Strategic Implementation Framework: Network Access Control (NAC) Pilot Delivery and Operational Expectations

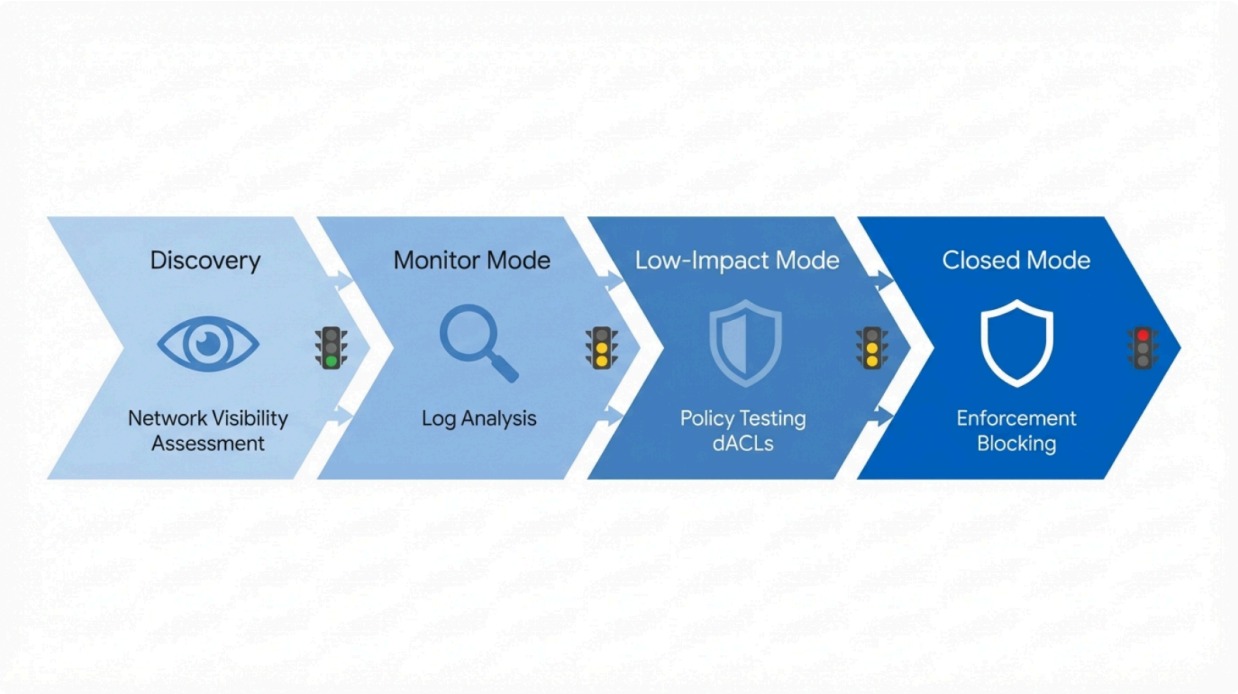
1. Executive Summary and Strategic Context

The initiation of a Network Access Control (NAC) pilot represents a pivotal transformation in the organization's cybersecurity posture. It marks a definitive shift from a legacy, perimeter-focused defense model—where trust was often implicit based on physical connectivity—to a robust Zero Trust Architecture (ZTA). In this new paradigm, trust is never assumed; it is explicitly verified for every user, device, and application attempting to access corporate resources. The stated objective of stopping non-SMD-LLC devices from accessing the network is conceptually straightforward but operationally complex, requiring the rigorous orchestration of identity validation, device profiling, granular policy enforcement, and continuous operational governance.

This report serves as the comprehensive strategic plan for the upcoming pilot with the network team. It is designed to manage expectations by detailing the architectural dependencies, project phases, and operational realities that accompany such a significant infrastructure change. The transition to a secured network edge is not merely a technical upgrade involving switch configurations and server deployments; it is a fundamental operational change that affects every entity connecting to the infrastructure.

The success of this initiative hinges on understanding that NAC is not a "set and forget" technology. It is a lifecycle program that demands continuous tuning, monitoring, and management. This document outlines a pragmatic, risk-averse path to delivery, emphasizing a phased approach that prioritizes visibility and business continuity while steadily increasing security enforcement. By adhering to the strategies detailed herein, the organization can effectively mitigate the risks associated with deployment friction and achieve the ultimate goal of a secure, compliant, and observable network environment.

NAC Pilot Maturity Roadmap: From Visibility to Enforcement



The NAC implementation lifecycle follows a risk-averse path. The pilot begins with passive visibility to inventory assets, moves to a monitor-only mode to test policies without blocking, and transitions to enforcement only after validation.

2. Architectural Foundations and Dependencies

The viability of the NAC pilot rests on a complex web of architectural dependencies. Before a single policy can be enforced, the underlying infrastructure must be capable of supporting the rigorous demands of 802.1X authentication and dynamic authorization. This section dissects the critical components that must be validated prior to pilot launch.

2.1 The Central Role of Visibility and Discovery

The foundational axiom of any NAC deployment is that one cannot secure what one cannot see. Effective implementation begins not with blocking, but with establishing comprehensive network visibility.[1] In many legacy environments, the "known" network inventory is merely a subset of the actual connected assets. Shadow IT, unauthorized switches, and unmanaged IoT devices often populate the dark corners of the network, invisible to standard audits but fully active on the wire.

