If you see “No Valid Threat License”, you need to check for Dynamic updates. In WebGUI, go to Device > Dynamic Updates and click “Check now.” After the new update is listed, download and install it.

**CCDC PA Firewall Notes**

**1.** The entire competition uses private IP addresses. This makes it easy to block outbound connections to private IP addresses which seriously prohibits the red teams ability to get connections back to themselves.

**2.** Not enough “noise”, it is very easy to determine between the red team and the scoring engine when looking at access logs and firewall traffic logs.

**3.** The scored DNS only resolves internal addresses which makes it easy to block toole like DNScat by blocking all outbound DNS queries. Since the environment is virtual, it is easy to resolve from your host and then find the IP from there, or throw stuff on transfer.sh or pastebin and get to that by IP from inside the environment.

# Ports

**Based on Functional Services:**

HTTP 80 TCP/UDP

HTTPS 443 TCP/UDP

SMTP 25 TCP (TCP port 465, 587 as well?) (TCP port 3535 is SMTP alternate)

POP3 110 TCP

SSH 22 TCP

DNS 53 TCP/UDP

**Other:**

NTP 123 UDP

137, 138, 139 NetBIOS TCP/UDP

43 whois TCP

# Day Before Setup

From Matt:

So this, to me, is a critical part of the precompetition planning.  Having a good staging site (or two or three) is great.  We've used file.io with great luck (since you can curl on the linux side) then just write down the URL for the writer or let them take over the console and write it down or copy paste to pull the information down from the file.io site.

This is also a huge thing to have going into the competition.  Upload inject templates, exe's that you want to run, scripts, GPO templates, FW templates, Windows Updates, etc etc and write down the URLs.  Print them off then access your sites in the environment.  This is allowed per the current rules, since these are technically public sites and anyone with the URL can download the content during the time frame.

# Strategy

## Points

**Functional Services**

Certain services are expected to be operational at all times or as specified throughout the competition. In addition to being up and accepting connections, the services must be functional and serve the intended business purpose. At random intervals, certain services will be tested for function and content where appropriate. Precise services to be scored are configured by the scoring management team, but will be delineated via the ISE/Team Portal.

HTTP

A request for a specific web page will be made. Once the request is made, the result will be stored in a file and compared to the expected result. The returned page must match the expected content for points to be awarded.

HTTPS

A request for a page over SSL will be made. Again, the request will be made, the result stored in a file, and the result compared to the expected result. The returned page needs to match the expected file for points to be awarded.

SMTP

Email will be sent and received through a valid email account via SMTP. This will simulate an employee in the field using their email. Each successful test of email functionality will be awarded points.

POP3

POP3 connections will be performed against the system using usernames from Active Directory. Once connected a series of commands will be run and the output examined. Correct responses will be awarded points.

SSH

An SSH session will be initiated to simulate a vendor account logging in on a regular basis to check error logs. Each successful login and log check will be awarded points.

DNS

DNS lookups will be performed against the DNS server. Each successfully served request will be awarded points.

## Zero Trust Notes

* Micro-Segmentation
* Granular Perimeters Enforcement based on user data, and location.
* Limit lateral movement.
* Zero Trust – assume any computer device and user can be compromised; inspect all traffic entering and exiting each of your network devices.
  + <https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture>
  + Layer 7 threat prevention
  + Identify a “protect service” containing all critical data, assets, applications, and services (DAAS).
  + Identify how traffic moves across the organization in relation to protect surface.
    - Who are the uers
    - Which applications are they using
    - How are they connecting
  + Understand interdependencies between the DAAS, infrastructure, services and users; then place controls in palce as close to the protect surface as possible, create a microperimeter around it.
    - A next-gen firewall (also called a segmentation gateway) can be used to create the microperimeter.
    - Kipling Method: defines Zero Trust policy based on who, what, when, where, why and how.
    - Only possible at Layer 7.
  + After building, continue to monitor and maintain in real time.

Zero Trust Action Plan:

1. Identify the protect surface
2. Map the transaction flows
3. Build a Zero Trust architecture
4. Create Zero Trust policy
5. Monitor and maintain