Como se prevenir e atuar durante um incidente de segurança

Ênfase no uso de flows de rede

Intrarede - 13 de julho de 2022

Alexandre Berto Nogueira
CSIRT Unicamp

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

Agenda

- Apresentação do CSIRT Unicamp
- Bases da Prevenção
- Uso de Flows na Prevenção e Atuação em ISC
- Conclusão

INTRAREDE 2022

nic.br

Apresentação do CSIRT Unicamp- 25 anos

- Recebe, analisa, processa e responde os incidentes de segurança da Universidade
- Analisa flows de rede
- Realiza testes de detecção de vulnerabilidades
- Ministra palestras de conscientização para usuários finais
- Emite certificados digitais (projeto Globalsign/RNP)
- É um CSIRT de Coordenação: Não atua no ambiente computacional interno dos órgãos da Universidade

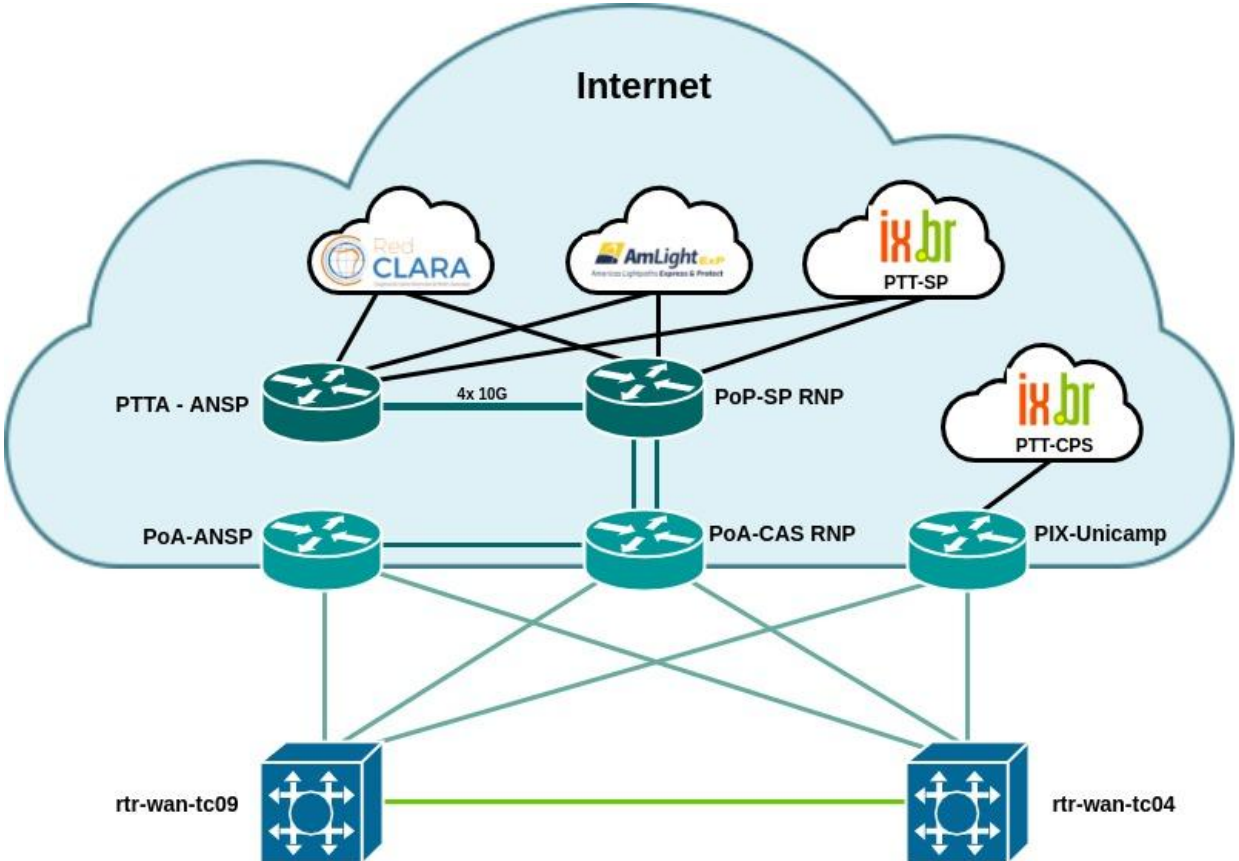
CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

