

ptguard

Uma ferramenta para identificação, análise e controle de aplicações ponto-a-ponto

Gustavo Beltrami Rossi
Antonio Montes Filho

<http://www.lac.inpe.br/security>

Redes e Segurança de Sistemas de Informação
Laboratório Associado de Computação e Matemática Aplicada
Instituto Nacional de Pesquisas Espaciais
12227-010 São José dos Campos – SP





Introdução

- Cenário Atual
- Propósito e Motivação
- Protocolos Ponto-a-Ponto
- Descrição do Problema
- Tecnologia Atual
 - Softwares de Controle
 - Dispositivos Específicos
 - Vantagens e Desvantagens



Cenário Atual

- Fortes restrições impostas pelos órgãos responsáveis pelos direitos autorais
 - *Recording Industry Association of America (RIAA)*
 - *Motion Picture Association of America (MPAA)*
- Evidencia nos noticiários
 - Condenação da empresa Napster
 - Bloqueios e filtros impostos no mecanismo de busca do software Audiogalaxy
 - etc...
- Potencial relacionado a problemas de segurança
- Crescimento da utilização dos softwares ponto-a-ponto (P2P)



Cenário Atual

THIS WEEK	Popular Titles in Windows Week Ending November 02	Last Week	Weeks On Chart	Downloads This Week	Total Downloads
1	Kazaa Media Desktop	1	79	2,170,601	291,027,428
2	AOL Instant Messenger	2	56	646,386	25,648,472
3	ICQ Lite	3	56	614,436	32,352,028
4	iMesh	4	184	437,590	60,559,837
8	ICQ Pro 2003b	6	319	306,531	237,209,311
9	Morpheus	9	131	173,040	116,811,359
11	Trillian	11	98	139,606	13,705,317
17	LimeWire	21	15	101,850	16,687,287

Fonte: c|net DOWNLOAD.COM

<http://download.com.com/3101-2001-0-1.html?tag=pop>



Propósito e Motivação

- Metodologia para identificação de protocolos P2P ou de protocolos com portas variáveis
 - propor,
 - desenvolver e
 - testar
- Permitir seu bloqueio ou controle
- Desenvolvimento de uma ferramenta capaz de:
 - auxiliar os administradores de rede
 - política de segurança e de uso aceitável
 - garantir o correto funcionamento e utilização da rede



Protocolos Ponto-a-Ponto

- Definição
 - Conjunto de recursos heterogêneos distribuídos que estão conectados por uma rede
 - (Meta Computing, 2001, Wray, 1994)
 - Arquitetura oposto ao da arquitetura Cliente/Servidor
 - (Singh, 2001, Thomas, 1998)
- Conceito da entidade **Servent**
 - *server* “Serv-”
 - *client* “-ent”
 - Representa a capacidade dos nós em uma rede P2P de atuarem como um servidor, assim como um cliente, ao mesmo tempo.



Protocolos Ponto-a-Ponto

- Definição atual
 - Uma **arquitetura distribuída** de rede pode ser chamada de rede P2P, se os seus participantes **compartilham** alguma parte de seus **recursos de hardware**. Esses recursos compartilhados são necessariamente para prover o serviço e conteúdo oferecido pela rede e devem **estar acessíveis aos outros nós diretamente**, sem passar por entidades intermediárias.
 - Schollmeier, Rüdiger.



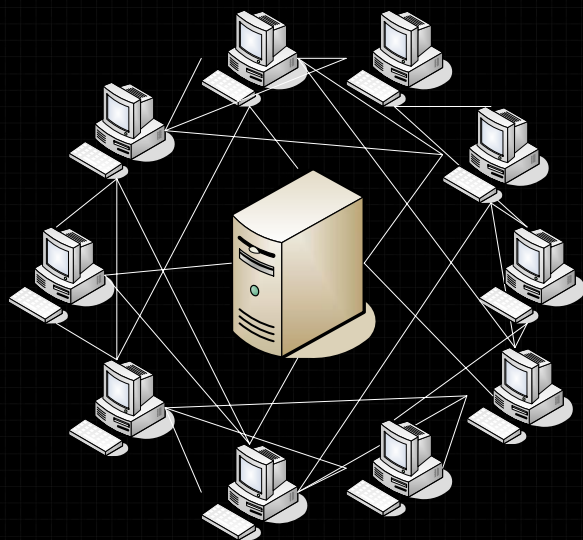
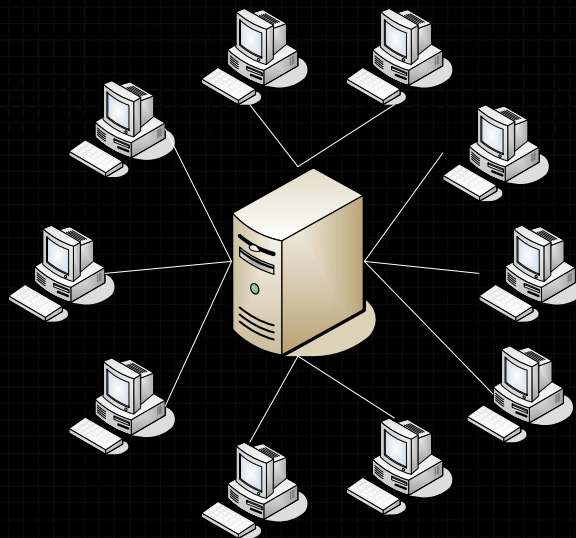
Protocolos Ponto-a-Ponto

