paloalto TECHDOCS

Symantec Web Security Services Integration Guide

1.0.0

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

March 22, 2022

Table of Contents

Integrate Prisma SD-WAN and Symantec Web Security Services

This guide explains the integration between Prisma SD-WAN and Symantec Web Security Services.

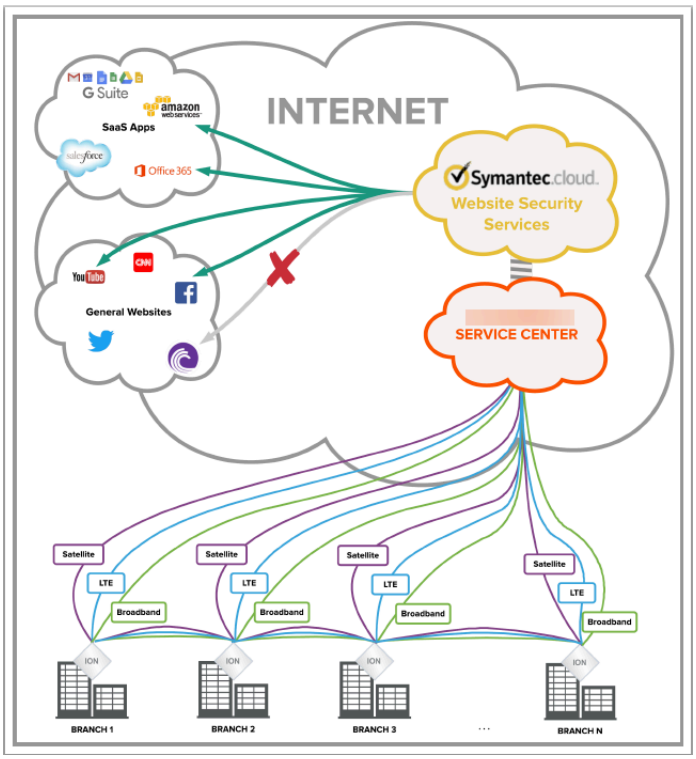
Prisma SD-WAN and Symantec Web Security Services

As enterprises rely on SaaS or Cloud-based delivery models for business-critical applications, there is a compelling need for per-application policy enforcement without increasing remote office infrastructure footprint. Traditional hardware-router based approaches are limited by heavy-handed 'all or nothing' policies for direct-to-Internet versus per-application policy enforcement. Additionally, because router based approaches are packet-based versus application-session based, they fail to meet application session symmetry requirements, causing network and security outages.

Symantec Corporation, the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. Find out more at www.symantec.com

Prisma SD-WAN and Symantec Web Security Services help enterprises integrate the Cloud directly with the branch office with per-application policies. The combined solution ensures:

- A very light remote office infrastructure footprint by integrating with Symantec cyber security solutions hosted in the cloud.
- That flows traverse symmetrical paths, both to and from the application, while dynamically selecting the best performing path.



Prerequisites to Integrate Prisma SD-WAN and Symantec Security Services

The following items are required to configure Prisma SD-WAN and Symantec Web Security Services integration:

Prisma SD-WAN

- Active Prisma SD-WAN subscription.
- Prisma SD-WAN fabric deployed at one or more locations.
- Physical and/or virtual ION devices running release 4.5.1b26 or later.
- One or more physical, virtual, or cloud sites able to be configured as ‘Service Center Data Centers’ for integration.

Symantec

- Active Symantec Web Security Services subscription.
- Licenses for Firewall/VPN connections.
- 'All Ports License' is recommended but not required.

