

Feature Brief



Managing NAT Pools

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.

Overview

In computer networking, the process of Network Address Translation (NAT) involves re-writing the source and/or destination address of IP packets as they pass through a router or firewall. Most systems using NAT do so in order to enable multiple hosts on a private network to access the Internet using a single public IP address. Many network administrators find NAT a convenient technique and use it widely. Nonetheless, NAT can introduce complications in communication between hosts and can have a performance impact.

In a typical configuration, a local network uses one of the designated "private" IP address subnets. According to RFC1918 Private Network Addresses are 192.168.x.x, 172.16.x.x through 172.31.x.x, and 10.x.x.x - using CIDR notation, 192.168/16, 172.16/12, and 10/8. A router on that network has a private address, such as 192.168.0.1 in that address space. As traffic passes from the local network to the Internet, the source address in each packet is translated on the fly from the private addresses to the public address or addresses.

It has been argued that the wide adoption of IPv6 would make NAT useless, as the latter is a method of handling the shortage of IPv4 address space. However, this argument either ignores the natural firewall provided by NAT, or assumes that consumer-grade

network routing devices, which are often installed by purchasers lacking knowledge of firewall configuration, would always be factory configured to block incoming server requests.

NAT Pools

NAT Pools makes it possible to translate source addresses of UDP, TCP and ICMP packets to more than one IP address. Usually you want to translate a large number of local host IP addresses to a smaller set of externally visible IP addresses. A NAT Pool can be used in one of three modes; Fixed, Stateless and Stateful. This Feature Brief will describe the implementation and operability of the NAT Pool subsystem, and how to best use them in your network setup.

NAT Pools are usually employed when there is a requirement for huge numbers of unique port connections. The Clavister CorePlus™ Port Manager has a limit of approximately 65,000 connections for a unique combination of source and destination IP addresses. Where a large number of internal clients are using applications such as file sharing software, very large numbers of ports can be required for each client. The situation can be similarly demanding if a large number of clients are accessing the Internet through a proxy server. The port number limitation is overcome by allocating extra external IP addresses for Internet access and using NAT Pools to allocate new connections across them.

Modes of Operation

The NAT Pool can operate in one of three modes.

- Fixed NAT Pool
- Stateless NAT Pool
- Stateful NAT Pool

Fixed NAT Pool

When operating in Fixed mode the internal IP address will be mapped directly to a fixed IP address in the NAT Pool. An internally translated IP address will always be mapped to the same external IP address.

The Fixed option has the advantage of not requiring memory for a state table and providing very fast processing for new connection establishment. Although explicit load balancing is not part of this option, there should be spreading of the load across the external connections due to the random nature of the allocating algorithm.

Stateless NAT Pool

When you configure the system to operate in Stateless mode, the least used IP address from the NAT Pool will be the one that the NAT Pool assigns as the IP address. There is no guarantee that new connections from the same host will be mapped to the same external IP address.

The advantage of a Stateless NAT Pool is that there is good spreading of new connections between external IP addresses with no requirement for memory allocated to a state table and there is less processing time involved in setting up each new connection. The disadvantage is that it is not suitable for communication that requires a constant external IP address.

Stateful NAT Pool

In Stateful mode, the least used IP address will be chosen if the source address have not been NAT'd before. All new NAT'd connections will be NAT'd through the same IP address. When the last NAT'd connection from a certain local IP address is closed, there will be a delay before the state of the local IP address is removed. This will help to ensure that new connections will be NAT'd to the same IP address.

The advantage of the Stateful approach is that it can balance connections across several external ISP links while ensuring that an external host will always communicate back to the same IP address which will be essential with protocols such as HTTP when

cookies are involved. The disadvantage is the extra memory required by Clavister CorePlus™ to track the usage in its state table and the small processing overhead involved in processing a new connection.

IP Pool Support

In normal cases, IP addresses are statically loaded into the NAT Pool when the configuration is loaded. However, it is also possible to load the NAT Pool with IP addresses retrieved using the DHCP server. This is accomplished by connecting a NAT Pool to an IP Pool object. When a NAT Pool is configured to use an IP Pool in order to fetch IP addresses, the number of addresses to fetch is specified together with the IP Pool to use.

Using NAT Pools

NAT Pools are used in conjunction with NAT IP rules. When defining a NAT rule, the dialog includes the option to select a NAT Pool to use with the rule. This association brings the NAT Pool into use. In the following example we will first set up a NAT Pool and later create a NAT IP rule that use the newly created NAT Pool. This example creates a NAT Pool which will be applied the external IP address range 10.6.13.10 to 10.16.13.15 and then uses the NAT Pool in a NAT IP rule for HTTP traffic on the Wan interface.

1. Start your Clavister FineTune application, if it is not already started, and select the Security Editor from the Tools menu.
2. Right-click on the Security Gateway to bring up the contextual menu and select Version Control > Check Out. You can also select the Security Gateway and use Ctrl-O.
3. Expand the Security Gateway by clicking on the + (plus) sign. Expand the Local Object folder by clicking on the + (plus) sign.
4. Right-click on the NAT Pools icon to bring up the contextual menu and select New NAT Pool.... You can also select the NAT Pools icon and use Ctrl-N.
5. The NAT Pools Properties dialog is shown. Select the NAT Pool tab and enter the following information for our first pipe:

```
Name: my_natpool
Type: Stateful
Address Range: 10.6.13.10-10.16.13.15
```

6. Select the Proxy ARP tab and enter the following information:

```
Interface: WAN
```

7. Click OK to accept all changes.
8. Next we create the NAT rule that use the newly created NAT Pool. Expand the Rules folder by clicking on the + (plus) sign.
9. We will add this rule to the Main rule set. Right-click on the Main rule icon to bring up the contextual menu and select New Rule.... You can also select the Main rule icon and use Ctrl-N.
10. The Rule Properties dialog is shown. Select the Rule tab and enter the following information for our first pipe:

```
Name: natpool_rule
Action: NAT
Source Interface: int
Source Network: int-wan
Destination Interface: wan
Destination Network: all-nets
```

11. Select the Service tab and enter the following information:

```
Pre-defined: HTTP
```

12. Select the Address Translation tab and select Use NAT Pool. Select from the drop-down list the newly created NAT Pool:

```
NAT Pool: my_natpool
```

13. Click OK to accept all changes.

Conclusion

This Feature Brief describes how to manage NAT Pools 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.

NAT Pools Key Benefits

- Supports a huge number of unique port connections for very large and traffic intense networks.
- Supports extremely NAT'd environments, such as telecommunication environments.
- The NAT Pools functionality breaks the 65,000 connection limit imposed by the Clavister CorePlus™ Port Manager and enables NAT Pools to handle 65,000 connections per IP address.
- Three different modes of operations to suite a versatile number of installations and usage. This allows for a very fine granular administration which is useful in large networks where there might be a diversified need for how the addresses are assigned for different users groups.

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 options. 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 and in your email. 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-nat_pools \(0801\)](#)