Department of Defense (DoD) Cloud Native Access Point (CNAP) Reference Design (RD)

Version 1.0

29 July 2021

Approved by:

METZ.DANIELLE.A.1295851046 Digitally signed by METZ.DANIELLE.A.1295851046 Date: 2021.08.17 13:42:58 -04'00'

DANIELLE A. METZ
Deputy Department of Defense
Chief Information Officer for
Information Enterprise

JONES.JEFFREY.RAY.1106950926 Digitally signed by JONES.JEFFREY.RAY.1106950926 Date: 2021.08.16 10:44:59 -04'00'

JEFFREY R. JONES
Vice Director for Command, Control,
Communications, and Computers/Cyber, J6

SNODDY.DAVID.W.1077276277 Digitally signed by SNODDY.DAVID.W.1077276277 Date: 2021.08.17 10:32:03 -04'00'

DAVID W. SNODDY
Brigadier General, USAF
Deputy Director of Current Operations
USCYBERCOM

Prepared By:

LAM.NGOAN.THOMAS.1229438960 Digitally signed by LAM.NGOAN.THOMAS.1229438960 Date: 2021.08.12 08:07:46 -04'00'

N. Thomas Lam
Cloud and Software Modernization
IE/Enterprise Capabilities
Department of Defense, Office of the Chief Information Officer (DoD CIO)

CHAILLAN.NICOLAS.MAXIME.1535056524 Digitally signed by CHAILLAN.NICOLAS.MAXIME.1535056524 Date: 2021.08.12 08:39:59 -04'00'

Nicolas Chaillan
Chief Software Officer
Department of the Air Force

Version History

Version	Date	Approved By	Summary of Changes
1.0	2021/07/29	DCIO-IE	• DMI EXCOM Approved

Executive Summary

The ability to deliver capability "at the speed of relevance" requires an innovative approach to providing secure access to cloud environments. As highlighted in a recent report by the Defense Innovation Board, *"...the threats that the United States faces are changing at an ever-increasing pace, and the Department of Defense's (DoD's) ability to adapt and respond is now determined by its ability to develop and deploy software to the field rapidly.*" To effectively and efficiently achieve the objective, access to cloud environments must be flexible, ubiquitous, and at the same time, provide the requisite level of security and monitoring to protect from, detect, respond to, and recover from cyber-attacks. The purpose of a Cloud Native Access Point (CNAP) is to provide secure authorized access to DoD resources in a commercial cloud environment, leveraging zero trust architecture (ZTA), by authorized DoD users and endpoints from anywhere, at any time, from any device.

The purpose of this CNAP Reference Design (RD) is to describe and define the set of capabilities, fundamental components, and data flows within a CNAP. It presents logical design patterns and derived reference implementations for deploying, connecting to, and operating a CNAP. It is a future state design to guide the development of next generation connectivity and cybersecurity capabilities to improve internet-based machine and user access into DoD cloud (in particular, commercial cloud-hosted) resources and services. A CNAP provides person entities (PE) (i.e., end users and privileged users) and non-person entities (NPE) access to cloud enclaves using a combination of cloud native and cloud ready security mechanisms. Further, a CNAP allows authorized outbound access to the internet, for example, to enable software repository synchronization of COTS patches or new versions of Free and Open-Source Software (FOSS) projects and system-to-system interfaces with mission partners such as other Federal Departments.

The CNAP RD is intended for the Combatant Commanders, Military Departments, Defense Information Systems Agency (DISA), other Defense Agencies, and mission partners who require access to DoD resources in the commercial cloud and government cloud. It serves as DoD enterprise-level guidance for establishing secure internet ingress and egress to cloud-hosted development, test, and production environments.

Contents

Figures

Introduction

The pace of software development, testing, and delivery has increased significantly over the last 10 years. This increase in speed is due largely to the use of cloud computing and adoption of Development, Security and Operations (DevSecOps[1]) practices as part of the software lifecycle. For DoD, creating a technical and tactical advantage in the battlespace relies on software modernization, based on a foundation of cloud computing and DevSecOps, for rapid delivery of capability to the warfighter. The ability to deliver capability requires an innovative approach to providing secure access to cloud environments for the continuous integration and continuous delivery (CI/CD) of software. Of equal importance is the ability for authenticated and authorized users to securely access cloud resources from any device, at any time, from anywhere.

"U.S. national security increasingly relies on software to execute missions, integrate and collaborate with allies, and manage the defense enterprise. The ability to develop, procure, assure, deploy, and continuously improve software is thus central to national defense. At the same time, the threats that the United States faces are changing at an ever-increasing pace, and the Department of Defense's (DoD's) ability to adapt and respond is now determined by its ability to develop and deploy software to the field rapidly."– Defense Innovation Board

Currently, software development in the DoD is not optimized to rapidly procure, assure, deploy, and continuously improve. To optimize software development and increase the ability to adapt and respond to changing threats, a new cloud access capability is needed. With exception to environments like the Mission Partner Environment (MPE) or the Medical Community of Interest, the current implementation for accessing DoD Mission Owner (MO) commercial cloud enclaves from the internet is through DoD Internet Access Points (IAP), across the Defense Information Systems Network (DISN), and through boundary cloud access points (BCAP). Therefore, access to DoD commercial cloud environments must traverse multiple, independently managed security stacks.

While secure, this legacy design increases latency and can lead to network performance and quality of service problems, and it does not provide the flexibility, elasticity, timeliness, or efficiency needed. Rather, access to MO cloud enclaves must be flexible and ubiquitous, while providing the requisite level of security to defend DoD data and resources within commercial cloud-hosted environments. A CNAP creates an agile, highly scalable, and available security capability for access into MO cloud enclaves without going through a cloud access point that is hosted on the DoD Information Network (DoDIN). By leveraging cloud native security services and tools[2], a CNAP is very efficient in terms of maintenance, management, monitoring, and compliance. It is also very effective in facilitating a Zero Trust Architecture by utilizing conditional access policies, micro-segmentation[3], and continuous monitoring.

A CNAP is a virtual Internet Access Point (vIAP) that provides modernized cybersecurity capabilities based on the DoD Zero Trust Reference Architecture (ZTRA). It is an access point for person entities (PE) and non-person entities (NPE) to DoD resources in a commercial cloud environment from the internet (i.e., non-DODIN).

This document establishes a vendor/solution agnostic RD, which is aligned with the DoD Digital Modernization Strategy and the DoD Cloud Computing Strategy, for implementing a CNAP that relies on

[1] DevSecOps is a set of software development practices that combines software development (Dev), security (Sec), and information technology operations (Ops) to secure the outcome and shorten the development lifecycle (https://public.cyber.mil/devsecops/).

[2] Cloud native services and tools are designed to leverage cloud capabilities and are optimized to run in cloud environments. These can be provided by the cloud service provider or by third party vendors.

[3] Micro-segmentation is a logical division of the internal network into distinct security segments at the service/API level.

cloud hosted gateways and security services to support secure access from the internet for all types of DoD authenticated and authorized entities. While the RD is agnostic, examples of specific solutions are given to provide reference to available options. DoD does not endorse any specific vendor or solution for the CNAP RD. The CNAP design may be implemented at the DoD enterprise level to secure access to a software as a service capability (e.g., DoD365); as part of a platform to provide CNAP as a service for mission application owners (e.g., CNAP for USAF Platform One); or by mission application owners for secure access to their own virtual cloud environment from the internet. Determining implementation type is a MO decision.

The following summarizes the sections of this document:

- Section 1 provides the purpose and scope for this document along with an overview of the DoD enterprise, including the user community and computing environment. It also describes what the RD provides to the intended audience and identifies a set of user stories describing the required capabilities.
- Section 2 describes the assumptions and principles for the RD and its implementation.
- Section 3 describes the DoD CNAP vision, presents the CNAP concept, and provides an overview description of each of the CNAP capabilities.
- Section 4 describes the data flows between the CNAP components.
- Section 5 describes the CNAP logical pattern, and four reference implementations intended to demonstrate how capabilities may be implemented to meet a broad set of mission needs.
- Section 6 provides the shared roles and responsibilities among the DoD Enterprise, MO, and Cloud Service Provider (CSP).

1.1. Purpose

The purpose of the CNAP RD is to describe and define the set of capabilities, fundamental components, data flows, logical design pattern, and derived reference implementations for deploying, connecting to, and operating a CNAP. The RD guides the development of next generation cybersecurity capabilities to enable connectivity from the internet into DoD resources and services hosted in commercial cloud environments.

The purpose of a CNAP is to provide secure authenticated and authorized access to DoD resources hosted in commercial cloud following zero trust architecture (ZTA) principles[4]. Zero trust principles enable authorized privileged user access to cloud resources while limiting end user access to authorized application interfaces. A CNAP provides person entities (PE) (e.g., end users and privileged users) and non-person entities (NPE) (e.g., laptop, servers, smartphone, etc.) access to cloud enclaves using a combination of cloud native and cloud ready security mechanisms. Further, a CNAP allows authorized outbound access to the internet, for example, to enable software repository synchronization of COTS patches or new versions of Free and Open-Source Software (FOSS) projects and system-to-system interfaces with mission partners such as other Federal Departments. The security design reduces the attack surface by enforcing zero trust concepts including authentication, Software Defined Perimeter (SDP), micro-segmentation, separation of duties, and dynamic authorization to provide secure access from untrusted environments.

1.2. Scope

This CNAP RD provides the basic design for developing the capability to provide secure internet ingress and egress access to and from MO cloud enclaves[5]. The guidance applies to unclassified environments at

[4] The CNAP RD cannot include all ZTA principles as the scope of ZTA is much larger than access point security.
[5] A MO cloud enclave is the virtual private cloud space (all subnets) associated with an organization cloud account (e.g., Azure Tenant, AWS VPC).

Impact Levels 4 and 5 (IL4/5)[6]. However, the zero trust principles and zero trust network architecture in this reference design can be applied to IL6 environments but would not provide for internet access. The RD includes capabilities and reference implementations for a CNAP to access MO cloud environments only.

1.3. Intended Audience

The CNAP RD is for the Combatant Commands, Military Departments, DISA, other Defense Agencies, and Mission Partners who develop, test, secure, operate, and use applications in the cloud. The intended audience for this RD includes the following:

- Application Developers and Testers – This RD provides application developers and testers a high-level technical understanding of using the CNAP to access cloud resources from the internet for different types of clients (i.e., thick, thin, zero).
- Systems Engineers – This RD provides systems engineers design aspects on required infrastructure components to be deployed as configured for establishing a CNAP.
- Systems Administrators – This RD provides systems administrators the basic technical layout of a CNAP and the capabilities that systems administrators must configure, operate, and monitor.
- Security Engineers – This RD provides security engineers, including personnel from security operation centers (SOC) and/or Cybersecurity Service Providers (CSSP), the fundamental security design and components required to secure and monitor CNAPs.

