Capacitação IPv6.br

Segurança em IPv6

Agenda

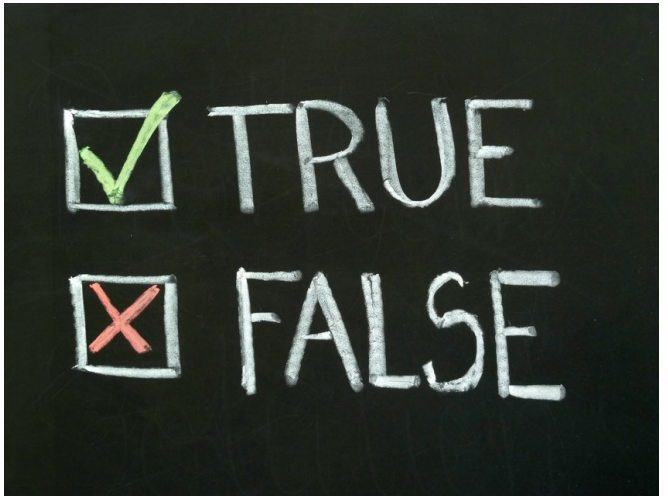
- Objetivos
- Lendas
- Ferramentas
- Neighbor Discovery Protocol
- SEND, NDPmon e RA Guard
- Endereçamento IPv6
- Varredura de endereços em IPv6
- Firewall
- Transição de IPv4 para IPv6
- IPSEC
- Considerações Finais

Objetivos

- Introdução a segurança em IPv6
- Exercícios para entender e explorar segurança em IPv6
- Mostrar diferenças entre segurança em IPv6 e IPv4
- Não serão tratados todos os aspectos de segurança

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

Lenda 1

- 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

- **“IPsec é mandatório no IPv6, por isso, ele é mais seguro que o IPv4”**
- 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

Lenda 3

- 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

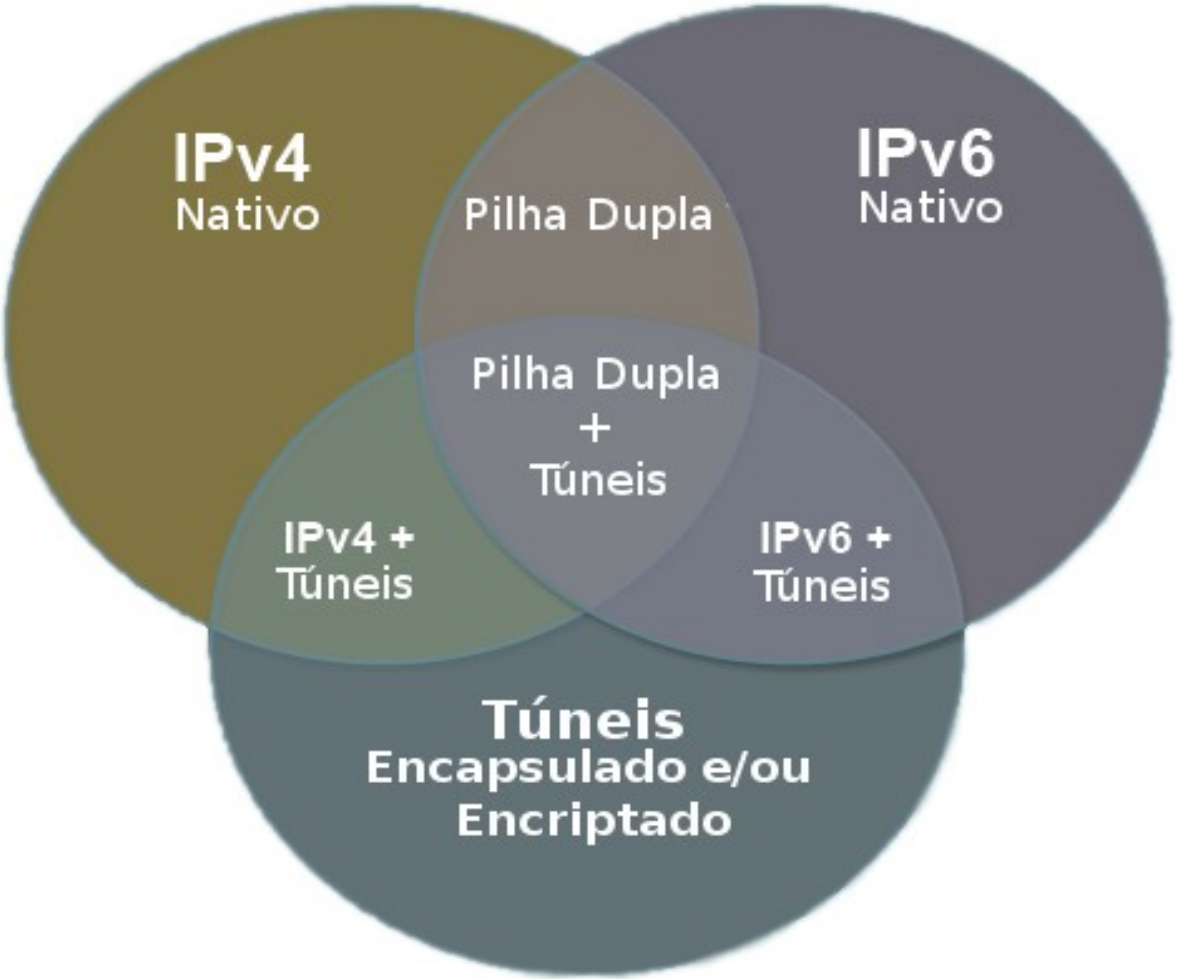
Ferramentas

- Existem diversas ferramentas para geração de ataques e para realizar defesas
- Nos laboratórios será utilizada a ferramenta THC-IPv6 (http://www.thc.org/thc-ipv6/) para realização de ataques
- Para defesa serão utilizadas ferramentas presentes ou portadas para o Linux, por exemplo, o NDPMON
- Simulação de rede feita com o CORE (http://cs.itd.nrl.navy.mil/work/core/)

