Rochester Institute of Technology
RIT Digital Institutional Repository

Presentations and other scholarship | Faculty & Staff Scholarship

2010

A Re-examination of network address translation security

Daryl Johnson

Bruce Hartpence

Follow this and additional works at: https://repository.rit.edu/other

Recommended Citation
Johnson, Daryl and Hartpence, Bruce, "A Re-examination of network address translation security" (2010). Accessed from
https://repository.rit.edu/other/761

This Conference Paper is brought to you for free and open access by the RIT Libraries. For more information, please contact repository@rit.edu.

A Re-examination of Network Address Translation Security

Bruce H. Hartpence and Daryl G. Johnson
Networking, Security and Systems Administration Department
Golisano College of Computing and Information Sciences
Rochester Institute of Technology
Rochester, NY, USA

Abstract - *The use of Network Address Translation (NAT) has greatly expanded in recent years. While originally an address management technique it has often been used for security. However, there are many implementations of NAT that are inherently insecure. Recently investigation into some of these has shown increased potential for security holes in NAT deployments. An understanding of the risks associated with NAT and the basic networking topics supporting a research in this area are critical to an information assurance student. This paper describes the basic operation of NAT, outlines one such security problem and its' mitigation, develops a testing methodology for use in information security curricula and suggests topics to be covered for student success.*

Keywords: Computer network security education, Address Translation, NAT

1 Introduction

With continued dependence on limited IPv4 addressing and the proliferation of network address translation (NAT) devices, it is important to understand the security risks associated with using these components in your network. This may be particularly true for SOHO environments that commonly deploy inexpensive solutions and users may not have the expertise to determine risks or properly configure these devices. It is just as important that information security/assurance curricula include a study of these vulnerabilities and the underlying networking concepts that facilitate a complete understanding of the situation. This paper will explain the basic operation of NAT, address some of these security issues, outline some of the experiments completed and offer methodologies for including these experiments in any curriculum. To make this available to the widest array of educational institutions, the test were done in both virtual and non-virtual environments.

2 What is NAT?

Translation is the process by which an internal, private address is converted to an external public address. Some or all of the traffic leaving the internal network will have the IP header of the packets modified before leaving the external interface of edge NAT device. This process is described in the original request for comments or RFC [1]. Associated with this document is RFC 1597 which describes private addressing. Three address ranges are removed from the public IP address space:

Table I
Private Address Ranges

Private Address Ranges
192.168.0.0/24
172.16.0.0 – 172.31.255.255/16
10.0.0.0/8 [2]

Note that the address space defined is extremely limited. While this RFC does not address NAT specifically, network address translators use these addresses for internal hosts. As transmissions are routed in the outbound direction, the source IP address from one of these address ranges is modified to be that of the outside interface of the NAT device. When using a single NAT device, this outside address will be part of the public address space of the Internet. Upon returning, the translation process is done in reverse. Critical to this process is the translation table maintained on the NAT device. This table maintains the mapping between the original inside source IP address and port to the outside address and port assigned by the NAT device.

It is important to realize that in addition to this translation, the NAT device is handling routing functions. In SOHO networks these devices are also known as home gateways. They can be deployed as stub networks or provide routing for larger topologies using routing protocols such as RIP.

2.1 The Problem

Though the RFCs indicate that NAT is an address management technique, it is often relied upon to be a security tool. This is because all of the internal private transmissions appear to have come from a single outside public address. Terms like "cloaking" are sometimes used. While it is true that the internal addresses are to some extent "invisible", RFC1631

points out several flaws (ex. addresses included in some application headers) in this assumption. In addition, NAT can also make security deployments difficult because of the changes to the IP header or trouble supporting VPN protocols. Running servers behind NAT routers may require ports to be opened up through the device. Nevertheless, we see the continued use of NAT devices for both purposes (address management and security) with the supposition that the internal network is protected.

A recent IEEE Network Magazine article points out that many are under the mistaken belief that device running NAT will suffice as an effective firewall. This is simply not true. Compounding these problems is the fact that because we have had so many changes to the applications run on a network, there have been a corresponding number of NAT traversal mechanisms deployed with the goal of running contemporary applications seamlessly. This has the very real potential of further degrading NAT device security. [2]

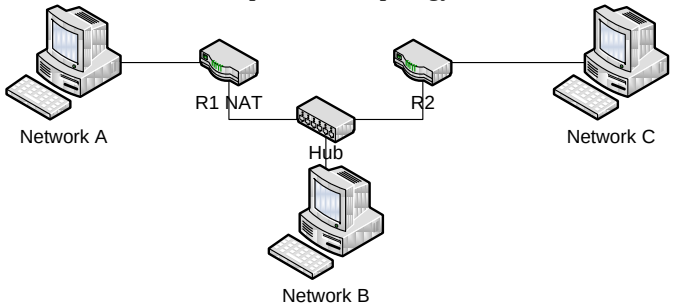
Many SOHO networks are entirely dependent on home class gateways such as CISCO/Linksys/NetGear routers to handle the routing and translation. With the increase in online gaming, social networking and file sharing, NAT boxes are being asked to do even more than just routing. No longer is it sufficient to provide port forwarding and port triggering; NAT boxes are now being configured to be peer-to-peer application friendly. This can serve to open up more holes to the internal network.

