



RNEP-GW

MÓDULO NETFLOW & DDOS



O QUE É O NETFLOW?

É um protocolo concebido para coletar informação de tráfego de redes IP

Implementado inicialmente pela Cisco no IOS 11.x em 1996

Atualmente suportado em quase todos os equipamentos Layer 3 (routers) no mercado



QUAIS OS BENEFÍCIOS NA SUA UTILIZAÇÃO?

Monitorizar o volume de tráfego na rede, assim como comunicações mais específicas

Ideal para redes com dimensões consideráveis

Informação pode ser relevante na despistagem de problemas de rede ou de segurança



COMO FUNCIONA?

Os equipamentos são configurados para exportar a informação coletada -- os "*flows*"

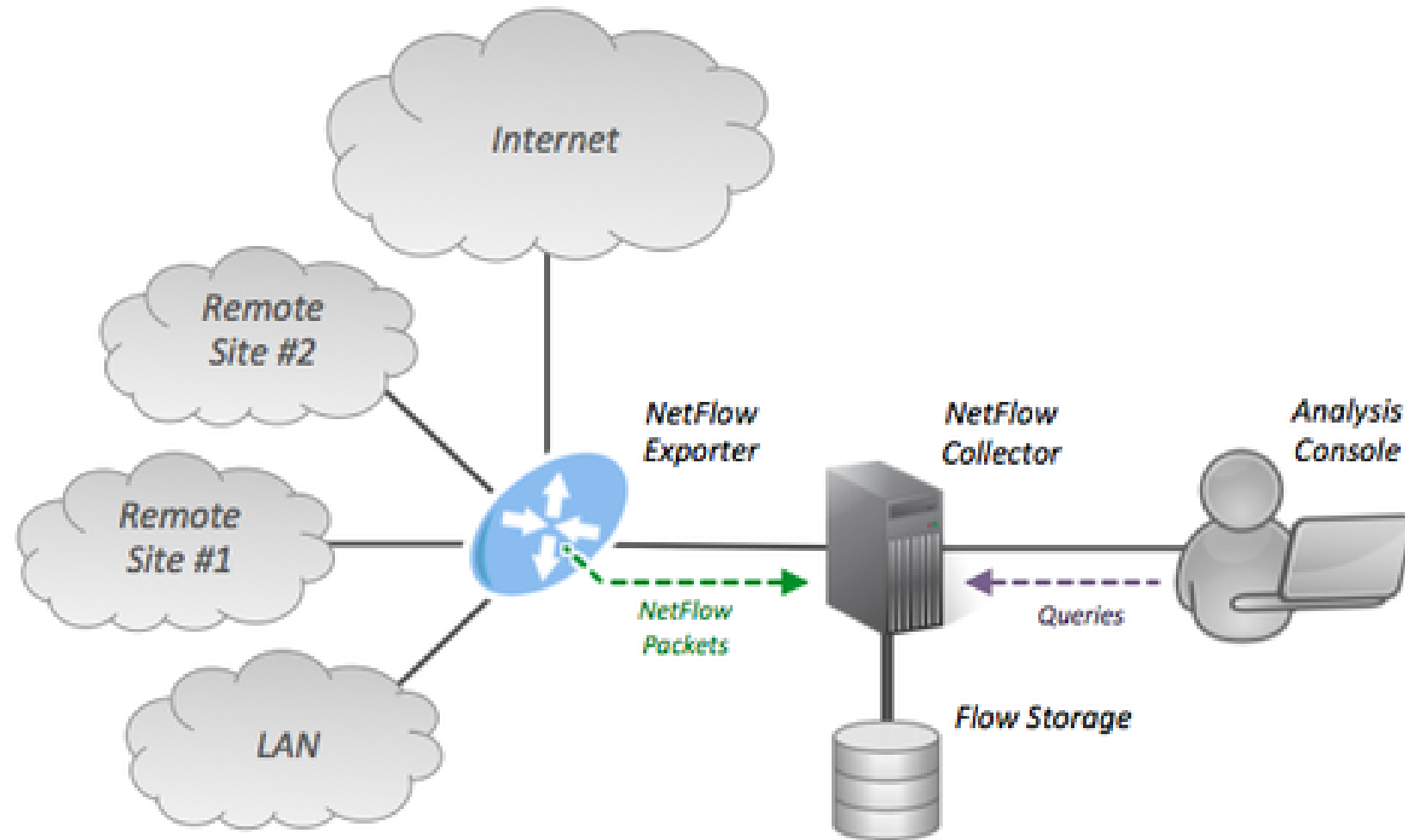
O equipamento que recebe esta informação necessita de ferramentas para extrair o conteúdo dos "*flows*"

O envio dos flows está sujeita a *sampling*

- amostragens por intervalo de tempo ou por quantidade de flows
- limitando a quantidade de informação para analisar



COMO FUNCIONA?



