
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

Tutorial IPv6 Avançado
Segurança

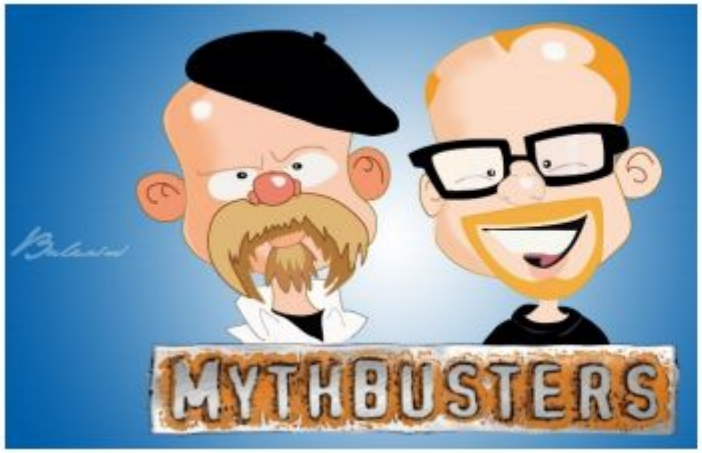
ceptro.br nic.br cgi.br

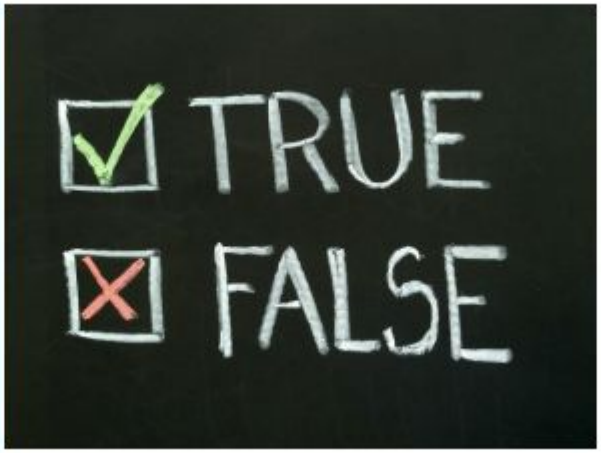
Agenda

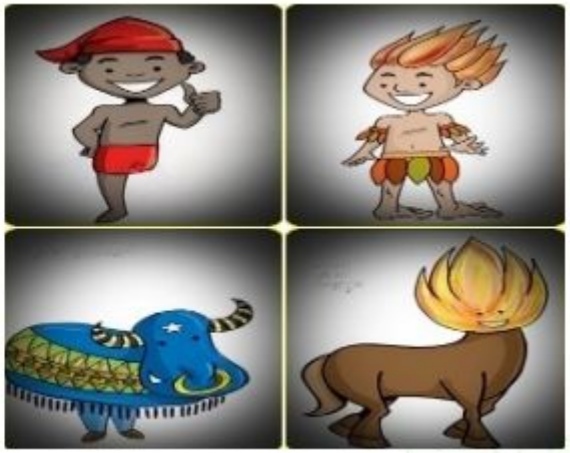
- Lendas
- Endereçamento IPv6
- Varredura de endereços em IPv6
- Firewall
- Transição de IPv4 para IPv6
- Considerações Finais

Lendas sobre segurança IPv6

- Por ser um assunto relativamente inexplorado muitas lendas existem
- Lendas são baseados em informações incompletas ou mal interpretadas







Lenda 1

- “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

- Usam-se os mais diversos argumentos na tentativa de defender um dos dois lados

- Podem acontecer cenários em que um protocolo possua uma falha que a outra versão não possui, mas estes cenários são geralmente bastante particulares

- Na prática 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

Lenda 2

- Especificação do IPv6 diz que a **inclusão** do IPsec é mandatória em toda implementação do protocolo
- Isto gerou a lenda que a utilização do IPsec é **mandatória**, o que não é verdade
- Discussões recentes sobre IPv6 estão tendendo para que a inclusão do IPsec passe a ser opcional como era no IPv4, principalmente para que dispositivos portáteis e com processamento e memórias limitados, possam utilizar IPv6 sem desrespeitar a especificação

Lenda 3

- “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
- 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

