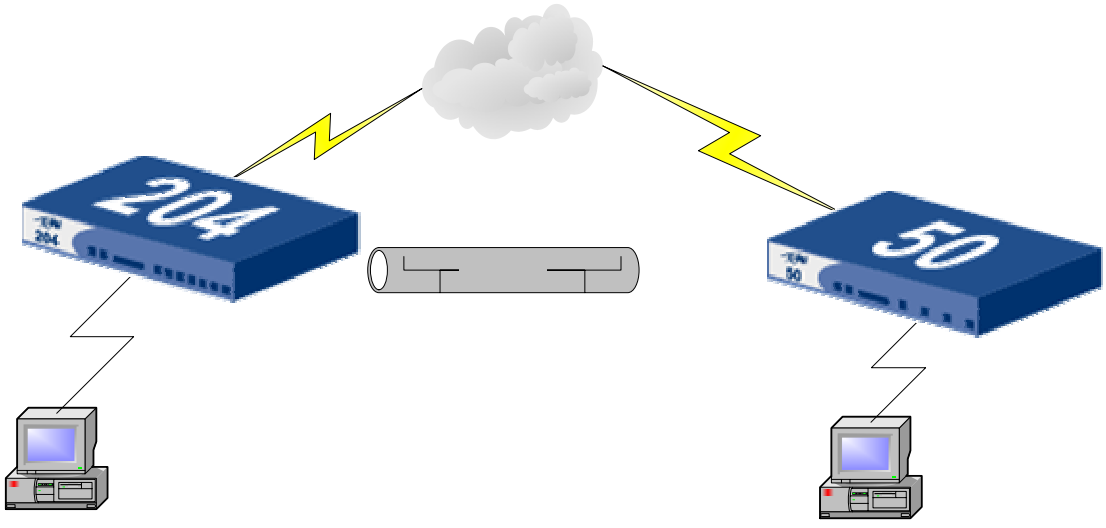
Route Based VPN Configurations to Hide the Private IP Behind one Private IP

Version 1.0
ScreenOS 5.0.0 and higher

Purpose
This paper goes through the basic procedure of configuring a Route Based LAN to LAN VPN with the requirement of hiding (or masquerading) all the private IP addresses behind one public IP address. This would be similar to policy based NAT, but for a tunnel interface

Requirement
Only requirement is the NetScreen device used must support route based VPN. Configuration will require use of a numbered tunnel interface. This example applies to ScreenOS 5.0.0 and higher.

Example



Assume we need to hide all of the 10.1.1.0/24 LAN from the NS-204 side. We will hide all the 10.1.1.0/24 PC's behind the tunnel interface address 50.50.50.1. In other words, the NS-204 will see all traffic from the trust side of the NS-208 as 50.50.50.1.

NS-204 Network Configurations

Configure Tunnel Interface

A numbered tunnel interface needs to be created. We will assign an IP address 50.50.50.1/24 to that tunnel interface. Additionally, we will bind this tunnel interface to the untrust zone, so that we can specify policy based NAT from trust to untrust through the tunnel interface as the egress interface.

Set interface tunnel.1 zone untrust
Set interface tunnel.1 ip 50.50.50.1/24

Route Traffic through the Tunnel Interface

The route table on the NetScreen must reflect that packets destined for the 172.16.10.0/24 network must traverse through the tunnel.1 interface.

Set route 172.16.10.0/24 interface tunnel.1

Configure Phase 1 IKE Gateway

set ike gate NS50GW address 2.2.2.1 main outgoing-interface ethernet3 preshare netscreen sec-level compatible

Configure Phase 2 VPN

Set vpn “NS50-VPN” gateway “NS50GW” no-replay tunnel idletime 0 sec-level compatible
Set vpn “NS50-VPN” monitor optimized rekey
Set vpn “NS50-VPN” id 1 bind interface tunnel.1
Set vpn “NS50-VPN” proxy-id local-ip 10.1.1.0/24 remote-ip 172.16.10.0/24 any

Configure the Policy

Now configure the policy to both allow the encrypted traffic to go through the NetScreen, and to nat the source IP address to the egress interface, which in this case is the tunnel interface:

Set policy from trust to untrust 10.1.1.0/24 172.16.10.0/24 any nat src permit

Note: Since this is a many to 1 NAT condition, traffic can only be initiated from the NS208 side (i.e. one way VPN tunnel).

NS-50 Network Configurations

Configure Tunnel Interface

The tunnel interface configuration on the NS-204 side will be very similar. Since we don't care about NAT'ing on this side, we can simply choose to configure a unnumbered tunnel interface, where the tunnel interface will borrow the IP address of another interface (in this example, we bind the tunnel interface to the interface ethernet3, and borrow the IP address of ethernet3 to assign the IP address to the tunnel interface).

