WHITE PAPER

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 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

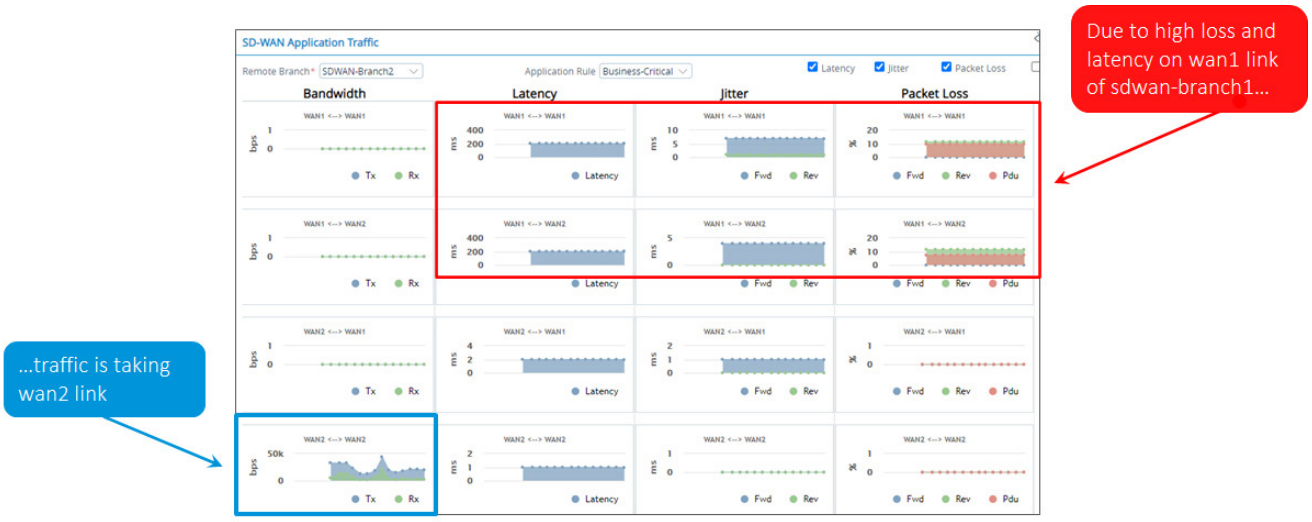
For Performance and Fault Monitoring, appliances running VOS periodically monitor the health of various overlay paths and applications using active or passive monitoring methods. The metrics include the following:

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

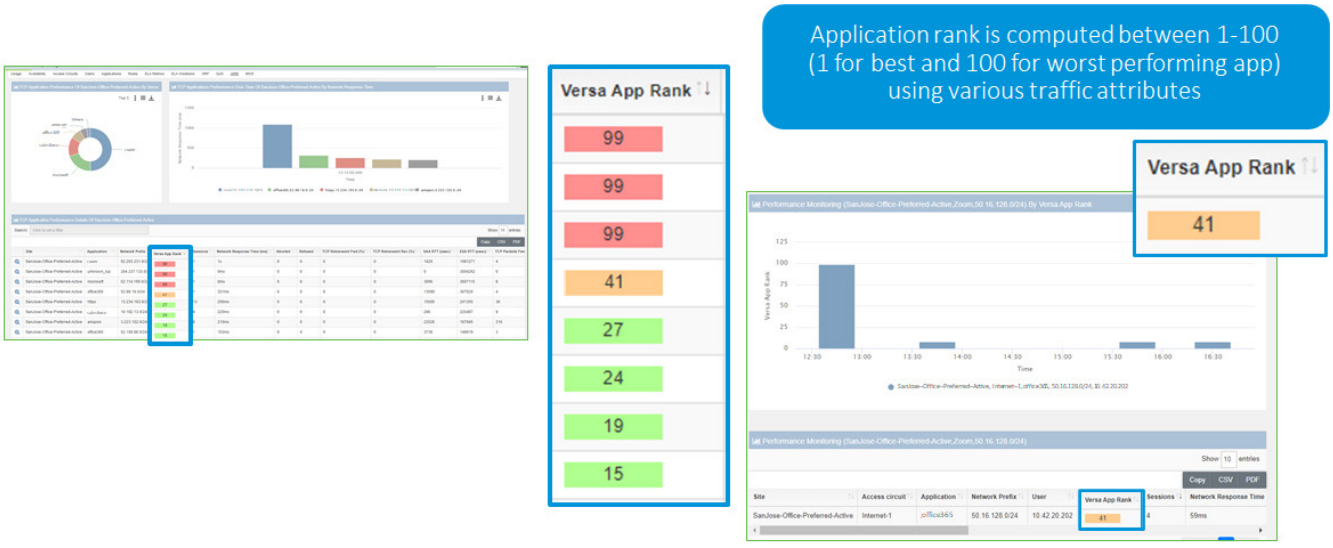
Metrics help determine Application Performance and Quality of Experience for traffic going through either overlay or local breakout.

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?

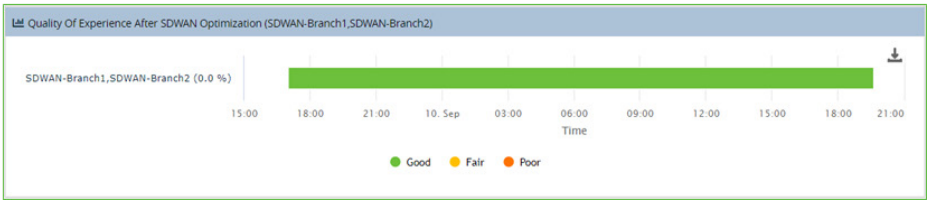


QOE Reports

Demonstrate how SD-WAN helps improve traffic performance

QOE before SDWAN

QOE after SDWAN



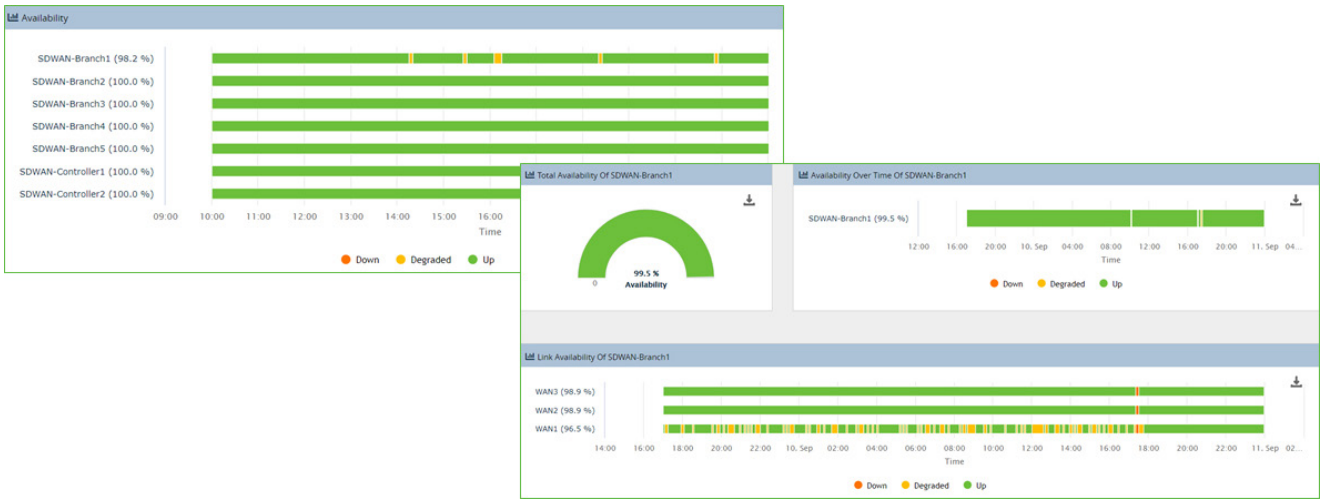
The quality of experience with SDWAN resulting from traffic steering, Forward Error Correction (FEC), replication

