

Fórum Internacional de Software Livre – FISL 7

Pré-Processadores Grupo SNORT-BR

Rodrigo Ribeiro Montoro aka Sp0oKeR – rodrigo@brc.com.br



BRCONNECTION
CRESCER SEGURO

Rodrigo Montoro aka Sp0oKeR

- Diretor BRConnection Porto Alegre
- Responsável Security Team BRmultiaccess
- Redhat Certified Engineer (RHCE)
- LPIC-I

BRconnection

- Desenvolvedora BRmultiaccess (UTM)
- MessengerPolicy (Controle de Acesso MSN)
- Parceira Distribuição Regras SourceFire
- Mais de 5000 servidores
- Demos no Stand 20
- Cadastro de Parceiros (Indicadores / Revendas)



Comunidades / Projetos

- Snort-BR
- Linuxchix-BR
- Grupo Usuarios Slackware

Introdução Snort

- Sniffer
- Packet Log
- Network Intrusion Detection (NIDS)
- Wireless IDS
- Intrusion Prevention System (IPS)

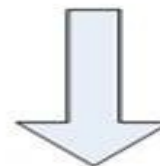


Broadcast / Libpcap
Captura os pacotes



Pré Processadores

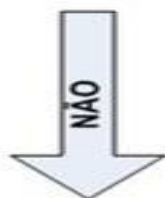
Frag2
HTTP
RPC



Plugins de Saída

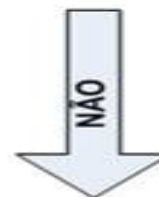


Sistema Detecção
(Assinaturas)



Alertas / Bloqueios

E-Mail
Logs
Popup
Firewall
SNMP



Segue Trafego sem
gerar alertas

Pré-Processadores

- Introduzido versão 1.5
- Após Decoder
- Antes Sistema Detecção
- Modularização
- Normalizar tráfego



Exemplos Pré-Processadores

Stream4

- Lançado 2001
- Remontagem Pacote (não modifica)
- Inspeção Stateful (anti ataques stateless - stick)
- Fluxo Cliente / Servidor e estado conexão (flow)
- Detecção Problemas Pacotes
- Manipulação de multiplas conexões simultaneas
 - Necessidades de mais de 256 conexões simultaneas.
 - Default: 8192 (mais de 100,000)



Frag3

- Sucessor frag2
- Frag2 (Splay Trees) x Frag3 (sfxhash)
- Ambiguidade RFC's (fragmentação)
- Target-Based host
- Analise Pacotes Fragmentados

– C-M-D-.-E-X-E



Lista de Target's

Fragmentation Policy	Platforms
BSD-right	HP JetDirect
BSD	AIX 2, 4.3, 8.9.3, FreeBSD, HP-UX B.10.20, IRIX 4.0.5F, 6.2, 6.3, 6.4, NCD Thin Clients, OpenBSD, OpenVMS, OS/2, OSF1, SunOS 4.1.4, Tru64 Unix V5.0A, V5.1, Vax/VMS
Linux	Linux 2.x
First	HP-UX 11.00, MacOS (version unknown), SunOS 5.5.1,5.6,5.7,5.8, Windows (95/98/NT4/ME/W2K/XP/2003)
Last	Cisco IOS