- Modelo totalmente descentralizado
 - todos os *hosts* possuem uma **participação igualitária**
 - não existem *hosts* com regras administrativas ou com facilidades especiais
 - difícil construção
- Modelo híbrido
 - utilização de uma **entidade central** para prover parte dos serviços de rede oferecidos
 - Napster: diretório contendo índices dos arquivos compartilhados na rede
 - ICQ: servidor para manter associação entre nome do usuário e seu endereço IP corrente

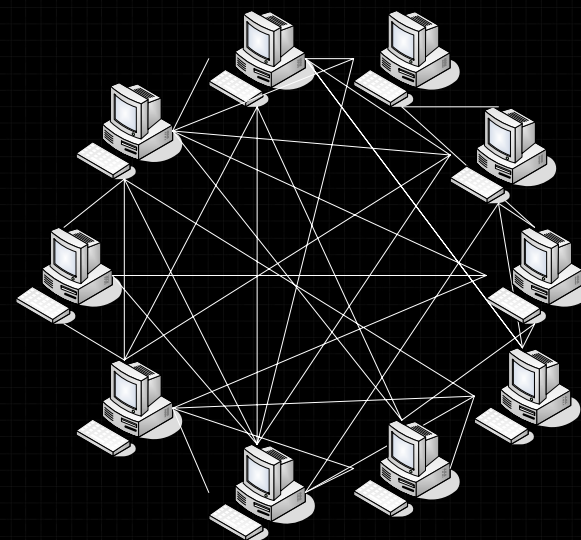


Protocolos Ponto-a-Ponto

Modelo Cliente/Servidor



Modelo P2P Híbrido



Modelo P2P Descentralizado



Descrição do Problema

- Para as **corporações**, os software P2P ameaçam:
 - Consumo de banda;
 - Violação das responsabilidades e uso aceitável definidos pela corporação;
 - Violação da política de segurança da corporação;
 - Distribuição de vírus e cavalos de tróia;
 - Revelação do endereço IP e MAC.



Descrição do Problema

- Para os **usuários domésticos**, os software P2P ameaçam:
 - Revelação do endereço IP e MAC;
 - Revelação da velocidade de conexão;
 - Compartilhamento de arquivos;
 - Distribuição de vírus e cavalos de tróia.



Tecnologia Atual

Softwares de Controle

- Linux netfilter/iptables
 - Utilização da diretiva *queue*
 - exemplo: **P2Pwall**
- Modificações para o *kernel* do Linux
 - Funcionalidades de reconhecimento de padrões
 - exemplo: **I7-filter**
- **Desvantagens:**
 - **Obrigar o *firewall* a analisar todo o conteúdo dos pacotes trafegados**
 - **Perda de performance**
 - **Não é viável para redes de alto desempenho**



Tecnologia Atual

Dispositivos Específicos

- Allot NetEnforcer

- AudioGalaxy
- eDonkey
- iMesh
- KaZaA
- Morpheus



- **Desvantagens:**

- **Preço \$\$\$**
- **Software fechado e proprietário**
- **Atualização com a capacidade de análise de novos protocolos**

- Packeteer PacketShaper

- AOL Instant Messenger
- ICQ Chat
- MSN Messenger
- Yahoo! Messenger
- Aimster
- AudioGalaxy
- Gnutella
- iMesh
- Napster
- Scour





Metodologia

- **Classificação**
 - Assinaturas de aplicações (*Layer-7*)
 - Endereços IP, sub-redes, ou lista de *hosts* (*Layer-3*)
 - Portas UDP e TCP, ou lista de portas (*Layer-4*)
- **Análise**
 - Performance das aplicações e eficiência da rede
 - Descrição da utilização de banda
- **Controle**
 - Prevenir congestionamento nos fluxos *inbound/outbound*
 - Controle avançado de políticas
 - Prover alocação de banda dinâmica
- **Relatório**
 - Utilização de banda e performance das aplicações
 - SNMP é utilizado para integrar com outros sistemas



