Network Security

By Walter T. Pan

Question 1: Faulty Firewall Suppose you have a firewall that's supposed to block SSH connections, but instead lets them through. How would you debug it?

Firewalls can block unauthorized SSH connections or all SSH connections to prevent malicious actors from accessing the network behind the firewall. A firewall that allows SSH connection when it is supposed to block the connection is clearly faulty and needs to be fixed. We can debug a firewall, otherwise known as network security group (NSG) rules, on an Azure VM by checking the firewall status, such as if one exists, inbound rules, rules priority, and allowed sources.

In my Azure ELK stack project, I set up a NSG for a virtual network (VN). The NSG includes default rules that restrict all access, including SSH, to the VN. Exercising the principle of least privilege, a network administrator may grant necessary access to the VN rather than restricting it. The NSG rules only allowed SSH (port 22) access from the internet to the VN jump box from a specific public IP address, and SSH access from the jump box to virtual machines within the VN. When a user attempts to SSH into the VN without rules allowing for SSH access, their communication with the VN would not be accepted and will time out.

If a virtual machine (VM) from my project accepts SSH connection, there is probably an inbound "allow" rule in the NSG allowing for SSH connection, and the rule may have a higher priority than rules restricting SSH access. So, the inbound rules that allow and restrict SSH access to the VN and their priority number needs to be double checked. Successful restriction of SSH access can be tested by attempting to SSH into a VM of the VN.

To investigate the problem on Azure, log into the VN's Azure account, search NSG on the search bar in the Azure webpage, select "Inbound rules" from the list of options on the left side of the NSG's page, and check the inbound rules listed. If there is a rule allowing SSH access to the VN, it needs to be removed. If there is no rule restricting SSH access to the VN, one needs to be added. If restricting SSH access to the VN is essential, the rule's priority number needs to be adjusted to have priority over other rules, especially over any rules allowing SSH access to the VN. The fix to restrict SSH access can be tested by attempting to SSH into a VM of the VN, and a failure to connect will indicate success.

The rules implemented above will restrict all port 22 SSH access to the VMs. However restricting port 22 SSH access restriction alone won't protect the VN from all unauthorized access. The VN can still be accessed through other ports if the inbound rules allow it. Some examples of ports that can be used to access the VN include port: 20, 21, 23, 25, 80, 443, and other port numbers. The NSG rules should be checked to ensure only ports essential to the function of the VN are opened to sources that need access. For example, if a single user needs port 20 access for data transfer, the NSG rules should only allow an IP used by the single user access to port 20 and no one else.