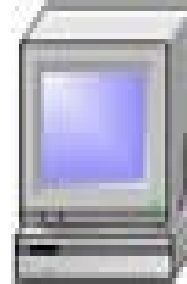
Evasion de Fragmentação



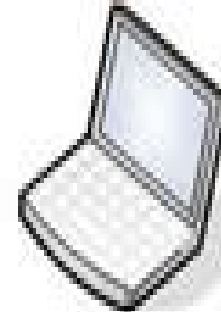
BRCONNECTION
CRESCER SEGURO



Attacker



NIDS
Frag_timeout=15 secs

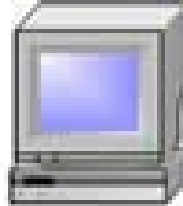


Victim
Frag_timeout=30 sec



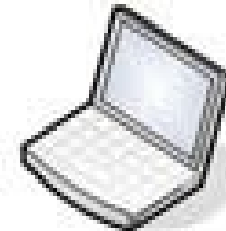


Attacker



NIDS

Frag_timeout = 60 secs



Victim

Frag_timeout = 30 sec



Time = 0 secs



Sending



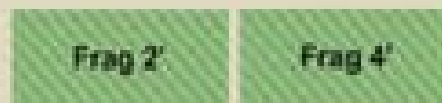
Received



Received

Time = 30 secs

Waiting



Frag Waiting

Fragments
Dropped

False Reassembly

30 secs < T < 60 secs



Sending



Received



Correct Reassembly

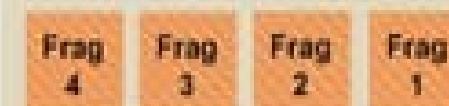
30 secs < T < 60 secs



Sending



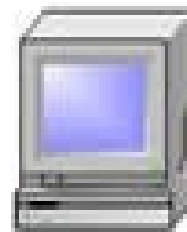
Received



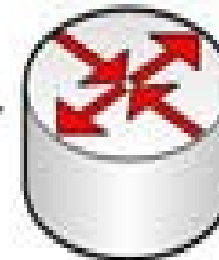
ATTACK



Attacker



NIDS



Router



Victim



Sending



Received



Received



Sending



Received



Frag 1

Frag Dropped at router



Frag 1

Waiting



Sending



False reassembly



Frag 3

Frag 1

Waiting



Sending



Received



Frag 3

Frag 2

Frag 1

Correct reassembly

Exemplo Frag3

```
preprocessor frag3_global: max_fragments 65536
```

```
preprocessor frag3_engine: policy linux \  
    bind_to [10.1.1.12/32,10.1.1.13/32] \  
    min_ttl 2
```

```
preprocessor frag3_engine: policy first \  
    bind_to 10.2.1.0/24 \  
    detect_anomalies
```

```
preprocessor frag3_engine: policy last \  
    bind_to 10.3.1.0/24
```

```
preprocessor frag3_engine: policy bsd
```



http_inspect

- Tráfego http (stateless)
 - Packet-by-packet
- IIS (Internet Information Server)
- Apache
- Profiles (IIS / Apache)
- Funcionalidades:
 - Barra dupla
 - Servidores Desconhecidos
 - Espaços
 - Unicode map
 - Etc ...



Profile all

Table 2.6: Options for the “all” Profile

Option	Setting
flow_depth	300
chunk encoding	alert on chunks larger than 500000 bytes
iis_unicode_map	codepoint map in the global configuration
ascii decoding	on, alert off
multiple slash	on, alert off
directory normalization	on, alert off
apache whitespace	on, alert off
double decoding	on, alert on
%u decoding	on, alert on
bare byte decoding	on, alert on
iis unicode codepoints	on, alert on
iis backslash	on, alert off
iis delimiter	on, alert off
webroot	on, alert on
non_strict URL parsing	on
tab_uri_delimiter	is set

Profile Apache

Table 2.7: Options for the “apache” Profile

Option	Setting
flow_depth	300
chunk encoding	alert on chunks larger than 500000 bytes
ascii decoding	on, alert off
multiple slash	on, alert off
directory normalization	on, alert off
webroot	on, alert on
apache whitespace	on, alert on
utf_8 encoding	on, alert off
non_strict url parsing	on
tab_uri_delimiter	is set

Profile IIS

Table 2.8: Options for the “iis” Profile

Option	Setting
flow_depth	300
chunk encoding	alert on chunks larger than 500000 bytes
iis_unicode_map	codepoint map in the global configuration
ascii decoding	on, alert off
multiple slash	on, alert off
directory normalization	on, alert off
webroot	on, alert on
double decoding	on, alert on
%u decoding	on, alert on
bare byte decoding	on, alert on
iis unicode codepoints	on, alert on
iis backslash	on, alert off
iis delimiter	on, alert on
apache whitespace	on, alert on
non_strict URL parsing	on

