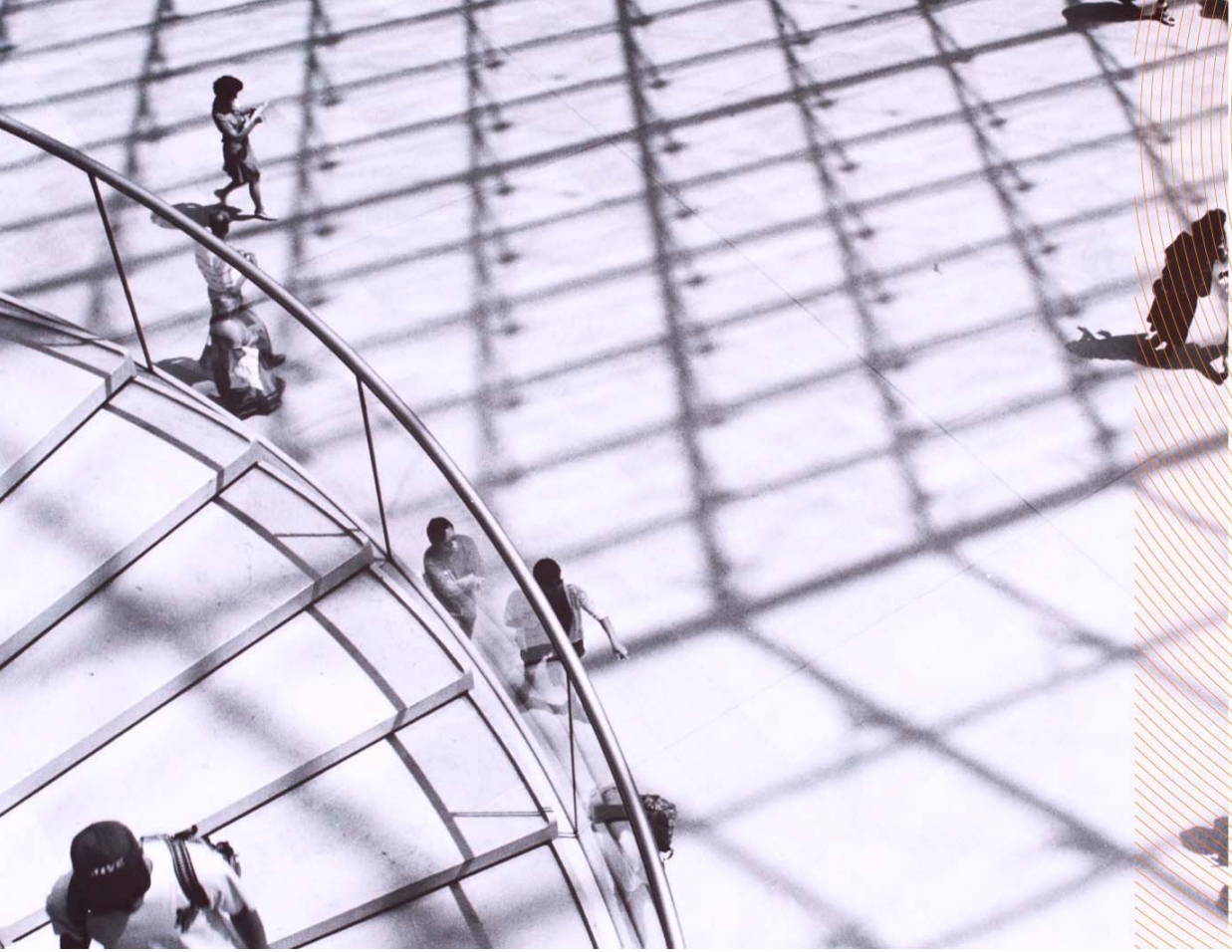


Beyond a sensor

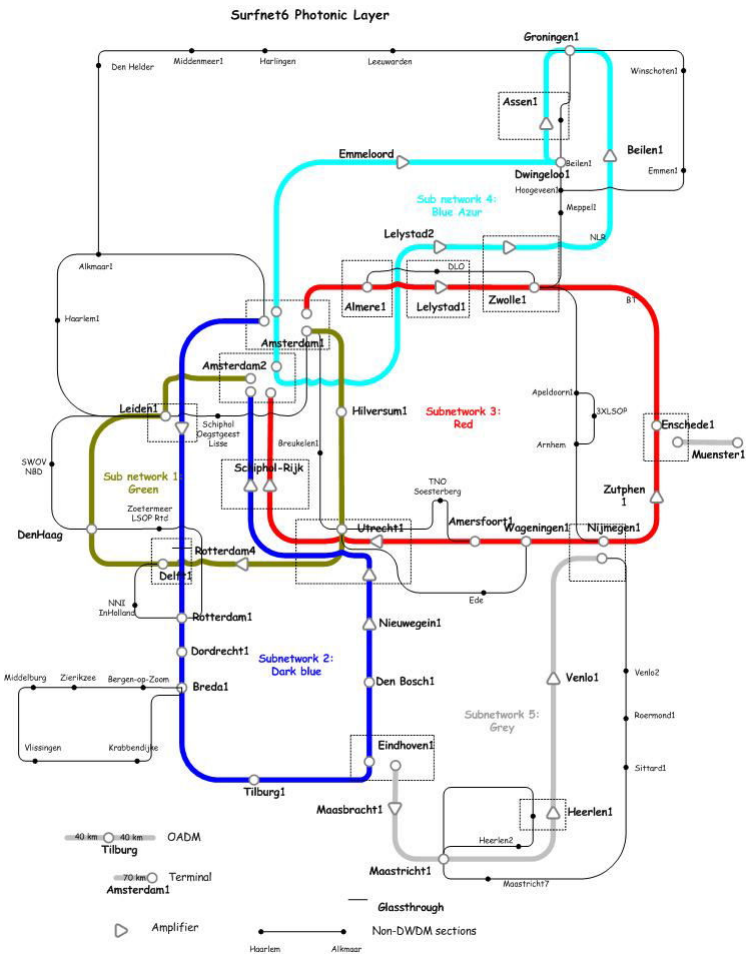
Towards the Globalization of SURFids

Wim.Biemolt@surfnet.nl

FIRST 20th Annual Conference — Vancouver, Canada

SURFnet6


Leeuwarden
Groningen
Winschoten
Assen
Westerbork
Dwingeloo
Den Helder
Emmen
Hoogeveen
Alkmaar
Meppel
Zwolle
Lelystad
Haarlem
Amsterdam
Schiphol-Rijk
Apeldoorn
Deventer
Enschede
Oegstgeest
Lisse
Leiden
Hilversum
Zutphen
Breukelen
Utrecht
Den Haag
Nieuwegein
Houten
Wageningen
Arnhem
Delft
Gouda
Rotterdam
Dordrecht
Oss
Nijmegen
Zierikzee
Den Bosch
Middelburg
Breda
Tilburg
Vlissingen
Yerseke
Bergen op Zoom
Eindhoven
Venlo
Maasbracht
Maastricht
Heerlen


Surfnet6 Photonic Layer
Groningen1
Den Helder
Middenmeer1
Harlingen
Leeuwarden
Winschoten1
Assen1
Beilen1
Emmeloord
Dwingeloo1
Sub network 4:
Blue Azur
Meppel1
Lelystad2
Alkmaar1
Haarlem1
Almere1
Lelystad1
Zwolle1
Amsterdam1
Amsterdam2
Leiden1
Hilversum1
Subnetwork 3:
Red
Apeldoorn1
Enschede1
Muenster1
Arnhem
Schiphol-Rijk
Sub network 1
Green
Breukelen1
SWOV
NBD
Zutphen
1
DenHaag
Utrecht1
Amersfoort1
Wageningen1
Nijmegen1
Rotterdam4
Delft1
Ede
Rotterdam1
Nieuwegein1
Dordrecht1
Subnetwork 2:
Dark blue
Middelburg
Zierikzee
Bergen-op-Zoom
Breda1
Den Bosch1
Venlo1
Venlo2
Roermond1
Sittard1
Subnetwork 5:
Grey
Vlissingen
Krabbendijke
Eindhoven1
Tilburg1
Maasbracht1
Heerlen1
Heerlen2
Maastricht1
Maastricht7
40 km
40 km
OADM
Tilburg
70 km
Terminal
Amsterdam1
Glassthrough
Amplifier
Non-DWDM sections

SURFcert

18th Annual FIRST Conference

A Distributed Intrusion Detection System Based on Passive Sensors

Rogier Spoor (SURFnet-CERT – SURFnet, NL)

Wednesday – June 28th, 16:00

SURFnet is a very high-speed network which connects the networks of Dutch universities, colleges, research centers, academic hospitals and scientific libraries to one another and to other networks in Europe and the rest of the world. SURFnet handles many computer security incidents in which a SURFnet customer is involved, either as a victim or as a suspect. In order to decrease the amount of computer security incidents, SURFnet is going to roll-out a Distributed Intrusion Detection System (D-IDS) as a service to SURFnet connected parties.

