

RE: Double authentication (User & Machine) with VPN SSL

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2005-10/0388.html>

From: Roger A. Grimes (roger_at_banneretcs.com)

Date: 10/19/05

Date: Wed, 19 Oct 2005 05:07:57 -0400

To: "Peyman" <peyman.secu@gmail.com>

Sorry for the late reply. I've been working a lot.

If you've got Windows and IIS, it should be pretty easy. You can require IPsec certs (i.e. machine certs) to connect the computers to the web server machine using the typical IPsec policy and normal IPsec certs. If your web server is located behind a NAT device, the server would have to be W2K3 (to do NAT Transversal). Then on IIS, Directory Security, enable and require SSL (the normal way), and then ALSO enable Require Client mapping. That feature will require that all connecting users have a User cert, previously mapped (i.e. attached to their Active Directory account) to connect.

If you need more details I can give them.

Roger

```
*****  
***  
*Roger A. Grimes, Banneret Computer Security, Consultant  
*CPA, CISSP, MCSE: Security (2000/2003/MVP), CEH, CHFI, TICS  
*email: roger@banneretcs.com  
*cell: 757-615-3355  
*Author of Honeypots for Windows (Apress)  
*http://www.apress.com/book/bookDisplay.html?bID=281  
*****  
****
```

-----Original Message-----

From: Peyman [<mailto:peyman.secu@gmail.com>]

Sent: Friday, October 14, 2005 4:49 AM

To: Roger A. Grimes

Cc: security-basics@securityfocus.com

Subject: Re: Double authentication (User & Machine) with VPN SSL

SecurityFocus BASICS: RE: Double authentication (User & Machine) with VPN SSL

Hi,

Here are some details on our environment :

- the devices are only on Windows (2k or xp)
- our users will soon have a certificate in a USB token; the laptops have a machine certificate in the Windows certificates container (we consider that this certificate cannot be stolen).
- there is no solution deployed for the moment; we'd like to provide a remote access, and are investigating to find the best solution. For some reasons, we don't want IPSec/L2TP, even if it allows us to make the user & machine authentication. That's why I'm asking my question about the VPN SSL solutions.

Thanks a lot
Peyman

On 10/14/05, Roger A. Grimes <roger@banneretcs.com> wrote:

- > *Need a little bit more about your environment:*
- >
- > *Using Windows or Linux, or both? Using what versions of OS?*
- >
- > *Using built-in software or is a third party solution solution*
- > *acceptable?*
- >
- > *Are smart cards or token devices an option, or do you want it to be a*
- > *software only implementation?*
- >
- > *Roger*
- >
- > *****
- > **
- > ***
- > **Roger A. Grimes, Banneret Computer Security, Consultant *CPA, CISSP,*
- > *MCSE: Security (2000/2003/MVP), CEH, CHFI, TICSA*
- > **email: roger@banneretcs.com*
- > **cell: 757-615-3355*
- > **Author of Honeypots for Windows (Apress)*
- > **<http://www.apress.com/book/bookDisplay.html?bID=281>*
- > *****
- > **
- > ****
- >
- >
- >
- > -----Original Message-----
- > *From: Peyman [mailto:peyman.secu@gmail.com]*
- > *Sent: Thursday, October 13, 2005 1:36 PM*
- > *To: security-basics@securityfocus.com*
- > *Subject: Double authentication (User & Machine) with VPN SSL*
- >
- > *Dear all,*

RE: Double authentication (User & Machine) with VPN SSL

SecurityFocus BASICS: RE: Double authentication (User & Machine) with VPN SSL

- >
- > *I was wondering if with a VPN SSL solution, it is possible to*
- > *authenticate the user and the machine both, with their certificates.*
- > *I know that this could be possible with IPSec Over L2TP (machine*
- > *authentication with L2TP, and user authentication with IPSec), and not*

- > *possible with pure IPSec (just a basic login/password with X-Auth*
- > *available in IKE for a user authentication).*
- > *Just to precise my needs :*
- > *– I'd like to authenticate my users with a certificate because this*

- > *is useful for a remote vpn connection, and also for others needs*
- > *(emails, access to some ressources, applications, etc.)*
- > *– I'd like to authenticate the corporate laptops with a unique*
- > *certificate stored securely on it : this is useful to only allow a*
- > *full network access to the corporate network to trusted machines, and*
- > *also to revoke certificates of laptops that might be stolen/lost.*
- >
- > *Thanks a lot for any help,*
- > *Peyman*
- >