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

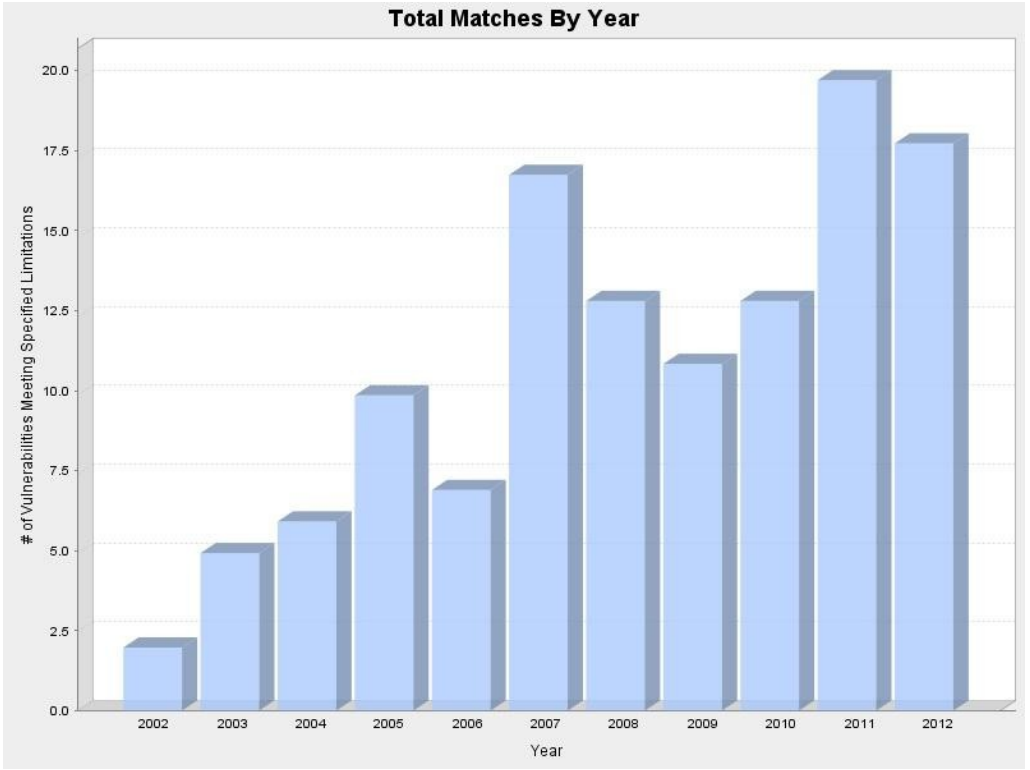


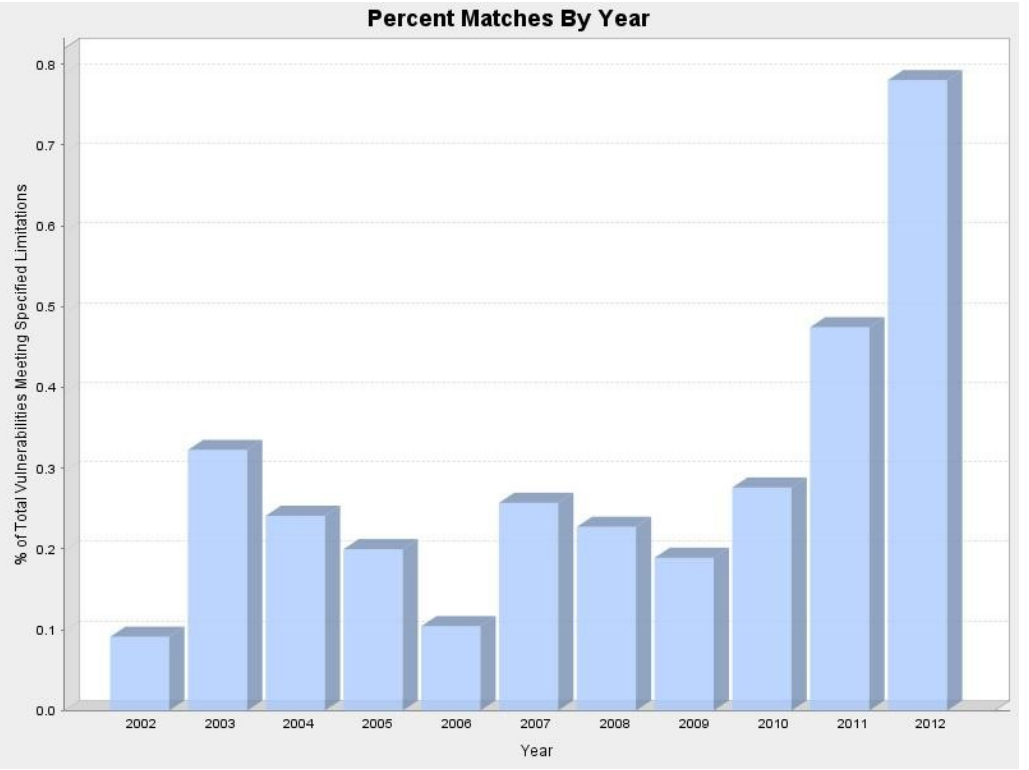
IPv6 em Sistemas Operacionais

- 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

Estatísticas – Vulnerabilidades IPv6





National Vulnerability Database / US-Cert: http://web.nvd.nist.gov/

13/07/2012

ICMPv6

- Versão atualizada do ICMPv4, mas não é compatível
- Desenvolvido como parte substancial da arquitetura IPv6
- Possui funcionalidades para reportar erros no processamento de pacotes, realizar diagnósticos e enviar mensagens sobre as caracteristícas da rede, também presentes no ICMPv4
- Assume funções de protocolo que existem isoladamente no IPv4:
  - ARP (Address Resolution Protocol)
  - RARP (Reverse Address Resolution Protocol)
  - IGMP (Internet Group Management Protocol)

