Running Head: NAT/PAT

Week 5: NAT and PAT Configuration

Jered McClure

Walden University

Week 5: NAT and PAT Configuration

Sw1 with ping showing successful configuration:



Screen shot of R1 configuration:



Screenshot of R2 configuration:



R1 showing PAT configuration:



Screenshot showing R1 configuration of ip nat translation:



While the most important reason to have NAT/PAT around is the preservation of IPv4 addresses, there will always be a need for NAT/PAT even when IPv4 is discontinued. NAT/PAT offers a way to easily separate local network traffic and foreign network traffic, without having to filter each individual node. If all traffic must go through a specific IP address, then all traffic through that IP address can be checked for threats, rather than having to check all traffic across a network at all times. Also, with the network separated, private internal data is secured from trespass.

The downside to NAT/PAT is the fact that it does separate internal and external traffic. If a node from the outside network needs to access a node on the internal network, then special routing rules must be made in order for the external node’s traffic to see the internal IP address. This can actually lead to a network slowdown for that connection due to address translation processes and possible limited routes to nodes. That being said, modern layer 3 switches can handle this traffic (Meyers, 2009).

There is one distinct problem with NAT, traffic collision. NAT collision is when two nodes connect to the same address/port on the same protocol, via NAT, simultaneously (Oracle, 2010). Of course, the chance of this happening is 1 in 32,000, the possible number of source ports. Nodes generally get around this by simply choosing a different source port then another connection which is trying to connect. Since there will always be some delay in a network, collisions fix themselves after a few moments.

NAT/PAT will be an integral part of secure networking for many years to come. While NAT’s primary purpose was for IPv4 extension, its security benefits will ensure its future use into IPv6 and beyond. Even the few problems it has can be seen to have beneficial value in network security. In essence, NAT is an extra layer of security, and that is never a bad thing.

Reference

Meyers, M. (2009). *CompTIA Netowrk+ Guide to Managing and Troubleshooting Networks* (2nd ed.). McGraw-Hill.

Oracle. (2010). *Dynamic NAT Collissions.* Retrieved May 19, 2012, from Oracle: http://docs.oracle.com/cd/E19047-01/sunscreen32/806-6347/6jfa0g881/index.html