FERRAMENTAS PARA ANÁLISE DE FLOWS (ALGUNS EXEMPLOS)

NfSen

Nfdump

Splunk

SolarWinds Netflow Analyzer

Paessler PRTG

ManageEngine

nProbe

NfSen



splunk>

Pesquisar flows

Processar/Pesquisar flows por período

Criar os próprios scripts para processar flows



NetFlow analyzer
by NFSen

nfsen.sourceforge.net

NFSEN - CARACTERÍSTICAS

Ferramenta open source

Apresentação de Dashboards

Disponibiliza os dados dos *flows*
através de *queries*



NFSEN - CARACTERÍSTICAS

Navegação e utilização acessível em ambiente web

Criação de perfis de tráfego com determinadas características

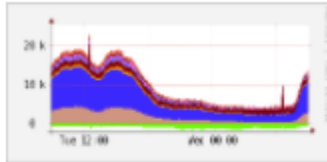
Criação de alertas para determinados padrões de tráfego



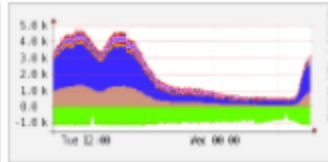
DADOS DOS FLOWS

Profile: live

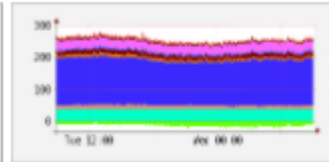
TCP



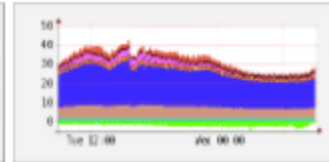
UDP



ICMP

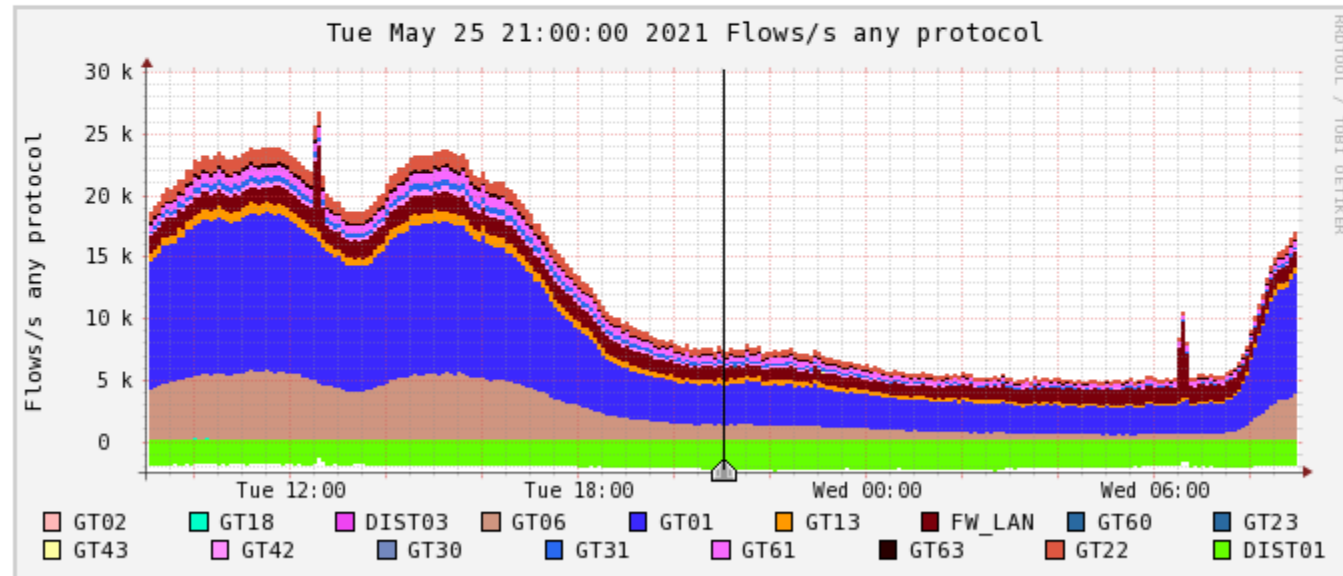


other



Profileinfo:

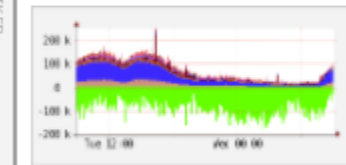
Type: live
Max: 5.0 TB
Exp: 300 days 0 hours
Start: Sep 20 2020 - 03:55 WET
End: May 26 2021 - 09:00 WET