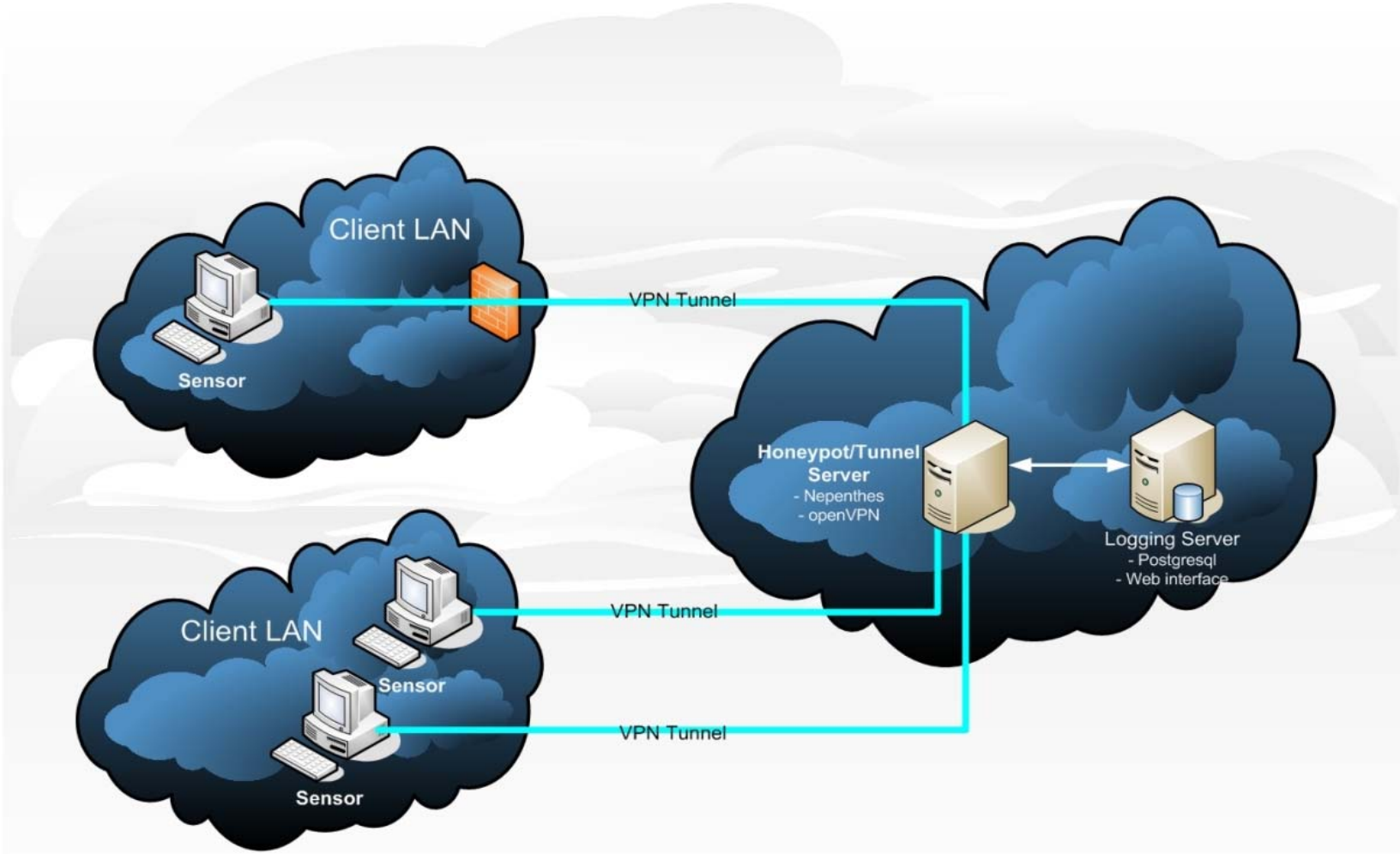
Goals

- Understanding:
  - types of malicious network traffic within a LAN
  - amount of malicious network traffic within a LAN
  - spreading of worms
- Setting up:
  - a scalable IDS solution
  - an IDS that is easy to manage and maintain
- Comparing results with other sensors
- Limit malicious outbound traffic from SURFnet

Why build something new?

- Sensor must be maintenance free
- IDS must be scalable and easy to manage
- No False Positives!
  - cannot use *snort*
- Design IDS based on high speed networks
  - LAN
  - WAN
- Design IDS “should” be able to analyze L2 traffic

Global overview



Sensor

- remastered Knoppix distribution
- USB boot
- OpenVPN between Sensor and Central Server
  - Portability.
  - Familiar daemon-style usage.
  - No kernel modifications required.
  - State-of-the-art cryptography
    - provided by the OpenSSL library
  - Comfortable with dynamic addresses or NAT.
  - Supports most operating systems
    - Linux, Windows, Mac OS X, BSD, and Solaris.

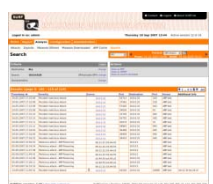
Needed

- Computer system
  - USB boot
  - 1 NIC
- DHCP or Static IP (2x)
- OpenVPN session
  - through local firewall (TCP 1194)
- HTTPS session
  - through local firewall (TCP 4443)

Servers

- Tunnel server
  - OpenVPN tunnel to sensor
  - Manage X509 certificates/keys of sensors
  - Source-based routing

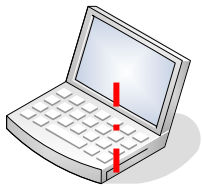
- Logging server
  - *Postgresql*
  - Web interface
  - Show statistics of sensors (groups/individual)
  - Show statistics of different attacks
  - Ranking of sensors
  - Mail logging
  - IDMEF



Honeypot

- Based on *nepenthes*
  - a low-interaction honeypot
  - http://nepenthes.mwcollect.org
  - mimics the replies generated by vulnerable services in order to collect the first stage exploit
  - Modules
    - Resolve DNS asynchronous
    - Emulate vulnerabilities
    - Download files
    - Submit the downloaded files
    - Trigger events
    - Shellcode handler

Working of SURFids



- Attacker/Worm/Virus/Hacker
- Attacks IP on server

- Layer 2 tunnel (tap device)
- Nepenthes simulates weakness
- Nepenthes handles attack

- Nepenthes logs attack

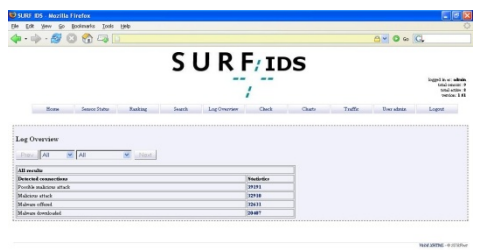
Honeypot/Tunnel Server
- Nepenthes
- OpenVPN

Logging Server
- Postgresql
- Web interface

- Sensor is booted
- OpenVPN is started

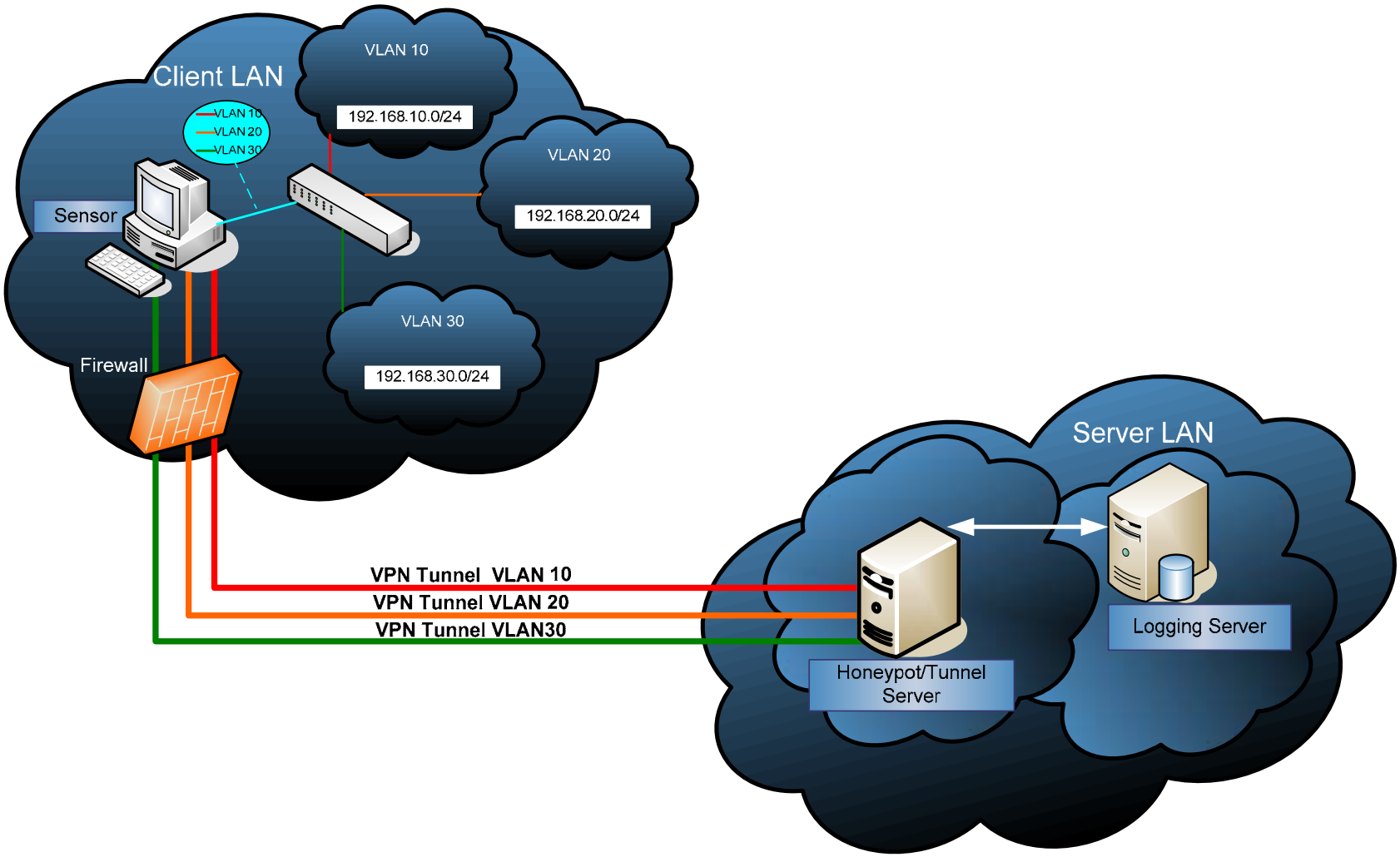
- Uses tcp port 1194
- Works with NAT !!

