LEVERAGING NETWORK ADDRESS TRANSLATION FOR ENHANCED LOCAL NETWORK SECURITY

Horiainova K.O.[1], Kapusta R.D.[2]
1. V.V. Popovskyy Department of Infocommunication Engineering, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine, Nauky Ave. 14, E-mail: karyna.horiainova@nure.ua

2. V.V. Popovskyy Department of Infocommunication Engineering, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine, Nauky Ave. 14, E-mail: roman.kapusta@nure.ua

Коротка анотація – Розглянуто та досліджено принцип роботи Network Address Translation (NAT) для забезпечення безпеки локальних мереж. Описано переваги та недоліки NAT з погляду безпеки, запропоновано методи захисту від атак із зовнішньої мережі та описано експеримент із використанням програми "pwnat" для демонстрації роботи NAT на операційній системі KaliLinux.

Keywords – NAT, cybersecurity, protection, pwnat, local network.

Introduction

In today's networking world, effectively managing IP address space and securing local networks are key challenges for organizations and Internet Service Providers (ISPs). NAT (Network Address Translation) works by changing the headers of a data packet containing the source/destination IP address and port. This process allows multiple devices on an internal LAN to use a single public IP address to access the Internet, which saves public IP addresses and increases the security of user data that uses the network [1].

I. THE PRINCIPLES OF NAT

The main purpose of NAT is to change the headers of the data packet containing the source/destination IP address and port. Table 1 presents the main steps describing the NAT operation principle.

TABLE 1

Main steps describing NAT operation

№	Key steps	Description
1	Private IP address	When a device on your local network sends data to the Internet, it uses a private IP address that is not recognized on the external network.
2	Address translation	The NAT in your router converts this private IP address into a public IP address that can be recognized on the Internet.
3	Sending data	The data is then sent to the Internet with this public IP address.
4	Incoming data	When data is returned, NAT converts the public IP address back to a private IP address and forwards the data to the appropriate device.

II. NAT Type: PAT

In NAT technology, there are three primary types. Consider the types of NAT using the example shown in Fig. 1.

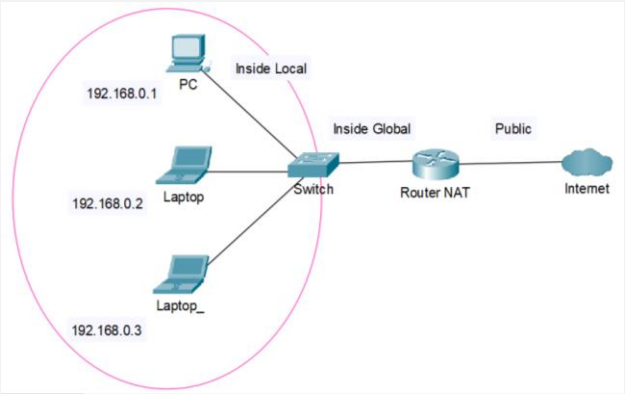

Fig. 1. Network topology

PAT (NAT overload) is a variant of dynamic NAT that maps multiple private IP addresses to a single public IP address using Port Address Translation technology. In PAT, when a client on the internal network communicates with an Internet host, the router alters the source port (TCP or UDP) to a different port number. These port mappings are recorded in a table. Upon receiving data from the Internet, the router accesses this table containing the port mappings and forwards the data packet to the original sender. The IP address calculation process is depicted in Table 2.

TABLE 2

Calculation of PAT IP addresses

NAT Translation			
Type	Inside Local IP:Port	Inside Global IP:Port	Public IPs
Many to Many with Ports	192.168.0.1:23	200.200.200.1:23	200.200.200.1
	192.168.0.2:25	200.200.200.1:25	
	192.168.0.3:47	200.200.200.1:47	

III. NAT security

NAT security is an important consideration when using Network Address Translation. Let us consider the advantages and disadvantages of NAT technology from a security point of view.

NAT offers several benefits, such as internal address hiding, which conceals internal IP addresses from external networks, and enhancing security by preventing direct access to internal hosts. It also restricts external hosts' direct access to internal devices, bolstering security. Additionally, NAT serves as a simplified firewall, helping to detect and prevent outside attacks like port scanning or service attacks. However, NAT introduces challenges such as difficulties configuring security policies due to port and address changes and tracking issues in identifying devices. Considering these factors is essential when implementing NAT in network settings, and proper configuration is crucial for maintaining network security.

Methods to protect against attacks from outside the network must also be applied. When using strict NAT, internal IP addresses are translated into one or more static external IP addresses. This allows connections passing through NAT to be identified and monitored. To protect the network against attacks from outside, the following methods are also recommended [2]: use of IDS/IPs systems; data encryption; use of effective antivirus and traffic scanners; use of software or hardware firewall; installation of rootkit blockers and sniffers.

