



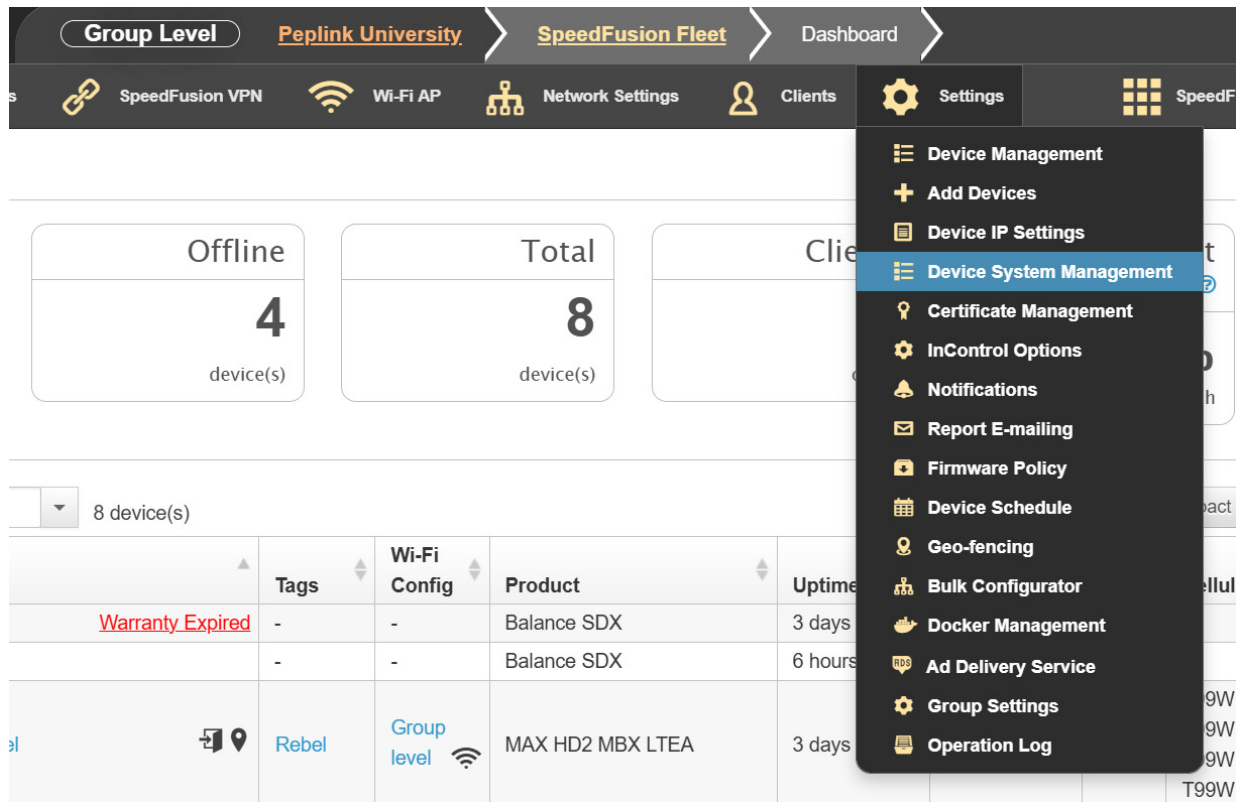
Peplink Router
PCI DSS 4
Hardening Guide

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



The screenshot shows the InControl2 Group Level Dashboard for 'Peplink University'. The top navigation bar includes 'Group Level', 'Peplink University', 'SpeedFusion Fleet', and 'Dashboard'. Below this is a secondary navigation bar with icons for SpeedFusion VPN, Wi-Fi AP, Network Settings, Clients, and Settings. The 'Settings' menu is open, showing a list of options: Device Management, Add Devices, Device IP Settings, Device System Management (highlighted), Certificate Management, InControl Options, Notifications, Report E-mailing, Firmware Policy, Device Schedule, Geo-fencing, Bulk Configurator, Docker Management, Ad Delivery Service, Group Settings, and Operation Log.

