Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Implementing NAT on Checkpoint Firewall-1

Network Address Translation is an important functionality of any firewall or security device. Understanding and implementing secure NAT rules and policies and excellent documentation on network topologies is a must. Until IP V6 has been fully developed and implemented, NAT will continue to be an integral part in any Internet Gateway security policy.

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

Implementing NAT on Checkpoint Firewall-1

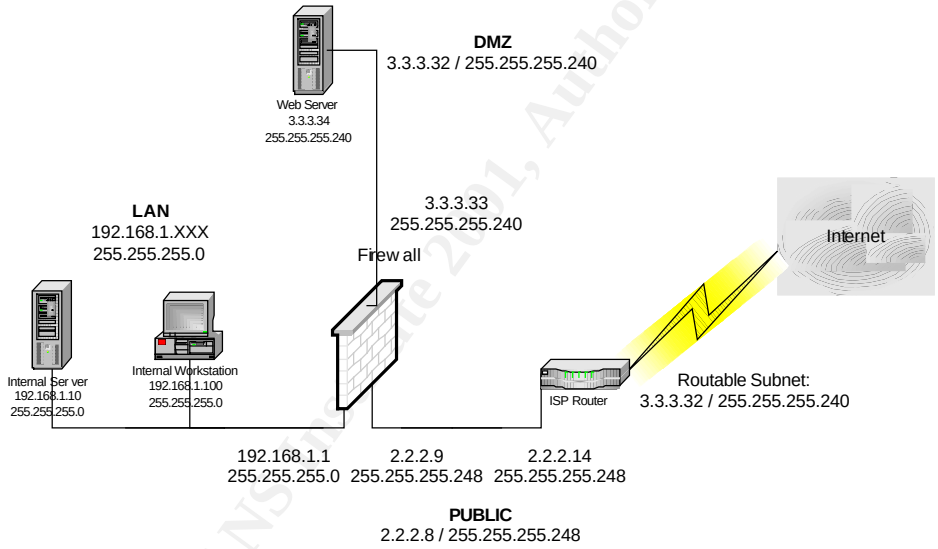
Network Address Translation:

Network Address Translation, or NAT as commonly referred to, was initially designed as a temporary fix, before IPv6, to allow additional workstations to access routable networks across the Internet, without utilizing a routable, or valid IP address. NAT is simply defined as connecting multiple computers to the Internet, using one IP address. Today, a multitude of proxies, firewalls, VPN devices, routers and SOHO devices now use NAT to allow internal hosts to the Internet. This document will examine how NAT is implemented, specifically on Checkpoint Firewall-1 4.1 for Windows NT 4.0.

Static, and Hide Mode:

There are two main types of NAT - static, and hide. Checkpoint Firewall 4.1 supports both of these. Let's first define our parameters for the discussion:

Network Diagram:



Internal server: Mail server on the "Inside" of the firewall, with an unroutable, private IP address of 192.168.1.10 / 255.255.255.0

Internal Workstation: PC on the "Inside" of the firewall, with an unroutable, private IP address of 192.168.1.100 / 255.255.255.0

Web Server: Web server accessible by both INTERNAL LAN and Internet, routable IP address of 3.3.3.34

ISP Router: Routable IP address on the Ethernet segment, with a public IP address of 2.2.2.6 / 255.255.255.252

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Firewall: Checkpoint Firewall with external Ethernet interface of 2.2.2.9 / 255.255.255.248. Internal Ethernet interface of 192.168.1.1 / 255.255.255.0. DMZ interface of 3.3.3.33 / 255.255.255.240

DMZ: De-militarized zone, semi-secure network segment where web servers, and other Internet accessible devices are placed. Routable network segment of 3.3.3.32 / 255.255.255.240 (useable range 3.3.3.33 – 3.3.3.46)

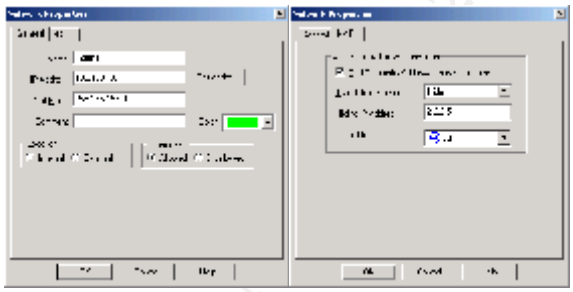
Routable IP subnet: Routable block of IP addresses as provided by the ISP, routed to our firewall, which will be used for our DMZ. In this example, 3.3.3.32 / 255.255.255.224 (useable range 3.3.3.33 – 3.3.3.62)

Hide NAT:

Hide mode of NAT is the easiest implementation of NAT on Checkpoint Firewall. As defined in the firewall software it self, Hide Translation is as follows: "Several invalid addresses are translated into a single valid address and dynamically assigned port numbers are used to distinguish between the invalid addresses." We can define hide mode NAT for the majority of our Internal users. This will give them access to the majority of the protocols they will use on the Internet, HTTP, HTTPS, FTP, POP3, DNS etc.