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.

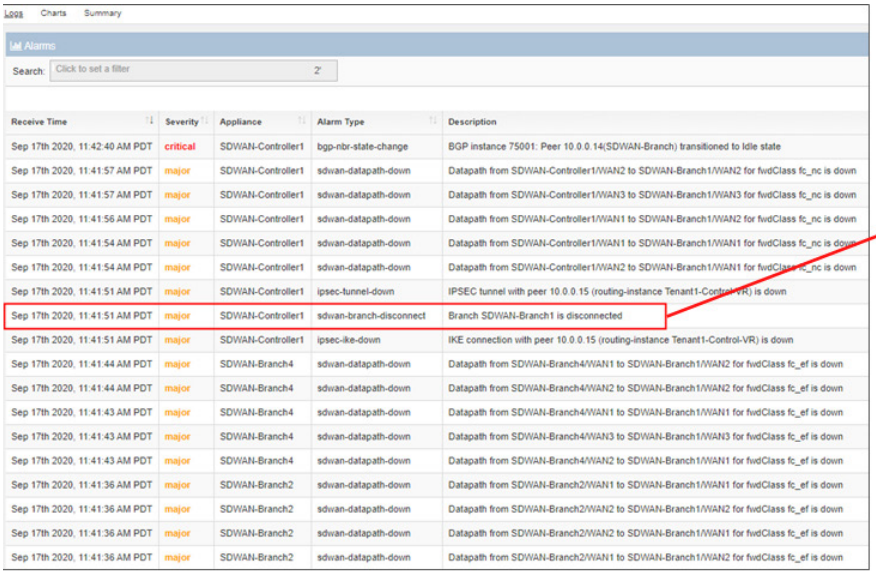
Troubleshooting: Site/link Availability

Is the site or link degraded or down?



Troubleshooting: Alarm Monitoring

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



Logs Charts Summary

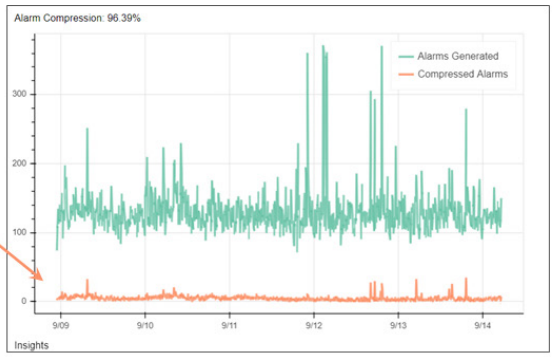
Alarms

Search: Click to set a filter

Receive Time	Severity	Appliance	Alarm Type	Description
Sep 17th 2020, 11:42:40 AM PDT	critical	SDWAN-Controller1	bgp-nbr-state-change	BGP instance 75001: Peer 10.0.0.14(SDWAN-Branch) transitioned to Idle state
Sep 17th 2020, 11:41:57 AM PDT	major	SDWAN-Controller1	sdwan-datapath-down	Datapath from SDWAN-Controller1/WAN2 to SDWAN-Branch1/WAN2 for fwdClass fc_nc is down
Sep 17th 2020, 11:41:57 AM PDT	major	SDWAN-Controller1	sdwan-datapath-down	Datapath from SDWAN-Controller1/WAN3 to SDWAN-Branch1/WAN3 for fwdClass fc_nc is down
Sep 17th 2020, 11:41:56 AM PDT	major	SDWAN-Controller1	sdwan-datapath-down	Datapath from SDWAN-Controller1/WAN1 to SDWAN-Branch1/WAN2 for fwdClass fc_nc is down
Sep 17th 2020, 11:41:54 AM PDT	major	SDWAN-Controller1	sdwan-datapath-down	Datapath from SDWAN-Controller1/WAN1 to SDWAN-Branch1/WAN1 for fwdClass fc_nc is down
Sep 17th 2020, 11:41:54 AM PDT	major	SDWAN-Controller1	sdwan-datapath-down	Datapath from SDWAN-Controller1/WAN2 to SDWAN-Branch1/WAN1 for fwdClass fc_nc is down
Sep 17th 2020, 11:41:51 AM PDT	major	SDWAN-Controller1	ipsec-tunnel-down	IPSEC tunnel with peer 10.0.0.15 (routing-instance Tenant1-Control-VR) is down
Sep 17th 2020, 11:41:51 AM PDT	major	SDWAN-Controller1	sdwan-branch-disconnect	Branch SDWAN-Branch1 is disconnected
Sep 17th 2020, 11:41:51 AM PDT	major	SDWAN-Controller1	ipsec-ike-down	IKE connection with peer 10.0.0.15 (routing-instance Tenant1-Control-VR) is down
Sep 17th 2020, 11:41:44 AM PDT	major	SDWAN-Branch4	sdwan-datapath-down	Datapath from SDWAN-Branch4/WAN1 to SDWAN-Branch1/WAN2 for fwdClass fc_ef is down
Sep 17th 2020, 11:41:44 AM PDT	major	SDWAN-Branch4	sdwan-datapath-down	Datapath from SDWAN-Branch4/WAN2 to SDWAN-Branch1/WAN2 for fwdClass fc_ef is down
Sep 17th 2020, 11:41:43 AM PDT	major	SDWAN-Branch4	sdwan-datapath-down	Datapath from SDWAN-Branch4/WAN1 to SDWAN-Branch1/WAN1 for fwdClass fc_ef is down
Sep 17th 2020, 11:41:43 AM PDT	major	SDWAN-Branch4	sdwan-datapath-down	Datapath from SDWAN-Branch4/WAN3 to SDWAN-Branch1/WAN3 for fwdClass fc_ef is down
Sep 17th 2020, 11:41:43 AM PDT	major	SDWAN-Branch4	sdwan-datapath-down	Datapath from SDWAN-Branch4/WAN2 to SDWAN-Branch1/WAN1 for fwdClass fc_ef is down
Sep 17th 2020, 11:41:36 AM PDT	major	SDWAN-Branch2	sdwan-datapath-down	Datapath from SDWAN-Branch2/WAN1 to SDWAN-Branch1/WAN1 for fwdClass fc_ef is down
Sep 17th 2020, 11:41:36 AM PDT	major	SDWAN-Branch2	sdwan-datapath-down	Datapath from SDWAN-Branch2/WAN2 to SDWAN-Branch1/WAN2 for fwdClass fc_ef is down
Sep 17th 2020, 11:41:36 AM PDT	major	SDWAN-Branch2	sdwan-datapath-down	Datapath from SDWAN-Branch2/WAN2 to SDWAN-Branch1/WAN1 for fwdClass fc_ef is down
Sep 17th 2020, 11:41:36 AM PDT	major	SDWAN-Branch2	sdwan-datapath-down	Datapath from SDWAN-Branch2/WAN1 to SDWAN-Branch1/WAN2 for fwdClass fc_ef is down

