Curso: T-ADS

Turma: 3º B - NOTURNO

Matéria: INTRODUÇÃO A REDES DE COMPUTADORES

Aluno: ARTHUR SILVA BERDUSCO DE SOUZA

ADO - 5: QUESTIONÁRIO DE REVISÃO

São Paulo

27 de outubro de 2023

1. Qual é o objetivo de uso do protocolo NAT?

- Resposta: O objetivo do Protocolo NAT (Network Address Translation) é permitir que vários dispositivos de uma rede local compartilhem um único endereço IP público para acessar a Internet.

2. Descreva como é o funcionamento do Protocolo NAT.

- Resposta: O NAT funciona traduzindo os endereços IP e números de porta dos dispositivos da rede local para um único endereço IP público. Quando os dispositivos internos enviam solicitações para a Internet, o NAT registra essas solicitações e cria uma tabela de mapeamento que associa as portas usadas internamente com o endereço IP público. As respostas da Internet são encaminhadas de volta com base nesse mapeamento, permitindo que os dispositivos internos recebam dados de volta.

3. Como ocorre o procedimento de um equipamento que necessita usar a Internet? Descreva cada etapa.

- Resposta:

1. O equipamento internamente emite uma solicitação para um servidor na Internet.

2. O dispositivo NAT registra a solicitação e cria uma entrada na tabela de mapeamento.

3. O NAT traduz o endereço IP e a porta do dispositivo interno para o endereço IP público do NAT e uma porta externa.

4. A solicitação é enviada para o servidor na Internet.

5. O servidor na Internet responde à porta externa do NAT.

6. O NAT consulta sua tabela de mapeamento para determinar a qual dispositivo interno a resposta deve ser encaminhada.

7. A resposta é encaminhada para o dispositivo interno apropriado.

4. Conforme sabemos, só temos um endereço público para ser utilizado pela rede interna. Caso aconteça de várias máquinas terem de acessar a Internet, o que vai acontecer?

- Resposta: Quando várias máquinas de uma rede interna precisam acessar a Internet, o NAT permite que todas compartilhem o mesmo endereço IP público. Isso é feito atribuindo portas externas únicas a cada conexão interna. O NAT mantém uma tabela de mapeamento para rastrear qual dispositivo interno está associado a cada porta externa, permitindo que as respostas da Internet sejam roteadas para os dispositivos apropriados.

5. Qual a função de utilizar o PAT (Tradução de Endereços de Porta)?

- Resposta: A função do PAT (Port Address Translation) é permitir que vários dispositivos de uma rede compartilhem o mesmo endereço IP público, traduzindo não apenas os endereços IP, mas também os números de porta. Isso torna possível para dispositivos múltiplos na rede interna se comunicarem com servidores externos usando um único endereço IP público, diferenciando-os pelas portas.

6. Como funciona o redirecionamento de porta, utilizado pelo Protocolo NAT?

- Resposta: O redirecionamento de porta, ou "port forwarding", permite que um dispositivo na rede interna seja acessível a partir da Internet. Funciona configurando o NAT para redirecionar solicitações que chegam a uma determinada porta externa para um dispositivo interno específico, com base na porta de destino. Isso permite a hospedagem de serviços, como servidores web ou jogos online, em dispositivos internos, tornando-os acessíveis a partir da Internet.

7. Qual a função do gateway?

- Resposta: A função do gateway é atuar como o ponto de entrada ou saída entre diferentes redes, encaminhando o tráfego de uma rede para outra. Em uma rede doméstica, o gateway é muitas vezes o roteador que conecta a rede local à Internet.

8. Um funcionário da empresa “A”, cuja rede é uma LAN, enviou um pacote com um convite diretamente para o equipamento de um amigo, que é funcionário na empresa “B”, em outra rede LAN. Analise a situação e descreva o que aconteceu. Justifique.

- Resposta: Se o funcionário da empresa "A" enviou um pacote diretamente para o equipamento de seu amigo na empresa "B", que está em outra rede LAN, é provável que o pacote tenha sido roteado pela Internet. O pacote deixou a rede LAN da empresa "A", passou pela Internet e entrou na rede LAN da empresa "B" por meio de roteadores. O sucesso da comunicação dependerá da configuração de roteamento, regras de firewall e configuração de gateway nas duas redes.

9. Qual a função do IP público que faz uso do “redirecionamento” de portas?

- Resposta: A função do IP público que faz uso do "redirecionamento" de portas é permitir que dispositivos internos sejam acessíveis a partir da Internet, direcionando o tráfego externo para portas específicas em dispositivos internos. Isso é comumente usado para hospedar serviços, como servidores web ou servidores de jogos, em dispositivos internos, tornando-os acessíveis a partir da Internet.

