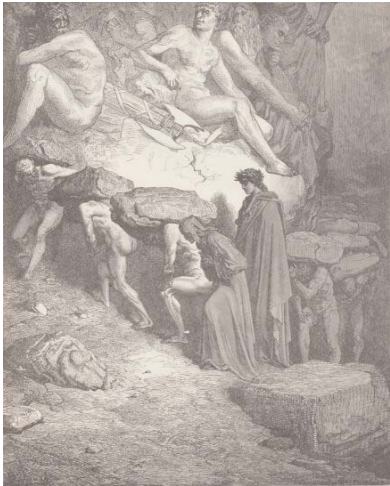


GET THE NETWORK TEAM OUT OF "SECURITY PURGATORY" AND COMPLEMENT YOUR DEFENSE-IN-DEPTH SECURITY STRATEGY WITH THE NETWORK PHYSICS NETSENSORY™ NETWORK APPLICATION MANAGEMENT SOLUTION

# THE SEVEN DEADLY NETWORK SECURITY SINS



PRIDE,  
ENVY,  
WRATH,  
SLOTH,  
AVARICE,  
GLUTTONY,  
LUST...

...the Seven Deadly Sins. To network managers it no doubt seems fitting to match up afflictions like worms and viruses, careless users, spam and the like with an entry from this list of bad habits first compiled by a sixth-century pope.

But there's more to the correspondence than that. Although few people can name them without some prompting, virtually everyone is familiar with the concept of the Seven Deadly Sins, not least because they've been used by artists down the centuries as frameworks for some very famous works, from classics such as Dante's Divine Comedy and Chaucer's Canterbury Tales to, believe it or not, Gilligan's Island, in which each of the seven characters represents one of the sins.

So perhaps it's no surprise that they also serve very well as a framework for discussing network security, its impact on your daily life as a network manager, and how the flow-based Network Physics NetSensory network application management solution can help as part of your defense-in-depth security strategy.

# Pride: Where Are Your Security Blindspots?



So, just as Dante did at the base of the mountain of Purgatory, let's start with pride. In Dante's Purgatory, the expiation for pride requires that one carry a huge rock up a steep slope—a theme he adapted from the Greek myth of Sisyphus, who also saw the rock crash repeatedly back down to where he'd started.

If you're a network manager, this probably looks like just another Monday morning. But it's also probable that a significant part of the rock you're hoisting involves some kind of security problem. The possibilities are legion—rogue usage, malware, sneaky extranet users, illicit data

transfers—and they all eat up time better spent on new initiatives or other more productive work.

But what does this have to do with pride? At first that seems an unlikely attitude to ascribe to the hapless network manager, all too well accustomed to being the focus of a "Beaufort-9 finger-storm" when something goes wrong. But we're so used to the phrase "the Seven Deadly Sins," with pride as the foremost, that it's easy to overlook that they were originally (as in Dante's Purgatory) the "Seven Vicious Habits:" patterns of behavior that, if unchecked, could

get you into serious trouble. And pride was the foundation of all of them, because it blinded you to your other faults. Likewise, a reliance on legacy network management systems, largely device- and probe-based, can blind you to network security problems. It's hard to see the blind spots in the tools you rely on daily.

But blind spots there are in profusion. Since these tools are dependent on device-level data, such as SNMP and RMON, that are not available from third-party networks, there are large parts of the network your business depends on that you can't see. Even for the parts you can see, the intermittent data supplied by traps, not to mention the network burden imposed by polling, restricts you to a limited sample of real-time activity, so you're very likely to miss transient events that signal trouble. And, in any case, device-level data is very hard to relate to application and user context. A link is saturated, but what applications are flowing through it, what users are affected? Is it bandwidth-stealing malware causing the problem, or is it simply time to buy a bigger link? What's going on?

*"As sometimes for support of ceiling or roof, by way of corbel, a figure is seen joining its knees to its breast, which out of its unreality makes a real pang rise in him who sees it, thus fashioned saw I these... they were more or less contracted according as they had more or less upon their backs..."*

## How Big Is Your Rock?

So ask yourself: do I really know the answers to the following questions, and how hard would it be to get them? How big is my rock, and how far will I have to carry it today?

### What's running on my network?

Can I see every application—even those installed by users? What else is there? Worms? Viruses? Spambots? Zombies?

### How much bandwidth am I giving away?

How much am I paying for games and music downloads? Or worse, zombie PCs trying to infect everything else? And how is this affecting business-critical applications?

### Do my firewall settings cover all the bases?

Outgoing as well as incoming? And what about internal traffic—the soft underbelly of my network? What impact do firewall changes have on other applications?

### Who is using my network?

And just what are they using it for? Who's affected by a specific problem; what's its priority?

These are just the questions that the flow-based NetSensory solution can answer. It's not going to make your life heaven, but by making it part of your defense-in-depth security strategy, you can definitely shorten your time in network security purgatory and make that rock a lot lighter.

