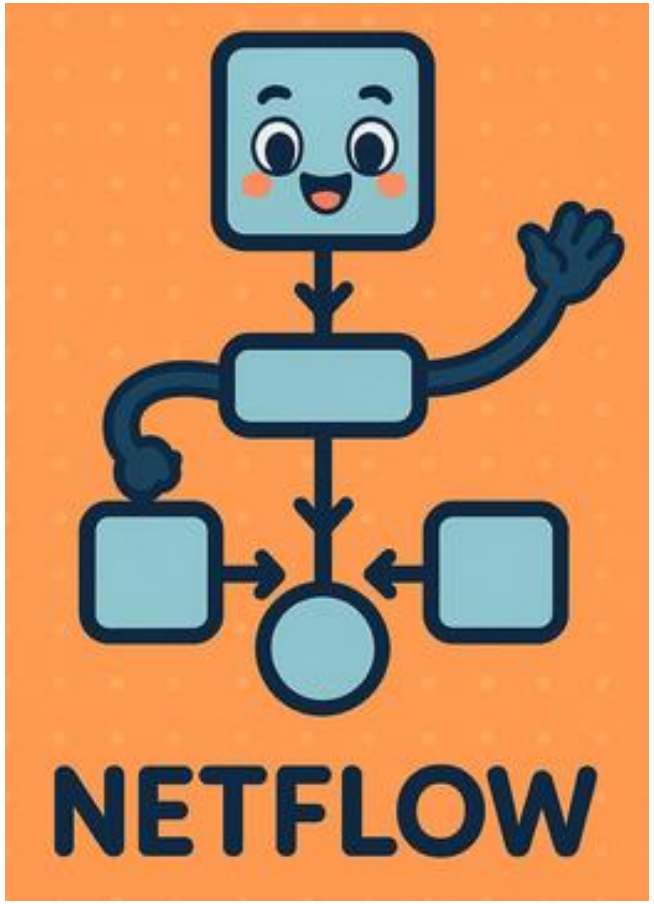
TLP:CLEAR

NetFlow na Linha de Frente: Visibilidade, Detecção e Resposta a Incidentes em Ambientes Financeiros

TLP:CLEAR

Uso de NetFlow
Visibilidade, Detecção, e Respostas

Demonstrar a Aplicação de NetFlow na Linha de Frente



Edney Fernandes

Administrador de Redes | Gerente Executivo no Banco da Amazônia

Membro do CSIRT,
Evangelizador IPv6,

Pai de duas meninas ;)

www.linkedin.com/in/edneyfer

Cenário atual de ameaças financeiras

TLP:CLEAR

Crescimento das Ameaças Cibernéticas

Fraude Eletrônica

Ransomware as a Service (RaaS)

Insider Threat

Ataques de **supply chain**

Sem visibilidade de rede, a resposta é sempre tardia.

Cenário atual de ameaças financeiras

TLP:CLEAR

Pressão Regulamentar e Conformidade

Banco Central (BACEN Resolução 4.893)

- Exige mecanismos de **Detecção** de ataques
- Procedimentos formais de **respostas** a incidentes
- **Retenção** de registros de eventos

LGPD (Lei Geral de Proteção de Dados):

Exige rastreabilidade completa em incidentes de vazamento de dados.

Normas internacionais com forte peso sobre auditoria de logs e análise de tráfego.

TLP:CLEAR

Cenário atual de ameaças financeiras

O Desafio da Visibilidade

Começa a dor de cabeça para os times de segurança e infraestrutura:

Grande parte do tráfego interno não é visível.

Muitos movimentos laterais não geram alertas tradicionais.

Acessos indevidos passam despercebidos se a instituição não tiver visibilidade de rede.

O que é NetFlow e como funciona

TLP:CLEAR

O que é NetFlow?

Tecnologia de **exportação de metadados** de tráfego IP.

Criado pela CISCO em 1990.
Monitoramento de tráfego, **análise de desempenho**, **cobrança baseada em uso.**

Resume sessões de comunicação em registros compactos chamados *flows* (fluxos).

VER COMPORTAMENTO SEM PRECISAR DO PAYLOAD.