Discovery is an active, ongoing process that interrogates the network infrastructure to build a real-time inventory of all connected assets.[2] This phase often reveals a significant delta between the perceived state of the network and operational reality. The pilot expectation

must be that the initial weeks will be dedicated almost exclusively to classification and profiling. This involves leveraging a combination of protocols—including DHCP, SNMP, HTTP User Agents, and potentially NMAP scanning—to fingerprint devices based on their inherent communication patterns and behavioral signatures.[3]

For the pilot to be successful, the security architecture must ensure that the NAC solution can ingest and correlate data from multiple disparate sources. It must integrate with the switching infrastructure to read MAC address tables and ARP caches, correlate this data with the Configuration Management Database (CMDB), and potentially interface with vulnerability scanners.[4] The objective is to establish a "single source of truth" for asset identity. If a device cannot be identified, it cannot be securely authorized. Therefore, a critical deliverable of the discovery phase is a detailed "Unknown Assets Report," which will necessitate manual investigation and remediation before strict enforcement policies can be safely applied.[5]

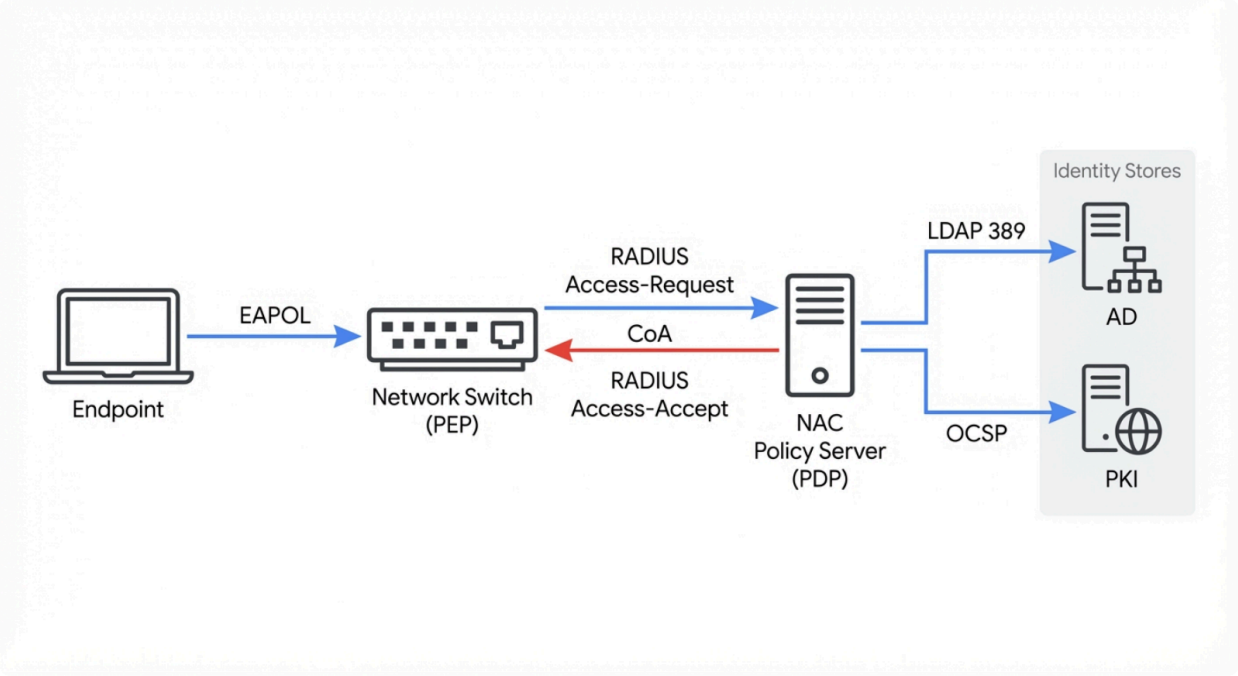
2.2 Authentication Infrastructure: PKI and Directory Services

To achieve the high-level goal of stopping non-SMD-LLC devices, the organization must rely on robust cryptographic proof of identity. For corporate-managed assets, the industry gold standard is certificate-based authentication using EAP-TLS (Extensible Authentication Protocol-Transport Layer Security). This method provides mutual authentication, where both the client (supplicant) and the server (authenticator) verify each other's digital certificates.[7] This mechanism effectively mitigates the risks of Man-in-the-Middle (MitM) attacks and credential harvesting, which are inherent vulnerabilities in password-based methods like PEAP-MSCHAPv2.[8]

However, the implementation of EAP-TLS introduces significant architectural dependencies on the Public Key Infrastructure (PKI). The pilot project plan must include a rigorous validation of the Certificate Authority (CA) hierarchy, ensuring its health, reachability, and proper configuration. Furthermore, the mechanisms for certificate distribution—whether through Active Directory Group Policy, Microsoft Intune, or another Mobile Device Management (MDM) solution—must be tested and verified.[9] A common point of failure in NAC pilots is the silent expiration or misconfiguration of client certificates, which results in valid corporate devices being rejected, creating immediate business disruption.[10]

In parallel, deep integration with directory services such as Active Directory (AD) or Azure Active Directory (AAD) is non-negotiable for user authorization. The NAC policy engine relies on real-time queries of group memberships and user attributes to make authorization decisions—for instance, assigning a user in the "Finance" AD group to the isolated "Finance VLAN".[6] The architecture must support high availability and low latency for these authentication sources. If the directory service becomes unreachable or slow to respond, the NAC solution must have a predefined operational behavior—either "fail-open" or "fail-closed"—a decision that carries profound risk implications which will be discussed in later sections.[11]

NAC Architectural Components and Traffic Flow



The NAC architecture relies on the interplay between the Supplicant (Endpoint), Authenticator (Switch), and Authentication Server (NAC). Key protocols include EAP for identity transport, RADIUS for policy communication, and LDAP/OCSP for backend validation.

