Netscreen Firewall - Interfaces

- Below is a screen shot for a Netscreen Firewall interface. All interfaces have an IPv6 address except ethernet0/0. We will step through configuring this interface.

Remember...The Help Menu is your friend!
Netscreen Firewall – IPv6

- To configure, enable IPv6, determine mode and enter IPv6 address with prefix.
- Use Host Mode to accept RA messages.
- User Router Mode to send RA messages.
Netscreen – Configure IPV6

- After configuring the IPv6 addresses and clicking apply, the Neighbor Discovery (ND) and Router Advertisement (RA) settings are now available for configuration.
Netscreen – ND/RA Settings (Host)

- If using Host Mode, determine if you would like to accept incoming router advertisements.
- Accept Incoming Router Advertisements learns of the existence and identity of IPv6 routers by accepting Router Advertisement (RA) messages.
Netscreen – ND/RA Settings (Router)

- Use RA Transmission to learn of the existence and identity of other IPv6 routers.
- Link MTU advertises the link-MTU in router advertisements.
- Link Layer Address enables the Link Layer Address flag, which includes the link-layer (MAC) address of the router in outgoing RA messages.
## Netscreen – IPv6 Route Table

- **Text**

<table>
<thead>
<tr>
<th>IP/Prefix</th>
<th>Gateway</th>
<th>Interface</th>
<th>Protocol</th>
<th>Preference</th>
<th>Metric</th>
<th>Vsyst</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 2001:abc:2480:3621::3/64</td>
<td>::</td>
<td>ethernet0/1</td>
<td>C</td>
<td></td>
<td></td>
<td>Root</td>
<td>-</td>
</tr>
<tr>
<td>* 2001:abc:2480:3621::3/128</td>
<td>::</td>
<td>ethernet0/1</td>
<td>H</td>
<td></td>
<td></td>
<td>Root</td>
<td>-</td>
</tr>
<tr>
<td>* 2001:abc:2480:3627::1/64</td>
<td>::</td>
<td>ethernet0/2</td>
<td>C</td>
<td></td>
<td></td>
<td>Root</td>
<td>-</td>
</tr>
<tr>
<td>* 2001:abc:2480:3627::1/128</td>
<td>::</td>
<td>ethernet0/2</td>
<td>H</td>
<td></td>
<td></td>
<td>Root</td>
<td>-</td>
</tr>
<tr>
<td>* 2001:abc:2480:36f7::254/128</td>
<td>::</td>
<td>loopback.1</td>
<td>C</td>
<td></td>
<td></td>
<td>Root</td>
<td>-</td>
</tr>
<tr>
<td>* 2001:abc:2480:35f7::254/128</td>
<td>::</td>
<td>loopback.1</td>
<td>H</td>
<td></td>
<td></td>
<td>Root</td>
<td>-</td>
</tr>
<tr>
<td>* 2001:abc:2480:35aa::7/64</td>
<td>::</td>
<td>ethernet0/0</td>
<td>C</td>
<td></td>
<td></td>
<td>Root</td>
<td>-</td>
</tr>
<tr>
<td>* 2001:abc:2480:35aa::7/128</td>
<td>::</td>
<td>ethernet0/0</td>
<td>H</td>
<td></td>
<td></td>
<td>Root</td>
<td>-</td>
</tr>
</tbody>
</table>

* Active route
P Permanent
D Dynamic
C Connected
I Imported
eB EBGP
O OSPF
E1 OSPF external type 1
H Host Route
S Static
A Auto-Exported
iB IBGP
R RIP
E2 OSPF external type 2
Netscreen – Add IPv6 Default Route

- Add ‘::/0’ to denote default route (all IPv6 addresses)
- Add next-hop IPv6 address
Netscreen – Verify Default IPv6 Route

- Verify the newly added IPv6 default route is now in the routing table and is active.

