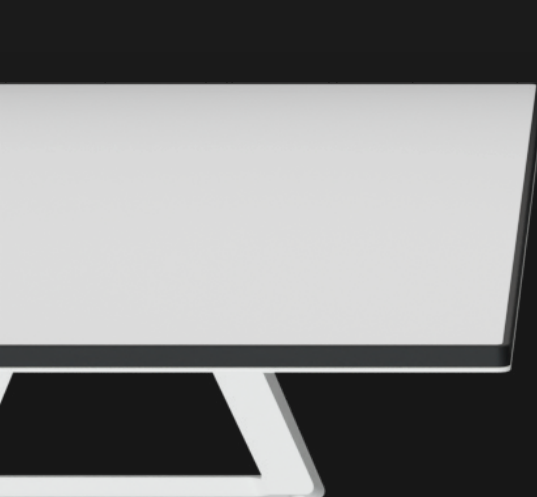




STARLINK

Technical Configuration Guide

Step-by-step procedures on bonding multiple Starlinks through a Peplink router using SpeedFusion, with three options for a remote endpoint:
SpeedFusion Connect, FusionHub, or a second Peplink device.

Contents

Step 0.	Prerequisites	3
Step 1.	Physical Connections.....	4
Step 2.	WAN Configuration per Starlink.....	6
Step 3.	SpeedFusion Bonding Configuration	10
Step 4.	Outbound Policy (Traffic Steering).....	17
Step 5.	Verification and Testing	24
Step 6.	Optimization and Troubleshooting.....	27
Step 7.	Scaling with InControl	29

Prerequisites

Complete all items below before starting the configuration. Missing any prerequisite will cause deployment issues that are difficult to diagnose later.

CRITICAL

All Starlink Routers Must Be in Bypass Mode

Every Starlink that includes a built-in router must be placed in bypass mode before connecting to the Peplink router. Without bypass mode, the Starlink router performs NAT, creating a double-NAT condition that prevents SpeedFusion tunnel establishment.

Bypass mode passes the Starlink connection directly to the Peplink router's WAN port, giving Peplink full control over routing and tunnel management.

See Starlink's support article to enable this mode: [🔗 What is bypass mode?](#)

Pre-Deployment Checklist

☐ **Starlink installed, activated, and confirmed working**

Follow Starlink's installation guide for each model (Standard, Mini, Performance.)

☐ **All Starlink routers set to bypass mode**

This is mandatory, not optional. Double-NAT breaks SpeedFusion.

☐ **Multiple Starlinks installed according to Starlink's proximity guidance**

Units placed too close together can cause interference.

See Starlink's article: [🔗 Considerations for installing Multiple Starlinks in close proximity](#)

☐ **Peplink router(s) with firmware 8.6.0 or later**

SpeedFusion Boost support requires firmware 8.6.0 or later on router(s) and FusionHub.

Check current firmware under System > Firmware via Web Admin or under Dashboard > Device Details via InControl.

☐ **Remote Endpoint with Public IP Available** (*choose one of the following*)

If using SpeedFusion Connect, ensure subscription is active and activate from the router's UI.

If using FusionHub, deploy an instance on AWS, Azure, or Vultr.

If using a second Peplink device, ensure device is running firmware 8.6.0 or later.

☐ **InControl account created and router claimed**

Required for monitoring, template management, and fleet-scale deployment (Step 7).

☐ **CAT-6 Ethernet cables for each Starlink connection**

Use the Starlink-supplied cable to connect each Starlink to a Peplink WAN port. One cable per Starlink.