One branch going down results in many alarms

- Alarm compression provides high level insights
- Highlights independent alarms and reduces noise from dependent alarms



Troubleshooting: Traffic Analysis

Per Service Flow Logging and Analysis

SDWAN Traffic Log (All)

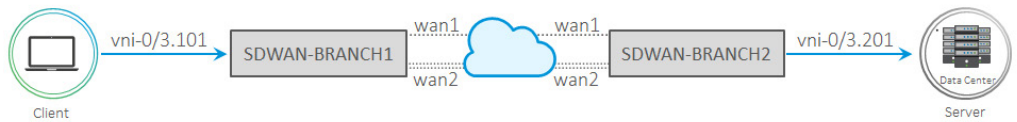
Show Domain Names

Search: (app:"linkedin"),(port:"46179")

? Show 10 entries

Copy CSV PDF

Receive Time	Appliance	Source Address	Destination Address	Source Port	Destination Port	Protocol	Application	Rule	Local Site	Forward Egress Site	Forward Egress Path	Reverse Ingress Site	Reverse Ingress Path	Forward Ingress Sit
Sep 21st 2020, 3:56:57 AM PDT	SDWAN-Branch1	172.16.11.110	172.16.21.10	46179	80	tcp	linkedin	APM-Rule	SDWAN-Branch1	SDWAN-Branch2	WAN3:WAN3	SDWAN-Branch2	WAN3:WAN3	
Sep 21st 2020, 3:56:52 AM PDT	SDWAN-Branch2	172.16.11.110	172.16.21.10	46179	80	tcp	linkedin	APM-Rule	SDWAN-Branch2		vni-0/3.201		vni-0/3.201	SDWAN-Branch1
Sep 21st 2020, 2:44:46 AM PDT	SDWAN-Branch2	172.16.11.108	172.16.21.10	46179	80	tcp	linkedin	APM-Rule	SDWAN-Branch2		vni-0/3.201		vni-0/3.201	SDWAN-Branch1
Sep 21st 2020, 2:44:36 AM PDT	SDWAN-Branch1	172.16.11.108	172.16.21.10	46179	80	tcp	linkedin	APM-Rule	SDWAN-Branch1	SDWAN-Branch2	WAN1:WAN1	SDWAN-Branch2	WAN1:WAN1	

