Security Controls for the LAN-to-WAN Domain in Financial Services

Bronte Hodson

Davenport University

IAAS332: Authentication & Audit

Tony McCutchen

Due Date: 10/5/2025

Security Controls for the LAN-to-WAN Domain in Financial Services

Introduction

The LAN-to-WAN domain represents the boundary between the financial institution's internal network (LAN) and the external systems (WAN), including the internet, partner networks, and cloud service providers. The boundary is an important access point for cyber threats and therefore should be continuously monitored to protect sensitive data and for meeting regulatory compliance (OCC, 2025, p. 4-6). Both the Office of the Comptroller of the Currency (OCC) and the Federal Financial Institutions Examination Council (FFIEC) deem it as a high-risk attack surface, and mandate a layered multi-controls approach, including documentation supporting the effectiveness of such controls (FFIEC, n.d., Section II.C.4, OCC, 2021, pp. 2, 4-6).

To adequately secure this domain financial institutions must employ a layered solution of technical, procedural, and human-factor controls that is resilient, updated continually and capable of adapting to shifting threat vectors of security and regulatory compliance frameworks such as the Gramm-Leach-Bliley Act (GLBA) (OCC, 2025, pp. 4-5). A comprehensive, evolving security framework grounded in regulatory guidance will assist in a continuous and strong security posture for regulatory compliance.

LAN-to-WAN Domain: Information Security and Risk Management Requirements

The LAN-to-WAN domain is a primary focus area for security control to maintain the confidentiality, integrity, and availability, or CIA, of private financial information (OCC, 2025, pp. 4–5). Financial institutions face regulatory compliance obligations, which may include PCI DSS, SOX, GLBA, NIST Cybersecurity Framework, and procedures/guides from the FFIEC (Johnson et al., pp. 30, 63, 66, 80, 488–489). These are set to significant levels for protecting data, continuous monitoring, incident response, and record-keeping (FFIEC, n.d., Section II). A LAN-to-WAN domain can be exposed to unauthorized access, data leakage, Denial of Service (DoS), and advanced malware. Breaches from an attack could result in regulatory fines, operational interruption of business, and reputational loss (OCC, 2025, p. 1). The FFIEC (n.d., Section II.C.4) recommends financial institutions use NIST 800 and ISO/IEC 27000 series technology standards to ensure the best practice for achieving effective security controls.

Regulators will look to see evidence that controls are in place and that they are effective. This can be in the form of logs, inspections, and frequently conducted assessments (FFIEC, n.d., Section IV.A.2(d)). Financial institutions could demonstrate this through conducting regular gap assessments, penetration tests, external audits, and frequent vulnerability scans to identify the threats they face and to ensure their security controls are current (FFIEC, n.d., Section II.C.4).

Data Privacy Protection Over the WAN

Data privacy is key. Both PCI DSS and ISO/IEC 27001 require strong encryption for sensitive data that is sent through public networks (FFIEC, n.d., Sections C.II.4, II.C.19). Financial institutions, according to Chandramouli (2022, p.p. 5-6, 8), must use up-to-date and secure encryption protocols such as TLS and IPsec to encrypt data and reduce the likelihood of an attacker intercepting this data. For working remotely from home or branches, connecting through secure VPNs should be utilized with strong multi-factor authentication (MFA). Also, Data Loss Prevention (DLP) tools can detect and monitor network traffic and prevent unauthorized data from being transmitted (Johnson, et al., 2022, p. 369). As financial institutions move services to the cloud, automated controls like encryption, access management, and audits help meet compliance, limit data breaches, and maintain customer trust (Johnson et al., 2022, pp. 102–103).

Filtering Undesirable Network Traffic from the Internet

Firewalls are typically the first line of defense at the LAN-to-WAN boundary. Firewall rules should follow a least privilege basis, allowing only traffic that is necessary and include information about the source and destination IPs, ports, protocols and user identity. The rules should be reviewed regularly, when business operations change or new threats emerge (Johnson, et al., 2022, p.p. 427, 413-414). Automated rule validation and change management tools can assist with auditability and prevent mistakes (FFIEC, n.d., Section II.C.4). Access Control Lists (ACLs) work alongside firewalls to allow or block specific types of network traffic based on factors such as IP addresses and ports (Chandramouli, 2022, p.p. 11-12).

Next-generation firewalls (NGFWs) provide enhanced capabilities such as deep packet inspection, application filtering, threat intelligence, and intrusion prevention. They can block traffic based upon geographic locations, detect known bad actors, and integrate with security information and event management (SIEM) tools to provide alerts in real time (Chandramouli, 2022, p.p. 7, 9-10).

Micro-segmentation, dividing the network into smaller secure sections, can help limit the ability for an attacker to move within the network, if they gain access (Chandramouli, 2022, p.p. 17-19). Financial institutions should use automated firewall management to authorize and document changes, ensuring security and minimizing errors in complex networks.