1.4. High Level User Stories

The CNAP RD is based on user stories. A user story is a tool used to capture a description of a software feature or capability from an end user perspective. The stories describe the type of user, what they want, and why. It helps to create a simplified description of a set of requirements. The following user stories are selective examples and are not meant to represent an exhaustive list of stories.

Software Team Access

- An authorized developer working from the company office on a company-provided laptop is supporting a DoD contract. The company has a contract with a DoD agency with applications located in a Federal Risk and Authorization Management Program (FedRAMP)-approved cloud with a DoD Provisional Authorization (PA) at Impact Levels 4 and 5 (IL4/5) and a Service Authorization to Operate, Authorization to Connect (ATO/ATC). The developer needs to access the agency's software factory from the company network using the company-provided laptop. In addition, the developer needs to pull updates from the internet into the development and testing environment.
    - Design Notes: Access to the software factory is either:
        - From the internet to the CSP SaaS DevSecOps pipeline.
        - From the internet to a DevSecOps software factory instantiated from hardened containers, such as Iron Bank[7] containers, via the cloud hosted CNAP.
- An authorized developer, working for a defense contractor company, working onsite at a DoD agency, is instructed to work remotely. The developer has a government furnished laptop. To optimize connectivity and increase efficiency and productivity, the developer needs direct access to the agency's software factory from home over the internet. The agency has applications located in a FedRAMP-approved cloud with a DoD PA at IL4/5.
    - Design Notes: Access to the software factory is either:

[6] Impact Level definitions can be found in the DISA Cloud Computing Security Requirements Guide. IL6 and above are not included in this RD.

[7] Iron Bank is a centralized artifacts repository with a pre-approved collection of solutions.

        - From the internet to the CSP SaaS DevSecOps pipeline. If using a Virtual Private Network (VPN) into the Non-classified Internet Protocol (IP) Router Network (NIPRNet), then must exit through the IAP first.
        - From the internet to a DevSecOps software factory instantiated from hardened containers, such as Iron Bank containers, via the cloud hosted CNAP.
- An authorized developer is working remotely upgrading code for a navigation system. The code is developed in the cloud but runs on a specific vehicle system platform (e.g., tank, jet, or ship). The developer uses an authorized end user device and needs to connect to a software factory in the cloud via the internet.
    - Design Notes: Access to the software factory is either:
        - From the internet to the CSP SaaS DevSecOps pipeline. The user's traffic must enter and exit through the IAP if using a VPN into the NIPRNet.
        - From the internet to a DevSecOps software instantiated hardened container, such as an Iron Bank container, via the cloud hosted CNAP.
- An authorized software tester, working for the U.S. Government, works exclusively from home on a personal computer. The agency has applications in a FedRAMP-approved cloud with a DoD PA at IL4/5. The tester needs to access the agency's testing tools from home over the internet and needs to access a set of SaaS-based tools from the internet to the testing environment.
    - Design Notes: Testing as Code is developed in the software factory. Access to the software factory is either:
        - From the internet to the CSP SaaS DevSecOps pipeline.
        - From the internet to a DevSecOps software factory instantiated from hardened containers, such as Iron Bank containers, via the cloud hosted CNAP.
    - Design Notes: Access directly to test tools in the development and test environments is via the CSP portal => bastion host.
- The repository for a DevSecOps software factory needs patches and version updates from a software firm or open-source project located on the public internet. The patches and updates can be pulled manually by a PE or automatically by an NPE tool. The source code must be scanned before it is added to the repo.
    - Design Notes: Access by authorized services to pull source code and/or binaries from authorized targets is via the cloud hosted CNAP.

System & Security Admin Access

- A system administrator needs access to the bastion host for the initial deployment of the Infrastructure as Code and Configuration as Code of a production environment. After initial setup, that administrator needs access to the software factory to sustain the Infrastructure as Code used to deploy, update, and monitor that production environment. They also need "just in time" access to the bastion host for "in emergency, break glass" access to resources in all environments.
    - Design Notes: Access to the bastion host is through the CSP portal.
    - Design Notes: Access to the code repo and pipeline is either:
        - From the internet to the CSP SaaS DevSecOps pipeline.
        - From the internet to a DevSecOps software factory instantiated from hardened containers, such as Iron Bank containers, via the cloud hosted CNAP.
        - From the DISN via BCAP to a software factory instantiated from hardened containers, such as Iron Bank containers, via the cloud hosted CNAP.

- A CSSP needs access to the security dashboard with drill-down capability to identify and remediate configuration non-compliance. A CSSP also needs access to log analysis to identify and perform root cause analysis on security incidents.[8]
    - Design Notes: Access to the security dashboard and tools is either:
        - From the internet to the CSP PaaS security dashboard.
        - From the internet to a security dashboard instantiated from hardened containers, such as Iron Bank containers, via the cloud hosted CNAP.
- An NPE needs access to interface with NPEs in the cloud to perform system/security administration tasks.
    - Design Notes: Access to NPEs from NPEs is either:
        - From MO on-premises, on DISN, NPEs.
        - From the internet Original Equipment Manufacturer (OEM) security patching/updating NPEs.
        - From other MO enclaves on the same CSP cloud backbone or internet.

End User Access

- PE or NPE on DISN needs access to/from a production application in the commercial cloud.
    - Design Notes: Access is via the BCAP or IAP.
- PE or NPE on the internet needs access to/from a production application in the commercial cloud.
    - Design Notes: Access is via the cloud hosted CNAP.
- PE or NPE on DISN needs access to/from a SaaS application in a Fit-for-Purpose Cloud.
    - Design Notes: Access is via zero trust network access (ZTNA).
- PE or NPE on the internet needs access to/from a SaaS application in a Fit-for-Purpose Cloud.
    - Design Notes: Access is via ZTNA.

The following sections describe a CNAP RD that satisfies the requirements in the user stories listed above.

[8] Log data collected or accessed from IL4/5 systems must be handled properly. Some log data may be classified CONFIDENTIAL or higher and therefore is subject to classified information handling and storing requirements.

2. Assumptions and Principles

2.1. Assumptions

This document makes the following assumptions:

- The CSP has a DoD PA at IL2/IL4/IL5 through the DoD Cloud Authorization Service managed by DISA.
    - Status of a CSP approval can be found at: https://disa.deps.mil/org/RMED/cas/SitePages/CSOCatalog.aspx
- For enterprise implementations of the CNAP, for example, with Platform One's CNAP as a Service, the CNAP is approved for DoD-wide use through reciprocity. For dedicated CNAP implementations, the MO's Authorizing Official is the approving official for the implementation of the CNAP.
- CNAP is a next generation virtual IAP[9] and not a BCAP, providing moderated access from the internet.
- The DoD Enterprise Identity Provider (IdP)[10] authenticates users with DoD approved PKI or DoD approved multifactor authentication (MFA) credentials and asserts that identity, along with associated claims, to the SaaS, CSP portal, or MO's Directory Service.
- Publicly routed IP space is not restricted to DoD allocated IP.
    - DoD specific systems can be assigned DoD IP.
- ZTA tenets, in whole or partially, are employed in the design.
    - All data sources and computing services are considered resources.
    - All communication is secured regardless of network location.
    - Access to individual enterprise resources is granted on a per-session basis.
    - Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting endpoint—and may include other behavioral and environmental attributes.
    - The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
    - All PE and NPE authentication and authorization are dynamic and strictly enforced before access is allowed.
    - The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.
- A migration to ZTA is necessary for MOs. This requires MOs to develop a migration strategy that is aligned to the DoD Zero Trust Strategy and Reference Architecture.
- A CNAP provides secure access for authenticated and authorized PE and NPE to cloud resources only, and not to MO on-premises resources.
- The CNAP RD is developed for IL4/5 and is not required for IL2.

2.2. Principles

There are several key principles in implementing CNAP:

- Access to SaaS and CSP portal environments leverage the CSP's perimeter and internal security capabilities, which have been evaluated as part of the DoD IL4/5 PA.

[9] Internet Access Points (IAP) employ security sensors providing more advanced cyber security capabilities where a Boundary Cloud Access Point (BCAP) on provides a whitelist of allowable IP addresses.
[10] Details regarding The DoD Enterprise Identity Provider (IdP) can be found in the ICAM Reference Design.

- Proposed solution is a Cloud Native "Access Point" solution leveraging zero trust principles and implemented using cloud native security or commercial solutions and access services that are fully elastic providing high availability and scalability, hosted on a cloud with a DoD PA.
- The CNAP architecture can be cloud agnostic, leveraging virtual appliances and COTS/FOSS software; can use CSP resources and services for cloud-specific instantiation; or can be a mix of both options, leveraging cloud agnostic services to add more security to the CSP resources and services design pattern. The best practice for instantiating and configuring a CNAP is through automated deployment (i.e., Infrastructure as Code (IaC)) using selectively developed templates specifically for the DoD to accelerate the ATO process[11].
- The CNAP architecture is based on zero trust principles: authenticated and authorized data flows, trusted sources of updates/libraries, and bi-directional PKI authentication for NPEs.
- A CSSP has access to the log and scan results data from the CNAP environment to perform the following functions:
    - Continuous monitoring
    - Vulnerability assessment
    - Endpoint security services
    - Incident management & response
    - User monitoring/insider threat
    - Attack sensing and warning
    - Log aggregation
    - INFOCON/CPCON notification
- Endpoints must have appropriate device state (e.g., configuration, security patches, system name, etc.) and users must have the appropriate identification, credential, authentication, and authorization to be allowed to connect. Bring Your Own Authorized Device (BYOAD)[12] endpoints are consistent with emerging BYOAD policies to allow device state verification.
- The CNAP uses DoD approved PKI or DoD approved MFA credentials, and uses the DoD Enterprise IdP for federated authentication in accordance with the Identity, Credential, and Access Management (ICAM) Reference Design.[13]

[11] DoD IaC templates are available at https://code.il2.dsop.io/dod-cloud-iac.
[12] Development of a BYOAD policy is a recommendation in Appendix C of this document.
[13] For details regarding DoD Enterprise IdP and federations, refer to the ICAM Policy and Reference Design.

3. Capability Overview

This section provides the high-level capability perspective of a CNAP and includes the transformational vision (DoD Architecture Framework (DoDAF) Capability Viewpoint (CV-1)), a description of CNAP goals and objectives, and the capability taxonomy (DoDAF CV-2).

The DoD CNAP vision is depicted in Figure 1. CNAP capabilities improve mission effectiveness by providing core secure connectivity to authenticated and authorized entities (person and non-person), and authorized ingress and egress capabilities, along with security monitoring and compliance enforcement. These operational capabilities define a CNAP.

