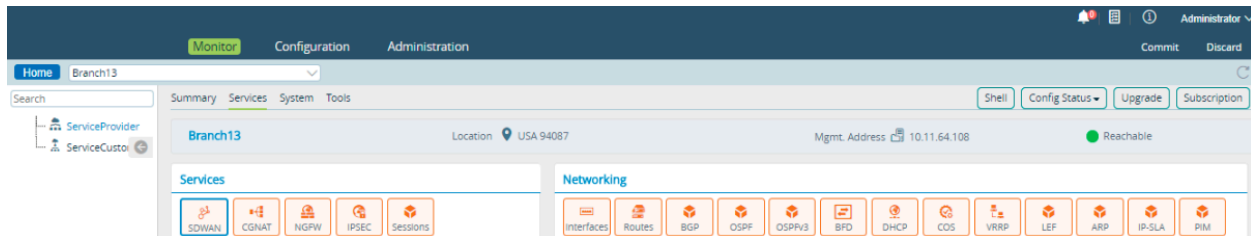


Monitor Device Services

 For supported software information, click [here](#).

To monitor device services that are running on a Versa Operating System™ (VOS™) device:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Monitor tab in the top menu bar.
3. Select the provider organization in the left menu bar.
4. Select the Services tab in the horizontal menu bar.



The Services tab has the following sections:

- Networking
- Services

This article describes the Services sections on the Services tab.

Services > SD-WAN

Click the SD-WAN tab. This tab displays the following tabs:

- Aggregate Traffic
- Application Metrics
- Forwarding Profiles
- Policies

- Sessions
- Sites
- SLA End-to-End Paths
- SLA Metrics
- SLA Paths
- Transport Paths

Aggregate Traffic

Click SD-WAN > Aggregate Traffic and then select a Controller or branch device to view its aggregate traffic and the incoming and outgoing bytes and packets.

Aggregate Traffic
Application Metrics
Forwarding Profiles
Policies
Sessions
Sites
SLA End To End Paths
SLA Metrics
SLA Paths
Transport Paths
Web Proxy

SDWAN-Branch2

Search

Ptvi Index	Encap Type	Rx Pkts	Rx Bytes	Tx Pkts	Tx Bytes
1246	plaintext	0	0	0	0
1247	encrypted	114756	20654224	114756	20654224

Application Metrics

Click SD-WAN > Application Metrics to display application metrics.

Forwarding Profiles

A forwarding profile determines the traffic path based on real-time SLA performance of traffic. The profile defines the properties of WAN circuits to be selected for traffic. It defines properties, such as the load balancing method to be used for traffic, priority of circuits, circuit type (broadband or MPLS), circuit media, and other associated attributes.

Click SD-WAN > Forwarding Profiles to displays the forwarding profile statistics. The data includes the profile name, hit count, valid link drop count, SLA fail drop count, SLA fail forward count, and turn redirect count.

Aggregate Traffic
Application Metrics
Forwarding Profiles
Policies
Sessions
Sites
SLA End To End Paths
SLA Metrics
SLA Paths
Transport Paths
Web Proxy

Search

Clear

Name	Hit Count	No Valid Link Drop Count	SLA Fail Drop Count	SLA Fail Fwd Count	Turn Redirect Count
Default-FP	0	0	0	0	0
yahoo-forwarding-profile	0	0	0	0	0

Click a policy name to view its configuration in CLI format.

Configuration : yahoo-forwarding-profile

```
{
- forwarding-profile: {
  name: "yahoo-forwarding-profile",
  sla-profile: "sla-yahoo",
  connection-selection-method: "weighted-round-robin",
  sla-violation-action: "forward",
  evaluate-continuously: "disable",
  recompute-timer: 300,
  encryption: "optional",
  symmetric-forwarding: "enable"
}
}
```

Close

Policies

Click SD-WAN > Policies and then select a policy to view statistics about SD-WAN policies.

Sites Aggregate Traffic Transport Paths SLA Paths SLA Metrics Policies Forwarding Profiles Sessions MOS

policy ||| ▼ Clear

Rule Name ↕		Hit Count	Tx Pkts Tunnel	Tx Bytes Tunnel	Rx Pkts Tunnel	Rx Bytes Tunnel
rule2	👁	0	0	0	0	0
rule1	👁	0	0	0	0	0

Click the 👁 Eye icon to view details.

Sites Aggregate Traffic Transport Paths SLA Paths SLA Metrics Policies Forwarding Profiles Sessions MOS

policy ||| ▼ | Clear

Rule Name	Hit Count	Tx Pkts Tunnel	Tx Bytes Tunnel	Rx Pkts Tunnel	Rx Bytes Tunnel
rule2	Statistics	Remote Branch	Controller1		

Circuit

Local Circuit	Remote Circuit	Hit Count	Tx Pkts Tunnel	Tx Bytes Tunnel	Rx Pkts Tunnel	Rx Bytes Tunnel
BB1	BB1	0	0	0	0	0
BB1	BB2	0	0	0	0	0
BB1-v6	BB1-v6	0	0	0	0	0
BB1-v6	BB2-v6	0	0	0	0	0
BB2	BB1	0	0	0	0	0
BB2	BB2	0	0	0	0	0
BB2-v6	BB1-v6	0	0	0	0	0
BB2-v6	BB2-v6	0	0	0	0	0
MPI S	MPI S	0	0	0	0	0

Remote Branch : Controller1

Click a rule name to view its configuration in CLI format.

Configuration : rule2

```

{
  - sdwan:rule: {
    name: "rule2",
    - match: {
      - source: {
        - user: {
          - local-database: {
            status: "disabled"
          },
          user-type: "any"
        }
      }
    },
    - set: {
      action: "allow",
      - lef: {
        profile-default: false,
        event: "never",
        rate-limit: 10
      }
    },
    - monitor: {
      interval: 3,
      threshold: 5
    }
  }
}

```

Close

Sessions

Click SD-WAN > Sessions to displays SD-WAN session details, including the total number of SD-WAN sessions, number of sessions created, and the number of sessions closed.

