Fatec São Caetano do Sul

Segurança em Sistemas Operacionais e Redes de Computadores II

Análise do tráfego de rede – Netflow

Fatec São Caetano do Sul

Análise do tráfego de rede – Netflow

Fluxo (flow)

- Tráfego unidirecional com um único conjunto (tuple) de características (IP de origem e destino, porta de origem e destino, TOS - tipo de serviço, interface de entrada e saída, etc.);
- Packets sem fluxo fazem com que um novo fluxo seja iniciado para manter o estado da informação refente a esse fluxo;
- Packets subsequentes com o mesmo “tuple” contribuirão para a contagem do fluxo (bytes e packets).

Análise do tráfego de rede – Netflow

Netflow

- Protocolo inicialmente desenvolvido pela Cisco no seu programa de Quality of Service (QoS);
- Diferente de ferramentas como o TCPdump ou o Wireshark que não são próprias para analisar grandes quantidades de dados, permite rastrear atividade de rede para determinar as causas de congestionamentos;
- Está presente em equipamentos de vários fabricantes tais como Cisco, Juniper, Nortel, Alcatel-Lucent, PCs e servidores (Linux, FreeBSD, NetBSD, OpenBSD), servidores VMware, etc.

Fatec São Caetano do Sul

Análise do tráfego de rede – Netflow

Netflow

- Ferramentas:
  - Cflowd
  - ARTS
  - Flowscan
  - Flow-Tools
  - Ntop
  - Nfdump

Análise do tráfego de rede – Netflow

Netflow

- Condições específicas para o início ou final de um fluxo:
  - Em conexões TCP, quando a conexão for encerrada (depois de um RST ou FIN);
  - Quando não ocorrer tráfego durante 15 segundos;
  - Caso o tempo exceder os 30 minutos a partir do início do fluxo;
  - Quando a tabela de fluxos estiver cheia.

Fatec São Caetano do Sul

Análise do tráfego de rede – Netflow

Netflow

- RFC 3954 - Cisco Systems NetFlow Services Export Version 9;
- ARTS – Especificação de arquivo binário para o armazenamento de dados de rede.

Fatec São Caetano do Sul

Análise do tráfego de rede – Netflow

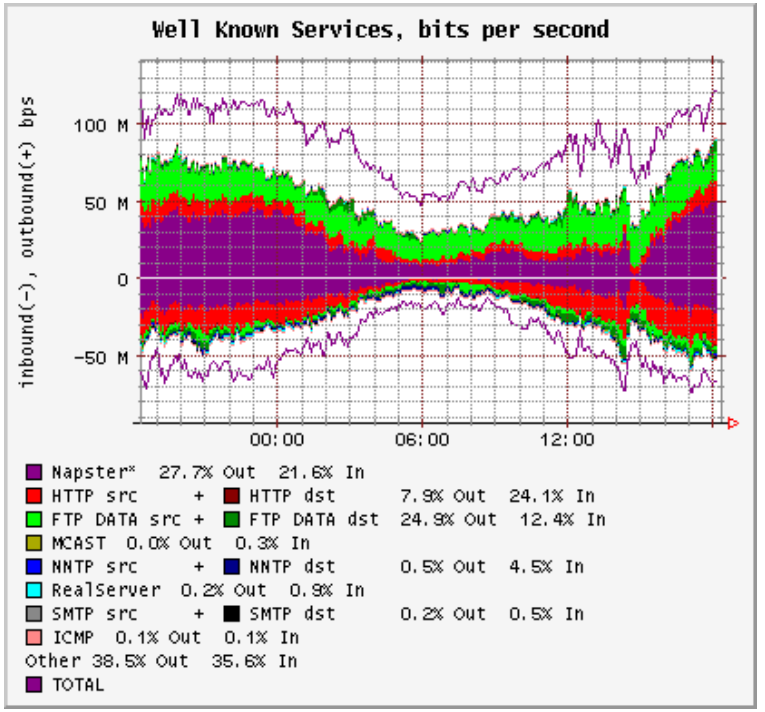
Exemplo de conjunto de ferramentas – cflowd

- É dividido em três programas distintos:
  - cflowmux – responsável pelo recebimento do fluxo proveniente dos roteadores Cisco e deixá-lo para para o host local;
  - cflowd – responsável por manter tabelas das entradas de cada roteador e passá-lo para o coletor central;
  - cfdcollect – responsável por recolher os dados tabelados de instâncias do cflowd.