Briefly, the NetSensory Solution's flow-based technology correlates performance and utilization data from time-stamped TCP/IP packet headers with other data such as BGP and traceroutes to discover and deliver detailed information about every application running on the network. You don't have to know up front what's there—NetSensory will show you. Since it's not dependent on device-level data such as SNMP, NetSensory can do this across any and all of the networks your enterprise depends on: LAN, WAN, MPLS, VPN, Internet, and third-party (e.g.,

customers and partners). NetSensory's ability to display aggregate metrics for business-relevant groups of IP addresses or autonomous systems (business groups) or ports (applications) not only links that information to its business impact (who's affected) for efficient prioritization of troubleshooting, but furnishes drill-downs that help isolate problems to the underlying devices responsible. Finally, the NetSensory solution can supply long-term and real-time information for quite large, complex networks from a single spanning port connection, so installation and maintenance are much easier than with legacy solutions.

So, put that rock down for a while and let's see how the NetSensory solution can help you deal with the Seven Deadly Network Security Sins.



*The Network Physics NetSensory NP-2000 appliance installs at a major data aggregation point in your network. The NP-2000 monitors actual network flows—all your traffic, all the time—through a passive gigabit Ethernet connection to a spanning port or tap. Installation takes less than an hour, and there is virtually no network impact and no interruption of service. An NP-Director global aggregation appliance can deliver a unified view of a very large or complex application infrastructure by combining the data from up to twenty NP-2000's into a NetSensory domain.*

## NETWORK DATA IN CONTEXT

**NetSensory helps network managers understand the business impact of application response problems—critical for prioritization and efficient troubleshooting—by displaying information and alerts in three contexts:**

*The user-experience context*

> How problems are perceived, judged, and reported

*The application context*

> Gives insight into application and server performance, highlights the business functions or processes impacted

*The business context*

> The business entities involved, such as branch offices, departments, buildings, users, customers, partners, server clusters, business applications, and end-to-end business services.

# Envy: Sewing Up Security Holes



“...a wire of iron pierces and sews up the eyelids of all; even as is done to a wild sparrow-hawk, because it stays not quiet.”

In the next level of Dante's Purgatory, we find the envious, those who hate the success of others. Although it's initially difficult to think of a network security problem based on envy, Dante's prescribed punishment makes envy a perfect match for the problem of external users (e.g., partners, customers, road warriors) peeking where they're not supposed to. The envious have their eyes sewn shut, and wear clothing that makes them look like dirt.

You certainly want to sew up any security holes in your network that let extranet users use resources and access data they're not supposed to. But how do you find those holes? Who's using them? Where are they looking? What applications are involved?

That's where flow-based network application management complements systems you already have in place. For instance, your DHCP server can supply the

identity of an IP address that a NetSensory IP conversation drill-down reveals to be abusing a resource, as in the illustration below. More urgently, when your Intrusion Detection System identifies an IP address with suspicious behavior, a flow-based solution can identify everything that address touches and even the bandwidth consumed, as well as other information.

For day-one violations, creating a business group (a range of IP addresses) to identify extranet users makes it easy to see what applications any external user is using and the resources in your network (e.g., bandwidth, servers or desktops) they have used or attempted to use, even if you've never seen that pattern of behavior before—and the data collected can be used to tune the IDS or firewall for even more effective interdiction.

Daily average for all dial-up users

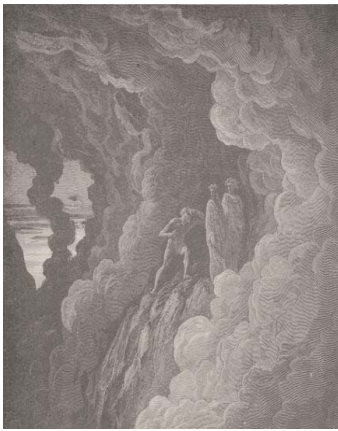
Specific Dialup users and the sites they visited: this particular user dialed into corporate and then spent a lot of time surfing the web.

Group	Throughput (Inbound and Outbound) [kbits/sec]	Application Response Time (TCP Clients) [msec]	Round Trip Time (Inbound) [msec]	Packet Loss (Inbound) [%]
Dialup DHCP	215.635	104.708	236.413	0.579
Applications				
Local Traffic	0.000			
Connected Groups				
Connected IPs				
Member IPs				
10.10.2.51	7.978	305.105	865.708	2.374
81.75.141.32	0.581	590.940	1781.960	0.000
66.35.240.8	0.053	500.822	104.837	0.420
80.170.128.91	0.304	332.034	2172.127	0.000
65.54.174.253	0.038	140.329	54.078	0.000
82.252.23.153	0.036	24.450	1800.086	17.301
82.216.229.168	0.594	13.687	1783.482	0.246
199.181.132.140	0.074	7.645	116.175	0.566
82.165.240.197	0.056	7.575	67.979	0.000
10.20.0.43	0.198	7.526	101.138	0.101
199.181.132.141	0.235	3.560	75.176	0.055
199.181.132.245	0.298	3.510	71.839	0.556
64.164.108.155	0.039	3.112	140.092	0.000
205.161.7.9	0.050	2.541	106.200	0.000
144.160.134.61	0.040	1.673	62.603	0.000
12.120.33.20	2.256	1.079	77.944	0.243
12.120.13.15	0.039	0.902	119.993	8.287
207.69.167.116	0.035	0.697	81.105	0.000
12.120.1.20	1.209	0.682	78.082	0.719
82.48.240.8	0.420		1742.205	0.000
212.194.254.5	0.278		1582.018	12.121

