Tecnólogo em Análise e Desenvolvimento de Sistemas
Introdução a Redes de Computadores – ADO V
Professor Carlos Lacerda

Nome: NATHAN HENRIQUE VIEIRA FERREIRA

Turma: TURMA A

Data:05/05/2024

1 – NAT permite compartilhar um único endereço IP público por meio da tradução de endereços IP e portas.

2 – O equipamento encapsula o pacote, roteia para o gateway, realiza tradução de endereço (se necessário), envia para o destino via Internet e desencapsula no destino.

3 – NAT atribui portas únicas para cada conexão interna quando há apenas um endereço IP público.

4 – PAT permite que várias conexões internas usem um único endereço IP público através de portas diferentes.

5 – O redirecionamento de porta redireciona pacotes de uma porta específica de um IP externo para um endereço interno.

6 – NAT funciona na camada de rede, traduzindo endereços; PAT atua na camada de transporte.

7 – O gateway conecta redes diferentes, roteando o tráfego entre elas.

8 – O roteador da empresa "A" encaminha o pacote para o gateway da empresa "A", que o envia para a Internet, onde é direcionado ao gateway da empresa "B" e, por fim, ao destino na empresa "B".

9 – O IP público, com redirecionamento de portas, permite que serviços internos sejam acessíveis na Internet.

10 – Roteamento é determinar a rota mais eficiente para dados entre redes, garantindo entrega correta e eficiente.

11 – Um roteador encaminha dados entre redes; sua função é determinar o melhor caminho para os pacotes.

12 – Encaminhamento de pacotes, interligação de redes e filtragem de tráfego.

13 – Endereços IP de origem e destino, e uma tabela de roteamento.

14 – Roteamento estático (configuração manual) e dinâmico (atualização automática).

15 – Envio de atualizações de rota para roteadores vizinhos para determinar o caminho mais curto.

16 – Troca de informações sobre o estado das conexões para calcular as melhores rotas.

17 – Dispositivo de segurança que monitora e controla tráfego de dados entre redes.

18 – Utiliza regras de filtragem para bloquear acesso não autorizado.

19 – Hardware dedicado ou software em um servidor.

20 – Configurações inadequadas, políticas de segurança fracas, exploração de vulnerabilidades ou ataques sofisticados.

21 – Programa de computador que implementa funcionalidades de firewall.

22 – Firewall de proxy.

23 – Intercepta solicitações do cliente e as encaminha para o destino.

24 – Firewall de próxima geração; combina recursos de firewall tradicional com funções avançadas.

25 – Firewall de aplicativos, prevenção de intrusões, controle de acesso, VPN, filtragem de conteúdo, etc.

26 – Isolar servidores ou serviços públicos da rede interna.

27 – Coloca sensores de detecção de intrusões em pontos estratégicos para monitorar atividades suspeitas.

28 – Firewall de perímetro e firewall de rede interna.