TechGeeks Consulting

Security & Infrastructure Decision Brief

Northstar Distribution

Document ID: OD-07 / SAMPLE-001
Prepared by: TechGeeks Consulting
Date: August 21, 2026
Classification: Illustrative—Not Client Work
Status: Synthetic sample

> Northstar Distribution is fictional. Every organization, system, observation, metric, address, finding, and outcome in this document was created solely to demonstrate deliverable structure. This is not a client report, testimonial, compliance assessment, or representation of work performed.

Document control

Field	Value
Document owner	TechGeeks Consulting
Engagement	Fictional infrastructure assessment and roadmap
Version	1.0
Date	August 21, 2026
Classification	Illustrative—Not Client Work
Distribution	Public sample; contains no real client information

Revision history

Version	Date	Author	Summary
1.0	August 21, 2026	TechGeeks Consulting	Initial synthetic sample

Executive decision

Northstar Distribution's twelve-site network can support its planned cloud and branch modernization, but the organization should define the security and operating architecture before selecting an SD-WAN platform or beginning a broad refresh.

The most consequential issue is not a single device or product. Trust boundaries, wireless access, WAN paths, internet egress, identity, monitoring, and site standards have evolved independently. A platform purchase made before these decisions are resolved would automate inconsistency and make future controls harder to explain and operate.

Recommended direction

Adopt a **security-integrated hybrid edge architecture** using standardized site tiers, identity-informed access, explicit trust zones, dual transport for critical sites, application-aware path policy, controlled local internet breakout, centralized visibility, and phased migration validation.

Security should be baked into the requirements, topology, access model, routing policy, and operating standard from the first design decision—not bolted on after connectivity is deployed.

Decision snapshot

Priority	Decision/action	Why it matters	Owner	Target
1	Approve trust-zone and traffic-policy model before platform selection	Establishes what the network must enforce	Security + Network Architecture	30 days
2	Approve three site tiers and resilience requirements	Prevents every location from becoming a custom design	Infrastructure	30 days
3	Pilot hybrid SD-WAN and controlled local breakout at two representative sites	Validates application, security, carrier, and operational assumptions	Network Operations	60–90 days
4	Standardize corporate, guest, and operational-device access	Reduces inconsistent wireless and wired trust decisions	Security + Endpoint + Network	90 days
5	Establish configuration, telemetry, and failover evidence as acceptance criteria	Makes resilience and supportability testable	Operations	Before rollout

Environment and objective

Fictional context

Northstar operates one headquarters, two distribution centers, and nine branch locations. The environment uses a mix of private WAN circuits and site internet connections. Most cloud traffic returns through headquarters. Campus and wireless configurations vary by site generation. The organization plans to move additional business applications to SaaS and IaaS over the next year.

Objectives

1. Determine whether the current architecture can support cloud growth and site resilience requirements.
2. Identify security and operational decisions that must precede SD-WAN procurement.
3. Define a repeatable campus, wireless, network security, and WAN target state.
4. Establish a phased modernization roadmap that the internal team can own.

Scope

Included	Boundary
Current-state architecture	Headquarters, two distribution centers, nine branches, cloud and internet edges
Network security	Segmentation, access, administrative paths, egress, logging, and trust relationships
Campus and wireless	Site patterns, authentication, corporate/guest/operational-device access
WAN and SD-WAN readiness	Topology, transport, path policy, resilience, cloud access, and migration dependencies
Operations	Configuration control, monitoring, documentation, lifecycle, ownership, and acceptance

Excluded: penetration testing, physical RF survey, carrier procurement, detailed implementation configuration, legal compliance opinion, and production change.

Evidence reviewed

This synthetic sample assumes the following fictional evidence set:

Evidence ID	Source	Coverage	Confidence
NS-EV-001	Logical topology and circuit inventory	12 sites; last revised 14 months earlier	Medium
NS-EV-002	Sanitized firewall and routing exports	Headquarters and distribution centers	High for captured state
NS-EV-003	Wireless configuration summaries	8 of 12 sites	Medium
NS-EV-004	Monitoring and incident summaries	Prior six months	Medium
NS-EV-005	Stakeholder working sessions	Security, infrastructure, service desk, applications	High for stated requirements
NS-EV-006	Controlled failover observation	One branch and one distribution center	High for tested scenarios only

Evidence gaps and scope limitations are carried into each conclusion rather than hidden.

Architecture observations

A-01 — Trust policy is implicit in device and firewall history

Decision priority: High
Affected scope: Corporate users, warehouse devices, guest access, management interfaces, shared services
Validation status: Supported by configuration review and stakeholder confirmation

Observation

Network segments exist, but a current trust-zone model does not define which user, device, application, and administrative relationships should be permitted. Similar device classes are placed differently across site generations, and exceptions are represented primarily in individual configurations.

