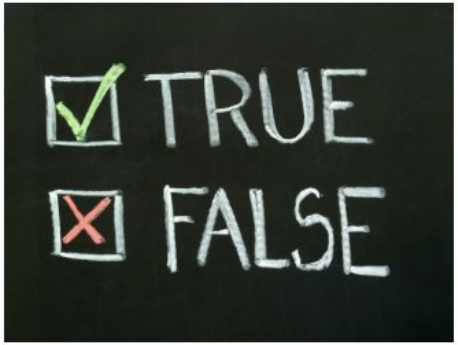

nic.br
Núcleo de Informação
e Coordenação do
Ponto BR
cgi.br
Comitê Gestor da
Internet no Brasil
registro.br cert.br cetic.br ceptro.br ceweb.br ix.br

Medidas básicas de segurança IPv6

ceptro.br nic.br cgi.br

Mitos sobre segurança IPv6

- Por ser um assunto relativamente inexplorado muitos mitos existem
- Mitos são baseados em informações incompletas ou mal interpretadas



“IPv6 é mais seguro que IPv4” ou “IPv4 é mais seguro que IPv6”

- Usados para se argumentar em favor de uma versão ou de outra do protocolo
- Podem acontecer cenários em que um protocolo possua uma falha que a outra versão não possui, mas estes cenários são geralmente bastante particulares

“IPv6 é mais seguro que IPv4” ou “IPv4 é mais seguro que IPv6”

- Na prática ambos possuem segurança e falhas similares
- IPv6 corrigiu alguns problemas conhecidos do IPv4
- IPv6 tem menos utilização e tempo de debug e pode possuir novas falhas que poderão ser exploradas

“Se o IPv6 não for implementado na minha rede, posso ignorá-lo”

- Seguir esta lenda, pode gerar sérios problemas para a sua rede. É necessário se preocupar com segurança IPv6 mesmo sem ter IPv6 nativo em sua rede
- Os sistemas operacionais atuais possuem suporte nativo a IPv6 e alguns possuem preferência pela utilização de IPv6

“Se o IPv6 não for implementado na minha rede, posso ignorá-lo”

- Usuários com pouco conhecimento técnico conseguem configurar túneis automáticos de IPv6 em IPv4, passando este tráfego por sua rede segura sem ser analisado
- IPv6 pode ser usado mesmo que não haja implementação oficial na sua rede
- Existem ataques que exploram o fato do IPv6 ser ignorado

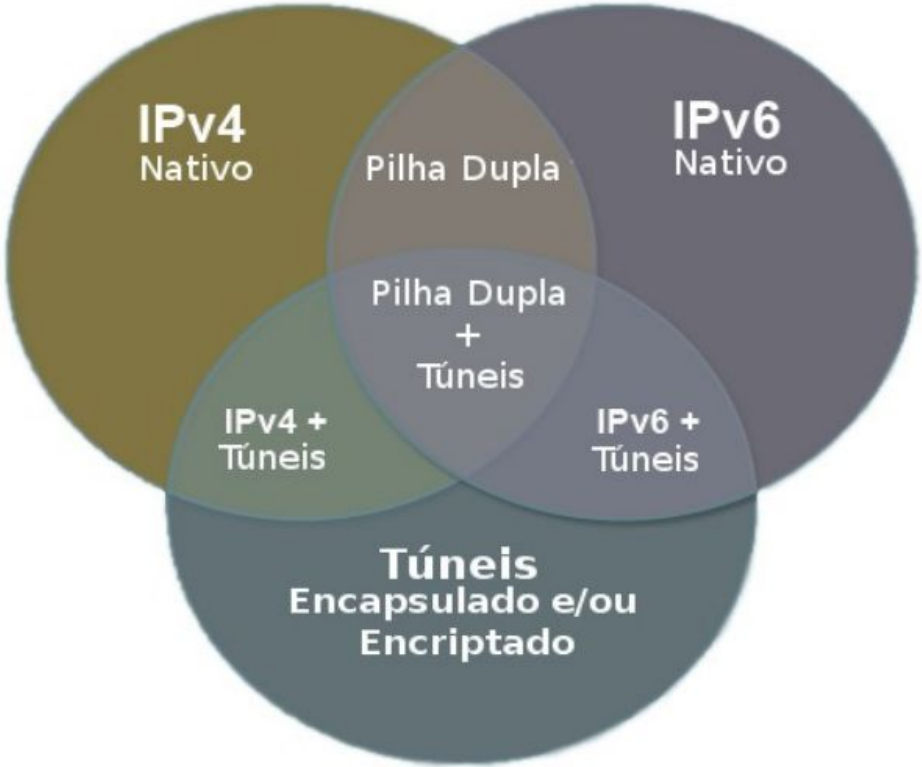
“Se o IPv6 não for implementado na minha rede, posso ignorá-lo”

