nic.br cgi.br | cert.br

Live Intra Rede – Principais Ataques na Internet

30 de setembro de 2020

Evento *Online*

Uso de *Netflows* para Segurança

Dr. Klaus Steding-Jessen
Gerente Técnico
jessen@cert.br

cert.br nic.br cgi.br

Objetivos

Provavelmente você já tem habilidade de gerar *netflow* nos seus elementos de rede

- custo zero

É possível fazer tudo com *software* livre

- custo zero

***Netflows* para segurança e não só para engenharia de tráfego**

- detectar *botnets*, DDoS saindo da sua rede, etc
- dados históricos para investigação de incidentes

Todos os exemplos mostrados utilizaram

- `nfcapd` ou `sfcapd` para coleta dos *netflows*
- `nfdump` para consulta

O que é um *NetFlow*

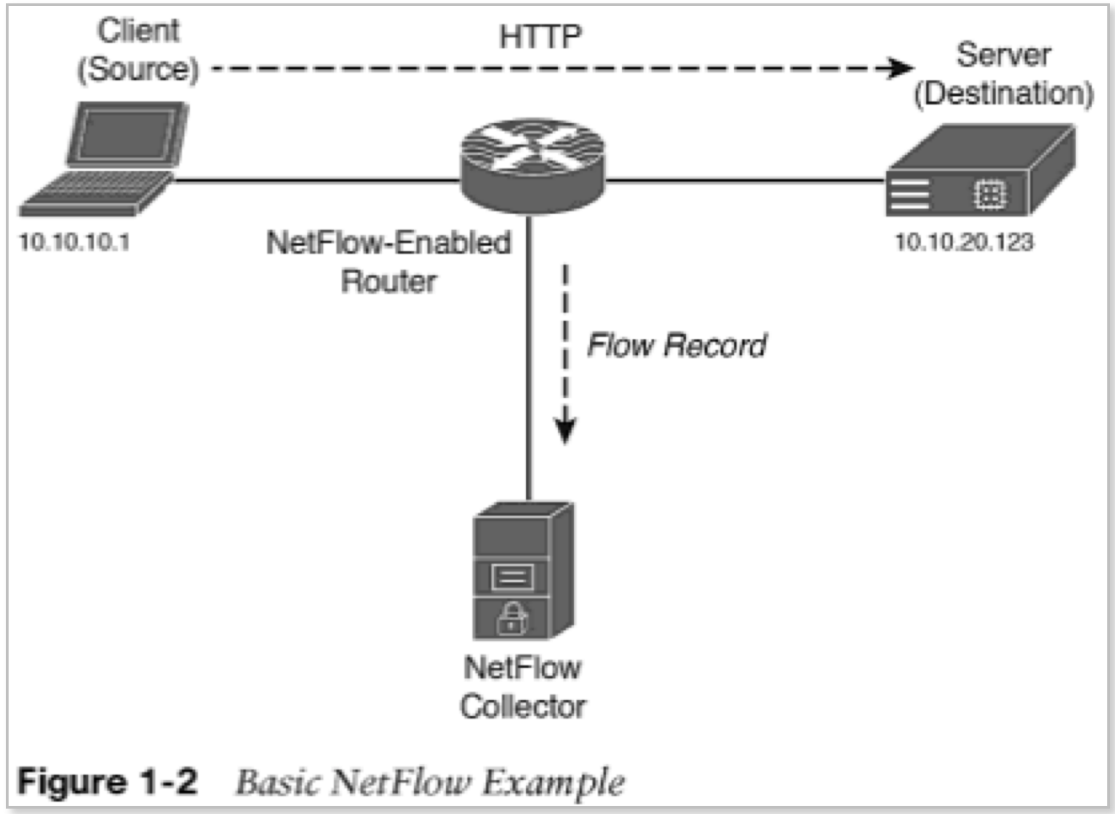

Figure 1-2 *Basic NetFlow Example*

Table 1-1 *NetFlow Five-Tuple*

Field	Value
Source IP address	10.10.10.1
Destination IP address	10.10.20.123
Source port	13578
Destination port	80
Protocol	TCP

Fontes:

Network Security with NetFlow and IPFIX: Big Data Analytics for Information Security
http://www.ciscopress.com/store/network-security-with-netflow-and-ipfix-big-data-analytics-9781587144387

