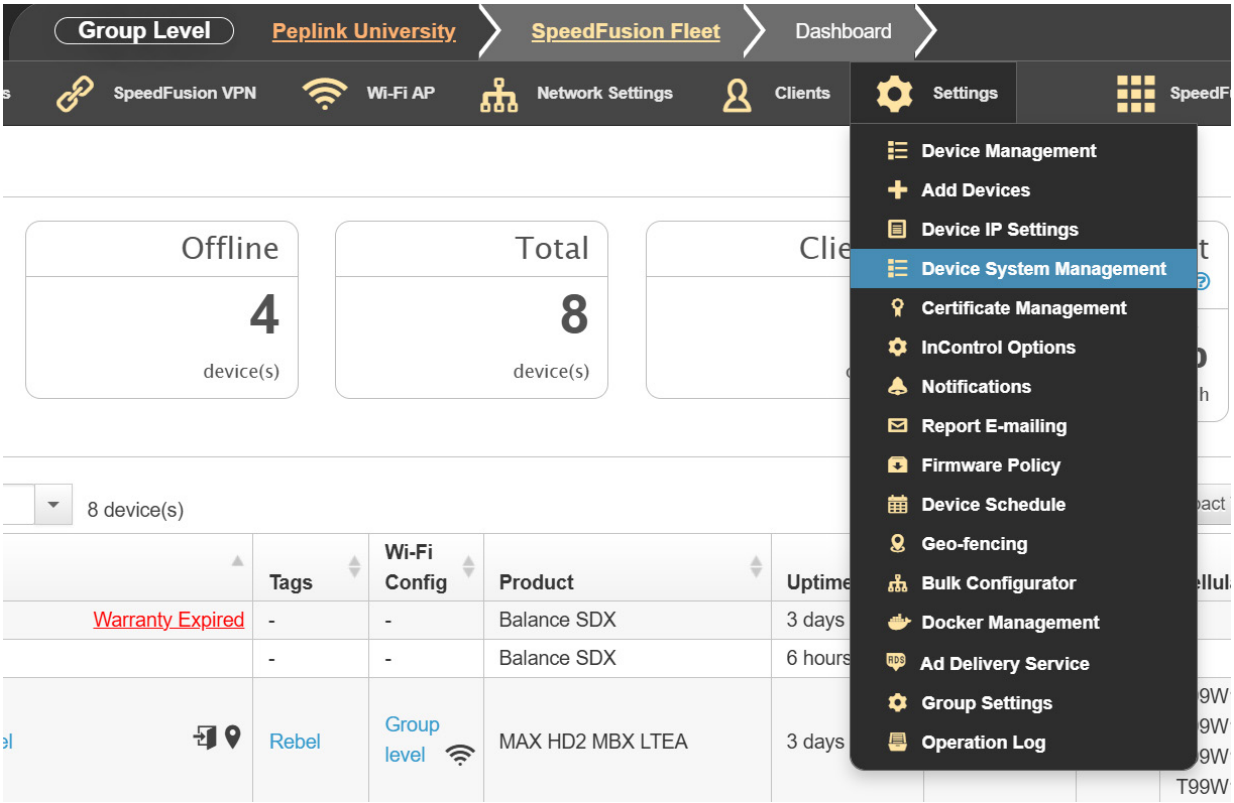
Peplink Router
PCI DSS 4
Hardening Guide

For best security and results, we recommend using InControl2. This article will be demonstrated using the InControl2 appliance, however most features outlined here can be accomplished via the local web admin. We will annotate if something requires InControl2 access exclusively.

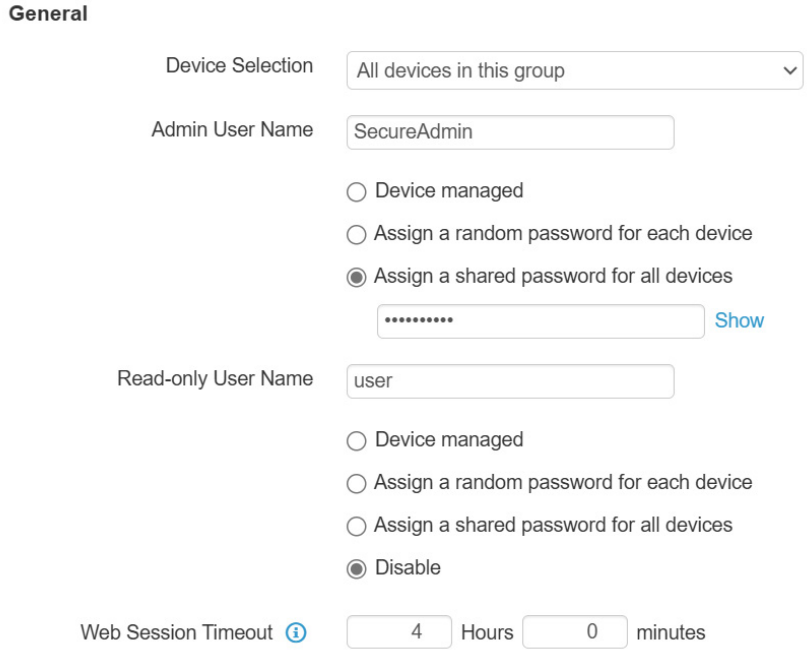
Change Default Username and Password

InControl2:

1: On the InControl 2 Group Level Dashboard, go to: Settings > Device System Management



2: Set your admin username, and set the desired password. Hit 'Save Changes' at the bottom to confirm username/password change.



Local Web Admin:

