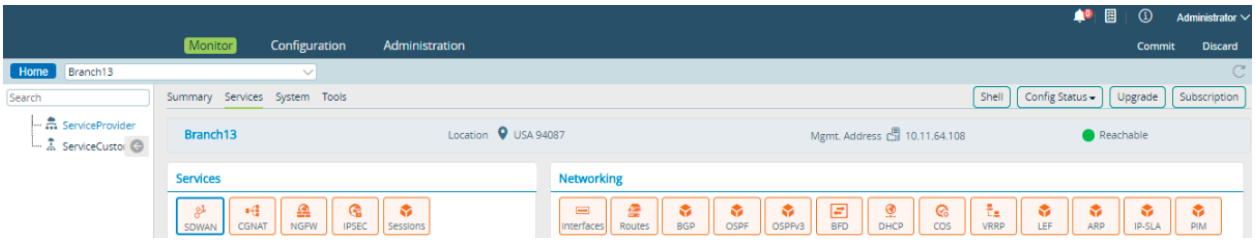
Monitor Device Services

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:

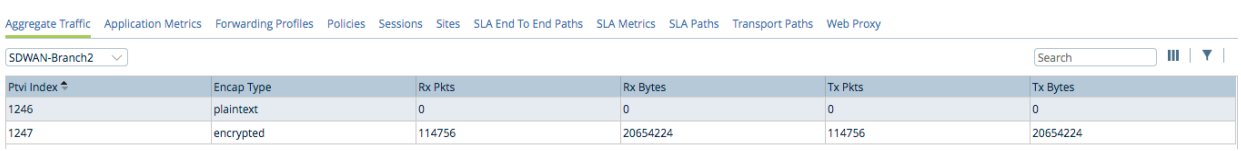
- Aggregate Traffic
- Application Metrics
- Forwarding Profiles
- Policies

Copyright © 2024, Versa Networks, Inc.

- 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.



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

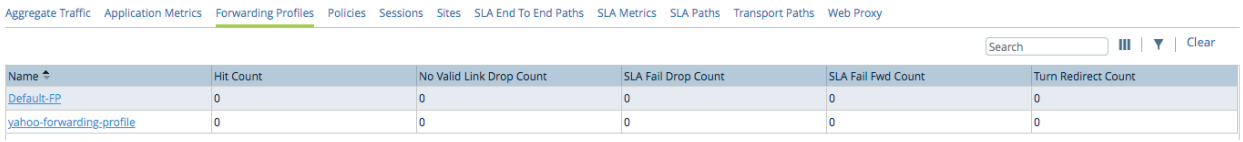
Application Metrics

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.



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.

Copyright © 2024, Versa Networks, Inc.

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.

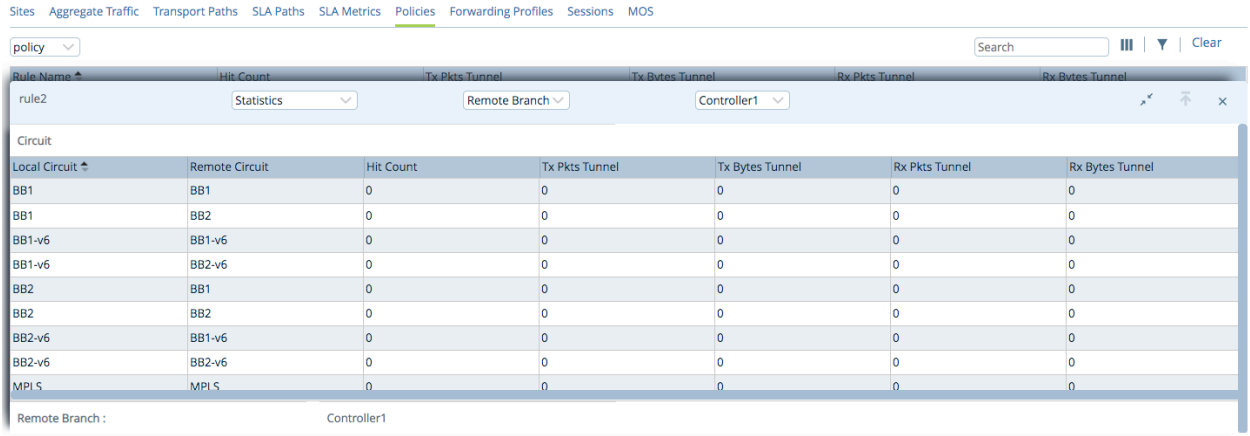
Sites | Aggregate Traffic | Transport Paths | SLA Paths | SLA Metrics | Policies | Forwarding Profiles | Sessions | MOS

policy | Search | 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.

Copyright © 2024, Versa Networks, Inc.

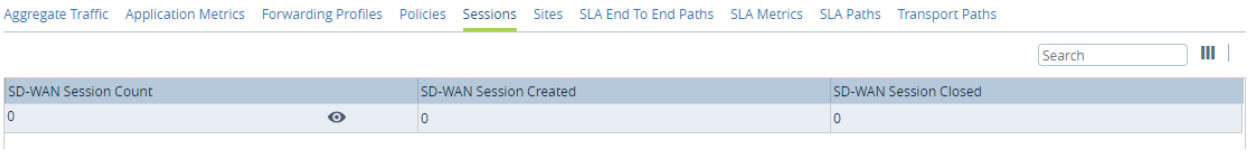


Click a rule name to view its configuration in CLI format.

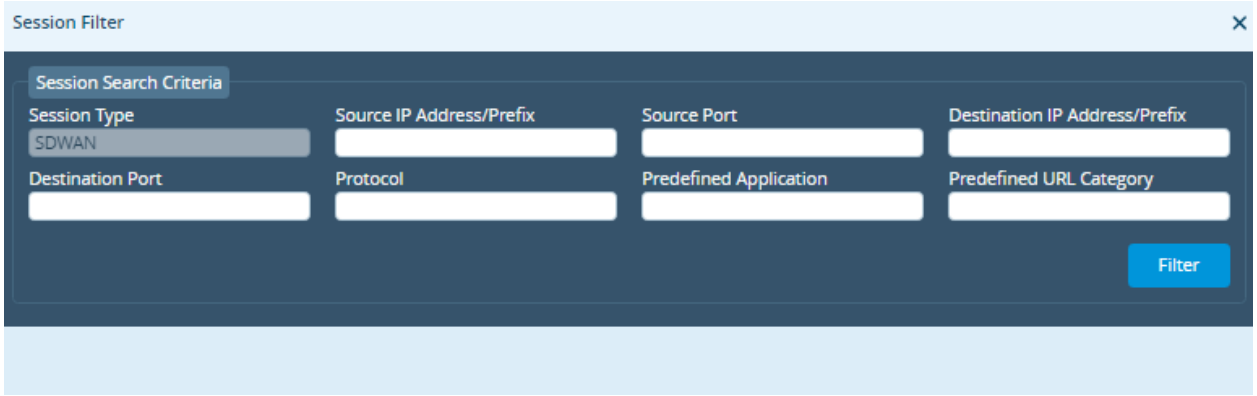
Sessions

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.

