HPE Aruba Networking SSE Test Drive

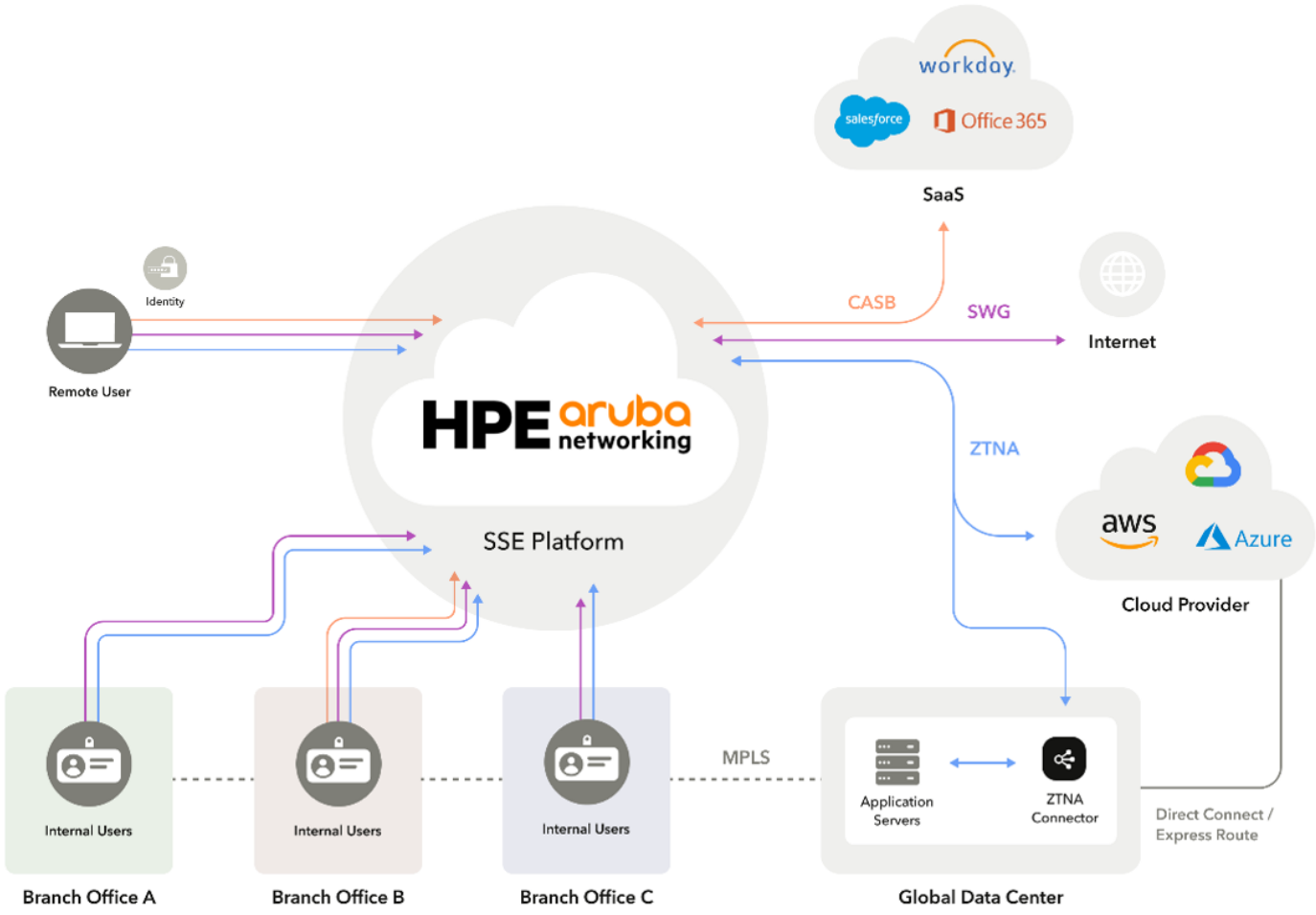
Welcome to the HPE Aruba Networking SSE Test Drive!