Search

SD-WAN Session Count	SD-WAN Session Created	SD-WAN Session Closed
0	0	0

Click the  Eye icon to view the filter session data.

Session Filter

Session Search Criteria

Session Type

SDWAN

Source IP Address/Prefix

Source Port

Destination IP Address/Prefix

Destination Port

Protocol

Predefined Application

Predefined URL Category

Filter

Sites

Click SD-WAN > Sites to display details about SD-WAN sites.

Services

SDWAN

NGFW

CGNAT

IPSEC

Sessions

Networking

Interfaces

Routes

BGP

OSPF

OSPFv3

BFD

DHCP

DNS Stats

COS

VRRP

LEF

ARP

IP-SLA

Endpoints


PIM

IGMP

Aggregate Traffic Application Metrics Forwarding Profiles Policies Sessions Sites SLA End To End Paths SLA Metrics SLA Paths Transport Paths Web Proxy

Search

Site Name	Management IP	Type	Up Time	Connectivity Status	Controller
SDWAN-Branch1	10.1.64.106	local	1d:2h:13m:30s	-	no
SDWAN-Branch2	10.1.64.104	remote	1d:2h:11m:21s	Connected	no
SDWAN-Branch4	10.1.64.108	remote	1d:2h:11m:21s	Connected	no
SDWAN-Branch5	10.1.64.101	remote	1d:2h:11m:21s	Connected	no
SDWAN-Controller1	10.1.64.1	remote	1d:2h:11m:21s	Connected	yes
SDWAN-Controller2	10.1.64.2	remote	1d:2h:11m:21s	Connected	yes

Click the 

SDWAN-Branch1																
Connectivity Status :				-				ESP Local IP :				10.1.64.106				
ESP Remote IP :				10.1.64.106				Management IP :				10.1.64.106				
Site Chassis ID :				A96067ac-35f3-4764-93d8-8e25d530d1c4				Site ID :				106				
Site Name :				SDWAN-Branch1				Site Network ID :				1				
Site SA :				Yes				Site Type :				Hub-Controller				
Up Time :				1d:2h:23m:9s				VXLAN Local IP :				10.1.0.106				
VXLAN Remote IP :				10.1.0.106												
Link	Circuit Family	Circuit Name	Link ID	Endpt IP	NAT Status	Public IP	Public Port	Datapath IP	Datapath Port	Link Encryption	Shaping Rate	Min Shaping R...	Tx Domain 1			
link1	ipv4	WAN1	1	192.168.11.101	true	101.101.101.1	56952	101.101.101.1	56952	optional	0	0	TD_Internet			
link2	ipv4	WAN2	2	192.168.12.101	true	101.101.102.1	62674	101.101.102.1	62674	optional	0	0	TD_Internet			
link3	ipv4	WAN3	3	192.168.13.101	false	192.168.13.101	4790	192.168.13.101	4790	optional	0	0	TD_Mpls			

SLA End-to-End Paths

Click SD-WAN > SLA End-to-End Paths.

SLA Metrics

Click SD-WAN > SLA Metrics to display SLA metrics.

Aggregate Traffic

Application Metrics

Forwarding Profiles

Policies

Sessions

Sites

SLA End To End Paths

SLA Metrics

SLA Paths

Transport Paths

Controller1

Search

|||

▼

Path Handle	Fwd Class	Local WAN Link	Remote WAN Li...	Local WAN Link ...	Remote WAN Li...	Two Way Delay...	Fwd Delay Var...	Rev Delay Var...	PDU Loss Ratio(...	Fwd Loss
70144	fc_nc	MPLS	MPLS	1	2	2	8	8	0.0	0.0
73984	fc_nc	Internet	Internet	2	1	2	7	7	0.0	0.0

SLA Paths

Click SD-WAN > SLA Paths to display SLA path status, including local site name, remote site name, local/remote WAN link names, forwarding class names, and connectivity status.

Aggregate Traffic

Application Metrics

Forwarding Profiles

Policies

Sessions

Sites

SLA End To End Paths

SLA Metrics

SLA Paths

Transport Paths

Controller1

Search

Path Handle	Fwd Class	Local WAN Link	Remote WAN Link	Local WAN Link ID	Remote WAN Lin...	Adaptive Monito...	Conn State	Flaps	Last Flapped
70144	fc_nc	MPLS	MPLS	1	2	disable	up	2	4d14h09m
73984	fc_nc	Internet	Internet	2	1	disable	up	648	1d10h51m

Transport Paths

Click SD-WAN > Transport Paths to display the amount of data that has been sent from a source to a destination.

Controller1

Search

Local Ackt Name	Remote Ackt Name	Encap Type	Local IP	Remote IP	Rx Pkts	Rx Bytes	Tx Pkts	Tx Bytes
MPLS	MPLS	plaintext	10.0.128.102	10.0.128.1	60	13985	93	28724
Internet	Internet	plaintext	10.0.128.102	10.0.128.1	4	424	20	9282
MPLS	MPLS	encrypted	10.0.192.102	10.0.192.1	431432	64672448	844104	329792304
Internet	Internet	encrypted	10.0.192.102	10.0.192.1	76063	14011000	110679	20364904

Services > CGNAT

CGNAT is a large-scale NAT that translates multiple private IPv4 addresses to a limited number public IPv4 addresses using Network Address and Port Translation (NAPT). In CGNAT, only port translation of source address is required for packets communicating from the network to outside. Port translation of destination address is not implemented.

CGNAT can replace NAT devices in enterprise networks. Using CGNAT, you can deliver seamless IPv4 connectivity even while using limited public addresses. You can define private IPv4 address in your network and use Versa CGNAT to manage address translation to the public IPv4 addresses.

Click the CGNAT tab. This tab has the following tabs:

- Rules
- Pools
- Sessions

Rules

Click CGNAT > Rules to display information about CGNAT rules.