Copyright © 2024, Versa Networks, Inc.

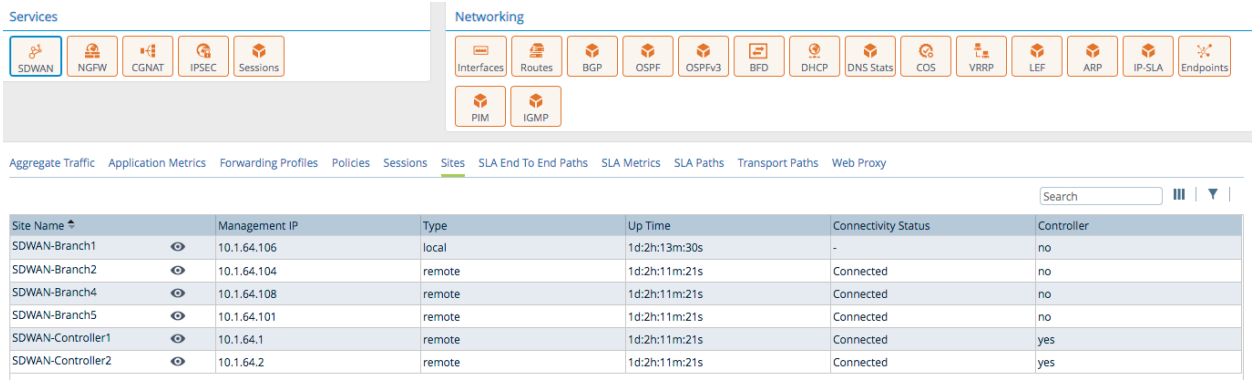


Click the Eye icon to view the filter session data.



Sites

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



Click the

Copyright © 2024, Versa Networks, Inc.

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

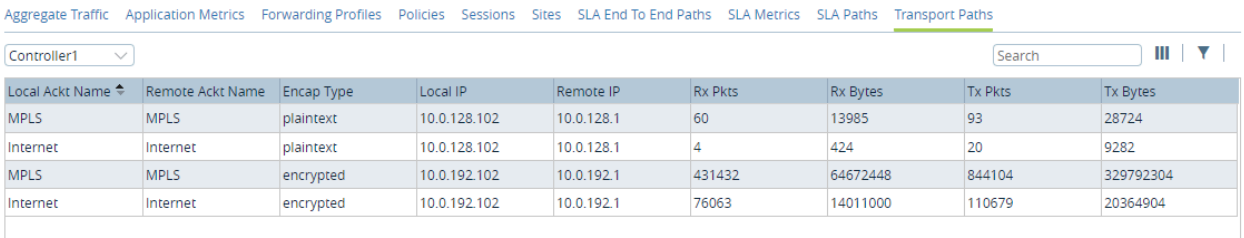
Controller1 Search

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.

Copyright © 2024, Versa Networks, Inc.



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.

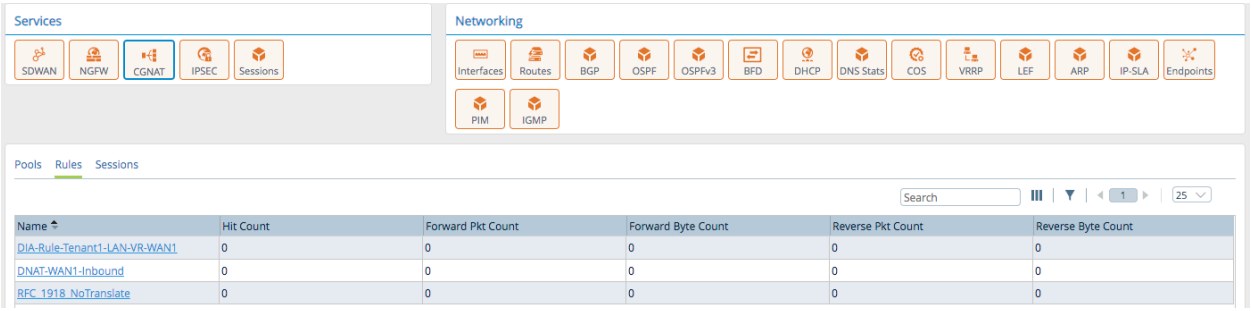
CGNAT can replace NAT devices in enterprise networks. Using CGNAT, you can deliver seamless IPv4 connectivity even while using limited public addresses. You can define private IPv4 address in your network and use Versa CGNAT to manage address translation to the public IPv4 addresses.

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

- Rules
- Pools
- Sessions

Rules

Click CGNAT > Rules to display information about CGNAT rules.



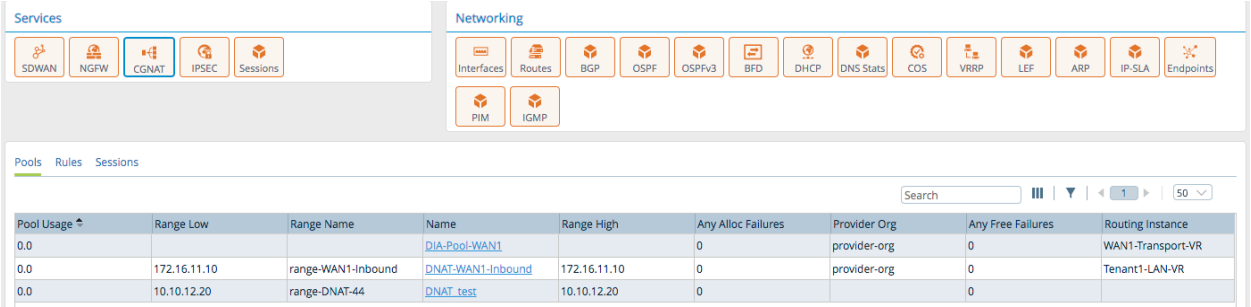
Name	Hit Count	Forward Pkt Count	Forward Byte Count	Reverse Pkt Count	Reverse Byte Count
DIA-Rule-Tenant1-LAN-VR-WAN1	0	0	0	0	0
DNAT-WAN1-Inbound	0	0	0	0	0
RFC_1918_NoTranslate	0	0	0	0	0

Click a rule name view its configuration.

Pools

Click CGNAT > Pools to display pool details.

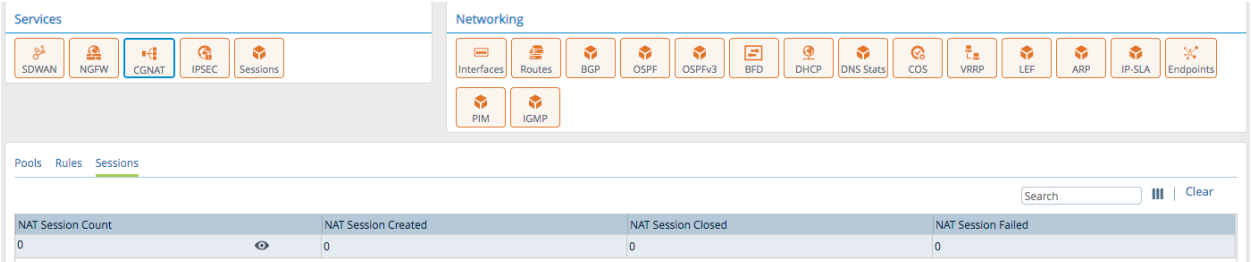
Copyright © 2024, Versa Networks, Inc.



