Versatility 2024

Secure SD-WAN and SASE Operational Excellence

VERSA

Secure SD-WAN and SASE Operational Excellence

Topic:	Secure SD-WAN and SASE Operational Excellence Capabilities such as Deploying, Monitoring and Resolving Issues at Scale
Abstract:	The convergence of networking and security has simplified the infrastructure. However, the evolution of the workforce and cloud to a hybrid approach requires you to adapt your capabilities to deploy and operate your infrastructure. In this session, Versa subject matter expert will cover SD-WAN and SASE operational excellence capabilities such as deploying, monitoring and resolving issues at scale with automation and Versa Verbo.
Presenters:	Naveen Kumar, Director Engineering Naveen is a Director of System Test and has been with Versa for 9 years. He is involved in the design, development, and testing of Versa products. He also helps manage deploying solutions for customer production.

Running Networks Efficiently & Securely

- Headend management
- Secure all components from bad actors
- Configuration management of the whole network
- Prioritize and apply path policies
- Zero Trust Network (ZTNA)
- Connecting SASE Fabric to Customer Network
- Different deployment scenarios and topologies
- Find anomalies in the network
- Monitor network performance
- Monitor application performance
- Monitor end to end
- Stay up to date with latest security, OSS pack, and software
- Disaster recovery

Headend Management

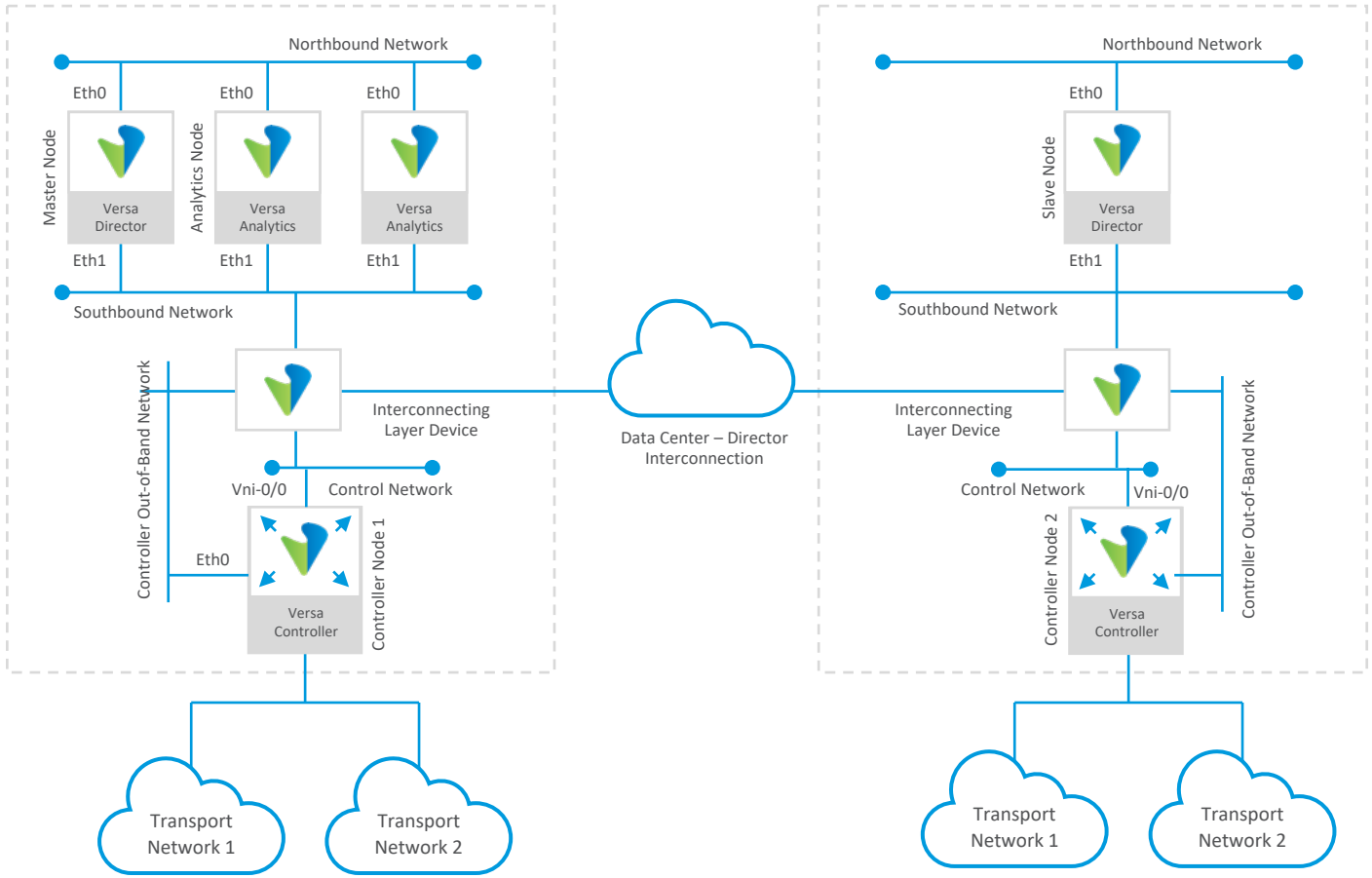
Getting the "Brains" of the Network Correct

- Chose right hardware required based on your scaling requirements

  Refer to sizing guidelines https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Headend_Deployment/Headend_Basics/02_Hardware_and_Software_Requirements_for_Headend

- Running on bare-metal vs virtual environments

- Concerns for running on private virtual cloud
  - Over subscription of CPU and memory
  - Disk I/O not optimized
  - Issues with hyperthreading enabled on hypervisor
  - Virtual NIC issues
  - Not using light weight and production quality hypervisors. Hypervisors may not be optimized for packet forwarding

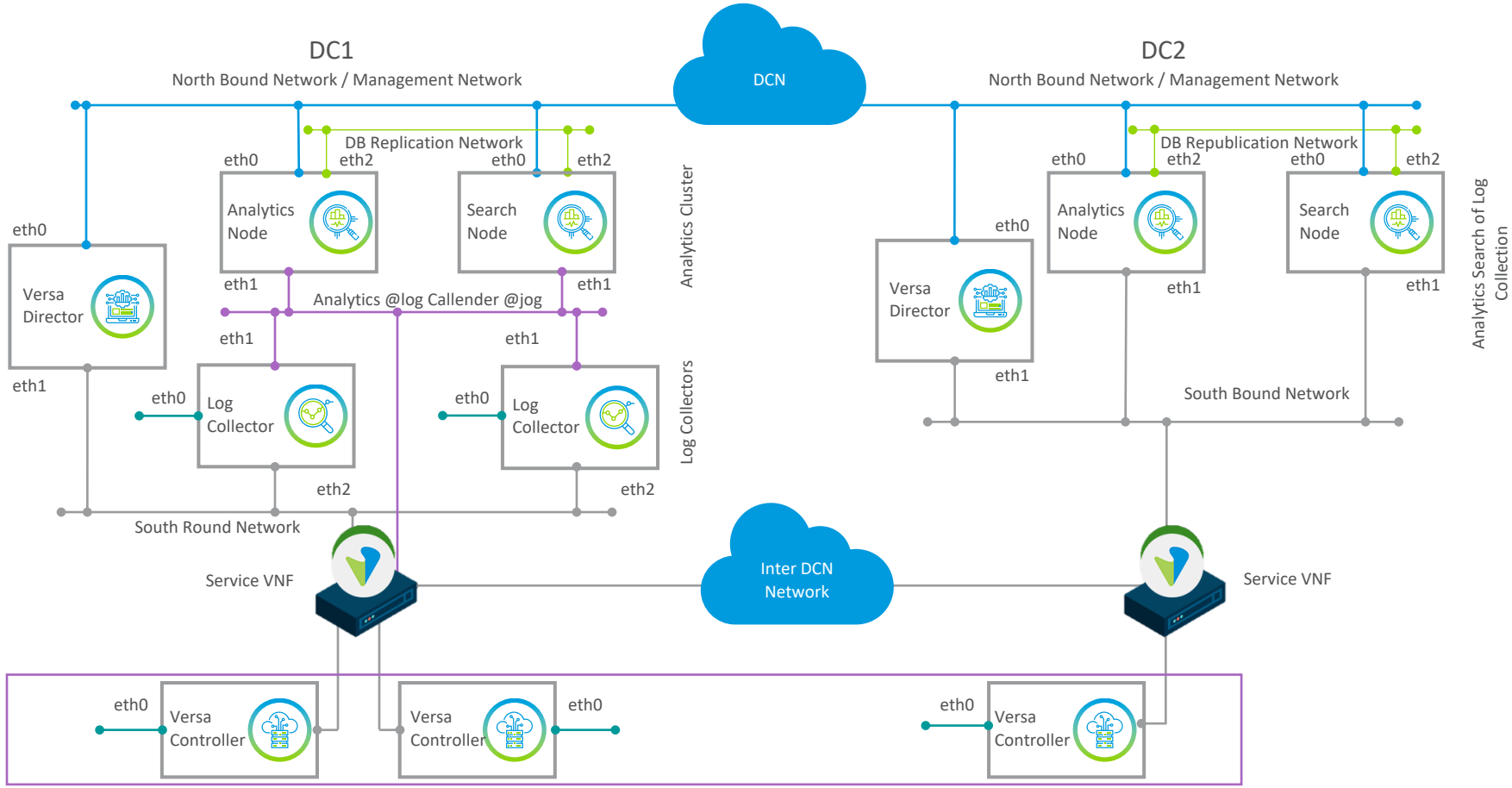


Versatility 2024

VERSA

Headend Management

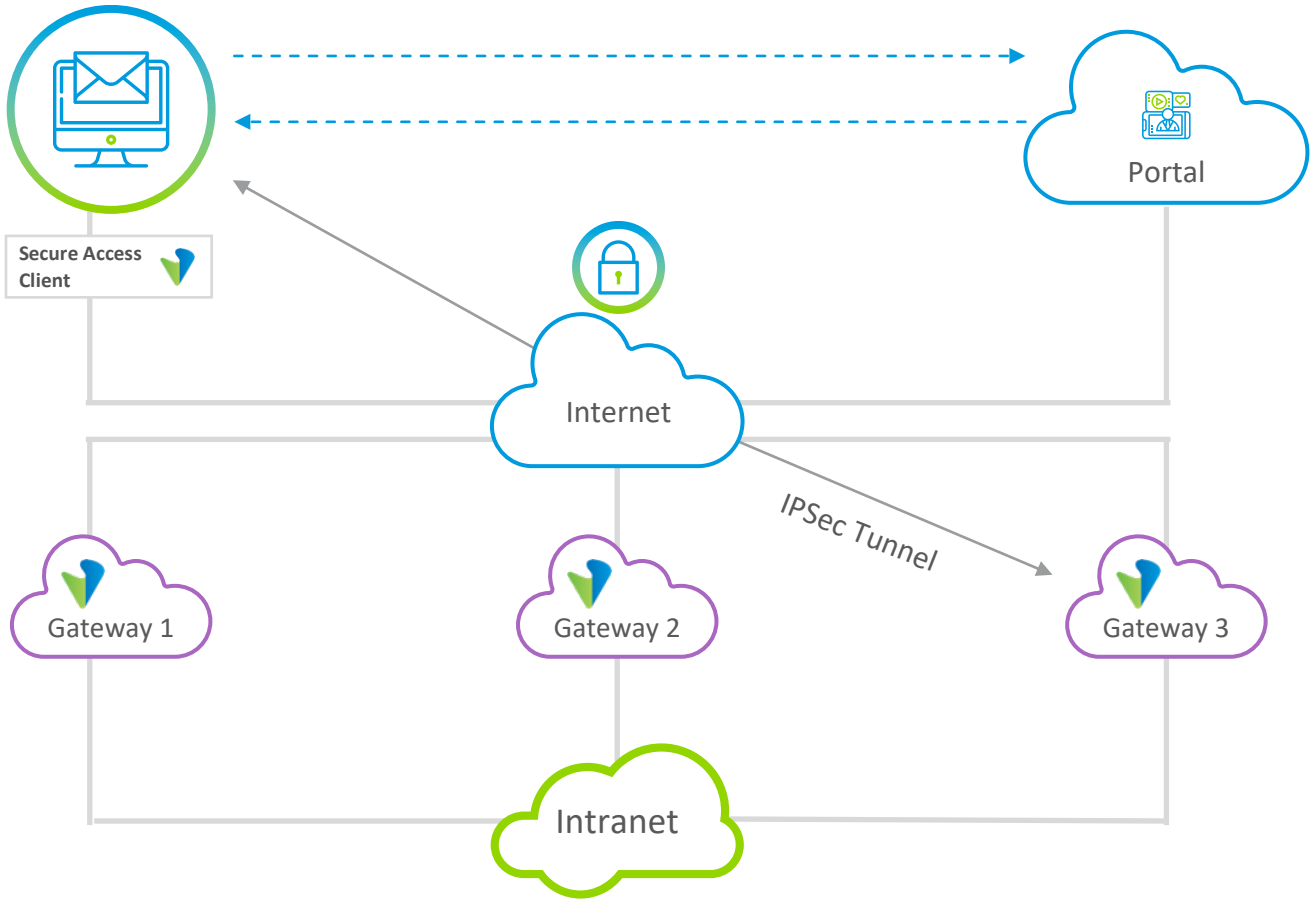
Getting the "Brains" of the Network Correct



- Run headend components in HA to avoid single point of failure
- Ensure the connectivity between two HA components is stable and reliable
- Monitor headend components
  - Stream alarms of headend components over syslog
  - Monitor memory, CPU, disk
  - Use external tools like Grafana

VERSA

Secure All Components from Bad Actors



- Change default password
- Enable external authentication for GUI, API, and SSH access
- Enable only required ports and disable all remaining ports
  Refer to the following Firewall requirements for which ports to open - https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Deployment_Basics/Firewall_Requirements
- Services must be activated only on required interfaces
- Enable API access via OAuth
- Run Director HA and Analytics cluster communication via southbound private network for better security practices

VERSA

Secure All Components from Bad Actors

- Install valid certificate for https access to Versa Director and Analytics
- Configure SSH banner on all components
- Configure NTP and DNS
- Enable stronger encryption, hash for SSH and IKE/IPsec for example AES256 SHA512 and higher
- Set complex passwords for GUI access, Rest API access, and SSH access
- Use Versa Advanced Security Tool (VAST) to security harden all the components automatically
  Refer to Versa Automation Hardening Doc https://docs.versa-networks.com/Solutions/System_Hardening/Perform_Automated_System_Hardening

VERSA

Configuration Management of the Entire Network

Templates

- Identify use cases
- Build templates for use cases and re-use them
- Generate templates from workflow
- Build service templates for use cases not supported by workflow
- Use common shared template if same use case applies across multiple customers

Deploying Devices in Bulk

- Group devices based on use cases
- Create device group for each unique use case
- Assign template, service, and shared templates to device group
- Attach to device group
- Attach service templates directly to devices for one-off use cases
- Import bind variables to bulk deploy from CSV
- Use Rest APIs for bulk deploy or modify

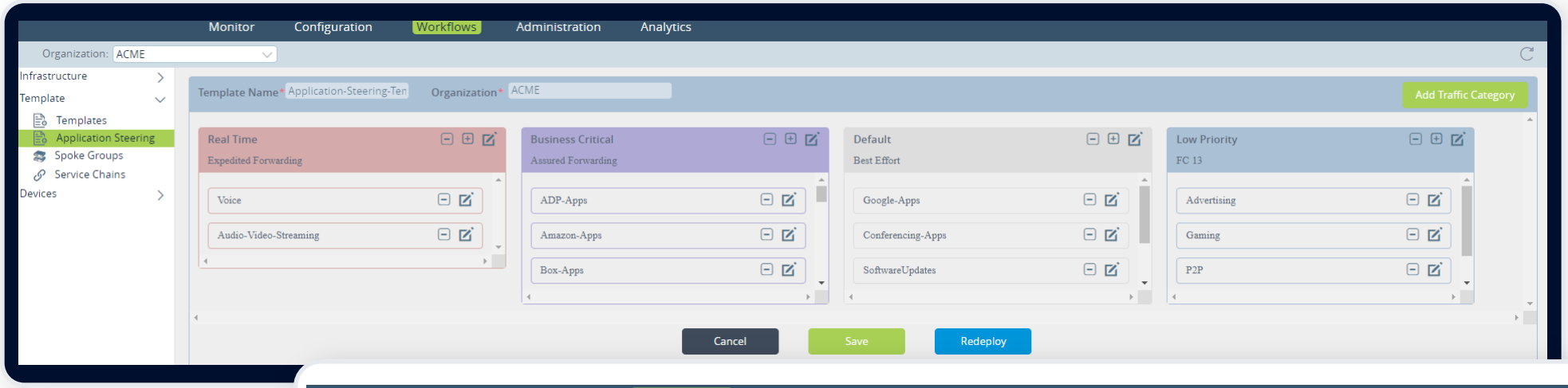
Prioritizing & Applying the Best Path Policies Based on Category of Traffic

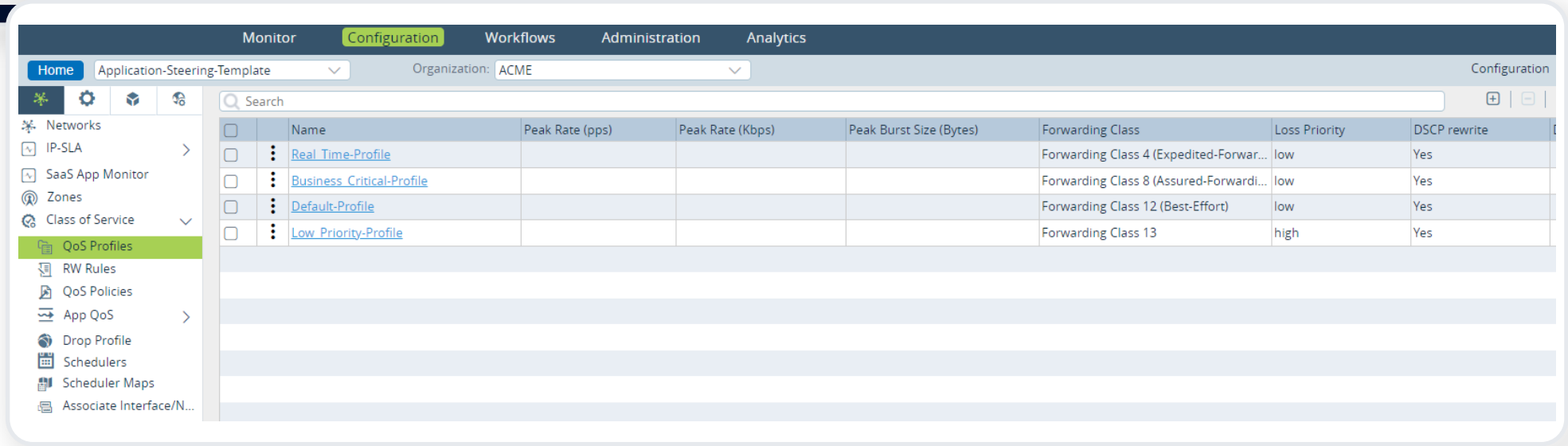
It is very important to classify traffic, prioritize and chose best path to get best user experience for customer traffic.

