Onclave TrustedPlatform: A Zero Trust Approach to Cryptographically Microsegmented Layer 2 Tunnels

Abstract

The Onclave TrustedPlatform presents a novel approach to network security through the implementation of cryptographically microsegmented Layer 2 tunnels. Based on a first-principles design, the platform integrates core zero-trust concepts with advanced cryptographic identity management and dynamic network refactoring, yielding a uniquely robust, adaptable, and future-proof secure communication framework. This paper details the foundational Platform Enablers and the unique characteristics of Onclave's Layer 2 tunnel creation, demonstrating its superiority over conventional solutions and those offered by competitors such as CISCO, Fortinet, Palo Alto, and ZSCALER.

Introduction

Traditional network security models often rely on perimeter-based defenses and implicit trust within the network boundary. However, the evolving threat landscape, characterized by sophisticated lateral movement techniques and the erosion of the traditional perimeter, necessitates a more granular and dynamic approach. Zero Trust Architecture (ZTA) has emerged as a leading paradigm, advocating for continuous verification and least privilege access. Onclave's TrustedPlatform embodies these principles, leveraging a unique combination of technologies to achieve cryptographically secure microsegmentation at Layer 2.

Platform Enablers: Foundational Technologies for Zero Trust Microsegmentation

Onclave's TrustedPlatform is built upon a set of core enablers that underpin its zero-trust capabilities:

- **Private Blockchain with Integrated Certificate Authority (CA):** At the heart of the platform lies a private blockchain that houses its own CA. This internal CA is responsible for issuing and managing all digital certificates within the Onclave ecosystem. This foundational use of a private blockchain, integrated CA, and strong device identity forms the bedrock of Onclave's zero-trust model and is a key differentiator from competitors who typically rely on external CAs and less robust identity mechanisms. The use of an internal CA ensures that all cryptographic identities are tightly controlled and cryptographically verifiable, eliminating the risks associated with external CA compromise.

- **Cryptographic Identity Management:** Each encrypting device within the TrustedPlatform during registration is provisioned with post-quantum PKI cryptographic credentials. The credential key pairs, issued by Onclave’s internal Asymmetric Algorithms Generator using NIST recommended algorithms, are security stored where the public key is stored in the Onclave private blockchain for the device and the private key is stored in the TPM chip of the appliance or VM host of the device. This rigorous identity management system ensures that only authenticated and authorized devices can participate in secure communication, establishing a strong foundation for zero trust.

- **Exponentially Reduced Management Overhead:** Onclave's architecture significantly reduces administrative overhead compared to traditional solutions. The integrated CA streamlines certificate management, while the "tunnel-in-tunnel" architecture simplifies firewall rules and ACL configuration. Furthermore, the platform's inherent agility minimizes the need for extensive licensing and hardware upgrades, resulting in significant cost savings.

- **Platform and Hardware Agnostic:** The Onclave TrustedPlatform is designed to operate seamlessly across diverse infrastructures. Its overlay approach, utilizing Layer 2 microsegmented tunnels, allows it to function with any underlying network, eliminating the need for costly "forklift" upgrades. The platform's support for physical, virtual, and cloud environments, including hybrid deployments, provides unparalleled flexibility. This hardware agnosticism ensures that organizations can adopt Onclave's solution incrementally, prioritizing critical segments without disrupting existing operations. It also allows for organic High Availability and Disaster Recovery capabilities without extra licensing costs.

Onclave's Unique Layer 2 Tunnel Creation: Achieving True Microsegmentation

Onclave's approach to Layer 2 tunnel creation further distinguishes it from conventional solutions, enabling a level of granularity and security that is difficult to achieve with traditional methods.

- **Zero Trust Tunnel Establishment:** Prior to the establishment of any secure tunnel, a bilateral trust relationship must be formed between the communicating devices. This trust is cryptographically verified using the unique credentials provisioned during the initial device onboarding process, ensuring that only authorized devices can establish secure communication channels.

- **Dynamic Network Refactoring:** Onclave's architecture supports the dynamic reconfiguration of enclaves post-deployment. This capability, termed "dynamic network refactoring," allows for the real-time addition, removal, or quarantining of network segments and devices without disrupting ongoing communication while maintaining zero-trust. This "dynamic network refactoring" capability is facilitated by the foundational zero-trust architecture and is crucial for maintaining ZTA controls in evolving operational environments. Competitors often require significant network re-architecture or downtime to achieve similar reconfiguration, highlighting the agility of Onclave's approach.

- **Layer 2 Operation with "Tunnel-in-Tunnel" Encapsulation:** Onclave operates at Layer 2, enabling true microsegmentation without altering the underlying IP addressing scheme. This Layer 2 operation, distinct from the Layer 3 approach of many competitors, allows for true microsegmentation without altering the underlying IP addressing scheme and obfuscates the IP address from being visible on the network. To enhance security and simplify firewall management, Onclave encapsulates Layer 2 traffic within Layer 3 constructs, creating a "tunnel-in-tunnel" architecture. The "tunnel-in-tunnel" architecture, coupled with single-port firewall management, provides a significant advantage in terms of security and operational simplicity, unlike solutions that rely on complex, multi-port firewall rulesets.

- **Quantum-Resistant Cryptography:** Onclave employs quantum-resistant encryption across both the TLS management tunnels and the embedded symmetric Layer 2 tunnels. Short-lived AES-256 keys or optionally, proprietary Qywit keys are used for Layer 2 encryption, while NIST approved

post-quantum algorithms secure the TLS tunnels. This proactive approach to quantum resistance is unique to Onclave's TrustedPlatform and not uniformly adopted by competitors and positions Onclave as a forward-looking solution in an evolving threat landscape.

- **Cryptographic Agility:** It is worth highlighting the added capability of the platform to incorporate proprietary or adjust cryptographic algorithms based on future needs, is a distinctive characteristic of Onclave. This adaptability sets it apart from competitors, who typically rely on fixed cryptographic implementations, underscoring Onclave's commitment to long-term security resilience.

Comparative Analysis and Conclusion

Collectively, these capabilities—rooted in an internal blockchain with its own Certificate Authority, a unique "tunnel-in-tunnel" architecture, dynamic network refactoring, and a strong emphasis on cryptographic agility including post-quantum algorithm support and enforced through strict zero-trust policies—yield a uniquely robust, adaptable, and future-proof secure communication framework that is not achievable through conventional solutions or those offered by competitors such as CISCO, Fortinet, Palo Alto, and ZSCALER. Onclave's TrustedPlatform offers a paradigm shift in network security. By embracing zero-trust principles and leveraging Onclave's exclusive combination of foundational technologies and innovative Layer 2 tunnel creation techniques, Onclave delivers a level of microsegmentation, agility, and future-proofing that surpasses traditional solutions. The platform's ability to operate seamlessly across diverse infrastructures, reduce administrative overhead, and proactively address emerging threats positions it as a leading solution for organizations seeking to implement a robust and adaptable zero-trust security posture.