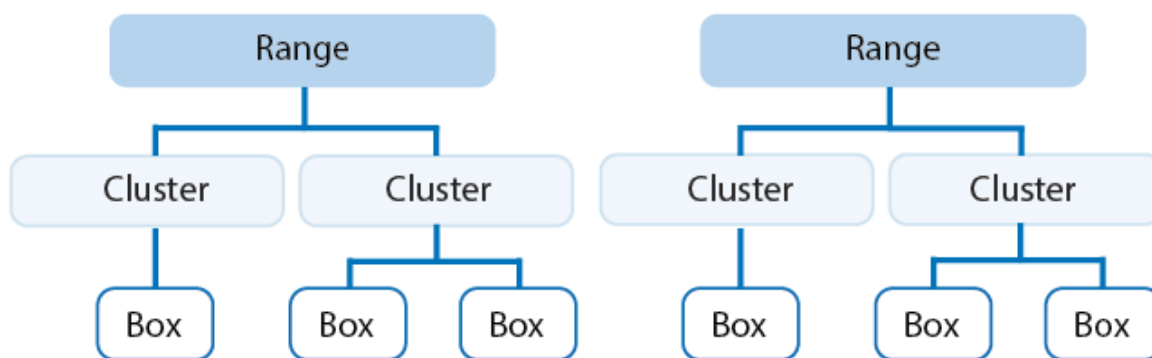


Central Management

<https://campus.barracuda.com/doc/73719457/>

The Barracuda Firewall Control Center is designed for the central management of CloudGen Firewalls. Control Center administers, configures security, content, traffic management, and network access policies from one central management interface. Template-based security information and configuration versions make it possible to manage all locations from one central system.

System Hierarchy: Ranges, Clusters, and Boxes



The Control Center organizes the managed Firewalls into a hierarchy of ranges and clusters, with the individual firewalls at the lowest level. The number of available ranges and clusters depends on which edition Control Center you are using. For more information on the available Control Center editions, see [Firewall Control Center](#)

Ranges

Ranges simplify central administration of globally distributed firewalls. For each range, you can define global settings, spanning all clusters in the range. You must create at least one cluster in a range to be able to add CloudGen Firewall boxes. To make configuration easier, you can define the following range-wide configuration settings:

- Range Objects
- Range GTI Editor
- Range Statistics
- Range Access Control Objects
- Range QoS Shaping Trees
- Activation Template

For more information, see [How to Manage Ranges and Clusters](#)

Clusters

At the second highest level, clusters represent groups of firewalls. To make configuration easier, you can define the following cluster-wide configuration settings:

- Cluster Objects
- Cluster GTI Editor
- Cluster Statistics
- Cluster Access Control Objects
- Cluster QoS Shaping Trees
- Activation Template

For more information, see [How to Manage Ranges and Clusters](#).

Boxes

Boxes represent the individual CloudGen Firewalls within a Control Center cluster.

For more information, see:

- [How to Import an Existing CloudGen Firewall into a Control Center](#)
- [How to Add a New CloudGen Firewall to the Control Center](#)
- [How to Move, Copy, and Delete CloudGen Firewalls in the Control Center](#)

Unmanaged Firewall

It is possible to display CloudGen Firewalls not managed by the Control Center, or the box layer of the Control Center in the Status Map.

For more information, see [How to Display the Control Center Box Layer on the Status Map](#).

System Health and Status Monitoring

The Control Center continuously monitors the system status of all managed units and displays a summary on the Barracuda Barracuda Firewall Admin **Status Map**.

For more information, see [CC Status Map Page](#).

Configuration Updates

The configuration for all managed firewalls is stored on the Control Center. When the admin activates a configuration change, it is automatically pushed out to the managed firewalls.

For more information, see [CC Configuration Updates](#).

Remote Management Tunnels

Remote firewalls not able to directly reach the Control Center connect to the Control Center via a remote management tunnel. These secure remote management tunnels are used for all communication, such as configuration updates, statistics, and monitoring updates.

For more information, see [How to Configure a Remote Management Tunnel for a CloudGen Firewall](#).

VPN Offloading

To reduce traffic load for large deployments, Control Center-managed CloudGen Firewalls can be configured to handle remote management tunnels.