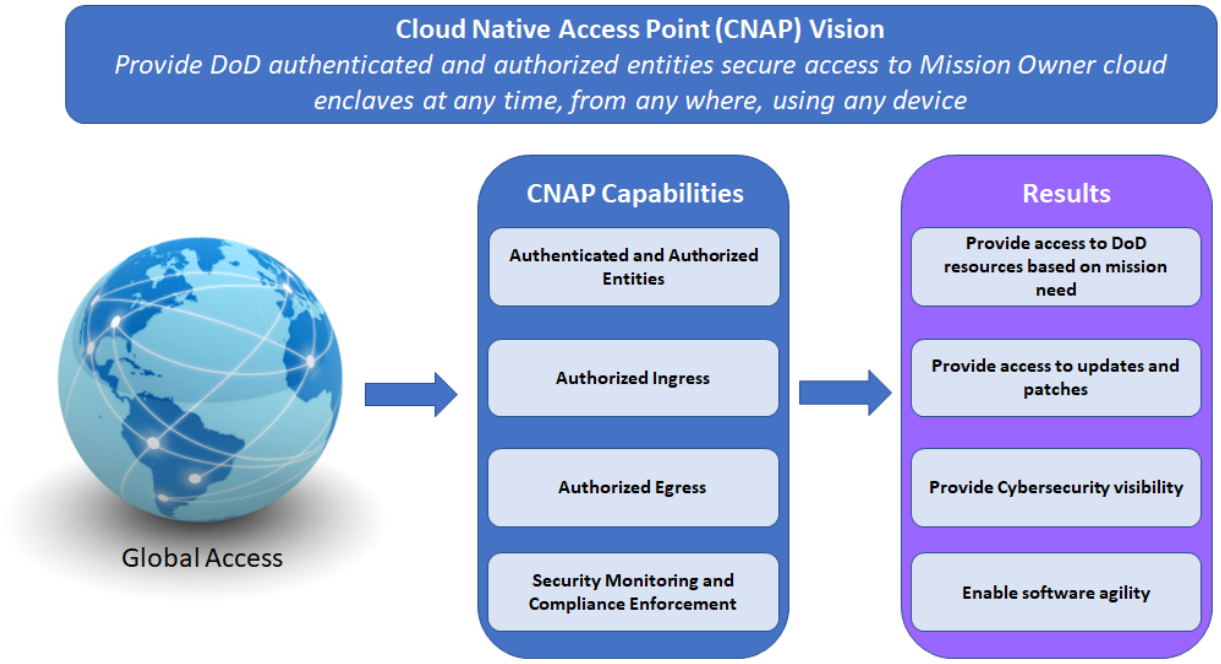

Figure 1 – Cloud Native Access Point Vision: Capability Viewpoint (CV-1)

A CNAP provides modernized cybersecurity capabilities. These capabilities are based on cloud services and align to the DoD ZTRA CV-2 Zero Trust Pillars of Connect (T1), Access (T2), and Monitoring and Compliance (T8).[14]

The high-level operational concept for CNAP including paths in and out of cloud environments is shown in Figure 2. This diagram serves as the DoDAF Operational Viewpoint (OV-1) and as an organizing construct for CNAP enablers, capabilities, business functions, and services. It identifies the classes of entities: authorized users (PEs) and authorized endpoints such as other systems or microservices (NPEs), authorized ingress, authorized egress, and security monitoring and compliance enforcement. The paths in and out of the cloud environment, via the CNAP, are depicted in Figure 2.

[14] The Zero Trust Pillars can be found in the DoD ZTRA at https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf

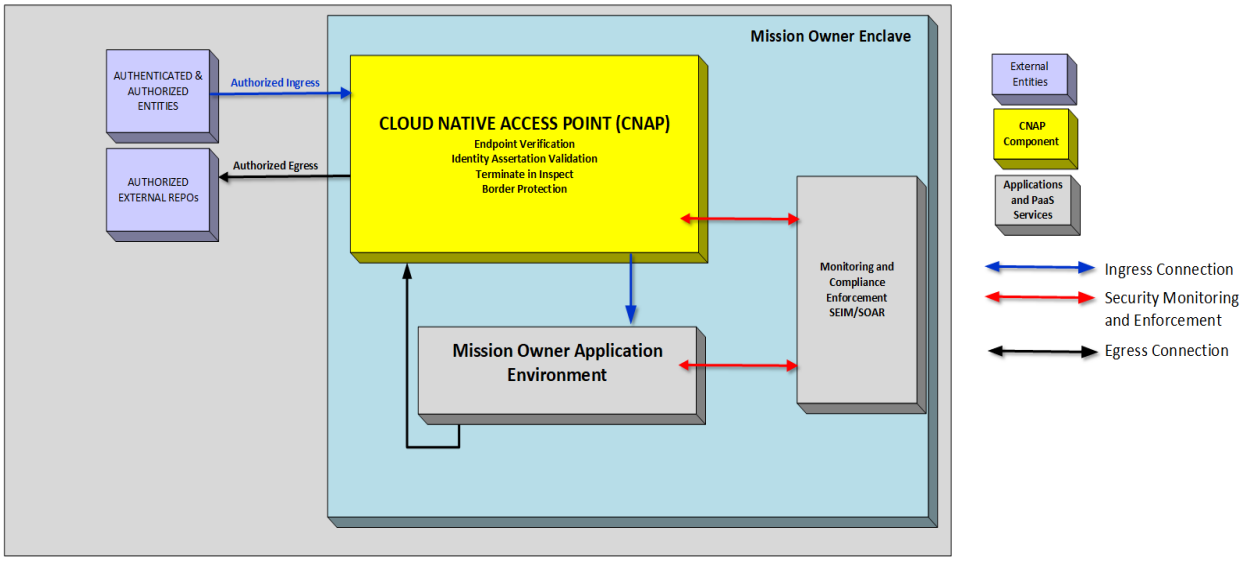

Figure 2 – Cloud Native Access Point Vision: Operational Viewpoint (OV-1)

3.1. CNAP Capability Taxonomy Overview (DoDAF CV-2)

The DoD CNAP capability taxonomy is shown in

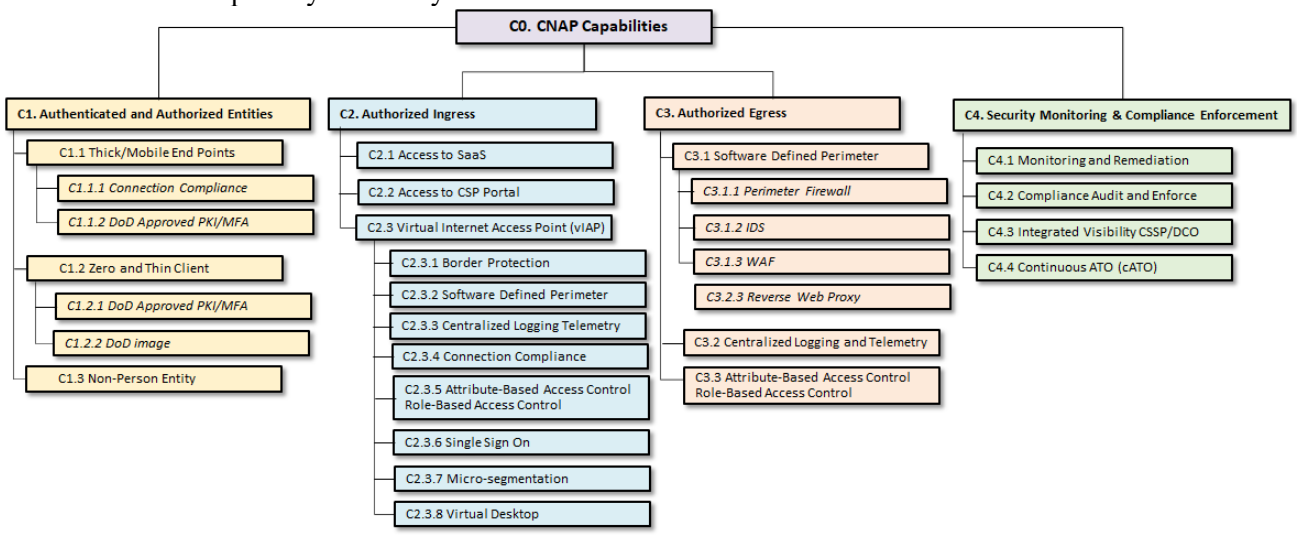

Figure 3. It consists of four high-level parent capabilities: Authenticated and Authorized Entities, Authorized Ingress, Authorized Egress, and Security Monitoring and Compliance Enforcement. These capabilities collectively provide the DoD with the ability to enable authenticated and authorized entities (persons and non-persons) access to MO cloud resources and applications in a secure manner. It provides some of the security layers within a ZTA which are referenced on page 6.

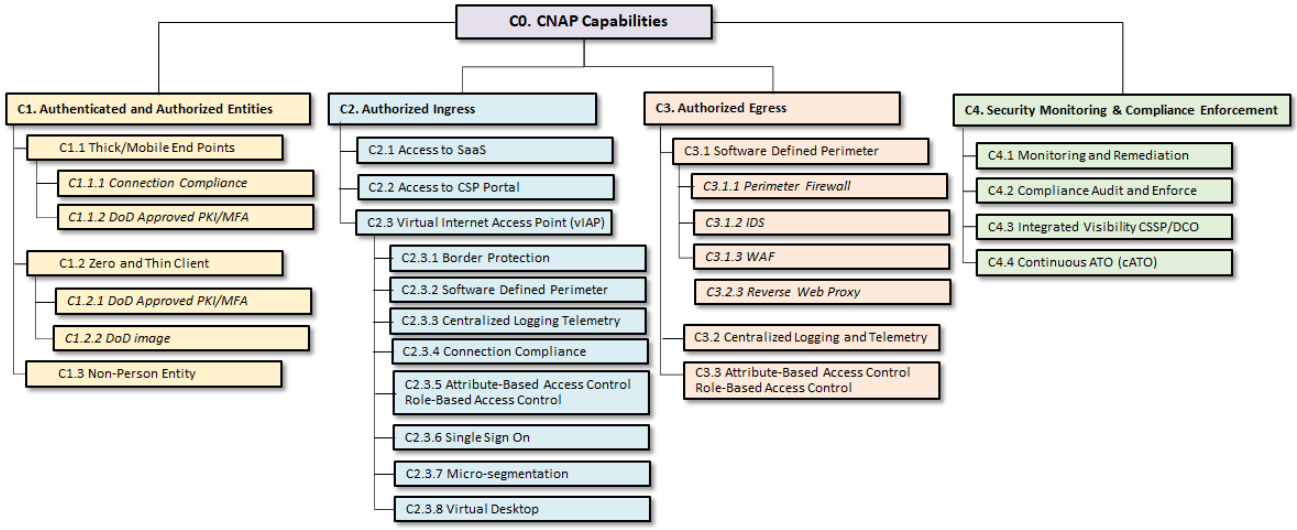

Figure 3 – CNAP Capability Taxonomy (CV-2)

3.2. Core CNAP Capabilities

The following sections describe the core CNAP capabilities, and their subcomponents identified in Figure 3. The intent of this section is to enumerate and describe the capabilities that must be part of a CNAP, but not to dictate exact implementations.