2.3 Network Infrastructure Compatibility and Readiness

A critical, often underestimated component of NAC delivery is the readiness of the network hardware itself. The switch layer functions as the Policy Enforcement Point (PEP), executing the authorization decisions made by the NAC Policy Decision Point (PDP).[1] It is imperative to recognize that not all switches possess the same capabilities. Older hardware or varied firmware versions may lack support for essential features such as dynamic VLAN assignment, Downloadable ACLs (dACLs), or Change of Authorization (CoA).[12]

The pilot planning phase must include a comprehensive compatibility assessment of all network devices within the pilot scope. This assessment involves verifying hardware models, IOS/firmware versions, and the support for specific RADIUS attributes required for the intended enforcement policies.[13] If the switching infrastructure cannot support the required enforcement methods (e.g., if it fails to process CoA packets for session termination), the project scope may need to be adjusted, or a hardware refresh may be required. This represents a significant potential risk to both the budget and the timeline that must be flagged and addressed early in the planning process.[12]

Additionally, the configuration of the network access devices (NADs) must be standardized.

Inconsistent configurations across switches—such as differing timeout values, re-authentication timers, or RADIUS server priorities—can lead to intermittent and difficult-to-troubleshoot connectivity issues. A "Golden Configuration" template for 802.1X interfaces should be developed and rigorously tested during the pilot.[9]

3. Defining the Pilot Scope and Operational Success Criteria

3.1 Strategic Selection of Pilot Participants

The selection of the pilot cohort is a strategic decision that directly influences the validity and utility of the project's findings. A frequent misstep in NAC pilots is the selection of a group that is too homogenous—often the IT department itself—which fails to stress-test the system against the diverse use cases and less predictable behaviors found in the broader organization.[14] To be effective, the pilot must include a representative cross-section of the user base, including standard office workers, executives, operational staff, and specialized departments such as Finance or R&D.

Furthermore, the pilot must encompass a variety of device types to test the profiling and policy engines thoroughly. This includes standard corporate laptops, printers, IP phones, specialized medical or industrial devices, and potentially even guest devices if they are in scope.[9] The physical location of the pilot is also a key consideration. Ideal candidates are branch offices or specific floors of a headquarters building where IT support is readily available to assist with physical connectivity issues if they arise.[15] The scope of the pilot must be rigidly defined in the project charter to prevent scope creep, a common cause of project stalls where the team attempts to "boil the ocean" rather than validating specific use cases.[16]

3.2 Defining Operational Success Metrics

Defining "success" for a NAC pilot requires moving beyond a binary "it works" assessment to a more nuanced evaluation of performance, stability, and user experience. The project team must establish quantifiable Key Performance Indicators (KPIs) that will serve as the "go/no-go" criteria for the subsequent global rollout.[17] These metrics provide the objective data needed to justify the expansion of the program and to identify areas requiring tuning.[18]

Key operational metrics to track during the pilot include:

- **Authentication Success Rate:** The percentage of valid access requests that are successfully authorized by the NAC system. A baseline of 95% or higher is typically required before moving to production enforcement.[9]
- **Authentication Latency:** The time taken for the NAC server to process a request and return a response to the switch. High latency can lead to 802.1X timeouts and connectivity failures, frustrating users.[19]
- **False Positive Rate:** The number of legitimate, compliant devices that were incorrectly blocked or quarantined by the policy logic. This metric is crucial for assessing the

accuracy of the profiling and policy rules.[14]

- **Helpdesk Ticket Volume:** The number of support incidents generated related to network access or connectivity. A significant spike in tickets indicates either technical issues or a lack of effective user communication and training.[20]
- **Device Profiling Accuracy:** The percentage of devices that are correctly identified by type, OS, and vendor. High accuracy is essential for granular policy enforcement and preventing identity spoofing.[6]

3.3 The Phased Rollout Strategy: From Monitor to Enforcement

To effectively manage risk and operational expectations, the pilot must follow a strict, phased deployment model. This approach allows the team to gain confidence in the system's behavior and the accuracy of its policies before actively intervening in user traffic.[1]

1. **Monitor Mode (Audit Only):** In this initial phase, the NAC system receives and processes authentication requests, evaluating them against the defined policies. However, the switch ports are configured in "open" or "multi-auth" mode, allowing all traffic regardless of the NAC authorization result.[6] This phase is purely for data gathering, policy simulation, and identifying misconfigured devices without causing any downtime. It allows the team to answer the question: "If we were enforcing today, who would be blocked?"
2. **Low-Impact Mode:** Once the policy logic is validated and the "Unknown" device list is minimized, the system transitions to Low-Impact Mode. In this phase, devices are authenticated, and basic policies are applied (e.g., assigning a VLAN). However, a "catch-all" permit rule or ACL is often left in place for unknown or failed devices to ensure business continuity while the team continues to refine the profiling rules.[3] This introduces the mechanism of enforcement without the full penalty of blocking.
3. **Closed Mode (Enforcement):** This is the final target state where the "default deny" posture is fully enabled. Only explicitly authorized and compliant devices are granted access to network resources. Any device that fails authentication or does not meet the policy criteria is moved to a quarantine VLAN or blocked entirely.[3] Reaching this phase in the pilot demonstrates the solution's readiness for production deployment and validates the organization's ability to operate a Zero Trust network access layer.

