Presented at Central Plains ISSA Meeting – October 7, 2005

Lancope StealthWatch Technology

Security Through Network Intelligence

www.lancope.com

STEALTH WATCH Xe

Lancope

- # Network Behavior Anomaly Detection Solution

- A Network Behavior Anomaly Detection (NBAD) solution is a fast, accurate and cost-effective solution that immediately detects malicious or unauthorized network activity, including new and otherwise unidentifiable threats. As a network-based system, NBAD solution overcomes the cost and complexity of deploying and maintaining signature- or host-based systems. With NBAD solutions, organizations can now identify and resolve network exposures, such as new, misconfigured or unauthorized devices and applications. These threats, which include rogue servers and P2P file sharing applications, result in 65% of network risks, according to a Gartner estimate. When unpreventable network events or host infections occur, NBAD solutions detects and contains the incident while delivering critical insight that accelerates resolution and minimizes damage.

Presented at Central Plains ISSA Meeting – October 7, 2005

What can NBAD’s do for you?

- Significantly improve the prevention and resolution of network security incidents
- Stop worms, viruses, trojans, and DoS attacks that other technologies miss
- Assess policy compliance and the impact of planned or unanticipated network events
- Identify and prioritize critical threats to resolve risks and events before they become crises
- Real-time, continuous monitoring of network traffic patterns for immediate response to unexpected or unforeseeable security events
- Host and network protection without requiring host agents or frequent attack signature database updates
- Flexible design that improves the performance of existing security investment and easily extends overall security strategy to new business opportunities
- Simple, straight-forward scalability across massive command-and-control enterprise deployments
- Cost-effective, easy-to-manage monitoring of large numbers of devices via powerful, graphical representations of current and expected network behavior

How to protect your environment from Internal attacks?

- Organizations should establish a trusted behavior baseline for each machine on the network.
- Look for changes in current foot print behavior.
- If these procedures are implemented effectively they can detect and protect systems against new malicious code and worms.
- Detect, mitigate and resolve internal and external threats, such as stealthy scans, new worms and Trojans that bypass firewalls and signature-based antivirus systems
- Continuous monitoring of enterprise network activity without installing host-based agents
- Immediate alerts based on policy violations, such as attempted access to servers from an unauthorized network zone
- Automate discovery and profiling of new or unauthorized network devices

Presented at Central Plains ISSA Meeting – October 7, 2005

Presented at Central Plains ISSA Meeting – October 7, 2005

How do internal security threats effect your network?

Internal security refers to a focused effort to secure resources on internal attacks, or LANs. These resources can include applications, data, servers, and end point devices. Internal attacks can happen either maliciously or inadvertently. But regardless of what prompts an internal security breach, one thing is for certain: The impact of internal security issues causes negative results on an organization from both a technical and business perspective.

How Enterprises Will Begin To Focus On Internal Attacks?

Companies of all sizes are beginning to shift their attention to the topic of internal security. They are starting to initiate change in how they protect resources on the LAN, and in turn, protect their employees' productivity. Once an organization is convinced they should invest time, money and resource on internal security their first step focuses on adding an extra layer of defense within their networks, including:

-Securing Endpoint Devices
-Implementing an additional layer of protection (Worm Defense)
-Enforcement of proper use through well articulated security policy
-Quarantine capabilities for isolating infected devices
-Segmenting LANs for threat containment
-Remediation Assistance

Presented at Central Plains ISSA Meeting – October 7, 2005

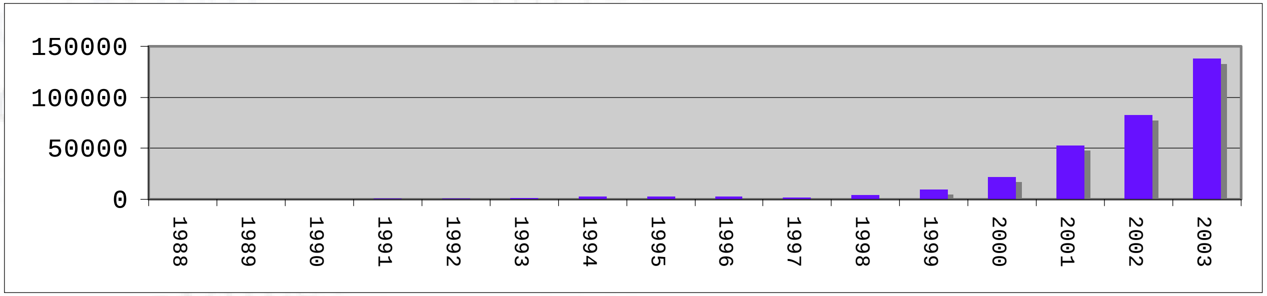
What are you doing about securing your business / network?

- **Do you have tools in place to identify internal threats?**
- **Do you have the ability to find the root cause of these security threats?**
- **Do you have historical logging of my security threats and flows?**
- **How do these solutions integrate with my current security tools?**
- **How much do they cost and how do I get back my investment?**

Lancope

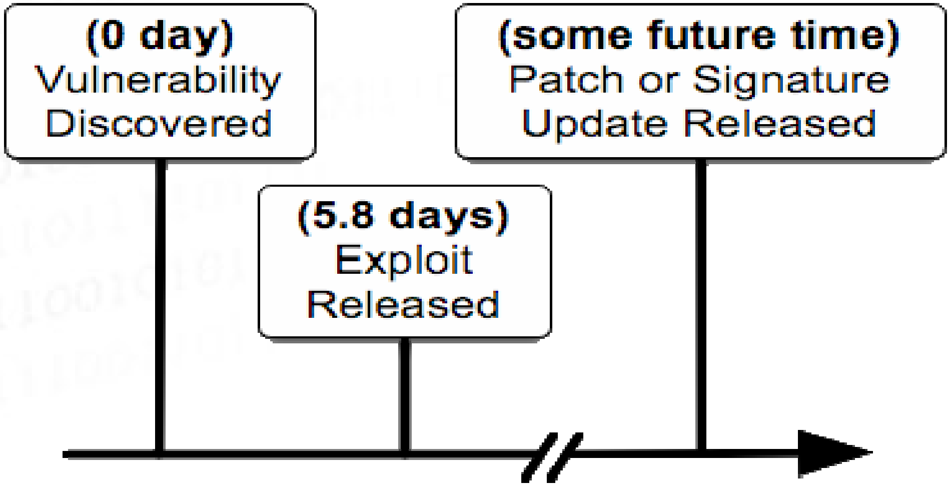
Presented at Central Plains ISSA Meeting – October 7, 2005

> “Given the widespread use of automated attack tools, attacks against Internet-connected systems have become so commonplace that counts of the number of incidents reported provide little information with regard to assessing the scope and impact of attacks. Therefore, as of 2004, we will no longer publish the number of incidents reported.”
>
> - CERT



Attack frequency increases…

…while discovery-to-exploit window decreases.