ICMPv6

- ARP e RARP operam entre as camadas 2 e 3, enquanto ICMPv6 funciona inteiramente na camada 3, sendo encapsulado em pacotes IP
- Firewalls na camada de rede exigem atenção extra com o IPv6, pois podem bloquear funções extremamente básicas como a descoberta de vizinhos e a autoconfiguração
- Adiciona os seguintes protocolos e funcionalidades:
  - MLD (Multicast Listener Discovery)
  - NDP (Neighbor Discovery Protocol)
  - Path MTU(Maximum Transfer Unity) Discovery
  - Mobility Support
  - Autoconfiguração Stateless

Neighbor Discovery Protocol (NDP)

- Desenvolvido com a finalidade de resolver os problemas de interação entre os nós vizinhos de uma rede
- Utilizado para verificar a presença de outros nós, determinar os endereços de seus vizinhos, encontrar roteadores e atualizar informações sobre rotas
- Atua sobre dois aspectos primordiais da comunicação IPv6, a autoconfiguração de nós e a transmissão de pacotes
- A autoconfiguração de nós, possui três funcionalidades:
  - Address Autoconfiguration
  - Parameter Discovery
  - Duplicate Address Detection

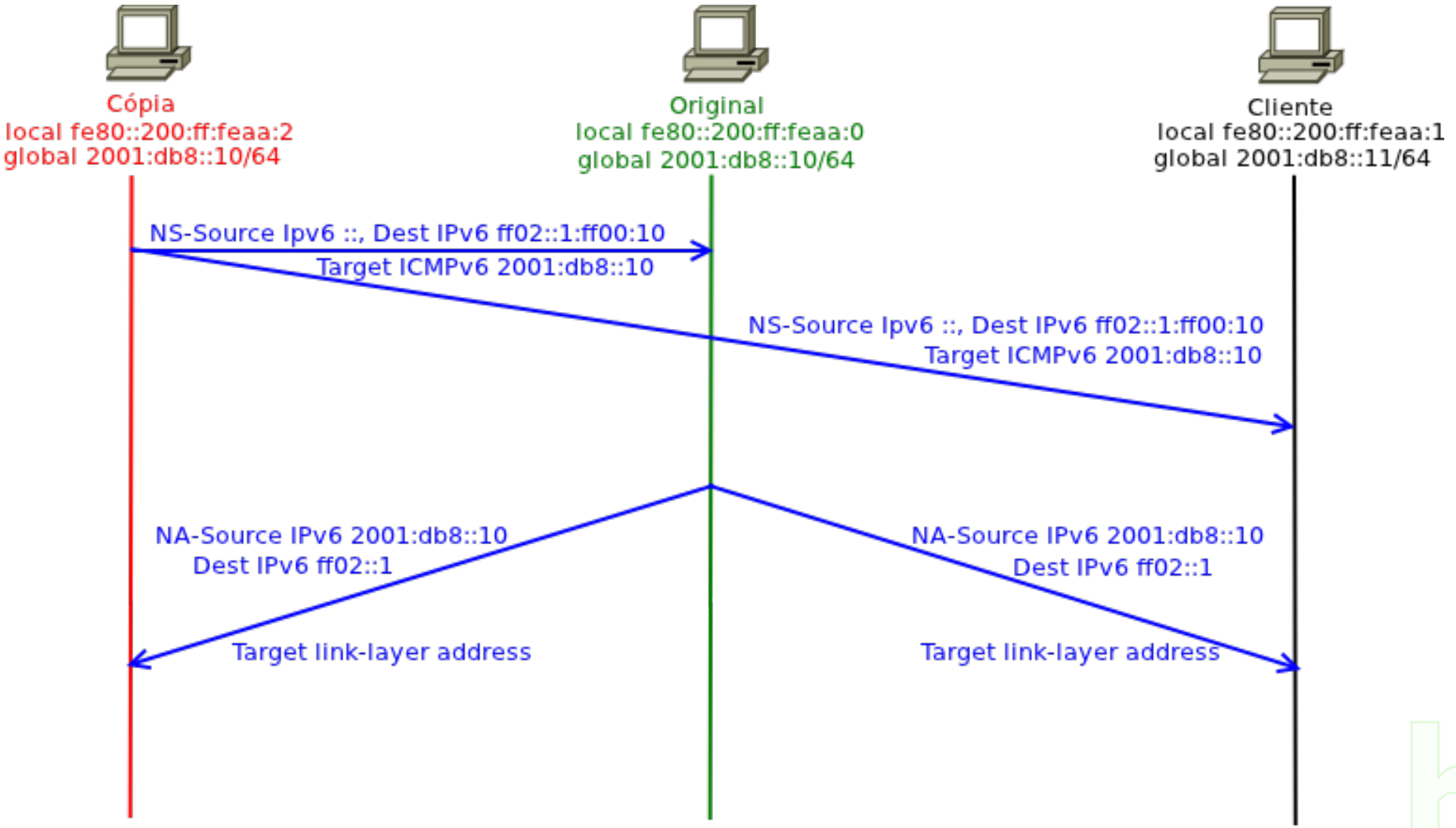
Neighbor Discovery Protocol (NDP)

- Na transmissão de pacotes entre nós contribui com o funcionamento de seis processos:
  - Router discovery
  - Prefix discovery
  - Address resolution
  - Neighbor Unreachability Detection
  - Redirect
  - Next-hop Determination

Neighbor Discovery Protocol (NDP)

- Utiliza as seguintes mensagens ICMPv6 para a realização de suas tarefas:
  - Router Solicitation (RS), tipo 133
  - Router Advertisement (RA), tipo 134
  - Neighbor Solicitation (NS), tipo 135
  - Neighbor Advertisement (NA), tipo 136
  - Redirect, tipo 137

Detecção de Endereço Duplicado (DAD)