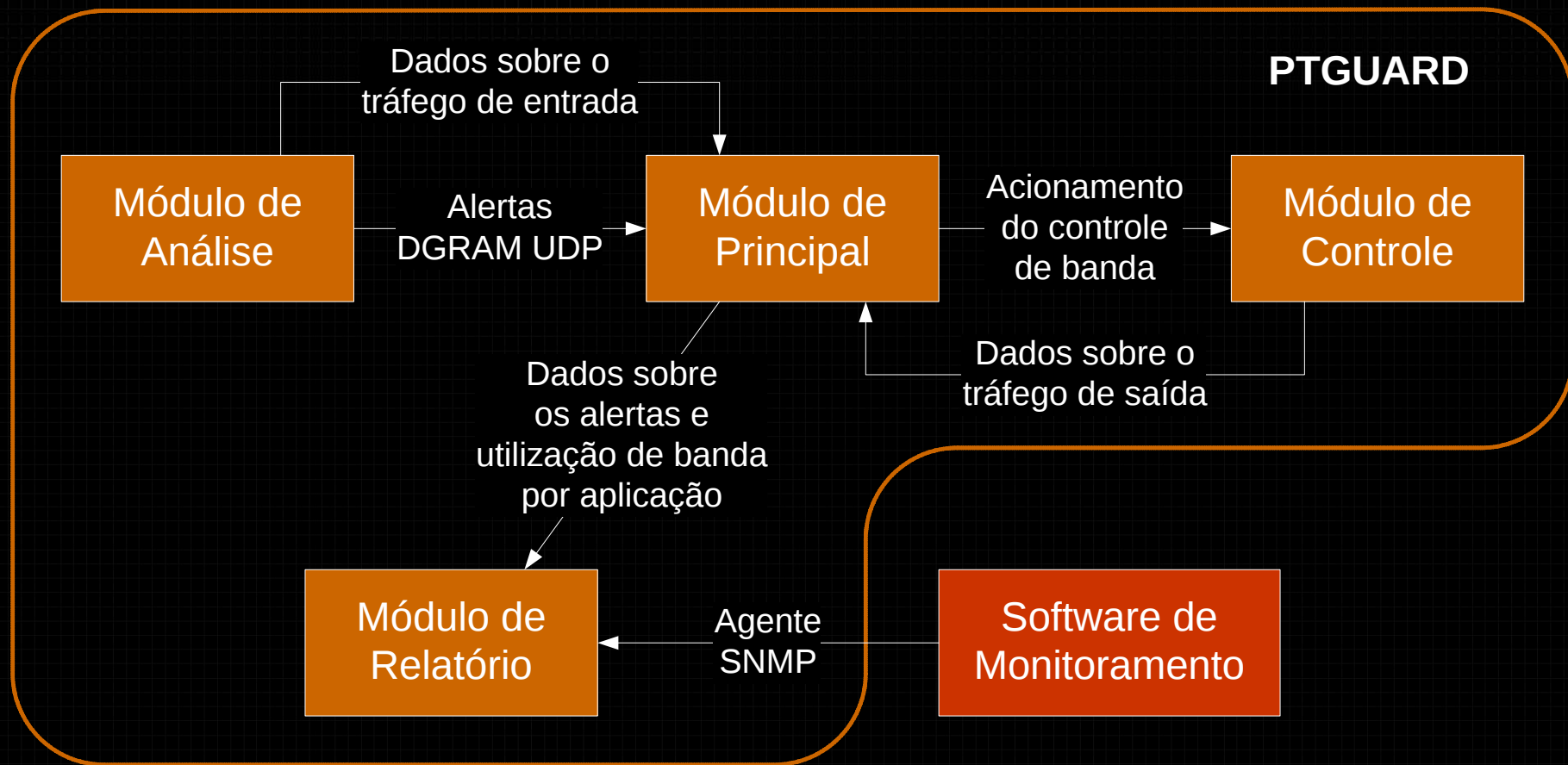
Metodologia

- A aplicação foi dividida em quatro grandes módulos:
 - **Módulo principal:**
 - inicialização e controle dos demais módulos
 - **Módulo de análise:**
 - captura e análise do tráfego de rede
 - **Módulo de controle:**
 - controle de banda e qualidade de serviço de rede
 - **Módulo de relatório:**
 - criação de relatórios contendo a utilização de banda por aplicação



