7

**NAT Policies**

Learning Note:

NAT Rules

NAT has been always a favorite topic network security professionals. It’s popular because of it’s complexity and it’s usability. It solves many pain areas in IP the internetworking. Let’s understand some of the pain areas addressed by NAT.

Pre-requisites: Let’s just re-cap the virtual network topology that we are using: -

1. We need to recap some of the networking basics. Please refresh your knowledge with some pointers below: -
   1. IPv4 is a 32-bit IP addressing scheme.
   2. Subnet mask is used along with an IP address. Without a subnet mask, an IP address does not make any sense.
   3. With the help of an IP address along with a subnet mask, we can easily understand the network and the host part.
   4. Being a 32-Bit IP address, it’s divided in 4 octets.
   5. Octet means, a block of 8 bits. Each bit in an octet is represented as per its position from right to left in an octet. The rightmost bit is termed as 20, then followed by 21, 22, 23…. and then the leftmost bit as 27. Lett’s see a table below to see the bit value depending on its position in an octet.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Bit Positioning | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| Bit Value | 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 |

* 1. Any individual bit can either be in an ON state or be in an OFF state. If any particular positioned bit is in OFF state which is represented as Zero, then that particular bit have no corresponding value, whereas if the Bit is turned ON which is represented as ONE, then that bit has some corresponding value, and that value depends on it’s positioning in an octet.
  2. ON bits represents network side of the subnet, and OFF bits represents Host side of the subnet.
  3. If all the bits in an Octet are turned ON, then value of the octet will be the sum of all bits. So, let’s add each bit’s value one by one; 1 + 2 + 4 + 8 + 16 + 32 + 64 + 128 = 255. And this is the maximum value. One thing to notice here is that now there is no space left for any host, cause all the bits are turned on and has been acquired by networks. Similarly, if all the bits are turned OFF then the value of an octet will be zero.
  4. IP addresses have been divided into private and public categories.
  5. Private categories contain those IP addresses which can be used by organizations to form their private networks. There are no financial charges for using private IP addresses.
  6. Private IP addresses also referred as ‘RFC 1918’ have been further categories into 3 different classes. See a table below for an easy reference: -

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Class | CIDR block | IP address range | Mask bits | Host ID size |
| Class A network | 10.0.0.0/8 | 10.0.0.0 – 10.255.255.255 | 8 bits | 24 bits |
| Class B network | 172.16.0.0/12 | 172.16.0.0 – 172.31.255.255 | 12 bits | 20 bits |
| Class C network | 192.168.0.0/24 | 192.168.0.0 – 192.168.255.255 | 16 bits | 16 bits |

1. One can choose the private IP address range on the basis of an organization side. If it’s a very large organization, then Class A network will fulfill all the requirements. And small organizations can start with Class C network.
2. Private IP addresses are free but non-routable, that means private IP addresses are not capable to route your packets over the INTERNET cloud (INTERNETWORK of ISPs). That means in our virtual lab environment – we are using 192.168.200.0/24, 192.168.70.0/24, and 192.168.80.0/24 as private IP addresses. So, as per the law of networking, these IP addresses are private IP addresses, and cannot route my traffic over to the INTERNET cloud.
3. Public IP addresses are routable that means they are capable to route IP packets over the INTERNET cloud (INTERNETWORK of ISPs), but they are not free. That means if I have a public IP address or any NATed IP address, that I can use to mask the entire internal network of 192.168.70.0 & 192.168.80.0 and then my packets will be able to traverse over INTERNET cloud.
4. The above 2 points are actually the pain area and the solution provided by the NAT technology.
5. Hope I was able to build relationship between several different concepts and join all these dots.

Advantages

1. If NAT technology was not there, then we would have run short of IPv4 addresses decades ago. cause that means every individual on earth needs a public IP address for accessing and browsing resources over the INTERNET cloud.

1. With the help of NAT technology (Hide technique) we are able to use private IP addressing schemes inside an organization and use public IP addresses to route the entire organization traffic over to the INTERNET cloud. Another advantage of using NAT hide technique is that the INTERNET community will not be able to see the real private IP address used inside an organization as it will be masked behind a public IP address. So, hacking community will not be able to enumerate the private IP address.
2. With the help of using PAT feature supported by the NAT technology, we can mask many thousands of IP addresses behind just one public IP address. That means any organization with some thousands of employees can operate over the INTERNET cloud with just a single public IP address. PAT stands for Port Address Translation. We will explore PAT in upcoming sections.

1. With the help of NAT technology (Static technique) we are able to map a public IP address with an application or web server in our organization and allow everybody in the world to connect to it over some restricted ports. This is doable cause the IP address mapped to the real private IP address of the web server is public in nature and it’s routable over the INTERNET cloud. ARP protocol plays an important role here. Static NAT works with the help of proxy NAT functionality supported by the Security Gateway.

Almost any layer3 device available in a market today can function as a NAT gateway and provides both the Hide and Static NAT techniques. Checkpoint Security Gateway has capabilities to act like a NAT Gateway. Checkpoint Security Gateway can also perform publishing or proxy ARP functionality.

Proxy ARP

**Proxy ARP** is a technique by which a [proxy server](https://en.wikipedia.org/wiki/Proxy_server) on a given network answers the [Address Resolution Protocol](https://en.wikipedia.org/wiki/Address_Resolution_Protocol) (ARP) queries for an [IP address](https://en.wikipedia.org/wiki/IP_address) that is not on that network. The proxy is aware of the location of the traffic's destination and offers its own [MAC address](https://en.wikipedia.org/wiki/MAC_address) as the (ostensibly final) destination.[[1]](https://en.wikipedia.org/wiki/Proxy_ARP#cite_note-1) The traffic directed to the proxy address is then typically routed by the proxy to the intended destination via another interface or via a [tunnel](https://en.wikipedia.org/wiki/Tunneling_protocol).

The process, which results in the proxy server responding with its own MAC address to an ARP request for a different IP address for proxying purposes, is sometimes referred to as *publishing*.



Understanding of Routing and ARP is a pre-requisite in order to understand NAT concepts well. If you lack in either of these 2 concepts, believe me you will never be able to understand the concept in-depth. I will try my best using scenarios and use cases to make sure that you understand both the concepts and apply this knowledge in your real production network.

let’s understand the Routing

you know that IPv4 addresses has been divided into 2 major categories: Private IP addresses and public IP addresses. And Private IP addresses, which can be used in a private network of any organization are free to use have some classes and IP addresses series/range reserved.

Let’s undestand the ARP

NAT is a part of Access Control Policy, and here you can create NAT rules. See the screenshot below: -

Security Gateways with NAT capabilities can easily modify either the source or the destination IP address in an IP packet or change both the IP addresses in a same connection.

When the source IP address is modified by the Security Gateway to any other routed IP address, this terms is known as ‘Source address translation’. And when the destination IP address is modified by the security Gateway to any other routed IP address, then this term is known as a ‘Destination Address Translation’.

Understanding of Routing

Hide NAT provides : Many to One relationship, unidirectional in nature. Unidirectional means that the traffic is always initiated from the private side or from the source side of the network.the destination side can never connect back to the real IP address behind the NATed IP address. They can connect to the NATed IP address, but there is no service hosted. So there is no harm. Concept of ARP is mandatory to understand in order to understand NAT concepts well.

Static NAT provides: One to One relationship, Many to Many relationship, and bi-directional in nature.

Format of a Translated Packet

There are 3 major fields in an IP packet; source IP address, destination IP address and a service. There are many other important fields in an IP packet, but for the purpose of NAT concept, we will only concentrate on 3 fields. But when NAT is enabled on any object/IP address using automatic NAT method or when you try to create a NAT rule manually for any object/IP address, then you need to understand these 6 fields.

These 6 fields make the structure of a NAT rule.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Original Packet | | | Translated Packet | | |
| Original Source | Original Destination | Original Service | Translated Source | Translated Destination | Translated Service |
|  |  |  |  |  |  |

Types of NAT

Checkpoint supports 2 types of NAT: (1) Hide NAT, and (2) Static NAT.

NAT Configuration types

There are 2 ways to configure NAT rules. Checkpoint Security Management Server offers automatic and manual ways to create and configure NAT rules. Automatic, as the name sounds is the simples form compared to the Manual way of NAT rules configuration.

Manual NAT rules require much knowledge.

# NAT Configuration

## Checkpoint NAT Types

Checkpoint offers 2 types of NAT functionalities. As a Firewall Administrator, you must understand both these NAT types. Each type of NAT functionality solves different purposes. Both the NAT types work independently, they are not related to each other. NAT Types supported by Checkpoint are: -

* Hide NAT
* Static NAT

Hide NAT is also popular with another term known as a ‘Dynamic NAT’.

## Ways to do NAT Configuration in Checkpoint

Checkpoint offers 2 ways to configure NAT functionalities using SmartConsole.

As you create firewall rules to secure the organization network, similarly you need to create NAT rules to achieve the advantages of address translation. Now these NAT rules can be created using 2 different ways using Checkpoint SmartConsole. These are the 2 different ways: -

* Automatic technique
* Manual Technique

If you choose automatic technique, then NAT rules will be populated automatically and shown in the NAT policy section. Whereas in Manual NAT rules, you need to create rules manually. Manual NAT is more powerful technique compared to automatic technique.