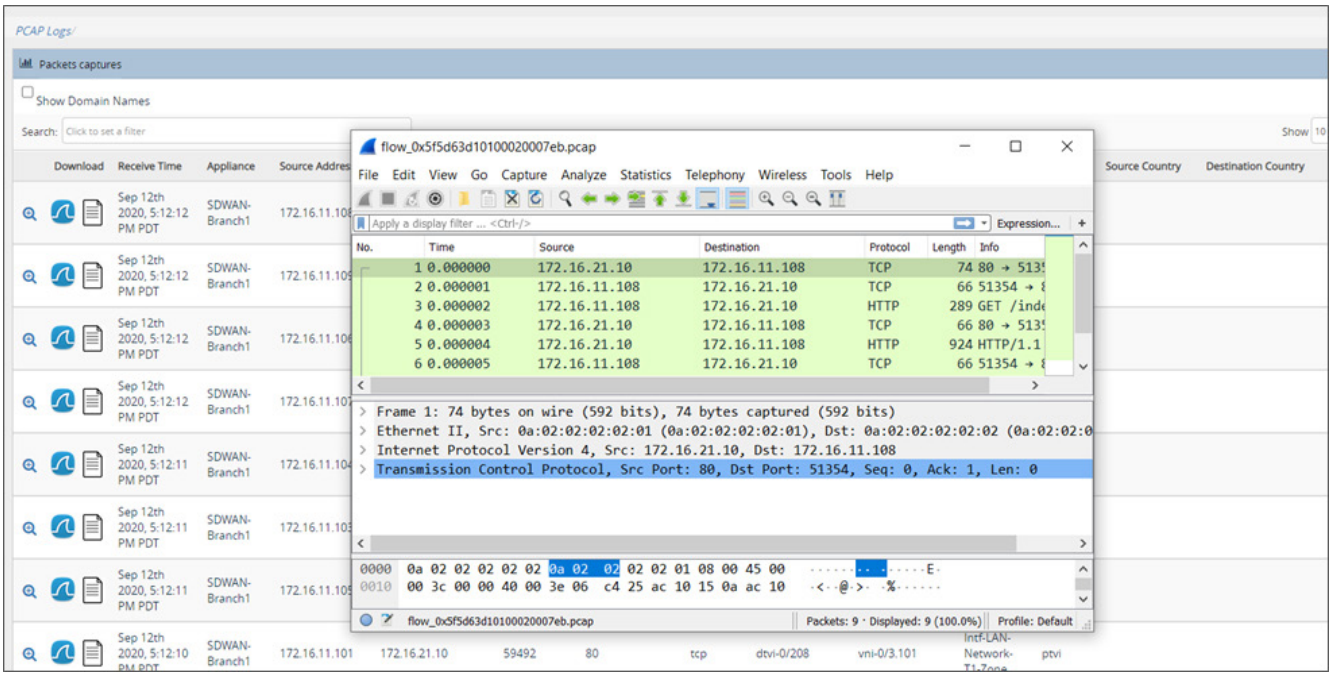


Client
172.16.11.108

Server
172.16.21.10

Client 172.16.11.108 accessing linkedin application on server 172.16.21.10

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

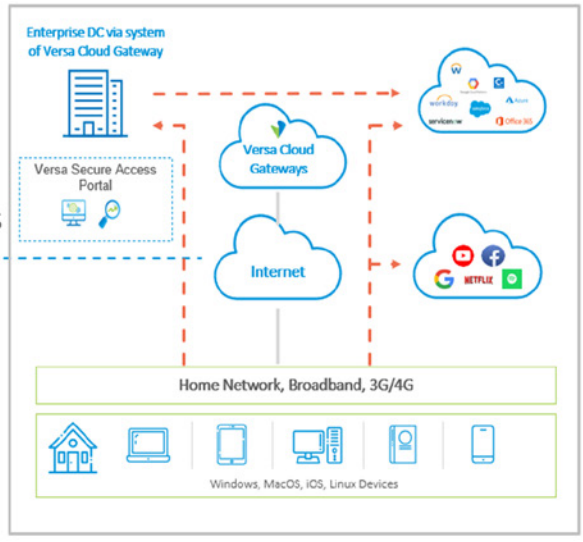
Components of Versa Secure Access

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

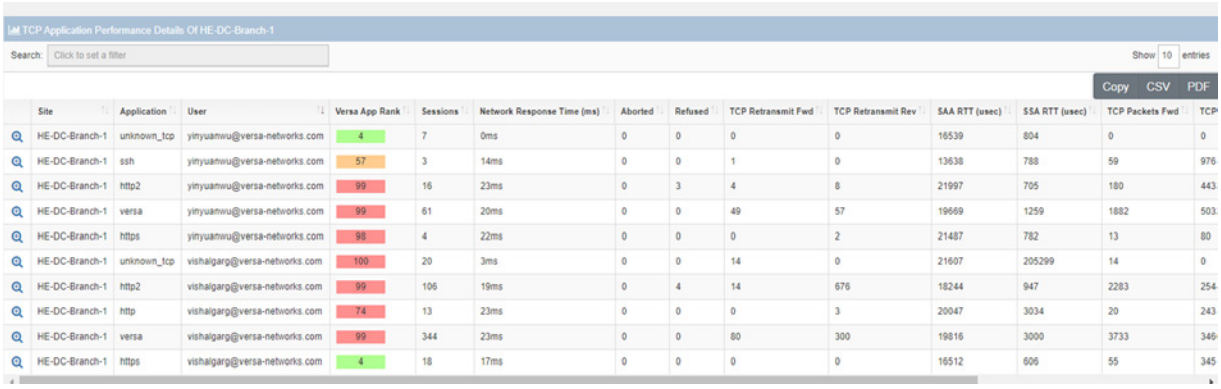


Performance and Experience Monitoring

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.

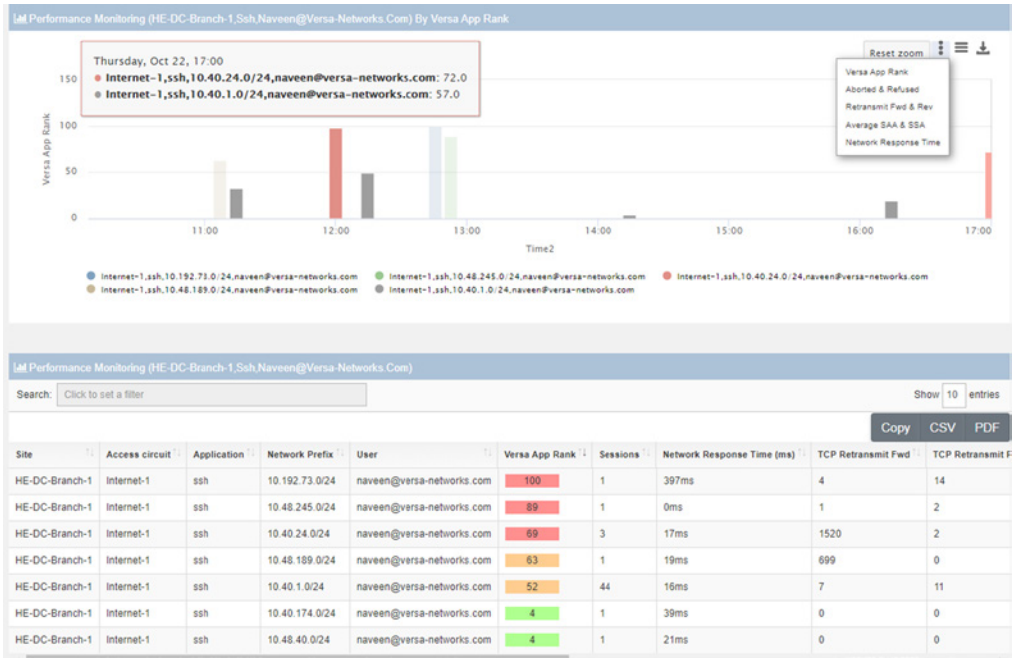
For remote workers' application traffic, the distributed system of Versa Cloud Gateways perform application performance monitoring and intelligent traffic steering towards the application server. Application performance metrics are exported to analytics. Analytics computes application rank algorithmically 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.



Site	Application	User	Versa App Rank	Sessions	Network Response Time (ms)	Aborted	Refused	TCP Retransmit Fwd	TCP Retransmit Rev	SAA RTT (usec)	SSA RTT (usec)	TCP Packets Fwd	TCP
HE-DC-Branch-1	unknown_tcp	yinyuanwu@versa-networks.com	4	7	0ms	0	0	0	0	16539	804	0	0
HE-DC-Branch-1	ssh	yinyuanwu@versa-networks.com	57	3	14ms	0	0	1	0	13638	788	59	976
HE-DC-Branch-1	http2	yinyuanwu@versa-networks.com	99	16	23ms	0	3	4	8	21997	705	180	443
HE-DC-Branch-1	versa	yinyuanwu@versa-networks.com	99	61	20ms	0	0	49	57	19669	1259	1882	503
HE-DC-Branch-1	https	yinyuanwu@versa-networks.com	98	4	22ms	0	0	0	2	21487	782	13	80
HE-DC-Branch-1	unknown_tcp	vishalgarg@versa-networks.com	100	20	3ms	0	0	14	0	21607	205299	14	0
HE-DC-Branch-1	http2	vishalgarg@versa-networks.com	99	106	19ms	0	4	14	676	18244	947	2283	254
HE-DC-Branch-1	http	vishalgarg@versa-networks.com	74	13	23ms	0	0	0	3	20047	3034	20	243
HE-DC-Branch-1	versa	vishalgarg@versa-networks.com	99	344	23ms	0	0	80	300	19816	3000	3733	346
HE-DC-Branch-1	https	vishalgarg@versa-networks.com	4	18	17ms	0	0	0	0	16512	606	55	345

The drilldown provides detailed metrics per application/destination.