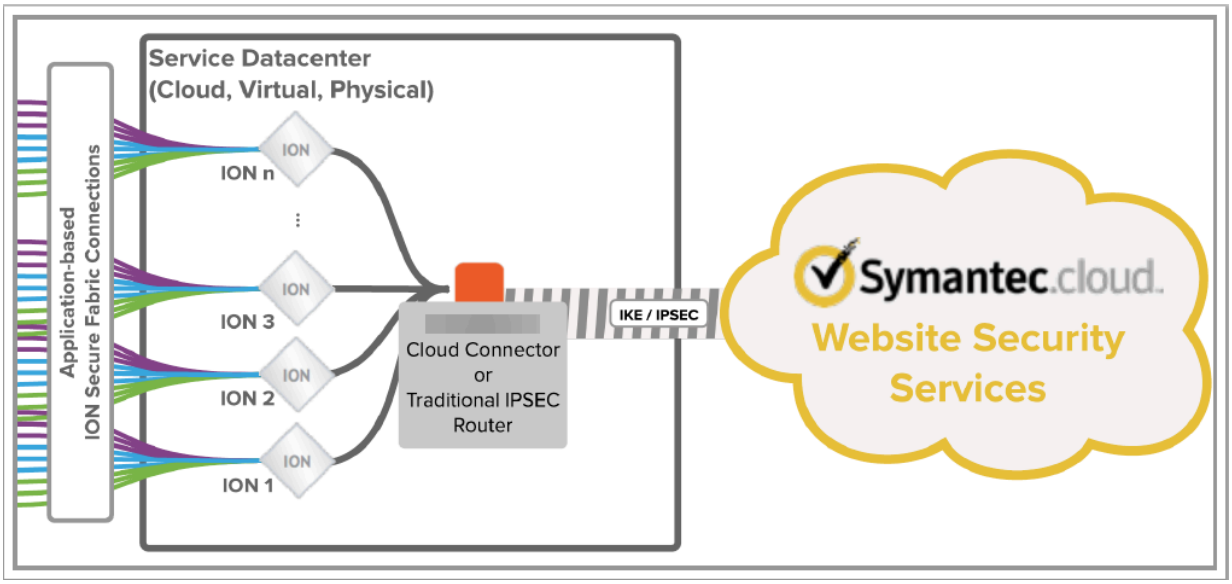
The images in this document may have references to CloudGenix and the term 3rd party / 3rd Party VPN. The CloudGenix instances now display as Prisma SD-WAN, and the new term for 3rd Party / 3rd Party VPN is Standard VPN on the Prisma SD-WAN web interface.

Plan the Deployment

The integration of Prisma SD-WAN with Symantec Web Security Services will occur using designated ‘Service Center Data Center’ objects. These can be physical, virtual, or cloud-based Data Centers.

When selecting existing or creating new Data Centers for integration, it is important to consider the following factors:

- Physical regions/locations of branches that will be served by these Service Center Data Centers.
- Regions for which the Web Security Services will be deployed (both active and backup).



It is recommended to select a Service Center Data Center location in close network proximity to one or more of the desired Web Security Services regions.

Prepare Prisma SD-WAN Network

The steps to prepare the Prisma SD-WAN fabric for the Web Security Services integration will vary based on the type of Service Center Data Center selected.

Physical or Virtual

STEP 1 | Create one or more data center objects in the Prisma SD-WAN network for use as a Service Center Data Center.

STEP 2 | For each data center, deploy one or more ION 7000 class physical or virtual devices.

STEP 3 | Deploy one or more traditional IPSEC routers (physical or virtual) that the ION cluster will access through eBGP and then use to connect to the Web Security Services cloud.

Cloud (AWS)

STEP 1 | Deploy Prisma SD-WAN ION 7000 series directly into your existing or new AWS Virtual Private Cloud (VPC).

STEP 2 | To gain access to the ION 7000 AMI, open a case via support@prismasdwan.com or https://support.prismasdwan.com. Prisma SD-WAN will assist in initial deployments of AWS-Data Centers.

Symantec Preparation

Following prerequisites ensure that the Symantec Web Security Services are available for configuration.

- Ensure that the https://portal.threatpulse.com management account is active and has the appropriate permissions.
- Ensure that the active Web Security Services Account has enough Firewall/VPN licenses for the number of Service Center Data Centers that are required.

