UNIVERSIDADE FEDERAL FLUMINENSE

Raphael Ruiz Martins

Uma Estratégia de Monitoramento do Tráfego de Redes baseada em NetFlow/IPFIX

Niterói / 2010

UNIVERSIDADE FEDERAL FLUMINENSE

RAPHAEL RUIZ MARTINS

Uma Estratégia de Monitoramento do Tráfego de Redes baseada em NetFlow/IPFIX

Dissertação de Mestrado submetida ao curso de Mestrado em Engenharia de Telecomunicações da Universidade Federal Fluminense, como requisito parcial para a obtenção do Grau de Mestre. Área de concentração: Sistemas de Telecomunicações. Linha de Pesquisa: Sistemas de Comunicação de Dados e Multimídia.

Orientador:

Luiz Claudio Schara Magalhães

NITEROI

2010

RAPHAEL RUIZ MARTINS

Uma Estratégia de Monitoramento do Tráfego de Redes baseada em NetFlow/IPFIX

Dissertação de Mestrado submetida ao curso de Mestrado em Engenharia de Telecomunicações da Universidade Federal Fluminense, como requisito parcial para a obtenção do Grau de Mestre. *Área de concentração:* Sistemas de Telecomunicações. *Linha de Pesquisa:* Sistemas de Comunicação de Dados e Multimídia.

Aprovada em 25 de novembro de 2010.

BANCA EXAMINADORA

_____

Luiz Claudio Schara Magalhães, Ph.D.
Universidade Federal Fluminense

_____

José Augusto Suruagy Monteiro, Ph.D.
Universidade Salvador - UNIFACS

_____

Carlos Alberto Malcher Bastos, D.Sc.
Universidade Federal Fluminense

Niterói
2010

Agradecimentos

A Deus por me permitir chegar até aqui.

Ao meu orientador por ter confiado a mim este trabalho e por viabilizar os recursos necessários a sua execução.

Aos meus pais pela educação recebida, pelo amor, proteção e por sempre acreditarem em mim.

A minha esposa Simone ao meu filho Philipe por todas as minhas ausências e por toda a colaboração.

Ao João pela amizade e por toda a ajuda que tanto enriqueceram este trabalho.

A todos os diretores do HUAP pelo apoio e incentivo.

Ao colega de Luiz Eduardo, pela valiosa dica sobre monitoramento de fluxos.

A toda a equipe da Assessoria de Informática do Hospital Universitário Antonio Pedro, particularmente ao meu amigo Rubinho.

Aos meus irmãos Alex e J. Junior pela lealdade e dedicação.

A toda a equipe do Núcleo de Tecnologia da Informação da UFF, particularmente ao Leonardo Rizzo, Felipe Pimenta e ao Alan durante as sucessivas ligações e acertos no servidor de monitoramento.

A toda a equipe do Mídiacom em particular aos ex-alunos Felipe Maia, Douglas e ao mais novo prof. do Departamento de Telecomunicações, Ricardo Carrano.

Resumo

O uso da Internet como ferramenta de trabalho vem crescendo a cada ano. Cada vez mais empresas dependem de recursos disponíveis exclusivamente na rede global e interrupções ou lentidão no acesso pode causar prejuízos consideráveis.

A crescente demanda por conectividade, disponibilidade e largura de banda torna essencial o gerenciamento da rede como forma de garantir condições de funcionamento. Neste cenário, o planejamento gerencial precisa ser fundamentado em diversas fontes de informações, sendo uma importante fonte o monitoramento do uso da rede.

Analisando as tecnologias existentes para monitoramento do uso da rede, as que se baseiam nos fluxos (Netflow/ IPFIX) têm se mostrado mais eficientes. Partindo deste conceito, já estão disponíveis aplicações *open source*, que permitem visualizar gráficos de intensidade do uso da rede, fornecendo informações detalhadas sobre a origem e o destino das transmissões.

Este trabalho apresenta um estudo de caso do monitoramento de redes da Universidade Federal Fluminense, considerada um WAN que atende, além dos campi localizados em Niterói, outras cidades no estado do Rio de Janeiro como Volta Redonda, Bom Jesus de Itabapoama e Rio das Ostras, além de Oriximiná no Pará. Através deste estudo demonstrou-se como as informações podem ser obtidas a partir do monitoramento de fluxos, e a importância da utilização dessa tecnologia para a garantia da qualidade e segurança das comunicações em redes de computadores.

Palavras chave: monitoramento de redes, fluxos, medições, redes de computadores, Internet.

Abstract

The use of the Internet as a business tool is growing every year. More and more companies depend on resources available exclusively on the global network, and interruptions or delays in access can cause considerable loss of revenue.

Considering the increasing demand for connectivity, availability and bandwidth, network management becomes an essential activity to ensure necessary conditions for network operation. In this scenario, the managing and planning must be based on several sources of information, and monitoring network usage is a rich source of information.

Analyzing the existing technology for monitoring network usage, those based on flows (NetFlow / IPFIX) have been shown more efficient than other technologies, and *open source* applications to visualize network use are already available, providing detailed information on the origin and destination of transmissions.

This work presents a case study of using of the Universidade Federal Fluminense (Niterói, Brasil) network, which is considered a WAN that serves, in addition to the campuses in Niterói, other cities in the estate of Rio de Janeiro such as Volta Redonda, Bom Jesus de Itabapoana, Rio das Ostras and also Oriximiná (Pará). Through this study, it was shown how information can be obtained from the flows monitoring and the importance of using this technology for ensuring quality and security of communications in computer networks.

Key words: network management, flow, measure, computers network, Internet.

Glossário

FIN: Sinalização do protocolo TCP para desconexão;
FTP: File Transfer Protocol;
ICMP: Internet Control Message Protocol;
IDS: Intrusion Detection System;
NDIS: Network Intrusion Detection System
IETF: Internet Engineering Task Force;
IP: Internet Protocol;
ISO: International Organization for Standardization;
LAN: Local Area Network;
MIB: Management Information Base
MPLS: Multi Protocol Label Switch;
PFR: Padrão de funcionamento da rede;
QoS: Quality of Service;
RFC: Request for comments;
SLA: Service Level Agreement;
SNMP: Simple Network Management Protocol;
SYN: Sinalização do protocolo TCP para início de conexão;
TCP: Transmission Control Protocol;
UDP: User Datagram Protocol;
VLAN: Virtual Lan;
WAN: Wide Area Network;

Sumário

Agradecimentos ..... *IV*
Resumo ..... *V*
Abstract ..... *VI*
Glossário ..... *VI*
Lista de figuras ..... *IV*

Capítulo I. - Introdução 1

1.1 A Rede UFF 2
1.2 Motivação 6
1.3 Objetivos 8
1.4 Organização da Dissertação 8

Capítulo II - Monitoramento de rede 9

2.0 Monitoramento de redes. 11
2.1 Sistemas de Monitoramento de redes 12
2.2 Traduzindo os registros obtidos através do monitoramento de redes. 13
2.3 Padrões de funcionamento da rede (PFR). 14
2.4 Aspectos sobre monitoramento de redes. 15
2.5 Tecnologias para monitoramento de redes. 16
2.6 Revisão da literatura. 22

Capítulo III - Estudo de caso 26

3.1 Objetivos 26
3.2 Metodologia utilizada 26
3.3 Criando perfis para armazenamento de fluxos. 30
3.4 Perfil RedeUFF 30
3.5 Perfil PROTOCOLOS 31
3.6 Perfil Anel UFF 32
3.7 Recursos utilizados 33
3.8 Scripts 33
3.9 Ajustes dos parâmetros para captura dos fluxos 34
3.10 Obtendo os dados 40
3.11 Criando perfis 41
3.12 Criando filtros 42

Capítulo IV. - Avaliação e resultados 44
4.1 Análises dos resultados por perfil. 44
4.2 Perfis Redes UFF 44
4.3 Processamento dos dados coletados – Execução dos scripts 53
4.4 Resultados obtidos 56
4.5 Utilização dos dados registrados. 60
4.6 Obtendo o PFR da rede. 67
4.7 Perfil PROTOCOLOS 69
4.8 Perfil Anel UFF 75
4.9 Perfil Live 77
4.10 Segurança 83
4.11 Origens e padrões de atividade de rede 84
4.12 Atividades de rede por origem 85
4.13 Incidentes de segurança e as portas do protocolo TCP/IP. 85
4.14 Alteração do PFR e detecção de incidentes de segurança. 86
4.15 Coletânea de casos de segurança 87
4.22 Programando alertas 101
4.23 Analisando os alertas emitidos 103
4.24 Simulando alertas 107
4.25 Recomendações 107
Capítulo V - Considerações Finais. 110
5.1 Trabalhos futuros 112
Referências bibliográficas 114
Apêndices 117
Apêndice 1 - Análise de ferramentas 117
Apêndice 2 - Rotinas para coleta de dados 127

Lista de figuras

Figura I-1 - Visão dos Campi da UFF em Niterói 2
Figura I-2 - Nuvem MPLS - Extensão da Rede UFF fora de Niterói 3
Figura I-3 - Topologia física da Rede UFF 4
Figura I-4 - Enlace de fibra entre a UFF e o CBPF passando pela Ponte Rio - Niterói 5
Figura I-5 - Mapa da Rede Rio de Computadores 6
Figura II-1 - Gráfico gerado pelo sistema de monitoramento de redes Nfsen.. 15
Figura II-2 - Estrutura de funcionamento do SNMP 18
Figura II-3 - Funcionamento do Netflow 21
Figura II-4 - UDP x TCP: Tráfego não Cooperativo – IN [5] 24
Figura III-1 - Capturando pacotes da rede usando o recurso de espelhamento de porta. 28
Figura III-2 - Configuração inicial do ambiente de monitoramento da Rede UFF. 29
Figura III-3 - Configuração final do ambiente de monitoramento 30
Figura III-4 - Perfil RedesUFF – Gráfico Semanal 31
Figura III-5 - Perfil PROTOCOLOS – Gráfico semanal 32
Figura III-6 - Perfil AnelUff – Gráfico Semanal 33
Figura III-7 - Consumo de CPU pelos softwares: Softflowd, Nfdump e Nfcapd 34
Figura III-8 - Janeiro 2009. Início do período de captura de dados – Sistema Cacti. 35
Figura III-9 - Fim do período de Captura de dados – Sistema Cacti. 35
Figura III-10 - Comparação dos Registros de tráfego CACTI x NFSEN 36
Figura III-11 - Alteração dos parâmetros no gerador (SOFTLOWD) 37
Figura III-12 - Redução do uso do processador 37
Figura III-13 - Comparação dos gráficos do Nfsen e do CACTI 38
Figura III-14 - Gráfico da quantidade de fluxos 39
Figura III-15 - Tela de criação de perfil. 41
Figura III-16 - Criando os canais do perfil Protocolos para filtrar as portas desejadas 41
Figura IV-1 - Tela do Nfsen - Perfil Redes UFF - Ponteiro de Seleção de evento 46
Figura IV-2 - Painel de visualização de fluxos 47
Figura IV-3 - Gráfico das redes que utilizaram o protocolo TCP 48
Figura IV-4 - Gráfico mostrado apenas das redes que utilizaram o protocolo UDP. 48
Figura IV-5 - Gráfico mostrando apenas as redes que utilizaram o protocolo ICMP. 50
Figura IV-6 - Gráfico filtrado, duas redes. Protocolo TCP. 50
Figura IV-7 - Painel de visualização de fluxos pacotes e tráfego.. 50
Figura IV-8 - Seleção de intervalo de tempo. Entre 7h e 22h do dia 21/10. 51
Figura IV-9 - Resultado da consulta feita ao Nfsen. 51
Figura IV-10 - Soma dos dados trafegados. 51
Figura IV-11 - Tela de consulta aos arquivos do perfil. 52
Figura IV-12 - Consulta e resultado utilizando a interface web do Nfsen. 53
Figura IV-13 - Script para coleta das informações 54
Figura IV-14 - Resultado do script de totalização de dados. 55
Figura IV-15 - Pastas das redes da UFF 55
Figura IV-16 - Estrutura das pastas de armazenamento e arquivos. 56
Figura IV-17 - Sumário, resultado de uma consulta mensal utilizando Nfdump 56
Figura IV-18 - Gráficos da rede 200.20.1.0. 58
Figura IV-19 - Gráficos da rede 200.20.2.0. 59
Figura IV-20 - Gráfico da rede 200.20.7.0. 59
Figura IV-21 - Consumo percentual dos recursos da rede UFF, por rede. 61
Figura IV-22 – Result. da consulta Nfdump via script. Rede 200.20.1.0 - bytes 61
Figura IV-23 – Result. da consulta Nfdump via script. Rede 200.20.1.0 - fluxos 62
Figura IV-24 – Result. da consulta Nfdump via script. Rede 200.20.2.0 - fluxos 62
Figura IV-25 – Result. da consulta Nfdump via script. Rede 200.20.2.0 - bytes. 62
Figura IV-26 - Acessos relacionados à porta 40999, Janeiro na rede 200.20.2.0 63
Figura IV-27 – Result. da consulta Nfdump via script. Rede 200.20.7.0 - fluxos 63
Figura IV-28 – Result. da consulta Nfdump via script. Rede 200.20.7.0 - bytes. 64
Figura IV-29 - Tabulação dos sumários do perfil RedesUFF - fluxos. 64
Figura IV-30 - Comparação das redes com mais fluxos registrados - 2009 65
Figura IV-31 - Comparativo das redes com mais fluxos registrados - 2009 - Ranking. .. 66
Figura IV-32 - Percentual de utilização das portas da rede 200.20.1.0 67
Figura IV-33 - Gráfico perfil PROTOCOLOS - janeiro de 2009. 69
Figura IV-34 - Seleção de Intervalo de tempo sistema Nfsen "*Sum*" habilitada. 70

Figura IV-35 - Gráfico Perfil PROTOCOLOS. de janeiro de 2009. 71
Figura IV-36 - Gráficos de utilização da porta 53 (DNS). 72
Figura IV-37 - Gráficos de utilização da porta 80 (WEB). 72
Figura IV-38 - Gráficos de utilização da porta 110 (POP3). 72
Figura IV-39 - Gráficos de utilização da porta 443 (HTTPS) 73
Figura IV-40 - Gráficos de utilização da porta 25 (SMTP). 73
Figura IV-41 - Gráficos de utilização da porta 23 (Telnet). 73
Figura IV-42 - Gráficos de utilização da porta 22(SSH) 74
Figura IV-43 - Gráficos de utilização da porta 161(IGMP). 74
Figura IV-44 - Gráfico demonstrativo do comportamento da rede - ano novo. 74
Figura IV-45 - Gráfico mensal da atividade de rede dos switches do Anel. 76
Figura IV-46 - Perfil Anel UFF - Total de fluxos – janeiro a maio de 2009. 76
Figura IV-47 - Perfil Anel UFF - Total de pacotes – janeiro a maio de 2009. 77
Figura IV-48 - Identificando a alteração do PFR no Switch do campus HUAP. 77
Figura IV-49 - Relação das 20 portas / fluxos – janeiro 2009 79
Figura IV-50 - Relação das 20 portas / fluxos – fevereiro 2009. 79
Figura IV-51 - Relação das 20 portas / fluxos – março 2009. 80
Figura IV-52 - Relação das 20 portas / fluxos - abril 2009 80
Figura IV-53 - Gráfico anual - Nfsen 2009 > 2010. Fluxos/s. 81
Figura IV-54 - Gráfico anual - Nfsen 2009 > 2010. Bits/s. 81
Figura IV-55 - Gráfico anual - Nfsen 2009 > 2010. Pacotes/s. 82
Figura IV-56 - Gráfico perfil *Live*. 82
Figura IV-57 - Gráfico de doze horas de funcionamento do perfil Redes UFF. 84
Figura IV-58 - Detecção visual alteração PFR. 88
Figura IV-59 - Localização da rede 200.156.100.64 no painel de visualização 89
Figura IV-60 – Result. consulta ip 200.156.100.105 - porta TCP 25 89
Figura IV-61 - Detecção visual do aumento de fluxos de uma rede no gráfico do Nfsen. 90
Figura IV-62 - Gráfico do Nfsen que apresenta apenas o protocolo TCP 91
Figura IV-63 - Gráfico do Nfsen que apresenta apenas o protocolo UDP. 91
Figura IV-64 - Identificação do IP 200.20.9.67 92
Figura IV-65 Consulta detalhada aos fluxos 92
Figura IV-66 – Casos de segurança entre Fevereiro de 2008 e Novembro de 2009. 93
Figura IV-67 – Identificação visual do aumento da quantidade de fluxos. 94
Figura IV-68 - Painel de visualização, protocolo SSH (porta 22 do TCP). 94
Figura IV-69 - Resultado da consulta ao sistema Nfsen, IP 200.156.105.101. 94
Figura IV-70 - Detalhes dos acessos do host 200.156.105.101 95
Figura IV-71 - DDOS a partir de hosts da rede 200.156.105.0. 95
Figura IV-72 - Ataque Syn Flood partindo do endereço IP 200.20.11.188. 96
Figura IV-73 - Perfil PROTOCOLO apresentando alteração do PFR 97
Figura IV-74 - Painel de informações de visualização de incidentes 97
Figura IV-75 - Gráfico do Perfil RedesUff 97
Figura IV-76 - Painel de visualização do sistema Nfsen,rede 200.20.10.64 98
Figura IV-77 – Relatório mostrando os 10 IPs da UFF c/ mais atividades 98
Figura IV-78 - Perfil PROTOCOLOS. 98
Figura IV-79 – Arquivos encontrados na máquina 200.20.10.73 99
Figura IV-80 - Extração dos sumários 100
Figura IV-81 - Resultado dos cálculos p/ obter os valores de referência 100
Figura IV-82 - Simulação efetuada na planilha a partir dos dados importados. 101
Figura IV-83 - Tela de configuração de alertas do sistema Nfsen. 102
Figura IV-84 - IP 200.20.7.37 102
Figura IV-85 - Alertas disparados pelo sistema Nfsen. 103
Figura IV-86 - Informações sobre o alerta emitido no dia 02 de julho de 2009. 104
Figura IV-87 - Resultado da consulta ao sistema Nfsen 105
Figura IV-88 - Retorno ao PFR após bloqueio do trafego suspeito. 105
Figura IV-89 - Resultado da análise do alerta emitido no dia 10/09/2009. 106
Figura IV-90 - Resultado da consulta ao sistema Nfsen / porta 22. 107

Nenhum homem realmente produtivo pensa como se estivesse escrevendo uma dissertação.

Albert Einstein

Capítulo I - **Introdução**

A Internet vem crescendo a um passo cada vez maior. Segundo pesquisa [1], o acesso à Internet no Brasil alcançou 15 milhões de novas conexões no segundo semestre de 2009. Contribuem para este aumento, em primeiro lugar, a constante queda nos preços dos equipamentos que popularizou o uso dos computadores portáteis e consecutivamente das redes sem fio. Aliada a estes fatores também houve uma grande oferta de serviços disponibilizados na rede, atraindo diariamente novos usuários domésticos e corporativos. Como conseqüência, grandes desafios têm sido impostos aos administradores de rede que são os responsáveis pela garantia da qualidade e segurança dos serviços prestados. Normalmente estes serviços são regidos pelos acordos de nível de serviço, ou SLA (*Service Level Agreement*). Diante deste cenário, conhecer a utilização dos recursos da rede torna-se fundamental. As informações obtidas ao monitorar uma rede viabilizam a realização de estudos visando o planejamento das ações de curto, médio e longo prazo, além de propiciarem um profundo conhecimento do comportamento da rede sob diversas situações. Estas informações podem revelar fragilidades estruturais a serem tratadas pela equipe de segurança.

O presente trabalho vem chamar a atenção para a importância da atividade de monitoramento de redes de computadores que vem se tornando cada vez mais necessário perante o aumento do uso dos recursos computacionais interligados. A crescente capacidade das conexões e inúmeras questões de segurança, requerem tecnologias que sejam eficazes e que contribuam para a efetiva garantia da qualidade dos serviços. Neste sentido, este trabalho destaca o monitoramento de fluxos, que se baseia nas informações de origem e destino das comunicações. Esta tecnologia, inicialmente proposta pela Cisco com o nome de Netflow, já se encontra em fase de padronização pelo IETF (*Internet Enginnering Task Force*) com o nome de IPFIX

através da RFC 3917. Para avaliá-la, este trabalho apresenta um estudo de caso, tendo como cenário a rede da Universidade Federal Fluminense, abrangendo todas as suas setenta e seis subredes. Constam deste estudo os aspectos práticos da configuração e operação de um sistema totalmente *open source* (Softflowd, Nfsen e Nfdump). Os resultados apresentados foram obtidos a partir de cinco meses de medições, quando inúmeros casos de falha de segurança foram detectados pela ferramenta e são descritos em detalhes. Além disso, eles mostraram que a partir do monitoramento dos fluxos IP é possível conhecer o padrão de funcionamento da rede, designado neste trabalho como PFR, cujas informações são essenciais para a administração, planejamento e segurança.

1.1 A Rede UFF

A Universidade Federal Fluminense (UFF) é uma instituição distribuída possuindo campi em mais de dez cidades do interior do Estado do Rio de Janeiro e no estado do Pará na cidade de Oriximiná.

A grande concentração de Campi da UFF se dá em Niterói. Entretanto, mesmo nesta cidade, a maiorias dos seus campi ficam distantes uns dos outros conforme mostra a Figura I-1. Além disso, existem unidades situadas em outras cidades como Angra dos Reis, Bom Jesus do Itabapoama, Pádua, Pinheiral, Itaperuna, Rio das Ostras, Campos

Figura I-1 - Visão dos Campi da UFF em Niterói – Anel primário (cor laranja) e anel e secundário (cor verde)

dos Goitacazes, Volta Redonda, Macaé, e Oriximiná, sendo esta última a mais distante. Todas são atendidas por uma nuvem MPLS (*Multi Protocol Label Switching*), Figura I-2.

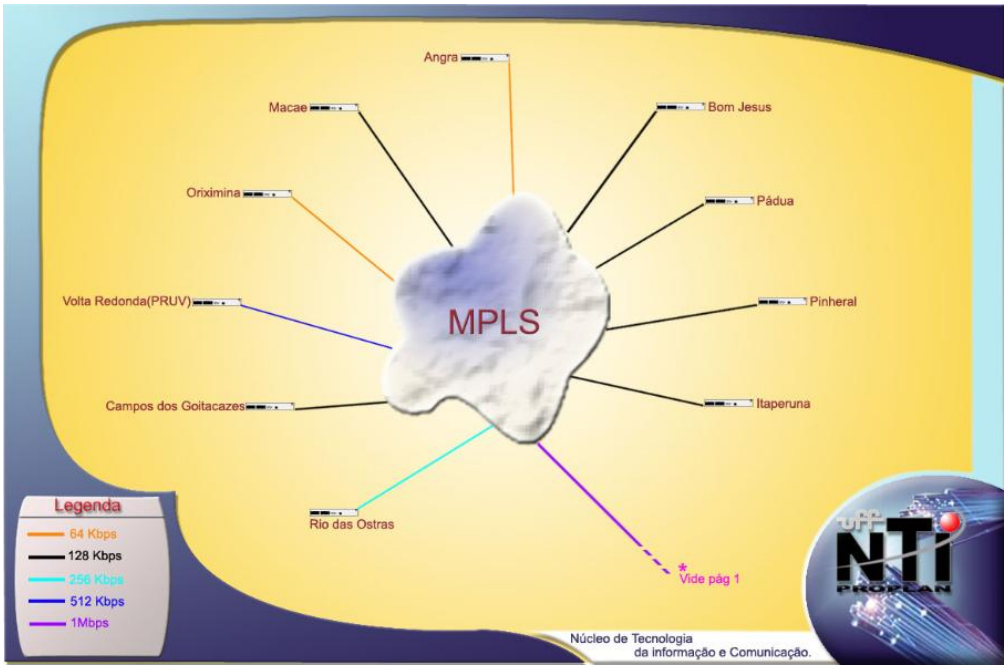


Figura I-2 - Nuvem MPLS - Extensão da Rede UFF fora de Niterói

Em 1994, a conexão externa da UFF com a Internet era feita por meio de um enlace de 64 kbps, ligando o Núcleo de Tecnologia da Informação da UFF – NTI/UFF ao *backbone* da Rede-Rio no bairro da Urca, no Rio de Janeiro. Em maio de 1998, foi inaugurada uma nova conexão, com taxa de transmissão de 2Mbps, entre a UFF e a Rede-Rio, através de um enlace de rádio entre o Centro Tecnológico (CTC) no campus da Praia Vermelha e o CBPF [2].

No início de 2002, o enlace via rádio foi atualizado para 11Mbps. Ao final de 2002, nova atualização elevou a capacidade do enlace para 34Mbps, com um novo rádio operando na freqüência de 7,5 GHz. Em abril de 2007, a conexão da UFF com a Rede Rio passou a ser por fibra ótica, pela Ponte Rio-Niterói, e com suporte a tráfego de até 100Mbit/s. Atualmente existem projetos em fase de execução para elevar a capacidade do enlace da Internet para 10Gbit/s através da substituição dos elementos ativos.

A infra-estrutura da rede da UFF tem três estruturas principais:

- as redes locais dos campi;
- a interconexão dos campi e;
- a conexão com a Internet.

As redes locais, presentes em todas as edificações da UFF são conectadas ao anel de fibra óptica que faz a interconexão entre elas, conforme mostra a Figura I-3.

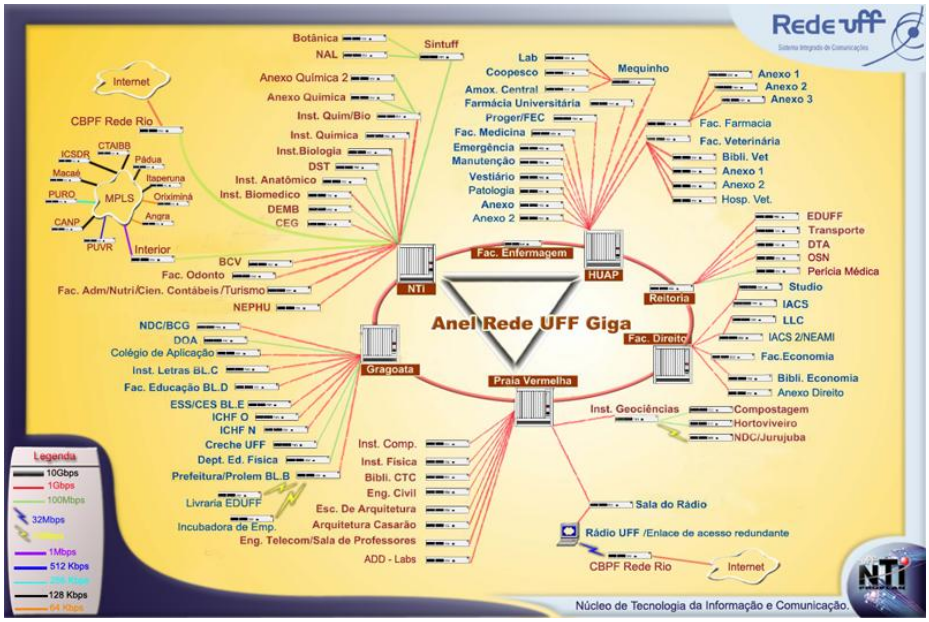


Figura I-3 - Topologia física da Rede UFF

Esta conexão se dá através de switches de borda (*border switch*) para as unidades e switches de núcleo para a espinha dorsal da rede (*backbone*). O anel possui redundância e é composto por sete switches localizados nos campi a seguir:

Principais (Taxa de 10Gbit/s)

- Campus da Praia Vermelha;
- Campus do Hospital Universitário Antonio Pedro; e
- Campus do Valonguinho.

Secundários (Taxa de 1Gbit/s)

- Campus da Reitoria;
- Campus da Faculdade de Enfermagem;

- Campus da Faculdade de Direito; e
- Campus do Gragoata.

Quando o enlace com a Rede-Rio era feito através de rádio, o campus de conexão com a Internet era o da Praia Vermelha, em função do posicionamento geográfico das antenas - visada entre o prédio da CPBF – (Centro Brasileiro de Pesquisas Físicas), na Urca e o campus da UFF. Em 2007, quando o enlace passou a ser através de fibra ótica, o campus de conexão passou a ser campus do Valonguinho, onde funciona o Núcleo de Tecnologia da Informação da UFF, (NTI/UFF), responsável pela conectividade e todos os serviços da rede. Esta fibra segue pela Ponte Rio - Niterói e vai até ao prédio da CPBF (Figura I-4).

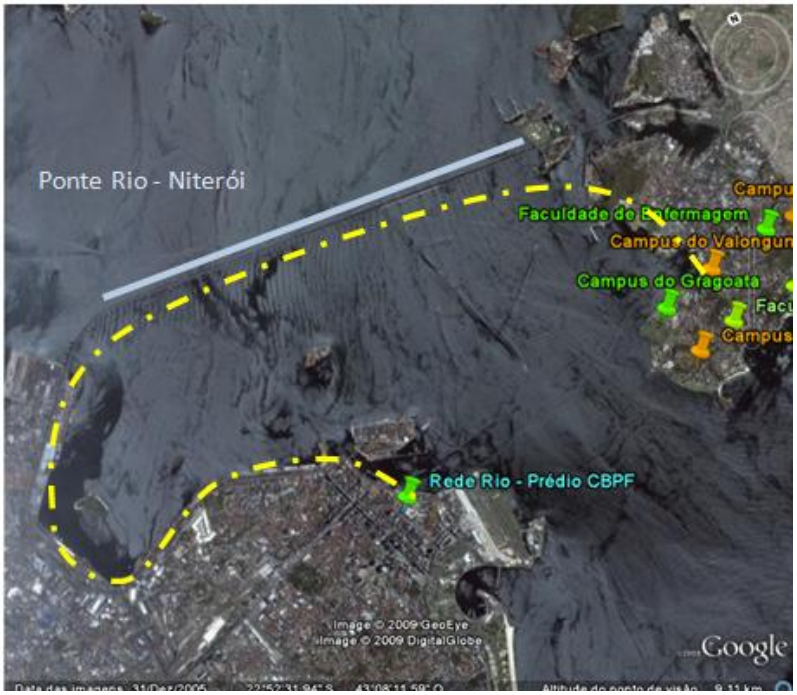


Figura I-4 - Enlace de fibra entre a UFF e o CBPF passando pela Ponte Rio - Niterói

Situado no bairro da URCA, no Rio de Janeiro, o CBPF é um dos cinco pontos principais de conexão da Rede Rio de Computadores, que em conjunto com os outros quatro formam um pentágono que dá acesso à Internet (Figura I-5) para as instituições públicas do Rio de Janeiro. Também ligado à CBPF, está a RNP (Rede Nacional de Ensino e Pesquisa), que fornece acesso aos enlaces nacionais e internacionais.

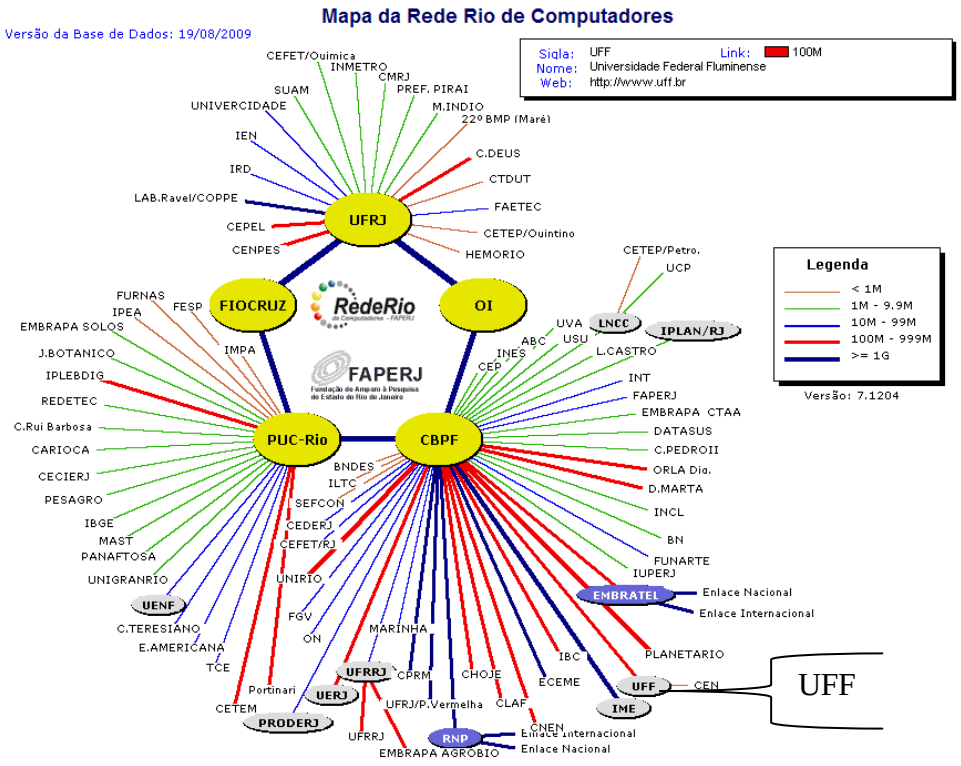


Figura I-5 - Mapa da Rede Rio de Computadores

1.2 Motivação

O monitoramento do uso da conexão de Internet (enlace com a Rede-Rio) é fundamental, considerando que atualmente são disponibilizados muitos serviços, tanto na área acadêmica quanto na área administrativa. A interrupção do acesso à Internet causa vários transtornos, podendo inviabilizar projetos, aulas, videoconferências, licitações, atrasos nas pesquisas e etc. Os administradores de rede têm enfrentado constantes ataques de vírus e de hackers que tentam incessantemente obter controle sobre os computadores para em seguida realizar outros ataques na grande rede mundial. Com o aumento da banda de conexão com a Internet, a UFF vem se tornando cada vez mais atrativa para a comunidade hacker. Sobre este aspecto, a UFF, sendo uma usuária da Rede-Rio, tem o compromisso de garantir que a utilização do enlace seja apenas para fins lícitos, devendo buscar a todo instante, formas que garantam o bom funcionamento dos recursos disponibilizados. Também para as redes locais dos Campi é de suma importância que seja feito o monitoramento do uso da Internet, considerando que uma rede isenta de vírus e hackers não destina tráfego desnecessário para o enlace de saída. Em uma audiência realizada no dia 7 de julho de 2009, a Comissão de Segurança da

Câmara dos Deputados revelou que as redes do governo (em torno de 320), sofreram em média 2000 ataques diários oriundos da Internet, segundo informações do diretor de segurança da informação do GSI (Gabinete de Segurança da Informação). Foi revelado também que, só em 2008 foram 3,8 milhões de ataques com as seguintes características: 1% de tentativas de invasão, em torno de 48 mil ataques diários; 200 novos malwares analisados a cada mês, sendo 70% objetivando informações bancárias, 15% informações pessoais, 10% informações da rede INFOSEG do Ministério da Justiça e 5% restantes buscando informações diversas. Ainda nesta pesquisa, foram relatados casos de seqüestro de senha com pedido de resgate no valor de US$350.000,00, além da utilização do espaço de armazenamento dos servidores de arquivos para publicação de propaganda, propaganda política, e exibição de filmes pornográficos contendo pedofilia [3]. Outra matéria publicada na Internet [4] relata o uso de sites do governo para elevar a posição de sites, nas pesquisas realizadas no Google, de empresas que comercializam medicamentos como Viagra. O objetivo é provocar acessos falsos partindo dos sites do governo em direção aos sites que comercializam o medicamento. Isto faz com que os mecanismos de busca do Google elevem a posição destes quando o usuário faz uma busca, que passam a ser listados entre os mais acessados.

Além da questão da utilização indevida, ameaças vindas da Internet podem deixar isolados diversos campi. Dependendo da intensidade do ataque, os recursos da rede (principalmente a memória utilizada pelas tabelas de rotas e de endereços físicos), podem ser esgotados levando o equipamento ao estado de inoperância, causando em resultado a paralisação da rede. Se o equipamento em questão for responsável por outras funções como, por exemplo, Redes Virtuais (VLAN - *Virtual LAN*) de uso exclusivo do Campus, até os sistemas internos serão comprometidos. Em outros casos, ataques utilizando o protocolo UDP, que é considerado não amigável para o protocolo TCP, acarretam a total utilização do enlace, conforme foi demonstrado em [5].

A crescente utilização de recursos multimídia através de sites como YouTube (www.youtube.com), Orkut (www.orkut.com), MySpace (www.myspace.com), trazem uma carga acentuada com grandes contribuições nos percentuais de utilização da conexão disponível. Do mesmo modo estima-se que as aplicações do tipo P2P, representem entre 80-90% do tráfego local e 40-60 % do trafego de saída [6]. Sendo

assim, o presente trabalho é motivado pela necessidade de monitoramento de redes frente aos desafios relacionados.

1.3 Objetivos

Os principais objetivos deste trabalho são:

a. Analisar as tecnologias disponíveis para o monitoramento da utilização da rede.

b. Realizar um estudo de caso tendo como cenário a rede da Universidade Federal Fluminense visando obter informações que caracterizem a utilização da conexão de Internet para cada uma das 76 (setenta e seis subredes).

c. Analisar os resultados obtidos ao longo de cinco meses de utilização

1.4 Organização da Dissertação

Este trabalho está organizado da seguinte maneira. O capítulo 2 apresenta um panorama sobre gerenciamento de redes, mostrando a evolução dessa atividade e as tecnologias que foram consolidadas ao longo do tempo. Em seguida é feita a revisão da bibliografia. O capítulo 3 descreve o estudo de caso e no capítulo 4 são apresentados os resultados obtidos, através da avaliação dos resultados. No capítulo 5 são feitas as considerações finais, apontando os trabalhos futuros. Também estão presentes no trabalho, dois apêndices: o apêndice 1 que faz a análise de duas ferramentas de monitoramento de rede além de detalhar os aspectos técnicos das ferramentas utilizadas no estudo de caso e o apêndice 2 que contém exemplos dos principais scripts utilizados.

O estudo em geral, a busca da verdade e da beleza são domínios em que nos é consentido permanecer crianças por toda a vida.

Albert Einstein

Capítulo II - **Monitoramento de rede**

No início dos anos 80, houve um grande crescimento da utilização das redes de computadores nas empresas, já que a implementação dessa tecnologia mostrava-se bastante vantajosa pela baixa relação custo/benefício. Surgia neste cenário uma urgente necessidade de automatização do gerenciamento de rede [**7]**. Com este objetivo, a ISO (*International Organization for Standardization),* através da norma ISO 7498, criou um modelo de gerenciamento de redes dividido em cinco áreas conceituais:

- Gerenciamento de falhas;
- Gerenciamento de contabilização;
- Gerenciamento de configurações;
- Gerenciamento de desempenho; e
- Gerenciamento de segurança.

O presente trabalho está relacionado a três áreas de gerenciamento ISO/IEC 7498-4 conforme descrito na Tabela I:

- Gerenciamento do desempenho;
- Gerenciamento de contabilização; e
- Gerenciamento da segurança.

Tabela I - Aspectos gerais de cada uma das áreas de gerenciamentos - ISO/IEC 7498-4.

Área	Objetivo
Gerenciamento de falhas	O gerenciamento de falhas engloba detecção de falhas, o isolamento e a correção de situações anormais no ambiente OSI (*Open System Interconnection*). As falhas levam os sistemas abertos a deixarem de cumprir seus objetivos e podem ser persistentes ou transitórias. Falhas se manifestam como eventos particulares no funcionamento de uma rede. A detecção de erro provê a capacidade de reconhecer estas falhas. O gerenciamento de falhas inclui funções para: • manter e examinar logs de erros; • aceitar e agir sobre notificações de detecção de erro; • rastrear e identificar falhas; • realizar sequências de diagnósticos e testes; e • corrigir falhas.
Gerenciamento de contabilização	O gerenciamento de contabilização permite estabelecer encargos ao uso dos recursos da rede. Inclui funções de: • Informar aos usuários sobre os recursos consumidos ou custos associados à utilização destes; • Permitir limitar o uso dos recursos e estabelecer tarifas para os recursos utilizados, diferenciados por horários; e • Permitir combinação de custos onde múltiplos recursos são requeridos para alcançar um determinado objetivo de comunicação.
Gerenciamento de configuração	O gerenciamento de configuração identifica, exerce controle sobre, coleta e provê dados com o objetivo de preparação e inicialização, além de prover o funcionamento contínuo e finalização de serviços interconectados. Inclui funções para: • Configurar os parâmetros que controlam a rotina operacional do sistema aberto; • Associar nomes aos objetos gerenciados e configurá-

	los; • Inicializar e fechar objetos gerenciados; • Coletar informações, sob demanda, sobre a condição atual do sistema aberto; e Obter anúncios de mudanças significativas nas condições dos sistemas abertos.
Gerenciamento de desempenho	Tem como objetivo gerenciar o desempenho dos recursos no ambiente OSI e a efetividade das atividades de comunicação a serem avaliadas. Inclui funções para: • Obter informações estatísticas; • Manter e examinar os logs históricos do estado do sistema; • Determinar o desempenho do sistema sob condições naturais e artificiais; e • Alterar os modos de operação do sistema para manter o desempenho dos objetos gerenciados.
Gerenciamento de segurança	O objetivo do gerenciamento de segurança é apoiar a aplicação de políticas de segurança por meio de funções que incluem: • A criação, exclusão e controle de serviços e mecanismos de segurança; • A distribuição de informação de segurança relevante; e • A comunicação de incidentes de segurança relevantes.

2.0 Monitoramento de redes.

Uma das principais atividades do gerenciamento de redes é o monitoramento. Esta tarefa consiste na coleta e registro de informações, obtidas a partir do funcionamento dos elementos que a compõem. Os objetivos desta tarefa podem ser variados, como por exemplo: estatísticos, manutenção de um estado, programação de alertas, dentre outros. A análise pode ser feita por um período, ou de forma contínua e, ainda, com base em

tecnologias diversas, muitas delas ainda em fase de desenvolvimento. Para escolher a melhor tecnologia de monitoramento de redes é necessário conhecer os objetivos do monitoramento para então selecionar os dados a serem coletados. A coleta dos dados corretos leva aos resultados esperados. Por exemplo, se o que se deseja saber é o percentual de disponibilidade mensal da rede, será necessário registrar dados que reflitam esta disponibilidade, como por exemplo, a quantidade de horas por mês que a rede ficou indisponível. Se por outro lado, o que se deseja saber são os horários de maior utilização, uma estratégia seria registrar, em períodos pré-estabelecidos, o total de bytes trafegados.

O monitoramento de redes está dividido em dois métodos: ativo e passivo. No método ativo, um tráfego de prova é gerado e transmitido de forma controlada ao longo de um ou mais caminhos (roteadores) da rede. Durante a transmissão, é observada nos receptores, a qualidade (características) dos dados trafegados. As métricas tradicionais de desempenho de rede são: retardo, perda de pacotes e vazão [8].

Ao utilizar este método é preciso considerar dois aspectos: o primeiro é que o desempenho da rede é afetado pelo próprio tráfego de prova e a segunda é que nos casos em que o roteamento seja dinâmico, o desempenho da medição pode ser melhor ou pior em função da rota escolhida. No método passivo, o tráfego real ou sua estatística é capturado em um ou mais pontos da rede, para então serem analisados [9].

2.1 Sistemas de Monitoramento de redes

Para facilitar a tarefa de monitoramento de redes foram criados softwares conhecidos como ”Sistemas de Monitoramento de Redes”. Eles agregam as tecnologias existentes na análise de redes à flexibilidade de programação, tornando a coleta e, muitas vezes a análise dos dados, um processo automatizado. No apêndice 2 “Análises de ferramentas” apresentaremos o teste de dois sistemas de monitoramento, Cacti e Dview.

Um dos recursos essenciais que deve estar presente em um sistema de monitoramento é o armazenamento dos dados coletados, visando a formação de históricos. A partir dos históricos de atividade de uma rede são feitas as análises, que podem servir a diversas finalidades como o planejamento de curto, médio e longo prazo visando a garantia da qualidade dos serviços executados na rede. Outro uso dos registros visa a garantia do

funcionamento da rede de acordo com critérios previamente estabelecidos como, por exemplo, os SLAs (*Service Level Agreements*). Os provedores de serviços na área de telecomunicações, cujos contratos estejam baseados em SLAs, devem adotar como prática o constante monitoramento das redes sob sua responsabilidade. Negligenciar tal controle pode acarretar prejuízos à empresa

2.2 Traduzindo os registros obtidos através do monitoramento de redes.

Os registros obtidos através do monitoramento de redes, como dados referente às conexões de rede, quanto tempo duraram e quais protocolos e portas foram usadas, podem revelar aspectos normalmente não evidenciados, dentre os quais podemos citar a tentativa de invasão. O armazenamento dos registros em banco de dados relacionais permite o cruzamento de informações. Assim, por exemplo, caso pretendamos saber quais foram os hosts que nos últimos seis meses trafegaram dados utilizando a porta 25 do protocolo TCP, entre 23h50m e 5h da manhã e com velocidade acima de 5Mbit/s, basta uma simples consulta aos dados armazenados. Além disso, depois de algum tempo monitorando a rede, as estatísticas do tráfego podem ser utilizadas para classificar a sua atividade em estados como:

- ociosa (Atividade da rede abaixo da média registrada de um período)
- normal (atividade da rede dentro da média registrada de um período)
- atividade extra (atividade da rede acima da média registrada de um período)
- anormal (Atividade de rede totalmente diferente dos padrões vistos anteriormente – Ex: Picos de utilização sem correspondência no histórico da rede).

Conhecer o conjunto de portas e protocolos mais utilizados revela aspectos importantes, como por exemplo: se nos registros de tráfego de saída, encontram-se as portas 80, 25, 110, 53 dentre as dez mais utilizadas, podemos dizer a princípio que esta é uma rede clássica e seus usuários de hábitos conservadores. Por outro lado se estas portas estão relacionadas entre as dez mais utilizadas nos registros do tráfego de entrada, isto pode significar que esta rede hospeda servidores Web, e-mail e DNS.

2.3 Padrões de funcionamento da rede (PFR).

Conhecer os padrões de funcionamento da rede, em seus diversos estados, é extremamente valioso para um administrador de redes. Quando algo não funciona como deveria é preciso ter parâmetros para avaliar se o que está sendo observado é normal ou não. O conjunto dos dados registrados em função da atividade de uma rede, em determinado período permite estabelecer, o que passaremos a chamar de PFR – Padrão de Funcionamento da Rede. O PFR pode ser considerado como um agregado de informações oriundas do tráfego de determinada rede, em determinado período, cujos elementos participantes são identificados com detalhes. Abaixo listamos como exemplo, algumas informações que podem compor um PFR.

- Total de fluxos registrados
- Total de bytes transmitidos
- Total de pacotes transmitidos
- As portas de origem mais utilizadas
- As portas de destino mais utilizadas

No capítulo 3, apresentaremos um estudo de caso onde após cinco meses de monitoramento foi possível conhecer o PFR de cada um das 76 redes da UFF. Na Figura II-1, é possível identificar claramente uma mudança do PFR. Devemos observar que a rede identificada pela cor azul-escuro apresenta seu comportamento alterado por volta das 12h, quando a quantidade de fluxos é elevada drasticamente. Deve-se ressaltar, entretanto, que esta alteração repentina pode ser considerada normal se houver regularidade nos eventos.

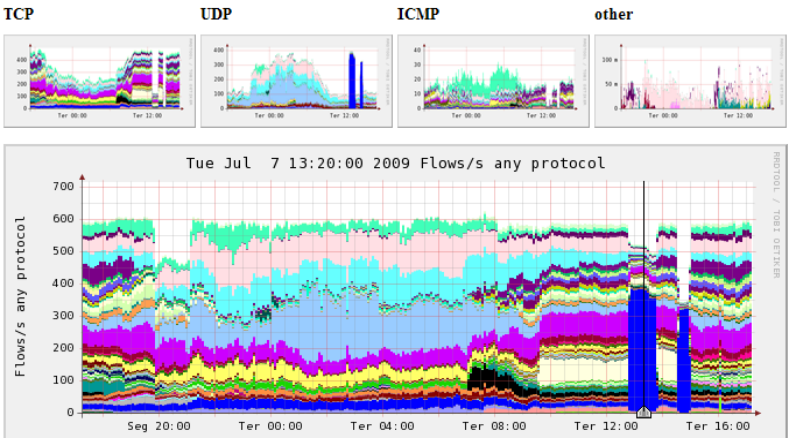


Figura II-1 - Gráfico gerado pelo sistema de monitoramento de redes Nfsen. O gráfico demonstra em fluxos por segundo a atividade das redes que são identificadas pelas diferentes cores. É possível verificar a alteração do PFR da rede identificada pela cor azul-escuro, por volta das 12h.

2.4 Aspectos sobre monitoramento de redes.

A tarefa de monitorar uma rede se torna mais complexa ou mais simples em função de alguns aspectos como:

- Tamanho da rede;
- Política de uso da rede e de segurança; e
- Topologia física e lógica.

Veremos agora, detalhes de cada um destes aspectos.

2.5 Tamanho da rede:

A rede pode ser maior ou menor em função da quantidade de:

- Enlaces externos;
- Enlaces internos;
- Roteadores;
- Hosts;
- Servidores; e
- Usuários.

Quanto maior a rede, maior será a relação de itens a serem monitorados e consecutivamente maior a quantidade de dados a serem armazenados e analisados. O

volume de dados vai influenciar diretamente no dimensionamento do sistema de monitoramento, de forma a garantir a robustez e eficiência do processo.

2.6 Política de uso da rede e de segurança:

A existência de regras claras sobre a utilização dos recursos computacionais de uma rede permitirá a criação de alertas automatizados de violação de regras. Saber o que é permitido facilita também a análise de grandes volumes de dados, pois possibilita a localização dos padrões de tráfego em desacordo com as regras instituídas.
Considerando que a cada dia mais e mais instituições estão conectadas entre si e à Internet, a troca de tráfego entre instituições constitui um dos elos frágeis da segurança, podendo oferecer riscos ao funcionamento da rede. De nada adianta uma política de segurança altamente restritiva, em relação à Internet, se existe tráfego oriundo de "redes parceiras", que não recebem por parte de seus administradores os devidos cuidados com a segurança. Neste aspecto, o monitoramento da rede pode ajudar a identificar ameaças potenciais através da detecção da alteração do PFR.

2.7 Topologia física e lógica da rede

Para a implantação de um sistema de monitoramento eficiente é necessário conhecer a topologia física e lógica da rede. Um estudo aprofundado, relacionando os seus elementos (roteadores, servidores, gateways), política de distribuição de endereços e enlaces é o primeiro passo. Isto pode ser chamado de mapa da rede. Em função deste estudo será possível optar por uma coleta de dados distribuída ou centralizada. Este aspecto é importante, pois dele dependerá a eficiência da captura do tráfego, considerando a necessidade do sistema receber informações sobre o tráfego de todos os segmentos que compõem a rede.

2.8 Tecnologias para monitoramento de redes.

A preocupação com o gerenciamento da rede nasceu junto com a elaboração do protocolo IP. Em [10] é citado a queda da Arpanet em 27 de outubro de 1980. Neste período um dos únicos recursos disponíveis aos administradores de rede era o ICMP [11] que tinha como objetivo principal reportar erros nos datagramas IP. A partir da proposta do modelo OSI para o gerenciamento de redes, surgiram vários protocolos dentre os quais podemos citar o CMISE/CMIP (*Common Management Information*

Service / Common Management Information Protocol) e o SNMP (*Simple Network Management Protocol*). Ambas as propostas tinham como idéia básica o processo "gerente / agente" onde um processo gerente requisita aos processos agentes, informações sobre o estado de funcionamento dos elementos da rede. Na prática o SNMP mostrou-se de fácil implementação, popularizando-se rapidamente. Hoje o protocolo SNMP está presente em todos os dispositivos gerenciáveis. O mesmo não ocorreu com CMISE/CMIP.

Vejamos a seguir o funcionamento do protocolo SNMP em detalhes.

2.9 SNMP

O SNMP é formado por uma estrutura modular. As informações são coletadas diretamente nos dispositivos de rede que possuem suporte a este protocolo, através da interação entre uma **Entidade Gerenciadora** e um **Agente de Gerenciamento**. A **Entidade Gerenciadora** pode gerenciar diversos dispositivos. Por sua vez, um dispositivo pode ter diversos **Objetos Gerenciados.** Os **Módulos MIB** são constituídos por **Objetos MIB** que em última análise constituem as funcionalidades propriamente ditas como: contabilização de perdas de pacotes, bytes transmitidos/ recebidos, taxa de transferência entre outras.

Com base na Figura II-2, iremos explicitar o funcionamento de um esquema de monitoramento baseado no protocolo SNMP, exemplificando os agentes envolvidos representados através da identificação das caixas.

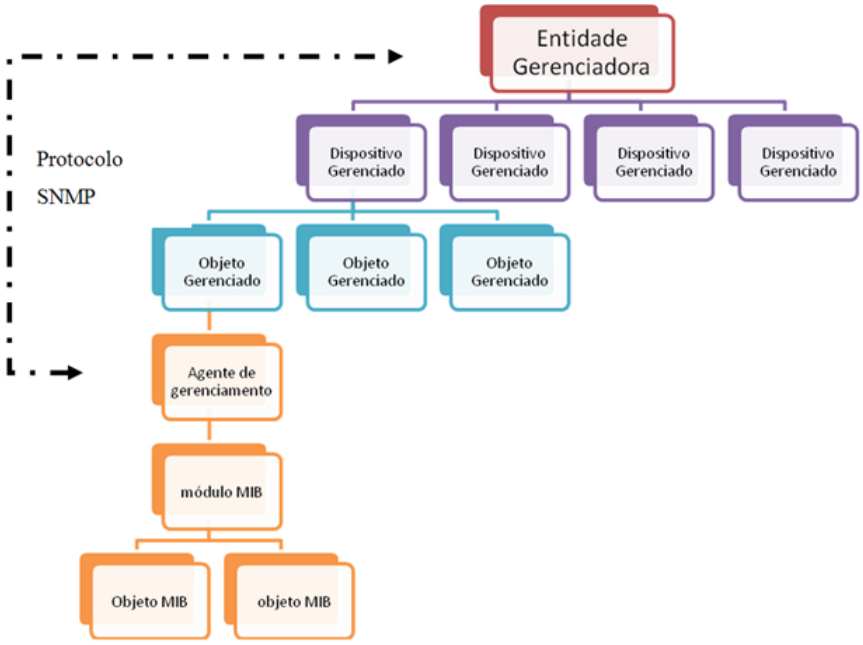


Figura II-2 - Estrutura de funcionamento do SNMP

ENTIDADE GERENCIADORA representa o NMS (*Network Management System*). Geralmente trata-se de um software sendo executado em um computador conectado à rede e que utiliza o protocolo SNMP para troca de informações com os demais componentes sob sua gerência.

DISPOSITIVO GERENCIADO é um equipamento de rede, incluindo o seu software. Pode ser um Switch, um Hub, um roteador, uma impressora ou mesmo outro computador. Como exemplo, vamos considerá-lo um Switch.

OBJETO GERENCIADO corresponde a uma parte do dispositivo gerenciado. Pode ser o processador, uma placa de rede ou um sensor de temperatura. Ainda para nosso exemplo, vamos considerar que este "Objeto Gerenciado" corresponde a uma das interfaces do "Dispositivo Gerenciado".

AGENTE DE GERENCIAMENTO corresponde a um processo sendo executado no Dispositivo Gerenciado. Este processo se comunica com a Entidade Gerenciadora recebendo comandos diversos para efeito de leitura e gravação de informações ou mesmo para comandar ações no Dispositivo Gerenciado.

MÓDULO MIB e OBJETO MIB formam o que podemos chamar de base de dados de informações do objeto gerenciado. Um OBJETO MIB pode ser um contador de pacotes, um contador de erros em uma interface ou um registrador do valor máximo da temperatura alcançada por um processador. Um conjunto de Objetos MIB forma uma MIB (*Management Information Base*).

Para nosso exemplo vamos considerar que o MÓDULO MIB possui três OBJETOS MIB: um para o registro dos pacotes descartados, um para o registro dos pacotes recebidos e outro para registrar os pacotes transmitidos. Neste cenário várias configurações podem ser efetuadas, por exemplo: a ENTIDADE GERENCIADORA, pode programar através do AGENTE DE GERENCIAMENTO, um evento em função do OBJETO MIB que registra os pacotes descartados, ou seja: "caso o percentual de pacotes descartados alcance 30%, dispare o evento". Neste caso, a ENTIDADE GERENCIADORA recebe as informações do AGENTE DE GERENCIAMENTO, por meio do protocolo SNMP, e inicia novos eventos, como por exemplo, enviar um e-mail para o administrador da rede ou até mesmo a desativar a porta.

Uma importante MIB é documentada na RFC 1757 [12] denominada RMON (*Remote Monitoring*), cujos objetivos principais são: operação *off-line*, monitoramento proativo, relato e detecção de problemas, e a possibilidade de operação de múltiplas Entidades Gerenciadoras. Umas das vantagens do RMON é a redução da troca de informação entre a Entidade gerenciadora e o Agente de monitoramento, uma vez que esta MIB prevê o armazenamento de informações do tráfego para posterior transmissão. Isto também é útil em situações onde a conectividade entre as entidades tenha sido comprometida.

No apêndice 2 são apresentadas análises de duas ferramentas de gerenciamento de redes baseados em SNMP. A primeira, desenvolvida pelo próprio fabricante dos equipamentos DLINK, chamada Dview e a segunda, *open source*, com exibição dos resultados através de gráficos gerados em função dos dados armazenados ao longo do tempo, chamada CACTI.