INTRAREDE 2022

nic.br

Diagrama Simplificado - Unicamp



CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

PREVENÇÃO	
	Identidade de um Time Formação e Dedicação - Canais de comunicação Abertos e Funcionais - Permeabilidade Organizacional - Controle e Histórico de um chamado - Indicadores - Processos Definidos
	Visão de sua Infraestrutura Qual o comportamento padrão de sua rede ? - Inventário Atualizado - Ferramentas de monitoramento - Infraestrutura de registro de logs sincronizados - Backup de dispositivos de rede -Flows de Rede - Netflow/sFlow/IPFIX
	Avaliação Continuada Varredura de Vulnerabilidades Regulares - Conscientização - Usuários e Grupos Técnicos - Capacitação - Threat Hunting

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

PREVENÇÃO

Identidade de um Time
Formação e Dedicação - Canais de comunicação Abertos e Funcionais - Permeabilidade Organizacional - Controle e Histórico de um chamado - Indicadores - Processos Definidos

Visão de sua Infraestrutura
Qual o comportamento padrão de sua rede ? - Inventário Atualizado - Ferramentas de monitoramento - Infraestrutura de registro de logs sincronizados - Backup de dispositivos de rede -**Flows de Rede - Netflow/sFlow/IPFIX**

Avaliação Continuada
Varredura de Vulnerabilidades Regulares - Conscientização - Usuários e Grupos Técnicos - Capacitação - Threat Hunting

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

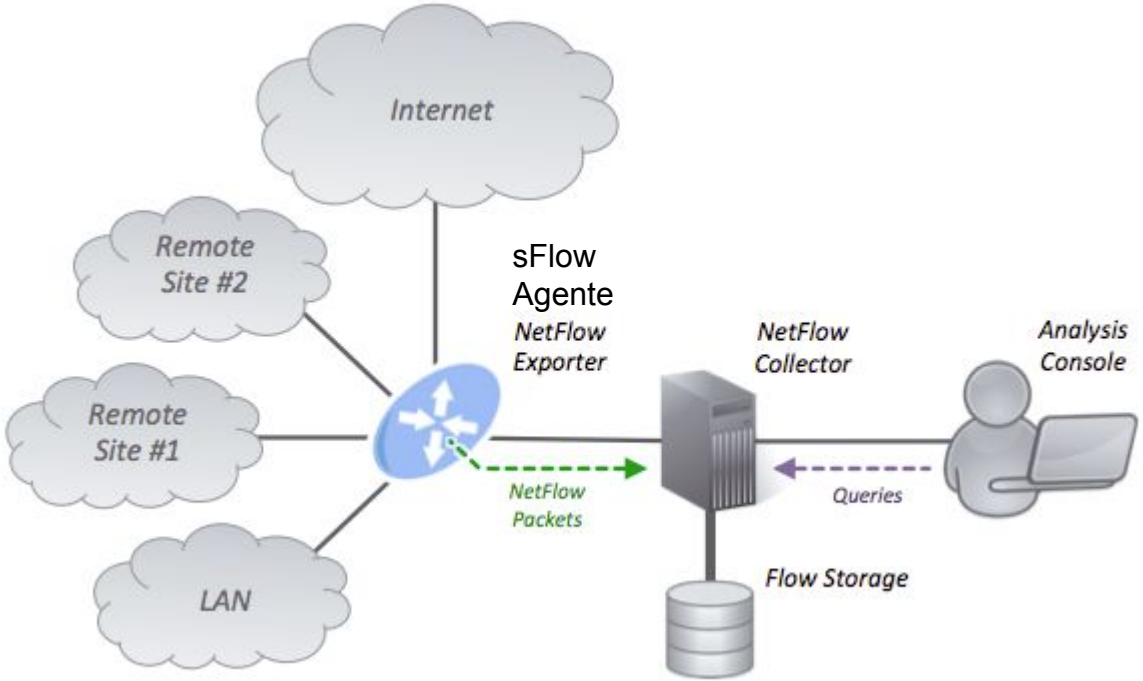
Flows de Rede

- **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."

