Connection Objects

https://campus.barracuda.com/doc/96026255/

Connection objects define the egress interface and source (NAT) IP address with the following **Translated Source IP Policies:**

- **Original Source IP** – The source IP address of the packet is not changed.
- **Dynamic NAT** – The firewall uses the routing table to find a suitable interface for routing the packet and uses the IP address of the relevant interface as the new source IP address.
- **First Shared IP** – Source NAT using the **First IP** of the **Shared IPs**.
- **Second Shared IP** – Source NAT using the **Second IP** of the **Shared IPs**.
- **Network Interface** – Source NAT using the first IP address assigned to the network interface. Only used for dynamic interfaces such as DHCP or PPP.
- **Single IP Network Object** – Source NAT using the IP address in the selected network object. The network object must use the type **Single IP Address**. For static interfaces, use **Explicit IP** instead.
- **Explicit IP** – Source NAT using the entered IP address as the translated source IP address.
- **Explicit Network Mapping** – Maps the source IP address to a new source network. Make sure that the source range using this connection is equal to or smaller than the map range. If not, the firewall will wrap the larger source net into the smaller bind net. For example, if you use X.X.X.X/24 network as the source and a Y.Y.Y.Y/25 as the map range, the IP address X.X.X.128 is mapped to Y.Y.Y.1.

Default Connection Objects

You can create custom connection objects, or use the predefined connection objects:

- **Dynamic NAT** – The firewall uses the routing table to find a suitable interface for routing the packet and uses the IP address of the relevant interface as the new source IP address.
- **Original Source IP** – The source IP address of the packet is not modified.
- **Translated IP from WWAN Interface** – The first IP address on the ppp5 device is used as the new source IP address.
- **Translated IP from DHCP Interface** – The first IP address on the DHCP device is used as the new source IP address.
- **Translated IP from DSL Interface** – The first IP address on the ppp1 device is used as the new source IP address.

Custom Connection Objects

Custom connection objects are needed for all connection methods that are not covered by the default connection objects. This also includes connection objects used for failover and load balancing as well as for VPN SD-WAN and dynamic mesh settings.

For more information, see How to Create a Custom Connection Object.

Failover and Link Load Balancing

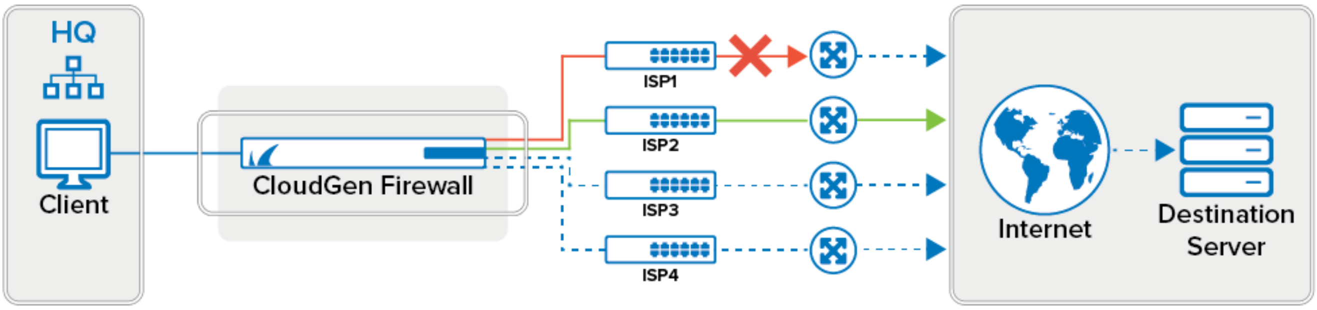
It is common for locations to use multiple Internet connections and share the bandwidth between them for both outgoing link balancing and failover. If one Internet connection goes down, traffic is simply routed over the other connections that are still running. Basic link failover functionality can be achieved by using different route metrics. A better solution, however, is to use custom connection objects to distribute the load and/or configure failover for different links. Using custom connection objects allows you to decide which Internet connection is used on a per-access-rule basis. The logic of how traffic is distributed over the available interfaces is configured in the **Failover and Load Balancing** section of the connection object. The policy can be set to:

None

No failover or connection cycling. When the connection goes down, the route is set to a metric of 65536 or higher. Routes above 65535 are considered to be down. If there is no other matching route, the firewall still attempts to use the route. This most likely results in a connection timeout.

