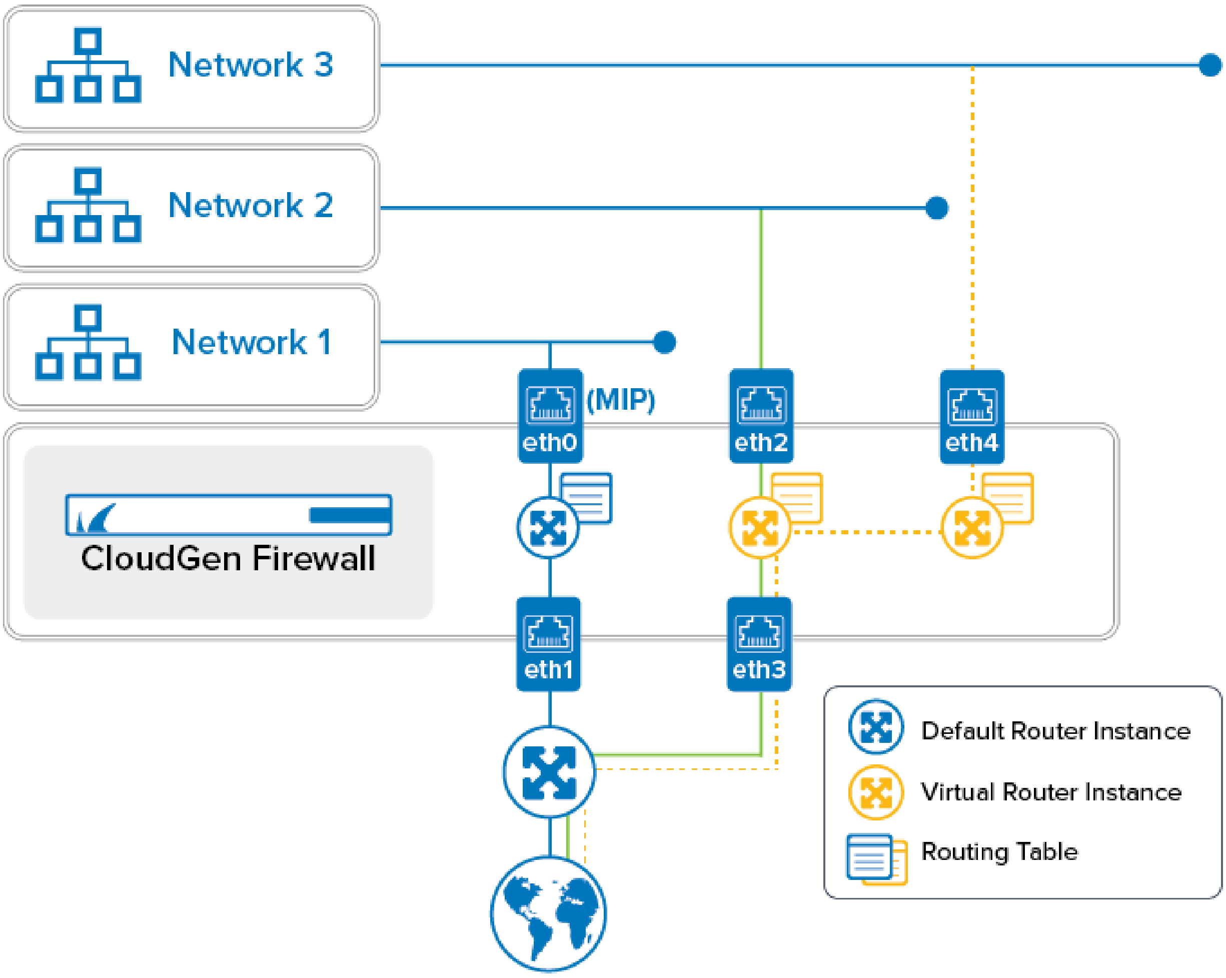
Virtual Routing and Forwarding (VRF)

https://campus.barracuda.com/doc/79462771/

Virtual routing and forwarding (VRF) is a technology based on the operating principle of a physical router. Unlike a single router, virtual routers (VR) can be run simultaneously as multiple instances. Each of these instances uses its own routing and forwarding table. Because each virtual router instance (VRI) runs autonomously, network traffic on the assigned interfaces is separated from the traffic managed by other virtual routers. This special separation of networks increases network security without having to use VPNs like on a common network. Because it is possible to use the same IP addresses or IP ranges on multiple virtual routers, which can even overlap without conflicting with each other, virtual routers can also be used for managing network traffic for multiple networks with identical network configurations simultaneously on the firewall.

