Identificação de Cenários de Intrusão pela Classificação, Caracterização e Análise de Eventos gerados por Firewalls

Fábio Elias Locatelli[1]
Fabiane Dillenburg[1]
Cristina Melchiors[2]
Luciano Paschoal Gaspary[2]

[1]Universidade do Vale do Rio dos Sinos (UNISINOS)
[2]Universidade Federal do Rio Grande do Sul (UFRGS)

paschoal@inf.ufrgs.br
http://www.inf.ufrgs.br/~paschoal

7a. Reunião do Grupo de Trabalho em Segurança de Redes (GTS-7)
27 de junho de 2006 – Porto Alegre

Roteiro

- Introdução
- Abordagem para classificação, caracterização e análise de eventos
- Identificação automática de cenários suspeitos
- A ferramenta SEFLA
- Estudo de caso
- Conclusões e trabalhos futuros

Introdução

- Uma das alternativas mais utilizadas pelas empresas como medida de proteção contra ataques é o *firewall*
- Os *firewalls* armazenam − para cada acesso bem sucedido ou tentativa frustrada − registros em arquivos de *log*
- Do ponto de vista da gerência de segurança este *log* é rico em informações, pois permite:
  - mensurar e identificar os acessos à rede privada e à externa
  - acompanhar historicamente o crescimento do volume de acessos
  - depurar problemas de configuração de regras de filtragem
  - reconhecer seqüências de eventos que indiquem estratégias usadas por invasores para tentar acessar estações e serviços

Introdução

- Controle manual dos arquivos de *log* é inviável
  - *Log* diário gerado pode ser maior que 1 GB
- Existem algumas ferramentas para a análise de *logs*
  - Não oferecem visão histórica de ocorrência dos eventos
  - Não dispõem de mecanismos para a visualização facilitada de eventos
  - Não são capazes de identificar atividades suspeitas automaticamente

- Apresentamos uma abordagem, acompanhada de uma ferramenta, para classificação, caracterização e análise de eventos gerados por *firewalls*
- Validamos a abordagem e a ferramenta usando *logs* reais gerados ao longo de uma semana pelo *firewall* da universidade

Abordagem para análise de eventos

01/03 05:15:39.751 347 Port Scan detected (66.66.77.77→10.200.160.161 Port 3526→79)
01/03 05:15:39.779 347 Port Scan detected (66.66.77.77→10.200.160.161 Port 3528→80)
01/03 05:15:39.821 347 Port Scan detected (66.66.77.77→10.200.160.161 Port 3530→81)
01/03 05:16:55.121 347 Port Scan detected (66.66.77.90 → 10.200.160.1 Port 1316 → 80)
01/03 05:16:55.168 347 Port Scan detected (66.66.77.90 → 10.200.160.2 Port 1340 → 80)
01/03 05:15:55.187 347 Port Scan detected (66.66.77.90 → 10.200.160.3 Port 1352 → 80)
01/03 05:15:55.198 347 Port Scan detected (66.66.77.90 → 10.200.160.4 Port 1354 → 80)
01/03 05:15:55.210 347 Port Scan detected (66.66.77.90 → 10.200.160.5 Port 1368 → 80)
01/03 06:01:07.074 201 1080/tcp: Access denied for 66.66.77.77 to 10.200.160.161
01/03 06:12:08.963 201 1080/tcp: Access denied for 66.66.77.77 to 10.200.160.2
01/03 09:30:49.625 121 Statistics: duration=56.88 sent=16721 rcvd=277 src=66.66.77.77/1278 dst=10.200.160.161/21 proto=ftp
01/03 09:45:20.125 121 Statistics: duration=25.00 sent=25010 rcvd=300 src=66.66.77.80/1285 dst=10.200.160.161/21 proto=ftp

Abordagem para análise de eventos

01/03 05:15:39.751 347 Port Scan detected (66.66.77.77→10.200.160.161 Port 3526→79)
01/03 05:15:39.779 347 Port Scan detected (66.66.77.77→10.200.160.161 Port 3528→80)
01/03 05:15:39.821 347 Port Scan detected (66.66.77.77→10.200.160.161 Port 3530→81)
01/03 05:16:55.121 347 Port Scan detected (66.66.77.90 → 10.200.160.1 Port 1316 → 80)
01/03 05:16:55.168 347 Port Scan detected (66.66.77.90 → 10.200.160.2 Port 1340 → 80)
01/03 05:15:55.187 347 Port Scan detected (66.66.77.90 → 10.200.160.3 Port 1352 → 80)
01/03 05:15:55.198 347 Port Scan detected (66.66.77.90 → 10.200.160.4 Port 1354 → 80)
01/03 05:15:55.210 347 Port Scan detected (66.66.77.90 → 10.200.160.5 Port 1368 → 80)
01/03 06:01:07.074 201 1080/tcp: Access denied for 66.66.77.77 to 10.200.160.161
01/03 06:12:08.963 201 1080/tcp: Access denied for 66.66.77.77 to 10.200.160.2
01/03 09:30:49.625 121 Statistics: duration=56.88 sent=16721 rcvd=277 src=66.66.77.77/1278 dst=10.200.160.161/21 proto=ftp
01/03 09:45:20.125 121 Statistics: duration=25.00 sent=25010 rcvd=300 src=66.66.77.80/1285 dst=10.200.160.161/21 proto=ftp