INTRAREDE 2022

nic.br

Arquitetura de Funcionamento



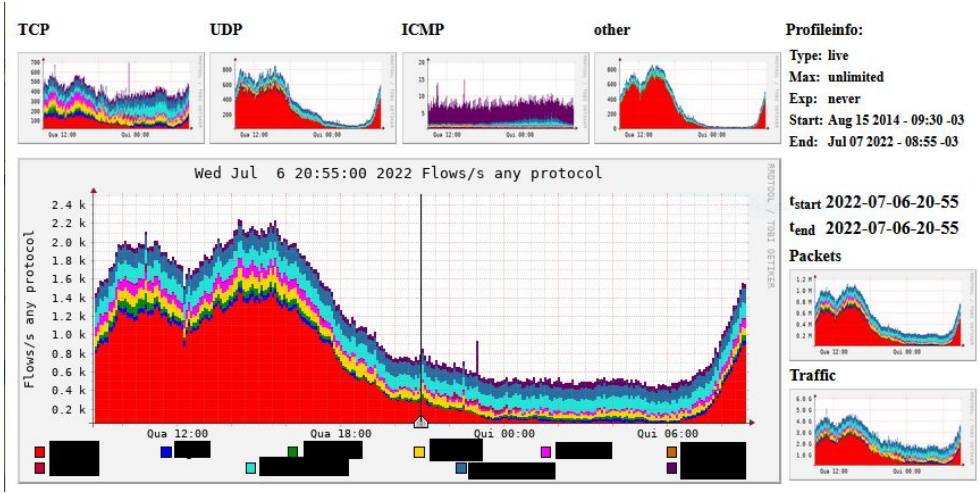
https://en.m.wikipedia.org/wiki/File:NetFlow_Architecture_2012.png

Tecnologia	Agentes/Exporters	Coletores e Frontends
sFlow	Alcatel-Lucent, Arista, Aruba, Cisco, Commscope, Dell, Extreme, F5, Fortinet, Huawei, Juniper. Linux, *BSD, OpenSwitch, Open vSwitch, Windows	nfdump-nfsen, ntop, PRTG, ELK, sflowtool*
IPFIX	Juniper, Mikrotik RouterOS , Linux, *BSD	PRTG, Scrutinizer, ELK
Netflow v9	*Cisco, Mikrotik RouterOS , Linux, *BSD*	nfdump-nfsen,ntop, PRTG, sflowtool*, ELK