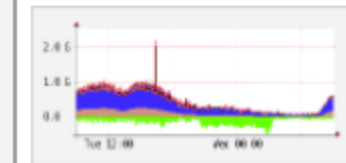
t_start 2021-05-25-21-00

t_end 2021-05-25-21-00

Packets



Traffic



Select Single Timeslot

Display: 1 day

☒ Lin Scale ☒ Stacked Graph
☐ Log Scale ☐ Line Graph

DADOS DOS FLOWS

Statistics timeslot May 25 2021 - 21:05

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
✓ GT22	437.0 /s	367.3 /s	60.9 /s	6.2 /s	2.7 /s	3.1 k/s	2.2 k/s	763.0 /s	6.7 /s	43.2 /s	20.8 Mb/s	16.1 Mb/s	4.4 Mb/s	4.9 kb/s	263.2 kb/s
✓ GT63	143.1 /s	118.4 /s	20.8 /s	2.8 /s	1.1 /s	1.1 k/s	1.0 k/s	121.0 /s	3.1 /s	2.2 /s	7.5 Mb/s	6.9 Mb/s	591.7 kb/s	1.9 kb/s	4.7 kb/s
✓ GT61	375.7 /s	256.6 /s	90.2 /s	27.5 /s	1.4 /s	2.4 k/s	1.5 k/s	729.0 /s	33.4 /s	167.9 /s	14.2 Mb/s	7.4 Mb/s	5.0 Mb/s	22.3 kb/s	1.8 Mb/s
✓ GT31	200.0 /s	152.5 /s	43.7 /s	3.7 /s	0.1 /s	1.8 k/s	1.2 k/s	652.2 /s	3.9 /s	2.0 /s	13.3 Mb/s	9.4 Mb/s	4.0 Mb/s	2.6 kb/s	14.6 kb/s
✓ GT30	0.0 /s	0 /s	0 /s	0 /s	0.0 /s	0.0 /s	0 /s	0 /s	0 /s	0.0 /s	4.8 b/s	0 b/s	0 b/s	0 b/s	4.8 b/s
✓ GT42	154.0 /s	106.9 /s	45.9 /s	0.9 /s	0.4 /s	463.9 /s	310.6 /s	149.3 /s	1.0 /s	3.0 /s	3.3 Mb/s	2.2 Mb/s	1.1 Mb/s	611.9 b/s	20.3 kb/s
✓ GT43	0.5 /s	0.1 /s	0.4 /s	0.0 /s	0.0 /s	0.6 /s	0.1 /s	0.5 /s	0.0 /s	0.0 /s	2.8 kb/s	289.5 b/s	2.5 kb/s	3.9 b/s	19.6 b/s
✓ GT23	1.3 /s	0.3 /s	0.8 /s	0.2 /s	0.0 /s	2.2 /s	0.3 /s	1.7 /s	0.2 /s	0.0 /s	14.8 kb/s	1.5 kb/s	13.2 kb/s	152.2 b/s	10.5 b/s
✓ GT60	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 b/s	0 b/s	0 b/s	0 b/s	0 b/s
✓ FW_LAN	1.0 k/s	998.7 /s	33.0 /s	14.4 /s	0.5 /s	2.6 k/s	1.5 k/s	1.1 k/s	14.0 /s	0.2 /s	13.9 Mb/s	2.2 Mb/s	11.7 Mb/s	10.9 kb/s	210.8 b/s
✓ GT13	396.7 /s	330.6 /s	58.7 /s	6.2 /s	1.3 /s	3.3 k/s	2.9 k/s	324.6 /s	7.0 /s	14.8 /s	11.1 Mb/s	9.8 Mb/s	1.2 Mb/s	5.1 kb/s	46.1 kb/s
✓ GT01	3.2 k/s	2.6 k/s	472.0 /s	134.8 /s	19.3 /s	20.2 k/s	14.7 k/s	5.1 k/s	147.6 /s	291.9 /s	131.2 Mb/s	94.5 Mb/s	34.2 Mb/s	290.4 kb/s	2.2 Mb/s
✓ GT06	1.2 k/s	971.4 /s	239.9 /s	12.2 /s	6.7 /s	7.9 k/s	5.6 k/s	2.2 k/s	13.4 /s	106.4 /s	58.7 Mb/s	42.2 Mb/s	16.2 Mb/s	17.6 kb/s	216.1 kb/s
✓ DIST03	0.2 /s	0.2 /s	0.0 /s	0 /s	0 /s	0.4 /s	0.4 /s	0.0 /s	0 /s	0 /s	138.1 b/s	122.3 b/s	15.7 b/s	0 b/s	0 b/s
✓ GT18	76.2 /s	33.7 /s	4.9 /s	36.5 /s	1.0 /s	190.5 /s	79.0 /s	65.6 /s	37.7 /s	8.2 /s	313.3 kb/s	63.3 kb/s	209.4 kb/s	26.2 kb/s	14.4 kb/s
✓ GT02	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 /s	0 b/s	0 b/s	0 b/s	0 b/s	0 b/s
✓ DIST01	2.3 k/s	1.4 k/s	977.7 /s	16.0 /s	2.7 /s	105.0 k/s	98.8 k/s	5.9 k/s	274.5 /s	45.7 /s	333.4 Mb/s	303.4 Mb/s	29.7 Mb/s	204.0 kb/s	46.2 kb/s