Time Selection: 2005-02-17 07:40 to 2005-02-18 07:40  
Data Source: firebird-Collo

A drill-down to the IP conversation level displays average throughput and performance characteristics for all dialup users, specific users, and each site they visited. Here the metrics Throughput Inbound and Outbound, Application Response Time, Round Trip Time, and Packet Loss have been selected as column headers, sorted by Application Response Time.

# Wrath: Those Cursed Worms and Viruses



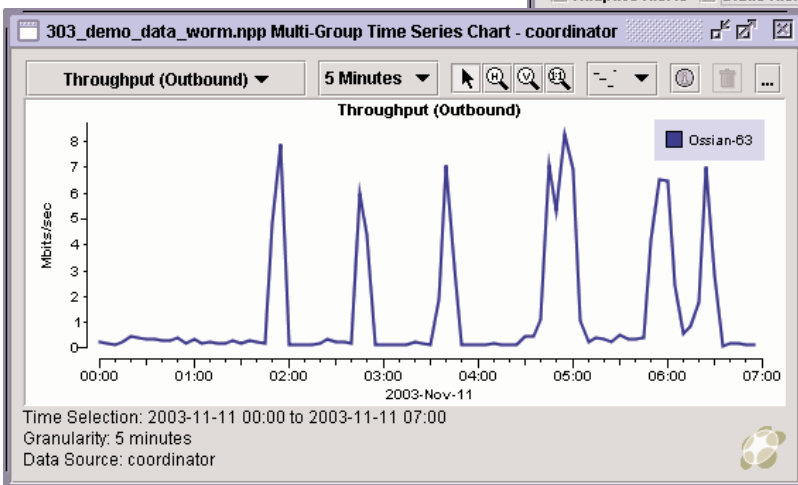
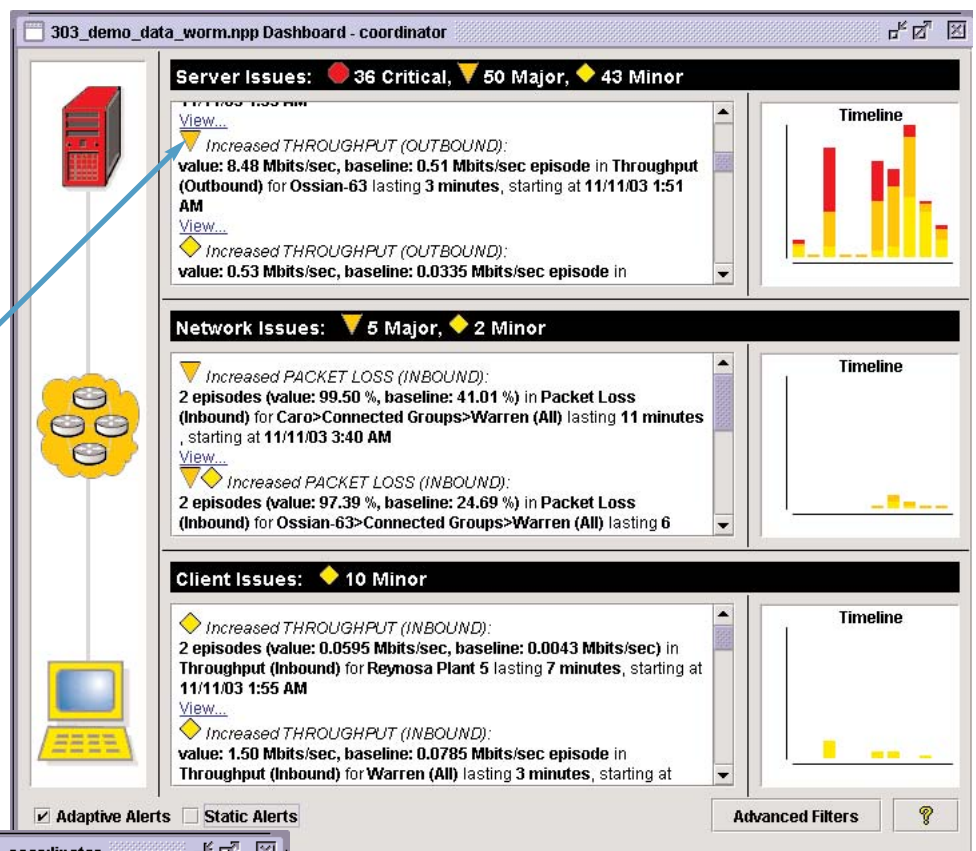
Gloom of hell, or of night deprived of every planet, under a barren sky, obscured by clouds as much as it can be, never made so thick a veil to my sight nor to my feeling so harsh of tissue as that smoke which covered us there...