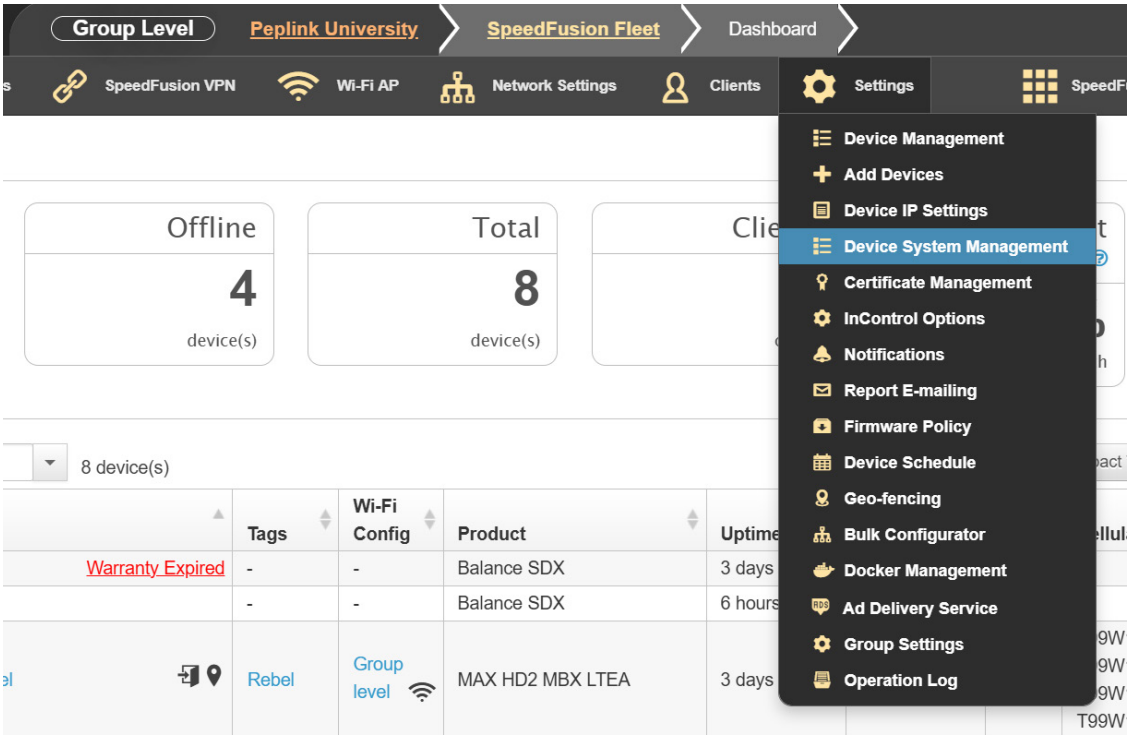
1: **Access the Web Admin Interface**: Log in to your router's web admin interface.

2: **Navigate to System > Admin Security**: Change the default username and password to something strong and unique.

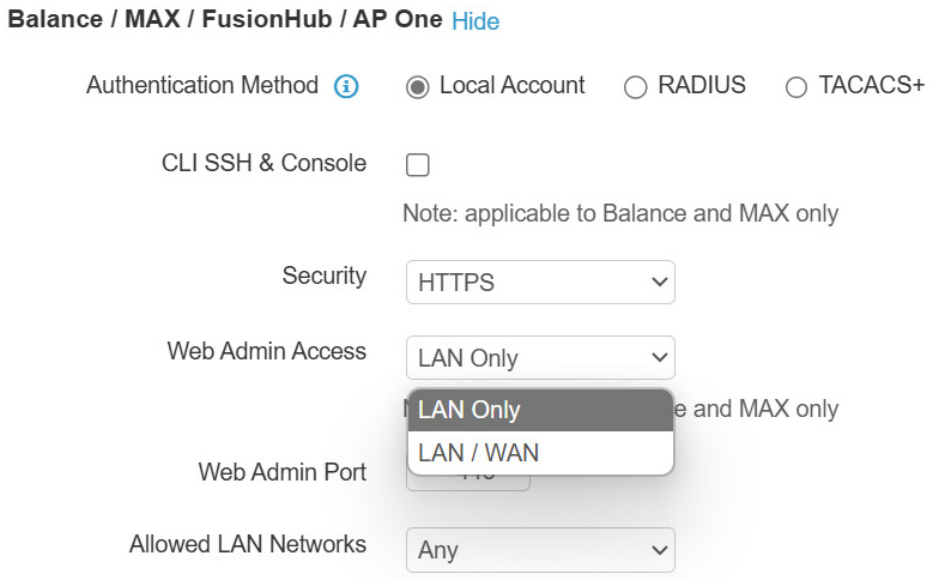
Disabling Management Access on the WAN

InControl2:

1: Navigate to Device System Management from the Group Level.
Settings > Device System Management



2: Select 'LAN Only' from the drop down for 'Web Admin Access'.



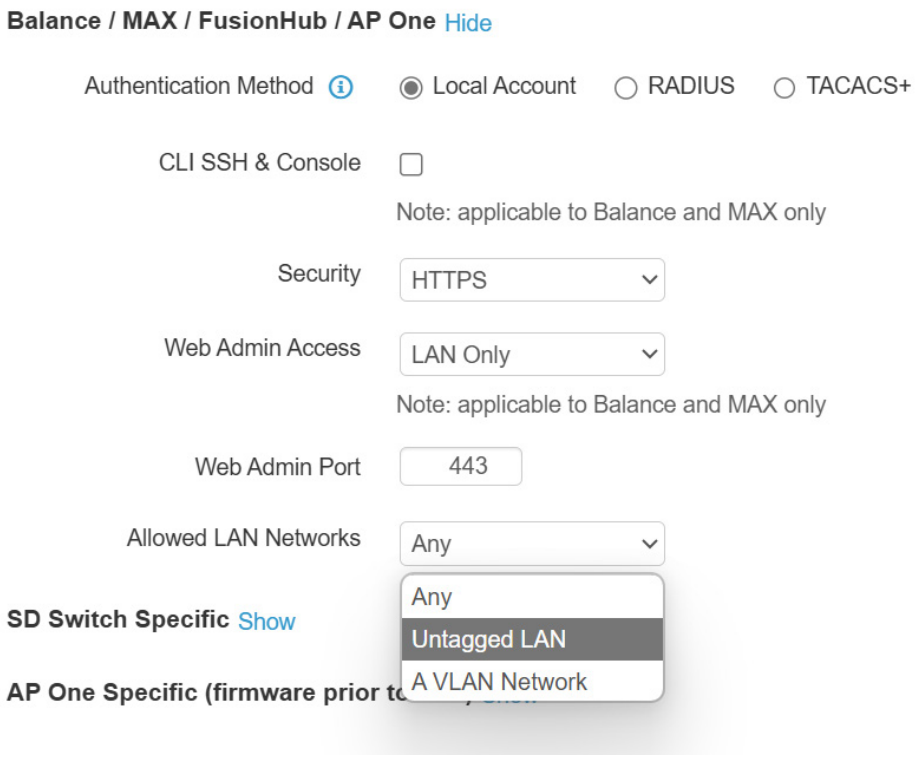
Local Admin:

1: Navigate to System > Admin Security: Ensure that the "Web Admin Access" and "SSH Access" are set to LAN only.

Secure LAN Management Access

InControl2:

1: Continuing from the Device System Management menu, scroll down to 'Allowed LAN Networks'.
2: Select a LAN that is secure and not accessible by Guest or Corporate users. In our example, it's the untagged.

