FICHA TRABALHO 8

MODALIDADE:	Jovem + Digital	Não aplicável	
CURSO:	J+D 2/2026 Cibersegurança		
UFCD:	Cibersegurança Ativa	CÓDIGO UFCD:	9196
FORMADOR/A:	Bruno Silva	DATA:	

OBJETIVOS

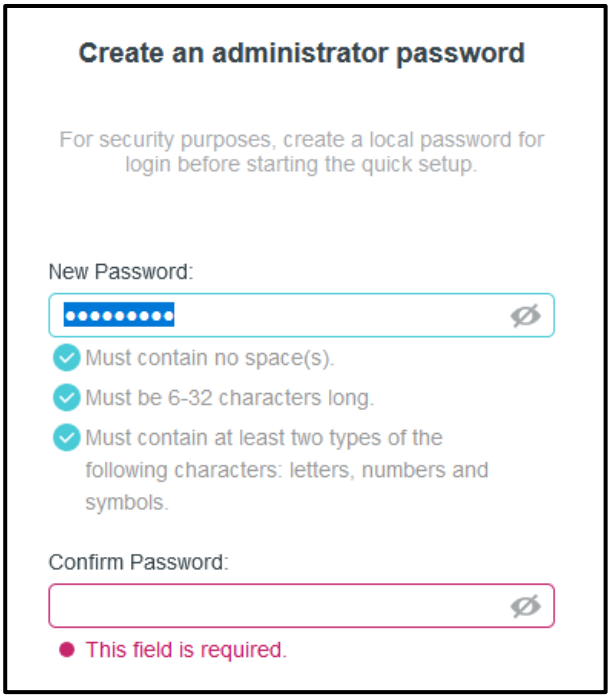
- Saber como instalar e configurar politicas de segurança em redes informáticas

Parte 1 – Configuração e proteção de redes informáticas

1 – Evitar a utilização da password que vem por defeito nos dispositivos

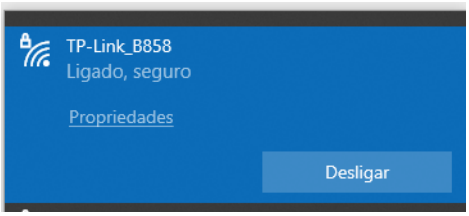
É aconselhável alterar a senha do administrador do equipamento. Devem seguir as boas normas de utilização de palavras-passe:

- Ter entre 8 e 32 carateres de comprimento;
- Não conter espaços;
- Usar pelo menos duas letras maiúsculas, minúsculas, números e carateres alfanuméricos;
- Não ser igual as 5 últimas passwords;

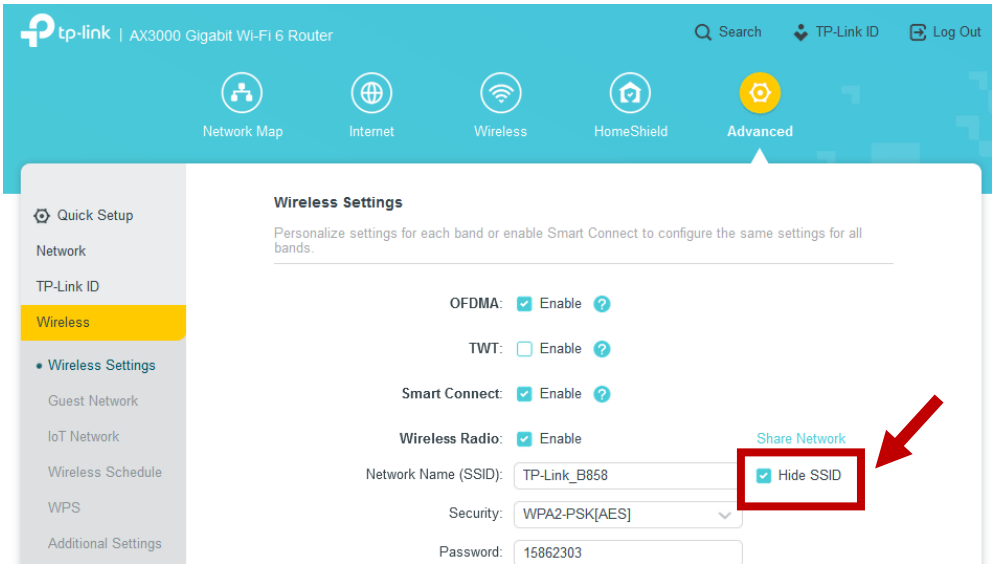


2 – Oculte a identificação do dispositivo de rede

Para conseguir encontrar uma rede precisamos do SSID (Service Set Identifier), para conseguir clicar e ligar na rede pretendida:

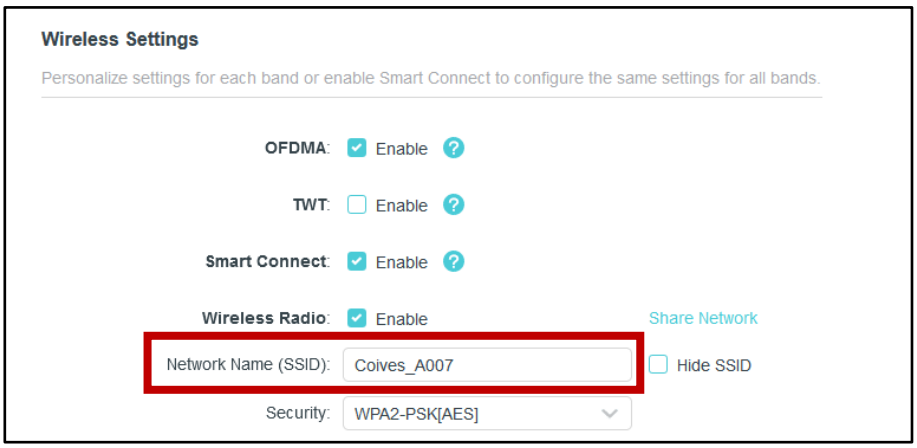


Para aumentar a segurança, poderá desligar a transmissão da identificação do SSID - para evitar que o vosso dispositivo mostre a sua presença:



