How to Install a Security Onion (SO) Manager Search Node

Task. Install a SO Manager Search Node.

Purpose. Security Onion is a free and open source platform for collecting, correlating, and escalating events using Intrusion Detection System (IDS) alerts, netflow, server transactions, Packet Capture files, and Windows Event logs. Depending on how it is deployed, SO can serve as a Security Event and Incident Management (SEIM) server and/or Network IDS (NIDS).

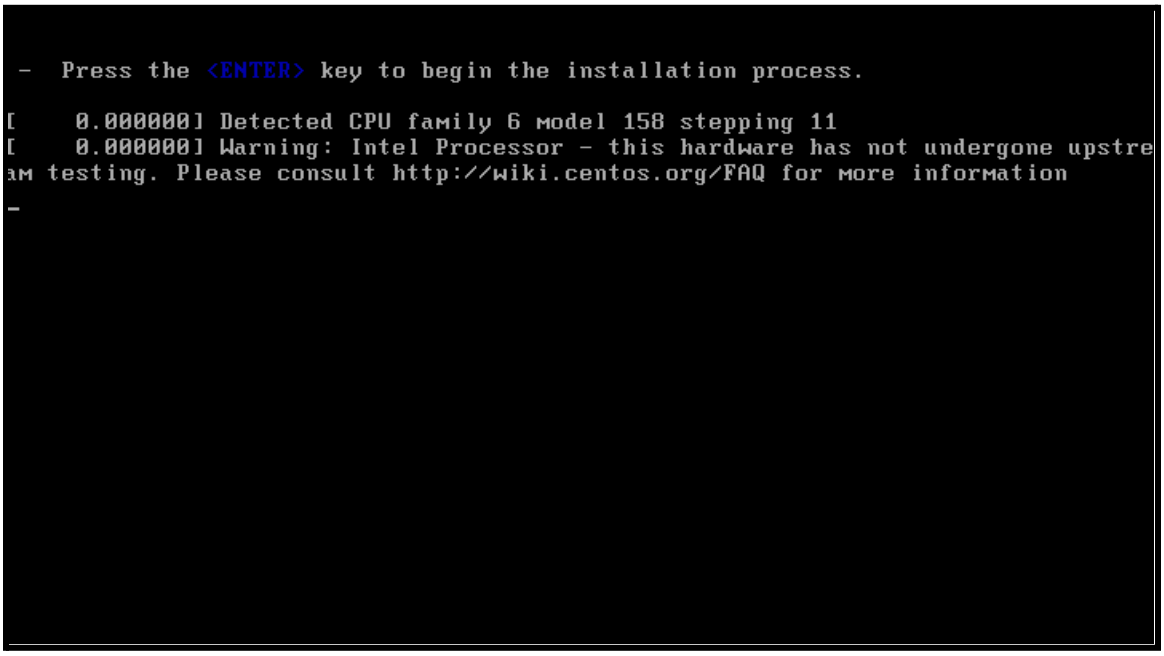
Conditions. You have a computer with 4 CPU cores, at least 24 GBs (24,576 MBs) of RAM, 100 GBs of storage, and two Network Interface Card (NIC) adapters. You have the latest SO optical disc image (a.k.a ISO file) downloaded. You have knowledge of the networking information you want the SO Manager Search Node to use.

- https://github.com/Security-Onion-Solutions/securityonion/blob/master/VERIFY_ISO.md

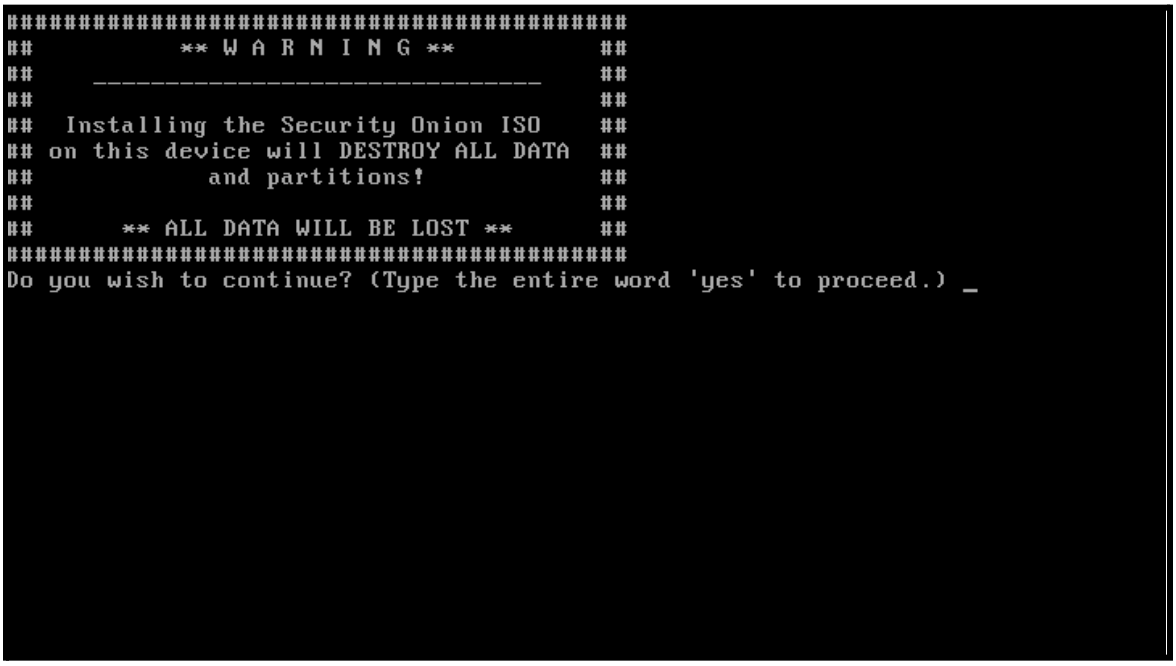
Standard. You were able to install a SO Manager Search Node and access it via a web browser.

Step 1. Boot the computer using ISO file. This requires either a bootable USB or CD with SO installed on it. Select “Install Security Onion in basic graphics mode” when prompted.

Step 2. Press the “Enter” key when prompted.



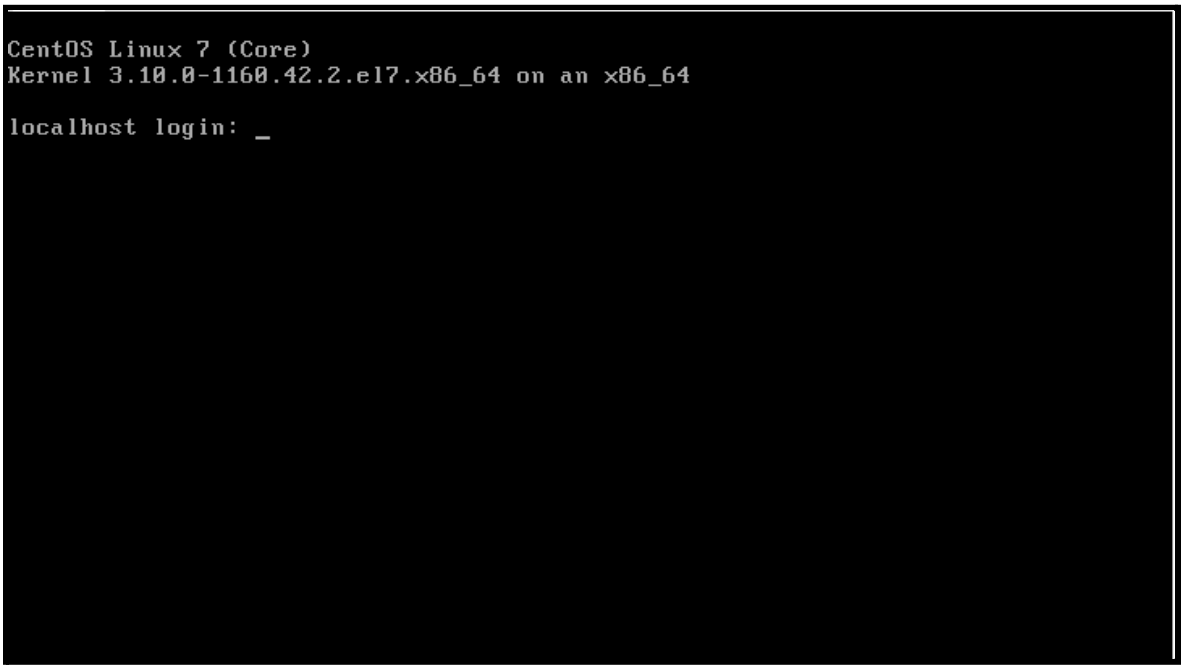
Step 3. Type “yes” when prompted to continue the installation process.



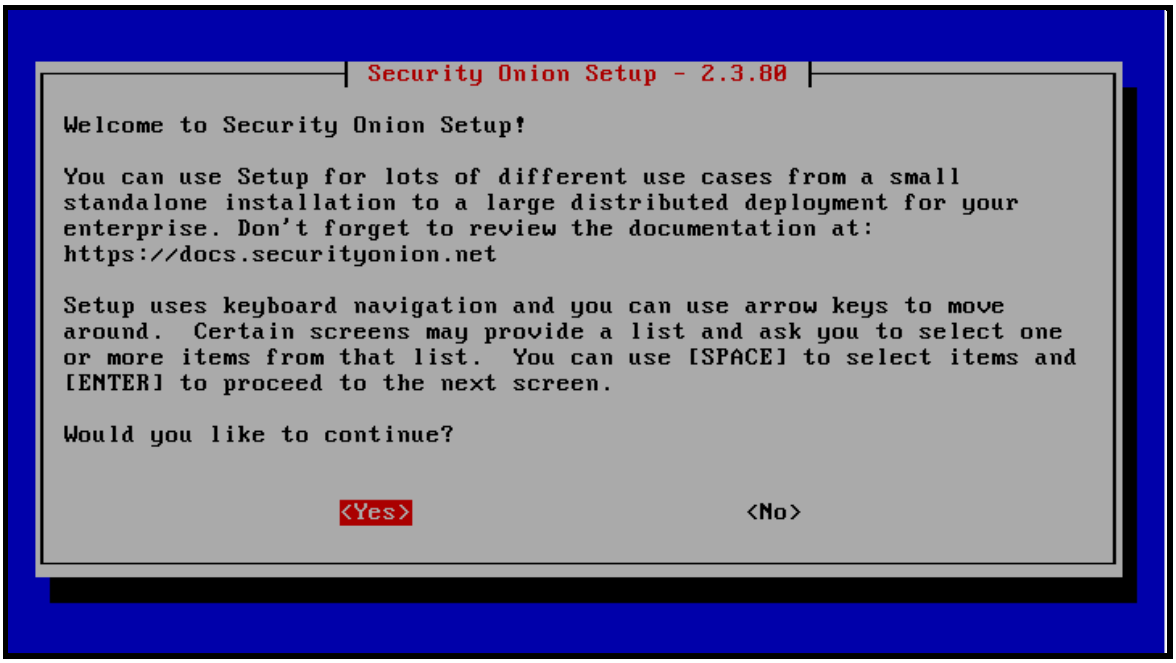
Step 4. Enter a username and password for the first local administrator account to be created. DO NOT create a generic username (i.e., admin, soadmin, etc.). Instead, specify the username of the person installing SO. For example, if Victor Fernandez is installing SO, type "victorfernandez." After declaring and confirming the first local administrator's password, press "Enter" and wait for the automatic installation and post-installation setup tasks to finish.

Step 5. Press "Enter" when prompted to reboot the computer.

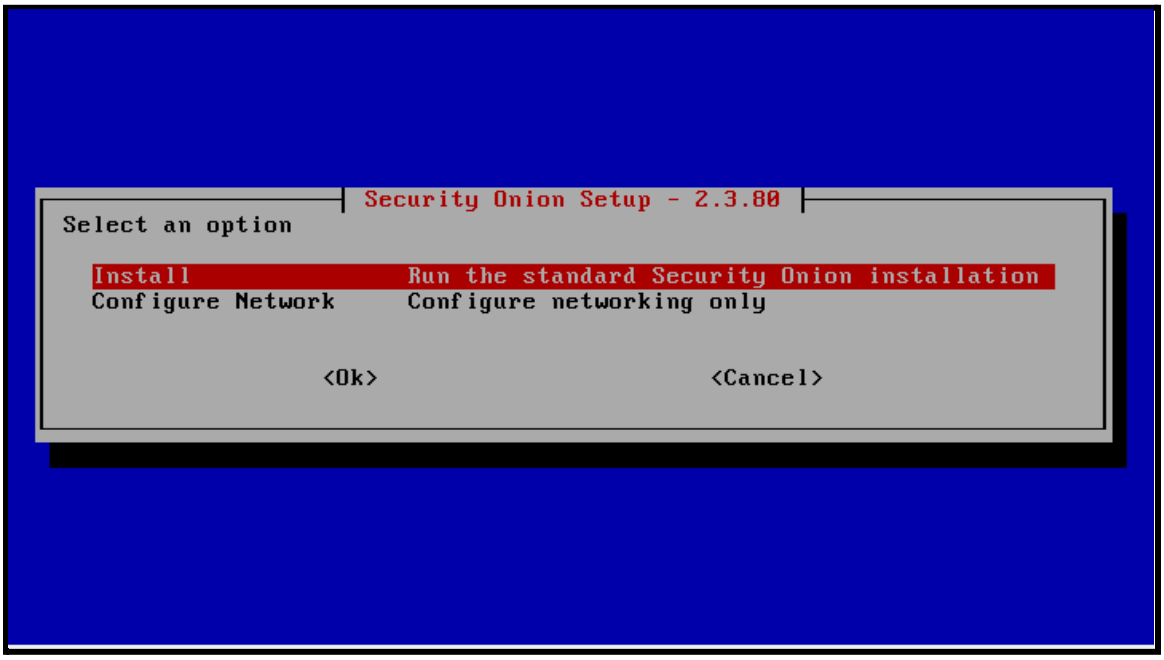
Step 6. Login using the credentials you specified for the first local administrator account.