This is a fully operational SSE (Security Service Edge) environment to help you familiarize yourself with the HPE Aruba Networking SSE platform. If this is your first time using this product, we've provided a simple guide to help orient you with some of the major features within the product. Please follow along with our guide below and enjoy.

HPE Aruba Networking SSE Architecture

HPE Aruba Networking SSE securely connects any user to any business application or resource, wherever they are in minutes through a single, centrally managed service. The solution provides continuous, application-centric visibility and Zero Trust controls to enable and secure organizations in today's age of digital transformation, work-from-anywhere, and integrated employee/contractor/3rd party business models.

The following illustration shows HPE Aruba Networking SSE, which provides a single unified platform for all application access while decoupling application access from the corporate network. Users irrespective of how they are accessing applications—whether in the office, remote or hybrid receive the same Zero Trust standard and consistent access experience.



ZTNA / VPN Replacement

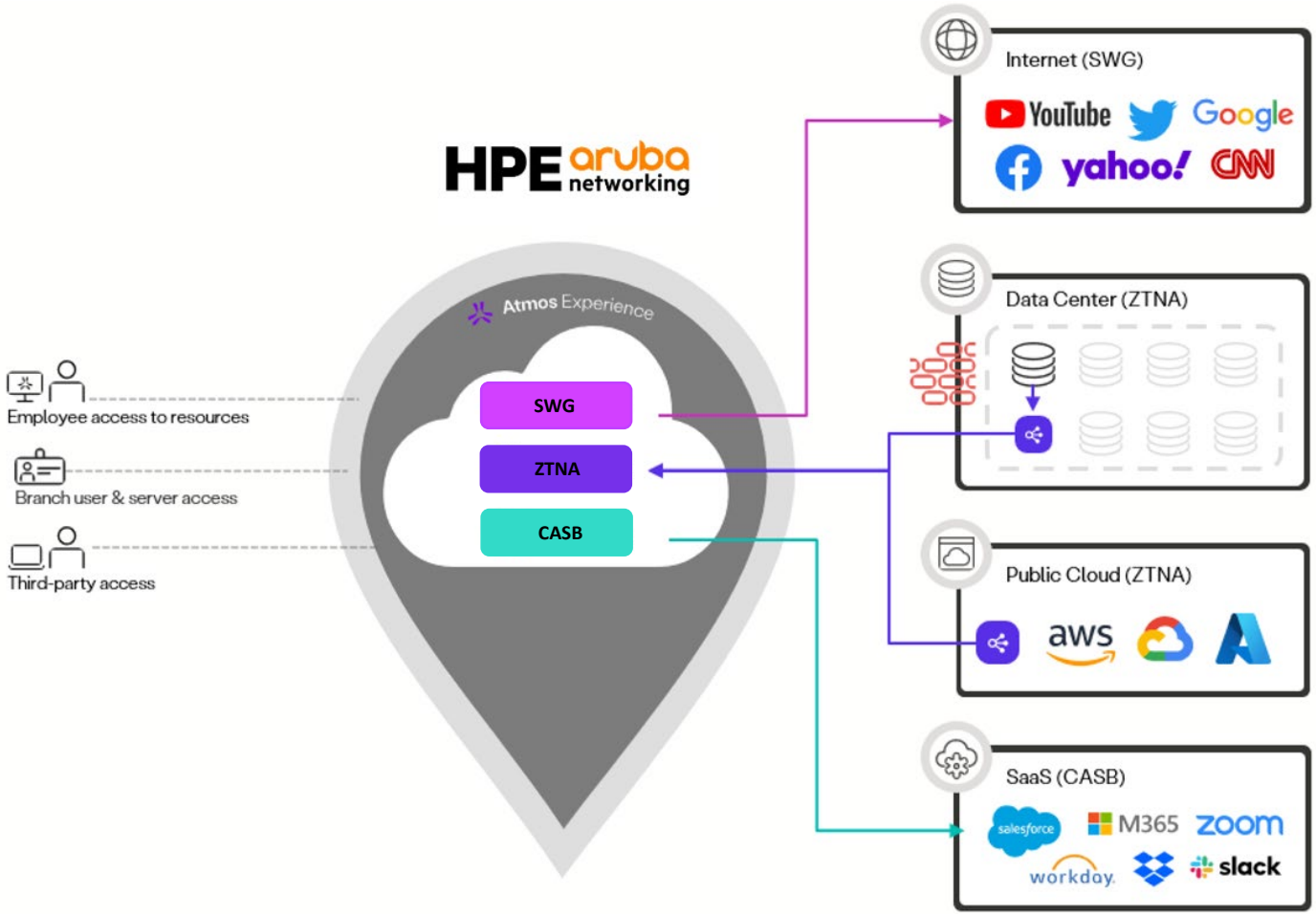
Zero trust network access (ZTNA) is defined as products and services that create an identity- and context-based, logical-access boundary that encompass an enterprise user and an internally hosted application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a collection of named entities. The broker verifies the identity, context, and policy adherence of the specified participants before allowing access, and minimizes lateral movement elsewhere in the network.