Abordagem para análise de eventos

01/03 05:15:39.751 347 Port Scan detected (66.66.77.77→10.200.160.161 Port 3526→79)
01/03 05:15:39.779 347 Port Scan detected (66.66.77.77→10.200.160.161 Port 3528→80)
01/03 05:15:39.821 347 Port Scan detected (66.66.77.77→10.200.160.161 Port 3530→81)
01/03 05:16:55.121 347 Port Scan detected (66.66.77.90 → 10.200.160.1 Port 1316 → 80)
01/03 05:16:55.168 347 Port Scan detected (66.66.77.90 → 10.200.160.2 Port 1340 → 80)
01/03 05:15:55.187 347 Port Scan detected (66.66.77.90 → 10.200.160.3 Port 1352 → 80)
01/03 05:15:55.198 347 Port Scan detected (66.66.77.90 → 10.200.160.4 Port 1354 → 80)
01/03 05:15:55.210 347 Port Scan detected (66.66.77.90 → 10.200.160.5 Port 1368 → 80)
01/03 06:01:07.074 201 1080/tcp: Access denied for 66.66.77.77 to 10.200.160.161
01/03 06:12:08.963 201 1080/tcp: Access denied for 66.66.77.77 to 10.200.160.2
01/03 09:30:49.625 121 Statistics: duration=56.88 sent=16721 rcvd=277 src=66.66.77.77/1278 dst=10.200.160.161/21 proto=ftp
01/03 09:45:20.125 121 Statistics: duration=25.00 sent=25010 rcvd=300 src=66.66.77.80/1285 dst=10.200.160.161/21 proto=ftp

Abordagem para análise de eventos

01/03 05:15:39.751 347 Port Scan detected (66.66.77.77→10.200.160.161 Port 3526→79)
01/03 05:15:39.779 347 Port Scan detected (66.66.77.77→10.200.160.161 Port 3528→80)
01/03 05:15:39.821 347 Port Scan detected (66.66.77.77→10.200.160.161 Port 3530→81)
01/03 05:16:55.121 347 Port Scan detected (66.66.77.90 → 10.200.160.1 Port 1316 → 80)
01/03 05:16:55.168 347 Port Scan detected (66.66.77.90 → 10.200.160.2 Port 1340 → 80)
01/03 05:15:55.187 347 Port Scan detected (66.66.77.90 → 10.200.160.3 Port 1352 → 80)
01/03 05:15:55.198 347 Port Scan detected (66.66.77.90 → 10.200.160.4 Port 1354 → 80)
01/03 05:15:55.210 347 Port Scan detected (66.66.77.90 → 10.200.160.5 Port 1368 → 80)
01/03 06:01:07.074 201 1080/tcp: Access denied for 66.66.77.77 to 10.200.160.161
01/03 06:12:08.963 201 1080/tcp: Access denied for 66.66.77.77 to 10.200.160.2
01/03 09:30:49.625 121 Statistics: duration=56.88 sent=16721 rcvd=277 src=66.66.77.77/1278 dst=10.200.160.161/21 proto=ftp
01/03 09:45:20.125 121 Statistics: duration=25.00 sent=25010 rcvd=300 src=66.66.77.80/1285 dst=10.200.160.161/21 proto=ftp

Identificação automática de cenários suspeitos

- Propomos a utilização do paradigma *Raciocínio Baseado em Casos* (RBC) para identificar cenários de intrusão de forma automática
- RBC utiliza o conhecimento de experiências anteriores para propor soluções em novas situações
  - As experiências passadas são armazenadas como casos
  - Para a resolução de uma nova situação, esta é comparada aos casos armazenados e os casos mais similares são utilizados para propor soluções ao problema corrente

Caso A

Parte Administrativa

- Id: Acesso_bem_Sucedido_Após_Varredura
- Desc_Obs: Acessos a rede interna por um endereço IP...

Parte Classificatória

- Classificador: MESMO_IP_ORIGEM

Parte Descritiva

- Sintoma S_1:
  - Relevância: 1
  - Similaridade_Min_Necess: PARCIAL_0.5
  - Num_Min_Eventos: 5
  - Atributos_Evento:
  - Tipo_Evento: PORT_SCANNING
- Sintoma S_2:
  - Relevância: 1
  - Similaridade_Min_Necess: TOTAL
  - Num_Min_Eventos: 1
  - Atributos_Evento:
  - Tipo_Evento: STATISTIC

Caso A

Parte Administrativa

- Id: Acesso_bem_Sucedido_Após_Varredura
- Desc_Obs: Acessos a rede interna por um endereço IP...

Parte Classificatória

- Classificador: MESMO_IP_ORIGEM

Parte Descritiva

- Sintoma S_1:
  - Relevância: 1
  - Similaridade_Min_Necess: PARCIAL_0.5
  - Num_Min_Eventos: 5
  - Atributos_Evento:
  - Tipo_Evento: PORT_SCANNING
- Sintoma S_2:
  - Relevância: 1
  - Similaridade_Min_Necess: TOTAL
  - Num_Min_Eventos: 1
  - Atributos_Evento:
  - Tipo_Evento: STATISTIC

