

SNORT IDS para todos os níveis

Rodrigo Montoro
aka
Sp0oKeR

Analista Segurança BRconnection



EU

- Analista Segurança BRconnection
- Certificados
 - RHCE (Redhat Certified Engineer)
 - LPI Nível I
 - SnortCP (Snort Certified Professional)
- Participante
 - snort-br , slackware-br , ISSA Brasil , Owasp-
BR ... etc



Agenda

- Empresa
- O que é um NIDS ?
- Tipos de Ataques
- Entendendo o Snort IDS
 - Funcionamento
 - Arquivos Configurações
- Ferramentas Auxiliares
 - IDS Policy Manager
 - BASE
 - Posicionamentos IDS



Empresa

- BRconnection
- BRMA (UTM)
- messengerPOLICY
- Parceira SourceFire (VRT Rules Integrator)



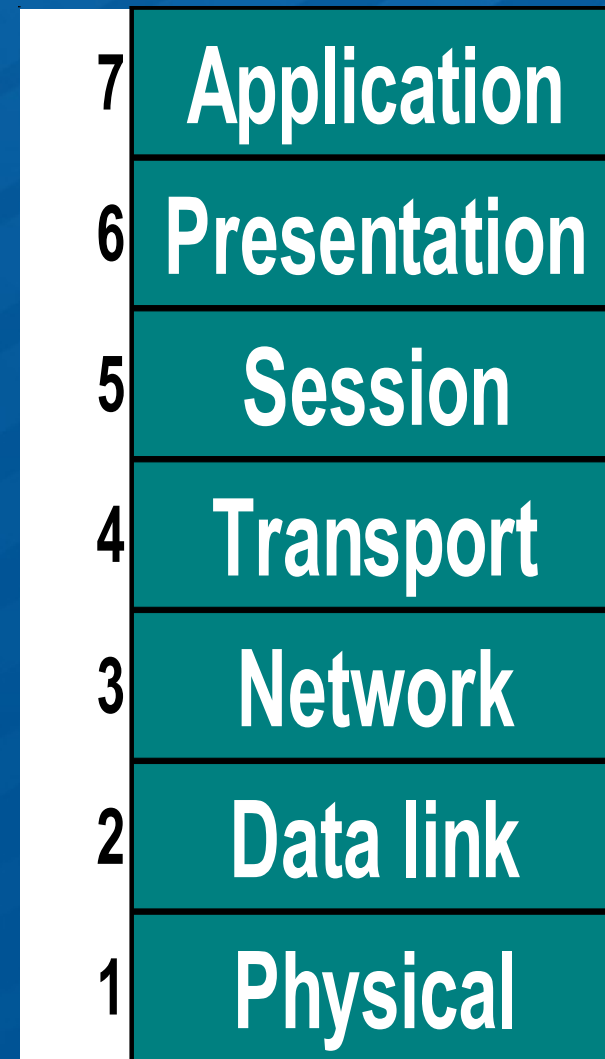
Necessidades de Segurança

- Funcionários Internos
- Worms
- Phishing
- Trojans
- Engenharia Social
- Vulnerabilidades



O que é um NIDS ?

- Sistema Detecção de Intrusos
- Analisa até camada 7 modelo OSI
- Apenas Monitoramento
- Pode tomar ações (NIPS)
- Tipos
 - Assinaturas
 - Comportamental



Tipos de Ataques

- Estrutturados
- Desestrutturados
- Internos
- Externos



Estruturados



Desestructurados



Motivadores

- Curiosidade
- Afirmação / Reconhecimento (Modificar Site)
- Roubo de Dados
- Derrubar serviços (DoS)
- Espionagem Industrial
- Outros Fins
 - Ataques DDoS
 - Hospedagem diversas
 - Ataques “jumpeados”



Somente o firewall é suficiente ?



