

Re: [fw-wiz] IPv6 and IPSec

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-08/0136.html>

From: Michael H. Warfield (*mhw_at_wittsend.com*)

Date: 08/31/04

To: "Paul D. Robertson" <paul@compuwar.net>

Date: Mon, 30 Aug 2004 19:07:44 -0400

On Mon, Aug 30, 2004 at 08:00:02AM -0400, Paul D. Robertson wrote:

> On Sun, 29 Aug 2004, Michael H. Warfield wrote:

:

> > IPv6 is VASTLY more interesting than this... There are lots
> > of things that are interesting (both in the good sense and the bad
> > sense) about IPv6 and security. Consider "privacy enhanced addresses".
> > Now, as a system administrator, how are you going to track down a virus
> > infected system that changes its address every half hour with no audit
> > trail?

> This is something I need to read up on, I don't recall it being around
> when I last looked, but perhaps I simply overlooked it... I was more
> interested in using the encapsulating headers to rope off control and
> provide transit a layer or two deep and add some separation for different
> populations - all problems I no longer have directly.

Yeah, privacy enhanced addresses were proposed to deal with the reported privacy issues associated with the automatically generated EUI-64 addresses (you can be, theoretically, tracked as you roam from network to network). They change each time you boot and can even change dynamically with time and at random. Just new in the last couple of years.

> > I restrict ssh to IPv6 only (hell, it's virtually unscannable and
> > has no broadcast address and is reachable from anywhere I am on IPv4, why
> > not...). Some of my external servers, the ssh listens only on certain
> > IPv6 addresses. And those addresses change every 15 minutes. A new address
> > is added every 15 minutes and the dns is updated (w/ TSIG). Each address
> > is valid for 2 hours (to allow for DNS TTL). After that time, it's
> > deprecated. When a deprecated address no longer has a resource (socket)
> > attached to it, it ceases to exist on the machine. Every IPv4 address
> > has an entire IPv6 NETWORK (65,536 subnets each containing 16 billion
> > billion host addresses). I have yet to find anywhere on the entire
> > internet where IPv6 does not work (private address space or global address

Firewall-Wizards: Re: [fw-wiz] IPv6 and IPSec

- > > *space), and it works well. I can reach all my IPv6 stuff from anywhere*
- > > *on IPv4. Why leave it expose and vulnerable (to scanning and probes) on*
- > > *IPv4? Even my virtual web server farm has web services on IPv4 but all*
- > > *the security stuff is tightly marshalled over IPv6.*

- > *Won't the 4<->6 gateway be vulnerable anyway? In a mixed environment, it*
- > *seems that you'd be stuck with the v4 problems until the environment isn't*
- > *so mixed anymore.*

Ah... Now that gets into implimentation details.

Actually, no, if you do it right. You provide a primary address from which errors are "sourced" but no services listen (blocked by the firewall). Someone connecting to a service has to know the complete IPv6 address (not just the upper 48 bit 6to4 prefix) so they have to figure out the 16 bit SLA and the 64 bit EUI. And, since errors return from that non-functional source addresses, using error returns don't help. I'm not even aware that anyone is even poking at 6to4 currently, but it can be shielded to not reveal what the valid SLA and EUI of the outward facing interface is. Without that, you aren't going to connect to that service. There are other groaddy details on removing addresses and deprecating them and dealing with things like persistent UDP sockets (like CIPE). It's not a solution to everything. Just another tool for specific applications. Nice thing is that, with IPv6, you can have so MANY addresses on the same box at the same time, that you can easily mix and match them to their purposes and schemes.

- > > *How do you scan for backdoors, when the intruder adds his own*
- > > *unique address (hell, you can add IPv6 to XP without even rebooting the*
- > > *damn thing and you have to reboot Linux to disable it) amongst*
- > > *16 billion-billion possible addresses on that wire? How do you deal*
- > > *with bot-nets, were every bot is given a unique contact addresses and*
- > > *the server has has thousands of addresses added without having to ask*
- > > *anyone?*

- > *Have you seen any botnets using v6 in the wild? I assume that you still*
- > *need some sort of v4<->v6 gateway for most leaf nodes these days, so the*
- > *traffic will still come down to a v4 address until everyone routes v6*
- > *directly.*

Several IRC bots have IPv6 patches. EggDrop has IPv6 amongst others. There has been quite a bit of activity in the underground around IPv6, particularly in Europe. Lance Spitzner had one of his honeypots broken into and the first thing the intruders did was to set up an IPv6 tunnel back out that slid right past all the IDS they had. That's what first got my attention, several years ago, and got me digging deeper. And the deeper I dug, the scarier it got.