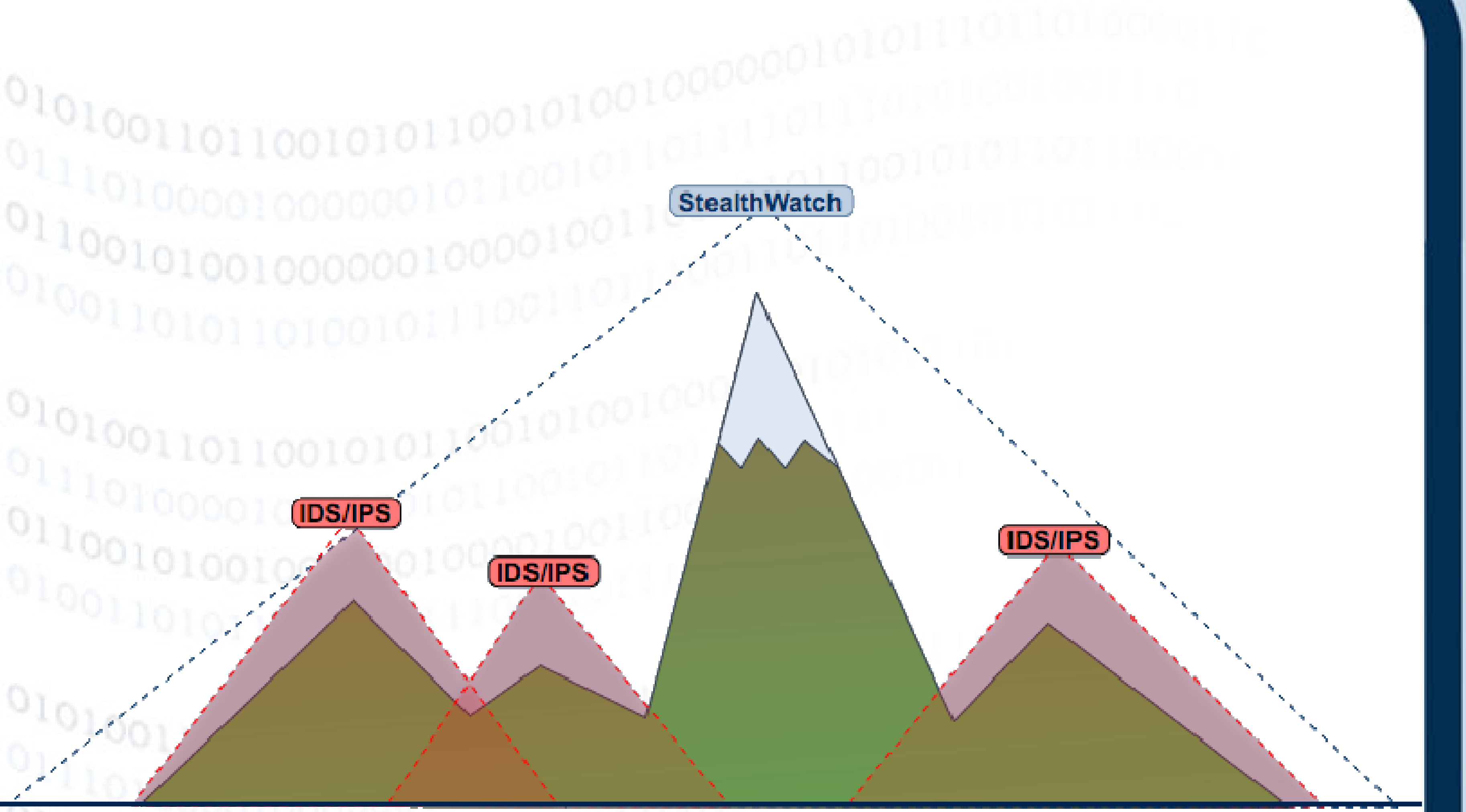
(0 day)
Vulnerability
Discovered

(5.8 days)
Exploit
Released

(some future time)
Patch or Signature
Update Released

Signatures Can’t Keep Up

Presented at Central Plains ISSA Meeting – October 7, 2005

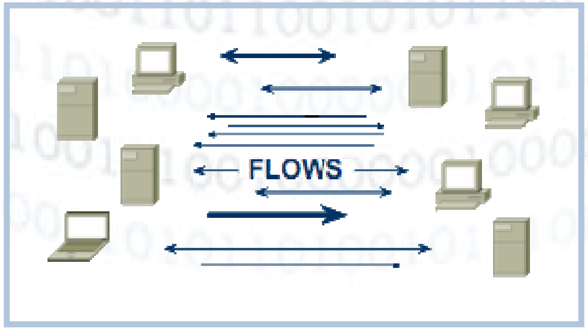


“Flows” provide total visibility across a wide network range by collecting data from routers in varying locations. This gives Stealth Watch total supervision over the network and provides an ability to track behavior throughout the network, from start to end.

NetFlow provides “Mountaintop visibility”