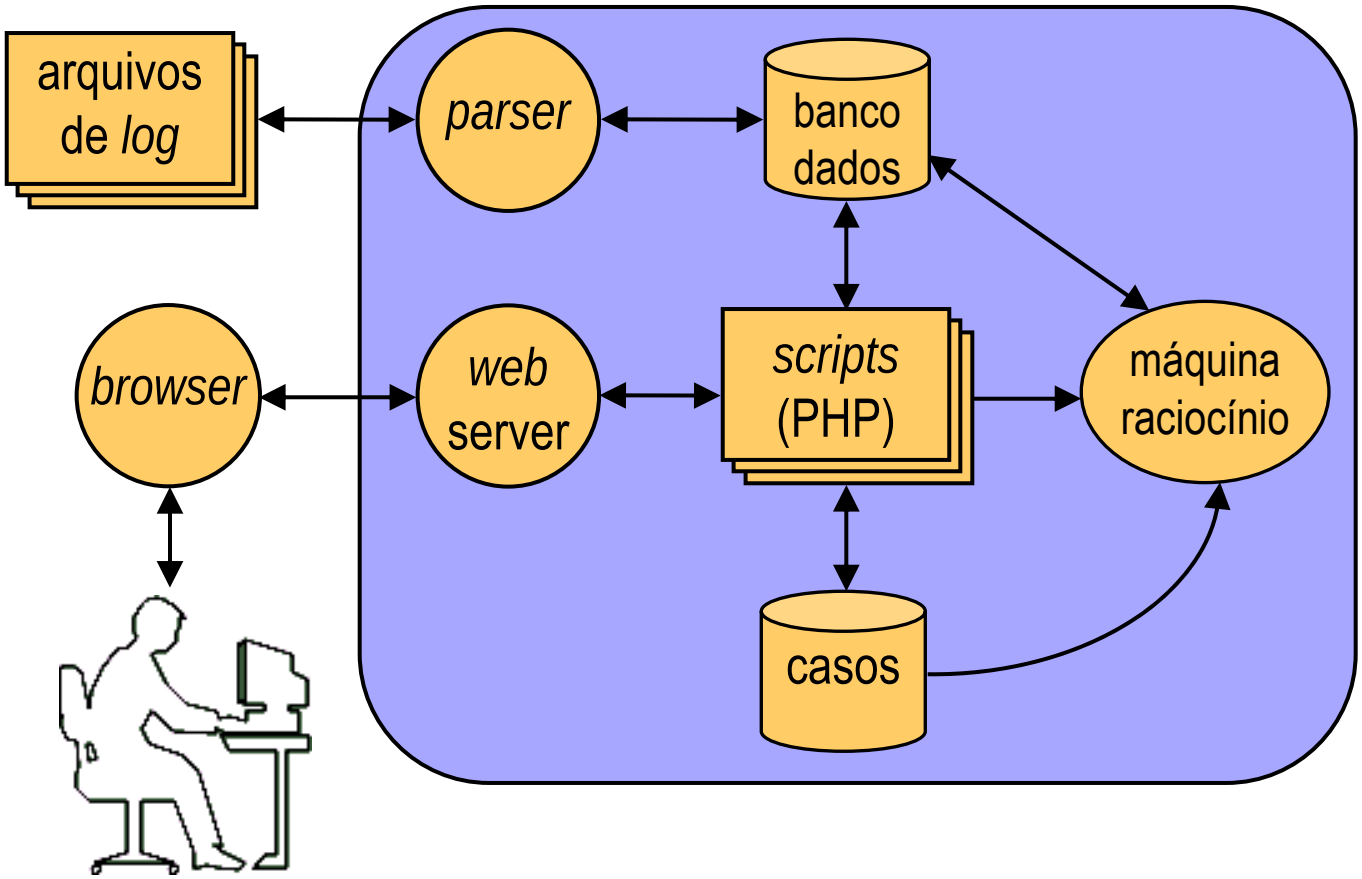
UNISINOS

```
01/03 05:15:39.751 347 Port Scan detected (66.66.77.77→10.200.160.161 Port 3526→79)
01/03 05:15:39.779 347 Port Scan detected (66.66.77.77→10.200.160.161 Port 3528→80)
01/03 05:15:39.821 347 Port Scan detected (66.66.77.77→10.200.160.161 Port 3530→81)
01/03 05:15:39.842 347 Port Scan detected (66.66.77.77 -> 10.200.160.161: Port 3532->82)
01/03 05:16:55.121 347 Port Scan detected (66.66.77.90 → 10.200.160.1 Port 1316 → 80)
01/03 05:16:55.168 347 Port Scan detected (66.66.77.90 → 10.200.160.2 Port 1340 → 80)
01/03 05:15:55.187 347 Port Scan detected (66.66.77.90 → 10.200.160.3 Port 1352 → 80)
01/03 05:15:55.198 347 Port Scan detected (66.66.77.90 → 10.200.160.4 Port 1354 → 80)
01/03 05:15:55.210 347 Port Scan detected (66.66.77.90 → 10.200.160.5 Port 1368 → 80)
01/03 06:01:07.074 201 1080/tcp: Access denied for 66.66.77.77 to 10.200.160.161
01/03 06:12:08.963 201 1080/tcp: Access denied for 66.66.77.77 to 10.200.160.2
01/03 09:30:49.625 121 Statistics: duration=56.88 sent=16721 rcvd=277
src=66.66.77.77/1278 dst=10.200.160.161/21 proto=ftp
```