ZTNA from HPE Aruba Networking SSE is a VPN replacement solution that secures connectivity as a service. HPE Aruba Networking SSE is a scalable cloud delivered service with over 250 edge locations and Point of presence around the world. The solution identifies and authenticates the user, validates their device posture, and provides connectivity to only the specific applications authorized for the user and/or user-group(s). The solution brokers the connection between the user and the application.

Front-end: User connects to the closest HPE Aruba Networking SSE PoP via agent or agentless access methodology.

Back-end: App connectors (lightweight Linux VM) deployed at locations where applications are hosted connect outbound to HPE Aruba Networking SSE.

Access is always outbound from both the front and the back end. ZTNA is a fundamental shift from IP/network-based access to user and application-level access with least privileges.



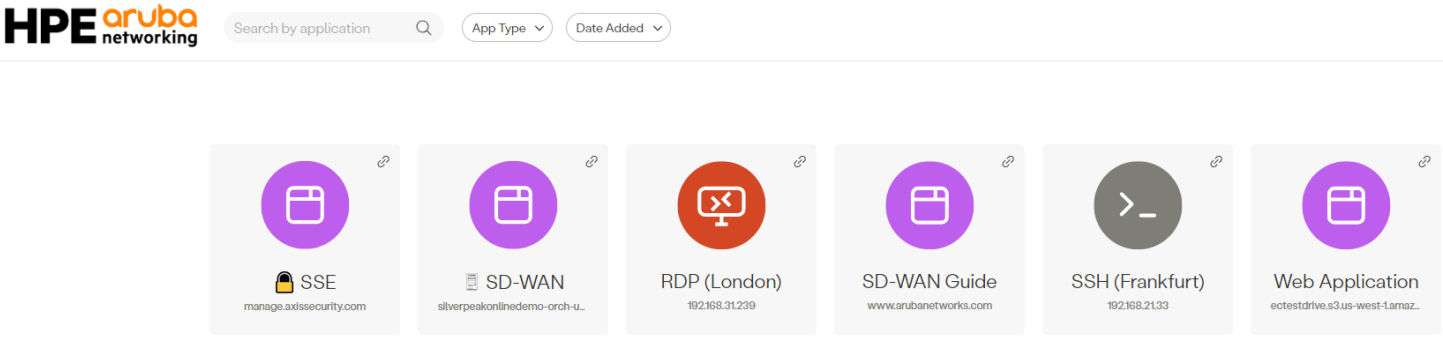
HPE Aruba Networking SSE Application Portal

The application portal provides Agentless Application access to Web, SSH, RDP, Git, and VNC applications.

https://axis-hpetestdrive.axisportal.io/apps

Workspace: hpetestdrive

Upon logging into the demo environment using the provided credentials, the user will be presented with various application tiles. These are the only applications that the user is authorized to access. Applications such as SSH and RDP can be accessed directly via a web socket connection or using a native application installed on the endpoint machine. User identity, authentication, and authorization can be managed using the Axis IDP (local user database) or through SAML/SCIM integration with other well-known providers such as OKTA, and Azure AD etc.