NAT rules are processed by the security gateway in a sequential order. But both Automatic and Manual NAT rules are processed by the Security Gateway in different ways. Lets try to understand this…..

So, try to understand the simple graph below: -

## 

## Automatic NAT

Let’s understand checkpoint Automatic NAT rules. We will discuss Automatic hide and Automatic static NAT rules in this section.

## Manual NAT

Let’s understand checkpoint Manual NAT rules.

## Automatic vs Manual NAT

## 

Both both these techniques are useful for a firewall administrator, but its important that you must understand the differences between them. Understanding of these differences will help you in making right decision of selecing the right technique in your organization while doing the NAT configuration. Please see pointers below:=

1. Automatic NAT is simple, while Manual NAT is complex.
2. Automatic NAT is also referred as an Object NAT, and manual NAT is manual NAT only.
3. Automatic NAT is configured by enabling the NAT on the desired object.
4. Every Network object in Checkpoint has a submenu for NAT configuration.
5. This submenu provides you a drop down to select between Hide and a Static NAT.
6. NAT Rules created using automatic technique are orderd, while in manual NAT, you need to order them manually.
7. This is how automatic NAT rules are ordered and organized by the SmartConsole: -
   1. 1st preference: Static automatic NAT rule for a Host object (include Security Gateway).
   2. 2nd Preference: Hide automatic NAT rule for a Host object (including Security Gateway).
   3. 3rd : Static automatic NAT rule for a Network or Address Range object.
   4. 4th : Hide automatic NAT rule for a Network or Address Range object.

1. Automatic NAT does not give you flexibility to translate both the source and the destination IP addresses in a single rule or in a single object, but using Manual NAT rules, you can translate both the source and the destination IP addresses at the same time using a single rule.

## Hide NAT – Using Automatic technique

Hide NAT simply means that it hides the real private network IP addresses behind the public IP address. It adds a secure layer to an organization private IP addressing scheme, cause now it’s not exposed to the outside world. Outside world only see the public IP address as a face of an organization instead of real private IP address behind the scene. PAT functionality is embedded in the NAT functionality.

Hide NAT is used to provide outbound INTERNET access to one or many private IP addresses in an organization. Outbound internet access is a typical use case of a Hide NAT. Imagine in our virtual lab, if we want to give INTERNET access to the whole network – 192.168.70.0/24 and 192.168.80.0/24. And we can also select any individual host for a Hide NAT. such as we can Hide NAT for one of the servers – 192.168.80.50.

Hide NAT offers one to one or many to one relationship. That means you can associate one public IP address with one specific private IP Address (Use case of NAT), or you can also associate one public IP address with many private IP addresses in an organization. Such as we will map the public IP address (in our virtual lab, not otherwise) 192.168.137.11 to hide these entire networks: -

192.168.200.0/24

192.168.70.0/24

192.168.80.0/24

Hide NAT is uni-directional in nature. That means inside LAN or private IP addresses once mapped with public IP address can access INTERNET resources. But nobody from the INTERNET side can initiate the connection and connect back to the public IP address which was used hide the internal network. I mean they can offcorse attempt to connect, but this connection will not be allowed by the Security Gateway.

Hide NAT is also known as a source address tranalation cause in this NAT type the actual source who initiated the traffic in the organization LAN is changed to any public IP address. So, the source IP address in packet is changed from real private IP address to the public IP address.

Hide NAT can be applied using (1) Automatic NAT technique as well as (2) Manual NAT Technique.

## Hide NAT – Using Manual technique

## Static NAT – Using Automatic technique

## Hide NAT – Using Manual technique

**Technical requirements**

**Pre-requisites**

**Virtualization Environment Readiness**

**Connectivity Testing Between Host and Virtual Machines**

**Address Translation in Checkpoint**

**Address Translation Types**

**Address Translation Techniques**

**NAT Global Policies**

------------------------------------------------------------------------------------------------------------------------------------------

**Labs and Use Cases for Automatic NAT**

Use Case # 7 – Automatic Hide NAT on the Network Object using Gateway IP.

Now comes the turn to address business needs and allow some of the most used protocols for the entire LAN in an organization with the help of firewall rules in an Access Control Policy. These rules attempt to connect to the internet hosted destination servers through the security gateway.

We will configure Automatic Hide NAT in this use case. ….

Let’s work on a use case below to get the correct understanding behind the Automatic NAT for the host object.

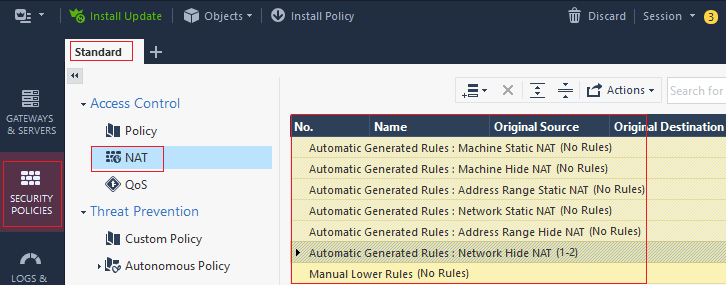
**Scenario:** Allow outbound internet access for internal network using NAT functionality.

**Task # 1:** Setup Automatic Hide NAT for an internal network 192.168.70.0/24 using ‘Hide behind the gateway’ NAT method.

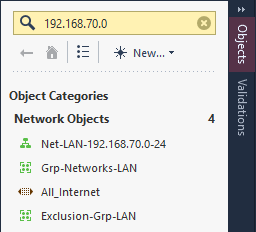
Once configuration is done, then see the NAT rules created automatically in the NAT policy. And generate some traffic to see relevant logs.

**Solution:** Please perform these steps to configure ‘Hide behind the gateway’ automatic Hide NAT method for a Network object: -

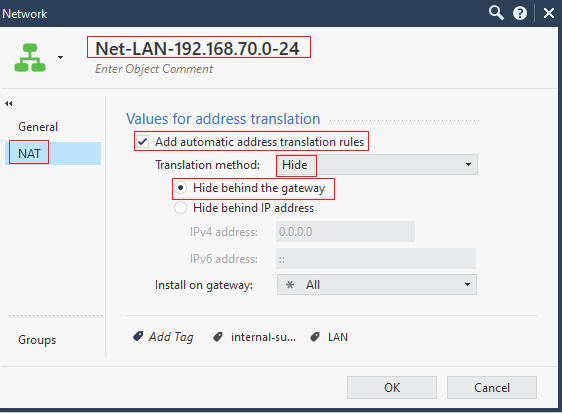
1. Login into SmartConsole R81.10 GUI client.
2. Go to NAT policies and observe current NAT policies visible there. At present there is no NAT rule in the current ‘Standard’ NAT Policy.
3. NAT policy is structed under 8 major sections, which are listed below: -
4. Automatic Generated Rules: Machine Static NAT
5. Automatic Generated Rules: Machine Hide NAT
6. Automatic Generated Rules: Address Range Static NAT
7. Automatic Generated Rules: Network Static NAT
8. Automatic Generated Rules: Address Range Hide NAT
9. Automatic Generated Rules: Network Hide NAT
10. Refer to the screenshot below to see the default NAT Policy.



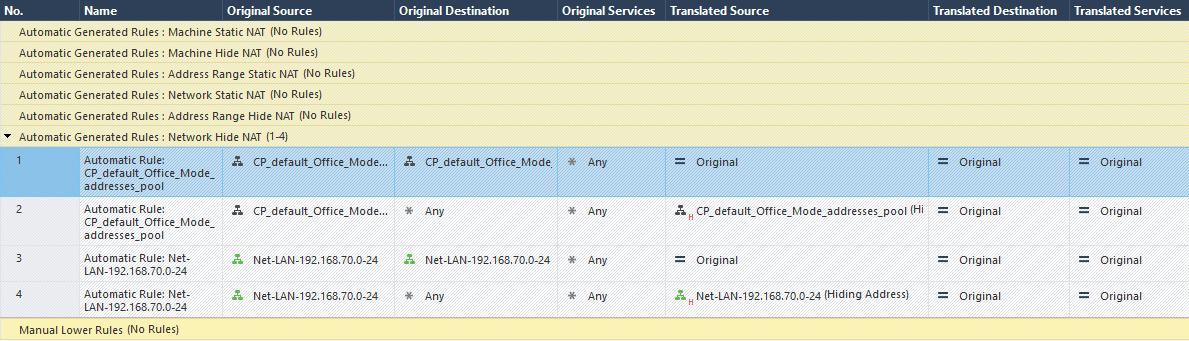
1. Go to Object pane, and search for the network object for internal network: 192.168.70.0. Refer to the screenshot below: -



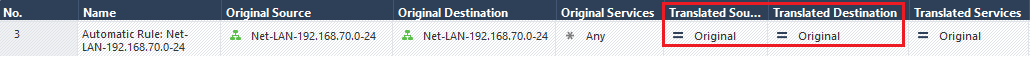
1. Access the network object.
2. Go to the ‘NAT’ tab in the object.
3. Select the option ‘Add automatic address translation rule’.
4. Choose the ‘Hide’ option in the ‘Translation Method’ field.
5. Select the option ‘Hide behind the gateway. Refer to the screenshot below: -