Entendendo o Snort IDS

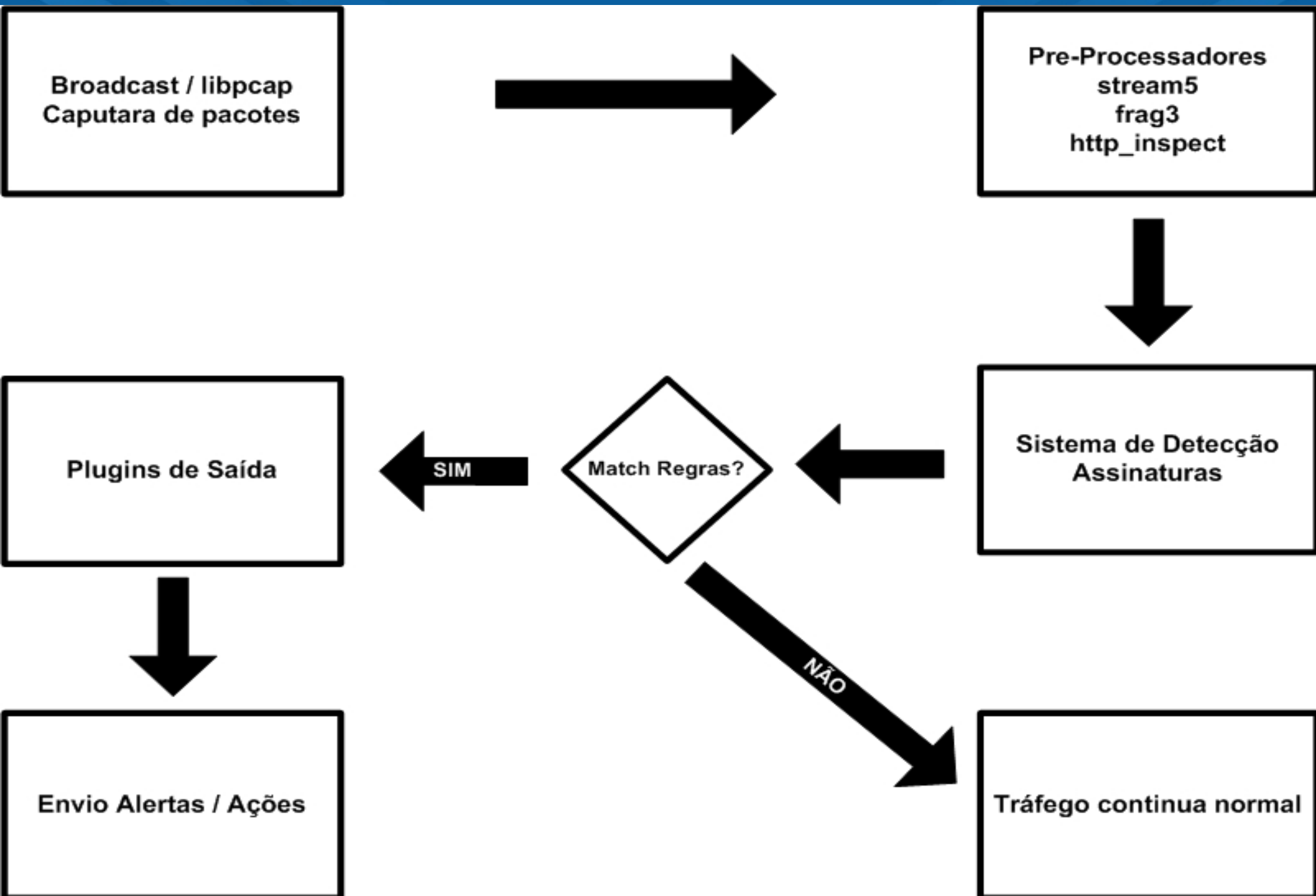


Pequena história Snort

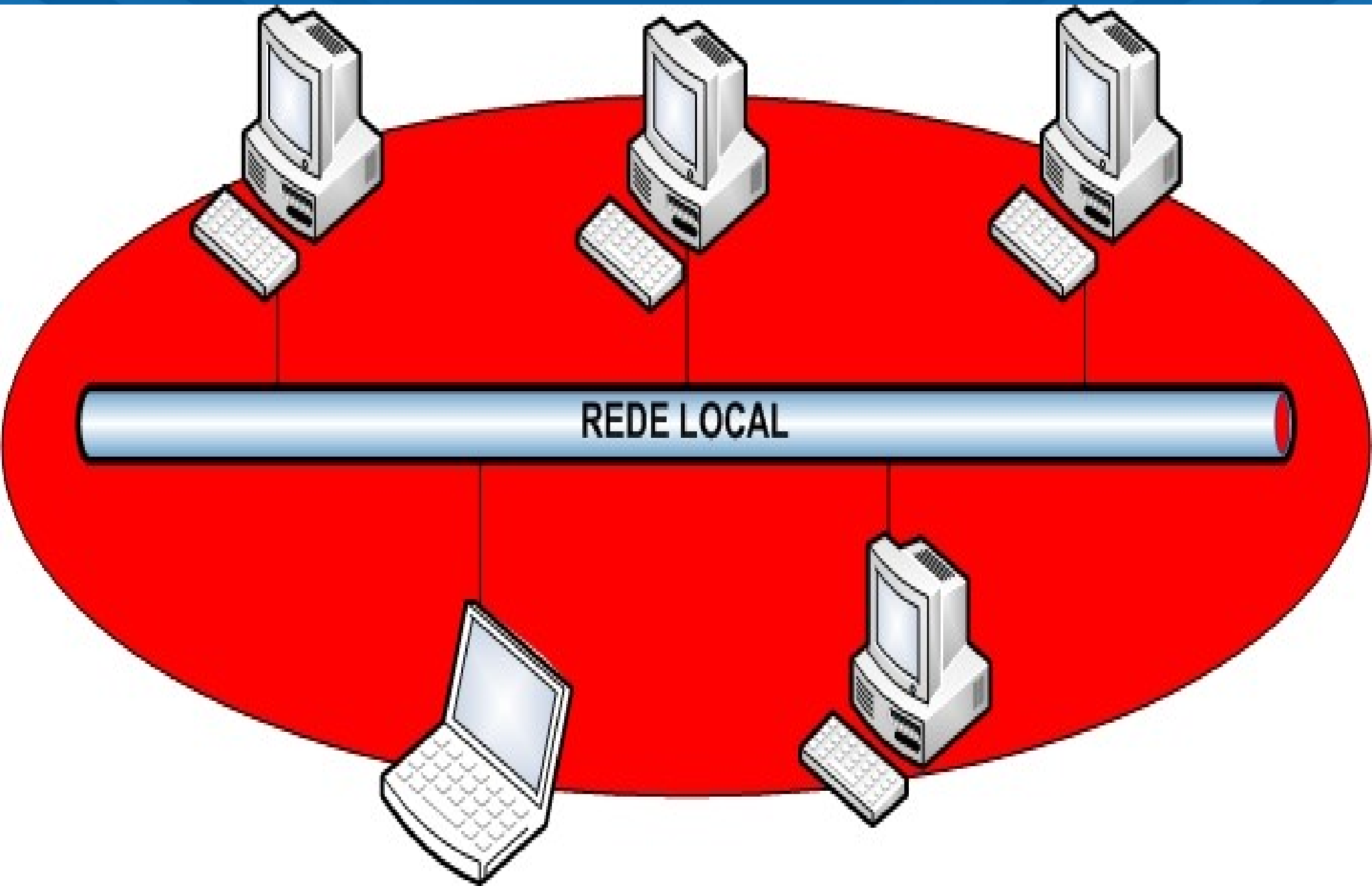
- Motivação (Marty Roesch)
 - Necessidade Específica
 - Falta de opções
- Quando
 - Iniciado em 1998 (Somente Sniffer)
 - Intrusion Detection System - 1999
 - Aproximadamente 1600 linhas de código
 - Versão Atual 2.8.0 (Suporte ipv6)



Fluxo Snort



Broadcast / Decoder



Pré - Processadores

- stream5
 - Policy
- http_inspect
 - Profiles (Apache / IIS)
- spp_dns
- spp_ssh
- spp_skype



Pré – Processadores (2)

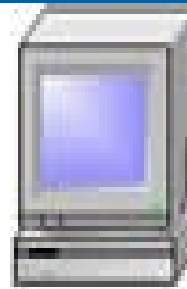
- frag3
 - Policy
- spp_telnet/ftp
- spp_smtp
- PerfMonitor
- sfportscan



