Firewall em estado ativo utilizando open-source software

Dagoberto Carvalio Junior

Instituto de Ciências Matemáticas e de Computação
dago@icmc.usp.br

Primeira Ação de um Cracker

- Estatisticamente os crackers mapeiam portas para realizar um determinado ataque (precursor).
- Para verificar a ação de um portscanner o administrador deverá checar os logs do sistema.
- O ideal é ter um IPS que realize o bloqueio automático do atacante que realizar um portscanner

Sobre o PortSentry

- PortSentry é uma aplicação muito simples de ser utilizada, barrando portscanners e outras tentativas de burlar sua segurança.

  PortSentry foi desenvolvido pelo pessoal da Psionic.com, que hoje faz parte da Cisco Systems®.

- http://newsroom.cisco.com/dlls/corp_102202.html

Sobre o Portsentry

- Parte do projeto *Sentry Tools*, que tem além dele o *LogCheck*.

- *Sentry Tools* veio para ajudar usuários e administradores que não tem muita experiência em segurança de informática.

  Recomendo uma visita ao site do projeto:
- http://sourceforge.net/projects/sentrytools/

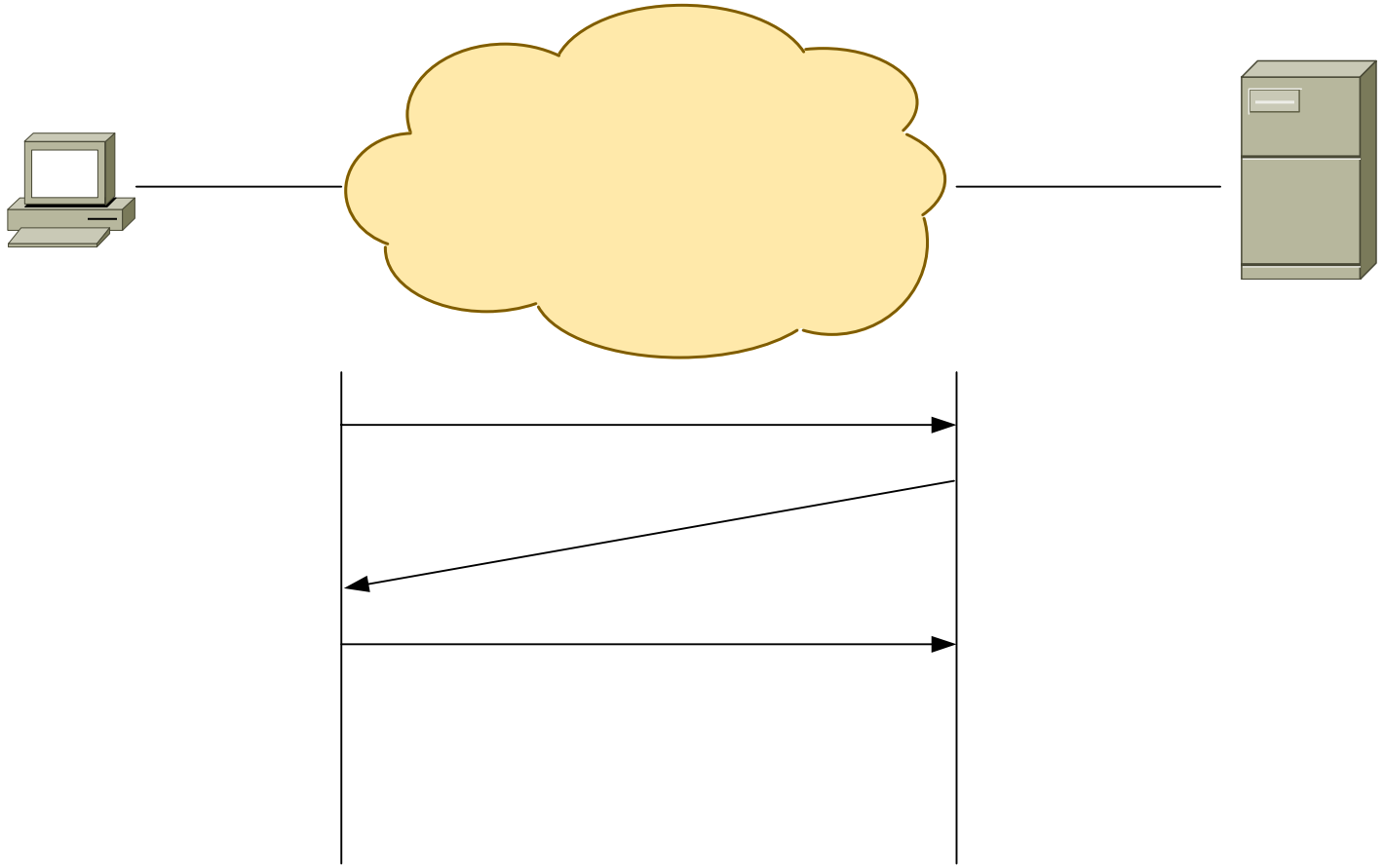
Teoria do PortSentry

- O PortSentry analisa porta TCP e UDP.