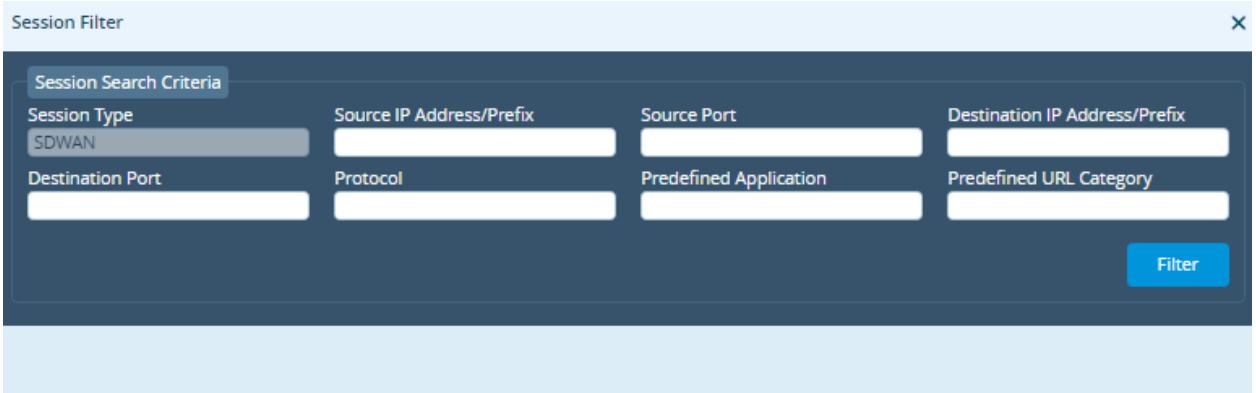
Click a pool name to view its configuration.

Sessions

Click CGNAT > Sessions to display NAT session details.



Click the Eye icon to filter sessions.



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

Copyright © 2024, Versa Networks, Inc.

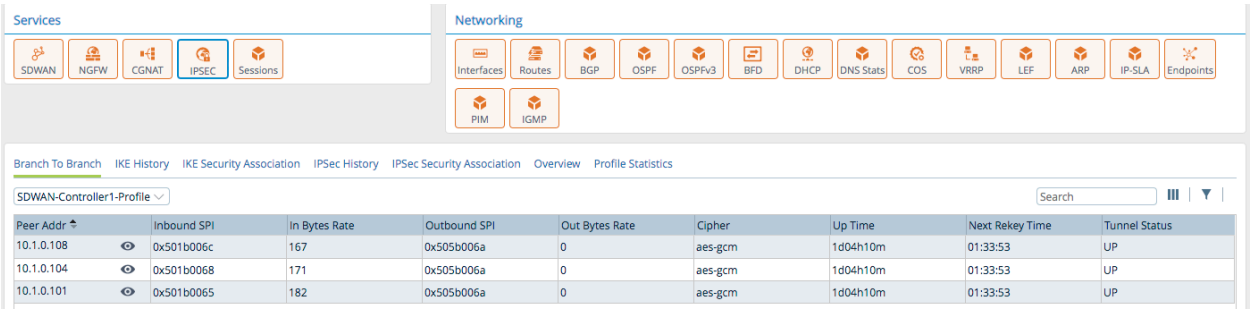
- Integrity
- Confidentiality
- Replay protection

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.

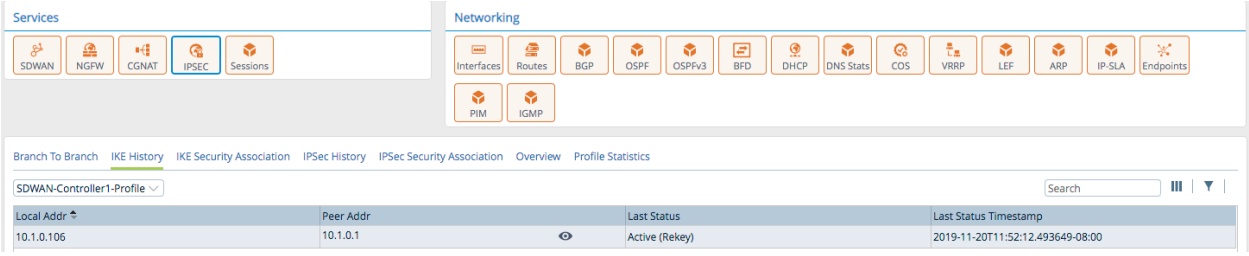


Click the Eye icon to view details.

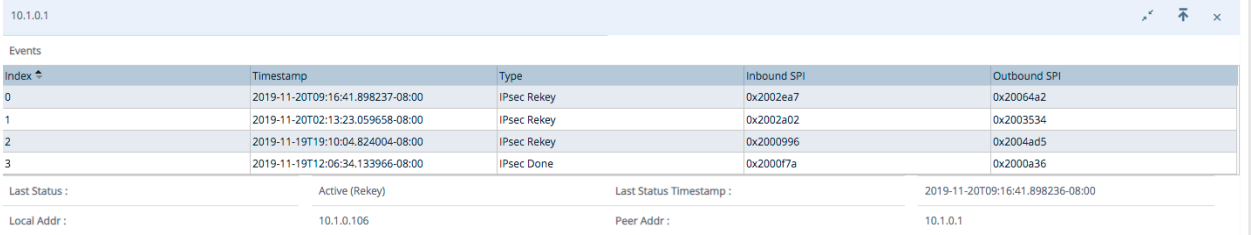
Copyright © 2024, Versa Networks, Inc.

IKE History

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

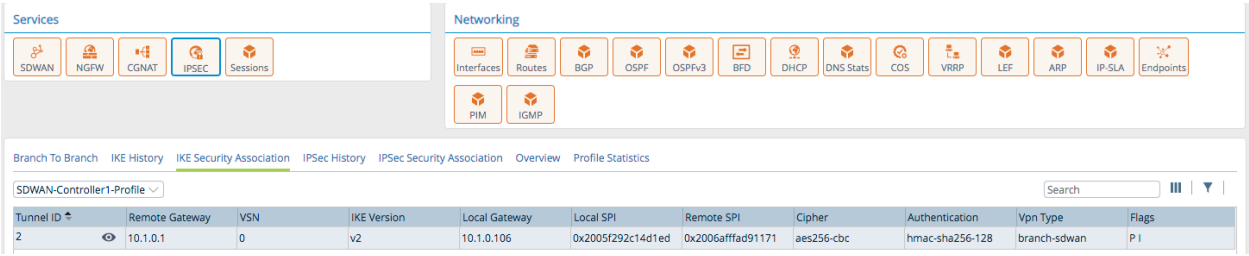


Click the Eye icon to view details.



