COMO PROTEGER UMA REDE WIFI

INTRODUÇÃO

Hoje em dia não é preciso ter uma porta arrombada para que criminosos possam entrar na nossa privacidade e aceder a informações confidenciais ou roubar o seu dinheiro. Como? Através da nossa rede WiFi, caso esteja mal protegida.

De uma forma simples, a rede WiFi é a ligação à internet sem fios. Geralmente envolve um router que envia um sinal, que depois é utilizado para se ligar à internet. Mas, a menos que sua rede sem fios esteja protegida por uma senha, qualquer dispositivo pode apanhar o sinal e usar a sua internet.

COMO PROTEGER A REDE WIFI

Depois dos técnicos instalarem a rede WiFi em minha casa, admito que conectei todos os dispositivos à rede e deixei as configurações padrão. Mas agora estou preocupado com a segurança da minha rede Wi-Fi e quero saber como protegê-la, portanto, procurei formas de proteger a minha rede.

Como proteger uma rede WiFi:

Passo 1: Alterar a senha de acesso

Por vezes, a password é alterada pelo técnico quando vai instalar o aparelho à casa. Mas o ideal é que voltemos a mudá-la para sermos os únicos a conhecê-la. Devemos usar passwords fáceis de memorizar e que também incluam números e carateres especiais, para dificultar o trabalho dos hackers.

Passo 2: Mudar o nome da rede

Os routers vêm configurados com o nome da rede WiFi, também denominado SSID (Service Set IDentifier). Este deve ser alterado para evitar que hackers consigam obter acesso à sua rede de internet sem fios. O SSID tem 32 caracteres, por isso devemos optar por uma pequena frase, que não inclua informações pessoais.

Passo 3: Verificar se o seu WiFi é WPA2

Mas o que é isso? WPA2 significa WiFi Protected Access 2 e é o protocolo de segurança mais eficaz para as redes WiFi. Se estiver ativado, evita que terceiros possam ligar-se à nossa rede sem fios. Além disso, realiza a criptografia dos nossos dados privados, redobrando a segurança da nossa informação.

Se o seu router não disponibilizar este protocolo, deve solicitar a troca por um aparelho mais recente. Se disponibilizar, mas não estiver ativado, deve entrar em contacto com a empresa que fornece o serviço de internet e pedir indicações para fazer a alteração.

Passo 4: Criar uma rede de “amigos e dispositivos”

A maioria dos routers permite criar uma segunda rede. Porque é que devemos fazê-lo? Quando vários computadores e dispositivos estão ligados à mesma rede doméstica, basta que um seja infetado para o malware se espalhar pelos restantes.

Passo 5: Ocultar o nome da rede WiFi

Ocultar a rede WiFi de casa pode aumentar a segurança, impedindo que utilizadores mal-intencionados a encontrem e se liguem. Desta forma, a rede WiFi nunca fica visível para todos. Mais uma vez, este procedimento pode ser realizado nas configurações do router.

Para, depois, ligá-la aos seus dispositivos, terá que clicar em “aceder a outras redes” e colocar o nome escolhido para a sua rede em “nome de rede”.

