

# Feature Brief



## Multiple IP Rule Sets

### Clavister SSP™ Security Services Platform

firewall • VPN termination • intrusion prevention • anti-virus  
anti-spam • content filtering • traffic shaping • authentication

# CLAVISTER®

Protecting Values

## Introduction

Clavister Security Services Platform (SSP™) is our proven, feature-rich, service-oriented framework for providing best-in-class security solutions. Clavister SSP™ consists of **Clavister Network Security Elements**, **Clavister Lifecycle Systems**, and **Clavister Lifecycle Services**. Clavister SSP™ combines precise control, fine-granular administration, and seamless scalability making it easy to provision the perfect solution for any customer; be it a small organization, a large Internet Service Provider, a Managed Security Service Provider, or a multimedia-ready telecommunication operator.

### Clavister Network Security Elements

These are the physical building blocks that you install in your network. Clavister SSP™ currently offers two network security elements; Clavister Security Gateway Series and Clavister Secure Access Gateway. The Clavister Security Gateway is available both as a pre-packaged turnkey appliance solution for fast and easy deployment or as a distributed software-only solution for your preferred hardware platform. The Clavister Secure Access Gateway Series is available as a pre-package turnkey appliance solution only and offers SSL VPN, Single Sign-On (SSO) and multi-factor authentication (MFA).

### Clavister Lifecycle Systems

The Clavister Lifecycle Systems is a set of software components enabling true network security management throughout the entire lifecycle, including deployment, monitoring and reporting, configuration and integration, as well as analysis, optimization and troubleshooting. Clavister FineTune™ and the Web-based administration user interface enable you to manage a large set of Clavister Network Security Elements. Clavister InSight™ is our premium Security Event and Information Management (SEIM) system, which does not only support Clavister security network elements, but also a majority of other network devices. By correlating data from all network elements, you get a complete log of all activities in your network. Clavister PinPoint™ completes the Clavister Lifecycle Systems suite with accurate and precise real-time information packaged in a convenient dashboard-style application.

### Clavister Lifecycle Services

The Clavister Lifecycle Services empowers you and your products with tools, services, and resources that help maximize benefits and eliminate problems, including planning, deployment, optimization, operations and maintenance. The Clavister Lifecycle Services include the Clavister Service Provisioning Network (CSPN) for automated signature updates, the Clavister xPansion Lines™ license upgrade framework and Clavister's award-winning Technical Support.

The Clavister SSP™ service-oriented framework provides you with a secure environment for your business; either as a service provided to you by a Managed Security Service Provider (MSSP) or as systems and services integrated in your own network.

For more information about Clavister products and services, please visit us at: [www.clavister.com](http://www.clavister.com).

## Overview

Constructing complex IP rule sets can sometimes be daunting, involving many rules and actions. To make it more readable you can insert comment rows in between rules. You use these comment rows to describe what the intent of a section is and how it should be used. Still, large rule sets can get very big and unmanageable.

However, there is an easier way of dealing with large rule sets. Clavister Security Gateway enables the administrator to define multiple IP rule sets. These rule sets can both simplify maintenance and provide greater flexibility when defining security policies.

There are many advantages by breaking up your IP rule sets:

- You can break a single large IP rule set into multiple, smaller, more manageable IP rule sets.
- It enables you to reuse common types of rules across many IP rule sets.
- A single named IP rule set can be associated with a routing table. This makes implementing virtual routing much simpler, since each router can have a dedicated IP rule set associated with it. For more information regarding Virtual Routers, please see **Feature Brief: Virtual Routers**.

The default IP rule set is always present and is named `main`. You can not change its name or delete it. Additional rule sets can be defined by the administrator and they must have a unique name.

The remainder of this text will explain the multiple IP rule sets and IP rules in general. For more information, please read the Clavister CorePlus™ Administration Guide.

## IP Rules Tables, IP Rules and Actions

Before we go into more detail on multiple IP tables, it is important to explain the relationship between IP rule sets, IP rules and actions. One Clavister Security Gateway contains at least one IP rule set, aptly named `main`. This IP rule set serves as the first point of entry for any IP packet. You can also create new IP rule sets.

IP rule sets are made up of zero or more IP rules. These rules consist of a number of filtering parameters and one action. Two actions are associated with multiple IP rule sets; the **Goto** action and the **Return** action. Using these two actions it is possible to branch out from an IP rule set to another and back to the previous IP rule set.