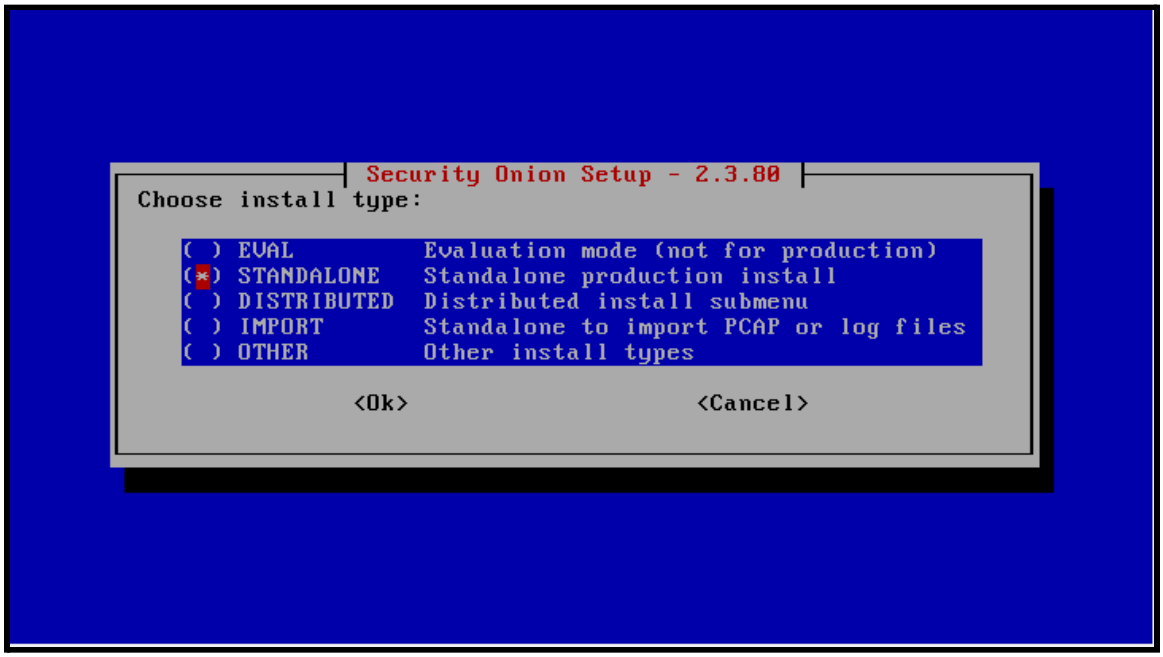
Step 7. Press “Enter” when prompted to begin configuring SO. As mentioned in the displayed text, the “space-bar,” “Enter,” and arrow keys will be used to navigate through the follow-on prompts. The “space-bar” will be used to select options. The “Enter” key is for proceeding to the next prompt. The arrow keys allow you to toggle between options.



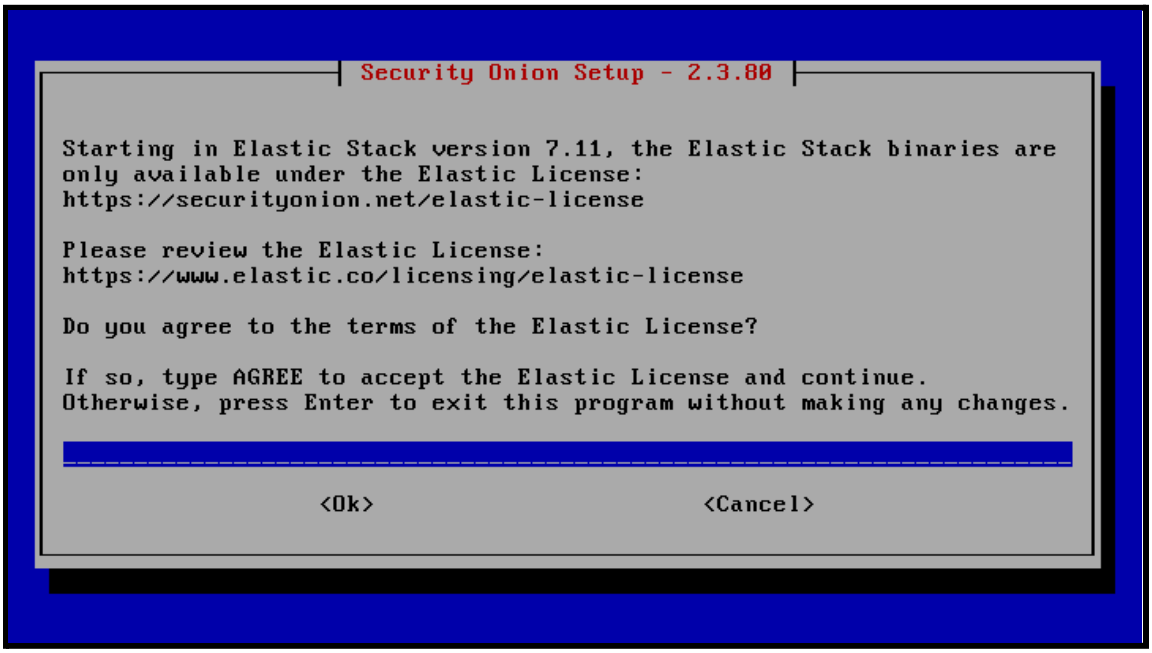
Step 8. Select “Install” and press “Enter” when prompted to specify the setup option.



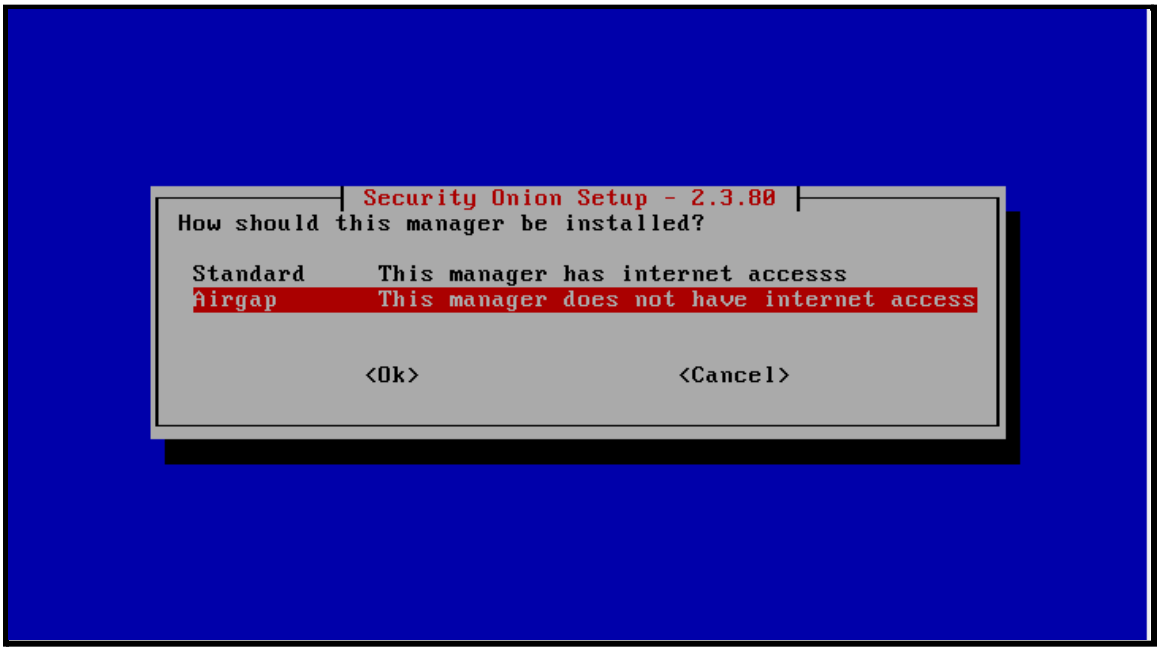
Step 9. Select “STANDALONE” and press “Enter” to specify the install type.



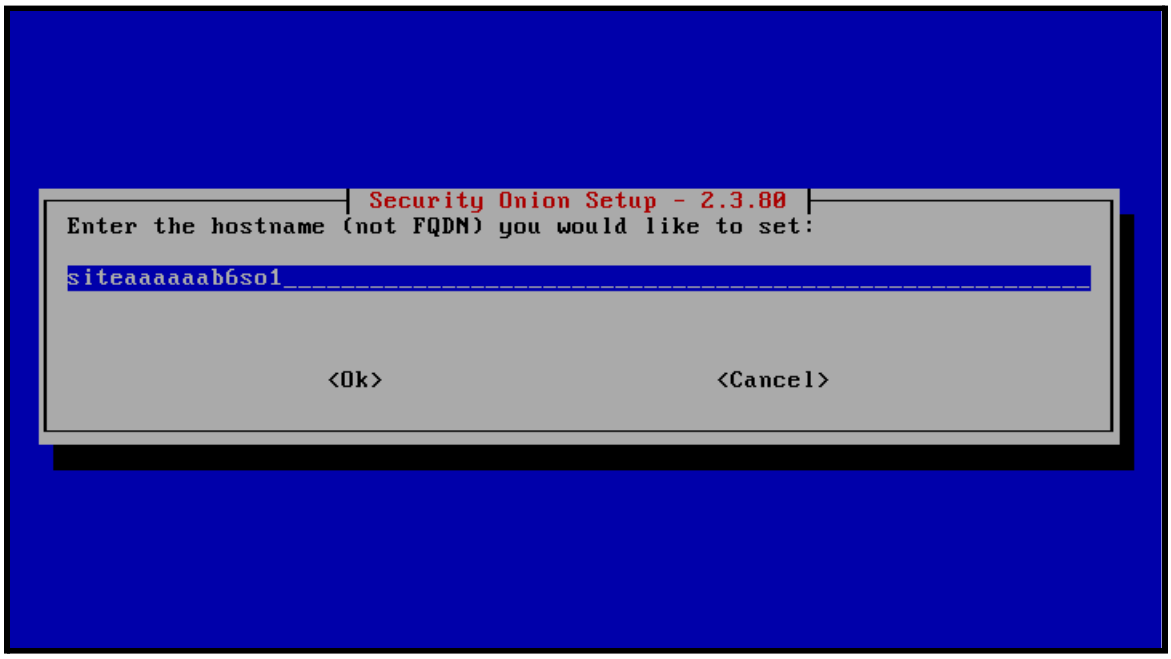
Step 10. Type “agree” when prompted to accept the Elastic License.



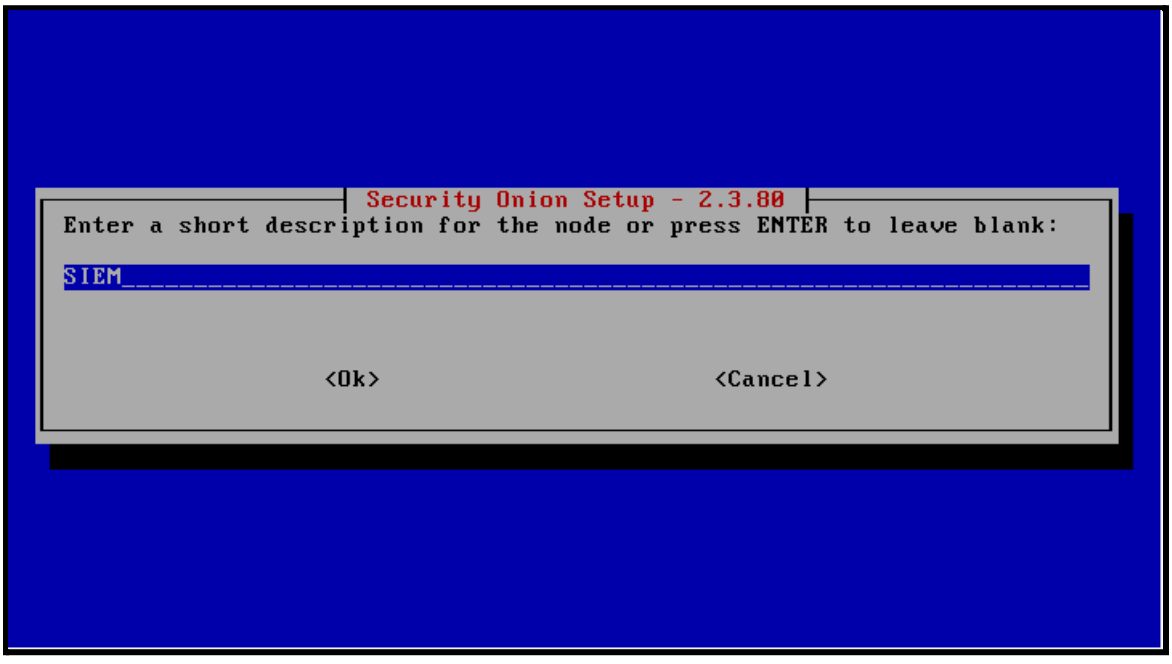
Step 11. Select “Airgap” when prompted to specify how the manager should be installed.