Metodologia

Relação entre os Módulos



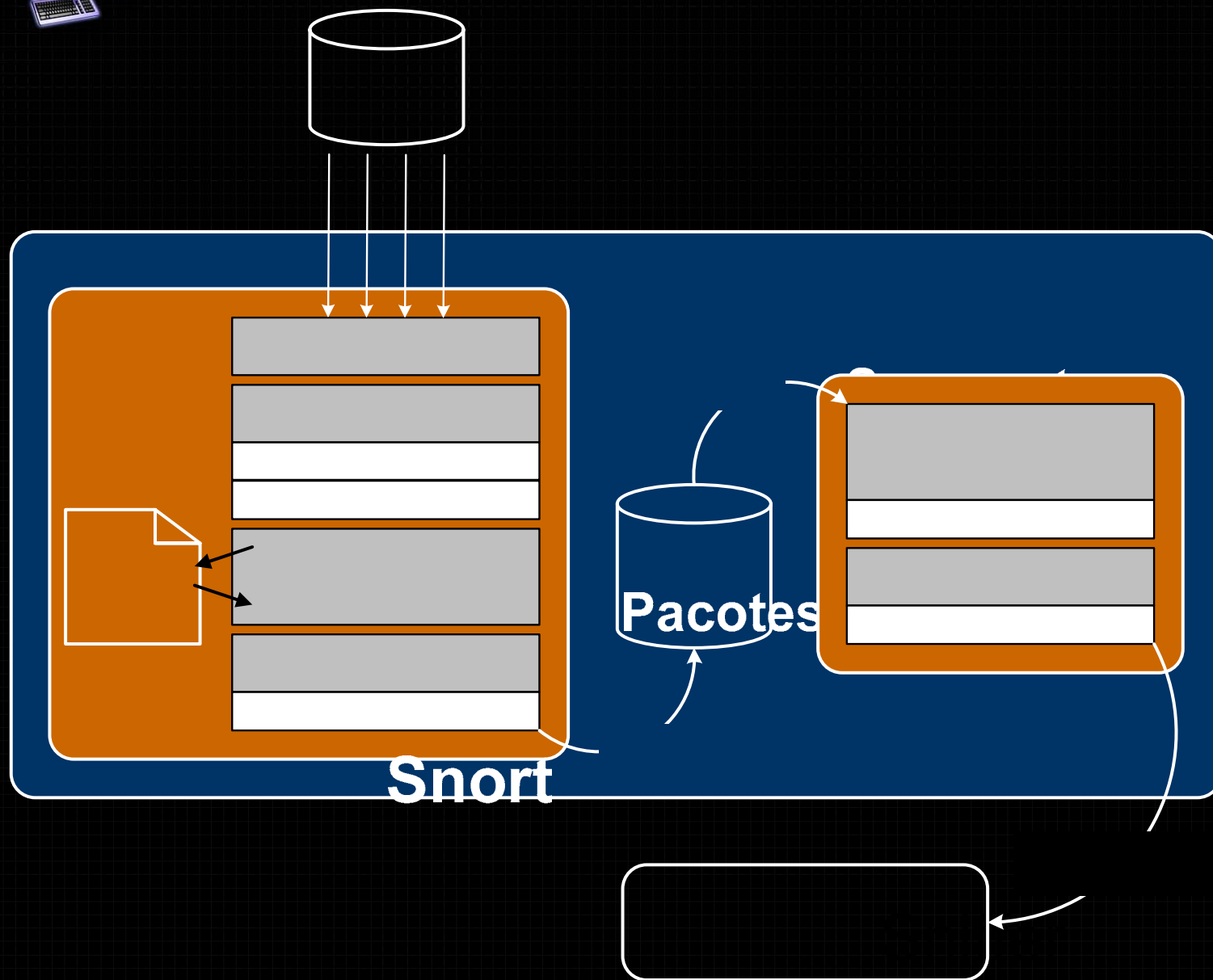


Módulo de Análise

- Responsável pela **captura e análise do tráfego de rede**.
- Busca de **padrões ou assinaturas** que identifiquem a utilização de algum protocolo.
- Quando o padrão é encontrado, o alerta é imediatamente enviado ao módulo principal.
- Necessidade de um profundo conhecimento do protocolo P2P analisado.



Módulo de Análise





Módulo de Controle

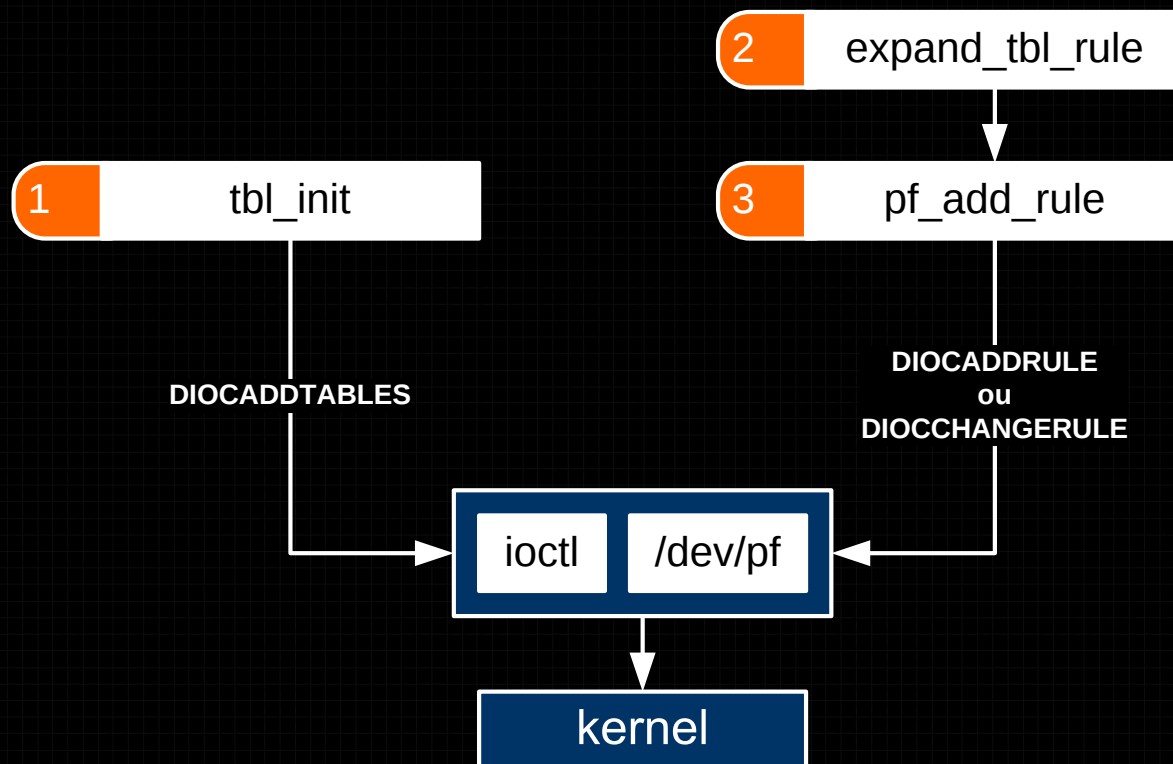
- Responsável pela **alocação de banda**.
- Modelagem e **priorização** de tráfego.
- Permitir que os administradores atuem com inteligência na classificação, análise e outras funções de monitoração da rede.
- Proteger aplicações críticas com garantia de banda.