O que é NetFlow e como funciona

TLP:CLEAR

⚠ **Importante Diferenciação Técnica**

- ❌ **NetFlow não é IDP/IPS**
- ❌ **NetFlow não é Full Packet Capture (PCAP)**
- ❌ **NetFlow não é SysLog ou Log de Firewall**

Resumo Estatístico de Tráfego

Não vê “o quê” foi transmitido

Vê “Quem falou com quem, quando e por quanto tempo”

O que é NetFlow e como funciona

TLP:CLEAR

Tipos e Versões

v5 — NetFlow v5 — Campos fixos, básico

Campos básicos (IP, porta, protocolo)

IPv6 v9 — NetFlow v9 — Campos flexíveis, templates

IPv6 — IPFIX — Padrão IETF aberto (RFC 7011–7015)

IPv6 — sFlow (Sampled Flow) — (RFC 3176), mantido pela sFlow.org

IPv6 — jFlow (Juniper Flow Monitoring), Equipamentos Juniper

Compatível com NetFlow v5/9, adaptado aos equipamentos Juniper

NetFlow v1, v5, v7 e v9

Ex: Netflow

```
{
  "srcaddr": "192.168.0.10",
  "dstaddr": "172.217.28.238",
  "srcport": 54321,
  "dstport": 443,
  "prot": 6,
  "tcp_flags": 0x1B,
  "packets": 12,
  "bytes": 6543,
  "start_time": "2025-07-27 12:01:45.321",
  "end_time": "2025-07-27 12:01:48.531",
  "src_mask": 24,
  "dst_mask": 24,
  "src_as": 0,
  "dst_as": 15169
}
```

FIN(0x01), SYN(0x02), PSH(0x08), ACK(0x10)

Arquitetura de Coleta e Análise

TLP:CLEAR

🧱 Arquitetura NetFlow — 3 Blocos Funcionais

Dispositivos que geram e enviam fluxos (flows).
Ex. switch (HP), router (CISCO), loadbalance (A-10), firewall (Fortinet), cloud (AWS)

Servidores que recebem, organizam e armazenam os dados de fluxo
Ex: Stealthwatch (Cisco), **Trafip (Telcomanager)**, Elastic Stack (ELK), Gigamon

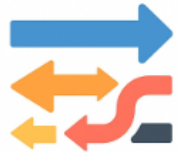
Ferramentas (NDR e SIEM) que analisam os flows e geram insights para o SOC.
Ex. Scrutinizer (Plixer), Flowmon (Progress), Darktrace, Vectra AI, Trend, Cisco.

NetFlow aplicado à infraestrutura

TLP:CLEAR

Identificação de top talkers

Análise de baseline de tráfego



Detecção de loops, floods e assimetria

Capacidade, latência indireta, jitter lógico

Top Talkers (Outbound Traffic)

Top Source IPs by Bytes

Rank	Src IP	Total Bytes	Total Packets	Avg bps	Flows
1	10.20.30.45	1.82 GB	1,245,000	48.5 Mbps	312
2	10.80.10.55	640 MB	412,300	17.0 Mbps	198
3	10.30.10.20	410 MB	298,100	10.9 Mbps	165
4	10.50.40.77	155 MB	132,900	4.1 Mbps	96
5	10.60.15.12	88 MB	79,500	2.3 Mbps	61

Top Destination IPs by Bytes

Rank	Dst IP	Total Bytes	Total Packets	Avg bps	Src Hosts
1	34.120.88.10	2.05 GB	1,402,000	54.6 Mbps	2
2	185.100.87.1	810 MB	560,400	21.6 Mbps	1
3	52.85.23.11	520 MB	360,100	13.9 Mbps	3
4	146.70.120.55	245 MB	198,300	6.5 Mbps	1
5	10.80.20.77	180 MB	154,800	4.8 Mbps	4

Top Applications / Ports

Rank	Dst Port	Protocol	Total Bytes	*% of Traffic*
1	443	TCP	3.10 GB	62%
2	53	UDP	810 MB	16%
3	445	TCP	540 MB	11%
4	22	TCP	260 MB	5%
5	3389	TCP	170 MB	3%

NetFlow Aplicado à Segurança (Detecção de Incidentes)

TLP:CLEAR

1) Beaconing (intervalos regulares)

Padrão: conexões curtas, baixo volume, repetidas em intervalo fixo.

Start Time	Dur	Proto	Src IP:Port	-> Dst IP:Port	Pkts	Bytes	bps	Flags	Exporter
10:00:00	2s	TCP	10.80.10.55:52144	-> 185.199.110.153:443	12	2.4K	9.6K	.AP..	core-fw-01
10:01:00	2s	TCP	10.80.10.55:52190	-> 185.199.110.153:443	11	2.2K	8.8K	.AP..	core-fw-01
10:02:00	2s	TCP	10.80.10.55:52231	-> 185.199.110.153:443	12	2.5K	10.0K	.AP..	core-fw-01
10:03:00	2s	TCP	10.80.10.55:52288	-> 185.199.110.153:443	11	2.3K	9.2K	.AP..	core-fw-01

➞ Intervalo regular de 60s + volume constante = **beaconing**.

