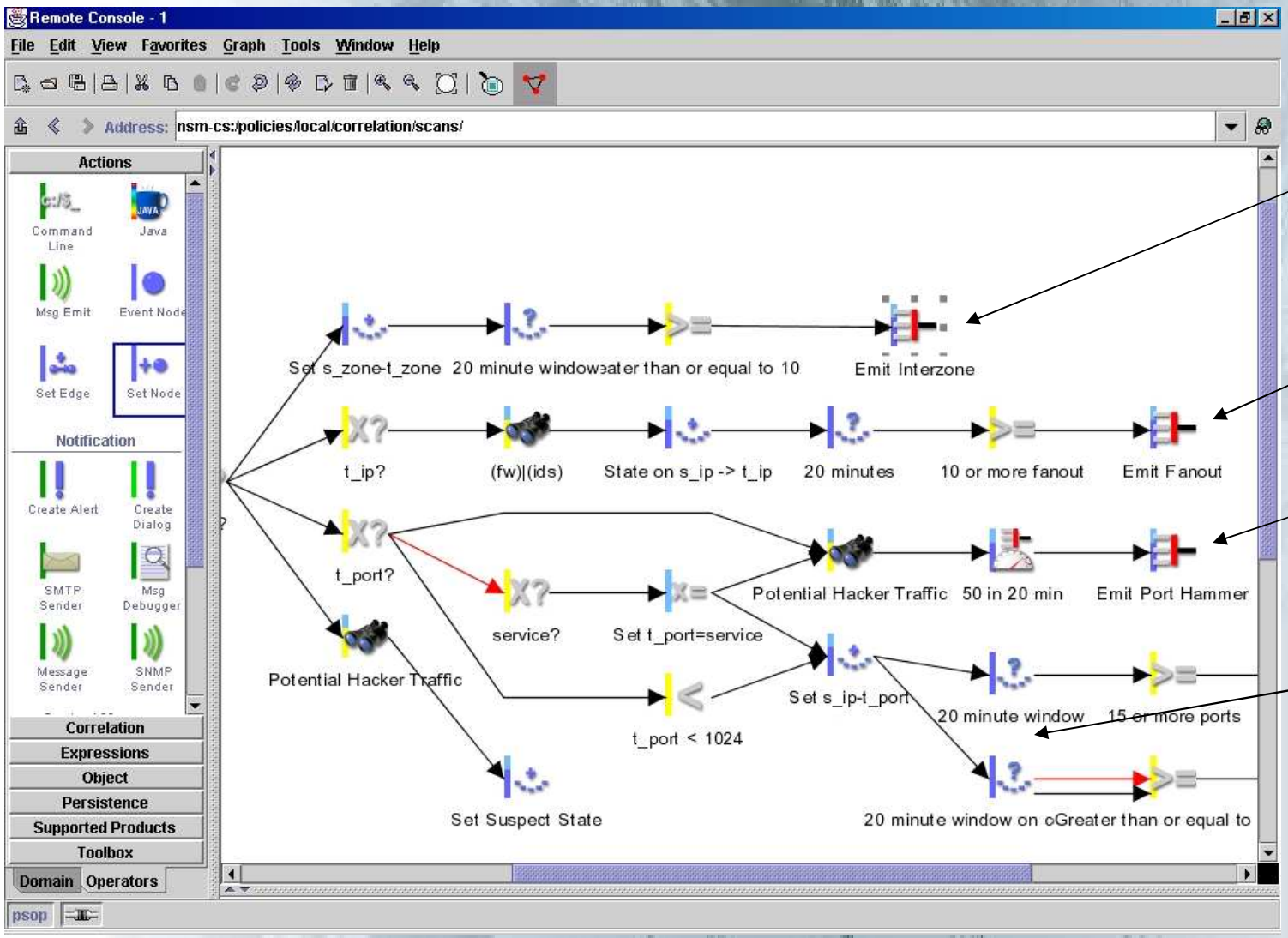
Hmm, it's just one host being hit



How did we do that?

- Each picture is just a ‘connect the dots’ with each node given a name, and what it relates to. Simple rules are given in a visual language to
  - a) extract features
  - b) build a semantic graph that we can look at
  - c) use different shapes/colors
- Essentially:
  - Event_id → taxonomy_type → t_ip.isa(real_host)