Passo 6: Certificar de que temos uma boa firewall

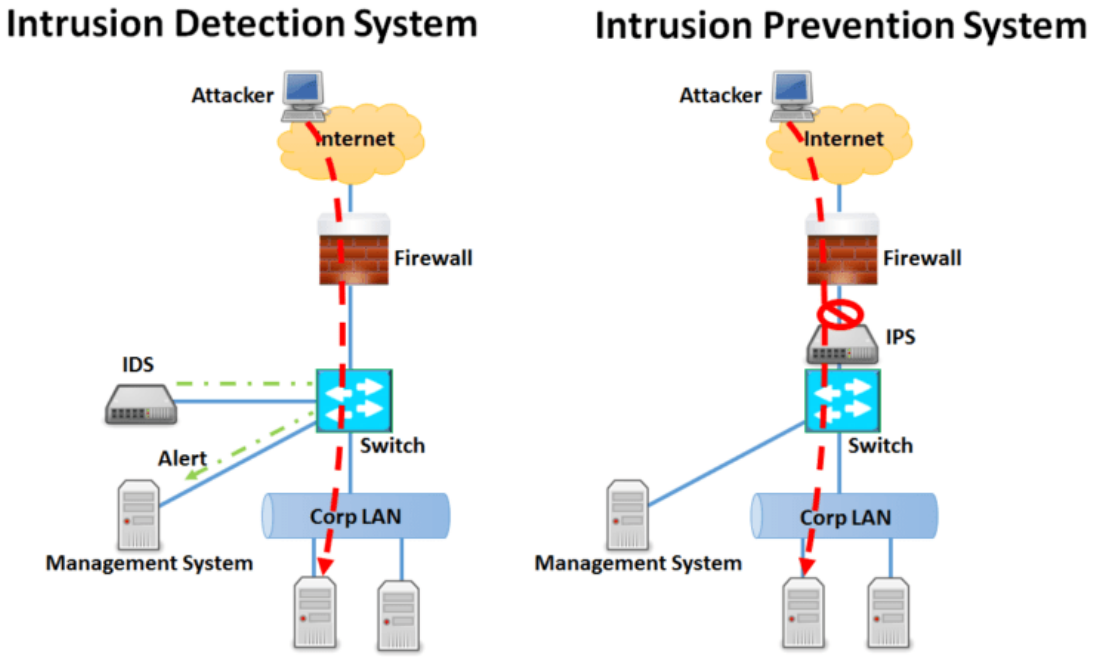
Uma firewall é projetada para proteger os computadores contra malwares, vírus e outras intrusões prejudiciais. Os routers também têm firewalls integradas, mas, por vezes, podem estar desativadas ou desatualizadas. Por isso, devemos verificar se está ativado.

Passo 7: Use uma ligação VPN

A VPN - Virtual Private Network (rede privada virtual) é uma ferramenta simples que protege a privacidade online e mantém a localização e tráfego ocultos. As VPNs encriptam o tráfego de internet, o que torna mais difícil para terceiros rastrear e entrar na nossa privacidade. Normalmente são instaladas nos computadores ou dispositivos, separadamente, como se tratasse de uma aplicação. No entanto, dependendo da tecnologia em causa, pode ser possível instalar a VPN no router e, assim, proteger a rede WiFi e todos os dispositivos que estiverem ligados à mesma.

IPS (SISTEMA DE PREVENÇÃO DE INRTRUSÃO)

Um Sistema de prevenção de intrusão (IPS) ajuda as organizações a identificar tráfego mal-intencionado e impede proativamente que esse tráfego entre na rede



CARACTERISTICAS DE UM IPS

Deteção de Intrusões em Tempo Real: O IPS analisa o tráfego de rede em busca de padrões de atividade suspeitos, como tentativas de acesso não autorizado, exploração de vulnerabilidades ou atividades de malwares.

Prevenção de Intrusões: Além de apenas detetar intrusões, um IPS também pode agir para bloquear ou interromper atividades maliciosas. Isso pode incluir bloqueio de tráfego de entrada ou saída associado a ataques conhecidos.

Análise de Tráfego: Um IPS analisa o tráfego de rede em várias camadas, desde o nível de pacote até protocolos de aplicativos específicos, procurando por indicadores de comprometimento ou comportamento anômalo.

