

RE: Cisco VPN client

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2002-02/0933.html>

From: Smith, Chris (csmith@Calence.com)

Date: 02/25/02

From: "Smith, Chris" <csmith@Calence.com>

To: "'cflynn.tech@angelfire.com'" <cflynn.tech@angelfire.com>, security-basics@securityfocus.com,

Date: Mon, 25 Feb 2002 11:32:30 -0700

The UDP port 10000 configuration reference is proprietary to the Cisco VPN 3000 concentrator (formerly Altiga). It does not replace the protocols above, but instead those protocols are encapsulated in the UDP packet for transit between the VPN client and the concentrator. This allows NAT to operate on the UDP header and not on the ISAKMP/ESP/AH directly. If the NAT modification was made on the IPSEC packet directly the integrity of the packet would be destroyed, as header information has been modified and the SHA/MD5 hash comparison would not match. The packet would then be discarded, and the tunnel will not be setup.

Chris

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

From: Cflynn . Tech [<mailto:cflynn.tech@angelfire.com>]

Sent: Monday, February 25, 2002 10:42 AM

To: 'cflynn.tech@angelfire.com'; security-basics@securityfocus.com;

Tumarinson, Max; Smith, Chris

Subject: RE: Cisco VPN client

I just wanted to add that I have not heard of an instance that IpSec was run over port 10000 its designated port is UDP 500, per the RFC. That is for the ISAKMP/Oakley tunnel connection. Then uses IP 50/51 ESP and AH for the IpSec section of the transmission. This is news to me...where did you obtain these facts from??? curious to know.

Regards,

On Fri, 22 Feb 2002 10:06:05 Smith, Chris wrote: >Check the policy/configuration of the VPN concentrator. The previous >version (3.0,3.1) provided the ability to wrap the encrypted IKE/IPSEC >traffic in a UDP packet. This provided the ability to prevent the traffic >from being corrupted due to NAT translation, and simplified firewall >rulesets as well. The downside is UDP isn't stateful, so WinProxy (or any >other firewall) may deny the return traffic from the VPN concentrator to >the client. Placing a rule in the firewall to let the udp traffic in from >the concentrator IP address over the specific UDP port (10000 is default) >may solve your problem. >>RTFL - Read The Fine Logs to determine the traffic being denied. >>Chris Smith >>-----Original Message----- >From: Cflynn . Tech [<mailto:cflynn.tech@angelfire.com>] >Sent: Thursday, February 21, 2002 10:55 AM >To: security-basics@securityfocus.com; Tumarinson, Max >Subject: Re:

RE: Cisco VPN client

SecurityFocus BASICS: RE: Cisco VPN client

Cisco VPN client > > >Are you passing both phase 1 and Phase 2 ... ??? Can you ping anything in >the local LAN?? >--- >Regards, > > >On Wed, 20 Feb 2002 12:11:38 > Tumarinson, Max wrote: >>I am trying to set up Cisco VPN client 3.5a behind a Winproxy 4.0h. I >>am able to authenticate, however I can reach anywhere on the LAN. I >>looked in Winproxy support site and they have a document how to fix it. >>However, that solution did not work for me. Does anybody have any >>idea/suggestion how to approach this problem. >> >>Thanks

>>***** *
>***** >>This message contains confidential information and is intended only >>for the individual named. If you are not the named addressee you >>should not disseminate, distribute or copy this e-mail or its attachments. >>Please notify the sender immediately by e-mail if you have received this >>e-mail in error and delete this e-mail from your system. >> >>E-mail transmission cannot be guaranteed to be secure or error-free >>as information could be intercepted, corrupted, lost, destroyed, >>arrive late or incomplete, or contain viruses. Amalgamated Bank therefore >>does not accept liability for any errors or omissions in the contents of >>this message which arise as a result of e-mail transmission. If >>verification is required please request a hard-copy version.

>>***** *
>***** >> >> >> >>Is your boss reading your email?Probably >Keep your messages private by using Lycos Mail. >Sign up today at <http://mail.lycos.com> > >

Is your boss reading your email?Probably Keep your messages private by using Lycos Mail. Sign up today at <http://mail.lycos.com>

- **Previous message:** [jnf: "Linux hardware firewall question"](#)
- **Maybe in reply to:** [Tumarinson, Max: "Cisco VPN client"](#)
- **Next in thread:** [Cflynn . Tech: "RE: Cisco VPN client"](#)
- **Messages sorted by:** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)