The wrathful stumble through thick, choking smoke, unable to see. Too good a fate, most network managers will insist, for those who create worms and viruses that spread like wildfire to choke servers and desktops. Every time you turn around it seems there's another worm probing your network; surely a little righteous anger is not out of place!

But worms in particular are easy for a flow-based solution to detect and track, for their common signature is a rise in the number of failed TCP connections as the worm scans random subnets looking for vulnerable systems. Again, business group aggregation is the key to drilling down to specific servers or desktops to identify infected hosts and the other systems they're infecting or trying to infect.

## Case Study: A Blaster Worm Incident

NetSensory Dashboard automatically alerted user to anomalous outbound throughput in Ossian server group.



The NetSensory Problem Management Dashboard uses sophisticated statistical techniques to create Adaptive Alerts without any user programming. The Dashboard determines baseline performance for servers, ISPs, and clients, sets thresholds based on moving averages, and detects violations of these thresholds. Drill-downs from the alerts enable quick diagnosis.

Time series of outbound throughput showed huge spikes in outbound traffic.

A huge increase in failed TCP connections was a result of the worm trying to propagate itself through random subnets.

Easily identified which applications were contributing to the failed connections. Port 135 is one of two well-known ports used to propagate Blaster.

Drilling down to the members of the business group easily showed the two infected hosts trying to spread the worm.

303\_demo\_data\_worm\_ossian.npp Traffic Group Table - coordinator

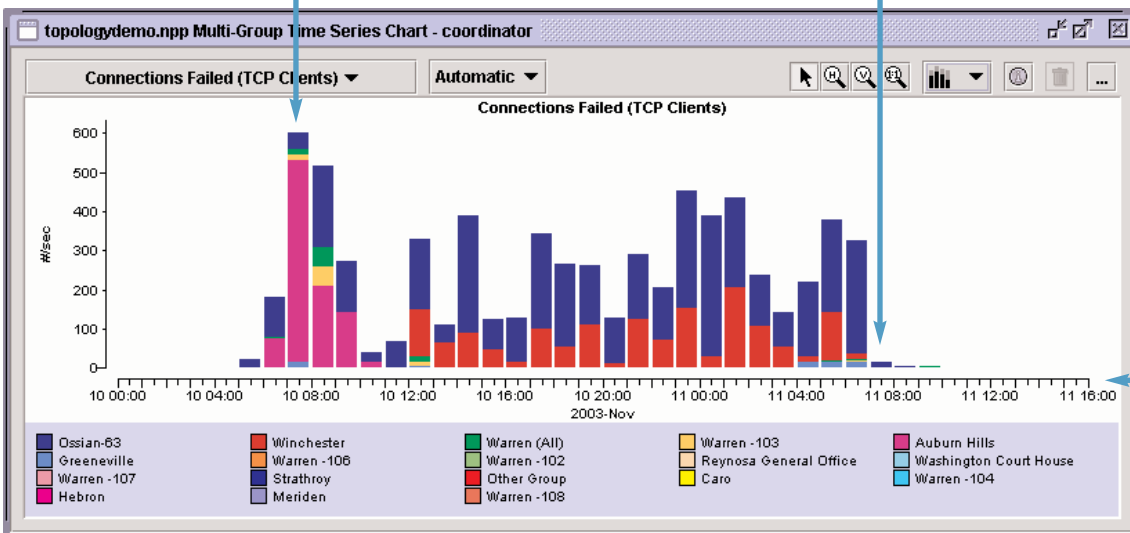
Show Business Group Top 20 By Connections Failed (TCP Clients)

Group	Information	Throug... (Inbound and Outbound)...	Throug... (Outbound) [Mbits/sec]	Connecti... Failed (TCP Clients) [#]	Connect... Failed (TCP Servers) [#]
Ossian-63	10.33.63.0	1.431	1.333	5486535	14433
Local Traffic	Local Traffic	0.000	0.000	0	0
Connected Groups	Connected Groups				
Connected IPs	Connected IPs				
Member IPs	Member IPs				
IP Protocols	IP Protocols				
TCP	TRANSMISSION ...	0.182	0.124	5486535	14433
Applications	Applications				
LOC-SRV	TCP Ports: 135	0.110	0.109	5484289	1494
Connected IPs	Connected IPs				
Member IPs	Member IPs				
10.33.63.127	10.33.63.127	0.063	0.062	3117654	0
10.33.63.66	10.33.63.66	0.047	0.047	2366635	0
10.33.63.251	10.33.63.251	0.000	0.000	0	790
10.33.63.91	10.33.63.91	0.000	0.000	0	380
10.33.63.69	10.33.63.69	0.000	0.000	0	24
HTTP	TCP Ports: 80	0.017	0.002	470	31
NETBIOS-SSN-TCP	TCP Ports: 139	0.018	0.005	389	2915
MICROSOFT-DS	TCP Ports: 445	0.001	0.001	118	926
TELNET	TCP Ports: 23	0.002	0.000	42	0
HTTPS	TCP Ports: 443	0.001	0.001	12	0
MSN-MESSENGER	TCP Ports: 1863	0.000	0.000	3	0
Other Ports	Other Ports				
ICMP	Protocol 1	1.237	1.206	0	0
UDP	USER DATAGRAM...	0.011	0.002	0	0
Winchester	10.30.51.0	0.551	0.499	1970529	22699
Hillsdale	10.30.19.0	0.052	0.020	371812	166310
Greeneville	10.33.20.0	0.078	0.014	142719	40584
Warren (All)	10.30.0.0	2.493	1.801	31824	152187
Warren -103	10.30.103.0	0.200	0.084	9903	205
Warren -1	10.30.1.0	0.003	0.001	6763	65