Configure Symantec Integration

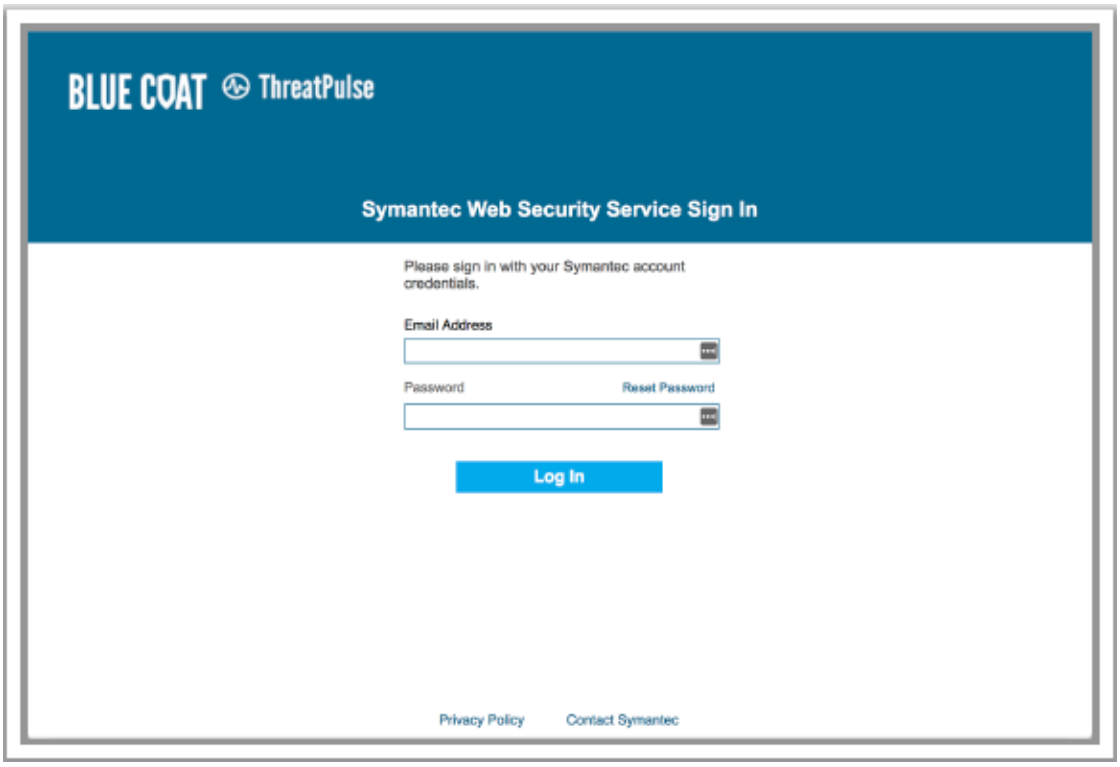
Deploying the Symantec and Prisma SD-WAN integration consists of three steps:

- Configure Symantec Web Security Services
- Configure IPSEC Tunnel to Symantec Web Security Service
- Sample Traditional IPSEC Router Configuration
- Configure Prisma SD-WAN Secure Application Fabric

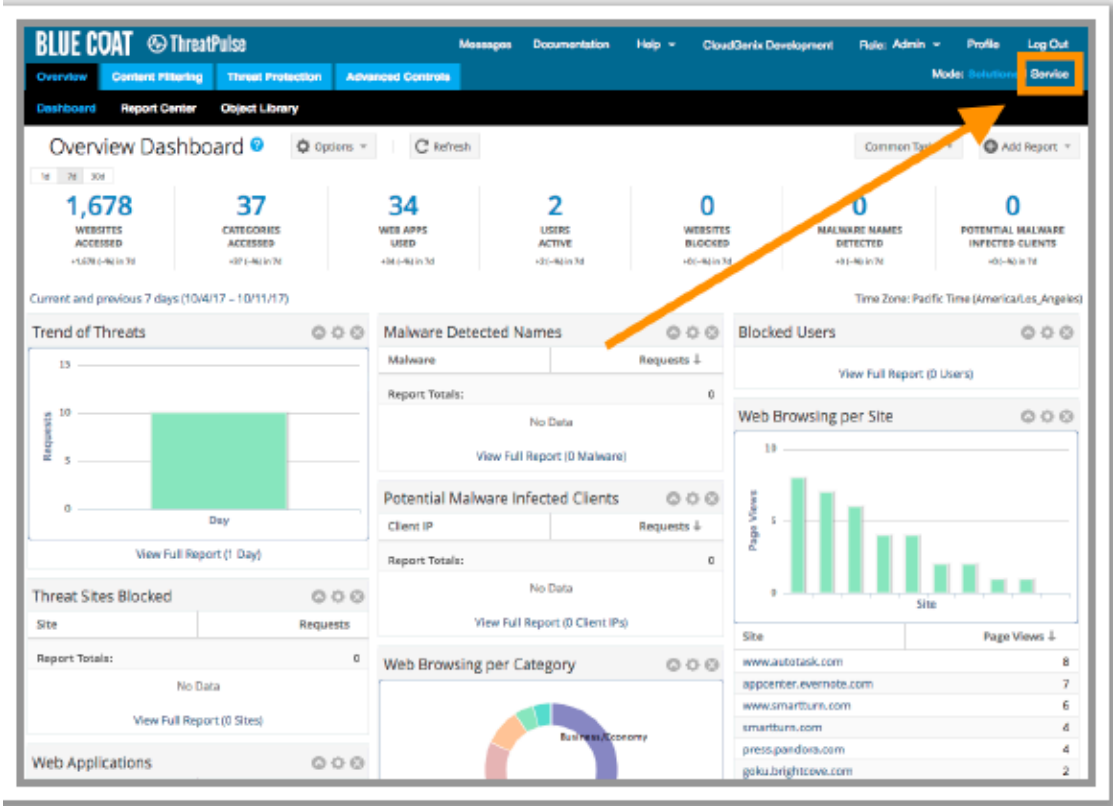
Configure Symantec Web Security Services

To configure Symantec Web Security Services:

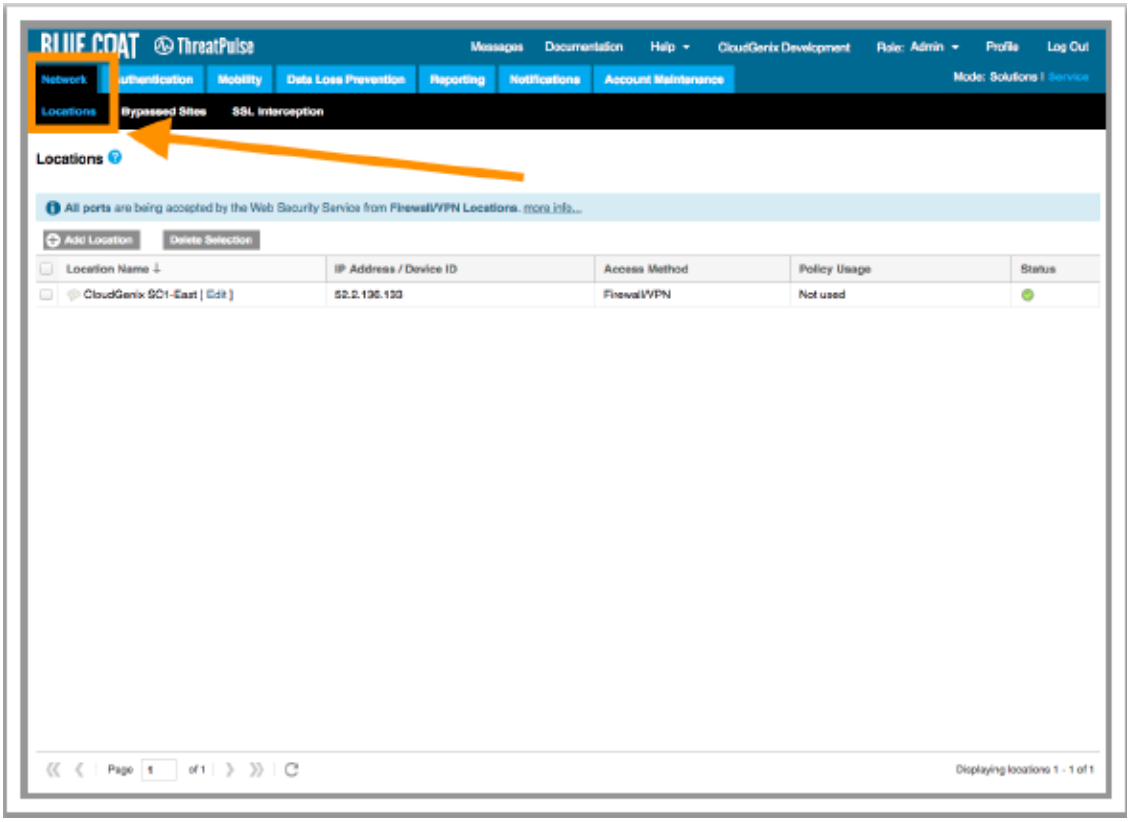
STEP 1 | Login to https://portal.threatpulse.com.



