Interface Failover with Route Based VPNs

Version 1.2
ScreenOS 5.1.0 and higher

Purpose
This paper describes how to configure VPN and Interface Failover using NetScreen-25/50/204/208. The failover mechanism is different than the Untrust Failover feature on the NetScreen-5GT platforms, and we will discuss the general procedure of setting this up. It is not as intuitive as the Untrust Failover on NS-5GT.

Requirement
For failover using Interface monitoring on the NetScreen-25/50/204/208, ScreenOS 5.1.0 and higher is required.

Example

The best way to discuss the interface failover and VPN is to make use of an example. In the diagram above,

In this example, our NetScreen-204 is configured with a trust network of 10.1.1.0/24. The primary untrust interface is 1.1.1.1/24, and when that interface fails, the backup connection will take over with an IP of 3.3.3.1/24. This example will use track-ip for interface monitoring.
Interface Failover with NetScreen-25 and Higher

On NetScreen-25 and higher, interface failover mechanism is done via interface monitoring feature. With Interface Monitoring, weighted sum of track-ip failures are compared to a set track-ip threshold. Once the weighted sum of track-ip failures meets or exceeds the track-ip threshold, an interface track-ip failure weight is assigned. The interface track-ip failure weight is then compared to the interface threshold. If the interface track-ip failure weight meets or exceeds the interface monitor threshold, the interface turns to a failed state.

Configure Interfaces

First, you'll need to configure two interfaces in the untrust zone. We will choose ethernet3 and ethernet4:

```
set interface "ethernet3" zone "Untrust"
set interface ethernet3 ip 1.1.1.1/24
set interface "ethernet4" zone "Untrust"
set interface ethernet4 ip 3.3.3.1/24
```

Interface Monitoring Using Track-IP

You can monitor the state of the primary interface by using one or more track-ip. The interface sends an ICMP packet to the specified track-ip at specified intervals. If the ICMP request to the track-ip fails, this is counted as one ping failure. If the total ping failures reach the threshold amount (which you configure), a weight for that track-ip failure is assigned (based on what you configure).

A sum of all track-ip failure weights is calculated. If the sum of the track-ip failure weights meets or exceeds the specified threshold, another weight is assigned to the weighted sum. If this weight meets or exceeds the interface threshold, the interface will go down.

This is illustrated in the flowchart below:
Interface Failover with Route Based VPNs

In our example, interface failover configuration for interface ethernet3 is as follows:

```
set interface ethernet3 monitor track-ip ip
set interface ethernet3 monitor track-ip threshold 100
set interface ethernet3 monitor track-ip weight 50
set interface ethernet3 monitor track-ip ip 2.2.2.100 weight 50
set interface ethernet3 monitor track-ip ip 2.2.2.10 weight 60
set interface ethernet3 monitor threshold 40
```

In this example, an ICMP is sent from interface ethernet3 to 2.2.2.100 and 2.2.2.10. One ICMP is every second. The default failure count threshold is 3. If there are 3 consecutive failed responses to the ICMP attempts, a track-ip weight for 2.2.2.100 of 50 is assigned. The track-ip weights are compared to the track-ip threshold, which is 100. Since 50 < 100, the track-ip for this
interface has not failed yet. However, if the track-ip ICMP’s to 198.6.1.3 fails 3 times, the track-ip weight for 2.2.2.10 of 60 is assigned. The sum of the track-ip weights is then 110, which is greater than 100. Therefore, the track-ip is in a failed condition, and the interface track-ip weight of 50 is assigned. This track-ip weight is then compared to the interface monitor threshold, which is 40. If this is the case, the interface is then set to failed condition, and the interface will go in down state.