An example of a visual language to select features



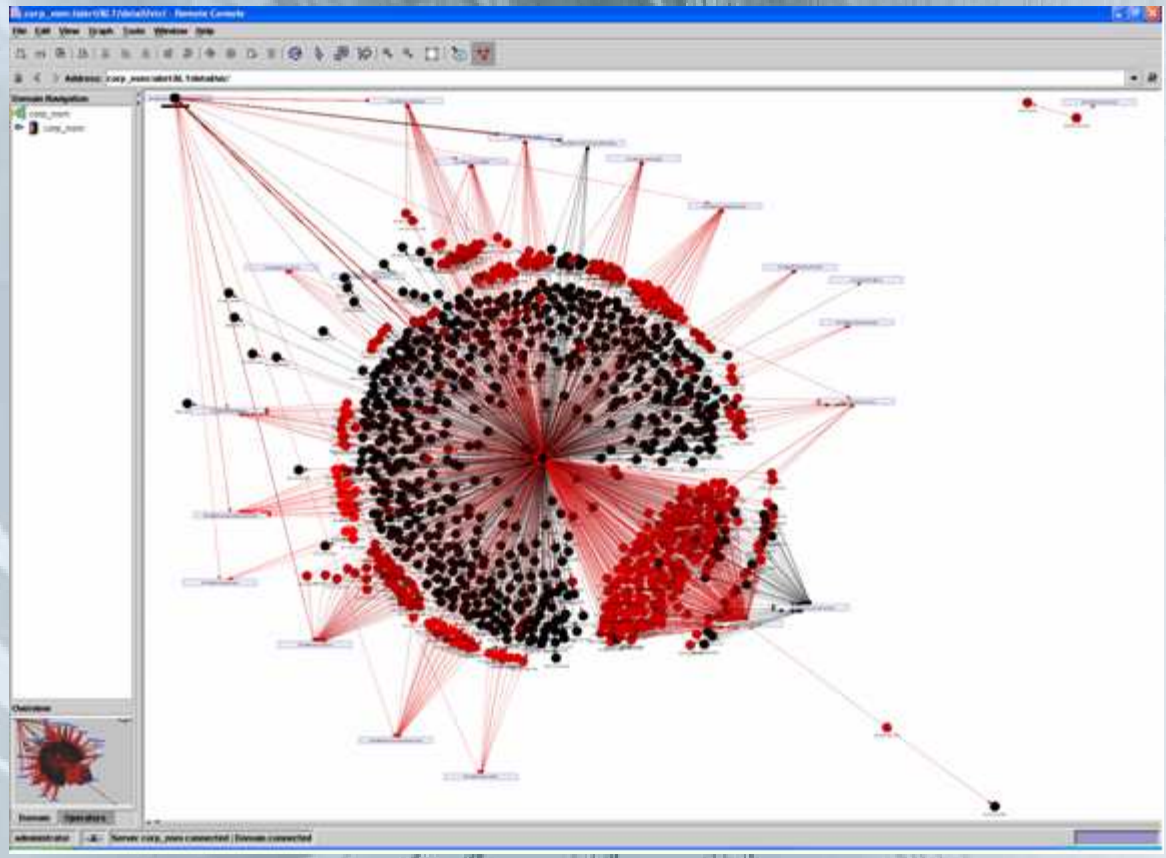
Business Unit Ingress/ egress

Scans/worms

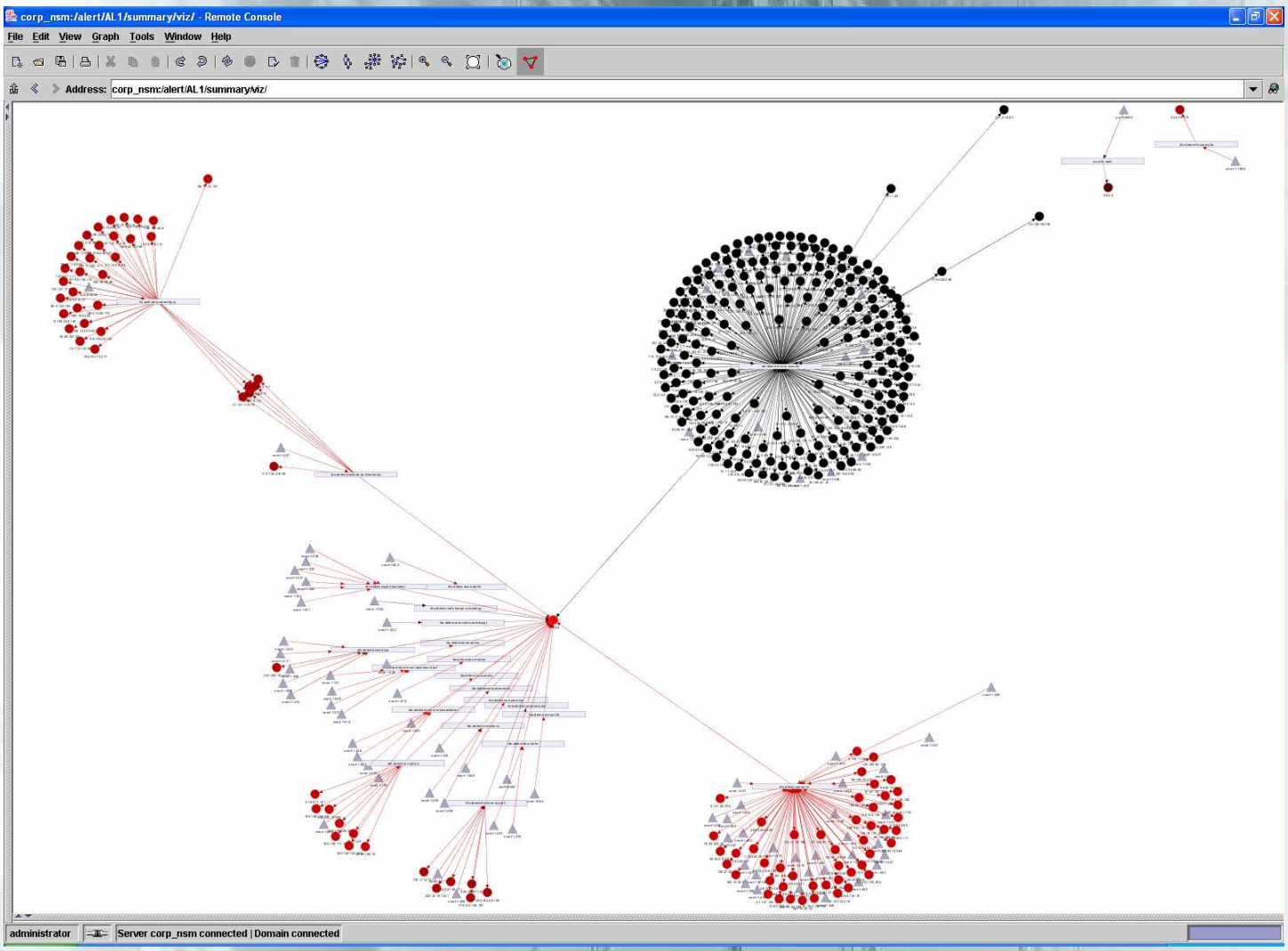
Port DOS Attacks

Quick Scans

Another SNOT attack on a different network topology



Same Feature Visualization

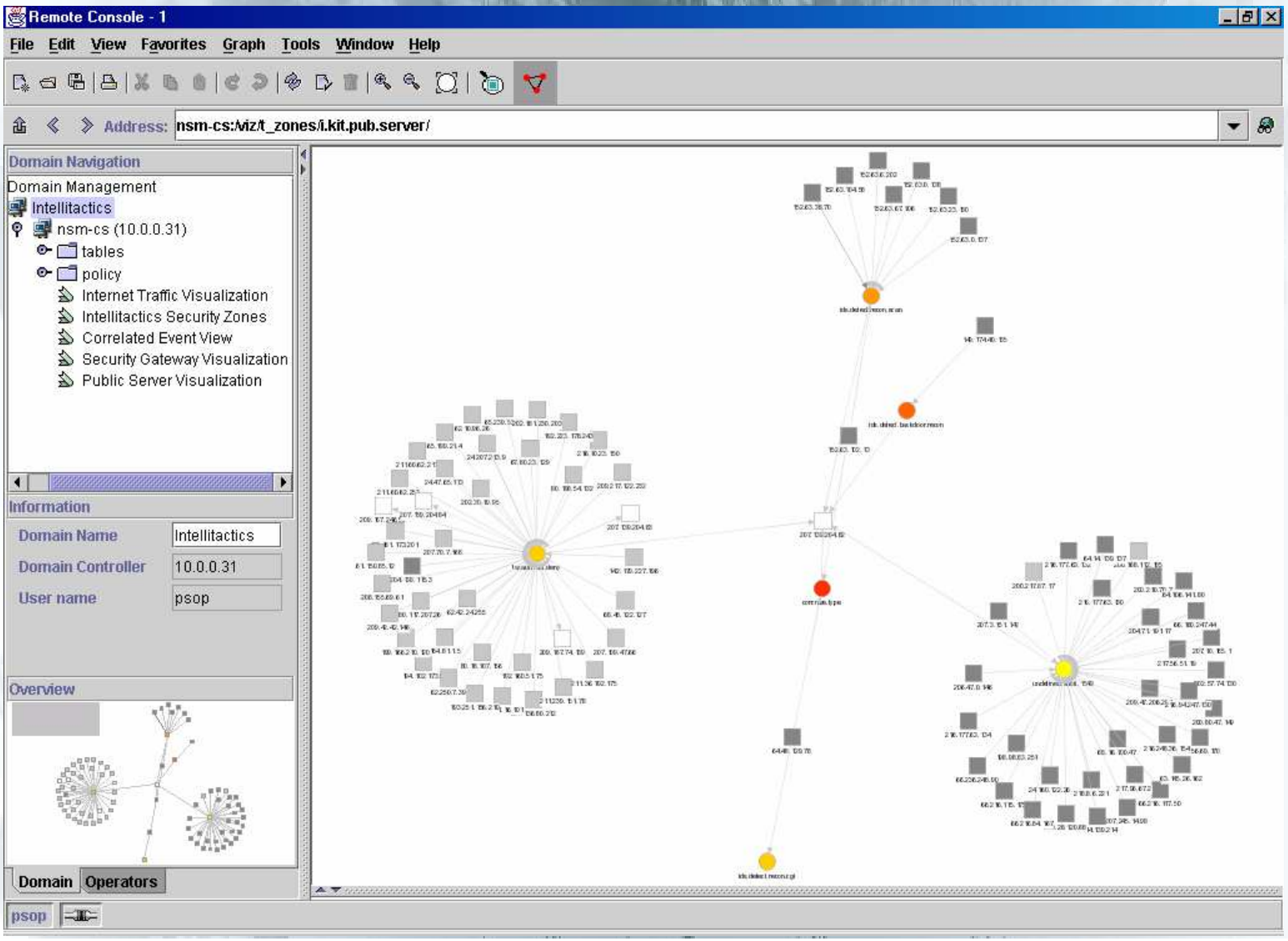


So, the ability to group features was deemed useful, people rejoiced

All we had to do was to:

- Store historic state for hosts
  - What ports it has open
  - What ports it is *USING* -- **big difference**
  - JUST WHO connects to the ports
  - WHEN do they connect
  - WHERE are they connecting to (IP, and logical names)
  - WHAT DOES THE HOST CONNECT TO?
  - Has it ever done anything bad?
- Use world knowledge not in sniffers, nessus, etc…
  - Classification of server (e.g. criticality)
  - Geographic and business unit membership