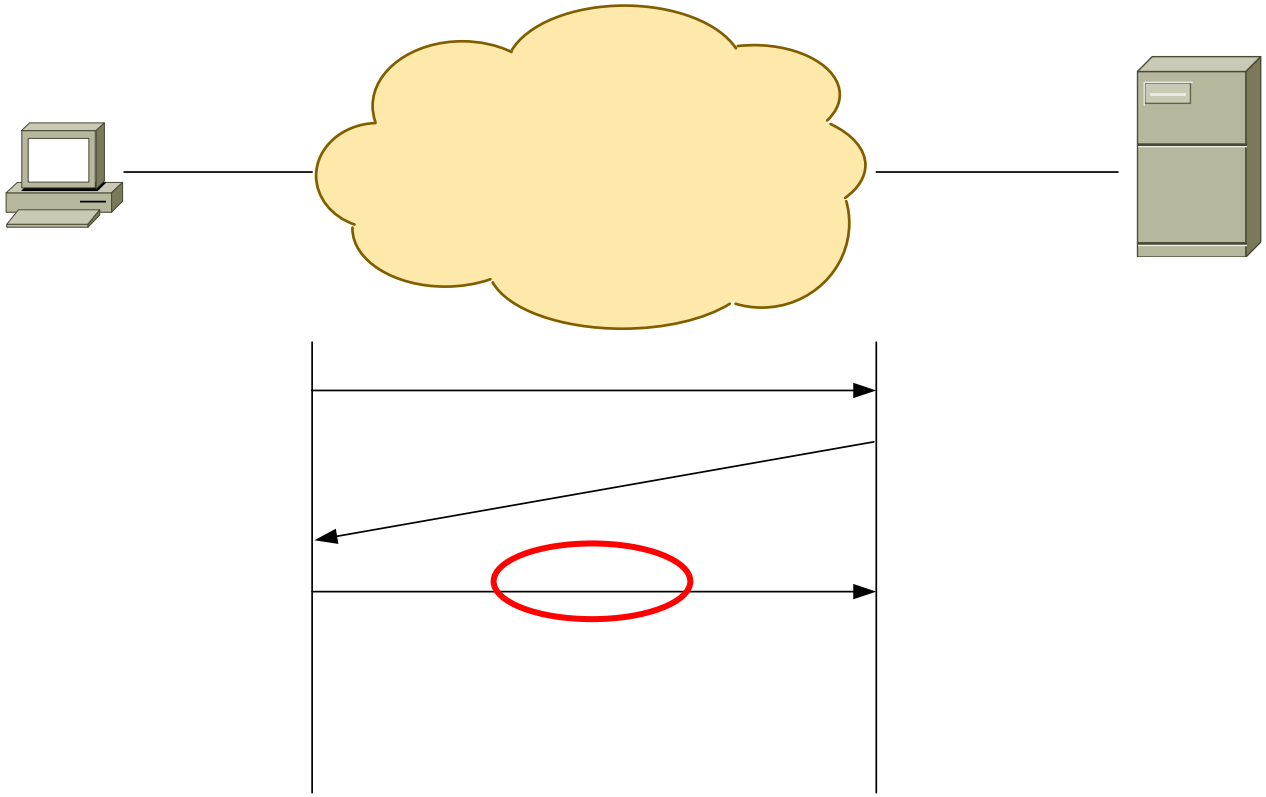
- Vários métodos de descoberta de portas são detectados pelo PortSentry, inclusive métodos avançados do nmap.

