Sobrevivendo a ataques (D)DoS

Rubens Kühl Jr.

UOL Inc.

rubens@email.com

Programa

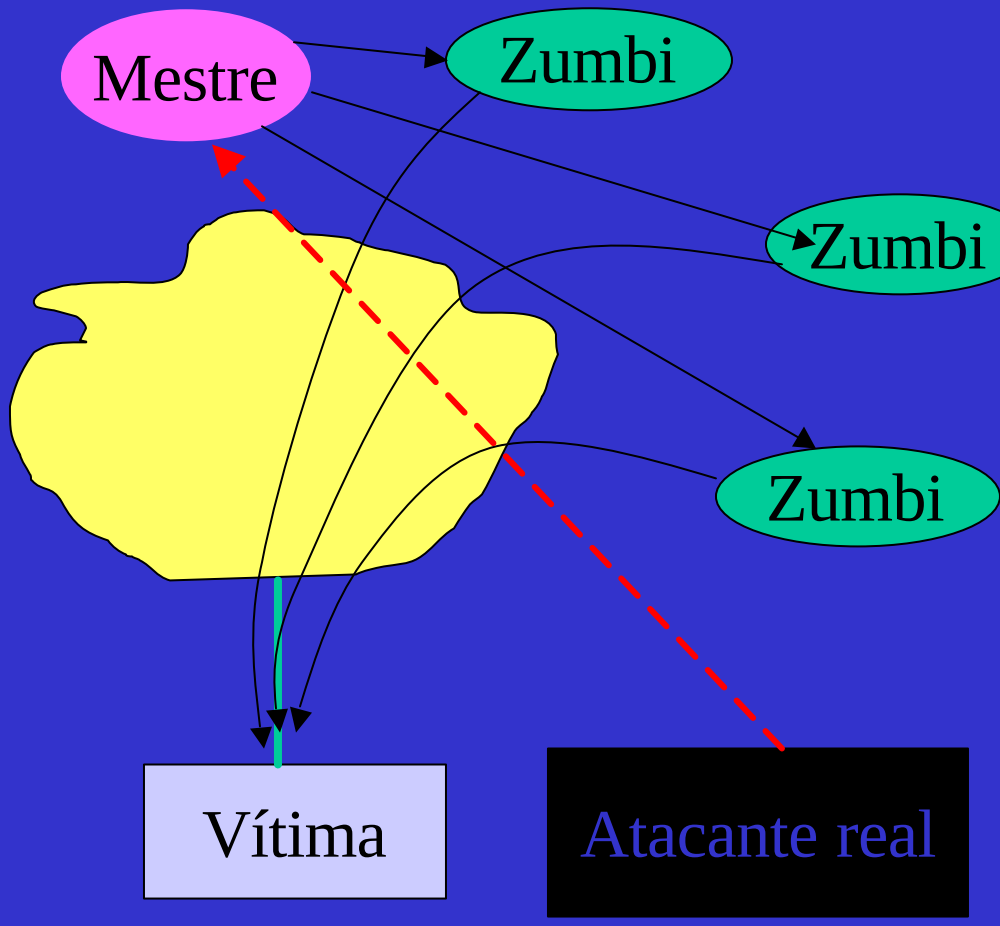
- Introdução: DoS e DDoS
- Anatomia, alvos e vítimas dos ataques DoS
- Percebendo, Reagindo e Resistindo a DoS
- Melhorando a resistência a DoS
- Evitando ser fonte de DoS
- Rastreando DoS em backbones
- Evoluções Tecnológicas
- Referências

Introdução – DoS

- DoS = Denial of Service
- DoS é tornar um serviço indisponível
- Mantra da Segurança:
  - Confidencialidade,
    Integridade,
    Disponibilidade (única afetada por DoS)
- Também pode ser visto sob a luz da Engenharia de Capacidade

Introdução - DDoS

- DDoS, Distributed DoS, é a agregação de poder de ataque
- DDoS é extremamente escalável
  - Poder de ataque nunca visto antes
- DDoS é tolerante a falha



Anatomia de DoS típicos

	Vazão de pps	Vazão de bps	Origem	IPs origem
SYN	Alta (10000+)	Baixa (5 Mbps)	Zumbis	Falsos
ICMP	Baixa	Alta (200+ Mbps)	Smurf Zumbis Exploits	Reais Falsos Reais
Frag	Baixa	Alta	Zumbis ICMP	Falsos Reais

Alvos e vítimas de DoS

- Quem são os alvos ?
  - IPs de serviços conhecidos (www.vitima.com.br)
  - IPs de hops de roteamento no caminho
  - Portas destino sabidamente abertas (HTTP em www)
  - Portas destino aleatórias
- Quem são as vítimas ?
  - Servidores
  - Canais de LAN e WAN
  - Roteadores, firewalls, load-balancers