Acceptable Use Policy (AUP)

Arogundade (2023, p.p. 33-34) states that Acceptable Use Policies (AUPs), based on the principle of least privilege are essential for preventing risky behavior and supporting compliance. Enforcement is through identity-aware web proxies. These proxies require users to log in, allowing different rules for different roles or departments and logging all internet activity to support audits and investigations. Zero Trust principles support access control by continually verifying the user’s identity and the device. According to Chandramouli (2022, p. 8), modern solutions combine threat intelligence with behavioral analytics. User and Entity Behavior Analytics (UEBA) can flag unusual or risky activity, such as repeated attempts to access restricted sites.

According to Arogundade (2023, p.p. 34-35), financial Institutions should link AUP controls with their identity management systems so that policies are applied consistently. Reviewing logs regularly and updating staff training helps identify new trends and risks. Best practice combines technical controls and regular staff training. AUPs help protect a financial institution’s reputation by blocking risky sites and reducing malware or data leaks caused by human error.

Creating a Secure Staging Zone for Anonymous Access: DMZ

According to Johnson et al. (2022, p. 410), a demilitarized zone (DMZ) is a secure space between public-facing networks and internal systems, hosting services like web portals, email gateways, and APIs that your organization wants to keep separate from your internal network. The best practice includes two firewalls or network segmentation with strict monitoring and logging of DMZ-to-LAN traffic (Arogundade, 2023, p. 33). For network visibility and rapid detection of threats, Intrusion Detection and Prevention Systems (IDS/IPS) are a key process, using signature and anomaly-based methods to identify attacks (Bendiab et al., 2022, pp. 92–94).

To strengthen DMZ security, financial institutions should use Web Application Firewalls (WAFs) to protect against web-based threats (Chandramouli, 2022, p.p. 9-10), enforce Access Control Lists (ACLs) to control which traffic is permitted between public-facing services and internal systems, keep devices updated, and have MFA (Arogundade, 2023, p. 33). These measures help financial institutions protect internal systems and customer data and comply with regulations.

Trapping/Tracking Attackers: Honeypots

Since the DMZ is exposed to outside threats, organizations should also use tools like honeypots to detect attacks early and respond quickly. Honeypots are often used within or adjacent to the DMZ to monitor and attract suspicious traffic. According to Bendiab et al., (2022, p.p. 92-94), organizations may apply honeypots, which are fabricated decoy systems tailored to attract attackers, identify and analyze attack characteristics, and gather intelligence. The author also states that these systems can allow early warnings of ongoing breaches before attackers reach sensitive internal information and fortify detection and incident response when used with IDS/IPS rules and detection algorithms. Financial institutions should maintain IDS/IPS with threat intelligence updates, regularly test incident response plans, and use honeypot data to continuously strengthen security controls and lower the risk of costly breaches.

Monitoring of Network Traffic and SIEM

Security Information and Event Management (SIEM) systems are important for financial institutions as they aggregate and analyze logs from all points in the network to help identify threats in real time, facilitate investigations, and generate audit-ready reports (FFIEC, n.d., Section II.C.22). Minimum logging requirements require secure storage and retention of logs and SIEM rules, alerts, and dashboards should be reviewed and updated to ensure alignment with risk levels **(**FFIEC, n.d., Section II.C.22**).**

According to Chandramouli, (2022, p. 12**)** modern SIEMs utilize machine learning and analytics-based approaches to identify subtle threats, like slow data exfiltration and privilege abuse. They can also integrate with automated response tools to respond quickly to incidents, e.g., blocking a compromised host. Financial institutions should integrate SIEMs with threat intelligence platforms to manage and/or inhibit attacks.

Hiding Internal IP Addresses—Network Address Translation (NAT)

Network Address Translation (NAT) is a technique for concealing internal Internet Protocol (IP) addresses to make it more difficult for attackers to discover an internal system (Cisco, 2025). NAT logs are helpful for investigations and compliance reports (FFIEC, n.d., Section II.C.22). NAT can also provide an additional means for privacy and security through segmentation and application gateways (Arogundade, 2023, p. 9). NAT should be used with supplementary firewall rules based on risk (FFIEC, n.d., Section II.C.4). According to Cisco (2025), supplementary security measures in IPv6 include features such as temporary address, privacy extensions and dynamic address configuration which help improve user privacy and reduce the risk of tracking. NAT is part of a multi-layer defense-in-depth. Regular auditing of NAT is essential to prevent exposing internal financial systems to external threats (Chandramouli, 2022, p. 12). For financial institutions, regularly auditing NAT as part of layered security helps protect sensitive data, support compliance, and reduce external threats.

