CONFIDENTIAL — SAMPLE / DEMONSTRATION

NETWORK PENETRATION TESTING REPORT

NorthStar Financial Services — Fictional Sample Assessment

2026 Illustrative Sample Deliverable

Organization	NorthStar Financial Services, Inc. (Fictional)
Industry	Financial Services / FinTech
Headquarters	New York, United States (Fictional)
Assessment	External and Internal Network Penetration Testing
Prepared By	TMG Security
Assessment Period	03 August 2026 – 28 August 2026
Report Date	10 September 2026
Classification	CONFIDENTIAL — SAMPLE / DEMONSTRATION

FICTIONAL SAMPLE — NOT AN ACTUAL CLIENT NETWORK PENETRATION TEST

All systems, IP addresses, hostnames, credentials, configurations, findings, and evidence shown in this document are fictional or synthetic.

DOCUMENT CONTROL

Document Title	Network Penetration Testing Report — NorthStar Financial Services (Fictional Sample)
Document ID	TMG-NET-NSF-2026-001
Version	1.0
Issue Date	10 September 2026
Assessment Period	03 August 2026 – 28 August 2026
Assessment Type	External and Internal Network Penetration Testing
Client	NorthStar Financial Services, Inc. (Fictional)
Environment	Fictional production-like enterprise environment with isolated test infrastructure
Standards Referenced	PTES concepts, NIST SP 800-115 concepts, CVSS v3.1-inspired scoring
Prepared By	TMG Security Offensive Security Team
Technical Lead	TMG Security — Lead Network Penetration Tester (Fictional Engagement Role)
Reviewed By	TMG Security Quality Assurance Lead
Classification	CONFIDENTIAL — SAMPLE / DEMONSTRATION

Version History

Version	Date	Author	Summary
1.0	10 September 2026	TMG Security Offensive Security Team	Initial issue — fictional sample deliverable.

Distribution List

The following fictional distribution list reflects the recipients TMG Security would designate for an engagement of this type; no real individuals are named.

Recipient (Fictional Role)	Organization	Purpose
Chief Information Security Officer	NorthStar Financial Services, Inc.	Executive sponsor and primary report recipient.
VP of Infrastructure Engineering	NorthStar Financial Services, Inc.	Remediation ownership and infrastructure prioritization.
Director of Network Security	NorthStar Financial Services, Inc.	Coordinates retest scheduling and finding tracking.
Engagement Manager	TMG Security	Client relationship management and delivery oversight.
Quality Assurance Lead	TMG Security	Independent technical review of this report prior to issue.

Authorship

Name (Fictional Role)	Role	Contribution
Daniel Reyes	Lead Network Penetration Tester	External/internal testing, attack-path validation, report authorship.
Priya Anand	Active Directory Security Consultant	AD assessment, segmentation testing, evidence collection.
Marcus Whitfield	Network Security Consultant	Network device, wireless, and cloud/hybrid testing.
Elena Marquez	Quality Assurance Lead	Independent technical review and report quality assurance.
David Okafor	Engagement Manager	Scoping, rules of engagement, and client coordination.

IMPORTANT DISCLAIMER

FICTIONAL SAMPLE REPORT — NOT AN ACTUAL CLIENT NETWORK PENETRATION TEST

This report has been produced solely for demonstration and portfolio purposes on behalf of TMG Security. It is intended to illustrate the structure, technical depth, and professional reporting standard of a network penetration testing deliverable built on PTES and NIST SP 800-115 concepts, and is presented as the network counterpart to TMG Security's companion API, Android, and iOS application sample reports. To ensure there is no ambiguity regarding the nature of this document, TMG Security sets out the following clarifications:

- NorthStar Financial Services, Inc. is a fictional entity. It does not correspond to any real company, and any resemblance to an actual organization is purely coincidental.
- All domains referenced throughout this report (northstar-example.com, vpn.northstar-example.com, portal.northstar-example.com, mail.northstar-example.com) are fictional, non-resolving placeholder domains used only for illustration.
- All IP addresses referenced throughout this report use documentation-only private ranges (10.40.0.0/16, 10.50.0.0/16, 172.20.0.0/16) and do not correspond to any real address allocation.
- No real client was engaged and no real client network, system, device, or infrastructure was tested.
- No production environment, network, cloud resource, or system of any kind was accessed, scanned, or tested in the creation of this report.
- No real user data, personal information, payment card data, or customer records were accessed, viewed, or processed.
- No real credentials — including device, application, VPN, domain, or network device credentials — were used or are disclosed anywhere in this report.
- All configuration excerpts, command output, log snippets, and network captures shown in this report are synthetic and constructed for illustration only.
- All vulnerabilities, findings, risk ratings, CVSS-style scores, dates, and remediation statuses described in this report are fictional and were constructed for demonstration purposes.
- All Proofs of Concept (PoCs) are illustrative, synthetic, and non-destructive; none were executed against a real or live target, network, or production backend.
- All screenshots and tool-style evidence panels (Nmap-style, SMB/LDAP enumeration-style, SNMP-style, terminal captures, dashboards) are synthetic mock-ups created specifically for this sample report, not real tool output.
- No real exploitation occurred at any point during the preparation of this document, and no actual customer impact occurred.
- TMG Security is not affiliated with, endorsed by, reviewed by, or certified by PTES, NIST, or any standards body; references to PTES and NIST SP 800-115 describe the testing methodology used and do not imply any official certification of NorthStar Financial Services or TMG Security.
- This report does not represent an actual TMG Security client engagement and must not be relied upon as evidence of the security posture of any real organization.

Intended Use

This sample report may be shared with prospective clients, partners, and other interested parties to illustrate TMG Security's network penetration testing methodology, technical reporting standards, and evidence-presentation quality. It should not be relied upon for any compliance, legal, contractual, or procurement decision, and does not constitute security advice regarding any real network or organization.

TABLE OF CONTENTS

01 EXECUTIVE SUMMARY

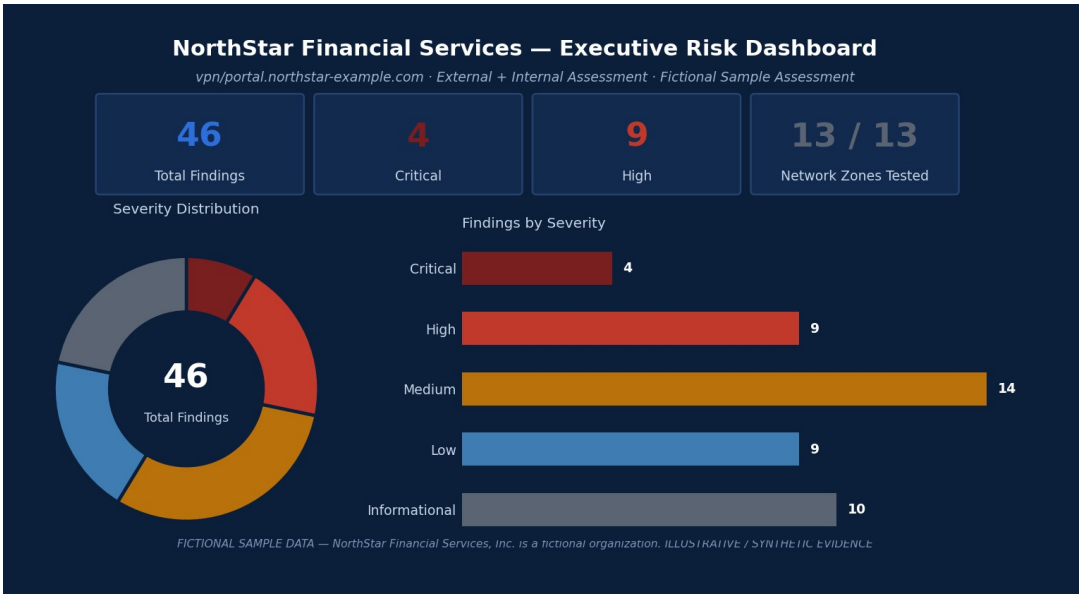
TMG Security has prepared this fictional, illustrative Network Penetration Testing report to represent NorthStar Financial Services, Inc., a hypothetical U.S.-based financial services organization headquartered in New York, and its enterprise network. This section presents a fictional executive-level summary of the simulated assessment — covering external perimeter testing, internal assumed-breach testing, Active Directory security, network segmentation validation, network device and wireless security, and cloud/hybrid connectivity — prepared as the network counterpart to TMG Security's companion API, Android, and iOS application sample reports, in the style and format TMG Security would use for an actual client engagement.

Overall Illustrative Security Posture

REQUIRES REMEDIATION

NorthStar's simulated network environment demonstrates a number of established security controls — including consistent centralized logging, application-aware perimeter filtering, and mandatory MFA on the primary VPN login path — but the fictional assessment identified material weaknesses concentrated in network segmentation, Active Directory credential hygiene, and network device management-plane exposure. These require prioritized remediation before the environment should be considered ready for a broader trust posture. This illustrative status reflects a sample network penetration-testing exercise and does not represent a certification or compliance decision.

Fictional Sample Dashboard



Illustrative severity distribution across all 46 fictional findings — FICTIONAL SAMPLE DATA.

Executive Risk Narrative

The fictional assessment identified 46 illustrative findings across NorthStar's external perimeter, internal network, and supporting infrastructure: 4 Critical, 9 High, 14 Medium, 9 Low, and 10 Informational. The four Critical findings concern the

most fundamental trust-boundary failures observed: a legacy VPN authentication endpoint that bypasses mandatory MFA (NET-001); a segmentation gap giving the User Workstation VLAN unrestricted reachability to the primary transactional database (NET-002); a Domain Admin-equivalent service account credential recoverable by any standard domain user from a legacy SYSVOL artifact (NET-003); and an exposed, default-credentialed management plane on the organization's core switch and internal firewall (NET-004).

The nine High findings span SMB signing gaps on critical servers (NET-005), cleartext LDAP credential exposure (NET-006), fleet-wide excessive helpdesk administrative rights (NET-007), weak legacy VPN cryptography (NET-008), guessable SNMP community strings on core network devices (NET-009), unrestricted RDP reachability across segmentation boundaries (NET-010), a wireless-based path to the management plane (NET-011), an unauthenticated backup repository reachable from the User VLAN (NET-012), and Kerberoastable service account credentials (NET-013). Consistent with the pattern observed in the Critical findings, these High-severity issues concentrate around network segmentation and Active Directory credential and privilege management — precisely the areas this report's methodology was designed to probe.

Medium-severity findings reflect defense-in-depth and hardening gaps — outdated TLS configuration on the remote access portal, DNS zone-transfer exposure, unauthenticated monitoring dashboards, unconstrained Kerberos delegation on a legacy application server, excessive Domain Admins membership, and a weak domain password policy, among others. Low and Informational findings are hardening and governance opportunities — wireless PSK rotation, network device firmware currency, configuration-backup storage hygiene, and positive-control observations such as consistent MFA enforcement on the primary VPN path and centralized SIEM logging — that support a stronger long-term security posture without representing an immediate exploitation path in this fictional sample.

TMG Security's simulated recommendation is that NorthStar prioritize closure of the four Critical and nine High findings within the first 60 days of the illustrative remediation roadmap (see Section 25), with particular attention to network segmentation, Active Directory credential exposure, and management-plane access control. Medium findings should be addressed within 90 days, and Low/Informational items tracked as part of an ongoing hardening and governance program, including the segmentation and firewall-rule recertification processes recommended in Sections 24-26.

02 ASSESSMENT OVERVIEW

This engagement was a fictional, illustrative external and internal network penetration test performed by TMG Security against a simulated enterprise environment representing NorthStar Financial Services, Inc. The assessment combined black-box/grey-box external testing with assumed-breach internal testing, and included a dedicated Active Directory security assessment, network segmentation validation, network device review, and wireless security testing.

Organization	NorthStar Financial Services, Inc. (Fictional)
Assessment Type	External and Internal Network Penetration Testing
Assessment Perspectives	External Black-Box/Grey-Box, Internal Assumed-Breach
Assessment Period	03 August 2026 – 28 August 2026
Report Date	10 September 2026
Standards Referenced	PTES concepts, NIST SP 800-115 concepts, CVSS v3.1-inspired scoring, CWE
Total Findings	46 (4 Critical, 9 High, 14 Medium, 9 Low, 10 Informational)
Total Test Cases Executed	152 (Appendix G)

Assessment Objective

The objective of this fictional assessment was to identify, safely validate, and provide remediation guidance for exploitable weaknesses across NorthStar's external attack surface and internal network — including Active Directory, network segmentation, network device configuration, and wireless infrastructure — and to demonstrate realistic, non-destructive attack paths an adversary could use to compromise sensitive systems and data.

03 SCOPE

The following fictional infrastructure was in scope for this assessment, spanning the external perimeter, internal network zones, network security devices, Windows/enterprise infrastructure, Linux/application infrastructure, cloud/hybrid connectivity, and wireless networks.

External Perimeter

- Internet-facing VPN gateway (vpn.northstar-example.com)
- Remote access portal (portal.northstar-example.com)
- Public web application gateway / WAF
- External DNS infrastructure
- Email security gateway (mail.northstar-example.com)
- External perimeter firewall
- External load balancer
- Bastion / jump host
- Externally reachable remote administration surface

Internal Network Zones

- User Workstation VLAN

- Server VLAN
- Application VLAN
- Database VLAN
- Identity / AD VLAN
- Management VLAN
- Security Tooling VLAN
- Backup VLAN

Network Security Devices

- Next-generation firewalls (external and internal)
- Core switch
- Distribution switches
- Wireless LAN controller
- Network management platform

Windows / Enterprise Infrastructure

- Active Directory domain controllers
- Windows file server
- Windows application server
- Windows management server
- Internal PKI / certificate services
- Internal DNS
- Internal monitoring server

Linux / Application Infrastructure

- Linux application server
- Internal API server
- Monitoring server
- Logging / SIEM collector
- Backup server

Cloud / Hybrid Connectivity

- Fictional cloud connectivity (site-to-site VPN)
- Hybrid identity synchronization server
- Cloud management interface

Wireless Networks

- Corporate SSID (NSF-CORP)
- Guest SSID (NSF-GUEST)
- Management SSID (NSF-WLAN-MGMT)

Out-of-Scope

- Any production system, network, or data belonging to a real organization — this entire engagement, its target environment, and its findings are fictional.
- Denial-of-service testing of any kind, including resource-exhaustion or availability-impacting techniques.
- Physical security testing (badge cloning, lock bypass, tailgating).
- Social engineering campaigns targeting fictional NorthStar personnel.
- Destructive exploitation, data modification, data deletion, or ransomware-style techniques.
- Third-party vendor infrastructure not directly operated by the fictional NorthStar IT organization.

- Cloud provider infrastructure below the fictional tenant/management layer explicitly listed in scope.
- Production change requests — all configuration observations are point-in-time and advisory.

04 RULES OF ENGAGEMENT

The following rules of engagement governed this fictional assessment, consistent with the format TMG Security uses for real client engagements.

Authorized Scope

Testing was authorized only against the assets, IP ranges, and domains explicitly listed in Section 03 (Scope) and Appendix A (Scope Register); this entire engagement is fictional and no real infrastructure was involved.

Testing Windows

External testing was conducted during a defined fictional testing window (03-14 August 2026); internal/assumed-breach testing was conducted 17-28 August 2026, both with fictional NorthStar IT operations notified in advance.

Safe Testing

All testing techniques were selected to avoid service disruption, data modification, or data loss; any technique with a meaningful availability risk required documented pre-approval.

Prohibited Activities

Denial-of-service techniques, destructive exploitation, physical security testing, and social engineering were explicitly out of scope for this engagement.

Emergency Contacts

A fictional emergency contact and stop-work escalation path was established with the client engagement sponsor and TMG Security's engagement manager for the duration of testing.

Evidence Handling

All evidence captured during testing is treated as confidential client data; for this fictional sample report, all evidence is synthetic and was never derived from a real system.

Data Handling

No production data was accessed, exfiltrated, or retained at any point, consistent with the fictional nature of this assessment.

Communication

Status updates were provided at agreed intervals throughout testing, with immediate notification procedures defined for any Critical finding requiring urgent client attention.

Stop Conditions

Testing would be paused immediately upon any sign of unintended service impact, with resumption only after client confirmation; no such condition arose during this fictional assessment.

05 TESTING METHODOLOGY

TMG Security's network penetration testing methodology draws on concepts from the Penetration Testing Execution Standard (PTES) and NIST SP 800-115, adapted to a network-appropriate structure rather than the OWASP web/mobile methodologies used in TMG Security's companion application security sample reports. TMG Security is not certified by, or affiliated with, PTES or NIST; these are referenced as methodology frameworks only.

Phase	Description
Pre-Engagement	Scope confirmation, rules of engagement sign-off, target and credential provisioning, and emergency-contact exchange with the fictional NorthStar engagement sponsor.
Rules of Engagement	Formal agreement on testing windows, authorized techniques, prohibited activities, and stop conditions, documented in Section 04 of this report.
Reconnaissance	Passive and active information gathering against the external attack surface — DNS, WHOIS, certificate transparency, and public-source review — without touching out-of-scope infrastructure.
Attack Surface Discovery	Enumeration of all in-scope external and internal hosts, culminating in the asset register (Appendix B).
Service Enumeration	Port and service discovery across all in-scope hosts, producing the service/port register (Appendix C).
Vulnerability Analysis	Correlation of enumerated services and configurations against known weakness classes, authenticated and unauthenticated.
Configuration Review	Manual review of firewall, network device, Active Directory, and wireless configuration against current hardening guidance.
Authentication Testing	Assessment of authentication mechanisms across VPN, remote administration, and directory services, including MFA enforcement consistency.
Network Segmentation Testing	Validation of the segmentation matrix (Appendix E) against observed live traffic flows across all documented zone pairs.
Active Directory Security Assessment	Domain architecture, trust, privileged group, service account, and credential-exposure review, summarized in the AD assessment matrix (Section 13).
Lateral Movement Assessment	Controlled, non-destructive demonstration of lateral movement paths made possible by chained findings.
Privilege Escalation Assessment	Controlled, non-destructive demonstration of privilege-escalation paths from standard to privileged access.
Exposure Validation	Confirmation that identified weaknesses represent genuine, reproducible exposure rather than false positives.
Controlled Exploitation	Safe, non-destructive proof-of-concept execution for Critical and High findings only, with no data modification, deletion, or service disruption.
Post-Exploitation Validation	Confirmation of the practical impact of a successful technique (e.g., session establishment, credential recovery) without further action.
Evidence Collection	Capture of illustrative evidence for every finding, mapped to the evidence register (Appendix I).
Risk Rating	Assignment of a CVSS-style illustrative score and severity rating to every finding per the methodology in Section 06.
Remediation	Development of finding-specific and program-level remediation guidance, consolidated in the management action plan and remediation roadmap.
Retest	Post-remediation validation methodology described in Section 26, to be performed once remediation activities are complete.

06 RISK RATING METHODOLOGY

TMG Security assigns each finding a severity rating using language inspired by the CVSS v3.1 scoring framework, considering exploitability, privileges required, user interaction, scope, and technical/business impact. All scores and vectors in this report are illustrative sample estimations assigned for this fictional exercise only — they are not derived from any real vulnerability and are not submitted to any CVSS authority.

Severity Definitions

Severity	Illustrative Score Range	Definition
CRITICAL	9.0 – 10.0	Directly exploitable with severe confidentiality, integrity, or availability impact; typically requires immediate remediation.
HIGH	7.0 – 8.9	Significant impact with limited prerequisites; requires prompt remediation.
MEDIUM	4.0 – 6.9	Moderate impact, often requiring specific conditions or providing defense-in-depth value when fixed.
LOW	0.1 – 3.9	Minor impact; hardening opportunity rather than a directly exploitable weakness.
INFORMATIONAL	N/A	Observation, positive-control note, or recommendation with no direct security-control failure.

Rating Factors Considered

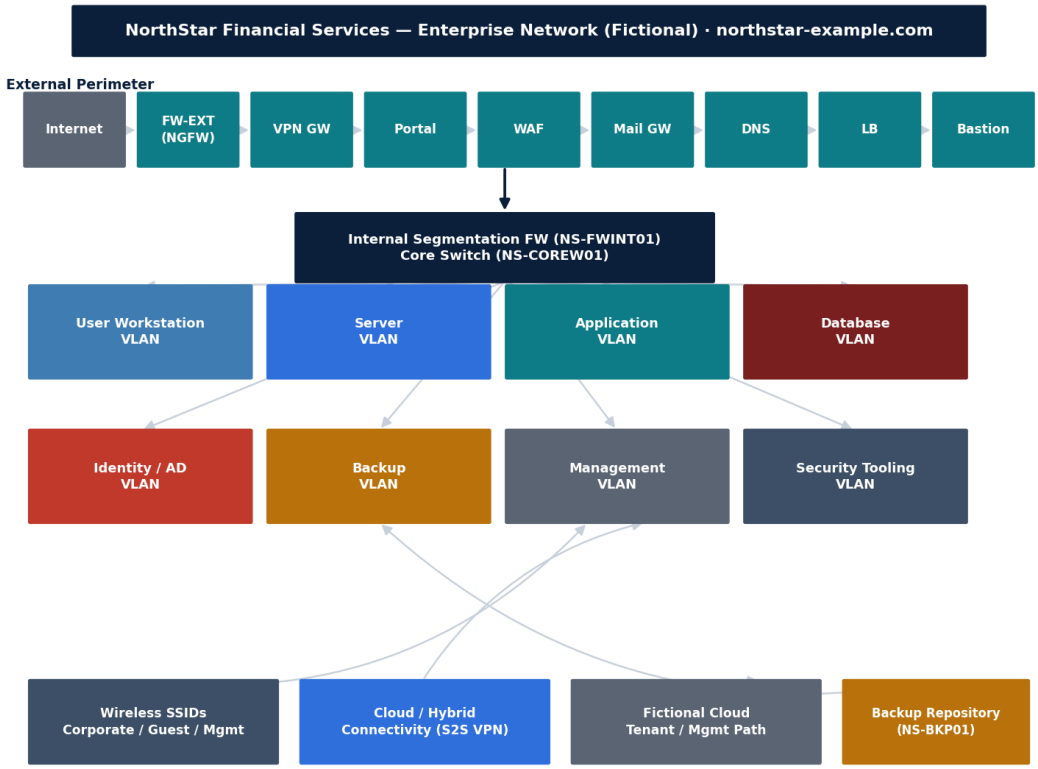
- Exploitability — how readily the fictional weakness could be exercised from the network position assumed.
- Privileges Required — the level of fictional access needed before the weakness is reachable.
- User Interaction — whether a fictional victim action is required.
- Attack Complexity — conditions beyond the attacker's control that must align.
- Scope — whether the weakness affects only the vulnerable component or crosses a trust boundary.
- Technical Impact — effect on confidentiality, integrity, and availability of network and data assets.
- Business Impact — fictional effect on fraud exposure, customer trust, and regulatory posture for a financial services organization.

IMPORTANT

All CVSS-style scores, vectors, severities, and risk ratings in this report are fictional and illustrative.

07 NETWORK ARCHITECTURE

The following fictional architecture diagram illustrates how NorthStar's enterprise network is organized into the external perimeter, thirteen internal network zones, and supporting infrastructure referenced throughout this report. It is provided to give this sample report realistic technical grounding for the findings in later sections.



Illustrative fictional enterprise network architecture — all hostnames, IP ranges, and infrastructure detail are fictional. ILLUSTRATIVE / SYNTHETIC EVIDENCE.

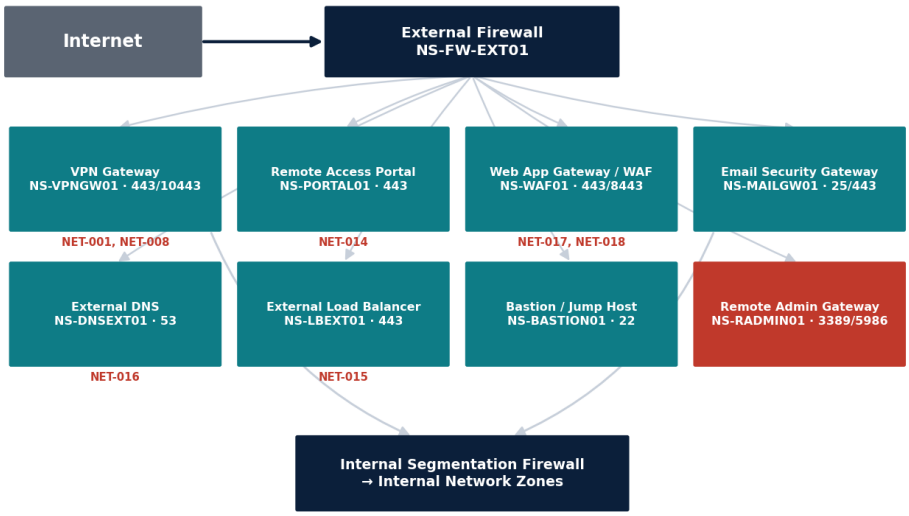
Network Zones

Zone	Address Range	Description
External Perimeter / DMZ	10.40.0.0/24	Internet-facing gateways, VPN, portal, mail, DNS, load balancer, bastion
User Workstation VLAN	10.40.10.0/24	Standard end-user Windows workstations, laptops, VDI clients
Server VLAN	10.40.20.0/24	Windows infrastructure servers — file, application, management, monitoring, PKI, internal DNS
Application VLAN	10.40.30.0/24	Linux application, internal API, logging/SIEM, and monitoring servers
Database VLAN	10.40.40.0/24	Primary transactional and reporting database instances
Identity / AD VLAN	10.40.50.0/24	Active Directory domain controllers and identity infrastructure
Backup VLAN	10.40.60.0/24	Backup repository and backup-management infrastructure
Management VLAN	172.20.10.0/24	Out-of-band management interfaces for network devices, core/distribution switches, firewalls, WLC
Security Tooling VLAN	172.20.20.0/24	Vulnerability scanning and EDR management infrastructure

Zone	Address Range	Description
Wireless — Corporate SSID	10.50.10.0/24	Corporate-issued and BYOD endpoints on the 802.1X corporate SSID
Wireless — Guest SSID	10.50.20.0/24	Guest and visitor wireless clients
Wireless — Management SSID	10.50.30.0/24	Wireless infrastructure management (APs, WLC control plane)
Cloud / Hybrid Connectivity	10.50.0.0/24	Site-to-site VPN termination and hybrid identity/cloud management path

08 EXTERNAL ATTACK SURFACE

NorthStar's fictional external attack surface consists of nine internet-facing systems, each assessed for exposed services, authentication strength, TLS configuration, and unnecessary functionality.

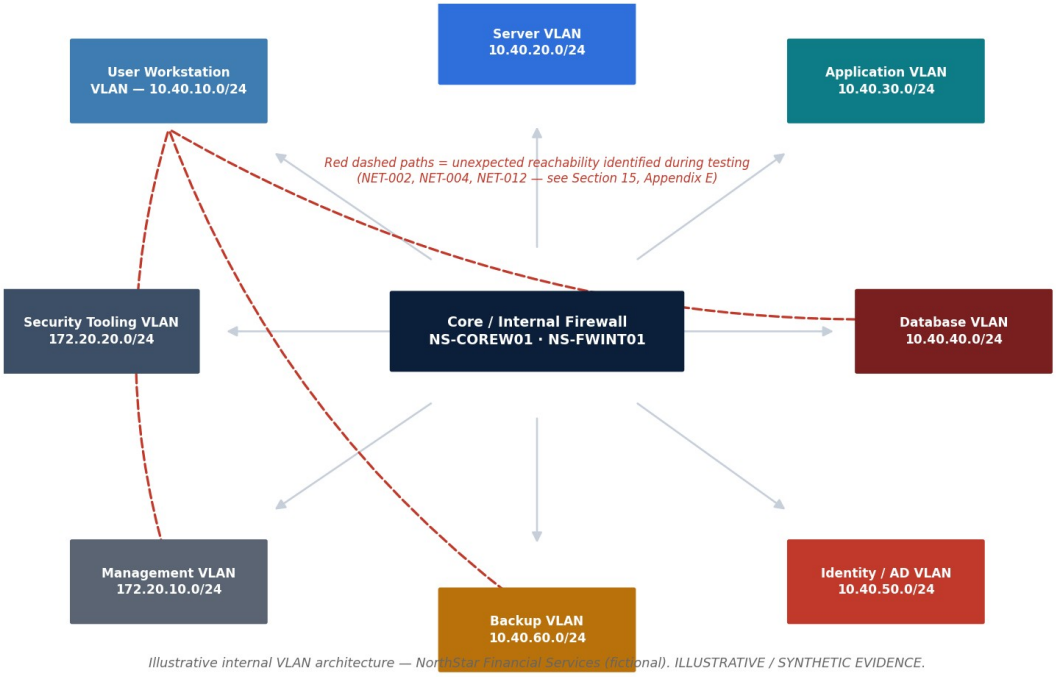


Illustrative external attack surface — NorthStar Financial Services (fictional). Reference tags mark related findings. ILLUSTRATIVE / SYNTHETIC EVIDENCE.

Asset ID	Hostname	IP Address	Purpose	Criticality
NS-A01	NS-FW-EXT01	10.40.0.1	External perimeter firewall / primary internet edge	Critical
NS-A02	NS-VPNGW01	10.40.0.10	Remote-access VPN gateway — vpn.northstar-example.com	Critical
NS-A03	NS-PORTAL01	10.40.0.11	Employee/partner remote access portal — portal.northstar-example.com	High
NS-A04	NS-WAF01	10.40.0.12	Fronts public-facing web applications	High
NS-A05	NS-MAILGW01	10.40.0.13	Inbound/outbound mail filtering — mail.northstar-example.com	High
NS-A06	NS-DNSEXT01	10.40.0.14	Authoritative DNS for northstar-example.com	High
NS-A07	NS-LBEXT01	10.40.0.15	TLS termination and load distribution for public services	Medium
NS-A08	NS-BASTION01	10.40.0.20	Administrative jump host for external vendor and remote admin access	Critical
NS-A09	NS-RADMIN01	10.40.0.21	Externally reachable WinRM/RDP administration surface for on-call engineers	Critical

09 INTERNAL NETWORK ARCHITECTURE

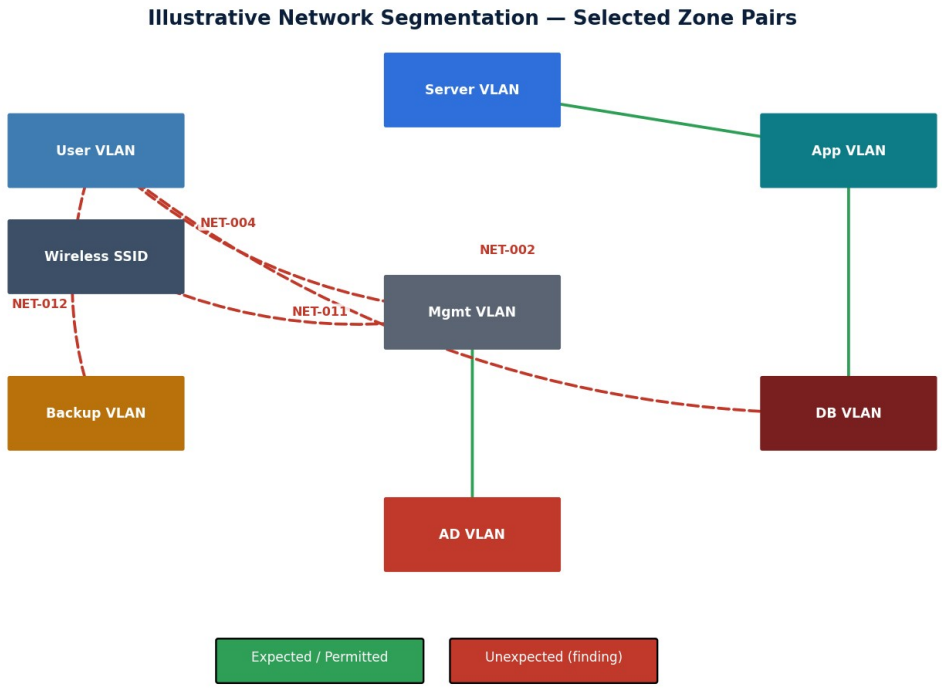
The internal network is organized into eight core VLANs plus three wireless SSIDs, a dedicated Security Tooling VLAN, and a Cloud/Hybrid Connectivity zone, all enforced by the internal segmentation firewall and core switch.



Red dashed paths indicate unexpected reachability identified during testing (see Section 10).

10 NETWORK SEGMENTATION ASSESSMENT

Network segmentation was tested by attempting connections between every documented zone pair and comparing the observed result against NorthStar's intended segmentation policy. The full matrix is provided in Appendix E; selected zone pairs are illustrated below.



Selected zone pairs from the full matrix in Appendix E. ILLUSTRATIVE / SYNTHETIC EVIDENCE.

Source Zone	Destination Zone	Expected	Observed	Risk
User Workstation VLAN	Database VLAN	Denied by default — no direct reachability	Permitted — unrestricted TCP/1433 reachability via overly broad rule	Critical
User Workstation VLAN	Management VLAN	Denied — management plane isolated	Permitted — HTTPS management console reachable, missing ACL	Critical
User Workstation VLAN	Server VLAN (RDP)	Denied — RDP only via NS-MGMT01 jump host	Permitted — direct RDP reachable to multiple servers	High
User Workstation VLAN	Backup VLAN	Denied — backup infrastructure isolated	Permitted — SMB share reachable with broad read permission	High
Guest Wireless SSID	Corporate Network (all zones)	Denied — full isolation	Denied, as expected	None
Guest Wireless SSID	Management VLAN	Denied — full isolation	Denied, as expected	None
Guest Wireless SSID	Printer Subnet (kiosk exception)	Permitted to kiosk device only	Permitted to broader printer subnet than intended	Low
Corporate Wireless SSID	Management VLAN	Denied — except WLC uplink	Permitted — Corporate SSID client range included in source object	High
Corporate Wireless SSID	User Workstation VLAN	Permitted — equivalent to wired user access	Permitted, as expected	None
Application VLAN	Database VLAN	Permitted — TCP/1433 only	Permitted — TCP/1433 plus TCP/135, UDP/1434, TCP/3389	Medium

Source Zone	Destination Zone	Expected	Observed	Risk
Application VLAN	Server VLAN	Permitted — documented integration ports only	Permitted, as documented	None
VPN (post-authentication)	Internal Network (all zones per role)	Full-tunnel, role-scoped split-tunnel exceptions only	Split tunneling enabled by default for all roles	Low
Backup VLAN	User Workstation VLAN	Denied — one-directional isolation	Denied, as expected	None
Identity / AD VLAN	All Zones (authentication/replication)	Permitted per AD functional requirements	Permitted, as expected and required	None
Security Tooling VLAN	All Zones (scoped scanning/EDR)	Permitted, scoped to scanning/EDR ports	Permitted, as documented	None
Cloud / Hybrid Connectivity	Server VLAN (identity sync)	Permitted — scoped to sync endpoints only	Permitted — broader reachability than the sync function requires	Low
External Perimeter / DMZ	User Workstation VLAN	Denied — no direct DMZ-to-user reachability	Denied, as expected	None
External Perimeter / DMZ	Server / Application / Database VLANs	Denied — external hosts do not reach internal tiers directly	Denied, as expected	None

11 EXTERNAL TESTING RESULTS

External testing simulated an internet-based attacker with no internal network access, targeting the VPN gateway, remote access portal, public web application gateway, DNS, email security gateway, load balancer, and bastion host. Findings from this phase are summarized below and detailed in full in Sections 19-23.