Operational Modes for NAC Deployment

Mode	ACL Configuration	Risk of Blocking	Primary Goal
Monitor Mode	Port ACL "Allow Any Any"	**None**	Visibility / Audit
Low-Impact Mode	Pre-Auth ACL (DHCP/DNS) + Permit Unknown	**Low**	Policy Validation
Closed Mode	Default Deny (DHCP only)	**High**	Enforcement / Security

Deployment modes allow for a gradual increase in security posture. Monitor Mode offers zero risk but no protection. Low-Impact Mode introduces visibility and partial control. Closed Mode provides full security but carries the highest risk of disruption.

Data sources: Intelligent Visibility, LookingPoint, Packet Pushers

4. Device Profiling and Identity Management

4.1 Distinguishing Managed from Unmanaged Devices

The core mandate of "stopping non-SMD-LLC devices" hinges on the ability to reliably and cryptographically distinguish between a corporate-managed asset and a rogue or unmanaged device. "SMD-LLC devices" in this context refers to assets that are owned, managed, and sanctioned by the corporation. The most robust method for this validation is **Machine Authentication** utilizing EAP-TLS with a machine certificate issued by the corporate Internal CA.[7]

When a managed device connects to the network, it presents its unique machine certificate during the 802.1X handshake. The NAC server validates the certificate chain, checks the validity dates, and queries the CRL or OCSP responder to ensure the certificate has not been revoked.[9] If the certificate is valid, the device is trusted as a corporate asset. This process happens seamlessly in the background before the user even logs in, ensuring that the device itself is authorized to be on the network.

However, a significant operational challenge arises with "unmanaged" devices that may still

have a legitimate business reason to connect. These could include contractor laptops, guest devices, or employee personal phones (BYOD). These devices do not possess corporate certificates and therefore cannot participate in EAP-TLS authentication. The pilot plan must explicitly define how these devices will be handled. Will they be blocked entirely? Or will they be shunted to a segregated "Guest" or "Internet Only" VLAN? This is a business policy decision, not just a technical one, and must be made by stakeholders prior to the pilot.[15]

4.2 The IoT and Legacy Device Challenge

The "silent killers" of NAC projects are the myriad of devices that do not support 802.1X authentication. This category includes printers, IP cameras, HVAC controllers, badge readers, and legacy industrial equipment.[12] These devices are often "headless"—lacking a user interface—and cannot accept a digital certificate or prompt a user for credentials.[22]

For these devices, the pilot will likely rely on **MAC Authentication Bypass (MAB)**. In this method, the switch sends the device's MAC address to the NAC server as both the username and password. While simple to implement, MAB is inherently insecure because MAC addresses are easily spoofed.[12] To mitigate this risk, MAB must be combined with advanced **Profiling**. The NAC solution analyzes the device's network behavior—such as its DHCP fingerprint (Option 55), HTTP User Agent string, and OUI—to confirm that the device claiming to be a printer is *actually* a printer and not a spoofed laptop.[24]

The pilot expectation must be that MAB requires significant manual effort to build, tune, and maintain the "allow lists" or "identity groups".[26] The project team should be prepared to hunt down "mystery MACs" during the discovery phase to classify them correctly before enforcement is turned on. Failure to do so will result in these devices being blocked, potentially disrupting building services or business operations.

4.3 Handling MAC Spoofing Risks

Given the inherent weakness of MAB, the report must address the risk of MAC spoofing. If an attacker clones the MAC address of a trusted printer, they could potentially gain access to the printer's VLAN.[27]

To counter this, the pilot architecture should enforce strict network segmentation. MAB-authenticated devices should be placed in restricted VLANs with Access Control Lists (ACLs) that strictly limit traffic to only what is necessary for that device's function. For example, a printer VLAN should only be allowed to communicate with the print server and potentially a management subnet, but explicitly denied access to the internet, the finance database, or other user segments.[27] This "Least Privilege" approach ensures that even if a device is spoofed, the attacker's ability to move laterally within the network is severely constrained.[6]

5. Policy Design and Enforcement Logic

5.1 The Policy Matrix

A clear expectation for the pilot meeting is the presentation and agreement on a **Policy Matrix**. This document serves as the "source of truth" for the NAC configuration, translating abstract business intent into concrete technical rules.[9]

The matrix typically defines the relationship between **Identity** (User Group, Device Type, Location), **Conditions** (Time of day, Posture status, Threat status), and **Results** (VLAN assignment, dACL, SGT, Bandwidth contract).[6]

For the pilot, the policy matrix should be kept simple to start, focusing on the primary use cases. Complexity can be layered in as the organization matures. A typical pilot matrix might include the following rules:

1. **Corporate User + Corporate Device:** Valid Certificate + AD User Group -> Full Access VLAN + Permit All ACL.
2. **Corporate User + Personal Device:** Valid AD Credentials + No Machine Cert -> Internet Only VLAN (BYOD).
3. **IoT/Printer (MAB + Profiled):** Known MAC + Device Profile Match -> Restricted IoT VLAN + Service-Specific ACL.
4. **Guest:** Guest Portal Auth -> Guest VLAN + Internet Only ACL.
5. **Unknown/Non-Compliant:** Default Deny -> Quarantine VLAN + Remediation ACL.