Lancope

Analyze Flows…



Establish baseline…

Number of concurrent flows

Packets per sec

Bits per second

New flows created

Number of SYNs sent

Time of day

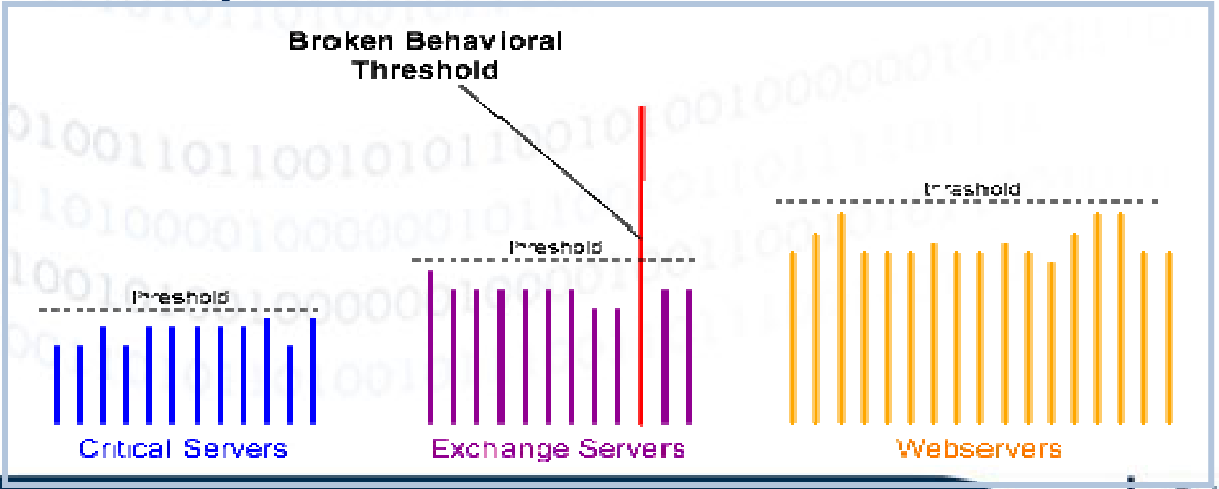
Number of SYNs received

Rate of connection resets

Duration of the flow

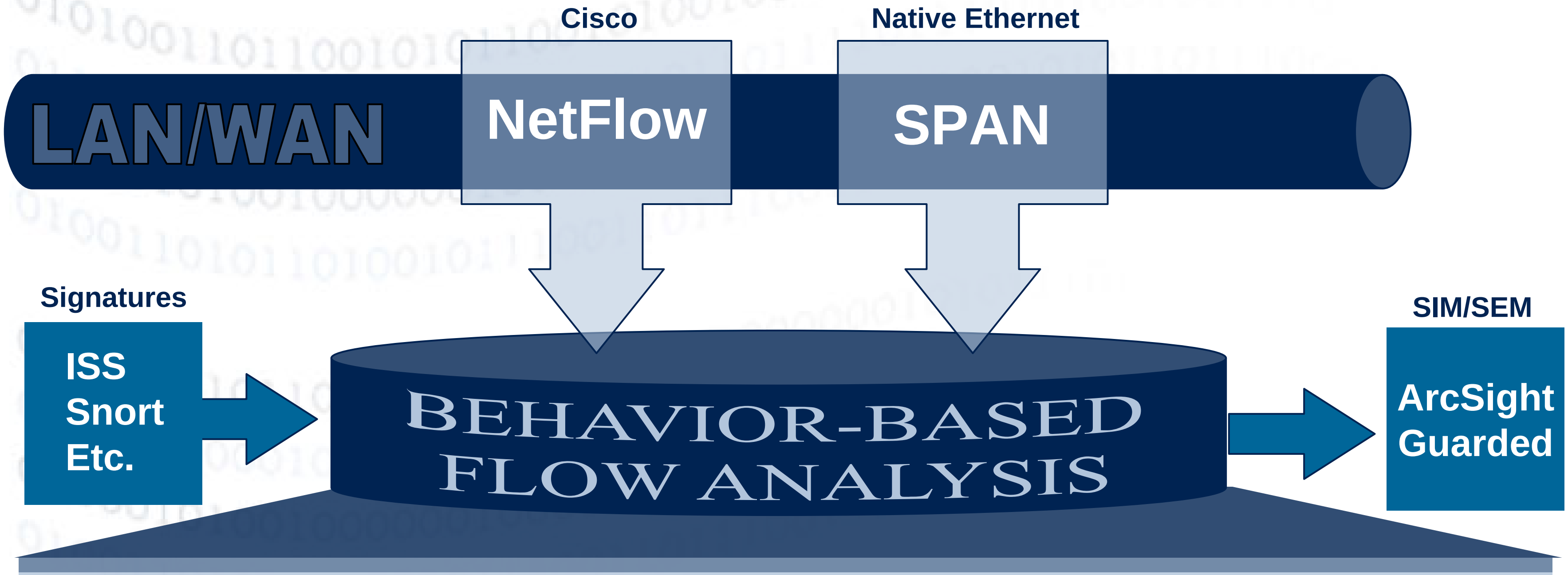
<Many others>

Alarm on changes in behavior…



BEHAVIOR RATHER THAN SIGNATURES

STEALTHWATCH: BEHAVIOR-BASED FLOW ANALYSIS



Cisco

Native Ethernet

LAN/WAN

NetFlow

SPAN

Signatures

ISS
Snort
Etc.

BEHAVIOR-BASED FLOW ANALYSIS

SIM/SEM

ArcSight
Guarded

Powerful audit, compliance reporting, and forensic capabilities

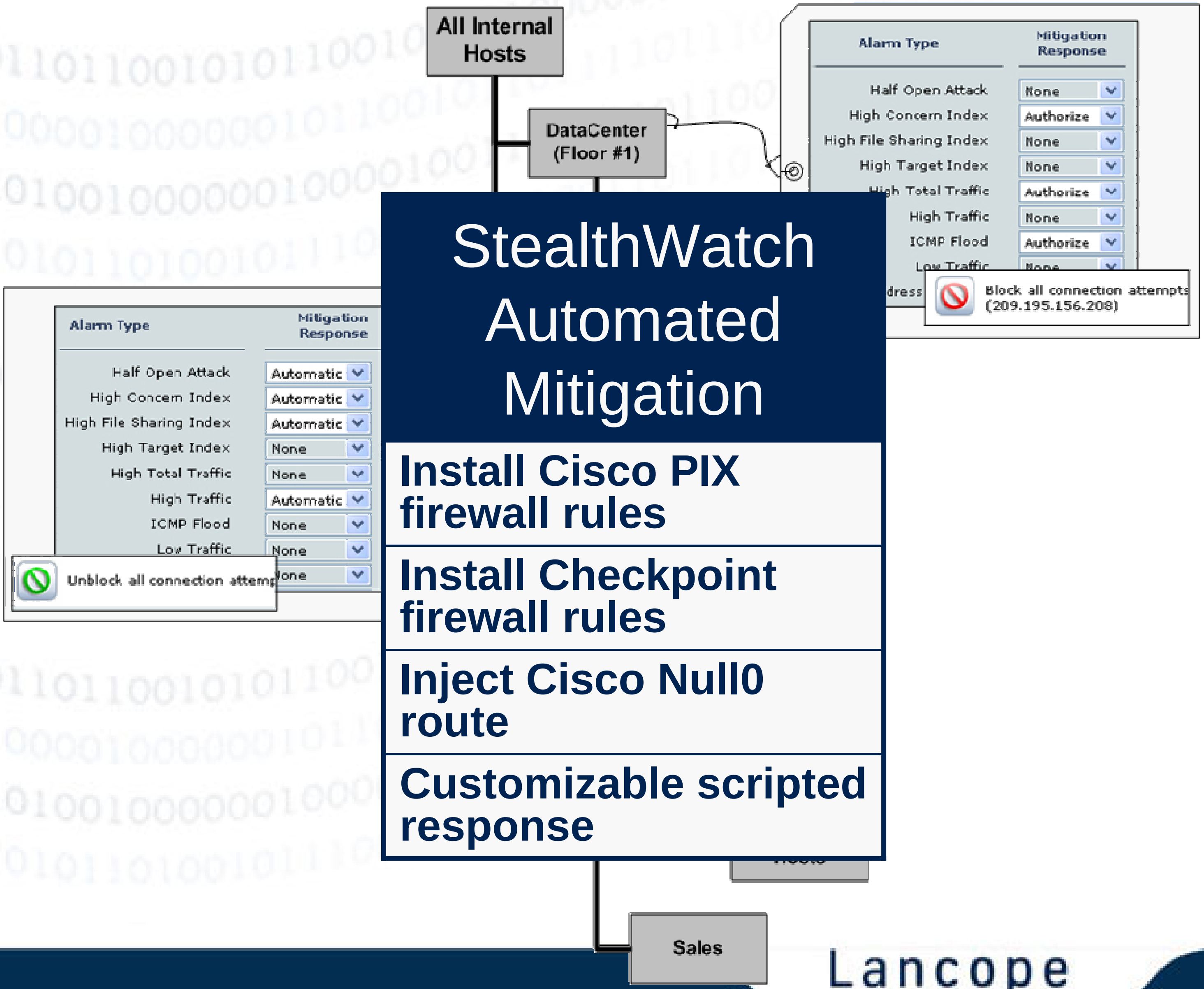
Streamline and shorten resolution time

Provides visibility into “most significant” network behaviors

Cost-effective, extended enterprise-wide protection and control

Presented at Central Plains ISSA Meeting – October 7, 2005

Lancope



Alarm Type	Mitigation Response
Half Open Attack	Automatic
High Concern Index	Automatic
High File Sharing Index	Automatic
High Target Index	None
High Total Traffic	None
High Traffic	Automatic
ICMP Flood	None
Low Traffic	None
	one

Unblock all connection attemp

Alarm Type	Mitigation Response
Half Open Attack	None
High Concern Index	Authorize
High File Sharing Index	None
High Target Index	None
High Total Traffic	Authorize
High Traffic	None
ICMP Flood	Authorize
Low Traffic	None

