SECURE WLAN PROPOSAL AND DESIGN

This document contains a complete proposal for a Secure WLAN implementation including hardware, software, and feature recommendations.

Jordan Patterson

2024

Table of Contents

Why CISCO? 2

Business case: 2

Cost Savings 2

Improved Collaboration 2

Increased Efficiency 2

Support for Modern Applications 2

Enhanced Security Features 2

Business Continuity 2

High level wireless LAN architecture and design 3

Vendor Selection: Cisco 3

Access Points (AP) and Controllers models for the headquarters and branch offices: 3

Integration with the Existing Network 3

SSID Design 3

Encryption and authentication method and implementation 4

Internal Corporate Network 4

BYOD network 4

Guest network 4

Fast roaming in the headquarters 4

Features of CISCO Catalyst 9166D1 for Fast Roaming: 4

Role-base access control & BYOD management 5

Wireless LAN management and monitoring 5

Security Policy Regarding WLAN 6

Password management 6

Reevaluate the WPA3 transition and apply WPA3-Enterprise 192-Bit if applicable 6

STA isolation and filtering 6

Avoid A-MSDU flag manipulation attacks 6

References 7

Why CISCO?

I chose cisco as the vendor, there are less expensive options out there, but cost was not a consideration in this exercise. Here are some non-technical reasons why we chose cisco:

- Cisco is a well-established and trusted brand in the networking industry. Their reputation for reliability and quality provides peace of mind to businesses.
- Cisco offers extensive customer support as well as a global presence, ensuring that help is available whenever and wherever it's needed.
- Cisco provides comprehensive training and certification programs, such as the Cisco Networking Academy, which can help employees develop their skills and advance their careers.
- Cisco has a vast network of partners and a strong ecosystem, which can provide additional resources and support for businesses.
- Cisco is known for its commitment to corporate social responsibility, including initiatives in education, sustainability, and community development.

Business case:

Implementing a wireless LAN can bring lots of advantages to a company, enhancing productivity and driving overall business growth. Here is a list of reasons to adopt a WLAN:

Cost Savings

- WLAN minimizes the need for extensive cabling and infrastructure compared to wired networks reducing upfront infrastructure costs.
- Wireless networks generally require less maintenance and can be easier to manage with centralized control systems reducing maintenance costs.
- Adding new devices or users to a wireless network is simpler and more cost-effective than wired alternatives making expansion with company growth easier and more cost effective.
- Employees can move freely within the office environment, enhancing mobility and productivity.

Improved Collaboration

- Employees can collaborate more effectively by accessing shared resources and communicating in real-time from any location within the office.
- WLAN supports remote work environments, allowing employees to connect seamlessly from various locations.

Increased Efficiency

- Employees can access company resources, files, and data quickly and efficiently, improving decision-making and reducing downtime.
- Employees can work from different locations within the office, enhancing flexibility and responsiveness.

Support for Modern Applications

- WLAN facilitates the use of cloud-based applications and services, streamlining workflows and improving productivity.
- A wireless network can support IoT devices, improving operational efficiency.

Enhanced Security Features

- Modern WLAN solutions come with security features that protect sensitive data and ensure network integrity.
- Centralized management tools allow for efficient monitoring and control of network access, mitigating potential security risks.

Business Continuity

- A WLAN can provide redundancy and minimize disruptions during infrastructure changes or maintenance, ensuring business continuity.

Investing in a wireless LAN can provide a firm with lots of strategic advantages, from cost savings and improved productivity. As businesses continue to adapt to evolving technological landscapes, WLAN offers the flexibility and scalability needed to support growth and innovation.

High level wireless LAN architecture and design

Vendor Selection: Cisco

Cisco is chosen for its reliability, security, and high-performance network solutions. Their products offer excellent integration capabilities, robust security features, and comprehensive support along with the next gen technologies making them ideal for the needs of Wealth Management Co. Being a Financial firm the security of the data and the reputation of the company is paramount and so we are choosing an industry pioneer like CISCO who has a reliable track record for their product lineups as the vendor for this WLAN architecture.

Access Points (AP) and Controllers models for the headquarters and branch offices:

Access Points (APs): The **Cisco Catalyst 9166D1** Access Point is a high-performance device engineered for demanding environments. Leveraging Wi-Fi 6E technology, it offers enhanced bandwidth, reduced latency, and improved capacity compared to its predecessors. The D1 model's integrated directional antenna makes it particularly suitable for areas with high ceilings or specific coverage needs.