1. Click on OK.
2. Click on the Install Policy button and fill in the necessary details to create a revision.
3. As we have understood from the concepts in above sections that ‘Automatic NAT’ is also referred as an ‘Object NAT’, once enabled automatically creates NAT rules in the NAT Policy. And as we have enabled ‘Automatic NAT’ on a network objects, we must see corresponding NAT rules created automatically.
4. Click on ‘Security Policy’ menu
5. Click on the ‘NAT’ menu under ‘Access Control Policy’ in SmartConsole.
6. Here you will see that 2 NAT rules are created for the network – 192.168.70.0/24 under category ‘Automatic Generated Rules: Network Hide NAT’. Refer to the screenshot below: -



1. Enabling NAT on the network object has created 2 NAT rule entries automatically in the NAT Policy.
2. 1st NAT rule entry says that in any packet/connection, if the source and the destination both IP addresses are in the same network ‘192.168.70.0/24’, then do not change anything. In this entry, ‘Translated Source’, and ‘Translated Destination’ are set to ‘Original’.
3. See a screenshot below for the 1st NAT entry: -



1. 2nd NAT entry says that in any packet/connection, if the ‘Original Source’ is any IP address in the network 192.168.70.0/24, and ‘Original Destination’ is set to ‘\* any’, then performs a Hide NAT. Look carefully in the ‘Translated Source’ field in this NAT rule entry. You will find this object there: -

,

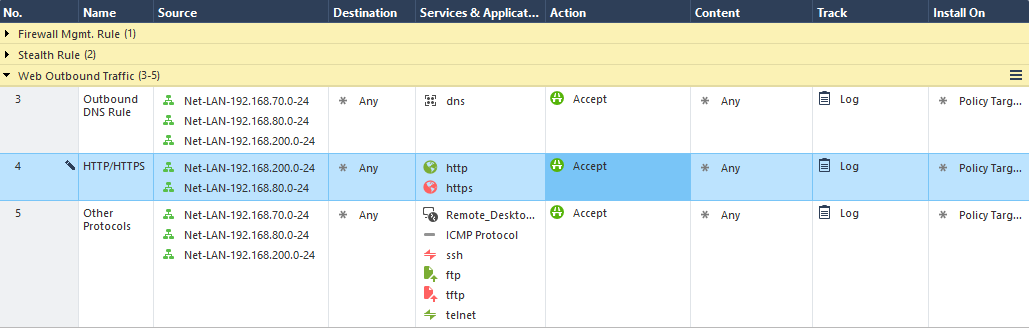
1. It means that now source translation is happeing using (H) Hide NAT in this rule. See a screenshot below for the 2nd NAT entry: -



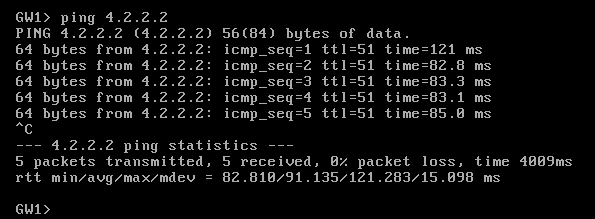
1. Automatic Hide NAT for the network object is completed in this use case. Next, we will do some outbound connectivity testing.

**Pre-requisite for Connectivity Testing**

1. Before we continue testing NAT connectivity, please make sure that you have completed the previous chapter and created all firewall rules as per demonstrated in all use cases. Please refer to the screenshot below, you must have all these firewall rules created in the policy package: -

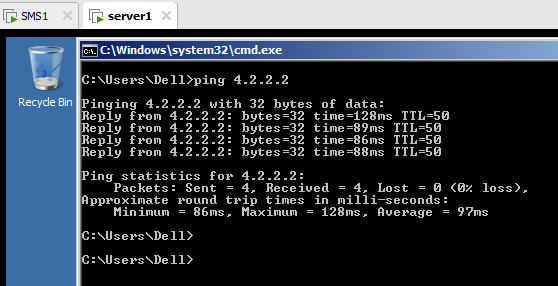


1. Remember that NAT configuration is not going to allow access, it is just going to translate either the source or the destination IP address in the original packet. If any specific access is not allowed in the Access Control List, then even if the NAT configuration is correct, then the desired connectivity will never work. For any NAT rules to give expected results, the corresponding Access Control must be allowed in the Security Policy.
2. Cause you are doing all these labs on top of VMware virtual machines hosted over your laptop or desktop. Please ensure that your laptop/desktop has internet connectivity up and running. Then go to either the Wi-Fi or the Ethernet NIC card/interface --> Go to Properties --> Go to Sharing tab --> and make sure that it is configured as per screenshot below: -
3. Now, to test if the Internet connection has been shared with the VMware VNET, login into Security Gateway ‘GW1’ VM, and try to ping the Global DNS Server. If you get the response back, that means the internet is accessible over VMs. Please see the screenshot below: -

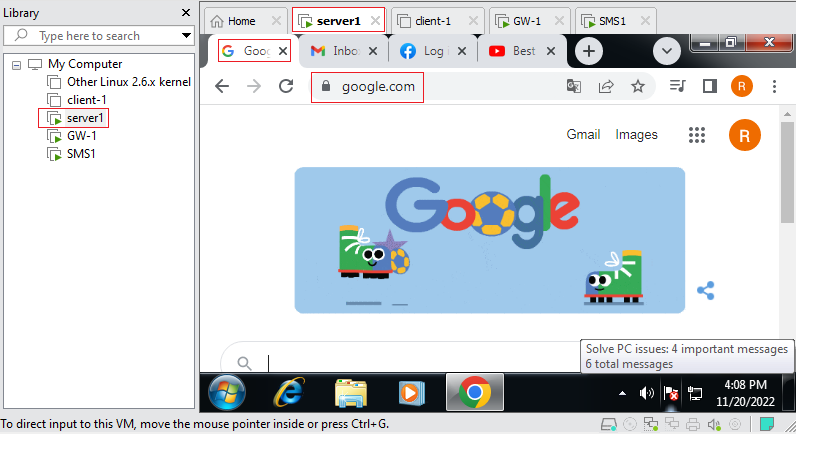


**Connectivity Testing:** please perform these steps to do connectivity testing: -

1. Login into CLI mode in ‘Server1’ VM and try to ping the Global DNS Server IP address – 4.2.2.2. This ping test should work. See screenshot below: -

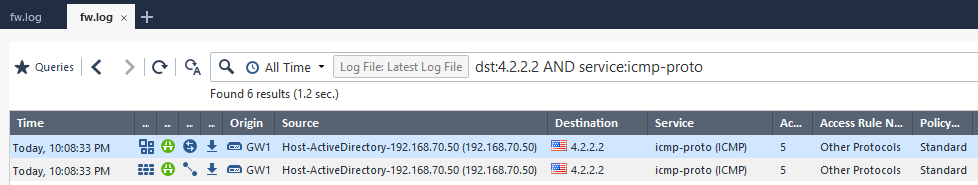


1. Open the Web Browser in the ‘server1’ VM and access <https://www.google.com>. This site should be accessible. See screenshot below: -

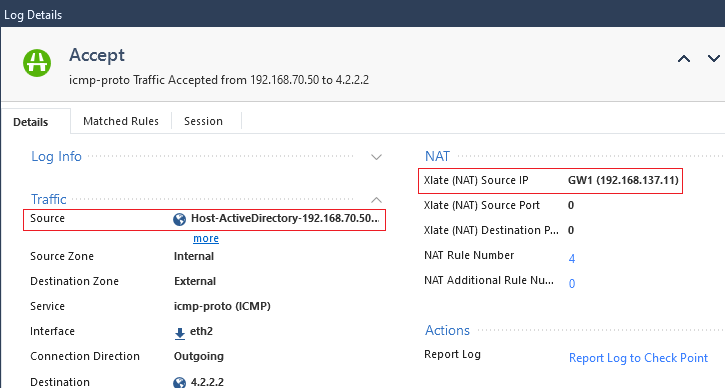
  
**Check relevant Logs:**

Now, we will check relevant logs to see if the original source IP address has been translated to the Security Gateway IP address or not.

1. Click on ‘Logs & Monitor’ menu
2. Type following query in the address bar - ‘dst:4.2.2.2 AND service:icmp-proto’. You will see log entries. Refer to the screenshot below: -



1. Now, double click on the first log entry, and investigate the NAT section. You will see that the translated source IP address is – 192.168.137.11. You can also the NAT rule number processed to do the source address translation. Refer to the screenshot below: -



1. With this we have successfully completed this use case.

Use Case # 8 – Automatic Hide NAT on the Host Object using Other IP.

If NAT is enabled on any network object, then this NAT setting will be applied to all the live and active IP addresses in this network. All IP addresses in the network will be translated using the same IP address. Imagine a situation in which you want one specific Server in the network to use a different IP address for the source translation than others in the same network. You keep facing such exceptions to NAT demands on a daily basis. Don’t worry, you can achieve this. Now, you just need to enable the Automatic Hide NAT on that Server Host object.

One thing always keeps in mind, and we have also discussed above, that the NAT rule for the host object will have a higher precedence than the NAT rule for the network object. That means NAT rule for the host object will be processed before the NAT for the network object.

Let’s work on a use case below to get the correct understanding behind the Automatic NAT for the host object.

