Parte 1: Firewalls – Guardiões da Rede (Aula Expositiva-Dialogada)

Objetivo: Compreender a função, importância e funcionamento dos firewalls na segurança de redes corporativas e domésticas.

Introdução (Diálogo inicial):

• "Olá a todos! Para começarmos nossa conversa, gostaria de perguntar: O que vocês imaginam que acontece quando conectamos nossos computadores à internet ou a uma rede interna? Quais são os riscos? E como podemos nos proteger?"

• (Aguardar e incentivar a participação dos alunos, anotando palavras-chave como "vírus", "invasão", "dados roubados", "proteção").

O que são Firewalls?

• **Firewalls são equipamentos ou softwares específicos que atuam como uma barreira de segurança em uma rede de computadores**.

• Eles são fundamentais para a **segurança da rede**, controlando todo o fluxo de dados que entra e sai.

• No ambiente corporativo, a gestão eficaz dos ativos de rede, incluindo firewalls, é crucial para o sucesso e o lucro de uma empresa.

Como os Firewalls Funcionam?

• "Imaginem um porteiro em um prédio, que só permite a entrada de pessoas autorizadas e barra qualquer um que represente uma ameaça. O firewall funciona de forma similar."

• Os firewalls **filtram as conexões**. Eles analisam os dados enviados e recebidos, e **decidem se são seguros ou não**, impedindo o acesso caso não sejam.

• Eles atuam como um **intermediário de segurança**, protegendo a rede contra ataques externos.

• Um firewall permite que os administradores de rede **controlem o acesso a conteúdos e ferramentas específicas**, garantindo que apenas usuários autorizados acessem informações confidenciais. Por exemplo, um gerente pode ter acesso amplo, enquanto um operador tem acesso limitado às suas funções.

Por que os Firewalls Bloqueiam Portas Específicas?

• "Vocês já se perguntaram por que, às vezes, não conseguimos acessar certos sites ou serviços, mesmo com internet? Ou por que programas de segurança alertam sobre 'portas abertas'?"

• As portas são locais virtuais em um sistema operacional onde as conexões de rede começam e terminam, ajudando os computadores a classificar o tráfego.

• **Existem 65.535 portas possíveis**. Muitas são reservadas para protocolos específicos (por exemplo, porta 80 para HTTP e 443 para HTTPS).

• Invasores frequentemente tentam enviar tráfego malicioso para **portas aleatórias na esperança de que estejam "abertas"**.

• **Firewalls configurados corretamente bloqueiam o tráfego para a maioria das portas por padrão**, permitindo apenas as que são conhecidas e necessárias para serviços legítimos (como e-mail, tráfego web). Bloquear portas específicas, como a 3389 (usada para Protocolo de Desktop Remoto - RDP), pode impedir ataques direcionados a essas vulnerabilidades.

• **Manter o firewall atualizado é essencial** para a segurança das operações e do ambiente tecnológico.

Conclusão (Diálogo):

• "Vimos que o firewall é um componente ativo crucial para a segurança de qualquer rede. Qual a principal lição que tiramos hoje sobre a importância do firewall?"

• "Vocês conseguem pensar em situações do dia a dia onde um firewall (mesmo que invisível) está protegendo vocês?"

Parte 2: Pontos de Acesso sem Fio (Access Points) – Expandindo a Conectividade (Aula Expositiva-Dialogada)

Objetivo: Entender o papel dos pontos de acesso sem fio na criação de redes sem fio e suas tecnologias subjacentes.

Introdução (Diálogo inicial):

• "Agora que falamos sobre segurança, vamos falar sobre como nos conectamos. Quem aqui usa Wi-Fi em casa, na escola ou em um café? Como essa conexão sem fio funciona? O que são aqueles 'aparelhinhos' que nos dão o Wi-Fi?"

• (Aguardar e incentivar a participação, direcionando para o conceito de "rede sem fio" e o dispositivo que a possibilita).

O que são Pontos de Acesso sem Fio (Access Points)?

• Redes de computadores podem ser estabelecidas **sem fio usando ondas de rádio ou outros meios eletromagnéticos**.

