How to Configure a Distributed Firewall

The distributed (or cascaded) firewall is a shared service deployed on a per-cluster basis on the Barracuda NextGen Control Center. The service can be assigned to all managed NextGen F-Series Firewalls in the cluster and allows them to use the same firewall ruleset with local modifications for each individual unit.

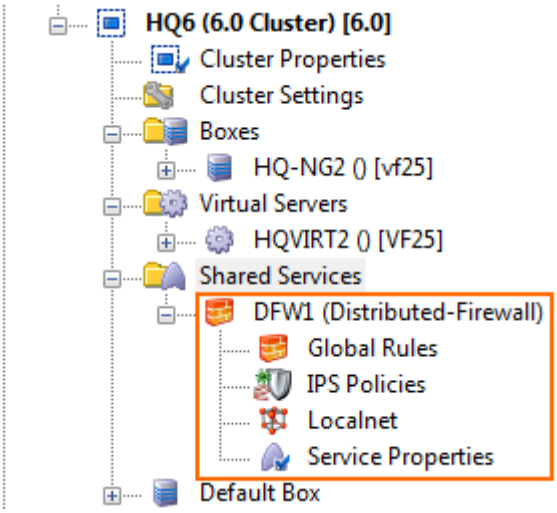
Before You Begin

If you want to use Application Control 2.0, the Control Center and the all the managed firewalls must have at least firmware version 5.4.4. For a list of requirements, see the section **Requirements for Application Control 2.0** in Distributed Firewall.

Step 1. Create the Distributed-Firewall Service

1. Right-click on the **Shared Services** page for your cluster (**Multi-Range > *your range* > *your cluster* > Shared Services**) and select **Create Shared Service**.
2. Enter a **Service Name**.
3. Select **Firewall** as the **Software Module**.
4. Click **Finish**.
5. Click **Activate**.

The distributed firewall service is visible in the **Shared Services** of your cluster.



Step 2. Add the Distributed-Firewall Service to a Virtual Server

You can add the shared service to every Barracuda NextGen Firewall F-Series in the same cluster.

Add to all Virtual Servers

1. Expand **Multi-Range > *your range* > *your cluster* > Virtual Servers**.
2. Right-click **Virtual Servers** and select **Add Shared Service**. The **Select Object** window opens.
3. Select the distributed firewall service from the list.
4. Click **OK**.
5. Click **Activate**.

The distributed firewall service is now added to all virtual servers in your cluster. Existing standalone firewall services on the virtual servers are automatically deactivated.

Add to one Virtual Server

1. Expand **Multi-Range** > ***your range*** > ***your cluster*** > **Virtual Servers** > ***your virtual server***.
2. Right-click ***your virtual server*** *and* select **Add Shared Service.** The **Select Object** window opens.
3. Select the distributed firewall service from the list.
4. Click **OK**.
5. Click **Activate**.

The distributed firewall service is now added to your virtual server. If a standalone firewall service already exists on the virtual server it is automatically deactivated.

Step 3. Add Global Access Rules

Create access rules to be used by all firewalls in the cluster. You can create access rules individually or link the global rules to a repository for simplified maintenance.

For more information, see Access Rules.

Step 4. Add networks to Localnet and Specialnet

The **Localnet** networks are cluster-wide, trusted local networks. These trusted networks are determined for use in the entire cluster service. You must use a cascade access rule in the global rules for the local rules to be evaluated. Use a cascade back access rule in the local rules to go back to the global rules if desired.

The **Specialnet** networks are server service-wide networks. Specialnet objects are configured below the **Distributed-Firewall Specific** node, with server service-wide validity.

The values entered into the **Trusted Local Networks** and **specialnet** network objects configuration window are not visible in the configuration dialog of the network object **localnet** or **specialnet.**

Step 5. Create Local and Special Access Rules

Use the **Locals Rules** section to define rules that can generally be applied to servers within a cluster, and should be maintained centrally. Use the **Special Rules** section to define rules that should only apply to specific server services or network segments. You must use cascade rules in the global ruleset for the local and special ruleset to the evaluated.

Local Rules

Local rules are defined per server service. They can contain a complete ruleset with full functionality. The **Local Rules** section is evaluated, if the **Global Rules** cascades to the **Local Rules**. You must create a cascade back access rule to continue evaluating the global rules.

Special Rules

Special rules are defined per server service. The **Special Rules** section is only applicable if the **Global Rules** cascades to **Special Rules**. You must create a cascade back access rule to continue evaluating the global rules.

Figures