Site	Access circuit	Application	Network Prefix	User	Versa App Rank	Sessions	Network Response Time (ms)	TCP Retransmit Fwd	TCP Retransmit F
HE-DC-Branch-1	Internet-1	ssh	10.192.73.0/24	naveen@versa-networks.com	100	1	397ms	4	14
HE-DC-Branch-1	Internet-1	ssh	10.48.245.0/24	naveen@versa-networks.com	89	1	0ms	1	2
HE-DC-Branch-1	Internet-1	ssh	10.40.24.0/24	naveen@versa-networks.com	69	3	17ms	1520	2
HE-DC-Branch-1	Internet-1	ssh	10.48.189.0/24	naveen@versa-networks.com	63	1	19ms	699	0
HE-DC-Branch-1	Internet-1	ssh	10.40.1.0/24	naveen@versa-networks.com	52	44	16ms	7	11
HE-DC-Branch-1	Internet-1	ssh	10.40.174.0/24	naveen@versa-networks.com	4	1	39ms	0	0
HE-DC-Branch-1	Internet-1	ssh	10.48.40.0/24	naveen@versa-networks.com	4	1	21ms	0	0

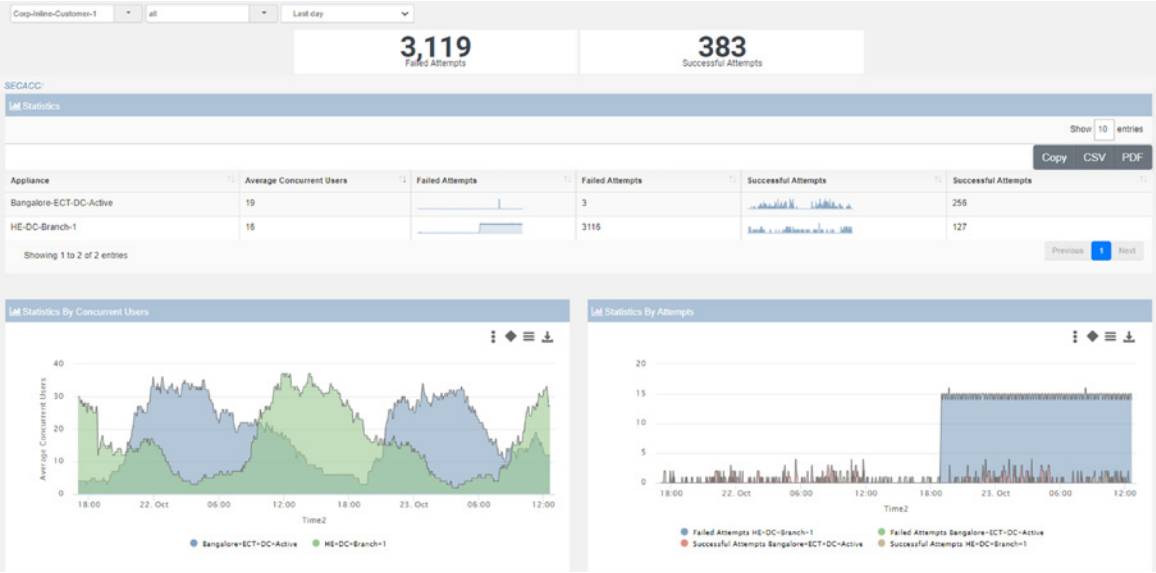
Problem Identification and Remediation

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

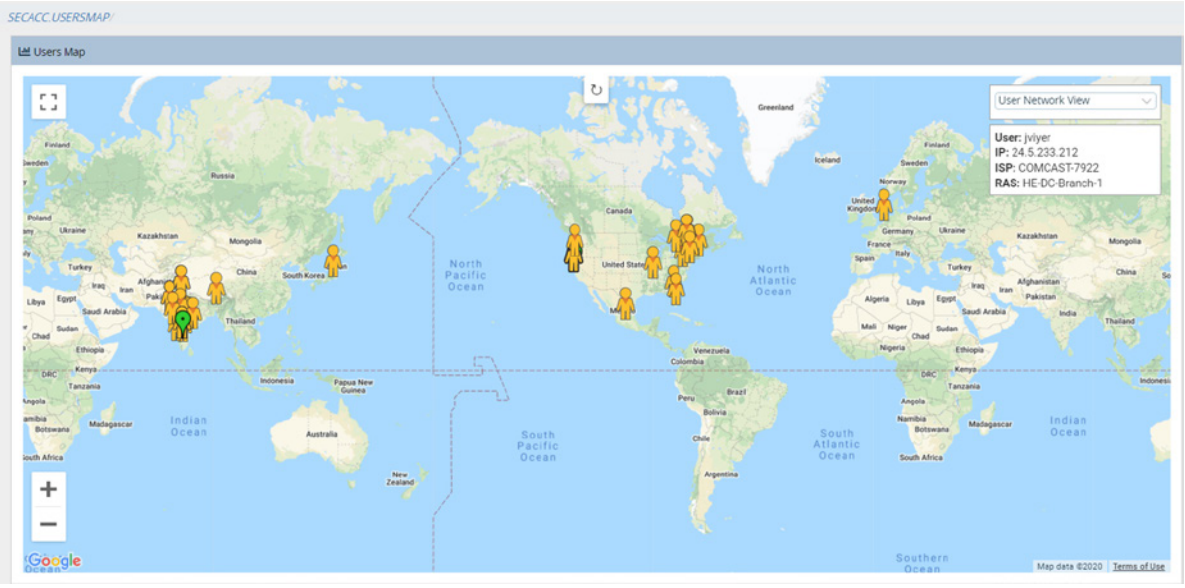
In tenant view, analytics shows the summary and historical view of following metrics via the distributed system of Versa Cloud Gateways:

- concurrent users
- successful/failed attempts

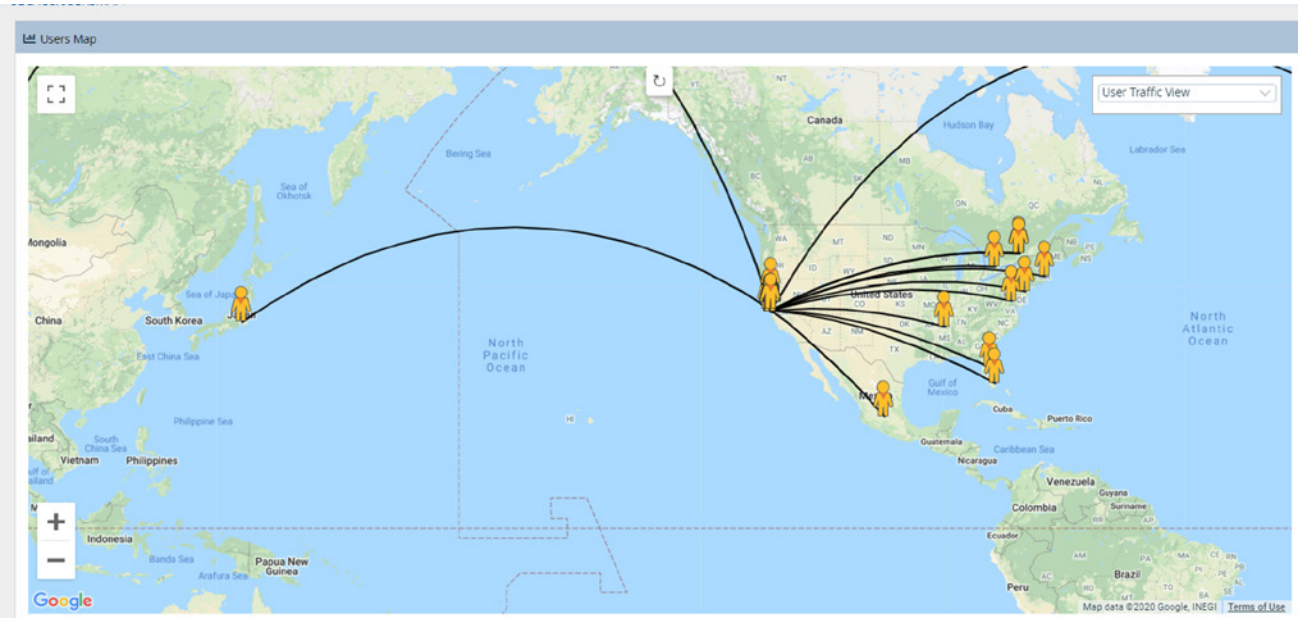


User Map

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.