Finding ID	Severity	Title
NET-001	CRITICAL	External VPN Authentication Can Be Bypassed Through Legacy Authentication Workflow
NET-008	HIGH	Weak VPN Security Configuration Permits Legacy Cryptographic Negotiation
NET-014	MEDIUM	Outdated TLS Configuration on External Remote Access Portal
NET-015	MEDIUM	Certificate Configuration Issue on External VPN Gateway
NET-016	MEDIUM	DNS Configuration Weakness Permits Zone Transfer from External DNS Server
NET-017	MEDIUM	Exposed Service With Unnecessary Functionality on External Load Balancer
NET-018	MEDIUM	Information Disclosure Through Verbose Error Messages on Public Web Application Gateway
NET-037	INFORMATIONAL	Positive Observation — Next-Generation Firewall Enforces Application-Aware Policy at External Perimeter
NET-039	INFORMATIONAL	Positive Observation — Multi-Factor Authentication Enforced on Primary VPN Login Path
NET-044	INFORMATIONAL	Informational — Legacy DNS Records Identified for Decommissioned Hosts

12 INTERNAL TESTING RESULTS

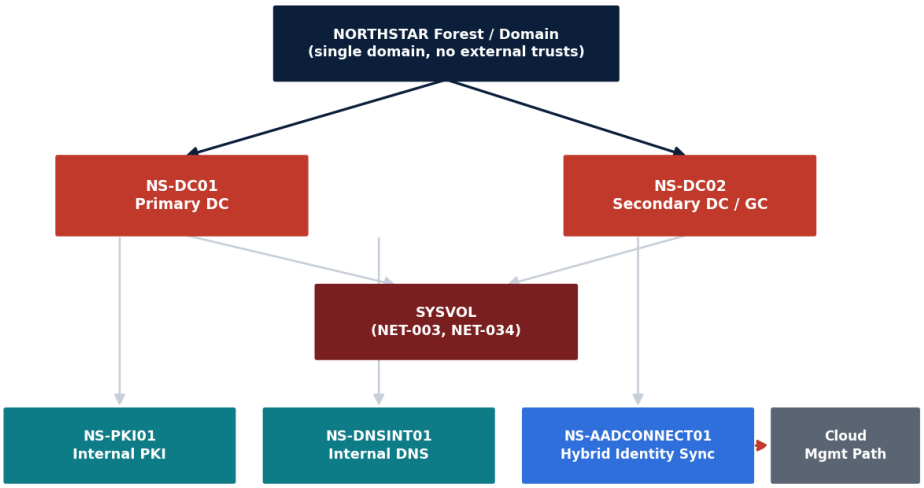
Internal testing simulated a low-privileged internal user with a standard domain-joined workstation on the User Workstation VLAN, consistent with an assumed-breach methodology. Findings from this phase are summarized below and detailed in full in Sections 19-23.

Finding ID	Severity	Title
NET-002	CRITICAL	Insufficient Internal Network Segmentation Enables Unauthenticated Reachability from User VLAN to Database VLAN
NET-005	HIGH	SMB Signing Not Enforced on Critical Internal Windows Servers
NET-007	HIGH	Excessive Administrative Access Across User Network Segment via Helpdesk Group Policy
NET-010	HIGH	RDP Accessible Across Improperly Segmented Network Boundaries
NET-012	HIGH	Sensitive Backup Repository Reachable From User VLAN Without Authentication Segmentation
NET-019	MEDIUM	Legacy/Insecure Protocol Exposure — SMBv1 Still Enabled on Internal File Server

Finding ID	Severity	Title
NET-020	MEDIUM	Unnecessary East-West Connectivity Between Application VLAN and Database VLAN Beyond Required Ports
NET-021	MEDIUM	Insecure Monitoring Interface Exposes Sensitive Telemetry Without Authentication
NET-022	MEDIUM	Weak Internal TLS Configuration on Internal API Server
NET-038	INFORMATIONAL	Positive Observation — Centralized Logging and SIEM Collection Implemented Across Core Infrastructure
NET-041	INFORMATIONAL	Recommendation — Formalize Network Segmentation Review Cadence
NET-042	INFORMATIONAL	Recommendation — Expand SIEM Detection Coverage for Lateral Movement Techniques
NET-045	INFORMATIONAL	Recommendation — Implement Network Access Control (802.1X) on Wired User Ports

13 ACTIVE DIRECTORY ASSESSMENT

The NORTHSTAR Active Directory domain was assessed across domain architecture, trust relationships, privileged groups, service accounts, password policy, LDAP, Kerberos, SMB, SYSVOL, GPO security, and administrative pathways. Findings are not overstated merely because a configuration is uncommon; each finding reflects a validated, reproducible weakness.



Privileged groups (NET-024), service accounts (NET-013), LDAP (NET-006, NET-033), Kerberos delegation (NET-023), and administrative pathways (NET-007, NET-026, NET-040) assessed across this architecture.

Illustrative Active Directory architecture — NorthStar Financial Services (fictional). ILLUSTRATIVE / SYNTHETIC EVIDENCE.

Assessment Area	Summary	Related Findings
Domain Architecture	Single-domain, single-forest design (NORTHSTAR), consistent with the organization's size; no unnecessary forest/domain trust complexity observed.	

Assessment Area	Summary	Related Findings
Domain Controllers	Two domain controllers (NS-DC01, NS-DC02) provide redundancy; both carry the same exposure for LDAP and Kerberos findings identified in this assessment.	NET-006, NET-013, NET-033
Trust Relationships	No external or forest trusts are configured; this significantly limits cross-domain lateral movement risk and was validated as a positive architectural characteristic.	
Privileged Groups	Domain Admins membership exceeds the minimum required for genuine Tier-0 activity, including several accounts used for routine application support.	NET-024
Service Accounts	Several SPN-registered service accounts use stale, non-rotated passwords vulnerable to Kerberoasting; a Domain Admin-equivalent service account credential was recoverable from a legacy SYSVOL artifact.	NET-003, NET-013
Password Policy	The Default Domain Policy enforces only an 8-character minimum with no banned-password-list screening, below current guidance for the organization's risk profile.	NET-025
LDAP	Both domain controllers accept unsigned, unencrypted simple binds, and a limited anonymous bind discloses RootDSE/naming-context information.	NET-006, NET-033
Kerberos	Stale SPN-registered account passwords are Kerberoastable; one legacy application server is configured for unconstrained delegation.	NET-013, NET-023
SMB	SMB signing is not enforced on several critical Windows servers, and SMBv1 remains enabled on the primary file server for legacy device compatibility.	NET-005, NET-019
SYSVOL	A legacy Group Policy Preferences file exposes a Domain Admin-equivalent credential; a related stale credential-path reference was identified in a legacy logon script.	NET-003, NET-034
GPO Security	Group Policy is used appropriately for baseline configuration in most areas reviewed; the Restricted Groups misconfiguration (NET-007) and legacy GPP artifact (NET-003) are the two exceptions identified.	NET-003, NET-007
Administrative Pathways	Tier-1 helpdesk accounts hold both standing local administrator rights fleet-wide and direct interactive RDP access to domain controllers, both inconsistent with a tiered administration model.	NET-007, NET-026
Workstation / Server Trust	No unconstrained delegation was identified on workstation-tier systems; the single instance identified is scoped to a legacy application server (NET-023).	NET-023
Privileged Access	No PAW (Privileged Access Workstation) model is currently in use for Tier-0 administrative activity.	NET-040
Monitoring	AD-relevant events (authentication, privileged group changes) are forwarded to the centralized SIEM; specific detection content for the lateral-movement techniques used in this assessment was not confirmed during interview.	NET-038, NET-042

Assessment Area	Summary	Related Findings
Credential Exposure	The most severe finding of this assessment (NET-003) is a credential-exposure issue; combined with NET-006 and NET-013, credential exposure is the dominant theme across the AD assessment.	NET-003, NET-006, NET-013

Active Directory Findings

Finding ID	Severity	Title
NET-003	CRITICAL	Privileged Active Directory Service Account Credential Exposed Through Insecure Group Policy Preferences Configuration
NET-006	HIGH	Insecure LDAP Configuration Permits Credential Exposure via Unsigned, Unencrypted Bind
NET-013	HIGH	Weak Service Account Security Enables Lateral Movement via Kerberoasting
NET-023	MEDIUM	Kerberos Configuration Weakness — Unconstrained Delegation Enabled on Legacy Application Server
NET-024	MEDIUM	Excessive Privilege Assignment — Standard Support Accounts Present in Domain Admins Group
NET-025	MEDIUM	Weak Password Policy Permits Short, Non-Complex Domain Passwords
NET-026	MEDIUM	Insecure Administrative Pathway — Helpdesk Staff Granted Direct RDP to Domain Controllers
NET-033	LOW	Excessive Domain Information Disclosure via Unauthenticated LDAP Enumeration
NET-034	LOW	SYSVOL-Related Sensitive Configuration Reference in Legacy Logon Script
NET-040	INFORMATIONAL	Recommendation — Adopt Privileged Access Workstations for Tier-0 Administrative Activity

14 NETWORK DEVICE ASSESSMENT

Firewalls, switches, the wireless LAN controller, and the network management platform were reviewed for management protocol security, SNMP configuration, administrator access, ACL scoping, management-plane segmentation, configuration backup handling, logging, firmware lifecycle, and default settings.

Area	Observation	Findings
Management Protocols	HTTPS and SSH are used for device management; Telnet was not observed on any in-scope device.	
SNMP	SNMPv1/v2c remains enabled alongside SNMPv3 on core and distribution switches, using guessable community strings.	NET-009, NET-029
Administrator Access	Default vendor administrative credentials were not rotated on the core switch and internal firewall.	NET-004
ACLs	Management-plane ACLs are missing on the core switch/internal firewall and overly broad on distribution switches.	NET-004, NET-032
Management-Plane Segmentation	Management interfaces are reachable from the User VLAN and Corporate Wireless SSID due to missing/overly broad ACLs.	NET-004, NET-011
Configuration Backups	Automated configuration backups are stored unencrypted on a broadly-accessible general IT share.	NET-031
Logging	Device-level logging is forwarded to the centralized SIEM for the core switch and firewalls; consistent with the positive logging observation elsewhere in this report.	NET-038
Firmware Lifecycle	The wireless LAN controller is running firmware two release trains behind current with no formal upgrade cadence identified.	NET-030
Default Settings	Vendor default credentials were identified on two of the highest-criticality devices in scope (core switch, internal firewall).	NET-004

Network Device Findings

Finding ID	Severity	Title
NET-004	CRITICAL	Exposed Management Plane Enables Administrative Access to Core Network Devices from User VLAN
NET-009	HIGH	SNMP Community String Configuration Exposes Network Device Information
NET-029	LOW	Insecure SNMP Configuration — SNMPv2c Enabled Alongside SNMPv3 on Distribution Switches
NET-030	LOW	Outdated Device Firmware on Wireless LAN Controller
NET-031	LOW	Configuration Backup Exposure — Unencrypted Device Configurations Stored on Shared Drive
NET-032	LOW	Weak Network-Device ACL Permits Broader Source Range Than Required for SSH Management

Finding ID	Severity	Title
NET-043	INFORMATIONAL	Informational — Management VLAN Naming Convention Inconsistent Across Network Documentation
NET-046	INFORMATIONAL	Recommendation — Establish Formal Firewall Rule Review and Recertification Process

15 WIRELESS ASSESSMENT

Three wireless SSIDs were assessed: Corporate, Guest, and Management, covering authentication model, encryption, client isolation, VLAN mapping, and management-plane access.

SSID	Broadcast Name	Authentication	Mapped Zone	Client Population
Corporate SSID	NSF-CORP	WPA2-Enterprise (802.1X / PEAP-MSCHAPv2)	Wireless — Corporate SSID (10.50.10.0/24)	Domain-joined and BYOD corporate endpoints
Guest SSID	NSF-GUEST	WPA2-Personal (PSK, captive portal)	Wireless — Guest SSID (10.50.20.0/24)	Visitors and unmanaged devices
Management SSID	NSF-WLAN-MGMT	WPA2-Personal (PSK)	Wireless — Management SSID (10.50.30.0/24)	AP-to-WLC control plane and wireless infrastructure management

Wireless Review Notes

Area	Observation	Findings
Authentication Model	Corporate SSID uses 802.1X/PEAP-MSCHAPv2 as its primary method but retains a legacy shared-PSK fallback for IoT-style devices that has not been rotated in over two years.	NET-027
Encryption	WPA2 is used consistently across all three SSIDs; WPA3 migration has not yet begun for client devices that support it.	
Guest Isolation	Guest-to-corporate and guest-to-management isolation is correctly enforced; a narrow exception intended for a print-release kiosk was found to be broader than intended.	NET-028
VLAN Mapping	Each SSID maps to a dedicated VLAN as designed; the Management SSID (WLC control plane) is correctly isolated from client SSIDs.	
Client Isolation	Client-to-client isolation is enforced within the Guest SSID; no peer-to-peer traffic was observed between guest clients during testing.	
Management Access	An overly broad firewall source object allows Corporate SSID clients (not just the WLC uplink) to reach Management VLAN interfaces.	NET-011
Rogue Device Considerations	Wireless intrusion detection is enabled on NS-WLC01 and flagged no unauthorized access points during the assessment window (fictional/illustrative).	

Wireless Findings

Finding ID	Severity	Title
NET-011	HIGH	Insecure Firewall Rule Permits Management-Plane Access From Corporate Wireless Segment
NET-027	MEDIUM	Weak Corporate Wireless Configuration — Shared PSK Fallback Available Alongside 802.1X
NET-028	LOW	Guest Wireless Network Isolation Weakness Permits Limited Reachability to Printer VLAN

16 CLOUD / HYBRID ASSESSMENT

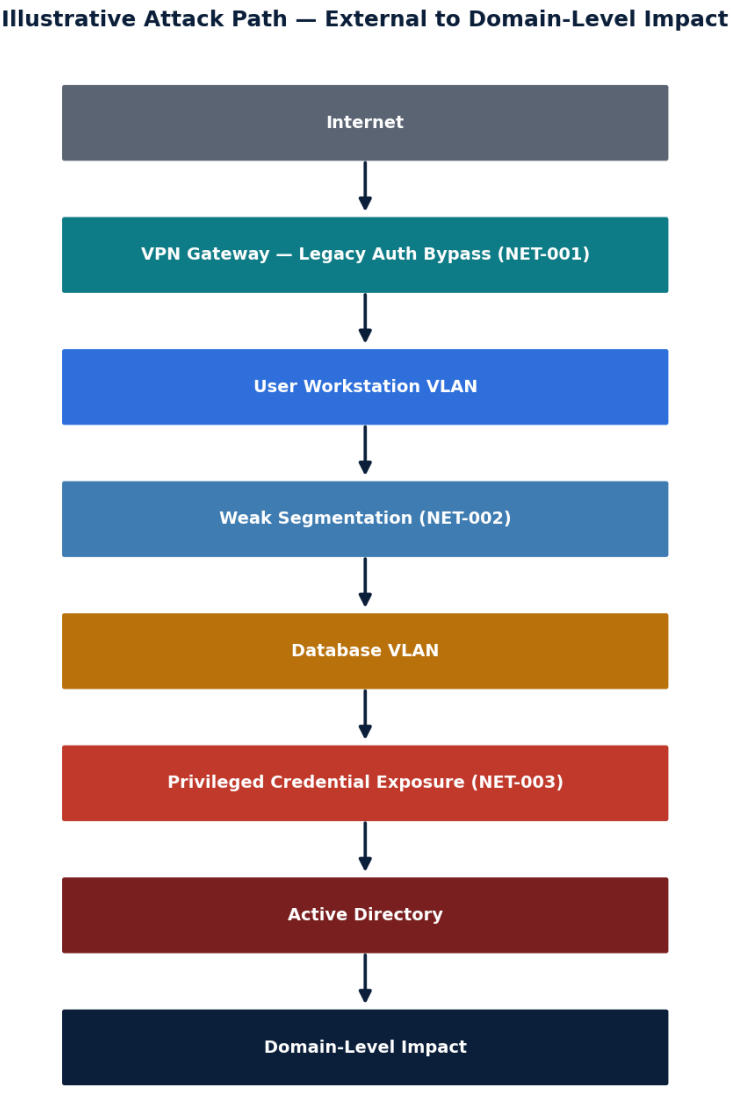
NorthStar's fictional hybrid environment connects the on-premises network to a fictional cloud tenant via a site-to-site VPN and a hybrid identity synchronization server. This assessment reviewed cryptographic configuration, network path scoping, and administrative access to the cloud management interface.

Finding ID	Severity	Title
NET-035	LOW	Overly Permissive VPN Trust Allows Split-Tunnel Access to Sensitive On-Prem Resources
NET-036	LOW	Weak Hybrid Segmentation Between On-Prem Identity Sync Server and Cloud Management Path

17 ATTACK PATH ANALYSIS

The following fictional, non-destructive attack chains illustrate how individually-rated findings combine into realistic compromise paths — the central value of a manual penetration test over automated vulnerability scanning.

Attack Path 1 — External to Domain-Level Impact

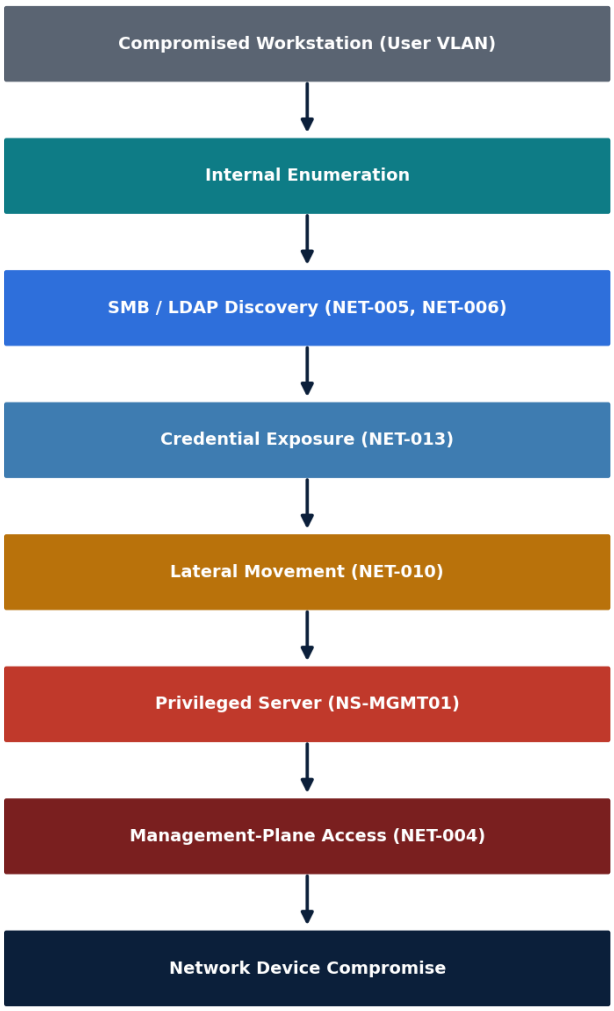


Illustrative, non-destructive fictional attack chain. ILLUSTRATIVE / SYNTHETIC EVIDENCE.

Starting from the internet, an attacker exploits the legacy VPN authentication bypass (NET-001) to obtain network access using only a single valid credential. From the User Workstation VLAN, the insufficient segmentation gap (NET-002) provides direct reachability to the Database VLAN. Independently, the SYSVOL credential exposure (NET-003) provides a Domain Admin-equivalent credential to any authenticated user, completing a path to full domain-level impact.

Attack Path 2 — Assumed-Breach Lateral Movement

Illustrative Attack Path — Assumed-Breach Lateral Movement

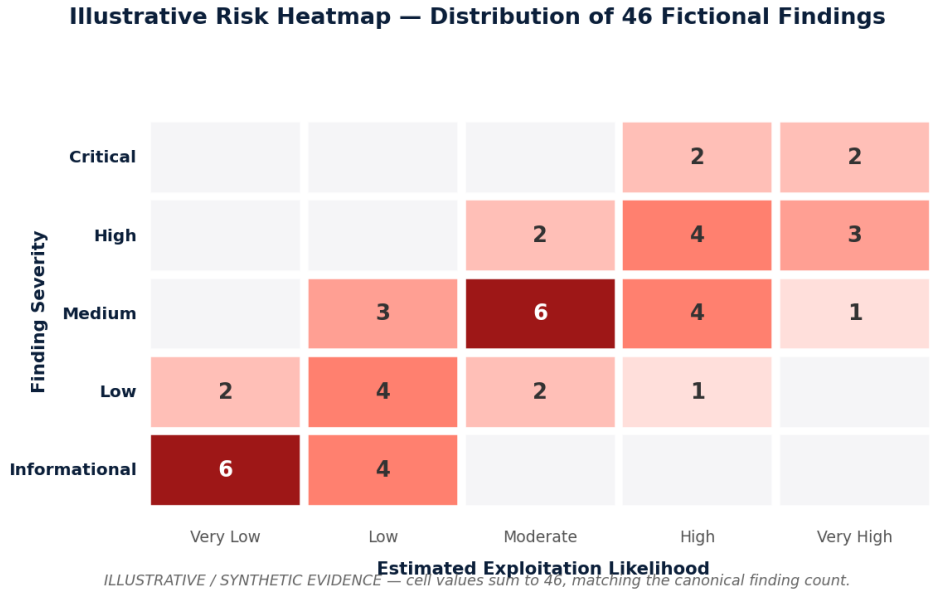


Illustrative, non-destructive fictional attack chain. ILLUSTRATIVE / SYNTHETIC EVIDENCE.

Starting from a compromised User VLAN workstation (the internal assumed-breach starting point), internal enumeration discovers SMB and LDAP configuration weaknesses (NET-005, NET-006) that expose credential material (NET-013). The recovered credential is used for lateral movement to a privileged administrative server (NET-010), from which the exposed management plane (NET-004) provides a path to network device compromise.

18 FINDINGS SUMMARY

This fictional assessment identified 46 illustrative findings across NorthStar's external perimeter, internal network, Active Directory, network devices, and wireless infrastructure, summarized below: 4 Critical, 9 High, 14 Medium, 9 Low, and 10 Informational. Full detail for every finding, including safe proof-of-concept evidence, is provided in Sections 19-23.



Illustrative risk heatmap — likelihood versus impact — ILLUSTRATIVE / SYNTHETIC EVIDENCE.

Findings at a Glance

Finding ID	Severity	Title	Status
NET-001	CRITICAL	External VPN Authentication Can Be Bypassed Through Legacy Authentication Workflow	Remediation In Progress
NET-002	CRITICAL	Insufficient Internal Network Segmentation Enables Unauthenticated Reachability from User VLAN to Database VLAN	Remediation In Progress
NET-003	CRITICAL	Privileged Active Directory Service Account Credential Exposed Through Insecure Group Policy Preferences Configuration	Remediation In Progress
NET-004	CRITICAL	Exposed Management Plane Enables Administrative Access to Core Network Devices from User VLAN	Remediation In Progress
NET-005	HIGH	SMB Signing Not Enforced on Critical Internal Windows Servers	Remediation Planned
NET-006	HIGH	Insecure LDAP Configuration Permits Credential Exposure via Unsigned, Unencrypted Bind	Remediation Planned
NET-007	HIGH	Excessive Administrative Access Across User Network Segment via Helpdesk Group Policy	Remediation Planned

Finding ID	Severity	Title	Status
NET-008	HIGH	Weak VPN Security Configuration Permits Legacy Cryptographic Negotiation	Remediation Planned
NET-009	HIGH	SNMP Community String Configuration Exposes Network Device Information	Remediation Planned
NET-010	HIGH	RDP Accessible Across Improperly Segmented Network Boundaries	Remediation Planned
NET-011	HIGH	Insecure Firewall Rule Permits Management-Plane Access From Corporate Wireless Segment	Remediation Planned
NET-012	HIGH	Sensitive Backup Repository Reachable From User VLAN Without Authentication Segmentation	Remediation Planned
NET-013	HIGH	Weak Service Account Security Enables Lateral Movement via Kerberoasting	Remediation Planned
NET-014	MEDIUM	Outdated TLS Configuration on External Remote Access Portal	Remediation Planned
NET-015	MEDIUM	Certificate Configuration Issue on External VPN Gateway	Remediation Planned
NET-016	MEDIUM	DNS Configuration Weakness Permits Zone Transfer from External DNS Server	Remediation Planned
NET-017	MEDIUM	Exposed Service With Unnecessary Functionality on External Load Balancer	Remediation Planned
NET-018	MEDIUM	Information Disclosure Through Verbose Error Messages on Public Web Application Gateway	Remediation Planned
NET-019	MEDIUM	Legacy/Insecure Protocol Exposure — SMBv1 Still Enabled on Internal File Server	Remediation Planned
NET-020	MEDIUM	Unnecessary East-West Connectivity Between Application VLAN and Database VLAN Beyond Required Ports	Remediation Planned
NET-021	MEDIUM	Insecure Monitoring Interface Exposes Sensitive Telemetry Without Authentication	Remediation Planned
NET-022	MEDIUM	Weak Internal TLS Configuration on Internal API Server	Remediation Planned
NET-023	MEDIUM	Kerberos Configuration Weakness — Unconstrained Delegation Enabled on Legacy Application Server	Remediation Planned
NET-024	MEDIUM	Excessive Privilege Assignment — Standard Support Accounts Present in Domain Admins Group	Remediation Planned
NET-025	MEDIUM	Weak Password Policy Permits Short, Non-Complex Domain Passwords	Remediation Planned
NET-026	MEDIUM	Insecure Administrative Pathway — Helpdesk Staff Granted Direct RDP to Domain Controllers	Remediation Planned
NET-027	MEDIUM	Weak Corporate Wireless Configuration — Shared PSK Fallback Available Alongside 802.1X	Remediation Planned
NET-028	LOW	Guest Wireless Network Isolation Weakness Permits Limited Reachability to Printer VLAN	Remediation Planned
NET-029	LOW	Insecure SNMP Configuration — SNMPv2c Enabled Alongside SNMPv3 on Distribution Switches	Remediation Planned
NET-030	LOW	Outdated Device Firmware on Wireless LAN Controller	Remediation Planned

Finding ID	Severity	Title	Status
NET-031	LOW	Configuration Backup Exposure — Unencrypted Device Configurations Stored on Shared Drive	Remediation Planned
NET-032	LOW	Weak Network-Device ACL Permits Broader Source Range Than Required for SSH Management	Remediation Planned
NET-033	LOW	Excessive Domain Information Disclosure via Unauthenticated LDAP Enumeration	Remediation Planned
NET-034	LOW	SYSVOL-Related Sensitive Configuration Reference in Legacy Logon Script	Remediation Planned
NET-035	LOW	Overly Permissive VPN Trust Allows Split-Tunnel Access to Sensitive On-Prem Resources	Remediation Planned
NET-036	LOW	Weak Hybrid Segmentation Between On-Prem Identity Sync Server and Cloud Management Path	Remediation Planned
NET-037	INFORMATIONAL	Positive Observation — Next-Generation Firewall Enforces Application-Aware Policy at External Perimeter	Observation Only
NET-038	INFORMATIONAL	Positive Observation — Centralized Logging and SIEM Collection Implemented Across Core Infrastructure	Observation Only
NET-039	INFORMATIONAL	Positive Observation — Multi-Factor Authentication Enforced on Primary VPN Login Path	Observation Only
NET-040	INFORMATIONAL	Recommendation — Adopt Privileged Access Workstations for Tier-0 Administrative Activity	Observation Only
NET-041	INFORMATIONAL	Recommendation — Formalize Network Segmentation Review Cadence	Observation Only
NET-042	INFORMATIONAL	Recommendation — Expand SIEM Detection Coverage for Lateral Movement Techniques	Observation Only
NET-043	INFORMATIONAL	Informational — Management VLAN Naming Convention Inconsistent Across Network Documentation	Observation Only
NET-044	INFORMATIONAL	Informational — Legacy DNS Records Identified for Decommissioned Hosts	Observation Only
NET-045	INFORMATIONAL	Recommendation — Implement Network Access Control (802.1X) on Wired User Ports	Observation Only
NET-046	INFORMATIONAL	Recommendation — Establish Formal Firewall Rule Review and Recertification Process	Observation Only

19 CRITICAL FINDINGS

The following 4 fictional Critical-severity findings represent this assessment's highest-priority illustrative results, each reproducible with a controlled, non-destructive fictional Proof of Concept and each carrying a direct path toward fictional account, credential, or network compromise.

NET-001 — External VPN Authentication Can Be Bypassed Through Legacy Authentication Workflow	**CRITICAL**
CVSS-Style Score	9.4 (Critical) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N — Illustrative vector only
CWE	CWE-287 — Improper Authentication
Affected Asset(s)	NS-VPNGW01 (10.40.0.10)
Affected Network Segment	External Perimeter / DMZ
Affected Service / Port	TCP/10443 — HTTPS (legacy VPN login endpoint)
Affected Technology	SSL VPN Gateway — legacy authentication module
Description	NS-VPNGW01 exposes NorthStar's primary SSL VPN client portal at vpn.northstar-example.com, which correctly enforces mandatory multi-factor authentication (push approval) for all interactive logins. A fictional legacy login endpoint (/remote/legacy-login, historically retained for a decommissioned thin-client VPN agent) remains reachable on TCP/10443 and completes full session establishment using username and password alone, with no MFA challenge issued at any point in the flow.
Business Context	The VPN gateway is NorthStar's primary remote-access control for employees and third-party administrators. MFA on the primary login path is the control the organization relies on to defeat credential-stuffing and password-spray attacks against internet-facing authentication.
Technical Impact	Any attacker in possession of a single valid domain credential (via phishing, credential stuffing against a breached-password list, or password spray) can establish a full VPN session and reach the internal network without ever satisfying the second authentication factor.
Business Impact	Full bypass of the organization's primary internet-facing control point exposes the internal network — including the User, Server, Application, and Database VLANs reachable post-VPN — to any actor holding one valid password, materially undermining NorthStar's regulatory posture as a financial services provider.
Attack Preconditions	A single valid NorthStar domain username and password, obtainable via credential stuffing, phishing, or password spray against the external attack surface.
Attack Path	Internet → NS-VPNGW01 legacy login endpoint (TCP/10443) → single-factor authentication accepted → full-tunnel VPN session established → direct reachability into User VLAN and, per NET-002, onward into Database VLAN.
Safe Proof of Concept (Summary)	*A fictional test session authenticated to the legacy endpoint using a synthetic test credential and received a valid VPN session token with no MFA challenge presented at any step. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-001, EV-NET-002

Expected Behavior	Every authentication path exposed by the VPN gateway — including legacy or deprecated endpoints — should enforce the same mandatory MFA policy applied to the primary login flow.
Observed (Fictional) Behavior	The legacy login endpoint completed session establishment using password-only authentication, with no MFA prompt issued and no policy flag blocking the deprecated code path.
Root Cause	The legacy authentication module was retained for backward compatibility with a decommissioned VPN client and was never brought under the MFA enforcement policy applied to the primary login flow, nor was it disabled when the legacy client was retired.
Security Risk	Complete bypass of the organization's primary internet-facing authentication control using only a single-factor credential, with a direct path into internal network segments.
Recommendation	Disable the legacy VPN authentication endpoint entirely; if backward compatibility is still required, bring it under the same mandatory MFA enforcement policy as the primary login flow before re-enabling it.
Remediation Guidance	1) Confirm no active client population depends on the legacy endpoint via connection logs; 2) disable the /remote/legacy-login code path at the VPN gateway configuration; 3) if retained, integrate it with the existing MFA provider and enforce policy parity with the primary login flow; 4) add a configuration-drift alert so future changes to authentication endpoints require security sign-off.
Management Response	*NorthStar engineering (fictional) has accepted this finding and will disable the legacy authentication endpoint ahead of the next scheduled maintenance window.*
Owner / Priority / Target / Status	Network Security Engineering Lead (Fictional Role) | Immediate — 0-30 Days | 10 October 2026 | Remediation In Progress
Retest Recommendation	*Retest by confirming the legacy endpoint returns a connection failure or, if retained, enforces the same MFA challenge as the primary login flow.*

CATEGORY	RELATED FINDINGS	STATUS
External Network	NET-002, NET-008, NET-039	**Remediation In Progress**

FULL EVIDENCE PANEL — ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE

Legacy VPN Authentication Bypass — Session Establishment (Fictional / Synthetic)

```
$ curl -sk https://vpn.northstar-example.com:10443/remote/legacy-login \
    -d 'username=test.fictional.user&password=FICTIONAL-PW-0091'

HTTP/1.1 200 OK
X-Session-Token: NSVPN-FICTIONAL-7f3ae9c1d0b2
X-Auth-Factors-Satisfied: password
X-MFA-Challenge-Issued: false

# Result: full-tunnel VPN session established — NO MFA CHALLENGE ISSUED
```

TECHNICAL EVIDENCE SUMMARY

Attack Preconditions	A single valid NorthStar domain credential and network reachability to NS-VPNGW01 on TCP/10443.
Observed Result	The legacy login endpoint issued a valid session token after password-only authentication, with no MFA factor requested or verified.
Security Impact	Complete bypass of the organization's mandatory MFA control for remote access, reducing authentication strength to a single factor for any attacker using this endpoint.
Business Impact	Unauthorized network access using only a stolen or guessed password, with downstream exposure to internal VLANs described in NET-002.
Evidence Collected	EV-NET-001 (legacy endpoint authentication capture), EV-NET-002 (VPN gateway configuration excerpt).

Retest Validation	Repeat the authentication attempt against the legacy endpoint post-remediation and confirm the connection is refused or an MFA challenge is issued before session establishment.

