

Re: Is there any thing like Bubbleip

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2005-04/0211.html>

From: Walter Roberson (*roberson_at_ibd.nrc-cnrc.gc.ca*)

Date: 04/18/05

Date: 18 Apr 2005 07:00:03 GMT

In article <1113765183.322236.89770@l41g2000cwc.googlegroups.com>, <premdeepbanga@gmail.com> wrote:
:Thanks for above guidance,

:but if we try to test it using the free static DNS service provided by
:the dynDNS, then it detects my network administrator's server address,
:and i am not allowed to access it, i mean to say, suppose the network
:administaror have ip address(public) 203.65.15.87
:and my local ip address is 172.16.2.15, then my detected ip address is
:203.65.15.87, and logically that is the only way through which i am
:accessing the net, sa if i want my VNC to work, it has to be installed
:on the admins machine, and i want that my machine must be recognized,
:hows that possible, can you exlan it to me,

If your local IP is 172.16.2.15 and when you go out to the net, the net knows you as 203.65.15.87, then your network is using Network Address Translation (NAT).

There are four important forms of NAT:

a) one-to-one NAT. Each inside address gets translated to an outside address that will not be used for any other inside device until the inside host finishes all its active conversations. When this form of NAT is used, yusually as long as you have that same address, anyone from outside can reach you, provided they pass any other security checks.

On a Statefull Packet Inspection (SPI) firewall, one of the other security checks might be that the incoming packet is coming from the of the addresses (or address+port combinations) that the inside host has requested to talk to. When such a check is in place, the only people who could reach in would be those the inside host had already reached out to. Any security controls on the network would also have to be satisfied.

b) many-to-one NAT achieved by manipulating port numbers.
More commonly known as PAT, Port Address Translation.

When PAT is in use, usually there is no way to reach inward from the outside, unless the firewall is inspecting the flow of traffic and protocol such as FTP or SIP is being used that negotiates ports or IP addresses. VNC is not one of the protocols with address or port negotiation, so outside VNC would seldom be not usually be able to start new connections to inside VNC servers.

c) static NAT. The inside address is translated to a constant outside IP that does not change [until the firewall is reconfigured.]

When static NAT is used, usually arbitrary hosts can make connections from the outside inward to the inside host, by naming the IP address that shows up to the outside world (e.g., would show up for dynDNS purposes.) Any firewall access controls would still need to be satisfied. That is, the firewall administrator would have to have configured to allow the VNC port through.

d) static PAT. Similar to static NAT except particular ports are held fixed when communicating to the outside, and the other ports might be completely dynamic.

When static PAT is in use, you would not usually be able to reach from the outside to the inside, not unless the firewall administrator had –specifically– set it up.

One problem with static PAT is that the IP address used for the protocol + port that would contact dyDNS is not necessarily going to be the same IP address that would reach the VNC port, making things even less certain.

Thus whether a facility such as dynDNS would be useful would depend on the kind of NAT in use, and the strength of the firewall rules.

Nearly all the cases in which dynDNS would –not– work for you with NAT, are the same cases in which NOTHING direct would work for you.

If you are inside a NAT system then the NAT system might well have Statefull Packet Inspection, and would effectively only allow replies to conversations that were initiated from the inside. In such a case, the only way for others to reach you is to connect to an intermediate system *and hold that port open*, with the intermediate system relaying connections for you.

comp.security.misc: Re: Is there any thing like Bubbleip

I was going to suggest setting up a VPN server that everyone connected to over IPSec --- you could send any packets over IPSec --- but earlier you said that the solution had to be free, and setting up a VPN server requires that a computer be used [but you can get free software.] In theory you could use one of the travelling systems even, but whatever system acts as the server would need to have static NAT or the network otherwise set up to send the packets through to that particular inside host.

Generally speaking if you are on the inside of NAT and the network administrator hasn't set things up to allow you to make connections inward, then there isn't any way to make a direct connection inward. It isn't just a matter of finding a good registry or something like that: the network equipment just won't let the packets in.

To answer a question that sometimes gets asked: No, there is no way to send an IP packet to the outside IP of a NAT device and have the NAT device redirect to an inside host named in the packet --- not unless you are using a VPN.

--

This signature intentionally left... Oh, darn!