C.1 - Authenticated and Authorized Entities

The authenticated and authorized entities focus on three second level capabilities – thick/mobile endpoints, zero/thin clients, and NPE system/microservice interfaces. Below is a description of each of the three capabilities:

Thick and Mobile Endpoints – Thick and mobile endpoints for access into the CNAP are managed through a connection compliance and zero trust model. Endpoint management can be client agent based or server based. Authentication is via DoD approved PKI or DoD approved MFA. The CNAP uses Attribute and Role-Based Access Control – for example – user role in Active Directory, geo-fencing, time of the day, or device state for decision and enforcement of coarse-grained access control.

Zero and Thin Clients – Virtual Desktop Infrastructure (VDI) can be accomplished using similar capabilities of the thick and mobile endpoint access, such as MFA, single sign on, and identity management protections. Advantages of using zero or thin clients include the following example: system administrators can centrally manage the desktop image, the boot image is reset for each login, and sensitive data such as source code remains under the control of the MO.

NPE System/Microservice Interfaces – NPE to NPE system interface patterns are accommodated in a CNAP design. In modern architectures, applications are decomposed into smaller microservices which each perform a single function. This allows for less complexity in maintaining each microservice, which provides software agility. For the entire system to function, there is considerable east-west communications among the microservices and with other systems. These microservices and partner systems can reside in the cloud, in a different cloud, or on-premises. The CNAP RD accommodates both traditional and modernized NPE to NPE patterns.

C.2 - Authorized Ingress

Authorized ingress is either via a CSP managed front end in a SaaS offering, or via the virtual IAP in front of developed applications in the general-purpose cloud.

Terminate and Inspect – Inbound connections are terminated and inspected at CNAP's ingress.

Access to SaaS – The SaaS perimeter security acts as the gateway for users and system interfaces to access the MO tenant. Access is via HTTPS (HTTP over TLS). The CSP is approved to provide boundary protection in front of the SaaS entry point (which is an inherently Government function, as defined in the CIO Memo, "DoD Cybersecurity Activities Performed for Cloud Service Offerings).

Access to CSP Portal – The CSP portal acts as the gateway for software team access into the MO's enclave. Access is via HTTPS (HTTP over TLS). The CSP is approved to provide boundary protection in front of the SaaS entry point (which is an inherently government function, as defined in the CIO Memo, "DoD Cybersecurity Activities Performed for Cloud Service Offerings). Access to manage cloud IaaS and PaaS resources is via the CSP portal. For "break glass" access to resources, access to jump servers such as a bastion host is through the CSP portal via HTTPS; the bastion host then connects to the resource via SSH or RDP internally. Additionally, the zero-trust controller can make specific endpoints accessible to privileged access users to allow other network protocols such as SSH or RDP.

Virtual Internet Access Point (vIAP) – The vIAP acts as the gateway to developed applications, IaaS, and PaaS over web protocols including HTTPS, formatted messaging – Advanced Message Queuing Protocol (AMQP), chat – Extensible Messaging and Presence Protocol (XMPP), and streaming voice and video – Real-time Transport Protocol (RTP).

The CNAP directs authenticated PE and NPE ingress traffic to a Policy Enforcement Point which refers to a Policy Decision Point (PDP) to make dynamic access control decisions based on a managed set of digital security policies. Some authorization rules[15] are managed centrally; fine grained application- and data object-level authorization rules are delegated to the mission application/data owner.

Authorization decisions for access to DoD commercial and government cloud resources behind the CNAP take into consideration several additional factors beyond the authentication of the credential presented by the user such as the type and state of the endpoint client device (managed vs unmanaged), the geographic location from where the user is accessing the requested resource, what time the access is being requested, and the user's role and level of privilege, in accordance with the DoD enterprise Identity, Credential, and Access Management (ICAM) Reference Design.[16]

The Policy Enforcement Point leverages a suite of cybersecurity services, which includes, at a minimum, firewall, web application firewall, intrusion detection and prevention, some of which may be implemented as cloud native services configured by the CNAP provider.

The CNAP RD provides a set of capabilities and design patterns which can be tailored to meet an individual MO's requirement. The following security capabilities must be enabled at the CNAP boundary in some form. However, specific technologies used to establish capabilities are not mandated.

- Border Protection:
    - Perimeter Firewall – Inline security component that identifies network traffic and applies filtering rules to determine inbound/outbound access and can ingest threat intelligence

[15] Standard digital security authorization rules that are centrally managed are to be determined.
[16] The CNAP RD is aligned to the ICAM Reference Design. Details regarding ICAM principles can be found in the ICAM Reference Design document.

from external sources to enhance functionality. This firewall is applicable to non-HTTP/HTTPS traffic.
    - Intrusion Prevention System – Inline security component that scans for malicious network traffic using both signature-based and anomaly-based detection to support decisions to allow or drop traffic packets in near real-time.
    - Web Application Firewall – Inline security component that protects connections over HTTP or HTTPS against targeted attacks at the application layer through the application of rulesets which addresses common threats such as cross-site scripting and SQL injection.

- Software Defined Perimeter (SDP):
    - Each device is authenticated and authorized via the DoD Enterprise IdP using DoD approved PKI.
    - Each managed device is subject to continuous monitoring of security baseline compliance.
    - Access for each device is restricted using Single Packet Authorization (SPA).[17]
    - Each entity is authenticated and authorized via the DoD Enterprise IdP using DoD approved PKI or DoD approved MFA.
    - Encrypted and authenticated communication sessions leveraging Mutual TLS (mTLS) are used to set up micro-segmentation restricting network level access to authorized resources only. Security controls within the Controller provide granular access control enforcement based on a security attestation regarding the user's roles and privileges, attribute values, and environmental conditions (e.g., endpoint is patched, geolocation, time of day).

- Centralized Logging and Telemetry: Log, alert, and event data generated by the CNAP security and access management services are tagged, logged, and sent to a centralized log management service. CNAP telemetry is made available to the designated CSSP in the cloud environment. The CSSP provides Defensive Cyber Operations (DCO) services for the CNAP including continuous monitoring, incident handling & management, attack sensing & warning, and insider threat detection.

- Connection Compliance/Device Enforcement: Connection compliance and device enforcement enforces control of managed thick or mobile client endpoints connecting through the CNAP. Endpoint devices must be authenticated and authorized.

- Attribute Based Access Control (ABAC)/Role Based Access Control (RBAC): ABAC and RBAC are used to support authorization decisions. User attributes asserted by the identity provider, as well as device attributes, are evaluated against the roles and privileges associated with the user to inform connection compliance decisions[18]. Anomalous events such as a user attempting to connect from a geographic location which deviates significantly from their attribute profile requires further evaluation by the Policy Decision Point.

- Single Sign On (SSO): Federation among the DoD Enterprise IdP, mission partner IdPs, and the CSP's internal IdP enables single sign-on using DoD approved PKI and DoD approved MFA.

[17] SPA is a technique for securely communicating authentication and authorization information across closed firewall ports to allow temporary access. SPA cloaks/hides all surrounding resources rendering them undiscoverable.
[18] For information pertaining to which user and device attributes are asserted for ABAC, refer to the ICAM RD.

- Micro-segmentation: Micro-segmentation is the logical division of the internal network into distinct security segments at the service/API level. Use of micro-segmentation enables granular access control to, and visibility of, discrete service interface points through the creation of dedicated virtual network segments. Micro-segmentation, using Software Defined Networking (SDN), enables the automatic enforcement of digital security policies at a granular level and provides dynamic management.

- Virtual Desktop (optional service): Users with zero or thin client devices can connect to cloud resources by utilizing a cloud based VDI service hosted in the MO enclave. Connecting directly to the VDI enables the user to interface seamlessly with resources hosted in the cloud without additional security requirements being levied upon the endpoint device from which the user is connecting. Once the user has authenticated to the VDI service, all further session transactions take place within the cloud.

Security functions executed at the CNAP boundary may be pre-configured and integrated by the CSP; deployable via configuration templates made available by the CSP, via Infrastructure as Code (IaC) deployments published to an enterprise repository; or leveraging existing PaaS or SaaS CSP approved solutions. Further customization of these configuration templates, or additional GOTS or COTS solutions may be deployed to provide additional security at the CNAP boundary at the provider's discretion.

C.3 - Authorized Egress

A CNAP allows outbound connections initiated by authorized internal, cloud based NPEs (e.g., source code repositories, VDI session) to authorized external resources (e.g., COTS/FOSS software repositories). Request response conversations can be initiated by authorized NPE from the cloud to authorized targets on the internet. This functionality enables cloud-based software factories to check for software updates or security patches from trusted external sources. These connections must be explicitly defined by the MO and allowed upon request.

NPE identity creation, credentialing, maintenance, and decommission is expanded upon in the DoD ICAM Reference Design.

Additionally, for VDI use cases, users can access the internet from the VDI network segment only.

Authorized egress traffic traverses the CNAP protection suite of security capabilities. This set of capabilities includes the following:

Terminate and Inspect – Outbound connections are terminated and inspected prior to allowing egress from the cloud enclave.

Software Defined Perimeter– This includes perimeter firewall, IDS/IPS, web application firewall, and reverse web proxy.

Centralized Logging and Telemetry – Log, alert, and event data generated by the CNAP security and access management services are tagged, logged, and sent to a centralized log management service. CNAP telemetry is made available to the designated CSSP in the cloud environment. The CSSP provides DCO services for the CNAP including continuous monitoring, incident handling & management, attack sensing & warning, and insider threat detection.

ABAC/RBAC – ABAC and RBAC are used to support authorization decisions. Device attributes asserted by the identity provider are evaluated against the roles and privileges associated with the device to inform connection compliance decisions. Anomalous events such as a device attempting to connect to unauthorized targets are not allowed.

All telemetry generated as a result are monitored within the MO's environment by the CSSP and reported as appropriate. Additional scanning and validation of the data and resources, such as source code, is required to be brought into the cloud environment, but is outside the scope of the CNAP RD.

C.4 - Security Monitoring and Compliance Enforcement

CNAP security monitoring provides comprehensive threat mitigation and compliance enforcement capabilities. The recommended solution is to leverage CSP PaaS using approved templates such as Blueprints and Cloud Formations or Cloud Agnostic templates in Repo One[19] using Terraform. Note that when the target production environment is not in the cloud (e.g., embedded systems in weapons platforms) or when being cloud agnostic is an important operational consideration, a solution using instances of hardened artifacts from a DoD Centralized Artifact Repository (DCAR) (e.g., Iron Bank) should be implemented.

The tools and services used to provide this capability should be the same set of CSP PaaS based security services and tools used for the rest of the MO cloud environment. All applications, appliances, and devices that comprise the CNAP are monitored in accordance with applicable DoD Security Requirements Guides and DoD Security Technical Implementation Guides. CNAP security monitoring and compliance capabilities should align to, and be integrated as needed, with DCO.