NET-002 — Insufficient Internal Network Segmentation Enables Unauthenticated Reachability from User VLAN to Database VLAN	**CRITICAL**
CVSS-Style Score	9.1 (Critical) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H — Illustrative vector only
CWE	CWE-284 — Improper Access Control
Affected Asset(s)	NS-FWINT01 (172.20.10.10), NS-SQL01 (10.40.40.10)
Affected Network Segment	User Workstation VLAN → Database VLAN
Affected Service / Port	TCP/1433 — MSSQL
Affected Technology	Internal segmentation firewall — inter-VLAN policy
Description	NS-FWINT01, the internal segmentation firewall responsible for enforcing east-west policy between VLANs, contains an overly broad rule (permit any-any between the 10.40.0.0/16 supernet objects used for User and Database VLAN grouping) that was introduced during a fictional migration project and never narrowed. As a result, hosts on the User Workstation VLAN can establish direct TCP/1433 connections to NS-SQL01, the primary transactional database, with no intermediate application tier or jump host in the path.
Business Context	The Database VLAN is intended to be reachable only from the Application VLAN, over the specific ports the payments application requires. Direct user-to-database reachability defeats the layered defense NorthStar's architecture is designed around and was a specific in-scope segmentation-testing objective for this assessment.
Technical Impact	A compromised or malicious workstation on the User VLAN can connect directly to the primary transactional database, bypassing every control enforced at the application tier, including input validation, authorization checks, and query-level audit logging.
Business Impact	Combined with any credential-harvesting technique (see NET-013), this exposure creates a direct path from a single compromised end-user device to the core financial database, with no requirement to compromise the application or API tier first.
Attack Preconditions	Network access to the User Workstation VLAN (e.g., a compromised end-user device or a device connected to an unauthenticated wired port) and any set of valid or crackable database credentials.
Attack Path	Compromised workstation (User VLAN) → direct TCP/1433 connection to NS-SQL01 (Database VLAN) → authentication using credentials obtained via NET-013 or NET-025 → direct query access to the primary transactional database, bypassing the application tier entirely.
Safe Proof of Concept (Summary)	*From a fictional test host on the User VLAN, a direct TCP/1433 connection to NS-SQL01 was established and a database login banner was returned, confirming unrestricted reachability with no intermediate control point. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-003, EV-NET-004
Expected Behavior	The Database VLAN should be reachable only from the Application VLAN on the specific ports required by the payments application; direct User VLAN-to-Database VLAN traffic should be denied by default.

Observed (Fictional) Behavior	An any-any policy object on NS-FWINT01 permitted the User VLAN full TCP/1433 reachability to the Database VLAN with no source or destination restriction.
Root Cause	A temporary broad rule created during a fictional infrastructure migration was never replaced with the intended least-privilege segmentation policy, and no periodic firewall rule review process caught the oversight.
Security Risk	A single compromised user endpoint can reach the core financial database directly, collapsing the organization's network-layer defense-in-depth model into a single control point.
Recommendation	Replace the broad any-any object with an explicit rule permitting only the Application VLAN to reach the Database VLAN on TCP/1433, and deny all other User VLAN-to-Database VLAN traffic by default.
Remediation Guidance	1) Identify and remove the overly broad supernet-based rule on NS-FWINT01; 2) implement an explicit allow rule scoped to the Application VLAN subnet and NS-SQL01/NS-SQL02 destination objects on TCP/1433 only; 3) add an explicit deny-and-log rule for User VLAN-to-Database VLAN traffic; 4) validate against the full segmentation matrix in Appendix E; 5) schedule quarterly firewall rule recertification (see NET-046).
Management Response	*NorthStar engineering (fictional) has accepted this finding as the top segmentation-remediation priority from this assessment and will implement the corrected policy ahead of the next change window.*
Owner / Priority / Target / Status	Network Security Engineering Lead (Fictional Role) | Immediate — 0-30 Days | 10 October 2026 | Remediation In Progress
Retest Recommendation	*Retest by confirming TCP/1433 connections from a User VLAN test host to NS-SQL01 and NS-SQL02 are denied, and that Application VLAN reachability remains intact.*

CATEGORY	RELATED FINDINGS	STATUS
Internal Network	NET-001, NET-010, NET-013, NET-020	**Remediation In Progress**

FULL EVIDENCE PANEL — ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE

Direct User VLAN → Database VLAN Reachability (Fictional / Synthetic)

```
$ nmap -Pn -p 1433 10.40.40.10
Starting Nmap ( fictional sample scan )
Nmap scan report for ns-sql01.northstar-example.com (10.40.40.10)
PORT     STATE SERVICE
1433/tcp open  ms-sql-s

$ python3 mssql_banner_check.py --host 10.40.40.10 --port 1433
[*] TDS pre-login response received from 10.40.40.10:1433
[*] Source host: 10.40.10.47 (User Workstation VLAN)
[*] Result: DIRECT REACHABILITY CONFIRMED — no intermediate control point observed
```

TECHNICAL EVIDENCE SUMMARY

Attack Preconditions	Network access to any host on the User Workstation VLAN; no VPN, jump host, or application-tier credential required to reach the database service port.
Observed Result	TCP/1433 connections from a User VLAN test host to NS-SQL01 completed a full TDS pre-login handshake with no firewall interruption.
Security Impact	The Database VLAN's isolation boundary is effectively absent for the User VLAN source zone, collapsing the intended multi-tier trust model.
Business Impact	A compromised end-user device becomes a direct pivot point to the core financial database, sharply shortening the fictional attacker's path to sensitive data.
Evidence Collected	EV-NET-003 (segmentation port-reachability scan), EV-NET-004 (NS-FWINT01 policy configuration excerpt).

Retest Validation	Repeat the reachability test post-remediation from the same User VLAN source and confirm the connection is blocked while Application VLAN reachability is preserved.

NET-003 — Privileged Active Directory Service Account Credential Exposed Through Insecure Group Policy Preferences Configuration	**CRITICAL**
CVSS-Style Score	9.8 (Critical) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H — Illustrative vector only
CWE	CWE-522 — Insufficiently Protected Credentials
Affected Asset(s)	NS-DC01 (10.40.50.10), NS-DC02 (10.40.50.11)
Affected Network Segment	Identity / AD VLAN (SYSVOL, reachable from all domain-joined zones)
Affected Service / Port	TCP/445 — SMB (SYSVOL share)
Affected Technology	Active Directory Group Policy Preferences
Description	A legacy Group Policy Object retained in the NORTHSTAR domain's SYSVOL share contains a Group Policy Preferences 'Scheduled Task' item created before Microsoft's 2014 deprecation of client-side credential storage in GPP. The encrypted cpassword value stored in the policy's XML file uses the well-documented static AES key Microsoft published for GPP, allowing any authenticated domain user to decrypt it and recover the plaintext credential for svc-backupsync, a service account holding Domain Admins-equivalent rights for the fictional backup pipeline.
Business Context	svc-backupsync authenticates the enterprise backup pipeline against domain controllers, file servers, and the database tier, and was provisioned with Domain Admin-equivalent privileges to simplify backup-agent deployment several years ago. The account's privilege level was never subsequently reduced.
Technical Impact	Any authenticated domain user — including a standard end-user account with no special privileges — can read SYSVOL, locate the legacy GPP XML file, decrypt the cpassword using the published static key, and obtain Domain Admin-equivalent credentials.
Business Impact	This finding alone constitutes a complete domain-compromise path from any standard user account, with no additional technique required — the most severe finding identified during this fictional assessment.
Attack Preconditions	Any valid, low-privileged domain user account with standard SYSVOL read access (the default for all domain members).
Attack Path	Authenticated low-privileged domain user → SYSVOL share read access → locate legacy Scheduled Tasks GPP XML → decrypt cpassword using published static AES key → authenticate as svc-backupsync → Domain Admin-equivalent access to NS-DC01, NS-DC02, and every domain-joined system in scope.
Safe Proof of Concept (Summary)	*A fictional test account with only standard domain-user rights located and decrypted a synthetic cpassword value from the legacy GPP XML file stored in SYSVOL, recovering credentials for a privileged fictional service account. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-005, EV-NET-006
Expected Behavior	No credential material should be stored in Group Policy Preferences; privileged service accounts should never be recoverable by a standard domain user, and service accounts used for automation should carry least-privilege delegated rights rather than Domain Admin-equivalent membership.

Observed (Fictional) Behavior	A legacy GPP XML file containing an encrypted cpassword for a Domain Admin-equivalent service account remained present and readable in SYSVOL by any domain user.
Root Cause	The Scheduled Task GPO predates the organization's adoption of the current credential-management standard and was never remediated following Microsoft's 2014 GPP security advisory; no SYSVOL audit process exists to catch legacy credential artifacts.
Security Risk	A single low-privileged domain account is sufficient to obtain Domain Admin-equivalent access to the entire NORTHSTAR Active Directory forest.
Recommendation	Remove the legacy GPP XML file from SYSVOL, rotate the svc-backupsync credential immediately, and re-provision the account with least-privilege delegated rights scoped only to the backup pipeline's actual requirements.
Remediation Guidance	1) Immediately rotate the svc-backupsync password; 2) delete the legacy Scheduled Tasks GPO and confirm no other GPP Groups/Drives/Services XML files contain cpassword values (audit all of SYSVOL); 3) re-provision svc-backupsync using a group Managed Service Account (gMSA) with delegated rights scoped to backup targets only, removing Domain Admins membership; 4) enable SYSVOL access auditing; 5) add a recurring SYSVOL credential-artifact scan to the security tooling baseline.
Management Response	*NorthStar engineering (fictional) has treated this as a sev-1 finding, rotated the affected credential under emergency change control, and will complete the least-privilege re-provisioning within the immediate remediation window.*
Owner / Priority / Target / Status	Active Directory Engineering Lead (Fictional Role) | Immediate — 0-30 Days | 10 October 2026 | Remediation In Progress
Retest Recommendation	*Retest by confirming SYSVOL no longer contains any GPP file with a cpassword attribute and that svc-backupsync no longer holds Domain Admins-equivalent membership.*

CATEGORY	RELATED FINDINGS	STATUS
Active Directory	NET-004, NET-013, NET-024, NET-034	**Remediation In Progress**

FULL EVIDENCE PANEL — ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE

```
SYSVOL GPP Credential Recovery (Fictional Domain Account) (Fictional / Synthetic)
PS C:\> Get-ChildItem \\northstar-example.com\SYSVOL -Recurse -Filter *.xml | Select-String cpassword

\\...\Policies\{FICTIONAL-GUID}\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml:
  <Task ... ><Properties runAs="NORTHSTAR\svc-backupsync"
    cpassword="FICTIONAL+ENCRYPTED+GPPVALUE==" .../>

PS C:\> Decrypt-GPPPassword -EncryptedValue 'FICTIONAL+ENCRYPTED+GPPVALUE=='
[+] Decrypted (fictional): NSF-Backup-2019!Rotate
[+] Account: NORTHSTAR\svc-backupsync
[+] Group Membership (fictional): Domain Admins
```

TECHNICAL EVIDENCE SUMMARY

Attack Preconditions	Any authenticated domain user account with default SYSVOL read access.
Observed Result	A legacy GPP XML file containing an encrypted cpassword for a Domain Admins-equivalent service account was present in SYSVOL and successfully decrypted using the published static key.
Security Impact	Complete, unauthenticated-relative-to-privilege compromise of the Active Directory forest from any standard domain account.
Business Impact	This finding represents the shortest and most severe compromise path identified in the assessment — full domain compromise with no additional technique required.
Evidence Collected	EV-NET-005 (SYSVOL GPP XML extraction), EV-NET-006 (decrypted credential validation, non-destructive bind test).

Retest Validation	Confirm the legacy GPO and its GPP XML file are removed from SYSVOL, the credential has been rotated, and the account no longer holds privileged group membership.

NET-004 — Exposed Management Plane Enables Administrative Access to Core Network Devices from User VLAN	**CRITICAL**
CVSS-Style Score	9.6 (Critical) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H — Illustrative vector only
CWE	CWE-284 — Improper Access Control
Affected Asset(s)	NS-COREW01 (172.20.10.1), NS-FWINT01 (172.20.10.10)
Affected Network Segment	User Workstation VLAN → Management VLAN
Affected Service / Port	TCP/443 — HTTPS (device management console)
Affected Technology	Core switch and internal firewall management plane
Description	The HTTPS management interfaces of NS-COREW01 (core switch) and NS-FWINT01 (internal segmentation firewall) are reachable directly from the User Workstation VLAN due to a missing management-plane ACL, rather than being restricted to the Management VLAN as NorthStar's network standard requires. Both interfaces additionally accept a fictional vendor-default administrative credential that was never rotated during initial deployment.
Business Context	The Management VLAN exists specifically to isolate administrative interfaces for core network infrastructure from general user traffic; its purpose is defeated when those interfaces are reachable — and authenticable — directly from the User VLAN.
Technical Impact	An attacker with User VLAN access can reach the administrative web console of the organization's core switch and internal firewall and authenticate using an unrotated default credential, gaining full configuration control over core network infrastructure.
Business Impact	Compromise of the core switch and internal segmentation firewall gives an attacker the ability to alter routing, disable or rewrite every segmentation control validated elsewhere in this report (including the remediation for NET-002), and intercept or redirect traffic across the enterprise network.
Attack Preconditions	Network access to the User Workstation VLAN and network-layer reachability to the Management VLAN management interfaces (present due to the missing ACL).
Attack Path	Compromised workstation (User VLAN) → direct HTTPS reachability to NS-COREW01 and NS-FWINT01 management consoles (missing management-plane ACL) → authentication using unrotated fictional vendor-default credential → full administrative control of core switching and segmentation firewall infrastructure.
Safe Proof of Concept (Summary)	*A fictional test session reached the core switch's HTTPS management console directly from a User VLAN test host and authenticated using a synthetic default credential, confirming both the missing ACL and the credential weakness. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-007, EV-NET-008
Expected Behavior	Management-plane interfaces for core network infrastructure should be reachable only from the Management VLAN, and all vendor-default credentials should be rotated during deployment as required by NorthStar's build standard.

Observed (Fictional) Behavior	Both devices' management interfaces were reachable from the User VLAN with no intervening ACL, and both accepted a fictional unrotated vendor-default administrative credential.
Root Cause	The management-plane ACL was omitted during the original core-switch and firewall deployment, and the deployment checklist step requiring default-credential rotation was not completed or verified.
Security Risk	Full administrative compromise of the organization's core network fabric is achievable from any User VLAN foothold with no privileged credential required beyond an unrotated default.
Recommendation	Restrict management-interface reachability to the Management VLAN via ACL on both devices and rotate all default administrative credentials immediately, replacing them with unique, centrally-managed credentials.
Remediation Guidance	1) Rotate the default administrative credential on NS-COREW01 and NS-FWINT01 immediately; 2) implement a management-plane ACL permitting HTTPS/SSH management access only from the Management VLAN and designated jump hosts; 3) audit all remaining network devices in Appendix D for the same two conditions; 4) integrate device administrative accounts with centralized authentication (TACACS+/RADIUS) rather than local accounts; 5) add default-credential verification to the standard deployment checklist.
Management Response	*NorthStar engineering (fictional) has rotated the affected credentials under emergency change control and will implement the corrected management-plane ACL ahead of the next change window.*
Owner / Priority / Target / Status	Network Operations Lead (Fictional Role) | Immediate — 0-30 Days | 10 October 2026 | Remediation In Progress
Retest Recommendation	*Retest by confirming management-interface reachability from the User VLAN is blocked and that default credentials no longer authenticate on either device.*

CATEGORY	RELATED FINDINGS	STATUS
Network Devices	NET-002, NET-009, NET-011, NET-032	**Remediation In Progress**

FULL EVIDENCE PANEL — ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE

Core Switch Management-Plane Reachability and Default Credential (Fictional / Synthetic)

```
$ curl -sk -I https://172.20.10.1/ --interface eth0  # sourced from User VLAN test host
HTTP/1.1 200 OK
Server: FictionalNOS-WebUI/4.2

$ curl -sk https://172.20.10.1/api/v1/login -d 'user=admin&pass=FICTIONAL-DEFAULT-PW'
HTTP/1.1 200 OK
{"session":"fictional-session-8a71c","role":"administrator"}

# Result: administrative session established from User VLAN using unrotated default credential
```

TECHNICAL EVIDENCE SUMMARY

Attack Preconditions	Network access to the User Workstation VLAN; no prior credential compromise required beyond the unrotated fictional vendor default.
Observed Result	Both NS-COREW01 and NS-FWINT01 management consoles were reachable from the User VLAN and authenticated successfully with the default credential.
Security Impact	Full administrative takeover of core switching and segmentation-firewall infrastructure is achievable from a standard User VLAN foothold.
Business Impact	An attacker holding this level of access could disable or rewrite every network segmentation control described elsewhere in this report.
Evidence Collected	EV-NET-007 (management-plane reachability scan), EV-NET-008 (default-credential authentication test, non-destructive).

Retest Validation	Confirm management-interface reachability from the User VLAN is blocked and both devices reject the previous default credential.

20 HIGH FINDINGS

The following 9 fictional High-severity findings should be prioritized immediately after the Critical findings in Section 19.

NET-005 — SMB Signing Not Enforced on Critical Internal Windows Servers	HIGH
CVSS-Style Score	8.1 (High) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N — Illustrative vector only
CWE	CWE-300 — Channel Accessible by Non-Endpoint (Man-in-the-Middle)
Affected Asset(s)	NS-FILE01 (10.40.20.10), NS-APPSRV01 (10.40.20.11), NS-MGMT01 (10.40.20.12)
Affected Network Segment	Server VLAN
Affected Service / Port	TCP/445 — SMB
Affected Technology	Windows Server SMB configuration
Description	NS-FILE01, NS-APPSRV01, and NS-MGMT01 do not require SMB signing, leaving them susceptible to NTLM relay attacks in which authentication traffic captured or coerced from a victim host is relayed to these servers to obtain an authenticated session without knowledge of the underlying credential.
Business Context	NS-MGMT01 in particular is used as an administrative jump server, meaning a successful relay could yield a session with elevated administrative context.
Technical Impact	An attacker positioned on the Server VLAN (or able to coerce authentication from a victim, e.g., via NET-006-style protocol abuse) can relay captured NTLM authentication to these servers and obtain an authenticated SMB session.
Business Impact	NTLM relay against NS-MGMT01 could yield administrative-equivalent access to a server used to manage the broader Windows estate, materially shortening a lateral-movement path.
Attack Preconditions	Network position on the Server VLAN capable of intercepting or coercing NTLM authentication traffic (e.g., via a rogue responder-style listener in a non-destructive test configuration).
Attack Path	Server VLAN foothold → coerce or capture NTLM authentication from a privileged context → relay to NS-MGMT01 over unsigned SMB → authenticated session without credential disclosure → administrative pivot.
Safe Proof of Concept (Summary)	*A fictional relay test demonstrated that unsigned SMB on NS-MGMT01 accepted a relayed NTLM authentication attempt without requiring message signing. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-009
Expected Behavior	SMB signing should be required (not merely negotiated) on all Windows servers, particularly those used for administrative purposes.
Observed (Fictional) Behavior	All three servers accepted SMB sessions without signing enforced, confirmed via protocol negotiation capture.
Root Cause	SMB signing enforcement was never included in the Windows Server hardening baseline applied during server provisioning.
Security Risk	NTLM relay attacks against administrative infrastructure become practical without any credential compromise.

Recommendation	Enforce SMB signing (Require, not merely negotiate) on all Windows servers via Group Policy, prioritizing NS-MGMT01 and other administrative-tier hosts.
Remediation Guidance	1) Enable 'Microsoft network server: Digitally sign communications (always)' via GPO scoped to the Server VLAN OU; 2) validate no legacy application breaks under enforced signing; 3) extend the policy domain-wide; 4) add SMB signing status to the periodic configuration-compliance scan.
Management Response	*NorthStar engineering (fictional) has accepted this finding and will apply the signing-enforcement GPO within the 31-60 day remediation window.*
Owner / Priority / Target / Status	Active Directory Engineering Lead (Fictional Role) | 31-60 Days | 09 November 2026 | Remediation Planned
Retest Recommendation	*Retest by confirming SMB protocol negotiation reports signing as required on all three hosts.*

CATEGORY	RELATED FINDINGS	STATUS
Internal Network	NET-006, NET-013, NET-019	**Remediation Planned**

FULL EVIDENCE PANEL — ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE

```
SMB Signing Negotiation — NS-MGMT01 (Fictional / Synthetic)
$ smbclient -L //10.40.20.12 -N --option='client min protocol=SMB2'
Protocol negotiation (fictional capture):
  Dialect: SMB 3.1.1
  Signing Required: FALSE
  Signing Enabled: TRUE (negotiated, not enforced)

# Result: server will accept an unsigned session if the client declines signing
```

TECHNICAL EVIDENCE SUMMARY

Attack Preconditions	Network position on the Server VLAN capable of relaying or capturing NTLM authentication.
Observed Result	SMB signing was negotiable but not required on NS-FILE01, NS-APPSRV01, and NS-MGMT01.
Security Impact	NTLM relay attacks against these hosts are not blocked at the protocol layer.
Business Impact	A relay against the administrative jump server could yield elevated access without credential theft.
Evidence Collected	EV-NET-009 (SMB signing negotiation capture, all three hosts).
Retest Validation	Confirm signing is reported as required (not merely negotiated) post-remediation.

NET-006 — Insecure LDAP Configuration Permits Credential Exposure via Unsigned, Unencrypted Bind

HIGH

CVSS-Style Score	7.6 (High) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N — Illustrative vector only
CWE	CWE-319 — Cleartext Transmission of Sensitive Information
Affected Asset(s)	NS-DC01 (10.40.50.10), NS-DC02 (10.40.50.11)
Affected Network Segment	Identity / AD VLAN
Affected Service / Port	TCP/389 — LDAP
Affected Technology	Active Directory Domain Services — LDAP channel binding / signing

Description	Both domain controllers accept simple LDAP binds over unencrypted TCP/389 without requiring LDAP signing or channel binding. Several fictional legacy line-of-business applications authenticate against LDAP this way, transmitting the bind credential — including, in several cases, privileged service account credentials — in cleartext across the Server and Application VLANs.
Business Context	LDAP simple bind is used by at least three fictional legacy applications that have not been migrated to LDAPS or Kerberos authentication.
Technical Impact	Any attacker positioned to observe traffic between these applications and the domain controllers can capture cleartext credentials, including service account credentials with elevated directory permissions in some cases.
Business Impact	Passive credential harvesting from LDAP traffic provides a low-noise path to valid domain credentials without triggering the authentication-failure alerting NorthStar's SOC relies on.
Attack Preconditions	Network visibility into traffic between an LDAP-simple-bind application and a domain controller (e.g., a compromised host on the same VLAN or a device capable of ARP-based traffic redirection in a controlled test).
Attack Path	Network position on Server/Application VLAN → passive capture of LDAP simple-bind traffic → cleartext credential recovered → credential reused against other services (see NET-002, NET-010).
Safe Proof of Concept (Summary)	*A fictional passive capture of LDAP traffic recovered a synthetic cleartext bind credential during a scheduled legacy-application authentication cycle. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-010
Expected Behavior	LDAP simple binds should require TLS (LDAPS) or channel binding/signing, and cleartext LDAP should be disabled at the domain controller.
Observed (Fictional) Behavior	Both domain controllers accepted unsigned, unencrypted LDAP simple binds with no channel-binding enforcement.
Root Cause	LDAP channel binding enforcement (per Microsoft's 2020 guidance) was never enabled, largely to avoid breaking the legacy applications that still rely on simple bind.
Security Risk	Cleartext credential exposure across internal network segments, including for privileged service accounts in some observed cases.
Recommendation	Enable LDAP channel binding and signing enforcement on both domain controllers, and migrate remaining legacy applications to LDAPS or Kerberos authentication ahead of enforcement.
Remediation Guidance	1) Inventory all applications performing LDAP simple bind (event ID 2887/2889 auditing); 2) migrate each to LDAPS; 3) enable 'LDAP server signing requirements: Require signing' and channel binding via GPO; 4) rotate any credentials confirmed as legacy-bound during the inventory.
Management Response	*NorthStar engineering (fictional) will complete the legacy-application inventory and begin phased LDAPS migration within the 31-60 day window.*
Owner / Priority / Target / Status	Active Directory Engineering Lead (Fictional Role) | 31-60 Days | 09 November 2026 | Remediation Planned
Retest Recommendation	*Retest by confirming both domain controllers reject unsigned/unencrypted simple binds.*

CATEGORY	RELATED FINDINGS	STATUS
Active Directory	NET-005, NET-013, NET-033	**Remediation Planned**

FULL EVIDENCE PANEL — ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE

Cleartext LDAP Simple Bind Capture (Fictional / Synthetic)

```
$ tshark -i eth0 -Y 'ldap.bind_request' -T fields -e ldap.name -e ldap.simple
cn=svc-legacyapp,ou=ServiceAccounts,dc=northstar-example,dc=com    FICTIONAL-PW-Legacy24!

# Result: cleartext bind DN and password captured — LDAP signing/channel binding not enforced
```

TECHNICAL EVIDENCE SUMMARY

Attack Preconditions	Network visibility into LDAP traffic between a legacy application and a domain controller.
Observed Result	A cleartext bind credential was captured during a routine authentication cycle in the fictional test environment.
Security Impact	Domain credentials, including service accounts, are exposed to passive network observation.
Business Impact	Credentials obtained this way can be reused against other services without triggering failed-logon alerting.
Evidence Collected	EV-NET-010 (LDAP simple-bind traffic capture).
Retest Validation	Confirm cleartext simple binds are rejected and only LDAPS/signed LDAP succeeds.

NET-007 — Excessive Administrative Access Across User Network Segment via Helpdesk Group Policy

HIGH

CVSS-Style Score	7.8 (High) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H — Illustrative vector only
CWE	CWE-269 — Improper Privilege Management
Affected Asset(s)	All User Workstation VLAN endpoints (represented by NS-WKS-FIN07, NS-WKS-OPS12)
Affected Network Segment	User Workstation VLAN
Affected Service / Port	N/A — local group membership
Affected Technology	Group Policy — Restricted Groups configuration
Description	A Restricted Groups GPO scoped to the entire Workstations OU adds the NORTHSTAR\Helpdesk-All security group — which contains every member of the IT service desk, including Tier-1 staff — to the local Administrators group on every domain-joined workstation, rather than scoping this to a narrower, ticket-driven just-in-time model.
Business Context	This configuration was intended to let helpdesk staff resolve issues without escalation, but grants standing local admin rights on the entire user fleet to a large, comparatively high-turnover staff population.
Technical Impact	Compromise of any single Tier-1 helpdesk account grants local administrative rights on every domain-joined workstation, a substantially larger blast radius than intended.
Business Impact	A phished or reused-password helpdesk account becomes a fleet-wide lateral movement and credential-harvesting foothold across the entire User VLAN.
Attack Preconditions	Compromise of any account that is a member of NORTHSTAR\Helpdesk-All (a comparatively large, standard-privilege group).
Attack Path	Phished Helpdesk-All credential → local Administrator rights on any domain-joined workstation → credential harvesting (LSASS access) from privileged users who have logged onto that workstation → lateral movement.
Safe Proof of Concept (Summary)	*A fictional test account added to Helpdesk-All was confirmed to hold local Administrator rights on multiple randomly-sampled workstation test hosts. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-011
Expected Behavior	Administrative access to end-user workstations should be granted on a scoped, just-in-time basis (e.g., via a PAM/LAPS-style workflow) rather than standing group membership across the entire helpdesk population.

Observed (Fictional) Behavior	All members of Helpdesk-All held standing local Administrator rights on every domain-joined workstation.
Root Cause	The Restricted Groups GPO was configured for administrative convenience without a least-privilege or just-in-time access review.
Security Risk	A single compromised helpdesk account provides a fleet-wide privilege-escalation and lateral-movement foothold.
Recommendation	Replace standing Helpdesk-All local admin membership with a scoped, time-bound elevation mechanism (LAPS-managed local admin plus a PAM workflow, or a ticket-linked JIT elevation tool).
Remediation Guidance	1) Deploy Windows LAPS for unique, rotated local admin passwords per workstation; 2) remove Helpdesk-All from the Restricted Groups GPO; 3) implement a JIT elevation workflow tied to ticket approval; 4) audit for any other broad Restricted Groups assignments.
Management Response	*NorthStar engineering (fictional) has accepted this finding and will pilot LAPS deployment within the 31-60 day window ahead of full rollout.*
Owner / Priority / Target / Status	IT Service Desk Manager (Fictional Role) | 31-60 Days | 09 November 2026 | Remediation Planned
Retest Recommendation	*Retest by confirming Helpdesk-All is no longer present in local Administrators on a sample of workstations post-remediation.*

CATEGORY	RELATED FINDINGS	STATUS
Internal Network	NET-024, NET-026	**Remediation Planned**

FULL EVIDENCE PANEL — ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE

Helpdesk-All Local Administrator Membership (Fictional / Synthetic)

```
PS C:\> Get-LocalGroupMember -Group Administrators   # run on NS-WKS-OPS12 (fictional)
ObjectClass  Name
-----------  ----
Group        NORTHSTAR\Domain Admins
Group        NORTHSTAR\Helpdesk-All

# Result: entire Helpdesk-All membership (fictional, ~40 accounts) holds local admin on this
workstation
```

TECHNICAL EVIDENCE SUMMARY

Attack Preconditions	Compromise or credential reuse of any Helpdesk-All member account.
Observed Result	Helpdesk-All held standing local Administrator rights on every sampled domain-joined workstation.
Security Impact	A single compromised standard-privilege account yields fleet-wide administrative access.
Business Impact	Materially increases the blast radius of routine phishing or credential-reuse incidents.
Evidence Collected	EV-NET-011 (local group membership enumeration, sampled hosts).
Retest Validation	Confirm Helpdesk-All is removed from local Administrators and a scoped JIT mechanism is in place.

NET-008 — Weak VPN Security Configuration Permits Legacy Cryptographic Negotiation

HIGH

CVSS-Style Score	7.4 (High) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N — Illustrative vector only
CWE	CWE-327 — Use of a Broken or Risky Cryptographic Algorithm

Affected Asset(s)	NS-VPNGW01 (10.40.0.10)
Affected Network Segment	External Perimeter / DMZ
Affected Service / Port	UDP/500, UDP/4500 — IKEv1/IKEv2
Affected Technology	Site-to-site and legacy client IPsec VPN configuration
Description	NS-VPNGW01 continues to offer IKEv1 Aggressive Mode alongside IKEv2, using a Diffie-Hellman Group 2 (1024-bit) key exchange and a pre-shared key for a subset of legacy site-to-site tunnels. Aggressive Mode exchanges authentication material — including a hash derived from the PSK — before the encrypted channel is established, making offline PSK-cracking attempts feasible if that exchange is captured.
Business Context	The affected tunnels connect to a small number of fictional legacy branch-office routers that have not yet been upgraded to support IKEv2 with certificate-based authentication.
Technical Impact	An attacker able to capture the Aggressive Mode exchange can attempt offline dictionary/brute-force recovery of the pre-shared key without any interaction with the live gateway after capture.
Business Impact	Recovery of a site-to-site PSK could allow an attacker to establish a rogue tunnel or impersonate the affected branch peer, undermining the authenticity and integrity of that VPN connection.
Attack Preconditions	Ability to observe or capture the IKEv1 Aggressive Mode exchange (e.g., from a position on the external segment during tunnel establishment/rekey).
Attack Path	Capture IKEv1 Aggressive Mode exchange → offline PSK-cracking attempt against captured hash → (if successful) rogue tunnel establishment or peer impersonation for the affected branch link.
Safe Proof of Concept (Summary)	*A fictional capture of the Aggressive Mode negotiation confirmed DH Group 2 and PSK-based authentication were offered and accepted by the gateway for the legacy tunnel set. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-012
Expected Behavior	IKEv1 Aggressive Mode should be disabled; all tunnels should use IKEv2 with a minimum of DH Group 14 (2048-bit) or elliptic-curve groups, and certificate-based authentication where feasible.
Observed (Fictional) Behavior	IKEv1 Aggressive Mode with DH Group 2 and PSK authentication remained enabled and was offered to a fictional legacy peer.
Root Cause	Legacy branch-office equipment constraints led to Aggressive Mode being retained as a compatibility fallback, without a compensating control or upgrade timeline.
Security Risk	Offline PSK-cracking exposure for legacy site-to-site tunnels using weak cryptographic parameters.
Recommendation	Disable IKEv1 Aggressive Mode, require DH Group 14 or higher for all tunnels, and prioritize upgrading the remaining legacy branch equipment to support IKEv2 with certificate authentication.
Remediation Guidance	1) Disable Aggressive Mode gateway-wide; 2) raise minimum DH group to 14+ across all IKE proposals; 3) build an upgrade/replacement plan for legacy branch routers; 4) rotate PSKs for all affected tunnels as an interim compensating step.
Management Response	*NorthStar engineering (fictional) will disable Aggressive Mode and rotate affected PSKs within the 31-60 day window while the branch hardware upgrade is scheduled separately.*
Owner / Priority / Target / Status	Network Security Engineering Lead (Fictional Role) | 31-60 Days | 09 November 2026 | Remediation Planned
Retest Recommendation	*Retest by confirming Aggressive Mode is no longer offered and all active tunnels negotiate DH Group 14 or higher.*

CATEGORY	RELATED FINDINGS	STATUS
External Network	NET-001, NET-015, NET-035	**Remediation Planned**

FULL EVIDENCE PANEL — ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE

IKEv1 Aggressive Mode Negotiation Capture (Fictional / Synthetic)

```
$ ike-scan --aggressive --id=fictional-branch-07 10.40.0.10
Starting ike-scan (fictional sample capture)
10.40.0.10  Aggressive Mode Handshake returned
  SA=(Enc=AES-256 Hash=SHA1 Group=2:modp1024 Auth=PSK)
  ID(Type=ID_FQDN, Value=fictional-branch-07.northstar-example.com)

# Result: Aggressive Mode + DH Group 2 (1024-bit) + PSK offered and accepted
```

TECHNICAL EVIDENCE SUMMARY

Attack Preconditions	Network visibility of IKE negotiation traffic to NS-VPNGW01 during tunnel establishment or rekey.
Observed Result	IKEv1 Aggressive Mode with DH Group 2 and PSK authentication was offered and accepted for the legacy tunnel set.
Security Impact	The captured exchange is susceptible to offline PSK-cracking attempts.
Business Impact	A recovered PSK could allow rogue tunnel establishment or impersonation of the affected branch peer.
Evidence Collected	EV-NET-012 (IKE Aggressive Mode negotiation capture).
Retest Validation	Confirm Aggressive Mode is disabled and all tunnels negotiate DH Group 14+ post-remediation.

