6WIND VPN Concentrator Deployment Guide

Release 3.0

6WIND

Mar 10, 2021

Contents

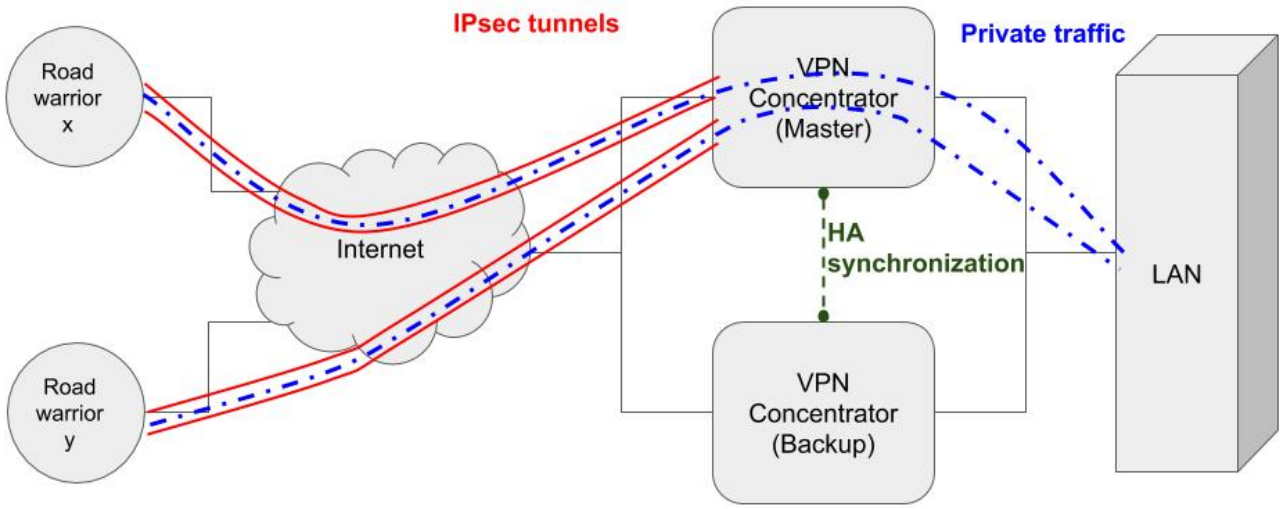
1. Overview

The purpose of this document is to guide the user in deploying the vRouter for a VPN concentrator use case. It focuses on the concepts that are relevant to this specific use case, in order to provide a practical example. Exhaustive documentation of the vRouter features that are not covered in the use case can be found in the standard vRouter documentation (https://doc.6wind.com/turbo-router-3.x/).

Follow the Getting Started guide (https://doc.6wind.com/turbo-router-3.x/getting-started/index.html) to install the software in your environment and get a remote console with SSH.

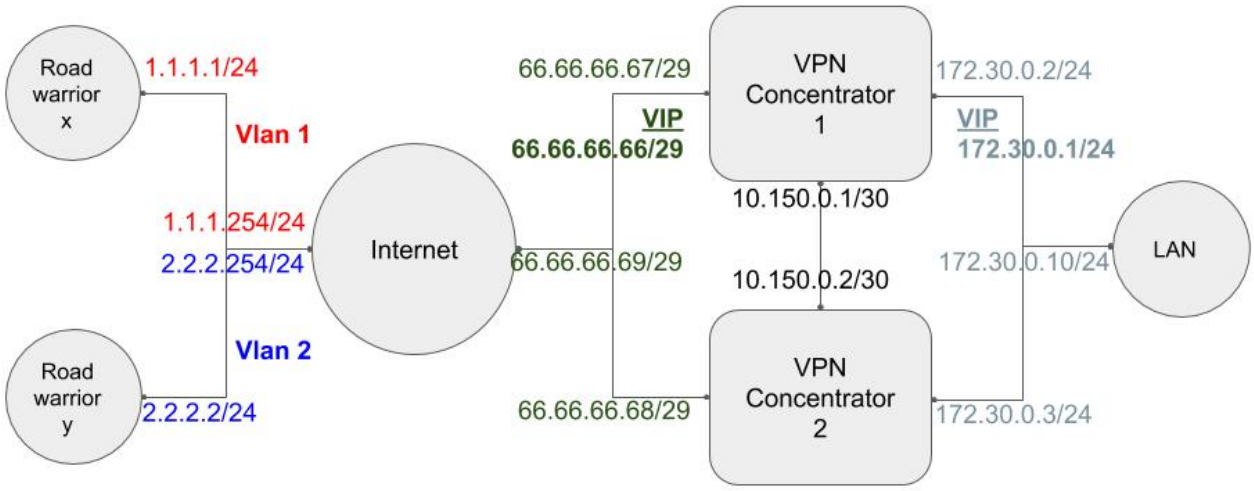
2. Use case: VPN concentrator with roadwarriors

2.1 Overview



A VPN Concentrator is a component of a company's network architecture, whose role is to offer on-demand VPN access to private resources (in LAN/WAN) intended for employees connecting from arbitrary access points over the Internet. In the IPSEC (Internet Protocol Security) terminology, the so connected employees are referred to as "road warriors"; this term will be used in the rest of this document to refer to clients connecting to the VPN Concentrator.

2.2 Platform description



The key element in this use case is the VPN Concentrator. It should naturally have access to the resources located in the private network, on one hand; and access to the Internet, on the other hand.

In order to provide HA (High Availability), we will have 2 vRouter appliances running as VRRP (Virtual Router Redundancy Protocol) master/backup with synchronized IKE (Internet Key Exchange) SAs (Security Associations), IPsec counters and address pools.

Each road warrior will use a vRouter appliance. It should have a public IP address attributed by its ISP and will also receive a private address from the pool configured on the VPN concentrator, upon IKE negotiations.

Road warriors connect to the VPN Concentrator through the Internet. One node running a vRouter will represent the Internet. It is the road warriors' default gateway; and advertises routes via BGP (Border Gateway Protocol) to the VPN concentrators.

The target resources sought by road warriors are located in the LAN. They will be represented by a Linux VM (Virtual Machine).

2.3 Configuration

2.3.1 License

For each vRouter node of this setup, follow the Getting Started guide (https://doc.6wind.com/turbo-router-3.x/getting-started/index.html) to provide a minimal Day-1 configuration and install a valid and relevant license.

A valid Turbo IPsec Application License is required. Using `show license`, check that IPSEC is `activated`.

```
vrouter> show license
Active perpetual license for Turbo Router
Current activations 2/2
Connected to license server
Serial number is xxxxxxxxxxxxxx
Computer ID is 1QdTFhWxVSh47fooo+iA
License was activated online
Support is valid until Thu Dec 31 07:00:00 2020 (standard mode)
Max throughput 10.0G (currently used 0.0G)
IPsec activated for 10 tunnels (currently used 0)
```

2.3.2 Network connectivity

VPN Concentrator node

Note: The following configuration is for the VRRP Master node; the matching Backup configuration should be set on the VRRP Backup node.

Hostname

Using the vRouter CLI (Command Line Interface), let us start with setting the hostname.

```
vrouter> edit running
vrouter running config# system hostname concentrator1-vm
vrouter running config# commit
concentrator1-vm running config#
```

Interfaces

Allocate the ports that will be involved in data plane processing into the fast path:

```
concentrator1-vm running config# / system fast-path
concentrator1-vm running fast-path#! port pci-b0s4
concentrator1-vm running fast-path# port pci-b0s5
concentrator1-vm running fast-path# port pci-b0s6
```

After wiping the Day-1 configuration, set up the corresponding physical interfaces: one to connect to the internet, with a public IP address; another one to connect to the LAN; and yet another one that will be used to exchange HA synchronization data between Master and Backup nodes.

```
concentrator1-vm running fast-path# del / vrf main
concentrator1-vm running fast-path# / vrf main
concentrator1-vm running vrf main# interface physical ntfp1
concentrator1-vm running physical ntfp1#! port pci-b0s4
concentrator1-vm running physical ntfp1# description ISP
concentrator1-vm running physical ntfp1# ipv4 address 66.66.66.67/29
concentrator1-vm running physical ntfp1# .. physical ntfp2
concentrator1-vm running physical ntfp2#! port pci-b0s5
concentrator1-vm running physical ntfp2# description LAN
concentrator1-vm running physical ntfp2# ipv4 address 172.30.0.2/24
concentrator1-vm running physical ntfp2# .. physical ntfp3
concentrator1-vm running physical ntfp3#! port pci-b0s6
concentrator1-vm running physical ntfp3# description IKE_HA
concentrator1-vm running physical ntfp3# ipv4 address 10.150.0.1/30
```

Review the configuration and commit it:

```
concentrator1-vm running physical ntfp3# show config nodefault /
vrf main
    interface
        physical ntfp1
            port pci-b0s4
            description ISP
(...)
concentrator1-vm running physical ntfp3# commit
Configuration committed.
```


See also:

The User's Guide for more information about:

- CLI basics (https://doc.6wind.com/turbo-router-3.x/user-guide/cli/basics/index.html)
- Fast path configuration (https://doc.6wind.com/turbo-router-3.x/user-guide/cli/system/fast-path.html)
- Ethernet interfaces configuration (https://doc.6wind.com/turbo-router-3.x/user-guide/cli/network-interface/types/ethernet.html)

DNS

The VPN concentrators require a valid DNS server to contact the license server:

```
concentrator1-vm running physical ntfp3# / vrf main dns server 8.8.8.8
concentrator1-vm running physical ntfp3# commit
Configuration committed.
```

VRRP

For VRRP, we will need to set a virtual IP address that will be the unique VPN address for road warriors, and a virtual IP address on the LAN side as well. The two instances should be grouped together in order to always have both virtual IPs (VIPs) associated with the same node.

