Work-From-Home with Versa Analytics
Versa WFH Solutions

Versa Work-From-Home solutions include

- Versa Secure SD-WAN with Versa Operating System (VOS™) running on an appliance for Work-from-Home
- Versa Secure Access with client running on a personal end device for Work-From-Home and Work-from-Anywhere

Versa Secure SD-WAN with VOS™ Running on an Appliance

Capabilities

Versa Secure SD-WAN with VOS™ running on an appliance is typically for executives, specialized workers, and employees requiring full VOS and working from home. It gives the following capabilities:

- Optionally use of two or more Internet connections for additional reliability, performance and throughput along with back up connectivity
- Full security functionality at via comprehensive integrated security within VOS™
- Prioritization of business-critical traffic with application segmentation and full Secure SD-WAN functionality
- Link selection based on application, networking, and traffic steering policies (e.g. allow only business critical on LTE link if it is last resort link)
- Privacy of data for family members, co-residents, and shared networks (opaque to visibility part)
- Direct to Internet Access for SaaS Apps for business-critical traffic
- Direct to Internet Access for leisure apps from family members and guests
- OpEx subscription model while still using an appliance and VOS software
- Split billing based on business use vs non-business use

Performance and Experience Monitoring

For Performance and Fault Monitoring, appliances running VOS periodically monitor the health of various overlay paths and applications using active or passive monitoring methods. The metrics include the following:

- Latency
- Jitter
- Loss
- Mean Opinion Score
- Application Rank
- Availability

Metrics help determine Application Performance and Quality of Experience for traffic going through either overlay or local breakout.
Application Performance Monitoring

- SD-WAN solution tracks and reports application performance per path.
- This graph shows real time performance of business-critical application traffic on various traffic paths.

Why is my SaaS application performing badly?

Application rank is computed between 1-100 (1 for best and 100 for worst performing app) using various traffic attributes.
QOE Reports

Demonstrate how SD-WAN helps improve traffic performance

The quality of experience with SDWAN resulting from traffic steering, Forward Error Correction (FEC), replication

Problem Identification and Remediation

Analytics data exported from the remote branch helps in troubleshooting day to day issues with connectivity, traffic experience, interoperability, and misconfiguration. This helps detect intermittent availability issues with site/link, determine if it is an underlay/overlay issue, and trace the traffic using per flow logging/packet capture utilities.

Troubleshooting: Site/link Availability

Is the site or link degraded or down?
Troubleshooting: Alarm Monitoring

- Alarm correlation helps generate insights
- Filtering on alarm fields help isolate the issue

Troubleshooting: Traffic Analysis

Per Service Flow Logging and Analysis
Policy Driven Packet Capture Facilitates Deeper Analysis

Use Cases
Versa Secure SD-WAN with VOS™ running on an appliance at home or a remote worker location provides analytics for all of the use cases below:

- Performance & Fault Monitoring
  - Application Performance
  - Poor VoIP/Video Issues
  - Application Connectivity Issues
  - Control Plane Issues: DDoS Attack, Protocol Storms
  - Rogue Flows
  - Underlay or Overlay Issues
- Usage Monitoring
  - Capacity Management
  - Capacity Planning (QoS)
- Security Monitoring
  - Detect Infections via Viruses and Malwares
  - Local or Network wide Threats
- Troubleshooting
  - Traffic Analysis
  - Availability Tracking
Versa Secure Access with Client

Capabilities
Versa Secure Access with client running on a personal end device is designed for an elastic workforce. It gives the following capabilities:

- Work from *Anywhere* with Secure, Reliable Connectivity
- Assured Experience for Business Applications
- Cloud Managed, Cloud Delivered, SaaS
- Seamless integration with existing IT infra
- Zero Trust Network Access (ZTNA)
  - Micro Segmentation
    - Per Application & Gateway segmentation
    - Isolate applications to specific gateways
    - Segment critical applications/gateways from users who don’t need to access
  - Multi Factor Authentication
    - Integrates MFA to verify user identity
    - OTP – SMS or Email supported
  - Per Application Authorization
    - Granular, per user application control
    - User Authentication with preferred identity mgt system
    - Per user policy controls access to each application
  - Network and User Visibility
    - Real-time and historical visibility
    - User/Application information

Components of Versa Secure Access

- **Versa Secure Access Portal**
  Visibility & Control to Users, Apps and more for Enterprise admin

- **Versa Cloud Gateways (VCG)**
  Cloud deployed, Securely connect to Enterprise network and Cloud/SaaS

- **Any available Internet Access**
  Wired, Wireless, Cellular

- **Versa Secure Access client (VSAC)**
  Windows & MacOS, iOS with automated installation
Performance and Experience Monitoring

For Performance and Fault Monitoring the Versa Secure Access client periodically measures round trip time, loss, and other SLA metrics to the distributed system of Versa Cloud Gateways. These metrics can help derive the QOE for client’s traffic through different service providers and identify if it is a local issue or a network wide issue.

For remote workers’ application traffic, the distributed system of Versa Cloud Gateways perform application performance monitoring and intelligent traffic steering towards the application server. Application performance metrics are exported to analytics. Analytics computes application rank algorithmically using various traffic metrics such as network response time, retransmissions, syn/syn-ack time, syn-ack/ack time etc. seen by the actual traffic. The rank expresses perceived user experience in simple metrics with 1 considered as good performance and 100 as bad performance.

Below table shows how remote access user applications are performing.

The drilldown provides detailed metrics per application/destination.
Problem Identification and Remediation

To troubleshoot a remote user’s connectivity and traffic issues, there are several reports available at a per tenant, gateway, user level as shown below.

Tenant View

In tenant view, analytics shows the summary and historical view of following metrics via the distributed system of Versa Cloud Gateways:

- concurrent users
- successful/failed attempts

User Map

User map shows location of the users active in the specified time range. On clicking on a specific user icon, further details of the user are shown such as WAN IP, ISP, server it is connecting to etc.
Traffic view provides the gateway the users are connected to as shown below.

User View: Tracking User Connectivity Events
Helps determine if there were any failures/flaps in the connections from remote access client.
Authentication failures caused due to invalid username/password from the client, OTP mismatch, cipher mismatch, server tunnel IP address exhaustion etc. can be tracked as follows.

User View: Usage monitoring

Top Remote Access Users Per Tenant Based on Traffic Activity.

Summary of All User’s Traffic Activity.
A drilldown into a specific user provides the user’s traffic activity, applications accessed, events, and logs as follows.

Applications/application categories accessed by user Naveen.

Application performance metrics for applications accessed by user Naveen.
User View: Tracking all logs for a specific user

User events and actions taken for user traffic can be tracked at per traffic flow level. As an example, for user Naveen, all log events can be viewed as follows for a specified time range. Log events here shows IDP event, traffic monitoring events, IPSEC alarms etc.