- Web interface makes data representable



Sensor

Multiple VLAN support

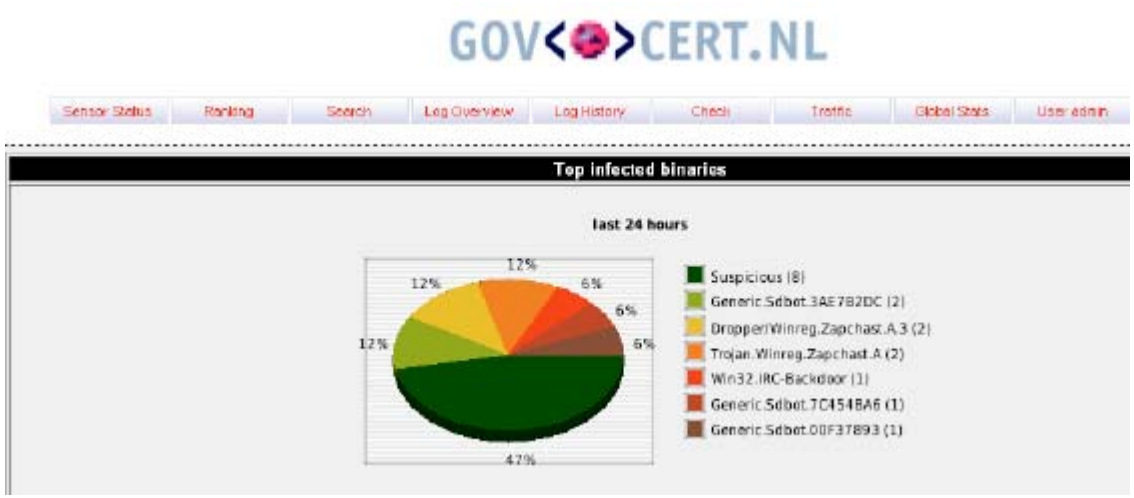


Users

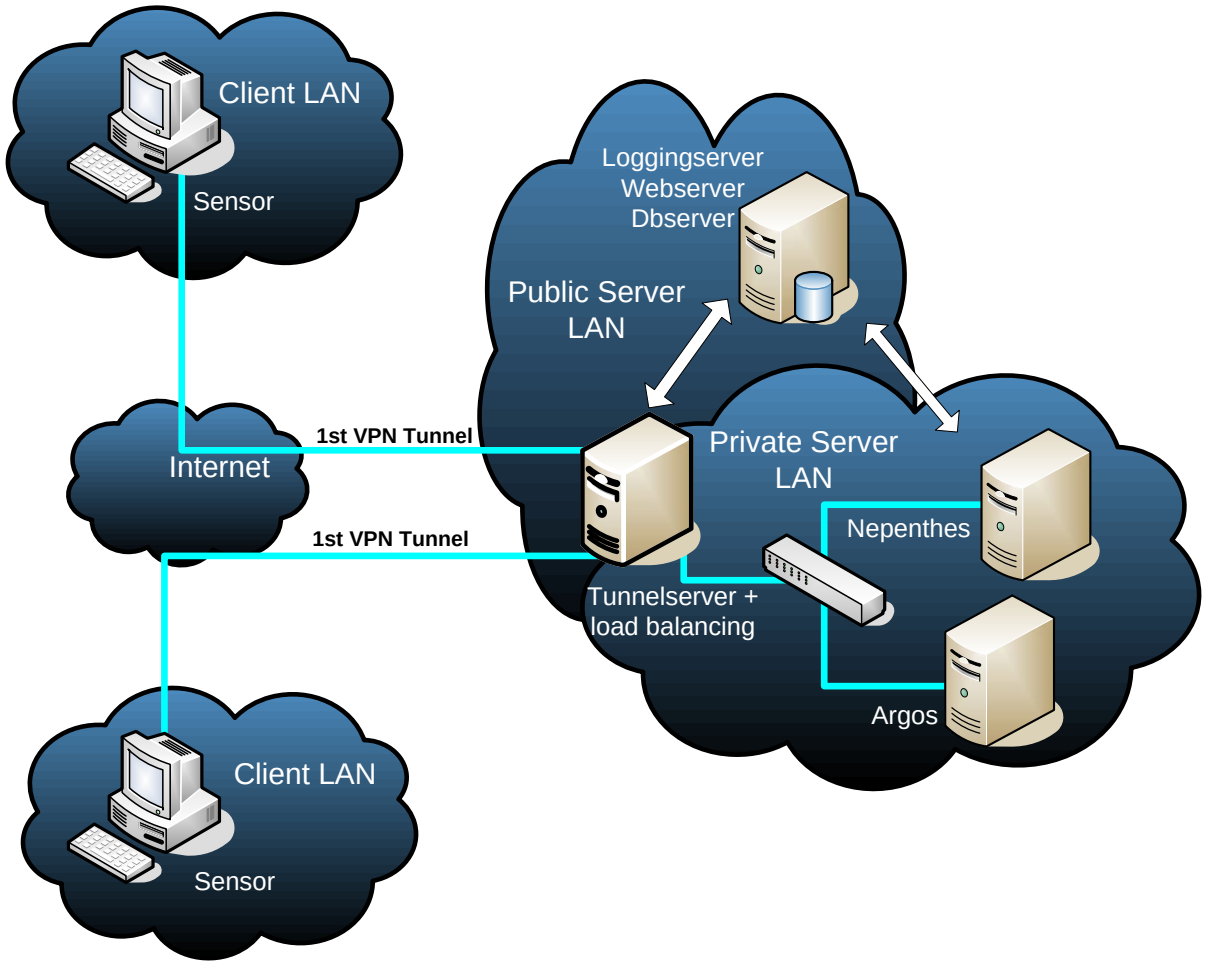
- Wisconsin University (USA)
- NTT-CERT (Japan)
- GOVCERT.NL
- SITEC (Sweden)
- HEANET (Ireland)
- ArCERT (Argentina)

Partnership

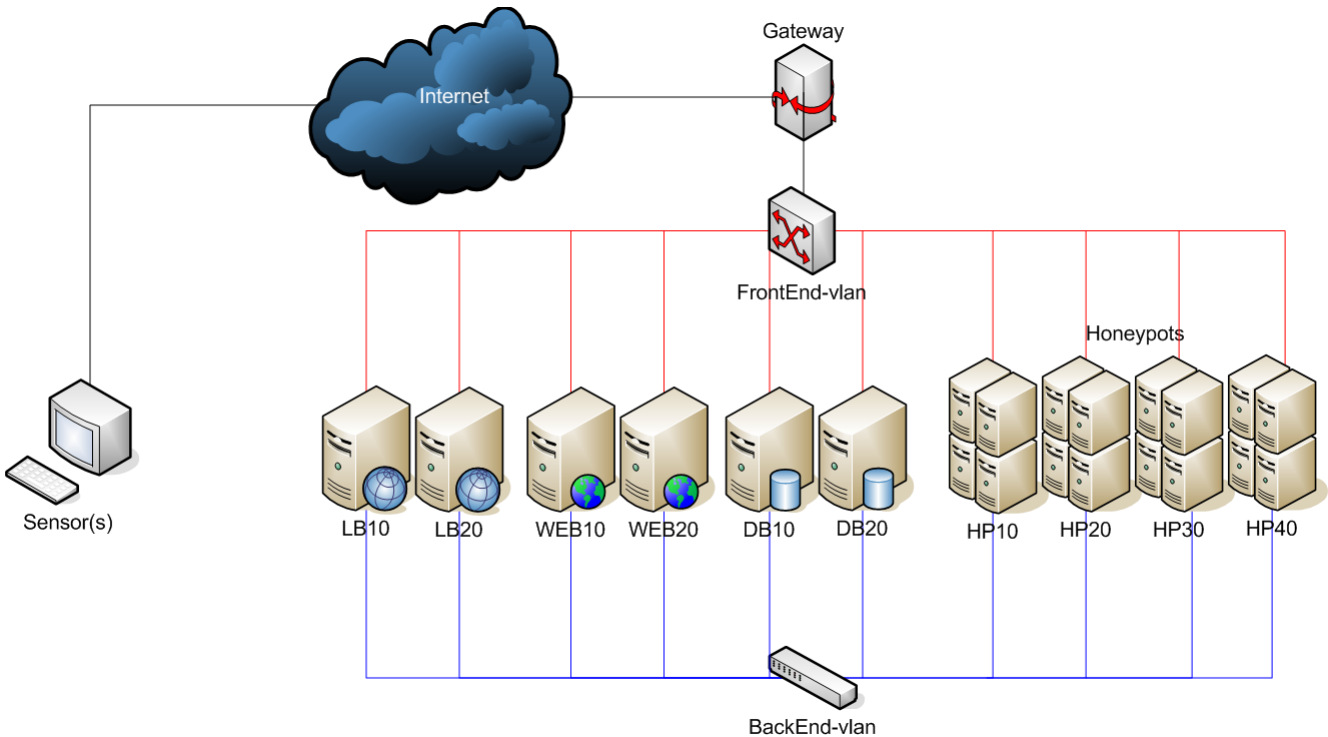
- GOVCERT.NL
  - Knowledge sharing
  - Add additional resources
  - Additional monitoring technics
  - Future development
  - Letter of intent



