1.Configurações de segurança wireless

Uma preocupação óbvia de segurança em redes sem fio é que todas as informações são transmitidas pelo ar. Isso significa que um invasor próximo pode ouvir essa comunicação e, se algo estiver sendo enviado sem criptografia, ele poderá ver tudo o que está sendo transmitido.

Outro desafio é garantir que apenas usuários autorizados possam acessar a rede sem fio. Normalmente, solicitamos um nome de usuário, senha ou algum outro tipo de autenticação quando um dispositivo tenta se conectar pela primeira vez. A configuração padrão da maioria das redes privadas sem fio é criptografar todo o tráfego, garantindo que, mesmo que um invasor intercepte os dados, ele não consiga lê-los.

Além da criptografia, também precisamos garantir que estamos usando protocolos que garantam **integridade** dos dados. Isso significa que qualquer tráfego enviado pela estação de origem deve ser recebido exatamente da mesma forma como foi transmitido. Esse processo de verificação de integridade da mensagem é chamado de **MIC (Message Integrity Check)**.

Por muitos anos, nossas redes sem fio usaram um protocolo de criptografia conhecido como **WPA2** para proteger os dados transmitidos. No entanto, o **WPA2** apresenta uma vulnerabilidade de segurança significativa durante a conexão inicial à rede. Durante essa conexão, ocorre um processo chamado **handshake de quatro vias**, onde um código de autenticação (hash) é gerado. O objetivo de um invasor é capturar esse hash e, em seguida, usar ataques de **força bruta** para tentar descobrir a chave pré-compartilhada (pre-shared key, ou PSK).

Com o avanço das tecnologias, novas formas de ataques foram desenvolvidas para quebrar senhas de forma mais eficiente. Hoje, é possível usar **processadores gráficos (GPUs)** ou até mesmo **serviços de computação em nuvem** para realizar ataques de força bruta que podem quebrar a senha de uma rede WPA2 em questão de dias. Isso se torna um problema especialmente em redes domésticas, onde todos os dispositivos usam a mesma chave pré-compartilhada para se conectar.

Para solucionar essa vulnerabilidade, foi desenvolvido o **WPA3**, que introduziu novas tecnologias para evitar ataques de força bruta. Um dos principais avanços é o uso de um novo modo de cifra chamado **GCMP (Galois Counter Mode Protocol)**, que oferece uma criptografia mais forte do que a utilizada no WPA2. O GCMP também inclui um **código de autenticação de mensagem Galois**, garantindo maior integridade dos dados.

Com o **WPA3**, o processo de autenticação e handshake foi completamente reformulado. Agora, há uma autenticação mútua entre o **dispositivo cliente** e o **ponto de acesso**, e as chaves de sessão são geradas diretamente nos dispositivos, em vez de

serem transmitidas pela rede. Como o **handshake de quatro vias** do WPA2 foi removido, não há mais um hash de sessão disponível para que um invasor possa capturá-lo e quebrá-lo por força bruta.

Esse novo método de derivação de chaves no **WPA3** é chamado de **SAE (Simultaneous Authentication of Equals)** e é baseado no protocolo de **troca de chaves Diffie-Hellman**. Com essa mudança, cada dispositivo conectado à rede recebe uma chave de sessão única, mesmo que todos utilizem a mesma chave pré-compartilhada. Isso significa que um usuário conectado à rede não pode mais ver o tráfego de outro usuário, aumentando a privacidade e segurança.

O método de troca de chaves do WPA3 foi adotado pelos **padrões IEEE**, e às vezes ele é referido como **dragonfly handshake** nos documentos técnicos. O WPA3 trouxe uma ênfase maior na segurança do processo de autenticação, o que é essencial, pois os usuários podem estar conectando-se à rede de qualquer lugar.

A autenticação na rede sem fio pode ser feita de duas maneiras principais. O método mais comum em redes domésticas é o uso de **chaves pré-compartilhadas (PSK - Pre-Shared Key)**, onde todos os dispositivos utilizam a mesma senha para acessar a rede. No entanto, em ambientes corporativos, esse método é considerado inseguro.

