Professor: Macêdo Firmino
Disciplina: Segurança de Rede
Prática 20: VPN com OpenVPN e PfSense.

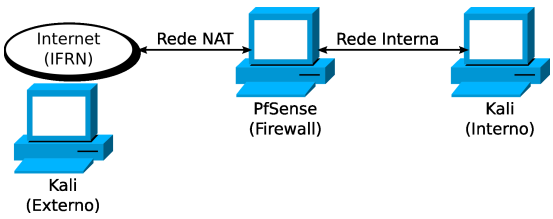
Olá, meus alunos!! Na aula de hoje iremos compreender os conceitos e aplicações de redes privadas virtuais (VPNs) e a implementar uma solução prática utilizando o pfSense como servidor VPN com OpenVPN. Vamos lá!!! Preparados???

Configurando o Ambiente

Para estudarmos estes conceitos e ferramentas iremos utilizar três máquinas virtuais. Uma será a máquina com Firewall (PfSense) e as outras máquinas será Kali Linux (cliente interno e externo) para testarmos as as configurações.

A máquina Firewall deverá ter duas placas de Rede (uma em NAT e outra em Rede Nat). A máquina Kali interna na rede interna e o cliente Kali externa com a placa de rede em Rede NAT..

Lembrando que o PfSense foi apresentado, instalado e configurado nas Práticas 11 e 12.



Rede Privada Virtual (VPN)

Uma rede privada é desenvolvida para uso interno em uma organização. Ela possibilita o acesso a recursos compartilhados e, ao mesmo tempo, fornece privacidade. Uma organização pequena com uma única sede pode usar uma LAN isolada garantindo privacidade ao transferir informações. Entretanto, uma organização maior, com várias sedes, para prover a comunicação entre as diversas sedes pode usar a Internet global. Mas e a segurança nestas comunicações?

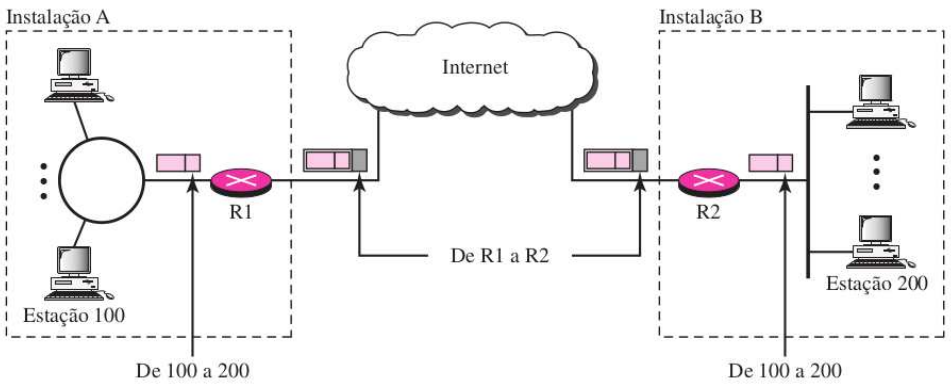
Uma VPN é uma rede lógica que utiliza uma infraestrutura de rede pública para estabelecer conexões privadas entre dispositivos ou redes. A VPN prove confidencialidade, integridade e autenticidade no tráfego de dados, ao criar túneis criptografados sobre redes não confiáveis.

Ela opera encapsulando dados para protegê-los por meio de criptografia e autenticação, a VPN simula a experiência de uma rede local, ainda que os dispositivos estejam fisicamente distantes. Entre os principais benefícios da VPN, destacam-se:

- Segurança: proteção de dados contra interceptação, por meio de criptografia.
- Anonimato: possibilidade de ocultação do endereço IP real e da localização geográfica.
- Acesso remoto seguro: viabilização do trabalho remoto com acesso à intranet corporativa.
- Bypass de censura e restrições geográficas: acesso a conteúdos bloqueados por região.

Normalmente, a VPN usa o modo túnel virtual para transmitir os dados de forma segura. Neste caso, seu endereço IP real é mascarado e substituído pelo endereço IP do servidor VPN. Isso ajuda a proteger a identidade do usuário e a localização geográfica, permitindo acesso a conteúdos que podem estar restritos com base na localização.

As VPNs são empregadas por organizações, instituições governamentais e usuários individuais, especialmente no contexto de home office, mobilidade corporativa e segurança de redes Wi-Fi públicas.



