WIKIPEDIA

Reverse connection

A **reverse connection** is usually used to bypass firewall restrictions on open ports. A firewall usually blocks incoming connections on open ports, but does not block outgoing traffic. In a normal forward connection, a client connects to a server through the server's open port, but in the case of a reverse connection, the client opens the port that the server connects to. The most common way a reverse connection is used is to bypass firewall and router security restrictions.

For example, a backdoor running on a computer behind a firewall that blocks incoming connections can easily open an outbound connection to a remote host on the Internet. Once the connection is established, the remote host can send commands to the backdoor. Remote administration tools (RAT) that use a reverse connection usually send SYN packets to the client's IP address. The client listens for these SYN packets and accepts the desired connections.

If a computer is sending SYN packets or is connected to the client's computer, the connections can be discovered by using the netstat command or a common port listener like “Active Ports”. If the Internet connection is closed down and an application still tries to connect to remote hosts it may be infected with malware. Keyloggers and other malicious programs are harder to detect once installed, because they connect only once per session. Note that SYN packets by themselves are not necessarily a cause for alarm, as they are a standard part of all TCP connections.

There are honest uses for using reverse connections, for example to allow hosts behind a NAT firewall to be administered remotely. These hosts do not normally have public IP addresses, and so must either have ports forwarded at the firewall, or open reverse connections to a central administration server.

External links

- [1] (https://www.howtoforge.com/reverse-ssh-tunneling)