Evasion Pacotes Fragmentados



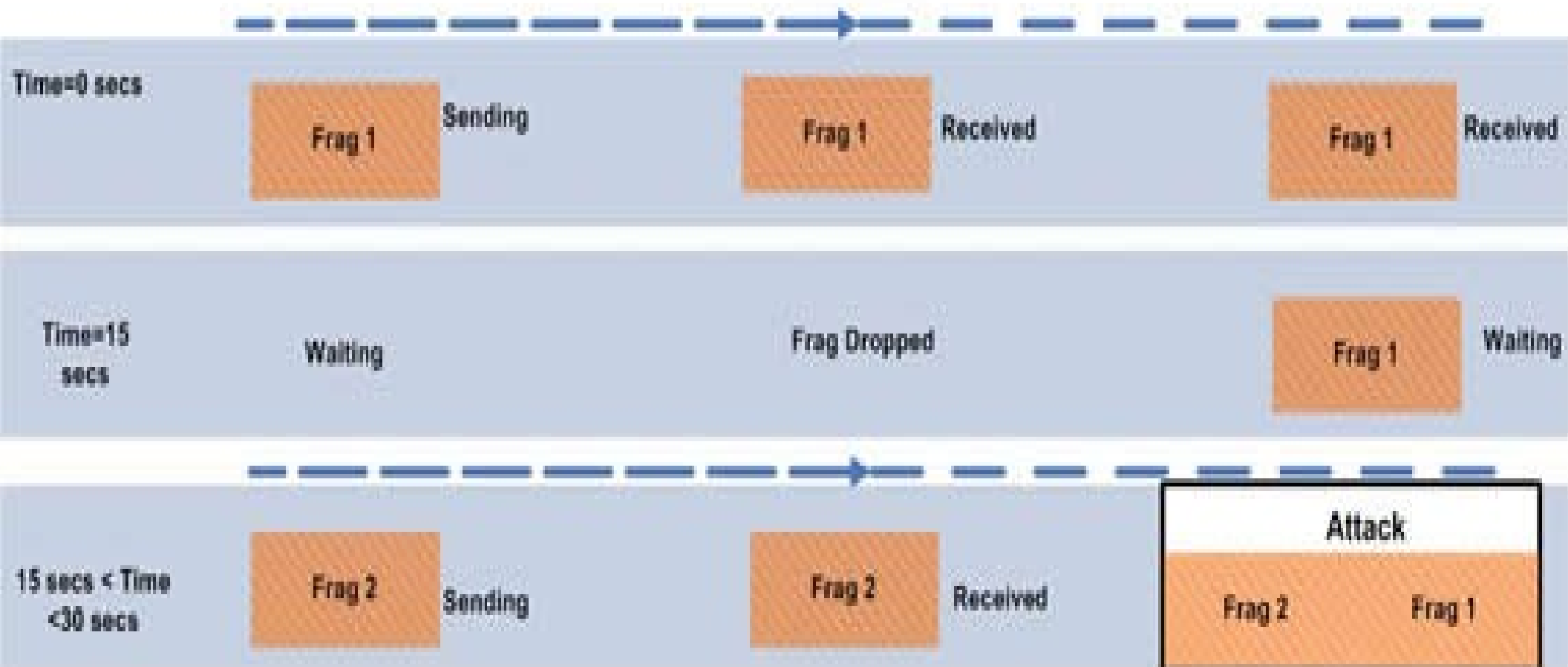
Attacker



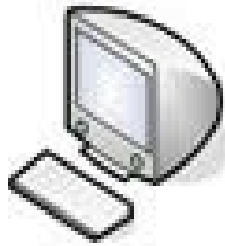
NIDS
Frag_timeout=15 secs



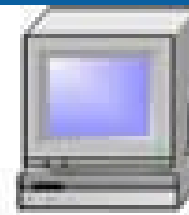
Victim
Frag_timeout=30 sec



Evasion Pacotes Fragmentados (2)



Attacker



NIDS
Frag_timeout = 60 secs



Victim
Frag_timeout = 30 sec



Time = 0 secs



Time = 30 secs

Waiting



Fragments
Dropped

False Reassembly

30 secs < T < 60 secs



30 secs < T < 60 secs



ATTACK

http_inspect

→ / = %2f

→ .. = %2e%2e

→ \ = %5c

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS  
(msg:"WEB-ATTACKS ping command attempt"; flow:to_server,established;  
content:"/bin/ping";nocase; sid:1359; classtype:web-application-attack; rev:4;)
```

Se não tivesse o pre-processador normalizando o tráfego, usando

%2fbin%2fping

Iria fazer o evasion no IDS



Plugins de Saída

- Syslog
- Banco de Dados
 - MySQL
 - PostgreSQL
- Formato tcpdump
- snortsam
- Outros ...



Arquivos Configurações

- snort.conf
- threshold.conf
- /etc/snort/rules



Programas Auxiliares



IDS Policy Manager

- Versão atual 2.2 (01 Novembro 2007)
- Interface Gráfica para gerenciar regras snort e arquivos de configurações.
- Adiciona novas regras snort para as regras snort existentes.
- Fácil edição regras snort.
- Update das regras via web.
- Fácil gerenciar multiplos sensores com diferentes políticas.



IDS Policy Manager (2)

- Upload dos arquivos de política do snort via SFTP, FTP, cópia de arquivos.
- Completo suporte para Snort® 2.8.
- Uso de conjunto de regras do BleedingSnort e/ou regras comunidade Snort (VRT após 30 dias).
- Fácil para aprender detalhes sobre as assinaturas.
- Reiniciar sensores após upload .
- É Free !!!!



IDS Policy Manager

Snort Policies

Conisli

Rule Groups

- attack-responses(17)
- backdoor(713)
- bad-traffic(13)
- chat(34)
- content-replace(0)
- ddos(32)
- decoder(0)
- dns(25)
- dos(32)
- experimental(0)
- exploit(194)
- finger(14)
- ftp(82)
- icmp(22)
- icmp-info(93)
- imap(69)
- info(8)
- local(0)
- misc(69)
- multimedia(10)
- mysql(14)
- netbios(5311)
- nntp(13)
- oracle(321)
- other-ids(3)
- p2p(26)
- policy(62)
- pop2(4)
- pop3(36)
- porn(27)
- preprocessor(0)
- rpc(149)
- rservices(13)
- scan(21)
- shellcode(31)
- smtp(90)

Drag a column header here to group by that column.

Enabled	Name	Directory	Last Modified	Description
True	content-replace	\$RULE_PATH	11/03 11:11:43	
True	ddos	\$RULE_PATH	09/30 23:34:55	
False	decoder	\$PREPROC_RULE_PATH	09/28 21:14:13	
True	dns	\$RULE_PATH	09/30 23:34:55	
True	dos	\$RULE_PATH	09/30 23:34:55	
True	experimental	\$RULE_PATH	09/28 21:14:13	
True	exploit	\$RULE_PATH	09/30 23:34:55	
True	finger	\$RULE_PATH	09/30 23:34:55	
True	ftp	\$RULE_PATH	09/30 23:34:55	
True	icmp	\$RULE_PATH	09/30 23:34:55	
False	icmp-info	\$RULE_PATH	09/30 23:34:55	
True	imap	\$RULE_PATH	09/30 23:34:55	
False	info	\$RULE_PATH	09/30 23:34:55	
True	local	\$RULE_PATH	09/28 21:14:13	
True	misc	\$RULE_PATH	09/30 23:34:55	
False	multimedia	\$RULE_PATH	09/30 23:34:55	
True	mysql	\$RULE_PATH	09/30 23:34:55	
True	netbios	\$RULE_PATH	09/30 23:34:55	
True	nntp	\$RULE_PATH	09/30 23:34:55	
True	oracle	\$RULE_PATH	09/30 23:34:55	
True	other-ids	\$RULE_PATH	09/30 23:34:55	
False	p2p	\$RULE_PATH	09/30 23:34:55	
False	policy	\$RULE_PATH	09/30 23:34:55	
True	pop2	\$RULE_PATH	09/30 23:34:55	
True	pop3	\$RULE_PATH	09/30 23:34:55	
False	porn	\$RULE_PATH	09/30 23:34:55	
False	preprocessor	\$PREPROC_RULE_PATH	09/28 21:14:13	
True	rpc	\$RULE_PATH	09/30 23:34:55	

Rule - WEB-IIS cmd32.exe access

Name

Group

Enabled Signature ID Revision

- Settings**
- Raw Editor
- Suppression
- Threshold
- Web References

Action	Protocol	Classification	Priority	
<input type="text" value="alert"/>	<input type="text" value="tcp"/>	<input type="text" value="web-application-attack"/>	<input type="text" value="1"/>	
Source IP/Mask	Source Port	Direction	Destination IP/Mask	Destination Port
<input type="text" value="\$EXTERNAL_NET"/>	<input type="text" value="any"/>	<input type="text" value="->"/>	<input type="text" value="\$HTTP_SERVERS"/>	<input type="text" value="\$HTTP_PORTS"/>

Rule Options

References

Type	Value
------	-------

IDS Policy Manager



- Snort Policies
 - Conisli
 - Rule Groups
 - Classifications
 - Variables
 - Port Variables
 - Custom Rule Types
 - Preprocessors
 - Output Modules
 - Thresholds
 - Suppressions
 - Config Options
 - wan
 - Snort Sensors

Drag a column header here to group by that column.

Enabled ▾	Name ▾	Value ▾
True	HTTP_PORTS	[80,2301,3128,8000,8080,8180,8888]
True	SHELLCODE_PORTS	!80
True	ORACLE_PORTS	1521
True	AUTH_PORTS	113
True	DNS_PORTS	53
True	FINGER_PORTS	79
True	FTP_PORTS	21
True	IMAP_PORTS	143
True	IRC_PORTS	[6665,6666,6667,6668,6669,7000]
True	MSSQL_PORTS	1433
True	NNTP_PORTS	119
True	POP2_PORTS	109
True	POP3_PORTS	110
True	SUNRPC_PORTS	[111,32770,32771,32772,32773,32774,32775,32776,32777,32778,32779]
True	RLOGIN_PORTS	513
True	RSH_PORTS	514
True	SMB_PORTS	[139,445]
True	SMTP_PORTS	25
True	SNMP_PORTS	161
True	SSH_PORTS	22
True	TELNET_PORTS	23
True	MAIL_PORTS	[25,143,465,691]
True	SSL_PORTS	[25,443,465,636,993,995]

IDS Policy Manager

- Snort Policies
 - Conisli Update Polides
 - Rule Groups
 - Classifications
 - Variables
 - Port Variables
 - Custom Rule Types
 - Preprocessors
 - Output Modules
 - Thresholds
 - Suppressions
 - Config Options
- wan
- Snort Sensors

Drag a column header here to group by that column.

Enabled	Name	Value
<input type="radio"/>	stream4	disable_evasion_alerts
<input type="radio"/>	stream4_reassemble	
<input checked="" type="radio"/>	stream5_global	max_tcp 8192, track_tcp yes, track_udp no
<input checked="" type="radio"/>	stream5_tcp	policy first, use_static_footprint_sizes
<input type="radio"/>	stream5_udp	ignore_any_rules
<input type="radio"/>	perfmonitor	time 300 file /var/snort/snort.stats pktcnt 10000
<input checked="" type="radio"/>	http_inspect	global iis_unicode_map unicode.map 1252
<input checked="" type="radio"/>	http_inspect_server	server default profile all ports { 80 8080 8180 } oversize_dir_length 500
<input type="radio"/>	http_inspect_server	server 1.1.1.1 ports { 80 3128 8080 } \
<input checked="" type="radio"/>	rpc_decode	111 32771
<input type="radio"/>	bo	noalert { client server general snort_attack } drop { client server general snort_attack }
<input type="radio"/>	bo	noalert { general server } drop { snort_attack }
<input checked="" type="radio"/>	bo	
<input type="radio"/>	telnet_decode	
<input type="radio"/>	dynamicpreprocessor	file <full path to libsf_ftptelnet_preproc.so>
<input checked="" type="radio"/>	ftp_telnet	global encrypted_traffic yes inspection_type stateful
<input checked="" type="radio"/>	ftp_telnet_protocol	telnet normalize ayt_attack_thresh 200
<input checked="" type="radio"/>	ftp_telnet_protocol	ftp server default def_max_param_len 100 alt_max_param_len 200 { CWD } cmd_validity MODE < char ASBCZ > cmd_validity MDTM < [date nnnnnnnnnnnn[n(n[n]]
<input checked="" type="radio"/>	ftp_telnet_protocol	ftp client default max_resp_len 256 bounce yes telnet_cmds yes
<input type="radio"/>	dynamicpreprocessor	file <full path to libsf_smtp_preproc.so>
<input checked="" type="radio"/>	smtp	ports { 25 587 691 } inspection_type stateful normalize_cmds normalize_cmds { EXPN VRFY RCPT } alt_max_command_line_len 260 { MAIL } alt_max_command_line_
<input checked="" type="radio"/>	sfportscan	proto { all } memcap { 10000000 } sense_level { low }
<input type="radio"/>	arp spoof	
<input type="radio"/>	arp spoof_detect_host	192.168.40.1 f0:0f:00:f0:0f:00
<input type="radio"/>	dynamicpreprocessor	file <full path to libsf_ssh_preproc.so>
<input type="radio"/>	ssh	server_ports { 22 } max_client_bytes 19600 \
<input type="radio"/>	dynamicpreprocessor	file <full path to libsf_dcerpc_preproc.so>
<input checked="" type="radio"/>	dcerpc	autodetect max_frag_size 3000 memcap 100000
<input type="radio"/>	dynamicpreprocessor	file <full path to libsf_dns_preproc.so>
<input checked="" type="radio"/>	dns	ports { 53 } enable_rdata_overflow

IDS Policy Manager

- Snort Policies
 - Conisli
 - Rule Groups
 - Classifications
 - Variables
 - Port Variables
 - Custom Rule Types
 - Preprocessors
 - Output Modules
 - Thresholds
 - Suppressions
 - Config Options
 - wan
 - Snort Sensors

Drag a column header here to group by that column.

Enabled	Name	Value
True	AIM_SERVERS	[64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9.0/24,205.188.153.0/24,205.188.179.0/24]
True	DNS_SERVERS	\$HOME_NET
True	EXTERNAL_NET	any
False	HOME_NET	10.1.1.0/24
False	HOME_NET	\$eth0_ADDRESS
True	HOME_NET	[10.1.1.0/24,192.168.1.0/24]
True	HTTP_SERVERS	\$HOME_NET
True	PREPROC_RULE_PATH	./preproc_rules
True	RULE_PATH	./rules
True	SMTP_SERVERS	\$EXTERNAL_NET
True	SNMP_SERVERS	\$HOME_NET
True	SQL_SERVERS	\$HOME_NET
True	TELNET_SERVERS	\$HOME_NET

BASE

(Basic Analysis and Security Engine)

É uma interface web para realizar análises das tentativas de invasões que o snort detectou.