Time Selection: 2003-11-11 00:00 to 2003-11-11 07:00  
Data Source: coordinator

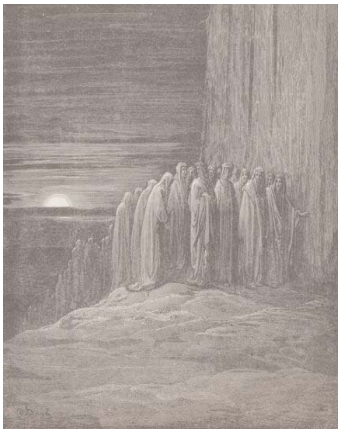
Track the worm as it spreads. Reduce the cost of "fire fighting" by knowing where to attack the worm.

Port blocked at firewall. Attempts to spread worm are no longer visible on the network.



Historical data provides insight into the start and duration of the infection.

# Sloth: Keeping Up with Lazy Users



Soon they were upon us; because, running, all that great crowd was moving on...

The slothful were forced to run continually, and certainly, keeping up with users in an extended enterprise network is a never-ending race, especially when it involves users that it's difficult to keep a lid on, such as road warriors or university students.

Users get lazy, or careless about freeware, and before you know it you've got zombies relaying spam to thousands or millions of unhappy recipients. Better shut them down quick, before you fall into a black hole.

Legacy network management solutions can't help, even though you know where your real SMTP servers are. But with a flow-based solution, they're in one or more business groups, and those are the only ones that should have significant outbound SMTP traffic. It's easy to scan for suspicious SMTP traffic in other, likely groups, then drill down within the group to identify the hosts or users responsible.

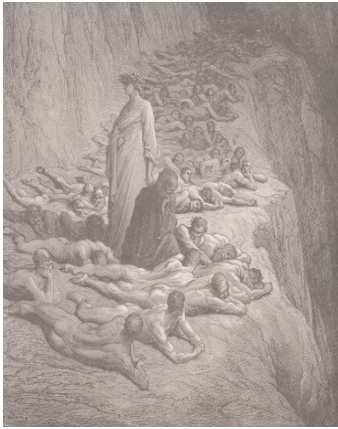
Group	Information	Throughput (Inbound and Outbound) [Mbits/sec]	Throughput (Inbound) [Mbits/sec]	Throughput (Outbound) [Mbits/sec]	Traffic (Inbound) [MB]	Traffic (Outbound) [MB]
☐ TCP	TRANSMISSION CONTROL PROTOCOL	235.287	90.335	144.952	38767.657	62206.707
☐ Applications	Applications					
☐ HTTP	TCP Ports: 80	49.314	32.590	16.724	13986.053	7177.101
☐ SSH	TCP Ports: 22	24.014	7.362	16.652	3159.547	7146.182
☐ MICROSOFT-DS	TCP Ports: 445	19.403	4.464	14.939	1915.615	6411.146
☐ NETBIOS-SSN-TCP	TCP Ports: 139	7.200	1.595	5.605	684.386	2405.312
☐ HTTPS	TCP Ports: 443	3.899	1.334	2.565	572.328	1100.777
☐ GNUTELLA-TCP	TPC Ports: 6346-6347	2.651	0.281	2.369	120.684	1016.873
☐ SMTP	TCP Ports: 25	1.484	1.108	0.376	475.469	161.532
☐ External IPs	External IPs					
☐ Internal IPs	Internal IPs					
☐ 128.196.133.25		0.595	0.578	0.018	247.884	7.626
☐ 128.196.214.11		0.355	0.006	0.349	2.741	149.585
☐ 199.104.148.89		0.121	0.012	0.109	5.220	46.886
☐ 128.196.166.185		0.081	0.002	0.080	0.727	34.151
☐ 128.196.133.142		0.066	0.002	0.063	0.906	27.227
☐ 128.196.210.37		0.064	0.042	0.021	18.121	9.213
☐ 128.196.190.7		0.060	0.057	0.003	24.657	1.098
☐ 128.196.72.37		0.060	0.030	0.030	12.906	12.704
☐ 140.252.1.54		0.054	0.018	0.036	7.890	15.322
☐ 128.196.64.1		0.054	0.034	0.020	14.571	8.406
☐ 150.135.40.100		0.048	0.046	0.003	19.643	1.107
☐ 150.135.218.224		0.043	0.027	0.016	11.585	6.894
☐ 128.196.207.202		0.041	0.016	0.025	6.967	10.553
☐ 128.196.40.5		0.037	0.032	0.005	13.519	2.943
☐ 150.135.220.64		0.033	0.001	0.032	0.452	13.740
☐ 150.135.250.51		0.031	0.030	0.001	12.833	0.471
☐ 128.196.241.5		0.028	0.009	0.020	3.676	8.377
☐ 128.196.109.88		0.025	0.001	0.025	0.322	10.613
☐ 128.196.37.178		0.024	0.001	0.024	0.225	10.282
☐ 150.135.156.2		0.024	0.000	0.024	0.174	10.329
☐ POP3	TCP Ports: 110	0.514	0.044	0.471	18.750	201.962
☐ IMSP	TCP Ports: 554, 8554	0.495	0.438	0.057	187.914	24.481
☐ IMAP	TCP Ports: 143	0.372	0.053	0.319	22.614	137.090
☐ TELNET	TCP Ports: 23	0.354	0.092	0.262	39.562	112.514
☐ YAHOO-MESSENGER-TCP	TCP Ports: 5000-5001,5050,5100	0.092	0.071	0.020	30.642	8.688
☐ AIM-TCP	TCP Ports: 5190	0.041	0.033	0.008	14.080	3.622
☐ FTP	TCP Ports: 20-21	0.036	0.017	0.019	7.162	8.229
☐ MSN-MESSENGER	TCP Ports: 1863	0.017	0.009	0.008	3.766	3.573
☐ LOC-SRV	TCP Ports: 135	0.017	0.008	0.008	3.903	3.306
☐ H323	TCP Ports: 1720	0.000	0.000	0.000	0.027	0.001
☐ NETBIOS-NS-TCP	TCP Ports: 137	0.000	0.000	0.000	0.021	0.000
☐ Other Ports	Other Ports					
☐ UDP	USER DATAGRAM PROTOCOL	3.924	2.678	1.246	1149.242	534.879
☐ Other IP Protocols	Other IP Protocols	2.011	1.213	0.798	520.369	342.674
☐ ICMP	Protocol 1	0.094	0.050	0.044	21.312	19.037