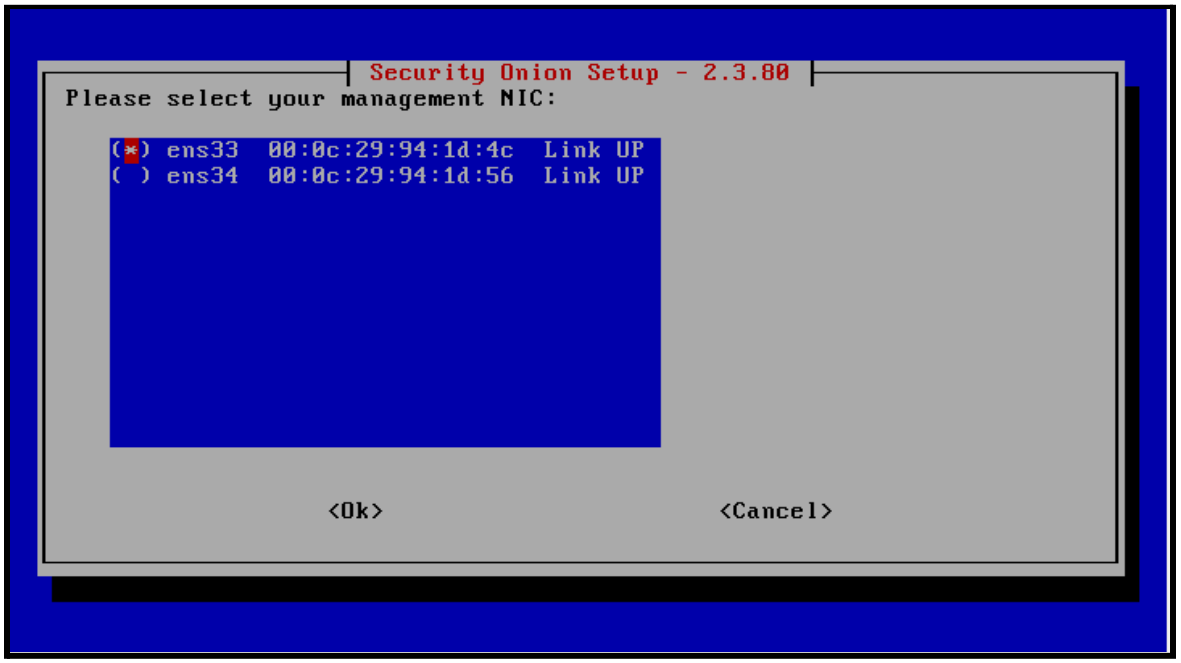
Step 12. Specify your desired hostname (DO NOT use uppercase letters) and press “Enter” when prompted.



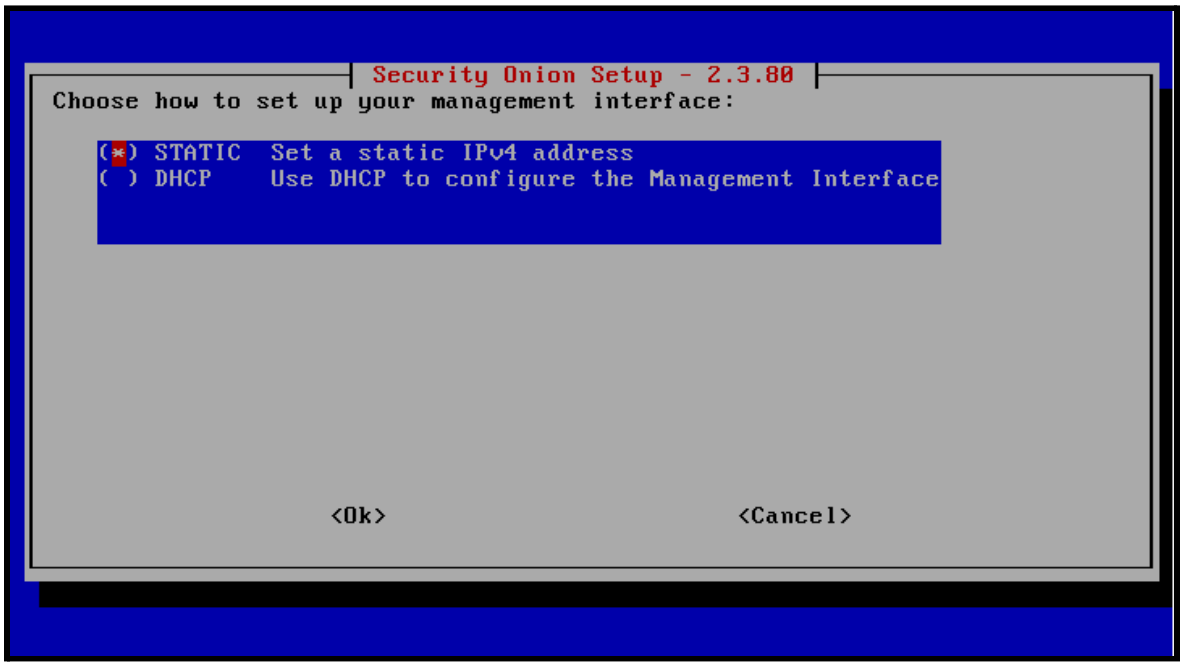
Step 13. Type “SIEM” and press “Enter” when prompted to specify a short description for the node.



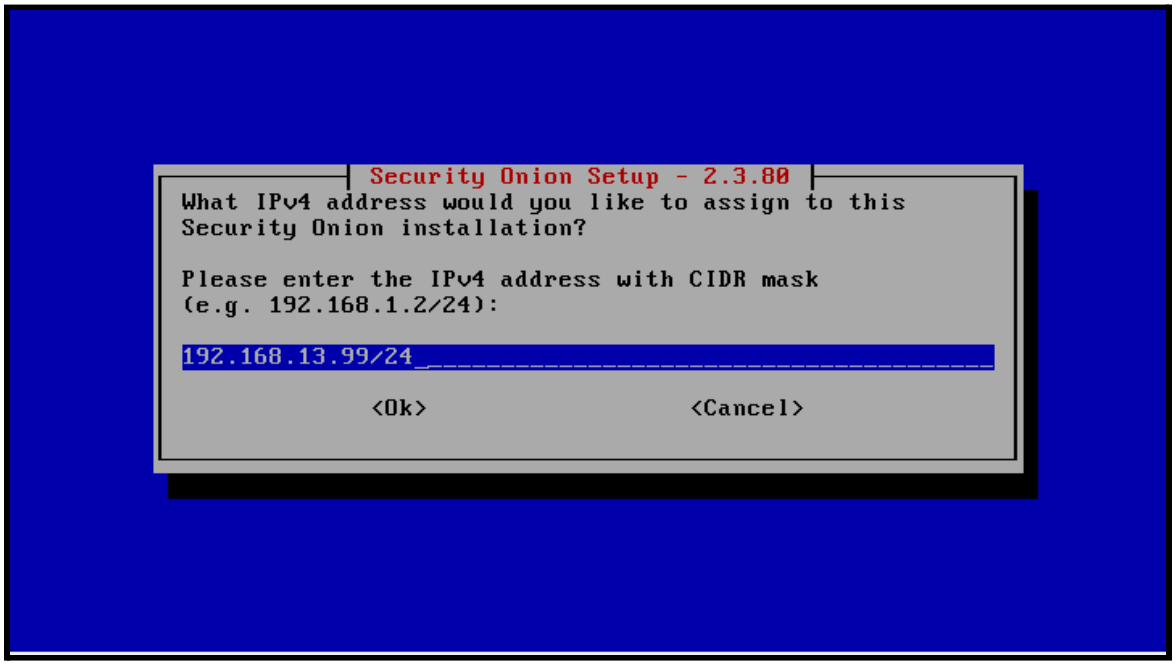
Step 14. Select your management NIC and press “Enter” when prompted.



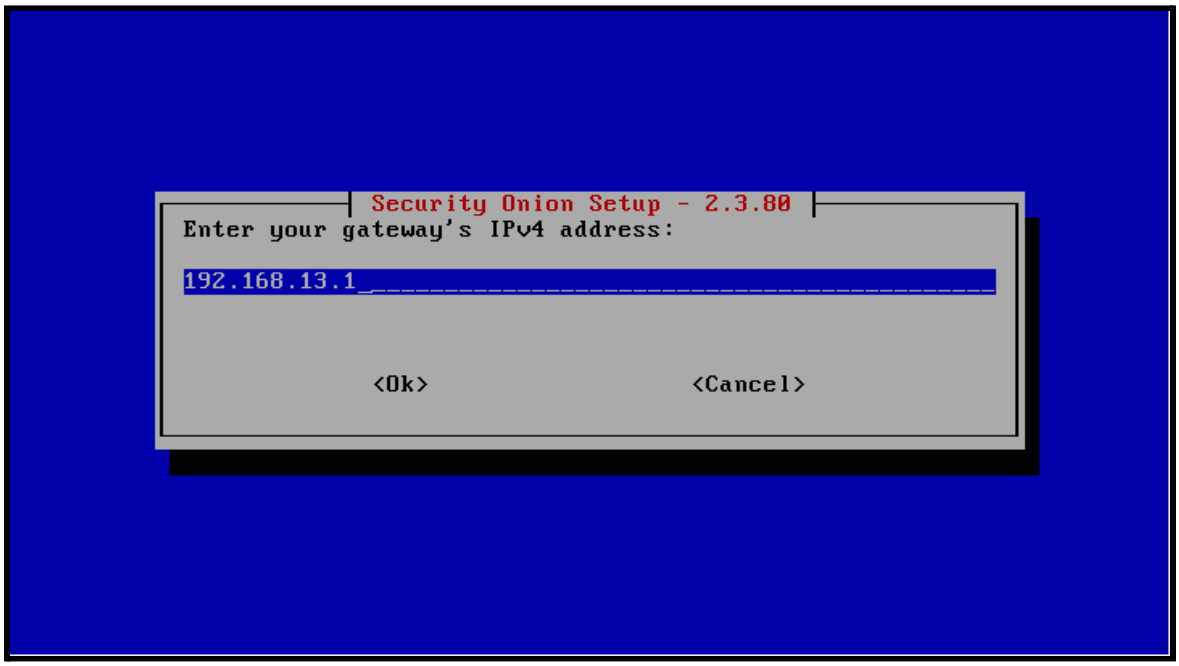
Step 15. Select “STATIC” and press “Enter” when prompted to start configuring a static IP address.



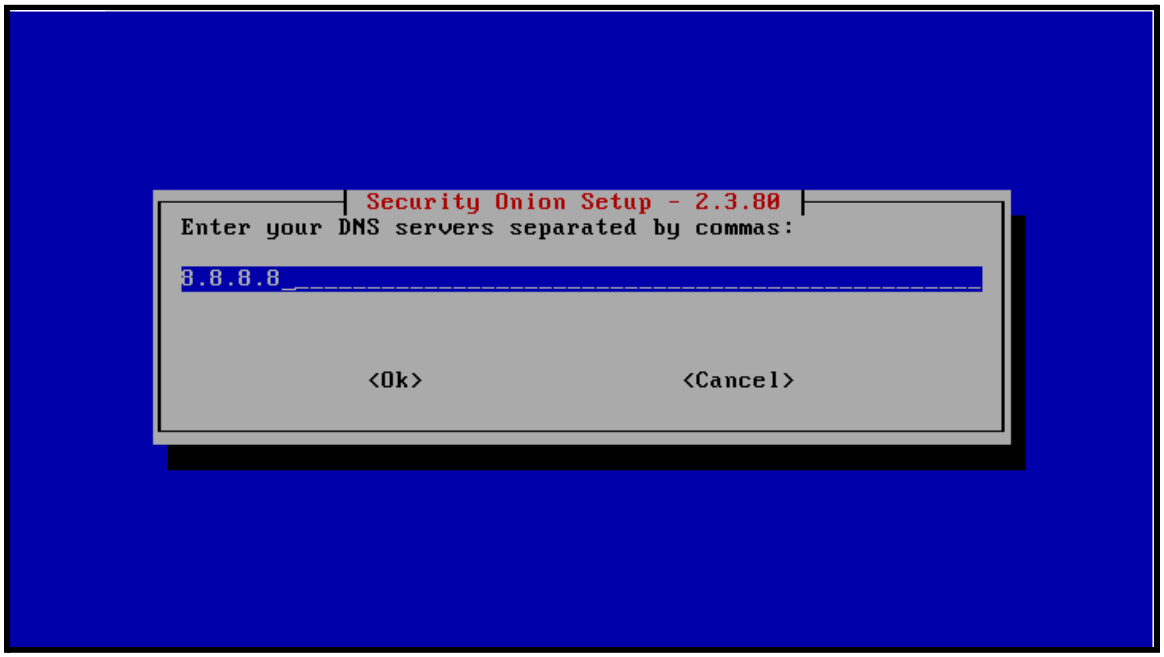
Step 16. Specify your desired IP address followed by its correct CIDR mask and press “Enter” when prompted.