- É possível trafegar pacotes IPv6 dentro de pacotes IPv4, com tunelamento
- Qualquer dispositivo com IPv6 ativado pode se comunicar na rede local através do endereço Link local, sem precisar de um roteador

“IPv6 garante comunicação fim a fim”

- A especificação do IPv6 prevê a comunicação fim a fim, assim como acontecia com a especificação do IPv4
- Entretanto mecanismos como firewalls e sistemas de detecção de intrusão controlam a comunicação fim a fim

Superfície de ataque

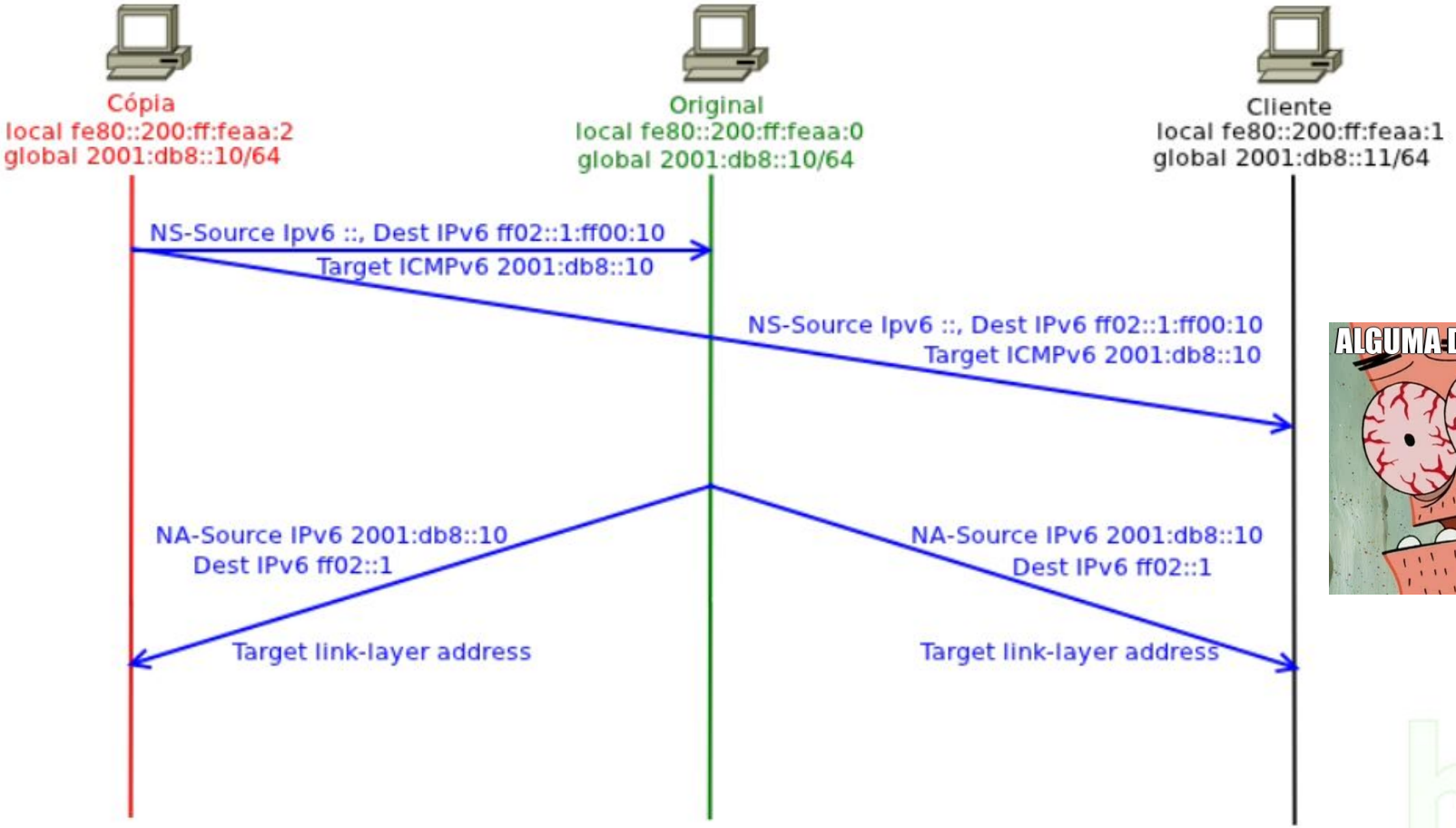


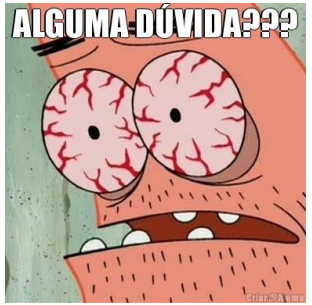
Neighbor Discovery Protocol (NDP)

- Protocolo utilizado para várias coisas na LAN
  - Entre elas Detecção de Endereço Duplicado (DAD)
- Pode ser utilizado para vários ataques
  - Entre eles para não deixar mais ninguém entrar na rede com um endereço IPv6
  - Espécie de Negação de Serviço (DoS)

Detecção de Endereço Duplicado (DAD)

- Antes de entrar na rede com um endereço IPv6
  - A máquina pergunta se alguém já está utilizando o endereço
  - Se alguém na rede estiver utilizando aquele endereço, ele responderá que está em uso
  - A máquina então ao receber este aviso não poderá usar aquele endereço IPv6


Cópia
local fe80::200:ff:feaa:2
global 2001:db8::10/64
Original
local fe80::200:ff:feaa:0
global 2001:db8::10/64
Cliente
local fe80::200:ff:feaa:1
global 2001:db8::11/64
NS-Source Ipv6 ::, Dest IPv6 ff02::1:ff00:10
Target ICMPv6 2001:db8::10
NS-Source Ipv6 ::, Dest IPv6 ff02::1:ff00:10
Target ICMPv6 2001:db8::10
NA-Source IPv6 2001:db8::10
Dest IPv6 ff02::1
Target link-layer address
NA-Source IPv6 2001:db8::10
Dest IPv6 ff02::1
Target link-layer address


ALGUMA DÚVIDA???

Detecção de Endereço Duplicado Ataque

