Sistema de Monitoramento Remoto de Segurança

Tiago Barabasz[1,2] Vitor Monte Afonso[1,2] Antonio Montes[1]

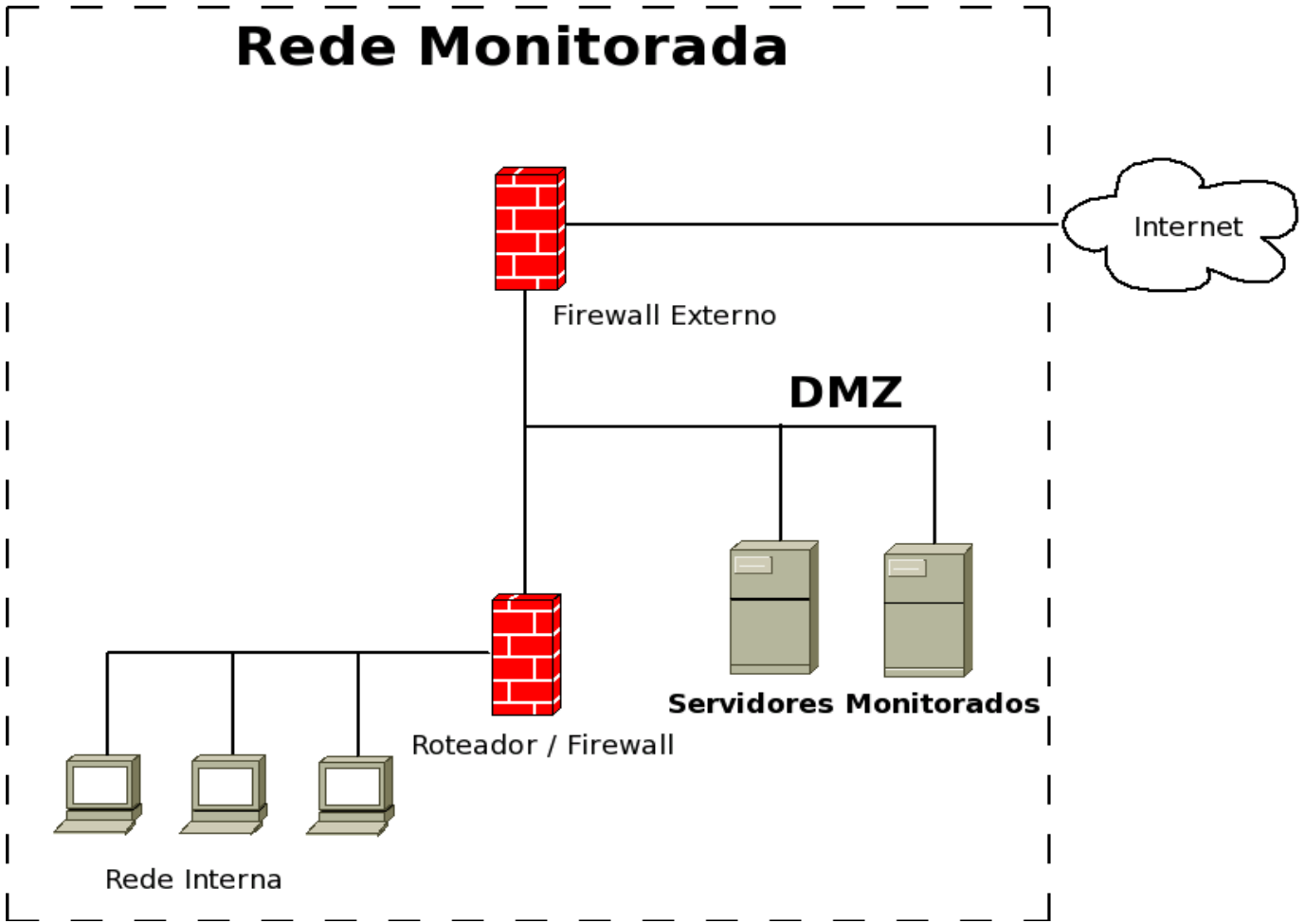
[1]Cenpra - Divisão de Segurança de Sistemas de Informação
[2]Universidade Estadual de Campinas

GTS-10 2007

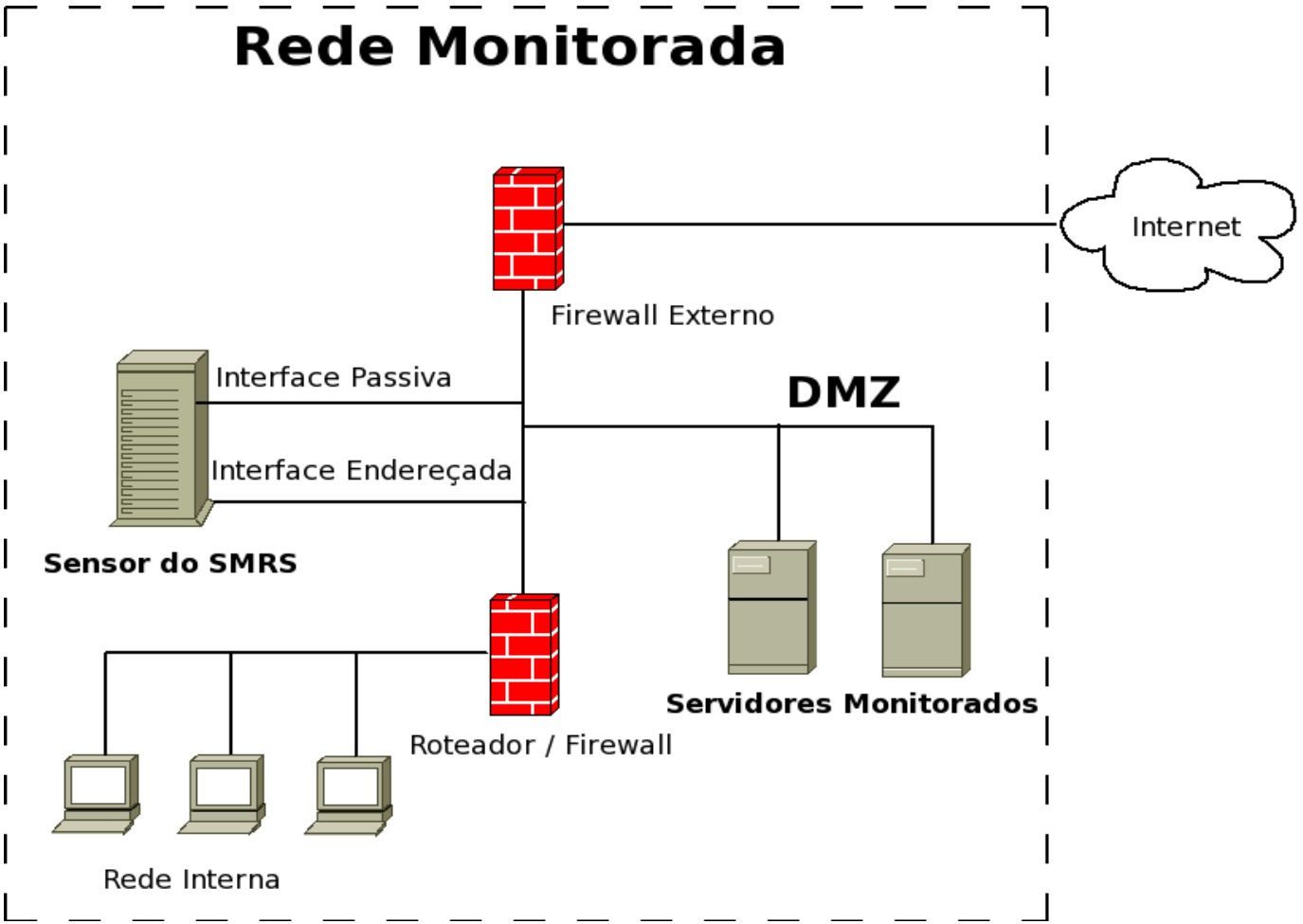
Introdução

- Motivação
  - Prover sistema de monitoramento remoto de redes, que permita a analistas detectar problemas de segurança

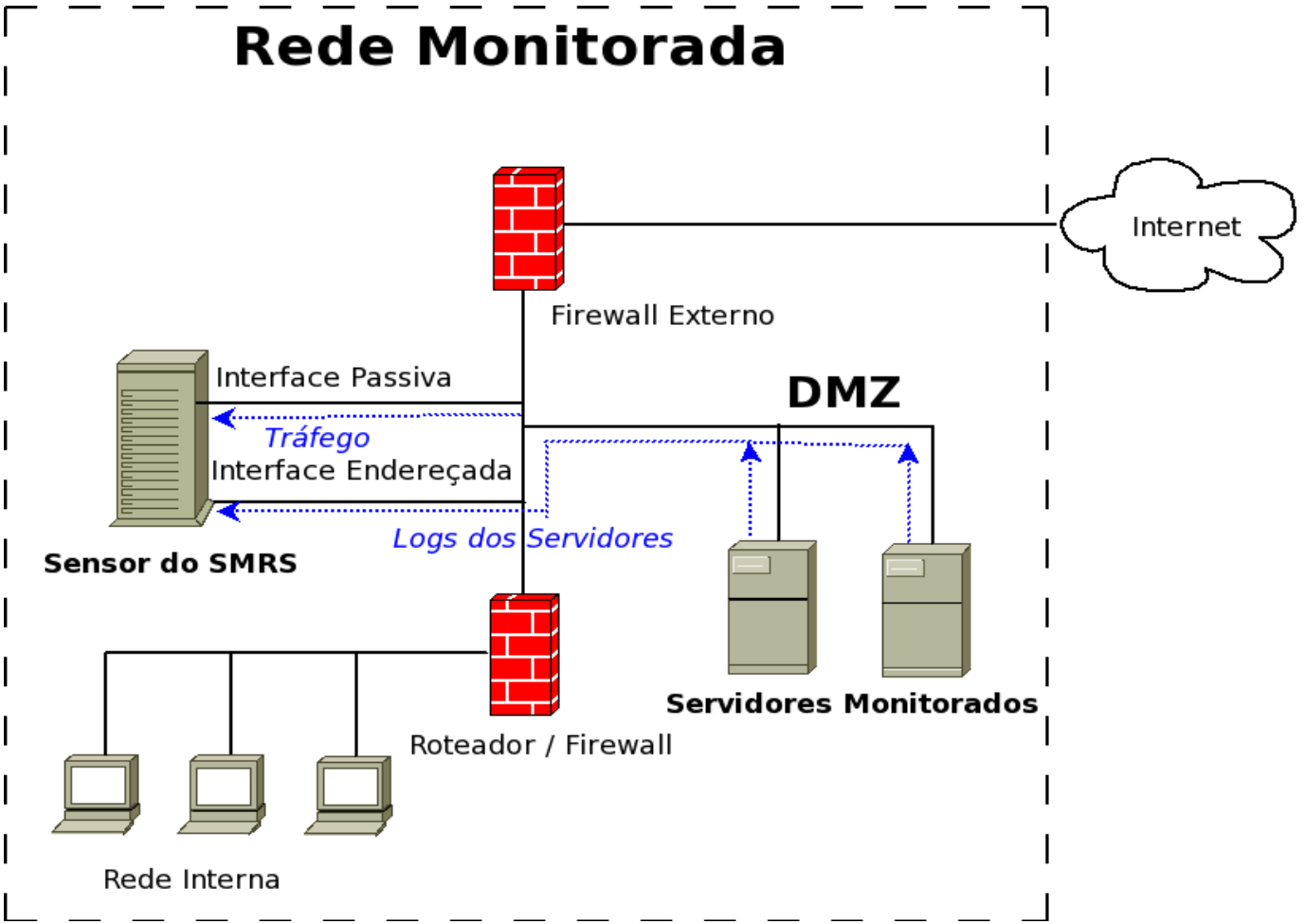
Estrutura


Rede Monitorada
Internet
Firewall Externo
DMZ
Servidores Monitorados
Roteador / Firewall
Rede Interna

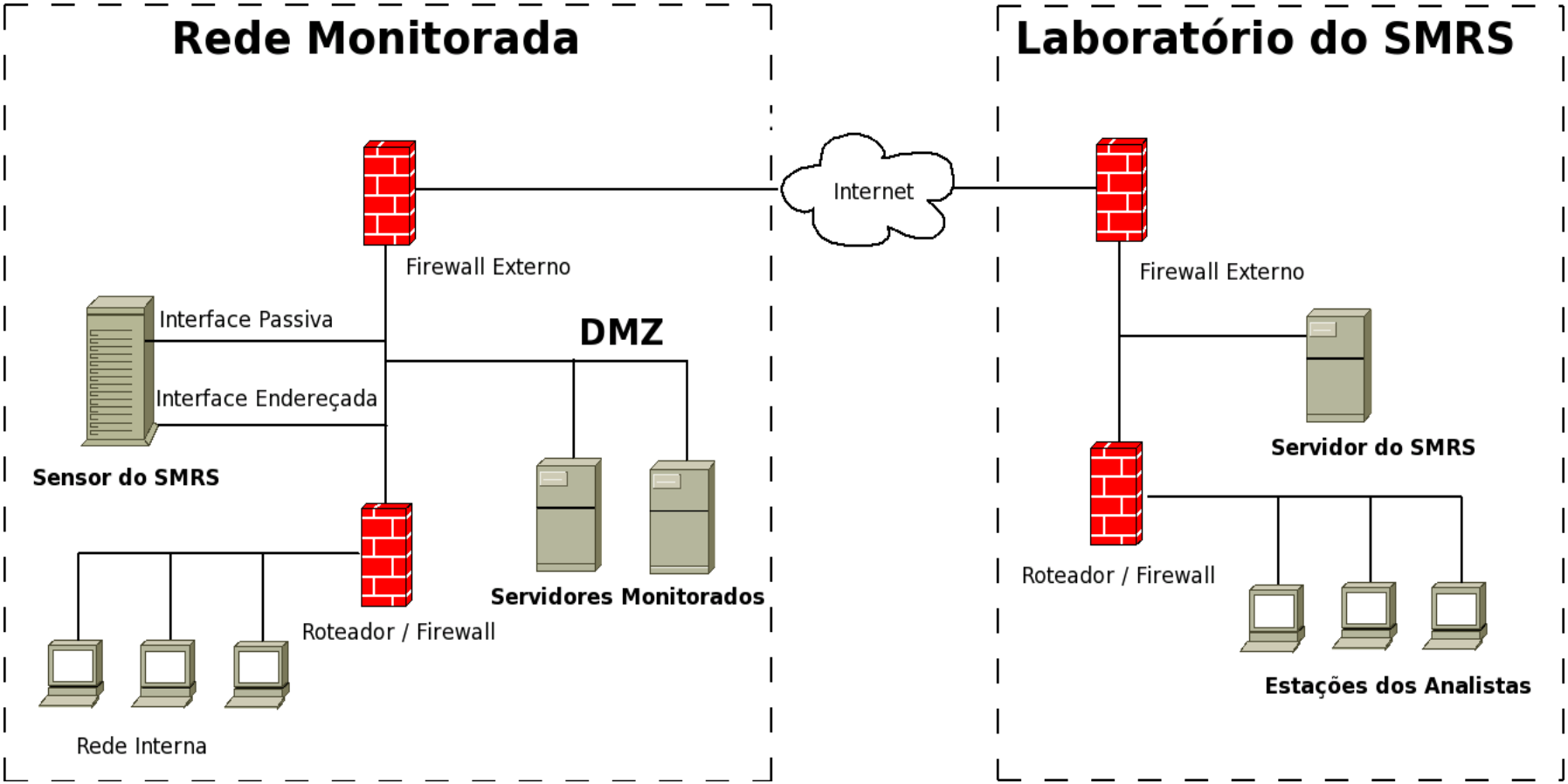
Estrutura


Rede Monitorada
Internet
Firewall Externo
Interface Passiva
DMZ
Interface Endereçada
Sensor do SMRS
Servidores Monitorados
Roteador / Firewall
Rede Interna