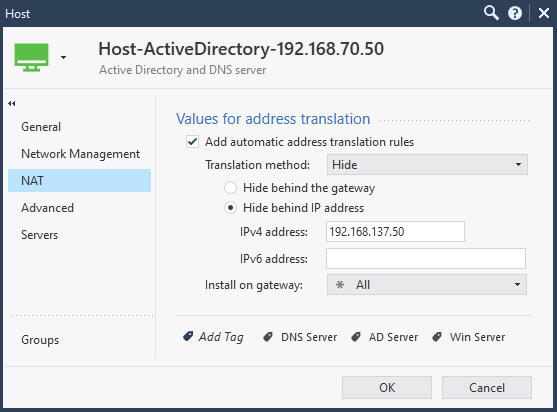
**Scenario:** Allow outbound internet access for an internal server ‘192.168.70.50’ using NAT functionality.

**Task:** Setup Automatic Hide NAT for an internal server 192.168.70.50 using ‘Hide behind IP address’ NAT method. Hide this Server behind IP Address – 192.168.137.50.

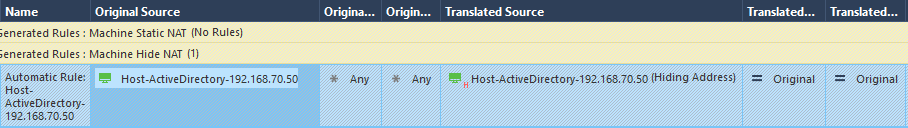
Once configuration is done, then see the NAT rules created automatically in the NAT policy. And generate some traffic to see relevant logs.

**Solution:** Please perform these steps to configure ‘Hide behind IP address’ automatic Hide NAT method for a Host object: -

1. Login into SmartConsole R81.10 GUI client.
2. Go to NAT policies and observe current NAT policies visible there. At present there are automatic Hide NAT rules configured the network – 192.168.70.0/24. There is not yet any automatic NAT rule for the Host object.
3. Go to Object pane, and search for the Host object for a server: 192.168.70.50. If the object does not exist, then please create a host object. Refer to Chapter # 4 in case you want to refresh your concepts related to Objects creation.
4. Access the Host object for a server – 192.168.70.50
5. Go to the ‘NAT’ tab in the object & select the option ‘Add automatic address translation rule’.
6. Choose the ‘Hide’ option in the ‘Translation Method’ field.
7. Select the option ‘Hide behind IP address’ and put IP address 192.168.137.50. Refer to the screenshot below: -



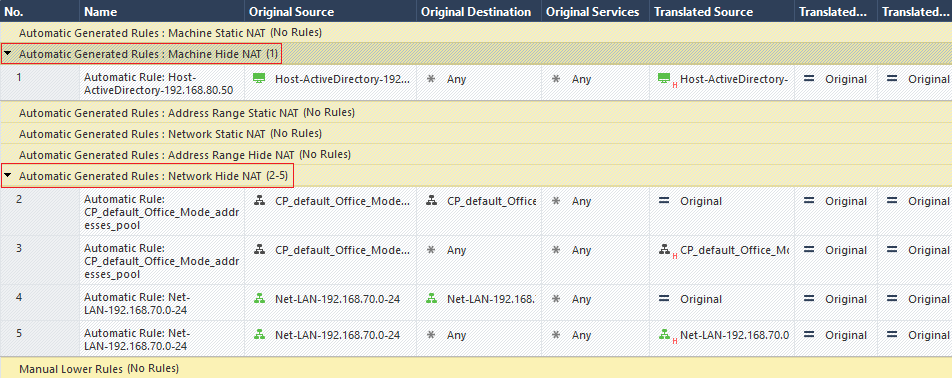
1. Click on OK.
2. Click on the Install Policy button and fill in the necessary details to create a revision.
3. Click on ‘Security Policy’ menu
4. Click on the ‘NAT’ menu under ‘Access Control Policy’ in SmartConsole.
5. Here you will see a single NAT rule is created for the Host object – 192.168.70.50 under the category ‘Automatic Generated Rules: Machine Hide NAT’. Refer to the screenshot below: -



1. This NAT entry says that in any packet/connection, if the ‘Original Source’ is the Server IP address, and ‘Original Destination’ is set to ‘\* any’, then performs a Hide NAT. Look carefully in the ‘Translated Source’ field in this NAT rule entry. You will find this object there: -



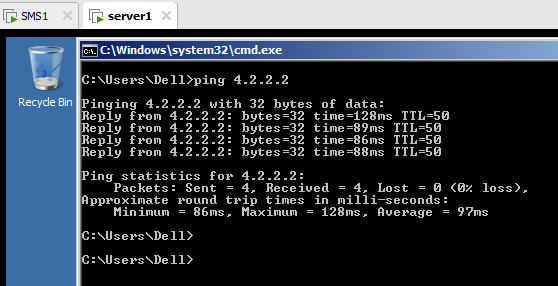
1. One thing you need to focus on is that 2 NAT rules were created for the NAT configuration on the Network object, and a single NAT rule is created for the NAT configuration on the Host object.
2. Automatic NAT for the Host object takes higher precedence than Automatic NAT for the Network object. Please refer to the screenshot below to the see the complete NAT policy page: -



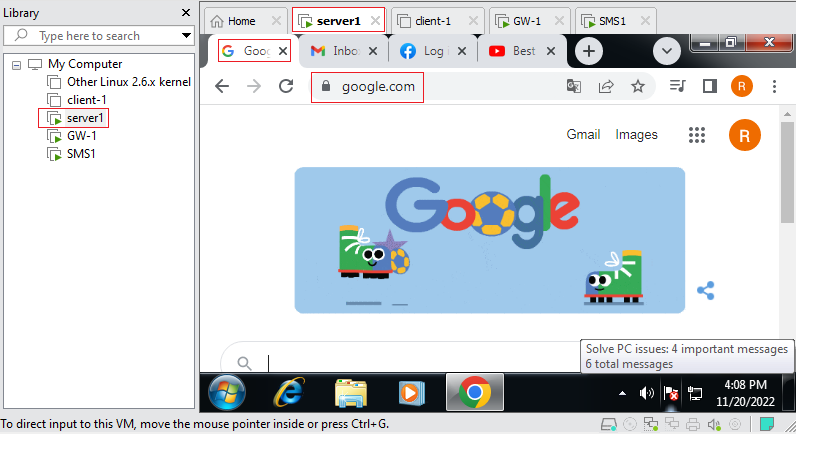
1. Automatic Hide NAT for the Server object is completed in this use case. Next, we will do some outbound connectivity testing.

**Connectivity Testing:** please perform these steps to do connectivity testing: -

1. Login into CLI mode in ‘Server1’ VM and try to ping the Global DNS Server IP address – 4.2.2.2. This ping test should work. See screenshot below: -

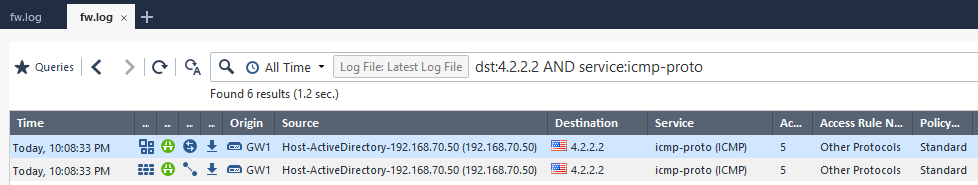


1. Open the Web Browser in the ‘server1’ VM and access <https://www.google.com>. This site should be accessible. See screenshot below: -

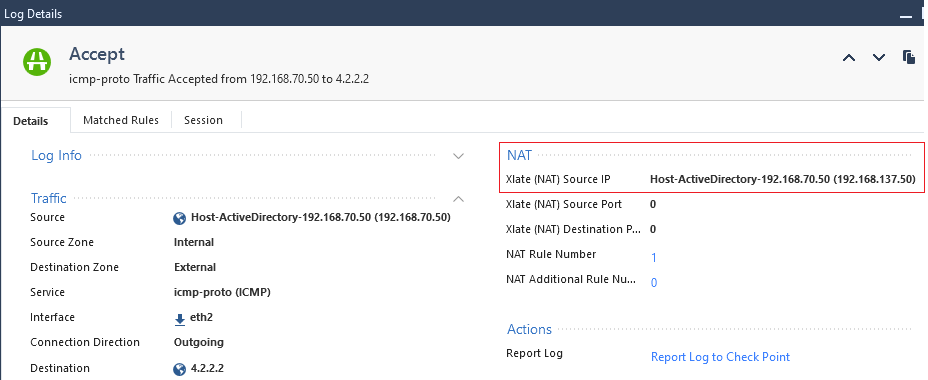
  
**Check relevant Logs:**

Before checking logs, just remember that if the connection is initiated from the Server – 192.168.70.50 Host object, then it should be NATed behind an IP address – 192.168.137.50, whereas if the connection is initiated from any other IP address in the network object 192.168.70.0/24, then it should be NATed to the Gateway IP address – 192.168.137.11 as we saw in the last use case.