NET-009 — SNMP Community String Configuration Exposes Network Device Information

HIGH

CVSS-Style Score	7.2 (High) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N — Illustrative vector only
CWE	CWE-200 — Exposure of Sensitive Information to an Unauthorized Actor
Affected Asset(s)	NS-COREW01 (172.20.10.1), NS-DSW01 (172.20.10.2), NS-DSW02 (172.20.10.3)
Affected Network Segment	Management VLAN (reachable from Server VLAN due to related exposure)
Affected Service / Port	UDP/161 — SNMP
Affected Technology	SNMPv1/v2c community-string configuration
Description	The core switch and both distribution switches respond to SNMPv2c queries using a fictional default-pattern community string ('public' for read, a guessable variant for read-write), and SNMPv1/v2c remains enabled alongside SNMPv3 rather than being disabled in favor of it.
Business Context	SNMP is used by NS-NMS01 for device monitoring and configuration backup; the read-write community string in particular allows configuration changes if guessed.
Technical Impact	An attacker able to reach UDP/161 on these devices can enumerate device configuration, routing tables, interface details, and — if the read-write string is guessed — alter device configuration via SNMP SET operations.
Business Impact	Detailed network topology and configuration disclosure materially aids further attack planning, and read-write access could allow direct device reconfiguration.
Attack Preconditions	Network reachability to UDP/161 on the affected devices (present due to the management-plane exposure described in NET-004).

Attack Path	Network access to Management VLAN scope (via NET-004) → SNMPv2c community-string guessing → device information disclosure or configuration SET via SNMP.
Safe Proof of Concept (Summary)	*A fictional SNMP walk using a guessed community string returned device system information, interface tables, and routing details from all three devices. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-013
Expected Behavior	SNMPv1/v2c should be disabled in favor of SNMPv3 with authentication and privacy (authPriv), and community strings, where still required for legacy tooling, should be unique, high-entropy, and access-list restricted.
Observed (Fictional) Behavior	All three devices accepted SNMPv2c queries using a fictional default-pattern community string, with SNMPv1/v2c enabled alongside SNMPv3.
Root Cause	SNMPv3 migration was completed for network management tooling but the legacy v2c community strings were never removed as a fallback.
Security Risk	Network topology, configuration, and potentially write access is exposed to any actor who can reach the management plane and guess a weak community string.
Recommendation	Disable SNMPv1/v2c on all network devices, standardize exclusively on SNMPv3 authPriv, and restrict SNMP access via ACL to NS-NMS01 only.
Remediation Guidance	1) Disable SNMPv1/v2c community strings device-wide; 2) confirm NS-NMS01 and all monitoring tooling support SNMPv3 authPriv; 3) apply an SNMP access-list restricting queries to NS-NMS01's address only; 4) rotate SNMPv3 credentials as a precaution.
Management Response	*NorthStar engineering (fictional) will complete the SNMPv3-only migration within the 31-60 day window.*
Owner / Priority / Target / Status	Network Operations Lead (Fictional Role) | 31-60 Days | 09 November 2026 | Remediation Planned
Retest Recommendation	*Retest by confirming SNMPv1/v2c queries are rejected and only SNMPv3 authPriv succeeds from the authorized management host.*

CATEGORY	RELATED FINDINGS	STATUS
Network Devices	NET-004, NET-029	**Remediation Planned**

FULL EVIDENCE PANEL — ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE

SNMPv2c Community String Enumeration (Fictional / Synthetic)

```
$ snmpwalk -v2c -c public 172.20.10.1 system
SNMPv2-MIB::sysDescr.0 = FictionalNOS 15.2, Core-Switch (fictional)
SNMPv2-MIB::sysName.0 = ns-corew01.northstar-example.com
IF-MIB::ifTable: (47 interfaces enumerated, fictional)

# Result: full system/interface disclosure via guessable v2c community string
```

TECHNICAL EVIDENCE SUMMARY

Attack Preconditions	Network reachability to UDP/161 on the affected devices.
Observed Result	All three devices responded to SNMPv2c queries using a guessable community string, disclosing configuration and topology data.
Security Impact	Detailed device and network configuration disclosure aids further attack planning; write access is possible if the RW string is guessed.
Business Impact	Supports rapid reconnaissance of the core network fabric with minimal attacker effort.
Evidence Collected	EV-NET-013 (SNMPv2c walk output, three devices).
Retest Validation	Confirm SNMPv1/v2c is disabled and only authenticated SNMPv3 queries from NS-NMS01 succeed.

NET-010 — RDP Accessible Across Improperly Segmented Network Boundaries	HIGH
CVSS-Style Score	8.0 (High) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L — Illustrative vector only
CWE	CWE-284 — Improper Access Control
Affected Asset(s)	NS-APPSRV01 (10.40.20.11), NS-MGMT01 (10.40.20.12), NS-SQL01 (10.40.40.10)
Affected Network Segment	User Workstation VLAN → Server VLAN, Database VLAN
Affected Service / Port	TCP/3389 — RDP
Affected Technology	Windows Remote Desktop Protocol; firewall policy
Description	TCP/3389 is reachable directly from the User Workstation VLAN to multiple Server and Database VLAN hosts, rather than being restricted to originate only from NS-MGMT01 (the designated administrative jump server) as NorthStar's remote-administration standard specifies.
Business Context	Direct user-to-server RDP access bypasses the jump-host model NorthStar's administrative access design relies on for session recording and centralized credential control.
Technical Impact	Any workstation with valid or crackable credentials for a local or domain account with logon rights on these servers can establish an interactive administrative session directly, without passing through the monitored jump-host path.
Business Impact	This exposure both widens the lateral-movement attack surface and removes visibility NorthStar's SOC otherwise has over administrative sessions via the jump-host path.
Attack Preconditions	Network access to the User VLAN and valid or crackable credentials for an account with RDP logon rights on the target server.
Attack Path	Compromised workstation (User VLAN) → direct RDP to NS-APPSRV01/NS-MGMT01/NS-SQL01 → interactive session with the compromised account's privilege level, bypassing the jump-host control point.
Safe Proof of Concept (Summary)	*A fictional test host on the User VLAN established a direct RDP negotiation with all three servers with no firewall interruption observed. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-014
Expected Behavior	RDP to Server and Database VLAN hosts should be permitted only from the designated administrative jump host (NS-MGMT01); direct User VLAN-to-server RDP should be denied.
Observed (Fictional) Behavior	Direct RDP reachability from the User VLAN to all three servers was confirmed with no intervening restriction.
Root Cause	The segmentation policy was never updated to restrict RDP source zones following the introduction of the jump-host administrative model.
Security Risk	Bypass of the organization's jump-host administrative control model, widening the lateral-movement surface for any compromised credential.
Recommendation	Restrict inbound RDP on Server and Database VLAN hosts to originate only from NS-MGMT01, denying direct User VLAN RDP reachability.
Remediation Guidance	1) Implement Windows Firewall / GPO-based RDP source restriction limiting inbound RDP to NS-MGMT01's address; 2) mirror the restriction at NS-FWINT01; 3) validate against the segmentation matrix in Appendix E; 4) enable RDP session auditing/logging centrally via NS-SIEM01.
Management Response	*NorthStar engineering (fictional) will implement the RDP source restriction within the 31-60 day window as part of the broader segmentation remediation.*

Owner / Priority / Target / Status	Network Security Engineering Lead (Fictional Role) | 31-60 Days | 09 November 2026 | Remediation Planned
Retest Recommendation	*Retest by confirming direct User VLAN RDP to the affected servers is denied while access via NS-MGMT01 remains functional.*

CATEGORY	RELATED FINDINGS	STATUS
Internal Network	NET-002, NET-026	**Remediation Planned**

FULL EVIDENCE PANEL — ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE

Direct User VLAN → Server VLAN RDP Reachability (Fictional / Synthetic)

```
$ nmap -Pn -p 3389 10.40.20.11 10.40.20.12 10.40.40.10
10.40.20.11  3389/tcp open  ms-wbt-server
10.40.20.12  3389/tcp open  ms-wbt-server
10.40.40.10  3389/tcp open  ms-wbt-server

# Result: RDP reachable directly from User VLAN test host — jump-host path not enforced
```

TECHNICAL EVIDENCE SUMMARY

Attack Preconditions	Network access to the User VLAN and any valid/crackable RDP-authorized credential.
Observed Result	TCP/3389 was directly reachable from the User VLAN to three Server/Database VLAN hosts with no firewall restriction.
Security Impact	Bypasses the organization's jump-host administrative control and session-recording model.
Business Impact	Widens the lateral-movement path available to any compromised end-user credential with server logon rights.
Evidence Collected	EV-NET-014 (RDP reachability scan, three targets).
Retest Validation	Confirm direct User VLAN RDP is blocked while jump-host-originated RDP continues to function.

NET-011 — Insecure Firewall Rule Permits Management-Plane Access From Corporate Wireless Segment

HIGH

CVSS-Style Score	8.3 (High) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Illustrative vector only
CWE	CWE-284 — Improper Access Control
Affected Asset(s)	NS-WLC01 (172.20.10.5), NS-FWINT01 (172.20.10.10)
Affected Network Segment	Wireless — Corporate SSID → Management VLAN
Affected Service / Port	TCP/443 — HTTPS
Affected Technology	Internal firewall policy — wireless-to-management path
Description	A firewall rule intended to permit only the wireless controller's uplink to reach the Management VLAN was written using an overly broad source object that also includes the entire Corporate SSID client address range, allowing any device connected to the corporate wireless network to reach management HTTPS interfaces on NS-WLC01 and NS-FWINT01 directly.
Business Context	The Corporate SSID is used by a large population of laptops and BYOD devices; it is not intended to have any direct reachability to network management infrastructure.
Technical Impact	Any device joined to the Corporate SSID — including a compromised or unmanaged BYOD device — can reach the wireless controller and internal firewall's management interfaces directly.

Business Impact	Combined with NET-004's credential weakness, this creates a second independent path to management-plane compromise, this time requiring only corporate wireless network access rather than wired User VLAN access.
Attack Preconditions	Corporate SSID network access (802.1X credential or a device already provisioned on the corporate wireless network) and, per NET-004, the unrotated default credential.
Attack Path	Corporate SSID join → direct HTTPS reachability to NS-WLC01/NS-FWINT01 management interfaces → authentication (see NET-004) → management-plane compromise.
Safe Proof of Concept (Summary)	*A fictional test device on the Corporate SSID reached both management interfaces directly, confirming the overly broad source object. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-015
Expected Behavior	Only the wireless controller's designated uplink interface — not the Corporate SSID client range — should be permitted to reach Management VLAN interfaces.
Observed (Fictional) Behavior	The full Corporate SSID client subnet was included in the permitted source object for management-plane access.
Root Cause	The firewall rule was written against a supernet object that inadvertently included both the intended uplink and the client-facing SSID range.
Security Risk	A second, wireless-based path to management-plane compromise independent of wired network access.
Recommendation	Narrow the firewall rule's source object to the wireless controller's specific uplink address only, removing the Corporate SSID client range.
Remediation Guidance	1) Identify and correct the overly broad source object on NS-FWINT01; 2) validate against the segmentation matrix (Appendix E, Wireless → Management row); 3) confirm no legitimate dependency exists on the broader access before removal.
Management Response	*NorthStar engineering (fictional) will correct the firewall object within the 31-60 day window as part of the broader segmentation remediation.*
Owner / Priority / Target / Status	Wireless Infrastructure Lead (Fictional Role) | 31-60 Days | 09 November 2026 | Remediation Planned
Retest Recommendation	*Retest by confirming Corporate SSID clients other than the WLC uplink can no longer reach Management VLAN interfaces.*

CATEGORY	RELATED FINDINGS	STATUS
Wireless	NET-004, NET-027	**Remediation Planned**

FULL EVIDENCE PANEL — ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE

Corporate SSID → Management VLAN Reachability (Fictional / Synthetic)

```
$ curl -sk -I https://172.20.10.5/  # sourced from a Corporate SSID test client
HTTP/1.1 200 OK
Server: FictionalWLC-WebUI/3.1

# Result: WLC management interface directly reachable from a standard Corporate SSID client
```

TECHNICAL EVIDENCE SUMMARY

Attack Preconditions	Corporate SSID network access (standard 802.1X-authenticated join).
Observed Result	A test client on the Corporate SSID reached management HTTPS interfaces on NS-WLC01 and NS-FWINT01 directly.
Security Impact	Establishes a wireless-based path to management-plane infrastructure independent of wired access.
Business Impact	Expands the population of devices that could serve as a launch point for management-plane compromise.

Evidence Collected	EV-NET-015 (Corporate SSID to Management VLAN reachability test).
Retest Validation	Confirm only the designated WLC uplink — not general Corporate SSID clients — can reach Management VLAN interfaces.

NET-012 — Sensitive Backup Repository Reachable From User VLAN Without Authentication Segmentation	**HIGH**
CVSS-Style Score	8.6 (High) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N — Illustrative vector only
CWE	CWE-732 — Incorrect Permission Assignment for Critical Resource
Affected Asset(s)	NS-BKP01 (10.40.60.10)
Affected Network Segment	User Workstation VLAN → Backup VLAN
Affected Service / Port	TCP/445 — SMB
Affected Technology	Backup repository share permissions
Description	The primary backup repository share on NS-BKP01 is reachable from the User Workstation VLAN and permits read access to the 'Domain Users' group at the share level, rather than being restricted to the backup service account and a small administrative group. The share contains full or incremental backups of NS-DC01/NS-DC02 system state and NS-SQL01/NS-SQL02 database backups.
Business Context	Backup data is a high-value target because it typically bypasses the access controls enforced on the live systems it was captured from — a database backup file, for example, is not protected by the database's own authentication.
Technical Impact	Any authenticated domain user can browse and download AD system-state and database backup files directly from the User VLAN.
Business Impact	This is functionally equivalent to exposing the contents of the domain controllers and core database to every employee, sharply increasing the risk of large-scale data exposure from a single compromised standard user account.
Attack Preconditions	Any valid, standard domain user account and network reachability to the Backup VLAN from the User VLAN (present due to the missing segmentation control).
Attack Path	Standard domain user → SMB access to backup share (Domain Users read permission) → download AD system-state or database backup files → offline extraction of credential material or sensitive data.
Safe Proof of Concept (Summary)	*A fictional test account with standard domain-user rights listed and read a sample backup-catalog file from the NS-BKP01 share, confirming both the segmentation gap and the excessive share permission. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-016
Expected Behavior	The Backup VLAN should not be reachable from the User VLAN, and backup share permissions should be limited to the backup service account and a small administrative group — never Domain Users.
Observed (Fictional) Behavior	Both the network reachability and the share-permission control were absent: a standard domain user could reach and read the backup share from the User VLAN.
Root Cause	The backup share's NTFS/share permissions were left at a broad default during initial configuration, and no segmentation rule was created to isolate the Backup VLAN when it was introduced.

Security Risk	Any standard employee account provides read access to AD and database backup contents, a scope of exposure disproportionate to a single compromised credential.
Recommendation	Restrict the backup share to the backup service account and a named administrative group, and isolate the Backup VLAN from the User VLAN at the firewall.
Remediation Guidance	1) Remove Domain Users from the backup share ACL and replace with a scoped administrative group; 2) add a Backup VLAN isolation rule to NS-FWINT01 denying User VLAN reachability; 3) enable access auditing on the share; 4) review backup encryption-at-rest configuration as a defense-in-depth measure.
Management Response	*NorthStar engineering (fictional) has treated this as a high-priority remediation item and will correct both the share permissions and network segmentation within the 31-60 day window.*
Owner / Priority / Target / Status	Infrastructure Operations Lead (Fictional Role) | 31-60 Days | 09 November 2026 | Remediation Planned
Retest Recommendation	*Retest by confirming the backup share is unreachable from the User VLAN and that Domain Users no longer has read access.*

CATEGORY	RELATED FINDINGS	STATUS
Internal Network	NET-002, NET-003, NET-020	**Remediation Planned**

FULL EVIDENCE PANEL — ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE

```
Backup Share Access From User VLAN (Fictional / Synthetic)
$ smbclient //10.40.60.10/BackupRepo -U northstar\\fictional.user
smb: \> ls
  AD-SystemState-2026-08-27.bak      1,204,982,331   Fri Aug 28 02:14:02 2026
  NS-SQL01-Full-2026-08-27.bak       8,911,204,552   Fri Aug 28 03:41:19 2026

# Result: standard domain user read access to AD and database backup files confirmed
```

TECHNICAL EVIDENCE SUMMARY

Attack Preconditions	Any standard, authenticated domain user account.
Observed Result	The backup share was reachable from the User VLAN and permitted Domain Users to list and read AD and database backup files.
Security Impact	Backup data equivalent to full AD system-state and database contents is exposed to the entire employee population.
Business Impact	Sharply increases the risk of mass sensitive-data exposure from a single low-privilege compromised account.
Evidence Collected	EV-NET-016 (backup share access and directory listing).
Retest Validation	Confirm the share is unreachable from the User VLAN and permissions are limited to the backup service account and administrative group.

NET-013 — Weak Service Account Security Enables Lateral Movement via Kerberoasting

HIGH

CVSS-Style Score	7.9 (High) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N — Illustrative vector only
CWE	CWE-522 — Insufficiently Protected Credentials
Affected Asset(s)	NS-DC01 (10.40.50.10), NS-DC02 (10.40.50.11)
Affected Network Segment	Identity / AD VLAN
Affected Service / Port	TCP/UDP 88 — Kerberos

Affected Technology	Active Directory service account configuration
Description	Several fictional Service Principal Name (SPN)-registered service accounts in the NORTHSTAR domain use passwords that have not been rotated in over three years and do not meet the organization's standard complexity policy for interactive accounts, making them feasible targets for a Kerberoasting attack: requesting a service ticket for the SPN and attempting offline password recovery against the ticket's encrypted portion.
Business Context	Kerberoasting requires only a standard authenticated domain account — no elevated privilege — to request service tickets for any SPN in the domain.
Technical Impact	An attacker with any valid domain credential can request service tickets for all SPN-registered accounts and attempt offline cracking without generating the failed-logon events that would trigger standard alerting.
Business Impact	Successful cracking of a service account password can grant the privileges associated with that account, in several fictional cases including elevated rights on application and database tiers.
Attack Preconditions	Any valid, standard domain user credential (no elevated privilege required to request service tickets).
Attack Path	Standard domain credential → request service tickets for SPN-registered accounts → offline cracking attempt against weak/stale passwords → (if successful) authenticate as the compromised service account.
Safe Proof of Concept (Summary)	*A fictional test using a standard domain account requested service tickets for several SPN-registered accounts; offline analysis of a synthetic sample ticket confirmed weak password material within a bounded, non-destructive test. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-017
Expected Behavior	SPN-registered service account passwords should be long (25+ characters), randomly generated, and rotated regularly, or accounts should be migrated to group Managed Service Accounts (gMSA) where feasible.
Observed (Fictional) Behavior	Multiple SPN-registered accounts used passwords that had not been rotated in over three years and did not meet standard complexity requirements.
Root Cause	Service account password rotation was never automated or enforced with the same rigor as interactive user accounts, and gMSA migration has not been prioritized for legacy services.
Security Risk	Any standard domain user can obtain crackable material for privileged service accounts with no elevated starting privilege.
Recommendation	Migrate SPN-registered service accounts to gMSA where supported; for accounts that cannot be migrated, enforce 25+ character randomly generated passwords with regular rotation.
Remediation Guidance	1) Inventory all SPN-registered accounts and their current password age; 2) prioritize migration to gMSA for supported workloads; 3) for remaining accounts, generate high-entropy passwords and establish a rotation schedule; 4) monitor for abnormal service-ticket request volume (event ID 4769) as a compensating detective control.
Management Response	*NorthStar engineering (fictional) will complete the service account inventory and begin phased gMSA migration within the 31-60 day window.*
Owner / Priority / Target / Status	Active Directory Engineering Lead (Fictional Role) | 31-60 Days | 09 November 2026 | Remediation Planned
Retest Recommendation	*Retest by re-sampling SPN-registered account password age and confirming ticket-cracking attempts fail against a reasonable time budget.*

CATEGORY	RELATED FINDINGS	STATUS
Active Directory	NET-002, NET-003, NET-023, NET-025	**Remediation Planned**

FULL EVIDENCE PANEL — ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE

SPN Service Ticket Enumeration (Fictional / Synthetic)

```
PS C:\> Get-DomainSPNTicket -SPN * | Select SamAccountName,PasswordLastSet
SamAccountName        PasswordLastSet
--------------        ---------------
svc-reporting         2023-02-11 (fictional)
svc-legacyapp         2022-09-04 (fictional)

# Result: two SPN-registered accounts with password age exceeding three years
```

TECHNICAL EVIDENCE SUMMARY

Attack Preconditions	Any valid, standard domain user account with no elevated privilege.
Observed Result	Service tickets were successfully requested for stale SPN-registered accounts, confirmed vulnerable to offline cracking attempts.
Security Impact	Privileged service account compromise is achievable without triggering standard failed-logon detections.
Business Impact	A cracked service account could grant elevated application or database-tier privileges to an attacker starting from a standard user credential.
Evidence Collected	EV-NET-017 (SPN enumeration and password-age review).
Retest Validation	Confirm migrated accounts no longer expose crackable material and remaining accounts meet the high-entropy password standard.

21 MEDIUM FINDINGS

The following 14 fictional Medium-severity findings reflect defense-in-depth and hardening gaps recommended for remediation within the 61-90 day window of the illustrative roadmap (Section 25).

NET-014 — Outdated TLS Configuration on External Remote Access Portal	MEDIUM
CVSS-Style Score	5.9 (Medium) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N — Illustrative vector only
CWE	CWE-326 — Inadequate Encryption Strength
Affected Asset(s)	NS-PORTAL01 (10.40.0.11)
Affected Network Segment	External Perimeter / DMZ
Affected Service / Port	TCP/443 — HTTPS
Affected Technology	TLS configuration
Description	NS-PORTAL01 continues to negotiate TLS 1.0 and TLS 1.1, along with several CBC-mode cipher suites deprecated by current guidance, alongside its primary TLS 1.2/1.3 configuration.
Technical Impact	Clients (or an attacker performing a downgrade attempt) can negotiate a weaker protocol version, increasing exposure to known TLS 1.0/1.1 protocol weaknesses.
Business Impact	Legacy protocol exposure on an authentication-handling portal is inconsistent with NorthStar's stated security posture as a financial services provider and may affect compliance attestations.
Safe Proof of Concept (Summary)	*A fictional TLS scan confirmed TLS 1.0 and 1.1 remain negotiable on NS-PORTAL01 alongside TLS 1.2/1.3. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-018
Expected vs. Observed (Fictional)	Expected: Only TLS 1.2 and 1.3 should be offered, with weak/CBC cipher suites disabled. // Observed: TLS 1.0 and 1.1 were both negotiable, alongside several deprecated cipher suites.
Root Cause	The TLS configuration was inherited from an older load-balancer template and never updated to the current hardening baseline.
Security Risk	Unnecessary cryptographic downgrade exposure on an internet-facing authentication portal.
Recommendation	Disable TLS 1.0/1.1 and deprecated cipher suites, restricting the portal to TLS 1.2/1.3 with modern cipher suites only.
Management Response	*NorthStar engineering (fictional) will update the TLS profile within the 61-90 day window.*
Owner / Priority / Target / Status	Network Security Engineering Lead (Fictional Role) | 61-90 Days | 09 December 2026 | Remediation Planned
Retest Recommendation	*Retest by confirming only TLS 1.2/1.3 are negotiable and deprecated ciphers are removed.*

CATEGORY	RELATED FINDINGS	STATUS
External Network	NET-015, NET-022	**Remediation Planned**

NET-015 — Certificate Configuration Issue on	MEDIUM

External VPN Gateway	
CVSS-Style Score	5.3 (Medium) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N — Illustrative vector only
CWE	CWE-295 — Improper Certificate Validation
Affected Asset(s)	NS-VPNGW01 (10.40.0.10)
Affected Network Segment	External Perimeter / DMZ
Affected Service / Port	TCP/443 — HTTPS
Affected Technology	TLS certificate configuration
Description	NS-VPNGW01's TLS certificate for the primary VPN portal was observed to expire within 21 days of the assessment window and uses a SHA-1 signature on one intermediate in the chain, inconsistent with current best practice.
Technical Impact	Certificate expiry would interrupt remote-access availability; the SHA-1 intermediate, while not immediately exploitable, does not meet current cryptographic guidance.
Business Impact	An unplanned VPN outage during a certificate lapse would affect all remote employees and third-party administrators simultaneously.
Safe Proof of Concept (Summary)	*A fictional certificate inspection confirmed a 21-day validity window remaining and a SHA-1 signed intermediate certificate in the chain. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-019
Expected vs. Observed (Fictional)	Expected: Certificates should be renewed well ahead of expiry via automated lifecycle management, and the full chain should use SHA-256 or stronger signatures. // Observed: The certificate was nearing expiry with no automated renewal observed, and one intermediate used a SHA-1 signature.
Root Cause	Certificate renewal for this specific gateway is performed manually rather than through NorthStar's automated certificate-lifecycle tooling.
Security Risk	Service interruption risk from expiry, plus a weakened trust chain from the legacy signature algorithm.
Recommendation	Bring NS-VPNGW01 under automated certificate lifecycle management and replace the SHA-1 signed intermediate.
Management Response	*NorthStar engineering (fictional) will renew the certificate immediately and complete automated enrollment within the 61-90 day window.*
Owner / Priority / Target / Status	Network Security Engineering Lead (Fictional Role) | 61-90 Days | 09 December 2026 | Remediation Planned
Retest Recommendation	*Retest by confirming certificate validity exceeds 60 days and the full chain uses SHA-256 or stronger.*

CATEGORY	RELATED FINDINGS	STATUS
External Network	NET-008, NET-014	**Remediation Planned**

NET-016 — DNS Configuration Weakness Permits Zone Transfer from External DNS Server	MEDIUM
CVSS-Style Score	5.8 (Medium) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N — Illustrative vector only
CWE	CWE-200 — Exposure of Sensitive Information to an Unauthorized Actor

Affected Asset(s)	NS-DNSEXT01 (10.40.0.14)
Affected Network Segment	External Perimeter / DMZ
Affected Service / Port	TCP/53 — DNS
Affected Technology	Authoritative DNS zone transfer (AXFR) configuration
Description	NS-DNSEXT01 permits AXFR zone transfer requests from arbitrary source addresses for the northstar-example.com zone, rather than restricting transfers to designated secondary name servers.
Technical Impact	Any external party can request a full zone transfer and enumerate every published record in a single query, rather than needing to brute-force subdomains.
Business Impact	Accelerates external reconnaissance by disclosing the organization's full public DNS footprint in one step, including several fictional legacy or staging hostnames.
Safe Proof of Concept (Summary)	*A fictional AXFR request against NS-DNSEXT01 returned the full synthetic zone file for northstar-example.com. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-020
Expected vs. Observed (Fictional)	Expected: Zone transfers should be restricted via ACL to designated secondary name servers only. // Observed: AXFR succeeded from an arbitrary, unauthorized test source address.
Root Cause	The zone-transfer ACL was never configured when the authoritative DNS service was deployed.
Security Risk	One-step disclosure of the organization's complete public DNS record set to any external party.
Recommendation	Restrict AXFR zone transfers to designated secondary name server addresses only.
Management Response	*NorthStar engineering (fictional) will apply the transfer ACL within the 61-90 day window.*
Owner / Priority / Target / Status	Network Security Engineering Lead (Fictional Role) | 61-90 Days | 09 December 2026 | Remediation Planned
Retest Recommendation	*Retest by confirming AXFR requests from unauthorized sources are refused.*

CATEGORY	RELATED FINDINGS	STATUS
External Network	NET-044	**Remediation Planned**

NET-017 — Exposed Service With Unnecessary Functionality on External Load Balancer

MEDIUM

CVSS-Style Score	6.4 (Medium) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N — Illustrative vector only
CWE	CWE-16 — Configuration
Affected Asset(s)	NS-WAF01 (10.40.0.12)
Affected Network Segment	External Perimeter / DMZ
Affected Service / Port	TCP/8443 — HTTPS (management API)
Affected Technology	Web Application Firewall management API
Description	The WAF's administrative REST API is reachable on TCP/8443 from the public interface rather than being restricted to the Management VLAN, exposing configuration and rule-management functionality unnecessarily to the internet.

Technical Impact	The management API accepts connections from the internet, increasing the attack surface available to brute-force or vulnerability-based attacks against the API itself.
Business Impact	Compromise of the WAF management plane could allow an attacker to disable or bypass protections for the public web applications it fronts.
Safe Proof of Concept (Summary)	*A fictional external scan confirmed the WAF management API responded on the public interface with an authentication prompt reachable from the internet. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-021
Expected vs. Observed (Fictional)	Expected: The WAF management API should be reachable only from the Management VLAN, never from the public interface. // Observed: The management API was reachable and responded to requests from an external test source.
Root Cause	The management interface was bound to all addresses during initial deployment rather than the intended management-only interface.
Security Risk	Unnecessary internet exposure of a sensitive administrative control point for the organization's public-facing web protections.
Recommendation	Rebind the WAF management API to the Management VLAN interface only and block TCP/8443 at the external firewall.
Management Response	*NorthStar engineering (fictional) will complete the rebind within the 61-90 day window.*
Owner / Priority / Target / Status	Network Security Engineering Lead (Fictional Role) | 61-90 Days | 09 December 2026 | Remediation Planned
Retest Recommendation	*Retest by confirming TCP/8443 no longer responds on the public interface.*

CATEGORY	RELATED FINDINGS	STATUS
External Network	NET-004	**Remediation Planned**

NET-018 — Information Disclosure Through Verbose Error Messages on Public Web Application Gateway

MEDIUM

CVSS-Style Score	4.3 (Medium) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N — Illustrative vector only
CWE	CWE-209 — Generation of Error Message Containing Sensitive Information
Affected Asset(s)	NS-WAF01 (10.40.0.12)
Affected Network Segment	External Perimeter / DMZ
Affected Service / Port	TCP/443 — HTTPS
Affected Technology	Backend application error handling
Description	Malformed requests to several fictional public-facing endpoints behind NS-WAF01 return backend stack traces revealing internal framework versions, internal hostnames, and file-system paths rather than a generic error page.
Technical Impact	Internal implementation details — framework version, internal hostname references, and file paths — are disclosed via crafted malformed requests.
Business Impact	Lowers the effort required for an attacker to identify version-specific vulnerabilities in the backend stack.
Safe Proof of Concept (Summary)	*A fictional malformed request returned a backend stack trace disclosing internal framework and path information. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-022

Expected vs. Observed (Fictional)	Expected: Generic, non-revealing error pages should be returned for all error conditions on public-facing endpoints. // Observed: Backend stack traces were returned directly to the client for several malformed-request scenarios.
Root Cause	Custom error-page handling was not configured for these endpoints; the backend framework's default debug-style error output remains active.
Security Risk	Reconnaissance-value information disclosure that eases follow-on vulnerability targeting.
Recommendation	Configure generic custom error pages for all public-facing endpoints and disable backend debug-mode error output.
Management Response	*NorthStar engineering (fictional) will disable debug-mode error output within the 61-90 day window.*
Owner / Priority / Target / Status	Backend/API Engineering Lead (Fictional Role) | 61-90 Days | 09 December 2026 | Remediation Planned
Retest Recommendation	*Retest using the same malformed-request set and confirm only generic error output is returned.*

CATEGORY	RELATED FINDINGS	STATUS
External Network	NET-025	**Remediation Planned**

NET-019 — Legacy/Insecure Protocol Exposure — SMBv1 Still Enabled on Internal File Server

MEDIUM

CVSS-Style Score	6.8 (Medium) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H — Illustrative vector only
CWE	CWE-327 — Use of a Broken or Risky Cryptographic Algorithm
Affected Asset(s)	NS-FILE01 (10.40.20.10)
Affected Network Segment	Server VLAN
Affected Service / Port	TCP/445, TCP/139 — SMBv1
Affected Technology	Windows Server SMB protocol configuration
Description	NS-FILE01 continues to have the SMBv1 protocol enabled to support a small number of fictional legacy departmental scanning devices, rather than the SMBv1 dependency having been eliminated and the protocol disabled outright.
Technical Impact	SMBv1's protocol-level weaknesses make the file server a comparatively higher-value target for any attacker with internal network access, independent of application-layer vulnerabilities.
Business Impact	Retaining SMBv1 for a small number of legacy devices exposes the entire file server to protocol-level risk disproportionate to the convenience gained.
Safe Proof of Concept (Summary)	*A fictional protocol negotiation confirmed SMBv1 remained enabled and negotiable on NS-FILE01. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-023
Expected vs. Observed (Fictional)	Expected: SMBv1 should be disabled; legacy devices requiring it should be isolated to a dedicated, tightly-scoped network segment if they cannot be replaced. // Observed: SMBv1 remained enabled and negotiable server-wide.
Root Cause	SMBv1 was never disabled following the identification of the legacy scanning-device dependency; no compensating isolation was implemented either.
Security Risk	Unnecessary protocol-level attack surface retained for the convenience of a small number of legacy devices.