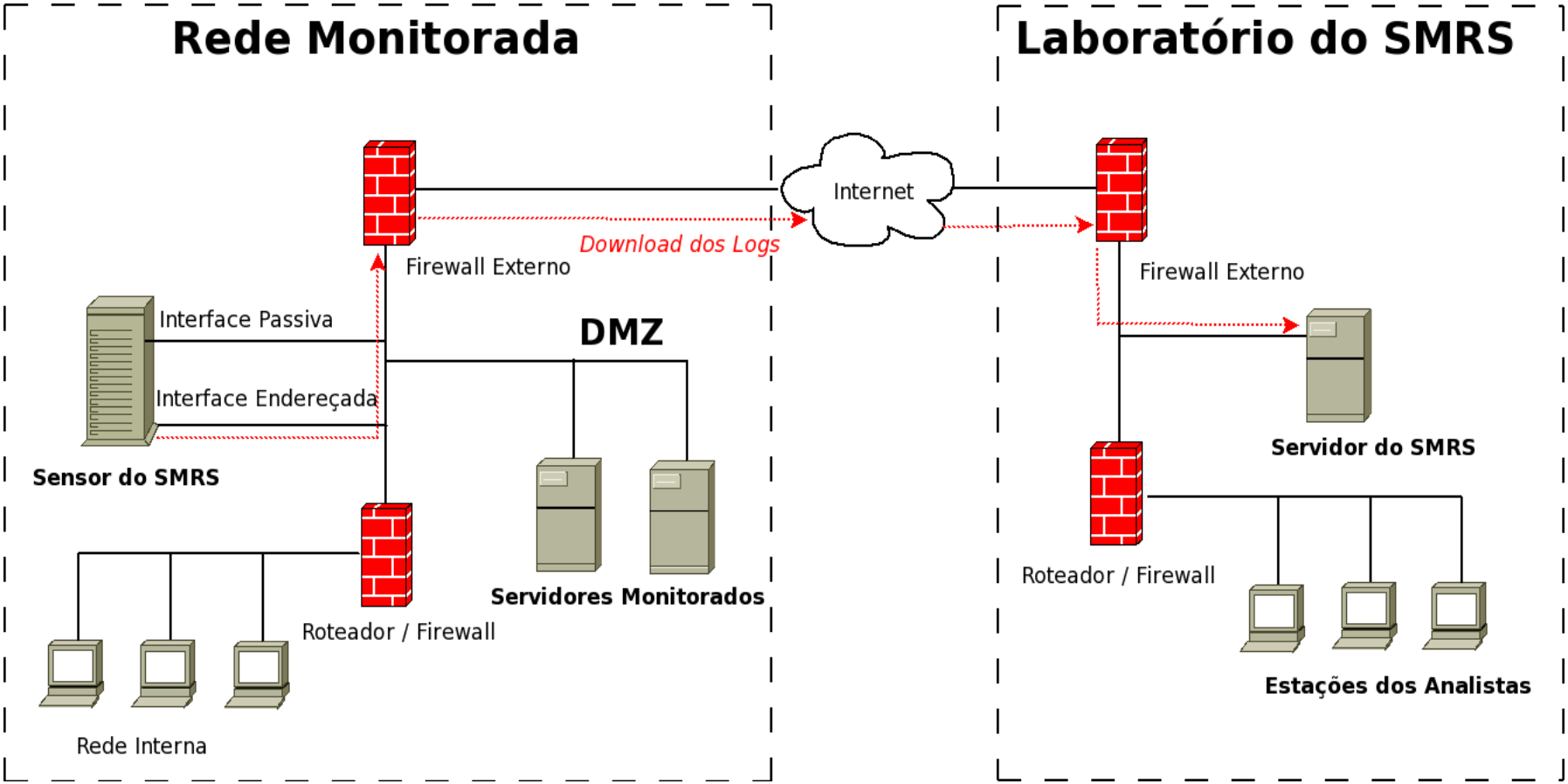
Estrutura


Rede Monitorada
Internet
Firewall Externo
Interface Passiva
DMZ
Tráfego
Interface Endereçada
Logs dos Servidores
Sensor do SMRS
Servidores Monitorados
Roteador / Firewall
Rede Interna

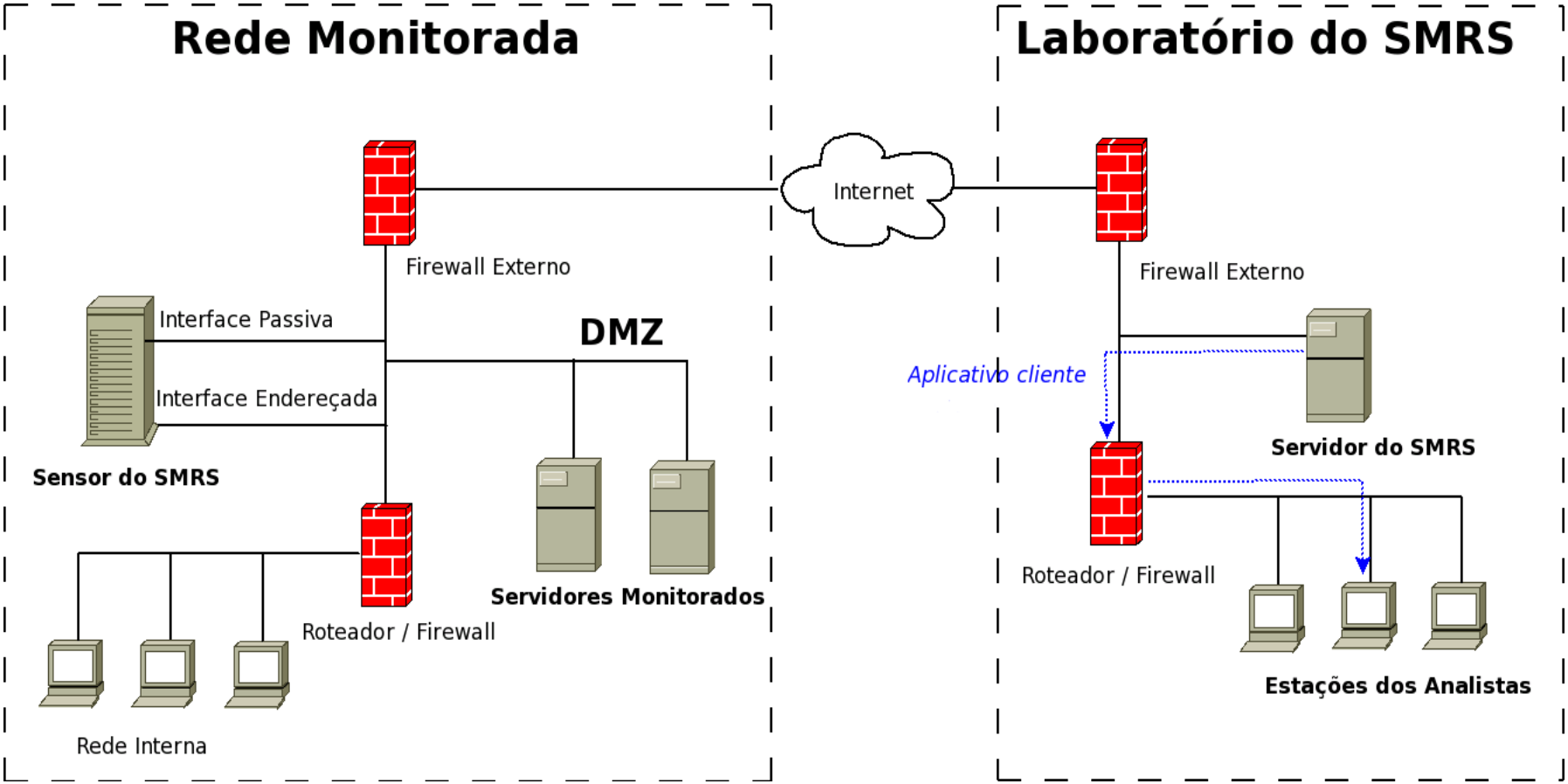
Estrutura


Rede Monitorada
Laboratório do SMRS
Internet
Firewall Externo
Interface Passiva
Interface Endereçada
DMZ
Sensor do SMRS
Servidores Monitorados
Roteador / Firewall
Rede Interna
Firewall Externo
Servidor do SMRS
Roteador / Firewall
Estações dos Analistas

Estrutura


Rede Monitorada
Laboratório do SMRS
Internet
Download dos Logs
Firewall Externo
Interface Passiva
Interface Endereçada
DMZ
Sensor do SMRS
Servidores Monitorados
Roteador / Firewall
Rede Interna
Firewall Externo
Servidor do SMRS
Roteador / Firewall
Estações dos Analistas

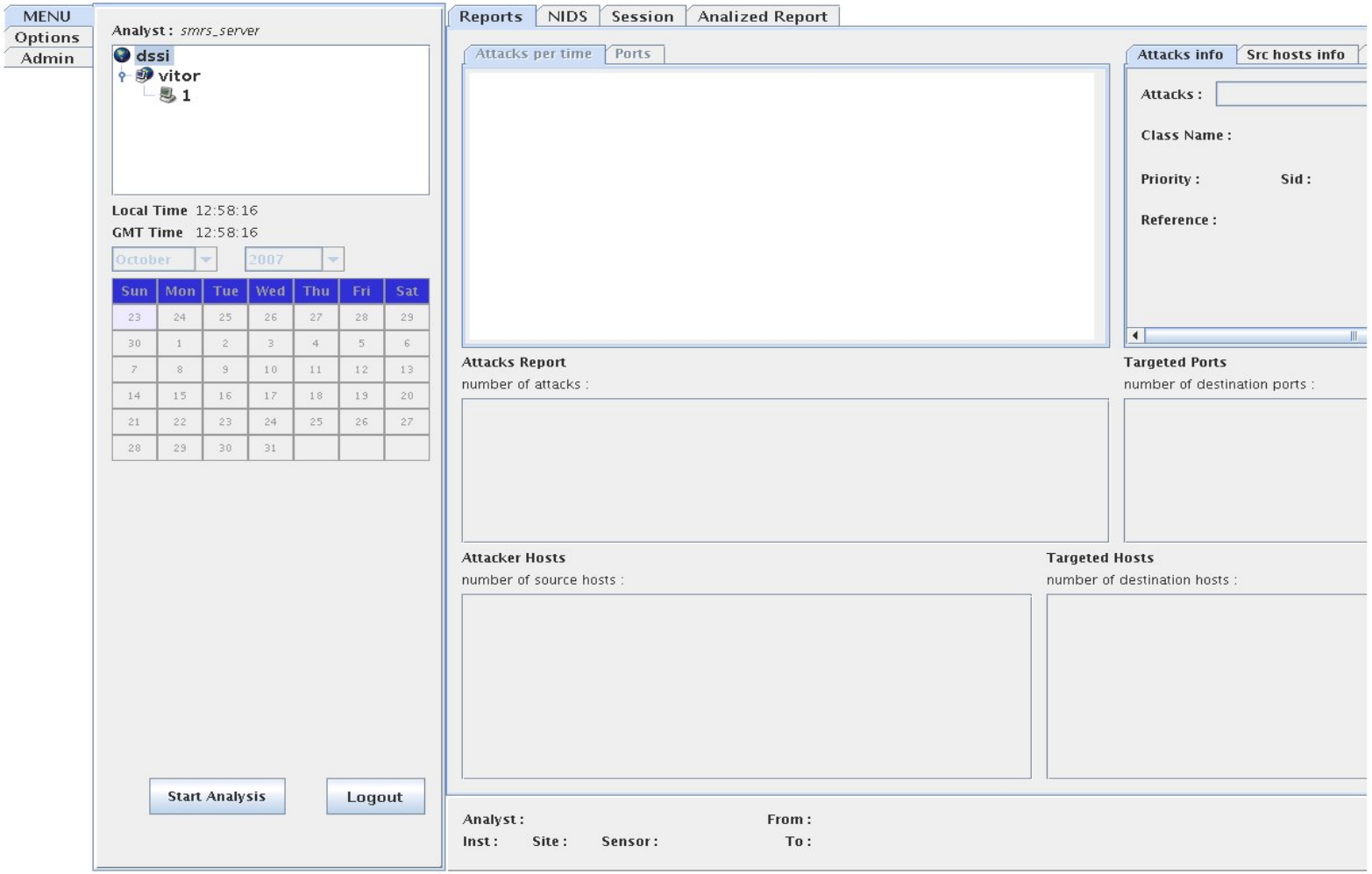
Estrutura


Rede Monitorada
Laboratório do SMRS
Internet
Firewall Externo
Interface Passiva
DMZ
Interface Endereçada
Sensor do SMRS
Servidores Monitorados
Roteador / Firewall
Rede Interna
Firewall Externo
Aplicativo cliente
Servidor do SMRS
Roteador / Firewall
Estações dos Analistas

