Formação IPv6 - Maputo

Segurança

Maputo 28 de Agosto de 2008

Carlos Friaças e Pedro Lorga

Segurança

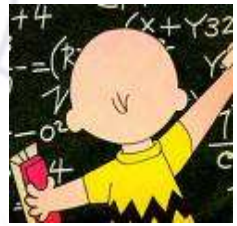
Agenda/Índice

- O que há de novo no IPv6?
- Ameaças
- IPsec
- Firewall
- Conclusão

O que há de novo no IPv6?

- A Segurança foi uma preocupação desde início

- Áreas que beneficiaram da forma de ver a rede trazida pelo IPv6:
  - Ameaças ao acesso móvel e ao IP móvel
  - Endereços gerados Criptograficamente
  - Protocolos para Autenticação e Acesso à Rede
  - IPsec
  - Tornar as intrusões mais difíceis



Ameaças

- Escuta passiva e activa
- Repetição
- Análise de Tráfego
- Negação de Serviço
- Ataque Físico
- *Passwords*
- Vírus, Cavalos de Tróia, W*orms*
- Acesso Acidental
- Desastres Naturais
- Engenharia Social

Ameaças

- Scanning de Gateways e Máquinas
- Scanning de Endereços Multicast
  - Não havendo broadcast é possível recorrer a outros métodos
- Spoofing
- Controle de acesso não autorizado
  - Ter em atenção a criação de listas para IPv6

Ameaças

- Ataque ao Encaminhamento IPv6
  - É recomendado o uso dos tradicionais mecanismos no BGP e IS-IS
  - O IPsec garante a segurança de protocolos como o OSPFv3 e o RIPng
- *«Sniffing»*
  - Sem o recurso ao IPsec, o IPv6 está tão exposto a este tipo de ataque como o IPv4

- Mecanismos de transição
  - Ataques específicos para diferentes mecanismos

Ameaças

- Ataques *«Man-in-the-Middle»*
  - Sem o uso de IPsec, este tipo de ataques em IPv6 ou IPv4 é semelhante
- *Flooding - DDOS*
  - Idênticos em IPv4 e IPv6
- Ataques ao nível da Aplicação
  - Actualmente, a maioria das vulnerabilidades na Internet é ao nível da aplicação, que não beneficia do uso do IPsec

Scanning em IPv6

- *Scanning* = «Varrimento»
- O tamanho de cada rede é incomparavelmente maior
  - As LANs têm **2^64** endereços. Deixa de ser razoável pesquisar por um endereço sequencialmente
    - Com 1 milhão de endereços/segundo, seriam necessários mais de 500 mil anos para percorrer todos os endereços de uma única LAN
  - A ferramenta NMAP por exemplo, nem sequer suporta *scanning* em IPv6

Scanning em IPv6

- Os métodos de *Scanning* em IPv6 vão provavelmente evoluir
  - Os servidores públicos necessitam de estar registados no DNS, o que constitui um alvo fácil
  - Os Administradores das redes podem adoptar endereços fáceis de memorizar (por exemplo… ::1,::2,::53)
  - Os endereços EUI-64 têm uma componente fixa (de 16 bits)
  - Os códigos que identificam os fabricantes das placas de rede são bem conhecidos (primeiros 24 bits do endereço MAC)
  - Outras técnicas incluem obtenção de informação através de zonas de DNS ou de *logs*
    - Negar a transferência de zona (para o mundo) é prática corrente
  - Ao comprometer pontos importantes da arquitectura (*ex: routers*), um atacante pode detectar a existência de muitos alvos possíveis

