CCDC Firewall/Palo Strategy:

Step 1: Login to the Palo and immediately change the admin passwords. There should be two accounts: admin and administrator. The "admin" account is the one we need for administrating the Palo. The other account is superfluous. Change passwords for both.

Step 2: Monitor the logs and start writing down the addresses that are hitting the firewall most. This step is best done before the red team is released, as before the flag drop the only hosts communicating with our internal servers are the scoring engines. Monitor both the addresses and the ports (services) that are being connected to. Most of them should be coming from the same VLAN segment (ex: 10.10.xx.xx).

Wiki for log monitoring

Step 3: Pay careful attention to the different zones in the firewall. Most of our servers should be in the "internal" and "user" zones, which are mostly grouped by VLANs. Hosts that are coming from outside our network are in the "External" zone. This is the originating zone for most of the traffic. Interzone traffic must also be monitored, as attackers could leave trojans inside our network. These trojans may piggyback on our servers and mount additional attacks.

Step 4: Start creating ingress and egress rules for the firewall. The rules in Palo are read top-to-bottom, which means that when a packet is first received by the firewall, its source and destination attributes are matched with the first rule in the table first, second rule second and so on. Which means, the very first rule in the rulebase table needs to be "drop any and all". This is a catchall rule for all packets that do not match any of the subsequent "allow" rules.

Wiki for creating rules

Step 5: Have a running list of potential scoring engine hosts. We need to let them through the firewall so that they can monitor the services that we need to provide and maintain. Services that the scoring engine needs to reach are (but not limited to): DNS, Active Directory, Splunk, NTP etc. Block everything else.

Step 6: Monitor the logs throughout the entire competition. Suspicious hosts always spam the firewall with various port scans. Port 22 (SSH) is especially suspicious. Block this port even inside our network, and notify your teammates that they need to access their servers through physical terminals.

Step 7: During injects, you will need to provide various internal services to your teammates, such as opening up FTP servers, allow HTTPS etc. At this point, the firewall should reach a steady state operation, with very few tweaks to the rulebase.

Additional work: Careful consideration must be given to injects throughout the entire competition. They are worth quite a few points.

Also, it is worth having a list of addresses that belong to our internal servers. Keep it near the desk where the team lead sits, so that it can be easily accessed by all team members.