Firewall

Dicas e Boas Práticas

by Rogerio Bastos
CERT.Bahia

Quem somos

É responsável pela conexão das instituições baianas à rede acadêmica Brasileira (Rede Ipê) e operação da Rede Metropolitana de Salvador (Remessa).

Coordenação de Segurança da Informação e Comunicações da STI/UFBA, responsável pela ETIR da Universidade Federal da Bahia.

É um CSIRT de coordenação para as instituições clientes do PoP-BA/RNP e parceiras da Remessa.


EnSI
VII Encontro de Segurança em Informática
do CERT.Bahia
REALIZAÇÃO:
CERT B@hia
CO-PROMOÇÃO:
Safer net
PATROCÍNIO:
cgi.br
PROEXT
APOIO:
RNP

Firewall

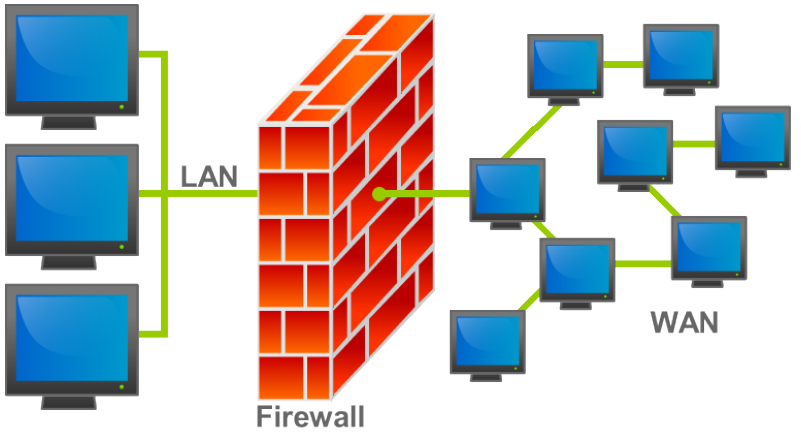
- É um sistema de segurança de rede que monitora e controla o tráfego baseado em regras de segurança.

- Normalmente é utilizado como primeira linha de defesa de uma rede.

Firewall

- **Firewall de Host** – controla o tráfego de rede que entra e sai somente do dispositivo em que é executado.

- **Firewall de Rede** – controla o tráfego entre duas ou mais redes.



Firewall

- A configuração adequada das regras do firewall não é uma tarefa simples, pois as recomendações e boas práticas estão espalhadas em diversos documentos e RFCs, e implicitamente na definição dos protocolos.

- Além disso, faz-se necessário conhecer as técnicas de ataques utilizadas contra as redes e aplicações.

Recomendações Gerais

- Bloquei tudo e permita apenas o que é necessário, inclusive o tráfego que sai da sua rede.

- É mais fácil liberar o tráfego legítimo do que bloquear o tráfego malicioso.

- Exemplo:
  - iptables -P INPUT DROP
  - iptables -P OUTPUT DROP
  - iptables -P FORWARD DROP

Recomendações Gerais

- Defina um padrão para os objetos e regras do firewall.
- Adicione o tempo de validade das regras temporárias usando comentários.
- Revise as regras de firewall periodicamente, pelo menos duas vezes por ano.
- Tenha backup e controle de versão das regras.

Recomendações Gerais

- Evite regras que utilizam objetos que geram consultas DNS.

- A ordem das regras altera o resultado. Coloque regras mais específicas primeiro.

- [BAD] Exemplo:
  - iptables -A INPUT -i eth0 -j DROP
  - iptables -A INPUT -s 192.0.2.0.1 -j ACCEPT

NAT

- O uso de NAT deve ser considerado como uma forma de roteamento e não como um mecanismo de proteção.

- Prevenir que um host externo inicie uma conexão com um host atrás do firewall pode ser feito com regras de firewall de forma mais eficiente.

- Caso utilize o recurso de NAT, deve haver registro das traduções de endereço.

Logging

- Habilite o log das regras e monitore esses logs.