Why it matters

SD-WAN, wireless refresh, network access control, and firewall changes will each require the same trust decisions. Without an owned model, migration may reproduce inconsistent access and create unclear enforcement responsibility.

Recommendation

Approve a trust-zone model covering corporate users, administrators, servers, warehouse/operational devices, guest access, network management, and shared services. Record permitted relationships, enforcement points, exceptions, logging, and policy ownership before product configuration begins.

A-02 — Resilience exists as components but not as a tested service behavior

Decision priority: High
Affected scope: Distribution centers and six revenue-dependent branches
Validation status: Partially validated; two controlled scenarios observed

Observation

Several sites have two circuits, but routing convergence, DNS dependencies, security inspection paths, application session behavior, and operational response are not covered by a common acceptance test. One observed branch retained internet reachability during circuit failure but lost access to a required internal name-resolution service.

Why it matters

Carrier or appliance redundancy does not by itself establish application continuity. A future SD-WAN design needs service-level failure requirements and evidence, not only dual links.

Recommendation

Define site-tier availability requirements, failure scenarios, recovery expectations, dependency maps, monitoring signals, and acceptance tests. Require pilot evidence before broad rollout.

A-03 — Wireless access differs by site generation

Decision priority: Medium
Affected scope: Corporate, guest, handheld, scanner, and operational-device wireless access
Validation status: Supported for eight reviewed sites; four-site evidence gap

Observation

SSID purpose, authentication method, guest isolation, device onboarding, and VLAN mapping differ across site generations. Operational devices with limited authentication capability are handled through local exceptions that are not centrally inventoried.

Why it matters

Inconsistent identity and segmentation decisions increase support effort and make risk dependent on location. A wireless platform refresh alone will not resolve the policy inconsistency.

Recommendation

Define a wireless design basis and exception process by device class. Standardize corporate, guest, and operational-device patterns, authentication dependencies, segmentation, monitoring, and lifecycle ownership.

A-04 — Architecture and configuration evidence is not maintained as an operating asset

Decision priority: Medium
Affected scope: Network and security operations
Validation status: Supported by document/configuration comparison

Observation

Topology, circuit, configuration, and dependency records use different identifiers and update rhythms. Current state had to be reconstructed through interviews and configuration exports.

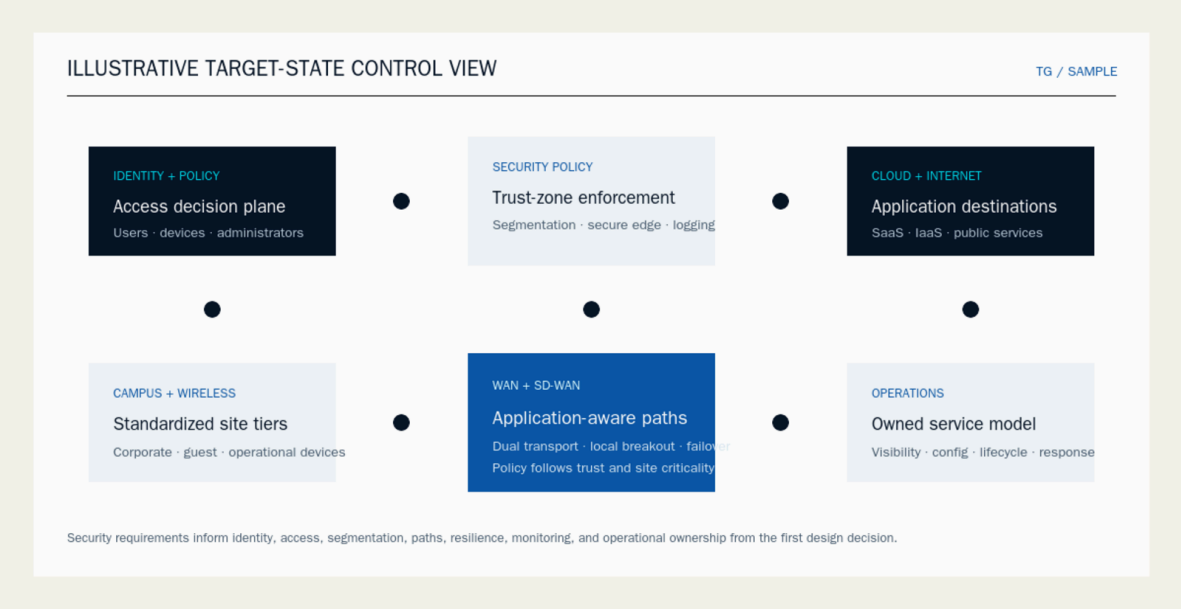
Why it matters

Modernization, incident response, troubleshooting, and change review all depend on a reliable representation of the environment. A new platform would not automatically create ownership or documentation discipline.

