

## Re: Domain authentication

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-10/0016.html>

---

**From:** Steven L Umbach (*n9rou\_at\_nospam-comcast.net*)

**Date:** 10/01/05

Date: Sat, 1 Oct 2005 10:19:41 -0500

There is no easy solution since internet access "usually" only needs the right default gateway IP address and does not require any sort of computer or user authentication. There are ways to control access to switches on those switches that support 802.1X though this requires an infrastructure that distributes computer certificates to 802.1X capable domain computers to use for authentication via an IAS/radius server before port access is allowed. Microsoft Server 2000/2003 can be a Certificate Authority and IAS server. Another solution could be to use Microsoft ISA 2004 to manage your internet gateway. Then an ipsec require policy could possibly be configured on the ISA 2004 server that would prevent non domain computers from accessing it if user based rules were enabled on it or it otherwise required communications with the client computer so that it was not just a default gateway for the computer. The ISA 2004 newsgroup would be a good place to ask a question about such a possibility and you can download and try ISA 2004 for free with the Evaluation Edition to see if it suits your needs. A non technical solution would be a strict computer use policy that employees review and sign that prohibits unauthorized computers on the network. Such policies need to state possible consequences and be enforced to be effective. An unauthorized computer can be a huge risk as in it could contain a backdoor or a worm on it. --- Steve

<http://www.microsoft.com/isaserver/evaluation/overview/default.msp> ---  
ISA 2004

[http://www.hp.com/rnd/pdf\\_html/guest\\_vlan\\_paper.htm](http://www.hp.com/rnd/pdf_html/guest_vlan_paper.htm) --- example of 802.1X  
using an HP Procurve switch

"HiFi\_Guy" <HiFi\_Guy@discussions.microsoft.com> wrote in message  
news:7C3557A1-1BC5-44A0-9E92-DADCEA4DB1D1@microsoft.com...  
> *HI friends. i m running windows 2003 server having more then 300 clients.*  
> *i want users to join domain if they want to use internet, if they just log*  
> *locally*  
> *on their computers they should not be able to use internet..so any idea*  
> *about this*  
> *plz reply as soon as possible*  
>  
> *have a nice day.*  
>