- Exemplo:
  - iptables -A INPUT -d 192.0.2.1 -j LOG
    --log-prefix "FIREWALL 39 -- ACCEPT "
  - iptables -A INPUT -d 192.0.2.1 -j ACCEPT

Logging (NAT)

- Logging de NAT no IPTables/Netfilter
  - https://github.com/italovalcy/nfct-snatlog
- Logging de NAT no PFSense/PF
  - https://github.com/italovalcy/pfnattrack
- Exemplo:

```
2016-06-19,21:44:34 proto=6 osrc=192.168.100.105:51496 tsrc=192.168.25.4:2474
odst=192.168.25.7:22 tdst=192.168.25.7:22 duration=117

2016-06-19,22:07:05 proto=17 osrc=192.168.100.105:37205 tsrc=192.168.25.4:22834
odst=8.8.8.8:53 tdst=8.8.8.8:53 duration=30
```

IPv6

- Instituições que não utilizam IPv6 devem bloquear todo tipo de tráfego IPv6, nativo ou tunelado (6-to-4, 4-to-6, Teredo, ISATAP, etc).
- Para realizar testes, libere somente para um segmento de rede específico, ou crie uma rede específica para fazer o teste.
- Caso utilize IPv6, devem haver regras de firewall equivalentes para IPv4 e IPv6.

Endereços de Propósito Específico

- A RFC 6890 documenta os blocos de endereços IP de propósito especial.

- Ela define os endereços que não são válidos como origem ou destino.

- A RFC 8190 atualiza o documento anterior com pequenas correções.

Endereços de Propósito Específico

- Alguns endereços não são válidos quando utilizados na comunicação entre hosts.

- Pacotes utilizando esses endereços devem ser bloqueados em qualquer firewall (endpoint e perímetro).

Endereços de Propósito Específico

- 127.0.0.0/8 – Loopback (RFC 1122)
- 192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24 Documentação (RFC 5737)
- 240.0.0.0/4 – Reservado (RFC 1112)

- ::1/128 – Loopback (RFC 4291)
- 2001:db8::/32 – Documentação (RFC 3849)
- 2001:10::/28 – ORCHID (RFC 4843) [Expirado]

Endereços de Propósito Específico

- Alguns endereços não são válidos para uso na Internet.

- Pacotes utilizando esses endereços devem ser bloqueados em interfaces com IP público do firewall de perímetro.

Endereços de Propósito Específico

- 0.0.0.0/8 – (RFC 1122)
- 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
  Rede Local (RFC 1918)
- 100.64.0.0/10 – Carrier-Grade NAT (RFC 6598)
- 169.254.0.0/16 – Link-Local (RFC 3927)
- 192.0.0.0/29 – Dual-Stack Lite (RFC 6333)
- 198.18.0.0/15 – Benchmarking (RFC 2544)
- 255.255.255.255/32 – Broadcast (RFC 0919)

Endereços de Propósito Específico

- ::/128 – (RFC 4291)
- 100::/64 – Prefixo de descarte (RFC 6666)
- 2001::/32 – TEREDO (RFC 4380)
- 2001:2::/48 – Benchmarking (RFC 5180)
- fc00::/7 – Unique-Local (RFC 4193)
- ::ffff:0:0/96 – IPv4 mapeado em IPv6 (RFC 4291)
- fe80::/10 – Link-Local (RFC 4291)
  - Exceto fe80::/64 - Neighbour Discovery Protocol

Endereços de Propósito Específico

- Alguns endereços apesar de válidos para uso na Internet, podem ser bloqueados de acordo com a política da Instituição.

- Pacotes utilizando esses endereços podem ser bloqueados no firewall de perímetro.