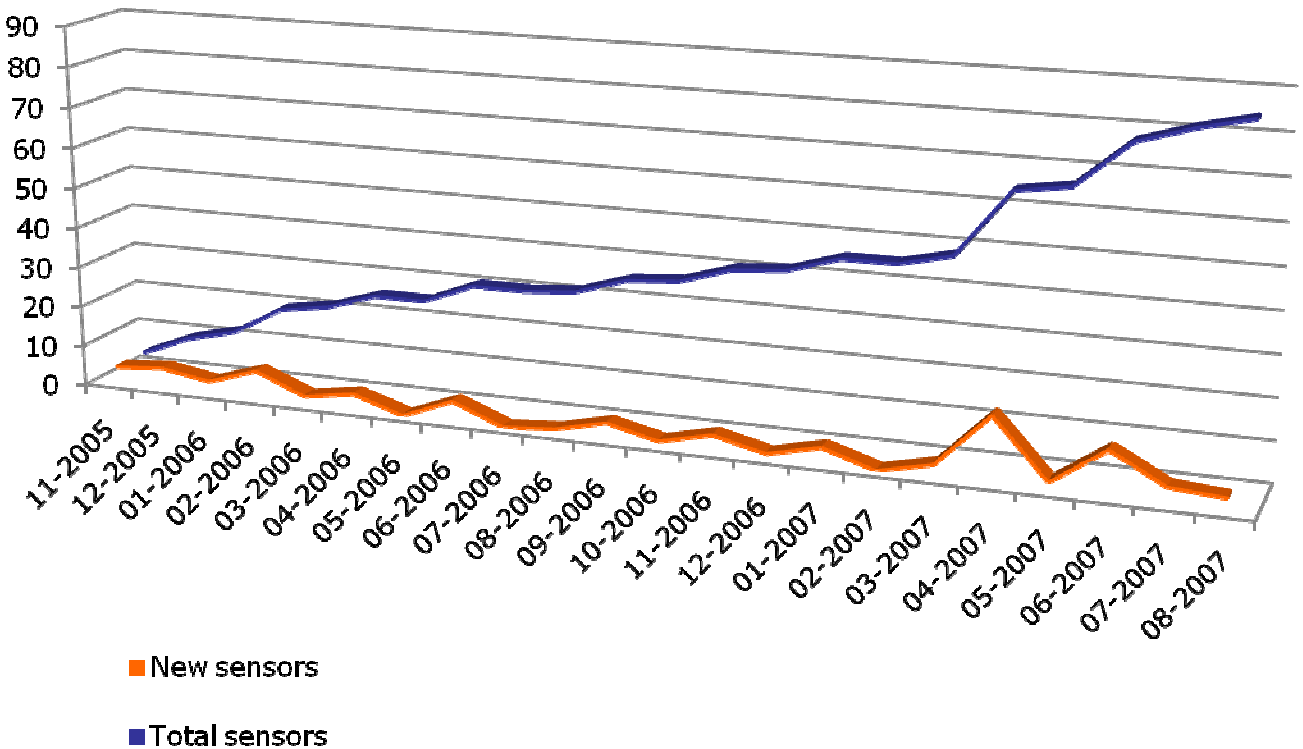
Current IDS setup



Logical design



Sensors deployed

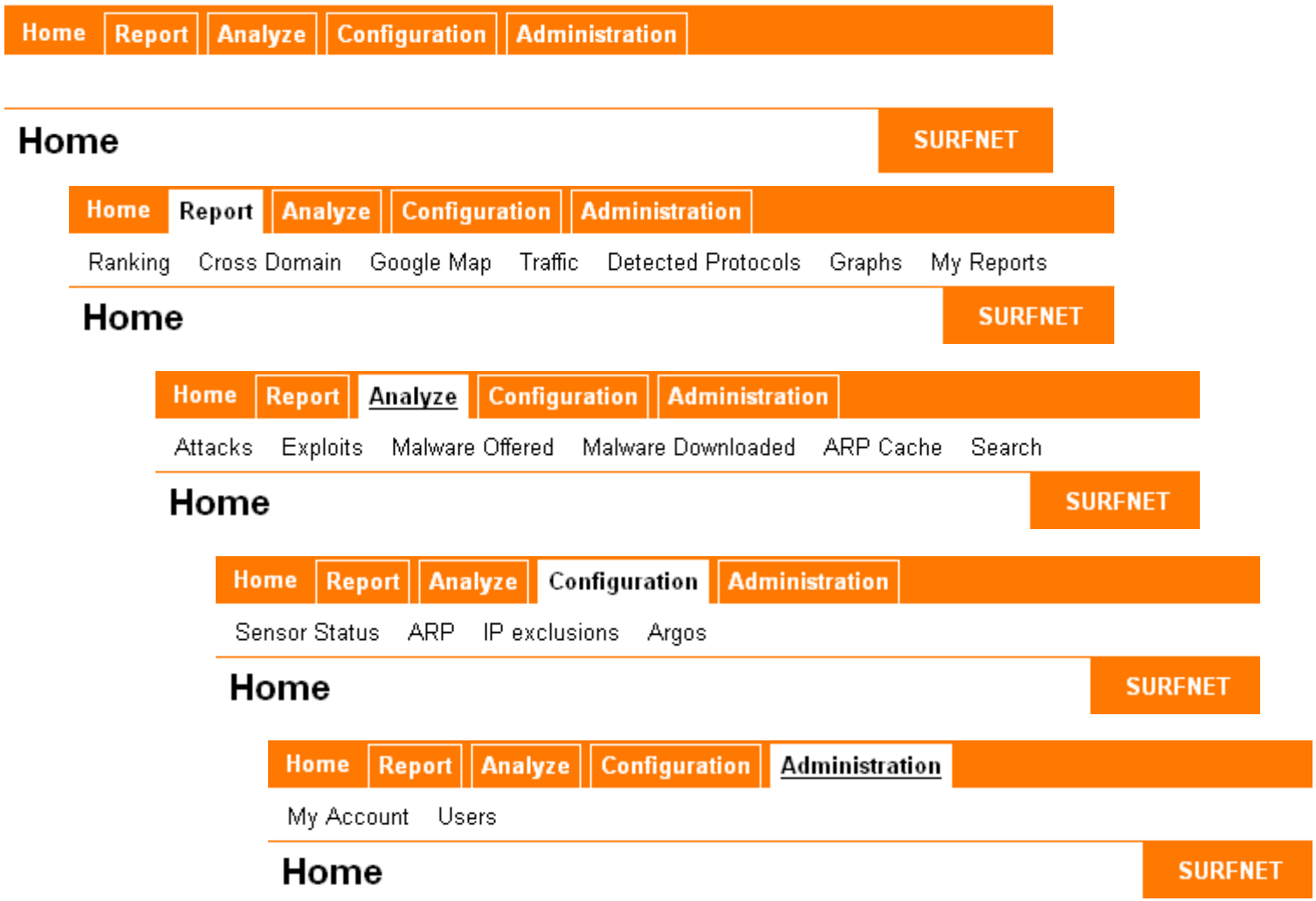


Results

- What do we see
  - Automated attacks
    - No end-user interaction
  - Attacks on OS and applications
  - Scans
  - Probes
  - Offered malware

- What we don’t see
  - Targeted attacks
  - System hacking

Menu


Home
Report
Analyze
Configuration
Administration
Home
SURFNET
Home
Report
Analyze
Configuration
Administration
Ranking
Cross Domain
Google Map
Traffic
Detected Protocols
Graphs
My Reports
Home
SURFNET
Home
Report
Analyze
Configuration
Administration
Attacks
Exploits
Malware Offered
Malware Downloaded
ARP Cache
Search
Home
SURFNET
Home
Report
Analyze
Configuration
Administration
Sensor Status
ARP
IP exclusions
Argos
Home
SURFNET
Home
Report
Analyze
Configuration
Administration
My Account
Users
Home
SURFNET

Attacks

Attacks

Detected connections	Statistics
Possible malicious attack [?]	123,086 ↘
Malicious attack [?]	33,991 ↘
Nepenthes	33,911 ↘
Argos	25 ↘
Rogue DHCP server	55 ↘
Malware offered [?]	32,567 ↘
Malware downloaded [?]	3,628 ↘

Malware Downloaded

Malware Downloaded

SURFNET | Period: Today | From: 24-06-2008 00:00 Until: 25-06-2008 00:00

Malware Downloaded

Malware	BitDefender	Kaspersky	F-Prot	AVAST	Antivir	ClamAV	Stats
39b8..	Suspicious	Suspicious	Suspicious	Win32:Rootkit-gen	Suspicious	Suspicious	1
c117..	Win32.Virtob.3.Gen	Virus.Win32.Virut.n	W32/Virut.9264	Win32:Virut	W32/Virut.Gen	W32.Virut.di	1
df51..	Suspicious	Suspicious	Suspicious	Suspicious	Suspicious	Suspicious	1
3228..	Backdoor.SDbot.DFNQ	Suspicious	Suspicious	Suspicious	Suspicious	Suspicious	1
eb90..	Suspicious	Suspicious	Suspicious	Suspicious	Suspicious	Trojan.Mybot-10186	1
1f8a..	Backdoor.SDbot.DFNQ	Suspicious	Suspicious	Suspicious	Suspicious	Suspicious	1
98eb..	Backdoor.SDbot.DFNQ	Suspicious	Suspicious	Suspicious	Suspicious	Suspicious	1
9019..	Backdoor.Rbot.FAW	Suspicious	Suspicious	Suspicious	Suspicious	Suspicious	1
c5ff..	Backdoor.Rbot.FAW	Suspicious	Suspicious	Suspicious	Suspicious	Suspicious	1
total %	6 / 9 = 66 %	1 / 9 = 11 %	1 / 9 = 11 %	2 / 9 = 22 %	1 / 9 = 11 %	2 / 9 = 22 %	

Binary info

Binary	39b81ab57624d9b174d9f13e0b73691a
Size	111 KB
Info	MS-DOS executable PE for MS Windows (GUI) Intel 80386 32-bit
First Seen	10-02-2008 11:04:55
Last Seen	24-06-2008 09:29:44

Filenames Used

host.exe
ssms.exe
RPof7g==
uKlf+A==
hvEf+A==

Binary History

Timestamp	BitDefender	Kaspersky	F-Prot	AVAST	Antivir	ClamAV
13-02-2008 09:22:10			Suspicious	Suspicious	TR/Crypt.XPACK.Gen	Trojan.Eggdrop-51
31-05-2008 10:35:50			Suspicious	Win32:Rootkit-gen	TR/Crypt.XPACK.Gen	Trojan.Eggdrop-51
18-06-2008 00:04:02	Suspicious	Suspicious	Suspicious	Win32:Rootkit-gen	Suspicious	Suspicious

Sensor Status

Sensors

View online sensors

Sensor ▲	Label	Config method	Device IP	Uptime	Status	Action	
sensor114	PRODUCTIE	DHCP	192	7d 8h 59m 45s	Online	None	Update
sensor232	AS1103.NET	DHCP	192	4d 6h 42m 23s	Online	None	Update
sensor283-118	WERKnet	VLAN Static	192	32d 7h 56m 55s	Online	None	Update
sensor85	PRUTSNET	DHCP	192	4d 6h 43m 57s	Online	None	Update
sensor86	AS1101.NET	DHCP	192	7d 6h 11m 15s	Online	None	Update

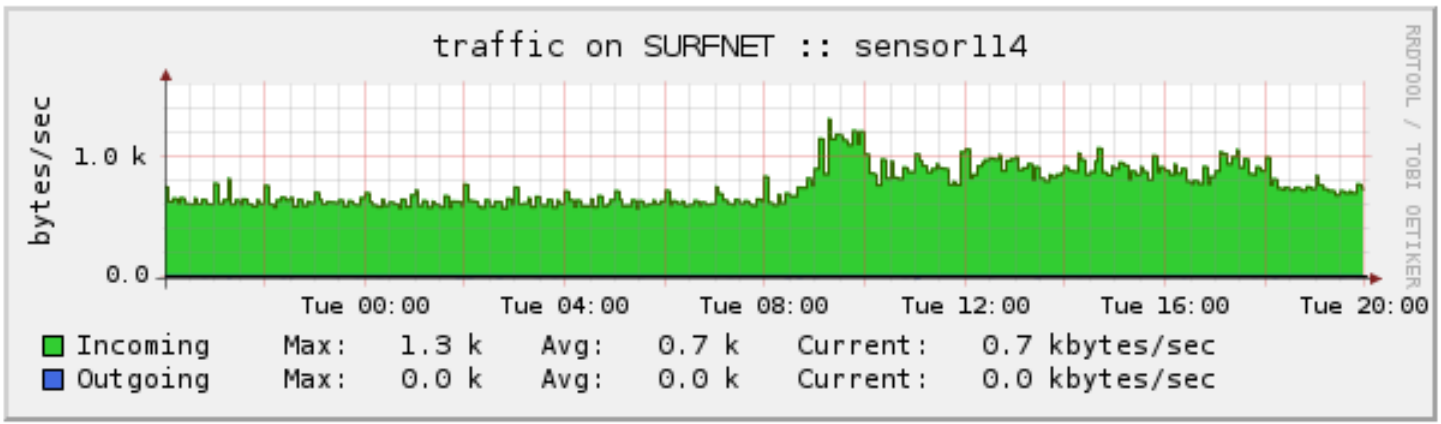
Legend

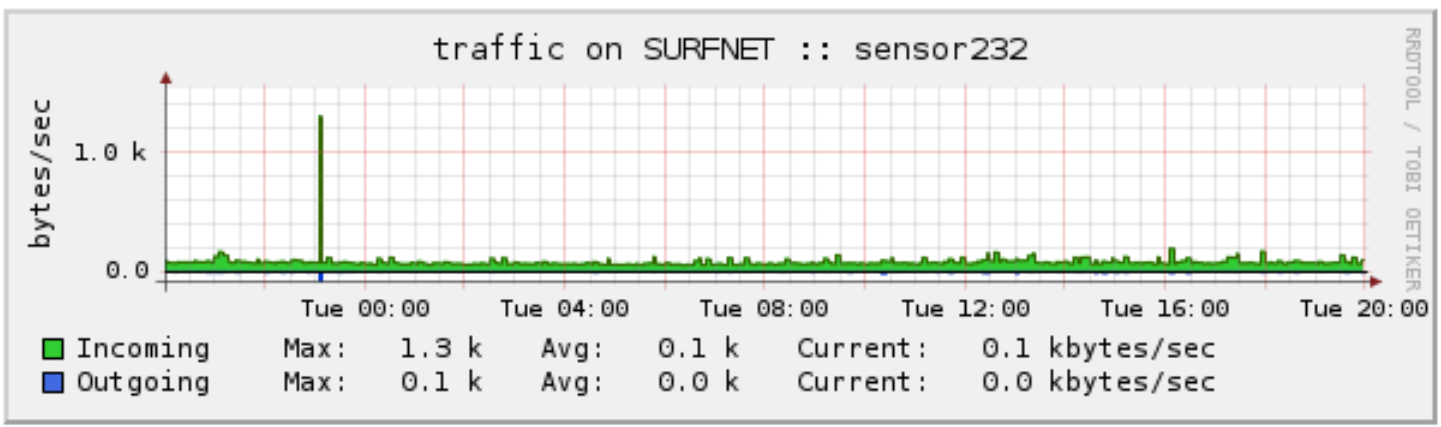
Offline	Missing keepalive
Online	Configuration
Disabled by admin	Starting up
Ignored	Out of date