Application Steering Templates contains following components to achieve this requirement:

- Classify traffic
  - Real time – Audio, video calls
  - Business Critical apps
  - Best Effort
  - Low priority
- Apply QoS
- Apply best path selection

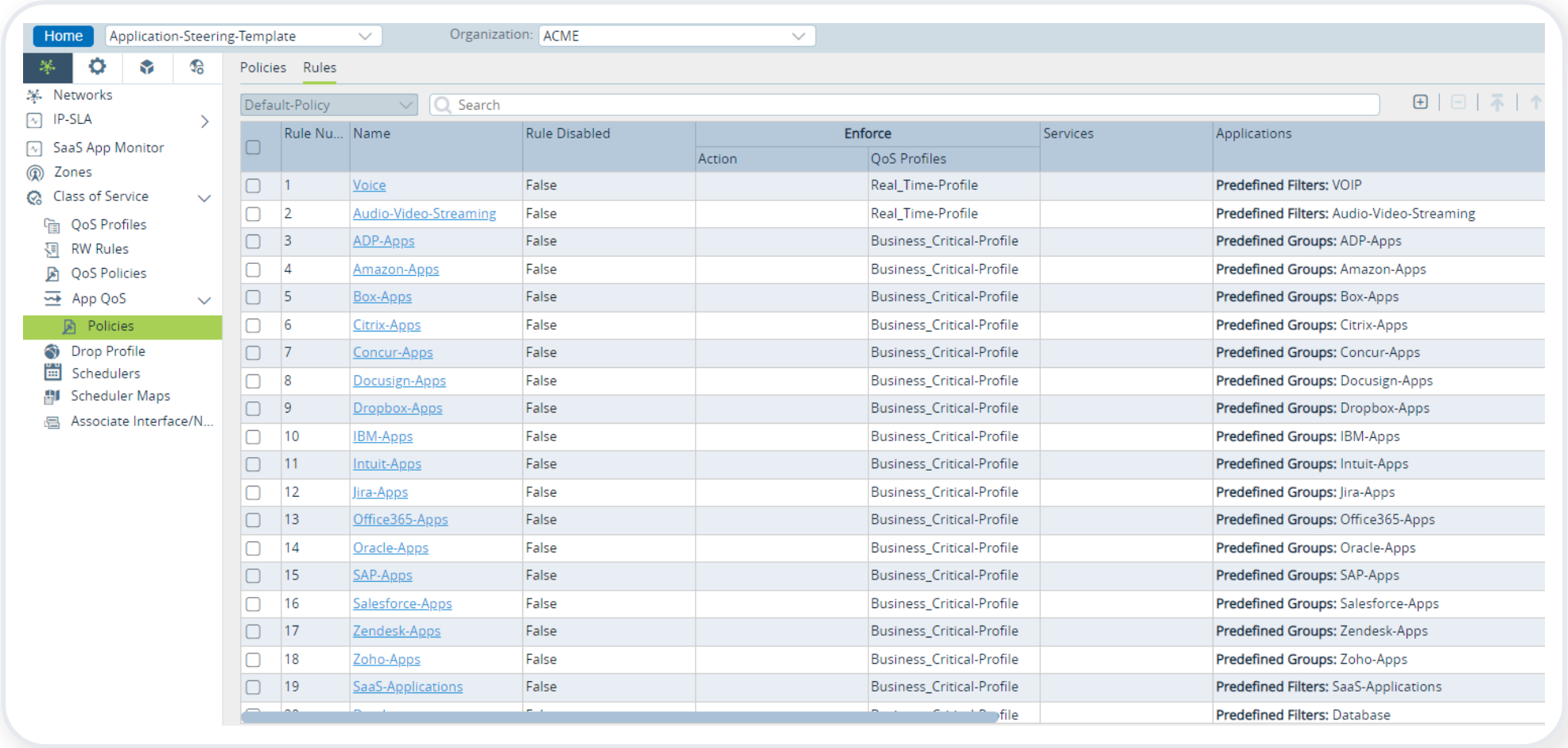
Classify Traffic into Different Buckets





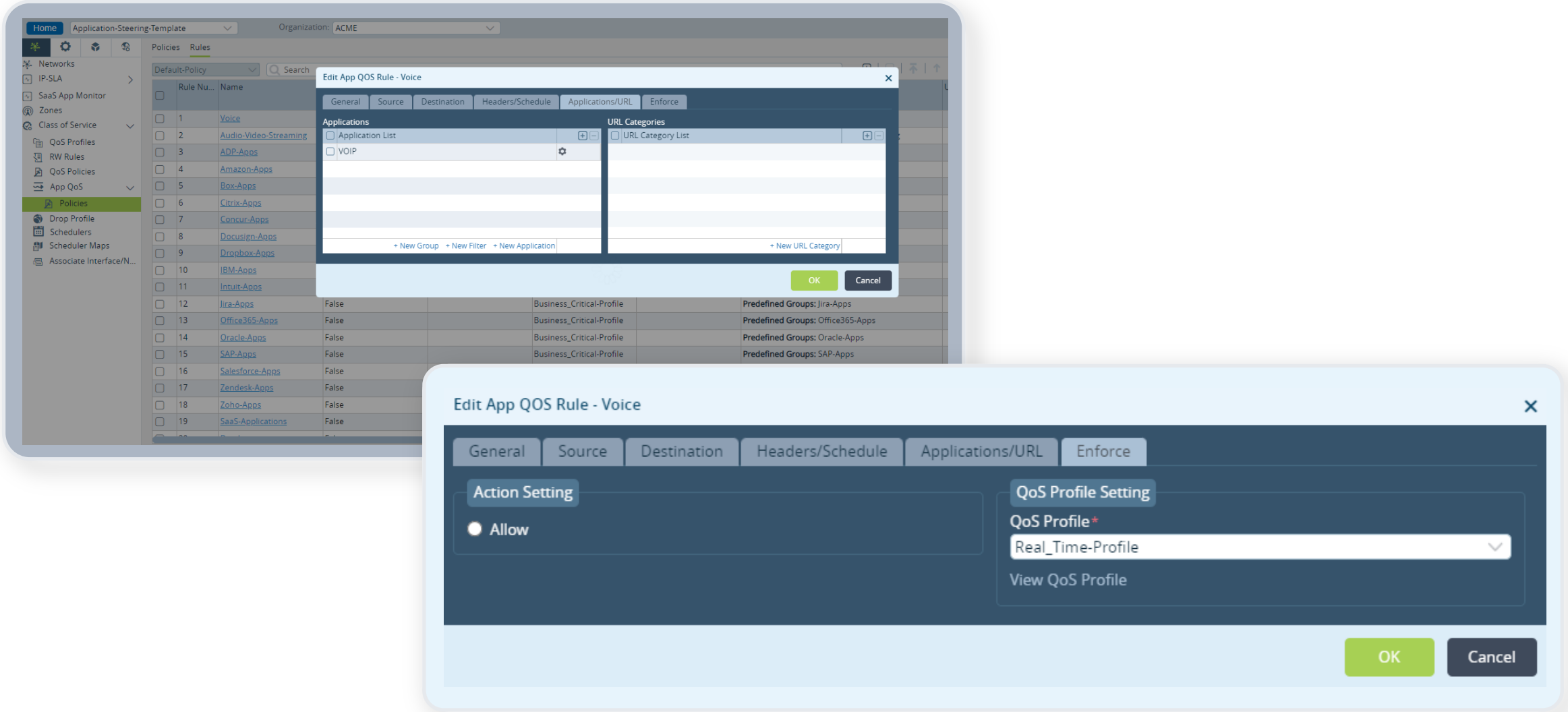
Apply QoS

Prioritize the traffic by applying classified traffic with different priority queues



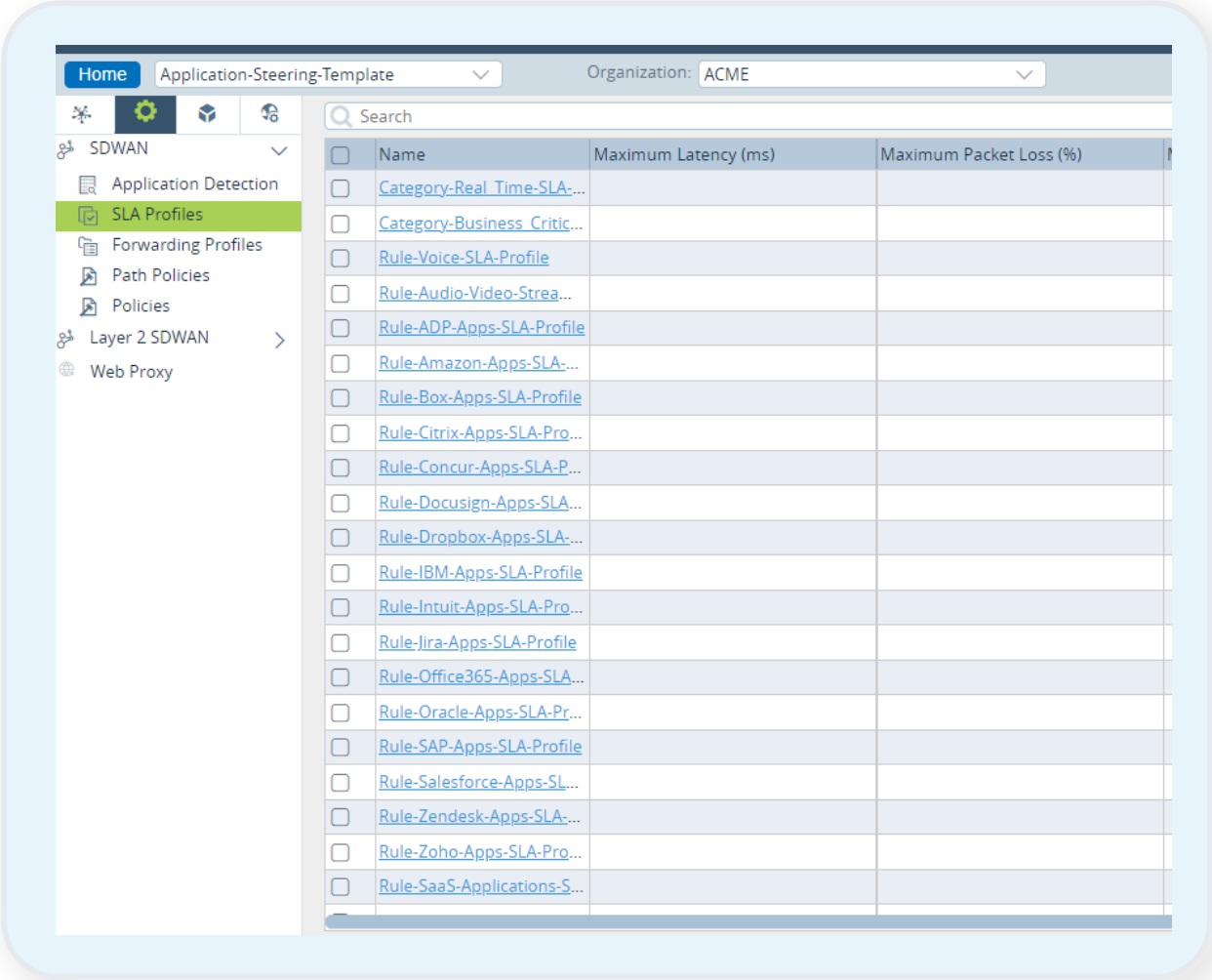
	Rule Nu...	Name	Rule Disabled	Enforce		Services	Applications
				Action	QoS Profiles		
	1	Voice	False		Real_Time-Profile		**Predefined Filters:** VOIP
	2	Audio-Video-Streaming	False		Real_Time-Profile		**Predefined Filters:** Audio-Video-Streaming
	3	ADP-Apps	False		Business_Critical-Profile		**Predefined Groups:** ADP-Apps
	4	Amazon-Apps	False		Business_Critical-Profile		**Predefined Groups:** Amazon-Apps
	5	Box-Apps	False		Business_Critical-Profile		**Predefined Groups:** Box-Apps
	6	Citrix-Apps	False		Business_Critical-Profile		**Predefined Groups:** Citrix-Apps
	7	Concur-Apps	False		Business_Critical-Profile		**Predefined Groups:** Concur-Apps
	8	Docusign-Apps	False		Business_Critical-Profile		**Predefined Groups:** Docusign-Apps
	9	Dropbox-Apps	False		Business_Critical-Profile		**Predefined Groups:** Dropbox-Apps
	10	IBM-Apps	False		Business_Critical-Profile		**Predefined Groups:** IBM-Apps
	11	Intuit-Apps	False		Business_Critical-Profile		**Predefined Groups:** Intuit-Apps
	12	Jira-Apps	False		Business_Critical-Profile		**Predefined Groups:** Jira-Apps
	13	Office365-Apps	False		Business_Critical-Profile		**Predefined Groups:** Office365-Apps
	14	Oracle-Apps	False		Business_Critical-Profile		**Predefined Groups:** Oracle-Apps
	15	SAP-Apps	False		Business_Critical-Profile		**Predefined Groups:** SAP-Apps
	16	Salesforce-Apps	False		Business_Critical-Profile		**Predefined Groups:** Salesforce-Apps
	17	Zendesk-Apps	False		Business_Critical-Profile		**Predefined Groups:** Zendesk-Apps
	18	Zoho-Apps	False		Business_Critical-Profile		**Predefined Groups:** Zoho-Apps
	19	SaaS-Applications	False		Business_Critical-Profile		**Predefined Filters:** SaaS-Applications
					file		**Predefined Filters:** Database

Apply QoS



VERSA

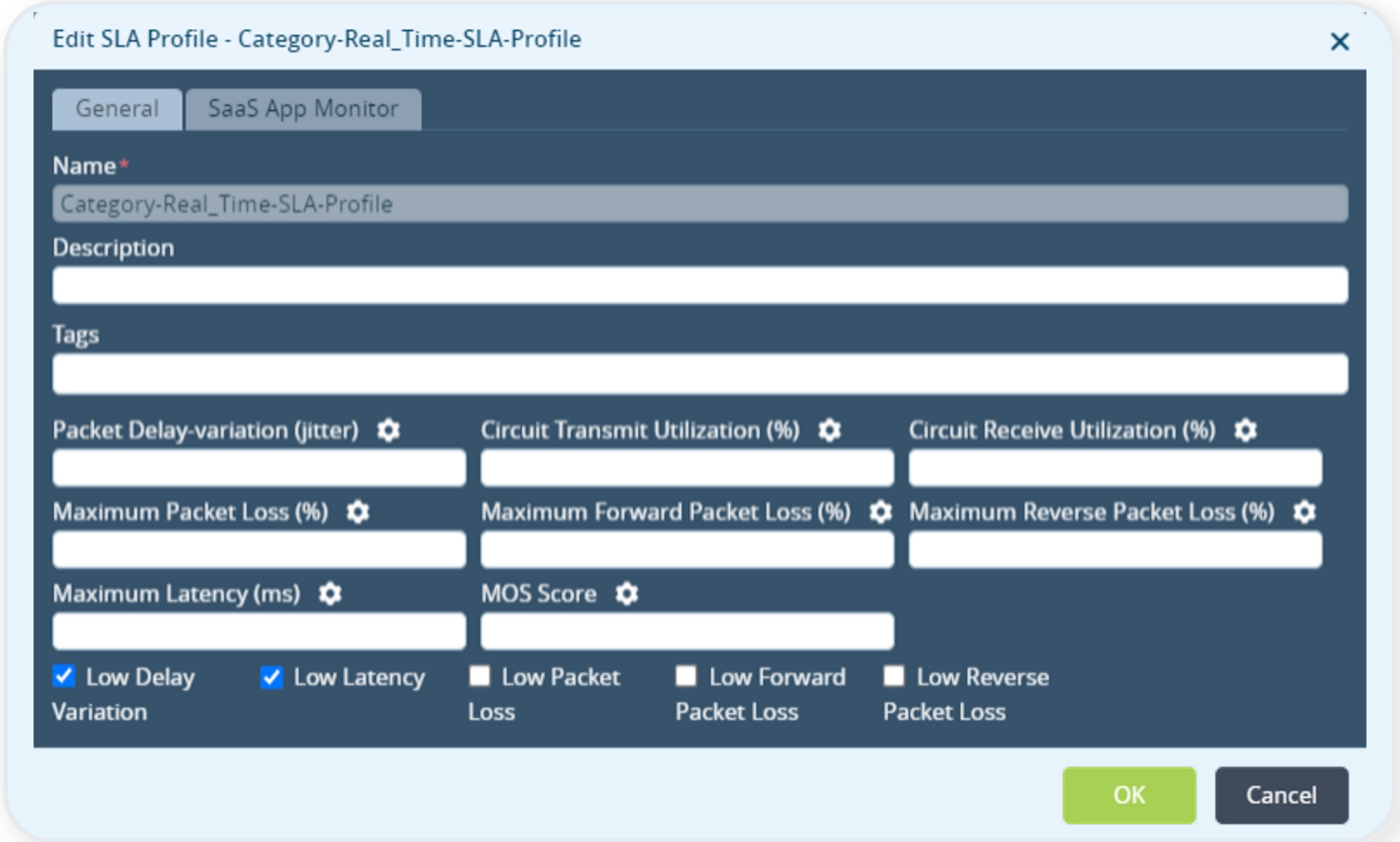
Apply Best Path Selection – Configure SLA Profiles



- The first step in configuring the best path selection is to create SLA profiles for each category of traffic.
- SLA profile defines latency, jitter, packet loss, MOS, bandwidth requirements

