Distributed Firewall

https://campus.barracuda.com/doc/48203140/

The distributed firewall (formerly Cascaded Firewall or cfirewall) is a firewall service distributed across multiple NextGen F-Series Firewalls. It is a variant of the regular firewall service, designed to simplify firewall administration by multiple administrators. The distributed firewall is a shared-service and replaces the standalone firewall service. You cannot run a distributed firewall service and a standalone firewall service together on a virtual server.

Rule Set Structure

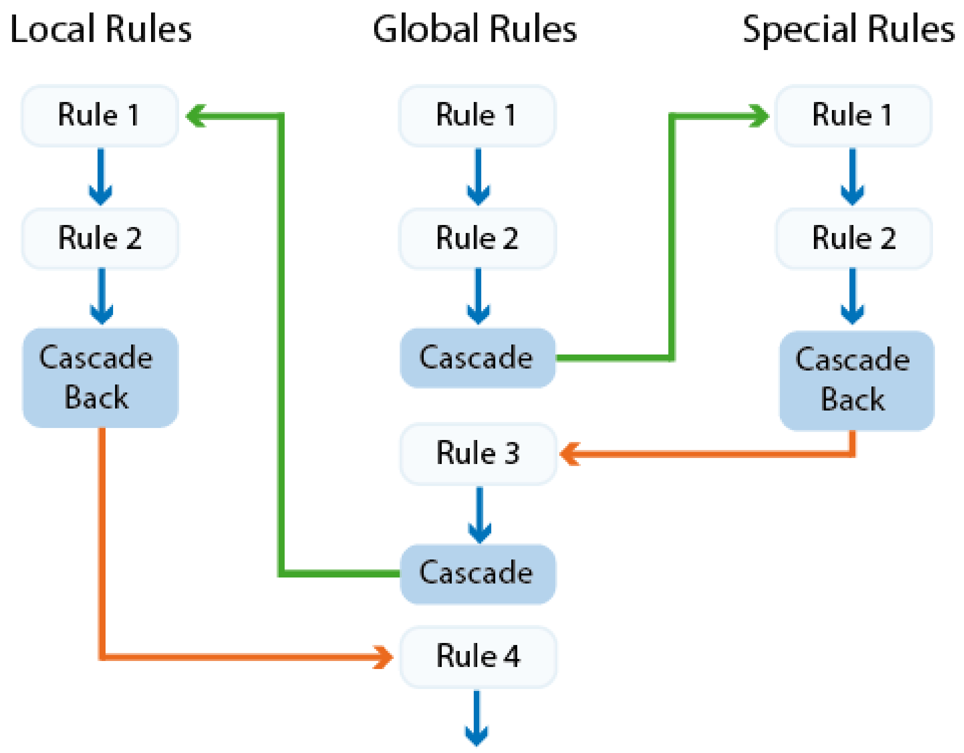
The distributed firewall includes all features of the regular firewall service and is created as a shared service in a cluster on the Barracuda NextGen Control Center. Unlike the standalone firewall service the distributed firewall is organized into three rule sets:

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

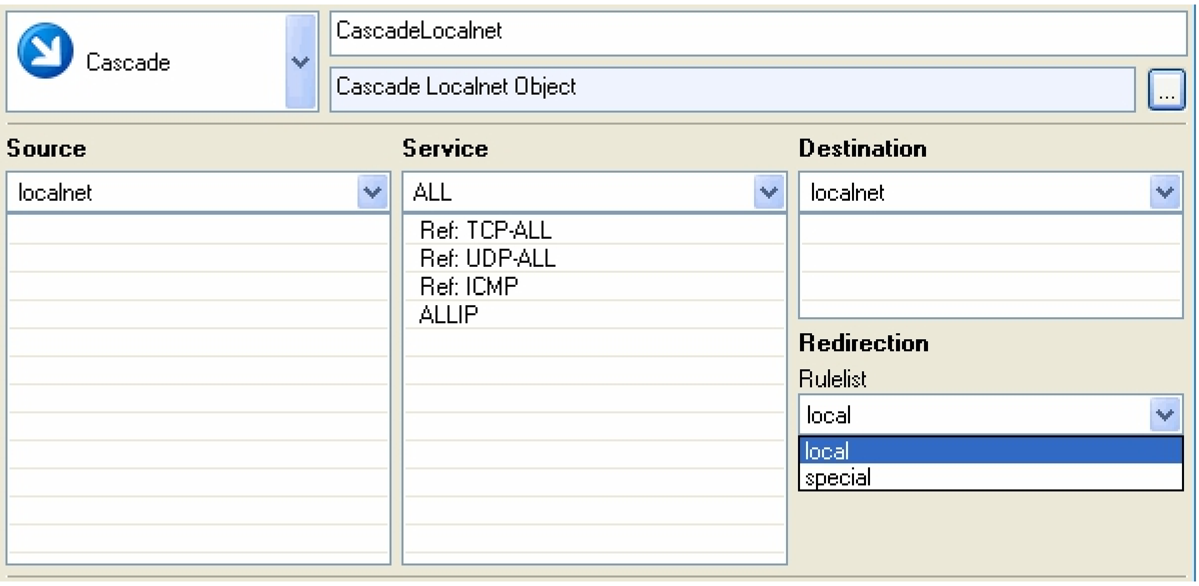
The Global Rules set is evaluated first and contains the global access rules that apply to all firewalls using the shared service.

Rule Set Processing

Incoming traffic is matched against the access rules defined in the global rules. All access rules which are the the same for all firewalls using the shared service are listed here. The local and special rules contain rules which are specific to the individual NextGen Firewall F-Series. The local and special ruleset are only evaluated if the global ruleset contains a CASCADE access to the rule set. Local and special rules are coequal but both come after global rules. Local and special rules can only work 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 **Special-** or **Local Rules** section. As a final step, from there 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

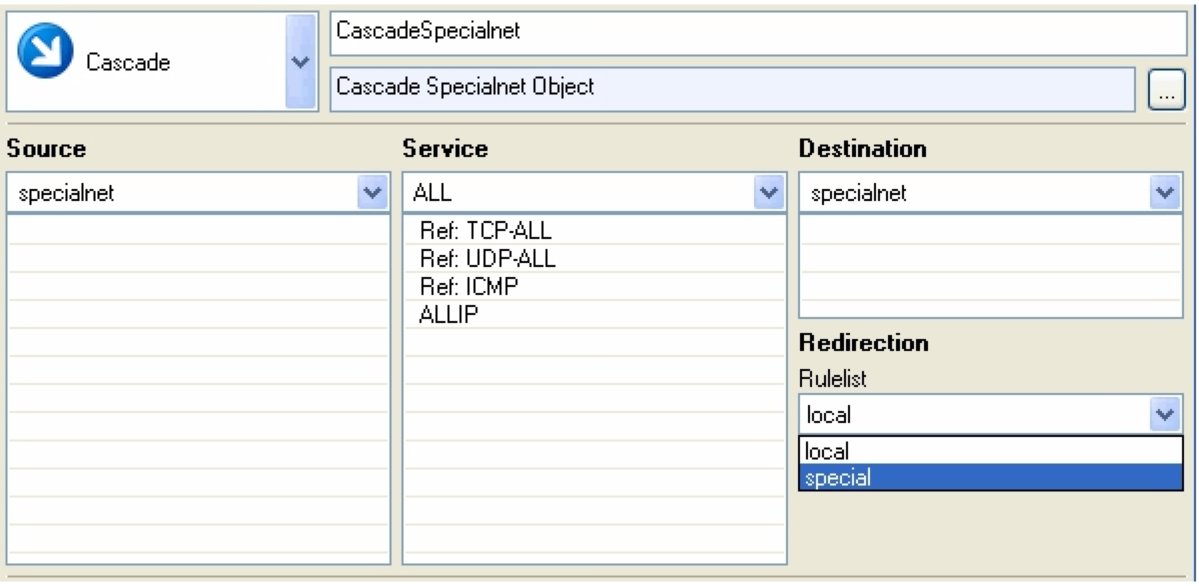
Destination

localnet

Redirection

Rulelist

local



Cascade

CascadeSpecialnet

Cascade Specialnet Object

Source

specialnet

Service

ALL

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

Destination

specialnet

Redirection

Rulelist

local

Global Rules

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

Localnet Node

The **Localnet** configuration area serves for specification of trusted local networks. These trusted networks are determined for *cluster-service-wide* use. 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. Use global firewall objects if you need more granular control.