Traffic

Traffic

Traffic — View online sensors





Statistics

- Exploit statistics
- UDP/TCP port statistics
- Malware filenames
- Download protocol
- Attack OS

Exploits

SURFNET | Period: 171 day(s) | From: 01-01-2008 00:00 Until: 21-06-2008 00:00

Top 5 exploits of all sensors		
#	Exploit	Total
1.	DCOM	21,986 (39%)
2.	Symantec AV	18,905 (34%)
3.	ASN1	7,102 (13%)
4.	LSASS	4,262 (8%)
5.	IIS	3,919 (7%)

Top 5 exploits of your sensors		
#	Exploit	Total
1.	Symantec AV	10,527 ↘ (34%)
2.	DCOM	10,516 ↘ (34%)
3.	ASN1	4,640 ↘ (15%)
4.	IIS	2,897 ↘ (9%)
5.	LSASS	2,688 ↘ (9%)

UDP / TCP ports

Top 10 ports of all sensors			
#	Port	Port Description	Total
1	445	microsoft-ds	106538 (34%)
2	135	msrpc	73162 (23%)
3	139	netbios-ssn	44657 (14%)
4	2967	No description	42229 (13%)
5	8555	No description	18208 (6%)
6	80	http	18173 (6%)
7	21	ftp	8132 (3%)
8	10000	No description	2692 (1%)
9	1957	No description	2113 (1%)
10	2968	No description	1497 (0%)

Top 10 ports of your sensors			
#	Port	Port Description	Total
1	445	microsoft-ds	50975 ↘ (33%)
2	135	msrpc	44082 ↘ (29%)
3	2967	No description	22844 ↘ (15%)
4	139	netbios-ssn	11146 ↘ (7%)
5	8555	No description	10152 ↘ (7%)
6	80	http	7616 ↘ (5%)
7	21	ftp	3179 ↘ (2%)
8	1957	No description	1676 ↘ (1%)
9	10000	No description	653 ↘ (0%)
10	2968	No description	499 ↘ (0%)

Malware filenames

Top 10 filenames of all sensors		
#	Filename	Total
1	ssms.exe	6150 (21%)
2	runsvc32.exe	5064 (17%)
3	win.exe	4221 (14%)
4	sys.exe	2962 (10%)
5	feedfetcher.html	2555 (9%)
6	host.exe	2278 (8%)
7	antivir.exe	2174 (7%)
8	rpcall.exe	2156 (7%)
9	sdhost.exe	1148 (4%)
10	0	1147 (4%)

Top 10 filenames of your sensors		
#	Filename	Total
1	ssms.exe	4724 ↘ (22%)
2	win.exe	2824 ↘ (13%)
3	runsvc32.exe	2773 ↘ (13%)
4	feedfetcher.html	2555 ↘ (12%)
5	sys.exe	2028 ↘ (10%)
6	host.exe	1976 ↘ (9%)
7	antivir.exe	1509 ↘ (7%)
8	rpcall.exe	1395 ↘ (7%)
9	sdhost.exe	867 ↘ (4%)
10	msnnmaneger.exe	604 ↘ (3%)

Download protocol

Top 5 download protocols of all sensors		
#	Protocol	Total
1	ftp	35982 (52%)
2	tftp	15236 (22%)
3	link	11552 (17%)
4	http	3992 (6%)
5	blink	2561 (4%)

Top 5 download protocols of your sensors		
#	Protocol	Total
1	ftp	20667 (57%)
2	tftp	11658 (32%)
3	http	2882 (8%)
4	link	838 (2%)
5	csend	32 (0%)

Attack OS

Top 5 attacker OS's of all sensors		
#	OS	Total
1	Windows	386881 (96%)
2	Linux	9154 (2%)
3	NMAP	4897 (1%)
4	FreeBSD	645 (0%)
5	Novell	348 (0%)

Top 5 attacker OS's of your sensors		
#	OS	Total
1	Windows	187901 (97%)
2	NMAP	3252 (2%)
3	Linux	2399 (1%)
4	FreeBSD	154 (0%)
5	ULTRIX	122 (0%)

Attack sources

Top 10 source addresses of all sensors		
#	Address	Total
1	124.246	19286 (24%)
2	203.8	17066 (22%)
3	124.246	15884 (20%)
4	64.203	10070 (13%)
5	82.80	3738 (5%)
6	209.85	3226 (4%)
7	69.41	3171 (4%)
8	58.251	3095 (4%)
9	66.42.	2020 (3%)
10	71.195	1524 (2%)

Attack sources

Top 10 source addresses of your sensors		
#	Address	Total
1	203.8	11080 ↘ (21%)
2	124.246	10357 ↘ (19%)
3	64.203	10070 ↘ (19%)
4	124.246.	9599 ↘ (18%)
5	209.85	3226 ↘ (6%)
6	69.41	2685 ↘ (5%)
7	58.251	1940 ↘ (4%)
8	82.80	1869 ↘ (3%)
9	68.94	1350 ↘ (3%)
10	66.42	1301 ↘ (2%)

My reports

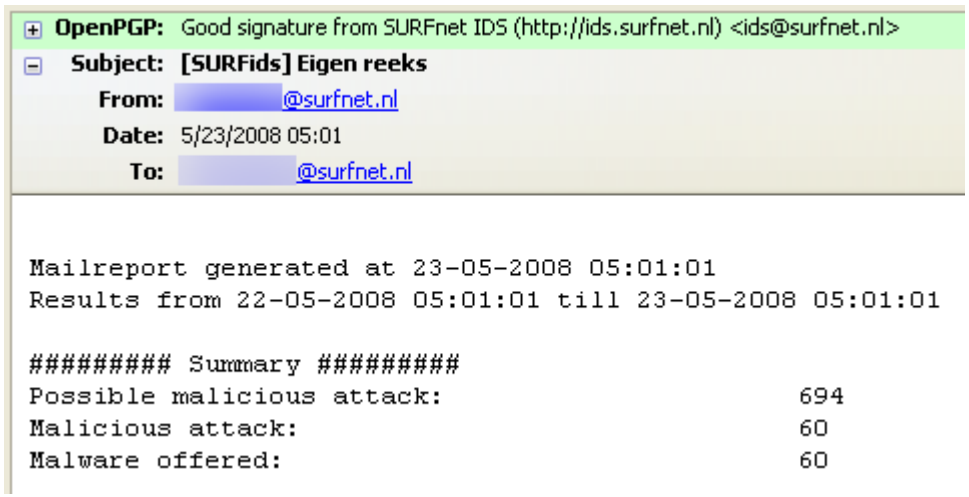
Actions

- Add Report
- Disable all reports
- Enable all reports
- Reset all timestamps

Reports of wimbie wimbie

Title	Last sent ▲	Template	Time options	Type	Status	Delete
Drempel sensor 85	17-11-2007 16:15	All attacks	Malicious attack > 20	Mail - Summary	Active	[Delete]
Drempel sensor 86	07-01-2008 03:00	All attacks	Malicious attack > 20	Mail - Summary	Active	[Delete]
Drempel sensor 232	22-05-2008 18:01	All attacks	Malicious attack > 20	Mail - Summary	Active	[Delete]
Daily status sensor 86	27-05-2008 05:01	Sensor status	Daily at 5:00	Mail - Summary + Detail	Active	[Delete]
Daily status sensor 85	29-05-2008 05:01	Sensor status	Daily at 5:00	Mail - Summary + Detail	Active	[Delete]
Own range	07-06-2008 05:01	Own ranges	Daily at 5:00	Mail - Summary + Detail	Active	[Delete]
Daily status sensor 232	20-06-2008 05:01	Sensor status	Daily at 5:00	Mail - Summary + Detail	Active	[Delete]
Daily Summary All Sensors	24-06-2008 06:01	All attacks	Daily at 6:00	Mail - Summary + Detail	Active	[Delete]
All Attacks	24-06-2008 20:01	All attacks	Hourly	Mail - Summary + Detail	Active	[Delete]

My reports - mail



OpenPGP: Good signature from SURFnet IDS (http://ids.surfnet.nl) <ids@surfnet.nl>
Subject: [SURFids] Eigen reeks
From: [redacted]@surfnet.nl
Date: 5/23/2008 05:01
To: [redacted]@surfnet.nl

```
Mailreport generated at 23-05-2008 05:01:01
Results from 22-05-2008 05:01:01 till 23-05-2008 05:01:01

######### Summary #########
Possible malicious attack:                    694
Malicious attack:                             60
Malware offered:                              60
```

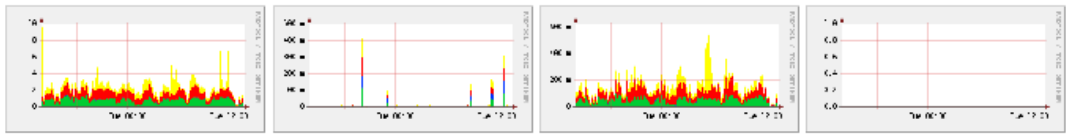
My reports - RSS

Reports of surfflow — surfflow

Title	Last sent ▲	Template	Time options	Type	Status	Delete
NfSen - Possible malicious attack	24-06-2008 20:41	All attacks	Hourly	RSS - Summary + Detail	Active	[Delete]
NfSen - Malicious attack	24-06-2008 20:41	All attacks	Hourly	RSS - Summary + Detail	Active	[Delete]
NfSen - Malware downloaded	24-06-2008 20:41	All attacks	Hourly	RSS - Summary + Detail	Active	[Delete]
NfSen - Malware offered	24-06-2008 20:41	All attacks	Hourly	RSS - Summary + Detail	Active	[Delete]

