

Re: Basic NAT / Firewall Question

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2006-08/msg00226.html>

- *From:* Christopher Stromblad <cs@xxxxxxxxxxxxx>
 - *Date:* Fri, 18 Aug 2006 23:01:09 +0100
-

Never apologize for asking questions, I don't :)

There are two basic types of NAT (Network Address Translation) which you need to understand.

1. NAPT (Network Address Port Translation) commonly referred to as simply NAT.
2. Static NAT.

NAPT simply maps port numbers to a given address. Take your OWA example, we are very likely talking about a port translation. The firewall has been instructed to forward all incoming connections on port 80 (and/or 443). This involves a step process:

1. A remote client decides to connect to your OWA server. A packet is sent your way.
 1. Your firewall will make a note from where the connection was originally coming (SRC address and SRC port) and then re-write the IP header and possibly the TCP/UDP header. It substitutes the SOURCE address and possibly the SRC port (where the connection was coming from) with its own address and then sends this "new" packet out on its local network interface. (The internal network for example).
 2. The OWA server will process the request, and reply back to, what it think, is a connecting client.
 3. When the OWA reply reaches the firewall it will remember that this packet was actually from another address and will now replace the old substituted details with the original data. Now however, they will be put as DESTINATION address and port.

So, when you do a portscan of your external IP it will be affected by the firewall yes. If the firewall was to take ALL network traffic and send it to the NATed address then we would talking about a static NAT.

So it really depends on which type of NAT you are using. Either all traffic go to a specific IP address (not entirely true, but that's besides the point in this example), or all traffic destined for a certain port will be forwarded to a given IP address.

So you are correct about your last assumption, you will only be scanning the 1 port. Well nmap will with default settings scan a few thousand

Re: Basic NAT / Firewall Question

specific ports, but only one port will respond, your OWA one. (Assuming no other ports are NATed.

At this late hour I'm not entirely sure if it's possible to figure out a way to determine if a server is NATed or not.

What you can do is something called TTL ramping. It might be somewhat complex to understand if you are just beginning to play around with networks. The IP header has a field call TTL which stands for Time To Live. For each hop your packets go through this value is decreased by one. It is used to prevent packets from getting into trouble, like endless routes et cetera, anyhow. What you do is you set this value to 1, and then you keep increasing it by one until you reach the external IP address. When you've got the correct value you construct a "real" packet and send it to the server. What will happen here however is the interesting part and might also be the part which makes this whole idea fail.

When the packet reaches the firewall it will check the TCP/UDP header for the DST port. Say this is 80, but the TTL value in your IP datagram is 0, the packet will not be able to reach its destination and the firewall will reply with an ICMP message of type 11 (Time Exceeded). But, if the DST port was 81, or anything else, and has nothing waiting on the other end, the firewall might simply drop the packet or reply back saying, connection refused.

So in this case, it would show that the firewall is actually NATing an address on port 80. If the firewall was blocking it would instead reply with a connection refused immediately.

Hope this helps, and mind you, I'm no expert so I might be wrong here ;)

// Christopher

thatch wrote:

forgive me if this question seems pretty basic but could anyone tell explain this to me.

i'm performing a practice assesment and i have located an IP of a web based mail server (OWA). this server is sitting behind a hardware firewall (say PIX or Checkpoint)that is NATing the IP Address to an internal non-routable address. Now, if i use a tool such as Nmap to scan that external IP are my scan results influenced by the Firewall. Do firewalls when NATing take all traffic from the external IP and pass it to the internal network and expect the server to have the remainig services closed down or do they only take traffic destined for a port and drop everything else. if it's the later, when i scan am i only scanning the 1 port that is allowing traffic to be forward to it?

Re: Basic NAT / Firewall Question

Is there a way of determining if the firewall is blocking the traffic to the other ports or if the Server has been locked down and is blocking them?

Any help would be appreciated.

Regards

Thatch

--

Christopher Stromblad
Security Architect

90 Long Acre
Covent Garden
London, WC2E9RZ
cs@xxxxxxxxxxxxxx
www.outpost24.com
t :+44 (0) 207 849 3097
m :+44 (0) 771 725 8053
f :+44 (0) 207 849 3140

=====
This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed.

If you have received this email in error please notify the system manager.

This list is sponsored by: Norwich University

EARN A MASTER OF SCIENCE IN INFORMATION ASSURANCE – ONLINE

The NSA has designated Norwich University a center of Academic Excellence in Information Security. Our program offers unparalleled Infosec management education and the case study affords you unmatched consulting experience.

Using interactive e-Learning technology, you can earn this esteemed degree, without disrupting your career or home life.

<http://www.msia.norwich.edu/secfocus>