Historical Behavior and Business Heuristics

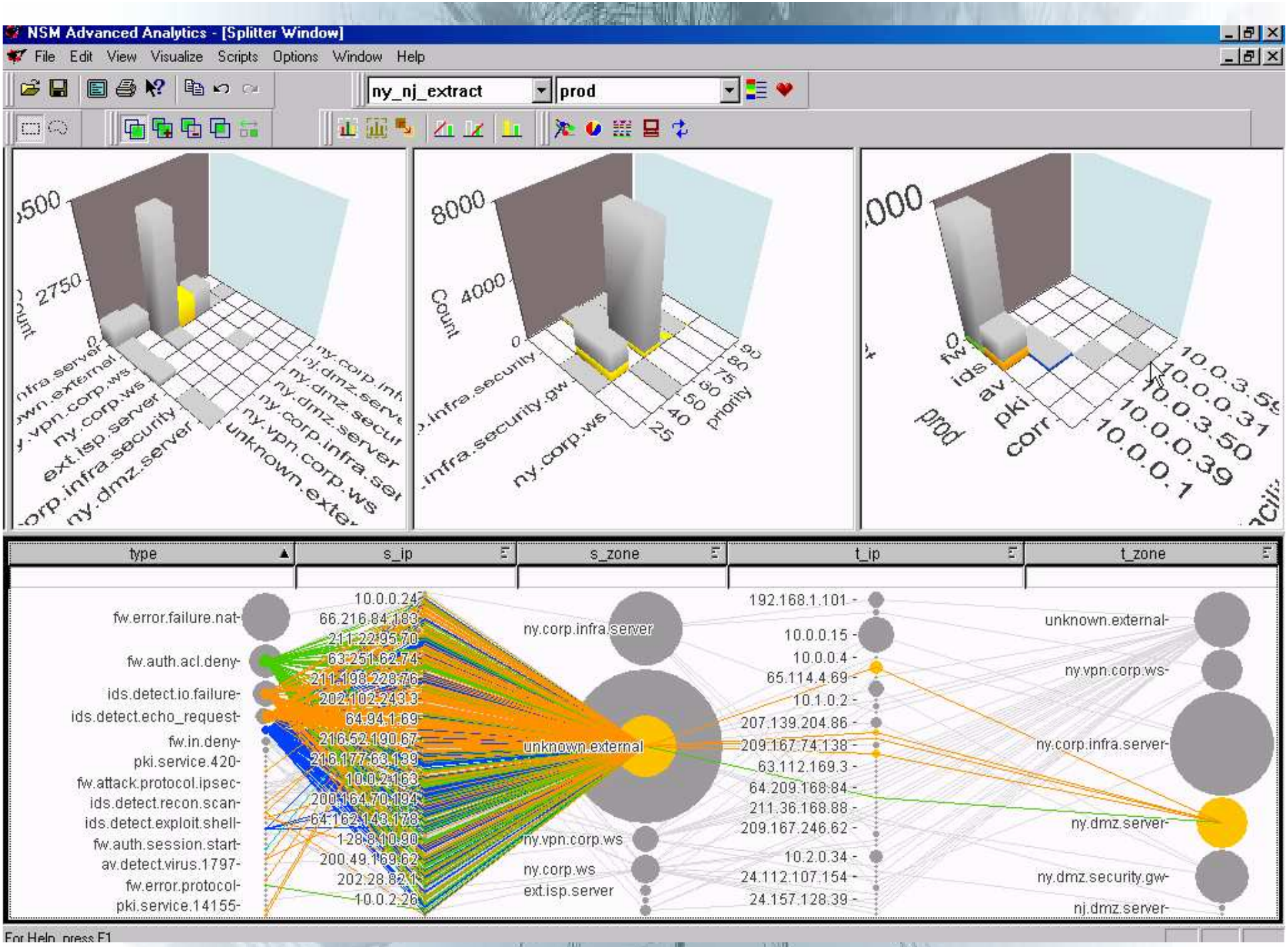


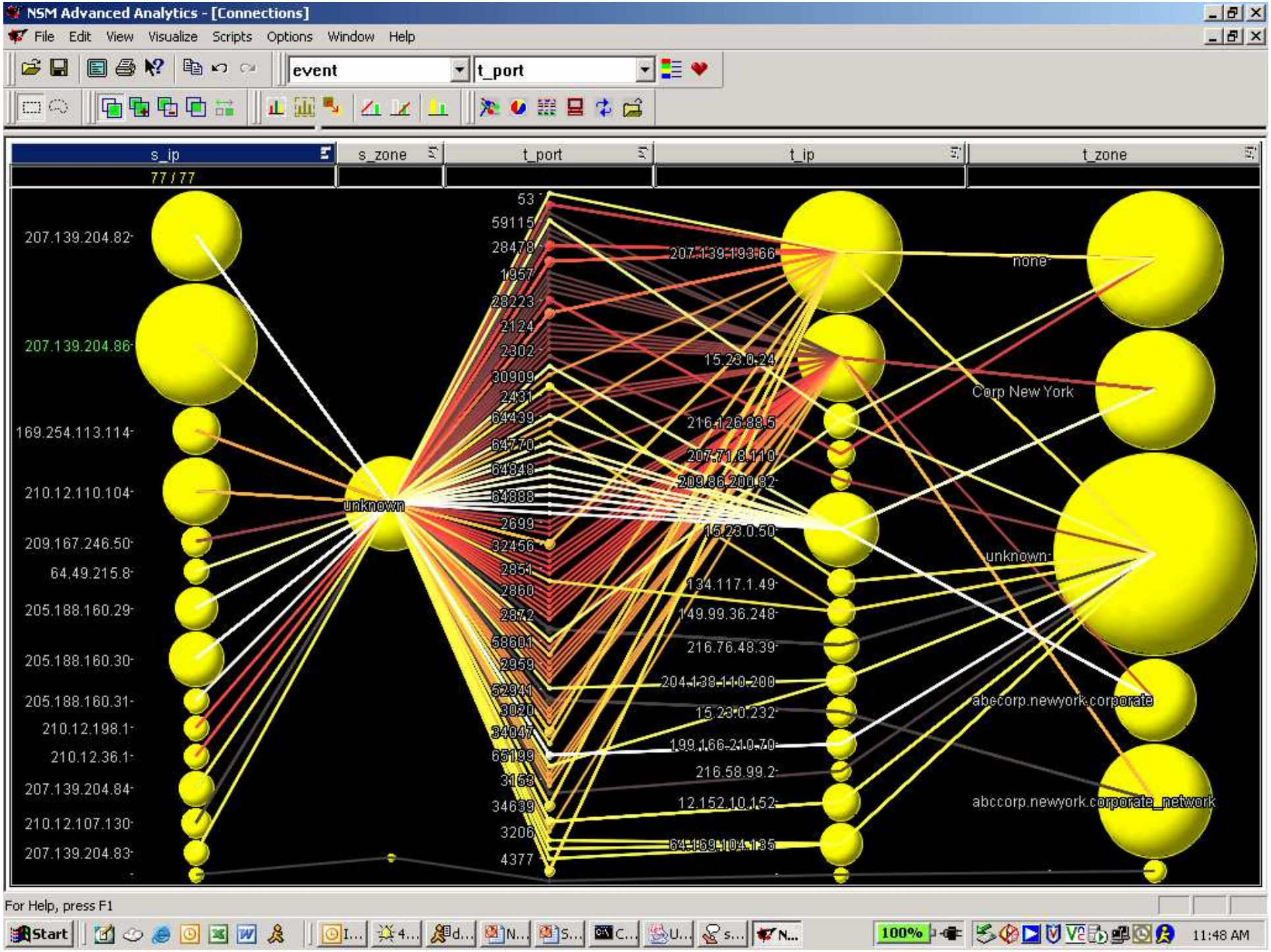
Quest UPDATE

- I had found simple ways to set up rules to select specific features
  - No SQL needed – visual object flow diagram
  - Updated all models as events came in
  - Supplied great insights into networks - fingerprints
- It was also
  - Pretty slow! Ate lots of RAM and CPU too!
  - Everyone appreciated their desktop upgrades!
  - Not so good for ad-hoc analysis, filtering, or pivots.
- YOU CAN DO IT FOR FREE
  - Anyone can do much the same with shell scripting and AT&T's GraphViz for free!