To define Hide Translation is quite straight forward:

1. Define your Internal Networks:



2. Click on the NAT tab, check Add Automatic Address Translation Rules (can also be defined manually) Enter the hiding IP address, this is the IP address that Checkpoint will use to substitute the Internal IP with its external IP address of the external interface.

3. When we return to the Address Translation Tab, we have a rule which is automatically created for us by Checkpoint. It is defined as follows:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Original Packet			Translated Packet		
Source	Destination	Service	Source	Destination	Service
Internal	Internal	Any	= Original	= Original	= Original
Internal	Any	Any	Internal (Hiding Address)	= Original	= Original

The rule base is read as follows. The first line states that traffic destined from our Internal network to our Internal network, leave the Translated Source packet IP address as original, or unchanged. The second rule states that any traffic from Internal to ANY, or in our case the Internet, the translated packet should be changed to our Hiding Address which we defined above.

For the case of Hiding IP addresses using the external Ethernet interface of the firewall, there is no additional routing requirement. If you use a different IP address to NAT, the same requirements for routing or arp with static translation take effect. These two methods will be discussed below.

Static Translation:

Static IP address translation is exactly what it means, it takes a single unroutable private IP address and statically assigns a routable IP address each time the device accesses the Internet. Static IP address translation would be used for web servers, e-mail servers or DNS servers, video conferencing software, or VPN client, etc, or any device which requires a unique statically mapped IP address. Checkpoint defines static translation as follows: Static - Each invalid address is translated to a corresponding static address.

Static Address Translation requires again, the definition of our network objects, a static translation address as well as either a routing table change or an arp table entry modification. Both of these methods will be discussed.

Defining our requirements:

Again referring to our previous diagram, we will require to statically NAT the Internal Server in order to receive SMTP e-mail messages from the Internet. (Please note that Checkpoint has a secure SMTP proxy / relaying feature which does not require the mail server to be directly connected to the Internet, however for the purposes of this document, we will not use the SMTP Security Server) In order to allow inbound connections for SMTP, TCP port 25, we will need to have a routable IP address assigned to our mail server.

Again, the steps for setting up the address translation will be identical to those defined during hide mode. We will set up the network object, in this case it will be a single IP address, or a workstation, with an IP address of 192.168.1.10. We will then click on the NAT tab of the workstation and select Static, then with a hiding entry of 2.2.2.10

Routing requirements:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Due to the implementation of NAT, in order for Checkpoint to correctly route the packets to the final destination (internal server), the routable valid IP address must be routed to the firewall. This route must be placed on the ISP router at the customer premise. Without this route, static NAT will NOT operate properly.

ARP:

In some instances, ISP's or service providers are unwilling or unable to add a static route to the router, during these circumstances, Checkpoint provides a way to route IP addresses to itself using a technique known as proxy arp, and these entries are located in a file called local.arp.

ARP or address resolution protocol is used to map MAC addresses of machine on the local network to an IP address. In our example, the firewall will need to announce to devices on the external network segment that it is the primary device for responding to a specific IP address.

Again, in our example above, the routable segment between the ISP router and our firewall is 2.2.2.8 / 255.255.255.248 (valid IP's from 2.2.2.9 – 2.2.2.14) Under ordinary conditions, in order to use one of those IP addresses, a device must be plugged into that network segment and follow the IP addressing and information (i.e. gateway etc) for that particular subnet. In our scenario, we would like to use the IP address of 2.2.2.10 for our e-mail server. This will require an entry in our Windows NT Checkpoint Firewall. The file to modify can be found under C:\WINNT\FW1\4.1\STATE\local.arp. The format of this file is as follows:

IP address MAC Address

2.2.2.10 08-00-20-76-ea-77

Once we have defined the IP address we wish to use, and entered the MAC address of the external Ethernet interface of our firewall, we need to re-install our firewall policy. This will allow any packets destined for 2.2.2.10 to be "routed" to our firewall. The router sees that the firewall's MAC address is listening for packets with IP addresses of both 2.2.2.10 and 2.2.2.9.