There are six applications available in this demo environment.

- SSE – The HPE Aruba Networking SSE management portal. Read-only access to view the security dashboard, logging, and policy
- SD-WAN – EdgeConnect SD-WAN Orchestrator management console for the test drive environment
- RDP (London) – Remote desktop Windows machine
- SD-WAN guide – Secure link to HPE Aruba Networking test-drive documentation
- SSH (Frankfurt) – SSH access to Ubuntu server in Frankfurt
- Web App – http(s) static website

Note: All the applications are available via both agent and agentless access methods. Due to security and compliance reasons, we are unable to provide login credentials for RDP and SSH.

HPE Aruba Networking SSE Management Console

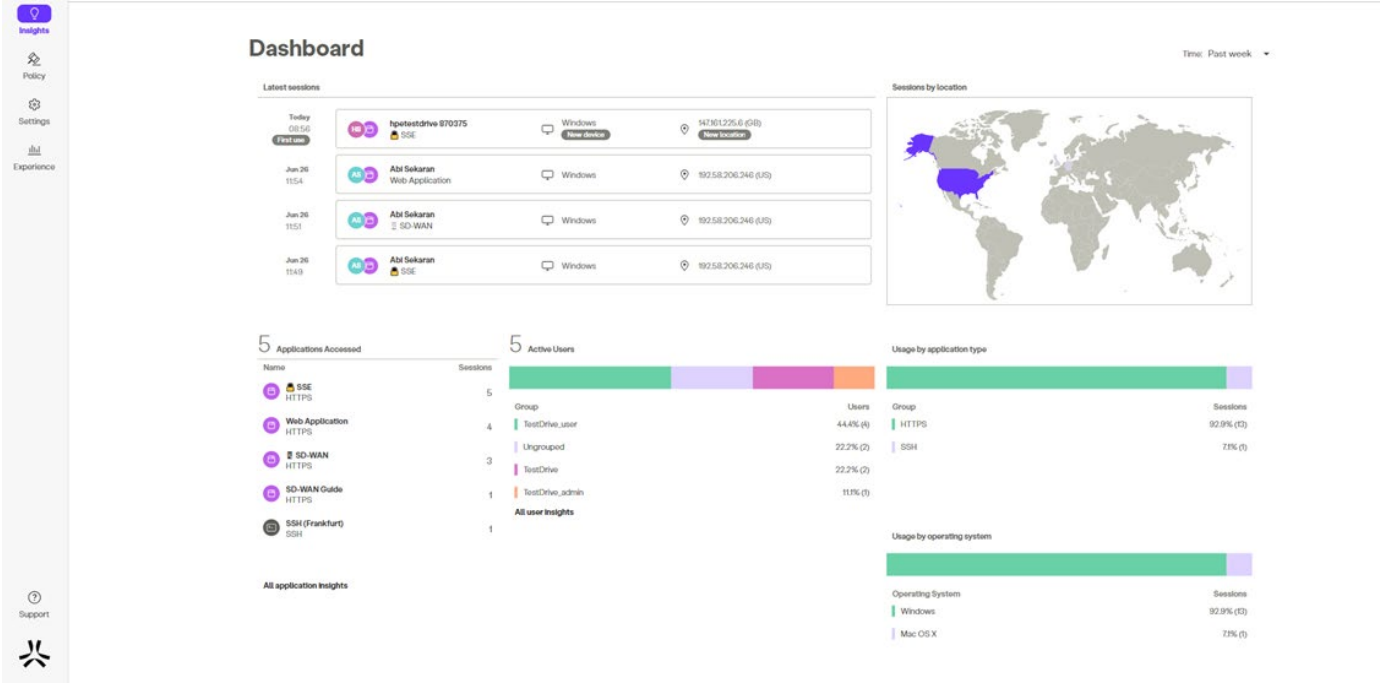
The HPE Aruba Networking SSE management console provides read-only administrator access to visibility, reporting and the policy engine.