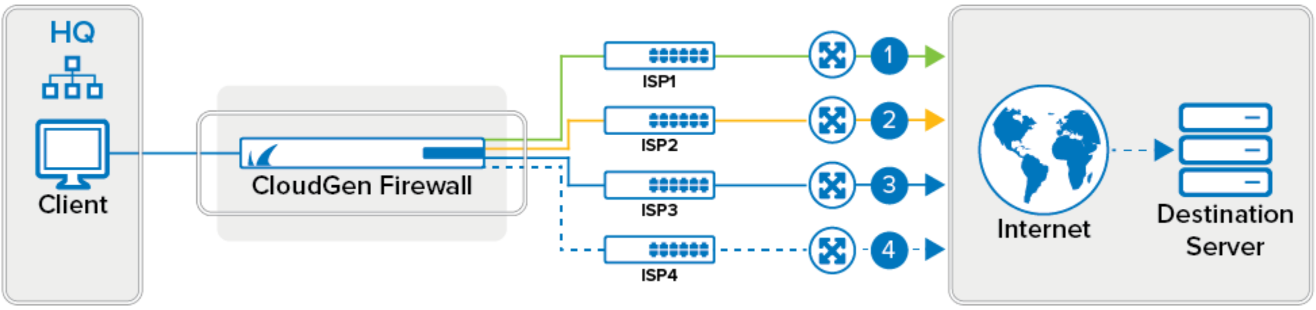
Failover

Failover to alternative interface or source IP address. Traffic is rerouted over the next configured alternative until no further options are available.



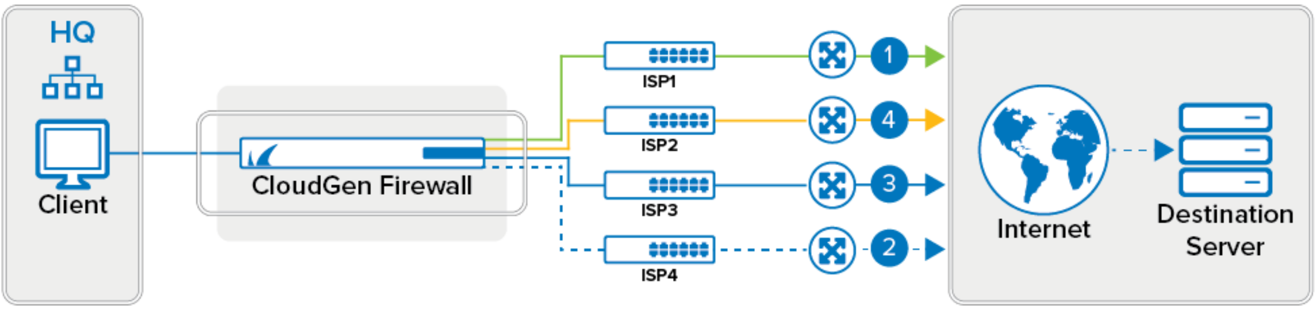
Weighted Round Robin

Sequentially cycles through the configured primary and alternative connections. You can influence the distribution by assigning a weight to the source IP or interface. Interfaces with higher weight numbers are used more often. When a link is not available (route is over 65535 or not present at all), the session fails over to the next configured alternative, without regard to the configured weight. To mitigate this problem, group the connections with higher weight numbers together. Doing so will enable you to avoid failure of high bandwidth links causing too much traffic on a slower, alternative link.