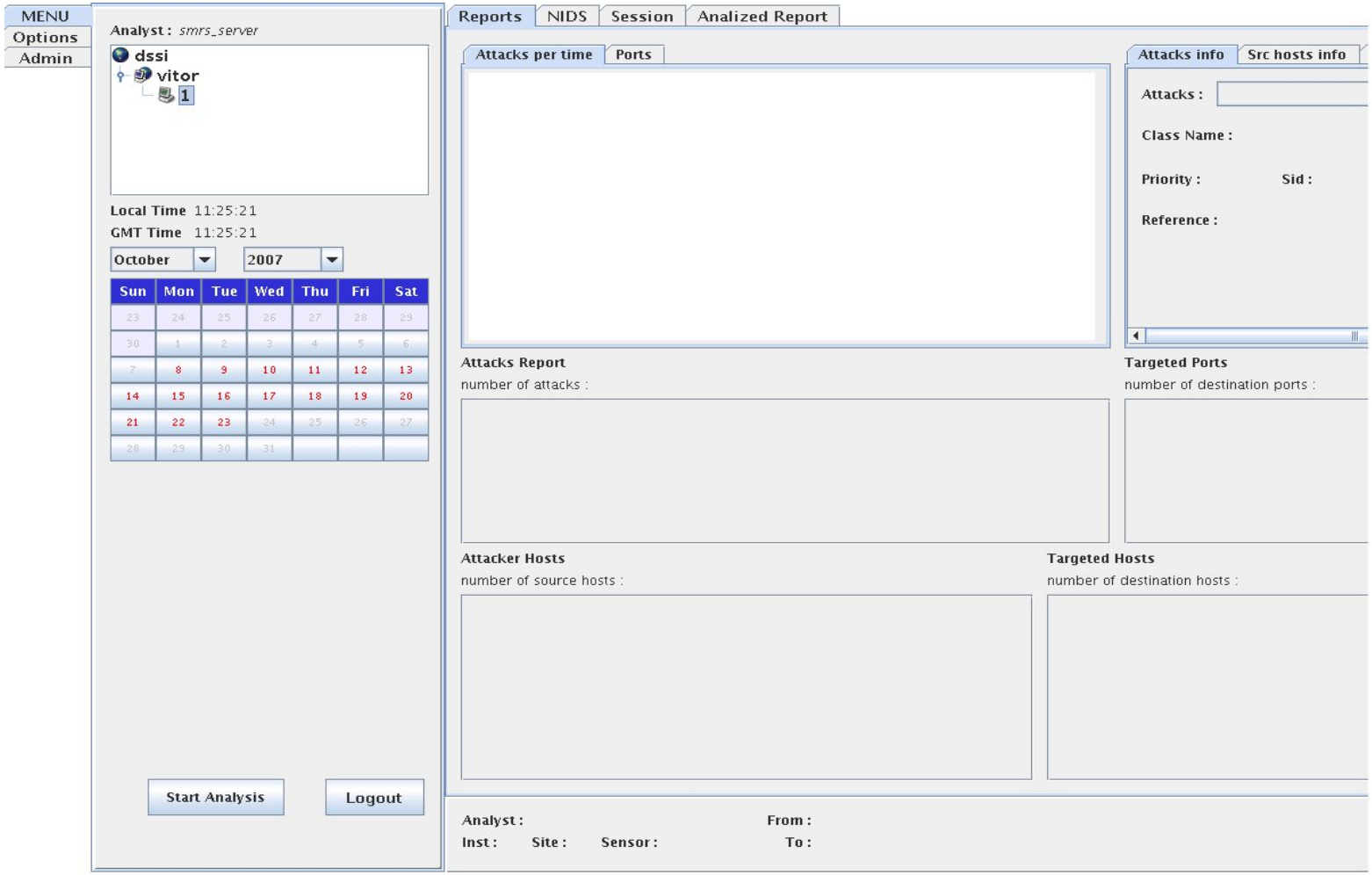
Processo de análise

- Seleção de escopo
- Visualização de relatórios estatísticos
- Verificação de alertas de segurança
- Geração de relatórios

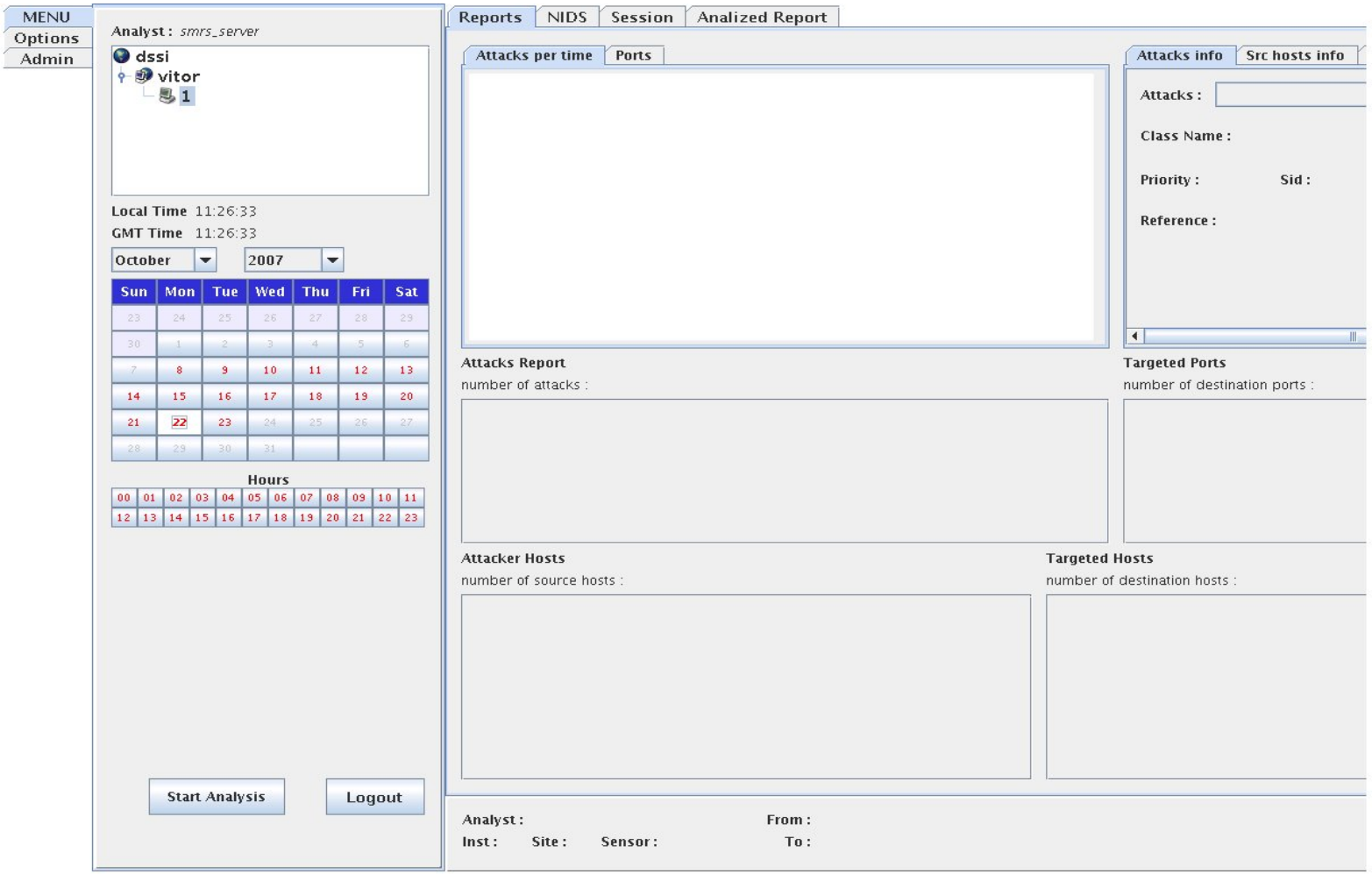
Seleção de escopo



Seleção de escopo



Seleção de escopo



Visualização de relatórios estatísticos

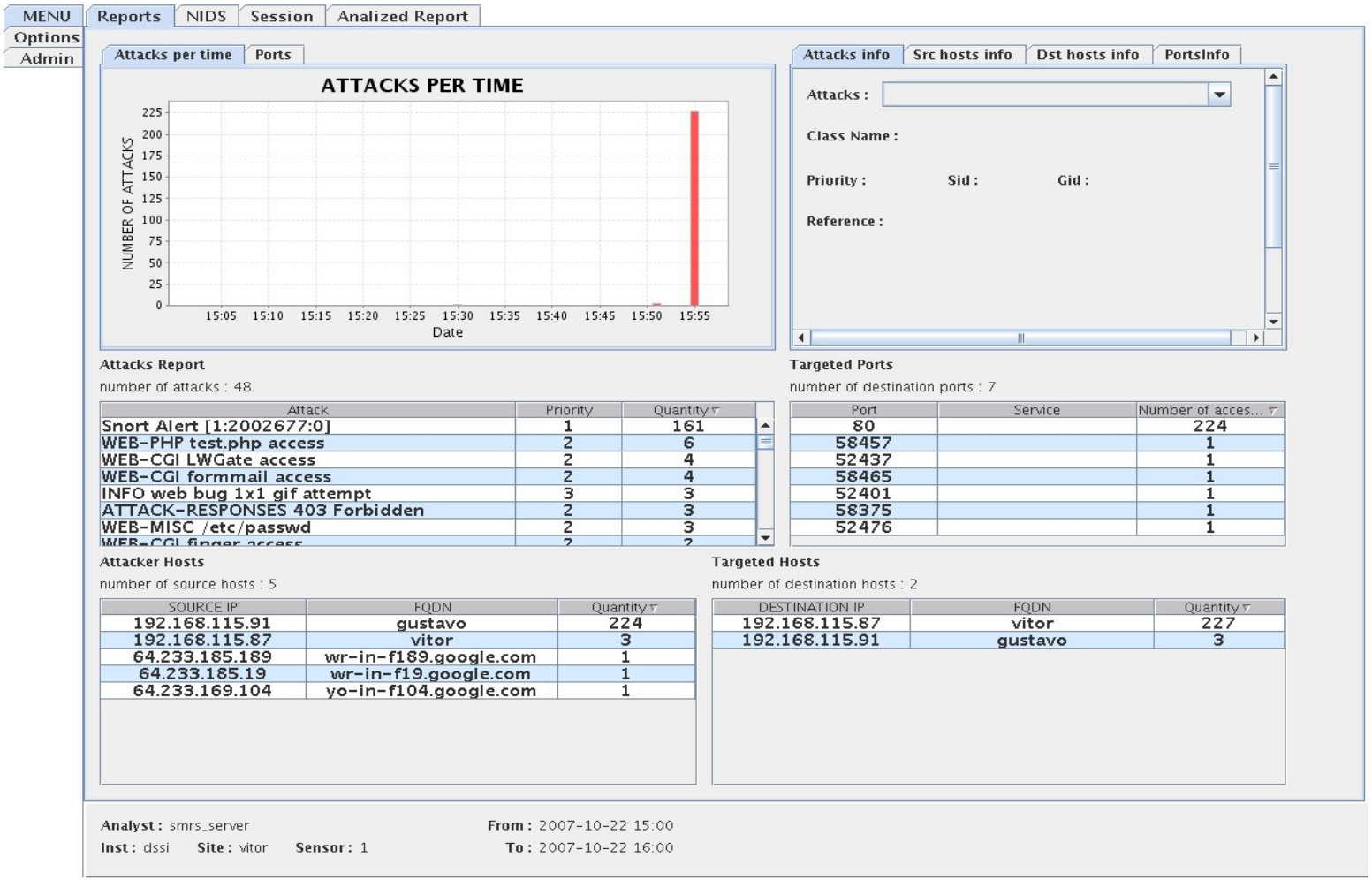
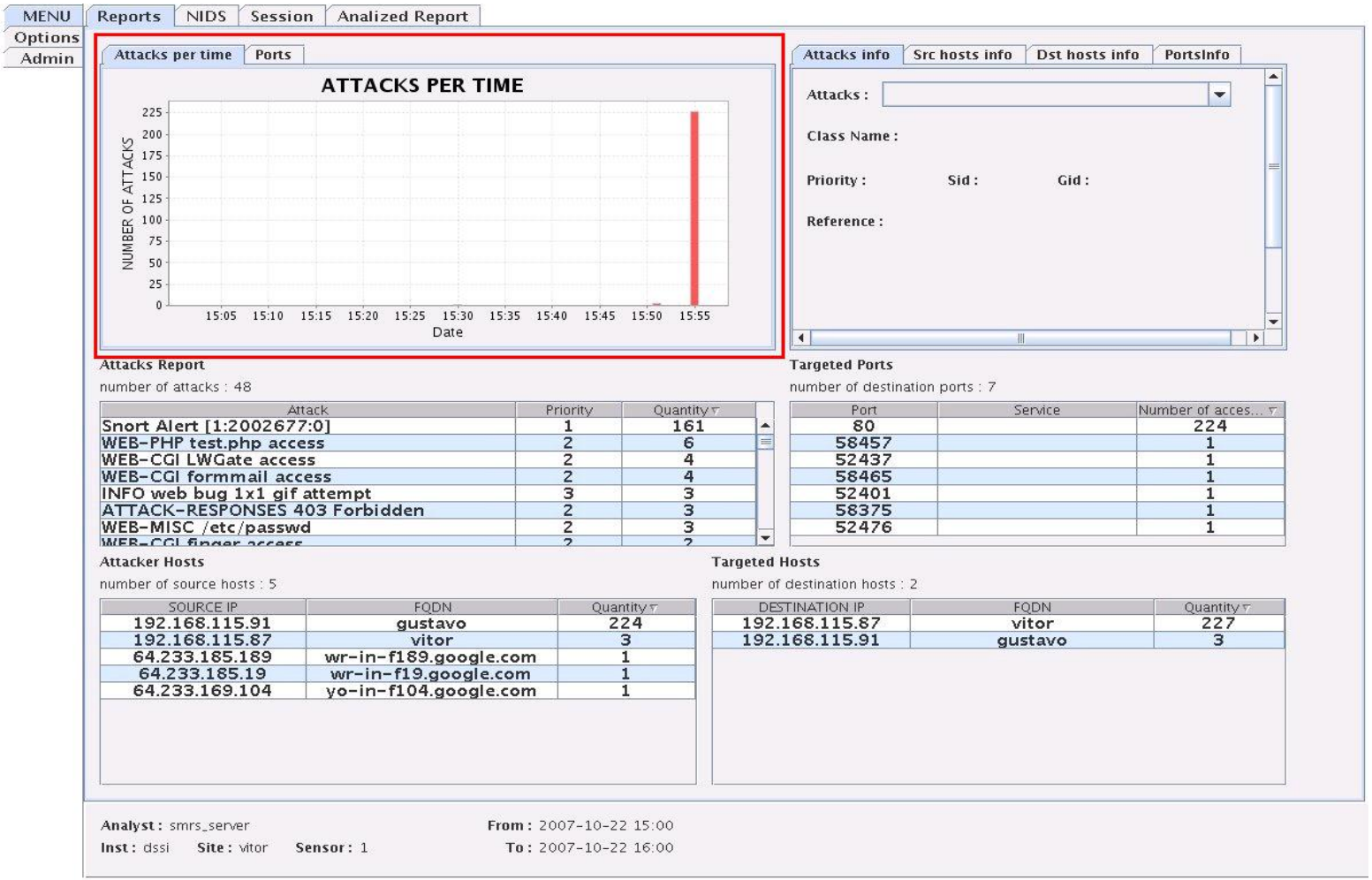