Note: `priority` should be set to 150 on the Master node and left to its default value (100) on the Backup node.

While we are at VRRP, let's go one step ahead and configure HA for IKE — although it is not needed for bare network connectivity, and could be added later. Our VRRP group will control the HA state, meaning that the VRRP state (Master or Backup) will be the HA state for IKE, and any later change on the VRRP state will be replicated on IKE HA.

```
concentrator1-vm running physical ntfp3# / vrf main interface vrrp vrrp_lan
concentrator1-vm running vrrp vrrp_lan#! link-interface ntfp2
concentrator1-vm running vrrp vrrp_lan#! vrid 1
concentrator1-vm running vrrp vrrp_lan# priority 150
concentrator1-vm running vrrp vrrp_lan# preempt-delay 60
concentrator1-vm running vrrp vrrp_lan# track-fast-path true
concentrator1-vm running vrrp vrrp_lan# virtual-address 172.30.0.1/24
concentrator1-vm running vrrp vrrp_lan# .. vrrp vrrp_public
concentrator1-vm running vrrp vrrp_public#! link-interface ntfp1
concentrator1-vm running vrrp vrrp_public#! vrid 2
concentrator1-vm running vrrp vrrp_public# priority 150
concentrator1-vm running vrrp vrrp_public# preempt-delay 60
concentrator1-vm running vrrp vrrp_public# track-fast-path true
concentrator1-vm running vrrp vrrp_public# virtual-address 66.66.66.66/29
```

(continues on next page)

(continued from previous page)

```
concentrator1-vm running vrrp vrrp_public# / vrf main vrrp
concentrator1-vm running vrrp# router-id concentrator1-vm
concentrator1-vm running vrrp# group vrrp_group
concentrator1-vm running group vrrp_group# instance vrrp_lan
concentrator1-vm running group vrrp_group# instance vrrp_public
concentrator1-vm running group vrrp_group# notify-ha-group ha_for_ike
concentrator1-vm running group vrrp_group#! / ha group ha_for_ike
concentrator1-vm running group ha_for_ike# commit
Configuration committed.
```

See also:

The User's Guide for more information about:

- VRRP (https://doc.6wind.com/turbo-router-3.x/user-guide/cli/high-availability/vrrp.html)
- HA Groups (https://doc.6wind.com/turbo-router-3.x/user-guide/cli/high-availability/ha-group.html)

Routing

Our VPN Concentrators are directly connected to the LAN, so there is no particular routing configuration to add on the LAN side.

On the other hand, we will need to configure a BGP peering with the Internet node in order to get routes to the road warriors. No routes need to be announced from the VPN Concentrators to the internet, so we will filter out connected subnets in EBGP (External BGP) and include them in IBGP (Internal BGP).

```
concentrator1-vm running group ha_for_ike# / vrf main routing bgp
concentrator1-vm running bgp#! as 65001
concentrator1-vm running bgp# router-id 66.66.66.67
concentrator1-vm running bgp# address-family ipv4-unicast redistribute connected
concentrator1-vm running bgp# neighbor 66.66.66.68
concentrator1-vm running neighbor 66.66.66.68#! remote-as 65001
concentrator1-vm running neighbor 66.66.66.68# neighbor-description concentrator2-
↪vm
concentrator1-vm running neighbor 66.66.66.68# address-family ipv4-unicast
concentrator1-vm running ipv4-unicast# nexthop-self force true
concentrator1-vm running ipv4-unicast# soft-reconfiguration-inbound true
concentrator1-vm running ipv4-unicast# .. .. .. neighbor 66.66.66.69
concentrator1-vm running neighbor 66.66.66.69#! remote-as 65002
concentrator1-vm running neighbor 66.66.66.69# neighbor-description ISP
concentrator1-vm running neighbor 66.66.66.69# address-family ipv4-unicast
concentrator1-vm running ipv4-unicast# prefix-list out prefix-list-name deny_any_
↪ipv4
concentrator1-vm running ipv4-unicast#! prefix-list in prefix-list-name filter_
↪bogons
concentrator1-vm running ipv4-unicast#! soft-reconfiguration-inbound true
concentrator1-vm running ipv4-unicast#! / routing
concentrator1-vm running routing#! ipv4-prefix-list deny_any_ipv4 seq 10 address 0.
↪0.0.0/0 policy deny
```

(continues on next page)

(continued from previous page)

```
concentrator1-vm running routing#! ipv4-prefix-list filter_bogons
concentrator1-vm running ipv4-prefix-list filter_bogons#! seq 5 address 0.0.0.0/8␣
↪policy deny le 32
concentrator1-vm running ipv4-prefix-list filter_bogons# seq 10 address 10.0.0.0/8␣
↪policy deny le 32
concentrator1-vm running ipv4-prefix-list filter_bogons# seq 15 address 127.0.0.0/
↪8 policy deny le 32
concentrator1-vm running ipv4-prefix-list filter_bogons# seq 20 address 169.254.0.
↪0/16 policy deny le 32
concentrator1-vm running ipv4-prefix-list filter_bogons# seq 25 address 172.16.0.0/
↪12 policy deny le 32
concentrator1-vm running ipv4-prefix-list filter_bogons# seq 30 address 192.168.0.
↪0/16 policy deny le 32
concentrator1-vm running ipv4-prefix-list filter_bogons# seq 35 address 224.0.0.0/
↪3 policy deny le 32
concentrator1-vm running ipv4-prefix-list filter_bogons# seq 40 address 0.0.0.0/0␣
↪policy permit le 32
concentrator1-vm running ipv4-prefix-list filter_bogons# commit
Configuration committed.
```

See also:

The User's Guide for more information about:

- BGP (https://doc.6wind.com/turbo-router-3.x/user-guide/cli/routing/bgp/index.html)
- IP Prefixes (https://doc.6wind.com/turbo-router-3.x/user-guide/cli/routing/tools.html#ip-prefix-list)

Troubleshooting

After committing the configuration on both VPN Concentrator nodes, we can check basic connectivity between the two VPN Concentrator nodes and the state of VRRP.

```
concentrator1-vm running ipv4-prefix-list filter_bogons# exit
concentrator1-vm> show interface details
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default␣
↪qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST> mtu 1500 qdisc fq_codel state DOWN group default␣
↪qlen 1000
    link/ether de:ad:de:01:02:03 brd ff:ff:ff:ff:ff:ff
6: ntfp1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group␣
↪default qlen 1000
    link/ether de:ed:01:71:da:ed brd ff:ff:ff:ff:ff:ff
    inet 66.66.66.67/29 scope global ntfp1
```

(continues on next page)

(continued from previous page)

```
       valid_lft forever preferred_lft forever
    inet6 fe80::dced:1ff:fe71:daed/64 scope link
       valid_lft forever preferred_lft forever
7: ntfp2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group␣
↪default qlen 1000
    link/ether de:ed:02:18:7f:04 brd ff:ff:ff:ff:ff:ff
    inet 172.30.0.2/24 scope global ntfp2
       valid_lft forever preferred_lft forever
    inet6 fe80::dced:2ff:fe18:7f04/64 scope link
       valid_lft forever preferred_lft forever
8: ntfp3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group␣
↪default qlen 1000
    link/ether de:ed:03:b6:8f:aa brd ff:ff:ff:ff:ff:ff
    inet 10.150.0.1/30 scope global ntfp3
       valid_lft forever preferred_lft forever
    inet6 fe80::dced:3ff:feb6:8faa/64 scope link
       valid_lft forever preferred_lft forever
9: vrrp_lan@ntfp2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state␣
↪UP group default qlen 1000
    link/ether 00:00:5e:00:01:01 brd ff:ff:ff:ff:ff:ff
    inet 172.30.0.1/24 scope global vrrp_lan
       valid_lft forever preferred_lft forever
10: vrrp_public@ntfp1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue␣
↪state UP group default qlen 1000
    link/ether 00:00:5e:00:01:02 brd ff:ff:ff:ff:ff:ff
    inet 66.66.66.66/29 scope global vrrp_public
       valid_lft forever preferred_lft forever
concentrator1-vm> cmd ping 10.150.0.2 count 4
PING 10.150.0.2 (10.150.0.2) 56(84) bytes of data.
64 bytes from 10.150.0.2: icmp_seq=1 ttl=64 time=1.11 ms
64 bytes from 10.150.0.2: icmp_seq=2 ttl=64 time=0.187 ms
64 bytes from 10.150.0.2: icmp_seq=3 ttl=64 time=0.197 ms
64 bytes from 10.150.0.2: icmp_seq=4 ttl=64 time=0.237 ms

--- 10.150.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3055ms
rtt min/avg/max/mdev = 0.187/0.433/1.114/0.394 ms
concentrator1-vm>
```