Scanning em IPv6 - Multicast

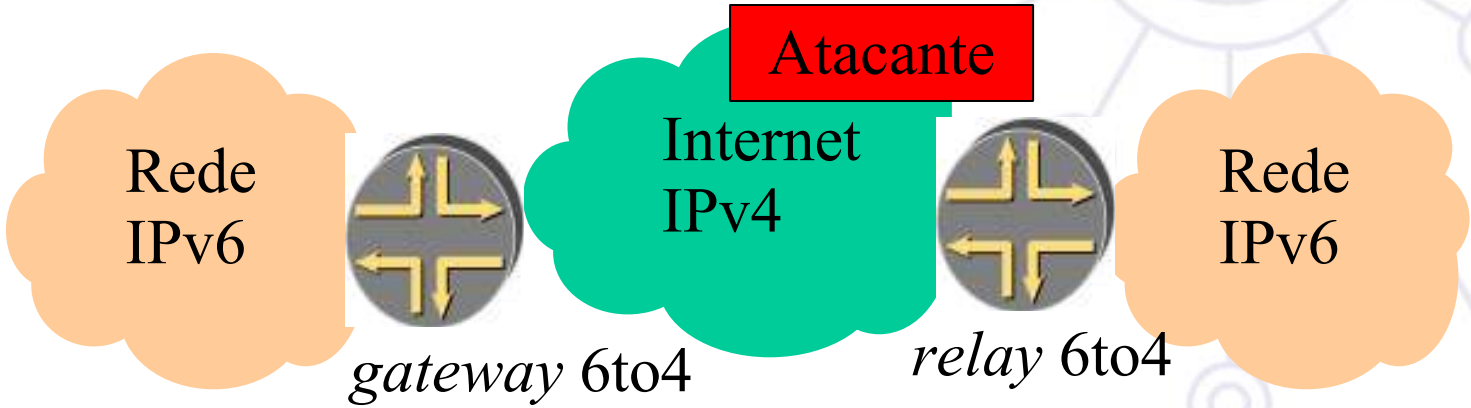
- Novos vectores de ataque
- Uso de endereços Multicast para «emular» funções de *router* ou servidor DHCPv6
  - Todos os nós (FF02::1)
  - Todos os *routers* (FF05::2)
  - Todos os servidores DHCPv6 (FF05::5)
- Estes endereços devem ser filtrados em cada ponto de «fronteira»
  - Este é o comportamento por omissão se o IPv6 Multicast não estiver activo no *Backbone*

Spoofing em IPv6

- A maior agregação que é possível com o IPv6, torna menos complexa a filtragem para impedir o *spoofing* em pontos estratégicos da rede
- O aspecto negativo tem a ver com os últimos 64 bits
  - Para identificar um utilizador através de um endereço IPv6, seria necessário manter constantemente o mapeamento entre endereços IPv6 e endereços MAC

Spoofing em IPv4 com *6to4*

- Através de tráfego injectado da Internet IPv4 para uma rede IPv6, recorrendo às características do mecanismo de transição *6to4*
  - Origem IPv4: Origem IPv4 *spoofed*
  - Destino IPv4: *Relay 6to4 Anycast* (192.88.99.1)
  - Origem IPv6: Origem IPv6 *spoofed*, com prefixo *2002*::
  - Destino IPv6: Válido



Controle de acesso

- A implementação da política é ainda feita nas firewalls (ou listas de acesso nos routers)
- Algumas considerações
  - Filtrar endereços multicast nos pontos de *fronteira*
  - Filtrar endereços IPv4 mapeados em IPv6

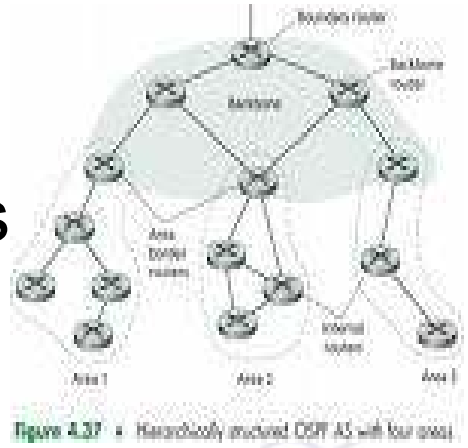
Action	Src	Dst	Src port	Dst port
permit	a:b:c:d::e	x:y:z:w::v	any	ssh
deny	any	any		

Controle de acesso

- Criar filtros para endereços *bogon*
  - em IPv4 é mais fácil negar os *bogon* + redes privadas
  - em IPv6 é mais fácil permitir os endereços legítimos