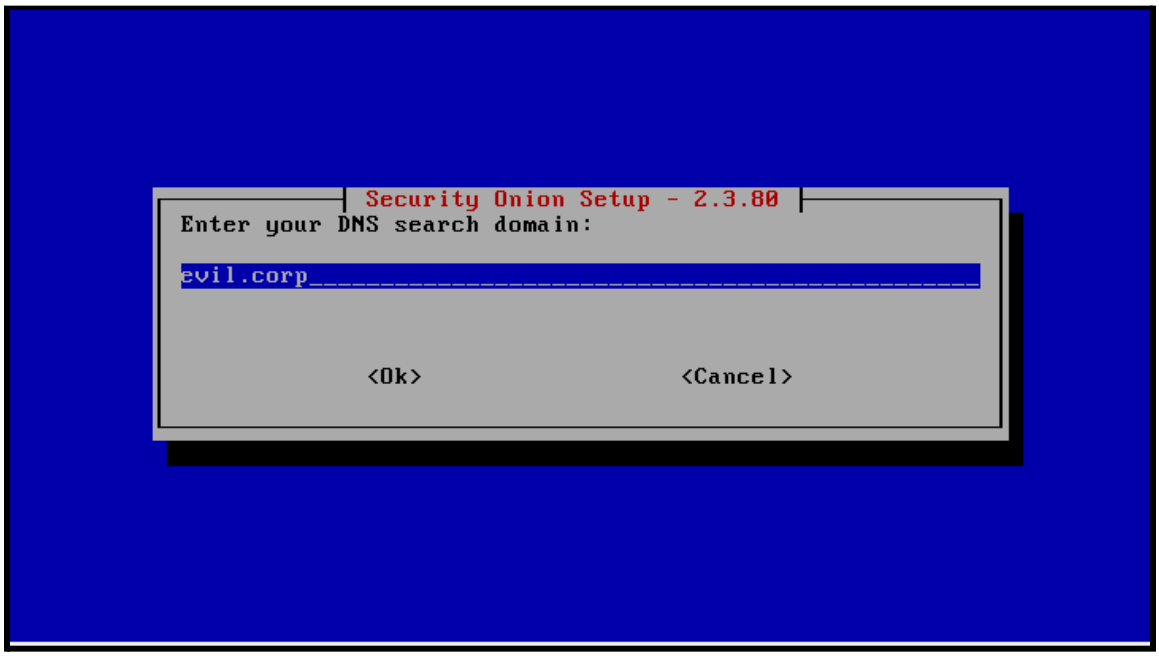
Step 17. Specify your desired gateway IP address and press “Enter” when prompted.



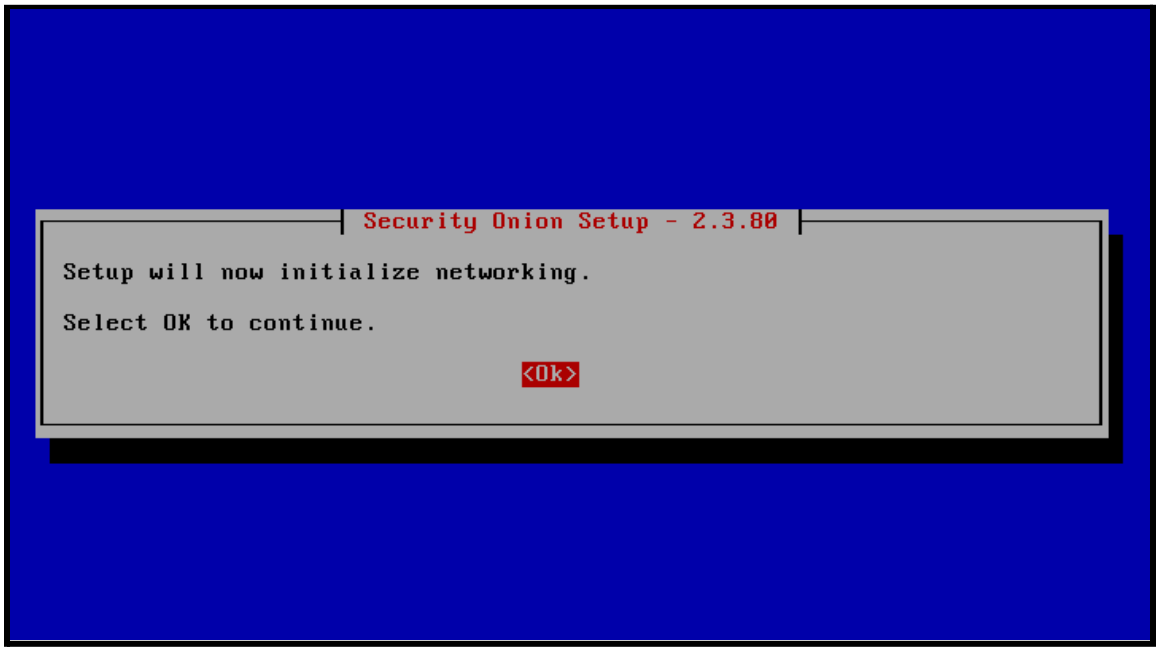
Step 18. Specify your desired DNS server(s) and press “Enter” when prompted.



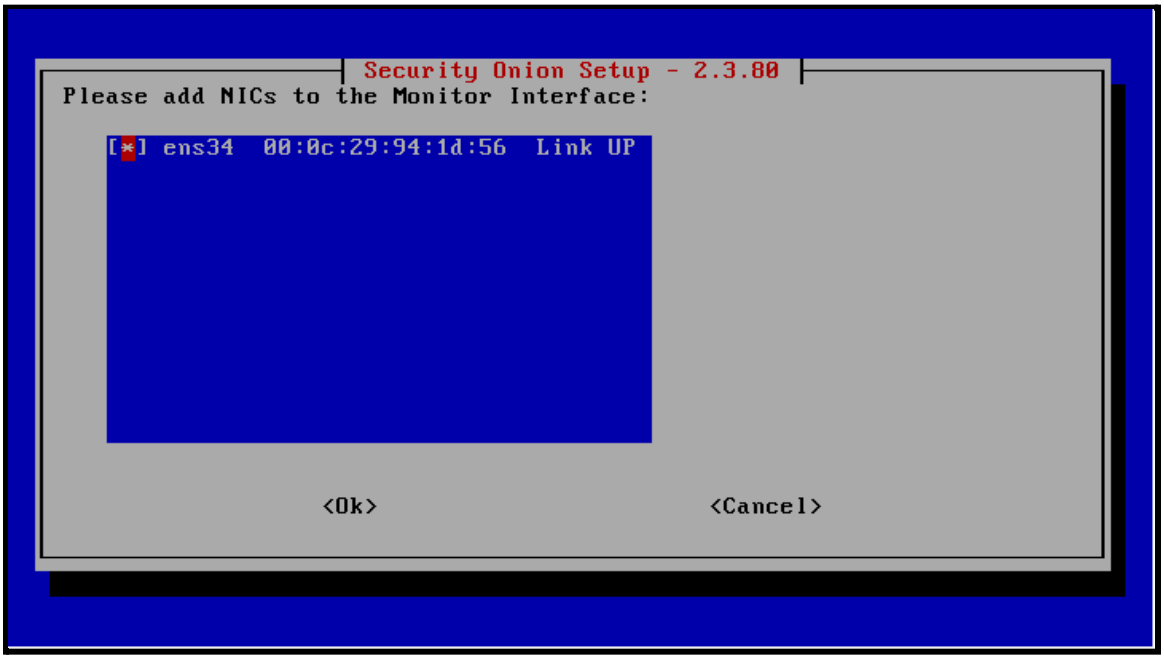
Step 19. Specify your desired domain and press “Enter” when prompted.



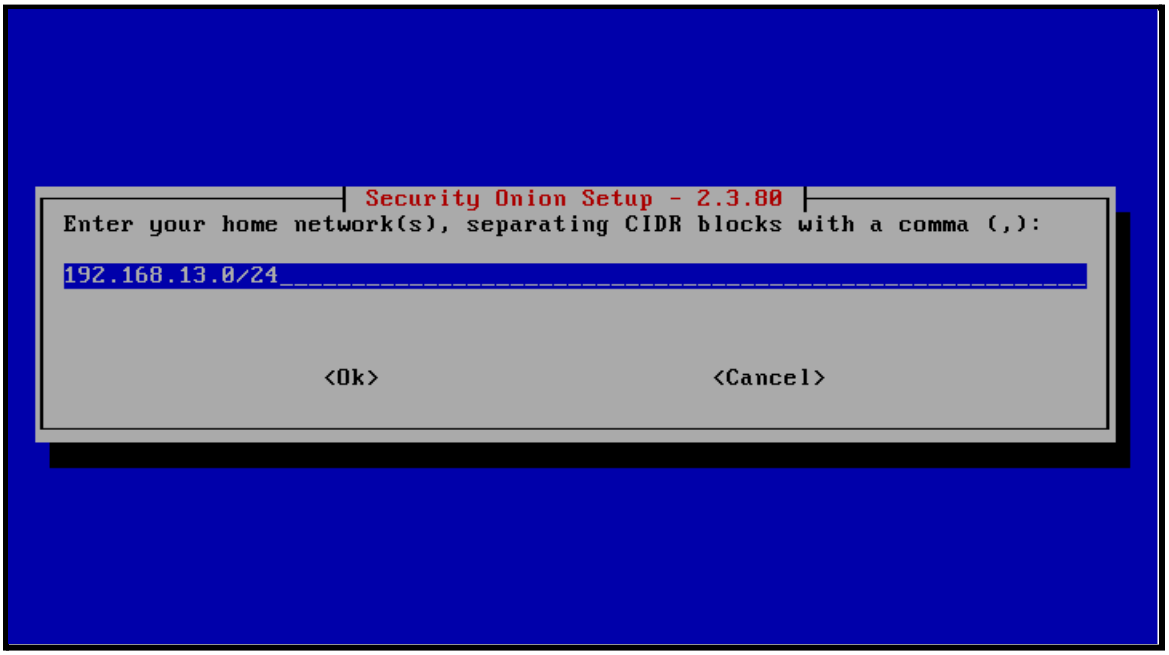
Step 20. Press “Enter” when prompted to initialize networking.



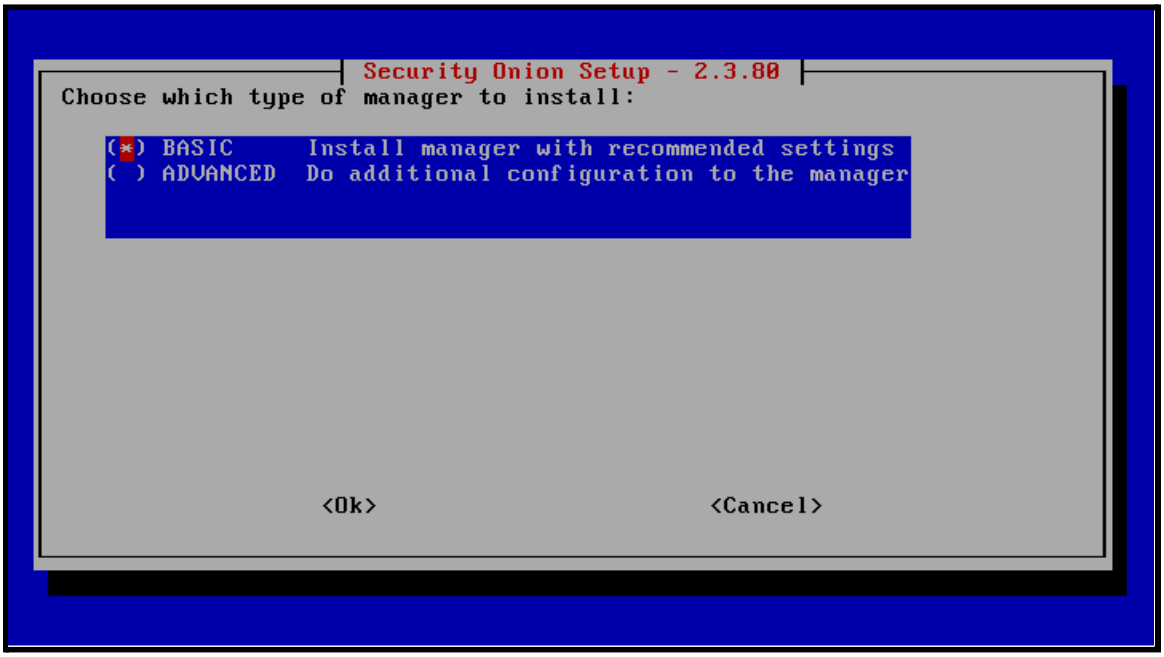
Step 21. Select your monitor (sniffing) NIC and press “Enter” when prompted.



