TLP : CLEAR

WireGuard com MFA utilizando DefGuard

Projeto Piloto

Eduardo Costa [1]

[1] raposo@ipb.pt

Agenda

TLP : CLEAR

Motivações

O Defguard

Instalação

Configuração

Testes

Conclusão

Motivações

Motivações

TLP : CLEAR

- Atualmente para os nossos acessos VPN usamos o OpenVPN assente numa firewall OPNsense, mas este será descontinuado nas próximas versões do OPNsense.
- O WireGuard é uma excelente opção de VPN por ser rápido, seguro e fácil de configurar, mas não suporta 2FA/MFA nativamente.
- A maioria dos nossos utilizadores que utilizam VPN para aceder a serviços importantes não tem o mínimo de cuidado.

- O **Defguard** é uma solução opensource que nos permite adicionar MFA ao WireGuard de forma eficiente.

Em resumo:

- Queremos manter uma conexão VPN rápida e segura com WireGuard.
- Precisamos de MFA para proteger melhor os nossos acessos.
- Como o OpenVPN será descontinuado, o WireGuard + DefGuard é uma solução moderna e sustentável.

O Defguard

O Defguard

TLP : CLEAR

- O DefGuard VPN é uma plataforma que oferece um serviço de VPN focado na segurança, velocidade e facilidade de uso.
- Utiliza o protocolo WireGuard, que é conhecido por ser leve, rápido e eficiente, garantindo uma navegação mais segura e com menor latência.
- A autenticação multifator (MFA) adiciona uma camada extra de proteção, dificultando acessos não autorizados.

Vantagens:

- Alta velocidade e desempenho
- Segurança reforçada com 2FA/MFA
- Gestão do ciclo de vida da conta com integração remota segura de contas
- Fácil de configurar e usar
- Integração com plataformas como OPNsense ou PFsense
- Opensource

Desvantagens:

- Recursos limitados na versão gratuita
- Dependência de uma conexão estável
- Compatibilidade com Sistemas Operativos e dispositivos
- Necessidade de configuração adequada

Instalação

Instalação

TLP : CLEAR

A instalação do Defguard deve ser feita seguindo a documentação oficial (https://docs.defguard.net/) e usando as opções mais adequadas para o nosso cenário.
O Defguard é composto por quatro componentes principais:

- Serviço principal (Core)
- Serviço de Proxy
- Servidor/Gateway VPN
- Estação de aprovisionamento

Todos estes componentes consomem poucos recursos, sendo que os recursos mínimos para uma instalção são: CPU 1GHz, RAM 2GB, Disco 2GB e funciona em arquitecturas x86_64 ou ARM64.

O Defguard requer um servidor com IP público e dois domínios a apontar para esse mesmo IP.
Depois de todos os componentes estarem intalados é necessário configurar o iptables com as seguinte regras:

- Portos **tcp/80** e **tcp/443** devem estar abertos
- Porto **tcp/50055** apenas deve estar aberto para o IP das gateways

Para implementar uma gateway Defguard no OPNsense é necessário instalar neste dois pacotes:

- defguard-1.2.0_x86_64-unknown-freebsd.pkg
- defguard-gateway_1.2.1_x86_64-unknown-opnsense.pkg

Configuração

Configuração

TLP : CLEAR

A entrada no Web GUI é feita com as credênciais fornecidas durante a instalação. Após a autenticação escolher na barra de navegação do lado esquerdo a opção "VPN Overview" e configurar uma "VPN Location".

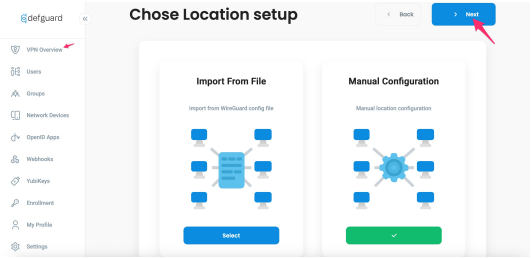

Figure: VPN Overview

Preencher o formulário com os seguintes campos:

- *Location Name* - preencher com o nome da gateway
- *Gateway VPN IP address and netmask* - Gama de IPs que a gateway vai atribuir aos clientes
- *Gateway address* - endereço IP da gateway (OPNsense ou outra)
- *Gateway Port* - 51820
- *Allowed IPs* - tipicamente 0.0.0.0/0
- *DNS* - servidores de DNS
- Definir se queremos *MFA* (checkbox)
- *Keepalive interval* - 5s
- *Peer disconnect threshold* - 300s

Depois de criada a *VPN Location*, editá-la e copiar o token para configurar a VPN gateway.

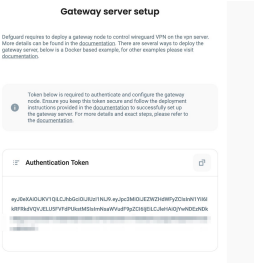

Figure: Authentication Token

No OPNsense no menu escolher opção VPN e depois Defguard Gateway e preencher os campos:

- *Defguard VPN Location Auth Token* - preencher com o token copiado
- *Defguard Core gRPC URL* - preencher com o url do Defguard com **:50055** no fim
- *Path to custom SSL CA cerficiate* - caminho para a CA que assina o certificado do Defguard
- *Gateway name* - o mesmo nome que foi definido no campo *VPN Location* no Defguard
- *Network interface* - interface associada (wg0)
- *Enable Defguard Gateway* - ativar o serviço

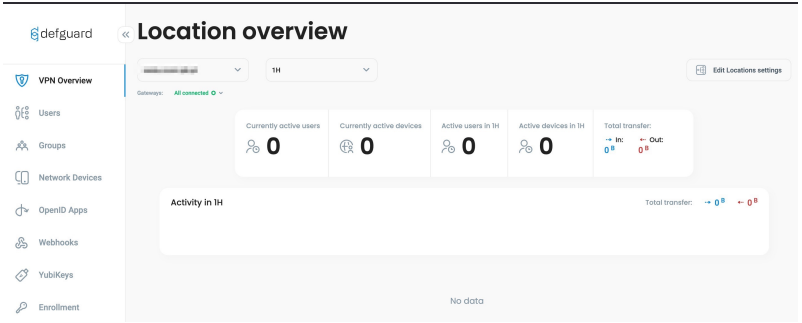

Figure: Estado da VPN

Falta então criar utilizadores e adicionar dispositivos aos mesmos. Escolher no menu do lado esquerdo a opção *Users* para criar um novo utilizador.

Depois de criada a nova conta o utilizador entrar com as suas credênciais, editar o seu perfil e ativar o MFA. Deve usar uma aplicação apropriada para ler o QR Code gerado e colocar o código gerado para finalizar a ativação.

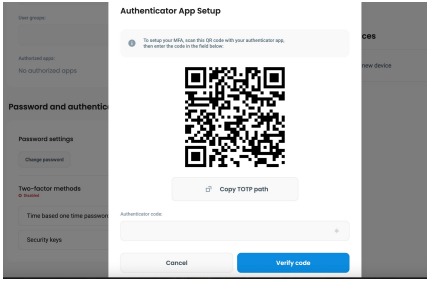

Figure: MFA

Para adicionar um dispositivo é preciso estar no modo de edição do perfil e escolher a opção *Add new device*. Escolher a opção *Configure Desktop Client*, e seguir. Descarreguar o cliente para o sistema operativo do dispositivo e copiar o token para carregar no cliente.

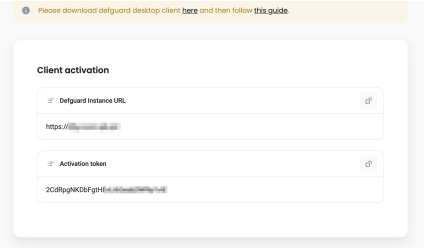

Figure: Adicionar novo dispositivo

Configurar o cliente com o url e o token do dispositivo copiado anteriormente.

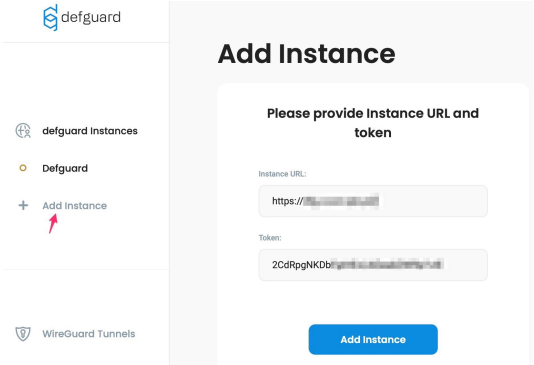

Figure: Configuração do cliente

Testes

Testes

TLP : CLEAR

No Defguard o modo de funcionamento do MFA consiste na criação dinâmica de um perfil, que após autenticação com sucesso, esse perfil é sincronizado com as gateways correspondentes e no termino da sessão é destruído.

Para testar basta entrar no cliente e fazer *connect*.

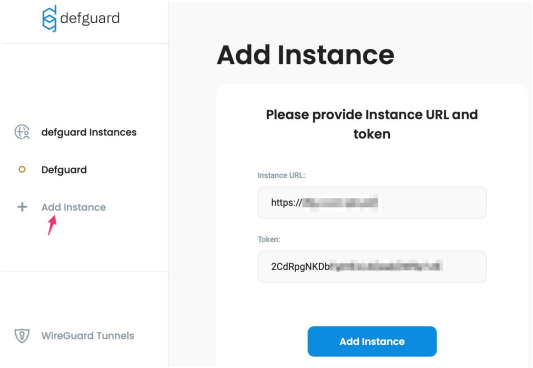

Figure: Conexão

Preencher o campo com o segundo fator de autenticação quando for pedido.

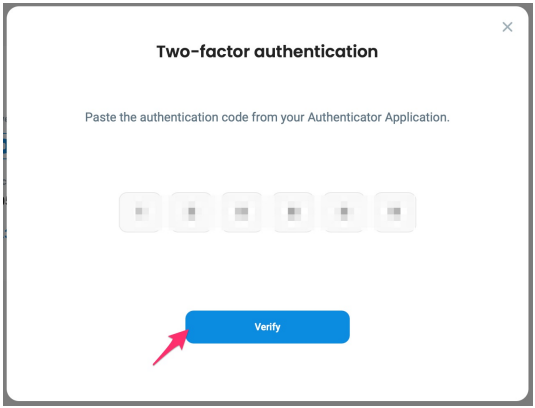

Figure: 2FA

Depois de conetados podemos verificar algumas estatísticas no cliente.

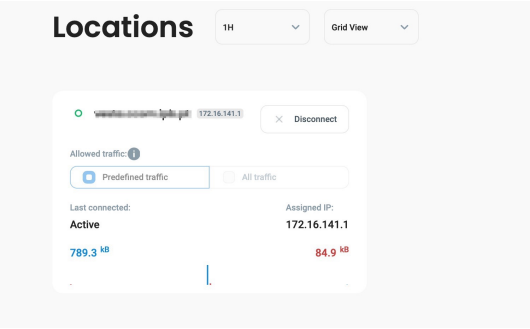

Figure: Cliente conetado

No *Dasboard* da administração do Defguard também podemos ver quantos e quem são os utilizadores/dispositivos conetados.

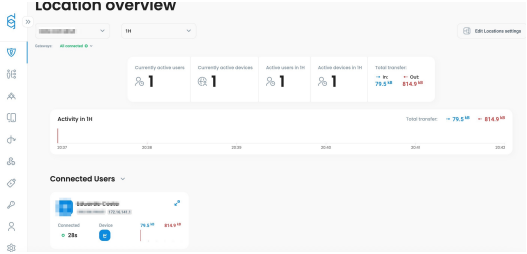

Figure: Dashboard

Conclusão

Conclusão

TLP : CLEAR

- Permite-nos aumentar a segurança em relação à solução atual e à alternativa que seria o WireGuard, ou seja ficamos com as vantagens do WireGuard e acrescentamos mais segurança.
- As ligações são mais rápidas do que as que temos com OpenVPN.
- A versão não paga tem algumas limitações, mas numa instalação *self-hosted* como a que fizemos nenhuma dessas limitações afeta a nossa implementação.
- O Defguard só permite aquando da geração do perfil definir ou um endereço IPv4 ou um endereço IPv6. Esperemos que em futuras versões já suporte dual-stack.

Trabalho futuro

TLP : CLEAR

- Colocar este projeto em produção num cenário com vários utilizadores e necessidades de acesso diferentes.

Questões

TLP : CLEAR

Obrigado.

Questões?


ipb
INSTITUTO POLITÉCNICO
DE BRAGANÇA
CSIRT