Versa Networks Integration with Third Party SSE Services

This document summarizes how Versa Networks SD-WAN integrates with Secure Services Edge (SSE) services from third party vendors.

Summary

The attack surface for bad actors has significantly increased over the last decade with the movement of applications to cloud service providers and private data centers, adoption of SaaS services, hybrid workforce, and the use of BYOD devices. With so many ways to access content from all types of places and devices, no one can be trusted. Every person is simply trustworthy for the moment. John Does is allowed to access an application or share content based on the user, group, geolocation, and risk rating of the user and device, as well as the risk rating of the application being accessed.

Versa Networks SD-WAN integrates with SSE services from third-party vendors. This integration provides complete flexibility regarding the traffic carried to the SSE Gateways. Versa Networks offers various options to carry traffic to the SSE gateways. In addition, it can ingest security analytics from third-party SSE vendors to provide visibility about applications used by users behind a branch and for security at the branch. Integration requires minimal input from the tenant administrator.

Details

Versa Networks SD-WAN integrates with SSE services from third-party vendors. It requires minimal input from the tenant administrator.

This integration provides complete flexibility regarding the traffic carried to the SSE gateways. Specific latency-sensitive applications can be DIA-ed from the SD-WAN branch node, and other traffic can be sent to an SSE vendor’s security gateways.

Versa Networks provides various options to carry traffic to the SSE gateways. A tenant administrator can use GRE or IPsec tunnels. Versa Networks supports both policy-based and route-based IPsec VPNs. In the case of route-based IPsec VPNs, one can use static routing or E-BGP. In addition, Versa supports TWAMP for active monitoring of this tunnel. Versa Networks also supports proxy chaining for connecting to SASE Gateways.

In addition, it can ingest security analytics from third-party SSE vendors to provide visibility about applications used by users behind a branch and for security at the branch. A tenant administrator can gain visibility on the applications accessed by the users within the branch. Threat intelligence learned from this integration with SSE vendors relating to

bad IP addresses, bad FQDN, user risk score, device risk score, and application risk score is communicated to all Versa SD-WAN nodes. The SD-WAN nodes can enforce security based on this information (bad IP addresses, bad FQDN, user risk score, device risk score, and application risk score) without expending too much CPU resources.

Versa Networks integrates with the SSE vendors for the following reasons.

- Selective and optimal steering of application traffic to the security gateways.
- Gathering security analytics and threat intelligence for both visibility and enforcement.

The current list of SSE vendors with which Versa SD-WAN integrates is given below.

- Crowd Strike
- Microsoft CASB, Microsoft Defender 365, Microsoft Entra
- Netskope SSE
- Palo Alto SSE
- Sentinel One
- Zscaler SSE

Figure 1 below provides information about setting up a connector to Microsoft Defender for cloud applications.