IKE Security Association

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



Click the Eye icon to view details.

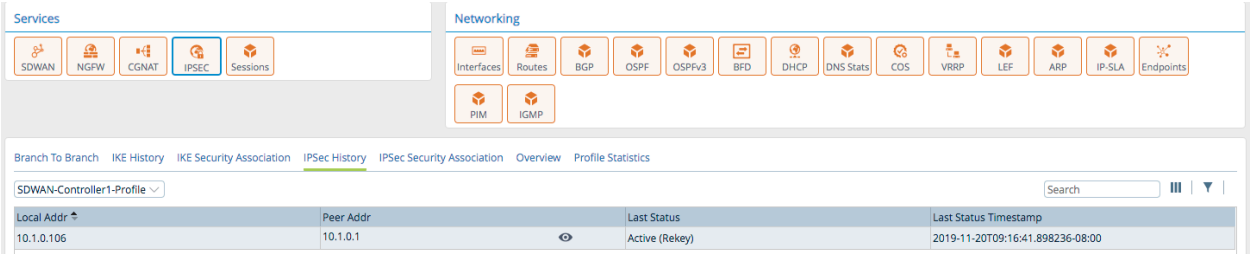
Copyright © 2024, Versa Networks, Inc.

2

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 :	0x2006afffad91171	Tunnel ID :	2
Vpn Type :	Branch-Sdwan	VSN :	0

IPsec History

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



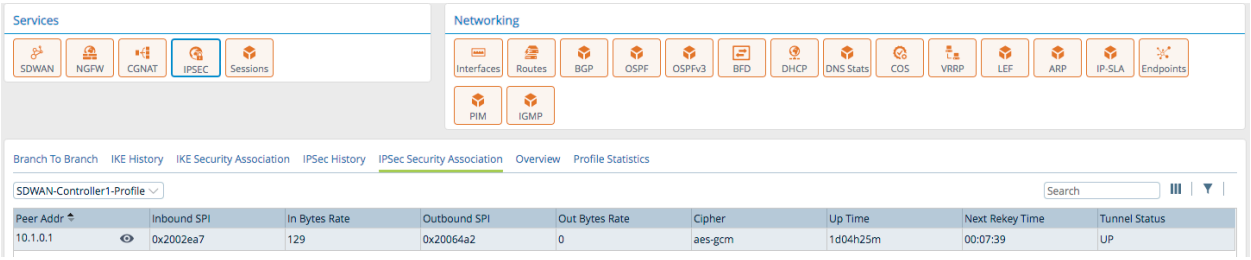
Click the Eye icon to view details.

10.1.0.1

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.



Copyright © 2024, Versa Networks, Inc.

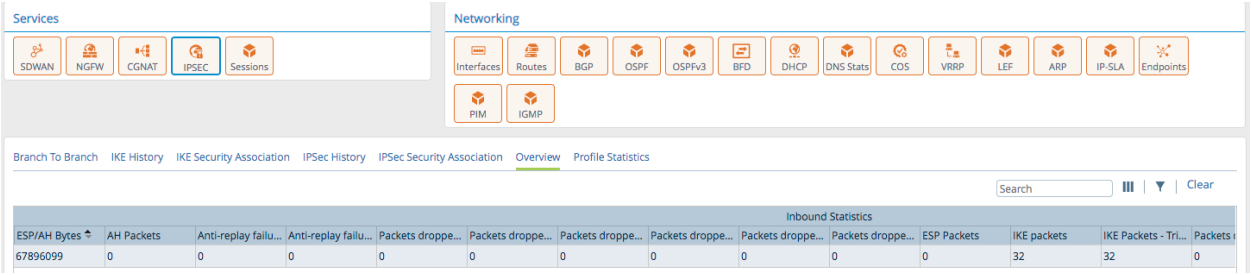
Click the Eye icon to view details.

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

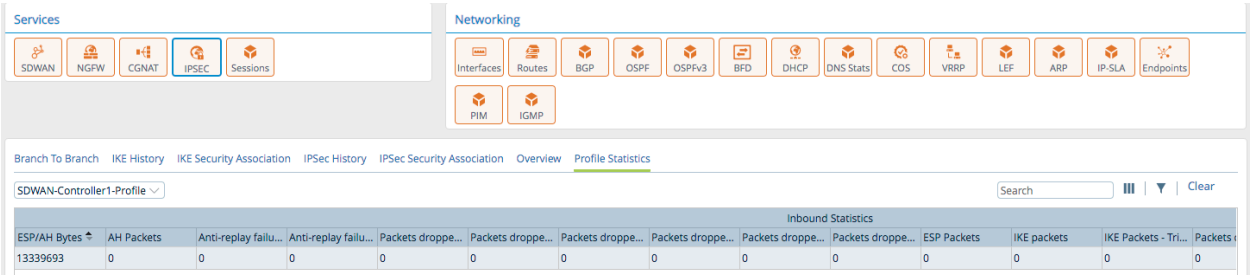
Overview

Click IPsec > Overview to display IPsec packet details.



Profile Statistics

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



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

Copyright © 2024, Versa Networks, Inc.

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.

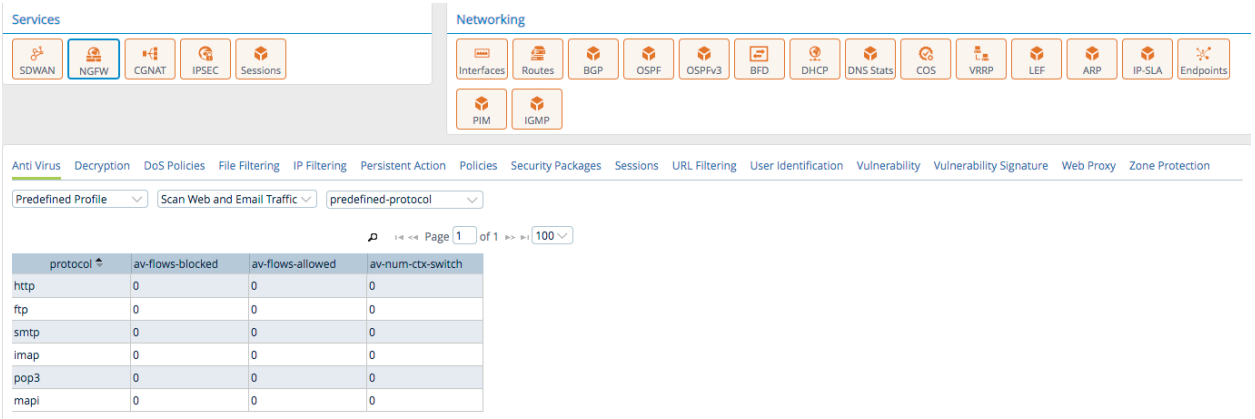
Click the NGFW tab.This tab displays the following tabs:

- Antivirus
- Decryption
- DoS Policies
- File Filtering
- IP Filtering
- Persistent Action
- Policies
- Security Packages
- Sessions
- URL Filtering
- Vulernability
- 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.



