Firewall Requirements

For supported software information, click here.

The functions of the Versa Networks solution are fully distributed among the headend devices—Director, Analytics, and Controller—and the Versa Operating System™ (VOS™) hub and branch devices. The headend devices might be colocated within a single data center or they might be distributed among multiple data centers. If your network has firewall devices, you must ensure that the ports required for the Versa Networks solution to operate are open so that the necessary communication between and among the Versa components can occur. If you use security zoning for the headend components, you must design your security policies so that they do not interfere with these communication channels.

This article lists the firewall requirements for Director, Analytics, Controller, and VOS (branch) devices, and for Versa Concerto, which is a component of the Versa self-service portal based for secure SD-WAN and SASE users.

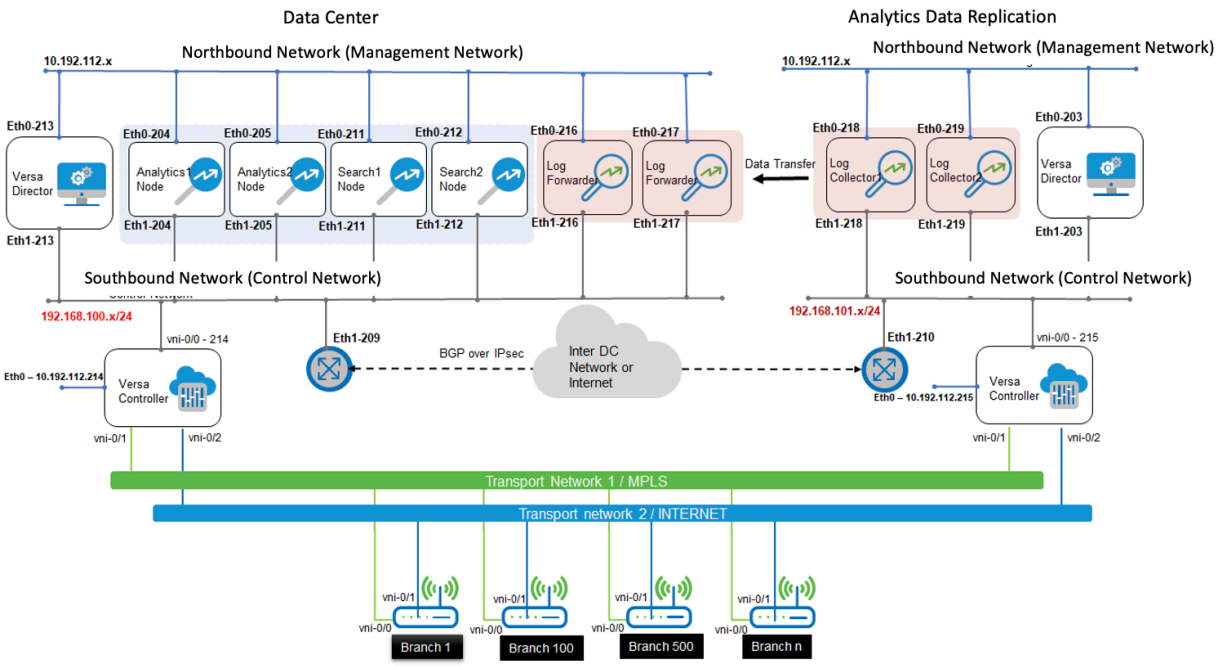
When discussing the firewall requirements for headend and VOS devices, the following terminology is used to describe the traffic direction:

- Inbound—Traffic flows from the network into the Versa headend or VOS device using the specified protocol and through the specified port or ports.
- Outbound—Traffic flows out from the Versa headend or VOS device to the network using the specified protocol and through the specified port or ports

When discussing the firewall requirements for headend devices, the following terminology is used to describe interfaces:

- Northbound network—Interface connects to the management network. You can use this interface to integrate with external services such as third-party orchestrators, automation tools, and OSS/BSS applications. On Analytics and Director nodes, the northbound interface is eth0.
- Southbound network—Interface connects to the network that is used to send control traffic for communication between the headend components and the VOS branch devices. On Analytics and Director nodes, the southbound interface is eth1.

The following topology shows an example of the northbound and southbound networks, illustrating how the interfaces on Versa Director, Analytics, and Controller nodes connect to these two networks. These interfaces are used for control traffic. The VOS branch devices and the Controller nodes connect to one or more transport networks, and these networks are used for data traffic.



Analytics Firewall Requirements

Analytics nodes use the following ports to communicate with other devices in the network. On an Analytics node, the northbound interface is eth0, which is the management interface, and the southbound interface is eth1.

Note that Versa Director and Versa Analytics nodes are management devices and thus send only control plane traffic. They do not route any data plane traffic. Only a VOS device can be configured as a router to route data traffic among its interfaces.