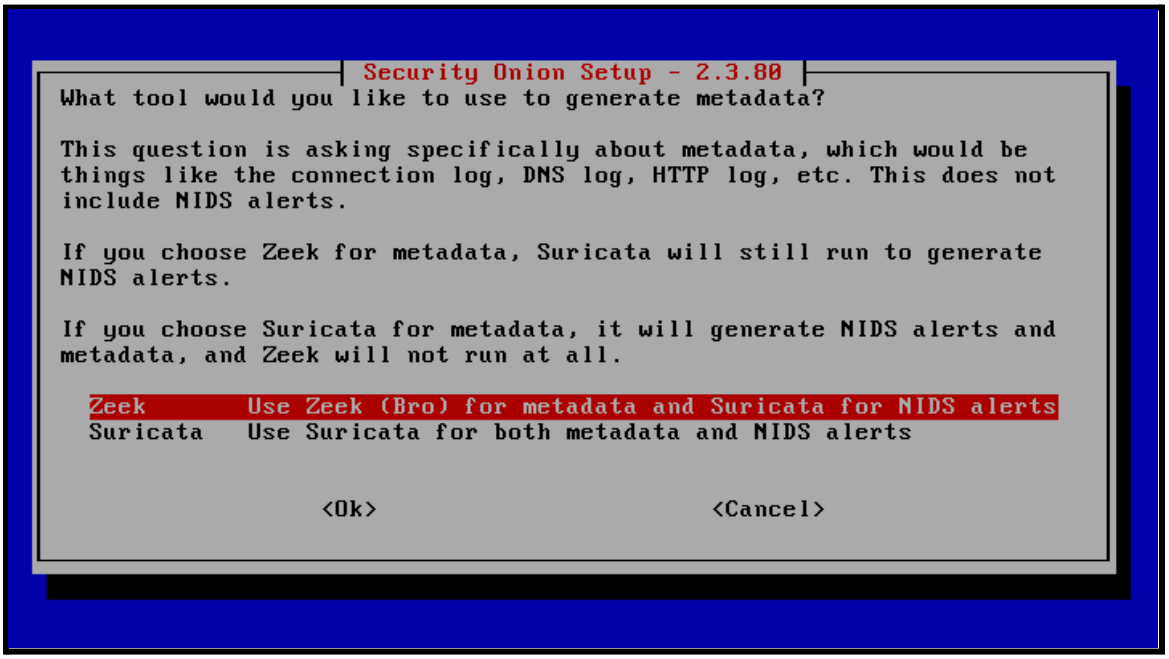
Step 22. Specify your desired home network followed by its correct CIDR mask and press “Enter” when prompted.



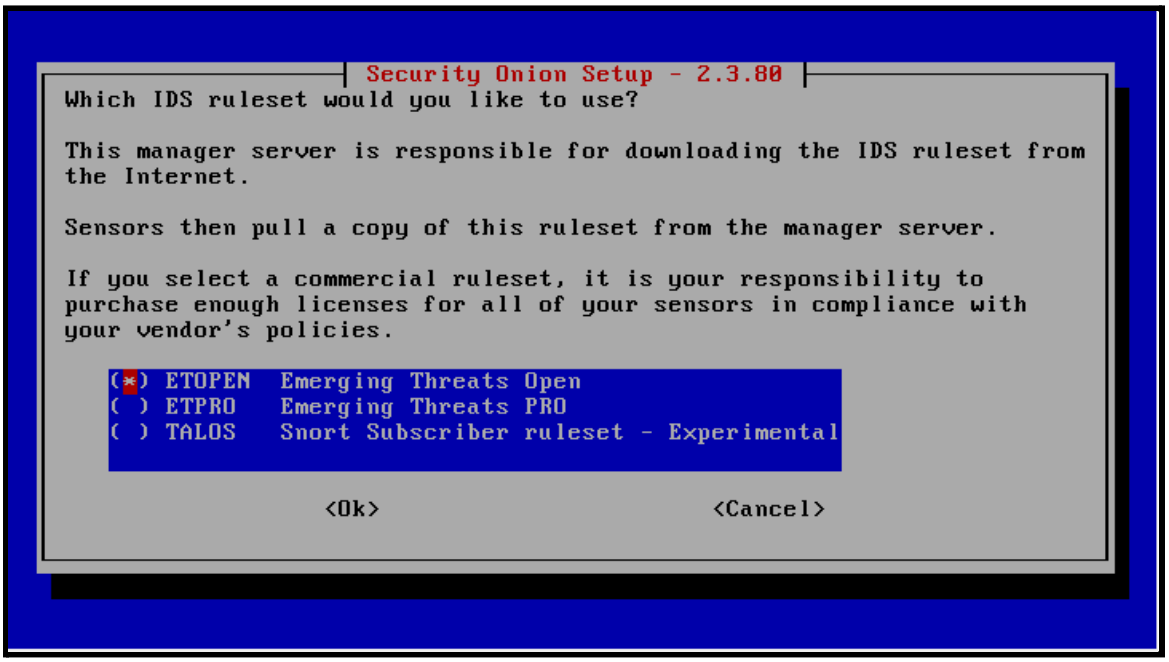
Step 23. Select “BASIC” when prompted to specify the type of manager to install.



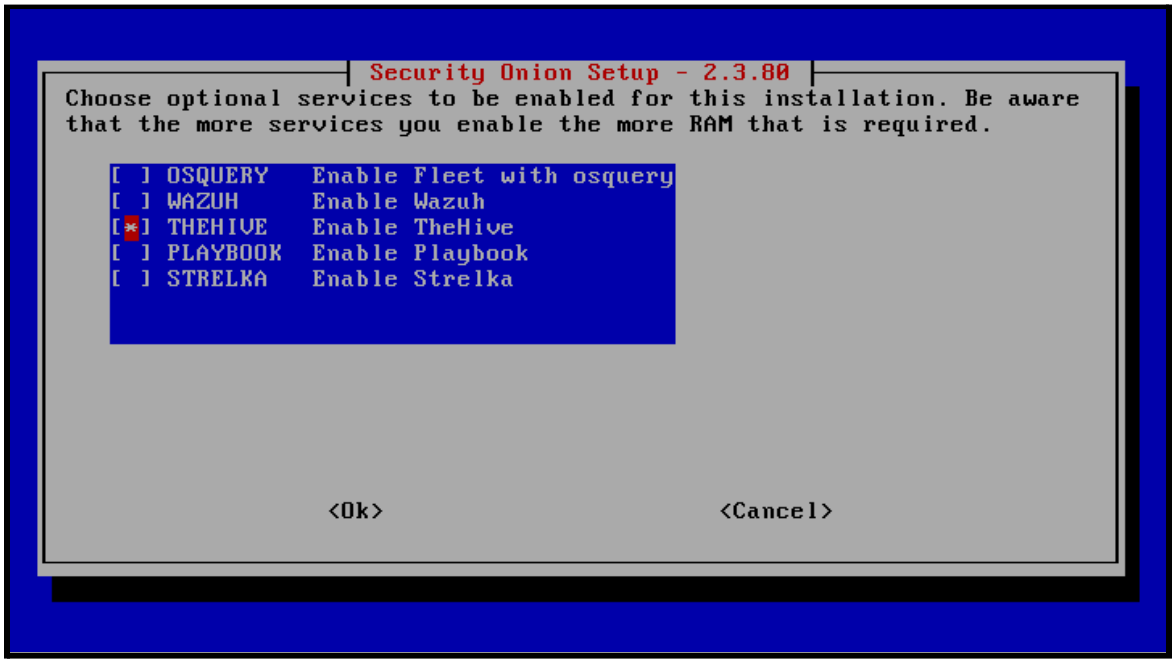
Step 24. Select “Zeek” when prompted to specify the tool you would like to generate network traffic metadata.



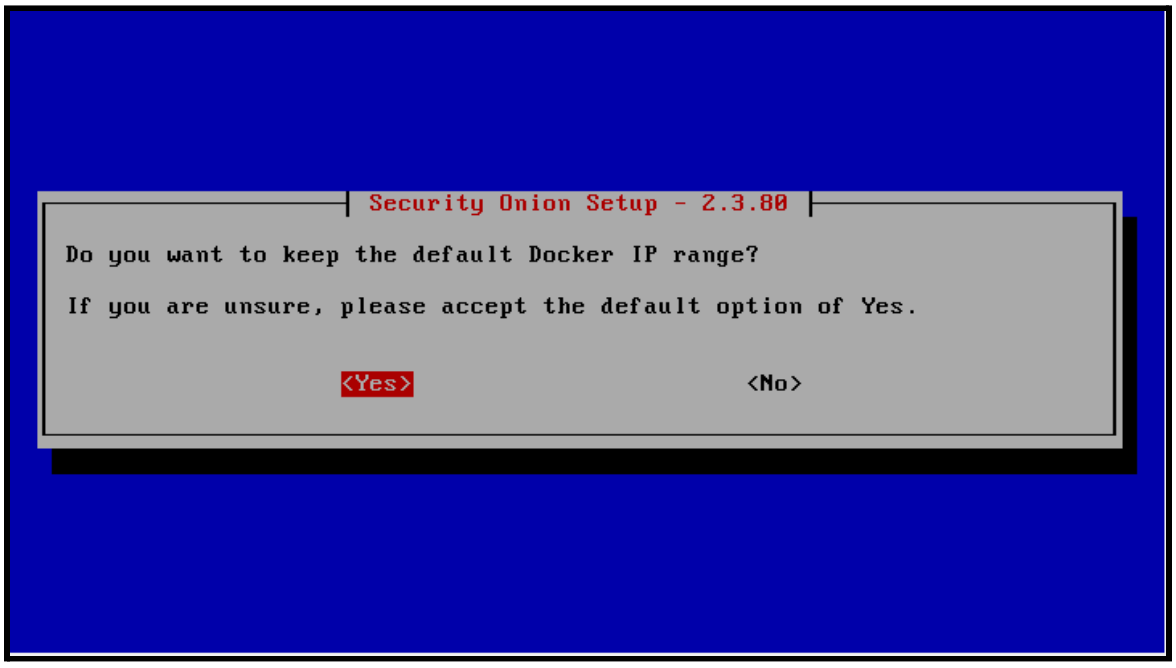
Step 25. Select “ETOPEN” when prompted to specify the IDS ruleset you would like to use.



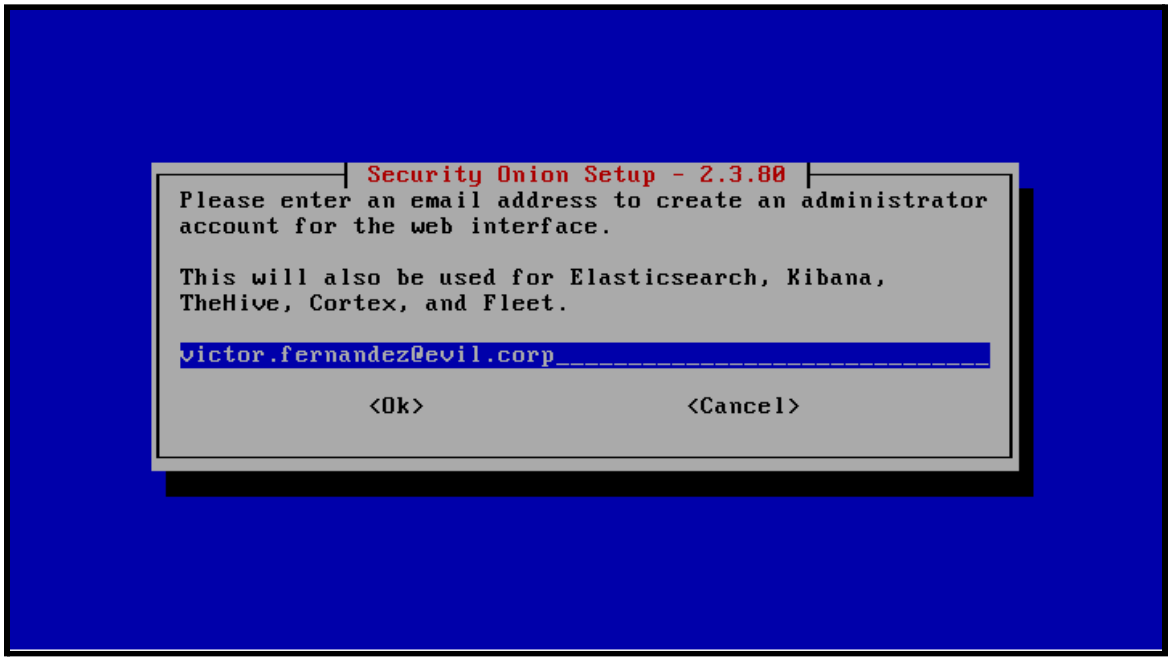
Step 26. Select “THEHIVE” when prompted to specify the optional service you want enabled. TheHive is an Incident Management System (IMS).



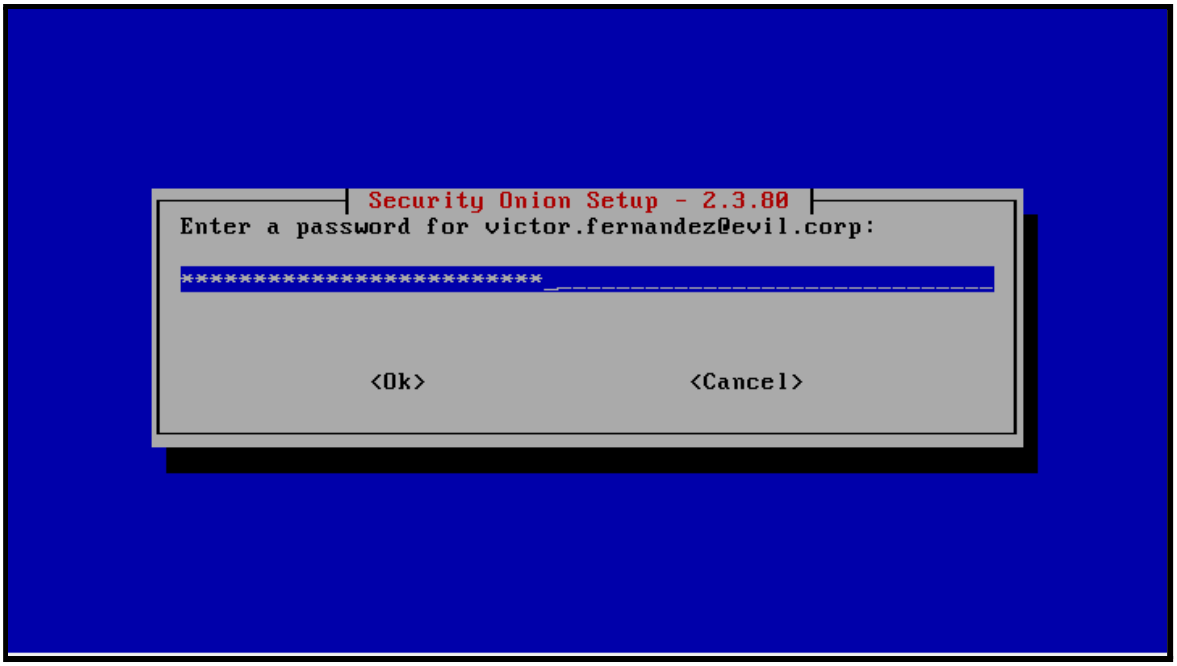
Step 27. Select “Yes” when prompted to keep the default Docker IP range.



