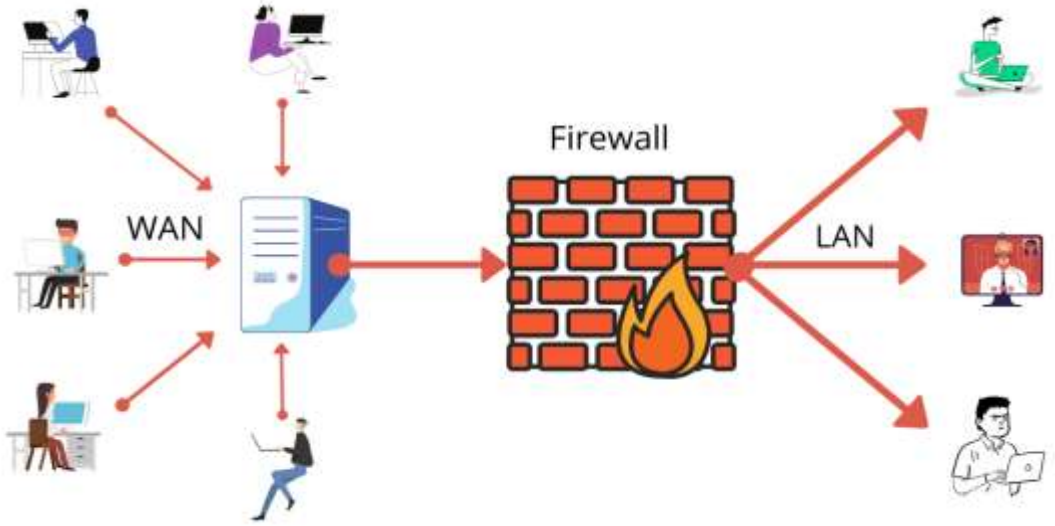
Securing Wireless Stations, Wi-Fi and IoT



Securing Wireless Stations

In today's connected world, almost everyone has at least one internet-connected device. With the number of these devices on the rise, it is important to implement a security strategy to minimize their potential for exploitation

The following ways are used to improve the network security in wireless infrastructure

- Understand Wireless Network Threats
- Choose the Right Wireless Equipment
- Set Up a Strong Network Encryption
- Practice Proper SSID Management

Securing Wireless Stations

- Implement MAC Address Filtering
- Set Up Effective Network Segmentation and Guest Networks
- Complete Regular Firmware Updates
- Consider Advanced Security Features
- Don’t Underestimate the Value of Employee Training and Policies
- Conduct Ongoing Monitoring and Regular Audits
- Take Intentional Steps to Strengthen Network Security

Securing Wireless Stations

Choose the Right Wireless Equipment

- Investing in top-tier wireless equipment is the first line of defense.
- Business operations demand reliability and robust security, far beyond what consumer-grade gear offers.
- Unlike their consumer counterparts, these devices typically have enhanced security features, better range, and the ability to handle a higher number of connected devices.
- Industry-leading brands are renowned for offering equipment specifically tailored for corporate needs. Also, make sure to prioritize devices that come with regular security updates and patches.
- The right equipment acts as a solid foundation, ensuring both performance and security for the network's entire lifespan.

Securing Wireless Stations

Set Up a Strong Network Encryption

Wired Equivalent Privacy (WEP): Once hailed for its pioneering approach to Wi-Fi security, WEP now stands as an outdated relic. Its static encryption keys make it susceptible to contemporary hacking techniques. Given its vulnerabilities, WEP is now practically obsolete and should be avoided.

Wi-Fi Protected Access (WPA): A step up from WEP, WPA brought dynamic encryption keys into the picture, presenting a tougher challenge for potential hackers; however, as cybersecurity is an ever-evolving field, WPA's own vulnerabilities became apparent over time. Today, it is seldom the choice for businesses that are aware of its limitations.

Securing Wireless Stations

Set Up a Strong Network Encryption

Wi-Fi Protected Access II (WPA2): Building on WPA's foundation, WPA2 ushered in enhanced security protocols, making it a staple for many networks; however, it is not immune to threats, the most notorious being the KRACK (Key Reinstallation Attack), whic exploits weaknesses in the WPA2 protocol to compromise network security.