https://manage.axissecurity.com

Workspace: hpetestdrive

HPE Aruba Networking SSE Dashboard

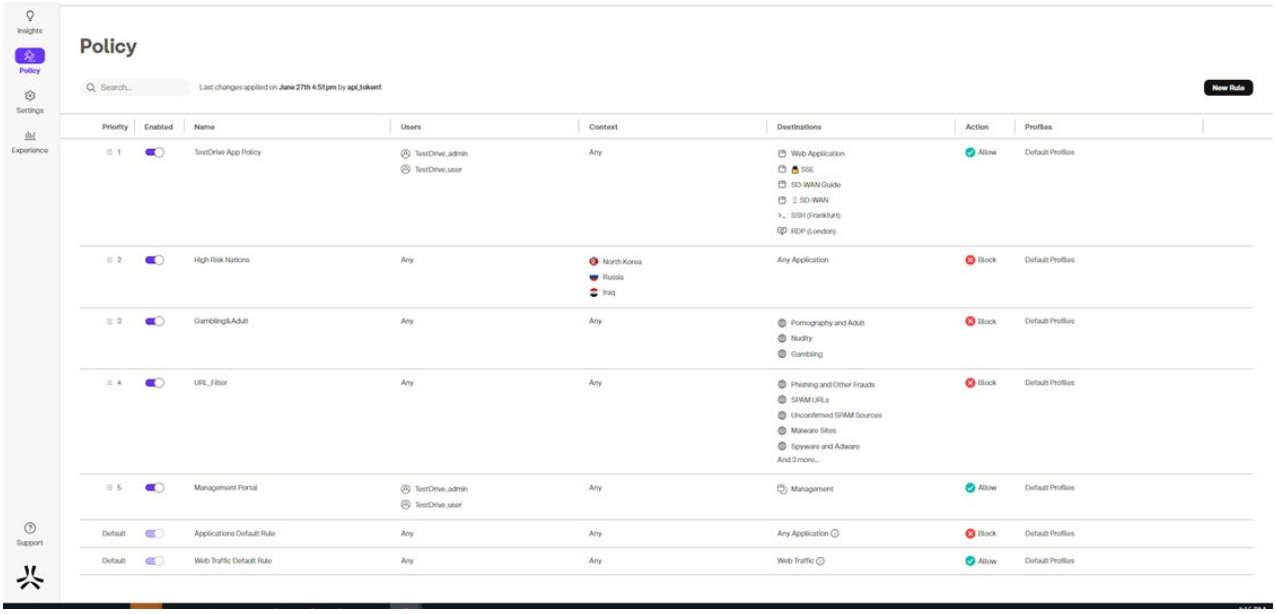
Upon logging into the management console using the credentials received in your registration confirmation email, a detailed snapshot of network and user activity is presented in the dashboard. Applications accessed, active sessions with activity/command log, geographic location, and other telemetry are presented in a graphical format.



HPE Aruba Networking SSE Security Policy

HPE Aruba Networking SSE provides a single pane of glass dashboard to manage corporate security policy including ZTNA, FWaaS, SWG, and CASB. Security rules are processed in a top-down order. Applications and Users can be assigned to groups allowing the security administrator to define consistent security policy for their users irrespective of how they are connecting to the network.

For this demo environment–we have rules created that block traffic destined to High-Risk Nations, Gambling, Adult content and known Malware/Spam websites. All other traffic is permitted by policy and logged. SSL inspection, a key part of FwaaS/SWG functionality can be done at scale for all allowed traffic for complete visibility and control of user web traffic. However, in this demo environment–SSL is not inspected due to the complexity associated with use and management of certificates on end hosts.



Security Log

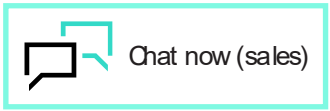
Administrations can view all Internet bound traffic generated by a managed host (with agent installed) or behind an SD-WAN appliance. Consistent security policy is enforced irrespective of where and how the user accesses the Internet.

Relevant Axis Links

Documentation

29 Minutes to Master ZTNA – Webinar recording

Make the right purchase decision.
Contact our presales specialists.



© Copyright 2023 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty.
Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett Packard Enterprise