Distributed Firewall

https://campus.barracuda.com/doc/96026401/

The Distributed Firewall is a firewall service running simultaneously on multiple firewalls in a cluster. As a shared service, the Distributed Firewall replaces the stand-alone firewall service on the box. You cannot run a Distributed Firewall service and a stand-alone firewall service together on a CloudGen Firewall.

Ruleset Structure

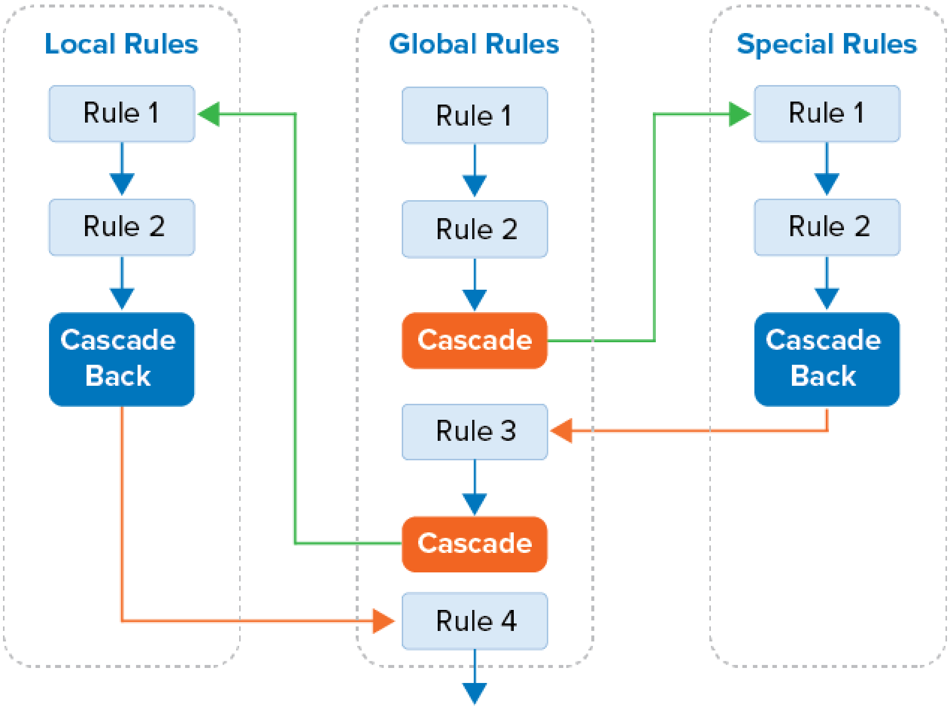
The Distributed Firewall, that includes all features of the regular firewall service, is created as a shared service in a cluster on the Barracuda Firewall Control Center. Unlike the stand-alone firewall service, the Distributed Firewall is organized into three rulesets:

- **Global Rules**
- **Local Rules**
- **Special Rules**

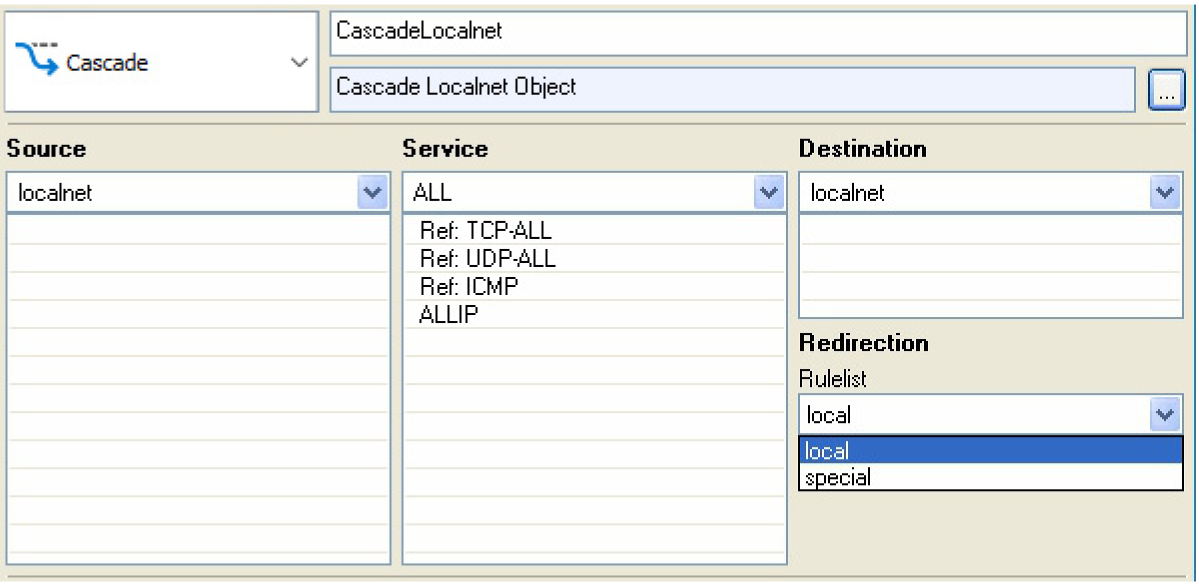
The Global Rules set is evaluated first and contains the global access rules that apply to all firewalls using the shared service.