Wi-Fi Protected Access III (WPA3): WPA3 is generally considered the gold standard of Wi Fi encryption. Launched in 2018, WPA3 not only patched the vulnerabilities found in WPA2 but also introduced cutting-edge features. With individualized data encryption, even open networks become more secure, reducing the risks associated with man-in-the-middle attacks. Additionally, its resistance to brute-force attacks ensures encrypted data remains inaccessible to unauthorized entities.

Securing Wireless Stations

Practice Proper SSID Management

A Service Set Identifier (SSID) is essential for wireless network's name.

When naming SSIDs, it's wise to avoid direct references to the business name or any sensitive identifiers, as these can give malicious actors clues about potential targets.

Also, disabling the SSID broadcast or hiding it can make it harder for outsiders to pinpoint and exploit.

Implement MAC Address Filtering

Every device on your network has a unique Media Access Control (MAC) address. By setting up MAC address filtering, you essentially create an exclusive list, permitting only known devices to connect to the network, like a VIP list for a private event. It acts as an added layer of protection, making unauthorized access significantly tougher for intruders.

Securing Wireless Stations

Set Up Effective Network Segmentation and Guest Networks

Network segmentation can help you achieve improved security through intentional divisio

By creating Virtual Local Area Networks (VLANs), different departments can operate on separate networks, each tailored to its specific needs.

This not only optimizes performance but ensures that a breach in one segment doesn't compromise the entire network.

Additionally, guest networks serve as isolated lanes for visitors. Rather than providing access to the primary network, businesses can offer guests a separate network, ensuring that their traffic is completely isolated from sensitive business operations. A guest network acts as a buffer, minimizing risks associated with unknown devices.

Securing Wireless Stations

Complete Regular Firmware Updates

The firmware acts as the brain behind your networking equipment, so it is vital to keep it safe.

Keeping firmware up to date is paramount, as updates often contain security patches addressing known issues.

Failing to update can leave doors open for exploitation. Some modern devices offer automated updates, but if yours doesn't, set regular reminders.

Periodically visiting the manufacturer's website or using dedicated software tools can help you ensure you're armed with the latest defense mechanisms against emerging threats.

Securing Wireless Stations

Consider Advanced Security Features

Virtual Private Networks (VPNs) create encrypted passages for data transmission, ensurin that even if data packets are intercepted, they remain undecipherable. For businesses, deploying VPNs for remote workers or accessing the business network from outside locations is crucial.

Firewalls act as gatekeepers, deciding which traffic enters or exits based on preset rules. They are instrumental in fending off unwanted access attempts or malicious content.

Intrusion Detection Systems (IDS) continuously monitor the network, raising alarms for any suspicious activities.

Intrusion Prevention Systems (IPS) detect and then actively block or prevent suspicious activities, thwarting potential breaches in real-time.

Securing Wireless Stations

Employee Training and Policies

To prevent social engineering attack, employee training is indispensable.

Regular sessions highlighting the latest cyber threats, phishing schemes, and best practices can create a vigilant workforce.

Establishing robust policies (like mandating strong passwords, cautioning against unknown email attachments, or regulating device usage) creates a culture of security consciousness.

Remember, a well-informed team is a business's last line of defense.

Securing Wireless Stations

Conduct Ongoing Monitoring and Regular Audits

Deploying network monitoring tools provides real-time insights into traffic patterns, bandwidth usage, and any anomalies.

This proactive approach can identify potential threats before they escalate.

Furthermore, periodic security audits—assessing the network's current defenses, scanning for vulnerabilities, and ensuring compliance with security standards—are paramount. These audits provide a roadmap for necessary upgrades or modifications.

In cybersecurity, complacency can be costly. Regular monitoring and audits

Securing Wireless Stations

Take Intentional Steps to Strengthen Network Security

Building a secure wireless network is a commitment to safeguarding your business's digital assets, reputation, and future growth. By combining cutting-edge technologies with proactive strategies and a well-informed workforce, you can ensure robust defense against the myriad of cyber threats lurking in the digital realm.