Purpose	Traffic Direction	Interface	Protocol	Port Numbers
Application port for REST access	Inbound	Northbound network	TCP	443 (Releases 21.1 and later), 8080 (before Release 21.1.0), 8443
Communication with Director node	Outbound	Southbound network	TCP, UDP	9182, 9183
DNS server, for reverse lookup	Outbound	Northbound or southbound, depending on location of DNS server	UDP	53
Intercluster database and client communication	—	Southbound network	TCP	7000, 7001, 7199, 8983, 9042, 9160 Release 20.x Fusion-specific: 2181, 2888, 3888
Log collector health monitor	Inbound	Southbound network	ICMP	
Log collector port where logs are received	Inbound	Southbound network	TCP	User configurable
Monitoring agent ports to retrieve health status and statistics about Analytics nodes	Inbound	Northbound network	TCP	8010, 8020
REST access port configuration and diagnostics of various services running on Analytics nodes	Inbound	Southbound network	TCP	5000, 5010, 8008
SMTP mail server, for reporting	Outbound	Northbound network	TCP	User configurable
Standard NTP, for time synchronization	Inbound	Northbound or southbound, depending on location of NTP	UDP	123

		server		
Standard SSH	Inbound	Northbound network	TCP	22
Troubleshooting and debugging of search engine using web portal	Inbound	Northbound network	TCP	8983

Concerto Firewall Requirements

Concerto orchestrator uses the following ports to access and communicate with other devices in the network.

Purpose	Traffic Direction	Protocol	Port Numbers
Docker control plane communication, for communication between nodes within the Concerto cluster	Inbound	TCP, UDP	7946
Docker swarm cluster	Inbound	TCP	2377
Encapsulating Security Payload (ESP) for Docker overlay	Inbound	IP	—
GlusterFS cluster	Inbound	TCP	24007
GlusterFS rpcbind	Inbound	TCP	111
GlusterFS service port corresponding to brick	Inbound	TCP	49152
HTTP	Inbound	TCP	80
HTTPS	Inbound	TCP	443
Kafka brokers client for Concerto cluster	Inbound	TCP	9092 - (9091 + *i*), where *i* is the number of Concerto nodes in the cluster
Overlay network traffic	Inbound	UDP	4789

Purpose	Traffic Direction	Protocol	Port Numbers
SSH	Inbound	TCP	22
Zookeeper client for Concerto cluster	Inbound	TCP	2181

Director Firewall Requirements

To allow seamless connectivity among the devices across intermediary firewalls and routing elements, ensure that the ports listed in the following table are open on the Director node. On a Director node, the northbound interface is eth0, which is the management interface, and the southbound interface is eth1.

Note that Versa Director and Versa Analytics nodes are management devices and thus send only control plane traffic. They do not route any data plane traffic. Only a VOS device can be configured as a router to route data traffic among its interfaces.

Purpose	Traffic Direction	Interface	Protocol	Port Numbers
Access between active and standby Director nodes, to share HA-related information from the NCS database—Open only between the active and standby Director nodes; block the ports to other systems.	Inbound	Northbound or southbound network, but preferably southbound	TCP	4566, 4570
Access between active and standby Director nodes, to share HA-related information from the PostgreSQL database—Open only between the active and standby Director nodes; block the ports to other systems.	Inbound	Southbound network, especially if Northbound network is public-facing	TCP	5432
Access between	Inbound	Northbound or	IP (protocol 50)	—

Purpose	Traffic Direction	Interface	Protocol	Port Numbers
active and standby Director nodes, when secure mode is enabled in Director using Encapsulating Security Payload (ESP)		southbound network, but preferably southbound or, interface or IP address on which high availability is enabled		
Access between active and standby Director nodes, when secure mode is enabled in Director for IPsec IKE—Open only between the active and standby Director nodes; block the ports to other systems.	Inbound	Northbound or southbound network, but preferably southbound or, interface or IP address on which high availability is enabled	UDP	500, 4500
HTTPS access to Director GUI from any host	Inbound	Northbound network	TCP	443
HTTPS REST API—Access from Analytics node, Concerto nodes, VMS nodes, and peer Directors. Additionally, if the Director acts as a central authentication server, allow access from central-auth client.	Inbound	Northbound or southbound, depending on topology	TCP	9182, 9183
If central authentication method is used, allow HTTPS REST API access to the central authentication server.	Outbound	Northbound or southbound, depending on the API access interface	TCP	9182, 9183
Netconf	Outbound	Southbound network	TCP	2022

Purpose	Traffic Direction	Interface	Protocol	Port Numbers
communication with CPE devices over the overlay network				
Receive alarms from Analytics node	Inbound	Northbound or southbound, depending on topology	TCP, UDP	20514
REST API communication with CPE devices over the overly network	Outbound	Southbound network	TCP	8443
SSH access between the Analytics and Director nodes, and communication between HA-enabled Director nodes for replication; required for access from Director node to VOS branch, for ZTP	Inbound	Northbound or southbound,	TCP	22
uCPE VM console access to Director GUI from any host—Open only if you need uCPE access; otherwise, block the port.	Inbound	Northbound network	TCP	6080
uCPE VNF proxy access to Director GUI from any host—Open only if you need uCPE access; otherwise, block the port.	Inbound	Northbound network	TCP	9090

VOS Device Firewall Requirements

VOS devices use the following WAN network ports to communicate with Director, Analytics, and Controller nodes, as well as with other devices in the network. Note that a Versa Controller device is simply a VOS instance.

