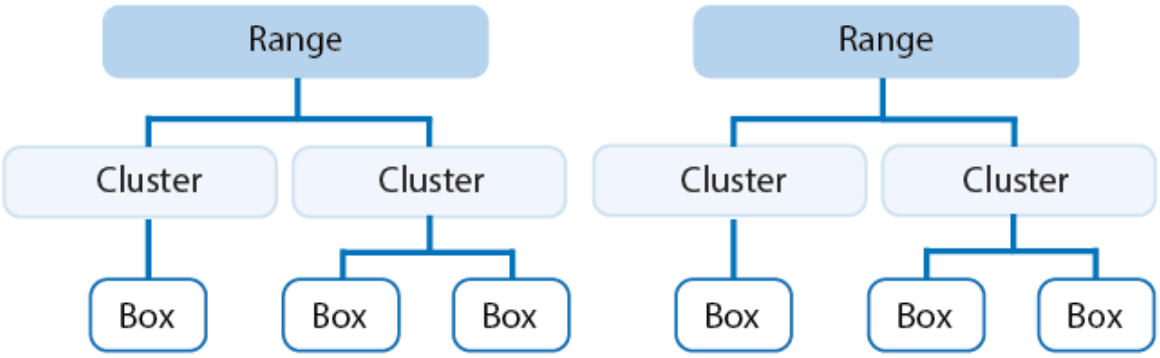
# Central Management

https://campus.barracuda.com/doc/53248446/

The Barracuda NextGen Control Center is designed for the central management of F-Series Firewalls. Control Center admins configure 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 box configurations at the lowest level. The number of available ranges and clusters depends on which edition Control Center you are using:

- **Standard Edition** – One range, one cluster, unlimited number of managed Firewalls.
- **Enterprise Edition** – One range, unlimited number of clusters, unlimited number of managed Firewalls.
- **Global Edition** – Five ranges with the option to add additional ranges, unlimited number of clusters, unlimited number of managed Firewalls.

#### 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 F-Series 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 F-Series Firewalls within a Control Center cluster.

For more information, see:

- How to Import an Existing F-Series Firewall into a Control Center
- How to Add a new F-Series Firewall to the Control Center
- How to Move, Copy, and Delete F-Series Firewalls in the Control Center

#### Unmanaged Firewall

It is possible to display NextGen 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 NextGen 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 an F-Series Firewall.

## VPN Offloading

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

For more information, see How to Configure Management Tunnel Offloading using an Access Concentrator.

## Licensing on the NextGen 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.

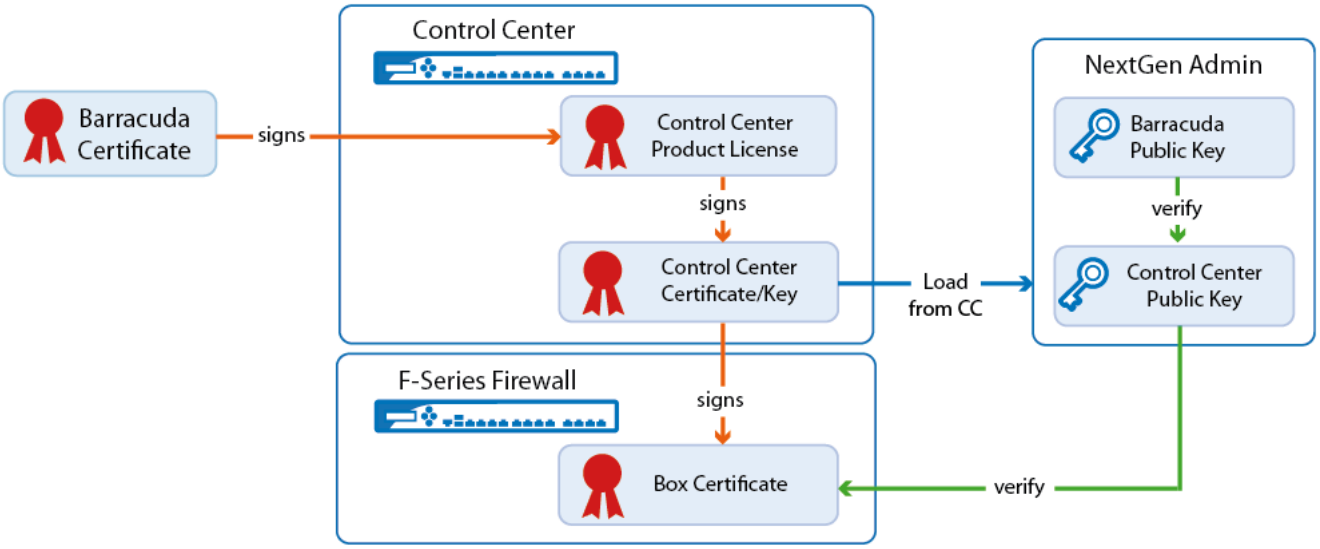
For more information, see Licensing F-Series Firewalls in the Control Center.

## 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 Standalone F-Series Firewalls.

## Control Center Trust Center Model




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

- **Control Center connects to a managed NextGen Firewall F-Series** – 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 NextGen Admin** – NextGen 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 NextGen Firewall F-Series with NextGen Admin** – NextGen Admin downloads the public key from the Control Center and then uses that key to verify the box certificate of the managed F-Series 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