Contents

Introduction

Terminating two ISP's on ASA/PIX

Design
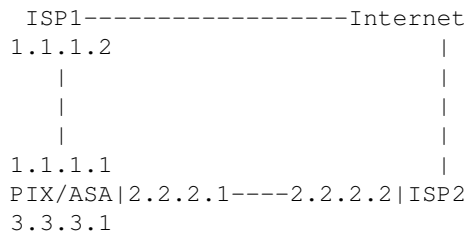
```
   ISP1----------------Internet
1.1.1.2                        |
    |                          |
    |                          |
    |                          |
1.1.1.1                        |
PIX/ASA|2.2.2.1----2.2.2.2|ISP2
3.3.3.1

||

   Internal Network
```

Configuration

Lets say customer has above setup, with ISP1 being the Primary ISP and ISP2 being the Secondary ISP.

I'm assuming that you all know how ISP failback is configured and how it functions. To summarize, in ISP failback all traffic goes out using ISP1 and if it fails, ASA/PIX starts routing traffic via ISP2.

Scenario I

==

Now, customer does not want to configure ISP failback, but he needs to route Web (port 80,443) traffic via ISP2 and all other traffic via ISP1. This requires PBR, which is not supported on ASA/PIX, but we can configure a workaround on ASA/PIX to make it work.

Following are the commands which will achieve it-

route ISP1 0 0 1.1.1.2 //Default route pointing to ISP1 route ISP2 0 0 2.2.2.2 2 //Default route with Metric 2 via ISP2

static (ISP2,inside) tcp 0.0.0.0 80 0.0.0.0 80 static (ISP2,inside) tcp 0.0.0.0 443 0.0.0.0 443

sysopt noproxyarp inside

nat (inside) 1 0 0 global (ISP1) 1 interface global (ISP2) 1 interface

Thats it !! Now all the traffic destined to any address on port 80/443 will be forcibly put on ISP2 interface and routed from there.

Note: This stuff requires that we KNOW what the destination ports are, if there is some traffic which uses dynamic ports, like voice traffic we will have to route it via ISP1 and cannot make it route via ISP2.

Scenario II

=

In the same setup, if customer says that he wants half traffic to go via ISP1 and half traffic via ISP2, first you need to explain customer that ASA is NOT a load-balancer or packet-shaper. Hence we cannot *truly* achieve this, but we may configure ASA in such a manner that traffic for some destination IP address is routed via ISP1 and some is routed via ISP2. Following would be configuration commands in this scenario-

nat (inside) 1 0 0 global (ISP1) 1 interface global (ISP2) 1 interface

route ISP1 128.0.0.0 128.0.0.0 1.1.1.2 route ISP2 0.0.0.0 128.0.0.0 2.2.2.2

The first creates a default route that routes addresses with the first bit of 1 to 1.1.1.2 of ISP1.

The second creates a default route that routes addresses with the first bit of 0 to 2.2.2.2 of ISP2.

Note: This will do traffic routing based on *Destination* IP addresses and NOT based on traffic load. As I mentioned, ASA is NOT a packet-shaper.