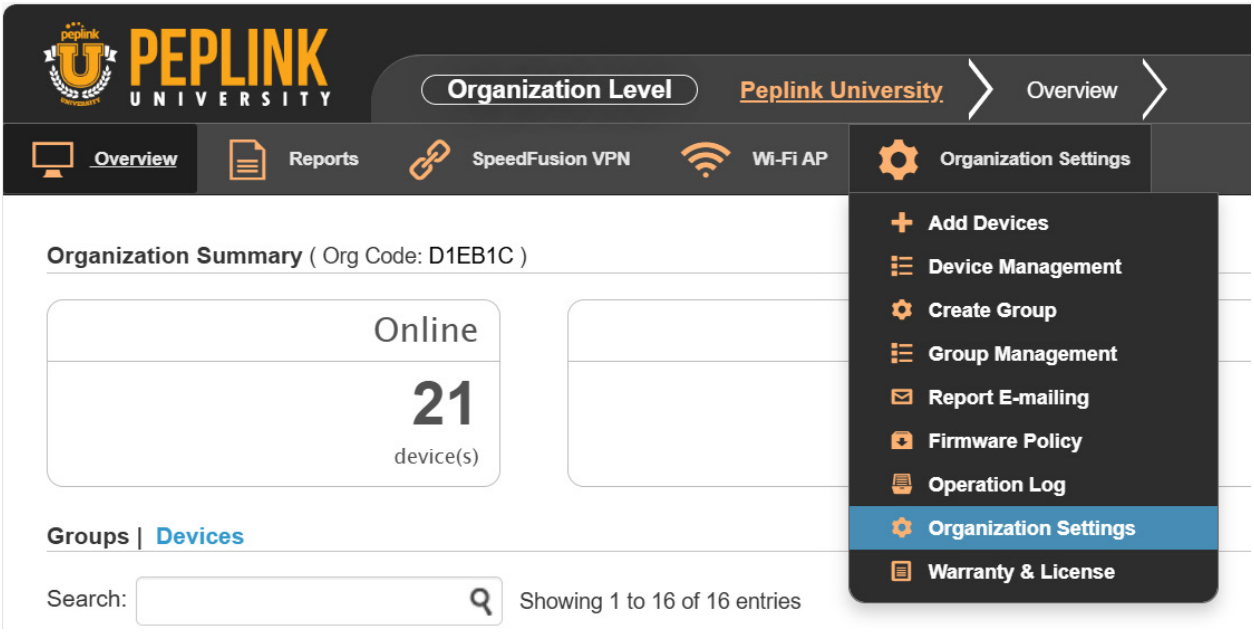


Local Admin:

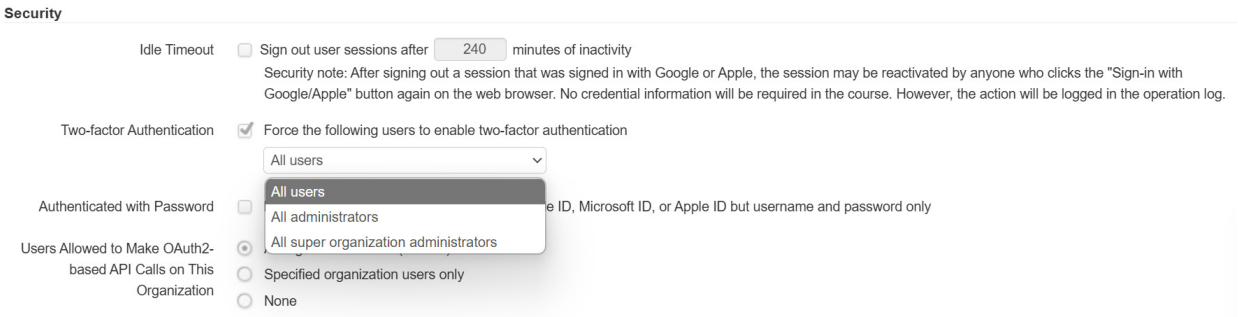
1: Enable HTTPS: Ensure that the web admin interface is accessible only via HTTPS.
2: Restrict IP Addresses: Limit access to the web admin interface to specific IP addresses within your LAN.

InControl2 for Management with Multi-Factor Authentication (MFA)

1: Navigate to ‘Organization Settings’, then select ‘Organization Settings’ from the submenu from the InControl2 dashboard.

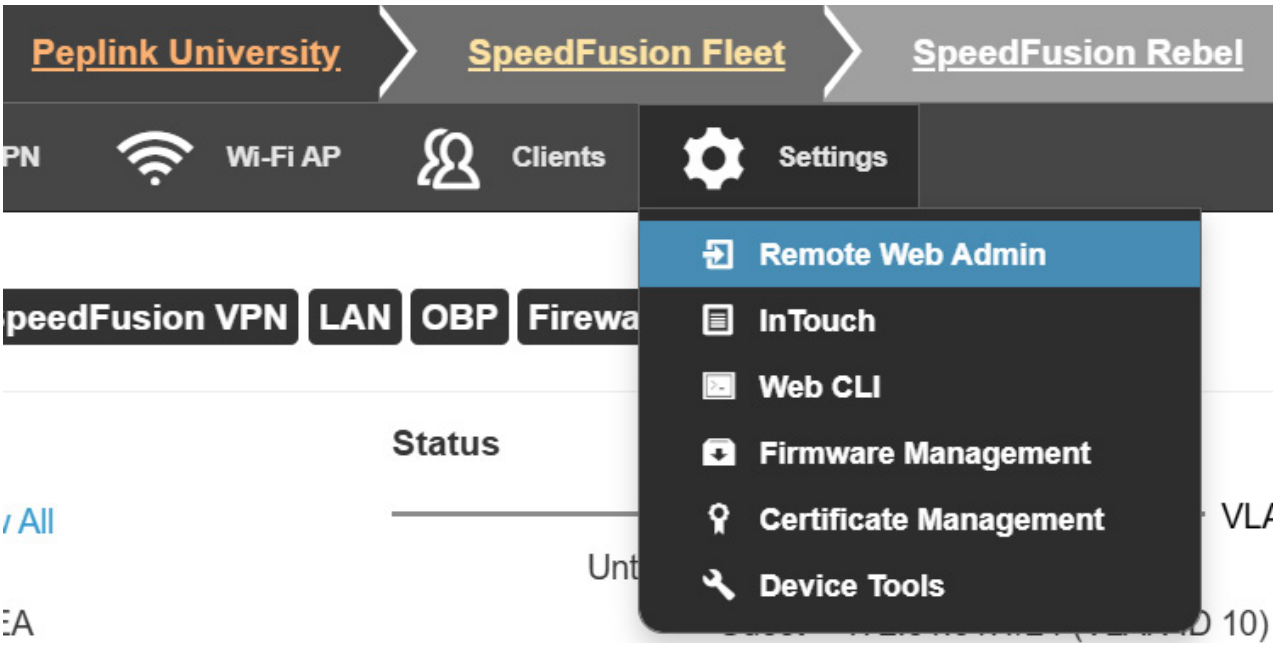


2: Check the box labeled ‘Two-Factor Authentication’. This will require your listed set of users to use two-factor authentication when logging into their InControl2 accounts for an extra layer of security.

