

Versatility 2024

Secure SD-WAN and SASE Operational Excellence



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

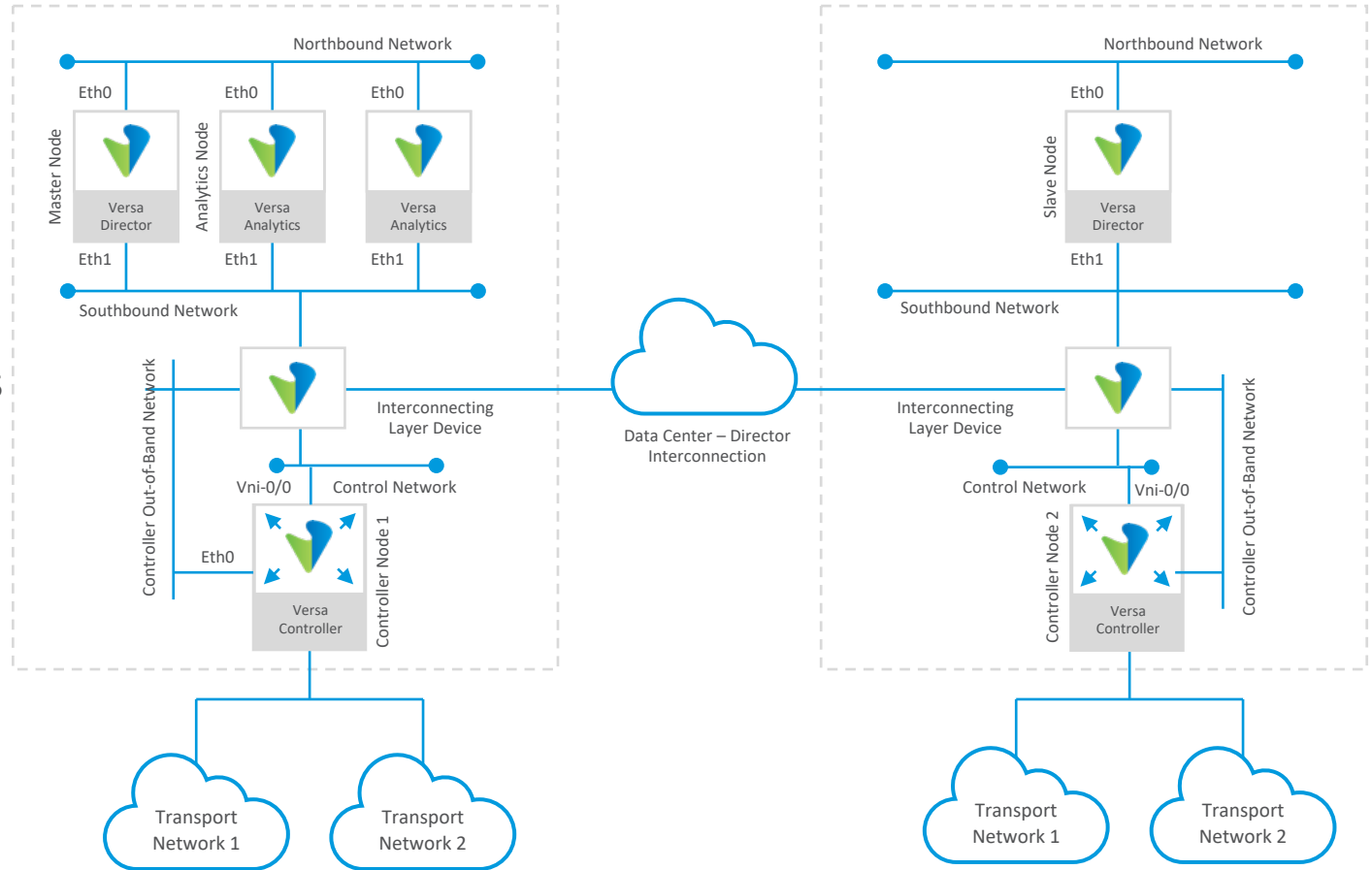


Running on bare-metal vs virtual environments



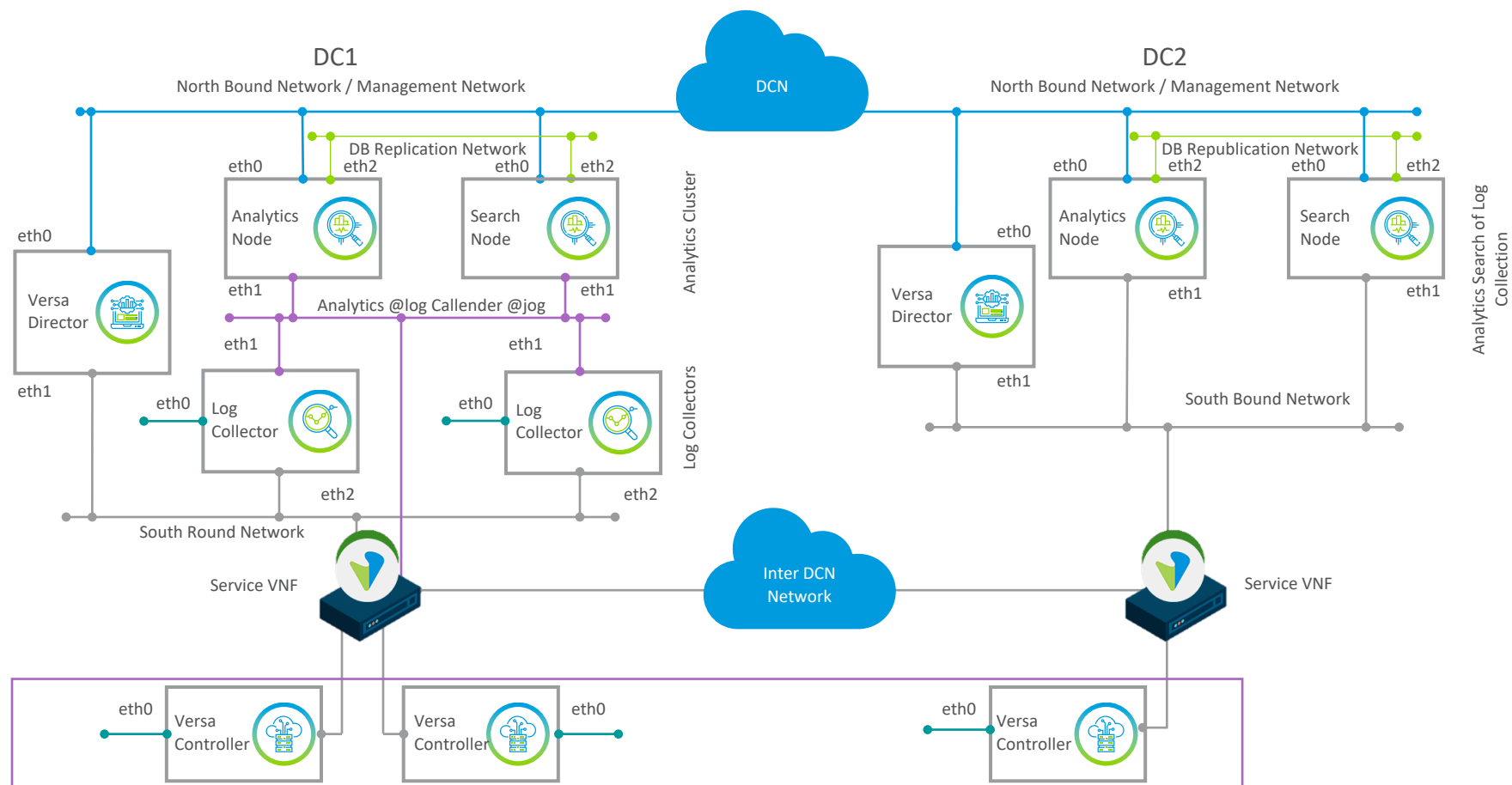
Concerns for running on private virtual cloud

- 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



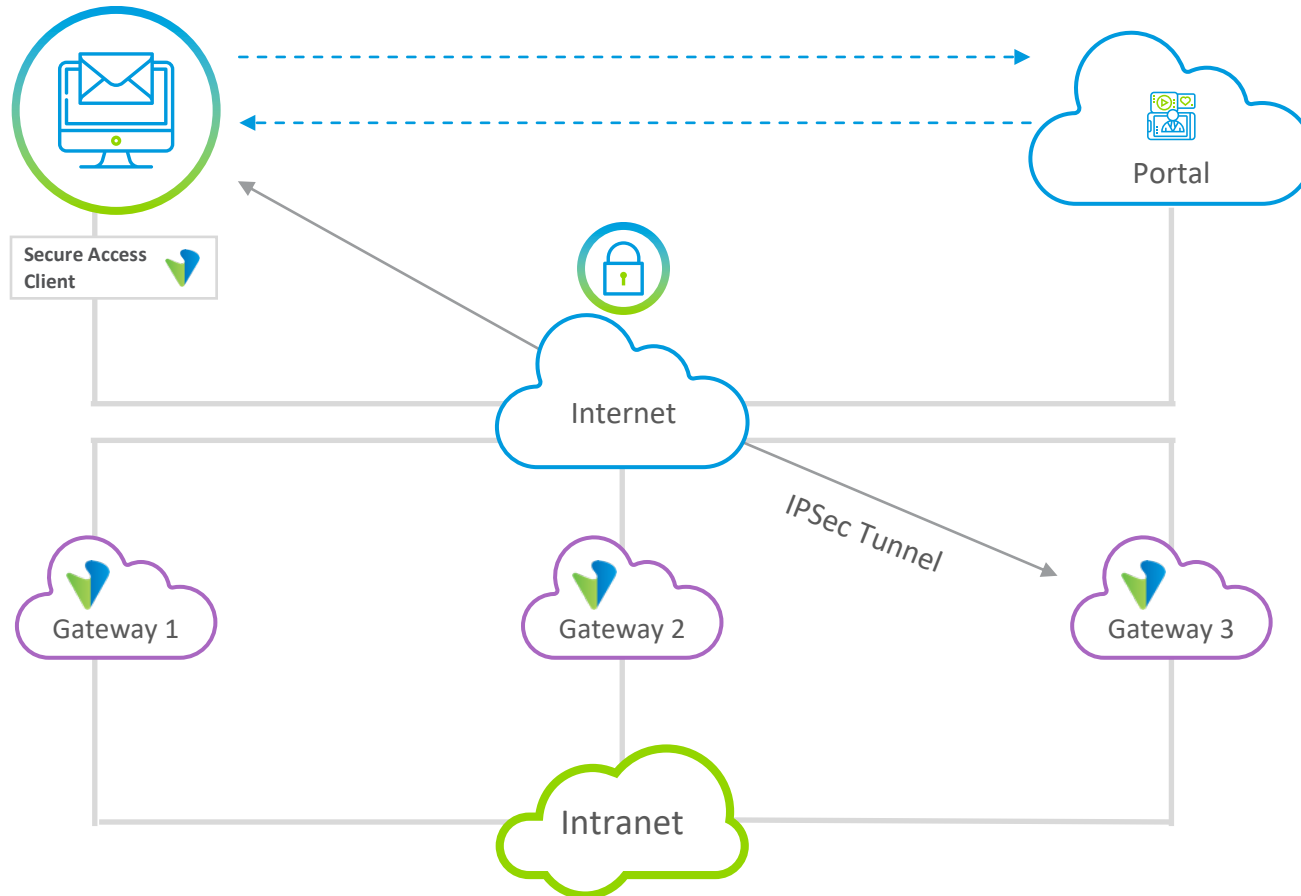
Headend Management

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

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

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](https://docs.versa-networks.com/Solutions/System_Hardening/Perform_Automated_System_Hardening)



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

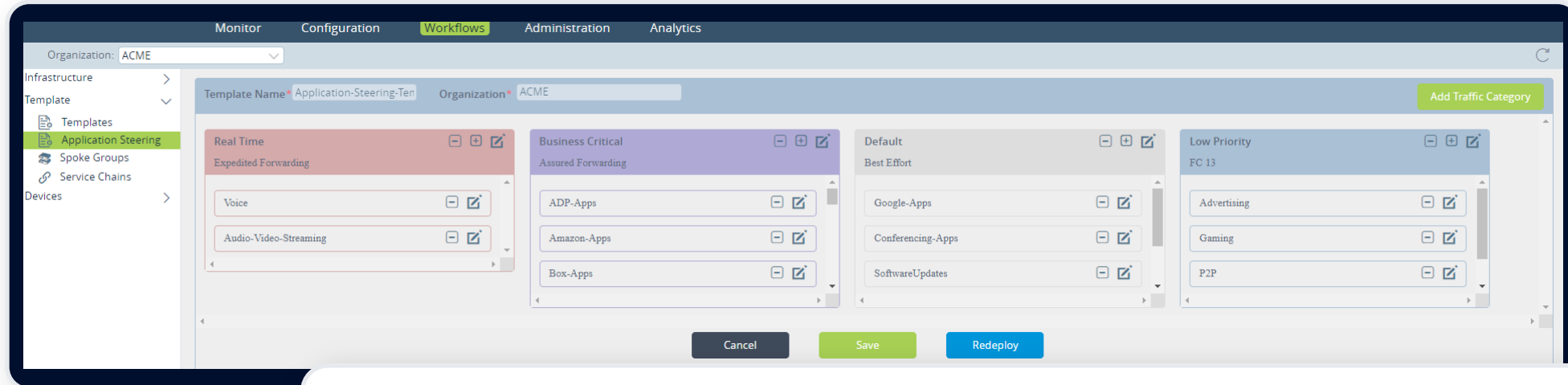
Prioritizing & Applying the Best Path Policies Based on Category of Traffic

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

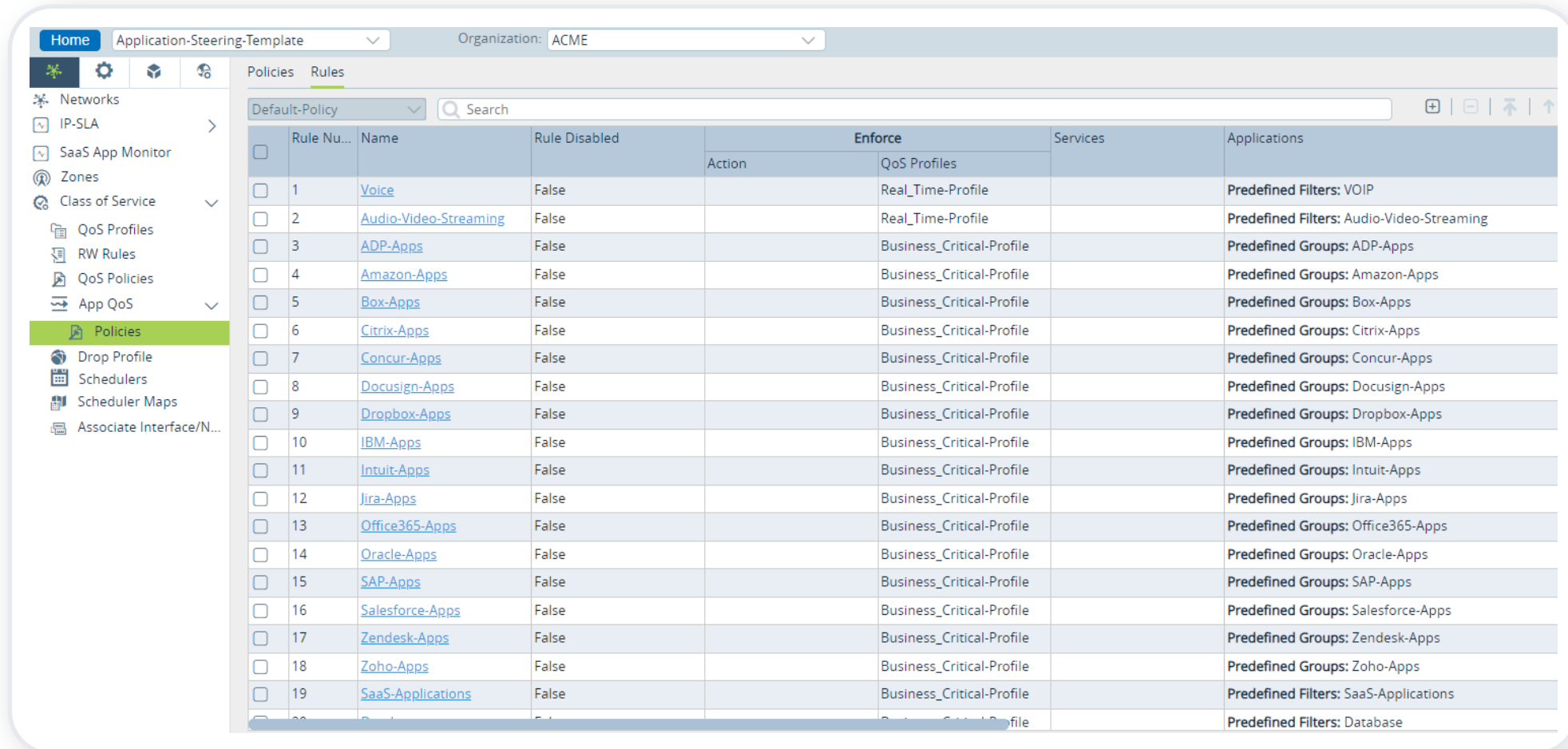


This screenshot shows the 'Configuration' tab in the Versa configuration interface. The 'Application-Steering-Template' is selected, and the 'Organization' is set to 'ACME'. The 'QoS Profiles' section is expanded, showing a table of configured profiles.