For more information, see [How to Configure Management Tunnel Offloading using an Access Controller](#).

Licensing on the Firewall Control Center

The Control Center automatically completes license activation for new firewalls. If pool licenses are used, the Control Center can assign and update license information for remote systems firewalls using these licenses.

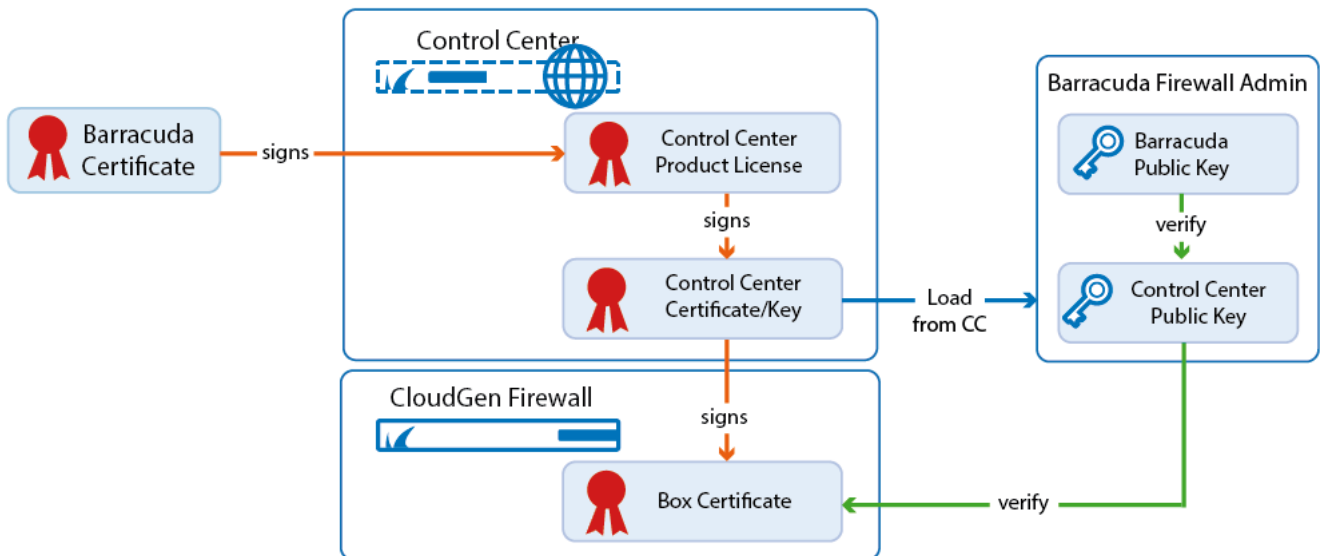
For more information, see [Licensing CloudGen Firewalls in the Control Center](#).

Firmware Updates on Managed Firewalls

The Control Center manages deployment of hotfixes and firmware updates for all managed units. Updates and changes are pushed to the managed units and can be triggered manually or automatically at a preset time.

For more information, see [How to Update Control Center-Managed CloudGen Firewalls](#).

Control Center Trust Center Model



Connections between the Control Center, CloudGen Firewalls, and Barracuda Barracuda Firewall Admin are authenticated with X509 private/public keys. The Control Center handles the certificate and authentication of remote firewalls and Barracuda Firewall Admin. The Control Center also stores a list of valid SSH keys for all managed units.

- **Control Center connects to a managed CloudGen Firewall** - During deployment, the public keys for the box certificate and the Control Center certificate are exchanged. These keys are used to authenticate all SSL connections between the Control Center and the managed units.
- **Connecting to the Control Center with Barracuda Firewall Admin** - Barracuda Firewall Admin can verify if the Control Center certificate is valid and if it is communicating with the intended Control Center by checking the certificate with the Control Center public key it has previously downloaded from the Control Center.
- **Connecting to a managed CloudGen Firewall with Barracuda Firewall Admin** - Barracuda Firewall Admin downloads the public key from the Control Center and then uses that key to verify the box certificate of the managed CloudGen Firewall.

For information on how to troubleshoot the certificate chain of trust, see the **Authentication Level** section in [Control Center Troubleshooting](#).

Figures

1. cc_hierarchy-01.png
2. CC_Certificates.png

© Barracuda Networks Inc., 2019 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.