

Firewalls

1. O que é um firewall de acordo com Cheswick & Bellovin?

- a) Uma barreira física que protege o hardware de uma rede.
- (b)** Um link entre redes que protege um perímetro seguro de uma rede insegura como a Internet.
- c) Um software que protege contra vírus e malware.
- d) Um protocolo de comunicação que assegura a transmissão de dados.

2. Qual das seguintes afirmações melhor descreve a implementação centralizada de políticas de segurança de um firewall?

- a) Maximiza o impacto de vulnerabilidades locais.
- b) Facilita a adoção de posições mais flexíveis em relação à segurança.
- (c)** Centraliza a detecção de problemas e o seu tratamento.
- d) Torna mais difícil a gestão de políticas de segurança.

3. Quais são as funcionalidades de um firewall? (Escolha duas)

- (a)** Supervisionar toda a comunicação dentro e fora da rede.
- b) Armazenamento de dados de tráfego para análise futura.
- (c)** Ativação de mecanismos de gateway para ocultar a estrutura do perímetro protegido.
- d) Conexão direta entre servidores internos e externos sem restrições.

4. Qual é a importância dos firewalls, conforme descrito no slide 5?

- a) Desnecessária, já que os ataques a sistemas públicos são raros.
- (b)** Extrema, devido à constância dos ataques a sistemas públicos.
- c) Baixa, pois os sistemas operacionais modernos são inherentemente seguros.
- d) Média, apenas sistemas desatualizados necessitam de firewalls.

5. O que é uma DMZ em relação à segurança de redes?

- a) Uma zona de rede altamente segura que contém os dados mais críticos.
- (b)** Uma rede desmilitarizada que contém servidores expostos ao mundo.
- c) Uma nova tecnologia de firewall que desativa automaticamente ataques de DoS.
- d) Um tipo de software de firewall personalizado para usuários domésticos.

6. Qual é a função principal de um packet filter segundo os slides?

- a) Analisar e filtrar o tráfego baseado nos endereços de IP de origem e destino.
- b) Gerenciar políticas de controle de acesso de usuários e dispositivos.
- c) Proteger contra softwares maliciosos e ataques de phishing.
- d) Regular o tamanho e a fragmentação dos pacotes de dados.

7. O que caracteriza os firewalls do tipo "stateful packet filters"?

- a) Filtragem de conteúdo baseada em estados pré-definidos.
- b) Filtragem de pacotes de dados com consideração do contexto ou histórico.
- c) Controle de tráfego através de um conjunto fixo de regras imutáveis.
- d) Análise de pacotes em tempo real sem retenção de informações de estado.

8. Como a DMZ é protegida em uma configuração de firewall típica?

- a) Por um único firewall altamente restritivo.
- b) Pelo sistema operacional do servidor que hospeda a DMZ.
- c) Por um sistema de dois firewalls com regras distintas.
- d) Por uma única camada de segurança aplicada externamente.

9. O que é um "Bastion" em termos de segurança de rede?

- a) Um servidor que executa versões seguras de sistemas operacionais e serviços essenciais.
- b) Uma aplicação específica que detecta e bloqueia automaticamente ataques de DoS.
- c) Um protocolo de comunicação que criptografa dados entre redes.
- d) Um dispositivo que se conecta diretamente aos servidores públicos sem nenhuma proteção.

10. Qual dos seguintes não é uma limitação comum dos firewalls, como mencionado nos slides?

- a) Incapacidade de controlar interações disfarçadas ou ocultas.
- b) Dificuldade de gerir em ambientes com interesses heterogéneos.
- c) Falta de eficiência no controlo de todas as conexões externas.
- d) Proteção automática contra todos os tipos de vírus e malwares.

11. O que é o iptables no contexto dos firewalls?

- a) Uma aplicação de firewall pessoal para sistemas operacionais não Linux.
- b) Uma ferramenta para a gestão de redes privadas virtuais (VPNs).

(c) Uma ferramenta integrada no kernel do Linux para filtragem de pacotes e NAT.

d) Um protocolo de segurança para autenticação e autorização de usuários.

12. Qual é o propósito dos firewalls pessoais?

a) Proteger exclusivamente as redes corporativas de ataques externos.

b) Permitir que os administradores de rede definam políticas de controle de acesso centralizadas.

(c) Fornecer uma camada de segurança adicional para hosts individuais/pessoais.

d) Substituir a necessidade de firewalls corporativos e soluções de segurança em profundidade.

13. Quais são as principais vantagens da utilização do fail2ban com iptables?

a) Acelerar o tráfego de rede e melhorar a performance do sistema.

(b) Prevenir ataques de força bruta e DoS ao monitorizar padrões de tráfego.

c) Facilitar a comunicação entre diferentes sub-redes dentro de uma organização.

d) Gerir automaticamente as atualizações de segurança para o sistema operacional Linux.

14. Como os firewalls aplicacionais (application gateways) diferem dos firewalls de filtragem de pacotes?

a) Os firewalls aplicacionais controlam o tráfego ao nível da rede, enquanto os de filtragem de pacotes operam ao nível da aplicação.

b) Os firewalls aplicacionais são menos seguros porque apenas filtram tráfego com base em endereços IP e portas.

(c) Os firewalls aplicacionais gerem o tráfego a nível aplicacional e podem analisar e modificar o conteúdo dos dados.

d) Os firewalls de filtragem de pacotes são mais fáceis de configurar e requerem menos manutenção regular.