1. Click on ‘Logs & Monitor’ menu
2. Type following query in the address bar - ‘dst:4.2.2.2 AND service:icmp-proto’. You will see log entries. Refer to the screenshot below: -



1. Now, double click on the first log entry, and investigate the NAT section. You will see that the translated source IP address is – 192.168.137.50. You can also the NAT rule number processed to do the source address translation. Refer to the screenshot below: -



1. With this we have successfully completed this use case.

Use Case # 9 – Automatic Hide NAT on the Network Range Object using Other IP.

There comes a situation in which you want to create a block of some IP addresses with exact count, and this is not possible with the help of defining subnet mask. There are some of the limitations with Subnetting as well. Imagine you have a block of 10 SAP Servers used by the HR department in the network – 192.168.70.0/2. IP addresses used by these SAP Servers are contiguous, from 192.168.70.81 to 192.168.70.91.

One thing to remember is that these 10 IP addresses used by the SAP servers are part of the network – 192.168.70.0/24. Automatic Hide NAT using the Gateway IP address is already configured for this network object. So, that means the same NAT should also be applied and inherited by the SAP Servers, because they are also part of the same network.

But, as per the requirement, we need to source NAT these 10 SAP servers IP addresses behind IP address - 192.168.137.91. Simply, we do not want to Source NAT these SAP servers behind the Gateway IP address.

You can create an Address Range Object to represent this range of contiguous IP addresses. And enable Automatic Hide NAT on the object with ‘other IP address’ method.

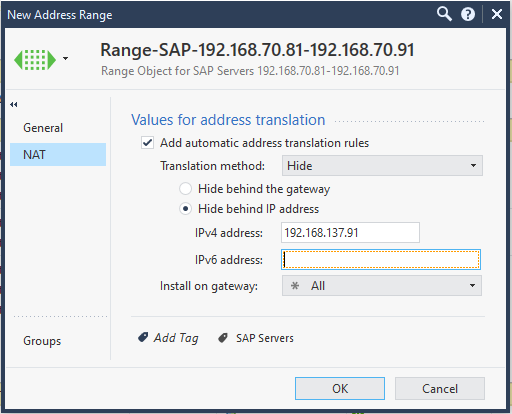
**Scenario:** Allow outbound internet access for an address range ‘192.168.70.81 till 192.168.70.91’ using NAT functionality.

**Task:** Setup Automatic Hide NAT for an address range ‘192.168.70.81 till 192.168.70.91’ using ‘Hide behind IP address’ NAT method. Hide this Server behind IP Address – 192.168.137.91.

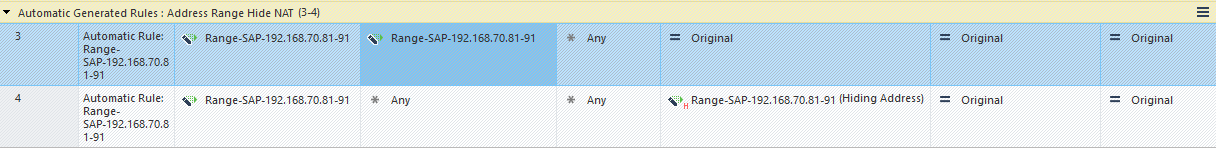
Once configuration is done, then see the NAT rules created automatically in the NAT policy. And generate some traffic to see relevant logs.

**Solution:** Please perform these steps to configure ‘Hide behind IP address’ automatic Hide NAT method for an Address Range object: -

1. Login into SmartConsole R81.10 GUI client.
2. Go to NAT policies and observe current NAT policies visible there. At present there are automatic Hide NAT rules configured as follows: -
3. Automatic Hide NAT for the network – 192.168.70.0/24, using Hide behind the Gateway’ IP address (192.168.137.11)
4. Automatic Hide NAT for the host – 192.168.70.50 ‘using Hide behind IP address (192.168.137.50)’ method.
5. Go to Object pane, and search for an Address Range object. If the object does not exist, then please create an Address Range object. Refer to Chapter # 4 in case you want to refresh your concepts related to objects creation.
6. Access the Address Range object for SAP servers.
7. Go to the ‘NAT’ tab in the object & select the option ‘Add automatic address translation rule’.
8. Choose the ‘Hide’ option in the ‘Translation Method’ field.
9. Select the option ‘Hide behind IP address’ and put IP address 192.168.137.91. Refer to the screenshot below: -



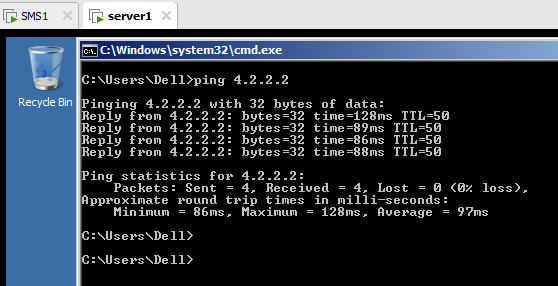
1. Click on OK.
2. Click on the Install Policy button and fill in the necessary details to create a revision.
3. Click on ‘Security Policy’ menu
4. Click on the ‘NAT Policy’ under ‘Access Control Policy’ in SmartConsole.
5. Here you will see that 2 NAT rules are created automatically for an Address Range object under the category ‘Automatic Generated Rules: Address Range Hide NAT’. Refer to the screenshot below: -



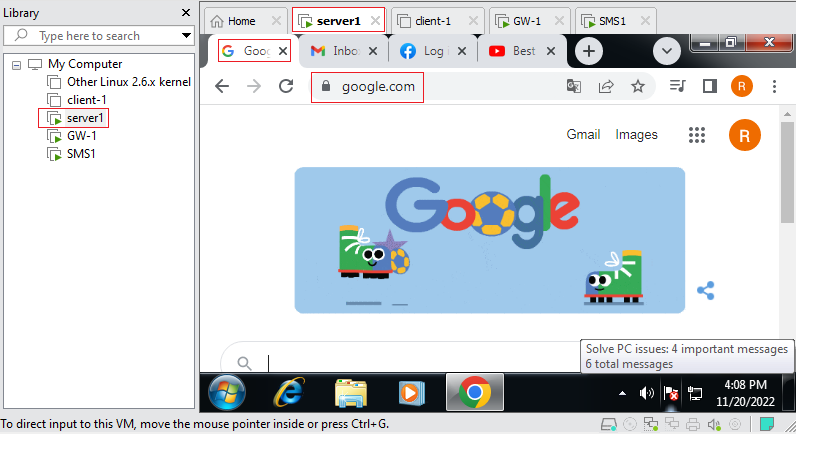
1. Enabling NAT on this Address Range object created 2 NAT rule entries automatically in the NAT Policy.
2. 1st NAT rule entry says that in any packet/connection, if the source and the destination both IP addresses are in the same Address Range object’, then do not change anything. In this entry, ‘Translated Source’, and ‘Translated Destination’ are set to ‘Original’. Read the first NAT entry carefully.
3. 2nd NAT entry says that in any packet/connection, if the ‘Original Source’ is any IP address in the Address Range object and ‘Original Destination’ is set to ‘\* any’, then performs a Hide NAT. Look carefully in the ‘Translated Source’ field in this NAT rule entry. Read the 2nd NAT entry carefully.
4. Automatic Hide NAT for the Address Range object is completed in this use case. Next, we will do some outbound connectivity testing.

**Connectivity Testing:** please perform these steps to do connectivity testing: -

1. Login into CLI mode in the ‘Server1’ VM, its current IP address is 192.168.70.50.
2. Change the IP address of this VM to – 192.168.70.85.
3. Now, try to ping the Global DNS Server IP address – 4.2.2.2 from the Server VM. This ping test should work. See screenshot below: -



1. Open the Web Browser in the ‘server1’ VM and access <https://www.google.com>. This site should be accessible. See screenshot below: -



**Check relevant Logs:**

Before checking logs, just remember these pointers: -

* If the connection is initiated from the Server with an IP address ‘192.168.70.85’, then it’s a part of an Address Range object, and its entire source traffic is NATed behind an IP address - ‘192.168.137.91’.
* Whereas if the connection is initiated from any other IP address in the network object 192.168.70.0/24, then it should be NATed to the Gateway IP address – 192.168.137.11 as we saw in the last use case.

1. Click on ‘Logs & Monitor’ menu.
2. Type following query in the address bar - ‘dst:4.2.2.2 AND service:icmp-proto’. You will see log entries. Refer to the screenshot below: -

Image:

1. Now, double click on the first log entry, and investigate the NAT section. You will see that the translated source IP address is – 192.168.137.91. You can also the NAT rule number processed to do the source address translation. Refer to the screenshot below: -

Image: -

1. With this we have successfully completed this use case.

Note: please change the IP address of the Server VM from 192.168.70.85 to 192.168.70.50.

Use Case # 10 – Automatic static NAT on the Host object with the Firewall Rule.

Now we will deal with Inbound Access. All above uses cases were solving the purpose the providing an Outbound Access. Outbound access is provided using Hide flavor of NAT.

But, where we need to provide an inbound access to some of our Web Applications to some or many users throughout the world, there we will use Static NAT. AS Static NAT is bi-directional in nature, that means either the source side or the destination side in the connection can initiate the traffic. But

With Static NAT in place, Security Gateway behaves differently, and allows external traffic to access the internal servers and applications. Automatic Static NAT can be configured on the Host Object, Network Object, as well as Address Range Object.

As a firewall rule is needed for Hide NAT to work properly, and provide an Outbound access, similarly a firewall rule is needed for Static NAT to work properly and provide inbound access.