- > > > *Want to check out something really NASTY, check out Teredo.*
- > > *That's IPv6 over UDP. A buddy at MS refers to this as the "Evil*
- > > *Firewall Destroying Deamon from Hell". Do you worry about UDP traffic*

Firewall-Wizards: Re: [fw-wiz] IPv6 and IPSec

> > *over port 3544? Should you be? Some people have already found out,
> > to their regret, that they should be.*

> *Tunnels have always been an issue for protected networks. It's one of the
> reasons that I wouldn't allow anything that wasn't proxied when I was
> running operational user networks. From there, you normally just need to
> do utilization reporting to detect whole-network tunnels, though traffic
> inspection at some point becomes necessary once the tunnel thresholds go
> under normal usage.*

Teredo is especially troubling because its on a high order UDP port that is commonly not blocked.

> > *IPv6 has LOTS of security implications. They're just not obvious.
> > And a lot of people (particularly in North America) have their heads in the
> > sands vis-a-vis IPv6. At many of my talks, I've had people walk up to
> > me later and tell me that they've been seeing this strange traffic on
> > their network for ages, they just didn't know what it was. And now they
> > know, and now they need to figure all this out... IPv6 arrived several
> > years ago and anyone who thinks they don't have IPv6 just doesn't know
> > that they have it already, and that they don't control it, and that it's
> > uniformly routable, and that it's globally addressible (whether their IPv4
> > addresses are globally addressible or not).*

> *Hmmm, but won't the default deny access lists on my border stop it unless
> I specifically allow IPv6 in? It seems to me that if I'm doing all the
> right things[1], my exposure should be tunnels and mistakes. Tunnels are
> an issue with IPv6 as well, though blocking v6 DNS does seem like a
> reasonable bit of defense in depth if I'm not quite ready to deal with the
> other issues.*

Basically true. Except there are so many transition mechanisms over which IPv6 can be tunneled that it's actually cheaper and easier to provide it properly than it is to try and prohibit it. I'm now even playing with protocol 41 (aka SIT, aka IPv6, aka 6over4) over NAT. Turns out that a lot of NAT devices support this (more by accident than anything else, I strongly suspect, they just don't exclude it from the NAT logic and don't know what else to do with it). You just need to know how to configure the tunnels so both ends and both layers "get it right". But then it works. :-) New toys to play with...

> > *But... Back on the original topic... IPSec is not required
> > to use IPv6. It's only required by implimentations to be supported in
> > order to be "IPv6 compliant". Use it if you wish, or don't use it if
> > you wish. You don't have to support IPSec to be IPv4 compliant, but you
> > do have to support it for IPv6. Outside of just supporting it, it's
> > the same as it ever was.*

> > *OTOH... IPSec CAN be REALLY usefull in supporting IPv6! My
> > laptop has over a dozen different ways of connecting to IPv6 no matter
> > where I am in the world. If I can pull a native prefix, great. If not,*

Firewall-Wizards: Re: [fw-wiz] IPv6 and IPSec

> > *I can go 6to4 or 6over4, no problem. If that doesn't work, my next fall
> > back is IPSec on IPv4 (to tunnel my IPv6 stuff over a VPN) and IPSec NAT-T
> > (IPSec over UDP port 4500) next. If those fail, then I start resorting
> > to things like PPP over stunnel or PPP over ssh (both of which have been
> > tested). Beyond that, there are even more access methods that I've never
> > tested because I've never run into a circumstance where none of the above
> > didn't work. In most corporate environment with really strict rules,
> > IPSec NAT-T (forcing NAT-T even when not cross a NAT) works like a champ.
> > Have never been force to resort to things like CCTT, even though they
> > are there and ready if I ever find anything that gets in the way of what
> > I normally use. IPSec (particular NAT-T) is a great firewall bypass tool.
> > Ya don't need to run IPSec on IPv6 when you are already tunnelling IPv6
> > over IPSec. :-)*

> *Dammit, I don't have _time_ to play... But now you're gonna make me...*

I know... I know... I just keep making peoples lives around
me more complicate. Story of my life. :-)

> *Paul*

>

> *Paul D. Robertson "My statements in this message are personal opinions
> paul@compuwar.net which may have no basis whatsoever in fact."
> probertson@trusecure.com Director of Risk Assessment TruSecure Corporation*

Later!

Mike

--

Michael H. Warfield		(770) 985-6132		mhw@WittsEnd.com
/\ \ =mhw=\ \ /		(678) 463-0932		http://www.wittsend.com/mhw/
NIC whois: MHW9		An optimist believes we live in the best of all		
PGP Key: 0xDF1DD471		possible worlds. A pessimist is sure of it!		

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

- application/pgp-signature attachment: stored