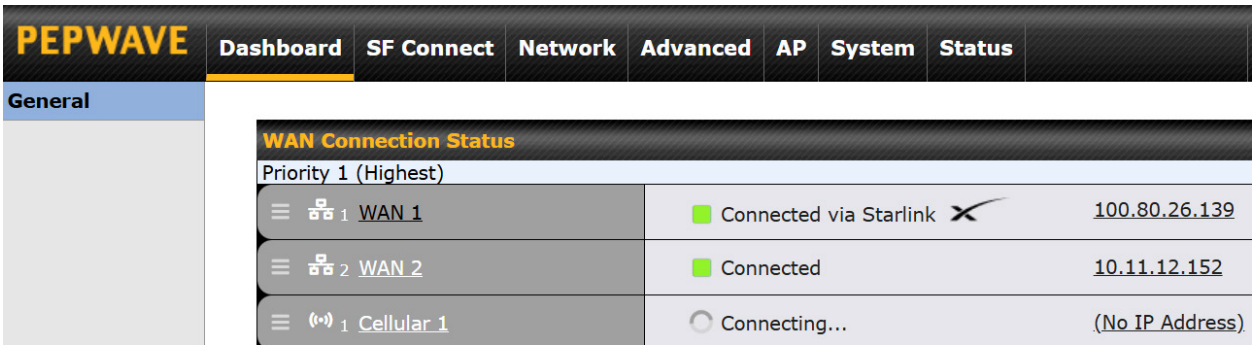


Disable ICMP Response on WAN Interfaces

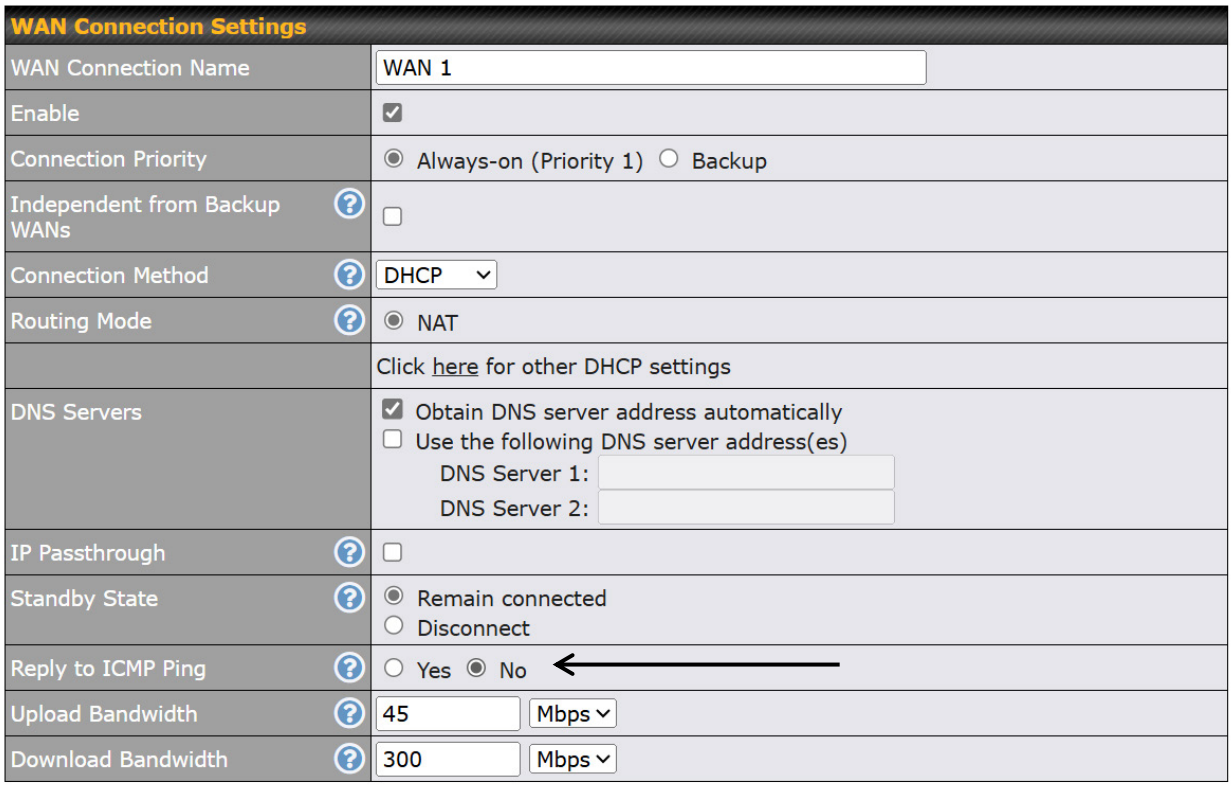
1: Access the device's web admin interface. For InControl2 users, this done by navigating to: Settings > Remote Web Admin from the Device Level.



2: From the web admin dashboard, open each WAN connection's settings by clicking the name of the connection.



