DISA

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Thunderdome

Alan Rosner
Thunderdome PMO

November 2022

The information provided in this briefing is provided for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government.

What is Zero Trust?

"A data-centric security model that eliminates the idea of trusted or untrusted networks, devices, personas or processes and shifts to ***multi-attribute-based confidence levels that enable authentication and authorization policies*** under the concept of least privileged access."

– DoD Digital Modernization Strategy

Verify the User & Device	Conditional Access & Privileges	Data and Application Centric Protections
		
NEVER TRUST, ALWAYS VERIFY	*ASSUME BREACH*	*VERIFY EXPLICITLY*

Purpose

The Thunderdome prototype is DISA's initial implementation of a **Zero Trust Architecture (ZTA) focused on Zero Trust Network Access (ZTNA)**

- Thunderdome's goals are as follows:
  - Reduce redundant and complex cybersecurity architectures while increasing effectiveness
  - Use lessons learned from the prototype to expand a ZTNA to Enterprise.
  - Post prototype, coordinate with Services, Combatant Commands (CCMDs), Defense Agencies, and Field Activities to begin expansion to Mission Partner sites.

Thunderdome Pilot

DISA

News Release

DISA announces contract award for Thunderdome Prototype

DISA awarded an OTA for a prototype-driven pilot concluding in Q1FY23

GOALS

- Implement Zero Trust principles on a production network
- Develop operational experience for Enterprise ZTNA Deployment
- Lay foundations for enterprise service offering

SCOPE

- Leverages OTA allowing adjustments to approach & technology components
- Initial pilot supports a maximum of 5,400 users at three DISA sites
- Includes cybersecurity evaluation as part of Operational Assessment

Thunderdome Prototype Components

Thunderdome's components work together to modernize DISA's infrastructure and integrate with other agency-efforts to increase automation, efficiency and security

SASE

- Highly available Palo Alto Prisma cloud service replaces Remote Access VPN services
- Remote Users are authenticated using enterprise identity services
- Users get conditional access to applications and resources based on identity attributes and device posture
- User traffic doesn't traverse DISN to reach cloud services or internet services

SD-WAN CESS

- Customer Edge Security Stack (CESS) moves security functions (NGFW, IPS/IDS, DLP) closer to the user at the customer edge
- Provides software-defined routing capabilities
- Is an overlay to the existing DISN routing infrastructure
- Creates multi-tenancy hierarchy with Parent / child relationships for baseline and secondary security policies for on prem users

AppSS

- Provides containerized, readily deployable security solution
- Reduces the burden of application security on individual applications owners
- Multiple solutions with either PA Container Security or F5 WAF + PA Next Gen Firewalls managed by Palo Alto Panorama
- DISA will provide Infrastructure as a Code (IaC) templates to automatically provision VM's or leverage Ansible for physical devices. Customers responsible for OEM licensing (F5 & Palo Alto)

Cloud DCO

- Increases visibility across the DoD's Cloud applications
- All user and telemetry data will be ingested, enriched and filtered w/o the need to duplicate data
- Normalize data, automate analyst workflows and enable analysts to apply Machine Learning (ML) models to streaming data
- Cloud agnostic architecture can leverage commercial cloud services or reside on-premise

Thunderdome Phased Approach

February 2022 - October 2022

Phase I

Spiral One Operational and Technology Assessment

Development Testing

Evaluate Thunderdome solution against the Zero Trust Reference Architecture (ZTRA)

Begin Operational Assessment of Thunderdome

Conduct Interoperability testing between different Zero Trust solutions to inform the department strategy moving forward

October 2022 - January 2023

Phase II

Spiral Two Operational Assessment

Continue Operational Assessment including SASE

Continue integrating Endpoint Security Solutions

Perform Cumulative Penetration and Vulnerability Assessment (CVPA)