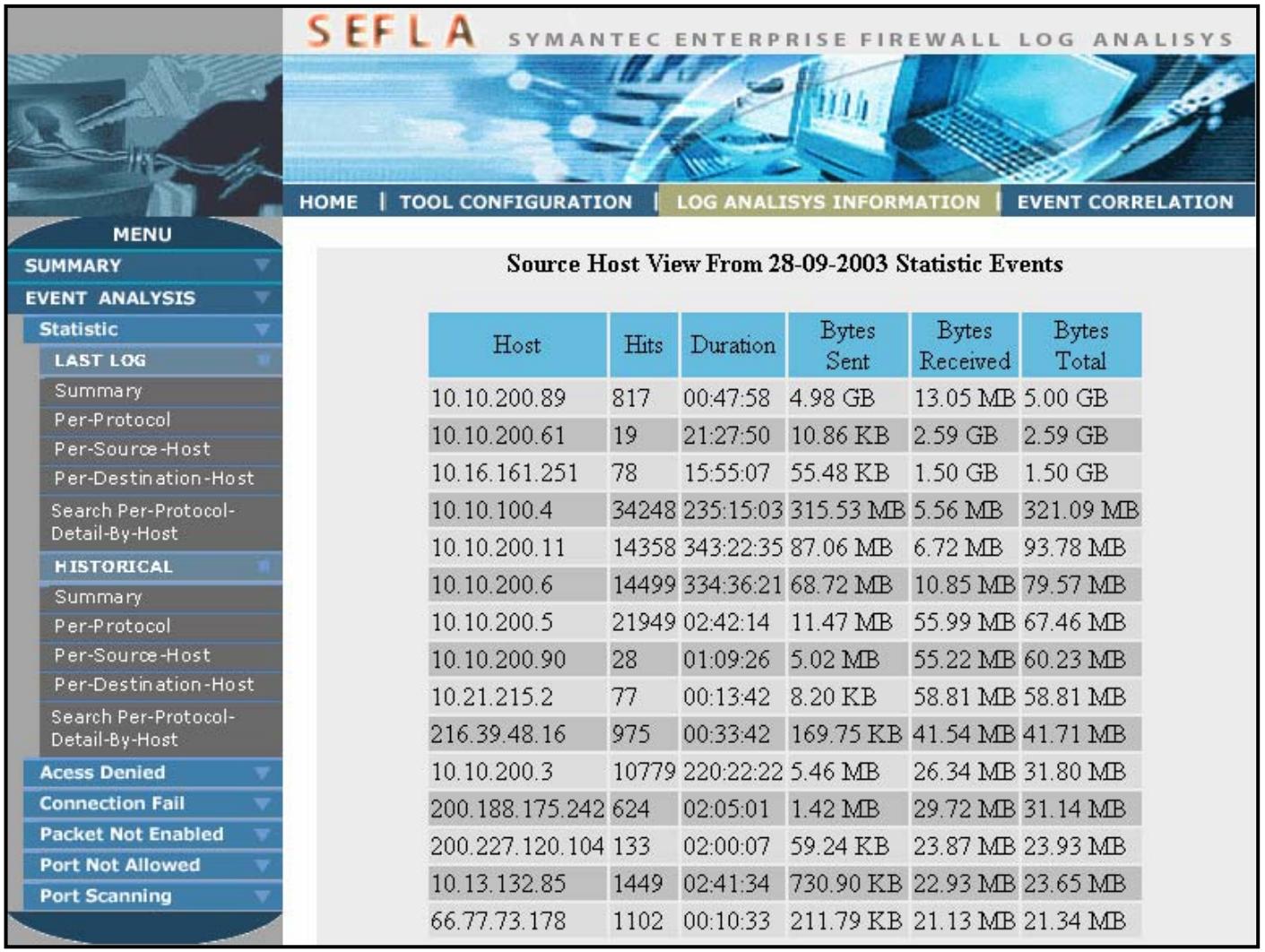
Caso A
Parte Administrativa
▪Id: Acesso_bem_Sucedido_Após_Varredura ▪Desc_Obs: Acessos a rede interna por um endereço IP...
Parte Classificatória
▪Classificador: MESMO_IP_ORIGEM
Parte Descritiva
▪Sintoma S_1: ▪Relevância: 1 ▪Similaridade_Min_Necess: PARCIAL_0.5 ▪Num_Min_Eventos: 5 ▪Atributos_Evento: ▪Tipo_Evento: PORT_SCANNING ▪Sintoma S_2: ▪Relevância: 1 ▪Similaridade_Min_Necess: TOTAL ▪Num_Min_Eventos: 1 ▪Atributos_Evento: ▪Tipo_Evento: STATISTIC

