Secure-Sonic-WAN: A Modern Zero-Trust IPv6 Architecture for Secure Edge Connectivity

1. Executive Summary

The Secure-Sonic-WAN project represents a next-generation approach to building secure, flexible, and cost-effective Wide Area Network (WAN) infrastructures.
It leverages open-source networking software, IPv6-native design, and Zero Trust principles to provide a scalable, identity-driven networking architecture.
The system is built around SONiC (Software for Open Networking in the Cloud) as the foundational network operating system, extended by containerized services for tunneling, identity, and policy management.

2. Background and Motivation

Traditional enterprise WAN architectures rely heavily on static IPv4 networks, VLAN-based segmentation, and perimeter-based firewalls.
These legacy designs are not well-suited to modern, distributed IT environments where users, devices, and applications are spread across many locations and clouds.
IPv4-based networks are inherently limited by address space, rely on NAT, and lack native end-to-end security and mobility support.

Secure-Sonic-WAN aims to solve these issues by combining an IPv6-native underlay, Zero Trust networking (ZTN) principles, and open-source building blocks
to create a distributed network that is secure by design (“security architected-in”), scalable to thousands of sites, and flexible enough for multi-cloud and IoT use cases.

3. Architecture Overview

At the core of the architecture is a SONiC-based virtual or physical network appliance that serves as the data plane and routing fabric.
Instead of modifying SONiC directly, new functionality is added via containerized sidecars

running directly on the SONiC host.
These containers provide tunneling, identity, and policy enforcement capabilities.

The design follows a modular principle: SONiC handles switching, routing, and ACLs; containers handle overlay networking (ZeroTier, WireGuard), identity (IAM agent), and policy enforcement (OPA-based).
This ensures clean separation of concerns, high maintainability, and ease of automation.

4. Key Architectural Principles

1. IPv6 Everywhere: Every device and network segment operates natively with IPv6, eliminating the need for NAT and simplifying global addressing.
2. Zero Trust Networking: No implicit trust. All communications are authenticated, authorized, and encrypted. Traffic is always initiated outbound.
3. Identity-Centric Networking: Devices and users are identified through IAM systems using certificates or tokens, replacing static IP or VLAN-based policies.
4. Open Source and Hardware Independence: All components are built from open-source software and run on commodity “white box” hardware or virtual machines.
5. Automation and Observability: Infrastructure as Code and telemetry are integral. All policies, configurations, and certificates are managed automatically.

5. Core Components

- SONiC Network Operating System — Open-source switch and router platform providing L2/L3 forwarding, ACLs, and routing protocols such as BGP and EVPN.
- ZeroTier Container — Provides dynamic overlay connectivity for site-to-site and edge-to-cloud communication with minimal configuration.
- WireGuard Container — Offers encrypted tunnels for secure internet or SASE connectivity.
- IAM Agent — Handles device identity, certificate management, and integration with a central IAM or PKI system (e.g., Keycloak, SPIRE, HashiCorp Vault).
- Policy Enforcement Agent — Enforces routing and access policies locally using Open Policy Agent (OPA) rules.
- Telemetry and Logging — Integrated observability via open-source stacks such as Prometheus, Grafana, and ELK.

6. IPv6-First Networking Model

The IPv6-based design provides each device with a globally unique address, removing the complexity of NAT and overlapping subnets.
End-to-end connectivity is restored, enabling direct device-to-service communication while still being protected through Zero Trust enforcement.

With IPv6, each network segment (formerly VLAN) is represented by a /64 subnet.
Routing and segmentation are handled logically based on identity and policy, not by static VLANs or IP ranges.
This allows networks to scale to thousands of sites and millions of devices without complex address planning.

7. Zero Trust and Identity-Based Security

The Zero Trust principle of "never trust, always verify" is embedded at every layer.
All devices, users, and applications authenticate through an Identity and Access Management (IAM) system before being granted access.
Policies are based on verified identity, device posture, and context — not on network location.

Instead of perimeter firewalls, each edge node enforces micro-segmentation policies locally.
Outbound-only tunnel connections (e.g., via WireGuard or ZeroTier) ensure that no inbound traffic is accepted unless explicitly authorized.
This drastically reduces the attack surface and prevents lateral movement.

8. Industrial and IoT Use Cases

a) Factory IoT Scenario

In a modern factory, hundreds of IoT sensors connect via WiFi and transmit operational data to a local message concentrator.
The concentrator preprocesses data and securely forwards it to a central ERP/MES system through a WireGuard tunnel.
Each sensor and concentrator authenticates via IAM, receives a certificate, and is assigned an IPv6 address.

Zero Trust policies ensure sensors can only communicate with their local concentrator and IAM endpoints — nowhere else.

b) Renewable Energy Park Scenario

In a distributed wind or solar park, each turbine or inverter sends telemetry data to a central controller.
Each device connects over IPv6 and establishes an outbound-encrypted session to the site concentrator.
From there, traffic is aggregated and securely tunneled to the cloud-based energy management system via ZeroTier or WireGuard.
Identity-based policies prevent compromised devices from affecting others and allow fine-grained control of command distribution.

9. Advantages over Legacy IPv4/VLAN Architectures

- Elimination of NAT and overlapping networks — simplifies connectivity and management.
- Identity replaces IP or VLAN as the basis for policy — enabling true micro-segmentation.
- Outbound-only encrypted communication — minimizes exposure to external attacks.
- Horizontal scalability — easy to add sites and devices without renumbering.
- Vendor neutrality — full stack built from open-source software, deployable on white-label uCPEs.
- Built-in automation and observability — reduces operational complexity.

10. Open Source and White-Label Hardware Strategy

Secure-Sonic-WAN embraces open standards and open-source components to ensure transparency, flexibility, and cost-efficiency.
It runs on commercial off-the-shelf (COTS) or white-label uCPE devices using x86 or ARM architectures, allowing enterprises to avoid vendor lock-in.
All major building blocks — SONiC, WireGuard, ZeroTier, OPA, and Keycloak — are open source and community-driven.

This openness not only lowers total cost of ownership but also enables continuous innovation and security audits from the community.
Organizations can integrate their own orchestration, monitoring, or automation

frameworks without restrictions.

11. Implementation and Deployment Model

The system can be deployed as a virtual appliance, a containerized node within Containerlab for testing, or as a physical uCPE at the network edge.
Automation scripts handle onboarding, identity registration, and policy synchronization with the central IAM system.

For large-scale deployments, policies and configurations are managed centrally through Infrastructure-as-Code frameworks such as Ansible or Terraform,
while local nodes enforce rules autonomously using cached policies for resilience.

12. Future Enhancements

Future iterations will integrate enhanced telemetry and AI-driven threat detection, support for post-quantum cryptography,
and deeper integration with cloud-native IAM systems.
Support for segment routing over IPv6 (SRv6) and automated service mesh integration are also planned to further streamline large-scale deployments.

13. Conclusion

Secure-Sonic-WAN defines a new paradigm for secure, scalable, and flexible WAN connectivity.
It replaces static, perimeter-based architectures with an identity-driven, Zero Trust design that is inherently secure and adaptable to modern workloads.
By leveraging IPv6, open-source software, and commodity hardware, it provides enterprises and operators with a future-proof solution that combines low cost, high performance, and uncompromising security — truly “architected-in” from the start.