In terms of security, the 9166D1 incorporates advanced features such as WPA3, enhanced encryption protocols, and intrusion detection systems. Its versatility is evident in its support for both on-premises and cloud-managed environments, providing flexibility in network administration. Additionally, the device includes integrated sensors and IoT radios, facilitating Internet of Things applications.

Wireless LAN Controllers: The **Cisco CW9800 Wireless LAN Controller** series is designed to manage large-scale wireless networks, making it an ideal solution for headquarters and multiple branch offices. These controllers offer high performance, efficiently managing numerous access points and clients. They incorporate robust security measures to safeguard the wireless network and seamlessly integrate with Cisco Catalyst Center for centralized network management and visibility. Advanced functionalities, such as machine learning algorithms for network optimization and troubleshooting, further enhance their capabilities.

For guest networks: The **Cisco Meraki MR57** Access Point presents an optimized solution. This device supports Wi-Fi 6E, ensuring high performance and capacity in guest Wi-Fi environments. Managed through the Meraki cloud platform, it offers straightforward configuration and monitoring. The MR57 includes built-in security features to protect guest networks from unauthorized access and supports OWE, captive portal functionality for guest authentication and onboarding.

Integration with the Existing Network

The wireless LAN will integrate seamlessly with the existing wired network infrastructure. The CISCO CW9800 Controllers at the headquarters will be connected to the core switches, ensuring efficient traffic management and network stability. The branch offices' APs will connect to the local switches, which in turn connect to the headquarters via secure VPN tunnels, ensuring secure and reliable connectivity.

SSID Design

To accommodate various security requirements across different network segments, a tiered approach can be implemented. For guest networks (Guest-WealthMgmt_Co) and BYOD (Bring Your Own Device) environments (BYOD-WealthMgmt_Co), a WPA3 and WPA2 transition mode can be employed. This configuration ensures compatibility with a wide range of devices while still offering enhanced security. In contrast, the internal corporate network (Internal-WealthMgmt_Co) can be configured to use WPA3 Enterprise exclusively, providing the highest level of security for sensitive business operations.

The BYOD (Bring Your Own Device) network is implemented as a dedicated SSID for employee's personal devices, providing secure access to corporate resources. This network utilizes WPA3-Enterprise/WPA2-Enterprise mixed mode for robust security, ensuring data protection and user authentication.

Network segmentation is achieved through VLANs, isolating BYOD traffic from other corporate network segments. This approach enhances security and simplifies network management. Authentication can be handled by Cisco, identify services Engine with additional security provided by a certificate-based system using the company's internal Public Key Infrastructure (PKI).

A Network Access Control (NAC) solution is to be deployed to enforce security policies, assessing device compliance before granting network access. For secure remote access, BYOD devices are required to use a VPN client, such as Cisco AnyConnect, creating encrypted tunnels for data transmission.

Role-Based Access Control (RBAC) can be implemented to manage access levels, with dynamic VLAN assignment based on user roles. This ensures appropriate resource access, while maintaining security. Additionally, a Mobile Device Management (MDM) solution can also be integrated to enforce security policies, monitor compliance, and enable remote device management of mobile devices & profiles.

Encryption and authentication method and implementation

For the different SSIDs with tiered approach design, different encryption and authentication methods should be implemented subject to their design and needs. Using Extensible Authentication Protocol (EAP) authentication framework, the network can be secured with various authentication methods.

A RADIUS server is necessary to perform authentication for the EAP protocols intended to be used, which Cisco ISE will be implemented to perform required authentication.

Internal Corporate Network

For Internal Corporate Network, it is suggested to maximize its security due to access to internal network is required. WPA3-Enterprise with GCMP256 encryption and EAP-Transport Layer Security (EAP-TLS) is proposed to achieve this goal. Using WPA3-Enterprise observes additional requirements of Protected Management Frames and minimum requirements for authentication, encryption and key derivation (Wi-Fi Alliance, n.d.). GCMP256 encryption is more secure using a 256-bit key size. EAP-TLS is considered the most secure protocol and effectively protect the network from attacks such as Man-in-the-middle (Grubbs, n.d.).

The setup requires a certificate on both the wireless client (i.e. Corporate Laptops) and the RADIUS server. They are authenticating to each other with public-private key cryptography (i.e. X509 certificates), which effectively protects the network and creates a password-less environment that also prevents credential theft/leakage.

A small number of laptops might need to be replaced or upgraded to support the use of WPA3-Enterprise protocol.