In addition to the RFCs' security concerns, flaws in network device operating systems and in basic translation behaviour may create greater security problems. We will outline one such problem and run a series of tests against an experimental topology seeking to circumvent the privacy allegedly afforded by the NAT device. The topology will be typical of many deployments and tested in both virtual and non-virtual environments. For the non-virtual tests we used Cisco and Linksys equipment. This will provide a representative sample for both SOHO and more advanced networking equipment. For the virtual tests we used VMware and a VMware virtual router called VYATTA. The configurations of these devices will be explained in the next couple of sections.

2.2 The Experiment

The basic topology depicted in figure 1 was constructed.

Figure 1
Experiment Topology



In this diagram there are three networks separated by a pair of routers. For the purposes of the test, we considered R1 to be the edge of the home or private network. This topology was built in order to test a particular vulnerability when running NAT and the premise that the network behind the NAT router is invisible. Our question: Can the internal network be reached by taking advantage of the basic translation/routing behaviour without compromising the NAT device itself?

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 out of the associated interface. However, if the destination is not on a network directly attached, 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.

Our supposition is that knowledge of the private, unadvertised network in use behind the NAT device could be used to compromise the private address space. Once a host or router on the outside was given a route to that private network via the outside interface of the NAT device, the NAT router would complete the routing without having to perform an attack on the device. This is contrary to the understood behavior of the NAT device preventing all uninitiated traffic from the outside.

2.3 Learning the Inside Network

For this experiment to work, we had to be able to configure R2 with information about the inside network; network A. So the question is, how do we get this information? The reality is that attackers do not have to work very hard to learn the address of the internal network. The default characteristics of many NAT devices (such as IP addressing) are well known to the online community. An example of this can be seen in [3]. In addition, any wireless network running behind the NAT device would potentially advertise these addresses making them available via simple packet capture or through the use of a program like NetStumbler. The wireless port is in the same layer 2 network as the wired nodes in a device like a Linksys gateway. Advertisements or traffic between the wireless node and the gateway will use the same network addressing as the wired

nodes. Scanning tools like Nmap and Nessus allow us to automate searches for potential targets and pinging a range of addresses until you are successful will also work. Finally, there are a limited number of private addresses specified in the RFCs and so the entire range can be tested.

The outside address of the NAT device is also able to be obtained via packet capture (depending on the network) or a fairly straight-forward scan of the network. Access is often simple as many companies provide network jacks in their common areas or conference rooms. Any organization providing free Wi-Fi is willing to allow a certain amount of access to their network as well. Once the gateway or outside interface of the NAT device is known, the attacker then adjusts the routing table of the next hop router – R2. Thus, this entire set of scenarios and tests described here could be accomplished via methods that are, or very nearly are, completely passive. These methods also require very little technical ability beyond an understanding of routing and NAT.

2.4 Routing in the Topology

The routing table of R1, Table 2, shows that it is directly connected to networks A and B, while R2 is directly connected to networks B and C. R1 is also running NAT. To complete the setup, R1 is given a default route to R2. This emulates a typical router configuration for a stub network.

Table II
Initial Routing Tables for R1 & R2

Router R1 (NAT)	Router R2
Connected: network A Connected: network B Gateway = R2	Connected: network B Connected: network C

In the case of a SOHO network, the outside interface (WAN port) is commonly a DHCP client and will obtain its' IP address and the address of the default router from the ISP network. This insulates the home user from having to know information about the ISP network when doing initial setup. Similarly, a router such as a Cisco 2621 acting as R1 must be given a default route to the next router. In this case, the 2621 is not usually a DHCP client.

2.5 The Scenarios

What follows is a discussion of the four separate scenarios run on this topology (in both physical and virtual environments) and our tests. Our four scenarios are as follows;

Table III
Test Scenarios Employed

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.

Note that in all cases, while both R1 and R2 are providing routing services, only R1 is running NAT. There were three different test cases run against each one of these scenarios;

Table IV
Test Case Descriptions

Test	Activity
1	Simple routing from network C to network A (R2 to R1)
2	Default routing from a host on network B (the host default route points to R1)
3	Redirection for a host on network B to network A via R2. The gateway for the host is R2.