Below the navigation bar, the dashboard displays summary statistics: Offline (4 device(s)) and Total (8 device(s)). A table below shows details for 8 device(s):

Tags	Wi-Fi Config	Product	Uptime
Warranty Expired	-	Balance SDX	3 days
-	-	Balance SDX	6 hours
Rebel	Group level	MAX HD2 MBX LTEA	3 days

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

General

Device Selection	All devices in this group
Admin User Name	SecureAdmin
	☐ Device managed ☐ Assign a random password for each device ☒ Assign a shared password for all devices ***** Show
Read-only User Name	user
	☐ Device managed ☐ Assign a random password for each device ☐ Assign a shared password for all devices ☒ Disable
Web Session Timeout ⓘ	4 Hours 0 minutes

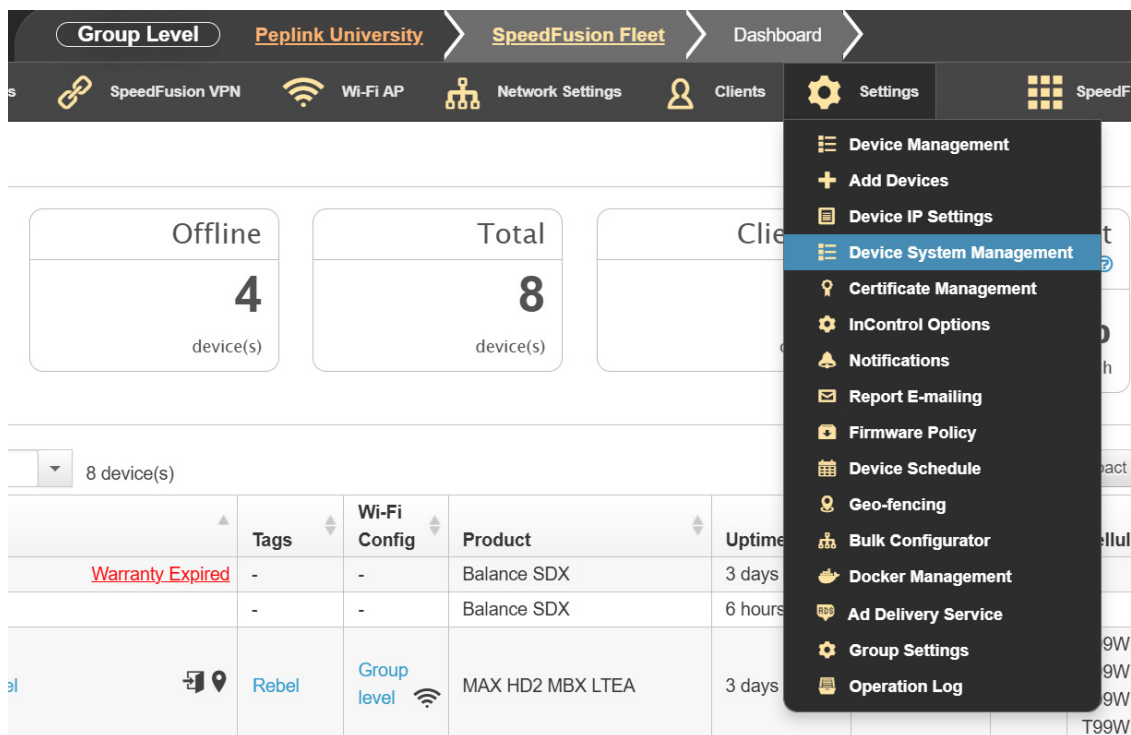
Local Web Admin:

- 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



The screenshot shows the InControl2 web interface. The top navigation bar includes 'Group Level', 'Peplink University', 'SpeedFusion Fleet', and 'Dashboard'. Below this, there are icons for 'SpeedFusion VPN', 'Wi-Fi AP', 'Network Settings', 'Clients', and 'Settings'. The 'Settings' menu is open, showing options like 'Device Management', 'Add Devices', 'Device IP Settings', 'Device System Management' (highlighted), 'Certificate Management', 'InControl Options', 'Notifications', 'Report E-mailing', 'Firmware Policy', 'Device Schedule', 'Geo-fencing', 'Bulk Configurator', 'Docker Management', 'Ad Delivery Service', 'Group Settings', and 'Operation Log'. The main content area shows a summary of device status: 'Offline 4 device(s)' and 'Total 8 device(s)'. Below this is a table with columns for 'Tags', 'Wi-Fi Config', 'Product', and 'Uptime'. The table lists two devices: 'Balance SDX' and 'MAX HD2 MBX LTEA'.

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

Balance / MAX / FusionHub / AP One [Hide](#)

Authentication Method [i](#) ☒ Local Account ☐ RADIUS ☐ TACACS+

CLI SSH & Console ☐

Note: applicable to Balance and MAX only

Security

Web Admin Access

LAN Only

LAN / WAN

Web Admin Port

Allowed LAN Networks

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.