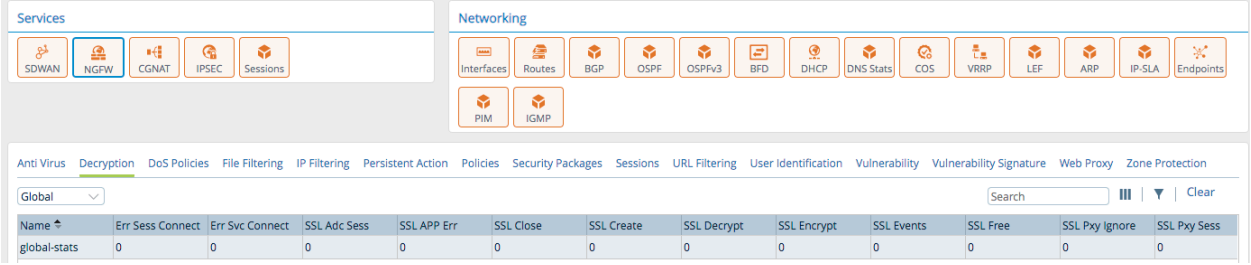
Copyright © 2024, Versa Networks, Inc.

Decryption

NGFW enables decryption of SSL traffic to detect malware and other suspicious data or prevent confidential data from leaving your organization. The Decryptio 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.
- Profilel—Display the decryption data for user-defined profiles.
- Policy—Display the decryption data for user-defined policies.



DoS Policies

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

Click a rule name to view its configuration.

Copyright © 2024, Versa Networks, Inc.

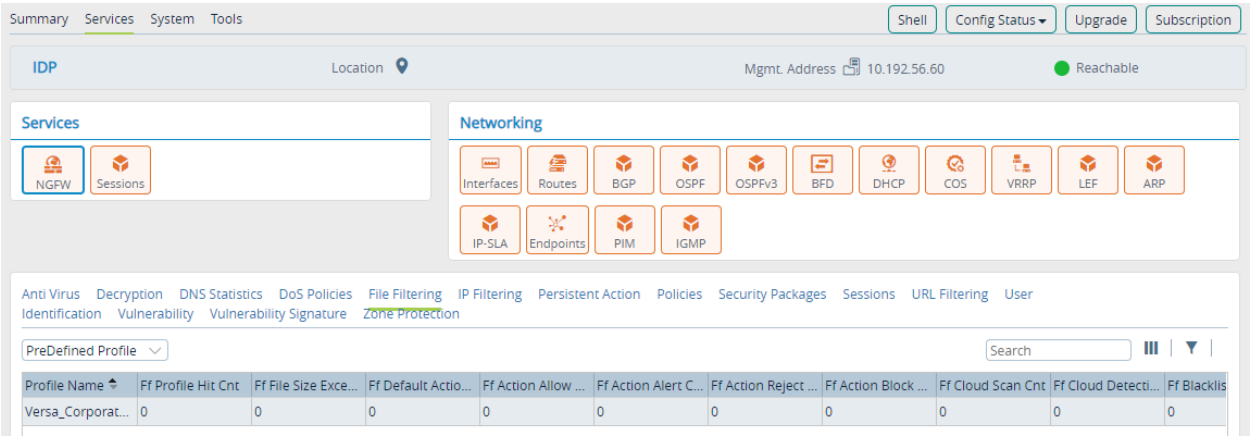
Configuration : DoS-Rule1

```
{
  - dos-policy: {
        name: "DoS-Rule1",
      - set: {
            action: "protect",
          - lef: {
                profile-default: true
            },
          - dos-profile: {
                aggregate: "DoS_Profile1"
            }
        }
    }
}
```

Close

File Filtering

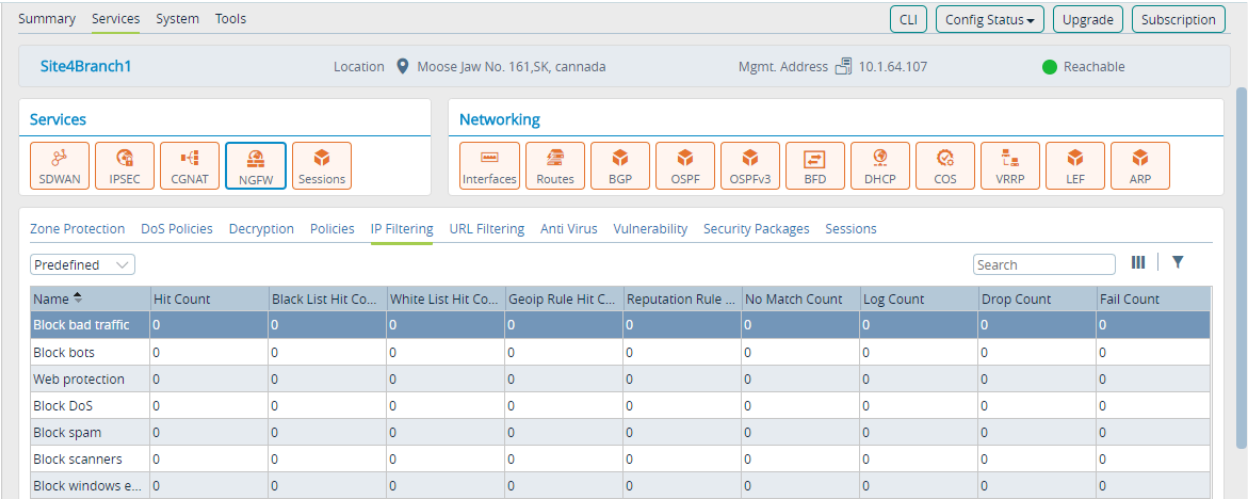
Click NGFW > File Filtering and then select a predefined or user-defined profile to view file filtering information.



IP Filtering

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

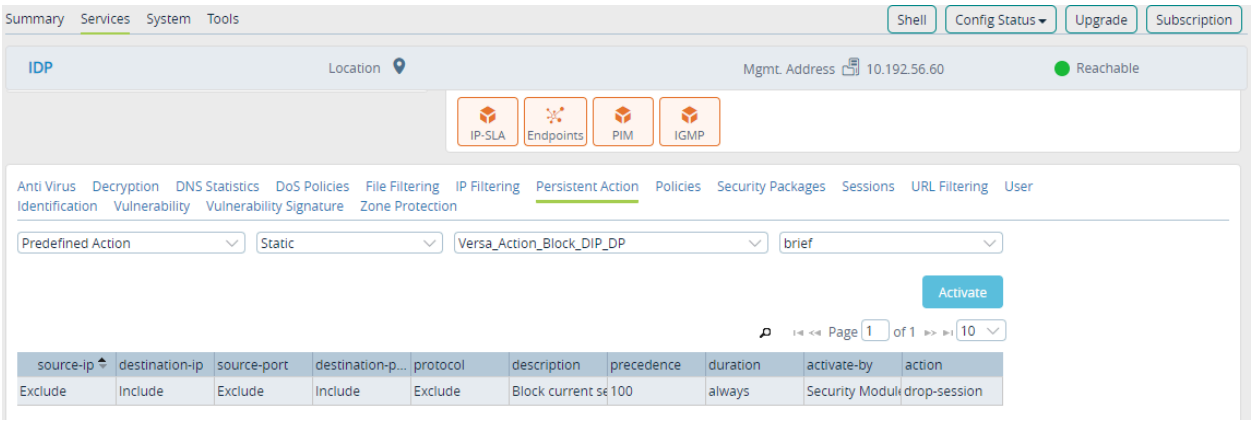
Copyright © 2024, Versa Networks, Inc.



