NAT(Network Address Translation) for Security

Pravin Shinde, Jaya Verma, Ruchika
Indian Institute of Technology, Patna

April 29, 2025

1 Introduction

Network Address Translation (NAT) is a process by which multiple devices on a private network can connect to the internet using a single public IP address. NAT is responsible for translating the IP address of every device connected to a router into a public IP address at the gateway so that those devices can connect to the internet.It is usually implemented on a network device, such as a router or a firewall at the boundary between a private network and the public internet.

"The network device, like a router, will have one interface in the local (private) network and one interface in the global (public) network. When a packet is sent outside the local network, the NAT converts the private IP address to a public IP address. When a packet enters the local network, the public IP address is converted back to a private IP address by referring to the NAT table. For this process, a translation table is maintained on the NAT device. This table contains a mapping between the private source IP address and the public IP address assigned by the NAT device.

It was originally introduced to address the problem of exhaustion of available IPv4 addresses, but it has some additional advantages, like enhancing the security of private networks by separating the internal network from the external network. External devices can only see the public IP address; they cannot see the individual IP addresses of the devices on the private network. This makes it difficult for attackers to target specific devices within the internal network because they would first need to determine the local IP address of the target device.

NAT is considered a security mechanism due to the understanding that the private addresses of internal hosts are hidden from the Internet. However, this perception has significant flaws. While NAT can complicate attacks like unsolicited port scans, it does not inspect or block malicious traffic. Therefore, it cannot be considered a substitute for a firewall.

NAT is often used in combination with firewalls, where NAT manages IP address translation and the firewall enforces traffic policies. However, this combination can lead to vulnerabilities if not configured properly.

Intrusion detection and prevention systems can increase security, but they face challenges when used in NAT environments. NAT hides the original IP addresses and ports, making the analysis and remediation of security issues more complicated. Solutions like NAT-aware IDS/IPS architectures with identification modules have been proposed to resolve these issues.

This paper explores the security implications of NAT. It aims to understand the actual security benefits of NAT, examine how it interacts with other security systems, and evaluate whether NAT alone can be considered a reliable security barrier

2 Background and Types of NAT

When the internet was first designed, most people connected to it through dial-up connections. During that era, each device or network was assigned a unique IP address from the IPv4 address space. An IPv4 address is 32 bits long, which means it can support up to 2^{32} unique IP addresses—approximately 4.3 billion. When the IPv4 standard was introduced in 1981, these number of addresses seemed more than sufficient, as the internet was primarily used by a limited number of institutions, researchers, and early adopters.

Also, with dial up connection, the user would connect for a short time and then they disconnect. When they disconnect, their IP address could be reassigned to someone else.

But when the number of internet connected devices grew rapidly, the 4.3 billion IP addresses from IPv4 which seemed huge at one time became insufficient. This led to development of many solutions. Out of which one was Network Address Translation (NAT).

2.1 How NAT operates in IP network

To solve the problem of limited addressing, Private IP addresses and NAT was designed. There are two different types of IPv4 addresses.

- Public IP addresses

- Private IP addresses

Public IP address addresses are publicly registered on the Internet. You must have a public IP address to access the internet. There are approximately 4 billion IP addresses available, which we found in our previous section that they are not sufficient.

Private IP addresses are different. They are not publicly registered. So you cannot directly access the internet with a private IP. Private IP addresses are used when we create a local network such as by setting up Wifi at home or creating a hotspot. Suppose that there is a person A who has shared his hotspot with person B. Now they have created a local network. Now Person A might get a private address 192.168.1.10 and person B might get private IP addresses like 192.168.1.11. This is the concept of private IP address. Private IP addresses are used in a home or business. They are not used on public internet . Router (if you are using wifi) is the one that assigns your internal devices a private IP addresses.

Now let's see where NAT will come into picture. Most home and business will have multiple devices that need access to the internet. So those devices need a public IP addresses.

Now when our device needs to access the internet, there IP address will be translated by NAT in router to the one public IP addresses that we have been given. This is what NAT does it translates a set of Ips addresses.Now just it translates private to public but it also translates public to private.

