Gerência de segurança

Gerência de segurança refere-se ao controle das operação e ao monitoramento do uso dos recursos no ambiente da rede

Atividades da gerência de segurança

- Controle das chaves criptográficas de comunicação
  - DNSSec, Certificados digitais, VPNs, etc.
- Senhas e controle de acesso aos equipamentos da rede
- Monitoração e controlar o acesso à rede
- Monitorar e controlar informação obtida por equipamentos de rede
  - Dados de fluxos, dump de tráfego
- Logs e registros de auditoria
- Ativar e desativar ‘tapping de rede’

- NOC e SOC compartilham estas atividades

Dados e ferramentas utilizadas

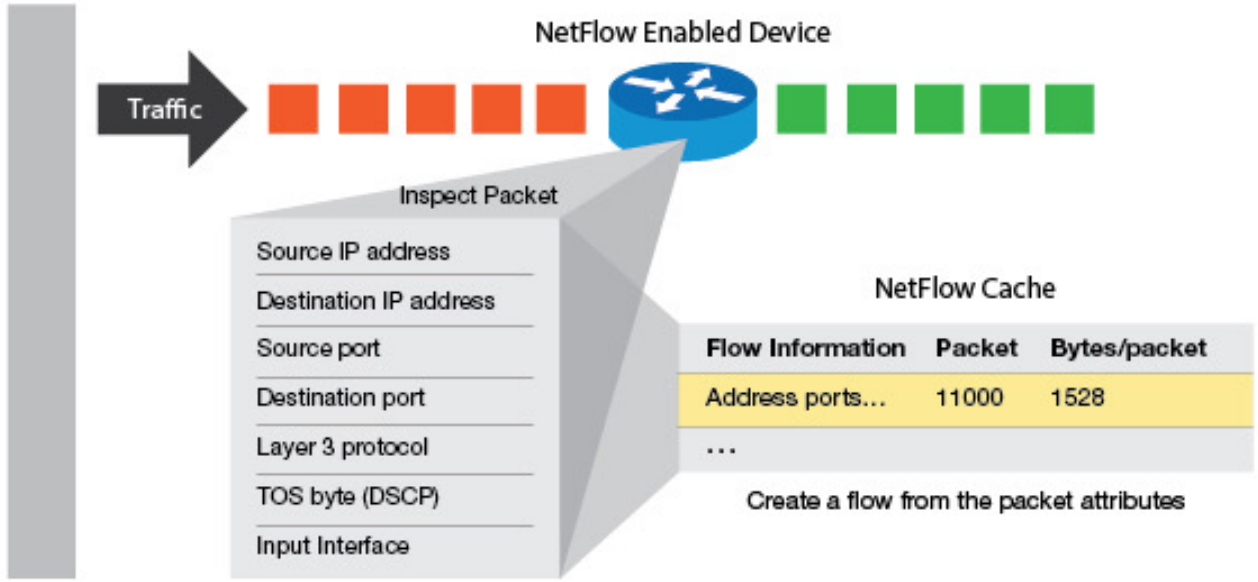
- Dados **SNMP** de todas as camadas
- Coleta de **Dumps** e **Fluxo de dados**
  - Frames Ethernet (DHCP, ARP, RARP)
  - IP (origem e destino), spoofing, filtros
  - TCP/UDP
- **Logs** de equipamentos de redes
  - Ex.: para validar filtros em roteadores e switches
  - BCP38/ RFC2827: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
  - BCP84 / RFC3704 RFC8704: Ingress filtering for Multihomed networks

SNMP continua sendo a principal - e mais simples fonte de dados

- Em DDoS os primeiros alarmes costumam ser:
  - pacotes-por-segundo
  - carga do servidor
  - Numero de conexões TCP
  - Alteração de baseline de outros protocolos (ex: UDP/DNS)

Fluxo de dados

Melhor custo x benefício como mecanismo de segurança
Você deve implementar em sua rede