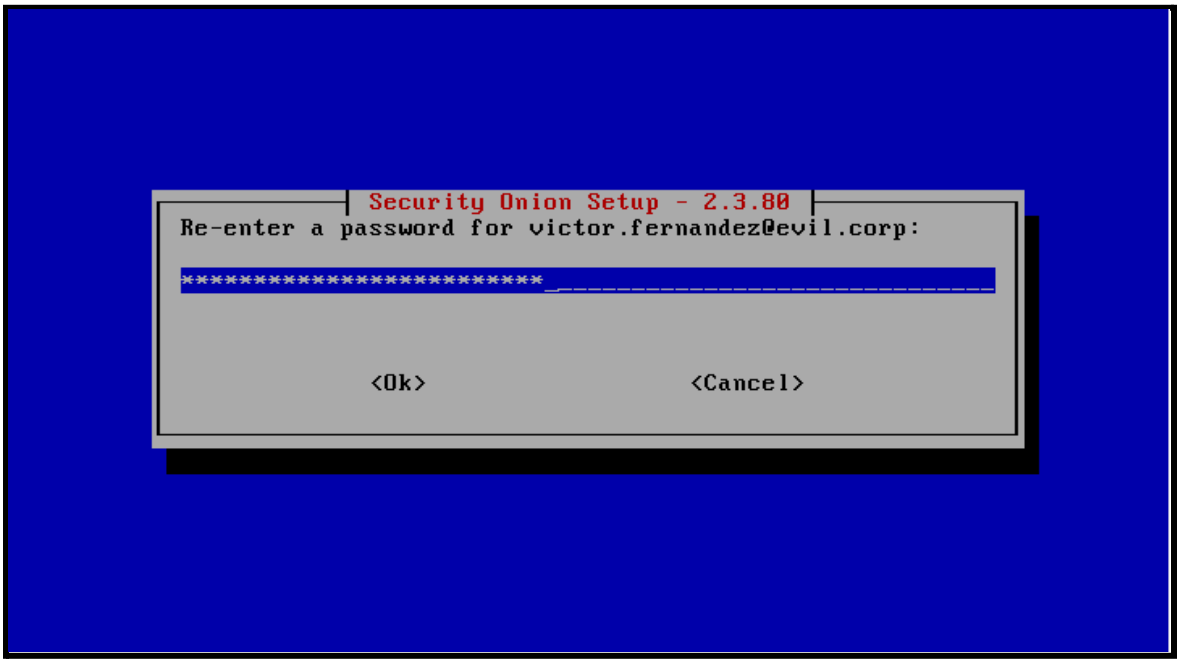
Step 28. Specify the email address of the first security analyst account and press “Enter” when prompted. This email address does not need to be accessible or real. It only serves as the “username” to the web apps hosted on SO.



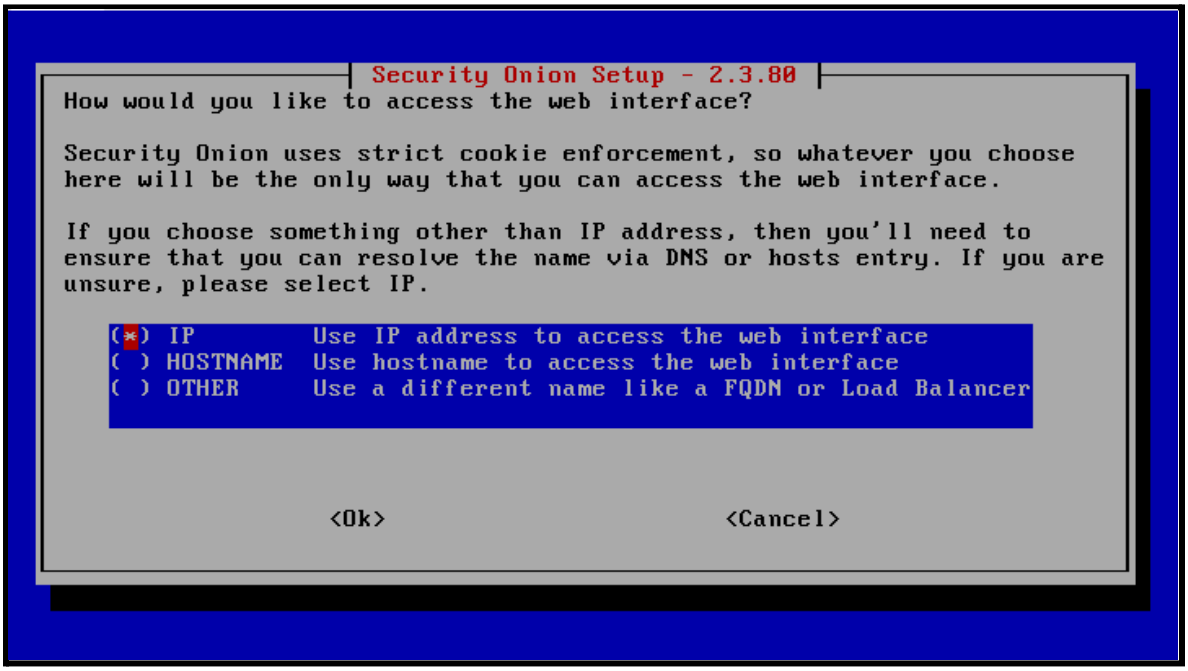
Step 29. Specify the password of the first security analyst account and press “Enter” when prompted.



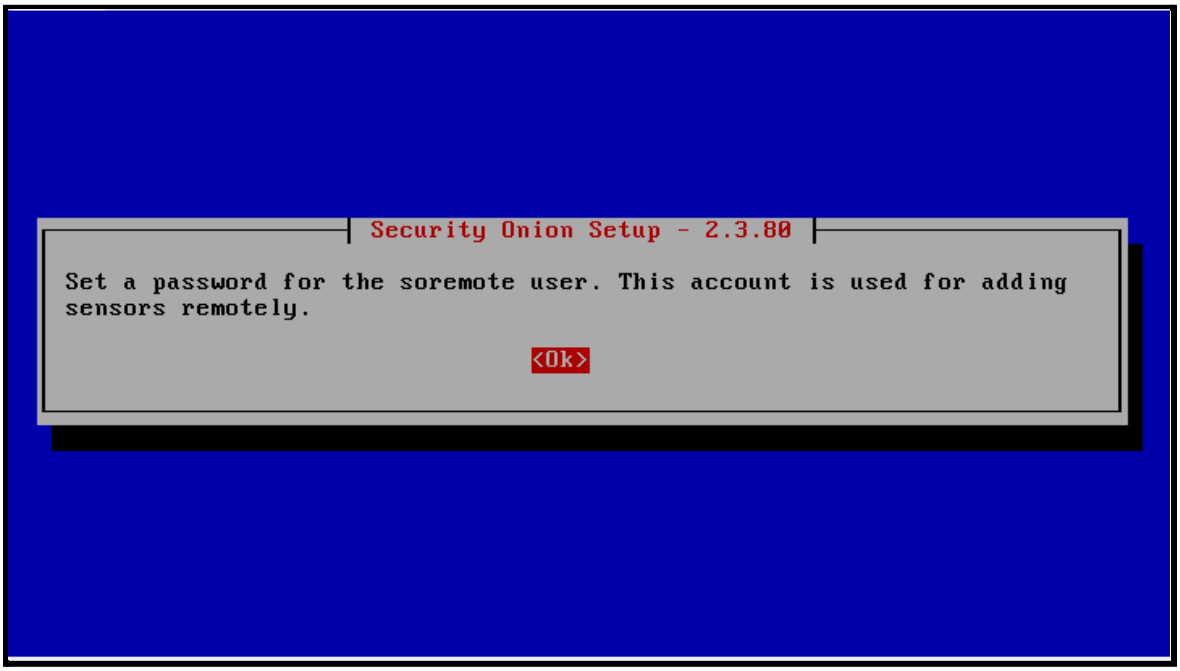
Step 30. Re-enter the password of the first security analyst and press “Enter” when prompted.



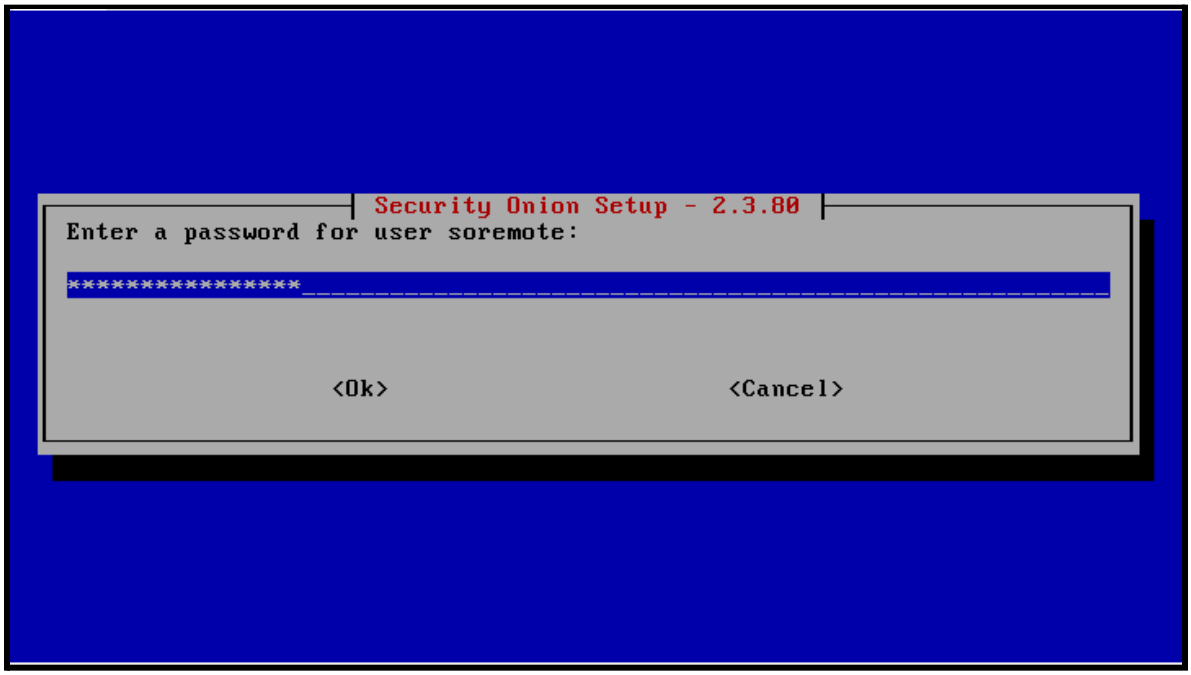
Step 31. Select “IP” when prompted to specify how you would like to access the SO web interface.



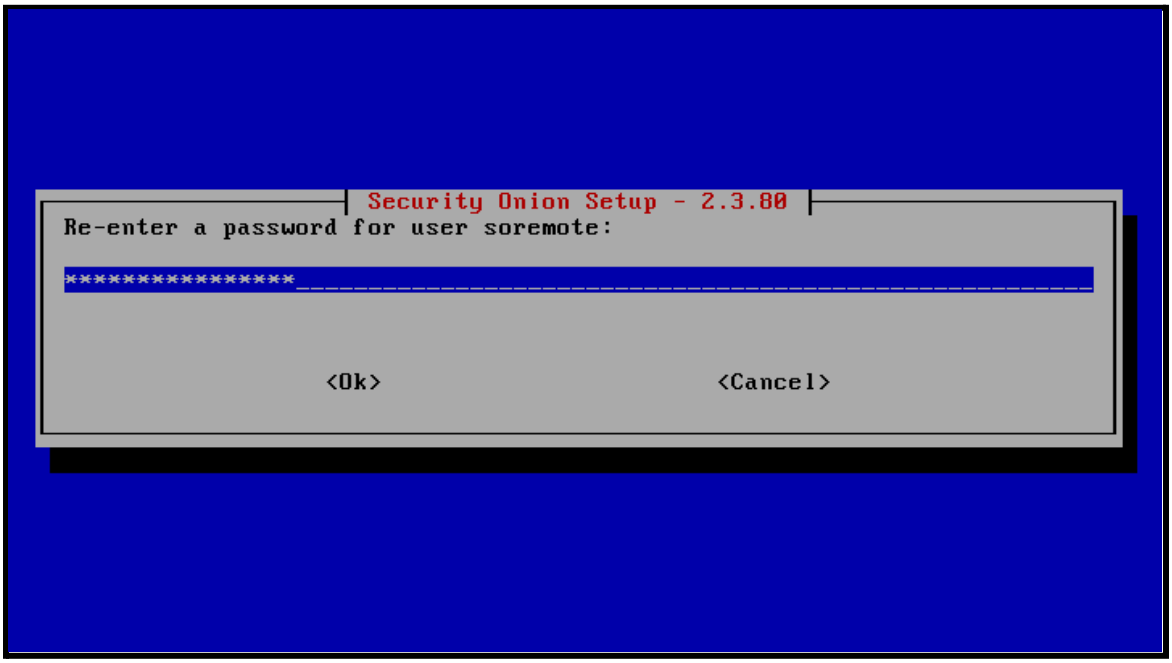
Step 32. Press “Enter” when prompted to specify the password of the “soremote” user.