VRRP state on VPN Concentrator 1:

```
concentrator1-vm> show state vrf main vrrp
vrrp
    enabled true
    router-id concentrator1-vm
    traps-enabled false
    group vrrp_group
        instance vrrp_lan
        instance vrrp_public
```

(continues on next page)

(continued from previous page)

```
        notify-ha-group ha_for_ike
        state master
        ..
    ..
concentrator1-vm>
```

VRRP interfaces state on VPN Concentrator 1:

```
concentrator1-vm> show state vrf main interface vrrp
vrrp vrrp_lan
    mtu 1500
    promiscuous false
    enabled true
    oper-status UP
    counters
        in-octets 0
        in-unicast-pkts 2
        in-discards 0
        in-errors 0
        out-octets 24180
        out-unicast-pkts 450
        out-discards 0
        out-errors 0
        ..
    ipv4
        address 172.30.0.1/24
        ..
    ethernet
        mac-address 00:00:5e:00:01:01
        ..
    state master
    version 2
    link-interface ntfp2
    garp-delay 5
    use-vmac true
    vmac-xmit-base false
    vrid 1
    priority 150
    init-state backup
    preempt true
    preempt-delay 60
    advertisement-interval 1000
    track-fast-path true
    virtual-address 172.30.0.1/24
    ..
vrrp vrrp_public
    mtu 1500
    promiscuous false
    enabled true
```

(continues on next page)

(continued from previous page)

```
    oper-status UP
    counters
        in-octets 756
        in-unicast-pkts 20
        in-discards 0
        in-errors 0
        out-octets 24180
        out-unicast-pkts 450
        out-discards 0
        out-errors 0
        ..
    ipv4
        address 66.66.66.66/29
        ..
    ethernet
        mac-address 00:00:5e:00:01:02
        ..
    state master
    version 2
    link-interface ntfp1
    garp-delay 5
    use-vmac true
    vmac-xmit-base false
    vrid 2
    priority 150
    init-state backup
    preempt true
    preempt-delay 60
    advertisement-interval 1000
    track-fast-path true
    virtual-address 66.66.66.66/29
    ..
concentrator1-vm>
```

VRRP state on VPN Concentrator 2:

```
concentrator2-vm running ipv4-prefix-list filter_bogons# exit
concentrator2-vm> show state vrf main vrrp
vrrp
    enabled true
    router-id concentrator2-vm
    traps-enabled false
    group vrrp_group
        instance vrrp_lan
        instance vrrp_public
        notify-ha-group ha_for_ike
        state backup
        ..
    ..
concentrator2-vm>
```


VRRP interfaces state on VPN Concentrator 2:

```
concentrator2-vm> show state vrf main interface vrrp
vrrp vrrp_lan
    mtu 1500
    promiscuous false
    enabled true
    oper-status UP
    counters
        in-octets 0
        in-unicast-pkts 493
        in-discards 0
        in-errors 0
        out-octets 108
        out-unicast-pkts 2
        out-discards 0
        out-errors 0
        ..
    ethernet
        mac-address 00:00:5e:00:01:01
        ..
    state backup
    version 2
    link-interface ntfp2
    garp-delay 5
    use-vmac true
    vmac-xmit-base false
    vrid 1
    priority 100
    init-state backup
    preempt true
    preempt-delay 60
    advertisement-interval 1000
    track-fast-path true
    virtual-address 172.30.0.1/24
    ..
vrrp vrrp_public
    mtu 1500
    promiscuous false
    enabled true
    oper-status UP
    counters
        in-octets 1050
        in-unicast-pkts 518
        in-discards 0
        in-errors 0
        out-octets 108
        out-unicast-pkts 2
        out-discards 0
        out-errors 0
        ..
```

(continues on next page)

(continued from previous page)

```
    ethernet
        mac-address 00:00:5e:00:01:02
        ..
    state backup
    version 2
    link-interface ntfp1
    garp-delay 5
    use-vmac true
    vmac-xmit-base false
    vrid 2
    priority 100
    init-state backup
    preempt true
    preempt-delay 60
    advertisement-interval 1000
    track-fast-path true
    virtual-address 66.66.66.66/29
    ..
concentrator2-vm>
```

The routing table should look like this at this point (the Internet node is not configured yet):

```
concentrator1-vm> show ipv4-routes
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route


VRF main:
C>* 10.150.0.0/30 is directly connected, ntfp3, 00:09:44
C * 66.66.66.64/29 is directly connected, vrrp_public, 00:09:31
C>* 66.66.66.64/29 is directly connected, ntfp1, 00:09:44
C * 172.30.0.0/24 is directly connected, vrrp_lan, 00:09:31
C>* 172.30.0.0/24 is directly connected, ntfp2, 00:09:44
concentrator1-vm>
```

Road warrior node

Interfaces

On the road warriors, we basically need to configure one VLAN (Virtual Local Area Network) interface with a public IP address (make sure to wipe the Day-1 configuration first).

```
vrouter> edit running
vrouter running config# system
```

(continues on next page)

(continued from previous page)

```
vrouter running system# hostname warrior1-vm
vrouter running system# fast-path port pci-b0s4
vrouter running system# del / vrf main
vrouter running system# / vrf main interface physical ntfp1 port pci-b0s4
vrouter running system# / vrf main interface vlan int_vlan1
vrouter running vlan int_vlan1#! description ISP
vrouter running vlan int_vlan1#! ipv4 address 1.1.1.1/24
vrouter running vlan int_vlan1#! vlan-id 1
vrouter running vlan int_vlan1#! link-interface ntfp1
vrouter running vlan int_vlan1# commit
Configuration committed.
```

DNS

The road warriors require a valid DNS server to contact the license server:

```
warrior1-vm vlan int_vlan# / vrf main dns server 8.8.8.8
warrior1-vm vlan int_vlan# commit
Configuration committed.
```

Routing

Routing will just consist of adding a static route pointing to the Internet node in order to declare it as a default gateway.

```
warrior1-vm running vlan int_vlan1# / vrf main routing static ipv4-route 0.0.0.0/0␣
↪next-hop 1.1.1.254
warrior1-vm running vlan int_vlan1# commit
Configuration committed.
```

See also:

The User's Guide for more information about:

- VLAN interfaces (https://doc.6wind.com/turbo-router-3.x/user-guide/cli/network-interface/types/vlan.html)
- static routes (https://doc.6wind.com/turbo-router-3.x/user-guide/cli/routing/static-routes.html)

Troubleshooting

After committing the configuration, we can check the routing table of the road warrior and make sure 1.1.1.254 is the default gateway

```
warrior1-vm running vlan int_vlan1# exit
warrior1-vm> show ipv4-routes
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route


VRF main:
S>* 0.0.0.0/0 [1/0] via 1.1.1.254, int_vlan1, 00:00:13
C>* 1.1.1.0/24 is directly connected, int_vlan1, 00:01:28
warrior1-vm>
```

Internet node

Interfaces

This node will connect road warriors to the VPN Concentrators, so it must have a VLAN interface per road warrior (it will be its default gateway), an interface in the same IP subnet as the VPN Concentrators, and an interface enabling access to Internet.

```
vrouter> edit running
vrouter running config# system
vrouter running system# hostname internet-vm
vrouter running system# fast-path
vrouter running fast-path#! port pci-b0s3
vrouter running fast-path# port pci-b0s4
vrouter running fast-path# port pci-b0s5
vrouter running fast-path# del / vrf main
vrouter running fast-path# / vrf main interface physical internet
vrouter running physical internet#! port pci-b0s3
vrouter running physical internet# description internet_wan_access
vrouter running physical internet# ipv4 dhcp enabled true
vrouter running physical internet# .. physical ntfp1
vrouter running physical ntfp1#! port pci-b0s4
vrouter running physical ntfp1# description interco_roadwarriors
vrouter running physical ntfp1# .. physical ntfp2
vrouter running physical ntfp2#! port pci-b0s5
vrouter running physical ntfp2# description interco_concentrators
vrouter running physical ntfp2# ipv4 address 66.66.66.69/29
vrouter running physical ntfp2# .. vlan int_vlan1
vrouter running vlan int_vlan1#! description "ipsec roadwarrior 1"
```

(continues on next page)

(continued from previous page)

```
vrouter running vlan int_vlan1#! ipv4 address 1.1.1.254/24
vrouter running vlan int_vlan1#! vlan-id 1
vrouter running vlan int_vlan1#! link-interface ntfp1
vrouter running vlan int_vlan1# .. vlan int_vlan2
vrouter running vlan int_vlan2#! description "ipsec roadwarrior 2"
vrouter running vlan int_vlan2#! ipv4 address 2.2.2.254/24
vrouter running vlan int_vlan2#! vlan-id 2
vrouter running vlan int_vlan2#! link-interface ntfp1
vrouter running vlan int_vlan2# commit
Configuration committed.
```