### Other Clavister Security Gateway Rule Sets

There are more rules besides the IP rule set available in the Clavister Security Gateway. These rules use the same filtering parameters as IP rules. The available rules are:

- IP rules
- Pipe rules
- Policy-Based Routing rules
- Intrusion and Detection Prevention (IDP) rules
- Authentication rules

---

**NOTE: Authentication rules have only source network and source interface parameters.**

---

## IP Rules

IP rules are fundamental building blocks in a Clavister Security Gateway network setup. Network administrators and security officers design these security policies based on how they want traffic to flow through their Clavister Security Gateways. These IP rules share a common set of filtering parameter which determine the type of traffic to which they will apply. Table 1 below outlines the filtering parameter.

FILTERING PARAMETER	DESCRIPTION
Source Interface	An Interface or Interface Group where the packet is received at the Clavister Security Gateway. This can also be a VPN tunnel.
Source Network	The network that contains the source IP address of the packet. This might be a Clavister CorePlus™ IP object which could define a single IP address or range of addresses.
Destination Interface	An Interface or an Interface Group from which the packet would leave the Clavister Security Gateway. This can also be a VPN tunnel.
Destination Network	The network to which the destination IP address of the packet belongs. This might be a Clavister CorePlus™ IP object which could define a single IP address or range of addresses.
Service	The protocol type to which the packet belongs. Service objects define a protocol/port type. Examples might be SIP, HTTP or ICMP. It is also possible to define custom services.

**Table 1: IP Rules Filtering Parameters**

## Specifying Any Interface or Network

When specifying the filtering parameter in any of the rules using the IP rule filtering parameters specified above there are three useful pre-defined filtering options that can be used. Table 2 below describes these filtering options.

FILTERING OPTIONS	DESCRIPTION
all-nets	For a Source or Destination Network, this filtering option is equivalent to IP address 0.0.0.0/0, which means that any IP address is acceptable.
any	For Source or Destination Interface, specifying this filtering option means that Clavister CorePlus™ will not care about which interface the traffic is going to or coming from.
core	The Destination Interface can also be specified as core. This means that traffic, such as an ICMP Ping is destined for the Clavister Security Gateway itself and it is Clavister CorePlus™ that will respond to it.

Table 2: Pre-Defined Filtering Options

## IP Rule Actions

A rule consists of two parts: the filtering parameters and the action to take if there is a match with those filtering parameters. As described above, the filtering parameters of any rule, including IP rules are:

- Source Interface
- Source Network
- Destination Interface
- Destination Network
- Service

The Service filter parameter is important in an IP rule because if an Application Layer Gateway (ALG) object is to be applied to traffic then it must be associated with a Service object.

When an IP rule is triggered by a filter parameter match then an associated action is executed. The available actions are shown in Table 3 below.

ACTION	DESCRIPTION
Drop	This action instructs the Clavister Security Gateway to immediately discard the packet. No reply is sent back to the sender. This is often preferable since it gives a potential attacker no clues about what happened to their packets.
Reject	This action acts like the Drop action, but will return a TCP RST or ICMP Unreachable message, informing the sending computer that the packet was disallowed.
FwdFast	This action let the packet pass through the Clavister Security Gateway without setting up a state for it in the state table. This means that the stateful inspection process is bypassed and is therefore less secure than the Allow action or NAT action. Packet processing time is also slower than the Allow action since every packet is checked against the entire rule set.
Allow	This action allows packets to pass. As the rule is applied to only the opening of a connection, an entry in the state table is made to record that a connection is open. The remaining packets related to this connection will pass through the Clavister Security Gateway's stateful engine.
NAT	This action functions like the Allow action, except with dynamic address translation (NAT) enabled.
SAT	This action performs a static address translation. A SAT action always requires a matching Allow, NAT or FwdFast action further down the rule set.

ACTION	DESCRIPTION
SLB_SAT	This action instructs the Clavister Security Gateway to handle Server Load-Balancing (SLB) using Static Address Translation (SAT).
Multiplex_SAT	This action instructs the Clavister Security Gateway to handle multicast forwarding using Static Address Translation (SAT).
Goto	Jump to specified rule set.
Return	Return to the previous rule set.

Table 3: IP Rule Actions

## Bidirectional Connections

A common mistake when setting up IP rules is to define two rules, one rule for traffic in one direction and another rule for traffic coming back in the other direction. In fact nearly all IP rule types allow bidirectional traffic flow once the initial connection is set up. The Source Network and Source Interface filter parameters specified in the rule means the source of the initial connection request. Once a connection is permitted and established, traffic can then flow in either direction.