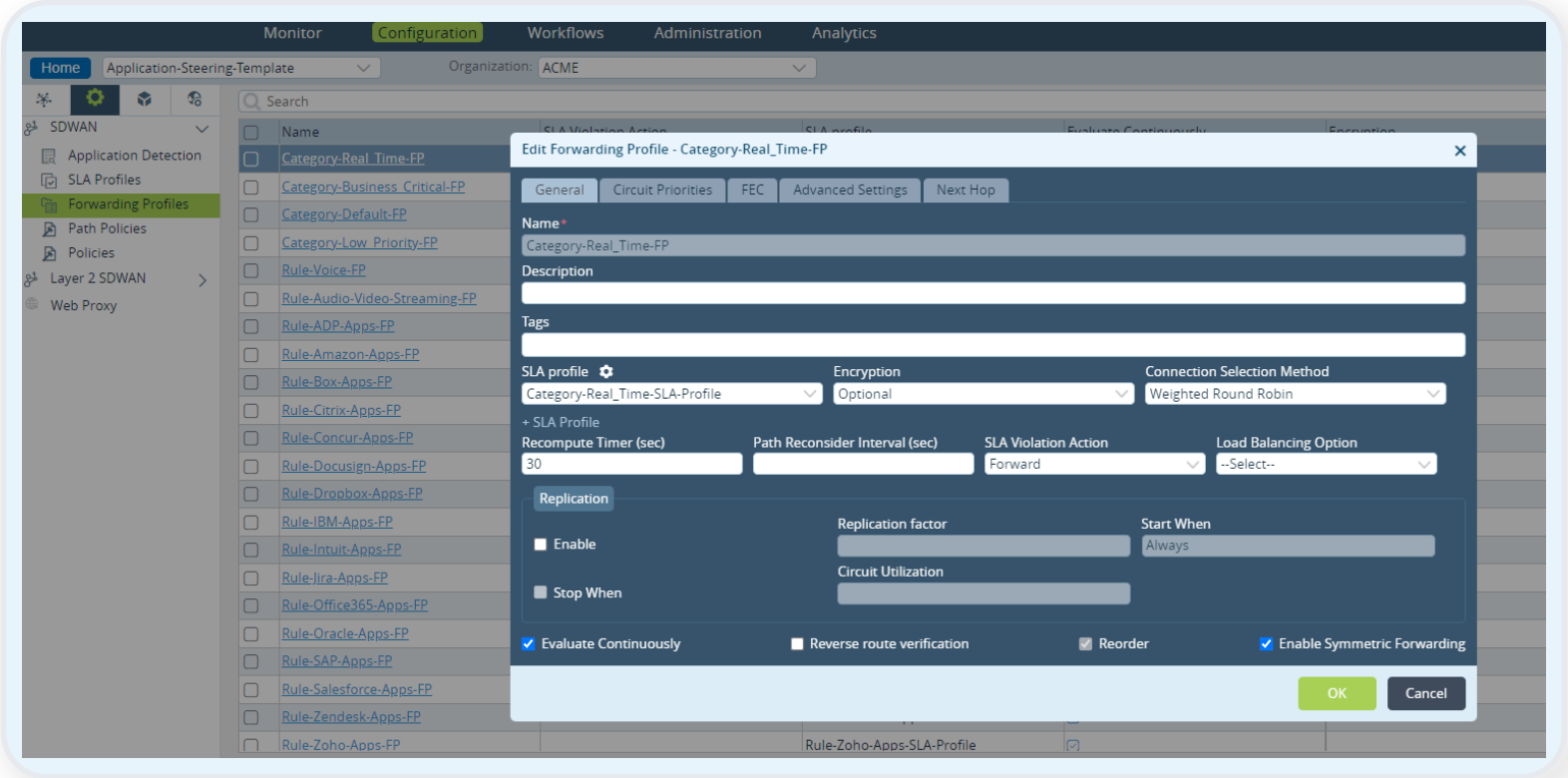
VERSA

Configure SLA Profiles



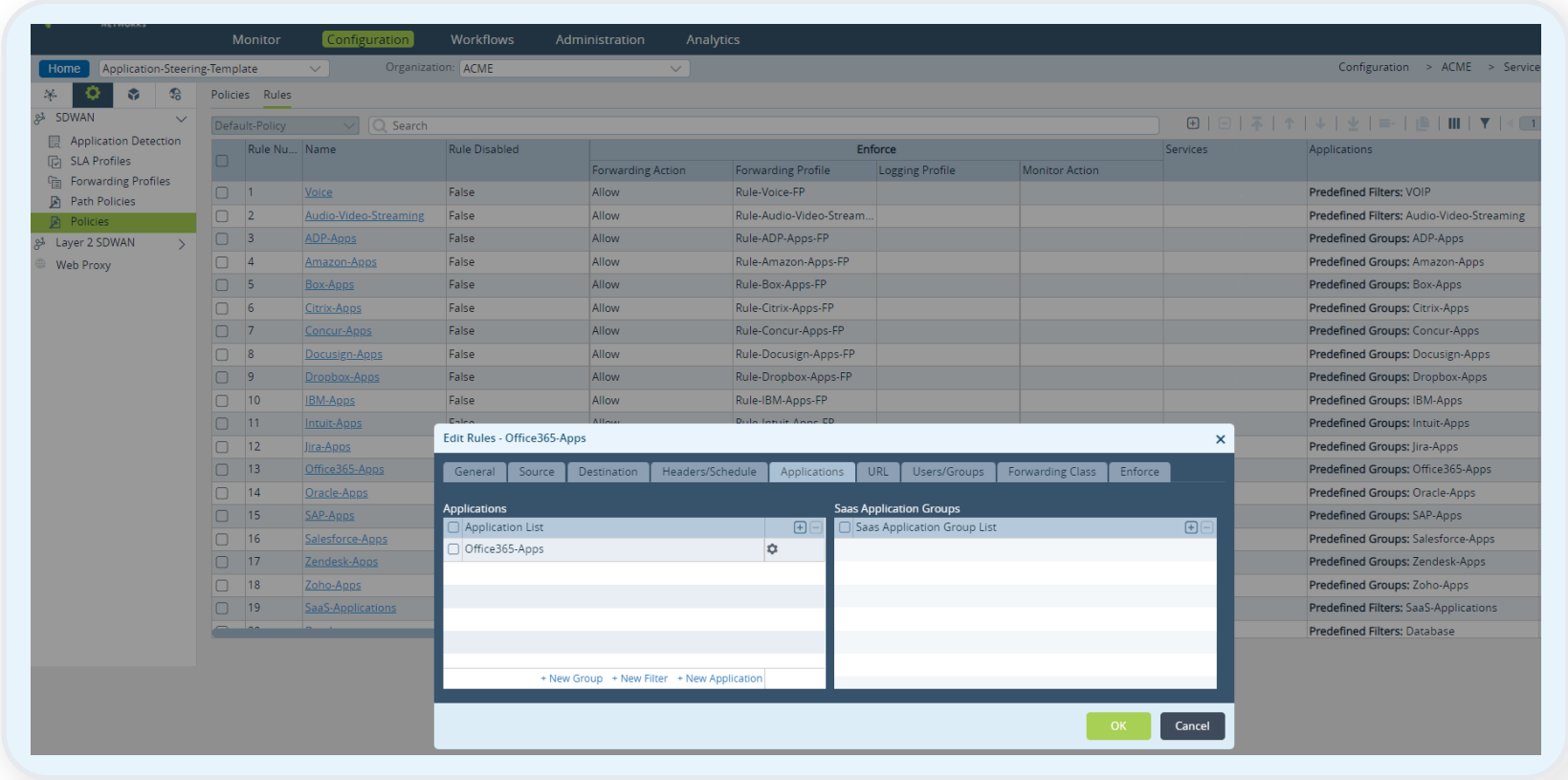
Configure Forwarding Profiles

Forwarding profiles defines the best path to be used based on requirements defined in SLA profiles



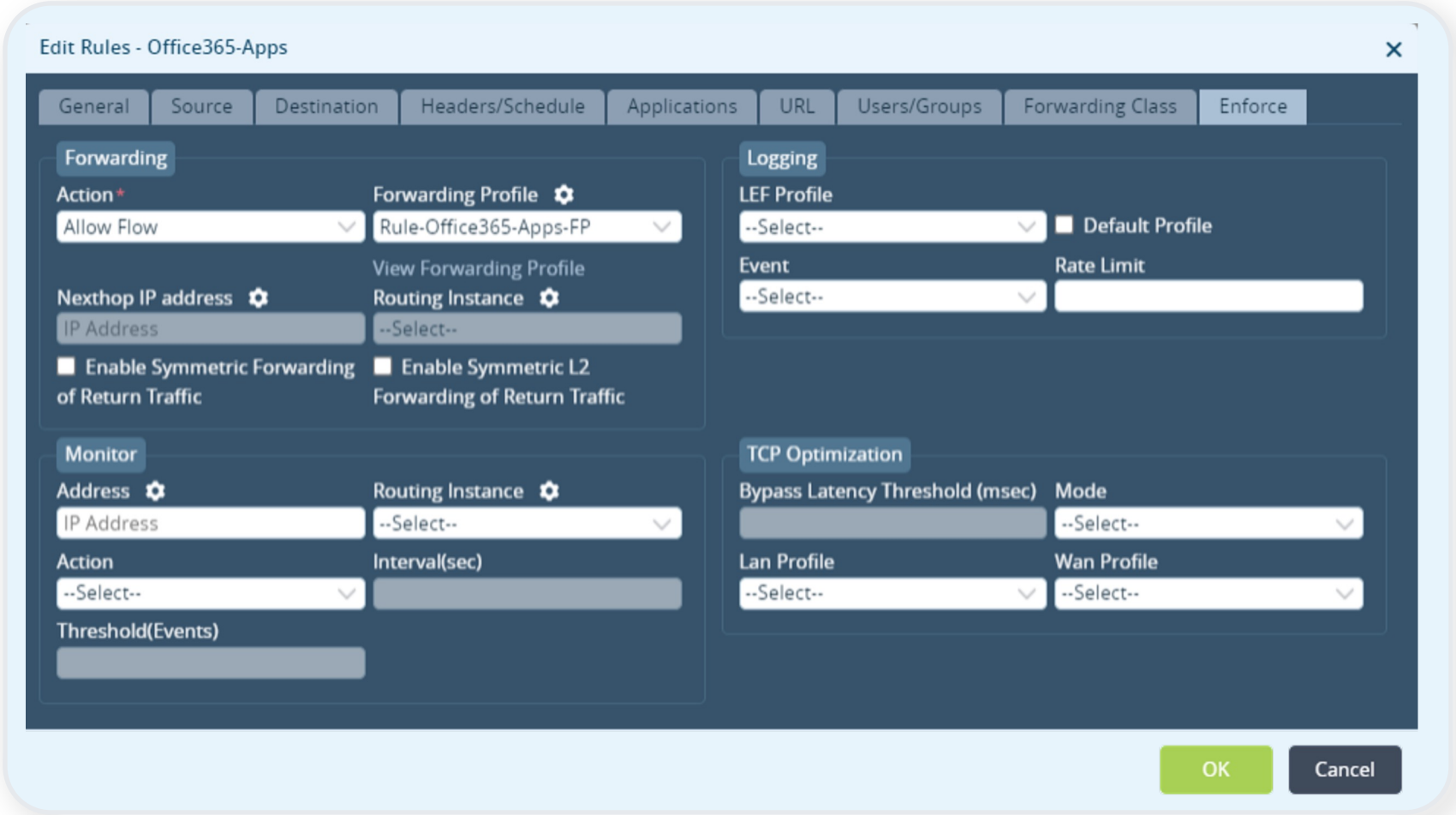
Configure SD-WAN Policies

SD-WAN polices is created to match traffic based on L2 to L7 and attaches forwarding profile. There will be SD-WAN policy created for each of customer traffic category.



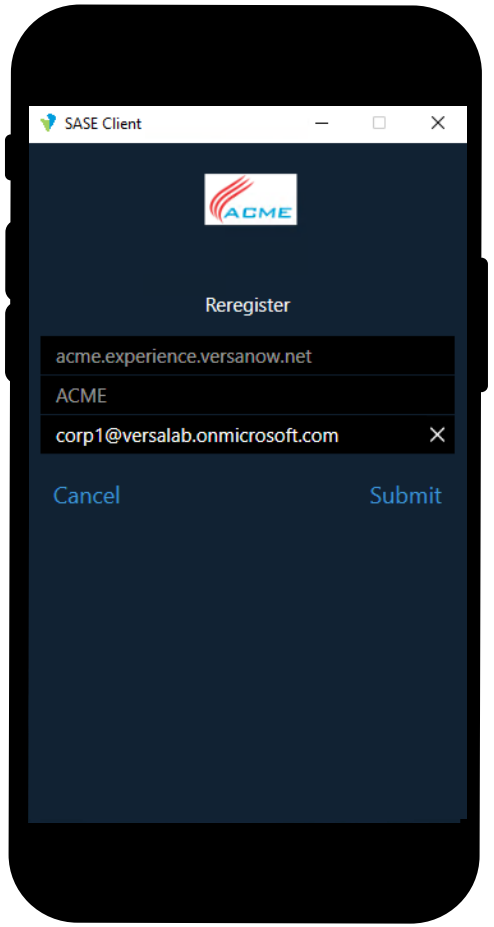
Configure SD-WAN Policies

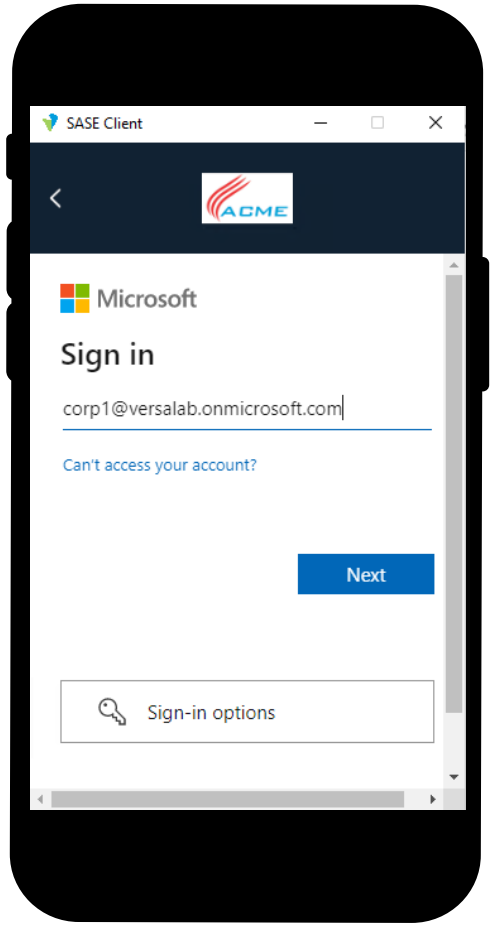
Example of attaching forwarding profile to SD-WAN policy created for Office365 apps



Zero Trust Network Access

Portal Policies





Versatility 2024

Authenticate before connecting to portal and gateway

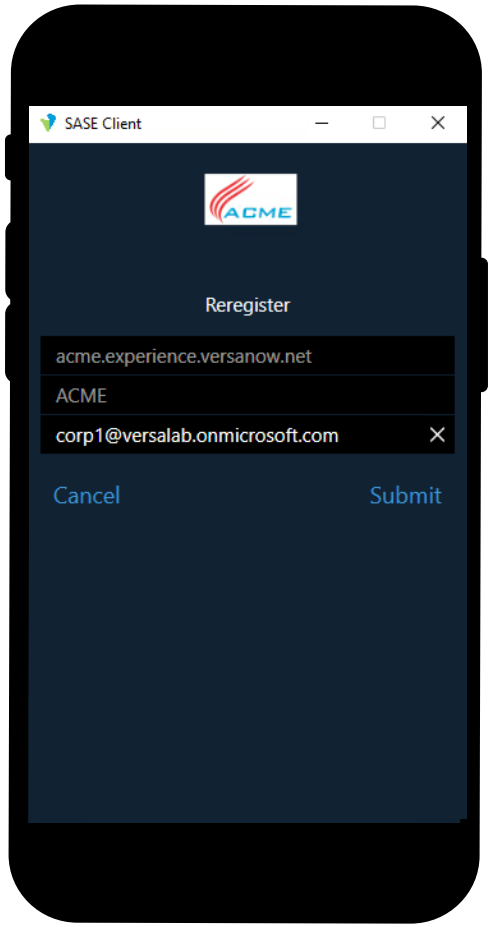
- Use standard authentication like LDAP, SAML
- Enable MFA
- Enable email-based OTP
- Enable TOTP

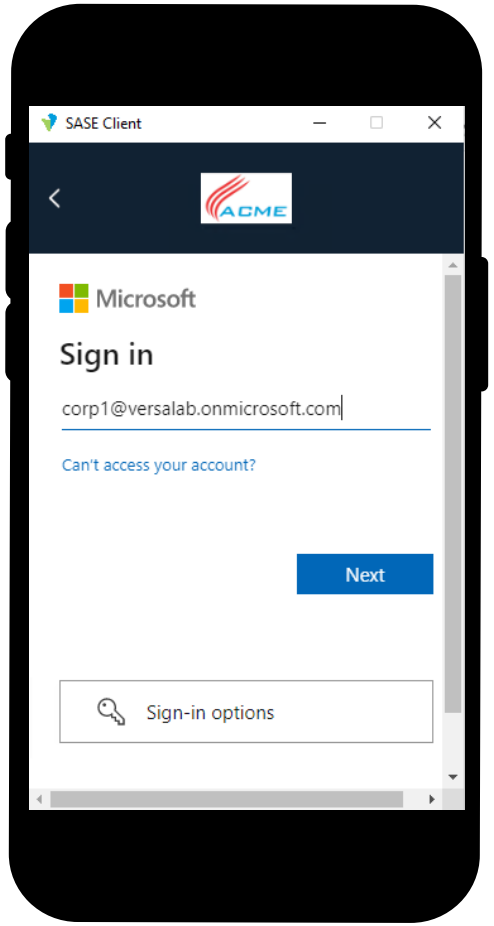
Check device posture

- Check device is complaint
- Check device is upgraded to latest OS software pack
- Check firewall service is enabled
- Check device is running antimalware software
- Check device is running anti-phishing software
- Check device is running correct browser software version
- Integrate with Microsoft intune

VERSA NETWORKS

Zero Trust Network Access





Check user posture

- User and Entity Behavior Analytics (UEBA(
- Bulk delete, Bulk upload, Bulk failed logins, risk country, impossible trave etc.
- EDR
- Configure policy by matching UCS and ECS

CASB

- Enable granular policies based on application events

DLP

- Configure policies to avoid loss of sensitive information

Advanced threat protection (ATP)

- Sandboxing
- AI/ML
- Malware analysis

VERSA NETWORKS

Connecting SASE Fabric & Customer Private Networks

Connection Methods

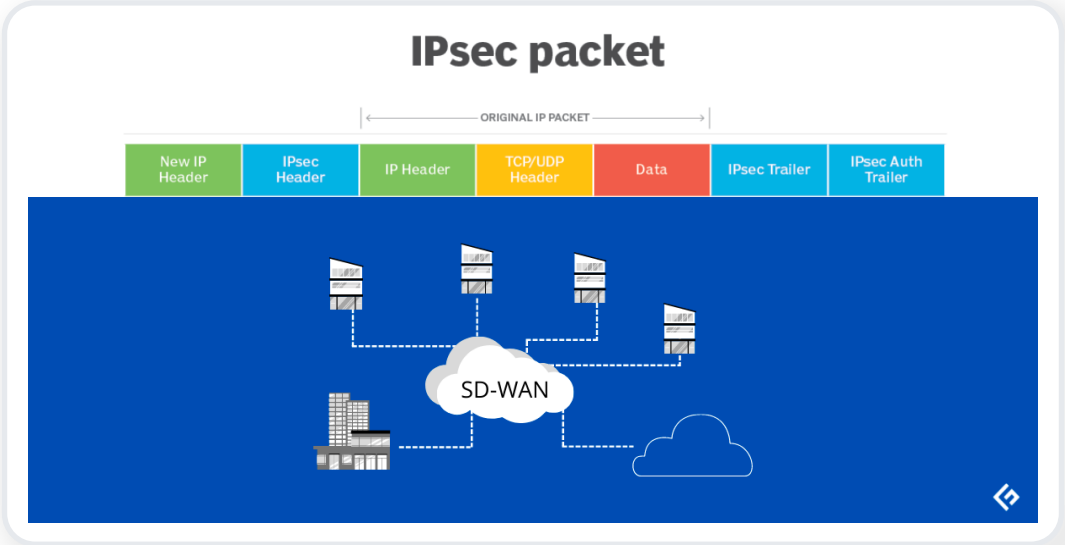
- Select the best option for your client
  - IPSEC
  - GRE
  - SD-WAN
- Routing between network segments
  - Static routing
  - BGP
  - BFD

Best Connectivity Options

- Site-to-site IPSec/Concentrator
  - Use strong encryption such as AES128/AES256
  - Use strong hashing – SHA256/SHA512
  - Avoid using MD5/3DES
- Open necessary ports:
  - UDP 500 for IKE Phase 1 (ISAKMP)
  - UDP 4500 for IKE phase 2

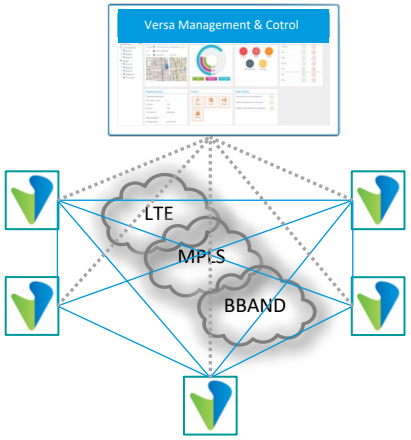
Use SD-WAN for best of all

- Benefits of SD-WAN:
  - Constant link monitoring
  - Traffic steering
  - Traffic conditioning (FEC/Replication)
  - Multiple paths
  - End-to-end monitoring

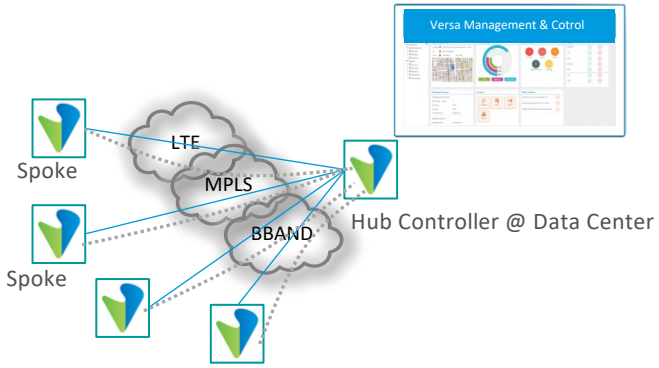


VERSA

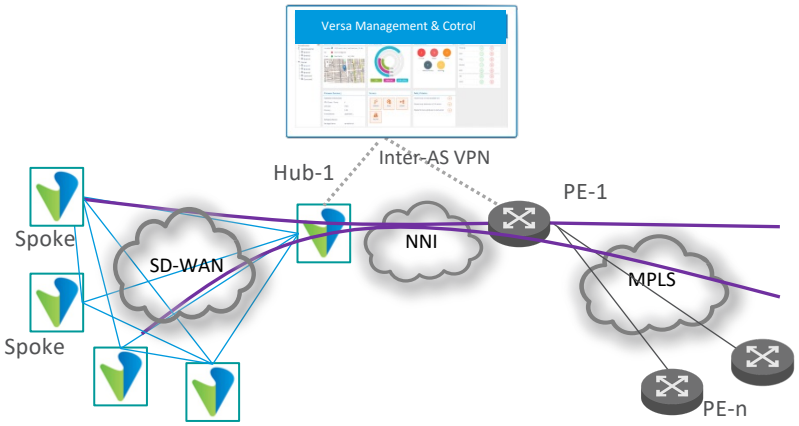
Different deployment scenarios and topologies