Gráfico de alertas X tempo



Informações extras

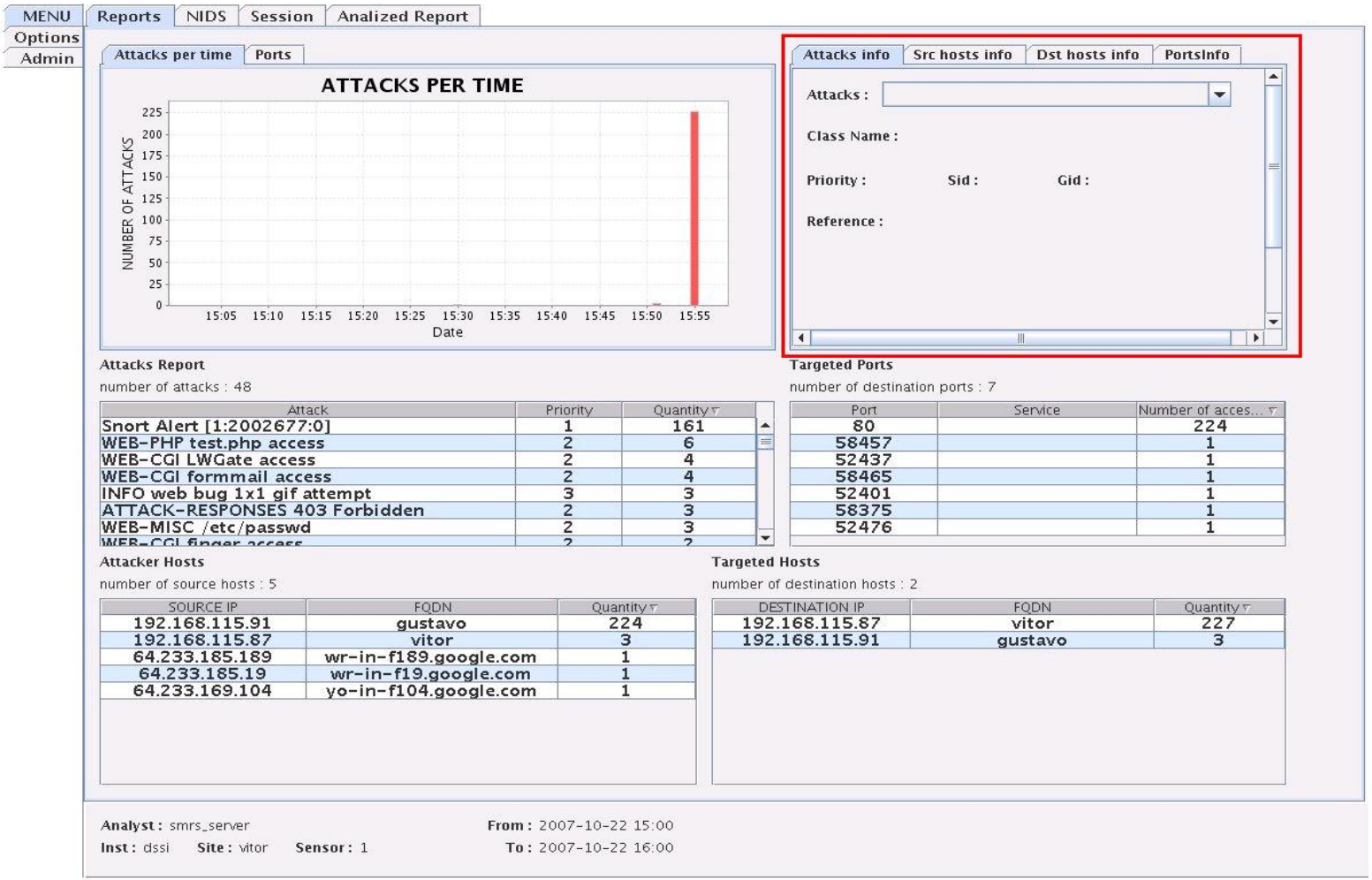


Tabela com alertas

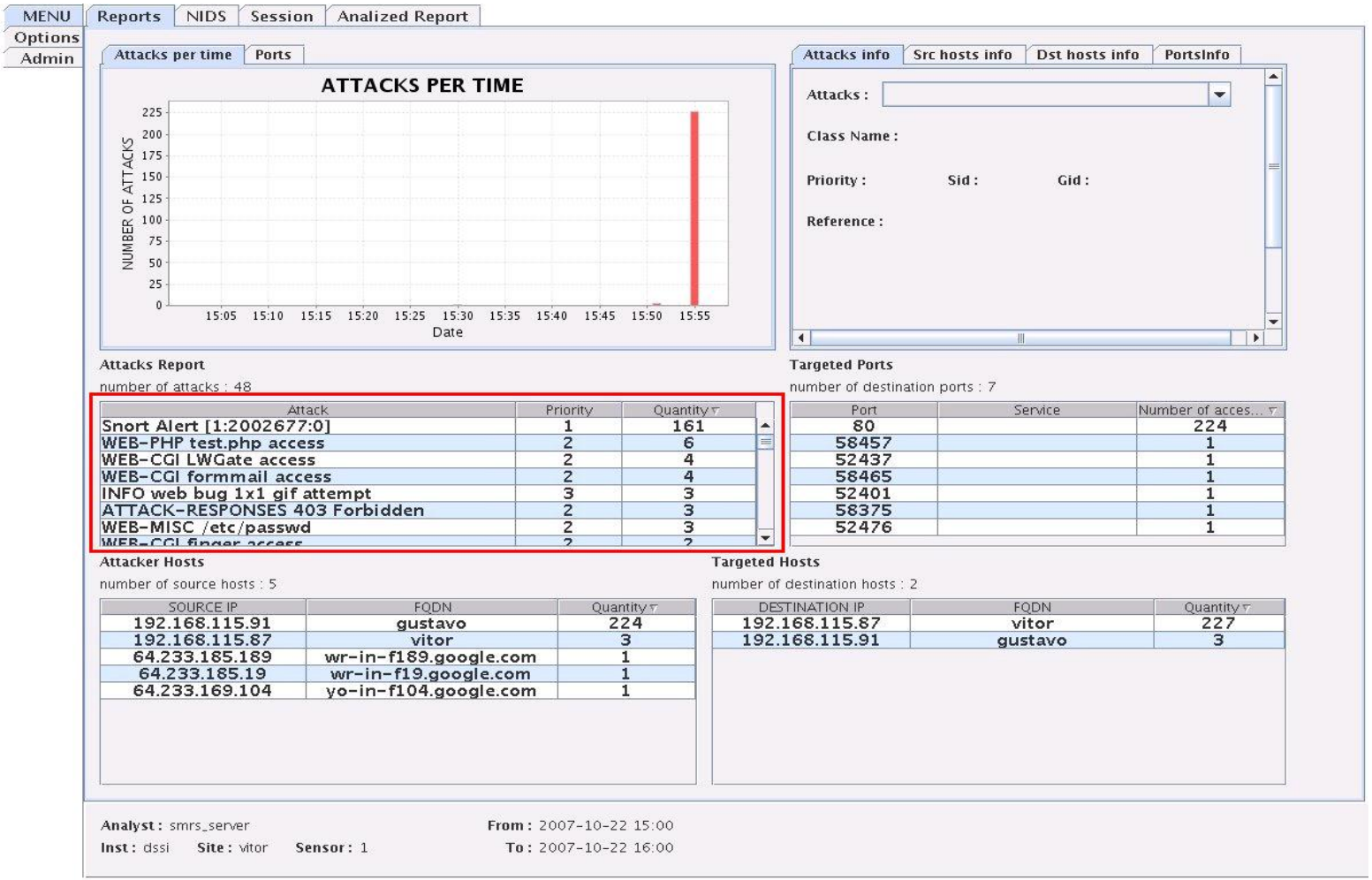


Tabela com portas de destino

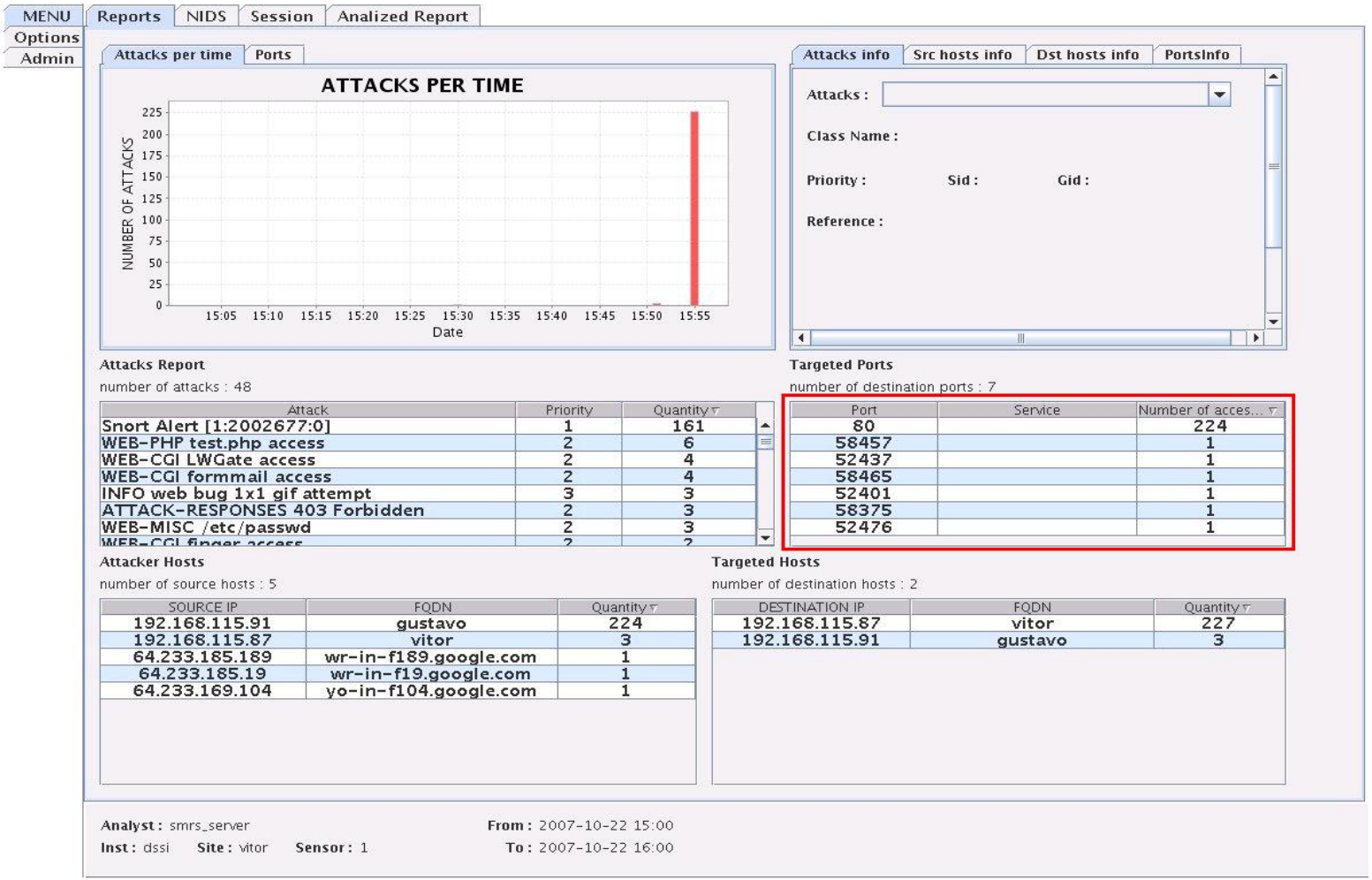


Tabela com endereços de origem

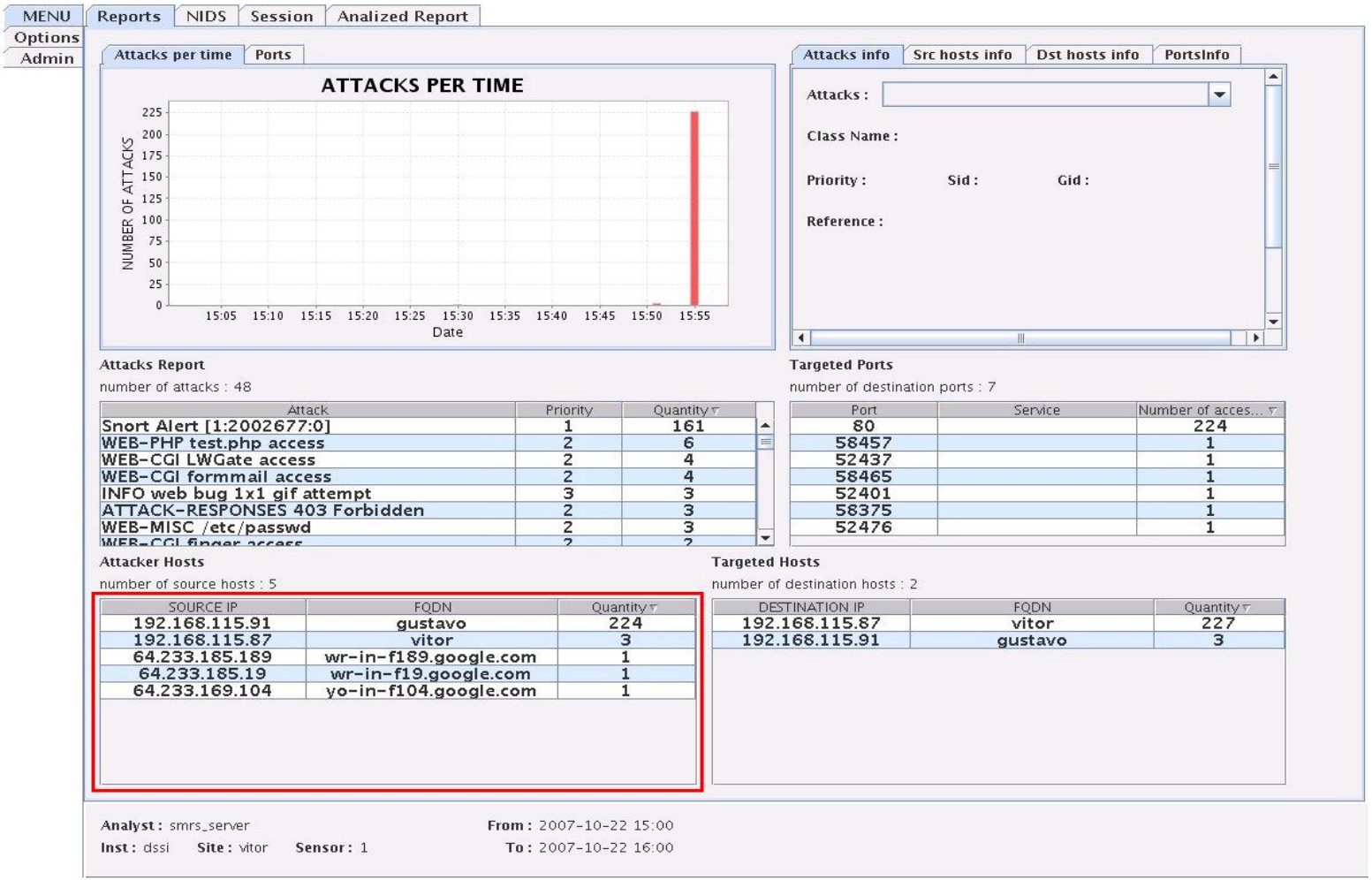
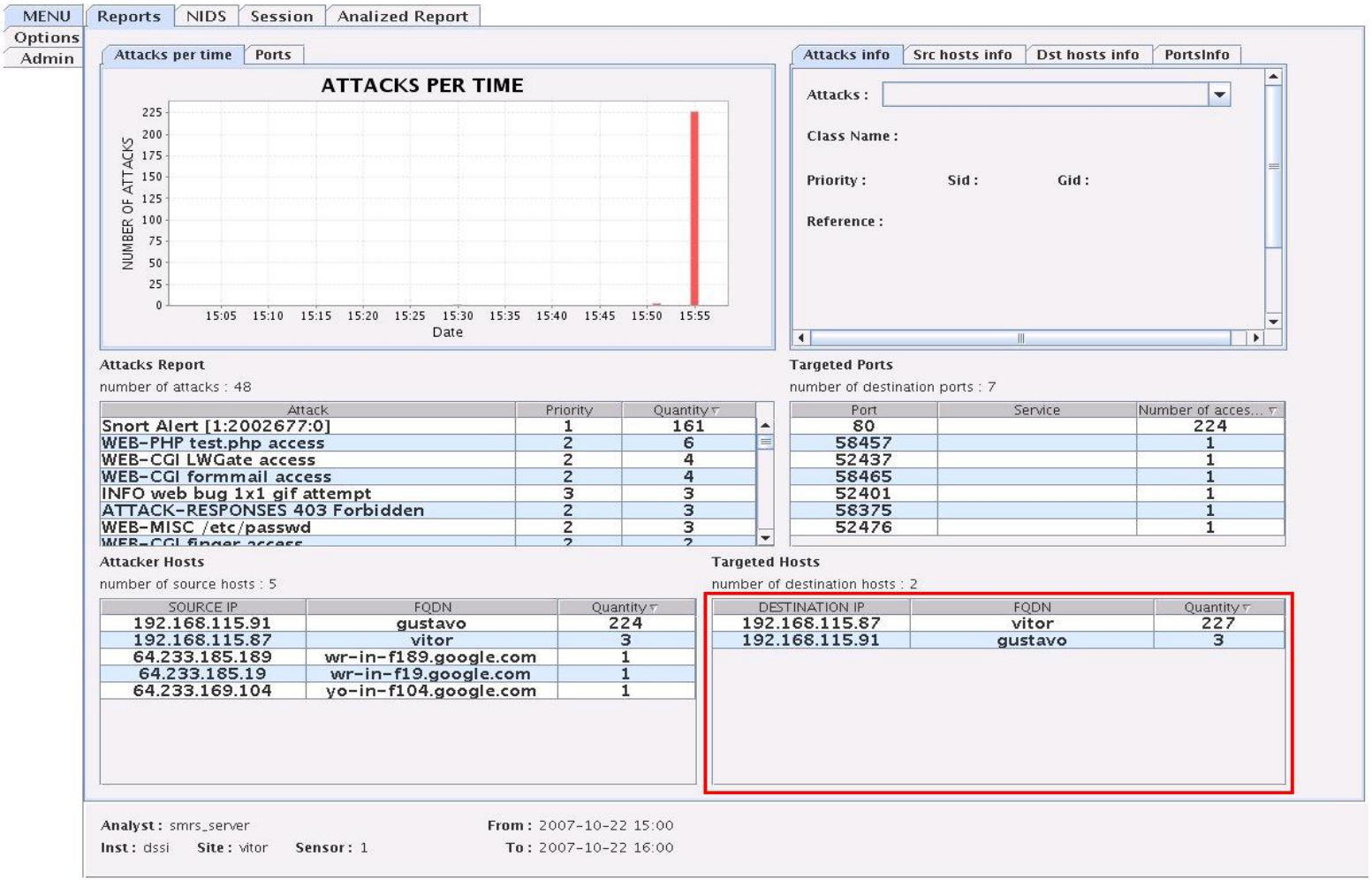
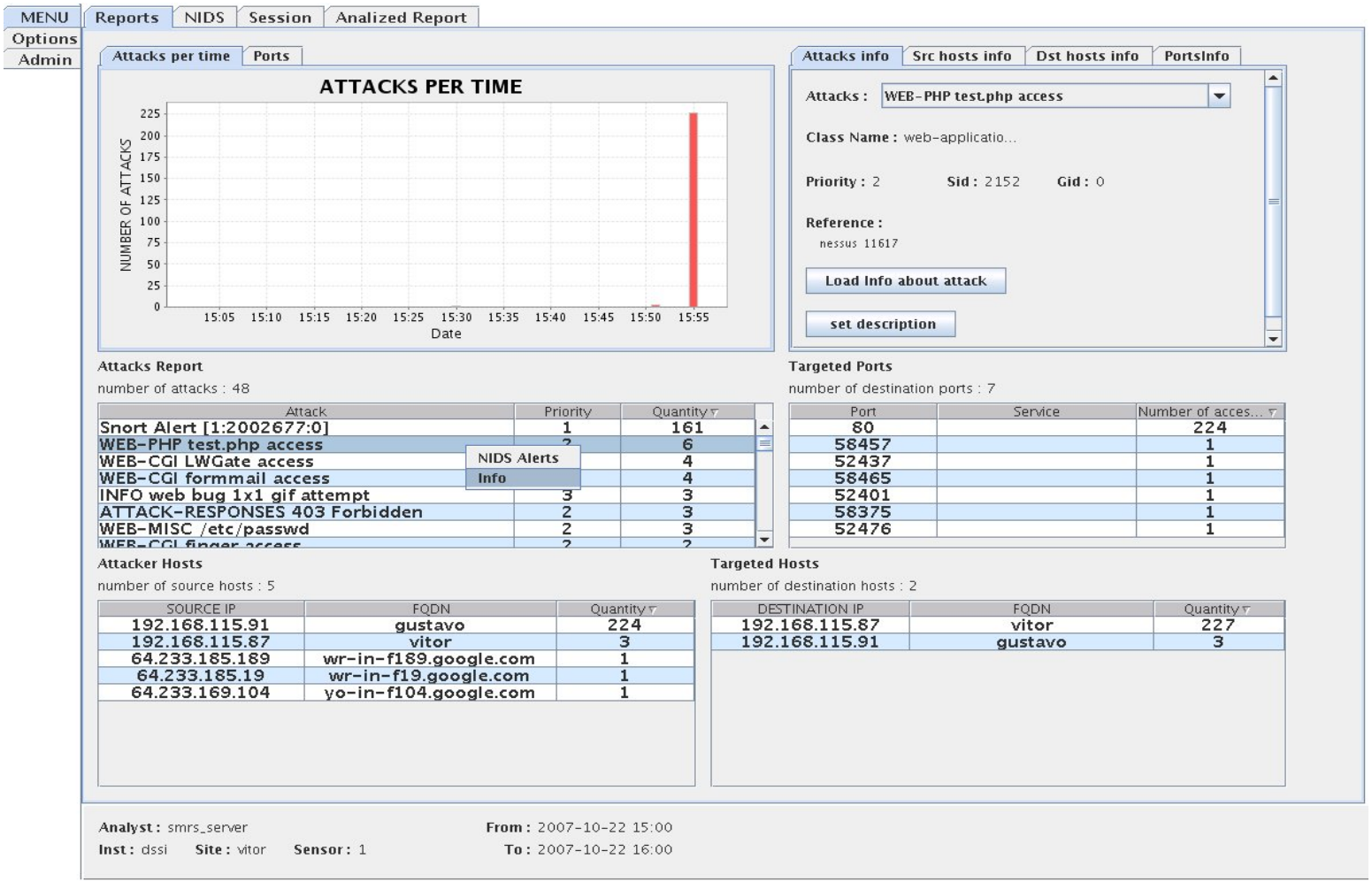


