anm

PRACTICAL STEPS TO BUILDING A MODERN NETWORK WITH SD-WAN & SASE

EBOOK

OUR BIGGEST DIFFERENTIATOR IS UNDERSTANDING YOU

At ANM, we believe understanding your business is just as important as understanding technology. That's why we always keep your end goals in mind and work closely alongside you to achieve them. Our team takes pride in providing engineering excellence and quality customer service with a local focus. We specialize in the fastest-growing areas of IT, including risk mitigation, enterprise infrastructure and digital transformation.

DEEP ENGINEERING EXPERTISE

In addition to having six engineers per salesperson, with ANM you get a team of engineering expertise who are not only book smart on the technologies, but also street smart. This means we can help you best operationalize the technologies and avoid common pitfalls.

VENDOR INDEPENDENT RECOMMENDATIONS

The technology landscape is crowded and confusing. Our team of experts make tailored recommendations for your needs. We understand the best partners for your needs are the ones who have an opinion and can help you get technology selection right.

AN ACCELERANT, NOT A BOTTLENECK

We all know technology and business processes have enough bottlenecks. Our goal is to help you move faster so you can expect a sense of urgency when you work with our team.

EBOOK INTRODUCTION

PRACTICAL STEPS TO BUILDING A MODERN NETWORK WITH SD-WAN & SASE

The network has become the lifeline of the modern enterprise. Cloud adoption, mobile workforces, and SaaS applications are pushing legacy infrastructure to its limits. And now with SD-WAN and SASE, these technologies promise agility, security, and centralized management amidst complexity.

This eBook provides an in-depth guide to understanding, implementing, and scaling SD-WAN and SASE solutions with a focus on real-world applicability and best practices.

THE SHIFT
TOWARD MODERN NETWORK ARCHITECTURES

Traditional WAN architectures, often built around hub-and-spoke models and expensive MPLS circuits, were designed for a world where applications lived in centralized data centers and users accessed resources from fixed office locations. In today's environment — where apps live in the cloud and users work from anywhere — this model breaks down.

CHALLENGES DRIVING THE SHIFT:

- **Rising demand for cloud services and SaaS:** Cloud applications like Microsoft 365, Salesforce, Zoom, and countless others have become core to business operations. These applications live outside the traditional data center and require direct internet access to perform well. Routing this traffic back through a centralized hub (as in traditional WAN) introduces latency, degrades user experience, and wastes bandwidth. Businesses need an architecture that enables direct-to-cloud connectivity without sacrificing visibility or security.

- **Increased use of remote and hybrid work:** The hybrid workforce is here to stay. Employees now expect seamless access to business applications from home, on the road, or at the coffee shop. Traditional WANs, which are tightly coupled to physical office locations, weren't designed to support this level of distributed access.

  Organizations need to ensure consistent policy enforcement, user experience, and security no matter where a user connects from — something traditional WAN cannot easily deliver.

- **Need for granular security across all access points:** With users, data, and applications more distributed than ever, the attack surface has grown exponentially. Centralized security appliances (e.g., firewalls at HQ) leave remote sites and users exposed or require complex and costly workarounds. What's needed is a security model that follows the user — inspecting and enforcing policies at every access point, in real time. This is especially critical for achieving Zero Trust security frameworks.

- **High cost and inflexibility of MPLS-based networks:** MPLS circuits are notoriously expensive and can take weeks or even months to provision. Scaling them to support new branches, cloud connectivity, or temporary workspaces is both time-consuming and cost-prohibitive. They also offer limited bandwidth compared to modern broadband or 5G. Businesses need flexible, cost-effective options that allow them to adapt quickly to changing demands without sacrificing performance or control.

THE WAY FORWARD: DECOUPLING NETWORKING AND SECURITY

In response to these challenges, organizations are embracing an approach that decouples networking and security from physical infrastructure. SD-WAN allows intelligent, policy-driven routing over any transport — MPLS, broadband, LTE/5G — while SASE provides cloud-delivered security that enforces policies consistently across all users and locations.

This shift puts control back in the hands of IT teams, enabling them to:

- Deploy services faster
- Secure remote users at scale
- Improve application performance
- Reduce operational complexity

In short, it's a foundational step toward building a more agile, secure, and scalable digital enterprise.

