PROTOCOLO NETFLOW

Motivação

- As crescentes mudanças de comportamento e uso da rede nos últimos anos fomentaram o desenvolvimento de um protocolo de gerenciamento de redes capaz de analisar informações mais detalhadas sobre o fluxo de tráfego de dados, uma vez que o protocolo padrão SNMP não era capaz de fornecer tal nível de detalhamento.
- O surgimento de aplicações em tempo real como VoIP, videoconferência e VPN tornou necessário que os administradores de redes conhecessem a composição do tráfego e não apenas o seu volume total, para estimar com mais precisão se um determinado tráfego é esperado ou inesperado ou até mesmo se há um uso indesejável da rede.
- Surgiu então o protocolo NetFlow como alternativa para fornecer estatísticas mais precisas sobre tráfego de rede e uso de largura de banda.

Definição

- O NetFlow é um protocolo de gerenciamento de redes desenvolvido pela Cisco Systems com o intuito de promover a coleta e registro de informações sobre todo o tráfego IP nas interfaces de entrada e saída de um roteador ou switch, considerando-se que este protocolo esteja habilitado em tais interfaces.
- Em termos gerais, este protocolo considera os pacotes como sendo parte de um fluxo ao invés de simplesmente conta-los unitariamente.
- Um fluxo corresponde a uma sequência unidirecional de pacotes entre máquinas de origem e destino e, portanto, deve haver sempre dois fluxos em cada sessão.
- Na medida em que os pacotes são agrupados em fluxos, os administradores de redes são capazes de compreender de forma mais abrangente as aplicações que fazem uso da rede.

Funções

- Quando um pacote desconhecido chega a um roteador ou switch por meio de uma interface, o dispositivo em questão decide se deve ou não encaminhar tal pacote.
- Se o pacote for encaminhado para o destino, cria-se uma entrada no *Flow Cache* do dispositivo com os campos de identificação relativos a tal pacote.
- A medida em que novos pacotes IP entram por uma interface, o protocolo NetFlow identifica o seu fluxo e verifica se já existe uma entrada deste fluxo na tabela *cache*. Caso exista, o NetFlow comuta diretamente para a interface de destino especificada. Caso não exista, o NetFlow realiza um *lookup* nas tabelas de roteamento e nas tabelas de *access-list*.
- Se os pacotes possuírem alguma restrição nas tabelas de *access-list* ou se o IP destino não for encontrado nas tabelas de roteamento, o pacote é então encaminhado para a interface "NULL" (um pacote com destino para esta interface identifica que ele foi descartado). O NetFlow cria uma entrada na tabela *cache* para o destino "NULL".
- Outra função importante do NetFlow é a exportação de fluxos, conhecida como *flow-export*. O *flow-export* é realizado através do envio de dados encapsulados em pacotes UDP e o seu destino é o IP do coletor configurado previamente no roteador ou switch.
- Um fluxo mantido no *cache* de um roteador ou switch é exportado para um coletor nas seguintes situações: (i) o fluxo permanece ocioso por mais de 15 segundos, (ii) sua duração excede 30 minutos, (iii) uma conexão TCP é encerrada com a *flag* "FIN" ou "RST", (iv) a tabela de fluxo está cheia, (v) o usuário redefine as configurações de fluxo.
- A partir do fluxo recebido, o coletor pode então analisar tais dados e criar gráficos e relatórios precisos para permitir que o administrador de redes possa ter uma visão panorâmica da situação da rede.

Campos de Identificação

- O NetFlow analisa os fluxos IP ao invés de contar unitariamente pacotes nas interfaces de entrada e saída de um roteador ou switch.

- Um fluxo corresponde a um feixe de pacotes IP contendo pelo menos 8 (oito) campos de identificação:
    - Endereço IP de Origem.
    - Endereço IP de Destino.
    - Porta de Origem.
    - Porta de Destino.
    - Protocolo de Camada 3.
    - Tipo de Serviço (ToS).
    - Interface de Origem.
    - Interface de Destino.

- É importante frisar que a depender da versão do NetFlow, pode-se incluir todos esses campos e ainda informações adicionais, como rótulos MPLS e endereços IPv6.