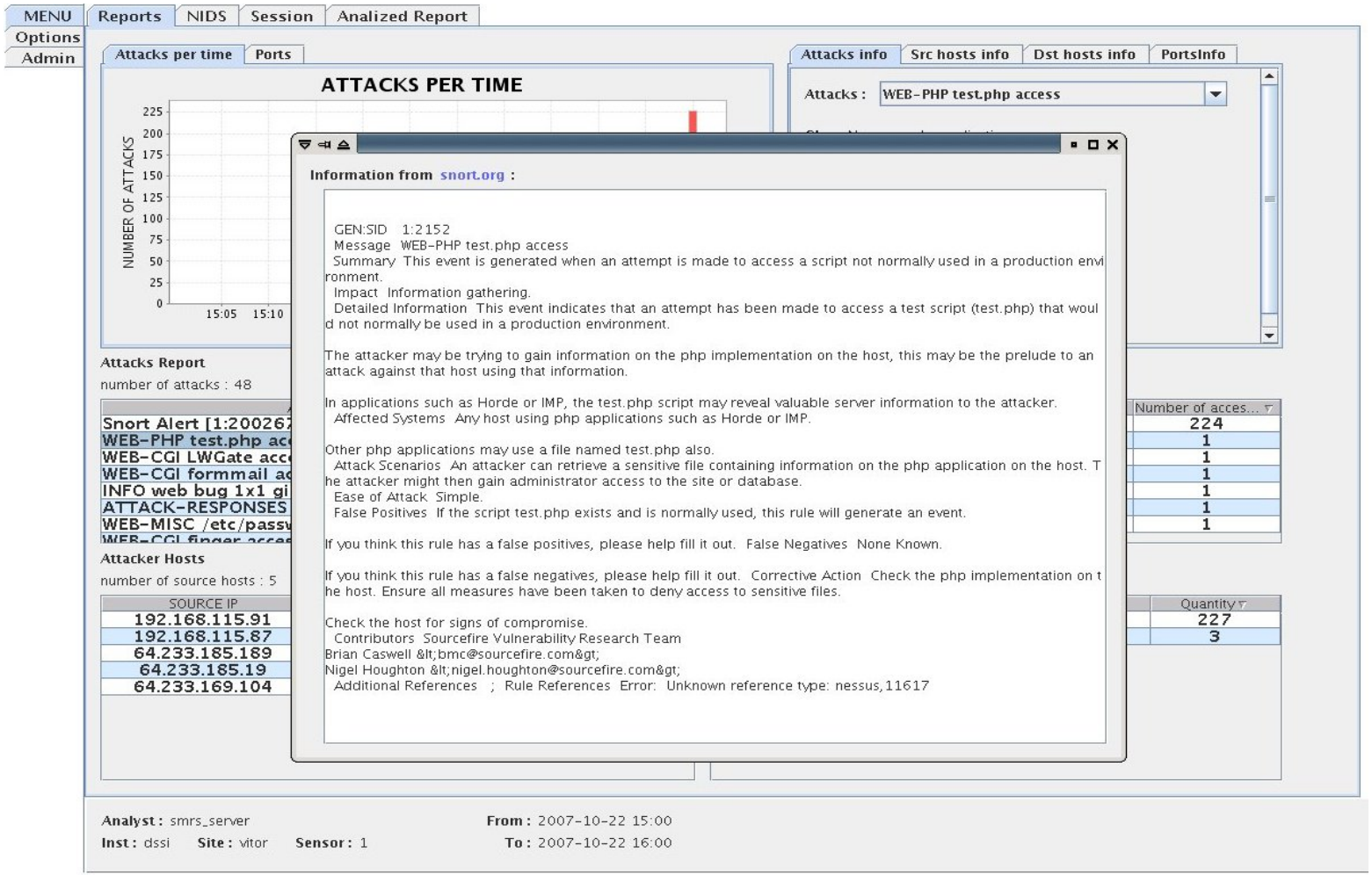
Tabela com endereços de destino



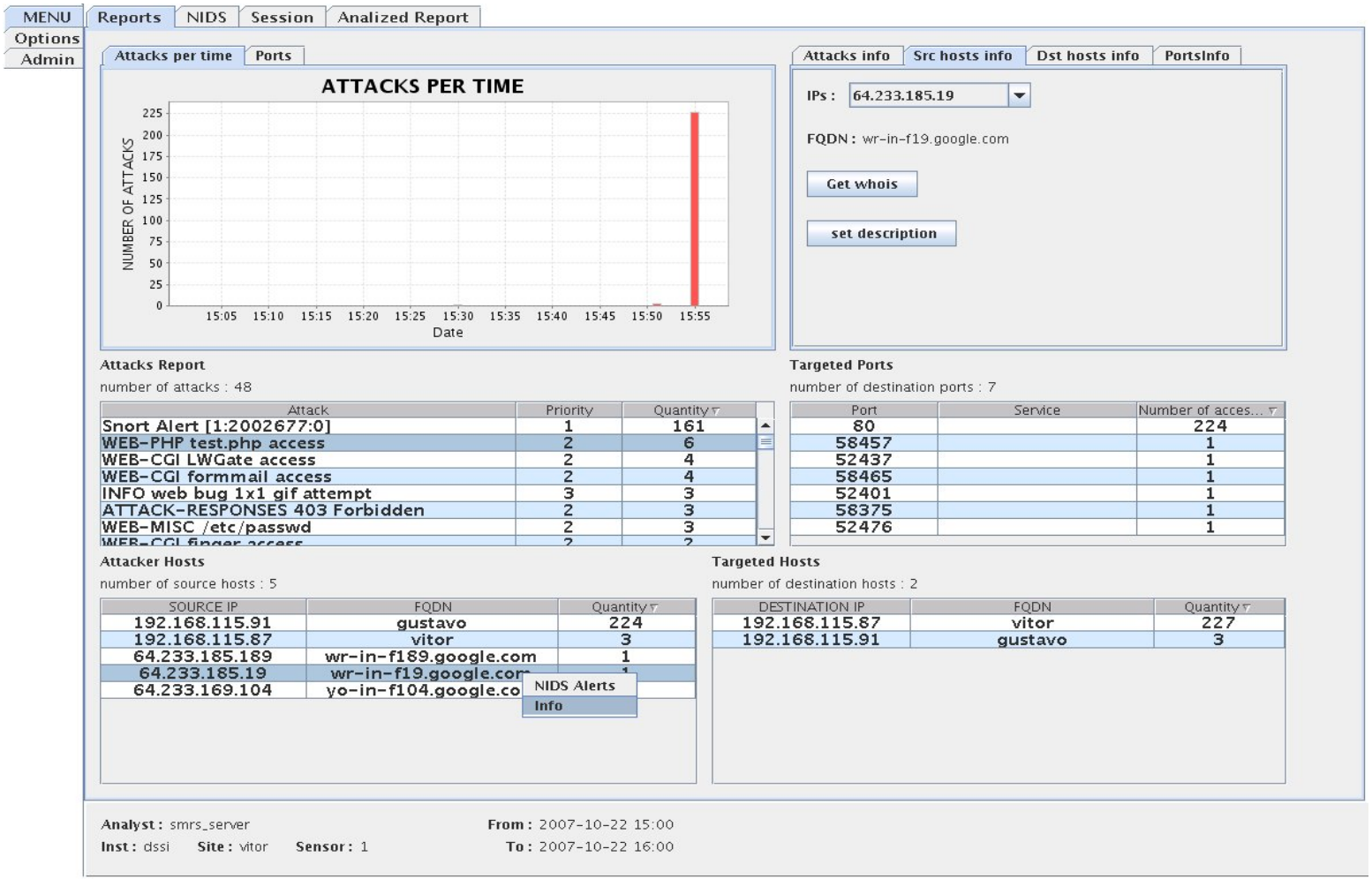
Informações sobre determinado alerta



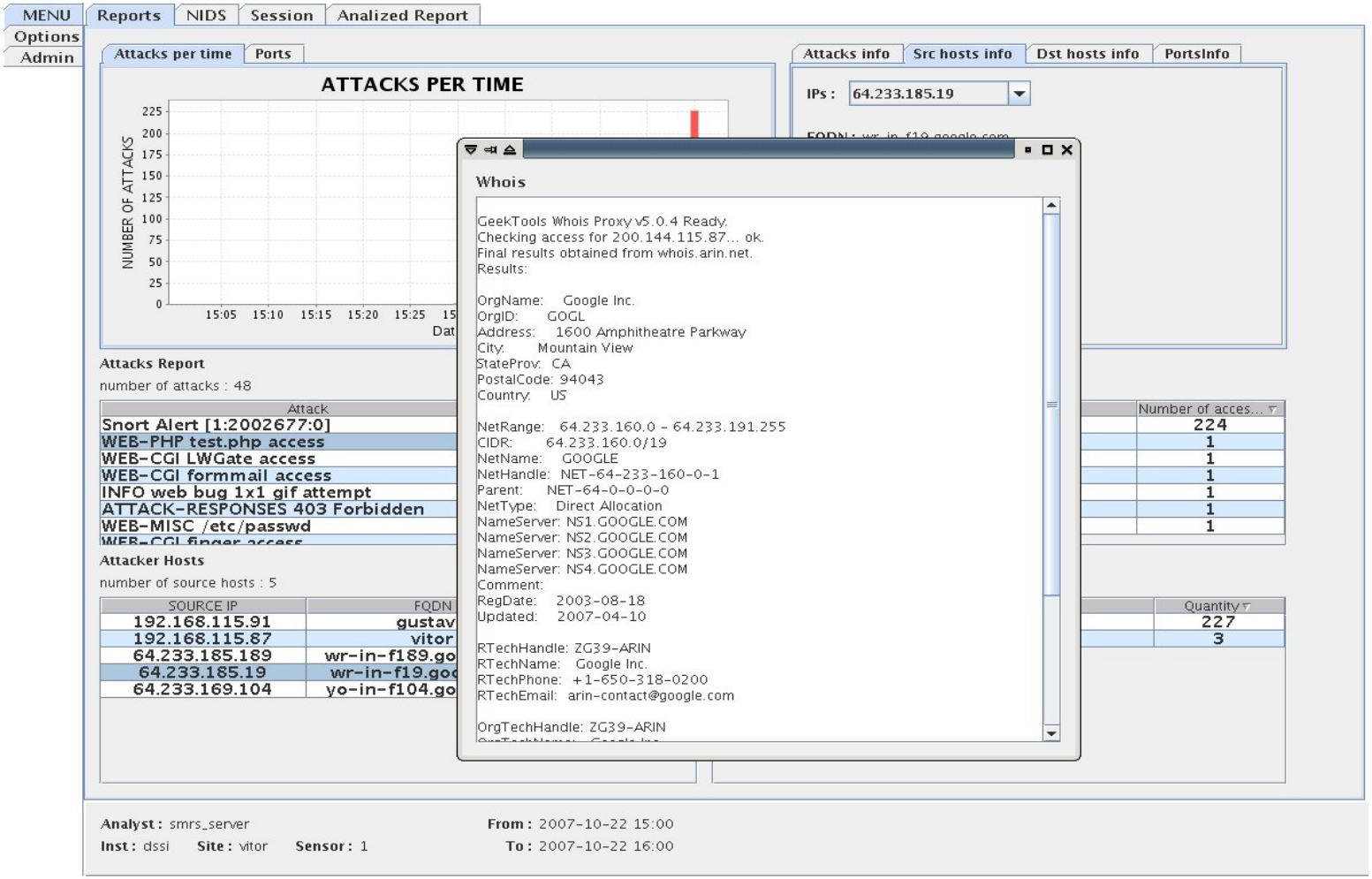
Informações do snort.org sobre o alerta



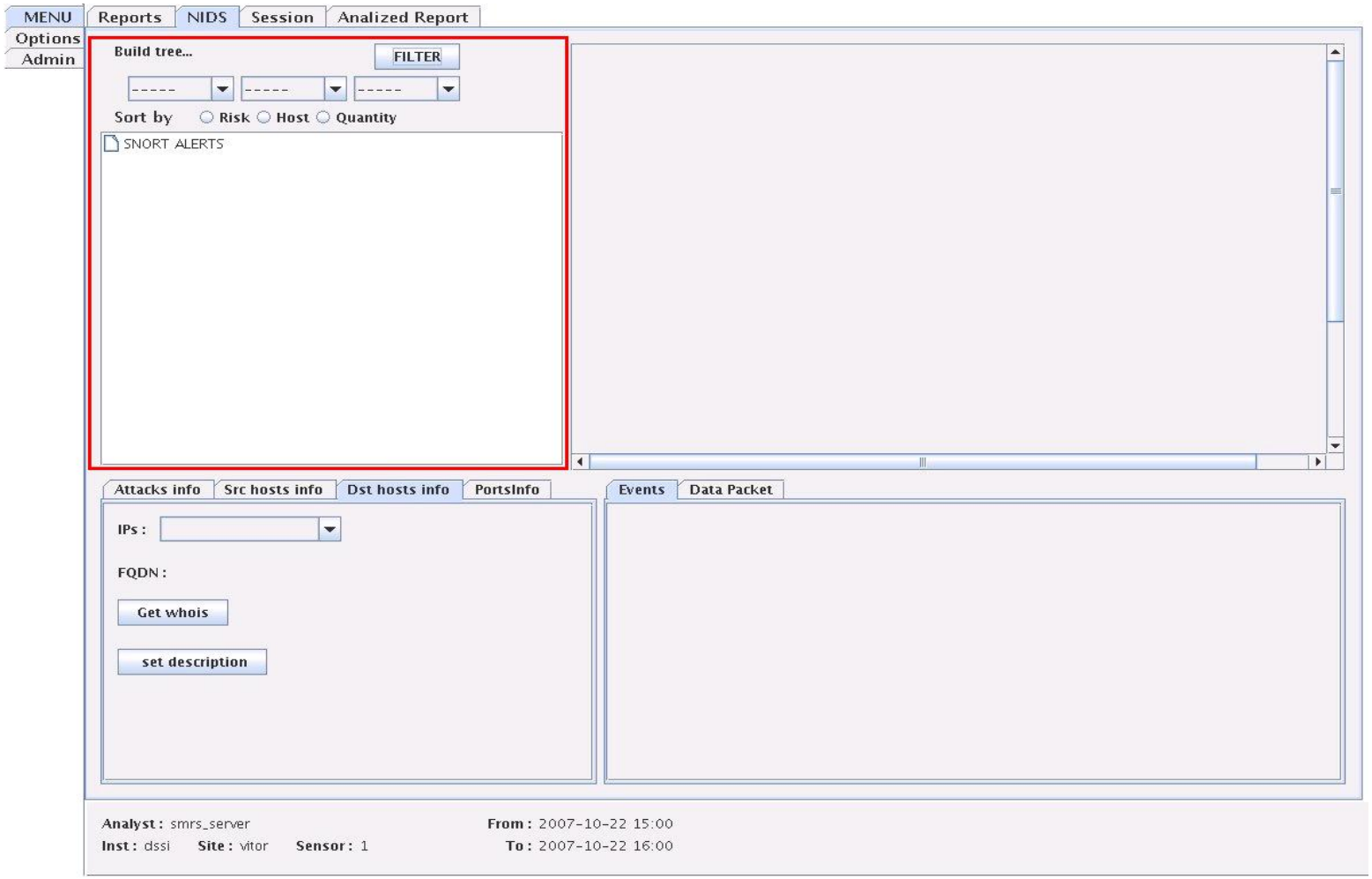
Informações sobre determinado host



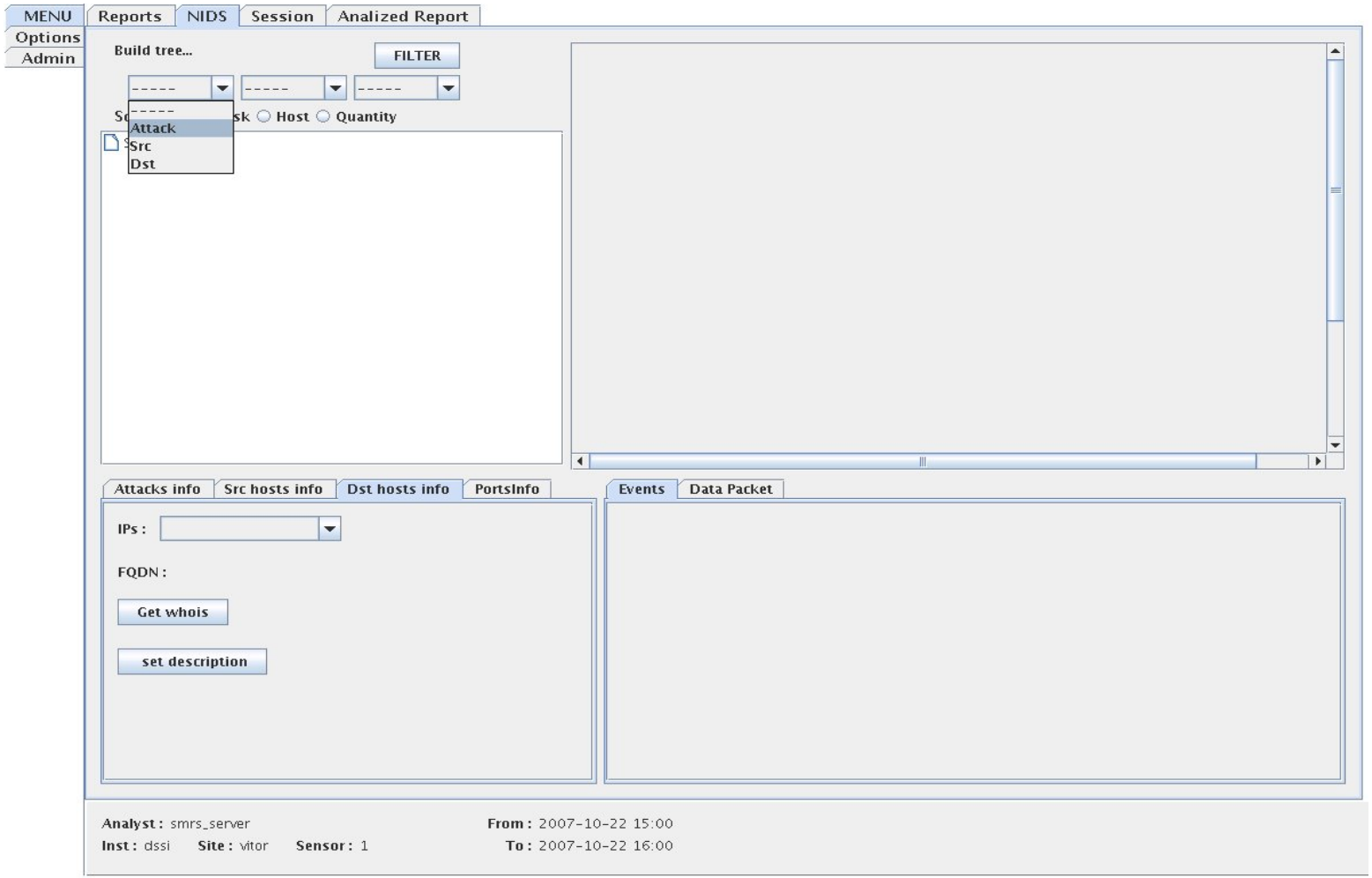
Whois do endereço



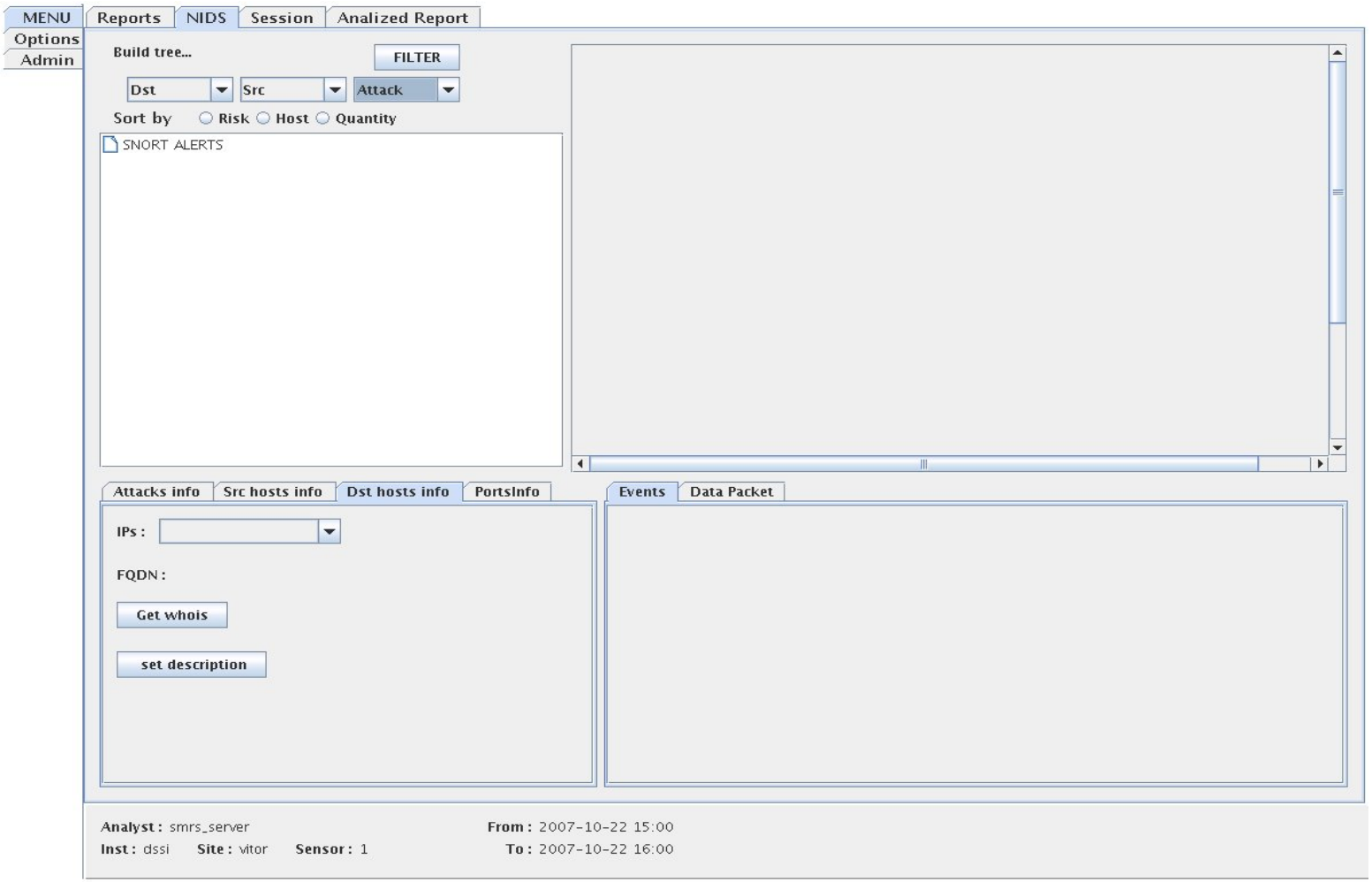
Verificação de alertas de segurança



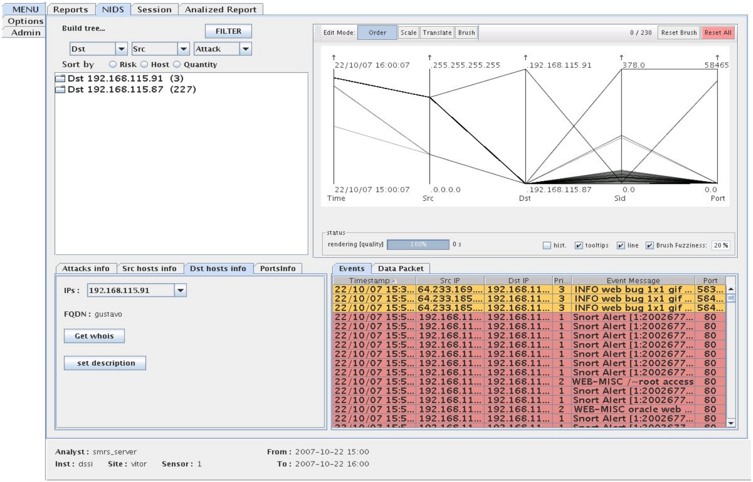
Verificação de alertas de segurança