Ruleset Processing

Incoming traffic is matched against the access rules defined in the global rules. All access rules that are the the same for all firewalls using the shared service are listed here. The local and special rules contain rules specific to the individual CloudGen Firewall. The local and special rulesets are evaluated only if the global ruleset contains a CASCADE access to the ruleset. Local and special rules are coequal, but both come after global rules. Local and special rules can work only with network objects that have been cascaded to them from the **Global Rules** section.



The workflow of rules in the **Global Rules** section is intercepted through cascading to either the **Special Rules** or **Local Rules** section. From there, as a final step, the workflow is returned to the **Global Rules** section with a **Cascade Back** rule.


Cascade

CascadeLocalnet

Cascade Localnet Object

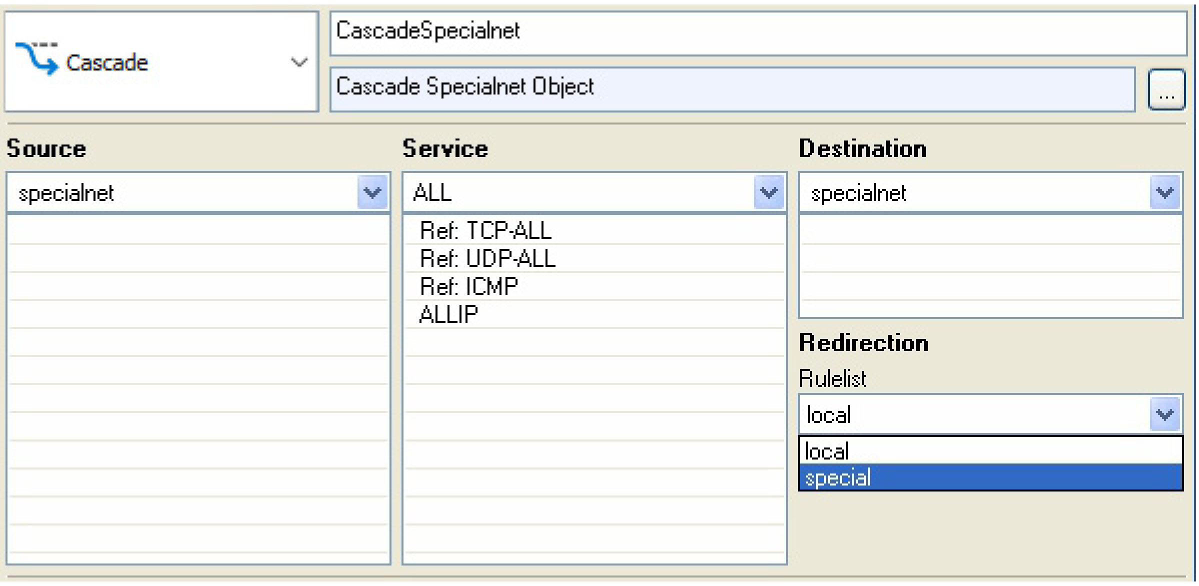
Source: localnet

Service: ALL
Ref: TCP-ALL
Ref: UDP-ALL
Ref: ICMP
ALLIP

Destination: localnet

Redirection

Rulelist: local
local
special



Cascade

CascadeSpecialnet

Cascade Specialnet Object

Source	Service	Destination
specialnet	ALL	specialnet
	Ref: TCP-ALL Ref: UDP-ALL Ref: ICMP ALLIP	

Redirection

Rulelist: local

Global Rules

In the **Global Rules** section, rules are managed that are valid for all distributed firewall services bound to a specific cluster service. To simplify maintenance, the global rules node can be linked into a repository. A consistent ruleset architecture can therefore be set up and administered.

Localnet Node

The **Localnet** configuration area serves to specify trusted local networks. These trusted networks are determined for use across the cluster service. Every value entered in the **Trusted Local Networks** dialog results in an entry in the network object *localnet* in the **Global Rules** section. There is only one localnet object. If you need more granular control, use global firewall objects.

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

To enable configuration of specific rules related to trusted networks, the localnet network object must be cascaded to the **Local Rules** section. Ensure to cascade the object back (**Cascade Back**) if you want to return to the workflow of the global ruleset.