DEEP DIVE INTO SD-WAN

As businesses increasingly adopt cloud-based applications and support a distributed workforce, the limitations of traditional WAN architectures become clear. SD-WAN (Software-Defined Wide Area Networking) emerges as a powerful solution to address these challenges by transforming how enterprise networks are built, managed, and optimized.

At its core, SD-WAN separates the control plane (management and policy decisions) from the data plane (actual traffic forwarding), allowing for centralized orchestration and policy enforcement while still leveraging multiple transport links at each site.

Instead of relying solely on costly MPLS circuits, SD-WAN enables the use of broadband, fiber, LTE/5G, and satellite connections — dynamically routing traffic based on real-time conditions, application needs, and security policies.

LET'S DIVE DEEPER INTO THE FOUR FOUNDATIONAL PILLARS OF SD-WAN:

1 **Centralized Management:** With SD-WAN, IT teams manage the entire network — branches, users, applications, and policies — from a single pane of glass (SPOG). This centralized approach significantly reduces configuration errors, accelerates deployments, and improves operational efficiency. New branches can be brought online with minimal effort through zero-touch provisioning, while consistent security and QoS (Quality of Service) policies can be deployed network-wide in minutes.

2 **Transport Independence:** SD-WAN allows the use of any mix of connectivity options — MPLS, broadband, DIA, 5G, satellite — to form the network underlay. This flexibility reduces dependency on expensive legacy circuits and allows enterprises to choose the best-performing or most cost-effective transport for each site. More importantly, it enables link redundancy and load balancing, which helps maintain uptime and application performance even when individual circuits experience degradation.

3 **Application-Aware Routing:** Unlike traditional WANs that treat all traffic equally, SD-WAN is application-aware. It identifies traffic by application type and dynamically assigns it the appropriate path based on pre-defined business policies. For example, mission-critical apps like VoIP or video conferencing can be prioritized over file downloads or social media traffic. This ensures users get a consistent and optimized experience regardless of network conditions.

4 **Dynamic Path Selection:** SD-WAN continuously monitors all available WAN links for metrics like latency, jitter, packet loss, and congestion. Based on real-time network conditions, it can reroute traffic to the most optimal path — automatically and instantly. This self-healing behavior improves reliability and supports SLA compliance, especially for latency-sensitive applications.

By shifting from a hardware-centric WAN model to a software-driven approach, SD-WAN delivers a number of strategic benefits:

- Simplified Network Operations: Unified management, centralized policy control, and automated configuration updates reduce the burden on IT teams.
- Enhanced User Experience: Intelligent traffic steering ensures users experience high-performance access to cloud and on-premises applications.
- Faster Deployment: New sites and remote users can be brought online in days instead of weeks, supporting agile business expansion.
- Lower Costs: The ability to use broadband or 5G alongside or in place of MPLS reduces overall WAN expenditures.

WHY IT MATTERS

In today's digital enterprise, the network must adapt to cloud-first, mobile-first realities. SD-WAN delivers the agility, visibility, and performance needed to support this evolution. But on its own, SD-WAN doesn't solve the full picture — especially when it comes to security. That's where SASE (Secure Access Service Edge) comes in, extending the power of SD-WAN with tightly integrated, cloud-delivered security capabilities.

CORE CAPABILITIES OF SD-WAN

Let's break down what makes SD-WAN powerful...

- Centralized Management: Control the entire network via a single pane of glass. Streamline updates, push policies, and monitor performance from a centralized controller.
- Separation of Control and Data Planes: Enables agility and scalability. Routing decisions are made centrally and pushed to edge devices for execution.
- Transport Independence: Mix MPLS, broadband, DIA, 5G, or satellite links. SD-WAN selects the best path for each application dynamically.
- Encryption: Secure communication with IPSec or TLS-based tunnels, ensuring data confidentiality across all paths.
- Segmentation: Virtual Routing and Forwarding (VRF) allows logical separation of traffic, enforcing policies for compliance and security.
- On-Box Security: Firewalls, IPS/IDS, and URL filtering are built into edge appliances, reducing dependency on external tools.
- SSE Integration: APIs and tunneling options enable SD-WAN to integrate with cloud-delivered Security Service Edge platforms.
- WAN Optimization and Analytics: Features like packet duplication, forward error correction, and traffic shaping enhance application performance. Deep analytics provide insight into usage and anomalies.