NetFlow – Wikipedia
https://en.wikipedia.org/wiki/NetFlow

Exemplo de *NetFlow*: **Clientes Consultando DNS do Google**

```
$ nfdump -R /var/log/flows/2017/12/06 \
  'proto udp and dst port 53 and (dst host 8.8.4.4 or dst host 8.8.8.8)'
Date first seen          Duration Proto     Src IP Addr:Port     Dst IP Addr:Port
2017-12-06 00:00:30.833    0.000 UDP    xxx.xxx.10.134:56263 ->     8.8.8.8:53
2017-12-06 00:02:04.330    0.000 UDP     xxx.xxx.77.56:54475 ->     8.8.8.8:53
2017-12-06 00:03:47.530    0.000 UDP    xxx.xxx.10.134:40439 ->     8.8.8.8:53
2017-12-06 00:03:50.097    0.000 UDP     xxx.xxx.77.56:57897 ->     8.8.8.8:53
2017-12-06 00:08:23.849    0.000 UDP     xxx.xxx.62.27:53777 ->     8.8.8.8:53
2017-12-06 00:09:02.758    0.000 UDP    xxx.xxx.10.210:55233 ->     8.8.8.8:53

[...]

2017-12-06 15:38:43.989    0.000 UDP     xxx.xxx.11.83:46347 ->     8.8.8.8:53
2017-12-06 15:38:45.134    0.000 UDP     xxx.xxx.77.56:47928 ->     8.8.8.8:53
2017-12-06 15:39:34.757    0.000 UDP    xxx.xxx.13.106:32768 ->     8.8.4.4:53
2017-12-06 15:39:36.639    0.000 UDP     xxx.xxx.11.83:35310 ->     8.8.8.8:53
2017-12-06 15:39:43.110    0.000 UDP   xxx.xxx.115.110:57283 ->     8.8.4.4:53
Summary: total flows: 3341, total bytes: 149035520, total packets: 1710592, avg
  bps: 21144, avg pps: 30, avg bpp: 87
Time window: 2017-12-06 00:00:00 - 2017-12-06 15:39:59
Total flows processed: 53147598, Blocks skipped: 0, Bytes read: 3409846180
Sys: 10.574s flows/second: 5025915.9  Wall: 10.563s flows/second: 5031249.4
```

Detecção de CPEs Comprometidos:
Via Acessos a Servidores DNS Maliciosos

Sugestão de consulta *NetFlow*

- protocolo UDP porta destino 53 (DNS)
- origem no bloco de clientes
- cujo destino **não** seja
  - o seu recursivo
  - os servidores do Google (ou outros servidores públicos)

```
$ nfdump -R /var/log/flows/2017/12/06 'proto udp and dst port 53 and src net
  xx.xx.xx.xx/nn and not (dst host 8.8.4.4 or dst host 8.8.8.8 or dst host
  <seu-recursivo>)'
```

Como interpretar o resultado

- todo IP que aparecer no resultado consultou um DNS potencialmente malicioso
  - provavelmente está invadido
  - é necessário atuar
    - ex: atualizar *firmware*, trocar senha padrão, corrigir vulnerabilidades, etc

Detecção de *Botnets* IoT:
Via Acessos a IPs de Comando e Controle

Sugestão de consulta *NetFlow*

- destino a IPs publicamente listados como comando e controle de *botnets* IoT (que incluem *botnets* de CPEs)

  https://www.abuseat.org/iotcc.txt

```
$ nfdump -R /var/log/flows/2017/12/06 'proto tcp and dst ip in [ @include iotcc.txt ]'
```

Como interpretar o resultado

- todo IP que aparecer no resultado acessou o comando e controle
  - provavelmente é um IoT ou um CPE invadido
  - é necessário atuar
    - se for IoT de cliente: contatá-lo para atualizar *firmware*, trocar senha padrão, corrigir vulnerabilidades, etc;
    - se for um CPE invadido: atualizar *firmware*, trocar senha padrão, corrigir vulnerabilidades, etc

Outra fonte de IPs maliciosos
https://urlhaus.abuse.ch/downloads/text_online/

Ataques DDoS:
Detecção de grandes geradores de tráfego (1/2)