All

None

Display: ☐ Sum ☒ Rate

QUERIES – DADOS ESTATÍSTICOS

Netflow Processing

Source: **Filter:**

GT22
GT63
GT61
GT31
GT30
GT42
All Sources

ip 1.1.1.1

and <none>

Options:

☐ List Flows ☒ Stat TopN

Top: 10

Stat: Any IP Address order by flows

Limit: ☐ Packets > 0 -

Output: ☐ / IPv6 long

Clear Form process

```
** nfdump -M /data/nfsen/profiles-data/live/GT22:GT63:GT61:GT31:GT30:GT42:GT43:GT23:GT60:FW_LAN:GT13:GT01:GT06:DIST03:GT18:GT02:DIS
```

```
nfdump filter:
```

```
ip 1.1.1.1
```

```
Top 10 IP Addr ordered by flows:
```

Date first seen	Duration	Proto	IP Addr	Flows(%)	Packets(%)	Bytes(%)	pps	bps	bpp
2021-05-25 20:34:14.634	2129.885	any	1.1.1.1	1404(100.0)	1588(100.0)	162764(100.0)	0	611	102
2021-05-25 21:04:39.186	304.319	any	193.136.203.164	254(18.1)	257(16.2)	22049(13.5)	0	579	85
2021-05-25 21:04:40.877	303.642	any	194.210.4.91	123(8.8)	125(7.9)	6837(4.2)	0	180	54
2021-05-25 21:04:44.176	298.780	any	194.210.216.100	104(7.4)	104(6.5)	10617(6.5)	0	284	102
2021-05-25 21:04:37.126	297.645	any	194.210.151.8	79(5.6)	79(5.0)	6676(4.1)	0	179	84
2021-05-25 21:04:36.571	307.029	any	193.136.97.243	76(5.4)	77(4.8)	6369(3.9)	0	165	82
2021-05-25 21:01:17.304	443.406	any	193.137.3.67	57(4.1)	57(3.6)	17298(10.6)	0	312	303
2021-05-25 21:04:37.020	299.347	any	193.137.75.159	53(3.8)	53(3.3)	6960(4.3)	0	186	131
2021-05-25 21:04:43.410	300.053	any	194.210.151.4	45(3.2)	45(2.8)	4192(2.6)	0	111	93
2021-05-25 21:04:53.487	233.987	any	193.137.94.161	34(2.4)	34(2.1)	3277(2.0)	0	112	96

```
Summary: total flows: 1404, total bytes: 162764, total packets: 1588, avg bps: 611, avg pps: 0, avg bpp: 102
```

```
Time window: 2021-05-24 04:56:10 - 2021-05-25 21:10:02
```

```
Total flows processed: 2886458, Blocks skipped: 0, Bytes read: 198845724
```

```
Sys: 0.799s flows/second: 3608627.3 Wall: 1.695s flows/second: 1702203.0
```

