GuardDog Fido Installation & Configuration Requirements

Hardware Requirements:

1. **ISP Router or Equivalent**: While Fido monitors traffic from the network switch, it requires an active internet connection (usually provided by an ISP router or equivalent device) for communication with external services, registration, and other functionalities.
2. **Active Internet Connection**: Ensure a reliable internet connection is available. This is crucial for Fido to register and maintain a continuous data flow with the Protective Cloud Service.
3. **Network Switch**: This is essential for Fido to monitor local traffic. Ensure the switch supports port mirroring if you plan to use Fido in a passive monitoring setup.
4. **Fido Unit**: Ensure that the Fido device is physically intact, comes with its serial number and PIN (usually located on the box or the device), and is accompanied by the necessary peripherals such as antennas and power cables. **(install guide provided in box)**

Network Configuration:

1. **Switch Port Configuration**: can be deployed on a Layer 2 or Layer 3 switch port and configure accordingly.
2. **Port Mirroring**: If Guarddog's FIDO is to monitor network traffic passively, consider setting up a mirrored port (SPAN) on your switch.
3. **Physical Installation**: Ensure the Fido device, if there's dedicated hardware, is properly installed in the data center or server room, with necessary power and cooling considerations.
4. **Connectivity**: Ensure necessary network cables are available and connect Guarddog's FIDO to the network.
5. **Firewall Configuration**: Ensure that the specific ports and IP addresses listed in the installation checklist are allowed through any firewalls or security groups in the network environment to ensure that Fido can communicate effectively with the required external services. (see appendix a.)
6. **Network Environment**: Fido is designed to work on a DHCP-enabled network, ensuring that your network supports DHCP before initiating the installation process.

Additional Configuration and Setup:

1. **Account Registration**: An active account is necessary for Fido's management dashboard. If you have not already, visit the provided URL to register and validate your account.
2. **Fido Registration**: With an active account, proceed to register your Fido unit using its unique serial number and PIN.
3. **Dashboard Familiarization**: Once registered, take some time to familiarize yourself with the dashboard – understanding key indicators, vulnerability reports, network activity, and more.
4. **Troubleshooting**: Keep a list of common troubleshooting steps and solutions handy in case any issues arise during or after the installation process.

Conclusion:

Thank you for choosing GuardDog's Fido to bolster your network's security. Should you encounter any challenges or have additional questions, refer to the full manual or contact the support team for assistance.

Appendix A.

Table: Firewall Configuration for Fido

Destination IP	Protocol	Site	TCP/UDP
142.250.141.82	https	Google	TCP
142.250.72.10	https	“ “	TCP
172.217.11.202	https	“ “	TCP
172.217.11.208	https	“ “	TCP
172.217.15.240	https	“ “	TCP
172.217.164.16	https	“ “	TCP
172.217.15.234	https	“ “	TCP
172.217.164.10	https	“ “	TCP
172.217.7.106	https	“ “	TCP
172.217.7.110	https	“ “	TCP
172.217.15.238	https	“ “	TCP
https	https	“ “	TCP
173.194.194.206	Secure-mqtt	MQTT Gateways	TCP
173.194.195.206	Secure-mqtt	“ “	TCP
74.125.201.206	Secure-mqtt	“ “	TCP
188.177.68.34	Secure-mqtt	“ “	TCP
34.68.177.188	Secure-mqtt	“ “	TCP
140.82.112.3	https	GitHub	TCP
140.82.112.6	https	“ “	TCP
140.82.114.5	https	“ “	TCP
185.199.108.133	https	“ “	TCP
185.104.208.93	https	Vulners	TCP
49.12.234.183	https	Ident.me	TCP
52.38.107.102		Remote.it	UDP
91.189.91.157	ntp	NTP Ubuntu	UDP
8.8.8.8	https	DNS Google	TCP