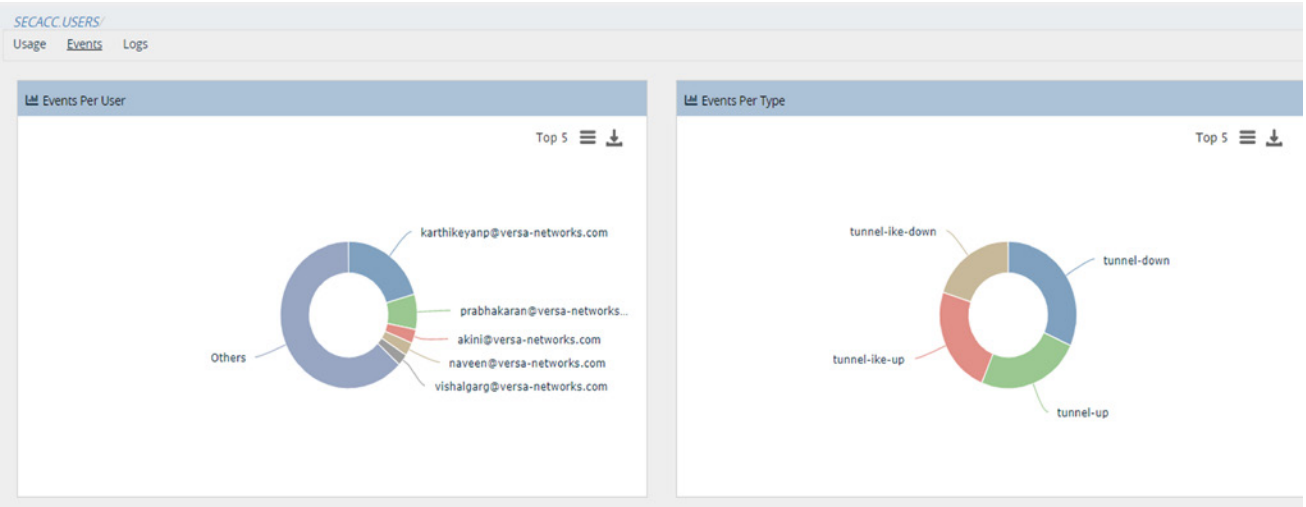


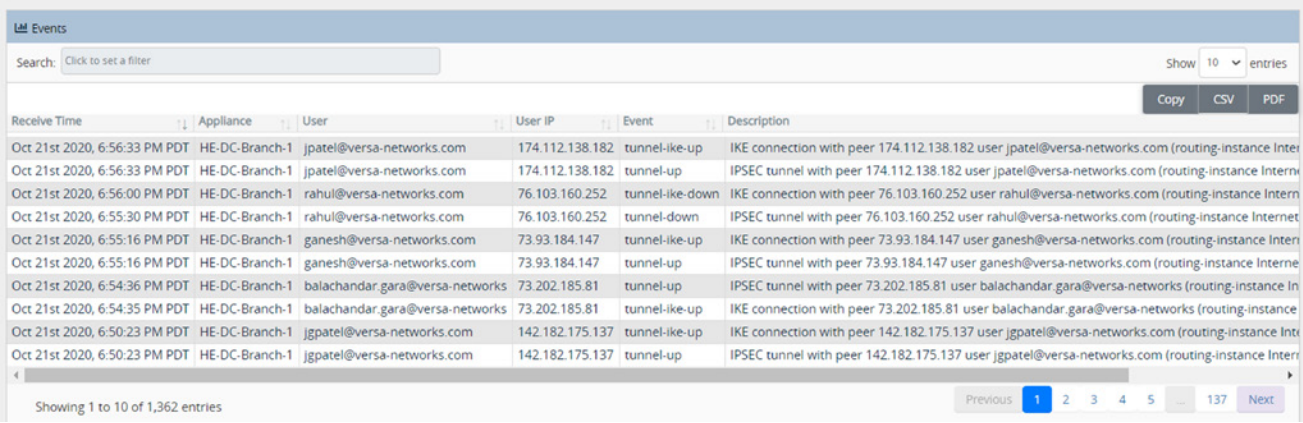
Traffic view provides the gateway the users are connected to as shown below.



User View: Tracking User Connectivity Events

Helps determine if there were any failures/flaps in the connections from remote access client.