	Name	Peak Rate (pps)	Peak Rate (Kbps)	Peak Burst Size (Bytes)	Forwarding Class	Loss Priority	DSCP rewrite
☐	Real Time-Profile				Forwarding Class 4 (Expedited-Forward...	low	Yes
☐	Business Critical-Profile				Forwarding Class 8 (Assured-Forwardi...	low	Yes
☐	Default-Profile				Forwarding Class 12 (Best-Effort)	low	Yes
☐	Low Priority-Profile				Forwarding Class 13	high	Yes

Apply QoS

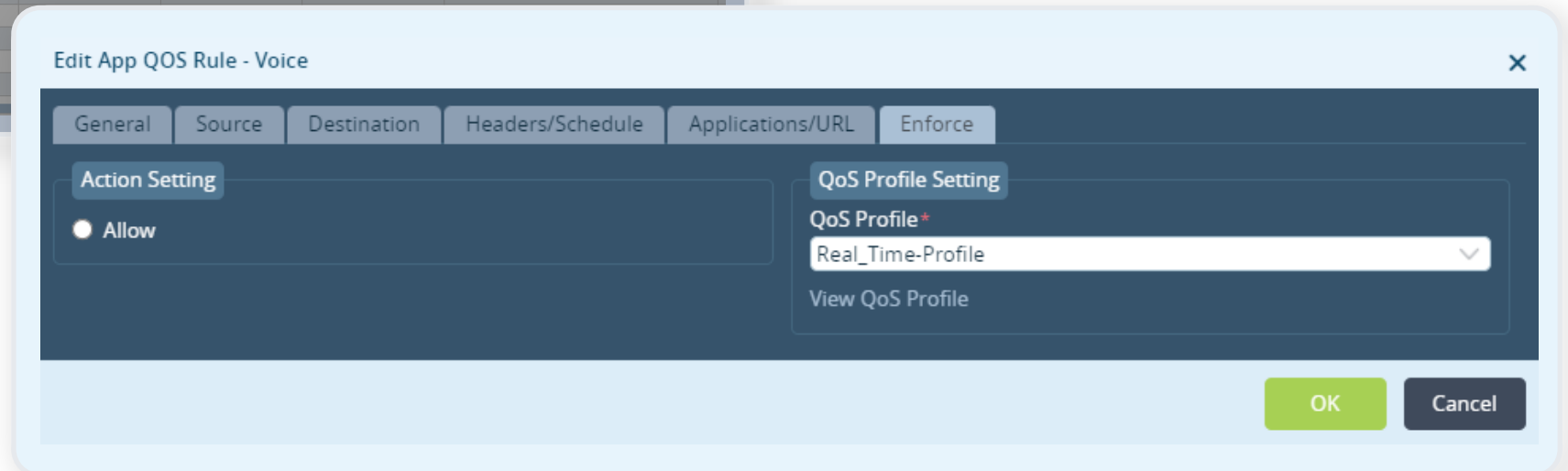
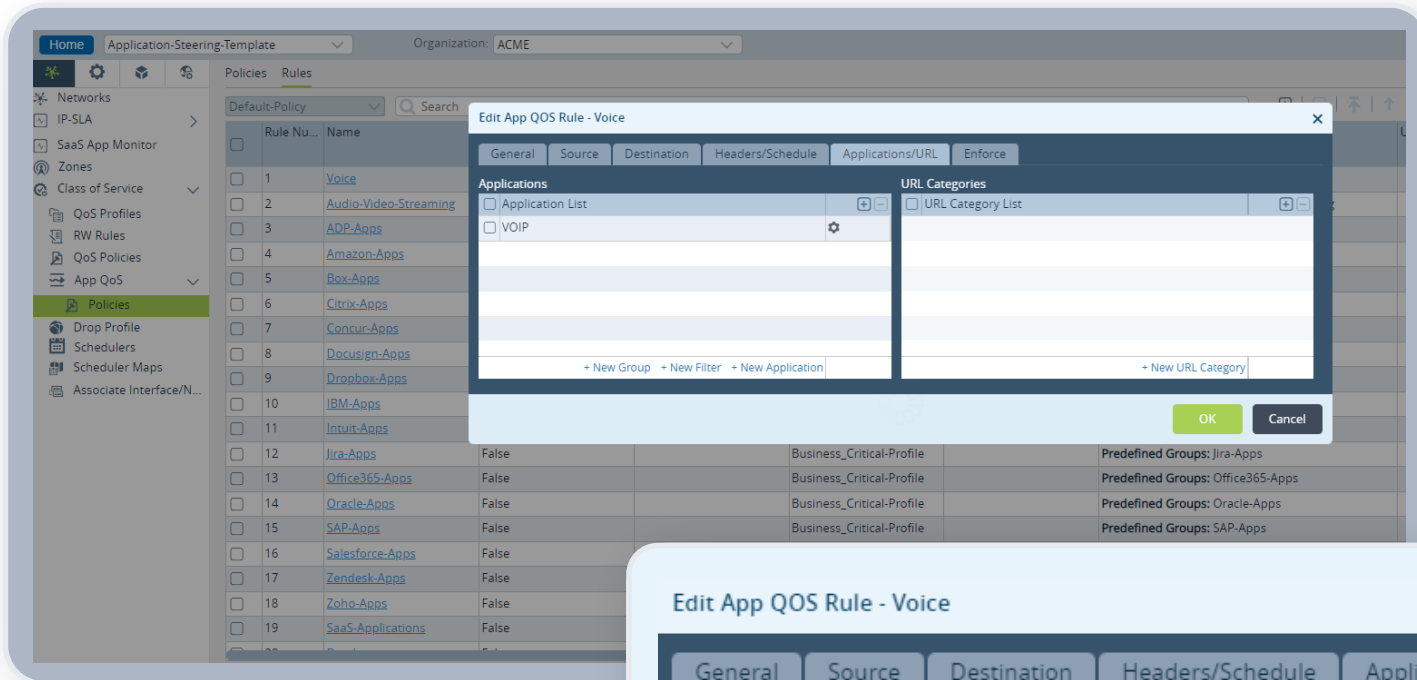
Prioritize the traffic by applying classified traffic with different priority queues



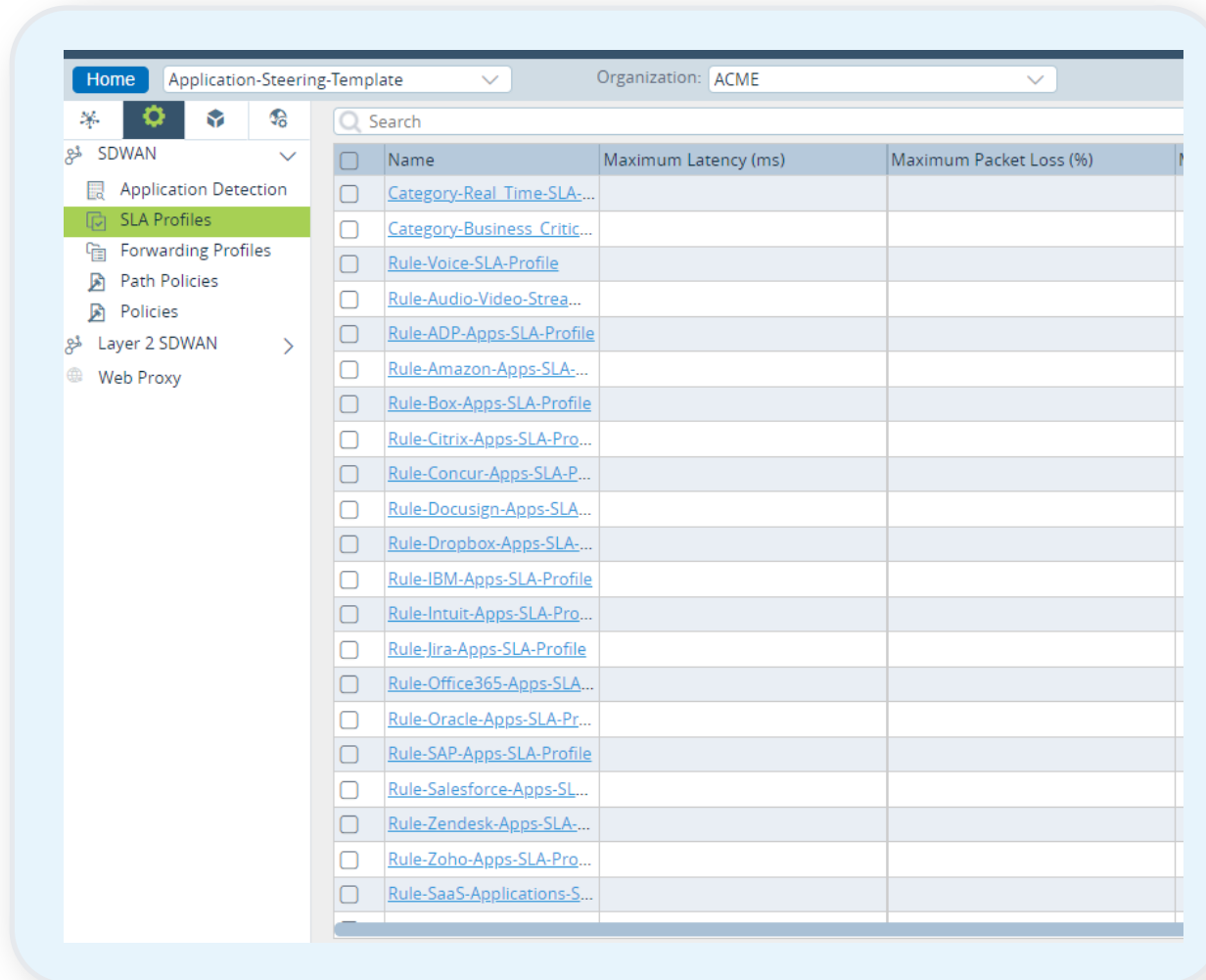
The screenshot displays the Versa Application-Steering-Template interface. The top navigation bar includes 'Home', 'Application-Steering-Template', and 'Organization: ACME'. The left sidebar lists various configuration options, with 'Policies' currently selected. The main content area shows a table of rules under the 'Rules' tab. The table has columns for 'Rule Nu...', 'Name', 'Rule Disabled', 'Enforce' (with sub-columns 'Action' and 'QoS Profiles'), 'Services', and 'Applications'. The table lists 19 rules, each with a checkbox, a rule number, a name (e.g., 'Voice', 'Audio-Video-Streaming', 'ADP-Apps'), a 'Rule Disabled' status (all 'False'), an 'Enforce' action (all 'Business_Critical-Profile'), and a 'QoS Profiles' value (either 'Real_Time-Profile' or 'Business_Critical-Profile'). The 'Applications' column lists predefined filters or groups for each rule.

	Rule Nu...	Name	Rule Disabled	Action	QoS Profiles	Services	Applications
☐	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
☐	20	Database	False		Business_Critical-Profile		Predefined Filters: Database