The next goal:

- The next goals was to make it easier to looking at network traffic by
  - Reducing dimensions (too many IP's!)
    - Signatures →Taxonomy of events
    - IP Addresses → Business units
  - Time travel (zoom in and out)
    - Wanted like MRTG, but interactive

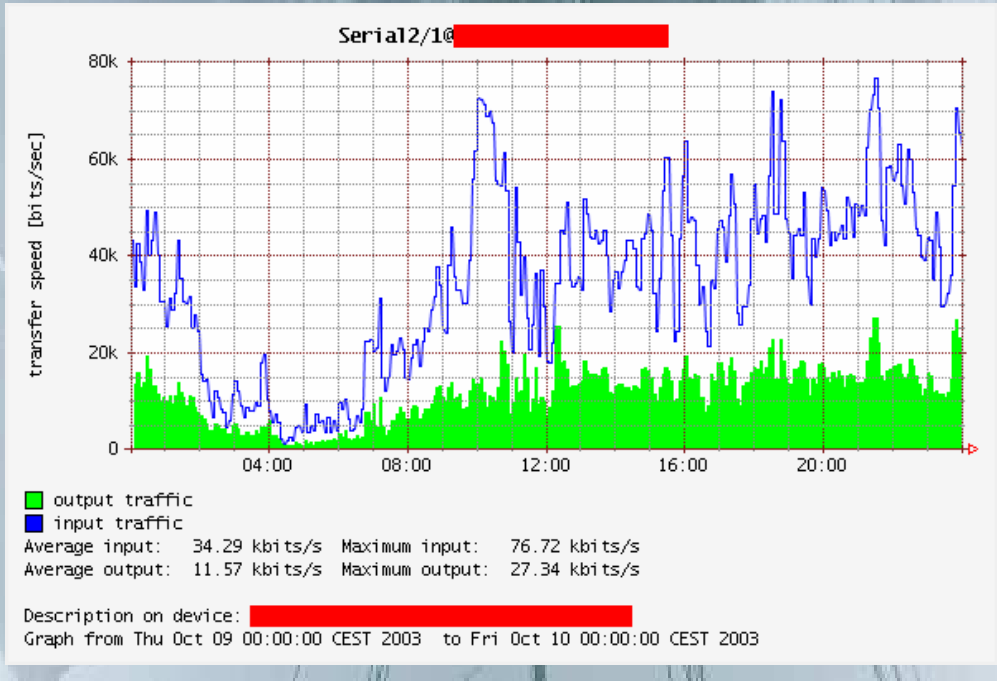

NSM Advanced Analytics - [Splitter Window]
File Edit View Visualize Scripts Options Window Help
ny_nj_extract
prod
Count
priority
prod
type
s_ip
s_zone
t_ip
t_zone
fw.error.failure.nat-
fw.auth.acl.deny-
ids.detect.io.failure-
ids.detect.echo_request-
fw.in.deny-
pki.service.420-
fw.attack.protocol.ipsec-
ids.detect.recon.scan-
ids.detect.exploit.shell-
fw.auth.session.start-
av.detect.virus.1797-
fw.error.protocol-
pki.service.14155-
ny.corp.infra.server
unknown.external
ny.vpn.corp.ws
ny.corp.ws
ext.isp.server
192.168.1.101 -
10.0.0.15 -
10.0.0.4 -
65.114.4.69 -
10.1.0.2 -
207.139.204.86 -
209.167.74.138 -
63.112.169.3 -
64.209.168.84 -
211.36.168.88 -
209.167.246.62 -
10.2.0.34 -
24.112.107.154 -
24.157.128.39 -
unknown.external-
ny.vpn.corp.ws-
ny.corp.infra.server-
ny.dmz.server-
ny.dmz.security.gw-
nj.dmz.server-
For Help, press F1