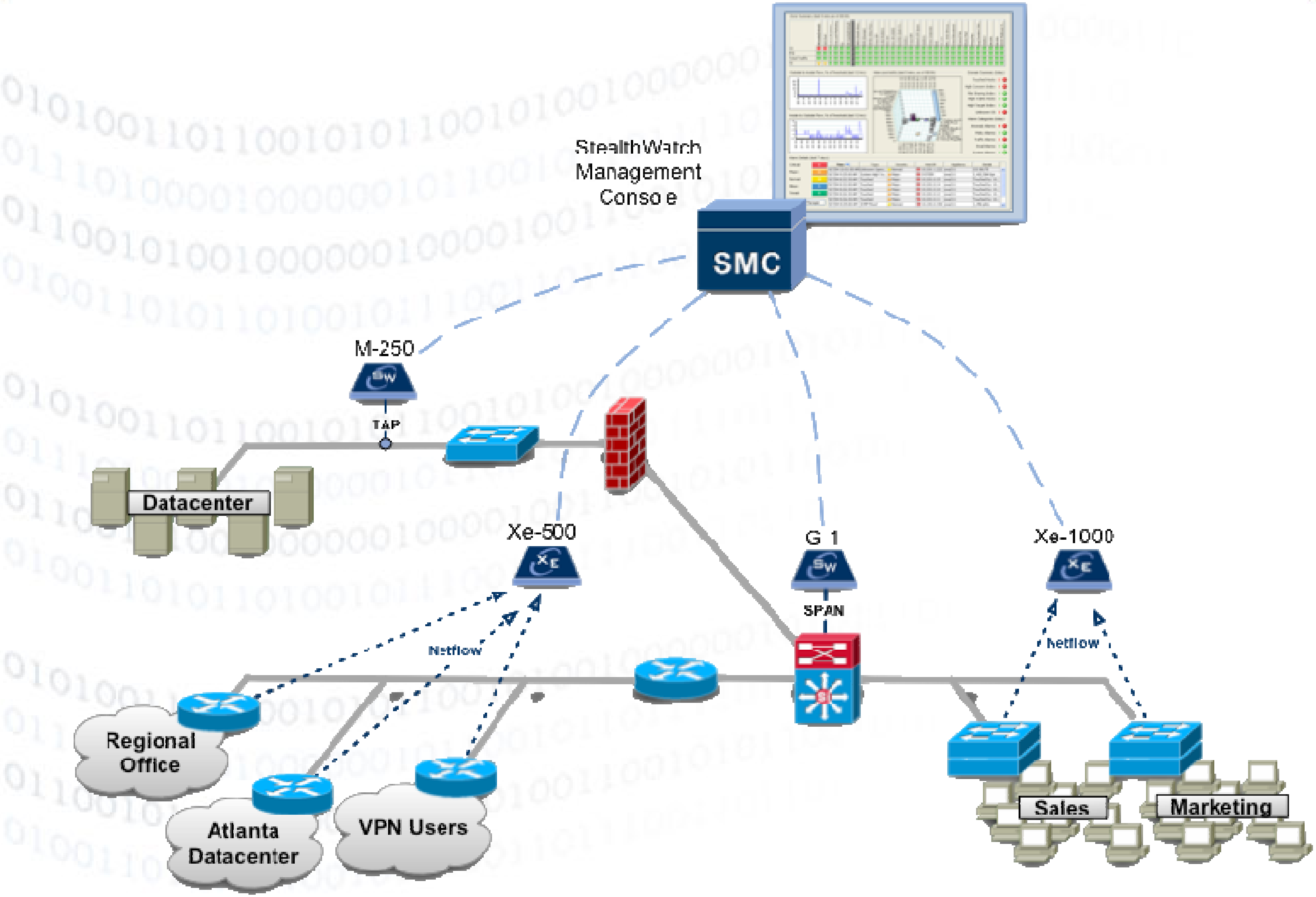
dress

Block all connection attempts (209.195.156.208)

StealthWatch Automated Mitigation

- **Install Cisco PIX firewall rules**
- **Install Checkpoint firewall rules**
- **Inject Cisco Null0 route**
- **Customizable scripted response**

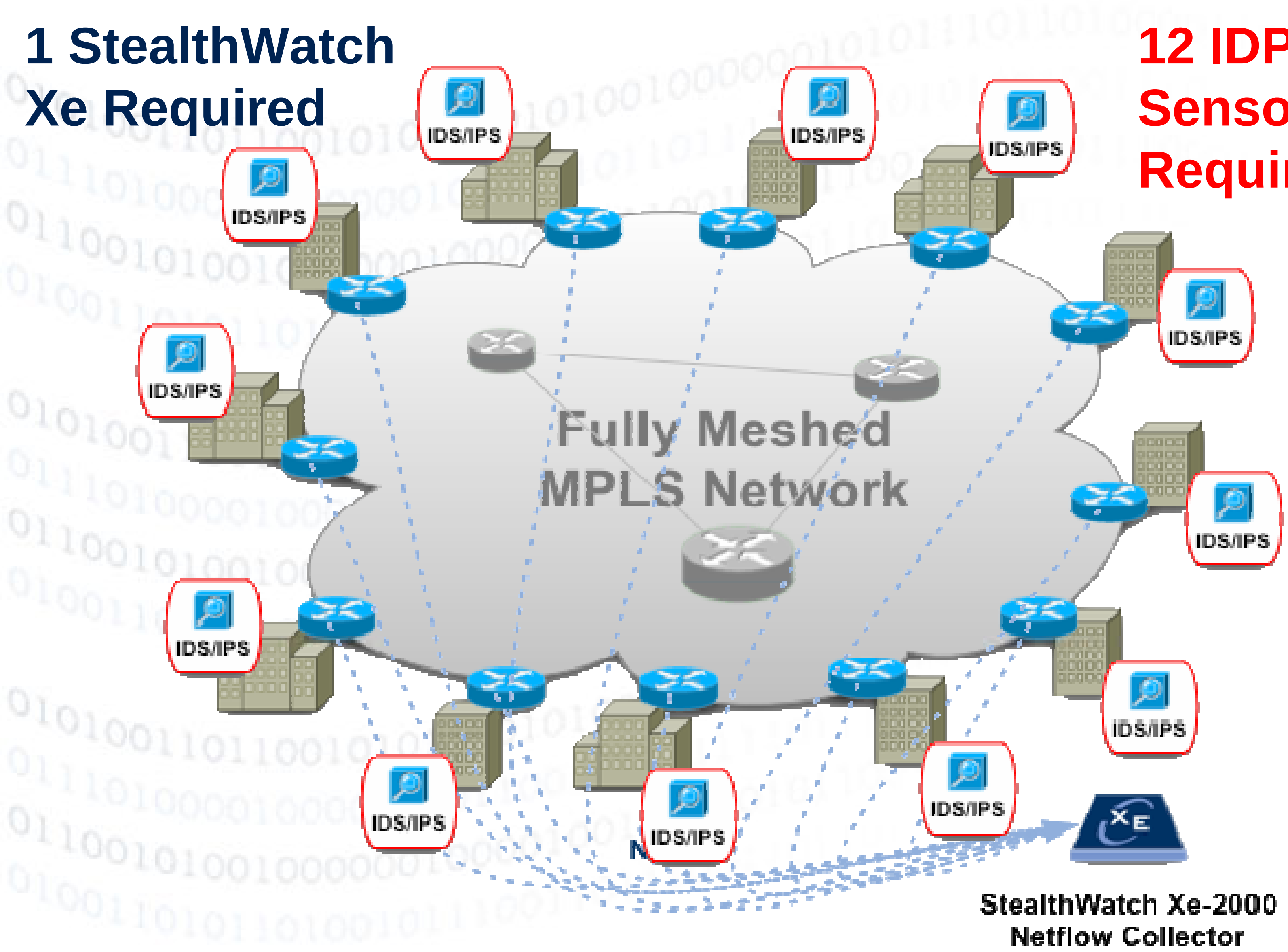
Presented at Central Plains ISSA Meeting – October 7, 2005



Deployment: How do we collect flows?