Apply QoS



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

Configure SLA Profiles

Edit SLA Profile - Category-Real_Time-SLA-Profile

General

SaaS App Monitor

Name*

Category-Real_Time-SLA-Profile

Description

Tags

Packet Delay-variation (jitter) ⚙

Circuit Transmit Utilization (%) ⚙

Circuit Receive Utilization (%) ⚙

Maximum Packet Loss (%) ⚙

Maximum Forward Packet Loss (%) ⚙

Maximum Reverse Packet Loss (%) ⚙

Maximum Latency (ms) ⚙

MOS Score ⚙

☒ Low Delay Variation

☒ Low Latency

☐ Low Packet Loss

☐ Low Forward Packet Loss

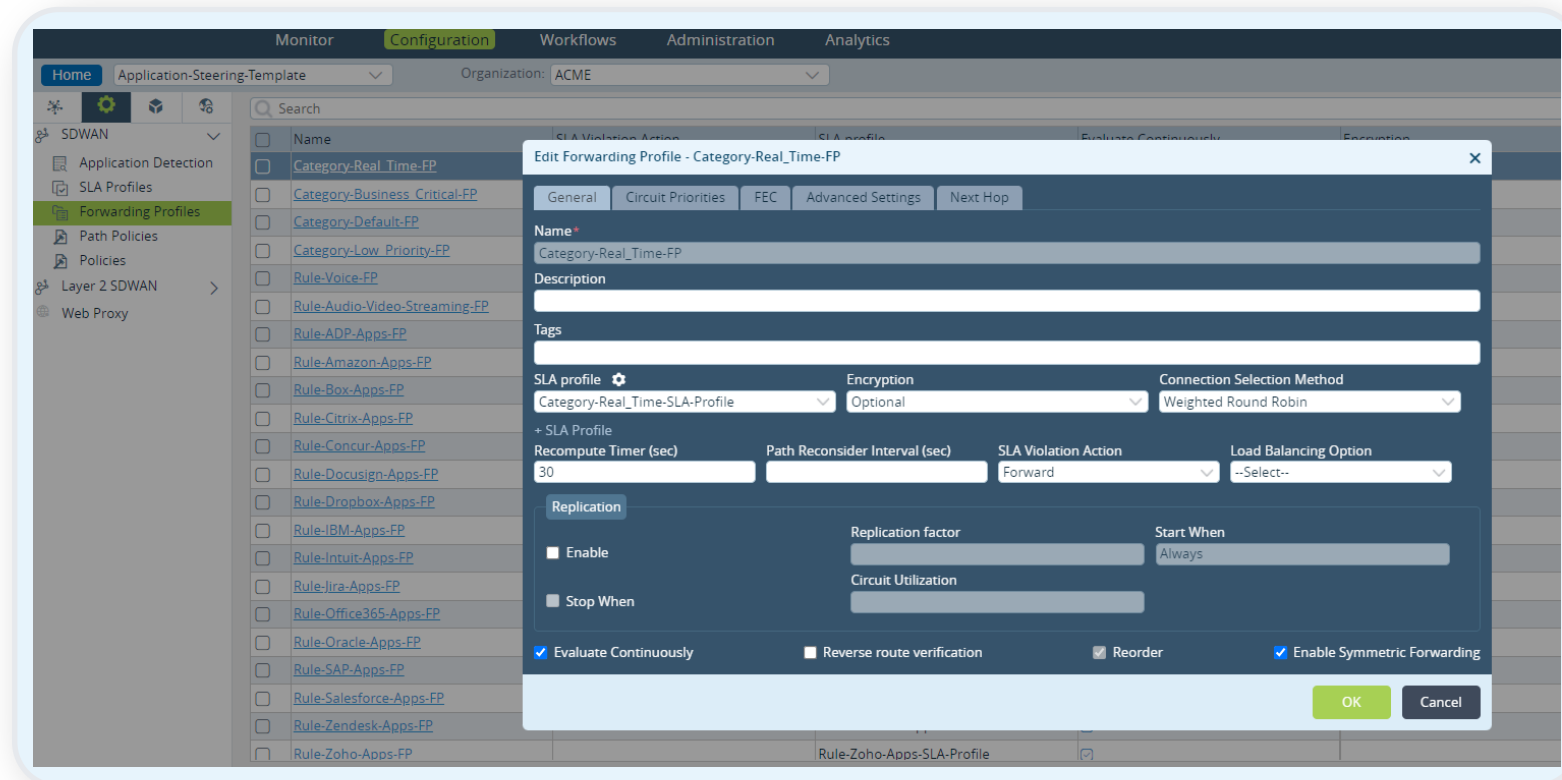
☐ Low Reverse Packet Loss

OK

Cancel

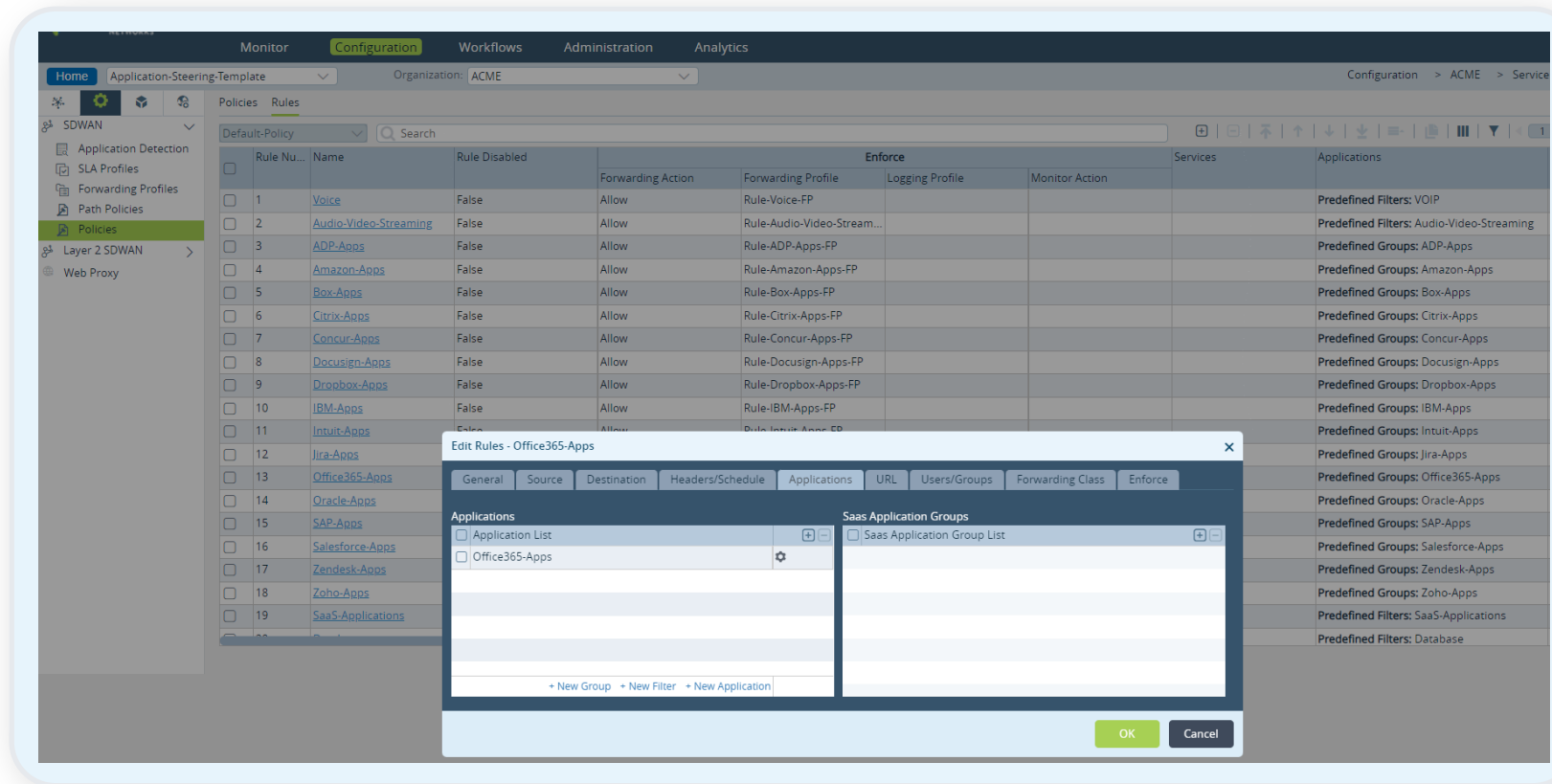
Configure Forwarding Profiles

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



Configure SD-WAN Policies

SD-WAN policies are 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

Edit Rules - Office365-Apps

General Source Destination Headers/Schedule Applications URL Users/Groups Forwarding Class Enforce

Forwarding

Action* Forwarding Profile

View Forwarding Profile

Nexthop IP address Routing Instance

☐ Enable Symmetric Forwarding of Return Traffic ☐ Enable Symmetric L2 Forwarding of Return Traffic

Monitor

Address Routing Instance

Action Interval(sec)

Threshold(Events)

Logging

LEF Profile ☐ Default Profile

Event Rate Limit

TCP Optimization

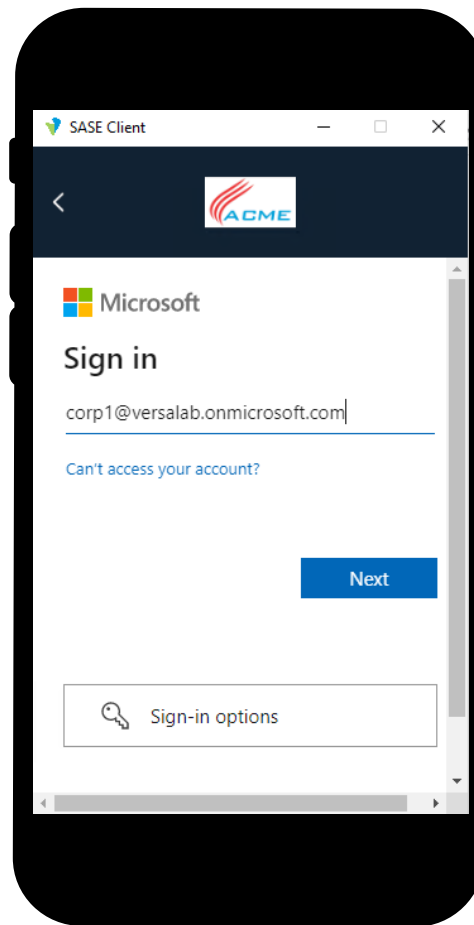
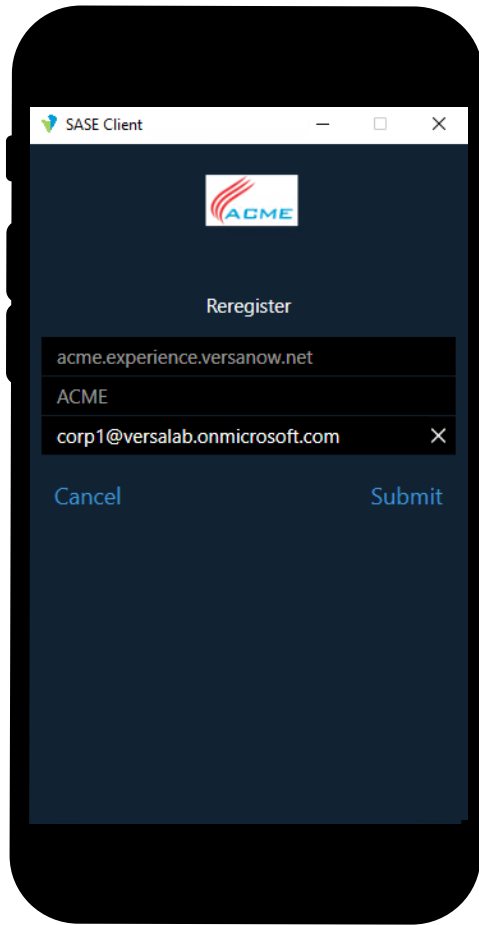
Bypass Latency Threshold (msec) Mode

Lan Profile Wan Profile

OK Cancel

Zero Trust Network Access

Portal Policies



Authenticate before connecting to portal and gateway

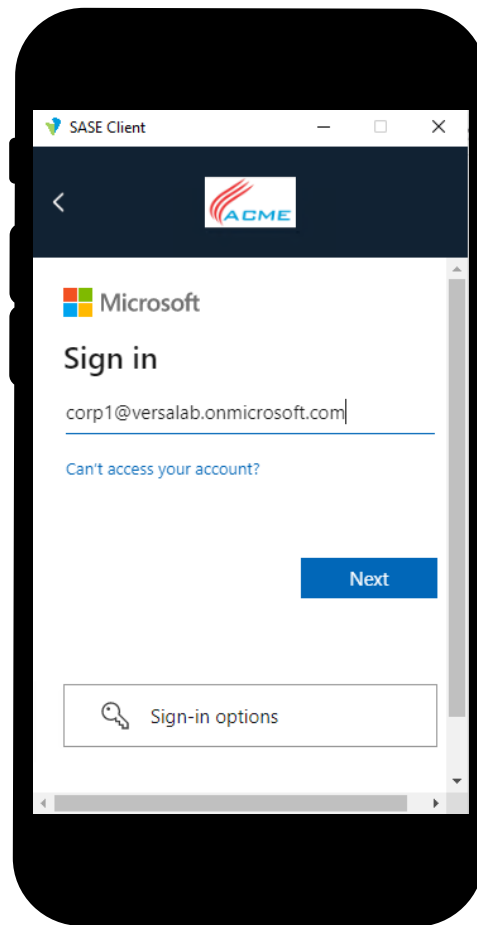
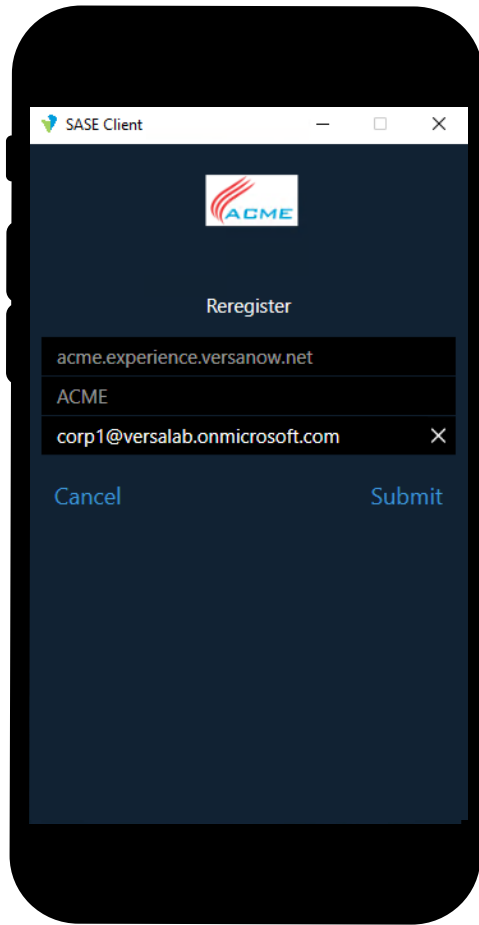
- Use standard authentication like LDAP, SAML
- Enable MFA
- Enable email-based OTP
- Enable TOTP

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

Versatility 2024

Zero Trust Network Access



Versatility 2024

© 2024 Versa and/or its affiliates. All rights reserved

Check user posture

- User and Entity Behavior Analytics (UEBA)
- Bulk delete, Bulk upload, Bulk failed logins, risk country, impossible travel 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



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

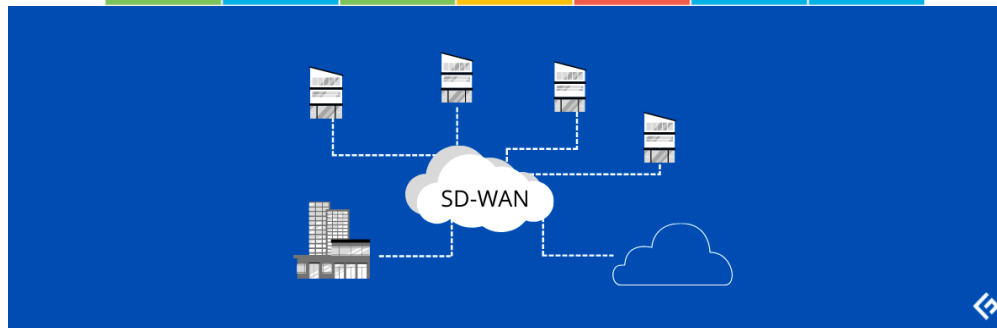
Best Connectivity Options

- 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

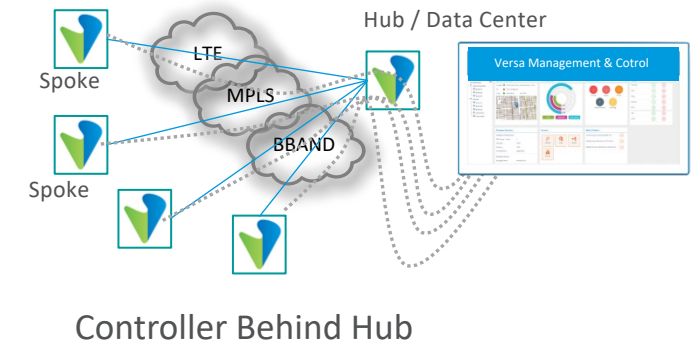
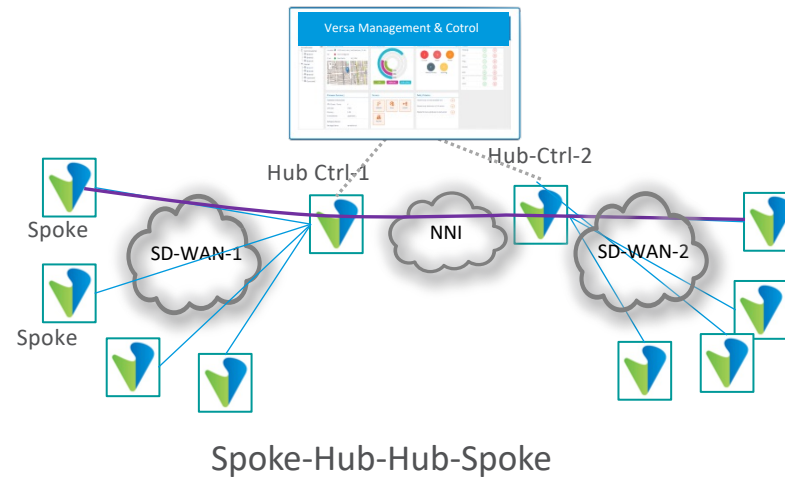
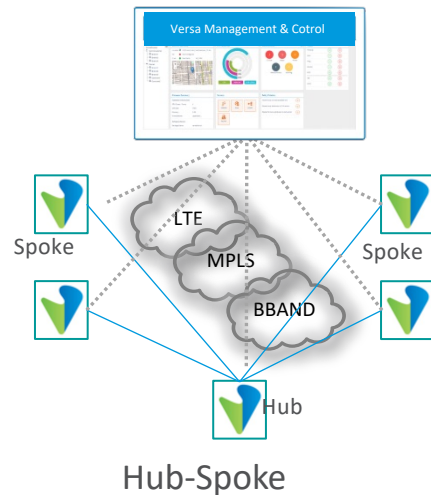
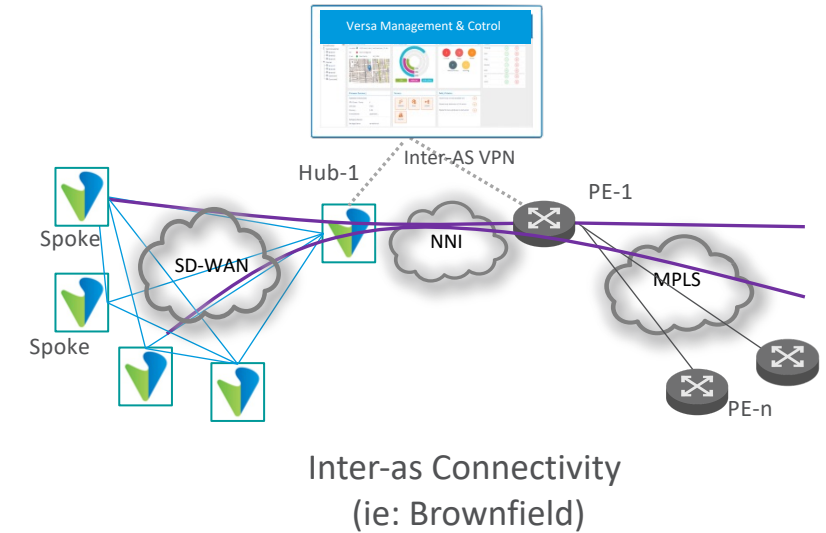
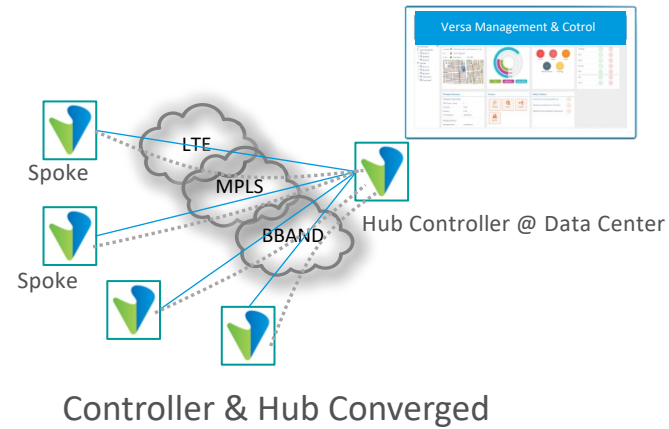
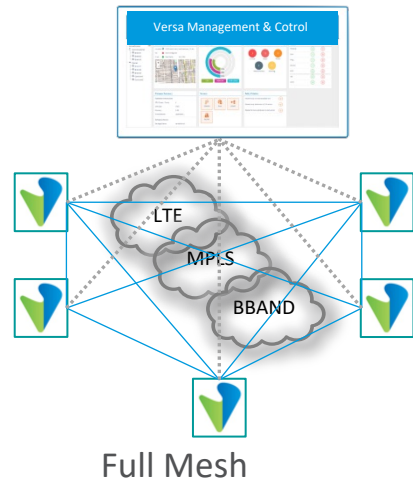
Use SD-WAN for best of all