Teoria do PortSentry

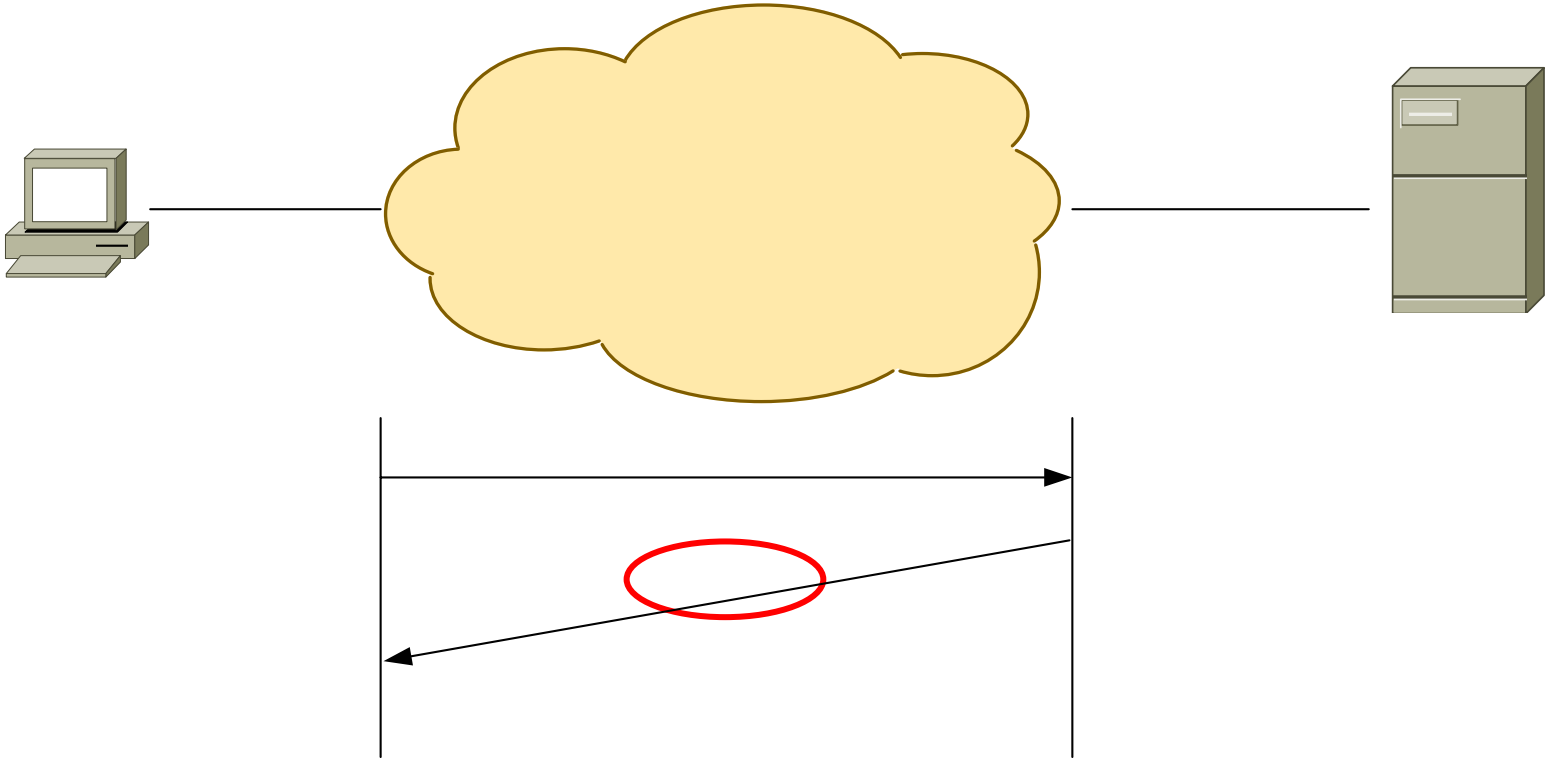
- Método Conecte Scan



- Método SYN Scan



- Método FIN Scan



Teoria do PortSentry

- **NULL scans** – Uso de pacotes sem o uso de nenhuma flag, retorna RST.
- **XMAS scans** – Uso de pacotes com flags FIN, URG e PUSH no cabeçalho TCP, retorna RST.
- **FULL-XMAS** scan – Uso de pacotes com todas as flags, pacote nunca deveria ser encaminhado, retorna RST.
- **UDP scan** – O scan é detectado através de múltiplos pacotes UDPs originados do mesmo IP.

Configuração do PortSentry

- Como configurar ?
- *portsentry.conf*.
- **TCP_PORTS="1,11,15,79,111,119,143,540,635,1080,1524,2000,5742,[..]"**
  UDP_PORTS="1,7,9,69,161,162,513,635,640,641,700,37444,34555,[..]"
- NÃO DEVEM SER INSERIDAS AS PORTAS VERDADEIRAS DO SEU SISTEMA !

Configuração do PortSentry

- **Ações do PortSentry.**

- IGNORE_FILE="/usr/local/psionic/portsentry/portsentry.ignore"
  ignora os ip´s de estão listados

- HISTORY_FILE="/usr/local/psionic/portsentry/portsentry.history“
  cria um histórico dos bloqueios

- BLOCKED_FILE="/usr/local/psionic/portsentry/portsentry.blocked“
  lista negra dos ip´s bloqueados

Configuração do PortSentry

Como criar regra de bloqueio ?

- KILL_ROUTE. Esta função como já diz o nome, cria uma regra de bloqueio do atacante.

- Se for Linux: `KILL_ROUTE="/usr/local/sbin/iptables -I INPUT -s $TARGET$ -j DROP"`

- TCP Wrappers: `KILL_HOSTS_DENY="ALL: $TARGET$ # PortSentry blocked"`

External Command !