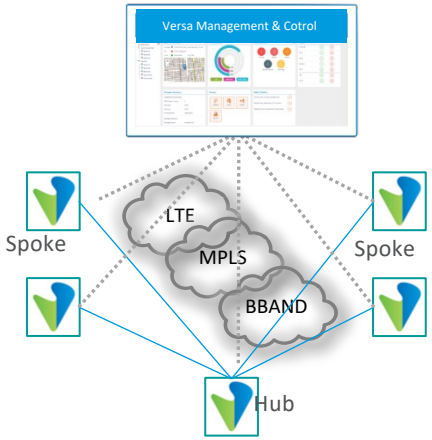
Full Mesh



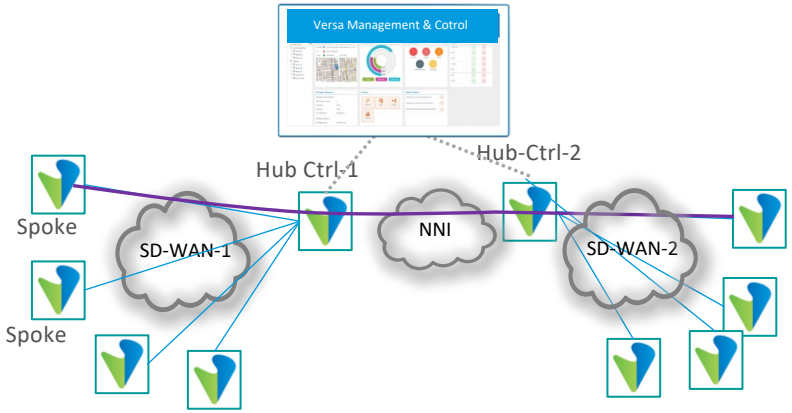
Controller & Hub Converged



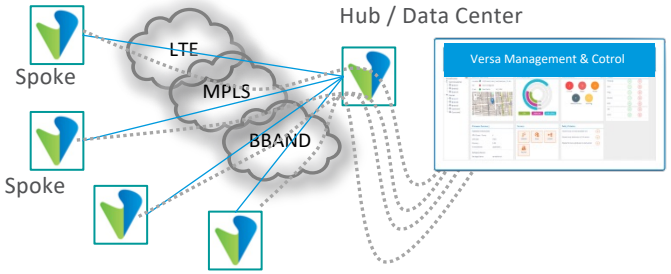
Inter-as Connectivity
(ie: Brownfield)



Hub-Spoke



Spoke-Hub-Hub-Spoke



Controller Behind Hub

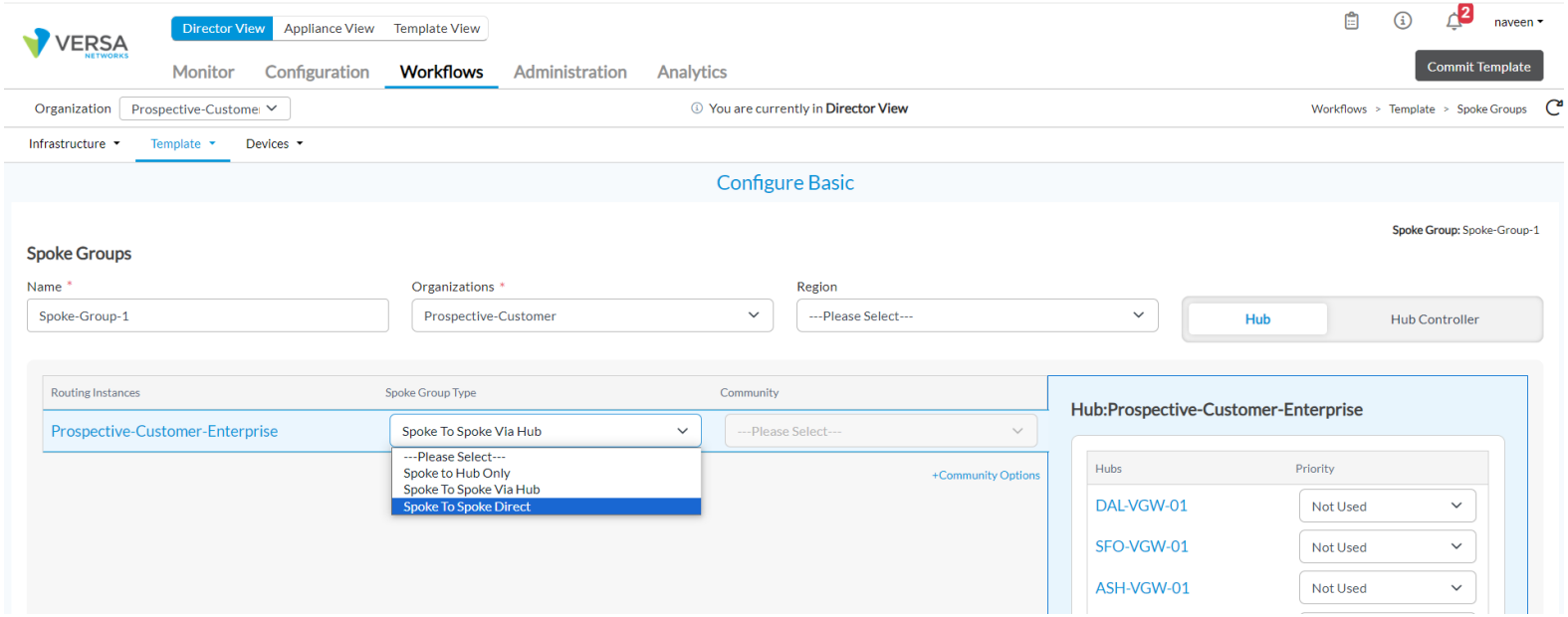
VERSA

Different deployment scenarios and topologies

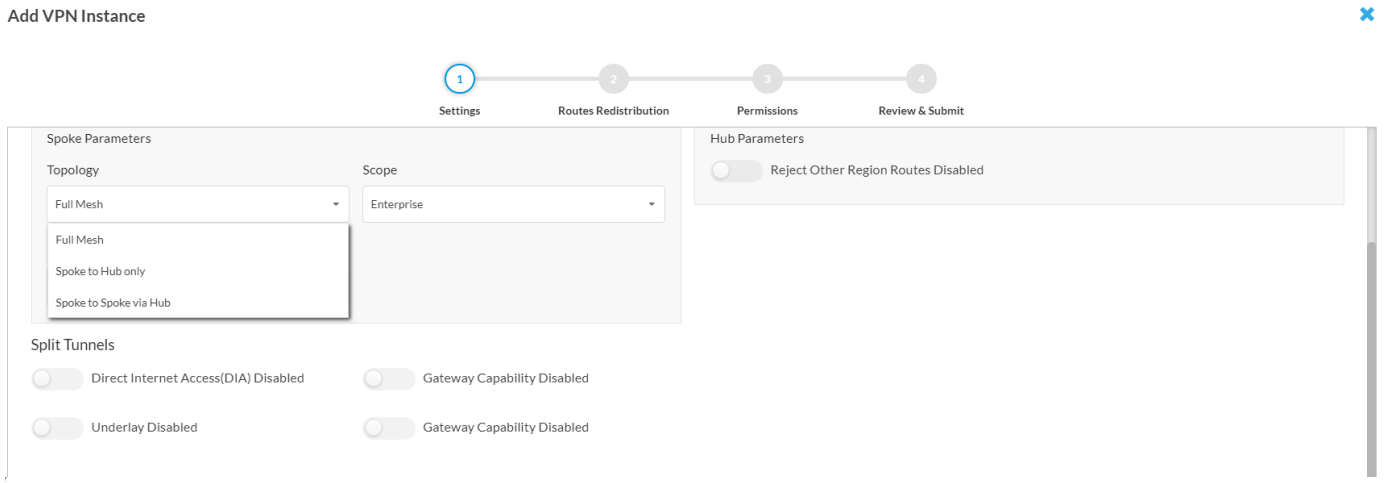
- Use Director and Concerto workflows to create

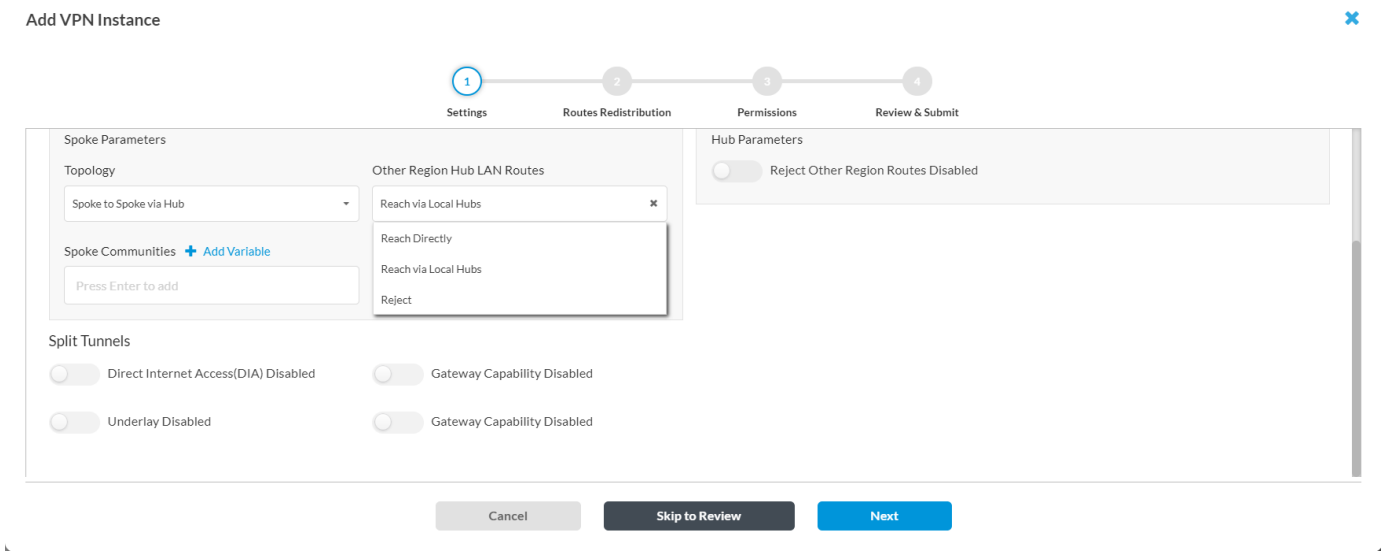
Different topologies

- Full mesh
- Spoke to Hub only
- Spoke to Spoke via Hub
- Spoke-Hub-Hub-Spoke (SHHS)
- Partial mesh (make use of regions)



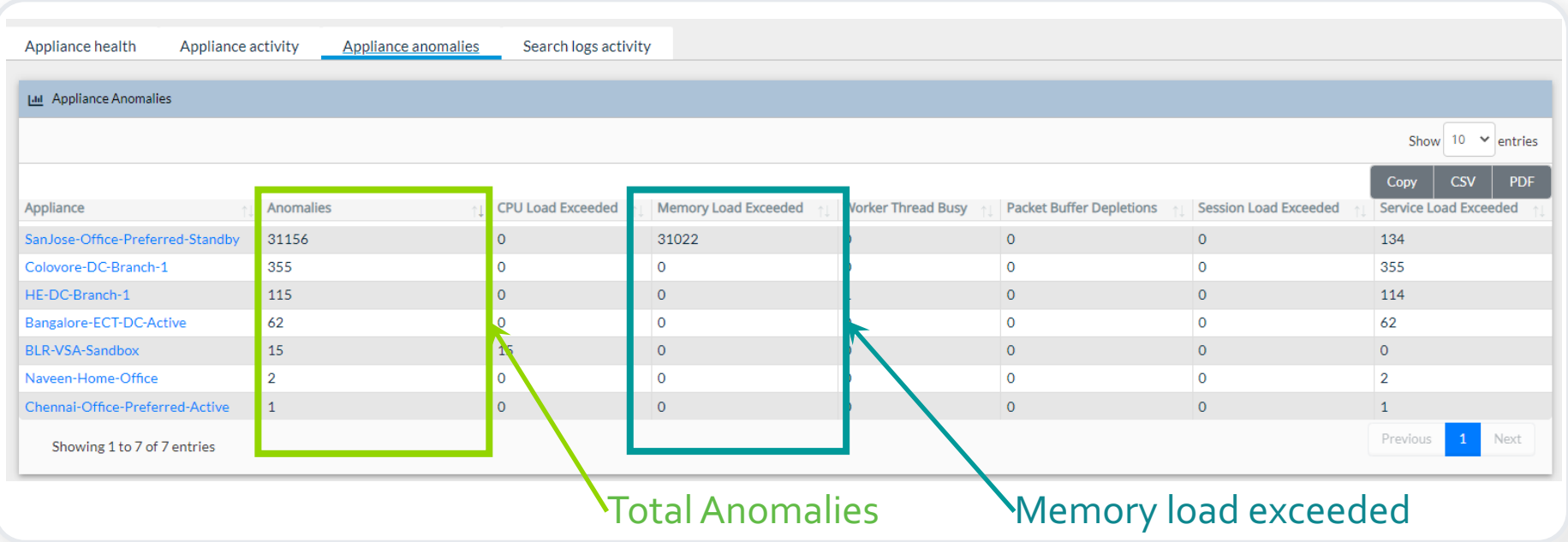
Different deployment scenarios and topologies





Find Anomalies

Monitor for unusual events



- Max session exceeded
- CPU load exceed
- Memory load exceed
- Packet buffer depletion
- Worker thread busy

- User generating a high number of traffic flows
  - Restrict max session per user using DDOS
- User using majority of network bandwidth
  - Restrict max bandwidth per user using per user policer

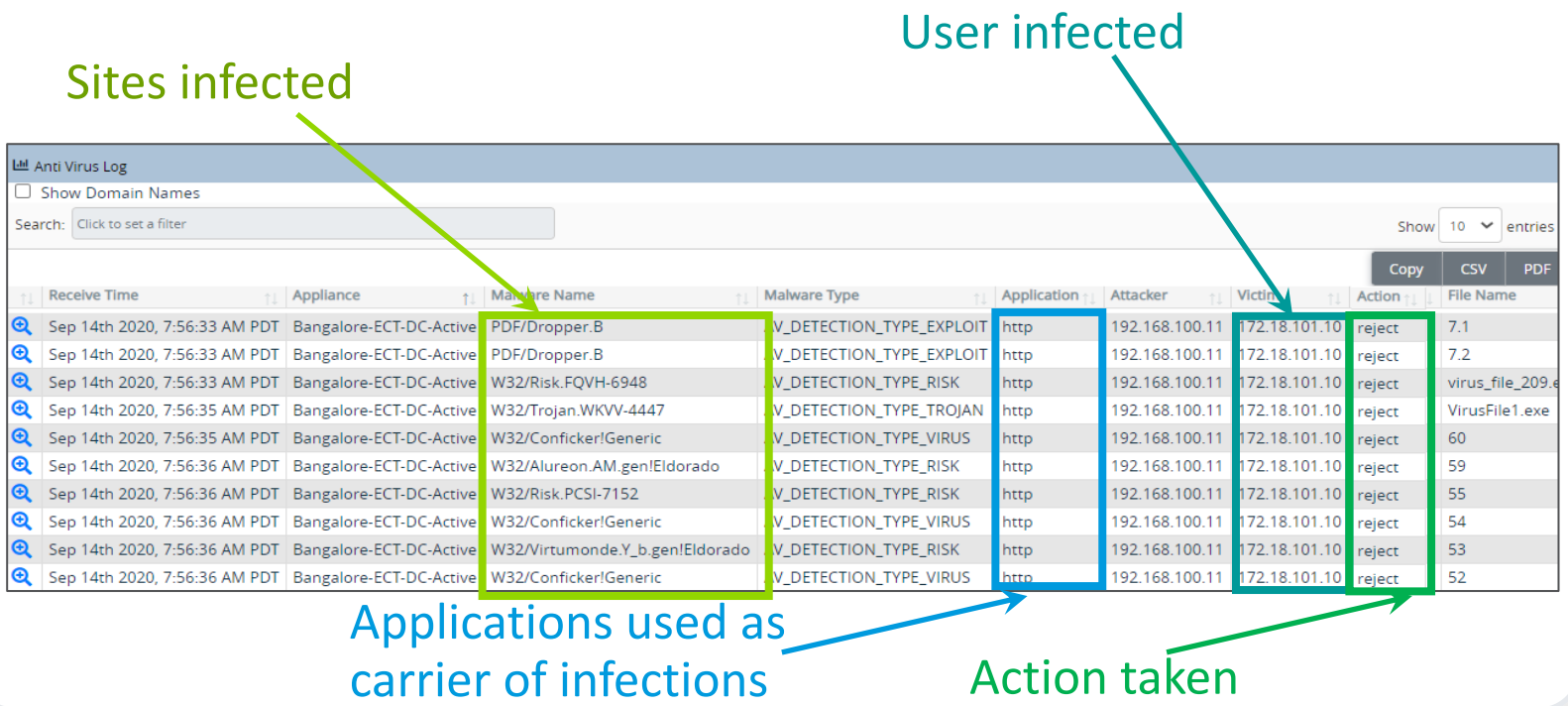
- Don't struggle endlessly if there are basic issues in your network such as duplicate IP in WAN and LAN, monitor alarms in Analytics

VERSA

Find Anomalies

Monitor for unusual user activities

Monitor UTM threat events on Analytics to find the following malware, spyware, and ransomware



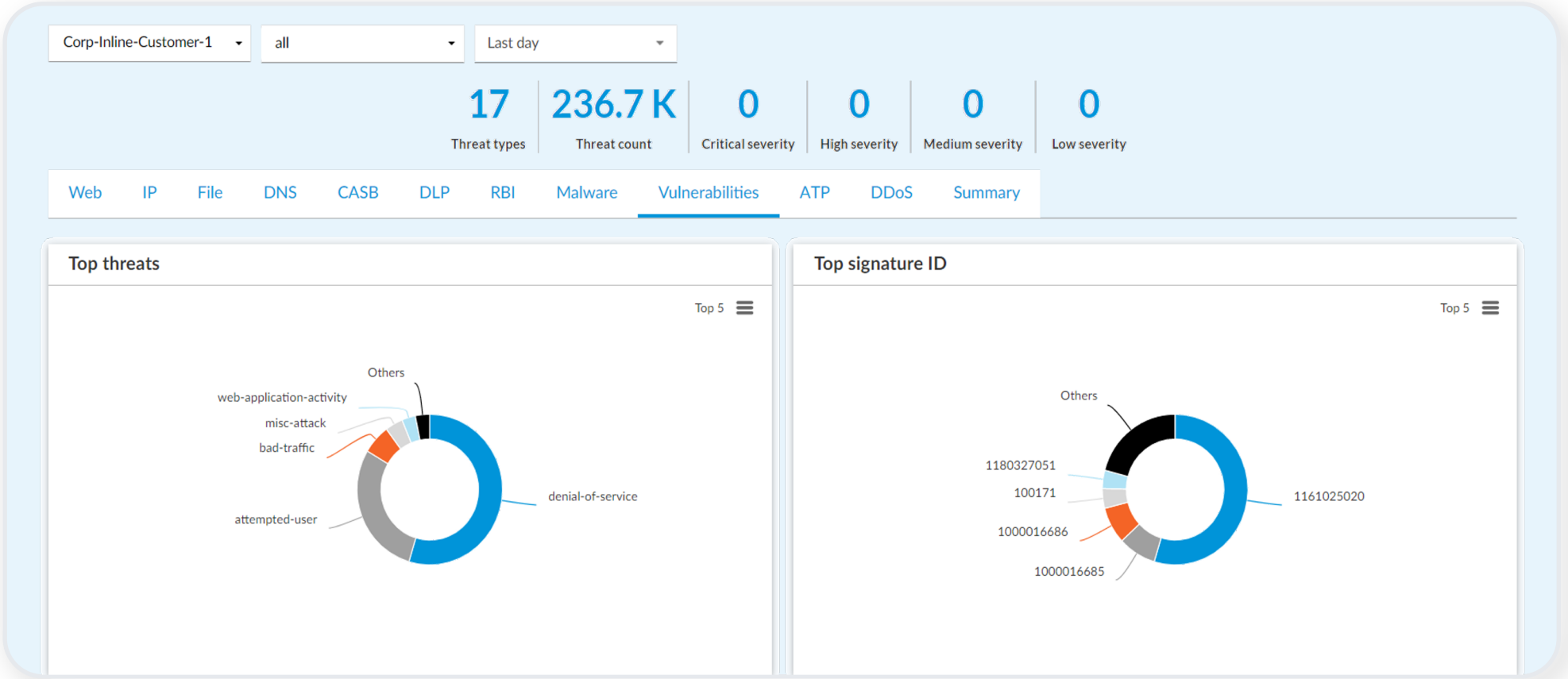
- Users accessing content with malware
- Users accessing content which is potentially malicious
- Users accessing URLs which are not compliant with organization policies
- Users accessing sites which are categorized as Phishing, Proxy, Exploits, etc.