Balance / MAX / FusionHub / AP One [Hide](#)

Authentication Method [i](#) ☒ Local Account ☐ RADIUS ☐ TACACS+

CLI SSH & Console ☐

Note: applicable to Balance and MAX only

Security

Web Admin Access

Note: applicable to Balance and MAX only

Web Admin Port

Allowed LAN Networks

SD Switch Specific [Show](#)

AP One Specific (firmware prior to 1.0.0)

- Any
- Untagged LAN
- A VLAN Network

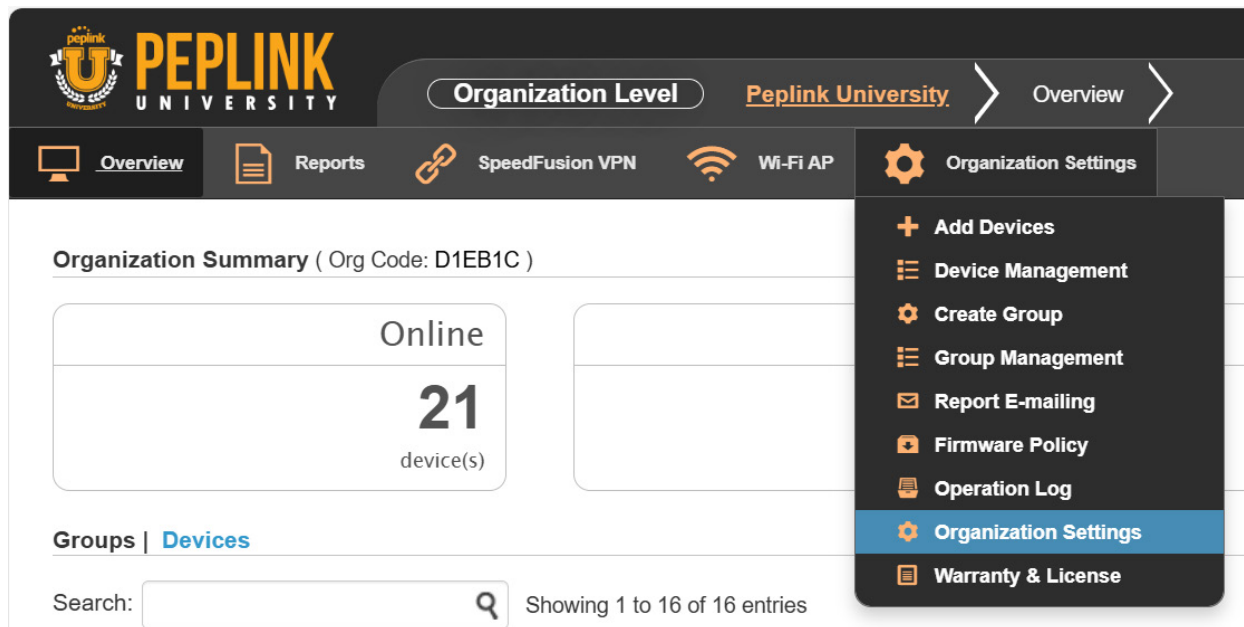
Local Admin:

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.

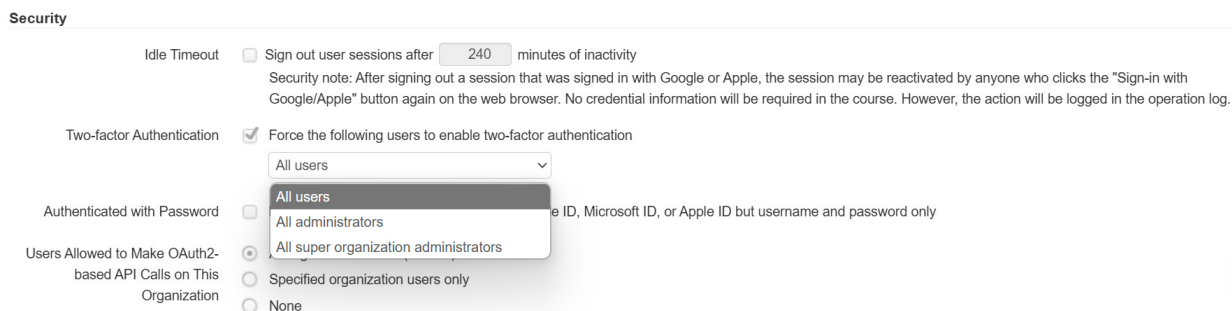
InControl2 for Management with Multi-Factor Authentication (MFA)

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



The screenshot shows the Peplink InControl2 dashboard for Peplink University. The top navigation bar includes 'Organization Level', 'Peplink University', and 'Overview'. The main navigation menu on the left includes 'Overview', 'Reports', 'SpeedFusion VPN', 'Wi-Fi AP', and 'Organization Settings'. The 'Organization Settings' menu is open, showing options: 'Add Devices', 'Device Management', 'Create Group', 'Group Management', 'Report E-mailing', 'Firmware Policy', 'Operation Log', 'Organization Settings' (highlighted), and 'Warranty & License'. The main content area shows the 'Organization Summary' with 'Online 21 device(s)' and a search bar.