10. No que consiste realizar um roteamento?

- Realizar um roteamento envolve encaminhar pacotes de dados de uma rede para outra, tomando decisões com base nas informações do endereço de destino contidas nos pacotes. O roteamento determina a melhor rota para que os pacotes alcancem seu destino, considerando a topologia da rede e as tabelas de roteamento.

11. Qual a importância de realizar o roteamento?

- O roteamento é essencial para a comunicação eficiente e eficaz em redes, pois permite que os pacotes de dados sejam encaminhados de forma apropriada de uma

rede para outra. Isso é fundamental para conectar redes locais à Internet e garantir que o tráfego alcance seu destino de maneira rápida e confiável.

12. Defina o que é um roteador e qual a sua função?

- Um roteador é um dispositivo de rede que atua como um ponto de interconexão entre várias redes. Sua função principal é rotear pacotes de dados entre essas redes, determinando a rota mais adequada com base nos endereços de destino dos pacotes.

13. Cite as 3 funções de um roteador.

- As três funções de um roteador são:

1. Roteamento: Encaminhar pacotes de dados entre redes diferentes.

2. Encaminhamento: Tomar decisões

sobre a melhor rota para os pacotes com base em tabelas de roteamento.

3. Interface: Conectar redes locais e dispositivos à rede maior, incluindo a Internet.

14. Quando se realiza um roteamento, quais os dois itens necessários para que o roteamento aconteça?

- Para que o roteamento aconteça, são necessários dois itens:

1. Tabelas de roteamento que contêm informações sobre as redes e os caminhos disponíveis.

2. Um dispositivo de roteamento (roteador) que toma decisões de encaminhamento com base nas informações das tabelas de roteamento.

15. Quais os dois tipos de roteamento que foram apresentados? Defina cada um deles.

- Os dois tipos de roteamento apresentados são:

1. Roteamento de Vetor de Distância: Nesse tipo de roteamento, os roteadores trocam informações sobre suas tabelas de roteamento com os vizinhos e calculam a rota mais curta para as redes de destino com base em contagens de saltos.

2. Roteamento de Estado de Enlace: Nesse tipo de roteamento, os roteadores trocam informações detalhadas sobre a topologia da rede, incluindo o estado das conexões (enlaces), e calculam as rotas com base em métricas, como largura de banda disponível.

16. Como funciona o roteamento de Vetor de Distância?

- No roteamento de Vetor de Distância, os roteadores trocam informações sobre suas tabelas de roteamento com os roteadores vizinhos. Cada roteador mantém uma tabela que lista as redes de destino, a contagem de saltos (hops) para alcançá-las e o próximo salto (próximo roteador). O roteador atualiza suas tabelas com base nas informações recebidas dos vizinhos e escolhe a rota com a menor contagem de saltos para encaminhar pacotes.

17. Como funciona o roteamento de Estado de Enlace?

- No roteamento de Estado de Enlace, os roteadores trocam informações detalhadas sobre a topologia da rede, incluindo o estado das conexões (enlaces), largura de banda disponível e outras métricas. Com base nessas informações, os roteadores calculam as rotas mais eficientes para as redes de destino. Esse tipo de roteamento leva em consideração mais informações do que o roteamento de Vetor de Distância, o que o torna mais preciso em redes complexas.

18. Quais são os três motivos para termos diversos tipos de roteamento?

- Os três motivos para termos diversos tipos de roteamento são:

1. Adaptabilidade: Diferentes tipos de roteamento são mais adequados para diferentes cenários de rede, permitindo uma adaptação às necessidades específicas.

2. Escalabilidade: Alguns tipos de roteamento são mais escaláveis em redes grandes e complexas, enquanto outros são mais simples e adequados para redes menores.

3. Precisão: Roteamento de diferentes tipos oferece diferentes níveis de precisão na escolha das rotas, dependendo das informações disponíveis.

19. O que é um firewall e para o que serve?

- Um firewall é um dispositivo ou software de segurança que atua como uma barreira entre uma rede ou sistema de computador e a Internet ou outras redes. Sua função principal é monitorar e controlar o tráfego de entrada e saída, permitindo ou bloqueando pacotes com base em regras de segurança predefinidas, a fim de proteger a rede contra ameaças e acessos não autorizados.

20. Sabendo que o firewall é a primeira linha de defesa de uma rede, descreva o que o firewall utiliza para impedir o acesso de programas ou invasores mal-intencionados?

- O firewall utiliza várias técnicas para impedir o acesso de programas ou invasores mal-intencionados, incluindo:

- Regras de Firewall: Define regras que determinam quais tipos de tráfego são permitidos ou bloqueados com base em endereços IP, portas, protocolos e outros critérios.