As technology evolves, so do cyber threats, making continuous vigilance an adaptability crucial. Regularly revisiting and refining your network security strategies can help you be confident that your wireless network is as safe an

Securing Wi-Fi

Securing Wi-Fi

When wireless devices in a network are "open" or unsecured, they're accessible to any Wi-Fi-enabled device, such as a computer or smartphone, that's within range of their wireless signals.

Using open or unsecured networks can be risky for users and organizations. Adversaries using internet-connected devices can collect users' personal information and steal identities, compromise financial and other sensitive business data, "eavesdrop" on communications, and more.

Securing Wi-Fi

One basic best practice for Wi-Fi security is to change default passwords for network devices.

Media Access Control (MAC) addresses -Another basic approach to Wi-Fi security is to use MAC addresses, which restrict access to a Wi-Fi network.

Encryption-A more common method of protecting Wi-Fi networks and devices is the use of security protocols that utilize encryption. There are several types of encryption standards in use today, including Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2).

Securing Wi-Fi

Virtual private networks (VPNs)-VPNs are another source of Wi-Fi network security. They allow users to create secure, identity-protected tunnels between unprotected Wi-Fi networks and the internet.

Security software-A vast array of security software aimed at the consumer and enterprise markets can provide protection to wireless networks and Wi-Fi-enabled devices such as routers, switches, controllers, and access points. Many of these solutions are downloadable to wireless LANs (WLANs) and mobile devices. Some newer software solutions designed to secure Wi-Fi are built into the backbone of the internet and are available via cloud platforms.

Securing Wi-Fi

Types of wireless security protocols

WEP-The first wireless security protocol was WEP (Wired Equivalent Privacy). It used only basic (64-/128-bit) encryption. WEP is no longer considered secure and should be replaced by a newer protocol such as WPA2.

WPA- WPA (Wi-Fi Protected Access) was developed in 2003. It delivers stronger (128-/256-bit) encryption than WEP by using a security protocol known as Temporal Key Integrity Protocol (TKIP).

Securing Wi-Fi

Types of wireless security protocols

WPA2- WPA2, a later version of WPA, was developed in 2004. It's easier to configure and provides even greater network security than WPA by using a security protocol known as the Advanced Encryption Standard (AES).

WPA3-A new generation of WPA, known as WPA3, is designed to deliver simpler configuration and even stronger (192-/256-/384-bit) encryption and security than any of its predecessors. It is also meant to work across the latest Wi-Fi 6 networks.

Securing Wi-Fi

Types of Wi-Fi network security devices

Active device - There are several types of commercially available devices that can provide network security by blocking adversarial attacks and unwanted network traffic. One type is known as an "active" device, which is **hardware** configured to block surplus network traffic. Examples of these devices for Wi-Fi network security include firewalls, antivirus scanners, and content-filtering devices.

Securing Wi-Fi

Types of Wi-Fi network security devices

Passive device- Passive Wi-Fi network security devices detect and report on unwanted network traffic. Passive devices use less power than other Wi-Fi devices. They also have an extra layer of security because they can communicate with Wi-Fi routers only when the routers are seeking them. That extra layer makes man-in-the-middle (MITM) attacks more difficult. In an MITM attack, an adversary attempts to intercept communications between two parties to "listen in" on their activity or to modify the traffic traveling between them.

Securing Wi-Fi

Types of Wi-Fi network security devices

Preventive device-A preventive device, such as a wireless intrusion prevention system (WIPS), can scan networks to identify potential security issues. A WIPS can be integrated into networks or overlaid using standalone sensors. Some WIPSs, however, conduct only intermittent monitoring, leaving networks occasionally vulnerable.

Securing Wi-Fi

Types of Wi-Fi network security devices

Unified threat management (UTM) systems- UTM systems incorporate vital elements of network security: firewalls, content filtering, VPN, antivirus detection, and others. A UTM system offers a simplified way to integrate multiple security functions. It provides these functions at a single point on the network, eliminating the need for point solutions from multiple vendors.

UTM devices can be network hardware appliances, virtual appliances, or cloud services.