DEEP DIVE INTO SASE

As enterprises embrace modern work, their attack surfaces expand dramatically. Employees now work from anywhere, applications reside in the cloud, and sensitive data flows across a web of devices and locations. Traditional perimeter-based security models — built around centralized firewalls and static policies — can no longer keep up.

SASE was developed to address this paradigm shift. Introduced by Gartner in 2019, SASE is a cloud-native architecture that converges networking and security functions into a unified, globally distributed service model.

Rather than forcing traffic through a central location for inspection and control, SASE brings security to the user, wherever they are, and enforces consistent policy enforcement at the edge — whether that edge is a branch office, a coffee shop, or a mobile phone.

CORE COMPONENTS OF SASE

A true SASE platform consists of several tightly integrated technologies, each solving a critical piece of the security puzzle:

Zero Trust Network Access (ZTNA)

ZTNA replaces traditional VPNs by applying the principle of least privilege — users are only granted access to the specific applications or resources they need, based on identity, device posture, and context. ZTNA also enforces microsegmentation, helping to contain breaches by ensuring that lateral movement is restricted.

Benefits:

- Reduces attack surface
- Supports secure, conditional access
- Delivers a better experience than legacy VPNs
- Enhances insider threat protection

Secure Web Gateway (SWG)

SWGs act as a barrier between users and the internet, inspecting web traffic for malware, phishing, and policy violations. Unlike traditional proxies, cloud-based SWGs provide security and compliance at scale, without the need for backhauling traffic through a data center.

Benefits:

- Real-time threat prevention for web traffic
- Enforces acceptable use policies
- Protects users even when they're off-network
- Seamlessly integrates with SSL/TLS decryption

Cloud Access Security Broker (CASB)

A CASB sits between users and cloud applications, providing visibility, control, and compliance for SaaS usage. It helps detect shadow IT, monitors data sharing, and enforces granular policies based on user behavior and risk level.

Benefits:

- Prevents unauthorized data sharing
- Ensures SaaS compliance with regulations (e.g., HIPAA, GDPR)
- Detects risky user behaviors and account compromise
- Supports DLP and encryption for cloud data

Firewall as a Service (FWaaS)

FWaaS delivers traditional firewall capabilities — like access control, intrusion prevention, and logging — as a scalable, cloud-delivered service. Unlike physical firewalls, FWaaS scales elastically, applies policies consistently across all locations, and supports remote users without needing hardware.

Benefits:

- Centralized policy enforcement
- Simplified operations and scaling
- No physical appliances to manage
- Protects east-west and north-south traffic

Data Loss Prevention (DLP)

DLP solutions detect and prevent the unauthorized movement of sensitive information — such as PII, PHI, or intellectual property — across email, web, and cloud applications. Integrated with other SASE functions, DLP helps enforce data handling rules and avoid costly breaches.

Benefits:

- Prevents data exfiltration
- Enforces compliance requirements
- Reduces insider risk
- Works seamlessly with CASB, SWG, and ZTNA

WHY SASE MATTERS

SASE enables organizations to build a modern security posture that aligns with today's cloud-first, user-centric reality. With its distributed, policy-based framework, SASE helps companies:

- **Enforce Consistent Security Policies Everywhere**
  Whether a user connects from the office, home, or abroad, SASE applies the same level of control and protection — without relying on complex backhaul architectures or fragmented point solutions.

- **Support Remote and Mobile Users Securely**
  SASE ensures every user session is authenticated, inspected, and secured in real time, no matter the location or device. This is especially valuable in hybrid work environments, where mobile and remote access are the norm.

- **Provide Visibility and Control Across All Traffic**
  From sanctioned SaaS apps to unsanctioned shadow IT, SASE gives IT and security teams deep visibility into all user activity, with the tools to enforce granular controls, investigate threats, and remediate quickly.

