SOLUTION BRIEF

VERSA NETWORKS

Strengthening the Defense Department's Zero Trust Posture

Versa Networks, DISA Thunderdome Capability Partner

The Defense Information Systems Agency (DISA) has produced a successful Thunderdome prototype, its Joint Regional Security Stack (JRSS) replacement program that takes a key step toward meeting the Pentagon's Zero Trust vision, while delivering network modernization to the DoD Enterprise. The program represents a fundamental change in the DoD's approach to security and networking – and better enables the Warfighter mission.

Background

Thunderdome is a new Zero Trust security and network architecture prototype developed with the goal of fortifying the U.S. Department of Defense's networks and deterring the growing threats posed by adversaries intent on undermining U.S. national security interests and international order. It implements a Zero Trust architecture built on Secure Access Service Edge (SASE). DISA's Thunderdome prototype successfully proved that commercial technologies can improve both security and network performance.

Thunderdome is intended to evolve from the siloed nature of the classic defense-in-depth information security model and move the DoD toward end-to-end security from the user all the way to the application and data being accessed. The initiative replaces a loosely integrated legacy suite of technologies and services that DoD information systems have historically relied on for network, firewalls, intrusion detection, and identity. These legacy technologies together provided strong network visibility, but faced challenges that include disjointed integration between security and networking technologies, poor performance, management complexity, disjointed visibility across data sets, and difficulty troubleshooting across partner networks. Notably, the move towards Zero Trust was deemed a necessary evolution by the Department of Defense as Warfighter requirements evolved.

An Evolution: Thunderdome

Thunderdome is designed to replace JRSS, and to bring DISA into alignment with a cybersecurity executive order issued by President Joe Biden in 2021. It will also put a greater emphasis on protecting data and incorporating technologies and concepts like Secure Access Service Edge (SASE) and Software-Defined Wide-Area Networks (SD-WAN) — that were recommended in a Zero Trust plan developed by DISA in 2020.

Notably, the initiative proposes an integrated set of technical capabilities that deliver a unified user experience. Specifically, the requirements include high performance connectivity via SD-WAN to bring enhanced mechanisms to access cloud capabilities for remote users, paired with a natively integrated Zero Trust and cloud security stack that pushes security to the edge.

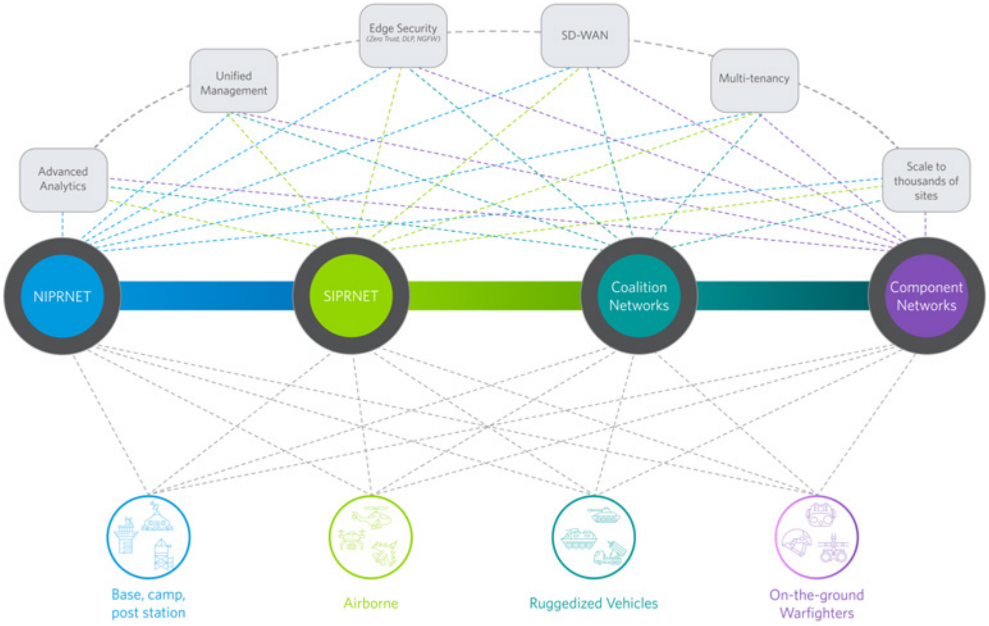

Figure 1: Thunderdome Reference Architecture

The approach is designed to deliver the Defense Department's future security and network architecture to meet diverse operating requirements that include:

- Multi-tenant approach to support multiple discreet organizations and mission partners.
- Foundational architecture that can scale to support thousands of sites across services and agencies.
- Support for both NIPR (unclassified) and SIPR (classified networks).
- As coalition warfare becomes increasingly prevalent, interoperability of the DoD IE with coalition networks.

Zero Trust in Thunderdome

Based upon data and attributes about a user, endpoint device security posture and session, DISA will have control over the level of access. In this model, if a verified user is operating a personal device or accessing a public network, their system access could be adjusted accordingly. This security strategy is a part of DISA's SASE effort which consolidates security enablers such as identity, credential and access management in a single cloud-delivered service model.

Versa: A Thunderdome Capabilities Partner

As a Thunderdome Capabilities Partner, Versa is setting the foundation for Thunderdome;

a. **SD-WAN** – for seamless connectivity and traffic optimization between users, applications, and devices regardless of their location.

b. **Zero Trust Edge security** – Zero Trust conditional access in conjunction with NGFW, NGIPS, and DLP that is built-in the same technology stack as networking, not bolted on. This includes least privilege access to both apps and network segments.

c. **Unified Management** - A unified solution that delivers a single experience for monitoring and troubleshooting, simplifying the process and improving operational efficiency.

d. **Multi-tenancy** – to support a scalable segmentation model that secures and segments a range of organizations and missions partners. Versa Networks supports multi-tenancy at every level from orchestration to edge devices.

e. **Advanced Analytics**

All communications are FIPS140-2 encrypted between Versa devices, and admin interfaces require https and/or SSH. Versa provides STIG hardened images for the DoD. All Versa components can be installed across multiple classification levels (Unclassified, Secret, Top Secret, and above (SAP/ SAR)).

Summary

Not long ago, federal agencies were wondering how and where to start on their Zero Trust journey. Now, we see more agencies looking to accelerate their approach to meet aggressive zero trust implementation deadlines . More importantly, we are hearing from agency IT leaders who are seeking to use DISA's Thunderdome pilot as the reference architecture for meeting Zero Trust implementation guidelines while enabling better performance collaboration between component services and coalition networks.

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054 | Tel: +1 408.385.7660 | Email: info@versa-networks.com | www.versa-networks.com