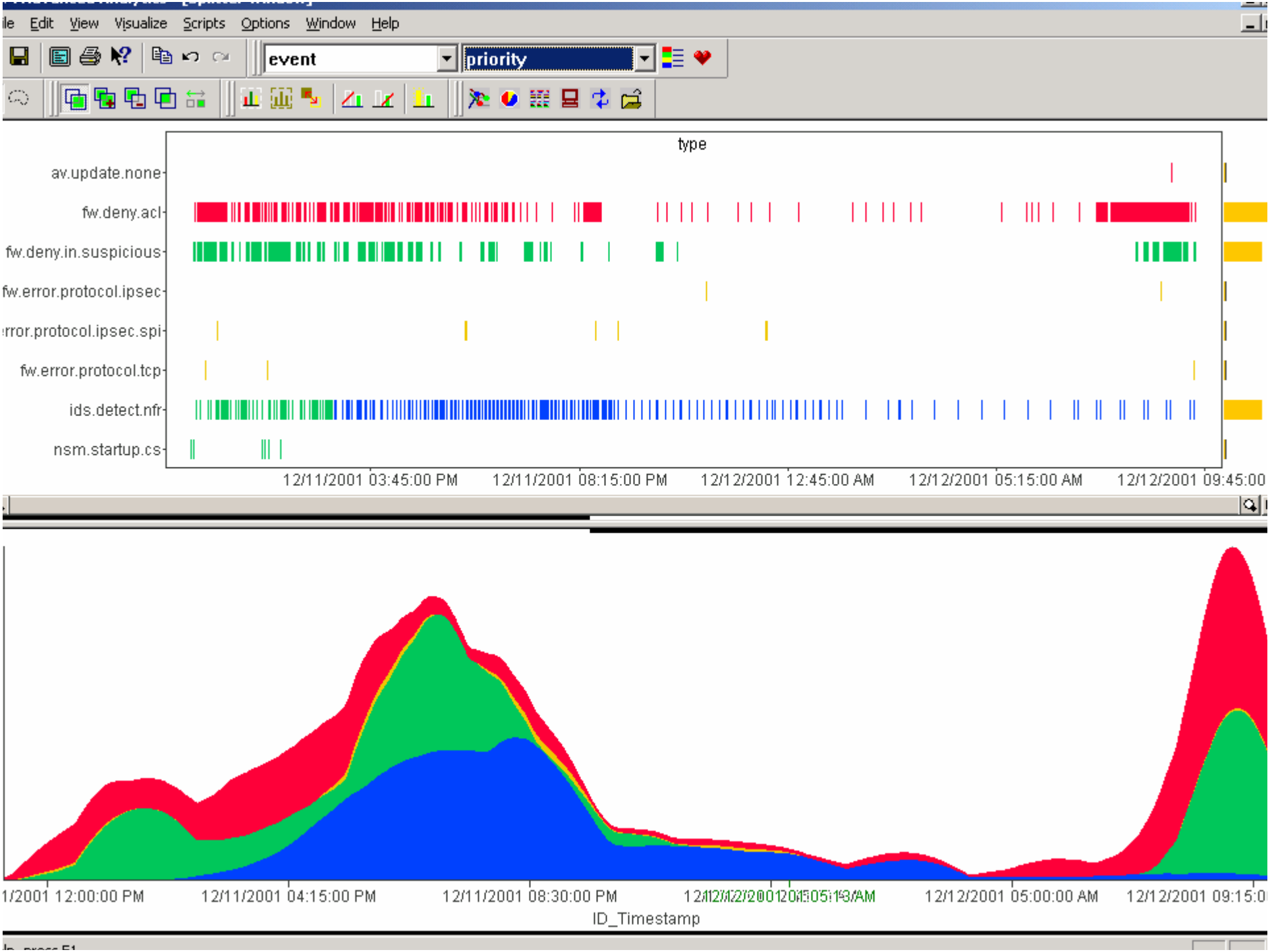

NSM Advanced Analytics - [Connections]
File Edit View Visualize Scripts Options Window Help
event
t_port
s_ip
s_zone
t_port
t_ip
t_zone
77 / 77
207.139.204.82
207.139.204.86
169.254.113.114
210.12.110.104
209.167.246.50
64.49.215.8
205.188.160.29
205.188.160.30
205.188.160.31
210.12.198.1
210.12.36.1
207.139.204.84
210.12.107.130
207.139.204.83
unknown
53
59115
28478
1957
28223
2124
2302
30909
2431
64439
64770
64848
64888
2699
32456
2851
2860
2872
58601
2959
52941
3020
34047
65199
3168
34639
3206
4377
207.139.198.66
15.23.0.24
216.126.88.5
207.71.8.110
209.86.200.82
15.23.0.50
134.117.1.49
149.99.36.248
216.76.48.39
204.138.110.200
15.23.0.232
199.166.210.70
216.58.99.2
12.152.10.152
64.169.104.135
none
Corp New York
unknown
abccorp.newyork.corporate
abccorp.newyork.corporate_network
For Help, press F1
Start
100%
11:48 AM

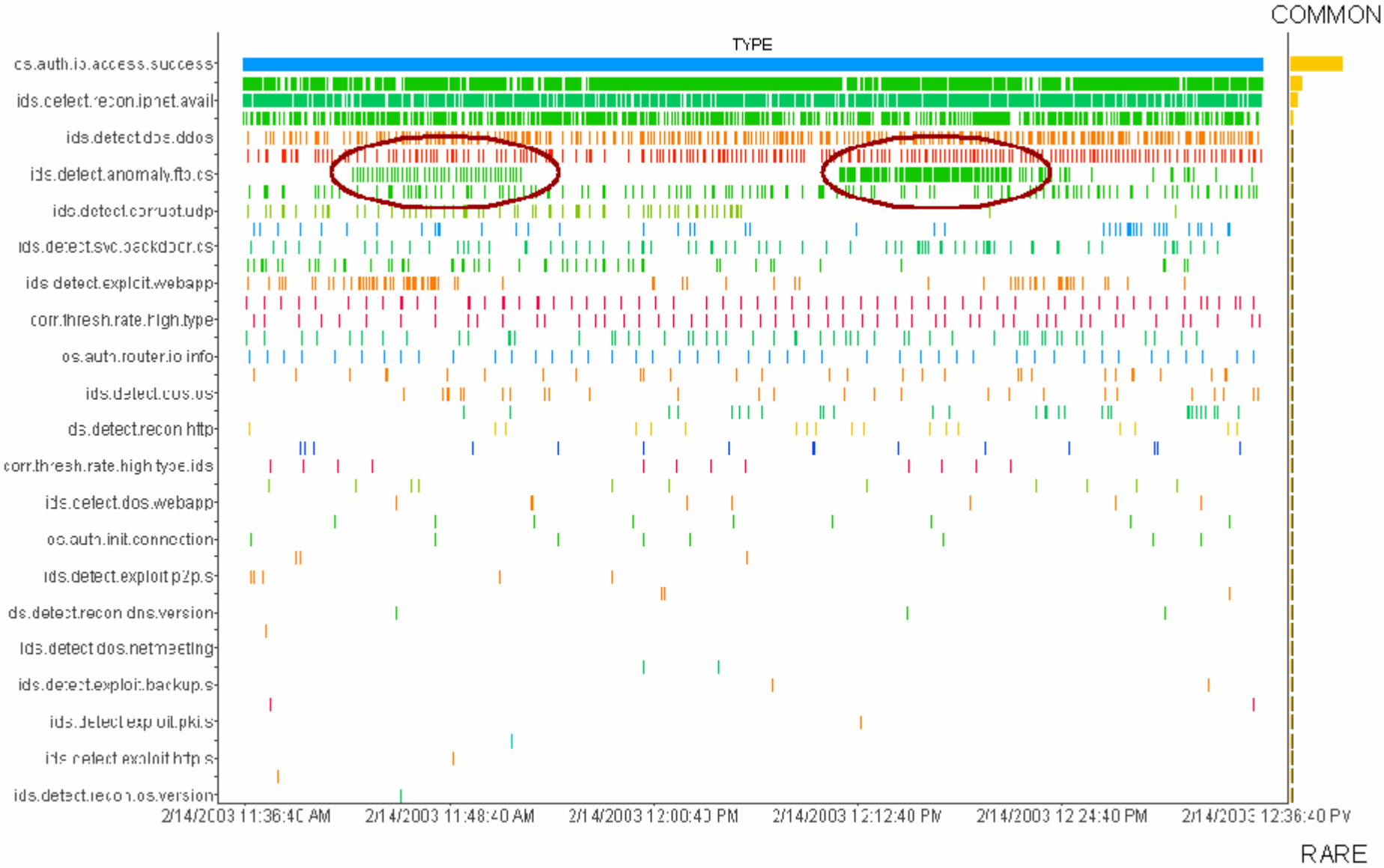
Business Labels = Big Happy

- So business labels were a good idea and helped everyone understand traffic's legitimacy in a business context for the first time.
  - Where do you put this in network devices in a consistent and structured way? I don't see it!

- But all the things you've shown so far seem to lack the **<u>time dimension</u>**. Often, we need to know what happened before something else.




Edit View Visualize Scripts Options Window Help
event
priority
type
av.update.none
fw.deny.acl
fw.deny.in.suspicious
fw.error.protocol.ipsec
rror.protocol.ipsec.spi
fw.error.protocol.tcp
ids.detect.nfr
nsm.startup.cs
12/11/2001 03:45:00 PM
12/11/2001 08:15:00 PM
12/12/2001 12:45:00 AM
12/12/2001 05:15:00 AM
12/12/2001 09:45:00
1/2001 12:00:00 PM
12/11/2001 04:15:00 PM
12/11/2001 08:30:00 PM
12/12/2001 05:00:00 AM
ID_Timestamp


COMMON
TYPE
cs.auth.io.access.success
ids.detect.recon.ipnet.avail
ids.detect.dos.ddos
ids.detect.anomaly.fto.cs
ids.detect.corrupt.udp
ids.detect.svc.backdoor.cs
ids.detect.explicit.webapp
corr.thresh.rate.high.type
os.auth.router.io.info
ids.detect.dos.os
ds.detect.recon.http
corr.thresh.rate.high.type.ids
ids.detect.dos.webapp
os.auth.init.connection
ids.detect.exploit.p2p.s
ds.detect.recon.dns.version
ids.detect.dos.netmeeting
ids.detect.exploit.backup.s
ids.detect.exploit.pki.s
ids.detect.exploit.http.s
ids.detect.recon.os.version
2/14/2003 11:36:40 AM
2/14/2003 11:48:40 AM
2/14/2003 12:00:40 PM
2/14/2003 12:12:40 PM
2/14/2003 12:24:40 PM
2/14/2003 12:36:40 PM
RARE

So!

- It seems that we can look at
  - Frames and Packets
  - Traffic Groupings
  - Business Centric views
- But a lot is still left up to interpretation by the analyst and their experience. One might assume that two analysts looking at the same visualization will have different takes on what they see.
- That's because it's a perceptual problem.
- What can we do about coding common perceptions so the software will be even smarter?

CHECKPOINTING

- Feature map built from by
  - Compositional rules to build visualization graphs (you could call it correlation)
  - Ontological membership
  - Business labels: geographic, criticality
- Lots of ways to view said info
  - Directed Graphs (shapes, colors)
  - 3D business label
  - Connection flow diagrams
  - Unique scatter plots of events/time uncovered new ways of looking at data
  - NO PIE AND BAR CHARTS NEED APPLY!