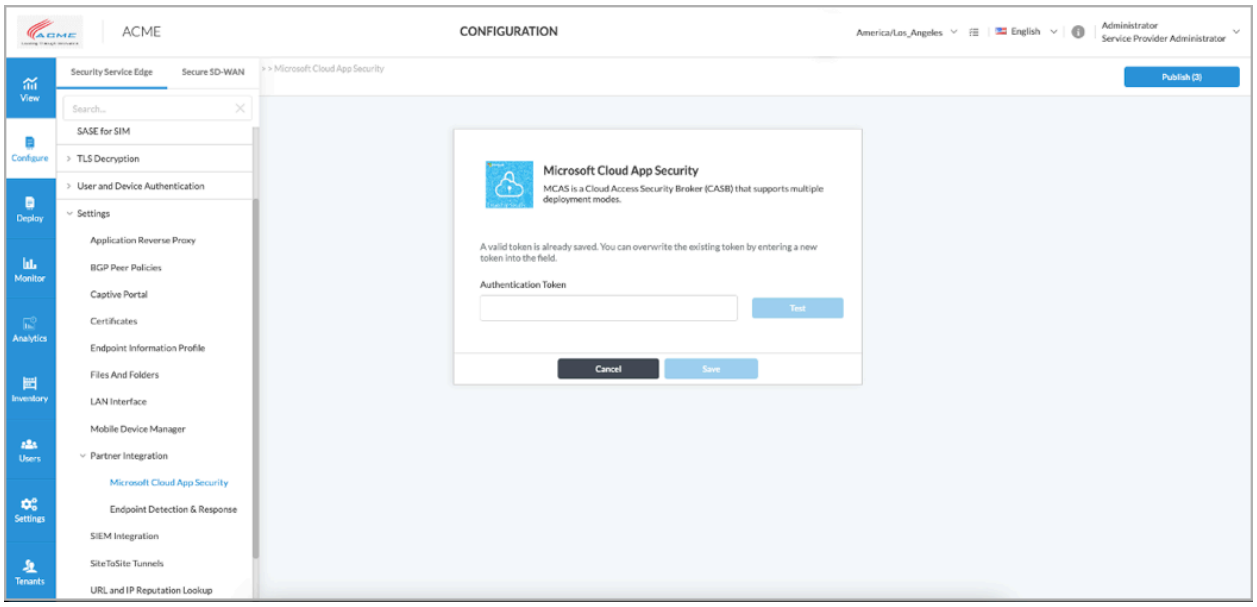

Figure-1.

Figure 2 below provides information about setting up a connector to Microsoft Defender 365 for endpoints.

Updated: Thu, 24 Oct 2024 10:53:57 GMT

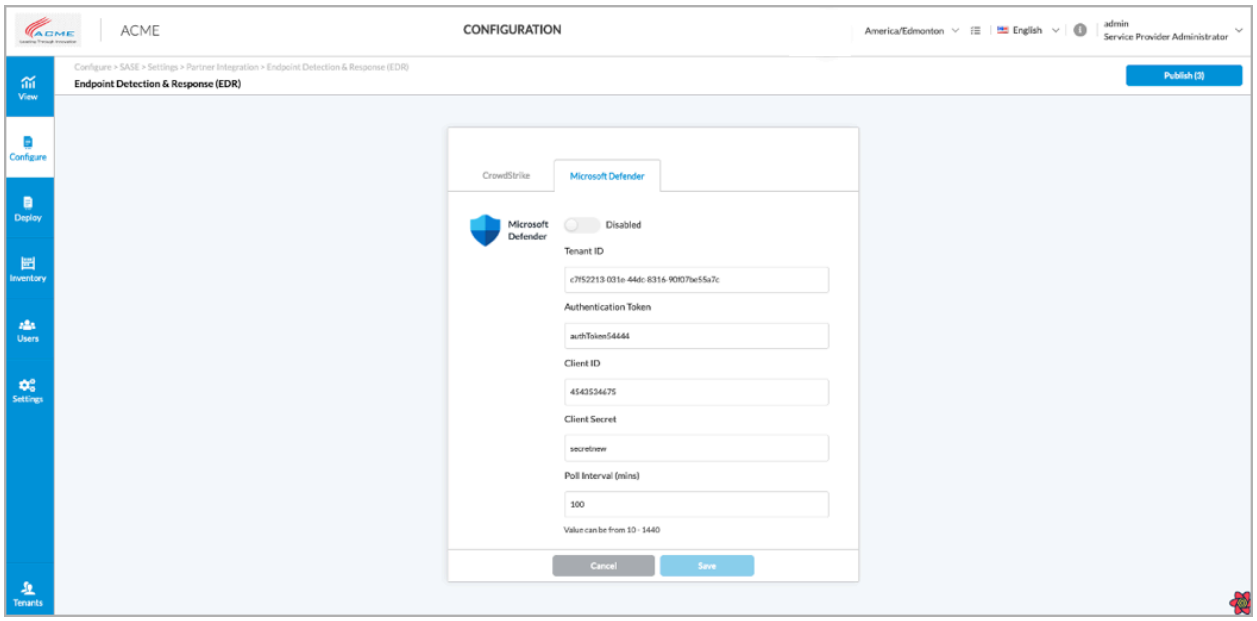

Figure-2.

Figure 3 below provides information about setting up a connector for SSE providers such as Zscaler, Netskope, and others.

