

nic.br

Núcleo de Informação
e Coordenação do
Ponto BR

cgib.br

Comitê Gestor da
Internet no Brasil



registro.br cert.br cetic.br ceptro.br ceweb.br ix.br

nic.br cgi.br

ceptro.br

Segurança IPv6

ceptro.br nic.br egi.br

Licença de uso do material

Esta apresentação está disponível sob a licença

Creative Commons

Atribuição – Não a Obras Derivadas (by-nd)

<http://creativecommons.org/licenses/by-nd/3.0/br/legalcode>



Você pode:

- **Compartilhar** — copiar, distribuir e transmitir a obra.
- **Fazer uso comercial da obra.**
- Sob as seguintes condições:

Atribuição — Ao distribuir essa apresentação, você deve deixar claro que ela faz parte do Curso de Formação para Sistemas Autônomos do CEPTR0.br/NIC.br, e que os originais podem ser obtidos em <http://ceptro.br>. Você deve fazer isso sem sugerir que nós damos algum aval à sua instituição, empresa, site ou curso.

Vedada a criação de obras derivadas — Você não pode modificar essa apresentação, nem criar apresentações ou outras obras baseadas nela..

Se tiver dúvidas, ou quiser obter permissão para utilizar o material de outra forma, entre em contato pelo e-mail:
info@nic.br.

RFC 9099

Operational Security Considerations for IPv6 Networks

RFC 9099

- Endereçamento
- Cabeçalho de Extensão
- Segurança no Enlace
- Segurança no Control Plane
- Segurança no Roteamento
- Monitoramento e Logs
- Transição
- Segurança Corporativa
- Segurança no ISP
- Segurança no Cliente Doméstico

Endereçamento

- Importância de um bom plano de endereçamento
- Recomenda-se o uso de ferramentas IPAM (IP Address Management)
- Cada host pode ter múltiplos endereços IPv6
- Endereços ULAs (Unique Local Addresses) não devem ser usados para acesso a Internet
- Links ponto-a-ponto devem ser configurados utilizando /127
- Loopbacks podem ser alocados em um único /64 para facilitar o controle

Endereçamento

- Endereços estáveis: simples vs complexos
 - Há vantagens e desvantagens
- Alocações de IPv6 via SLAAC
 - A maioria dos sistemas não utiliza mais a geração de endereços via EUI-64, dando preferência para endereços temporários (RFC 8961 e RFC 7721)

DHCPv6

- Mesmo problema que o DHCPv4
 - Necessário prevenir contra servidores DHCP indesejáveis
 - Diferente do DHCPv4, o DHCPv6 identifica o cliente através do DUID (DHCP Unique Identifier), pois o DHCPv6 pode alocar múltiplos endereços para um mesmo cliente

DNS

- Mesmas considerações de segurança se aplicam tanto para IPv4 como para IPv6
 - Atenção especial caso se utilize DNS64 com DNSSEC

Cabeçalhos de extensão

- Problemas podem ocorrer caso os cabeçalhos venham em ordem errada ou haja repetição de cabeçalhos
 - Utilizado em alguns tipos de ataque
 - Recomendação que os roteadores aceitem apenas os cabeçalhos na ordem correta e sem repetição
 - Pode-se utilizar um firewall para reforçar essa proteção

Cabeçalhos de extensão

- Hop-by-hop header
 - Na especificação original do IPv6 (RFC 2460) era obrigatório que todos os nós da rede processassem este cabeçalho
 - Isso pode ser utilizado como forma de ataque de negação de serviço
 - Na nova especificação do IPv6 (RFC 8200) o processamento do hop-by-hop é opcional e configurável no roteador