Recommendation

Establish authoritative sources for devices, circuits, topology, configuration, ownership, and site standards. Include evidence currency and configuration recovery in operational acceptance.

Target-state control view



Illustrative target-state architecture

Architecture principles

1. **Security by design:** Trust, identity, enforcement, visibility, and administrative boundaries are requirements from the beginning.
2. **Site tiers over site exceptions:** Repeatable patterns with an explicit exception owner.
3. **Application-aware resilience:** Failure behavior is defined and tested at the service level.
4. **Local access with controlled policy:** Cloud and internet paths follow segmentation, inspection, identity, and logging requirements.
5. **Operations is part of the architecture:** Monitoring, configuration, lifecycle, documentation, support, and rollback are designed—not deferred.

Options considered

Option	Security fit	Resilience/performance	Operational effect	Migration risk	Disposition
A — Refresh existing private-WAN model	Supports central controls but retains implicit trust and backhaul dependence	Familiar; cloud path remains inefficient	Lowest near-term process change	Defers key design decisions	Not recommended as target state
B — SD-WAN with centralized internet/security only	Improves path control and circuit diversity	Cloud traffic may still depend on central edges	Moderate platform change	Could preserve concentration risk	Viable transitional pattern
C — Hybrid SD-WAN with security-integrated local breakout	Strongest fit when trust zones, secure edge, and identity are defined together	Best alignment to cloud and site tiers	Requires stronger policy, visibility, and operations	Higher design discipline; phased pilot reduces risk	**Recommended, subject to pilot**

Architecture decision record

Decision: Proceed to requirements and pilot for Option C, hybrid SD-WAN with security-integrated local breakout.
Status: Proposed—requires sponsor approval and pilot evidence
Context: Cloud adoption, site growth, inconsistent wireless/access patterns, and incomplete resilience evidence.
Requirements: Explicit trust zones, identity dependencies, approved application classes, dual transport by site tier, secure local internet path, centralized logging, configuration recovery, and tested failover.
Tradeoffs: The recommended direction improves cloud access and path flexibility but increases the importance of policy governance, edge security consistency, telemetry, and operational readiness.
Dependencies: Identity and DNS design, security policy, circuit inventory, provider requirements, application testing, site readiness, monitoring, and support ownership.
Reversibility: Use two representative pilots with coexistence and rollback. Do not commit all sites before acceptance criteria are met.
Next action: Approve requirements workshop and pilot scope; owner: Infrastructure Director; target: 30 days.

Phased roadmap

Horizon	Action	Dependency	Owner	Success evidence
0–30 days	Approve trust-zone, site-tier, application, and resilience requirements	Security, applications, operations participation	Architecture council	Signed requirements and decision record
0–30 days	Reconcile site, circuit, device, and dependency inventory	Authoritative owners and identifiers	Network Operations	Inventory confidence and gap register
30–60 days	Define pilot design, provider constraints, rollback, and acceptance tests	Requirements approved	Network Architecture	Approved high-level design and ROE/change plan
60–90 days	Pilot one branch and one distribution center	Equipment, circuits, change windows	Delivery team	Application, failover, security, telemetry evidence
90–120 days	Resolve pilot findings and approve rollout standard	Pilot acceptance	Architecture council	Accepted standard and exception process
120–180 days	Begin phased site migration by tier	Site readiness and operations capacity	Program owner	Wave acceptance and controlled rollback record

Measures that matter

- Percentage of sites conforming to an approved reference pattern
- Percentage of user/device classes mapped to an owned trust policy
- Critical application success during approved failure scenarios
- Configuration backup currency and tested restoration
- Time to identify site path, policy, and ownership during an incident
- Open exceptions with owner, rationale, expiration, and review status

Assumptions and limitations

- This is a synthetic example and no real environment was assessed.
- A real engagement would validate exact application flows, provider policies, configurations, site constraints, and ownership.

- The sample does not select a vendor or assert product capability.
- No penetration testing, RF survey, performance benchmark, carrier analysis, cost model, or compliance assessment is represented.
- Priority reflects the fictional decision context, not a universal risk rating.

Closeout record

Item	Illustrative disposition
Executive decision	Pending sponsor approval
Material factual corrections	None—synthetic sample
Evidence repository	Contains synthetic source records only
Credentials/test artifacts	Not applicable
Retention	Public sample retained; no client data
Next decision	Approve requirements and pilot scope

Capability context

This sample demonstrates how **Infrastructure & Network Architecture Advisory** can connect network security architecture, wireless and campus design, WAN and SD-WAN strategy, resilience, operations, and migration planning. A real engagement may also incorporate Security & Risk Assessments, Penetration Testing & Security Validation, or Vulnerability Assessment & Management when explicitly scoped.

Sample control: OD-07 · Version 1.0 · Illustrative—Not Client Work · TechGeeks Consulting · techgeeks.cc