Services					Networking														
SDWAN	NGFW	CGNAT	IPSEC	Sessions	Interfaces	Routes	BGP	OSPF	OSPFv3	BFD	DHCP	DNS Stats	COS	VRRP	LEF	ARP	IP-SLA	Endpoints	
					PIM	IGMP													
Pools																			
Rules																			
Name	Hit Count	Forward Pkt Count	Forward Byte Count	Reverse Pkt Count	Reverse Byte Count														
DIA-Rule-Tenant1-LAN-VR-WAN1	0	0	0	0	0														
DNAT-WAN1-Inbound	0	0	0	0	0														
RFC 1918 NoTranslate	0	0	0	0	0														

Click a rule name view its configuration.

Pools

Click CGNAT > Pools to display pool details.

Services

SDWAN

NGFW

CGNAT

IPSEC

Sessions

Networking

Interfaces

Routes

BGP

OSPF

OSPFv3

BFD

DHCP

DNS Stats

COS

VRRP

LEF

ARP

IP-SLA

Endpoints

PIM

IGMP

Pools

Rules

Sessions

Search

III

▼

◀

1

▶

50▼

Pool Usage	Range Low	Range Name	Name	Range High	Any Alloc Failures	Provider Org	Any Free Failures	Routing Instance
0.0			DIA-Pool-WAN1		0	provider-org	0	WAN1-Transport-VR
0.0	172.16.11.10	range-WAN1-inbound	DNAT-WAN1-inbound	172.16.11.10	0	provider-org	0	Tenant1-LAN-VR
0.0	10.10.12.20	range-DNAT-44	DNAT_test	10.10.12.20	0		0	

Click a pool name to view its configuration.

Sessions

Click CGNAT > Sessions to display NAT session details.

Services

SDWAN

NGFW

CGNAT

IPSEC

Sessions

Interfaces

Routes

BGP

OSPF

OSPFv3

BFD

DHCP

DNS Stats

COS

VRRP

LEF

ARP

IP-SLA

Endpoints

PIM

IGMP

Pools

Rules

Sessions

Search

Clear

NAT Session Count	NAT Session Created	NAT Session Closed	NAT Session Failed
0	0	0	0

Click the  Eye icon to filter sessions.

Session Filter

Session Search Criteria

Session Type

SDWAN

Destination Port

Source IP Address/Prefix

Protocol

Source Port

Predefined Application

Destination IP Address/Prefix

Predefined URL Category

Filter

Services > IPsec

The Internet Protocol Security (IPsec) is a set of protocols that secure communications over IP networks by deploying cryptographic encryption services. IPsec provides the following security services:

- Authenticity

https://docs.versa-networks.com/Management_and_Orchestration/Versa_Director/Monitoring_with_Versa_Director/Monitor_D...

Updated: Thu, 24 Oct 2024 10:47:29 GMT

Copyright © 2024, Versa Networks, Inc.

- Integrity
- Confidentiality
- Replay protection

Click the IPsec tab. This tab displays the following tabs:

- Branch to Branch
- IKE History
- IKE Security Association
- IPsec History
- IPsec Security Association
- Overview
- Profile Statistics

IPsec Branch to Branch

Click IPsec > Branch to Branch and select an entity to view connection details.

Services

SDWAN

NGFW

CGNAT

IPSEC

Sessions

Networking

Interfaces

Routes

BGP

OSPF

OSPFv3

BFDD

DHCP

DNS Stats

COS

VRRP

LEF

ARP

IP-SLA

Endpoints

PIM

IGMP

Branch To Branch

IKE History

IKE Security Association

IPSec History

IPSec Security Association


Overview

Profile Statistics

SDWAN-Controller1-Profile

Search

Peer Addr	Inbound SPI	In Bytes Rate	Outbound SPI	Out Bytes Rate	Cipher	Up Time	Next Rekey Time	Tunnel Status
10.1.0.108	0x501b006c	167	0x505b006a	0	aes-gcm	1d04h10m	01:33:53	UP
10.1.0.104	0x501b0068	171	0x505b006a	0	aes-gcm	1d04h10m	01:33:53	UP
10.1.0.101	0x501b0065	182	0x505b006a	0	aes-gcm	1d04h10m	01:33:53	UP

Click the  Eye icon to view details.

10.1.0.108

Anti Replay :	Enable	Cipher :	Aes-Gcm
Dst Port :	0	Dst Prfx Len :	0
Hmac :	None	In Anti-Replay Dup :	0
In Anti-Replay OOO :	0	In Bytes :	17082938
In Drop Anti-Replay :	0	In Drop MAC :	0
In Invalid :	0	In Pkts :	161173
In Plain :	161173	In Bytes Rate :	1017
In Pkts Rate :	9	Inbound SPI :	0x501b006c
IPSec Mode :	Tunnel	IPSec Protocol :	Esp
Key Length :	128	Local Addr :	10.1.0.106
Local Auth Type :	Psk	Local ID String :	SDWAN-Branch1@Tenant1.Com

IKE History

Click IPsec > IKE History and then select an entity to view its IKE history.

Services

SDWANNGFWCGNATIPSECSessions

Networking


InterfacesRoutesBGPOSPFOSPFv3BFDDHCPDNS StatsCOSVRRPLEFARPIP-SLAEndpointsPIMIGMP

Branch To BranchIKE HistoryIKE Security AssociationIPSec HistoryIPSec Security AssociationOverviewProfile Statistics

SDWAN-Controller1-Profile

Local AddrPeer AddrLast StatusLast Status Timestamp

10.1.0.10610.1.0.1Active (Rekey)2019-11-20T11:52:12.493649-08:00

Click the  Eye icon to view details.

10.1.0.1

Events

Index	Timestamp	Type	Inbound SPI	Outbound SPI
0	2019-11-20T09:16:41.898237-08:00	IPsec Rekey	0x2002ea7	0x20064a2
1	2019-11-20T02:13:23.059658-08:00	IPsec Rekey	0x2002a02	0x2003534
2	2019-11-19T19:10:04.824004-08:00	IPsec Rekey	0x2000996	0x2004ad5
3	2019-11-19T12:06:34.133966-08:00	IPsec Done	0x2000f7a	0x2000a36

Last Status : Active (Rekey)Last Status Timestamp : 2019-11-20T09:16:41.898236-08:00

Local Addr : 10.1.0.106Peer Addr : 10.1.0.1

IKE Security Association

Click IPsec > IKE Security Association and then select an entity to view its IKE security details.