2.10 Monitoramento de fluxos - Netflow e IPFIX

O aumento da complexidade das redes demandou um maior detalhamento da informação sobre os dados trafegados. O SNMP, apesar de toda a sua versatilidade, não oferecia facilidades para formação de bases de dados que auxiliasse na descoberta de aspectos mais subjetivos como a disponibilização de novos serviços na rede ou da ocorrência de ataques e negação de serviço. Uma tentativa foi feita, chamada de METER MIB, padronizada pelo IETF na RFC2720 [13] de 1999, entretanto, segundo [14] não houve aceitação pela indústria. Nesta época, uma tecnologia da empresa CISCO SYSTEM chamada de Netflow, tornava-se cada vez mais popular. Em outubro de 2001, o IETF reuniu um novo grupo de trabalho para especificar os requisitos de um protocolo de exportação de dados de fluxos (IPFIX - *IP Flow Information eXport*). Era preciso algo que revelasse as tendências e comportamentos da rede levando a uma caracterização de tráfego mais detalhada e próxima dos elementos geradores de tráfego, contribuindo para atividades como engenharia de tráfego, contabilidade, segurança, entre outros. Considerando a popularização da Internet como rede global e tendo como base o protocolo IP, com seus campos de endereço de origem e de destino e portas de origem e de destino, nascia então um novo padrão de coleta de informações sobre a rede baseada nos registro dos fluxos do protocolo IP. Em 2004, a IETF liberou a RFC 3917 (*Requirements for IP Flow Information eXport (IPFIX*). Mais tarde, através da RFC3955, (após avaliação de quatro outros protocolos: CRANE, Diameter, LFAP e Streaming IPDR), selecionou o protocolo Netflow versão 9 como base para a especificação do IPFIX. A justificativa para a escolha do Netflow deveu-se à simplicidade deste protocolo [15].

2.11 Netflow

A versão 9 do protocolo Netflow apresenta o seguinte funcionamento:

“Elementos de rede (roteadores e switches) reúnem dados sobre os fluxos e exportam para um coletor. Os dados coletados fornecem uma medição de granulação fina, altamente detalhada e flexível, para contabilidade dos recursos utilizados.” [15].

Em [16], a Cisco System identifica um fluxo como um conjunto de pacotes IP, com os mesmos atributos, que atravessa um roteador ou switch. Estes atributos são a

identificação do pacote IP ou impressão digital do pacote e determina se o pacote é único ou similar a outros pacotes.

A seguir são relacionados os atributos do pacote IP usados pelo Netflow v9:

- Endereço IP de origem
- Endereço IP de destino
- Porta de origem
- Porta de destino
- Tipo de protocolo de camada 3
- Classe de Serviço
- Interface do roteador ou Switch

Todos os pacotes de mesmo endereço IP de origem e destino, porta de origem e destino, protocolo, interface e classe de serviço são agrupados em um fluxo e a partir daí pacotes e bytes são registrados. Um novo fluxo só é registrado, quando é recebido um pacote que não pertence a nenhum outro fluxo. Um fluxo é unidirecional. Isto significa que os dados enviados de uma máquina A para uma máquina B constituem um fluxo e os dados da máquina B transmitidos em resposta à transmissão inicial da máquina A constituem outro fluxo. A tecnologia é escalável, pois uma grande quantidade de informação da rede é condensada em uma base de dados chamada Netflow Cache.

A Figura II-3 ilustra o funcionamento do Netflow.

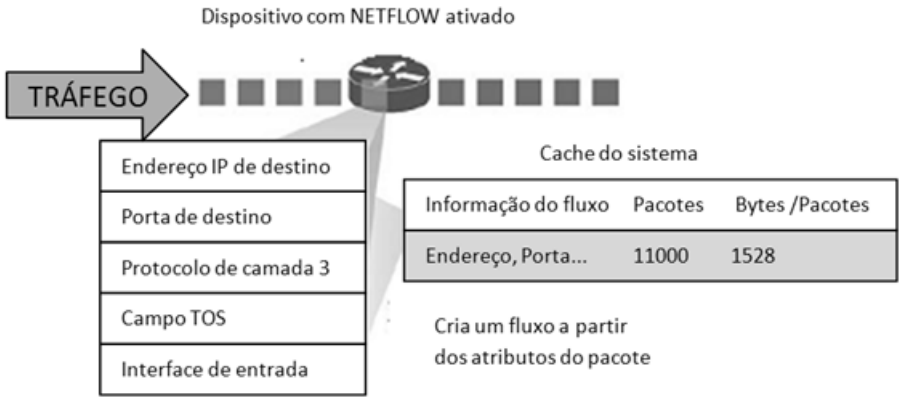


Figura II-3 - Funcionamento do Netflow

Existem duas maneiras de obter acesso aos fluxos registrados no roteador ou switch. A primeira é através da interface de comandos. Desta forma o acesso à informação é

imediato. A outra forma é exportar os fluxos para um servidor, chamado pela Cisco de Netflow Colector. O Netflow Colector tem a tarefa de montagem dos fluxos exportados além de combinar ou agregá-los para produção de relatórios que podem ser utilizados, por exemplo, para análise do tráfego e da segurança. Ao contrário do SNMP, o processo que exporta os fluxos é acionado por condicionantes próprias e uma vez configurado o IP do Netflow Colector, este receberá os fluxos sempre que:

- Um fluxo chegar ao fim (Quando o segmento TCP possuir a flag FIN)
- Quando um fluxo expirar.

Um fluxo é considerado expirado sempre que:

- Estiver inativo por um determinado tempo (Nenhum pacote é recebido para este fluxo)
- Se o tempo de vida do um fluxo for maior do que o tempo limite configurado. (longos downloads sendo executados).

O valor de tempo padrão para fluxos inativos é de 15 segundos e para o tempo máximo de vida do fluxo é de 30 minutos. Em torno de 30 a 50 fluxos são agrupados e normalmente transportados via protocolo UDP para o servidor Netflow Colector que cria um histórico a partir dos dados recebidos. Atualmente existem ferramentas que exibem gráficos diretamente dos históricos armazenados e com grande facilidade de consultas utilizando filtros por IP, PORTA ou qualquer outro atributo do IP considerado pelo protocolo Netflow. Existem também softwares que escutam o tráfego a partir de determinada interface de rede e geram os pacotes no formato Netflow, podendo exportá-los para um ou mais coletores. Isto permite que mesmo em redes que não possuam equipamentos com recurso Netflow, possamos obter suas funcionalidades por meio de softwares, muitos deles do tipo *opensource*. No subseção 3.2, analisaremos uma dessas ferramentas, o Softflowd (Software que gera e exporta pacotes no formato Netflow).

2.12 Revisão da literatura.

O artigo [17] apresenta a arquitetura de uma plataforma de medições, consolidada na ferramenta batizada de *Basic Meter*, no padrão Ipfix. O autor explica os aspectos relacionados aos métodos de medições passivas. Uma observação é feita com relação

ao uso de bases de dados do tipo SQL, que não fazem parte do padrão IPFIX. Ainda sobre armazenamento, menciona problemas relacionados ao desempenho e quanto à entrega dos resultados processados. Apesar de a ferramenta apresentada utilizar atualmente o protocolo UDP, como o Netflow, os autores informam que pretendem utilizar o protocolo TCP em conjunto com o SSL ou protocolo SCTP (RFC2960), de acordo com as recomendações do padrão IPFIX.

Em [18], são produzidos dados estatísticos sobre a utilização da conexão com a Internet pelos usuários da Universidade de Coimbra, onde a ferramenta foi testada, relacionando os protocolos utilizados. A tecnologia escolhida foi o protocolo Netflow do Cisco IOS. Inicialmente, quando a velocidade do enlace era de 2Mbps, utilizaram o software *Cisco Netflow Flow Colector* e o *Cisco Flow Analyser*. Porém o armazenamento no formato ASCII e a ineficiente gestão de armazenamento de espaço em disco, aliado ao baixo desempenho e pouca flexibilidade, determinaram a busca por outras opções. Após pesquisas iniciadas pelo CFLOWD, sem que isso satisfizesse os objetivos de obter uma visão global e simultaneamente departamental em termos de consumo e de detalhes de tráfego, optou-se por desenvolver uma solução alternativa suportada por uma base de dados relacional (*Traffic Colector / Analiser - Colana*).

O artigo [19] descreve a ferramenta FLOWTOOLS, desenvolvida pela Universidade de Ohio. Trata-se de uma suíte de ferramentas para coletar, filtrar, imprimir e analisar fluxos no formato Netflow. A motivação inicial para o desenvolvimento desta suíte foi a necessidade de determinar o percentual do tráfego de Internet utilizado pelas redes Coranet e Cicnet. Em [20] são apresentadas as direções futuras apontadas em recentes pesquisas sobre monitoramento e medição de fluxos em redes. São abordados os desafios na área como engenharia de tráfego em redes heterogêneas de larga escala, aplicações inteligentes, identificação de fluxo pesado, detecção de incidentes, análises de padrões em tempo real, alocação de recursos e otimização de QoS para classes de tráfego. Fica evidente a preocupação dos autores com o assunto de medições frente ao grande aumento da utilização da Internet. Enfatizam a tecnologia de "Medição de Fluxo Flexível" que consiste em técnicas otimizadas de captura de fluxo, que consigam observar o trafego com precisão e sem consumir demasiado processamento e memória.

Sobre a escalabilidade da tecnologia de medições de fluxos, informam que o número de fluxos ativos é uma das questões centrais sendo considerados como fatores limitantes e de precisão, citam o tamanho da memória e o poder de processamento do modulo de medição, principalmente em redes gigabits onde os recursos podem não ser suficientes para processar e armazenar todos os fluxos. Com relação a este aspecto, são abordadas técnicas de amostragem de pacotes, que buscam a otimização do uso dos recursos. Por fim, ressaltamos deste artigo, o tópico de medição de tráfego para segurança de rede e detecção de comportamentos anômalos, onde o autor mostra a importância da medição e análise do tráfego frente a desafios como detecção de anomalias em tempo real, sistemas de detecção de intrusão e análise estatística de pacotes malformados e suas origens.

Em [21] é proposto um sistema que, a partir do monitoramento de fluxos, obtém informações sobre o estado dos enlaces e tenta evitar o congestionamento do tráfego TCP causado pela utilização do protocolo UDP. Um sistema de tarifação e reserva de recursos é imposto a todo tráfego que utilize o protocolo UDP. Através de gráficos, como ilustrado na Figura II-4, o autor demonstra a proporcional degradação do desempenho do protocolo TCP em função do uso do protocolo UDP; declara ainda que este último protocolo é designado por outros autores como "*not TCP friendly*"

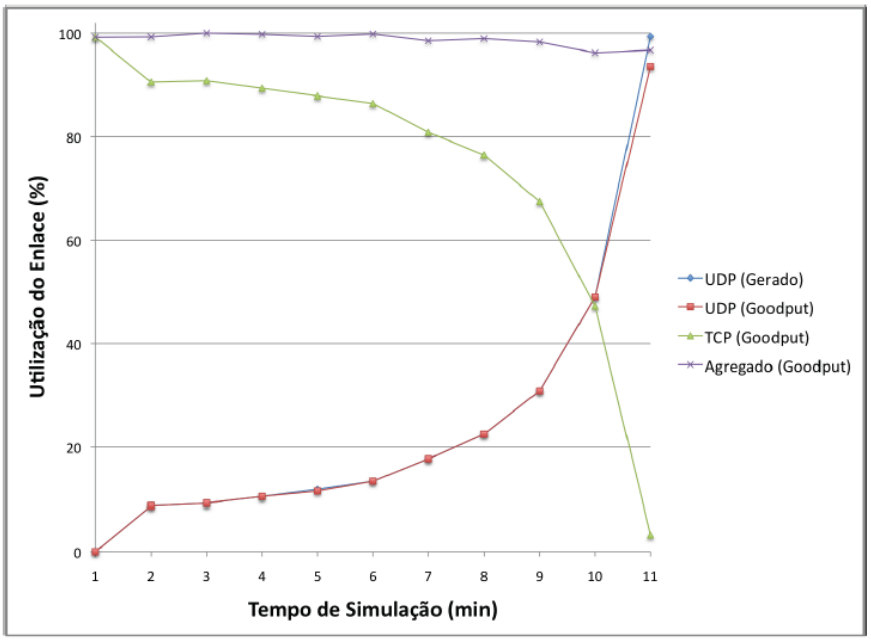


Figura II-4 - UDP x TCP: Tráfego não Cooperativo – IN [5]

Em [22] é descrito um trabalho de medições realizado em um em backbone de primeiro nível na California, EUA, que observou o tempo de vida dos fluxos IP. Os resultados foram comparados com recentes medições feitas na Universidade de Auckland, na Nova Zelândia. Os testes mostraram que ao ignorar fluxos de curta duração (6 pacotes ou menos), o sistema manteve a média de fluxos ao longo do tempo. O autor explica que este comportamento reforça a hipótese de que os picos observados são causados por ataques do tipo rajada de curta duração. De acordo com as estimativas do trabalho acredita-se que para efeito de contabilidade do trafego, cerca de 2% não correspondam a utilização dos usuários. Para a realização deste trabalho foi utilizada a ferramenta NETRAMET, com modificações para descartar os fluxos de curta duração.

Nem tudo o que pode ser contado conta, e nem tudo o que conta pode ser contado.

Albert Einstein

Capítulo III - **Estudo de caso**

Considerando como cenário a rede da Universidade Federal Fluminense apresentada no capítulo I, além de todos os aspectos relacionados ao gerenciamento e monitoramento abordados no capitulo II, descreveremos neste capítulo o estudo de caso que objetivou avaliar a tecnologia de monitoramento de fluxos IP, na rede da Universidade, evidenciada na revisão de literatura como a mais promissora.

3.1 Objetivos

A. Objetivos gerais:

   Avaliar a tecnologia de monitoramento de fluxos IP na rede da UFF.

B. Objetivos específicos:

   1- Montar uma estrutura de monitoramento de fluxos, na rede da Universidade Federal Fluminense.

   2- Coletar os dados visando obter a caracterização de tráfego da rede da UFF, de forma global e individual para cada uma das 76 redes que a compõem.

   3- Analisar os resultados obtidos.

3.2 Metodologia utilizada

Segundo o modelo proposto pela CISCO e aceito pela IETF através da RFC 3955, o “gerador" é um recurso do roteador ou switch, que quando habilitado, exporta os fluxos para um coletor. Inicialmente, habilitar nos switches da UFF o recurso de exportação de

fluxos seria a opção mais simples, entretanto, de acordo com fabricante (Dlink) os modelos existentes (DES 3226-GSR) não dispunham de tal funcionalidade.

Este fato determinou a busca por alternativas em software que possibilitassem montar uma estrutura similar ao modelo aprovado pela IETF. Os softwares selecionados encontram-se relacionados na Tabela II.

Tabela II – Alternativas em software para o monitoramento de fluxos.

FUNÇÃO	ALTERNATIVA / SOFTWARE	ATIVIDADE	Autor
Gerador	Softflowd	Escuta o trafego no ponto de observação escolhido; Gera o pacote no formato Netflow; Transmite o pacote para o coletor.	[23]
Coletor	Nfdump	Registra em perfis individuais informações sobre as redes IP a serem monitoradas. Recebe e armazena o pacote enviado pelo gerador, de acordo com o perfil das redes cadastradas. Permite a realização de consultas aos dados armazenados através de linha de comando	[24]
INTERFACE GRÁFICA	Nfsen	Gera os gráficos a partir dos fluxos armazenados pelo coletor, (Nfdump). Fornece uma interface amigável para consultas e relatórios personalizáveis Fornece uma estrutura para automatização de tarefas.	[24]

Dentre eles, o programa Softflowd, pode ser obtido no site do autor com toda a documentação necessária para a correta instalação. O Softflowd atua como o gerador de pacotes no formato Netflow. Os programas Nfdump e Nfsen fazem parte do projeto chamado Nfsen Project. Em [24] é possível ver uma apresentação das funcionalidades dessas ferramentas. O Nfdump é o coletor, enquanto que o Nfsen exibe os dados coletados através de gráficos em função do tempo e de perfis (filtros personalizáveis).

Considerando a inexistência da funcionalidade de geração de pacotes no formato Netflow / IPFIX, nos Switches da UFF, foi solicitado ao NTI a instalação do programa Softflowd em um computador conectado ao switch principal do anel de fibra ótica, por onde passa todo o tráfego da Internet, sendo este o ponto de observação escolhido.

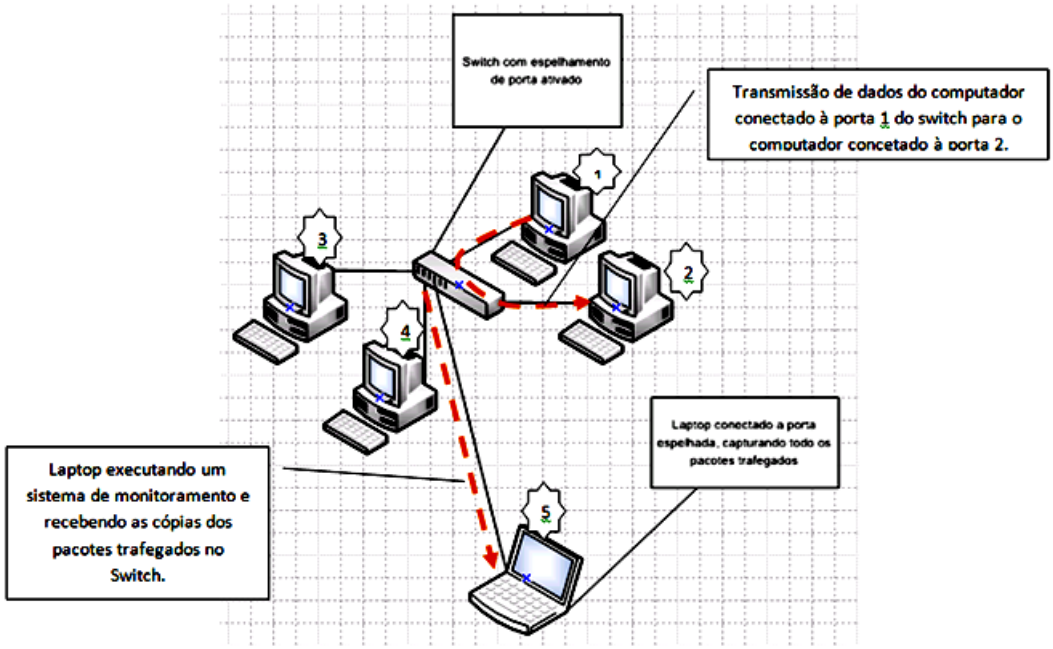


Figura III-1 Capturando pacotes da rede usando o recurso de espelhamento de porta no switch.

Para tanto, foi utilizado o recurso de espelhamento de porta na interface de conexão com o gerador. O espelhamento de porta envia uma cópia de tudo o que é trafegado em uma ou mais portas, para uma determinada porta do switch, conforme a ilustração da Figura III-1.

Isto permitiu a inspeção, pelo gerador, de todos os pacotes transmitidos no enlace de Internet e assim a geração e transmissão dos pacotes no formato Netflow para o coletor.

Esta estratégia funcionou corretamente. No entanto, devido ao fato do gerador e coletor estarem em campi diferentes, conforme mostra a Figura III-2, houve um aumento no tráfego dos switches que interconectam esses campi, devido à grande quantidade de pacotes UDP enviados do gerador para o coletor.

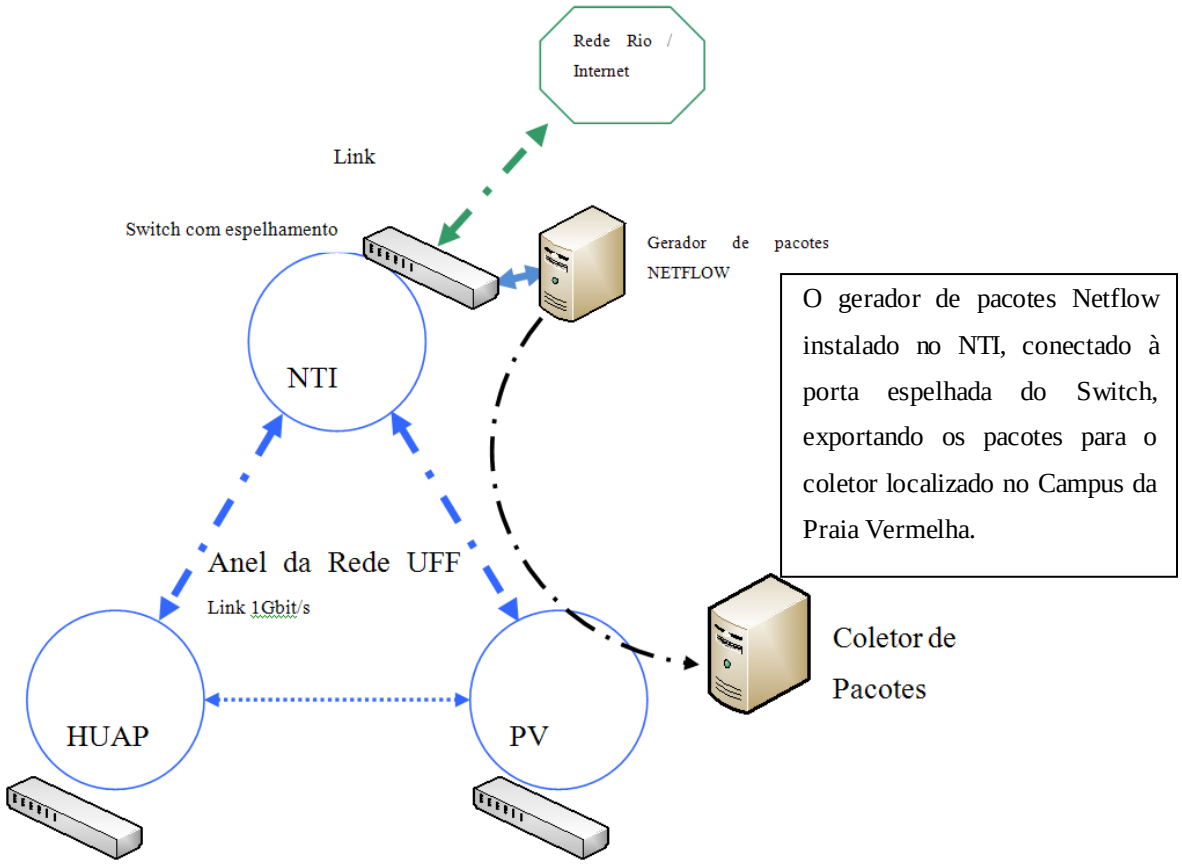


Figura III-2 - Configuração inicial do ambiente de monitoramento da Rede UFF.

Para solucionar este problema, o coletor foi transferido para o NTI. O gerador e o coletor foram instalados no mesmo computador, deste modo, uma mesma máquina ficou responsável por capturar o tráfego, gerar os pacotes e enviar para si mesma, fazendo na sequência o processamento e armazenamento dos fluxos. O cenário definitivo de monitoramento pode ser observado na Figura III-3.

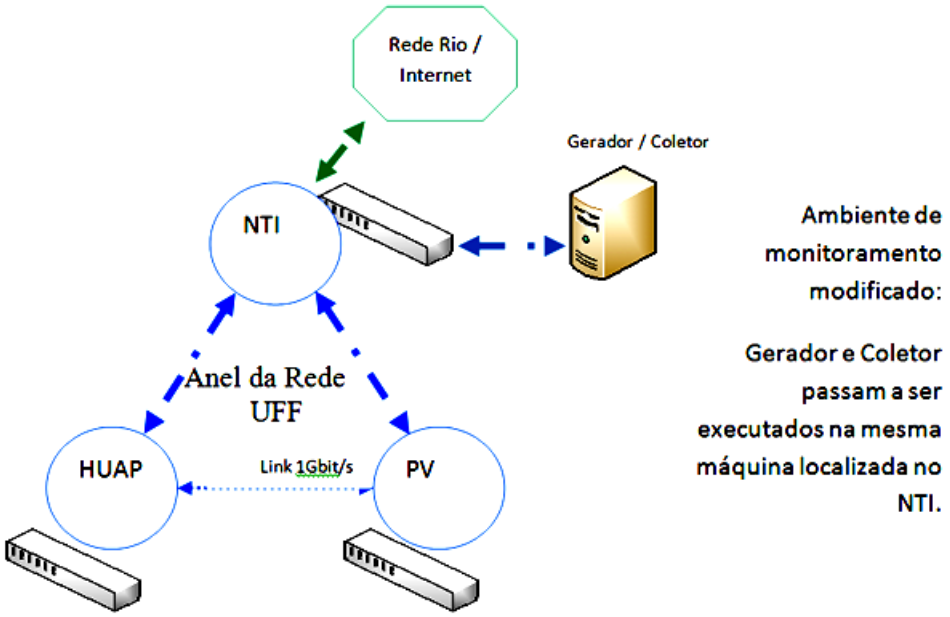


Figura III-3 - Configuração final do ambiente de monitoramento

3.3 Criando perfis para armazenamento de fluxos.

3.4 Perfil RedeUFF

Com o objetivo de monitorar individualmente cada uma das 76 redes da UFF, foi criado um perfil chamado RedeUFF onde foram adicionados filtros para cada uma das 76 redes. Desta forma, foi possível gerar gráficos em função da atividade de cada rede, individualmente. A Figura III-4 mostra um gráfico semanal onde a atividade de cada rede é representada por uma cor.

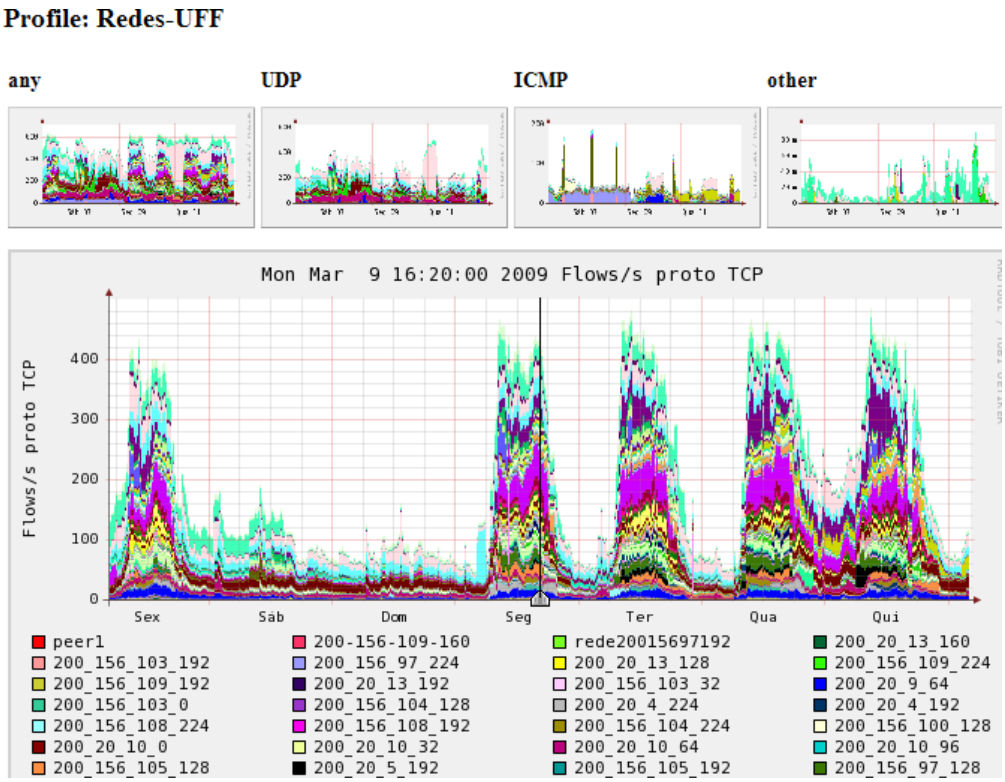


Figura III-4 - Perfil RedesUFF – Gráfico Semanal

3.5 Perfil PROTOCOLOS

Da mesma forma que foram criados filtros para o tráfego individual para cada rede da UFF, também, o mesmo procedimento foi feito para os protocolos mais comuns utilizados na Internet como:

- HTTP – Navegação WEB. Protocolo TCP na porta 80;
- HTTPS – Navegação WEB segura. Protocolo TCP na porta 443;
- SMTP – Envio de emails. Protocolo TCP na porta 25;
- POP3 – Recebimento de e-mail. TCP na porta 110;
- FTP – Transferência de arquivos – TCP nas portas 20 e 21;
- TELNET – Terminal remoto – TCP na porta 23;
- SSH – Terminal remoto seguro – RCP na porta 22;
- DNS – Resolução de nomes – UDP na porta 53;
- SNMP – Monitoramento de redes – UDP 161; e
- SQL – Consulta a banco de dados - TCP 3306.

Também neste caso foram atribuídas cores para cada um dos protocolos. A Figura III-5 apresenta um gráfico semanal.

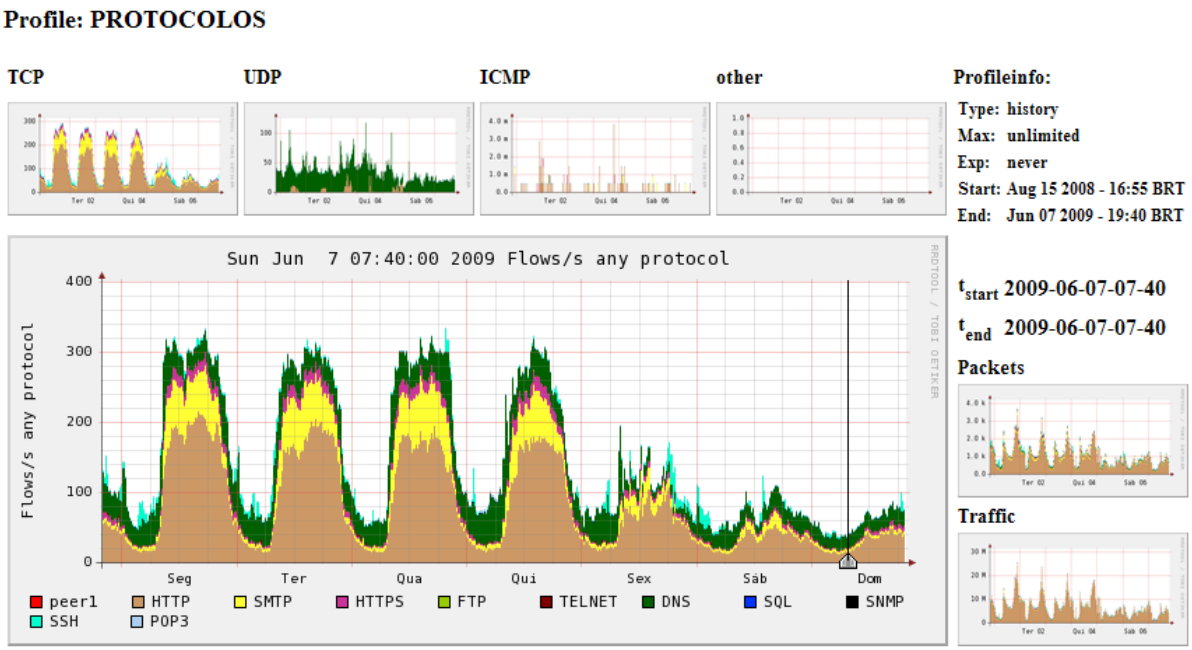


Figura III-5 - Perfil PROTOCOLOS – Gráfico semanal

3.6 Perfil Anel UFF

Um perfil de nome AnelUFF foi criado exclusivamente para monitorar a tráfego de controle entre os switches do anel: Valonguinho (NTI), HUAP e Praia Vermelha, Direito e Reitoria (Figura III-6).

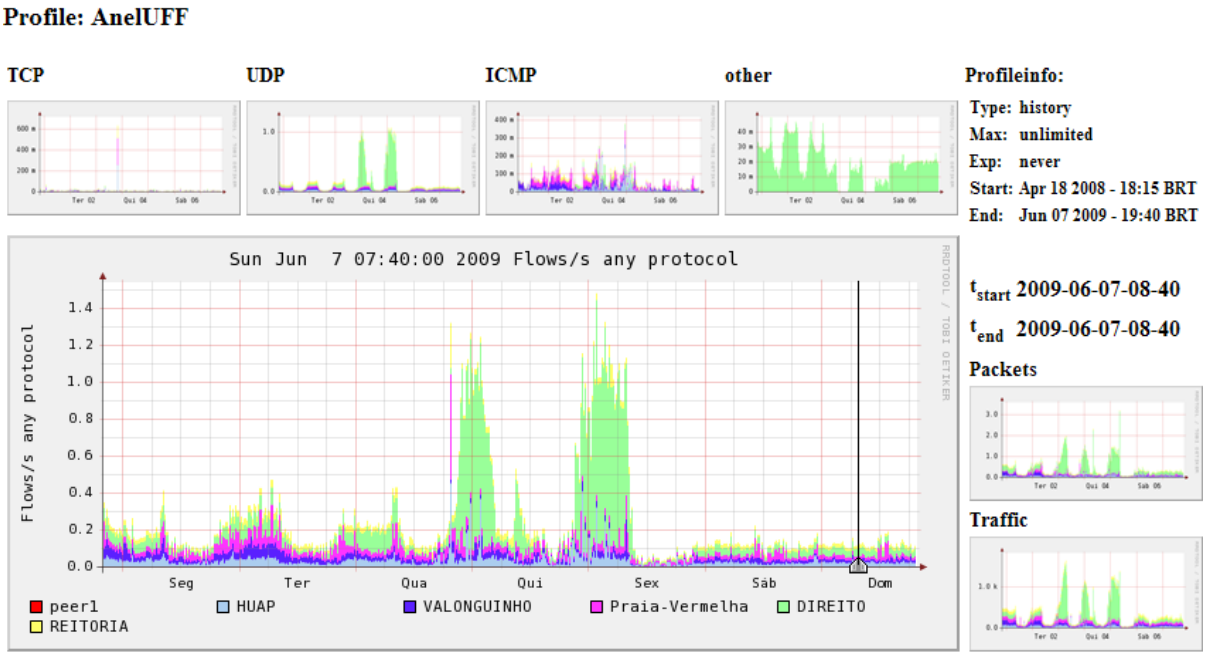


Figura III-6 - Perfil AnelUff – Gráfico Semanal

3.7 Recursos utilizados

a) Hardware

Para a realização deste estudo de caso foi utilizado um servidor, fornecido pelo Laboratório Midiacom, com as seguintes características: processador com dois núcleos de 3.2 GHz, 2GB de memória RAM, placa de rede de 1Gbit ethernet e quatro discos SATA de 160 GB. Posteriormente os discos de 160 foram substituídos por dois discos de 500GB (01 Terabyte), de forma a aumentar a capacidade de armazenamento do tráfego ao logo do tempo.

b) Software

O sistema operacional utilizado pelo servidor de monitoramento foi a distribuição Linux Fedora, versão 10. Todas as bibliotecas auxiliares foram instaladas através do software Yum, de acordo com as exigências das aplicações instaladas.

3.8 Scripts

Apesar da grande facilidade de visualização dos gráficos e consultas dos fluxos a partir de filtros por IP, PROTOCOLO, e todos os demais campos do protocolo IP, o software coletor (Nfsen) apresentou problemas para exibir os gráficos com mais de dois

meses de dados. Além disso, a versão utilizada não ofereceu facilidades para a extração dos dados filtrados, cabendo ao usuário a tarefa de copiar e colar os resultados. Estes fatos motivaram a elaboração de scripts para coleta das informações diretamente nas pastas de armazenamento. Também foi programado, através dos scripts, o tratamento dos dados de modo a facilitar a criação dos gráficos em outros programas. A relação de scripts pode ser vista no apêndice 2.

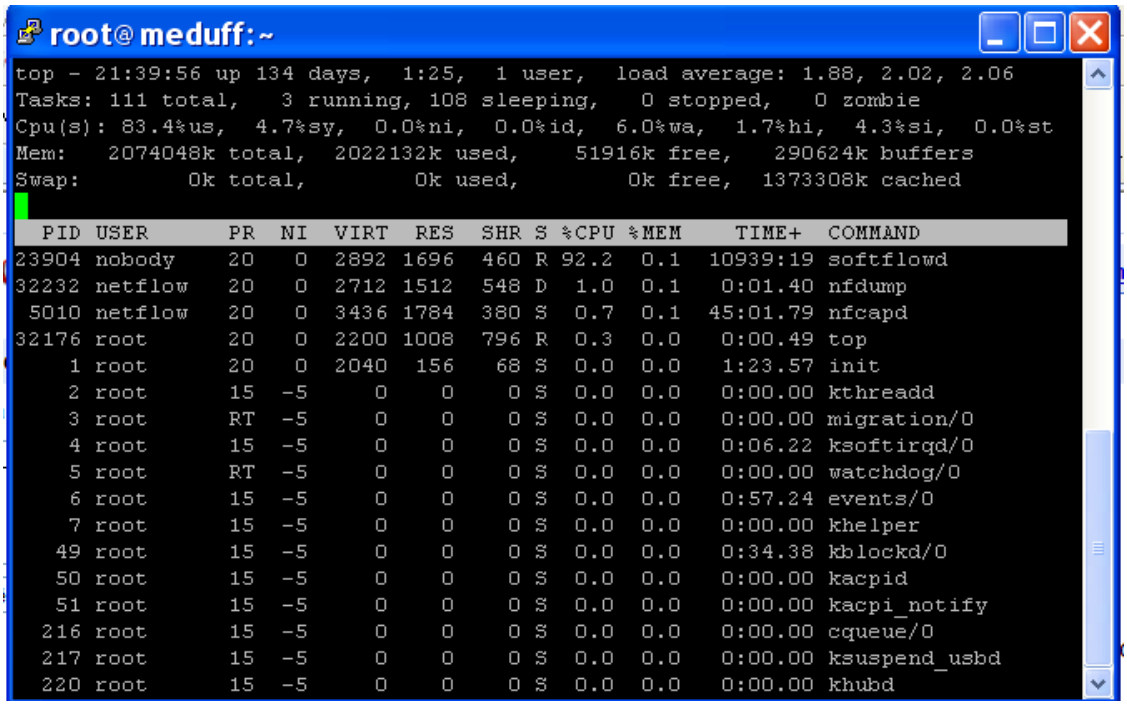


Figura III-7 - Consumo de CPU pelos softwares: Softflowd, Nfdump e Nfcapd

3.9 Ajustes dos parâmetros para captura dos fluxos

Foi possível capturar os fluxos com os softwares atuando em conjunto (Softflowd, Nfdump e Nfsen) de maneira bem estável considerando os aspectos das interfaces entre as ferramentas. Por restrição dos recursos de hardware disponíveis, a mesma máquina executou os três aplicativos, embora durante o primeiro período de coleta de dados tenha ficado evidente (por conta do percentual de uso de CPU), que o ideal seria separar cada serviço em máquinas independentes ou pelo menos o gerador, (Softflowd), que foi o que mais consumiu recursos, como mostra a Figura III-7. Os parâmetros utilizados durante os cinco meses de captura foram: softflowd –v9 –t max_life=300 -i eth0 –n 200.20.0.156. A validação destes parâmetros, quanto à fidelidade do volume de dados trafegados, foi feita através da comparação da quantidade de bits trafegados entre o

sistema Nfsen e o sistema CACTI, também instalado na mesma máquina. (vide apêndice 2 para maiores informações sobre o sistema CACTI).

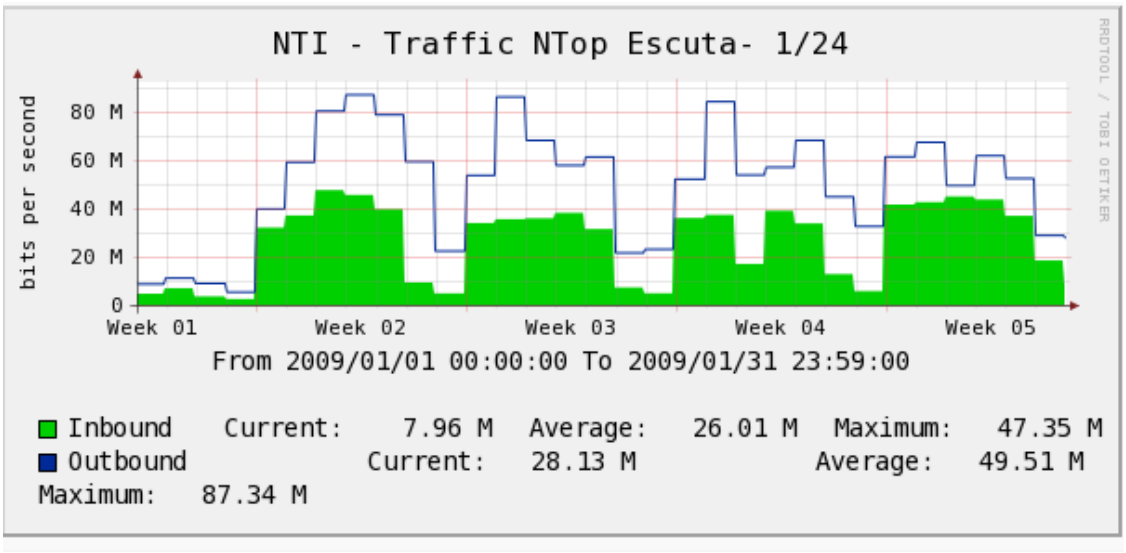


Figura III-8 - Janeiro 2009. Início do período de captura de dados – Sistema Cacti.

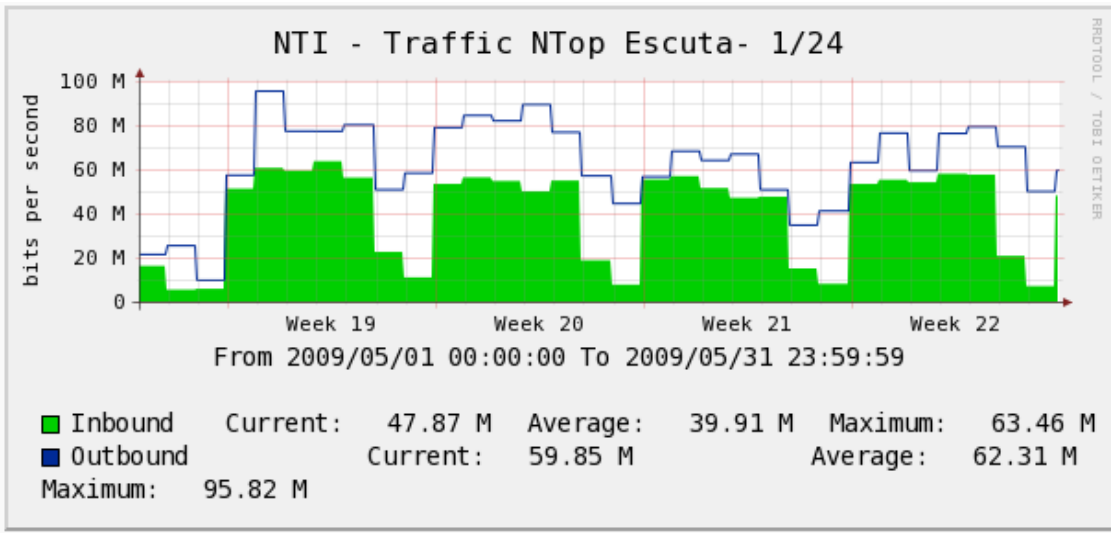


Figura III-9 - Fim do período de Captura de dados – Sistema Cacti.

O sistema Cacti obtém os dados diretamente da interface de rede do Switch, através do protocolo SNMP. Desta forma, as informações sobre a quantidade de bits correspondem exatamente aos bits trafegados, independente do tipo de protocolo. Não há processamento das informações por parte do Cacti, apenas a leitura daquilo que está gravado nos registradores instalados nos dispositivos de rede. Ao contrário, os sistemas avaliados (Softflowd – Nfsen/Nfdump) precisam escutar o tráfego passando por um

ponto de observação (uma interface de rede), capturar e analisar para identificar se já existem fluxos registrados, de modo a realizar a agregação dos dados por fluxos. Depois disso, ele precisa exportar os fluxos finalizados para o coletor, de acordo com os critérios previamente estabelecidos. Este processamento é diretamente afetado pela quantidade de dados processados. Quanto mais dados passando pela interface, mais processamento.

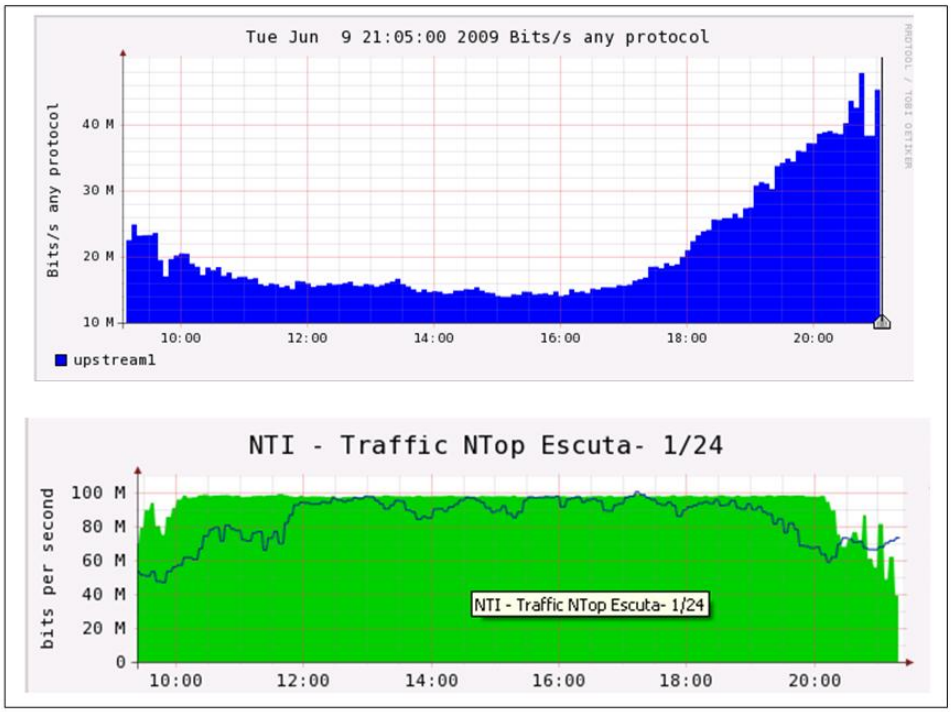


Figura III-10 - Comparação dos Registros de tráfego entre o sistema Nfsen e o sistema CACTI em Junho 2009

Após a fase de captura dos dados, durante a fase de análise dos resultados, foi observada uma grande diferença entre a quantidade de bits processados entre o sistema Nfsen e o sistema CACTI. O que havia de significativo para explicar os motivos desta diferença era o aumento do tráfego no período, uma vez que no início da captura dos dados, os sistemas apresentavam uma correspondência bem próxima entre eles. Os valores médios do tráfego de entrada e de saída passaram, respectivamente, de iniciais 26Mbit/s e 49Mbit/s obtidos em janeiro de 2009 (Figura III-8), para 39Mbit/s e 62Mbit/s registrados no mês de maio (Figura III-9). Em setembro do mesmo ano, o sistema Cacti já registrava a partir das 12h, uma saturação da conexão com a Internet que prosseguia até as 18h30minh quando o tráfego começava a reduzir (Figura III-10). Em

contrapartida o sistema Nfsen começava registrando 25Mbit/s, e seguia em queda registrando às 12h taxas em torno de 17Mbit/s. Quando o uso da rede começava a diminuir, o Nfsen começava a registrar elevação da taxa de transferência tendendo a um ponto de equilíbrio com relação ao CACTI. Diante destas observações, concluiu-se que durante o dia, devido à grande quantidade de fluxos a serem analisados pelo servidor através do sistema Softflowd, este não conseguia processar todas as informações conforme é possível observar, na Figura III-7 o registro do intenso uso da CPU pelo software Softflowd. À medida que a quantidade de fluxo era reduzida isto se tornava possível.

Parâmetros de captura do Softflowd utilizados durante entre Janeiro e Maio de 2009

Softflowd –v 9 –t maxlife=300 –i eth1 –n 200.20.0.156:9995

Parâmetros de captura do Softflowd utilizados a partir de Outubro de 2009:

Softflowd –v 9 –m 100000000 –i eth1 –n 200.20.0.156:9995

Figura III-11 - Alteração dos parâmetros no gerador (SOFTLOWD)

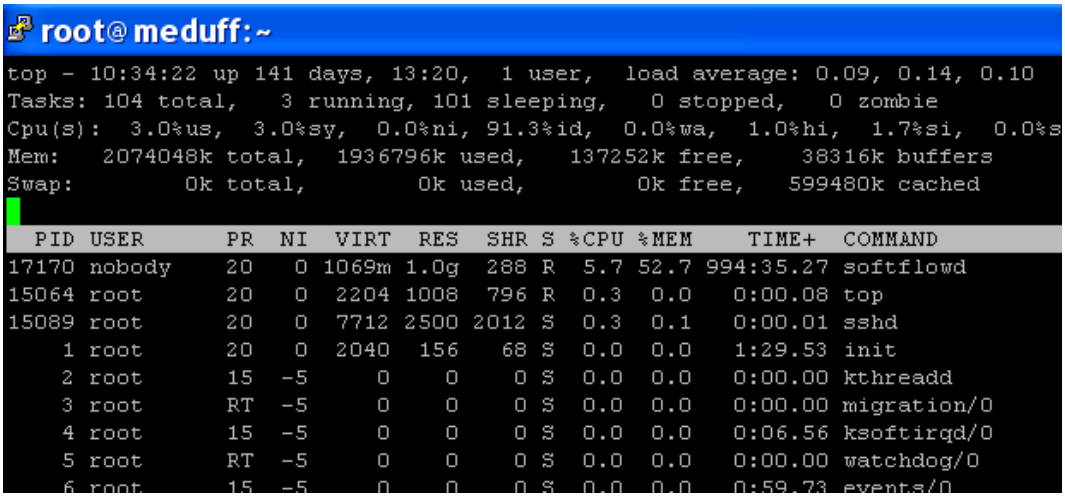


Figura III-12 - Redução do uso do processador e aumento do uso da memória após alterações nos parâmetros de execução do gerador (Softflowd)

Considerando que o período de captura dos dados já havia terminado, foram alterados os parâmetros do gerador (Softflowd), como tentativa de se obter uma melhor correspondência dos valores de tráfego mostrados entre o sistema CACTI e Nfsen.

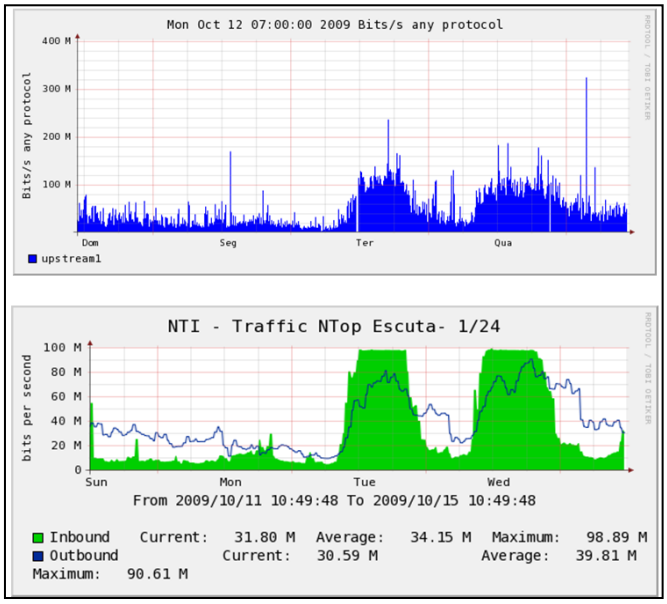
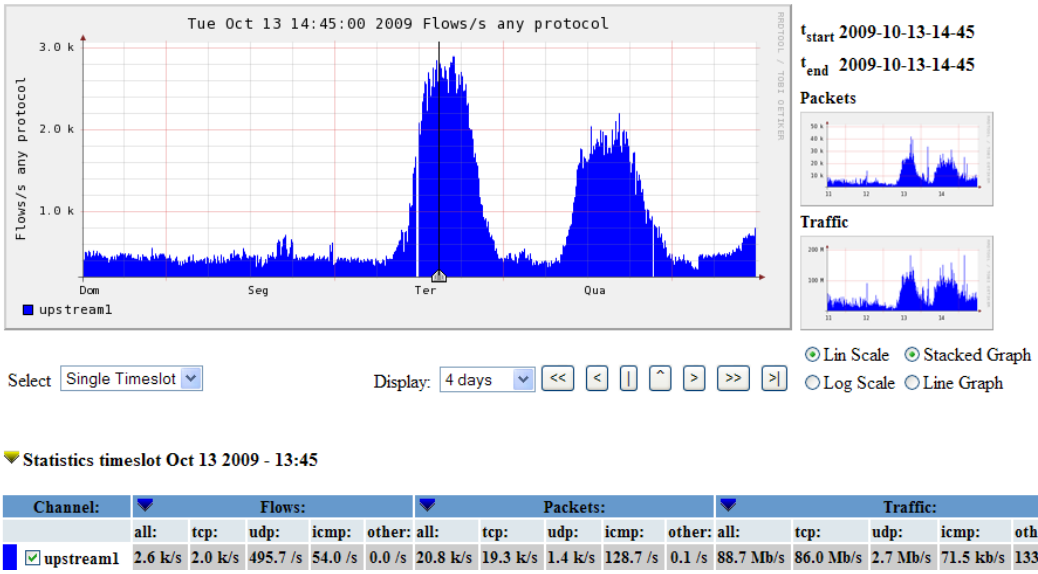


Figura III-13 - Comparação dos gráficos do Nfsen e do CACTI após alteração dos parâmetros do Softflowd.

Após vários ensaios de alterações e testes, foram obtidos melhores resultados (Figura III-13), inclusive com redução do percentual de uso do processador conforme mostra a Figura III-12. Um detalhe a ser observado na Figura III-13 é que depois das modificações o Nfsen passou a registrar taxas superiores a 100Mbit/s que é a velocidade máxima da conexão de Internet da UFF, fato este que não se reproduziu no sistema CACTI. Isto pode ser explicado se considerarmos as diferenças entre as técnicas de monitoramento utilizadas por estes sistemas. O Cacti informa o tráfego que passa pela interface de rede, cuja capacidade está limitada a 100Mbit/s, enquanto que o Softflowd escuta este mesmo tráfego, através da interface de rede do servidor de monitoramento que tem capacidade de 1Gbit/s e está conectada a uma porta do *switch*, de mesma capacidade, com recurso de espelhamento habilitada. Isto significa que ela é capaz de registrar para o sistema, taxas superiores à do enlace. Muito provável é que este tráfego excedente a capacidade do enlace, represente a demanda interna que é reprimida pelo gargalo da conexão, que apesar de não seguir para a Internet é registrado pelo Softflowd. Neste caso, para equiparar a leitura do tráfego entre os sistemas, o ideal seria transferir o coletor de dados para a extremidade de conexão da Rede Rio, onde o tráfego já haveria sido transmitido pelo enlace de 100 Mbit/s)

Durante os testes constatou-se que os parâmetros utilizados no GERADOR (durante a fase de coleta de dados vide Figura III-11), o aumento do tráfego na conexão com a Internet, ocorrido entre janeiro e maio, não permitiu o armazenamento temporário na memória do sistema de todos os fluxos ativos registrados durante a atividade da rede até que este verificasse o seu término natural. Verificamos que, por padrão, o Softflowd limita-se a manter em memória 8192 fluxos e quando este valor é ultrapassado todos os fluxos, a partir dos mais antigos, são finalizados de maneira forçada. Além disso, a utilização do parâmetro **–t maxlife=300** fixava em 300 segundos o tempo máximo de vida de um fluxo, forçando também ao término todos os fluxos que ultrapassassem este período. Este processo de finalizar e exportar os fluxos excedentes a 8192, bem como aqueles que ultrapassassem os valores estabelecidos para ***maxlife*** para o servidor, levavam a CPU a alcançar percentuais de utilização muito elevados, variando entre 90% e 99% conforme mostra a Figura III-7.



Statistics timeslot Oct 13 2009 - 13:45

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
upstream1	2.6 k/s	2.0 k/s	495.7 /s	54.0 /s	0.0 /s	20.8 k/s	19.3 k/s	1.4 k/s	128.7 /s	0.1 /s	88.7 Mb/s	86.0 Mb/s	2.7 Mb/s	71.5 kb/s	133.1 b/s

Figura III-14 - Gráfico da quantidade de fluxos após alteração dos parâmetros do Softflowd

Partindo dessas constatações, foi retirado o parâmetro –t maxlife=300 e acrescentado o parâmetro –m 100.000.000. Este parâmetro informa ao sistema que o número máximo de fluxos ativos é limitado a 100.000.000. Este valor foi atribuído no sentido de conhecer o número máximo de fluxos a serem registrados pelo sistema a partir dos novos parâmetros. Na prática verificou-se um número bem menor, com a máxima em torno de 2.600.000 fluxos durante a semana e 390.000 nos finais de semana, conforme

pode ser observado no gráfico da Figura III-14; valores bem superiores aos 8192 definidos pelo padrão do sistema.