You can check the condition of the interface monitoring by issuing the command

```
get interface ethernet3 monitor
```

To check the condition of each interface track-ip ip address:

```
ns50-> get interface ethernet3 track-ip ip
Ip address     intval threshold wei gateway         fail-count success
2.2.2.100      1         3  50 0.0.0.0                 63 77%
2.2.2.10       1         3  60 0.0.0.0                 63 88%
```

failure weight: 50, threshold: 100, failed: 2 ip(s) failed, weighted sum = 110

ns50-> get interface ethernet3 monitor
interface ethernet3 monitoring threshold: 40, failure action: interface logically down, weighted sum: 0, not failed
interface ethernet3 monitor interfaces:
interface ethernet3 monitor zones:

Here is a sample where the interface failed over due to track-ip failures:

```
n50-> get interface ethernet3 monitor track-ip
Ip address     intval threshold wei gateway         fail-count success
2.2.2.100      1         3  50 0.0.0.0                 63 77%
2.2.2.10       1         3  60 0.0.0.0                 63 88%
```

failure weight: 50, threshold: 100, failed: 2 ip(s) failed, weighted sum = 110

ns50-> get interface ethernet3 monitor
interface ethernet3 monitoring threshold: 40, failure action: interface logically down, weighted sum: 50, failed
interface ethernet3 monitor interfaces:
interface ethernet3 monitor zones:

Here, the weighted sum is 110, which exceeds the threshold 100. A failure weight of 50 has been assigned. This failure weight is then compared to the interface monitor threshold, which is 40. The failure weight exceeds the interface monitor threshold, and therefore the interface has failed.

When interface ethernet3 is restored, it will regain it’s physical link up status, due to the track-ip monitor threshold tests/comparisons.

**Configuring Redundant VPN with Interface Failover**

To configure VPNs to follow the interface (no matter if it fails over or not), route based VPN configuration is required. One set of IKE gateways are required for each outgoing interface (i.e. one VPN tunnel for primary, one VPN tunnel for backup outgoing interface).

On the peer gateway, there will also be two sets of VPN tunnels to the NS-204 (one for primary, and one for backup). We will configure the VPNs according to the table below:
Interface Failover with Route Based VPNs

### NS-204:

<table>
<thead>
<tr>
<th>IKE Gateway</th>
<th>Gateway Address</th>
<th>P1 Proposal</th>
<th>Outgoing-if</th>
<th>P2 Proposal</th>
<th>Local Proxy-id</th>
<th>Remote Proxy-id</th>
<th>tunnel-if</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>2.2.2.1</td>
<td>Compatible</td>
<td>ethernet3</td>
<td>Compatible</td>
<td>10.1.1.0/24</td>
<td>172.16.10.0/24</td>
<td>tunnel.1</td>
</tr>
<tr>
<td>Backup</td>
<td>2.2.2.1</td>
<td>Compatible</td>
<td>ethernet4</td>
<td>Compatible</td>
<td>10.1.1.0/24</td>
<td>172.16.10.0/24</td>
<td>tunnel.2</td>
</tr>
</tbody>
</table>

The equivalent VPN configurations for each device is shown below

### NS-204:

```bash
set interface "tunnel.1" zone "Untrust"
set interface "tunnel.2" zone "Untrust"
set interface tunnel.1 ip unnumbered interface ethernet3
set interface tunnel.2 ip unnumbered interface ethernet4
set ike gateway "ns208gw primary" address 2.2.2.1 Main outgoing-interface "ethernet3"
preshare "XF3N5aHNH6n3KsVh4CnxRgP4nmCd1BC1w==" sec-level standard
set ike gateway "ns208gw backup" address 2.2.2.1 Main outgoing-interface "ethernet4"
preshare "ITBkIKGNN7AuOaZ04CBvEKwQunnk42FKA==" sec-level standard
set vpn "ns208vpn primary" gateway " ns208gw primary" no-replay tunnel idletime 0 sec-level standard
set vpn " ns208vpn primary" monitor optimized rekey
set vpn " ns208vpn primary" id 3 bind interface tunnel.1
set vpn "ns208vpn backup" gateway " ns208gw backup" no-replay tunnel idletime 0 sec-level standard
set vpn "ns208vpn backup" monitor optimized rekey
set vpn "ns208vpn backup" id 2 bind interface tunnel.2
set vpn "ns208vpn primary" proxy-id local-ip 10.1.1.0/24 remote-ip 172.16.10.0/24 "ANY"
set vpn "ns208vpn backup" proxy-id local-ip 10.1.1.0/24 remote-ip 172.16.10.0/24 "ANY"
```