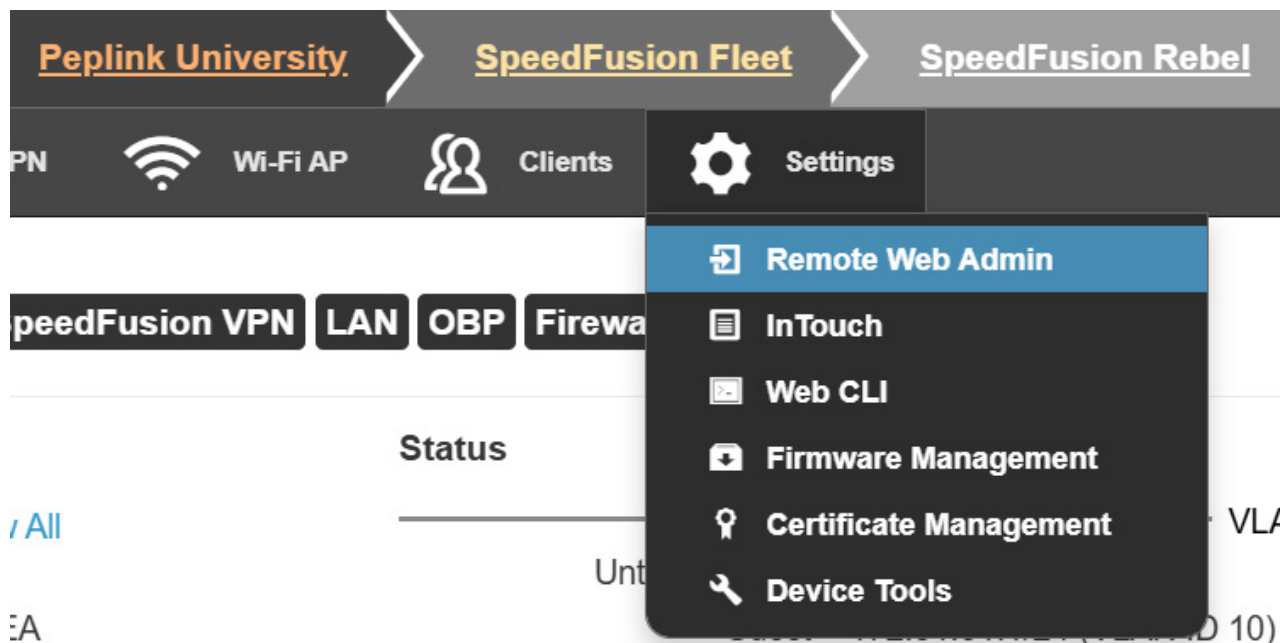
2: Check the box labeled 'Two-Factor Authentication'. This will require your listed set of users to use two-factor authentication when logging into their InControl2 accounts for an extra layer of security.



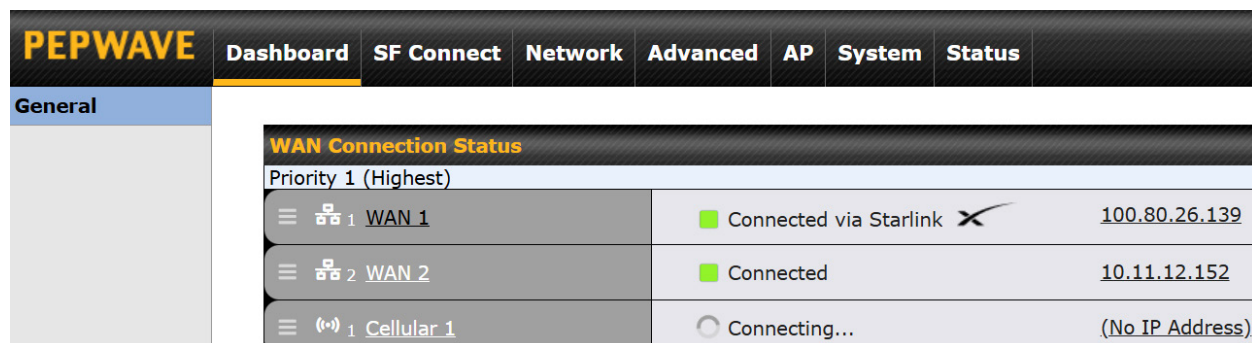
The screenshot shows the 'Security' settings page. The 'Two-factor Authentication' section is checked, and the dropdown menu is open, showing 'All users' selected. The 'Authenticated with Password' section is unchecked. The 'Users Allowed to Make OAuth2-based API Calls on This Organization' section is set to 'All super organization administrators'.

