Versa Identity and Authentication Engine

Introduction

Identity is central to Enterprise Networks. Zero Trust Network Access Framework considers identity as critical context around which network security is defined. Thus, for a network administrator, being able to efficiently authenticate and authorize the users and to get visibility into authentication attempts is critical.

As part of digital transformation initiatives, a number of enterprise services are migrating from on-premises identity providers (e.g., Microsoft Active Directory) to a cloud/SaaS based identity providers (e.g., Azure AD, OKTA, Ping ID etc). This results in added complexity when managing and monitoring the authentication infrastructure.

- Migration to cloud-based identity providers (IdPs): After an enterprise decides to migrate to a SaaS based identity provider, enterprise may have to maintain multiple identity providers for the duration of the migration. The migration effort can last anywhere between few weeks to few months. During this period, network and security infrastructure (Versa Secure SDWAN CPEs and Cloud Gateways) are configured with each of these identity providers.
- Using Cloud based IdPs for remote users: Many enterprises now have a part of the employee base working in hybrid mode: i.e., partly from office and partly remotely. For employees who are remote (either permanent or hybrid), SaaS based IdPs provides a more optimized experience. For office-based employees, on-premises IdPs are optimal. Thus, many enterprise customers are moving to a dual IdP model.
- Different IdPs for Employees, Contractors and Partners: A number of enterprises choose to use different IdPs for employees, contractors and partners in order to provide a clean separation between different class of users.

A common theme across above listed use-cases is the need to leverage multiple IdPs across the entire network and security infrastructure. Even if the configuration is done via a template (i.e., bulk-update), the change needs to be monitored individually during the change event as well as later to ensure that authentications are progressing smoothly. Any breakage needs to be fixed individually.

Such requirements can slow down the network policy upgrades and new deployments. This architecture also increases the risk of misconfiguration denying network access to impacted users or worse allowing full access to the network without authentication. Identity and Authentication Engine aims at minimizing the configuration required on network and security infrastructure (WAN Edge Devices, SD-LAN Switches and Access points, Firewalls and Cloud Gateways) allowing the customers to define policies in a central location without managing at individual edges one by one for each identity service

So far we have talked about the importance of simplifying the IdP configuration in order to simplify the experience of administrator to implement new policies. It is equally important to focus on simplifying the authentication experience for the user. Keeping the interruptions to a minimum and reducing the delay in users accessing the requested resources goes a long way in improving the user experience. To address such needs, Identity and Authentication Engine implements:

- Ability to transfer the user and user group context from IdPs (e.g., Active Director, LDAP Servers, VDI etc) to the network
- Ability to transfer dynamically learned user authentication context across network and security infrastructure (WAN Edge Device, SDLAN switch etc)
- Ability to synchronize databases from multiple IdPs and to normalize identity and authentication information

Thanks to such capabilities, customers of Identity and Authentication Engine will benefit from:

- Improved network and security agility due to simplified configuration in network and security infrastructure
- Improved security posture due to centralized IdP configuration and visibility
- Better user experience due to reduced captive portal screens
- Better scaling solution with centralized points to manage authentication and authorization activities