QUERIES – COMUNICAÇÕES ESPECÍFICAS

Netflow Processing

Source: **Filter:** **Options:**

Source: GT22, GT63, GT61, GT31, GT30, GT42, All Sources

Filter: ip 1.1.1.1

Options: ☒ List Flows ☐ Stat TopN

Limit to: 20 Flows

Aggregate: ☐ bi-directional, ☐ proto, ☐ srcPort, ☐ dstPort

Sort: ☐ start time of flows

Output: auto ☐ /IPv6 long

Clear Form process

```
** nfdump -M /data/nfsen/profiles-data/live/GT22:GT63:GT61:GT31:GT30:GT42:GT43:GT23:GT60:FW_LAN:GT13:GT01:GT06:DIST03:GT18:GT02:DIST01 -T -r 2021/05/25/nfcapd.202105252105 -c 20
nfdump filter:
ip 1.1.1.1
Date first seen      Event XEvent Proto      Src IP Addr:Port      Dst IP Addr:Port      X-Src IP Addr:Port      X-Dst IP Addr:Port      In Byte Out Byte
2021-05-25 21:04:43.024 IGNORE Ignore UDP        1.1.1.1:53 -> 194.210.211.64:57131 0.0.0.0:0 -> 0.0.0.0:0 159 0
2021-05-25 21:04:43.508 IGNORE Ignore TCP        1.1.1.1:443 -> 193.136.53.11:60272 0.0.0.0:0 -> 0.0.0.0:0 40 0
2021-05-25 21:04:44.392 IGNORE Ignore TCP        1.1.1.1:443 -> 193.136.53.11:60277 0.0.0.0:0 -> 0.0.0.0:0 619 0
2021-05-25 21:04:44.628 IGNORE Ignore TCP        1.1.1.1:443 -> 193.136.53.11:60282 0.0.0.0:0 -> 0.0.0.0:0 91 0
2021-05-25 21:04:44.784 IGNORE Ignore TCP        193.136.53.11:60287 -> 1.1.1.1:443 0.0.0.0:0 -> 0.0.0.0:0 40 0
2021-05-25 21:04:55.908 IGNORE Ignore UDP        193.136.37.14:33452 -> 1.1.1.1:53 0.0.0.0:0 -> 0.0.0.0:0 72 0
2021-05-25 21:04:57.964 IGNORE Ignore TCP        193.137.38.253:52789 -> 1.1.1.1:443 0.0.0.0:0 -> 0.0.0.0:0 133 0
2021-05-25 21:05:01.088 IGNORE Ignore UDP        193.137.65.126:46568 -> 1.1.1.1:53 0.0.0.0:0 -> 0.0.0.0:0 68 0
2021-05-25 21:05:05.724 IGNORE Ignore UDP        1.1.1.1:53 -> 193.137.32.165:49043 0.0.0.0:0 -> 0.0.0.0:0 119 0
2021-05-25 21:05:19.920 IGNORE Ignore UDP        193.137.65.126:50765 -> 1.1.1.1:53 0.0.0.0:0 -> 0.0.0.0:0 68 0
2021-05-25 21:05:25.336 IGNORE Ignore UDP        1.1.1.1:53 -> 193.137.65.104:62749 0.0.0.0:0 -> 0.0.0.0:0 148 0
2021-05-25 21:05:25.976 IGNORE Ignore UDP        1.1.1.1:53 -> 193.136.33.223:35455 0.0.0.0:0 -> 0.0.0.0:0 80 0
2021-05-25 21:05:19.952 IGNORE Ignore UDP        193.137.55.26:60680 -> 1.1.1.1:53 0.0.0.0:0 -> 0.0.0.0:0 72 0
2021-05-25 21:05:41.588 IGNORE Ignore UDP        1.1.1.1:53 -> 194.210.237.151:56351 0.0.0.0:0 -> 0.0.0.0:0 112 0
2021-05-25 21:05:45.648 IGNORE Ignore UDP        193.136.60.35:49876 -> 1.1.1.1:53 0.0.0.0:0 -> 0.0.0.0:0 73 0
2021-05-25 21:05:49.312 IGNORE Ignore UDP        193.137.65.126:42333 -> 1.1.1.1:53 0.0.0.0:0 -> 0.0.0.0:0 68 0
2021-05-25 21:05:51.676 IGNORE Ignore UDP        193.137.28.243:54138 -> 1.1.1.1:53 0.0.0.0:0 -> 0.0.0.0:0 61 0
2021-05-25 21:05:56.888 IGNORE Ignore UDP        193.137.65.126:52693 -> 1.1.1.1:53 0.0.0.0:0 -> 0.0.0.0:0 68 0
2021-05-25 21:05:57.364 IGNORE Ignore UDP        193.137.65.126:43009 -> 1.1.1.1:53 0.0.0.0:0 -> 0.0.0.0:0 68 0
2021-05-25 21:06:06.680 IGNORE Ignore UDP        193.137.65.126:34662 -> 1.1.1.1:53 0.0.0.0:0 -> 0.0.0.0:0 68 0
Summary: total flows: 20, total bytes: 2227, total packets: 20, avg bps: 212, avg pps: 0, avg bpp: 111
Time window: 2021-05-25 20:34:58 - 2021-05-25 21:09:59
Total flows processed: 34947, Blocks skipped: 0, Bytes read: 2097132
Sys: 0.048s flows/second: 713335.1 Wall: 0.049s flows/second: 708088.5
```

QUERIES - EXEMPLOS

“IP x.x.x.x” – Comunicações com o IP x.x.x.x

“IP x.x.x.x and IP y.y.y.y” – Comunicações entre o IP x.x.x.x e o IP y.y.y.y

“Flags S and flags A” – Pacotes TCP com a flag SYN e ACK



QUERIES - EXEMPLOS

“Proto icmp” – todas as comunicações com o protocolo icmp

“IP x.x.x.x and port 443” – Comunicações com o IP x.x.x.x e que envolva o porto 443, seja na origem ou destino



“Src ip x.x.x.x and dst port 22” – Comunicações com IP de origem x.x.x.x e porto de destino 22



