# Ephemeral ports and network security

Tags: ACG

Is opening Ephemeral ports safe? Are we not opening our network to the hackers?

The short answers are yes, and yes. The only difference between a customer and a hacker is intent. You cannot service Customers without opening these ports, so how do we exclude hackers?

Security is implemented by having multiple tools and methods that narrows the traffic to just what is needed, and then again filters the the content of the traffic.

In networking there is the concept of the OSI stack (external site, opens in new tab) which describes the network as a series of layers that ranging form the purely binary signals up to complex applications. While originally intended to describe communication protocols, it is also useful to describe the layers of filtering that can be used in security.

In the lower layers we can exclude traffic from certain addresses and using certain protocols. This done in layer 3 & 4. This is where the Security Groups and network Access Control Lists (nACLs) work. As noted before we have to let some traffic in to provide service to our customers, so what is to stop a bad player from coming in the same ports and attacking you.

The answer is they do try. However we use the other layers to filter them out, layers 5 through 7. For instance session state will allow us to seperate conversations that we are already having with authenticated people, from unauthenticated people trying to start a new conversation. New conversations may need to go through an application (layer 7) authentication process. We can use application code (layer 7) to filter what can come in to the application. This may mean that embedded scripts or commands or binary objects are blocked or stripped out preventing bad players from using them to try and bypass the application security. These tools and methods are part of application design and the tools that a developer chooses to use in the application.

With regard to the Ephemeral ports. There are intended to only be used in an established communication stream. The Operating System network stack enforces rules that prevent new conversations being started on these ports unless explicitly authorised by a higher level application. This is quite robust assuming two things:

1. You do your patching so that the operating system is kept up to date with any discovered weaknesses.
2. You don't allow a virus or trojan into your system though some other means which could then issue the right instructions to open these ports from the inside.

Those who are malicious can easily craft a script to work directly on the NIC to direct traffic to the ephemeral ports on your instance.

However that is a reason that we use the provided tooling, do patching, and hosting providers deploy all those expensive network protection services for us.

Our defenses are:

- We maintain a healthy un-compromised Network stack that will not accept new inbound conversations on the ephemeral ports (unless you tell them to).
  They have tests to confirm that it is response traffic and has the correct hand shaking.
- We maintain our anti-virus / anti-malware tooling to block attacks from the inside.
- We use per-device fire walls functionality such as Security Groups and nACLs.
- Our hosting provider's perimeter Network firewalls
- Plus, optional network IDPS systems to monitor for odd behaviour on the networks.

There are many smart, motivated, and well funded people who will try to compromise your system. (Even a lab machine can be useful as an attack bot). So it is incumbent on you to take all reasonable precautions, even in a lab. For instance, even though it is just a lab practice limiting inbound traffic to just your personal workstation (or your external firewall) and just the ports you need. You can find this via the SG console or web services like what is my IP address.

Only use 0.0.0.0/0 or any port when you determine that it is necessary, and you have sufficient other protections in place appropriate to the situation.

Protect your keys. Seriously! Protect them. Use encrypted folders, or an encrypted USB key, or a reliable password-vault.

Pretend that your financial future is at stake and think about what you can do to make things less open. What you practice in the labs can be used in real world commercial situations.

See more about security on Trend Micro (external site, opens in new tab).

---

If you need help, please email Pluralsight Support (opens email form) for 24/7 assistance.