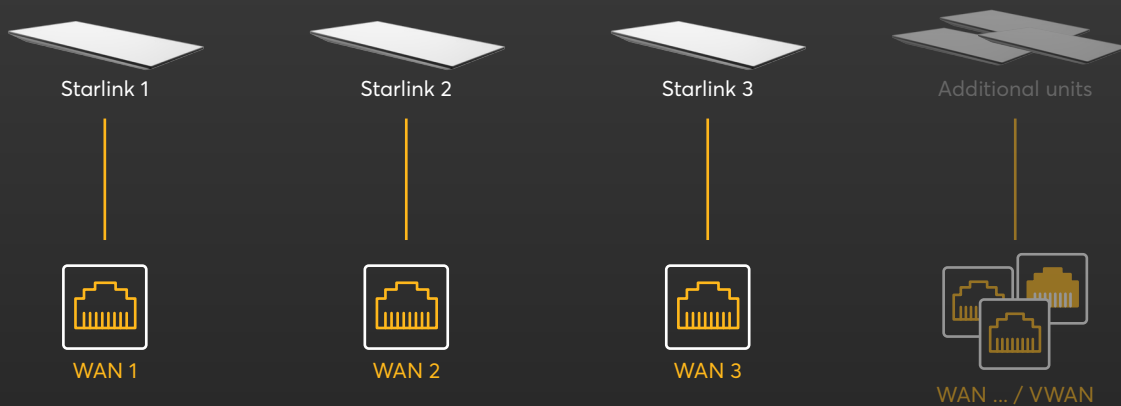
Physical Connections

Connect each Starlink's Ethernet output to a WAN port on the Peplink router. Each Starlink occupies one WAN port.

CONNECT

Starlink to Peplink WAN Port

Use the Ethernet cable from each Starlink (after bypass mode is enabled) and plug it directly into a WAN port on the Peplink router. Each Starlink gets its own dedicated WAN port.



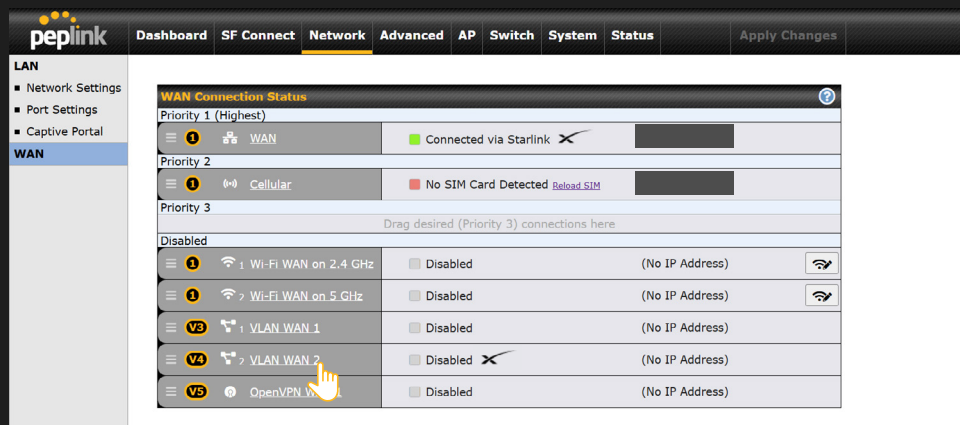
IF NEEDED

Virtual WAN: When You Have More Starlinks Than WAN Ports

If the number of Starlinks exceeds the available physical WAN ports, convert LAN ports to Virtual WAN (VWAN) interfaces using VLAN tagging.

VWAN Configuration Steps:

Step 1. Navigate to **Network > WAN > VLAN WAN** in Web Admin.



Step 2. Set **Uplink Interface** to **LAN**. Enter the number of VLANs you want to enable, e.g. 199.

DNS Server 1:
 DNS Server 2:

Standby State: ☒ Remain connected ☐ Disconnect

Reply to ICMP Ping: ☒ Yes ☐ No

Upload Bandwidth: Gbps

Download Bandwidth: Gbps

Enforce Bandwidth Limit: ☐

Physical Interface Settings

MTU: ☒ Auto ☐ Custom

MSS: ☒ Auto ☐ Custom

Uplink Interface:

VLAN:

Health Check Settings

Health Check Method:

Health Check DNS Servers:

☒ Use first two DNS servers as Health Check DNS Servers

Step 3. Navigate to **Network > LAN > Port Settings**.

Port Settings

ID	Name	Port Type	VLAN Networks	PVID	Speed	
1	HD2	Trunk	Any	Untagged LAN (1)	Auto	
2		Trunk	Any	Untagged LAN (1)	Auto	
3		Access	Reserved VLAN (199)	Auto	Auto	
4	HD2	Trunk	Any	Untagged LAN (1)	Auto	

Physical Interface Settings

Jumbo Frame: ☐ Enable

Save

Step 4. Set **Port Type** to **Access**. Match **VLAN Networks** from Step 2. Save the setting.