VERSA

Find Anomalies in the Whole Network

Vulnerabilities

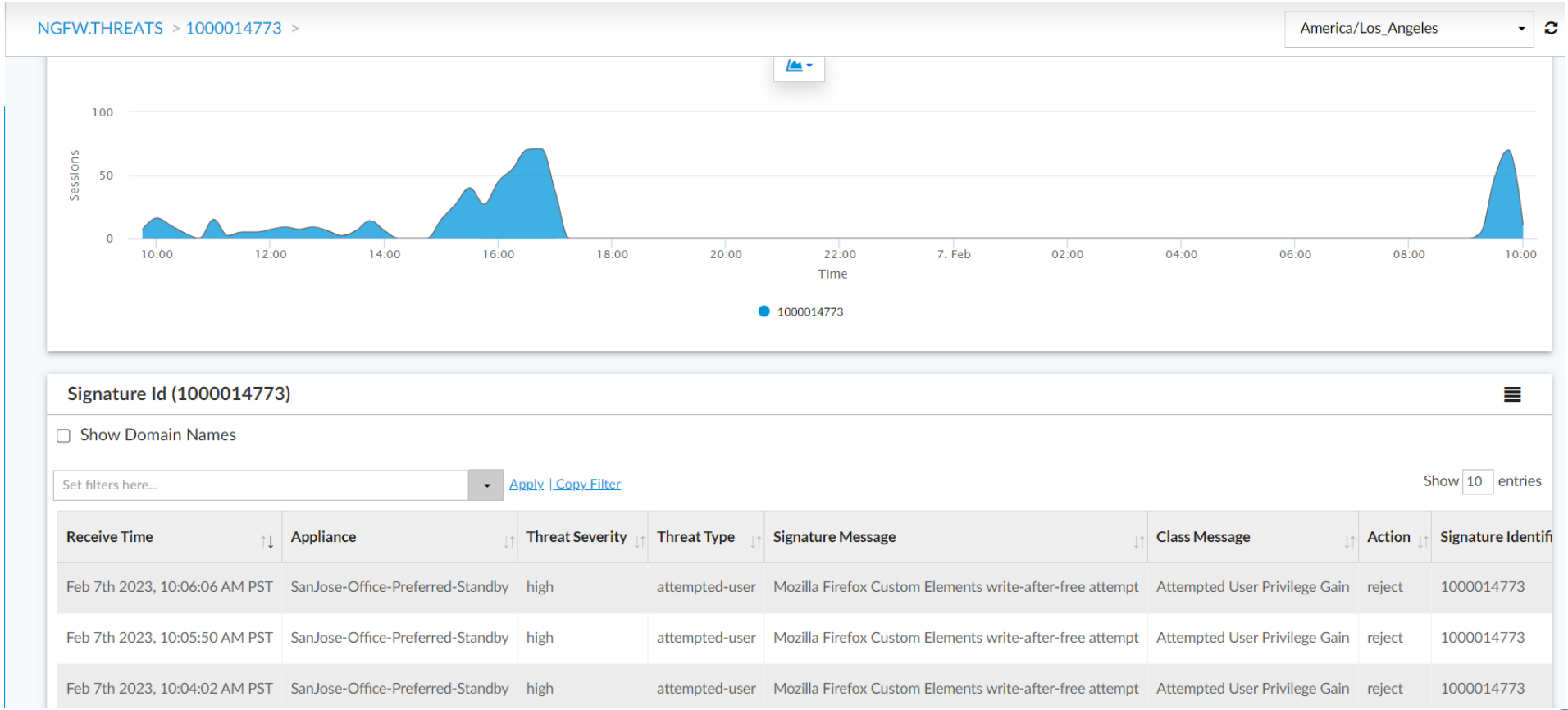
- Find users accessing apps or servers with vulnerabilities



Find Anomalies in the Whole Network

Vulnerabilities Continued

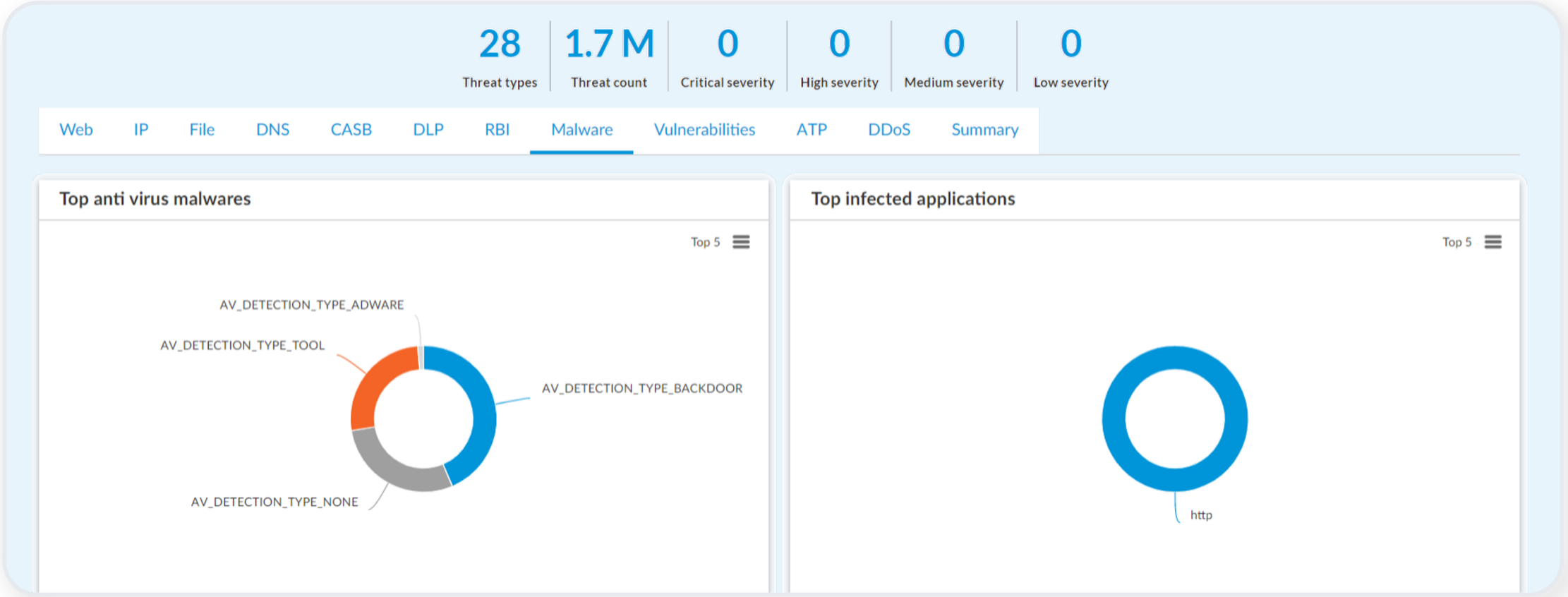
- Find users accessing apps or servers with vulnerabilities



Find Anomalies in the Network

Malwares

- Find users accessing sites or resources which have malwares



Find Anomalies in the Network

Malwares Continued

- Find users accessing sites or resources which has malwares

Anti virus log (Bangalore-New-DC-Active)

Show Domain Names

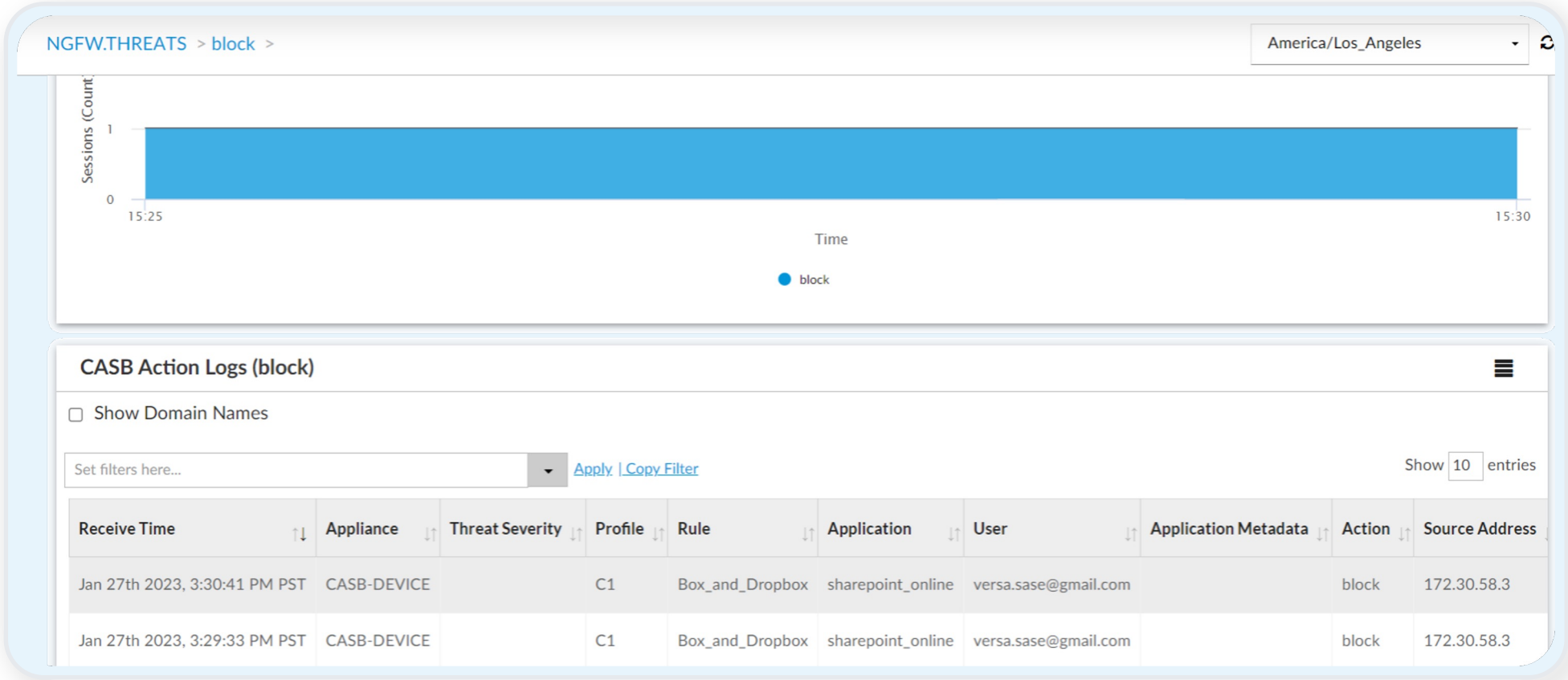
Set filters here... Apply | Copy Filter Show 10 entries

Receive Time	Appliance	Threat Severity	Malware Name	Malware Type	Application	User	Attacker	Victim	File Type	File Name
Jan 22nd 2023, 10:40:31 PM PST	Bangalore-New-DC-Active	critical	Archive Bomb	AV_DETECTION_TYPE_BACKDOOR	http	Unknown	23.201.220.95	10.145.0.31	exe	SecurityScan_Release.exe
Jan 22nd 2023, 10:39:59 PM PST	Bangalore-New-DC-Active	critical	Archive Bomb	AV_DETECTION_TYPE_BACKDOOR	http	Unknown	23.201.220.95	10.145.0.31	exe	SecurityScan_Release.exe
Jan 22nd 2023, 10:40:15 PM PST	Bangalore-New-DC-Active	critical	Archive Bomb	AV_DETECTION_TYPE_BACKDOOR	http	Unknown	23.201.220.95	10.145.0.31	exe	SecurityScan_Release.exe
Jan 22nd 2023, 10:38:00 PM PST	Bangalore-New-DC-Active	critical	Archive Bomb	AV_DETECTION_TYPE_BACKDOOR	http	Unknown	23.201.220.95	10.145.0.31	exe	SecurityScan_Release.exe
Jan 20th 2023, 6:08:52 AM PST	Bangalore-New-DC-Active	critical	Archive Bomb	AV_DETECTION_TYPE_BACKDOOR	http	Unknown	10.210.47.11	10.192.209.174	Unknown	sha256:8679e4648d480fa7fd5e
Jan 20th 2023, 6:01:40 AM PST	Bangalore-New-DC-Active	critical	Archive Bomb	AV_DETECTION_TYPE_BACKDOOR	http	Unknown	10.210.47.11	10.192.209.174	Unknown	sha256:8679e4648d480fa7fd5e
Jan 20th 2023, 6:01:34 AM PST	Bangalore-New-DC-Active	critical	Archive Bomb	AV_DETECTION_TYPE_BACKDOOR	http	Unknown	10.210.47.11	10.192.209.174	Unknown	sha256:582fb99abc61b81c30ff4
Jan 23rd 2023, 2:40:47 AM PST	Bangalore-New-DC-Active	critical	Archive Bomb	AV_DETECTION_TYPE_BACKDOOR	http	Unknown	10.210.47.11	10.192.105.2	Unknown	sha256:582fb99abc61b81c30ff4
Jan 23rd 2023, 2:40:49 AM PST	Bangalore-New-DC-Active	critical	Archive Bomb	AV_DETECTION_TYPE_BACKDOOR	http	Unknown	10.210.47.11	10.192.105.2	Unknown	sha256:8679e4648d480fa7fd5e

Find Anomalies in the Network

Restricted Apps or Sites

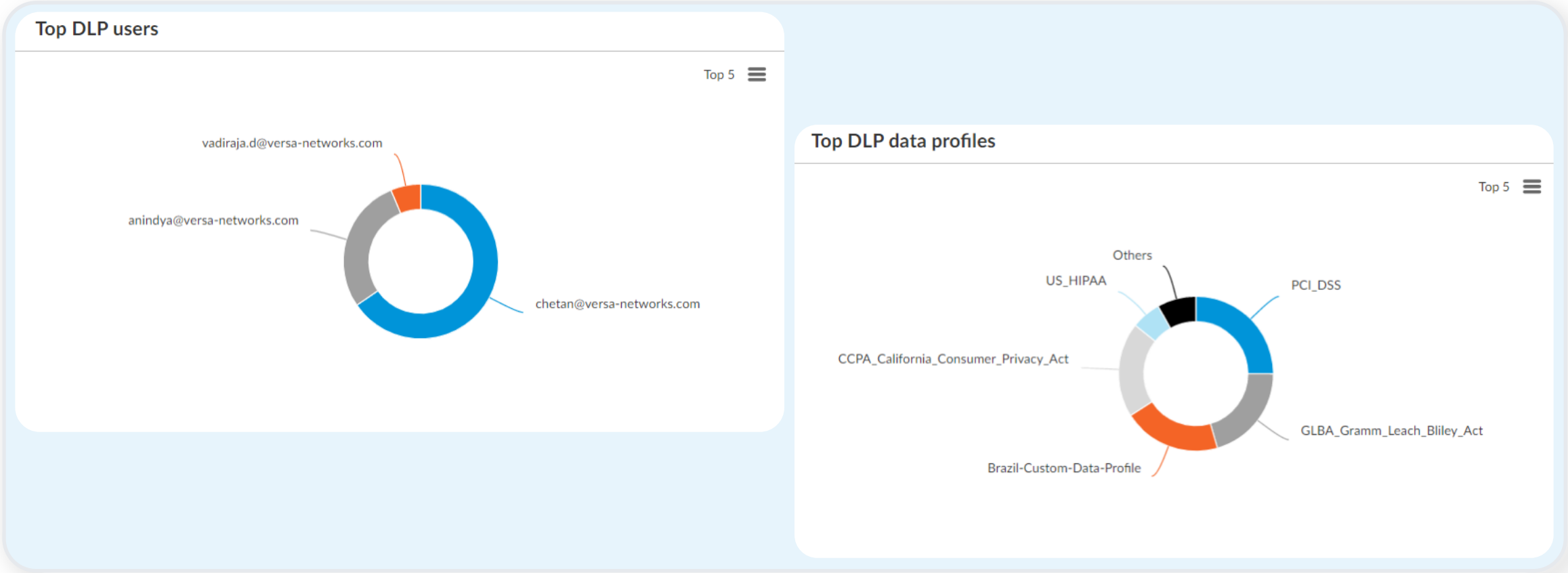
- Find users accessing restricted sites or apps



Find Anomalies in the Network

Leaking Sensitive Information

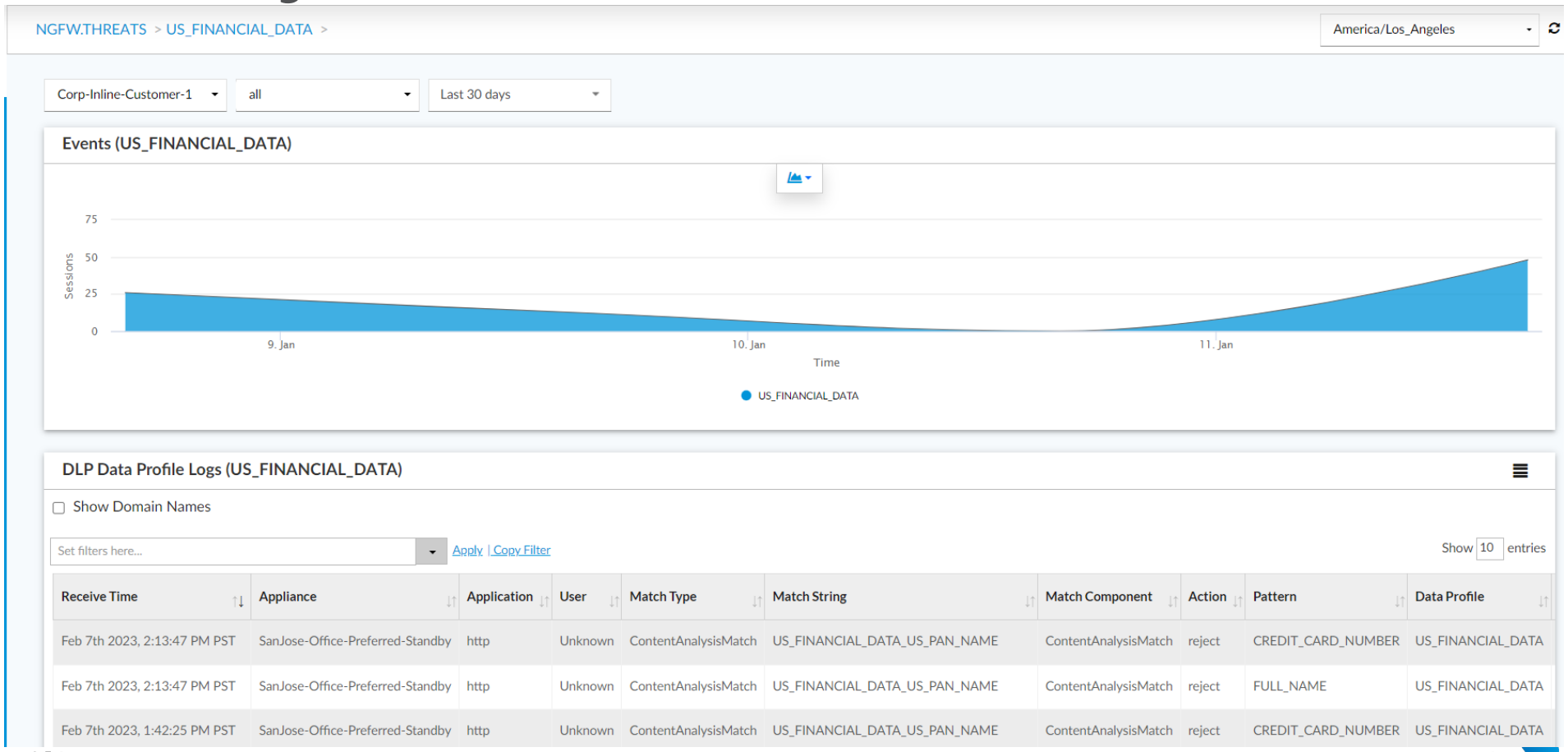
- Find users leaking sensitive information