Vários outros aspectos foram modificados em função da aplicação dos novos parâmetros. O processador, que antes era consumido basicamente para forçar o término dos fluxos, reduziu o percentual de uso da faixa dos 90% para menos de 10%. A memória que era utilizada pelo Softflowd, em média 2MBytes, saltou para 1GBytes (Figura III-12) devido à elevação da quantidade de fluxos ativos, antes limitada a 8192, ou seja, por não poder armazenar a quantidade de fluxos necessária ao volume de tráfego da rede, o sistema fazia o rodízio entre o novo fluxo observado e os fluxos mais antigos. Está atividade intensa consumia grande parte dos recursos do servidor de monitoramento. Além disso, os gráficos apresentavam uma proporção inversa à utilização da rede. Durante o dia, período de utilização máxima da rede, os gráficos de representação do tráfego mostravam taxas decrescentes e que aumentavam ao final do dia. Em contrapartida, durante à noite as taxas alcançavam os maiores patamares. Esta situação foi corrigida conforme mostra a Figura III-13, em comparação com a Figura III-10.

3.10 Obtendo os dados

Para a obtenção dos dados foram criados três perfis de captura dos fluxos: Redes UFF, Protocolos e Anel UFF, que serão detalhados a seguir:

A. Redes UFF

   Neste perfil foram configurados filtros para registrar a atividade individual de cada rede da UFF.

B. Protocolos

   Neste perfil foram configurados filtros para registrar a atividade das portas do protocolo TCP e UDP mais utilizados na Internet.

C. Anel UFF

   Neste perfil foram configurados filtros para registrar a atividade dos switches que compõem o Anel da rede da UFF.

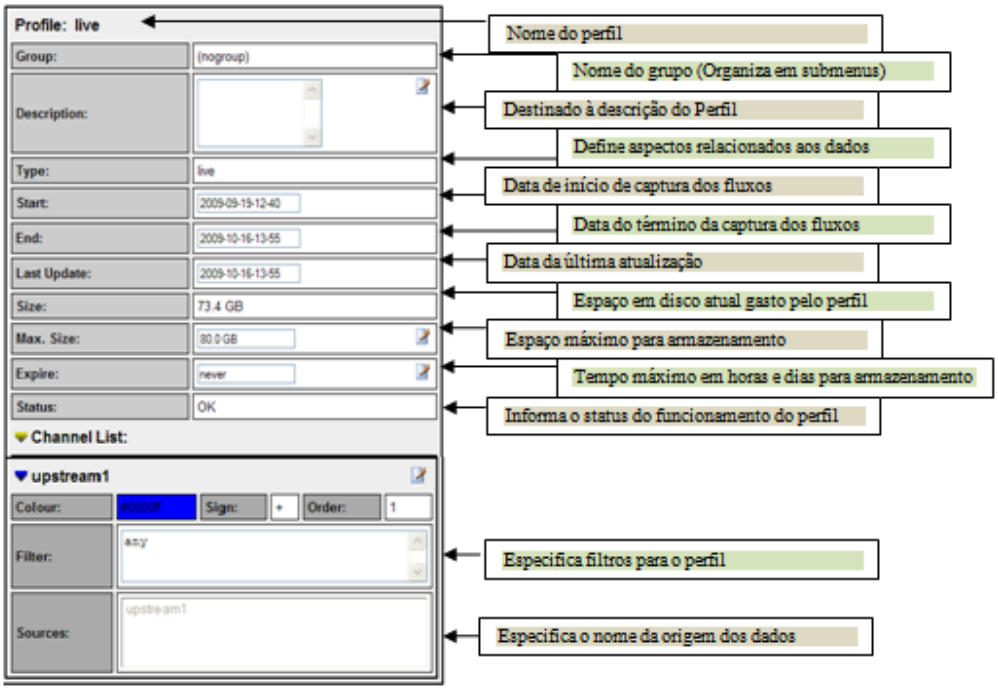


Figura III-15 Tela de criação de perfil.

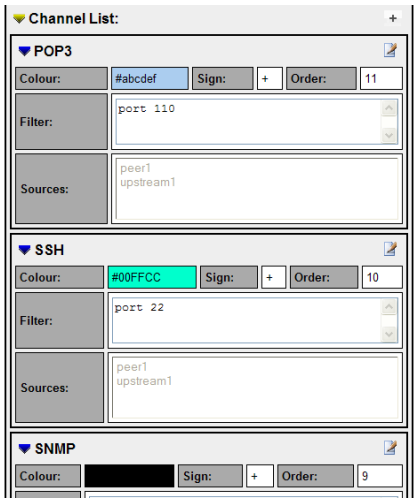


Figura III-16 - Criando os canais do perfil Protocolos para filtrar as portas desejadas

3.11 Criando perfis

Os sistemas Nfsen e Nfdump trabalham em conjunto. É possível criar um perfil utilizando o programa Nfdump através da linha de comando, entretanto esta tarefa se torna mais simples através das telas do Nfsen. A Figura III-15 mostra as informações necessárias para criar um perfil através deste sistema. O perfil mostrado na Figura III-15

é chamado *Live*. Ele já vem criado e não pode ser excluído, uma vez que, por definição, todos os demais perfis buscam seus dados a partir dele. É possível escolher entre quatro tipos de perfis, no que diz respeito ao modo de registro das informações. O programa oferece quatro opções: *Continuous profile*, *History profile*, *Continuous profile* / *Shadow* e *History profile* / *Shadow*. As características de cada um são descritas a seguir:

- *Continuous profile* - Não existe período determinado para coleta de fluxos. Os arquivos são armazenados em uma pasta com o nome do perfil.
- *History profile*– É determinado um período para coleta de fluxos. Os arquivos são armazenados em uma pasta com o nome do perfil.
- *Continuous profile / Shadow* – Não existe um período determinado para coleta de fluxos. Não há repositório de dados à parte, todas as informações dependem dos arquivos armazenados no perfil *Live*.
- *History profile / Shadow* - É determinado um período para coleta de fluxos. Não há repositório de dados a parte, todas as informações dependem dos arquivos armazenados no perfil *Live*.

Quando um perfil é configurado como *Shadow*, não existe duplicação de dados. Todos os fluxos são oriundos do perfil *Live* - É uma boa opção para economia de disco. Os perfis que não são do tipo *Shadow,* copiam do perfil live todos os registros de fluxos que correspondam aos critérios definidos durante a criação do perfil, o que replica os dados aumentando o consumo de espaço de armazenamento. Por outro lado, os perfis criados na modalidade *Continuos Profile*, facilitam o processamento de scripts uma vez que o armazenamento de arquivos é feito em pastas separadas, ou seja, cada perfil possui uma estrutura de pastas que recebe cópias oriundas do perfil *Live*, em função dos filtros definidos. Na prática isso se traduz em uma melhor administração dos arquivos armazenados com ganhos de velocidade na execução dos scripts. Por este motivo, neste Estudo de Caso foi utilizado o modo *Continuous Profile*.

3.12 Criando filtros

Após a criação do perfil, é necessário fazer a programação dos filtros ou canais, como são chamados no Nfsen. Um filtro, deixa passar para o perfil apenas os fluxos que correspondam aos critérios, definidos, sendo que, o mais comum, é definir filtros por: protocolo: (**TCP, UDP, ICMP, GRE, ESP, AH, RSVP),** versão de protocolo tcp (ipv4, ipv6),

endereço ip, origem e destino, rede, porta, interface ou a combinação destes através de expressões. A Figura III-16 mostra a tela onde são configurados os filtros para o protocolo TCP. É possível observar um filtro para a porta 110 e outro para a porta 22. A intenção neste caso foi monitorar as atividades de e-mail do tipo pop3 e de terminais seguros do tipo SSH (Secure Shell). É claro que pode haver aplicações destas categorias que operem em outras portas. No entanto, o objetivo, neste caso, foi monitorar as portas definidas pela IANA (Internet Assigned Numbers Authority) para estes serviços.

Ao final das configurações, ou seja, da criação do perfil e configuração dos filtros, o sistema está pronto para gerar os gráficos da atividade de rede, de acordo com os critérios definidos.

A imaginação é mais importante do que a ciência, porque a ciência é limitada, ao passo que a imaginação abrange o mundo inteiro.

Albert Einstein

Capítulo IV - **Avaliação e resultados**

No estudo de caso apresentado no capítulo III, foram abordados aspectos de uso e validação da tecnologia de monitoramento de fluxos dentro do cenário da rede da Universidade Federal Fluminense. Serão apresentados neste capítulo os resultados obtidos e a análise dos dados coletados, além dos aspectos operacionais inerentes aos processos utilizados para a captura dos fluxos, através da implementação do esquema de monitoramento. Foi possível obter, com riqueza de detalhes, as características individuais do funcionamento de cada rede e que neste trabalho chamamos de PFR, conforme já descrito no Capítulo II. Ao final, apresentaremos uma seleção de incidentes, onde discutiremos vários aspectos relacionados à segurança, a partir da análise dos dados coletados ao longo do trabalho.

4.1 Análises dos resultados por perfil.

4.2 Perfil RedesUFF

Este perfil objetivou registrar individualmente a atividade de cada rede da UFF. Foram criados 76 filtros, um para cada rede. A Figura IV-1 foi retirada do sistema já em operação e se refere ao gráfico da atividade da rede, correspondente a uma semana de monitoramento, onde cada cor representa a atividade de uma rede.

Os arquivos gerados pelo sistema contêm cinco minutos do tráfego de cada rede e são identificados por ano, dia, mês, hora e minutos. Todos os arquivos foram armazenados na pasta e subpastas do perfil RedesUFF. Cada pasta recebeu como nome o endereço de uma rede da UFF. Cinco meses de dados foram coletados inicialmente e mais um mês adicional visando conhecer os impactos das modificações efetuadas nos parâmetros de configuração do gerador de pacotes, (programa Softflowd). Para o processamento dos

dados coletados, foram utilizados scripts do Linux (*shell script*), em conjunto com as ferramentas AWK e o próprio Nfdump. A relação de scripts encontra-se no apêndice 3.

Os gráficos gerados pelo sistema permitem acompanhar o funcionamento de cada rede. Quanto mais fluxos, pacotes e tráfego são gerados, maior é a área colorida ocupada, pela cor que representa a rede no respectivo gráfico. Existe uma defasagem de 5 minutos com relação ao que está sendo observado na interface do Nfsen. Isto ocorre devido ao funcionamento do sistema que a cada cinco minutos lê os arquivos gravados pelo sistema Nfdump. A possibilidade de recuar e avançar no histórico da atividade constitui uma forma eficiente de pesquisa, sendo possível escolher entre visualizar as últimas doze horas, a última semana, as últimas duas semanas, o último mês ou ano. Isto possibilita a comparação do comportamento da rede em diferentes períodos e também a comparação entre redes.

Como representado na Figura IV-1, os gráficos espelham a atividade das redes. Quem olhar para um gráfico do perfil RedesUFF pela primeira vez pode achar confuso. Entretanto, ao interpretá-lo e com a ajuda dos arquivos associados é possível obter informações que mostram quais foram os elementos responsáveis pela atividade de rede registrada no gráfico. Cada cor representa a atividade dos hosts pertencentes a uma rede. Se nenhum host da rede for ligado, nada será mostrado; por outro lado, se um único host gerar atividade isto será representado pela área colorida. As cores são dispostas uma sobre as outras e a intensidade do tráfego gerado pela rede faz com que o tamanho da cor aumente verticalmente e horizontalmente de acordo com a duração. Por padrão, o ponteiro de seleção (Figura IV-1) sempre faz a leitura de cinco minutos em relação à sua posição. Porém, veremos mais adiante, que também é possível selecionar períodos maiores.

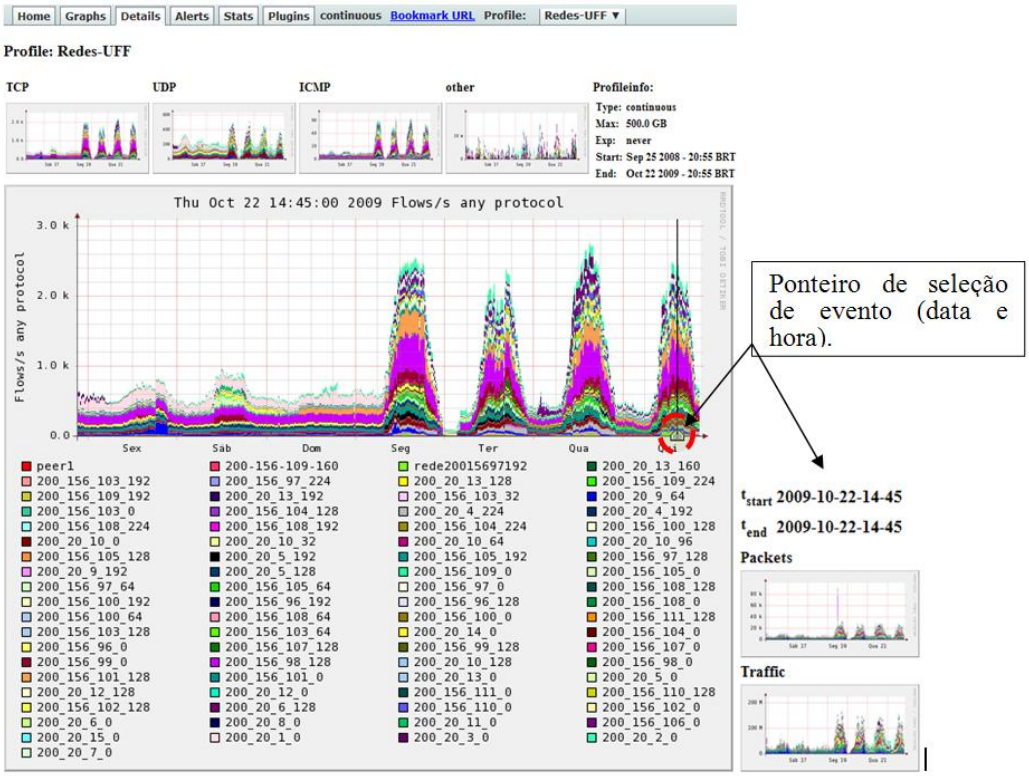


Figura IV-1 Tela do Nfsen - Perfil Redes UFF - Ponteiro de Seleção de evento

Statistics timeslot Oct 22 2009 - 14:45

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
200_20_7_0	23.6 /s	21.7 /s	1.1 /s	0.9 /s	0 /s	1.4 k/s	1.4 k/s	1.4 /s	0.9 /s	0 /s	5.2 Mb/s	5.2 Mb/s	1.5 kb/s	472.9 b/s	0 b/s
200_20_2_0	150.4 /s	123.3 /s	25.2 /s	1.9 /s	0 /s	786.1 /s	745.3 /s	37.4 /s	3.5 /s	0 /s	2.7 Mb/s	2.6 Mb/s	55.6 kb/s	1.8 kb/s	0 b/s
200_20_3_0	59.9 /s	45.7 /s	12.6 /s	1.6 /s	0.0 /s	1.7 k/s	1.6 k/s	20.8 /s	2.1 /s	0.3 /s	10.1 Mb/s	10.1 Mb/s	19.7 kb/s	1.2 kb/s	853.9 b/s
200_20_1_0	68.4 /s	28.0 /s	39.0 /s	1.4 /s	0 /s	3.3 k/s	3.2 k/s	121.4 /s	1.7 /s	0 /s	17.3 Mb/s	17.2 Mb/s	106.7 kb/s	1.5 kb/s	0 b/s
200_20_15_0	20.7 /s	17.1 /s	3.2 /s	0.4 /s	0 /s	419.9 /s	403.6 /s	15.5 /s	0.8 /s	0 /s	2.3 Mb/s	2.3 Mb/s	13.7 kb/s	545.6 b/s	0 b/s
200_156_106_0	96.0 /s	75.2 /s	18.3 /s	2.4 /s	0 /s	302.1 /s	279.1 /s	18.5 /s	4.6 /s	0 /s	603.9 kb/s	586.7 kb/s	14.9 kb/s	2.3 kb/s	0 b/s
200_20_11_0	31.3 /s	28.5 /s	1.3 /s	1.4 /s	0 /s	104.8 /s	98.9 /s	2.7 /s	3.3 /s	0 /s	187.9 kb/s	184.0 kb/s	2.4 kb/s	1.5 kb/s	0 b/s
200_20_8_0	1.1 /s	0.7 /s	0.3 /s	0.2 /s	0 /s	8.6 /s	7.4 /s	0.8 /s	0.4 /s	0 /s	31.7 kb/s	31.1 kb/s	446.0 b/s	206.9 b/s	0 b/s
200_20_6_0	47.6 /s	31.3 /s	15.0 /s	1.3 /s	0 /s	627.7 /s	506.0 /s	119.9 /s	1.7 /s	0 /s	2.8 Mb/s	2.6 Mb/s	223.6 kb/s	1.0 kb/s	0 b/s
200_156_102_0	9.3 /s	5.1 /s	4.2 /s	0.0 /s	0 /s	1.1 k/s	1.1 k/s	5.4 /s	0.2 /s	0 /s	7.7 Mb/s	7.7 Mb/s	5.6 kb/s	111.5 b/s	0 b/s
200_156_110_0	70.6 /s	69.2 /s	0.1 /s	1.3 /s	0 /s	151.6 /s	149.1 /s	0.2 /s	2.3 /s	0 /s	114.0 kb/s	112.7 kb/s	182.3 b/s	1.1 kb/s	0 b/s
200_20_6_128	7.9 /s	6.6 /s	1.1 /s	0.2 /s	0 /s	120.2 /s	118.6 /s	1.3 /s	0.2 /s	0 /s	586.1 kb/s	584.2 kb/s	1.8 kb/s	106.1 b/s	0 b/s
200_156_102_128	3.6 /s	1.7 /s	1.7 /s	0.2 /s	0 /s	54.3 /s	51.6 /s	2.5 /s	0.2 /s	0 /s	289.9 kb/s	287.3 kb/s	2.5 kb/s	142.9 b/s	0 b/s
200_156_110_128	43.6 /s	29.4 /s	12.8 /s	1.5 /s	0 /s	761.0 /s	723.7 /s	35.5 /s	1.7 /s	0 /s	4.6 Mb/s	4.4 Mb/s	122.9 kb/s	1.0 kb/s	0 b/s
200_156_111_0	0.2 /s	0.1 /s	0.0 /s	0.0 /s	0 /s	0.4 /s	0.3 /s	0.1 /s	0.0 /s	0 /s	176.5 b/s	138.2 b/s	32.3 b/s	6.0 b/s	0 b/s
200_20_12_0	11.0 /s	5.5 /s	4.8 /s	0.7 /s	0 /s	198.5 /s	191.4 /s	6.3 /s	0.7 /s	0 /s	1.3 Mb/s	1.3 Mb/s	7.4 kb/s	403.5 b/s	0 b/s
200_20_12_128	36.7 /s	31.7 /s	4.2 /s	0.8 /s	0 /s	256.9 /s	147.9 /s	107.7 /s	1.3 /s	0 /s	633.4 kb/s	312.9 kb/s	319.8 kb/s	759.7 b/s	0 b/s
200_20_5_0	82.9 /s	78.9 /s	1.9 /s	2.1 /s	0 /s	267.0 /s	260.7 /s	3.0 /s	3.3 /s	0 /s	656.7 kb/s	652.1 kb/s	3.0 kb/s	1.6 kb/s	0 b/s
200_20_13_0	22.9 /s	2.2 /s	19.9 /s	0.9 /s	0 /s	83.9 /s	60.1 /s	22.6 /s	1.1 /s	0 /s	234.4 kb/s	201.0 kb/s	31.6 kb/s	1.8 kb/s	0 b/s
200_156_101_0	58.4 /s	57.6 /s	0.0 /s	0.7 /s	0 /s	135.7 /s	134.5 /s	0.0 /s	1.2 /s	0 /s	117.7 kb/s	117.1 kb/s	7.3 b/s	570.2 b/s	0 b/s
200_156_101_128	230.2 /s	225.6 /s	2.3 /s	2.4 /s	0 /s	663.3 /s	655.3 /s	2.9 /s	5.1 /s	0 /s	971.4 kb/s	966.1 kb/s	2.8 kb/s	2.5 kb/s	0 b/s
200_156_98_0	19.1 /s	18.7 /s	0.3 /s	0.2 /s	0 /s	63.5 /s	62.9 /s	0.4 /s	0.3 /s	0 /s	150.6 kb/s	149.9 kb/s	605.9 b/s	127.7 b/s	0 b/s
200_20_10_128	6.4 /s	4.3 /s	2.0 /s	0.1 /s	0 /s	76.0 /s	73.6 /s	2.3 /s	0.1 /s	0 /s	349.3 kb/s	347.4 kb/s	1.9 kb/s	43.5 b/s	0 b/s
200_156_98_128	484.0 /s	475.9 /s	2.7 /s	5.5 /s	0 /s	2.6 k/s	2.6 k/s	42.7 /s	8.0 /s	0 /s	13.7 Mb/s	13.6 Mb/s	60.1 kb/s	3.9 kb/s	0 b/s
200_156_99_0	182.5 /s	171.0 /s	9.6 /s	2.0 /s	0 /s	1.1 k/s	1.1 k/s	34.0 /s	2.6 /s	0 /s	3.3 Mb/s	3.2 Mb/s	41.4 kb/s	1.4 kb/s	0 b/s
200_156_107_0	13.8 /s	10.7 /s	1.2 /s	1.8 /s	0 /s	175.5 /s	171.7 /s	1.9 /s	1.9 /s	0 /s	788.7 kb/s	786.3 kb/s	1.4 kb/s	1.0 kb/s	0 b/s
200_156_99_128	46.4 /s	41.3 /s	4.5 /s	0.6 /s	0 /s	136.4 /s	127.3 /s	8.2 /s	0.8 /s	0 /s	191.9 kb/s	184.5 kb/s	7.0 kb/s	435.5 b/s	0 b/s
200_156_107_128	14.6 /s	8.9 /s	3.8 /s	1.9 /s	0 /s	114.4 /s	108.5 /s	3.8 /s	2.0 /s	0 /s	397.6 kb/s	391.9 kb/s	4.3 kb/s	1.4 kb/s	0 b/s
200_156_96_0	12.3 /s	10.3 /s	1.9 /s	0.0 /s	0 /s	271.3 /s	269.0 /s	2.2 /s	0.1 /s	0 /s	1.6 Mb/s	1.6 Mb/s	2.4 kb/s	28.7 b/s	0 b/s
200_156_104_0	22.5 /s	13.7 /s	8.8 /s	0.1 /s	0 /s	199.0 /s	182.8 /s	16.0 /s	0.1 /s	0 /s	423.2 kb/s	408.4 kb/s	14.8 kb/s	77.4 b/s	0 b/s
200_20_14_0	1.2 /s	1.2 /s	0.0 /s	0 /s	0 /s	13.0 /s	12.9 /s	0.0 /s	0 /s	0 /s	55.9 kb/s	55.9 kb/s	19.6 b/s	0 b/s	0 b/s
200_156_103_64	2.0 /s	2.0 /s	0.0 /s	0.0 /s	0 /s	21.6 /s	21.6 /s	0.0 /s	0.0 /s	0 /s	86.4 kb/s	86.4 kb/s	2.2 b/s	20.9 b/s	0 b/s
200_156_103_128	12.2 /s	2.9 /s	9.2 /s	0.1 /s	0 /s	414.9 /s	401.6 /s	13.2 /s	0.1 /s	0 /s	2.5 Mb/s	2.5 Mb/s	11.1 kb/s	68.7 b/s	0 b/s
200_156_111_128	0.0 /s	0.0 /s	0 /s	0.0 /s	0 /s	0.1 /s	0.0 /s	0 /s	0.1 /s	0 /s	94.7 b/s	5.1 b/s	0 b/s	89.6 b/s	0 b/s
200_156_100_0	2.2 /s	2.2 /s	0.0 /s	0.0 /s	0 /s	25.0 /s	25.0 /s	0.1 /s	0.0 /s	0 /s	112.3 kb/s	112.2 kb/s	44.0 b/s	3.0 b/s	0 b/s
200_156_108_64	2.0 /s	1.0 /s	0.1 /s	0.9 /s	0 /s	10.4 /s	9.3 /s	0.2 /s	1.0 /s	0 /s	30.6 kb/s	30.0 kb/s	134.5 b/s	490.0 b/s	0 b/s
200_156_100_64	3.4 /s	0.5 /s	2.7 /s	0.1 /s	0 /s	11.2 /s	8.2 /s	2.9 /s	0.2 /s	0 /s	40.3 kb/s	36.3 kb/s	3.8 kb/s	136.2 b/s	0 b/s
200_156_108_0	0.6 /s	0.5 /s	0.1 /s	0.0 /s	0 /s	7.5 /s	6.7 /s	0.7 /s	0.1 /s	0 /s	35.6 kb/s	34.0 kb/s	1.5 kb/s	30.9 b/s	0 b/s
200_156_96_128	0.3 /s	0.2 /s	0.1 /s	0.0 /s	0 /s	0.4 /s	0.2 /s	0.1 /s	0.0 /s	0 /s	189.5 b/s	72.7 b/s	106.3 b/s	10.5 b/s	0 b/s
200_156_96_192	6.6 /s	6.5 /s	0.0 /s	0.0 /s	0 /s	65.2 /s	65.0 /s	0.1 /s	0.0 /s	0 /s	223.8 kb/s	223.7 kb/s	71.8 b/s	5.3 b/s	0 b/s
200_156_100_192	0.5 /s	0.4 /s	0.0 /s	0.0 /s	0 /s	12.3 /s	12.3 /s	0.1 /s	0.0 /s	0 /s	69.4 kb/s	69.3 kb/s	35.2 b/s	3.4 b/s	0 b/s
200_156_108_128	0.1 /s	0.0 /s	0.0 /s	0.1 /s	0 /s	0.1 /s	0.0 /s	0.0 /s	0.1 /s	0 /s	72.8 b/s	14.9 b/s	2.8 b/s	55.0 b/s	0 b/s
200_156_97_0	4.8 /s	4.8 /s	0.0 /s	0.0 /s	0 /s	117.6 /s	117.5 /s	0.0 /s	0.0 /s	0 /s	635.5 kb/s	635.5 kb/s	9.2 b/s	3.0 b/s	0 b/s

Figura IV-2 Painel de visualização de fluxos, pacotes e tráfego, disponível no sistema Nfsen.

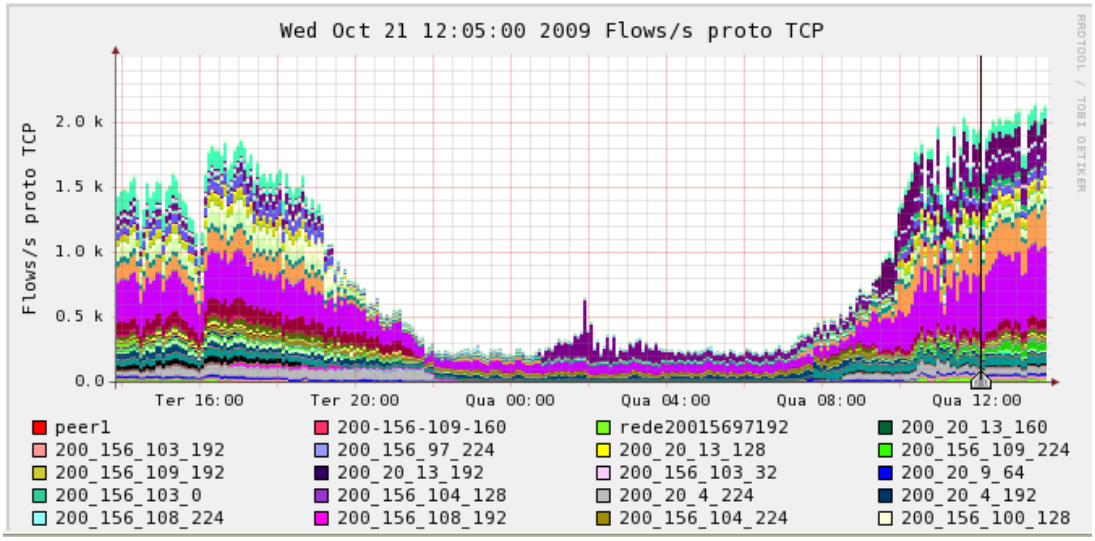


Figura IV-1 - Exemplo de gráfico mostrando apenas das redes que utilizaram o protocolo TCP.

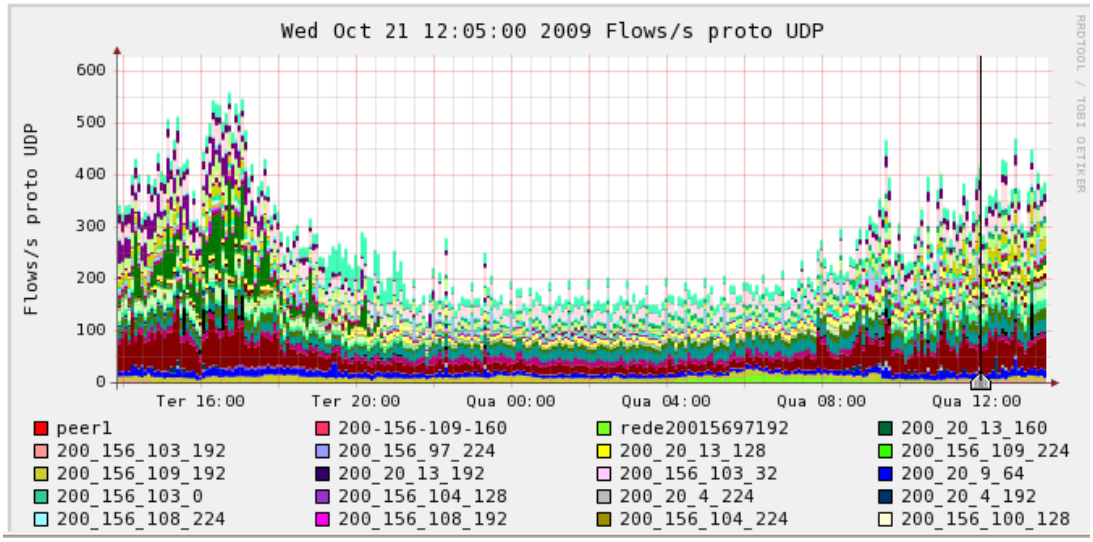


Figura IV-2 Exemplo de gráfico mostrado apenas das redes que utilizaram o protocolo UDP.

Dada a grande quantidade de redes representadas em um único gráfico, a estratégia utilizada para garantir a identificação da atividade de uma rede dentre as demais foi intercalar cores contrastantes, conforme mostra a Figura IV-1. Desta forma, apesar de existirem redes representadas pela mesma cor, pelo fato de estarem posicionadas espacialmente entre cores diferentes, é possível identificar a atividade de uma ou de outra, pois a posição de uma cor em relação às demais é mantida. Esta posição é definida no momento de cadastramento da rede no perfil, ou seja, as primeiras redes cadastradas ficarão na parte superior do gráfico e as demais serão acrescentadas

seqüencialmente, ficando as últimas redes inseridas na parte inferior do gráfico, sem que a ordem seja alterada.

Também na Figura IV-1 é possível constatar a presença regular das cores lilás e laranja, sendo que a primeira aparece durante o dia e a noite, enquanto a segunda, predominante durante o dia. Uma provável explicação para esta observação encontra-se na constituição das redes da UFF. Muitas delas pertencem à administração, secretarias ou laboratórios de alunos cujos computadores são desligados à noite e nos finais de semana. Por outro lado, existem redes que possuem seus próprios servidores, como por exemplo, de páginas web e de e-mail, que estão sempre em atividade.

O perfil RedesUff é apresentado pelo sistema Nfsen conforme mostra a Figura IV-1. Nesta tela do sistema, ao clicar sobre as miniaturas dos gráficos é possível colocá-las em evidência. Existe um ponteiro de seleção de evento (circulo vermelho) que indica para o sistema a data e a hora a serem utilizadas como referência para extrair a listagem dos hosts que geravam fluxos naquele momento, bem como para a composição do painel de visualização (Figura IV-2). Para identificar a rede que gerou um incidente no gráfico, é preciso executar as seguintes etapas:

1. Escolher o gráfico que contém o evento.
2. Selecionar o evento através do ponteiro de seleção.
3. Identificar no painel de visualização, a cor que possua o maior valor de fluxo, pacote ou tráfego, conforme o tipo do gráfico escolhido, ou seja, se for um gráfico de fluxos, deve-se procurar no painel o maior valor de fluxos, da mesma forma para pacotes ou tráfego.

O processo de identificação por associação pode ser observado nas Figura IV-3 a IV-10. Neste ponto é conhecida a rede que gerou o incidente, porém ainda é preciso saber quais foram os endereços IPs que atuaram de forma significativa causando a alteraração do gráfico. Para isso utiliza-se a consulta aos arquivos do perfil (Figura IV-9 e Figura IV-10). O resultado da consulta pode ser observado na Figura IV-8. Neste caso, os IPs, cujas redes foram evidenciadas através do gráfico, devem estar entre as primeiras posições no relatório. Este processo é recomendado apenas para identificar as redes e os endereços IPs, a partir dos incidentes selecionados nos gráficos. Para obter os gráficos

para cada rede, o sistema permite selecionar de forma independente as redes desejadas, como mostra a Figura IV-6.

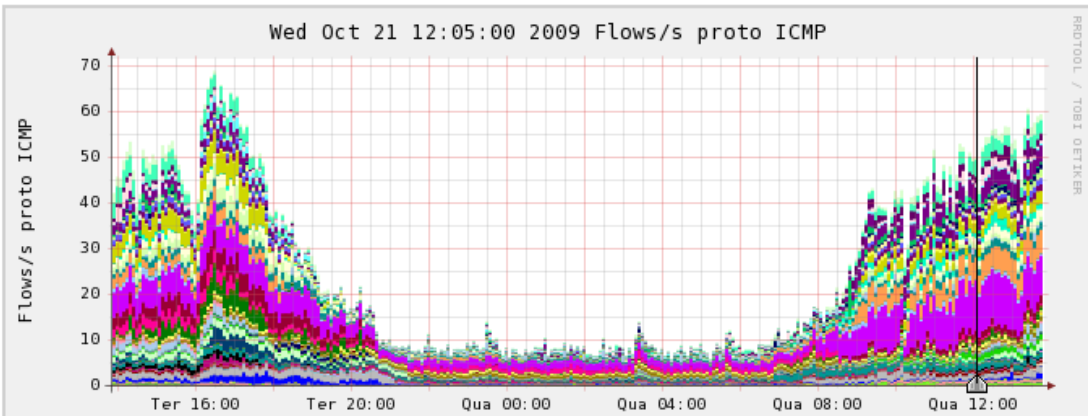


Figura IV-3 Exemplo de gráfico mostrando apenas as redes que utilizaram o protocolo ICMP.

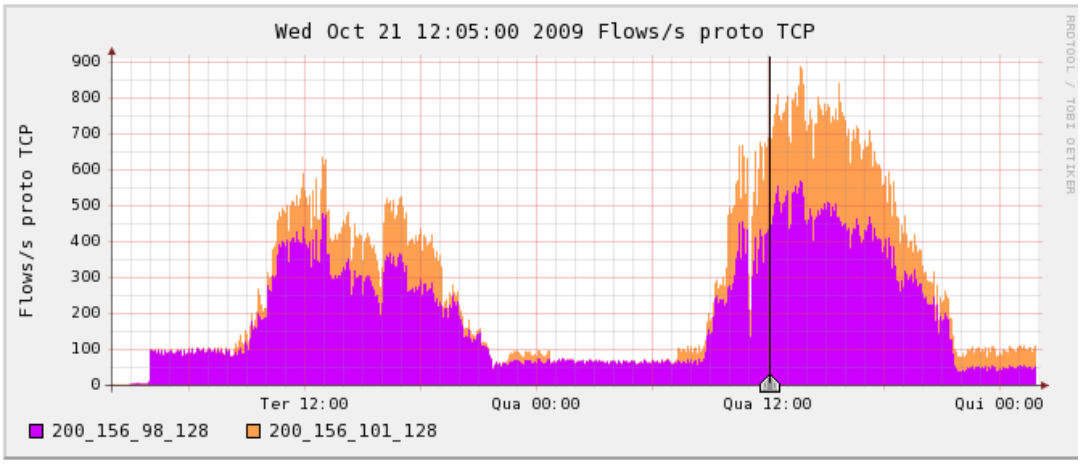


Figura IV-4 - Gráfico filtrado, mostrando atividade de somente duas redes. Protocolo TCP.

☐ 200_20_13_0	5.6 /s	2.4 /s	3.1 /s	0.1 /s	0 /s	74.6 /s	69.0 /s	5.3 /s	0.2 /s	0 /s	389.6 kb/s	385.1 kb/s	4.3 kb/s	273.9 b/s	0 b/s
☐ 200_156_101_0	43.0 /s	41.2 /s	0.0 /s	1.7 /s	0 /s	127.9 /s	125.3 /s	0.0 /s	2.6 /s	0 /s	237.6 kb/s	236.3 kb/s	2.5 b/s	1.3 kb/s	0 b/s
☑ 200_156_101_128	257.3 /s	252.2 /s	0.2 /s	4.9 /s	0 /s	634.2 /s	622.1 /s	0.4 /s	11.8 /s	0 /s	779.5 kb/s	773.5 kb/s	328.3 b/s	5.6 kb/s	0 b/s
☐ 200_156_98_0	5.0 /s	4.9 /s	0.0 /s	0.1 /s	0 /s	57.2 /s	56.9 /s	0.2 /s	0.1 /s	0 /s	291.4 kb/s	291.2 kb/s	102.4 b/s	41.4 b/s	0 b/s
☐ 200_20_10_128	2.9 /s	2.7 /s	0.0 /s	0.2 /s	0 /s	192.8 /s	192.5 /s	0.0 /s	0.2 /s	0 /s	1.4 Mb/s	1.4 Mb/s	22.2 b/s	113.5 b/s	0 b/s
☑ 200_156_98_128	448.9 /s	434.9 /s	3.0 /s	11.0 /s	0 /s	983.8 /s	961.1 /s	3.7 /s	19.0 /s	0 /s	750.6 kb/s	735.4 kb/s	6.0 kb/s	9.3 kb/s	0 b/s
☐ 200_156_99_0	59.3 /s	55.4 /s	2.4 /s	1.5 /s	0 /s	1.0 k/s	1.0 k/s	2.8 /s	2.5 /s	0 /s	6.1 Mb/s	6.1 Mb/s	2.0 kb/s	1.3 kb/s	0 b/s
☐ 200_156_107_0	12.0 /s	11.1 /s	0.7 /s	0.2 /s	0 /s	70.0 /s	68.4 /s	1.0 /s	0.6 /s	0 /s	216.0 kb/s	214.9 kb/s	811.7 b/s	291.8 b/s	0 b/s

Figura IV-5 - Painel de visualização de fluxos pacotes e tráfego. - Resultados obtidos a partir da seleção do intervalo de tempo (5 minutos) no gráfico da Figura IV-4.

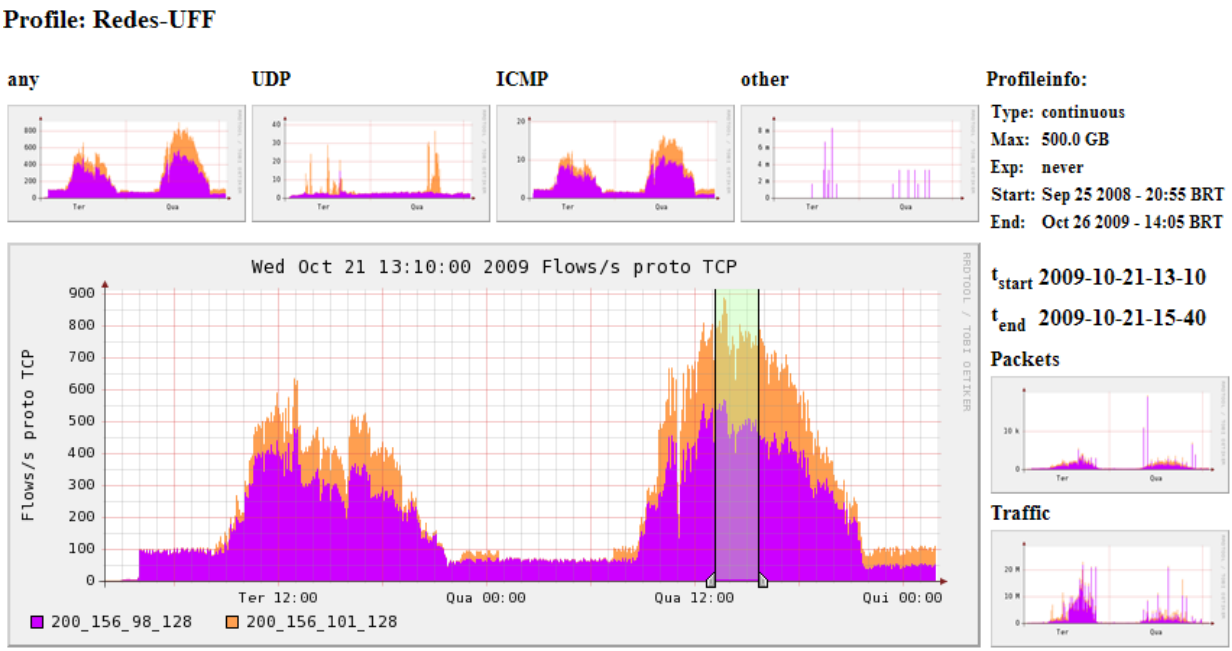


Figura IV-6 - Seleção de intervalo de tempo. Entre 7h e 22h do dia 21/10.

```
** nfdump -M /usr/local/nfsen/nfsen/profiles-data/Redes-UFF/200_156_101_128:200_156_98_128  -T  -R 2009/10/21/nfcap
nfdump filter:
proto TCP
Top 10     IP Addr ordered by flows:
Date first seen          Duration Proto          IP Addr    Flows  Packets    Bytes      pps      bps   bpp
2009-10-21 12:09:02.487 4307721.290 any     200.156.101.193   500210   975228   45.8 M        0       89    49
2009-10-21 12:09:02.375 4307744.862 any     200.156.101.237   395847   798455   50.3 M        0       97    66
2009-10-21 12:09:02.333 4307744.480 any      200.156.98.157   339080   684064   46.3 M        0       90    70
2009-10-21 12:09:02.315 4307744.536 any      200.156.98.151   316986   624316   30.4 M        0       59    51
2009-10-21 12:09:02.359 4307745.057 any     200.156.101.200   312942   614926   30.2 M        0       58    51
2009-10-21 12:09:02.338 4307744.489 any      200.156.98.162   312271   637184   51.7 M        0      100    85
2009-10-21 12:09:02.363 4307744.158 any      200.156.98.154   296398   583842   31.3 M        0       60    56
2009-10-21 12:09:02.385 4307742.120 any     200.156.101.207   280899   548851   25.8 M        0       50    49
2009-10-21 12:09:02.404 4307742.311 any      200.156.98.160   268892   524465   25.1 M        0       48    50
2009-10-21 12:09:02.357 4307744.811 any      200.156.98.178   265003   519454   26.4 M        0       51    53

Summary: total flows: 7086966, total bytes: 4.5 G, total packets: 18.6 M, avg bps: 8968, avg pps: 4, avg bpp: 247
Time window: 2009-10-21 12:09:00 - 2009-12-10 08:44:47
Total flows processed: 7304569, Records skipped: 0, Bytes read: 379843360
Sys: 10.010s flows/second: 729692.4   Wall: 22.273s flows/second: 327944.4
```

Figura IV-7 - Resultado da consulta feita ao Nfsen em função do intervalo de tempo selecionado na Figura IV-6.

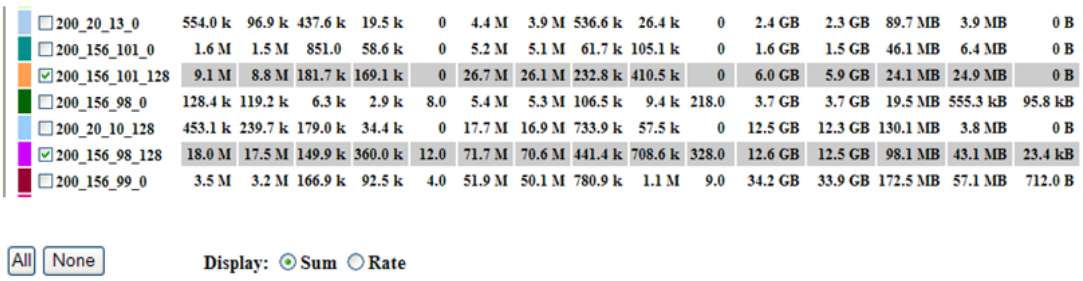


Figura IV-8 - Soma dos dados trafegados no intervalo exibido na Figura IV-6, redes de cor laranja e lilás.

A interface Web do sistema Nfsen oferece diversas funcionalidades de consultas, inclusive com a possibilidade de uso de comandos personalizados como mostra a Figura IV-10, onde, na caixa FILTER, foi digitado a linha "src ip 200.20.1.46" indicando ao sistema que apenas fluxos originados (SRC = source) pelo ip 200.20.1.46, devem ser trazidos como resultado. É possível observar também que na caixa SOURCE, a rede 200.20.1.0 está selecionada. Esta opção é útil para economizar processamento quando se sabe exatamente a rede onde se deseja buscar informações. Caso contrário, todas as redes serão inseridas como fonte de pesquisa, o que irá aumentar consideravelmente o tempo de resposta. Um ponto fraco desta funcionalidade é a lentidão de todo o processo. Tudo deve começar com a seleção do intervalo de tempo através do ponteiro de seleção no gráficos Figura IV-. Este primeiro passo é demorado, pois o sistema faz o cálculo dos valores de todas as redes para o preenchimento do painel mostrado na Figura IV-2. O próximo passo é preencher os critérios de busca, de acordo com as opções disponíveis, como mostra a Figura IV-9.


```
** nfdump -M /usr/local/nfsen/nfsen/profiles-data/live/upstream1  -T  -r 2009/11/27/nfcapd.200911271625 -n 10 -s ip/flows
nfdump filter:
src ip 200.20.0.18
Top 10     IP Addr ordered by flows:
Date first seen          Duration Proto          IP Addr    Flows  Packets    Bytes      pps      bps   bpp
2009-11-27 16:19:03.683 4295264.051 any        200.20.0.18    14563    18989    4.0 M        0        7   221
2009-11-27 16:19:03.685 4295263.832 any      200.156.99.68     1358     1810   393403        0        0   217
2009-11-27 16:19:05.214 4295262.336 any      200.156.96.10     1018     1069   227081        0        0   212
2009-11-27 16:19:05.887 4295258.338 any      200.20.12.242      845     1713   388500        0        0   226
2009-11-27 16:19:05.426 4295261.917 any       200.20.1.125      378      384    59819        0        0   155
2009-11-27 16:19:05.993 4295260.896 any       200.20.0.232      314      319    73788        0        0   231
2009-11-27 16:19:03.826 4295262.241 any     200.156.96.110      312      340    61584        0        0   181
2009-11-27 16:19:05.745 4295261.208 any      200.156.101.2      274      278    75413        0        0   271
2009-11-27 16:19:04.108 4295259.644 any       200.20.1.200      272      275    70358        0        0   255
2009-11-27 16:19:12.493 4295253.104 any    200.156.101.240      264      264    59389        0        0   224

Summary: total flows: 14563, total bytes: 4.0 M, total packets: 18989, avg bps: 7, avg pps: 0, avg bpp: 221
Time window: 2009-11-27 15:24:03 - 2010-01-16 09:29:47
Total flows processed: 818560, Records skipped: 0, Bytes read: 42565732
Sys: 0.115s flows/second: 7057646.9  Wall: 0.582s flows/second: 1404373.2
```

Figura IV-9 - Tela de consulta aos arquivos do perfil.

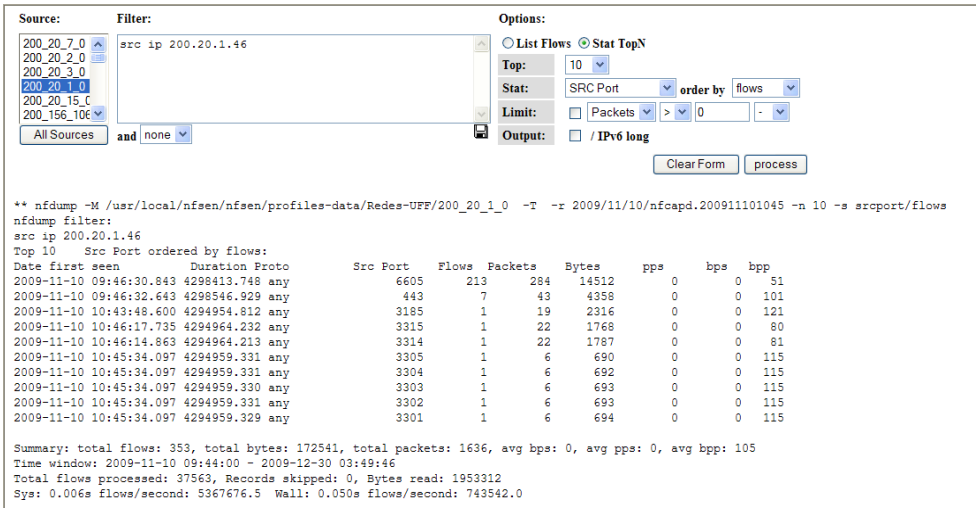


Figura IV-10 - Consulta e resultado utilizando a interface web do Nfsen.

Em "*Options*" é possível exibir entre 10 e 500 registros com as maiores ocorrências. Existem outras opções para filtragem, considerando os campos do cabeçalho IP e ordenação por quantidade de fluxos, bytes ou pacotes. A Opção "*Limit*" permite filtrar o tráfego pelo tamanho do pacote. Outro inconveniente do Nfsen é a inexistência de mecanismo de arquivamento dos resultados das consultas. Cabe ao usuário a tarefa de copiar e colar os relatórios em outro programa para então poder salvar os arquivos. Estes motivos levaram à elaboração de scripts, conforme veremos no tópico a seguir.

4.3 Processamento dos dados coletados – Execução dos scripts

Após o término do período de captura dos fluxos, iniciou-se o processamento dos arquivos armazenados, visando conhecer o perfil de funcionamento da rede – PFR, através da consolidação dos registros de tráfego de cada rede da UFF. Os scripts foram escritos utilizando as linguagens: *shell script*, Awk e o próprio Nfdump, sendo que a primeira foi utilizada para as rotinas básicas de programação, a segunda para os recursos de ordenação e filtragem e a terceira para leitura dos arquivos. As rotinas consistiam em varrer todas as pastas de armazenamento do perfil RedesUff, entrando na pasta correspondente a cada mês e executando o comando Nfdump seguido dos parâmetros de modo a obter a totalização dos dados trafegados.

```
dir="/dados/profiles-data/Redes-UFF"
for i in `cat diretorio`
do
cd $i/2009
echo "Processando rede $i"
for b in `cat /$dir/meses`
do
nfdump -R $b -T -n 20 -s port/flows > $dir/result/$i-$b-port-flow-2009
nfdump -R $b -T -n 20 -s srcport/flows > $dir/result/$i-src-port-$b-2009
nfdump -R $b -T -n 20 -s dstport/flows > $dir/result/$i-$b-dst-port-2009
nfdump -R $b -T -n 20 -s port/bytes > $dir/result/$i-$b-port-bytes-2009
nfdump -R $b -T -n 20 -s dstport/bytes > $dir/result/$i-$b-dst-port-2009
nfdump -R $b -T -n 20 -s srcport/bytes > $dir/result/$i-$b-src-port-2009
nfdump -R $b -T -n 20 -s ip/bytes > $dir/result/$i-$b-ip-port-2009
nfdump -R $b -T -n 20 -s srcip/bytes > $dir/result/$i-$b-srcip-bytes-2009
nfdump -R $b -T -n 20 -s dstip/bytes > $dir/result/$i-$b-dst-bytes-2009
nfdump -R $b -T -n 20 -s ip/flows > $dir/result/$i-$b-ip-flows-2009
nfdump -R $b -T -n 20 -s srcip/flows > $dir/result/$i-$b-srcip-flows-2009
nfdump -R $b -T -n 20 -s dstip/flows > $dir/result/$i-$b-dst-ip-flows-2009
done
cd $dir
done
```

Figura IV-11 - Script para coleta das informações registradas mensalmente no perfil Redes-UFF

A Figura IV-11 mostra um script para a totalização dos dados mensais trafegados por cada rede, ordenados por critérios diversos. O comando FOR busca em um arquivo texto os nomes de todas as pastas do perfil RedesUff, atribuindo-os a variável “i” . Mais adiante a variável “b” recebe os nomes dos meses, também de um arquivo. Nas linhas seguintes, para cada mês atribuído à variável “b” são realizadas consultas com o programa nfdump, onde os valores adicionados após o parâmetro “-s” constituem os critérios da busca e ordenação, por exemplo: port/bytes que trará como resultado as informações constantes na Figura IV-12, ou seja, as 20 portas ordenadas por aquelas que tiveram a maior quantidade de bytes trafegados. Os resultados são redirecionados para uma pasta chamada “*result*” onde os arquivos são gravados, identificados pelo nome da rede, mês, parâmetro de pesquisa e o ano. A Figura IV-12, mostra o conteúdo de um arquivo, resultado de uma consulta que relaciona as 20 portas com o maior valor de bytes trafegados.

```
Top 20    Dst Port ordered by bytes:
Date first seen          Duration Proto         Dst Port    Flows  Packets    Bytes      pps      bps   bpp
2009-02-28 23:57:43.582 6973496.436 any             52543   12.0 M  109.6 M   40.8 G       16    50306   381
2009-02-28 23:59:59.993 6973263.117 any             40024    4.7 M   45.4 M   31.0 G        6    38243   700
2009-02-28 23:58:40.104 6973438.003 any              6881  539697   20.4 M   16.1 G        3    19882   808
2009-02-28 23:57:37.679 6973503.238 any                80    8.9 M  137.2 M   13.5 G       20    16636   100
2009-02-28 23:59:59.996 6973362.295 any                 0   10.1 M   16.4 M   12.9 G        2    15951   806
2009-03-01 02:17:38.993 6965095.294 any             57135    1.2 M   30.4 M   12.7 G        4    15658   427
2009-03-01 02:41:31.997 6897008.285 any             22352  137862   11.4 M   11.7 G        1    14516  1044
2009-03-01 02:06:13.993 6935442.494 any             16751  197727   37.1 M    9.3 G        5    11472   255
2009-03-01 00:00:34.969 6971844.214 any             26174    2.0 M   12.9 M    6.4 G        1     7867   507
2009-03-01 00:20:09.996 6972127.760 any             51413  155039   10.6 M    5.6 G        1     6920   540
2009-03-01 00:38:21.995 6970530.631 any             62468  290919    5.5 M    5.4 G        0     6634  1011
2009-03-01 00:04:45.654 6972974.889 any              5900   66241   12.4 M    4.8 G        1     5876   393
2009-03-01 00:23:48.985 6970628.930 any              4381    2019    3.1 M    4.5 G        0     5505  1482
2009-03-01 00:01:12.989 6973250.621 any              4662  220921    8.9 M    4.5 G        1     5501   514
2009-03-01 00:23:01.995 6955490.070 any             63029    1287    3.1 M    4.4 G        0     5405  1439
2009-03-01 00:37:34.998 6970854.372 any              4756    3020    2.5 M    3.7 G        0     4504  1490
2009-02-28 23:59:59.982 6972112.055 any             19592    8.2 M   22.9 M    3.5 G        3     4331   157
2009-02-28 23:59:59.984 6892935.730 any             17780     941    2.4 M    3.1 G        0     3837  1301
2009-03-01 02:06:20.997 6963036.298 any              2651    2628    2.1 M    2.9 G        0     3617  1428
2009-03-01 03:31:49.998 6955606.563 any             43728    1160    2.0 M    2.9 G        0     3537  1458

Summary: total flows: 265733643, total bytes: 1.1 T, total packets: 1.7 G, avg bps: 1.4 M, avg pps: 254, avg bpp: 703
Time window: 2009-02-28 23:57:32 - 2009-05-20 17:02:46
Total flows processed: 265733643, Records skipped: 0, Bytes read: 13818399888
Sys: 68.108s flows/second: 3901614.0   Wall: 544.988s flows/second: 487595.0
```

Figura IV-12 - Resultado do script de totalização de dados trafegados por uma rede, no mês de Fevereiro, relacionando as 20 portas com mais bytes trafegados.

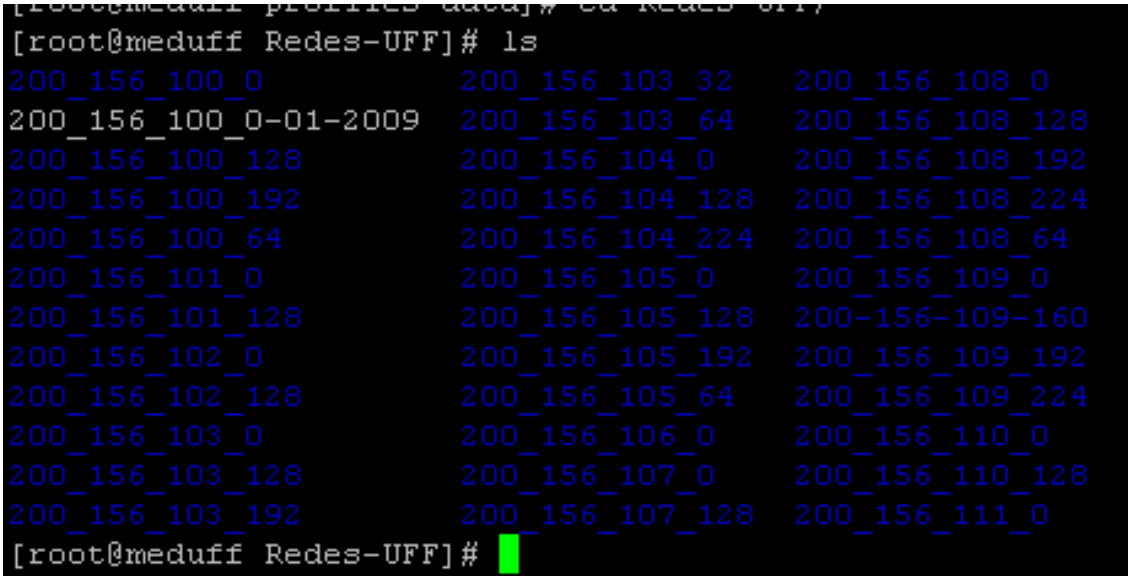


Figura IV-13 - Pastas das redes da UFF armazenadas na pasta principal do perfil RedesUff.