DNS

As a vRouter, this node require a valid DNS server to maintain its license active. We declare a public DNS server for that purpose:

```
internet-vm vlan int_vlan2# / vrf main dns server 8.8.8.8
internet-vm vlan int_vlan2# commit
Configuration committed.
```

Routing

Routing will consist of a BGP peering with the VPN Concentrators, redistributing connected subnets (meaning subnets of the road warriors).

```
internet-vm running vlan int_vlan2# / vrf main routing bgp
internet-vm running bgp#! as 65002
internet-vm running bgp# router-id 66.66.66.69
internet-vm running bgp# address-family ipv4-unicast redistribute connected
internet-vm running bgp# address-family ipv4-unicast redistribute static
internet-vm running bgp# neighbor 66.66.66.67
internet-vm running neighbor 66.66.66.67#! remote-as 65001
internet-vm running neighbor 66.66.66.67# neighbor-description concentrator1-vm
internet-vm running neighbor 66.66.66.67# address-family ipv4-unicast
internet-vm running ipv4-unicast# nexthop-self force true
internet-vm running ipv4-unicast# soft-reconfiguration-inbound true
internet-vm running ipv4-unicast# .. .. .. neighbor 66.66.66.68
internet-vm running neighbor 66.66.66.68#! remote-as 65001
internet-vm running neighbor 66.66.66.68# neighbor-description concentrator2-vm
internet-vm running neighbor 66.66.66.68# address-family ipv4-unicast
internet-vm running ipv4-unicast# nexthop-self force true
internet-vm running ipv4-unicast# soft-reconfiguration-inbound true
internet-vm running ipv4-unicast# commit
Configuration committed.
```


NAT

As this node is the default gateway for all others, we add a NAT rule to masquerade all outgoing requests:

```
internet-vm running ipv4-unicast# / vrf main nat
internet-vm running nat# source-rule 1 outbound-interface internet translate-to␣
↪output-address
internet-vm running nat# commit
Configuration committed.
```

Troubleshooting

After committing the configuration, we can check the routing table of the Internet node.

```
internet-vm running nat# exit
internet-vm> show ipv4-routes
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route


VRF main:
S>* 0.0.0.0/0 [1/0] via 10.0.2.2, internet, 00:00:20
C>* 1.1.1.0/24 is directly connected, int_vlan1, 00:00:20
C>* 2.2.2.0/24 is directly connected, int_vlan2, 00:00:20
C>* 10.0.2.0/24 is directly connected, internet, 00:00:20
C>* 66.66.66.64/29 is directly connected, ntfp2, 00:00:20
internet-vm>
```

LAN node

Interfaces and routing

This node, representing LAN resources, will have an interface in the LAN subnet. Additionally, in order to be able to respond to requests coming from the road warriors through the VPN, it needs a route to the 172.31.0.0/24 subnet (pool subnet) which points to the VPN Concentrators' VIP.

```
root@hostlan-vm:~# ip address add 172.30.0.10/24 brd + dev ntfp1
root@hostlan-vm:~# ip link set dev ntfp1 up
root@hostlan-vm:~# ip route add 172.31.0.0/24 via 172.30.0.1
```


Troubleshooting

Print routes:

```
root@hostlan-vm:~# ip route list
172.30.0.0/24 dev ntfp1 proto kernel scope link src 172.30.0.10
172.31.0.0/24 via 172.30.0.1 dev ntfp1
root@hostlan-vm:~#
```

Ping the VIP:

```
root@hostlan-vm:~# ping 172.30.0.1
PING 172.30.0.1 (172.30.0.1) 56(84) bytes of data.
64 bytes from 172.30.0.1: icmp_seq=1 ttl=64 time=1.70 ms
64 bytes from 172.30.0.1: icmp_seq=2 ttl=64 time=0.341 ms
^C
--- 172.30.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.341/1.024/1.707/0.683 ms
```

Network connectivity troubleshooting

At this point, we can check again the routing table of the VPN Concentrator: new entries should have been learned via BGP.

```
concentrator1-vm> show ipv4-routes
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route


VRF main:
B>* 0.0.0.0/0 [20/0] via 66.66.66.69, ntfp1, 00:01:32
B>* 1.1.1.0/24 [20/0] via 66.66.66.69, ntfp1, 00:01:32
B>* 2.2.2.0/24 [20/0] via 66.66.66.69, ntfp1, 00:01:32
C>* 10.150.0.0/30 is directly connected, ntfp3, 00:14:47
C * 66.66.66.64/29 is directly connected, vrrp_public, 00:14:34
C>* 66.66.66.64/29 is directly connected, ntfp1, 00:14:47
C * 172.30.0.0/24 is directly connected, vrrp_lan, 00:14:34
C>* 172.30.0.0/24 is directly connected, ntfp2, 00:14:47
concentrator1-vm>
```

The routing table of the Backup VPN Concentrator should be similar, except for the VRRP-related routes.

A ping from a road warrior to the VPN address should work:


```
warrior1-vm> cmd ping 66.66.66.66
PING 66.66.66.66 (66.66.66.66) 56(84) bytes of data.
64 bytes from 66.66.66.66: icmp_seq=1 ttl=63 time=1.78 ms
64 bytes from 66.66.66.66: icmp_seq=2 ttl=63 time=0.303 ms
64 bytes from 66.66.66.66: icmp_seq=3 ttl=63 time=0.307 ms
64 bytes from 66.66.66.66: icmp_seq=4 ttl=63 time=0.324 ms
^C
--- 66.66.66.66 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3044ms
rtt min/avg/max/mdev = 0.303/0.679/1.785/0.638 ms
warrior1-vm>
```

A ping from a road warrior to the LAN, however, should not work at this point.

2.3.3 IPsec

- *VPN Concentrator node*
- *Road warrior node*
- IPsec *troubleshooting*

VPN Concentrator node

The following commands will set:

- a default pre-shared key, and a specific pre-shared key for user1 and user2,
- an IKE template called `ike_templ1` containing one proposal for an encryption algorithm, an authentication algorithm, and a Diffie-Hellman group,
- an IPsec template called `ipsec_templ1` containing one proposal for ESP (Encapsulating Security Payload) mode,
- a VPN configuration using these templates and defining the VPN's address, an address pool and a security policy with protected VPN subnets.

```
concentrator1-vm> edit running
concentrator1-vm running config# / vrf main ike
concentrator1-vm running ike# pre-shared-key hq_psk secret default_psk
concentrator1-vm running ike# pre-shared-key user1
concentrator1-vm running pre-shared-key user1#! id user1@dev.6wind.com
concentrator1-vm running pre-shared-key user1#! secret psk_for_user1
concentrator1-vm running pre-shared-key user1# .. pre-shared-key user2
concentrator1-vm running pre-shared-key user2#! id user2@dev.6wind.com
concentrator1-vm running pre-shared-key user2#! secret psk_for_user2
```

(continues on next page)

(continued from previous page)

```
concentrator1-vm running pre-shared-key user2# .. ike-policy-template ike_templ1␣
↪ike-proposal 1
concentrator1-vm running ike-proposal 1#! enc-alg aes128-cbc
concentrator1-vm running ike-proposal 1#! auth-alg hmac-sha512
concentrator1-vm running ike-proposal 1#! dh-group modp2048
concentrator1-vm running ike-proposal 1# .. .. ipsec-policy-template ipsec_templ1␣
↪esp-proposal 1
concentrator1-vm running esp-proposal 1#! enc-alg aes128-cbc
concentrator1-vm running esp-proposal 1#! auth-alg hmac-sha256
concentrator1-vm running esp-proposal 1# dh-group modp2048
concentrator1-vm running esp-proposal 1# .. .. vpn vpn_hq ike-policy
concentrator1-vm running ike-policy#! template ike_templ1
concentrator1-vm running ike-policy#! keying-tries 10
concentrator1-vm running ike-policy#! .. ipsec-policy template ipsec_templ1
concentrator1-vm running ike-policy# ..
concentrator1-vm running vpn vpn_hq# description vpn_access_to_hq
concentrator1-vm running vpn vpn_hq# local-address 66.66.66.66
concentrator1-vm running vpn vpn_hq# local-id concentrator.6wind.com
concentrator1-vm running vpn vpn_hq# vip-pool roadwarriors_ha_pool
concentrator1-vm running vpn vpn_hq# security-policy access_to_lan local-ts subnet␣
↪172.30.0.0/24

concentrator1-vm running vpn vpn_hq# show config nodefault / vrf main ike
ike
    pre-shared-key hq_psk
        secret default_psk
        ..
    pre-shared-key user1
        id user1@dev.6wind.com
        secret psk_for_user1
        ..
    pre-shared-key user2
        id user2@dev.6wind.com
        secret psk_for_user2
        ..
    ike-policy-template ike_templ1
        ike-proposal 1
            enc-alg aes128-cbc
            auth-alg hmac-sha512
            dh-group modp2048
            ..
        ..
    ipsec-policy-template ipsec_templ1
        esp-proposal 1
            enc-alg aes128-cbc
            auth-alg hmac-sha256
            dh-group modp2048
            ..
        ..
```