Find Anomalies in the Network

Leaking Sensitive Information Continued

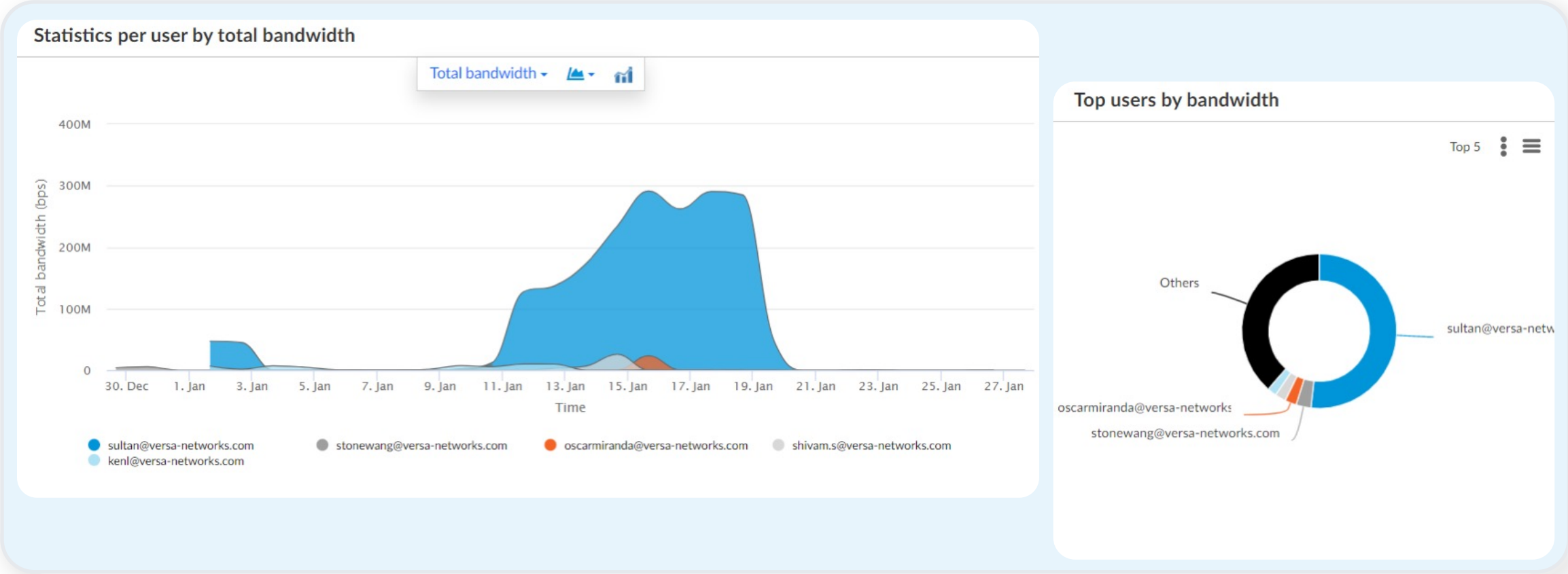
- Find users leaking sensitive information



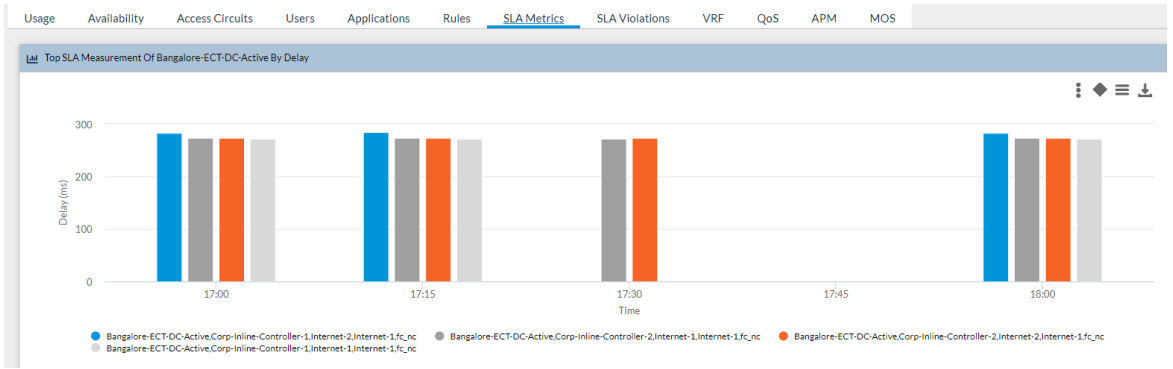
Find Anomalies in the Network

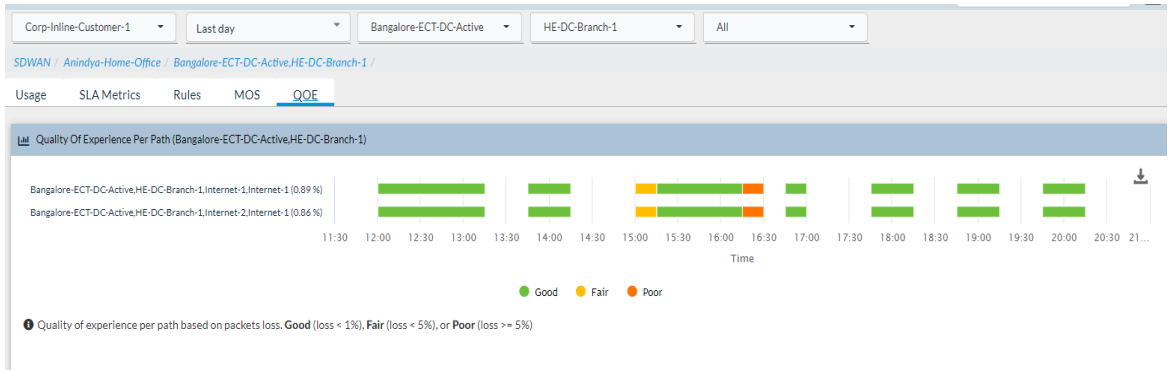
Over Utilizing Resources

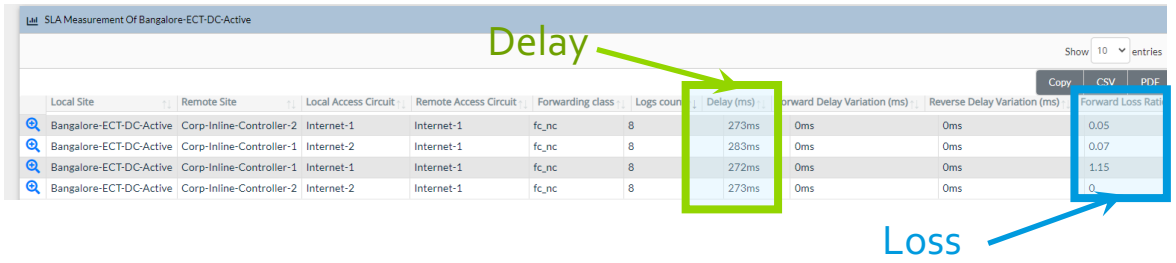
- Find users over utilizing network bandwidth

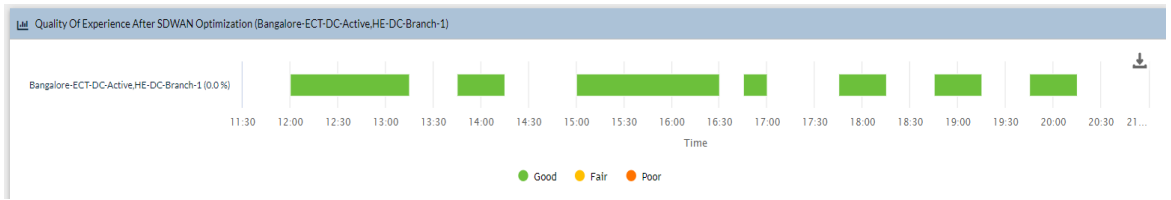


Monitor Network Performance









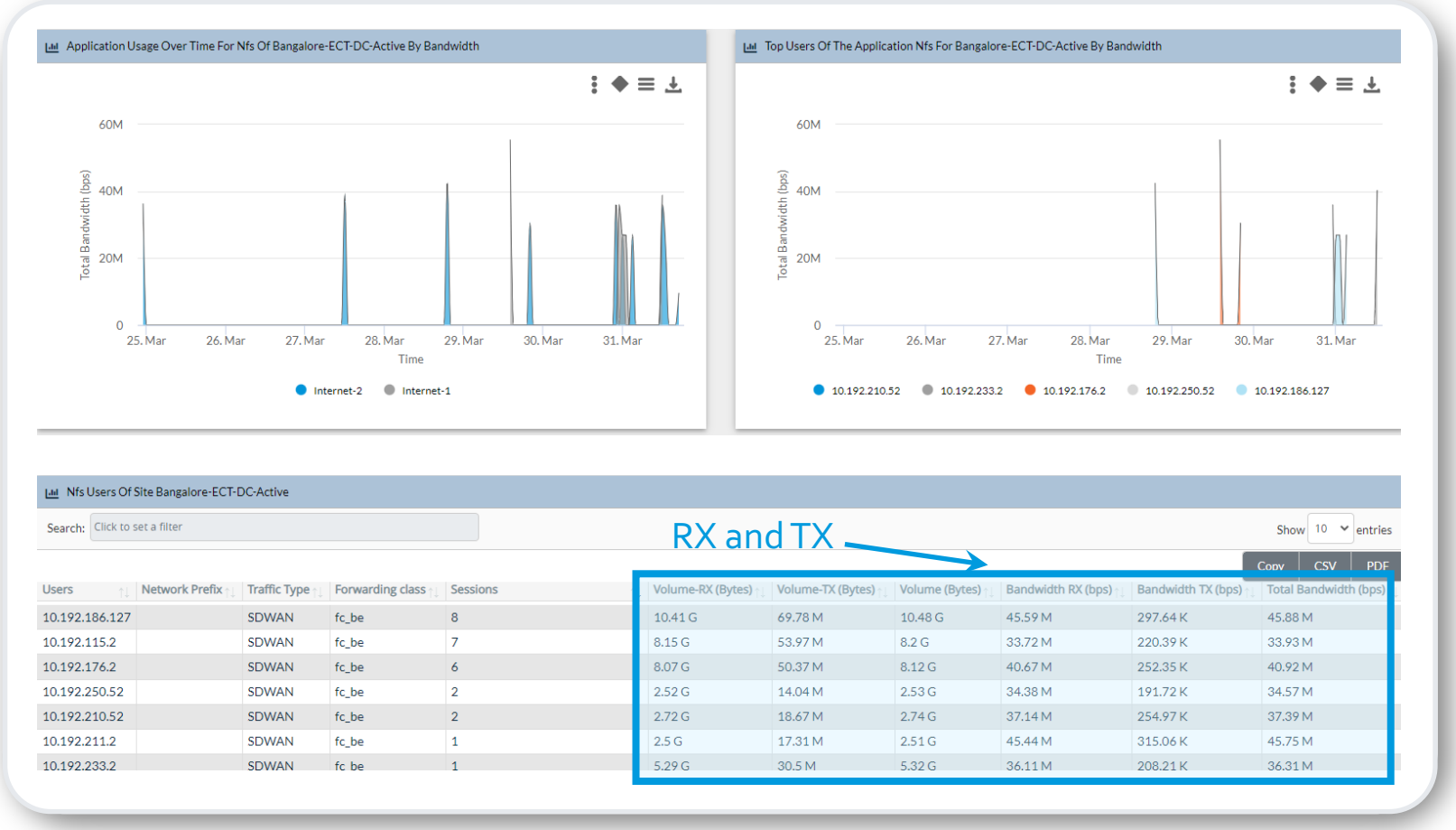
- Packet loss on underlay paths
- Latency and jitter on underlay paths
- Complete black out of underlay paths
- Quality of Experience (QoE)

Versatility 2024

VERSA

Monitor Application Performance

Historical Application Performance



VERSA

Monitor Application Performance

If the Network performance is good, Is it server issue or application issue?

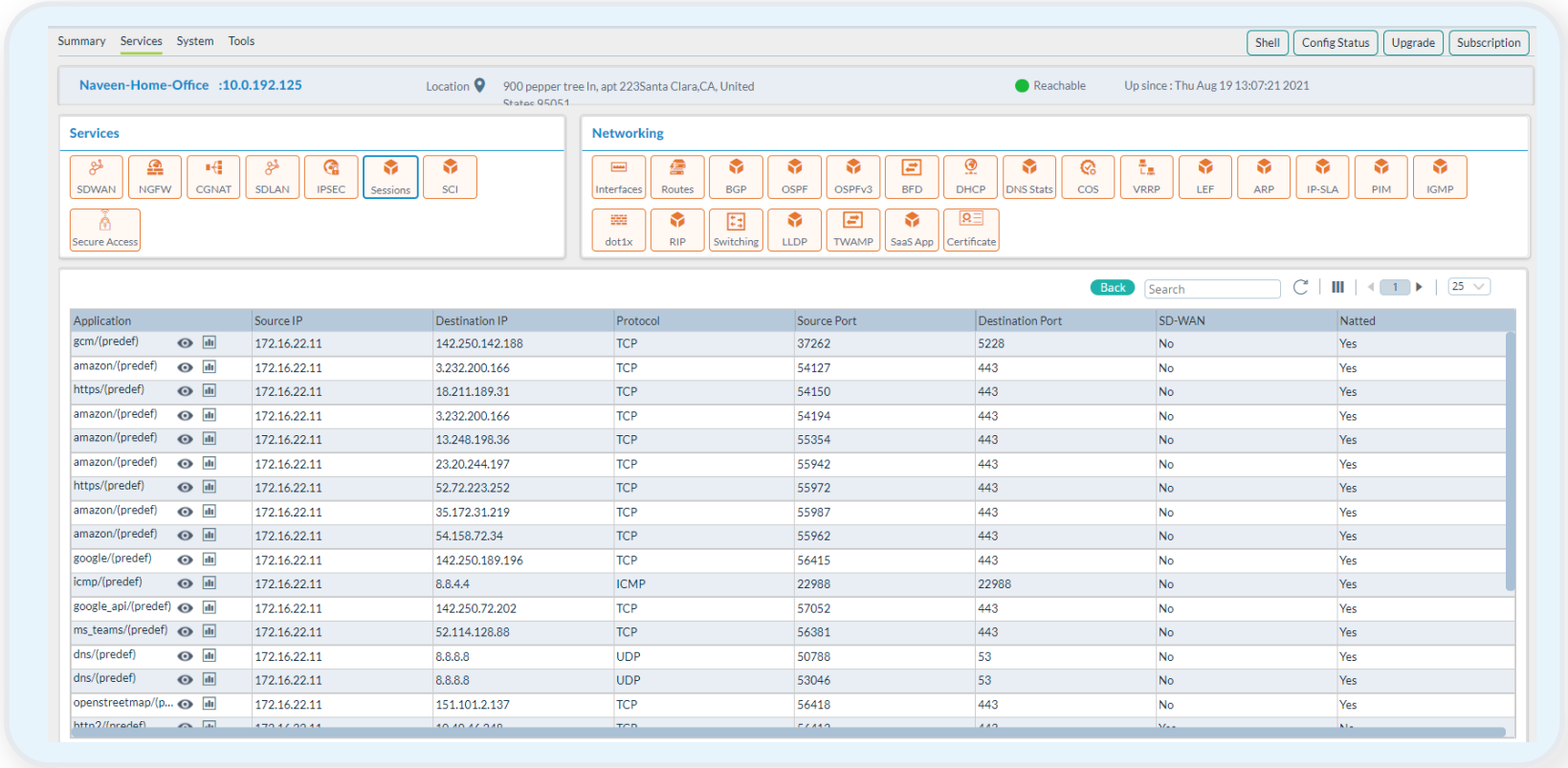
Monitor application historical performance and Versa App rank

Users	Network Prefix	Versa App Rank	Sessions	Network Response Time (ms)	TCP Retransmit Fwd	TCP Retransmit Rev	SAA RTT (usec)	SSA RTT (usec)	TCP Packets Fwd	TCP Packets Rev	Syn Retransmiss
10.192.186.3	10.48.0.0/24	99	108	283ms	0.91	2.68	512	282835	110	112	0
10.192.211.2	10.48.0.0/24	99	7	244ms	0.05	0.08	2063	1287825	1920	1956398	0
10.192.211.203	10.48.0.0/24	99	109	281ms	0	1.8	9654	282884	109	111	1
10.192.186.103	10.48.0.0/24	99	109	282ms	0.91	0.91	638	281671	110	110	0
10.192.186.52	10.48.0.0/24	99	12	285ms	10	0	676	283947	20	18	0
10.192.186.128	10.48.0.0/24	90	129	283ms	0.52	0.52	552	282140	193	193	0
10.192.233.2	10.40.1.0/24	61	6	283ms	0	0.22	301	282664	2105	2190811	0
10.192.176.2	10.48.0.0/24	60	14	285ms	0	0.2	468	284555	6071	6327100	0
10.192.186.127	10.48.0.0/24	58	12	293ms	0	0.18	504	292444	5699	5854288	0
10.192.211.27	10.48.0.0/24	57	5	283ms	0	0.18	262	282419	1931	1958900	0

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

Live Monitoring of Application Performance

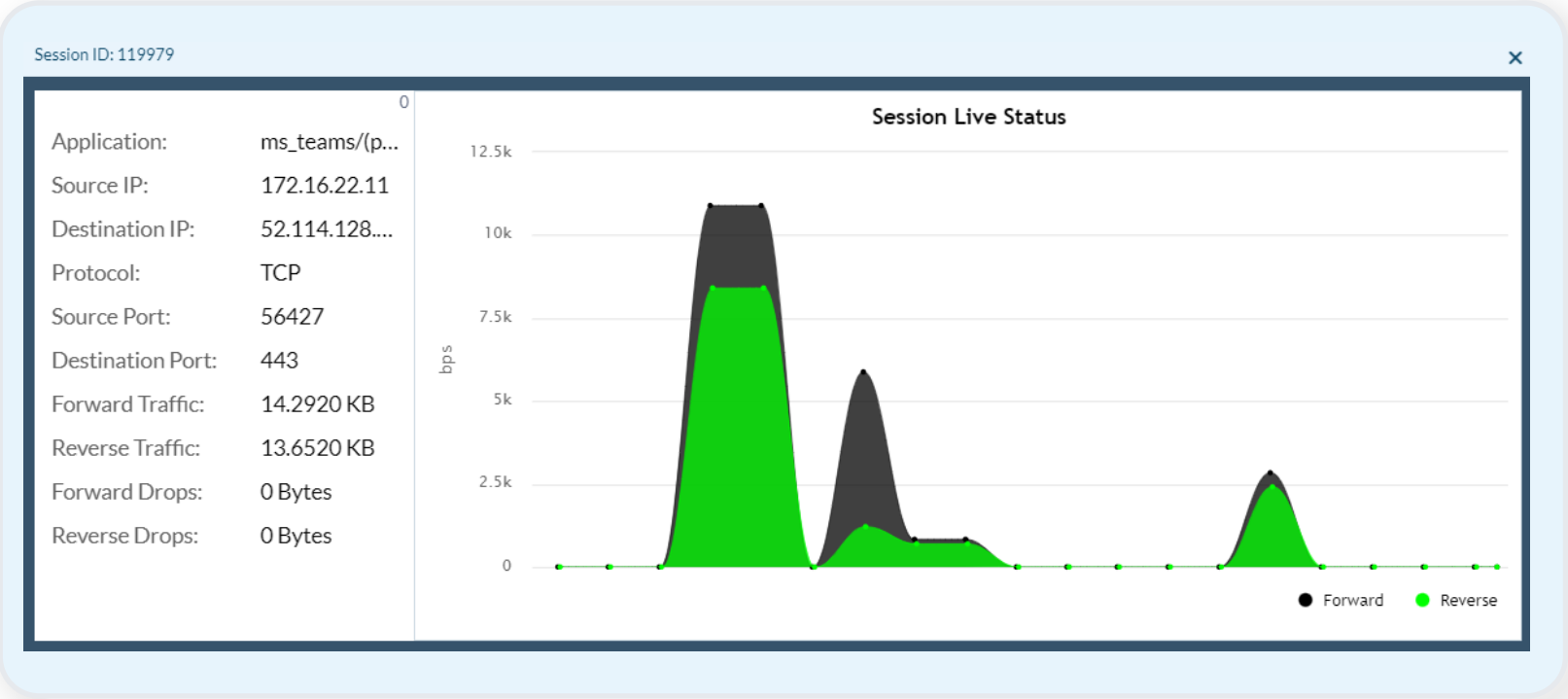
Monitor application performance in real-time



VERSA

Monitor Application Performance

Live Monitoring of MS Teams application



VERSA

Guidelines for External Monitoring Tools

- Do not use basic auth while sending RestAPI requests to director. Use OAuth instead of basic auth.
- Versa recommend to use streaming alarms and events from analytics to your collector and use that data instead of any pull models like API calls to director or SNMP walk
- Limit monitor APIs to lesser than 50 APIs/second to director.