Todos os dados foram produzidos pelo programa Nfdump. O sumário na parte inferior mostra que foram trafegados 1.1 terabytes de dados em 265 Milhões de fluxos trafegando em média de 1.4 Mbit/s. A Figura IV-13, mostra o repositório de pastas do perfil RedesUff.

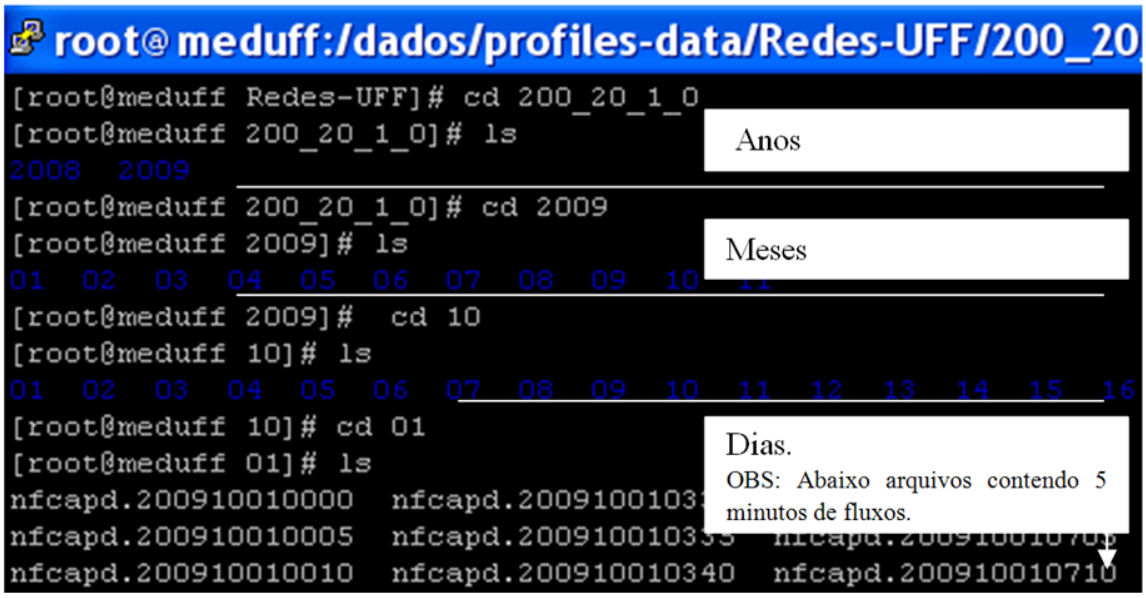


Figura IV-14 - Estrutura das pastas de armazenamento e arquivos.

Como os arquivos só podem ser lidos através do programa nfdump, os scripts se resumiram em rotinas para acessar as pastas e ler os arquivos com o comando nfdump. Quanto à ordenação e filtragem, foi utilizado o programa AWK, algumas vezes no próprio script, outras em scripts à parte, após a obtenção dos dados. Sobre a execução dos scripts, ficou constatado que o processamento destes na própria máquina de monitoramento afetou o funcionamento do sistema como um todo, reduzindo a capacidade de captura de dados. Portanto, é recomendado que os arquivos sejam movidos para outra máquina onde poderão ser processados ou, de outra forma, que os sistemas de monitoramento (Softflowd, Nfsen, Nfdump) sejam desligados.

```
Summary: total flows: 5049609, total bytes: 956.1 M, total packets: 5.2 M, avg bps: 776, avg pps: 0, avg bpp: 183
```

Figura IV-15 - Sumário, resultado de uma consulta mensal utilizando Nfdump

4.4 Resultados obtidos

Inicialmente a consulta aos arquivos gerados pelo sistema buscou conhecer as vinte maiores ocorrências para cada rede, de acordo com os seguintes critérios:

Portas ordenadas por quantidade de fluxos

Portas ordenadas por quantidade de bytes

Além disso, foram coletados os sumários mensais onde constam:

- Total de fluxos;
- Total de bytes;
- Total de pacotes;
- Média de bits/s;
- Média de pacotes/s; e
- Média de bits por pacotes.

Um exemplo do sumário da consulta do Nfdump pode ser visualizado na Figura IV-15. Qualquer consulta feita com o programa Nfdump, gera, além dos dados consultados, um sumário em função do intervalo de tempo delimitado para a consulta. Originalmente cada arquivo armazena cinco minutos de tráfego. Entretanto, através do parâmetro –R é possível fazer consultas considerando todos os arquivos existentes em uma pasta. Neste sentido, o parâmetro –R facilitou a obtenção de informações, uma vez que o sistema trabalha com o armazenamento dos arquivos separados por pastas identificadas por ano, mês e dia. Para conhecer os valores totais do tráfego das redes foi utilizado o programa AWK para filtrar as linhas começadas como a palavra ”*Summary*” existentes ao final de cada resultado. Posteriormente, os Sumários foram salvos em arquivos para serem importados por outros programas para a produção dos gráficos. O resultado da consulta realizada pelo Nfsen é idêntico ao resultado do Nfdump na linha de comando, isso porque o Nfsen, através da linguagem PHP, chama o Nfdump passando os parâmetros inseridos pelo usuário nas telas do sistema. O benefício do uso de scripts, como dito anteriormente, está na agilidade e facilidade de obtenção dos dados. Este fator se mostrou essencial considerando o volume de consultas realizadas, como foi o caso do perfil RedesUff composto por 76 redes.

Ao comparar os gráficos das figuras Figura IV-16 e Figura IV-17, verificou-se que, no mês de janeiro, as redes 200.20.1.0 e 200.20.2.0, registraram valores semelhantes com relação aos fluxos, entretanto, nos meses seguintes ocorreram reduções progressivas nos registros da rede 200.20.2.0. Ao buscar as razões para a redução da quantidade de fluxos da rede 200.20.2.0, verificou-se que dos 232.000.000 de fluxos registrados em janeiro, 149.300.000 estavam relacionados à porta 40999 e ao ip 200.20.2.206 como é possível observar na Figura IV-25 e Figura IV-24, sendo este host foi o responsável direto pelo

colocação da rede 200.20.2.0 em primeiro lugar. Isto reforça a necessidade de conhecer a natureza das demandas, uma vez que, se a atividade de rede registrada pelo endereço 200.20.2.206 não for de interesse da instituição, os administradores de rede poderão ser levados a providênciar melhorias na estrutura que não irão beneficiar necessariamente a instituição.

Nos gráficos das Figura IV-16, Figura IV-17 e Figura IV-18 foram acrescentadas informações sobre o mês de outubro de 2009, visando perceber as alterações decorrentes das modificações realizadas no sistema, descritas no capítulo III, item 3.9.

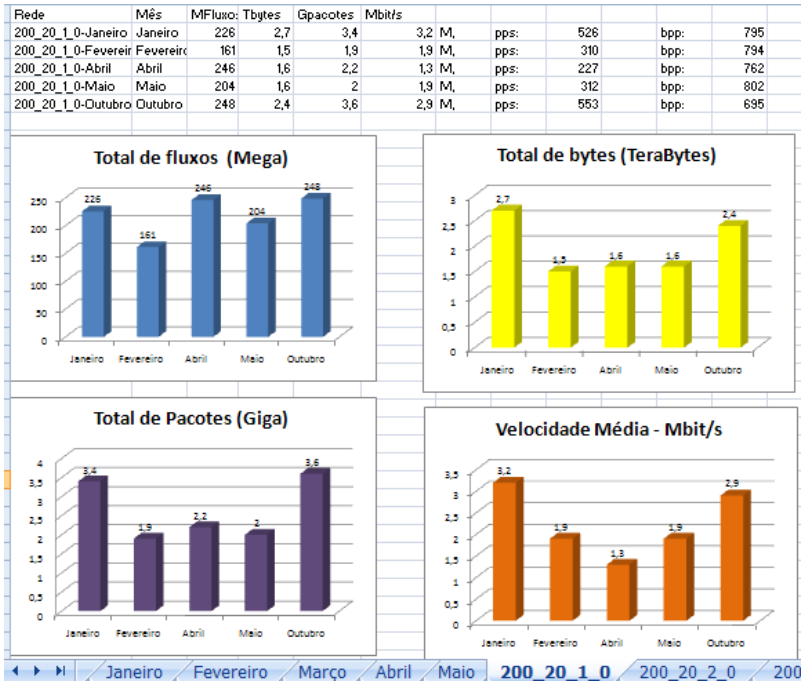


Figura IV-16 - Gráficos da rede 200.20.1.0. Informações sobre a quantidade de fluxos, bytes, pacotes e bit/s registrados entre Janeiro e Maio e o mês de Outubro de 2009.

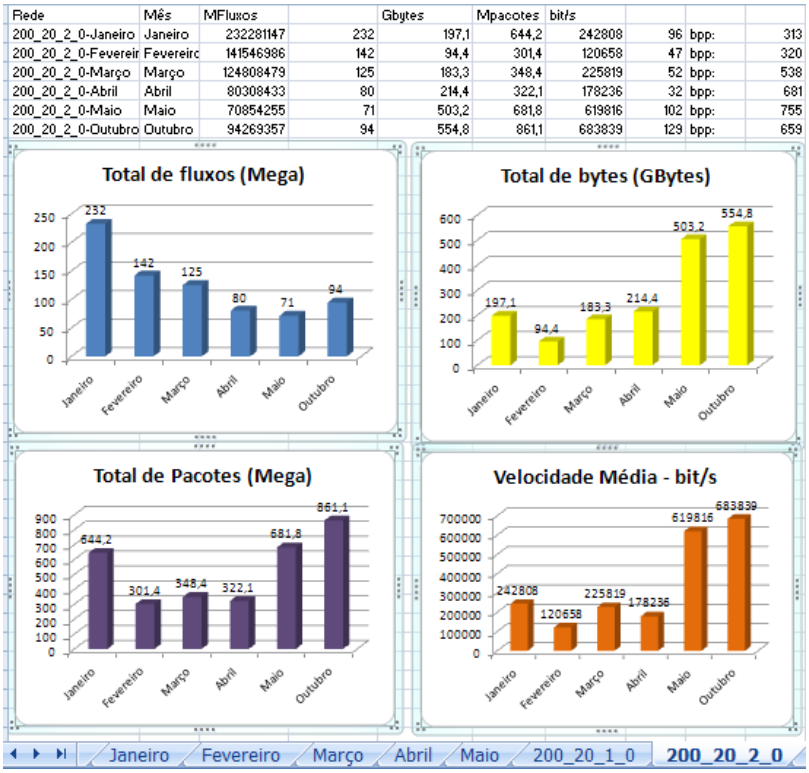


Figura IV-17 - Gráficos da rede 200.20.2.0. Informações sobre a quantidade de fluxos, bytes, pacotes e bit/s registrados entre Janeiro e Maio e o mês de Outubro 2009.

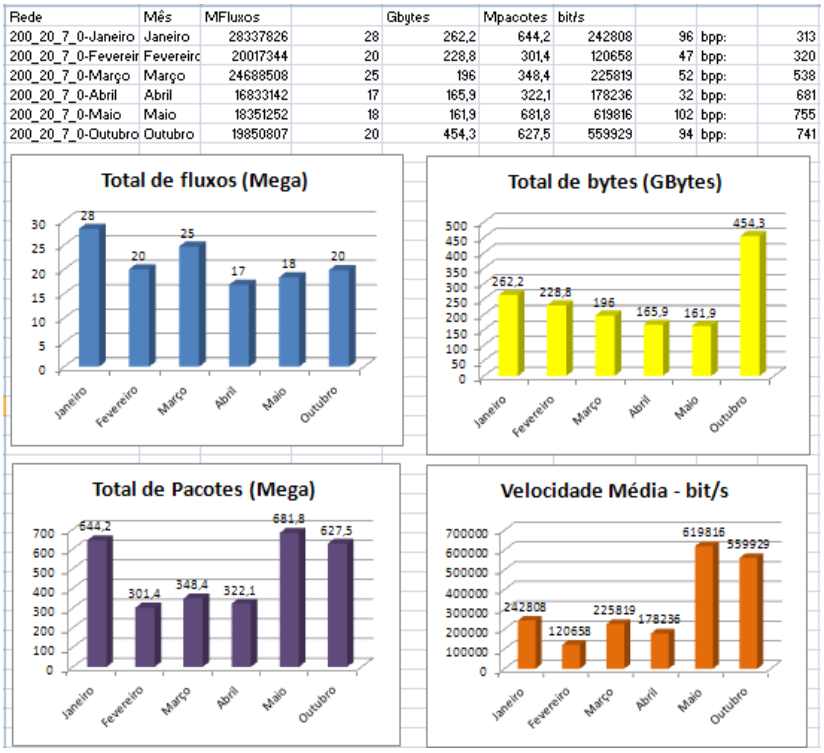


Figura IV-18 - Gráfico da rede 200.20.7.0. Informações sobre a quantidade de fluxos, bytes, pacotes e bit/s registrados entre Janeiro e Maio mais o mês de Outubro 2009.

As figuras III.20, III.21, III.22, III.23, III.25 e III.26 constituem os resultados obtidos através da execução do script mostrado na Figura IV-11, com relação às redes 200.20.1.0, 200.20.2.0 e rede 200.20.7.0. O script foi executado em todas as 76 redes e objetivou conhecer o universo das portas mais utilizadas e a sua expressividade com relação ao total de recursos consumidos pela própria rede, bem como o impacto causado na Rede UFF como um todo. Os sumários existentes ao final de cada resultado emitido pelo programa Nfdump serviram para construção de rankings mensais, em função da quantidade de fluxos registrados, como mostrado na Figura IV-27 As figuras, III.28 e III.29 mostraram as alterações ocorridas na posição de cada rede, no ranking, entre janeiro e maio de 2009.

4.5 Utilização dos dados registrados.

Inicialmente, os dados registrados a partir do perfil RedesUFF permitiram:

a. Conhecer o universo das redes que mais consomem os recursos da Rede UFF
b. Conhecer o universo das portas utilizadas por cada rede. (Figuras de III.20 a III.26)
c. Determinar o consumo dos recursos da rede, por porta, em relação ao consumo total da rede. (Figura IV-30)
d. Determinar o valor percentual do consumo dos recursos individuais de cada rede, em relação ao total registrado para a rede da UFF no período. (Figura IV-19)
e. Gerar os gráficos comparativos e de acompanhamento (figuras III.30 a III.32).
f. Programar alertas em função da alteração do PRF da rede, conforme será demonstrado no tópico sobre segurança.

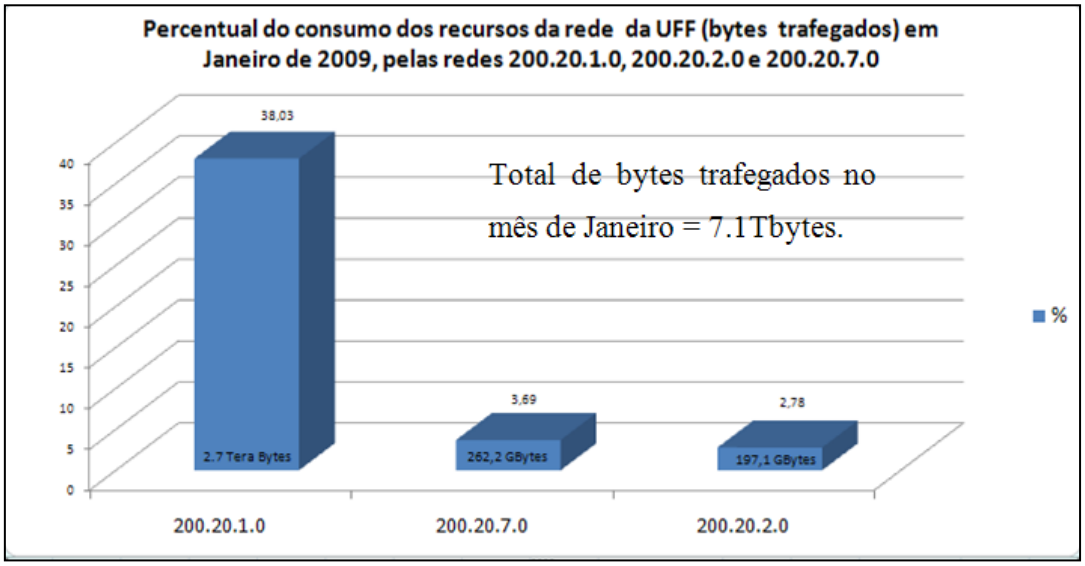


Figura IV-19 - Consumo percentual dos recursos da rede UFF, por rede.

```
Top 20        Port ordered by bytes:
Date first seen          Duration Proto            Port    Flows  Packets    Bytes      pps      bps   bpp
2008-12-31 23:58:55.761 6973421.555 any            52543   12.9 M  598.5 M  529.3 G       90   651944   905
2008-12-31 23:59:05.574 6973399.612 any               80   26.0 M  539.1 M  460.4 G       81   567180   874
2009-01-01 00:02:14.118 6973197.979 any             4662    4.9 M  471.2 M  432.3 G       70   532493   939
2009-01-01 15:53:13.946 6915648.246 any            26665    3.0 M  353.6 M  289.7 G       53   359829   838
2008-12-31 23:58:58.649 6973399.633 any               22   15.4 M  181.7 M  113.2 G       27   139450   638
2009-01-01 07:20:23.759 6946912.496 any            16751    2.5 M  106.5 M   81.0 G       16   100193   778
2008-12-31 23:58:54.909 6973393.396 any             6882    3.2 M  107.4 M   71.8 G       16    88422   684
2008-12-31 23:58:54.913 6973395.534 any                0    2.8 M  109.7 M   71.0 G       16    87486   662
2009-01-01 00:10:57.543 6972678.950 any            26174    3.8 M   63.1 M   59.3 G        9    73047   962
2009-01-01 00:01:41.652 6973012.938 any            56121    1.6 M   56.4 M   57.4 G        8    70744  1042
2009-01-01 02:17:00.637 6902331.099 any              873     9758   54.0 M   53.8 G        8    66978  1021
2009-01-01 00:08:27.424 6972835.587 any            54302    2.3 M   40.1 M   32.1 G        6    39514   818
2009-01-01 00:12:55.954 6968830.006 any            29311  858063   47.6 M   28.5 G        7    35168   614
2009-01-01 00:00:03.077 6973348.092 any             3128    2.9 M   26.5 M   17.5 G        3    21610   677
2009-01-01 01:29:35.692 6957801.856 any            41252    3265   13.8 M   14.0 G        2    17324  1041
2008-12-31 23:59:51.268 6972971.448 any             5900  589699   20.8 M   13.5 G        3    16670   665
2009-01-01 01:14:12.736 6968507.083 any            57135  473677   12.1 M   10.5 G        1    12987   892
2009-01-01 00:02:41.525 6966782.937 any            47460    2404    8.1 M    9.6 G        1    11802  1217
2009-01-01 00:30:17.158 6970825.635 any            48220    2523    7.9 M    8.8 G        1    10863  1140
2009-01-01 08:36:51.668 6936383.894 any            43853    1.6 M   43.5 M    8.2 G        6    10210   194

Summary: total flows: 225530705, total bytes: 2.7 T, total packets: 3.4 G, avg bps: 3.2 M, avg pps: 526, avg bpp: 795
Time window: 2008-12-31 23:58:54 - 2009-03-22 16:02:43
Total flows processed: 225530705, Records skipped: 0, Bytes read: 11727820172
Sys: 73.345s flows/second: 3074893.9   Wall: 396.961s flows/second: 568142.7
```

Figura IV-20 - Resultado da consulta utilizando Nfdump via script. As 20 portas mais utilizadas pela rede 200.20.1.0, no mês de Janeiro de 2009, ordenadas por bytes.

```
Top 20        Port ordered by flows:
Date first seen          Duration Proto             Port    Flows  Packets    Bytes      pps      bps   bpp
2009-01-03 03:38:05.766 6769830.329 any              445   27.0 M   41.7 M    2.1 G        6     2627    50
2008-12-31 23:59:05.574 6973399.612 any               80   26.0 M  539.1 M  460.4 G       81   567180   874
2008-12-31 23:58:58.649 6973399.633 any               22   15.4 M  181.7 M  113.2 G       27   139450   638
2008-12-31 23:59:24.069 6973359.335 any            19299   14.3 M   30.3 M    2.9 G        4     3598    98
2008-12-31 23:58:55.761 6973421.555 any            52543   12.9 M  598.5 M  529.3 G       90   651944   905
2009-01-01 00:07:21.890 6972884.488 any             6605   11.2 M   15.4 M    2.1 G        2     2536   137
2008-12-31 23:59:01.190 6973379.237 any            11082    8.8 M   14.3 M    1.5 G        2     1839   107
2008-12-31 23:59:27.147 6973369.396 any            27491    7.6 M    8.7 M    1.6 G        1     1977   189
2009-01-01 09:28:02.064 6939254.482 any            19592    6.5 M   15.4 M    6.1 G        2     7503   403
2009-01-01 00:00:35.684 6970338.177 any            32870    5.0 M   12.4 M    4.8 G        1     5973   400
2009-01-01 00:02:14.118 6973197.979 any             4662    4.9 M  471.2 M  432.3 G       70   532493   939
2009-01-01 00:56:22.994 6964731.556 any             6195    4.6 M    6.2 M  690.2 M        0      831   111
2009-01-01 00:10:57.543 6972678.950 any            26174    3.8 M   63.1 M   59.3 G        9    73047   962
2008-12-31 23:58:56.840 6973393.261 any               53    3.5 M    4.4 M  445.8 M        0      536   100
2008-12-31 23:58:54.909 6973393.396 any             6882    3.2 M  107.4 M   71.8 G       16    88422   684
2009-01-01 00:10:09.990 6972725.151 any             4672    3.0 M    4.2 M  594.3 M        0      714   142
2009-01-01 15:53:13.946 6915648.246 any            26665    3.0 M  353.6 M  289.7 G       53   359829   838
2009-01-01 00:49:25.442 6952933.705 any            31727    3.0 M    3.6 M  862.9 M        0     1041   239
2009-01-01 00:00:03.077 6973348.092 any             3128    2.9 M   26.5 M   17.5 G        3    21610   677
2008-12-31 23:58:54.913 6973395.534 any                0    2.8 M  109.7 M   71.0 G       16    87486   662

Summary: total flows: 225530705, total bytes: 2.7 T, total packets: 3.4 G, avg bps: 3.2 M, avg pps: 526, avg bpp: 795
Time window: 2008-12-31 23:58:54 - 2009-03-22 16:02:43
Total flows processed: 225530705, Records skipped: 0, Bytes read: 11727820172
Sys: 73.574s flows/second: 3065324.8  Wall: 399.621s flows/second: 564360.5
```

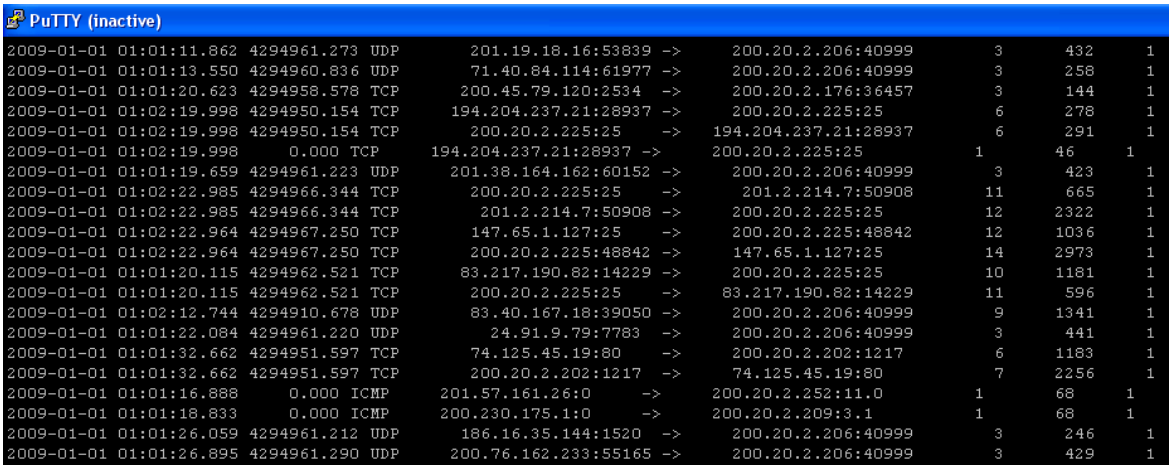
Figura IV-21 - Resultado da consulta utilizando Nfdump via script. As 20 portas mais utilizadas pela rede 200.20.1.0 ordenadas por fluxos

```
Date first seen          Duration Proto         Dst Port    Flows  Packets    Bytes      pps      bps   bpp
2008-12-31 23:59:04.000 6973404.668 any            40999   70.9 M   94.6 M   13.9 G       14    17114   150
2008-12-31 23:59:47.618 6973346.524 any               80    2.3 M  167.3 M    8.7 G       25    10770    53
2009-01-01 00:01:54.863 6972920.709 any             7249    5.4 M   33.7 M    4.1 G        5     4997   123
2009-01-02 19:30:13.998 6815237.087 any            18121    3993    2.9 M    4.0 G        0     5029  1404
2009-01-02 15:14:31.583 6823634.463 any             1513    9210    2.9 M    3.9 G        0     4963  1391
2009-01-05 22:34:17.290 6543925.988 any            26759    4367    2.6 M    3.6 G        0     4709  1401
2009-01-02 17:47:04.303 6822880.669 any             1052   57695    2.7 M    3.5 G        0     4408  1325
2009-01-01 01:01:32.662 6969070.294 any             1217   14646    2.5 M    3.4 G        0     4157  1404
2009-01-01 00:05:29.662 6973017.870 any              443    7.2 M   22.0 M    3.3 G        3     4057   152
2009-01-01 10:20:17.946 6930071.990 any             1725    5276    2.3 M    3.2 G        0     3933  1405
2009-01-03 15:12:25.281 6729894.031 any            56382    2349    2.4 M    3.1 G        0     3924  1299
2009-01-02 16:08:16.982 6819548.441 any             3001    3356    2.2 M    3.0 G        0     3757  1407
2009-01-01 00:07:17.011 6972899.543 any            27938   14.7 M   16.8 M    2.2 G        2     2686   133
2009-01-03 13:58:41.642 6746995.723 any            50025    5278    1.3 M    1.8 G        0     2307  1401
2009-01-01 22:20:49.781 6892615.090 any             2380    3501    1.3 M    1.8 G        0     2253  1442
2009-01-02 17:52:14.204 6822464.393 any             1138   14050    1.3 M    1.8 G        0     2250  1381
2009-01-05 09:11:43.856 6593676.241 any            61283    2994    1.2 M    1.7 G        0     2167  1405
2009-01-01 19:39:03.993 6901844.010 any            51666    1612    1.1 M    1.5 G        0     1889  1411
2009-01-01 04:10:14.312 6952118.539 any             2395    7516    1.1 M    1.5 G        0     1829  1397
2009-01-05 10:24:08.059 6587263.333 any            21241    3110    1.0 M    1.4 G        0     1803  1409

Summary: total flows: 232281147, total bytes: 197.1 G, total packets: 644.2 M, avg bps: 242808, avg pps: 96, avg bpp: 313
Time window: 2008-12-31 23:59:03 - 2009-03-22 16:02:34
Total flows processed: 232281147, Records skipped: 0, Bytes read: 12078857628
Sys: 67.781s flows/second: 3426900.9  Wall: 419.002s flows/second: 554367.4
```

Figura IV-22 - Resultado da consulta utilizando Nfdump via script. As 20 portas de destino mais utilizadas pela rede 200.20.2.0 no mês de Janeiro de 2009, ordenadas por fluxos.

```
Top 20        Port ordered by bytes:
Date first seen          Duration Proto             Port    Flows  Packets    Bytes      pps      bps   bpp
2009-01-01 00:01:54.863 6972920.709 any             7249   11.5 M   88.0 M   69.7 G       13    85913   811
2008-12-31 23:59:10.416 6973383.726 any               80    4.2 M  198.1 M   48.2 G       29    59378   249
2008-12-31 23:59:04.000 6973404.668 any            40999  149.3 M  199.5 M   28.6 G       29    35255   146
2009-01-01 08:56:23.153 6935777.078 any            54640   528992   10.0 M    8.4 G        1    10433   859
2009-01-01 00:05:29.662 6973017.870 any              443   14.9 M   45.6 M    6.6 G        6     8086   147
2009-01-01 00:07:17.011 6972899.543 any            27938   30.6 M   34.7 M    6.5 G        5     7961   190
2009-01-02 19:30:13.998 6815237.087 any            18121    7785    4.5 M    4.1 G        0     5127   920
2009-01-01 03:10:44.031 6953462.015 any             1513   19290    4.7 M    4.0 G        0     4976   879
2009-01-01 02:56:48.029 6961229.475 any             1326   16721    4.2 M    3.7 G        0     4530   893
2009-01-05 22:34:17.290 6543925.988 any            26759    8545    4.2 M    3.7 G        0     4807   897
2009-01-01 02:17:19.596 6965065.376 any             1052  117589    4.4 M    3.6 G        0     4429   835
2009-01-01 01:01:32.662 6969070.294 any             1217   30410    3.8 M    3.4 G        0     4239   924
2009-01-01 10:20:17.946 6930071.990 any             1725   11620    2.8 M    3.2 G        0     3963  1187
2009-01-02 18:51:43.448 6803135.864 any            56382    4334    3.8 M    3.1 G        0     3962   855
2009-01-01 08:06:11.089 6940438.319 any             3001    7196    3.6 M    3.1 G        0     3777   862
2009-01-02 15:29:09.235 6827613.665 any            26679   97232    3.0 M    2.9 G        0     3587   974
2009-01-01 11:12:21.877 6932722.994 any             2380    7878    2.2 M    1.9 G        0     2293   880
2009-01-02 15:49:02.802 6826774.563 any            50025   10639    2.1 M    1.9 G        0     2328   895
2009-01-01 11:10:28.842 6927497.119 any               81   29880    5.4 M    1.8 G        0     2264   348
2009-01-01 10:57:30.831 6933747.766 any             1138   28967    1.9 M    1.8 G        0     2253   979

Summary: total flows: 232281147, total bytes: 197.1 G, total packets: 644.2 M, avg bps: 242808, avg pps: 96, avg bpp: 313
Time window: 2008-12-31 23:59:03 - 2009-03-22 16:02:34
Total flows processed: 232281147, Records skipped: 0, Bytes read: 12078857628
Sys: 78.907s flows/second: 2943733.0  Wall: 422.742s flows/second: 549463.0
```

Figura IV-23 - Resultado da consulta utilizando NFDUMP via script. As 20 portas mais utilizadas pela rede 200.20.2.0 no mês de Janeiro de 2009, ordenadas por bytes.



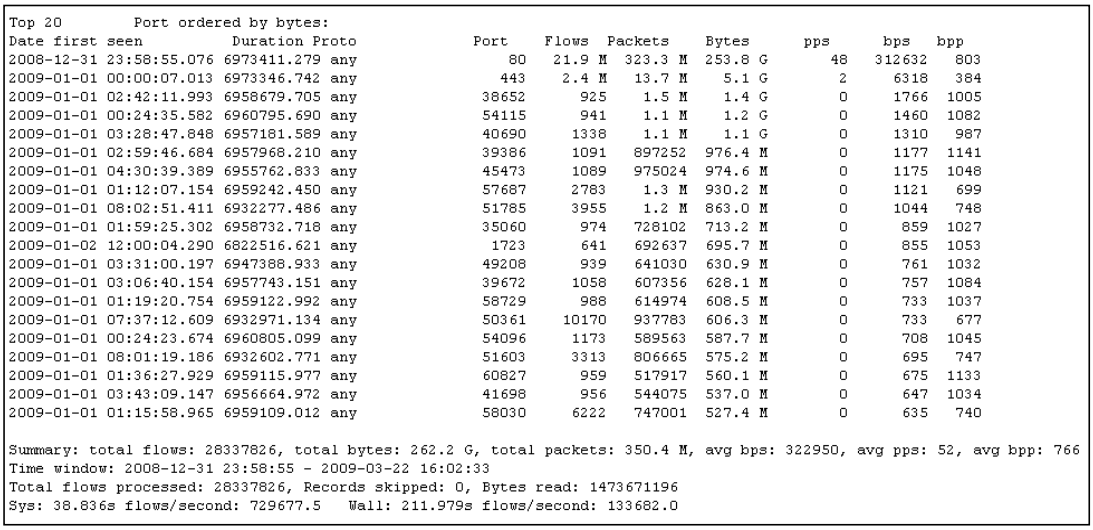
PuTTY (inactive)

```
2009-01-01 01:01:11.862 4294961.273 UDP       201.19.18.16:53839 ->     200.20.2.206:40999        3       432      1
2009-01-01 01:01:13.550 4294960.836 UDP       71.40.84.114:61977 ->     200.20.2.206:40999        3       258      1
2009-01-01 01:01:20.623 4294958.578 TCP      200.45.79.120:2534  ->     200.20.2.176:36457        3       144      1
2009-01-01 01:02:19.998 4294950.154 TCP     194.204.237.21:28937 ->     200.20.2.225:25           6       278      1
2009-01-01 01:02:19.998 4294950.154 TCP       200.20.2.225:25    ->   194.204.237.21:28937        6       291      1
2009-01-01 01:02:19.998     0.000 TCP     194.204.237.21:28937 ->     200.20.2.225:25           1        46      1
2009-01-01 01:01:19.659 4294961.223 UDP     201.38.164.162:60152 ->     200.20.2.206:40999        3       423      1
2009-01-01 01:02:22.985 4294966.344 TCP       200.20.2.225:25    ->      201.2.214.7:50908       11       665      1
2009-01-01 01:02:22.985 4294966.344 TCP        201.2.214.7:50908 ->     200.20.2.225:25          12      2322      1
2009-01-01 01:02:22.964 4294967.250 TCP       147.65.1.127:25    ->     200.20.2.225:48842       12      1036      1
2009-01-01 01:02:22.964 4294967.250 TCP       200.20.2.225:48842 ->     147.65.1.127:25          14      2973      1
2009-01-01 01:01:20.115 4294962.521 TCP      83.217.190.82:14229 ->     200.20.2.225:25          10      1181      1
2009-01-01 01:01:20.115 4294962.521 TCP       200.20.2.225:25    ->    83.217.190.82:14229       11       596      1
2009-01-01 01:02:12.744 4294910.678 UDP       83.40.167.18:39050 ->     200.20.2.206:40999        9      1341      1
2009-01-01 01:01:22.084 4294961.220 UDP         24.91.9.79:7783  ->     200.20.2.206:40999        3       441      1
2009-01-01 01:01:32.662 4294951.597 TCP       74.125.45.19:80    ->     200.20.2.202:1217         6      1183      1
2009-01-01 01:01:32.662 4294951.597 TCP       200.20.2.202:1217  ->     74.125.45.19:80           7      2256      1
2009-01-01 01:01:16.888     0.000 ICMP     201.57.161.26:0      ->     200.20.2.252:11.0         1        68      1
2009-01-01 01:01:18.833     0.000 ICMP     200.230.175.1:0      ->     200.20.2.209:3.1          1        68      1
2009-01-01 01:01:26.059 4294961.212 UDP      186.16.35.144:1520  ->     200.20.2.206:40999        3       246      1
2009-01-01 01:01:26.895 4294961.290 UDP      200.76.162.233:55165 ->     200.20.2.206:40999        3       429      1
```

Figura IV-24 - Detalhes dos acessos relacionados à porta 40999, realizados no mês de Janeiro na rede 200.20.2.0, pelo host 20.20.2.206.

```
Top 20        Port ordered by flows:
Date first seen          Duration Proto             Port    Flows  Packets    Bytes      pps      bps   bpp
2008-12-31 23:58:55.076 6973411.279 any               80   21.9 M  323.3 M  253.8 G       48   312632   803
2009-01-01 00:00:07.013 6973346.742 any              443    2.4 M   13.7 M    5.1 G        2     6318   384
2008-12-31 23:59:02.496 6973253.013 any                0    1.2 M    1.5 M   91.8 M        0      110    62
2008-12-31 23:59:02.496 6973253.004 any             2048 1038655    1.1 M   72.3 M        0       87    63
2008-12-31 23:59:42.152 6973333.186 any               53  621824    3.4 M  223.9 M        0      269    65
2009-01-01 00:17:07.781 6970836.853 any               22  590500    3.7 M  475.0 M        0      571   129
2009-01-01 04:01:47.385 6950475.796 any            32771   97724    2.2 M  151.5 M        0      182    68
2008-12-31 23:59:12.881 6969533.219 any             2816   69209   109461    6.5 M        0        7    62
2009-01-01 00:05:05.402 6935564.510 any             1433   49480   462219  191.4 M        0      231   434
2008-12-31 23:58:58.339 6973268.055 any              110   40132   741507   69.0 M        0       82    97
2008-12-31 23:59:32.315 6961749.995 any              769   39702    78873    4.9 M        0        5    64
2009-01-01 00:02:17.111 6972721.305 any             5900   36055    55923    2.6 M        0        3    49
2009-01-01 02:13:52.226 6963828.315 any             1025   31873    83415    5.6 M        0        6    70
2009-01-01 08:06:21.952 6900308.945 any               23   26459    56316    6.6 M        0        7   121
2009-01-01 22:30:08.741 6630510.284 any             2769   25912    59363    3.8 M        0        4    67
2009-01-02 07:20:05.473 6857669.117 any            11395   25776    89712    5.0 M        0        6    58
2009-01-01 09:16:10.741 6886496.917 any             4899   24489    50052    2.3 M        0        2    48
2009-01-02 08:25:02.991 6740538.350 any            23000   23088   111622   44.0 M        0       54   412
2009-01-01 00:50:45.955 6967087.870 any             1004   23042    90810    7.3 M        0        8    84
2009-01-02 16:13:30.442 6460813.560 any             2311   20915    46989    3.0 M        0        3    66

Summary: total flows: 28337826, total bytes: 262.2 G, total packets: 350.4 M, avg bps: 322950, avg pps: 52, avg bpp: 766
Time window: 2008-12-31 23:58:55 - 2009-03-22 16:02:33
Total flows processed: 28337826, Records skipped: 0, Bytes read: 1473671196
Sys: 38.836s flows/second: 729677.5   Wall: 211.979s flows/second: 133682.0
```

Figura IV-25 - Resultado da consulta utilizando Nfdump via script. As 20 portas mais utilizadas pela rede 200.20.7.0 no mês de Janeiro de 2009, ordenadas por fluxos.



```
Top 20        Port ordered by bytes:
Date first seen          Duration Proto             Port    Flows  Packets    Bytes      pps      bps   bpp
2008-12-31 23:58:55.076 6973411.279 any              80   21.9 M  323.3 M  253.8 G       48   312632   803
2009-01-01 00:00:07.013 6973346.742 any             443    2.4 M   13.7 M    5.1 G        2     6318   384
2009-01-01 02:42:11.993 6958679.705 any           38652      925    1.5 M    1.4 G        0     1766  1005
2009-01-01 00:24:35.582 6960795.690 any           54115      941    1.1 M    1.2 G        0     1460  1082
2009-01-01 03:28:47.848 6957181.589 any           40690     1338    1.1 M    1.1 G        0     1310   987
2009-01-01 02:59:46.684 6957968.210 any           39386     1091   897252  976.4 M        0     1177  1141
2009-01-01 04:30:39.389 6955762.833 any           45473     1089   975024  974.6 M        0     1175  1048
2009-01-01 01:12:07.154 6959242.450 any           57687     2783    1.3 M  930.2 M        0     1121   699
2009-01-01 08:02:51.411 6932277.486 any           51785     3955    1.2 M  863.0 M        0     1044   748
2009-01-01 01:59:25.302 6958732.718 any           35060      974   728102  713.2 M        0      859  1027
2009-01-02 12:00:04.290 6822516.621 any            1723      641   692637  695.7 M        0      855  1053
2009-01-01 03:31:00.197 6947388.933 any           49208      939   641030  630.9 M        0      761  1032
2009-01-01 03:06:40.154 6957743.151 any           39672     1058   607356  628.1 M        0      757  1084
2009-01-01 01:19:20.754 6959122.992 any           58729      988   614974  608.5 M        0      733  1037
2009-01-01 07:37:12.609 6932971.134 any           50361    10170   937783  606.3 M        0      733   677
2009-01-01 00:24:23.674 6960805.099 any           54096     1173   589563  587.7 M        0      708  1045
2009-01-01 08:01:19.186 6932602.771 any           51603     3313   806665  575.2 M        0      695   747
2009-01-01 01:36:27.929 6959115.977 any           60827      959   517917  560.1 M        0      675  1133
2009-01-01 03:43:09.147 6956664.972 any           41698      956   544075  537.0 M        0      647  1034
2009-01-01 01:15:58.965 6959109.012 any           58030     6222   747001  527.4 M        0      635   740

Summary: total flows: 28337826, total bytes: 262.2 G, total packets: 350.4 M, avg bps: 322950, avg pps: 52, avg bpp: 766
Time window: 2008-12-31 23:58:55 - 2009-03-22 16:02:33
Total flows processed: 28337826, Records skipped: 0, Bytes read: 1473671196
Sys: 38.836s flows/second: 729677.5   Wall: 211.979s flows/second: 133682.0
```

Figura IV-26 - Resultado da consulta utilizando Nfdump via script. As 20 portas mais utilizadas pela rede 200.20.7.0 no mês de Janeiro de 2009, ordenadas por bytes.

	Rede	Fluxos	Bytes		Pacotes		bit/s		pps	bpp
2	200_20_2_0	232281147	197.1	G,	644.2	M,	242808		96	313
3	200_20_1_0	225530705	2.7	T,	3.4	G,	3.2	M,	526	795
4	200_20_9_192	137666723	195.8	G,	749.6	M,	241219		112	267
5	200_20_15_0	137016890	1.2	T,	1.7	G,	1.4	M,	258	706
6	200_20_9_64	116636915	2.0	T,	2.4	G,	2.4	M,	373	848
7	200_20_10_64	84174675	1.2	T,	1.6	G,	1.4	M,	242	747
8	200_20_5_128	45253120	147.9	G,	279.1	M,	182155		41	542
9	200_20_10_0	42792013	41.0	G,	106.1	M,	50517		15	395
10	200_20_12_0	37626254	306.4	G,	411.9	M,	377484		61	761
11	200_20_7_0	28337826	262.2	G,	350.4	M,	322950		52	766
12	200_156_99_0	27108216	818.9	G,	995.9	M,	1008776		149	842
13	200_156_104_0	26184521	321.8	G,	413.5	M,	396451		62	797
14	200_156_110_128	25121112	295.2	G,	404.5	M,	363627		60	747
15	200_156_103_128	23350884	707.3	G,	857.8	M,	871288		128	844
16	200_156_99_128	22985625	203.1	G,	276.3	M,	250234		41	752
17	200_156_97_0	22888296	210.1	G,	274.0	M,	258842		41	785
18	200_156_101_0	21120847	337.8	G,	486.1	M,	416084		73	711
19	200_20_3_0	20298827	174.3	G,	232.1	M,	214756		34	769
20	200_156_105_0	16943589	44.2	G,	73.7	M,	54439		11	614
21	200_156_101_128	16917841	36.2	G,	60.3	M,	44582		9	614
22	200_20_10_128	16891142	67.3	G,	99.8	M,	82908		15	690
23	200_156_98_128	16274091	104.9	G,	686.4	M,	129180		103	156

Gráficos (2) | Gráficos | RankingII | **Janeiro** | Fevereiro | Março | Abril | Maio

Figura IV-27 - Tabulação dos sumários do perfil RedesUFF, ranking do mês de Janeiro, selecionando as 20 redes com a maior quantidade de fluxos.

Ranking	Janeiro	Fevereiro	Março	Abril	Maio
1º	200_20_2_0	200_20_1_0	200_20_1_0	200_20_1_0	200_20_1_0
2º	200_20_1_0	200_20_2_0	200_20_2_0	200_20_15_0	200_156_105_64
3º	200_20_9_192	200_20_15_0	200_20_15_0	200_156_105_64	200_156_98_128
4º	200_20_15_0	200_156_105_64	200_156_104_0	200_20_2_0	200_20_15_0
5º	200_20_9_64	200_20_10_64	200_20_12_0	200_156_98_128	200_20_2_0
6º	200_20_10_64	200_156_104_0	200_156_98_128	200_20_12_0	200_20_10_128
7º	200_20_5_128	200_20_9_64	200_20_10_64	200_20_9_64	200_20_12_0
8º	200_20_10_0	200_20_12_0	200_20_9_64	200_20_5_0	200_156_106_0
9º	200_20_12_0	200_156_98_128	200_156_106_0	200_156_105_192	200_156_99_128
10º	200_20_7_0	200_20_5_128	200_156_99_0	200_156_106_0	200_156_99_0
11º	200_156_99_0	200_20_10_0	200_156_110_128	200_20_10_128	200_20_10_64
12º	200_156_104_0	200_156_99_0	200_156_105_64	200_156_110_128	200_20_10_0
13º	200_156_110_128	200_20_5_0	200_20_10_0	200_20_10_64	200_20_9_64
14º	200_156_103_128	200_20_9_192	200_20_7_0	200_156_104_0	200_156_110_128
15º	200_156_99_128	200_20_7_0	200_156_99_128	200_156_99_0	200_156_96_0
16º	200_156_97_0	200_156_106_0	200_20_5_0	200_156_96_0	200_20_3_0
17º	200_156_101_0	200_156_99_128	200_20_3_0	200_20_10_0	200_20_6_128
18º	200_20_3_0	200_156_105_0	200_20_10_128	200_20_3_0	200_20_11_0
19º	200_156_105_0	200_156_102_128	200_20_11_0	200_20_7_0	200_20_5_0
20º	200_156_101_128	200_20_10_128	200_156_105_0	200_156_99_128	200_156_102_0

Figura IV-28 - Comparação mês a mês entre as 20 redes com mais fluxos registrados. Período de Janeiro a Maio de 2009.

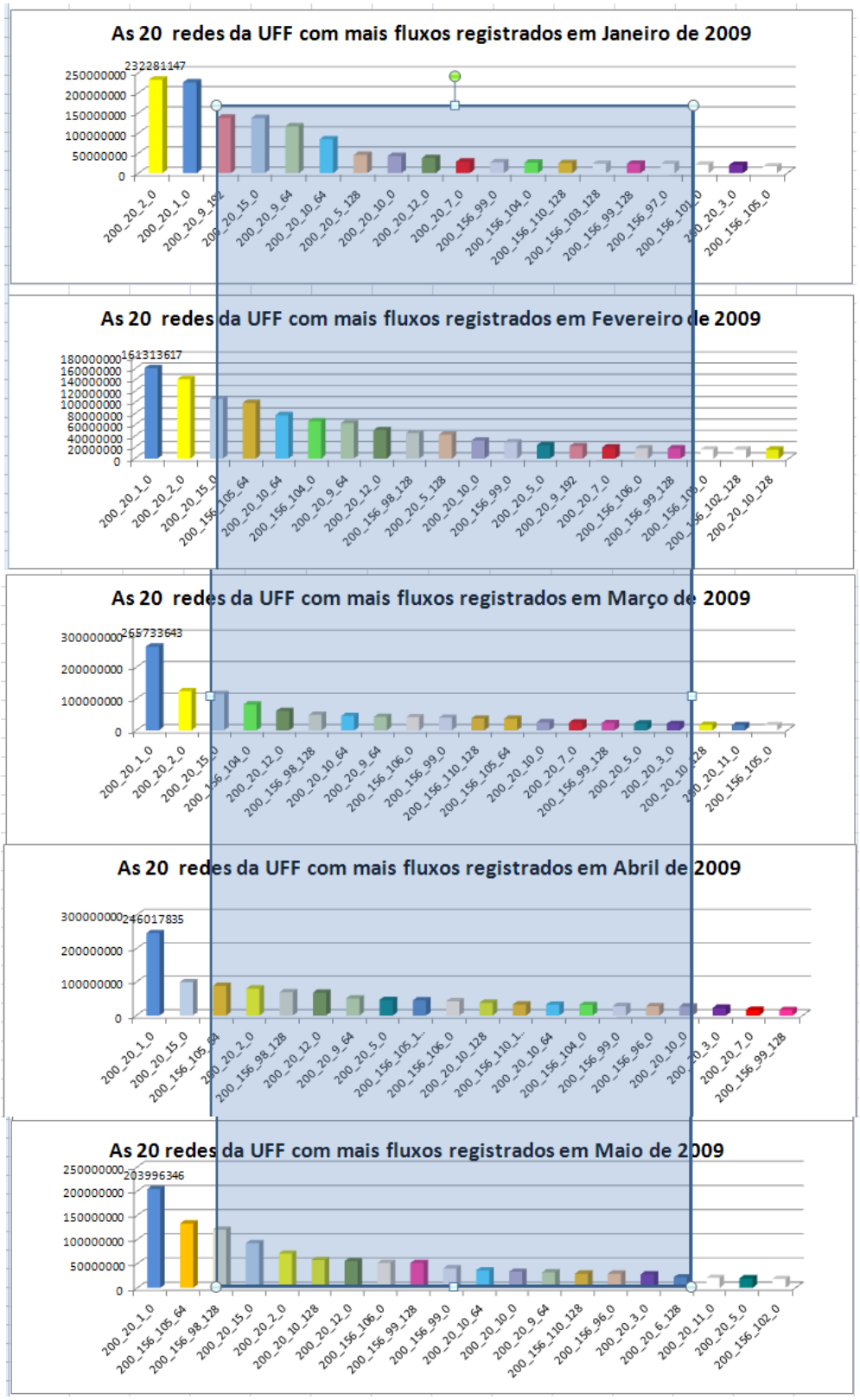


Figura IV-29 - Comparativo dos gráficos mensais das 20 redes da UFF com mais fluxos registrados entre Janeiro e Maio de 2009 – o detalhe mostra as posições com maior ocorrência de variações no ranking.

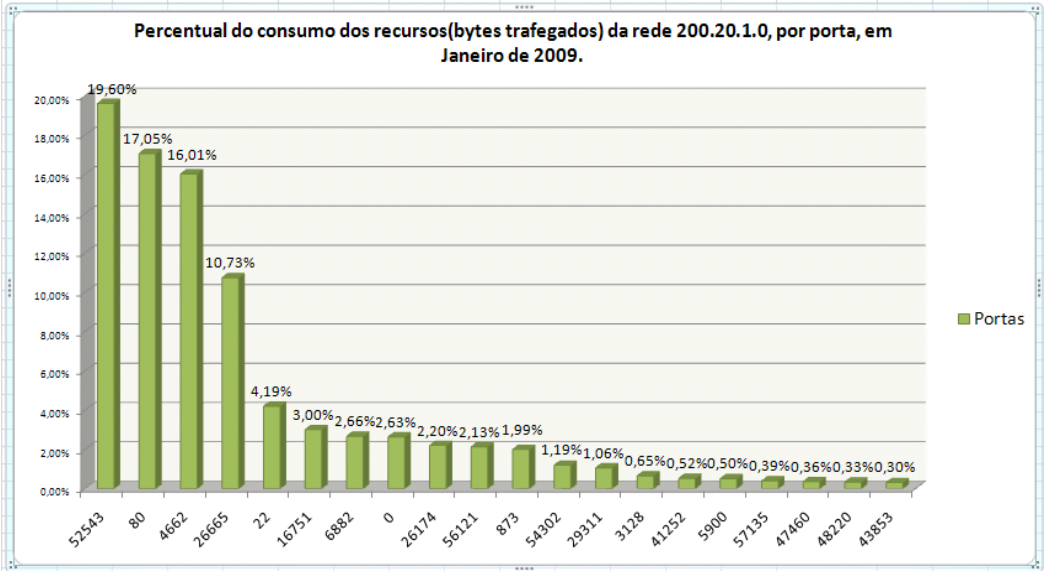


Figura IV-30 - Percentual de utilização das portas da rede 200.20.1.0 (bytes trafegados), em Janeiro de 2009. Total de bytes trafegados = 2.7 Tera bytes.

Demonstramos desta forma, que os dados colhidos pelo sistema de monitoramento de fluxos fornecem informações úteis para o gerenciamento de redes. O trafego de cada rede é consolidado a cada cinco minutos, gerando ao final do dia um conjunto de 288 arquivos (24 horas X 60 minutos / 5 minutos). Estes arquivos são armazenados em pastas hierarquicamente organizadas no formato **"rede/ano/mês/dia".** A partir destes arquivos foi possível obter com riqueza de detalhes as características individuais do funcionamento de cada rede, o PFR.

4.6 Obtendo o PFR da rede.

O PFR é obtido após um período de monitoramento da rede, concentrando-se em parâmetros como:

- Média de fluxos, bytes, pacotes.
- Relação de portas mais utilizadas.

Todos os resultados mostrados até agora contribuem para estabelecer o PFR de cada rede da UFF. Como exemplo, podemos citar a relação das 20 portas, mais utilizadas, no mês de janeiro para a rede 200.20.1.0 (Figura IV-20). Foi possível delimitar o universo das portas utilizadas pelas aplicações que consomem mais recursos da rede. Também foi possível extrair os dados estatísticos, Figura IV-16, através da contabilização dos sumários da atividade mensal da rede. E finalmente, foi possível comparar a atividade

dessa rede com as demais redes, através da composição de um ranking, Figura IV-28 e Figura IV-29, e acompanhar a variabilidade da posição da rede ao longo de cinco meses.

Para comprovar a utilidade do PFR, mostraremos ao final deste capítulo, no tópico sobre segurança, como foi possível configurar alertas a partir do monitoramento dos parâmetros do PFR.

O PFR de uma rede é determinado através da análise dos dados oriundos do funcionamento desta. Uma rede que possua 200 estações de trabalho, um servidor web e um servidor de e-mail e que pertença a uma metalúrgica, terá um PFR diferente de uma rede de mesma infra-estrutura, mas que pertença, por exemplo, a um curso de computação. As atividades e sistemas particulares de uma ou outra área de atuação terão influência direta nos resultados obtidos. É muito provável que os registros do monitoramento da metalúrgica revelem uma atividade de rede mais regular do que os registros da rede do curso de computação, pois nesta última, testes podem ser executados, provocando alterações repentinas e intensas na variedade de portas, quantidade de fluxos e bytes trafegados.

As pesquisas realizadas nos registros coletados com o programa Nfdump, através dos scripts, permitem gerar relatórios a partir de diversos campos do cabeçalho do TCP/IP. Por exemplo; o comando: ***nfdump –R /pasta_da_rede 'ip 200.20.2.206 and ip 200.20.7.30' –s port/flow***, mostrará todos dos acessos dos IPs 200.20.2.206 e 200.20.7.30, ordenados pelas portas que registraram a maior quantidade de fluxos. Já o comando: ***nfdump –R /rede-x/aquivo_data_hora_inicial:arquiv_.data_hora_final –c 100 ' port 40999',*** trará como resultado os 100 primeiros registros ocorridos entre à hora inicial e a hora final, revelando os hosts da rede-x, que neste período, utilizaram a porta 40999.