### NS-208:

```bash
set interface "tunnel.1" zone "Untrust"
set interface "tunnel.2" zone "Untrust"
set interface tunnel.1 ip unnumbered interface ethernet3
set interface tunnel.2 ip unnumbered interface ethernet3
set ike gateway "ns204gw primary" address 3.3.3.1 Main outgoing-interface "ethernet3"
preshare "7IdjSGXaNaD+jFsKKECjMI+YoEnL6A3o3w==" sec-level standard
set ike gateway "ns204gw backup" address 3.3.3.1 Main outgoing-interface "ethernet3"
preshare "4xo8fzrMN3hxs6fCGIVUC1g1n88WN3A==" sec-level standard
set ike respond-bad-spi 1
set vpn "ns204vpn primary" gateway "ns204gw primary" no-replay tunnel idletime 0 sec-level standard
set vpn " ns204vpn primary" monitor optimized rekey
set vpn " ns204vpn primary" id 1 bind interface tunnel.1
set vpn "ns204vpn backup" gateway " ns204gw backup" no-replay tunnel idletime 0 sec-level standard
set vpn "ns204vpn backup" monitor optimized rekey
set vpn "ns204vpn backup" id 2 bind interface tunnel.2
set vpn "ns204vpn primary" proxy-id local-ip 172.16.10.0/24 remote-ip 10.1.1.0/24 "ANY"
set vpn "ns204vpn backup" proxy-id local-ip 172.16.10.0/24 remote-ip 10.1.1.0/24 "ANY"
```
Routing Considerations

When the primary link is up, we want all traffic to route through interface ethernet3. We only want traffic to go through ethernet4 when the ethernet3 link goes down. Therefore, we separate these by setting a lower metric on the backup route for both default route and for tunnel routes. Also, avoid using permanent routes, as this would prevent route failovers to work.

NS204:

set route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.254
set route 0.0.0.0/0 interface ethernet4 gateway 3.3.3.254 metric 10
set route 172.16.10.0/24 interface tunnel.1
set route 172.16.10.0/24 interface tunnel.2

Routing Table of NS204 when Primary is up:

Dest Routes for <untrust-vr> (0 entries)
--------------------------------------------------------------------------------
C - Connected S - Static A - Auto-Exported I - Imported R - RIP P - Permanent
iB - IBGP eB - EBGP O - OSPF E1 - OSPF external type 1
E2 - OSPF external type 2

Dest Routes for <trust-vr> (7 entries)
--------------------------------------------------------------------------------
ID  IP-Prefix     Interface  Gateway   P  Pref  Mtr  Vsys
--------------------------------------------------------------------------------
*   5  0.0.0.0/0    eth3       1.1.1.254 S   20     1 Root
6   0.0.0.0/0    eth4       3.3.3.254 S   20    10 Root
*   8  172.16.10.0/24 tun.1     0.0.0.0   S   20     1 Root
10  172.16.10.0/24 tun.2     0.0.0.0   S   20    10 Root
*   7  10.1.1.0/24  eth1       0.0.0.0   C    0      0 Root
*   4  3.3.3.0/24  eth4       0.0.0.0   C    0      0 Root
*   3  1.1.1.0/24  eth3       0.0.0.0   C    0      0 Root

Routing Table of NS204 when Backup (e4) is Up and Primary (e3) is Down:

Dest Routes for <untrust-vr> (0 entries)
--------------------------------------------------------------------------------
C - Connected S - Static A - Auto-Exported I - Imported R - RIP P - Permanent
iB - IBGP eB - EBGP O - OSPF E1 - OSPF external type 1
E2 - OSPF external type 2

