Instalação e configuração nfdump e nfsen

Requisitos

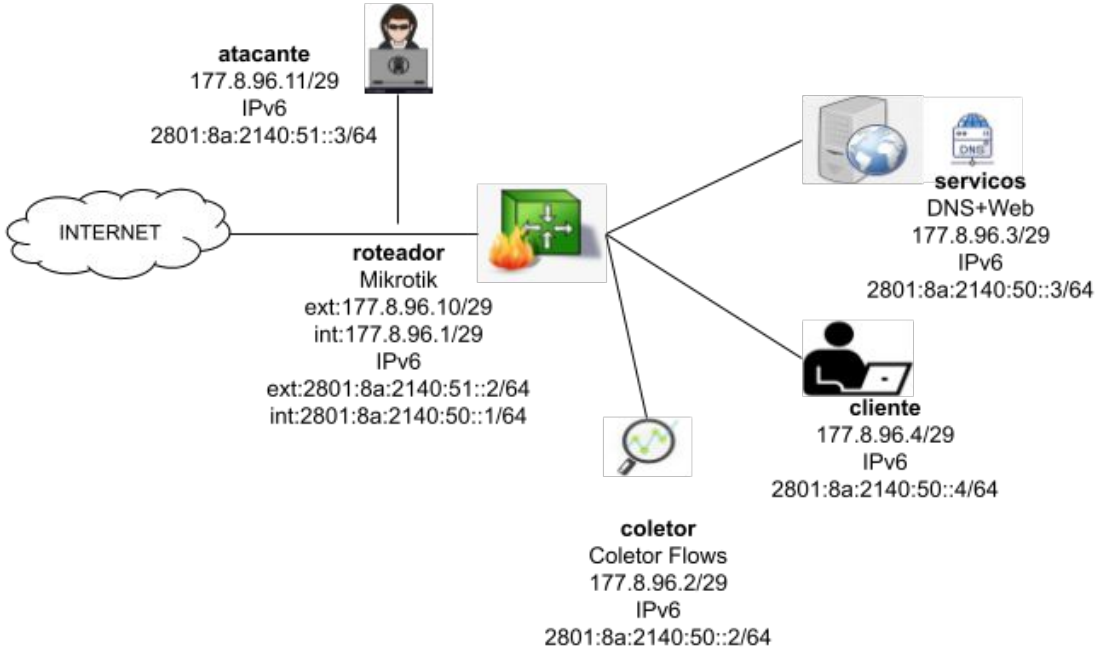
Hardware:

- 2G RAM
- 20G de disco
- 2 cores.

Sistema Operacional:

- Debian 11.6
- Instalação básica
- tcpdump
- sudo

Ambiente para este treinamento



Preparando o ambiente

Aplicações necessárias: servidor web, PHP, Perl, RRDTool e módulos relacionados

```
$ sudo apt install git pkg-config php php-dev apache2 libapache2-mod-php rrdtool librrd-dev
rrdtool librrds-perl libmailtools-perl libsocket6-perl
```

Preparando o ambiente

Servidor web - configuração básica para fins de demonstração:

- Alterar o DocumentRoot para /var/www
- Somente http

```
<VirtualHost *:80>

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>
```

Preparando o ambiente

Relembrando, o nfdump é um conjunto de ferramentas onde estão incluídos:

- **nfcapd**: Recebe os datagramas enviados pelo(s) agente(s) e armazena os dados em formato binário, rotacionando automaticamente a cada 5 minutos. Suporta as versões 5,7 e 9 do netflow;
- **sfcapd**: Similar ao nfcapd, trata flows obtidos por sFlow e armazena os dados em formato binário, sempre compatíveis com o formato NetFlow;
- **nfdump**: Permite análise minuciosa dos dados armazenados pelos coletores. Conta com sintaxe similar à do tcpdump, possibilita *filtrar* e *agregar* os dados de acordo com parâmetros definidos pelo usuário.

Preparando o ambiente

O nfdump:

- Mantido e documentado por Peter Haag no Github;
- Diversas versões, atenção para incompatibilidades com agentes;
- Utilizaremos a versão 1.6.16
- Fácil instalação.

Instalar as dependências:

```
$ sudo apt install doxygen byacc flex libbz2-dev libtool bison librrd-dev gawk
```

Preparando o ambiente

Obter e descompactar o pacote:

```
$ cd /opt
$ sudo wget https://github.com/phaag/nfdump/archive/refs/tags/v1.6.16.tar.gz
$ sudo tar -xvzf v1.6.16.tar.gz
$ cd nfdump-1.6.16
```

Preparando o ambiente

Compilar e instalar

$ sudo ./configure --enable-sflow --enable-nfprofile
$ sudo make
$ sudo make check *(opcional, mas é interessante para verificar se está tudo ok)*
$ sudo make install
$ sudo ldconfig *(para atualizar a relação de bibliotecas e os aplicativos. Usado quando alterar versão)*

Preparando o ambiente

Integração do RRDTool e PHP

- Instalação da biblioteca do RRDTool para php:

```
$ sudo pecl install rrd
```

- Criar arquivo /etc/php/7.4/mods-available/rrd.ini e inserir a linha abaixo:

```
extension=rrd.so
```

- Ativar o módulo rrd para PHP:

```
$ sudo phpenmod rrd
```

Preparando o ambiente

O NfSen:

- Interface web para o nfdump;
- Exibe os dados de flow armazenados pelos coletores;
- Permite a navegação nos dados;
- Processa dados de flow em tempo e filtros;
- Construir estatísticas tipo Top N e agregações por endereços, portas, protocolos, etc.