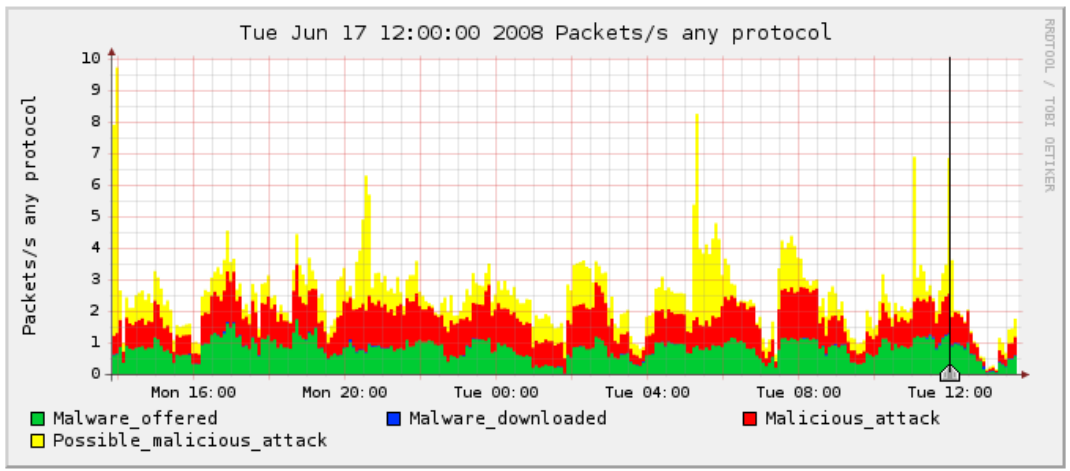
Netflow

TCP UDP ICMP other



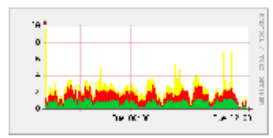
Profileinfo:

Type: continuous
Max: unlimited
Exp: never
Start: May 19 2008 - 13:10 CEST
End: Jun 17 2008 - 13:50 CEST

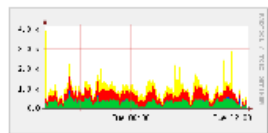


t_{start} 2008-06-17-12-00
t_{end} 2008-06-17-12-00

Flows



Traffic



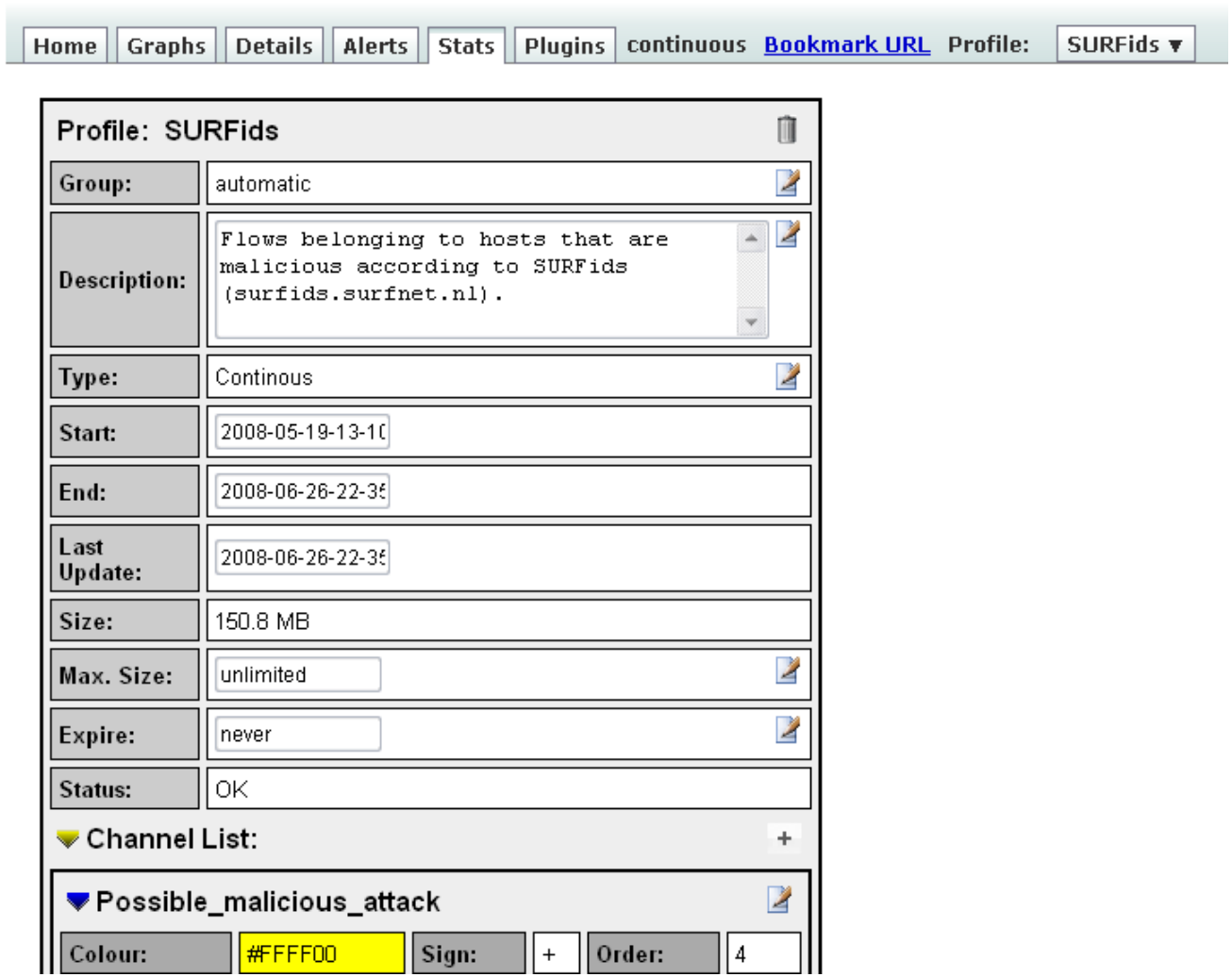
Select Single Timeslot Display: 1 day << < | ^ > >> >|

Lin Scale Stacked Graph
Log Scale Line Graph

Statistics timeslot Jun 17 2008 - 12:00

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
Possible_malicious_attack	4.2 /s	4.2 /s	0 /s	0.1 /s	0 /s	4.3 /s	4.2 /s	0 /s	0.1 /s	0 /s	1.9 kb/s	1.8 kb/s	0 b/s	37.3 b/s	0 b/s
Malicious_attack	1.2 /s	1.2 /s	0 /s	0.1 /s	0 /s	1.3 /s	1.2 /s	0 /s	0.1 /s	0 /s	492.4 b/s	459.5 b/s	0 b/s	32.9 b/s	0 b/s
Malware_downloaded	0.0 /s	0.0 /s	0 /s	0.0 /s	0 /s	0.0 /s	0.0 /s	0 /s	0.0 /s	0 /s	16.9 b/s	15.4 b/s	0 b/s	1.5 b/s	0 b/s
Malware_offered	1.2 /s	1.2 /s	0 /s	0.1 /s	0 /s	1.3 /s	1.2 /s	0 /s	0.1 /s	0 /s	492.4 b/s	459.5 b/s	0 b/s	32.9 b/s	0 b/s

Stats


Home
Graphs
Details
Alerts
Stats
Plugins
continuous
Bookmark URL
Profile:
SURFids ▾
Profile: SURFids
Group:
automatic
Description:
Flows belonging to hosts that are malicious according to SURFids (surfids.surfnet.nl).
Type:
Continous
Start:
2008-05-19-13-1(
End:
2008-06-26-22-3(
Last Update:
2008-06-26-22-3(
Size:
150.8 MB
Max. Size:
unlimited
Expire:
never
Status:
OK
Channel List:
Possible_malicious_attack
Colour:
#FFFF00
Sign:
+
Order:
4

Netflow processing

Statistics timeslot Jun 26 2008 - 08:00 - Jun 26 2008 - 20:00

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
Possible_malicious_attack	0.2 /s	0.1 /s	0.0 /s	0.0 /s	0 /s	0.2 /s	0.1 /s	0.0 /s	0.0 /s	0 /s	78.4 b/s	64.8 b/s	10.6 b/s	3.1 b/s	0 b/s
Malicious_attack	0.1 /s	0.1 /s	0.0 /s	0.0 /s	0 /s	0.2 /s	0.1 /s	0.0 /s	0.0 /s	0 /s	78.0 b/s	63.6 b/s	10.7 b/s	3.7 b/s	0 b/s
Malware_downloaded	0.0 /s	0.0 /s	0.0 /s	0.0 /s	0 /s	0.0 /s	0.0 /s	0.0 /s	0.0 /s	0 /s	13.7 b/s	4.8 b/s	8.6 b/s	0.3 b/s	0 b/s
Malware_offered	0.2 /s	0.1 /s	0.0 /s	0.0 /s	0 /s	0.2 /s	0.1 /s	0.0 /s	0.0 /s	0 /s	81.3 b/s	66.7 b/s	10.7 b/s	3.9 b/s	0 b/s

All None Display: Sum Rate

Netflow Processing

Source:

Possible_malicious_attack
Malicious_attack
Malware_downloaded
Malware_offered

All Sources

Filter:

and none

Options:

List Flows Stat TopN

Top: 10

Stat: Any IP Address order by flows

Limit: Packets > 0 -

Output: / IPv6 long

Clear Form process

Possible malicious attack

Top 10 Dst Port ordered by flows:

Proto	Dst Port	Flows	Packets	Bytes	pps	bps	bpp
any	2967	3105	3123	170053	0	0	54
any	135	1043	1052	61872	0	0	58
any	80	894	900	43362	0	0	48
any	445	875	882	46198	0	9	52
any	781	132	136	7616	0	0	56
any	0	77	83	4660	0	0	56
any	69	49	122	3955	0	0	32
any	2816	37	39	2184	0	0	56
any	769	34	34	1904	0	0	56
any	25	17	19	1163	0	0	61

Summary: total flows: 6604, total bytes: 426447, total packets: 6790

Malicious attack

Top 10 Dst Port ordered by flows:

Proto	Dst Port	Flows	Packets	Bytes	pps	bps	bpp
any	2967	2816	2831	154619	0	30	54
any	135	1535	1545	90772	0	0	58
any	445	1461	1470	75472	0	14	51
any	781	185	192	10752	0	0	56
any	0	89	91	5155	0	0	56
any	69	49	122	3955	0	0	32
any	2816	39	40	2240	0	0	56
any	769	35	35	1960	0	0	56
any	25	17	19	1163	0	0	61
any	139	12	12	688	0	0	57

Summary: total flows: 6483, total bytes: 424024, total packets: 6659

Malware offered

Top 10 Dst Port ordered by flows:

Proto	Dst Port	Flows	Packets	Bytes	pps	bps	bpp
any	2967	3118	3135	172859	0	34	55
any	135	1522	1531	89924	0	0	58
any	445	1451	1460	74904	0	14	51
any	781	196	203	11368	0	0	56
any	0	90	92	5211	0	0	56
any	69	49	122	3955	0	0	32
any	2816	41	42	2352	0	0	56
any	769	38	38	2128	0	0	56
any	25	17	19	1163	0	0	61
any	139	12	12	688	0	0	57

Summary: total flows: 6784, total bytes: 441996, total packets: 6961

Malware downloaded

Top 10 Dst Port ordered by flows:

Proto	Dst Port	Flows	Packets	Bytes	pps	bps	bpp
any	135	290	294	17544	0	0	59
any	445	49	49	3024	0	0	61
any	69	29	90	2880	0	0	32
any	781	15	15	840	0	0	56
any	25	13	15	959	0	12	63
any	33613	7	9	4896	0	275	544
any	0	7	7	459	0	0	65
any	33601	5	9	4896	0	368	544
any	33594	3	3	1632	0	420	544
any	33599	3	4	2176	0	52	544

Summary: total flows: 471, total bytes: 74361, total packets: 589

Developments

- Redesigned webinterface
- Improved email reporting
- RSS reports
- Multiple honeypot
- Argos integration
- Layer 2 detection
  - ARP poisoning attack detection
  - Rogue DHCP server detection
- IP exclusions
- CWSandbox support

[02-11-07] SURFids VMware demo

We have released a demo VMware image which is basically a debian vmware image with the SURFids 2.0-rc2 installed and configured on it. This will enable you to take a look at a working SURFids system within a few minutes of work. This image can become a sensor as well as the server, meaning it can detect just like a sensor would with just it's local network interface.