A ferramenta SEFLA

- Symantec Enterprise Firewall Log Analysis



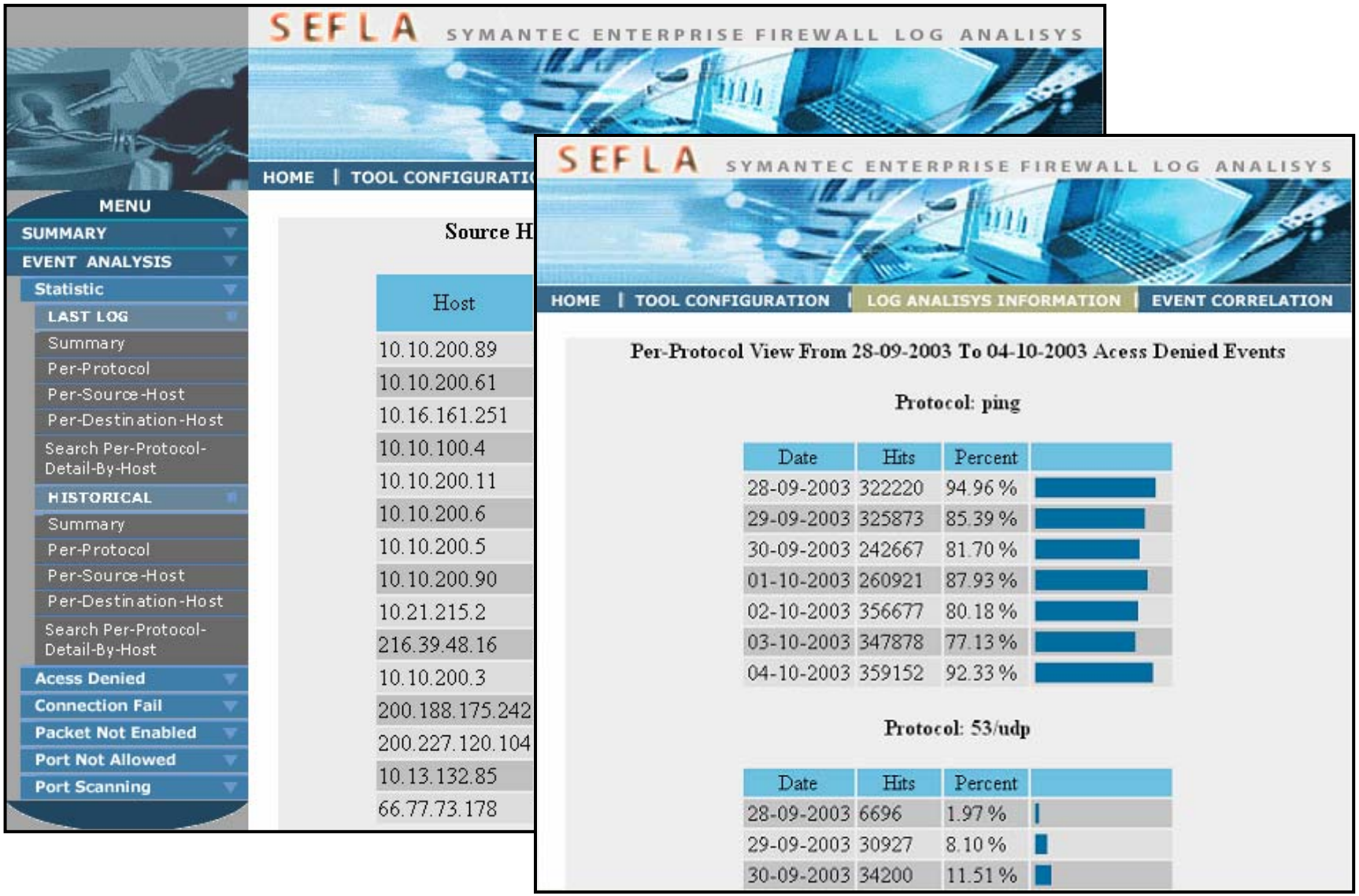
A ferramenta SEFLA



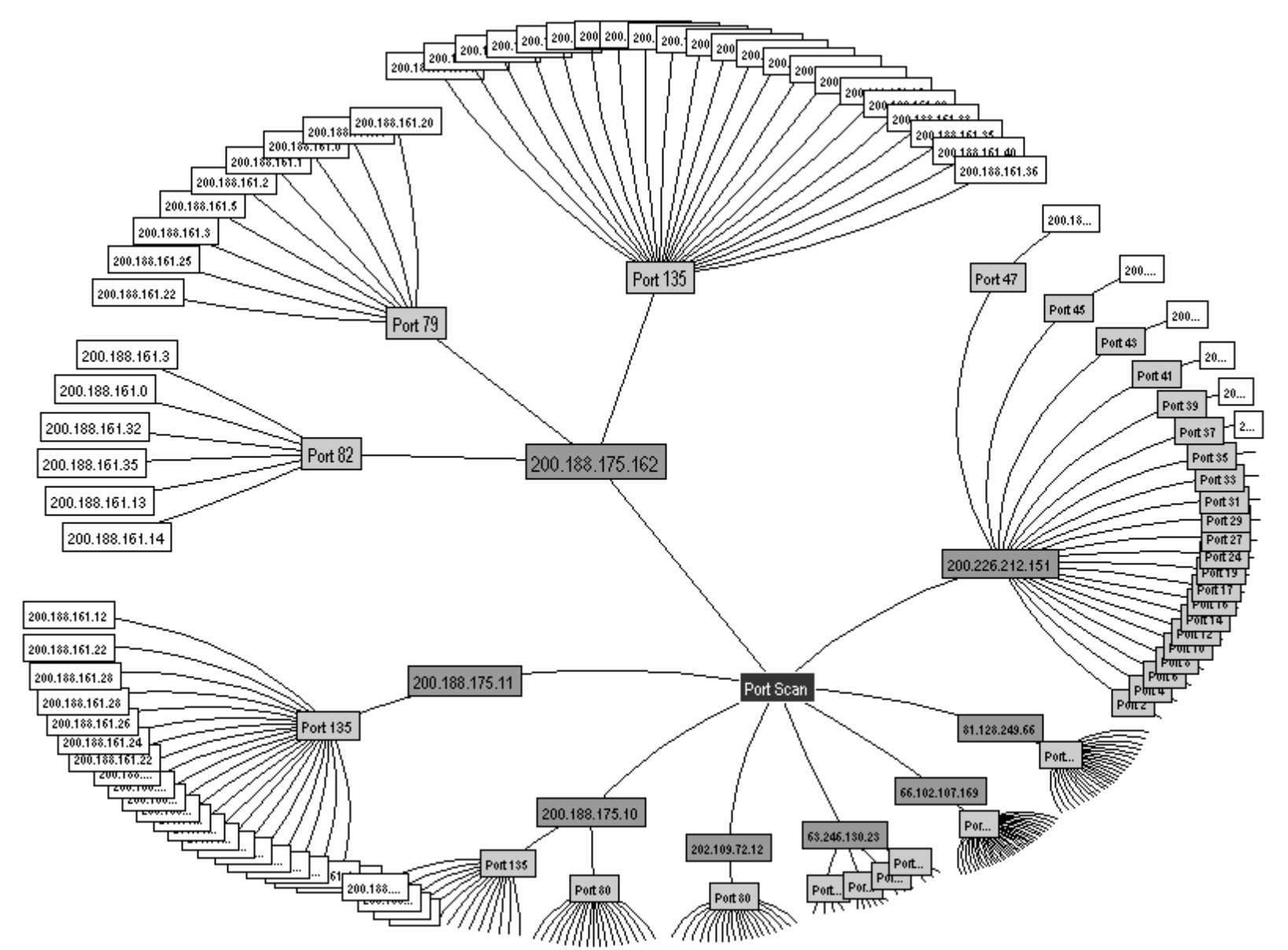
Source Host View From 28-09-2003 Statistic Events