Políticas de Segurança Personalizáveis: Os administradores podem configurar políticas de segurança específicas para atender às necessidades de sua rede

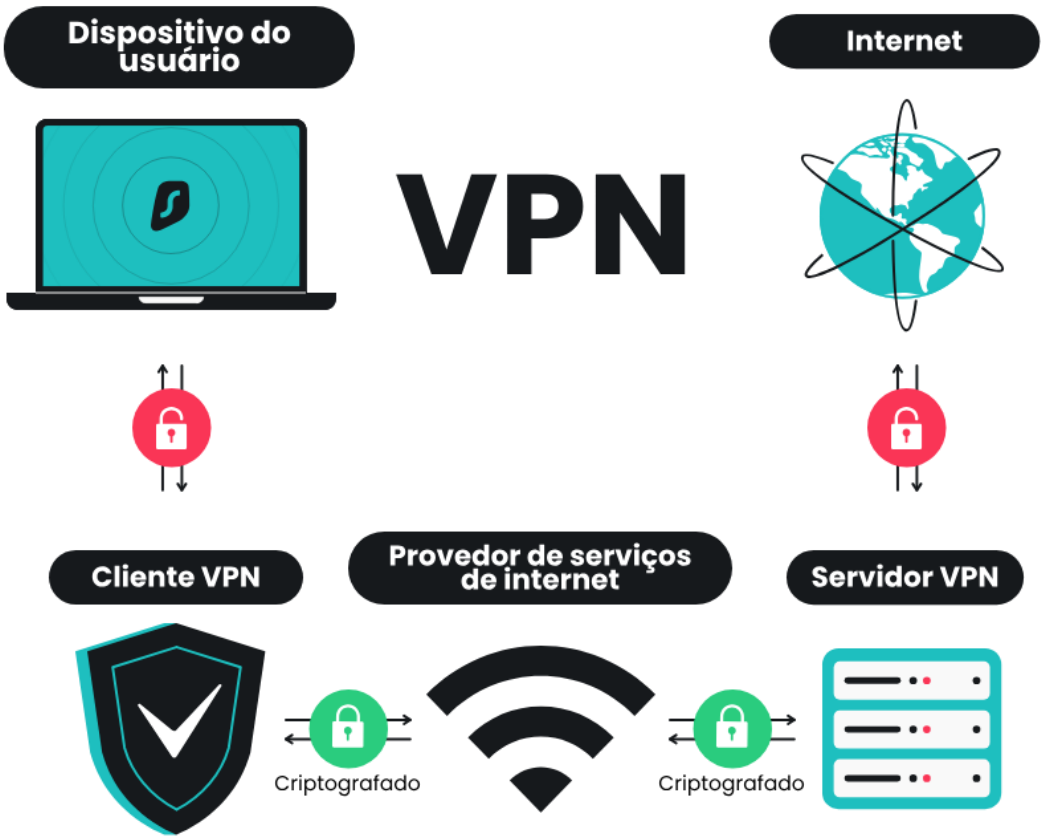
Integração com Outras Soluções de Segurança: Um IPS muitas vezes trabalha em conjunto com outros componentes do sistema de segurança, como firewalls, sistemas de deteção de intrusões (IDS), sistemas de gerenciamento de eventos e informações de segurança (SIEM) e soluções de prevenção de vazamento de dados (DLP), para fornecer uma defesa em camadas mais abrangente.

Atualizações de Assinatura e Inteligência de Ameaças: Para permanecer eficaz contra ameaças em evolução, um IPS requer atualizações regulares de assinatura de ameaças e feeds de inteligência de ameaças.

Relatórios e Análises: Um IPS geralmente fornece recursos de geração de relatórios e análises para ajudar os administradores a entender o panorama de ameaças de sua rede, identificar padrões de atividade suspeitos e tomar medidas proativas para fortalecer a segurança.

VPN

Uma VPN (Rede Privada Virtual) é uma tecnologia que estabelece uma ligação segura e encriptada entre dispositivos através de uma rede pública, como a Internet. Permite aos usuários aceder a recursos de rede de forma segura, como se estivessem diretamente ligados à rede privada, independentemente da sua localização física.



CARACTERÍSTICAS E BENEFÍCIOS DO USA DE UMA VPN

Segurança: Uma VPN cria um túnel encriptado entre o dispositivo do usuário e o servidor VPN. Isto protege os dados transmitidos de serem intercetados por terceiros mal-intencionados, tornando a comunicação mais segura, especialmente em redes públicas ou não confiáveis.

Privacidade: Ao utilizar uma VPN, o tráfego de Internet é encaminhado através do servidor VPN, mascarando o endereço IP real do utilizador. Isto ajuda a proteger a privacidade online, ocultando a atividade de navegação do provedor de serviços de Internet (ISP) e de outros observadores.

Acesso Remoto: As VPNs são comumente usadas por funcionários que precisam de aceder a recursos de rede corporativos de forma segura enquanto estão fora do escritório. Isto permite acesso remoto a sistemas, aplicativos e ficheiros internos, como se estivessem fisicamente presentes na rede da empresa.

Bypass de Restrições Geográficas: Uma VPN pode ser usada para contornar restrições geográficas impostas por determinados serviços online, permitindo que os utilizadores acedam a conteúdo que normalmente estaria indisponível na sua região.

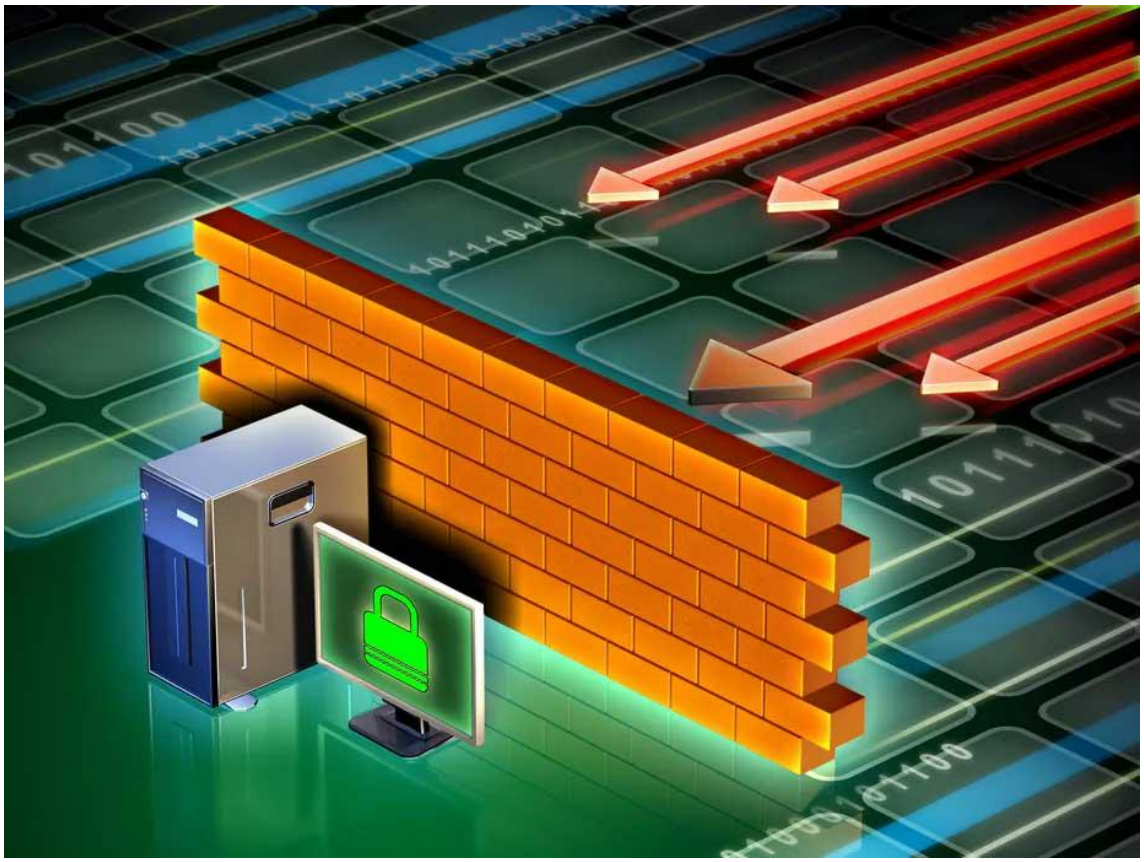
Anonimato: Embora uma VPN proteja a privacidade ao ocultar o endereço IP real, é importante observar que não oferece anonimato completo na Internet. Outras medidas, como o uso de navegadores anónimos e práticas de segurança adicionais, são necessárias para garantir um alto nível de anonimato.