Purpose	Traffic Direction	Protocol	Port Numbers
Certificate access	Inbound	TCP	8080
Encapsulating Security Payload (ESP)	Both	IP (protocol 50)	—
High availability (HA) between HA-enabled VOS nodes	Both	TCP and UDP	TCP ports: 1024 through 1120, 3000 through 3003, 9878 UDP ports: 3002, 3003
IPsec IKE	Both	UDP	500, 4500
Management interface that has the public IP address, for CMS-based cloud deployment. Note that after deploying the cloud VOS branch/ hub-controller with the CMS connector, you must remove the public IP address of eth0 from the cloud instance portal. The Director node will manage the VOS branch/hub-controller using the SD-WAN overlay IP address, and will not use the eth0 public IP address. Additionally, you must change the default passwords for all cloud-hosted VOS nodes, for admin and versa accounts.	Inbound Both Both	TCP TCP ICMP	2022 22 —
Netconf from Director node to VOS device	Inbound	TCP	2022

Purpose	Traffic Direction	Protocol	Port Numbers
Resolve FQDN of staging Controller node	Outbound	TCP	53
REST port, for fetching operational information from VOS device	Inbound	TCP	8443
Speed test	Both	TCP	5201
SSH; required for access between VOS branch and Director node, for ZTP; optional on other ports, such as management, WAN, and LAN	Both	TCP	22
URL-based ZTP	Both	ICMP	—
VXLAN communication between VOS hub, VOS branch, and Controller device	Both	UDP	4790
VXLAN communication between VOS hub, VOS branch, and Controller devices for HA setups that have cross-connect links (failover pool created using CGNAT)	Both	UDP	Default port range: 1024 through 32000

VMS Firewall Requirements

For Releases 21.2.1 and later.

Versa Messaging Service (VMS) uses the following control node and worker node ports to access and communicate with other devices in the network.

VMS Control Nodes

Purpose	Traffic Direction	Protocol	Port Numbers	Used By	Interfaces
etcd server client	Inbound	TCP	2379 through	etcd, kube-	All

Purpose	Traffic Direction	Protocol	Port Numbers	Used By	Interfaces
API			2380	apiserver	
Kube controller manager	Inbound	TCP	10252	Self	All
Kube scheduler	Inbound	TCP	10251	Self	All
Kubelet API	Inbound	TCP	10250	Self, control plane	All
Kubernetes API server	Inbound	TCP	6443	All	Management

VMS Worker Nodes

Purpose	Traffic Direction	Protocol	Port Numbers	Used By	Interfaces
Communication between Active Directory and WMI	Inbound	TCP	389	WMI	All
Communication with Director node	Outbound	TCP, UDP	9182, 9183	VMS, for API calls to Director node	All
In-memory database	Inbound	TCP	6379	VOS device	Internal only
Kubelet API	Inbound	TCP	10250	Self, control plane	All
Message server, HA	Inbound	TCP	3074, 3101, 3102	VOS device	All
Node port services	Inbound	TCP	30000 through 32767	All	Internal
Versa Director connector	Inbound	TCP	8080	VOS device	Internal only
Versa package service	Inbound	TCP	443	VOS device	All
Versa passive authentication application	Inbound	TCP	7000	VOS device	Internal only
Versa passive authentication collector, for port between WMI	Inbound	TCP	3092	WMI	All

(client) and VMS (server)					

Additional Security Hardening

For security reasons, Versa recommends that you allow inbound traffic from authorized IP addresses only. The following two examples illustrate types of inbound traffic to allow:

- You should open port 22 (for TCP) only for the IP addresses of devices from which you connect to the Versa component for management purposes.
- You should allow communication between headend components, such two Versa Directors in a high availability (HA) deployment, only from the IP addresses of the headend components. For example, if the southbound IP addresses are 10.0.0.1 for the active Director node and 20.0.0.1 for the standby Director node, the standby Director node should allow access to its ports 4566, 4570 and 5432 only from the IP address of the active Director node (10.0.0.1).

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Releases 21.2.1 and later support Versa Messaging Service (VMS).
- Releases 22.1.4 and later allow inbound access to ports 9182 and 9183 between HA pair Directors.

Additional Information

Enable Secure Mode
Install Concerto
Perform Initial Software Configuration