2) Comunicação com C2 (Command & Control)

Padrão: sessão mais longa, baixo volume, destino raro.

Start Time	Dur	Proto	Src IP:Port	-> Dst IP:Port	Pkts	Bytes	bps	Flags	Exporter
10:15:10	210s	TCP	10.80.10.55:52310	-> 45.155.205.18:443	420	68.0K	2.6K	.AP..	core-fw-01

➞ Sessão persistente, baixo throughput, destino incomum = **canal C2**.

NetFlow Aplicado à Segurança (Detecção de Incidentes)

TLP:CLEAR

3) Exfiltração de dados (long flows + baixo PPS)

Padrão: fluxo muito longo, muitos bytes no total, poucos pacotes por segundo.

```
Start Time Dur    Proto Src IP:Port        -> Dst IP:Port       Pkts Bytes  PPS bps     Exporter
---------- ------------------------------------------------------------------------------------
02:05:00   1800s TCP   10.20.40.12:60211 -> 34.120.88.10:443 9000 620.0M 5   2.7Mbps wan-edge-01
```

➞ 30 minutos de sessão, ~5 PPS, volume alto = **exfiltração "low and slow"**.

4) Scans internos e laterais (movimento lateral)

Padrão: muitas tentativas curtas, mesma porta, vários destinos internos.

```
Start Time Dur  Prot Src IP:Port        -> Dst IP:Port      Pkts Bytes Flags  Exporter
---------- ------------------------------------------------------------------------
11:05:00   0.2s TCP  10.80.10.55:51001 -> 10.80.20.77:445   3    180  S....  dc-leaf-03
11:05:01   0.2s TCP  10.80.10.55:51002 -> 10.80.20.78:445   3    180  S....  dc-leaf-03
11:05:02   0.2s TCP  10.80.10.55:51003 -> 10.80.20.79:445   3    180  S....  dc-leaf-03
11:05:03   0.2s TCP  10.80.10.55:51004 -> 10.80.20.80:445   3    180  S....  dc-leaf-03
```

➞ SYNs rápidos em sequência para SMB = **scan/movimento lateral**.

Muitos ataques modernos
não precisam de payload visível.

NetFlow no Ciclo de Resposta a Incidentes

TLP:CLEAR

DETECÇÃO
Visibilidade Inicial com NetFlow

Desvios de baseline

CONTENÇÃO
Resposta Baseada em Fluxos

Quem isolar primeiro

ERRADICAÇÃO
Monitoramento Pós-Mitigação

Confirmar erradicação do tráfego

LIÇÕES APRENDIDAS
Forense com NetFlow

Verificar o histórico do incidente

NetFlow acelera decisão e reduz erro humano.

Caso Simulado 1: Exfiltração via DNS Túnel

TLP:CLEAR

1 Cenário do Incidente

- Host interno comprometido: `10.0.5.42`
- Objetivo do atacante: **exfiltrar dados** evitando HTTPS e proxies
- Técnica: **DNS Tunneling**

- **Característica-chave:**
  - Muitas consultas DNS
  - Alto número de pacotes
  - Volume pequeno por pacote
  - Comunicação contínua com **um único DNS externo**

2 O que aparece no ElastiFlow

🔷 Painel 1 – Flow Table (Outbound DNS)

Filtro no ElastiFlow

dst.port:53 AND network.direction:outbound

🔍 **Sinais de alerta**

- Mesmo **src.ip** → mesmo **dst.ip**
- DNS direto para Internet
- Alto número de pacotes
- Bytes por pacote muito consistentes
- Fluxos contínuos e paralelos

📊 Tabela de Fluxos

@timestamp	src.ip	dst.ip	proto	src.port	dst.port	packets	bytes	flow.duration
14:32:00	10.0.5.42	185.100.87.1	UDP	53421	53	670	199 KB	3m
14:32:00	10.0.5.42	185.100.87.1	UDP	53422	53	645	193 KB	3m
14:32:00	10.0.5.42	185.100.87.1	UDP	53423	53	660	197 KB	3m
14:32:00	10.0.5.42	185.100.87.1	UDP	53424	53	688	206 KB	3m

Caso Simulado 1: Exfiltração via DNS Túnel

TLP:CLEAR

🔷 Painel 2 – Time Series (DNS Traffic)

📈 DNS Queries over Time

Time	DNS Packets/s
14:30	0
14:31	0
14:32	45
14:33	47
14:34	46
14:35	48

➞ Tráfego **constante**, sem picos, típico de “low and slow”.

