Creating Multiple Logical Networks on a Single ProxySG Appliance with Routing Domains

Version 7.1.x

Guide Revision: 12/6/2019

Symantec

Table of Contents

Overview of Routing Domains

In large network architectures, it is common for multiple logical networks to traverse the same set of physical network devices. Often, segregation of these networks is required to:

- Increase visibility
- Reduce maintenance cost
- Minimize security risk

Routing domains provide this segregation by partitioning network interfaces into disjoint groups that only allow traffic to be constrained to other interfaces in the same group. Traffic cannot traverse interfaces in different routing domains. Thus, network traffic is effectively segregated and can never cross routing domains.

Each routing domain object includes its own routing table that enforces Layer 3 segregation as follows:

- Each routing table is associated with one or more logical interfaces.
- IP traffic that arrives on these interfaces is subject to routing and forwarding decisions defined by the routing table.
- Traffic never crosses multiple routing domains.

Interfaces that are not assigned to any routing domain are automatically added to the default routing domain, which is subject to the configuration specified in the ProxySG appliance Management Console in **Configuration > Network > Routing**.

> **Note:** See "Limitations" on page 15 for more information about feature interoperability with the Routing Domains feature.

Use with Multi-Tenancy

You can associate routing domains with tenant identifiers to enforce tenant-specific policy on traffic. Configure a *tenant criterion*, which is what the appliance uses to associate traffic from a user network with a particular tenant ID when policy is evaluated. For more information, see "Configure Routing Domains for Multi-Tenancy" on page 14 and refer to the *Multi-Tenant Policy Deployment Guide* at MySymantec.

Create Routing Domains

Perform the following steps to create a routing domain:

Using the CLI

The procedures in this document assume that you are in Command Line Interface (CLI) configuration mode. Type the following commands to establish a connection with the CLI and enter configuration mode:

1. Open an SSH session with the appliance.
2. Enter your user name and password.
3. From standard mode, type the following commands to enter enable mode:

```
> en
Enable Password:
# conf t
Enter configuration commands, one per line.  End with CTRL-Z.
# (config)
```

Plan the Routing Domain

Before creating a routing domain, gather information about the existing network architecture. This document assumes that your network is already configured with the following.

Planning step	Required information
Associate physical or virtual interfaces with a routing domain	Physical interfaces or VLANs
Set the default routing table used for some services (see Limitations)	IPv4 or IPv6 IP address to be used as the default gateway
Specify the static routing table for a routing domain	Destination subnet, gateway
Associate a forwarding group with a routing domain	DNS forwarding group name
Associate an authentication realm with a routing domain	IWA-BCAAA or LDAP realm name

Identify and Configure Interfaces to be Used in the Routing Domain

To segregate traffic, you must associate the routing domain with one or more interfaces. These can be physical interfaces or VLAN interfaces.

Using the network information gathered in Task 1, decide which interfaces to use for each routing domain. Then, configure these interfaces as described in the following sections.

Configure Physical Interfaces

To assign IP addresses to a physical interface using the CLI:

1. Enter CLI configuration mode (as described in "Using the CLI" on page 4).
2. Enter the interface editing mode:

   ```
   # (config) interface adapter_number:interface_number
   ```

3. Set the IP address and subnet mask or prefix length:

   IPv4:

   ```
   # (config interface adapter:interface) ip-address ip_address {subnet_mask | network_prefix_
   length}
   ```

   IPv6:

   ```
   # (config interface adapter:interface) ip-address ip_address network_prefix_length
   ```

Example

IPv4:

```
# (config) interface 1:1
# (config interface 1:1) ip-address 198.51.100.7 255.255.255.0
  ok
```

IPv6:

```
# (config) interface 1:1
# (config interface 1:1) ip-address 2001:db8:85a3::8a2e:370:7334 48
  ok
```

Configure VLAN Interfaces

To assign IP addresses to a VLAN interface using the CLI:

1. Enter CLI configuration mode (as described in "Using the CLI" on page 4).
2. Enter the VLAN interface editing mode:

   ```
   # (config) interface adapter_number:interface_number.vlan_id
   ```

3. Set the IP address and subnet mask or prefix length:

   IPv4:

   ```
   # (config interface adapter:interface.vlan_id) ip-address ip_address {subnet_mask | network_prefix_length}
   ```

   IPv6:

   ```
   # (config interface adapter:interface.vlan_id) ip-address ip_address network_prefix_length
   ```

Example

IPv4:

```
# (config) interface 1:1.2
# (config interface 1:1.2) ip-address 198.51.100.7 255.255.255.0
  ok
```

IPv6:

```
# (config) interface 1:1.2
# (config interface 1:1.2) ip-address 2001:db8:85a3::8a2e:370:7334 48
  ok
```

Create and Configure the Routing Domain

Complete the following tasks to create and configure the routing domain.

1. Create the routing domain.
   a. Enter CLI configuration mode (as described in "Using the CLI" on page 4).
   b. Enter the routing domain mode:

      ```
      # (config) routing-domains
      ```

   c. Create the routing domain:

      ```
      # (config routing-domains) create routing_domain_name
      ```

   d. Edit the routing domain you just created:

      ```
      # (config routing-domains) edit routing_domain_name
      ```

2. Associate interfaces to the routing domain.

   Physical interface:

   ```
   # (config routing_domain_name) interface adapter_number:interface_number
   ```

   VLAN interface:

   ```
   # (config routing_domain_name) interface adapter_number:interface_number.vlan_ID
   ```

3. Define the default route for the routing domain. Optionally, specify an existing preference group for the gateway and assign a relative weight. The weight determines how much bandwidth a gateway is given relative to the other gateways within the group.

   ```
   # (config routing_domain_name) default-gateway ip_address [preference_group [weight]]
   ```

   where *preference_group* is a value between 1 and 10 and *weight* is a value between 1 and 100.

4. (Optional) Define static routes for the routing domain.

   ```
   # (config routing_domain_name) inline static-route-table EOF
   {destination subnet_mask | destination/network_prefix_length} gateway
   {destination subnet_mask | destination/network_prefix_length} gateway
   {destination subnet_mask | destination/network_prefix_length} gateway
   ...
   EOF
   ```

5. (Optional) Create a DNS forwarding group and associate it with the routing domain.

```
# (config dns-forwarding) create group_alias [host_ip]
# (config dns-forwarding) edit group_alias
# (config dns-forwarding group_alias) routing-domain routing_domain_name
```

6. (Optional) Associate an LDAP authentication realm with a routing domain.

```
# (config) security ldap edit realm_name
# (config ldap realm_name) routing-domain routing_domain_name
```

7. (Optional) Associate an IWA-BCAAA authentication realm with a routing domain.

```
# (config) security iwa-bcaaa edit realm_name
# (config iwa-bcaaa realm_name) routing-domain routing_domain_name
```

8. Enable IP Forwarding to handle bypass traffic.

```
# (config) tcp-ip ip-forwarding enable
```

Example

```
# (config) routing-domains
# (config routing-domains) create Midwest_Center
  ok
# (config routing-domains) edit Midwest_Center
# (config Midwest_Center) interface 1:1
  ok
# (config Midwest_Center) default-gateway 198.51.100.1
  ok
# (config Midwest_Center) inline static-route-table EOF
198.51.101.0 255.255.255.0 198.51.100.1
198.51.102.0 255.255.255.0 198.51.100.1
198.51.203.0 255.255.255.0 198.51.100.2
2001:db8:100::/48 2001:db8:85a3::1
EOF
# (config Midwest_Center) exit
# (config routing-domains) exit
# (config) dns-forwarding
# (config dns forwarding) create primary
 ok
# (config dns forwarding) edit primary
# (config dns forwarding primary) routing-domain Midwest_Center
  ok
# (config dns-forwarding primary) exit
# (config dns-forwarding) exit
# (config) security ldap edit LDAP1
# (config ldap ldap1) routing-domain Midwest_Center
  ok
# (config) tcp-ip ip-forwarding enable
  ok
```

Verify the Routing Domain

Verify that the routing domain is configured correctly to reach target addresses and how to view routing domain information.