• Um **ponto de acesso sem fio** (ou Access Point) é um dispositivo de rede que facilita e dá suporte ao uso de uma rede de computadores, permitindo que dispositivos se conectem sem a necessidade de cabos físicos.

• Na prática, em uma rede em estrela, os **clientes sem fio (como seus celulares ou laptops) se associam a um ponto de acesso sem fio central**.

Como Funcionam as Redes Sem Fio e os Access Points?

• "Os Access Points são como a torre de celular em miniatura da sua casa ou escritório, transmitindo o sinal para seus dispositivos."

• As **Redes Locais sem Fio (WLANs) usam uma tecnologia de rádio de alta frequência**, semelhante à celular digital.

• O padrão **IEEE 802.11** define essa tecnologia de ondas de rádio sem fio, amplamente conhecida como **Wi-Fi**.

• Para estender o alcance do sinal, especialmente em grandes áreas ou para cobrir "zonas mortas", **repetidores são muito utilizados na tecnologia wireless**. Eles recebem e aumentam o sinal de um segmento de rede e o retransmitem para outro segmento.

• Um roteador residencial, por exemplo, frequentemente integra a funcionalidade de um Access Point, permitindo a conexão de computadores, dispositivos e máquinas industriais à internet tanto por cabo quanto por Wi-Fi.

Tipos de Redes Habilitadas por Access Points:

• **Rede de Área Pessoal (PAN):** Redes para comunicação entre dispositivos próximos a uma pessoa (ex: computadores, impressoras, celulares). Pode incluir dispositivos com e sem fio, com alcance de até 10 metros. Tecnologias como Bluetooth e infravermelho formam uma PAN sem fio.

• **Rede de Área Local (LAN):** Uma rede que conecta computadores e dispositivos em uma área geográfica limitada (casa, escola, escritório). As LANs com fio são mais comuns em Ethernet, mas as redes sem fio (WLANs) são um tipo de LAN.

Conclusão (Diálogo):

• "Os Access Points, por vezes integrados em roteadores, são essenciais para a nossa conectividade moderna, permitindo a flexibilidade das redes sem fio. Quais são as vantagens e desvantagens de usar uma rede sem fio em comparação com uma rede cabeada, pensando na segurança e na agilidade?"

• "Como a evolução da tecnologia sem fio impactou o nosso dia a dia e o ambiente corporativo?"

Parte 3: Configuração de um Roteador Residencial com Cisco Packet Tracer (Aula Prática Demonstrativa)

Observação Importante: As fontes fornecidas não contêm instruções passo a passo para a configuração de um roteador no Cisco Packet Tracer. Portanto, esta seção será elaborada com base em conhecimentos gerais sobre a ferramenta e a configuração de roteadores residenciais, e **deverá ser explicitamente informada aos alunos como material complementar e não diretamente extraído das fontes**.

Objetivo: Demonstrar a configuração básica de um roteador residencial em um ambiente simulado para fornecer conectividade LAN e Wi-Fi.

Ferramenta: Cisco Packet Tracer

Materiais Necessários (no Packet Tracer):

• 1 Roteador Sem Fio (Wireless Router – geralmente o modelo Linksys WRT300N ou similar em Packet Tracer)

• 2 PCs (Desktop/Laptop)

• 1 Tablet ou Smartphone (para testar a conexão sem fio)

• Cabos Ethernet (Automaticamente escolhidos ou Crossover/Straight-through conforme necessário)

Passos da Configuração:

1. **Montar o Cenário no Packet Tracer:**

◦ Abra o Cisco Packet Tracer.

◦ Na barra de dispositivos na parte inferior, clique em "Wireless Devices" (dispositivos sem fio) e arraste um "Wireless Router" para a área de trabalho.

◦ Clique em "End Devices" (dispositivos finais) e arraste dois "PCs" (computadores) e um "Tablet" para a área de trabalho.

2. **Conectar os Dispositivos Físicos:**

◦ Clique no ícone de "Connections" (raio) na barra inferior.

◦ Selecione o cabo "Copper Straight-Through" (cabo reto de cobre).

◦ Clique em um **PC** (por exemplo, PC0) e selecione a porta "FastEthernet0".