Vantagens do NetFlow

- As principais vantagens da utilização do protocolo NetFlow são:
    - Funcionamento como *cache* para acelerar os *lookups* nas tabelas de roteamento.
    - Dispensa a verificação de tabelas de *access-list* (apenas de entrada) toda vez que um pacote chega, tornando mais eficiente o processo de roteamento.
    - Permite a exportação das informações de fluxo utilizadas pelo *cache* do NetFlow, facilitando a coleta de dados para futuras análises sem a necessidade de colocar um analisador em cada enlace.

Versões do NetFlow

- As diferentes versões do protocolo NetFlow são:
    - v1 (obsoleta): Primeira implementação. Restrita a IPv4.
    - v5: Versão mais comum, disponível em muitos roteadores. Ainda restrita a IPv4.
    - v6 (obsoleta): Já não suportada pela Cisco.
    - v7 (obsoleta): Idêntica a versão 5, mas incluindo um campo de roteador de origem.
    - v8 (obsoleta): Possui várias formas de agregação.
    - v9: Baseada em *templates*, disponível em muitos roteadores. Principalmente usada em IPv6, MPLS e BGP.
    - v10 (IPFIX): Norma IETF baseada no NetFlow v9, mas incorporando vários aprimoramentos.

Softwares Open-Source para Análise de NetFlow

- Dentre os softwares open-source disponíveis comercialmente para análise de dados NetFlow, podem ser citados:
    - Flowscan.
    - Cflowd.
    - NTop.
    - EHNT.
    - Flow-tools.
    - BPFT.
    - AnonTool.
    - Panoptis.

Propostas de Monitoramento com Análise de NetFlow

- O NetFlow é um protocolo de monitoramento de redes capaz de oferecer estatísticas detalhadas sobre o tráfego de dados em uma determinada rede. Dentre as propostas de monitoramento possíveis com a utilização dos parâmetros disponibilizados por este protocolo, podem ser citadas:
    - Monitoramento de Largura de Banda: Os softwares que realizam o monitoramento de largura de banda a partir de análises de NetFlow (e.g. NetFlow Analyzer) gerenciam a rede em tempo real com o intuito de identificar quais são os agentes que podem consumir maior largura de banda. Estes agentes podem ser usuários, aplicativos, protocolos ou endereços IP. É possível ainda implementar um monitor de largura de banda de rede que utiliza as análises do NetFlow de forma programada para meses, dias ou até mesmo minutos, sendo possível obter um conjunto de dados a longo e curto prazo. Dessa forma, é possível que o administrador de redes obtenha gráficos e relatórios detalhados sobre a utilização da largura de banda da rede monitorada.
    - Monitoramento de Picos de Tráfego: Os picos de tráfego em uma rede podem ser monitorados a partir da utilização de softwares que lidam com análises de NetFlow, como o próprio NetFlow Analyzer. Esta ferramenta permite que o administrador de redes possa monitorar o fluxo de pacotes de forma reativa ou proativa. Em outras palavras, é possível monitorar o fluxo de pacotes em interfaces de um determinado roteador ou switch e verificar se o volume de tráfego excede um valor limiar com base em parâmetros pré-definidos, como horário do dia, dia da semana, entre outros. É possível ainda monitorar o fluxo de pacotes de forma não-pontual, ou seja, verificar quais são os roteadores ou switches em uma rede que possuem volume de tráfego acima de um valor limiar com base nos mesmos parâmetros citados anteriormente. Sendo assim, é possível que o administrador de redes obtenha gráficos e relatórios detalhados sobre os picos de tráfego que ocorrem no(s) ativo(s) que compõe(m) a rede monitorada.
    - Monitoramento de Ataques DDoS: Os ataques DDoS podem ser monitorados e até mesmo mitigados com a utilização de softwares que lidam com análises de NetFlow, como o NetFlow Analyzer. Em termos gerais, é possível analisar os picos anormais de tráfego utilizando um mecanismo de alerta disponível em tais softwares e identificar e mitigar ataques DDoS. É possível ainda configurar o algoritmo de detecção de ataques DDoS de acordo o projeto da rede e os tipos de ameaças que mais a afetam. Dessa forma, conseguem-se gerar gráficos e relatórios detalhados sobre o volume de tráfego e sobre alertas de possíveis ataques DDoS.