Recommendation	Disable SMBv1 on NS-FILE01 and isolate any remaining legacy-device dependency to a dedicated, restricted VLAN if it cannot be eliminated.
Management Response	*NorthStar engineering (fictional) will disable SMBv1 and isolate any remaining legacy devices within the 61-90 day window.*
Owner / Priority / Target / Status	Infrastructure Operations Lead (Fictional Role) | 61-90 Days | 09 December 2026 | Remediation Planned
Retest Recommendation	*Retest by confirming SMBv1 is no longer negotiable on NS-FILE01.*

CATEGORY	RELATED FINDINGS	STATUS
Internal Network	NET-005	**Remediation Planned**

NET-020 — Unnecessary East-West Connectivity Between Application VLAN and Database VLAN Beyond Required Ports

MEDIUM

CVSS-Style Score	5.6 (Medium) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N — Illustrative vector only
CWE	CWE-284 — Improper Access Control
Affected Asset(s)	NS-LINAPP01 (10.40.30.10), NS-API01 (10.40.30.11), NS-SQL01 (10.40.40.10), NS-SQL02 (10.40.40.11)
Affected Network Segment	Application VLAN → Database VLAN
Affected Service / Port	TCP/135, TCP/1434, TCP/3389 (in addition to required TCP/1433)
Affected Technology	Internal firewall policy
Description	In addition to the required TCP/1433 (MSSQL) path, the Application VLAN is permitted broader reachability to the Database VLAN, including RPC endpoint mapper (TCP/135), the legacy SQL Server browser service (UDP/1434), and RDP (TCP/3389) — none of which the application tier requires.
Technical Impact	The additional permitted ports provide unnecessary interaction surface with the database tier beyond the application's functional requirement, including a remote administrative protocol (RDP).
Business Impact	Widens the practical blast radius of an Application VLAN compromise into additional interaction paths with the Database VLAN.
Safe Proof of Concept (Summary)	*A fictional port sweep from an Application VLAN test host confirmed reachability to TCP/135, UDP/1434, and TCP/3389 on the database hosts in addition to the required TCP/1433. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-024
Expected vs. Observed (Fictional)	Expected: Application VLAN to Database VLAN reachability should be scoped strictly to TCP/1433, with all other ports denied. // Observed: Additional ports beyond the functional requirement were permitted between the two zones.
Root Cause	The original firewall rule set was built using a broader application-layer object rather than a strict port-scoped rule.
Security Risk	Unnecessary lateral interaction surface between the application tier and the database tier.
Recommendation	Scope the Application VLAN-to-Database VLAN firewall rule strictly to TCP/1433 and deny all other ports.
Management Response	*NorthStar engineering (fictional) will scope the rule within the 61-90 day window.*

Owner / Priority / Target / Status	Network Security Engineering Lead (Fictional Role) | 61-90 Days | 09 December 2026 | Remediation Planned
Retest Recommendation	*Retest by confirming only TCP/1433 remains reachable between the two zones.*

CATEGORY	RELATED FINDINGS	STATUS
Internal Network	NET-002, NET-012	**Remediation Planned**

NET-021 — Insecure Monitoring Interface Exposes Sensitive Telemetry Without Authentication	**MEDIUM**
CVSS-Style Score	6.1 (Medium) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N — Illustrative vector only
CWE	CWE-306 — Missing Authentication for Critical Function
Affected Asset(s)	NS-MON02 (10.40.30.13)
Affected Network Segment	Application VLAN
Affected Service / Port	TCP/3000 — HTTP (dashboard)
Affected Technology	Monitoring dashboard application
Description	The monitoring dashboard on NS-MON02 is reachable over plain HTTP on TCP/3000 without authentication configured, exposing infrastructure and application telemetry — including, in several dashboards, internal hostnames, service topology, and error-rate detail — to any host that can reach the Application VLAN.
Technical Impact	Any internal host can view detailed infrastructure telemetry without authenticating, aiding reconnaissance of the internal environment.
Business Impact	Detailed operational visibility into NorthStar's infrastructure is available to any internal actor, including a low-privileged compromised host.
Safe Proof of Concept (Summary)	*A fictional test request to the dashboard returned full telemetry views with no authentication prompt. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-025
Expected vs. Observed (Fictional)	Expected: The monitoring dashboard should require authentication (SSO-integrated where possible) before displaying any telemetry. // Observed: The dashboard was fully accessible with no authentication configured.
Root Cause	Default authentication settings were left disabled during initial deployment.
Security Risk	Unauthenticated disclosure of internal infrastructure telemetry to any internal network position.
Recommendation	Enable authentication on the monitoring dashboard, integrated with NorthStar's SSO provider where supported.
Management Response	*NorthStar engineering (fictional) will enable authentication within the 61-90 day window.*
Owner / Priority / Target / Status	Infrastructure Operations Lead (Fictional Role) | 61-90 Days | 09 December 2026 | Remediation Planned
Retest Recommendation	*Retest by confirming the dashboard requires authentication before displaying telemetry.*

CATEGORY	RELATED FINDINGS	STATUS
Internal Network	NET-025	**Remediation Planned**

NET-022 — Weak Internal TLS Configuration on Internal API Server	MEDIUM
CVSS-Style Score	5.0 (Medium) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N — Illustrative vector only
CWE	CWE-295 — Improper Certificate Validation
Affected Asset(s)	NS-API01 (10.40.30.11)
Affected Network Segment	Application VLAN
Affected Service / Port	TCP/8443 — HTTPS
Affected Technology	Internal API TLS configuration
Description	NS-API01 presents a self-signed certificate for its internal API endpoint, and internal client integrations observed during testing were configured to accept it without validation (certificate pinning or CA validation disabled), rather than relying on NorthStar's internal PKI (NS-PKI01).
Technical Impact	An attacker positioned on the Application VLAN could present a spoofed certificate and intercept traffic to the internal API without detection, since clients do not validate the certificate.
Business Impact	Undermines confidentiality and integrity assurances for internal API traffic carrying core banking integration data.
Safe Proof of Concept (Summary)	*A fictional interception test confirmed a client integration accepted a substituted self-signed certificate without validation error. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-026
Expected vs. Observed (Fictional)	Expected: NS-API01 should present a certificate issued by NS-PKI01 (internal CA), and client integrations should validate the certificate chain rather than disabling validation. // Observed: A self-signed certificate was presented and accepted without validation by the tested client integration.
Root Cause	The API server was deployed with a self-signed certificate as a temporary measure during initial rollout, and certificate validation was disabled client-side to avoid trust errors, with neither ever revisited.
Security Risk	Internal API traffic is susceptible to interception without detection due to disabled certificate validation.
Recommendation	Issue NS-API01 a certificate from the internal PKI and re-enable certificate validation on all client integrations.
Management Response	*NorthStar engineering (fictional) will complete the certificate reissuance within the 61-90 day window.*
Owner / Priority / Target / Status	Backend/API Engineering Lead (Fictional Role) | 61-90 Days | 09 December 2026 | Remediation Planned
Retest Recommendation	*Retest by confirming a PKI-issued certificate is presented and client integrations enforce validation.*

CATEGORY	RELATED FINDINGS	STATUS
Internal Network	NET-014, NET-036	**Remediation Planned**

NET-023 — Kerberos Configuration Weakness — Unconstrained Delegation Enabled on Legacy Application Server	MEDIUM

CVSS-Style Score	6.7 (Medium) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N — Illustrative vector only
CWE	CWE-269 — Improper Privilege Management
Affected Asset(s)	NS-APPSRV01 (10.40.20.11)
Affected Network Segment	Server VLAN
Affected Service / Port	TCP/UDP 88 — Kerberos
Affected Technology	Active Directory Kerberos delegation configuration
Description	The computer account for NS-APPSRV01 is configured for unconstrained Kerberos delegation, a legacy setting that allows the server to cache and reuse the full Kerberos ticket-granting ticket (TGT) of any user who authenticates to it — including, potentially, a domain administrator performing routine maintenance.
Technical Impact	An attacker who compromises NS-APPSRV01 can extract cached TGTs for any user who has authenticated to it, potentially including privileged accounts, and impersonate them domain-wide.
Business Impact	If a privileged account happens to authenticate to this server for routine administration, its full domain rights become available to an attacker who has compromised the server.
Safe Proof of Concept (Summary)	*A fictional review of the NS-APPSRV01 computer account confirmed the unconstrained delegation flag (TRUSTED_FOR_DELEGATION) was set. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-027
Expected vs. Observed (Fictional)	Expected: Unconstrained delegation should not be used; servers requiring delegation should use constrained or resource-based constrained delegation scoped to specific target services. // Observed: NS-APPSRV01's computer account had unconstrained delegation enabled.
Root Cause	The setting was applied years ago to resolve a double-hop authentication issue for the legacy application and was never revisited following the availability of constrained delegation models.
Security Risk	Compromise of a single legacy server could expose the domain-wide privileges of any administrator who authenticates to it.
Recommendation	Migrate NS-APPSRV01 to constrained or resource-based constrained delegation scoped to the specific services it requires, removing the unconstrained delegation flag.
Management Response	*NorthStar engineering (fictional) will complete the delegation model migration within the 61-90 day window.*
Owner / Priority / Target / Status	Active Directory Engineering Lead (Fictional Role) | 61-90 Days | 09 December 2026 | Remediation Planned
Retest Recommendation	*Retest by confirming the unconstrained delegation flag is removed and constrained delegation is correctly scoped.*

CATEGORY	RELATED FINDINGS	STATUS
Active Directory	NET-003, NET-013, NET-024	**Remediation Planned**

NET-024 — Excessive Privilege Assignment — Standard Support Accounts Present in Domain Admins Group

MEDIUM

CVSS-Style Score	6.5 (Medium) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N — Illustrative vector only

CWE	CWE-269 — Improper Privilege Management
Affected Asset(s)	NS-DC01 (10.40.50.10)
Affected Network Segment	Identity / AD VLAN
Affected Service / Port	N/A — directory group membership
Affected Technology	Active Directory privileged group membership
Description	The Domain Admins group in the NORTHSTAR domain contains several fictional individual accounts used for day-to-day application-support work, in addition to the small number of accounts reserved for Tier-0 administrative activity, rather than following a tiered administration model.
Technical Impact	Every account in Domain Admins represents a full domain-compromise path if phished or otherwise compromised, and a larger membership proportionally increases that exposure.
Business Impact	Routine day-to-day application-support activity is being performed using accounts with unnecessary full domain-administrative privilege, disproportionate to the task.
Safe Proof of Concept (Summary)	*A fictional enumeration of Domain Admins membership identified several accounts whose day-to-day activity (per interview) did not require Tier-0 privilege. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-028
Expected vs. Observed (Fictional)	Expected: Domain Admins should contain only the minimum accounts required for genuine Tier-0 activity, with day-to-day work performed using appropriately scoped delegated permissions. // Observed: Domain Admins membership included several accounts used for routine application-support tasks not requiring Tier-0 privilege.
Root Cause	Domain Admins membership has historically been granted as a convenient way to resolve permission issues rather than through a formal tiered-administration and delegation model.
Security Risk	An unnecessarily large population of full domain-compromise-equivalent accounts increases the likelihood that a routine phishing or credential-reuse incident escalates to full domain compromise.
Recommendation	Reduce Domain Admins membership to the minimum required Tier-0 accounts and implement delegated permissions for day-to-day application-support activity.
Management Response	*NorthStar engineering (fictional) will complete the membership review and delegation redesign within the 61-90 day window.*
Owner / Priority / Target / Status	Active Directory Engineering Lead (Fictional Role) | 61-90 Days | 09 December 2026 | Remediation Planned
Retest Recommendation	*Retest by re-enumerating Domain Admins membership and confirming it is limited to genuine Tier-0 accounts.*

CATEGORY	RELATED FINDINGS	STATUS
Active Directory	NET-003, NET-007, NET-026, NET-040	**Remediation Planned**

NET-025 — Weak Password Policy Permits Short, Non-Complex Domain Passwords

MEDIUM

CVSS-Style Score	5.4 (Medium) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N — Illustrative vector only
CWE	CWE-521 — Weak Password Requirements
Affected Asset(s)	NS-DC01 (10.40.50.10), NS-DC02 (10.40.50.11)
Affected Network Segment	Identity / AD VLAN

Affected Service / Port	N/A — domain password policy
Affected Technology	Active Directory Default Domain Policy
Description	The domain's default password policy permits an 8-character minimum length with standard complexity, and does not enforce a banned-password list against commonly breached or predictable patterns, falling short of current guidance for organizations of NorthStar's risk profile.
Technical Impact	Shorter, non-screened passwords are more susceptible to offline cracking (in combination with NET-013) and online password-spray attacks.
Business Impact	Weak password policy compounds the risk of several other findings in this report that depend on password guessability or crackability.
Safe Proof of Concept (Summary)	*A fictional review of the Default Domain Policy confirmed an 8-character minimum length with no banned-password list configured. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-029
Expected vs. Observed (Fictional)	Expected: A minimum of 12-14 characters with banned-password-list screening against known breached and predictable patterns, consistent with current password-policy guidance. // Observed: An 8-character minimum with standard complexity and no banned-password screening was in effect.
Root Cause	The Default Domain Policy has not been updated since initial domain deployment and predates NorthStar's adoption of current password-policy guidance.
Security Risk	Weaker resistance to offline cracking and online password-spray attacks across the domain.
Recommendation	Raise the minimum password length to 12-14 characters and deploy banned-password-list screening (e.g., an Azure AD Password Protection-style tool or equivalent) against the on-premises domain.
Management Response	*NorthStar engineering (fictional) will update the domain password policy within the 61-90 day window.*
Owner / Priority / Target / Status	Active Directory Engineering Lead (Fictional Role) | 61-90 Days | 09 December 2026 | Remediation Planned
Retest Recommendation	*Retest by confirming the updated policy is enforced and banned-password screening is active.*

CATEGORY	RELATED FINDINGS	STATUS
Active Directory	NET-001, NET-013	**Remediation Planned**

NET-026 — Insecure Administrative Pathway — Helpdesk Staff Granted Direct RDP to Domain Controllers

MEDIUM

CVSS-Style Score	6.3 (Medium) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N — Illustrative vector only
CWE	CWE-284 — Improper Access Control
Affected Asset(s)	NS-DC01 (10.40.50.10), NS-DC02 (10.40.50.11)
Affected Network Segment	Identity / AD VLAN
Affected Service / Port	TCP/3389 — RDP
Affected Technology	Domain controller logon rights configuration

Description	A small number of Tier-1 helpdesk accounts hold direct interactive RDP logon rights on both domain controllers for routine password-reset assistance, rather than using a delegated, non-interactive administrative tool scoped to that specific task.
Technical Impact	Any Tier-1 helpdesk account with this logon right, if compromised, provides an interactive session directly on a domain controller.
Business Impact	Extends domain-controller-level exposure to a broader, higher-turnover staff population than intended for Tier-0 infrastructure.
Safe Proof of Concept (Summary)	*A fictional review of domain controller logon rights confirmed several Tier-1 helpdesk accounts held direct RDP access. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-030
Expected vs. Observed (Fictional)	Expected: Password-reset and similar Tier-1 tasks should be performed through a delegated administrative tool (e.g., a scoped self-service or helpdesk console) rather than direct interactive logon to a domain controller. // Observed: Several helpdesk accounts held direct RDP logon rights to both domain controllers.
Root Cause	Direct RDP access was granted as an interim measure when the delegated password-reset tool was first introduced and was never revoked once the tool was fully adopted.
Security Risk	Extends the population of accounts capable of interactive domain-controller access beyond the intended Tier-0 administrative group.
Recommendation	Revoke direct RDP logon rights on domain controllers for Tier-1 helpdesk accounts and confirm password-reset tasks are performed exclusively through the delegated tool.
Management Response	*NorthStar engineering (fictional) will revoke the affected logon rights within the 61-90 day window.*
Owner / Priority / Target / Status	Active Directory Engineering Lead (Fictional Role) | 61-90 Days | 09 December 2026 | Remediation Planned
Retest Recommendation	*Retest by confirming the affected accounts can no longer establish an RDP session to either domain controller.*

CATEGORY	RELATED FINDINGS	STATUS
Active Directory	NET-007, NET-010, NET-024	**Remediation Planned**

NET-027 — Weak Corporate Wireless Configuration — Shared PSK Fallback Available Alongside 802.1X

MEDIUM

CVSS-Style Score	4.8 (Medium) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N — Illustrative vector only
CWE	CWE-521 — Weak Password Requirements
Affected Asset(s)	NS-WLC01 (172.20.10.5)
Affected Network Segment	Wireless — Corporate SSID
Affected Service / Port	N/A — wireless authentication configuration
Affected Technology	WLC SSID authentication configuration
Description	In addition to the primary 802.1X/PEAP-MSCHAPv2 authentication method, the Corporate SSID retains a legacy shared-PSK fallback method (originally provisioned for a small population of IoT-style devices that cannot perform 802.1X), and the shared PSK has not been rotated in over two years.

Technical Impact	Any device retaining the legacy PSK — including a departed employee's personal device or a decommissioned IoT device — can rejoin the Corporate SSID without triggering an access-revocation event tied to individual credentials.
Business Impact	Weakens the assurance that only currently authorized devices are connected to the corporate wireless network.
Safe Proof of Concept (Summary)	*A fictional review of NS-WLC01's SSID configuration confirmed the legacy PSK fallback method remained active with a rotation date exceeding two years. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-031
Expected vs. Observed (Fictional)	Expected: IoT-style devices unable to perform 802.1X should be isolated to a dedicated, tightly-scoped SSID/VLAN with a regularly rotated PSK, separate from the primary Corporate SSID. // Observed: The legacy PSK fallback shared the Corporate SSID's broadcast and VLAN with 802.1X-authenticated devices, and had not been rotated in over two years.
Root Cause	The IoT exception was added to the existing Corporate SSID for convenience rather than being placed on a dedicated segment when first introduced.
Security Risk	Reduces the assurance that Corporate SSID access is limited to currently authorized, individually identifiable devices.
Recommendation	Migrate IoT-style devices requiring PSK authentication to a dedicated, isolated SSID/VLAN and rotate the legacy PSK immediately.
Management Response	*NorthStar engineering (fictional) will rotate the PSK immediately and complete IoT SSID migration within the 61-90 day window.*
Owner / Priority / Target / Status	Wireless Infrastructure Lead (Fictional Role) | 61-90 Days | 09 December 2026 | Remediation Planned
Retest Recommendation	*Retest by confirming the Corporate SSID no longer offers a PSK fallback method.*

CATEGORY	RELATED FINDINGS	STATUS
Wireless	NET-011	**Remediation Planned**

22 LOW FINDINGS

The following 9 fictional Low-severity findings are hardening opportunities recommended for the 90+ day window of the illustrative roadmap.

NET-028 — Guest Wireless Network Isolation Weakness Permits Limited Reachability to Printer VLAN	LOW
CVSS-Style Score	3.4 (Low) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N — Illustrative vector only
CWE	CWE-923 — Improper Restriction of Communication Channel to Intended Endpoints
Affected Asset(s)	NS-PRINT-FL3 (10.40.10.90)
Affected Network Segment	Wireless — Guest SSID → User Workstation VLAN (printer subnet)
Affected Service / Port	TCP/9100, TCP/631 — Printing
Affected Technology	Guest SSID client-isolation configuration
Description	Guest SSID client isolation correctly blocks guest-to-guest and guest-to-corporate traffic, but an exception rule intended only for a guest-accessible print-release kiosk inadvertently permits guest clients to reach the general User VLAN printer subnet, including several non-kiosk departmental printers.
Technical Impact	Guest clients can submit print jobs or query status on departmental printers beyond the intended kiosk, and in principle could access printer web-management interfaces if not separately secured.
Business Impact	Minor — limited to printer-subnet interaction with no path to core internal systems, but inconsistent with the intended isolation scope.
Safe Proof of Concept (Summary)	*A fictional test guest client reached NS-PRINT-FL3 and submitted a benign, non-disruptive test query confirming reachability. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-032
Expected vs. Observed (Fictional)	Expected: The guest exception rule should be scoped only to the specific kiosk device, not the general printer subnet. // Observed: The exception rule matched the broader printer subnet rather than the single kiosk device address.
Root Cause	The exception rule was written against a subnet object rather than a host object during initial guest-network configuration.
Recommendation	Scope the guest exception rule to the specific kiosk device address only.
Management Response	*NorthStar engineering (fictional) will narrow the exception rule during the next wireless maintenance window.*
Owner / Priority / Target / Status	Wireless Infrastructure Lead (Fictional Role) | 90+ Days | 31 January 2027 | Remediation Planned
Retest Recommendation	*Retest by confirming guest clients can reach only the designated kiosk device.*

CATEGORY	RELATED FINDINGS	STATUS
Wireless	NET-027	**Remediation Planned**

NET-029 — Insecure SNMP Configuration — SNMPv2c Enabled Alongside SNMPv3 on Distribution Switches	LOW
CVSS-Style Score	3.1 (Low) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N — Illustrative vector only
CWE	CWE-16 — Configuration
Affected Asset(s)	NS-DSW01 (172.20.10.2), NS-DSW02 (172.20.10.3)
Affected Network Segment	Management VLAN
Affected Service / Port	UDP/161 — SNMP
Affected Technology	SNMP protocol configuration
Description	SNMPv2c remains enabled with a low-entropy community string on both distribution switches alongside SNMPv3, presenting the same category of exposure as NET-009 at a smaller scale (distribution- rather than core-layer, and reachable only from within the Management VLAN itself given other findings' remediation).
Technical Impact	Read-only device information disclosure to any actor with Management VLAN reachability.
Business Impact	Minor incremental reconnaissance value beyond what NET-009 already discloses at the core layer.
Safe Proof of Concept (Summary)	*A fictional SNMPv2c walk against both distribution switches succeeded using the same community string pattern identified in NET-009. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-033
Expected vs. Observed (Fictional)	Expected: SNMPv1/v2c disabled in favor of SNMPv3 authPriv, consistent with NET-009's recommendation. // Observed: SNMPv2c remained enabled and responsive on both distribution switches.
Root Cause	Same root cause as NET-009 — incomplete SNMPv3 migration.
Recommendation	Remediate alongside NET-009 as part of the same SNMPv3 migration project.
Management Response	*NorthStar engineering (fictional) will include these devices in the NET-009 remediation scope.*
Owner / Priority / Target / Status	Network Operations Lead (Fictional Role) | 90+ Days | 31 January 2027 | Remediation Planned
Retest Recommendation	*Retest alongside NET-009.*

CATEGORY	RELATED FINDINGS	STATUS
Network Devices	NET-009	**Remediation Planned**

NET-030 — Outdated Device Firmware on Wireless LAN Controller	LOW
CVSS-Style Score	3.7 (Low) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N — Illustrative vector only
CWE	CWE-1104 — Use of Unmaintained Third Party Components
Affected Asset(s)	NS-WLC01 (172.20.10.5)
Affected Network Segment	Management VLAN

Affected Service / Port	N/A — firmware version
Affected Technology	Wireless LAN Controller firmware
Description	NS-WLC01 is running a fictional firmware version two release trains behind the vendor's current recommended release, missing several fictional stability and security fixes published in the interim.
Technical Impact	The device is missing fixes for issues addressed in later releases, though no actively exploited fictional vulnerability was confirmed applicable during this assessment.
Business Impact	Increases exposure surface over time as the firmware gap widens without a deliberate upgrade cadence.
Safe Proof of Concept (Summary)	*A fictional version check confirmed the device firmware was two release trains behind current. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-034
Expected vs. Observed (Fictional)	Expected: Network infrastructure firmware should be kept current per a defined upgrade cadence and vendor security-bulletin review process. // Observed: Firmware was two release trains behind current with no scheduled upgrade identified.
Root Cause	No formal firmware-currency review cadence exists for wireless infrastructure.
Recommendation	Establish a firmware upgrade cadence for network infrastructure devices, prioritizing NS-WLC01 for near-term upgrade.
Management Response	*NorthStar engineering (fictional) will schedule the upgrade within the 90+ day window.*
Owner / Priority / Target / Status	Wireless Infrastructure Lead (Fictional Role) | 90+ Days | 31 January 2027 | Remediation Planned
Retest Recommendation	*Retest by confirming the device is running a current, vendor-recommended firmware release.*

CATEGORY	RELATED FINDINGS	STATUS
Network Devices	NET-046	**Remediation Planned**

NET-031 — Configuration Backup Exposure — Unencrypted Device Configurations Stored on Shared Drive

LOW

CVSS-Style Score	3.9 (Low) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N — Illustrative vector only
CWE	CWE-312 — Cleartext Storage of Sensitive Information
Affected Asset(s)	NS-FILE01 (10.40.20.10)
Affected Network Segment	Server VLAN
Affected Service / Port	TCP/445 — SMB
Affected Technology	Network device configuration backup process
Description	NS-NMS01's automated configuration-backup job writes plaintext device configuration files — including, for several devices, locally-defined enable-secret hashes and SNMP community strings — to a general IT share on NS-FILE01 rather than a restricted, access-controlled backup location.
Technical Impact	Any user with read access to the general IT share (a broader population than intended) can review device configuration detail, including hashed secrets suitable for offline cracking attempts.
Business Impact	Provides an alternate path to sensitive device configuration detail beyond the live devices themselves.

Safe Proof of Concept (Summary)	*A fictional review of the general IT share located device configuration backup files containing hashed enable secrets. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-035
Expected vs. Observed (Fictional)	Expected: Configuration backups should be stored in a restricted location accessible only to network engineering staff, ideally with secrets redacted or separately encrypted. // Observed: Configuration backups were stored on a broadly-accessible general IT share.
Root Cause	The backup job's output path was never moved from its original convenience location to a properly restricted share.
Recommendation	Relocate configuration backups to a restricted share limited to network engineering staff and evaluate secret redaction in the backup process.
Management Response	*NorthStar engineering (fictional) will relocate the backup output within the 90+ day window.*
Owner / Priority / Target / Status	Network Operations Lead (Fictional Role) | 90+ Days | 31 January 2027 | Remediation Planned
Retest Recommendation	*Retest by confirming configuration backups are no longer present on the general IT share.*

CATEGORY	RELATED FINDINGS	STATUS
Network Devices	NET-009	**Remediation Planned**

NET-032 — Weak Network-Device ACL Permits Broader Source Range Than Required for SSH Management

LOW

CVSS-Style Score	3.3 (Low) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N — Illustrative vector only
CWE	CWE-284 — Improper Access Control
Affected Asset(s)	NS-DSW01 (172.20.10.2), NS-DSW02 (172.20.10.3)
Affected Network Segment	Management VLAN
Affected Service / Port	TCP/22 — SSH
Affected Technology	Network device management-plane ACL
Description	The SSH management ACL on both distribution switches permits the entire Management VLAN as a source, rather than the smaller set of specific jump-host and NMS addresses that actually require SSH access.
Technical Impact	Any host on the Management VLAN — a broader population than the intended jump-host/NMS set — can attempt SSH authentication against the distribution switches.
Business Impact	Minor incremental exposure given the Management VLAN is already a restricted-access segment; addressed as defense-in-depth.
Safe Proof of Concept (Summary)	*A fictional review of the ACL configuration confirmed the full Management VLAN subnet was permitted rather than specific host addresses. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-036
Expected vs. Observed (Fictional)	Expected: SSH management access should be scoped to specific jump-host and NMS addresses rather than the full Management VLAN subnet. // Observed: The full Management VLAN subnet was permitted as an SSH source.
Root Cause	The ACL was written using the VLAN subnet object for simplicity rather than a scoped host-group object.

Recommendation	Narrow the SSH management ACL to specific jump-host and NMS addresses.
Management Response	*NorthStar engineering (fictional) will narrow the ACL within the 90+ day window.*
Owner / Priority / Target / Status	Network Operations Lead (Fictional Role) | 90+ Days | 31 January 2027 | Remediation Planned
Retest Recommendation	*Retest by confirming SSH access from non-designated Management VLAN hosts is denied.*

CATEGORY	RELATED FINDINGS	STATUS
Network Devices	NET-004	**Remediation Planned**

NET-033 — Excessive Domain Information Disclosure via Unauthenticated LDAP Enumeration

LOW

CVSS-Style Score	3.6 (Low) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N — Illustrative vector only
CWE	CWE-200 — Exposure of Sensitive Information to an Unauthorized Actor
Affected Asset(s)	NS-DC01 (10.40.50.10)
Affected Network Segment	Identity / AD VLAN
Affected Service / Port	TCP/389 — LDAP
Affected Technology	Active Directory anonymous LDAP bind configuration
Description	NS-DC01 permits a limited anonymous LDAP bind that returns the directory's RootDSE and schema-naming-context information, which — while not itself sensitive user data — assists an attacker in confirming domain structure and functional level without any credential.
Technical Impact	An unauthenticated actor with network reachability can confirm the domain's naming context, functional level, and site topology.
Business Impact	Minor reconnaissance value; no user or credential data is exposed via this specific path.
Safe Proof of Concept (Summary)	*A fictional anonymous LDAP query returned RootDSE attributes confirming domain naming context and functional level. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-037
Expected vs. Observed (Fictional)	Expected: Anonymous LDAP responses should be minimized where organizational policy requires it, accepting that some RootDSE disclosure is a default AD behavior. // Observed: RootDSE and naming-context information was returned to an unauthenticated query.
Root Cause	Default Active Directory behavior; not a misconfiguration introduced by NorthStar, but flagged as a hardening opportunity given the broader reconnaissance value it adds when combined with other findings.
Recommendation	Treat as a low-priority hardening item; ensure network segmentation (addressed elsewhere) limits who can reach TCP/389 at all.
Management Response	*NorthStar engineering (fictional) will evaluate anonymous-bind restriction options as a longer-term hardening item.*
Owner / Priority / Target / Status	Active Directory Engineering Lead (Fictional Role) | 90+ Days | 31 January 2027 | Remediation Planned
Retest Recommendation	*Not required as a standalone retest; addressed as part of broader AD hardening review.*

CATEGORY	RELATED FINDINGS	STATUS
Active Directory	NET-006	Remediation Planned

NET-034 — SYSVOL-Related Sensitive Configuration Reference in Legacy Logon Script

LOW

CVSS-Style Score	2.6 (Low) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N — Illustrative vector only
CWE	CWE-200 — Exposure of Sensitive Information to an Unauthorized Actor
Affected Asset(s)	NS-DC01 (10.40.50.10)
Affected Network Segment	Identity / AD VLAN (SYSVOL)
Affected Service / Port	TCP/445 — SMB
Affected Technology	Legacy domain logon script
Description	A legacy logon script retained in SYSVOL references a deprecated credential-file path on a decommissioned fictional server, which — while the referenced file no longer exists — indicates a historical pattern of storing credential material in a network-accessible location and represents housekeeping debt worth resolving.
Technical Impact	No currently exploitable condition — the referenced path does not resolve — but indicates the pattern that produced NET-003 was not isolated.
Business Impact	Minor; primarily a signal to audit for any other similar historical artifacts during the NET-003 remediation.
Safe Proof of Concept (Summary)	*A fictional review of SYSVOL logon scripts identified the stale reference during the same audit pass conducted for NET-003. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-038
Expected vs. Observed (Fictional)	Expected: Logon scripts should not reference credential file paths at all, current or historical. // Observed: A stale, non-resolving reference to a deprecated credential file path was present.
Root Cause	Same historical pattern identified in NET-003 — credential material was historically managed via network-accessible files rather than a proper secrets-management approach.
Recommendation	Remove the stale script reference and complete the broader SYSVOL credential-artifact audit initiated for NET-003.
Management Response	*NorthStar engineering (fictional) will address this as part of the NET-003 remediation.*
Owner / Priority / Target / Status	Active Directory Engineering Lead (Fictional Role) | 90+ Days | 31 January 2027 | Remediation Planned
Retest Recommendation	*Retest alongside NET-003.*

CATEGORY	RELATED FINDINGS	STATUS
Active Directory	NET-003	Remediation Planned

NET-035 — Overly Permissive VPN Trust Allows Split-Tunnel Access to Sensitive On-Prem Resources

LOW

CVSS-Style Score	3.8 (Low) (Illustrative CVSS v3.1-inspired score)

CVSS Vector (Illustrative)	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N — Illustrative vector only
CWE	CWE-284 — Improper Access Control
Affected Asset(s)	NS-VPNGW01 (10.40.0.10)
Affected Network Segment	External Perimeter / DMZ
Affected Service / Port	N/A — VPN client policy
Affected Technology	VPN client split-tunnel configuration
Description	The default VPN client profile enables split tunneling for all users rather than only the subset of roles with a documented business need, meaning a connected client's local network (e.g., an untrusted home or public network) has simultaneous routing alongside the authenticated tunnel to internal resources.
Technical Impact	A compromised local network segment on a split-tunnel client's untrusted side could, in principle, be used to pivot toward the client's simultaneously-active internal tunnel session.
Business Impact	Marginal increase in risk from untrusted client-side networks given the broad default application of split tunneling.
Safe Proof of Concept (Summary)	*A fictional review of the default VPN client profile confirmed split tunneling was enabled for all roles by default. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-039
Expected vs. Observed (Fictional)	Expected: Split tunneling should be disabled by default, with exceptions granted only to specific roles with a documented need. // Observed: Split tunneling was enabled by default for the entire user population.
Root Cause	The default profile was configured for broad convenience during initial VPN rollout without a role-based exception review.
Recommendation	Disable split tunneling by default and grant it only to specific roles with a documented business justification.
Management Response	*NorthStar engineering (fictional) will update the default profile within the 90+ day window.*
Owner / Priority / Target / Status	Network Security Engineering Lead (Fictional Role) | 90+ Days | 31 January 2027 | Remediation Planned
Retest Recommendation	*Retest by confirming the default client profile no longer enables split tunneling.*

CATEGORY	RELATED FINDINGS	STATUS
Cloud / Hybrid	NET-001, NET-008	**Remediation Planned**

NET-036 — Weak Hybrid Segmentation Between On-Prem Identity Sync Server and Cloud Management Path

LOW

CVSS-Style Score	3.5 (Low) (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N — Illustrative vector only
CWE	CWE-284 — Improper Access Control
Affected Asset(s)	NS-AADCONNECT01 (10.40.20.16), NS-CLOUDMGMT01 (10.50.0.11)
Affected Network Segment	Server VLAN → Cloud / Hybrid Connectivity
Affected Service / Port	TCP/443 — HTTPS
Affected Technology	Hybrid identity synchronization network path

Description	NS-AADCONNECT01, the hybrid identity synchronization server, has broader-than-required outbound reachability to the fictional cloud management path via NS-CLOUDMGMT01, including several cloud-management API endpoints unrelated to its actual identity-synchronization function.
Technical Impact	Compromise of NS-AADCONNECT01 would provide broader reachability into the cloud management path than its function requires, widening the potential blast radius.
Business Impact	Marginal increase in hybrid-environment exposure if this specific server were compromised via another finding in this report.
Safe Proof of Concept (Summary)	*A fictional outbound connectivity review from NS-AADCONNECT01 confirmed reachability to cloud management API endpoints beyond the identity-sync function. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-040
Expected vs. Observed (Fictional)	Expected: Outbound reachability from the identity sync server should be scoped strictly to the specific endpoints its synchronization function requires. // Observed: Broader reachability to unrelated cloud management API endpoints was observed.
Root Cause	The outbound firewall rule for this server was written broadly during initial hybrid identity rollout and never subsequently scoped down.
Recommendation	Scope NS-AADCONNECT01's outbound reachability strictly to the required identity-synchronization endpoints.
Management Response	*NorthStar engineering (fictional) will scope the outbound rule within the 90+ day window.*
Owner / Priority / Target / Status	Cloud & Hybrid Identity Lead (Fictional Role) | 90+ Days | 31 January 2027 | Remediation Planned
Retest Recommendation	*Retest by confirming outbound reachability is limited to the documented identity-sync endpoints.*

CATEGORY	RELATED FINDINGS	STATUS
Cloud / Hybrid	NET-022	**Remediation Planned**

23 INFORMATIONAL FINDINGS

The following 10 fictional Informational observations carry no direct exploitation path — several document positive security controls already in place — and are recommended for the ongoing network-security governance and defense-in-depth backlog.