ARP

Actions for sensor232

The ARP module is enabled

ARP Module configuration AS1103.NET

MAC address ▲	IP address	Type	Sensor	Action
00:06:d6:cc:60:39			sensor232	[delete] [Del router] [Add DHCP]
00:15:c5:ea:a3:a7		DHCP	sensor232	[delete] [Add router] [Del DHCP]
00:19:56:ee:b1:c9			sensor232	[delete] [Del router] [Add DHCP]
		☐ Router/Gateway ☐ DHCP Server ☐ Server ☐ Host	sensor232	Add

Detected Protocols

Detected Protocols

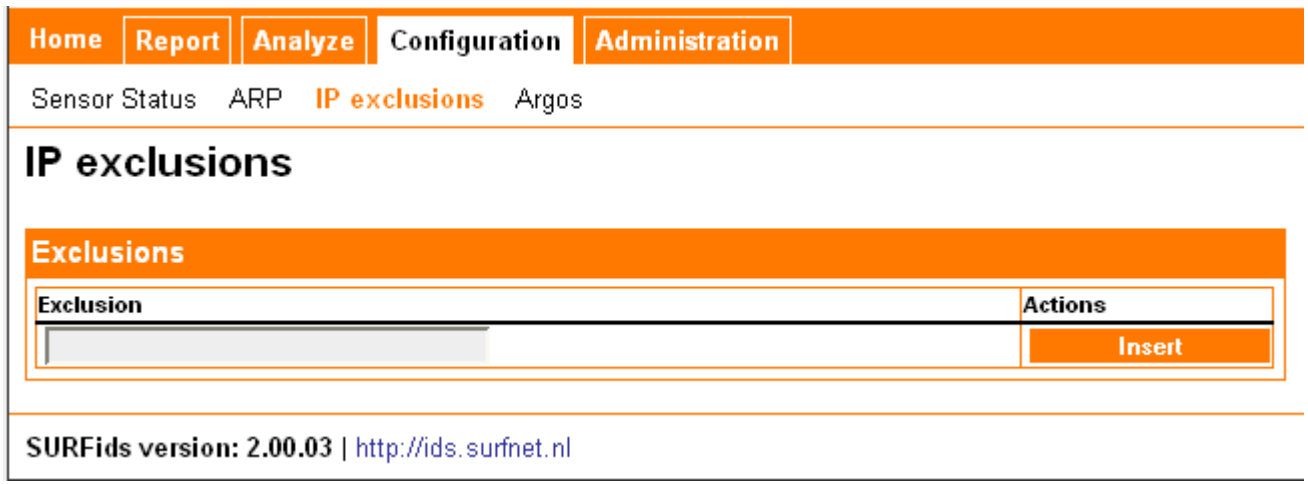
Actions

Clear Detected Protocols

Detected protocols PRUTSNET

Parent Protocol	Type Number	Type
Ethernet	50	Unknown
Ethernet	2048	Internet IP (IPv4)
Ethernet	2054	ARP
Ethernet	24578	DEC MOP Remote Console
Internet IP (IPv4)	1	ICMP
Internet IP (IPv4)	6	TCP
Internet IP (IPv4)	17	UDP
ICMP	0	Echo Reply
DHCP	8	DHCPINFORM

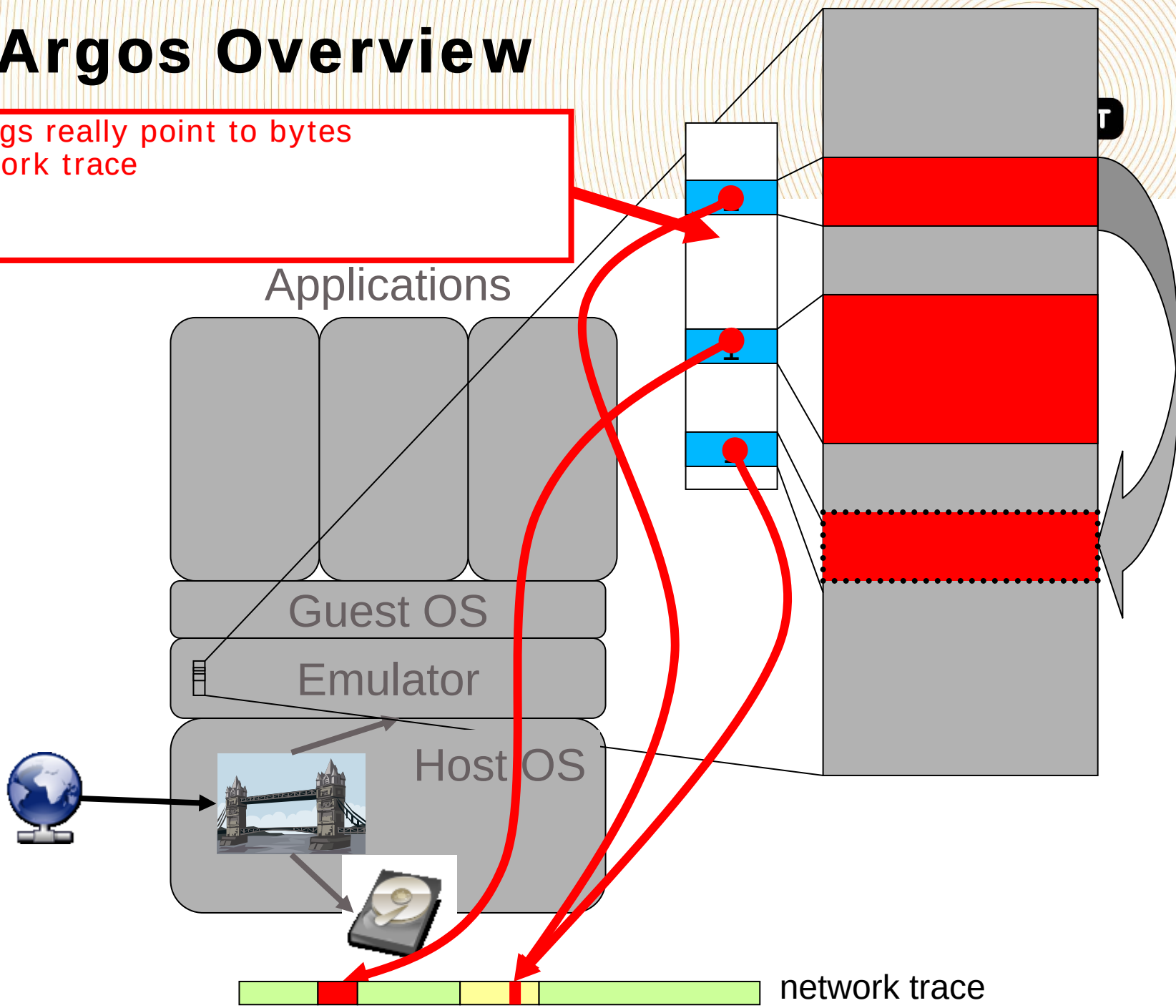
IP exclusion



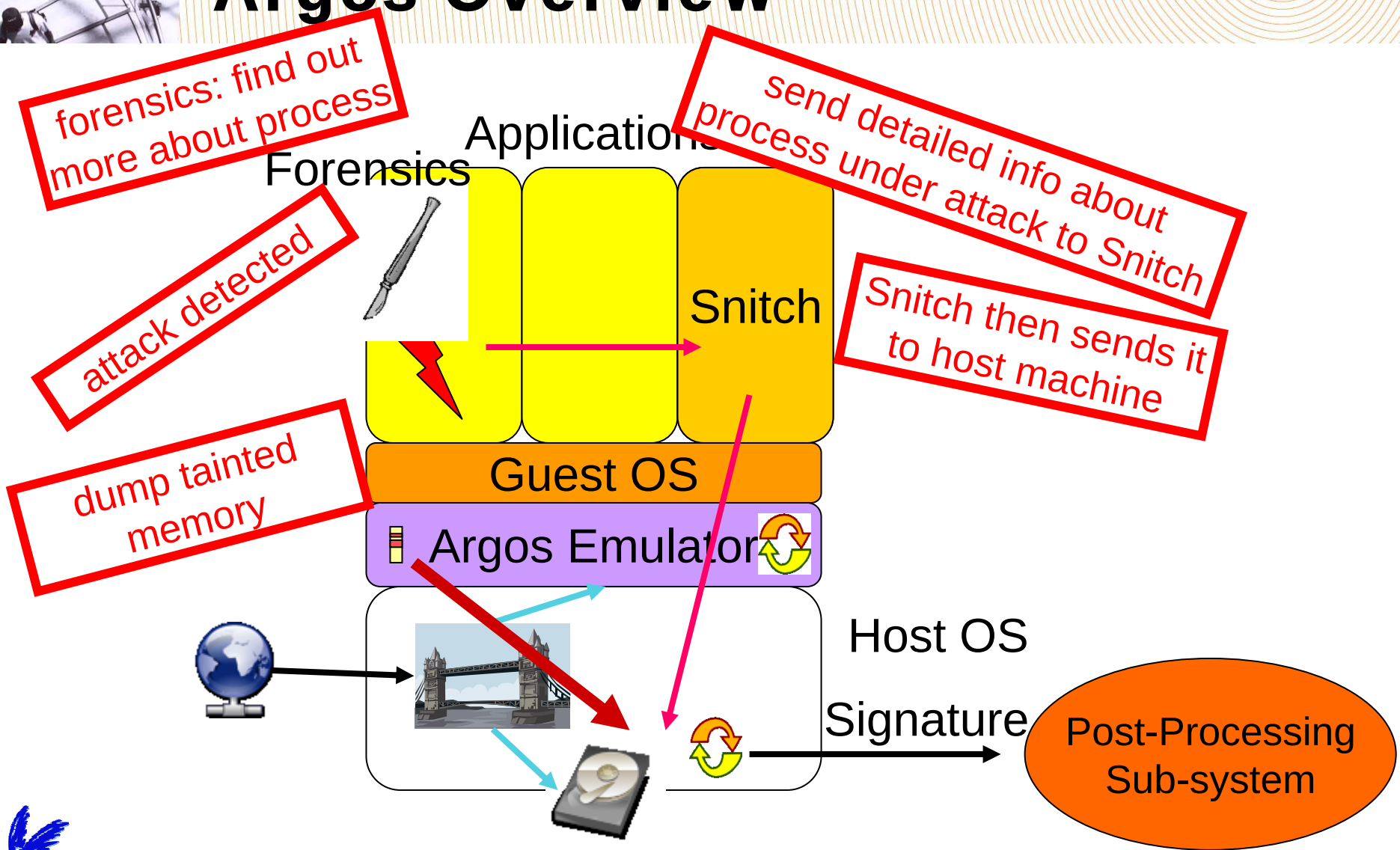
Argos Overview

Argos Overview

taint tags really point to bytes
in network trace



Argos Overview



Argos

Argos

Sensor redirects

Sensor [?]	Device IP [?]	Imagename [?]	Template [?]	Timespan [?]		
AS1103.NET	192	Windows 2000	All Traffic	Last 24 hour	Update	Delete
WIMBIEnet	192	Windows XP SP2	All Traffic	Last 24 hour	Update	Delete
WIMBIEnet		Windows XP SP2	All Traffic	Last 24 hour	Add	