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

IPsec packet



Different deployment scenarios and topologies



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)

VERSA NETWORKS

Director View | Appliance View | Template View

Monitor | Configuration | **Workflows** | Administration | Analytics

Organization: Prospective-Customer | You are currently in Director View

Infrastructure | **Template** | Devices

Workflows > Template > Spoke Groups

Commit Template

Configure Basic

Spoke Group: Spoke-Group-1

Spoke Groups

Name: Spoke-Group-1 | Organizations: Prospective-Customer | Region: ---Please Select---

Hub | Hub Controller

Routing Instances	Spoke Group Type	Community
Prospective-Customer-Enterprise	Spoke To Spoke Via Hub ---Please Select--- Spoke to Hub Only Spoke To Spoke Via Hub Spoke To Spoke Direct	---Please Select---

+Community Options

Hub:Prospective-Customer-Enterprise

Hubs	Priority
DAL-VGW-01	Not Used
SFO-VGW-01	Not Used
ASH-VGW-01	Not Used

Different deployment scenarios and topologies

Add VPN Instance

1 2 3 4
Settings Routes Redistribution Permissions Review & Submit

Spoke Parameters

Topology

- Full Mesh
- Full Mesh
- Spoke to Hub only
- Spoke to Spoke via Hub

Scope

Enterprise

Hub Parameters

☐ Reject Other Region Routes Disabled

Split Tunnels

☐ Direct Internet Access(DIA) Disabled ☐ Gateway Capability Disabled

☐ Underlay Disabled ☐ Gateway Capability Disabled

Add VPN Instance

1 2 3 4
Settings Routes Redistribution Permissions Review & Submit

Spoke Parameters

Topology

Spoke to Spoke via Hub

Spoke Communities [+ Add Variable](#)

Press Enter to add

Other Region Hub LAN Routes

- Reach via Local Hubs
- Reach Directly
- Reach via Local Hubs
- Reject

Hub Parameters

☐ Reject Other Region Routes Disabled

Split Tunnels

☐ Direct Internet Access(DIA) Disabled ☐ Gateway Capability Disabled

☐ Underlay Disabled ☐ Gateway Capability Disabled

Cancel Skip to Review Next

Find Anomalies

Monitor for unusual events

Appliance health Appliance activity Appliance anomalies Search logs activity

Appliance Anomalies

Show 10 entries

Copy CSV PDF

Appliance	Anomalies	CPU Load Exceeded	Memory Load Exceeded	Worker Thread Busy	Packet Buffer Depletions	Session Load Exceeded	Service Load Exceeded
SanJose-Office-Preferred-Standby	31156	0	31022		0	0	134
Colovore-DC-Branch-1	355	0	0		0	0	355
HE-DC-Branch-1	115	0	0		0	0	114
Bangalore-ECT-DC-Active	62	0	0		0	0	62
BLR-VSA-Sandbox	15	0	0		0	0	0
Naveen-Home-Office	2	0	0		0	0	2
Chennai-Office-Preferred-Active	1	0	0		0	0	1

Showing 1 to 7 of 7 entries

Previous 1 Next

Total Anomalies

Memory load exceeded

- ✓ 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

Find Anomalies

Monitor for unusual user activities

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

Sites infected

User infected

Anti Virus Log

☐ Show Domain Names

Search:

Show 10 entries

Receive Time	Appliance	Malware Name	Malware Type	Application	Attacker	Victim	Action	File Name
Sep 14th 2020, 7:56:33 AM PDT	Bangalore-ECT-DC-Active	PDF/Dropper.B	V_DETECTION_TYPE_EXPLOIT	http	192.168.100.11	172.18.101.10	reject	7.1
Sep 14th 2020, 7:56:33 AM PDT	Bangalore-ECT-DC-Active	PDF/Dropper.B	V_DETECTION_TYPE_EXPLOIT	http	192.168.100.11	172.18.101.10	reject	7.2
Sep 14th 2020, 7:56:33 AM PDT	Bangalore-ECT-DC-Active	W32/Risk.FQVH-6948	V_DETECTION_TYPE_RISK	http	192.168.100.11	172.18.101.10	reject	virus_file_209.e
Sep 14th 2020, 7:56:35 AM PDT	Bangalore-ECT-DC-Active	W32/Trojan.WKV-4447	V_DETECTION_TYPE_TROJAN	http	192.168.100.11	172.18.101.10	reject	VirusFile1.exe
Sep 14th 2020, 7:56:35 AM PDT	Bangalore-ECT-DC-Active	W32/Conficker!Generic	V_DETECTION_TYPE_VIRUS	http	192.168.100.11	172.18.101.10	reject	60
Sep 14th 2020, 7:56:36 AM PDT	Bangalore-ECT-DC-Active	W32/Alureon.AM.gen!Eldorado	V_DETECTION_TYPE_RISK	http	192.168.100.11	172.18.101.10	reject	59
Sep 14th 2020, 7:56:36 AM PDT	Bangalore-ECT-DC-Active	W32/Risk.PCSI-7152	V_DETECTION_TYPE_RISK	http	192.168.100.11	172.18.101.10	reject	55
Sep 14th 2020, 7:56:36 AM PDT	Bangalore-ECT-DC-Active	W32/Conficker!Generic	V_DETECTION_TYPE_VIRUS	http	192.168.100.11	172.18.101.10	reject	54
Sep 14th 2020, 7:56:36 AM PDT	Bangalore-ECT-DC-Active	W32/Virtumonde.Y_b.gen!Eldorado	V_DETECTION_TYPE_RISK	http	192.168.100.11	172.18.101.10	reject	53
Sep 14th 2020, 7:56:36 AM PDT	Bangalore-ECT-DC-Active	W32/Conficker!Generic	V_DETECTION_TYPE_VIRUS	http	192.168.100.11	172.18.101.10	reject	52

Applications used as
carrier of infections

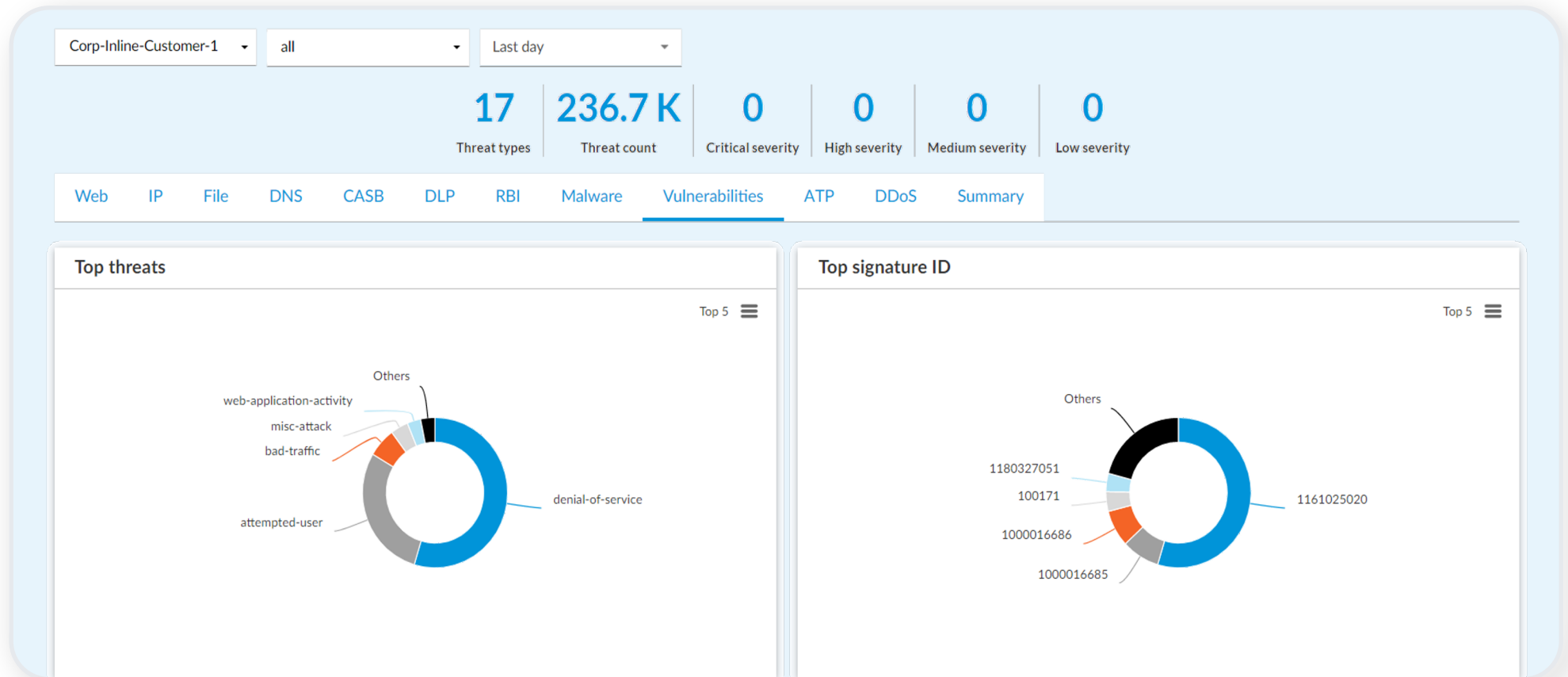
Action taken

- ✓ 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.

Find Anomalies in the Whole Network

Vulnerabilities

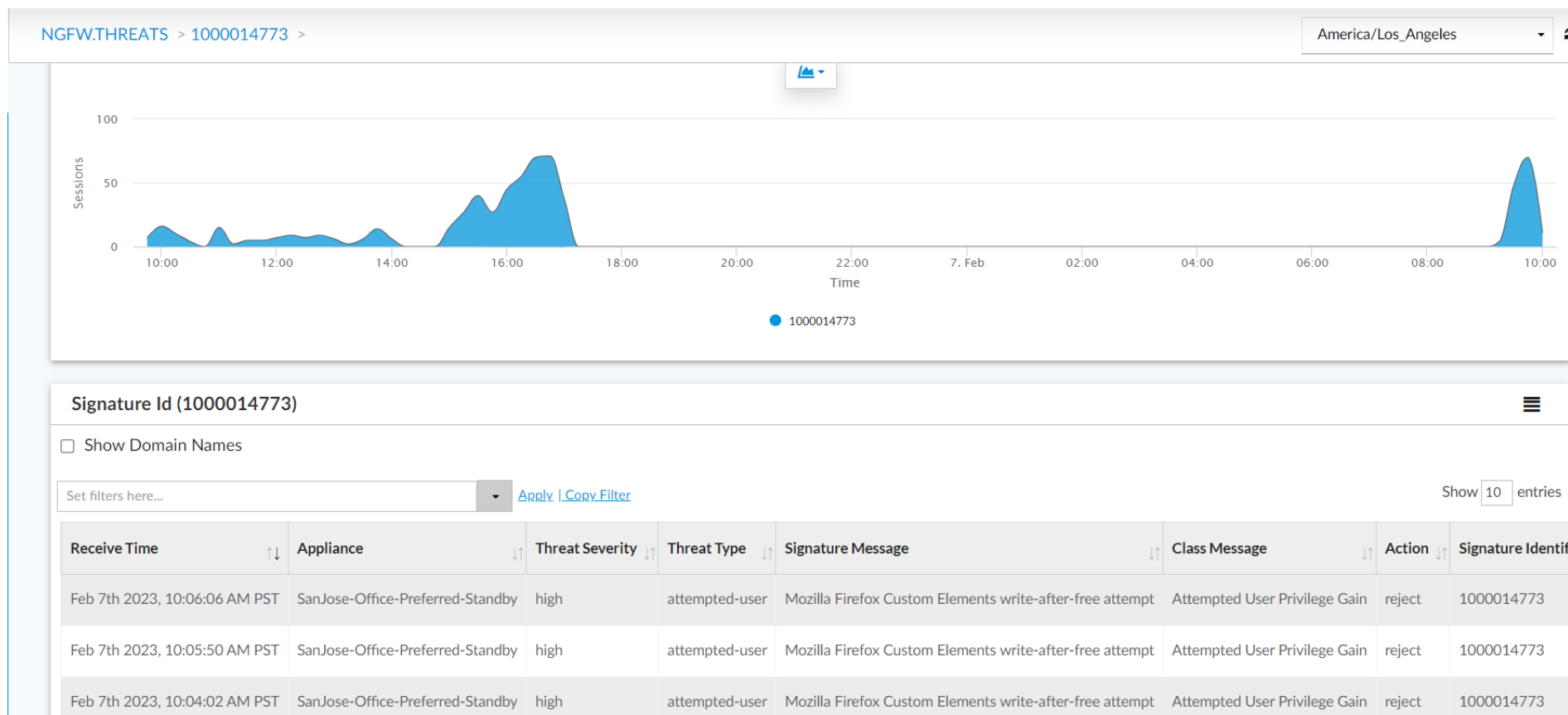
- Find users accessing apps or servers with vulnerabilities



Find Anomalies in the Whole Network

Vulnerabilities Continued

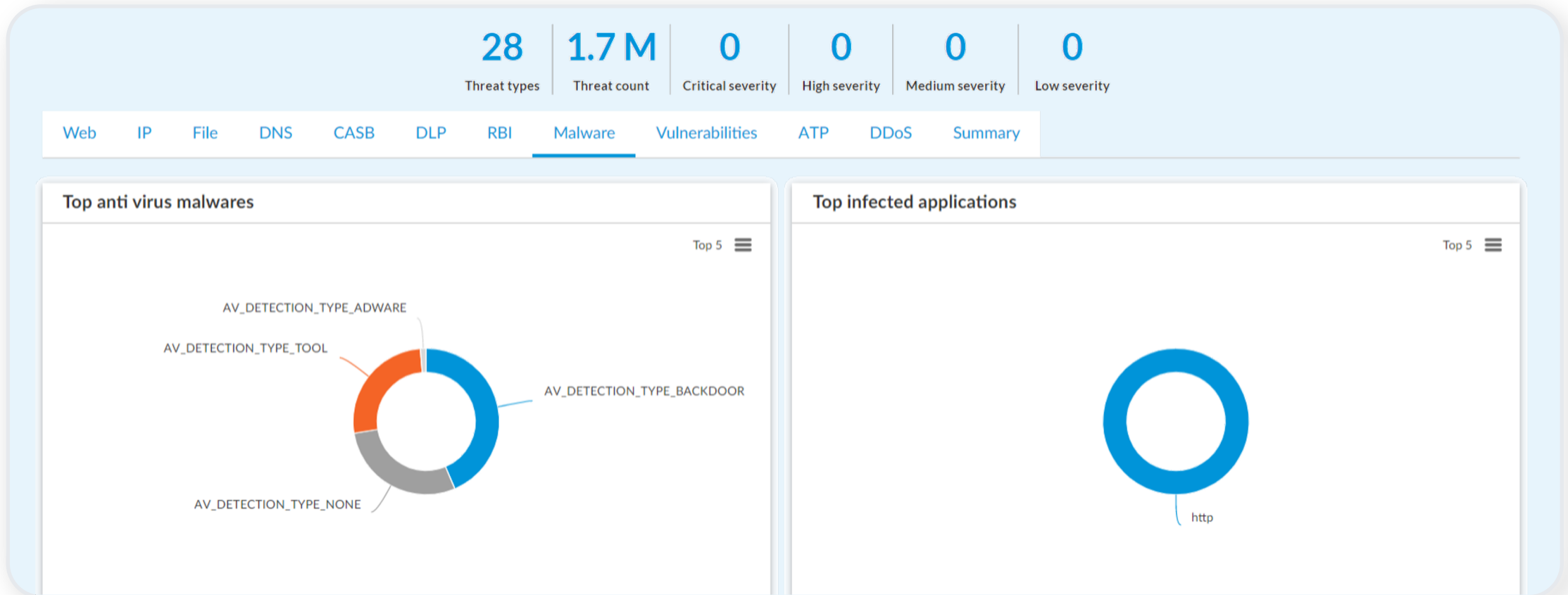
- Find users accessing apps or servers with vulnerabilities