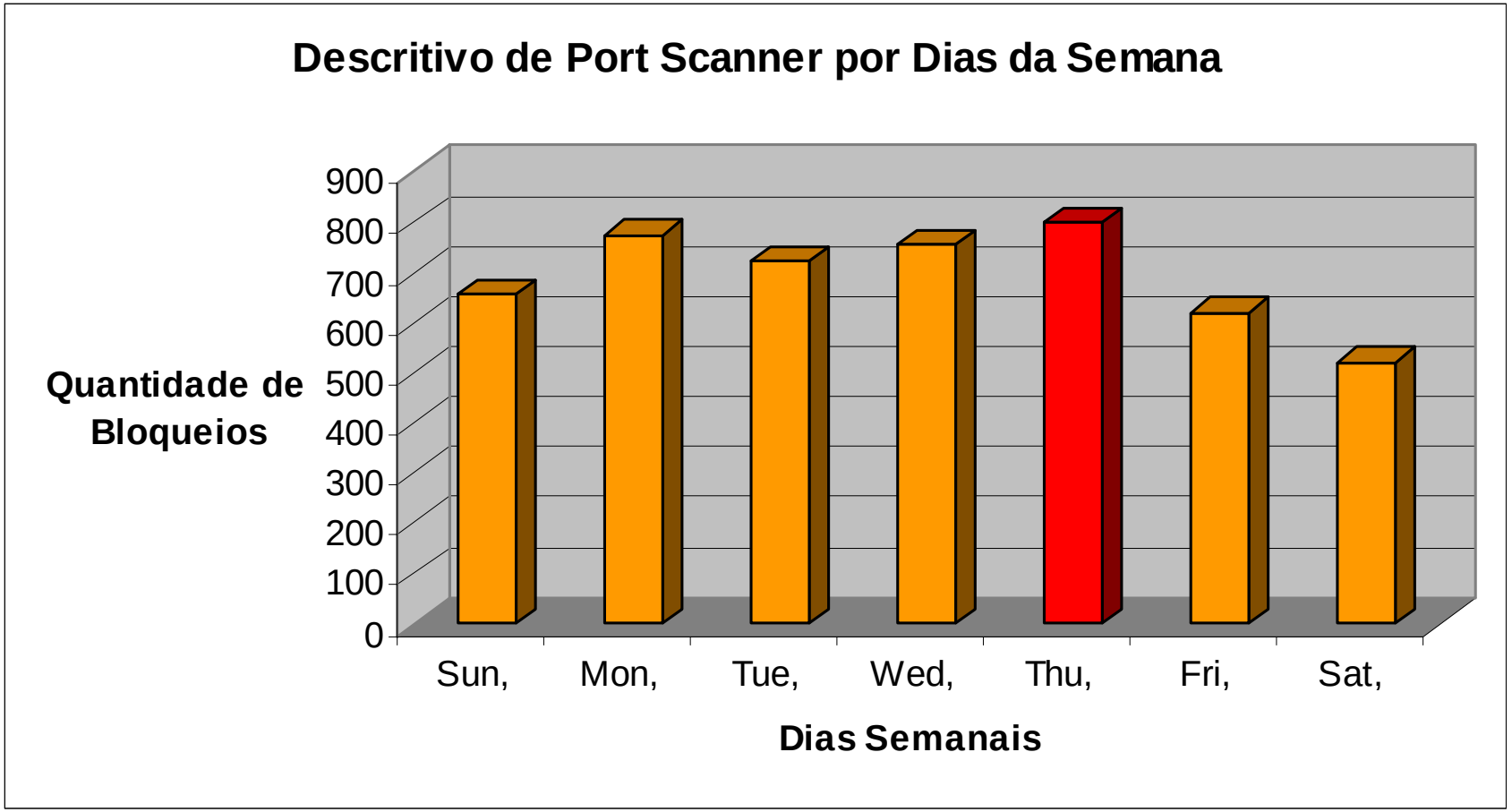
Essa parte permite você realizar um comando externo ao PortSentry para reagir ao ataque ou para escrever algum log especial. Bom para a função Mail.

```
KILL_RUN_CMD="/some/path/here/script $TARGET$ $PORT$"
```