Percebendo DoS

- O que costuma ser monitorado ?
  - Banda
  - Estado do link (up/down)
  - Serviço funciona (sim/não)
- O que esses índices mostram durante DoS ?
  - Banda pode estar muito abaixo, muito acima ou normal
  - Link pode parecer down (BGP down ou falta de keepalive)
  - Estado dos serviços pode parecer funcional internamente

Percebendo DoS

- O que monitorar ?
  - Bytes/s, pacotes/s (rede) e requisições/s (máquinas)
  - Perdas
  - Flows
  - Distribuição de IP origem
  - Distribuição de tamanho de pacote
  - Relações quantitativas ICMP/IP, TCP-SYN/TCP, Frag/IP
  - Conexões em SYN_RECEIVED

Percebendo DoS

- Alguns indícios de DoS
  - Variações abruptas de quantidades: flows/s, pacotes/s, requisições/s
  - Excesso de conexões em SYN_REC
  - Distorções de distribuição (IP origem, tamanho de pacotes, fragmentos, ICMP, TCP-SYN)
- Gotchas:
  - Falhas naturais podem gerar os mesmos sintomas
  - Estatísticas podem ficar indisponíveis
  - Falsos positivos (meia-noite, sábado 14h etc.)

Reagindo a DoS

- Caracterize o ataque:
  - Alvo(s) e vítima(s) do ataque
  - Caminho(s) de onde vem o ataque
  - Tipo de ataque
- Ferramentas
  - Gráficos de tráfego, pacotes, CPU
  - show interface, netstat -an
  - access-lists/firewall-filters
- Defina então a tática a seguir e recursos alocados

Reagindo a DoS

- “Erguer Escudos”
  - Filtro bloqueando ICMPs ou Fragmentos (alerta: tratamento de fragmentos)
  - Filtro privilegiando IPs origem (pode gerar algumas reclamações...)
  - Rate-limit de SYNs, e/ou faixas de IP (se o roteador aguentar...)
  - TCP-Intercept (depende de flow-state)

Reagindo a DoS

- “Manobras Evasivas”
  - Mudar o IP do alvo e propagar o DNS
  - Anunciar rotas mais específicas
  - Mudar communities em anúncios de rotas
  - Desabilitar seletivamente alguns links
- “Abra um Canal”
  - Contacte o peer ou upstream por canais pré-combinados de resposta “clueful” e ágil
  - Conheça as políticas de tempo de resposta e colocação de filtros de cada rede

Melhorando a resistência a DoS

- Seguir princípios de hierarquia de redes
- Utilizar recursos com folga da capacidade máxima
- Bloquear pacotes endereçados a elementos de rede diretamente nas bordas
- Limitar quantidades de pacotes típicas de ataques (ICMP, TCP SYN, Fragmentos)
- Melhorar performance de bloqueio e log de roteadores e firewalls (ex: Syslog x NetFlow)

Melhorando a resistência a DoS

- Filtrar pacotes vindos de IPs não listados na tabela de roteamento global
  - ip verify unicast source reachable-via any (IOS)
- Utilizar dispositivos de camada 4-7 na frente de servidores (ArrowPoint, Alteon, Foundry, TopLayer)
- Utilizar stacks TCP/IP com priorização de conexões estabelecidas versus embrionárias (Solaris 7+, FreeBSD 3+, Linux 2.4+?)