Find Anomalies in the Network

Malwares

- Find users accessing sites or resources which have malwares



Find Anomalies in the Network

Malwares Continued

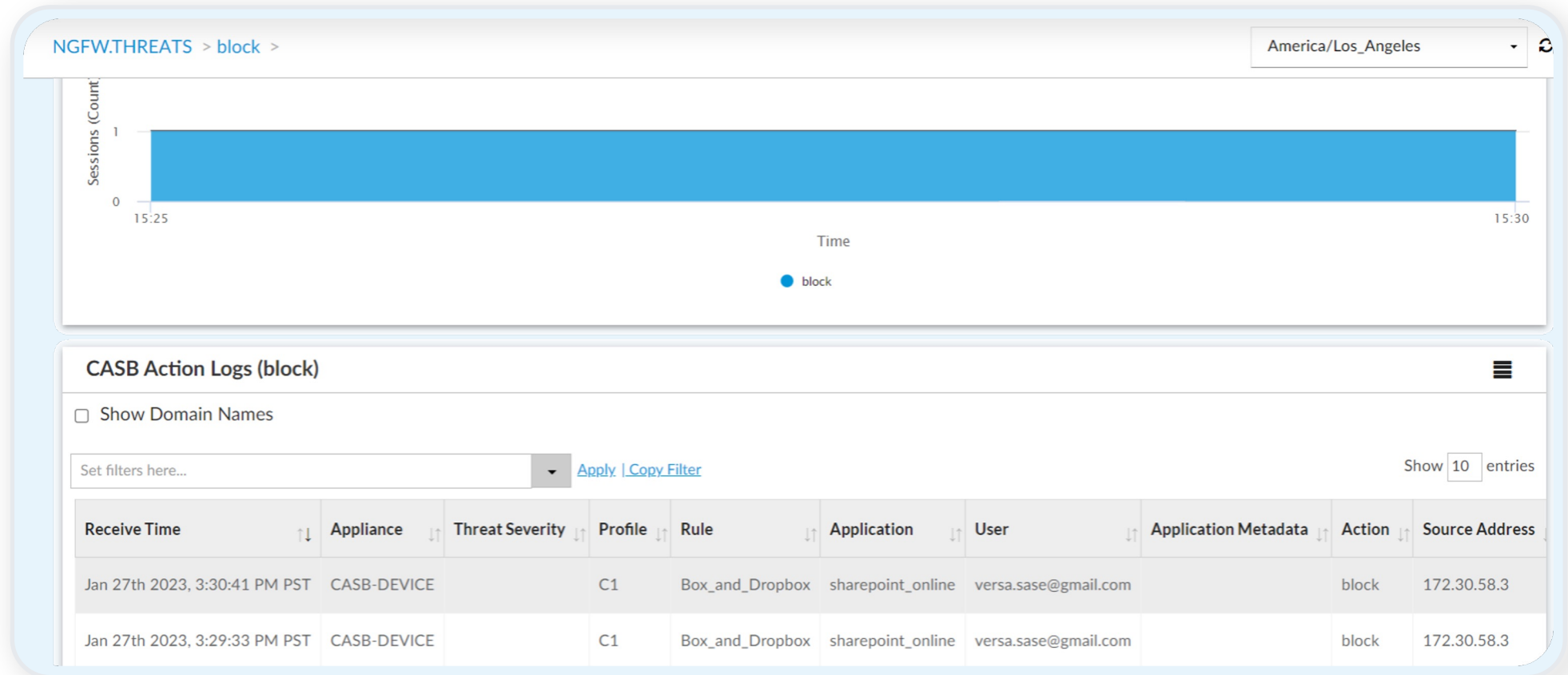
- Find users accessing sites or resources which has malwares

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



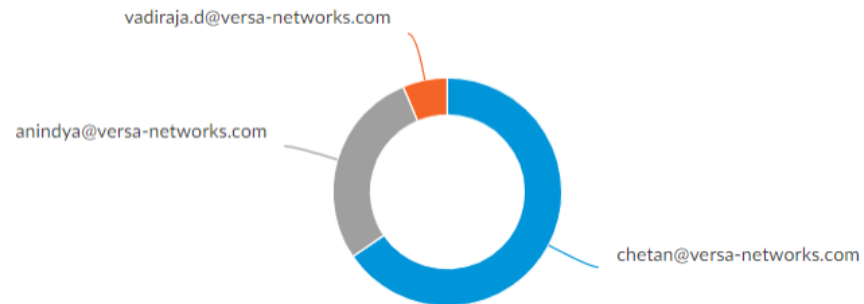
Find Anomalies in the Network

Leaking Sensitive Information

- Find users leaking sensitive information

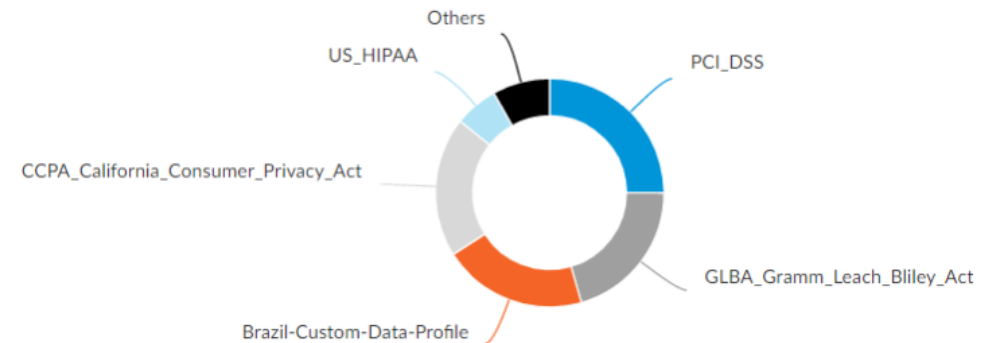
Top DLP users

Top 5



Top DLP data profiles

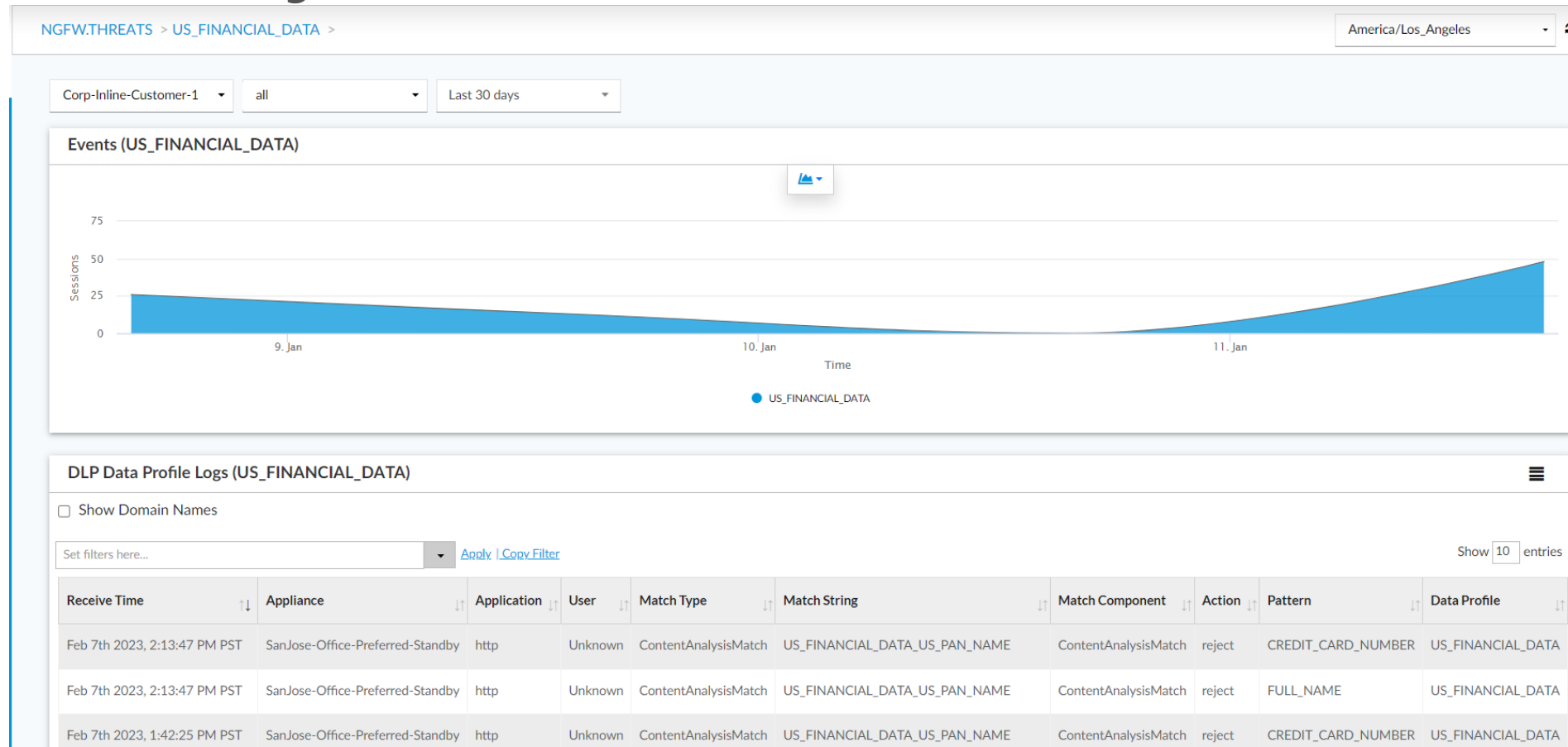
Top 5



Find Anomalies in the Network

Leaking Sensitive Information Continued

- Find users leaking sensitive information

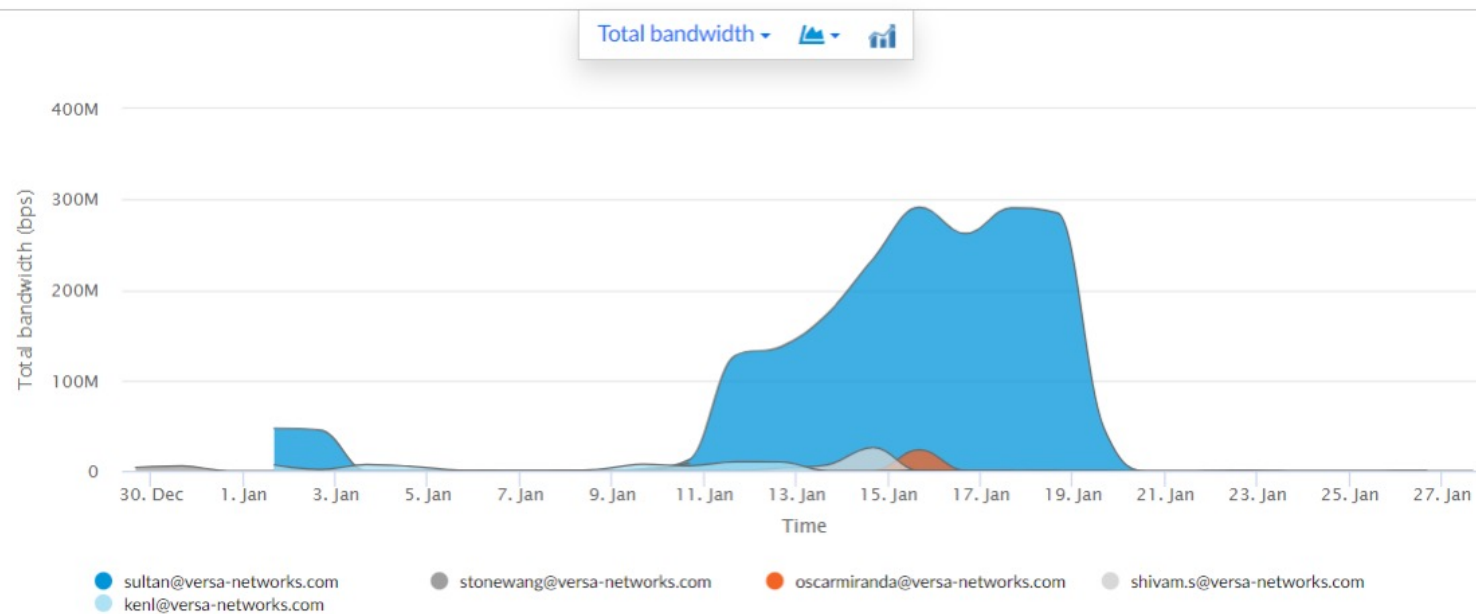


Find Anomalies in the Network

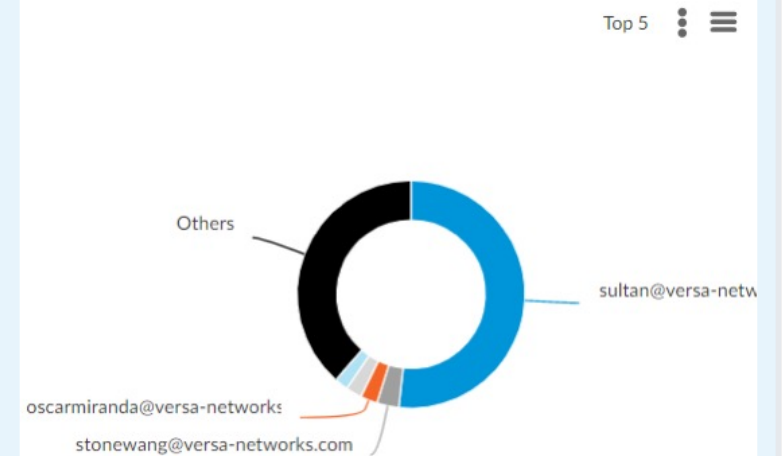
Over Utilizing Resources

- Find users over utilizing network bandwidth

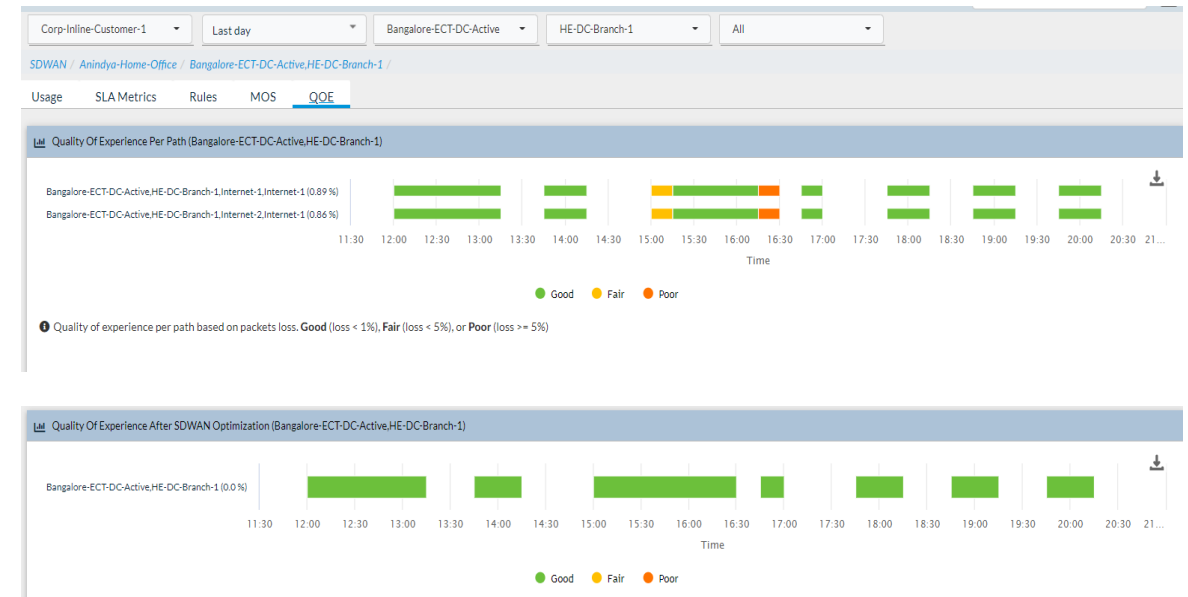
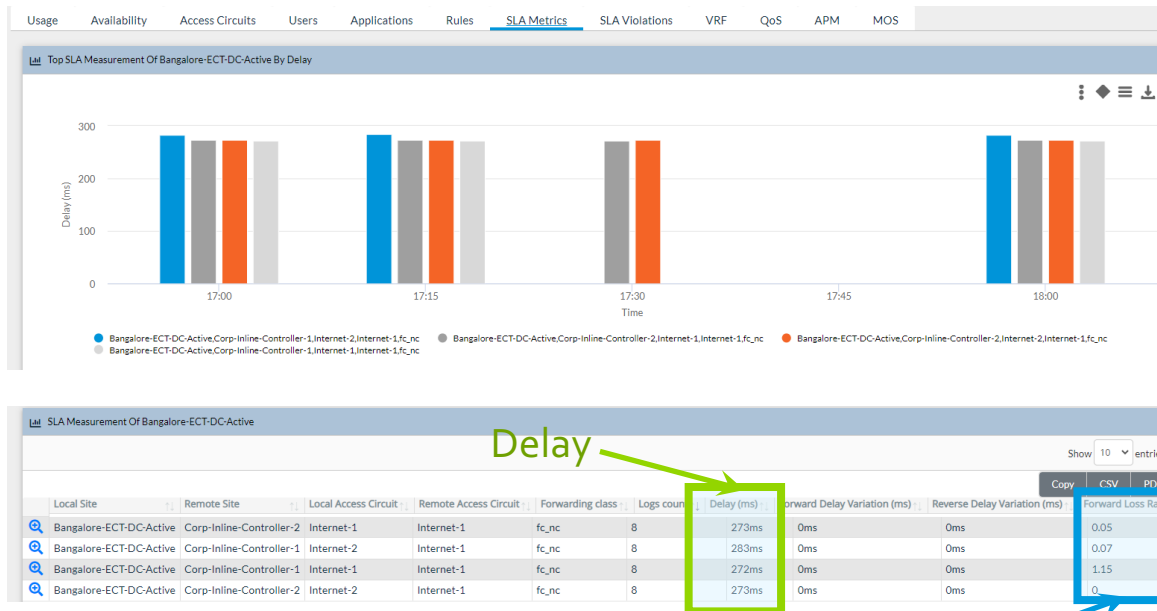
Statistics per user by total bandwidth



