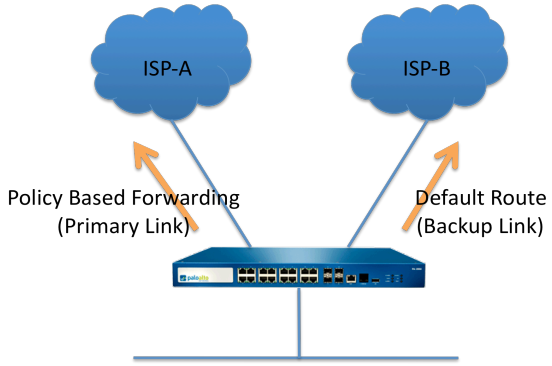
# Dual ISP Branch Office Configuration

This document describes the steps to configure a dual ISP configuration for a Branch office. In this scenario an office is connected to two ISPs and redundancy for outbound connectivity is desired. This configuration uses a combination of static routing, policy based forwarding (PBF), and destination interface based source NAT translation. This solution provides automatic outbound Internet redundancy without the need for BGP routing protocol between ISPs.




The static default route will be configured to point to the backup ISP. A PBF rule with path monitoring will be used to route traffic out to the primary ISP. If the path monitor finds the primary PBF path is no longer available, traffic will automatically begin flowing over the backup static default route.

Two source NAT rules will be configured to make sure the outbound traffic is source translated to the correct IP address depending on the egress interface (primary or backup).

## Prerequisites

- PANOS 3.1.1 and above

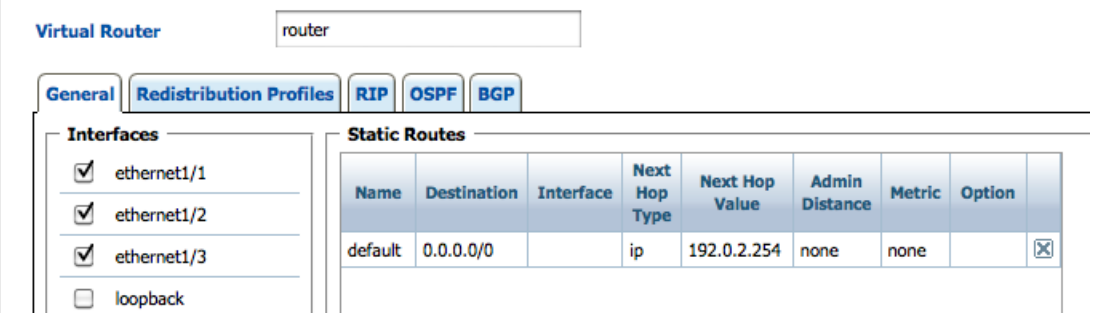
## Part 1: Configuration

1. Configure both Internet-facing interfaces in the same zone (e.g. Untrust)

| Interface | Interface Type | Management Profile | Link State | IP Address | Virtual Router | Tag | VLAN/ Virtual Wire | Security Zone |
|---|---|---|---|---|---|---|---|---|
| ethernet1/1 | L3 | | | 192.0.2.1/30 | router | Untagged | | Untrust |
| ethernet1/2 | L3 | | | 192.0.2.253/30 | router | Untagged | | Untrust |
| ethernet1/3 | L3 | | | 10.1.1.1/24 | router | Untagged | | Trust |

```
set network interface ethernet ethernet1/1 layer3 ip 192.0.2.1/30
set network interface ethernet ethernet1/2 layer3 ip 192.0.2.253/30
set network interface ethernet ethernet1/3 layer3 ip 10.1.1.1/24
set zone Trust network layer3 ethernet1/3
set zone Untrust network layer3 ethernet1/1
set zone Untrust network layer3 ethernet1/2
```

2. Configure a static default route within your Virtual Router to you backup ISP

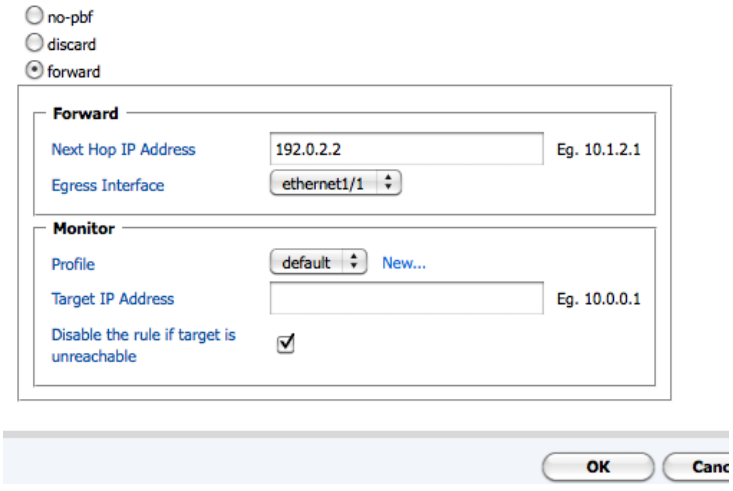



```
set network virtual-router router routing-table ip static-route default
destination 0.0.0.0/0

set network virtual-router router routing-table ip static-route default
metric 1

set network virtual-router router routing-table ip static-route default
nexthop ip-address 192.0.2.254
```

3. Configure a PBF rule that forces all traffic from the trust Zone to any address other than the local subnet(s) to use the primary ISP link. Make sure to negate the local subnet(s) in the Destination Address for best results.