Results (page 1: 1 - 1 of 1)

◀ 1 ▶ All

Timestamp ▲	Severity	Source	Port	Destination	Port	Sensor	Additional Info
24-06-2008 19:38:39	Malicious attack - Argos	91.171	1620	192	135	AS1103.NET	svchost.exe

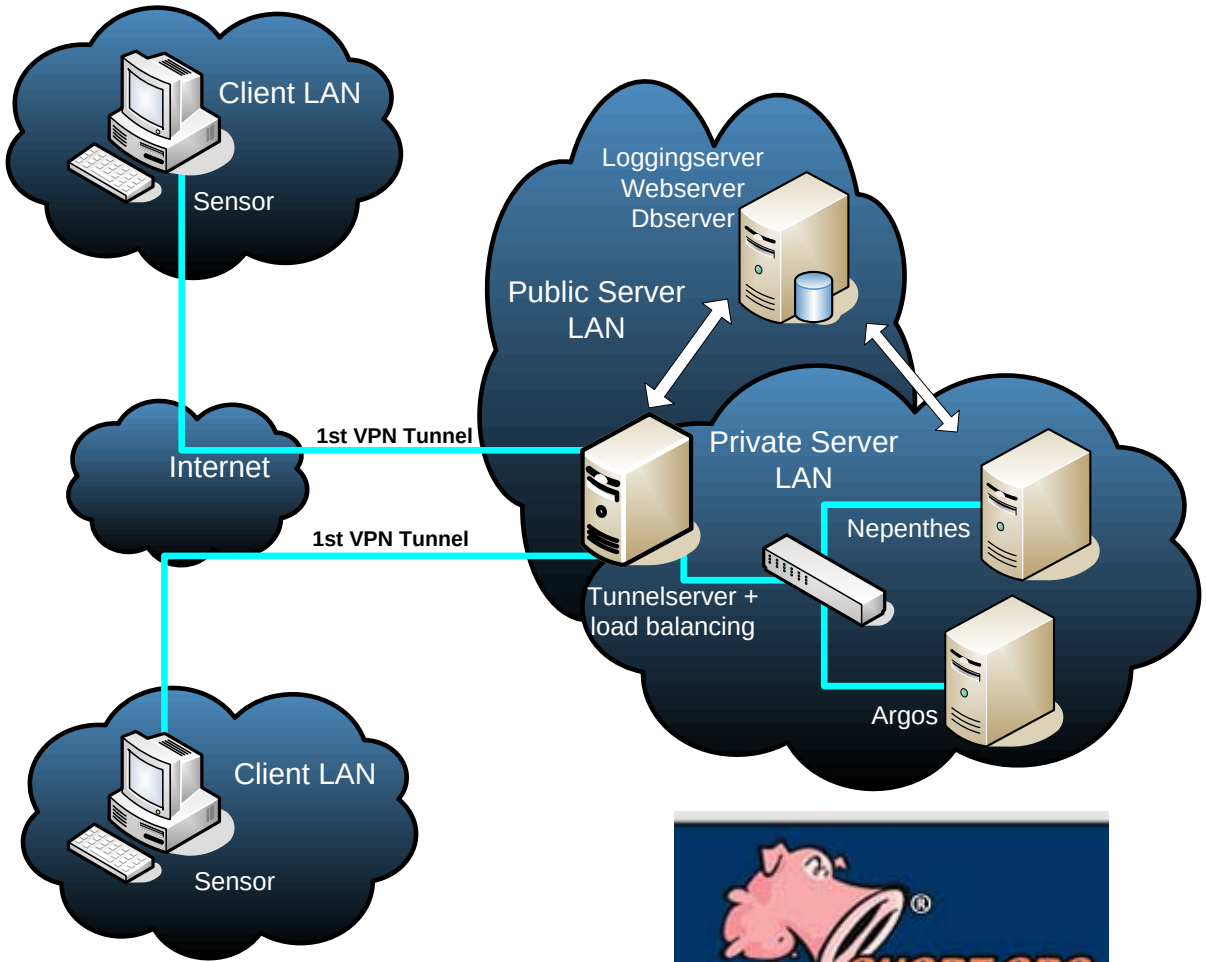
Attack detail

Details of attack ID: 1671266	
Type	**Info**
Argos ID	1116062997
Process ID	384
OS	win2k
Imagename	win2k-configured-clean.img
Module	svchost.exe
TCP Port	135
TCP Port	4514
TCP Port	8721
TCP Port	4729
TCP Port	1027
UDP Port	135

Snort

- Added value
- Placement
- Integration

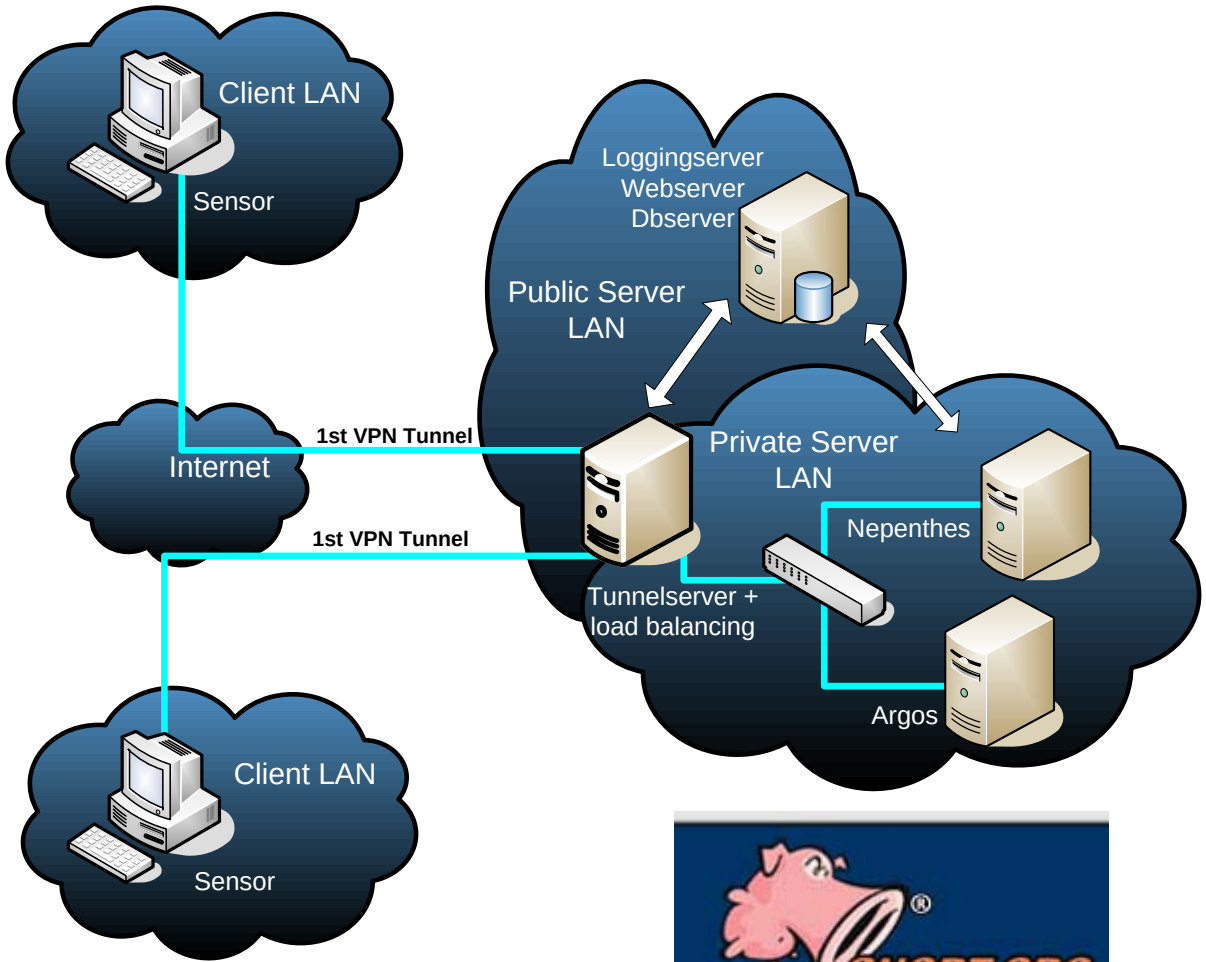
Snort before Argos



Results

- Over 90% of the attacks registered by Argos were detected by Snort
- Other attacks also recognized

Snort on tunnel server



Results

- Over 90% of the attacks registered by Nepenthes were detected by Snort
- Identification of 10% of the possible malicious attacks

Recent issues

[16-05-08] OpenSSL vulnerability in Debian

The recent OpenSSL vulnerability in Debian has a rather high impact on the SURFids system. This basically means recreating all the certificates used by the SURFids system. A document explaining how to do this for a live SURFids environment can be found here.

Version

[29-11-07] SURFids 2.00 stable released

The day is finally here, SURFids 2.00 has been released as a stable version. Visit our Subversion page for information on how to get the SURFids 2.00 stable release.
In the (unlikely) event that you find a bug, please report this in our Trac environment located here.

[13-12-07] SURFids 2.00.01 stable released

This stable release includes 3 critical bug fixes:

- Fixed an XSS & SQL injection vulnerability.
- Fixed a bug in the redirect argos script.
- Fixed a bug with sensor certificate generation.

[05-03-08] SURFids 2.00.02 stable released

SURFids 2.00.02 stable has been released. This release contains several bugfixes to the webinterface as well as some bugfixes to a few tunnel scripts. For a more detailed list of bugfixes: Trac

Future goals

- Correlation
  - Data between the different (honey) projects.
  - Data provided by other teams!
- HoneyClients
  - Build a network of honey-clients
    - Catch 0-Day attacks on IE and other browsers
    - Watch for active exploitation of known and new client-side vulnerabilities
  - Honey-clients are fed with URL's from SPAM and other sources

Conclusion

- SURFids
  - Successful solution
  - Very easy to deploy
  - Actively developed