1 StealthWatch Xe Required

12 IDP/IPS Sensors Required



Presented at Central Plains ISSA Meeting – October 7, 2005

StealthWatch Xe: Monitor Remote Locations

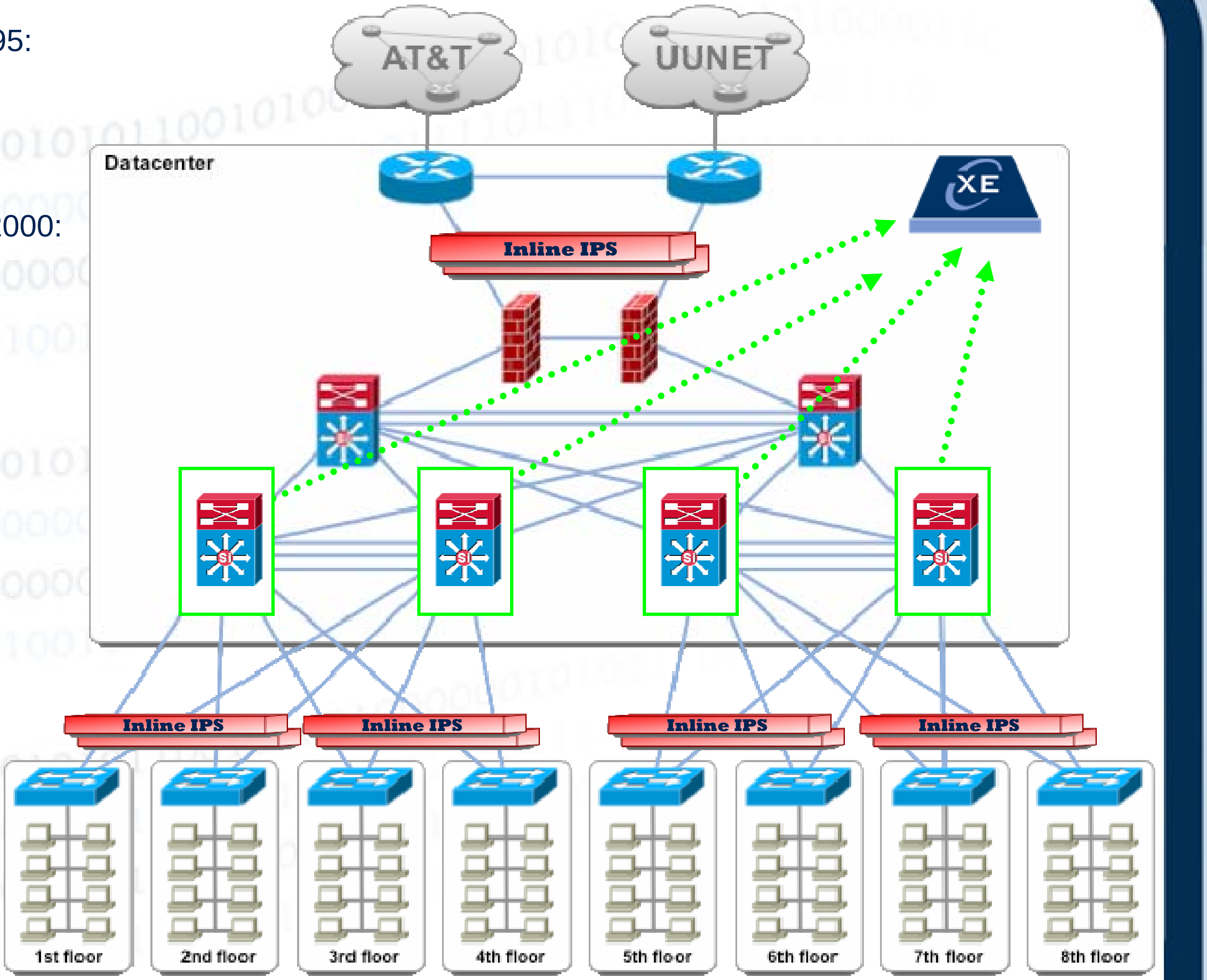
Lancope

8 Inline IPS @ $64,995:

$519,960

1 Netflow-based Xe-2000:

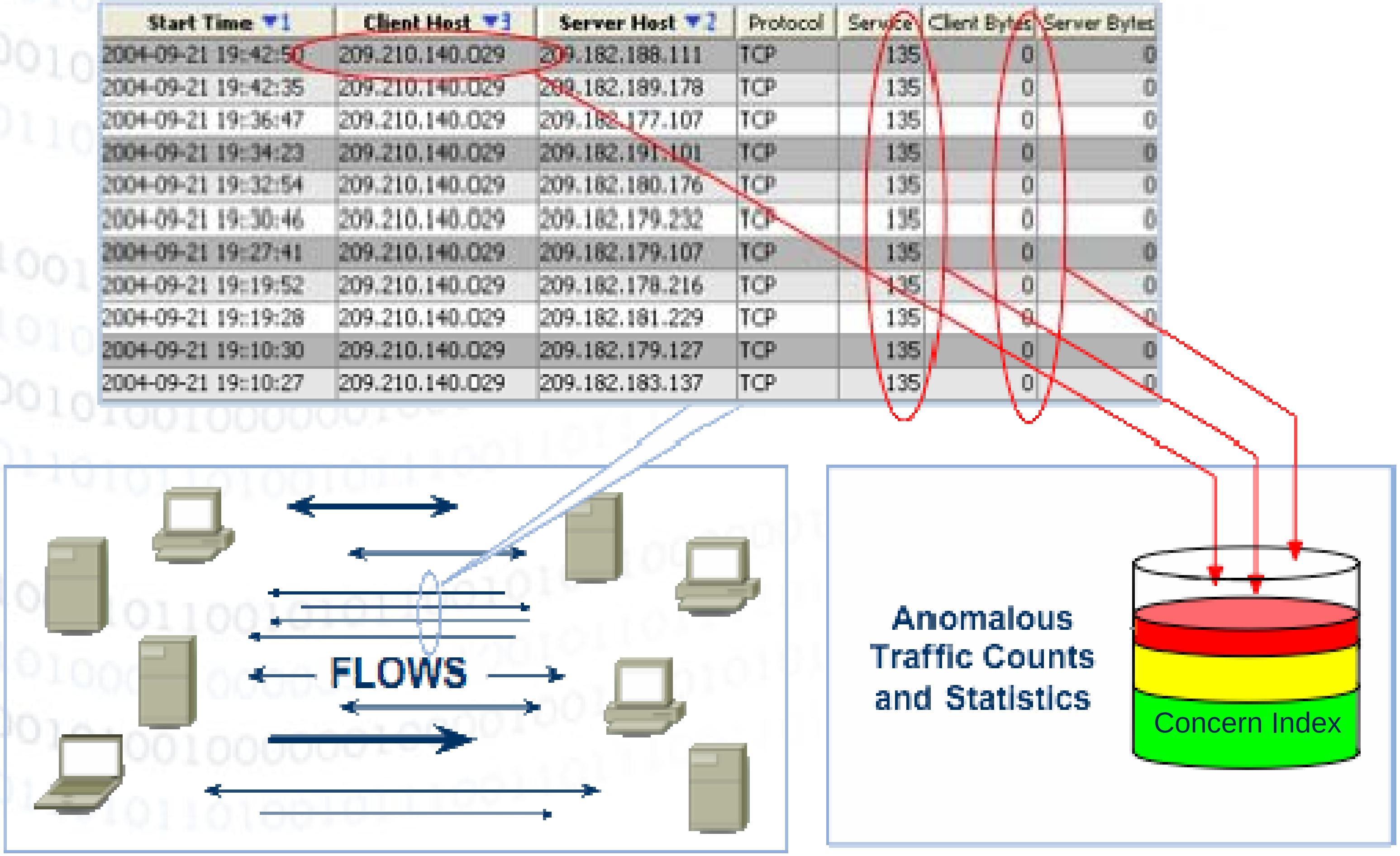
<$50,000



Presented at Central Plains ISSA Meeting – October 7, 2005

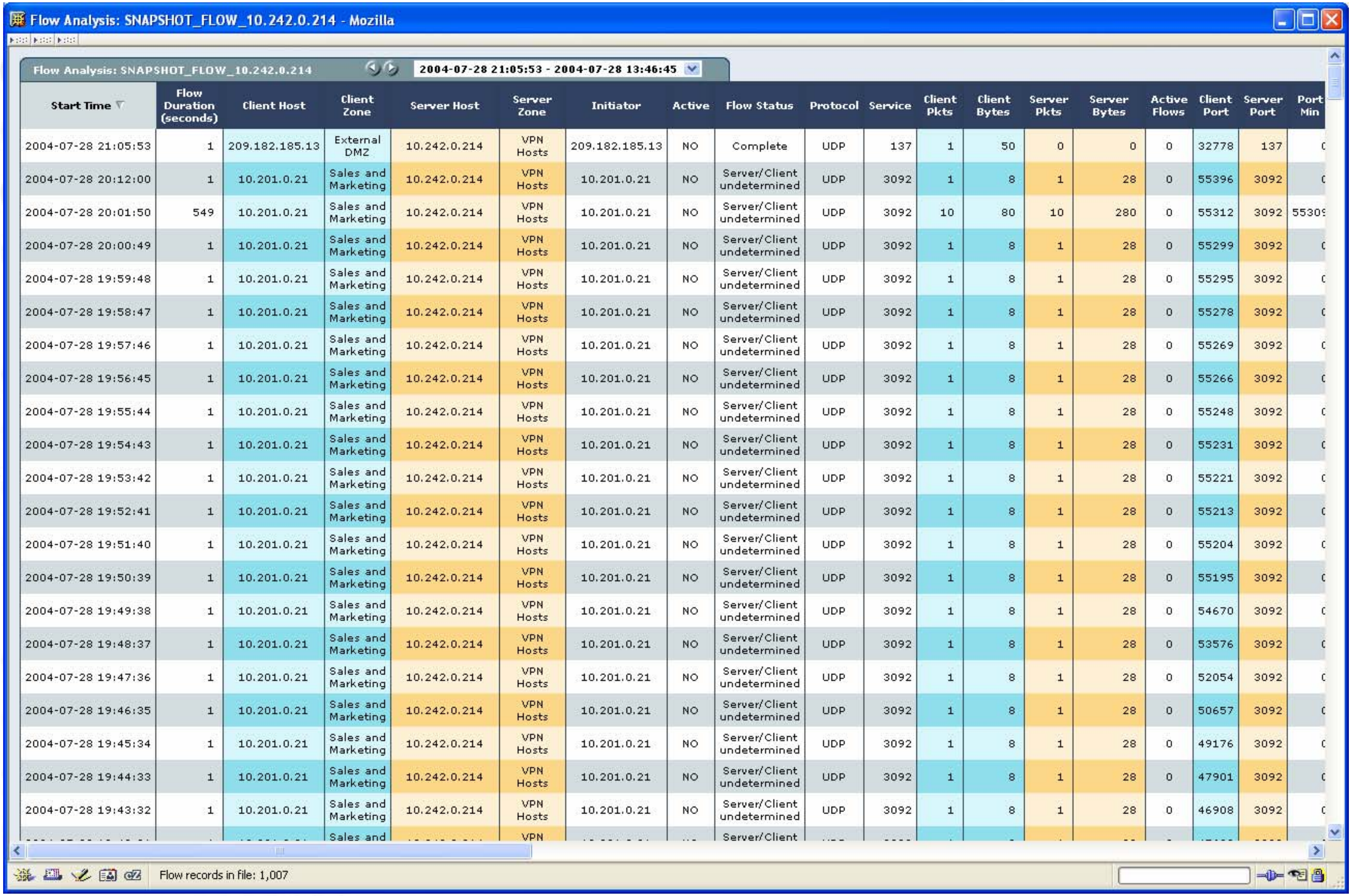
Overcome complex deployments and latency

PRE-EXISTING CONDITIONS ARE DETECTED



Start Time ▼1	Client Host ▼3	Server Host ▼2	Protocol	Service	Client Bytes	Server Bytes
2004-09-21 19:42:50	209.210.140.029	209.182.188.111	TCP	135	0	0
2004-09-21 19:42:35	209.210.140.029	209.182.189.178	TCP	135	0	0
2004-09-21 19:36:47	209.210.140.029	209.182.177.107	TCP	135	0	0
2004-09-21 19:34:23	209.210.140.029	209.182.191.101	TCP	135	0	0
2004-09-21 19:32:54	209.210.140.029	209.182.180.176	TCP	135	0	0
2004-09-21 19:30:46	209.210.140.029	209.182.179.232	TCP	135	0	0
2004-09-21 19:27:41	209.210.140.029	209.182.179.107	TCP	135	0	0
2004-09-21 19:19:52	209.210.140.029	209.182.178.216	TCP	135	0	0
2004-09-21 19:19:28	209.210.140.029	209.182.181.229	TCP	135	0	0
2004-09-21 19:10:30	209.210.140.029	209.182.179.127	TCP	135	0	0
2004-09-21 19:10:27	209.210.140.029	209.182.183.137	TCP	135	0	0