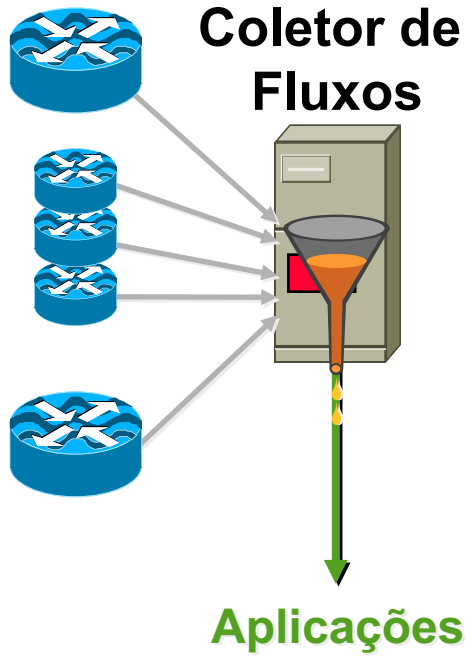


Definição do termo “flow” e características gerais

- Registro Netflow (flow): Sequência unidirecional de pacotes entre dois pontos de comunicação. Uma vez identificado o fluxo, são armazenadas as seguintes informações:
  - Conjunto IP/porta origem
  - Conjunto IP/porta destino
  - Tipo de protocolo
  - TOS (Type of Service)
  - Interface de entrada do fluxo
  - Hora inicial e final do fluxo
  - Número de pacotes e octetos
  - Sistema autônomo origem e destino

NETFLOW

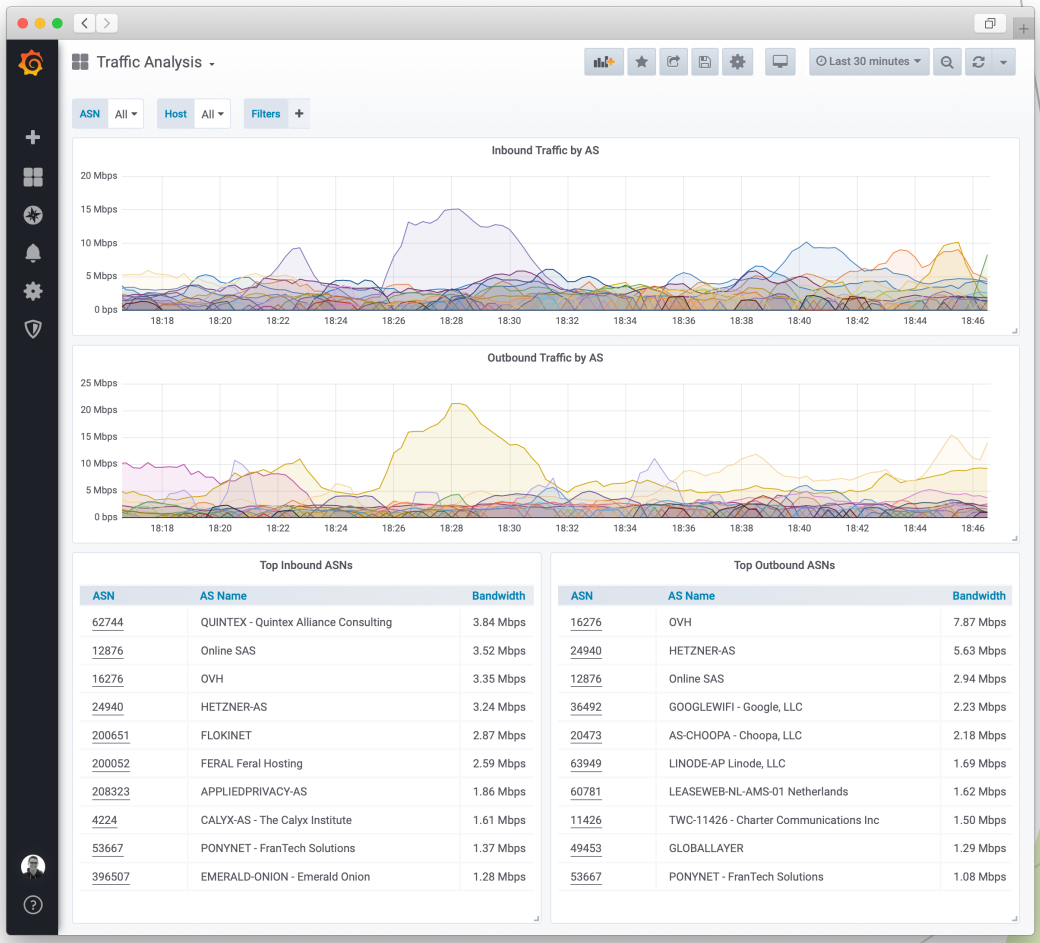
- Conjunto de ferramentas para monitoração de tráfego e exportação de modelos de dados.
- Surgiu em 1996 em implementação da Cisco.
- Hoje temos:
  - Netflow v5/v9 - cisco
  - Jflow – juniper
  - Sflow – vários fabricantes
- O IETF padronizou o **IFPIX**