THE POWER OF CONVERGENCE

Individually, these technologies solve important problems — but when combined under the SASE model, they deliver a unified, adaptive, and cloud-scale security fabric. This convergence is what makes SASE so transformative: fewer tools, fewer gaps, and a stronger, more agile security posture.

SD-WAN AND SASE: BETTER TOGETHER

Modern enterprise networks are no longer confined to the data center or traditional branch offices. With users, applications, and data spread across cloud platforms, remote workforces, and mobile devices, IT leaders need a unified solution that delivers both high-performance connectivity and end-to-end security — without increasing complexity.

This is where SD-WAN and SASE converge to deliver a powerful, cloud-native architecture that is agile, secure, and scalable.

SD-WAN brings agility and intelligence to network connectivity — enabling dynamic path selection, application-aware routing, and transport independence.

SASE brings cloud-delivered security to the edge — protecting users and data wherever they are, with consistent, identity-driven policy enforcement.

Together, they represent the digital foundation of the modern enterprise network.

BENEFITS OF SD-WAN AND SASE CONVERGENCE

Consistent User Experience

By combining intelligent traffic routing with security that follows the user, organizations can deliver a seamless experience across any location or device.

- SD-WAN ensures low-latency, high-throughput access to cloud applications by routing traffic along the best-performing paths in real time.
- SASE ensures that every session is authenticated, inspected, and encrypted without degrading performance — even when users are off-network.

The result: Fast, secure, and reliable access for employees, partners, and contractors — whether in the office, at home, or on the move.

Centralized Policy Enforcement

In legacy environments, security and network policies are often scattered across disparate tools and appliances, making them difficult to manage and easy to misconfigure.

WITH SD-WAN AND SASE:

- Network policies (e.g., traffic prioritization, routing rules) and security policies (e.g., access controls, threat prevention, DLP rules) are managed from a centralized, cloud-based console.
- Policies can be defined once and applied consistently across all users, applications, and locations — eliminating gaps and ensuring compliance.

This centralization empowers IT teams to maintain control and visibility across a highly distributed environment without the burden of manual, device-by-device configuration.

Reduced Complexity and Overhead

Historically, delivering both secure connectivity and access control required layering multiple hardware appliances at each site — firewalls, VPNs, proxies, WAN optimizers — all needing separate management, maintenance, and licensing.

THE SD-WAN + SASE MODEL SIMPLIFIES THIS BY:

- Replacing multiple point products with a unified cloud-native platform
- Eliminating the need for backhauling traffic to a central location for inspection
- Allowing for zero-touch provisioning and faster site onboarding

This not only reduces hardware and operational costs but also makes it easier to scale and adapt to future business needs — like adding new remote locations, users, or cloud apps.

Enhanced Threat Detection and Response

Traditional perimeter-based defenses were designed for a static world. Today's threats target users wherever they are, using sophisticated, multi-vector attacks.

WITH SD-WAN + SASE, ENTERPRISES BENEFIT FROM:

- Inline traffic inspection across all ports and protocols
- Real-time threat intelligence fed into every edge location
- Context-aware access control and behavioral analysis to detect anomalies
- Security functions such as sandboxing, CASB, and DLP integrated into the network fabric

This tight integration ensures threats are detected closer to the user, contained before they move laterally, and remediated swiftly — improving the overall security posture.

THE STRATEGIC VALUE OF CONVERGENCE

Bringing SD-WAN and SASE together is not just about tools — it's about enabling digital transformation safely and efficiently. Whether you're moving to multi-cloud, adopting a hybrid workforce, or deploying IoT at the edge, this convergence provides the agility, security, and visibility you need to stay ahead.

Think of SD-WAN as the circulatory system — delivering performance and reliability — and SASE as the immune system — defending and securing at every endpoint. Together, they keep the business healthy and resilient.

PRACTICAL STEPS
FOR ADOPTING SD-WAN AND SASE

Adopting SD-WAN and SASE isn't just a technology upgrade—it's a strategic transformation. To get it right, organizations must align technical implementation with clear business objectives and a phased, data-driven approach. This section outlines a set of practical, actionable steps that guide you from initial planning through ongoing optimization, helping ensure that your SD-WAN and SASE deployments deliver measurable value in performance, security, and manageability.

1. **Define Clear Business Goals:** Know what you're solving for: cost reduction, improved performance, better security, or all the above.