Top users by bandwidth



Monitor Network Performance



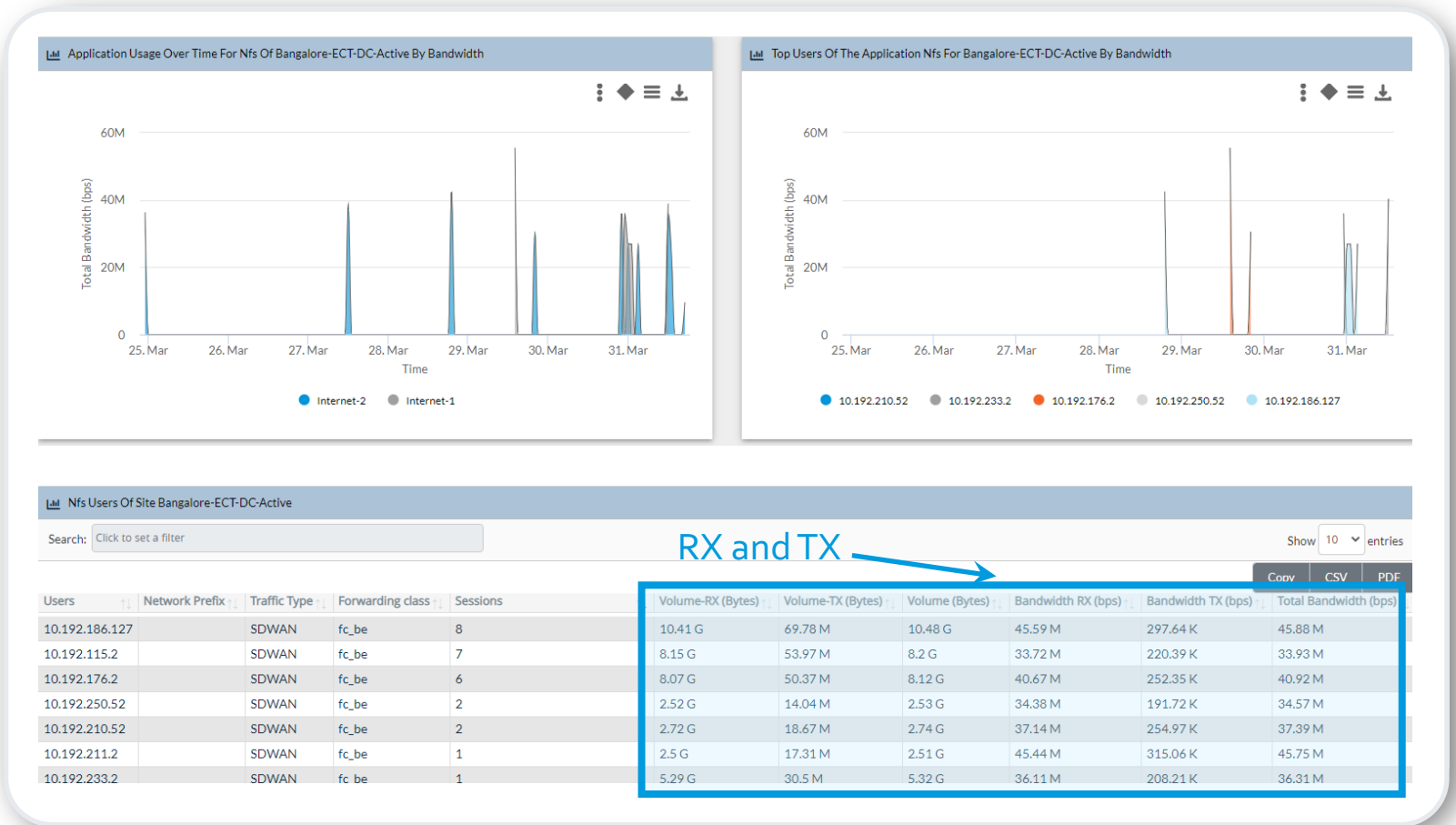
- ✓ Packet loss on underlay paths
- ✓ Latency and jitter on underlay paths

- ✓ Complete black out of underlay paths
- ✓ Quality of Experience (QoE)

Monitor Application Performance



Historical Application Performance



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

Summary Services System Tools

Shell Config Status Upgrade Subscription

Naveen-Home-Office :10.0.192.125 Location 900 pepper tree ln, apt 223 Santa Clara, CA, United States 95051 ● Reachable Up since : Thu Aug 19 13:07:21 2021

Services

SDWAN NGFW CGNAT SDLAN IPSEC Sessions SCI Secure Access

Networking

Interfaces Routes BGP OSPF OSPFv3 BFD DHCP DNS Stats COS VRRP LEF ARP IP-SLA PIM IGMP dot1x RIP Switching LLDP TWAMP SaaS App Certificate

Back Search 1 25

Application	Source IP	Destination IP	Protocol	Source Port	Destination Port	SD-WAN	Natted
gcm/(predef)	172.16.22.11	142.250.142.188	TCP	37262	5228	No	Yes
amazon/(predef)	172.16.22.11	3.232.200.166	TCP	54127	443	No	Yes
https/(predef)	172.16.22.11	18.211.189.31	TCP	54150	443	No	Yes
amazon/(predef)	172.16.22.11	3.232.200.166	TCP	54194	443	No	Yes
amazon/(predef)	172.16.22.11	13.248.198.36	TCP	55354	443	No	Yes
amazon/(predef)	172.16.22.11	23.20.244.197	TCP	55942	443	No	Yes
https/(predef)	172.16.22.11	52.72.223.252	TCP	55972	443	No	Yes
amazon/(predef)	172.16.22.11	35.172.31.219	TCP	55987	443	No	Yes
amazon/(predef)	172.16.22.11	54.158.72.34	TCP	55962	443	No	Yes
google/(predef)	172.16.22.11	142.250.189.196	TCP	56415	443	No	Yes
icmp/(predef)	172.16.22.11	8.8.4.4	ICMP	22988	22988	No	Yes
google_api/(predef)	172.16.22.11	142.250.72.202	TCP	57052	443	No	Yes
ms_teams/(predef)	172.16.22.11	52.114.128.88	TCP	56381	443	No	Yes
dns/(predef)	172.16.22.11	8.8.8.8	UDP	50788	53	No	Yes
dns/(predef)	172.16.22.11	8.8.8.8	UDP	53046	53	No	Yes
openstreetmap/(p...	172.16.22.11	151.101.2.137	TCP	56418	443	No	Yes
http2/(predef)	172.16.22.11	151.101.2.137	TCP	56418	443	No	Yes

Monitor Application Performance

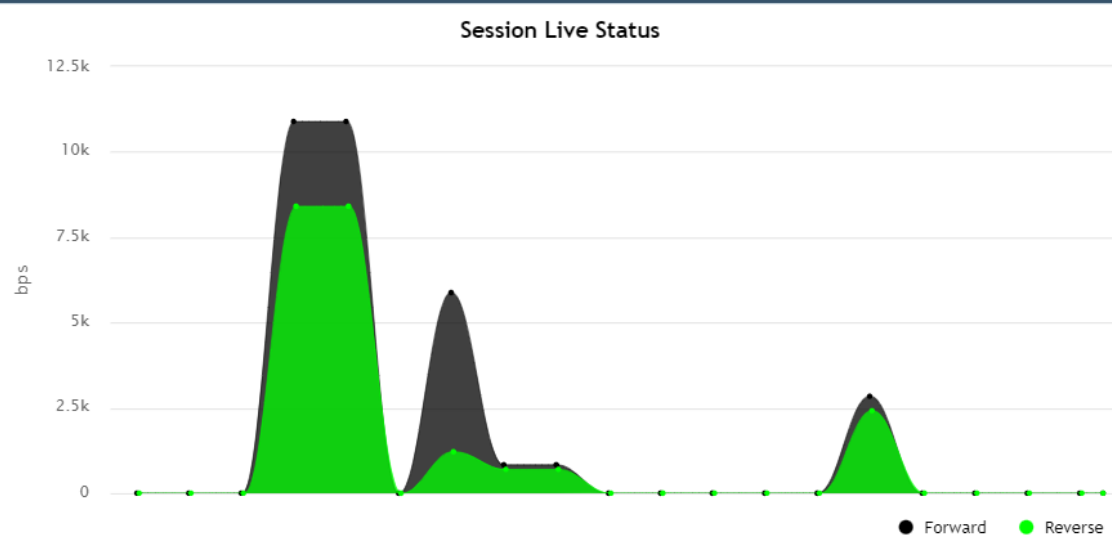


Live Monitoring of MS Teams application

Session ID: 119979

X

Application: ms_teams/(p...
Source IP: 172.16.22.11
Destination IP: 52.114.128....
Protocol: TCP
Source Port: 56427
Destination Port: 443
Forward Traffic: 14.2920 KB
Reverse Traffic: 13.6520 KB
Forward Drops: 0 Bytes
Reverse Drops: 0 Bytes



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

© 2024 Versa and/or its affiliates. All rights reserved. Versa Networks Confidential

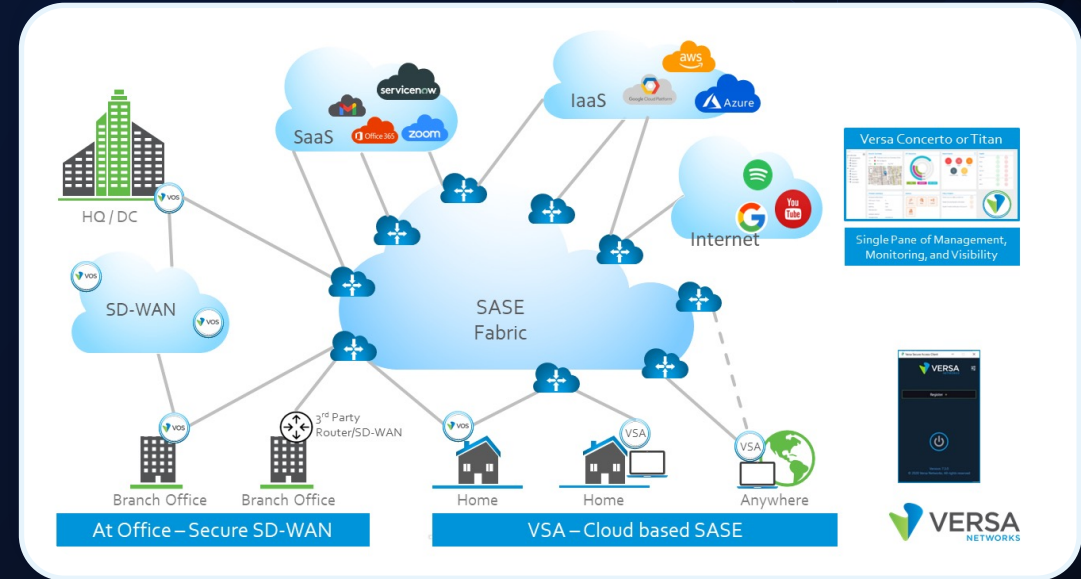


Digital Experience Monitoring (DEM)

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

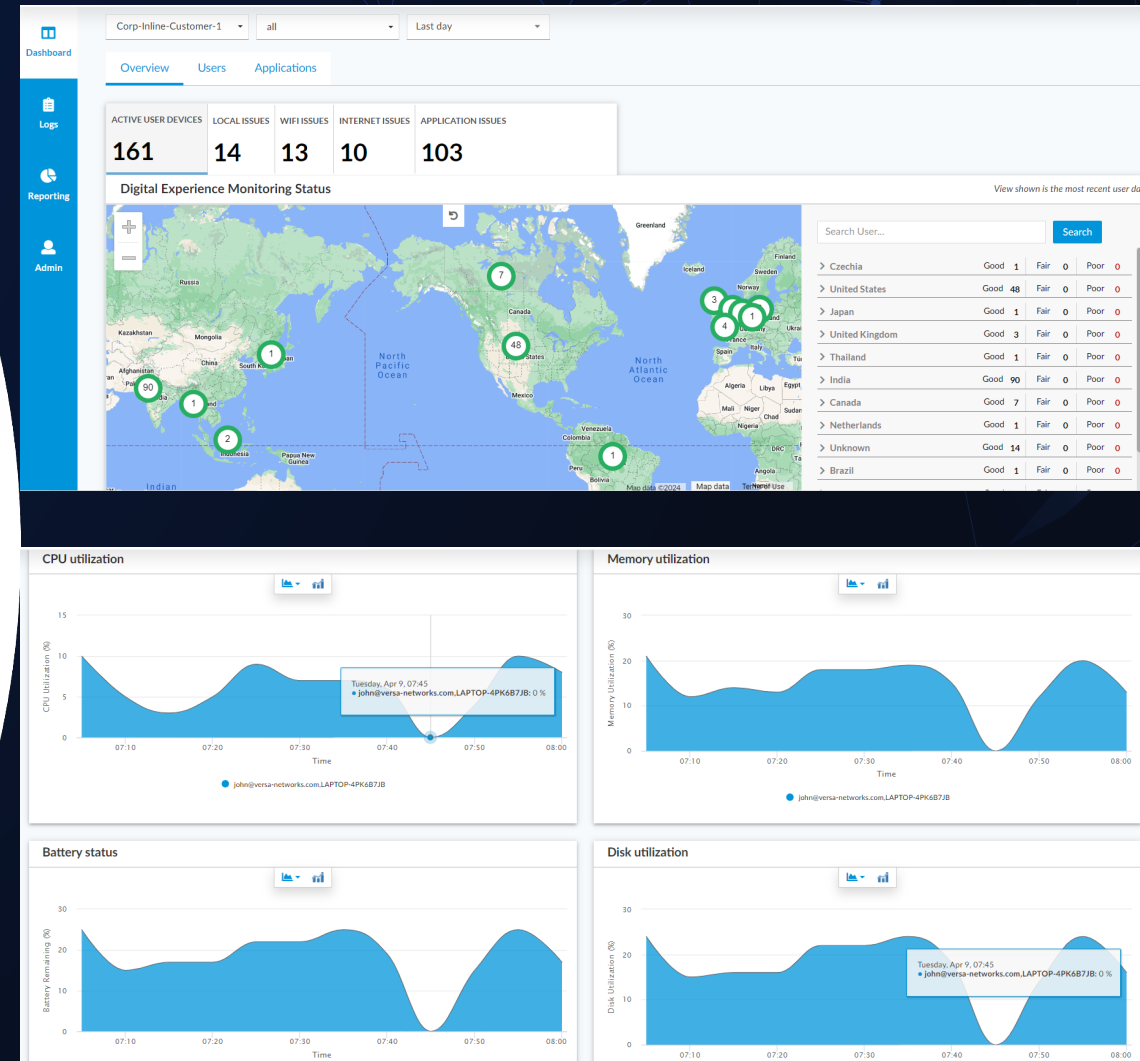


Digital Experience Monitoring (DEM)