Host	Hits	Duration	Bytes Sent	Bytes Received	Bytes Total
10.10.200.89	817	00:47:58	4.98 GB	13.05 MB	5.00 GB
10.10.200.61	19	21:27:50	10.86 KB	2.59 GB	2.59 GB
10.16.161.251	78	15:55:07	55.48 KB	1.50 GB	1.50 GB
10.10.100.4	34248	235:15:03	315.53 MB	5.56 MB	321.09 MB
10.10.200.11	14358	343:22:35	87.06 MB	6.72 MB	93.78 MB
10.10.200.6	14499	334:36:21	68.72 MB	10.85 MB	79.57 MB
10.10.200.5	21949	02:42:14	11.47 MB	55.99 MB	67.46 MB
10.10.200.90	28	01:09:26	5.02 MB	55.22 MB	60.23 MB
10.21.215.2	77	00:13:42	8.20 KB	58.81 MB	58.81 MB
216.39.48.16	975	00:33:42	169.75 KB	41.54 MB	41.71 MB
10.10.200.3	10779	220:22:22	5.46 MB	26.34 MB	31.80 MB
200.188.175.242	624	02:05:01	1.42 MB	29.72 MB	31.14 MB
200.227.120.104	133	02:00:07	59.24 KB	23.87 MB	23.93 MB
10.13.132.85	1449	02:41:34	730.90 KB	22.93 MB	23.65 MB
66.77.73.178	1102	00:10:33	211.79 KB	21.13 MB	21.34 MB