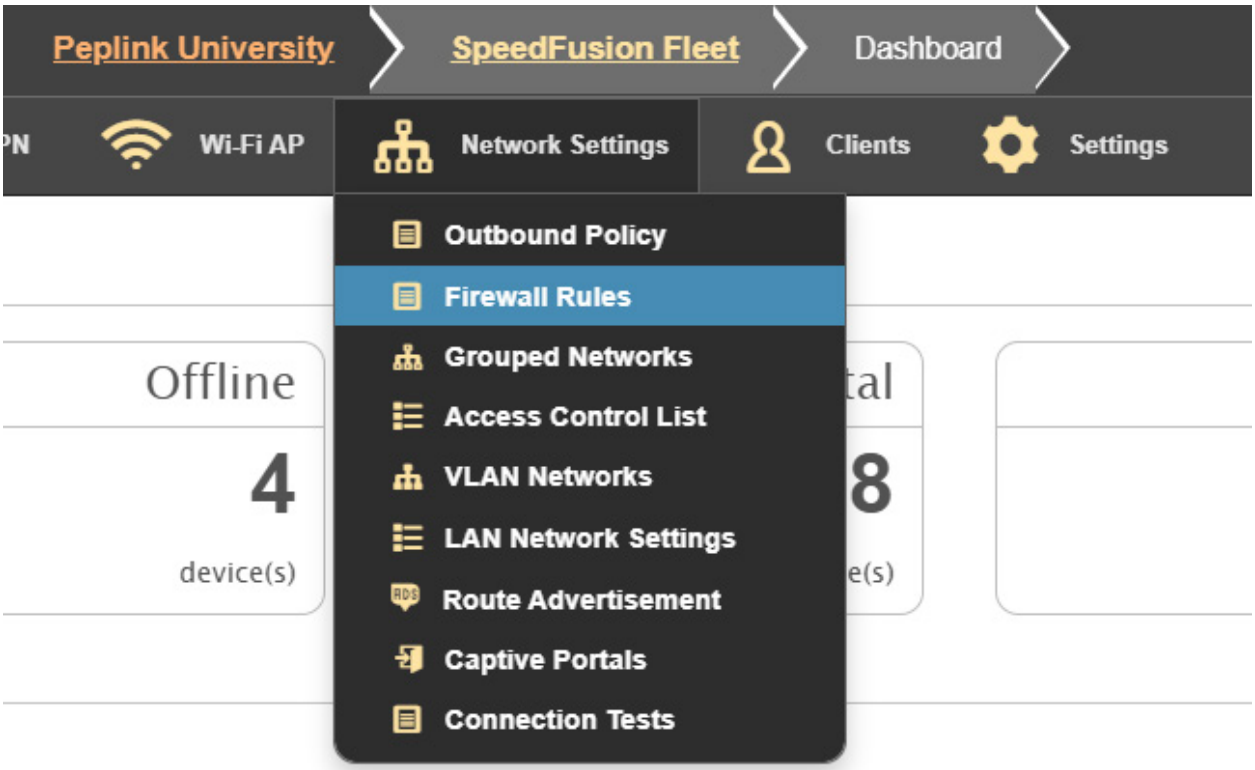
3: Within that menu, scroll down and select 'No' beside the 'Reply to ICMP Ping' option.



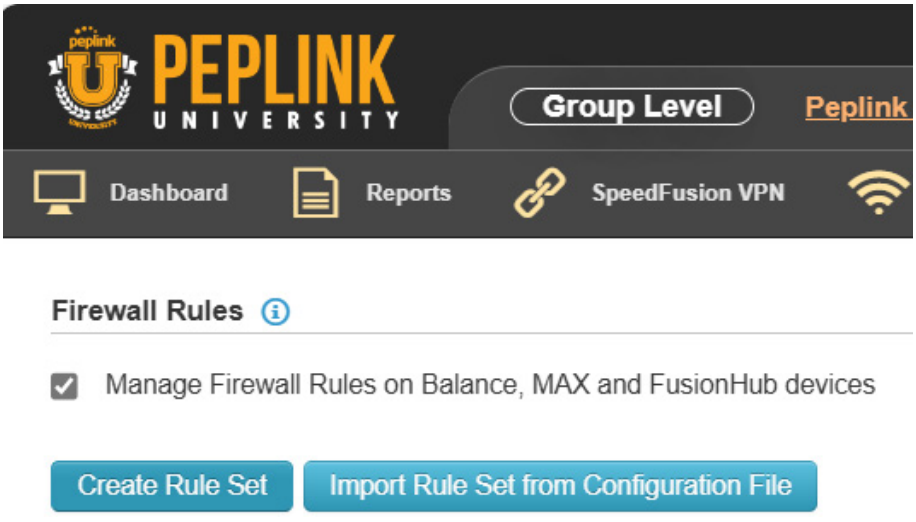
Enable Firewall with Default Deny on Inbound Traffic

InControl2:

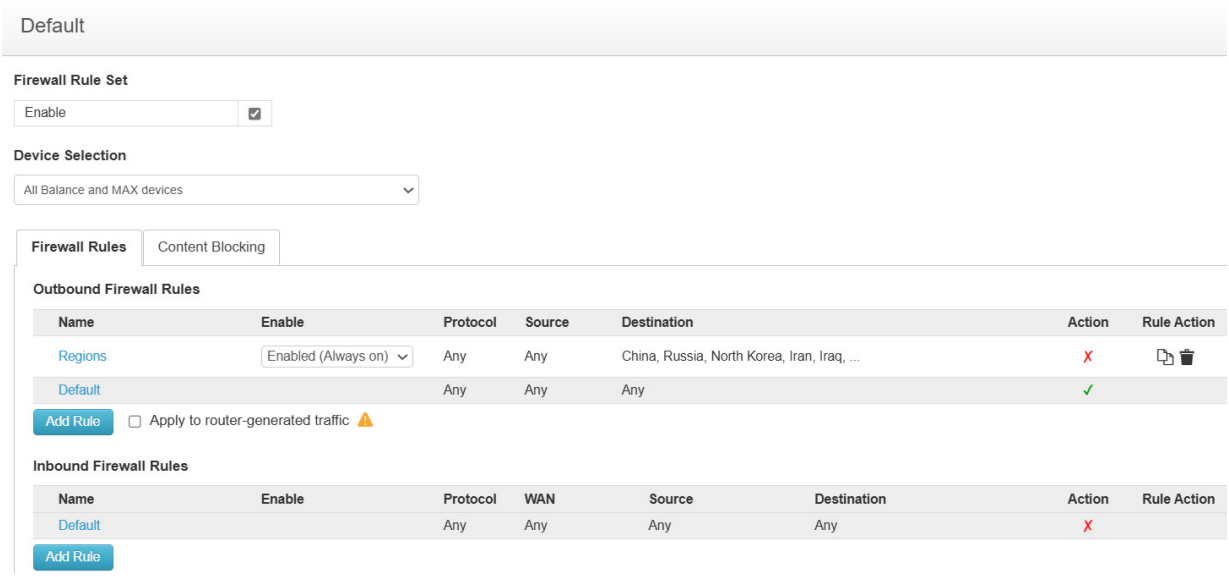
1: From the Group Level, navigate to 'Network Settings' and select 'Firewall Rules' from the submenu.