3 - Alterar do identificador SSID do seu dispositivo

Se deseja deixar o SSID ativo, altere o nome SSID padrão do dispositivo e tente evitar o uso de um nome que pode ser adivinhado facilmente:



4 – Utilizar a criptografia de dados mais recente

A criptografia de dados tem sido parte da segurança das redes. Ao longo da evolução da tecnologia, surgiram vários modos de criptografia de dados, tais, como o WEP e WPA.

WEP e WPA são protocolos de criptografia de dados utilizados em redes sem fio e servem para proteger uma rede Wi-Fi contra acessos indesejados.

- *WEP*

  WEP (*Wired Equivalent Privacy,* é o protocolo que foi lançado em 1997 e trata-se do primeiro padrão de criptografia utilizado para proteger redes Wi-Fi.

  O WEP foi ***baseado no algoritmo de criptografia RC4***, com trocas de dados encriptados em chaves de segurança de até ***152 bits em caracteres hexadecimais***. Isso significa que as senhas precisam ter, obrigatoriamente, 10, 26 ou 32 dígitos, com números de 0-9 e letras de A-F.

  A chave WEP tem maior vulnerabilidade em comparação com padrões lançados posteriormente, como WPA, WPA2 e WPA3. A utilização da criptografia WEP é desaconselhada e considerada obsoleta pela Wi-Fi Alliance. A maioria dos roteadores Wi-Fi atuais não incluem suporte para a tecnologia.

- *WPA*

  WPA (Wi-Fi Protected Access), foi lançado em 2002 e protege as redes Wi-Fi com o ***protocolo TKIP (Temporal Key Integrity Protocol)*** e utiliza chave de criptografia de ***128 bits para cada pacote transmitido entre o router e o dispositivo***.

  Além de ser mais seguro que o padrão WEP, uma das grandes vantagens fornecidas pelo WPA é a utilização da ***chave pré-compartilhada (PSK)***, que permite um tamanho flexível de senhas para rede Wi-Fi e utilização de ***caracteres não-hexadecimais.***

- *WPA2*

  O WPA2 é a ***atualização*** do padrão WPA, sendo a segunda geração do protocolo WPA. Foi certificado em 2004 e ainda é o modelo de criptografia mais utilizado para proteger redes sem fio. O WPA2 utiliza o ***protocolo de modo CCM (CCMP)***, padrão que substituiu o antigo TKIP e dificulta a identificação de padrões para quebra da segurança dos pacotes transmitidos na rede sem fio.

  O WPA2 também trouxe a ***criptografia do tipo AES*** (Advanced Encryption Standard), que utiliza chaves de até ***256 bits e utiliza chaves iguais para criptografar e descriptografar dados***.

  O WPA2 também introduziu um modo EAP (Extensible Authentication Protocol), voltado para uso empresarial e corporativo também conhecido como WPA2-Entreprise). Com o EAP é possível ter autenticação avançada para múltiplas pessoas através de utilizador e senha, ***sendo necessário utilizar um servidor para controlo de acesso (RADIUS)***.

O WPA2 é baseado no mecanismo de rede de segurança robusta (RSN) e opera em dois modos: ***Modo pessoal*** ou ***chave pré-compartilhada*** (WPA2-PSK) – que depende de uma senha compartilhada para acesso e geralmente é usada em ambientes domésticos.

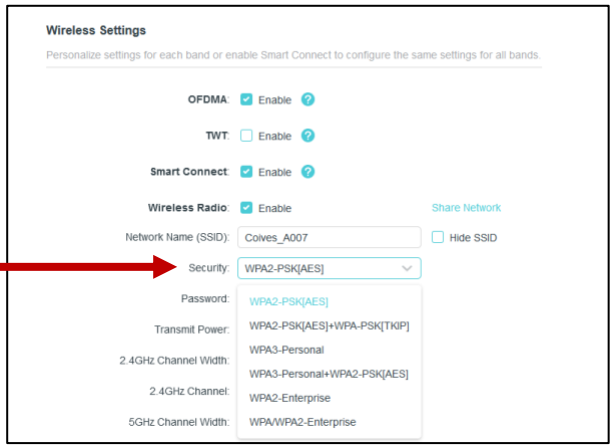
- *WPA3*

WPA3 é a terceira geração do WPA e foi lançado em 2018. A principal característica em comparação com os padrões anteriores é a ***adoção de chaves criptográficas maiores, ou seja, chaves até 256 bits***.

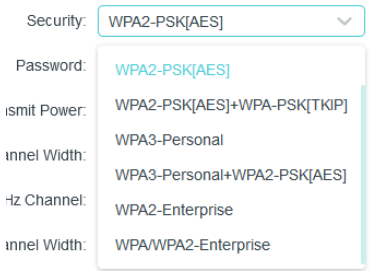
Mais seguro do que os padrões anteriores, o WPA3 utiliza a tecnologia Simultaneous Authentication of Equals (SAE), que protege as redes de ataques de força bruta. O WPA3 também tem suporte via NFC com criptografia individualizada para cada dispositivo adicionado.