BYOD network

For BYOD network, considering the variety of devices that our employees may use as well as convenience of setup, compatibility and security needs, WPA3-Enterprise Transition Mode (WPA3+ WPA2-Enterprise mixed mode) with CCMP128 encryption and PEAP-MSCHAPv2 (Cisco, 2024). WPA2-Enterprise being supported since older devices may not support WPA3-Enterprise, as well as the use of CCMP128 for better compatibility with older devices. PEAP-MSCHAPv2 is chosen as it can be integrated with the existing Active Directory such that employees can use their AD credentials for authentication (Raphaely, n.d.).

The setup will also require a trusted certificate issued by a public Certificate Authority on the RADIUS server for clients to validate the legitimacy of the network, without installing corporate specific root certificate on their device, and help protecting the network from Man-in-the-middle attack.

Guest network

For the guest network, Opportunistic Wireless Encryption (OWE) in transition mode will be used. While the network is open for everyone to connect, the data transmission is encrypted with a pairwise master key secret generated through the process of Diffie-Hellman key exchange (Alomoush & Antunes, 2023). However, as OWE is supported on newer devices only, the transition mode which is supported on Cisco CW9800 WLC for the guest network allows older devices to fall back to Open connection without encryption. After connecting to the guest network, a captive portal will be shown which the guests are required to enter their email address and agree to the conditions to access to the internet (Cisco Systems, Inc., 2014).

Though Cisco Meraki MR57 AP does not support OWE transition mode at the moment, we assume that will be supported by a future software update. The choice of AP will be changed to a compatible model if it is still not supported when the project is being implemented.

Fast roaming in the headquarters

Features of CISCO Catalyst 9166D1 for Fast Roaming:

1. 802.11r (Fast BSS Transition)

The CISCO Catalyst 9166D1 supports the 802.11r standard, allowing for fast and secure handoffs between access points. This minimizes the time it takes for a device to roam from one AP to another, which is crucial in the headquarters environment where users would frequently move between areas.

2. 802.11k (Radio Resource Management)

These APs support 802.11k, which helps devices quickly identify the best available APs to connect to. This improves the efficiency and speed of roaming decisions, reducing latency and ensuring a stable connection.

3. 802.11v (Wireless Network Management)

The 9166D1's support 802.11v, allowing for better management of client devices. The network can guide devices to the optimal AP based on factors like load and signal strength, ensuring balanced network performance and improved connectivity.

4. Pre-Authentication

CISCO's controller CW9800, which will be used in conjunction with the Catalyst 9166D1 APs, supports pre-authentication. This feature allows devices to authenticate with multiple APs before actually connecting to them, reducing the time required for authentication during roaming.

The CISCO Catalyst 9166D1 APs, along with the CISCO CW9800 controllers, fully support fast roaming technologies. This ensures that the wireless LAN in the headquarters will provide seamless connectivity and superior user experience, even as employees move throughout the building.

Role-base access control & BYOD management

For Role-based access control (RBAC), we have decided to use another Cisco solution called Cisco Identity Services Engine (ISE). This solution is fully compatible with cisco devices such as Cisco Catalyst 9166D1 AP and fully integrates with Azure AD for user provisioning, de-provisioning, and group management. Among the features of ISE for RBAC, the following are the most important for the implementation on Wealth Management Co.

Enhanced Security: Cisco ISE allows for precise control over who can access specific network resources based on their role. This way, we are applying the principle of "Need to Know" and reducing the risk of a data breach.

Compliance: Companies as Wealth Management Co that handle sensitive financial information from their clients must adhere to strict regulatory requirements. Cisco ISE helps ensure compliance by providing detailed audit logs and reports on user access and activities.

Scalability: Cisco ISE is designed to handle large and complex environments ensuring that the system can grow with potential company expansions over time.

Flexibility: The system supports various authentication methods, including passwords, certificates, and multi-factor authentication.

User-Friendly Interface: The Web Graphical User Interface (GUI) of Cisco ISE makes it easy to configure and manage, reducing the complexity of network administration.

Integration: Cisco ISE can integrate with other solutions such as Azure AD for functionalities such as Single Sign on and Cloud Identity Management.

For BYOD Management, we have selected Microsoft Intune. Since the company already works on a Windows environment, the integration with other Microsoft products is seamless.

The main features considered for choosing Microsoft Intune as BYOD management solution are the following:

Enhanced Security: Intune provides robust security features such as conditional access policies, encryption, and remote wipe capabilities. This ensures that sensitive financial data remains protected, even on employee-owned devices.