(continues on next page)

(continued from previous page)

```
    vpn vpn_hq
        ike-policy
            template ike_templ1
            keying-tries 10
            ..
        ipsec-policy
            template ipsec_templ1
            ..
        description vpn_access_to_hq
        local-address 66.66.66.66
        local-id concentrator.6wind.com
        vip-pool roadwarriors_ha_pool
        security-policy access_to_lan
            local-ts subnet 172.30.0.0/24
            ..
        ..
    ..
concentrator1-vm running vpn vpn_hq# commit
Configuration committed.
```

IKE HA will be implemented using the following commands. Basically, the IKE HA instance subscribes to the `ha_for_ike` HA group (using the `listen-ha-group` command), which in turn is controlled by the VRRP group `vrrp_group`, in order to inherit its state.

```
concentrator1-vm running vpn vpn_hq# / vrf main ike ha
concentrator1-vm running ha#! listen-ha-group ha_for_ike
concentrator1-vm running ha#! node-id 1
concentrator1-vm running ha#! interface ntfp3
concentrator1-vm running ha#! local-address 10.150.0.1
concentrator1-vm running ha#! remote-address 10.150.0.2
concentrator1-vm running ha# pool roadwarriors_ha_pool address 172.31.0.0/24
concentrator1-vm running ha# commit
Configuration committed.
```

Note: `ha local-address` and `ha remote-address` should be inverted and the `node_id` should be incremented on the Backup node.

For monitoring purposes, we also enable the IKE SNMP (Simple Network Management Protocol) MIB (Management Information Base):

```
concentrator1-vm running ha# .. global-options snmp true
concentrator1-vm running ha# commit
Configuration committed.
```

See also:

The User's Guide for more information about:

- VPN Settings (https://doc.6wind.com/turbo-router-3.x/user-guide/cli/security/ike.html)
- HA IKE (https://doc.6wind.com/turbo-router-3.x/user-guide/cli/high-availability/ha-ike.html)

Road warrior node

IKE will be configured on a road warrior according to the configuration made on the VPN Concentrators. Typically, there should be matching IKE and IPSEC proposals, the pre-shared key must be correct, the VPN address should be the VIP hosted by VPN Concentrators, the allowed remote subnet must be the one allowed on the VPN Concentrators side, etc.

Additionally, `start-action` and `close-action` commands should be set to `start` in order to initiate IKE negotiations at start-up or when the other end closes the VPN.

```
warrior1-vm> edit running
warrior1-vm running config# / vrf main ike
warrior1-vm running ike# pre-shared-key hq_psk secret psk_for_user1
warrior1-vm running ike# ike-policy-template ike_templ1 ike-proposal 1
warrior1-vm running ike-proposal 1#! enc-alg aes128-cbc
warrior1-vm running ike-proposal 1#! auth-alg hmac-sha512
warrior1-vm running ike-proposal 1#! dh-group modp2048
warrior1-vm running ike-proposal 1# .. .. ipsec-policy-template ipsec_templ1 esp-
↪proposal 1
warrior1-vm running esp-proposal 1#! enc-alg aes128-cbc
warrior1-vm running esp-proposal 1#! auth-alg hmac-sha256
warrior1-vm running esp-proposal 1# dh-group modp2048
warrior1-vm running esp-proposal 1# ..
warrior1-vm running ipsec-policy-template ipsec_templ1# start-action start
warrior1-vm running ipsec-policy-template ipsec_templ1# close-action start
warrior1-vm running ipsec-policy-template ipsec_templ1# .. vpn vpn_hq ike-policy
warrior1-vm running ike-policy#! template ike_templ1
warrior1-vm running ike-policy#! keying-tries 10
warrior1-vm running ike-policy#! .. ipsec-policy template ipsec_templ1
warrior1-vm running ike-policy# ..
warrior1-vm running vpn vpn_hq# description vpn_access_to_hq
warrior1-vm running vpn vpn_hq# remote-address 66.66.66.66
warrior1-vm running vpn vpn_hq# local-id user1@dev.6wind.com
warrior1-vm running vpn vpn_hq# remote-id concentrator.6wind.com
warrior1-vm running vpn vpn_hq# vip-request 0.0.0.0
warrior1-vm running vpn vpn_hq# security-policy access_to_lan remote-ts subnet 172.
↪30.0.0/24

warrior1-vm running vpn vpn_hq# show config nodefault / vrf main ike
ike
    pre-shared-key hq_psk
        secret psk_for_user1
        ..
    ike-policy-template ike_templ1
        ike-proposal 1
            enc-alg aes128-cbc
```

(continues on next page)

(continued from previous page)

```
            auth-alg hmac-sha512
            dh-group modp2048
            ..
        ..
    ipsec-policy-template ipsec_templ1
        esp-proposal 1
            enc-alg aes128-cbc
            auth-alg hmac-sha256
            dh-group modp2048
            ..
        start-action start
        close-action start
        ..
    vpn vpn_hq
        ike-policy
            template ike_templ1
            keying-tries 10
            ..
        ipsec-policy
            template ipsec_templ1
            ..
        description vpn_access_to_hq
        remote-address 66.66.66.66
        local-id user1@dev.6wind.com
        remote-id concentrator.6wind.com
        vip-request 0.0.0.0
        security-policy access_to_lan
            remote-ts subnet 172.30.0.0/24
            ..
        ..
    ..
warrior1-vm running vpn vpn_hq# commit
Configuration committed.
```

IPsec troubleshooting

After committing, we can check the state of IKE on the different nodes:

Summary IKE SA (Security Association) from the VPN Concentrator (Master):

```
concentrator1-vm running ha# exit
concentrator1-vm> show state vrf main ike ike-sas
ike-sas
    total 2
    half-open 0
    ..
concentrator1-vm>
```

Detailed IKE SA from the VPN Concentrator (Master):

```
concentrator1-vm> show ike ike-sa details
vpn_hq: #2, ESTABLISHED, IKEv2, 7a0e17fba5af1ed4_i b7d2d02835fd0952_r
  local  'concentrator.6wind.com' @ 66.66.66.66[500]
  remote 'user2@dev.6wind.com' @ 2.2.2.2[500]
  aes128-cbc/hmac-sha512/hmac-sha512/modp2048
  established 14s ago, rekeying in 14116s
  access_to_lan: #2, reqid 2, INSTALLED, TUNNEL, esp:aes128-cbc/hmac-sha256
    installed 14s ago, rekeying in 3288s, expires in 3946s
    in  c7b832c7, 0 bytes, 0 packets
    out c104ceb4, 0 bytes, 0 packets
    local  172.30.0.0/24
    remote 172.31.0.2/32
vpn_hq: #1, ESTABLISHED, IKEv2, 080d80b4b06a2b2c_i ae34351d8c1c30d0_r
  local  'concentrator.6wind.com' @ 66.66.66.66[500]
  remote 'user1@dev.6wind.com' @ 1.1.1.1[500]
  aes128-cbc/hmac-sha512/hmac-sha512/modp2048
  established 37s ago, rekeying in 13864s
  access_to_lan: #1, reqid 1, INSTALLED, TUNNEL, esp:aes128-cbc/hmac-sha256
    installed 37s ago, rekeying in 3345s, expires in 3923s
    in  ca18ffbd, 0 bytes, 0 packets
    out c095e9c5, 0 bytes, 0 packets
    local  172.30.0.0/24
    remote 172.31.0.1/32
concentrator1-vm>
```

State of IKE SA from VPN Concentrator (Master):

```
concentrator1-vm> show state vrf main ike ike-sa
ike-sa unique-id 2
    name vpn_hq
    version 2
    state established
    local-address 66.66.66.66
    remote-address 2.2.2.2
    local-port 500
    remote-port 500
    local-id concentrator.6wind.com
    remote-id user2@dev.6wind.com
    initiator-spi 7a0e17fba5af1ed4
    responder-spi b7d2d02835fd0952
    enc-alg aes128-cbc
    auth-alg hmac-sha512
    prf-alg hmac-sha512
    dh-group modp2048
    established-time 263
    rekey-time 13867
    udp-encap false
    mobike false
    child-sa unique-id 2
        name access_to_lan
```

(continues on next page)

(continued from previous page)

```
        state installed
        reqid 2
        protocol esp
        udp-encap false
        mobike false
        spi-in c7b832c7
        spi-out c104ceb4
        enc-alg aes128-cbc
        auth-alg hmac-sha256
        esn false
        bytes-in 0
        packets-in 0
        bytes-out 0
        packets-out 0
        installed-time 263
        rekey-time 3039
        life-time 3697
        local-ts
            subnet 172.30.0.0/24
            ..
        remote-ts
            subnet 172.31.0.2/32
            ..
        ..
    ..
ike-sa unique-id 1
    name vpn_hq
    version 2
    state established
    local-address 66.66.66.66
    remote-address 1.1.1.1
    local-port 500
    remote-port 500
    local-id concentrator.6wind.com
    remote-id user1@dev.6wind.com
    initiator-spi 080d80b4b06a2b2c
    responder-spi ae34351d8c1c30d0
    enc-alg aes128-cbc
    auth-alg hmac-sha512
    prf-alg hmac-sha512
    dh-group modp2048
    established-time 286
    rekey-time 13615
    udp-encap false
    mobike false
    child-sa unique-id 1
        name access_to_lan
        state installed
        reqid 1
```