Tabela comparativa que detalha o que muda entre WEP, WPA, WPA2 e WPA3:

	WEP	WPA	WPA2	WPA3
Protocolo de criptografia	RC4	TKIP	AES	AES
Método de autenticação	CRC	PSK	PSK	SAE
Tamanho da chave	10, 26 ou 32 dígitos hexadecimais	8 a 64 caracteres	8 a 64 caracteres	8 a 64 caracteres
Dispositivos compatíveis/suporte	Alto	Alto	Alto	Baixo
Nível de segurança	Fraca	Média	Alta	Altíssima

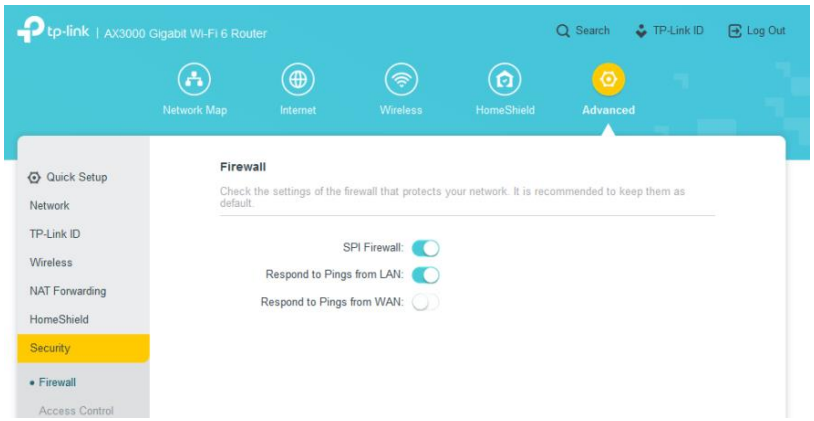


Em termos empresarias, devem sempre que possível acrescer graus de segurança mais elevados, como por exemplo, a utilização criptografia WPA-Entreprise, WPA2-Entreprise ou WPA3-Entreprise (dependendo do que o equipamento consegue suportar).



5 – Ativar a firewall do router

Sempre que possível, verifique se a firewall da rede está ativa no dispositivo. Certos equipamentos trazem a opção para permitir respostas ou bloqueios aos pedidos PING dentro e fora das redes LAN e WAN:



6 – Utilização das frequências de transmissão 2.4GHZ e 5GHZ

Muitas vezes os routers vêm com 2 redes configuradas: rede 2.4 GHZ e 5 GHZ (do qual pode ativar apenas uma das mesmas e indicar o poder de transmissão do sinal).

As principais diferenças entre as ligações Wi-Fi a 2,4 GHz e a 5 GHz são a velocidade e o alcance.

A frequência de 2,4 GHz do *router* Wi-Fi proporciona uma maior área de cobertura e é melhor para atravessar objetos sólidos, embora com uma velocidade máxima da ordem de 150 Mbps.

A frequência de 5 GHz do *router* Wi-Fi oferece maiores velocidades. Contudo, proporciona uma menor área de cobertura e tem maior dificuldade de atravessar objetos sólidos.

Assim, uma transmissão a 2,4 GHz assegura Internet numa área maior, mas a menor velocidade, enquanto uma transmissão a 5 GHz proporciona velocidades maiores, mas menor alcance.

