

# Re: Port 443 Outbound

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2009-04/msg01265.html>

---

- *From:* "Cliff Galiher" <[cgaliher@xxxxxxxxxx](mailto:cgaliher@xxxxxxxxxx)>
  - *Date:* Fri, 17 Apr 2009 17:06:26 -0600
- 

In theory, yes, but in practice, not really.

The truth is that there is a very small number of firewall OS's out there. If you've done what you should with your network (only admins can install apps, etc) then malware has gotten behind your network because \*it\* has admin access, and it is trivial for malware to \*use\* that admin access to reconfigure a firewall, whether that is software or hardware.

I remember when ZoneAlarm made a big deal that they checksum files on their allow list and Symantec's product didn't. Within about a week there was a new trojan that installed itself as a DLL in IE, so IE's checksum still worked out and it got past ZoneAlarm with no problem.

All I'm saying is that if something has access to your network then you have bigger problems and it getting past your firewall to "phone home" is the least of your problems. It can lie, alter logs, or alter other machines to find away around your precautions. Or worst case scenario, (and there are viruses that do this) trigger a doomsday payload because they \*can't\* call home...where if they did, they'd quietly keep collecting data.

In a weird way, I think I'd rather have something do what it is programmed to do, so I can get IP addresses and \*maybe\* recover from it. But relying on egress filtering for security is, in my opinion, nearly worthless. I know others may disagree.

-Cliff

"John gordon" <[johngordon@xxxxxxxxxxxxxxxx](mailto:johngordon@xxxxxxxxxxxxxxxx)> wrote in message [news:#2oTo05vJHA.5836@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:#2oTo05vJHA.5836@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Thanks for that.

Agreed - I would much rather nothing got on the network in the first place and have Trend and auditing set up (not Snort admittedly) but surely a device that could monitor 443 outbound would only act as an extra layer of defence ?

"Cliff Galiher" <[cgaliher@xxxxxxxxxx](mailto:cgaliher@xxxxxxxxxx)> wrote in message [news:O2InkX5vJHA.3832@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:O2InkX5vJHA.3832@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Here is my take.

An edge device should \*not\* be used to block or even detect malware on your network. Even if you do successfully stop it from calling home, it is

## Re: Port 443 Outbound

already behind your firewall and thus has unprecedented access to your network. Who knows what the payload is or what its instructions are if it \*can't\* contact home. No no...an edge device is used for inbound blocking and filtering, but is not an effective security boundary for malware already in your network.

You can use outbound filtering to prevent some abuses by employees such as email port blocking from all IP's but the server, or DNS filtering to prevent lookups of certain sites such as youTube. But those aren't necessarily "security" related as much as they are policy related.

No, there is no substitute for good internal network monitoring. Centralized AV is a good start, but auditing is also important. Microsoft Baseline Security Analyzer, Snort, etc, are all good tools to have set up and running regularly.

-Cliff

"John gordon" <johngordon@xxxxxxxxxxxxxx> wrote in message  
news:e2L\$wizvJHA.5100@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

I recently came across articles discussing malware's use of ports 443 and 80 outbound to "call home".

I have always set my own systems up to use egress filtering to for instance only allow email traffic out to my ISP's Smart Host from my server's IP (but these two ports—443 and 80 I leave open outbound in order to allow web browsing etc). In one article

(<http://blogs.windowsecurity.com/shinder/2008/02/03/tcp-443-the-universal-firewall-port-1>

Dr Tom Shinder talks about web proxies from Blue Coat and Collective Software. What is the best way to counter this threat of malware communicating outbound over 443 and 80 in an SBS 2008 environment ? Can any of the hardware firewalls that have been discused in this forum such as those from Watchguard and Sonicwall see inside an outbound 443 connection ? Or are such proxies the answer ? Comments would be welcome. Or am I talking rubbish ?