A ferramenta SEFLA



A ferramenta SEFLA

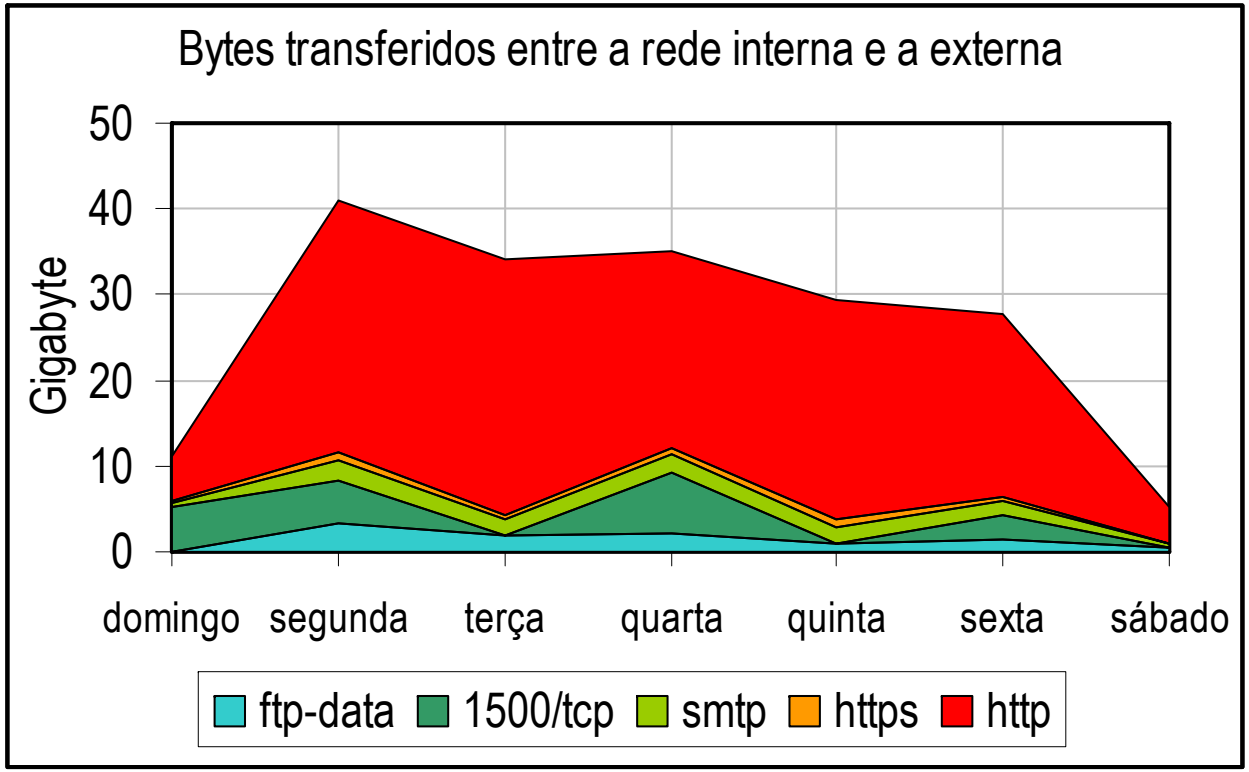


Estudo de caso

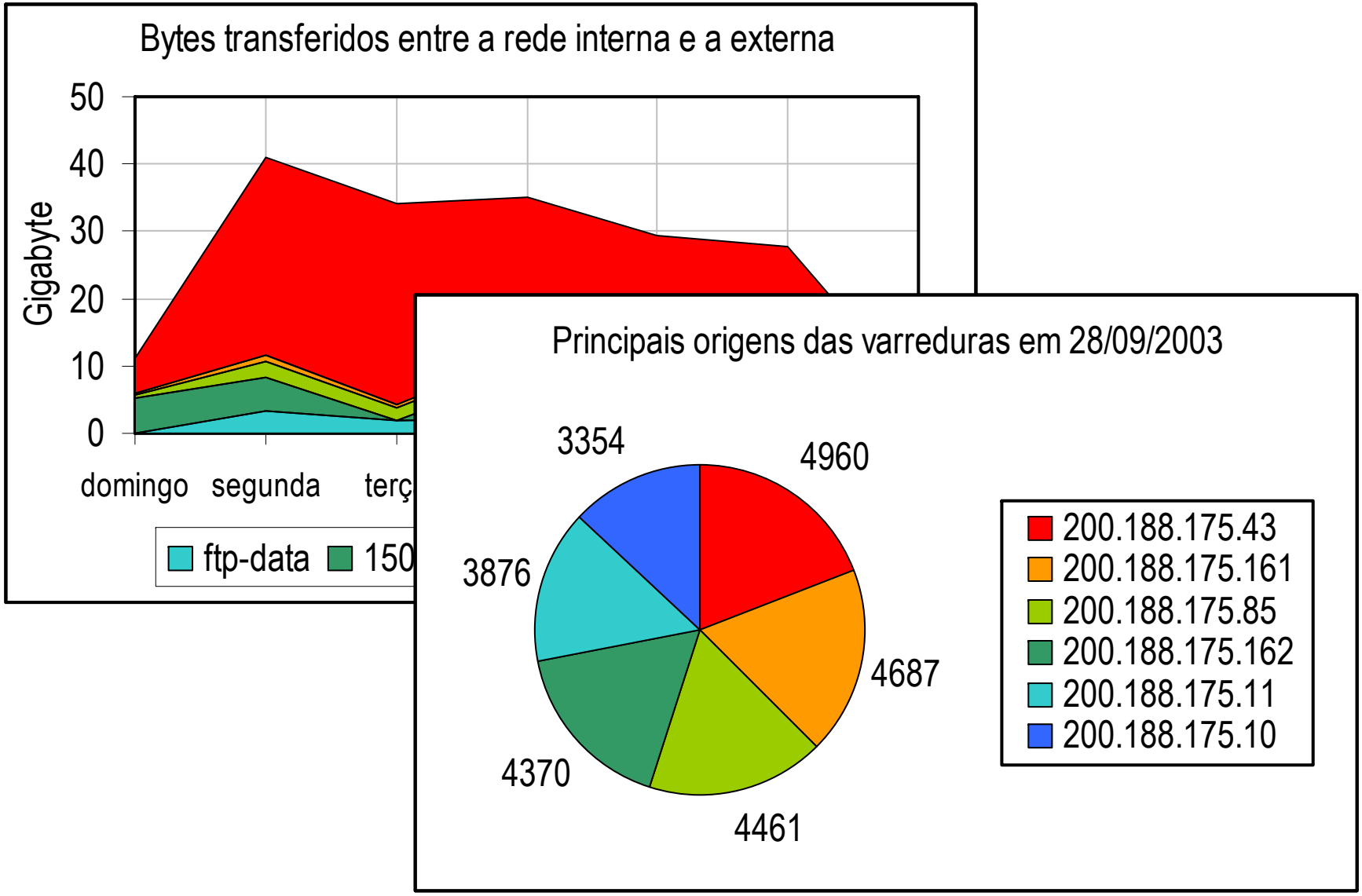
- Foi utilizada a rede acadêmica da Unisinos ≈ 4.100 computadores
- Firewall se encontra na borda dessa rede
- Foram coletados arquivos de log durante o período de uma semana

Data do *log*	Tamanho do *log* (em GB)	Eventos processados (em milhões)	Tempo de processamento (em minutos)	Tamanho acumulado da base de dados (em GB)
28/09/2003	0,69	1,30	8,1	0,15
29/09/2003	2,53	3,84	28,7	0,72
30/09/2003	2,55	3,79	28,4	1,27
01/10/2003	2,37	3,52	24,0	1,82
02/10/2003	2,28	3,58	23,6	2,31
03/10/2003	1,93	3,10	22,6	2,75
04/10/2003	0,70	1,40	9,1	2,92
Totais	13,05	20,53	144,5	2,92