Sugestão de consulta *NetFlow*

- procurar por todos os IPs que geraram muito tráfego
- somente em uma rede específica (CIDR)
- excluindo todos os serviços legítimos (como servidores web, vídeo conferência, etc)

```
$ nfdump -R /var/log/flows/2017/12/07 -s srcip/bytes -L 10G -n 10 'src net
  xx.xx.xx.xx/nn and not dst net xx.xx.xx.xx/nn and not ip in [ @include servers.txt ]'
```

Parâmetros da consulta:

- **`-s srcip/bytes`** – mostra estatísticas por IP, ordenado por *bytes*
- **`-L 10G`** – mostra somente os *flows* com 10 Gbytes ou mais de tráfego
- **`-n 10`** – mostra somente os top 10 IPs
- **`xx.xx.xx.xx/nn`** – deve ser o bloco CIDR de sua rede que você deseja ver se tem algum **amplificador** ou ***botnet* IoT**
- **`src net xx.xx.xx.xx/nn`** – especifica que só interessa o tráfego com origem na sua rede
- **`not dst net xx.xx.xx.xx/nn`** – especifica que o destino deve ser fora da sua rede (ou seja, não pega tráfego interno)
- **`not ip in`** – exclui todos os IPs de uma lista específica de IPs
- **`servers.txt`** – um arquivo ASCII que contém uma lista com todos os servidores da rede que geram muito tráfego e que você não está interessado em consultar pois já sabe que geram muito tráfego (exemplo: servidores *web*, *e-mail*, etc)

Ataques DDoS:
Detecção de grandes geradores de tráfego (2/2)

Resultado da consulta *NetFlow*

```
$ nfdump -R /var/log/flows/2017/12/07 -s srcip/bytes -L 10G -n 10 'src net xx.xx.xx.xx/nn and not dst net
  xx.xx.xx.xx/nn and not ip in [ @include servers.txt ]'

Top 10 Src IP Addr ordered by bytes:
     Src IP Addr  Flows(%)     Packets(%)       Bytes(%)      pps      bps   bpp
    xxx.xxx.9.28  1.9 M(16.6) 983.8 M(16.6)   1.4 T(38.6) 17919  206.0 M  1436
   xxx.xxx.18.85 154428( 1.3)  79.1 M( 1.3) 100.8 G( 2.8)  1443   14.7 M  1275
   xxx.xxx.62.49 128903( 1.1)  66.0 M( 1.1)  94.6 G( 2.6)  2102   24.1 M  1432
   xxx.xxx.46.36 266474( 2.3) 136.4 M( 2.3)  93.3 G( 2.6)  2486   13.6 M   683
    xxx.x.106.10 109648( 0.9)  56.1 M( 0.9)  80.9 G( 2.2)  1126   13.0 M  1440
  xxx.xxx.75.167 108737( 0.9)  55.7 M( 0.9)  80.5 G( 2.2)  1296   15.0 M  1446
    xxx.xxx.2.21 134183( 1.2)  68.7 M( 1.2)  80.0 G( 2.2)  1251   11.7 M  1164
 xxx.xxx.236.103 103314( 0.9)  52.9 M( 0.9)  75.2 G( 2.1)   965   11.0 M  1421
  xxx.xxx.10.215  73854( 0.6)  37.8 M( 0.6)  54.9 G( 1.5)   688    8.0 M  1451
   xxx.xxx.125.2  83531( 0.7)  42.8 M( 0.7)  46.2 G( 1.3)   779    6.7 M  1080

Summary: total flows: 11587182, total bytes: 3657941800960, total packets: 5932637184, avg bps: 533034287, avg
  pps: 108062, avg bpp: 616
Time window: 2017-12-07 00:00:00 - 2017-12-07 15:14:59
Total flows processed: 41883344, Blocks skipped: 0, Bytes read: 2687644604
Sys: 16.990s flows/second: 2465146.9  Wall: 16.975s flows/second: 2467332.3
```

Como interpretar o resultado

- todo IP que aparecer no resultado potencialmente gerou um ataque DDoS para fora da rede
  - necessário investigar se é um amplificador ou parte de uma *botnet*

NetFlows: **Referências**

RFC 7011 / STD 77: *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information*

- https://tools.ietf.org/html/rfc7011

NetFlow version 9

- https://www.cisco.com/c/en/us/products/ios-nx-os-software/netflow-version-9/

NFDUMP/ NfSen

- http://nfdump.sourceforge.net

Mikrotik Traffic Flow

- https://wiki.mikrotik.com/wiki/Manual:IP/Traffic_Flow

Juniper Flow Monitoring

- https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/services-interfaces/flow-monitoring.html

