

Re: need comments on proposed network architecture—correct diagram this time

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2003-08/0399.html>

From: John (jwholmes_at_earthlink.net)

Date: 08/06/03

Date: Wed, 06 Aug 2003 06:45:01 GMT

On Tue, 05 Aug 2003 18:54:39 -0700, ike lozada wrote:

> Lars M. Hansen <badnews@hansenonline.net> wrote in message
news:<nm2vivc8dmkt3tr8oj1352h8877ivogvqp@4ax.com>...

>> On 5 Aug 2003 01:43:43 -0700, ike lozada spoketh

>>

>> >hi all,

>> >

>> >my company is currently planning to upgrade our network infrastructure

>> >which by the way, really needs upgrading. our current setup is like

>> >this

>> >

>> >internet-->router-->hub-->internal network

>> >

>> >it sucks, i know. but we are thinking of upgrading it to this setup:

>> >

>> >internet-->border-->dmz-->packet-filterng-->switch-->internal netwrk1

>> > router router -->switch-->internl netwrk2

>> > -->switch->internal netwrk3

>> > ..and so on...

>> >

>> >dmz will host our mail servers, ids, load balancer, www and ras

>> >server. internal network1 will have an application server (backend

>> >lotus notes) that www server (web portal) will need to have access to.

>> >

>> >now my questions:

>> >

>> >1. will our planned setup work? what are the advantages/disadvantages

>> >to this and what can you guys recommend to make it better? im afraid

>> >for the packet filtering router that sits between the different

>> >switches because it would mean a single point of failure and if it

>> >goes down, whole netwrk will go down!

>> >

>> >2. how can we allow www server in the dmz to access the backend in one

>> >of the trusted networks? vpn or by proxy perhaps? please give ideas on

>> >how to set this up.

comp.security.firewalls: Re: need comments on proposed network architecture—correct diagram this time

>> >
>> >3. *where should we put domain controllers and dhcp servers? we are*
>> >*thinking of putting them in each of the different LAN segments...*
>> >
>> >
>> >*thanks for any comments*
>>
>> *You probably shouldn't have your packet filtering router do your VLAN*
>> *routing for you. Call it a "firewall", and let it do only that. Then*
>> *you'll get:*
>>
>> *Internet---BR---DMZ---FW---LAN*
>>
>> *You should treat this as two separate jobs. One is reorganizing your*
>> *internet connection, the second is reorganizing your internal LAN.*
>>
>> *You can allow the WWW server to gain access through the firewall to get*
>> *to the backend. The rule to allow it just has to be very specific. Or,*
>> *you could have another backend server in the DMZ that queries the real*
>> *backend on the LAN. Then it alone can have access to the LAN. In the*
>> *event that the webserver is compromised, there won't be a direct path*
>> *into your LAN...*
>>
>> *For your LAN solution, you could do this with VLAN, or simply with*
>> *multiple separate switches all connected to a very fast router with many*
>> *ports. The Cisco 3550 switch can do that routing for you much faster*
>> *than many routers...*
>>
>> *One idea would be to use some Cisco 2950-48's for the LANs, all*
>> *connected with GigaStack stacking GBIC connectors, and have one Cisco*
>> *3550-12T to provide Ethernet gigabit connections to servers. Or, you can*
>> *go with the 3550-24 SMI (much cheaper) if you don't need any ethernet*
>> *gigabit connections. Connect them like this:*
>>
>> |---
>> *Switch1 |*
>> ||
>> *Switch2 |*
>> ||
>> *Switch3 |*
>> ||
>> *Switch4 |*
>> |---
>>
>> *Although it look like a loop (and it is), STP will ensure that one path*
>> *gets disabled, and it'll only be enabled in the event that one uplink or*
>> *switch fails. Have the Gigabit connectors trunked (part of all VLANs),*
>> *and have switch4 (the 3550) do the VLAN routing for you.*
>>
>> *You can put your servers on it's own VLAN, and have the DHCP server give*
>> *out several ranges of IP addresses (one range for each VLAN). The use of*

Re: need comments on proposed network architecture—correct diagram this time

comp.security.firewalls: Re: need comments on proposed network architecture—correct diagram this time

>> *an ip-helper-address on the switch (essentially, giving the DHCP
>> server(s) virtual IP addresses on each VLAN) will allow all clients on
>> any VLAN to see the DHCP server(s).*
>>
>> *Lars M. Hansen*
>> *<http://www.hansenonline.net>*
>> *(replace 'badnews' with 'news' in e-mail address)*
>
>
> *Hi again, in the dmz, we plan to put a mail server, www server (load
> balancer next time), an IDS...any problems with these? also, where
> should we put the dhcp servers... in the dmz? or one dhcp server per
> vlan? is a vlan==subnet (i.e. network segment)?*
>
> *thanks*

You really need 1 dhcp server per lan segment (I did not say per switch, see Lars comments above). It is possible to forward dhcp broadcasts but it is a lousy idea. Not sure why you would need a dhcp server in the dmz. Anything that goes in there should require public access and that means it needs a static ip (minus the IDS which is a different subject). Put the dhcp behind the firewall on the internal network and don't let it out.

The IDS should have a static address, not be in dns and preferably only be reachable from the console but that depends on the system.

Also, why not get a firewall with more interfaces and do away with the dmz router? It will be cheaper and a real firewall will give you better protection in the dmz, be easier to maintain and make for a more reliable network by cutting down on boxes and cables. If you were getting by with a hub before how many switches do you need now anyway? I like vlans but keep things as simple as you can. They mean fitting a router in somewhere to route between them. A flat network will cause less problems up until your traffic volume gets heavy. By then you will probably need more addresses and here comes the router anyway!

Basically, check your current traffic load, projected growth rate, budget and level of expertise in-house before complicating too much.

--

John Holmes
jwholmes@earthlink.net