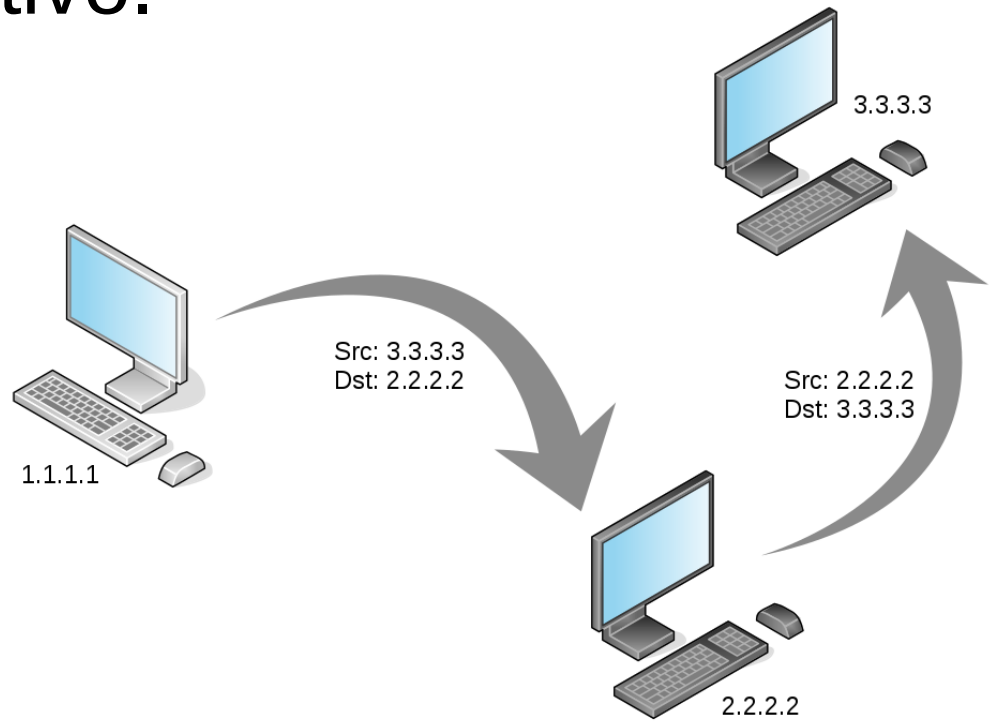
Endereços de Propósito Específico

- 192.88.99.0/24 – 6to4 Relay Anycast (RFC 3068)
- 224.0.0.0/4 – Multicast (RFC 5771)

- 64:ff9b::/96 – NAT64 (RFC 6052)
- 2002::/16 – 6to4 (RFC 3056)

Filtro Anti-Spoofing

- IP Spoofing é o uso de endereço IP falso para esconder a identidade ou personificar outro dispositivo.



Filtro Anti-Spoofing

- Nas interfaces de rede interna do firewall, permitir apenas pacotes com endereço de origem no range da sub-rede.

- Exemplo:
  - iptables -I INPUT -i eth0 ! -s 192.0.2.0/24 -j DROP
  - iptables -I FORWARD -i eth0 ! -s 192.0.2.0/24 -j DROP

- Permitir pacotes de DHCP com endereço de origem 0.0.0.0, caso seja utilizado.

Filtro Anti-Spoofing

- Não é possível fazer filtro anti-spoofing na interface do firewall com a Internet.

- A RFC 2827 (ou BCP 38) recomenda a aplicação de filtro para bloquear a saída de pacotes da sua rede com endereço falso (Ingress Filtering).

- Também pode ser implementado no roteador de borda utilizando o firewall do roteador ou o protocolo uRPF.

Gerando Pacotes com Endereço Falso

- Hping
  - hping3 --icmp --spoof 203.0.113.1 192.0.2.1
  - hping3 --icmp --rand-source 192.0.2.1

Filtro de Pacotes ICMP

- Pacotes ICMP são normalmente utilizados para controle e diagnostico da rede.

- Também são gerados pelos dispositivos em situações de erros.

- Exemplo: um pacote ICMP é enviado ao host de origem quando um pacote não pode ser entregue ao endereço de destino devido a problema de MTU.

Filtro de Pacotes ICMP

- O ICMP não deve ser bloqueado completamente, mas alguns tipos de mensagem ICMP podem ser usados de forma maliciosa e devem ser filtrados.

- A RFC 5927 documenta alguns ataques utilizando ICMP, como por exemplo o uso do ICMP tipo 4 (source quench) para degradar conexões IPv4 e IPv6.

- A RFC 6918 documenta os tipos de ICMP que são considerados obsoletos.

Filtro de Pacotes ICMP

- O ping e traceroute são largamente usados para localização e troubleshooting, porém não são essenciais para a comunicação.

- O ICMP tipo 0 e tipo 8 são usados para ping e o tipo 11 para traceroute.

- Caso não queira revelar a localização dos hosts via ICMP, pode-se bloquear esses três tipos de pacotes ICMP.

