Commands Overview

**nat-control Command**

The **nat-control** command is used to enforce address hiding on the inside and outside interfaces of a Security Appliance. With **nat-control** enabled, all packets that flow through the Security Appliance require a NAT rule, or the packets will be denied access through the appliance. If an inside NAT policy is enabled on an interface, each inside address must have an inside NAT rule configured or communication will not be permitted through the Security Appliance. Additionally, if an outside NAT policy is enabled on an interface, all outside addresses must have an outside NAT rule configured or communication will not be permitted through the Security Appliance.

The **nat-control** command is not enabled by default, requiring that only hosts that undergo NAT need a NAT rule.

**global Command**

The **global** command is used to define the address or range of addresses into which the addresses defined by the **nat** command are translated. It is important that the *nat-id* be identical to the *nat-id* used in the **nat** command. The *nat-id* pairs the IP address defined by the **global** and **nat** commands so that network translation can take place. The syntax of the **global** command is as follows:

global (if-name) nat-id global-ip | global-ip-global-ip [netmask netmask]

**dhcp Command**

dhcpd address ip1[-ip2] if-name

dhcpd auto-config [outside]

dhcpd dns dns1 [dns2]

dhcpd wins wins1 [wins2]

 dhcpd lease lease-length

 dhcpd domain domain-name

 dhcpd enable if-name

dhcpd option 66 ascii {server-name | server-ip-str}

dhcpd option 150 ip server-ip1 [ server-ip2]

dhcpd ping-timeout timeout

debug dhcpd event

 debug dhcpd packet

**NTP Command**

ntp server ip-address [key number] source if-name [prefer]

show ntp

show ntp associations [detail]

show ntp status