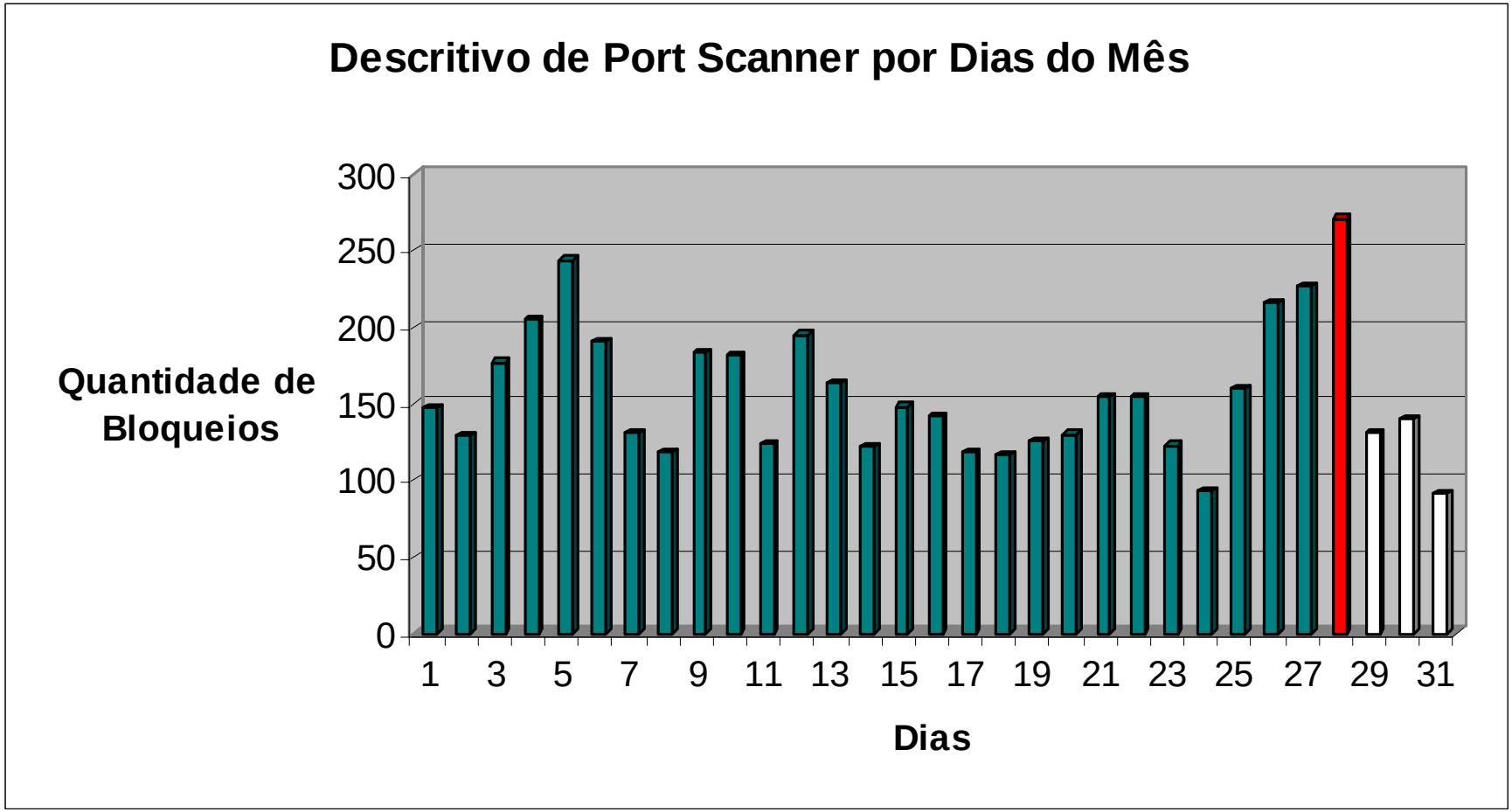
PortSentry no ICMC

- Utilizamos o PortSentry desde 2003.
- Foram criadas 3572 regras no firewall de forma automática no ano de 2005.
- Utilizamos como router o FreeBSD.

