MODERN APPROACHES TO NETWORK ACCESS SECURITY

Recent findings[1] by the Cybersecurity & Infrastructure Security Agency (CISA), New Zealand's Government Communications Security Bureau (GCSB), New Zealand's Computer Emergency Response Team (CERT-NZ) and The Canadian Centre for Cyber Security (CCCS) highlight the critical need for modern network access solutions.

As traditional VPNs become increasingly vulnerable to cyber threats, organisations in New Zealand and globally must adopt innovative security approaches to protect their digital assets and infrastructure in today's cloud-centric landscape.

WHAT'S DRIVING THIS CHANGE?

Legacy VPN solutions have become a prime target for cyber attackers, with over 22 Known Exploited Vulnerabilities identified. These vulnerabilities, combined with the limitations of traditional remote access and the rapid shift to cloud services, are exposing organizations to significant security risks and driving the need for more robust, modern network access solutions.

VPN vulnerabilities leading to network compromises.

Limitations of traditional remote access solutions

Increasing cloud service usage

56% of organisations surveyed have been targets of cyberattacks exploiting VPN security vulnerabilities in the last year.[2]

THE APPROACH TO SECURITY NEEDS TO CHANGE

MODERNISING NETWORK SECURITY: ZERO TRUST, SSE & SASE

To address the evolving threat landscape, cybersecurity experts recommend three key modern approaches: Zero Trust, Secure Service Edge (SSE), and Secure Access Service Edge (SASE).

These solutions offer enhanced security, granular access control, and improved integration of network and security functions, particularly suited for today's hybrid and cloud-centric environments.

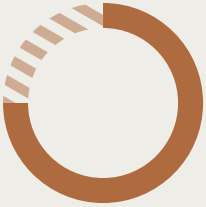
KEY SOLUTIONS

Zero Trust Security

Secure Service Edge (SSE)

Secure Access Service Edge (SASE)

ZERO TRUST



72% of decision-makers are planning to or currently deploying a Zero Trust security model.[3]

The core principle driving Zero Trust is simple yet powerful: Assume every request is a potential threat, regardless of its origin. Zero Trust is built on five key components that work together to enhance security. Always verify users, ensuring continuous authentication for every access attempt. Grant minimal access, giving users only the permissions they need for their specific tasks. Divide the network into segments to contain potential breaches. Secure all devices, treating every endpoint as a potential vulnerability. Protect data everywhere, whether at rest or in transit. This approach significantly reduces the attack surface and improves overall security posture.

SECURE SERVICE EDGE (SSE)

Secure Service Edge unifies cloud-based security functions to protect modern, distributed networks. SEE capabilities are made up of Zero Trust Network Access, Cloud Secure Web Gateway, Cloud Access Security Broker and Firewall-as-a-Service:

1. **ZTNA (Zero Trust Network Access):**
An IT security solution that provides secure remote access to applications and services based on strictly defined access control policies.

2. **SWG (Cloud Secure Web Gateway):**
A security solution that protects users and devices from web-based threats and enforces security policies within the network.

3. **CASB (Cloud Access Security Broker):**
A cloud security solution that helps organisations manage data across multiple software-as-a-service applications and when data is in transit to cloud environments.

4. **FWaaS (Firewall-as-a-Service):**
A cloud-based security solution that enables organisations to monitor and aggregate traffic from multiple sources, such as data centers, offices, and cloud infrastructures.

SECURE ACCESS SERVICE EDGE (SASE)

Secure Access Service Edge (SASE) is a cloud architecture that combines network and security-as-a-service capabilities, providing a comprehensive approach to securing modern, distributed networks.

Key Components:

1. Software-Defined Wide Area Networking (SD-WAN)
2. Secure Web Gateway
3. Cloud Access Security Broker
4. Next-Generation Firewall
5. Zero Trust Network Access

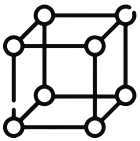
How it works

- SASE goes beyond SSE by integrating networking capabilities with security functions.
- Combines networking (like SD-WAN) and security services into a single, unified cloud platform.
- Dynamically routes enterprise traffic to cloud-based services, often using SD-WAN for efficient routing.
- Applies consistent security policies across all network edges, enabling granular control.
- Uses a single platform for monitoring and reporting, facilitating efficient incident response.
- Easily adapts to changing needs, eliminating multiple point solutions and streamlining security infrastructure.

10 BEST PRACTICES FOR MODERN NETWORK SECURITY

CENTRALISED MANAGEMENT

Implement centralised management by controlling remote access and simplifying network administration.



NETWORK SEGMENTATION

Adopt network segmentation by denying connections by default, especially for OT networks.

SECURITY AUTOMATION

Automate security processes by using SOAR for automated responses to security events.

INCIDENT RESPONSE

Maintain updated incident response plans by regularly drilling and updating plans for various scenarios.

VULNERABILITY MANAGEMENT

Conduct regular vulnerability scans by automating scans on public-facing assets and implementing compensatory controls.

ROBUST AUTHENTICATION

Deploy robust authentication by using phishing-resistant multifactor authentication (MFA).

10 BEST PRACTICES FOR MODERN NETWORK SECURITY (CONT)

LEAST PRIVILEGE ACCESS

Implement least privilege access by granting access on a just-in-time, need-to-know basis.

SECURITY TRAINING

Conduct regular security training through annual sessions on basic security concepts for all employees and contractors.

DATA BACKUPS

Perform regular backups by storing them separately and testing at least annually.

HARDWARE SEGMENTATION

Use hardware-enforced segmentation for the most consequential systems through unidirectional technologies.

REFERENCES

1 – Modern Approaches to Network Access Security, 18th June 2024 – CISA – Link

2 – ThreatLabz 2024 Annual Report, 7th May 2024 – Zscaler – Link

3 – Lessons Learned From The World's Biggest Data Breaches And Privacy Abuses, 28th February 2024 – Forrester – Link