<table>
<thead>
<tr>
<th>IP/Prefix</th>
<th>Gateway</th>
<th>Interface</th>
<th>Protocol</th>
<th>Preference</th>
<th>Metric</th>
<th>Vsys</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 2001:b:2480:3621::3/64</td>
<td>::</td>
<td>ethernet0/1</td>
<td>C</td>
<td></td>
<td></td>
<td>Root</td>
<td>-</td>
</tr>
<tr>
<td>* 2001:b:2480:3621::3/128</td>
<td>::</td>
<td>ethernet0/1</td>
<td>H</td>
<td></td>
<td></td>
<td>Root</td>
<td>-</td>
</tr>
<tr>
<td>* 2001:b:2480:3627::1/64</td>
<td>::</td>
<td>ethernet0/2</td>
<td>C</td>
<td></td>
<td></td>
<td>Root</td>
<td>-</td>
</tr>
<tr>
<td>* 2001:b:2480:3627::1/128</td>
<td>::</td>
<td>ethernet0/2</td>
<td>H</td>
<td></td>
<td></td>
<td>Root</td>
<td>-</td>
</tr>
<tr>
<td>* 2001:b:2480:36f7::254/128</td>
<td>::</td>
<td>loopback.1</td>
<td>C</td>
<td></td>
<td></td>
<td>Root</td>
<td>-</td>
</tr>
<tr>
<td>* 2001:b:2480:36f7::254/128</td>
<td>::</td>
<td>loopback.1</td>
<td>H</td>
<td></td>
<td></td>
<td>Root</td>
<td>-</td>
</tr>
<tr>
<td>* 2001:b:2480:36aa::7/64</td>
<td>::</td>
<td>ethernet0/0</td>
<td>C</td>
<td></td>
<td></td>
<td>Root</td>
<td>-</td>
</tr>
<tr>
<td>* 2001:b:2480:36aa::7/128</td>
<td>::</td>
<td>ethernet0/0</td>
<td>H</td>
<td></td>
<td></td>
<td>Root</td>
<td>-</td>
</tr>
<tr>
<td>* ::/0</td>
<td>2001:b:2480:3621::1</td>
<td>ethernet0/1</td>
<td>SP</td>
<td>20</td>
<td>1</td>
<td>Root</td>
<td>Remove</td>
</tr>
</tbody>
</table>
Netscreen Policies – Allow ICMP6

- As with IPv4, do not block all ICMP6!
- See RFC4890 - Recommendations for Filtering ICMPv6 Messages in Firewalls
- Traffic That Must Not Be Dropped
  - Destination Unreachable (Type 1) - All codes
  - Packet Too Big (Type 2)
  - Time Exceeded (Type 3) - Code 0 only
  - Parameter Problem (Type 4) - Codes 1 and 2 only
  - Echo Request (Type 128)
  - Echo Response (Type 129)

- This is not all inclusive, there are other recommendations in RFC.
Netscreen IPv6 Policies

- IPv6 policies are separate policies from IPv4.
- Can add policy elements & groups for IPv6 just as IPv4.
- Implement policies for IPv6 the same as for IPv4.
Netscreen CLI – Verify Routing

- Use the ‘get route v6’ to view IPv6 routing table.
Netscreen CLI – Verify IPv6 Neighbors

- Use ‘get ndp’ to determine IPv6 neighbors.
Netscreen CLI – Verify Reachability

- Use the Ping command to ping the upstream router.

![Ping command output](image1)

- SSH to the IPv6 Firewall Address.

![SSH output](image2)
IPv6 Interface Configuration –
set interface ethernet0/1 ip 168.168.201.3/29
set interface "ethernet0/1" ipv6 mode "router"
set interface "ethernet0/1" ipv6 ip 2001:abc:3621::3/64
set interface "ethernet0/1" ipv6 enable
set interface ethernet0/1 route

IPv6 Router Advertisement Settings –
set interface ethernet0/1 ipv6 ra prefix 2001:abc:3621::/64 autonomous onlink
set interface ethernet0/1 ipv6 ra link-address
set interface ethernet0/1 ipv6 ra transmit
set interface ethernet0/1 ipv6 ra link-mtu
set interface ethernet0/1 ipv6 nd nud

IPv6 Default Route –
set route ::/0 interface ethernet0/1 gateway 2001:abc:3621::1 permanent

Policy Using ‘Multiple’ Source and ‘Multiple’ Destination –
set policy id 994274 from "SAN_Zone" to "Untrust" "Any9 IPv6 - 2001:abc:2480:a000::90/64" "Any10 IPv6 - 2001:abc:4300::240:95/64" "ANY" permit
set policy id 994274
set src-address "Any11 IPv6 - 2001:abc:2480:a000::93"
set src-address "Any12 IPv6 - 2001:abc:2480:a000::92"
set src-address "Any13 IPv6 - 2001:abc:2480:a000::91/64"
set dst-address "Any14 IPv6 - 2001:abc:4300::2400:119/64"
set dst-address "Any15 IPv6 - 2001:abc:4300::2400:138/64"
set dst-address "Any16 IPv6 - 2001:abc:4300::2400:120"

Set Policy Group –
set group address "SAN_Zone" "SAN_Servers"
set group address "SAN_Zone" "SAN_Servers" add "Any11 IPv4 - 127.32.148.172/32"
set group address "SAN_Zone" "SAN_Servers" add "Any12 IPv4 - 127.32.148.175/32"
set group address "SAN_Zone" "SAN_Servers" add "Any13 IPv4 - 127.32.148.174/32"
set group address "SAN_Zone" "SAN_Servers" add "Any14 IPv4 - 127.32.148.173/32"