NAC Policy Enforcement Matrix

Permit Access Quarantine / Remediation

RULE NAME	CONDITIONS (IDENTITY + CONTEXT)	PERMISSIONS (RESULT)
Corp Managed	Group Domain Computers Cert Valid	VLAN Corporate ACL Permit_All
IoT Device	Group IoT_Printers Profile HP_Printer	VLAN IoT_Segment ACL Print_Only
Non-Compliant ⚠	Group Domain Computers Posture Fail	VLAN Quarantine ACL Remediation_Only
Default	Any	VLAN Guest ACL Internet_Only

The Policy Matrix serves as the rulebook for the NAC engine. Rules are evaluated top-down. The 'Conditions' column combines multiple attributes (Identity, Device Type, Posture) to determine the granular 'Permissions' (VLAN, ACL).

Data sources: Cloudi-Fi, Intelligent Visibility, Cisco Community

5.2 Posture Assessment and Remediation

To truly realize the goal of "stopping non-SMD-LLC devices," the organization may wish to go beyond simple identity checks and verify the *security posture* or health of the connecting device. Posture Assessment involves checking if the device meets specific security criteria, such as having up-to-date antivirus definitions, current OS patches, active encryption, and a running firewall.[2]

However, implementing posture assessment in a pilot phase adds significant complexity and potential for user friction. It typically requires a persistent or dissolvable agent to be installed on the endpoint.[28] If a device fails a posture check (e.g., AV definitions are 3 days old), it is moved to a quarantine VLAN where it can only access remediation services (such as WSUS or AV update servers).[9]

For the pilot meeting, the recommended strategy is to decouple Identity (Who are you?) from Posture (Are you healthy?). The pilot should prioritize stabilizing Identity-based enforcement (802.1X/MAB) first. Posture checks should be introduced in a subsequent phase once the base connectivity is stable. This approach prevents overwhelming the helpdesk with tickets

from users who are authenticated but blocked due to minor compliance issues, allowing for a smoother adoption curve.[30]

6. Operational Governance and Exception Handling

6.1 The Exception Management Process

In every NAC deployment, there will inevitably be devices that *cannot* comply with the standard security policy but *must* connect to the network for critical business reasons. These might include legacy R&D systems running outdated operating systems, specialized medical devices, or third-party vendor systems that cannot accept corporate agents.[31] Without a formal, rigorous exception process, the security team will be bombarded with ad-hoc requests to "just open the port," leading to policy drift and a proliferation of "shadow exceptions" that are never reviewed or revoked.[31]

The pilot plan must establish a clear **Governance Workflow** for managing exceptions:

1. **Request:** A formal request must be submitted via a standardized form, detailing the specific device (MAC address), the business justification for the exception, and the expected duration of the need.[32]
2. **Risk Assessment:** The security team conducts a risk assessment. Can the device be isolated in a DMZ? Can compensating controls (like a dedicated firewall or strict ACL) be applied?.[33]
3. **Approval:** The exception must be approved by both the business owner (who accepts the operational risk) and the CISO or Security Architect.[34]
4. **Implementation:** Upon approval, the device is added to a specific "Exception Group" in the NAC solution, typically with a time-limited access policy.[24]
5. **Review:** All exceptions must be subject to periodic recertification (e.g., every 90 days). If the exception is not renewed, access is automatically revoked.[33]

6.2 Fail-Open vs. Fail-Closed Decisions

A critical architectural decision that must be made prior to the pilot involves the system's behavior during a failure. If the NAC server (RADIUS) becomes unreachable due to a WAN outage, server crash, or other failure, what happens to the switch ports? This decision represents a trade-off between **Availability** and **Security**.

- **Fail-Open (Critical Authentication VLAN):** In this scenario, if the switch cannot reach the NAC server, it fails open and allows traffic on a specific VLAN.
    - *Pro:* Business continuity is maintained; users can still work, and critical systems remain online.
    - *Con:* The security posture is compromised. During the outage, unauthorized devices could potentially connect to the network.[11]
- **Fail-Closed:** In this scenario, if the NAC server is unreachable, the switch blocks all new authentication attempts.
    - *Pro:* The security perimeter remains intact; no unauthorized access is possible.

    - *Con:* Significant business disruption. No new users can log in, and re-authenticating devices will be dropped.[11]