Comprehensive Device Management: Intune offers both Mobile Device Management (MDM) and Mobile Application Management (MAM), allowing organizations to manage devices and applications without requiring device enrollment.

Conditional Access Policies: Intune allows for the creation of conditional access policies that can restrict access based on device compliance, user location, and other factors

Integration with Microsoft Ecosystem: Intune seamlessly integrates with other Microsoft services like Azure Active Directory, Microsoft 365, and Azure Information Protection.

Wireless LAN management and monitoring

For our Wireless LAN management and monitoring solution we have decided to continue our all-Cisco solution by implementing Cisco Catalyst Center. Cisco Catalyst Center is compatible with our Cisco Catalyst 9166D1 AP's and other devices.

Cisco Catalyst Center offers the following benefits/features:

Centralized Management: Manage all APs from one interface.

Real-Time Monitoring: This will allow us to monitor the health of our network and devices

Application performance visibility: Monitor network performance on a per-application basis to ensure that our most important applications are performing well and being prioritized on the network.

AI-Analytics: AI and Machine learning will provide insights and recommendations for our network based on performance, device, placement, number of devices, etc.

Proactive Alerting: Using AI, Cisco Catalyst Center will notify administrators of any potential issues before they occur so that they may be remediated before impacting users.

Zero-Touch Provisioning and Policy-Based Management: Automatically configure our Catalyst 9166D1 AP's and other devices and assign them all with our security, QoS, and Access control policies so that each device is consistent.

Software-Defined Access: Enforce policies to segment the network.

Threat Detection and Response: This feature integrates with Cisco security appliances to extend their functionality.

Identity Services Engine (ISE): Enhances network access control and ensures that only authorized devices and/or users can connect to the network by integrating with Cisco ISE.

Dynamic Optimization: Adjusts network settings in real-time for optimal performance

Capacity Planning: Uses AI tools to forecast and plan network capacity based on usage trends.

Security Policy Regarding WLAN

Password management

Although WPA3 provides safeguards against brute force attacks, it is useless if the password is very predictable. Generally speaking, the password should be at least 12 characters and a combination of uppercase and lowercase letters, numbers, and symbols. Although in this case we're using certificate for internal company network authentication, it's still recommended to implement proper password management process on the BYOD network.

Reevaluate the WPA3 transition and apply WPA3-Enterprise 192-Bit if applicable

Compared to WPA2 Enterprise, WPA3 introduces Management Frame Protection (MFP) which protects the wireless network against DoS and honeypot attacks. However, since not every device supports WPA3 and the BYOD policy needs to take them into consideration, it is recommended that the company roll out WPA3/WPA2 setup for BYOD and reevaluate the WPA2 appliance periodically. For company-owned digital devices, WPA3-Enterprise 192-Bit should be mandatory since it is the most secure wireless setup by far (Fortinet, 2024).

STA isolation and filtering

Although sometimes it is necessary for STAs to be able to communicate with each other within the network, that also makes STAs vulnerable to insider attacks if threat actors gain access to the network. To manage the risk, it is suggested that STA isolation should be implemented, and BSS bridging should be disabled. Moreover, the AP should set the group data cipher suite to 00-07-AC:7 to disallow group addressed traffic. If STA-to-STA communication is required, such as printing, sharing and display services, STA filtering rules should be configured to limit the scope of forwarded packets (Wi-Fi Alliance, 2024).

Avoid A-MSDU flag manipulation attacks

According to the research by Mathy Vanhoef, attackers can easily send A-MSDU frames to receivers without authentication whereas the receivers would incorrectly interpret the payload as containing A-MSDU subframes and sensitive user information may be solicited. To remediate the wireless design flaw, the company is suggested to either assure only SPP A-MSDUs are used or set a rule to drop the full A-MSDU frame if the destination address is AA:AA:03:00:00:00 (Vanhoef, 2021).