Persistent Action

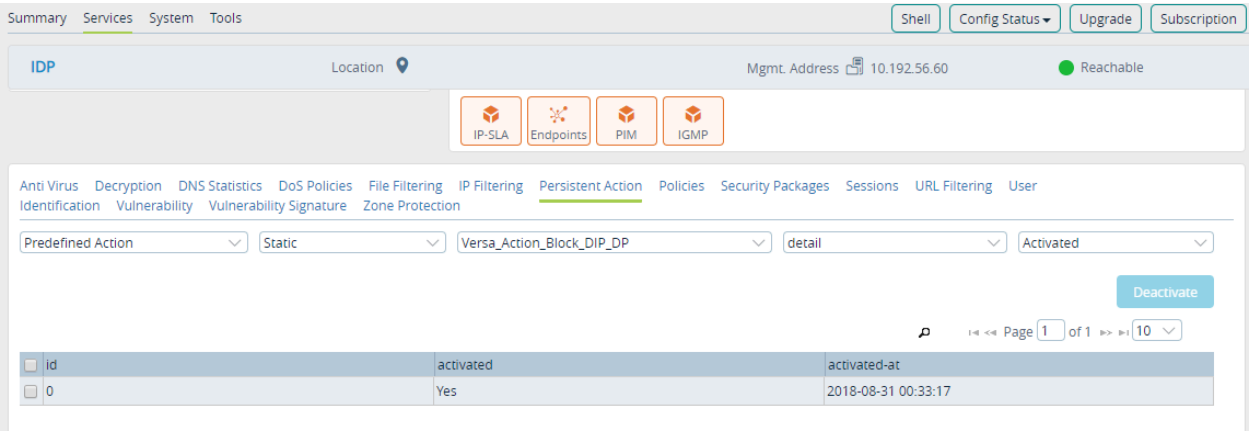
Click NGFW > Persistent Action, and then select a predefined or user-defined action, an action type (static or dynamic), an action name, and the action operation to display information about persistent actions.

- For a static action:

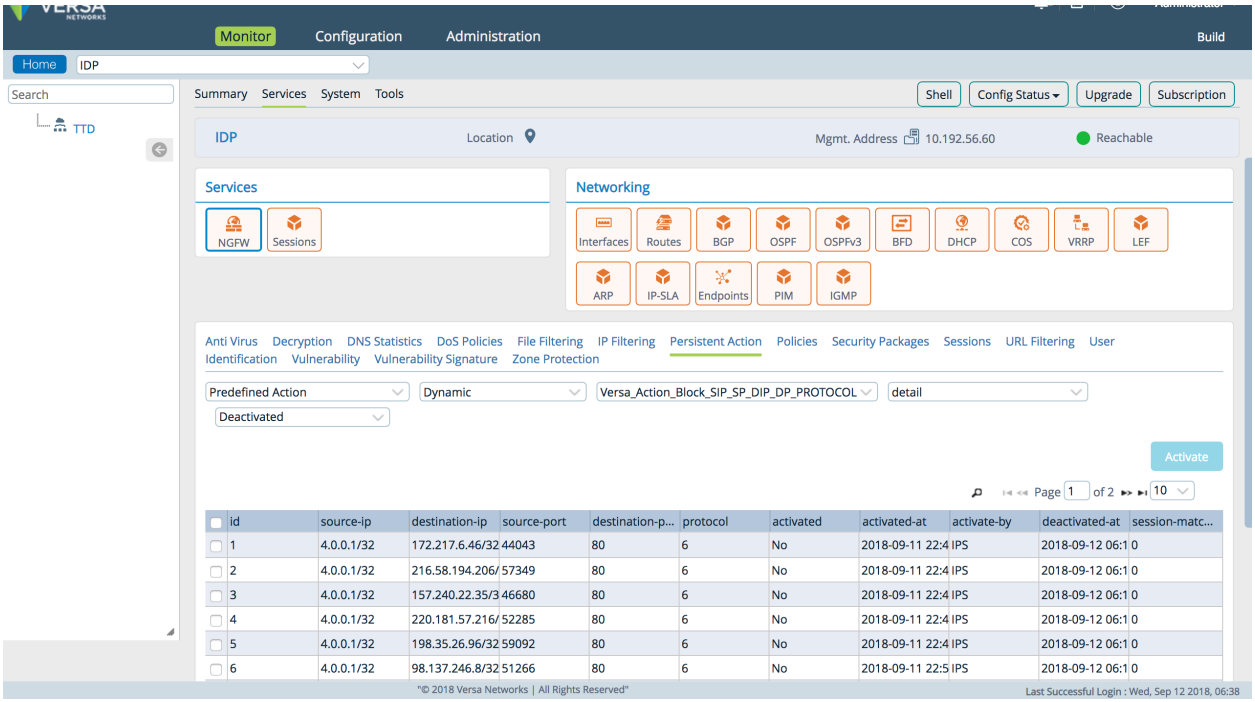


- For a static action whose ID is 0:

Copyright © 2024, Versa Networks, Inc.



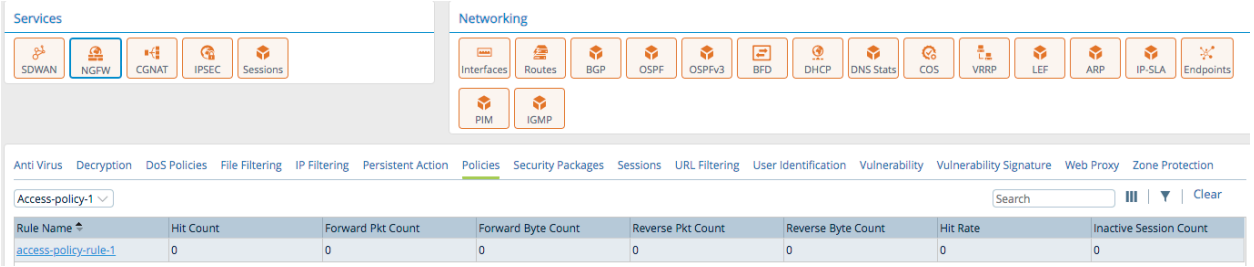
- To activate configured objects, click Activate.
- To deactivate configured objects, click Deactivate.
- To activate or deactivate multiple configured objects, select all such objects and click Activate or Deactivate:



Policies

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

Copyright © 2024, Versa Networks, Inc.

