Segurança Informática e nas Organizações

Resumos
2016/2017

João Alegria | 68661

Capítulo 8

Firewalls

Uma *firewall* tem dois objetivos fundamentais:

1) Proteção por isolamento de máquinas ligadas à rede
2) Controlo de interações entre máquinas

Em ambos os casos as decisões tomadas por uma firewall são controladas por um conjunto de regras e aplicação que as interpretam e reagem em função do tráfego que chega à firewall.

A proteção por isolamento de uma máquina ligada à rede é atualmente um requisito critico, tanto para máquinas pessoais como organizacionais.

É uma vantagem, porque lhe permite usar serviços contactando outras máquinas ligadas direta ou indiretamente a essa rede. É também uma vantagem, porque lhe permite disponibilizar serviços a essas mesmas máquinas.

Mas é um risco, pois expõe vulnerabilidades da máquina que podem ser exploradas por atacantes.

É também um risco para outras máquinas, visto que a máquina pode ser usada para lançar ataques, o que pode acontecer independentemente da vontade dos seus utentes (por exemplo, após o comprometimento da mesma por uma ciberpraga).

Permite…	**Funcionalidades**
- Minimizar o impacto de vulnerabilidades locais - Facilitar a tomada de posições mais drásticas - Centralizar a deteção de problemas e o seu tratamento	- Supervisão de toda comunicação in <-> out - Controlo (uso dos recursos protegidos; uso da rede exterior pelas máquinas) - Defesa (contra ataques externos ao perímetro protegido; contra ataques iniciados no interior lançados para o exterior)
Limitações	
- Não resolvem o problema dos atacantes dentro da rede interna - Só são eficazes se controlarem totalmente as ligações ao exterior - São difíceis de administrar em ambientes com interesses heterogéneos (universidades)	

Uma firewall é um elo de ligação entre os sistemas computacionais (conjunto de redes e máquinas) que se pretende proteger, designado por perímetro protegido e as redes a que esse perímetro está ligado através da firewall.

É um elemento indispensável na ligação de máquinas pessoais e redes privadas a redes alheias potencialmente perigosas, nomeadamente a Internet.

A firewall é construída por diversas componentes funcionais, quer de hardware – máquinas, redes e equipamentos de interligação como hubs, switches, gateways, routers, etc – quer de software – aplicações específicas para filtrar, controlar e modificar fluxos de comunicação. Ou seja, uma firewall não é uma máquina, mas sim uma infraestrutura, que isola um perímetro protegido de redes perigosas a que o mesmo se liga.

Tipos de Firewalls

Packet-Filters Filtro de Datagramas	- É um filtro que atua fundamentalmente ao nível da rede, nomeadamente ao nível da troca de datagramas IP. Estes filtros normalmente limitam-se a aceitar ou rejeitar a passagem de um datagrama pela firewall, no âmbito do seu encaminhamento através da mesma. - Rejeitam interacções não autorizadas segundo o conteúdo dos pacotes IP (endereços IP, através das opções de cabeçalho, dimensão dos datagramas) - Podem registar fluxos informação ou conteúdo do tráfego - É transparente para as aplicações responsáveis pelos fluxos que avalia
Application-Level Gateways Filtro Aplicacional	- As firewalls do tipo "filtro aplicacional" operam ao nível do protocolo aplicacional. A sua função é dividir a parte ou a totalidade das interações aplicacionais entre interlocutores remotos, localizados em redes inteligentes pela firewall, de forma a controlar a execução desse mesmo protocolo. Por isso, as firewalls deste tipo são normalmente concretizadas usando um conjunto de aplicações designadas como *proxies* que executam em máquinas firewall. Para cada protocolo aplicacional é preciso que exista um mediador próprio, ao contrário dos filtros de datagramas. - Controlam interações ao nível da aplicação - Existe normalmente uma firewall diferente por protocolo - Protocolo proxy (controlo de acessos por utilizador, análise e alterações de conteúdos) - Focam-se na troca de dados aplicacionais e trabalham com conteúdos enviados de um lado para o outro - Não é aplicado filtros aos pacotes, só filtros aos fluxos
Circuit Gateways Filtro de Circuitos	- As firewalls do tipo "filtro de circuitos" controlam o estabelecimento de circuitos de formas não acessíveis aos filtros de datagramas, mas sem interferir de forma alguma com o protocolo aplicacional. - Podem registar fluxos informação ou conteúdo do tráfego - Detém facilmente conteúdos perigosos em fluxos de dados aplicacionais específicos - Obriga a que existam múltiplas aplicações, uma para cada tipo de tráfego aplicacional - Exemplo: Redigir o estabelecimento de ligações TCP - Exemplo: Autorizar ou não o estabelecimento de um circuito virtual após autenticação do requerente
Stateful Packet Filter	- Realizam Stateful Packet Inspection que analisa pacotes completamente incluindo o seu contexto, determinando e caracterizando a aplicação em causa e aplicam regras de filtragem/limitação. - Essa filtragem é feita a partir dos pacotes de IP.