Verify Network Paths

Use the `ping` command to verify that traffic is routed properly through your routing domain. The command accepts the routing domain name as an argument. The syntax is as follows:

```
# ping ip_address routing_domain_name
```

Example

IPv4:

```
# ping 198.51.100.11 Midwest_Center
```

IPv6:

```
# ping6 2001:db8:85a3::1 routedomain1
```

Confirm Routing Domain Information

Display all configured routing domains:

```
# (config) routing-domains
# (config routing-domains) view
```

Example

```
# (config) routing-domains
# (config routing-domains) view
   Supply1
   Supply2
   Supply3
```

Display configuration information about a specified routing domain:

```
# (config) routing-domains
# (config routing-domains) edit routing_domain_name
# (config routing_domain_name) view
```

Example

```
# (config) routing-domains
# (config routing-domains) edit MidWest_Center
# (config Midwest_Center) view
Routing domain 1 : Midwest_Center
Internet:
Destination        Gateway            Flags    Refs      Use      Netif Expire
Internet6:
Destination                             Gateway                         Flags       Net

                               if Expire
fe80::%1:1/64                     link#3                          UC            1:1
fe80::2d0:83ff:fe05:a7d4%1:1      00:d0:83:05:a7:d4               UHL      loopback
ff01:3::/32                       link#3                          UC            1:1
ff02::%1:1/32                     link#3                          UC            1:1
```

Display information about the default routing table and all routing domains:

```
# show ip-route-table
```

Example

```
# show ip-route-table
Routing tables
Route-domain 0 : default
Internet:
Destination        Gateway            Flags    Refs      Use      Netif Expire
default            10.9.40.1          GS          1      346        1:0
10.9.40.0/22       link#4             UC          0        0        1:0
10.9.40.1          link#4             UHRLW       1       10        1:0
127.0.0.1          127.0.0.1          UH          1  1265965   loopback
Internet6:

Destination                       Gateway                       Flags        Netif Expire
::1                               link#1                        UHL      loopback
fdbd:f29e:8f1c::                  00:d0:83:05:a7:d2             UHL      loopback =>
fdbd:f29e:8f1c::/48               link#2                        UC            0:0
fe80::%0:0/64                     link#2                        UC            0:0
fe80::2d0:83ff:fe05:a7d2%0:0      00:d0:83:05:a7:d2             UHL      loopback
fe80::%1:0/64                     link#4                        UC            1:0
fe80::2d0:83ff:fe05:a7d3%1:0      00:d0:83:05:a7:d3             UHL      loopback
ff01:1::/32                       ::1                           UC       loopback
ff01:2::/32                       link#2                        UC            0:0
ff01:4::/32                       link#4                        UC            1:0
ff02::%loopback/32                ::1                           UC       loopback
ff02::%0:0/32                     link#2                        UC            0:0
ff02::%1:0/32                     link#4                        UC            1:0
```

```
Route-domain 1 : Midwest_Center
Internet:
Destination        Gateway            Flags     Refs      Use      Netif Expire
Internet6:
Destination                       Gateway                       Flags        Netif Expire
fe80::%1:1/64                     link#3                        UC            1:1
fe80::2d0:83ff:fe05:a7d4%1:1      00:d0:83:05:a7:d4             UHL      loopback
ff01:3::/32                       link#3                        UC            1:1
ff02::%1:1/32                     link#3                        UC            1:1
```

Configure Routing Domains for Multi-Tenancy

You can use existing routing domains to determine tenancy in a multi-tenant deployment, for example, with the CLI command `# (config general) multi-tenant criterion $(client.interface.routing_domain)`. Refer to the *Multi-Tenant Policy Deployment Guide* at MySymantec for details.