Análise do tráfego de rede – Netflow

Exemplo de conjunto de ferramentas – Flowscan

- Ferramenta de visualização e relatório. É composto por:
  - Motor (engine) de coleta (cflowd modificado);
  - Banco de dados de alta performance (RRD – round robin database);
  - Ferramenta de visualização (RRDtool);
  - RRGrapher (front-end web para o RRDTool).



Fatec São Caetano do Sul

Análise do tráfego de rede – Netflow

Exemplo de conjunto de ferramentas

- Flow-tools – Biblioteca e coleção de programas para coletar e processar dados de Netflow
  - Flow-capture – coleta, comprime, guarda e gerencia o espaço em disco;
  - Flow-cat – concatena os arquivos de fluxo;
  - Flow-fanout – facilita múltiplos coletores para um único roteador;
  - Flow-report – gera relatórios para os conjuntos de dados Netflow;
  - Flow-tag – identifica os fluxos;
  - Flow-filter – filtra fluxos baseado em qual um dos campos de exportação;
  - Flow-import – importa dados a partir dos formatos ASCII ou cflowd;
  - Flow-export – exporta dados para os formatos ASCII ou cflowd;

Fatec São Caetano do Sul

Análise do tráfego de rede – Netflow

Exemplo de conjunto de ferramentas

- Flow-tools – Biblioteca e coleção de programas para coletar e processar dados de Netflow (cont.)
  - Flow-send – envia dados pela rede usando o protocolo Netflow;
  - Flow-receive – recebe dados exportados via protocolo Netflow sem guardá-los como faz o flow-capture;
  - Flow-gen – gera dados de teste;
  - Flow-dscan – detecta alguns tipos de ataques de varredura e Denial of Service;
  - Flow-merge – mescla arquivos de fluxo em ordem cronológica;
  - Flow-xlate – realiza traduções de alguns campos de fluxo;
  - Flow-expire – expira fluxos usando a mesma política do flow-capture;
  - Flow-header – apresenta a meta informação de um arquivo de fluxo;
  - Flow-split – divide arquivos em arquivos menores.

Fatec São Caetano do Sul

Análise do tráfego de rede – Netflow

Exemplo de conjunto de ferramentas

- Fprobe – ferramenta baseada na biblioteca libpcap que coleta tráfego de rede e o emite como fluxo Netflow na direção de um coletor especificado;
- Nfdump – conjunto de ferramentas que coleta e processa dados netflow;
- NfSen – Front-end gráfico para o nfdump.

Fatec São Caetano do Sul

Análise do tráfego de rede – Netflow

Exemplo de conjunto de ferramentas

- nfdump
  - nfcapd – Daemon para captura de Netflow. Lê os dados da rede e salva-os em arquivos;
  - nfdump – Lê os dados salvos pelo nfcapd. A sus sintaxe é semelhante ao tcpdump;
  - nfprofile – perfila dados de Netflow. Lê os dados salvos pelo nfcapd e filtra-os de acordo com o conjunto de filtros (profiles) e grava os dados filtrados para uso futuro;
  - nfreplay - Lê os dados salvos pelo nfcapd e os envia através da rede para outro host;
  - nfclean.pl – Limpa dados antigos;
  - ft2nfdump – Lê e converte dados do flow-tools.

Fatec São Caetano do Sul

Análise do tráfego de rede – Netflow

Exemplo de conjunto de ferramentas (cont.)

- nfSen
  - Apresenta os dados de Netflow: Fluxos, packets, e bytes usando RRD (Round Robin Database);
  - Navega facilmente através de dados de Netflow;
  - Processa dados de Netflow dentro de um intervalo especificado de tempo;
  - Cria perfis históricos e contínuos;
  - Define alertas em várias condições;
  - Podem ser escritos plugins para processar dados de Netflow em intervalos regulares.

Fatec São Caetano do Sul

Análise do tráfego de rede – Netflow

- Fontes
  - ubuntu.com;
  - fprobe.sourceforge.net;
  - www.caida.org;
  - www.cisco.com;
  - www.splintered.net;
  - nfdump.sourceforge.net;
  - nfsen.sourceforge.net;
  - SKODIS E, LISTON T. Counter Hack Reloaded, Second Edition: A Step-by-Step Guide to Computer Attacks and Effective Defenses.