Patch Management

Patch management is an essential element of security. According to the FFIEC (n.d., Section II.C.10(d)), it involves finding, testing, and installing software updates to fix security issues, improve how systems run, or fix problems in operating systems and applications. Data breaches are often via unpatched systems. The OCC (2025, p. 14) recommends regularly monitoring for weaknesses in systems, applying patches in a timely manner, and regularly scanning for vulnerabilities to reduce cyber risks. According to FFIEC (n.d., Section II.C.10(d)), automated patching enables financial institutions to discover, review, and release updates in a timely manner. Automated patching can safely download, verify, and install updates both to operating systems and applications (Chandramouli, 2022, p. 12).

According to FFIEC (n.d., Section II.C.10(d)), automated alerts may help catch an error during patching and make it more efficient. By documenting each patch status and activity, financial institutions can maintain the evidence required by auditors. Effective patch management includes prioritizing critical updates, testing patches before deployment, and having rollback procedures in place to maintain system stability (Arogundade, 2023, p. 36). Patch management shows how technical controls strengthen security and support regulatory compliance for financial institutions.

The Human Factor

One important area of compliance is human error and insider threats. Regular security awareness training, such as mobile device security, helps employees understand their responsibilities in keeping LAN-to-WAN security strong and recognize social engineering attacks, like phishing, and observe policies (FFIEC, n.d., Section: II.C.7(e)). Keeping documentation of the management plan, testing controls, and evidence supports audit requirements, improves security operations, and reinforces LAN-to-WAN protection through regulatory compliance (FFIEC, n.d., Appendix A). Extra security measures like role-based permissions, the principle of least privilege, strong password rules, and MFA help prevent internal threats in financial institutions (OCC, 2021, p. 4).

Controls for LAN-to-WAN Security

A defense-in-depth strategy using many diverse controls at the LAN-to-WAN boundary has been recognized as the accepted standard for security and compliance (OCC, 2025, p. 6). This includes digital controls (firewalls, DMZs, IDS/IPS, SIEM, NAT, patch management), enterprise processes, and educated users (OCC, 2025, pp. 6–7). Risk-based frameworks, such as NIST and ISO/IEC 27000 series, outline the framework for continued risk assessment, selecting controls for use, and responding (FFIEC, n.d., Section II.C.4; OCC, 2025, p. 8). Compliance should be ongoing, continuously monitored and risk assessed as U.S. regulators require documentary evidence of compliance (FFIEC, Appendix A). Continuous improvement verified by external auditors is a necessary for maintaining effective security in the long term. Continuous evaluation and learning protect financial institutions against both existing and invisible threats (OCC, 2025, p. 9).

Conclusion

Securing the LAN-to-WAN domain in financial institutions needs a defense-in-depth strategy evolving as risks and regulations change. This integrates encryption, firewalls, DMZs, IDS/IPS, SIEM, NAT, patch management and employee training to ensure compliance and audit readiness. The effectiveness of LAN-to-WAN security relies upon continual integration, review and updates through risk assessments, control testing, and policy updates. based on identified threats. Security awareness training, incident response and simulation exercises improve the human and procedural side of compliance. A layered, policy-driven, and adaptive approach provides effective security and fulfills regulatory obligations for financial services organizations.

References

Arogundade, O. R. (2023). Network security concepts, dangers, and defense best practical. *Computer Engineering and Intelligent Systems*, *14*(2). https://www.researchgate.net/publication/369739760_Network_Security_Concepts_Dangers_and_Defense_Best_Practical

Bendiab, G., Boukhtouta, A., Debbabi, M., & Hanna, S. (2022). Honeypots for network security: A survey of current developments and research challenges. *Computers & Security*, 117, 102677. https://pure.port.ac.uk/ws/portalfiles/portal/88038032/978-1-68083-835-0.ch6.pdf

Chandramouli, R. (2022). *Guide to a secure enterprise network landscape* (NIST Special Publication 800-215). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-215.pdf

Cisco. (2025). *What is network address translation (NAT)?* Cisco. https://www.cisco.com/site/us/en/learn/topics/networking/what-is-network-address-translation-nat.html

Federal Financial Institutions Examination Council. (n.d.). *Information security*. FFIEC IT Handbook. https://ithandbook.ffiec.gov/it-booklets/information-security/

Johnson, R., Weiss, M., & Solomon, M. G. (2022). *Auditing IT infrastructures for compliance* (3rd ed). Jones & Bartlett Learning. https://ebookcentral.proquest.com/lib/davuport-ebooks/reader.action?c=UERG&docID=7077803

Office of the Comptroller of the Currency. (OCC). (2021). *Cybersecurity: Threats and vulnerabilities – risk management and control practices for cybersecurity* (OCC Bulletin 2021-36a). U.S. Department of the Treasury. https://www.occ.gov/news-issuances/bulletins/2021/bulletin-2021-36a.pdf

References

Office of the Comptroller of the Currency. OCC (2025). *Cybersecurity and financial system resilience: A report on the OCC's cybersecurity objectives and priorities*. U.S. Department of the Treasury. https://www.occ.gov/publications-and-resources/publications/cybersecurity-and-financial-system-resilience/files/pub-2025-cybersecurity-report.pdf