4.7 Perfil PROTOCOLOS

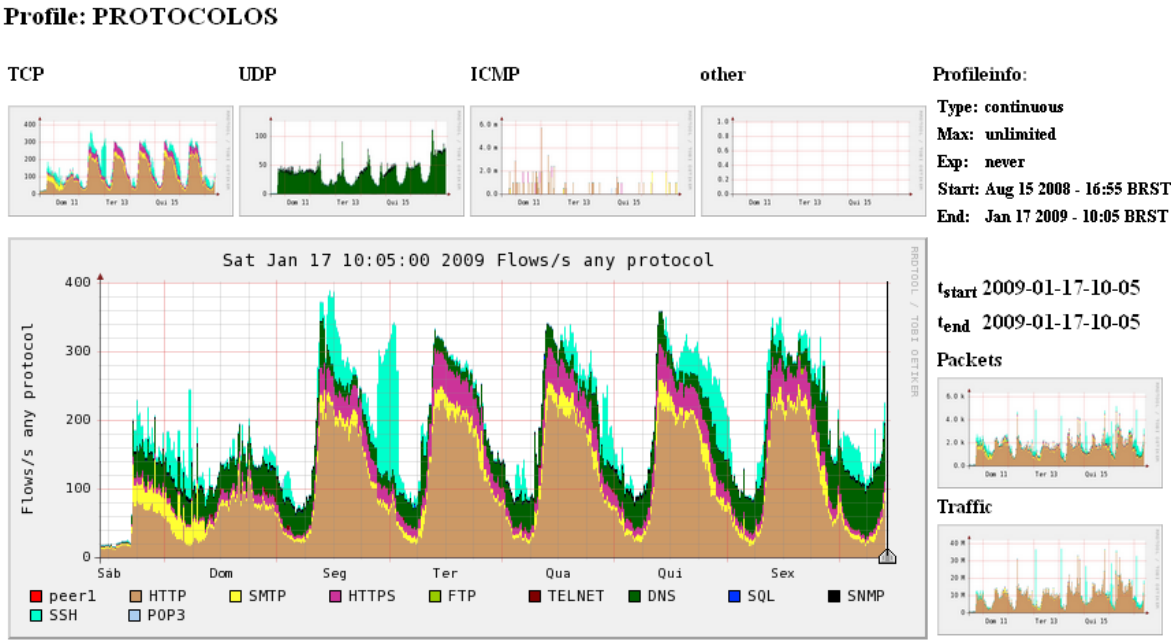
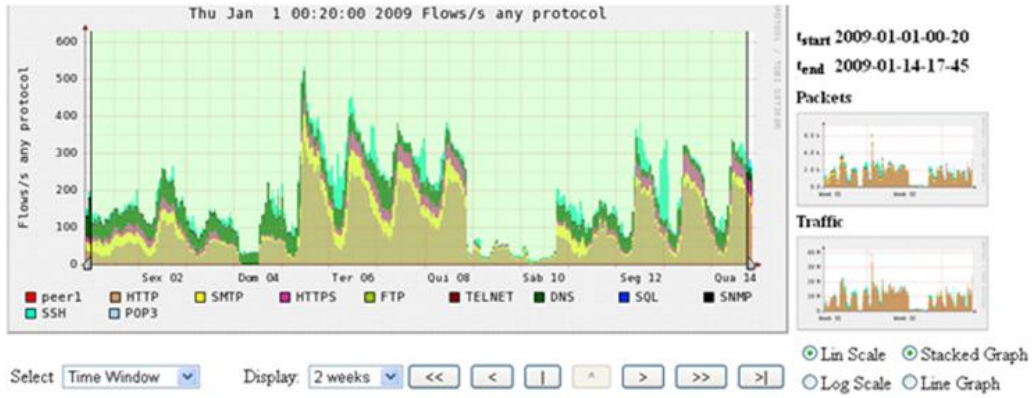


Figura IV-31 - Gráfico semanal do perfil PROTOCOLOS obtido em 17 de janeiro de 2009, referente aos dias compreendidos entre 10 e 17 de janeiro de 2009

O mesmo processo utilizado para a filtragem, armazenamento e processamento realizado no perfil RedesUFF foi aplicado aos dados que foram registrados a partir do perfil PROTOCOLOS. A diferença é que neste, todo o tráfego da UFF foi filtrado considerando apenas as portas: 80 (Web), 443 (HTTPS), 110 (POP3), 22 (SSH), 25 (SMTP), 23 (TELNET), 161 (SNMP) e a porta 53 (DNS). Foram registrados todos os fluxos que continham no cabeçalho do protocolo de transporte (TCP ou UDP), no campo destinado à porta de origem ou de destino, uma das portas acima descritas. A partir deste perfil foi possível conhecer a proporcionalidade do uso das aplicações clássicas da Internet na rede da UFF e observar diversas situações de alteração do PFR. A Figura IV-31, mostra um gráfico gerado utilizando o sistema Nfsen que representa uma semana de atividade da rede da UFF, sob a perspectiva do perfil protocolo. É possível observar que no início de cada dia ocorre a maior quantidade de fluxo. É possível observar também que com exceção da porta 22 (cor verde) as demais portas apresentam um padrão de repetição diário. Veremos no capítulo sobre segurança que, em muitas situações onde o PFR foi alterado de maneira repentina, foram detectados um ou mais hosts, internos ou externos, cuja segurança havia sido comprometida por

hackers ou por vírus e outras vezes o comportamento sugeria utilização de aplicativos do tipo Peer-to-Peer.



Statistics timeslot Jan 01 2009 - 00:20 - Jan 14 2009 - 17:45

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
POP3	613.0 k	608.8 k	4.1 k	1.0	0	11.4 M	11.3 M	6.5 k	1.0	0	7.5 GB	7.5 GB	1.0 MB	46.0 B	0 B
SSH	20.4 M	20.4 M	10.1 k	2.0	0	191.7 M	191.1 M	509.9 k	2.0	0	88.0 GB	87.9 GB	24.6 MB	92.0 B	0 B
SNMP	3.1 M	135.0	3.1 M	0	0	6.2 M	141.0	6.2 M	0	0	476.3 MB	8.2 kB	476.3 MB	0 B	0 B
SQL	117.0 k	114.1 k	2.9 k	2.0	0	918.1 k	914.6 k	3.5 k	2.0	0	327.6 MB	327.2 MB	378.1 kB	92.0 B	0 B
DNS	42.0 M	136.2 k	41.9 M	0	0	49.3 M	329.5 k	49.0 M	0	0	6.4 GB	21.0 MB	6.4 GB	0 B	0 B
TELNET	438.5 k	434.5 k	4.0 k	0	0	1.2 M	1.1 M	4.5 k	0	0	149.9 MB	149.4 MB	533.6 kB	0 B	0 B
FTP	31.0 k	27.8 k	3.3 k	0	0	454.1 k	450.3 k	3.8 k	0	0	315.1 MB	314.7 MB	416.5 kB	0 B	0 B
HTTPS	23.1 M	23.0 M	25.8 k	30.0	0	90.3 M	90.3 M	27.8 k	30.0	0	28.9 GB	28.8 GB	3.7 MB	1.4 kB	0 B
SMTP	23.2 M	23.2 M	6.9 k	56.0	0	155.7 M	155.7 M	10.6 k	99.0	0	49.4 GB	49.4 GB	1.5 MB	4.6 kB	0 B
HTTP	108.8 M	108.6 M	174.8 k	346.0	0	1.6 G	1.6 G	431.9 k	402.0	0	1.3 TB	1.3 TB	67.6 MB	18.5 kB	0 B
peer1	0	0	0	0	0	0	0	0	0	0	0 B	0 B	0 B	0 B	0 B

All None Display: Sum Rate

Figura IV-32 - Seleção de Intervalo de tempo (de 01 a 14 de Janeiro) utilizando o sistema Nfsen com a opção "*Sum*" habilitada.

A Figura IV-32 apresenta uma das funcionalidades do sistema Nfsen. A partir da seleção do gráfico (foi selecionado todo o gráfico), através da opção de soma (botão *Sum* marcado abaixo da tabela) foi possível obter a totalização do volume trafegado em FLUXOS, PACOTES E TRÁFEGO, para cada uma das portas que foram configuradas no filtro do perfil. Este recurso é muito útil, pois os cálculos são obtidos automaticamente.

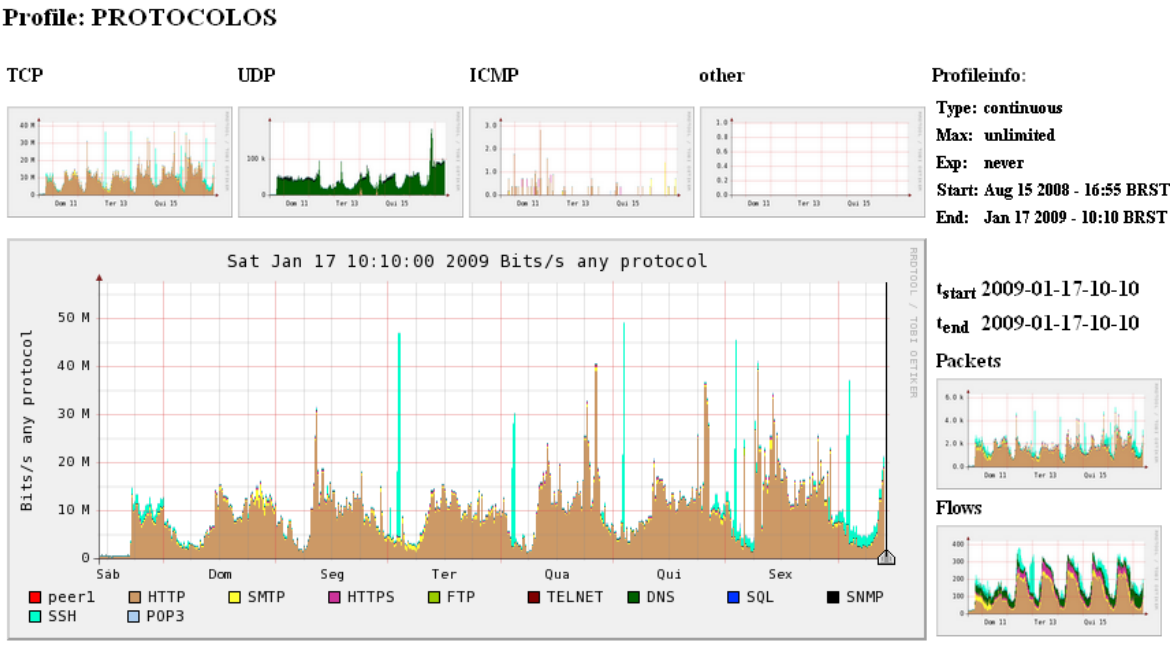


Figura IV-33 - Gráfico semanal do Perfil PROTOCOLOS. Bits por segundo trafegados por protocolo, referente aos dias compreendidos entre 10 e 17 de janeiro de 2009.

A Figura IV-33, representa a quantidade de bit/s para cada porta filtrada pelo perfil. Nota-se, neste caso, que ocorrem picos regulares de tráfego na porta 22 (SSH), iniciando na madrugada de segunda-feira que se repete regulamente a cada dia da semana, até a madrugada de sexta-feira. Ao analisar situações como esta, deve-se buscar, por exemplo:

- conhecer a natureza da demanda, ou seja, se a mesma constitui uma atividade lícita e de interesse institucional;
- mensurar o impacto da demanda no contexto geral da rede;
- conhecer a taxa de crescimento da demanda.

Para isso, a tecnologia de monitoramento de fluxos oferece amplo suporte, pois permite fazer contabilizações considerando origens, destinos, protocolos e portas.

Da Figura IV-34 até a Figura IV-41, são computadas as informações sobre totais de fluxo e bytes, a cada mês. No mês de março é possível observar uma redução no registro de praticamente todas as portas monitoradas, com exceção da portas 80 (WEB), 443 (WEB Seguro) e 161 (SNMP Gerenciamento de rede), novamente isso configura uma situação onde se faz necessário investigar, pois pode significar a utilização de um

protocolo para transportar conteúdo de aplicações bloqueadas na rede de modo disfarçado [25].

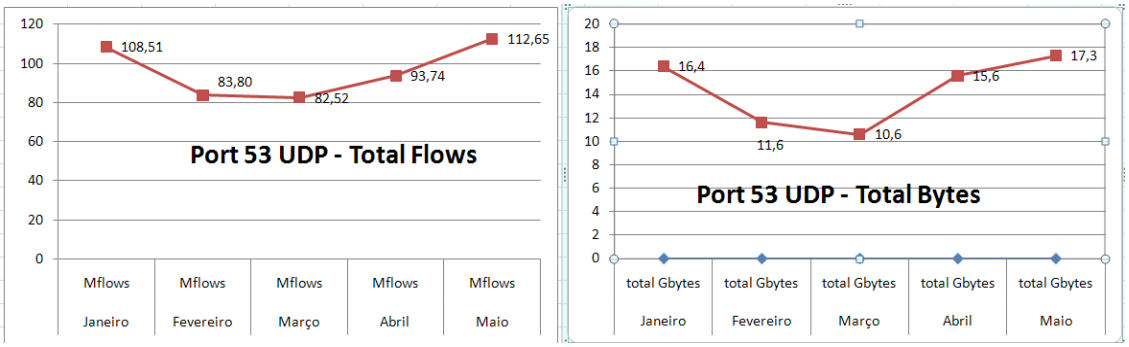


Figura IV-34 - Gráficos de utilização da porta 53 (DNS) do protocolo UDP entre janeiro e maio de 2009. Fluxos e Bytes.

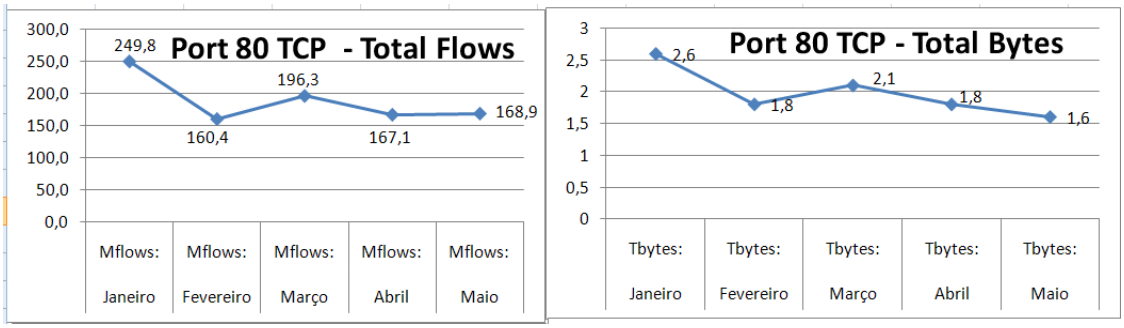


Figura IV-35 - Gráficos de utilização da porta 80 (WEB) do protocolo TCP entre janeiro e maio de 2009. Fluxos e Bytes.

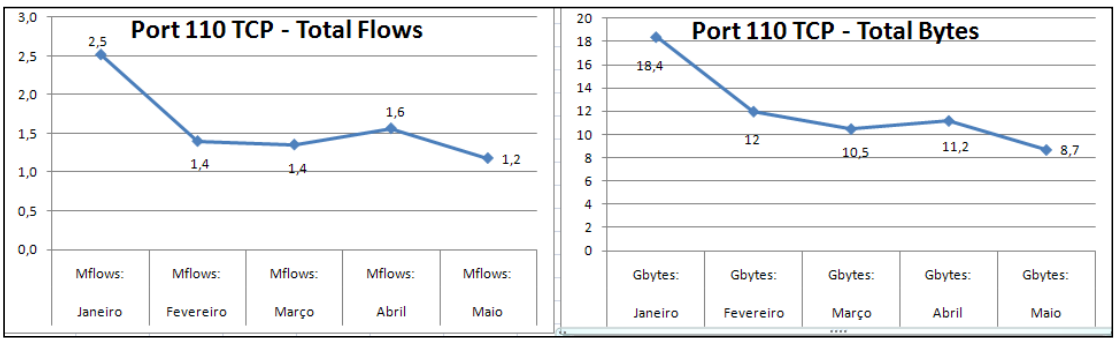


Figura IV-36 - Gráficos de utilização da porta 110 (POP3) do protocolo TCP entre janeiro e maio de 2009. Fluxos e Bytes.

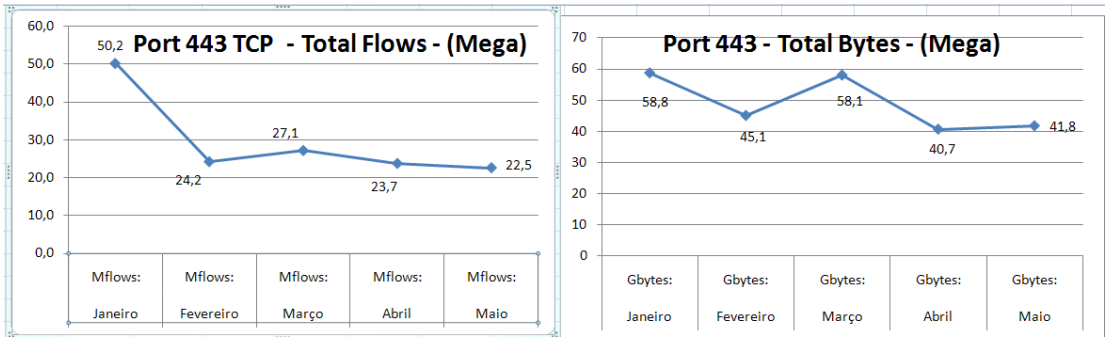


Figura IV-37 - Gráficos de utilização da porta 443 (HTTPS) do protocolo TCP entre janeiro e maio de 2009. Fluxos e Bytes.

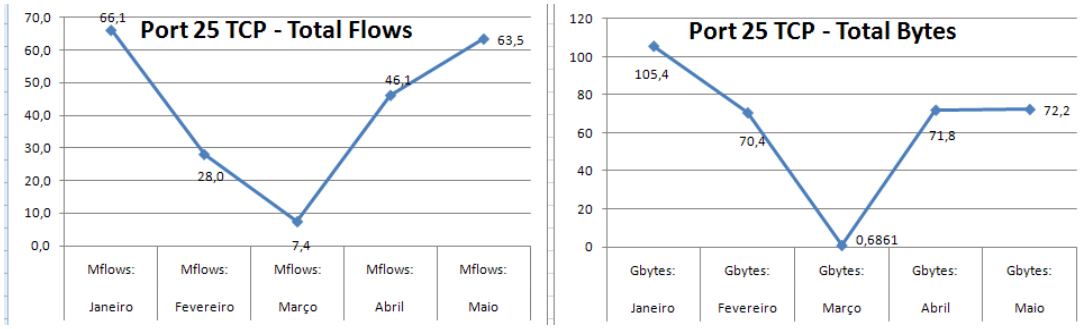


Figura IV-38 - Gráficos de utilização da porta 25 (SMTP) do protocolo TCP entre janeiro e maio de 2009. Fluxos e Bytes.

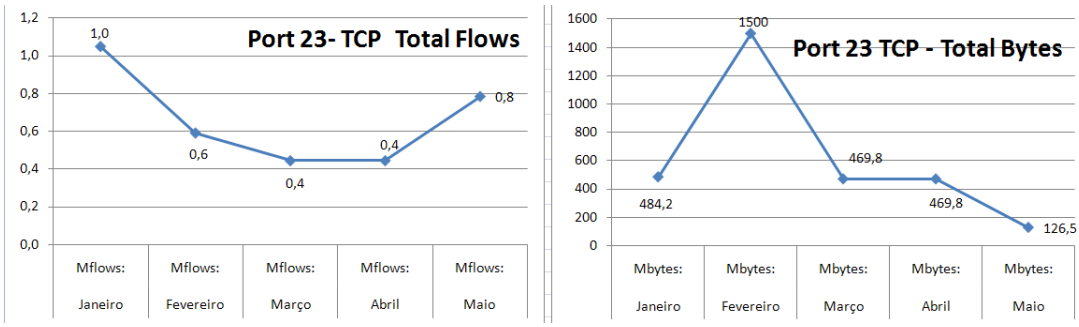


Figura IV-39 - Gráficos de utilização da porta 23 (Telnet) do protocolo TCP entre janeiro e maio de 2009. Fluxos e Bytes.

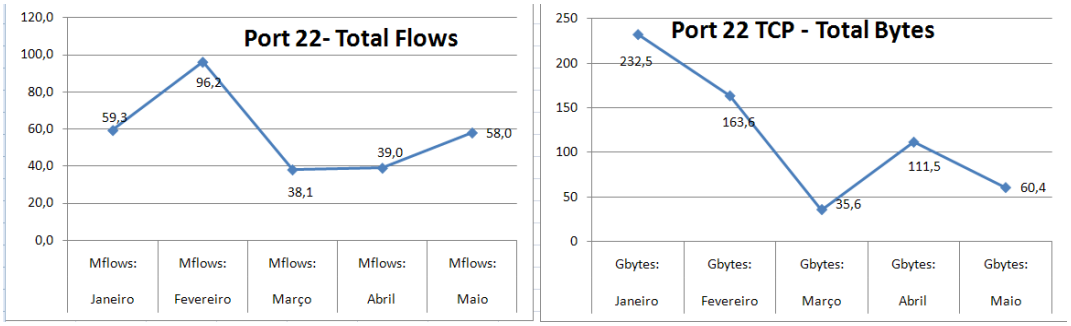


Figura IV-40 - Gráficos de utilização da porta 22(SSH) do protocolo TCP entre janeiro e maio de 2009. Fluxos e Bytes.

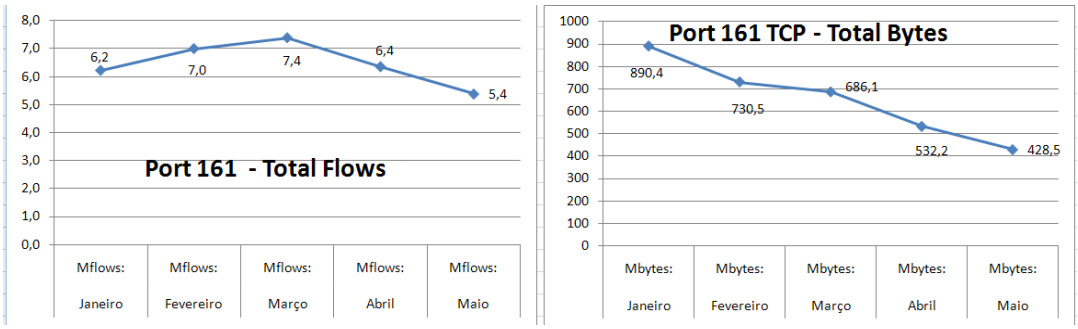


Figura IV-41 - Gráficos de utilização da porta 161(IGMP) do protocolo TCP entre janeiro e maio de 2009. Fluxos e Bytes.

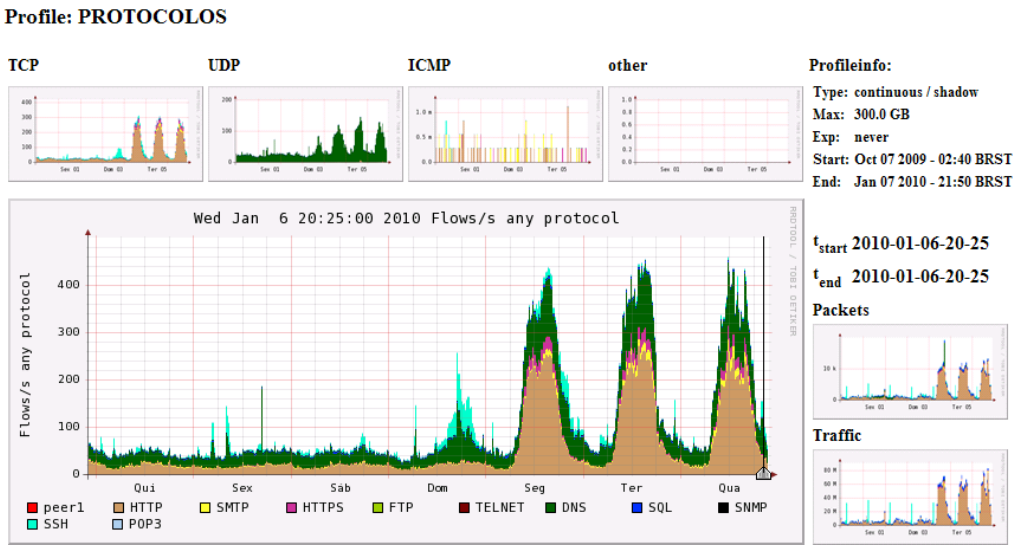


Figura IV-42 - Gráfico demonstrativo do comportamento da rede na noite de ano novo do ano de 2009 para 2010 (dia 31 na quinta-feira), sendo possível observar a baixa utilização dos recursos da rede da UFF até o domingo. A partir de segunda-feira ocorre a retomada demanda de uso cotidiano da rede da universidade.

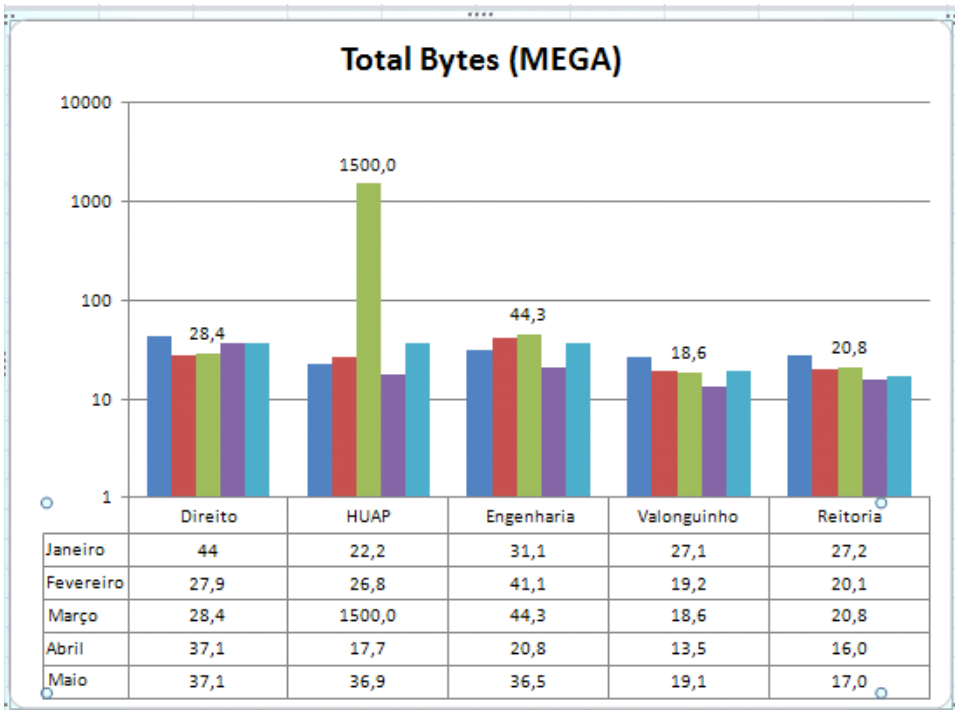
4.8 Perfil Anel UFF

O perfil Anel UFF, buscou acompanhar a atividade de rede dos switches do Anel principal da UFF. Como descrito no capítulo 2, o chamado Anel Ótico da UFF é formado por 7 switches localizados nos seguintes campi:

- Campus da Praia Vermelha;
- Campus HUAP;
- Campus do Valonguinho;
- Campus do Gragoata;
- Faculdade de Direito;
- Escola de Enfermagem; e
- Reitoria.

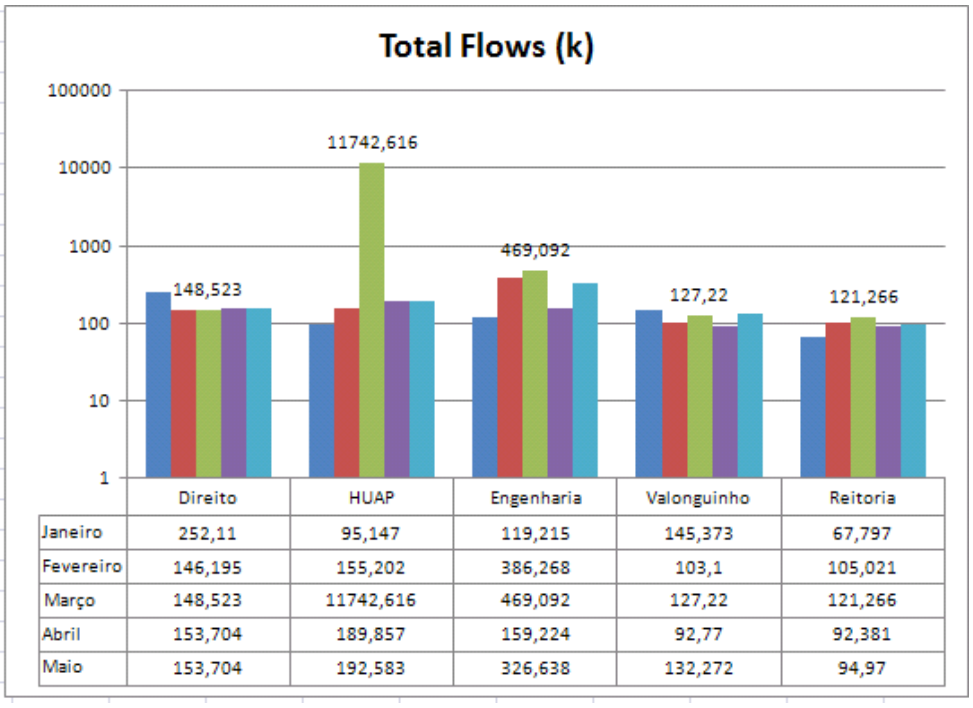
O filtro do perfil foi constituído do endereço IP de cada switch. Qualquer pacote transmitido ou recebido por estes endereços foram registrados nos arquivos armazenados pelo NFdump e grafados pelo Nfsen. A atividade dos switches do Anel apresenta um PFR com baixos índices de fluxos, bytes e pacotes. Observa-se basicamente os protocolos IGMP (Internet Group Management Protocol) [26], ICMP, SNMP, uma vez que se trata de uma rede de serviço, entretanto, como veremos mais adiante, uma brusca alteração no PFR do switch do campus HUAP revelou uma utilização anômala.

Os gráficos do perfil Anel UFF (Figura IV-43, Figura IV-44 e Figura IV-45) apresentaram grande homogeneidade, com exceção dos resultados obtidos do mês de março no Switch do campus HUAP. Ao consultar o sistema Nfsen buscando saber o motivo de tal elevação, identificamos registros que mostram a transferência de 1.4 Gbytes partindo do endereço IP atribuído ao Switch do HUAP e dois endereços IPs (200.20.1.167 e 200.20.1.234) (Figura IV-46), pertencentes ao Núcleo de Tecnologia da UFF. Acreditamos que a causa possa ter origem em operações de manutenção como, por exemplo, backup ou mesmo um teste de desempenho.



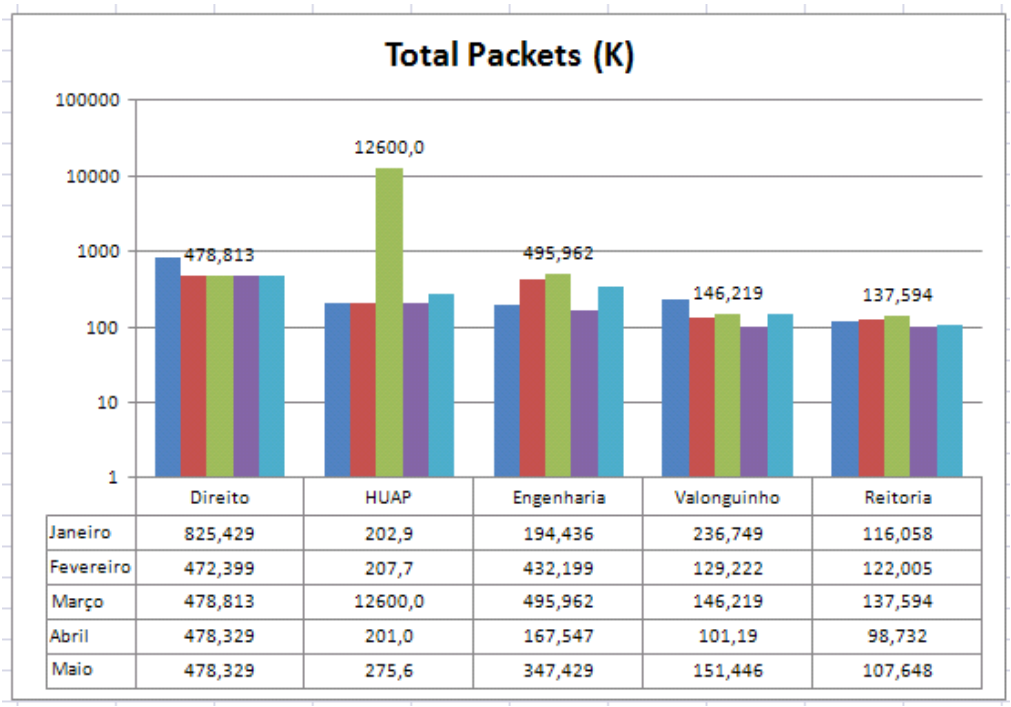
	Direito	HUAP	Engenharia	Valonguinho	Reitoria
Janeiro	44	22,2	31,1	27,1	27,2
Fevereiro	27,9	26,8	41,1	19,2	20,1
Março	28,4	1500,0	44,3	18,6	20,8
Abril	37,1	17,7	20,8	13,5	16,0
Maio	37,1	36,9	36,5	19,1	17,0

Figura IV-43 - Gráfico mensal da atividade de rede dos switches do Anel ótico da Rede UFF registrada entre janeiro e maio de 2009. Total de bytes trafegados.



	Direito	HUAP	Engenharia	Valonguinho	Reitoria
Janeiro	252,11	95,147	119,215	145,373	67,797
Fevereiro	146,195	155,202	386,268	103,1	105,021
Março	148,523	11742,616	469,092	127,22	121,266
Abril	153,704	189,857	159,224	92,77	92,381
Maio	153,704	192,583	326,638	132,272	94,97

Figura IV-44 - Perfil Anel UFF - Total de fluxos – janeiro a maio de 2009.



	Direito	HUAP	Engenharia	Valonguinho	Reitoria
Janeiro	825,429	202,9	194,436	236,749	116,058
Fevereiro	472,399	207,7	432,199	129,222	122,005
Março	478,813	12600,0	495,962	146,219	137,594
Abril	478,329	201,0	167,547	101,19	98,732
Maio	478,329	275,6	347,429	151,446	107,648

Figura IV-45 - Perfil Anel UFF - Total de pacotes – janeiro a maio de 2009.

```
Top 10     IP Addr ordered by flows:
Date first seen          Duration Proto          IP Addr    Flows  Packets    Bytes      pps      bps   bpp
2009-03-10 20:50:05.995 4466558.491 any       200.20.0.134   10.0 M   11.4 M    1.4 G        2     2668   124
2009-03-10 20:50:14.956 4349681.328 any       200.20.1.167    5.5 M    6.2 M  773.5 M        1     1491   125
2009-03-10 20:50:14.946 4349681.329 any       200.20.1.234    4.5 M    5.2 M  646.1 M        1     1246   125
2009-03-10 20:50:14.958 4331232.328 any       200.20.0.129     2653     3091   472923        0        0   153
2009-03-10 20:50:05.995 172481.003 any          224.0.0.9     2540     2540   438080        0       20   172
2009-03-10 20:51:24.992 4327725.283 any       200.20.1.50      1205     1363   114492        0        0    84
2009-03-10 22:45:59.976 4383813.313 any    118.161.243.168      531      542    30352        0        0    56
2009-03-10 20:52:52.989 4466329.303 any      146.164.48.5       225      225    17100        0        0    76
2009-03-10 20:52:47.995 172081.996 any    200.159.254.173      215      215    14340        0        0    66
2009-03-11 06:43:42.983 53222.006 any      69.64.145.225       165      165    11535        0        1    69

Summary: total flows: 10504465, total bytes: 1.4 G, total packets: 11.4 M, avg bps: 2668, avg pps: 2, avg bpp: 124
Time window: 2009-03-10 20:50:05 - 2009-05-01 13:32:44
Total flows processed: 10504465, Records skipped: 0, Bytes read: 546245860
Sys: 1.867s flows/second: 5624233.4   Wall: 2.349s flows/second: 4470531.1
```

Figura IV-46 - Consulta detalhada para identificar a alteração do PFR no Switch do campus HUAP.

4.9 Perfil Live

O perfil Live é o principal, sendo essencial para o funcionamento do sistema do sistema Nfsen/Nfdump. Os dados coletados e armazenados neste perfil permitiram a totalização de todos os fluxos, bytes e pacotes da rede da UFF, de uma forma abrangente. Também foi possível validar as informações de taxa de transferência mediante comparações com as mesmas informações registradas no sistema Cacti. Lembrando que o Cacti opera em conformidade com protocolo SNMP, obtendo as informações diretamente das interfaces

de rede dos switches[1], tais informações, portanto, podem ser bastante precisas. Por outro lado, o Nfsen faz estimativas em função dos valores presentes no cabeçalho do protocolo TCP/IP. A partir das comparações entre os dois sistemas foi possível detectar divergências e fazer os ajustes nos parâmetros do Softflowd, de modo a obter dados mais próximos da realidade, sabendo, entretanto, que igualar o resultado apresentado pelos sistemas não seria possível, considerando as diferentes metodologias de medição utilizadas por um e outro sistema.

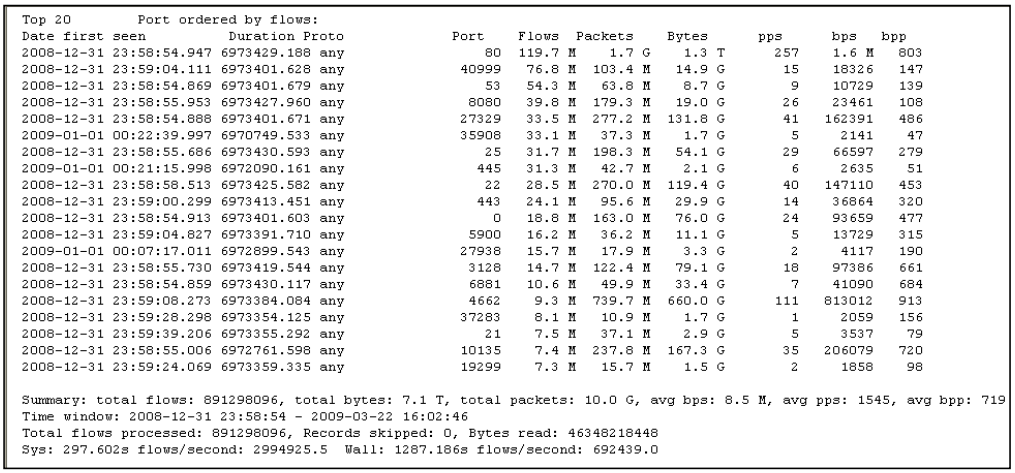
Não foram observadas nos gráficos deste perfil, alterações que levassem à identificação de anomalias no funcionamento da rede, devido à grande concentração de fluxos.

Os relatórios das vinte portas com maior quantidade de fluxos registrados, contidas nas figuras compreendidas entreFigura IV-47 atéFigura IV-50 e permitem realizar análises sobre as aplicações mais utilizadas. As vinte portas foram escolhidas forma empírica, objetivando encontrar neste universo as informações mais significativas para a análise do uso da rede. A partir da quantidade de fluxos, bytes e pacotes é possível avaliar a importância do uso dessas aplicações na rede. Ao identificar as máquinas internas que estão utilizando cada porta, pode-se descobrir a aplicação. O mapeamento de portas, versus aplicações, favorece aos administradores da rede o controle do tráfego, separando as atividades legítimas dos vírus e hackers, que objetivam causar danos e obter vantagens das pessoas e instituições. Do contrário, caso seja observada perda de desempenho da rede e não seja possível identificar onde os recursos estão sendo consumidos, é provável que se decida aumentar a oferta. No entanto, no caso de aplicações maliciosas, quanto mais recursos forem oferecidos, mais serão consumidos: é a chamada geração da procura pela oferta. Quanto mais recursos forem ofertados, mais recursos serão consumidos e esta situação favorece os agentes maliciosos.

Na Figura IV-47, é possível observar que em janeiro, a porta 40999 ficou em segundo lugar na relação das portas com a maior quantidade de fluxos, perdendo apenas para a porta 80 (Web). Esta porta foi responsável por colocar a rede 200.20.2.0 em primeiro

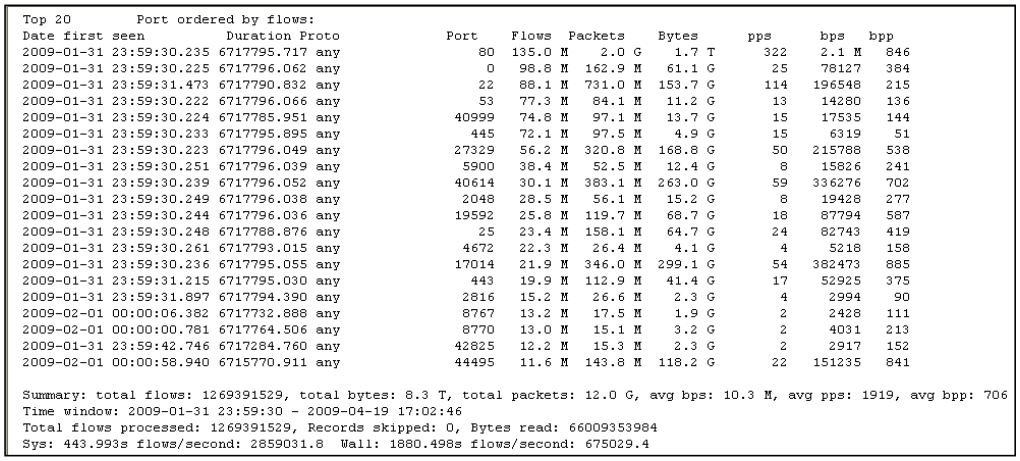
[1] Conforme informações contidas no apêndice 1

lugar no ranking das redes mais ativas no mesmo mês. Diante dessas informações, considera-se de suma importância saber que aplicações estão associadas a que portas e quais são de interesse da instituição, uma vez que os dados estatísticos mostram que elas ocupam uma posição de significância. Como exemplo, podemos citar a porta 27015, que ficou em décimo primeiro lugar no mês de abril (Figura IV-50) e foi identificada em sites na Internet como uma das portas utilizadas pelo programa *Half Life* no qual se baseiam diversos jogos online, como por exemplo, o famoso *Counter Strike*.



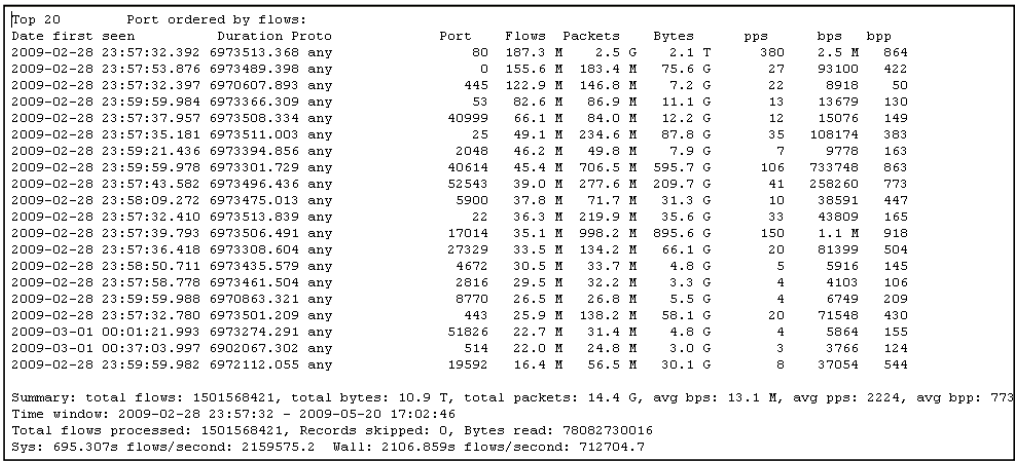
```
Top 20        Port ordered by flows:
Date first seen          Duration Proto             Port    Flows  Packets    Bytes      pps      bps   bpp
2008-12-31 23:58:54.947 6973429.188 any               80  119.7 M    1.7 G    1.3 T      257    1.6 M   803
2008-12-31 23:59:04.111 6973401.628 any            40999   76.8 M  103.4 M   14.9 G       15    18326   147
2008-12-31 23:58:54.869 6973401.679 any               53   54.3 M   63.8 M    8.7 G        9    10729   139
2008-12-31 23:58:55.953 6973427.960 any             8080   39.8 M  179.3 M   19.0 G       26    23461   108
2008-12-31 23:58:54.888 6973401.671 any            27329   33.5 M  277.2 M  131.8 G       41   162391   486
2009-01-01 00:22:39.997 6970749.533 any            35908   33.1 M   37.3 M    1.7 G        5     2141    47
2008-12-31 23:58:55.686 6973430.593 any               25   31.7 M  198.3 M   54.1 G       29    66597   279
2009-01-01 00:21:15.998 6972090.161 any              445   31.3 M   42.7 M    2.1 G        6     2635    51
2008-12-31 23:58:58.513 6973425.582 any               22   28.5 M  270.0 M  119.4 G       40   147110   453
2008-12-31 23:59:00.299 6973413.451 any              443   24.1 M   95.6 M   29.9 G       14    36864   320
2008-12-31 23:58:54.913 6973401.603 any                0   18.8 M  163.0 M   76.0 G       24    93659   477
2008-12-31 23:59:04.827 6973391.710 any             5900   16.2 M   36.2 M   11.1 G        5    13729   315
2009-01-01 00:07:17.011 6972899.543 any            27938   15.7 M   17.9 M    3.3 G        2     4117   190
2008-12-31 23:58:55.730 6973419.544 any             3128   14.7 M  122.4 M   79.1 G       18    97386   661
2008-12-31 23:58:54.859 6973430.117 any             6881   10.6 M   49.9 M   33.4 G        7    41090   684
2008-12-31 23:59:08.273 6973384.084 any             4662    9.3 M  739.7 M  660.0 G      111   813012   913
2008-12-31 23:59:28.298 6973354.125 any            37283    8.1 M   10.9 M    1.7 G        1     2059   156
2008-12-31 23:59:39.206 6973355.292 any               21    7.5 M   37.1 M    2.9 G        5     3537    79
2008-12-31 23:58:55.006 6972761.598 any            10135    7.4 M  237.8 M  167.3 G       35   206079   720
2008-12-31 23:59:24.069 6973359.335 any            19299    7.3 M   15.7 M    1.5 G        2     1858    98

Summary: total flows: 891298096, total bytes: 7.1 T, total packets: 10.0 G, avg bps: 8.5 M, avg pps: 1545, avg bpp: 719
Time window: 2008-12-31 23:58:54 - 2009-03-22 16:02:46
Total flows processed: 891298096, Records skipped: 0, Bytes read: 46348218448
Sys: 297.602s flows/second: 2994925.5   Wall: 1287.186s flows/second: 692439.0
```

Figura IV-47 - Relação das 20 portas ordenadas pela quantidade de fluxos – janeiro 2009



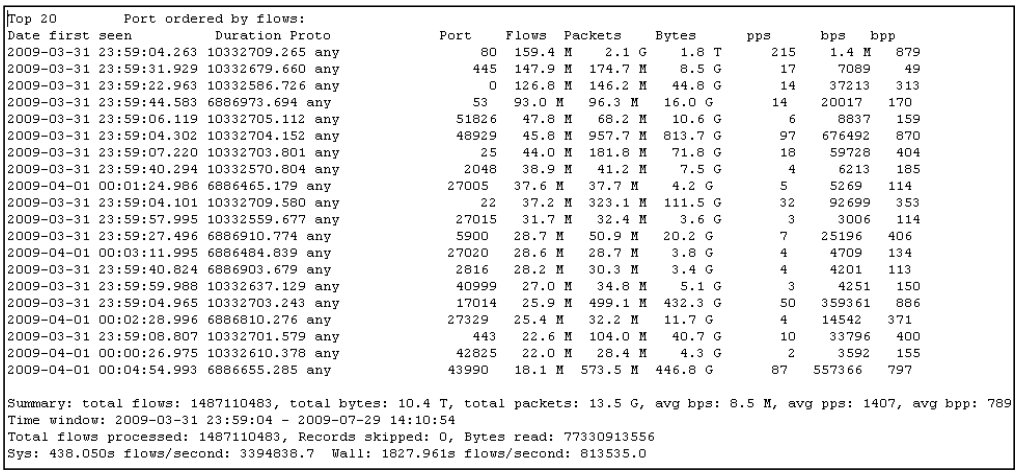
```
Top 20        Port ordered by flows:
Date first seen          Duration Proto             Port    Flows  Packets    Bytes      pps      bps   bpp
2009-01-31 23:59:30.235 6717795.717 any               80  135.0 M    2.0 G    1.7 T      322    2.1 M   846
2009-01-31 23:59:30.225 6717796.062 any                0   98.8 M  162.9 M   61.1 G       25    78127   384
2009-01-31 23:59:31.473 6717790.832 any               22   88.1 M  731.0 M  153.7 G      114   196548   215
2009-01-31 23:59:30.222 6717796.066 any               53   77.3 M   84.1 M   11.2 G       13    14280   136
2009-01-31 23:59:30.224 6717785.951 any            40999   74.8 M   97.1 M   13.7 G       15    17535   144
2009-01-31 23:59:30.233 6717795.895 any              445   72.1 M   97.5 M    4.9 G       15     6319    51
2009-01-31 23:59:30.223 6717796.049 any            27329   56.2 M  320.8 M  168.8 G       50   215788   538
2009-01-31 23:59:30.251 6717796.039 any             5900   38.4 M   52.5 M   12.4 G        8    15826   241
2009-01-31 23:59:30.239 6717796.052 any            40614   30.1 M  383.1 M  263.0 G       59   336276   702
2009-01-31 23:59:30.249 6717796.038 any             2048   28.5 M   56.1 M   15.2 G        8    19428   277
2009-01-31 23:59:30.244 6717796.036 any            19592   25.8 M  119.7 M   68.7 G       18    87794   587
2009-01-31 23:59:30.248 6717788.876 any               25   23.4 M  158.1 M   64.7 G       24    82743   419
2009-01-31 23:59:30.261 6717793.015 any             4672   22.3 M   26.4 M    4.1 G        4     5218   158
2009-01-31 23:59:30.236 6717795.055 any            17014   21.9 M  346.0 M  299.1 G       54   382473   885
2009-01-31 23:59:31.215 6717795.030 any              443   19.9 M  112.9 M   41.4 G       17    52925   375
2009-01-31 23:59:31.897 6717794.390 any             2816   15.2 M   26.6 M    2.3 G        4     2994    90
2009-02-01 00:00:06.382 6717732.888 any             8767   13.2 M   17.5 M    1.9 G        2     2428   111
2009-02-01 00:00:00.781 6717764.506 any             8770   13.0 M   15.1 M    3.2 G        2     4031   213
2009-01-31 23:59:42.746 6717284.760 any            42825   12.2 M   15.3 M    2.3 G        2     2917   152
2009-02-01 00:00:58.940 6715770.911 any            44495   11.6 M  143.8 M  118.2 G       22   151235   841

Summary: total flows: 1269391529, total bytes: 8.3 T, total packets: 12.0 G, avg bps: 10.3 M, avg pps: 1919, avg bpp: 706
Time window: 2009-01-31 23:59:30 - 2009-04-19 17:02:46
Total flows processed: 1269391529, Records skipped: 0, Bytes read: 66009353984
Sys: 443.993s flows/second: 2859031.8   Wall: 1880.498s flows/second: 675029.4
```

Figura IV-48 - Relação das 20 portas ordenadas pela quantidade de fluxos – fevereiro 2009.



```
Top 20        Port ordered by flows:
Date first seen          Duration Proto             Port    Flows  Packets    Bytes      pps      bps   bpp
2009-02-28 23:57:32.392 6973513.368 any              80  187.3 M    2.5 G    2.1 T      380    2.5 M   864
2009-02-28 23:57:53.876 6973489.398 any               0  155.6 M  183.4 M   75.6 G       27    93100   422
2009-02-28 23:57:32.397 6970607.893 any             445  122.9 M  146.8 M    7.2 G       22     8918    50
2009-02-28 23:59:59.984 6973366.309 any              53   82.6 M   86.9 M   11.1 G       13    13679   130
2009-02-28 23:57:37.957 6973508.334 any           40999   66.1 M   84.0 M   12.2 G       12    15076   149
2009-02-28 23:57:35.181 6973511.003 any              25   49.1 M  234.6 M   87.8 G       35   108174   383
2009-02-28 23:59:21.436 6973394.856 any            2048   46.2 M   49.8 M    7.9 G        7     9778   163
2009-02-28 23:59:59.978 6973301.729 any           40614   45.4 M  706.5 M  595.7 G      106   733748   863
2009-02-28 23:57:43.582 6973496.436 any           52543   39.0 M  277.6 M  209.7 G       41   258260   773
2009-02-28 23:58:09.272 6973475.013 any            5900   37.8 M   71.7 M   31.3 G       10    38591   447
2009-02-28 23:57:32.410 6973513.839 any              22   36.3 M  219.9 M   35.6 G       33    43809   165
2009-02-28 23:57:39.793 6973506.491 any           17014   35.1 M  998.2 M  895.6 G      150     1.1 M   918
2009-02-28 23:57:36.418 6973308.604 any           27329   33.5 M  134.2 M   66.1 G       20    81399   504
2009-02-28 23:58:50.711 6973435.579 any            4672   30.5 M   33.7 M    4.8 G        5     5916   145
2009-02-28 23:57:58.778 6973461.504 any            2816   29.5 M   32.2 M    3.3 G        4     4103   106
2009-02-28 23:59:59.988 6970863.321 any            8770   26.5 M   26.8 M    5.5 G        4     6749   209
2009-02-28 23:57:32.780 6973501.209 any             443   25.9 M  138.2 M   58.1 G       20    71548   430
2009-03-01 00:01:21.993 6973274.291 any           51826   22.7 M   31.4 M    4.8 G        4     5864   155
2009-03-01 00:37:03.997 6902067.302 any             514   22.0 M   24.8 M    3.0 G        3     3766   124
2009-02-28 23:59:59.982 6972112.055 any           19592   16.4 M   56.5 M   30.1 G        8    37054   544

Summary: total flows: 1501568421, total bytes: 10.9 T, total packets: 14.4 G, avg bps: 13.1 M, avg pps: 2224, avg bpp: 773
Time window: 2009-02-28 23:57:32 - 2009-05-20 17:02:46
Total flows processed: 1501568421, Records skipped: 0, Bytes read: 78082730016
Sys: 695.307s flows/second: 2159575.2  Wall: 2106.859s flows/second: 712704.7
```

Figura IV-49 - Relação das 20 portas ordenadas pela quantidade de fluxos – março 2009.



```
Top 20        Port ordered by flows:
Date first seen          Duration Proto             Port    Flows  Packets    Bytes      pps      bps   bpp
2009-03-31 23:59:04.263 10332709.265 any              80  159.4 M    2.1 G    1.8 T      215    1.4 M   879
2009-03-31 23:59:31.929 10332679.660 any             445  147.9 M  174.7 M    8.5 G       17     7089    49
2009-03-31 23:59:22.963 10332586.726 any               0  126.8 M  146.2 M   44.8 G       14    37213   313
2009-03-31 23:59:44.583 6886973.694 any               53   93.0 M   96.3 M   16.0 G       14    20017   170
2009-03-31 23:59:06.119 10332705.112 any           51826   47.8 M   68.2 M   10.6 G        6     8837   159
2009-03-31 23:59:04.302 10332704.152 any           48929   45.8 M  957.7 M  813.7 G       97   676492   870
2009-03-31 23:59:07.220 10332703.801 any              25   44.0 M  181.8 M   71.8 G       18    59728   404
2009-03-31 23:59:40.294 10332570.804 any            2048   38.9 M   41.2 M    7.5 G        4     6213   185
2009-04-01 00:01:24.986 6886465.179 any            27005   37.6 M   37.7 M    4.2 G        5     5269   114
2009-03-31 23:59:04.101 10332709.580 any              22   37.2 M  323.1 M  111.5 G       32    92699   353
2009-03-31 23:59:57.995 10332559.677 any           27015   31.7 M   32.4 M    3.6 G        3     3006   114
2009-03-31 23:59:27.496 6886910.774 any             5900   28.7 M   50.9 M   20.2 G        7    25196   406
2009-04-01 00:03:11.995 6886484.839 any            27020   28.6 M   28.7 M    3.8 G        4     4709   134
2009-03-31 23:59:40.824 6886903.679 any             2816   28.2 M   30.3 M    3.4 G        4     4201   113
2009-03-31 23:59:59.988 10332637.129 any           40999   27.0 M   34.8 M    5.1 G        3     4251   150
2009-03-31 23:59:04.965 10332703.243 any           17014   25.9 M  499.1 M  432.3 G       50   359361   886
2009-04-01 00:02:28.996 6886810.276 any            27329   25.4 M   32.2 M   11.7 G        4    14542   371
2009-03-31 23:59:08.807 10332701.579 any              443   22.6 M  104.0 M   40.7 G       10    33796   400
2009-04-01 00:00:26.975 10332610.378 any           42825   22.0 M   28.4 M    4.3 G        2     3592   155
2009-04-01 00:04:54.993 6886655.285 any            43990   18.1 M  573.5 M  446.8 G       87   557366   797

Summary: total flows: 1487110483, total bytes: 10.4 T, total packets: 13.5 G, avg bps: 8.5 M, avg pps: 1407, avg bpp: 789
Time window: 2009-03-31 23:59:04 - 2009-07-29 14:10:54
Total flows processed: 1487110483, Records skipped: 0, Bytes read: 77330913556
Sys: 438.050s flows/second: 3394838.7  Wall: 1827.961s flows/second: 813535.0
```

Figura IV-50 - Relação das 20 portas ordenadas pela quantidade de fluxos - abril 2009

Toda a capacidade do disco (01 Terabyte) foi utilizada. Em função das divergências entre as informações detectadas entre o sistema Nfsen/Nfdump e o sistema CACTI, podemos dizer que, até setembro, os valores registrados são inferiores à realidade.

É possível observar que na Figura IV-51 há uma espécie de teto limitando o registro dos valores maiores da quantidade de fluxos - fato que só foi superado ao final de setembro após os ajustes nos parâmetros da aplicação (Softflowd), conforme descrito no capítulo 2. A partir deste ponto verifica-se a elevação dos valores, com o fim do teto e a ocorrência de picos de diversas intensidades. Isto também pode ser observado nas Figura IV-52 e Figura IV-53.