Ferramentas para Flows

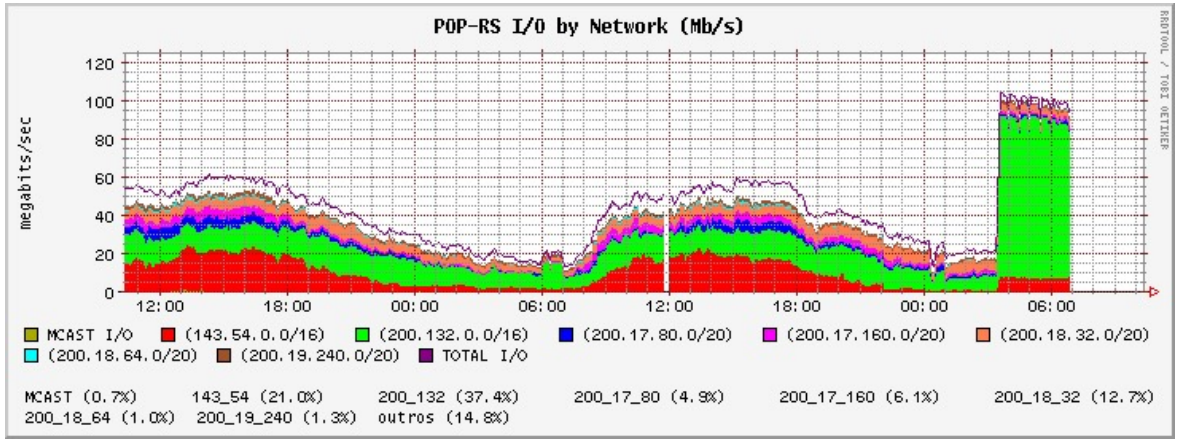
Várias opções para manipular / exportar flows:

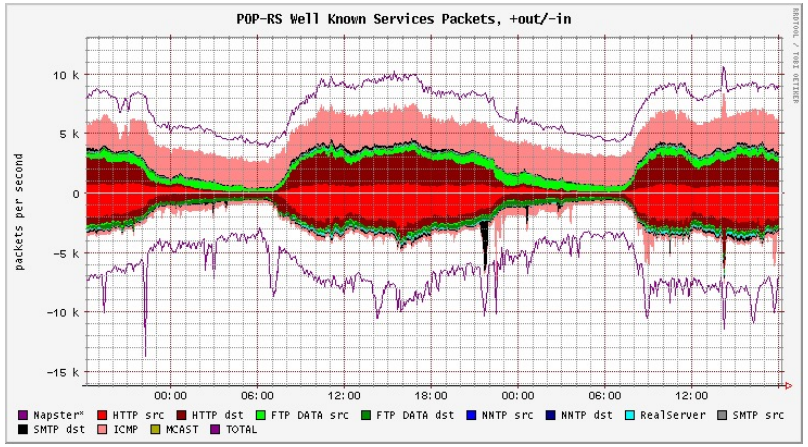
- Ntopng
- Flow-exporter
- Nfsen



https://github.com/neptune-networks/flow-exporter

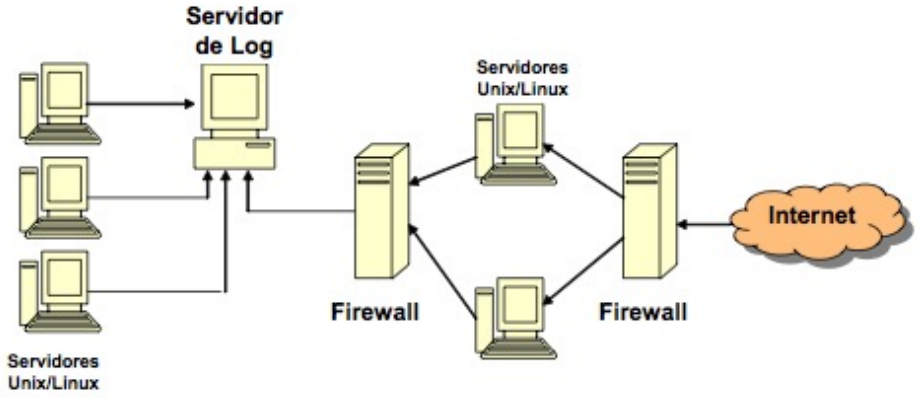
Como se parecem os fluxos de um ataque em andamento?





Gerencia e Análise de LOGs

- Lembre-se: LOGs são privados
- O Servidor de LOGS deve ser especialmente configurado (bastion host)
- Ele deve ficar na gerencia out-of-band
- Os dados são replicados em outro servidor para análise



Ferramentas para análise de logs

- https://www.graylog.org/products
- https://www.ossec.net/
- https://github.com/elastic/logstash

Gerência de segurança