Para resolver esse problema, as empresas utilizam um método de autenticação centralizada baseado no **padrão 802.1X**. Esse tipo de autenticação exige que os usuários forneçam um **nome de usuário e senha** ao tentar se conectar à rede. O sistema valida as credenciais antes de conceder acesso à rede, garantindo que apenas usuários autorizados possam se conectar.

Se você acessar as configurações de Wi-Fi no seu **roteador doméstico** ou em um ponto de acesso sem fio, verá várias opções de segurança. Algumas dessas opções incluem:

- **Open System** (Sistema Aberto) ou **None** (Nenhuma) – Indica que a rede não possui qualquer tipo de autenticação ou criptografia.
- **WPA3-Personal** – Também chamado de **WPA-PSK (Pre-Shared Key)**, que exige que todos os dispositivos utilizem a mesma senha para se conectar à rede.
- **WPA3-Enterprise** – Também conhecido como **WPA3-802.1X**, que exige um nome de usuário e senha e usa um **servidor de autenticação centralizado** baseado em **RADIUS, LDAP ou TACACS**.

O **servidor de autenticação centralizado** é frequentemente chamado de **servidor AAA (Authentication, Authorization, Accounting)**, que gerencia os acessos à rede. O processo AAA inclui três etapas principais:

1. **Autenticação** – O usuário fornece suas credenciais (nome de usuário e senha), que são verificadas pelo servidor.
2. **Autorização** – Define quais recursos o usuário pode acessar dentro da rede após ser autenticado.
3. **Contabilização (Accounting)** – Registra informações sobre o acesso, como horário de login, tempo de conexão e quantidade de dados transferidos.

Por exemplo, se você estiver acessando uma **VPN corporativa**, o servidor AAA verificará suas credenciais antes de conceder acesso à rede interna da empresa.

Um dos protocolos mais utilizados para autenticação é o **RADIUS (Remote Authentication Dial-In User Service)**, que permite centralizar a autenticação de dispositivos na rede. Esse protocolo é amplamente suportado por roteadores, switches, servidores e VPNs. Sempre que você digita um nome de usuário e senha para se conectar a um recurso de rede, suas credenciais provavelmente estão sendo verificadas por um servidor **RADIUS**.

Outro recurso essencial para redes empresariais é o **802.1X**, também chamado de **Network Access Control (NAC)**. Esse protocolo impede que qualquer dispositivo se conecte à rede sem antes passar por um processo de autenticação. O **802.1X** pode ser usado tanto em **redes sem fio** quanto em **redes cabeadas** e, geralmente, trabalha em conjunto com um **servidor AAA**, como **RADIUS, LDAP ou TACACS**.

A autenticação 802.1X utiliza o **EAP (Extensible Authentication Protocol)**, um protocolo que permite diferentes métodos de autenticação, como certificados digitais e autenticação multifator. Como o EAP é altamente flexível, os fabricantes podem personalizar o processo para atender às necessidades específicas da empresa.

O processo de autenticação 802.1X geralmente envolve três partes:

1. **O suplicante (Supplicant)** – O dispositivo tentando acessar a rede.
2. **O autenticador (Authenticator)** – O ponto de acesso ou switch que solicita credenciais do dispositivo.
3. **O servidor de autenticação (Authentication Server)** – O servidor AAA que verifica as credenciais do usuário.

Quando um usuário tenta se conectar à rede, o autenticador impede o acesso até que ele forneça credenciais válidas. Essas credenciais são enviadas para o servidor de autenticação, que valida as informações e, se aprovadas, concede acesso à rede.

Esse processo acontece rapidamente e, na maioria das vezes, o usuário não percebe toda a comunicação acontecendo em segundo plano. Desde que o nome de usuário, senha e outros fatores de autenticação estejam corretos, o protocolo **802.1X e EAP** cuidará de todo o restante.