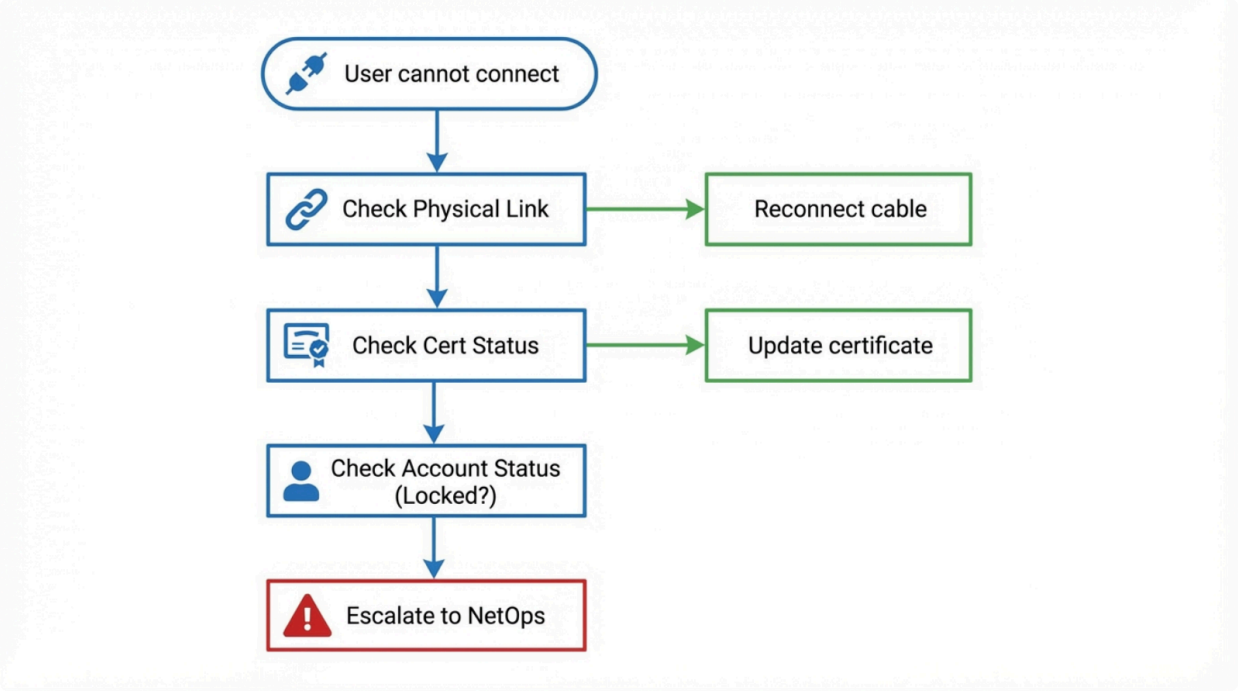
For the pilot and most general corporate office environments, a **Fail-Open** approach is strongly recommended to prioritize availability and minimize disruption. The risk of a temporary security gap during a server outage is generally considered acceptable compared to the cost of a complete site outage.[11] However, for high-security zones such as R&D labs or Data Centers, a Fail-Closed model might be appropriate. This decision must be explicitly documented in the project's risk register.[36] The risk assessment matrix inherently places "Fail-Open" in the quadrant of "High Security Risk / Low Availability Risk" and "Fail-Closed" in "Low Security Risk / High Availability Risk," guiding stakeholders to choose based on their specific risk appetite for the pilot site.

6.3 Helpdesk Enablement and Troubleshooting

The immediate impact of a NAC pilot will be felt most acutely by the Helpdesk. When a user cannot connect to the network, the perception is almost always that "the network is down." Without proper tools, training, and workflows, the Helpdesk will escalate every connectivity issue to the Network or Security team, creating a bottleneck that can stall the project.[20]
The pilot delivery plan must therefore include robust enablement for the support team:

- **Decision Trees:** Simple, logic-based flowcharts for Tier 1 support to diagnose issues. For example: "Is the certificate expired?" -> "Re-enroll via portal" -> "Issue Resolved".[37]
- **Access to Logs:** Tier 1 and 2 support should be granted read-only access to the NAC "Live Logs" or a simplified dashboard. This allows them to see *why* a user was rejected (e.g., "Wrong Password," "Certificate Expired," "Unknown Device") rather than guessing.[9]
- **Remediation Scripts:** Automated tools or clear, step-by-step instructions on how to remediate common compliance issues (e.g., force a Group Policy update, restart the dot3svc service, renew a certificate).[28]

Tier 1 Troubleshooting Logic for NAC Connectivity



This decision tree empowers Tier 1 support to resolve common NAC issues without escalation. It focuses on validating physical connectivity, credential health, and device compliance before flagging the issue as a network fault.

7. Implementation Roadmap and Next Steps

The following roadmap outlines the immediate actions required to initiate the pilot and guide the project through to a successful conclusion.

7.1 Phase 0: Preparation (Weeks 1-4)

- **Activities:** Conduct a detailed inventory of network devices and assess compatibility with 802.1X/MAB.[1] Verify the health of the PKI and the efficacy of certificate distribution mechanisms.[9] Define the Pilot Group (users, devices, locations) and ensure it represents a cross-section of the organization.[16] Establish the Governance and Exception processes.[33]
- **Deliverables:** Network Readiness Assessment, Pilot Charter, Exception Policy Document.

7.2 Phase 1: Discovery & Visibility (Weeks 5-8)

- **Activities:** Enable NAC in "Monitor Mode" at the pilot site. Configure the system to ingest data from DHCP, SNMP, and switch tables.[6] Collect data for at least 4 weeks to

capture a full monthly business cycle (e.g., month-end processing, backups).[3] Analyze "Unknown" devices and begin building MAB groups and profiling rules.[1]
- **Deliverables:** Asset Inventory Report, Unknown Device Remediation Plan.

7.3 Phase 2: Policy Validation (Weeks 9-12)

- **Activities:** Draft the Policy Matrix based on the data gathered during Discovery.[9] Simulate policies against historical logs to determine impact ("What would have been blocked?").[39] Move the pilot site to "Low-Impact Mode" (Auth enabled, but with a Permit-All ACL/VLAN for failed devices) to test the authentication flow without blocking traffic.[3]
- **Deliverables:** Finalized Policy Matrix, Pilot Test Results, Helpdesk Training Sessions.

7.4 Phase 3: Enforcement (Weeks 13+)

- **Activities:** Transition to "Closed Mode" (Enforcement) for the pilot group.[3] Closely monitor helpdesk metrics, authentication latency, and user feedback.[14] Review and refine policies based on false positives and exception requests.[40] Begin planning for the global rollout based on pilot lessons learned.
- **Deliverables:** Pilot Success Report, Global Rollout Plan.

