

## Re: Secure Server & Services

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2004-08/0269.html>

---

**From:** Oli Restorick [MVP] ([oli\\_at\\_mvps.org](mailto:oli_at_mvps.org))

**Date:** 08/29/04

Date: Sun, 29 Aug 2004 22:32:43 +0100

IPSec is the ideal solution here, but it does take some setting up and careful consideration of what traffic you want to use IPSec for.

If you just want to make it difficult for people to use non-domain members, consider using IPSec to make the most commonly-accessed resource accessible only by domain members. You can use IPSec AH with Kerberos to do this. If you're not careful, though, it's very easy to set an IPSec policy with Group Policy that it prevents communication with your domain controllers. From here, you have no way to undo this, so be careful and do plenty of testing.

Sometimes a technical solution is not always the best for those who breach company policy. The most likely reason that your staff don't want to be domain members is that they plug their laptops into their home networks and mistakenly believe that if they're joined to the domain, they won't be able to do this. Since these machines are outside your control, you have no way to patch them against vulnerability-of-the-day and no way to ensure they get patched. It won't be long before your network gets the next Blaster, Sasser, Nimda, Code Red or Slammer unless you get support from your managers to stop this happening. It's not really about being BOFH, it's about protecting your company and protecting yourself, because no doubt the fingers will be pointing at you rather than the idiots with the laptops when the next worm hits your network.

Hope this helps

Oli

"BOFH" <[john.hamilton70@ntlworld.com](mailto:john.hamilton70@ntlworld.com)> wrote in message [news:2peuf8FjhcllU1@uni-berlin.de](mailto:news:2peuf8FjhcllU1@uni-berlin.de)...

- > *It was an answer from another newgroup when I asked the same*
- > *question...and*
- > *I searched for it too with no useful results. Must have been a flight of*
- > *fancy!*
- >
- > *How do I filter MAC addresses? (Another reply)*
- >
- > *I have 6 Windows 2003 servers, serving 250 or so PCs and 60 laptops. Its*
- > *the damn laptops I have a problem with as some staff refuse to be a member*

> of the domain. Being a BOFH I want to enforce company policy and restrict  
> access to network resources and internet if they plug it in.  
>  
> Thanks for all your help :)  
>  
> "Miha Pihler" <mihap-news@atlantis.si> wrote in message  
> news:eaw7legjEHA.1048@tk2msftngp13.phx.gbl...  
>> Domain verification is not a term I am familiar with in a context to what  
>> you are looking for. Also if you run a search on Microsoft or Google it  
>> doesn't give any useful result to what you are looking for.  
>>  
>> Where did you hear this term and in what context?  
>>  
>> Mike  
>>  
>> "BOFH" <john.hamilton70@ntlworld.com> wrote in message  
>> news:2pes2dFjismqU1@uni-berlin.de...  
>>> Thanks Mike...  
>>>  
>>> Could you tell me what 'Domain Verification' is?  
>>>  
>>> I am so desperate to stop non-domain equipment from accessing my  
> network.  
>>>  
>>> "Miha Pihler" <mihap-news@atlantis.si> wrote in message  
>>> news:umoPh3ajEHA.3972@tk2msftngp13.phx.gbl...  
>>>> Hi,  
>>>>  
>>>> For now, there is no easy solution to prevent DHCP server issuing IPs  
> to  
>>> non  
>>>> domain clients. This is usually a problem when clients come in the  
>> office  
>>>> and want to plug their computer into your LAN. If you are worried  
> about  
>>>> attacks well you should be. Even without DHCP it is pretty easy to  
>> figure  
>>>> out what IPs you use on your LAN. E.g. if you use Exchange mail  
>>>> server  
> I  
>>> can  
>>>> look in header of any e-mail from your organization and find out on  
> what  
>>> IP  
>>>> your Exchange server is running)... Now I can pretty much guess what  
> IP  
>>> I  
>>>> have to set manually to get access to your LAN and Internet even  
> without  
>>>> DHCP.  
>>>>

>>>> *There are few things you can do.*  
>>>> *If you only want to prevent access to internet and you don't have*  
>> *problem*  
>>>> *with customers browsing your LAN setup a proxy (e.g. ISA server). You*  
>> *can*  
>>>> *setup ISA in a way that would require every user to authenticate*  
>>> *themselves*  
>>>> *before they are granted access to the internet (user need a valid*  
>> *account*  
>>> *in*  
>>>> *domain or some other database).*  
>>>>  
>>>> *If you also want to prevent access to LAN first thing you can do,*  
> *don't*  
>>>> *patch all network outlets to network backbone. Even if someone comes*  
> *to*  
>>>> *your*  
>>>> *office and plugs his computer with his own cable to the network*  
>>>> *outlet*  
>>>> *he/she still won't have any access to the network.*  
>>>>  
>>>> *Next thing you can do is port authentication (IEEE 802.1x). This is*  
>>> *probably*  
>>>> *not the cheapest solution since you need switches that support IEEE*  
>>> *802.1x.*  
>>>> *Next thing you need are clients that are Windows 2000 SP4 or newer.*  
> *Once*  
>>>> *the*  
>>>> *client connects to the network they have to present authentication*  
>>>> *parameters (username and password) and these are checked against e.g.*  
>>>> *Active*  
>>>> *Directory (using IAS – RADIUS)...*  
>>>>  
>>>> *You could also setup IPSec policy for your domain. This would prevent*  
>> *any*  
>>>> *computer that is not part of domain to communicate with other members*  
> *of*  
>>>> *domain since Kerberos is used for IPSec authentication.*  
>>>> *Even if virus infected computer comes to your office and it is not*  
> *part*  
>> *of*  
>>>> *your domain other computers will discard any connection from this*  
>> *computer*  
>>>> *since it doesn't use IPSec...*  
>>>>  
>>>> *I hope this helps,*  
>>>>  
>>>> *Mike*  
>>>>  
>>>> *"BOFH" <john.hamilton70@ntlworld.com> wrote in message*  
>>>> *news:2pdlclFjhe24U1@uni-berlin.de...*

>>>> *I have DHCP on the server, it issues addresses to non-domain  
> computers*  
>>>> *too,*  
>>>> *which allows them use of the internet. I wish to block this.*  
>>>>>  
>>>>> *I have heard the term 'Domain Verification'...what is it and what  
> can*  
>> *it*  
>>>> *do*  
>>>>> *for me?*  
>>>>>  
>>>>>  
>>>>> **BOFH**  
>>>>>  
>>>>>  
>>>>  
>>>>  
>>>  
>>>  
>>  
>>  
>  
>