OpenVPN

O OpenVPN é uma das soluções mais populares e confiáveis para a criação de redes privadas virtuais (VPNs). Desenvolvido como um software de código aberto, ele utiliza os protocolos SSL/TLS para autenticação e criptografia dos dados transmitidos. Ele permite a criação de túneis seguros através da Internet ou de outras redes públicas, simulando uma rede privada.

Por ser software livre e multiplataforma (Windows, Linux, macOS, Android, iOS), o OpenVPN ganhou grande adesão da comunidade de segurança da informação e administradores de rede.

Ele pode operar sobre TCP ou UDP, adaptando-se ao tipo de rede e exigência de confiabilidade ou desempenho. A porta padrão UDP é 1194, mas é configurável para operar em outras portas.

O OpenVPN pode ser usado em dois cenários principais:

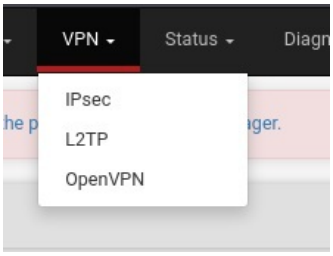
- Acesso Remoto: usuários remotos instalam um cliente OpenVPN e se conectam ao servidor da empresa. Essa configuração permite que o cliente acesse os recursos internos como se estivesse na rede local, com segurança e autenticação adequada.
- Site-to-Site: duas redes separadas geograficamente podem ser conectadas por meio de servidores OpenVPN em cada lado, formando um túnel entre elas. Isso é útil para integrar filiais ou conectar redes em ambientes de nuvem.

O OpenVPN está disponível em duas versões: OpenVPN Community Edition (versão gratuita e de código aberto) e a OpenVPN Access Server (paga com mais recursos). Iremos utilizar a versão gratuita.

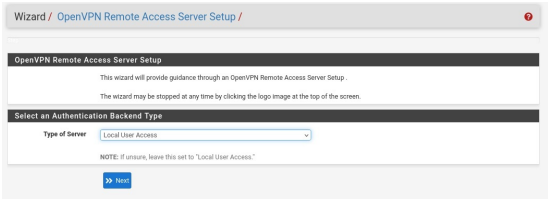
Configurando o OpenVPN no PfSense

Para o OpenVPN ser utilizado na aula de hoje precisaremos criar uma Autoridade Certificadora, criar o Certificado do Servidor OpenVPN, executar o Assistente do OpenVPN para configuração, criar um usuário e seu respectivo certificado digital. Para isso, siga os passos:

1. Acesse o pfSense: https://<ip-do-pfsense> e insira o usuário e senha.
2. Inicialmente vamos selecionar a aba de VPN e em seguida vamos clicar em OpenVPN.

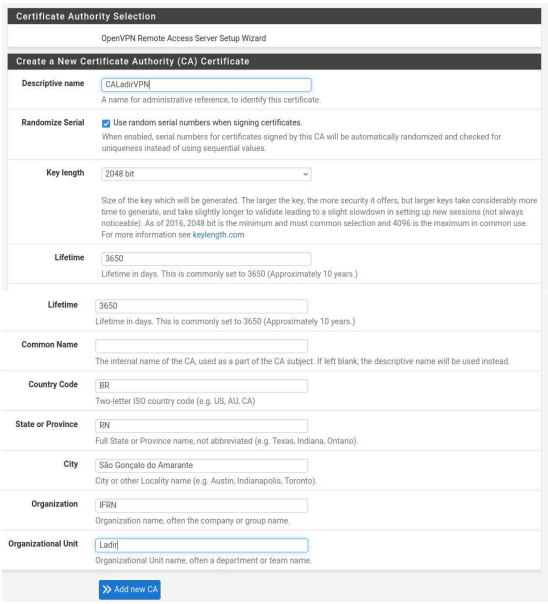


3. Selecione a aba e em “Wizards” e em “Type of Server” selecione “Local User Access” e clique em “Next”. Dessa forma, o servidor OpenVPN dentro do pfSense será usado para a autenticação dos usuários da VPN.