Disable ICMP Response on WAN Interfaces

1: Access the device's web admin interface. For InControl2 users, this is 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.



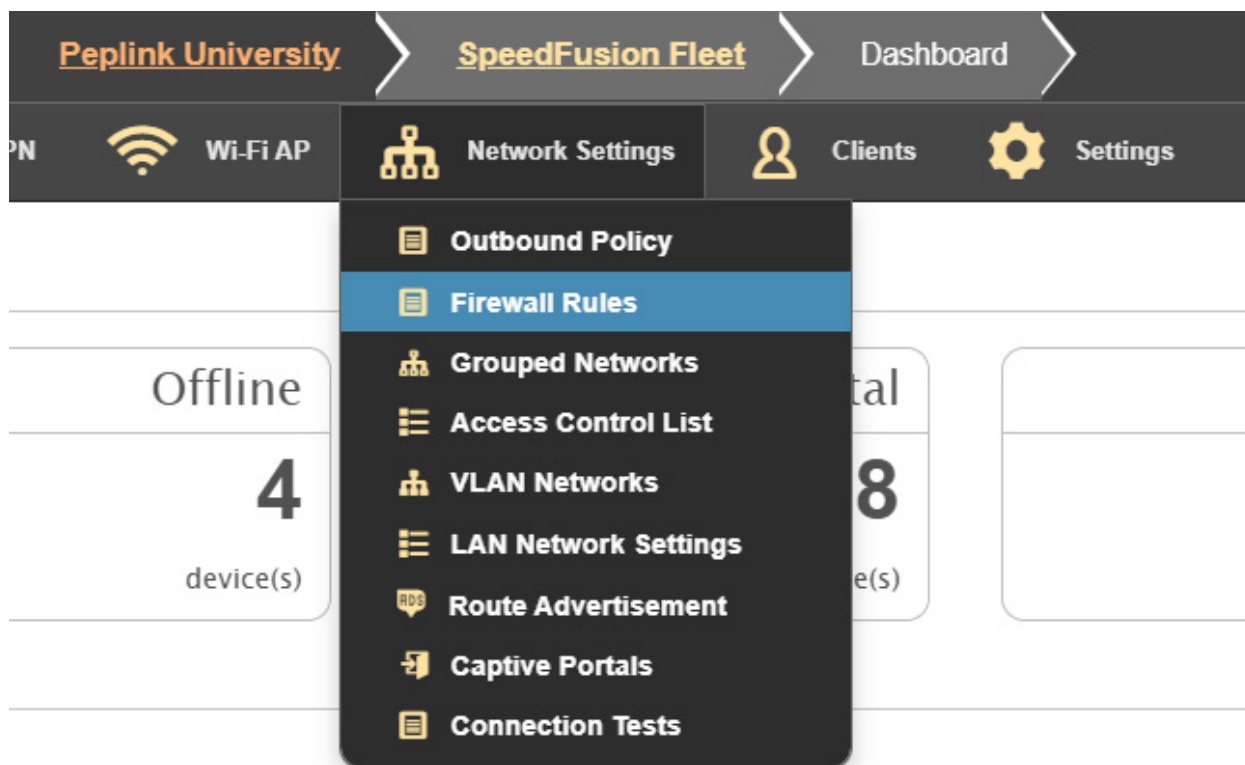
3: Within that menu, scroll down and select 'No' beside the 'Reply to ICMP Ping' option.

WAN Connection Settings	
WAN Connection Name	WAN 1
Enable	☒
Connection Priority	☒ Always-on (Priority 1) ☐ Backup
Independent from Backup WANs	☐
Connection Method	DHCP
Routing Mode	☒ NAT
	Click here for other DHCP settings
DNS Servers	☒ Obtain DNS server address automatically ☐ Use the following DNS server address(es) DNS Server 1: DNS Server 2:
IP Passthrough	☐
Standby State	☒ Remain connected ☐ Disconnect
Reply to ICMP Ping	☐ Yes ☒ No ←
Upload Bandwidth	45 Mbps
Download Bandwidth	300 Mbps

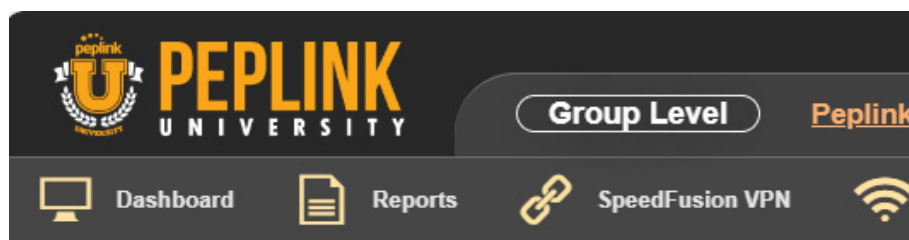
Enable Firewall with Default Deny on Inbound Traffic

InControl2:

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



2: Press 'Create Rule Set'.