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

Versatility 2024

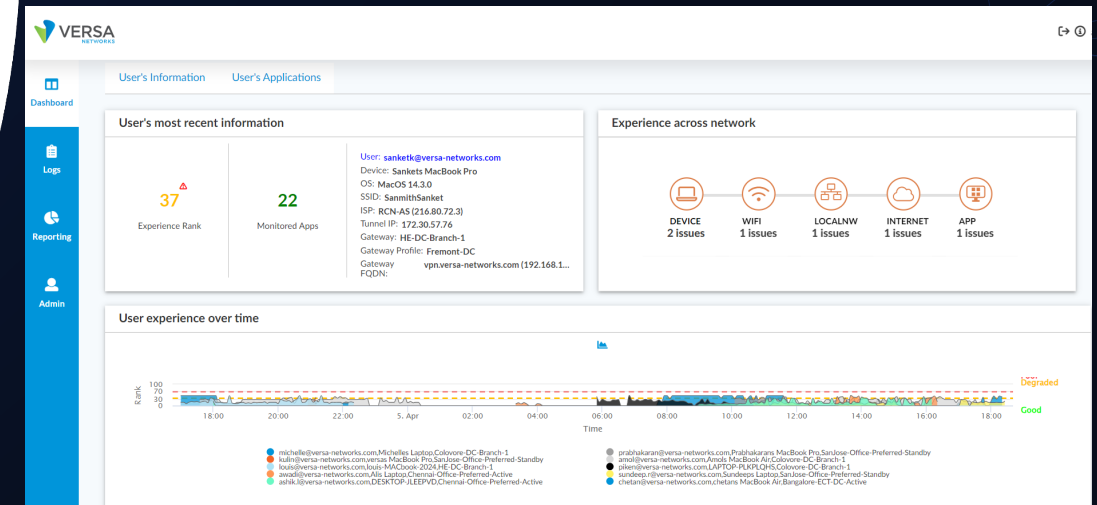
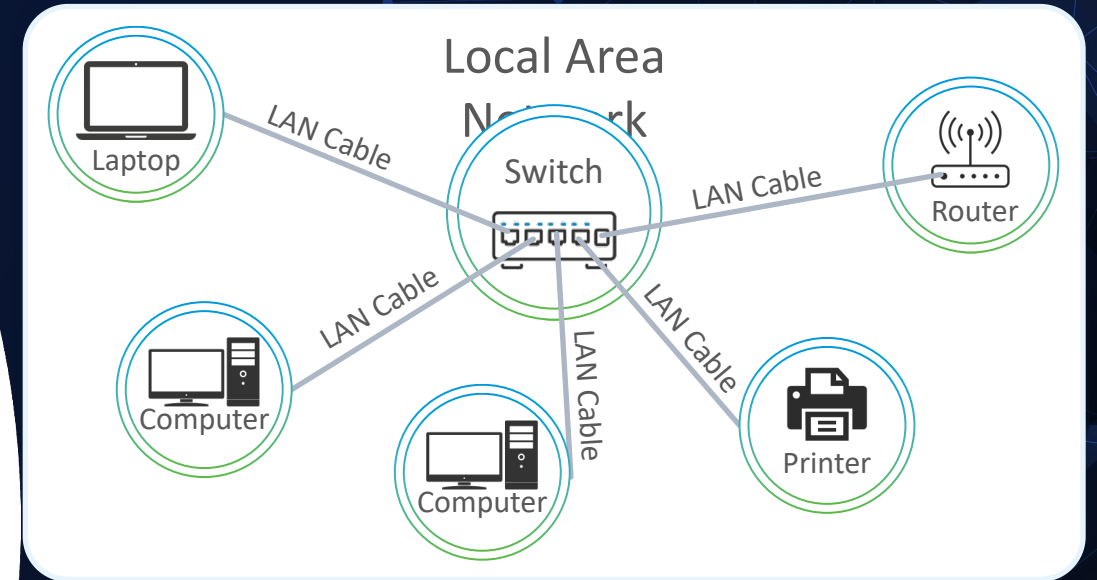


Digital Experience Monitoring (DEM)

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

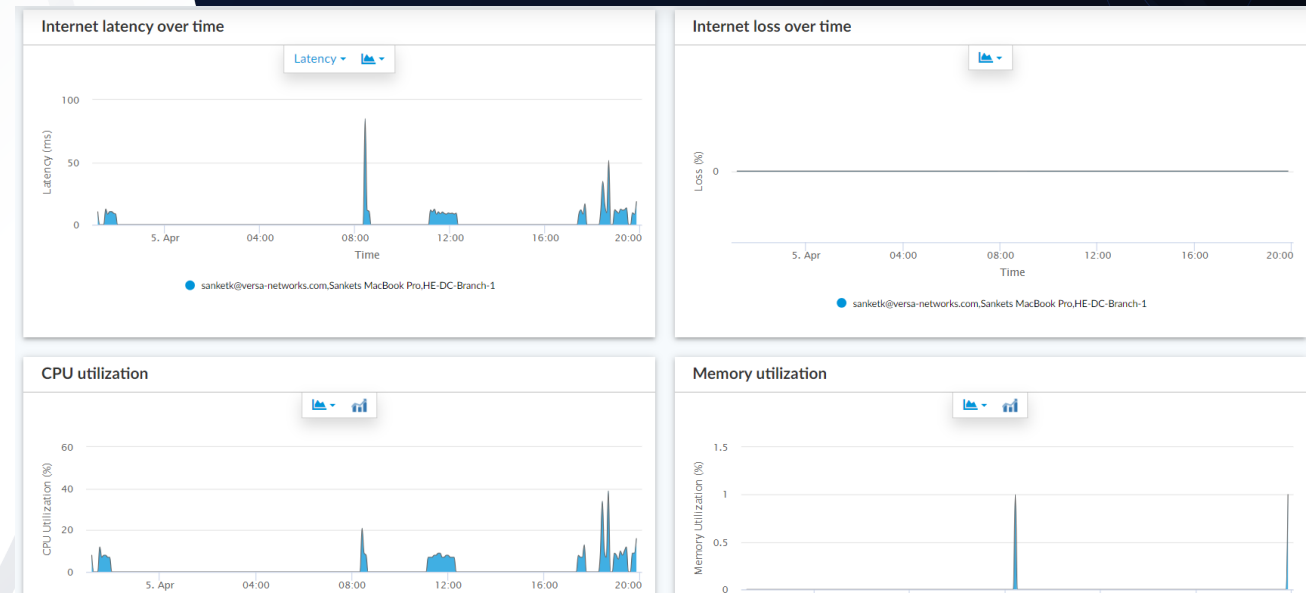
Versatility 2024



Digital Experience Monitoring (DEM)

Monitor Transport Issues

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

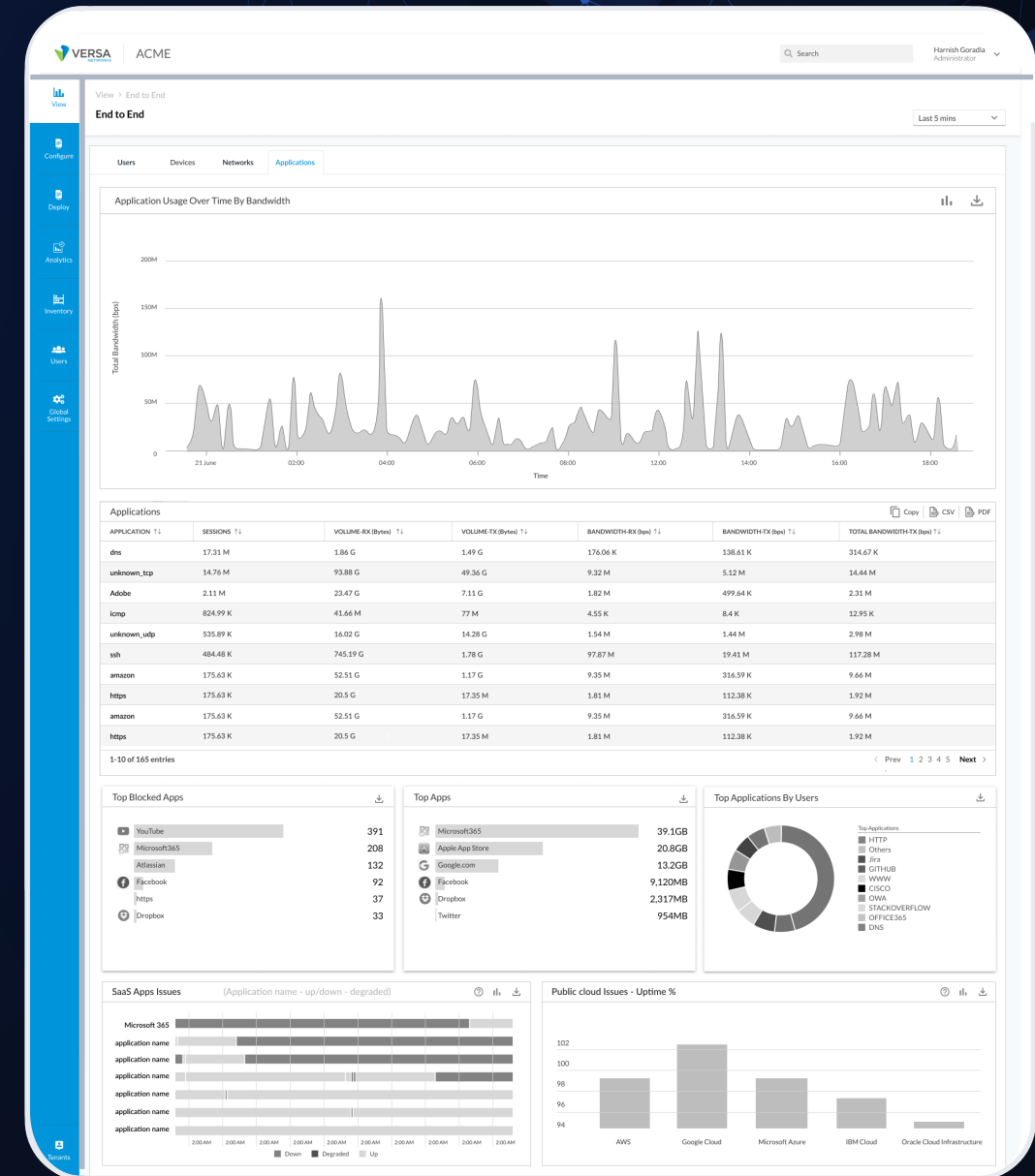


Digital Experience Monitoring (DEM)

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

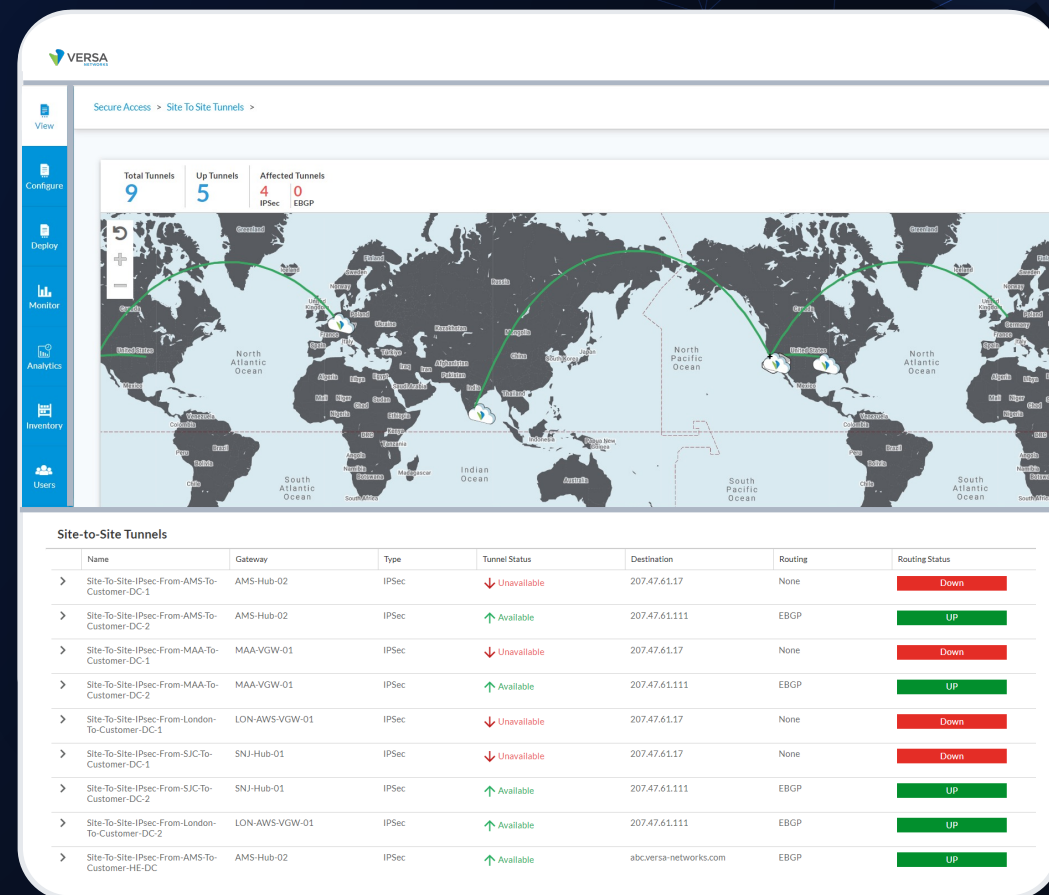
Versatility 2024



Digital Experience Monitoring (DEM)

Monitor Connectivity between
SASE & Customer Network

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



Digital Experience Monitoring (DEM)

Monitor Connectivity between SASE & Customer Network Continued

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

Secure Access > Site To Site Tunnels >

Site-To-Site-IPsec-From-AMS-To-Customer-DC-2	AMS-Hub-02	IPSec	Available	207.47.61.111	EBGP	UP
Detail						
VPN Name	Source Address	Destination Address	Status	Sent	Received	
Naveen_11_3_1-Tenant-1-Enterprise	172.31.101.4	207.47.61.111	UP	2.220 MB	10.50 MB	
Authentication	Interface Address					
psk	169.254.208.1/32					
IKE/IPSec Information						
Phase 1 Encryption Algorithms	Phase 1 Integrity Algorithms	Phase 1 DH Group Numbers	Phase 1 Lifetime			
aes256-cbc	hmac-sha1-96	mod2	28800			
Phase 2 Encryption Algorithms	Phase 2 Integrity Algorithms	Phase 2 DH Group Numbers	Phase 2 Lifetime			
aes256-cbc	hmac-sha1-96	mod-none	28800			
IKE Version	DPD Timeout	IKE History	IPSec History			
v2	30	View details	View details			
IKE Security Association	IPSec Security Association					
View details	View details					
BGP						

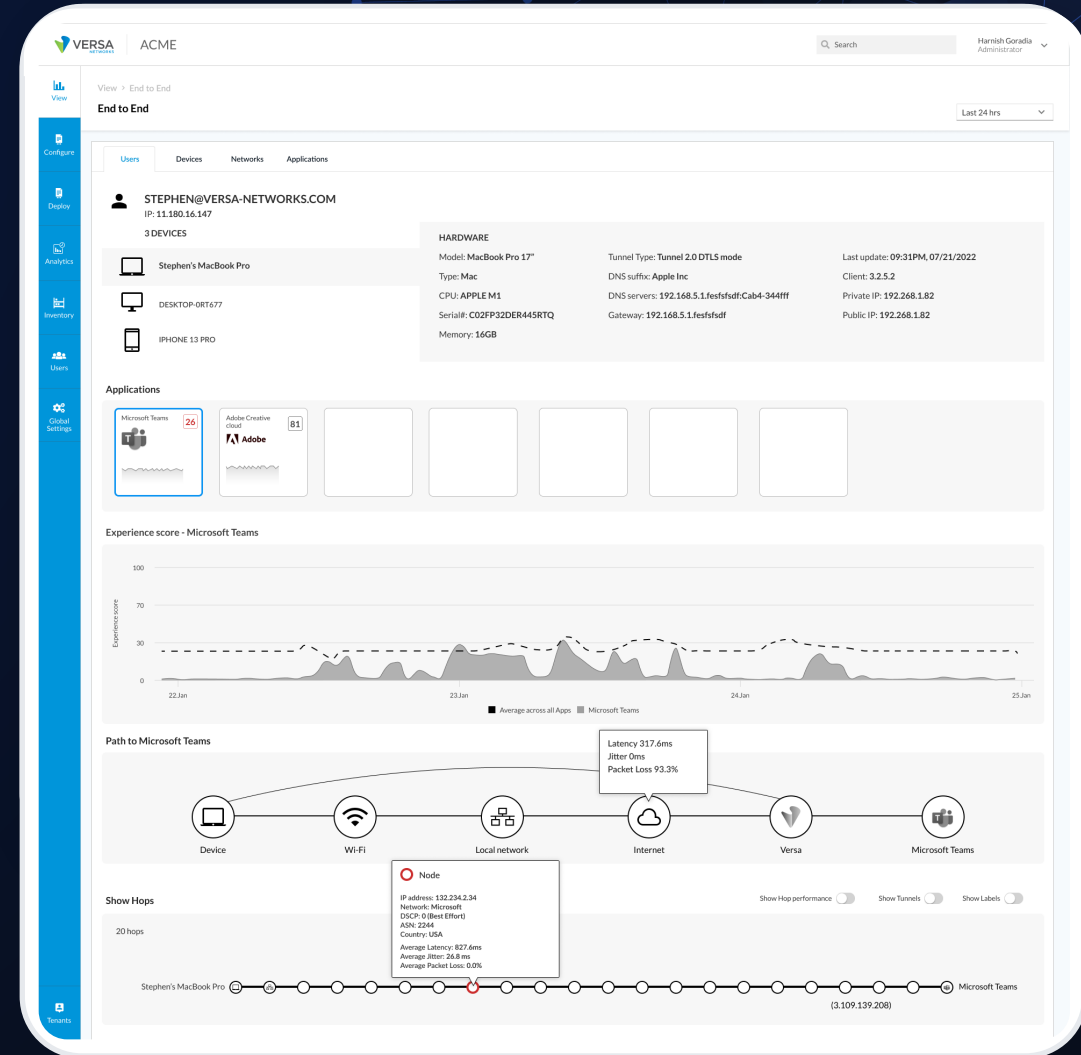
Secure Access > Site To Site Tunnels >

VPN Name	Source Address	Destination Address	Status	Sent	Received
Naveen_11_3_1-Tenant-1-Enterprise	172.31.101.4	207.47.61.111	UP	2.220 MB	10.50 MB
Authentication	Interface Address				
psk	169.254.208.1/32				
IKE/IPSec Information					
Phase 1 Encryption Algorithms	Phase 1 Integrity Algorithms	Phase 1 DH Group Numbers	Phase 1 Lifetime		
aes256-cbc	hmac-sha1-96	mod2	28800		
Phase 2 Encryption Algorithms	Phase 2 Integrity Algorithms	Phase 2 DH Group Numbers	Phase 2 Lifetime		
aes256-cbc	hmac-sha1-96	mod-none	28800		
IKE Version	DPD Timeout	IKE History	IPSec History		
v2	30	View details	View details		
IKE Security Association	IPSec Security Association				
View details	View details				
BGP					
State	Received Prefixes	Sent Prefixes	Received Messages	Sent Messages	
Established	14	125	15847	15557	
Established Time	Local ASN	Neighbor ASN	Local Address	Neighbor Address	
3d20h08m	65507	65508	169.254.208.1	169.254.208.2	