Dest Routes for <trust-vr> (7 entries)
--------------------------------------------------------------------------------
ID  IP-Prefix     Interface  Gateway   P  Pref  Mtr  Vsys
--------------------------------------------------------------------------------
*   6  0.0.0.0/0    eth4       3.3.3.254 S   20    10 Root
5   0.0.0.0/0    eth3       1.1.1.254 S   20     1 Root
*  10  172.16.10.0/24 tun.2     0.0.0.0   S   20    10 Root
8  172.16.10.0/24 tun.1     0.0.0.0   S   20     1 Root
*   7  10.1.1.0/24  eth1       0.0.0.0   C    0      0 Root
*   4  3.3.3.0/24  eth4       0.0.0.0   C    0      0 Root
3   1.1.1.0/24  eth3       0.0.0.0   C    0      0 Root
Interface Failover with Route Based VPNs

Security Associations Table:

With primary link active, the SA on the NS-204 side will look like the following:

Ns204→ get sa
total configured sa: 2

<table>
<thead>
<tr>
<th>HEX ID</th>
<th>Gateway</th>
<th>Port Algorithm</th>
<th>SPI</th>
<th>Life:sec kb</th>
<th>Sta</th>
<th>PID vsys</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000001&lt;</td>
<td>2.2.2.1</td>
<td>500 esp:3des/sha1 0afccfd7</td>
<td>2160 unlim A/U</td>
<td>-1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>00000001&gt;</td>
<td>2.2.2.1</td>
<td>500 esp:3des/sha1 3d982f16</td>
<td>2160 unlim A/U</td>
<td>-1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>00000002&lt;</td>
<td>2.2.2.1</td>
<td>500 esp:3des/sha1 00000000 expire unlim I/I</td>
<td>-1</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00000002&gt;</td>
<td>2.2.2.1</td>
<td>500 esp:3des/sha1 0afccfd7</td>
<td>2160 unlim I/I</td>
<td>-1</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

ns50→

The SA on the NS-208 side will look like the following:

Ns208→ get sa

<table>
<thead>
<tr>
<th>HEX ID</th>
<th>Gateway</th>
<th>Port Algorithm</th>
<th>SPI</th>
<th>Life:sec kb</th>
<th>Sta</th>
<th>PID vsys</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000001&lt;</td>
<td>3.3.3.1</td>
<td>500 esp:3des/sha1 0afccfd7</td>
<td>2019 unlim A/U</td>
<td>-1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>00000001&gt;</td>
<td>3.3.3.1</td>
<td>500 esp:3des/sha1 3d982f16</td>
<td>2019 unlim A/U</td>
<td>-1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>00000002&lt;</td>
<td>1.1.1.1</td>
<td>500 esp:3des/sha1 0afccfd8</td>
<td>3564 unlim A/U</td>
<td>-1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>00000002&gt;</td>
<td>1.1.1.1</td>
<td>500 esp:3des/sha1 0afccfd7</td>
<td>2160 unlim A/U</td>
<td>-1</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

ns5gt→

After failover, the SA on the NS-204 side will look like the following:

Ns204→ get sa

<table>
<thead>
<tr>
<th>HEX ID</th>
<th>Gateway</th>
<th>Port Algorithm</th>
<th>SPI</th>
<th>Life:sec kb</th>
<th>Sta</th>
<th>PID vsys</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000001&lt;</td>
<td>2.2.2.1</td>
<td>500 esp:3des/sha1 0afccfd7</td>
<td>1929 unlim A/U</td>
<td>-1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>00000001&gt;</td>
<td>2.2.2.1</td>
<td>500 esp:3des/sha1 3d982f16</td>
<td>1929 unlim A/U</td>
<td>-1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>00000002&lt;</td>
<td>2.2.2.1</td>
<td>500 esp:3des/sha1 0afccfd8</td>
<td>3564 unlim A/U</td>
<td>-1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>00000002&gt;</td>
<td>2.2.2.1</td>
<td>500 esp:3des/sha1 0afccfd7</td>
<td>3564 unlim A/U</td>
<td>-1</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

ns50→

The SA on the NS-208 side will look like the following:

Ns208→ get sa

<table>
<thead>
<tr>
<th>HEX ID</th>
<th>Gateway</th>
<th>Port Algorithm</th>
<th>SPI</th>
<th>Life:sec kb</th>
<th>Sta</th>
<th>PID vsys</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000001&lt;</td>
<td>3.3.3.1</td>
<td>500 esp:3des/sha1 3d982f17</td>
<td>3562 unlim A/U</td>
<td>-1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>00000001&gt;</td>
<td>3.3.3.1</td>
<td>500 esp:3des/sha1 0afccfd8</td>
<td>3562 unlim A/U</td>
<td>-1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>00000002&lt;</td>
<td>1.1.1.1</td>
<td>500 esp:3des/sha1 3d982f16</td>
<td>1926 unlim A/U</td>
<td>-1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>00000002&gt;</td>
<td>1.1.1.1</td>
<td>500 esp:3des/sha1 0afccfd7</td>
<td>1926 unlim A/U</td>
<td>-1</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Question: Why are there SA’s active on both VPN tunnels?

Answer: Since this is a route based VPN, determination on if a VPN tunnel is up is based on the healthchecks due to the VPN Monitor mechanism. The defaults for VPNMonitor healthcheck is the following:

Ns204→ get vpnmonitor
Vpn monitor interval : 10(seconds)
Vpn monitor threshold: 10

Ns204→

This means one VPN monitor healthcheck packet is sent every 10 seconds. The VPN failure threshold is set to 10, so it would take 100 seconds before the SA would be marked down. This would also account for no VPN traffic response until 100 seconds after the interface failover occurred.

It is recommended to modify the VPNMonitor settings so that the SA would mark itself down in a shorter timeframe. If you choose an interval of 2 seconds, and a threshold of 2, the SA would mark itself down 4 seconds after interface failover occurs.

Ns204→ set vpnmonitor threshold 2
Interface Failover with Route Based VPNs

Ns204-> set vpnmonitor interval 2
Ns204-> get vpnmonitor
Vpn monitor interval : 2(seconds)
Vpn monitor threshold: 2
Ns204->

Caution: Using the lowest interval and threshold may cause the VPN to go down before it actually should be. You should tweak this value after several trial and error cycles.

After the SA’s bound to the inactive interface marks itself down, the get sa on each side of the tunnel will look like the following:

**NS204:**

<table>
<thead>
<tr>
<th>HEX ID</th>
<th>Gateway</th>
<th>Port</th>
<th>Algorithm</th>
<th>SPI</th>
<th>Life:sec</th>
<th>kb</th>
<th>Sta</th>
<th>PID</th>
<th>vsys</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000001&lt;</td>
<td>2.2.2.1</td>
<td>500</td>
<td>esp:3des/sha1</td>
<td>0afcffd7</td>
<td>1209</td>
<td>unlim</td>
<td>I/I</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>00000001&gt;</td>
<td>2.2.2.1</td>
<td>500</td>
<td>esp:3des/sha1</td>
<td>3d982f16</td>
<td>1209</td>
<td>unlim</td>
<td>I/I</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>00000002&lt;</td>
<td>2.2.2.1</td>
<td>500</td>
<td>esp:3des/sha1</td>
<td>0afcffd8</td>
<td>2844</td>
<td>unlim</td>
<td>A/U</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>00000002&gt;</td>
<td>2.2.2.1</td>
<td>500</td>
<td>esp:3des/sha1</td>
<td>3d982f17</td>
<td>2844</td>
<td>unlim</td>
<td>A/U</td>
<td>-1</td>
<td>0</td>
</tr>
</tbody>
</table>