Virtual routing can be used to segment network paths without using additional devices. The number of network paths is limited only by the number of available network interfaces. The concept of keeping traffic on multiple network paths separated can be overridden by configuring access rules that forward specific traffic from one path to another. As an example, all traffic from different network paths can be routed to a common path that leads to the Internet, thereby reducing the overhead of configuring access rules for routed traffic that flows from different networks to the Internet simultaneously. By combining different types of interface types, like network, VLAN, or bundled interfaces, the different possibilities offer a huge variety of applications.



Because the access point daemon currently only operates in the default namespace, Wi-Fi interfaces are currently not supported in non-default namespaces.

Virtual Routing and Forwarding therefore does not currently support Wi-Fi!

Virtual Router Naming and Identification

For configuration purposes, each virtual router instance receives a unique logical ID and a name. The firewall's standard routing instance is named 'default' and has the virtual router ID = 0. These two values cannot be changed. Unlike a user-defined virtual router instance, the default router instance cannot be deleted. Every additional virtual router instance can be configured individually. The virtual router IDs are set automatically in the range between 1 and 255 when a new instance is created. The virtual router ID can also be entered manually for special purposes, e.g., for configuring an HA cluster where all virtual routers must be configured identically on both HA partners. In addition, this ID is required for assigning virtual router instances in VPN configurations.

Never change a VR ID that has already been assigned to a VR instance!

If it is necessary to change the VR ID of a virtual router instance, be prepared to *plan* the usage of VR IDs. In case VR instances are already configured, delete existing VR instances completely from the firewall before assigning new IDs!

Maximum Number of Virtual Router Instances for a Certain Model

---

Virtual Routers help split traffic from a single stream into multiple streams with less traffic per each additional VR instance and thus contribute to a better overview. However, a VR instance does not add further resources like additional memory or bandwidth capacity to the appliance.

IMPORTANT

Keep in mind that using a virtual router instance does not add memory or bandwidth capacity to your firewall.

Because every firewall is already operating with a default router, every additional virtual router instance will share the built-in memory and thus reduce the remaining free memory for each further instance. Also, consider that every additional VR instance requires some of the shared memory for its own management.

Keep track of the memory usage at **DASHBOARD > RESOURCES**, **Memory Usage**.

The following table lists the maximum number of additionally configurable router instances depending on a certain firewall model:

Model	Total VRF Instances including the Default Router Instance
F12	11
F18	11
F80	11
F82	11

F93	11
F180	11
F183R	11
F183	11
F183R	11
F193R	11
F200, F201, F300, F301	n.a.
F280	11
F380	11
F400	11
F600	11
F800	16
F900	21
F1000	26
Cloud Level 1	1
Cloud Level 2	2
Cloud Level 4	4
Cloud Level 6	6
Cloud Level 8	8
VF10, TSF10, TSFp10	1
VF25, TSF25, TSFp25	1
VF50, TSF50, TSFp50	1
VF100, TSF100, TSFp100	2
VF250, TSF250, TSFp250	2
VF500, TSF500, TSFp500	4
VF1000, TSF1000, TSFp1000	6
VF2000, TSF2000, TSFp2000	8
VF4000, TSF4000, TSFp4000	10
VF8000, TSF8000, TSFp8000	20
VFC1	1
VFC2	2
VFC4	4
VFC6	6
VFC8	8
T100, T200, T400, T600	11
T900	21

VT100	2
VT500	4
VT1500	8
VT3000	10
VT5000	20

Virtual Routers, Network and Dynamic Interfaces, VLAN, and Ethernet Bundled Interfaces

VLANs can be configured for each network interface. If necessary, both network and VLAN interfaces can be combined with Ethernet bundled interfaces. With their specific characteristics, each of these interface types can be assigned to a virtual router.

Interface	Supported
Network Interfaces (eth0, eth1, ...)	Yes
Bundled Interfaces	Yes
VLAN Interfaces	Yes
Dynamic Interfaces	No

Management Interface and Virtual Routers

Because licenses are bound to the MAC address of the network interface on which the management IP is configured, the management interface must always reside under the control of the default router.

Never assign the management IP to an interface that is managed by an additional virtual router instance unless you want your firewall to fall back into grace mode.

For more information about the grace period and the validity of licenses, see Validity.

Remote Management Tunnels and Virtual Routers

Default routes can also be assigned to VR instances. When you must manage your firewall via a remote management tunnel, always configure a default route on the default router instance. This is necessary because the connection service on port 692 for the remote management tunnel is supported only in the default router instance.