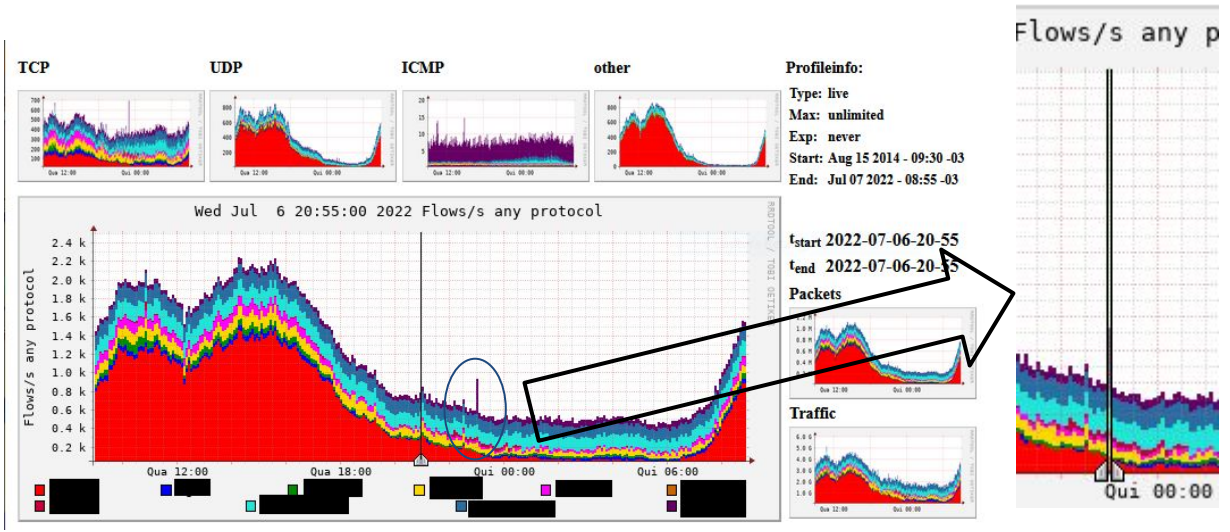
Possibilidades com os Flows

- Criar relatórios - Top Talkers, Top protocols, Top networks, Top ASN´s, etc
- Correlação de endereços e timeline de incidentes
- Ações preventivas como buscar serviços UDP/TCP que não deveriam estar abertos. Aderência a normas como gerência de porta 25 e Spoofing
- Sinais de Comprometimento analisando o seu tráfego com listas de endereços fontes conhecidas - C&C, Botnet, Miners, Rogue DNS, Threat Hunting.
- Scripts personalizados - ex. uso IPv4

Exemplo nfsen Comportamento de tráfego



Exemplo nfsen Comportamento de tráfego



Filter:

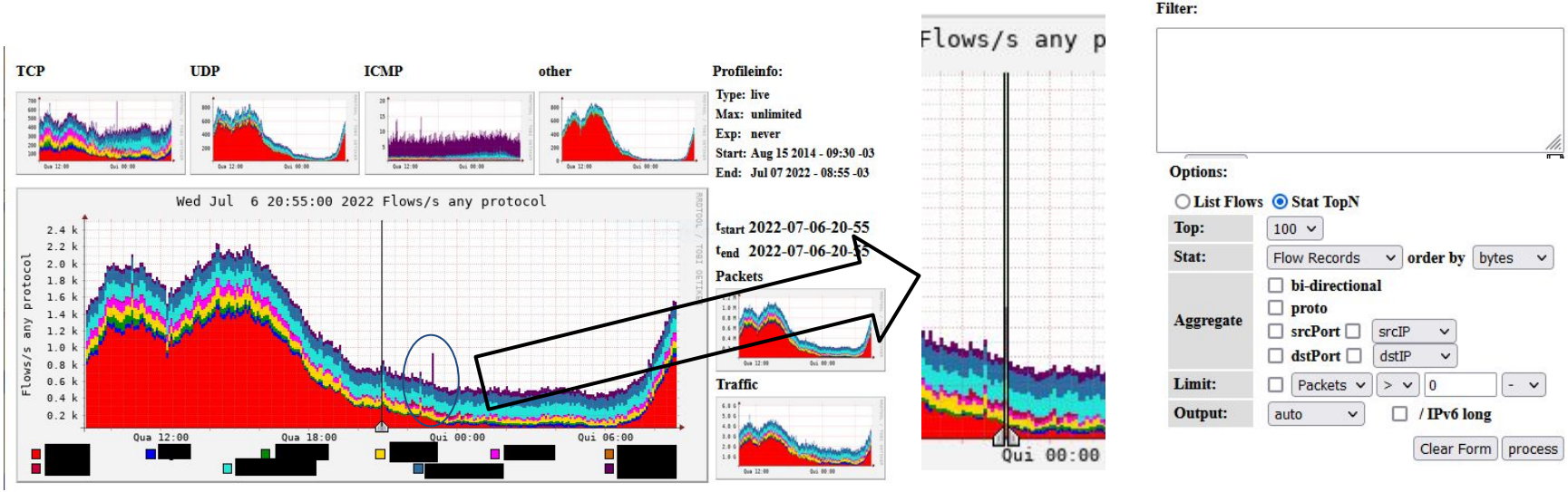
Options:

List Flows | Stat TopN

Top:	100
Stat:	Flow Records order by bytes
Aggregate	bi-directional proto srcPort srcIP dstPort dstIP
Limit:	Packets > 0 -
Output:	auto / IPv6 long

Clear Form process

Exemplo nfsen Comportamento de tráfego




```
** nfdump -M /data/nfsen/profiles-data/live/obj1  -T  -R
2022/07/06/nfcapd.202207062255:2022/07/06/nfcapd.202207062300 -n 100 -s record/bytes
Date first seen          Duration Proto Src IP Addr:Port    Dst IP Addr:Port       Packets     Bytes  Flows
2022-07-06 23:00:10.370    12.166 TCP   xxx.xxx.xxx.xxx:22  yyy.yyy.yyy.yy:30468     83708    128.2M 41854
2022-07-06 23:00:06.110     6.168 TCP   zzz.zzz.zzz.zz:22   yyy.yyy.yyy.yy:21699     31772     48.6M  15886
```

Exemplo de versatilidade com nfdump

- Início do confronto UK-RU - Ataques DDoS de provedores brasileiros com destino a Ucrânia.
- Parseamento de uma fonte de AS´s numbers ex. ipinfo.io
- Consulta em CLI utilizando o nfdump

```
# nfdump -M /data/nfsen/profiles-data/live/device1:device2  -T  -R
2022/07/04/nfcapd.202207040800:2022/07/04/nfcapd.202207042000 -n 5 -o long -s record/bytes 'as in [
@include asukr.txt ]'
Date first seen          Duration Proto Src IP Addr:Port     Dst IP Addr:Port     Packets    Bytes  Flows
2022-07-04 12:54:29.513    24.178 TCP   xxx.xxx.xx.xx:443    176.37.aaa.aa:53590 1536       2.3 M      3
2022-07-04 10:57:35.034     0.280  TCP   yyy.yyy.y.yy:443     46.119.bb.ccc:65033 1024       1.6 M      2
2022-07-04 11:40:04.669   207.401 UDP   zzz.zzz.zz.zzz:16024 217.175.d.eee:8999  1536       640512     3
```

Uso de Flows na Unicamp - nfdump/nfsen

vm 6 núcleos 12 GB de RAM, 500GB de disco

Tráfego Internet	3,8 Gbp/s
Taxa Máxima de Flows coletados	2.500 flows/s
Uso de Disco 1 dia de flows	1,2 GB
Tráfego de Rede	5 - 10 Mbps
Uso de Memória	1 - 2 GB
Pico máximo de carga	1.56
Histórico 1 ano e 6 meses	400 GB

Sugestão de Leituras

- **Exemplos de Configurações de Dispositivos - sFlow e IPFIX**
  - https://www.manageengine.com/products/netflow/help/configuring-mikrotik-ipfix.html
- **Lista de coletores sFlow**
  - https://sflow.org/products/collectors.php
- **Manual sFlowtool**
  - https://github.com/sflow/sflowtool
- **NFSen**
  - http://nfsen.sourceforge.net/
- **NFDump**
  - http://nfdump.sourceforge.net/

CSIRT UNICAMP
Computer Security Incident Response Team

UNICAMP

Obrigado!

Diretor: Eduardo Trettel (Segurança e Redes)

Adilson Paz da Silva

Alexandre Berto Nogueira

Daniela Regina Barbetti

Vanderlei Busnardo Filho

security@unicamp.br

berto@unicamp.br

INTRAREDE 2022

nic.br