

Re: Outbound ports

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2003-10/1332.html>

From: Leythos (void_at_nowhere.com)

Date: 10/23/03

Date: Wed, 22 Oct 2003 22:30:21 GMT

In article <Xns941C8DBE58A2Ajuergenniever@nieveler.org>, juergen.niever.nospam@arcor.de says...

> Leythos <void@nowhere.com> wrote:

>

>> *I would not want to allow more than port 80 and 443 outbound on a public web server sitting in my DMZ.*

>

> *How are people going to use it, then? Destination Port 80 outbound means that you allow people ON your webserver to surf to other webservers ;-)*

You really gotta be kidding – I hope. I would never allow more than port 80/443 outbound from the WAN to the DMZ (maybe FTP, depending on the resource need) (or inbound for the DMZ). Yea, I made a little mistake by saying ourbound and not qualifying the direction – sorry.

>

>> *If the machine were compromised blocking outbound on all but those ports could prevent traffic from infecting other machines on the internet.*

>>

>> *If you block outbound ports, except the ones you actually need, you limit what things your computers can do should they become compromised.*

>

> *Caveat: This only applies for real firewalls, not "Desktop Firewalls".*

When it comes to security I only consider REAL firewalls, not personal ones. Who would use a desktop firewall on a server?

>> *For instance, if you don't allow 135~139, 445, and 8 outbound you don't have to worry about people making standard windows share connections to machines on the internet and you don't have to worry about your machines pinging them either.*

>

> *Uh... you're confusing inbound and outbound again. And pinging doesn't require ANY ports, it only requires the ICMP protocol – that's an important difference.*

comp.security.firewalls: Re: Outbound ports

If you don't allow LAN OUTBOUND of 135~139, & 445 then you don't have to worry about your internal machines trying to connect to external machines (outbound). So, if your internal machines get infected they can't get out on normal RCP ports to hit other machines. Sure, they can get out on the DNS, HTTP, HTTPS, FTP ports, but they don't really need to make mapped share connections to some unknown users computer in China do they?

OK, I'll admit it, I made a mistake in PING and trying to state port 8, it would have been correct to block ICMP and UDP through the firewall from DMZ to LAN, from WAN to ALL, and from DMZ to WAN – you might want to allow LAN to WAN, but I still block it. I do allow ping from one set of internal machines to exit the firewall WAN port from the LAN side.

> *Not to mention that it would be rather stupid to prevent your own machine from pinging others – how do you troubleshoot connections without ping?*

Why would that be your only tool?

In my DMZ, none of the systems can PING anything outside of the DMZ, why would they need too? I can see in the firewall manager what's happening with each IP/port, so I don't really need to PING anything.

Rather than banter back and forth, tell me how many subnets you have in your home/office and what you use for a firewall – then tell me how many servers and what OS they are running.

I have 9 servers running W2K/IIS and 3 with RH9.1 (test servers), also have email and MS SQL/ Oracle 9i. These sit in the DMZ, I have more servers in the LANs. I have two WG firewall appliances and 5 subnets behind them. I have an additional set of Linksys routers for development areas and test areas just to isolate them from the development network users. This is just in my home (not counting all the workstations).

When it comes to protecting my home I'm as anal about security as anyone can be, and I'm the same way when I design a network for customers. In 20+ years of working with computers (unix, mainframe, PC, etc...) not one computer I own or control has been compromised.

I can assure you that just shutting down services is not doing to protect your investment, it takes looking at security at many more levels that just services running on a computer.

--
--

spamfree999@rrochio.com
(Remove 999 to reply to me)