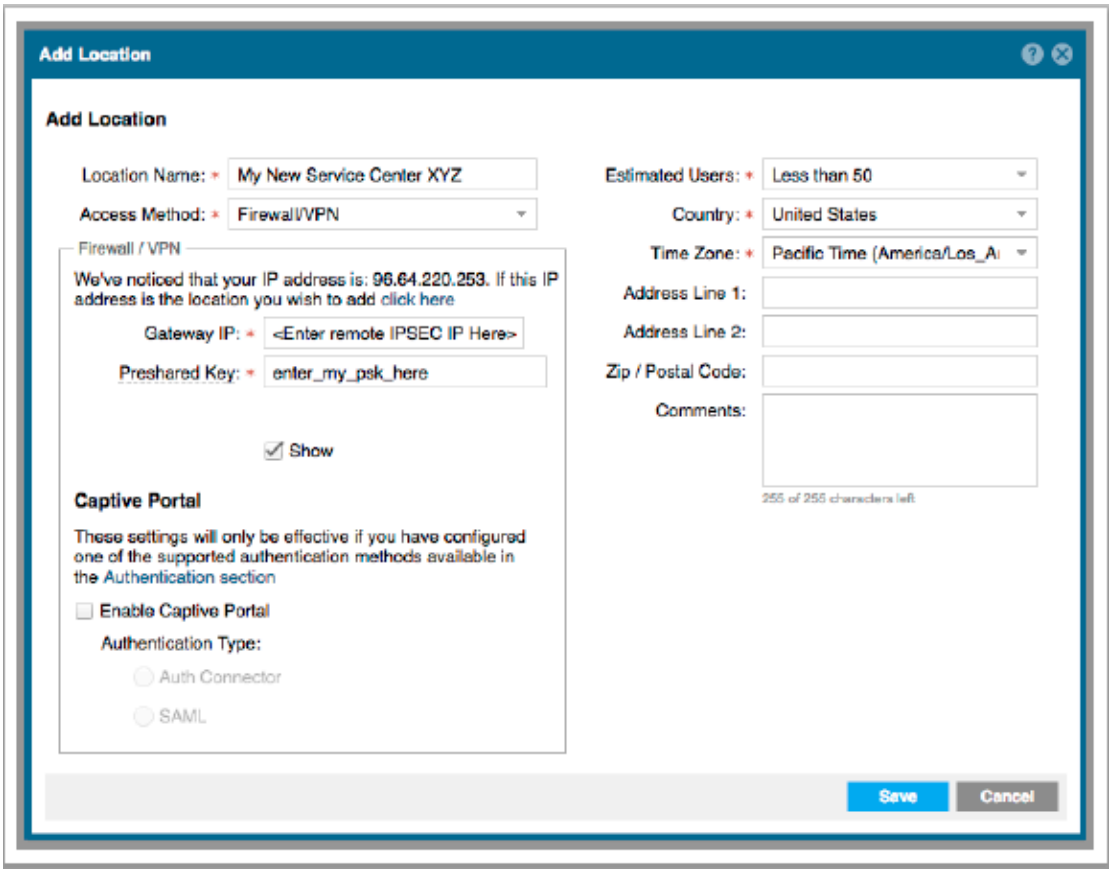
STEP 2 | Navigate to **Service** configuration.



STEP 3 | In the **Service** view, navigate to the **Networks** > **Locations** tab.



STEP 4 | Add a new **Location** for each Service Center Data Center you wish to onboard.



- **Location Name**: Add a descriptive name for the Service Center Data Center location.
- **Access Method**: Select 'Firewall/VPN' from the drop-down list.
- **Estimated Users**: Select the estimated number of users, taking into account the number of users from ‘ALL remote locations that will use this Service Center.
- **Country**: Select the Country of the Service Center Data Center.
- **Time Zone**: Select the Time Zone of the Service Center Data Center.
- **Firewall/VPN – Gateway IP**: Enter the Public IP of the Standard VPN IPSEC endpoint in the Service Center Data Center.
- **Firewall/VPN – Preshared Key**: Enter the Preshared key that is or will be used for this Service Center Data Center.

STEP 5 | Select **Save**.

Configure IPSEC Tunnel to Symantec Web Security Service

Traditional IPSEC routers or Prisma SD-WAN Service Center Cloud Connector are used to bridge the Prisma SD-WAN Secure Fabric to the Symantec Web Security Service.

Physical/Virtual Traditional IPSEC Router

STEP 1 | Configure the IPSEC router to perform the following:

1. BGP peer with the Prisma SD-WAN ION 7000 cluster.
2. Terminate IPSEC to the Symantec Firewall service.

STEP 2 | While every router configuration is different and a comprehensive guide is beyond the scope of this document, refer to the open-source router configuration example here.

1. Refer here to locate Symantec Web Security Services enpoint IP addresses.

Service Center Cloud Connector

Open a case via support@cloudgenix.com or https://support.prismasdwan.com to request early access to the Prisma SD-WAN Service Center Cloud Connector.

Sample Traditional IPSEC Router Configuration

Below is an example open-source router configuration that can be used optionally for Virtual Data Centers where desired.