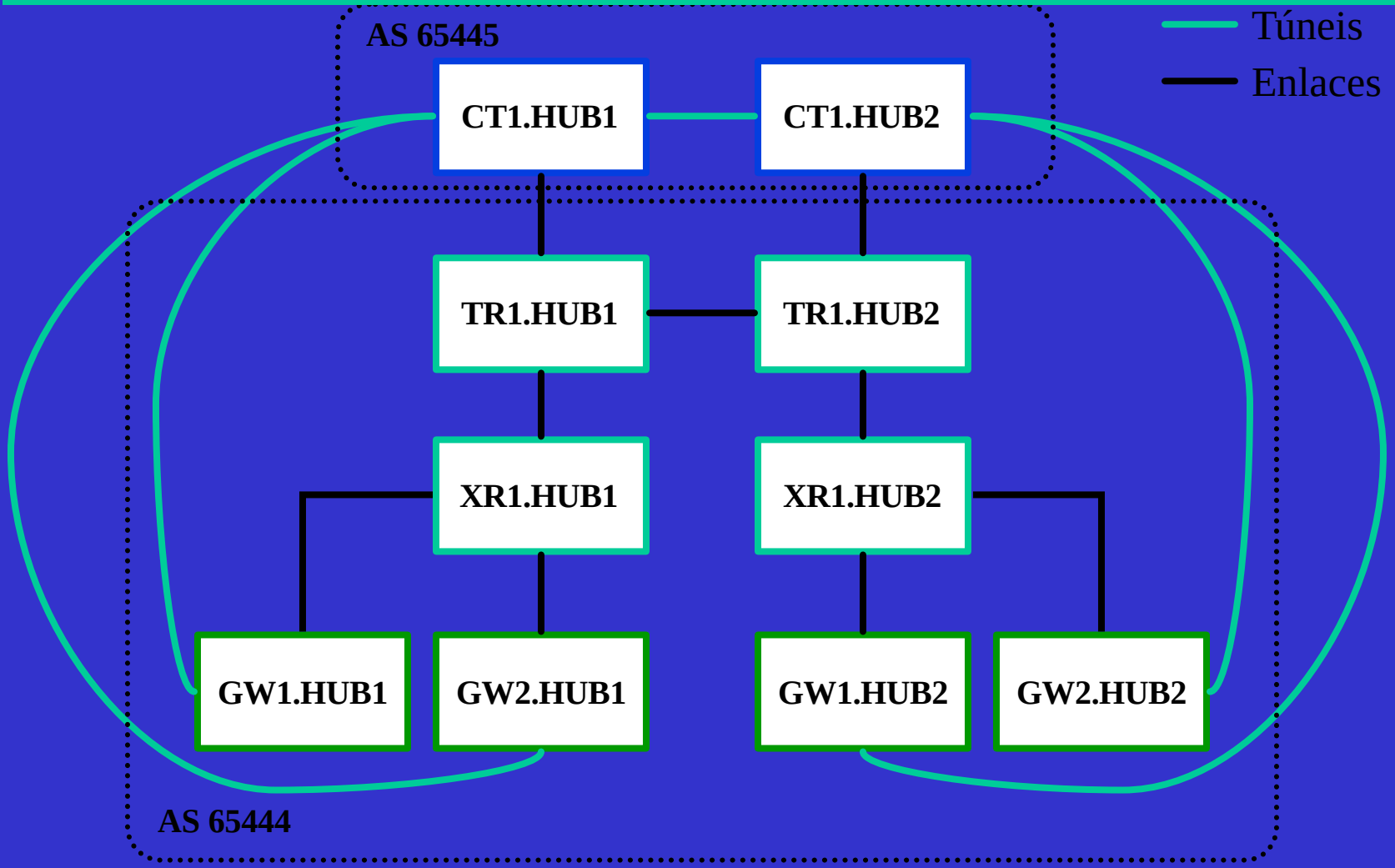
Evitando ser fonte de DoS

- Filtrar spoofing (RFC 2827) em todos os caminhos de roteamento simétrico
  - ip verify unicast reverse-path (IOS)
  - access-list/firewall-filter com os IPs designados
- Bloqueio de tráfego de saída desnecessário (filtragem costuma focar apenas entrada)
- Desabilitar directed-broadcast
- Zelo na segurança de máquinas para evitar implantação de zumbis

Rastreando DoS em backbones

- Checar vazões (pacotes e bytes/s) nos links (BGP principalmente) procurando o aumento já detectado na interface vítima
- ACLs como contadores nas interfaces
- Registros de Flows
- CenterTrack – Túneis IP (ou MPLS) para roteadores de inspeção

CenterTrack



Evoluções Tecnológicas

- Estratégia de IDS aplicada à DoS
  - Utilização de métricas (NetFlow, probes passivos, probes ativos) para detectar DoS, com eventual automação de reação
  - Soluções ainda em desenvolvimento/maturação
- ICMP Traceback, Traceback with Intention, Pushback
  - Dependem de grandes alterações em roteadores

Referências

- Mãe de todos os links sobre DoS:
  http://www.denialinfo.com/
  (Inclui RFC 2827 e Cisco IOS Essentials)
- Minimizing the Effects of DoS Attacks
  http://www.juniper.net/techcenter/app_note/350001.html
- Denial of Service Attacks
  http://www.nanog.org/mtg-0002/bellovin.html
  (Inclui ICMP Traceback)

Referências

- CenterTrack: An IP Overlay Network for Tracking DoS Floods
  http://www.nanog.org/mtg-9910/robert.html
- Security Attacks and Detection on OC-12 and Above Backbones
  http://www.nanog.org/mtg-9905/jiang.html
- Inferring Denial-of-Service activity
  http://www.cs.ucsd.edu/~savage/papers/UsenixSec01.pdf