The information field displays IP address, name, or other information about drill-downs

Time Selection: 2004-10-08 14:18 to 2004-10-08 15:18  
Data Source: np2000

A protocol drilldown can reveal the internal or external users of any application and how much bandwidth they are consuming.

# Avarice: Dealing with Intellectual Property Theft



*When I was come forth on the fifth round, I saw people upon it who were weeping, lying upon the earth all turned downward.*

The greedy were forced to lie face down on the ground, a position in which one cannot see anything one might desire. Greed is a prime motivation for theft, and on the network this can often mean theft of intellectual property: from illicit downloading of copyrighted material to the more serious insider crime of illicit data transfer.

We'll see in a later section how the application involved, such as FTP or streaming media, can easily be detected; here we see how easy it is to identify possible greed on

your network through an IP drilldown in a NetSensory table.

The table below reveals the IP addresses, internal and external, that are using an FTP server. The anomalously high traffic for the internal address at the top of the drill-down might be cause for concern. An IP-IP drilldown could reveal what other destinations this user was accessing at the time; a check with the DHCP server logs for that time period would identify the user;

Top IP's connected to server based on average daily throughput

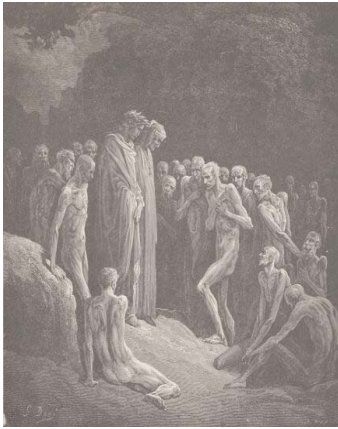
Average daily inbound and outbound throughput for FTP server and top connected IP addresses

Total megabytes transferred for FTP server and top connected IP addresses

Group	Throughput (Inbound and Outbound) [kbits/sec]	Traffic (Inbound) [MB]
FTP Server	421.371	3139.762
Local Traffic	0.093	0.479
Applications		
Connected Groups		
Connected IPs		
10.20.0.15	139.716	1404.945
65.75.179.10	8.950	89.424
64.171.5.43	5.993	8.653
67.169.18.142	5.815	7.627
69.35.41.10	5.124	14.217
24.5.7.146	4.659	10.809
68.229.95.66	4.462	11.898
10.20.0.1	4.301	44.276
205.158.104.130	4.269	43.941
68.215.224.28	4.067	8.102
199.184.165.136	3.781	37.968
160.36.178.159	3.721	37.473
65.66.246.185	3.719	22.486
24.238.66.121	3.510	12.019
83.115.172.26	3.219	21.467
82.189.39.250	2.893	6.412
63.146.199.38	2.324	19.903
141.154.79.117	2.293	4.196
12.120.33.20	2.257	22.731
64.125.133.201	1.880	18.918

Time Selection: 2005-02-17 07:40 to 2005-02-18 07:40  
Data Source: firebird-Collo