Action	Src	Dst	Src port	Dst port
deny	2001:db8::/32	host/net		
permit	2001::/16	host/net	any	service
permit	2002::/16	host/net	any	service
permit	2003::/16	host/net	any	service
permit	3ffe::/16	host/net	any	service
deny	any	any		

Encaminhamento



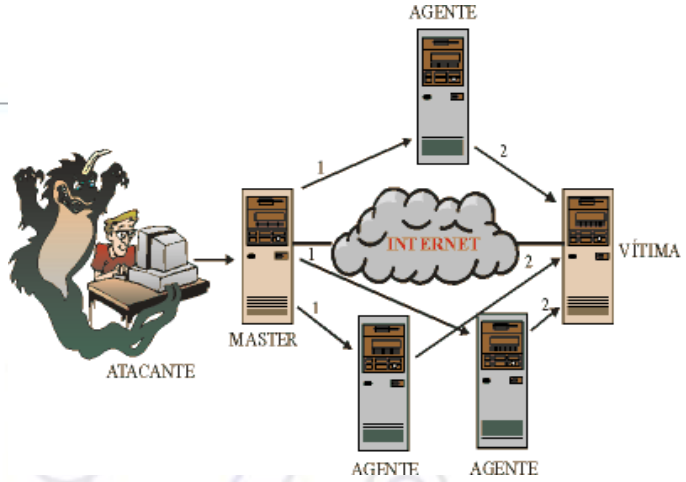
- Devem utilizar-se as mesmas medidas de protecção que em IPv4
  - Autenticação de vizinhos (BGP)
  - Filtragem de anúncios inválidos
  - Cifragem de mensagens de encaminhamento
- Basicamente deve aplicar-se o mesmo nível de segurança em IPv6 e em IPv4

Nota: atenção nos routers a todos os serviços que estão a correr (ex: http,telnet, ssh). Estes devem estar também protegidos contra acessos indevidos em IPv6.

Mecanismos de Transição

- Há cerca de 15 métodos com várias combinações possíveis
- Dual stack:
  – aplicar o mesmo nível de segurança para ambos os protocolos
- Túneis
  – iptunnel – utiliza o **Protocolo 41** para atravessar a firewall
  – túnel GRE – será mais aceitável uma vez que já era usando anteriormente ao aparecimento do IPv6.

DDoS



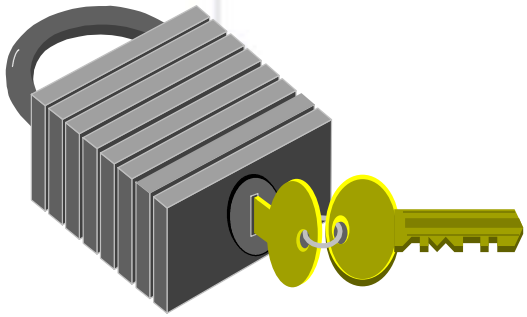
- **Não existem endereços *broadcast* em IPv6**
  - Evita ataques através do envio de pacotes ICMP para o endereço de *broadcast*

- As especificações do IPv6 proibem a geração de pacotes ICMPv6 em resposta a mensagens enviadas para endereços globais *multicast* (com a excepção da mensagem «*Packet too big*»).
  - Muitos sistemas operativos seguem a especificação
  - Ainda há alguma incerteza sobre o perigo que pode ser criado por pacotes ICMPv6 com origem em endereços *multicast* globais

Mitigação de DDoS em IPv6

- Ter a certeza que os sistemas implementam o descrito no RFC 4443
- Implementar **filtragens** recomendadas nos RFCs 2827 e 3704, à entrada do sistema autónomo
- Implementar **filtragem** à entrada de pacotes IPv6 com endereços de origem IPv6 *multicast* na rede local