Criando a Autoridade Certificadora

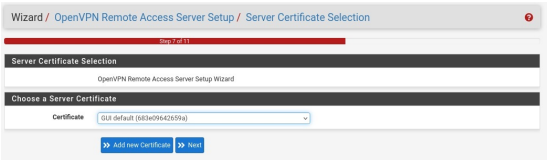
4. Agora vamos criar a nossa autoridade certificadora (CA). Para isso vamos preencher alguns campos:
   - Descriptive name: Aqui vamos dar o nome da Autoridade Certificadora. Em nosso caso estamos usando o nome “CALadirVPN”.
   - Key length: O tamanho da chave, para esse tutorial vamos usar o tamanho padrão de 2048 bit.
   - Country Code,State or Province, City e Organization: Essa é a parte onde inserimos informações sobre o código do país, estado, cidade e o nome da organização. Usaremos BR, RN, São Gonçalo e IFRN.



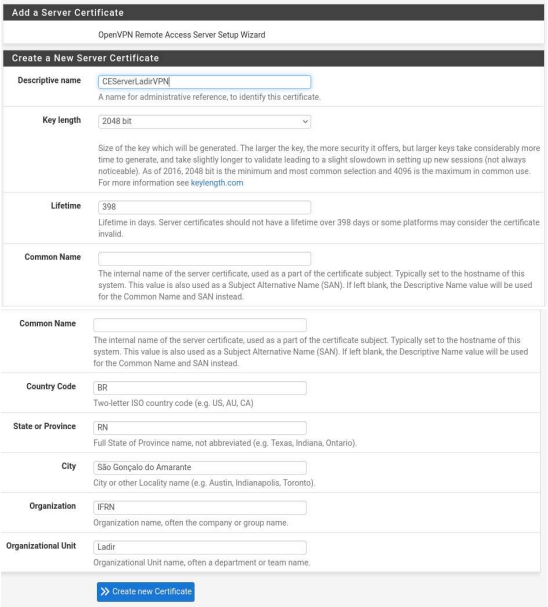
5. Em seguida vamos clicar em “Add new CA” para criar a nova Autoridade Certificadora.

Criando Certificado do Servidor

6. O próximo passo é o criar o certificado do Servidor OpenVPN. Para isso, em Certificate selecione “GUI Default” e clique em “Add New Certificate”.



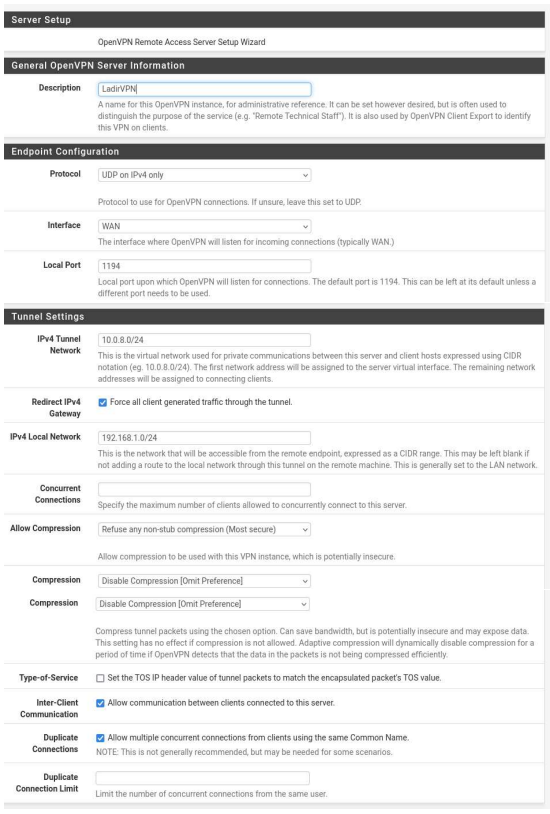
7. Na sequência, iremos preencher os dados do certificado do Servidor. Iremos atribuir o nome “CEServerLadirVPN”. Muitos campos foram preenchidos automaticamente com as informações que inserimos na criação da Autoridade Certificadora. Clique em “Create new Certificate”.



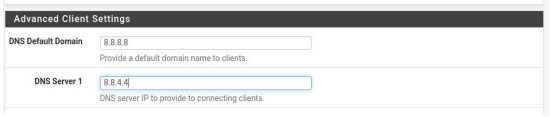
Configuração do Servidor VPN

8. Agora iremos inserir as informações do servidor OpenVPN para permitir o acesso dos clientes. As principais configurações são:

- Description: um nome para o cliente identificar em qual VPN está se conectando. Vamos usar a description “LadirVPN”.
- Protocol: podemos os protocolos. Nesta aula, vamos usar o UDP e IPv4.
- Interface: corresponde a qual interface o servidor OpenVPN vai operar. Nesse caso, utilizaremos a interface “WAN”.
- Local Port: informa a porta do servidor OpenVPN. Vamos escolher a porta padrão “1194”.
- Cryptographic Settings: deixe as opções padrões para TLS Authentication, TLS Key, DH Parameters Length, Data Encryption Algorithms, Fallback Data Encryption Algorithm e Auth Digest Algorithm.
- Tunnel Network: inserimos a rede que será usada no túnel VPN. Em nosso caso, vamos usar a rede “10.0.8.0/24”.
- Redirect Gateway: para clientes usar o gateway do servidor OpenVPN como gateway padrão. Dessa forma, todo o tráfego para Internet passará pelo servidor OpenVPN.
- Local Network: definir a rede local da VPN. Nesse caso, vamos informar a rede “192.168.1.0/24”.
- Inter-Client Communication: permitir que os clientes do OpenVPN possam se comunicar.
- Duplicate Connections: para o mesmo usuário de VPN pode manter mais de uma conexão com a VPN.
- Duplicate Connection Limit: para limitar o número de conexões simultâneas que um mesmo usuário pode fazer com o Servidor OpenVPN. Usaremos 2 conexões.

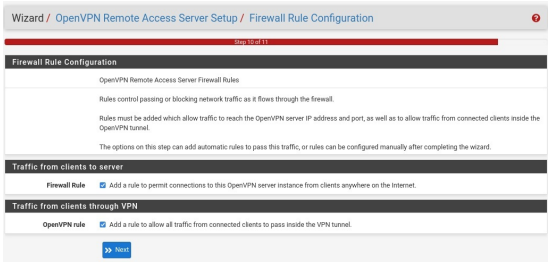


- DNS Default Domain & DNS Server 1-4 : aqui podemos indicar os servidores DNS que serão usados pelos clientes da nossa VPN. Nesse caso estamos usando o "DNS Default Domain" apontando para o DNS da google "8.8.8.8" e o "DNS Server 1" apontando para um segundo DNS da google "8.8.4.4".



9. Depois de preenchido os dados clique em "Next".

10. Na sequência iremos aplicar as regras de firewall. Para isso, selecione "Firewall Rule " e "OpenVPN rule" para aplicar as regras de VPN em nosso firewall. Clique em "Next" e "Finish".

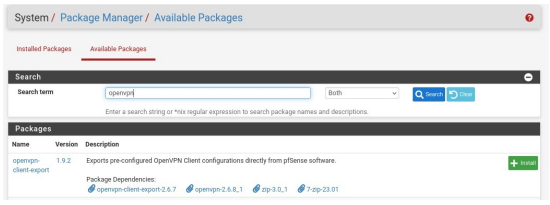


Instalando Pacote para Exportar as Configurações dos Clientes

Agora terminamos a instalação do servidor OpenVPN. O próximo passo é instalar um pacote que vai permitir exportar a configuração dos clientes de nossa VPN. Lembre de verificar sua conexão com a Internet antes da instalação.

11. Para isso, vamos clicar em "System" e "Package Manager".

12. Depois vamos clicar em "Available packages" e pesquisar por openvpn. Depois disso vamos clicar em "Install" e em "Confirm" para o pacote "openvpn-client-export" .



Ao final deverá aparecer a mensagem pfsense-pkg-openvpn-client-export installation successfully completed.

Criação do Usuário

O próximo passo é criar um usuário para a VPN.

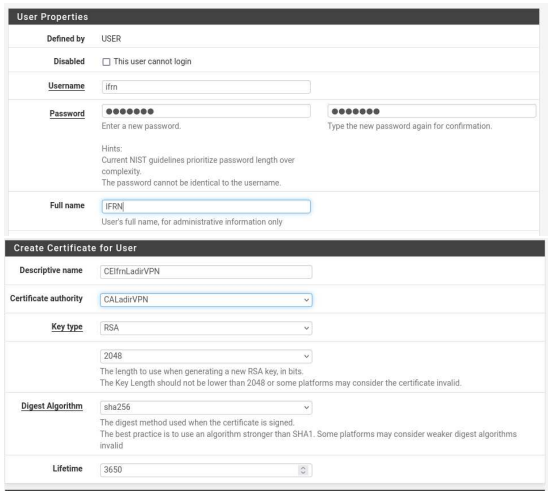
13. Para criar um usuário para nossa VPN, vamos clicar em "System" e "User Manager". Em seguida, vamos clicar na aba "User" e depois em "Add".