8. Operational Realities: The "Day 2" Challenge

While the architectural design and pilot phases often garner the most attention, the long-term success of a NAC deployment is ultimately determined by "Day 2" operations—the ongoing management and maintenance of the system after the initial rollout. The project team must be prepared for the reality that the network is a living organism; new devices are constantly introduced, employees change roles, and business processes evolve. A rigid NAC policy that does not adapt to these changes will inevitably become a blocker to business agility, leading to its eventual disablement or bypass.[22]

8.1 Lifecycle Management of Certificates and Secrets

A critical operational expectation is the ongoing management of the credentials that underpin the trust model. Machine and user certificates have finite lifespans. If the automated renewal process (e.g., via SCEP or Group Policy) fails, devices will suddenly be rejected from the network, causing mass outages that appear to be network failures but are actually PKI failures.[9] The pilot must include rigorous testing of the certificate renewal workflow to ensure it is seamless. Additionally, the "shared secrets" used for RADIUS communication between switches and the NAC servers must be rotated periodically in accordance with security best practices, a process that requires careful coordination to prevent downtime.[41]

8.2 The "My Device is Blocked" Fatigue

Security teams must anticipate "alert fatigue" and "blocking fatigue." In the early stages of enforcement, valid business devices *will* inevitably be blocked due to missing profiles or

unusual behavior. If the process to unblock a device is cumbersome (e.g., a 24-hour SLA ticket), users will find workarounds—such as plugging into an unmanaged port or using a cellular hotspot—creating "shadow IT" that defeats the purpose of NAC.[31] The expectation for the pilot is to establish a "rapid response" channel for NAC blocks, potentially empowering local IT support with limited administrative rights to override a block temporarily while a root cause is investigated.[6]

8.3 Integration with Security Operations (SecOps)

Finally, the NAC solution should not operate in a silo. It is a rich source of telemetry that should be fed into the organization's SIEM (Security Information and Event Management) system. The logs generated by NAC—who connected, from where, with what device, and at what time—are invaluable for incident response and threat hunting.[6] For the pilot, the expectation should be that NAC logs are forwarded to the SIEM, and basic correlation rules are established (e.g., alerting on repeated authentication failures or unauthorized MAC spoofing attempts).[6] This integration transforms NAC from a simple gatekeeper into a proactive sensor in the wider cybersecurity mesh.

By setting these clear expectations—emphasizing the need for visibility, the complexity of architectural dependencies, and the rigorous operational governance required—the organization can approach the NAC pilot not as a simple hardware install, but as a strategic security transformation. This plan prioritizes business continuity while steadily marching towards the goal of a secured, zero-trust network edge.

Works cited

1. NAC Cyber Security: Core Components, Pros/Cons and Best Practices - Tigera.io, accessed February 3, 2026, https://www.tigera.io/learn/guides/microsegmentation/nac-cyber-security/
2. Network Access Control (NAC): Use Cases & Best Practices - Fortinet, accessed February 3, 2026, https://www.fortinet.com/blog/industry-trends/use-cases-for-network-access-control-nac-solutions
3. Heavy Networking 608: Everything You Ever Wanted To Know About NAC (And Then Some), accessed February 3, 2026, https://packetpushers.net/podcasts/heavy-networking/hn608-everything-you-ever-wanted-to-know-about-nac-and-then-some/
4. Service Now CMDB - ClearPass - HPE Aruba Networking, accessed February 3, 2026, https://arubanetworking.hpe.com/techdocs/NAC/clearpass/integrations/asset-management/service-now/
5. Managed vs. Unmanaged Network Devices: Why It Matters for Commercial Real Estate Companies - 5Q Partners, accessed February 3, 2026, https://www.5qpartners.com/post/managed-vs-unmanaged-network-devices
6. LAN Segmentation & Network Access Control (NAC) Best Practices - Intelligent Visibility, accessed February 3, 2026,

https://intelligentvisibility.com/campus-networking/segmentation-network-access-control
7. EAP-TLS Explained: How It Works and Why It's Secure, accessed February 3, 2026, https://www.securew2.com/blog/what-is-eap-tls
8. Extensible Authentication Protocol (EAP) for network access in Windows | Microsoft Learn, accessed February 3, 2026, https://learn.microsoft.com/en-us/windows-server/networking/technologies/extensible-authentication-protocol/network-access
9. Implementing Network Access Control: Checklist for IT Teams - Cloudi-Fi, accessed February 3, 2026, https://www.cloudi-fi.com/blog/implementing-network-access-control-checklist-for-it-teams
10. User or machine EAP-TLS authentication for the first time - Cisco Community, accessed February 3, 2026, https://community.cisco.com/t5/network-access-control/user-or-machine-eap-tls-authentication-for-the-first-time/td-p/5254520
11. Fail-open & Fail-close explanation - Cisco Community, accessed February 3, 2026, https://community.cisco.com/t5/security-knowledge-base/fail-open-amp-fail-close-explanation/ta-p/5012930
12. Understanding 802.1X and NAC: 3 Problems to Avoid - Fortinet, accessed February 3, 2026, https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-understanding-nac.pdf
13. NAC Deployment: A Five Step Methodology - Opus One®, accessed February 3, 2026, http://www.opus1.com/www/whitepapers/nac_deployment.pdf
14. 7 Tips for a Successful Pilot: How Large Organizations Evaluate Samsara's ROI, accessed February 3, 2026, https://www.samsara.com/blog/tips-for-successful-pilot-evaluating-roi
15. 5 Best Practices for Agencies to Implement Network Access Control | StateTech Magazine, accessed February 3, 2026, https://statetechmagazine.com/article/2018/06/5-best-practices-agencies-implement-network-access-control
16. Pilot Project: Meaning, Benefits and Example - ProjectManager, accessed February 3, 2026, https://www.projectmanager.com/blog/pilot-project
17. Project Success Criteria Guide | Smartsheet, accessed February 3, 2026, https://www.smartsheet.com/content/project-success-criteria
18. Competency Assessment and Evaluation for Pilots, Instructors and Evaluators Guidance Material - IATA, accessed February 3, 2026, https://www.iata.org/contentassets/c0f61fc821dc4f62bb6441d7abedb076/competency-assessment-and-evaluation-for-pilots-instructors-and-evaluators-gm.pdf
19. Troubleshooting Common Issues in NAC Implementation - EOXS, accessed February 3, 2026, https://eoxs.com/new_blog/troubleshooting-common-issues-in-nac-implementation/