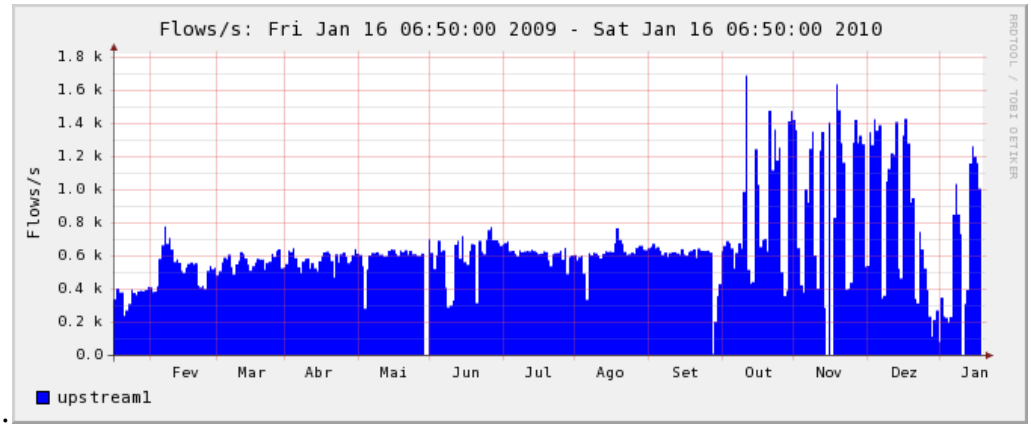


Figura IV-51 - Gráfico anual gerado pelo sistema Nfsen entre 01 de Janeiro 2009 e 16 de Janeiro de 2010. Fluxos/s.

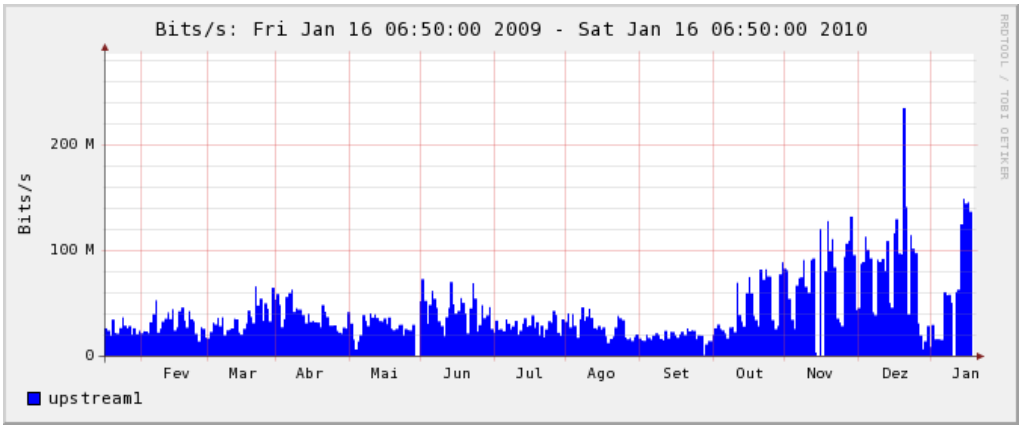


Figura IV-52 - Gráfico anual gerado pelo sistema Nfsen entre 01 de Janeiro 2009 e 16 de janeiro de 2010. Bits/s.

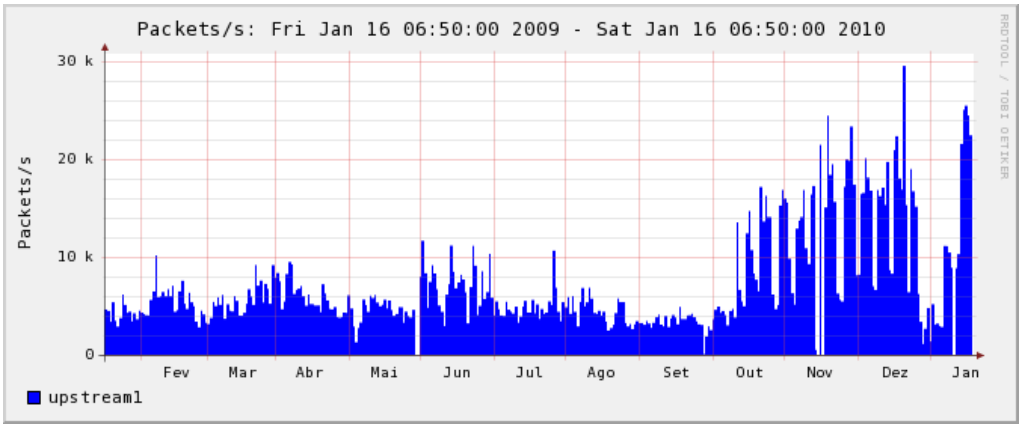


Figura IV-53 - Gráfico anual gerado pelo sistema Nfsen entre Janeiro 2009 e 16 de janeiro de 2010. Pacotes/s.

Na Figura IV-54 é possível acompanhar as estatísticas gerais da rede da UFF com relação à totalização de fluxos, bytes, pacotes e a média em bit/s registrados de janeiro a abril de 2009. Não foi possível ter a totalização do mês de maio, devido a problemas de espaço em disco. O perfil Live, em maio, foi sacrificado em benefício da manutenção dos demais perfis.

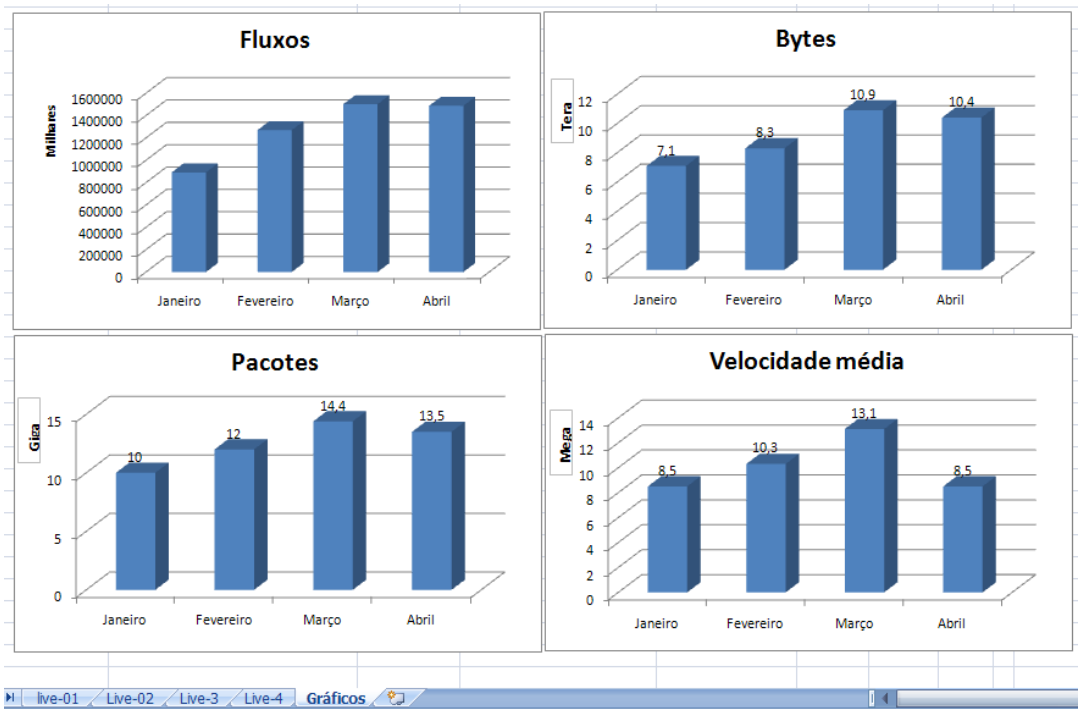


Figura IV-54 - Gráfico das estatísticas da rede a partir dos dados do perfil *Live*. De janeiro a abril de 2009

4.10 Segurança

Tradicionalmente, atividades de detecção de invasões em redes estão associadas a sistemas classificados como IDS (Intrusion Detection System) [27]. Estes sistemas, originalmente, capturam os pacotes trafegados na rede analisando-os na tentativa de identificar incidentes de segurança, comparando com padrões de assinaturas previamente catalogados. Entretanto, tecnologias como SSL ou IPSEC [28] onde os dados são criptografados antes da transmissão tem impostos obstáculos ao seu funcionamento, uma vez que isso impede a inspeção dos pacotes. Outra dificuldade é encontrada na análise do grande volume de dados transportados pelas redes de alta velocidade (1G, 10G) cada vez mais comuns. Para sanar esses problemas estão sendo desenvolvidas variações de IDS com o IDPS (Intrusion Detection Prevent System) [29] ou o NIDS (Network Intrusion Detection System). O IDPS busca outros fontes de informações além da do tráfego de rede como logs de um servidor e registro de fluxos. Além disso, registra informações sobre os incidentes observados e notifica administradores de rede. O IDPS, também pode ser configurado para modificar o ambiente de rede, por exemplo, alterando as regras de um firewall de modo a interromper um ataque.

Neste sentido, podemos dizer que as técnicas de detecção de incidentes experimentadas neste trabalho se assemelham mais ao funcionamento do IDPS, uma vez que foi possível gerar alertas em função dos incidentes detectados através do envio de e-mails, a ser demonstrado mais adiante.

Dentre os aspectos observados sobre a tecnologia de monitoramento de fluxos, destaca-se a capacidade de identificar ataques e uso indevido da rede. São evidenciadas situações onde estações de trabalho e servidores se tornam agentes controlados por terceiros e não economizam os recursos computacionais disponíveis, causando prejuízos ao funcionamento de toda a estrutura de comunicação da UFF.

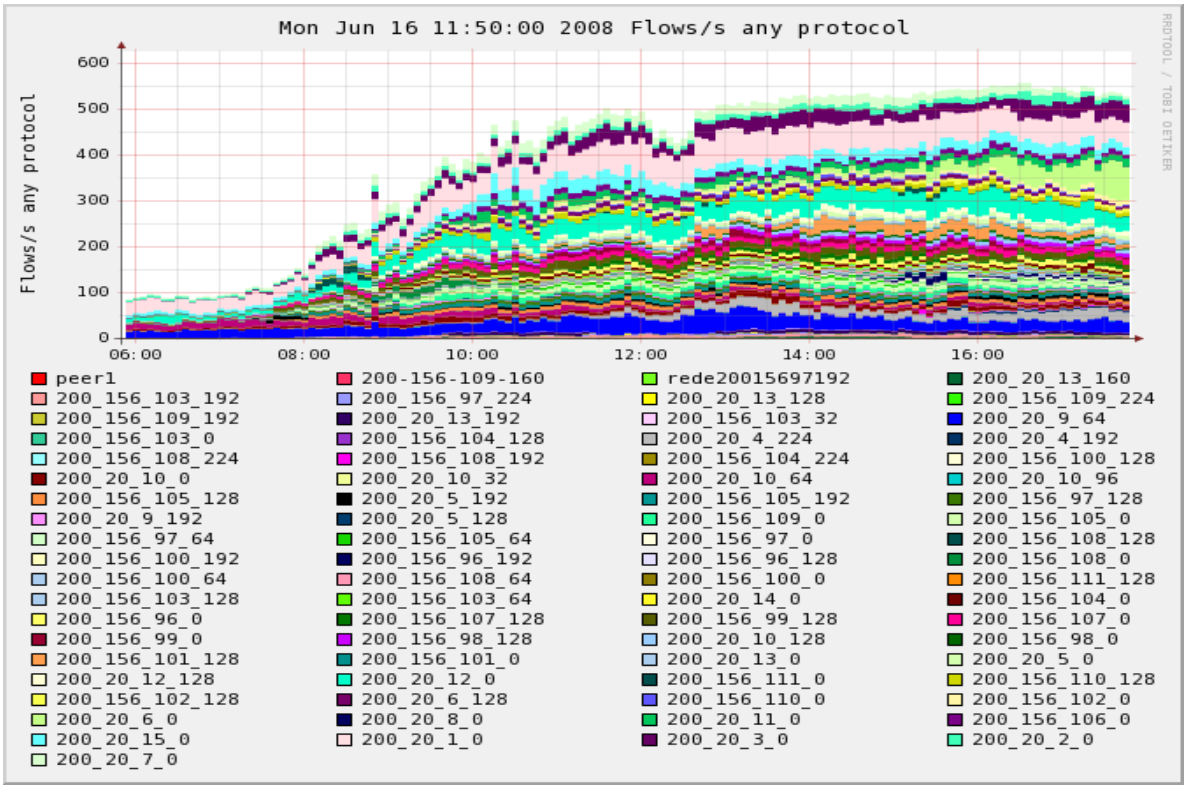


Figura IV-55 - Gráfico de doze horas de funcionamento do perfil Redes UFF.

Na Figura IV-55, gráfico do perfil RedeUff, é possível observar o crescimento gradual da atividade das redes representada pelas diferentes cores ao longo de 12 horas. A análise de gráficos como este, permitiu identificar alterações no PFR que levaram a descoberta de incidentes de segurança conforme veremos mais adiante.

4.11 Origens e padrões de atividade de rede

Toda a atividade de rede representa demandas que podem ter origem interna (da própria rede), ou externa (redes conectadas). Normalmente as demandas possuem determinadas características, por exemplo: o acesso a uma página web tem início com uma pequena requisição (uma URL de alguns bytes) direcionada a um servidor de paginas (WWW) e recebe como resposta a página principal do servidor que a hospeda (que pode variar entre alguns kbytes a algumas dezenas de Mbytes). A página é recebida em forma de rajada, de acordo com a velocidade e disponibilidade do enlace. Sites de vídeos como Youtube, terão a abertura da página inicial da mesma forma, entretanto, caso o usuário solicite a exibição de algum vídeo, será iniciada a transferência de um fluxo de bits que pode ser constante ou também em rajada. Já os clientes Peer-to-Peer em redes como Gnutella ou através do protocolo BitTorrent, utilizam técnicas de compartilhamento de

arquivos onde um nó (host) se conecta a um ou mais nós, de modo a pesquisar e transferir arquivos; normalmente músicas e filmes, no menor tempo possível [30]. Para isso centenas de conexões são realizadas entre os nós participantes, do início da busca até o fim da transferência do arquivo, caracterizando desta forma, outro comportamento a ser observado na rede. A seguir listamos algumas demandas que geram atividade na rede, classificadas por origem.

4.12 Atividades de rede por origem:

A. Interna

- A atividade direta de usuários através do uso de aplicativos web, e-mail, p2p, jogos, videoconferências, etc.
- A atividade indireta de usuários através do uso de aplicações utilitárias para manutenção de estações trabalho e que são ativados por demanda autônoma como: atualizações de sistemas operacionais, antivírus e drivers de dispositivo.
- Atividade de servidores Web, E-mail, banco de dados, imagens, e outros serviços de interesse institucional, ou não.
- Conexões a serviços externos (Cloud Computing [31]).
- Atividade de rede gerada por vírus, cavalos de Tróia, hackers e dispositivos de rede defeituosos.

B. Externa

- Acesso aos serviços oferecidos pela rede (acesso remoto, a servidores, e-mail e p2p).
- Atividade de vírus (fases de contaminação, propagação e ataque).
- Atividade de hackers (tentativas de invasão, controle de hosts sob domínio).

4.13 Incidentes de segurança e as portas do protocolo TCP/IP.

Normalmente um servidor web responde com atividade de rede nas portas (80 e 443) do protocolo TCP, no entanto, em casos de invasão, serviços adicionais podem ser disponibilizados em outras portas. Também estão sujeitas a estas situações, as estações de trabalho afetadas pela ação de vírus, hackers e outras pragas virtuais. Sendo assim, torna-se possível identificar as alterações no PFR, pela detecção da atividade de rede em portas diferentes daquelas registradas anteriormente pelo sistema. Entretanto, ao longo

deste trabalho, detectamos incidentes que utilizaram tanto portas desconhecidas, quanto portas clássicas da web como TCP: 80, 25 e 110. Neste caso, o que permitiu detectar a ocorrência do incidente de segurança foi a alteração repentina do PFR, em função do aumento da carga de trabalho imposta pelo incidente, por exemplo, aumento da quantidade de fluxos, bytes ou pacotes. Na prática, observa-se uma atividade de rede que difere do que se tem registrado anteriormente.

4.14 Alteração do PFR e detecção de incidentes de segurança.

Os elementos da rede que tenham o seu padrão de funcionamento alterado podem estar sob alguma das seguintes situações:

A. Sob ataque: Normalmente observa-se o aumento da atividade de uma ou mais redes, de uma ou mais portas ou de toda a rede, que levam à descoberta de um ou mais endereços IPs associados a elementos da rede, responsáveis por provocar a alteração do PFR. Neste trabalho foi possível identificar o uso de técnicas conhecidas como DDOS (*Distributed Denial of Service*) ou na maioria das vezes varredura de portas (Portscan) seguidas de ataques de dicionário;
B. Sob controle: Nesta situação, a segurança já foi comprometida. hackers, cavalo de tróia, vírus ou qualquer outra ameaça detém o controle do recurso e pode utilizá-lo indevidamente, a qualquer momento;
C. Sob comando: Acontece após o recurso estar sob o controle. O recurso atende aos comandos do invasor.

Tanto na situação A como na C, alterações no PFR serão percebidas com facilidade, entretanto, a situação B constitui um estado intermediário, que já passou pela situação A e pode evoluir para a situação C ou não. Contudo, existem situações em que um recurso da rede pode ter seu PFR alterado sem que isto configure uma das situações de segurança citadas anteriormente. Neste caso, é preciso conhecer a natureza das demandas, quanto à sua licitude. Sendo assim estudar o comportamento da rede sob diversas situações torna-se tarefa essencial, pois as informações colhidas possibilitarão avaliar se os recursos estão respondendo a uma demanda de interesse institucional ou não. Para isso, um ponto de partida pode ser o cadastramento de todos os elementos que compõem a rede. Isto poderia ser feito através de um sistema que classificasse hosts,

servidores, switches e roteadores e permitisse associar, a cada um, informações sobre o seu funcionamento. Este sistema teria como base de operação o PFH – Padrão de Funcionamento do Host, e analisaria individualmente a atividade de cada elemento da rede [32].

4.15 Coletânea de casos de segurança

Apresentaremos a seguir uma coleção de casos, incidentes de segurança, detectados a partir da detecção da alteração do PFR em função de tentativas de invasão, busca por serviços na rede e atividade de vírus.

4.16 Caso 1- Em busca de serviços na porta TCP 25.

Neste caso, como nos demais, a identificação do incidente é feita através da percepção do aumento da área ocupada por determinada cor, como pode ser visto no detalhe da Figura IV-56. Nesta imagem o ponteiro de seleção de incidente encontra-se sobre a área circulada, pois isto é necessário para que o sistema Nfsen faça a contabilização dos dados conforme mostra a Figura IV-57, onde é possível constatar que a quantidade de fluxos encontra-se bem acima das demais redes (139,7fluxos/s). Nesta mesma figura identificamos o endereço da rede 200.156.100.64, representado na Figura IV-56, pela cor azul-claro. De posse do endereço da rede, consulta-se o sistema novamente para saber quais endereços pertencentes a esta rede encontram-se entre aqueles que geraram mais fluxos no período. O resultado mostra, que o IP 200.156.100.105, (Figura IV-58), fez acessos consecutivos e ininterruptos a uma grande variedade de endereços da Internet direcionados à porta 25 que é destinada ao protocolo SMTP. O que caracteriza a geração de SPAM. Novamente, na Figura IV-56, é possível observar como a atividade modificou a construção do gráfico. Este tipo de incidente de segurança, não consome muitos recursos da rede considerando o aspecto banda disponível. Contudo, os roteadores têm suas tabelas poluídas pela grande variedade de endereços que são acessados (139.7 fluxos/s) em um curto espaço de tempo. A UFF, durante muito tempo, utilizou roteadores que possuíam pequena quantidade de memória disponível para suas tabelas de endereços e constantemente estes equipamentos entravam em colapso

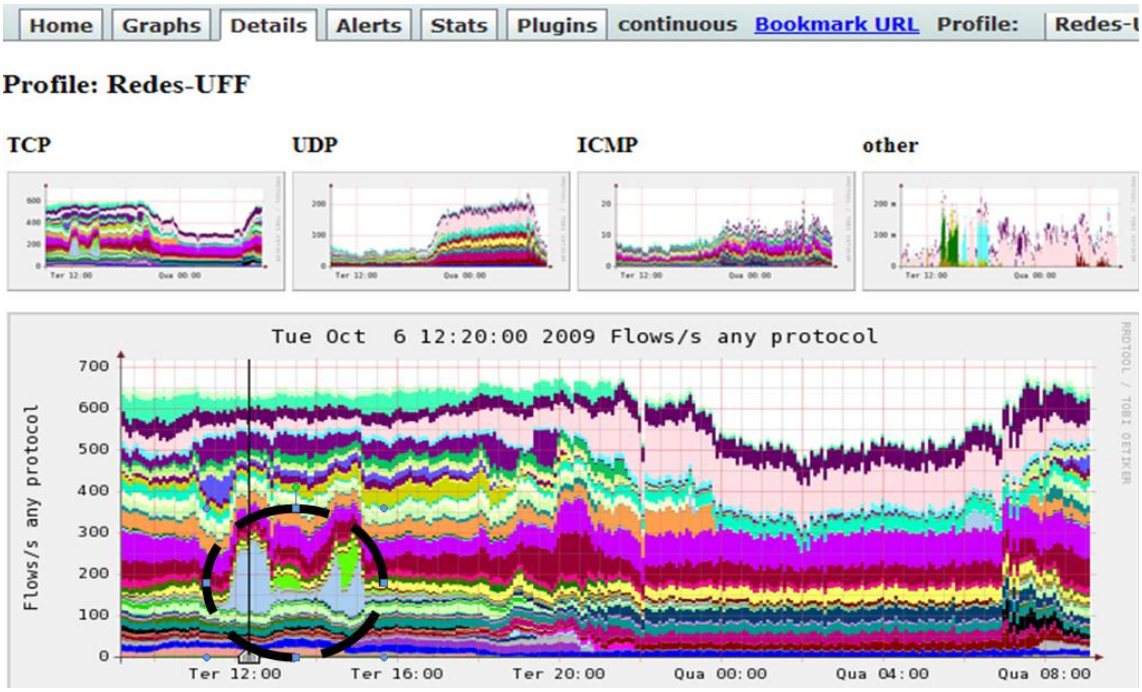
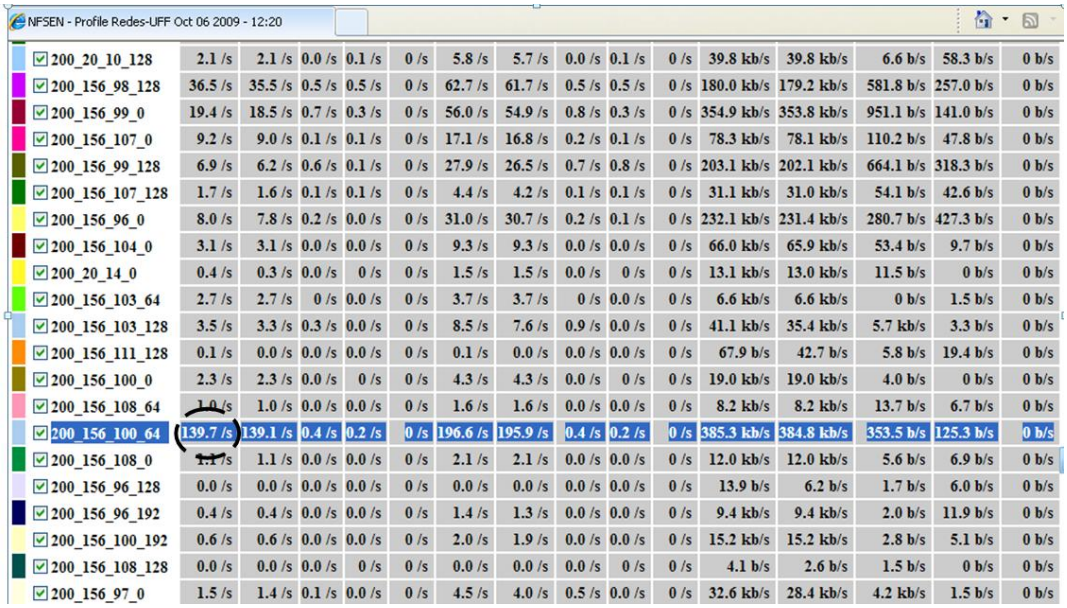


Figura IV-56 - Detecção visual do aumento da área representada pela cor azul-claro, por volta das 12h, no gráfico do Perfil RedesUFF. Foi posicionado o cursor nesta área para obtenção de mais informações.

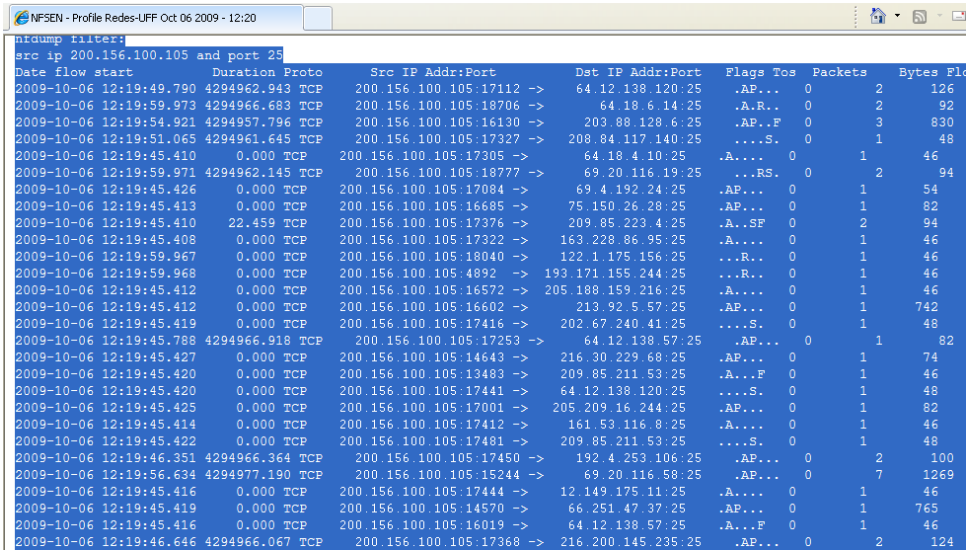
causando extrema lentidão na rede. Naquela situação um procedimento que atenuava o problema era aplicar, periodicamente, um comando do próprio roteador que esvaziava a tabela. Na época os administradores da rede associavam o incidente a ataques e a baixa capacidade dos equipamentos, porém, sem ter mais detalhes do que realmente ocorria. O que se sabia sobre os incidentes era que:

- não ocorria o tempo todo;
- ocorriam em lugares alternados;
- ocorriam sempre com mesmo modelo de equipamento; e
- ao isolar determinado segmento da rede (provavelmente o alvo do ataque), o funcionamento da rede voltava ao normal.



200_20_10_128	2.1 /s	2.1 /s	0.0 /s	0.1 /s	0 /s	5.8 /s	5.7 /s	0.0 /s	0.1 /s	0 /s	39.8 kb/s	39.8 kb/s	6.6 b/s	58.3 b/s	0 b/s
200_156_98_128	36.5 /s	35.5 /s	0.5 /s	0.5 /s	0 /s	62.7 /s	61.7 /s	0.5 /s	0.5 /s	0 /s	180.0 kb/s	179.2 kb/s	581.8 b/s	257.0 b/s	0 b/s
200_156_99_0	19.4 /s	18.5 /s	0.7 /s	0.3 /s	0 /s	56.0 /s	54.9 /s	0.8 /s	0.3 /s	0 /s	354.9 kb/s	353.8 kb/s	951.1 b/s	141.0 b/s	0 b/s
200_156_107_0	9.2 /s	9.0 /s	0.1 /s	0.1 /s	0 /s	17.1 /s	16.8 /s	0.2 /s	0.1 /s	0 /s	78.3 kb/s	78.1 kb/s	110.2 b/s	47.8 b/s	0 b/s
200_156_99_128	6.9 /s	6.2 /s	0.6 /s	0.1 /s	0 /s	27.9 /s	26.5 /s	0.7 /s	0.8 /s	0 /s	203.1 kb/s	202.1 kb/s	664.1 b/s	318.3 b/s	0 b/s
200_156_107_128	1.7 /s	1.6 /s	0.1 /s	0.1 /s	0 /s	4.4 /s	4.2 /s	0.1 /s	0.1 /s	0 /s	31.1 kb/s	31.0 kb/s	54.1 b/s	42.6 b/s	0 b/s
200_156_96_0	8.0 /s	7.8 /s	0.2 /s	0.0 /s	0 /s	31.0 /s	30.7 /s	0.2 /s	0.1 /s	0 /s	232.1 kb/s	231.4 kb/s	280.7 b/s	427.3 b/s	0 b/s
200_156_104_0	3.1 /s	3.1 /s	0.0 /s	0.0 /s	0 /s	9.3 /s	9.3 /s	0.0 /s	0.0 /s	0 /s	66.0 kb/s	65.9 kb/s	53.4 b/s	9.7 b/s	0 b/s
200_20_14_0	0.4 /s	0.3 /s	0.0 /s	0 /s	0 /s	1.5 /s	1.5 /s	0.0 /s	0 /s	0 /s	13.1 kb/s	13.0 kb/s	11.5 b/s	0 b/s	0 b/s
200_156_103_64	2.7 /s	2.7 /s	0 /s	0.0 /s	0 /s	3.7 /s	3.7 /s	0 /s	0.0 /s	0 /s	6.6 kb/s	6.6 kb/s	0 b/s	1.5 b/s	0 b/s
200_156_103_128	3.5 /s	3.3 /s	0.3 /s	0.0 /s	0 /s	8.5 /s	7.6 /s	0.9 /s	0.0 /s	0 /s	41.1 kb/s	35.4 kb/s	5.7 kb/s	3.3 b/s	0 b/s
200_156_111_128	0.1 /s	0.0 /s	0.0 /s	0.0 /s	0 /s	0.1 /s	0.0 /s	0.0 /s	0.0 /s	0 /s	67.9 b/s	42.7 b/s	5.8 b/s	19.4 b/s	0 b/s
200_156_100_0	2.3 /s	2.3 /s	0.0 /s	0 /s	0 /s	4.3 /s	4.3 /s	0.0 /s	0 /s	0 /s	19.0 kb/s	19.0 kb/s	4.0 b/s	0 b/s	0 b/s
200_156_108_64	1.0 /s	1.0 /s	0.0 /s	0.0 /s	0 /s	1.6 /s	1.6 /s	0.0 /s	0.0 /s	0 /s	8.2 kb/s	8.2 kb/s	13.7 b/s	6.7 b/s	0 b/s
200_156_100_64	139.7 /s	139.1 /s	0.4 /s	0.2 /s	0 /s	196.6 /s	195.9 /s	0.4 /s	0.2 /s	0 /s	385.3 kb/s	384.8 kb/s	353.5 b/s	125.3 b/s	0 b/s
200_156_108_0	1.1 /s	1.1 /s	0.0 /s	0.0 /s	0 /s	2.1 /s	2.1 /s	0.0 /s	0.0 /s	0 /s	12.0 kb/s	12.0 kb/s	5.6 b/s	6.9 b/s	0 b/s
200_156_96_128	0.0 /s	0.0 /s	0.0 /s	0.0 /s	0 /s	0.0 /s	0.0 /s	0.0 /s	0.0 /s	0 /s	13.9 b/s	6.2 b/s	1.7 b/s	6.0 b/s	0 b/s
200_156_96_192	0.4 /s	0.4 /s	0.0 /s	0.0 /s	0 /s	1.4 /s	1.3 /s	0.0 /s	0.0 /s	0 /s	9.4 kb/s	9.4 kb/s	2.0 b/s	11.9 b/s	0 b/s
200_156_100_192	0.6 /s	0.6 /s	0.0 /s	0.0 /s	0 /s	2.0 /s	1.9 /s	0.0 /s	0.0 /s	0 /s	15.2 kb/s	15.2 kb/s	2.8 b/s	5.1 b/s	0 b/s
200_156_108_128	0.0 /s	0.0 /s	0.0 /s	0 /s	0 /s	0.0 /s	0.0 /s	0.0 /s	0 /s	0 /s	4.1 b/s	2.6 b/s	1.5 b/s	0 b/s	0 b/s
200_156_97_0	1.5 /s	1.4 /s	0.1 /s	0.0 /s	0 /s	4.5 /s	4.0 /s	0.5 /s	0.0 /s	0 /s	32.6 kb/s	28.4 kb/s	4.2 kb/s	1.5 b/s	0 b/s

Figura IV-57 - Localização da rede 200.156.100.64 no painel de visualização correspondente à cor azul-claro identificada anteriormente. Detalhe mostrando que a quantidade de fluxos neste momento é superior as demais redes



Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Flags	Tos	Packets	Bytes	Flo
2009-10-06 12:19:49.790	4294962.943	TCP	200.156.100.105:17112	->	64.12.138.120:25	.AP...	0	2	126	
2009-10-06 12:19:59.973	4294966.683	TCP	200.156.100.105:18706	->	64.18.6.14:25	.A.R..	0	2	92	
2009-10-06 12:19:54.921	4294957.796	TCP	200.156.100.105:16130	->	203.88.128.6:25	.AP..F	0	3	830	
2009-10-06 12:19:51.065	4294961.645	TCP	200.156.100.105:17327	->	208.84.117.140:25	....S.	0	1	48	
2009-10-06 12:19:45.410	0.000	TCP	200.156.100.105:17305	->	64.18.4.10:25	.A....	0	1	46	
2009-10-06 12:19:59.971	4294962.145	TCP	200.156.100.105:18777	->	69.20.116.19:25	...RS.	0	2	94	
2009-10-06 12:19:45.426	0.000	TCP	200.156.100.105:17084	->	69.4.192.24:25	.AP...	0	1	54	
2009-10-06 12:19:45.413	0.000	TCP	200.156.100.105:16685	->	75.150.26.28:25	.AP...	0	1	82	
2009-10-06 12:19:45.410	22.459	TCP	200.156.100.105:17376	->	209.85.223.4:25	.A..SF	0	2	94	
2009-10-06 12:19:45.408	0.000	TCP	200.156.100.105:17322	->	163.228.86.95:25	.A....	0	1	46	
2009-10-06 12:19:59.967	0.000	TCP	200.156.100.105:18040	->	122.1.175.156:25	...R..	0	1	46	
2009-10-06 12:19:59.968	0.000	TCP	200.156.100.105:4892	->	193.171.155.244:25	...R..	0	1	46	
2009-10-06 12:19:45.412	0.000	TCP	200.156.100.105:16572	->	205.188.159.216:25	.A....	0	1	46	
2009-10-06 12:19:45.412	0.000	TCP	200.156.100.105:16602	->	213.92.5.57:25	.AP...	0	1	742	
2009-10-06 12:19:45.419	0.000	TCP	200.156.100.105:17416	->	202.67.240.41:25	....S.	0	1	48	
2009-10-06 12:19:45.788	4294966.918	TCP	200.156.100.105:17253	->	64.12.138.57:25	.AP...	0	1	82	
2009-10-06 12:19:45.427	0.000	TCP	200.156.100.105:14643	->	216.30.229.68:25	.AP...	0	1	74	
2009-10-06 12:19:45.420	0.000	TCP	200.156.100.105:13483	->	209.85.211.53:25	.A...F	0	1	46	
2009-10-06 12:19:45.420	0.000	TCP	200.156.100.105:17441	->	64.12.138.120:25	....S.	0	1	48	
2009-10-06 12:19:45.425	0.000	TCP	200.156.100.105:17001	->	205.209.16.244:25	.AP...	0	1	82	
2009-10-06 12:19:45.414	0.000	TCP	200.156.100.105:17412	->	161.53.116.8:25	.A....	0	1	46	
2009-10-06 12:19:45.422	0.000	TCP	200.156.100.105:17481	->	209.85.211.53:25	....S.	0	1	48	
2009-10-06 12:19:46.351	4294966.364	TCP	200.156.100.105:17450	->	192.4.253.106:25	.AP...	0	2	100	
2009-10-06 12:19:56.634	4294977.190	TCP	200.156.100.105:15244	->	69.20.116.58:25	.AP...	0	7	1269	
2009-10-06 12:19:45.416	0.000	TCP	200.156.100.105:17444	->	12.149.175.11:25	.A....	0	1	46	
2009-10-06 12:19:45.419	0.000	TCP	200.156.100.105:14570	->	66.251.47.37:25	.AP...	0	1	765	
2009-10-06 12:19:45.416	0.000	TCP	200.156.100.105:16019	->	64.12.138.57:25	.A...F	0	1	46	
2009-10-06 12:19:46.646	4294966.067	TCP	200.156.100.105:17368	->	216.200.145.235:25	.AP...	0	2	124	

Figura IV-58 - Resultado da consulta detalhada aos fluxos da rede 200.156.100.64, onde o ip 200.156.100.105 aparece acessando diversas máquinas na Internet em busca daquelas que respondam positivamente a porta TCP 25.

Após a atualização da rede através da instalação de equipamentos mais modernos, os incidentes deixaram de ser percebidos, entretanto, verificamos que o Caso 1 teria condições de provocar o mesmo efeito de lentidão nos antigos roteadores, considerando a quantidade de endereços que foram acessados. Conforme dissemos anteriormente,

havendo esgotamento dos recursos da rede sem que sejam identificadas as origens das demandas, é muito provável que se decida por investimentos em equipamentos mais modernos, visando à solução do problema, entretanto, novamente fazendo referência ao Caso 1, os recursos não seriam consumidos em favor dos interesses da instituição e sim do agente gerador do incidente. Em uma rede com monitoramento deficiente não é possível saber onde os recursos estão sendo consumidos. Se for disponibilizado 1Mbit/s, será consumido 1Mbit/s e o mesmo irá ocorrer se for disponibilizado 100Mbit/s ou 1Gbit/s. Portanto, o monitoramento de redes constitui atividade de vital importância capaz de apontar onde os recursos estão sendo consumidos, garantindo assim que os investimentos tragam benefícios reais e não apenas amenizem a lentidão da rede causada por vírus e harckes pela simples oferta de conexões mais velozes. Na verdade, na falta de mecanismo de monitoramento e controle, a melhoria terá caráter temporário, pelos motivos expostos anteriormente.

4.17 Caso 2 – Uso de aplicativos Peer to Peer ?

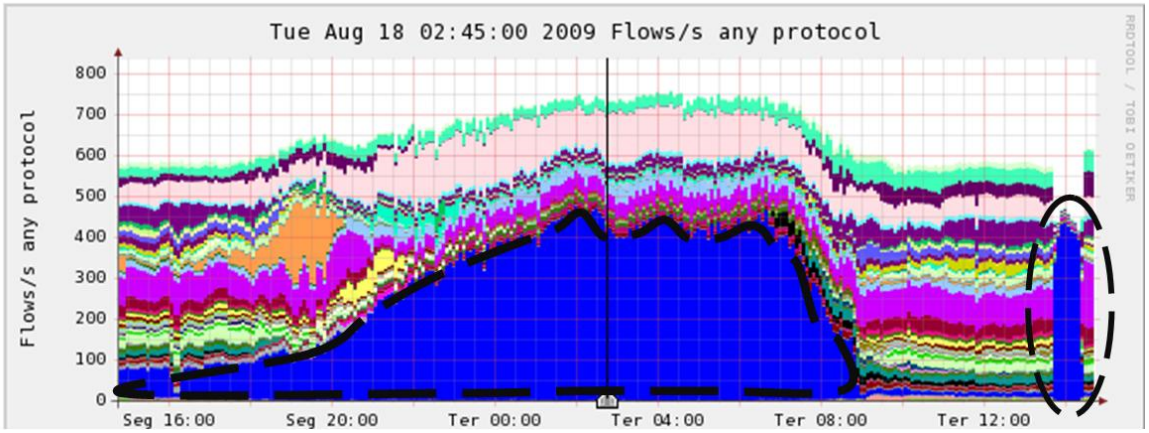


Figura IV-59 - Detecção visual do aumento de fluxos de uma rede no gráfico do Nfsen.

Este caso chama atenção devido à grande alteração observada no PFR, conforme mostra a Figura IV-59. O incidente teve início antes das 14h do dia 17/08/09 durou até as 8h da manhã do dia 18/08/09, recomeçando por volta das 14h.

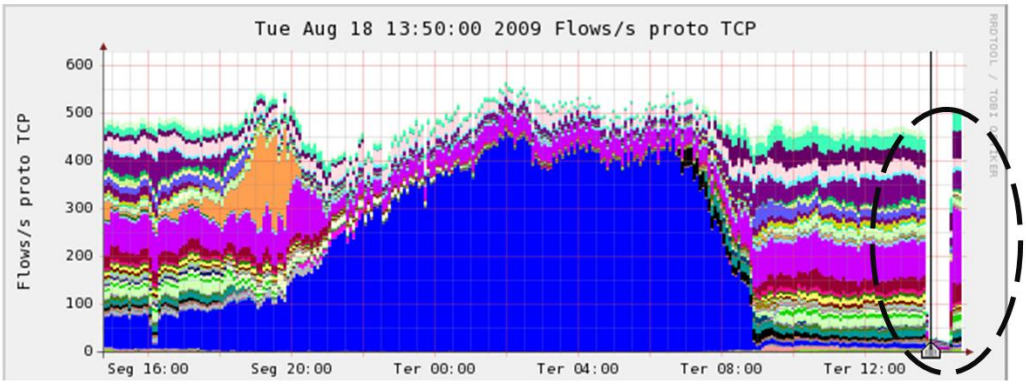


Figura IV-60 - Gráfico do Nfsen que apresenta apenas o protocolo TCP. Uma observação nesta figura quanto a lacuna que aparece na parte circulada.

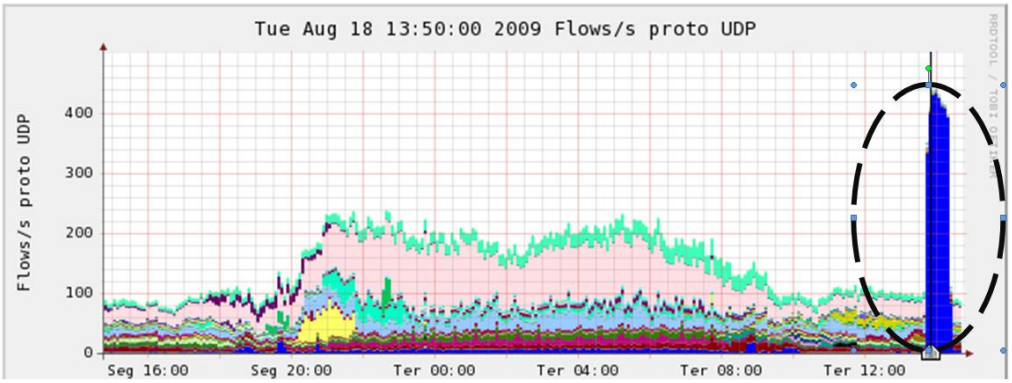
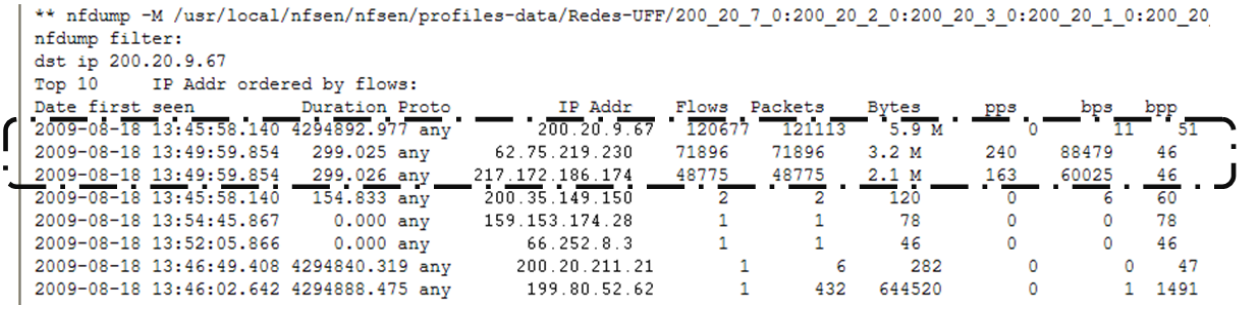


Figura IV-61 - Gráfico do Nfsen que apresenta apenas o protocolo UDP. Repare que a lacuna observada na Figura IV-60, que se restringia apenas ao protocolo TCP, aparece preenchida neste gráfico, pela cor azul.

Um detalhe observado neste incidente é que ele se divide em duas partes. A primeira utilizando o protocolo TCP (Figura IV-60) e a segunda utilizando o protocolo UDP (Figura IV-61). O mais interessante ocorre quando o protocolo TCP é afetado pelo intenso uso do protocolo UDP. Isto é evidenciado na lacuna existente no gráfico da Figura IV-60 em função da elevada atividade do protocolo UDP mostrado na Figura IV-61. Este efeito provocado pelo uso do protocolo UDP é citado no capítulo 2 item 2.8 Revisão de Literatura, como “not TCP Friendly”.

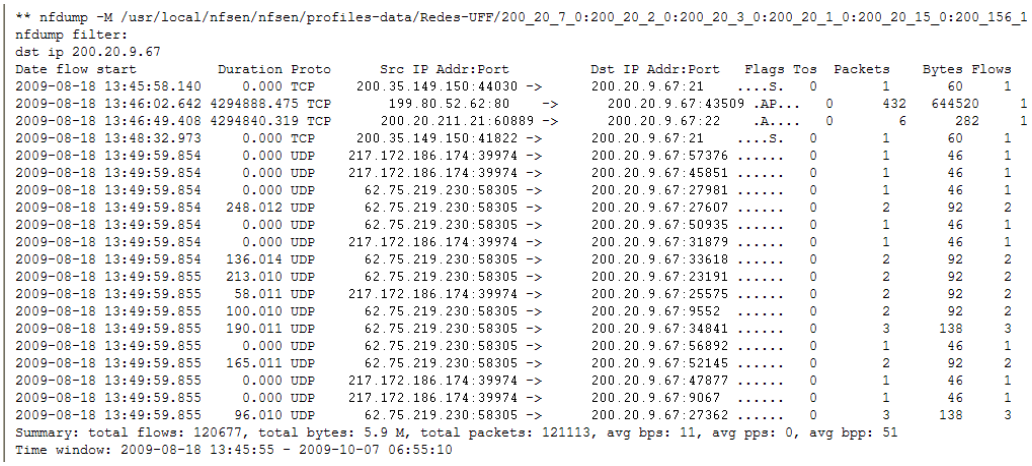
Os números mostram que o incidente foi de atividade intensa e que durante o uso do protocolo UDP, todo o funcionamento da rede foi afetado conforme mostra a Figura IV-60. Em cinco minutos o IP 200.20.9.67, recebeu 120667 fluxos a uma velocidade de 402.2 fluxos por segundo.

A Figura IV-62, mostra os três endereços IPs que tiveram a maior quantidade de fluxos registrados. O primeiro (200.20.9.67), da UFF, é o IP de destino e os outros dois são os IPs de origem. Além desses existem outros que podem ser vistos na Figura IV-63.



```
** nfdump -M /usr/local/nfsen/nfsen/profiles-data/Redes-UFF/200_20_7_0:200_20_2_0:200_20_3_0:200_20_1_0:200_20
nfdump filter:
dst ip 200.20.9.67
Top 10     IP Addr ordered by flows:
Date first seen          Duration Proto        IP Addr    Flows  Packets    Bytes     pps     bps   bpp
2009-08-18 13:45:58.140 4294892.977 any      200.20.9.67   120677   121113   5.9 M       0      11    51
2009-08-18 13:49:59.854    299.025 any    62.75.219.230    71896    71896   3.2 M     240   88479    46
2009-08-18 13:49:59.854    299.026 any  217.172.186.174    48775    48775   2.1 M     163   60025    46
2009-08-18 13:45:58.140    154.833 any   200.35.149.150        2        2     120       0       6    60
2009-08-18 13:54:45.867      0.000 any   159.153.174.28        1        1      78       0       0    78
2009-08-18 13:52:05.866      0.000 any     66.252.8.3          1        1      46       0       0    46
2009-08-18 13:46:49.408 4294840.319 any   200.20.211.21         1        6     282       0       0    47
2009-08-18 13:46:02.642 4294888.475 any    199.80.52.62         1      432  644520       0       1  1491
```

Figura IV-62 - Identificação do IP 200.20.9.67, que aparece com o maior número de fluxos (120.677), seguido do IP 62.75.219.230 e IP 217.172.186.174.



```
** nfdump -M /usr/local/nfsen/nfsen/profiles-data/Redes-UFF/200_20_7_0:200_20_2_0:200_20_3_0:200_20_1_0:200_20_15_0:200_156_1
nfdump filter:
dst ip 200.20.9.67
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Flags Tos  Packets    Bytes Flows
2009-08-18 13:45:58.140     0.000 TCP     200.35.149.150:44030 ->      200.20.9.67:21    ....S.  0        1       60     1
2009-08-18 13:46:02.642 4294888.475 TCP       199.80.52.62:80    ->      200.20.9.67:43509 .AP...  0      432   644520     1
2009-08-18 13:46:49.408 4294840.319 TCP      200.20.211.21:60889 ->      200.20.9.67:22    .A....  0        6      282     1
2009-08-18 13:48:32.973     0.000 TCP     200.35.149.150:41822 ->      200.20.9.67:21    ....S.  0        1       60     1
2009-08-18 13:49:59.854     0.000 UDP    217.172.186.174:39974 ->      200.20.9.67:57376 ......  0        1       46     1
2009-08-18 13:49:59.854     0.000 UDP    217.172.186.174:39974 ->      200.20.9.67:45851 ......  0        1       46     1
2009-08-18 13:49:59.854     0.000 UDP      62.75.219.230:58305 ->      200.20.9.67:27981 ......  0        1       46     1
2009-08-18 13:49:59.854   248.012 UDP      62.75.219.230:58305 ->      200.20.9.67:27607 ......  0        2       92     2
2009-08-18 13:49:59.854     0.000 UDP      62.75.219.230:58305 ->      200.20.9.67:50935 ......  0        1       46     1
2009-08-18 13:49:59.854     0.000 UDP    217.172.186.174:39974 ->      200.20.9.67:31879 ......  0        1       46     1
2009-08-18 13:49:59.854   136.014 UDP      62.75.219.230:58305 ->      200.20.9.67:33618 ......  0        2       92     2
2009-08-18 13:49:59.855   213.010 UDP      62.75.219.230:58305 ->      200.20.9.67:23191 ......  0        2       92     2
2009-08-18 13:49:59.855    58.011 UDP    217.172.186.174:39974 ->      200.20.9.67:25575 ......  0        2       92     2
2009-08-18 13:49:59.855   100.010 UDP      62.75.219.230:58305 ->      200.20.9.67:9552  ......  0        2       92     2
2009-08-18 13:49:59.855   190.011 UDP      62.75.219.230:58305 ->      200.20.9.67:34841 ......  0        3      138     3
2009-08-18 13:49:59.855     0.000 UDP      62.75.219.230:58305 ->      200.20.9.67:56892 ......  0        1       46     1
2009-08-18 13:49:59.855   165.011 UDP      62.75.219.230:58305 ->      200.20.9.67:52145 ......  0        2       92     2
2009-08-18 13:49:59.855     0.000 UDP    217.172.186.174:39974 ->      200.20.9.67:47877 ......  0        1       46     1
2009-08-18 13:49:59.855     0.000 UDP    217.172.186.174:39974 ->      200.20.9.67:9067  ......  0        1       46     1
2009-08-18 13:49:59.855    96.010 UDP      62.75.219.230:58305 ->      200.20.9.67:27362 ......  0        3      138     3
Summary: total flows: 120677, total bytes: 5.9 M, total packets: 121113, avg bps: 11, avg pps: 0, avg bpp: 51
Time window: 2009-08-18 13:45:55 - 2009-10-07 06:55:10
```

Figura IV-63 Consulta detalhada aos fluxos destinados ao host de endereço IP 200.20.9.67. É possível observar que os hosts de endereços IP 217.172.186.174 e 62.75.219.230, aparecem enviando pacotes UDP a partir de portas fixas (58305 e 39974) para o host da UFF (200.20.9.67).

De acordo com o funcionamento do Netflow, um sistema de monitoramento só computa um novo fluxo, caso não encontre fluxos correspondentes para agregá-lo à sua base de dados. No Caso 2, onde são registrados 402.2 novos fluxos a cada segundo, podemos dizer que não se trata de aplicações tradicionais como clientes Web, de e-mail, FTP, ou comunicadores instantâneos, mas talvez de algum tipo de software Peer-to-Peer, considerando a quantidade de endereços envolvidos, característicos de funcionamento de sistemas distribuído ao qual o incidente observado se assemelha.

4.18 Caso 3 – Em busca de serviço na porta 22 do TCP

O Caso 3, de acordo com o gráfico da Figura IV-64, representa o incidente de segurança cujas características mais se repetiram durante a realização deste trabalho. Trata-se da varredura da rede em busca de máquinas executando serviços na porta 22 do TCP. Acreditamos que a maior incidência destes, deva-se ao fato de que a porta 22, de acordo como a IANA, é destinada a aplicações de acesso remoto seguro. Este tipo de aplicação vem habilitado, por padrão, em muitas distribuições do sistema operacional Linux e dá ao usuário com as devidas credenciais, total controle sobre a máquina. Existem vários ataques que visam esta porta, inclusive ataques simples de força bruta como o de dicionário de senhas que exploram instalações inseguras feitas por neófitos.

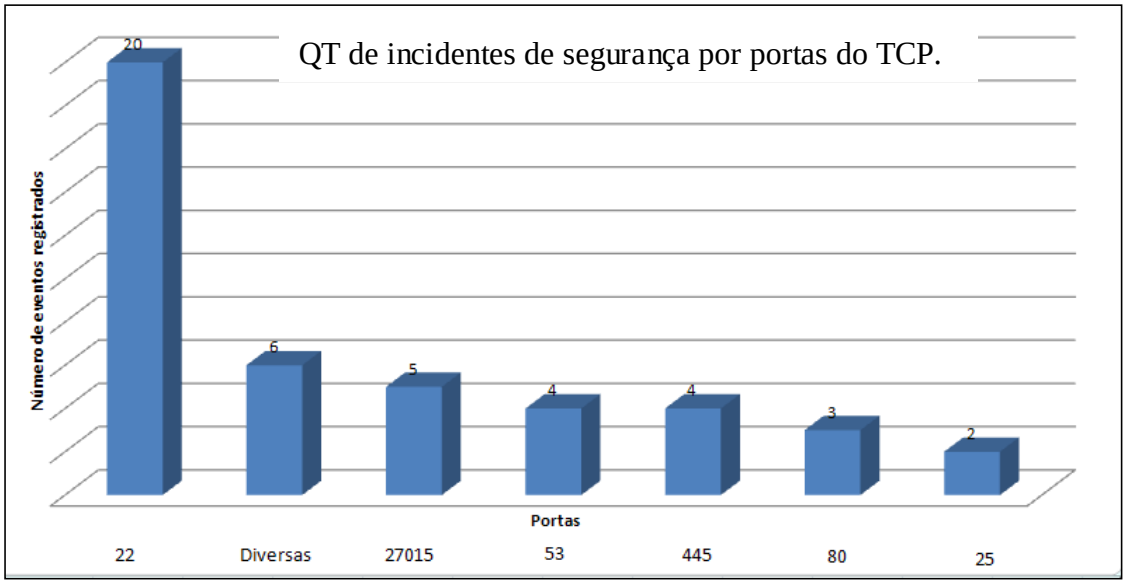


Figura IV-64 – Registro de 44 casos de segurança entre Fevereiro de 2008 e Novembro de 2009.

A sequência é mesma descrita para o Caso 1. Primeiro identifica-se a alteração no gráfico (Figura IV-65), depois são verificadas as informações que levam até o agente gerador do incidente. Na Figura IV-66, verifica-se a intensidade do ataque, 690.5 fluxos por segundo. Na Figura IV-67, através do relatório que relaciona 10 endereços IPs ordenados pela quantidade de fluxo, identifica-se o IP 200.156.105.101 no primeiro lugar do ranking. Na Figura IV-68 verifica-se a ação do IP 200.156.105.101, vasculhando diversas redes em busca de endereços IP que comecem com prefixo 128.194. e tenham serviço na porta 22.

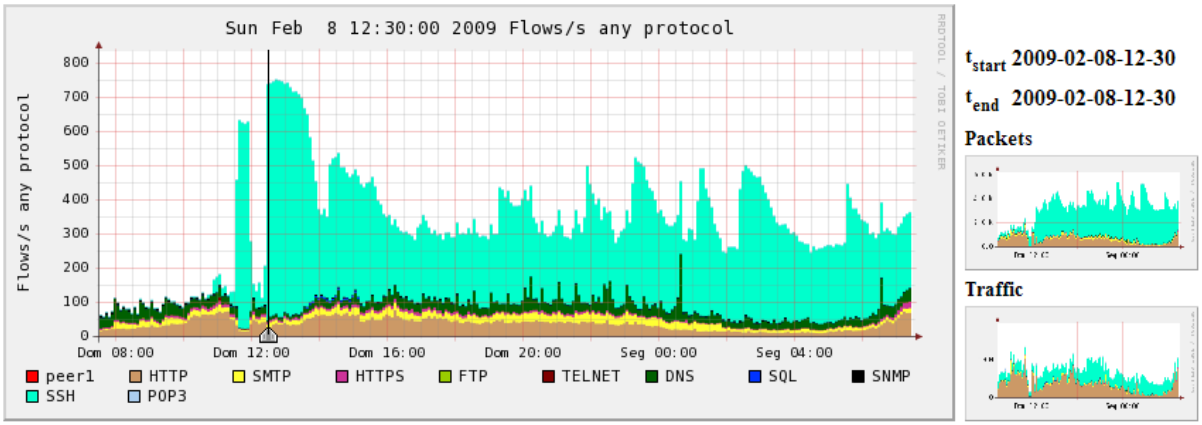


Figura IV-65 – Identificação visual do aumento da quantidade de fluxos utilizando a porta 22 do protocolo TCP representada no gráfico pela cor verde-claro.