14. Vamos criar um usuário chamado "ifrn" e vamos usar a senha "pfsense". Para isso, preencha principais campos: Username, password e selecione a opção "Certificate"

15. Na mesma tela em Create Certificate, insira:

- Description Name: CEIfrnLadirVPN;
- Certificate Authority: CALadirVPN;

16. O resto dos campus pode deixar padrão. Em seguida podemos clicar em "Save".



Exportando o Certificado e As Configurações do Cliente

Por último iremos exportar o certificado e as configurações da VPM para usuário cadastrado.

17. Clique em "VPN" e "OpenVPN". Em seguida, vamos clicar em "Client Export".

Se a aba Client Export não aparecer significa que a instalação do plugin não deu certo. Tente novamente realizar a instalação (passo 13).

18. Na tela do Client Export, em OpenVPN Client procure o usuário IFRN. Vamos exportar para uma máquina Linux então vamos escolher a opção "Inline Configuration" e "Most Clients". Faça o download do arquivo "ovpn" para um diretório do seu computador e posteriormente envie para o cliente.

Acessando a VPN no Cliente (Kali)

Para conectar o Kali Linux a uma VPN (como OpenVPN), inicialmente baixe o arquivo ".ovpn" gerado no passo 18. Lembre que o seu Kali deverá estar ligado ao firewall pela porta WAN, desta forma, coloque a placa de rede do Kali em "Rede Nat".

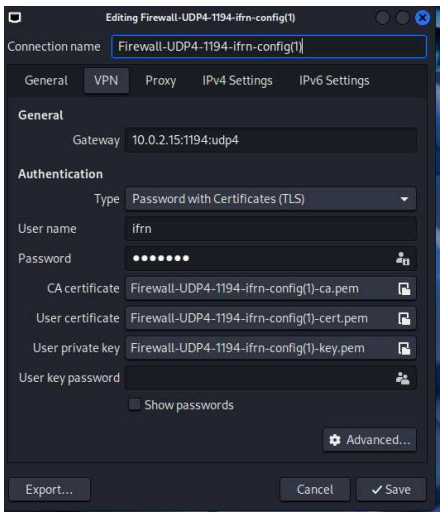
Iremos realizar a configuração usando a interface gráfica (Network Manager). Para isso, siga os passos:

1. Na área de trabalho, clique no ícone do Gerenciador de Rede no canto superior direito da tela. Selecione "Conexões VPN" e "Adicionar uma conexão VPN". O Gerenciador de Rede será exibido.

2. No menu, selecione "Importar uma configuração VPN salva..." e clique em "Create".

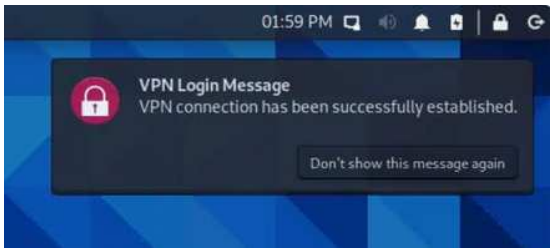
3. Selecione o arquivo .openvpn.

4. Surgirá uma janela com as configurações da VPN. Inclua o usuário "ifrn" e a senha "pfsense". Clique em "Salvar".

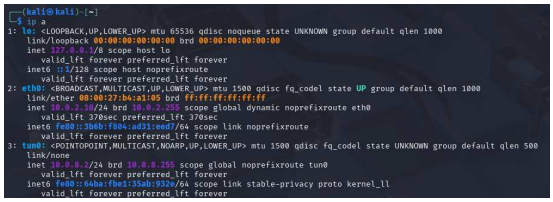


5. Para habilitar sua nova conexão VPN, clique no ícone do "Gerenciador de Rede", "Conexão VPN" e na sua VPN recem criada.

6. Após a conexão bem-sucedida, você verá uma notificação informando que agora você está conectado à VPN.



Agora teremos uma interface de rede virtual ligada a VPN e os dados poderá ser mandado por ela para Podemos ver que agora tenho um endereço IP da VPN e poderá acessar o rede Interna com segurança.



Atividades

1. Realize os passos apresentaos na aula, instale, configure e teste o VPN com o PfSense.

2. Crie um usuário com o seu nome e a senha sendo sua matrícula. Exporte o arquivo de configuração e anexe no Google Sala de Aula, nos comentários informe a sua matrícla e o nome utilizado.