What I felt was next step

- The widgets were pretty good, but specifying features got hard.
  - Easy to specify things that were terribly inefficient. (happens to most expert systems)
- I decided to **refactor** and use something called **ProtoForm** language (PFL) and create a database of about 150 deduction rules.
  - Mapped into GCL (generalized constraint langauge)

Decision Table

Name	A_1	A_j	A_n	D
$Name_1$	a_{11}	a_{1j}	a_{in}	d_1
.	.	.	.	.
$Name_k$	a_{k1}	a_{kj}	a_{kn}	d_1
$Name_{k+1}$	$a_{k+1,1}$	$a_{k+1,j}$	$a_{k+1,n}$	d_2
.	.	.	.	.
$Name_l$	a_{l1}	a_{lj}	a_{ln}	d_l
.	.	.	.	.
$Name_n$	a_{m1}	a_{mj}	a_{mn}	d_r

A_j: The jth symptom

a_{ij}: The value of jth symptom name

D: Diagnosis

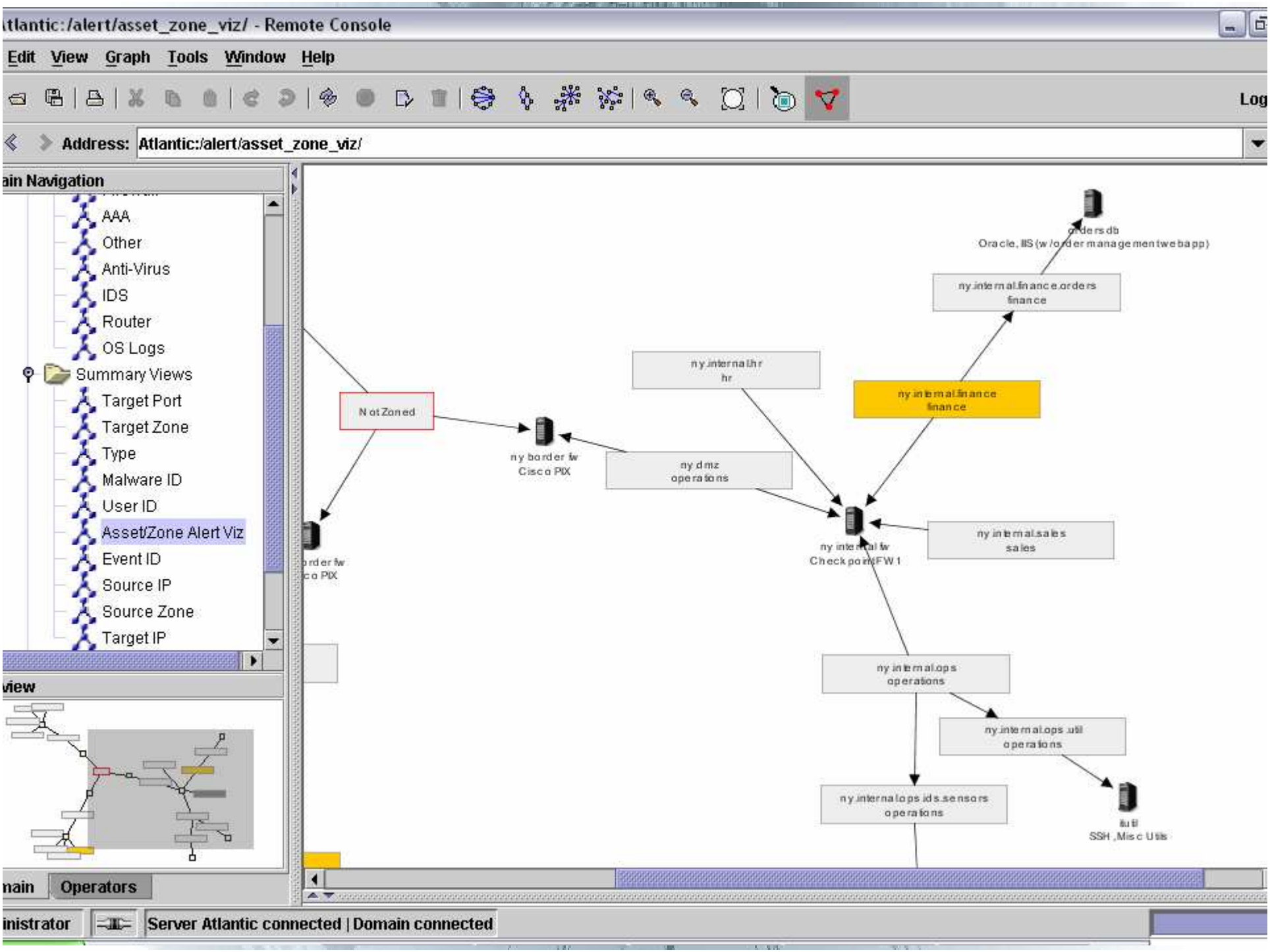
Fuzzy knowledgebase

- Fuzzy if then rules:
- (X isp R) and (X,Y) is S)
- (X isr R) is unlikely) and (X iss S) is likely
- if X is small then Y is large

- equality constraints
- inequality
- subsethood
- possibilistic constraint
- veristic constraint
- probabalistic constraint
- random set constraint
- fuzzy graph constraint
- usuality constraint (X isu R means usually (X is R)
- Pawlak set constraint (upper and lower approximations to X)

So I came up with 150 features

- I brainstormed in 2004 for several months and came up with about 150 ‘views’ on the world that I’d like to see.
  - Users getting lots of spam
  - Users wasting time on the internet
  - Rare/first time connections to sensitive assets
  - Any asset that gets connections from more than 3 business units
  - …


Atlantic:/alert/asset_zone_viz/ - Remote Console
Edit View Graph Tools Window Help
Log
Address: Atlantic:/alert/asset_zone_viz/
Main Navigation
AAA
Other
Anti-Virus
IDS
Router
OS Logs
Summary Views
Target Port
Target Zone
Type
Malware ID
User ID
Asset/Zone Alert Viz
Event ID
Source IP
Source Zone
Target IP
View
Main
Operators
Not Zoned
ny.border.fw
Cisco PIX
ny.dmz
operations
ny.internal.hr
hr
ny.internal.finance
finance
ny.internal.finance.orders
finance
ordersdb
Oracle, IIS (w/ordermanagementwebapp)
ny.internal.fw
Checkpoint FW1
ny.internal.sales
sales
ny.internal.ops
operations
ny.internal.ops.util
operations
util
SSH, Misc Utils
ny.internal.ops.ids.sensors
operations
Administrator
Server Atlantic connected | Domain connected

Atlantic:/alert/alertviews/secondary/ids/ - Remote Console

File Edit View Graph Tools Window Help

Log Out

Address: Atlantic:/alert/alertviews/secondary/ids/

Domain Navigation

- Atlantic
  - Atlantic
    - Alert Monitoring (SOC)
      - Primary Alerts
      - Secondary (Device Class)
        - ISM Correlation
        - Database
        - Firewall
        - AAA
        - Other
        - Anti-Virus
        - IDS
        - Router
        - OS Logs
      - Summary Views
        - Target Port
        - Target Zone