- Se uma máquina na rede responder a todos os avisos de pergunta se o endereço já está em uso, ninguém mais poderá entrar na rede por falta de endereços IPv6 disponíveis

Laboratório

Experiência 3.1

Ataque DoS ao NDP

Página 177

Varredura de endereços (Scanning)

- Tornou-se mais complexo, mas não impossível!
- Com uma máscara padrão /64 e percorrendo 1 milhão de endereços por segundo, seria preciso mais de 500.000 anos para percorrer toda a sub-rede

Varredura de endereços (Scanning)

- Novas técnicas:
  - Explorar endereços de servidores públicos divulgados no DNS
  - Procura por endereços fáceis de memorizar utilizados por administradores de redes
    - ::10, ::20, ::DAD0, ::CAFE
    - Low-byte – incremental: ::1, ::2, ::3 etc
    - Endereço IPv4 ou parte dele

Combatendo a Varredura

- Pode-se utilizar formas mais seguras de gerações de endereços
  - Utilizar endereços CGA (RFC3972)
  - Utilizar endereços temporários (RFC4941)
  - Utilizar geração semi aleatória (RFC7217)

Firewall

- NAT não é segurança, uma forma de obscuridade!
- No IPv6 não tem NAT!
- Utilize endereços globais se quiser ter conectividade na Internet!
- Caso queira se bloquear conexões entrantes, coloque uma regra de firewall

Firewall

- ICMPv6 faz funções que no IPv4 eram realizadas pelo ARP, logo o ICMPv6 não pode ser completamente bloqueado no firewall de borda como ocorria no IPv4
- Se bloquear ele completamente, a rede não funciona!

Firewall

- Tudo que você já bloqueia em IPv4 e não quer funcionando na sua rede, precisa ser bloqueado em IPv6
- Lembre-se que existem técnicas de transição
  - Se você não utiliza, é bom bloquear
  - Diminui a superfície de ataque

Obrigado!!!

Equipe de cursos do CEPTRO.br

cursosceptro@nic.br

ipv6@nic.br

nic.br cgi.br

www.nic.br | www.cgi.br