Port 2

Name:

Enable: ☒

PoE Enable: ☒

Speed:

Port Type:

VLAN Networks:

Save Cancel

Step 5. Navigate to **Dashboard > General**. Activate the VLAN WAN by dragging it to a different priority.

WAN Connection Status

Priority 1 (Highest)

WAN	Connected	
Wi-Fi WAN 1	Connected	
VLAN WAN 2	Connected via Starlink	
WAN 1	Connected via Starlink	

Priority 2

USB 2	No Cable Detected	(No IP Address)
-------	-------------------	-----------------

WAN Configuration per Starlink

Configure and apply the correct settings to each WAN port connected to a Starlink.



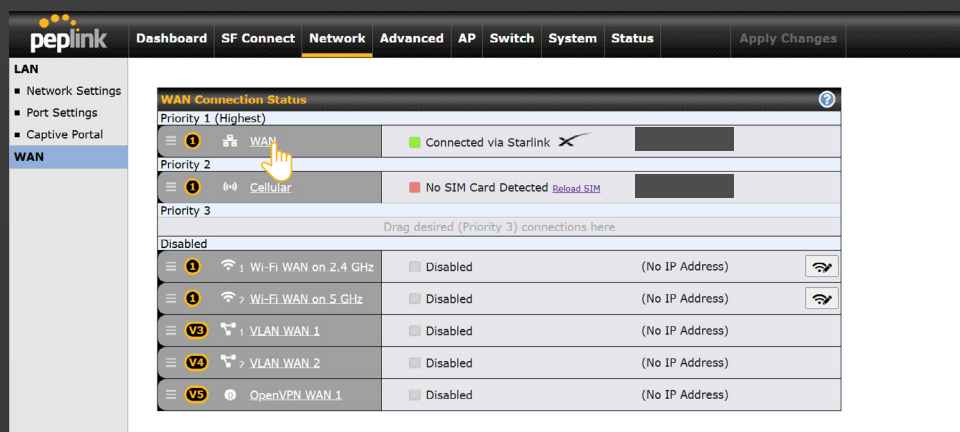
Recommendation

Watch [Manage Starlink Connections](#) to learn how to view and manage your Starlink connections in InControl.

