

Re: [fw-wiz] Info Request: Looking for alternatives in HA/Load balancing firewallsthat are also scalable and modular.

Re: [fw-wiz] Info Request: Looking for alternatives in HA/Load balancing firewallsthat are also scalable and modular. . .

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2006-04/msg00052.html>

- *From:* David Lang <dlang@xxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 12 Apr 2006 16:10:07 -0700 (PDT)
-

On Mon, 10 Apr 2006, Arkanoid wrote:

Well, i guess it is firewall to protect some kind of public server, that's the only configuration where you need truly scalable HA solution.

When it comes to protecting LANs it is better to have multiple branch firewalls.

Am i right?

actually I would think the opposite, Internet bandwidth is generally FAR more limited then LAN bandwidth. a 'high bandwidth' server farm on the Internet is generally doing traffic in the tens to hundreds of Mb/sec, a 'high bandwidth' server on a LAN is probably connected to multiple 100Mb or 1Gb ethernets. In both the Internet and LAN environments I lean towards multiple smaller firewalls, each doing one thing (with a simple config) as opposed to a large firewall doing it all (with a complex config). it's just easier to do simple things right repeatedly then to do complex things right.

in general I don't think that people realize this, the mentality seems to be 'I need a big, scaleable firewall to protect my Internet servers' and at the same time 'oh, that's only on the lan, it doesn't need a big firewall to protect it'. In part I think that this is becouse Internet bandwidth is very expensive compared to LAN bandwidth, so people think that the firewalls to protect them should be priced accordingly.

yes there are extremely high end server farms that can have Gb/sec of traffic, but those are relatively rare, and each is a special case that provides different logical ways to segment the traffic.

(Again, my favorite rant: there are actually at least 3 completely different device types all of them called "firewalls", and they differ in functional requirements and architecture. It leads to major misunderstading.)

very true

David Lang

Re: [fw-wiz] Info Request: Looking for alternatives in HA/Load balancing firewallsthat are also scalable and

Re: [fw-wiz] Info Request: Looking for alternatives in HA/Load balancing firewallsthat are also scalable and modular.

On Fri, Apr 07, 2006 at 01:20:48PM -0700, David Lang wrote:

On Tue, 4 Apr 2006, Keith A. Glass wrote:

. . . Here's my situation:

We're currently spec'ing functional requirements for a new web-based implementation of a number of enterprise apps. One obvious problem is the firewall system: it needs to be both load-balancing and high-availability, AND scalable. We're still getting a feel for potential traffic, but we expect to have a requirement for in-line expansion of the system while remaining online.

high-availability is easy to understand the requirements for.

load-balancing is only a requirement from a marketing/management point of view unless you can define your third point

scalable. scaleable to what? are you talking an Internet connection where you have a need for multiple T-1 lines? multiple DS-3 lines? multiple OC-12 lines? or are you talking local networks where you have 100Mb ethernet? or gig ethernet? or 10gig ethernet? are you talking just a couple of these networks or are you talking about dozens of these networks?

as others noted load balanceing is seldom needed for technical reasons, and it's impossible to answer anything about scalability without knowing what sort of scale you are talking about. In most cases a single high-capacity box (plus HA backup) can easily handle the full load, and the percentage of cases like this is growing as boxes get faster (which is happening at a faster rate then the communications links)

sorry for the rant, but you managed to hit one of my current sore points (I just got out of a meeting with an engineer who claimed that we couldn't do something because of the huge load that it would cause, when that load consisted of one extra network hop for one out of hundred connections :-/)

David Lang

--

There are two ways of constructing a software design. One way is to make it

Re: [fw-wiz] Info Request: Looking for alternatives in HA/Load balancing firewallsthat are also scalable and

Re: [fw-wiz] Info Request: Looking for alternatives in HA/Load balancing firewallsthat are also scalable and modular.

so simple that there are obviously no deficiencies. And the other way is to make it so complicated that there are no obvious deficiencies.

— C.A.R. Hoare

firewall-wizards mailing list
firewall-wizards@xxxxxxxxxxxxxxxxxxxxx
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

firewall-wizards mailing list
firewall-wizards@xxxxxxxxxxxxxxxxxxxxx
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

—
There are two ways of constructing a software design. One way is to make it so simple that there are obviously no deficiencies. And the other way is to make it so complicated that there are no obvious deficiencies.

— C.A.R. Hoare

firewall-wizards mailing list
firewall-wizards@xxxxxxxxxxxxxxxxxxxxx
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

Re: [fw-wiz] Info Request: Looking for alternatives in HA/Load balancing firewallsthat are also scalable and