Set interface tunnel.1 zone untrust
Set interface tunnel.1 ip unnumbered interface ethernet3

Route Traffic through the Tunnel Interface

The route table on the NetScreen must reflect that packets destined for the mipped address which would be the 50.50.50.0/24 network. This network must traverse through the tunnel.1 interface.

Set route 50.50.50.0/24 interface tunnel.1

Configure Phase 1 IKE Gateway

set ike gate NS204GW address 2.2.2.1 main outgoing-interface ethernet3 preshare netscreen sec-level compatible

Configure Phase 2 VPN

Set vpn "NS50-VPN" gateway "NS50GW" no-replay tunnel idletime 0 sec-level compatible
Set vpn "NS50-VPN" monitor optimized rekey
Set vpn "NS50-VPN" id 1 bind interface tunnel.1
Set vpn "NS50-VPN" proxy-id local-ip 172.16.10.0/24 remote-ip 10.1.1.0/24 any

Configure the Policy

Since the packets coming through the VPN will appear as the tunnel interface address from the other side of the tunnel, the ingress policy needs to reflect that specific IP address.

Set policy from untrust to trust 50.50.50.0/24 172.16.10.0/24 Any permit

Traffic should now be able to traverse through the VPN tunnel, and all packets will appear as they are coming from IP address 50.50.50.1.

NS-204 Configuration File:

```
ns204-> get config
Total Config size 2961:
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 "tunnel.1" 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 tunnel.1 ip 50.50.50.1/24
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet1 ip manageable
set interface ethernet3 ip manageable
set interface ethernet2 manage ssh
set interface ethernet2 manage telnet
set interface ethernet2 manage snmp
set interface ethernet2 manage ssl
set interface ethernet2 manage web
set console page 0
set hostname ns204
```

```
set address "Trust" "10.1.1.0/24" 10.1.1.0 255.255.255.0
set address "Untrust" "172.16.10.0/24" 172.16.10.0 255.255.255.0
set ike gateway "NS50GW" address 2.2.2.1 Main outgoing-interface "ethernet3" preshare
"qxIeJRaRNsLtqHscg0CUeh7lg0nF4DRybQ==" sec-level compatible
set ike respond-bad-spi 1
set vpn "NS50-VPN" gateway "NS50GW" no-replay tunnel idletime 0 sec-level compatible
set vpn "NS50-VPN" monitor optimized rekey
set vpn "NS50-VPN" id 1 bind interface tunnel.1
set policy id 1 from "Trust" to "Untrust"  "10.1.1.0/24" "172.16.10.0/24" "ANY" nat src permit log
set policy id 2 from "Untrust" to "Trust"  "172.16.10.0/24" "10.1.1.0/24" "ANY" permit log
set vpn "NS50-VPN" proxy-id local-ip 10.1.1.0/24 remote-ip 172.16.10.0/24 "ANY"
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set ssh version v2
set config lock timeout 5
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  172.16.10.0/24 interface tunnel.1
set route  0.0.0.0/0 interface ethernet3 gateway 2.2.2.1
exit
```

NS-50 Configuration File:

```
ns50-> get config
Total Config size 3268:
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 "tunnel.1" zone "Untrust"
set interface vlan1 ip 192.168.1.1/24
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
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface vlan1 ip manageable
set interface ethernet1 ip manageable
set interface ethernet3 ip manageable
set interface ethernet2 manage ssh
set interface ethernet2 manage telnet
set interface ethernet2 manage snmp
set interface ethernet2 manage ssl
set interface ethernet2 manage web
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 console page 0
set hostname ns50
set address "Trust" "172.16.10.0/24" 172.16.10.0 255.255.255.0
set address "Untrust" "10.1.1.0/24" 10.1.1.0 255.255.255.0
set address "Untrust" "50.50.50.0/24" 50.50.50.0 255.255.255.0
set ike gateway "NS204GW" address 1.1.1.1 Main outgoing-interface "ethernet3" preshare
"glee/aW9NF5SuBsBtXCXEkxsXPnLoJ2eQg==" sec-level compatible
set ike respond-bad-spi 1
set vpn "NS204 VPN" gateway "NS204GW" no-replay tunnel idletime 0 sec-level compatible
set vpn "NS204 VPN" monitor optimized rekey
set vpn "NS204 VPN" id 3 bind interface tunnel.1
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set policy id 0 from "Trust" to "Untrust"  "172.16.10.0/24" "10.1.1.0/24" "ANY" permit
set policy id 1 from "Untrust" to "Trust"  "50.50.50.0/24" "172.16.10.0/24" "ANY" permit
set vpn "NS204 VPN" proxy-id local-ip 172.16.10.0/24 remote-ip 10.1.1.0/24 "ANY"
set ssh version v2
set config lock timeout 5
set snmp name "ns50"
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  50.50.50.0/24 interface tunnel.1
exit
```