

Feature Brief



Virtual Routers

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.

Virtual Routers

Clavister Security Gateway supports the creation of multiple, logically separated systems with their own routing tables and rule sets, communicating between them just as physically separate systems would.

The basic building blocks are:

- Policy-Based Routing (PBR) - one routing table for each virtual system
- Per-interface PBR table membership - to make interface IP addresses reachable only in the desired routing table
- Pairs of loopback interfaces - for inter-system communication

Nearly everything that can be done with physically separate units can also be done with virtual systems, including running dynamic routing processes, such as OSPF on each system.

PBR in and of its own can solve many of the problems that virtual systems can. However, very large configurations tend to become unwieldy as the number of all-to-all mappings grow. Consider for instance the problem of one physical unit managing two separate organizations, both using the same IP span.

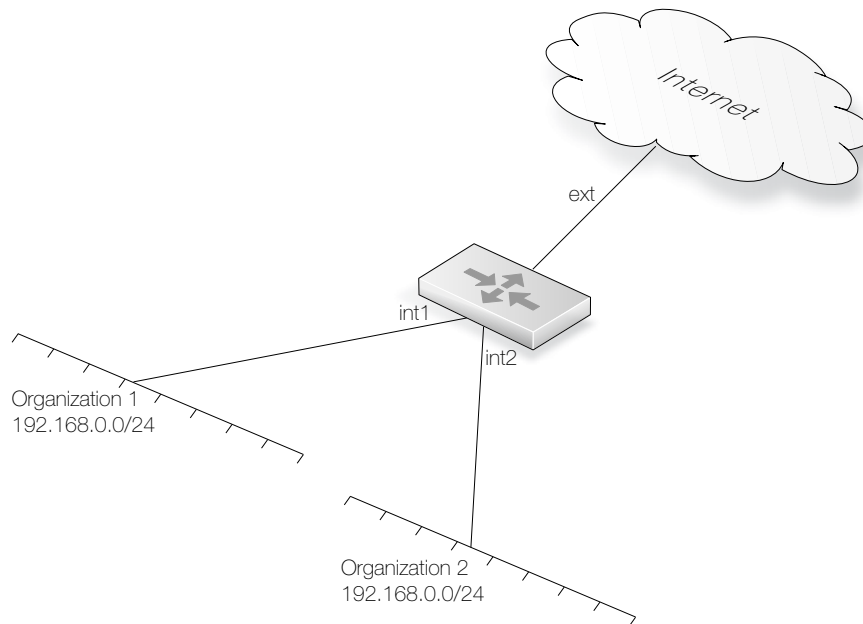


Figure 1: Routing using One Physical Router

This router would use two PBR routing tables, one for each organization:

PBRTABLE1			
ID	Interface	Network	Gateway
1	ext	0.0.0.0/0	gw-world
2	int1		

PBRTABLE2			
ID	Interface	Network	
1	ext	0.0.0.0/0	
2	int2		

Getting traffic from each network to and from the Internet is fairly straightforward here. Assuming only outbound traffic, it takes two PBR rules. Assuming that each organization has a public IP address which maps to servers on the respective networks, we handle outbound as well as inbound traffic with four rules:

```
Rule # 1:  
Name: org1-in  
Source Interface: ext  
Source Network: 0.0.0.0/0  
Destination Network: pubip-org1  
Forward PBR: pbrtable1  
Return PBR: pbrtable1
```

```
Rule # 2:  
Name: org1-out  
Source Interface: int1  
Source Network: 0.0.0.0/0  
Destination Network: 0.0.0.0/0  
Forward PBR: pbrtable1  
Return PBR: pbrtable1
```

```
Rule # 3:  
Name: org2-in  
Source Interface: ext  
Source Network: 0.0.0.0/0  
Destination Network: pubip-org2  
Forward PBR: pbrtable2  
Return PBR: pbrtable2
```

```
Rule # 4:  
Name: org2-out  
Source Interface: int2  
Source Network: 0.0.0.0/0  
Destination Network: 0.0.0.0/0  
Forward PBR: pbrtable2  
Return PBR: pbrtable2
```

This works as long as the organizations do not attempt to access each other's public resources. When that happens, we would need two more rules, before the other four.

```
Rule # 5:  
Name: org1-org2  
Source Interface: int1  
Source Network: 0.0.0.0/0  
Destination Network: pubip-org2  
Forward PBR: pbrtable2  
Return PBR: pbrtable1
```

```
Rule # 6:  
Name: org2-org1  
Source Interface: int2  
Source Network: 0.0.0.0/0  
Destination Network: pubip-org1  
Forward PBR: pbrtable1  
Return PBR: pbrtable2
```

So, with two organizations, two policies are enough. However, with three organizations, six rules are needed. And with four organizations, twelve policies are needed. With five, twenty. The list continues: 30, 42, 56, 72, 90... Things go steeply downhill from there.