Services

SDWANNGFWCGNATIPSECSessions

Networking


InterfacesRoutesBGPOSPFOSPFv3BFDDHCPDNS StatsCOSVRRPLEFARPIP-SLAEndpointsPIMIGMP

Branch To BranchIKE HistoryIKE Security AssociationIPSec HistoryIPSec Security AssociationOverviewProfile Statistics

SDWAN-Controller1-Profile

Tunnel IDRemote GatewayVSNIKE VersionLocal GatewayLocal SPIRemote SPICipherAuthenticationVpn TypeFlags

210.1.0.100v210.1.0.1060x2005f292c14d1ed0x2006afffad91171aes256-cbchmac-sha256-128branch-sdwanP I

Click the  Eye icon to view details.

Cipher :	Aes256-Cbc	Dh Group :	Mod19
Flags :	P I	Hmac :	Hmac-Sha256-128
IKE Version :	V2	Local Auth Type :	Psk
Local Gateway :	10.1.0.106	Local ID String :	SDWAN-Branch1@Tenant1.Com
Local ID Type :	Email	Local SPI :	0x2005f292c14d1ed
Negotiation Life Time :	28800	Peer Auth Type :	Psk
Peer ID String :	SDWAN-Controller1@Tenant1.Com	Peer ID Type :	Email
Remaining Life Time :	12304	Remote Gateway :	10.1.0.1
Remote SPI :	0x2006affad91171	Tunnel ID :	2
Vpn Type :	Branch-Sdwan	VSN :	0

IPsec History

Click IPsec > IPsec History and then select an entity to view its IPSEC history details.

Services

SDWAN
NGFW
CGNAT
IPSEC
Sessions

Networking

Interfaces
Routes
BGP
OSPF
OSPFv3
BFD
DHCP
DNS Stats
COS
VRRP
LEF
ARP
IP-SLA
Endpoints
PIM
IGMP

Branch To Branch
IKE History
IKE Security Association
IPSec History
IPSec Security Association
Overview
Profile Statistics

SDWAN-Controller1-Profile

Search

Local Addr	Peer Addr	Last Status	Last Status Timestamp
10.1.0.106	10.1.0.1	Active (Rekey)	2019-11-20T09:16:41.898236-08:00

Click the  Eye icon to view details.

Timestamp	Index	Outbound SPI	Type	Inbound SPI
2018-02-05T01:40:44.813943-08:00	0	0x2003044	IPsec Rekey	0x200032a
2018-02-04T18:53:29.338991-08:00	1	0x20078d8	IPsec Done	0x200245b
2018-02-04T11:56:22.440872-08:00	2	0x20065ee	IPsec Done	0x20075a9
2018-02-04T04:59:10.921681-08:00	3	0x2000817	IPsec Done	0x2003de7
2018-02-03T22:02:06.602725-08:00	4	0x2001e4b	IPsec Rekey	0x2000be3
2018-02-03T15:14:39.025694-08:00	5	0x2006bc0	IPsec Done	0x2000b5a

IPsec Security Association

Click IPsec > IPsec Security Association and then select an entity to view the security association details.

Services

SDWAN
NGFW
CGNAT
IPSEC
Sessions

Networking

Interfaces
Routes
BGP
OSPF
OSPFv3
BFD
DHCP
DNS Stats
COS
VRRP
LEF
ARP
IP-SLA
Endpoints
PIM
IGMP

Branch To Branch
IKE History
IKE Security Association
IPSec History
IPSec Security Association
Overview
Profile Statistics

SDWAN-Controller1-Profile

Search

Peer Addr	Inbound SPI	In Bytes Rate	Outbound SPI	Out Bytes Rate	Cipher	Up Time	Next Rekey Time	Tunnel Status
10.1.0.1	0x2002ea7	129	0x20064a2	0	aes-gcm	1d04h25m	00:07:39	UP

https://docs.versa-networks.com/Management_and_Orchestration/Versa_Director/Monitoring_with_Versa_Director/Monitor_D...

Updated: Thu, 24 Oct 2024 10:47:29 GMT

Copyright © 2024, Versa Networks, Inc.

Click the  Eye icon to view details.

10.1.0.1			
Anti Replay :	Enable	Cipher :	Aes-Gcm
Dst Port :	0	Dst Prfx Len :	0
Hmac :	None	In Anti-Replay Dup :	0
In Anti-Replay OOO :	0	In Bytes :	12286
In Drop Anti-Replay :	0	In Drop MAC :	0
In Invalid :	0	In Pkts :	128
In Plain :	128	In Bytes Rate :	132
In Pkts Rate :	1	Inbound SPI :	0x20056c0
IPSec Mode :	Tunnel	IPSec Protocol :	Esp
Key Length :	128	Local Addr :	10.1.0.106
Local Auth Type :	Psk	Local ID String :	SDWAN-Branch1@Tenant1.Com

Overview

Click IPsec > Overview to display IPsec packet details.

Services				Networking			
SDWAN	NGFW	CGNAT	IPSEC	Sessions	Interfaces	Routes	BGP
					OSPF	OSPFv3	BFD
					DHCP	DNS Stats	COS
					VRP	LEF	ARP
					IP-SLA	Endpoints	
					PIM	IGMP	
Branch To Branch IKE History IKE Security Association IPsec History IPsec Security Association Overview Profile Statistics							
Inbound Statistics							
ESP/AH Bytes	AH Packets	Anti-replay failu...	Anti-replay failu...	Packets droppe...	Packets droppe...	Packets droppe...	Packets droppe...
67896099	0	0	0	0	0	0	0

Profile Statistics

Click IPsec > Profile Statistics and then select an entity to view profile statistics.