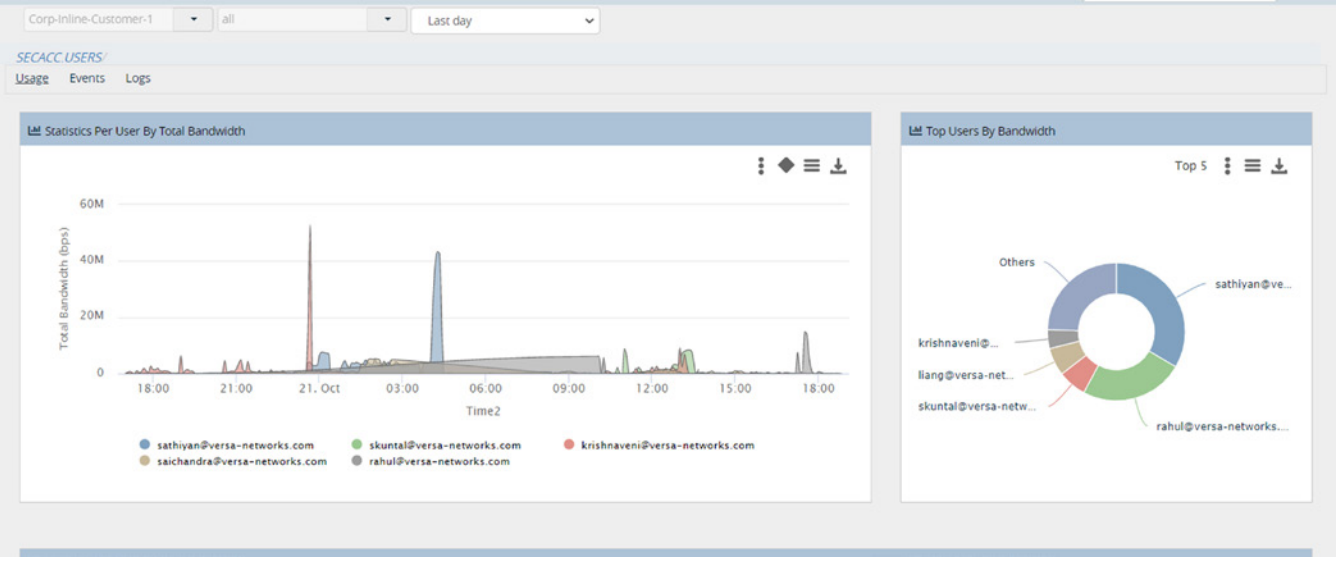


Authentication failures caused due to invalid username/password from the client, OTP mismatch, cipher mismatch, server tunnel IP address exhaustion etc. can be tracked as follows.

Receive Time	Severity	Appliance	Alarm Type	Description	Class
Oct 19th 2020, 5:21:36 PM PDT	indeterminate	HE-DC-Branch-1	ipsec-ike-auth-failure	IKE authentication with peer 207.47.61.9 user abhishubham@versa-networks.com (routing-instance Internet-1-Transport-VR) failed	new
Oct 19th 2020, 5:21:20 PM PDT	indeterminate	HE-DC-Branch-1	ipsec-ike-auth-failure	IKE authentication with peer 207.47.61.9 user abhishubham@versa-networks.com (routing-instance Internet-1-Transport-VR) failed	new
Oct 19th 2020, 5:21:06 PM PDT	indeterminate	HE-DC-Branch-1	ipsec-ike-auth-failure	IKE authentication with peer 207.47.61.9 user abhishubham@versa-networks.com (routing-instance Internet-1-Transport-VR) failed	new
Oct 19th 2020, 5:20:56 PM PDT	indeterminate	HE-DC-Branch-1	ipsec-ike-auth-failure	IKE authentication with peer 207.47.61.9 user abhishubham@versa-networks.com (routing-instance Internet-1-Transport-VR) failed	new
Oct 19th 2020, 3:43:42 PM PDT	indeterminate	HE-DC-Branch-1	ipsec-ike-auth-failure	IKE authentication with peer 207.47.61.9 user abhishubham@versa-networks.com (routing-instance Internet-1-Transport-VR) failed	new
Oct 19th 2020, 3:43:38 PM PDT	indeterminate	HE-DC-Branch-1	ipsec-ike-auth-failure	IKE authentication with peer 207.47.61.9 user abhishubham@versa-networks.com (routing-instance Internet-1-Transport-VR) failed	new

User View: Usage monitoring

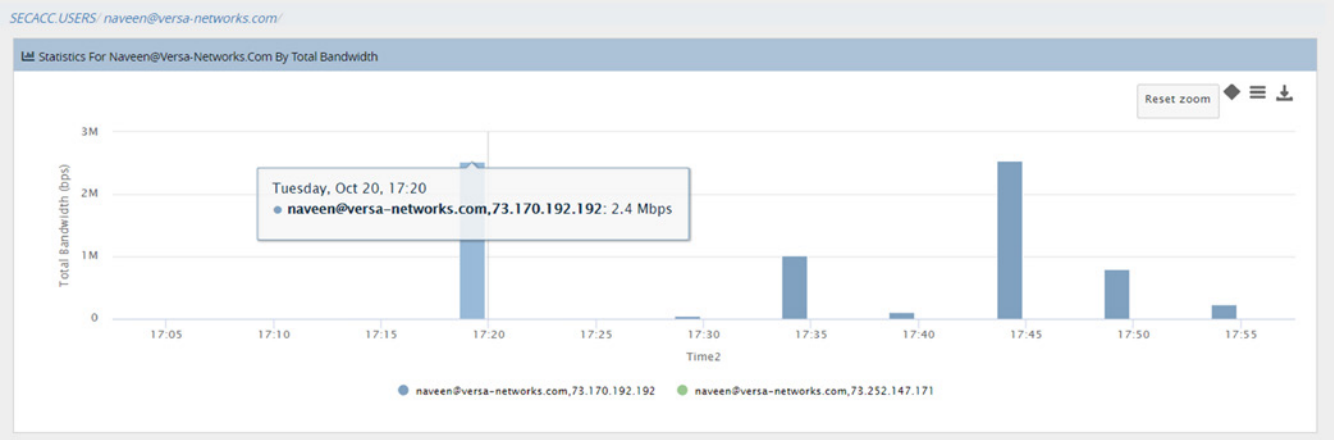
Top Remote Access Users Per Tenant Based on Traffic Activity.



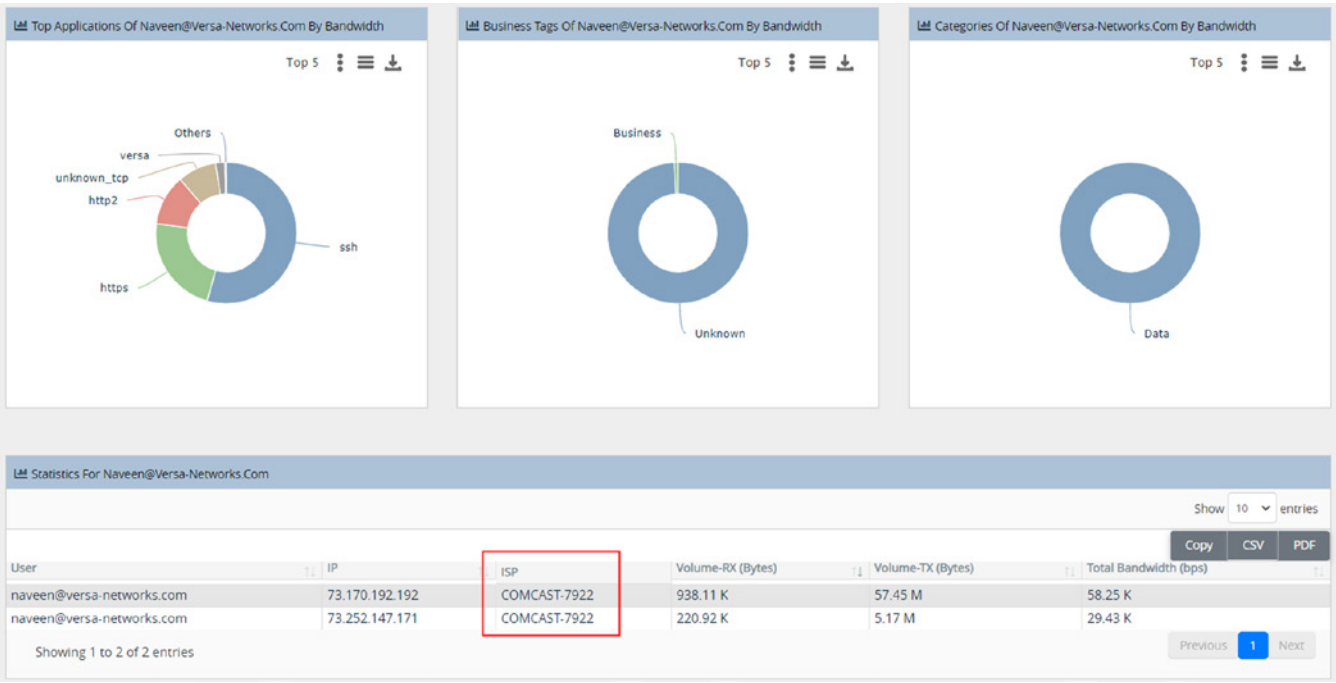
Summary of All User's Traffic Activity.