Let’s work on a use case below to get the correct understanding behind the Automatic Static NAT for the host object.

**Scenario:** Allow Inbound access for an internal server ‘192.168.70.50’ on Remote Desktop Protocol – TCP/3389 for all users.

**Task:** Setup Automatic Static NAT for an internal server 192.168.70.50 using Public IP address – 192.168.137.50 as per our virtual lab environment, and create a firewall rule in the ‘Stanard’ Policy Package with below conditions: -

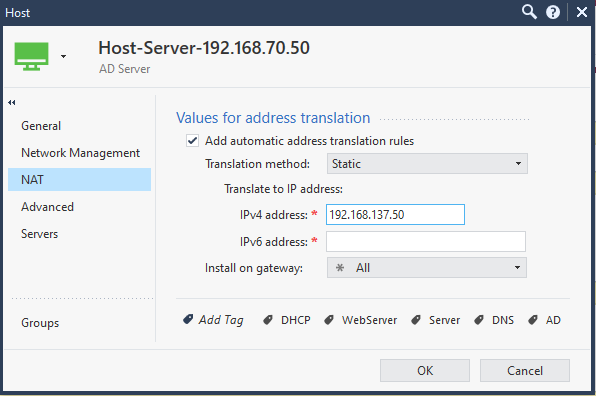
* Source: \* Any
* Destination: 192.168.137.50
* Service: TCP-3389, and ICMP protocol.
* Action: Accept
* Track: Log

Put this rule above all Outbound Rules. And create a section title for this rule as ‘Inbound Access for Servers’.

Once the Static NAT is enabled on the Server Object, then you will see some NAT rules created automatically for you in the NAT Policy under section ‘Automatic Generated Rules: Machine Static NAT’. And if you have also created a firewall rule as per specifications shared above, then you should be able to connect to this Server VM from the Host (Laptop/Desktop) on IP address – 192.168.137.50 over port TCP-3389.

**Solution:** Please perform these steps to configure the Static NAT for the Server – 192.168.70.50: -

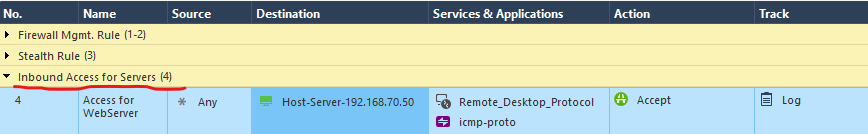
1. Login into SmartConsole R81.10 GUI client.
2. Go to Object pane, and search for the Host object for a server: 192.168.70.50.
3. Access the Host object for a server – 192.168.70.50
4. Go to the ‘NAT’ tab in the object & select the option ‘Add automatic address translation rule’.
5. Choose the ‘Static’ option in the ‘Translation Method’ field.
6. Enter an IP address 192.168.137.50 in the box. Refer to the screenshot below: -



1. Click on OK. Now, Automatic Static NAT configuration for the Host object is done.
2. With this you should see Statis NAT rules created automatically in the NAT Policy. Refer to the screenshot below to see automatic Static NAT rules: -



1. Observe the rule carefully that it’s a bi-directional rule created for the Automatic Static NAT. Also observe that this rule is created on the topmost position in the NAT policy. Automatic Static NAT rules have always higher precedence.
2. Create a new Firewall Rule above existing outbound firewall rules in the ‘Standard’ Policy Package. This new rule will be empty in the beginning.
3. Hover your mouse on the source field and select ‘Switch to Any’.
4. And in the destination field, click on the ‘+’ icon, and select the host object for the server with an IP address – 192.168.70.50.
5. Hover your mouse on the ‘Services & Application field’ and add Microsoft Remote Desktop Protocol – TCP/3389, and ICMP protocol.
6. Hover your mouse on the Action field and select ‘Accept’ as an action.
7. Hover your mouse on the Tracking field and select ‘Log’ as an action.
8. Right click on this rule and create a section title above. Name the section title as ‘Inbound Access for Servers’.
9. This is how this firewall rule should look like: -



1. Click on the Install Policy button and fill in the necessary details to create a revision.
2. Install the policy.
3. Automatic Static NAT for the Server object is completed in this use case. Next, we will do some inbound connectivity testing.

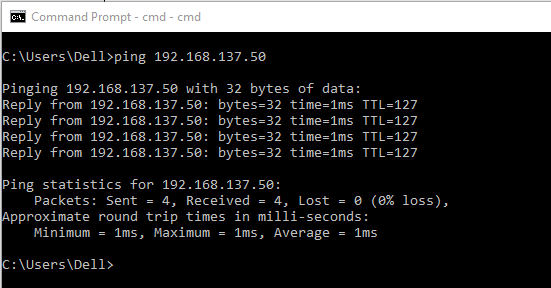
**Connectivity Testing:** please perform these steps to do connectivity testing: -

This connectivity will be bit different. Cause we need to access this Server from the External network.

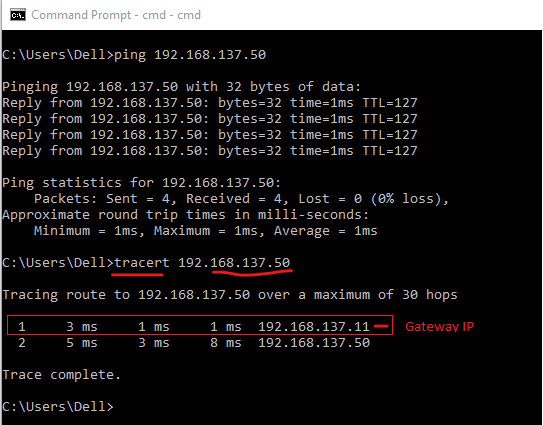
This internal server with an IP Address 192.168.70.50 has been Static NATed behind an IP address – 192.168.137.50.

Before you do this testing, please make sure that the Server VM is powered on, and it’s IP address is 192.168.70.50.

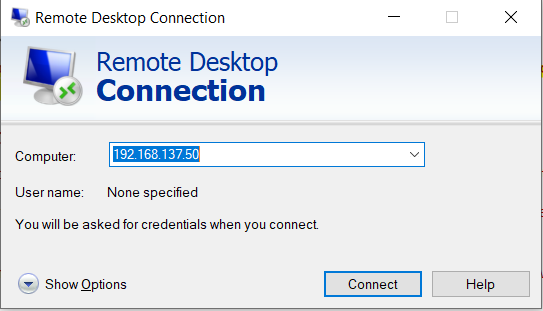
1. Go to the Host (Laptop/Desktop) machine, and open the CMD session.
2. Ping the NATed IP address – 192.168.137.50.
3. You should get a ICMP reply back. It;s working in my lab, please see the screenshow below: -



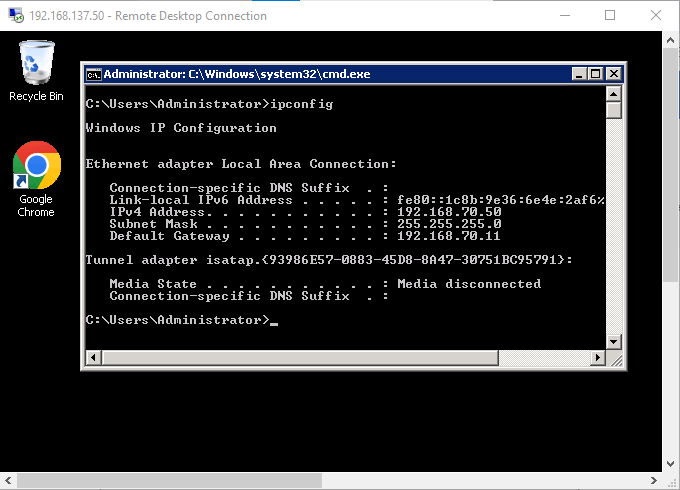
1. Now run the traceroute command to the NATed IP address from the Host System, and you will see that this traffic has crossed the Security Gateway IP address – 192.168.137.11 as it’s first hop, and then it reaches the real server – 192.168.70.50. Please refer to the screenshot below: -



1. and launch the Remote Desktop agent using ‘mstsc’ command from the Host system. Write ‘mstsc’ command in the Windows Search box. It will show ‘Remote Desktop App’. Click on the App to launch it.
2. Now, write down the IP address in the ‘computer field box’ in the Remote Desktop App, and click on the ‘Connect’ button. Refer to the screenshot below: -



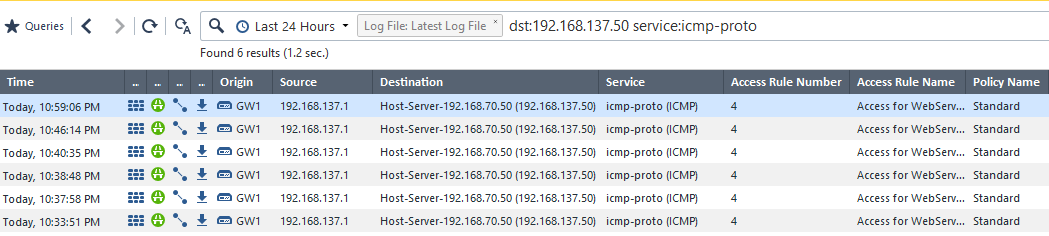
1. It will ask you for credentials, enter correct username and password.
2. Now you should see a Desktop being loaded as a new screen. Refer to the screenshot below: -



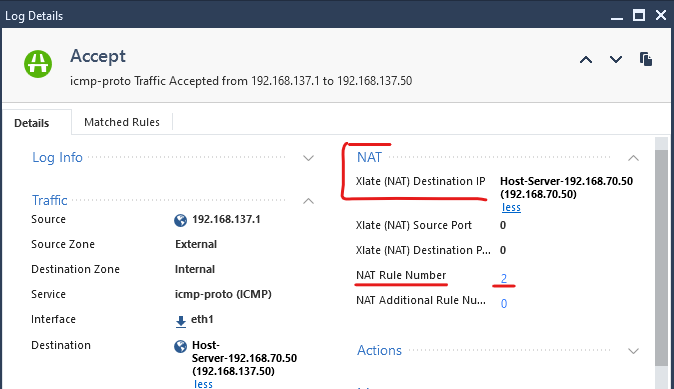
1. We have tested this connectivity using three different protocols; ICMP, traceroute, and RDP. And all these tests are positive and working correctly.
2. Now, we will check logs to see the Address translation happening.