Overview

Domain | Operators

Last Seen	Ris...	Priority	Events	Type	Source Host	Target Host
2005/12/02 15:08:13	465	55	1	ids.detect.exploit	6.99.167.155	ordersdb
2005/12/02 15:08:12	865	55	1	ids.detect.exploit.web	10.1.4.41	ordersdb
2005/12/02 15:08:11	465	55	1	ids.detect.corrupt.ip	41.101.128.139	ordersdb
2005/12/02 15:08:09	465	55	1	ids.detect.exploit	216.177.208.248	ordersdb
2005/12/02 15:08:07	465	55	1	ids.detect.exploit	50.96.3.47	ordersdb
2005/12/02 15:08:05	480	60	1	ids.detect.recon.backdoor.avail	9.65.196.94	ordersdb
2005/12/02 15:08:01	465	55	1	ids.detect.exploit	154.153.173.118	ordersdb
2005/12/02 15:07:55	425	55	1	ids.detect.exploit	179.136.202.123	ordersdb
2005/12/02 15:07:53	425	55	1	ids.detect.exploit	160.159.96.76	ordersdb
2005/12/02 15:07:51	410	50	1	ids.detect.recon.portscan	80.106.70.79	ordersdb
2005/12/02 15:07:49	425	55	1	ids.detect.exploit	94.202.65.24	ordersdb
2005/12/02 15:07:45	410	50	1	ids.detect.anomaly.ip	206.150.164.205	ordersdb
2005/12/02 15:07:43	425	55	1	ids.detect.exploit	186.177.63.104	ordersdb
2005/12/02 15:07:41	410	50	1	ids.detect.anomaly.lib	191.56.139.201	ordersdb
2005/12/02 15:07:39	425	55	1	ids.detect.exploit	233.31.19.211	ordersdb
2005/12/02 15:07:35	545	95	1	ids.detect.compromise.backd...	176.97.253.215	ordersdb
2005/12/02 15:07:33	425	55	1	ids.detect.exploit	220.178.247.140	ordersdb
2005/12/02 15:07:27	425	55	1	ids.detect.exploit	15.163.6.157	ordersdb
2005/12/02 15:07:25	545	95	1	ids.detect.compromise.backd...	165.131.192.121	ordersdb
2005/12/02 15:07:23	425	55	1	ids.detect.exploit	96.244.166.184	ordersdb
2005/12/02 15:07:21	425	55	1	ids.detect.exploit	71.156.14.12	ordersdb
2005/12/02 15:07:19	445	75	1	ids.detect.error.comsec.decr...	207.24.71.18	ordersdb
2005/12/02 15:07:17	385	55	1	ids.detect.corrupt.ip	130.243.29.104	ordersdb
2005/12/02 15:07:15	370	50	1	ids.detect.recon.net.topology	130.243.29.104	ordersdb
2005/12/02 15:07:13	385	55	1	ids.detect.exploit	56.93.196.34	ordersdb
2005/12/02 15:07:11	385	55	1	ids.detect.exploit	155.225.97.193	ordersdb
2005/12/02 15:07:09	385	55	1	ids.detect.exploit	17.65.154.24	ordersdb
2005/12/02 15:07:07	385	55	1	ids.detect.exploit	194.102.134.74	ordersdb

Play Stop Play

administrator | Server Atlantic connected | Domain connected

- And party with our friends with better screens, like this:

tlantic:/alert/alertviews/primary/ - Remote Console

Edit View Graph Tools Window Help

Log

Address: Atlantic:/alert/alertviews/primary/

ain Navigation

- tlantic
- Atlantic
- Alert Monitoring (SOC)
  - Primary Alerts
  - Secondary (Device Class)
    - ISM Correlation
    - Database
    - Firewall
    - AAA
    - Other
    - Anti-Virus
    - IDS
    - Router
    - OS Logs
  - Summary Views
    - Target Port
    - Target Zone

view

nain | Operators

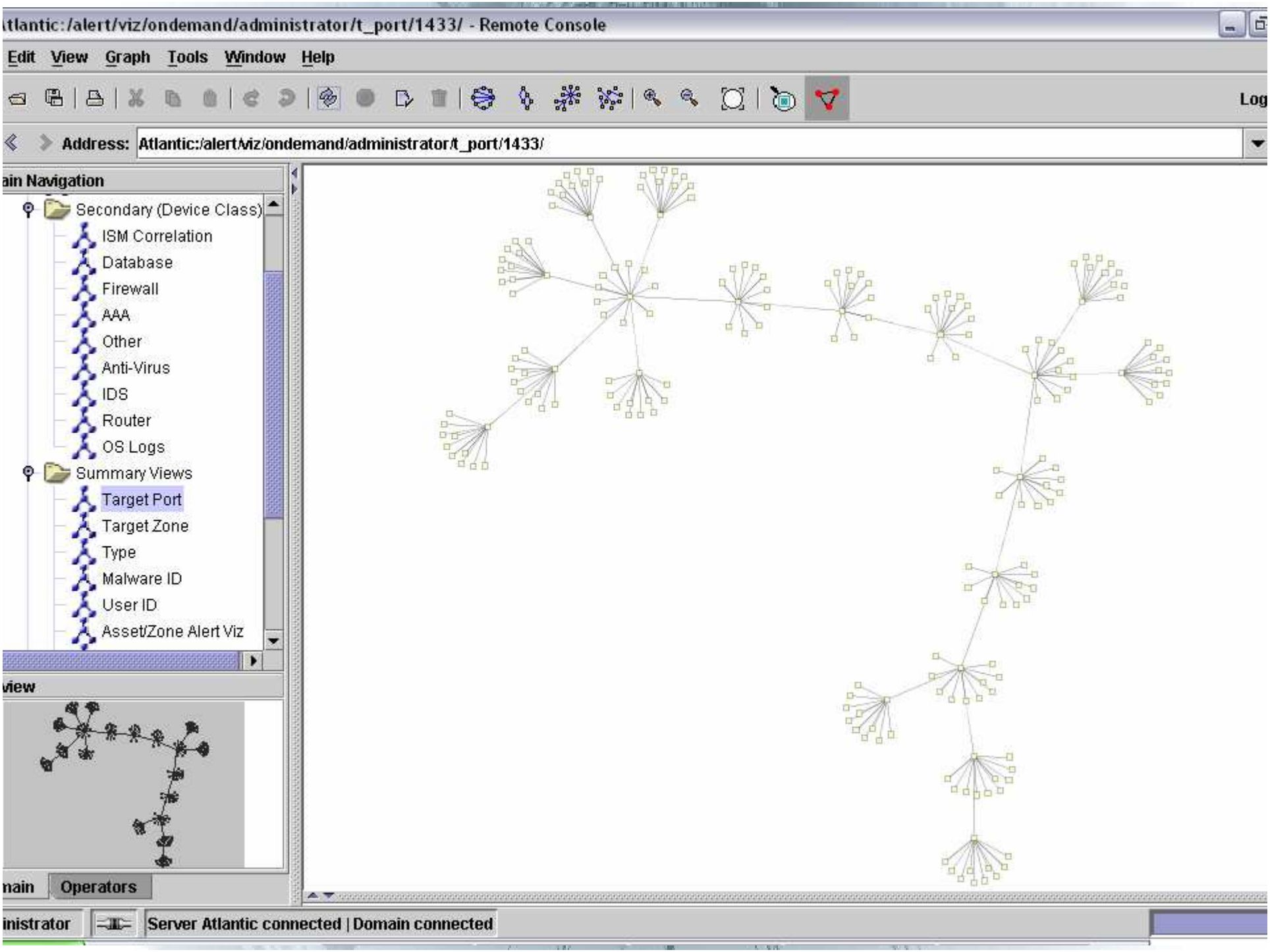
Last Seen	Risk	Source	Target	Type	Events
2005/12/02 15:08:10	885	10.1.4.41	ordersdb	error.web.bug	1
2005/12/02 15:08:12	865	10.1.4.41	ordersdb	ids.detect.exploit.web	1
2005/12/02 15:04:39	825	*multiple*	*multiple*	ism.corr.multiple.worm	1
2005/12/02 15:00:16	700	10.1.2.231	atldc2	auth.os.login.grant (Default Administrator)	1
2005/12/02 15:00:13	700	atlac1552	atldc2	auth.os.login.deny (Disabled Account)	1
2005/12/02 15:00:12	675	atlac1323	dc2	auth.os.access.shun (Important User)	1
2005/12/02 15:04:45	665	10.2.4.95	*multiple*	ism.corr.wormactivity	1
2005/12/02 15:04:37	665	10.1.4.202	*multiple*	ism.corr.wormactivity	1
2005/12/02 15:09:03	525	*multiple*	ordersdb	ism.corr.multiple.ids.signatures	1