To configure routing domains for multi-tenancy:

1. Assemble information about the existing network, such as:
    - VLAN architecture (VLAN IDs, subnet information)
    - How you want to isolate the subnets.
2. Plan your routing domains, such as:
    - Network information (default route, required static routes)
    - Associate the specified routing domain with a supported authentication realm and refer to the realm in tenant-specific policy. IWA-BCAAA and LDAP are supported for multi-tenant authentication.
3. Configure routing domains in the CLI. See "Create and Configure the Routing Domain" on page 8 for instructions.
4. Set up the multi-tenant deployment. Refer to the *Multi-Tenant Policy Deployment Guide* at MySymantec.

Limitations

The routing domains feature has the following limitations:

- Only IWA-BCAAA and LDAP realms are supported for multi-tenant authentication.
- Overlapping subnets between routing domains are not supported.
- The following traffic, services, and features can use only the default routing table:
  - All ProxySG appliance management traffic.
  - WCCP configuration on the appliance.
  - VLANs, ICAP services, and forwarding hosts configured on the appliance.
  - All requests originating from the appliance (such as subscriptions, access log upload, and support case upload).

Supporting Documentation

Before implementing the best practices described in this document, and as needed to maintain your deployment, refer to the following documents available at MySymantec.

Document	Overview
Multi-Tenant Policy Deployment Guide https://www.symantec.com/docs/DOC10360	How to configure Multi-Tenant Policy configurations in SGOS 6.6.x and later. A ProxySG appliance administrator can employ Multi-Tenant policy to segregate policy for distinct groups of users.
Command Line Interface Reference https://www.symantec.com/docs/DOC11475	Commands available in the ProxySG appliance CLI and how to use them to perform configuration and management tasks.
SGOS Upgrade/Downgrade Guide https://www.symantec.com/docs/DOC9794	Steps for upgrading or downgrading SGOS. Also covers behavior changes and policy deprecations.
ProxySG Web Visual Policy Manager WebGuide https://www.symantec.com/docs/DOC11478	How to create and implement policy in the ProxySG appliance's web-based Visual Policy Manager, including layer interactions, object descriptions, and advanced tasks.
Legacy Visual Policy Manager Reference https://www.symantec.com/docs/DOC11477	How to create and implement policy in the ProxySG appliance's legacy Visual Policy Manager.
Content Policy Language Reference https://www.symantec.com/docs/DOC11416	CPL gestures available for writing the policy by which the ProxySG appliance evaluates web requests.
SGOS Administration Guide https://www.symantec.com/docs/DOC11474	Detailed information for configuring and managing the ProxySG appliance.
Required ports, protocols, and services for the ProxySG appliance https://www.symantec.com/docs/INFO5294	Basic configurations, and some commonly used options, for ports and protocols.
First Steps Deployment Guide http://www.symantec.com/docs/DOC10940	How to get a ProxySG up and running in a Secure Web Gateway (SWG) deployment.
SSL Proxy Deployment Guide http://www.symantec.com/docs/DOC10325	Best practices for deploying the SSL proxy. The SSL proxy improves visibility into SSL traffic, allowing security policies and logging to be applied to encrypted requests and responses, and can enhance performance by caching encrypted data.
Reverse Proxy Deployment WebGuide http://www.symantec.com/docs/DOC11574	How to deploy a ProxySG appliance as a front-end for Internet-based users to access secure application, content, and web servers.

Document	Overview
Web Application Firewall Solutions Guide http://www.symantec.com/docs/DOC10451	How to configure Symantec WAF solution to protect your web servers, accelerate web content, and simplify operation.
Secure Web Gateway - Content Analysis Policy Best Practices Improvement http://www.symantec.com/docs/DOC10920	Provides a secure and customizable policy model for bypassing content scanning to improve the user experience where needed or save resources by excluding low-risk/high-volume traffic. This document identifies weak policy conditions and is intended to reduce risk by using different sets of policy conditions.
SGOS 7.1.x Documentation https://www.symantec.com/docs/DOC11385	Full list of documentation published for SGOS 7.1.x.
SGOS Release Notes SGOS Release Notes are available on the **Downloads** page. Log in to MySymantec with your MySymantec credentials to access the release image and release notes.	Changes, issues, fixes, and limitations pertaining to SGOS releases. Also includes any related security advisory (SA) fixes.

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

www.symantec.com

Friday, December 6, 2019