NetWitness® Platform

Version 12.5.1

SASE Integration Overview Guide

NETWITNESS

Platform

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by RSA.

It is advised not to deploy third-party repos or perform any change to the underlying NetWitness Operating System that is not part of the supported NetWitness version. Any such change outside of the NetWitness approved image may result in a service or functionality conflict and require a reimage of the NetWitness system to bring NetWitness back to an optimized functional state. In the event a third-party repo is deployed, or other non-supported change is made by the customer without NetWitness approval, the customer takes full responsibility for any system malfunction until the issue can be remediated through troubleshooting efforts or a reimage of the service.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

November, 2024

Contents

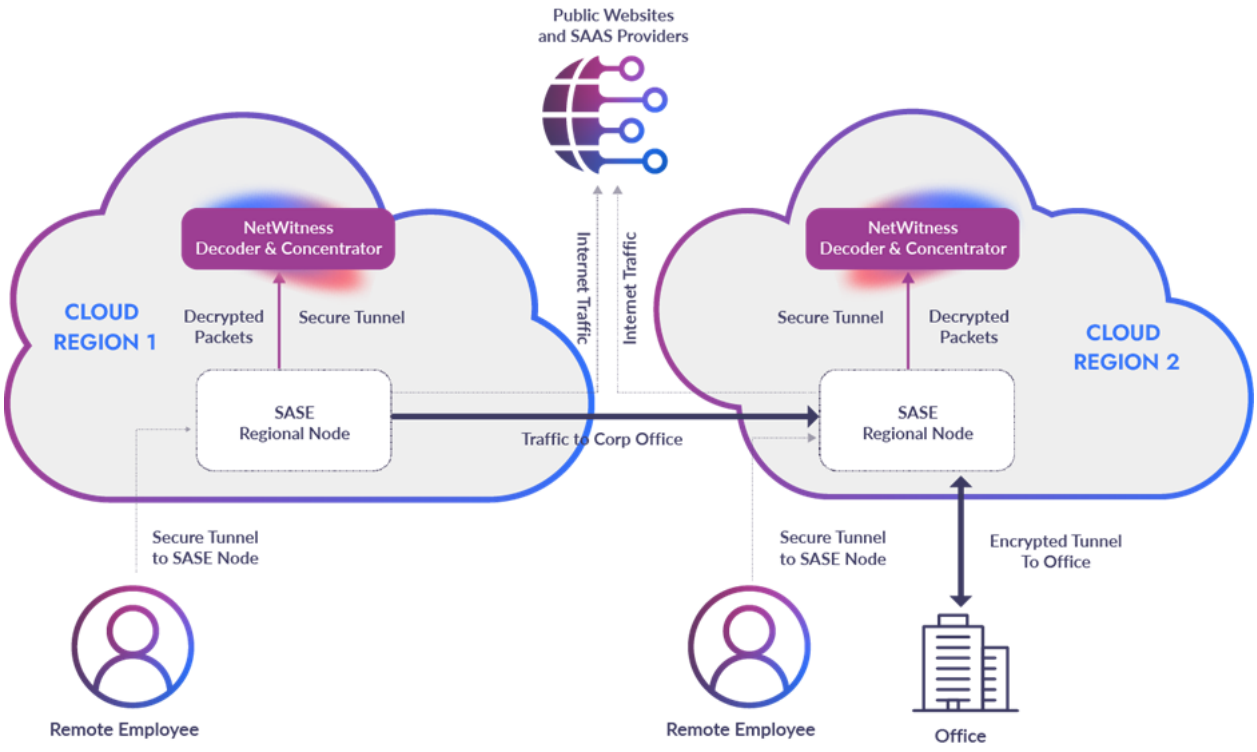
Overview

NetWitness Secure Access Service Edge (SASE) Integrations give organizations complete visibility into encrypted traffic, remote users, and cloud workloads. By partnering with major SASE vendors on technical integrations, NetWitness supports SASE use cases and critical hybrid use cases across on-premises and cloud data. With NetWitness SASE integrations, customers receive the best of both worlds: SASE flexibility and inherent Security Service Edge (SSE) advantages to include packet capture, full threat detection and response visibility.For more information, refer NetWitness SASE Whitepaper.

Organizations have a wide array of SASE specific needs that include various SASE vendors, Cloud vendors, and unique hybrid cloud/on-prem deployments. NetWitness provides a flexible deployment model that supports the many organizational SASE footprint requirements.

To optimize SSE based packet capture and analysis, NetWitness Decoder(s) and Concentrator(s) utilize the same cloud vendor and are co-located in the same region as the SASE VPN Vendor.

NetWitness SASE Architecture



The NetWitness Platform transforms raw data into actionable insights through real-time enrichment with business context and threat intelligence from multiple sources. By applying a standardized taxonomy across all data sources, the NetWitness Platform enhances the detection of both known and unknown threats, boosting organizational resilience and minimizing risks through faster threat detection and response.

NetWitness integration within Secure Access Service Edge (SASE) delivers a cloud-based security solution with comprehensive visibility and protection across on-premises, cloud, and multi-cloud environments.

