

## Re: Blocking by MAC Address –

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.networking/2005-11/msg00652.html>

---

- *From:* "Miha Pihler [MVP]" <[mihap-news@xxxxxxxxxxxxx](mailto:mihap-news@xxxxxxxxxxxxx)>
  - *Date:* Mon, 28 Nov 2005 19:11:25 +0100
- 

Again an attacker could still bypass 802.1x with this configuration.

Switch will only see one MAC. What is stopping an attacker to assign himself same MAC as a valid computer? There are few other ways to fool switch into allowing more then one MAC per port (even if configured otherwise).

This is very well described here under: "Why 802.1X on wired networks is insufficient"

<http://www.microsoft.com/technet/community/columns/secmgmt/sm0805.mspx>

--  
Mike  
Microsoft MVP – Windows Security

"Antonio Cardoso" <[AntonioCardoso@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:AntonioCardoso@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message [news:7C7362AC-1264-4782-961B-D602C1B85F50@xxxxxxxxxxxxxxxxxxxxx](mailto:news:7C7362AC-1264-4782-961B-D602C1B85F50@xxxxxxxxxxxxxxxxxxxxx)

- > not quite,
- >
- > the idea is to change dynamicaly the VLAN of the port.
- >
- > VLAN A-> Connection VLAN
- > VLAN B-> Validation VLAN
- > VLAN C-> Production VLAN
- >
- > user allways connect to VLAN A
- > user must go to server from VLAN B to validate the machine is OK
- > user pass machine OK, then go to VLAN C
- >
- > allways check if there is a 2 MAC in one port, if so, port-down ... :-)
- > this means no hubs in the enviroment.
- >
- > regards
- >
- > "Miha Pihler [MVP]" wrote:
- >
- >> As an attacker I can still bypass 802.1x on the switch.
- >>
- >> --

Re: Blocking by MAC Address –

>> Mike  
>> Microsoft MVP – Windows Security  
>>  
>> "Antonio Cardoso" <AntonioCardoso@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in  
>> message [news:8A2BC001-F1B7-4E67-8726-1ABAA3457E72@xxxxxxxxxxxxxxxxxxxx](mailto:news:8A2BC001-F1B7-4E67-8726-1ABAA3457E72@xxxxxxxxxxxxxxxxxxxx)  
>> > You can do this by validating the switches ... if you have cisco you  
>> > can  
>> > send  
>> > a trap each time a mac is added to a port and then validate that the  
>> > mac  
>> > is  
>> > authorized ....  
>> >  
>> > regards  
>> >  
>> > "Miha Pihler [MVP]" wrote:  
>> >  
>> >> Hi,  
>> >>  
>> >> You don't have to use encryption. You can set up ESP-Null. In this  
>> >> case  
>> >> packets only get authenticated. This will still add up a bit to the  
>> >> processor since it has to check every packet but this will in general  
>> >> be  
>> >> few  
>> >> percents (3-5). Most of server's CPU is more or less below 10% so  
>> >> adding  
>> >> 3-5% should not be a problem.  
>> >>  
>> >> --  
>> >> Mike  
>> >> Microsoft MVP – Windows Security  
>> >>  
>> >> "FabrizioV" <FabrizioV@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
>> >> [news:7037C317-BE2F-4ECC-9CB1-3C42882E71BB@xxxxxxxxxxxxxxxxxxxx](mailto:news:7037C317-BE2F-4ECC-9CB1-3C42882E71BB@xxxxxxxxxxxxxxxxxxxx)  
>> >> > Good morning Mike.  
>> >> > The article is really interesting and IPSEC is an option to  
>> >> > consider.  
>> >> > An issue (IMHO) is the overhead you'll have on the clients and (most  
>> >> > important) on the servers, when you encrypt all the traffic on your  
>> >> > network.  
>> >> > As you can see in this article :  
>> >> > <http://www.microsoft.com/technet/community/chats/trans/network/net0610.mspx>  
>> >> >  
>> >> > "CPU on servers can be a problem but it can be mitigated by using  
>> >> > IPSEC  
>> >> > offload card from vendors like 3COM and Intel."  
>> >> >  
>> >> > So, if you already have or you are going to buy SSL/IPSEC dedicated  
>> >> > cards  
>> >> > for your data center IPSEC is a good choice.



- Index(es):
  - ◆ *Date*
  - ◆ *Thread*