NET-037 — Positive Observation — Next-Generation Firewall Enforces Application-Aware Policy at External Perimeter	INFORMATIONAL
CVSS-Style Score	Informational — no CVSS score applicable (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	N/A
CWE	N/A — positive control observation
Affected Asset(s)	NS-FW-EXT01 (10.40.0.1)
Affected Network Segment	External Perimeter / DMZ
Affected Service / Port	N/A
Affected Technology	Next-Generation Firewall policy engine
Description	NS-FW-EXT01 consistently enforces application-aware policy (rather than port-based rules alone) across the external perimeter rule base, correctly blocking several fictional out-of-policy protocol-evasion attempts made during testing.
Technical Impact	None — positive observation.
Business Impact	None — positive observation.
Safe Proof of Concept (Summary)	*Fictional protocol-evasion attempts against the external perimeter were consistently blocked by application-aware inspection. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-041
Expected vs. Observed (Fictional)	Expected: Application-aware filtering should be enforced at the external perimeter. // Observed: Consistently enforced during testing.
Root Cause	N/A — positive control.
Recommendation	No action required; continue to validate this control during future assessments and firewall policy changes.
Management Response	*Acknowledged; NorthStar engineering (fictional) will maintain this control.*
Owner / Priority / Target / Status	Network Security Engineering Lead (Fictional Role) | N/A — Informational | N/A | Observation Only
Retest Recommendation	*No retest required; re-verify opportunistically in future assessments.*

CATEGORY	RELATED FINDINGS	STATUS
External Network	None	**Observation Only**

NET-038 — Positive Observation — Centralized Logging and SIEM Collection Implemented Across Core Infrastructure	INFORMATIONAL
CVSS-Style Score	Informational — no CVSS score applicable (Illustrative CVSS v3.1-inspired score)

CVSS Vector (Illustrative)	N/A
CWE	N/A — positive control observation
Affected Asset(s)	NS-SIEM01 (10.40.30.12)
Affected Network Segment	Application VLAN
Affected Service / Port	N/A
Affected Technology	Centralized log aggregation
Description	Windows Security event logs, firewall logs, and VPN authentication logs are consistently forwarded to NS-SIEM01, providing a meaningful detective baseline that several findings in this report reference as a retest/monitoring resource.
Technical Impact	None — positive observation.
Business Impact	None — positive observation.
Safe Proof of Concept (Summary)	*Fictional test authentication events and firewall denies generated during testing were confirmed present in NS-SIEM01 within an expected ingestion window. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-042
Expected vs. Observed (Fictional)	Expected: Centralized logging should cover core infrastructure with timely ingestion. // Observed: Confirmed present and timely for the sampled log sources.
Root Cause	N/A — positive control.
Recommendation	Expand detection content (see NET-042) to make fuller use of this logging foundation.
Management Response	*Acknowledged; NorthStar engineering (fictional) will continue expanding SIEM detection coverage.*
Owner / Priority / Target / Status	Network Security Engineering Lead (Fictional Role) | N/A — Informational | N/A | Observation Only
Retest Recommendation	*No retest required.*

CATEGORY	RELATED FINDINGS	STATUS
Internal Network	NET-042	**Observation Only**

NET-039 — Positive Observation — Multi-Factor Authentication Enforced on Primary VPN Login Path

INFORMATIONAL

CVSS-Style Score	Informational — no CVSS score applicable (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	N/A
CWE	N/A — positive control observation
Affected Asset(s)	NS-VPNGW01 (10.40.0.10)
Affected Network Segment	External Perimeter / DMZ
Affected Service / Port	N/A
Affected Technology	VPN authentication policy
Description	The primary VPN login path (distinct from the legacy endpoint described in NET-001) correctly enforces mandatory push-based MFA for all users, with no observed bypass on this specific path.
Technical Impact	None — positive observation.
Business Impact	None — positive observation.

Safe Proof of Concept (Summary)	*Fictional test logins against the primary VPN path consistently required MFA approval before session establishment. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-043
Expected vs. Observed (Fictional)	Expected: MFA should be required on all authentication paths. // Observed: Consistently enforced on the primary path.
Root Cause	N/A — positive control.
Recommendation	Extend this same enforcement to the legacy endpoint identified in NET-001.
Management Response	*Acknowledged.*
Owner / Priority / Target / Status	Network Security Engineering Lead (Fictional Role) | N/A — Informational | N/A | Observation Only
Retest Recommendation	*No retest required.*

CATEGORY	RELATED FINDINGS	STATUS
External Network	NET-001	**Observation Only**

NET-040 — Recommendation — Adopt Privileged Access Workstations for Tier-0 Administrative Activity

INFORMATIONAL

CVSS-Style Score	Informational — no CVSS score applicable (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	N/A
CWE	N/A — recommendation
Affected Asset(s)	NS-MGMT01 (10.40.20.12) and Tier-0 administrative accounts
Affected Network Segment	Server VLAN / Identity AD VLAN
Affected Service / Port	N/A
Affected Technology	Administrative access model
Description	Tier-0 administrative activity is currently performed from standard IT workstations rather than dedicated, hardened Privileged Access Workstations (PAWs), an architecture recommended alongside the tiered-administration remediation in NET-024.
Technical Impact	None directly — a hardening recommendation.
Business Impact	None directly — a hardening recommendation.
Safe Proof of Concept (Summary)	*N/A — architectural recommendation based on interview and configuration review. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-044
Expected vs. Observed (Fictional)	Expected: Tier-0 administrative activity should be performed exclusively from dedicated PAWs. // Observed: Currently performed from standard IT workstations.
Root Cause	N/A — architectural gap rather than a misconfiguration.
Recommendation	Design and roll out a PAW model for Tier-0 administrative accounts alongside the NET-024 tiered-administration remediation.
Management Response	*NorthStar engineering (fictional) will scope a PAW pilot as part of the broader tiered-administration initiative.*
Owner / Priority / Target / Status	Active Directory Engineering Lead (Fictional Role) | N/A — Informational | N/A | Observation Only
Retest Recommendation	*No retest required; track as a long-term architectural initiative.*

CATEGORY	RELATED FINDINGS	STATUS

Active Directory	NET-024	**Observation Only**

NET-041 — Recommendation — Formalize Network Segmentation Review Cadence

INFORMATIONAL

CVSS-Style Score	Informational — no CVSS score applicable (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	N/A
CWE	N/A — recommendation
Affected Asset(s)	NS-FWINT01 (172.20.10.10)
Affected Network Segment	All internal zones
Affected Service / Port	N/A
Affected Technology	Firewall rule governance process
Description	Several Critical/High findings in this report (NET-002, NET-010, NET-020) trace back to segmentation rules that were correct when created but drifted from policy intent over time with no periodic review catching the drift.
Technical Impact	None directly — a process recommendation.
Business Impact	None directly — a process recommendation.
Safe Proof of Concept (Summary)	*N/A — process recommendation based on the pattern observed across NET-002, NET-010, and NET-020. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-045
Expected vs. Observed (Fictional)	Expected: A periodic (e.g., quarterly) segmentation review validating live traffic flows against the intended policy matrix. // Observed: No such recurring review process was identified.
Root Cause	N/A — process gap.
Recommendation	Establish a quarterly segmentation review comparing live flow data against the segmentation matrix in Appendix E.
Management Response	*NorthStar engineering (fictional) will formalize this review as part of the broader remediation program.*
Owner / Priority / Target / Status	Network Security Engineering Lead (Fictional Role) | N/A — Informational | N/A | Observation Only
Retest Recommendation	*No retest required; track as a governance initiative.*

CATEGORY	RELATED FINDINGS	STATUS
Internal Network	NET-002, NET-010, NET-020	**Observation Only**

NET-042 — Recommendation — Expand SIEM Detection Coverage for Lateral Movement Techniques

INFORMATIONAL

CVSS-Style Score	Informational — no CVSS score applicable (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	N/A
CWE	N/A — recommendation
Affected Asset(s)	NS-SIEM01 (10.40.30.12)
Affected Network Segment	Application VLAN

Affected Service / Port	N/A
Affected Technology	SIEM detection content
Description	Building on the positive logging foundation noted in NET-038, detection content specific to the lateral-movement techniques demonstrated in this assessment (Kerberoasting event patterns, NTLM relay indicators, abnormal service-ticket volume) was not confirmed present during interview.
Technical Impact	None directly — a recommendation.
Business Impact	None directly — a recommendation.
Safe Proof of Concept (Summary)	*N/A — recommendation based on interview and the technique set exercised during this assessment. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-046
Expected vs. Observed (Fictional)	Expected: Detection content should cover the technique categories exercised during penetration testing. // Observed: Coverage for several specific techniques was not confirmed.
Root Cause	N/A — detection-engineering backlog.
Recommendation	Prioritize detection content for Kerberoasting, NTLM relay, and abnormal RDP/SMB lateral-movement patterns using this report's attack paths as test cases.
Management Response	*NorthStar engineering (fictional) will prioritize this detection content in the next SIEM content sprint.*
Owner / Priority / Target / Status	Network Security Engineering Lead (Fictional Role) | N/A — Informational | N/A | Observation Only
Retest Recommendation	*No retest required; validate via a future purple-team exercise.*

CATEGORY	RELATED FINDINGS	STATUS
Internal Network	NET-005, NET-006, NET-013, NET-038	**Observation Only**

NET-043 — Informational — Management VLAN Naming Convention Inconsistent Across Network Documentation

INFORMATIONAL

CVSS-Style Score	Informational — no CVSS score applicable (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	N/A
CWE	N/A — documentation observation
Affected Asset(s)	N/A — documentation only
Affected Network Segment	Management VLAN
Affected Service / Port	N/A
Affected Technology	Network documentation
Description	Internal network diagrams reviewed during the engagement referred to the Management VLAN using two different naming conventions across different documents, creating minor confusion during scoping and evidence cross-referencing.
Technical Impact	None — documentation observation.
Business Impact	None — documentation observation.
Safe Proof of Concept (Summary)	*N/A — documentation review observation. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-047

Expected vs. Observed (Fictional)	Expected: Consistent naming conventions across all network documentation. // Observed: Two different naming conventions observed for the same VLAN.
Root Cause	N/A — documentation drift over time.
Recommendation	Standardize VLAN naming across all network documentation as part of routine documentation hygiene.
Management Response	*Acknowledged; will be corrected during the next documentation refresh.*
Owner / Priority / Target / Status	Network Operations Lead (Fictional Role) | N/A — Informational | N/A | Observation Only
Retest Recommendation	*No retest required.*

CATEGORY	RELATED FINDINGS	STATUS
Network Devices	None	**Observation Only**

NET-044 — Informational — Legacy DNS Records Identified for Decommissioned Hosts

INFORMATIONAL

CVSS-Style Score	Informational — no CVSS score applicable (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	N/A
CWE	N/A — hygiene observation
Affected Asset(s)	NS-DNSEXT01 (10.40.0.14)
Affected Network Segment	External Perimeter / DMZ
Affected Service / Port	N/A
Affected Technology	Public DNS records
Description	The zone data recovered during NET-016 testing included several fictional DNS records referencing hosts described in interview as decommissioned, which should be removed as routine hygiene.
Technical Impact	None directly — a hygiene item.
Business Impact	None directly — a hygiene item.
Safe Proof of Concept (Summary)	*N/A — identified during the NET-016 zone review. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-020
Expected vs. Observed (Fictional)	Expected: DNS records should be removed when the corresponding host is decommissioned. // Observed: Several stale records remained in the zone.
Root Cause	N/A — decommissioning checklist gap.
Recommendation	Remove stale records and add DNS cleanup to the standard decommissioning checklist.
Management Response	*Acknowledged; will be addressed alongside NET-016 remediation.*
Owner / Priority / Target / Status	Network Security Engineering Lead (Fictional Role) | N/A — Informational | N/A | Observation Only
Retest Recommendation	*No retest required.*

CATEGORY	RELATED FINDINGS	STATUS
External Network	NET-016	**Observation Only**

NET-045 — Recommendation — Implement Network Access Control (802.1X) on Wired User

INFORMATIONAL

Ports	
CVSS-Style Score	Informational — no CVSS score applicable (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	N/A
CWE	N/A — recommendation
Affected Asset(s)	NS-DSW01 (172.20.10.2), NS-DSW02 (172.20.10.3)
Affected Network Segment	User Workstation VLAN
Affected Service / Port	N/A
Affected Technology	Wired port authentication
Description	Wired User VLAN ports do not currently require 802.1X authentication before granting network access, meaning any device physically connected to an open port (e.g., in an unoccupied office or conference room) reaches the User VLAN without identity verification.
Technical Impact	None directly — an architectural recommendation.
Business Impact	None directly — an architectural recommendation.
Safe Proof of Concept (Summary)	*N/A — architectural recommendation based on configuration review. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-048
Expected vs. Observed (Fictional)	Expected: Wired user ports should require 802.1X authentication before granting VLAN access. // Observed: No port-based authentication was required.
Root Cause	N/A — architectural gap.
Recommendation	Pilot 802.1X wired authentication on a representative floor before a phased full rollout.
Management Response	*NorthStar engineering (fictional) will scope a pilot for the next fiscal planning cycle.*
Owner / Priority / Target / Status	Network Operations Lead (Fictional Role) | N/A — Informational | N/A | Observation Only
Retest Recommendation	*No retest required; track as a long-term architectural initiative.*

CATEGORY	RELATED FINDINGS	STATUS
Internal Network	None	**Observation Only**

NET-046 — Recommendation — Establish Formal Firewall Rule Review and Recertification Process	INFORMATIONAL
CVSS-Style Score	Informational — no CVSS score applicable (Illustrative CVSS v3.1-inspired score)
CVSS Vector (Illustrative)	N/A
CWE	N/A — recommendation
Affected Asset(s)	NS-FW-EXT01 (10.40.0.1), NS-FWINT01 (172.20.10.10)
Affected Network Segment	All zones
Affected Service / Port	N/A
Affected Technology	Firewall rule governance
Description	No formal recurring recertification process exists for firewall rules on either the external or internal firewalls, consistent with the drift pattern observed in NET-002, NET-010, NET-017, and NET-020.

Technical Impact	None directly — a governance recommendation.
Business Impact	None directly — a governance recommendation.
Safe Proof of Concept (Summary)	*N/A — pattern observed across multiple findings in this assessment. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	EV-NET-049
Expected vs. Observed (Fictional)	Expected: A formal, recurring (e.g., semi-annual) firewall rule recertification process with documented business justification for every rule. // Observed: No such process was identified.
Root Cause	N/A — governance gap.
Recommendation	Establish a semi-annual firewall rule recertification process for both external and internal firewalls, requiring documented business justification for every active rule.
Management Response	*NorthStar engineering (fictional) will establish this process as part of the broader remediation program.*
Owner / Priority / Target / Status	Network Security Engineering Lead (Fictional Role) | N/A — Informational | N/A | Observation Only
Retest Recommendation	*No retest required; track as a governance initiative.*

CATEGORY	RELATED FINDINGS	STATUS
Network Devices	NET-002, NET-010, NET-017, NET-020, NET-030	**Observation Only**

24 MANAGEMENT ACTION PLAN

The table below consolidates every finding with its accountable owner, priority, target date, and current status, providing NorthStar's management team a single tracking view for this fictional assessment's remediation program.

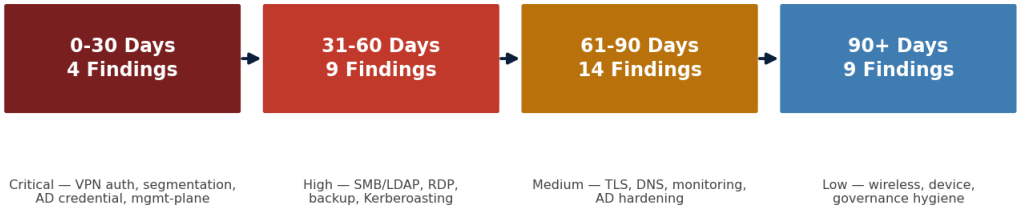
Finding ID	Severity	Owner	Priority	Target Date	Status
NET-001	CRITICAL	Network Security Engineering Lead (Fictional Role)	Immediate — 0-30 Days	10 October 2026	Remediation In Progress
NET-002	CRITICAL	Network Security Engineering Lead (Fictional Role)	Immediate — 0-30 Days	10 October 2026	Remediation In Progress
NET-003	CRITICAL	Active Directory Engineering Lead (Fictional Role)	Immediate — 0-30 Days	10 October 2026	Remediation In Progress
NET-004	CRITICAL	Network Operations Lead (Fictional Role)	Immediate — 0-30 Days	10 October 2026	Remediation In Progress
NET-005	HIGH	Active Directory Engineering Lead (Fictional Role)	31-60 Days	09 November 2026	Remediation Planned
NET-006	HIGH	Active Directory Engineering Lead (Fictional Role)	31-60 Days	09 November 2026	Remediation Planned
NET-007	HIGH	IT Service Desk Manager (Fictional Role)	31-60 Days	09 November 2026	Remediation Planned
NET-008	HIGH	Network Security Engineering Lead (Fictional Role)	31-60 Days	09 November 2026	Remediation Planned
NET-009	HIGH	Network Operations Lead (Fictional Role)	31-60 Days	09 November 2026	Remediation Planned
NET-010	HIGH	Network Security Engineering Lead (Fictional Role)	31-60 Days	09 November 2026	Remediation Planned
NET-011	HIGH	Wireless Infrastructure Lead (Fictional Role)	31-60 Days	09 November 2026	Remediation Planned
NET-012	HIGH	Infrastructure Operations Lead (Fictional Role)	31-60 Days	09 November 2026	Remediation Planned
NET-013	HIGH	Active Directory Engineering Lead (Fictional Role)	31-60 Days	09 November 2026	Remediation Planned
NET-014	MEDIUM	Network Security Engineering Lead (Fictional Role)	61-90 Days	09 December 2026	Remediation Planned
NET-015	MEDIUM	Network Security Engineering Lead (Fictional Role)	61-90 Days	09 December 2026	Remediation Planned
NET-016	MEDIUM	Network Security Engineering Lead (Fictional Role)	61-90 Days	09 December 2026	Remediation Planned
NET-017	MEDIUM	Network Security Engineering Lead (Fictional Role)	61-90 Days	09 December 2026	Remediation Planned
NET-018	MEDIUM	Backend/API Engineering Lead (Fictional Role)	61-90 Days	09 December 2026	Remediation Planned
NET-019	MEDIUM	Infrastructure Operations Lead (Fictional Role)	61-90 Days	09 December 2026	Remediation Planned
NET-020	MEDIUM	Network Security Engineering Lead (Fictional Role)	61-90 Days	09 December 2026	Remediation Planned

Finding ID	Severity	Owner	Priority	Target Date	Status
NET-021	MEDIUM	Infrastructure Operations Lead (Fictional Role)	61-90 Days	09 December 2026	Remediation Planned
NET-022	MEDIUM	Backend/API Engineering Lead (Fictional Role)	61-90 Days	09 December 2026	Remediation Planned
NET-023	MEDIUM	Active Directory Engineering Lead (Fictional Role)	61-90 Days	09 December 2026	Remediation Planned
NET-024	MEDIUM	Active Directory Engineering Lead (Fictional Role)	61-90 Days	09 December 2026	Remediation Planned
NET-025	MEDIUM	Active Directory Engineering Lead (Fictional Role)	61-90 Days	09 December 2026	Remediation Planned
NET-026	MEDIUM	Active Directory Engineering Lead (Fictional Role)	61-90 Days	09 December 2026	Remediation Planned
NET-027	MEDIUM	Wireless Infrastructure Lead (Fictional Role)	61-90 Days	09 December 2026	Remediation Planned
NET-028	LOW	Wireless Infrastructure Lead (Fictional Role)	90+ Days	31 January 2027	Remediation Planned
NET-029	LOW	Network Operations Lead (Fictional Role)	90+ Days	31 January 2027	Remediation Planned
NET-030	LOW	Wireless Infrastructure Lead (Fictional Role)	90+ Days	31 January 2027	Remediation Planned
NET-031	LOW	Network Operations Lead (Fictional Role)	90+ Days	31 January 2027	Remediation Planned
NET-032	LOW	Network Operations Lead (Fictional Role)	90+ Days	31 January 2027	Remediation Planned
NET-033	LOW	Active Directory Engineering Lead (Fictional Role)	90+ Days	31 January 2027	Remediation Planned
NET-034	LOW	Active Directory Engineering Lead (Fictional Role)	90+ Days	31 January 2027	Remediation Planned
NET-035	LOW	Network Security Engineering Lead (Fictional Role)	90+ Days	31 January 2027	Remediation Planned
NET-036	LOW	Cloud & Hybrid Identity Lead (Fictional Role)	90+ Days	31 January 2027	Remediation Planned
NET-037	INFORMATIONAL	Network Security Engineering Lead (Fictional Role)	N/A — Informational	N/A	Observation Only
NET-038	INFORMATIONAL	Network Security Engineering Lead (Fictional Role)	N/A — Informational	N/A	Observation Only
NET-039	INFORMATIONAL	Network Security Engineering Lead (Fictional Role)	N/A — Informational	N/A	Observation Only
NET-040	INFORMATIONAL	Active Directory Engineering Lead (Fictional Role)	N/A — Informational	N/A	Observation Only
NET-041	INFORMATIONAL	Network Security Engineering Lead (Fictional Role)	N/A — Informational	N/A	Observation Only
NET-042	INFORMATIONAL	Network Security Engineering Lead (Fictional Role)	N/A — Informational	N/A	Observation Only
NET-043	INFORMATIONAL	Network Operations Lead (Fictional Role)	N/A — Informational	N/A	Observation Only

Finding ID	Severity	Owner	Priority	Target Date	Status
NET-044	INFORMATIONAL	Network Security Engineering Lead (Fictional Role)	N/A — Informational	N/A	Observation Only
NET-045	INFORMATIONAL	Network Operations Lead (Fictional Role)	N/A — Informational	N/A	Observation Only
NET-046	INFORMATIONAL	Network Security Engineering Lead (Fictional Role)	N/A — Informational	N/A	Observation Only

25 REMEDIATION ROADMAP

The illustrative sample remediation roadmap below sequences all 46 fictional findings across four phases, directly derived from each finding's priority field, prioritizing the four Critical findings and the nine High findings first.



+ 10 Informational observations/recommendations tracked outside the formal remediation SLA (process, documentation, architecture).

Illustrative sample remediation roadmap — fictional sequencing and dates. ILLUSTRATIVE / SYNTHETIC EVIDENCE.

Immediate — 0-30 Days (4 findings)

- External VPN Authentication Can Be Bypassed Through Legacy Authentication Workflow — NET-001 (CRITICAL)
- Insufficient Internal Network Segmentation Enables Unauthenticated Reachability from User VLAN to Database VLAN — NET-002 (CRITICAL)
- Privileged Active Directory Service Account Credential Exposed Through Insecure Group Policy Preferences Configuration — NET-003 (CRITICAL)
- Exposed Management Plane Enables Administrative Access to Core Network Devices from User VLAN — NET-004 (CRITICAL)

31-60 Days (9 findings)

- SMB Signing Not Enforced on Critical Internal Windows Servers — NET-005 (HIGH)
- Insecure LDAP Configuration Permits Credential Exposure via Unsigned, Unencrypted Bind — NET-006 (HIGH)
- Excessive Administrative Access Across User Network Segment via Helpdesk Group Policy — NET-007 (HIGH)
- Weak VPN Security Configuration Permits Legacy Cryptographic Negotiation — NET-008 (HIGH)
- SNMP Community String Configuration Exposes Network Device Information — NET-009 (HIGH)
- RDP Accessible Across Improperly Segmented Network Boundaries — NET-010 (HIGH)
- Insecure Firewall Rule Permits Management-Plane Access From Corporate Wireless Segment — NET-011 (HIGH)
- Sensitive Backup Repository Reachable From User VLAN Without Authentication Segmentation — NET-012 (HIGH)
- Weak Service Account Security Enables Lateral Movement via Kerberoasting — NET-013 (HIGH)

61-90 Days (14 findings)

- Outdated TLS Configuration on External Remote Access Portal — NET-014 (MEDIUM)
- Certificate Configuration Issue on External VPN Gateway — NET-015 (MEDIUM)
- DNS Configuration Weakness Permits Zone Transfer from External DNS Server — NET-016 (MEDIUM)
- Exposed Service With Unnecessary Functionality on External Load Balancer — NET-017 (MEDIUM)
- Information Disclosure Through Verbose Error Messages on Public Web Application Gateway — NET-018 (MEDIUM)
- Legacy/Insecure Protocol Exposure — SMBv1 Still Enabled on Internal File Server — NET-019 (MEDIUM)
- Unnecessary East-West Connectivity Between Application VLAN and Database VLAN Beyond Required Ports — NET-020 (MEDIUM)
- Insecure Monitoring Interface Exposes Sensitive Telemetry Without Authentication — NET-021 (MEDIUM)
- Weak Internal TLS Configuration on Internal API Server — NET-022 (MEDIUM)
- Kerberos Configuration Weakness — Unconstrained Delegation Enabled on Legacy Application Server — NET-023 (MEDIUM)

- Excessive Privilege Assignment — Standard Support Accounts Present in Domain Admins Group — NET-024 (MEDIUM)
- Weak Password Policy Permits Short, Non-Complex Domain Passwords — NET-025 (MEDIUM)
- Insecure Administrative Pathway — Helpdesk Staff Granted Direct RDP to Domain Controllers — NET-026 (MEDIUM)
- Weak Corporate Wireless Configuration — Shared PSK Fallback Available Alongside 802.1X — NET-027 (MEDIUM)

90+ Days (9 findings)

- Guest Wireless Network Isolation Weakness Permits Limited Reachability to Printer VLAN — NET-028 (LOW)
- Insecure SNMP Configuration — SNMPv2c Enabled Alongside SNMPv3 on Distribution Switches — NET-029 (LOW)
- Outdated Device Firmware on Wireless LAN Controller — NET-030 (LOW)
- Configuration Backup Exposure — Unencrypted Device Configurations Stored on Shared Drive — NET-031 (LOW)
- Weak Network-Device ACL Permits Broader Source Range Than Required for SSH Management — NET-032 (LOW)
- Excessive Domain Information Disclosure via Unauthenticated LDAP Enumeration — NET-033 (LOW)
- SYSVOL-Related Sensitive Configuration Reference in Legacy Logon Script — NET-034 (LOW)
- Overly Permissive VPN Trust Allows Split-Tunnel Access to Sensitive On-Prem Resources — NET-035 (LOW)
- Weak Hybrid Segmentation Between On-Prem Identity Sync Server and Cloud Management Path — NET-036 (LOW)

Informational Track (10 observations)

Tracked outside the formal remediation SLA as process, documentation, and architectural improvements (see Section 23).

26 RETEST METHODOLOGY

TMG Security recommends a full retest of all Critical and High findings, and a sampled retest of Medium findings, following completion of remediation activities. Retest methodology mirrors the original test case for each finding, documented in the 'Retest Recommendation' field of each finding card in Sections 19-23.

Retest Prerequisites

- Written confirmation that remediation activity for the finding(s) under retest is complete.
- Access equivalent to the original test (network position, credentials, or scope) to allow like-for-like validation.
- A change log or summary of what was modified, to help scope the retest efficiently.

Evidence Requirements

Each retested finding receives an updated status and a brief evidence note confirming the specific validation performed, consistent with the finding-level Evidence Register (Appendix I).

Finding Status Model

Status	Definition
Open	Finding has not yet been addressed; no remediation activity has begun.
Remediation In Progress	Remediation activity is actively underway.
Remediation Planned	Remediation has been scoped and scheduled but has not yet begun.
Resolved	Remediation has been completed and independently validated via retest.
Accepted Risk	The organization has formally accepted the residual risk rather than remediating, with documented business justification and sign-off.
Not Reproducible	The finding could not be reproduced during retest and is considered a false positive or environment-specific artifact.

27 LIMITATIONS

- No denial-of-service testing was performed at any point during this assessment.
- No destructive exploitation, data modification, or data deletion was performed or attempted.
- No persistence mechanisms were installed on any system.
- No production disruption occurred or was attempted during testing.
- Credential limitations applied where noted — testing reflects the access levels and credentials provided or obtained during the assessment, not necessarily every conceivable privilege level.
- This was a time-boxed assessment; findings reflect the state of the environment during the testing window and may not reflect subsequent changes.
- Third-party systems not directly operated by the client organization were excluded from scope.
- Cloud provider infrastructure below the tenant/management layer explicitly listed in scope was excluded.
- This report and its entire target environment are fictional; these limitations are presented in the same form TMG Security would use for a real engagement.

28 CONCLUSION

This fictional, illustrative assessment identified 46 findings across NorthStar Financial Services' external and internal network, with the four Critical and nine High findings concentrated in network segmentation, Active Directory credential and privilege management, and network device management-plane exposure. TMG Security's simulated recommendation is that these findings be prioritized for immediate and near-term remediation per the roadmap in Section 25, with a full retest of Critical and High findings once remediation is complete.

This document is a fictional sample report prepared by TMG Security to illustrate its network penetration testing methodology and reporting standard. TMG Security thanks the reader for reviewing this sample and welcomes the opportunity to discuss a real network penetration testing engagement scoped to your organization's environment.

APPENDIX A — SCOPE REGISTER

Complete register of all in-scope categories and representative items for this fictional assessment.

Category	Item	Status
External Perimeter	Internet-facing VPN gateway (vpn.northstar-example.com)	In Scope
External Perimeter	Remote access portal (portal.northstar-example.com)	In Scope
External Perimeter	Public web application gateway / WAF	In Scope
External Perimeter	External DNS infrastructure	In Scope
External Perimeter	Email security gateway (mail.northstar-example.com)	In Scope
External Perimeter	External perimeter firewall	In Scope
External Perimeter	External load balancer	In Scope
External Perimeter	Bastion / jump host	In Scope
External Perimeter	Externally reachable remote administration surface	In Scope
Internal Network Zone	User Workstation VLAN	In Scope
Internal Network Zone	Server VLAN	In Scope
Internal Network Zone	Application VLAN	In Scope
Internal Network Zone	Database VLAN	In Scope
Internal Network Zone	Identity / AD VLAN	In Scope
Internal Network Zone	Management VLAN	In Scope
Internal Network Zone	Security Tooling VLAN	In Scope
Internal Network Zone	Backup VLAN	In Scope
Network Security Device	Next-generation firewalls (external and internal)	In Scope
Network Security Device	Core switch	In Scope
Network Security Device	Distribution switches	In Scope
Network Security Device	Wireless LAN controller	In Scope
Network Security Device	Network management platform	In Scope
Windows / Enterprise	Active Directory domain controllers	In Scope
Windows / Enterprise	Windows file server	In Scope
Windows / Enterprise	Windows application server	In Scope
Windows / Enterprise	Windows management server	In Scope
Windows / Enterprise	Internal PKI / certificate services	In Scope
Windows / Enterprise	Internal DNS	In Scope
Windows / Enterprise	Internal monitoring server	In Scope
Linux / Application	Linux application server	In Scope
Linux / Application	Internal API server	In Scope
Linux / Application	Monitoring server	In Scope
Linux / Application	Logging / SIEM collector	In Scope
Linux / Application	Backup server	In Scope
Cloud / Hybrid	Fictional cloud connectivity (site-to-site VPN)	In Scope
Cloud / Hybrid	Hybrid identity synchronization server	In Scope
Cloud / Hybrid	Cloud management interface	In Scope
Wireless	Corporate SSID (NSF-CORP)	In Scope
Wireless	Guest SSID (NSF-GUEST)	In Scope
Wireless	Management SSID (NSF-WLAN-MGMT)	In Scope

APPENDIX B — ASSET REGISTER

Complete fictional asset register — 40 in-scope systems. All hostnames and IP addresses are fictional.

Asset ID	Hostname	IP Address	Zone	Purpose	Exposure	Criticality
NS-A01	NS-FW-EXT01	10.40.0.1	External Perimeter / DMZ	External perimeter firewall / primary internet edge	External	Critical
NS-A02	NS-VPNGW01	10.40.0.10	External Perimeter / DMZ	Remote-access VPN gateway — vpn.northstar-example.com	External	Critical
NS-A03	NS-PORTAL01	10.40.0.11	External Perimeter / DMZ	Employee/partner remote access portal — portal.northstar-example.com	External	High
NS-A04	NS-WAF01	10.40.0.12	External Perimeter / DMZ	Fronts public-facing web applications	External	High
NS-A05	NS-MAILGW01	10.40.0.13	External Perimeter / DMZ	Inbound/outbound mail filtering — mail.northstar-example.com	External	High
NS-A06	NS-DNSEXT01	10.40.0.14	External Perimeter / DMZ	Authoritative DNS for northstar-example.com	External	High
NS-A07	NS-LBEXT01	10.40.0.15	External Perimeter / DMZ	TLS termination and load distribution for public services	External	Medium
NS-A08	NS-BASTION01	10.40.0.20	External Perimeter / DMZ	Administrative jump host for external vendor and remote admin access	External	Critical
NS-A09	NS-RADMIN01	10.40.0.21	External Perimeter / DMZ	Externally reachable WinRM/RDP administration surface for on-call engineers	External	Critical
NS-A10	NS-WKS-FIN07	10.40.10.47	User Workstation VLAN	Finance department workstation — assumed-breach test host	Internal	Medium
NS-A11	NS-WKS-OPS12	10.40.10.62	User Workstation VLAN	Operations department workstation	Internal	Medium
NS-A12	NS-WKS-IT03	10.40.10.15	User Workstation VLAN	IT helpdesk / Tier-1 admin workstation	Internal	High
NS-A13	NS-FILE01	10.40.20.10	Server VLAN	Departmental and corporate file shares	Internal	High
NS-A14	NS-APPSRV01	10.40.20.11	Server VLAN	Internal portal / legacy line-of-business application backend	Internal	High
NS-A15	NS-MGMT01	10.40.20.12	Server VLAN	RSAT / administrative jump server for AD and server management	Internal	Critical
NS-A16	NS-MON01	10.40.20.13	Server VLAN	Infrastructure monitoring and alerting (Windows-hosted)	Internal	Medium
NS-A17	NS-PKI01	10.40.20.14	Server VLAN	Enterprise certificate authority and certificate lifecycle management	Internal	High
NS-A18	NS-DNSINT01	10.40.20.15	Server VLAN	Active Directory-integrated internal DNS	Internal	High

Asset ID	Hostname	IP Address	Zone	Purpose	Exposure	Criticality
NS-A19	NS-AADCONNECT01	10.40.20.16	Server VLAN	On-prem AD to fictional cloud identity synchronization	Internal	Critical
NS-A20	NS-DC01	10.40.50.10	Identity / AD VLAN	Forest root / primary domain controller (NORTHSTAR domain)	Internal	Critical
NS-A21	NS-DC02	10.40.50.11	Identity / AD VLAN	Secondary domain controller / global catalog	Internal	Critical
NS-A22	NS-LINAPP01	10.40.30.10	Application VLAN	Customer-facing payments processing application tier	Internal	High
NS-A23	NS-API01	10.40.30.11	Application VLAN	Internal mobile/API integration layer for core banking services	Internal	Critical
NS-A24	NS-SIEM01	10.40.30.12	Application VLAN	Centralized log aggregation and correlation platform	Internal	High
NS-A25	NS-MON02	10.40.30.13	Application VLAN	Infrastructure and application telemetry dashboards	Internal	Medium
NS-A26	NS-SQL01	10.40.40.10	Database VLAN	Core banking and payments transactional data store	Internal	Critical
NS-A27	NS-SQL02	10.40.40.11	Database VLAN	Reporting warehouse replicated from primary transactional store	Internal	High
NS-A28	NS-BKP01	10.40.60.10	Backup VLAN	Enterprise backup repository for AD, database, and file server data	Internal	Critical
NS-A29	NS-COREW01	172.20.10.1	Management VLAN	Core network switching fabric / management VIP	Internal	Critical
NS-A30	NS-DSW01	172.20.10.2	Management VLAN	Distribution-layer switch — server/application VLANs	Internal	High
NS-A31	NS-DSW02	172.20.10.3	Management VLAN	Distribution-layer switch — user/wireless VLANs	Internal	High
NS-A32	NS-WLC01	172.20.10.5	Management VLAN	Centralized control plane for corporate/guest/management SSIDs	Internal	High
NS-A33	NS-NMS01	172.20.10.6	Management VLAN	Centralized configuration, monitoring, and firmware management	Internal	High
NS-A34	NS-FWINT01	172.20.10.10	Management VLAN	Inter-VLAN segmentation enforcement point	Internal	Critical
NS-A35	NS-VULN01	172.20.20.10	Security Tooling VLAN	Authenticated/unauthenticated internal vulnerability scanning platform	Internal	Medium
NS-A36	NS-EDR01	172.20.20.11	Security Tooling VLAN	Endpoint detection and response management plane	Internal	High
NS-A37	NS-S2SVPN01	10.50.0.10	Cloud / Hybrid Connectivity	IPsec tunnel termination to fictional cloud environment	Internal / Hybrid	High

Asset ID	Hostname	IP Address	Zone	Purpose	Exposure	Criticality
NS-A38	NS-CLOUDMGMT01	10.50.0.11	Cloud / Hybrid Connectivity	Administrative path to fictional cloud tenant management plane	Internal / Hybrid	Critical
NS-A39	NS-AP-CORP-14	10.50.10.5 (mgmt)	Wireless — Management SSID	Representative access point serving Corporate + Guest SSIDs, Harrisonville-pattern branch	Internal	Medium
NS-A40	NS-PRINT-FL3	10.40.10.90	User Workstation VLAN	Floor 3 shared print/scan device	Internal	Low

APPENDIX C — SERVICE / PORT REGISTER

Complete fictional service/port register — 54 entries.

