AIONCLOUD

Secure Internet Access

SSE Service Ensuring Secure Internet Access in Hybrid Work Environments

Adapting Security Architectures

Enterprises are increasingly adopting Software-as-a-Service (SaaS) and moving critical data and applications to SaaS environments. Since data and applications that need protection no longer reside in corporate data centers, traditional perimeter-based security models are no longer adequate.
Furthermore, the emergence of hybrid work environments has blurred the boundaries of network security and highlighted the limitations of existing security models as company resources are accessed through various networks and devices.
Consequently, today's enterprises require a next-generation security architecture that can effectively address cloud-based work environments and cyber security threats.

New Environments and New Security Structures

The new digital business landscape necessitates a new security strategy. The Security Service Edge (SSE) Cloud-Based Security Service, based on Zero Trust principles, has emerged to simplify complex network architectures, centralize security, and ensure secure internet access for users anytime, anywhere while protecting corporate assets.

SSE(Security Service Edge)?

SSE, a term defined by Gartner, is a new platform-based network architecture that brings together various solutions to securely protect all user traffic heading to the internet, cloud applications, and enterprise applications. SSE integrates multiple security solutions such as SWG, CASB, FWaaS, ATP, RBI, and ZTNA within a single cloud-native framework.

AIONCLOUD SSE - Secure Internet Access

AIONCLOUD Secure Internet Access service tunnels all traffic to the edge closest to the user, applying consistent security policies based on identity and context, regardless of the user's location, device, or target service. It provides continuous and integrated internet security from a single point, irrespective of the user's access location, device, or target service.

Benefits

A Single Service for Multiple Solutions

Operating efficiency is improved by using various security solutions needed by users on a single integrated service. Centralized management and an intuitive console provide visibility into all user traffic.

Enhanced User Experience

Network latency is significantly reduced because security services are provided by tunneling to the global edge closest to the user and device. A complete internet security system is implemented without complex backhauling or VPNs.

Integrated Cyber Threat Intelligence

Extensive data is collected from global edge locations and integrated with our cyber threat intelligence platform to establish a cutting-edge security system that responds quickly and effectively to unknown threats. This allows users to always maintain the most up-to-date security posture.

Zero Trust Security

Through identity, context, and policy-based checks, users and devices are granted the minimum amount of access needed to highly segmented networks.

TCO Reduction

Security operating costs are greatly reduced by subscribing only to necessary security solutions.

Security for Hybrid Work Environments

The Secure Internet Access service manages security policies centrally and provides consistent security policies to all endpoints and users based on identity and context.
This allows users to safely access the web and cloud SaaS applications using various devices, regardless of time and location.

Enhanced Visibility and Control

Presents a security system suitable for cloud-based work environments by providing visibility and control over users, access devices, targets, protocols, and applications.
Real-time monitoring and analysis results of user and application traffic are visually delivered through the console's dashboard and logs.
Security personnel can grasp users' internet usage at a glance and optimize security policies based on this information.

Simplified Security

Enhances operational convenience by providing various security solutions and control functions through a single integrated console.
Security personnel can perform granular access control, data protection, and threat response for web and cloud applications consistently and efficiently. Moreover, as a cloud-based security service, the latest security features can be utilized without separate hardware deployment or license management.

Secure Internet Access Solutions

Secure Web Gateway (SWG)

Protects users accessing the internet from web-based threats, such as Ransomware and zero-day attacks, ensuring a secure browsing experience.

Cloud Access Security Broker (CASB)

Provides visibility and access control for corporate-authorized cloud SaaS applications.

Firewall as a Service (FWaaS)

Service-based network firewall that inspects network traffic and blocks unauthorized traffic according to predefined security rules.

NG Deep Packet Inspection (NG DPI)

Offers visibility and management for network applications and protocols.

ATP (Advanced Threat Prevention)

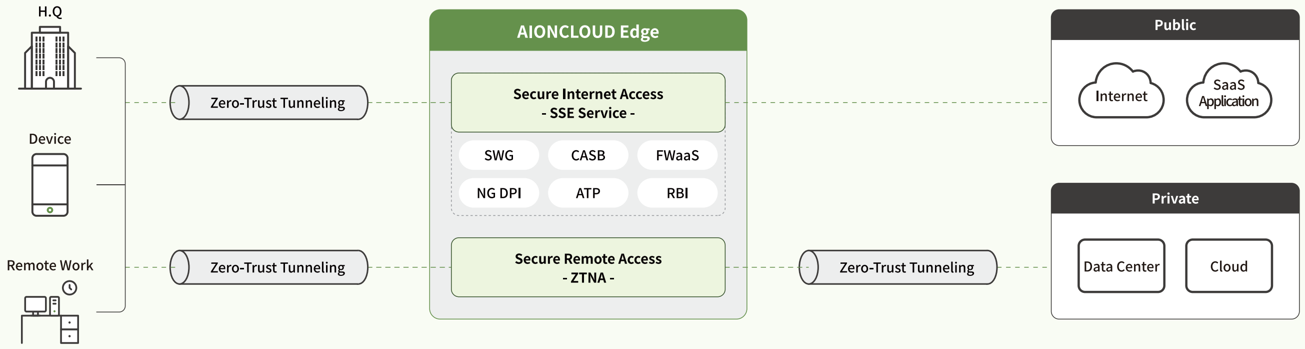
Detects emerging and evolving threats like the latest ransomware and malware to defend the corporate network.

RBI (Remote Browser Isolation)

Executes web browsing sessions on remote servers, shielding user devices from direct exposure to malicious code.

Enabling Secure and Flexible Work in the Digital Era

In the era of digital transformation, a flexible environment that allows work to be performed anytime and anywhere, unrestricted by location or time, is essential. The Secure Internet Access service, powered by AIONCLOUD, is enhanced through integration with the Zero Trust Network Access (ZTNA) and Secure Remote Access services, yielding a more robust security posture. This enables users to connect securely and smoothly to the internet, cloud SaaS applications, and corporate applications.
The Secure Internet Access service is thus a vital for cybersecurity best practices in the digital transformation era, enhancing both security and accessibility to ensure business continuity, regardless of time or place



AIONCLOUD | Secure Internet Access

Datasheet

Copyright © 2024 AIONCLOUD. All rights reserved | www.aioncloud.com

Fore more information, please contact sales@aioncloud.com