Filtro de Pacotes ICMP

Tipo	Descrição	Ação
0	Echo Reply	Permitir
3	Destination Unreachable	Permitir
8	Echo Request	Permitir
11	Time Exceeded	Permitir
Outros		Bloquear

Gerando Pacotes ICMP

- Hping
  - hping3 --icmp --icmptype 8 --icmpcode 0 192.0.2.1
  - hping3 --icmp --icmptype 0 --icmpcode 0 192.0.2.1

Filtro de Pacotes ICMP

- iptables -I INPUT -i eth0 -m icmp -p icmp --icmp-type 0 -j ACCEPT
- iptables -I INPUT -i eth0 -m icmp -p icmp --icmp-type 3 -j ACCEPT
- iptables -I INPUT -i eth0 -m icmp -p icmp --icmp-type 8 -j ACCEPT
- iptables -I INPUT -i eth0 -m icmp -p icmp --icmp-type 11 -j ACCEPT
- iptables -I INPUT -i eth0 -m icmp -p icmp -j DROP

Filtro de Pacotes ICMPv6

- ICMPv6 é essencial para o funcionamento do IPv6. Funções como descoberta de vizinhos, autoconfiguração e multicast dependem dele.

- A RFC 4890 documenta recomendações de filtros para pacotes ICMPv6 para permitir mensagens que são essenciais para o funcionamento da rede e bloquear mensagens potencialmente perigosas.

- No Apêndice B da RFC 4890 há um exemplo de script de configurações de firewall para ICMPv6.

Filtro de Pacotes ICMPv6

- Os critérios de bloqueios a seguir são para pacotes que atravessam o firewall.

- Para tabela FORWARD do firewall de rede.

Filtro de Pacotes ICMPv6

- Pacotes ICMPv6 que NÃO DEVEM ser bloqueados.

- O bloqueio desses pacotes pode impedir ou impactar severamente alguns tipos de tráfego.

Filtro de Pacotes ICMPv6

- Pacotes que atravessam o firewall.

Tipo	Descrição	Ação
1	Destination Unreachable	Permitir
2	Packet Too Big	Permitir
3	Time Exceeded	Permitir
4	Parameter Problem	Permitir
128	Echo Request	* Permitir
129	Echo Response	* Permitir

* Necessário para o host ser alcançado a partir de túnel Teredo.

Filtro de Pacotes ICMPv6

- Pacotes ICMPv6 que NÃO DEVERIAM ser bloqueados, a menos que se tenha uma boa razão para fazer.

Filtro de Pacotes ICMPv6

- Pacotes que atravessam o firewall.

Tipo	Descrição	Ação
144	Home Agent Address Discovery Request	* Permitir
145	Home Agent Address Discovery Reply	* Permitir
146	Mobile Prefix Solicitation	* Permitir
147	Mobile Prefix Advertisement	* Permitir

* Necessário para suportar Mobile IPv6

Filtro de Pacotes ICMPv6

- Pacotes ICMPv6 que são descartados automaticamente, sem necessidade de regras.

- Alguns tipos ICMPv6 são válidos apenas com endereço de link-local e o firewall/router não encaminha (ou não deveria) para outras interfaces.

Filtro de Pacotes ICMPv6

- Mesmo que estas mensagens sejam enviadas com endereços non-link-local, elas são rejeitadas no host de destino (caso ele siga a RFC).

- O administrador pode criar regras de bloqueio para garantir que estes pacotes serão bloqueados.

Filtro de Pacotes ICMPv6

- Pacotes que atravessam o firewall.

Tipo	Descrição	Ação
133, 134, 135, 136, 137, 141, 142	Address Configuration and Router Selection	Descartar
130, 131, 132, 143	Link-local Multicast Receiver Notification	Descartar
148, 149	SEND Certificate Path Notification	Descartar
151, 152, 153	Multicast Router Discovery	Descartar

Filtro de Pacotes ICMPv6

- Pacotes ICMPv6 que PODEM ser bloqueados de acordo com a política de Instituição.

Filtro de Pacotes ICMPv6

- Pacotes que atravessam o firewall.

Tipo	Descrição	Ação
150	Seamoby Experimental	Depende da Política
5-99, 102-126	Error messages not currently defined	Depende da Política
154-199, 202-254	Unallocated Informational messages	Depende da Política

Filtro de Pacotes ICMPv6

- Pacotes ICMPv6 que DEVEM ser bloqueados, a menos que se tenha uma boa razão para não fazer.

Filtro de Pacotes ICMPv6

- Pacotes que atravessam o firewall.

Tipo	Descrição	Ação
138	Router Renumbering	Bloquear
139, 140	Node Information	Bloquear
100, 101, 200, 201	Experimental Messages	Bloquear
127, 255	Reserved for expansion	Bloquear

Filtro de Pacotes ICMPv6

- Os critérios de bloqueios são para pacotes destinados à interface do firewall.

- Para os firewalls de endpoint e para tabela INPUT do firewall de rede.

Filtro de Pacotes ICMPv6

- Pacotes ICMPv6 que NÃO DEVEM ser bloqueados.

- O bloqueio desses pacotes pode impedir ou impactar severamente alguns tipos de tráfego.

Filtro de Pacotes ICMPv6

- Pacotes destinados à interface do firewall.

Tipo	Descrição	Ação
1	Destination Unreachable	Permitir
2	Packet Too Big	Permitir
3	Time Exceeded	Permitir
4	Parameter Problem	Permitir
128	Echo Request	* Permitir
129	Echo Response	* Permitir

* Necessário para o host ser alcançado a partir de túnel Teredo.

Filtro de Pacotes ICMPv6

- Pacotes destinados à interface do firewall.

Tipo	Descrição	Ação
133, 134, 135, 136, 141, 142	Address Configuration and Router Selection	Permitir
130, 131, 132, 143	Link-Local Multicast Receiver Notification	Permitir
148, 149	SEND Certificate Path Notification	Permitir
151, 152, 153	Multicast Router Discovery	Permitir

Filtro de Pacotes ICMPv6

- Pacotes ICMPv6 que são descartados automaticamente, sem necessidade de regras.

Filtro de Pacotes ICMPv6

- Pacotes destinados à interface do firewall.

Tipo	Descrição	Ação
138	Router Renumbering	Reque autenticado usando IPsec
144, 145, 146, 147	Mobile IPv6	Descartar
150	Seamoby Experimental	Descartar

Filtro de Pacotes ICMPv6

- Pacotes ICMPv6 que PODEM ser bloqueados de acordo com a política de Instituição.

Filtro de Pacotes ICMPv6

- Pacotes destinados à interface do firewall.

Tipo	Descrição	Ação
137	Redirect	Depende da Política
139, 140	Node Information	Depende da Política
5-99, 102-126	Error messages not currently defined	Depende da Política

Filtro de Pacotes ICMPv6

- Pacotes ICMPv6 que DEVEM ser bloqueados, a menos que se tenha uma boa razão para não fazer.

Filtro de Pacotes ICMPv6

- Pacotes destinados à interface do firewall.

Tipo	Descrição	Ação
100, 101, 200, 201	Experimental Messages	Bloquear
154-199, 202-254	Unallocated Informational messages	Bloquear
127, 255	Reserved for expansion	Bloquear

Gerando Pacotes ICMPv6

SI6 Networks' IPv6 Toolkit

https://www.si6networks.com/tools/ipv6toolkit/

- icmp6: A tool to perform attacks based on ICMPv6 error messages.
- na6: A tool to send arbitrary Neighbor Advertisement messages.
- ni6: A tool to send arbitrary ICMPv6 Node Information messages.
- ns6: A tool to send arbitrary Neighbor Solicitation messages.
- path6: A versatile IPv6-based traceroute tool.
- ra6: A tool to send arbitrary Router Advertisement messages.
- rd6: A tool to send arbitrary ICMPv6 Redirect messages.
- rs6: A tool to send arbitrary Router Solicitation messages.

Filtro de Pacotes ICMPv6

- ip6tables -I INPUT -i eth0 -m icmpv6 -p icmpv6
  --icmpv6-type 0 -j ACCEPT

- ip6tables -I INPUT -i eth0 -m ipv6-icmp -p ipv6-icmp
  --icmpv6-type 0 -j ACCEPT

Filtro de Tráfego Multicast

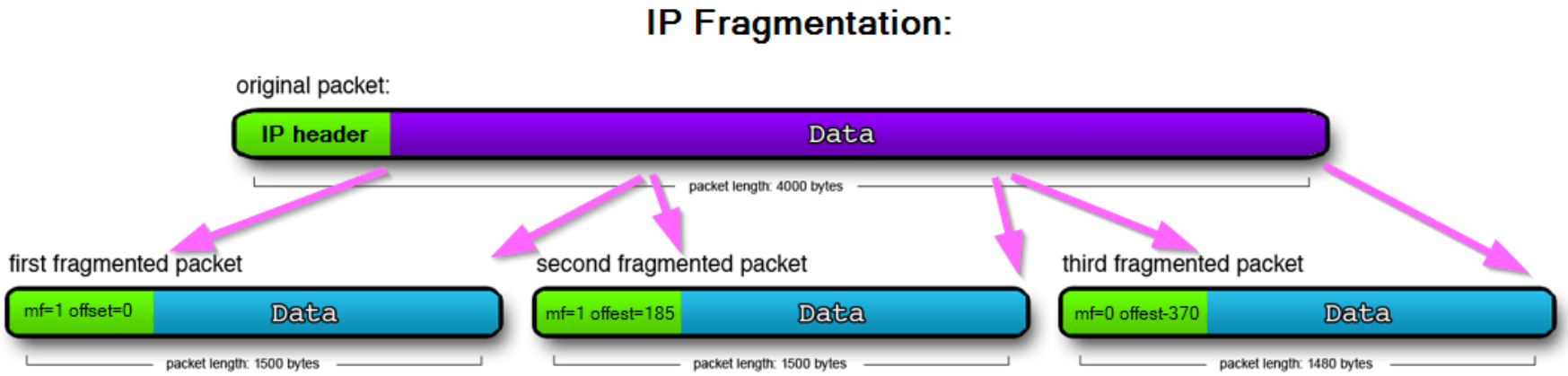
- O administrador deve analisar se e como sua rede pode ser alcançada via tráfego multicast.

- Dependendo da situação, é possível bloquear parcialmente ou completamente o tráfego multicast. Na maioria dos casos nenhum tráfego multicast externo é necessário para os serviços da rede.

- A RFC 2588 documenta possíveis problemas e medidas de controles que podem ser implementadas no firewall de perímetro.

Pacotes Fragmentados

- Recurso do protocolo IP que permite dividir um pacote em pacotes menores.



Pacotes Fragmentados

- Pode ser utilizado para ataques de DoS, aumentando o intervalo de transmissão ou o tamanho dos fragmentos.

- Pode passar despercebido pelo firewall ou pelo IDS, a depender do algoritmo de remontagem dos pacotes.

- Pode consumir recursos do firewall, caso ele faça a remontagem dos pacotes passantes.

Pacotes Fragmentados

- Qual o comportamento do seu firewall diante de pacotes fragmentados?
  - Descarta sem analisar
  - Encaminha sem analisar
  - Remonta o pacote para analisar
  - Have no idea!!!

Pacotes Fragmentados

Broken packets: IP fragmentation is flawed

18 Aug 2017 by Marek Majkowski.

As opposed to the public telephone network, the internet has a Packet Switched design. But just how big can these packets be?

CC BY 2.0 image by ajmexico, inspired by

https://blog.cloudflare.com/ip-fragmentation-is-broken/

Pacotes Fragmentados

- Overlapping Fragments é um ataque que explora uma falha no algoritmo de remontagem do pacote fragmentado para sobrescrever fragmentos enviados anteriormente.

- Pode ser usado para sobrescrever campos do cabeçalho TCP (e.g. porta).

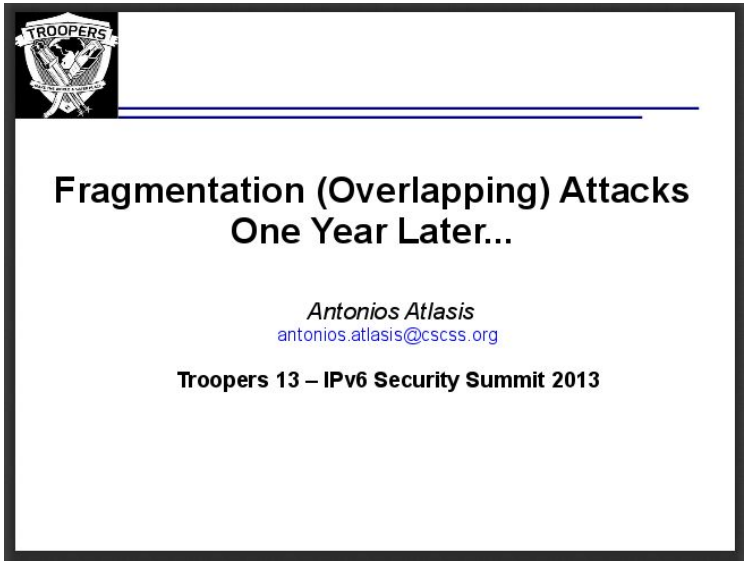
- Documentado nas RFC 1858 (IPv4) e RFC 5722 (IPv6).