IV. NAT operation using "pwnat" demonstration

To demonstrate how NAT works, an experiment with building a working connection between a client and a server was conducted. Here, PAT (NAT overload) was a type of dynamic NAT. For this purpose, we used the KaliLinux (version kali-linux-2023.4-virtualbox-amd64) operating system and the "pwnat" software tool, which implements NAT through a virtual machine, tunneling TCP data through UDP. This tool can act as a server or a client. The server listens on a UDP port and creates a connection to a TCP server at the client's request. The client receives TCP data and sends it to the UDP server, which forwards it to the established TCP connection with the specified TCP server [3]. The scheme of the experiment is shown in Fig. 2.

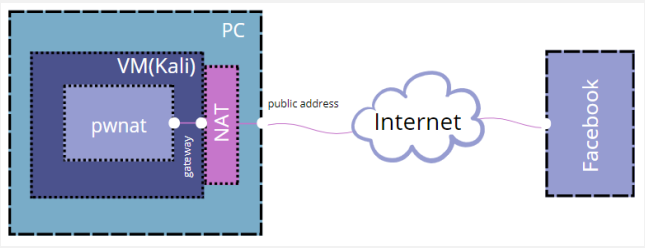

Fig. 2 Experiment scheme.

"pwnat" is the foundational tool for implementing this experiment. It allows a client behind a NAT to communicate with a server behind a separate NAT, without the need for port forwarding or DMZ configuration on routers. Also, no intermediaries, proxies, or UPnP are required, and there is no need for spoofing or DNS tricks. The server does not need to know the client's IP address in advance, and the client can connect to any host or port on the remote host or to a fixed host and port defined by the server. It is a proxy server that works effectively behind NAT, even if the client is also behind NAT.

On the server side, allowing any proxy:

./pwnat –s 10.0.2.15

Client wants to connect to facebook.com 40:

./pwnat -c 4040 pwnat.server.com facebook.com40

The result of running the client and server on the virtual machine KaliLinux is shown in Fig. 3 and Fig. 4.

```
┌──(root㉿kali)-[~]
└─# pwnat -c 4040 127.0.0.1 facebook.com 40
Listening on TCP 0.0.0.0:4040
```

Fig. 3. Result of client startup.

```
root@kali: ~
File  Actions  Edit  View  Help
^Z
zsh: suspended  pwnat -s 10.0.2.15

┌──(root㉿kali)-[~]
└─# pwnat -s 10.0.2.15 8080
Listening on UDP 10.0.2.15:8080
Got packet from 127.0.0.1
Got connection request from 127.0.0.1
Got packet from 127.0.0.1
Got connection request from 127.0.0.1
```

Fig. 4. Result server startup.

To confirm the work of NAT, we use the tool Wireshark, which makes it possible to track the traffic transfer between the client and the server as shown in the Fig. 5. As a result, we see that the server also periodically sends ICMP echo requests to the address 3.3.3.3 (hard-coded IP).

No.	Time	Source	Destination	Protocol
81	155.898284815	10.0.2.15	3.3.3.3	ICMP
82	157.219262889	127.0.0.1	127.0.0.4	ICMP
83	157.224332368	127.0.0.1	127.0.0.1	UDP
84	160.971442235	10.0.2.15	3.3.3.3	ICMP

Fig. 5. Running the client and server and tracking traffic with Wireshark.

Conclusion

NAT is a key part of IP address management and network security. It hides internal addresses and restricts direct access from the outside. Another use of NAT is to prevent IP address overlap. This happens when different nodes with the same IP address try to access the same destination node. Also, NAT technology has been put into practice using "pwnat". The "pwnat" program, which implements a type of PAT (NAT overload), demonstrates the capabilities of NAT by allowing the client and server behind NAT to communicate without port forwarding. Wireshark confirmed the NAT effectiveness.

References

[1] “RFC 2663: IP Network Address Translator (NAT) Terminology and Considerations”. IETF Datatracker. Date of the call: 14 Mar. 2024. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc2663.

[2] “The Myth of Network Address Translation as Security”. F5, Inc. Date of the call: 14 Mar. 2024. [Online]. Available: https://www.f5.com/resources/white-papers/the-myth-of-network-address-translation-as-security.

[3] “GitHub - samyk/pwnat: The only tool/technique to punch holes through firewalls/NATs where multiple clients & server can be behind separate NATs without any 3rd party involvement. Date of the call: 14 Mar. 2024. [Online]. Available: https://github.com/samyk/pwnat