Bastião

Deve executar versões seguras de sistemas operativos com uma configuração segura tendo instalados apenas os serviços considerados essenciais como Proxy de Telnet, DNS, FTP, SMTP e autenticação.
Em geral é uma plataforma para *application-level gateways* mas quanto mais *proxies* houverem no bastião, menor será o seu desempenho. Os *proxies* podem ser executados em *appliances* específicas. O bastião apenas encaminha tráfego para as *appliances* apropriadas. Este executa os *application-level gateways* de forma segura, ou seja, independente do comprometimento de um não afeta os restantes e sem privilégios especiais em que o seu comprometimento não permite afetar a máquina.
Os servidores públicos não devem ser colocados num bastião, como por exemplo: DNS, SMTP, HTTP, FTP, SSH, RAS, etc. Devem executar em máquinas dentro de DMZs. Assim, o bastião apenas encaminha tráfego para a máquina apropriada dentro de uma DMZ.

- Estação bastião é uma máquina segura instalada num ponto crítico da rede, onde executa um sistema operacional estável e seguro e um conjunto mínimo, seguro e controlado de serviços. Pode ser plataforma para Firewalls gateways de aplicação ou a nível de circuito.
- Gateway exposto a ataques, ou seja, não protegido por um filtro (normalmente o OUT)

Topologia Dual-Homed

Arquitetura	Vantagens
Uma única máquina - gateway bastião 	- Simplicidade - Economia de recursos
	Problemas / Desvantagens
	- O comprometimento da máquina desativa a firewall - A carga de processamento da firewall está toda sobre uma única máquina - Os serviços públicos estão dentro da rede protegida

Serviços de Segurança

Autorização	- De fluxo de dados (Packet Filtering) - De utentes (App-Level / Circuit-Level)
Redirecionamento de Tráfego	- Para máquinas dedicadas (mail, www, ftp) - Proxying (explícito ou transporte)
Processamento de Conteúdos	- Alteração de conteúdos (alteração de protocolos de alto nível) - Análise de conteúdos
Comunicação Segurança	- VPN (cifra e controlo de integridade de fluxos de dados sobre redes públicas (inseguras)) - Encapsulamento (IPsec Tunneling)
Defesa contra Tentativas de DoS	- Deteção de ataques - Filtragem de datagramas perigosos

Firewalls Pessoais

As firewalls pessoais não são mais do que firewalls que se destinam a proteger uma única maquina e fazem parte do sistema da mesma.
Uma firewall pessoal normalmente é um sistema de software que executa na mesma máquina que se quer proteger, ou seja, a firewall e o perímetro protegido são exatamente a mesma máquina.
As firewalls pessoais distinguem-se também das demais por permitirem controlar quais as aplicações locais capazes de efectuar determinadas interações com o exterior. Este controlo é importante para detetar acessos ilegítimos à rede exterior.

- Permite controlar aspetos interessantes que são impossíveis para as demais em que as aplicações estão ou não autorizadas a efetuar determinada comunicação.
- Permite minimizar o comprometido de máquinas alheias no mesmo perímetro de segurança.
- Tem a capacidade de controlar o tráfego de aplicações concretas.
- É uma firewall que atual tipicamente como Filtro Aplicacional (Application Gateway) e Filtro de Pacotes (Packet Filter)
- São arquiteturalmente mais simples. Não existe filtro interior nem DMZ, o perímetro protegido confunde-se com o gateway e o filtro exterior a existir, é providenciado por quem fornece a ligação à rede.

• ***Problemas***

Nem todos os utentes são especialistas em segurança em redes, pois não sabem nada de protocolos de comunicação e não sabem também como devem forçar um nível de privilégio mínimo. A variedade de interações remotas leva a um grande número de regras onde existem ambientes de trabalho distintos, onde existem diferentes requisitos de segurança, tratamento uniforme / diferenciado de múltiplas interfaces de rede e onde a confusão e as incoerências são vulnerabilidades difíceis de detetar.

Componentes

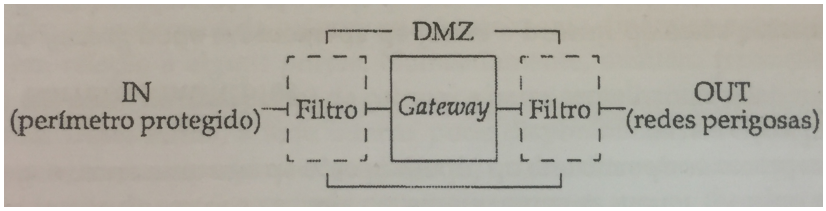
Uma firewall é formada por um gateway, dois filtros e uma rede de interligação de todas estas componentes, denominada por DMZ - zona desmilitarizada.

- A gateway é constituída por uma ou mais máquinas cuja função é controlar e encaminhar corretamente a comunicação IN-OUT, ou seja, entre o perímetro protegido e as redes perigosas exteriores.
- Os filtros destinam-se a fazer alguma filtragem do tráfego autorizado a passar através da firewall e, mais importante, impedir que o gateway possa ser contactado diretamente por outras máquinas, tanto da zona IN como da OUT.

DMZ - Zona Desmilitarizada

A DMZ é a rede inerente à firewall, ou seja, a rede que estabelece a ligação entre os filtros e a gateway. A DMZ, como o seu nome sugere, uma “zona de ninguém”, não pode ser considerada uma rede do perímetro protegido porque parte das suas componentes podem ser comprometidas; e não é uma rede exterior porque é controlada pela organização que se pretende defender com a firewall.

- Porção de rede onde se colocam máquinas que são expostas a tráfego perigoso do exterior
- Porção de rede onde não existem máquinas endereçáveis a partir do exterior



Tradução de Endereços (NAT)

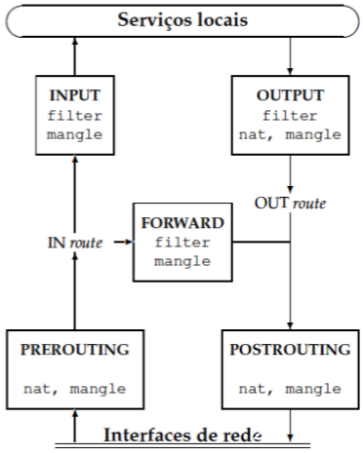
O NAT tem duplo objetivo: (i) simplificar a gestão de endereços das redes internas ligadas à Internet através da gateway; e (ii) impedir um endereçamento *ad hoc* de máquinas internas originado na rede externa.

Caso de Estudo: iptables

- O *iptable* é um filtro de pacotes integrado com uma cadeira de processamento de pacotes IP dentro do sistema operativo Linux. Passível de estendido de várias maneiras: em módulos do sistema operativo e, aplicações em modo utilizador.
- As firewalls *iptables* aceitam, rejeitam ou alteram pacotes que fluem através de uma máquina - firewall do tipo Packet Filter.
- Servem para controlar o tráfego que entra e sai de uma máquina.
- O *iptable* usa um conceito de cadeias (chains) para analisar datagramas. Uma cadeia é uma sequência de regras e cada regra possui zero ou mais condições de aplicabilidade e uma decisão.

O *iptables* possui cinco cadeias padrão:

- INPUT - aplica-se a datagramas recebidos pela máquina e que lhe são dirigidos
- OUTPUT - aplica-se a datagramas enviados pela máquina e com origem na mesma
- FORWARD - aplica-se a datagramas recebidos pela máquina mas que não lhe são dirigidos, ou seja, que passam em transito pela máquina que faz o seu encaminhamento
- PREROUTING - aplica-se a todos os datagramas recebidos pela máquina
- POSROUTING - aplica-se a todos os datagramas enviados pela máquina



O *iptables* usa tabelas para subdividir a aplicação de regras em cada cadeia para agrupar modelos de operação e dependem do modo como o *iptables* foi criado e instalado.
Existem três tabelas base:

- filter - existe sempre por omissão e serve para filtrar datagramas, ou seja, para decidir apenas sobre a sua aceitação ou rejeição
- nat - serve para detetar e atuar em situações em que seja necessário fazer NAT
- mangle - serve para efetuar diversos tipos de alterações nos datagramas

A decisão (target) expressa por cada regra é uma decisão-padrão ou o nome de outra cadeira, porque a decisão deverá ser tomada pelas regras dessa cadeia.
As decisões base são:

ACCEPT - indica que o datagrama deve ser aceite
DROP - datagrama deve ser descartado
QUEUE - o datagrama deve ser enviado para uma fila de espera destinada a uma aplicação local
RETURN - indica que a cadeia atual deve ser abandonada e retomada a análise de regras na regra seguinte da cadeia anterior)

Vantagens	Desvantagens
- O facto de ser um produto comparável em eficácia as demais firewalls comerciais, - Ser apenas o núcleo de uma arquitetura mais complexa e extensível - Ser relativamente estável, confiável e escalável - Ser económico em termos de recursos computacionais necessários	- O facto de se ter de perceber bem como funciona a interação entre o núcleo LINUX, o *iptables* e diversos outros módulos que interagem com os dois anteriores. - Não ser uma solução “chave na mão” - Falta de ferramentas gráficas adequadas aos administradores menos habituados à administração de máquinas LINUX