Exemplo 1 http_inspect

```
preprocessor http_inspect_server: server 10.1.1.1 \  
  ports { 80 3128 8080 } \  
  flow_depth 0 \  
  ascii no \  
  double_decode yes \  
  chunk_length 500000 \  
  non_strict \  
  no_alerts
```



Exemplo 2 http_inspect

```
preprocessor http_inspect_server: server default \  
  ports { 80 3128 } \  
  non_strict \  
  non_rfc_char { 0x00 } \  
  flow_depth 300 \  
  apache_whitespace yes \  
  directory no \  
  iis_backslash no \  
  u_encode yes \  
  ascii no \  
  iis_unicode yes \  
  multi_slash no
```



Not Found

The requested URL /rodrigo/snort was not found on this server.

Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.

Apache/1.3.33 Server at www.spooker.com.br Port 80

Not Found

The requested URL /rodrigo,snort was not found on this server.

Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.

Apache/1.3.33 Server at www.spooker.com.br Port 80

Not Found

The requested URL /teste.cgi?cmd=rm was not found on this server.

Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.

Apache/1.3.33 Server at www.spooker.com.br Port 80

sfPortscan

- Desenvolvido pela SourceFire
- Fase de reconhecimento
 - Protocolos
 - Portas
- Detecção de Portscan
 - TCP, UDP , ICMP portscan
 - TCP, UDP , ICMP Decoy Portscan
 - TCP,UDP , ICMP portscan distribuido
 - TCP, UDP , ICMP portsweep



Exemplo sfPortscan

preprocessor sfportscan: proto <protocols>

scan_type <portscan|portswEEP|decoy_portscan|distributed_portscan|all>

sense_level <low|medium|high>

watch_ip <IP or IP/CIDR>

ignore_scanners <IP list>

ignore_scanned <IP list>

logfile <path and filename>

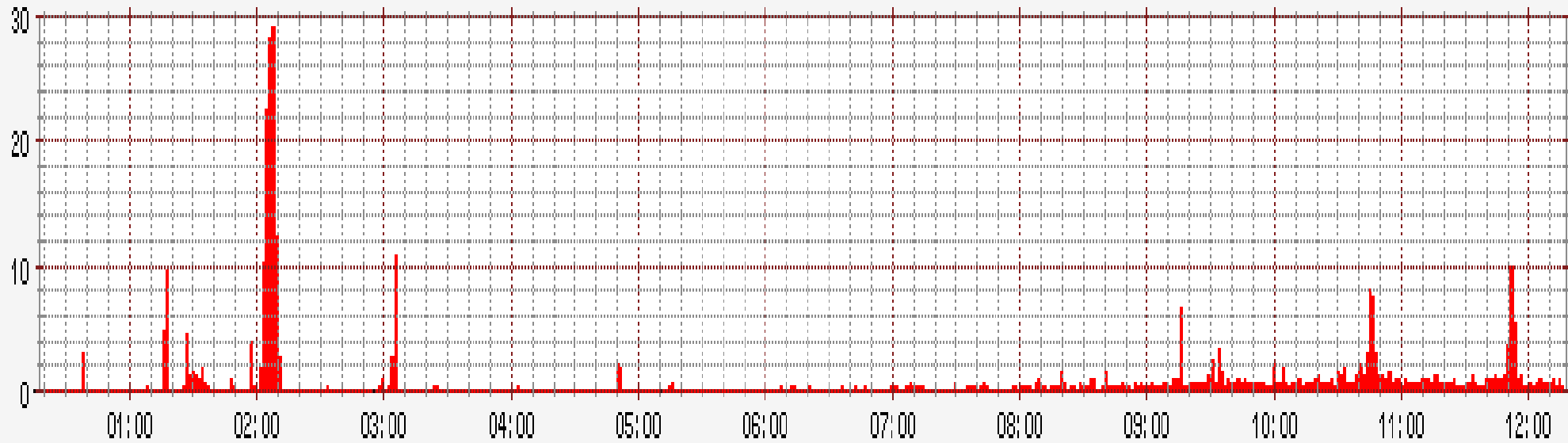


PerfMonitor

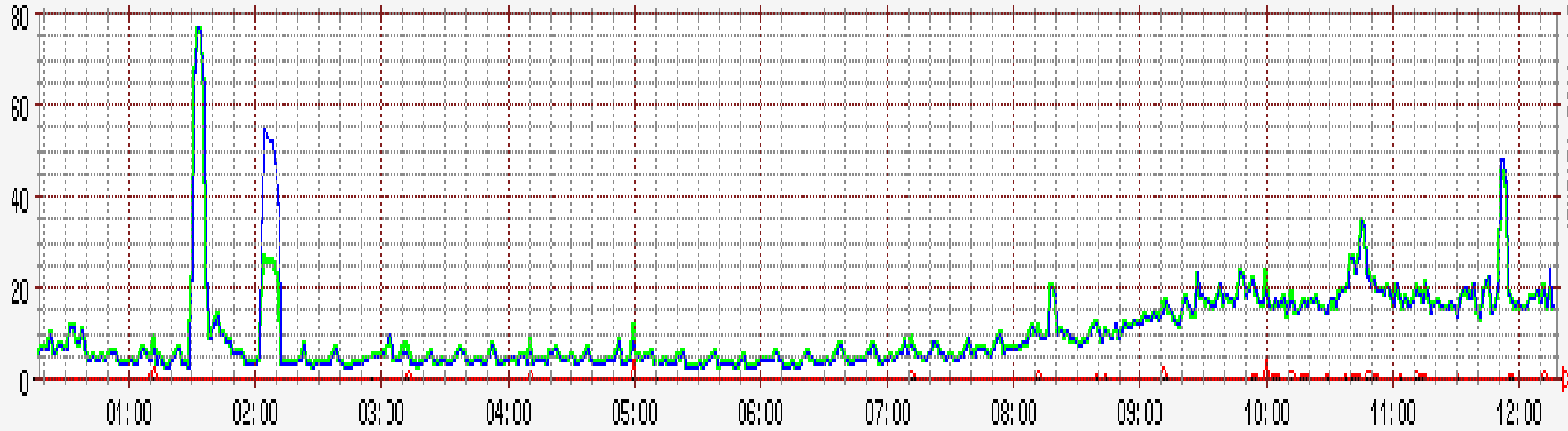
- Gráficos de estatísticas do Snort
 - Syn / SynAck
 - Status do Processador (CPU)
 - Eventos Fragmentação
 - Média Pacotes
 - Analisar performance Hardware



Dropped packets (%)



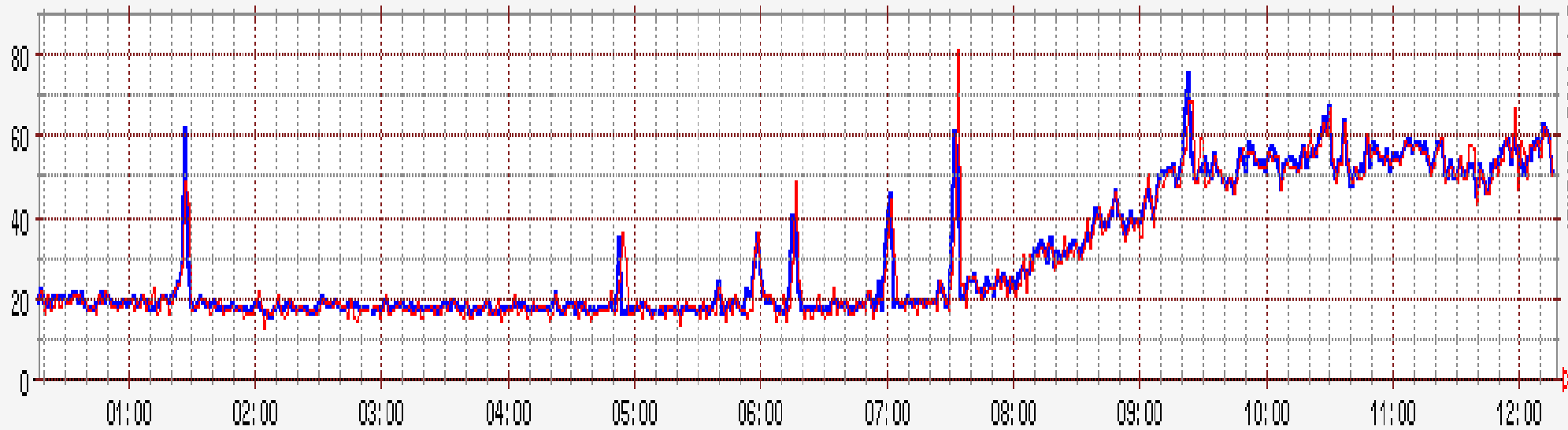
Mbit per second



PROTOCOL: TORRE_021118



Session events per second

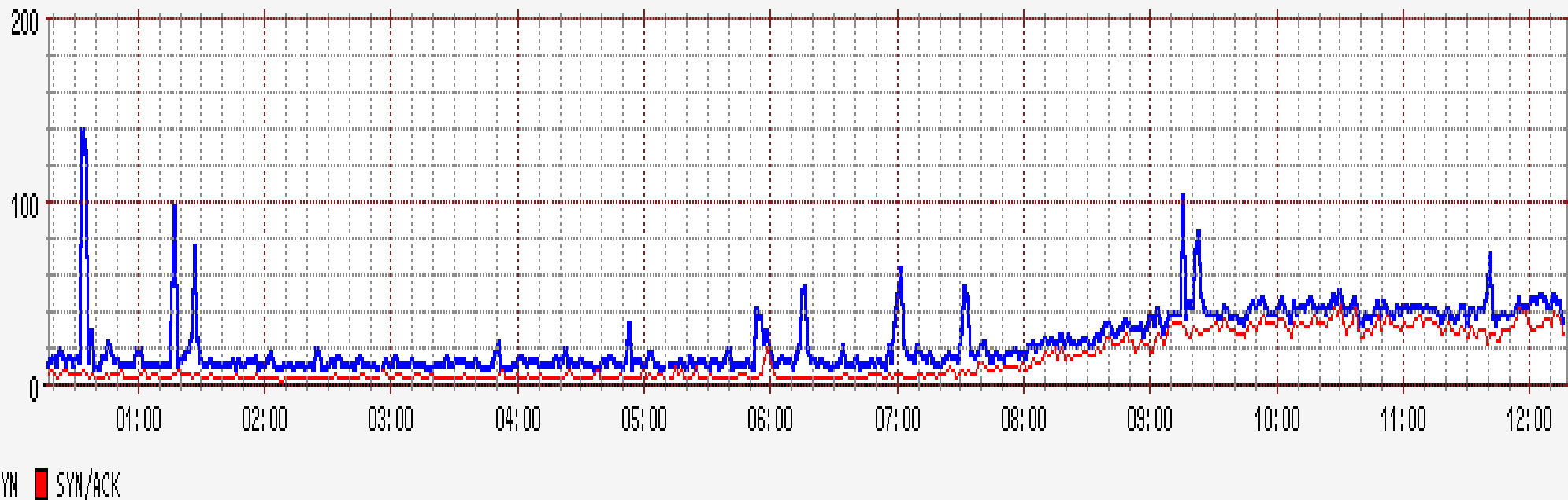


■ new ■ deleted

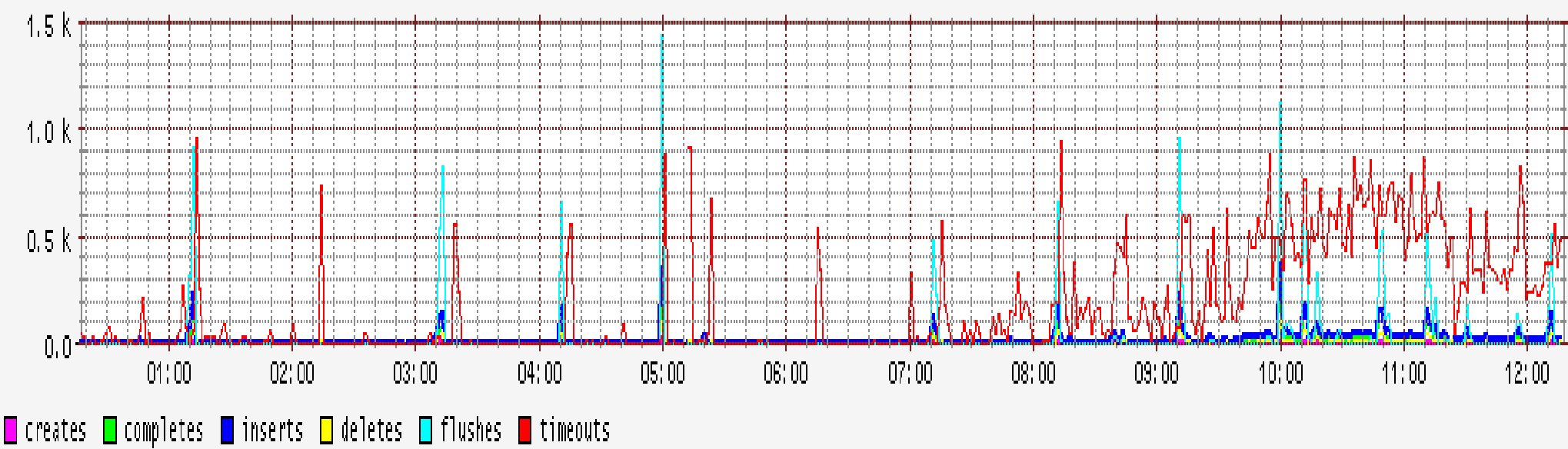


BRCONNECTION
CRESCER SEGURO

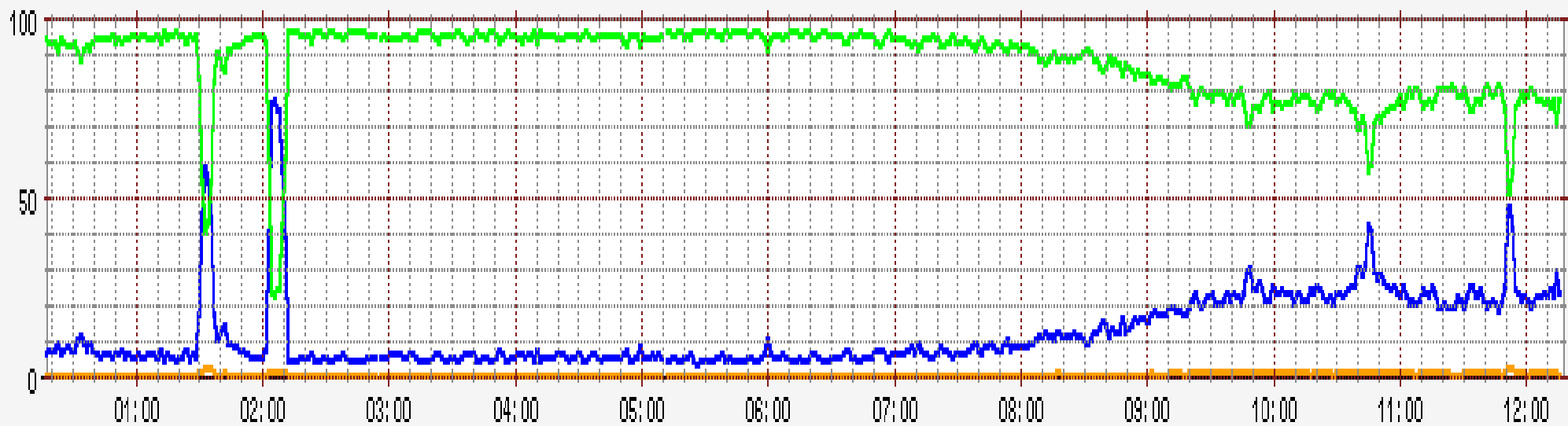
SYN + SYN/ACK packets per second



frag events per second



CPU1 stats (%)



■ user ■ system ■ idle

Mais Pré-Processadores ...

- Clamav
 - Scanear dados em pacotes por virus
- Fnord
 - Detecção Ataques Polimorficos
- Arp Spoof
 - Arp Poison



Snort 2.6

- Fase BETA
- Novidades
 - Plugins Dinamicos
 - Pre-Processadores (SMTP /FTPTELNET)
 - Validação de configuração de Pre-Processadores



Carregamento Módulos Dinamicos

```
#Parametro inicializcao  
--dynamic-preprocessor-lib
```

```
#Caminho Modulos (.so)
```

FTPTELNET

```
/usr/local/lib/snort_dynamicpreprocessor/libsf_ftptelnet_preproc.so
```

SMTP

```