Módulo de Controle

Inicialização do Módulo

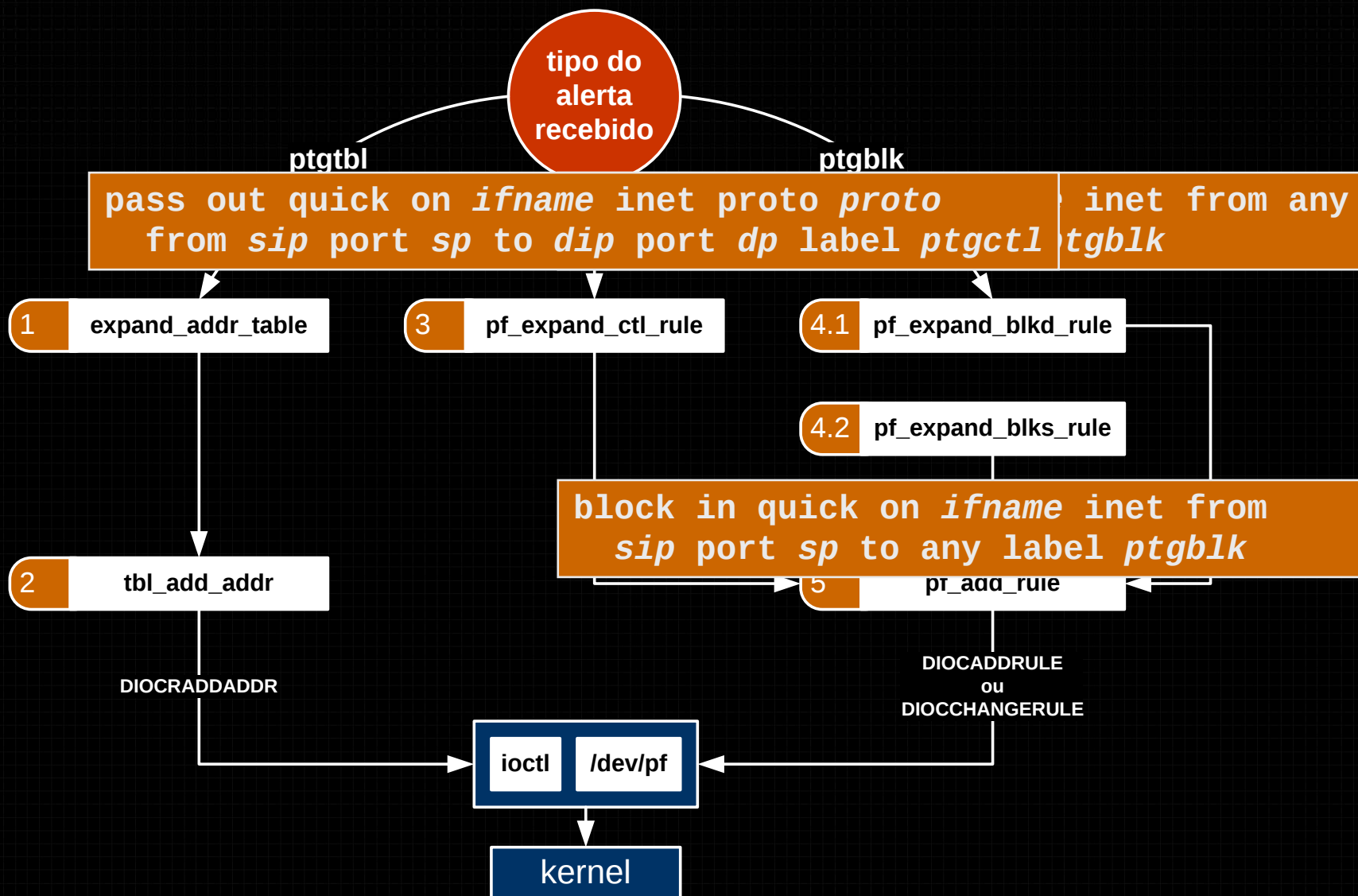
pass out quick on *ifname* inet from any to
tname port *dp* queue *tname* label *ptgtbl*