The exception to this bidirectional flow is the **FwdFast** action. If the **FwdFast** action is used then the rule will not allow traffic to flow from the destination back to the source. If bidirectional flow is required, then two rules with **FwdFast** action is needed, one for either direction. This is also the case when **FwdFast** actions are used with **SAT** actions.

## Using Reject

In certain situations the **Reject** action is recommended instead of the **Drop** action because a polite reply is required from Clavister CorePlus™. An example could be when responding to the IDENT user identification protocol.

## Multiple IP Rule Sets

### Processing Multiple Rule Sets

When multiple IP rule sets are defined, the way they are processed for a new connection is as follows:

- The main IP rule set, defined as `main`, is always searched first for matches of source/destination and interface/network filter parameters.
- If an IP rule contains a **Goto** action with a specified IP rule set name and if the traffic matches the **Goto** rule; then the IP rule look-up continues from the start of that named IP rule set.
- If the search in the named IP rule set does not find a match, the connection is dropped.
- If a match is found in the named IP rule set, the action is executed. The IP rule set could contain another **Goto** action in which case the IP rule scanning jumps to the start of this named IP rule set.
- If the action is **Return** and the IP rule scanning return to the previous IP rule set, it resumes at that IP rule which follows the last **Goto** action. If there was no last **Goto** then the connection is dropped and IP rule scanning stops.

---

**NOTE: A Goto action may never use the `main` IP rule set as its target.**

---



---

**NOTE: It is possible to have multiple Goto and Return actions in an IP rule set with different filtering parameters.**

---

To illustrate the concept of multiple IP rule sets we have defined three IP rule sets; `main`, `B` and `C`. In IP rule set `main` there is a **Goto** action to IP rule set `B`, which in turn has a **Goto** action to IP rule set `C`. Once IP rule set `C` reaches the **Return** action it will

return to IP rule set B to continue. In IP rule set B there is also a **Return** action that will return the traffic flow back to IP rule set main. This traffic flow is illustrated in Figure 1 below.

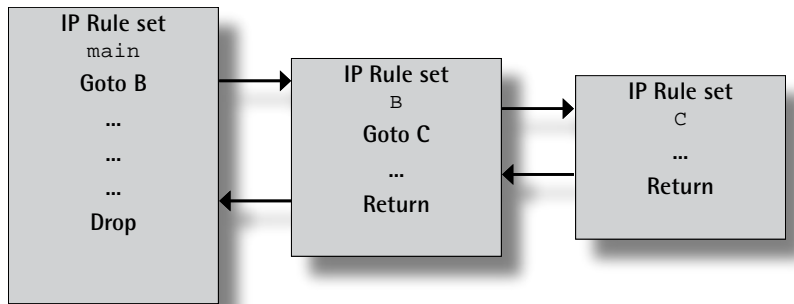


Figure 1: Multiple IP Rule Sets

### Loop Avoidance

It is conceivable that a sequence of **Goto** actions results in an infinite looping scanning sequence. Clavister CorePlus™ detects such logical errors when a configuration is initially uploaded. The erroneous configuration is rejected, along with an explanatory error message. The loop avoidance mechanism has to be efficient to enable fast configuration upload and for this reason it uses an algorithm that might sometimes find a fault in correct but complex logic. In this case it may be necessary to simplify the rule logic so the configuration can be uploaded.

### A Usage Example

Below are two simple IP rule sets which illustrate how multiple IP rule sets might be used. The main IP rule set contains a first rule which has a **Goto** action referencing another rule set named otherRule.

The administrator has defined this IP rule set which contains a rule with a **NAT** action and a rule with a **SAT** action. If neither is triggered then the final rule has a **Return** action. This action will cause the scanning process to go back to the IP rule set that invoked the IP rule set otherRule, in this case the main IP rule set and continue with the rule following the rule with the **Goto** action, in this example the rule with the **Allow** action.

#	ACTION	SOURCE INTERFACE	SOURCE NETWORK	DESTINATION INTERFACE	DESTINATION NETWORK	SERVICE
1	Goto otherRule	any	all-nets	core	172.16.40.0/24	all
2	Allow	any	192.168.0.0/24	core	172.16.0.0/16	all

Table 4: The main IP Rule Set

#	ACTION	SOURCE INTERFACE	SOURCE NETWORK	DESTINATION INTERFACE	DESTINATION NETWORK	SERVICE
1	SAT	any	all-nets	any	172.16.40.66	all
2	NAT	if2	176.16.0.0/16	any	all-nets	all
3	Return	if2	all-nets	any	all-nets	all

Table 5: The otherRule IP Rule Set

### Common Usage

Although there are no two network that look the same, there are some common themes that can be applied when managing your IP rules. Here is a set of guidelines that can be applied.