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



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



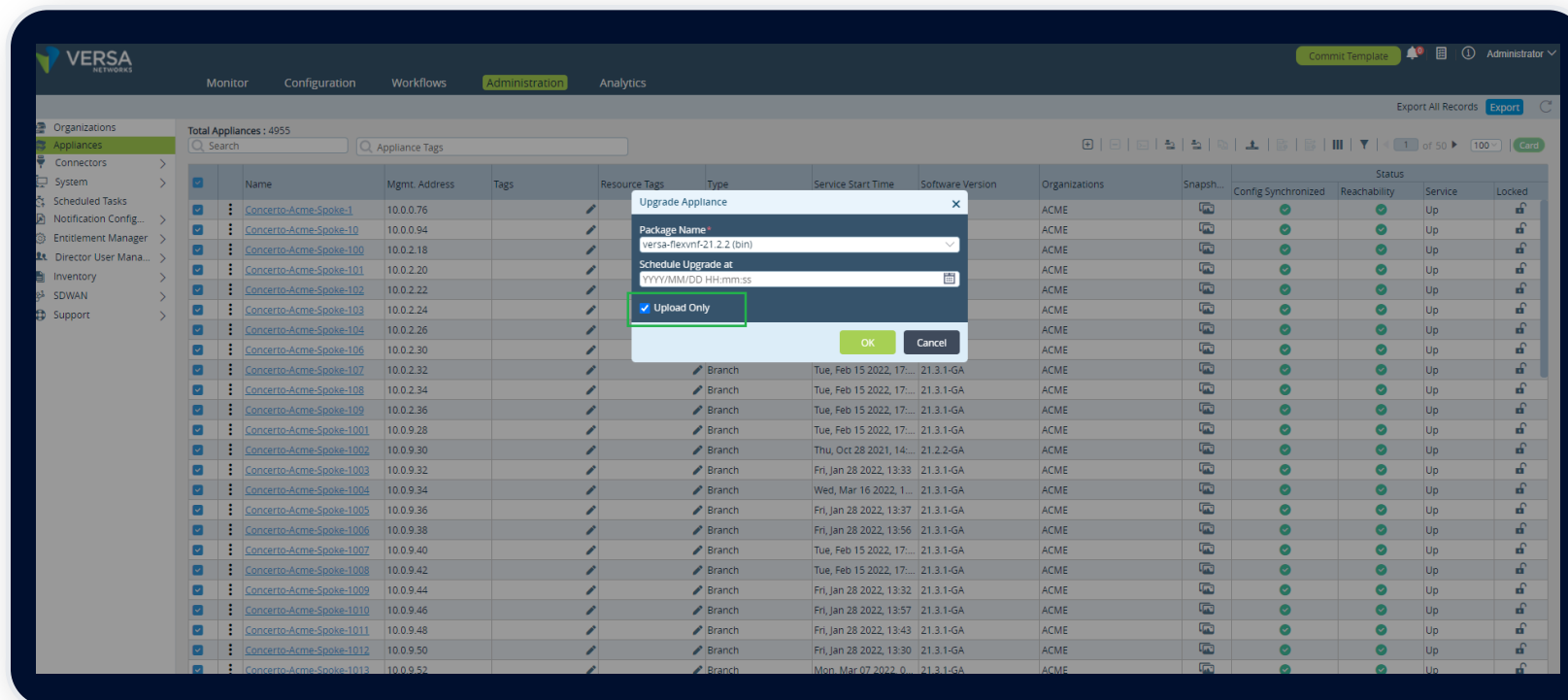
Upgrade to latest based OS (ubuntu)

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

Installing VOS Image on Edge Devices

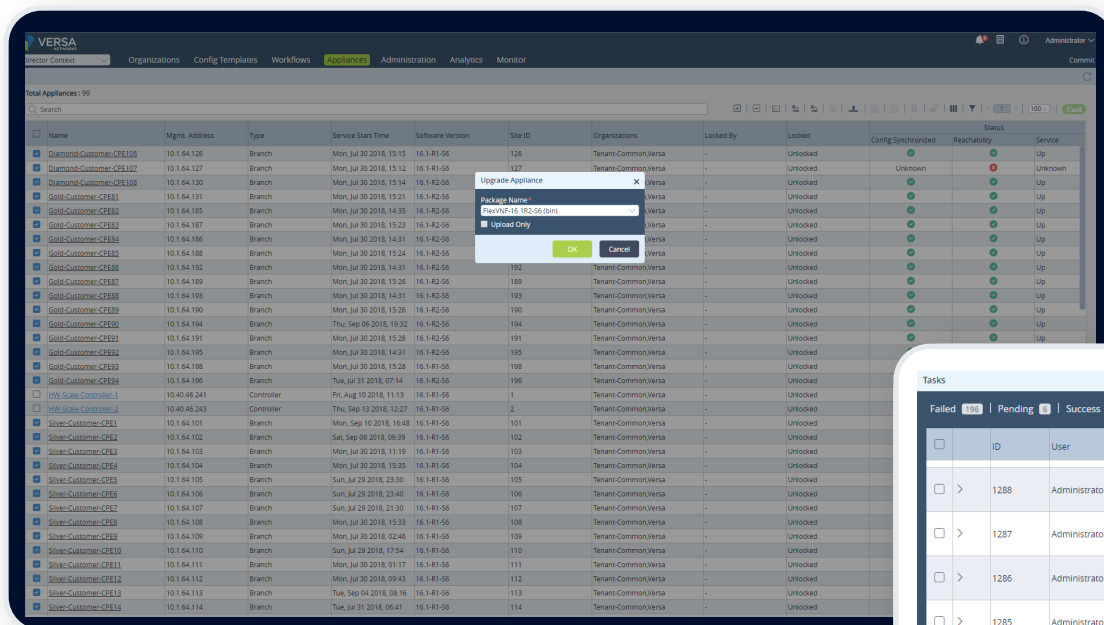
Upload VOS image in advance

- ✓ 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



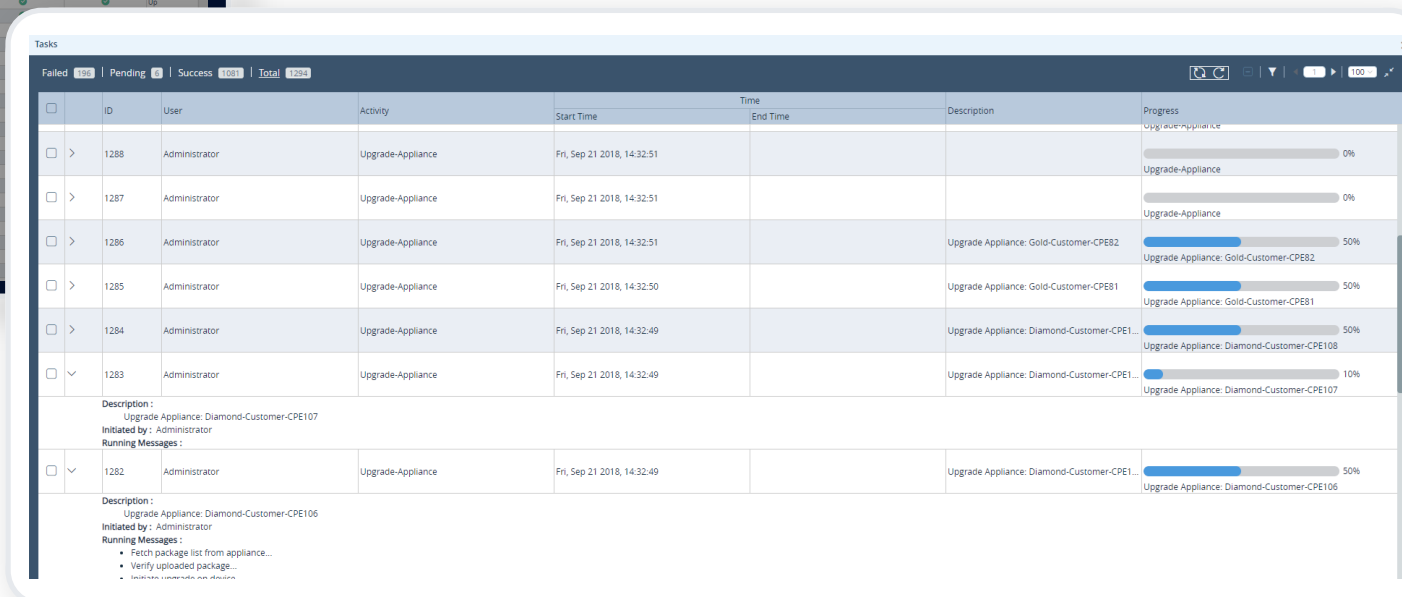
Installing VOS Image on Edge Devices

Parallel upgrade of devices from Versa Director



The image shows a screenshot of the Versa Director interface, specifically the 'Appliances' tab. A table lists various appliances with columns for Name, Mgmt. Address, Type, Service Start Time, Software Version, Site ID, Organizations, Locked By, Locked, Config Synchronization, Reachability, and Service. A modal window titled 'Upgrade Appliance' is open, showing a dropdown for 'Pushing Name' with 'Diamond-CPE107' selected and buttons for 'OK' and 'Cancel'.

Name	Mgmt. Address	Type	Service Start Time	Software Version	Site ID	Organizations	Locked By	Locked	Config Synchronization	Reachability	Service
Diamond-Customer-CPE106	10.1.64.126	Branch	Mon, Jul 30 2018, 15:15	16.1-R1-56	126	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Diamond-Customer-CPE107	10.1.64.127	Branch	Mon, Jul 30 2018, 15:12	16.1-R1-56	127	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Unknown
Diamond-Customer-CPE108	10.1.64.128	Branch	Mon, Jul 30 2018, 15:14	16.1-R1-56	128	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Gold-Customer-CPE81	10.1.64.131	Branch	Mon, Jul 30 2018, 15:21	16.1-R1-56	131	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Gold-Customer-CPE82	10.1.64.135	Branch	Mon, Jul 30 2018, 14:35	16.1-R1-56	135	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Gold-Customer-CPE83	10.1.64.187	Branch	Mon, Jul 30 2018, 15:23	16.1-R1-56	187	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Gold-Customer-CPE84	10.1.64.186	Branch	Mon, Jul 30 2018, 14:31	16.1-R1-56	186	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Gold-Customer-CPE85	10.1.64.188	Branch	Mon, Jul 30 2018, 15:24	16.1-R1-56	188	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Gold-Customer-CPE86	10.1.64.192	Branch	Mon, Jul 30 2018, 14:31	16.1-R1-56	192	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Gold-Customer-CPE87	10.1.64.189	Branch	Mon, Jul 30 2018, 15:26	16.1-R1-56	189	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Gold-Customer-CPE88	10.1.64.193	Branch	Mon, Jul 30 2018, 14:31	16.1-R1-56	193	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Gold-Customer-CPE89	10.1.64.190	Branch	Mon, Jul 30 2018, 15:26	16.1-R1-56	190	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Gold-Customer-CPE90	10.1.64.194	Branch	Thu, Sep 06 2018, 19:32	16.1-R1-56	194	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Gold-Customer-CPE91	10.1.64.191	Branch	Mon, Jul 30 2018, 15:26	16.1-R1-56	191	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Gold-Customer-CPE92	10.1.64.195	Branch	Mon, Jul 30 2018, 14:31	16.1-R1-56	195	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Gold-Customer-CPE93	10.1.64.198	Branch	Mon, Jul 30 2018, 15:28	16.1-R1-56	198	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Gold-Customer-CPE94	10.1.64.196	Branch	Tue, Jul 31 2018, 07:34	16.1-R1-56	196	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
HW-Steel-Controller-1	10.40.46.241	Controller	Fri, Aug 10 2018, 11:13	16.1-R1-56	1	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
HW-Steel-Controller-2	10.40.46.243	Controller	Thu, Sep 13 2018, 12:27	16.1-R1-56	2	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Silver-Customer-CPE1	10.1.64.101	Branch	Mon, Sep 10 2018, 16:48	16.1-R1-56	101	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Silver-Customer-CPE2	10.1.64.102	Branch	Sat, Sep 08 2018, 09:39	16.1-R1-56	102	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Silver-Customer-CPE3	10.1.64.103	Branch	Mon, Jul 30 2018, 11:19	16.1-R1-56	103	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Silver-Customer-CPE4	10.1.64.104	Branch	Mon, Jul 30 2018, 15:35	16.1-R1-56	104	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Silver-Customer-CPE5	10.1.64.105	Branch	Sun, Jul 29 2018, 23:30	16.1-R1-56	105	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Silver-Customer-CPE6	10.1.64.106	Branch	Sun, Jul 29 2018, 23:40	16.1-R1-56	106	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Silver-Customer-CPE7	10.1.64.107	Branch	Sun, Jul 29 2018, 21:30	16.1-R1-56	107	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Silver-Customer-CPE8	10.1.64.108	Branch	Mon, Jul 30 2018, 15:33	16.1-R1-56	108	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Silver-Customer-CPE9	10.1.64.109	Branch	Mon, Jul 30 2018, 02:46	16.1-R1-56	109	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Silver-Customer-CPE10	10.1.64.110	Branch	Sun, Jul 29 2018, 17:54	16.1-R1-56	110	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Silver-Customer-CPE11	10.1.64.111	Branch	Mon, Jul 30 2018, 01:17	16.1-R1-56	111	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Silver-Customer-CPE12	10.1.64.112	Branch	Mon, Jul 30 2018, 09:43	16.1-R1-56	112	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Silver-Customer-CPE13	10.1.64.113	Branch	Tue, Sep 04 2018, 08:16	16.1-R1-56	113	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up
Silver-Customer-CPE14	10.1.64.114	Branch	Tue, Jul 31 2018, 06:41	16.1-R1-56	114	Tenant-Common-Versa	-	Unlocked	Unknown	Up	Up



The image shows a screenshot of the Versa Director 'Tasks' tab. It displays a table of tasks with columns for ID, User, Activity, Start Time, End Time, Description, and Progress. The tasks are categorized by status: Failed (186), Pending (0), Success (1087), and Total (1294). The tasks are listed in descending order of ID. The progress bar for each task shows the percentage of completion.

ID	User	Activity	Start Time	End Time	Description	Progress
1288	Administrator	Upgrade-Appliance	Fri, Sep 21 2018, 14:32:51		Upgrade Appliance: Diamond-Customer-CPE107	0%
1287	Administrator	Upgrade-Appliance	Fri, Sep 21 2018, 14:32:51		Upgrade Appliance: Diamond-Customer-CPE108	0%
1286	Administrator	Upgrade-Appliance	Fri, Sep 21 2018, 14:32:51		Upgrade Appliance: Gold-Customer-CPE82	50%
1285	Administrator	Upgrade-Appliance	Fri, Sep 21 2018, 14:32:50		Upgrade Appliance: Gold-Customer-CPE81	50%
1284	Administrator	Upgrade-Appliance	Fri, Sep 21 2018, 14:32:49		Upgrade Appliance: Diamond-Customer-CPE108	50%
1283	Administrator	Upgrade-Appliance	Fri, Sep 21 2018, 14:32:49		Upgrade Appliance: Diamond-Customer-CPE107	10%
1282	Administrator	Upgrade-Appliance	Fri, Sep 21 2018, 14:32:49		Upgrade Appliance: Diamond-Customer-CPE106	50%

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

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



Versatility 2024

© 2024 Versa and/or its affiliates. All rights reserved. Versa Networks Confidential



Thank you

Versatility 2024