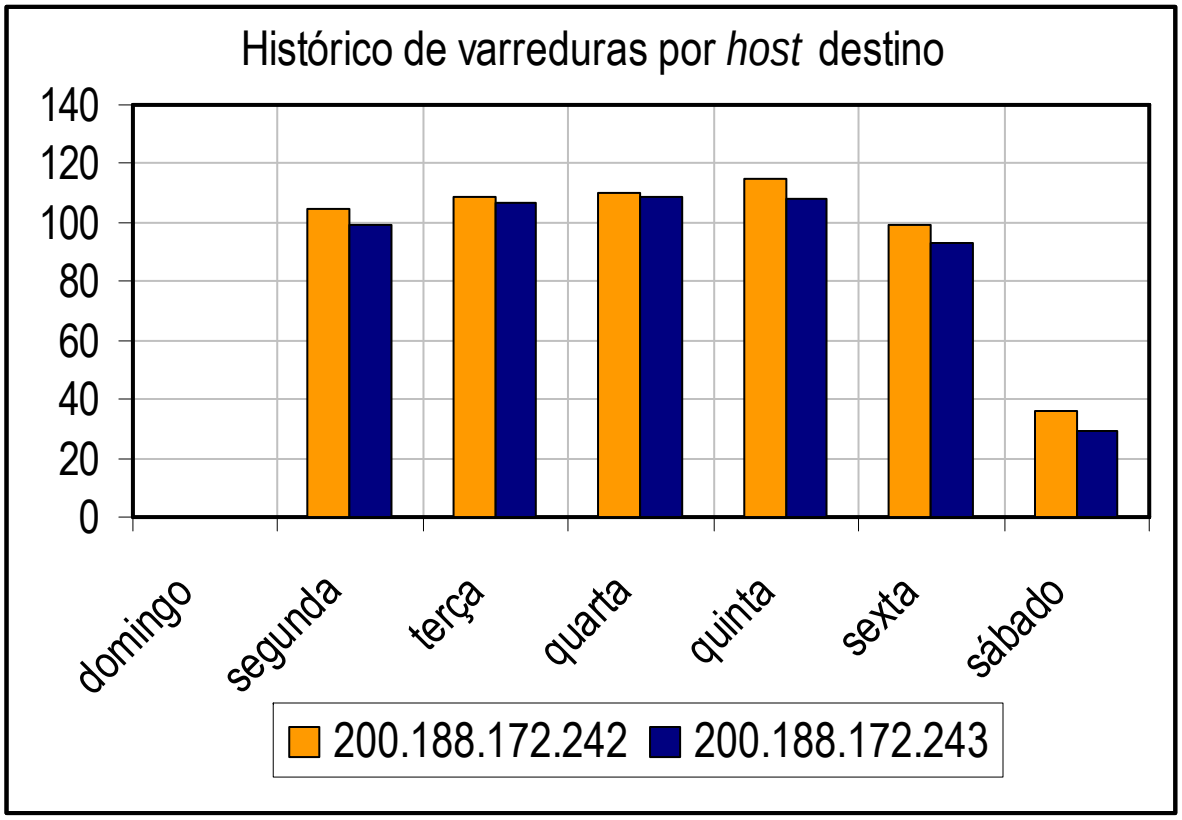
Estudo de caso



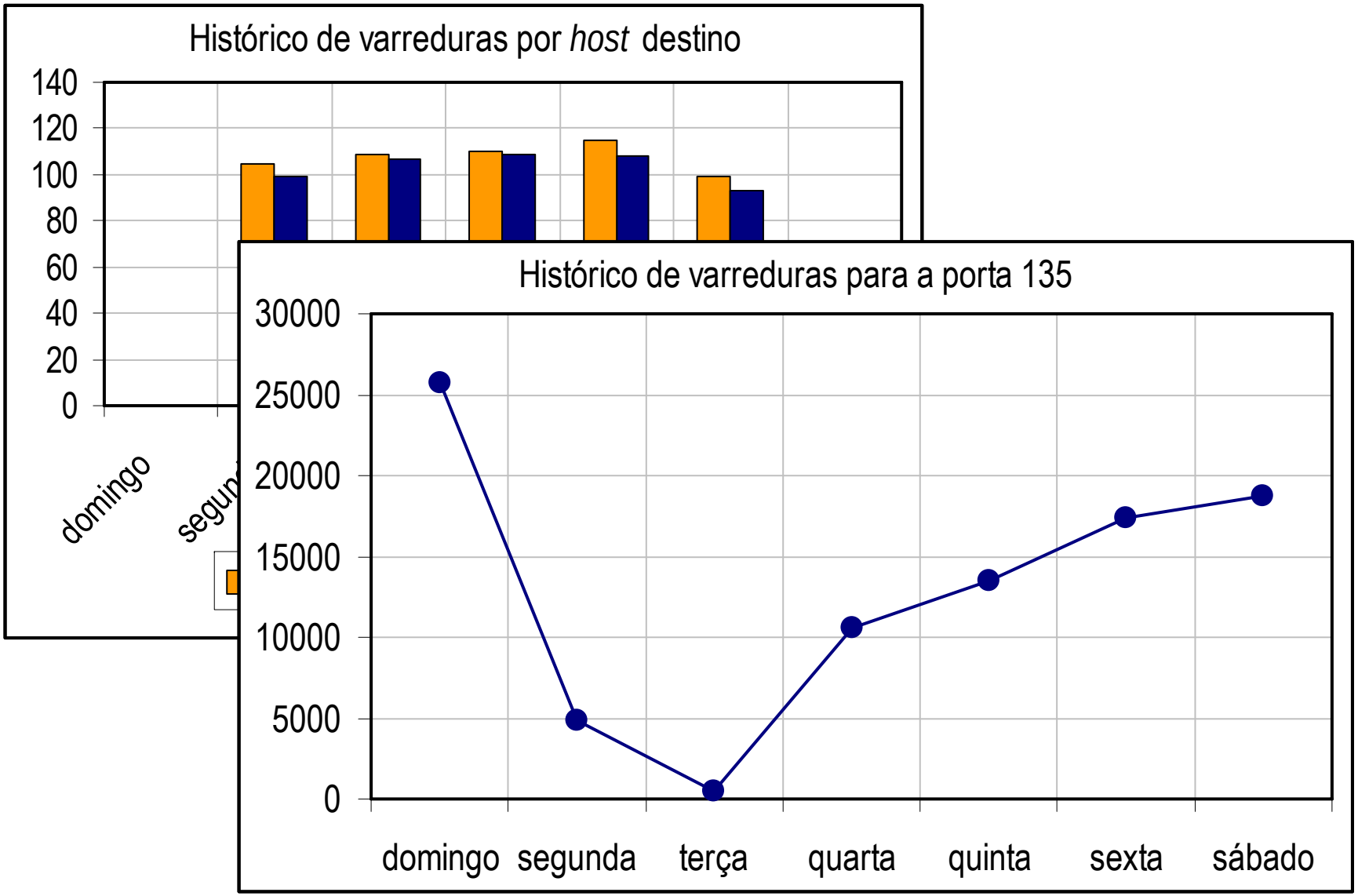
Estudo de caso



Estudo de caso



Estudo de caso



Conclusões e trabalhos futuros

- Apresentamos uma abordagem, acompanhada de uma ferramenta, para classificação, caracterização e análise de eventos gerados por *firewalls*
  - Nossa abordagem não substitui outros sistemas, como os de detecção de intrusão
- A organização da abordagem em duas partes permite manipular tanto informações quantitativas, quanto qualitativas
- O mecanismo de visualização incorporado à ferramenta é outro ponto positivo a ser destacado
- Algumas dificuldades encontradas:
  - O grande número de eventos processados e armazenados requer um tratamento especial de questões relacionadas a desempenho
  - A máquina de raciocínio precisa ser ajustada de modo a otimizar as consultas à base de dados
- Avaliação da máquina de raciocínio precisa ser realizada

Identificação de Cenários de Intrusão pela Classificação, Caracterização e Análise de Eventos gerados por Firewalls

Fábio Elias Locatelli[1]
Fabiane Dillenburg[1]
Cristina Melchiors[2]
Luciano Paschoal Gaspary[2]

[1]Universidade do Vale do Rio dos Sinos (UNISINOS)
[2]Universidade Federal do Rio Grande do Sul (UFRGS)

paschoal@inf.ufrgs.br
http://www.inf.ufrgs.br/~paschoal

7a. Reunião do Grupo de Trabalho em Segurança de Redes (GTS-7)
27 de junho de 2006 – Porto Alegre