User	Volume-RX (Bytes)	Volume-TX (Bytes)	Total Bandwidth (bps)
rahul@versa-networks.com	210.3 M	796.68 M	2.17 M
sathiyan@versa-networks.com	91.7 M	3.08 G	2.98 M
saichandra@versa-networks.com	27.98 M	1007.25 M	340.17 K
krishnaveni@versa-networks.com	23.8 M	1.4 G	406.06 K
nsandrapati@versa-networks.com	18.07 M	212.82 M	197.49 K
liang@versa-networks.com	17.97 M	711.92 M	594.87 K
skuntal@versa-networks.com	15.48 M	522.24 M	611.81 K
sparasar@versa-networks.com	10.65 M	47.55 M	41.76 K
vinit@versa-networks.com	9.32 M	299.57 M	290.85 K
ganapathi@versa-networks.com	7.92 M	170.98 M	122.13 K
swatisnata@versa-networks.com	7.31 M	175.24 M	97.94 K
paulx@versa-networks.com	6.9 M	159.31 M	31.62 K
nraghu@versa-networks.com	6.51 M	101.23 M	127.91 K
surajm@versa-networks.com	6.08 M	24.94 M	17.29 K
srusti@versa-networks.com	5.8 M	134.47 M	29.43 K

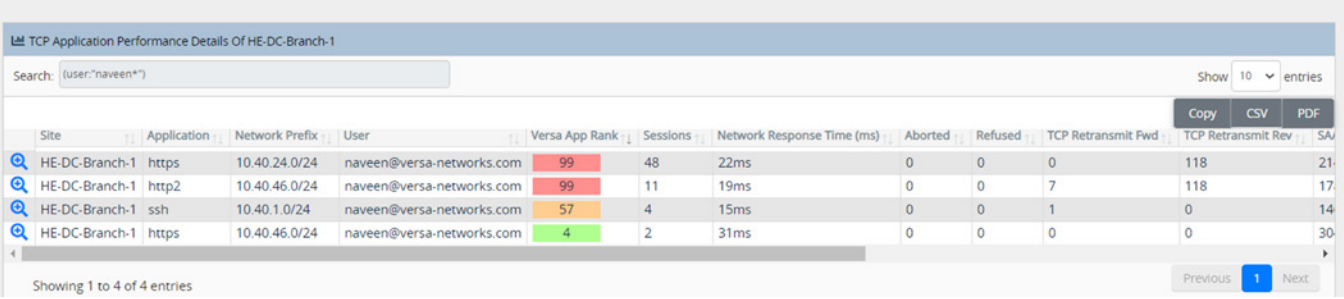
A drilldown into a specific user provides the user's traffic activity, applications accessed, events, and logs as follows.



Applications/application categories accessed by user Naveen.

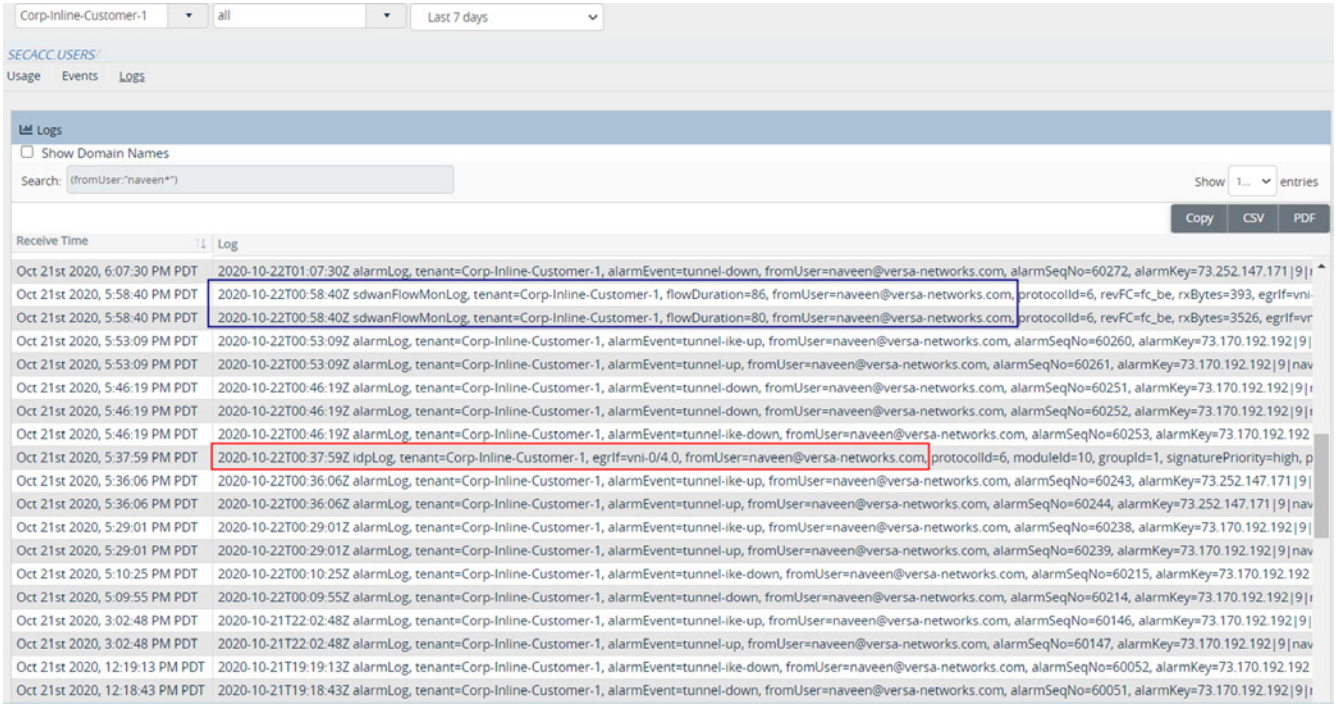


Application performance metrics for applications accessed by user Naveen.



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.



Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054
+1 408.385.7660 | info@versa-networks.com | www.versa-networks.com