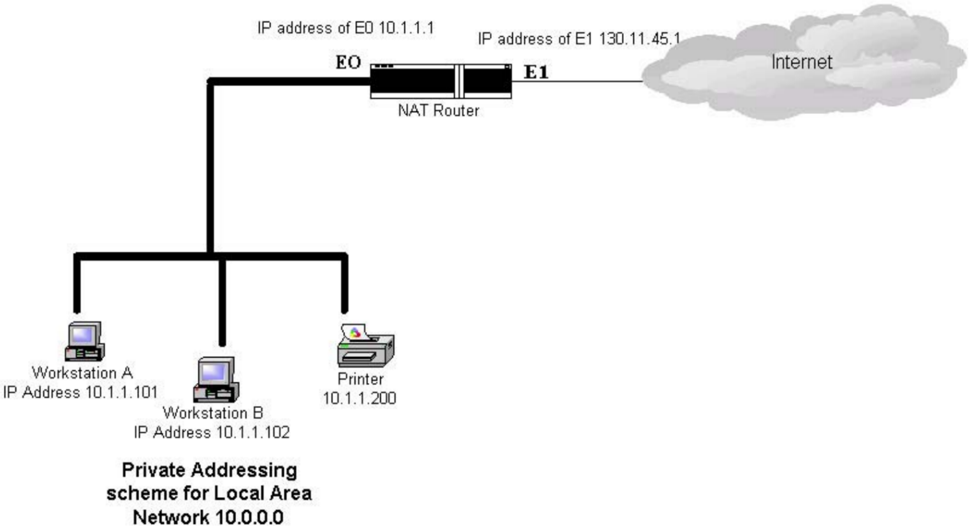

Figure 1: Network Address Translation (NAT)

For example, the above figure shows a NAT enabled router with a network address of 10.1.1.1. When any device from the internal LAN tries accessing the Internet, NAT will translate the private 10.0.0.0 addresses to 130.11.45.1. The internal devices can access any host on the external network. For the devices outside the internal network, it would appear that all inbound and outbound data are originating from a single IP address of 130.11.45.1.

2.2 Types of NAT

2.2.1 Static NAT

Static NAT is a NAT method where a private IP in a local network is permanently mapped to a specific public IP. It is a one to one mapping. Each private IP assigned to one public IP.

Device	Private IP	Public IP
Device 1	192.168.1.2	203.0.113.100
Device 2	192.168.1.3	203.0.113.101
Device 3	192.168.1.4	203.0.113.102

Table 1: Static NAT Example

Limitation of Static NAT: You need a unique public IP for each private IP in static NAT. For this reason, it can't be used in large network.

2.2.2 Dynamic NAT

Dynamic NAT is a type of NAT in which router is given a pool of public IPs. NAT uses these pool of IPs to convert private IP address to corresponding public address.

Let's imagine a scenario in which there are three Devices A, B ,C . The private IP of devices are as shown below in the table.

Device	Private IP
Device A	192.168.1.2
Device B	192.168.1.3
Device C	192.168.1.4

Table 2: Private IPs Assigned to Internal Devices

Pool of Public IPs
203.0.113.100
203.0.113.101

Table 3: Available Public IPs for NAT

Now suppose Device 1 want to access internet. Both of the Public IP from pool are free so any one can be assigned to it. Let's say 203.0.113.100 is assigned to it. Now B wants to access internet then public IP 203.0.113.101 can be assigned to it. Now let's say that C also want to connect to internet, Now there were only two public IP in the pool so now Device has to wait.

Device	Private IP	Public IP
Device A	192.168.1.2	203.0.113.100
Device B	192.168.1.3	203.0.113.101
Device C	192.168.1.4	*Wait*

Table 4: NAT table showing public IP assignments and waiting state

Now suppose Device B has finishes its task so the public IP 203.0.113.101 is free. So Now Device C can get public IP 203.0.113.101.

Device	Private IP	Public IP
Device A	192.168.1.2	203.0.113.100
Device C	192.168.1.4	203.0.113.101

Table 5: Updated NAT Table After Device B Disconnects

Now suppose Device A has finishes its task so 203.0.113.100 this is free. Device B again wants to connect to internet. Now 203.0.113.100 is free so the device B can get that IP.

Device	Private IP	Public IP
Device B	192.168.1.3	203.0.113.100
Device C	192.168.1.4	203.0.113.101

Table 6: Final NAT Table After Device B Reconnects

Note: Earlier device B got 203.0.113.101. Now it got 203.0.113.100.