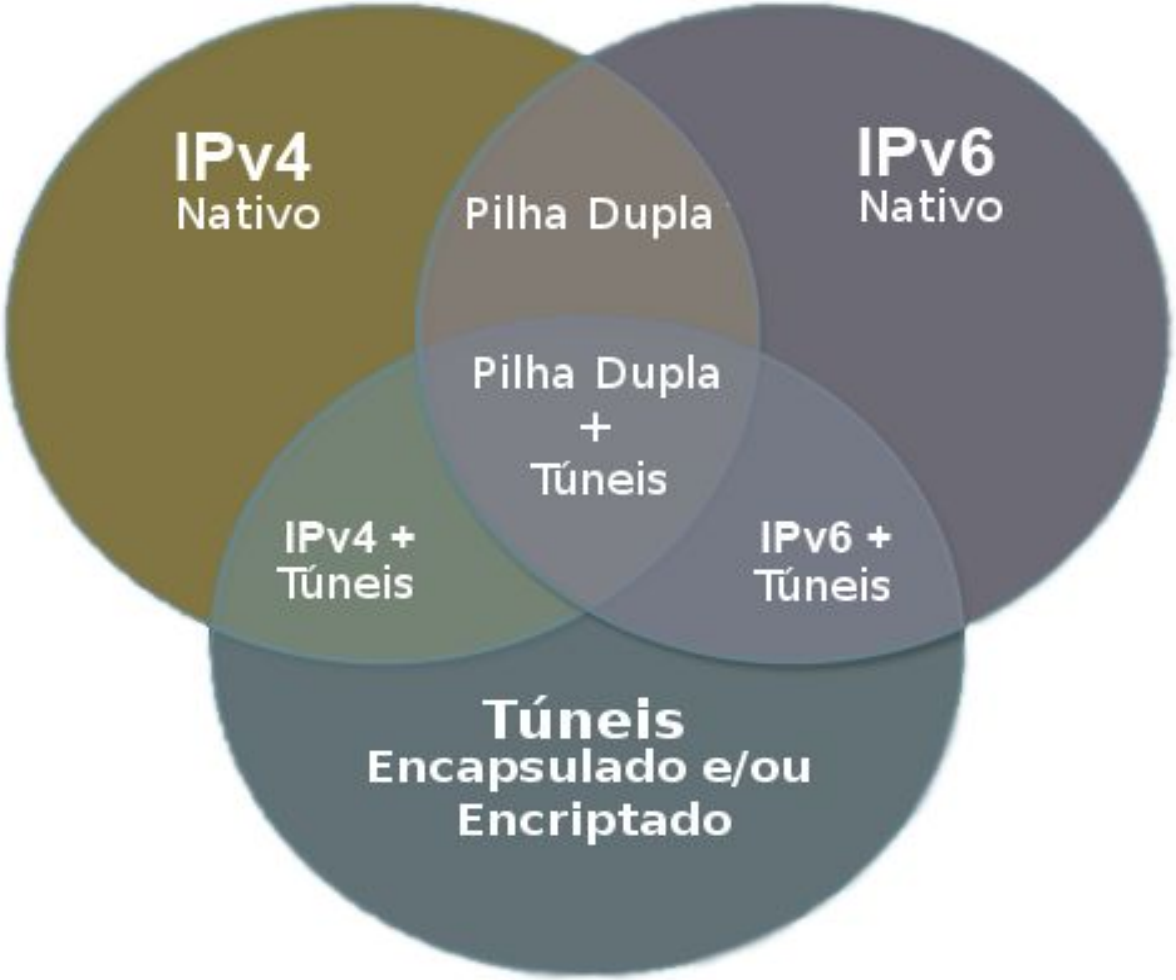
Lenda 4

- “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

Falhas, ataques e defesas no IPv6

Falha	Ataque	Defesa
Possibilidade de falsificação do Neighbor Discovery	Negação de serviço impedindo obtenção de endereço IPv6 válido	SEND, NDPmon
Possibilidade de falsificação do Router Advertisement	Man-in-the-middle ou negação de serviço por configuração inválida	SEND, RA Guard, NDPmon
Conteúdo exposto e falta de autenticação	Man-in-the-middle ou falsificação de pacotes	IPsec
	Varredura de Rede	Crypto-generated Address
	Varredura de Rede	Unique Local Addresses
	Varredura de Rede	Privacy Addresses
	Varredura de Rede	Grande quantidade de endereços
Utilizar MAC na definição do IP	Rastreabilidade de Dispositivos	RFC4941 (random address) e hash por prefixo de rede
Ignorar ou mal implementar o IPv6	Novidade / Complexidade	Treinamento de equipes
Ignorar ou mal implementar o IPv6	Falta de políticas, treinamentos e ferramentas	Treinamento de equipes
Ignorar ou mal implementar o IPv6	Túnel automático	
Túnel automático	Contornar segurança IPv4	Firewall, desabilitar túneis automáticos
6to4, Teredo	Fake relay, man in the middle	Firewall, Tunnel Broker, Túnel Manual
Falta de Familiaridade com o Modelo Fim a Fim	Ataques diretos a vulnerabilidades	Firewall, IDS

Falhas, ataques e defesas no IPv6



IPv6 em Sistemas Operacionais

- Habilitado por padrão em diversos sistemas
- Ignorar IPv6 deixa máquina exposta

Data	Produtos	Suporte ao IPv6	IPv6 Habilitado
1996	OpenBSD / NetBSD / FreeBSD	Sim	Sim
	Linux Kernel 2.1.6	Sim	Não
1997	AIX 4.2	Sim	Não
2000	Windows 95/98/ME/NT 3.5/NT 4.0	Sim (pacotes adicionais)	Não
	Windows 2000	Sim	Não
	Solaris 2.8	Sim	Sim
2001	Cisco IOS (12.x e superior)	Sim	Não
2002	Juniper (5.1 e superior)	Sim	A maioria
	IBM z/OS	Sim	Sim
	Apple OS/10.3	Sim	Sim
	Windows XP	Sim	Não
	Linux Kernel 2.4	Sim	Não
	AIX 6	Sim	Sim
	IBM AS/400	Sim	Sim
2006	Roteadores Linksys (Mindspring)	Sim	Não
	Telefones Celulares (Vários)	Sim	Sim
	Solaris 2.10	Sim	Sim
	Linux Kernel 2.6	Sim	Sim
2007	Apple Airport Extreme	Sim	Sim