IDEIAS CHAVE



A análise de flows é indispensável para termos visibilidade sobre o tráfego



Devido ao volume de dados, é frequente recorrer-se a *sampling*



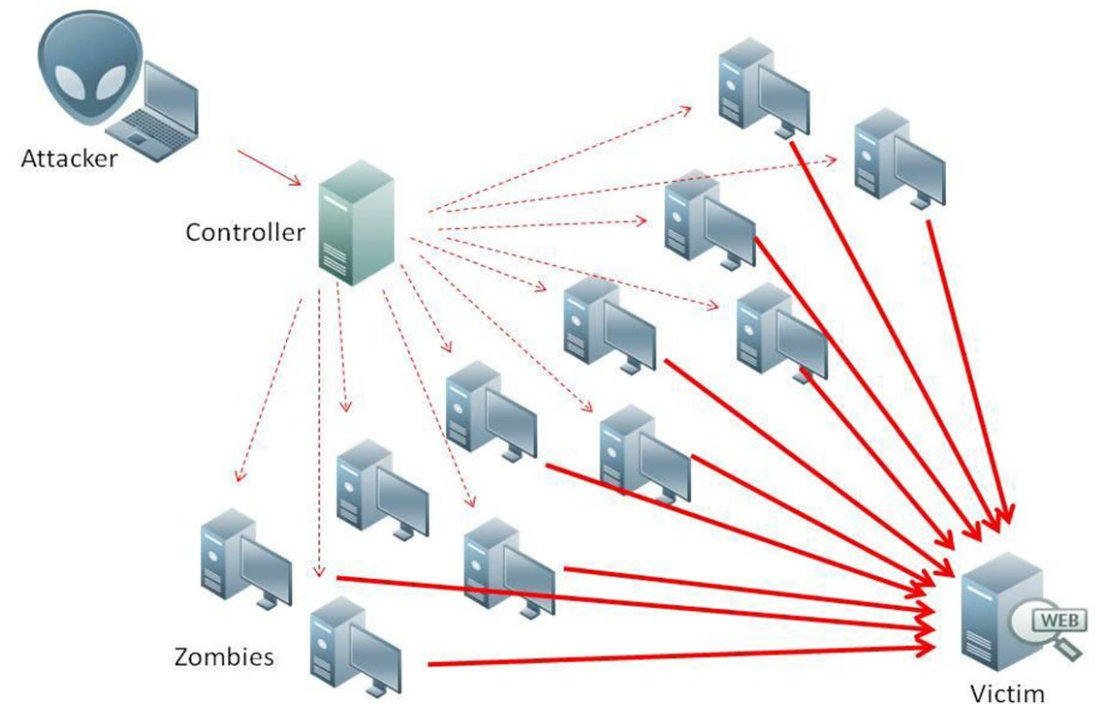
Obter dados relevantes é tipicamente um processo moroso

O QUE É UM DDOS?

É um ataque de negação de serviço com origem distribuída

Por a origem ser distribuída torna-se mais difícil de mitigar

Mas existem técnicas que tornam possível o combate a este fenómeno



ATAQUES MAIS COMUNS

Ataques de Amplificação/Reflexão

Tipicamente usam o protocolo UDP

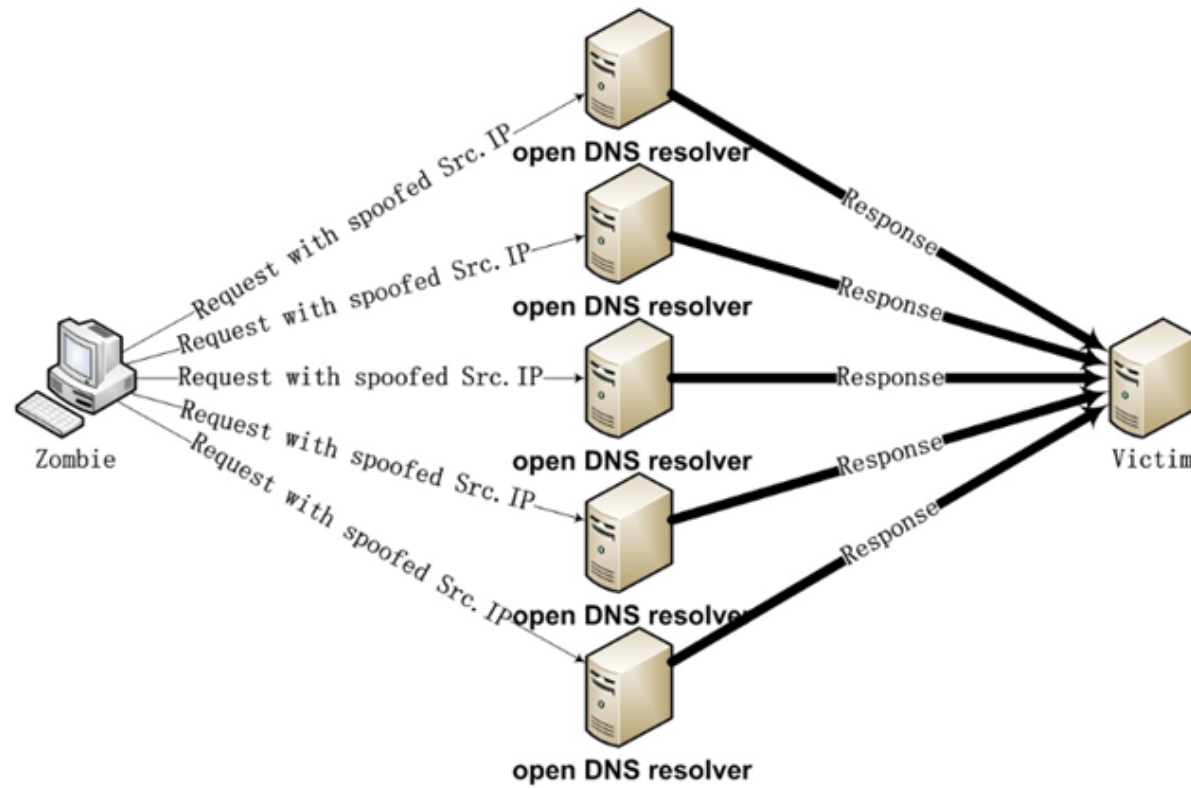
O tráfego é amplificado e refletido para a vítima