Asset ID	Hostname	Port	Protocol	Service	Notes
NS-A01	NS-FW-EXT01	443	TCP	HTTPS (mgmt)	Firewall management console — restricted to Management VLAN by policy
NS-A02	NS-VPNGW01	443	TCP	HTTPS / SSL-VPN	Primary SSL VPN client portal
NS-A02	NS-VPNGW01	10443	TCP	HTTPS (legacy)	Legacy VPN login endpoint (see NET-001)
NS-A02	NS-VPNGW01	500/4500	UDP	IKEv2 / IPsec	Site-to-site and client IPsec VPN negotiation
NS-A03	NS-PORTAL01	443	TCP	HTTPS	Remote access portal — portal.northstar-example.com
NS-A04	NS-WAF01	443	TCP	HTTPS	Public web application front door
NS-A04	NS-WAF01	8443	TCP	HTTPS (mgmt)	WAF management API (see NET-017)
NS-A05	NS-MAILGW01	25	TCP	SMTP	Inbound/outbound mail relay
NS-A05	NS-MAILGW01	443	TCP	HTTPS	Mail gateway administration
NS-A06	NS-DNSEXT01	53	TCP/UDP	DNS	Authoritative DNS for northstar-example.com (see NET-016)
NS-A07	NS-LBEXT01	443	TCP	HTTPS	TLS termination for public services
NS-A08	NS-BASTION01	22	TCP	SSH	Administrative jump host
NS-A09	NS-RADMIN01	3389	TCP	RDP	Externally reachable RDP (see NET-010 related exposure)
NS-A09	NS-RADMIN01	5986	TCP	WinRM (HTTPS)	Remote PowerShell administration
NS-A12	NS-WKS-IT03	3389	TCP	RDP	Local RDP (admin workstation)
NS-A13	NS-FILE01	445	TCP	SMB	File shares (see NET-005, NET-019)
NS-A13	NS-FILE01	139	TCP	NetBIOS Session	Legacy NetBIOS
NS-A14	NS-APPSRV01	443	TCP	HTTPS	Internal portal application
NS-A14	NS-APPSRV01	445	TCP	SMB	Application file share (see NET-005)
NS-A15	NS-MGMT01	5985/5986	TCP	WinRM	Remote administration of servers
NS-A15	NS-MGMT01	3389	TCP	RDP	Administrative RDP jump path

Asset ID	Hostname	Port	Protocol	Service	Notes
NS-A16	NS-MON01	443	TCP	HTTPS	Monitoring dashboard (Windows)
NS-A17	NS-PKI01	443	TCP	HTTPS	Certificate services web enrollment
NS-A18	NS-DNSINT01	53	TCP/UDP	DNS	AD-integrated internal DNS
NS-A19	NS-AADCONNECT01	443	TCP	HTTPS	Hybrid identity sync service (see NET-036)
NS-A20	NS-DC01	389	TCP/UDP	LDAP	Directory services (see NET-006, NET-033)
NS-A20	NS-DC01	636	TCP	LDAPS	Directory services (encrypted)
NS-A20	NS-DC01	88	TCP/UDP	Kerberos	Authentication (see NET-013, NET-023)
NS-A20	NS-DC01	445	TCP	SMB	SYSVOL / NETLOGON (see NET-034)
NS-A20	NS-DC01	3268/3269	TCP	Global Catalog	Forest-wide directory queries
NS-A21	NS-DC02	389/636/88/445	TCP/UDP	AD Services	Secondary domain controller — mirrors NS-DC01 exposure
NS-A22	NS-LINAPP01	443	TCP	HTTPS	Payments application tier
NS-A22	NS-LINAPP01	22	TCP	SSH	Administrative access
NS-A23	NS-API01	8443	TCP	HTTPS (internal API)	Internal mobile/API integration layer (see NET-022)
NS-A24	NS-SIEM01	443	TCP	HTTPS	SIEM web console
NS-A24	NS-SIEM01	514	UDP	Syslog	Centralized log ingestion
NS-A25	NS-MON02	3000	TCP	HTTP (dashboard)	Monitoring dashboard — unauthenticated by default (see NET-021)
NS-A26	NS-SQL01	1433	TCP	MSSQL	Primary transactional database (see NET-002)
NS-A27	NS-SQL02	1433	TCP	MSSQL	Reporting database
NS-A28	NS-BKP01	445	TCP	SMB	Backup repository share (see NET-012)
NS-A28	NS-BKP01	443	TCP	HTTPS	Backup management console
NS-A29	NS-COREW01	22	TCP	SSH	Core switch management
NS-A29	NS-COREW01	161	UDP	SNMP	Device monitoring (see NET-009, NET-029)
NS-A29	NS-COREW01	443	TCP	HTTPS	Web management console (see NET-004)
NS-A30	NS-DSW01	22/161/443	TCP/UDP	SSH/SNMP/HTTPS	Distribution switch management
NS-A31	NS-DSW02	22/161/443	TCP/UDP	SSH/SNMP/HTTPS	Distribution switch management
NS-A32	NS-WLC01	443	TCP	HTTPS	Wireless controller management (see NET-011, NET-030)
NS-A33	NS-NMS01	443	TCP	HTTPS	Network management platform console
NS-A34	NS-FWINT01	443/22	TCP	HTTPS/SSH	Internal firewall management (see NET-004, NET-011)
NS-A35	NS-VULN01	443	TCP	HTTPS	Vulnerability scanner console
NS-A36	NS-EDR01	443	TCP	HTTPS	EDR management console
NS-A37	NS-S2SVPN01	500/4500	UDP	IKEv2/IPsec	Site-to-site VPN to fictional cloud environment
NS-A38	NS-CLOUDMGMT01	443	TCP	HTTPS	Cloud management interface (see NET-036)
NS-A40	NS-PRINT-FL3	9100/515/631	TCP	Printing (RAW/LPD/IPP)	Networked print services

APPENDIX D — NETWORK ARCHITECTURE REGISTER

Zone-level architecture register cross-referencing the diagrams in Sections 07-09.

Zone	Address Range	Description
External Perimeter / DMZ	10.40.0.0/24	Internet-facing gateways, VPN, portal, mail, DNS, load balancer, bastion
User Workstation VLAN	10.40.10.0/24	Standard end-user Windows workstations, laptops, VDI clients
Server VLAN	10.40.20.0/24	Windows infrastructure servers — file, application, management, monitoring, PKI, internal DNS
Application VLAN	10.40.30.0/24	Linux application, internal API, logging/SIEM, and monitoring servers
Database VLAN	10.40.40.0/24	Primary transactional and reporting database instances
Identity / AD VLAN	10.40.50.0/24	Active Directory domain controllers and identity infrastructure
Backup VLAN	10.40.60.0/24	Backup repository and backup-management infrastructure
Management VLAN	172.20.10.0/24	Out-of-band management interfaces for network devices, core/distribution switches, firewalls, WLC
Security Tooling VLAN	172.20.20.0/24	Vulnerability scanning and EDR management infrastructure
Wireless — Corporate SSID	10.50.10.0/24	Corporate-issued and BYOD endpoints on the 802.1X corporate SSID
Wireless — Guest SSID	10.50.20.0/24	Guest and visitor wireless clients
Wireless — Management SSID	10.50.30.0/24	Wireless infrastructure management (APs, WLC control plane)
Cloud / Hybrid Connectivity	10.50.0.0/24	Site-to-site VPN termination and hybrid identity/cloud management path

Network Devices

Asset ID	Hostname	IP Address	Role
NS-A01	NS-FW-EXT01	10.40.0.1	External perimeter firewall / primary internet edge
NS-A02	NS-VPNGW01	10.40.0.10	Remote-access VPN gateway — vpn.northstar-example.com
NS-A07	NS-LBEXT01	10.40.0.15	TLS termination and load distribution for public services
NS-A29	NS-COREW01	172.20.10.1	Core network switching fabric / management VIP
NS-A30	NS-DSW01	172.20.10.2	Distribution-layer switch — server/application VLANs
NS-A31	NS-DSW02	172.20.10.3	Distribution-layer switch — user/wireless VLANs
NS-A32	NS-WLC01	172.20.10.5	Centralized control plane for corporate/guest/management SSIDs
NS-A33	NS-NMS01	172.20.10.6	Centralized configuration, monitoring, and firmware management
NS-A34	NS-FWINT01	172.20.10.10	Inter-VLAN segmentation enforcement point

Asset ID	Hostname	IP Address	Role
NS-A39	NS-AP-CORP-14	10.50.10.5 (mgmt)	Representative access point serving Corporate + Guest SSIDs, Harrisonville-pattern branch

APPENDIX E — NETWORK SEGMENTATION MATRIX

Complete segmentation register, duplicated here for appendix traceability (see also Section 10).

Source Zone	Destination Zone	Expected	Observed	Risk	Finding
User Workstation VLAN	Database VLAN	Denied by default — no direct reachability	Permitted — unrestricted TCP/1433 reachability via overly broad rule	Critical	NET-002
User Workstation VLAN	Management VLAN	Denied — management plane isolated	Permitted — HTTPS management console reachable, missing ACL	Critical	NET-004
User Workstation VLAN	Server VLAN (RDP)	Denied — RDP only via NS-MGMT01 jump host	Permitted — direct RDP reachable to multiple servers	High	NET-010
User Workstation VLAN	Backup VLAN	Denied — backup infrastructure isolated	Permitted — SMB share reachable with broad read permission	High	NET-012
Guest Wireless SSID	Corporate Network (all zones)	Denied — full isolation	Denied, as expected	None	—
Guest Wireless SSID	Management VLAN	Denied — full isolation	Denied, as expected	None	—
Guest Wireless SSID	Printer Subnet (kiosk exception)	Permitted to kiosk device only	Permitted to broader printer subnet than intended	Low	NET-028
Corporate Wireless SSID	Management VLAN	Denied — except WLC uplink	Permitted — Corporate SSID client range included in source object	High	NET-011
Corporate Wireless SSID	User Workstation VLAN	Permitted — equivalent to wired user access	Permitted, as expected	None	—
Application VLAN	Database VLAN	Permitted — TCP/1433 only	Permitted — TCP/1433 plus TCP/135, UDP/1434, TCP/3389	Medium	NET-020
Application VLAN	Server VLAN	Permitted — documented integration ports only	Permitted, as documented	None	—
VPN (post-authentication)	Internal Network (all zones per role)	Full-tunnel, role-scoped split-tunnel exceptions only	Split tunneling enabled by default for all roles	Low	NET-035
Backup VLAN	User Workstation VLAN	Denied — one-directional isolation	Denied, as expected	None	—
Identity / AD VLAN	All Zones (authentication/replication)	Permitted per AD functional requirements	Permitted, as expected and required	None	—
Security Tooling VLAN	All Zones (scoped scanning/EDR)	Permitted, scoped to scanning/EDR ports	Permitted, as documented	None	—
Cloud / Hybrid Connectivity	Server VLAN (identity sync)	Permitted — scoped to sync endpoints only	Permitted — broader reachability than the sync function requires	Low	NET-036
External Perimeter / DMZ	User Workstation VLAN	Denied — no direct DMZ-to-user reachability	Denied, as expected	None	—
External Perimeter / DMZ	Server / Application / Database VLANs	Denied — external hosts do not reach internal tiers directly	Denied, as expected	None	—

APPENDIX F — ACTIVE DIRECTORY ASSESSMENT MATRIX

Assessment Area	Summary	Related Findings
Domain Architecture	Single-domain, single-forest design (NORTHSTAR), consistent with the organization's size; no unnecessary forest/domain trust complexity observed.	
Domain Controllers	Two domain controllers (NS-DC01, NS-DC02) provide redundancy; both carry the same exposure for LDAP and Kerberos findings identified in this assessment.	NET-006, NET-013, NET-033
Trust Relationships	No external or forest trusts are configured; this significantly limits cross-domain lateral movement risk and was validated as a positive architectural characteristic.	
Privileged Groups	Domain Admins membership exceeds the minimum required for genuine Tier-0 activity, including several accounts used for routine application support.	NET-024
Service Accounts	Several SPN-registered service accounts use stale, non-rotated passwords vulnerable to Kerberoasting; a Domain Admin-equivalent service account credential was recoverable from a legacy SYSVOL artifact.	NET-003, NET-013
Password Policy	The Default Domain Policy enforces only an 8-character minimum with no banned-password-list screening, below current guidance for the organization's risk profile.	NET-025
LDAP	Both domain controllers accept unsigned, unencrypted simple binds, and a limited anonymous bind discloses RootDSE/naming-context information.	NET-006, NET-033
Kerberos	Stale SPN-registered account passwords are Kerberoastable; one legacy application server is configured for unconstrained delegation.	NET-013, NET-023
SMB	SMB signing is not enforced on several critical Windows servers, and SMBv1 remains enabled on the primary file server for legacy device compatibility.	NET-005, NET-019
SYSVOL	A legacy Group Policy Preferences file exposes a Domain Admin-equivalent credential; a related stale credential-path reference was identified in a legacy logon script.	NET-003, NET-034
GPO Security	Group Policy is used appropriately for baseline configuration in most areas reviewed; the Restricted Groups misconfiguration (NET-007) and legacy GPP artifact (NET-003) are the two exceptions identified.	NET-003, NET-007
Administrative Pathways	Tier-1 helpdesk accounts hold both standing local administrator rights fleet-wide and direct interactive RDP access to domain controllers, both inconsistent with a tiered administration model.	NET-007, NET-026
Workstation / Server Trust	No unconstrained delegation was identified on workstation-tier systems; the single instance identified is scoped to a legacy application server (NET-023).	NET-023

Assessment Area	Summary	Related Findings
Privileged Access	No PAW (Privileged Access Workstation) model is currently in use for Tier-0 administrative activity.	NET-040
Monitoring	AD-relevant events (authentication, privileged group changes) are forwarded to the centralized SIEM; specific detection content for the lateral-movement techniques used in this assessment was not confirmed during interview.	NET-038, NET-042
Credential Exposure	The most severe finding of this assessment (NET-003) is a credential-exposure issue; combined with NET-006 and NET-013, credential exposure is the dominant theme across the AD assessment.	NET-003, NET-006, NET-013

APPENDIX G — TEST CASE REGISTER

The register below documents all 152 fictional test cases executed during this illustrative assessment, spanning the 24 testing categories presented across this report. Every 'Fail' or 'Observation' result maps to a corresponding finding in Sections 19-23.

Test ID	Category	Test Description / Objective	Result	Finding
TC-NET-001	External Reconnaissance	Enumerate publicly registered domains, subdomains, and IP ranges associated with the client via passive OSINT sources.	Pass	
TC-NET-002	External Reconnaissance	Review public breach-data sources for previously exposed NorthStar employee credentials (fictional).	Observation	
TC-NET-003	External Reconnaissance	Identify externally hosted services and technology fingerprints via passive means (certificate transparency logs, WHOIS, DNS).	Pass	
TC-NET-004	External Reconnaissance	Review employee-facing metadata (job postings, public documents) for technology stack disclosure.	Pass	
TC-NET-005	External Reconnaissance	Enumerate email format and employee naming convention from public sources for later password-spray target list construction.	Observation	
TC-NET-006	External Reconnaissance	Review certificate transparency logs for undocumented or forgotten subdomains.	Pass	
TC-NET-007	External Reconnaissance	Assess public code repositories and paste sites for inadvertently disclosed configuration or credentials (fictional, non-destructive).	Pass	
TC-NET-008	External Reconnaissance	Review historical DNS resolution data for infrastructure changes indicating stale attack-surface documentation.	Pass	
TC-NET-009	External Reconnaissance	Enumerate ASN and IP allocation ownership for in-scope address ranges.	Pass	
TC-NET-010	External Service Enumeration	Perform a full TCP/UDP port scan against all in-scope external IP addresses.	Pass	
TC-NET-011	External Service Enumeration	Enumerate service banners and versions for all identified external listening services.	Pass	
TC-NET-012	External Service Enumeration	Identify the external web application gateway's management interface exposure.	Fail	NET-017
TC-NET-013	External Service Enumeration	Enumerate the external load balancer's supported protocols and cipher suites.	Pass	
TC-NET-014	External Service Enumeration	Test the external mail gateway for open relay configuration.	Pass	
TC-NET-015	External Service Enumeration	Enumerate the bastion host's exposed SSH configuration and supported authentication methods.	Pass	
TC-NET-016	External Service Enumeration	Test externally reachable administrative surfaces for default or common credentials.	Pass	
TC-NET-017	External Service Enumeration	Review externally reachable services for known unpatched vulnerabilities.	Pass	
TC-NET-018	External Service Enumeration	Test externally reachable services for HTTP method handling weaknesses (TRACE, PUT, DELETE).	Pass	

Test ID	Category	Test Description / Objective	Result	Finding
TC-NET-019	External Service Enumeration	Enumerate virtual host / SNI-based routing configuration on the external load balancer.	Pass	
TC-NET-020	Authentication	Test the primary VPN login path for mandatory MFA enforcement.	Pass	NET-039
TC-NET-021	Authentication	Test all discoverable authentication endpoints (including legacy/deprecated paths) for consistent MFA enforcement.	Fail	NET-001
TC-NET-022	Authentication	Perform a controlled password-spray test against a synthetic account population using common patterns.	Pass	
TC-NET-023	Authentication	Test account lockout and rate-limiting behavior on the external portal.	Pass	
TC-NET-024	Authentication	Assess password reset workflow for account enumeration weaknesses.	Pass	
TC-NET-025	Authentication	Review domain password policy for minimum length, complexity, and breached-password screening.	Fail	NET-025
TC-NET-026	Authentication	Test session-timeout enforcement on the remote access portal.	Pass	
TC-NET-027	Authentication	Test for username enumeration via differing error messages on the login form.	Pass	
TC-NET-028	Authentication	Review MFA enrollment coverage across the employee population via interview.	Pass	
TC-NET-029	VPN	Enumerate supported IKE/SSL VPN authentication methods and protocol versions.	Fail	NET-008
TC-NET-030	VPN	Test VPN split-tunnel default configuration.	Fail	NET-035
TC-NET-031	VPN	Test VPN gateway TLS certificate validity and chain configuration.	Fail	NET-015
TC-NET-032	VPN	Test VPN gateway for IKE Aggressive Mode exposure.	Fail	NET-008
TC-NET-033	VPN	Assess post-authentication network reachability granted to a standard VPN session.	Observation	NET-002
TC-NET-034	VPN	Test VPN client posture-check enforcement (where applicable).	Pass	
TC-NET-035	VPN	Test VPN client certificate revocation checking behavior.	Pass	
TC-NET-036	TLS	Scan all externally reachable HTTPS services for supported protocol versions and cipher suites.	Fail	NET-014
TC-NET-037	TLS	Scan internal HTTPS services for certificate trust chain validity.	Fail	NET-022
TC-NET-038	TLS	Test for TLS downgrade and renegotiation weaknesses on external services.	Pass	
TC-NET-039	TLS	Review certificate expiration windows across all in-scope TLS-terminating services.	Fail	NET-015
TC-NET-040	TLS	Assess HSTS and secure-cookie header configuration on externally reachable web services.	Pass	
TC-NET-041	TLS	Test for mixed-content or weak-cipher warnings on internal web applications.	Pass	
TC-NET-042	DNS	Test the external authoritative DNS server for unrestricted zone transfer (AXFR).	Fail	NET-016
TC-NET-043	DNS	Enumerate DNS records for stale or decommissioned host references.	Fail	NET-044

Test ID	Category	Test Description / Objective	Result	Finding
TC-NET-044	DNS	Test internal DNS for cache-poisoning susceptibility (non-destructive configuration review).	Pass	
TC-NET-045	DNS	Review DNSSEC configuration status for the external zone.	Observation	
TC-NET-046	DNS	Test for DNS-based internal hostname disclosure via external-facing records.	Pass	
TC-NET-047	DNS	Test internal DNS for split-horizon consistency between internal and external views.	Pass	
TC-NET-048	Firewall	Review external firewall rule base for overly permissive any-any style rules.	Pass	
TC-NET-049	Firewall	Review internal segmentation firewall rule base for overly permissive rules between VLANs.	Fail	NET-002
TC-NET-050	Firewall	Test firewall logging and alerting for denied traffic across segmentation boundaries.	Pass	
TC-NET-051	Firewall	Assess firewall change-management and recertification process via interview.	Fail	NET-046
TC-NET-052	Firewall	Test firewall handling of fragmented and malformed packets at the external perimeter.	Pass	
TC-NET-053	Firewall	Review firewall rule base for unused or shadowed rules.	Pass	
TC-NET-054	Firewall	Test external firewall handling of source-routed and spoofed-source packets.	Pass	
TC-NET-055	Firewall	Review firewall high-availability failover configuration.	Pass	
TC-NET-056	Network Segmentation	Test User VLAN to Database VLAN reachability against the segmentation matrix.	Fail	NET-002
TC-NET-057	Network Segmentation	Test User VLAN to Management VLAN reachability against the segmentation matrix.	Fail	NET-004
TC-NET-058	Network Segmentation	Test Application VLAN to Database VLAN reachability scope.	Fail	NET-020
TC-NET-059	Network Segmentation	Test Guest Wireless SSID isolation from all corporate/management zones.	Fail	NET-028
TC-NET-060	Network Segmentation	Test Corporate Wireless SSID reachability to the Management VLAN.	Fail	NET-011
TC-NET-061	Network Segmentation	Test Backup VLAN isolation from the User Workstation VLAN.	Fail	NET-012
TC-NET-062	Network Segmentation	Test RDP reachability boundaries between User VLAN and Server/Database VLANs.	Fail	NET-010
TC-NET-063	Network Segmentation	Validate the full segmentation matrix (Appendix E) against observed live traffic flows.	Fail	NET-002, NET-004, NET-010, NET-011, NET-012, NET-020, NET-028
TC-NET-064	Network Segmentation	Test Security Tooling VLAN reachability scope to Server/Application/Database VLANs.	Pass	
TC-NET-065	Network Segmentation	Test Identity/AD VLAN reachability boundaries from non-domain-controller zones.	Pass	
TC-NET-066	SMB	Test SMB signing enforcement on all in-scope Windows servers.	Fail	NET-005
TC-NET-067	SMB	Test for SMBv1 protocol availability across the Windows server estate.	Fail	NET-019

Test ID	Category	Test Description / Objective	Result	Finding
TC-NET-068	SMB	Enumerate accessible SMB shares and effective permissions across the Server VLAN.	Fail	NET-012
TC-NET-069	SMB	Test SMB null-session enumeration against domain-joined hosts.	Pass	
TC-NET-070	SMB	Test for SMB relay susceptibility (NTLM relay) against critical servers.	Fail	NET-005
TC-NET-071	SMB	Test SMB encryption (SMB 3.x) availability and enforcement on file services.	Pass	
TC-NET-072	LDAP	Test domain controllers for LDAP signing and channel binding enforcement.	Fail	NET-006
TC-NET-073	LDAP	Test for anonymous LDAP bind information disclosure.	Fail	NET-033
TC-NET-074	LDAP	Enumerate LDAP-exposed directory attributes reachable by a standard authenticated account.	Pass	
TC-NET-075	LDAP	Test LDAPS availability and certificate validity on both domain controllers.	Pass	
TC-NET-076	LDAP	Review LDAP query rate-limiting to mitigate enumeration/DoS-style abuse.	Pass	
TC-NET-077	Kerberos	Enumerate SPN-registered service accounts and request service tickets for offline analysis.	Fail	NET-013
TC-NET-078	Kerberos	Test for AS-REP roasting exposure (accounts with Kerberos pre-authentication disabled).	Pass	
TC-NET-079	Kerberos	Review Kerberos delegation configuration across domain-joined computer objects.	Fail	NET-023
TC-NET-080	Kerberos	Test Kerberos ticket lifetime and renewal policy configuration.	Pass	
TC-NET-081	Kerberos	Test for pass-the-ticket susceptibility given current logging/detection coverage.	Observation	NET-042
TC-NET-082	Active Directory	Enumerate Domain Admins and other Tier-0 privileged group membership.	Fail	NET-024
TC-NET-083	Active Directory	Review domain trust configuration for unnecessary or risky trust relationships.	Pass	
TC-NET-084	Active Directory	Audit SYSVOL for legacy Group Policy Preferences credential artifacts.	Fail	NET-003
TC-NET-085	Active Directory	Review domain controller interactive logon rights for non-Tier-0 accounts.	Fail	NET-026
TC-NET-086	Active Directory	Review Restricted Groups GPO configuration for overly broad local administrator assignment.	Fail	NET-007
TC-NET-087	Active Directory	Review GPO permissions for unauthorized modification rights.	Pass	
TC-NET-088	Active Directory	Assess AD-integrated DNS for dynamic update security configuration.	Pass	
TC-NET-089	Active Directory	Review fine-grained password policy (if any) applied to privileged accounts.	Fail	NET-025
TC-NET-090	Active Directory	Review AdminSDHolder and protected-group configuration for unexpected permissions.	Pass	
TC-NET-091	RDP	Test RDP reachability from the User VLAN to Server and Database VLAN hosts.	Fail	NET-010

Test ID	Category	Test Description / Objective	Result	Finding
TC-NET-092	RDP	Test RDP Network Level Authentication (NLA) enforcement on in-scope Windows servers.	Pass	
TC-NET-093	RDP	Review RDP session logging and centralization via the jump-host model.	Pass	
TC-NET-094	RDP	Test for RDP credential caching or cached-credential exposure on shared administrative hosts.	Pass	
TC-NET-095	RDP	Test Restricted Admin mode availability/enforcement for RDP administrative sessions.	Pass	
TC-NET-096	WinRM	Test WinRM (5985/5986) reachability scope across the Server VLAN.	Pass	
TC-NET-097	WinRM	Test WinRM authentication mechanism configuration (Kerberos vs. Basic/NTLM).	Pass	
TC-NET-098	WinRM	Test externally reachable WinRM administration surface (NS-RADMIN01) for authentication strength.	Observation	NET-001
TC-NET-099	WinRM	Review WinRM certificate-based authentication availability as an alternative to Kerberos for cross-forest scenarios.	Pass	
TC-NET-100	Network Devices	Test core and distribution switches for vendor default administrative credentials.	Fail	NET-004
TC-NET-101	Network Devices	Review management-plane ACL scoping across all in-scope network devices.	Fail	NET-032
TC-NET-102	Network Devices	Review firmware currency across all in-scope network devices against vendor-recommended releases.	Fail	NET-030
TC-NET-103	Network Devices	Review configuration backup storage location and access controls.	Fail	NET-031
TC-NET-104	Network Devices	Test device administrative account centralization (TACACS+/RADIUS vs. local accounts).	Observation	NET-004
TC-NET-105	Network Devices	Test network device console/AUX port security configuration where physically accessible during the internal assessment.	Pass	
TC-NET-106	SNMP	Enumerate SNMP community strings across in-scope network devices.	Fail	NET-009
TC-NET-107	SNMP	Test SNMP write-community (RW) access for configuration-modification exposure.	Fail	NET-009
TC-NET-108	SNMP	Test SNMPv3 configuration for authentication and privacy protocol strength where enabled.	Pass	
TC-NET-109	SNMP	Review SNMP trap destination configuration for unauthorized trap receivers.	Pass	
TC-NET-110	Wireless	Assess Corporate SSID authentication model for 802.1X enforcement and PSK fallback presence.	Fail	NET-027
TC-NET-111	Wireless	Test Guest SSID client isolation scope.	Fail	NET-028
TC-NET-112	Wireless	Test Management SSID isolation from client-facing SSIDs.	Pass	
TC-NET-113	Wireless	Review wireless intrusion detection/prevention configuration and alerting.	Pass	

Test ID	Category	Test Description / Objective	Result	Finding
TC-NET-114	Wireless	Test for rogue access point detection capability.	Pass	
TC-NET-115	Wireless	Test wireless signal leakage assessment at building perimeter (non-intrusive, informational only).	Observation	
TC-NET-116	Backup Infrastructure	Test backup repository share reachability from the User VLAN.	Fail	NET-012
TC-NET-117	Backup Infrastructure	Review backup share permission configuration.	Fail	NET-012
TC-NET-118	Backup Infrastructure	Review backup encryption-at-rest configuration.	Observation	NET-012
TC-NET-119	Backup Infrastructure	Test backup management console authentication strength.	Pass	
TC-NET-120	Backup Infrastructure	Review backup job scheduling and retention configuration for ransomware-resilience characteristics (immutability/air-gap).	Observation	
TC-NET-121	Monitoring	Test internal monitoring dashboards for unauthenticated access.	Fail	NET-021
TC-NET-122	Monitoring	Review centralized logging coverage across core infrastructure categories.	Pass	NET-038
TC-NET-123	Monitoring	Review SIEM detection content coverage for lateral-movement technique categories exercised during testing.	Fail	NET-042
TC-NET-124	Monitoring	Test log-ingestion timeliness for authentication and firewall-deny events.	Pass	NET-038
TC-NET-125	Monitoring	Review alert-fatigue indicators (alert volume vs. triage capacity) via interview.	Observation	
TC-NET-126	Cloud/Hybrid	Test site-to-site VPN tunnel cryptographic configuration to the fictional cloud environment.	Pass	
TC-NET-127	Cloud/Hybrid	Review hybrid identity synchronization server outbound connectivity scope.	Fail	NET-036
TC-NET-128	Cloud/Hybrid	Test cloud management interface authentication and network exposure.	Observation	NET-036
TC-NET-129	Cloud/Hybrid	Review hybrid identity synchronization account privilege scope.	Pass	
TC-NET-130	Cloud/Hybrid	Review conditional access policy alignment between on-prem MFA policy and cloud identity provider.	Pass	
TC-NET-131	Lateral Movement	Attempt lateral movement from a compromised User VLAN host to the Server VLAN via captured/relayed credentials.	Fail	NET-002, NET-005, NET-010
TC-NET-132	Lateral Movement	Attempt lateral movement using a Kerberoasted service account credential.	Fail	NET-013
TC-NET-133	Lateral Movement	Attempt lateral movement via the SYSVOL-exposed privileged credential to reach domain controllers.	Fail	NET-003
TC-NET-134	Lateral Movement	Test detection and alerting during simulated lateral-movement activity.	Fail	NET-042
TC-NET-135	Lateral Movement	Attempt lateral movement via excessive Application-to-Database VLAN port reachability.	Fail	NET-020

Test ID	Category	Test Description / Objective	Result	Finding
TC-NET-136	Privilege Escalation	Attempt privilege escalation from standard domain user to Domain Admin via the SYSVOL GPP credential path.	Fail	NET-003
TC-NET-137	Privilege Escalation	Attempt privilege escalation via Helpdesk-All local administrator group membership.	Fail	NET-007
TC-NET-138	Privilege Escalation	Attempt privilege escalation via unconstrained delegation on NS-APPSRV01.	Fail	NET-023
TC-NET-139	Privilege Escalation	Review local privilege escalation vectors on sampled Windows workstation images.	Pass	
TC-NET-140	Privilege Escalation	Attempt privilege escalation via direct domain-controller RDP access using a compromised Tier-1 helpdesk credential.	Fail	NET-026
TC-NET-141	Logging/Detection	Validate firewall deny-log generation for denied segmentation-boundary traffic.	Pass	
TC-NET-142	Logging/Detection	Validate authentication-failure alerting for the VPN gateway.	Pass	
TC-NET-143	Logging/Detection	Validate detection coverage for SNMP community-string brute-force attempts.	Observation	NET-009
TC-NET-144	Logging/Detection	Validate detection coverage for anomalous SPN service-ticket request volume (Kerberoasting indicator).	Fail	NET-042
TC-NET-145	Logging/Detection	Validate detection coverage for unauthorized network device management-plane access attempts.	Fail	NET-004
TC-NET-146	Configuration Review	Review Windows Server hardening baseline application across the Server VLAN.	Fail	NET-005, NET-006
TC-NET-147	Configuration Review	Review network device build/deployment checklist for credential-rotation verification steps.	Fail	NET-004
TC-NET-148	Configuration Review	Review certificate lifecycle management coverage across all TLS-terminating services.	Fail	NET-015
TC-NET-149	Configuration Review	Review firewall change-management documentation for business-justification completeness.	Fail	NET-002, NET-046
TC-NET-150	Configuration Review	Review overall network documentation for consistency across diagrams and configuration references.	Fail	NET-043
TC-NET-151	Configuration Review	Review wireless configuration baseline for PSK rotation policy documentation.	Fail	NET-027
TC-NET-152	Configuration Review	Review monitoring/dashboard deployment checklist for authentication-enablement verification.	Fail	NET-021

APPENDIX H — FINDING REGISTER

Complete register of all 46 fictional findings identified during this illustrative assessment, sorted by severity then finding ID.