3.2.4.1 Monitoring and Remediation

This RD encourages the use of cloud-based log aggregation, security information event management (SIEM), and security orchestration automated response (SOAR). All components within CNAP are monitored for security events and configuration compliance. To do this, security monitoring services must be able to connect to these logs, analyze events as they occur, and determine if a threat exists or is emerging.

Additionally, CSPs' tools offer connectors or have open APIs that allow security event data to be exported to market leading 3rd party tools that might be used in DCO. Most of these tools have advanced threat intelligence using machine learning (ML) and artificial intelligence capabilities. This threat intelligence capability identifies real and potential threats and automatically remediates within seconds. Two examples of this type of service are AWS GuardDuty and Azure Sentinel. The use of these commercial CSP cloud security services for monitoring a CNAP are highly encouraged in this RD. However, 3rd party monitoring and remediation tools are not excluded and may be required in certain cases.

3.2.4.2 Compliance Auditing and Enforcement

Configuration of components that comprise a CNAP are controlled and managed through automation using cloud-based compliance tools. These tools provide a continuous auditing capability that allow MOs to see in near real-time the compliance status of systems. Additionally, these tools can be configured to enforce compliance ensuring configuration drift does not occur and RBAC assignments do not change. Examples of such tools are Azure Blueprints and AWS CloudFormation. Cloud agnostic IaC options such as Terraform or Ansible can also be used; these tools require separate sets of declarative statements for each CSP environment.

3.2.4.3 Integrated Visibility with CSSP/DCO

Event data collected by the CNAP monitoring capability is aggregated into a centralized log stack so it can be easily transmitted, or otherwise made available, for upper-level CSSP and/or DCO Boundary Cyber Defenders. This can be accomplished by establishing live feeds to a centralized CSSP/DCO

[19] Repo One is the DoD repository for source code for DevSecOps development methodology.

repository. In doing so, MOs provide DoD upper tier security providers with visibility of the cybersecurity posture allowing correlation, analysis, and identification of attacks across the enterprise.

3.2.4.4 Continuous Authorization to Operate (cATO)

The monitoring and compliance capabilities, with integrated visibility, facilitate an ability to maintain Continuous Authorization (CA). Compliance information is provided to an Authorizing Official via CSP security and compliance dashboards. The information is provided in near real-time creating the ability for AOs to audit compliance of systems on demand and without relying on IT staff. A CA Guide/Playbook is currently in draft.

4. Data Flows

This section provides generic data flows for the CNAP capabilities described above. Figure 4 shows the data flow of a CNAP within its context.

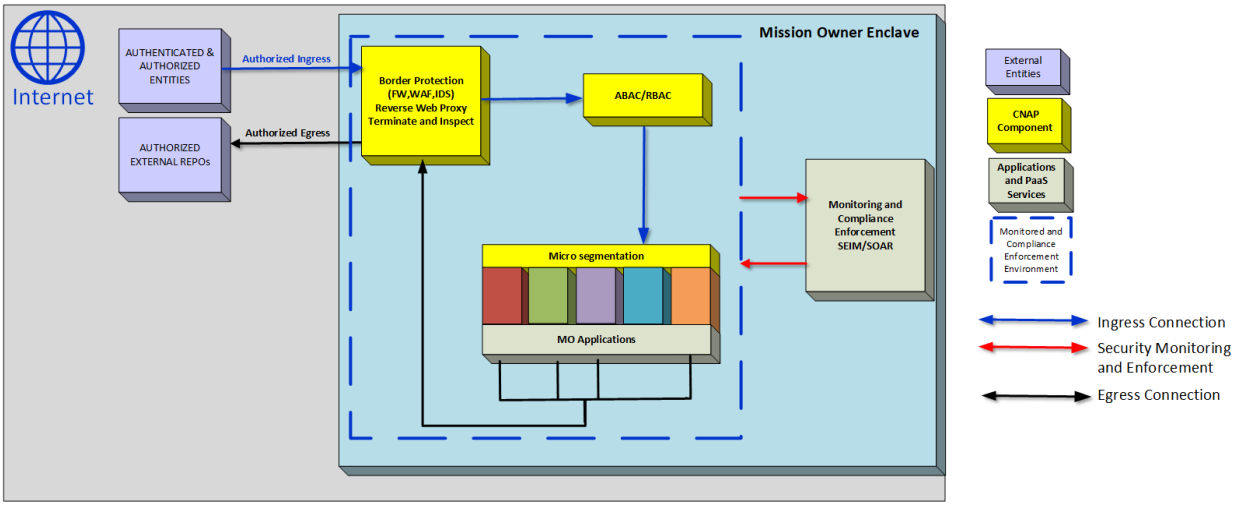

Figure 4 – CNAP Data Flow

The use of SDN facilitates micro-segmentation, an underpinning capability in ZTAs. This allows for separation, or disaggregation, of network traffic creating a Control Plane for functions including, but not limited to, authentication, authorization, NPE-to-NPE management, and security administration including coarse-grained grant/deny authorization decisions, and a Data Plane for PE and NPE connections to applications and data.

4.1. CSP Portal Access

Access to a CSP's portal (depicted in Figure 6) is permitted for all authenticated and authorized privileged users via an encrypted session using NSA-approved cryptography. This session is set up using the CSP's PKI certificates. Access to the CSP's portal for all authenticated and authorized privileged users is via a TLS encrypted session. The TLS session is set up using the CSP's PKI certificates. CSPs are approved to provide Boundary Protections for portal access to MO cloud enclaves. Authentication uses the DoD Enterprise IdP (via directory federations[20]), which asserts the user's identity and attributes to the CSP portal. Authentication uses DoD approved PKI or DoD approved MFA. Authorization using ABAC and RBAC is performed within the portal using business rules and role assignments that are managed by the MO.

4.2. SaaS Access

Access to SaaS services is permitted for all authenticated and authorized users via an encrypted session using NSA-approved cryptography. This session is set up using the SaaS provider's PKI certificates. CSPs are approved to provide Boundary Protections (which is an inherently government function, as defined in the CIO Memo, "DoD Cybersecurity Activities Performed for Cloud Service Offerings"). Authentication uses the DoD Enterprise IdP, which asserts the user's identity and attributes to SaaS services. Authentication uses DoD approved PKI or DoD approved MFA. Authorization using ABAC and

[20] Directory federation provides users with single sign-on access to systems and applications across organizational boundaries. Federation with the DoD Enterprise IdP allows for the use of DoD approved PKI or MFA.

RBAC is performed within the SaaS service using business rules and role assignments that are managed by the MO.

If the CSP provides sufficient native capability at the perimeter for centralized logging, log analysis, and alerting, it is recommended that the MO use that capability. As a specific example, the DoD CIO has directed that the native capabilities shall be used for Microsoft 365. (See Supplemental Guidance to the Federated Implementation of Office Collaboration Capabilities for the Department of Defense, 25 November 2020, DoD CIO.) If such native capabilities are not available from the CSP, then an enterprise approach to ZTNA should be leveraged in accordance with the DoD Zero Trust Reference Architecture[21].

A ZTNA intermediary may be configured to be in-line with SaaS resource access. The ZTNA terminates the encrypted session, invokes federated authentication via the DoD Enterprise IdP, and forwards the requesting entity's requests only to those resources to which it is authorized. Gartner, Inc. has identified the two approaches to ZTNA:

- Endpoint-Initiated ZTNA is client based ZTNA where an agent is installed on a BYOAD end user device. The agent sends information about its security context to a controller, which prompts the user for authentication. Endpoint-initiated ZTNA is problematic to implement on BYOAD devices because of the requirement to install an agent. Agentless, service based ZTNA, can also be used. In a service based ZTNA, the endpoint is inspected for security/compliance information rather than having an agent send the information. This approach is dependent upon local security policies of the client allowing the inspection. This RD does not prefer one approach over the other. Implementers need to consider the trade-offs between the two.
- Service-Initiated ZTNA is typically from the Cloud Access Security Broker/Secure Access Service Edge (CASB/SASE) market segment. A connector is installed from the application to the ZTNA provider's cloud and establishes and maintains an outbound connection. Users authenticate to the ZTNA provider via federated authentication with the DoD Enterprise IdP. The provider validates the user authorization. Only after validation does traffic pass through the ZTNA provider's cloud, which isolates applications from direct access via a proxy. The advantage of Service-Initiated ZTNA is that no agent is required on the end user's device, making it an attractive approach for unmanaged/BYOAD devices. The disadvantage is that application protocols are typically limited to HTTP/HTTPS.

Note that if multiple ZTNA products are implemented, there may be "per user" license fee impacts. It is recommended to use an enterprise approach to ZTNA to mitigate this potential cost.

4.3. Authorized Ingress

This section describes the flows into the MO's enclave as depicted in Figure 4.

Network traffic entering the MO enclave via the CNAP is forwarded differently depending on several factors, such as the type of endpoint client the traffic is originating from, as well as the service or application that the client is attempting to connect to.

Note that the primary difference in the ICAM architecture between PEs and NPEs is in the credentialing process.

For thick-client or mobile endpoint connecting directly from the internet via the Software Defined Perimeter:

1. The user initiates a connection to the MO's enclave, with the CNAP as an intermediary.

[21] DoD Zero Trust Reference Architecture v1.0, February 2021

2. An encrypted and authenticated communication session leveraging NSA-approved cryptography is initiated using the DoD PKI certificate in the CNAP.
3. The user authenticates via the DoD Enterprise IdP, or an IdP federated with DoD Enterprise IdP, using DoD approved PKI or DoD approved MFA.
4. Once authenticated and authorized, an encrypted micro-segmented connection is established between the client and the requested resource.
5. All user requests, CNAP actions, and requested resource actions are logged. Log entries are tagged and sent to a centralized log aggregation service.
    - A copy of the logs is sent to the Tier 2 CSSP.
6. End user can now communicate via an encrypted connection only with the resources they are approved to access.

For thin-client or zero-client endpoint access to VDI service:

1. The user authenticates via the DoD Enterprise IdP, or an IdP federated with DoD Enterprise IdP, using DoD approved PKI or DoD approved MFA.
2. VDI service receives an assertion and provides user access to VDI.
3. All further transactions are internal to the MO's enclave.

4.4. Authorized Egress

This section shows the flows out of the MO's enclave.

- The CNAP provides egress access from authorized cloud resources and authorized VDI applications to internet resources. This enables automatic pulling of patches and updates from internet hosted repositories and allows VDI users to access technical material on internet hosted FOSS, vendor, and training websites.
- The CNAP must use public IP addresses (IPv6 or IPv4) to enable egress routing as these addresses should be globally unique and public by default.
- IDs of specific cloud resources that are allowed to establish outbound connections must be identified at and explicitly authorized at the CNAP boundary. The CNAP should allow by exception, upon request.
- Response to egress requests, including web content and files such as source code, must be scanned. Scanning of source code is outside the scope of the CNAP and not a dependency.