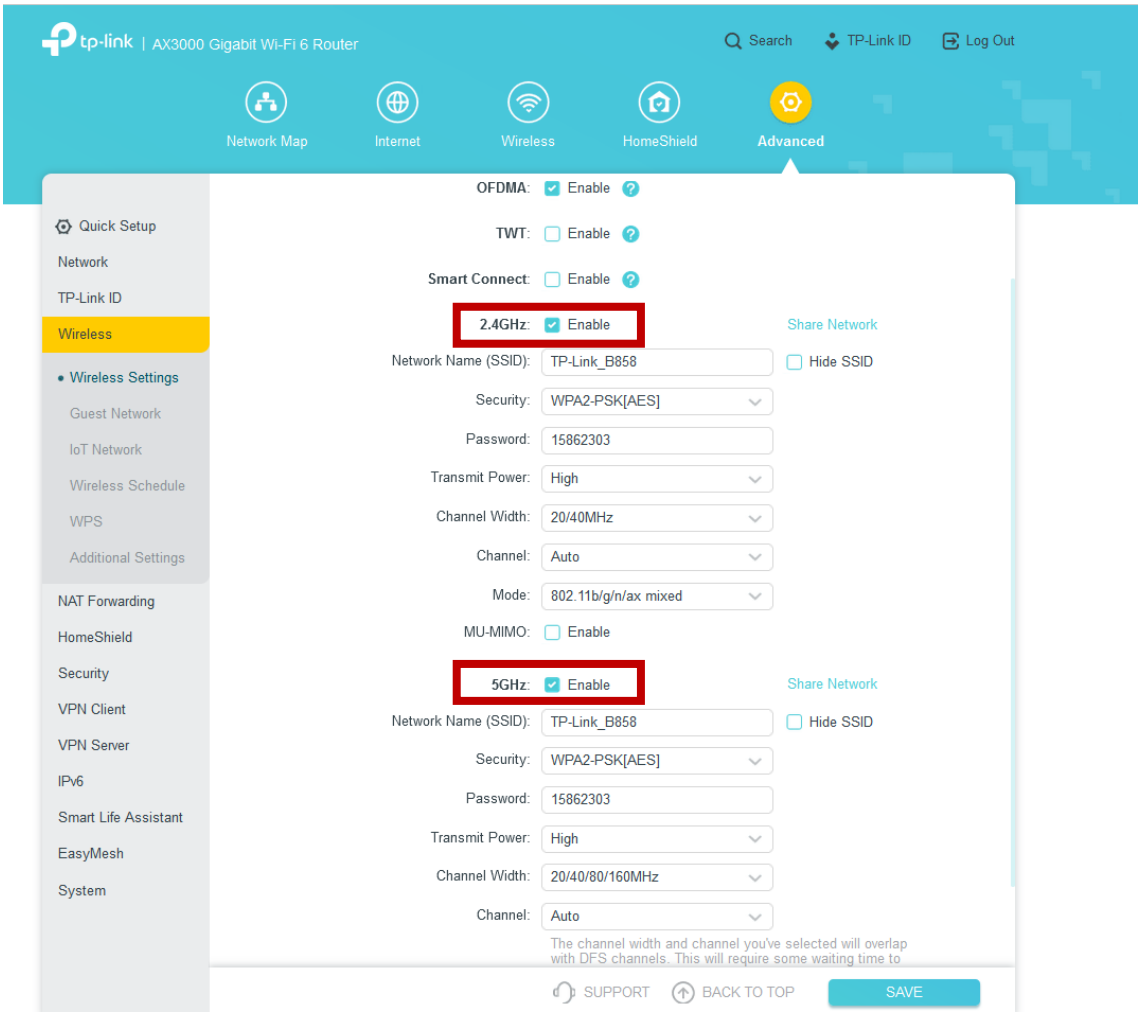
Se pretender um alcance maior para os seus dispositivos, use 2,4 GHz. Se necessitar de uma velocidade maior e puder sacrificar o alcance, use a frequência de 5 GHz.

Interferências

A frequência de 2,4 GHz é mais suscetível a interferências devido também ao número de dispositivos que usam esta faixa de frequências, como *routers* mais antigos, micro-ondas, dispositivos *Bluetooth*, equipamentos de monitorização de bebés, comandos de portas de garagem, entre outros.

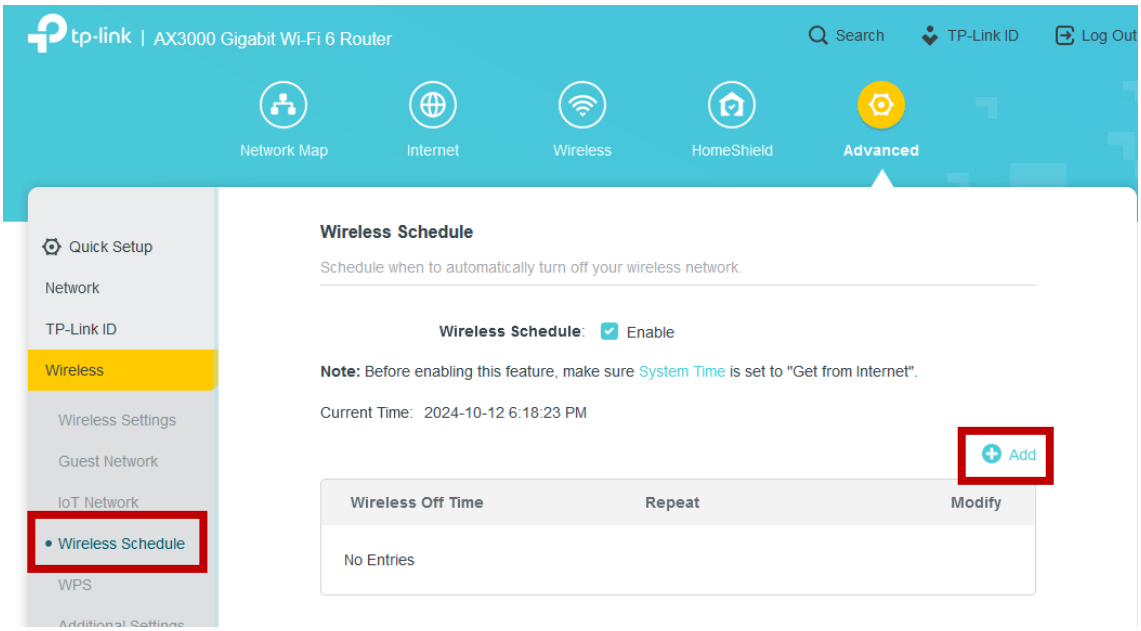
Idealmente, a frequência de 2,4 GHz pode ser usada quando for requerida menor velocidade de acesso, como numa mera navegação na Internet.