Firewall Rules [i](#)

☒ Manage Firewall Rules on Balance, MAX and FusionHub devices

Create Rule Set

Import Rule Set from Configuration File

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

Default

Firewall Rule Set

Enable ☒

Device Selection

All Balance and MAX devices

Firewall Rules Content Blocking

Outbound Firewall Rules

Name	Enable	Protocol	Source	Destination	Action	Rule Action
Regions	Enabled (Always on)	Any	Any	China, Russia, North Korea, Iran, Iraq, ...	X	 
Default		Any	Any	Any	✓	

Add Rule ☐ Apply to router-generated traffic

Inbound Firewall Rules

Name	Enable	Protocol	WAN	Source	Destination	Action	Rule Action
Default		Any	Any	Any	Any	X	

Add Rule

Inbound Default Rule

Action ☐ Allow ☒ Deny [Reset Default](#)

[OK](#) [Cancel](#)

4: Enable Intrusion Detection and DDOS Prevention.

Intrusion Detection and DoS Prevention

Enable ☒

Local Web Admin:

1: Access your device via the web admin.

a: Advanced > Firewall > Access Rules.

PEPWAVE
Dashboard
SF Connect
Network
Advanced
AP
System
Status
Apply Changes

Advanced

- SpeedFusion VPN
- IPsec VPN
- GRE Tunnel
- OpenVPN
- Outbound Policy
- Port Forwarding

NAT Mappings
Edge Computing

- Docker

QoS

- User Groups
- Bandwidth Control
- Application Queue
- Application

Firewall

- Access Rules**
- Content Blocking

This configuration is being managed by InControl. Local changes on this page will be overridden without warning.

Outbound Firewall Rules

Drag and drop rows by the left to change rule order

Rule	Protocol	Source	Destination	Action	
Regions	Any	Any	China	Deny	X
Regions	Any	Any	Russia	Deny	X
Regions	Any	Any	North Korea	Deny	X
Regions	Any	Any	Iran	Deny	X
Regions	Any	Any	Iraq	Deny	X
Regions	Any	Any	Turkey	Deny	X
Default	Any	Any	Any	Allow	

Add Rule

Inbound Firewall Rules

Drag and drop rows by the left to change rule order

Rule	Protocol	WAN	Source	Destination	Action	
Default	Any	Any	Any	Any	Allow	

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

Edit Inbound Default Policy

Action
Allow
Deny
Reset Default

Save
Cancel

Regions	Any	Any	North Korea	Deny	X
Regions	Any	Any	Iran	Deny	X
Regions	Any	Any	Iraq	Deny	X
Regions	Any	Any	Turkey	Deny	X
Default	Any	Any	Any	Allow	

Add Rule

Inbound Firewall Rules

Drag and drop rows by the left to change rule order

Rule	Protocol	WAN	Source	Destination	Action	
Default	Any	Any	Any	Any	Allow	

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



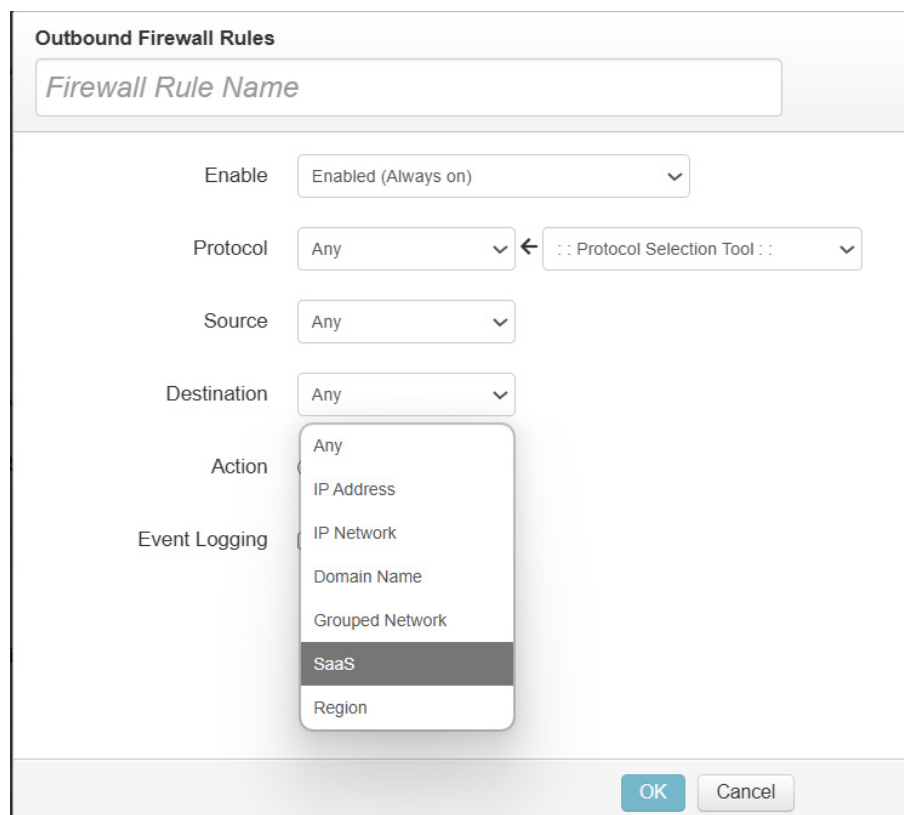
4: At the top of the page, press 'Apply Changes' and wait until confirmation that the changes have been applied.