Weighted Random

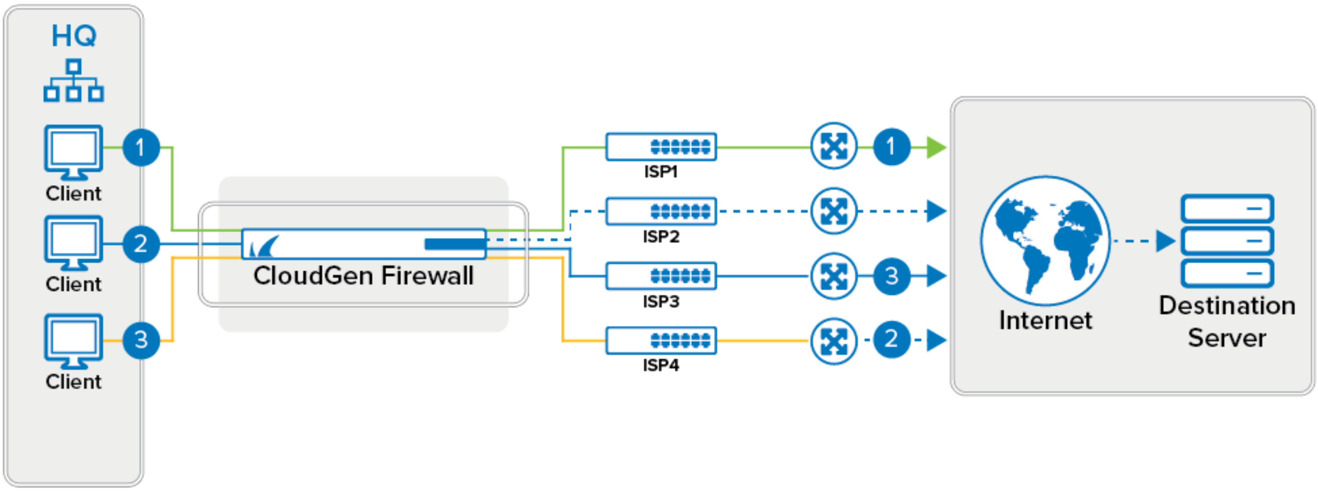
Randomizes the source IP addresses or interfaces. Sessions are distributed randomly over all configured source IP addresses/interfaces. You can influence the distribution by assigning a weight to the source IP or interface. Interfaces with higher weight numbers are used more often.



Source IP Hash

The hash of the source IP address is used to determine the egress interface. For applications that require sticky sessions, use this load-balancing policy. This setting is persistent as long as the source IP address of the client is not changed. When a link is not available (route is over 65535 or not present at all), the session fails over to the next configured alternative, without regard to the configured weight.

For more information, see How to Configure Link Balancing and Failover for Multiple WAN Connections.



Provider Optimization

Provider Optimization selects the optimal TCP connection by determining the provider with the fastest response time to TCP probing packets sent by the CloudGen Firewall.

For more information, see How to Configure Failover and Load Balancing in Custom Connection Objects.

NAT Tables (Translation Maps)

NAT Tables are an expanded type of source NAT for a network. The NAT Tables connection object rewrites the source IP address to the translated network. To rewrite both the destination and the source address of the connection, you can choose to use a NAT Table connection object with a MAP access rule. You can enter multiple rewriting maps that are processed from the top to the bottom. The first matching rewrite map is used.

For more information, see How to Create NAT Tables (Translation Maps).

Multipath Routing

Multipath routing is used when multiple paths are used to route traffic through a single target network. Multipath routing offers benefits such as increased bandwidth. When a session is established, the firewall assigns a network path to the session based on the source address.

For more information, see How to Configure Multipath Routing.

VPN SD-WAN Settings

The SD-WAN settings of the connection objects allow you to assign a VPN transport to the traffic matching the rule. You can also define the failover behavior and the SD-WAN primary/secondary settings.

For more information, see SD-WAN.

Dynamic Mesh Settings

If you are using a dynamic mesh VPN network, the dynamic mesh settings in the SD-WAN section allow you to configure if traffic matching this rule should use a dynamic tunnel and if the traffic should keep the dynamic tunnel open.

For more information, see Dynamic Mesh VPN Networks.

Figures