(continues on next page)

(continued from previous page)

```
        protocol esp
        udp-encap false
        mobike false
        spi-in ca18ffbd
        spi-out c095e9c5
        enc-alg aes128-cbc
        auth-alg hmac-sha256
        esn false
        bytes-in 0
        packets-in 0
        bytes-out 0
        packets-out 0
        installed-time 286
        rekey-time 3096
        life-time 3674
        local-ts
            subnet 172.30.0.0/24
            ..
        remote-ts
            subnet 172.31.0.1/32
            ..
        ..
    ..
concentrator1-vm>
```

State of IKE SA from VPN Concentrator (Backup):

```
concentrator2-vm> show state vrf main ike ike-sa
ike-sa unique-id 2
    name vpn_hq
    version 2
    state passive
    local-address 66.66.66.66
    remote-address 2.2.2.2
    local-port 500
    remote-port 500
    local-id concentrator.6wind.com
    remote-id user2@dev.6wind.com
    initiator-spi 7a0e17fba5af1ed4
    responder-spi b7d2d02835fd0952
    enc-alg aes128-cbc
    auth-alg hmac-sha512
    prf-alg hmac-sha512
    dh-group modp2048
    udp-encap false
    mobike false
    child-sa unique-id 2
        name access_to_lan
        state installed
```

(continues on next page)

(continued from previous page)

```
        reqid 2
        protocol esp
        udp-encap false
        mobike false
        spi-in c7b832c7
        spi-out c104ceb4
        enc-alg aes128-cbc
        auth-alg hmac-sha256
        esn false
        bytes-in 0
        packets-in 0
        bytes-out 0
        packets-out 0
        installed-time 463
        rekey-time 3117
        life-time 3497
        local-ts
            subnet 172.30.0.0/24
            ..
        remote-ts
            subnet 172.31.0.2/32
            ..
        ..
    ..
ike-sa unique-id 1
    name vpn_hq
    version 2
    state passive
    local-address 66.66.66.66
    remote-address 1.1.1.1
    local-port 500
    remote-port 500
    local-id concentrator.6wind.com
    remote-id user1@dev.6wind.com
    initiator-spi 080d80b4b06a2b2c
    responder-spi ae34351d8c1c30d0
    enc-alg aes128-cbc
    auth-alg hmac-sha512
    prf-alg hmac-sha512
    dh-group modp2048
    udp-encap false
    mobike false
    child-sa unique-id 1
        name access_to_lan
        state installed
        reqid 1
        protocol esp
        udp-encap false
        mobike false
```

(continues on next page)

(continued from previous page)

```
        spi-in ca18ffbd
        spi-out c095e9c5
        enc-alg aes128-cbc
        auth-alg hmac-sha256
        esn false
        bytes-in 0
        packets-in 0
        bytes-out 0
        packets-out 0
        installed-time 476
        rekey-time 2922
        life-time 3484
        local-ts
            subnet 172.30.0.0/24
            ..
        remote-ts
            subnet 172.31.0.1/32
            ..
        ..
    ..
concentrator2-vm>
```

We can see that SPI (Security Parameters Index)s are synchronized between Master and Backup nodes. Note the `passive` state of each IKE SA on the Backup node. Let's check if we have the corresponding IPSEC sessions on the road warriors side.

IKE SA from road warrior 1:

```
warrior1-vm> show ike ike-sa details
vpn_hq: #1, ESTABLISHED, IKEv2, 080d80b4b06a2b2c_i ae34351d8c1c30d0_r
  local  'user1@dev.6wind.com' @ 1.1.1.1[500]
  remote 'concentrator.6wind.com' @ 66.66.66.66[500]
  aes128-cbc/hmac-sha512/hmac-sha512/modp2048
  established 629s ago, rekeying in 13732s
  access_to_lan: #1, reqid 1, INSTALLED, TUNNEL, esp:aes128-cbc/hmac-sha256
    installed 629s ago, rekeying in 2815s, expires in 3331s
    in  c095e9c5, 0 bytes, 0 packets
    out ca18ffbd, 0 bytes, 0 packets
    local  172.31.0.1/32
    remote 172.30.0.0/24

warrior1-vm>
```

State of IKE SA from road warrior 1:

```
warrior1-vm> show state vrf main ike ike-sa
ike-sa unique-id 1
    name vpn_hq
    version 2
```

(continues on next page)

(continued from previous page)

```
    state established
    local-address 1.1.1.1
    remote-address 66.66.66.66
    local-port 500
    remote-port 500
    local-id user1@dev.6wind.com
    remote-id concentrator.6wind.com
    initiator-spi 080d80b4b06a2b2c
    responder-spi ae34351d8c1c30d0
    enc-alg aes128-cbc
    auth-alg hmac-sha512
    prf-alg hmac-sha512
    dh-group modp2048
    established-time 694
    rekey-time 13667
    udp-encap false
    mobike false
    child-sa unique-id 1
        name access_to_lan
        state installed
        reqid 1
        protocol esp
        udp-encap false
        mobike false
        spi-in c095e9c5
        spi-out ca18ffbd
        enc-alg aes128-cbc
        auth-alg hmac-sha256
        esn false
        bytes-in 0
        packets-in 0
        bytes-out 0
        packets-out 0
        installed-time 694
        rekey-time 2750
        life-time 3266
        local-ts
            subnet 172.31.0.1/32
            ..
        remote-ts
            subnet 172.30.0.0/24
            ..
        ..
    ..
warrior1-vm>
```

Another look at the routing table of the road warrior shows that a new entry has been added upon receiving the 172.31.0.1 address from the pool:

```
warrior1-vm> show ipv4-routes
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route


VRF main:
S>* 0.0.0.0/0 [1/0] via 1.1.1.254, int_vlan1, 02:47:41
C>* 1.1.1.0/24 is directly connected, int_vlan1, 02:47:42
C>* 172.31.0.1/32 is directly connected, int_vlan1, 01:09:35
warrior1-vm>
```

Let's send a ping request from this road warrior to the LAN:

```
warrior1-vm running config# cmd ping 172.30.0.10 source 172.31.0.1
PING 172.30.0.10 (172.30.0.10) from 172.31.0.1 : 56(84) bytes of data.
64 bytes from 172.30.0.10: icmp_seq=1 ttl=63 time=0.996 ms
64 bytes from 172.30.0.10: icmp_seq=2 ttl=63 time=0.446 ms
64 bytes from 172.30.0.10: icmp_seq=3 ttl=63 time=0.554 ms
64 bytes from 172.30.0.10: icmp_seq=4 ttl=63 time=0.501 ms
^C
--- 172.30.0.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3050ms
rtt min/avg/max/mdev = 0.446/0.624/0.996/0.218 ms
```

2.3.4 Logging

Logging can be useful for both troubleshooting and monitoring events on the network.

In order to enable IKE and IPSEC logging at level 2, and default at level 1, we can proceed as follows:

```
concentrator1-vm> edit running
concentrator1-vm running config# / vrf main ike logging authpriv
concentrator1-vm running authpriv# default 1
concentrator1-vm running authpriv# ike 2
concentrator1-vm running authpriv# ipsec 2
concentrator1-vm running authpriv# commit
Configuration committed.
```

See also:

The User's Guide for more information about logging (https://doc.6wind.com/turbo-router-3.x/user-guide/cli/security/ike.html#logging).