SASE Monitoring Digital Experience Monitoring (DEM)

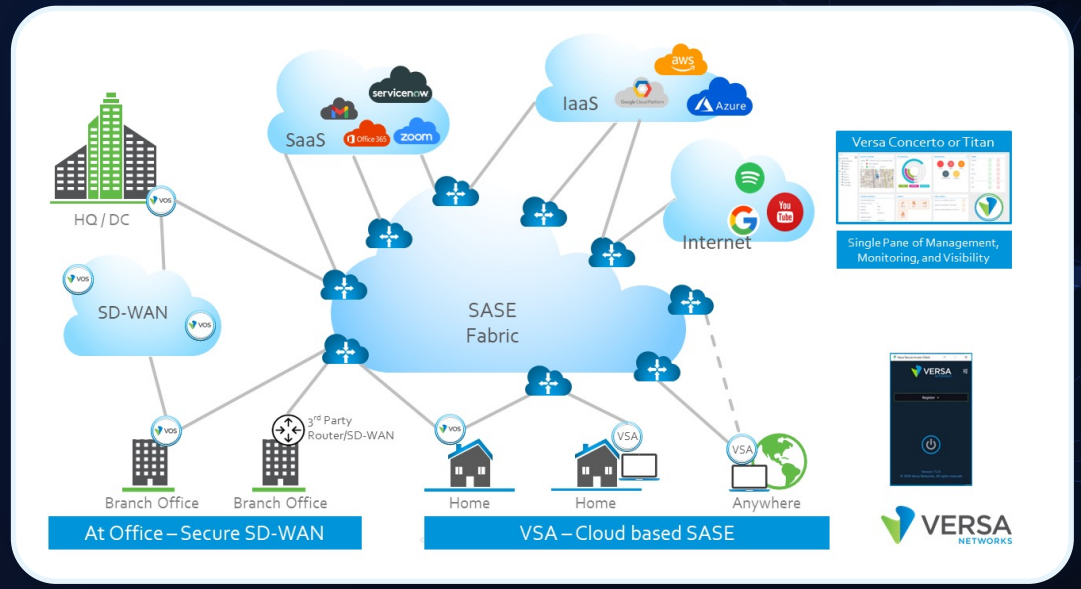
Versatility 2024

VERSA

Digital Experience Monitoring (DEM)

End-to-End Monitoring

- Monitor Customer End Device
- Monitor Customer LAN Network
- Monitor Transport Issues
- Monitor Application Performance
- Monitor Connectivity Between SASE & Customer Network
- Hop by Hop Monitoring



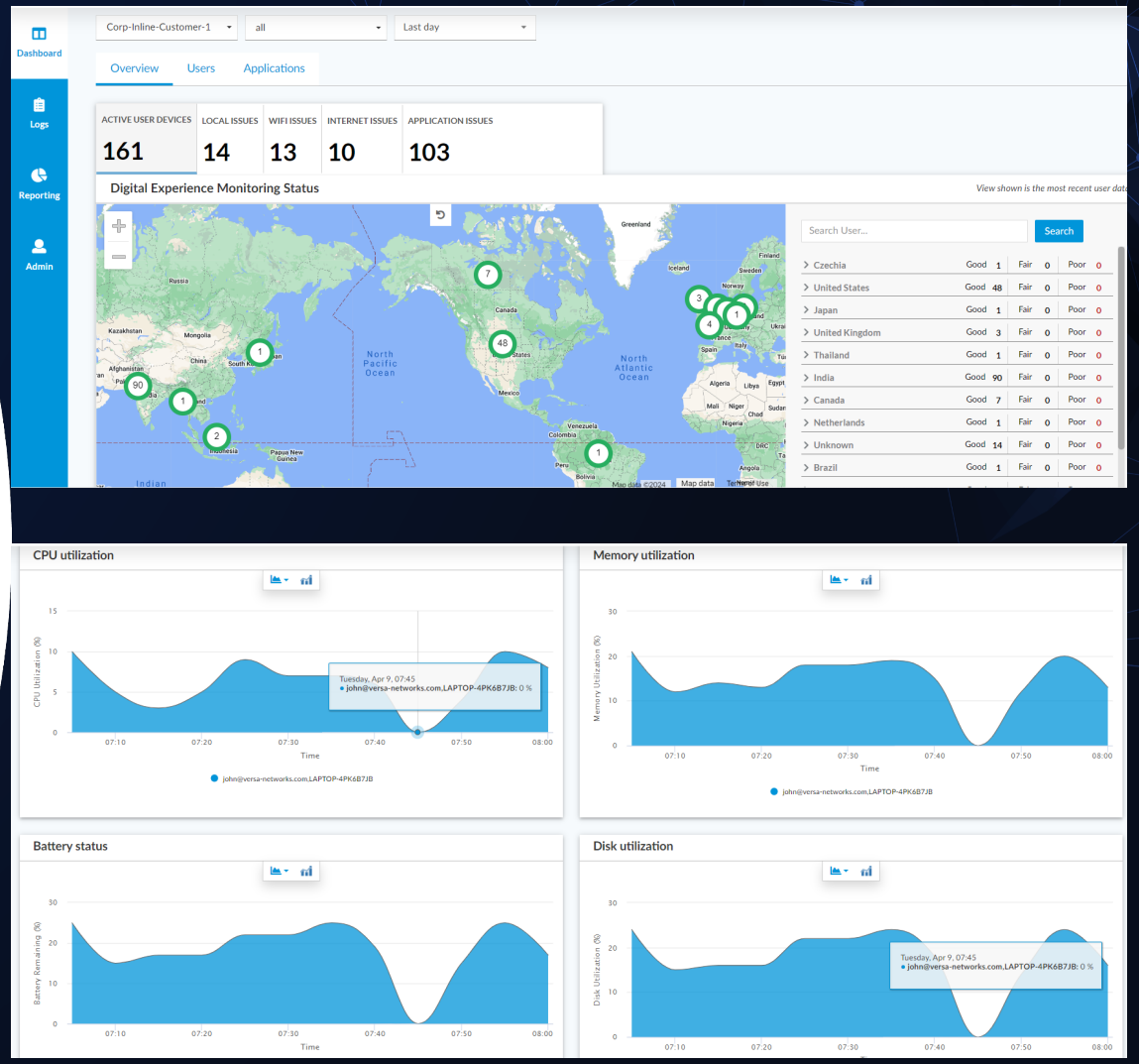
Versatility 2024

VERSA

Digital Experience Monitoring (DEM)

Monitor Customer End Device

- Monitor for High CPU
- Monitor for High Memory
- Monitor for High Disk I/O
- Monitor for Weak WiFi Signals
- Monitor for LTE Signal Strength
- Monitor for Unstable Nexthop Connectivity

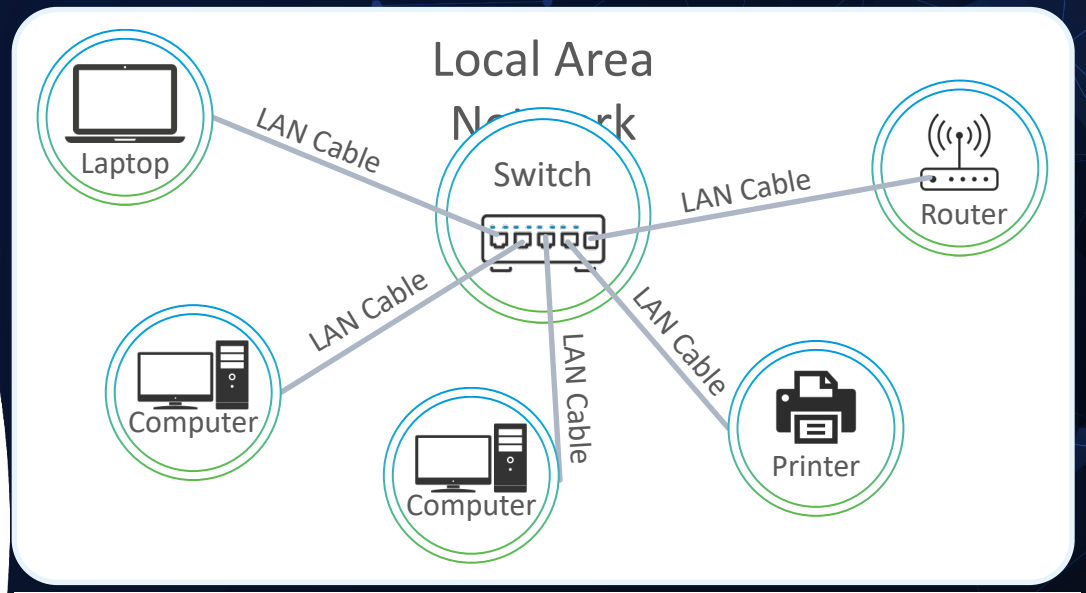


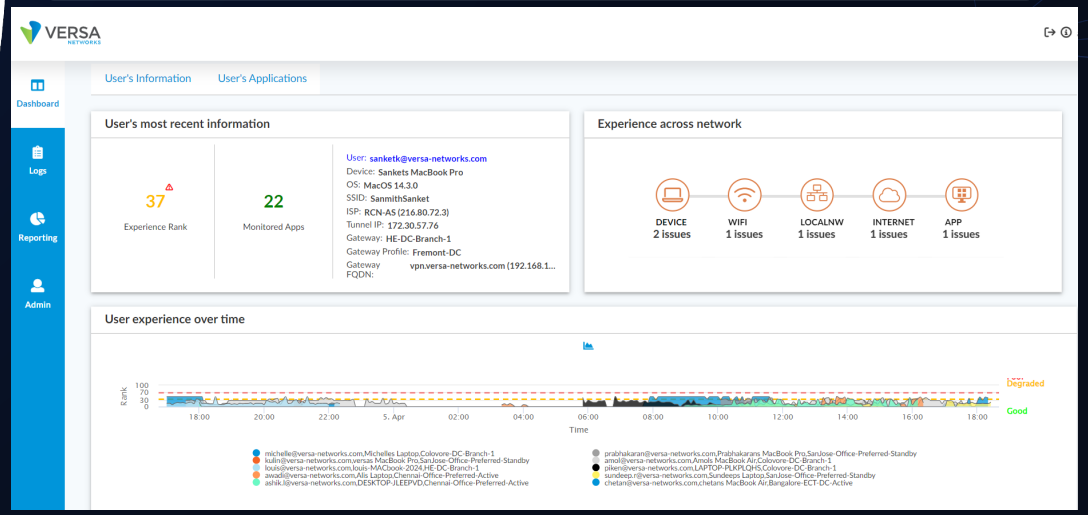
VERSA

Digital Experience Monitoring (DEM)

Monitor Customer LAN Network

- Monitor L2 Loops
- Monitor ARP Issues
  - ARP Flood, ARP Not Resolved, etc.
- Monitor for Routing Issues
  - Routing Missing, Route Loops
- Monitor for Duplicate IPS
- Monitor for Bandwidth Issues
- Monitor for Latency Issues
- Monitor for Duplicate DHCP Server Issues





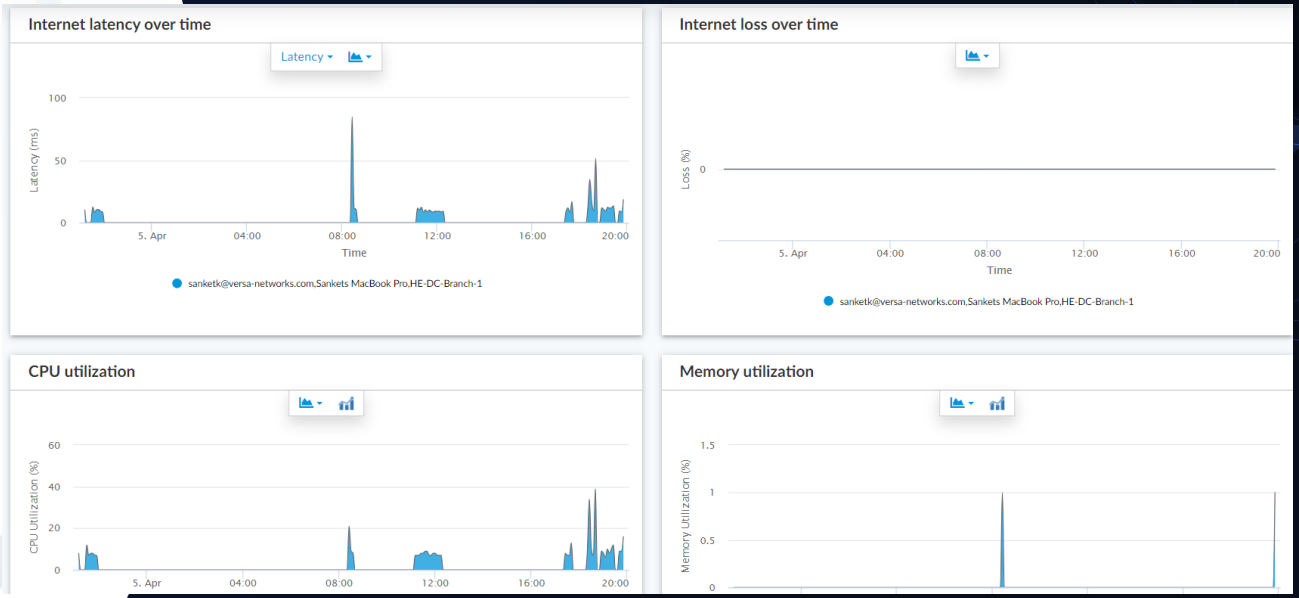
Versatility 2024

VERSA

Digital Experience Monitoring (DEM)

Monitor Transport Issues

- Monitor Packet Loss on Transport/WAN
- Monitor Latency and Jitter on Transport/WAN
- Monitor Bandwidth

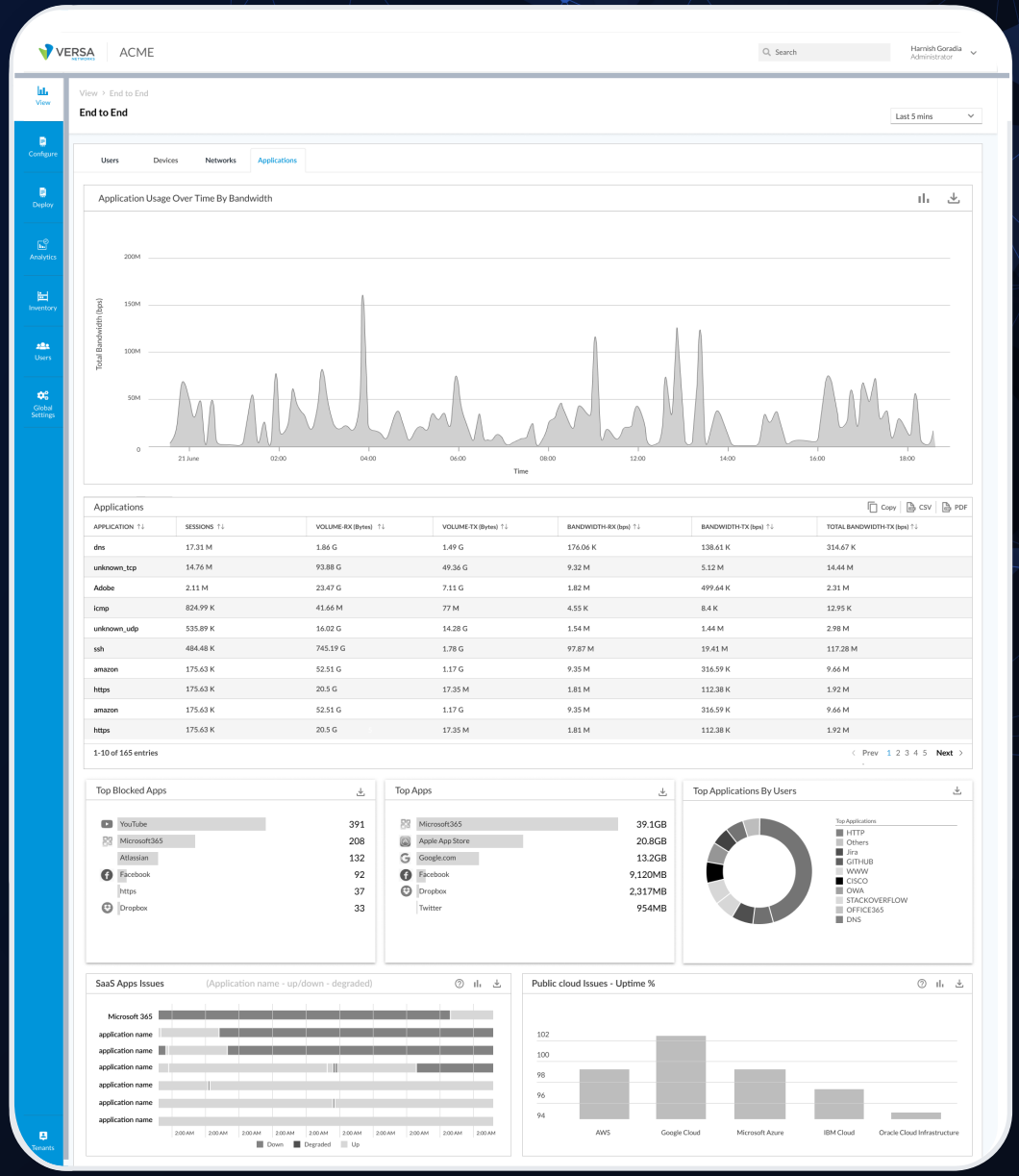


VERSA

Digital Experience Monitoring (DEM)

Monitor Application Performance

- Monitor Network Response Time
- Monitor Re-Transmissions
- Monitor Connections Aborted, Refused
- Monitor Passive Bandwidth Usage of Applications and Come Up With Score
- Monitor for Outages in SaaS Applications like Office365, Salesforce, etc.
- Monitor for Outages in Public Clouds like AWS, Azure, GCP, etc. based on where the user apps are located



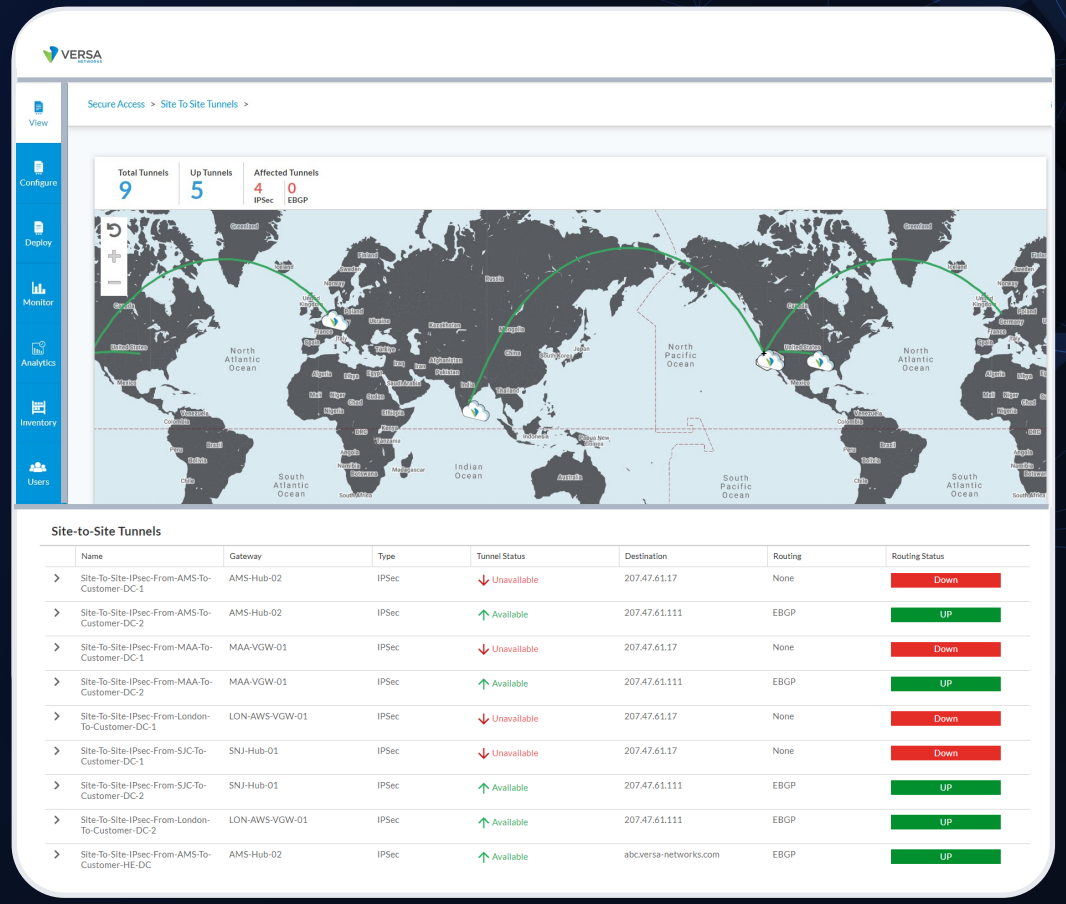
Versatility 2024

VERSA

Digital Experience Monitoring (DEM)