20. Decision Trees for Helpdesk Advisor Graphs - arXiv, accessed February 3, 2026, https://arxiv.org/pdf/1710.07075
21. Cisco ISE: Wired 802.1X Deployment in Monitor Mode - LookingPoint, accessed February 3, 2026, https://www.lookingpoint.com/blog/cisco-ise-wired-802.1x-deployment-monitor mode
22. Why NAC Projects Stall: The Hidden Technical Complexities and NAC Alternatives Reshaping Network Security - Elisity, accessed February 3, 2026, https://www.elisity.com/blog/why-nac-projects-stall-the-hidden-technical-complexities-and-nac-alternatives-reshaping-network-security
23. Best practices to prevent MAC spoofing for wired devices that can't do 802.1x - Reddit, accessed February 3, 2026, https://www.reddit.com/r/networking/comments/1o6q07w/best_practices_to_prevent_mac_spoofing_for_wired/
24. ClearPass Wired Policy Enforcement Guide | TechDocs - NAC - HPE Aruba Networking, accessed February 3, 2026, https://arubanetworking.hpe.com/techdocs/NAC/clearpass/platform/wired-policy-enforcement/
25. ISE Profiling Design Guide - Cisco Community, accessed February 3, 2026, https://community.cisco.com/t5/security-knowledge-base/ise-profiling-design-guide/ta-p/3739456
26. Take the IoT Guesswork Out of Your NAC Solution - Palo Alto Networks Blog, accessed February 3, 2026, https://www.paloaltonetworks.com/blog/network-security/take-the-iot-guesswork-out-of-your-nac-solution/
27. NAC bypass with MAC spoofing - Information Security Stack Exchange, accessed February 3, 2026, https://security.stackexchange.com/questions/201849/nac-bypass-with-mac-spoofing
28. [Day 144] Cisco ISE Mastery Training: Automated Remediation for Non-Compliance - Network Journey, accessed February 3, 2026, https://networkjourney.com/day-144-cisco-ise-mastery-training-automated-remediation-for-non%E2%80%91compliance/
29. ISE Posture Compliance - Part 1 - YouTube, accessed February 3, 2026, https://www.youtube.com/watch?v=XSv7BIXqpAs
30. [Day 143] Cisco ISE Mastery Training: Advanced Posture Multi-Condition Compliance, accessed February 3, 2026, https://networkjourney.com/day-143-cisco-ise-mastery-training-advanced-posture-multi%E2%80%91condition-compliance/
31. When NAC Meets Reality: Exceptions Everywhere - Genians, accessed February 3, 2026, https://www.genians.com/learn-more/insights/when-nac-meets-reality-exceptions-everywhere/
32. Information Security Policy Exception Process - UCSD Blink, accessed February 3, 2026, https://blink.ucsd.edu/technology/security/policies/exception.html

33. Information Security Exception Policy - CIS, accessed February 3, 2026, https://www.cisecurity.org/wp-content/uploads/2020/06/Information-Security-Exception-Policy.docx
34. Security Policy and Risk Exception Request Form, accessed February 3, 2026, https://www.mdc.edu/oit/documents/security-policy-and-risk-exception-request-form.pdf
35. Fail Open or Fail Closed? - HYAS, accessed February 3, 2026, https://www.hyas.com/blog/fail-open-or-fail-closed
36. Fail Closed, Fail Open, Fail Safe and Failover: ABCs of Network Visibility | Keysight Blogs, accessed February 3, 2026, https://www.keysight.com/blogs/en/tech/nwvs/2020/05/20/fail-closed-fail-open-fail-safe-and-failover-abcs-of-network-visibility
37. Using Decision Tree to Troubleshoot - NetBrain, accessed February 3, 2026, https://www.netbraintech.com/docs/ie100/help/using-decision-tree-to-troubleshoot.htm
38. What Is a Helpdesk Decision Tree? - Process Shepherd, accessed February 3, 2026, https://processshepherd.com/content/what-is-a-helpdesk-decision-tree/
39. Troubleshooting Cisco's ISE without TAC - Network World, accessed February 3, 2026, https://www.networkworld.com/article/950272/troubleshooting-ciscos-ise-without-tac.html
40. How to Set up a Successful NAC Project - Portnox, accessed February 3, 2026, https://www.portnox.com/blog/network-access-control/how-to-set-up-a-successful-nac-project/
41. Cisco ISE Troubleshooting - Part 1 - YouTube, accessed February 3, 2026, https://www.youtube.com/watch?v=AxgtXynug_E