# Gluttony: Users and Applications That Eat Up Links

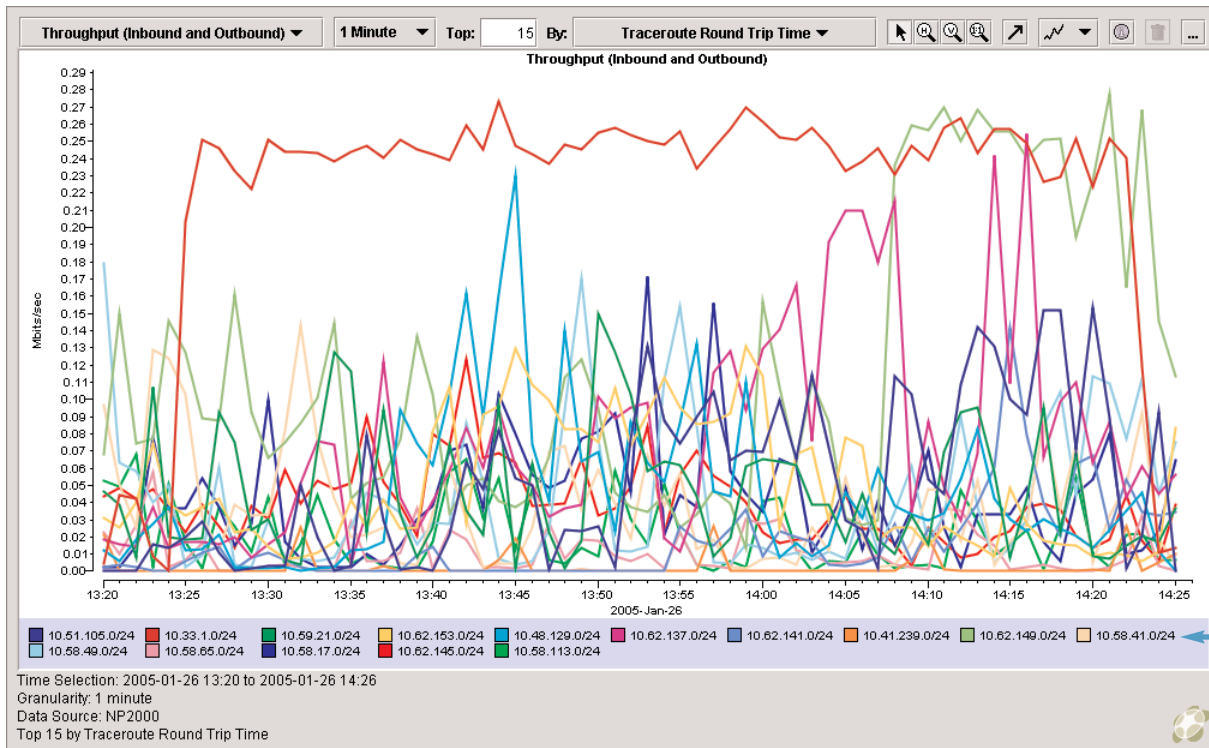


*Each was dark and hollow in the eyes, pallid in the face, and so wasted that the skin took its shape from the bones... The sockets of their eyes seemed rings without gems... Who would believe that the scent of an apple, begetting longing, and that of water, could have such mastery...*

Gluttony is the opposite of temperance. Some people, and too many applications, are never satisfied. They grab intemperately for bandwidth, sometimes all at once, as is frequently the case with streaming media. All too often the result is a saturated link as the application takes over the pipe. And even if it leaves some for your business apps, it's chewing up bandwidth that your enterprise pays good money for, and probably slowing down those critical application.

But before you can put the users responsible on the network equivalent of a starvation diet, the fate of the gluttonous in Dante's Purgatory, you have to find them. Fortunately, the sudden ("zero slope") traffic surge caused by many such applications, and the link saturation that results, are easy to spot.

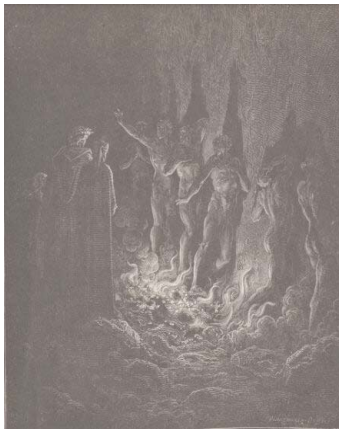
Below, a graph of the total inbound and outbound throughput of the twenty remote offices (represented by /24 IP prefixes) with the highest Traceroute Round Trip Time (which soars on a saturated link), reveals two offices with "zero-slope" applications that are saturating their link.



On this customer site, remote offices are assigned their own /24 IP prefixes

Two remote offices (15.33.1.0/24 & 10.62.142.0/24) are saturating their link to the main data center. Since their Internet connectivity is supplied through the main data center, this could either be streaming media or similar rogue applications, or an indication that more bandwidth is needed for critical applications. A protocol drill-down from the problem offices will quickly reveal which is the case.