Serviços vulneráveis ou mal configurados
ex: dns, chargen, ntp, snmp, ssdp, etc

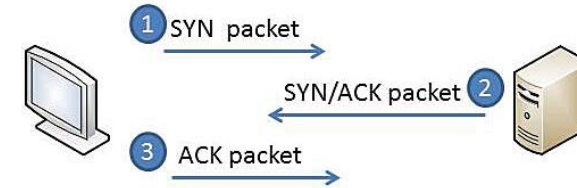


ATAQUES MAIS COMUNS

Ataques por reflexão - Exemplo



ATAQUES MAIS COMUNS



SYN Flood: Envio massivo de pacotes TCP com a *flag SYN*

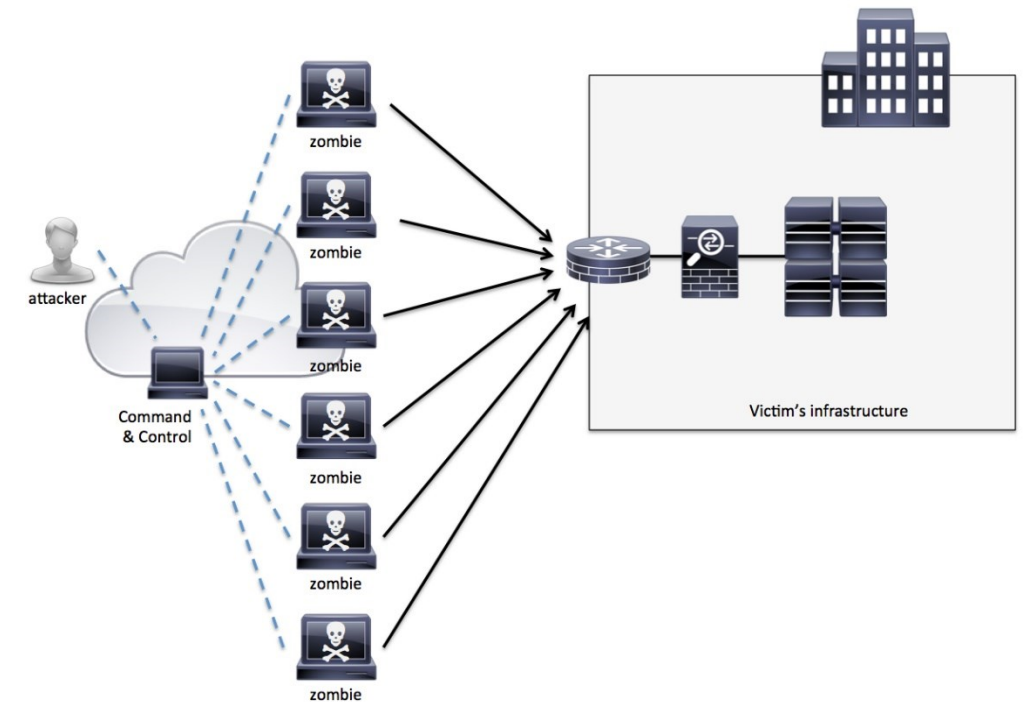
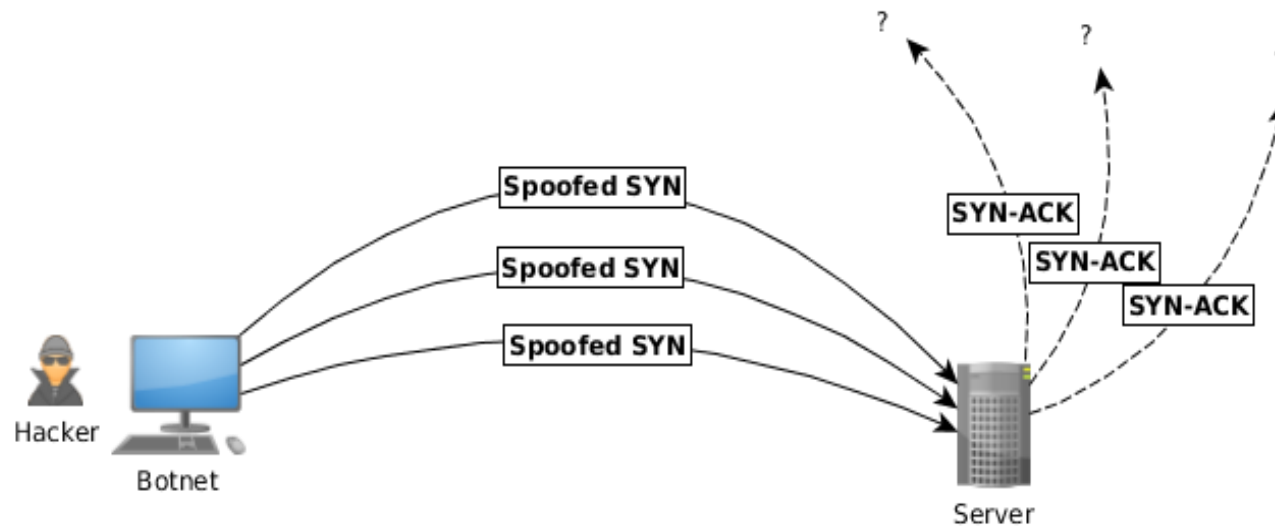
Usam o protocolo TCP

