CIC0201 - Segurança Computacional - 2025/1

Profa. Priscila Solis Barreto

Trabalho de Implementação 3

Implementação de um Firewall

Neste laboratório, você configurará um Firewall para restringir o acesso à rede de acordo com os requisitos administrativos.

Sua topologia de rede deve conter os elementos seguintes:

- "Internet Pública" - Uma sub-rede que representa dispositivos externos à sua organização
- "DMZ" (zona desmilitarizada) - Uma sub-rede contendo servidores que devem ser acessíveis publicamente
- "Servidores Internos" - Uma sub-rede contendo servidores que devem ser acessíveis apenas a partir de dispositivos internos
- "Estações de Trabalho Internas" - Uma sub-rede contendo computadores de usuários finais (laptops, estações de trabalho, etc.) que devem ser acessíveis apenas a partir de dispositivos internos

O ambiente de rede deve ser montado em algum simulador de rede como o GNS3 ou em um ambiente com mais de um computador e o uso de virtualização para criar máquinas virtuais/servidores virtuais que deverão emular os diversos elementos da rede. A Figura 1 exemplifica a topologia básica necessária para este projeto. A Subnet 5 pode possuir diversos hosts, inclusive sem fio.

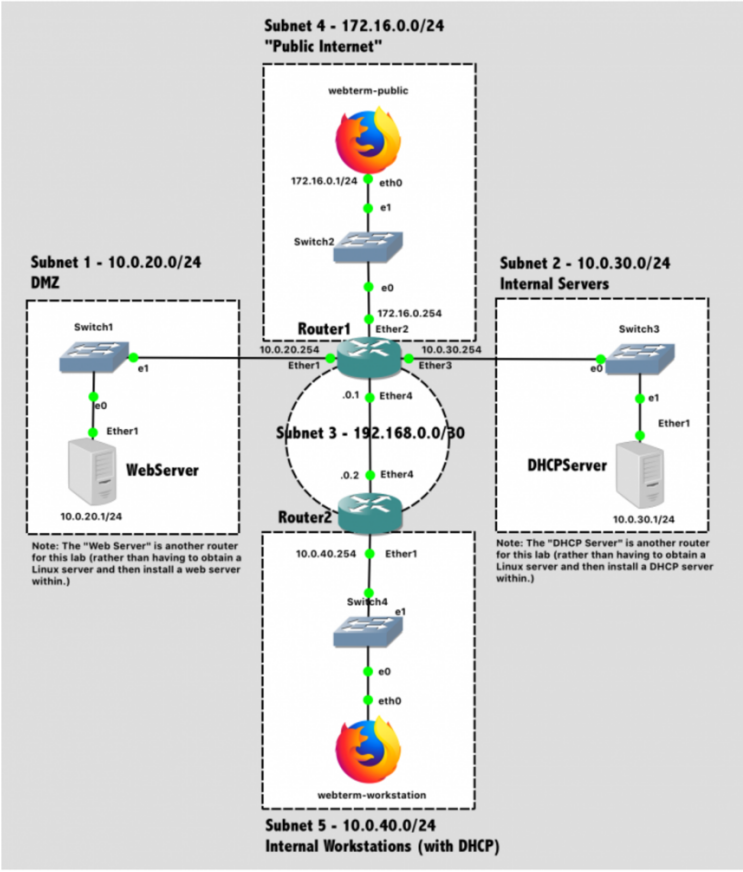

Figura 1. Topologia básica da rede (sugestão)

Algumas dicas de configuração da rede:

1. Configure os nomes de host dos roteadores
2. Configure endereços IP em todas as interfaces do roteador conectadas a sub-redes.
3. Configure roteamento dinâmico/estático entre as sub-redes 1 a 5. Após a configuração, verifique se todos os elementos de rede são alcançáveis.
4. Atribua um nome de host (WebServer e DHCPServer) aos servidores
5. Atribua um endereço IP aos servidores
6. Atribua uma rota padrão estática ao "servidor", para que ele envie todo o tráfego para o Roteador 1. Para torná-la uma rota padrão, o endereço de destino deve ser 0.0.0.0/0 (ou seja, todos os endereços) e o gateway deve ser o endereço IP do Roteador 1 que faz parte da mesma sub-rede. Graças ao LPM (Longest Prefix March) os endereços de destino dentro da sub-rede local poderão ser acessados diretamente, mas todos os outros destinos irão para o gateway padrão.