Disponível em: https://sourceforge.net/projects/nfsen/

Preparando o ambiente

Criar o diretório “/data”. Em produção planejar um file system separado “/data” com o tamanho adequado. Isto vai depender do volume de tráfego, quantidade de agentes e por quanto tempo você deseja armazenar os dados.

```
$ sudo mkdir /data && sudo mkdir -p /data/nfsen && cd /data/nfsen
$ sudo cp /home/csirt/nfsen-1.3.6p1.tar.gz .
$ ls
nfsen-1.3.6p1.tar.gz
$  sudo tar -xvzf nfsen-1.3.6p1.tar.gz
$  cd nfsen-1.3.6p1/
```

Editar o arquivo /data/nfsen/nfsen-1.3.6p1/libexec/NfSenRRD.pm na linha 76 para aceitar a versão 1.7 do RRD.

```
if ( $rrd_version >= 1.2 && $rrd_version < 1.8 )
```

Preparando o ambiente

Criar o usuário **netflow** e adicioná-lo no grupo www-data. Este é o usuário padrão que usaremos no nfsen.conf. Em seguida, altere a conta do usuário **netflow** para **nologin** utilizando o comando **vipw.**

```
# adduser netflow www-data
# vipw

$ sudo < /etc/group grep netflow
www-data:x:33:netflow
netflow:x:1001:
```

Preparando o ambiente

Criar o arquivo de configuração do NfSen e editá-lo de acordo com nosso ambiente:

```
$  sudo cp /data/nfsen/nfsen-1.3.6p1/etc/nfsen-dist.conf /data/nfsen/nfsen-1.3.6p1/etc/nfsen.conf
$  sudo vi /data/nfsen/nfsen-1.3.6p1/etc/nfsen.conf
```

Preparando o ambiente

```
$BASEDIR     = "/data/nfsen";
$HTMLDIR     = "/var/www/nfsen/";
$PREFIX      = '/usr/local/bin';
$USER        = "netflow";
$WWWUSER     = "www-data";
$WWWGROUP    = "www-data";
```

Preparando o ambiente

```
%sources = (
'roteador' => { 'port' => '9995', 'col' => '#0000ff', 'type' => 'netflow', 'IP' => '177.8.96.1' },
'servicos' => { 'port' => '9996', 'col' => '#ffd700', 'type' => 'sflow', 'IP' => '177.8.96.3' },
);
```

- Se houver na sua infraestrutura agentes sflow e netflow, basta agrupar em portas diferentes.

Preparando o ambiente

Instalar o NfSen

Ao executar o instalador alguns processos são feitos:

- Cria o ambiente do NFSen debaixo do BASEDIR;
- Copia os arquivos php e html para o HTMLDIR;
- Cria o perfil live e prepara sua base RRD;
- Cria e configura o config.php.

```
$ cd /data/nfsen/nfsen-1.3.6p1
$ sudo ./install.pl ./etc/nfsen.conf
```

Preparando o ambiente

Neste momento será:

- Verificado as dependências do Perl;
- Instalado as aplicações na estrutura indicada no nfsen.conf;
- Criada a estrutura padrão de diretórios utilizada pelo nfsen indicada na variável SUBDIRLAYOUT.

Comandos básicos:

Iniciar o serviço
$ sudo /data/nfsen/bin/nfsen start

Após alteração no nfsen.conf. executar o reconfig
$ sudo /data/nfsen/bin/nfsen reconfig

Status do nfsen
$ sudo /data/nfsen/bin/nfsen status

Preparando o ambiente

Listar os processos ativos:

```
$ ps aux|grep capd

netflow   27862  0.0  0.4  14264  4296 ?        S    15:25   0:00 /usr/local/bin/nfcapd -w
-D -p 9995 -u netflow -g www-data -B 200000 -S 1 -P /data/nfsen/var/run/p9995.pid -z -l
roteador -l /data/nfsen/profiles-data/live/roteador

netflow   27865  0.0  0.3  13180  3952 ?        S    15:25   0:00 /usr/local/bin/sfcapd -w
-D -p 9996 -u netflow -g www-data -B 200000 -S 1 -P /data/nfsen/var/run/p9996.pid -z -l
servicos -l /data/nfsen/profiles-data/live/servicos
```

Preparando o ambiente

Iniciar o servidor web apache2:

```
$ sudo systemctl start apache2
```

Neste momento já é possível acessar **http://hostname/nfsen/nfsen.php** mas por enquanto ainda não temos dados para visualizar.