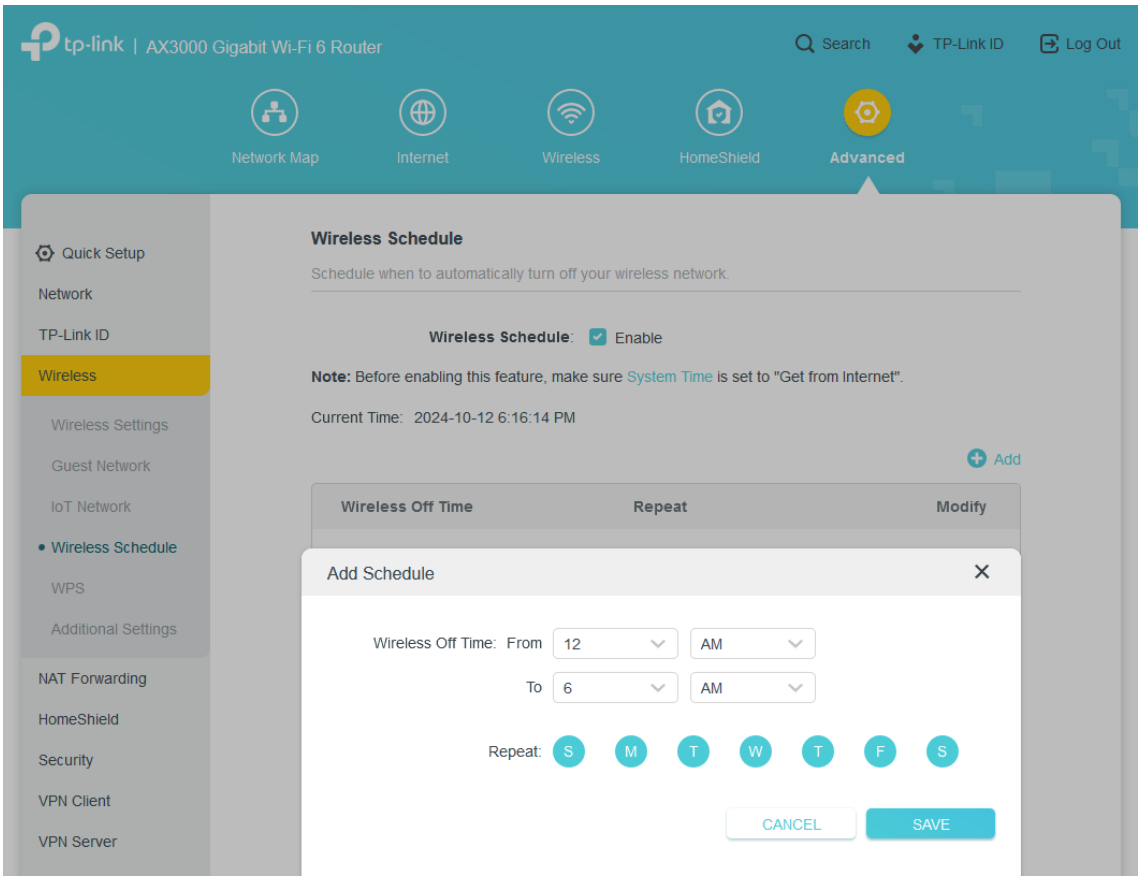
A frequência de 5 GHz é preferível se o dispositivo estiver próximo do *router*/ponto de acesso. É menos suscetível à sobreposição de outros dispositivos, sendo menor o potencial de interferência e proporciona uma ligação Wi-Fi mais rápida. A frequência de 5 GHz é uma opção mais adequada no caso, por exemplo, de jogos *online* ou *streaming* de HDTV.



7 – Colocar limitações de horário na rede

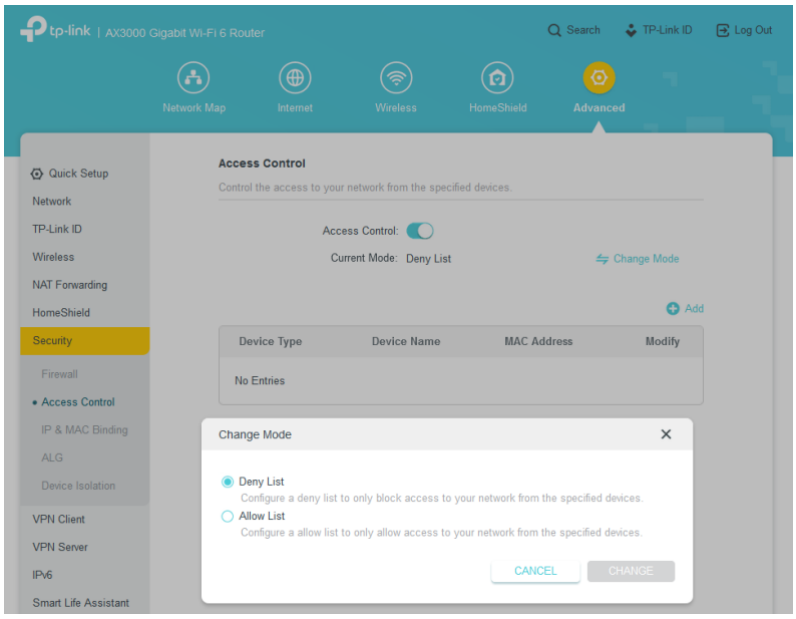
Pode configurar e limitar o acesso a rede por horários. Como por exemplo, se ninguém trabalhar na empresa de noite, pode bloquear o acesso por horário. Alguns exemplos de configuração:



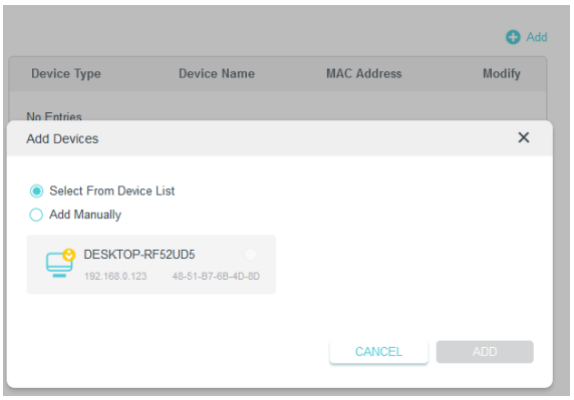


8 - Limitar acessos através de filtragem dos MAC Address

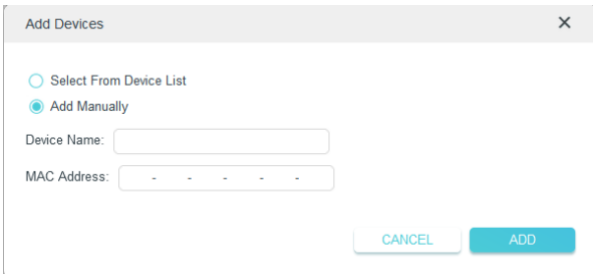
Pode configurar e limitar o acesso a rede pelo endereço MAC das placas de rede. Nos equipamentos de rede poderá dar permissões (WhiteList /Allow List) ou bloquear acesso (BlackList / Deny List):



Indicar pelo nome do equipamento que é detetado na rede:

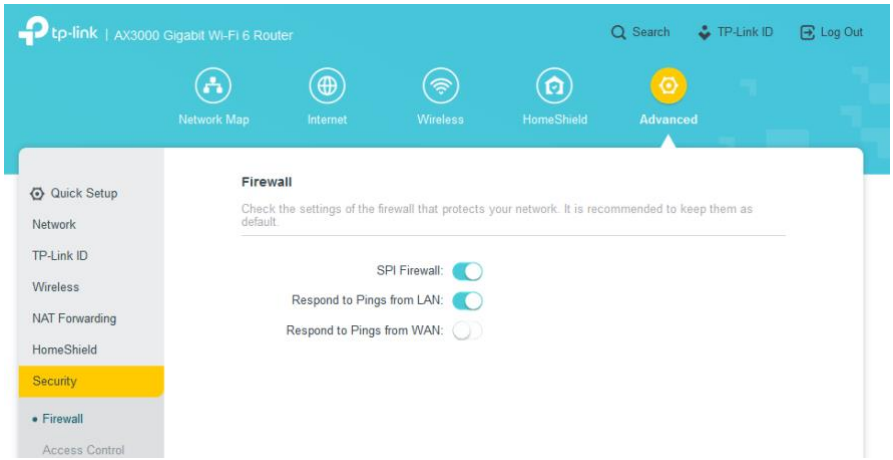


Indicar o endereço do equipamento de forma manual:

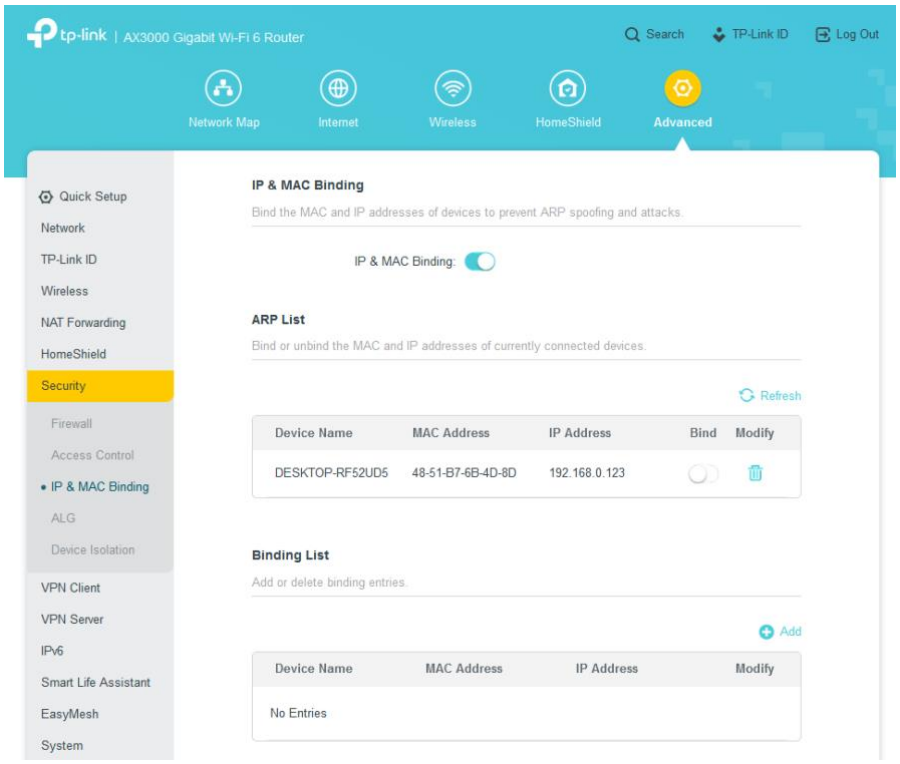


9 - Proteger contra malware e ataques na Internet

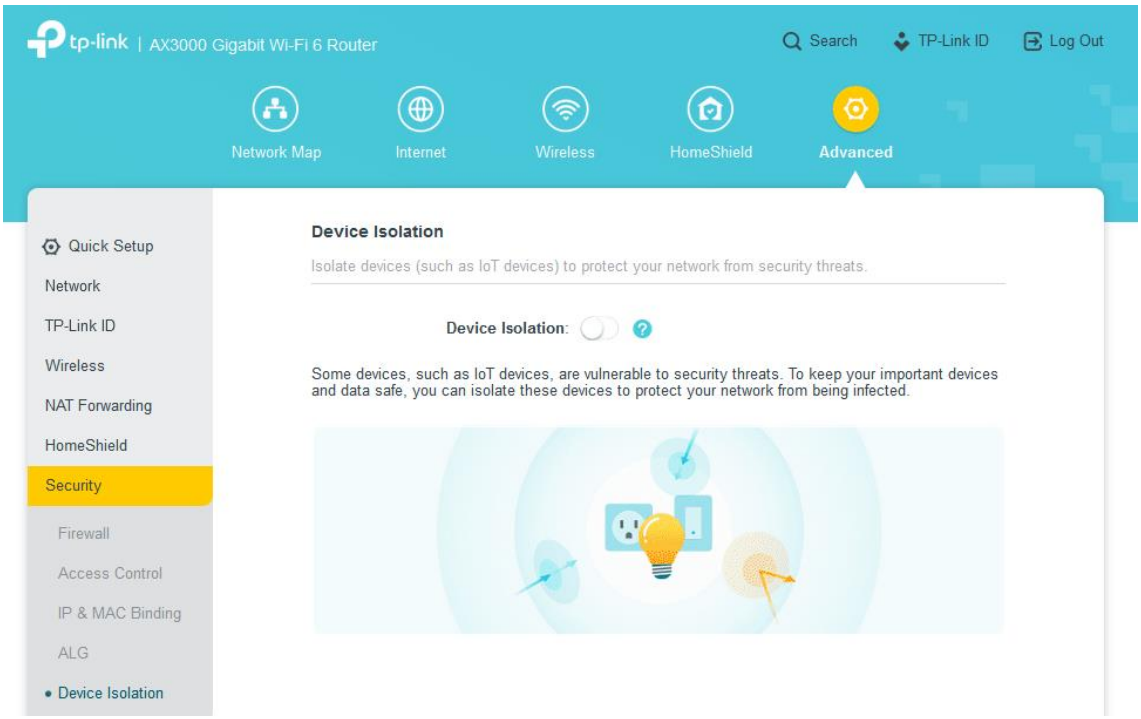
Na gestão de segurança dos equipamentos, deve verificar sempre que possível se tem a firewall ativa:



Verificar se tem a opções para prevenir ataques de pacotes ARP (ARP Spoffing attacks) e colocar a identificação dos equipamentos na lista:



Em equipamentos mais recentes, podemos ativar a proteção para dispositivos inteligentes (IoT). Para tal, ativamos a isolação de sinal do dispositivo, para não haver tentativas de acesso ao equipamento:



10 - Configurar uma rede de convidados

Quando chegam a casa de uma pessoa, escola ou empresa, a primeira coisa que a maioria dos visitantes pede é a senha do Wi-Fi. E a realidade é que em muitas das situações simplesmente compartilham a senha sem pensar nas consequências.

Essa é uma das piores práticas de segurança que pode fazer. Qualquer pessoa com essa senha tem acesso à rede. Um utilizador mal-intencionado pode procurar sistemas vulneráveis e começar com ataques de rede.

Mas também, existe utilizadores sem intenção maliciosa e que podem:

- acidentalmente instalar ou transmitir malware, ransomware, keyloggers e muito mais;
- podem fazer downloads ilegais ou fazer coisas maliciosas pela Internet que seriam rastreadas até o seu endereço IP de origem;

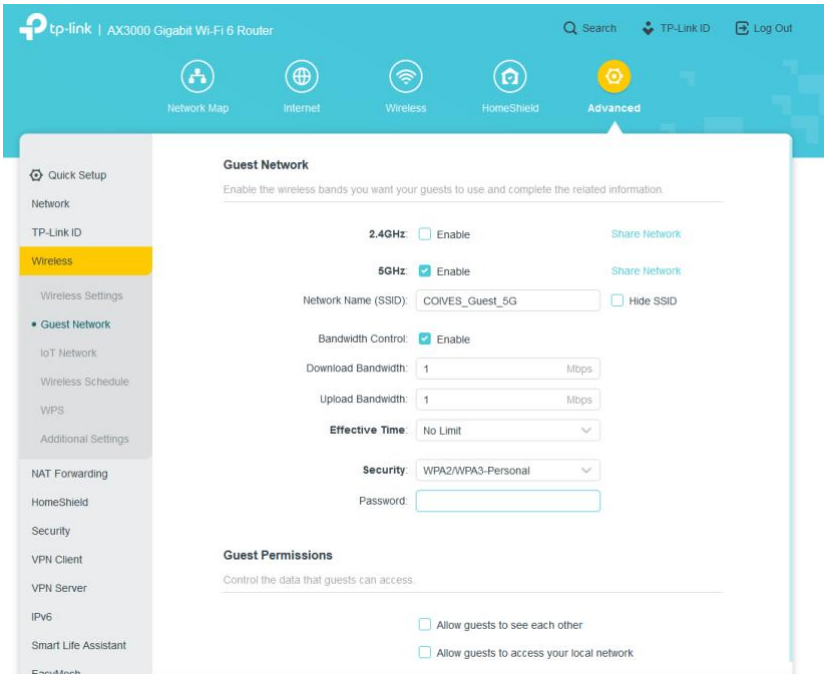
Para tal, vamos criar uma rede apenas para os convidados. A maioria dos routers Wi-Fi e pontos de acesso oferecem essa opção. Isso dá aos utilizadores acesso à Internet e nada mais.