Services				Networking			
SDWAN	NGFW	CGNAT	IPSEC	Sessions	Interfaces	Routes	BGP
					OSPF	OSPFv3	BFD
					DHCP	DNS Stats	COS
					VRP	LEF	ARP
					IP-SLA	Endpoints	
					PIM	IGMP	
Branch To Branch IKE History IKE Security Association IPsec History IPsec Security Association Overview Profile Statistics							
SDWAN-Controller1-Profile							
Inbound Statistics							
ESP/AH Bytes	AH Packets	Anti-replay failu...	Anti-replay failu...	Packets droppe...	Packets droppe...	Packets droppe...	Packets droppe...
13339693	0	0	0	0	0	0	0

Services > NGFW

Next-generation firewall (NGFW) policy includes all the match criteria of a stateful firewall policy, in addition to Layer 7 match criteria such as application and URL category. The application for a session is automatically determined based on

various identification methods, such as applying signatures, heuristics, and statistical identification. NGFW supports more than 3,000 predefined applications and more than 80 URL categories.

NGFW supports creation of custom applications and custom URL categories by the customer. NGFW policy rules can be specified based on predefined and/or custom application/URL categories.

Click the NGFW tab. This tab displays the following tabs:

- Antivirus
- Decryption
- DoS Policies
- File Filtering
- IP Filtering
- Persistent Action
- Policies
- Security Packages
- Sessions
- URL Filtering
- Vulnerability
- Vulnerability Signature
- Zone Protection

Antivirus

VOSdevices have a built-in antivirus engine. At least one antivirus profile needs to be configured to enable scanning of files for viruses. In the Next Generation Firewall Policy Rule, one of the enforcement actions available is to enable an antivirus profile. For all traffic that matches the security policy rule, the antivirus profile will be applied if configured.

Click NGFW > Antivirus, and then select the antivirus type the scanning profile, and the profile type.

Services

SDWAN

NGFW

CGNAT

IPSEC

Sessions

Networking

Interfaces

Routes

BGP

OSPF

OSPFv3

BFD

DHCP

DNS Stats

COS

VRRP

LEF

ARP

IP-SLA

Endpoints

PIM

IGMP

Anti Virus

Decryption

DoS Policies

File Filtering

IP Filtering

Persistent Action

Policies

Security Packages

Sessions

URL Filtering

User Identification

Vulnerability

Vulnerability Signature

Web Proxy

Zone Protection

Predefined Profile

Scan Web and Email Traffic

predefined-protocol

Page 1 of 1

protocol	av-flows-blocked	av-flows-allowed	av-num-ctx-switch
http	0	0	0
ftp	0	0	0
smtp	0	0	0
imap	0	0	0
pop3	0	0	0
mapi	0	0	0

Decryption

NGFW enables decryption of SSL traffic to detect malware and other suspicious data or prevent confidential data from leaving your organization. The Decryption tab displays statistics of SSL traffic across multiple parameters.

Click NGFW > Decryption and then select a decryption filter:

- Global—Display all decryption data for the organization.
- Profile—Display the decryption data for user-defined profiles.
- Policy—Display the decryption data for user-defined policies.

The screenshot shows the NGFW interface with the 'Decryption' tab selected. The 'Global' filter is chosen. The table displays the following data:

Name	Err Sess Connect	Err Svc Connect	SSL Adc Sess	SSL APP Err	SSL Close	SSL Create	SSL Decrypt	SSL Encrypt	SSL Events	SSL Free	SSL Pxy Ignore	SSL Pxy Sess
global-stats	0	0	0	0	0	0	0	0	0	0	0	0