2. **Conduct a Readiness Assessment:** Evaluate your existing network, traffic patterns, cloud dependencies, and security posture.

3. **Start with a Pilot:** Choose a few branches for an initial deployment. Measure success metrics like uptime, latency, user experience, and ease of management.

4. **Leverage Transport Diversity:** Take advantage of multiple WAN links. Use SD-WAN to dynamically assign the best path for each application.

5. **Enable Zero Trust Principles:** With SASE, enforce identity-based access controls and device posture checks to minimize risk.

6. **Integrate SSE and SD-WAN Seamlessly:** Select platforms with tight native or API-based integration. Tunnel-based setups work but can add complexity.

7. **Train Teams Together:** Unify network and security operations under a shared strategy. Invest in cross-skilling and shared tools.

8. **Monitor and Optimize Continuously:** Use analytics to monitor app performance, security events, and policy enforcement. Adjust as needed.

The road to SD-WAN and SASE adoption doesn't have to be complex or overwhelming. By following these practical steps—from defining your goals to continuous optimization—you can build a network and security architecture that's resilient, agile, and ready for the demands of a cloud-first world. The key is to approach the journey thoughtfully, integrate cross-functional teams, and remain adaptable as technologies and business needs evolve.

VENDOR SELECTION AND EVALUATION CRITERIA

Choosing the right SD-WAN and SASE vendor is a critical step that can make or break your deployment. Beyond marketing promises, it's important to evaluate vendors based on how well their offerings align with your organization’s technical requirements, operating model, and long-term goals.

KEY CONSIDERATIONS SHOULD INCLUDE:

- Ease of Deployment and Ongoing Management:
  Look for solutions that offer centralized orchestration, intuitive dashboards, and automated policy enforcement. A streamlined deployment process reduces time-to-value and lowers operational overhead.

- Integration Capabilities:
  Evaluate how well the platform integrates with your existing infrastructure—firewalls, identity providers, endpoint management tools, and third-party analytics. Native or API-based integration is key to maintaining operational efficiency and minimizing friction across tools.

- Security Features:
  Ensure the vendor provides robust, enterprise-grade security baked into the platform. This includes threat prevention, data loss protection, secure web gateways, firewall-as-a-service (FWaaS), and identity-based access controls aligned with Zero Trust principles.

- **Cloud-Native Architecture:**
  A truly cloud-native architecture enables elastic scaling, global reach, and high availability. Look for vendors with a distributed edge presence and support for multi-cloud and hybrid environments to ensure optimal performance

- **Licensing and Cost Structure:**
  Understand how licensing is packaged—whether it's based on users, bandwidth, sites, or feature tiers. Transparent pricing and scalability are essential to avoiding cost surprises as your deployment grows.

- **Support and Service-Level Agreements (SLAs):**
  Reliable support can be the difference between a quick fix and prolonged downtime. Evaluate the vendor's support model, availability, responsiveness, and the strength of their SLAs around uptime, issue resolution, and performance guarantees.

To validate vendor claims, conduct proof of concepts (POCs) in your own environment. Focus on real-world performance metrics, user experience, manageability, and support responsiveness. In addition, engage peer references—other organizations in your industry or with similar scale and complexity—to gain candid insights into vendor strengths, weaknesses, and real-world support experiences.

The goal is not just to choose a product, but to select a strategic partner that will grow with your business and continuously evolve to meet emerging security and networking demands.

FUTURE-PROOFING YOUR NETWORK

SD-WAN AND SASE SHOULD BE STEPPINGSTONES, NOT FINAL DESTINATIONS. STAY AHEAD BY:

- Prioritizing cloud-native solutions
- Embracing AI/ML for traffic insights and anomaly detection
- Supporting multi-cloud environments
- Preparing for edge computing and IoT expansion

In today's non-stop digital world, agility, performance, and security are non-negotiable. SD-WAN and SASE offer a modern foundation to meet these demands. Organizations that embrace these technologies with clear goals, a thoughtful plan, and a collaborative approach will position themselves for long-term success.

Let your network be an enabler, not a bottleneck.

Need help designing your SD-WAN and SASE strategy? Reach out to our team of experts.