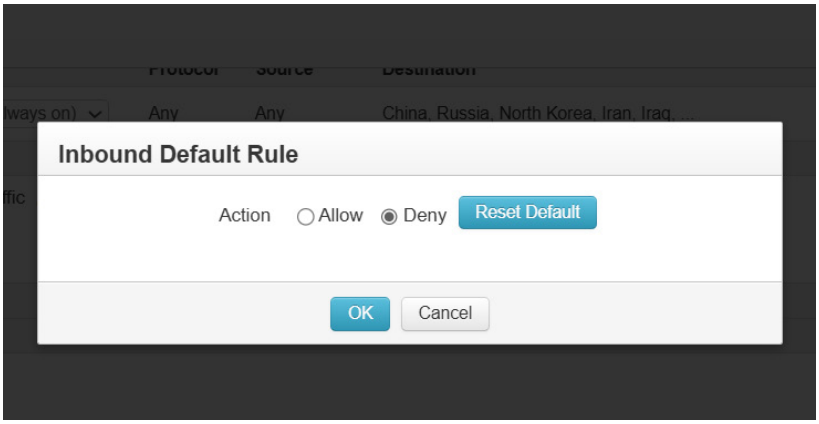


2: Press 'Create Rule Set'.

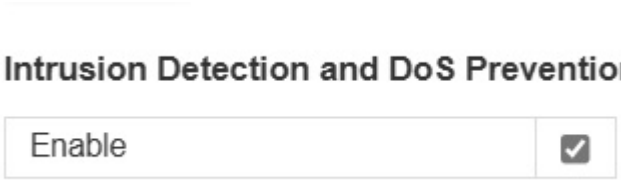


3: Under the ‘Inbound Firewall Rules’, press the option for ‘Deny’ within the Default rule.



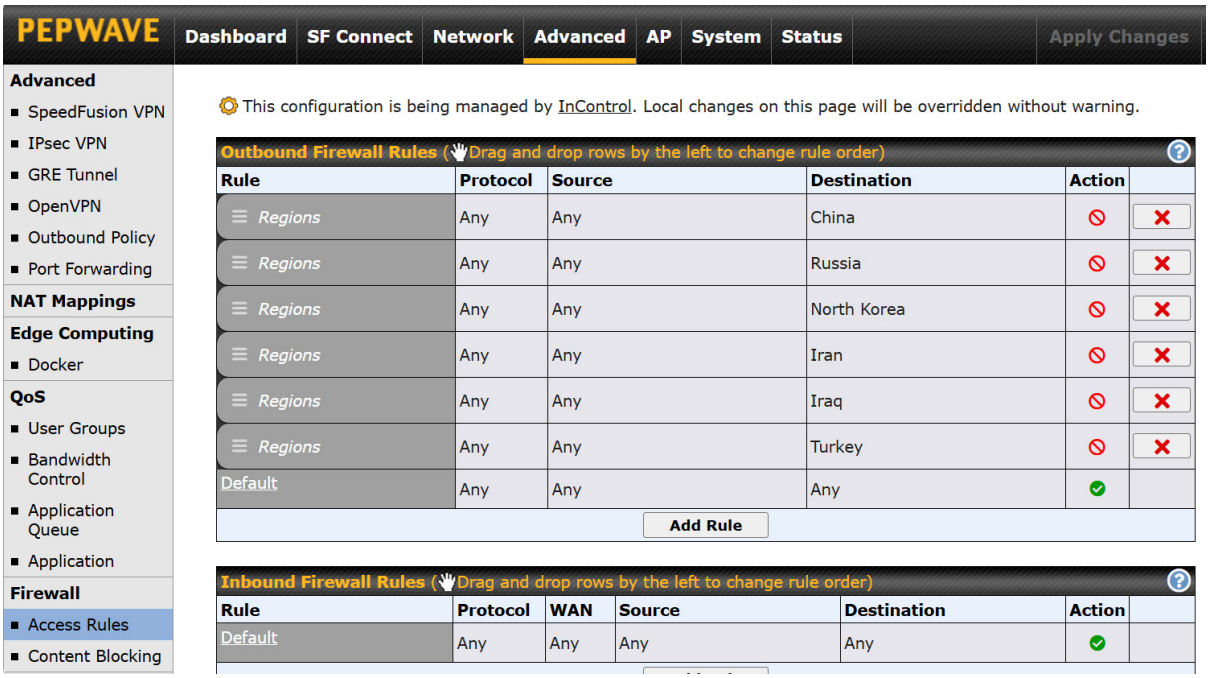


4: Enable Intrusion Detection and DDOS Prevention.

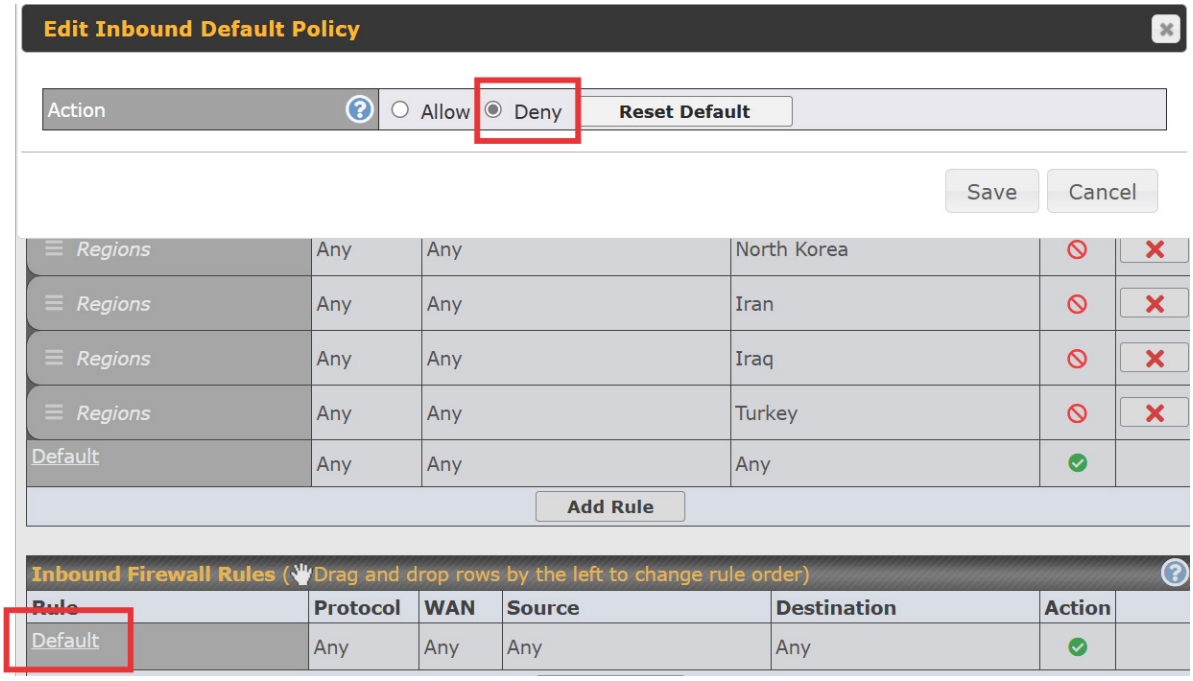


Local Web Admin:

1: Access your device via the web admin.
a: Advanced > Firewall > Access Rules.