4.5. Security Monitoring and Compliance Enforcement

The monitoring and compliance data flow are depicted in Figure 5. Figure 5 describes data flows in the context of the major CV-2 areas shown in Figure 3. This RD encourages the use of cloud native security monitoring and tools and allows for the use of 3rd party tools from Iron Bank. In general, there are four flow patterns. Implementers are reminded that segregation of duties and least privilege apply when setting up the security monitoring and compliance enforcement capabilities. Figure 5 illustrates the fundamental framework for monitoring/remediating and compliance auditing/enforcement.

- **Flow 1 - Data Collection Flow.** All resources push log entries to a centralized (to the MO owner) log store. The information is collected from the targets to a central repository or workspace. The logs are analyzed for security and compliance using a SIEM/SOAR tool such as Azure Sentinel, AWS GuardDuty, Splunk, or ELK. Advanced cyber intelligence and compliance auditing tools determine if action is required on a system or collection of systems based on alerts, patterns, and baseline configuration.
- **Flow 2 - Remediation and Enforcement Flow.** This is a push to the monitored targets remediating any threats or non-compliant configuration.

- **Flow 3 - Configuration Compliance Flow.** Compliance is monitored using cloud native services such as AWS Config or Azure Policies or using 3rd party tools such as Chef Inspec. A dashboard displays the near real-time state of compliance of the environment.
- **Flow 4 - Data Sharing Flow.** This flow is mandatory and can be a push or pull of security data to an external tier 2 and above CSSP. This flow contributes to the larger DoD cybersecurity visibility capability but does not provide the ability for the upper tier CSSP to actively manage security in the MO enclave.

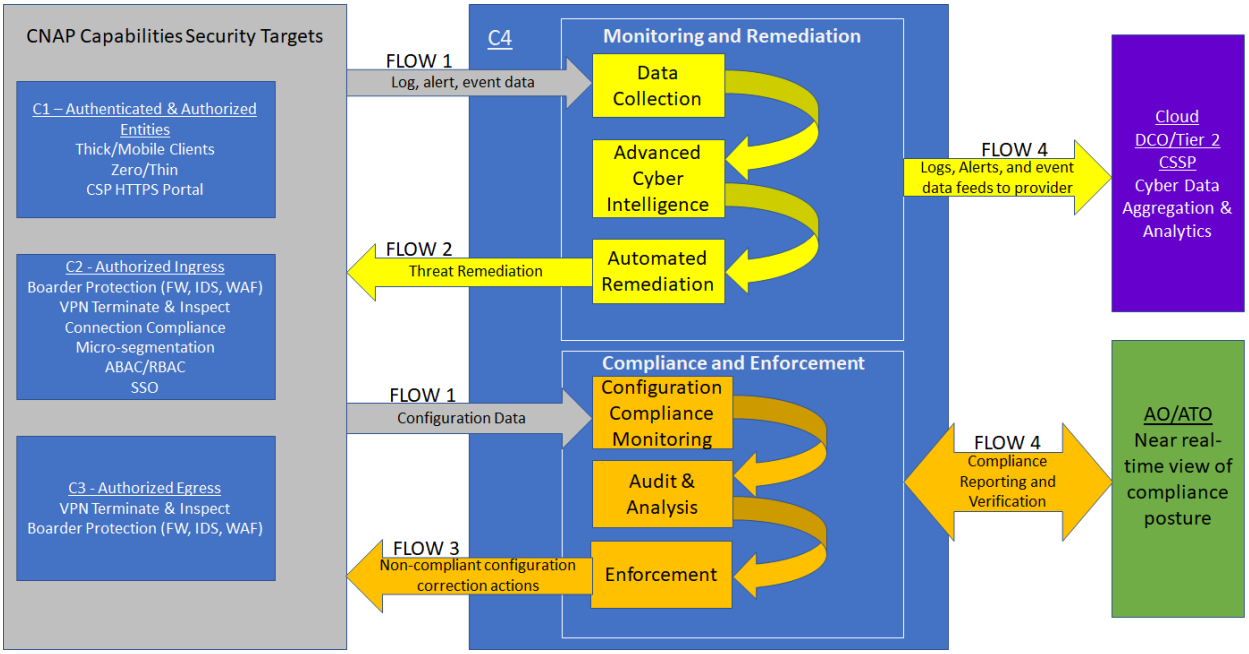

Figure 5 – High Level Monitoring and Compliance Data Flow

5. Logical Design Patterns

This section describes two logical design patterns for a CNAP.

The first logical design pattern is a CNAP that provides access from the internet and DISN to a MO cloud enclave for authenticated and authorized entities. In this pattern, entities must pass through the MO's cloud enclave front-end security platform (such as an SDP) where policy-based access is enforced prior to continuing into the MO cloud enclave (see Figure 6). This pattern is applicable to non-privileged entities for access to MO applications running in a production environment, and to privileged entities accessing MO provided platform resources and services[22].

The second logical design pattern is a CNAP that provides privileged and non-privileged entities access to SaaS services via a front-end ZTNA security platform, where policy-based access is enforced prior to continuing to the SaaS resource.

The ZTNA enforces authentication and authorization of entity requests and makes decisions to grant or deny access based on the requesting entity's identity, need-to-know, and device posture. They hide the network and resource details to mitigate the most common network-based attacks.

5.1. Access to MO Cloud Enclave

This section presents a logical design pattern for access to the MO's cloud enclave via the CNAP and ZTNA (Figure 6). An example of a CNAP in use currently is the USAF Platform One. The Platform One CNAP instance is one of several possible methods for instantiating what is in this logical design. Alternatively, curated IaC is available to instantiate a CNAP leveraging CSP resources and services.

Design Principles

- Provide global, unified, secure, and simple access to privileged and non-privileged entities.
    - Seamless and fast access to applications/services.
    - Security and access controls for all entities should be designed and applied globally.
        - Trust based on authenticated identity using DoD approved PKI/MFA.
        - Grant/deny access decisions based on authorization policy.
- Identity awareness enables comprehensive visibility and fine-grained access control.
    - Support fine granular routing and access policies using on-demand micro-segmentation.
    - Visibility into who is accessing which applications/services.
    - Attribution and non-repudiation in logs.

Implementation

- Non-Privileged Entity Access
    - All access using encrypted and authenticated communication sessions leveraging NSA-approved cryptography.
        - HTTPS to access perimeter security using ZTNA.
            - DoD managed PKI.
    - Access to mission applications over specified ports and protocols such as HTTPS, AMQP, XMPP, and RTP.
- Privileged Entity (Developer/Engineer/Administrator) Access
    - All access using encrypted and authenticated communication sessions leveraging NSA-approved cryptography.

[22] Platform services are DevSecOps software development services and environments provided to multiple MO via a single platform and allowing for separation between MO within the platform. Refer to the DevSecOps Reference Design v2 for more details.

        - HTTPS to access perimeter security using ZTNA.
            - DoD managed PKI.
        - Encrypted and authenticated communication sessions leveraging NSA-approved cryptography to access deployed resources.
    - Baseline configuration of environment implemented using IaC, produced via CI/CD pipeline.
        - Cloud resources and services, and application resources and code should be treated as immutable infrastructure – deploy new instances rather than patch or update in place.
    - Access to MO provided platform services via bastion host or session manager.
- Layered Security Features
    - PROTECT
        - Federated authentication using DoD IdP.
        - ABAC/RBAC to authorization decisions at all layers.
        - IaC – Hardened configuration of deployed components.
            - Perimeter: Firewall, WAF.
            - Network micro-segmentation.
            - Application layer resources.
        - Immutable infrastructure – deploy new instances rather than patch in place.
    - DETECT
        - Log everything, send to centralized logging capability for the enclave.
        - Continuous monitoring of the state of compliance of the environment.
        - Log analysis and netflow analysis for event & incident detection.
    - RESPOND
        - Automated remediation of non-compliant resources.
        - Alerting and recommended remediations.
        - Machine learning denial of access for malicious activities.
- Tier 3 CSSP Tools
    - Access via HTTPS.
    - Log storage, SIEM analysis, security console, dashboard.
- Egress
    - Access is granted from authorized resources such as a code repository for requesting updated software packages, patches, and configuration files from approved repositories hosted on the internet.
    - Retrieved objects run through the CI/CD pipeline to scan and harden; trust in the supply chain is limited to DoD approved sources and all retrieved objects are verified. Guidance for hardening objects/code can be found in the Container Hardening Guide.[23]

[23] https://dl.dod.cyber.mil/wp-content/uploads/devsecops/pdf/Final_DevSecOps_Enterprise_Container_Hardening_Guide_1.1.pdf

