

RE: [fw-wiz] Apple's iSight and Firewalls

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-08/0077.html>

From: Dave Killion (Dkillion_at_netscreen.com)

Date: 08/20/03

To: "'black@galaxy.silvren.com'" <black@galaxy.silvren.com>, Dave Killion <Dkillion@netscreen.com>
Date: Wed, 20 Aug 2003 11:25:46 -0700

Black,

Some firewalls support monitoring the H.240 command channel for 'open data channel' commands. For those that don't support this application layer monitoring, you'd have to open up a huge range of ports (typically UDP) for the data channels to work. This is the Swiss-cheese problem.

H.323 is one of the most firewall-hostile protocols I've ever seen. Which I why I recommended that instead of opening up all sorts of ports (always a bad idea) that instead they point-to-point encrypt it, and be done with the matter.

There are a variety of different ways to solve this problem, the ideal solution depending on what skill sets Jim has, what sort of features his current equipment has, and what kind of money his management is willing to spend on such a system.

VPN's a drop-dead simple solution with obvious side benefits. But only if your infrastructure supports VPN's.

-Dave

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

From: black@galaxy.silvren.com [<mailto:black@galaxy.silvren.com>]
Sent: Wednesday, August 20, 2003 10:58 AM
To: Dave Killion
Cc: 'firewall-wizards@honor.icsalabs.com'
Subject: RE: [fw-wiz] Apple's iSight and Firewalls

For h.323 an netmeeting, all I needed to do was open udp 1719 to the gatekeeper's address... am I missing something here or where does the "swiss cheese" come into play?

On Wed, 20 Aug 2003, Dave Killion wrote:

> *Jim,*

RE: [fw-wiz] Apple's iSight and Firewalls

Firewall-Wizards: RE: [fw-wiz] Apple's iSight and Firewalls

>
> *If it's a site-to-site video conferencing system, where both sides are*
> *firmly under your control (Corp HQ to Corp Office, etc), I'd strongly*
> *recommend a VPN tunnel, which solves most of the Swiss-cheese problems.*
> *This is something you should already have, anyway.*
>
> *Just a thought...*
>
> *Dave Killion*
> *Senior Security Engineer*
> *Security Group, NetScreen Technologies, Inc.*
>
>
>
> -----Original Message-----
> *From: jseymour@LinxNet.com [mailto:jseymour@LinxNet.com]*
> *Sent: Tuesday, August 19, 2003 5:43 PM*
> *To: firewall-wizards@honor.icsalabs.com*
> *Subject: [fw-wiz] Apple's iSight and Firewalls*
>
>
> *Hi All,*
>
> *My company would like to set up inexpensive video-conferencing.*
> *They've been bugging me for a solution for some time. The partner*
> *company, being All Windows, All The Time, of course immediately*
> *suggested NetMeeting. ISTR a discussion about NetMeeting here, perhaps*
> *prompted by me, and, IIRC, it pretty much requires one make swiss*
> *cheese of their firewall for it to work. I vetoed it, and management*
> *backed me up. Doing a search on "NetMeeting" on SecurityFocus was not*
> *encouraging, either.*
>
> *Recently they bought me an iBook to do some WebObjects development*
> *with. It just hit me today that maybe Apple's iSight product would do*
> *the trick for video conferencing.*
>
> *Problem is: I've no idea what iSight would need through the firewall.*
>
> *There's this:*
>
> <http://www.macosxhints.com/article.php?story=20030623203213301>
>
> *If 5060 and 16384 through 16403 UDP are all that are required, and I*
> *can specify the only allowed IP address inside they would forward to,*
> *well, that might be acceptable.*
>
> *Comments? Opinions? Suggestions? Flames? ;)*
>
> *Thanks,*
> *Jim*
> --

RE: [fw-wiz] Apple's iSight and Firewalls

Firewall-Wizards: RE: [fw-wiz] Apple's iSight and Firewalls

> *Jim Seymour / PGP Public Key available at:*
> *jseymour@LinxNet.com /*
> *<http://www.uk.pgp.net/pgpnet/pks-commands.html>*
> *[http://jimsun.LinxNet.com /](http://jimsun.LinxNet.com/)*
> _____
> *firewall-wizards mailing list*
> *firewall-wizards@honor.icsalabs.com*
> *<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>*
>

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

- application/x-pkcs7-signature attachment: [smime.p7s](#)