IPsec



- Mecanismos gerais de segurança IP
- Fornece…
  - Autenticação
  - Confidencialidade
  - Gestão de Chaves – necessita de uma infraestrura de chaves públicas (PKI)
- Aplicável ao uso em LANs, e WANs públicas & privadas, e na Internet. Definido como obrigatório nas normas do IPv6
- O IPsec não é apenas um único protocolo. O IPsec contém um conjunto de algoritmos e uma infraestrutura que permite a comunicação entre duas partes, independentemente do algoritmo apropriado para dotar de segurança essa comunicação

IPsec

- Trabalho emanado do IPsec-wg do IETF
- Aplica-se tanto ao IPv4 como ao IPv6 e a sua implementação é:
  - Mandatória para IPv6
  - Opcional para IPv4
- Modos IPsec: Transporte & Túnel
- Arquitectura IPsec: RFC 4301
- Protocolos IPsec:
  - *Authentication Header* – AH (RFC 4302)
  - *Encapsulating Security Payload* - ESP (RFC 4303)

IPsec - Arquitectura

- Políticas de Segurança: Que tráfego é tratado?
- Associações de Segurança: Como é processado o tráfego?
- Protocolos de Segurança: Que protocolos (extensões do cabeçalho) são usados?
- Gestão de Chaves: *Internet Key Exchange* (IKE)
- Algoritmos: Autenticação e Cifragem

IPsec - Modos

- Modo de **Transporte**
  - Acima do nível IP
  - Apenas o *payload* dos datagramas IP são protegidos
- Modo de **Túnel**
  - IP dentro de IP
  - Todos os datagramas que atravessam o túnel são protegidos

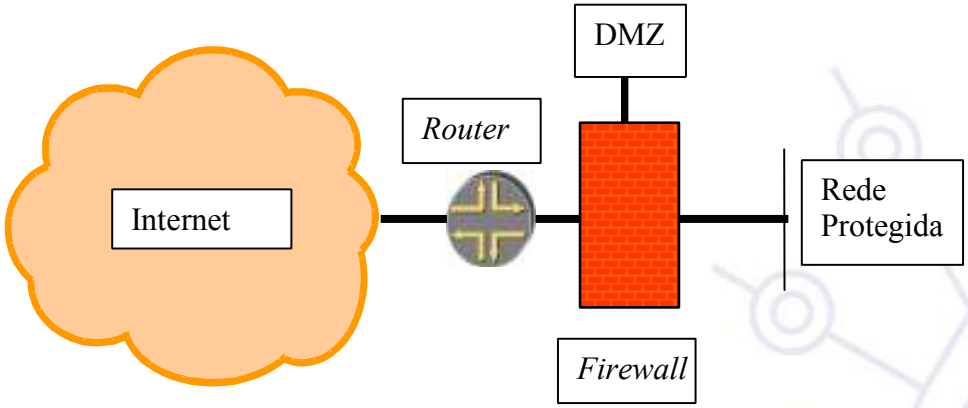
IPsec : Gestão de Chaves

- Manual
  - Chaves configuradas em cada sistema
- Automática: IKEv2 (*Internet Key Exchange* v2, RFC 4306)
  - Negociação da Associação de Segurança: ISAKMP
    - Diferentes blocos (*payloads*) são ligados a seguir ao cabeçalho ISAKMP
  - Protocolos de Troca de Chaves: **Oakley**, **Scheme**
- Algoritmos: Autenticação e Cifragem