Anomalous Traffic Counts and Statistics



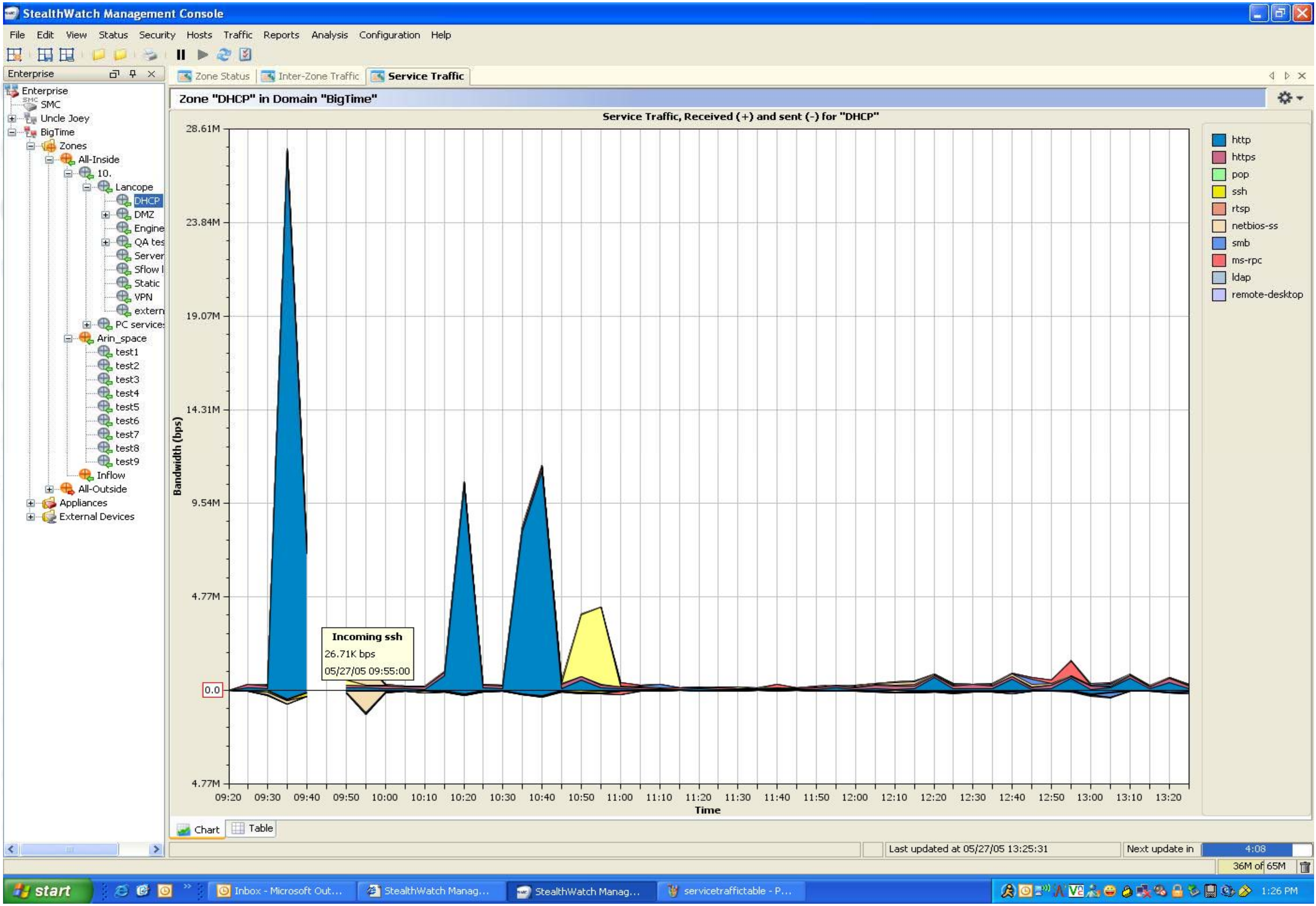
Flow Analysis: SNAPSHOT_FLOW_10.242.0.214 - Mozilla

Flow Analysis: SNAPSHOT_FLOW_10.242.0.214 — 2004-07-28 21:05:53 - 2004-07-28 13:46:45

Start Time	Flow Duration (seconds)	Client Host	Client Zone	Server Host	Server Zone	Initiator	Active	Flow Status	Protocol	Service	Client Pkts	Client Bytes	Server Pkts	Server Bytes	Active Flows	Client Port	Server Port	Port Min
2004-07-28 21:05:53	1	209.182.185.13	External DMZ	10.242.0.214	VPN Hosts	209.182.185.13	NO	Complete	UDP	137	1	50	0	0	0	32778	137	0
2004-07-28 20:12:00	1	10.201.0.21	Sales and Marketing	10.242.0.214	VPN Hosts	10.201.0.21	NO	Server/Client undetermined	UDP	3092	1	8	1	28	0	55396	3092	0
2004-07-28 20:01:50	549	10.201.0.21	Sales and Marketing	10.242.0.214	VPN Hosts	10.201.0.21	NO	Server/Client undetermined	UDP	3092	10	80	10	280	0	55312	3092	5530
2004-07-28 20:00:49	1	10.201.0.21	Sales and Marketing	10.242.0.214	VPN Hosts	10.201.0.21	NO	Server/Client undetermined	UDP	3092	1	8	1	28	0	55299	3092	0
2004-07-28 19:59:48	1	10.201.0.21	Sales and Marketing	10.242.0.214	VPN Hosts	10.201.0.21	NO	Server/Client undetermined	UDP	3092	1	8	1	28	0	55295	3092	0
2004-07-28 19:58:47	1	10.201.0.21	Sales and Marketing	10.242.0.214	VPN Hosts	10.201.0.21	NO	Server/Client undetermined	UDP	3092	1	8	1	28	0	55278	3092	0
2004-07-28 19:57:46	1	10.201.0.21	Sales and Marketing	10.242.0.214	VPN Hosts	10.201.0.21	NO	Server/Client undetermined	UDP	3092	1	8	1	28	0	55269	3092	0
2004-07-28 19:56:45	1	10.201.0.21	Sales and Marketing	10.242.0.214	VPN Hosts	10.201.0.21	NO	Server/Client undetermined	UDP	3092	1	8	1	28	0	55266	3092	0
2004-07-28 19:55:44	1	10.201.0.21	Sales and Marketing	10.242.0.214	VPN Hosts	10.201.0.21	NO	Server/Client undetermined	UDP	3092	1	8	1	28	0	55248	3092	0
2004-07-28 19:54:43	1	10.201.0.21	Sales and Marketing	10.242.0.214	VPN Hosts	10.201.0.21	NO	Server/Client undetermined	UDP	3092	1	8	1	28	0	55231	3092	0
2004-07-28 19:53:42	1	10.201.0.21	Sales and Marketing	10.242.0.214	VPN Hosts	10.201.0.21	NO	Server/Client undetermined	UDP	3092	1	8	1	28	0	55221	3092	0
2004-07-28 19:52:41	1	10.201.0.21	Sales and Marketing	10.242.0.214	VPN Hosts	10.201.0.21	NO	Server/Client undetermined	UDP	3092	1	8	1	28	0	55213	3092	0
2004-07-28 19:51:40	1	10.201.0.21	Sales and Marketing	10.242.0.214	VPN Hosts	10.201.0.21	NO	Server/Client undetermined	UDP	3092	1	8	1	28	0	55204	3092	0
2004-07-28 19:50:39	1	10.201.0.21	Sales and Marketing	10.242.0.214	VPN Hosts	10.201.0.21	NO	Server/Client undetermined	UDP	3092	1	8	1	28	0	55195	3092	0
2004-07-28 19:49:38	1	10.201.0.21	Sales and Marketing	10.242.0.214	VPN Hosts	10.201.0.21	NO	Server/Client undetermined	UDP	3092	1	8	1	28	0	54670	3092	0
2004-07-28 19:48:37	1	10.201.0.21	Sales and Marketing	10.242.0.214	VPN Hosts	10.201.0.21	NO	Server/Client undetermined	UDP	3092	1	8	1	28	0	53576	3092	0
2004-07-28 19:47:36	1	10.201.0.21	Sales and Marketing	10.242.0.214	VPN Hosts	10.201.0.21	NO	Server/Client undetermined	UDP	3092	1	8	1	28	0	52054	3092	0
2004-07-28 19:46:35	1	10.201.0.21	Sales and Marketing	10.242.0.214	VPN Hosts	10.201.0.21	NO	Server/Client undetermined	UDP	3092	1	8	1	28	0	50657	3092	0
2004-07-28 19:45:34	1	10.201.0.21	Sales and Marketing	10.242.0.214	VPN Hosts	10.201.0.21	NO	Server/Client undetermined	UDP	3092	1	8	1	28	0	49176	3092	0
2004-07-28 19:44:33	1	10.201.0.21	Sales and Marketing	10.242.0.214	VPN Hosts	10.201.0.21	NO	Server/Client undetermined	UDP	3092	1	8	1	28	0	47901	3092	0
2004-07-28 19:43:32	1	10.201.0.21	Sales and Marketing	10.242.0.214	VPN Hosts	10.201.0.21	NO	Server/Client undetermined	UDP	3092	1	8	1	28	0	46908	3092	0
			Sales and		VPN			Server/Client										