Basic Analysis and Security Engine (BASE)

- Most recent Alerts: [any protocol](#), [TCP](#), [UDP](#), [ICMP](#)
- Today's: alerts [unique](#), [listing](#); IP [src](#) / [dst](#)
- Last 24 Hours: alerts [unique](#), [listing](#); IP [src](#) / [dst](#)
- Last 72 Hours: alerts [unique](#), [listing](#); IP [src](#) / [dst](#)
- Most [recent 15 Unique Alerts](#)
- Last Source Ports: [any](#), [TCP](#), [UDP](#)
- Last Destination Ports: [any](#), [TCP](#), [UDP](#)
- Most [frequent 5 Alerts](#)
- Most Frequent Source Ports: [any](#), [TCP](#), [UDP](#)
- Most Frequent Destination Ports: [any](#), [TCP](#), [UDP](#)
- Most frequent 15 addresses: [source](#), [destination](#)

Added 0 alert(s) to the Alert cache

Queried on : Thu October 14, 2004 22:02:36

Database: snort_log@localhost (schema version: 106)

Time window: [2004-09-02 16:05:49] - [2004-10-08 11:25:41]

[Search](#)

[Graph Alert data](#)

Graph alert [detection time](#)

Sensors: 1

Unique Alerts: 14

categories:5

Total Number of Alerts: 84

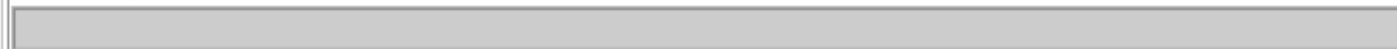
- Src IP addr: 5
- Dest. IP addr: 9
- Unique IP links 13
- Source Ports: 68
 - TCP (68) UDP (0)
- Dest. Ports: 12
 - TCP (12) UDP (0)

Traffic Profile by Protocol

TCP (96%)



UDP (0%)



ICMP (4%)



Portscan Traffic (0%)



[Alert Group Maintenance](#) | [Cache & Status](#) | [Administration](#)

BASE 0.9.7.2 (by [Kevin Johnson](#) and the BASE Project Team

Built on ACID by [Roman Danyliw](#))

[Loaded in 0 seconds]

Basic Analysis and Security Engine (BASE)

[Home](#) | [Search](#) | [AG Maintenance](#)

[[Back](#)]

Added 0 alert(s) to the Alert cache

Queried DB on : Thu October 14, 2004 22:04:44

Meta Criteria	<i>any</i>
IP Criteria	<i>any</i>
TCP Criteria	<i>any</i>
Payload Criteria	<i>any</i>

Summary Statistics

- **Sensors**
- **Unique Alerts** ([classifications](#))
- Unique addresses: [source](#) | [destination](#)
- **Unique IP links**
- **Source Port:** [TCP](#) | [UDP](#)
- **Destination Port:** [TCP](#) | [UDP](#)
- **Time profile** of alerts

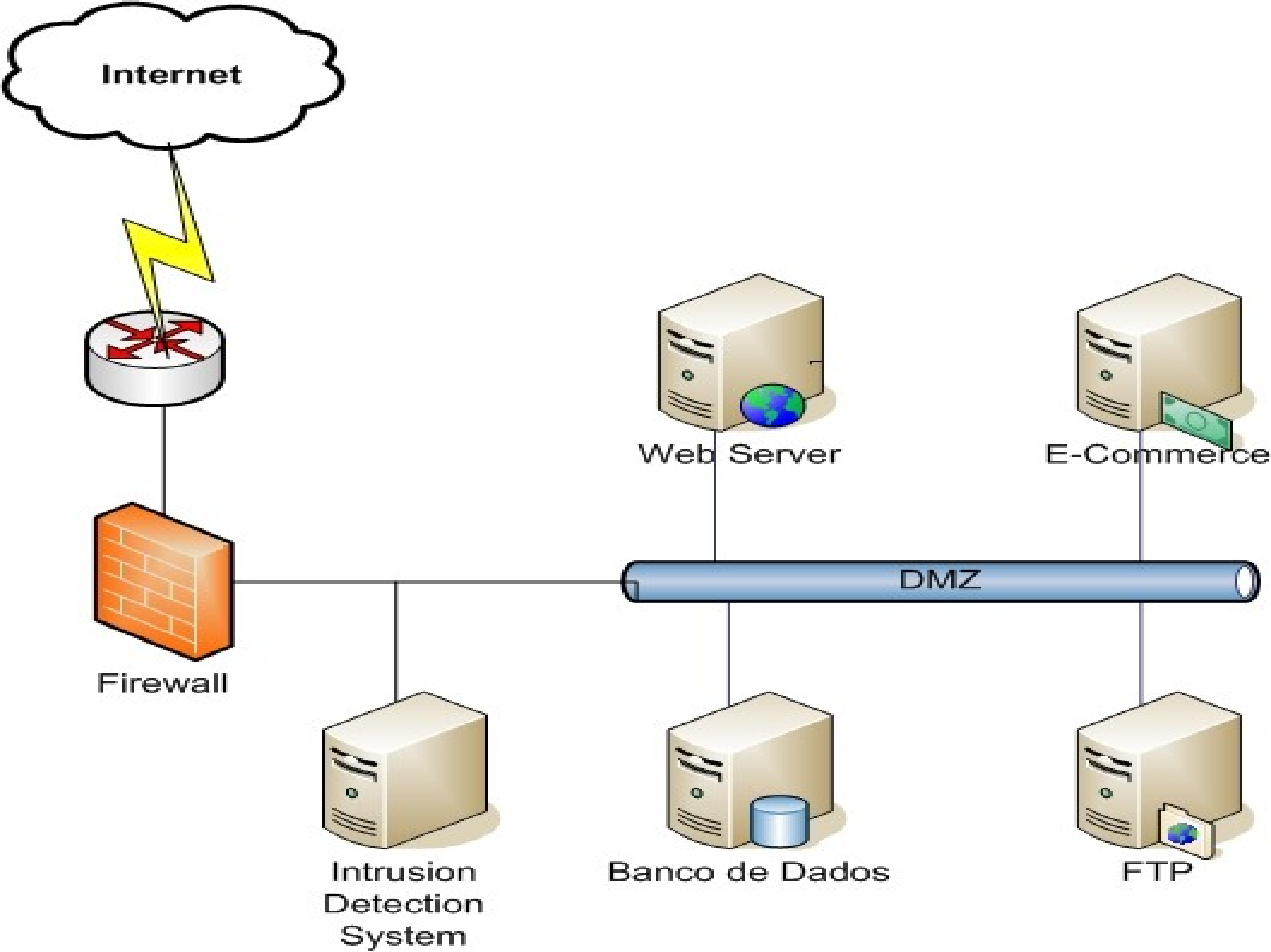
Displaying alerts 1-50 of 81 total

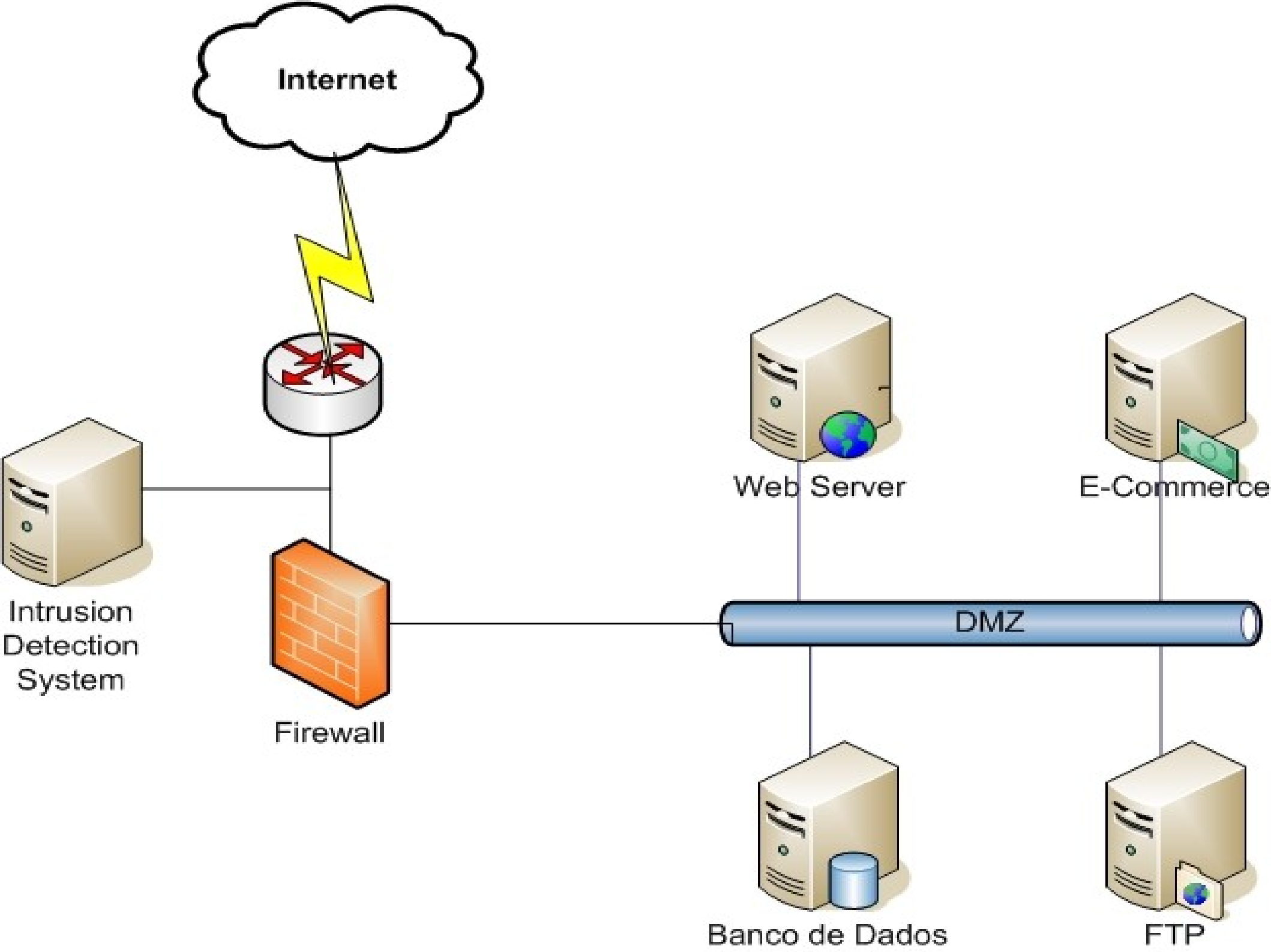
<input type="checkbox"/>	ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
<input type="checkbox"/>	#0-(1-84)	[snort] NETBIOS SMB IPC\$ share unicode access	2004-10-08 11:25:41	192.168.1.100 :1613	192.168.1.4 :139	TCP
<input type="checkbox"/>	#1-(1-83)	[snort] NETBIOS SMB IPC\$ share unicode access	2004-10-08 11:25:31	192.168.1.100 :1608	192.168.1.4 :139	TCP
<input type="checkbox"/>	#2-(1-82)	[snort] NETBIOS SMB IPC\$ share unicode access	2004-10-08 11:25:05	192.168.1.100 :1601	192.168.1.4 :139	TCP
<input type="checkbox"/>	#3-(1-80)	[snort] (http_inspect) OVERSIZE CHUNK ENCODING	2004-10-04 22:25:41	192.168.1.4 :42164	67.19.245.228 :80	TCP
<input type="checkbox"/>	#4-(1-81)	[snort] (http_inspect) OVERSIZE CHUNK ENCODING	2004-10-04 22:25:41	192.168.1.4 :42163	67.19.245.228 :80	TCP

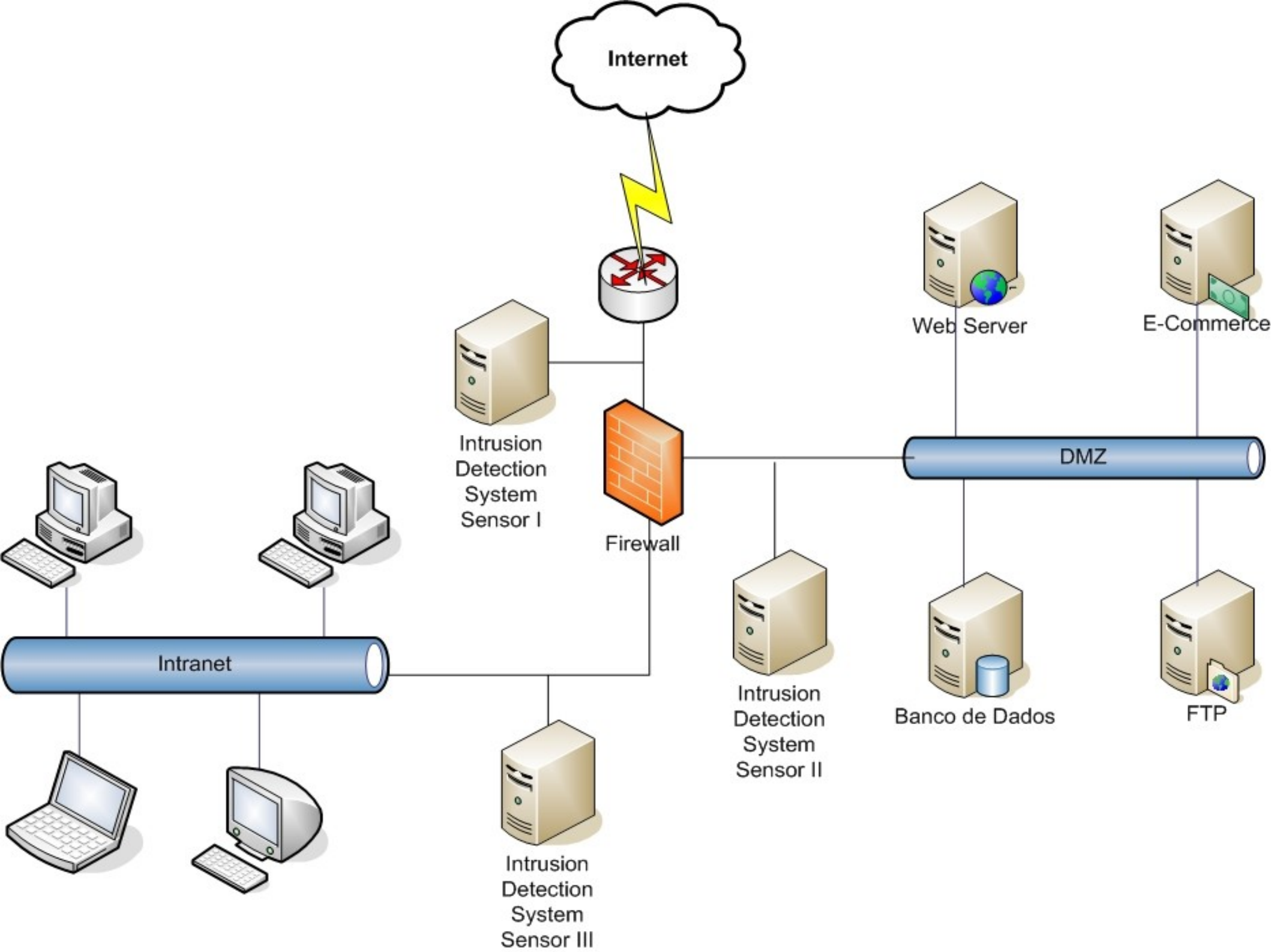
Posicionamento SNORT

- Lan
- DMZ
- Wan
- Combinado









Outras Ferramentas

- SnortSAM
- Sguil
- Barnyard



SGUIL

Sguil (pronounced sgweel) is built by network security analysts for network security analysts. Sguil's main component is an intuitive GUI that provides **access to realtime events, session data, and raw packet captures**. Sguil facilitates the practice of Network Security Monitoring and event driven analysis. The Sguil client is written in tcl/tk and can be run on any operating system that supports **tcl/tk (including Linux, *BSD, Solaris, MacOS, and Win32)**



RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	gateway	2.6422	2007-03-19 23:05:14	63.26.198.32		209.120.188.193		1	BLEEDING-EDGE WORM Allapple ICMP Sweep Ping Inbound
RT	64	gateway	2.6424	2007-03-19 23:13:28	203.193.56.133	45026	209.120.188.193	22	6	BLEEDING-EDGE Potential SSH Scan
RT	1	gateway	2.6489	2007-03-19 23:52:22	213.7.12.116		209.120.188.193		1	BLEEDING-EDGE WORM Allapple ICMP Sweep Ping Inbound
RT	1	gateway	2.6496	2007-03-20 00:28:10	24.178.8.170		209.120.188.193		1	BLEEDING-EDGE WORM Allapple ICMP Sweep Ping Inbound

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	gateway	2.5980	2007-03-18 20:31:06	85.188.1.26	6667	209.120.188.193	58870	6	BLEEDING-EDGE POLICY IRC connection
RT	1	gateway	2.6298	2007-03-19 08:03:51	87.240.48.122	1173	209.120.188.193	1434	17	MS-SQL version overflow attempt