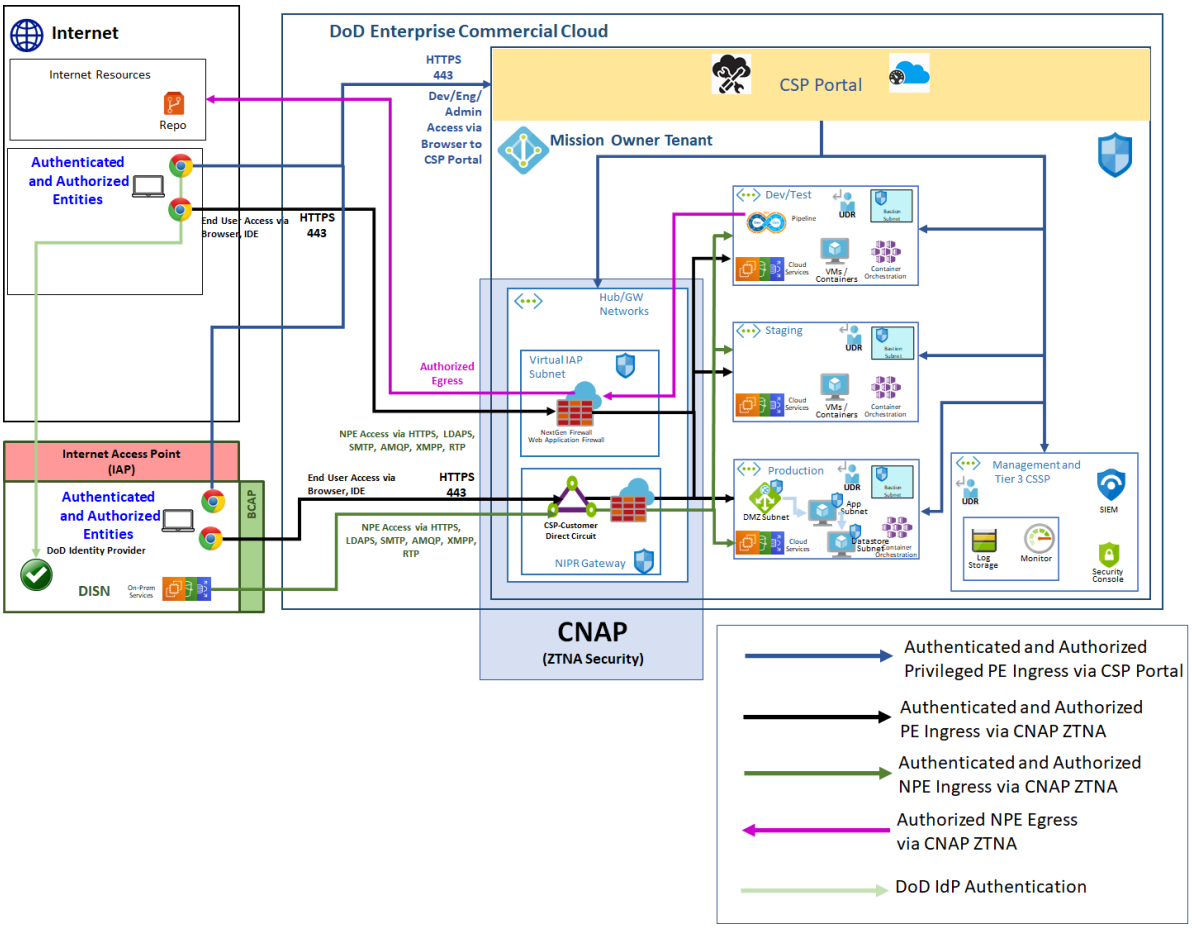

Figure 6 – CNAP Access to MO Enclave

The CNAP capabilities can be provided using CSP resources and services or can be provided using virtual appliances augmented by hardened containers from Iron Bank. A ZTNA may be provided as an enterprise service using a 3rd party SaaS offering, or may be provided as an SDP provisioned at the boundary of the MO's environment using a COTS product that has been hardened and containerized, and available from Iron Bank.

5.2. Access to SaaS Services

This section describes access to SaaS services, illustrated in Figure 7, using CNAP ZTNA at the MO enclave edge and CSP SaaS connectors. Examples of SaaS services include office automation, case management, service desk, human resources, and cloud management portals. The SaaS offering already has perimeter and internal security capabilities in place that have been evaluated as part of FedRAMP and the DoD IL4/5 PA. This section describes augmentations to those security capabilities outside of the SaaS cloud, and guidance for configuration (e.g., least privileges) that the SaaS provider enables.

Design Principles

- Global, unified, secure, and simple access.
  - Seamless and fast access to applications/services.
  - Security and access controls for all entities should be designed and applied globally.
    - Trust based on authenticated identity using DoD approved PKI/MFA.
    - Grant/deny access decisions based on authorization policy.
- Identity awareness enables comprehensive visibility and fine-grained access control.

- Support routing and access policies using on-demand micro-segmentation.
- Visibility into who is accessing which applications/services.
- Attribution and non-repudiation in logs.

Implementation

- Non-Privileged Entity Access
  - All access using an encrypted and authenticated communication session leveraging NSA-approved cryptography.
  - Entity authentication at the ZTNA via integration to DoD Enterprise IdP.
  - The ZTNA enforces authorization decisions to provide coarse-grained access control, allowing access only to end user facing interface.
  - SaaS offering enforces configured authorization decisions to provide fine-grained access control.
- Privileged Entity (Sysadmin and CSSP) Access
  - All access using an encrypted and authenticated communication session leveraging NSA-approved cryptography.
  - Entity authentication at the ZTNA via integration to DoD Enterprise IdP.
  - The ZTNA enforces authorization decisions to provide coarse-grained access control, allowing access only to administrator-facing interface.
  - SaaS offering enforces configured authorization decisions to provide fine-grained access control.
- Layered Security
  - 3rd party ZTNA offerings shift the security focus from managing network security appliances to policy-based security services. Security is based on the identity of the entity, the device, the requested resource, and environmental conditions such a geolocation, time of day, or state of compliance of the end user device.
    - TLS Endpoint
      - DoD managed PKI.
      - Decrypt and inspect encrypted traffic once.
    - Integration with DoD Enterprise IdP service.
    - Enforces authorization decisions to provide coarse-grained access control.
    - Log everything, send events as per a service level agreement to a DoD centralized logging capability.
  - CSP provided perimeter security – assessed as part of DoD PA.
    - Log everything, send events as per a service level agreement to a DoD centralized logging capability.
  - Configured security within SaaS – SaaS offerings include a set of pre-defined roles for IT privileged users and for functional privileged users. These roles are organized to support least privilege concepts. When assigning entities to roles, the following examples of separation of duties should be considered:
    - Role administrators cannot access workflows, data.
    - Workflow administrators cannot access roles, data.
    - Data configuration administrators cannot access roles, workflows, or actual data.
    - Workflow approvers cannot access roles, workflows; can access data only in relation to their assigned gates in the workflows.

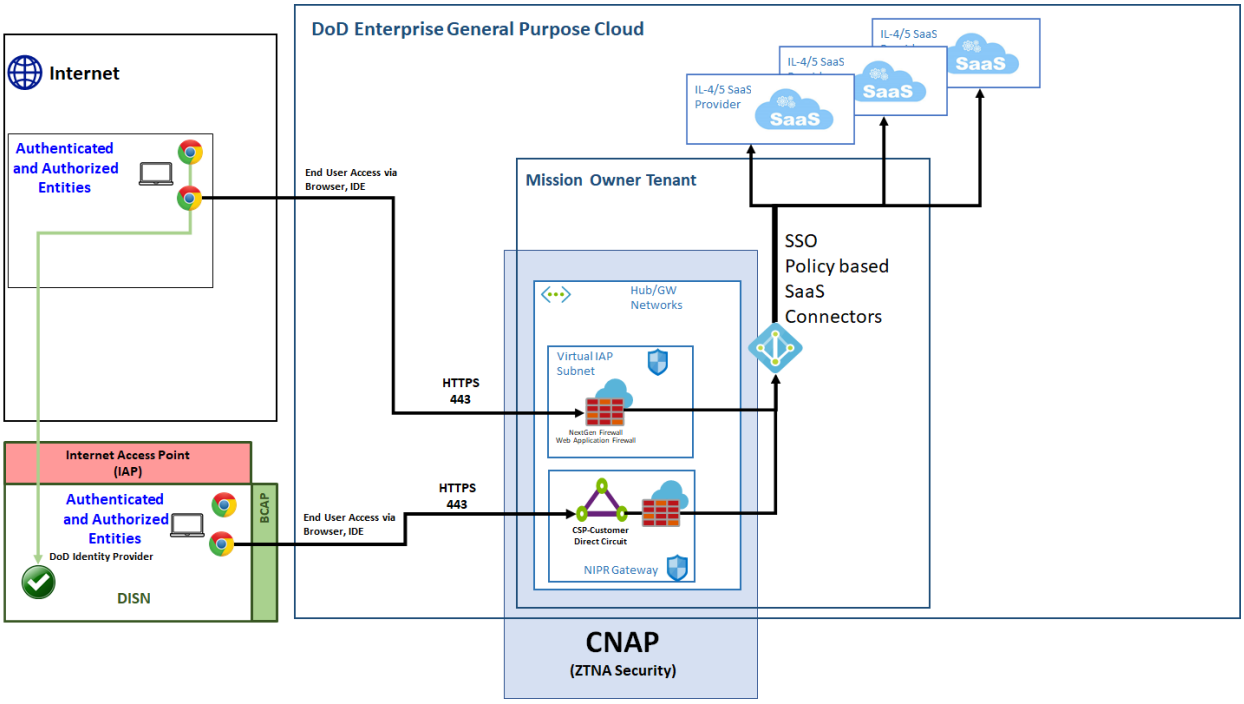

Figure 7 – Access to SaaS Services

If the CSP provides sufficient native capability at the perimeter and for centralized logging, log analysis, and alerting, it is recommended that the MO use that capability. As a specific example, the DoD CIO has directed that the native capabilities shall be used for Microsoft 365. (See Supplemental Guidance to the Federated Implementation of Office Collaboration Capabilities for the Department of Defense, 25 November 2020, DoD CIO.) If such native capabilities are not available from the CSP, then an enterprise approach to ZTNA should be leveraged.

6. Implementation Responsibilities

This section describes responsibilities for implementing a CNAP (see Figure 8). The implementation responsibility lies primarily with the MO. However, there are a few areas where responsibilities are shared. The sections below describe the roles and responsibilities for each entity related to a CNAP.

6.1. DoD Enterprise Responsibilities

In general, the DoD enterprise is responsible for the transport and security of the data to and from the CNAP. The data transport and security vary slightly if the user is accessing the CNAP from the internet or within the NIPRNET. If coming from the internet, the DoD enterprise is responsible for secure transport of the data by enforcing transport security at the CNAP. If coming from the NIPRNET to access the CNAP, the DoD enterprise is responsible for the local base routing and security stacks (which potentially may include JRSS) along with the outbound IAP connection to the internet, which then connects to the CNAP.

In both cases, the assigned upper-level (Tier 2) CSSP monitors the DoD tenant that the CNAP is hosted in via log feeds/access from/to CNAP components. JFHQ-DODIN and USCYBERCOM have authority over the CNAP, as it is part of the DoDIN. The MO is responsible for ensuring the CSSP, JFHQ-DoDIN, and USCYBERCOM have access to the requested data and access logs to properly monitor a CNAP and to initiate cyber defensive measures within the DISN (i.e., blocking at the DISN BCAP) if required. Blocking network traffic at the CNAP is performed by the MO. For example, the firewall, WAF, or IDS/IPS within the CNAP would block network traffic based on port, protocol, IP address, or signature. These blocks can be based on information from JFHQ-DODIN or the CSSP and are implemented by the MO.

Finally, any Government Furnished Equipment (GFE) required to access the CNAP, such as laptops or CACs, is the responsibility of the broader DoD enterprise and outside the scope of the CNAP.

6.2. MO Responsibilities

The MO's role is the implementer, owner, and operator of the CNAP. The MO's responsibility is to implement the components that deliver CNAP capabilities based on the design patterns laid out in this document, obtain an ATO, and operate the CNAP in accordance with the CC SRG, SCCA, DISA STIGS, and applicable NIST 800-53 Risk Management Framework controls. The most efficient way to implement a CNAP is by using DoD pre-built templates[24], commonly referred to as IaC, that automatically deploy requisite infrastructure components and establish roles, policies, monitoring, and reporting. MOs may choose to manually implement a CNAP if IaC templates do not meet their requirements. However, a better approach is to examine the IaC template and determine if small alterations would satisfy the requirement. Figure 8 summarizes the role and responsibilities for the MO for each CNAP capability cluster.

[24] DoD IaC templates that include CNAP components for Azure and AWS are available from DISA.