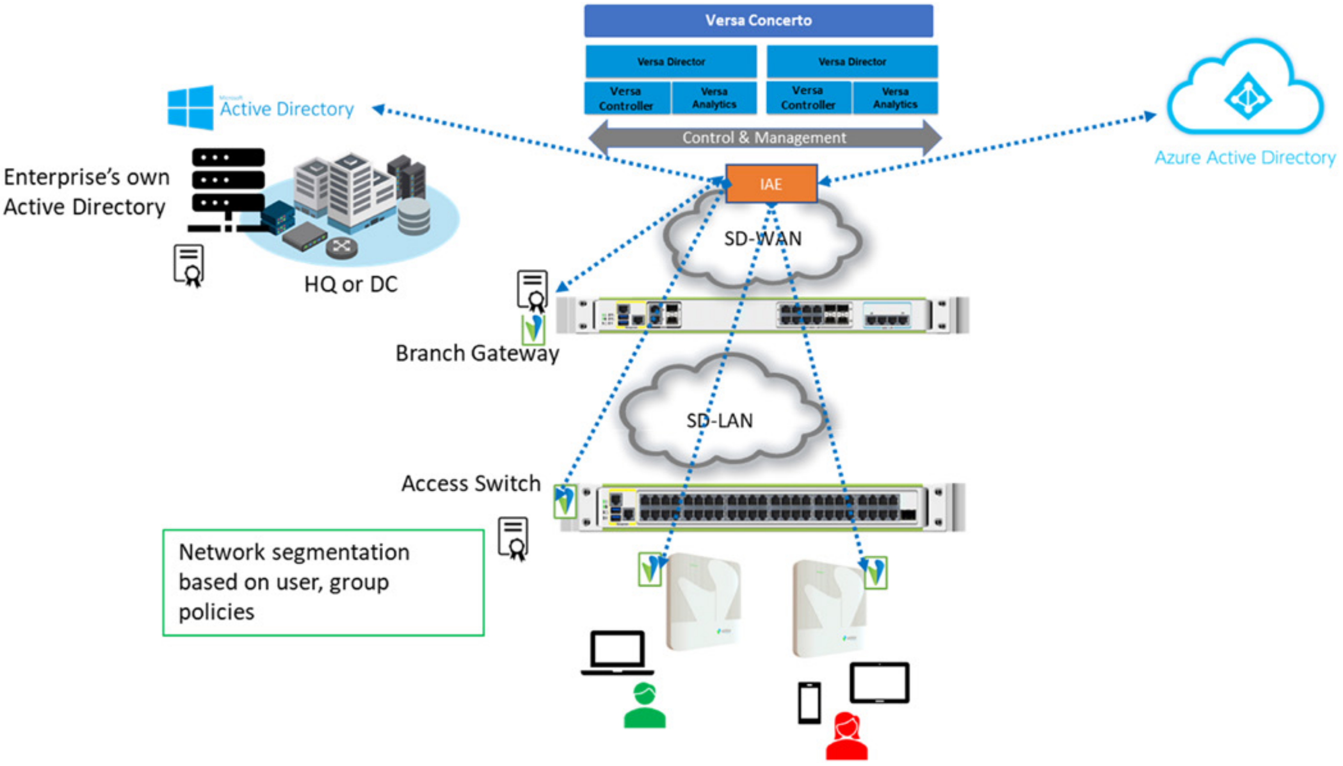
Centralized Identity Provider Configuration

Versa Identity and Authentication Engine provides a centralized identity provider configuration. New identity providers can be configured with automated workflow. The network and security infrastructure is not impacted for every change in the configuration whether for configuration of new IdP, certificate migration or user authentication policies.

Centralized identity configuration simplifies deployments where:

- Gradual Migration is planned from one IdP to another
- Different IdPs are used for different set of users (e.g., M&A, partner access etc)

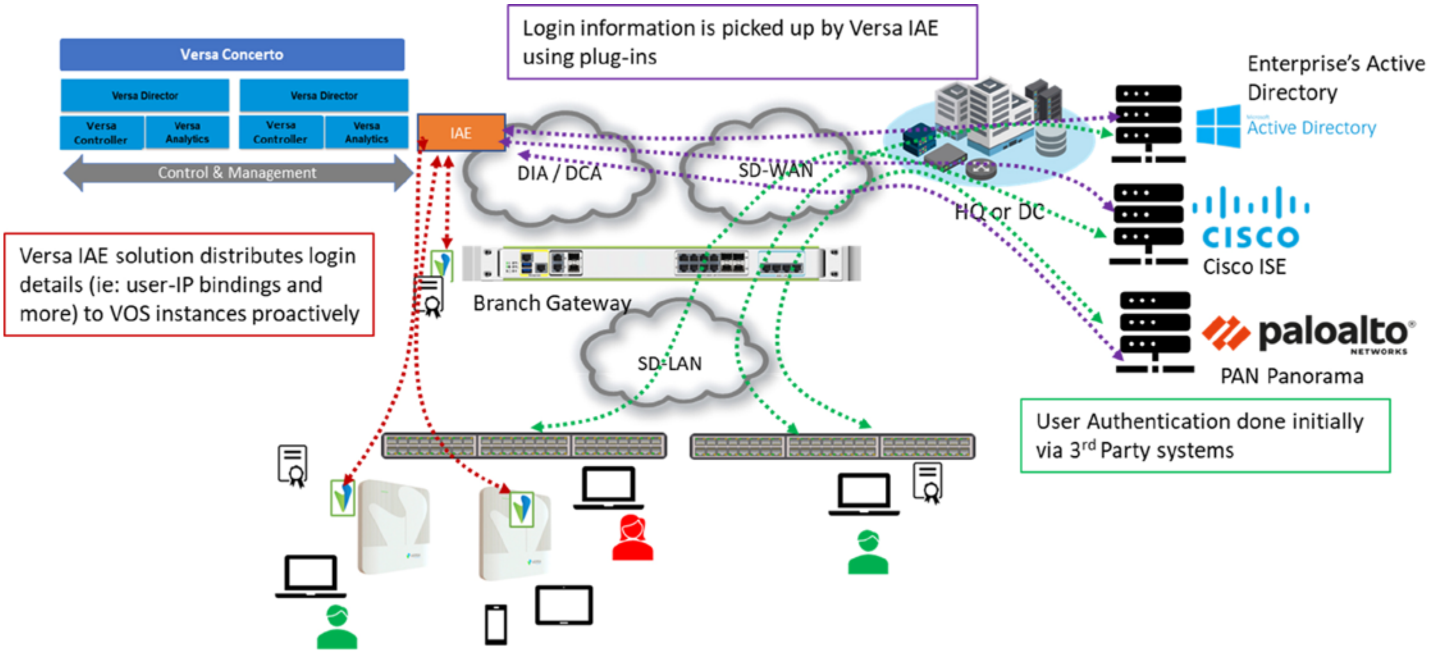
The IAE solution supports all major authentication protocols: LDAP, SAML, RADIUS.