2: Under the ‘Inbound Firewall Rules’, select ‘Default’, and change the selection to ‘Deny’, and click save.



3: Scroll down and enable 'Intrusion Detection and DoS Prevention'.

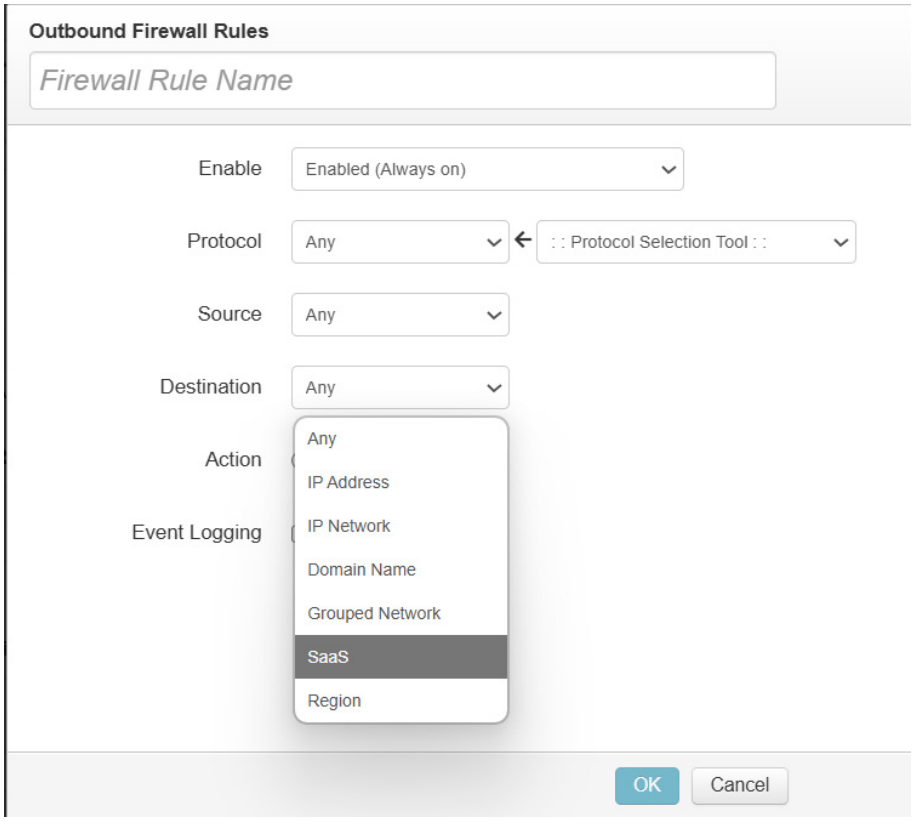
4: At the top of the page, press 'Apply Changes' and wait until confirmation that the changes have been applied.

Optional Measures: Use InControl2 Firewall Setting to Restrict Outbound Traffic

Restrict Outbound Traffic: Use InControl2 to create firewall rules that restrict outbound traffic to your country and allow only necessary SaaS applications like Microsoft and Google.

1: From the Group Level of InControl2, go to: **Network Settings > Firewall Rules**

Select the rule set, and press 'Add Rule' under the 'Outbound Firewall Rules'. During creation of the new outbound rule, change the destination to 'SaaS' or 'Region'.



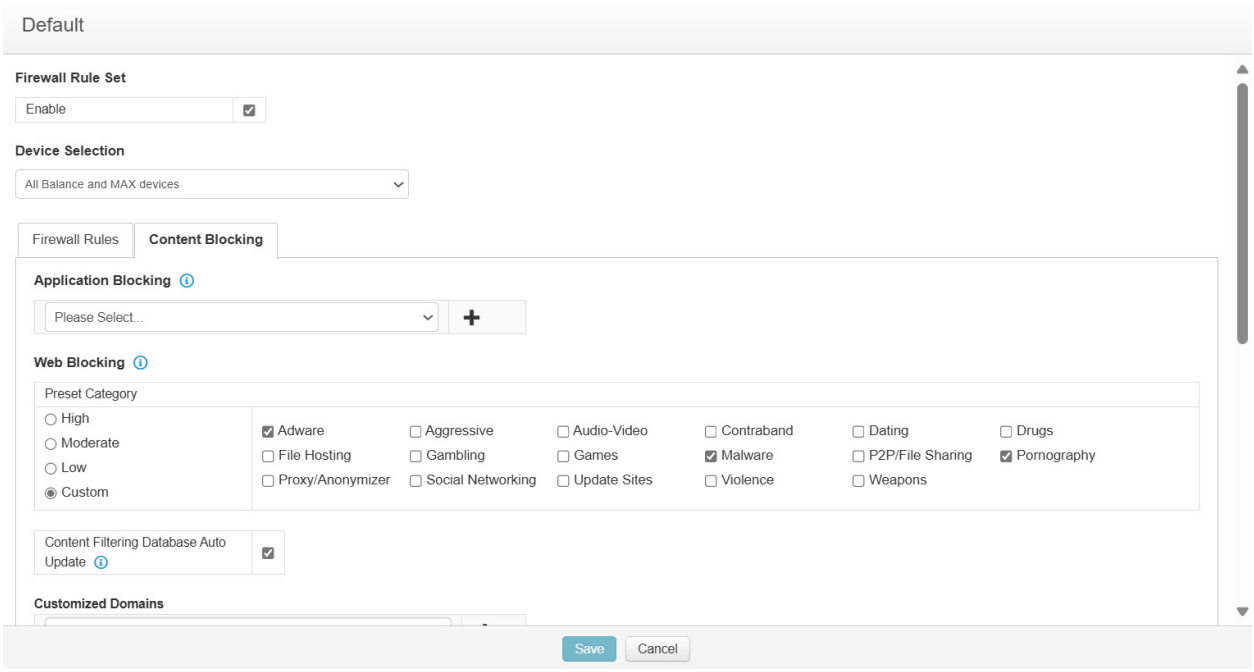
Use Application and Content Blocking Where Applicable

Local Web Admin:

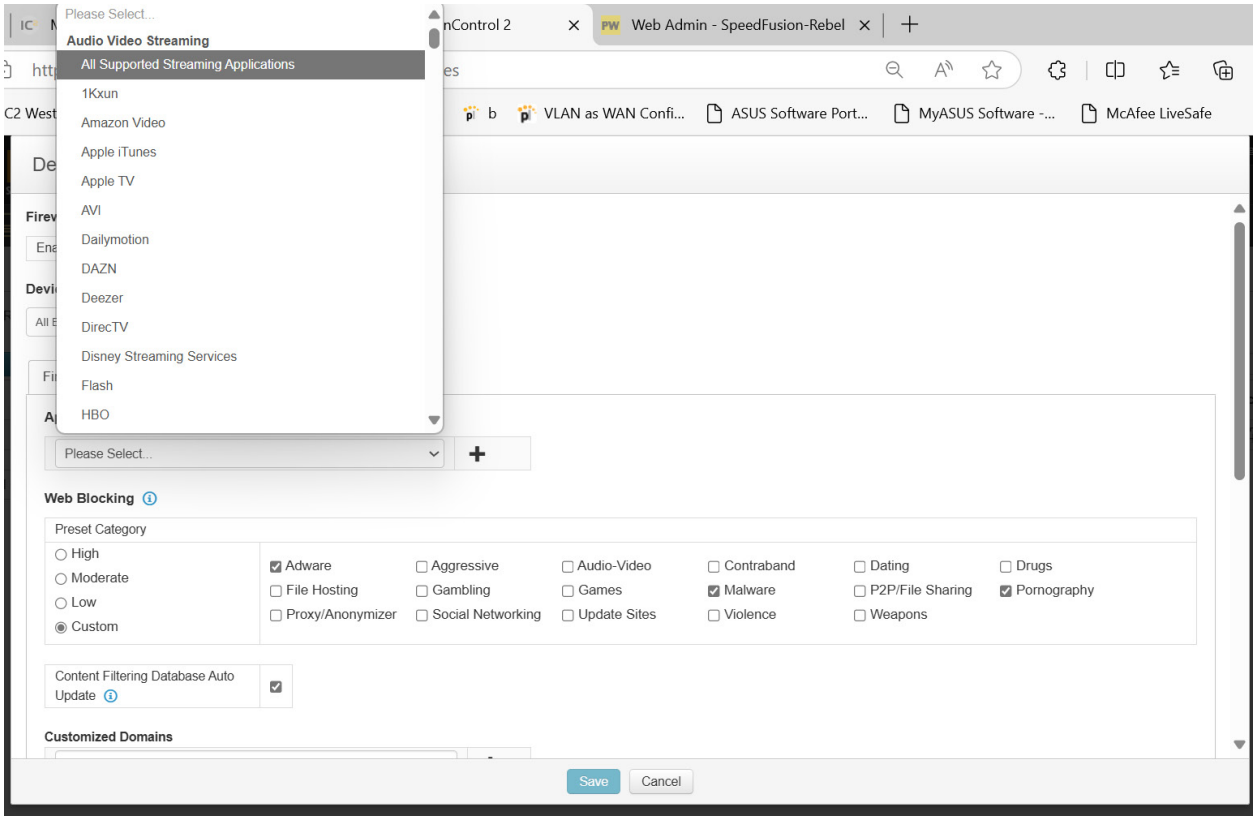
Navigate to Network > Firewall > Content Blocking: Enable content blocking and configure it to block unwanted applications and websites.

InControl 2:

1: From the Firewall Rule Set menu, change the active tab to 'Content Blocking'.



2: Select the desired content to be blocked from the Application menu, or the web blocking menu below.



Regular Review of Firewall and Router Rules

1. **Schedule regular reviews**: Set up a schedule to review your firewall and router configurations at least every six months. This ensures that the rules are still necessary and appropriate.
2. **Document changes**: Keep a detailed record of any changes made during the review. This documentation should include the reason for the change, the person who made the change, and the date of the change.
3. **Approval process**: Ensure that all changes are approved by authorized personnel. This adds an extra layer of security and accountability.

Relevant Link: **PCI DSS Requirement 1.1.7**: Review firewall and router rules at least every six months to ensure they are still necessary and appropriate*1*

Network Segmentation

1. **Implement network segmentation**: Divide your network into segments to isolate the Cardholder Data Environment (CDE) from other networks. This helps in reducing the scope of PCI DSS compliance and enhances security.
2. **Use firewalls**: Deploy firewalls to control traffic between different network segments. This ensures that only authorized traffic is allowed to pass between segments.

Relevant Link: **PCI DSS Requirement 1.2**: Restrict connections between untrusted networks and all system components in the cardholder data environment (CDE) with firewall and router configurations*1*

Secure Configuration for Network Devices

1. **Create secure configuration standards**: Develop and maintain secure configuration standards for your routers and firewalls. These standards should address all known security vulnerabilities and be consistent with industry-accepted system hardening standards.
2. **Regular updates**: Regularly update these standards to address new vulnerabilities. This ensures that your network devices are always protected against the latest threats.

Relevant Link: Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards*2*.

Logging and Monitoring

1. **Enable logging**: Ensure that logging is enabled on your routers and firewalls. This helps in tracking user activities and detecting anomalies.
2. **Review logs regularly**: Regularly review the logs for any suspicious activities. This helps in identifying potential security incidents early.

Relevant Link: **PCI DSS Requirement 10.1**: Implement logging mechanisms to track user activities and detect anomalies*2*

Incident Response Plan

1. **Develop an incident response plan**: Create a comprehensive incident response plan to address security incidents promptly. This plan should include steps for identifying, containing, eradicating, and recovering from incidents.
2. **Train your team**: Ensure that your team is trained to respond to security incidents involving your routers and firewalls. Regular training and drills can help in improving the effectiveness of your incident response plan.

Relevant Link: **PCI DSS Requirement 12.10**: Implement an incident response plan to respond to security incidents promptly*2*

Regular Security Testing

1. **Conduct penetration tests**: Perform regular penetration tests on your network devices to identify vulnerabilities. This helps in assessing the effectiveness of your security measures.
2. **Address vulnerabilities**: Address any vulnerabilities identified during the penetration tests. This ensures that your network devices are always protected against potential threats.

Relevant Link: **PCI DSS Requirement 11.3**: Implement a methodology for penetration testing that includes external and internal testing at least annually and after any significant infrastructure or application upgrade or modification*2*

Additional Resources

For more detailed instructions, you can refer to the PCI Security Standards Council and the Peplink Community.

If you have any specific questions or need further assistance with any of these steps, feel free to ask!

PCI DSS Firewall Requirements *2*: Breaking Down the PCI DSS 4.0 Requirements