Uso de *Flows* no Tratamento de Incidentes da Unicamp

- https://ftp.registro.br/pub/gts/gts26/01-flows-unicamp.pdf
- https://youtu.be/ckEX7vUFOzk

Como Melhorar o Cenário:
Investir no Básico

Manter Sistemas Atualizados

- Acompanhe todos os fabricantes do seu parque
- Atualize **TODOS** os sistemas e aplicações
  - mesmo que sejam “só internos”
- Defina regras para priorizar a aplicação de correções de segurança
  https://www.first.org/cvss/

Múltiplos Fatores de Autenticação

- Impede sucesso de força bruta de senhas
- Reduz impacto do comprometimento de credenciais

Tecnologias:

- Chaves criptográficas / certificados
- *Tokens*
  - em *hardware* (FIDO2/U2F)
  - em *software* (HOTP/TOTP)

Receber e Tratar Notificações

Acompanhar todas as notificações enviadas para

- *E-mail* do contato `abuse-c` do ASN no serviço `whois`
- *E-mail* de abuse ou do grupo de tratamento de incidentes

Considere que:

- Outras organizações e CSIRTs tem dados relevantes a passar
- Geralmente informações que podem utilizadas gratuitamente

Depois de Investir no Básico:
Adotar Protocolos Mais Modernos

	Padrões	Vantagens da Adoção
Criptografia forte	HTTPS mandatório e HSTS Versões atuais de TLS *Forward Secrecy*	Garantia das transações e da proteção de dados Reduz a chance de quebra da criptografia Impede quebra de cripto de tráfego antigo capturado
Segurança de DNS	DNSSEC	Proteção contra envenenamento de *cache* Habilitar o uso de outras tecnologias como o DANE
Segurança de *e-mail*	STARTTLS • idealmente c/ DANE DMARC, DKIM e SPF	Proteção contra *sniffing* (“espionagem”) Aumento da reputação da mensagem legítima (ajuda a prevenir *phishing* da sua marca)
Protocolo IP	IPv6 é o atual IPv4 é legado – e já acabou • novas redes só terão IPv6	Mais estabilidade • Não depender de CGN ou tradução v6 → v4 • Redes móveis tendem a ter IPv6 nativo no futuro Facilita o processo investigativo e de tratamento de incidentes
Segurança de roteamento	RPKI	Certificação de recursos Validação de origem no BGP

Padrões	Referências
Tokens em *hardware* (FIDO2/U2F)	https://fidoalliance.org/specifications/
Tokens em *software* (HOTP/TOTP)	https://tools.ietf.org/html/rfc4226 https://tools.ietf.org/html/rfc6238
HTTPS mandatório e HSTS Versões atuais de TLS *Forward Secrecy*	https://www.ssllabs.com/ssltest/ https://ssl-config.mozilla.org https://observatory.mozilla.org https://letsencrypt.org/
DNSSEC	https://registro.br/tecnologia/dnssec/dnssec-para-provedores/ https://ftp.registro.br/pub/doc/tutorial-dnssec.pdf https://dnsviz.net
STARTTLS [idealmente c/ DANE] DMARC, DKIM e SPF	https://starttls-everywhere.org https://english.ncsc.nl/publications/factsheets/2019/juni/01/factsheet-secure-the-connections-of-mail-servers https://mecsa.jrc.ec.europa.eu/en/technical#starttls https://havedane.net https://dmarc.org https://dmarc.globalcyberalliance.org
IPv6	https://ipv6.br https://test-ipv6.com
RPKI	https://bcp.nic.br/rpki

Precisamos um Ecossistema mais Saudável:
Programa por uma Internet mais Segura

PROGRAMA INTERNET +SEGURA

Objetivo principal:

- Reduzir o número de sistemas que possam ser abusados para gerar ataques DDoS

Incentivo à adoção de boas práticas:

- *Hardening*
- Segurança de roteamento (MANRS)
- *Anti-spoofing* (BCP 38)
- Reduzir serviços abertos que permitam amplificação

Iniciativa conjunta:

- ISOC, NIC.br, SindiTelebrasil, Abranet, Abrint, Abinee

https://bcp.nic.br/i+seg

Obrigado

jessen@cert.br

notificações para: cert@cert.br

@certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br