◦ Clique no **Wireless Router** e selecione uma das portas "FastEthernet" (por exemplo, FastEthernet0/1, 0/2, 0/3, 0/4 – *não* a porta Internet/WAN, que será para a conexão externa).

◦ Repita o processo para o outro **PC** (PC1), conectando-o a outra porta FastEthernet do roteador.

◦ Para o **Tablet**, a conexão será sem fio. Certifique-se de que o Tablet esteja ligado e com o Wi-Fi habilitado nas suas configurações.

3. **Configurar o PC para Acessar a Interface do Roteador:**

◦ Clique no **PC0**.

◦ Vá para a aba "Desktop" e selecione "IP Configuration".

◦ Altere para "DHCP". O PC0 deve receber um endereço IP automaticamente do roteador (geralmente na faixa 192.168.0.x ou 192.168.1.x, dependendo do modelo do roteador).

◦ Feche a janela de IP Configuration.

◦ Ainda na aba "Desktop" do PC0, clique em "Web Browser".

◦ Na barra de URL, digite o endereço IP padrão do roteador (geralmente **192.168.0.1** ou **192.168.1.1**). Pressione Enter.

◦ Uma janela de login aparecerá. As credenciais padrão são geralmente admin para o usuário e admin para a senha. (Em um cenário real, é crucial alterar isso imediatamente para segurança).

4. **Configuração Básica do Roteador Residencial (Interface Gráfica):**

◦ Após o login, você estará na interface de configuração do roteador.

◦ **Internet Setup (WAN):**

▪ Procure por uma seção como "Setup", "Basic Setup" ou "Internet Setup".

▪ Para um roteador residencial, a maioria dos provedores de internet usa DHCP (Automatic Configuration - DHCP). Deixe essa opção selecionada. Se fosse um provedor que exige IP fixo, você preencheria as informações de IP, máscara, gateway e DNS aqui.

▪ **Salvar alterações**.

◦ **Network Setup (LAN):**

▪ Verifique a seção "Network Setup" ou "LAN Setup".

▪ Você verá o IP do roteador (por exemplo, 192.168.0.1) e a máscara de sub-rede.

▪ **DHCP Server:** Certifique-se de que o servidor DHCP esteja ativado para que os dispositivos conectados recebam IPs automaticamente. Configure a faixa de IPs que o roteador irá distribuir (por exemplo, de 192.168.0.100 a 192.168.0.150).

▪ **Salvar alterações**.

◦ **Wireless Setup (WLAN):**

▪ Procure pela seção "Wireless", "Wireless Security" ou "Basic Wireless Settings".

▪ **Network Name (SSID):** Defina um nome para sua rede Wi-Fi (ex: MinhaRedeWi-Fi).

▪ **Security Mode:** Selecione um método de segurança. **WPA2 Personal (AES)** é o mais recomendado.

▪ **Passphrase:** Crie uma senha forte para sua rede Wi-Fi (ex: SenhaSegura123!).

▪ **Salvar alterações**.

5. **Verificar Conectividade:**

◦ **PC0 e PC1 (cabeados):**

▪ No PC0, feche o navegador e abra "Command Prompt" (Prompt de Comando).

▪ Digite ipconfig /all para ver os detalhes do IP e verificar se recebeu um IP da faixa configurada.

▪ Tente pingar o roteador: ping 192.168.0.1 (ou o IP do seu roteador).

▪ Tente pingar o outro PC: ping <IP_do_PC1>.

◦ **Tablet (sem fio):**

▪ Clique no **Tablet**.

▪ Vá para a aba "Desktop" e clique em "PC Wireless".

▪ Na janela de "PC Wireless", clique na aba "Connect".

▪ Clique em "Refresh". Você deve ver o SSID que você configurou (ex: MinhaRedeWi-Fi).

▪ Selecione sua rede e clique em "Connect".

▪ Digite a "Passphrase" (senha) que você configurou e clique em "Connect".

▪ O Tablet deve se conectar à rede sem fio e receber um endereço IP.

▪ No "Command Prompt" do Tablet, tente pingar o roteador e os PCs cabeados para confirmar a conectividade.

6. **Salvar o Projeto no Packet Tracer:**

◦ Vá em "File" -> "Save As..." e salve seu projeto.