Monitor Connectivity between SASE & Customer Network

- Monitor IPsec/GRE/SD-WAN Tunnel
- Monitor Dynamic Routing Protocols within Tunnels



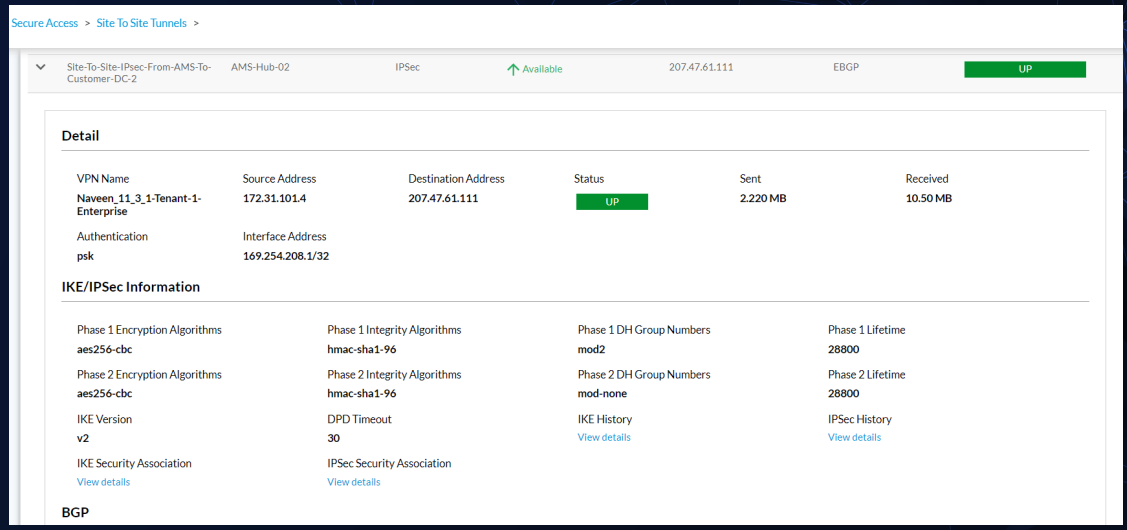
Versatility 2024

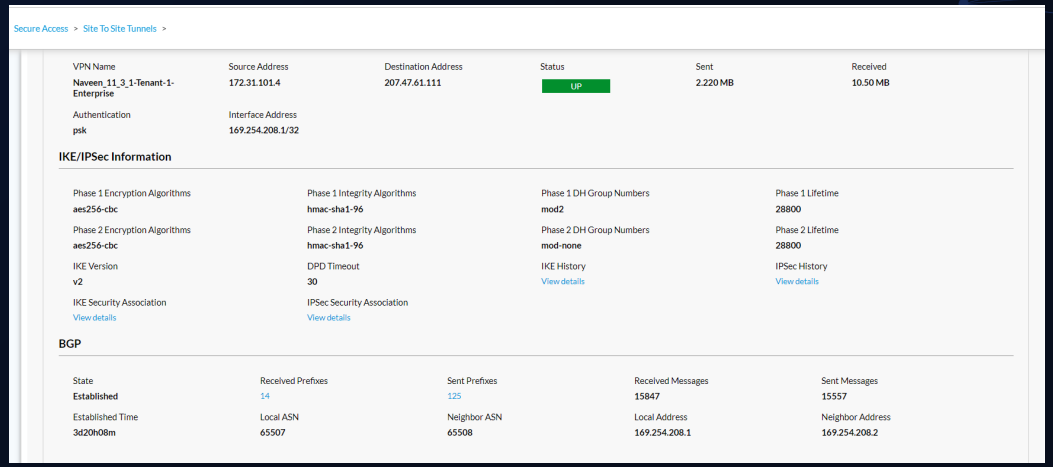
VERSA

Digital Experience Monitoring (DEM)

Monitor Connectivity between SASE & Customer Network Continued

- Monitor IPsec/GRE/SD-WAN Tunnel
- Monitor Dynamic Routing Protocols within Tunnels



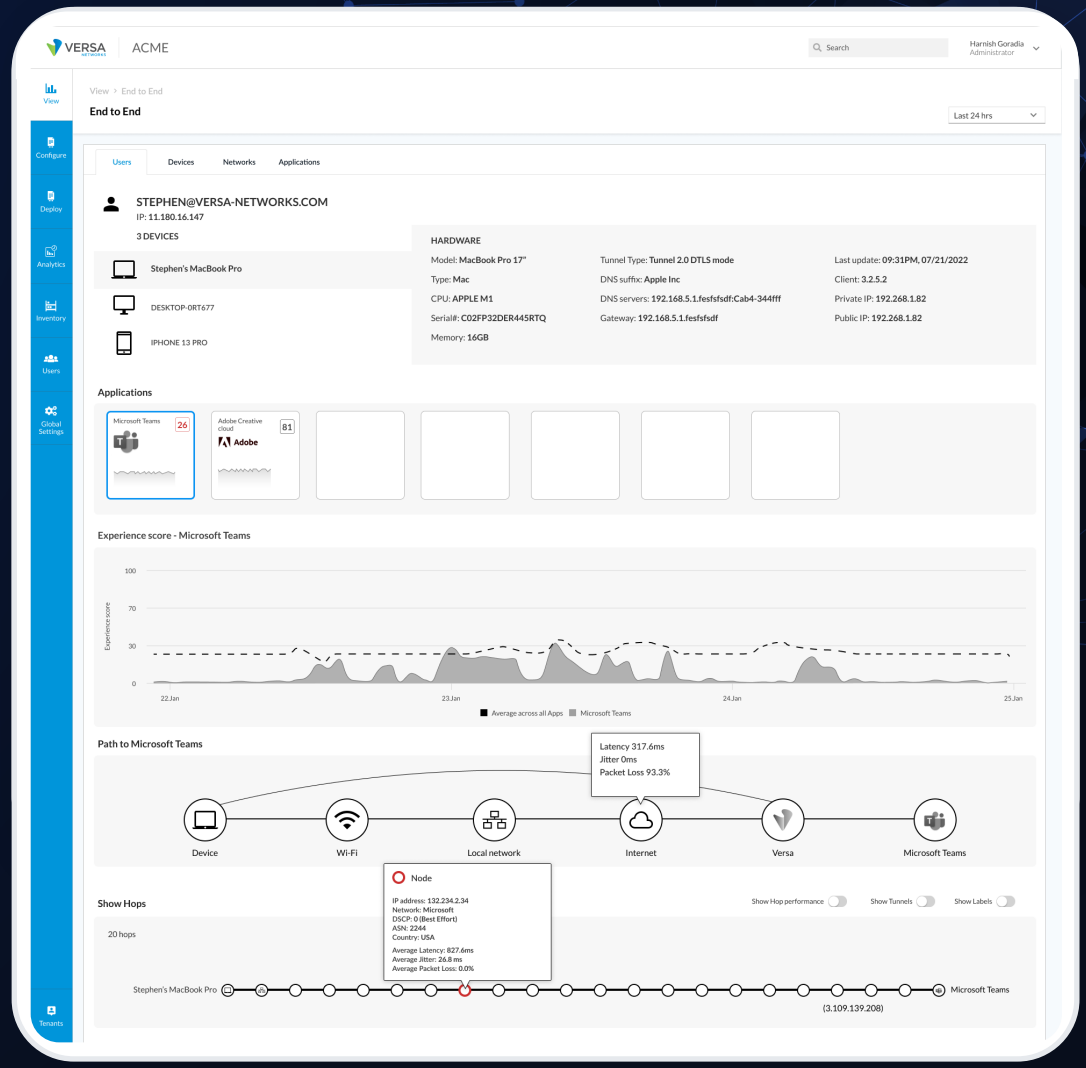


VERSA

Digital Experience Monitoring (DEM)

Hop by Hop Monitoring

- Report latency for every network hop from user device to user app
- Report jitter for every network hop between user device to user app
- Monitor packet loss for every network hop between user device to user app



Versatility 2024

VERSA

Stay Up-to-Date with the Latest Security, OSSpack, and Software

OSSpack released with fixes for vulnerabilities found in Linux open source packages

- Versa uses Ubuntu as base OS for running software.
  Any vulnerabilities discovered in Ubuntu are fixed
  in OSSpack
- Install latest OSSpack

Upgrade to latest Director, Analytics, VOS software

- Upgrade all headend components first
- Upload images to VOS devices prior to actual upgrade day
- Once images are uploaded to VOS devices, individual or group of devices can be upgraded.

SPACK is released frequently with fixes for new security issues discovered

- Enable automatic spack update for VOS devices directly over internet

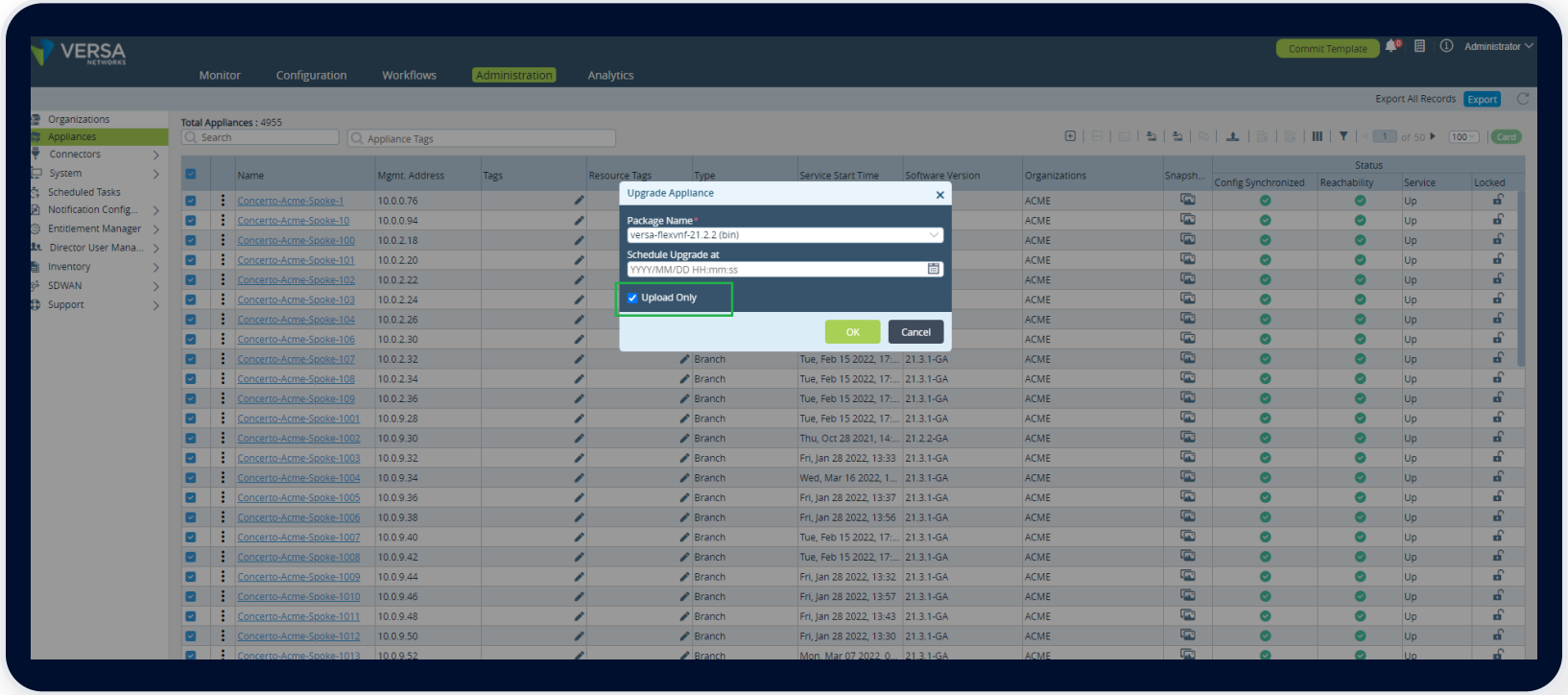
Upgrade to latest based OS (ubuntu)

- Install Versa base OS upgrade orchestrate
- Use Versa orchestrator and upgrade all Versa components

Installing VOS Image on Edge Devices

Upload VOS image in advance

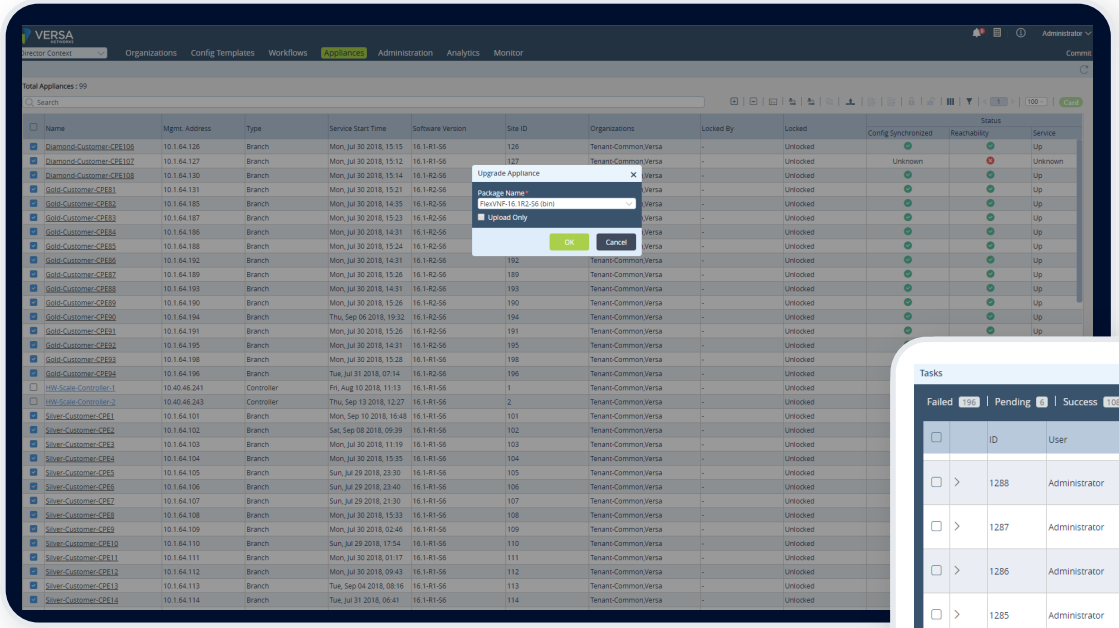
- Restrict the max bandwidth used for image transfer if needed
- Use the link which is not bandwidth sensitive and not carrying customer critical traffic to transfer software image

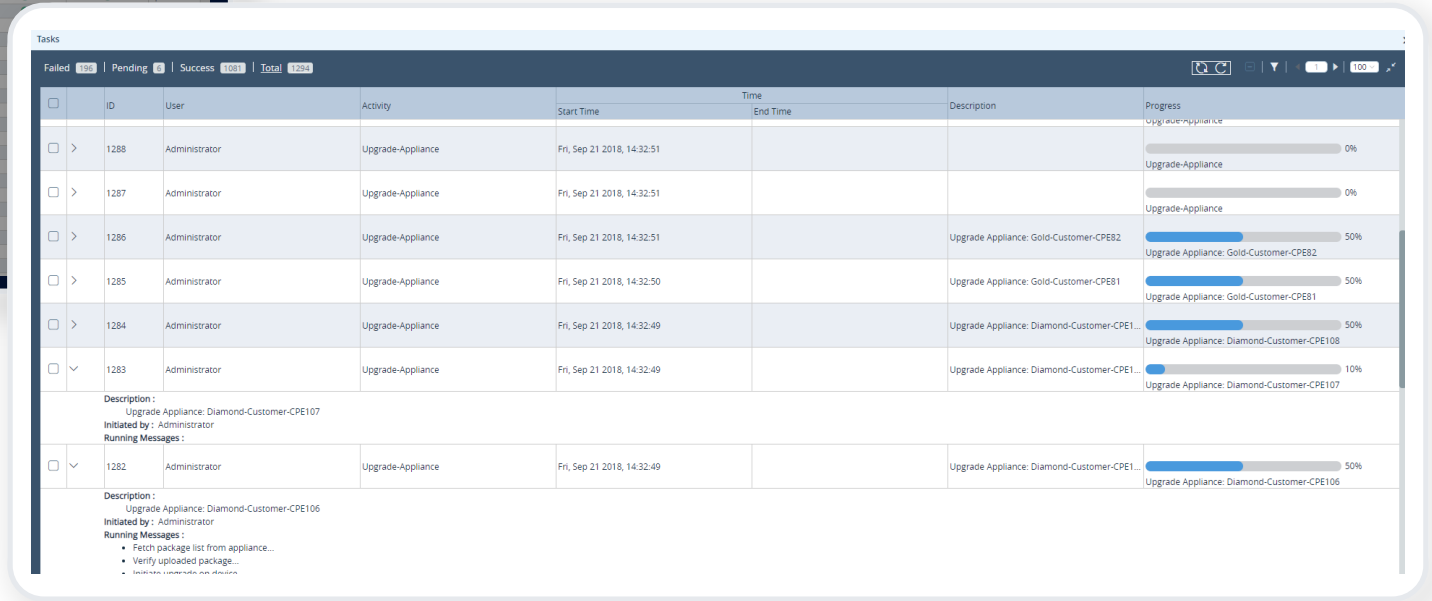


VERSA

Installing VOS Image on Edge Devices

Parallel upgrade of devices from Versa Director





Installing VOS Image on Edge Devices

Parallel upgrade of devices from Versa Director

Below are approximate times to upgrade 2,000 devices assuming 1 Gbps bandwidth between Versa Director and edge devices

Task	Software Upload	Software Upgrade
Task completion Time on a single device	30 seconds	10 minutes
Batch Processing supported (Y or N)	Y	Y
How many devices can be accommodated in a single Batch	10	100
Time Taken to complete all the Tasks per Batch	5 minute	15 minutes
Time taken to complete the Task for~2000 devices	20 hours	4 hour

Disaster Recovery

Plan ahead for any headend or DC failure where a headend is deployed

- Always take snapshots and recovery backups of Versa Director on a regular basis and keep this in a secure location
- Save snapshots of Versa Analytics in a secure location
- Save snapshots of Versa Controllers in a secure location

Restore the Headend components from snapshots

VERSA

Summary

- Run headend components on reliable hardware with stable network connectivity between these headend components
- Large scale networks can be configured efficiently using a few templates and can be easily deployed using APIs
- Secure users, devices and apps using Zero trust network architecture
- Monitor network and security anomalies for unusual symptoms and take corrective actions
- Monitor network for underlay performance issues from Analytics
  - Identify service provider network issues
  - Monitor quality of experience of each underlay paths
- Monitor application performance to understand any suboptimal user experiences
  - Find root cause for suboptimal application performance by looking at APM metrics and taking corrective actions
- Stay up-to-date with the latest security patches using auto updates of spack, osspack images
- Efficiently upgrade your network using bulk upgrade
- Always prepare for disaster recovery by taking periodic backups and then restore from backup
- Versa SD-WAN and SASE allows you to manage network and security with very less resources compared to managing traditional legacy networks

If you need any additional information on achieving operational excellence for your whole network with minimal resources, reach out to **versatility24@versa-networks.com**

Questions

VERSA

Thank you

VERSA