References

Alomoush, R., & Antunes, T. (2023, June 26). *Configure Enhanced Open SSID with Transition Mode - OWE*. Retrieved from Cisco Configuration Examples and TechNotes: https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/217737-configure-enhanced-open-ssid-with-transi.html

Cisco. (2024, April 9). *WPA3 Deployment Guide* . Retrieved from Cisco Technical References: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/technical-reference/wpa3-dg.html#WPA3EnterpriseTransitionMode

Cisco DNA Center. . (2024, February 6). Retrieved from Cisco: https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/series.html#~tab-documents

Cisco Systems, Inc. (2014, June). *Cisco Meraki White Paper Captive Portal Configuration Guide*. Retrieved from Cisco Systems, Inc.: https://meraki.cisco.com/lib/pdf/meraki_whitepaper_captive_portal.pdf

Cisco Systems, Inc. (2016). *802.11r BSS Fast Transition*. Retrieved from Cisco: https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/technotes/80211r-ft/b-80211r-dg.html

Cisco Systems, Inc. (2020, November 3). *Understand Admin Access and RBAC Policies on ISE*. Retrieved from https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200891-Understanding-Admin-Access-and-RBAC-Poli.html

Cisco Systems, Inc. (2023, November 29). *Cisco Catalyst 9166 Series Access Points Data Sheet* . Retrieved from Cisco: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9166-series-access-points/catalyst-9166-series-access-points-ds.html

Cisco Systems, Inc. (2024, May 6). *802.11k and 802.11r Overview* . Retrieved from Cisco Meraki: https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/802.11k_and_802.11r_Overview

Cisco Systems, Inc. (2024, April 25). *Cisco Catalyst CW9800H1 and CW9800H2 Wireless Controllers Data Sheet* . Retrieved from Cisco: https://www.cisco.com/c/en/us/products/collateral/networking/wireless/wireless-lan-controllers/cat-cw9800h1-cw9800h2-wireless-controllers-ds.html

Cisco Systems, Inc. (n.d.). *Catalyst Wireless Wi-Fi 6E Indoor Access Point | CW9166 | Cisco Meraki*. Retrieved from Cisco: https://meraki.cisco.com/product/wi-fi/indoor-access-points/cw9166/

Cisco Systems, Inc. (n.d.). *Cisco Catalyst Center Network Management*. Retrieved from Cisco Catalyst Center: https://www.cisco.com/site/us/en/products/networking/catalyst-center/index.html#tabs-a107e9a621-item-3f7ee2b544-tab

Cisco Systems, Inc. (n.d.). *Unified Access enabling the BYOD Smart Solution*. Retrieved from Cisco: https://www.cisco.com/assets/sol/xarch/asd/byod.html

Cisco Systems, Inc. (n.d.). *WiFi 6E Wireless Indoor Access Point | MR57 | Cisco Meraki*. Retrieved from Cisco: https://meraki.cisco.com/product/wi-fi/indoor-access-points/mr57/

Cisco Systems. Inc. (n.d.). *802.11r Fast Transition Roaming*. Retrieved from 802.11r, 802.11k, and 802.11w Deployment Guide, Cisco IOS-XE Release 3.3: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/5700/software/release/ios_xe_33/11rkw_DeploymentGuide/b_802point11rkw_deployment_guide_cisco_ios_xe_release33/b_802point11rkw_deployment_guide_cisco_ios_xe_release33_chapter_01.pdf

Fortinet. (2024). *Advantages of WPA3 Enterprise*. Retrieved from Fortinet Document Library: https://docs.fortinet.com/document/fortiap/7.4.0/wifi-6-7-design-and-planning-guide/612214/advantages-of-wpa3-enterprise

Grubbs, P. (n.d.). *What is EAP-TLS?* Retrieved from SecureW2: https://www.securew2.com/blog/what-is-eap-tls

Portnox. (n.d.). *What is WPA3 vs. WPA2?* Retrieved from Portnox: https://www.portnox.com/cybersecurity-101/wpa3/

Raphaely, E. (n.d.). *EAP-TLS vs. PEAP-MSCHAPv2: Which Authentication Protocol is Superior?* . Retrieved from SecureW2: https://www.securew2.com/blog/eap-tls-vs-peap-mschapv2-which-authentication-protocol-is-superior

Vanhoef, M. (2021). *FragAttacks: Forging Frames in Protected Wi-Fi Networks*. Retrieved from Black Hat: https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Fragattacks-Breaking-Wi-Fi-Through-Fragmentation-And-Aggregation-wp.pdf

Wi-Fi Alliance. (2024, June 10). *WPA3™ and Wi-Fi Enhanced™ Open Deployment and Implementation Guide*. Retrieved from Wi-Fi Alliance: https://www.wi-fi.org/system/files/WPA3%20and%20Wi-Fi%20Enhanced%20Open%20Deployment%20Guide_v1.0.pdf

Wi-Fi Alliance. (n.d.). *Discover Wi-Fi Security*. Retrieved from Wi-Fi Alliance: https://www.wi-fi.org/discover-wi-fi/security