These tests are different aspects of the same question: Will R1 forward traffic to network A when it receives a request on the outside interface even though the internal network is supposed to be invisible?

For test 1, the routing tables were manipulated as follows:

Table V
Test 1 Routing Tables for R1 & R2

Router R1 (NAT)	Router R2
Connected: network A Connected: network B Gateway = R2	Connected: network B Connected: network C Network A via R1

This modification tells R2 that in order to reach network A, it must send the traffic to the outside interface of R1.

In test 2, we do not actually have to know anything about the internal network. This is simply configuring an outside host to use the outside interface of R1 as its' default gateway. This is contrary to normal configuration because we typically want the default route to point in the direction of a majority of possible destinations.

Test 3 tests redirection. An ICMP redirect is generated when there is a better path to the destination than the one originally used. There are three requirements for a redirect; no source route information, the new forwarding router must be "reachable" by the source host and the original router must have to forward the message out of the same interface it came

in on. In this case, the router routing tables are modified as in test 1. The message flow starts as a request from a host on network B. The host sends this request to R2. R2 processes its' routing table and forwards the traffic back over to R1 and generates an ICMP redirect to the source host. From that point on, the host forwards traffic for the internal network (network A) to R1 only.

2.6 Configurations

The Cisco routers were running a basic form of NAT specifying the following; inside and outside interfaces, an ACL describing the inside network and a NAT statement telling the router to translate the inside network to the outside IP address. In this case, the purpose of the ACL was to indicate which addresses were to be translated. The pertinent lines of a configuration are included here;

Table VI
Cisco Configuration

```
interface f0/0
        ip address
ip nat inside
interface f0/1
        ip address
        ip nat outside
ip nat inside source list 1 interface f0/1 overload
        access-list 1 permit inside network
```

The Linksys router was using a default configuration, providing translation for outgoing traffic and acting as a DHCP server for the inside hosts. The Linksys was receiving the IP information for its' WAN connection from R2 which was acting as a DHCP server.

For scenarios 3 & 4, we downloaded VYATTA and Backtrack3 (a Linux Live distribution) virtual machines. We required three hosts, one for each network. After renaming Backtrack3 to INSIDE we created two linked clones and renamed them OUTSIDE and DISTANT. We also required two routers and so after renaming VYATTA to R1, we created a linked clone and renamed it R2. VMware's Player and Server are free making the cost of this exercise minimal.

The VMware NAT router is an included resource in the VMware line of virtualization products. It performs the NAT function between a virtual network (typically VMnet8) and the VMware host's outside network connection. The VMware host on which the virtual machines run also implements the virtual networks that interconnect the routes and hosts.

There are three types of network connections provided by VMware; Bridged to a physical NIC, NAT, and host only private network. Virtual machines can be connected to one or more of these networks. VMware gives us the ability, with very little hardware, to implement and experiment with complex network and host combinations that otherwise would be difficult and costly to create in a classroom or lab setting [4].

VYATTA is an open source router implemented on the Linux operating system which is also available as a VMware virtual machine. It can provide several network services such as DHCP, DNS, NTP and NAT as well as conventional routing between as many physical or virtual networks as are available. The VYATTA NAT solution is a layered service in much the same manner as the Cisco layered NAT facility [5]. It is enabled by a series of commands as detailed below;

Table VII
VYATTA Configuration

```
service {
   nat  {
      rule 1 {
         outbound-interface eth0
         source {
            address 192.168.112.0/24
         }
         Type masquerade
      }
   }
}
```

In all scenarios, packets captured on the outside interfaces (network B) revealed that the inside network addresses (network A) were in fact being translated. This means that all of the traffic generated on network A appears to have come from the outside interface of R1.

2.7 Methodology

For all three tests, we gave R2 a static route to R1 for network A. Once this was done, we simply pinged from host to host in the different networks. The program "ping" generates ICMP echo request packets. As proof that a test succeeded or failed we looked for both traffic on the target network and an indication via the command shell that an ICMP echo response was received. This ensured that a host (and not a router interface) was responding to the ICMP echo request.

2.8 The Results

In this section, a successful test is one in which the target was able to be pinged and proof that the response came from the intended target was obtained via packet capture. If there was no response, the test failed. The following matrix depicts the overall results. An "S" indicates success and an "F" indicates failure.

Table VIII
Results of Experiments

Scenarios	T1 C→A	T2 B→A	T3 Redirect
1 (Cisco)	S	S	S
2 (Linksys)	F	F	F
3 (VMware)	F	F	F
4 (VYATTA)	S	S	S

As can be seen, half of the tests resulted in successful pings to the internal "invisible" network hosts. Stated another way, half of all of the network devices did not protect/hide the internal devices. Both the Cisco router and the VYATTA virtual machine forwarded traffic to the internal network when asked to do so. Again, the RFC states that NAT should not be considered a security tool. Nonetheless, NAT is often placed in a security context. Examples can be seen on the Microsoft MSDN pages [6] and the Cisco FAQ pages about NAT [7]. Both of these devices can be given alternate configurations.