2.4 Monitoring

2.4.1 KPI (Key Performance Indicator)

The following commands will export KPIs (Key Performance Indicators) to a time-series database hosted by the LAN host, and which can then be used with a graphical tool, like Grafana.

```
concentrator1-vm> edit running
concentrator1-vm running config# / system kpi enabled true
concentrator1-vm running config# / vrf main kpi
concentrator1-vm running kpi# interface ntfp1
concentrator1-vm running kpi# interface ntfp2
concentrator1-vm running kpi# interface ntfp3
concentrator1-vm running kpi# telegraf influxdb-output url http://172.30.0.10:8086␣
↪database telegraf
concentrator1-vm running kpi# commit
Configuration committed.
```

See also:

- The User's Guide for more information about KPIs (https://doc.6wind.com/turbo-router-3.x/user-guide/cli/monitoring/kpi.html)
- 6WIND Grafana Setup on github (https://github.com/6WIND/supervision-grafana)

2.4.2 SNMP

Configuration

The following commands set a minimal SNMP support. Let's set a `monitor` community and authorize the LAN host to poll SNMP MIBs (Management Information Bases) and information from the VPN Concentrators.

```
concentrator1-vm running kpi# / vrf main snmp
concentrator1-vm running snmp# static-info
concentrator1-vm running static-info# location paris
concentrator1-vm running static-info# contact noc@6wind.com
concentrator1-vm running static-info# .. community local
concentrator1-vm running community local#! authorization read-only
concentrator1-vm running community local# source 127.0.0.1
concentrator1-vm running community local# .. community monitor
concentrator1-vm running community monitor#! authorization read-only
concentrator1-vm running community monitor# source 172.30.0.10
concentrator1-vm running community monitor# commit
Configuration committed.
```


Monitoring

From the LAN host, we can now browse the SNMP MIB of the VPN concentrators:

```
root@hostlan-vm:~# snmpwalk -c monitor -v 2c 172.30.0.2
iso.3.6.1.2.1.1.1.0 = STRING: "Linux concentrator1-vm 5.3.0-42-generic #34~18.04.1-
↪Ubuntu SMP Fri Feb 28 13:42:26 UTC 2020 x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (36263) 0:06:02.63
iso.3.6.1.2.1.1.4.0 = STRING: "noc@6wind.com"
iso.3.6.1.2.1.1.5.0 = STRING: "concentrator1-vm"
iso.3.6.1.2.1.1.6.0 = STRING: "paris"
iso.3.6.1.2.1.1.8.0 = Timeticks: (1) 0:00:00.01
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.6.3.13.3.1.3
[...]
```

The 6WIND custom IKE MIB provides information about the currently established VPNs:

```
root@hostlan-vm:~# snmpwalk -c monitor -v 2c 172.30.0.2 .1.3.6.1.4.1.7336.2.1
iso.3.6.1.4.1.7336.2.1.1.2.1.6.1.4.1.1.1.1.50.3472877975.0 = Gauge32: 0
iso.3.6.1.4.1.7336.2.1.1.2.1.6.1.4.2.2.2.2.50.3231952047.0 = Gauge32: 0
iso.3.6.1.4.1.7336.2.1.1.2.1.6.1.4.66.66.66.66.50.3300045186.0 = Gauge32: 0
iso.3.6.1.4.1.7336.2.1.1.2.1.6.1.4.66.66.66.66.50.3422768795.0 = Gauge32: 0
iso.3.6.1.4.1.7336.2.1.1.2.1.7.1.4.1.1.1.1.50.3472877975.0 = INTEGER: 1
iso.3.6.1.4.1.7336.2.1.1.2.1.7.1.4.2.2.2.2.50.3231952047.0 = INTEGER: 1
iso.3.6.1.4.1.7336.2.1.1.2.1.7.1.4.66.66.66.66.50.3300045186.0 = INTEGER: 1
iso.3.6.1.4.1.7336.2.1.1.2.1.7.1.4.66.66.66.66.50.3422768795.0 = INTEGER: 1
iso.3.6.1.4.1.7336.2.1.1.2.1.8.1.4.1.1.1.1.50.3472877975.0 = STRING: "BBBB"
iso.3.6.1.4.1.7336.2.1.1.2.1.8.1.4.2.2.2.2.50.3231952047.0 = STRING: "BBBB"
[...]
```

See also:

See the User's Guide for more information regarding:

- SNMP (https://doc.6wind.com/turbo-router-3.x/user-guide/cli/monitoring/snmp.html)

2.5 Validation

2.5.1 VRRP failover and HA swact

A first test will consist in forcing VPN Concentrator 1 - the VRRP Master - to become faulty by disabling one of its interfaces. Its VRRP state should move to `fault` and VPN Concentrator 2 should become `master`. Also, the IKE state should change accordingly and IKE sessions must transit to `ESTABLISHED` on VPN Concentrator 2 and `PASSIVE` on VPN Concentrator 1.

Disable a VRRP interface on VPN Concentrator 1:

```
concentrator1-vm> edit running
concentrator1-vm running config# vrf main interface physical ntfp1 enabled false
concentrator1-vm running config# commit
Configuration committed.
```

The VRRP state is changed to `fault`:

```
concentrator1-vm running config# show state vrf main vrrp
vrrp
    enabled true
    router-id concentrator1
    traps-enabled false
    group vrrp_group
        instance vrrp_lan
        instance vrrp_public
        notify-ha-group ha_for_ike
        state fault
        ..
    ..
concentrator1-vm running config#
```

The VRRP state is changed to `master` on VPN Concentrator 2:

```
concentrator2-vm> show state vrf main vrrp
vrrp
    enabled true
    router-id concentrator2
    traps-enabled false
    group vrrp_group
        instance vrrp_lan
        instance vrrp_public
        notify-ha-group ha_for_ike
        state master
        ..
    ..
concentrator2-vm>
```

The IKE state is changed to `PASSIVE` on VPN Concentrator 1:


```
concentrator1-vm running config# show ike ike-sa details
vpn_hq: #2, PASSIVE, IKEv2, 7a0e17fba5af1ed4_i b7d2d02835fd0952_r
  local  'concentrator.6wind.com' @ 66.66.66.66[500]
  remote 'user2@dev.6wind.com' @ 2.2.2.2[500]
  aes128-cbc/hmac-sha512/hmac-sha512/modp2048
  access_to_lan: #2, reqid 2, INSTALLED, TUNNEL, esp:aes128-cbc/hmac-sha256
    installed 781s ago, rekeying in 2521s, expires in 3179s
    in  c7b832c7, 0 bytes, 0 packets
    out c104ceb4, 0 bytes, 0 packets
    local  172.30.0.0/24
    remote 172.31.0.2/32
vpn_hq: #1, PASSIVE, IKEv2, 080d80b4b06a2b2c_i ae34351d8c1c30d0_r
  local  'concentrator.6wind.com' @ 66.66.66.66[500]
  remote 'user1@dev.6wind.com' @ 1.1.1.1[500]
  aes128-cbc/hmac-sha512/hmac-sha512/modp2048
  access_to_lan: #1, reqid 1, INSTALLED, TUNNEL, esp:aes128-cbc/hmac-sha256
    installed 804s ago, rekeying in 2578s, expires in 3156s
    in  ca18ffbd, 0 bytes, 0 packets
    out c095e9c5, 0 bytes, 0 packets
    local  172.30.0.0/24
    remote 172.31.0.1/32
concentrator1-vm running config#
```

The IKE state is changed to `ESTABLISHED` on VPN Concentrator 2:

```
concentrator2-vm> show ike ike-sa details
vpn_hq: #2, ESTABLISHED, IKEv2, 7a0e17fba5af1ed4_i b7d2d02835fd0952_r
  local  'concentrator.6wind.com' @ 66.66.66.66[500]
  remote 'user2@dev.6wind.com' @ 2.2.2.2[500]
  aes128-cbc/hmac-sha512/hmac-sha512/modp2048
  established 49s ago, rekeying in 13976s
  access_to_lan: #2, reqid 2, INSTALLED, TUNNEL, esp:aes128-cbc/hmac-sha256
    installed 829s ago, rekeying in 2751s, expires in 3131s
    in  c7b832c7, 0 bytes, 0 packets
    out c104ceb4, 0 bytes, 0 packets
    local  172.30.0.0/24
    remote 172.31.0.2/32
vpn_hq: #1, ESTABLISHED, IKEv2, 080d80b4b06a2b2c_i ae34351d8c1c30d0_r
  local  'concentrator.6wind.com' @ 66.66.66.66[500]
  remote 'user1@dev.6wind.com' @ 1.1.1.1[500]
  aes128-cbc/hmac-sha512/hmac-sha512/modp2048
  established 49s ago, rekeying in 13662s
  access_to_lan: #1, reqid 1, INSTALLED, TUNNEL, esp:aes128-cbc/hmac-sha256
    installed 842s ago, rekeying in 2556s, expires in 3118s
    in  ca18ffbd, 0 bytes, 0 packets
    out c095e9c5, 0 bytes, 0 packets
    local  172.30.0.0/24
    remote 172.31.0.1/32

concentrator2-vm>
```

2.5.2 VRRP and HA swact back to initial state

A second test will consist in launching a ping from road warrior 1 (it should be successful as it goes through VPN Concentrator 2), then bringing back the disabled interface on VPN Concentrator 1. VPN Concentrator 1 should hold for 60 seconds, then preempt its Master state; the IKE state should transit accordingly, and the ping should not be interrupted.