Advantage of Dynamic NAT: Efficient use of public IP

Disadvantage of Dynamic NAT: Limited pool of public IPs

2.2.3 Portable NAT

Portable address translation is a type of NAT. It allows many devices on a local network to share a single public IP address by assigning each connection a unique port number.

Suppose device A (192.168.1.2) want to visit site example1.com and Device B (192.168.1.3) want to visit site example2.com. Suppose our router has only one public address 203.0.113.5. Then it will assign same public IP address to each site by using different port numbers.

Internal IP + Port	External IP + Port
192.168.1.2:5000	203.0.113.5:30001
192.168.1.3:5001	203.0.113.5:30002

Table 7: NAT Mapping of Internal Addresses to External Ports (PAT)

3 NAT and Network Security

3.1 NAT as a Security Barrier

One of the major security advantages of Network Address Translation (NAT) is that it can hide internal private IP addresses from external networks. It acts as a basic security barrier by preventing direct access to the internal devices from the public internet. Since multiple internal hosts share a single public IP address, it is difficult for external entities to initiate connections with the target host.

NAT can create an abstraction layer and increase the complexity for attackers. It is difficult for attackers to determine the structure or existence of internal hosts because private IP addresses of hosts is not directly routable over the internet. Attacks like port scan where a malicious user probes a system's IP address to find open ports and services can be prevented because scanner can only see the public IP address, not the private IPs of internal hosts. Therefore, the scan will not yield any useful information.

However, NAT only prevents direct addressing of internal hosts. It does not inspect packets for malicious content or detect attacks. Therefore, we cannot rely solely on NAT for security. It cannot be treated as a replacement for a firewall.

3.2 NAT in Conjunction with Firewalls

NAT and firewalls are usually implemented in a single device, like a router. NAT handles address translation when multiple devices on a private network share a single public IP address, while the firewall provides security by controlling network traffic and preventing unauthorized access. NAT can also act as a basic level of protection by hiding the internal IP addresses of devices on the private network.

The firewall rules can be configured to work with the NAT settings to enhance security. In such setups, NAT handles address translation while the firewall enforces policy rules on incoming and outgoing traffic. A combination of both of them can prevent unauthorized access, filter packets, and block known attacks. The firewall can monitor traffic patterns and utilize NAT's session table to inspect context and enforce security rules more effectively.

Conflicts can occur if NAT and firewalls are not tightly integrated. For example, NAT may modify packet headers in such a way that firewall rules become ineffective unless the firewall rules are explicitly designed by considering NAT translation.

4 NAT aware Intrusion Detection Systems

In networks protected by Intrusions Detection Systems (IDS) and Intrusions prevention Systems (IPS), working with NAT can be a problem because the host information like IP address and port number are hidden by NAT. If the IDS detects a suspicious incoming packet then the alert generated will contain the victim's public IP address. So the security operator will find it difficult to determine the real victim because all incoming packets will have the same destination IP address. Also, if the IDS detects a suspicious outgoing packet then the alerts will contain the attacker's public IP address. So the security operator will find it difficult to determine the real attacker because all the outgoing packets will contain the same public address as the source IP address. Another problem is that if we have an IDS deployed above and below the NAT then both systems will mention the same occurrence of attack with different victim and attacker's identifiers.

With IPS, there is a bigger problem. If the IPS considers an incoming packet to be malicious, it can block the traffic to the victim. But this action will cause denial of service to all the users in our private network because the IP address of the victim is same as all the other hosts. If the IPS considers an outgoing packet as malicious then it can block the attacker but this will block the whole network because all the outgoing packets have the same source IP address.