Atividades:

Os dispositivos na Sub-rede 5 devem ser capazes de obter sua configuração de rede via DHCP. No entanto, o servidor DHCP não é o Roteador 2, que está conectado diretamente à sub-rede. Em vez disso, o servidor DHCP está localizado na Sub-rede 2. Portanto, o retransmissor DHCP é necessário.

1. Configure o Roteador 2 para funcionar como um retransmissor DHCP. Quando o Roteador 2 receber uma solicitação DHCP na interface especificada, ele a encaminhará para o Servidor DHCP.
2. Crie um pool DHCP com um intervalo de endereços IP para fornecer aos clientes. Você deverá excluir endereços usados pelo próprio roteador ou por quaisquer outros dispositivos de rede configurados estaticamente nessa sub-rede.
3. Habilite um servidor DHCP em uma interface específica, usando um conjunto específico de endereços IP e oferecendo "locações" de endereços IP por um período especificado. Observe que, para este comando é necessário usar um comando de DHCP Relay e especificar o endereço IP de onde essas solicitações DHCP retransmitidas foram capturadas.
4. Configure o DHCP para comunicar as informações da sub-rede, os servidores DNS desejados (se houver e o gateway padrão aos clientes.

Deve ser configurado um firewall no Roteador 1 para a rede. O firewall opera por meio de regras de firewall. Cada regra consiste em duas partes: o correspondente, que compara o fluxo de tráfego com as condições fornecidas, e a ação, que define o que fazer com o pacote correspondente, como permitir ou negar. As regras de filtragem do firewall são agrupadas em cadeias. Isso permite que um pacote seja correspondido com base em um critério comum em uma cadeia e, em seguida, passado para processamento com base em algum outro critério comum para outra cadeia. Existem três cadeias predefinidas, que não podem ser excluídas:

- Entrada - usada para processar pacotes cujo destino é o próprio roteador. Em outras palavras, pacotes cujo endereço IP de destino é um dos endereços do roteador. Os pacotes que passam pelo roteador não são processados de acordo com as regras da cadeia de entrada.
- Saída - usada para processar pacotes que se originaram do roteador e estão saindo dele por uma das interfaces. Os pacotes que passam pelo roteador não são processados de acordo com as regras da cadeia de saída.
- Encaminhamento - usada para processar pacotes que passam pelo roteador.

Crie regras de firewall no Roteador 1 que executem as seguintes ações:

1. Conexões HTTP de entrada da Sub-rede 4 para o servidor web devem ser permitidas:
2. Pacotes que fazem parte de conexões estabelecidas (ou relacionadas) devem ser permitidos. Isso permite que a resposta do servidor web retorne ao cliente solicitante.
3. Solicitações DHCP de entrada (Porta UDP 67) da Sub-rede 3 para o Servidor DHCP devem ser permitidas
4. Respostas DHCP de saída do Servidor DHCP para a Sub-rede 5 devem ser permitidas
5. Todo o restante deve ser negado

Os testes executados no ambiente devem demonstrar que:

1. O host webterm-public e outros hosts nesta subrede conseguem acessar a página web no Servidor Web
2. O host webterm-public e outros hosts na subrede 5 conseguem acessar a página web no Servidor DHCP
3. O host webterm-public consegue acessar a página web no Roteador

Os testes devem ser analisados e demonstrados no Roteador 1 com alguma ferramenta de sniffing de rede (Wireshark0.

Referências para consulta:

1. https://www.iptables.org/documentation/HOWTO/pt/packet-filtering-HOWTO.sgml
2. https://linuxconfig.org/collection-of-basic-linux-firewall-iptables-rules

Data de Entrega: 08/07/2025, plataforma Moodle, até 23:55h.

Apresentações: 08/07, 10/07 e 15/07.