# Lust: Rogue Applications That Burn Up Bandwidth



...turning to the right hand, we were intent upon another care. Here the bank shoots forth flame, and the ledge breathes a blast upward which drives it back, and sequesters a path from it.

In Dante's schema, lust is the opposite of prudence, and the lustful are consigned to the flames, which is pretty much the reaction of a network manager to imprudent users who install rogue applications that burn up bandwidth and reduce critical applications to a crawl.

These applications may not grab for bandwidth all at once, but the CIO still isn't going to want to pay for supplying Internet radio or P2P access to business users. Who knows, shut those rogues down and you may find you can wait a lot longer than you thought to buy more bandwidth!

That's easily done with a flow-based solution. Using business groups and applications it's easy to display all the applications being used on your network, identify the groups where illicit traffic exists, and then drill down to the offending hosts or users.

**A protocol drill-down from internal IP addresses quickly reveals illicit usage.**

Real Networks		Real Networks	1.544
External IPs	External IPs		
Internal IPs	Internal IPs		
10.130.198.244	10.130.198.244		0.249
64.157.128.162	loa-lvl3-ny22.rbn.com		0.249
10.130.69.46	10.130.69.46		0.131
10.130.152.173	10.130.152.173		0.122
209.247.111.152	loa-lvl3-tex13.rbn.com		0.110
64.156.70.80	unknown.Level3.net		0.010
64.156.70.91	unknown.Level3.net		0.002
217.163.2.201	217.163.2.201		0.000
10.130.89.74	10.130.89.74		0.051
205.188.216.25	od-dtc3s-0.stream.aol.com		0.026
64.12.56.161	demand3VIP1.stream.aol.com		0.025

## Standard web use

- > http
- > email
- > ftp

## Peer-to-peer (P2P) apps

- > Fasttrack-based applications (KazaA, Grokster, Morpheus)
- > Gnutella

## Potential virus or security issues

Group	Information	Total Outbound Throughput (Mbits/sec)	Total Inbound Throughput (Mbits/sec)
Total Traffic	Total Traffic	3.564	11.958
TCP	TCP	3.430	11.812
Port 80	HTTP	0.723	5.572
Port 1755	WINDOWS MEDIA PLAYER	0.024	0.686
Port 554	REAL NETWORKS	0.026	0.491
Port 20	FTP-DATA	0.105	0.424
Port 25	SMTTP	0.293	0.373
Port 139	NETBIOS-SSN	0.187	0.342
Port 443	HTTPS-MAIN	0.085	0.245
Port 445	MICROSOFT-DS	0.030	0.119
Port 1214	FASTTRACK P2P	0.274	0.085
Port 6346	GNUTELLA	0.071	0.079
Port 102	UNCLASSIFIED	0.089	0.073
Port 389	LDAP	0.032	0.029
Port 1521	NCUBE LICENSE MANAGER	0.066	0.017
Port 2234	OPEN FLASH POINT GAMES	0.074	0.017
Port 94	TIVOLI	0.031	0.016
Port 1092	UNCLASSIFIED	0.027	0.009
Port 1096	UNCLASSIFIED	0.021	0.007
Port 53	UNCLASSIFIED	0.028	0.006
Port 1086	UNCLASSIFIED	0.025	0.006
Port 2007	UNCLASSIFIED	0.030	0.001
UDP	UDP	0.125	0.142
Port 53	DNS	0.011	0.017
Port 88	KERBEROS	0.018	0.011
Port 138	NETBIOS-DCM	0.025	0.011
Port 5190	AIM	0.001	0.003
Port 49162	UNCLASSIFIED	0.002	0.002
Port 27960	GAMING - QUAKE III	0.001	0.002
Port 49180	UNCLASSIFIED	0.002	0.002
Port 49186	UNCLASSIFIED	0.002	0.002
Port 12203	GAMING - MEDAL OF HONOR	0.001	0.002
Port 5000	COMPLEX-MAIN	0.002	0.002
Port 137	NETBIOS-NS	0.003	0.002
Port 49204	UNCLASSIFIED	0.001	0.001
Port 123	NTP	0.001	0.001
Port 49178	UNCLASSIFIED	0.001	0.001
Port 2967	UNCLASSIFIED	0.001	0.001
Port 1031	TROJAN - XANADU	0.003	239.6E-6
Port 1434	SQL NAME SERVERS (WOR...	0.016	167.5E-6
Port 1029	UNCLASSIFIED	0.001	88.81E-6
Port 1298	UNCLASSIFIED	0.001	3.828E-6
Port 47806	UNCLASSIFIED	0.001	960E-12
Other Protocols	Other Protocols	0.008	0.004

## Streaming services

- > Real
- > Windows Media Player

## Gaming applications

- > Operation Flashpoint
- > Quake III
- > Medal of Honor

## Summary

The NetSensory solution offers network managers a way out of "security purgatory" by enabling them to quickly discover and isolate a wide variety of security violations on the network. Complementary to existing security solutions, such as Intrusion Detection Systems, NetSensory can be an important part of an enterprise's defense-in-depth security strategy.