Once traffic was allowed to the network behind the NAT router, we were able to scan this network for additional security holes. This is because even though a scan or some other attempt at privilege escalation may be an attack, the routing for packets of this type is still handled in the exact same way. Once a host is identified as having security holes, it can be attacked directly.

2.9 Mitigation

Since this particular exploit is not an attack per se, but rather taking advantage of the default behaviour of the NAT devices, the mitigation is also straight-forward. By placing filters prohibiting uninitiated traffic, the simple routing of inbound traffic is blocked. Additionally, there are several different methods that can be used when configuring NAT. The method used above (overload) translates all internal addresses as a single external address, does not filter any traffic and does not check for stateful connections. So, other implementations & configurations of NAT such as pools or one-to-one mapping may provide increased (or decreased) security. Lastly, some devices appear to "route first, NAT second" rather than try to determine if a packet should be allowed. What is critical is that when deploying a NAT device you must understand how it is going to behave.

2.10 Educational Use

Academia is often hamstrung by a lack of hardware, funding and network resources, making it difficult to provide a hands-on experience. This experiment lends itself to a virtual environment allowing a single system to emulate a small networking lab.

In addition to NAT and security, this series of activities represents a collection of many basic networking concepts that are integral components to a small routed environment, both virtual and non-virtual. These include topics such as host and router based routing tables, route selection and the routing protocols. Basic network topics such as the address resolution protocol (ARP), Internet Control Message Protocol (ICMP), IP addressing, protocol models (TCP/IP), tools, traffic processing and the manipulation of header are key components to a background in networking and security. Students that completely understand these building blocks are well prepared for either a career in the communications industry or further research. Those that do not will have difficulty moving onward due to the fundamental nature of these ideas.

Topologies like the one depicted in figure 1 also allow students to explore some basic networking equipment and common exploits. Equally important to explore is the mitigation of the exploit. This gives them valuable insight into security problems seen in networks today and the associated solutions. In our program, security is a pervasive topic, appearing in almost every single one of our networking and systems administration classes. Student should learn that there are security problems in every aspect of our communication architecture. Experiments like those outlined here can better prepare them for their next step.

The use of virtual machines is a growing trend. Both server virtualization and virtual end nodes are growing trends. Educational programs can benefit because there is limited licensing and most of the virtual machines are open source.

3 Conclusions

The purpose of this paper is to re-examine the potential security risks associated with network address translation and to discuss its' importance in communications curricula. For these results, it is clear that many NAT devices or configurations are far from secure. The level of security is highly dependent on the configuration and the device. We believe that the vast proliferation of NAT devices and their ever increasing use justifies further investigation. Additionally, the work done by [8,9] indicates that peer to peer networking may serve to open even wider holes in what many assume to be a secure environment. The truth is that most consumers believe NAT to be inherently secure and this belief is supported by many technical articles. These problems make this re-examination even more important. As can be seen from the various scenarios and the tests outlined here, there are many implementations of NAT that are vulnerable to the most basic exploitation of simple routing. This has been demonstrated in both virtual and non-virtual environments.

In order to properly prepare students for industry or for research, a fundamental education of the networking concepts indicated in this paper is critical. A topology and experiments such as those outlined here will serve to provide this foundation. In addition, these experiments do not require vast

resources and in fact can be done with little or no funding making them affordable for all programs.

4 References

[1] RFC1631 - The IP Network Address Translator

[2] Zhang, Lixia, "A Retrospective View of Network Address Translation", IEEE Network, Sept/Oct 2008

[3] Default usernames, passwords and IPs, http://any-tips.blogspot.com/2008/01/linksys-router-username-pasword-and-ip.html

[4] VMWare Advanced NAT configuration http://www.vmware.com/support/ws55/doc/ws_net_nat_advanced.html

[5] VYATTA commands, http://vyatta.com/downloads/documentation/VC4.1/Vyatta_CommandRef_VC4.1_v03.pdf

[6] MSDN Network Address Translation, http://msdn.microsoft.com/en-us/library/aa916720.aspx

[7] Cisco NAT FAQ, http://www.cisco.com/en/US/tech/tk648/tk361/technologies_q_and_a_item09186a00800e523b.shtml#qa1

[8] A. Müller, A. Klenk, and G. Carle, "On the Applicability of Knowledge - Based NAT-Traversal for Future Home Networks," *Proc. IFIP Networking 2008*, Springer, Singapore, May 2008.

[9] RFC 5128 - The State of Peer-to-Peer (P2P) Communication across Network Address Translators (NATs)