15. O que é um "Bastion" no contexto da segurança da rede?

a) Um tipo de firewall pessoal utilizado para proteger redes domésticas.

(b) Um servidor seguro que executa versões seguras de sistemas operacionais e serviços essenciais.

c) Um método de autenticação utilizado por firewalls de filtragem de pacotes.

d) Uma ferramenta de monitoramento de rede utilizada para detetar atividades suspeitas.

16. Como o NAT (Network Address Translation) é utilizado em firewalls?

a) Para permitir a comunicação direta entre redes internas e externas sem restrições.

(b) Para mascarar os endereços IP internos de uma rede, substituindo-os por um único endereço IP externo.

- c) Como um mecanismo para bloquear todo o tráfego de entrada e saída de uma rede.
- d) Para detetar e prevenir ataques de phishing e malware.
17. Qual é a principal limitação dos firewalls que não conseguem controlar interações disfarçadas ou ocultas?
- a) Eles não são capazes de filtrar o tráfego de entrada com eficácia.
- b) Eles não podem gerir adequadamente o tráfego de saída para a Internet.
- c) Eles são ineficazes contra ataques que utilizam técnicas de tunelamento ou multiplexação.
- d) Eles não suportam a segmentação da rede interna em várias sub-redes.
18. O que é uma DMZ (DeMilitarized Zone) e qual a sua função em uma arquitetura de segurança de rede?
- a) Uma área segura da rede que contém dados críticos e não está acessível a partir da Internet.
- b) Uma área da rede que contém servidores expostos ao mundo e é usada para serviços específicos.
- c) Uma configuração de firewall pessoal para proteger dispositivos individuais.
- d) Um protocolo de segurança que protege a rede interna contra ataques de negação de serviço (DoS).
19. Qual é a principal função do proxy em um firewall aplicacional?
- a) Atuar como um intermediário entre o cliente e o servidor, controlando e potencialmente modificando o tráfego.
- b) Fornecer um ponto de acesso direto para todos os dispositivos numa rede.
- c) Gerir a transferência de arquivos dentro de uma rede interna.
- d) Monitorizar o tráfego de entrada sem intervir ou modificar os dados.
20. O que significa "fail2ban" no contexto de firewalls?
- a) Um protocolo para banir falhas de conexão persistentes.
- b) Um serviço que bloqueia IPs com base em comportamentos anômalos detectados nos logs.
- c) Uma ferramenta de VPN que falha ao tentar estabelecer conexões seguras.
- d) Um tipo de firewall que utiliza técnicas de inteligência artificial para prever ataques.
21. Quais são as características dos firewalls "stateful packet filters"?
- a) Filtragem dinâmica de pacotes com base no estado ou contexto da conexão.
- b) Capacidade de redirecionar tráfego sem inspecionar o estado dos pacotes.
- c) Implementação simplificada sem a necessidade de manter o estado dos pacotes.

d) Uso exclusivo de tabelas NAT estáticas sem adaptação ao tráfego observado.

22. Qual das seguintes opções é uma vantagem do uso de "bastion" em firewalls?

- a) Reduz a necessidade de outros mecanismos de segurança, como antivírus.
- b) Oferece um único ponto de autenticação e autorização para todos os serviços.
- c) Executa versões seguras de sistemas operacionais e serviços essenciais.
- d) Permite a comunicação direta entre redes internas e externas sem restrições.

23. Como o "iptables" é utilizado em um ambiente Linux?

- a) Como uma ferramenta de monitoramento de rede para detetar atividades suspeitas.
- b) Para realizar o balanceamento de carga entre servidores em uma rede.
- c) Para a filtragem de pacotes e a implementação de NAT no kernel do Linux.
- d) Como um serviço de VPN integrado ao sistema operacional.

24. Quais são os problemas associados ao uso de firewalls pessoais, como indicado nos slides?

- a) São complexos de operar devido a diferentes políticas para ambientes e interfaces de rede.
- b) Exigem conhecimento avançado em segurança de rede para a sua configuração inicial.
- c) Não oferecem proteção contra malware e vírus.
- d) Tendem a bloquear o tráfego interno legítimo, causando interrupções de serviço.

25. Qual é a função do NAT em um firewall?

- a) Bloquear todo o tráfego de entrada e saída de uma rede.
- b) Permitir que redes internas se comuniquem diretamente com a Internet.
- c) Mascara os endereços IP internos, substituindo-os por um endereço IP externo.
- d) Fornecer criptografia de ponta a ponta para comunicações de dados.

26. Qual dos seguintes não é uma limitação dos firewalls convencionais?

- a) Incapacidade de controlar tráfego multiplexado por VPNs.
- b) Dificuldade em gerir ambientes com interesses heterogéneos.
- c) Ineficácia contra atacantes que já estão dentro da rede interna.
- d) Proteção automática contra vazamento de informações.

27. Qual é o propósito de uma DMZ em uma configuração de rede?

- a) Isolar servidores públicos do resto da rede interna.

- b) Oferecer uma área segura para dados críticos e sensíveis.
- c) Funcionar como o único ponto de acesso para a Internet.
- d) Atuar como uma rede privada virtual para usuários remotos.

28. Como as VLANs são utilizadas em conjunto com firewalls?

- a) Para proporcionar criptografia de dados e anonimato na rede.
- (b)** Para segregar o tráfego de rede e melhorar a segurança geral.
- c) Como uma alternativa mais segura e eficiente aos firewalls.
- d) Para aumentar a velocidade da rede e a eficiência do tráfego.