Uso de Flows de Rede para análise de tráfego e para detecção de ameaças de segurança

Flows no CSIRT Unicamp

Em produção desde 2014;

CERT.br principal incentivador;

Scripts geram relatórios periodicamente;

O que monitoramos:

- Comunicação com Botnets
- Atividade SMTP
- Atividade RDP
- Mineração de criptomoedas
- Alto tráfego
- Amplificação UDP

Investigação de incidentes de segurança e/ou anomalias;

Principal ferramenta de monitoramento.

Introdução ao conceito de Flow de Rede

Tráfego de rede é o nome dado a transferência de pacotes em uma rede de computadores e descreve o caminho que um pacote de dados percorre desde a origem até o destino, passando por vários dispositivos de rede, como switches e roteadores.

O tráfego de rede pode ser medido e analisado usando vários protocolos. Estes protocolos coletam informações sobre os pacotes enquanto trafegam pela rede, incluindo dados como endereços IP de origem e destino, quantidade de dados transmitidos, protocolos usados e a duração de cada fluxo.

Podemos conceituar este tráfego com o termo “flow de rede” .

Nosso objetivo é demonstrar como a análise do flow de rede é uma ferramenta poderosa e flexível para análise de tráfego de rede, sendo útil para que administradores de rede tenham uma visão detalhada do que ocorre em sua rede e uma ferramenta indispensável para o analista de segurança na detecção de ameaças e problemas de segurança.

Definição - Flow de rede

Cisco Netflow - 1996 - v1 - v8

“flow as a unidirectional sequence of packets that all share seven values which define a unique key for the flow.”

sFlow definido pela RFC 3176 - Setembro 2001

“A flow is defined as all the packets that are received on one interface, enter the Switching/Routing Module and are sent to another interface.”

Padronização formato NetFlow RFC 3954 - Outubro 2004

“A flow is defined as a unidirectional sequence of packets with some common properties that pass through a network device”

IPFIX RFC 5101 - Janeiro 2008

“A data network with IP traffic primarily consists of IP flows passing through the network elements.”

Comparativo: sFlow & NetFlow

sFlow

- Amostragem randômica ou baseada em tempo;
- Monitoramento de dispositivos;
- Informação de tráfego IP e não IP (camadas 2 a 4);

NetFlow

- Captura integral dos cabeçalhos dos pacotes;
- Quem, o que e como a rede é usada;
- Informação de tráfego IP;

Não importa qual tecnologia você está usando, desde que utilize ferramentas de análise e monitoramento adequadas para seu objetivo.

https://thwack.solarwinds.com/resources/b/geek-speak/posts/netflow-vs-sflow-differences-and-applications

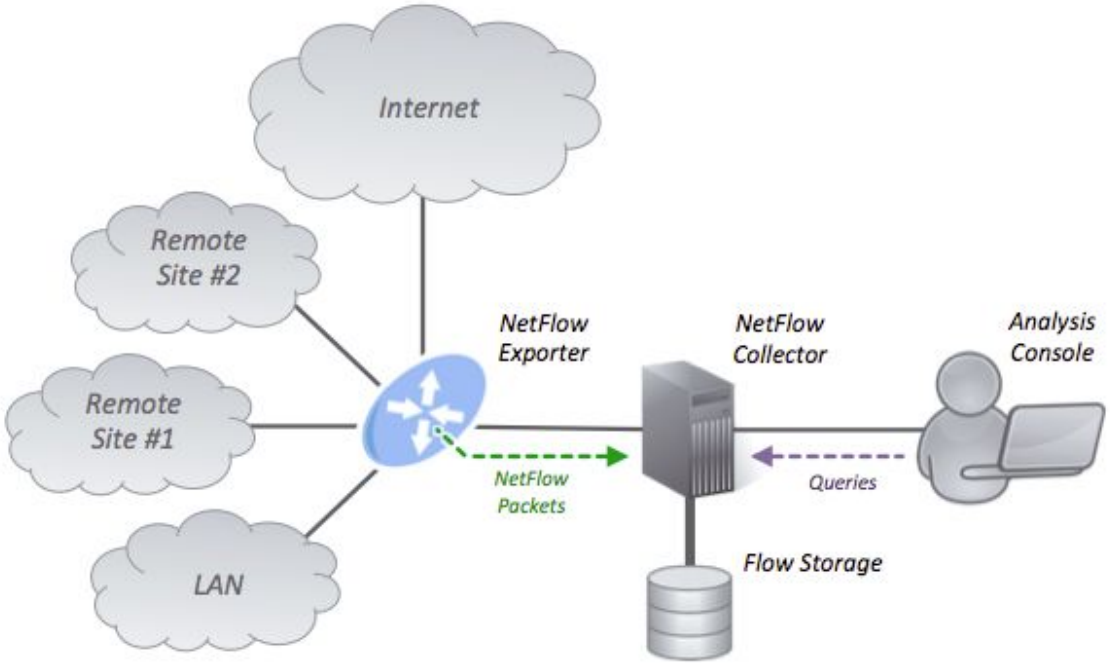
Uso em Análise de Tráfego de Rede

- Avaliar o uso dos recursos de rede pelos usuários/aplicações;
- Medir tráfego WAN e gerar estatísticas para criar políticas de uso;
- Análise de trilha de auditoria para identificar atividades de rede não autorizadas e rastrear as fontes de ataques;
- Detecção, diagnóstico e correção de problemas de rede;
- Acompanhar a largura de banda alocada através de parâmetros de QoS;
- Diagnosticar problemas de rede.

Uso em Segurança da Informação

- **Detecção de ameaças:** Time de SI pode identificar padrões de tráfego associados a ameaças conhecidas, como malware, botnet e ataques de phishing;
- **Detecção de invasão:** É possível detectar tentativas de acesso não autorizado, scan de portas e ataques de força bruta.
- **Análise de tráfego:** Por oferecer uma visão ampla do tráfego de rede, é possível analisar padrões e volume de tráfego, identificando ameaças de segurança ou problemas de performance.
- **Tratamento e resposta a incidentes:** Quando um incidente acontece, NetFlow permite reconstruir a atividade da rede, identificando origem de um ataque e alcance do comprometimento.

Flow de rede - Arquitetura



https://en.m.wikipedia.org/wiki/File:NetFlow_Architecture_2012.png

Componentes

Agente (sFlow/NetFlow)

Processo responsável por combinar estatísticas das interfaces e as amostras de tráfego em um datagrama, que é enviado para o coletor.

Coletor (sfcapd/nfcapd)

Fazem parte do conjunto de ferramentas nfdump e tem a função de receber os datagramas enviados pelo(s) agente(s) e armazenar os dados em formato binário, sempre compatíveis com o formato netflow.

Analisador (nfdump e nfsen)

Além dos coletores já mencionados, o nfdump oferece a ferramenta homônima que permite análise minuciosa dos dados armazenados pelos coletores. Conta com sintaxe similar à do tcpdump e permite *filtrar* e *agregar* os dados de acordo com parâmetros definidos pelo usuário. O NfSen oferece uma interface web para interagir com o nfdump, além de gráficos baseados nos dados armazenados.