Statistics timeslot Feb 08 2009 - 12:30

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
POP3	0.2 /s	0.2 /s	0 /s	0 /s	0 /s	0.8 /s	0.8 /s	0 /s	0 /s	0 /s	1.8 kb/s	1.8 kb/s	0 b/s	0 b/s	0 b/s
SSH	690.5 /s	690.5 /s	0.0 /s	0 /s	0 /s	1.8 k/s	1.8 k/s	0.0 /s	0 /s	0 /s	2.2 Mb/s	2.2 Mb/s	4.7 b/s	0 b/s	0 b/s
SNMP	0.4 /s	0 /s	0.4 /s	0 /s	0 /s	0.6 /s	0 /s	0.6 /s	0 /s	0 /s	377.3 b/s	0 b/s	377.3 b/s	0 b/s	0 b/s
SQL	0.1 /s	0.1 /s	0 /s	0 /s	0 /s	2.4 /s	2.4 /s	0 /s	0 /s	0 /s	8.8 kb/s	8.8 kb/s	0 b/s	0 b/s	0 b/s
DNS	4.0 /s	0.0 /s	4.0 /s	0 /s	0 /s	4.4 /s	0.0 /s	4.3 /s	0 /s	0 /s	4.6 kb/s	20.0 b/s	4.5 kb/s	0 b/s	0 b/s
TELNET	0.0 /s	0.0 /s	0 /s	0 /s	0 /s	0.1 /s	0.1 /s	0 /s	0 /s	0 /s	26.3 b/s	26.3 b/s	0 b/s	0 b/s	0 b/s
FTP	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 b/s	0 b/s	0 b/s	0 b/s	0 b/s
HTTPS	6.9 /s	6.9 /s	0.0 /s	0 /s	0 /s	22.1 /s	22.1 /s	0.0 /s	0 /s	0 /s	94.9 kb/s	94.9 kb/s	14.9 b/s	0 b/s	0 b/s
SMTP	9.8 /s	9.8 /s	0 /s	0 /s	0 /s	26.9 /s	26.9 /s	0 /s	0 /s	0 /s	42.1 kb/s	42.1 kb/s	0 b/s	0 b/s	0 b/s
HTTP	25.0 /s	24.9 /s	0.1 /s	0 /s	0 /s	196.1 /s	196.0 /s	0.1 /s	0 /s	0 /s	1.3 Mb/s	1.3 Mb/s	158.9 b/s	0 b/s	0 b/s

Figura IV-66 - Painel de visualização, mostrando que 690.5 fluxos por segundo são registrados para o protocolo SSH (porta 22 do TCP).

```
** nfdump -M /usr/local/nfsen/nfsen/profiles-data/PROTOCOLOS/POP3:SSH:SNMP:SQL:DNS:TELNET:FTP:HTTPS:SMTP:HTTP:peer
nfdump filter:
any
Top 10     IP Addr ordered by flows:
Date first seen          Duration Proto          IP Addr    Flows  Packets    Bytes      pps      bps   bpp
2009-02-08 12:29:45.150 4295280.911 any     200.156.105.101   206531   512284   65.4 M        0      127   133
2009-02-08 12:29:45.151 4295280.910 any     128.194.112.48    12320    12320   601264        0        1    48
2009-02-08 12:29:45.152 4295266.229 any     128.194.106.102   10002    28208    3.4 M        0        6   124
2009-02-08 12:29:45.160 4295266.216 any     128.194.229.165    9405    24458    3.2 M        0        6   139
2009-02-08 12:29:45.166 4295266.211 any     128.194.106.248    9351    26384    3.4 M        0        6   134
2009-02-08 12:29:45.163 4295266.220 any     128.194.105.184    9027    22621    3.1 M        0        6   143
2009-02-08 12:29:45.660 4295265.712 any      128.194.86.62     8816    24280    3.1 M        0        6   135
2009-02-08 12:29:45.156 4295266.225 any     128.194.102.7      8628    24024    3.1 M        0        6   137
2009-02-08 12:29:45.153 4295266.222 any     128.194.113.139    8516    19081    2.5 M        0        4   135
2009-02-08 12:29:45.872 4295265.511 any      128.194.169.38    7917    21958    2.8 M        0        5   134

Summary: total flows: 221110, total bytes: 129.4 M, total packets: 603840, avg bps: 252, avg pps: 0, avg bpp: 224
Time window: 2009-02-08 12:29:45 - 2009-03-30 04:37:46
Total flows processed: 221110, Records skipped: 0, Bytes read: 11497972
Sys: 0.058s flows/second: 3748262.4   Wall: 0.302s flows/second: 729931.1
```

Figura IV-67 - Resultado da consulta ao sistema Nfsen, onde é possível ver que o IP 200.156.105.101 é o primeiro da lista com 206.531 fluxos de um total 221.110 fluxos registrados no período.

```
** nfdump -M /usr/local/nfsen/nfsen/profiles-data/PROTOCOLOS/POP3:SSH:SNMP:SQL:DNS:TELNET:FTP:HTTPS:SMTP:HTTP:peer1  -T  -r 20
nfdump filter:
src ip 200.156.105.101
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Flags Tos  Packets    Bytes Flows
2009-02-08 12:29:47.050 4294965.413 TCP    200.156.105.101:38606 ->  128.194.105.184:22    .AP..F   0        2      102     1
2009-02-08 12:29:47.276 4294965.184 TCP    200.156.105.101:38738 ->  128.194.105.184:22    .AP..F   0        4      418     1
2009-02-08 12:29:47.546 4294964.921 TCP    200.156.105.101:33604 ->   128.194.90.115:22    .AP...   0        2      230     1
2009-02-08 12:29:47.276 4294965.191 TCP    200.156.105.101:37462 ->   128.194.149.4:22     .AP...   0        4      340     1
2009-02-08 12:29:47.754 4294964.706 TCP    200.156.105.101:53735 ->   128.194.75.12:22     .AP...   0        2      106     1
2009-02-08 12:29:46.495 4294965.965 TCP    200.156.105.101:53738 ->   128.194.75.12:22     .A....   0        1       46     1
2009-02-08 12:29:45.169      0.000 TCP    200.156.105.101:45267 ->   128.194.112.48:22    ....S.   0        1       52     1
2009-02-08 12:29:45.832 4294966.631 TCP    200.156.105.101:38755 ->  128.194.105.184:22    .AP...   0        2      230     1
2009-02-08 12:29:46.884 4294965.580 TCP    200.156.105.101:34232 ->  128.194.253.133:22    .AP...   0        4      592     1
2009-02-08 12:29:46.603 4294965.860 TCP    200.156.105.101:53832 ->   128.194.169.38:22    .AP...   0        3      240     1
2009-02-08 12:29:48.779 4294963.686 TCP    200.156.105.101:47487 ->  128.194.169.157:22    .AP..F   0        4      244     1
2009-02-08 12:29:46.812 4294965.651 TCP    200.156.105.101:57193 ->   128.194.143.77:22    ....S.   0        1       52     1
2009-02-08 12:29:46.151 4294966.316 TCP    200.156.105.101:42810 ->  128.194.107.194:22    .AP...   0        2      248     1
2009-02-08 12:29:46.839 4294965.628 TCP    200.156.105.101:38502 ->  128.194.105.184:22    .AP...   0        1      184     1
2009-02-08 12:29:48.398 4294964.067 TCP    200.156.105.101:57720 ->   128.194.246.50:22    .A....   0        1       46     1
2009-02-08 12:29:45.648 4294966.818 TCP    200.156.105.101:54348 ->  128.194.229.165:22    .AP...   0        1      184     1
```

Figura IV-68 - Detalhes dos acessos do host 200.156.105.101, em busca de hosts que respondam a consultas na porta do TCP 22.

4.19 Caso 4 – Ataque de negação de serviço distribuído, partindo de uma das redes da UFF.

O Caso 4 corresponde a um clássico ataque DDOS e pode ser observado na Figura IV-69. Registramos vinte e cinco IPs da UFF fazendo acessos simultâneos ao IP 80.244.248.46, na porta 80, registrado como www4.daj.ba, na Alemanha. O ataque partiu da rede 200.156.105.0, tendo como alvo o endereço IP 80.244.248.46. Acreditamos na hipótese de que este caso, ocorrido em setembro de 2009, esteja relacionado ao anterior (caso 3, registrado em fevereiro do mesmo ano), uma vez que o endereço IP 200.156.105.101 pertence a esta rede.

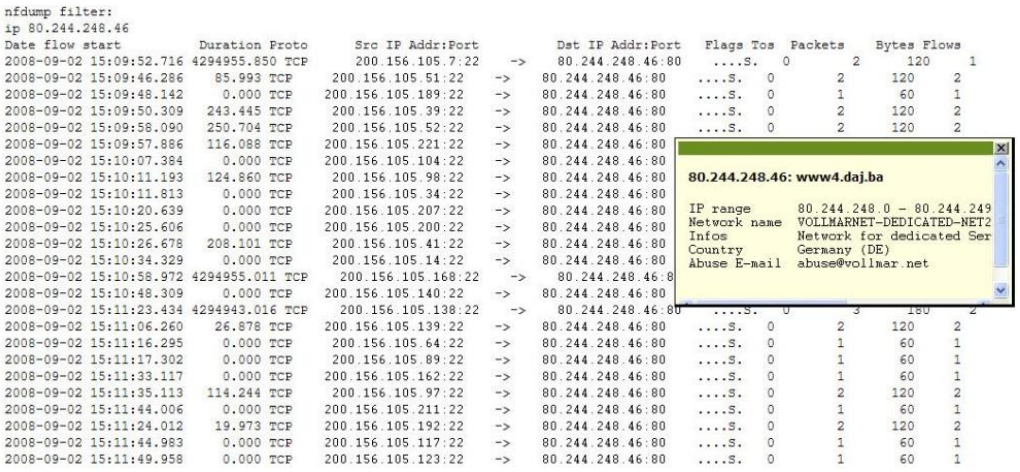


Figura IV-69 - DDOS a partir de hosts da rede 200.156.105.0.

4.20 Caso -5 - Ataque a hosts internacionais.

O caso 5 também possui uma característica muito presente durante o período de monitoramento. Situações onde os hosts internos atacavam hosts em países como China (Figura IV-70) e EUA, sugerindo o uso da rede da Universidade para guerra cibernética.

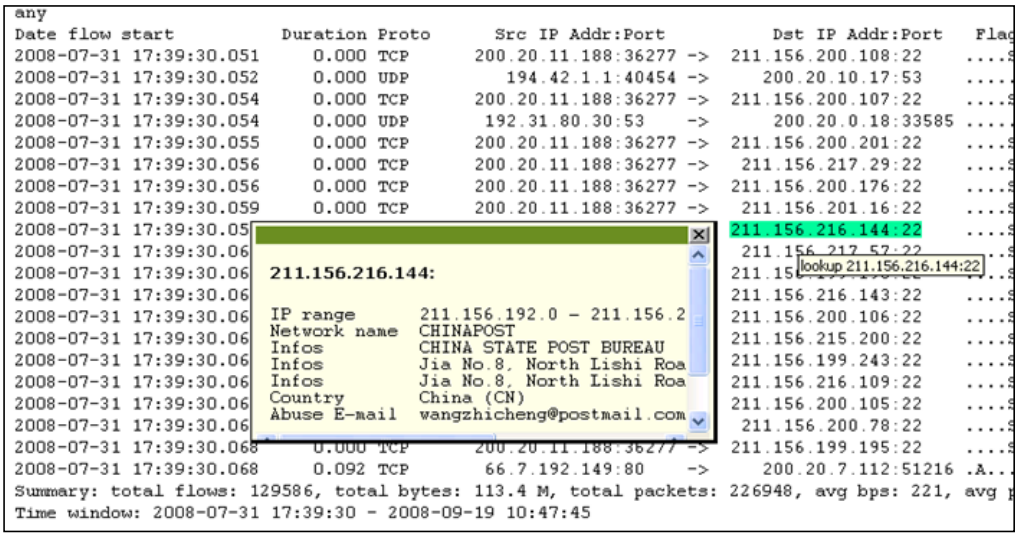


Figura IV-70 - Ataque Syn Flood partindo do endereço IP 200.20.11.188 (telemar.telecom.uff.br), para diversos IPs da China.

4.21 Caso 6 - Colocando a mãos no agressor

Muitos casos como que os que acabaram de ser mostrados se repetiram diariamente. Em um deles foi possível ter acesso a máquina para investigação. Tratava-se de uma estação de trabalho de um laboratório da Universidade, que foi invadida através de uma de suas contas com senha fraca do serviço de terminal remoto (SSH). Nesta máquina foram encontrados diversos scripts, cujos códigos tinham o objetivo de obter acesso a outros computadores utilizando ataques de dicionário.

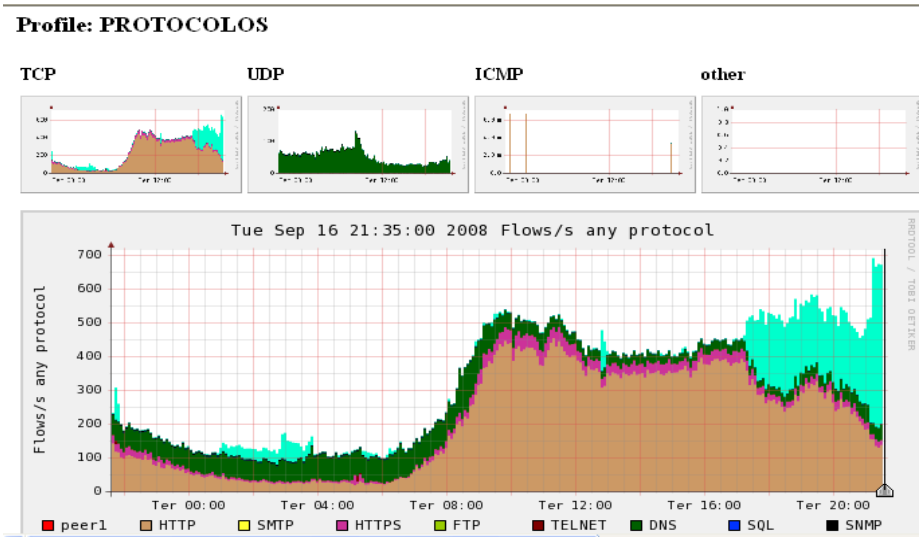
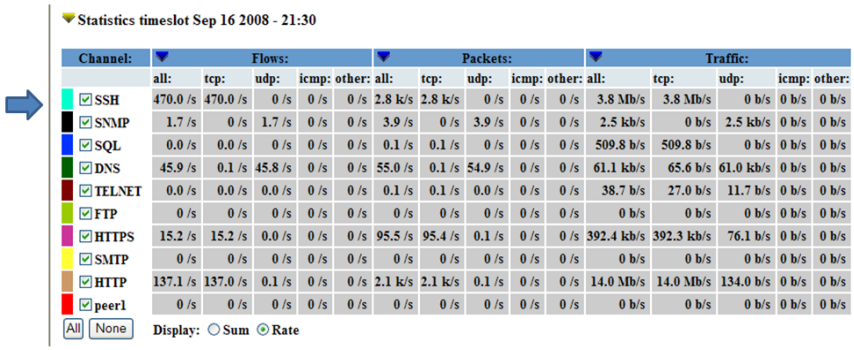


Figura IV-71 - Perfil PROTOCOLO apresentando alteração do PFR as 17:30 do dia 16/09/08.



Statistics timeslot Sep 16 2008 - 21:30

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
SSH	470.0 /s	470.0 /s	0 /s	0 /s	0 /s	2.8 k/s	2.8 k/s	0 /s	0 /s	0 /s	3.8 Mb/s	3.8 Mb/s	0 b/s	0 b/s	0 b/s
SNMP	1.7 /s	0 /s	1.7 /s	0 /s	0 /s	3.9 /s	0 /s	3.9 /s	0 /s	0 /s	2.5 kb/s	0 b/s	2.5 kb/s	0 b/s	0 b/s
SQL	0.0 /s	0.0 /s	0 /s	0 /s	0 /s	0.1 /s	0.1 /s	0 /s	0 /s	0 /s	509.8 b/s	509.8 b/s	0 b/s	0 b/s	0 b/s
DNS	45.9 /s	0.1 /s	45.8 /s	0 /s	0 /s	55.0 /s	0.1 /s	54.9 /s	0 /s	0 /s	61.1 kb/s	65.6 b/s	61.0 kb/s	0 b/s	0 b/s
TELNET	0.0 /s	0.0 /s	0.0 /s	0 /s	0 /s	0.1 /s	0.1 /s	0.0 /s	0 /s	0 /s	38.7 b/s	27.0 b/s	11.7 b/s	0 b/s	0 b/s
FTP	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 b/s	0 b/s	0 b/s	0 b/s	0 b/s
HTTPS	15.2 /s	15.2 /s	0.0 /s	0 /s	0 /s	95.5 /s	95.4 /s	0.1 /s	0 /s	0 /s	392.4 kb/s	392.3 kb/s	76.1 b/s	0 b/s	0 b/s
SMTP	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 b/s	0 b/s	0 b/s	0 b/s	0 b/s
HTTP	137.1 /s	137.0 /s	0.1 /s	0 /s	0 /s	2.1 k/s	2.1 k/s	0.1 /s	0 /s	0 /s	14.0 Mb/s	14.0 Mb/s	134.0 b/s	0 b/s	0 b/s
peer1	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 b/s	0 b/s	0 b/s	0 b/s	0 b/s

All None Display: Sum Rate

Figura IV-72 - Painel de informações de visualização de incidentes, indicando o valor de 470 fluxos por segundo.

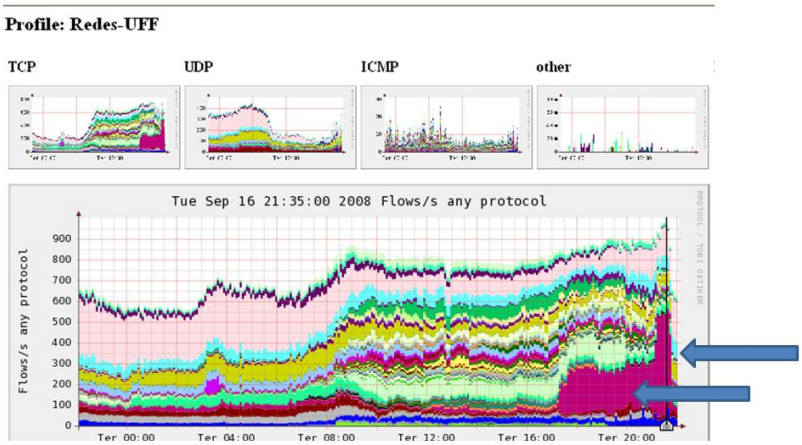


Figura IV-73 - Gráfico do Perfil RedesUff, mostrando um aumento da atividade da rede identificada pela cor lilás.

200_20_5_192	6.9 /s	5.1 /s	1.8 /s	0.1 /s	0 /s	148.4 /s	145.6 /s	1.9 /s	0.9 /s	0 /s	1.1 Mb/s	1.1 Mb/s	2.9 kb/s	472.8 b/s
200_156_105_128	1.4 /s	0.7 /s	0.7 /s	0 /s	0 /s	1.7 /s	1.0 /s	0.7 /s	0 /s	0 /s	754.4 b/s	405.0 b/s	349.4 b/s	0 b/s
200_20_10_96	0.0 /s	0 /s	0.0 /s	0 /s	0 /s	0.0 /s	0 /s	0.0 /s	0 /s	0 /s	8.5 b/s	0 b/s	8.5 b/s	0 b/s
200_20_10_64	477.4 /s	468.6 /s	8.4 /s	0.4 /s	0 /s	2.3 k/s	2.3 k/s	10.0 /s	2.1 /s	0 /s	2.6 Mb/s	2.6 Mb/s	11.2 kb/s	1.2 kb/s
200_20_10_32	0.1 /s	0.0 /s	0 /s	0.1 /s	0 /s	0.1 /s	0.0 /s	0 /s	0.1 /s	0 /s	36.3 b/s	3.8 b/s	0 b/s	32.4 b/s
200_20_10_0	15.7 /s	3.4 /s	11.9 /s	0.4 /s	0 /s	34.2 /s	20.4 /s	13.1 /s	0.7 /s	0 /s	96.1 kb/s	81.1 kb/s	14.7 kb/s	349.3 b/s
200_156_100_128	0.0 /s	0 /s	0.0 /s	0.0 /s	0 /s	0.0 /s	0 /s	0.0 /s	0.0 /s	0 /s	128.3 b/s	0 b/s	126.9 b/s	1.5 b/s
200_156_104_224	0.3 /s	0.1 /s	0.2 /s	0.0 /s	0 /s	5.5 k/s	5.5 k/s	0.3 /s	0.0 /s	0 /s	48.5 Mb/s	48.5 Mb/s	298.7 b/s	24.5 b/s
200_156_108_192	0.1 /s	0 /s	0.1 /s	0.0 /s	0 /s	0.1 /s	0 /s	0.1 /s	0.0 /s	0 /s	38.6 b/s	0 b/s	29.6 b/s	9.0 b/s
200_156_108_224	0.0 /s	0 /s	0 /s	0.0 /s	0 /s	0.0 /s	0 /s	0 /s	0.0 /s	0 /s	11.4 b/s	0 b/s	0 b/s	11.4 b/s

Figura IV-74 - Painel de visualização do sistema Nfsen, mostrando a rede 200.20.10.64, com elevada quantidade de fluxos.

```
** nfdump -M /usr/local/nfsen/nfsen/profiles-data/PROTOCOLOS/SSH:SNMP:SQL:DNS:TELNET:FTP:HTTPS:SMTP:HTTP:peer1  -I
nfdump filter:
any
Top 10     IP Addr ordered by flows:
Date first seen          Duration Proto          IP Addr     Flows  Packets     Bytes      pps      bps   bpp
2008-09-16 21:29:33.363 4295292.920 any       200.20.10.73   138753   764451   88.2 M        0      172   121
2008-09-16 21:29:33.365 4295292.916 any       200.20.0.21      5886    82883   63.4 M        0      123   801
2008-09-16 21:29:33.347 4295265.506 any       200.20.0.18      5354     6514   878158        0        1   134
2008-09-16 21:29:33.355 4295269.334 any       200.20.10.17     5260     6905    1.6 M        0        3   249
2008-09-16 21:29:36.068 4295269.163 any       200.20.1.180     3568   157595  135.4 M        0      264   901
2008-09-16 21:29:33.363 4295265.516 any       201.3.56.94      2851    10356   993658        0        1    95
2008-09-16 21:29:33.484 4295265.385 any       201.3.56.102     2838    10292   984776        0        1    95
2008-09-16 21:29:33.649 4295265.225 any       201.3.56.226     2763    10025   957132        0        1    95
2008-09-16 21:29:33.802 4295265.063 any       201.3.56.202     2739    10083   954226        0        1    94
2008-09-16 21:29:35.812 4295287.708 any       200.156.108.2    2734    13174    6.4 M        0       12   509

Summary: total flows: 201024, total bytes: 652.1 M, total packets: 1.4 M, avg bps: 1273, avg pps: 0, avg bpp: 452
Time window: 2008-09-16 21:29:33 - 2008-11-05 15:37:46
Total flows processed: 201024, Records skipped: 0, Bytes read: 10453452
Sys: 0.059s flows/second: 3350958.5   Wall: 0.349s flows/second: 575797.1
```

Figura IV-75 – Relatório mostrando os 10 endereços IPs da UFF com maior registros de fluxos. O IP 200.20.10.73 é o primeiro da lista.

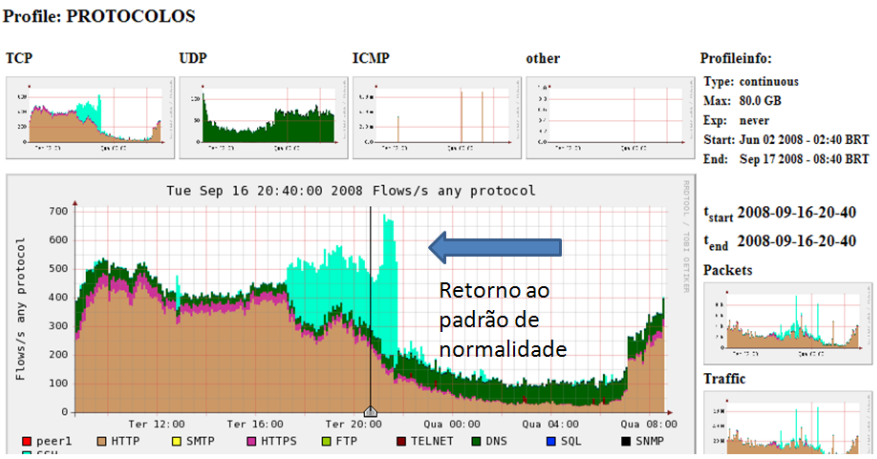


Figura IV-76 - Perfil PROTOCOLOS, mostrando que após o desligamento do computador que utilizava o IP 200.20.10.73, o gráfico voltou ao PFR anterior.

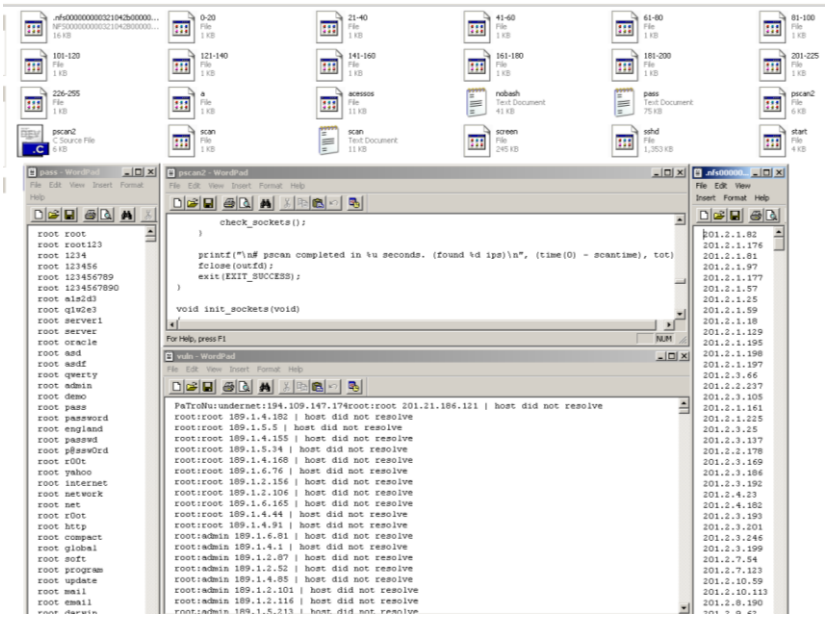


Figura IV-77 – Arquivos encontrados na máquina 200.20.10.73

Novamente, o mesmo procedimento de identificação do incidente foi adotado. Inicialmente através do perfil PROTOCOLOS, (Figura IV-71 e Figura IV-72) onde é possível verificar que a porta 22 apresenta um aumento repentino de utilização. No perfil RedesUFF é possível identificar a rede que está gerando a atividade (Figura IV-73 e Figura IV-74) e finalmente na Figura IV-75, é possível identificar o endereço IP utilizado (200.20.10.73). Após a identificação do endereço IP foi feito contato com os administradores da respectiva rede para que desligassem a máquina. Foi possível ter acesso ao computador onde após pesquisa nos logs do sistema, foi identificado que o método de acesso foi feito através da quebra de uma das senhas de usuário de composição fraca. No sistema de arquivos foram encontrados diversos scripts (Figura IV-77), cujo algoritmo tinha o objetivo de vasculhar redes específicas em busca de máquinas rodando aplicativos de acesso remoto. Uma vez identificadas os endereços outra parte do código se encarregava de disparar um ataque de dicionário, do tipo força bruta, na tentativa de ter acesso a máquina. A Figura IV-76 mostra que após o desligamento da máquina o incidente foi finalizado, mostrando que o mesmo partia do referido host.

```
flows: 2247 bytes: 47.2 M packets: 64053
flows: 1571 bytes: 19.6 M packets: 31647
flows: 1809 bytes: 41.8 M packets: 56939
flows: 971 bytes: 30.1 M packets: 38715
flows: 1131 bytes: 29.0 M packets: 49854
flows: 1222 bytes: 44.1 M packets: 51943
flows: 1220 bytes: 44.4 M packets: 51423
flows: 1103 bytes: 36.3 M packets: 44418
flows: 1048 bytes: 46.0 M packets: 54277
flows: 1619 bytes: 33.5 M packets: 42894
flows: 1147 bytes: 23.2 M packets: 35931
flows: 1902 bytes: 34.6 M packets: 48734
flows: 3815 bytes: 60.3 M packets: 81624
flows: 2960 bytes: 69.7 M packets: 89239
flows: 3316 bytes: 79.3 M packets: 95791
flows: 3848 bytes: 28.5 M packets: 51623
flows: 2492 bytes: 26.4 M packets: 43722
flows: 2760 bytes: 21.1 M packets: 38411
flows: 2531 bytes: 22.7 M packets: 37734
flows: 4374 bytes: 36.0 M packets: 58411
flows: 2236 bytes: 22.6 M packets: 44863
flows: 3005 bytes: 40.8 M packets: 61940
flows: 2187 bytes: 65.5 M packets: 71682
flows: 2162 bytes: 108.7 M packets: 114849
flows: 2247 bytes: 47.2 M packets: 64053
flows: 1571 bytes: 19.6 M packets: 31647
flows: 1809 bytes: 41.8 M packets: 56939
flows: 971 bytes: 30.1 M packets: 38715
flows: 1131 bytes: 29.0 M packets: 49854
flows: 1222 bytes: 44.1 M packets: 51943
flows: 1220 bytes: 44.4 M packets: 51423
flows: 1103 bytes: 36.3 M packets: 44418
flows: 1048 bytes: 46.0 M packets: 54277
flows: 1619 bytes: 33.5 M packets: 42894
flows: 1147 bytes: 23.2 M packets: 35931
flows: 1902 bytes: 34.6 M packets: 48734
flows: 3815 bytes: 60.3 M packets: 81624
flows: 2960 bytes: 69.7 M packets: 89239
flows: 3316 bytes: 79.3 M packets: 95791
flows: 3848 bytes: 28.5 M packets: 51623
flows: 2492 bytes: 26.4 M packets: 43722
flows: 2760 bytes: 21.1 M packets: 38411
flows: 2531 bytes: 22.7 M packets: 37734
```

Figura IV-78 - Extração dos sumários dos arquivos contendo 5 minutos de tráfego da rede 200.20.7.0, gerados entre Janeiro e Abril de 2009.

Quantidade de amostras	34500
Maior valor encontrado	72588
Média	2370,5
Quantidade de valores acima da média	13077
Desvio padrão	2863,61
Média+Desvio padrão	5234,11
Duas vezes o desvio padrão	5727,22

Figura IV-79 - Resultado dos cálculos efetuados em planilha eletrônica, dos sumários extraídos dos arquivos gerados em intervalos de 5 minutos, visando obter os valores de referência para uso no alerta de segurança da rede 200.20.7.0

30778	103		disparou
23313	78		disparou
27110	90		disparou
29018	97		disparou
18177	61		disparou
32512	108		disparou
32764	109		disparou
34324	114		disparou
31074	104		disparou
22054	74		disparou
42613	142		disparou
39609	132		disparou
34966	117		disparou
33423	111		disparou
28414	95		disparou
31874	106		disparou
29282	98		disparou
31303	104		disparou
23726	79		disparou
34323	114		disparou
45013	150		disparou
50301	168		disparou
38119	127		disparou
30017	100		disparou
28386	95		disparou
26589	89		disparou

Figura IV-80 - Simulação efetuada na planilha a partir dos dados importados.

4.22 Programando alertas

Após o período de monitoramento detectando os incidentes de segurança a partir da observação dos gráficos, buscou-se alternativas para automatizar este processo. Os mais de quarenta casos de segurança registrados durante o período (Figura IV-64) mostraram que houve expressivas elevações da quantidade de fluxos durante a ocorrência dos incidentes. Com base nessas informações, buscou-se uma forma de programar os alertas de acordo com as etapas a seguir:

1. Preparação e execução de scripts para extrair dos arquivos do sistema de monitoramento as informações referentes à quantidade de fluxos gerados por determinada rede.
2. Importação do arquivo resultante da execução do script em planilha eletrônica, de modo a calcular os valores de referência a serem utilizados para a programação do alerta.
3. Programação dos alertas no sistema Nfsen.
4. Avaliação dos alertas emitidos pelo sistema.

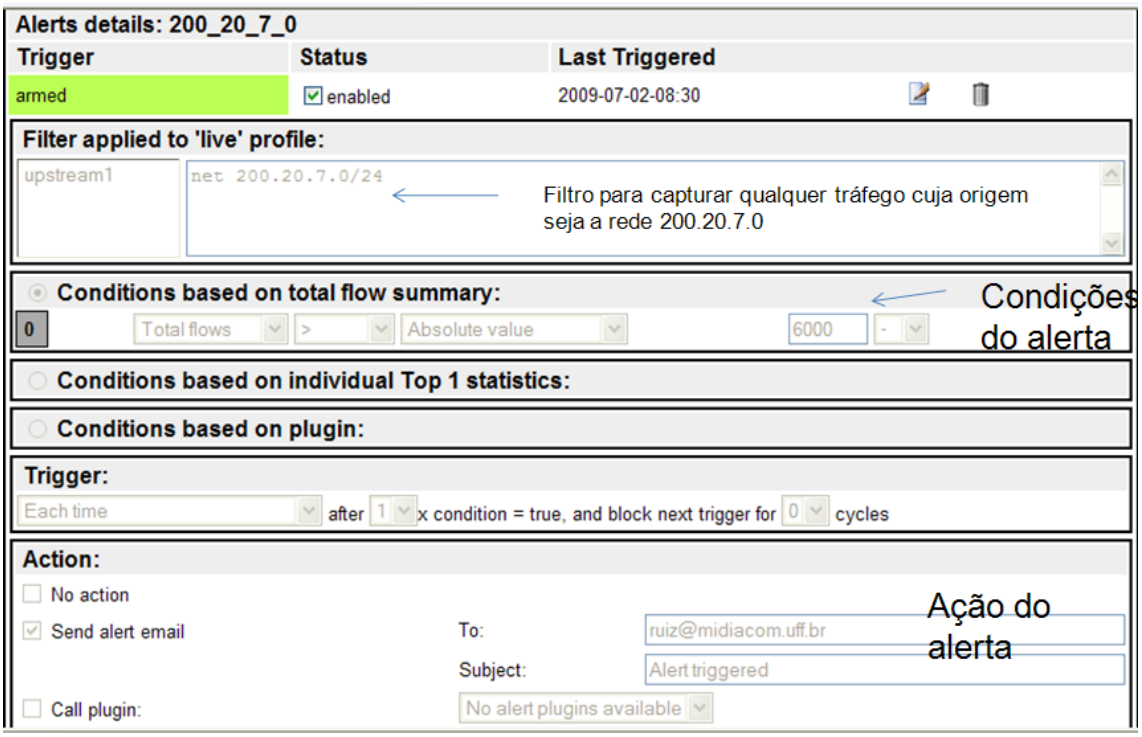


Figura IV-81 - Tela de configuração de alertas do sistema Nfsen.

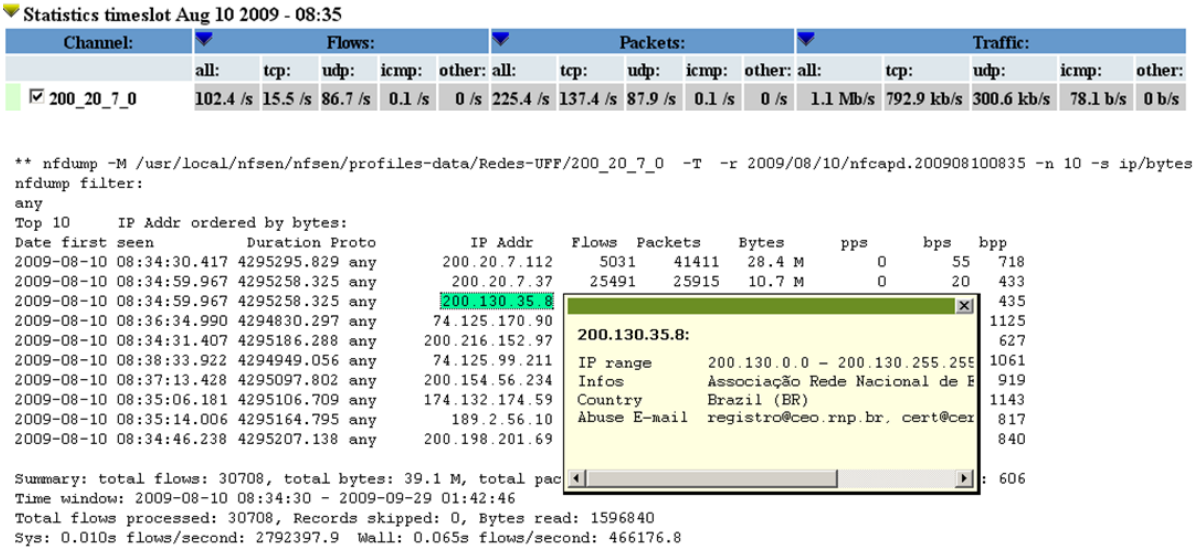


Figura IV-82 - IP 200.20.7.37 gerando 25491 fluxos/s direcionados ao IP 200.130.35.8

Os testes foram realizados utilizando uma funcionalidade do sistema Nfsen que permite programar alertas em função do acompanhamento das variáveis: fluxos, pacotes e bytes. Para a programação do alerta foi utilizado a variável fluxos conforme mostra a Figura IV-81. Após a execução dos scripts, os dados resultantes foram importados (Figura IV-78) para uma planilha eletrônica onde foram realizados os cálculos. A análise das

amostras apresentou correspondência a uma distribuição normal. O objetivo dos cálculos foi encontrar o valor ideal para que os alertas só fossem emitidos quando a quantidade de fluxos alcançasse índices que estivessem fora do padrão de funcionamento da rede (PFR). Por este motivo foi utilizado como referencia duas vezes o desvio padrão, com o arredondamento para cima (Figura IV-79). A rede utilizada para os testes foi a de endereço 200.20.7.0 e o período compreendido entre janeiro e abril de 2009.

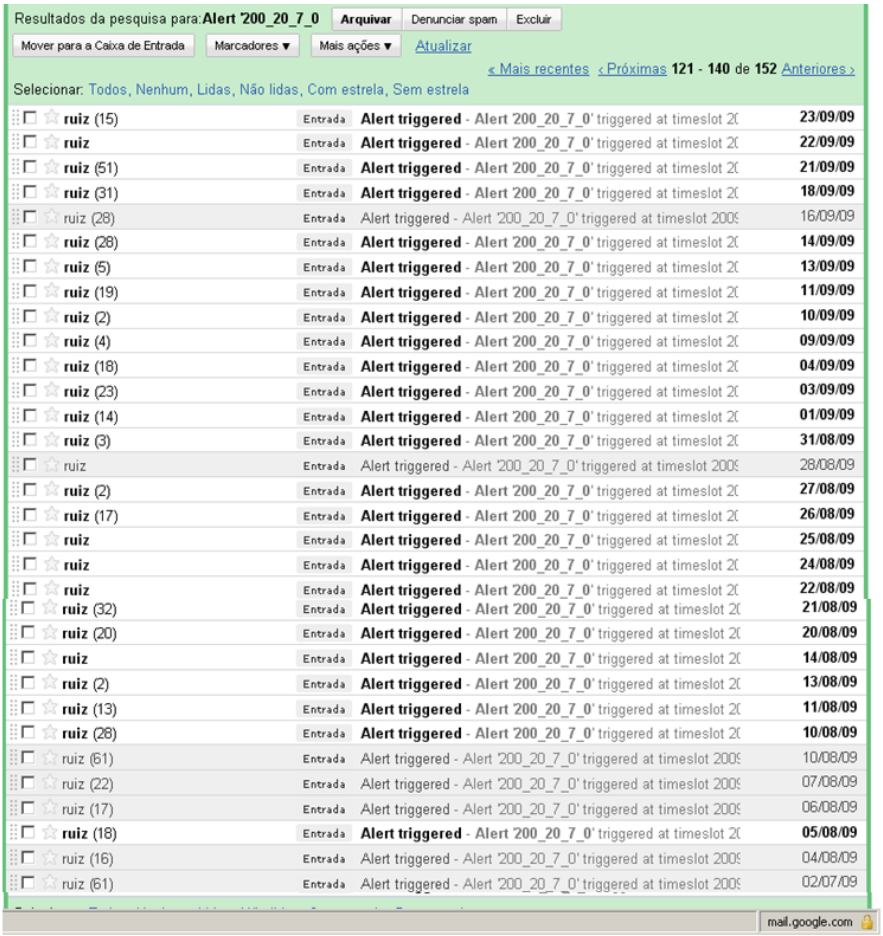


Figura IV-83 - Alertas disparados pelo sistema Nfsen entre julho e setembro de 2009. O número entre parênteses representa a quantidade de alertas recebidos no dia.

4.23 Analisando os alertas emitidos

Foram coletados alertas emitidos entre julho e setembro de 2009. Durante a análise foi constatado que alguns alertas foram emitidos pelo mesmo agente e que isto se repetiu durante todo o período de teste, de forma regular. Foi o caso do endereço IP 200.20.7.37, que fazia acessos com expressiva quantidade de fluxos (25491 fluxos/s) ao

endereço ip 200.130.35.8. A análise dos fluxos não evidenciou nenhum incidente de segurança. Considerando que os acessos eram direcionados a um único endereço (200.130.25.8), registrado para uma instituição parceira da UFF (Rede Nacional de Ensino e Pesquisa), acreditamos que os mesmos fossem de interesse das instituições. Neste caso um opção seria aplicar um filtro de modo que o sistema não emitisse alertas para os fluxos estabelecidos entre estes dois endereços.

Figura IV-84 - Informações sobre o alerta emitido no dia 02 de julho de 2009

Em outro caso, o endereço 200.20.7.112 acessou 1882 vezes o endereço 201.49.208.251 registrado como www.parperfeito.com.br (Figura IV-85), que somados à carga existente na rede fez com que o alerta fosse emitido. Para efeito do teste, foi feito o bloqueio do referido endereço acessado. Isto restabeleceu o PFR, conforme mostra a Figura IV-86, e o alerta deixou de ser emitido.

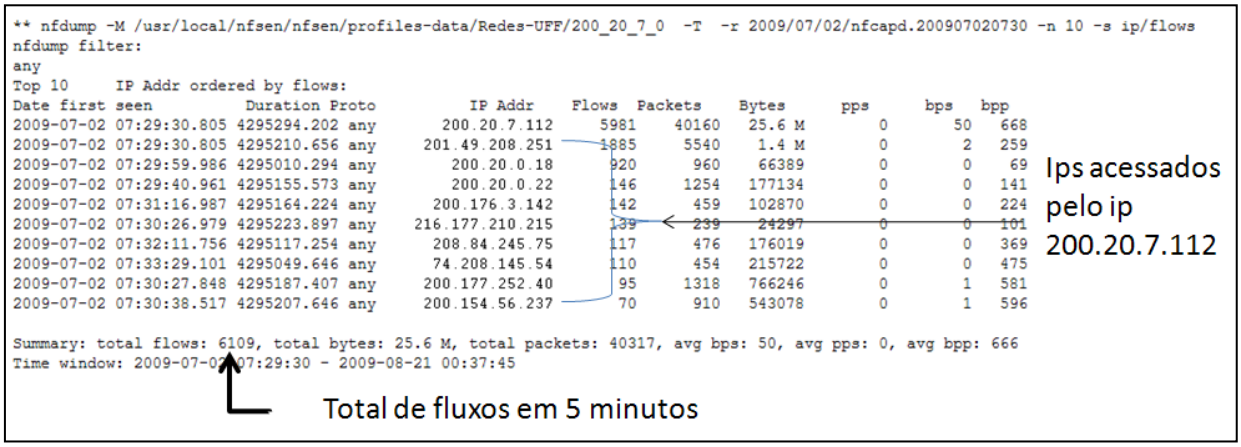


Figura IV-85 - Resultado da consulta ao sistema Nfsen, no intervalo de tempo indicado no alerta (02/07/2009 às 7:30).

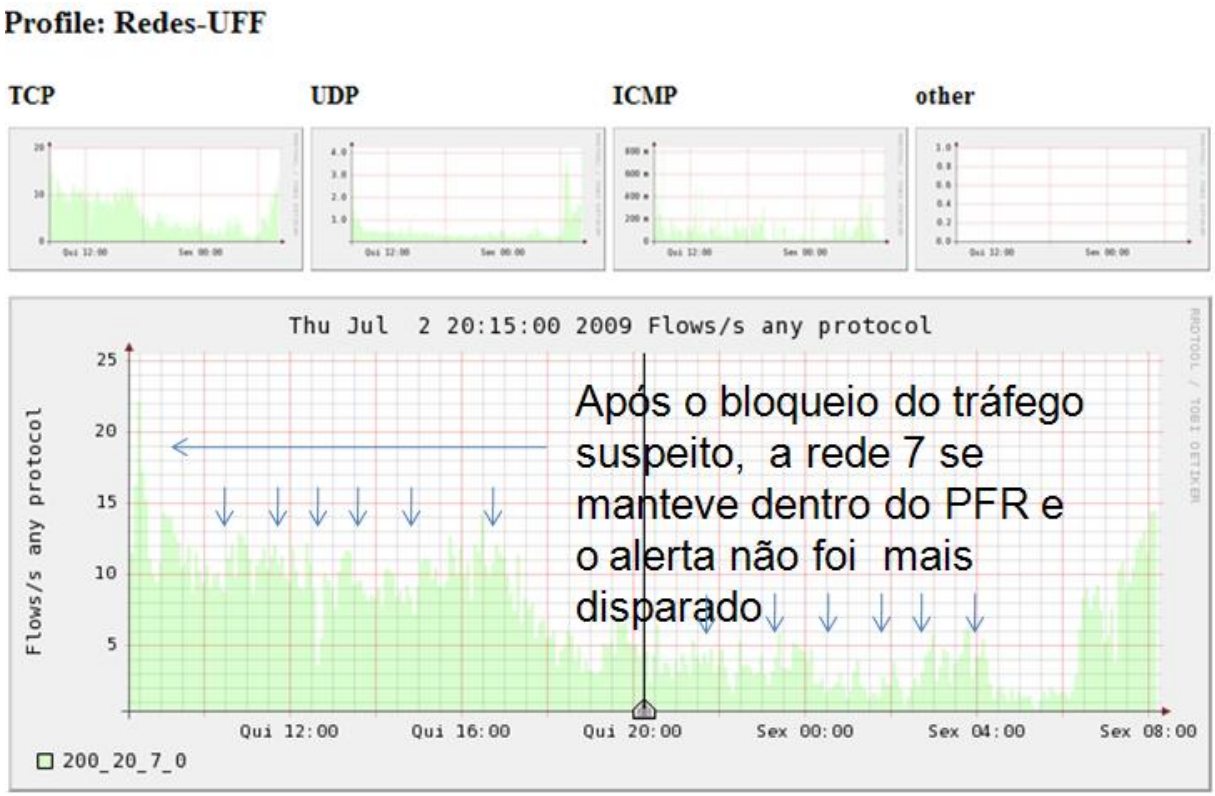


Figura IV-86 - Retorno ao PFR após bloqueio do trafego suspeito.

A hora do alerta, 07h30min da manhã, chamou atenção, pois, com base em registros anteriores, a rede deveria estar ociosa. Isto mostrou como as informações do PFR associadas ao tempo, contribuem para a identificação dos incidentes. Assim, consideramos que os cálculos que irão determinar os padrões de funcionamento da rede, deverão considerar diferentes períodos de funcionamento da rede, como por exemplo:

- 6h às 12h;
- 12h às 18h;
- 18h às 24h; e
- 24h e 6h.

Além disso, deverão ser considerados os finais de semana e feriados prolongados, do contrário, haverá comprometimento da eficácia dos alertas. Assim, para efeito de detecção de incidentes de segurança é necessário calcular a provável carga da rede, para cada período de funcionamento da mesma, evitando assim, emitir alertas falsos ou de não emitir alertas verdadeiros.

O último alerta analisado é apresentado na Figura IV-87, onde o endereço IP 200.20.7.147, é acessado por diversos endereços da Internet, utilizando o protocolo UDP na porta 15395. O comportamento observado se assemelha ao Caso 2, sugerindo a utilização de aplicativos Peer-to-Peer.

Statistics timeslot Sep 10 2009 - 08:15

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
☑ 200 20 7 0	24.1 /s	19.5 /s	3.9 /s	0.7 /s	0 /s	99.8 /s	95.2 /s	3.9 /s	0.7 /s	0 /s	475.6 kb/s	473.1 kb/s	2.1 kb/s	348.9 b/s	0 b/s

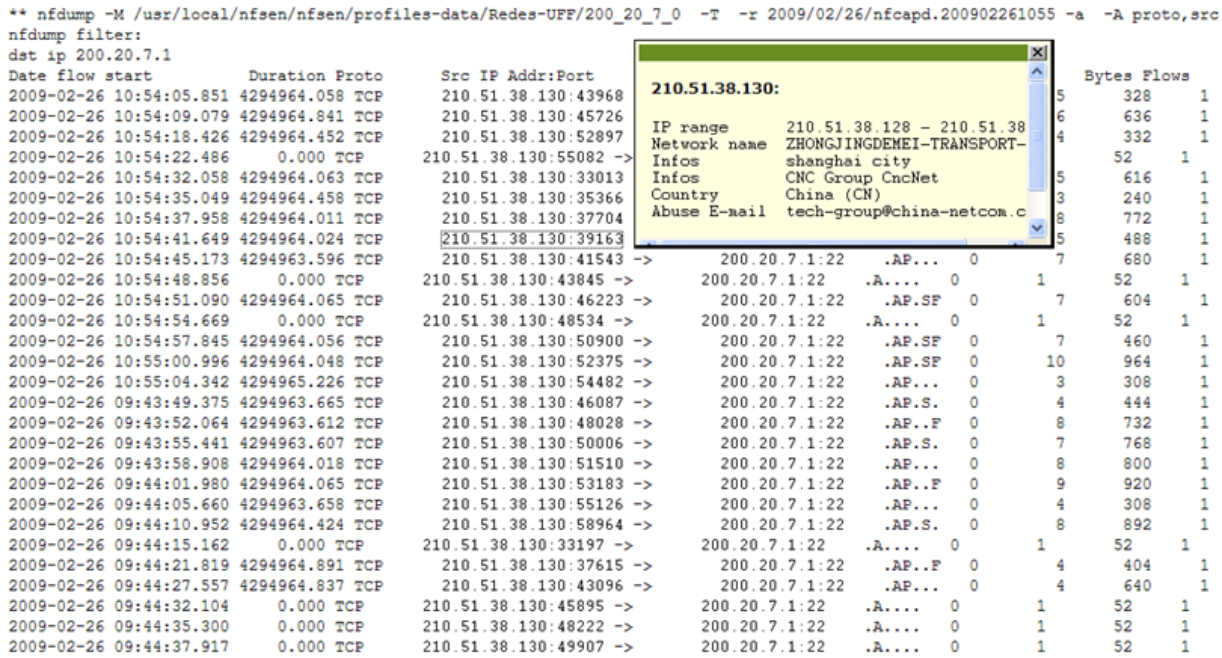
```
** nfdump -M /usr/local/nfsen/nfsen/profiles-data/Redes-UFF/200_20_7_0  -T  -r 2009/09/10/nfcapd.200909100815 -a  -A proto,sr
nfdump filter:
dst ip 200.20.7.147
```

Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Flags	Tos	Packets	Bytes	Flows
2009-09-10 08:14:59.976	0.000	UDP	123.232.114.68:32471	->	200.20.7.147:15395	.....	0	1	69	1
2009-09-10 08:14:59.989	0.000	UDP	221.1.104.196:3925	->	200.20.7.147:15395	.....	0	1	68	1
2009-09-10 08:14:59.972	0.000	UDP	221.207.186.75:36569	->	200.20.7.147:15395	.....	0	1	69	1
2009-09-10 08:14:59.987	161.986	UDP	119.184.155.75:27646	->	200.20.7.147:15395	.....	0	4	278	4
2009-09-10 08:15:00.943	0.000	UDP	60.7.98.21:61148	->	200.20.7.147:15395	.....	0	1	70	1
2009-09-10 08:15:03.978	76.996	UDP	218.25.40.114:1760	->	200.20.7.147:15395	.....	0	3	207	3
2009-09-10 08:15:03.976	8.016	UDP	221.1.223.2:41074	->	200.20.7.147:15395	.....	0	2	137	2
2009-09-10 08:15:03.975	0.000	UDP	61.161.131.18:12123	->	200.20.7.147:15395	.....	0	1	70	1
2009-09-10 08:15:03.974	40.020	UDP	60.211.253.18:13542	->	200.20.7.147:15395	.....	0	4	277	4
2009-09-10 08:15:03.975	0.000	UDP	221.0.95.252:62848	->	200.20.7.147:15395	.....	0	1	68	1
2009-09-10 08:15:03.975	0.000	UDP	221.1.178.123:23673	->	200.20.7.147:15395	.....	0	1	70	1
2009-09-10 08:15:04.971	37.012	UDP	221.213.253.11:1166	->	200.20.7.147:15395	.....	0	2	136	2
2009-09-10 08:15:05.982	11.978	UDP	218.28.172.166:1036	->	200.20.7.147:15395	.....	0	3	212	3
2009-09-10 08:15:05.973	272.001	UDP	221.6.98.2:18246	->	200.20.7.147:15395	.....	0	5	343	5
2009-09-10 08:15:05.969	0.000	UDP	221.215.141.213:8183	->	200.20.7.147:15395	.....	0	1	71	1
2009-09-10 08:15:06.988	3.995	UDP	125.46.18.74:15000	->	200.20.7.147:15395	.....	0	2	141	2
2009-09-10 08:15:07.974	4.015	UDP	122.193.48.43:43803	->	200.20.7.147:15395	.....	0	2	141	2
2009-09-10 08:15:07.956	36.025	UDP	58.16.70.32:15488	->	200.20.7.147:15395	.....	0	4	276	4
2009-09-10 08:15:09.992	7.956	UDP	60.211.112.86:21825	->	200.20.7.147:15395	.....	0	2	139	2
2009-09-10 08:15:09.992	31.992	UDP	60.210.100.142:1065	->	200.20.7.147:15395	.....	0	2	140	2
2009-09-10 08:15:09.995	39.986	UDP	60.220.252.130:14312	->	200.20.7.147:15395	.....	0	5	349	5
2009-09-10 08:15:09.997	240.982	UDP	124.130.150.173:21520	->	200.20.7.147:15395	.....	0	7	482	7
2009-09-10 08:15:09.990	85.990	UDP	116.245.113.20:2093	->	200.20.7.147:15395	.....	0	7	483	7
2009-09-10 08:15:09.992	0.000	UDP	60.212.250.66:2013	->	200.20.7.147:15395	.....	0	1	68	1
2009-09-10 08:15:09.977	44.000	UDP	125.46.18.2:19101	->	200.20.7.147:15395	.....	0	3	210	3
2009-09-10 08:15:09.990	0.000	UDP	218.58.156.10:5197	->	200.20.7.147:15395	.....	0	1	69	1
2009-09-10 08:15:11.995	196.982	UDP	221.203.152.162:29406	->	200.20.7.147:15395	.....	0	8	535	8
2009-09-10 08:15:11.993	31.991	UDP	221.212.98.202:14447	->	200.20.7.147:15395	.....	0	3	208	3
2009-09-10 08:15:11.994	31.989	UDP	123.130.206.245:9767	->	200.20.7.147:15395	.....	0	2	137	2
2009-09-10 08:15:12.994	25.987	UDP	60.212.158.24:11730	->	200.20.7.147:15395	.....	0	2	139	2
2009-09-10 08:15:13.993	35.994	UDP	61.53.134.244:10600	->	200.20.7.147:15395	.....	0	3	211	3

Figura IV-87 - Resultado da análise do alerta emitido no dia 10/09/2009. Endereço 200.20.7.147 sendo acessado por diversos endereços da Internet.