Start ping from road warrior 1:

```
warrior1-vm> show interface details name int_vlan1
7: int_vlan1@ntfp1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state␣
↪UP group default qlen 1000
    link/ether de:ed:01:53:da:36 brd ff:ff:ff:ff:ff:ff
    inet 1.1.1.1/24 scope global int_vlan1
       valid_lft forever preferred_lft forever
    inet 172.31.0.1/32 scope global int_vlan1
       valid_lft forever preferred_lft forever
    inet6 fe80::dced:1ff:fe53:da36/64 scope link
       valid_lft forever preferred_lft forever
warrior1-vm> cmd ping 172.30.0.10 source 172.31.0.1
PING 172.30.0.10 (172.30.0.10) from 172.31.0.1 : 56(84) bytes of data.
64 bytes from 172.30.0.10: icmp_seq=1 ttl=63 time=1.28 ms
64 bytes from 172.30.0.10: icmp_seq=2 ttl=63 time=0.770 ms
64 bytes from 172.30.0.10: icmp_seq=3 ttl=63 time=0.641 ms
(...)
```

Check VRRP and IKE states on VPN Concentrator 1 (respectively `backup` and `PASSIVE`):

```
concentrator1-vm running config# show ike ike-sa details
vpn_hq: #2, PASSIVE, IKEv2, 7a0e17fba5af1ed4_i b7d2d02835fd0952_r
  local  'concentrator.6wind.com' @ 66.66.66.66[500]
  remote 'user2@dev.6wind.com' @ 2.2.2.2[500]
  aes128-cbc/hmac-sha512/hmac-sha512/modp2048
  access_to_lan: #2, reqid 2, INSTALLED, TUNNEL, esp:aes128-cbc/hmac-sha256
    installed 781s ago, rekeying in 2521s, expires in 3179s
    in  c7b832c7, 0 bytes, 0 packets
    out c104ceb4, 0 bytes, 0 packets
    local  172.30.0.0/24
    remote 172.31.0.2/32
vpn_hq: #1, PASSIVE, IKEv2, 080d80b4b06a2b2c_i ae34351d8c1c30d0_r
  local  'concentrator.6wind.com' @ 66.66.66.66[500]
  remote 'user1@dev.6wind.com' @ 1.1.1.1[500]
  aes128-cbc/hmac-sha512/hmac-sha512/modp2048
  access_to_lan: #1, reqid 1, INSTALLED, TUNNEL, esp:aes128-cbc/hmac-sha256
    installed 804s ago, rekeying in 2578s, expires in 3156s
    in  ca18ffbd, 0 bytes, 0 packets
    out c095e9c5, 0 bytes, 0 packets
    local  172.30.0.0/24
    remote 172.31.0.1/32
```

(continues on next page)

(continued from previous page)

```
concentrator1-vm running config# show state vrf main vrrp
vrrp
    enabled true
    router-id concentrator1
    traps-enabled false
    group vrrp_group
        instance vrrp_lan
        instance vrrp_public
        notify-ha-group ha_for_ike
        state fault
        ..
    ..
concentrator1-vm running config#
```

The IPSEC traffic goes through VPN Concentrator 2:

```
concentrator2-vm> cmd show-traffic ntfp1 filter esp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ntfp1, link-type EN10MB (Ethernet), capture size 262144 bytes
08:57:16.354446 de:ed:02:69:30:81 > 00:00:5e:00:01:02, ethertype IPv4 (0x0800),␣
↪length 170: 1.1.1.1 > 66.66.66.66: ESP(spi=0xc146d5d6,seq=0x138), length 136
08:57:16.354710 de:ed:01:2e:23:19 > de:ed:02:69:30:81, ethertype IPv4 (0x0800),␣
↪length 170: 66.66.66.66 > 1.1.1.1: ESP(spi=0xce1daf17,seq=0x20131), length 136
08:57:17.378435 de:ed:02:69:30:81 > 00:00:5e:00:01:02, ethertype IPv4 (0x0800),␣
↪length 170: 1.1.1.1 > 66.66.66.66: ESP(spi=0xc146d5d6,seq=0x139), length 136
08:57:17.378724 de:ed:01:2e:23:19 > de:ed:02:69:30:81, ethertype IPv4 (0x0800),␣
↪length 170: 66.66.66.66 > 1.1.1.1: ESP(spi=0xce1daf17,seq=0x20132), length 136
(...)
```

Enable the interface previously shut down on VPN Concentrator 1 and check that after a while traffic starts flowing through VPN Concentrator 1:

```
concentrator1-vm running config# vrf main interface physical ntfp1 enabled true
concentrator1-vm running config# commit
Configuration committed.
concentrator1-vm running config# cmd show-traffic ntfp1 filter esp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ntfp1, link-type EN10MB (Ethernet), capture size 262144 bytes
08:59:52.002775 de:ed:02:69:30:81 > 00:00:5e:00:01:02, ethertype IPv4 (0x0800),␣
↪length 170: 1.1.1.1 > 66.66.66.66: ESP(spi=0xc146d5d6,seq=0x1d0), length 136
08:59:52.002964 de:ed:01:6b:02:ab > de:ed:02:69:30:81, ethertype IPv4 (0x0800),␣
↪length 170: 66.66.66.66 > 1.1.1.1: ESP(spi=0xce1daf17,seq=0x301c7), length 136
08:59:53.026740 de:ed:02:69:30:81 > 00:00:5e:00:01:02, ethertype IPv4 (0x0800),␣
↪length 170: 1.1.1.1 > 66.66.66.66: ESP(spi=0xc146d5d6,seq=0x1d1), length 136
08:59:53.026982 de:ed:01:6b:02:ab > de:ed:02:69:30:81, ethertype IPv4 (0x0800),␣
↪length 170: 66.66.66.66 > 1.1.1.1: ESP(spi=0xce1daf17,seq=0x301c8), length 136
08:59:54.050736 de:ed:02:69:30:81 > 00:00:5e:00:01:02, ethertype IPv4 (0x0800),␣
↪length 170: 1.1.1.1 > 66.66.66.66: ESP(spi=0xc146d5d6,seq=0x1d2), length 136
08:59:54.050957 de:ed:01:6b:02:ab > de:ed:02:69:30:81, ethertype IPv4 (0x0800),␣
↪length 170: 66.66.66.66 > 1.1.1.1: ESP(spi=0xce1daf17,seq=0x301c9), length 136
```

(continues on next page)

(continued from previous page)

```
(...)
^C
100 packets captured
100 packets received by filter
0 packets dropped by kernel
concentrator1-vm running config#
```

The VRRP state becomes `master` after some time, and the IKE state becomes `ESTABLISHED`:

```
concentrator1-vm running config# show state vrf main vrrp
vrrp
    enabled true
    router-id concentrator1
    traps-enabled false
    group vrrp_group
        instance vrrp_lan
        instance vrrp_public
        notify-ha-group ha_for_ike
        state backup
        ..
    ..
concentrator1-vm running config# show state vrf main vrrp
vrrp
    enabled true
    router-id concentrator1
    traps-enabled false
    group vrrp_group
        instance vrrp_lan
        instance vrrp_public
        notify-ha-group ha_for_ike
        state master
        ..
    ..
concentrator1-vm running config# show ike ike-sa details
vpn_hq: #2, ESTABLISHED, IKEv2, 7a0e17fba5af1ed4_i b7d2d02835fd0952_r
  local  'concentrator.6wind.com' @ 66.66.66.66[500]
  remote 'user2@dev.6wind.com' @ 2.2.2.2[500]
  aes128-cbc/hmac-sha512/hmac-sha512/modp2048
  established 1s ago, rekeying in 12983s
  access_to_lan: #2, reqid 2, INSTALLED, TUNNEL, esp:aes128-cbc/hmac-sha256
    installed 1055s ago, rekeying in 2247s, expires in 2905s
    in  c7b832c7, 0 bytes, 0 packets
    out c104ceb4, 0 bytes, 0 packets
    local  172.30.0.0/24
    remote 172.31.0.2/32
vpn_hq: #1, ESTABLISHED, IKEv2, 080d80b4b06a2b2c_i ae34351d8c1c30d0_r
  local  'concentrator.6wind.com' @ 66.66.66.66[500]
  remote 'user1@dev.6wind.com' @ 1.1.1.1[500]
  aes128-cbc/hmac-sha512/hmac-sha512/modp2048
```

(continues on next page)

(continued from previous page)

```
  established 1s ago, rekeying in 12823s
  access_to_lan: #1, reqid 1, INSTALLED, TUNNEL, esp:aes128-cbc/hmac-sha256
    installed 1078s ago, rekeying in 2304s, expires in 2882s
    in  ca18ffbd, 0 bytes, 0 packets
    out c095e9c5, 0 bytes, 0 packets
    local  172.30.0.0/24
    remote 172.31.0.1/32

concentrator1-vm running config#
```

The ping was not discontinued on road warrior 1 during the swact:

```
(...)
64 bytes from 172.30.0.10: icmp_seq=53 ttl=63 time=0.996 ms
64 bytes from 172.30.0.10: icmp_seq=54 ttl=63 time=0.906 ms
64 bytes from 172.30.0.10: icmp_seq=55 ttl=63 time=0.880 ms
64 bytes from 172.30.0.10: icmp_seq=56 ttl=63 time=0.945 ms
64 bytes from 172.30.0.10: icmp_seq=57 ttl=63 time=0.889 ms
64 bytes from 172.30.0.10: icmp_seq=58 ttl=63 time=0.851 ms
^C64 bytes from 172.30.0.10: icmp_seq=59 ttl=63 time=1.10 ms

--- 172.30.0.10 ping statistics ---
59 packets transmitted, 59 received, 0% packet loss, time 58662ms
rtt min/avg/max/mdev = 0.701/0.939/1.609/0.146 ms
warrior1-vm>
```