

Re: Solution for NAT and FW Traversal or Pass-through ?!

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-10/12195.html>

From:

Date: 10/21/02

Date: Mon, 21 Oct 2002 11:12:31 -0500

"Melinda Shore" <shore@panix.com> wrote in message
news:aoujpp\$ol0\$1@panix2.panix.com...

- > In article <3db2d07e\$0\$27767\$44c9b20d@news2.asahi-net.or.jp>,
- > Masaya Norifusa <m.norifusa@my.email.ne.jp> wrote:
- > >How about Permeo's solution? You can find details at www.permeo.com.
- >
- > Like some others that have been proposed here (Ridgeway) and
- > **unlike** the protocols mentioned by the original poster,
- > Permeo allows users to circumvent local firewall policy.
- > Application security is a good thing, but giving people
- > tools to defeat network security is a pretty bad idea on any
- > number of levels.

Permeo's server enforces user authentication to each application each time when it is invoked. This is fine grained security check and improves security. This mechanism is generic to any application, and insecure applications could be secure applications.

It supplements lack of the current firewall and coexists each other to provide better security with better connectivity.

- >
- > Also note that the Permeo stuff seems to send traffic over a
- > TCP tunnel. If the application in question is voice, it'll
- > pretty much destroy audio quality.

Not really, UDP is sent by UDP, and not encapsulated in TCP. Before sending UDP, it creates a TCP channel for control purpose. Through this TCP channel, user authentication and proxy negotiation is executed. And, based on these information, the proxy server takes connection authorization process. Since the UDP proxy is arranged after the authentication and proxy negotiation through the TCP (control purpose) channel, the proxy server can know and check whose (destination application server) packets should accept. It rejects UDP packets sent from other destinations.

comp.security.firewalls: Re: Solution for NAT and FW Traversal or Pass-through ?!

So, UDP performance can be kept as expected.

And, I suggest to take a look at explanation on its unique technology, Dynamic Port Management (DPM). It opens a port when needed.

And, on the proxy server, UDP ports are not remained as open when an application ends its communication. Opening and closing ports are synchronized with application behavior to avoid creating a hole on the middle-man,

> --

> *Melinda Shore – Software longa, hardware brevis – shore@panix.com*

> *If you send me harassing email, I'll probably post it*

--

Masaya Norifusa, CISSP
m.norifusa@my.email.ne.jp
m-norifusa@cq.jp.nec.com

- **Next message:** [Tavish Muldoon: "Re: ZA 3.0082 crashing system"](#)
- **Previous message:** [Hugh Pritchard: "Re: Small business firewall appliances"](#)
- **In reply to:** [Melinda Shore: "Re: Solution for NAT and FW Traversal or Pass-through ?!"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)