Unlike competitors with fragmented services, NetWitness Platform offers a unified approach, including the following key capabilities:

- Network Detection and Response (NDR)
- Endpoint Detection and Response (EDR)
- Cloud Access Security Broker (CASB)
- Secure Web Gateway (SWG)
- Zero Trust Network Access (ZTNA)
- Integrated threat intelligence

This holistic approach enables superior threat detection and response management across the entire attack surface, from endpoints to cloud applications, ensuring the platform meets today's evolving security demands. Designed for adaptability, it evolves alongside your infrastructure to address new threats and safeguard your systems into the future.

Deployment Options

There are two types of deployment options:

- NetWitness SASE Automated Deployment
- NetWitness SASE Manual Deployment

Additional NetWitness SASE deployment configurations are available, offering different levels of automation and network packet ingestion rates.

NetWitness SASE Automated Deployment

NetWitness has developed an data-driven automated deployment capability specific for NetWitness SASE based integrations. The NetWitness SASE Automated Deployment is currently only supported on the Google Cloud Provider (GCP) Cloud environment.

This NetWitness deployment capability utilizes a script based approach from an on-prem NetWitness Admin-Server to the customer's specified GCP Project. The NetWitness SASE Deployment capability utilizing a customer provided service account, automates the deployment of NetWitness SASE components such as Decoders/Concentrators instances, and the supporting cloud native infrastructure such as the networks and sub-networks, gateways, firewalls, etc. The deployment additional supports the attachment of configurable attached drive specifications based on ingest rate expectations. Refer ***SASE Node-x (Decoder/Concentrator) - GCP Persistent Disk (PD) Storage Configuration*** Section of the *NetWitness Storage Guide* for information on setting up cloud storage including sizing configurations.

Additionally, the NetWitness SASE Automated Deployment includes a secure overlay network that isolates and encrypts all NetWitness SASE based communication without requiring complicated VPN/Firewall configuration between the customer's on-prem Admin-Server and the NetWitness cloud based assets. For more information on SASE Automated Deployment, refer to SASE Hybrid Cloud Installation Guide. While the NetWitness SASE Deployment capability provides substantial automated configuration support and simplicity, the convenience must be balanced with the customer's desire for granular deployment control into their cloud project.

NetWitness SASE Manual Deployment

This deployment approach will not include the SASE Overlay network, and therefore communication between NetWitness Components will need to be enabled based on the NetWitness services and nodes included in the NetWitness SASE implementation. Refer Network Architecture and Ports for port architecture details. This approach is the most flexible but configuration intensive.

Refer Prepare Virtual or Cloud Storage Section of the *NetWitness Storage Guide* for information on the manual addition and configuration of external storage for the NetWitness nodes. The sizing of the attached storage required for SASE Cloud based Decoders and Concentrators can be derived from the **SASE Node-x (Decoder/Concentrator) - GCP Persistent Disk (PD) Storage Configuration** Section of the *NetWitness Storage Guide*. Although that section is specific to sizing external storage for NetWitness Decoders and Concentrators in the GCP Cloud Environment, the sizing principles are conceptually the same for other Cloud Provider manual deployments of Decoders and Concentrators.

NetWitness SASE Vendor Integration Support

Each NetWitness SASE Vendor integration has specific deployment configuration requirements beyond a baseline SASE deployment and configuration of NetWitness Decoders and Concentrators. The NetWitness SASE deployment is the basis for the SASE Vendor Integration. The deployment, whether using the NetWitness SASE Automated Deployment or the NetWitness SASE Manual Deployment, establishes the environment for SASE based packet capture. There are an unlimited number of possible deployment scenarios based on the three supported Cloud Vendors (AWS, GCP and Azure) and the locations (cloud or on-prem) of the Customer's NetWitness Admin-Server, Decoder(s), Concentrator(s), Broker(s), etc. The optimal deployment includes one or more NetWitness Decoders and one or more Concentrators deployed in the Cloud Vendor of choice for the Customer's specific SASE VPN Provider. The Decoder(s) and Concentrator(s) should be deployed in the same Cloud Region as the VPN Provider's artifacts. The Decoder(s) and Concentrator(s) must be orchestrated by the NetWitness Admin-Server and have the necessary available storage configuration based on the Customer's expected ingest rate, and the communication paths defined in Network Architecture and Ports or have utilized the NetWitness SASE Automated Deployment. Each SASE VPN Vendor Integration may have additional artifact deployment requirements.

Palo Alto Prisma

NetWitness Platform SASE enhances visibility into device and service behavior across on-premises, hybrid, and cloud environments. It streamlines investigations by providing a single interface for quick searches, metadata pivots, and session reconstructions. Analysts can perform forensic analysis on detections and hunt threats using retained raw network data. The platform enriches investigations by correlating network traffic with user activities, offering complete end-to-end insights. Additionally, it optimizes costs through advanced compression, selective data retention, and flexible cloud components.

After deploying the SASE Decoder and Concentrator through the NetWitness SASE Automated Deployment or manually, follow the instructions in Palo Alto SASE Configuration Guide. Go to NetWitness Community and download the *Palo Alto Prisma SASE Configuration Guide*. You can also view the online version of the Palo Alto Prisma SASE Configuration Guide in the NetWitness Community.

Troubleshooting NetWitness SASE Deployment

To view potential issues and solutions at the time of NetWitness SASE Deployment:

- Refer *Troubleshooting NetWitness SASE Deployment* section of the SASE Hybrid Cloud Installation Guide.
- Refer *Troubleshooting NetWitness SASE Deployment* section of the Palo Alto Prisma SASE Configuration Guide.