Share findings with CIO, CCMDs, and Services to inform ZTA path forward

January 2023 +

Phase III

Fielding Decision

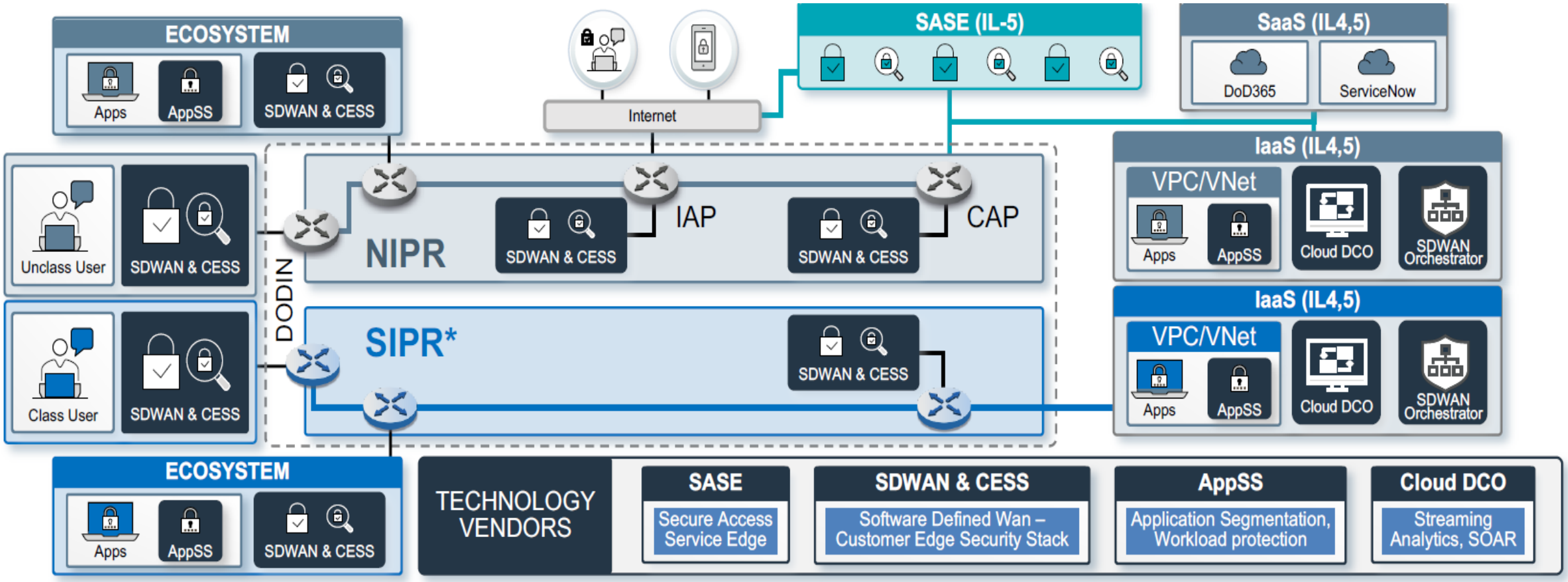
Make fielding decision

Conduct Adversarial Assessment of solution

Conduct an Operational Test

Continue Operational expansion to Enterprise

High-Level Thunderdome Solution Architecture



Why is Thunderdome Important

- **Zero Trust Network Access capabilities can reduce overall threat**
  - Thunderdome capabilities enable a paradigm shift providing conditional access controls based on identity attributes and device posture
- **Network user traffic has shifted significantly with many workers working remotely and many application workloads moving to the commercial cloud.**
  - TD SASE supports this, secures traffic at the edge and provides conditional access control to application workloads and offloads remote user traffic off the DoDIN
- **Opportunity for DoD adopt commercial practices in cybersecurity and orchestration**
  - Many commercial institutions have minimized the role of traditional MPLS networks, using SD-WAN/CESS components to reduce cost, improve efficiency and reliability, improve centralized orchestration, support the network with fewer people
- **JRSS is sunsetting by 2027**
  - Thunderdome brings modernized capabilities to the DoDIN while aligning with Zero Trust principles

Thunderdome Status Update

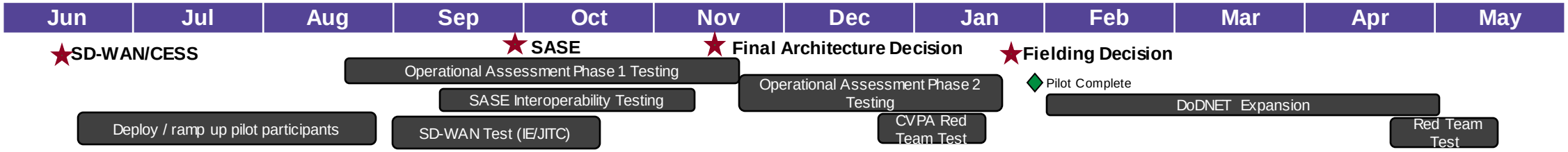
Accomplishments

- IATT granted // SASE Exception to Policy (E2P) granted
- Development Testing Complete (SASE, SDWAN, AppSS & Cloud DCO)
- ICAM & GFUD Integration completed
- Installation of SDWAN appliances at DISA PAC, DISA HQ, and Pentagon JSP completed
- Implementation of DISA PAC & DISA HQ SD-WAN complete and onboarding users
- Onboarded Global Service Desk for Tier 1 support
- Completed Operational Assessment Spiral 1
    - Tested out capabilities on the network

Upcoming Activities

- Expanding pilot user base within DISA
- Initiate Operational Service Manager (OSM) support with DISA Global
- Complete onboarding of CSSP support
- Complete Operational Assessment Spiral 2
- Complete initial Red Team (Cybersecurity) evaluation
- Establish service offerings
- Fielding Decision in early 2023

DISA PAC	DISA HQ	JSP PENTAGON	Thunderdome PMO
SDWAN/CESS has 39 users onboarded	SDWAN/CESS has 108 users onboarded	Implementation finalizing	Onboarded GSD, ServiceNow & Change Mgt in October
SASE Remote Access 39 users onboarded	SASE Remote Access 108 users onboarded	Onboarding On-Site Users in Nov	Finalizing DISA Global for OSM functions beginning mid-November
	Additional DODNET planning ongoing	SASE Remote Access in Nov	



Industry Collaboration

DISA is seeking to foster Standardization and Interoperability.

- DoD and our Federal partners will likely operate a variety of different ZT architectures, comprised of various SD-WAN and SASE solutions
  - Most SD-WAN solutions rely on custom protocols
  - Little to no interoperability between SASE solutions
  - Use of multiple non-interoperable SASE solutions in the Department could lead to a need to deploy and use multiple SASE agents to reach different applications
- DISA is seeking industry participation in the Internet Engineering Task Force (IETF) to foster the creation and adoption of open standards for SD-WAN
- DISA established a ZT Lab to assess current interoperability and encourage more collaboration between SASE vendors
- Ability to integrate SASE with a rich ecosystem of third-party applications is desired

DEFENSE INFORMATION SYSTEMS AGENCY

The IT Combat Support Agency

/DISA @USDISA /USDISA DISA.mil