4.24 Simulando alertas

Com base no valor de referência (6000 fluxos a cada 5 minutos), utilizado na programação de alertas através do sistema Nfsen, foi realizada uma simulação a partir dos fluxos importados na planilha eletrônica (Figura IV-80). O teste consistiu em uma fórmula para localizar os valores acima de 6000, escrevendo ao lado a palavra "disparou". A partir da identificação dos registros procurados, foi realizada uma consulta ao sistema Nfsen, tendo como base a data e a hora. Os resultados foram os endereços que provocaram a elevação da quantidade de fluxos. Um destes casos pode ser visualizado na Figura IV-88.



```
** nfdump -M /usr/local/nfsen/nfsen/profiles-data/Redes-UFF/200_20_7_0  -T  -r 2009/02/26/nfcapd.200902261055 -a  -A proto,src
nfdump filter:
dst ip 200.20.7.1
Date flow start          Duration Proto      Src IP Addr:Port                                                  Bytes Flows
2009-02-26 10:54:05.851 4294964.058 TCP      210.51.38.130:43968                                                 328     1
2009-02-26 10:54:09.079 4294964.841 TCP      210.51.38.130:45726                                                 636     1
2009-02-26 10:54:18.426 4294964.452 TCP      210.51.38.130:52897                                                 332     1
2009-02-26 10:54:22.486     0.000 TCP      210.51.38.130:55082 ->                                               52     1
2009-02-26 10:54:32.058 4294964.063 TCP      210.51.38.130:33013                                                 616     1
2009-02-26 10:54:35.049 4294964.458 TCP      210.51.38.130:35366                                                 240     1
2009-02-26 10:54:37.958 4294964.011 TCP      210.51.38.130:37704                                                 772     1
2009-02-26 10:54:41.649 4294964.024 TCP      210.51.38.130:39163                                                 488     1
2009-02-26 10:54:45.173 4294963.596 TCP      210.51.38.130:41543 ->      200.20.7.1:22    .AP...   0   7      680     1
2009-02-26 10:54:48.856     0.000 TCP      210.51.38.130:43845 ->      200.20.7.1:22    .A....   0   1       52     1
2009-02-26 10:54:51.090 4294964.065 TCP      210.51.38.130:46223 ->      200.20.7.1:22    .AP.SF   0   7      604     1
2009-02-26 10:54:54.669     0.000 TCP      210.51.38.130:48534 ->      200.20.7.1:22    .A....   0   1       52     1
2009-02-26 10:54:57.845 4294964.056 TCP      210.51.38.130:50900 ->      200.20.7.1:22    .AP.SF   0   7      460     1
2009-02-26 10:55:00.996 4294964.048 TCP      210.51.38.130:52375 ->      200.20.7.1:22    .AP.SF   0  10      964     1
2009-02-26 10:55:04.342 4294965.226 TCP      210.51.38.130:54482 ->      200.20.7.1:22    .AP...   0   3      308     1
2009-02-26 09:43:49.375 4294963.665 TCP      210.51.38.130:46087 ->      200.20.7.1:22    .AP.S.   0   4      444     1
2009-02-26 09:43:52.064 4294963.612 TCP      210.51.38.130:48028 ->      200.20.7.1:22    .AP..F   0   8      732     1
2009-02-26 09:43:55.441 4294963.607 TCP      210.51.38.130:50006 ->      200.20.7.1:22    .AP.S.   0   7      768     1
2009-02-26 09:43:58.908 4294964.018 TCP      210.51.38.130:51510 ->      200.20.7.1:22    .AP...   0   8      800     1
2009-02-26 09:44:01.980 4294964.065 TCP      210.51.38.130:53183 ->      200.20.7.1:22    .AP..F   0   9      920     1
2009-02-26 09:44:05.660 4294963.658 TCP      210.51.38.130:55126 ->      200.20.7.1:22    .AP...   0   4      308     1
2009-02-26 09:44:10.952 4294964.424 TCP      210.51.38.130:58964 ->      200.20.7.1:22    .AP.S.   0   8      892     1
2009-02-26 09:44:15.162     0.000 TCP      210.51.38.130:33197 ->      200.20.7.1:22    .A....   0   1       52     1
2009-02-26 09:44:21.819 4294964.891 TCP      210.51.38.130:37615 ->      200.20.7.1:22    .AP..F   0   4      404     1
2009-02-26 09:44:27.557 4294964.837 TCP      210.51.38.130:43096 ->      200.20.7.1:22    .AP...   0   4      640     1
2009-02-26 09:44:32.104     0.000 TCP      210.51.38.130:45895 ->      200.20.7.1:22    .A....   0   1       52     1
2009-02-26 09:44:35.300     0.000 TCP      210.51.38.130:48222 ->      200.20.7.1:22    .A....   0   1       52     1
2009-02-26 09:44:37.917     0.000 TCP      210.51.38.130:49907 ->      200.20.7.1:22    .A....   0   1       52     1

210.51.38.130:

IP range      210.51.38.128 - 210.51.38
Network name  ZHONGJINGDEMEI-TRANSPORT-
Infos         shanghai city
Infos         CNC Group CncNet
Country       China (CN)
Abuse E-mail  tech-group@china-netcom.c
```

Figura IV-88 - Resultado da consulta ao sistema Nfsen, tendo como base a data e hora, obtidos através da simulação feita na planilha, mostrando que um ataque externo foi desferido contra o ip 200.20.7.1, utilizando a porta 22.

4.25 Recomendações

Fica evidente durante todo o trabalho que, analisando a rede a partir das subredes, percebe-se diferentes resultados, originados pelos diferentes grupos de usuários. Assim podemos dizer que os interesses dos usuários são expressos durante o monitoramento da rede sob a forma do PFR. Neste sentido, salientamos a relevância do monitoramento de fluxos que, diferentemente do monitoramento de bytes e pacotes, tornam-se informações úteis imediatamente, uma vez que um fluxo traz em si mesmo dados

valiosos como origem e destino das comunicações, além de detalhes como as portas, que, em última análise, revelam as aplicações que deram origem à transmissão.

Os testes realizados seguiram rotinas para detecção de incidentes de segurança no modo on-line e off-line (post-mortem). No modo on-line, a partir da detecção de alteração do PFR, por um determinado número de vezes, o sistema emitia um e-mail com informações que permitiram identificar o endereço IP do host causador do incidente. No modo Off-line, a partir do repositório de informações dos fluxos registrados pelo sistema para uma determinada rede, foi possível identificar o momento em que a rede apresentava alteração do PFR.

Se no modo on-line é possível fazer um trabalho reativo, no modo off-line é possível fazer um trabalho pesquisa, mapeando os host da rede que são recorrentes em incidentes, conhecendo aspectos mais subjetivos da utilização da rede. Além disso, é possível classificar a rede em os seus diversos estados de funcionamento, conforme relatado no capítulo II, item 2.2. A tabela IV evidencia as diferentes características entre um e outro método.

Tabela IV – Detecção de incidentes no modo on-line e off-line.

Detecção do incidente	Modo	Resultado
Aumento de fluxos de determinada rede, detectado a partir do funcionamento do sistema.	On-line	Recebimento email com informações sobre a rede relacionada, 5 minutos após o ocorrido
Pesquisa em repositório do sistema, em busca de valores que representem alterações do PFR.	Off-line	Localização de todas as ocorrências registradas no repositório.

Ambos os métodos se baseiam na determinação do PFR para cada rede. Este cálculo precisar ser aprimorado, a levando-se em consideração, por exemplo, outras variáveis

com data e hora, sem os quais corre-se o risco e emitir falsos alertas ou de não emitir alertas legítimos.

Se, a princípio, a idéia não é absurda, então não há esperança para ela.

Albert Einstein

Capítulo V Considerações Finais.

O uso das redes de computadores vem se tornando cada vez mais importante na vida das pessoas e organizações. A cada dia, mais e mais tarefas do mundo real vão sendo transferidas para o mundo virtual, ou seja, pagar contas, realizar aplicações financeiras, fazer compras e doações, marcar consultas médicas, comprar ingressos para espetáculos, assistir a filmes, pesquisar, corresponder-se e uma infinidade de outras atividades que vão sendo disponibilizadas na Internet, agora fazem parte da rotina de um número cada vez maior de pessoas. Podemos dizer que, dentro em breve, a conectividade à Internet se tornará um dos serviços essenciais como energia elétrica, telefone e tantos outros que a sociedade vem incorporando aos lares, escolas e empresas. Assim, aspectos como qualidade de serviço, estabilidade, capacidade e, principalmente, segurança precisam ser garantidos através de investimentos em tecnologias que contribuam para o funcionamento da rede em níveis minimamente aceitáveis.

Considerando as áreas de gerenciamento de redes, o monitoramento de redes configura-se com uma das tarefas mais importantes, por obter informações a partir dos dados trafegados nos elementos da rede, subsidiando ações que irão contribuir para a melhoria da segurança das comunicações, engenharia de tráfego, qualidade de serviço, caracterização de tráfego, e a muitos outros campos do conhecimento.

Dentre os protocolos de gerenciamento de rede, o mais conhecido e amplamente utilizado é o SNMP. Ele permite, a partir da leitura das MIBs, uma eficiente forma de gerenciamento. Entretanto, considerando a grande quantidade de dados a ser analisada e a necessidade de se obter um melhor entendimento sobre o comportamento do tráfego, um novo padrão de monitoramento baseado no registro de fluxos, (informações contidas no cabeçalho do protocolo TCP/IP), foi proposto pela CISCO SYSTEM com o nome de Netflow. Esta tecnologia, que está sendo padronizada pelo IETF com o nome de IPFIX

(*Ip Flow Information eXport),* é apontada por diversos autores como o futuro do monitoramento de redes, conforme descrito no Capitulo III, seção 2.6.

O estudo de caso apresentado no Capítulo III evidenciou as diferenças entre o protocolo SNMP e o protocolo Netflow. Foi possível monitorar a rede da UFF utilizando essas duas tecnologias, simultaneamente, através das ferramentas: CACTI (SNMP) e o Softflowd, em conjunto com o Nfdump e o Nfsen. O resultado obtido no sistema Nfsen referente ao volume de trafego registrado, em Mbit/s, foi comparado com os valores obtidos no sistema CACTI (SNMP). Após o término do período de monitoramento, as divergências detectadas entre as informações obtidas entre os dois sistemas foram reduzidas em função de ajustes efetuados nos parâmetros de configuração do sistema softflowd. Foi possível gerar gráficos representativos da quantidade de fluxos que trafegaram na rede, em função da diversidade de portas, IPs mais ativos e ter acesso de forma pesquisável e seletiva aos registros do tráfego que consideramos ser de suma importância para a gestão dos recursos da rede. A consulta detalhada aos arquivos resultantes do monitoramento permitiu cruzar informações que levaram à descoberta de aspectos antes ocultos pelo grande volume do tráfego, como foi evidenciado através dos casos de segurança mostrados no capítulo III. A criação dos perfis de monitoramento permitiu contabilizar o tráfego de cada rede, de forma individual. Esta técnica filtra o tráfego de cada rede em tempo de monitoramento e armazena-os em pastas independentes, favorecendo os trabalhos de pesquisa e contabilização do tráfego por endereço IP, porta e protocolos entre outros. Assim, foi possível conhecer os grandes consumidores de recursos e as redes associadas. Foi possível conhecer também as interações realizadas entre os IPs da universidade e diversos endereços da Internet.

As técnicas apresentadas aqui oferecem excelentes possibilidades, tanto para as pesquisas acadêmicas, como para as atividades operacionais da rede através dos seus administradores que se vem desafiados pela constante convergência de serviços para as redes IP. A capacidade de identificação do elemento gerador do trafego anômalo fazem a tecnologia de monitoramento de fluxo uma grande aliada dos profissionais que atuam na área de segurança de redes de computadores. Neste sentido, determinar os padrões de funcionamento da rede, a partir de formação de bases de dados sobre a origem e o destino do tráfego, permitirá a criação de sistemas inteligentes, que contribuam para o bom funcionamento da rede [33]. Esta automatização de processos constitui requisito

de fundamental importância para garantir o crescimento seguro da utilização dos sistemas em rede [34].

As tecnologias utilizadas neste trabalho buscaram conhecer as características do tráfego de cada rede, sua expressividade com relação ao total de recursos consumidos, além do impacto causado na Rede UFF como um todo. Os sumários existentes ao final de cada relatório (emitido pelo programa Nfdump) serviram para construção de *rankings* mensais, em função da quantidade de fluxos registrados. Inicialmente, os dados registrados a partir do perfil RedesUFF permitiram:

- Conhecer o universo das redes que mais consumiram os recursos da Rede UFF.
- Conhecer o universo das portas utilizadas por cada rede.
- Determinar o consumo dos recursos da rede, por porta, em relação ao consumo total da rede.
- Determinar o valor percentual do consumo dos recursos individuais de cada rede, em relação ao total registrado para a rede da UFF no período.
- Gerar os gráficos comparativos e de acompanhamento.
- Programar alertas em função da alteração do PRF da rede.
- Detectar o uso indevido dos recursos.

Demonstramos, desta forma, que os dados colhidos pelo sistema de monitoramento de fluxos formaram um valioso manancial de informações. Demonstramos ainda, que o registro da interação entre os hosts confere poder de decisão aos administradores, uma vez que a capacidade de visão daquilo que ocorre na rede é aumentado. Na prática, o tráfego de cada rede foi consolidado a cada cinco minutos, gerando ao final do dia, um conjunto de 288 arquivos (24 horas X 60 minutos / 5 minutos) onde foram obtidas, com riqueza de detalhes, as características individuais do funcionamento de cada rede e a este resultado denominamos PFR (Padrão de Funcionamento da Rede). Foi possível delimitar o universo das portas utilizadas pelas aplicações que consomem mais recursos, bem como gerar, através de consultas específicas, a contabilização dos sumários da atividade mensal da rede. Finalmente, foi possível comparar as redes, através da composição de um *ranking*, e acompanhar a variabilidade da posição de cada rede ao longo de cinco meses.

Com relação à segurança, ao contrário do método utilizado pelos sistemas IDS, a detecção de comportamentos anômalos praticada neste trabalho não analisou a formação dos pacotes ou fragmentos de códigos em base de dados [35], mas procurou estabelecer

níveis que, sendo ultrapassados, sinalizaram a ocorrência de alterações no PRF. Essas alterações foram percebidas a partir do monitoramento da conexão da UFF com a Internet. Isso permitiu programar alertas sem a necessidade de grandes gastos computacionais, pois a análise do tráfego se deu ao nível do cabeçalho do protocolo IP. Este procedimento pode ser comparado às técnicas utilizadas pelos sistemas IDPS.

Salientamos, entretanto, que o método utilizado para programação dos alertas foi apenas uma escolha inicial para realização dos testes. Com certeza, tal procedimento merece um tratamento adequado, de forma a sistematizar o cálculo dos valores de referência para qualquer rede. É importante ressaltar, ainda, que os processos que irão determinar os padrões de funcionamento deverão considerar diferentes períodos de funcionamento da rede. Além disso, deverão ser considerados os finais de semana e feriados prolongados. Assim, para efeito de detecção de incidentes que comprometem a segurança, é necessário calcular a provável carga da rede, para cada período de funcionamento da mesma, sob pena de se emitirem alertas falsos ou ignorarem alertas importantes [36]. Neste sentido, consideramos que este assunto deva ser objeto de trabalhos futuros.

Destacamos, neste trabalho, que a tecnologia de monitoramento de fluxos foi capaz de monitorar a rede de uma grande universidade de forma eficiente e eficaz, promovendo expressiva economia de recursos, uma vez que foi utilizado apenas um servidor e todos os softwares utilizados foram do tipo *open source*.

5.1 Trabalhos Futuros.

Como toda tecnologia em fase de padronização, o protocolo de monitoramento de fluxos (Netflow/Ipfix) ainda carece da evolução de muitas pesquisas, entretanto, pelo que vimos até agora, já podemos considerá-lo um grande aliado no monitoramento de grandes redes. Com relação à determinação do PFR, para efeito de detecção de comportamentos anômalos, como dissemos anteriormente, é necessário considerar os diferentes períodos de funcionamento da rede, pois a maioria das redes reduz drasticamente a atividade durante a noite, feriados e finais de semana. Nestas situações, um valor ajustado para disparar com a rede em atividade normal, não iria funcionar caso houvesse um ataque e a rede estivesse ociosa. Para resolver esta situação é necessário que os cálculos considerem a provável carga da rede para os diferentes horários. Assim,

uma fórmula que pretenda calcular o nível de fluxo limítrofe entre o funcionamento normal e a ocorrência de um comportamento anômalo deve minimamente considerar:

- Provável carga da rede para os diversos períodos.
- O horário de funcionamento da rede (manhã, tarde, noite e madrugada)
- O Qualificador de período (sábado, domingos e feriados)

Isso reduziria a probabilidade de erros que pudessem ocasionar alertas falsos ou a não emissão de alertas.

A experiência adquirida nesse trabalho mostra que a quantidade de fluxos de uma estação de trabalho pode variar de zero a centenas de fluxos por segundo, sendo que os limites superiores só foram observados em condições de comportamento anômalo. O estudo de caso mostrou que uma rede com 600 hosts manteve, em média, 20 fluxos por segundo; em contrapartida, vimos que um único host, em situações atípicas, foi capaz de gerar mais de 400 fluxos/s. Assim, consideramos ser importante evoluir os estudos no sentido de determinar os valores ideais para a quantidade de conexões máximas (ideais para uma estação de trabalho) que permitam a um usuário comum realizar suas atividades e, caso a segurança de seu equipamento venha a ser comprometida, que isto não cause prejuízos ao funcionamento da rede. Neste cenário, uma alternativa seria encontrar o valor ideal de conexões por segundo para ser atribuído às estações de trabalho e servidores da rede. A estratégia teria como objetivo evitar que os recursos disponíveis fossem consumidos por poucos ou por um único elemento. Neste sentido fazemos analogia ao cálculo do tamanho do tronco proposto por Erlang,[37] utilizado nas redes de telefonia, ou seja, com base em algumas variáveis obtidas após um período de monitoramento (como por exemplo: quantidade de hosts, servidores, valores médios de fluxos por segundo) calcular o valor ideal para o limite máximo de conexões por segundo abertas por cada elementos da rede. Com base nos experimentos realizados neste trabalho, no que tange as técnicas de detecção comportamentos anômalos na rede, verificamos que quanto mais próximas as informações coletadas estiverem dos elementos geradores de tráfego, menores serão as possibilidades de falsos positivos ou negativos. Sendo assim, acreditamos que seriam válidos experimentos que levassem em consideração o padrão de funcionamento de cada host ao invés de um conjunto de hosts

como foi o caso do PFR. Neste sentido identificamos em [38] a utilização da técnica denominada *exponential smoothing*, que pode ser associada ao NFSEN, que neste trabalho não foi possível analisar, porém os conceitos serão objeto de estudo na continuidade das pesquisas.

Para finalizar, enfatizamos que todas as idéias propostas objetivaram conhecer o comportamento do tráfego, sem que isso comprometesse a neutralidade [39] da rede.

Referências bibliográficas.

[01] Bruder, J. P.: "Barômetro Cisco de Banda Larga no Brasil, 2005-2010" IDC - International Data Corporation - 2009

[02] Stanton, M. A.: "Soluções Alternativas Usadas na Rede de Comunicação da UFF", Rede Nacional de Ensino e Pesquisa – 1998

[03] Souza, J.: "Redes do governo brasileiro sofrem dois mil ataques por hora" Folha Uol, Inc. 2009

[04] Rodrigues, R.: "Sites do governo federal estão servindo de plataforma para spammers" International Data Group, Inc. 2010

[05] Carvalho, J. M. A.: "Arquitetura para Controle de Congestionamento e "Tarifação de Trafego Não-Cooperativo" - Instituto Militar de Engenharia,RJ, dissertação, 2009

[06] Halme A.:"Peer-to-peer Traffic: Impact on ISPs and Evaluation of Traffic Management Tools" - Helsinki University of Technology, Seminar on Internetworking, 2009

[07] Cisco, System, inc.: "Network Management Basics, Internetworking Technologies Handbook 1-58705-001-3" Internetworking technologies handbook. Cisco Press, c2001.

[08] Paxon V., - Almes G., - Mahdavi J., - Mathis M.: "Framework for IP Performance Metrics" http://www.ietf.org/rfc/rfc2330.txt, 1998.

[09] Callado A., - Kamienski C., - Fernandes S., - Sadok D., - Szabó G., - Gerő B. P.: "A Survey on Flow-based Internet Traffic Measurement Technologies", 33Rd Conference, Jakarta, 2005

[10] Kurose, J. F. and Ross, K. W.: "Redes de Computadores e a Internet", Addison-Wesley, pag 572, 2004.

[11] Postel, J. : "RFC 792 - Internet Control Message Protocol", http://www.ietf.org/rfc/rfc792.txt, 1981.

[12] Waldbusser S.: Remote Network Monitoring Management Information Base, Carnegie Mellon University, http://www.ietf.org/rfc/rfc1757.txt, 1995

[13] Brownlee, N.: "Traffic Flow Measurement: Meter MIB", The University of Auckland, http://www.ietf.org/rfc/rfc2720.txt, 1999

[14] Quittek, J.,- Zseby T., -Carle G. and Zander S.: "Traffic Flow Measurements within IP Networks:Requirements, Technologies, and Standardization" IEEE, Symposium, Japão ,2002

[15] Clayse, B.: "RFC 3954 - Cisco Systems NetFlow Services Export Version 9", http://www.ietf.org/rfc/rfc3954.txt, 2004.

[16] CISCO Systems, "Introduction to Cisco IOS® NetFlow", 2007

[17] Kleinová, A.,- Baláž A., -Trelová J.,- Ádám N.: " Measuring Platform Architecture Based on the IPFIX Standard" - Department of Computers and Informatics, Technical University of Košice, Conference, 2004.

[18] Pinheiro, P. V.,- Bernardes, M. - Boavida, F.: "COLANA – Uma ferramenta para recolha e análise de grandes volumes de tráfego", Congresso de Redes de Comunicação, Portugal, 2002

[19] Fullmer, M., - Romig, S.: “The OSUFlow-Tools Package and Cisco Netflow Log” ARTIGO, The Ohio Estate University, 2000
[20] Miloucheva I., Nassri A., Hofmann U. “Traffic Measurement and Monitoring Roadmap”, Information Society Tecnology, NGN, WorkShop, Germany, 2002.
[21] Carvalho, J., M., A.,: “Arquitetura para Controle de Congestionamento e Tarifação de Tráfego não Cooperativo” – Instituto Militar de Engenheria, Dissertação, RJ, 2009
[22] Brownlee, N.: “Some Observations of Internet Stream Lifetimes” CAIDA, UC San Diego, e The University of Auckland, New Zealand, 2004
[23] Miller D.: “A Software Netflow Probe”, http://code.google.com/p/softflowd , 2010
[24] Haag, P. “User Documentation nfdump & NfSen”2006
[25] Puleston, I., D.,: “Protocol Spoofing Control Protocol (PSCP)”, Network Working Group Internet Draft, 1996
[26] Júnior N. A., Albuquerque M. P., Dias B. Z., Braga N. C.:” Internet Group Management Protocol” Projeto Multicast, CAT/CPBF, 2002
[27] Magalhaes, R. M.: “Host-Based IDS vs Network-Based IDS”, http://www.windowsecurity.com/articles/Hids_vs_Nids_Part1.html?, printversion, 2003
[28] Alshamsi, A., Saito Y. Takamichi “A Technical Comparison of IPSec and SSL”, Tokyo University of Technology, http://eprint.iacr.org/2004/314.pdf, 2004
[29] Scarfone, K.,Mell,P.: Guide to Intrusion Detection and Prevention Systems (IDPS), http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf, National Institute of Standard and Technology, NIST, iSpecial Publication 800-94
[30] Halme, A., : “Peer-to-peer Traffic: Impact on ISPs and Evaluation of Traffic Management Tools” Helsinki University of Technology, Paper, 2005
[31] Armbrust M., Fox A., Griffith R., Joseph A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica I. e Zaharia, M.,: “Above the Clouds: A Berkeley View of Cloud Computing”, Report, 2009.
[32] Malmedal B.,: “Using Netflows for slow portscan detection” Department of Computer Science and Media Technology Gjøvik University College, Master’s Thesis, 2005
[33] Bin L., Chuang L., Jian Q., Jianping H., Ungsunan P. : “A NetFlow based flow analysis and monitoring system in enterprise networks” - Department of Computer Science and Technology, Tsinghua University, Beijing, China - School of Telecommunication Engineering, Beijing University of Posts and Telecommunications, Beijing, China, 2008.
[34] Clemm A.,: ”Device Instrumentation for Performance Monitoring and its Application in Service Level Management”, SBRC, Gramado, 2010.
[35] Proto A., Cansiam A. M., Corrêa J. L.,“Banco de dados de fluxos para análise de tráfego e de segurança” UNESP/FAPESP, Grupo de trabalho, 2008
[36] Miloucheva I., Nassri A., Hofmann U. “Traffic Measurement and Monitoring Roadmap”, Information Society Tecnology, NGN, 2002.
[37] ANGUS I., : “An Introduction to Erlang B and Erlang C” Telemanagement, magazine Canada, 2001
[38] Kalekar P. S., :”Time series Forecasting using Holt-Winters Exponential Smoothing” Kanwal Rekhi School of Information Technology, Seminar, 2004
[39] WuT. : “Network Neutrality, Broadband Discrimination”, Journal of Telecommunications and High Technology Law, Vol. 2, p. 141, 2003

APÊNDICE 1

ANÁLISE DE FERRAMENTAS

Antes do início dos testes com a ferramenta NFSEN, como parte da disciplina de Estudo Orientado, foram testadas duas ferramentas de monitoramento de rede na UFF: O Dview [1], cuja licença foi obtida junto com a aquisição do DXS3326GSR (novo elemento ativo de 10gbit/s), e o Cacti [2] *(open source*), ambos baseados no protocolo SNMP [3]. Veremos, agora, a análise das ferramentas.

1.0 Infra-estrutura utilizada

Um servidor duo processado de 3.2 GHz, com 2GB de memória RAM e quatro discos SATA de 160 GB. Foi instalado o sistema operacional Windows XP Educacional, requisito para o sistema Dview.

2.0 - Avaliação da ferramenta 1 (Dview)

Um software de fácil instalação em ambiente Windows, sendo necessário apenas habilitar no sistema operacional o suporte ao protocolo SNMP. Não trouxe nativamente o módulo de controle do switch - foi necessário fazer o download de um arquivo executável, de simples instalação, a partir do site do fabricante. Uma vez instalado este módulo, um painel frontal mostra o equipamento - é como se o operador estivesse fisicamente diante do hardware, podendo operá-lo. Após informar o nome da comunidade SNMP, já é possível controlar todo o equipamento.

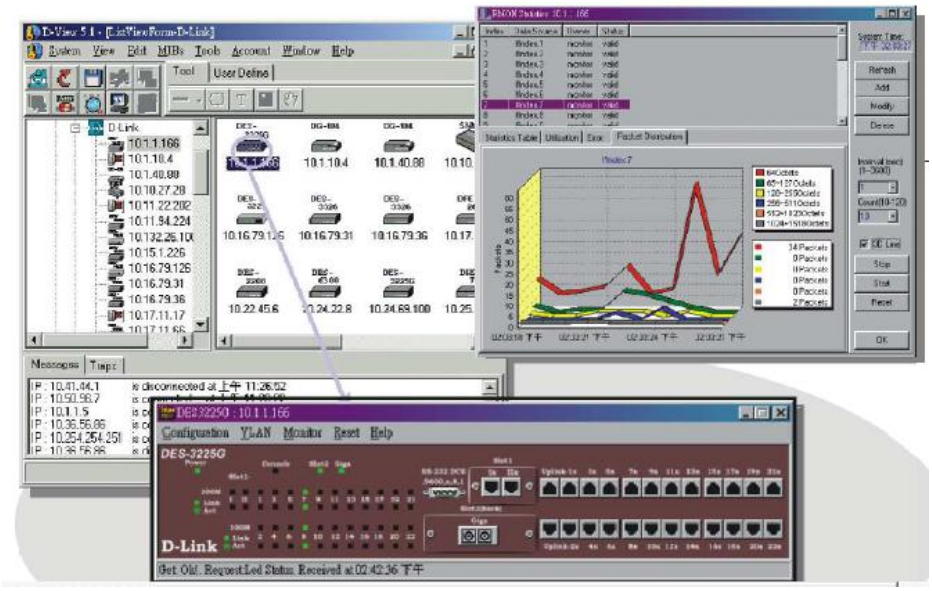


Figura -1 - Dview 5.1 – Telas do gerenciador de rede desenvolvido pela empresa DLINK.

3.0 - Operando a ferramenta.

O Dview é de facílimo uso. O operador que tiver conhecimento dos conceitos dos protocolos SNMP, RMON [4] e suas versões, não terá dificuldades no manuseio. É possível ver as portas ativas, alterar a taxa de operação ou mesmo desabitá-las.

4.0 - Registrando os dados

Após habilitar o protocolo RMON, nas portas escolhidas, o equipamento (switch) passa a registrar internamente, as estatísticas do tráfego.

É possível ver uma tabela com os seguintes dados do switch, por porta:

- Vazão,
- Latência,
- Fluxo total trafegado desde a ativação do RMON,
- Fluxo total de dados entrando,
- Fluxo total de dados saindo,
- Total de pacotes descartados,
- Unicast

- Multicast.

O objetivo desta ferramenta é o monitoramento e operações remotas. A interface é excelente, os painéis dos switches (figura 1) permitem, com grande facilidade, gerenciar os equipamentos, visualizar e configurar os *traps* (alarmes em função de eventos. Exemplo: nível máximo de utilização de uma porta para disparo de um e-mail ao administrador da rede), porém, não foi possível salvar os dados registrados para formação de base de dados em disco, no servidor. Tal fato foi devido a falta dessa funcionalidade na versão disponível na UFF, segundo informações do suporte técnico consultado. Esta informação determinou a busca por outras ferramentas.

5.0 - Avaliação da ferramenta 2 (Cacti)

O CACTI é um sistema de monitoramento com uma interface do tipo WebService, composto por diversas funcionalidades, cuja finalidade é monitorar dispositivos em uma rede, coletando os dados e armazenando em uma base de dados otimizada, com armazenamento local. A interface é provida pela linguagem de programação PHP. Os dados são armazenados no banco de dados Mysql [4] com a otimização da ferramenta RDDTOOL [6]. A captura de dados é feita através do protocolo SNMP.

O sistema possui versões para as plataformas Windows e Linux - Considerando a flexibilidade obtida nos sistemas open-source, a versão escolhida para avaliação foi a Linux.

7.1 - Requisitos para instalação.

Para instalar o CACTI é necessário:

- Sistema operacional (Linux ou Windows)
- Servidor WEB (Apache)
- Servidor MYSQL
- Linguagem de programação PHP
- Pacote RDDTOOL

- Pacote NET-SNMP

7.2 - Funcionamento da ferramenta.

Um dos pontos fortes da ferramenta é a fácil operação proporcionada pela interface. Em poucos minutos é possível adicionar um novo dispositivo, escolher as portas a serem monitoradas e iniciar a geração dos gráficos.

Dentre as MIBs disponíveis, foi utilizada a denominada "SNMP STATISTICS". Essa MIB faz consultas através do protocolo SNMP ao elemento ativo, trazendo as seguintes informações por porta:

- Vazão,
- Fluxo total de dados: entrando;
- Fluxo total de dados: saindo;
- Total de pacotes descartados;
- Total de pacotes do tipo unicast;
- Total de pacotes do tipo broadcast.

Uma consulta periódica aos elementos ativos configurados é agendada através do aplicativo CRONTAB do Linux. Por padrão do CACTI, ela é feita de cinco em cinco minutos, podendo ser alterada a critério do administrador, desde que seja feita a devida alteração também na configuração da interface Web. Os dados gerados por estas consultas são utilizados pelo sistema RDDTOOL, que fica encarregado de fazer o armazenamento e geração dos gráficos que podem ser acessados via navegador.

7.3 - Visualizações dos gráficos

É possível configurar a visualização dos gráficos em intervalos menores. Por exemplo: gráfico anual de um determinado elemento ativo mostrando intervalos de 30 dias, ou, gráfico semanal de um determinado elemento ativo mostrando intervalos de 01 dia.

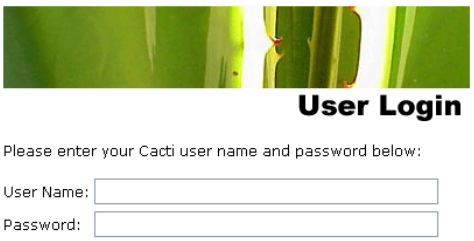


Figura -2 - Tela de Login do sistema Cacti

7.4 - Controle de acesso.

A interface acessada via Web, é dotada de módulo de autenticação, permitindo a criação de múltiplos usuários com diferentes níveis de acesso ao sistema (figura-2).

8.0 - A captura dos dados.

Considerando o tamanho da rede UFF, seja pela extensão ou pela quantidade de estações de trabalho, roteadores e elementos ativos, e o limitado tempo destinado a este trabalho, o foco da captura dos dados ficou restrito aos três principais elementos ativos do anel, que são:

1 - Switch Router Ethernet 10gbit/s localizado no campus do Valonguinho (Núcleo de Tecnologia da Informação)

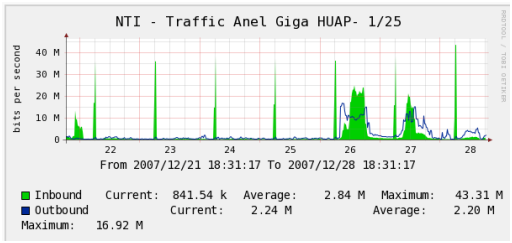
2 - Switch Router Ethernet 10gbit/s localizado no campus da Praia Vermelha (Escola de Engenharia)

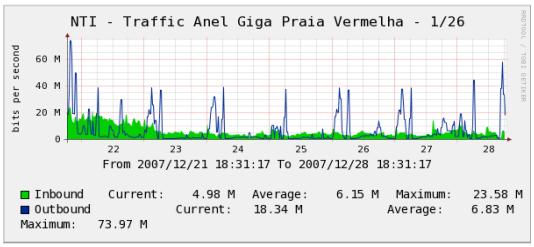
3 - Switch Router Ethernet 10gbit/s localizado no campus HUAP (Hospital Universitário Antonio Pedro).

9.0 Gráficos

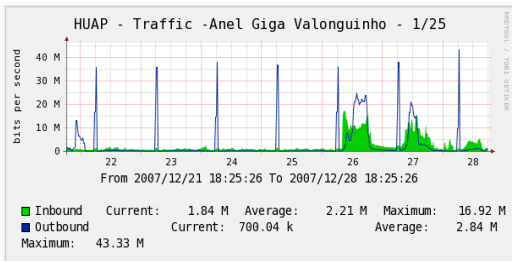
Os gráficos a seguir foram gerados pelo sistema CACTI a partir do funcionamento dos switches do anel da rede UFF. Cada gráfico representa uma porta de um switch do anel, que por sua vez está ligada a outra porta em outro switch, compondo assim o anel.

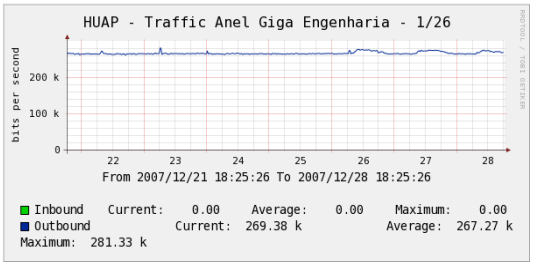
Gráficos de utilização do circuito de 10gbit/s do Anel UFF no período de 21 de dezembro de 2007 a 28 de dezembro de 2007.



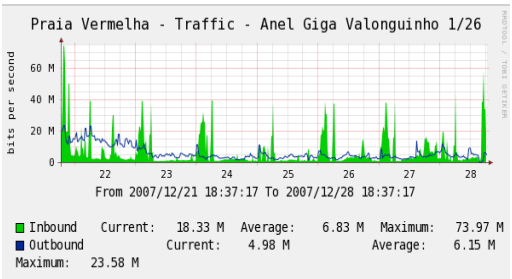


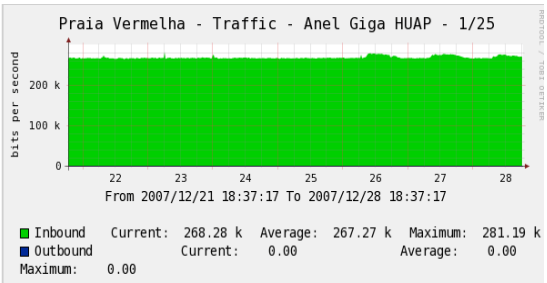
Gráficos 1 e 2 - Switch Router Dlink 10gbit/s, modelo DXS3326GSR localizado no campus do Valonguinho (NTI).





Gráficos 3 e 4 - Switch Router Dlink 10gbit/s, modelo DXS3326GSR localizado no campus do Hospital Universitário Antonio Pedro (HUAP).





Gráficos 5 e 6 - Switch Router Dlink 10gbit/s, modelo DXS3326GSR localizado no campus da Praia Vermelha (Engenharia).

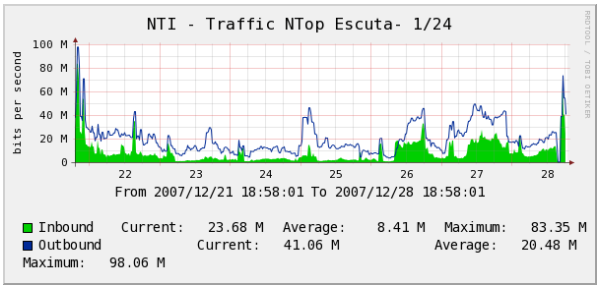


Gráfico-7 - Switch Router Dlink 10gbit/s, modelo DXS3326GSR localizado no campus do Valonguinho (NTI – Saída da Internet).

Nos gráficos 1 e 2 (NTI) é possível observar atividades relativas ao campus HUAP e campus da Praia Vermelha, respectivamente.

No gráfico 3 (HUAP), a grande utilização ocorre na porta 25 do Switch que está ligada ao Valonguinho (NTI), chegando a utilizar 20mbit/s (*downstream*). No gráfico 4, porta 26, existe um tráfego de 281kbit/s em direção ao switch do campus da Praia Vermelha que, segundo informações obtidas com no NTI, seriam geradas pelos protocolos de gerência da rede.

No gráfico 5 (Praia vermelha) o grande tráfego ocorre na porta 26, com picos acima dos 40mbit/s, ficando o gráfico 6, porta 25, com o tráfego de 281kbit/s oriundo do HUAP.

OBS: Os picos que ocorrem diariamente nos gráficos 1, 2,3 e 5, segundo informações do NTI, são gerados por operações de backup.

O Gráfico 7 registra o volume de tráfego demandado pelas solicitações feitas ao link da Internet com tráfego médio de 20.48mbit/s e com pico máximo de 83,35 Mbit/s. Lembrando que o limite deste enlace é de 100mbit/s.

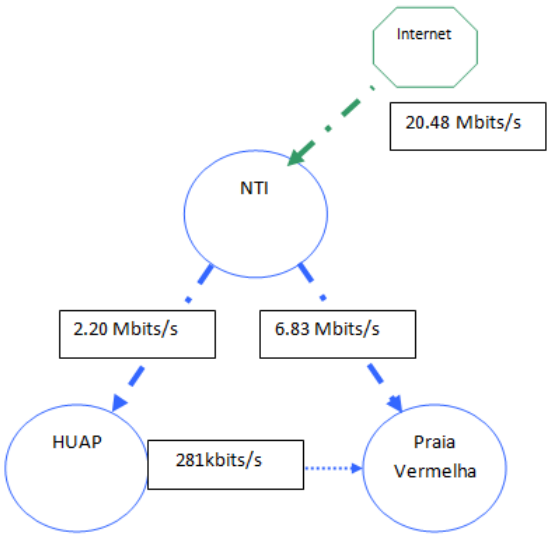


Figura 3 Fluxograma do anel UFF com médias de utilização em Downstream.

Na figura 3, cada circulo representa um switch do anel UFF. Os valores, grafados entre um círculo e outro, representam a taxa média do tráfego entre esses segmentos no sentido Internet x campus. A taxa média entre o segmento NTI e HUAP (2.20mbits/s) somados os valores registrados no segmento NTI e Praia Vermelha (6.83Mbit/s) totalizaram 9.03mbits. Subtraindo esse valor da taxa média registrada no link de Internet, obtemos o valor correspondente a taxa média do campus NTI (20.48Mbits/s – 9.03Mbits/s) que é de 11.45Mbits/s.

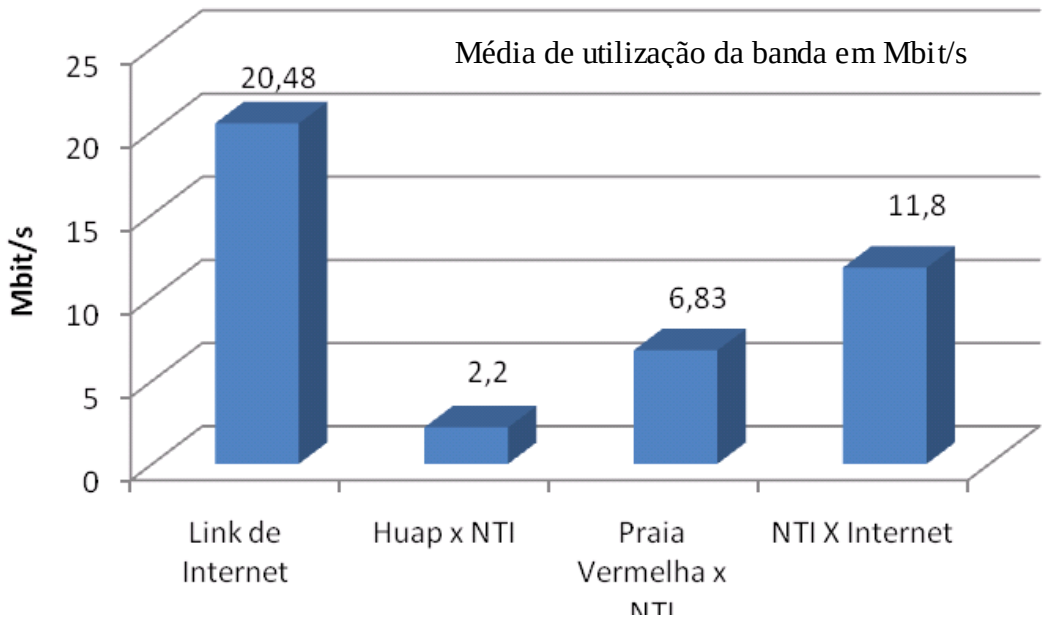


Figura 4- Gráfico comparativo da utilização dos recursos da rede UFF por Campi.

10.0 - Conclusões

Com um objetivo operacional, o Dview é de grande utilidade para o gerente da rede, que encontra recursos exclusivos, uma vez que a ferramenta foi desenhada em função dos switches. Entretanto, não foi possível salvar os dados em base de dados local, fator que tornou a ferramenta inadequada aos objetivos do trabalho. Mais tarde, novas visitas ao site do produto revelaram a capacidade de geração de base de dados no formato Microsoft Access, entretanto, devido ao limitado tempo, não foi possível fazer novas tentativas.

O Cacti mostrou-se de fácil utilização. O uso do software RDDTOOL, em conjunto com base de dados Mysql, permite o armazenamento de longos períodos de informação sobre a atividade dos switches, sem consumir grande quantidade de espaço em disco. A ferramenta também permite a programação de alertas, no entanto, ainda requer a edição e alteração de arquivos para sua instalação, o que exige do usuário familiaridade com o ambiente *open source*. Com relação aos dados obtidos, podemos observar na figura 4 que para nenhum dos campi os valores registrados podem ser considerados absolutos quanto à utilização do link externo, uma vez que não há como afirmar que todo o trafego registrado na porta dos switches passou através do citado link, já que a MIB utilizada computava os dados de forma geral. Isto significa que os acessos aos servidores de e-mail e Web hospedados no NTI, realizados a partir do campus HUAP ou pelo campus da Praia Vermelha foram contabilizados junto com o tráfego destinado à Internet. Neste cenário, somente tecnologias que considerem a origem e o destino do tráfego podem fornecer valores distintos para rotas específicas. Estas análises apontaram que o próximo teste deveria ser realizado com ferramentas baseadas nos conceitos de monitoramento de fluxo IP do tipo NETFLOW e IPFIX [7].

10.0 Referências aos softwares utilizados

[1] Dview. Software Dview. http://www.d-link.com/products/?pid=544&sec=2, acessado em 20 de Janeiro de 2010
[2] CACTI. Software Cacti. http://www.cacti.net, acessado em Outubro 2007
[3] Dias B.Z.; Jr. N. A.: "Protocolo de Gerenciamento SNMP", http://www.rederio.br/downloads/pdf/nt00601.pdf, acessado em Outubro de 2007
[4] Lessa D.,: "O Protocolo de Gerenciamento RMON", http://www.rnp.br/newsgen/9901/rmon.html, acessado em Outubro 2007
[5] Mysql. Banco de dados Mysl. http://www.mysql.com/why-mysql/, acessado em Julho 2010
[6] RRDTOOL. Software RRDTOOL, http://oss.oetiker.ch/rrdtool/, acessado em Julho 2010
[7] Haag P.: "User Documentation nfdump & NfSen" , Version 1.1, 18° Annual First Conference – Baltimore- Maryland USA, Renaissance Harborplace Hotel, 2006

APÊNDICE 2

ROTINAS PARA COLETA DE DADOS UTILIZANDO SHELL SCRIPT, NFDUMP E AWK.

Este apêndice apresenta alguns exemplos de rotinas escritas em Shell Script que, em conjunto com os programas NFDUMP e AWK, foram utilizados para a coleta e filtragem dos dados registrados. Os arquivos gerados pelo sistema no formato NFDUMP e os diversos parâmetros de consultas presentes no programa permitiram a elaboração de consultas que efetivamente contribuíram para um melhor entendimento do comportamento das redes da UFF. Veremos agora alguns dos scripts mais frequentemente utilizados.

Script 1 – Perfil Redes UFF

Resumo: Varre toda a estrutura de pastas do perfil Redes UFF e executa o programa NFDUMP para consultar os arquivos registrados. Utiliza AWK para filtrar apenas as linhas que contenham a palavra Summary, uma vez que estas contêm o somatório do tráfego.

Objetivo: Obter a totalização do tráfego de cada rede de forma individualizada. Realizar consultas agregando o tráfego por porta e por bytes. Coleta apenas a linha Summary de cada resultado

Código:

```
 #!/bin/bash
path="/dados/profiles-data/Redes-UFF"
for d in `cat diretorio` # Inicia loop para acessar todos as pastas do perfil RedesUff
do
for a in `cat mes` # Inicia loop para acessar todas os meses contidos no arquivo 'mês'
do

o=$path"/"$d"/"2009"/"$a # Atribui à variável 'o' o caminho para as pastas  correspondentes as rede
echo executando script na pasta $o
nfdump -R $o -T -n 20 -s port/flows >> ../resultados/Totais-redes/$d-$a-port-flows
nfdump -R $o -T -n 20 -s port/bytes >> ../resultados/Totais-redes/$d-$a-port-bytes
cat ../resultados/Totais-redes/$d-$a-port-flows | awk -F " " '/Summary/{print}' >> ../resultados/Totais-redes/$d-$a-Summary # Utiliza AWK para filtrar as linha com a palavra
```

```
Summary que contém o total de fluxos, bytes e pacotes
registrados no período.
done
echo "Imprimindo Summary"
cat ../resultados/Totais-redes/$d-$a-Summary
echo "|Rede $d do mes $a gravada"
done
echo "FIM"
```

Script 2 – Totalização Geral (Processa todos os registros do servidor, independente dos perfis existentes)

Resumo: Acessa o diretório principal onde estão armazenados todos os perfis configurados no sistema. Executa o programa NFDUMP com parâmetros para selecionar os resultados: portas ordenadas por quantidade de fluxo, portas de origem ordenadas por quantidade de fluxos, portas de destino ordenadas por quantidade de fluxos, ips ordenados por bytes e ips ordenados por fluxos.

Objetivo: Obter o volume total do tráfego da Rede da UFF registrado pelo servidor de monitoramento.

Código:

```
nfdump -R /dados/profiles-data/live/upstream1/2009/ -T -n
20 -s port/bytes -s port/flows srcport/bytes -s
srcport/flows -s dstport/bytes ip/bytes -s ip/flows
```

Script 3 – Processamento e coleta de dados individualizados das redes da UFF. Mensal.

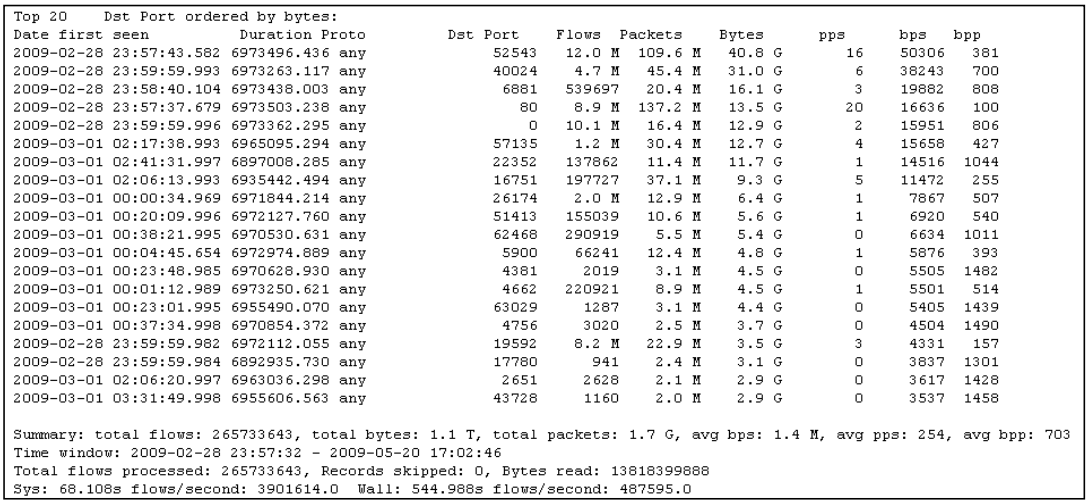
Resumo: Através de rotinas FOR, entra nos diretórios contendo os perfis de cada rede, mudando a cada loop para o diretório de cada mês e executando o programa NFDUMP com parâmetros diversos, de modo a coletar as informações sob diversas perspectivas. Salva o resultado em arquivos em individuais identificados pelo nome da rede e critério da consulta.

Objetivo: Extrair dos repositórios individuais de cada rede, informações que contribuam para um melhor entendimento do uso da rede, visando determinar o PFR (Padrão de funcionamento da rede).

Código:

```
dir="/dados/profiles-data/Redes-UFF"    # Variável para armazenar diretório principal dos dados
for i in `cat diretorio` # busca em arquivo de nomo 'diretorio' nomes das redes e atribui ao for.
do
cd $i/2009 # entra nos diretórios de cada rede
echo "Processando rede $i" # Indica a rede que esta sendo processada
for b in `cat /$dir/meses` # Entra no diretorio de cada mes do
nfdump -R $b -T -n 20 -s port/flows > $dir/result/$i-$b-port-flow-2009 # Lista as 20 portas da rede $i ordenadas pela maior quantidade de fluxos regitrado no mês $b
nfdump -R $b -T -n 20 -s srcport/flows > $dir/result/$i-src-port-$b-2009 # Lista as 20 portas de origem da rede $i ordenadas pela maior quantidade de fluxos registrado no mês $b
nfdump -R $b -T -n 20 -s dstport/flows > $dir/result/$i-$b-dst-port-2009 # Lista as 20 portas de destino da rede $i ordenadas pela maior quantidade de fluxos registrado no mês $b
nfdump -R $b -T -n 20 -s port/bytes > $dir/result/$i-$b-port-bytes-2009 # Lista as 20 portas  da rede $i ordenadas pela maior quantidade de bytes registrado no mês $b
nfdump -R $b -T -n 20 -s dstport/bytes > $dir/result/$i-$b-dst-port-2009 #  Lista as 20 portas de destino da rede $i ordenadas pela maior quantidade de bytes registrado no mês $b
nfdump -R $b -T -n 20 -s srcport/bytes > $dir/result/$i-$b-src-port-2009 # Lista as 20 portas de origem da rede $i ordenadas pela maior quantidade de bytes
nfdump -R $b -T -n 20 -s ip/bytes > $dir/result/$i-$b-ip-port-2009 # Lista os 20 endereços ip da rede $i ordenados por aqueles que possuam a maior quantidade de bytes registrados
nfdump -R $b -T -n 20 -s srcip/bytes > $dir/result/$i-$b-srcip-bytes-2009 # Lista os 20 endereços ip de origem ordenados por aqueles que possuam a maior quantidade de bytes registrados
nfdump -R $b -T -n 20 -s dstip/bytes > $dir/result/$i-$b-dst-bytes-2009 # Lista os 20 endereços ip de destino ordenados ordenados por aqueles que possuam a maior quantidade de bytes registrados
nfdump -R $b -T -n 20 -s ip/flows > $dir/result/$i-$b-ip-flows-2009
# Lista os 20 endereços ip ordenados por aqueles que possuam a maior quantidade de fluxos registrados
```

```
nfdump -R $b -T -n 20 -s srcip/flows > $dir/result/$i-$b-srcip-flows-2009 # Lista os 20 endereços ip de origem ordenados por aqueles que possuam a maior quantidade de fluxos registrados
nfdump -R $b -T -n 20 -s dstip/flows > $dir/result/$i-$b-dst-ip-flows-2009 # Lista os 20 endereços ip de destino ordenados por aqueles que possuam a maior quantidade de fluxos registrados
done
cd $dir
done
```



```
Top 20    Dst Port ordered by bytes:
Date first seen          Duration Proto         Dst Port    Flows  Packets    Bytes      pps      bps   bpp
2009-02-28 23:57:43.582 6973496.436 any             52543   12.0 M  109.6 M   40.8 G       16    50306   381
2009-02-28 23:59:59.993 6973263.117 any             40024    4.7 M   45.4 M   31.0 G        6    38243   700
2009-02-28 23:58:40.104 6973438.003 any              6881   539697   20.4 M   16.1 G        3    19882   808
2009-02-28 23:57:37.679 6973503.238 any                80    8.9 M  137.2 M   13.5 G       20    16636   100
2009-02-28 23:59:59.996 6973362.295 any                 0   10.1 M   16.4 M   12.9 G        2    15951   806
2009-03-01 02:17:38.993 6965095.294 any             57135    1.2 M   30.4 M   12.7 G        4    15658   427
2009-03-01 02:41:31.997 6897008.285 any             22352   137862   11.4 M   11.7 G        1    14516  1044
2009-03-01 02:06:13.993 6935442.494 any             16751   197727   37.1 M    9.3 G        5    11472   255
2009-03-01 00:00:34.969 6971844.214 any             26174    2.0 M   12.9 M    6.4 G        1     7867   507
2009-03-01 00:20:09.996 6972127.760 any             51413   155039   10.6 M    5.6 G        1     6920   540
2009-03-01 00:38:21.995 6970530.631 any             62468   290919    5.5 M    5.4 G        0     6634  1011
2009-03-01 00:04:45.654 6972974.889 any              5900    66241   12.4 M    4.8 G        1     5876   393
2009-03-01 00:23:48.985 6970628.930 any              4381     2019    3.1 M    4.5 G        0     5505  1482
2009-03-01 00:01:12.989 6973250.621 any              4662   220921    8.9 M    4.5 G        1     5501   514
2009-03-01 00:23:01.995 6955490.070 any             63029     1287    3.1 M    4.4 G        0     5405  1439
2009-03-01 00:37:34.998 6970854.372 any              4756     3020    2.5 M    3.7 G        0     4504  1490
2009-02-28 23:59:59.982 6972112.055 any             19592    8.2 M   22.9 M    3.5 G        3     4331   157
2009-02-28 23:59:59.984 6892935.730 any             17780      941    2.4 M    3.1 G        0     3837  1301
2009-03-01 02:06:20.997 6963036.298 any              2651     2628    2.1 M    2.9 G        0     3617  1428
2009-03-01 03:31:49.998 6955606.563 any             43728     1160    2.0 M    2.9 G        0     3537  1458

Summary: total flows: 265733643, total bytes: 1.1 T, total packets: 1.7 G, avg bps: 1.4 M, avg pps: 254, avg bpp: 703
Time window: 2009-02-28 23:57:32 - 2009-05-20 17:02:46
Total flows processed: 265733643, Records skipped: 0, Bytes read: 13818399888
Sys: 68.108s flows/second: 3901614.0   Wall: 544.988s flows/second: 487595.0
```

Figura 4 Exemplo de resultado de um script – As 20 portas de destino com maior quantidade de fluxos

Script 4 – Coleta de dados do perfil protocolo.

Resumo: Execução do programa NFDUMP na pasta do perfil Protocolos. Filtragem das linhas com a palavra Summary com o comando AWK .

Objetivo: Totalização do trafego registrado no Perfil Protocolos.

Código:

```
#!/bin/bash
dir="/dados/profiles-data/PROTOCOLOS"   # Atribuição do caminho do perfil protocolo a variável de nome 'dir'
res="/dados/profiles-data/resultados/PROTO" # Atribuição do caminho da pasta destinada aos resultados da consulta a variável de nome 'res'.
for b in `cat Proto-dir` # leitura do arquivo 'Proto-dir' contendo o nome de cada protocolo pelo comando FOR
do
```

```
for m in `cat mes` # Leitura de cada mês existente a partir
do arquivo 'mês'
do
echo "processando o protocolo $b do Mes $m"
nfdump -R $dir/$b/2009/$m | awk -F " " '/Summary/'
>$res/$b-$m # Execução programa NFDUMP para cada protocolo
em $b e cada mês em $m. Filtragem dos resultados salvos em
$res.
echo "Processado Proto $b de $m"
done
done
```

Script 5 - Coleta de dados do perfil AnelUFF.

Resumo: Execução do programa NFDUMP na pasta do perfil Protocolos. Filtragem das linhas com a palavra Summary com o comando AWK .

Objetivo: Totalização do trafego registrado no Perfil AneUFF.
Código:

```
#!/bin/bash
dir="/dados/profiles-data/AnelUFF"
res="/dados/profiles-data/resultados/ANEL"
for b in `cat Anel-dir`
do
for m in `cat mes`
do
echo "processando a rede do anel $b do Mes $m"
nfdump -R $dir/$b/2009/$m | awk -F " " '/Summary/'
>$res/$b-$m
echo "Processado rede do Anel $b de $m"
done
done
echo "FIM"
```