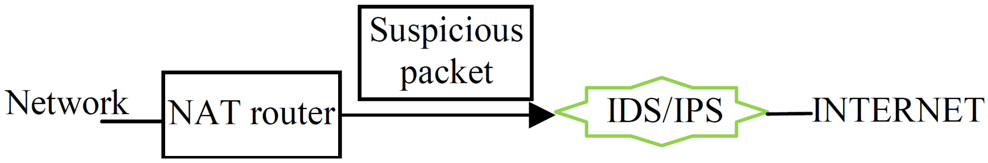

Figure 2: Suspicious Outgoing Packet

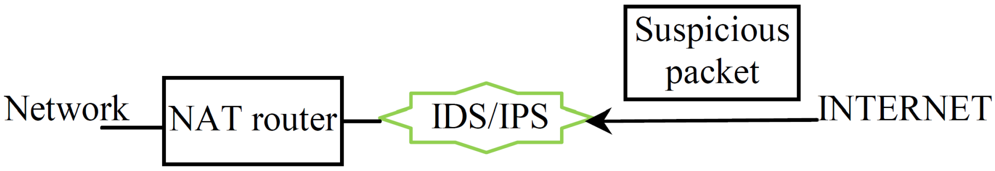

Figure 3: Suspicious Incoming Packet

For addressing these problems, we discuss the solution given by Meharouech et al. The authors suggest that in a local area network protected by IDS and IPS systems, the IDS/IPS deployed in the network should be aware that a NAT device that changes the packets headers is present. They propose a new architecture of IDS/IPS which uses the information in its analysis for correctly identifying the devices involved in security issues and takes the best decision. The networks with NAT, IDS or IPS deployed can be illustrated as in the below figure.

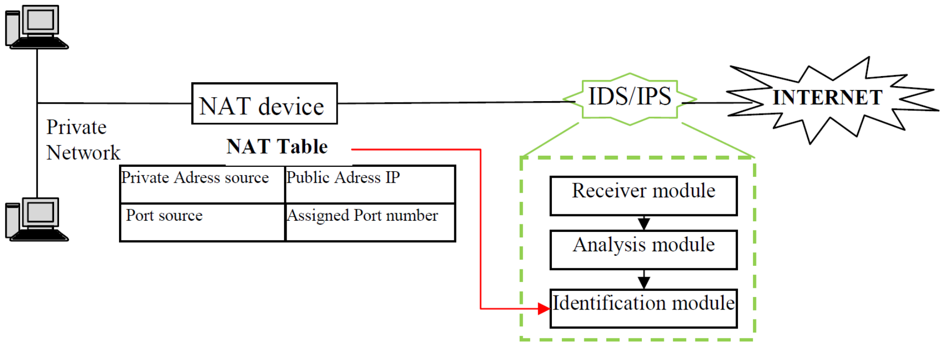

Figure 4: IDS/IPS architecture

The above figure also presents the proposed IDS/IPS architecture which consists of three components:

1. **Receiver Module** – collects network data and forwards traffic to the analysis module.

2. **Analysis Module** – analyses traffic to look for malicious or suspicious packets. The analysis module outputs an alert having four attributes: attacker, victim, attack and time. Below is a description of all the four fields.

   - *attack*: identifies the malicious action
   - *attacker*: identifies the entity source of attack
   - *victim*: destination of attack
   - *time*: determines when attack is detected

   This generated alert does not identify the real hosts involved in the security issue. Also, if there are two IDS/IPS systems, one deployed above the NAT and another below the NAT then both systems will refer to attacker and victim with different identities even if the alert is for the same attack. Both alerts will be considered as two different alarms which will increase the number of alerts and overwhelm the security operator.

   Due to this, we need to add another module in the IDS/IPS architecture.

3. **Identification Module** – the output of the analysis module is sent to this module. It determines the identities of the real hosts which are impacted by the security issue. After identifying the real hosts, the IDS sends an alert to the security operator with appropriate information, so that the operator can take the best decision.

   In case of IPS, active measures like blocking traffic or shutting down connections can be taken when a threat is detected. If the exact internal host is not known, a security system may

> blocking the entire internal or external network to be safe. Due to the Identification Module, the IPS knows that exactly which internal host is causing or is affected by the security incident. Therefore, the IPS can take action like blocking or isolating only on that specific host.

The authors propose that the identification module identifies the devices involved in sending or receiving suspicious traffic and also tracks the connections that were malicious.

The identification module process is based on two phases –

4.1 Initialization phase

The identification module builds a graph to discover the properties of hosts in the private network. It sorts all public IP addresses in a linked list. Each node in that linked list contains a public IP address and links to a set of connections containing the public IP address as source or destination.

This set is defined as an acyclic directed graph where each node represents a connection that is completely identified by the public address and the assigned port number. Since NAT changes ports for every new connection, each connection can be identified uniquely.

When a host initiates a connection, the identification module needs to create a new node and when the host ends a connection, the identification module should destroy the connection's node. This involves communication between the identification module and the NAT device.

