Q&A

Router Stops Passing Traffic

Q: Why does the router stop passing traffic after running for a period of time with the firewall on?

A: The NetVanta firewall creates rules for traffic based on sessions that are created for traffic flows. Whenever a packet that is part of a new traffic flow hits the firewall; the firewall checks to see if there is a rule for this packet. If the packet is allowed, there is a session created within the router for all traffic relating to that data flow. This traffic includes all relevant traffic from the destination of the first packet.

Because each session takes up memory on the router, there is a limited number of sessions that can be used. This number varies depending on the model as well as the available memory in that device. To view the number of policy sessions that are available as well as the number active, use the following command from the enable prompt:

Router#show ip policy-stats
Current sessions: 400
Maximum sessions: 100000

Policy-class “Private”:
  250 current sessions

Policy-class “Public”:
  150 current sessions

Policy-class "self":
  0 current sessions

Policy-class "default":
  0 current sessions

Once a session is created, it will remain in memory for the duration of the timeout associated with that traffic or until the flow is closed by either end of the connection. For instance, if a TCP session is created, it may not remain in memory for the duration of the timeout as a FIN and a FINACK will signal the end of the transfer. UDP, however, is connectionless, therefore there is no way for most UDP sessions to be closed before the timeout occurs.

If at any time the current sessions active on the router is the same or close to the same as the maximum sessions, the router will begin blocking all packets related to new traffic flows. Whenever this occurs, use the following clear command from a console connection to delete all active sessions:

Router#clear ip policy-sessions

After clearing the policy-sessions, traffic should begin to pass again. If policy-sessions are filled up frequently, it is possible that the timeout values have been changed and therefore old, unused policy-sessions are not being cleared which eventually will cause the maximum number of sessions to be reached. If this is possibly the case, it is recommended to set the timeout values to the default and monitor the firewall to see if the problem still exists. Below is the default configuration for different protocols:

ip policy-timeout tcp all-ports 600
ip policy-timeout udp all-ports 60
ip policy-timeout icmp 60
ip policy-timeout esp 60
ip policy-timeout ahp 60
ip policy-timeout gre 60

If after changing these settings to the default, the problem still exists, please contact Technical Support by phone at (888)4ADTRAN or by e-mail at support@adtran.com.