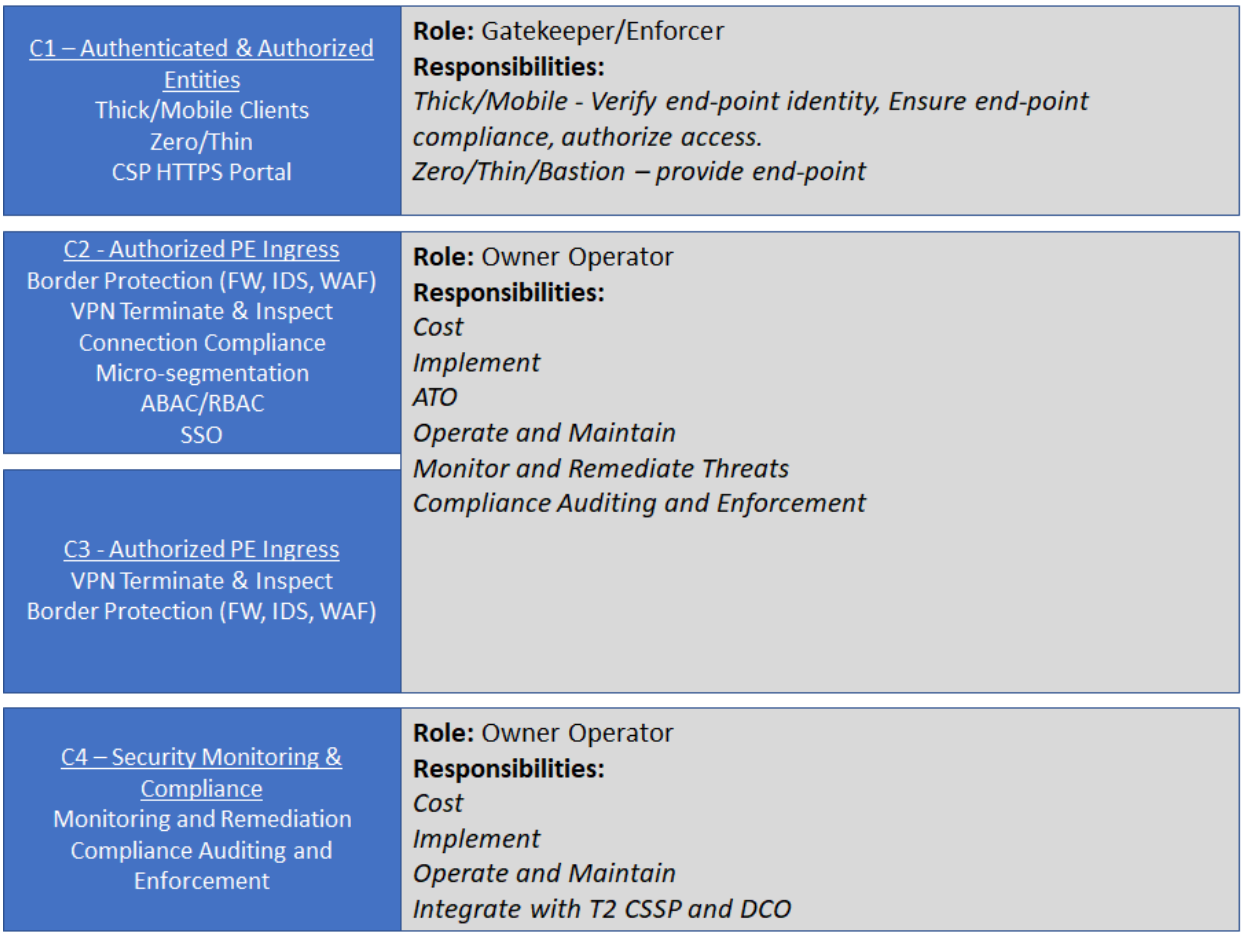

Figure 8 – MO Roles and Responsibilities

- C1. The MO is the steward for the CNAP and is responsible for ensuring mission partners are cognizant of the CNAP security including, but not limited to, endpoint client agents for thick clients and DoD approved PKI and MFA. Additionally, the MOs are responsible for educating mission partners on the egress restrictions and the process for approving egress access to an external software repository.
- C2. and C3. The MO is the owner and operator of the applications/systems that comprise the CNAP for authorized PE ingress and authorized NPE egress. The MO is responsible for associated costs, implementation, and ATO associated with CNAP capabilities. Additionally, the MO has the responsibility for security monitoring, remediation, compliance and compliance enforcement, and associated security reporting for CNAP components.
- C4. The MO can be the owner and operator of the applications and systems that provide SIEM and SOAR capabilities or may outsource these to an approved CSSP. The MO has the shared responsibility for integrating these capabilities, whether owned/operated or outsourced, with the Tier 2 CSSP and DCO.

6.3. Mission Partners

The Mission Partners' role is a consumer of MO cloud resources and services. They have the responsibility of ensuring federation with the DoD IdP.

6.4. CSP Responsibilities

The CSP provides a secure cloud environment that has been approved for DoD use by the DoD Cloud Authorization Service. The CSP is expected to follow the requirements laid out in the Cloud Computing Security Requirements Guide and is subject to the FedRAMP auditing process and responsible for obtaining PAs for PaaS CNAP components that may be implemented.

7. References

This RD references the following documents:

- DoD Digital Modernization Strategy, 12 July 2019; https://media.defense.gov/2019/jul/12/2002156622/-1/-1/1/dod-digital-modernization-strategy-2019.pdf
- DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design, June 2020; https://dodcio.defense.gov/Portals/0/Documents/Cyber/DoD_Enterprise_ICAM_Reference_Design.pdf
- DoD Enterprise DevSecOps Ref Design Version 1.0 12 AUG 2019; https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf?ver=2019-09-26-115824-583
- Department of Defense, "DoD Cloud Computing Strategy," December 2018; https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF
- DISA, "Department Of Defense Cloud Computing Security Requirements Guide, V1R3," 6 March, 2017; https://public.cyber.mil/dccs/
- DISA, "DoD Secure Cloud Computing Architecture (SCCA) Functional Requirements," January 31, 2017; https://disa.mil/~/media/files/disa/fact-sheets/secure-cloud-computing.pdf
- NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations; http://dx.doi.org/10.6028/NIST.SP.800-53r4
- Gartner, Inc., “Market Guide for Zero Trust Network Access,” June 2020
- DoD CIO, Supplemental Guidance to the Federated Implementation of Office Collaboration Capabilities for the Department of Defense, 25 Nov 2020
- DoD Zero Trust Reference Architecture v1.0, February 2021; https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf
- Container Hardening Guided, Version 1, Release 1, 15 OCT 2020; https://dl.dod.cyber.mil/wp-content/uploads/devsecops/pdf/Final_DevSecOps_Enterprise_Container_Hardening_Guide_1.1.pdf

Appendix A – Acronyms

Table 1 - Acronyms

Acronym	Definition
ABAC	Attribute-Based Access Control
AO	Authorizing Official
ATO	Authorization to Operate
AWS	Amazon Web Services
BCAP	Boundary Cloud Access Point
BYOAD	Bring Your Own Authorized Device
CA	Continuous Authorization
cATO	Continuous Authorization to Operate
CC SRG	Cloud Computing Security Requirements Guide
CI/CD	Continuous Integration and Continuous Delivery
CNAP	Cloud Native Access Point
CIO	Chief Information Officer
COTS	Commercial Off The Shelf
CPCON	Cyber Protection Condition
CSP	Cloud Service Provider
CSSP	Cybersecurity Service Provider
CYBERCOM	Cyber Command
CV	Capability View
DCIO IE	Deputy Chief Information Officer Information Enterprise
DCO	Defensive Cyber Operations
DevSecOps	Development, Security, and Operations
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DoD	Department of Defense
DODIN	Department of Defense Information Network
FedRAMP	Federal Risk and Authorization Management Program
FOSS	Free and Open Source Software
GFE	Government Furnished Equipment
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol - Secure
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
IAP	Internet Access Point
ICAM	Identity, Credential, and Access Management

Acronym	Definition
IdP	Identity Provider
IDS	Intrusion Detection System
IL	Impact Level
INFOCON	Information Operations Condition
IP	Internet Protocol
IPS	Intrusion Prevention System
JFHQ	Joint Force Headquarters
JRSS	Joint Regional Security Stack
MFA	Multi-Factor Authentication
ML	Machine Learning
MO	Mission Owner
mTLS	Mutual Transport Layer Security
NIPRNET	Non-Classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
PA	Provisional Authorization
PaaS	Platform as a Service
PDP	Policy Decision Point
PE	Person Entity
PKI	Public Key Infrastructure
RBAC	Role-Based Access Control
RD	Reference Design
RDP	Remote Desktop Protocol
RTP	Real-time Transport Protocol
SaaS	Software as a Service
SCCA	Secure Cloud Computing Architecture
SDP	Software Defined Perimeter
SIEM	Security Information Event Management
SOAR	Security Orchestration Automated Response
SSH	Secure Shell
STIG	Security Technical Implementation Guidance
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
vIAP	Virtual Internet Access Point
VNET	Virtual Network
VPC	Virtual Private Cloud
VPN	Virtual Private Network

Acronym	Definition
WAF	Web Application Firewall
ZTA	Zero Trust Architecture
ZTNA	Zero Trust Network Access

Appendix B – Glossary

Table 2 - Glossary

Term	Definition
Telemetry	The collection of measurements or other data at remote or inaccessible points and their automatic transmission to receiving equipment for monitoring.
Platform	Refers to the operating system and hardware of a server in an internet-based data center. It allows software and hardware products to co-exist remotely and at scale.
Software Defined Perimeter	A computer security framework to control access to resources based on identity and a need-to-know model in which device state and identity are verified before access to application infrastructure is granted.
Zero Trust	A security model in which devices should not be trusted by default even if they are connected to the same LAN and previously verified. An approach that advocates mutual authentication, including checking the identity and integrity of devices regardless of location and providing access to applications and services based on the confidence of device identity/health in combination with user authentication.
Impact Levels (IL)	Impact Levels are the combination of 1) the sensitivity of the information to be stored and/or processed in the cloud; and 2) the potential impact of an event that results in the loss of the confidentiality, integrity, or availability of that information.

Appendix C – Recommended Policy Updates

This section presents recommended DoD policy updates needed to enable the migration to CNAP and zero trust access.

- Current policy requires that access to DoD IL4/5 resources and services traverse an IAP to reach those services via the DISN. When those resources and services are hosted in a CSP with a DoD PA, they are not physically hosted on a DoD controlled physical or cyberspace. Policy should be updated for this hosting pattern to enable direct access from the internet, but with an appropriate zero trust architecture including perimeter and layered security capabilities.
- BYOAD is being updated currently. The new policy should accommodate devices that are under third-party management, such as other GFE from Government Agencies or corporate devices from the Defense Industrial Base.
- Currently there is no policy or guidance for Service Agencies or Military Departments clarifying the definition and authorities of the MO for CNAP in cases of cross-Service and cross-Platform capabilities when users originate from other Departments or agencies. Recommend the creation of a CNAP Governance and Policy Authorities Guide.