🔷 Painel 3 – Top DNS Destinations

📊 Top dst.ip (Port 53)

dst.ip	packets	bytes
185.100.87.1	5,420	1.61 MB

➞ A concentração anormal em **um único servidor DNS Externo.**

Caso Simulado 1: Exfiltração via DNS Túnel

TLP:CLEAR

🔷 Painel 4 – Bytes por Packet (Indicador-chave)

📊 Average Bytes per Packet

src.ip avg_bytes_per_packet

10.0.5.42 ~300 bytes

➞ Padrão típico de DNS tunneling (subdomínios longos e codificados).

Ex: Base64DoArquivo.exfil.credito-rural[.]com

🔷 Painel 5 – Geolocalização / ASN

📍 Enrichment

dst.ip: 185.100.87.1
ASN: Hosting Provider / Offshore
Country: Fora do país da operação

➞ DNS corporativo normalmente vai para **resolvedores conhecidos**, não para IPs isolados.

Caso Simulado 1: Exfiltração via DNS Túnel

TLP:CLEAR

SOC investigando com NetFlow

1

Alerta DNS Anômalo

2

SOC analisa

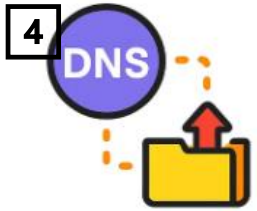
Quais IPs geraram os fluxos.
Quais servidores de DNS foram acionados.
Quando o comportamento iniciou.

3

Correlação

Logs de endpoint.
Identificação do usuário daquela estação.

4



Confirma exfiltração por DNS

5

Contenção rápida e precisa

Bloqueia comunicação
Bloqueia estação do usuário

Caso Simulado 2: Ransomware

TLP:CLEAR

🔷 1. Beaconing pré-encriptação

📊 ElastiFlow – Flow Table (Outbound TCP 443)

@timestamp	src.ip	dst.ip	dst.port	flow.duration	packets	bytes	bits_per_sec
10:00:00	10.80.10.55	185.199.110.153	443	2s	12	2.4 KB	9.6 Kbps
10:01:00	10.80.10.55	185.199.110.153	443	2s	11	2.2 KB	8.8 Kbps
10:02:00	10.80.10.55	185.199.110.153	443	2s	12	2.5 KB	10.0 Kbps
10:03:00	10.80.10.55	185.199.110.153	443	2s	11	2.3 KB	9.2 Kbps

📌 O que o ElastiFlow mostra claramente

- Mesmo src.ip → mesmo dst.ip
- Intervalo fixo de 60 segundos
- Volume quase idêntico
- Porta comum (443) → criptografado, sem payload

Caso Simulado 2: Ransomware

TLP:CLEAR

🔷 2. Comunicação externa suspeita (C2)

📊 ElastiFlow – *Top Destinations by Duration*

dst.ip	dst.as.name	flow.duration.	total bytes.total
45.155.205.18	Unknown ASN	3m 30s	68 KB

📊 ElastiFlow – *Flow Table*

@timestamp	src.ip	dst.ip	flow.duration	packets	bytes
10:15:10	10.80.10.55	45.155.205.18	210s	420	68 KB

➞ Sessão **longa**, **baixo volume**, **destino raro**.

Caso Simulado 2: Ransomware

TLP:CLEAR

🔷 3. Pós-C2: Movimento lateral

📊 ElastiFlow – *Top Internal Destinations*

src.ip	dst.ip	dst.port	packets	flow.duration
10.80.10.55	10.80.20.78	445	3	200 ms
10.80.10.55	10.80.20.77	445	3	200 ms
10.80.10.55	10.80.20.79	445	3	200 ms

➞ Tentativas SMB rápidas e sequenciais.

“Ransomware se anuncia na rede antes de causar impacto.”