RT	1	gateway	2.6380	2007-03-19 18:37:24	220.178.43.82	3064	209.120.188.193	1434	17	MS-SQL version overflow attempt
RT	1	gateway	2.6387	2007-03-19 19:16:20	202.101.62.218	1030	209.120.188.193	1434	17	MS-SQL version overflow attempt

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	gateway	4.3	2007-03-01 02:49:52	202.188.160.53	45398	209.120.188.193	22	6	PADS New Asset - ssh OpenSSH 3.9p1 (Protocol 1.99)
RT	1	gateway	4.4	2007-03-01 05:35:33	211.147.250.20	6000	209.120.188.193	3128	6	PADS New Asset - www squid/2.5.STABLE6
RT	1	gateway	4.5	2007-03-03 03:40:46	82.96.96.3	38419	209.120.188.193	23	6	PADS New Asset - ssh OpenSSH 3.9p1 (Protocol 1.99)
RT	1	gateway	4.6	2007-03-08 15:13:20	162.18.202.88	40942	209.120.188.193	44	6	PADS New Asset - ssh OpenSSH 4.3 (Protocol 2.0)

IP Resolution Agent Status Snort Statistics System Msgs User Msgs

Sid	Net	Hostname	Type	Last	Status
1	Ext_Net	gateway	pcap	2007-03-20 00:49:23	UP
2	Ext_Net	gateway	snort	2007-03-20 00:28:10	UP
3	Ext_Net	gateway	sancp	2007-03-19 01:59:34	UP
4	Ext_Net	gateway	pads	2007-03-08 15:13:20	UP

Show Packet Data Show Rule www.snort.org nvd.nist.gov

alert udp \$EXTERNAL_NET any -> \$HOME_NET 1434 (msg:"MS-SQL version overflow attempt", flowbits:isnotset,ms_sql_seen_dns; dsiz>100; content:"|04|"; depth:1; reference:bugtraq,5310; reference:cve,2002-0649; reference:nessus,10674; reference:www.microsoft.com/technet/security/bulletin/MS02-020.aspx; electrowire action: sid:3060; rev:0)

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	220.178.43.82	209.120.188.193	4	5	0	404	31898	0	0	115	13184
UDP	Source Port	Dest Port	Length		ChkSum						
	3064	1434	384		37652						
DATA	<pre> 04 01 DC C9 B0 42 EB 0E 01 01 01 01 01 01 01 70 AE 42 01 70 AE 42 90 90 90 90 90 90 90 68 DC C9 B0 42 B8 01 01 01 01 31 C9 B1 18 50 E2 FD 35 01 01 01 05 50 89 E5 51 68 2E 64 6C 6C 68 65 6C 33 32 68 6B 65 72 6E 51 68 6F 75 6E 74 68 69 63 6B 43 68 47 65 74 54 66 B9 6C 6C 51 68 33 32 2E 64 68 77 73 32 5F 66 B9 65 74 51 68 73 6F 63 6B 66 B9 74 6F 51 68 73 65 6E 64 BE 18 10 AE 42 8D 45 </pre>										

Update Interval (secs): 120 NOW

Search Packet Payload Hex Text NoCase



RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	gateway	2.6692	2007-03-20 19:45:42	86.85.219.170		209.120.188.193		1	ICMP PING NMAP
RT	1	gateway	2.6730	2007-03-20 20:00:34	83.69.111.67		209.120.188.193		1	BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound
RT	1	gateway	2.6769	2007-03-20 20:18:02	217.113.225.107		209.120.188.193		1	BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound
RT	1	gateway	2.6874	2007-03-20 20:50:05	201.8.143.68		209.120.188.193		1	BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound
RT	1	gateway	2.6907	2007-03-20 21:12:20	194.65.57.37		209.120.188.193		1	BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	gateway	2.6298	2007-03-19 08:03:51	87.240.48.122	1173	209.120.188.193	1434	17	MS-SQL version overflow attempt
RT	1	gateway	2.6380	2007-03-19 18:37:24	220.178.43.82	3064	209.120.188.193	1434	17	MS-SQL version overflow attempt
RT	1	gateway	2.6387	2007-03-19 19:16:20	202.101.62.218	1030	209.120.188.193	1434	17	MS-SQL version overflow attempt
RT	1	gateway	2.6541	2007-03-20 09:14:49	82.254.65.178	1984	209.120.188.193	80	6	http_inspect: OVERSIZE REQUEST-URI DIRECTORY

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	gateway	4.1	2007-03-01 00:19:49	162.18.202.71	39842	209.120.188.193	80	6	PADS New Asset - www Apache 2.0.52 (CentOS)
RT	1	gateway	4.2	2007-03-01 00:20:05	24.85.138.40	1269	209.120.188.193	7734	6	PADS New Asset - unknown unknown
RT	1	gateway	4.3	2007-03-01 02:49:52	202.188.160.53	45398	209.120.188.193	22	6	PADS New Asset - ssh OpenSSH 3.9p1 (Protocol 1.99)
RT	1	gateway	4.4	2007-03-01 05:35:33	211.147.250.20	6000	209.120.188.193	3128	6	PADS New Asset - www squid/2.5.STABLE6
RT	1	gateway	4.5	2007-03-03 03:40:46	82.96.96.3	38419	209.120.188.193	23	6	PADS New Asset - ssh OpenSSH 3.9p1 (Protocol 1.99)
RT	1	gateway	4.6	2007-03-08 15:13:20	162.18.202.88	40942	209.120.188.193	44	6	PADS New Asset - ssh OpenSSH 4.3 (Protocol 2.0)

IP Resolution Agent Status Snort Statistics System Msgs User Msgs

Reverse DNS

Src IP: 82.96.96.3
 Src Name: please.read.http.proxyscan.freenode.net

Dst IP: 209.120.188.193
 Dst Name: 193-188-120-209.static.mesanetworks.net

Whois Query: None Src IP Dst IP