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'.



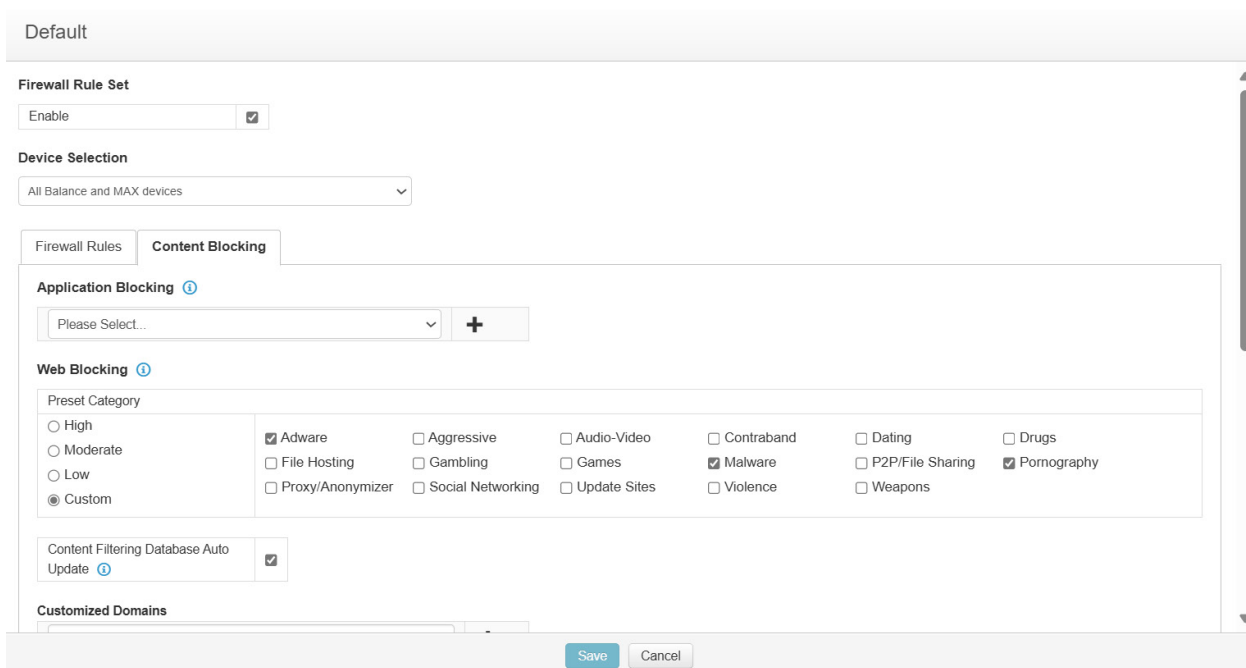
Use Application and Content Blocking Where Applicable

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'.



The screenshot shows the 'Content Blocking' configuration page in the InControl 2 interface. The page is titled 'Default' at the top. Under 'Firewall Rule Set', the 'Enable' checkbox is checked. The 'Device Selection' dropdown is set to 'All Balance and MAX devices'. The 'Content Blocking' tab is active, showing 'Application Blocking' and 'Web Blocking' sections. The 'Application Blocking' section has a dropdown menu set to 'Please Select...' and a '+' button. The 'Web Blocking' section has a 'Preset Category' dropdown set to 'Custom'. Below this, there are checkboxes for various content categories: Adware (checked), Aggressive, Audio-Video, Contraband, Dating, Drugs, File Hosting, Gambling, Games, Malware (checked), P2P/File Sharing, Pornography (checked), Proxy/Anonymizer, Social Networking, Update Sites, Violence, and Weapons. The 'Content Filtering Database Auto Update' checkbox is also checked. At the bottom, there is a 'Customized Domains' section and 'Save' and 'Cancel' buttons.

