PRESIDIO FEDERAL

Q&A

The Importance of Wireless Assessments for Existing WLANs in Federal Facilities

By Ven Taylor, Wireless Solutions Architect at Presidio Federal

WITNESSING IOT AND OT IN ACTION

In the rapidly evolving landscape of wireless technology, ensuring the robustness, efficiency, and security of your wireless network is more critical than ever. Federal facilities face unique challenges that necessitate specialized assessments and solutions. This blog delves into the importance of conducting wireless assessments for existing WLANs in federal environments, providing guidance on optimizing network performance and security.

UNDERSTANDING WIRELESS ASSESSMENTS

A wireless assessment is a comprehensive evaluation of your WLAN, involving site surveys, network analysis, performance testing, and security evaluation. These assessments are designed to identify coverage gaps, performance bottlenecks, and security vulnerabilities, providing actionable insights for network optimization. Advanced tools and technologies, such as Ekahau AI Pro, are used to gather and analyze data, ensuring precise and effective recommendations.

Q: Why is a wireless assessment necessary for my federal facility?

A: Wireless assessments are crucial for identifying and addressing specific issues in your WLAN, ensuring that your network is secure, efficient, and capable of handling increasing demands. They provide a detailed understanding of your network's strengths and weaknesses, allowing for targeted improvements. Additionally, they ensure compliance with federal standards such as FedRAMP, FIPS 140-2 and NIST guidelines.

UNIQUE CHALLENGES IN FEDERAL WLANS

Federal WLANs have distinct challenges that set them apart from typical enterprise networks. These include stringent security requirements, compliance with federal regulations, and the need for seamless integration of various authentication methods.

Q: What's unique about Federal Wi-Fi? Wi-Fi is Wi-Fi regardless of where it's deployed.

A: Federal Wi-Fi involves unique authentication methods, such as PIV/CAC cards, which are not common in typical enterprise environments. For instance, cell

phones without card readers need to authenticate via "derived credentials" through an MDM platform like Microsoft Intune, which securely passes credentials to the device according to defined policies. Additionally, federal networks must handle classified information securely, provide secure remote access, and implement zero-trust architectures.

BENEFITS OF CONDUCTING A WIRELESS ASSESSMENT

Conducting a wireless assessment offers numerous benefits, including enhanced security, optimized performance, and compliance with regulatory requirements.

ENHANCED SECURITY MEASURES

Wireless assessments identify vulnerabilities and outdated security protocols, providing comprehensive recommendations to bolster network security. These recommendations encompass a variety of advanced technologies and best practices to address the latest security threats and ensure robust protection against cyber-attacks.

Q: How can a wireless assessment improve my network's security?

A: Wireless assessments enhance network security in several ways:

- Identification of Vulnerabilities: Assessments uncover existing security gaps, such as outdated firmware, misconfigured access points, and weak encryption standards.
- Implementation of WPA3 and OWE: Upgrading to WPA3 ensures stronger encryption and improved authentication protocols. Opportunistic Wireless Encryption (OWE) secures open networks by encrypting data without requiring a password, protecting against eavesdropping.
- Network Segmentation: Recommendations for segmenting the network to isolate sensitive data and critical infrastructure from less secure areas, minimizing the risk of unauthorized access.
- Intrusion Detection and Prevention Systems (IDS/IPS): Integration of IDS/IPS to monitor network traffic for suspicious activities and respond to potential threats in real-time.
- Advanced Authentication Methods: Implementation of multifactor authentication (MFA) and support for PIV/CAC cards and derived credentials to ensure secure access for all users.
- Regular Firmware and Software Updates: Ensuring all network devices have the latest firmware and software updates to protect against known vulnerabilities.
- Secure Guest Access: Setting up secure guest access networks using techniques such as captive portals and role-based access control to limit guest access to the internal network.
- Encryption of Data in Transit and at Rest: Recommendations for encrypting data both in transit and at rest to protect sensitive information from interception and unauthorized access.
- Zero Trust Architecture: Adopting a zero-trust approach where every device and user is verified before gaining access to the network, ensuring continuous authentication and authorization.

By addressing these aspects, wireless assessments provide a comprehensive approach to strengthening network security, ensuring compliance with federal security standards, and safeguarding against evolving cyber threats.

OPTIMIZED PERFORMANCE AND CAPACITY

Assessments help detect interference, coverage gaps, and performance bottlenecks, optimizing network settings for technologies like OFDMA and higher QAM. This ensures better performance in high-density environments and reduces latency.

PRESIDIO® FEDERAL

Q: Can a wireless assessment help with network performance issues?

A: Yes, by identifying interference sources and optimizing configurations, assessments enhance network performance, reducing latency and improving data transmission efficiency.

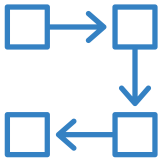
REGULATORY COMPLIANCE AND FUTURE-PROOFING

Wireless assessments ensure your network complies with federal regulations and is prepared for future technological advancements and increasing demands. They align your network with current federal regulations and recommend upgrades for emerging technologies, ensuring compliance and readiness for future developments.

Q: How does a wireless assessment ensure compliance and future-proofing?

A: By aligning your network with current federal regulations and recommending upgrades for emerging technologies, assessments ensure compliance and readiness for future developments.

THE ASSESSMENT PROCESS



A thorough wireless assessment involves several key steps:

- Initial Consultation and Requirements Gathering: Understanding specific needs and challenges of your federal facility.
- On-Site Surveys and Data Collection: Comprehensive site surveys to collect data on signal strength, interference, and user behavior.
- Detailed Analysis and Reporting: Analyzing collected data to identify issues and propose solutions.
- Action Plan Development and Implementation: Creating a tailored action plan and implementing recommended improvements.

Q: What does the wireless assessment process involve?

A: The process includes initial consultations, on-site surveys, data analysis, and the development of a customized action plan, ensuring a detailed and targeted approach to network optimization. Follow-up activities, such as post-implementation reviews and ongoing monitoring, are also part of the process.

CHOOSING THE RIGHT PARTNER FOR YOUR WIRELESS ASSESSMENT

Selecting a trusted advisor for conducting wireless assessments is crucial. Look for partners with experience in federal environments, a deep understanding of regulatory requirements, and a proven track record of successful assessments. Key considerations include the partner's experience with federal customers, knowledge of regulatory requirements, and a history of successful assessments and implementations. Certifications (e.g., CWNA, CWSP) and specific experience with similar federal agencies are also important.

Q: What should I consider when choosing a partner for a wireless assessment?

A: Key considerations include the partner's experience with federal customers, knowledge of regulatory requirements, and a history of successful assessments and implementations. Look for certifications and specific experience with similar federal agencies.

Wireless assessments are essential for maintaining secure, efficient, and high-performing WLANs in federal facilities. By addressing unique challenges and leveraging the latest technologies, these assessments ensure your network is prepared for the future. Regular assessments and staying current with technological advancements offer long-term benefits and mitigate risks. To learn more about how Presidio Federal can serve as your trusted advisor, visit PRESIDIOFEDERAL.COM.