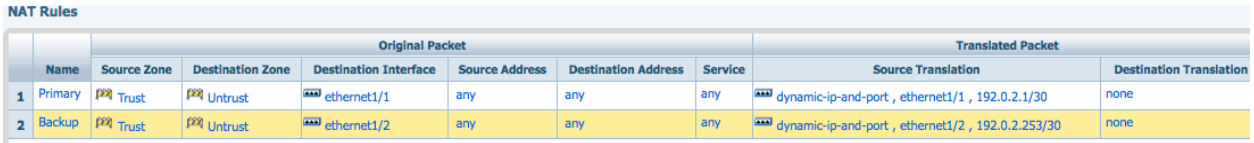

```
set rulebase pbf rules rule1 from zone Trust
set rulebase pbf rules rule1 source any
set rulebase pbf rules rule1 destination 10.1.1.0/24
set rulebase pbf rules rule1 service any
set rulebase pbf rules rule1 action forward egress-interface
ethernet1/1

set rulebase pbf rules rule1 action forward nexthop ip-address
192.0.2.2

set rulebase pbf rules rule1 source-user any
set rulebase pbf rules rule1 application any
set rulebase pbf rules rule1 negate-destination yes
```

4. Configure Path Monitoring on the PBF rule so it will only be active as long as the next hop (or some other IP beyond the next hop) is available. You can use the default monitor profile or configure a new one. If you leave the Target IP address blank the next-hop will be monitored.




```
set rulebase pbf rules rule1 action forward monitor profile default
set rulebase pbf rules rule1 action forward monitor disable-if-
unreachable yes
```

5. Configure two NAT rules to translate the source address for outbound Internet traffic. Make sure the source address is correct for each egress interface.

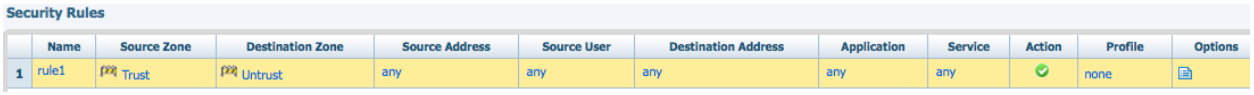


NAT Rules

| | | Original Packet | | | | | | Translated Packet | |
|---|---|---|---|---|---|---|---|---|---|
| | Name | Source Zone | Destination Zone | Destination Interface | Source Address | Destination Address | Service | Source Translation | Destination Translation |
| 1 | Primary | Trust | Untrust | ethernet1/1 | any | any | any | dynamic-ip-and-port , ethernet1/1 , 192.0.2.1/30 | none |
| 2 | Backup | Trust | Untrust | ethernet1/2 | any | any | any | dynamic-ip-and-port , ethernet1/2 , 192.0.2.253/30 | none |

```
set rulebase nat rules Primary from Trust
set rulebase nat rules Primary to Untrust
set rulebase nat rules Primary source any
set rulebase nat rules Primary destination any
set rulebase nat rules Primary service any
set rulebase nat rules Primary to-interface ethernet1/1
set rulebase nat rules Primary source-translation dynamic-ip-and-port
interface-address interface ethernet1/1

set rulebase nat rules Primary source-translation dynamic-ip-and-port
interface-address ip 192.0.2.1/30

set rulebase nat rules Backup from Trust
set rulebase nat rules Backup to Untrust
set rulebase nat rules Backup source any
set rulebase nat rules Backup destination any
set rulebase nat rules Backup service any
set rulebase nat rules Backup to-interface ethernet1/2
set rulebase nat rules Backup source-translation dynamic-ip-and-port
interface-address interface ethernet1/2

set rulebase nat rules Backup source-translation dynamic-ip-and-port
interface-address ip 192.0.2.253/30
```

6. Don't forget your security policy to allow the outbound traffic and **commit** your configuration.



Security Rules

| | Name | Source Zone | Destination Zone | Source Address | Source User | Destination Address | Application | Service | Action | Profile | Options |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | rule1 | Trust | Untrust | any | any | any | any | any | | none | |

```
set rulebase security rules rule1 from Trust
set rulebase security rules rule1 to Untrust
set rulebase security rules rule1 source any
set rulebase security rules rule1 destination any
set rulebase security rules rule1 service any
set rulebase security rules rule1 application any
set rulebase security rules rule1 source-user any
set rulebase security rules rule1 action allow
```