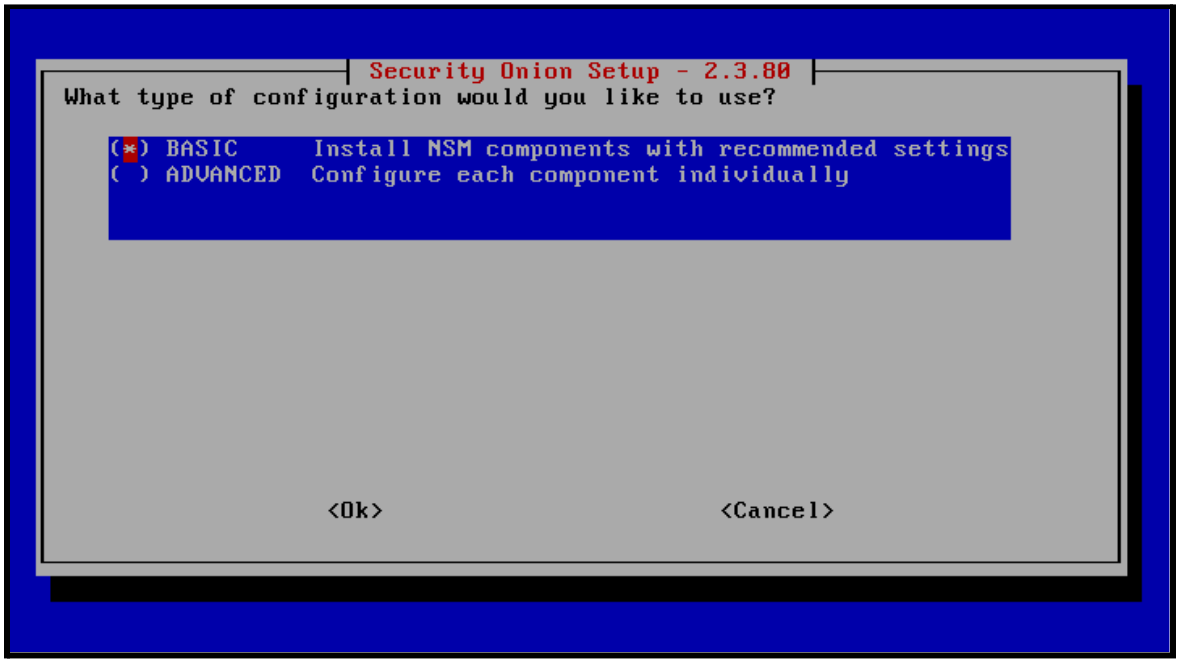
Step 33. Specify the password of the “soremote” user and press “Enter” when prompted.



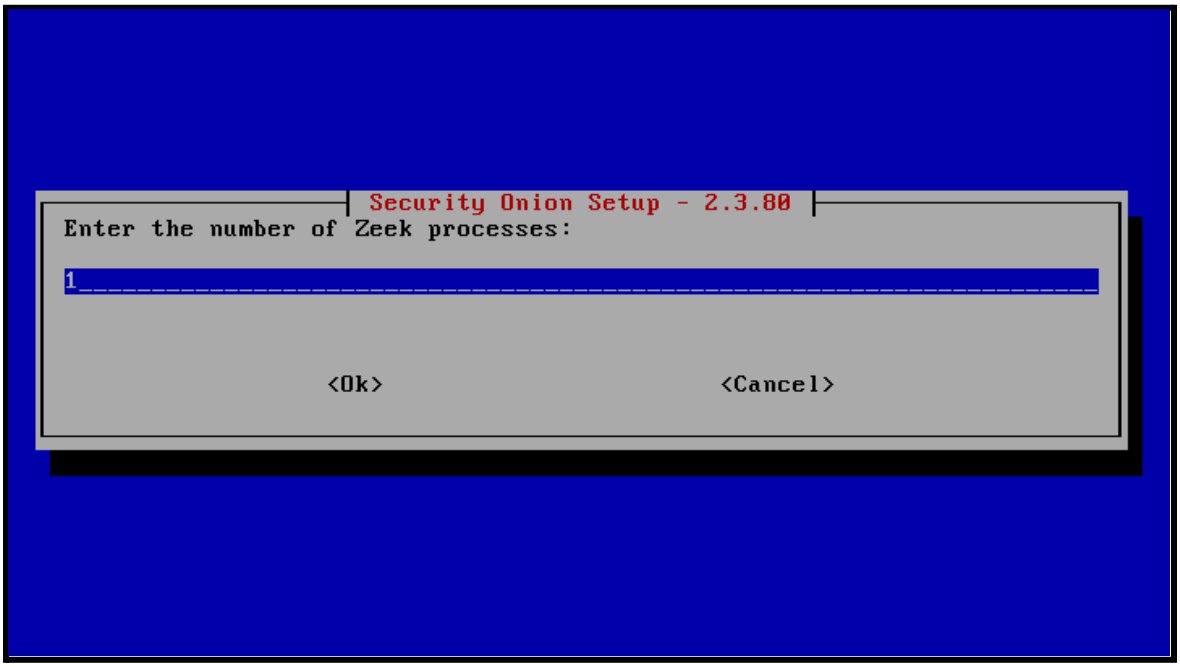
Step 34. Re-enter the password of the “soremote” and press “Enter” when prompted.



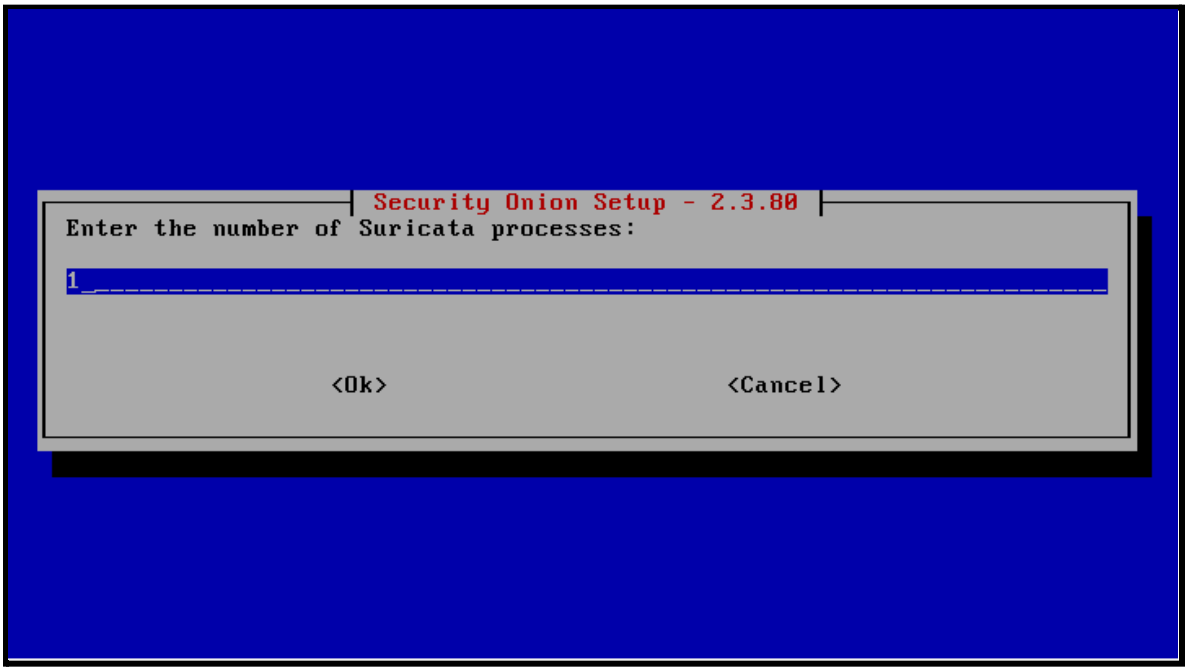
Step 35. Select “BASIC” and press “Enter” when prompted to specify the type of NSM configuration to use.



Step 36. Press “Enter” to accept the default number of Zeek processes to run.

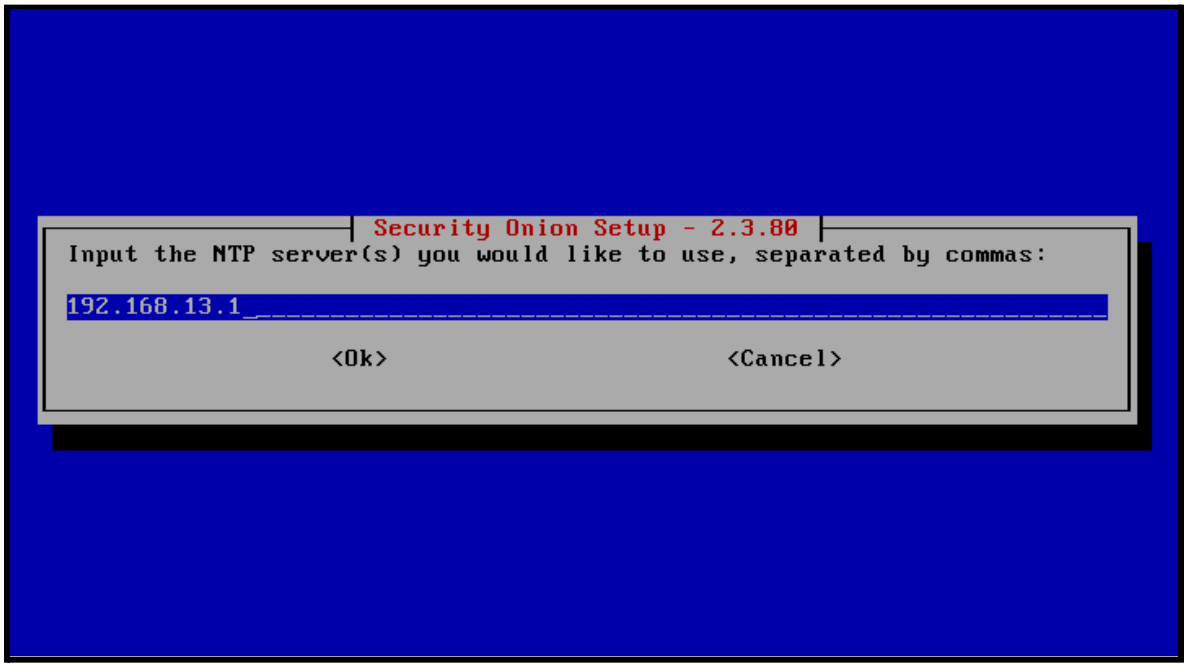


Step 37. Press “Enter” to accept the default number of Suricata processes to run.

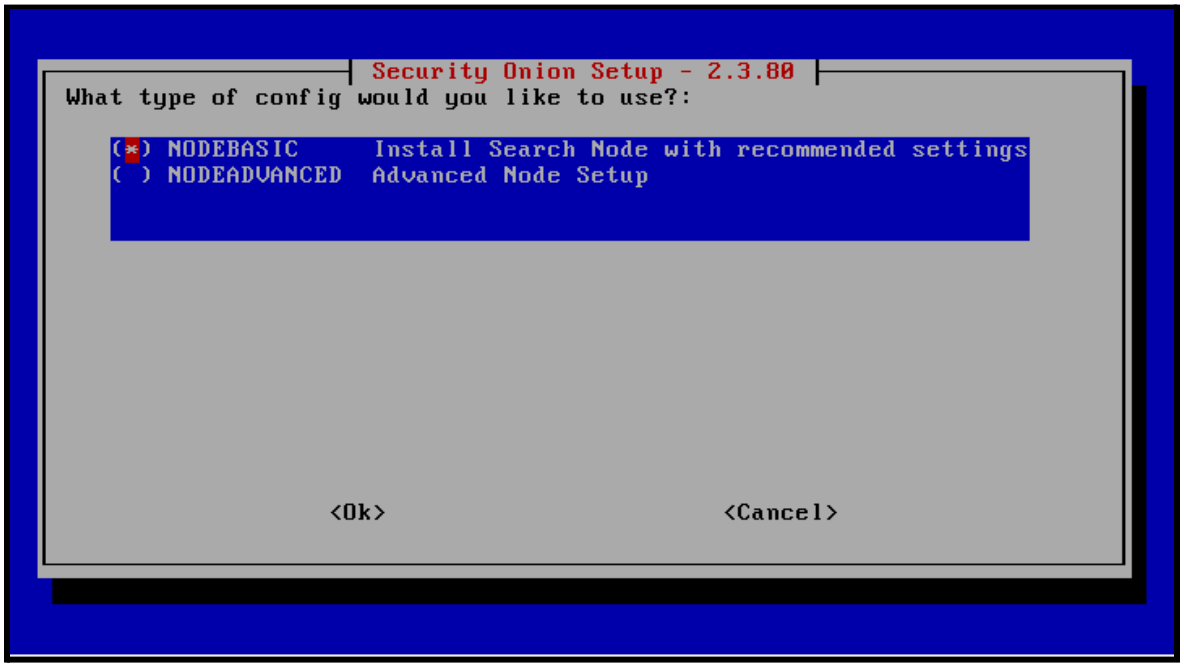


Step 38. Select “Yes” and press “Enter” when prompted to specify NTP servers.