Módulo de Controle

Inserir Regras de Controle





Módulo de Controle

Remover Regras de Controle

- O tratamento de limpeza de regras ocorre de três maneiras distintas
 - *host* inativo da tabela de endereços de uma regra do tipo ***ptgtbl***
 - `tbl_del_addr`
 - `DIOCRDELADDRS`
 - regra de controle do tipo ***ptgctl***
 - regra de bloqueio do tipo ***ptgblk***
 - `pf_del_rule`
 - `DIOCCHANGERULE`



Módulo de Relatório

- Responsável pela emissão de relatórios estatísticos
 - nome do protocolo analisado
 - descrição
 - *bytes* transferidos
 - número de pacotes trafegados
- Implementação dividida em três partes
 - desenvolvimento da MIB
 - desenvolvimento do agente SNMP
 - desenvolvimento de uma *thread* específica responsável por coletar as informações dos protocolos P2P configurados



Módulo de Relatório

Desenvolvimento da MIB e do Agente

```
+ -ptguard(1)
|
| -+-ptgObjects(1)
|   |
|   +-Integer32 ptgNumber(1)
|   +-TimeTicks ptgTableLastChange(2)
|
+ -ptgProtocol(2)
  |
  +-ptgTable(1)
    |
    +-ptgEntry(1)
    |   Index: ptgIndex
    |
    +-Integer32 ptgIndex(1)
    +-String ptgName(2)
    +-String ptgDescr(3)
    +-TimeTicks ptgLastChange(4)
    +-Counter ptgBytes(5)
    +-Counter ptgPkts(6)
```

Número de protocolos
configurados

Definição da tabela
de informações

Nome do protocolo
Descrição
Bytes transferidos
Pacotes trafegados



Módulo de Relatório

Desenvolvimento do Coletor de Dados

- *Thread* específica para extrair as informações dos contadores de cada fila de controle dos protocolos P2P configurados
 - `ptg_get_stat`
 - `DIOCGETQSTATS`
- Sumarização dos contadores
- Disponibilização dos dados para o uso do agente SNMP



Módulo Principal

- Responsável pela correta **inicialização do sistema PTGUARD**
 - Leitura do arquivo de configuração padrão XML
 - protocolos configurados
 - regra configurada no Snort
 - Inicialização dos demais módulos e *threads* do programa
 - Controlar toda a **comunicação entre os módulos**
 - endereços armazenados nas tabelas utilizadas nas regras *ptgtbl*
 - regras de filtragem referente as regras *ptgblk*



Regras de Detecção



Testes e Resultados

- Testes para as regras de detecção dos protocolos P2P utilizadas pelo Snort
 - falso-negativos
 - falso-positivos
- Testes da utilização do sistema PTGUARD
 - Desempenho e alocação de recursos
 - Bloqueio
 - Controle de banda
 - Utilização de banda de rede



Testes para as Regras de Detecção falso-negativo

Protocolo	Regras	Pacotes analisados	Estatística por protocolo	Alertas	Falso-negativos
BitTorrent	8	3464	TCP: 3464 (100.000%) UDP: 0 (0.000%)	123	0
DirectConnect	6	1213	TCP: 1213 (100.000%) UDP: 0 (0.000%)	14	0
eDonkey/ Overnet	20	1122	TCP: 1089 (97.059%) UDP: 33 (2.941%)	95	0
FastTrack	4	1102	TCP: 1049 (95.553%) UDP: 53 (4.447%)	24	0
Gnutella	6	1573	TCP: 1048 (66.624%) UDP: 525 (33.376%)	23	0
MP2P	8	1283	TCP: 519 (40.452%) UDP: 764 (59.548%)	411	0
RTSP	12	1589	TCP: 1589 (100.000%) UDP: 0 (0.000%)	9	0