Finding ID	Severity	Title	CVSS	Status	Owner	Zone	CWE
NET-001	CRITICAL	External VPN Authentication Can Be Bypassed Through Legacy Authentication Workflow	9.4	Remediation In Progress	Network Security Engineering Lead	External Perimeter / D	CWE-287
NET-002	CRITICAL	Insufficient Internal Network Segmentation Enables Unauthenticated Reachability from User VLAN to Database VLAN	9.1	Remediation In Progress	Network Security Engineering Lead	User Workstation VLAN	CWE-284
NET-003	CRITICAL	Privileged Active Directory Service Account Credential Exposed Through Insecure Group Policy Preferences Configuration	9.8	Remediation In Progress	Active Directory Engineering Lead	Identity / AD VLAN (SY	CWE-522
NET-004	CRITICAL	Exposed Management Plane Enables Administrative Access to Core Network Devices from User VLAN	9.6	Remediation In Progress	Network Operations Lead	User Workstation VLAN	CWE-284
NET-005	HIGH	SMB Signing Not Enforced on Critical Internal Windows Servers	8.1	Remediation Planned	Active Directory Engineering Lead	Server VLAN	CWE-300
NET-006	HIGH	Insecure LDAP Configuration Permits Credential Exposure via Unsigned, Unencrypted Bind	7.6	Remediation Planned	Active Directory Engineering Lead	Identity / AD VLAN	CWE-319
NET-007	HIGH	Excessive Administrative Access Across User Network Segment via Helpdesk Group Policy	7.8	Remediation Planned	IT Service Desk Manager	User Workstation VLAN	CWE-269
NET-008	HIGH	Weak VPN Security Configuration Permits Legacy Cryptographic Negotiation	7.4	Remediation Planned	Network Security Engineering Lead	External Perimeter / D	CWE-327
NET-009	HIGH	SNMP Community String Configuration Exposes Network Device Information	7.2	Remediation Planned	Network Operations Lead	Management VLAN (reach	CWE-200
NET-010	HIGH	RDP Accessible Across Improperly Segmented Network Boundaries	8.0	Remediation Planned	Network Security Engineering Lead	User Workstation VLAN	CWE-284
NET-011	HIGH	Insecure Firewall Rule Permits Management-Plane Access From Corporate Wireless Segment	8.3	Remediation Planned	Wireless Infrastructure Lead	Wireless — Corporate S	CWE-284

Finding ID	Severity	Title	CVSS	Status	Owner	Zone	CWE
NET-012	HIGH	Sensitive Backup Repository Reachable From User VLAN Without Authentication Segmentation	8.6	Remediation Planned	Infrastructure Operations Lead	User Workstation VLAN	CWE-732
NET-013	HIGH	Weak Service Account Security Enables Lateral Movement via Kerberoasting	7.9	Remediation Planned	Active Directory Engineering Lead	Identity / AD VLAN	CWE-522
NET-014	MEDIUM	Outdated TLS Configuration on External Remote Access Portal	5.9	Remediation Planned	Network Security Engineering Lead	External Perimeter / D	CWE-326
NET-015	MEDIUM	Certificate Configuration Issue on External VPN Gateway	5.3	Remediation Planned	Network Security Engineering Lead	External Perimeter / D	CWE-295
NET-016	MEDIUM	DNS Configuration Weakness Permits Zone Transfer from External DNS Server	5.8	Remediation Planned	Network Security Engineering Lead	External Perimeter / D	CWE-200
NET-017	MEDIUM	Exposed Service With Unnecessary Functionality on External Load Balancer	6.4	Remediation Planned	Network Security Engineering Lead	External Perimeter / D	CWE-16
NET-018	MEDIUM	Information Disclosure Through Verbose Error Messages on Public Web Application Gateway	4.3	Remediation Planned	Backend/API Engineering Lead	External Perimeter / D	CWE-209
NET-019	MEDIUM	Legacy/Insecure Protocol Exposure — SMBv1 Still Enabled on Internal File Server	6.8	Remediation Planned	Infrastructure Operations Lead	Server VLAN	CWE-327
NET-020	MEDIUM	Unnecessary East-West Connectivity Between Application VLAN and Database VLAN Beyond Required Ports	5.6	Remediation Planned	Network Security Engineering Lead	Application VLAN → Dat	CWE-284
NET-021	MEDIUM	Insecure Monitoring Interface Exposes Sensitive Telemetry Without Authentication	6.1	Remediation Planned	Infrastructure Operations Lead	Application VLAN	CWE-306
NET-022	MEDIUM	Weak Internal TLS Configuration on Internal API Server	5.0	Remediation Planned	Backend/API Engineering Lead	Application VLAN	CWE-295
NET-023	MEDIUM	Kerberos Configuration Weakness — Unconstrained Delegation Enabled on Legacy Application Server	6.7	Remediation Planned	Active Directory Engineering Lead	Server VLAN	CWE-269
NET-024	MEDIUM	Excessive Privilege Assignment — Standard Support Accounts Present in Domain Admins Group	6.5	Remediation Planned	Active Directory Engineering Lead	Identity / AD VLAN	CWE-269
NET-025	MEDIUM	Weak Password Policy Permits Short, Non-Complex Domain Passwords	5.4	Remediation Planned	Active Directory Engineering Lead	Identity / AD VLAN	CWE-521

Finding ID	Severity	Title	CVSS	Status	Owner	Zone	CWE
NET-026	MEDIUM	Insecure Administrative Pathway — Helpdesk Staff Granted Direct RDP to Domain Controllers	6.3	Remediation Planned	Active Directory Engineering Lead	Identity / AD VLAN	CWE-284
NET-027	MEDIUM	Weak Corporate Wireless Configuration — Shared PSK Fallback Available Alongside 802.1X	4.8	Remediation Planned	Wireless Infrastructure Lead	Wireless — Corporate S	CWE-521
NET-028	LOW	Guest Wireless Network Isolation Weakness Permits Limited Reachability to Printer VLAN	3.4	Remediation Planned	Wireless Infrastructure Lead	Wireless — Guest SSID	CWE-923
NET-029	LOW	Insecure SNMP Configuration — SNMPv2c Enabled Alongside SNMPv3 on Distribution Switches	3.1	Remediation Planned	Network Operations Lead	Management VLAN	CWE-16
NET-030	LOW	Outdated Device Firmware on Wireless LAN Controller	3.7	Remediation Planned	Wireless Infrastructure Lead	Management VLAN	CWE-1104
NET-031	LOW	Configuration Backup Exposure — Unencrypted Device Configurations Stored on Shared Drive	3.9	Remediation Planned	Network Operations Lead	Server VLAN	CWE-312
NET-032	LOW	Weak Network-Device ACL Permits Broader Source Range Than Required for SSH Management	3.3	Remediation Planned	Network Operations Lead	Management VLAN	CWE-284
NET-033	LOW	Excessive Domain Information Disclosure via Unauthenticated LDAP Enumeration	3.6	Remediation Planned	Active Directory Engineering Lead	Identity / AD VLAN	CWE-200
NET-034	LOW	SYSVOL-Related Sensitive Configuration Reference in Legacy Logon Script	2.6	Remediation Planned	Active Directory Engineering Lead	Identity / AD VLAN (SY	CWE-200
NET-035	LOW	Overly Permissive VPN Trust Allows Split-Tunnel Access to Sensitive On-Prem Resources	3.8	Remediation Planned	Network Security Engineering Lead	External Perimeter / D	CWE-284
NET-036	LOW	Weak Hybrid Segmentation Between On-Prem Identity Sync Server and Cloud Management Path	3.5	Remediation Planned	Cloud & Hybrid Identity Lead	Server VLAN → Cloud /	CWE-284
NET-037	INFORMATIONAL	Positive Observation — Next-Generation Firewall Enforces Application-Aware Policy at External Perimeter	Informational	Observation Only	Network Security Engineering Lead	External Perimeter / D	N/A
NET-038	INFORMATIONAL	Positive Observation — Centralized Logging and SIEM Collection Implemented Across Core Infrastructure	Informational	Observation Only	Network Security Engineering Lead	Application VLAN	N/A

Finding ID	Severity	Title	CVSS	Status	Owner	Zone	CWE
NET-039	INFORMATIONAL	Positive Observation — Multi-Factor Authentication Enforced on Primary VPN Login Path	Informational	Observation Only	Network Security Engineering Lead	External Perimeter / D	N/A
NET-040	INFORMATIONAL	Recommendation — Adopt Privileged Access Workstations for Tier-0 Administrative Activity	Informational	Observation Only	Active Directory Engineering Lead	Server VLAN / Identity	N/A
NET-041	INFORMATIONAL	Recommendation — Formalize Network Segmentation Review Cadence	Informational	Observation Only	Network Security Engineering Lead	All internal zones	N/A
NET-042	INFORMATIONAL	Recommendation — Expand SIEM Detection Coverage for Lateral Movement Techniques	Informational	Observation Only	Network Security Engineering Lead	Application VLAN	N/A
NET-043	INFORMATIONAL	Informational — Management VLAN Naming Convention Inconsistent Across Network Documentation	Informational	Observation Only	Network Operations Lead	Management VLAN	N/A
NET-044	INFORMATIONAL	Informational — Legacy DNS Records Identified for Decommissioned Hosts	Informational	Observation Only	Network Security Engineering Lead	External Perimeter / D	N/A
NET-045	INFORMATIONAL	Recommendation — Implement Network Access Control (802.1X) on Wired User Ports	Informational	Observation Only	Network Operations Lead	User Workstation VLAN	N/A
NET-046	INFORMATIONAL	Recommendation — Establish Formal Firewall Rule Review and Recertification Process	Informational	Observation Only	Network Security Engineering Lead	All zones	N/A

APPENDIX I — EVIDENCE REGISTER

The register below documents all 49 fictional evidence references cited throughout the detailed findings, mapped to the finding each item supports. All evidence is synthetic and constructed for this illustrative assessment.

Evidence ID	Type	Description	Finding
EV-NET-001	Authentication Capture	Fictional evidence supporting NET-001 (External VPN Authentication Can Be Bypassed Through Legacy Authentication Workflow).	NET-001
EV-NET-002	Configuration Excerpt	Fictional evidence supporting NET-001 (External VPN Authentication Can Be Bypassed Through Legacy Authentication Workflow).	NET-001
EV-NET-003	Port Reachability Scan	Fictional evidence supporting NET-002 (Insufficient Internal Network Segmentation Enables Unauthenticated Reachability from User VLAN to Database VLAN).	NET-002
EV-NET-004	Firewall Policy Excerpt	Fictional evidence supporting NET-002 (Insufficient Internal Network Segmentation Enables Unauthenticated Reachability from User VLAN to Database VLAN).	NET-002
EV-NET-005	SYSVOL File Extraction	Fictional evidence supporting NET-003 (Privileged Active Directory Service Account Credential Exposed Through Insecure Group Policy Preferences Configuration).	NET-003
EV-NET-006	Credential Validation Test	Fictional evidence supporting NET-003 (Privileged Active Directory Service Account Credential Exposed Through Insecure Group Policy Preferences Configuration).	NET-003
EV-NET-007	Management-Plane Reachability Scan	Fictional evidence supporting NET-004 (Exposed Management Plane Enables Administrative Access to Core Network Devices from User VLAN).	NET-004
EV-NET-008	Credential Authentication Test	Fictional evidence supporting NET-004 (Exposed Management Plane Enables Administrative Access to Core Network Devices from User VLAN).	NET-004
EV-NET-009	SMB Protocol Negotiation Capture	Fictional evidence supporting NET-005 (SMB Signing Not Enforced on Critical Internal Windows Servers).	NET-005
EV-NET-010	LDAP Traffic Capture	Fictional evidence supporting NET-006 (Insecure LDAP Configuration Permits Credential Exposure via Unsigned, Unencrypted Bind).	NET-006
EV-NET-011	Local Group Enumeration	Fictional evidence supporting NET-007 (Excessive Administrative Access Across User Network Segment via Helpdesk Group Policy).	NET-007
EV-NET-012	IKE Negotiation Capture	Fictional evidence supporting NET-008 (Weak VPN Security Configuration Permits Legacy Cryptographic Negotiation).	NET-008
EV-NET-013	SNMP Enumeration	Fictional evidence supporting NET-009 (SNMP Community String Configuration Exposes Network Device Information).	NET-009
EV-NET-014	Port Reachability Scan	Fictional evidence supporting NET-010 (RDP Accessible Across Improperly Segmented Network Boundaries).	NET-010

Evidence ID	Type	Description	Finding
EV-NET-015	Network Reachability Test	Fictional evidence supporting NET-011 (Insecure Firewall Rule Permits Management-Plane Access From Corporate Wireless Segment).	NET-011
EV-NET-016	SMB Share Access Test	Fictional evidence supporting NET-012 (Sensitive Backup Repository Reachable From User VLAN Without Authentication Segmentation).	NET-012
EV-NET-017	Kerberos Ticket Enumeration	Fictional evidence supporting NET-013 (Weak Service Account Security Enables Lateral Movement via Kerberoasting).	NET-013
EV-NET-018	TLS Configuration Scan	Fictional evidence supporting NET-014 (Outdated TLS Configuration on External Remote Access Portal).	NET-014
EV-NET-019	Certificate Inspection	Fictional evidence supporting NET-015 (Certificate Configuration Issue on External VPN Gateway).	NET-015
EV-NET-020	DNS Zone Transfer Capture	Fictional evidence supporting NET-016 (DNS Configuration Weakness Permits Zone Transfer from External DNS Server).	NET-016, NET-044
EV-NET-021	Service Reachability Scan	Fictional evidence supporting NET-017 (Exposed Service With Unnecessary Functionality on External Load Balancer).	NET-017
EV-NET-022	HTTP Error Response Capture	Fictional evidence supporting NET-018 (Information Disclosure Through Verbose Error Messages on Public Web Application Gateway).	NET-018
EV-NET-023	SMB Protocol Negotiation Capture	Fictional evidence supporting NET-019 (Legacy/Insecure Protocol Exposure — SMBv1 Still Enabled on Internal File Server).	NET-019
EV-NET-024	Port Reachability Scan	Fictional evidence supporting NET-020 (Unnecessary East-West Connectivity Between Application VLAN and Database VLAN Beyond Required Ports).	NET-020
EV-NET-025	Unauthenticated Access Test	Fictional evidence supporting NET-021 (Insecure Monitoring Interface Exposes Sensitive Telemetry Without Authentication).	NET-021
EV-NET-026	TLS Interception Test	Fictional evidence supporting NET-022 (Weak Internal TLS Configuration on Internal API Server).	NET-022
EV-NET-027	AD Computer Object Review	Fictional evidence supporting NET-023 (Kerberos Configuration Weakness — Unconstrained Delegation Enabled on Legacy Application Server).	NET-023
EV-NET-028	Privileged Group Enumeration	Fictional evidence supporting NET-024 (Excessive Privilege Assignment — Standard Support Accounts Present in Domain Admins Group).	NET-024
EV-NET-029	Group Policy Review	Fictional evidence supporting NET-025 (Weak Password Policy Permits Short, Non-Complex Domain Passwords).	NET-025
EV-NET-030	Logon Rights Review	Fictional evidence supporting NET-026 (Insecure Administrative Pathway — Helpdesk Staff Granted Direct RDP to Domain Controllers).	NET-026
EV-NET-031	Wireless Configuration Review	Fictional evidence supporting NET-027 (Weak Corporate Wireless Configuration — Shared PSK Fallback Available Alongside 802.1X).	NET-027
EV-NET-032	Wireless Reachability Test	Fictional evidence supporting NET-028 (Guest Wireless Network Isolation Weakness Permits Limited Reachability to Printer VLAN).	NET-028

Evidence ID	Type	Description	Finding
EV-NET-033	SNMP Enumeration	Fictional evidence supporting NET-029 (Insecure SNMP Configuration — SNMPv2c Enabled Alongside SNMPv3 on Distribution Switches).	NET-029
EV-NET-034	Firmware Version Check	Fictional evidence supporting NET-030 (Outdated Device Firmware on Wireless LAN Controller).	NET-030
EV-NET-035	File Share Review	Fictional evidence supporting NET-031 (Configuration Backup Exposure — Unencrypted Device Configurations Stored on Shared Drive).	NET-031
EV-NET-036	ACL Configuration Review	Fictional evidence supporting NET-032 (Weak Network-Device ACL Permits Broader Source Range Than Required for SSH Management).	NET-032
EV-NET-037	LDAP Anonymous Bind Test	Fictional evidence supporting NET-033 (Excessive Domain Information Disclosure via Unauthenticated LDAP Enumeration).	NET-033
EV-NET-038	SYSVOL Script Review	Fictional evidence supporting NET-034 (SYSVOL-Related Sensitive Configuration Reference in Legacy Logon Script).	NET-034
EV-NET-039	VPN Client Profile Review	Fictional evidence supporting NET-035 (Overly Permissive VPN Trust Allows Split-Tunnel Access to Sensitive On-Prem Resources).	NET-035
EV-NET-040	Outbound Connectivity Review	Fictional evidence supporting NET-036 (Weak Hybrid Segmentation Between On-Prem Identity Sync Server and Cloud Management Path).	NET-036
EV-NET-041	Firewall Policy Validation Test	Fictional evidence supporting NET-037 (Positive Observation — Next-Generation Firewall Enforces Application-Aware Policy at External Perimeter).	NET-037
EV-NET-042	SIEM Ingestion Validation	Fictional evidence supporting NET-038 (Positive Observation — Centralized Logging and SIEM Collection Implemented Across Core Infrastructure).	NET-038
EV-NET-043	MFA Enforcement Test	Fictional evidence supporting NET-039 (Positive Observation — Multi-Factor Authentication Enforced on Primary VPN Login Path).	NET-039
EV-NET-044	Interview Notes	Fictional evidence supporting NET-040 (Recommendation — Adopt Privileged Access Workstations for Tier-0 Administrative Activity).	NET-040
EV-NET-045	Interview / Process Review	Fictional evidence supporting NET-041 (Recommendation — Formalize Network Segmentation Review Cadence).	NET-041
EV-NET-046	Interview / Detection Content Review	Fictional evidence supporting NET-042 (Recommendation — Expand SIEM Detection Coverage for Lateral Movement Techniques).	NET-042
EV-NET-047	Documentation Review	Fictional evidence supporting NET-043 (Informational — Management VLAN Naming Convention Inconsistent Across Network Documentation).	NET-043
EV-NET-048	Configuration Review	Fictional evidence supporting NET-045 (Recommendation — Implement Network Access Control (802.1X) on Wired User Ports).	NET-045
EV-NET-049	Interview / Process Review	Fictional evidence supporting NET-046 (Recommendation — Establish Formal Firewall Rule Review and Recertification Process).	NET-046

APPENDIX J — REMEDIATION PRIORITY MATRIX

Finding ID	Severity	Title	Priority	Owner	Target Date	Status
NET-001	CRITICAL	External VPN Authentication Can Be Bypassed Through Legacy Authentication Workflow	Immediate — 0-30 Days	Network Security Engineering Lead	10 October 2026	Remediation In Progress
NET-002	CRITICAL	Insufficient Internal Network Segmentation Enables Unauthenticated Reachability from User VLAN to Database VLAN	Immediate — 0-30 Days	Network Security Engineering Lead	10 October 2026	Remediation In Progress
NET-003	CRITICAL	Privileged Active Directory Service Account Credential Exposed Through Insecure Group Policy Preferences Configuration	Immediate — 0-30 Days	Active Directory Engineering Lead	10 October 2026	Remediation In Progress
NET-004	CRITICAL	Exposed Management Plane Enables Administrative Access to Core Network Devices from User VLAN	Immediate — 0-30 Days	Network Operations Lead	10 October 2026	Remediation In Progress
NET-005	HIGH	SMB Signing Not Enforced on Critical Internal Windows Servers	31-60 Days	Active Directory Engineering Lead	09 November 2026	Remediation Planned
NET-006	HIGH	Insecure LDAP Configuration Permits Credential Exposure via Unsigned, Unencrypted Bind	31-60 Days	Active Directory Engineering Lead	09 November 2026	Remediation Planned
NET-007	HIGH	Excessive Administrative Access Across User Network Segment via Helpdesk Group Policy	31-60 Days	IT Service Desk Manager	09 November 2026	Remediation Planned
NET-008	HIGH	Weak VPN Security Configuration Permits Legacy Cryptographic Negotiation	31-60 Days	Network Security Engineering Lead	09 November 2026	Remediation Planned
NET-009	HIGH	SNMP Community String Configuration Exposes Network Device Information	31-60 Days	Network Operations Lead	09 November 2026	Remediation Planned
NET-010	HIGH	RDP Accessible Across Improperly Segmented Network Boundaries	31-60 Days	Network Security Engineering Lead	09 November 2026	Remediation Planned
NET-011	HIGH	Insecure Firewall Rule Permits Management-Plane Access From Corporate Wireless Segment	31-60 Days	Wireless Infrastructure Lead	09 November 2026	Remediation Planned
NET-012	HIGH	Sensitive Backup Repository Reachable From User VLAN Without Authentication Segmentation	31-60 Days	Infrastructure Operations Lead	09 November 2026	Remediation Planned

Finding ID	Severity	Title	Priority	Owner	Target Date	Status
NET-013	HIGH	Weak Service Account Security Enables Lateral Movement via Kerberoasting	31-60 Days	Active Directory Engineering Lead	09 November 2026	Remediation Planned
NET-014	MEDIUM	Outdated TLS Configuration on External Remote Access Portal	61-90 Days	Network Security Engineering Lead	09 December 2026	Remediation Planned
NET-015	MEDIUM	Certificate Configuration Issue on External VPN Gateway	61-90 Days	Network Security Engineering Lead	09 December 2026	Remediation Planned
NET-016	MEDIUM	DNS Configuration Weakness Permits Zone Transfer from External DNS Server	61-90 Days	Network Security Engineering Lead	09 December 2026	Remediation Planned
NET-017	MEDIUM	Exposed Service With Unnecessary Functionality on External Load Balancer	61-90 Days	Network Security Engineering Lead	09 December 2026	Remediation Planned
NET-018	MEDIUM	Information Disclosure Through Verbose Error Messages on Public Web Application Gateway	61-90 Days	Backend/API Engineering Lead	09 December 2026	Remediation Planned
NET-019	MEDIUM	Legacy/Insecure Protocol Exposure — SMBv1 Still Enabled on Internal File Server	61-90 Days	Infrastructure Operations Lead	09 December 2026	Remediation Planned
NET-020	MEDIUM	Unnecessary East-West Connectivity Between Application VLAN and Database VLAN Beyond Required Ports	61-90 Days	Network Security Engineering Lead	09 December 2026	Remediation Planned
NET-021	MEDIUM	Insecure Monitoring Interface Exposes Sensitive Telemetry Without Authentication	61-90 Days	Infrastructure Operations Lead	09 December 2026	Remediation Planned
NET-022	MEDIUM	Weak Internal TLS Configuration on Internal API Server	61-90 Days	Backend/API Engineering Lead	09 December 2026	Remediation Planned
NET-023	MEDIUM	Kerberos Configuration Weakness — Unconstrained Delegation Enabled on Legacy Application Server	61-90 Days	Active Directory Engineering Lead	09 December 2026	Remediation Planned
NET-024	MEDIUM	Excessive Privilege Assignment — Standard Support Accounts Present in Domain Admins Group	61-90 Days	Active Directory Engineering Lead	09 December 2026	Remediation Planned
NET-025	MEDIUM	Weak Password Policy Permits Short, Non-Complex Domain Passwords	61-90 Days	Active Directory Engineering Lead	09 December 2026	Remediation Planned
NET-026	MEDIUM	Insecure Administrative Pathway — Helpdesk Staff Granted Direct RDP to Domain Controllers	61-90 Days	Active Directory Engineering Lead	09 December 2026	Remediation Planned

Finding ID	Severity	Title	Priority	Owner	Target Date	Status
NET-027	MEDIUM	Weak Corporate Wireless Configuration — Shared PSK Fallback Available Alongside 802.1X	61-90 Days	Wireless Infrastructure Lead	09 December 2026	Remediation Planned
NET-028	LOW	Guest Wireless Network Isolation Weakness Permits Limited Reachability to Printer VLAN	90+ Days	Wireless Infrastructure Lead	31 January 2027	Remediation Planned
NET-029	LOW	Insecure SNMP Configuration — SNMPv2c Enabled Alongside SNMPv3 on Distribution Switches	90+ Days	Network Operations Lead	31 January 2027	Remediation Planned
NET-030	LOW	Outdated Device Firmware on Wireless LAN Controller	90+ Days	Wireless Infrastructure Lead	31 January 2027	Remediation Planned
NET-031	LOW	Configuration Backup Exposure — Unencrypted Device Configurations Stored on Shared Drive	90+ Days	Network Operations Lead	31 January 2027	Remediation Planned
NET-032	LOW	Weak Network-Device ACL Permits Broader Source Range Than Required for SSH Management	90+ Days	Network Operations Lead	31 January 2027	Remediation Planned
NET-033	LOW	Excessive Domain Information Disclosure via Unauthenticated LDAP Enumeration	90+ Days	Active Directory Engineering Lead	31 January 2027	Remediation Planned
NET-034	LOW	SYSVOL-Related Sensitive Configuration Reference in Legacy Logon Script	90+ Days	Active Directory Engineering Lead	31 January 2027	Remediation Planned
NET-035	LOW	Overly Permissive VPN Trust Allows Split-Tunnel Access to Sensitive On-Prem Resources	90+ Days	Network Security Engineering Lead	31 January 2027	Remediation Planned
NET-036	LOW	Weak Hybrid Segmentation Between On-Prem Identity Sync Server and Cloud Management Path	90+ Days	Cloud & Hybrid Identity Lead	31 January 2027	Remediation Planned
NET-037	INFORMATIONAL	Positive Observation — Next-Generation Firewall Enforces Application-Aware Policy at External Perimeter	N/A — Informational	Network Security Engineering Lead	N/A	Observation Only
NET-038	INFORMATIONAL	Positive Observation — Centralized Logging and SIEM Collection Implemented Across Core Infrastructure	N/A — Informational	Network Security Engineering Lead	N/A	Observation Only
NET-039	INFORMATIONAL	Positive Observation — Multi-Factor Authentication Enforced on Primary VPN Login Path	N/A — Informational	Network Security Engineering Lead	N/A	Observation Only
NET-040	INFORMATIONAL	Recommendation — Adopt Privileged Access Workstations for Tier-0 Administrative Activity	N/A — Informational	Active Directory Engineering Lead	N/A	Observation Only

Finding ID	Severity	Title	Priority	Owner	Target Date	Status
NET-041	INFORMATIONAL	Recommendation — Formalize Network Segmentation Review Cadence	N/A — Informational	Network Security Engineering Lead	N/A	Observation Only
NET-042	INFORMATIONAL	Recommendation — Expand SIEM Detection Coverage for Lateral Movement Techniques	N/A — Informational	Network Security Engineering Lead	N/A	Observation Only
NET-043	INFORMATIONAL	Informational — Management VLAN Naming Convention Inconsistent Across Network Documentation	N/A — Informational	Network Operations Lead	N/A	Observation Only
NET-044	INFORMATIONAL	Informational — Legacy DNS Records Identified for Decommissioned Hosts	N/A — Informational	Network Security Engineering Lead	N/A	Observation Only
NET-045	INFORMATIONAL	Recommendation — Implement Network Access Control (802.1X) on Wired User Ports	N/A — Informational	Network Operations Lead	N/A	Observation Only
NET-046	INFORMATIONAL	Recommendation — Establish Formal Firewall Rule Review and Recertification Process	N/A — Informational	Network Security Engineering Lead	N/A	Observation Only

APPENDIX K — TEST ACCOUNTS / FICTIONAL IDENTITIES

All accounts below are fictional and were provisioned solely for this illustrative assessment; no real credentials are disclosed.

Account (Fictional)	Type	Privilege Level	Purpose
fictional.user01	Standard Domain User	Standard	Assumed-breach internal testing baseline account.
svc-legacyapp	Service Account	Standard (SPN-registered)	Kerberoasting / SPN enumeration testing (NET-013).
helpdesk.test01	Helpdesk-All Member	Standard + Local Admin (fleet-wide)	Privilege escalation testing (NET-007).
vpn.test.user	VPN / Domain User	Standard	External VPN authentication testing (NET-001, NET-008).
fictional.readonly	LDAP Bind Account	Read-Only	LDAP configuration and enumeration testing (NET-006, NET-033).
guest.wifi.test	Guest Wireless Client	Unauthenticated / Guest	Wireless segmentation testing (NET-028).

APPENDIX L — TECHNOLOGY / SOFTWARE INVENTORY

Technology / Platform	Representative Roles
Embedded print OS (fictional)	Floor 3 shared print/scan device
Linux (BIND-style)	Authoritative DNS for northstar-example.com
Linux (EDR console)	Endpoint detection and response management plane
Linux (NMS appliance)	Centralized configuration, monitoring, and firmware management
Linux (WAF appliance)	Fronts public-facing web applications

Technology / Platform	Representative Roles
Linux (backup appliance)	Enterprise backup repository for AD, database, and file server data
Linux (cloud management jump)	Administrative path to fictional cloud tenant management plane
Linux (fictional distribution)	Centralized log aggregation and correlation platform, Customer-facing payments p
Linux (hardened jump host)	Administrative jump host for external vendor and remote admin access
Linux (load balancer appliance)	TLS termination and load distribution for public services
Linux (mail security appliance)	Inbound/outbound mail filtering — mail.northstar-example.com
Linux (reverse proxy)	Employee/partner remote access portal — portal.northstar-example.com
Linux (scanner appliance)	Authenticated/unauthenticated internal vulnerability scanning platform
Vendor AP OS (fictional)	Representative access point serving Corporate + Guest SSIDs, Harrisonville-patte
Vendor NGFW OS (fictional)	External perimeter firewall / primary internet edge, IPsec tunnel termination to
Vendor NOS (fictional)	Core network switching fabric / management VIP, Distribution-layer switch — serv
Vendor SSL-VPN Appliance (fictional)	Remote-access VPN gateway — vpn.northstar-example.com
Vendor Wireless OS (fictional)	Centralized control plane for corporate/guest/management SSIDs
Windows 11 Enterprise (fictional build)	Finance department workstation — assumed-breach test host, IT helpdesk / Tier-1
Windows Server (fictional build)	Active Directory-integrated internal DNS, Departmental and corporate file shares
Windows Server / RDBMS (fictional build)	Core banking and payments transactional data store, Reporting warehouse replicat

APPENDIX M — METHODOLOGY TRACEABILITY

Methodology Phase	Report Section Reference
Pre-Engagement	Section 04 (Rules of Engagement)
Reconnaissance	Section 08 (External Attack Surface)
Attack Surface Discovery	Appendix B (Asset Register)
Service Enumeration	Appendix C (Service/Port Register)
Vulnerability Analysis	Sections 11-16, 19-23
Configuration Review	Sections 13-15
Authentication Testing	Section 11, NET-001, NET-006, NET-025
Network Segmentation Testing	Section 10, Appendix E
Active Directory Security Assessment	Section 13, Appendix F
Lateral Movement Assessment	Section 17, Appendix N
Privilege Escalation Assessment	Section 17, NET-003, NET-007, NET-023
Controlled Exploitation	Sections 19-20 (Critical/High evidence panels)
Evidence Collection	Appendix I (Evidence Register)
Risk Rating	Section 06
Remediation	Sections 24-25, Appendix J
Retest	Section 26

APPENDIX N — ATTACK PATH REGISTER

Path ID	Name	Steps	Findings Involved
AP-01	External to Domain-Level Impact	Internet → VPN Gateway → User VLAN → Database VLAN → Active Directory → Domain-Level Impact	NET-001, NET-002, NET-003
AP-02	Assumed-Breach Lateral Movement	Compromised Workstation → Internal Enumeration → SMB/LDAP Discovery → Credential Exposure → Privileged Server → Management-Plane Access → Network Device Compromise	NET-005, NET-006, NET-010, NET-013, NET-004
AP-03	Wireless to Management Plane	Corporate Wireless SSID → Management VLAN (overly broad firewall object) → Default Credential Authentication → Network Device Compromise	NET-011, NET-004

APPENDIX O — GLOSSARY

Term	Definition
AD	Active Directory — Microsoft's directory service for Windows domain networks.
ACL	Access Control List — a set of rules controlling network or resource access.
AXFR	A DNS zone transfer request used to replicate an entire DNS zone.
CVSS	Common Vulnerability Scoring System — a framework for rating vulnerability severity.
CWE	Common Weakness Enumeration — a categorization of software/configuration weakness types.
DMZ	Demilitarized Zone — a network segment exposed to untrusted networks, isolated from internal systems.
gMSA	Group Managed Service Account — an Active Directory account type with automated password management.
IKE	Internet Key Exchange — the protocol used to negotiate IPsec VPN security associations.
Kerberoasting	A technique for requesting and offline-cracking Kerberos service tickets to recover service account credentials.
LAPS	Local Administrator Password Solution — a Microsoft tool for managing unique, rotated local admin passwords.
LDAP	Lightweight Directory Access Protocol — used to query and modify directory service information.
MFA	Multi-Factor Authentication — authentication requiring two or more independent verification factors.
NLA	Network Level Authentication — a pre-session authentication requirement for RDP.
NTLM Relay	An attack technique relaying captured NTLM authentication to another service to gain unauthorized access.
PAW	Privileged Access Workstation — a hardened, dedicated workstation used only for administrative activity.
PSK	Pre-Shared Key — a shared secret used for authentication, commonly in VPN or wireless configurations.
PTES	Penetration Testing Execution Standard — a widely referenced methodology framework for penetration testing engagements.
RBCD	Resource-Based Constrained Delegation — a Kerberos delegation model scoped to specific target resources.
SIEM	Security Information and Event Management — a platform for centralized log collection, correlation, and alerting.
SNMP	Simple Network Management Protocol — used for monitoring and managing network devices.
SPN	Service Principal Name — a unique identifier for a service instance used in Kerberos authentication.
SYSVOL	A shared Active Directory folder used to replicate Group Policy and logon script data across domain controllers.
TLS	Transport Layer Security — the cryptographic protocol securing network communications.
VLAN	Virtual Local Area Network — a logically segmented broadcast domain within a physical network.
WAF	Web Application Firewall — a control that filters and monitors HTTP traffic to a web application.
WIDS/WIPS	Wireless Intrusion Detection/Prevention System — monitors for and responds to unauthorized wireless activity.

APPENDIX P — CONTACT & DISCLAIMER

Contact (Fictional)

Role	Contact (Fictional)
Engagement Manager	David Okafor — TMG Security (fictional contact)
Technical Lead	Daniel Reyes — TMG Security (fictional contact)
General Inquiries	TMG Security — www.tmgsecurity.example (fictional, non-resolving)

Final Disclaimer

FICTIONAL SAMPLE — NOT AN ACTUAL CLIENT NETWORK PENETRATION TEST

All systems, IP addresses, hostnames, credentials, configurations, screenshots, command output, vulnerabilities, findings, and evidence shown in this document are fictional or synthetic and are provided solely for demonstration purposes. No real client infrastructure was tested. TMG Security is not claiming that the fictional vulnerabilities shown in this report exist in any real organization.