```
% This is the RIPE Whois query server #2.
% The objects are in RPSL format.
%
% Note: the default output of the RIPE Whois server
% is changed. Your tools may need to be adjusted. See
% http://www.ripe.net/db/news/abuse-proposal-20050331.html
% for more details.
%
% Rights restricted by copyright.
% See http://www.ripe.net/db/copyright.html
```

Display Detected Banner

```
01 01 08 0A EC 60 F8 C0 3A 6E 7B 0A 01 01 08 0A
EC 60 F8 C2 3A 6E 7B 0A 01 01 08 0A EC 60 F8 E3
3A 6E 7B 0A 53 53 48 2D 31 2E 39 39 2D 4F 70 65
6E 53 53 48 5F 33 2E 39 70 31 0A
.....:nE.....
.:nE. ....
:nE.SSH- 1.99-Ope
nSSH_3.9 p1.
```

Referências

- <http://www.snort.org>
- <http://sguil.sourceforge.net/>
- <http://taosecurity.blogspot.com/>
- <http://securitysauce.blogspot.com/>
- Skype

<http://www.snort.org/users/jbrvenik/Site/Code.html>



Treinamento SNORT

- Mundo IDS (NDIS, HIDS , WIDS , KIDS)
- Tipos de ataques
- Como funciona o SNORT
- Instalando e configurando o SNORT
- Gerenciando o Snort via IDS Policy Manager
- Relatórios de Ataques
- Básico sobre criação de Regras
- <http://www.temporealeventos.com.br/?area=87>



Perguntas ?

Rodrigo Montoro aka Sp0oKeR

spooker@gmail.com

<http://spookerlabs.multiply.com>

<http://www.snort.org>

<http://www.brc.com.br>