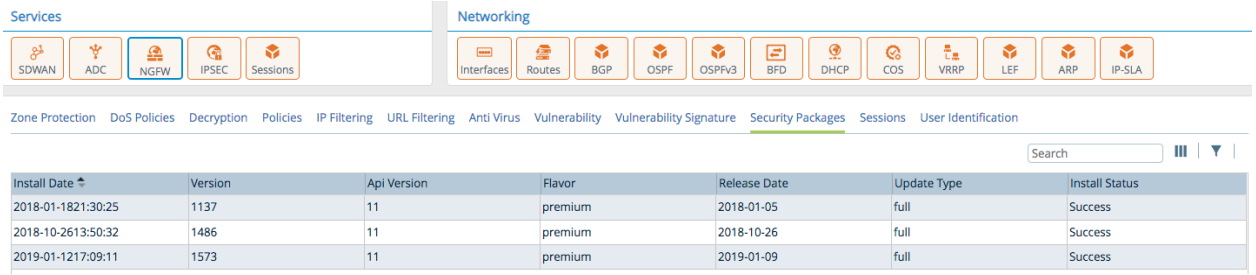


Click a rule name to view its configuration.

Security Packages

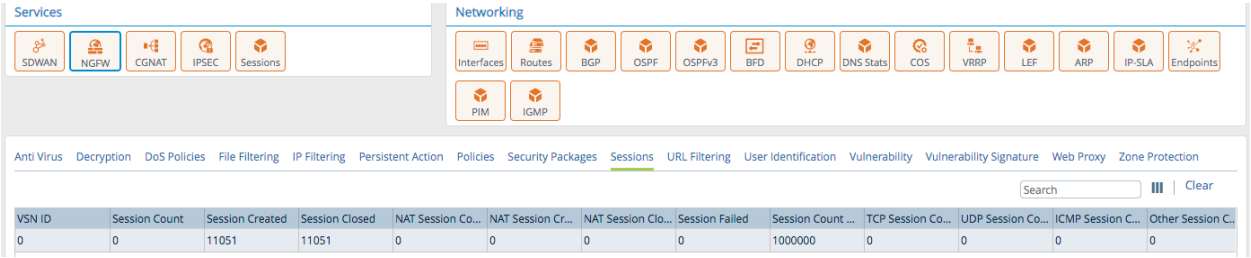
Click NGFW > Security Packages to display security package details, includingthe installation date, version, flavor, release date, update type, and installation status.

Copyright © 2024, Versa Networks, Inc.



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.



URL Filtering

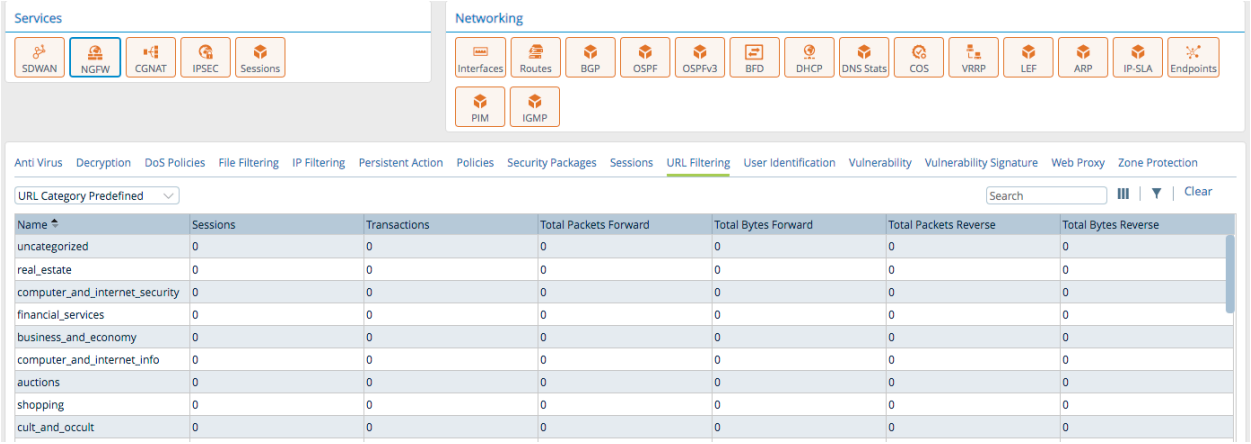
URL filtering controls access to Internet websites by permitting or denying access to specific websites based on information contained in a URL list.

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.

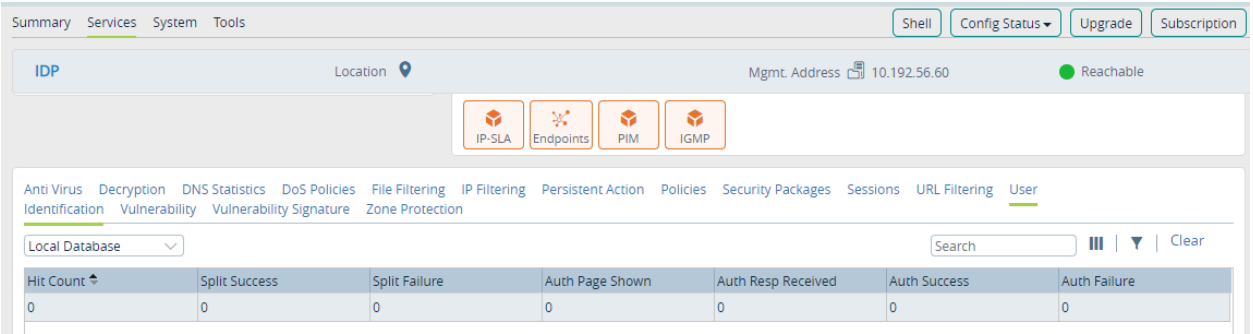
The screen displays the number of transactions and sessions for the selected URL filter.

Copyright © 2024, Versa Networks, Inc.



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.