Cabeçalhos de extensão

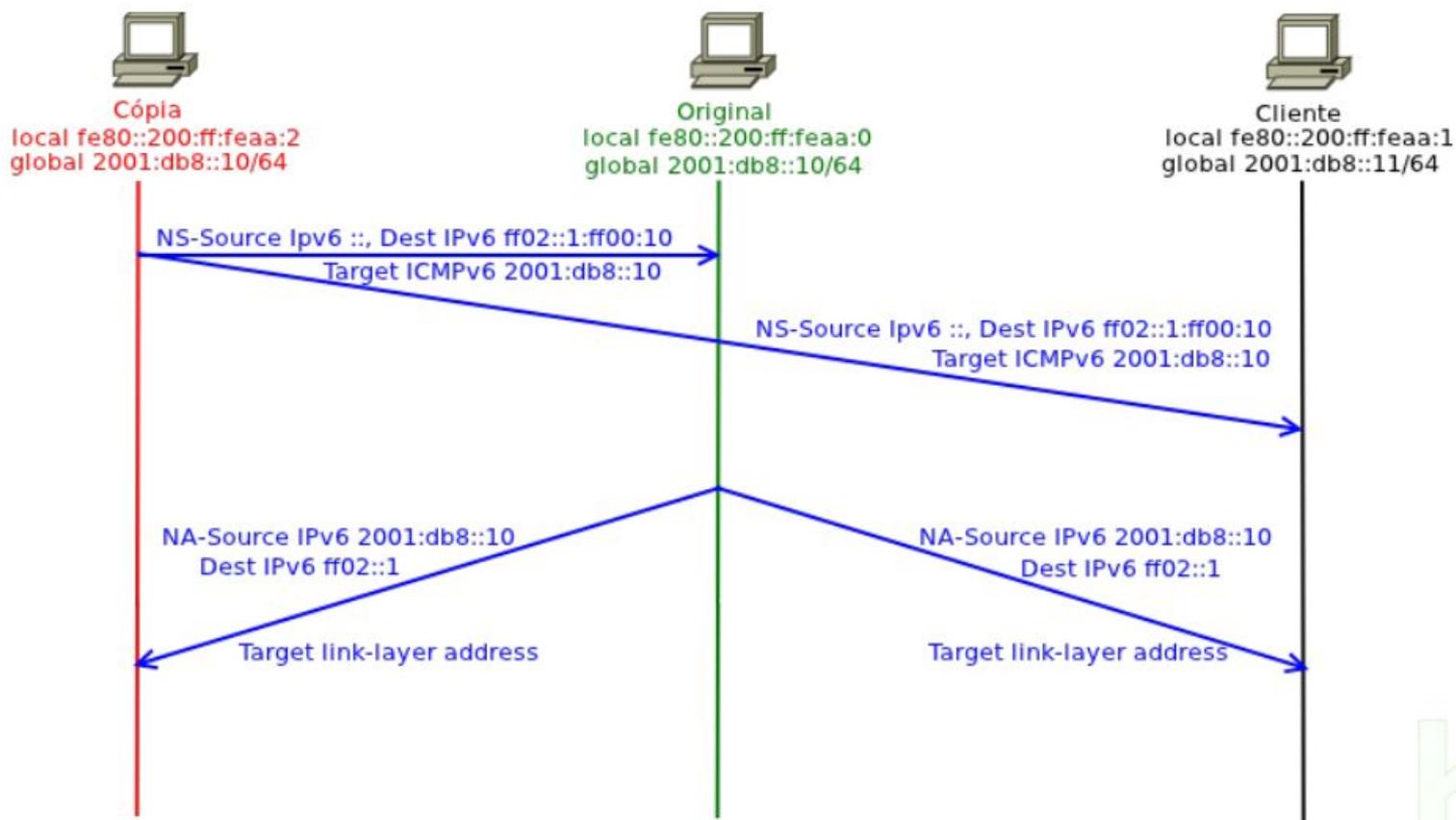
- Fragmentation Header
 - Possível ataque utilizando cabeçalhos de extensão em excesso
 - Recomendação que se filtre no firewall os primeiros pacotes de fragmentação que não contenham a cadeia completa de cabeçalhos (incluindo cabeçalho da camada de transporte)

IPsec

- Na especificação original do IPv6 (RFC 2460) o suporte a IPsec era obrigatório em qualquer aparelho que suportasse IPv6
- Na nova especificação do IPv6 (RFC 8200) o suporte a IPsec é opcional

Detecção de Endereço Duplicado (DAD)

- Possível ataque enviando respostas às requisições de DAD mesmo não possuindo o endereço requisitado



Detecção de Endereço Duplicado (DAD)

- O ataque consiste em enviar uma resposta de Neighbor Advertisement para todos os pacotes de Neighbor Solicitation recebidos
- Isto faz com que os endereços de tentativa nunca sejam validados, pois os dispositivos irão considerar que os IPs já estão em uso
- Sem IP válido, os novos dispositivos ficam impedidos de utilizar a rede

NDPmon

- Monitora todas as mensagens do protocolo NDP, guardando as informações recebidas
- Caso receba mensagens incoerentes, por exemplo, tentativa de negação de serviço ao DAD, gera logs e alarmes e pode enviar email ao administrador da rede
- Não é capaz de agir ativamente na rede para evitar os ataques

Laboratório

Experiência 3.1

Ataque DoS ao NDP

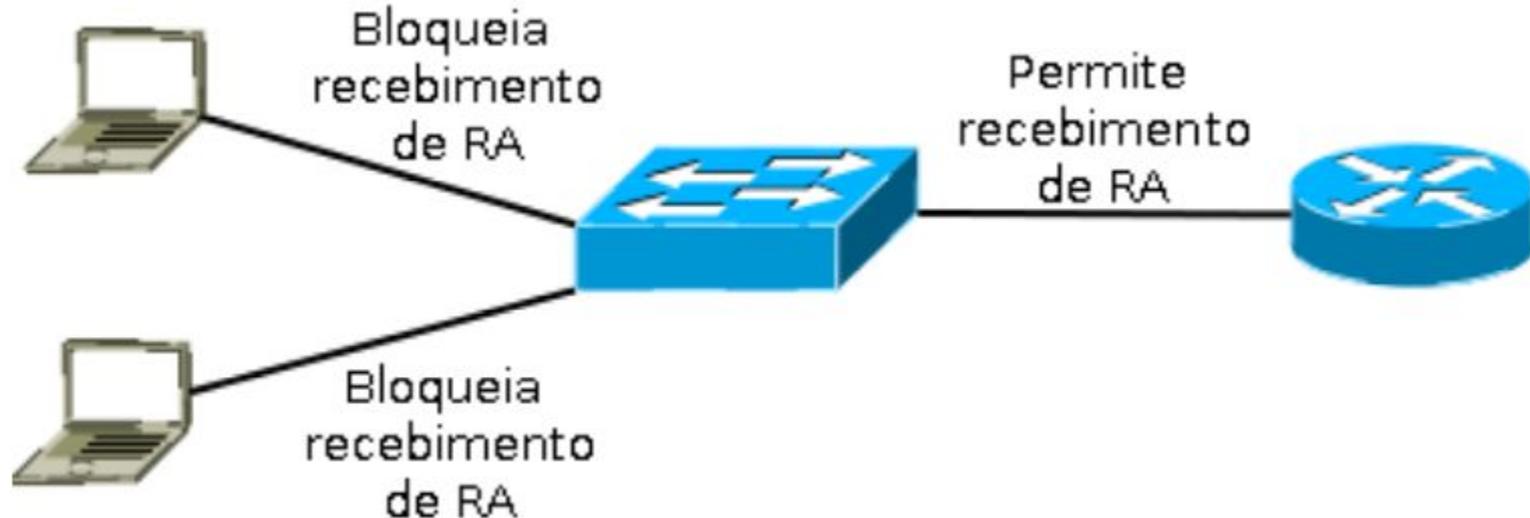
Página 177

Falsificação do Router Advertisement

- Dispositivo que não é um roteador envia mensagens de RA com as possíveis finalidades:
 - Tornar-se o roteador principal da rede, fazendo sniffing ou ataque de man-in-the-middle antes de encaminhar o pacote
 - Anunciar um roteador falso para criar um buraco negro, para onde o tráfego é direcionado, gerando negação de serviço

RA Guard

- Somente permite pacotes de Router Advertisement vindos de portas com roteadores conectados
- Pacotes de Router Advertisement vindos de outras portas são descartados pelo switch
- - Necessita que switch implemente esta função



Source Address Validation Improvements (SAVI)

- Técnica utilizada para evitar spoofing de pacotes
- Pode ser utilizada como forma de proteção adicional do NDP

DHCPv6-Shield

- RFC 7610
- Sistema equivalente ao DHCP snooping no IPv4
- Utilizado para proteger a rede contra servidores DHCP maliciosos

Multicast

- Endereço multicast all nodes (ff02::1) pode ser utilizado para ataques de spoofing (similar ao ataque de broadcast no IPv4)
- Pode-se limitar o uso desse multicast para evitar negação de serviço (mas não pode desabilitar!)

Secure Neighbor Discovery (SEND)

- RFC 3971
- Solução contra spoofing e negação de serviços que utilizam o NDP
- Existem poucas implementações no mercado para ser efetivo e prático

Segurança no Control Plane

- Deve-se utilizar ACLs ou firewalls para proteger os equipamentos da rede
- A maioria das regras de segurança é similar ao IPv4 (OSPF, BGP, SSH, etc.)
- Algumas exceções referente ao ICMPv6
 - Permitir a mensagem ICMPv6 Packet too big (mecanismo Path MTU Discovery)
 - Permitir ICMPv6 destination unreachable
 - Permitir mensagens de ICMPv6 do NDP dentro dos enlaces

Firewall

- Numa rede IPv4, onde normalmente se utiliza NAT, este funciona como um firewall stateful, permitindo apenas comunicações originadas de dentro da rede. Numa rede IPv6 não há NAT, então, se o administrador de rede decidir manter uma política de segurança similar a que utilizava com o IPv4, é necessário um cuidado redobrado na implantação de firewalls, a fim de forçar essa política.
- Com a adoção do protocolo IPv6 todos os hosts podem utilizar endereços válidos com conectividade direta a Internet e alcance a todos os hosts da rede interna que tenham IPv6 habilitado

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
- O firewall pode ser:
 - **Stateful:** solicitações da rede interna para a rede externa são gravadas para permitir o recebimento somente de solicitações feitas, mas necessita maior processamento e memória
 - **Stateless:** conjunto de regras fixas, pode permitir mensagens não solicitadas de tráfego permitido

Firewall

- Recomendações de Firewall baseadas na RFC 4890, detalhada em: NIST SP 800-119, Guidelines for the Secure Deployment of IPv6, December 2010

<http://csrc.nist.gov/publications/PubsSPs.html>

- Entretanto existem discussões de que essa RFC não foi pensada por administradores de redes corporativas, e que é permissiva demais para essa utilização

Técnicas de transição

- A RFC 4942 detalha a segurança com relação as técnicas de transição:
 - mesmo que sua rede não tenha IPv6, não o ignore
 - se você não deseja utilizar técnicas de tunelamento automático na sua rede, elas devem ser bloqueadas no firewall
 - técnicas de transição podem depender de servidores públicos não confiáveis

Técnica de Transição	Regra de filtragem
Túnel manual 6in4	IPv4.Protocol == 41
Túnel manual GRE	IPv4.Protocol == 47
Túneis automáticos 6to4	IPv4.Protocol == 41 IPv4.{src,dst} == 192.88.99.0/24
Túneis automáticos Teredo	IPv4.dst == servidores_teredo UDP.DstPort == 3544

Laboratório

Experiência 3.2

Firewall stateful

Página 185

Segurança no BGP e no OSPF

- As recomendações de segurança no BGP são as mesmas para IPv4 e IPv6
- No caso do OSPFv3, pode-se utilizar o IPsec como proteção adicional do protocolo

Filtros no BGP

- Fazer filtros de bogons (team cymru)
- Validar as rotas utilizando técnicas de validação automáticas
 - RPKI
 - IRR
- Autenticar a sessão BGP sempre que possível

Logs

- O IPv6 tem múltiplas formas de ser escrito. Exemplo
 - 2001:db8::1
 - 2001:DB8::1
 - 2001:0db8:0000:0000:0000:0000:0000:0001
 - 2001:0DB8:0000:0000:0000:0000:0000:0001
- Se possível adotar logs com uma única forma do IPv6
- Logs de DHCP não são tão confiáveis como no IPv4 por conta do SLAAC
- Os equipamentos podem ter múltiplos IPv6
- Lembrar que a comunicação pode envolver IPv4 e IPv6

Segurança no CPE

- Duas possíveis abordagens
 - Outbound-only: similar ao comportamento do NAT em IPv4, permite apenas respostas de requisições e bloqueia pacotes entrantes. Mais detalhes na RFC 6062
 - Transparente: permitir conexões entrantes a fim de manter o modelo fim a fim

IPSEC

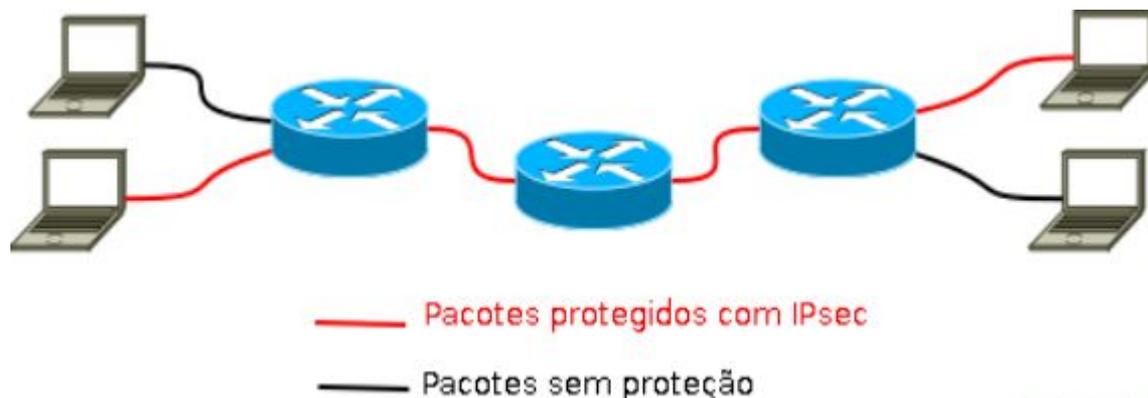
- Especificação IPv4 definiu que os dados enviados em um pacote IP não receberiam, nesta camada, qualquer tipo de ofuscamento ou criptografia
- Caso esta proteção fosse necessária, caberia à camada de aplicação esta responsabilidade
- A autenticidade do pacote também não foi prevista na concepção do protocolo IP, por exemplo, o endereço IP de origem contido no pacote pode ser alterado ou falsificado e o dispositivo destino não terá como validar sua autenticidade

IPSEC

- IPsec é uma suite de protocolos
- Visa prover serviços de segurança como autenticação, integridade e confidencialidade
 - Authentication Header (AH) - Integridade
 - Encapsulation Security Payload (ESP) - Confidencialidade e integridade
- Os serviços são providos na camada IP e oferecem proteção às camadas superiores
- A arquitetura do IPSEC foi originalmente especificada na RFC2401 em 1998 e posteriormente atualizada pela RFC4301 em 2005

IPSEC – Modo Transporte

- Tem o objetivo de realizar IPSEC entre dois pontos
- Configuração do IPSEC feita em cada um dos dispositivos
- Para cada comunicação IPSEC um par de configurações deve ser realizado
- Apesar de ser ponto a ponto pode passar por outros nós da rede



IPSEC – Modo Túnel

- Tem o objetivo de utilizar IPSEC para todo o tráfego que irá sair da rede local
- Ao invés de configurar todos os dispositivos para utilizar IPSEC, esta configuração é feita somente nos roteadores de borda que encapsulam o pacote original
- Ao chegar ao roteador de borda do destino o pacote é desencapsulado



Laboratório

Experiência 3.3

IPSec modo transporte

Página 217

Considerações finais

- Segurança em IPv6 é um assunto que ainda tem bastante a evoluir, mas é algo que foi buscado na criação do protocolo, diferentemente do IPv4
- Boas práticas são baseadas em IPv4 e terão de ser modificadas quando o IPv6 estiver em mais larga escala
- O fato do IPv6 ser mais novo pode levar a novos ataques que não haviam sido pensados anteriormente
- Não há razão para temer a segurança em IPv6 e informação e treinamento são as melhores maneiras de proteger sua rede

Dúvidas?



Obrigado !!!

nic.br egi.br

www.nic.br | www.cgi.br