/usr/local/lib/snort_dynamicpreprocessor/libsf_smtp_preproc.so
```

SMTP

- Analisa comandos SMTP (recebidos/respostas)
 - Stateful / Stateless
 - Comandos válidos / inválidos / desconhecidos
 - Normalização comandos



Exemplo SMTP

```
preprocessor smtp: \  
  ports { 25 } \  
  inspection_type stateful \  
  normalize cmds \  
  normalize_cmds { EXPN VRFY RCPT } \  
  alt_max_command_line_len 260 { MAIL } \  
  alt_max_command_line_len 300 { RCPT } \  
  alt_max_command_line_len 500 { HELP HELO ETRN } \  
  alt_max_command_line_len 255 { EXPN VRFY }
```



FTP/Telnet

- Melhoramento do Pré-Processador Telnet
- Manipula tráfego FTP (Servidor / Cliente)
- Normaliza tráfego de ambos (FTP / Telnet)



Exemplo 1 ftp telnet

```
preprocessor ftp_telnet: global \  
  encrypted_traffic yes \  
  inspection_type stateful
```

```
preprocessor ftp_telnet_protocol: telnet \  
  normalize \  
  ayt_attack_thresh 200
```

Exemplo 2 ftptelnet

```
preprocessor 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 nnnnnnnnnnnnnnn[n[n[n]]] ] string > \  
  chk_str_fmt { USER PASS RNFR RNTD SITE MKD } \  
  telnet_cmds yes \  
  data_chan
```

```
preprocessor ftp_telnet_protocol: ftp client default \  
  max_resp_len 256 \  
  bounce yes \  
  telnet_cmds yes
```

Grupo Snort-BR

- <http://snort.linuxsecurity.com.br>
- IRC
 - Irc.freenode.net (#snort-br)
- Lista Grupo
 - <http://listas.cipsga.org.br/cgi-bin/mailman/listinfo/snort->
 - Para postar uma mensagem a todos os membros da lista, envie um email para snort-ids@listas.cipsga.org.br



Links / Fontes

- <http://www.snort.org/docs/>
- <http://www.securityfocus.com/infocus/1852>
- <http://afrodita.unicauca.edu.co/~cbedon/snort/sno1>

Dúvidas ?

Rodrigo Ribeiro Montoro

rodrigo@brc.com.br

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

<http://www.brc.com.br/fisl7/>



BRCONNECTION
CRESCER SEGURO