**Check relevant Logs:**

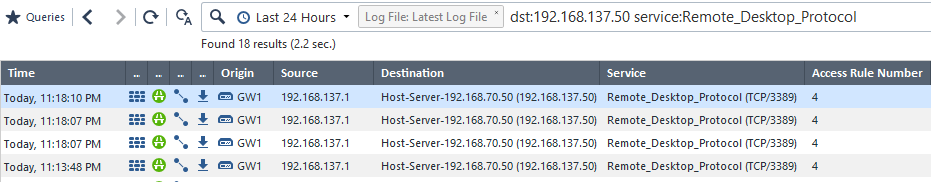
1. Click on ‘Logs & Monitor’ menu.
2. Type following query in the address bar - ‘dst:192.168.137.50 service:icmp-proto’. You will see a couple of log entries. Refer to the screenshot below: -



1. Now, double click on the first log entry, and investigate the NAT section. You will see that the translated destination IP address is – 192.168.70.50. You can also the NAT rule number processed to do the source address translation. Refer to the screenshot below: -



1. Now, type following query in the address bar - ‘dst:192.168.137.50 service:Remote\_Desktop\_Protocol’. You will see a couple of log entries. Refer to the screenshot below: -



1. You can double click any of the log entries, to see the address translation happening, and the translation rule number.
2. This use case is completed successfully with positive results.

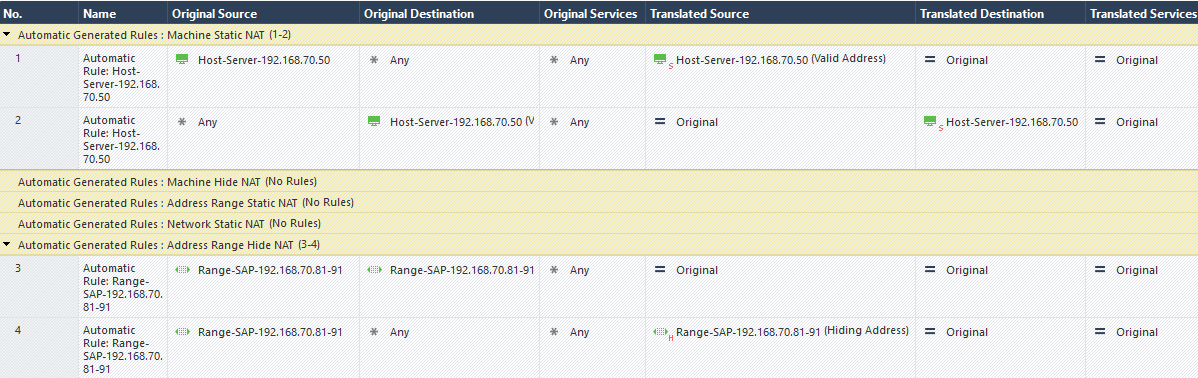
**Order of NAT Rule Encorcement**

**Labs and Use Cases for Manual NAT**

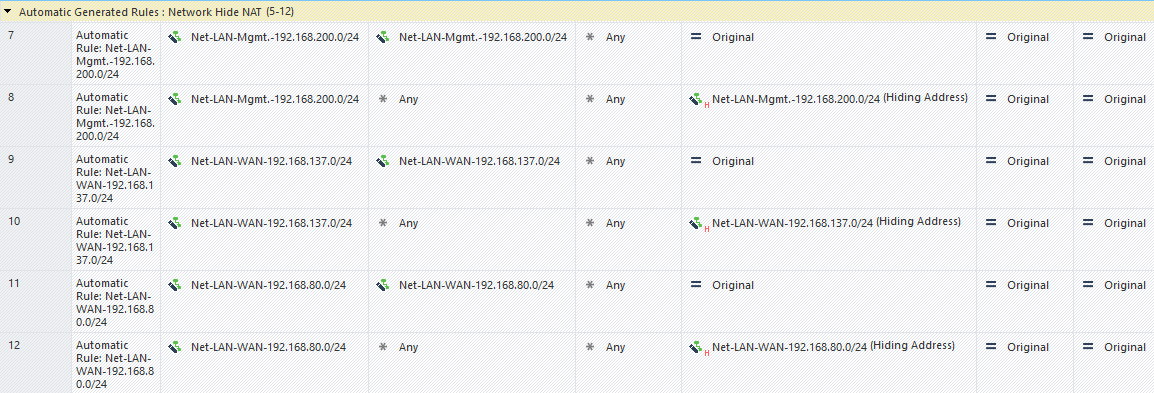
Now, let’s begin the real and interesting NAT configuration. To validate if the NAT rules created manually are working as per expectations, you must uncheck NAT configuration from all the objects. Once automatic NAT is removed from all objects (Host object, Network object and Address-Range object) then you will see that all the rules in the NAT policy are removed.

As of now Automatic Static NAT is enabled on the Windows Server Host object, and Automatic Hide NAT is enabled on the Network object and Address Range object. Refer to the screenshot below to see the current NAT Policy in 2 different screenshots shared below: -

Screenshot for NAT rules for Server and Address Range object: -



Screenshot for the NAT rules for all Network objects: -



Use Case # 11 – Remove Automatic NAT from all objects

Beofre we start creating manual NAT Rules,

Use Case # 12 – Manual Hide NAT on the Network Object using Gateway IP

Manual NAT is complex. Manual NAT is an advanced NAT technology which brings unique capabilities which cannot be obtained using Automatic NAT. We have already discussed the difference between both types in initial sections in the chapter.

Let’s work on a use case below to get the correct understanding behind the Manual NAT for the Network object.

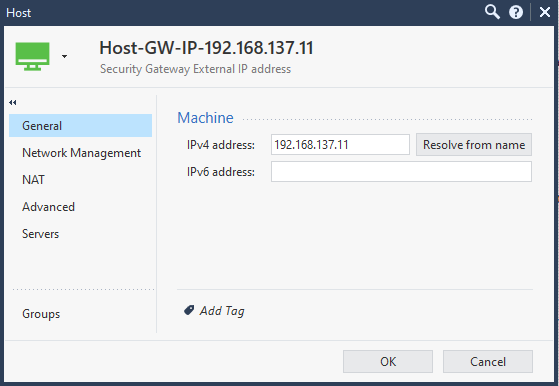
**Scenario:** Allow outbound internet access for an internal network ‘192.168.70.0/24’ using Manual Hide NAT functionality.

**Task:** Setup Manual NAT for an internal network ‘192.168.70.0/24’ using Security Gateway IP address.

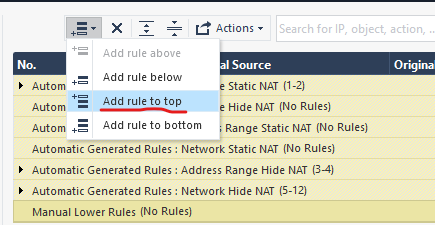
Once manual NAT rules are created in the NAT policy, initiate some traffic from the source machine in the 192.168.70.0/24 network and see relevant logs.

**Solution:** Please perform these steps to configure Manual Hide NAT for the network: -

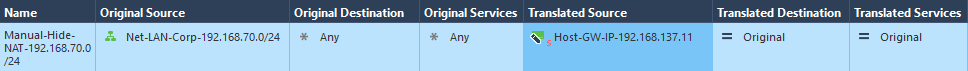
1. Login into SmartConsole R81.10 GUI client.
2. Check if the network object for the network – 192.168.70.0/24, and if it does not exist, please create a network object.
3. As we need to do a Manual NAT now, so you should have an object for the external IP address of the Security Gateway as well. Please create a host object for the IP address – 192.168.137.11. This is how this object should look like: -



1. Go to NAT Policy under Security Policy Menu.
2. Hover your mouse over the Add Rule menu, and click on ‘Add rule to top’. Refer to the screenshot below: -



1. Create a manual NAT rule as per configuration items below: -
   1. Name: Manual-Hide-NAT-Network
   2. Original Source: select the network object for the network – 192.168.70.0/24
   3. Original Destination: \*Any
   4. Original Service: \* Any
   5. Translated Source: select the host object for the Gateway external IP address – 192.168.137.11
   6. Translated Destination: leave it as ‘Original’
   7. Translated Service: Leave it as ‘Original’
2. This is how the newly created manual NAT rule should look like. Refer to the screenshot below: -



1. Ensure that there exists a firewall rule to allow internet access to the network - 192.168.70.0/24.
2. Install the policy.