Routing Table Entries:

Once the IP addresses have successfully been routed to the firewall, a final change must be made on the firewall itself. A static route will need to be added to pass the request onto an internal IP address. In our example, the static route will be:

Route add 2.2.2.10 MASK 255.255.255.255 192.168.1.10 –p

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The –p states that the route will become persistent and will remain in the routing table even after rebooted. If you try to initiate traffic from the internal mail server, the ISP router will become aware of the new arp entry.

NAT with a third Ethernet Interface – DMZ

Up until this point, the DMZ has remained simply a routable Ethernet segment off of the firewall. No special routing has been configured, except for the static route which resides on the ISP's router.

Once packets have reached the firewall, they are routed through the appropriate third interface.

However, NAT must also be performed, between the Internal and DMZ network segments. For example, from my web server, I need to map a drive, or ftp new software updates from an Internal server or workstation. In order to maintain addressing and your sanity, you probably would want to map drives from and to your DMZ using the IP addressing scheme defined. For example, if you wanted to map a drive from your internal workstation to the DMZ, then you would use the command net use g: \\3.3.3.8\inetpub; or from your web server, to map a drive to your internal program disk, \\192.168.1.10\programdsk.

In order to maintain IP addressing consistency between these two networks, we will discuss how to manually edit the Network Address Translation tabs within Checkpoint. By default, if you select Automatically Generate Address Translation Tables, as our hide translation above, Checkpoint will define address translation rule sets for you automatically. If we take our example with hide translation, an internal workstation which accesses our web server in the DMZ, would have their source address translated to their hide address. If a DMZ server required access to the specific workstation, then you would need to add a static translation rule for an internal host each time. Thank goodness for manual NAT entries. We take our example from above:

Original Packet			Translated Packet		
Source	Destination	Service	Source	Destination	Service
Internal	Internal	Any	= Original	= Original	= Original
Internal	Any	Any	Internal (Hiding Address)	= Original	= Original

In order to perform manual NAT, we will need to add a rule before the automatically generated one by Checkpoint. Order here is important, as Checkpoint begins from the top rule down. Therefore, if an object meets a certain criteria on rule 1, and it is also defined in rule 10, rule 1 will be implemented.

In order to define a manual NAT entry, we first need to go into the Address Translation Tab of our policy editor. Again, we will need to add our entry before the automatically translated rule set:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Our new rule will be as follows:

Original Packet			Translated Packet		
Source	Destination	Service	Source	Destination	Service
Internal	DMZ	Any	= Original	= Original	= Original

This rule defines that any traffic from the Internal Network to the DMZ, with any service, keep the source translated packet as the original IP address. A second rule could also be generated to allow traffic from the DMZ to the Internal Network to keep their translated packets as the original IP address.

Please note that a rule to allow traffic between the DMZ and the Internal network may be described as a security risk. Since devices on the DMZ are accessible via the Internet, should a host be compromised, no traffic should be allowed from the DMZ to the LAN. However for the purposes of this document, we have accepted these security issues to focus on technical explanation of NAT.

Conclusion:

Network Address Translation is an important functionality of any firewall or security device. Understanding and implementing secure NAT rules and policies and excellent documentation on network topologies is a must. Until IP V6 has been fully developed and implemented, NAT will continue to be an integral part in any Internet Gateway security policy.

Resources:

Fairhurst, Gary. "Address Resolution Protocol (ARP)." Jan 2001 URL: http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html (8 Aug. 2001)

Egevang, K. "The IP Network Address Translator (NAT)." May 1994 URL: http://www.ietf.org/rfc/rfc1631.txt (15 Aug. 2001)

Hasenstein, Michael "IP Address Network Translation." 1997 URL: http://www.suse.de/~mha/linux-ip-nat/diplom/nat.html (14 Aug. 2001)

Welch, Dameon. "Routing and ARP issues with NAT" December 1999 URL: http://www.phoneboy.com/faq/0006.html (12 Aug. 2001)

Welch, Dameon. "Proxy ARP's in Windows NT" December 1999 URL: http://www.phoneboy.com/faq/0008.html (12 Aug. 2001)

Dallas Courseware Development. Checkpoint Security Courseware – VPN-1 / Firewall-1 Management II Student Guide Checkpoint 2000 Edition

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced