WAN Connections

https://campus.barracuda.com/doc/95258636/

The Barracuda CloudGen Firewall supports all commonly used WAN connection types: static, DHCP, xDSL, Wireless WAN, and ISDN. Link failover and link balancing can be configured either on a per-access-rule basis by using custom connection objects, or in a more basic configuration via route metrics. You can also select different Internet connections based on the application type.

Static Internet Connections

If your ISP assigns a static IP address or network to your Internet connection, configure a static Internet connection to connect the firewall to the Internet. You must add a route on the box layer for the network port the ISP is connected to. The connection becomes active when the assigned IP address or the IP address within the assigned network is configured as a box IP address, for example, if the unit is remote managed and an additional IP address is defined on box layer.

For more information, see How to Configure an ISP with Static IP Addresses.

DHCP Connections

DHCP client connections are similar to xDSL links. When an interface is assigned to a DHCP client configuration, it is removed from the list of available interfaces. You can view your DHCP client connections on the **CONTROL > Network** page. A maximum number of twelve links can be connected.

For more information, see How to Configure an ISP with Dynamic IP Addresses (DHCP).

xDSL Connections

The firewall supports dial-in PPPoE, PPPoA, and PPTP connections using an external DSL modem, or PPPoE, PPPoA, and Ethernet connections for a CloudGen Firewall model using the internal DSL modem. Four parallel xDSL connections are supported for the external DSL modem, one active connection for the internal DSL modem. The internal DSL modem also supports an Active/ Passive Mode in which the DSL line connected to WAN2 is used in case the DSL line on WAN1 becomes unavailable. Ports ppp1 - ppp4 are reserved for xDSL connections. The port names can be edited with the names of the configured DSL links.

For more information, see xDSL WAN Connections.

Wireless WAN Connections

Wireless WAN connections are ideal for backup lines or for use in mobile offices or locations with no terrestrial Internet links. To use all WWAN features of the CloudGen Firewall, it is recommended that you use the Barracuda Networks 3G Modem.

For information on how to configure the Barracuda USB modem, see the Barracuda USB Modem Quick Start Guide (PDF).

For information on how to configure WWAN connections, see How to Configure an ISP using a WWAN Modem.

Wi-Fi Client Connections

The CloudGen Firewall can connect as a Wi-Fi client to wireless networks. Wi-Fi client connections are supported for all CloudGen Firewall F-Series models with built-in Wi-Fi cards.

For more information, see How to Configure Wi-Fi Client Connection.

ISDN Connections

The CloudGen Firewall ISDN configuration provides flexible dial-in options, dynamic DNS support, channel bonding (mppp), and usage of a second S0 bus with a different phone number. ISDN connections can be used with static or dynamic IP addresses.

For more information, see How to Configure an ISP with ISDN.

Link Balancing and Failover

Configure link balancing and failover to optimize usage of two or more WAN connections. Use custom connection objects to select the optimal connection for the traffic handled by that access rule. You can define multiple connection objects, each with a different failover or link balancing policy. You can

also use route metrics for basic link failover functionality.

For information on link balancing for multiple WAN connections, see How to Configure Link Balancing and Failover for Multiple WAN Connections.

For information on link balancing for multiple DHCP or xDSL connections, see How to Configure Failover with Multiple xDSL or DHCP WAN Connections.

For information on failover with connections in Standby Mode, see How to Configure Automatic Failover Dynamic WAN Connections in Standby Mode .

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.