	BlackBerry (Telefone Celular)	Sim	Não
	Windows Vista	Sim	Sim
	HP-UX 11iv2	Sim	Sim
	Open VMS	Sim	Sim
	Mac OS/X Leopard	Sim	Sim
2009	Cloud Computing e Sistemas embarcados	Sim	Sim

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
- Worms que utilizam varredura como era no IPv4 para infectar outros dispositivos, terão dificuldades para continuar se propagando

Varredura de endereços (Scanning)

- Devem surgir 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
  - – Explorar endereços atribuídos automaticamente com base no MAC, fixando a parte do número correspondente ao fabricante da placa de rede

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

Transição de IPv4 para IPv6

- O IPv6 foi concebido para funcionar junto o IPv4 em pilha dupla
- Isto não ocorreu e outras técnicas de transição foram concebidas (túneis, traduções etc)
- Transição de IPv4 para IPv6 abre brechas de segurança quando:
  - Rede IPv4 ignora a existência de IPv6, pois computadores e equipamentos que suportam IPv6 podem se comunicar em IPv6 evitando a segurança implementada para IPv4
  - Túneis automáticos são ignorados e a rede IPv4 não trata pacotes encapsulados, permitindo um atacante acessar a rede evitando a segurança IPv4 ou um usuário dentro da rede acessar conteúdo ou redes que seriam bloqueadas se o acesso fosse via IPv4

Transição de IPv4 para IPv6

- Técnicas de transição podem ser alvo de ataques. 6to4 e Teredo, por exemplo, dependem de servidores públicos para a criação do túnel que transporta IPv6 dentro de IPv4
  - Estes servidores não possuem garantia de qualidade e de confiabilidade e podem agir maliciosamente, como sniffer ou man-in-the-middle
  - Podem sofrer de indisponibilidade agindo como buracos negros
  - Pacotes podem ser facilmente forjados (spoofados)

Transição de IPv4 para IPv6

- 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 6over4	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

Firewall

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 modificas 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