> 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 has to be cascaded to the **Local Rules** section. Do not forget to cascade the object back (**Cascade Back**), if return to the workflow of the global ruleset is desired.

The Local Rules Section

Use the **Locals Rules** section to define rules which can generally be applied to servers within a cluster, and should be maintained centrally. Local rules are defined per server-service. They can again contain a complete ruleset with full functionality. The **Local Rules** section is only applicable, if the **Global Rules** section allows it, that means it has cascaded the **localnet** object to the **Local Rules** section. Do not forget to cascade the object back (**Cascade Back**), if return to the workflow of the global ruleset is desired.

The Special Rules Section

Use the **Special Rules** section to define rules which should only apply to specific server services or network segments. Special rules as well are defined per server-service. The **Special Rules** section is only applicable if the **Global Rules** section allows it, that means it has cascaded the **specialnet** object to the **Special Rules** section. Do not forget to cascade the object back (**Cascade Back**), if return to the workflow of the global ruleset is desired.

Specialnet Node

The **Specialnet** configuration area serves for special networks. Specialnet objects are configured in the **distributed firewall Specific** node, with *server-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 usually is a selective range of IP addresses, needed to configure a subset of rules and at the same time 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**.

Local- 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-**, **Special-** and **Local Rules** nodes, and 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 respectively.

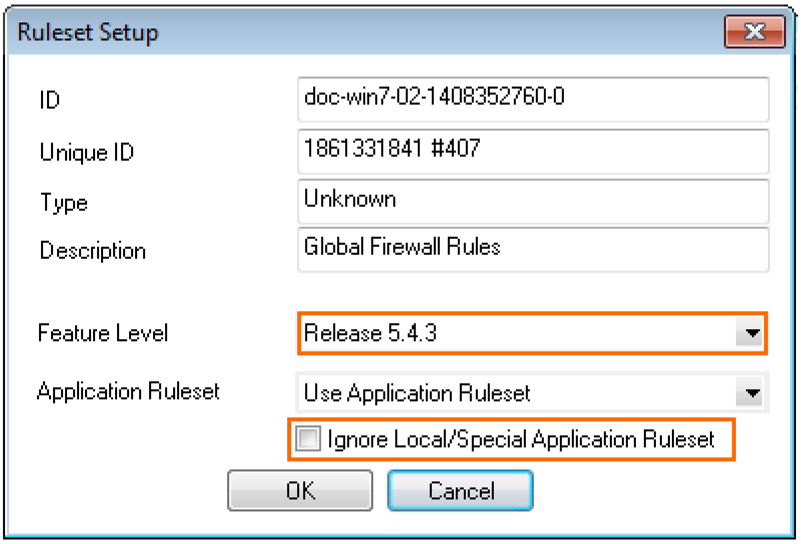
For more information, see Control Center Admins.

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)** – Per 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 in 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 rule set are applied.



ID: doc-win7-02-1408352760-0
Unique ID: 1861331841 #407
Type: Unknown
Description: Global Firewall Rules
Feature Level: Release 5.4.3
Application Ruleset: Use Application Ruleset
☐ Ignore Local/Special Application Ruleset

Requirements for Application Control

- Set the Feature level according to the list in How to Enable Application Control.
- SSL Interception and URL Filter will not work on managed F-Series Firewalls F10 and F100/101.
- Control Center and all managed firewalls using the distributed firewall must run firmware 6.1.0

or higher. If you are upgrading a distributed firewall service (firmware version 5.4.3 or lower), you must run the **treemigration** script on the command line interface of your Control Center to migrate to Application Control.

Application Control Migration for the Distributed Firewall Service

---

Migrate a cluster:

```
treemigration -c -m <range>/<cluster>
```

Migrate a range:

```
treemigration -c -m <range>
```

Figures

1. casc_ruleset.png
2. casc1.jpg
3. casc2.jpg
4. Distributed_Firewall_APP01.png