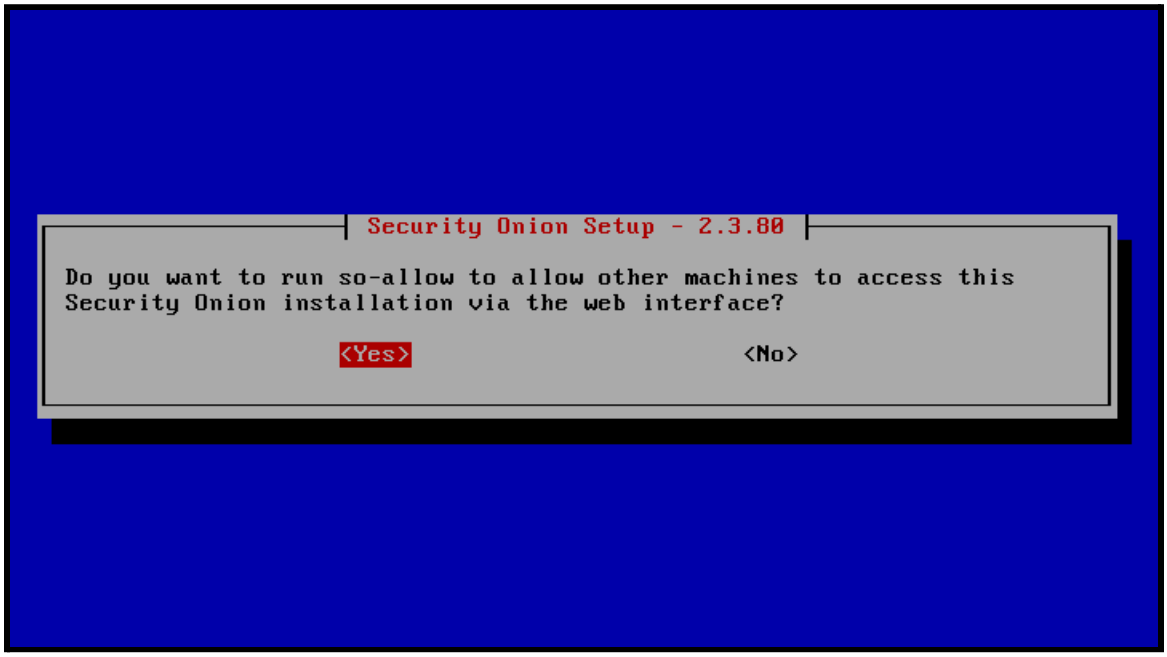
Step 39. Specify your desired NTP servers and press “Enter” when prompted.



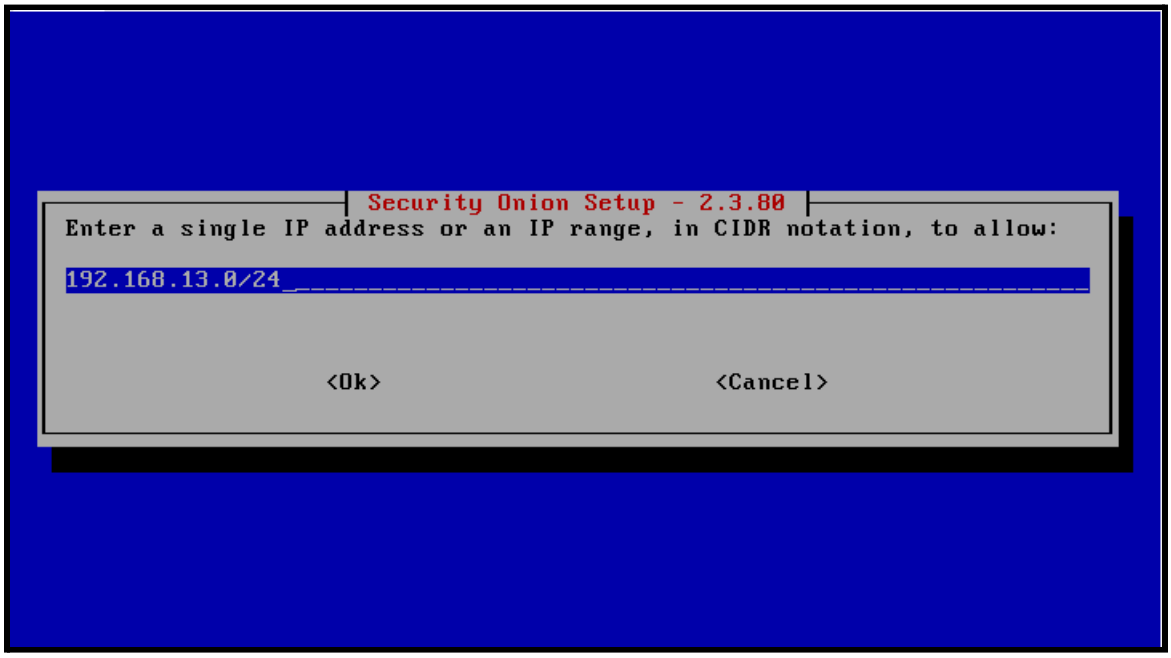
Step 40. Select “NODEBASIC” and press “Enter” when prompted to specify the type of Search Node configuration.



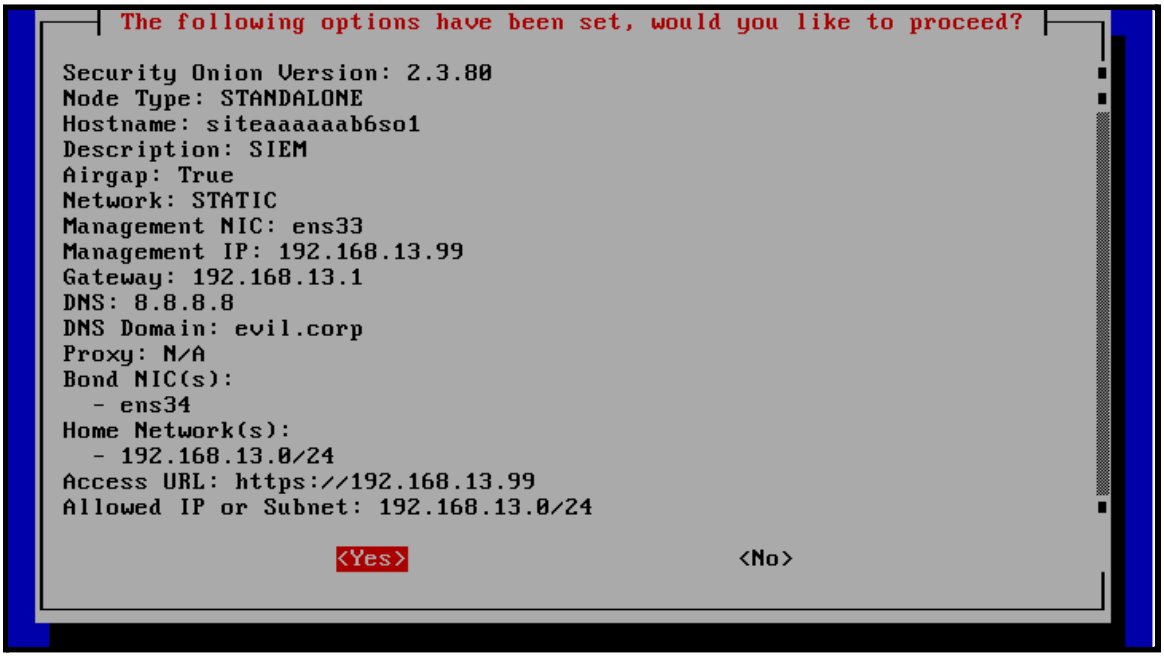
Step 41. Select “Yes” and press “Enter” when prompted to run the “so-allow” script. This script modifies SO’s local firewall so security analysts can access its on-board web apps.



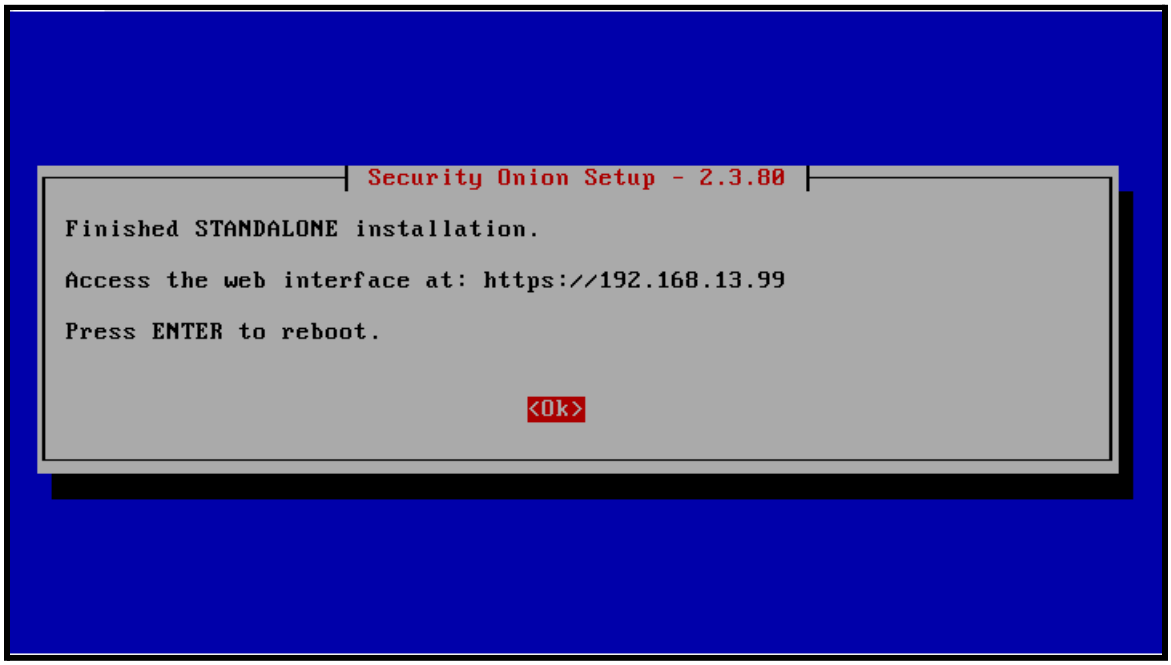
Step 42. Specify the IP address range, followed by the correct CIDR mask, of where your security analysts will connect to SO.



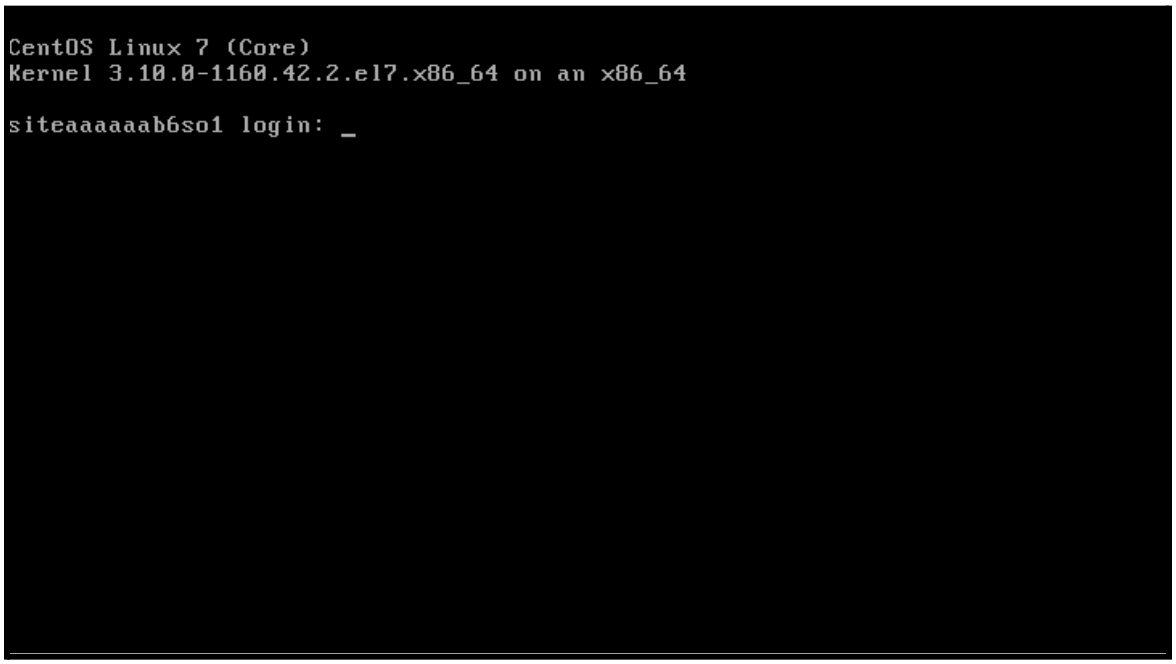
Step 43. Press “Tab,” select “Yes,” and press “Enter” to proceed with configuring SO.



Step 44. Press “Enter” when prompted to reboot the computer and finish the SO installation.



After the computer reboots, you should see a screen similar to below.



Step 45. Using a computer within the IP range you specified during Step 42, open a web browser and navigate to the interface mentioned during Step 44. Login using the credentials you declared between Steps 28 through 30.