**NS208:**

<table>
<thead>
<tr>
<th>HEX ID</th>
<th>Gateway</th>
<th>Port</th>
<th>Algorithm</th>
<th>SPI</th>
<th>Life:sec</th>
<th>kb</th>
<th>Sta</th>
<th>PID</th>
<th>vsys</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000001&lt;</td>
<td>3.3.3.1</td>
<td>500</td>
<td>esp:3des/sha1</td>
<td>3d982f17</td>
<td>2843</td>
<td>unlim</td>
<td>A/U</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>00000001&gt;</td>
<td>3.3.3.1</td>
<td>500</td>
<td>esp:3des/sha1</td>
<td>0afcffd8</td>
<td>2843</td>
<td>unlim</td>
<td>A/U</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>00000002&lt;</td>
<td>1.1.1.1</td>
<td>500</td>
<td>esp:3des/sha1</td>
<td>3d982f16</td>
<td>1207</td>
<td>unlim</td>
<td>I/I</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>00000002&gt;</td>
<td>1.1.1.1</td>
<td>500</td>
<td>esp:3des/sha1</td>
<td>0afcffd7</td>
<td>1207</td>
<td>unlim</td>
<td>I/I</td>
<td>-1</td>
<td>0</td>
</tr>
</tbody>
</table>
Interface Failover with Route Based VPNs

Configuration for NS-204:

Total Config size 4468:
set clock timezone 0
set vrouter trust-vr sharable
unset vrouter "trust-vr" auto-route-export
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set admin name "netscreen"
set admin password "nKVUM2rwMUzPcrkG5sWIHdCtqkAIbn"
set admin auth timeout 10
set admin auth server "Local"
set admin format dos
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "MGT" block
set zone "DMZ" tcp-rst
set zone "VLAN" block
set zone "VLAN" tcp-rst
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set interface "ethernet1" zone "Trust"
set interface "ethernet2" zone "DMZ"
set interface "ethernet3" zone "Untrust"
set interface "ethernet4" zone "Untrust"
set interface "tunnel.1" zone "Untrust"
set interface "tunnel.2" zone "Untrust"
unset interface vlan1 ip
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 route
set interface ethernet4 ip 3.3.3.1/24
set interface ethernet4 route
set interface tunnel.1 ip unnumbered interface ethernet3
set interface tunnel.2 ip unnumbered interface ethernet4
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet1 ip manageable
set interface ethernet3 ip manageable
set interface ethernet4 ip manageable
set interface ethernet3 manage ping
set interface ethernet3 manage ssh
set interface ethernet3 manage telnet
set interface ethernet3 manage snmp
set interface ethernet3 manage ssl
set interface ethernet3 manage web
set interface ethernet4 manage ping
set interface ethernet4 manage ssh
set interface ethernet4 manage telnet
set interface ethernet4 manage snmp
set interface ethernet4 manage ssl
set interface ethernet4 manage web
set interface ethernet3 monitor track-ip ip
set interface ethernet3 monitor track-ip threshold 100
set interface ethernet3 monitor track-ip weight 50
set interface ethernet3 monitor track-ip ip 2.2.2.100 weight 50
Interface Failover with Route Based VPNs

set interface ethernet3 monitor track-ip ip 2.2.2.10 weight 60
unset interface ethernet3 monitor track-ip dynamic
set interface ethernet3 monitor threshold 40
unset flow tcp-syn-check
set hostname ns204
set vpmmonitor interval 2
set vpmmonitor threshold 2
set ike gateway "ns208gw primary" address 2.2.2.1 Main outgoing-interface "ethernet3"
preshare "XF3N5aRHN6n3KsVh4CnxXpP4nnCdibC1iw==" sec-level standard
set ike gateway "ns208gw backup" address 2.2.2.1 Main outgoing-interface "ethernet4"
preshare "ITBkIkGGNe7AuOsZ04CBvEKyQuun42FRA==" sec-level standard
set ike respond-bad-spi 1
set vpn "ns208vpn primary" gateway "ns208gw primary" no-replay tunnel idletime 0 sec-level standard
set vpn "ns208vpn primary" monitor optimized rekey
set vpn "ns208vpn primary" id 3 bind interface tunnel.1
set vpn "ns208vpn backup" gateway "ns208gw backup" no-replay tunnel idletime 0 sec-level standard
set vpn "ns208vpn backup" monitor optimized rekey
set vpn "ns208vpn backup" id 2 bind interface tunnel.2
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set url protocol sc-cpa
exit
set policy id 1 from "Trust" to "Untrust" "Any" "Any" "ANY" permit
set policy id 2 from "Untrust" to "Trust" "Any" "Any" "ANY" permit
set vpn "ns208vpn primary" proxy-id local-ip 10.1.1.0/24 remote-ip 172.16.10.0/24 "ANY"
set vpn "ns208vpn backup" proxy-id local-ip 10.1.1.0/24 remote-ip 172.16.10.0/24 "ANY"
set nsmgmt bulkcli reboot-timeout 60
set ssh version v2
set config lock timeout 5
set dl-buf size 4718592
set snmp port listen 161
set snmp port trap 162
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
set route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.254
set route 0.0.0.0/0 interface ethernet4 gateway 3.3.3.254 metric 10
set route 172.16.10.0/24 interface tunnel.1
set route 172.16.10.0/24 interface tunnel.2 metric 10
exit
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
Interface Failover with Route Based VPNs

