Strengthening the Defense Department's Zero Trust Posture

Versa Networks foundational technologies supporting Thunderdome

Thunderdome is a new Zero Trust security and network architecture prototype implemented by the Defense Information Systems Agency (DISA) to fortify the U.S. Department of Defense's networks by deploying Secure Access Service Edge (SASE) and Software-Defined Wide Area Network (SD-WAN) technologies. In planning since 2020, it brings DISA into alignment with a cybersecurity executive order issued in 2021 and represents a key milestone in meeting the Zero Trust strategy published by the Pentagon in 2022. Importantly, the Thunderdome prototype successfully proved that commercial technologies can improve both security and network performance.

Thunderdome is intended to evolve the DoD from the siloed nature of the classic defense-in-depth information security model toward end-to-end security from the user 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 under the Department of Defense's Joint Regional Security Stack (JRSS) program. These legacy technologies together provided strong network visibility, but faced challenges that included 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.

Thunderdome brings security to the edge

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

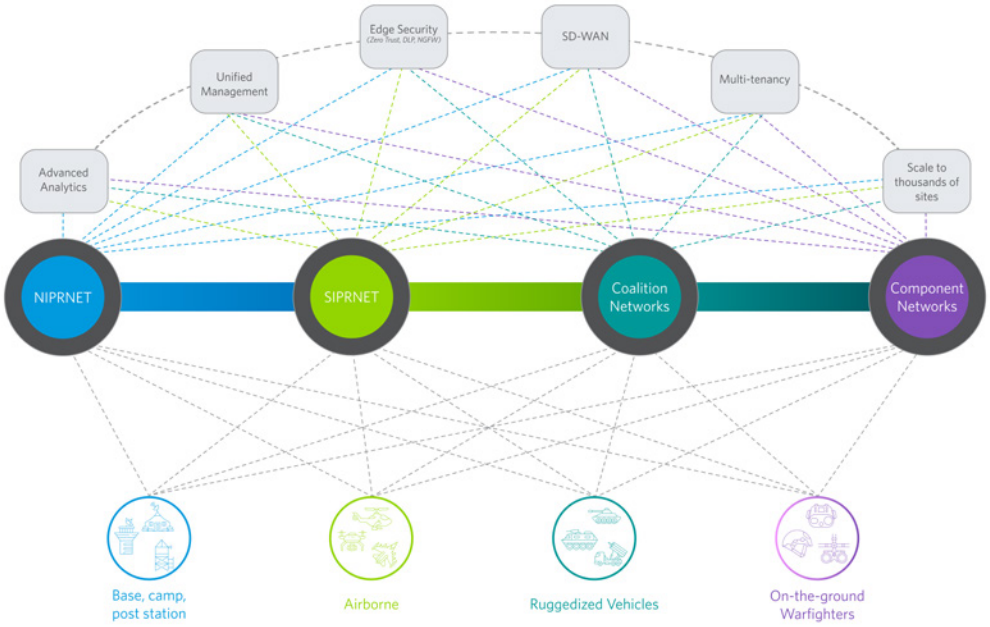

Figure 1: Thunderdome reference architecture

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

- A multitenant 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)
- Interoperability of the DoD IE with coalition networks as coalition warfare becomes increasingly prevalent

A single service model

Based upon data and attributes about a user, endpoint device security posture, and the 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.

Thunderdome Capability Partner

As a Thunderdome Capability Partner, Versa is setting the foundation for Thunderdome by contributing the following capabilities:

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

b. **Zero Trust edge security** for Zero Trust conditional access in conjunction with NGFW, NGIPS, and DLP that is built into the networking technology, not bolted on. This includes least privilege access to both apps and network segments.

c. **Unified management** 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 mission partners. Versa Networks supports multi-tenancy at every level, from orchestration to edge devices.

e. **Advanced analytics** to provide real-time and historical visibility, correlation, prediction and closed-loop feedback on the network.

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)).

Federal agency follow-on

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

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

© 2024 Versa Networks, Inc. All rights reserved. Portions of Versa products are protected under Versa patents, as well as patents pending. Versa Networks and VOS are trademarks or registered trademarks of Versa Networks, Inc. All other trademarks used or mentioned herein belong to their respective owners. Part# SB_THUNDERDOME-02.0