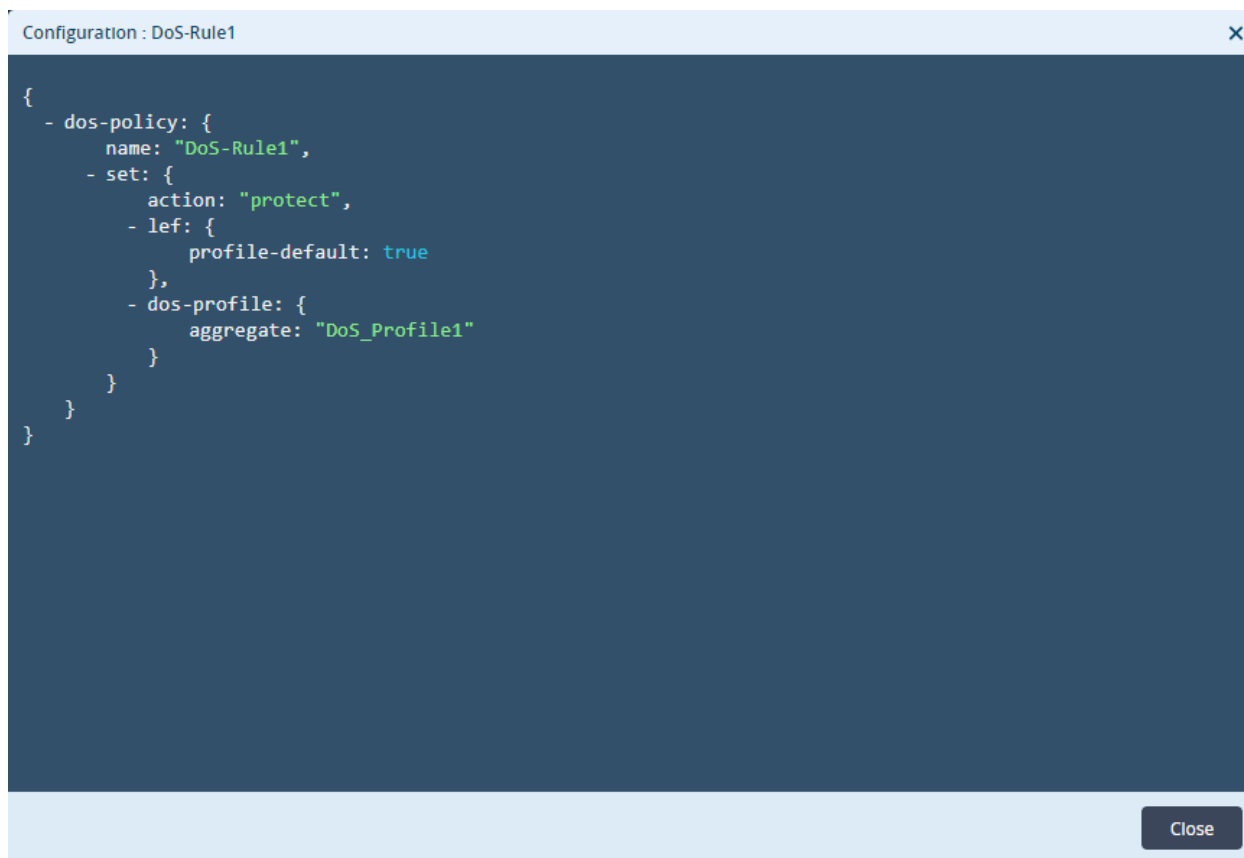
DoS Policies

Click NGFW > DoS Policies and then select the type of DoS policy to display DoS policy details.

The screenshot shows the NGFW interface with the 'DoS Policies' tab selected. The 'Customer1-DoS-Policy' filter is chosen. The table displays the following data:

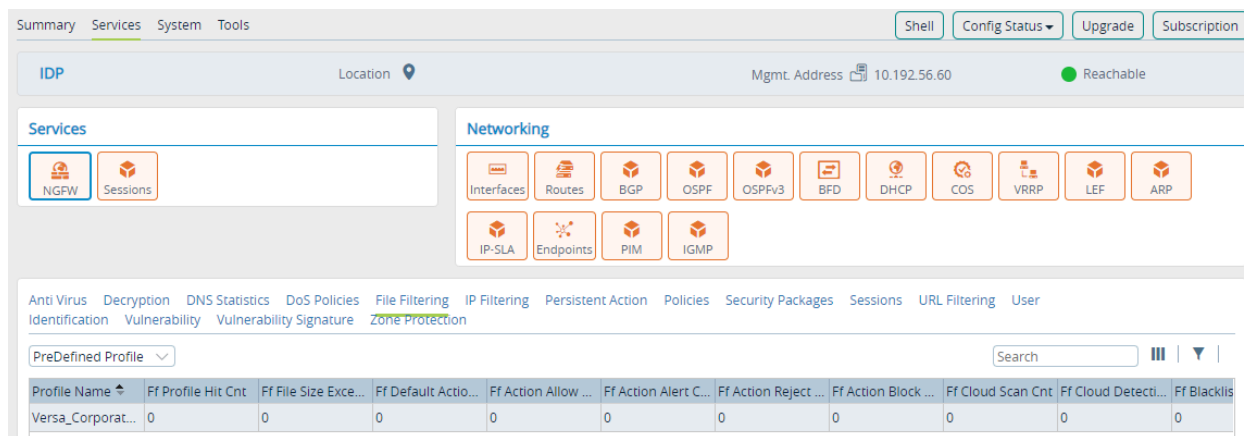
Rule Name	UDP Drop Count	ICMP Drop Count	ICMPv6 Drop Count	DG Drop Count	TCP Syn Drop Count	DoS Hit Count	SCRP Drop Count
DoS_Rule1	328752	11796	0	0	306	914108	0

Click a rule name to view its configuration.



File Filtering

Click NGFW > File Filtering and then select a predefined or user-defined profile to view file filtering information.



IP Filtering

Click NGFW > IP Filtering and select user-defined policies or predefined policies to display IP filtering information.

https://docs.versa-networks.com/Management_and_Orchestration/Versa_Director/Monitoring_with_Versa_Director/Monitor_D...

Updated: Thu, 24 Oct 2024 10:47:29 GMT

Copyright © 2024, Versa Networks, Inc.

Summary **Services** System Tools CLI Config Status Upgrade Subscription

Site4Branch1 Location 📍 Moose Jaw No. 161,SK, cannada Mgmt. Address 📄 10.1.64.107 🟢 Reachable

Services

SDWAN
IPSEC
CGNAT
NGFW
Sessions

Networking

Interfaces
Routes
BGP
OSPF
OSPFv3
BFD
DHCP
COS
VRRP
LEF
ARP

Zone Protection DoS Policies Decryption Policies **IP Filtering** URL Filtering Anti Virus Vulnerability Security Packages Sessions

Predefined 🔍 Search ☰ ▼

Name	Hit Count	Black List Hit Co...	White List Hit Co...	Geolp Rule Hit C...	Reputation Rule ...	No Match Count	Log Count	Drop Count	Fail Count
Block bad traffic	0	0	0	0	0	0	0	0	0
Block bots	0	0	0	0	0	0	0	0	0
Web protection	0	0	0	0	0	0	0	0	0
Block DoS	0	0	0	0	0	0	0	0	0
Block spam	0	0	0	0	0	0	0	0	0
Block scanners	0	0	0	0	0	0	0	0	0
Block windows e...	0	0	0	0	0	0	0	0	0

Persistent Action

Click NGFW > Persistent Action, and then select a predefined or user-defined action, an action type (static or dynamic), an action name, and the action operation to display information about persistent actions.