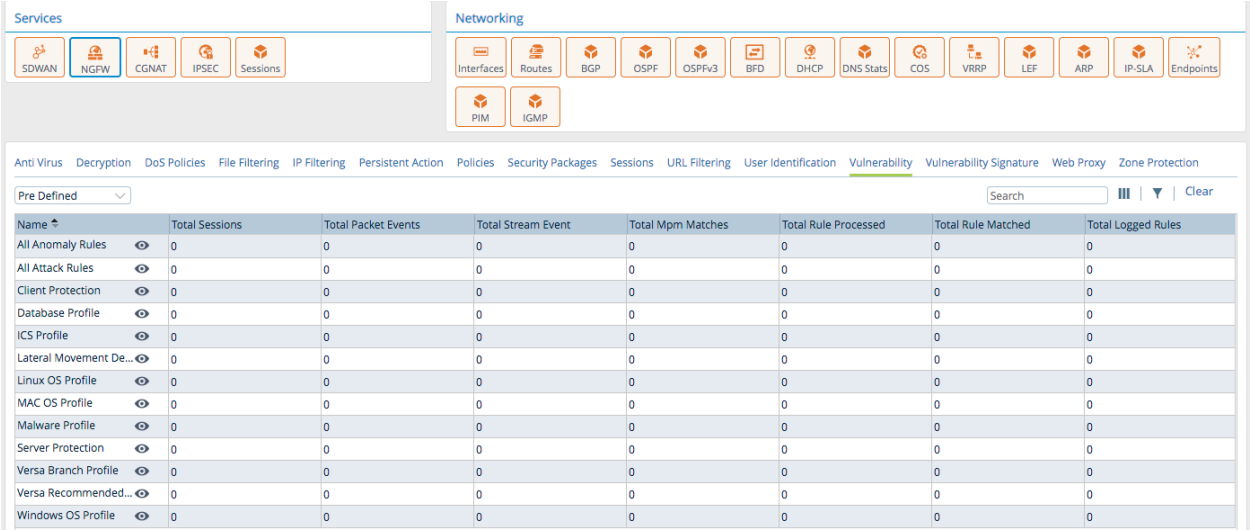
Vulnerability

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 vulnerabilitydetails:

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

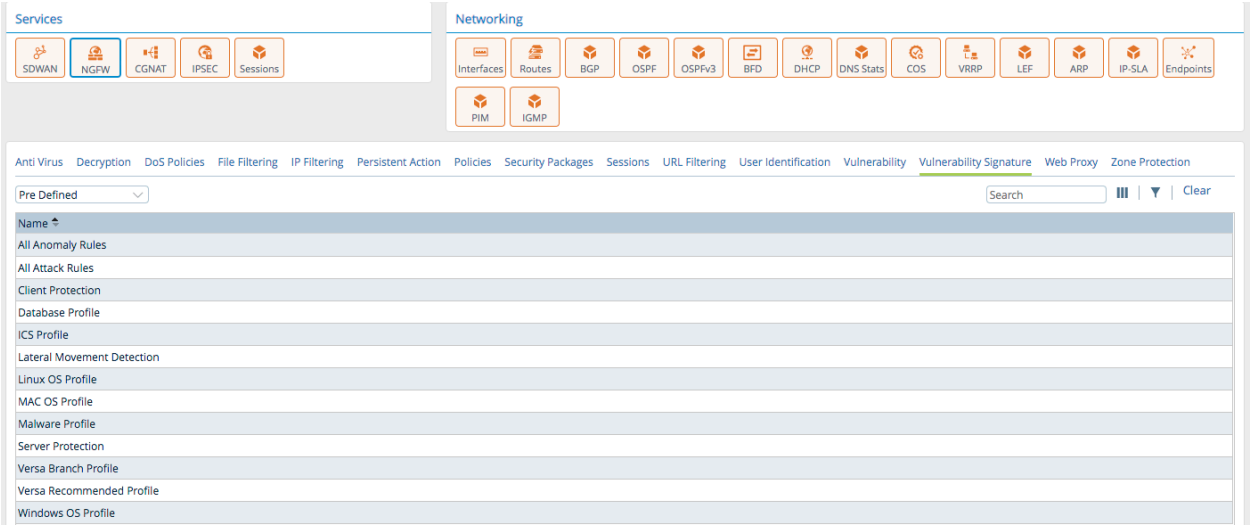
Copyright © 2024, Versa Networks, Inc.



Click the Eye icon to view details of the rules.

Vulnerability Signature

The screen displays the vulnerable profiles or rules for protection.



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

Copyright © 2024, Versa Networks, Inc.

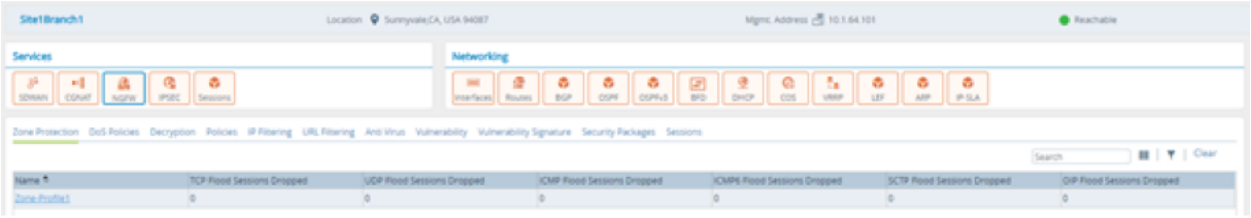
Versa Recommended Profile - Signature

Signature Id	Name	Reference Type	Reference Id
1100326070	"Apple Safari Right-to-Lef...	"cve"	"CVE-2010-0049"
1100511020	"Microsoft Windows Mail ...	"cve"	"CVE-2010-0816"
1100825090	"FLOWBITS: Adobe Shock...		
1101012380	"Microsoft Windows Com...	"cve"	"CVE-2010-2746"
1111018130	"FLOWBITS: cdr file"	"tsl"	"TSL20111018-13"
1120514050	"FLOWBITS: Adobe Photo...	"tsl"	"TSL20120514-05"

Zone Protection

Zone protection profiles provide additional protection between specific network zones against attacks. The profile protects zones from spoof or junk data packets.

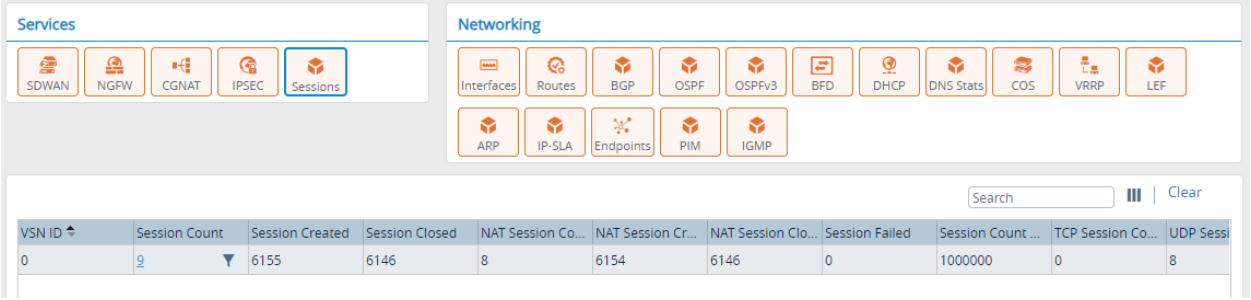
Click NGFW > Zone Protection to display statistics about zone protection profiles.



Click a rule name to view its configuration.

Services > Sessions

Click Services > Sessions to display the total session count, number of sessions cleared, number of sessions closed, number of NAT sessions closed, number of NAT sessions created, and other details for each VSN ID.



Copyright © 2024, Versa Networks, Inc.

Supported Software Information

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

Additional Information

Monitor Device Networking Services

Copyright © 2024, Versa Networks, Inc.