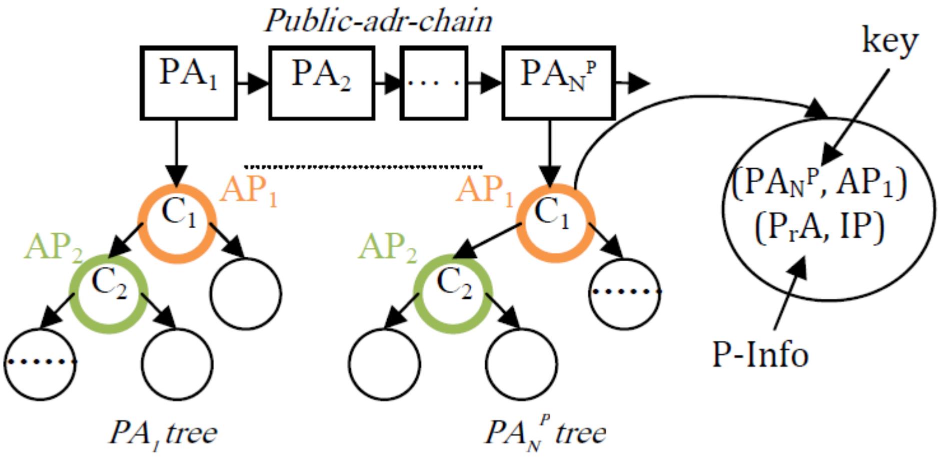

Figure 5: Graph created in Initialization phase

In the above figure, `Public-adr-chain` is a linked list containing public IP addresses. We assume that the number of available public addresses in a network is N^P. Therefore, the linked list may contain up to N^P nodes.

Each node of the linked list contains a public address PA_i, where $1 \leq i \leq N^P$.

PA_i `tree` is a directed acyclic graph (DAG) where each node represents a connection. A connection is uniquely identified by a public address PA_i and an assigned port number AP_k.

Assuming the number of available public addresses is N^P, the linked list may contain N^P nodes PA_i, where $1 \leq i \leq N^P$.

4.2 Operational phase

When an alert is generated by the analysis module, the identification module extracts the attacker and victim IP addresses and matches with the linked list of public addresses. Based on the port number it identifies the private host (attacker or victim) involved in the security issue. In case of IDS, the identification module will construct a new alert with the real values of address and port. In case of IPS, appropriate action can be taken against the real address and port.

5 Limitations of NAT

5.1 Impact on End-to-End Internet Communication

NAT changed the end-to-end communication model of the Internet architecture. Instead of allowing any host to directly talk to any other host on the Internet, all the hosts in a private network must go through the NAT device to reach others. Ongoing data exchange depends on the mapping entries at NAT device for translation. If the NAT device crashes, it could lose all the existing mappings and the data exchange between all the internal and external hosts will have to be restarted.

5.2 Security Implications

Although the original purpose of NAT was IP address conservation, it has increasingly been used as a security measure. It is important to understand the security risks associated with NAT devices especially in SOHO (Small Office/Home Office) networks because these networks usually use inexpensive solutions and the users may not have the expertise to determine risks or properly configure these devices.

NAT is often relied upon to be a security tool because all the transmissions appear to have come from a single public address but the internal private addresses could be included in some application headers. NAT can also make security deployments difficult due to the changes to the IP header and there could be difficulties in supporting VPN protocols.

NAT devices are now being configured to be peer-to-peer application friendly. They are no longer limited to routing and translation. A large number of NAT traversal mechanisms are being deployed with the goal of running contemporary applications seamlessly. This can degrade NAT device security.

Flaws in network device operating systems and translation behaviour may lead to greater security problems.

Hartpence et al conducted an experiment to answer the question about whether the private internal network is reachable without compromising the NAT device by taking advantage of the basic translation/routing behaviour.

A typical router will consult its routing table whenever it receives a packet. If the packet is destined for a network directly attached to the router, it is simply forwarded. However, if the destination is not on a directly attached network, or if it is unknown, then the router forwards the packet to either a next hop or its' own default gateway, similar to a host.

The author's supposition is that knowledge of the private network can be used to compromise the private address space. Once an external host or router is given a route to the private network through the outside interface of the NAT device, the NAT router would complete the routing. This conflicts with the understood behavior that the NAT device prevents all uninitiated traffic from the outside.