Boas Práticas de Implementação

TLP:CLEAR

Integrar o NetFlow com ecossistema SOC

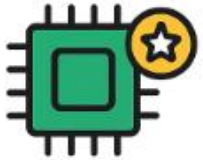
SIEM (correlação de alertas/logs)

NDR (detecção comportamental)

SOAR (resposta automatizada)

Planejamento de Coleta

+ pontos de coleta = + visibilidade



Enriquecimento de NetFlow

NetFlow v9/IPFIX ativo

Recomendação:

NetFlow v9 IPFIX

sempre que possśvel

Boas Práticas de Implementação

TLP:CLEAR

1 Onde o consumo realmente acontece

Pontos de consumo

- **Exportadores** (roteadores, firewalls, switches)
- **Coletores** (ElastiFlow)
- **Armazenamento** (Elasticsearch/OpenSearch)

Regra básica

Exportador mal configurado derruba o equipamento.
Coletor mal dimensionado derruba a análise.

2 No EXPORTADOR (rede)

🔷 Amostragem (Sampling)

Não use 1:1 em tudo

Recomendações:

- Core / Internet: **1:1000 ou 1:2000**
- Datacenter interno: **1:200 a 1:500**
- Links críticos de segurança: **1:1 ou 1:10**

✓ Reduz CPU e memória
✓ Mantém padrões comportamentais

🔷 Escopo de coleta

Colete **onde gera valor**

- borda (WAN/Internet)
- DC (leste-oeste crítico)

Evite coletar tudo em access layer

✓ Menos flows
✓ Menos ruído
✓ Menos custo

🔷 Templates e timers

Active timeout: 60–300s
Inactive timeout: 15–30s

✓ Evita explosão de flows longos
✓ Reduz carga no coletor

Boas Práticas de Implementação

TLP:CLEAR

3 No COLETOR (ElastiFlow)

🔷 Dimensionamento de ingestão

Planejar em **flows por segundo (fps)**, não em Mbps

Referência prática:

- 1.000 fps ≈ ~1–1,5 vCPU
- 5.000 fps ≈ ~6–8 vCPU
- 10.000 fps ≈ cluster obrigatório

✓ Dimensione com margem (30–40%)

🔷 Normalização e enriquecimento

Ative somente o necessário:

- GeoIP ✓
- ASN ✓
- DNS enrichment ✕ (alto custo)

Evite campos que não usa em dashboard

✓ Menos CPU
✓ Menos índice
✓ Queries mais rápidas

4 No ARMAZENAMENTO

🔷 Retenção por camadas (Tiering)

Hot (0–7 dias) - SOC, investigação ativa

Warm (7–30 dias) - Análise de tendência

Cold (30– > 90 dias) - Forense e compliance

Delete após prazo legal

✓ Controle de custo
✓ Performance previsível

Boas Práticas de Implementação

TLP:CLEAR

5 Estratégia de otimização

Camada	Boa prática-chave
Exportador	Amostragem correta
Coletor	Dimensionar por fps
Enriquecimento	Somente o essencial
Armazenamento	Retenção em camadas
Operação	Monitorar ingestão diariamente

6 Erros comuns (⚠ alerta)

- Coletar tudo “porque dá”
- Usar 1:1 em todos os links
- Reter NetFlow indefinidamente
- Enriquecer tudo sem necessidade
- Ignorar crescimento orgânico

✓ Resultado típico: cluster caro, lento e subutilizado.

NetFlow bem implementado é visibilidade barata.
Mal implementado vira custo e dor operacional.

Desafios

TLP:CLEAR

Volume de dados e impacto na infraestrutura

NetFlow → Volume Elevado

Impacta banco do coletor

Degrada queries no SOC

✅ **Boas Práticas**

Planejamento com folga

Retenção quente/morno/frio

Overhead de CPU e memória nos exportadores

NetFlow Export → Riscos em Roteadores/Switches

Sobrecarga de CPU

Atenção a hardware antigo

Teste antes de implantar

✅ **Boas práticas:**

Testes controlados em laboratório antes do rollout.

Custos Ocultos de NetFlow

Licenciamento

(Stealthwatch, Flowmon, Plixer)

Storage adicional

✅ **Boas Práticas**

Incluir o ecossistema do NetFlow no planejamento estratégico e orçamento

Conclusão

TLP:CLEAR

 **Confiar apenas na borda = risco**
A segurança moderna exige visibilidade interna.

 **Observabilidade interna é essencial**
Requisito básico para proteção em instituições financeiras.

 **"Dominar o fluxo é dominar a detecção moderna"**
NetFlow transforma o invisível em visível.

 **"NetFlow lê comportamento, não conteúdo"**
Isso permite revelar ações maliciosas ocultas.

“NetFlow = visibilidade estratégica”
Infraestrutura e segurança caminham juntas


PERGUNTAS?
NETFLOW

TLP:CLEAR

Obrigado!