Negação de Serviço com 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

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

Mitigação destes ataque ao NDP

- IPv6 possui um protocolo específico para o problema, chamado Secure Neighbor Discovery (SEND)
- Pode-se utilizar ferramentas que monitoram o NDP, por exemplo, NDPmon ou RA Guard
- Pode-se utilizar switch inteligente capaz de rejeitar mensagens de RA em portas que não possuam um roteador conectado
- O IPv4 possuí problema similar, o ARP Spoofing

SEND (RFC 3971)

- Utiliza autenticação dos dispositivos para evitar pacotes falsificados
- O funcionamento depende dos seguintes componentes:
  - Caminho de Certificação responsável por garantir a autoridade e autenticidade dos roteadores antes de aceitar um roteador como padrão
  - Endereços Criptograficamente Gerados (CGA): garantem que o originador de uma mensagem é o dono do endereço. Necessita par de chaves pública-privada para possuir um endereço CGA
  - Assinatura RSA que garante a integridade e autenticação do originador e da mensagem
  - Campos Timestamp e Nonce para evitar ataques do tipo replay
    - Timestamp: quando uma conexão não está estabelecida
    - Nonce: mensagens pareadas do tipo Solicitation-Advertisement

SEND (RFC 3971)

- Implementação através de um repositório central global ou local:
  - Necessita uma entidade central que valida e autoriza os roteadores
  - Para a utilização do SEND bastaria configurar em todos os dispositivos com a chave da entidade central
  - Esta entidade pode ser global sob controle da IANA ou de maneira cooperativa entre os RIRs (Registros Regionais), entretanto não existe tal entidade atualmente
  - Pode ser criada uma entidade central na rede do usuário

SEND (RFC 3971)

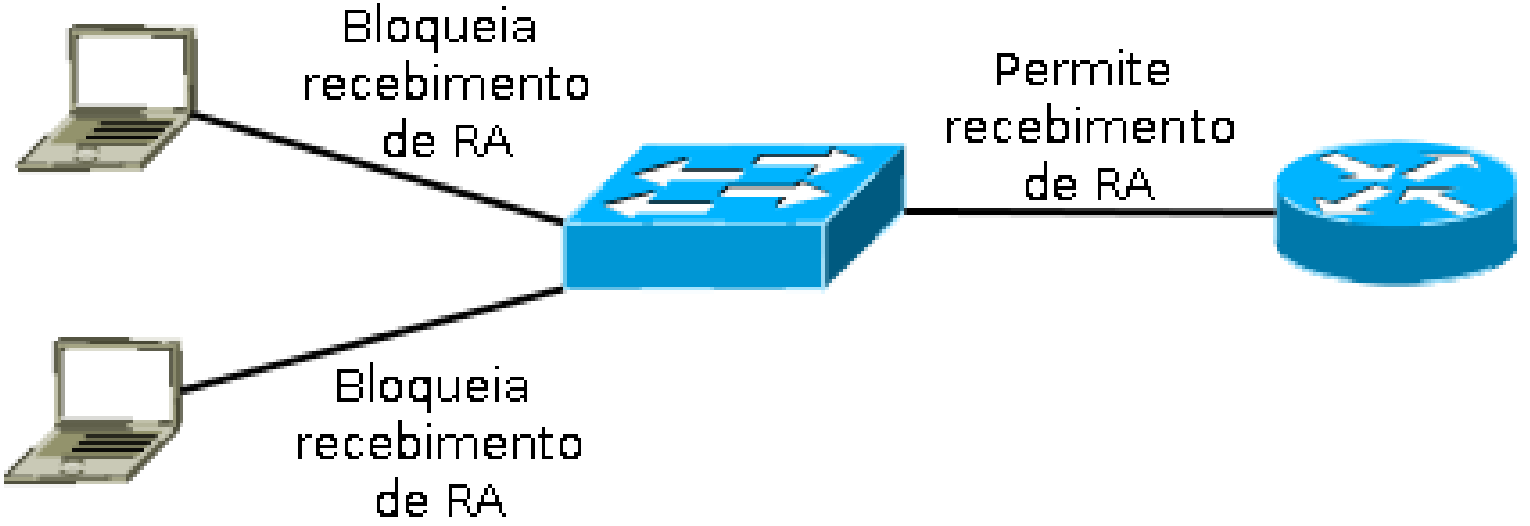
- Implementação através de um modelo mais descentralizado
  - Os dispositivos devem possuir uma coleção de chaves públicas confiáveis
  - Coleção pode ser gerada dentro da própria organização, pelo provedor de Internet ou por entidade terceirizada
  - Pode ser necessário que um dispositivo funcione sem o SEND caso não possua a chave de um novo roteador na rede
- Falta de suporte e de implementações impossibilita utilização em larga escala

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

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



Laboratório

Negação de Serviço

Ataque ao NDP

Endereçamento IPv6

- Um endereço IPv4 é formado por 32 bits
  - 2^{32} = 4.294.967.296
- Um endereço IPv6 é formado por 128 bits
  - 2^{128} = **340.282.366.920.938.463.463.374.607.431.768.211.456**

  ~ 79 octilhões ($7,9 \times 10^{28}$) de vezes a quantidade de endereços IPv4

Endereçamento IPv6

- A representação dos endereços IPv6, divide o endereço em oito grupos de 16 bits, separando-os por “:”, escritos com dígitos hexadecimais.