Pacotes Fragmentados

- O firewall precisa checar a sanidade do offset dos fragmentos. [CUSTOSO]

- O host de destino pode descartar o pacote.

- Antonios Atlasis avalia o comportamento dos S.O.s em diferentes situações.



Pacotes Fragmentados

- Outro ataque utilizando fragmentação (Tiny Fragments) explora a especificação do IPv4, que permite que um fragmento IP seja tão pequeno que o cabeçalho TCP seja transportado no segundo fragmento.

- Pode ser usado para burlar filtros do firewall e assinaturas de IDS.

Pacotes Fragmentados

- O firewall deve descartar pacotes cujos cabeçalhos relevantes não estejam no primeiro fragmento, ou seja, fragmentos com menos de 16 bytes.

- No Linux, se o primeiro fragmento não tem o cabeçalho TCP, o pacote não casa com nenhuma regra que especifica porta.

Gerando Pacotes Fragmentados

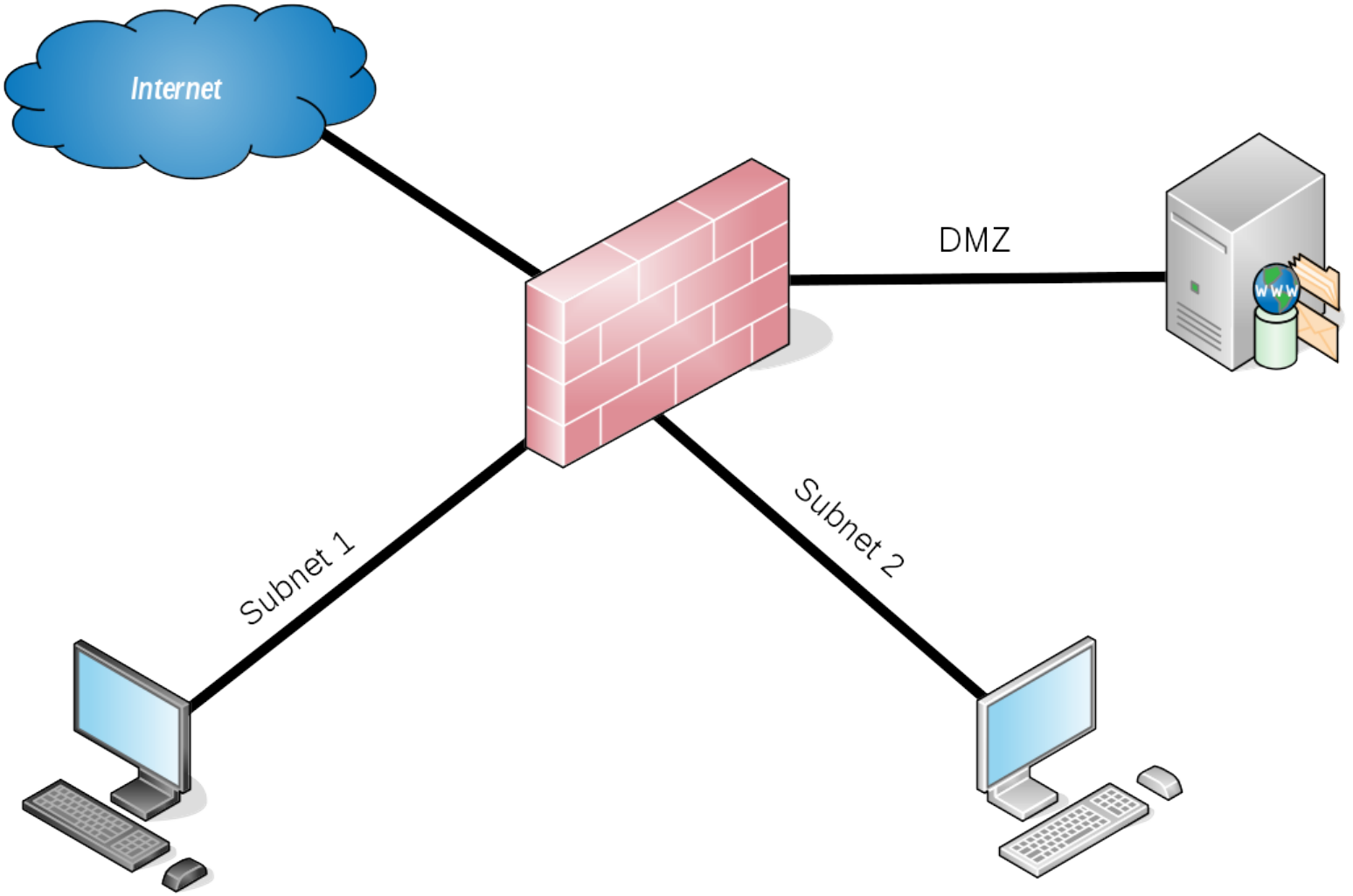
- ICMP
  - ping -s 5000 192.0.2.1
  - ping6 -s 5000 2001:db8::1
- DNSSEC
  - dig +notcp +dnssec DNSKEY org @199.19.56.1
  - dig +notcp +dnssec DNSKEY org @2001:500:f::1
- Hping
  - hping3 -S -p 80 --frag -d 1200 --mtu 15 192.0.2.1