Os ataques podem ter origem em máquinas «*zombie*»,
infetadas com *malware*

Os ataques podem ter origem nas máquinas do atacante,
os pacotes são forjados para não denunciar os IPs de
origem «reais» e dificultar a mitigação do ataque

ATAQUES MAIS COMUNS

SYN Flood - Exemplos



ATAQUES MAIS COMUNS

Smurf Attack – Envio massivo de pacotes ICMP “Echo request”

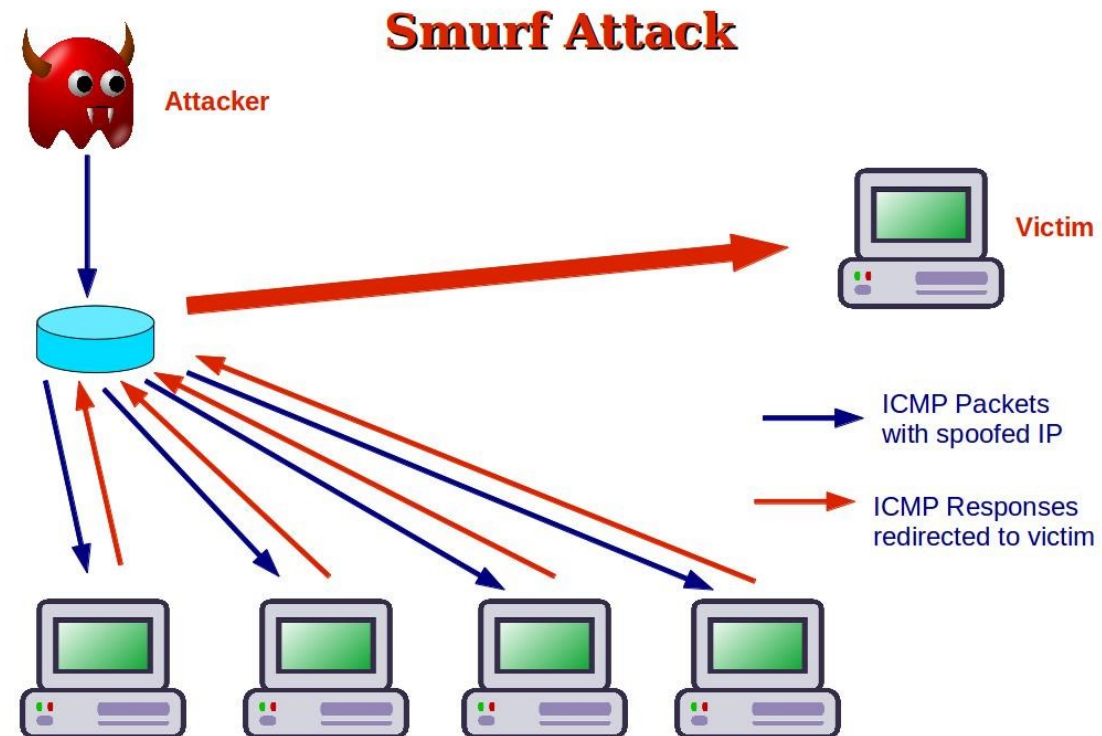
Usam protocolo ICMP

O atacante envia pacotes forjados com o IP de origem da vítima para endereços de *broadcast*



ATAQUES MAIS COMUNS

Smurf Attack - Exemplo



MEDIDAS DE CONTENÇÃO/MITIGAÇÃO

Objetivos

- Identificar o tipo de ataque
- Diferenciar o tráfego “bom” do tráfego “mau”
- Descartar o tráfego “mau” antes que chegue ao destino

STOP DOS

IDEIAS CHAVE



É importante combater os serviços vulneráveis a amplificação para reduzir o potencial dos DDoS



Dispositivos infectados são usados com frequência em ataques DDoS



Conseguir caracterizar um ataque é o primeiro passo para o conseguir mitigar



Questões?

Obrigado.



csirt.fct.pt/podcast



csirt.fct.pt/mooc



csirt.fct.pt/etc