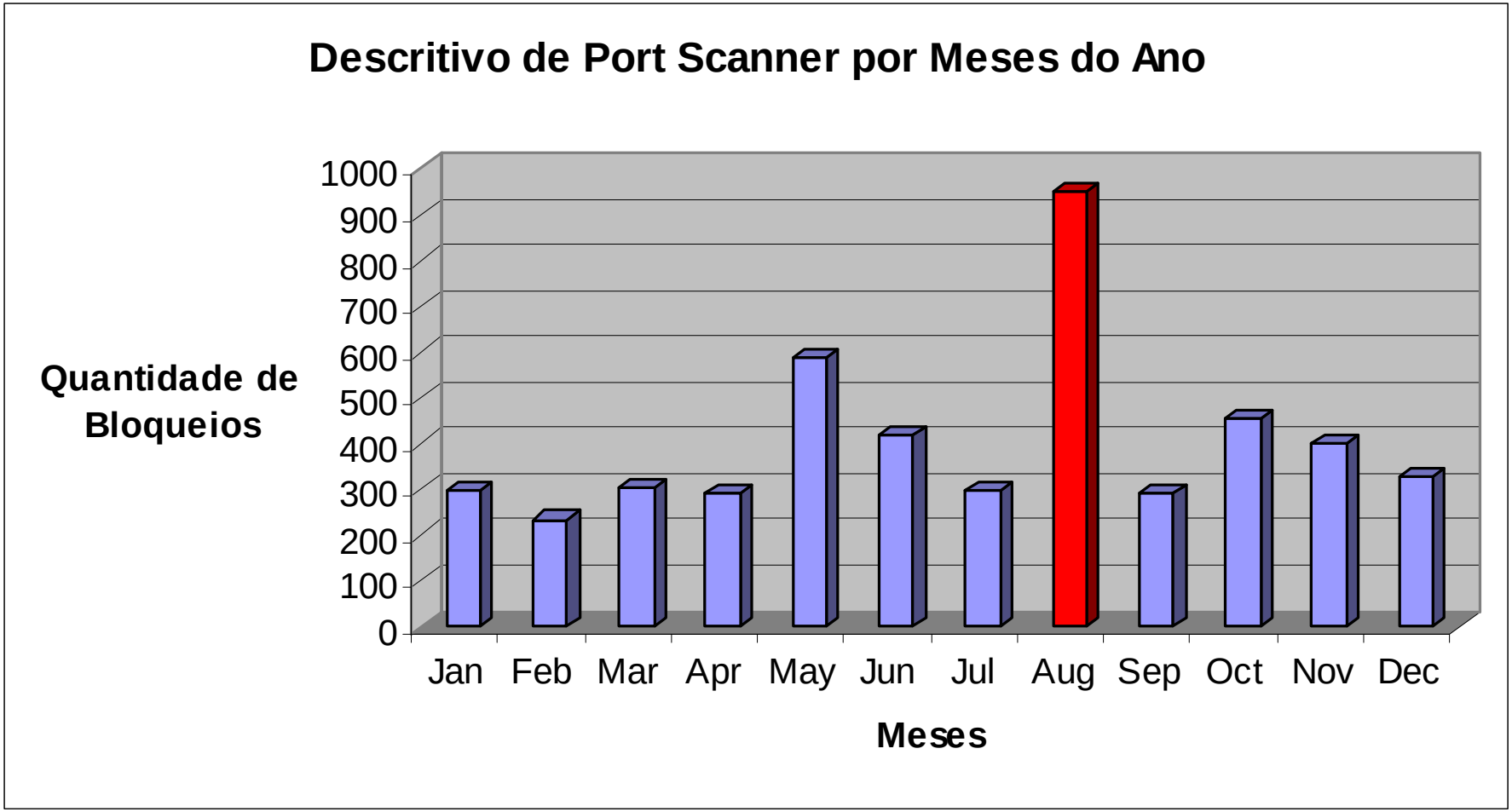
PortSentry no ICMC



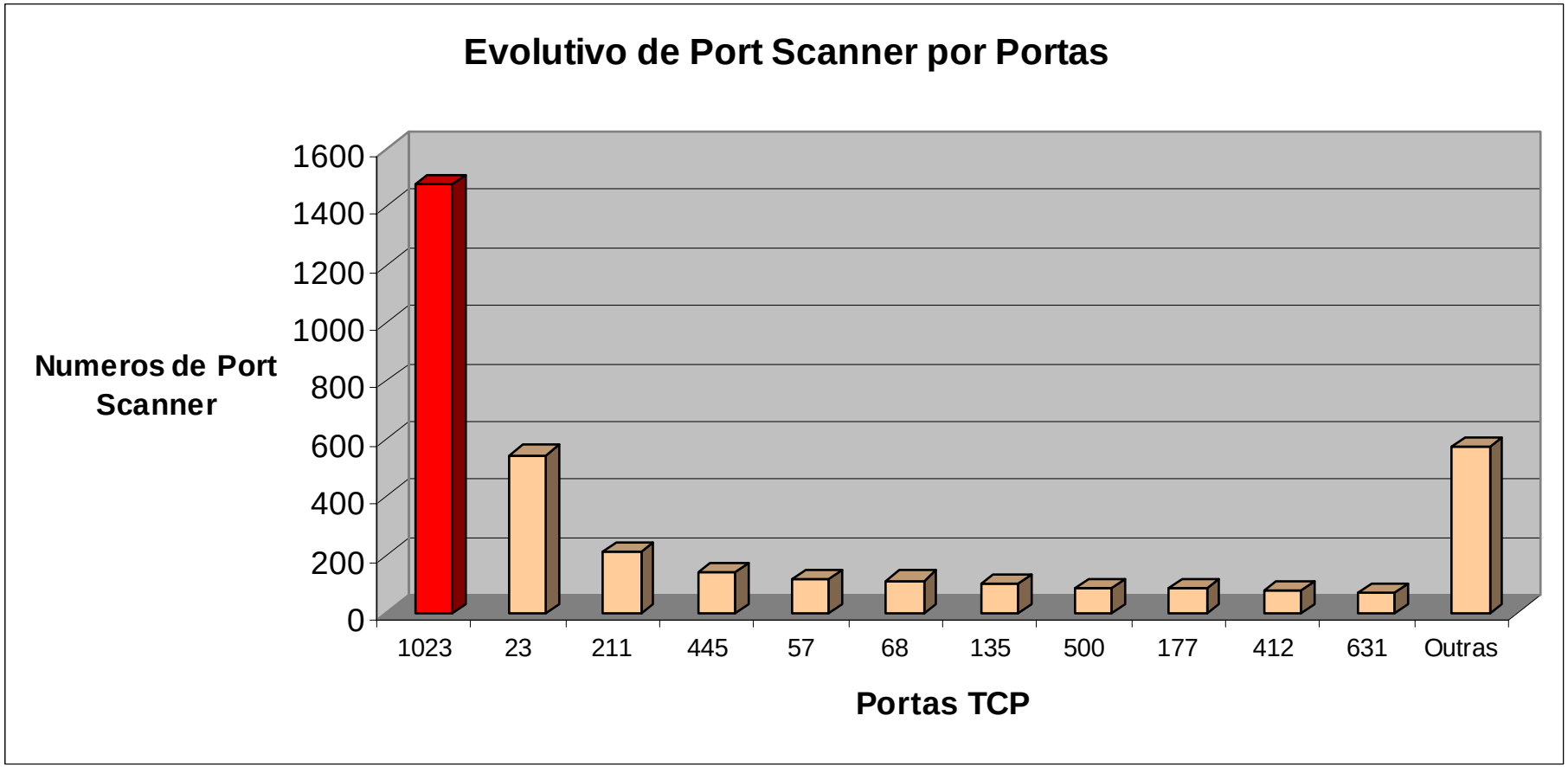
PortSentry no ICMC



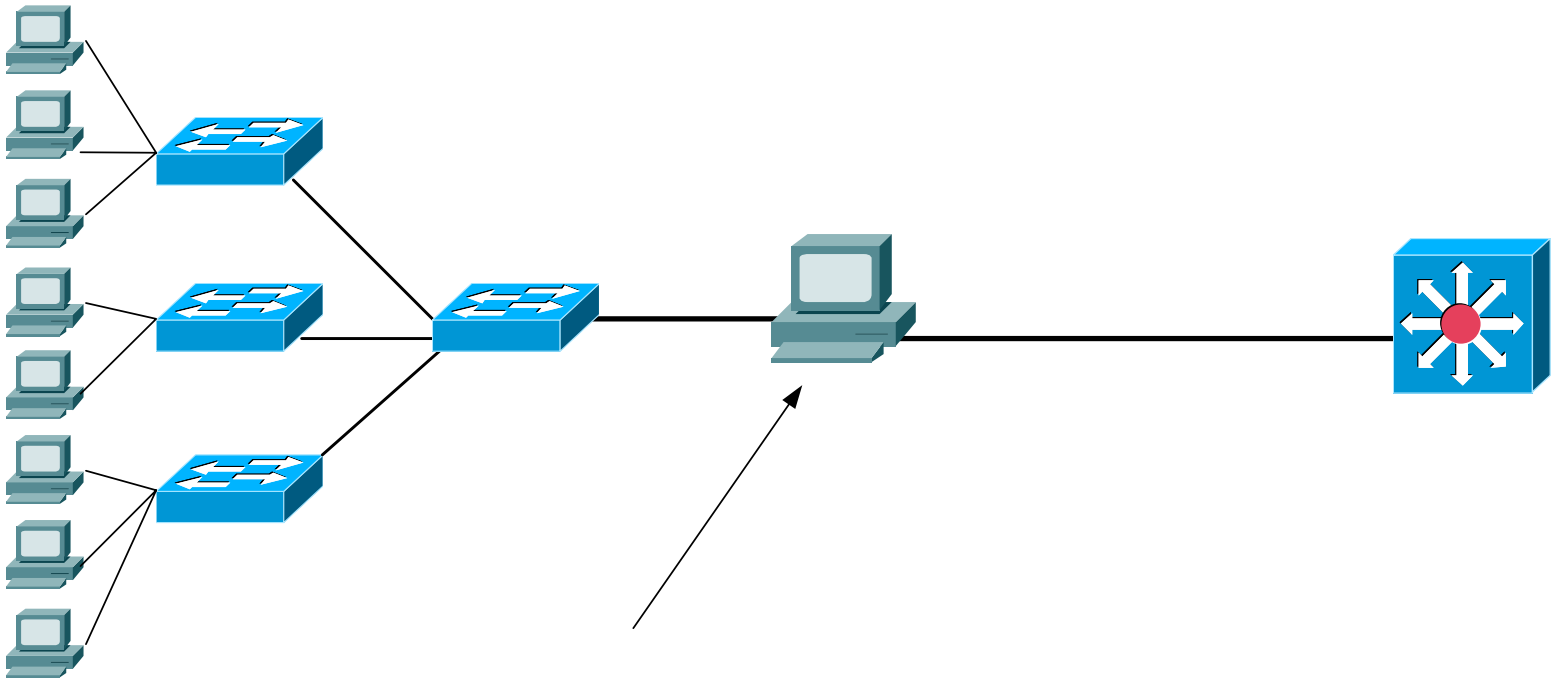
PortSentry no ICMC



PortSentry no ICMC



Topologia Lógica do PortSentry

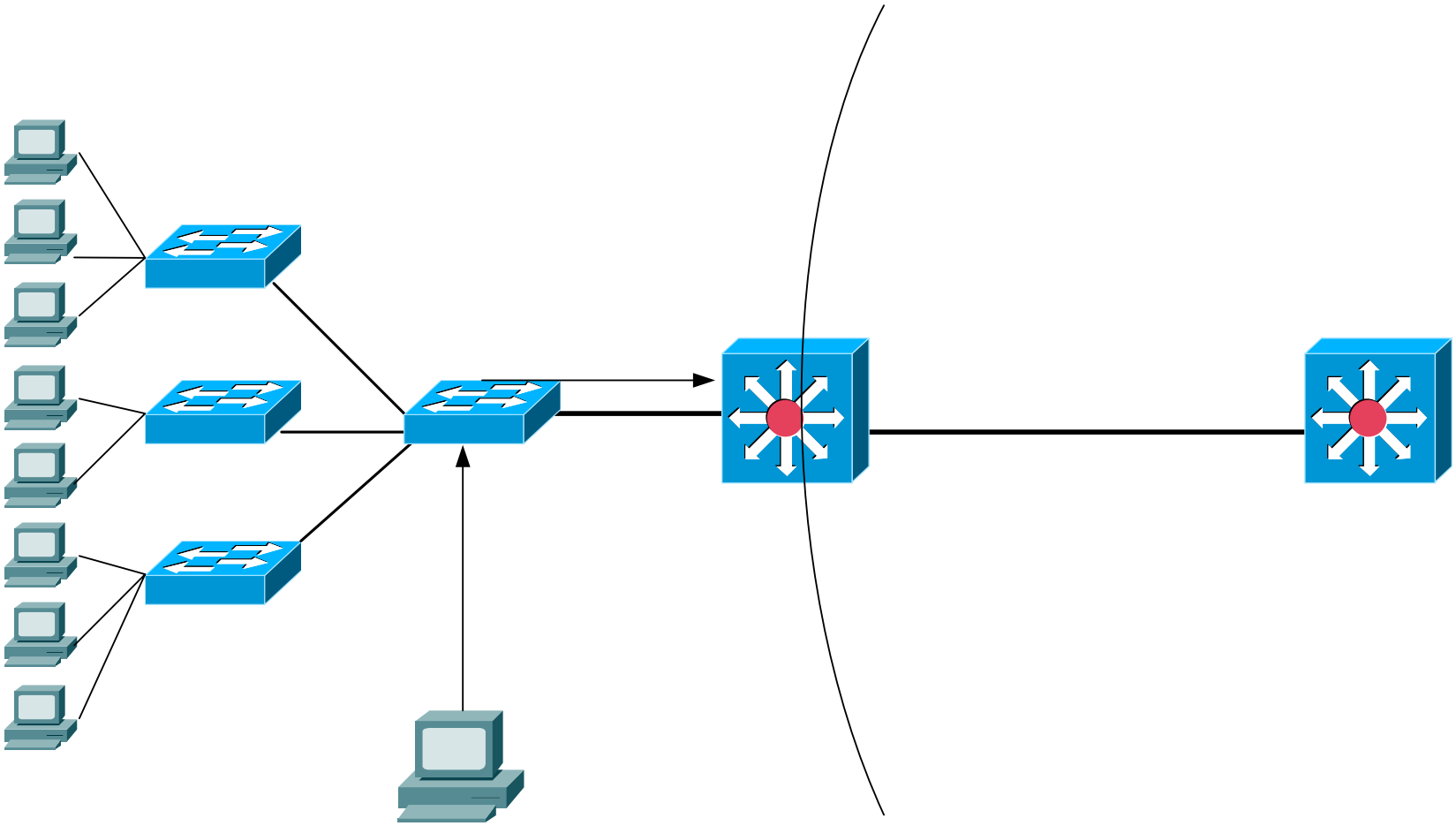


Rede Local da Unidade

Desafio

- **Criar um BOX para gerar regras automáticas através do PortSentry e através do SNMP enviar as ACLs para Routers de diversos fabricantes.**

Topologia Lógica - Desafio



Rede Local da
143.107.YYY

Conclusão

- Esta ferramenta é muito útil e pode ser usada para complementar outras formas de segurança, basicamente ele barra a exploração da sua rede.
- Muito pouco falso positivo é gerado pelo PortSentry.
- Um desafio futuro é a inclusão das regras automáticas de bloqueio em roteadores pontuais através do protocolo snmp (Simple Network Management Protocol), como Cisco, Foundry e outros.