Denial of Service and Attack Protection

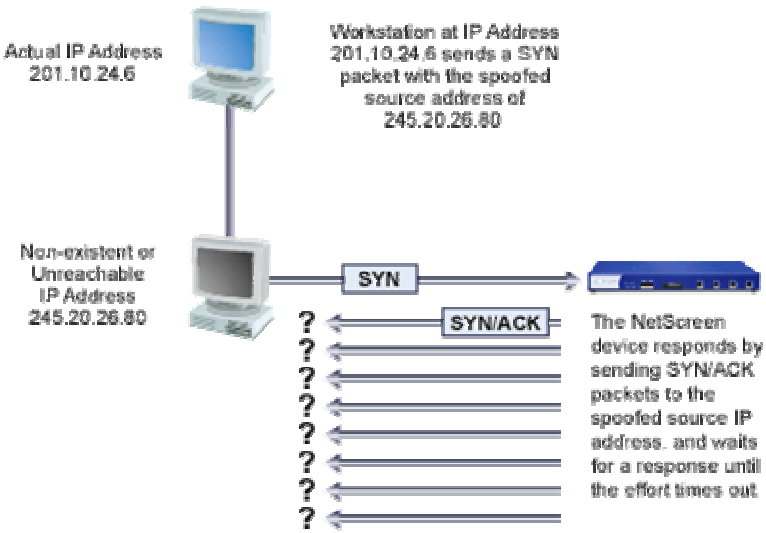
Juniper Networks integrated firewall/IPSec VPN solutions include built-in Denial of Service (DoS) and attack protection, leveraging Stateful inspection to look for and then allow or deny all connection attempts that require crossing an interface on their way to and from the intended destination. As a result, Juniper Networks solutions can be configured to protect against more than 30 different attacks, both internal and external.

Stateful inspection, however, is only one component in attack protection. Specific to DoS attacks, other protection components are performance related, including a high session ramp rate and up to 12GB of throughput. High session ramp rate and throughput are a direct benefit of Juniper's high performance hardware architecture, while Stateful inspection will scan for attack signatures and react against them based on the security policy. For those network segments that are more prone to application layer attacks, Juniper Networks can provide enterprises with a Deep Inspection firewall to protect the network perimeter and a robust intrusion detection and prevention solution to protect critical resources at the central site.

The following is an example of a SYN attack and how the Juniper Networks integrated firewall/IPSec VPN solution can detect and deflect them, as well as a few other attack types:

· **SYN Attack**: A SYN flood attack occurs when a network becomes so overwhelmed by SYN packets initiating uncompletable connection requests that it can no longer process legitimate connection requests, resulting in a denial of service (DoS). The way it works is as follows:

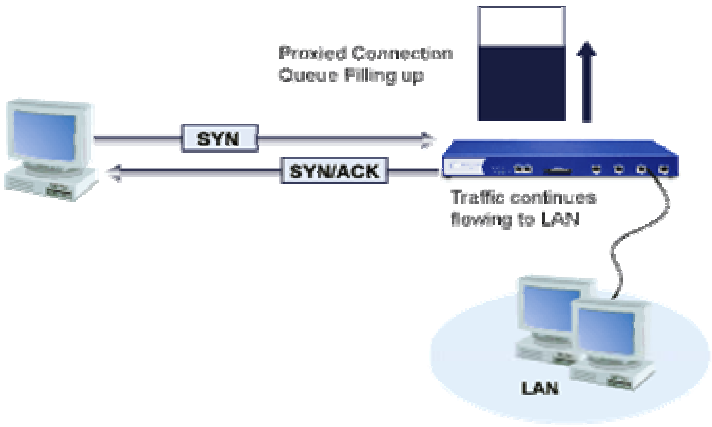
A TCP connection is established with a triple exchange of packets known as a three-way handshake: A sends a SYN packet to B; B responds with a SYN/ACK packet; and A responds with an ACK packet. A SYN Flood attack inundates a site with SYN packets containing forged ("spoofed") IP source addresses with nonexistent or unreachable addresses. The firewall responds with SYN/ACK packets to these addresses and then waits for responding ACK packets. Because the SYN/ACK packets are sent to nonexistent or unreachable IP addresses, they never elicit responses and eventually time out.



By flooding a server or host with connections that cannot be completed, the attacker eventually fills the host's memory buffer. Once this buffer is full, no further connections can be made and the host's operating system might be damaged. Either way, the attack disables the host and its normal operations. A SYN Flood attack is classified as a denial-of-service (DoS) attack.

Juniper Networks SYN Flood Attack Protection: Juniper Networks integrated firewall/VPN devices can impose a limit on the number of SYN packets per second permitted to pass through the firewall. When that threshold is reached, the device starts proxying

incoming SYN packets, sending out SYN/ACK responses for the host and storing the incomplete connections in a connection queue. The incomplete connections remain in the queue until the connection is completed or the request times out. In the following illustration, the SYN threshold has been passed and the integrated firewall/IPSec VPN device has begun proxying SYN packets.



· **ICMP Flood**: An ICMP flood occurs when ICMP pings overload a system with so many echo requests that the system expends all its resources responding until it can no longer process valid network traffic. When enabling the ICMP flood protection feature, administrators can set a threshold that once exceeded invokes the ICMP flood attack protection feature. (The default threshold value is 1000 packets per second.)

Juniper Networks ICMP Flood Protection: If the threshold is exceeded, the integrated firewall/VPN device ignores further ICMP echo requests for the remainder of that second plus the next second as well.

· **UDP Flood**: Similar to the ICMP flood, UDP flooding occurs when UDP packets are sent with the purpose of slowing down the system to the point that it can no longer handle valid connections. After enabling the UDP flood protection feature, administrators can set a threshold that once exceeded invokes the UDP flood attack protection feature. (The default threshold value is 1000 packets per second.)

Juniper Networks UDP Flood Protection: If the number of UDP packets from one or more sources to a single destination exceeds this threshold, the integrated firewall/VPN device ignores further UDP packets to that destination for the remainder of that second plus the next second as well.

· **Port Scan Attack**: A port scan attack occurs when one source IP address sends IP packets to 10 different ports at the same destination IP address within a defined interval (5,000 microseconds is the default). The purpose of this scheme is to scan the available services in the hopes that one port will respond, thus identifying a service to target.

Juniper Networks Port Scan Attack Protection: The integrated firewall/VPN device internally logs the number of different ports scanned from one remote source. Using the default settings, if a remote host scans 10 ports in 0.005 seconds (5,000microseconds), the device flags this as a port scan attack, and rejects all further packets from the remote source (regardless of the destination IP address) for the remainder of that second.