2001:0DB8:AD1F:25E2:CADE:CAFE:F0CA:84C1

- Na representação de um endereço IPv6 é permitido:
  - Utilizar caracteres maiúsculos ou minúsculos;
  - Omitir os zeros à esquerda; e
  - Representar os zeros contínuos por “::”
- Últimos 64 bits previstos para identificação do dispositivos, permitindo 2^{64} dispositivos por rede

Varredura de endereços (Scanning)

- Tornou-se mais complexo, mas não impossível
- Com uma mascara 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

Combatendo a Varredura

- Pode-se utilizar endereços CGA
- Endereços IPv6 gerados criptograficamente utilizando uma função hash de chaves públicas
  - Prefixo /64 da sub-rede
  - Chave pública do proprietário endereço
  - Parâmetro de segurança
- Utiliza certificados X.509
- Utiliza a função hash SHA-1

Combatendo a Varredura

- Endereços CGA são difíceis de administrar e identificar qual o IP de cada máquina na rede
- Modificações a RFC (draft-gont-6man-stable-privacy-addresses-01) estão sendo sugeridas para que os últimos 64 bits sejam sempre os mesmos enquanto o dispositivo permanecer na rede
- Ao mudar de rede os últimos 64 bits são alterados

Rastreabilidade de Dispositivos

- Quando um dispositivo utiliza autoconfiguração de endereço, o MAC address é usado como base para a geração dos últimos 64 bits
- Estes 64 bits são sempre iguais e formam um identificador único independente da rede
- draft-gont-6man-stable-privacy-addresses-01 também endereça esta questão, pois ao mudar de rede os últimos 64 bits mudam

Rastreabilidade de Dispositivos

- Estes identificador único baseado nos 64 bits permite a criação de um “Super Cookie” nos servidores identificando o usuário que iniciou a conexão sem necessidade de salvar ou verificar cookies na máquina cliente
- Entretanto isto já é possível sem o IPv6 baseando-se em informações do browser: https://panopticlick.eff.org/

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:
  - Statefull: 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

Firewall – Regras ICMPv6

	Recomendado não descartar	
Mensagem (Tipo)	Trânsito	Local
Mensagens de Erro:	Permite não local quando associado a conexões permitidas	
Time Exceeded (3) – Código 1	✔	✔
Parameter Problem (4) – Código 0	✔	✔
IPv6 Móvel:	Permite não local para dispositivos terminais permitidos	
Home Agent Address Discovery Request (144)	✔	
Home Agent Address Discovery Reply (145)	✔	
Mobile Prefix Solicitation (146)	✔	
Mobile Prefix Advertisement (147)	✔	

Firewall – Regras ICMPv6

	Obrigatório não descartar	
Mensagem (Tipo)	**Trânsito**	**Local**
Manutenção da Comunicação:	Permite não local quando associado a conexões permitidas	
Destination Unreachable (1) – Todos os códigos	✔	✔
Packet Too Big (2)	✔	✔
Time Exceeded (3) – Somente código 0	✔	✔
Parameter Problem (4) – Somente códigos 1 e 2	✔	✔
Verificação de Conectividade:	Permite/Nega de acordo com a política de segurança da topologia	
Echo Request (128)	✔	✔
Echo Response (129)	✔	✔
Configuração de Endereços e Seleção de Roteadores:	Permitido somente em tráfego link-local	
Router Solicitation (133)		✔
Router Advertisement (134)		✔
Neighbor Solicitation (135)		✔
Neighbor Advertisement (136)		✔
Inverse Neighbor Discovery Solicitation (141)		✔
Inverse Neighbor Discovery Advertisement (142)		✔

Firewall – Regras ICMPv6

	Obrigatório não descartar	
Mensagem (Tipo)	Trânsito	Local
Notificação de Recebedores de Multicast Link-Local:	Permitido somente em tráfego link-local	
Listener Query (130)		✔
Listener Report (131)		✔
Listener Done (132)		✔
Listener Report v2 (143)		✔
Notificação do Caminho de Certificação SEND:	Permitido somente em tráfego link-local	
Certification Path Solicitation (148)		✔
Certification Path Advertisement (149)		✔
Multicast Router Discovery:	Permitido somente em tráfego link-local	
Multicast Router Advertisement (151)		✔
Multicast Router Solicitation (152)		✔
Multicast Router Termination (153)		✔

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

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
- 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

- IPsec possui dois modos de operação
  - Modo Túnel
  - Modo Transporte
- IPsec possui dois protocolos:
  - AH (Authentication Header - Cabeçalho de Autenticação)
  - ESP (Encapsulated Security Payload - Dados Encapsulados com Segurança)