- Inspeção de Pacotes: Examina o conteúdo dos pacotes de dados para identificar padrões de tráfego malicioso ou suspeito.

- Proxy: Age como intermediário entre os dispositivos internos e a Internet, mascarando os endereços IP internos e ocultando a topologia da rede.

- Filtros de Conteúdo: Bloqueia ou permite o acesso a sites ou conteúdo com base em categorias, palavras-chave ou URLs.

- Detecção de Intrusões: Monitora o tráfego em busca de atividades suspeitas ou padrões de ataque e responde de acordo.

21. Quais são as duas maneiras de utilizarmos um firewall?

- As duas maneiras de utilizar um firewall são:

1. Firewall de Hardware: É um dispositivo dedicado que age como uma barreira entre a rede interna e a Internet, proporcionando proteção em nível de rede.

2. Firewall de Software: É um programa instalado em um computador ou servidor que fornece proteção em nível de host ou aplicativo.

22. Cite os motivos em que um firewall não consegue proteger a rede.

- Um firewall pode não ser capaz de proteger a rede nas seguintes situações:

1. Ataques Internos: Quando as ameaças vêm de dentro da rede, como um funcionário mal-intencionado.

2. Ameaças Avançadas: Alguns ataques sofisticados podem contornar as medidas de segurança de um firewall.

3. Configuração Incorreta: Se o firewall não estiver configurado corretamente, ele pode permitir o tráfego indesejado.

4. Ataques de Engenharia Social: Quando os invasores enganam os usuários para obter acesso à rede.

23. Defina Firewall de Software.

- Um firewall de software é um programa de segurança que é instalado em um computador ou servidor e atua como uma barreira entre esse dispositivo e a rede externa. Ele monitora e controla o tráfego de rede do dispositivo, aplicando regras de segurança para proteger o sistema contra ameaças e acessos não autorizados.

24. Qual é a tecnologia de firewall que atua como intermediário entre um computador situado na LAN e uma rede externa?

- A tecnologia de firewall que atua como intermediário entre um computador situado na LAN e uma rede externa é conhecida como "Proxy Firewall".

25. Como funciona um Proxy Services?

- Um Proxy Service atua como intermediário entre um cliente e um servidor. Quando um cliente solicita recursos ou serviços de um servidor, o Proxy Service encaminha a solicitação em nome do cliente e, em seguida, encaminha a resposta do servidor de volta ao cliente. Isso permite o controle de acesso, o cache de conteúdo e a anonimização das solicitações do cliente.

26. Qual é a tecnologia de firewall, moderna, de terceira geração que pode ser implementada em hardware ou software? Como ela funciona?

- A tecnologia de firewall moderna de terceira geração é conhecida como "Firewall de Próxima Geração" (Next-Generation Firewall - NGFW). Ela combina as funcionalidades de um firewall tradicional com recursos avançados, como inspeção profunda de pacotes, prevenção de intrusões, filtragem de aplicativos e controle de aplicativos. Pode ser implementada em hardware ou software para proteger redes contra ameaças avançadas.

27. Quais os tipos de serviços que podem ser utilizados em um firewall de gerenciamento de ameaças unificado?

- Um firewall de gerenciamento de ameaças unificado pode oferecer serviços como firewall de rede, prevenção de intrusões (IPS), antivírus, filtragem de conteúdo, VPN (Virtual Private Network), controle de aplicativos e análise de tráfego para proteger contra ameaças de segurança.

28. Qual é o objetivo de se instalar uma zona desmilitarizada?

- O objetivo de instalar uma zona desmilitarizada (DMZ) é criar uma área intermediária entre a rede interna (LAN) e a rede externa (geralmente a internet), onde

servidores expostos ao tráfego externo podem ser colocados. Isso ajuda a proteger a rede interna, permitindo um controle mais rígido sobre o acesso aos servidores da DMZ.

29. Descreva como funciona uma topologia do tipo IDS?

- Uma topologia do tipo IDS (Sistema de Detecção de Intrusões) envolve a implantação de sensores de IDS em locais estratégicos na rede para monitorar o tráfego em busca de atividades suspeitas. Os sensores coletam dados de tráfego, analisam padrões e eventos em busca de potenciais intrusões ou ameaças de segurança. Quando uma atividade suspeita é detectada, o IDS pode alertar os administradores ou tomar medidas para mitigar a ameaça.

30. Como são chamadas as arquiteturas de firewall? (Somente os nomes)

- As arquiteturas de firewall são chamadas de:
  - Stateless Firewall
  - Stateful Firewall
  - Proxy Firewall
  - Firewall de Próxima Geração (NGFW)
  - Firewall de Aplicativos da Web (WAF)
  - Firewall de Gerenciamento de Ameaças Unificado (UTM)