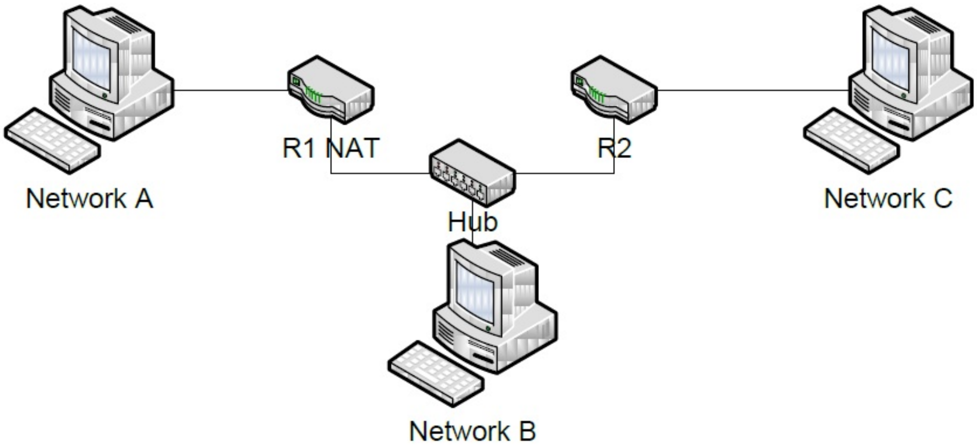

Figure 6: Experiment Topology

The author constructed the above experiment topology. There are three networks separated by a pair of routers. R1 is considered to be the edge of private network.

There are 3 networks: Network A (Internal), Network B (Middle), and Network C (External). R1 is directly connected to networks A and B. R2 is connecting B to external network C.

Goal is to test if hosts on Network C can reach hosts on Network A via routing configurations through R1 and R2. If an attacker can learn the internal network's address range (which is often predictable), then they can configure R2 to route traffic to Network A via R1's public interface.

Attackers can discover internal IP addresses using:

- Default configurations of many NAT devices, such as IP addressing, which are well known to the online community.

- Packet captures from public Wi-Fi or through wireless sniffing tools.

- Scanning tools like `Nmap` or `Nessus` to automate searches for potential targets or by pinging a range of addresses until successful.

There are a limited number of private addresses specified in the RFCs so the entire range can be tested.

Four configurations (physical and virtual) were used for testing.

Test	Scenario
1	Both R1 and R2 are Cisco 2621 routers. IOS version 12.3
2	R1 is a Linksys router, R2 is a Cisco 2621 router.
3	R1 is implemented using VMware's built-in NAT service. R2 is a VYATTA virtual machine running in VMware.
4	Both R1 and R2 are VYATTA virtual routers, R1 is configured with NAT.

Table 8: Test Scenarios for the Experiment

Only R1 runs NAT in each case.

Three test cases were run per scenario:

1. **Simple Routing (C to A)**: Configured R2 to route traffic from network C to A through R1's public IP.

2. **Default Routing (B to A)**: Host on B uses R1 as its default gateway and tries to reach A.

3. **ICMP Redirect (B to A)**: Host starts sending to A through R2, receives an ICMP redirect from R2 pointing to R1.

Below were the results:

- Cisco and VYATTA allowed traffic to pass through to internal hosts — NAT failed to protect in these cases.

- Linksys and VMware - NAT successfully blocked the unauthorized traffic and the internal network remained hidden.

Based on the author's experiment, we can conclude that NAT cannot be trusted to prevent external access. Understanding device behavior and configuration is important because some NAT devices perform routing before checking traffic origin. Simple routing knowledge can bypass NAT based protection if not properly configured.

6 Conclusion

While NAT offers some security benefits, it should never be considered a substitute for dedicated security mechanisms like firewalls, intrusion detection, or prevention systems. The integration of NAT with these technologies must be carefully designed to avoid conflicts and maximize protection. Ultimately, a deep understanding of NAT behavior and configuration is important for deploying secure and resilient network architectures

References

[1] Daryl Johnson and Bruce Hartpence, *A Re-examination of Network Address Translation Security*, Rochester Institute of Technology, 2010.

[2] Lixia Zhang, *A Retrospective View of Network Address Translation*, IEEE Network, University of California, Los Angeles, Sept/Oct 2008.

[3] Gregory D. Twitchell and Michael T. Frame, *Infrastructure of Electronic Information Management*.

[4] Sourour Meharouech, Adel Bouhoula, and Tarek Abbes, *Security Implications of Network Address Translation on Intrusion Detection and Prevention Systems*.