Compatibilidade: As VPNs são compatíveis com uma ampla variedade de dispositivos e sistemas operativos, incluindo computadores, smartphones, tablets, routers e até mesmo alguns dispositivos de Internet das Coisas (IoT).

Encriptação de Tráfego: A comunicação através de uma VPN é encriptada, o que adiciona uma camada adicional de segurança, protegendo os dados contra intercetação e espionagem.

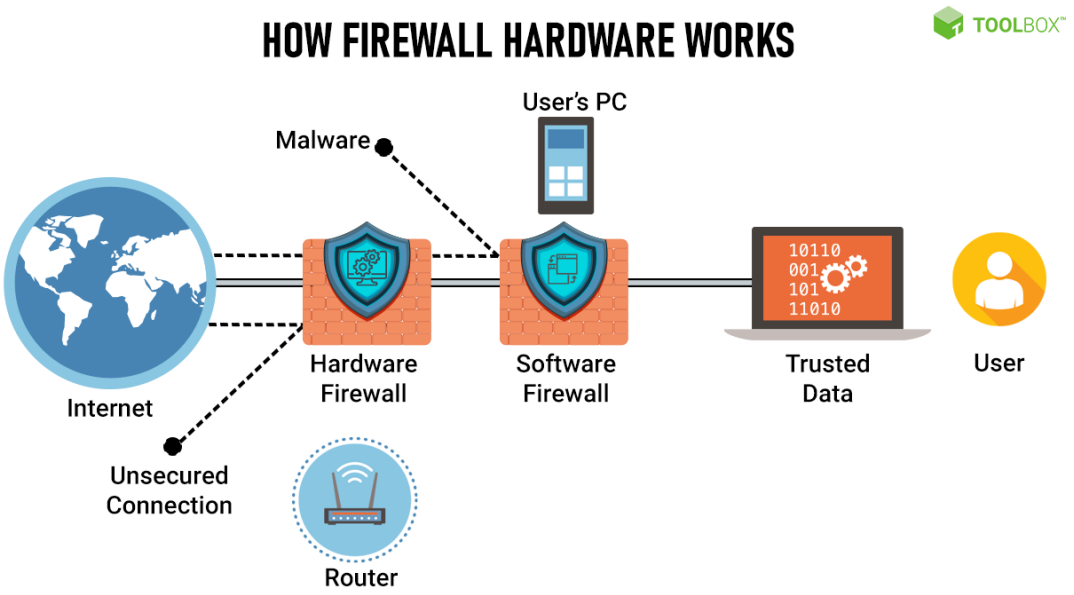
FIREWALLS

As firewalls são programas de software ou dispositivos de hardware que filtram e examinam as informações provenientes da ligação à Internet. Representam a primeira linha de defesa porque podem impedir que um programa malicioso ou atacante tenha acesso à rede e informações antes que qualquer potencial dano seja causado.



FIREWALL DE HARDWARE

As firewalls de hardware estão incluídas em alguns routers e não necessitam praticamente de configuração, porque estão integradas no hardware. Estas firewalls monitorizam o tráfego de todos os computadores e dispositivos ligados à rede desse router, o que significa que pode filtrar o acesso a todos com apenas um equipamento.



AS PRINCIPAIS CARACTERÍSTICAS DO HARDWARE DE FIREWALL INCLUEM:

Filtragem de Pacotes: Examina cada pacote de dados que passa pela rede e aceita ou rejeita com base em regras pré-determinadas.