**Connectivity Testing:** please perform these steps to do connectivity testing: -

1. Login into CLI mode in ‘Server1’ VM and check it’s IP address. It should have an IP address – 192.168.70.50
2. and try to ping the Global DNS Server IP address – 4.2.2.2. This ping test should work. See screenshot below: -
3. Open the Web Browser in the ‘server1’ VM and access <https://www.google.com>. This site should be accessible.

**Check relevant Logs:**

Now, we will check relevant logs to see if the original source IP address has been translated to the Security Gateway IP address or not.

1. Click on ‘Logs & Monitor’ menu
2. Type following query in the address bar - ‘dst:4.2.2.2 AND service:icmp-proto’. You will see log entries. Refer to the screenshot below: -
3. Paste a recent image here.
4. Now, double click on the first log entry, and investigate the NAT section. You will see that the translated source IP address is – 192.168.137.11. You can also the NAT rule number processed to do the source address translation. This should be processed by the NAT Rule # 1. Refer to the screenshot below: -
5. Paste the recent image here.
6. With this we have successfully completed this use case.

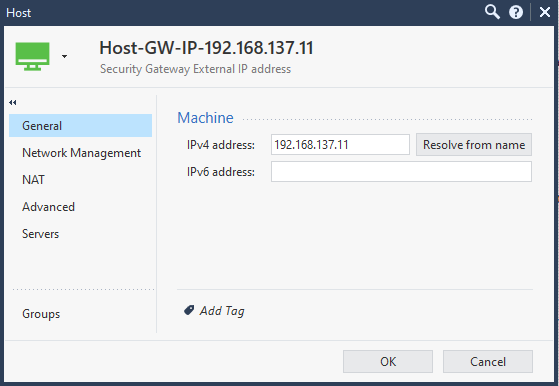
Use Case # 13 – Manual Hide NAT on the Host Object for using Other IP

**Scenario:** Allow outbound internet access for an internal server ‘192.168.70.50’ using Manual Hide NAT.

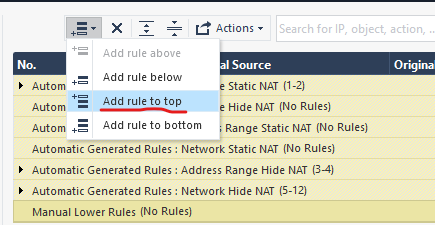
**Task:** Setup Manual Hide NAT for an internal server 192.168.70.50 using Other IP address than the Gateway IP. Use IP address 192.168.137.50 as a NAT IP address.

**Solution:** Please perform these steps to configure Manual Hide NAT for a Server: -

1. Check if the network object for the Server – 192.168.70.50, and if it does not exist, please create a Host object.
2. As we need to do a Manual NAT now, you should have an object for the other NAT IP address as well. Please create a host object for the IP address – 192.168.137.50. This is how this object should look like: -



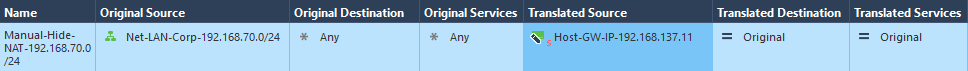
1. Go to NAT Policy under Security Policy Menu.
2. Hover your mouse over the Add Rule menu, and click on ‘Add rule to top’. Refer to the screenshot below: -



5. Create a manual NAT rule as per configuration items below: -

* 1. Name: Manual-Hide-NAT-for-Server
  2. Original Source: select the host object for the server – 192.168.70.50
  3. Original Destination: \*Any
  4. Original Service: \* Any
  5. Translated Source: select the host object for the NAT IP address – 192.168.137.50
  6. Translated Destination: leave it as ‘Original’
  7. Translated Service: Leave it as ‘Original’

1. This is how the newly created manual NAT rule should look like. Refer to the screenshot below: -



1. Ensure that there exists a firewall rule to allow internet access to the network - 192.168.70.0/24.
2. Install the policy.

**Connectivity Testing:** please perform these steps to do connectivity testing: -

1. Login into CLI mode in ‘Server1’ VM and check it’s IP address. It should have an IP address – 192.168.70.50
2. and try to ping the Global DNS Server IP address – 4.2.2.2. This ping test should work. See screenshot below: -
3. Open the Web Browser in the ‘server1’ VM and access <https://www.google.com>. This site should be accessible.

**Check relevant Logs:**

Now, we will check relevant logs to see if the original source IP address has been translated to the Security Gateway IP address or not.

1. Click on ‘Logs & Monitor’ menu
2. Type following query in the address bar - ‘dst:4.2.2.2 AND service:icmp-proto’. You will see log entries. Refer to the screenshot below: -

Paste a recent image here.

1. Now, double click on the first log entry, and investigate the NAT section. You will see that the translated source IP address is – 192.168.137.50 instead of 192.168.137.11 as per our previous lab. You can also process the NAT rule number to do the source address translation as well. This should be processed by the NAT Rule # 1. Refer to the screenshot below: -

Paste the recent image here.

1. With this we have successfully completed this use case.

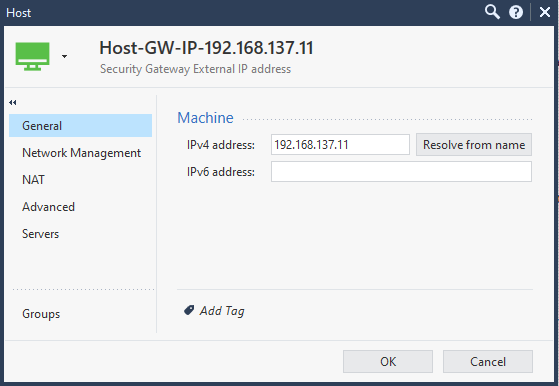
Use Case # 14 – Manual Static NAT on the Host Object with the Firewall Rule.

**Scenario:** Allow outbound internet access for an internal server ‘192.168.70.50’ using Manual Hide NAT.

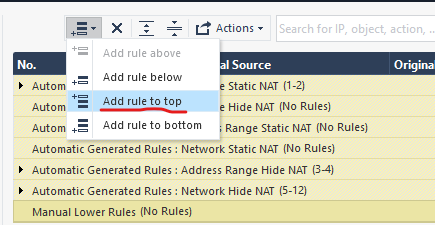
**Task:** Setup Manual Hide NAT for an internal server 192.168.70.50 using Other IP address than the Gateway IP. Use IP address 192.168.137.50 as a NAT IP address.

**Solution:** Please perform these steps to configure Manual Hide NAT for a Server: -

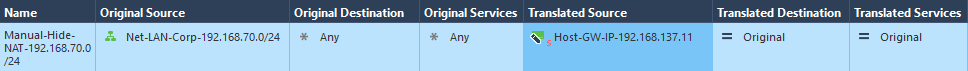
1. Check if the network object for the Server – 192.168.70.50, and if it does not exist, please create a Host object.
2. As we need to do a Manual NAT now, you should have an object for the other NAT IP address as well. Please create a host object for the IP address – 192.168.137.50. This is how this object should look like: -



1. Go to NAT Policy under Security Policy Menu.
2. Hover your mouse over the Add Rule menu, and click on ‘Add rule to top’. Refer to the screenshot below: -



1. Create a manual NAT rule as per configuration items below: -
   1. Name: Manual-Hide-NAT-for-Server
   2. Original Source: select the host object for the server – 192.168.70.50
   3. Original Destination: \*Any
   4. Original Service: \* Any
   5. Translated Source: select the host object for the NAT IP address – 192.168.137.50
   6. Translated Destination: leave it as ‘Original’
   7. Translated Service: Leave it as ‘Original’
2. This is how the newly created manual NAT rule should look like. Refer to the screenshot below: -



1. Ensure that there exists a firewall rule to allow internet access to the network - 192.168.70.0/24.
2. Install the policy.

**Connectivity Testing:** please perform these steps to do connectivity testing: -

1. Login into CLI mode in ‘Server1’ VM and check it’s IP address. It should have an IP address – 192.168.70.50
2. and try to ping the Global DNS Server IP address – 4.2.2.2. This ping test should work. See screenshot below: -
3. Open the Web Browser in the ‘server1’ VM and access <https://www.google.com>. This site should be accessible.

**Check relevant Logs:**

Now, we will check relevant logs to see if the original source IP address has been translated to the Security Gateway IP address or not.

1. Click on ‘Logs & Monitor’ menu
2. Type following query in the address bar - ‘dst:4.2.2.2 AND service:icmp-proto’. You will see log entries. Refer to the screenshot below: -

Paste a recent image here.

1. Now, double click on the first log entry, and investigate the NAT section. You will see that the translated source IP address is – 192.168.137.50 instead of 192.168.137.11 as per our previous lab. You can also process the NAT rule number to do the source address translation as well. This should be processed by the NAT Rule # 1. Refer to the screenshot below: -

Paste the recent image here.

1. With this we have successfully completed this use case.