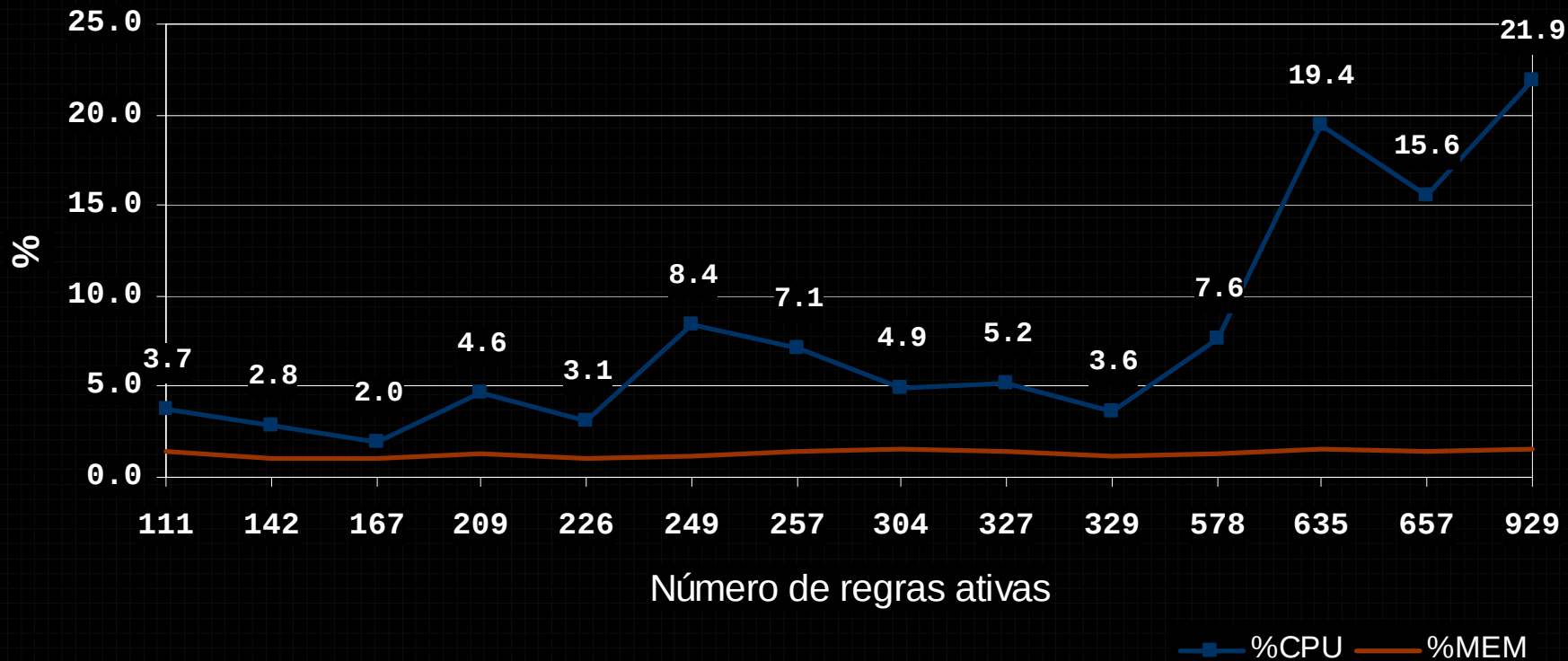
Testes para as Regras de Detecção falso-positivo

Protocolo	Regras	Pacotes analisados	Estatística por protocolo	Alertas	Falso-positivos
BitTorrent	8	Total: 35555 Analisados: 35555 Descartados: 0	TCP: 34867 (98.065%) UDP: 614 (1.727%) ICMP: 37 (0.104%)	23	0
DirectConnect	6	Total: 28504 Analisados: 28504 Descartados: 0	TCP: 27923 (94.463%) UDP: 535 (1.877%) ICMP: 31 (0.109%)	8	0
eDonkey/ Overnet	20	Total: 13553 Analisados: 13553 Descartados: 0	TCP: 12469 (92.002%) UDP: 973 (7.179%) ICMP: 64 (0.472%)	387	0
FastTrack	4	Total: 22657 Analisados: 22657 Descartados: 0	TCP: 21000 (92.687%) UDP: 1495 (6.598%) ICMP: 106 (0.468%)	16	0
Gnutella	6	Total: 42836 Analisados: 42836 Descartados: 0	TCP: 40464 (94.463%) UDP: 2164 (5.052%) ICMP: 120 (0.280%)	56	0
MP2P	8	Total: 57180 Analisados: 56202 Descartados: 978	TCP: 48602 (84.998%) UDP: 6166 (10.783%) ICMP: 449 (0.785%)	5027	0
RTSP	12	Total: 1902 Analisados: 1902 Descartados: 0	TCP: 1672 (87.907%) UDP: 203 (10.673%) ICMP: 13 (0.683%)	3	0



Desempenho e Alocação de Recursos

Alocação de Recursos





Configuração: Bloqueio

Protocolo Analisado	Teste de bloqueio	Observações
BitTorrent	OK	
Direct Conect	OK	
eDonkey / Overnet	OK	
FastTrack	FALHOU	Impossibilidade do desenvolvimento de uma regra de detecção para identificar a requisição de um cliente na rede.
Gnutella	OK	
MP2P	FALHOU	Ocorrência de uma condição de erro ao acessar o dispositivo /dev/pf. Esse erro foi provocado pelo mecanismo de conexão do cliente da rede MP2P.