Protecção – *Firewalls* IPv6

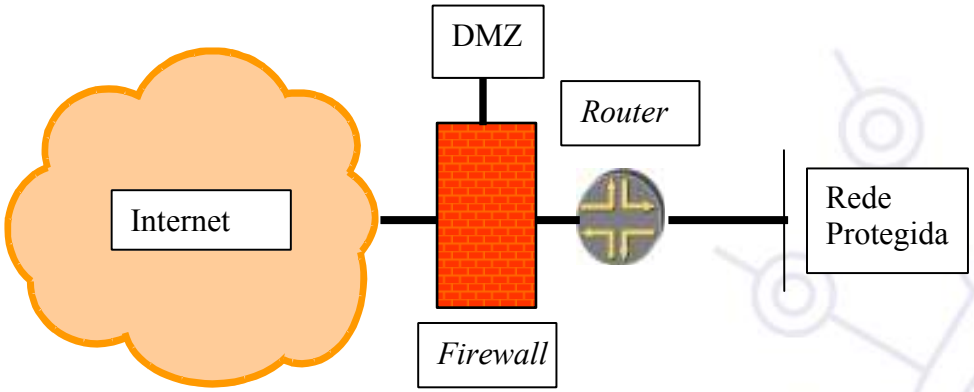
- IPv6 & *Firewalls*
  - Não elimina a segurança IPv4, se ela existir ☺
  - O processo do *firewall* IPv6 é em geral separado do *firewall* IPv4, mas pode ser efectuado no mesmo equipamento
    - É o caso da FCCN (Checkpoint & Cisco PIX -- no futuro)
  - Sem necessidade de gerir NATs
    - Mesmo nível de segurança e privacidade
    - Segurança fim-a-fim com recurso a IPsec
  - Suporte de transição e coexistência IPv4/IPv6

Firewall IPv6 – arquitectura #1



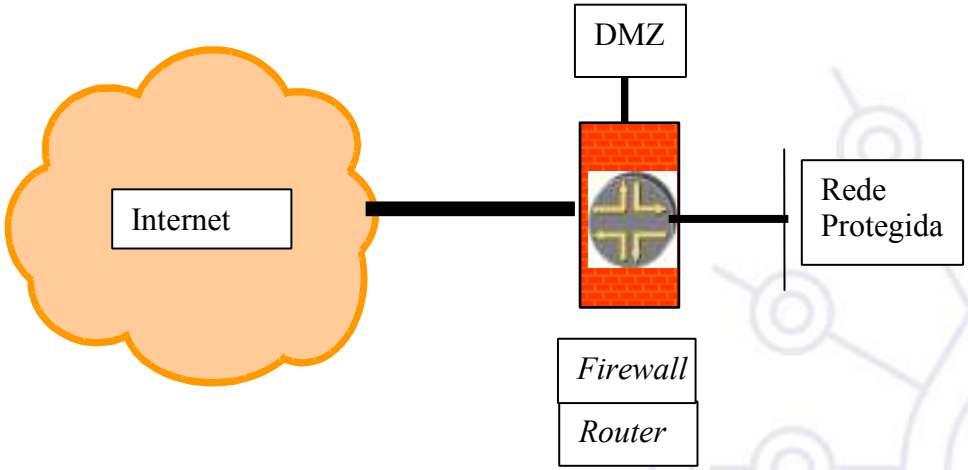
- Internet ↔ *router* ↔ *firewall* ↔ Rede
- Requisitos:
  - *Firewall* tem que suportar filtragem de pacotes *Neighbor Discovery*
  - *Firewall* tem que suportar filtragem de pacotes de Anúncio de *Router*
  - *Firewall* tem que suportar o protocolo MLD, se o Multicast é usado

Firewall IPv6 – arquitectura #2



- Internet ↔ *firewall* ↔ *router* ↔ Rede
- Requisitos:
  - *Firewall* tem que suportar filtragem de pacotes ND
  - *Firewall* tem que suportar filtragem de protocolos dinâmicos de encaminhamento (i.e. BGP, OSPF, IS-IS)
  - *Firewall* idealmente terá uma multiplicidade de *interfaces*

Firewall IPv6 – arquitectura #3



- Internet ↔ *firewall/router* ↔ Rede
- Requisitos
  - Apenas um ponto para funções de *routing* e implementação de políticas de segurança – comum em ambientes «SOHO»
  - Necessita suporte de todas as funções de *router* e também de *firewall*

Conclusão

- O IPv6 pode potencialmente melhorar a segurança na Internet
- Os elementos necessários à infraestrutura IPv6
  - Firewalls, Routers, DNS, etc.

  já estão prontos para serem utilizados com segurança
- Prestar a mesma atenção à segurança em IPv6 do que em IPv4. Apesar de não haver muitos ataques em IPv6 actualmente, eles irão certamente crescer no futuro.

Questões ?

Obrigado !