This configuration was tested with VyOS (https://vyos.io/) Version 1.1.7.

```
/*The following IPs must be changed to match your environment.=
 52.10.10.10= 10.1.1.100, 10.1.1.101= 13.10.10.10= 14.10.10.10=
 10.1.0.1= 10.1.0.10/24= 10.1.1.10/24Public IP (Service Center
 DataCenter) Prisma SD-WAN ION 7000sSymantec Public Endpoint IP
 ASymantec Public Endpoint IP BDefault GatewayLocal system IP
 eth0Local system IP eth1*/#vyos-configinterfaces {ethernet eth0
 {address dhcpduplex autosmp_affinity autospeed auto}ethernet
 eth1 {address 10.1.1.10/24}loopback lo {}Prisma SD-WAN - Public
 Application Note 14vti vti0 {address 192.168.1.254/32ip {source-
validation disable}mtu 1436}vti vti1 {address 192.168.1.253/32ip
 {source-validation disable}mtu 1436}}protocols {bgp 7501 {neighbor
 10.1.1.100 {peer-group CLOUDGENIX}neighbor 10.1.1.101 {peer-
group CLOUDGENIX}peer-group CLOUDGENIX {nexthop-selfremote-as
 7502}}Prisma SD-WAN - Public Application Note 15static {/*Static
 routes - for active/active, set same AD.active/backup, make
 backup higher.*/interface-route 0.0.0.0/0 {next-hop-interface
 vti0 {distance 206}next-hop-interface vti1 {distance 208}}route
 13.10.10.10/32 {next-hop 10.1.0.1 {}}route 14.10.10.10/32 {next-
hop 10.1.0.1 {}}route 12.101.3.4/32 {next-hop 10.1.0.1 {}}}}Prisma
 SD-WAN - Public Application Note 16service {cloudinit {environment
 ec2}ssh {disable-host-validationdisable-password-authenticationport
 22}}system {host-name SC-CUSTOMER-SymantecWSS-us-east-1-CORE-
ROUTERtime-zone UTC}vpn {ipsec {esp-group ESP-1W {compression
 disablelifetime 3600mode tunnelpfs dh-group2proposal 1 {encryption
 3deshash sha1}}ike-group IKE-1W {ikev2-reauth nokey-exchange
 ikev1lifetime 28800proposal 1 {dh-group 2encryption 3deshash
 sha1Prisma SD-WAN - Public Application Note 17}}ipsec-interfaces
 {interface eth0}nat-networks {allowed-network 0.0.0.0/0 {}}site-
to-site {peer 14.10.10.10 {authentication {id 52.10.10.10mode pre-
shared-secretpre-shared-secret <REMOVED-ENTER-YOUR-OWN>}connection-
type initiateike-group IKE-GR1ikev2-reauth inheritlocal-address
 10.1.0.10vti {bind vti1esp-group ESP-GR1}}peer 13.10.10.10
 {authentication {id 52.10.10.10mode pre-shared-secretpre-shared-
secret <REMOVED-ENTER-YOUR-OWN>}connection-type initiateike-group
 IKE-GR1ikev2-reauth inheritPrisma SD-WAN - Public Application Note
 18local-address 10.1.0.10vti {bind vti0esp-group ESP-GR1}}}}}
```


Configure Prisma SD-WAN Secure Application Fabric

After the Symantec Firewall Service and Service Center Data Center IPSEC router or Cloud Connector are configured, the next step is to steer branch application traffic to the Firewall Services.

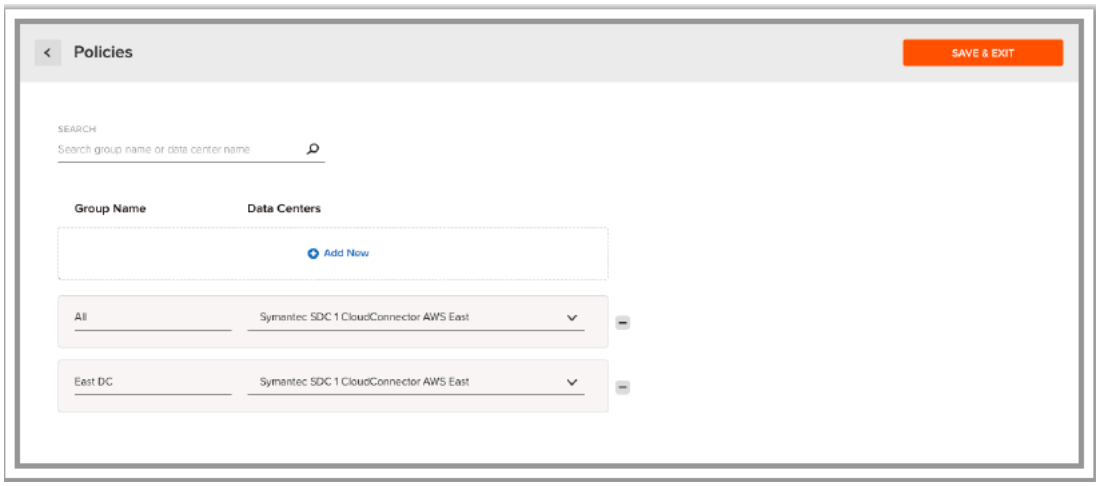
Some of the most common examples of how a traffic policy can be configured per application are:

- Send all Internet-bound traffic from a set of branches to the Symantec Firewall Service (Blanket Suspect list).
- Send all Internet-bound traffic from a set of branches to the Symantec Firewall service except for specific known applications. (Suspect list-Allow list).
- Send all Internet traffic direct to the Internet except for certain applications that need additional inspection or security. (Allow list-Suspect list).