Para configurar esse acesso, faça login no dispositivo como administrador e procure nas configurações do router para “Permitir acesso convidado” ou parecido. Em seguida, selecione um nome (o SSID de transmissão) para a rede e ative os recursos de segurança.

Defina uma senha forte.

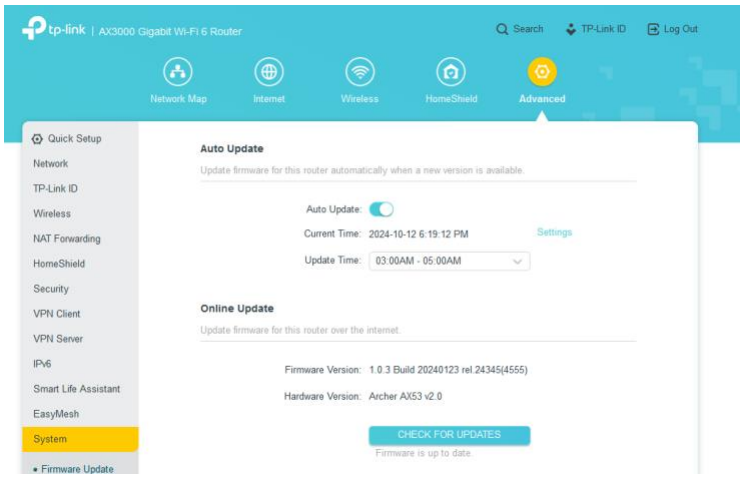
Permitir a encriptação.

E desmarque "Permitir acesso às configurações".

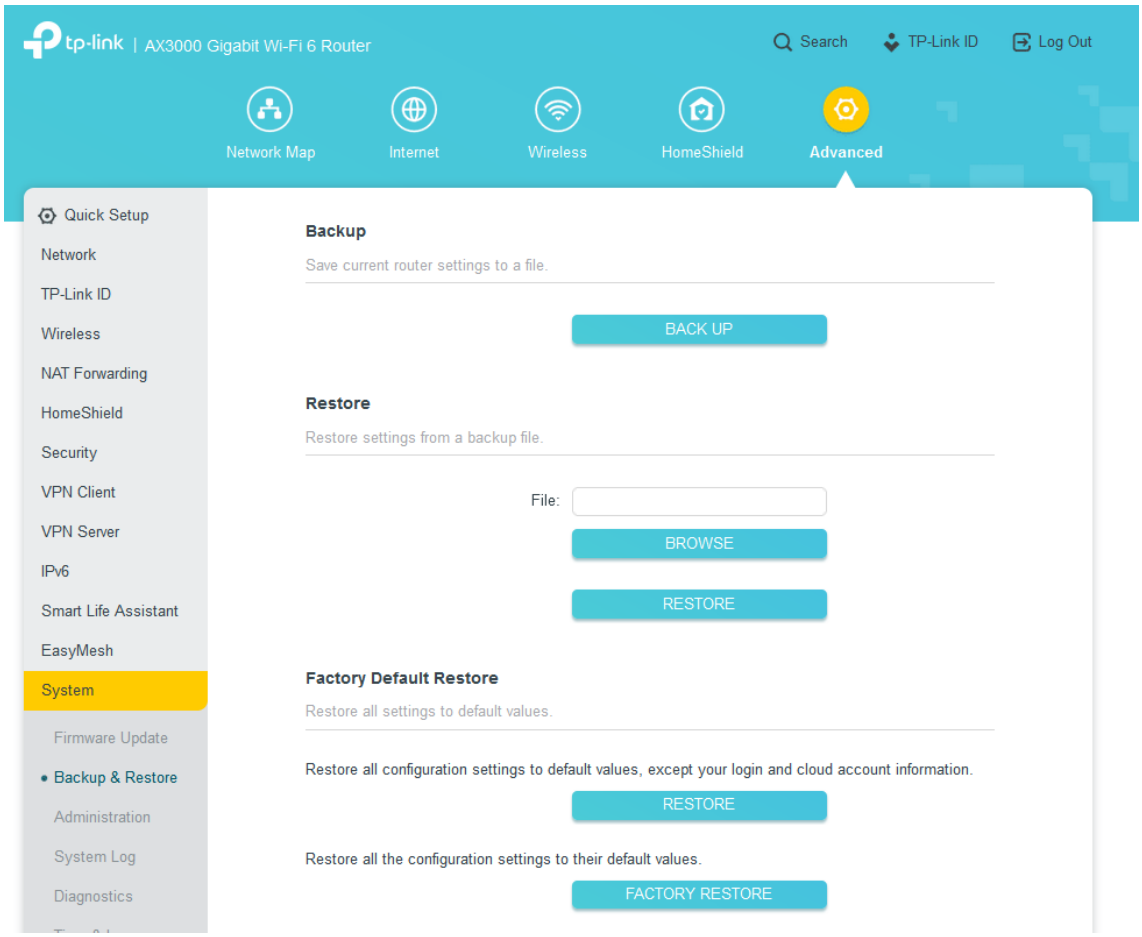


11 – Manter o software do equipamento atualizado

Sempre que possível, deve verificar e realizar as atualizações dos equipamentos para uma maior segurança e funcionamento dos mesmos:



12 – Mantenha um backup das configurações da rede



13 - Limite o acesso físico ao seu equipamento sem fio