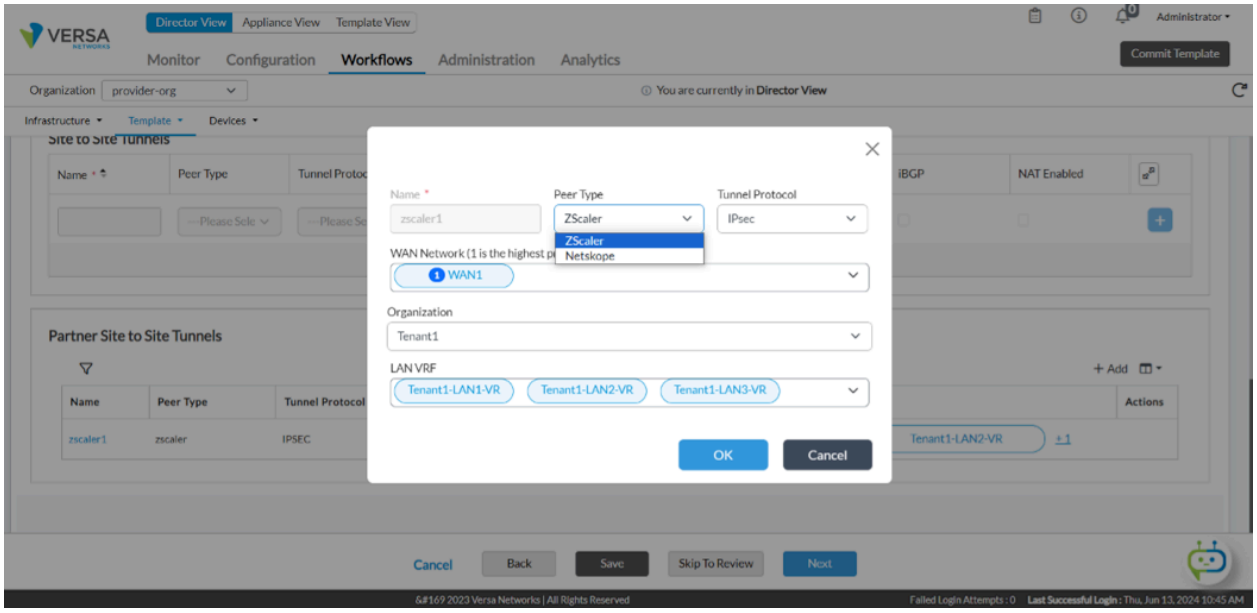

Figure-3.

Figure 4 provides information about setting up a connector to Crowd Strike.

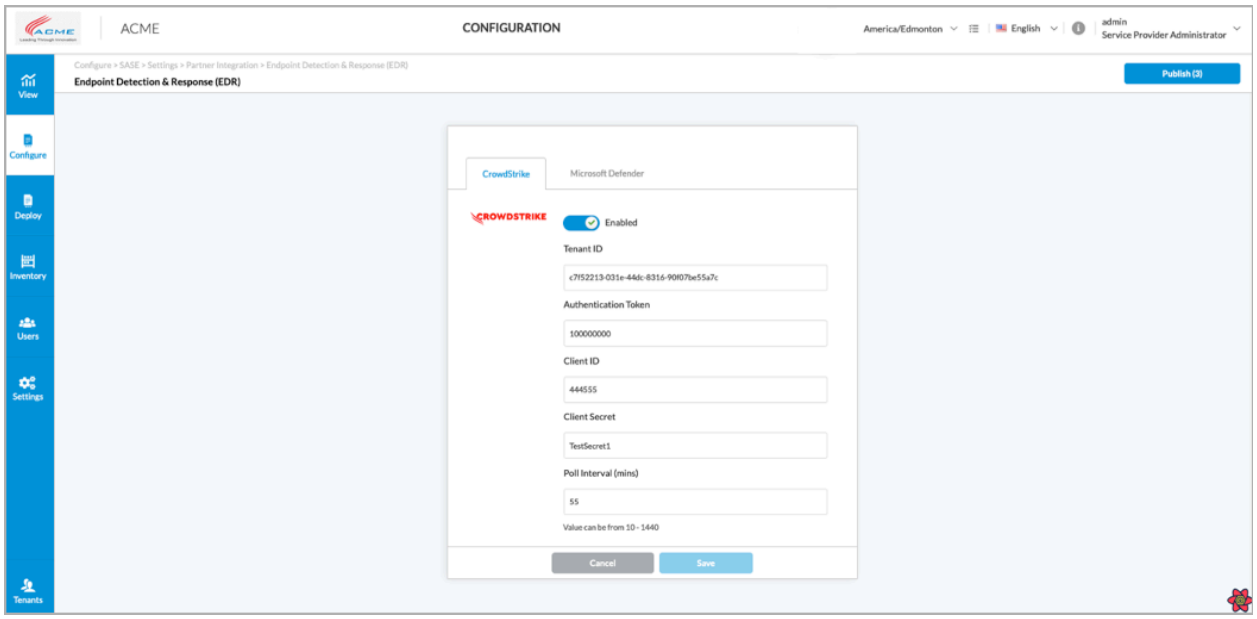

Figure-4.

Updated: Thu, 24 Oct 2024 10:53:57 GMT