The Benefits of Virtual Routing

One of the major benefits of Virtual Routing is eliminating the need for all-to-all mappings, such as demonstrated above. Also, in using interface PBR table membership rather than PBR rules, the configuration complexity is reduced overall. There is also the additional benefit of making the Clavister Security Gateway policies more clear by reducing the number of policy rules required in the same way that the number of PBR rules is reduced.

Taking the previous network layout as an example, we would construct three virtual routers:

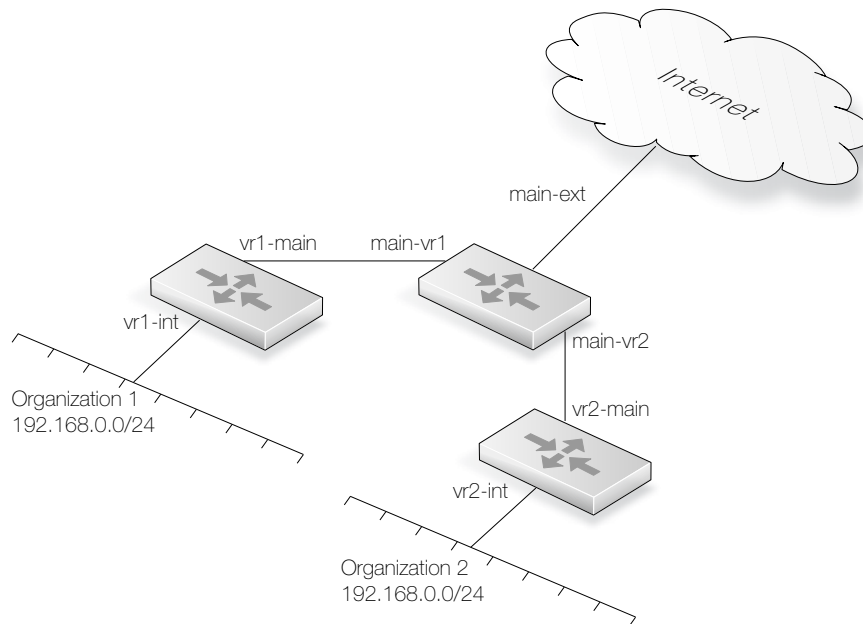


Figure 2: Routing using Virtual Routers

Each organization gets a virtual router of its own. Both connect to the "main" router, using pairs of loopback interfaces. First, we examine the routing tables:

MAIN			
ID	Interface	Network	Gateway
1	main-ext	0.0.0.0/0	gw-world
2	main-vr1	pubip-vr1	
3	main-vr2	pubip-vr2	

VR1			
ID	Interface	Network	Gateway
1	vr1-main	0.0.0.0/0	
2	vr1-int		

VR2			
ID	Interface	Network	Gateway
1	vr2-main	0.0.0.0/0	
2	vr2-int		

Using per-interface PBR membership, we can leave the PBR ruleset empty. The contents of the Ethernet and Loopback interface sections follow:

ETHERNET INTERFACES				
ID	Name	Driver	IP Address	PBR Table
1	main-ext	n/a	ip_main-ext	main
2	vr1-int	n/a	192.168.0.1	vr1
3	vr2-int	n/a	192.168.0.254	vr2

LOOPBACK INTERFACES				
ID	Interface	IP Address	Loop To	PBR Table
1	main-vr1	ip_main-ext	vr1-main	main

2	vr1-main	pubip-vr1	main-vr1	vr1
3	main-vr2	ip_main-ext	vr2-main	main
4	vr2-main	pubip-vr2	main-vr2	vr2

For each connection between a pair of virtual routers, two loopback interfaces are used; one in each virtual router. When a packet is sent through `main-vr1`, it arrives as a newly received packet on `vr1-main`. When a packet is sent through `vr1-main`, it is received on `main-vr1`. This is exactly the same as with two physically separate units: two interfaces, one in each, with a connection between them.

The PBR Table membership settings mean that if a connection arrives on an interface, it will be routed according to the PBR table that the interface is a member of.

Also make note of how the IP addresses of the internal interfaces of the virtual routers differ. If per-interface PBR table membership were not used, "core" routes for both IP addresses would be added in both routing tables, leading to `192.168.0.1` being unusable in `vr2` even though it shouldn't be, and `192.168.0.254` being unusable in `vr1`. However, with per-interface PBR table membership, interface IP addresses belonging to one virtual router will not interfere with other virtual routers.