When managing your firewall using a remote management tunnel, never delete the default route on your default router instance unless you want to avoid that your firewall is manageable by the Control Center!

For more information on how to configure a remote management tunnel, see How to Configure a Remote Management Tunnel for a CloudGen Firewall.

Virtual Routers and Services

All services that run on top of a server are available only for the default router instance. Some services can be used on additional virtual router instances if certain conditions are met:

Service / Feature	Availability for default VR	Availability for additional VRs	Comments
Access Control Service	*Yes	No	*Only for administrative purposes
DHCP Relay Service	Yes	No	
DHCP Service	Yes	No	
DNS Service	Yes	No	
FTP Gateway Service	Yes	No	
Firewall Service	Yes	*Yes	*Only if authenticated users are NOT defined.
HTTP Proxy	Yes	No	
IPS	Yes	*Yes	*Only if authenticated users are NOT defined.
Mail Gateway	Yes	No	
OSPF/RIP/BGP Service	Yes	No	
SNMP Service	Yes	No	
Spam Filter Service	Yes	No	
SSH Proxy Service	Yes	No	
URL Filter Service	Only available for HTTP Proxy. *Available for the Firewall service.	No	*Check license dependency for Application Control.
Access Controller VPN Service	Yes	No	

VPN Service	Yes	Yes: using VPN Interface Index. • Only TINA and site-to-site VPN. • No IKEv1/v2. • No client-to-site VPN.	
Virus Scanner Service	*Yes	*Yes	*If the feature is licensed. See also Virtual Routers and Application Control below.
Local DNS cache	Yes	No	Also available for additional virtual routers if traffic is redirected to the default router.
DNS Interception	Yes	No	Also available for additional virtual routers if traffic is redirected to the default router.

Virtual Routers and Application Control

If Application Control is licensed, some restrictions may apply.

Feature	Available to default VR	Available to additional VRs
Application Control	Yes	Yes
SSL Inspection	Yes	Yes
URL Filter in the Firewall	Yes	For firewall service only
Virus Scanner	Yes	Only configurable for default VR instance. Configuration of default router applies.
ATP	ATP scan is available. Quarantine available.	ATP scan is available. Quarantine is NOT available.
File Content Scan	Yes	Yes
Archive Content Scan	Yes	Yes
Mail DNSBL Check	Yes	Yes
Link Protection	Yes	Yes
SafeSearch	Yes	Yes
Google Accounts	Yes	Yes

Virtual Routers and Access Rules

Access rules control how and whether traffic can pass from one interface to another. If only one router is used on the firewall, managing an access rule in the rule list is straightforward. However, if multiple virtual router instances live side by side in a common environment, it is recommended to build rule lists in order to maintain an overview of the access rules that refer to different virtual router instances.

For more information, see How to Create New Rule Lists.

Configuring and Activating Virtual Routers

Configuring a virtual router is similar to configuring IP addresses and routing tables. However, there are some differences in the workflow due to the conditions described in this article.

For more information, see How to Configure and Activate a Virtual Router Instance with Hardware, Virtual, VLAN, or Bundled Interfaces.

Redirecting Traffic between Multiple Virtual Router Instances

The idea of virtual routers is to separate traffic between multiple network paths. In certain cases, however, it may be useful to redirect traffic between separated paths or from multiple paths to a common path, e.g., to the Internet.

For more information, see How to Redirect Traffic between Multiple Virtual Router Instances.

Virtual Routers and High Availability

Virtual routers can also be configured on HA partners. Because HA partners must (with some exceptions) be configured identically, there are three different ways of configuring virtual routers depending on how the partners are managed in a network environment. In all cases, the administrator is responsible for setting up an identical configuration in order to ensure that syncing between the two HA partners will work as expected.

- For more information on how to configure two stand-alone firewalls working as HA partners, see

How to Configure High Availability Stand-Alone CloudGen Firewalls for Virtual Routing.
- For more information on how to configure two CC-managed firewalls working as HA partners, see How to Configure High Availability CC-Managed CloudGen Firewalls for Virtual Routing.

Virtual Routers and VPN

Virtual routers also support Virtual Private Networks (VPNs). The VPN service is fully available to the default router instance. When using a VPN in connection with an additional virtual router, TINA and site-to-site VPN are the only protocols supported. Client-to-site VPN and IKEv1/V2 tunnels are not available to additional virtual routers.

Figures