Play Stop Play

inistrator | Server Atlantic connected | Domain connected

Some tests

- Now, instead of visualizing all traffic patterns, we can choose to visualize a specific feature, like this worm:
  - If source has fanout and traffic connecting hosts is long and source occasionally connects to random hosts
  - OR:
    - If source possibly infected


tlantic:/alert/viz/ondemand/administrator/t_port/1433/ - Remote Console
Edit View Graph Tools Window Help
Log
Address: Atlantic:/alert/viz/ondemand/administrator/t_port/1433/
ain Navigation
Secondary (Device Class)
ISM Correlation
Database
Firewall
AAA
Other
Anti-Virus
IDS
Router
OS Logs
Summary Views
Target Port
Target Zone
Type
Malware ID
User ID
Asset/Zone Alert Viz
view
main
Operators
inistrator
Server Atlantic connected | Domain connected

Atlantic:/alert/viz/ondemand/administrator/t_port/1433/ - Remote Console

File Edit View Graph Tools Window Help

Log Out

Address: Atlantic:/alert/viz/ondemand/administrator/t_port/1433/

Domain Navigation

- Secondary (Device Class)
  - ISM Correlation
  - Database
  - Firewall
  - AAA
  - Other
  - Anti-Virus
  - IDS
  - Router
  - OS Logs
- Summary Views
  - Target Port
  - Target Zone
  - Type
  - Malware ID
  - User ID
  - Asset/Zone Alert Viz

Overview

Domain Operators

administrator Server Atlantic connected | Domain connected

Atlantic:/alert/viz/ondemand/administrator/t_port/1433/ - Remote Console

File Edit View Graph Tools Window Help

Log Out

Address: Atlantic:/alert/viz/ondemand/administrator/t_port/1433/

Domain Navigation

- Secondary (Device Class)
  - ISM Correlation
  - Database
  - Firewall
  - AAA
  - Other
  - Anti-Virus
  - IDS
  - Router
  - OS Logs
- Summary Views
  - Target Port
  - Target Zone
  - Type
  - Malware ID
  - User ID
  - Asset/Zone Alert Viz

Overview

Domain | Operators

10.2.2.111

10.2.2.148

87.225.142.30

192.254.161.104

216.199.7.196

245.140.28.1

151.73.209.6

233.113.18.225

29.50.147.231

57.130.162.245

131.56.170.62

114.139.154.253

65.227.20.214

30.59.78.151

administrator | Server Atlantic connected | Domain connected

Atlantic:/alert/viz/ondemand/administrator/t_port/1433/ - Remote Console

File Edit View Graph Tools Window Help

Log Out

Address: Atlantic:/alert/viz/ondemand/administrator/t_port/1433/

Domain Navigation

- Secondary (Device Class)
  - ISM Correlation
  - Database

Attribute Properties - ids.detect.exploit.web-10.1.4.41-ordersdb-10.1.4.130-non...

Attributes | Advanced

Event Count	1
Source Host	10.1.4.41
Source Zone	ny.internal.ops.util
Target Zone	ny.internal.finance.orders
Target Host	ordersdb
Target Port	80
Generated By	10.1.4.130
User Name	none
Virus Name	none

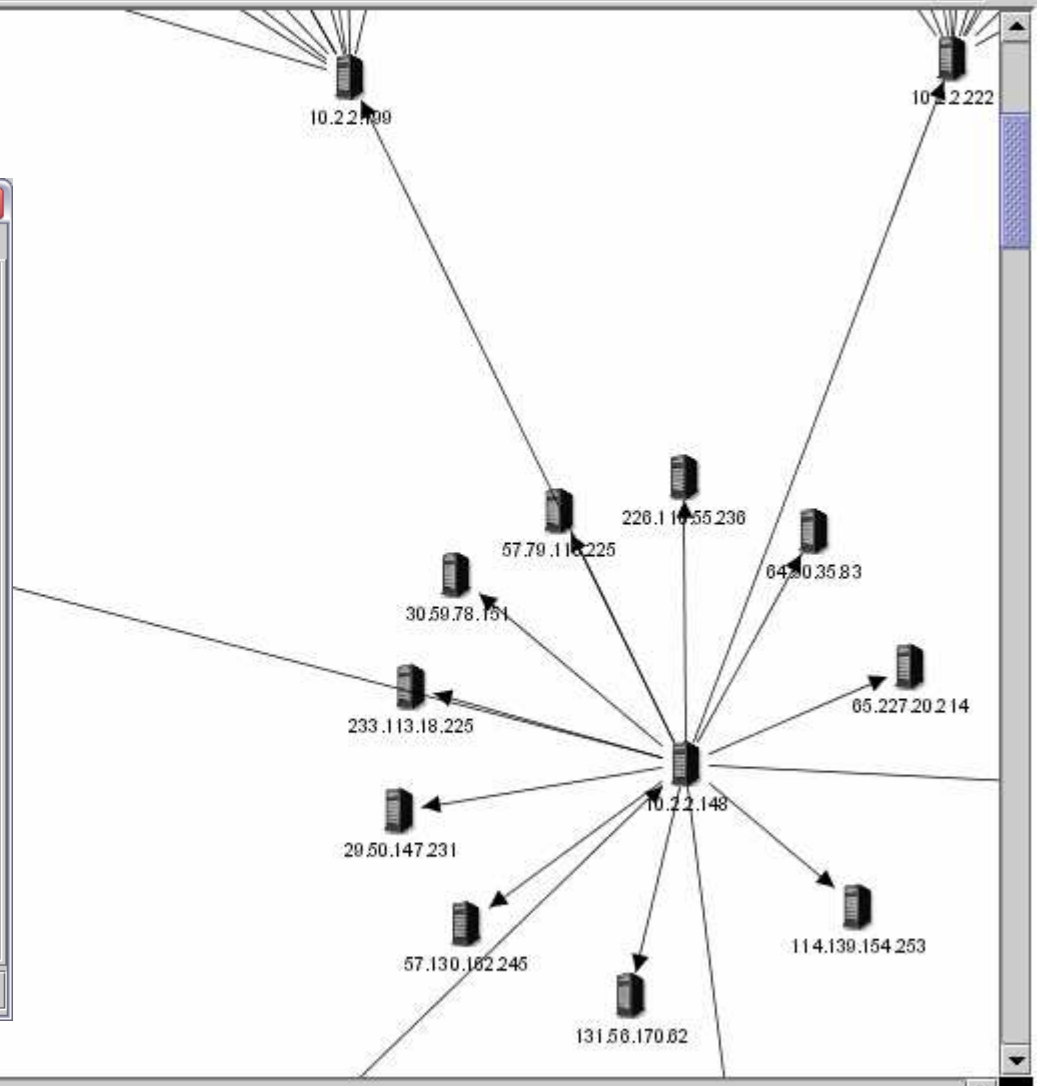
Alert Evidence

Evidence: Dec 02 20:08:12 10.1.4.130 snort: [1:1661:5] WEB-IIS cmd32.exe access [Classification: Web Application Attack] [Priority: 1]: {TCP} 10.1.4.41:50180 -> 10.1.2.20:80 — Enlarge

Risk Information

Risk Checks: Target operational risk = very high; Priority = 55 — Enlarge

Operator Help | OK | Cancel



Overview

Domain | Operators

administrator | Server Atlantic connected | Domain connected

So what’s a baseline then?

- I think it’s just a specification of features, and the ability to compute with information that matches and doesn’t match those features.
  - It’s better than ‘spikes’ and ‘statistical variances on behavior’.
  - The more ‘semantically meaningful’ the feature selections, the better.

Am I there yet?

- 10 years of work, some pretty pictures.
  - I'll sell you prints ☺
- Growing understanding of how to effectively baseline real (crazy) networks
- Found ways to capture experience by defining features as expressions visually
- Explored several visual approaches to representing information for different purposes and audiences

Thank you!
Hope you enjoyed it!

Paul Sop, CISSP, CISM, CISA
Chief Strategy Officer
RedWolf Security

paulsop@redwolfsecurity.com