

Re: Firewall Beginners Assistance

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-10/5172.html>

From:

Date: 07/19/02

Date: Fri, 19 Jul 2002 19:59:23 +0200

newbe tries to setup the following schema.

please correct me – good for the learning.

```

                                192.168.254.3
[u1] [ serv1 = web = testserver –
apache win32 2.39]
                                ^
[u2] ===== [sw]===== [cisco[ proxy / gateway][ serv2]
router PDC] = [sw]= internet
                                V
[u3] [ serv3 = ftp appserv BDC –
Serv-U (supports multiple domains) ----^
                                192.168.254.2
```

rules:

webserver listens on port 8001 (lana0=192.168.254.3)
*(e.g. apache 2.039 win32)
ftpserver listens on port 2121 (lana0=192.168.254.2)
*(e.g. Serv-U 4)
both accept only reqs from 192.168.254.1 or 192.168.254.2
res: PDC/BDC

rules and names:

start with intranet security access (exclude any external access first)
make primary internet access on port 8081 (group = internet_full)
limited access (filtered) (group=internet_extra)
specific services only (group=internet)

clients could update the browser using .pac files
these are scripts containing reference to DNS, GATEWAY etc..
if you tweak the browsers so these settings cannot be changed,
this will improve security – furthermore its possible to build
ready-steady install package which will include the preset settings
but that is aftermath.. (like using ghost images, installers, remote
updating etc..)

comp.security.firewalls: Re: Firewall Beginners Assistance

No DHCP? maybe not, but DHCP improves other services, like timesync and DNS – so, it might be wise to use it anyway.

Your PDC/BDC could sync with various atomic clocks and hence update all clients automatically.

DHCP users talk to 192.168.254.1/2 with port 67/68 only. PDC/BDC will auth users and forward web/ftp requests

(making rules toward ftp/web level access increases security)

users are connected with 10mb lines only (bandwidth limiting)

server–server use 100+ lines or faster (ring 0)

>>> *disadvantage: no dhcp service, no ip number..* :-(<<<

user–user connections are prohibited – user–user conditions are set by admin like users share a map for a group (like design or internal documents)

PDC and/or BDC decide whether external/internal users have rights to access web/ftp services – ipsec or vpn security / cerberus security authentication (important for external users) (not sure which is good)

PDC down, backup by BDC (backup Domain controller)

both down? no web/ftp access (which is good since it will prevent

unauthorized access)

Are we using ISP Dns services? Why, security?, then DNS IP numbers are those of ISP.

question: why owning a DNS server??

+ DNS service will make its own list of hosts and hence improve internet lookup speed. :-)

– DNS are target to external attacks and will ask for higher security measures :-(

owning a DNS server is also \$\$\$ + security \$\$\$

(for 3 clients really overkill anyway)

intranet:

Clients use proxy (PDC/BDC) to authenticate and connect to internet

Client use internal FTP domain ('full' XS (according to userlevel))

internal clients may have write/read according to userlevel

the best way is to 'write' to an temporarily web–storage (use review monitor) and update the web

according to set frequency/manually. Setting an AV filter on that particular map (shared maps – group wwwauthor)

e.g user should be part of the wwwauthor group to have rights to write data.

extranet/internet:

external FTP clients talk to another FTPport via Ident/PDC/BDC

[???] do these external clients have limited access?

the same for Web services which are limited to view (read–only) to external clients

well, it looks like i was somewhat creative today.. :)

please let me know (info.box@home.nl) i'm interested in your views and of all other readers ofcourse.

Sincerely,

Herauth –

"Martin" <mvinfotech@NOSPAMbtinternet.com> wrote in message news:3d37296e.1231140@news.btinternet.com...

> *Hi,*
>
> *I am currently running a network for my company which comprises the*
> *following:*
>
> *3 x Windows 2000 Servers in a domain*
> *A Cisco router using NAT connecting us to our ISP.*
>
> *These are in the following setup:*
>
> *ROUTER*
> *192.168.254.254*
>
> *DOMAIN CONTROLLER (Office File Server – Email Server)*
> *192.168.254.1*
>
> *DOMAIN CONTROLLER (Application Server)*
> *192.168.254.2*
>
> *TEST SERVER*
> *192.168.254.3*
>
> *Currently, our web site is hosted by our ISP. We use our office file*
> *server as our email server.*
>
> *We currently have 3 clients, and our aim is to host a web server*
> *internally, for each of these 3 clients and also host our own web*
> *site. We will use our Test Server for one of these, and will purchase*
> *a further 3 servers.*
>
> *We would like to be able to access each of the 6 servers internally.*
> *However we would only like each external client to have access to*
> *their own server externally. They should also have their own FTP area*
> *on their own server.*
>
> *What should the correct type of setup be? I am interested in a*
> *hardware firewall, where it should be sited, and how it should be*
> *configured. I am very new to this area, so would really appreciate*
> *some assistance in this area. Also any basic information on hardware*
> *firewalls and basic configuration information eg websites would be*
> *appreciated.*
>

comp.security.firewalls: Re: Firewall Beginners Assistance

> *Many thanks, and apologies for the long post!*

>

> *Martin.*

>

>

- *Next message:* : ["Random connections to intelonline.com"](#)
- *Previous message:* [news box: "Re: Agnitum stopping ICMP Echo Request to Microsoft site."](#)
- *In reply to:* [Martin: "Firewall Beginners Assistance"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)