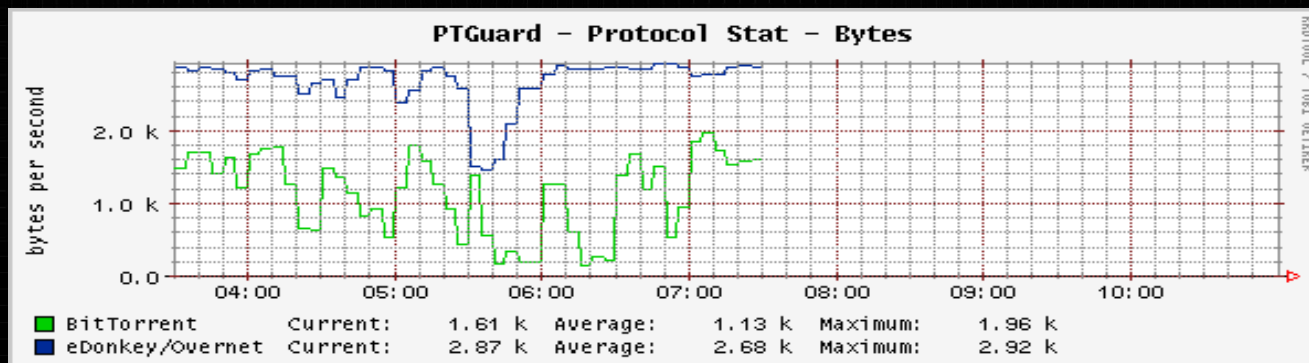
Configuração: Controle de Banda

Protocolo	Teste de controle / com porta padrão	Observações
BitTorrent	OK / OK	Porta padrão: 6881
DC	OK / Não aplicável	O protocolo não possui uma porta padrão de comunicação entre os clientes participantes da rede.
eDonkey / Overnet	OK / OK	Porta padrão: 4662
FastTrack	OK / OK	Porta padrão: 1214
Gnutella	OK / OK	Porta padrão: 6346
MP2P	OK / Não aplicável	O protocolo não possui porta padrão para a transferência de arquivos.
RTSP	OK / OK	Porta padrão: 554

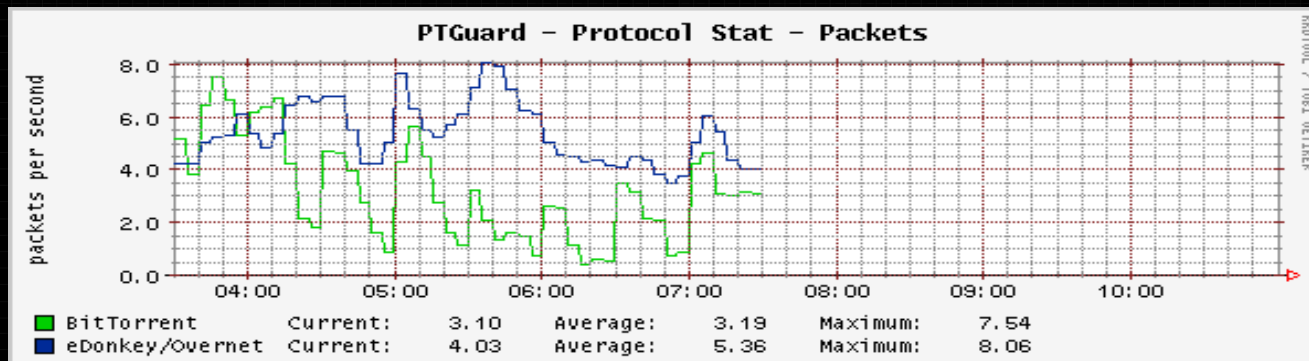


Utilização da Banda de Rede

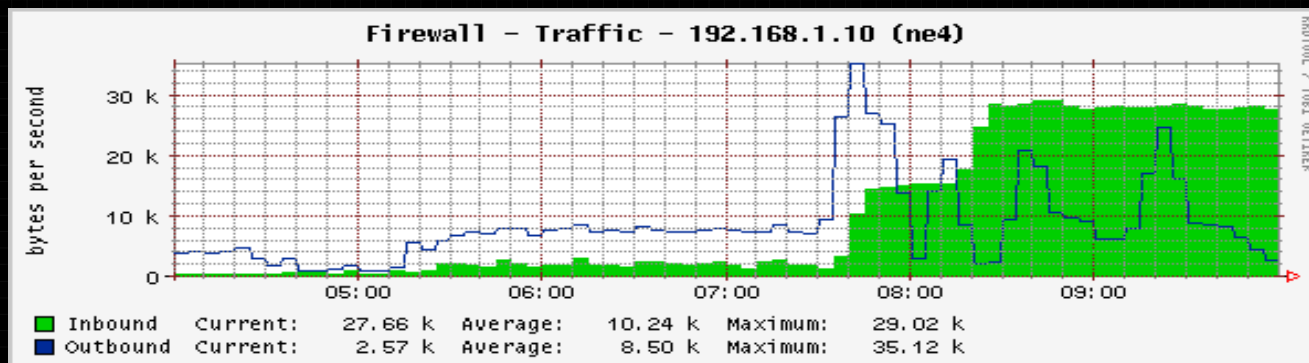
Bytes por seg.
BitTorrent
eDonkey/Overnet



Pacotes por seg.
BitTorrent
eDonkey/Overnet



Utilização da
banda de rede





Conclusão

- Ganho de visibilidade na rede e na performance das aplicações
- Controle da performance das aplicações de missão crítica
- Controle do tráfego para alocação de recursos
- Acelerar a performance do tráfego crítico



Use this slide for longer titles