1. Multiple IP rule sets can with favour be used in order to devide the policies into separate rule set tables per interface. Thus meaning that for example, the DMZ can have its own table with policies while the the internal LAN can have its policies. This can be extended to cover all relevant interfaces.
2. Multiple IP rule sets can also be used by Managed Security Service Providers (MSSP) to more easily manage several customers from within one Clavister Security Gateway. The common setup in this scenario is that each customer is assigned one or several VLANs. Each customer is then assigned its own policy table. The benefit of this solution is that the administrator can work with a specific customers policies without risking to create a conflict with the policies for other users. Basically, it makes the administration less complex and more secure as it eliminates a lot of the common mistakes that might be done if one single big policy set is being used.

There are of course a number of other scenarios where multiple IP rule sets could be used to break down long IP rule sets and make them more managable.

## Conclusion

This Feature Brief describes multiple rule sets and how to use it with your Clavister SSP™ installation. Below are some key customer benefits:

### Clavister SSP™ Key Benefits

- **Robust Security**  
The purpose-built security offering from Clavister provides a complete set of security features, including Stateful Packet Inspection (SPI) firewall with DoS and DDoS protection, VPN with strong encryption, and User Authentication.
- **Rapid Deployment**  
The Clavister Security Gateway provides effortless and rapid deployment. A trained technician can easily deploy and configure new network security elements within minutes, even across continents.
- **Flexible Traffic Control**  
The highly sophisticated bandwidth management capabilities in the Clavister Security Gateway make it possible to not only guarantee bandwidth for business critical applications or server, but also to optimize the entire traffic flow in your network and avoid inefficient bandwidth usage.
- **Lowered Costs for Administration**  
The powerful administration system that comes with Clavister Security Gateway enables organizations to lower the costs for administration through centralized management. The administration system makes it possible to deploy and configure all devices across the network, no matter if they are located next door or across the globe.
- **High Performance**  
Scalable performance with unsurpassed maximum bandwidth, concurrent connections and simultaneous VPN tunnels makes the Clavister Security Gateway the ideal choice even in the most demanding environments like Internet Service Provider Networks, Data Centers, and telecom operators.
- **Low Total Cost of Ownership (TCO)**  
Clavister's goal is to provide complete security solutions more cost efficiently than any competitor. Clavister SSP™ with its unique combination of integrated features, world-class service and support, and powerful administration system provide the lowest TCO and the best price/performance ratio possible.

### Multiple IP Rule Set Key Benefits

- Break a single large IP rule set into multiple, smaller and more manageable IP rule sets.
- Reuse common types of rules across many IP rule sets.
- Associated a single named IP rule set with a routing table; making is easier to implement virtual routing.

## Feedback

Clavister Product Marketing is always interested in feedback from our readers. Please direct suggestions, comments or questions regarding this document to [product-marketing@clavister.com](mailto:product-marketing@clavister.com). Please include the title of the document in your email.

---

### About Clavister

Clavister - a Swedish privately owned company developing IT security products, including its award-winning Clavister Security Services Platform (SSP™). This service-oriented framework enables organizations to monitor network traffic, protecting critical business assets and blocking undesirable surfing. It will also protect you against intrusion, viruses, worms, Trojans, and overload attacks. It requires minimal servicing, with central administration, and has exceptionally flexible configuration possibilities. Its seamless scalability makes it easy to provision the perfect solution for any customer; be it small organizations, large Internet Service Providers, Managed Security Service Providers, or multimedia-ready telecom operators.

Clavister was founded 1997 in Sweden, with R&D and headquarters based in Örnköldsvik and Sales and Marketing based in Stockholm. Its solutions are marketed and sold through International sales offices, distributors, and resellers throughout EMEA and Asia. Clavister also offers its technology to OEM manufacturers.

For more information, please visit us at [www.clavister.com](http://www.clavister.com).

---

### Limitation of Responsibilities

The information in this document represents the current view of Clavister AB on the issues discussed as of the date of publication. Because Clavister must respond to changing conditions, it should not be considered to be a commitment for Clavister, and Clavister cannot guarantee the accuracy of any information presented after the date of publication. This document is for informational purposes only. CLAVISTER MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the written permission of Clavister. Clavister may have trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Clavister, the furnishing of this document does not give you any license to these trademarks, copyrights, or other intellectual property.

Part Number: [clavister-fbr-multiple\\_ip\\_rule\\_sets \(0801\)](#)