Proactive Authentication

In a modern network and security infrastructure, there are many individual systems which need user context. Efficiently distributing identity information is critical for seamless and secure network access experience for the users.

Versa IAE provides centralized user context distribution. Versa IAE obtains the user authentication context from various identity providers (Active Directory, Azure AD, Cisco ISE, Palo Alto Networks Panorama etc) and distributes the information to Versa WAN Edge, SD-LAN/SD-WLAN devices and Versa Cloud Gateways. The distribution is completely transparent to the users. Appropriate user-based policies can now be applied across the network without the need for users to authenticate at different points across the network.



Login information is picked up by Versa IAE using plug-ins

Versa IAE solution distributes login details (ie: user-IP bindings and more) to VOS instances proactively

User Authentication done initially via 3rd Party systems

Seamless Authentication

This is an extension of Proactive Authentication. When a user is authenticated by any of the Versa network and security infrastructure, the user authentication context is transparently distributed across Versa infrastructure. Appropriate user based policies can be applied across the network without the need for users to authenticate repetitively at different points in the network.

Local Identity Provider

Versa IAE solution offers Identity Provider Service allowing user authentication and authorization on Versa network and security infrastructure. Enterprise user context is configured on the IAE user database. The users can now be authenticated and authorized by the Versa IAE solution. Versa IAE supports all major authentication protocols including: SAML, LDAP and RADIUS.

User Database Synchronization

User identities can be distributed across multiple IdPs in the enterprise network and in the cloud. Versa IAE provides an efficient mechanism to ensure that the user dentity database is synchronized across the entire network. The solution is integrated with all major IdP like Microsoft Active Director, Azure AD, and cloud based SSO providers like OKTA, Ping ID etc.

Features

Identity & Authentication Engine	License
Centralized authentication engine for VOS instances in the field (VMS based)	✓
Centralized Authentication support for Active Directory (user-id Login Events subscription OOB)	✓
Azure AD proxy support and user auth info updates	✓
Centralized Panorama integration support for user auth info updates	✓
Centralized Cisco ISE support for user auth info updates	✓
Centralized HPE Aruba Clearpass support for user auth info updates	✓
Centralized Inline ID Proxy for commonly used ID services	✓
Centralized RADIUS Proxy - primarily to scale 802.1X and to implement consistent policies across VOS instances	✓
Local Authentication Server/Identity Provider	✓
Centralized SAML 2.0 Identity Proxy (centralized) for branches (Inline Auth)	✓
Centralized distribution of user auth events by one VOS to all VOS instances across the network	✓
Terminal Server Agent	✓
SCIM Support	✓

Licensing and Pricing

Versa IAE is made available to our customers for use with appropriate licenses. For more information on licensing and pricing of Versa IAE, please contact your Versa partner or Versa sales representative.