The Prisma SD-WAN Secure Application Fabric enables granular controls for virtually unlimited number of policy permutations down to the sub-application level. The following configuration will use a **Blanket-Suspect list** style deployment:

STEP 1 | Create a Data Center Group that will include the Service Center Data Center(s).

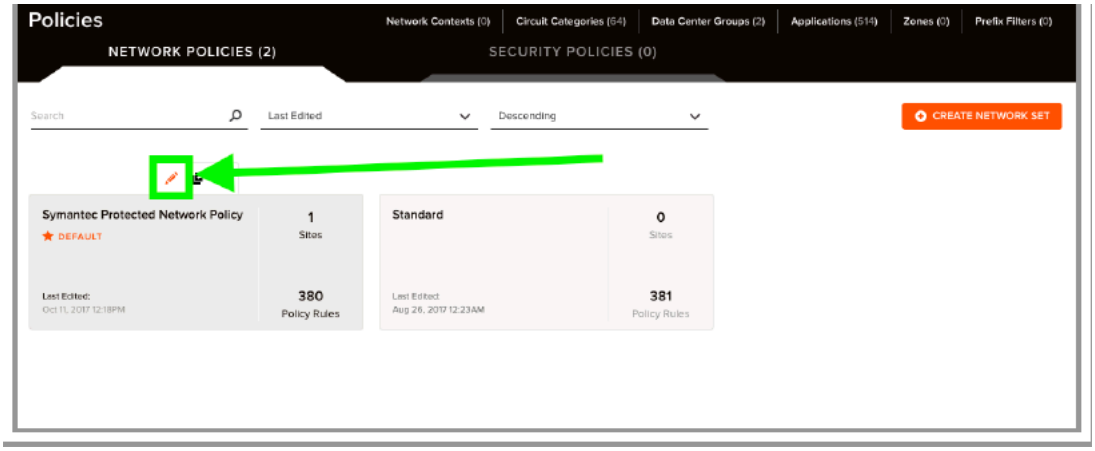
1. From the **Policies** tab, click **Data Center Groups**.
2. In the **Data Center Groups** window, click **Add New**.



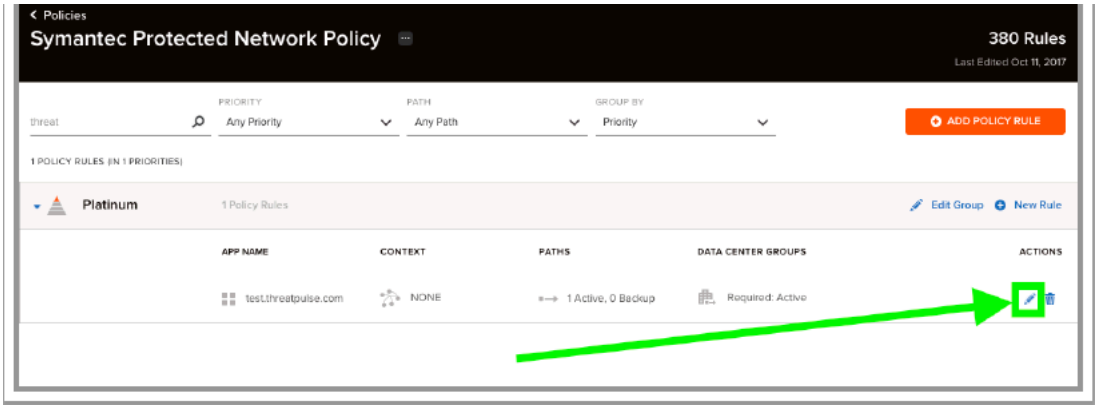
3. In the **Group Name** field, enter a descriptive name, such as **Web Security Services Bindings**.
4. Under **Data Centers**, select each Data Center that will participate in this group.

STEP 2 | Edit individual **Policy Set** rules to use the new **Service Bindings**.