- For a static action:

Summary **Services** System Tools Shell Config Status Upgrade Subscription

IDP Location 📍 Mgmt. Address 📄 10.192.56.60 🟢 Reachable

IP-SLA
Endpoints
PIM
IGMP

Anti Virus Decryption DNS Statistics DoS Policies File Filtering IP Filtering **Persistent Action** Policies Security Packages Sessions URL Filtering User Identification Vulnerability Vulnerability Signature Zone Protection

Predefined Action ▼ Static ▼ Versa_Action_Block_DIP_DP ▼ brief ▼ Activate

Page 1 of 1 10

source-ip	destination-ip	source-port	destination-p...	protocol	description	precedence	duration	activate-by	action
Exclude	Include	Exclude	Include	Exclude	Block current se	100	always	Security Modul	drop-session

- For a static action whose ID is 0:

Summary Services System Tools Shell Config Status Upgrade Subscription

IDP Location Mgmt. Address 10.192.56.60 Reachable

IP-SLA Endpoints PIM IGMP

Anti Virus Decryption DNS Statistics DoS Policies File Filtering IP Filtering Persistent Action Policies Security Packages Sessions URL Filtering User Identification Vulnerability Vulnerability Signature Zone Protection

Predefined Action Static Versa_Action_Block_DIP_DP detail Activated Deactivate

Page 1 of 1 10

id	activated	activated-at
0	Yes	2018-08-31 00:33:17

- To activate configured objects, click Activate.
- To deactivate configured objects, click Deactivate.
- To activate or deactivate multiple configured objects, select all such objects and click Activate or Deactivate:

VERSA Networks Monitor Configuration Administration Build

Home IDP Search TTD

Summary Services System Tools Shell Config Status Upgrade Subscription

IDP Location Mgmt. Address 10.192.56.60 Reachable

Services NGFW Sessions Networking Interfaces Routes BGP OSPF OSPFv3 BFD DHCP COS VRRP LEF ARP IP-SLA Endpoints PIM IGMP

Anti Virus Decryption DNS Statistics DoS Policies File Filtering IP Filtering Persistent Action Policies Security Packages Sessions URL Filtering User Identification Vulnerability Vulnerability Signature Zone Protection

Predefined Action Dynamic Versa_Action_Block_SIP_SP_DIP_DP_PROTOCOL detail Deactivated Activate

Page 1 of 2 10

id	source-ip	destination-ip	source-port	destination-p...	protocol	activated	activated-at	activate-by	deactivated-at	session-matc...
1	4.0.0.1/32	172.217.6.46/32	44043	80	6	No	2018-09-11 22:4	IPS	2018-09-12 06:1	0
2	4.0.0.1/32	216.58.194.206/	57349	80	6	No	2018-09-11 22:4	IPS	2018-09-12 06:1	0
3	4.0.0.1/32	157.240.22.35/3	46680	80	6	No	2018-09-11 22:4	IPS	2018-09-12 06:1	0
4	4.0.0.1/32	220.181.57.216/	52285	80	6	No	2018-09-11 22:4	IPS	2018-09-12 06:1	0
5	4.0.0.1/32	198.35.26.96/32	59092	80	6	No	2018-09-11 22:4	IPS	2018-09-12 06:1	0
6	4.0.0.1/32	98.137.246.8/32	51266	80	6	No	2018-09-11 22:5	IPS	2018-09-12 06:1	0

© 2018 Versa Networks | All Rights Reserved Last Successful Login : Wed, Sep 12 2018, 06:38

Policies

Click NGFW > Policies and then select the type of policy to display NGFW policy statistics.

https://docs.versa-networks.com/Management_and_Orchestration/Versa_Director/Monitoring_with_Versa_Director/Monitor_D...

Updated: Thu, 24 Oct 2024 10:47:29 GMT

Copyright © 2024, Versa Networks, Inc.

Services

SD-WAN

NGFW

CGNAT

IPSEC

Sessions

Networking

Interfaces

Routes

BGP

OSPF

OSPFv3

BFD

DHCP

DNS Stats

COS

VRRP

LEF

ARP

IP-SLA

Endpoints

PIM

IGMP

Anti Virus

Decryption

DoS Policies

File Filtering

IP Filtering

Persistent Action

Policies

Security Packages

Sessions

URL Filtering

User Identification

Vulnerability

Vulnerability Signature

Web Proxy

Zone Protection

Access-policy-1

Search

Clear

Rule Name	Hit Count	Forward Pkt Count	Forward Byte Count	Reverse Pkt Count	Reverse Byte Count	Hit Rate	Inactive Session Count
access-policy-rule-1	0	0	0	0	0	0	0

Click a rule name to view its configuration.

Configuration : access-policy-rule-1

```

{
  - access-policy: {
    name: "access-policy-rule-1",
    number: 12532,
  - match: {
    - source: {
      - user: {
        - local-database: {
          status: "disabled"
        },
        - external-database: {
          status: "disabled"
        },
        user-type: "any"
      }
    }
  },
  - set: {
    action: "allow",
    - lef: {
      event: "never",
      - options: {
        - send-pcap-data: {
          enable: false
        }
      }
    }
  }
}

```

Close

Security Packages

Click NGFW > Security Packages to display security package details, includingthe installation date, version, flavor, release date, update type, and installation status.

Services

SDWAN

ADC

NGFW

IPSEC

Sessions

Networking

Interfaces

Routes

BGP

OSPF

OSPFv3

BFD

DHCP

COS

VRRP

LEF

ARP

IP-SLA

Zone Protection

DoS Policies

Decryption

Policies

IP Filtering

URL Filtering

Anti Virus

Vulnerability

Vulnerability Signature

Security Packages

Sessions

User Identification

Search

Install Date	Version	Api Version	Flavor	Release Date	Update Type	Install Status
2018-01-1821:30:25	1137	11	premium	2018-01-05	full	Success
2018-10-2613:50:32	1486	11	premium	2018-10-26	full	Success
2019-01-1217:09:11	1573	11	premium	2019-01-09	full	Success

Sessions

Click NGFW > Sessions to display NGFW session details, including the total number of NGFW sessions, number of sessions created, number of sessions closed, total number of NAT sessions, number of NAT sessions created, number of NAT sessions closed, and number of NAT sessions failed.