## Part 2: Testing

1. Start a continuous ping out to the Internet. Do a “show session id xxx” to see the details of the ping session. While the primary link is available the session should be showing the PBF rule active and the primary Internet link being used. Also, the correct source NAT address should be displayed.

```
admin@PA-2050> show session all

--------------------------------------------------------------------------------
ID/vsys   application     state   type flag   src[sport]/zone/proto (translated IP[port])
                                              dst[dport]/zone (translated IP[port]
--------------------------------------------------------------------------------

39/1      ping            ACTIVE  FLOW  NS    10.1.1.100[1]/Trust/1 (192.0.2.1[1])
                                              4.2.2.2[1]/Untrust (4.2.2.2[1])


admin@PA-2050> show session id 39

session     39
        c2s flow:
                source:   10.1.1.100[Trust]
                dst:      4.2.2.2
                sport:    1             dport:    1
                proto:    1             dir:      c2s
                state:    INIT          type:     FLOW
                ipver:    4
                src-user: unknown
                dst-user: unknown
                PBF rule: rule1(1)
        s2c flow:
                source:   4.2.2.2[Untrust]
                dst:      192.0.2.1
                sport:    1             dport:    1
                proto:    1             dir:      s2c
                state:    INIT          type:     FLOW
                ipver:    4
                src-user: unknown
                dst-user: unknown
        start time            : Tue Mar 16 07:08:22 2010
        timeout               : 6 sec
        total byte count      : 148
        layer7 packet count   : 2
        vsys                  : vsys1
        application           : ping
        rule                  : rule1
        session to be logged at end      : yes
        session in session ager          : no
        session sync'ed from HA peer     : no
        address/port translation         : source
        nat-rule              : Primary(vsys1)
        layer7 processing                : enabled
        URL filtering enabled            : no
        ingress interface                : ethernet1/3
        egress interface                 : ethernet1/1
        session QoS rule                 : default (class 4)
```

2. Show the PBF rule to make sure it is active and forwarding packets out the Primary Internet interface.

```
admin@PA-2050> show pbf rule all

Rule       ID    State    Action   Egress IF        NextHop          Status
========== ===== ======== ======== ================ ================ ======
rule1      1     Active   Forward  ethernet1/1      192.0.2.2        UP

admin@PA-2050> show pbf rule name rule1

        Rule:          rule1(1)
        State:         Active
        Action:        Forward
        Egress IF:     ethernet1/1
        NextHop:       192.0.2.2
        Monitor IP:    192.0.2.2
        Rule Status:   UP
        Monitor:       Action:Fail-Over, Interval:3, Threshold:5
        Stats:         KA sent:194, KA got:177, Packet Matched:65915
```

3. Unplug the primary link and find another new session with the "show session id xxx" command. You should now see the PBF rule is no longer used, the backup egress interface being used, and the backup source NAT address being used.

```
admin@PA-2050> show session all

--------------------------------------------------------------------------------
ID/vsys   application     state   type flag   src[sport]/zone/proto (translated IP[port])
                                              dst[dport]/zone (translated IP[port]
--------------------------------------------------------------------------------

257/1     ping            ACTIVE  FLOW  NS    10.1.1.100[1]/Trust/1 (192.0.2.253[1])
                                              4.2.2.2[200]/Untrust (4.2.2.2[200])

admin@test2050> show session id 257

session     257
        c2s flow:
                source:   10.1.1.100[Trust]
                dst:      4.2.2.2
                sport:    1             dport:    200
                proto:    1             dir:      c2s
                state:    INIT          type:     FLOW
                ipver:    4
                src-user: unknown
                dst-user: unknown
        s2c flow:
                source:   4.2.2.2[Untrust]
                dst:      192.0.2.253
                sport:    200           dport:    1
                proto:    1             dir:      s2c
                state:    INIT          type:     FLOW
                ipver:    4
                src-user: unknown
                dst-user: unknown
        start time            : Tue Mar 16 07:13:37 2010
        timeout               : 6 sec
        total byte count      : 74
        layer7 packet count   : 1
        vsys                  : vsys1
        application           : ping
        rule                  : rule1
        session to be logged at end      : yes
        session in session ager          : no
        session sync'ed from HA peer     : no
        address/port translation         : source
        nat-rule              : Backup(vsys1)
        layer7 processing                : enabled
        URL filtering enabled            : no
        ingress interface                : ethernet1/3
        egress interface                 : ethernet1/2
        session QoS rule                 : default (class 4)
```

Notice no PBF rule listed here

4. You will now see the PBF rule is inactive

```
admin@PA-2050> show pbf rule all

Rule        ID     State    Action   Egress IF       NextHop          Status
=========== ====== ======== ======== =============== ================ ======
rule1       1      Disabled Forward  ethernet1/1     192.0.2.2        DOWN
```