Flow records in file: 1,007

Lancope



Zone "DHCP" in Domain "BigTime"

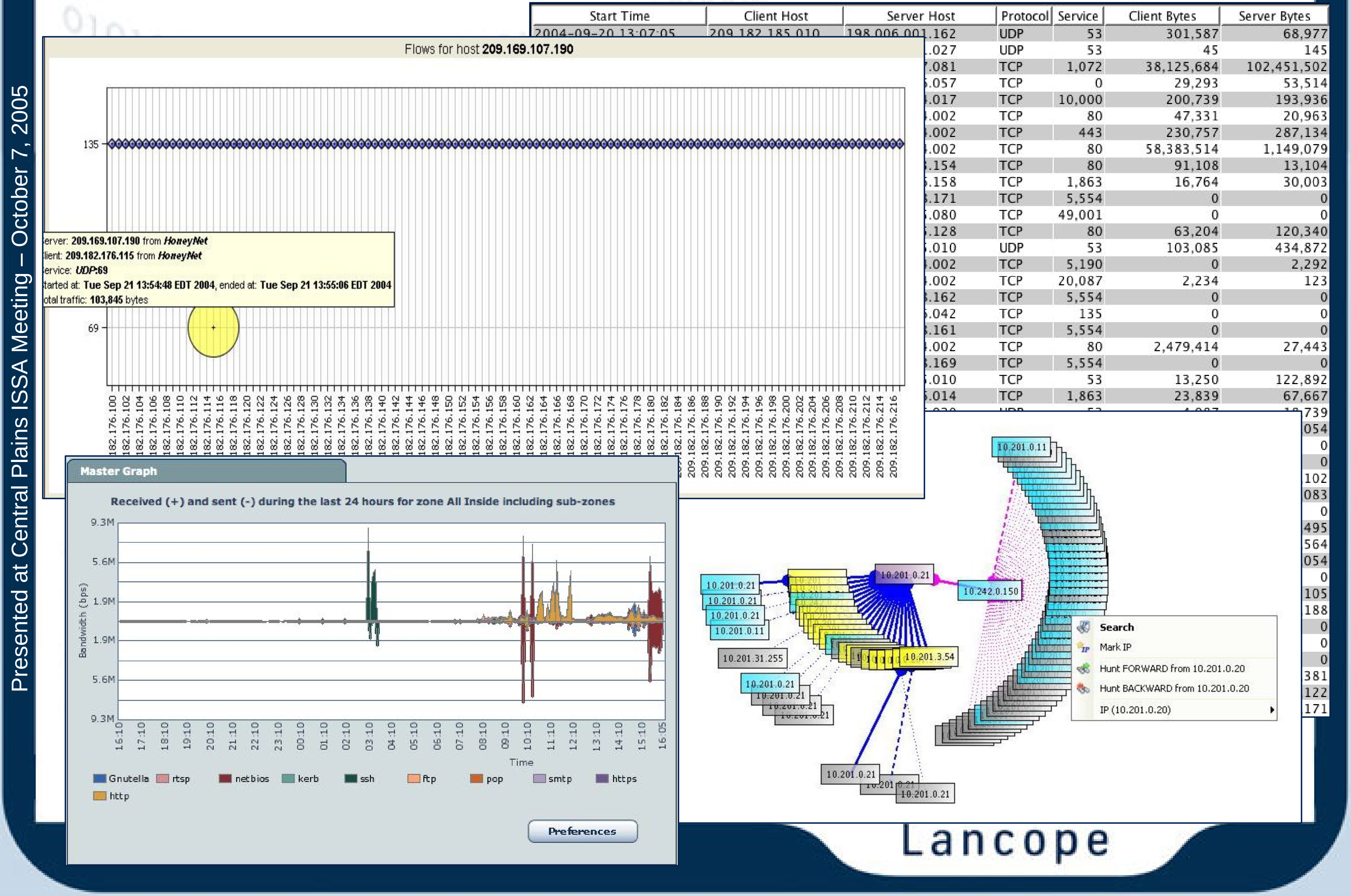
Service Traffic, Received (+) and sent (-) for "DHCP"

Incoming ssh
26.71K bps
05/27/05 09:55:00

Last updated at 05/27/05 13:25:31

Next update in 4:08

36M of 65M



Start Time	Client Host	Server Host	Protocol	Service	Client Bytes	Server Bytes
2004-09-20 13:07:05	209.182.185.010	198.006.001.162	UDP	53	301,587	68,977
		.027	UDP	53	45	145
		7.081	TCP	1,072	38,125,684	102,451,502
		5.057	TCP	0	29,293	53,514
		4.017	TCP	10,000	200,739	193,936
		4.002	TCP	80	47,331	20,963
		4.002	TCP	443	230,757	287,134
		4.002	TCP	80	58,383,514	1,149,079
		5.154	TCP	80	91,108	13,104
		5.158	TCP	1,863	16,764	30,003
		3.171	TCP	5,554	0	0
		5.080	TCP	49,001	0	0
		5.128	TCP	80	63,204	120,340
		5.010	UDP	53	103,085	434,872
		4.002	TCP	5,190	0	2,292
		4.002	TCP	20,087	2,234	123
		3.162	TCP	5,554	0	0
		5.042	TCP	135	0	0
		3.161	TCP	5,554	0	0
		4.002	TCP	80	2,479,414	27,443
		3.169	TCP	5,554	0	0
		5.010	TCP	53	13,250	122,892
		5.014	TCP	1,863	23,839	67,667
						18,739
						054
						0
						0
						102
						083
						0
						495
						564
						054
						0
						105
						188
						0
						0
						0
						381
						122
						171

Flows for host **209.169.107.190**

erver: **209.169.107.190** from ***HoneyNet***
lient: **209.182.176.115** from ***HoneyNet***
ervice: ***UDP*:69**
tarted at: **Tue Sep 21 13:54:48 EDT 2004**, ended at: **Tue Sep 21 13:55:06 EDT 2004**
otal traffic: **103,845** bytes

Lancope

Questions?

Thank you for your time!!

Aaron Torres
Senior Security Engineer
atorres@lancope.com
512-659-3726