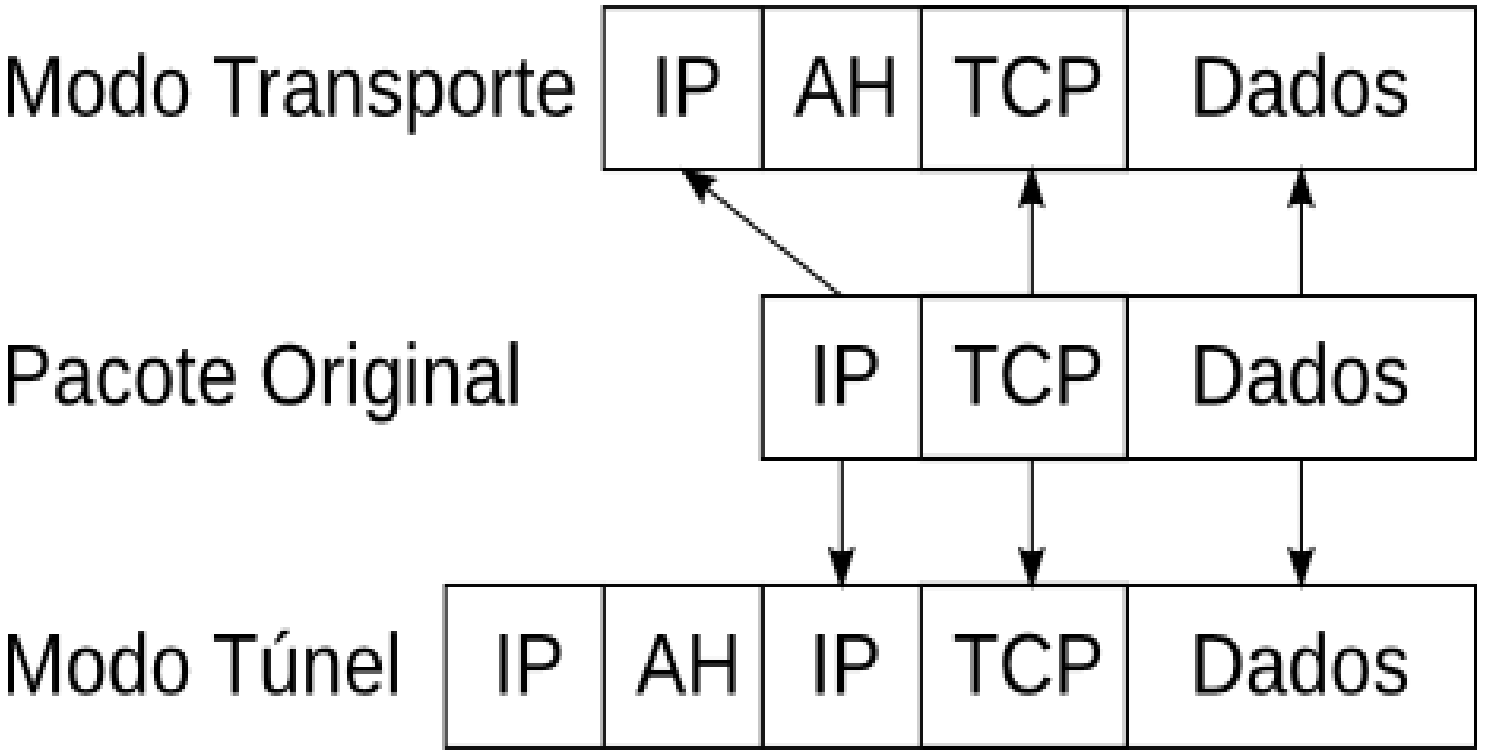
IPSEC – Modo Transporte

- 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

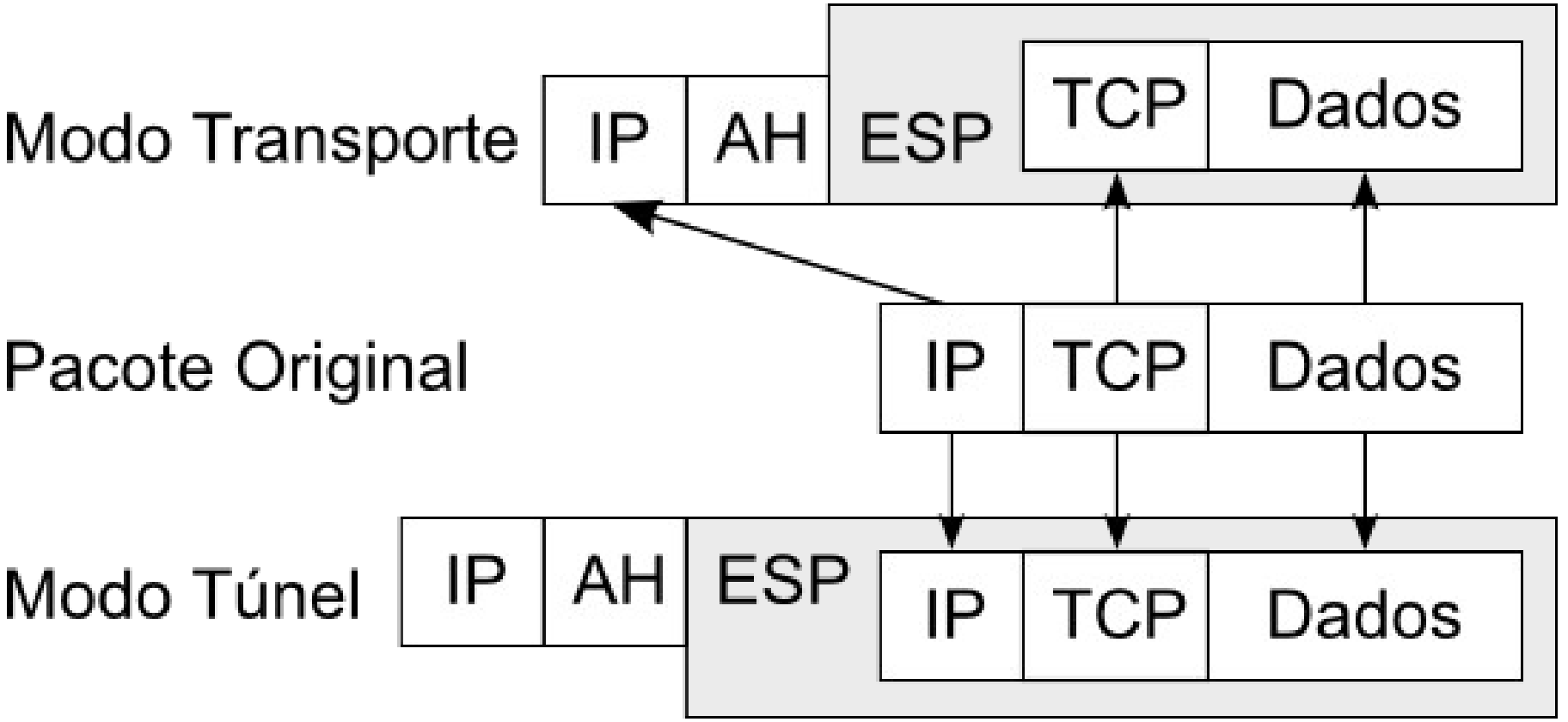
IPSEC – Modo Túnel

- 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

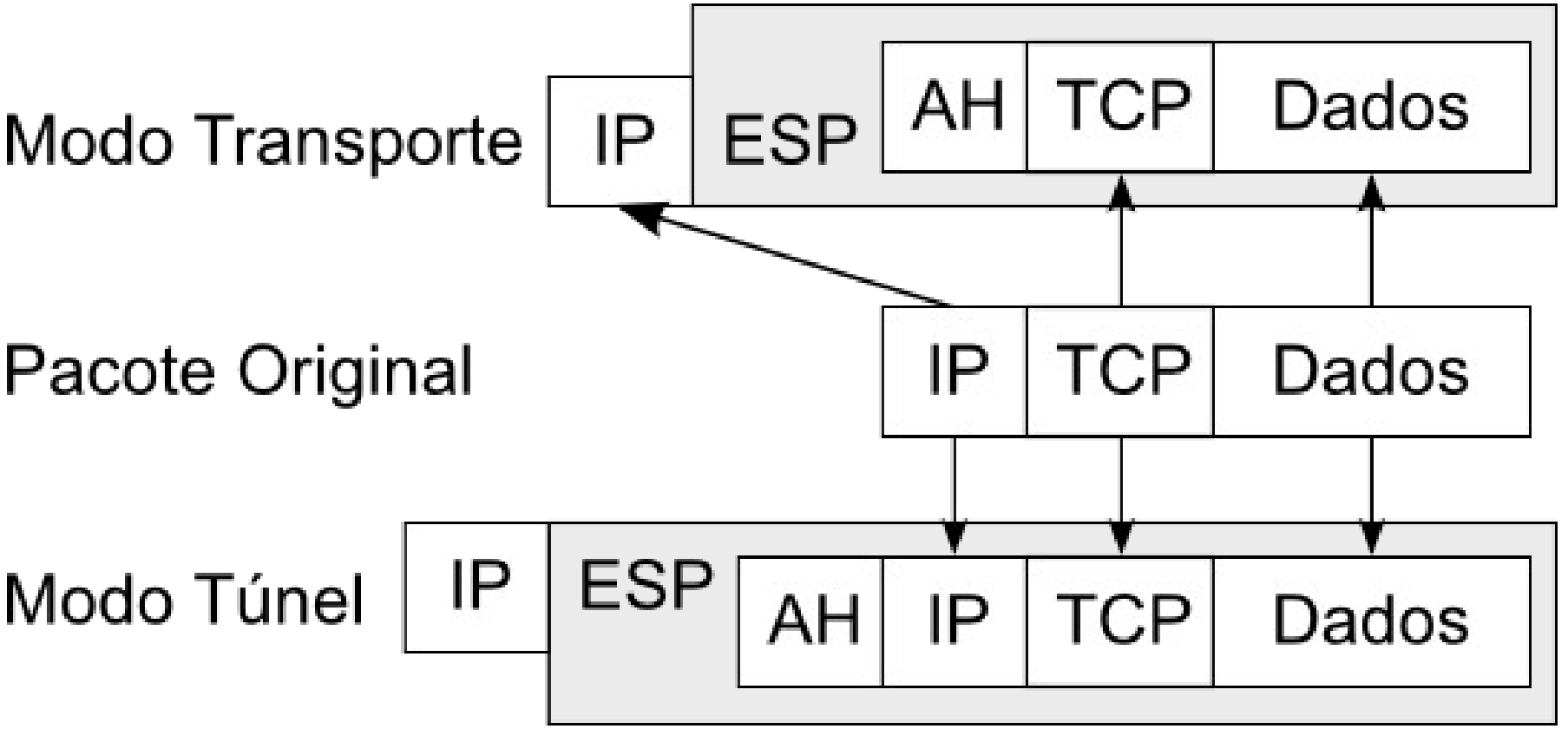
IPSEC – Transporte x Túnel



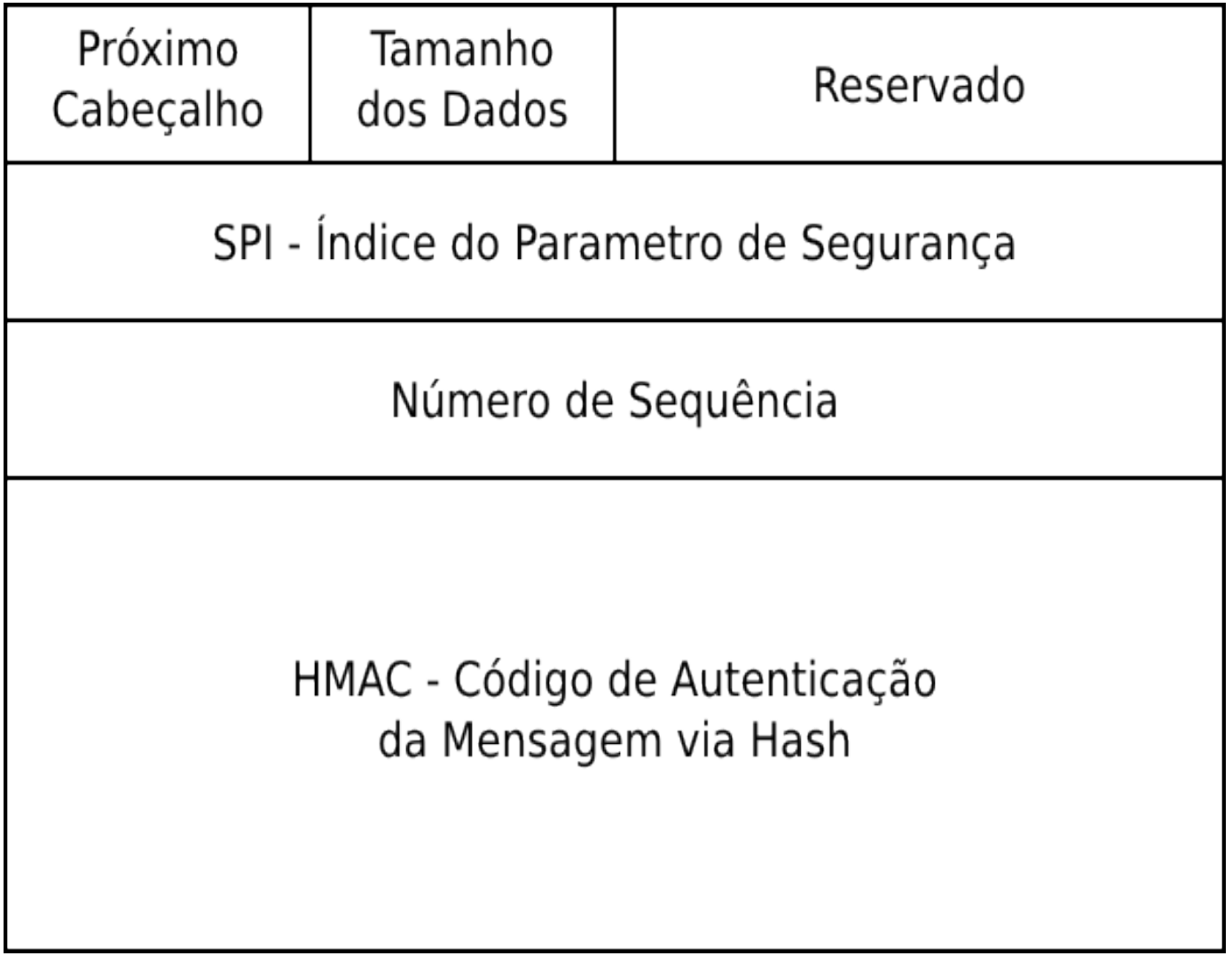
IPSEC – Transporte x Túnel



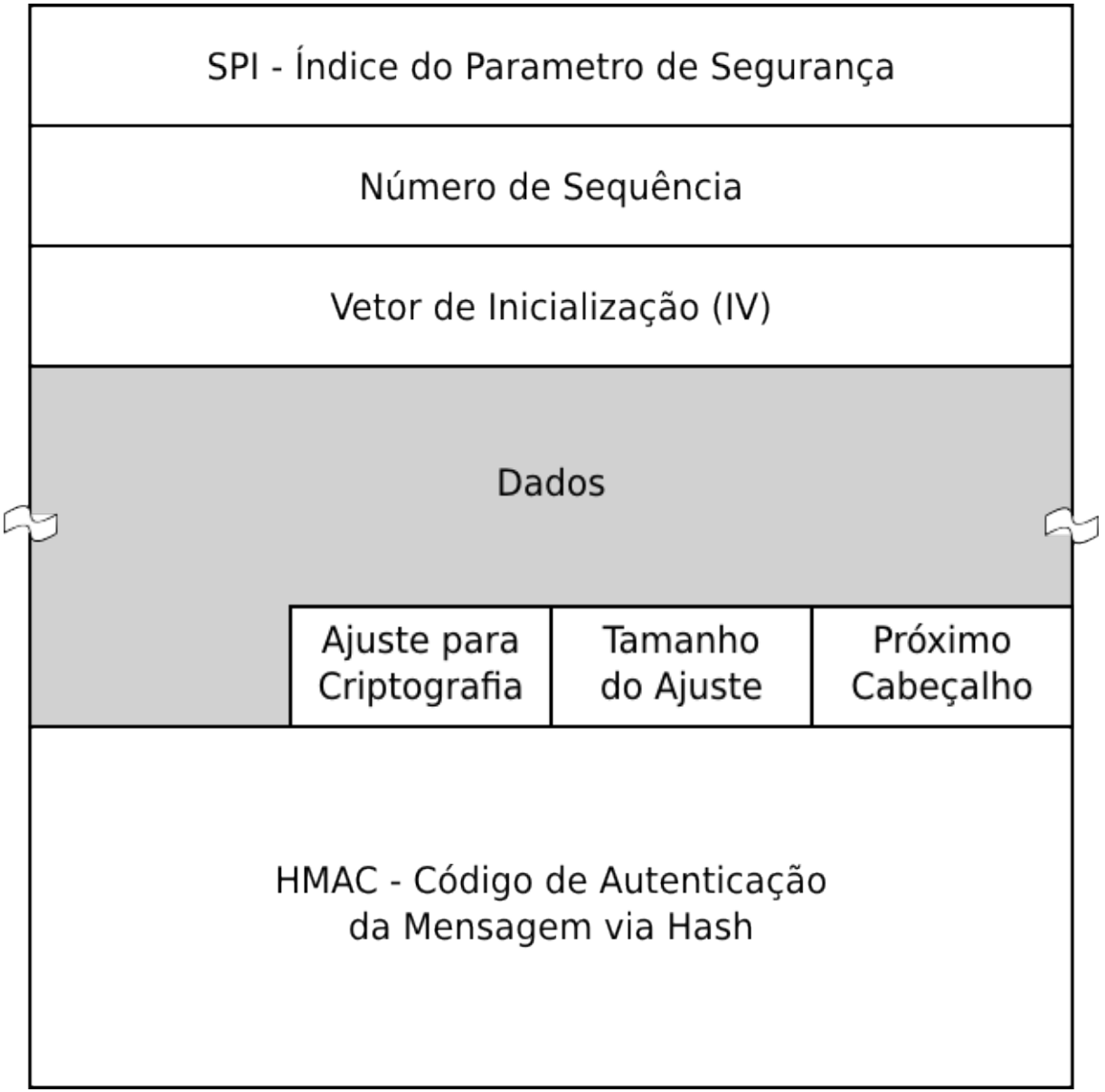
IPSEC – Transporte x Túnel



IPSEC – Authentication Header



IPSEC – Encapsulated Security Payload



IPSEC – Troca de chaves

- Um ponto fundamental para o funcionamento do IPSEC são as chaves para autenticação, integridade e criptografia
- É necessário que os dois lados saibam as chaves que devem ser usadas
- Um ponto recorrente quando se fala de criptografia é como trocar as chaves por um meio que ainda não está seguro
- As ideias básicas de utilizar outro meio como telefone ou email criptografado são válidas, mas necessitam de intervenção humana

IPSEC – Troca de chaves

- O IPSEC sugere a utilização do protocolo IKE que resolve a maior parte dos possíveis ataques. O protocolo IKE trabalha de dois modos:
  - chaves pré-compartilhadas
  - certificados X.509
- O protocolo IKE trabalha em duas fases:
  - Fase 1: a autenticidade dos dispositivos é verificada, através de uma série de mensagens trocadas, e uma chave ISAKMP SA (Internet Security Association Key Management Security Associantion) é gerada
  - Fase 2: a partir da ISAKMP SA as chaves para o AH e ESP para esta comunicação são geradas e o IPSEC começa a ser utilizado

Laboratório

IPSEC

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