Teste o Firewall

- Você não pode testar o firewall somente da rede interna.

- Realize testes em todas as interfaces do firewall e em todas as direções.

Teste o Firewall



Teste o Firewall

- Packet Generator
  - Hping
  - IPv6ToolKit (SI6 Networks)
  - Ftester (Inverse Path)
  - Scapy
- Performance
  - Iperf
- Port Scan
  - Nmap
  - Shodan.io
  - Censys.io
- Sniffer
  - Tcpdump
  - Wireshark

Última Recomendação

- O firewall não vai resolver todos os problemas de segurança.

Referências

Firewall Best Practices

Christian Winter
Advisor: Cornelius Diekmann
Seminar Future Internet SS2016
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: winterch@in.tum.de

ABSTRACT

With growing Internet usage in both private and commercial fields, filtering network traffic to prevent harmful use is gaining importance. But correctly filtering packets without restricting any wished functionality is complicated. New protocols are introduced and existing ones like ICMP and IP are updated. For each protocol, filtering rules have to be created separately. We summarize the most important best practices in firewall filtering for common protocols and give insights on why these filtering rules have to be applied. Additionally, we explain where information on creating individual policies can be found online and issues that need consideration are listed. The best practices summarized here are generic and can therefore be implemented for most firewall models. To give a concrete example, a filtering policy for a gateway firewall according to these generic best practices is given throughout this paper.

Keywords

Firewall, Best Practice, IP Filtering, ICMP Filtering, Packet Filtering

more it covers several aspects of the IP protocol family, like IPv6 extension headers and fragmentation, as well as attacks on those. Section 3 covers the dangers in the Internet Control Message Protocol (ICMP) in versions 4 and 6, lists possible attacks and gives recommendations which messages and types should be dropped in a firewall. Finally, Section 4 gives an outlook what else firewall administrators should consider, including IP tunnels, multicast messages, and other protocols. To give detailed filtering recommendations on some policy dependent best practices, this paper explains how a example firewall could be configured. We assume this firewall resides as a gateway between a local network and the Internet. Inside the protected network a web server should be reachable for HTTP requests from the Internet. This example will be used throughout the paper to show how filtering recommendations based on policies or services in the network could be implemented.

2 IP and Port Considerations

An often used method in packet filtering is deciding whether the packet may pass through the firewall or is dropped based

Referências

National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-41
Revision 1

Guidelines on Firewalls and Firewall Policy

Recommendations of the National Institute of Standards and Technology

Karen Scarfone
Paul Hoffman

Outras Referências

- RFC 7126 - Recommendations on Filtering of IPv4 Packets Containing IPv4 Options

- RFC 4942 - IPv6 Transition/Coexistence Security Considerations

- RFC 3511 - Benchmarking Methodology for Firewall Performance


“Eu não procuro saber as respostas, procuro compreender as perguntas.”
Confúcio