Securing IoT

Securing IoT

- Internet of Things (IoT) devices are computerized Internet-connected objects, such as networked security cameras, smart refrigerators, and WiFi-capable automobiles.
- IoT security is the process of securing these devices and ensuring they do not introduce threats into a network.
- Security was not considered during the design of IoT devices. The constant diversity and expansion of IoT devices and communication channels raises the possibility that cyber attacks may target your

Securing IoT

- IoT devices are increasingly part of everyday life, and both consumers and businesses may face IoT security challenges.
- Anything connected to the Internet is likely to face attack at some point. Attackers can try to remotely compromise IoT devices using a variety of methods, from credential theft to vulnerability exploits.
- Once they control an IoT device, they can use it to steal data, conduct distributed denial-of-service (DDoS) attacks, or attempt to compromise the rest of the connected network.

How Does IoT Security Work?

- IoT devices are any devices that can store data by connecting to the cloud.
- IoT devices need a special set of cyber security guidelines because they differ from conventional mobile devices. They lack the benefit of built-in security guidelines seen in mobile operating systems like iOS and Android.
- A lot of information is stored in the cloud, if an attacker manages to get access to the user's account, it might be exploited for identity theft or privacy invasion.
- Although there isn't a single solution for IoT security, cybersecurity experts have made it their mission to inform manufacturers and developers about secure coding practices and how to strengthen cloud activity defences

Importance of IoT Security

- Cyberattacks are a continual concern because of the unusual way that Io devices are manufactured and the enormous volume of data they proces
- Strong IoT security is desperately needed, as seen by the regular threat o vulnerabilities, data breaches, and other dangers related to the use of Io devices.
- IoT Security thus has a huge role in various industries because most of them are getting interconnected. Industries like health care, Manufacturing, Transportation ,Financial, Retail ,Government and agriculture need IoT security.

Types of IoT Security

IoT security encompasses a multi-layered approach to protect devices, networks, and data. It involves both user and manufacturer responsibilities.

1. Network Security
2. Device Security
3. Data Security

Network Security

This focuses on safeguarding the overall IoT network infrastructure. It involves:

Establishing a strong network perimeter: Implementing firewalls, intrusion detection systems, and access controls to prevent unauthorized entry.

Enforcing zero-trust architecture: Assuming every device and user is potentially malicious, requiring continuous verification.

Securing network communication: Encrypting data transmitted between devices and using secure protocols.

Device Security

This centers on protecting individual IoT devices:

Embedded security agents: Employing lightweight software to monito
device behavior and detect anomalies.

Firmware hardening: Ensuring device software is free from vulnerabilities through rigorous testing and updates.

Secure boot process: Verifying the integrity of the device's operating system before startup.

Data Security

This safeguards the information generated and transmitted by IoT devices:

Data encryption: Protecting data both at rest and in transit using strong encryption algorithms.

Data privacy: Implementing measures to protect sensitive information from unauthorized access.

Data integrity: Ensuring data accuracy and consistency through checksums and other techniques.

How to protect IoT systems and devices?

- **DNS filtering:** Using the Domain Name System to restrict harmful websites is known as DNS filtering. When DNS filtering is added to a network including IoT devices, it stops such devices from connecting to domains that are not authorized.
- **Encryption:** Without encryption, data transfers between IoT devices are susceptible to on-path and external attackers while travelling over the network. Consider encryption as a means of protecting a letter's contents during transit via the postal service, similar to an envelope.

How to protect IoT systems and devices?

- **Device authentication:** Internet of Things (IoT) devices are connected to servers, other networked devices, and one other. All connected devices must undergo authentication to prevent unwanted inputs or requests from third parties.
- **Security of credentials:** If at all feasible, IoT device admin credentials must be updated. It is recommended to avoid sharing login credentials between various apps and devices, instead every device should have its password. In doing so, credential-based attacks are less likely.

Tools to Secure IoT Devices

ForeScout Platform:

This protects and ensures on a network the consent of all managed and unmanaged devices, including IT, IoT, and OT devices, using zero trust principles.

Microsoft Defender for IoT:

Microsoft Defender for IoT helps enterprises manage, discover, and protect their IoT and OT devices. Extra features include network and device threat monitoring around the clock, identifying every asset and device.

Tools to Secure IoT Devices

Asimily:

Asimily is a complete IoT security platform that focuses on medical and laboratory equipment.

AWS IoT Device Defender:

AWS IoT Device Defender is Amazon's Internet of Things security management service. AWS IoT Device Defender allows administrators to authorize security measures such as authentication and permission.