Local Rules Section

Use the **Locals Rules** section to define rules that can generally be applied to firewalls within a cluster and that should be maintained centrally. Local rules are defined per service. They can also contain a complete ruleset with full functionality. The **Local Rules** section is applicable only if the **Global Rules** section allows it, which means it has cascaded the **localnet** object to the **Local Rules** section. Ensure to cascade the object back (**Cascade Back**) if you want to return to the workflow of the global ruleset.

Special Rules Section

Use the **Special Rules** section to define rules that should only apply to specific services or network segments. Special rules are also defined per service. The **Special Rules** section is applicable only if the **Global Rules** section allows it, which means it has cascaded the **specialnet** object to the **Special Rules** section. Ensure to cascade the object back (**Cascade Back**) if you want to return to the workflow of the global ruleset.

Specialnet Node

The **Specialnet** configuration area is for special networks. Specialnet objects are configured in the Distributed Firewall Specific node, with *service-wide* validity. Every value in the **Special Networks** dialog is an entry in the network object **Specialnet** in the **Global Rules** section. A specialnet is usually a selective range of IP addresses needed to configure a subset of rules. However, it should not be in the Localnet network object. The values entered into the **Special Networks** configuration window are not visible in the configuration dialog of the network object **Specialnet**.

> The **Local Rules** and **Special Rules** sections are generally suited for administration by distinct administrators. When delegating ruleset administration, make sure to set the appropriate user rights on the **Global Rules**, **Special Rules,** and **Local Rules** nodes, as well as on the **Localnet** and **Specialnet** nodes.

Administrator Permission for Distributed Firewalls

Administration rights for distinct distributed firewall administrators can be set through permissions on the firewall-related nodes in the configuration tree. Disallowed configuration areas will be set to readonly.

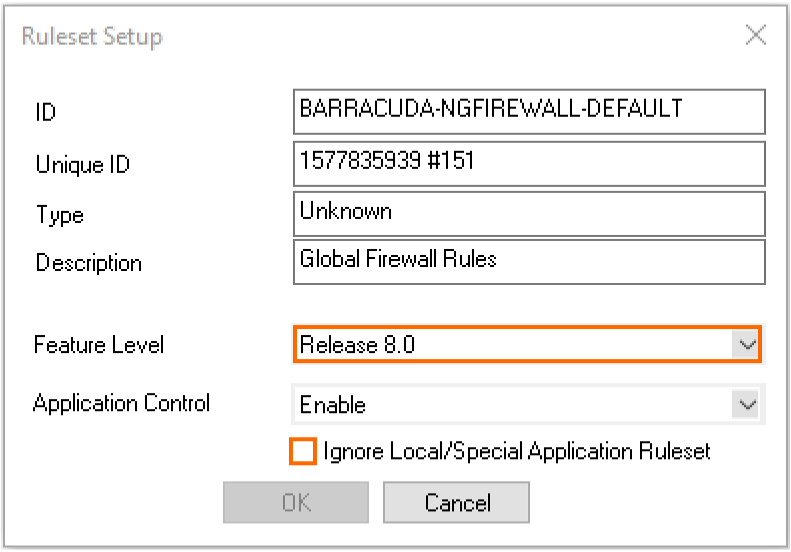
For more information, see Control Center Admins.

Application Control Rulesets in the Distributed Firewall

Application Control can be used in the global and local/special rulesets for the Distributed Firewall. Application rules can be created in the global/local and specialnet rulesets. You can determine which application rules are used for each ruleset:

- **Use both global and local/special application rules (default)** – By default, the application rules defined in the ruleset for the matching access rule are used. For example, a matching access rule in the Local Rules will evaluate the application rules defined in **Local Rules**. If no application rules are defined, the application rules from the Global Rules are used instead.
- **Only use global application rules** – If you want to use the application rules defined in the global ruleset exclusively, enable **Ignore Local/Special Application Ruleset** in the **Ruleset Setup** (**Forwarding Firewall > Setup**). Application rules in the **Local/Special Rules** are ignored.

When using the default **Kernel Space - Tree Lookup** in the **Advanced** firewall rule settings, the **Rule Mismatch Policy** for **Continue** or **Block on Mismatch** of application rules for the localnet and specialnet ruleset are ignored. Instead, the policies of the Global ruleset are applied.



Ruleset Setup

ID	BARRACUDA-NGFIREWALL-DEFAULT
Unique ID	1577835939 #151
Type	Unknown
Description	Global Firewall Rules
Feature Level	Release 8.0
Application Control	Enable

□ Ignore Local/Special Application Ruleset

Requirements for Application Control

- Set the feature level according to the list in How to Enable Application Control.
- SSL Inspection and URL Filter do not work on managed CloudGen Firewalls F10 and F100/101.

Figures