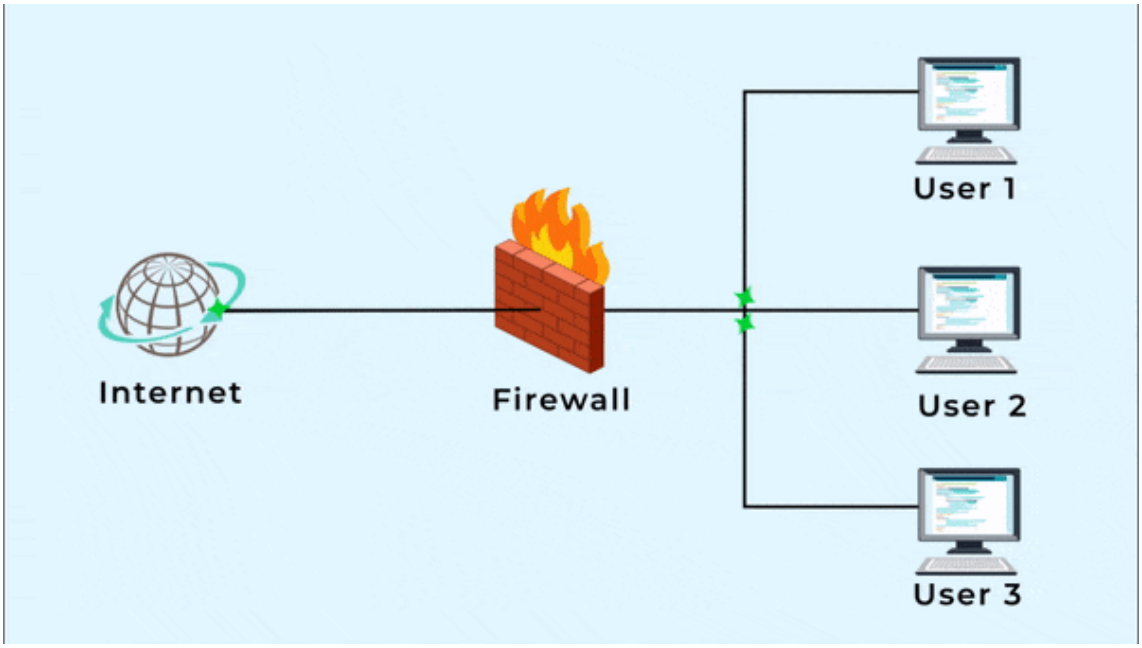
Serviços de Proxy: Atua como intermediário entre as redes interna e externa, inspecionando e filtrando o tráfego antes de passar.

Suporte a Rede Privada Virtual (VPN): Fornece acesso remoto seguro para os utilizadores, criptografando o tráfego sobre redes públicas.

Inspeção Profunda de Pacotes (DPI): Analisa o conteúdo dos pacotes em um nível mais profundo, permitindo um controle e inspeção mais granulares do tráfego de rede.

FIREWALL DE SOFTWARE

As firewalls de software são executadas como um programa no computador ou outros dispositivos e acompanham de perto o tráfego da rede para o ajudar a intercetar programas maliciosos antes que cheguem ao computador.



AS PRINCIPAIS CARACTERÍSTICAS DO SOFTWARE DE FIREWALL SÃO:

Filtragem de Pacotes: Examina cada pacote de dados que passa pela rede e aceita ou rejeita com base em regras pré-determinadas.

Serviços de Proxy: Atua como intermediário entre as redes interna e externa, inspecionando e filtrando o tráfego antes de passar.

Suporte a Rede Privada Virtual (VPN): Fornece acesso remoto seguro para os utilizadores, criptografando o tráfego sobre redes públicas.

Sistemas de Deteção e Prevenção de Intrusões (IDPS): Monitoriza o tráfego da rede em busca de atividades suspeitas e pode tomar medidas para prevenir ameaças potenciais.

Inspeção Profunda de Pacotes (DPI): Analisa o conteúdo dos pacotes em um nível mais profundo, permitindo um controle e inspeção mais granulares do tráfego de rede.