Configuration for NS-208:

```
set clock timezone 0
set vrouter "trust-vr" sharable
unset vrouter "trust-vr" auto-route-export
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set admin name "netscreen"
set admin password "nKVUMz+WMUzPcrkG5sWtHdCtqkAibn"
set admin auth timeout 10
set admin auth server "Local"
set admin format dos
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "MGT" block
set zone "DMZ" tcp-rst
set zone "VLAN" block
set zone "VLAN" tcp-rst
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set interface "ethernet1" zone "Trust"
set interface "ethernet2" zone "DMZ"
set interface "ethernet3" zone "Untrust"
set interface "tunnel.1" zone "Untrust"
set interface "tunnel.2" zone "Untrust"
unset interface vlan1 ip
set interface ethernet1 ip 172.16.10.1/24
set interface ethernet1 nat
set interface ethernet3 ip 2.2.2.1/24
set interface ethernet3 route
set interface tunnel.1 ip unnumbered interface ethernet3
set interface tunnel.2 ip unnumbered interface ethernet3
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet1 ip manageable
set interface ethernet3 ip manageable
set interface ethernet3 manage ping
set interface ethernet3 manage ssh
set interface ethernet3 manage telnet
set interface ethernet3 manage snmp
set interface ethernet3 manage web
unset flow no-tcp-seq-check
set flow tcp-syn-check
set hostname ns208
set vpmmonitor interval 2
set vpmmonitor threshold 2
set ike gateway "ns204gw primary" address 3.3.3.1 Main outgoing-interface "ethernet3"
preshare "OLdPT1r7NtYVfL3sAaAlC17/7uwonvOBOB38g==" sec-level standard
set ike gateway "ns204gw backup" address 1.1.1.1 Main outgoing-interface "ethernet3"
preshare "vHOMOQhPNY+kVqscB69RCXV7tM2LOKdKQ==" sec-level standard
set ike respond-bad-spi 1
set vpn "ns204vpn primary" gateway "ns204gw primary" no-replay tunnel idle-time 0 sec-level standard
set vpn "ns204vpn primary" monitor optimized rekey
set vpn "ns204vpn primary" id 1 bind interface tunnel.1
set vpn "ns204vpn backup" gateway "ns204gw backup" no-replay tunnel idle-time 0 sec-level standard
set vpn "ns204vpn backup" monitor optimized rekey
```
Interface Failover with Route Based VPNs

```
set vpn "ns204vpn backup" id 2 bind interface tunnel.2
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set url protocol sc-cpa
set cache size 500
exit

set policy id 1 from "Trust" to "Untrust"  "Any" "Any" "ANY" permit
set policy id 2 from "Untrust" to "Trust"  "Any" "Any" "ANY" permit
set vpn "ns204vpn primary" proxy-id local-ip 172.16.10.0/24 remote-ip 10.1.1.0/24 "ANY"
set vpn "ns204vpn backup" proxy-id local-ip 172.16.10.0/24 remote-ip 10.1.1.0/24 "ANY"
set nsmgmt bulkcli reboot-timeout 60
set ssh version v2
set config lock timeout 5
set dl-buf size 4718592
set snmp port listen 161
set snmp port trap 162
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
set route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.254
set route 10.1.1.0/24 interface tunnel.1
set route 10.1.1.0/24 interface tunnel.2
exit
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
```