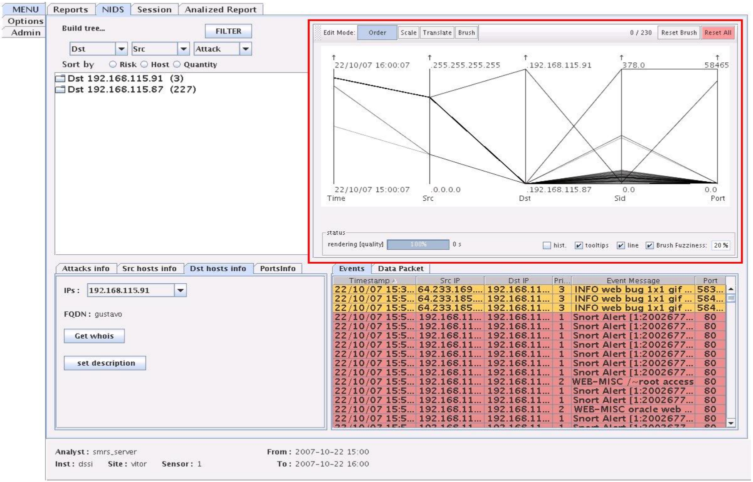
Verificação de alertas de segurança



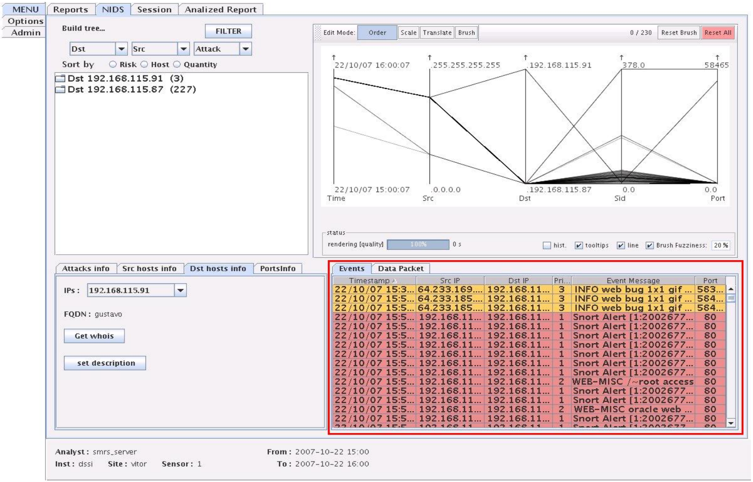
Verificação de alertas de segurança



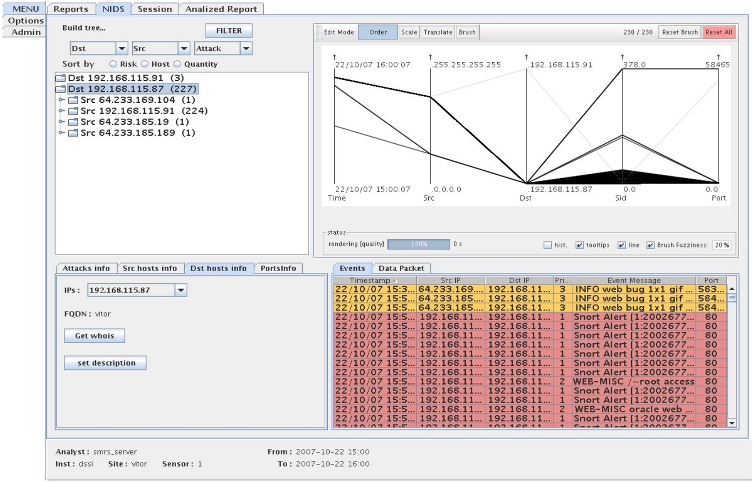
Verificação de alertas de segurança



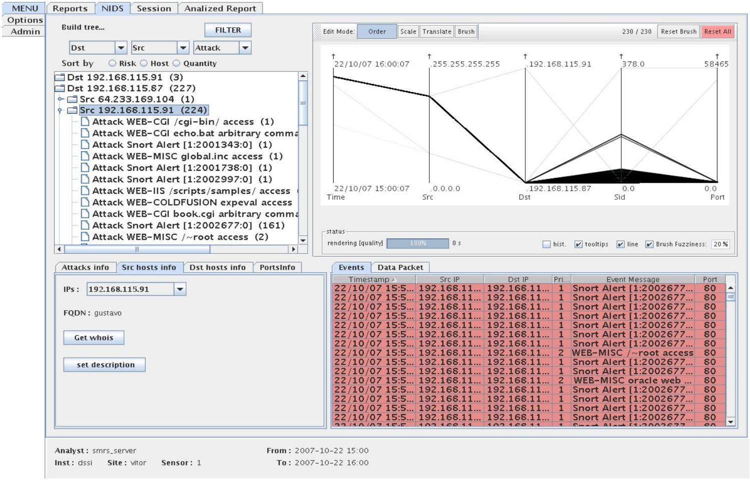
Verificação de alertas de segurança



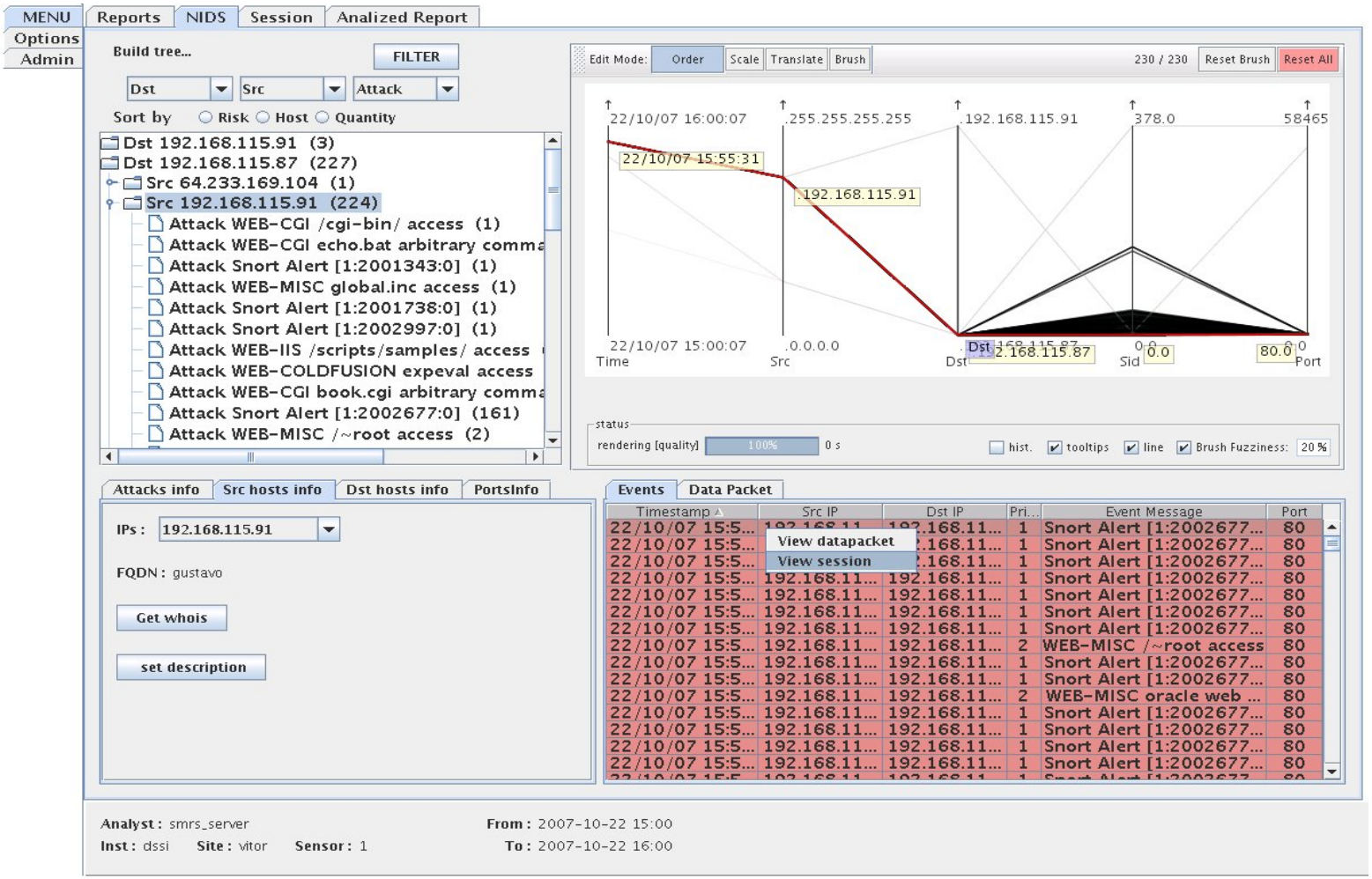
Verificação de alertas de segurança



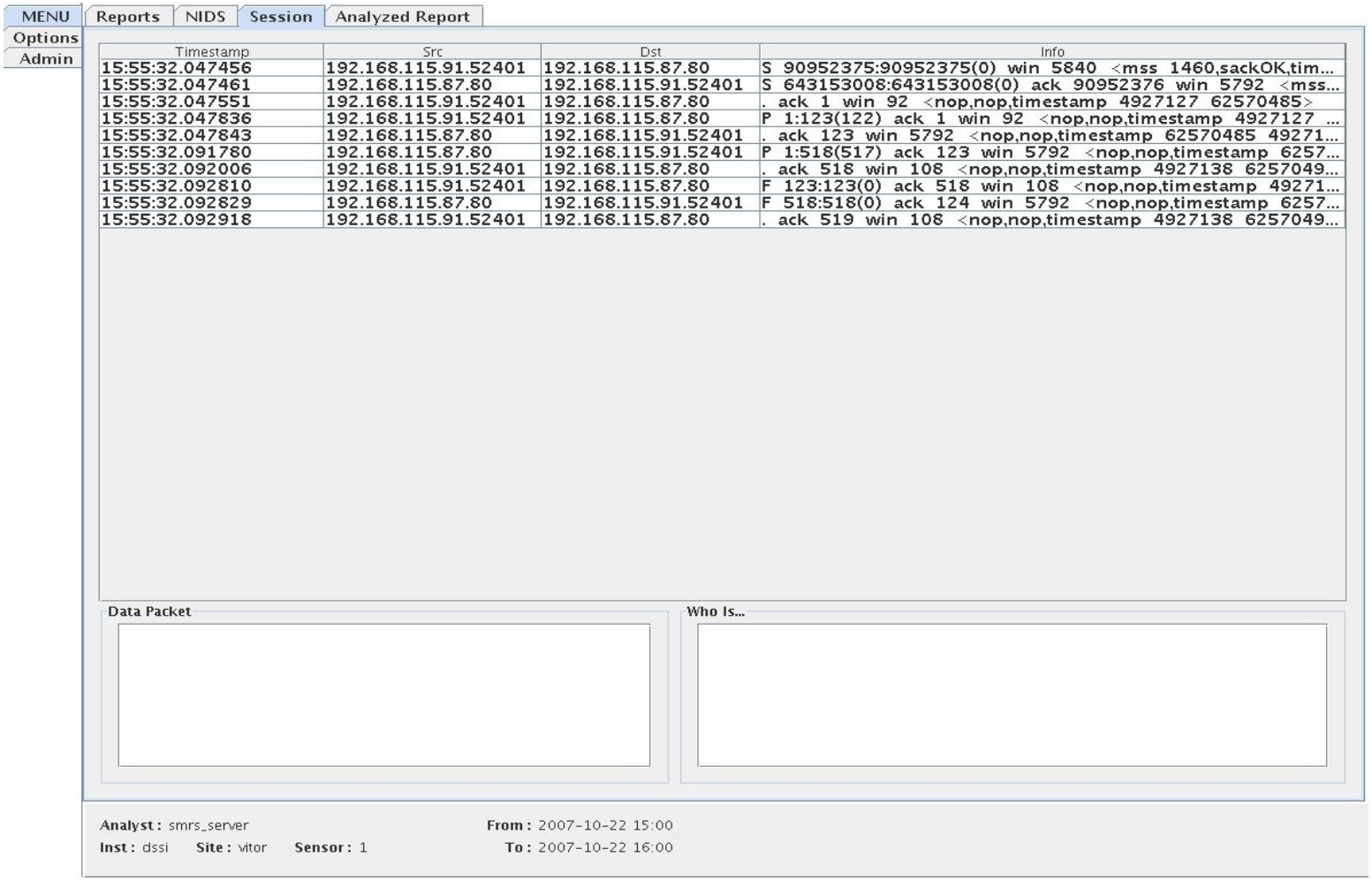
Verificação de alertas de segurança



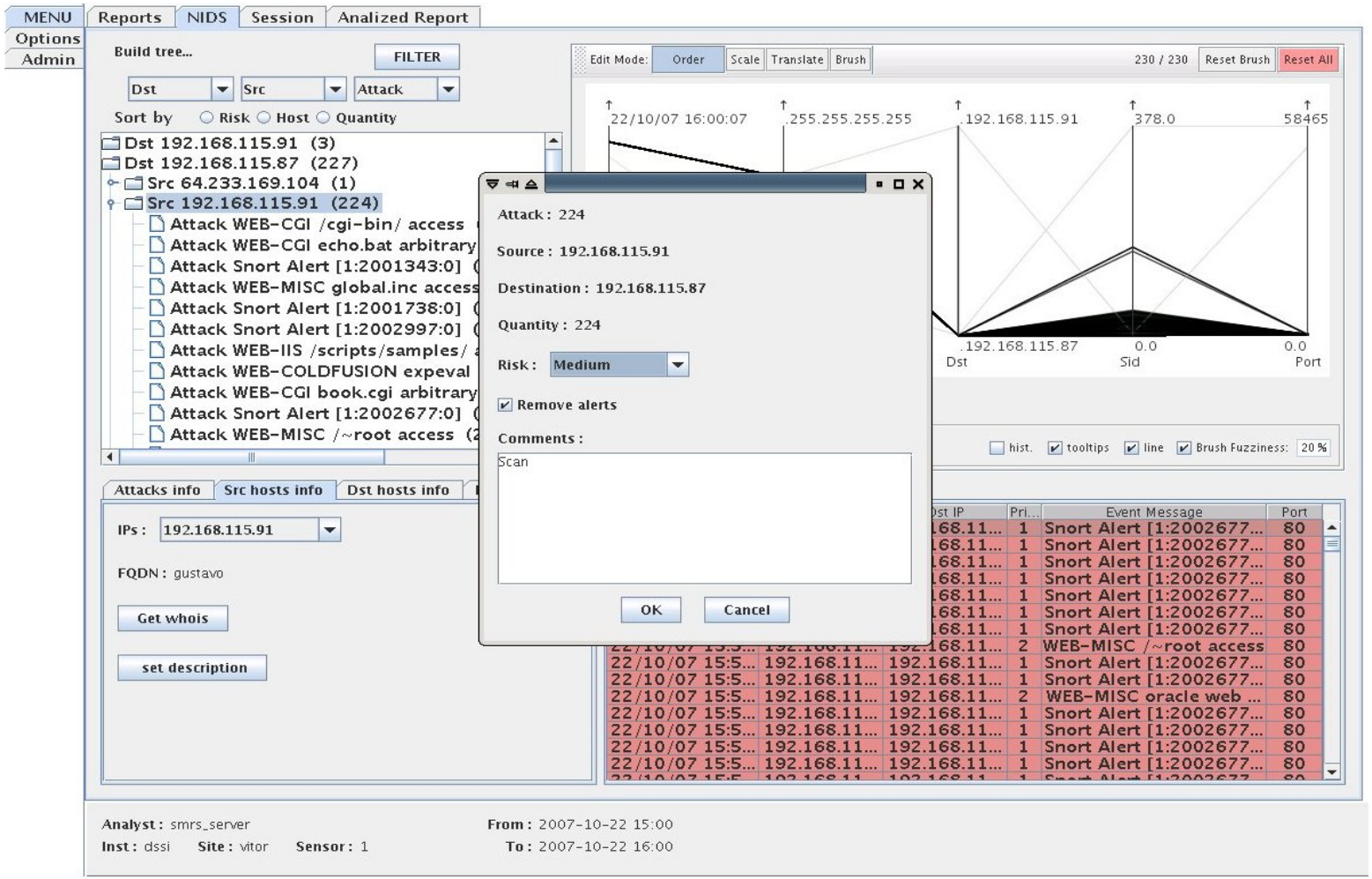
Verificação de alertas de segurança