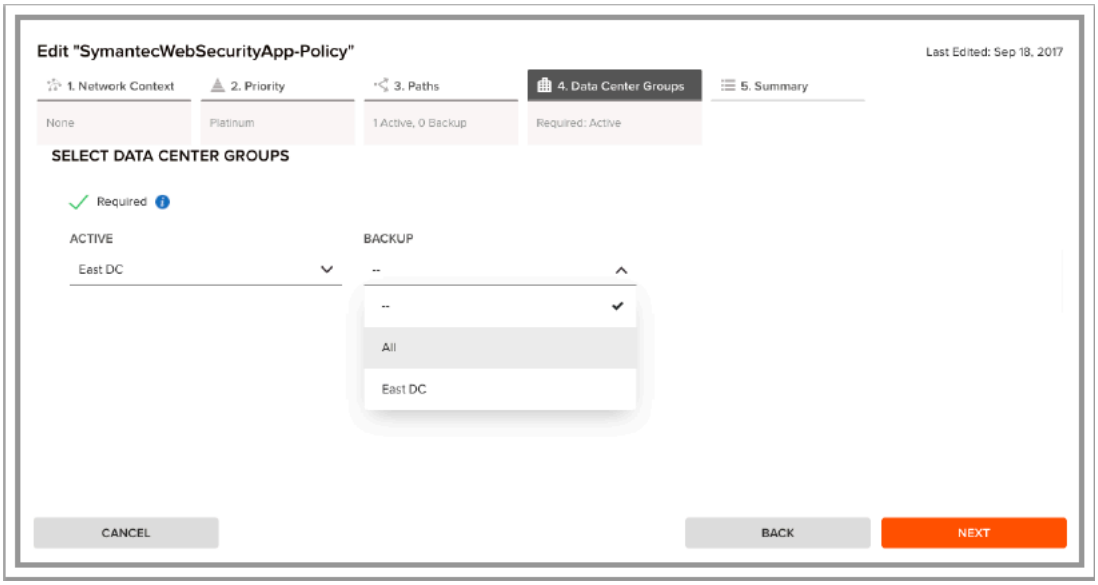
1. In the **Policies** screen, under the **Network Policies** tab, click the policy you wish to edit.



2. From this policy set, select one or more policy rules, and click the edit icon.

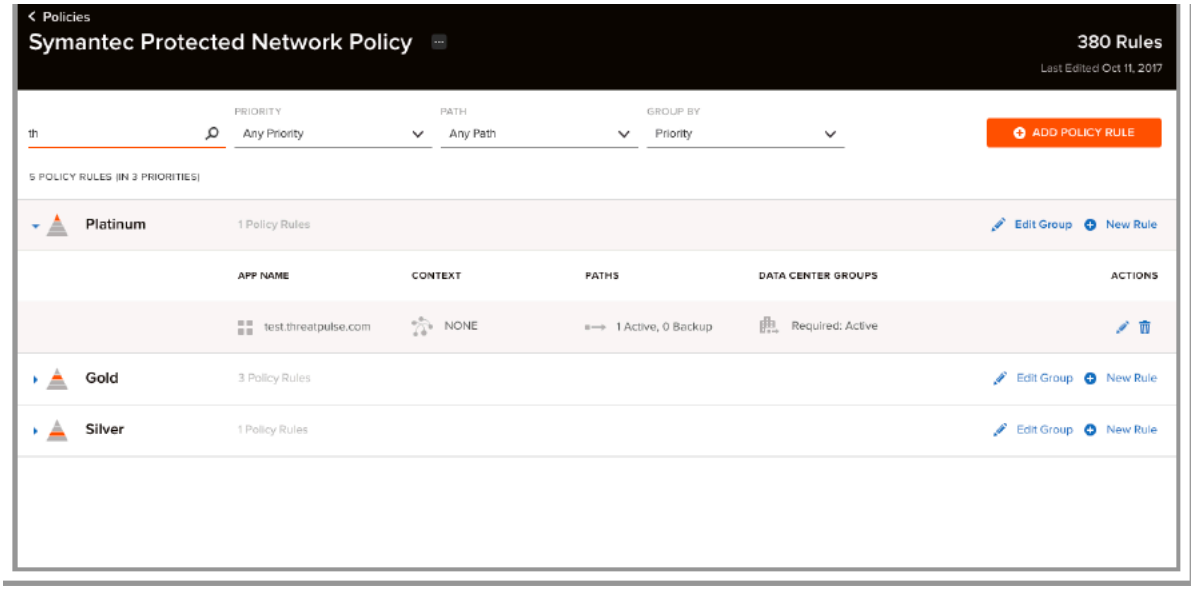


3. In the policy rule, click **Next** until you come to the **Service Group** option.
4. In Data Center Groups, select an Active and Backup Data Center Group for the application.



5. Optionally, the Data Center group can be flagged as **Required** for this policy rule.
   - If flagged as **Required**, the traffic must transit through these Data Centers or the traffic will be dropped.
   - Use of the **Required** flag also prevents any **Direct Internet** or **Direct MPLS** path from being allowed as an Active or Backup path.
6. Click **Next**, and select **Save** to apply the policy rule changes.

STEP 3 | Verify that the Policy rules have the appropriate Data Center Groups configured.



Enterprises can set up per-application, direct-to-cloud policies to deliver the cloud securely and with high performance to the remote office because of integration between Prisma SD-WAN and Symantec Web Security Services. At the same time, the remote office device footprint is minimal with rapid cloud-based services delivery.