Services

SDWAN

NGFW

CGNAT

IPSEC

Sessions

Networking

Interfaces

Routes

BGP

OSPF

OSPFv3

BFD

DHCP

DNS Stats

COS

VRRP

LEF

ARP

IP-SLA

Endpoints

PIM

IGMP

Anti Virus

Decryption

DoS Policies

File Filtering

IP Filtering

Persistent Action

Policies

Security Packages

Sessions

URL Filtering

User Identification

Vulnerability

Vulnerability Signature

Web Proxy

Zone Protection

Search

Clear

VSN ID	Session Count	Session Created	Session Closed	NAT Session Co...	NAT Session Cr...	NAT Session Clo...	Session Failed	Session Count ...	TCP Session Co...	UDP Session Co...	ICMP Session C...	Other Session C...
0	0	11051	11051	0	0	0	0	1000000	0	0	0	0

URL Filtering

URL filtering controls access to Internet websites by permitting or denying access to specific websites based on information contained in a URL list.

Click NGFW > URL Filtering and then select the type of URL filter:

- Profile—Display URL traffic data for user-defined profiles.
- Global—Display URL statistics based on the total URL traffic in an organization.
- User Category Predefined—A security administrator can apply various types of policies based on the predefined URL categories.
- User Category User-Defined—A security administrator can create user-defined URL category objects for certain URLs and override predefined URL categorization values.
- URL Reputation Predefined—A security administrator can filter websites based on their predefined reputation values.
- URL Reputation User-Defined—A security administrator can define URL reputation values and filter websites.

The screen displays the number of transactions and sessions for the selected URL filter.

Services

SDWAN

NGFW

CGNAT

IPSEC

Sessions

Networking

Interfaces

Routes

BGP

OSPF

OSPFv3

BFD

DHCP

DNS Stats

COS

VRRP

LEF

ARP

IP-SLA

Endpoints

PIM

IGMP

Anti Virus

Decryption

DoS Policies

File Filtering

IP Filtering

Persistent Action

Policies

Security Packages

Sessions

URL Filtering

User Identification

Vulnerability

Vulnerability Signature

Web Proxy

Zone Protection

URL Category Predefined

Search

Clear

Name	Sessions	Transactions	Total Packets Forward	Total Bytes Forward	Total Packets Reverse	Total Bytes Reverse
uncategorized	0	0	0	0	0	0
real_estate	0	0	0	0	0	0
computer_and_internet_security	0	0	0	0	0	0
financial_services	0	0	0	0	0	0
business_and_economy	0	0	0	0	0	0
computer_and_internet_info	0	0	0	0	0	0
auctions	0	0	0	0	0	0
shopping	0	0	0	0	0	0
cult_and_occult	0	0	0	0	0	0

User Identification

Click NGFW > User Identification and then select the user profile to view all user details (for example, Kerberos profile, LDAP profile, SAML profile) for specific profiles.

Summary

Services

System

Tools

Shell

Config Status

Upgrade

Subscription

IDP

Location

Mgmt. Address 10.192.56.60

Reachable

IP-SLA

Endpoints

PIM

IGMP

Anti Virus

Decryption

DNS Statistics

DoS Policies

File Filtering

IP Filtering

Persistent Action

Policies

Security Packages

Sessions

URL Filtering

User

Identification

Vulnerability

Vulnerability Signature

Zone Protection

Local Database

Search

Clear

Hit Count	Split Success	Split Failure	Auth Page Shown	Auth Resp Received	Auth Success	Auth Failure
0	0	0	0	0	0	0

Vulnerability

VOS devices support multiple vulnerability profiles on a per-tenant basis. The Versa security research team provides predefined vulnerability profiles via security package updates. The predefined vulnerability profiles are available for all tenants to configure and use.

Click NGFW > Vulnerability and select the type of vulnerability profile to view vulnerability details:

- User Defined—Profiles defined by an administrator.
- Predefined—System-defined profiles.
- Sessions—Vulnerable sessions during the current system uptime.

Services

SDWAN

NGFW

CGNAT

IPSEC

Sessions

Networking

Interfaces

Routes

BGP

OSPF

OSPFv3

BFD

DHCP

DNS Stats

COS

VRRP

LEF

ARP

IP-SLA

Endpoints

PIM

IGMP

Anti Virus

Decryption

DoS Policies

File Filtering

IP Filtering

Persistent Action

Policies

Security Packages

Sessions

URL Filtering

User Identification

Vulnerability

Vulnerability Signature

Web Proxy

Zone Protection

Pre Defined


Search

III

▼

Clear

Name	Total Sessions	Total Packet Events	Total Stream Event	Total Mpm Matches	Total Rule Processed	Total Rule Matched	Total Logged Rules
All Anomaly Rules	0	0	0	0	0	0	0
All Attack Rules	0	0	0	0	0	0	0
Client Protection	0	0	0	0	0	0	0
Database Profile	0	0	0	0	0	0	0
ICS Profile	0	0	0	0	0	0	0
Lateral Movement De...	0	0	0	0	0	0	0
Linux OS Profile	0	0	0	0	0	0	0
MAC OS Profile	0	0	0	0	0	0	0
Malware Profile	0	0	0	0	0	0	0
Server Protection	0	0	0	0	0	0	0
Versa Branch Profile	0	0	0	0	0	0	0
Versa Recommended...	0	0	0	0	0	0	0
Windows OS Profile	0	0	0	0	0	0	0

Click the  Eye icon to view details of the rules.

Vulnerability Signature

The screen displays the vulnerable profiles or rules for protection.

Services

SDWAN

NGFW

CGNAT

IPSEC

Sessions

Networking

Interfaces

Routes

BGP

OSPF

OSPFv3

BFD

DHCP

DNS Stats

COS

VRRP

LEF

ARP

IP-SLA

Endpoints

PIM

IGMP

Anti Virus

Decryption

DoS Policies

File Filtering

IP Filtering

Persistent Action

Policies

Security Packages

Sessions

URL Filtering

User Identification

Vulnerability

Vulnerability Signature

Web Proxy

Zone Protection

Pre Defined

Search

III

▼

Clear

Name
All Anomaly Rules
All Attack Rules
Client Protection
Database Profile
ICS Profile
Lateral Movement Detection
Linux OS Profile
MAC OS Profile
Malware Profile
Server Protection
Versa Branch Profile
Versa Recommended Profile
Windows OS Profile

Click view to display the signature ID associated with the policy.

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

[Monitor Device Networking Services](#)