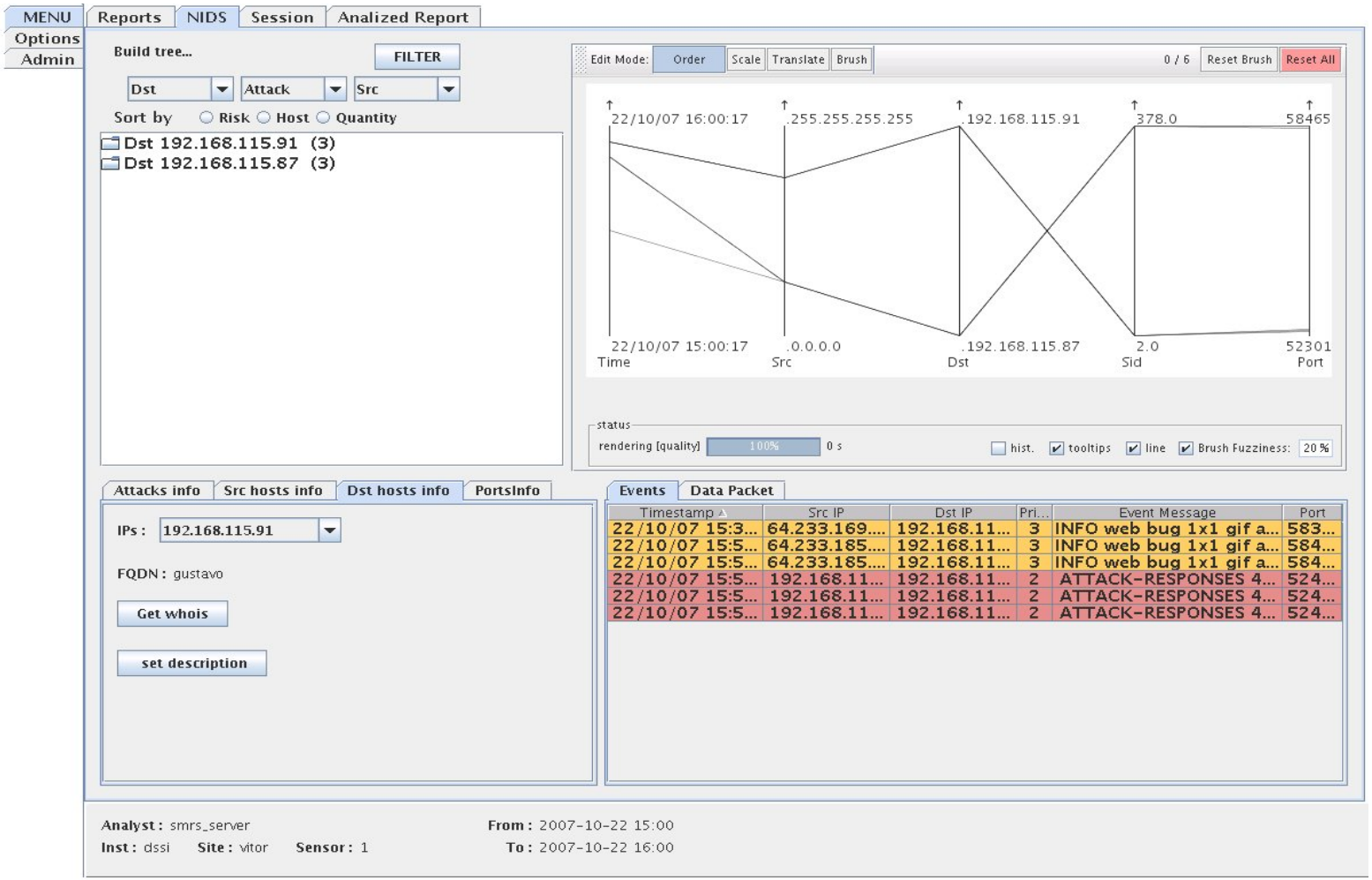
Tráfego da sessão associada



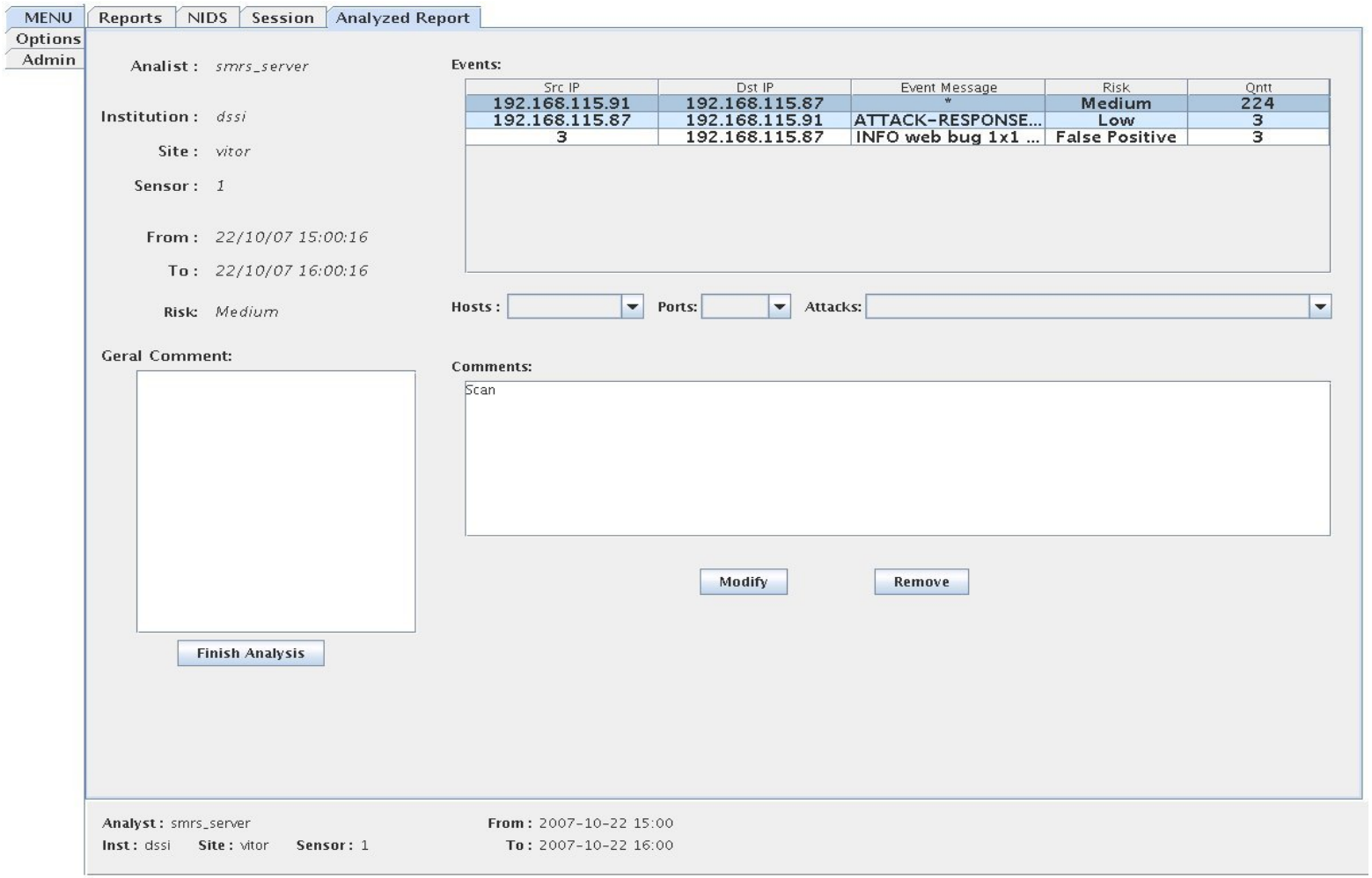
Verificação de alertas de segurança



Verificação de alertas de segurança



Geração de relatórios



Relatório gerado

Analysis report from SMRS
15/22/2007

Analyst: smrs_server

Institution: dssi
Site: vitor
Sensor: 1

From : 2007-10-22 15:00
Until: 2007-10-22 16:00

Risk: Medium

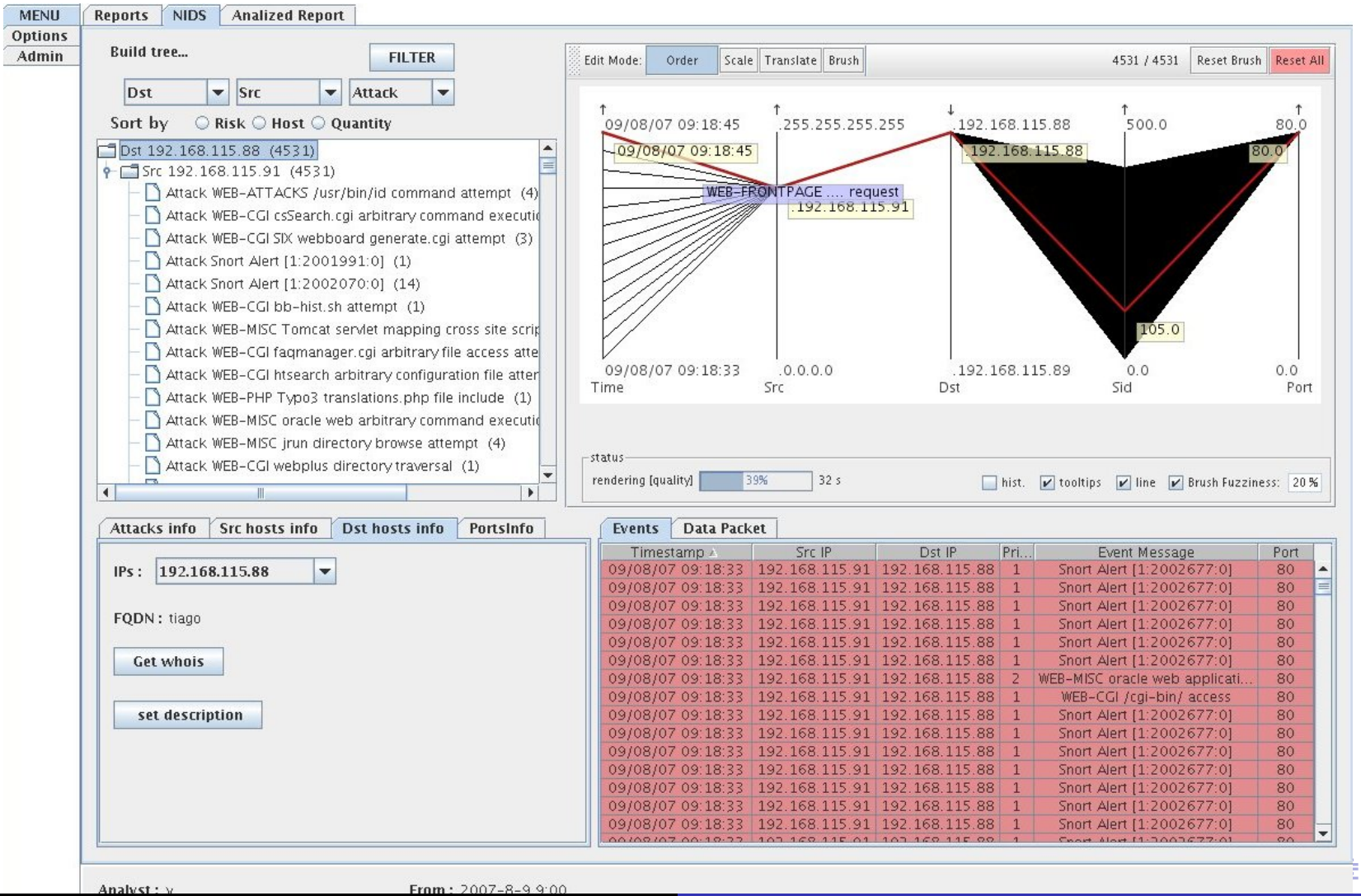
Alert Analysis :

Attack: *, **Risk: Medium**
From : 192,168,115,91 **To :** 192,168,115,87,
Quantity: 224,
Alert Priority: *,
Comment:
Scan attempt.

Attack: *ATTACK-RESPONSES 403 Forbidden*, **Risk: Low**
From : 192,168,115,87 **To :** 192,168,115,91,
Quantity: 3,
Alert Priority: 3,
Comment:
.

Attack: *INFO web bug 1x1 gif attempt*, **Risk: False Positive**
From : * **To :** 192,168,115,87
Quantity: 3,
Alert Priority: 3,
Comment:
.

Teste realizado com nikto



Conclusão

- O sistema atualmente está em fase de testes e estão sendo desenvolvidos programas para automatizar sua instalação.

Trabalhos futuros

- Incluir suporte a análise do tráfego de rede e de registros de aplicações

Apoio