The IP addresses of the `main-vr1` and `main-vr2` interfaces are the same as the IP address of the external interface. They could also have been set to something nonsensical, like `127.0.0.1`. Regular routing would still have worked just fine since loopback interfaces are raw IP interfaces -- the ARP protocol is not used over them. However, their IP addresses will be visible to users doing a traceroute from the inside, and also there is the issue of traffic originating from the firewall itself to the internal networks, such as pings or logging. Such traffic is most often routed according to the main routing table, and will be sourced from the IP address of the nearest interface in the main routing table.

Policies in Virtual Systems

Policies in different virtual systems are not split up into different sections, simply because there is no need for it. Rather, policies for different virtual systems all reside in the regular ruleset. There are also benefits to this approach, for instance the possibility to define "shared" or "global" rules that span over several or all virtual systems. For instance, if an aggressive worm strikes, it may be desirable to drop all communication on ports known to be used by the worm until countermeasures can be put into place. One single drop rule placed at the top of the ruleset can take care of this for all virtual systems in one physical unit.

Using the previous example as a basis, we show how policies might look in virtual systems:

INTERFACE GROUPS		
ID	Name	Interfaces
1	main-vrifs	main-vr1, main-vr2
2	main-ifs	main-ext, main-vrifs
3	vr1-ifs	vr1-main, vr1-int
4	vr2-ifs	vr2-main, vr2-int

RULES							
ID	Name	Action	Source Interface	Source Network	Dest Interface	Dest Network	Service
Rules for the "main" VR:							
1	main-allow-all	Allow	main-ifs	0.0.0.0/0	Any	0.0.0.0/0	All
Rules for "vr1":							
2	vr1-http-in	SAT	vr1-ifs	0.0.0.0/0	Any	pubip-vr1	http, SetDest 192.168.0.5
3	vr1-http-in	Allow	vr1-main	0.0.0.0/0	Any	pubip-vr1	http

RULES							
ID	Name	Action	Source Interface	Source Network	Dest Interface	Dest Network	Service
4	vr1-out	NAT	vr1-int	0.0.0.0/0	Any	0.0.0.0/0	All
Rules for "vr2":							
5	vr2-smtp-in	SAT	vr2-main	0.0.0.0/0	Any	pubip-vr2	smtp, SetDest 102.168.0.3
6	vr2-smtp-in	Allow	vr2-main	0.0.0.0/0	Any	pubip-vr2	smtp
7	vr2-http-out	NAT	vr2-int	192.168.0.4	vr2-main	0.0.0.0/0	http

The security policies for the respective organizations are clearly very different, and this is all handled easily with a virtual system setup.

Note how the SAT rules do not need to take into account that there are more organizations connected to the same physical unit. There is no direct connection between them; everything arrives through the same interface, connected to the "main" VR. If this was done without virtual routing, the Allow rules would have to be preceded by NAT rules for traffic from other organizations. Care would also have to be taken that such rules were in accordance with the security policy of each organization. All such problems are eliminated with virtual systems.

The source interface filters are very specific. "Any" is not used as source interface anywhere, since such a rule would trigger regardless of the VR processing context. Consider for instance what would happen if the "vr1-http-in" rules were to use "Any" as source interface. They would trigger as soon as packets destined to pubip-vr1 were received on "main-ext". The destination address would be rewritten to 192.168.0.5, and passed on, using the main routing table. The main routing table would not know what to do with 192.168.0.5 and pass it back out to the default gateway outside the firewall.

If you use the same naming scheme as shown in this example, you can quickly make sure that the source interfaces are correct. All the rules concerning the main VR have source interfaces beginning with "main-". All the ones concerning vr1 have source interfaces beginning with vr1-, and so on.

The destination interface filters, however, does not need to be as specific as the source interface filters. The possible destinations are limited by the routing tables used. If the vr1 table only includes routes through vr1- interfaces, "Any" filters can only mean "through other interfaces in the same virtual router". It may however be a sound practice to write tighter destination interface filters in case an error has snuck into the configuration elsewhere. In this example, rule 1 might use "main-ifs", rule 4 might use vr1-main. The SAT and corresponding Allow rules however are already fairly tight in that they only concern one single destination IP address.

Conclusion

This Feature Brief describes Virtual Routers and how to use them 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.

Virtual Router Key Benefits

- Supports the creation of multiple, logically separated systems
- Per-interface Policy-Based Routing (PBR) table membership

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. 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.

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-virtual_routers \(0801\)](#)