Default

Firewall Rule Set

Enable ☒

Device Selection

All Balance and MAX devices

Firewall Rules Content Blocking

Application Blocking ⓘ

Please Select...

Web Blocking ⓘ

Preset Category

☐ High ☒ Moderate ☐ Low ☒ Custom

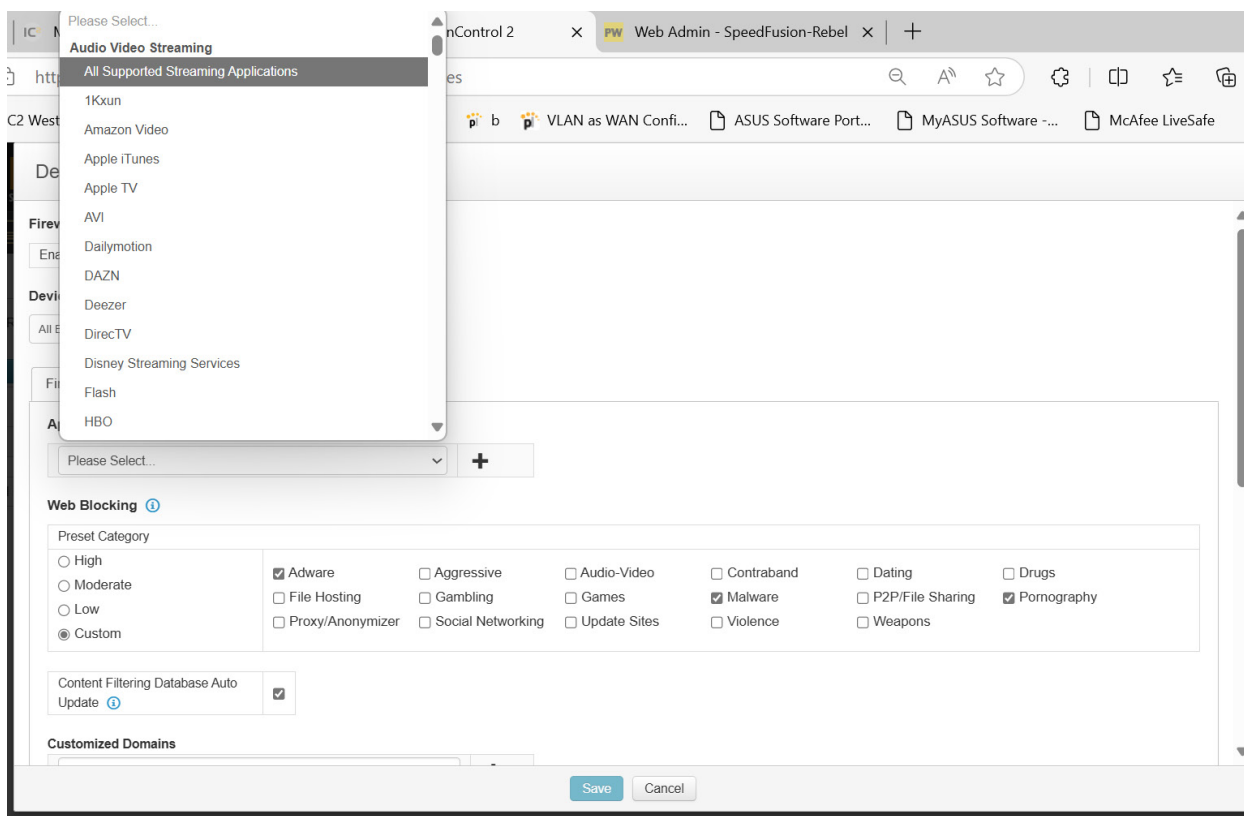
☒ Adware	☐ Aggressive	☐ Audio-Video	☐ Contraband	☐ Dating	☐ Drugs
☐ File Hosting	☐ Gambling	☐ Games	☒ Malware	☐ P2P/File Sharing	☒ Pornography
☐ Proxy/Anonymizer	☐ Social Networking	☐ Update Sites	☐ Violence	☐ Weapons	

Content Filtering Database Auto Update ⓘ ☒

Customized Domains

Save Cancel

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 standards2.](#)

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 anomalies2](#)

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 promptly2](#)

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 modification2](#)

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](#)