

Re: Two ISPs, One NAT'ed Internal Subnet, Firewall Policies

Source: <http://linux.derkeiler.com/Mailing-Lists/Fedora/2004-09/3609.html>

From: Daniel Bartlett (bartlett.d_at_gmail.com)

Date: 09/21/04

Date: Tue, 21 Sep 2004 10:11:09 +0100

To: For users of Fedora Core releases <fedora-list@redhat.com>

Hi,

> *Presumably you have separate (possibly dynamic) IP addresses from the two*
> *ISPs, and intend to use the connections for outbound (client) traffic,*
> *and not inbound (e.g., webserving) traffic? If so, an active/passive*
> *configuration can be rather simple.*

We are dealing with inbound mail(smtp/pop3), http & https traffic. One ISP is a static subnet of 8 IPs the other dynamic(1 IP). I have been thinking that getting a dynamic DNS account and updating on the failover(and regularly for the dynamic connection).

>
> > *Updating IPtables at the same time.*
>
> *If the connections to the ISPs are configured to use two different*
> *interfaces, the netfilter configuration can be static; have separate*
> *SNAT rules for each interface, and update the default route instead,*
> *which amounts to*
>
> */sbin/ip route replace default via \$GATEWAY dev \$DEV*

I think this would work if not for the inbound traffic, if a remote host opens a connection on one IP and the data goes back on the other packet headers will mean the packet just gets dropped.(Although a mangle rule might work here...if maybe quite confusing to setup)

>
> *That's the simple part. The more interesting part is detecting the "dead"*
> *gateway, for some definition of "dead". In the typical external ADSL*
> *or cable modem configuration, there can be a failure of communication*
> *between the Linux firewall and the ADSL/cable router, between the*
> *ADSL/cable router and the ISP, and between the ISP and the wider Internet*
> *(usually due to routing screwups, etc., at the ISP). So detecting whether*
> *the local gateway (i.e., the ADSL/cable router) is alive is of only*

Fedora: Re: Two ISPs, One NAT'ed Internal Subnet, Firewall Policies

- > *marginal utility; one usually wants to detect reachability of the wider*
- > *Internet, via pinging highly-available sites, or an equivalent method.*
- >
- > *Then there is the issue of DNS resolution. For many clients, if the ISP's*
- > *DNS servers are not working, the route to the internet is again of marginal*
- > *utility. One can configure DNS to use the nameservers of both ISP's, though*
- > *that doesn't help with certain Byzantine failures (that seem to occur in*
- > *real life), where one ISP's nameserver returns nonsense. For this and*
- > *other reasons, it is generally desirable to give priority to the DNS server*
- > *of the ISP that you are routing through, and a more active approach to*
- > *DNS server monitoring is often used.*

The DNS issue i was thinking of setting up a caching DNS server that had its configs updated on the connection failing, ie for the ISP nameservers.

- >
- >> *I was wondering if anyone could point me in a direction in this. I*
- >> *have looked at the failoverd daemon but as it's not supported anymore*
- >> *i was thinking there might be something newer.*
- >
- > *These topics are oft-discussed on the Linux Advanced Routing and*
- > *Traffic Control (lartc.org) mail list,*
- >
- > <http://mailman.ds9a.nl/pipermail/lartc/>
- >
- > *Julian Anastasov and others have invested considerable effort in*
- > *multiple *active* gateways (in contrast to an active/passive failover*
- > *configuration). See*
- >
- > <http://www.ssi.bg/~ja/#routes>
- >
- > *It is generally agreed that multiple active gateways are easier to*
- > *manage with Julian's patches. The patches effectively allow one to*
- > *statically configure a useful routing policy which otherwise would need*
- > *to be implemented with dynamic configuration in userspace. For your*
- > *simple active/passive failover configuration, the patches are unnecessary.*
- >
- > *A tool that is useful with the multiple-ISP configuration is TCP cutter,*
- >
- > <http://www.lowth.com/cutter/>
- >
- > *which is used to forcibly abort TCP sessions through a NAT gateway.*

I'll take a look at all of these, thanks.

Kind regards,
Daniel.

--
Daniel Bartlett

Fedora: Re: Two ISPs, One NAT'ed Internal Subnet, Firewall Policys

London, UK

--

fedora-list mailing list

fedora-list@redhat.com

To unsubscribe: <http://www.redhat.com/mailman/listinfo/fedora-list>