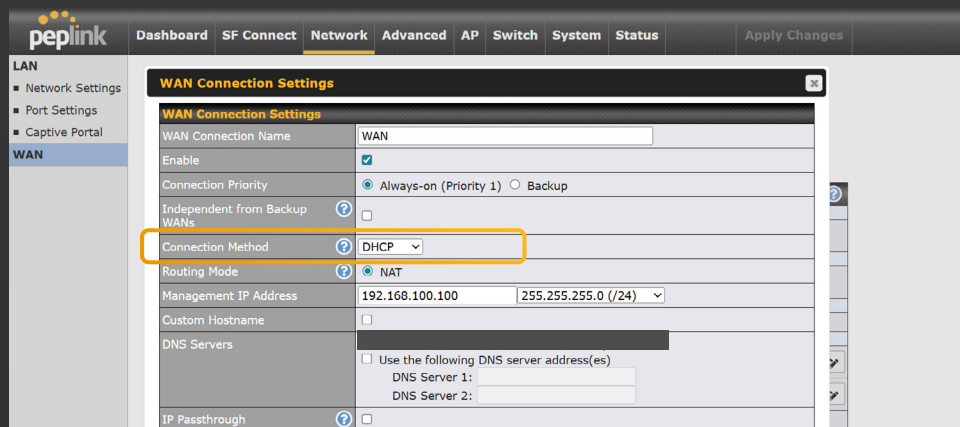
CONFIGURE

WAN Connection Settings

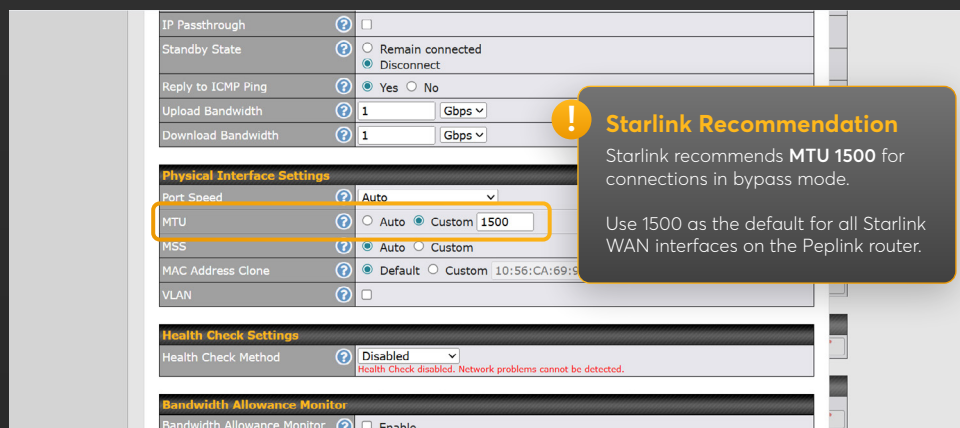
Step 1. Navigate to **Network > WAN** and select each Starlink-connected WAN.



Step 2. Set the **Connection Method** to **DHCP**.



Step 3. Set **MTU** to 1500.



Starlink Recommendation

Starlink recommends **MTU 1500** for connections in bypass mode.

Use 1500 as the default for all Starlink WAN interfaces on the Peplink router.

Step 4. Apply the **Health Check Settings**:

Health Check Settings

Health Check Method: PING

Host 1: 8.8.8.8

Host 2: 1.1.1.1

Use first two DNS servers as PING Hosts

Timeout: 5 second(s)

Health Check Interval: 10 second(s)

Health Check Retries: 5

Recovery Retries: 3

Bandwidth Allowance Monitor

Bandwidth Allowance Monitor: Enable

Additional IP Address Settings

Additional IP Address: IP Address

Step 5. Repeat this configuration for every WAN port connected to a Starlink. Each WAN should show as "Connected" on the **Dashboard** before SpeedFusion Bonding Configuration (Step 3).

WAN Connection Status

Priority 1 (Highest)

WAN: Connected

Wi-Fi WAN 1: Connected

VLAN WAN 2: Connected via Starlink

WAN 1: Connected via Starlink

Priority 2

USB 2: No Cable Detected (No IP Address)

OPTIONAL

Bandwidth Allowance

Web Admin

InControl

If your Starlink plan has data caps or priority thresholds, configure the Bandwidth Allowance setting on each WAN via Web Admin or InControl to track usage.

Web Admin

Step 1. Navigate to **Network > WAN**.

WAN Connection Status

Priority 1 (Highest)

WAN: Connected via Starlink

Priority 2

Cellular: No SIM Card Detected

Priority 3

Drag desired (Priority 3) connections here

Disabled

Wi-Fi WAN on 2.4 GHz: Disabled (No IP Address)

Wi-Fi WAN on 5 GHz: Disabled (No IP Address)

VLAN WAN 1: Disabled (No IP Address)

VLAN WAN 2: Disabled (No IP Address)

OpenVPN WAN 1: Disabled (No IP Address)

Step 2. Enable **Bandwidth Allowance**. Select the billing cycle start day and set the bandwidth allowance.

Timeout: 5 second(s)

Health Check Interval: 5 second(s)

Health Check Retries: 3

Recovery Retries: 3

Bandwidth Allowance Monitor

Bandwidth Allowance Monitor: ☒ Enable

Action: ☒ Notification is currently disabled. You can get notified when usage hits 75-95% of monthly allowance by enabling Email Notification.

☒ Disconnect when usage hits 100% of monthly allowance

Start Day: On 1st of each month at 00:00 midnight

Monthly Allowance: 100 GB

Additional IP Address Settings

Additional IP Address: IP Address: Subnet Mask: 255.255.255.255 (/32)

InControl

Step 1. Navigate to **Group Level > Network Settings > WAN Configurations**.

InControl²

Group Level Pismo Research-MY6 MY Team - Starlink Labs Dashboard

Dashboard Reports SpeedFusion VPN Wi-Fi AP Network Settings Clients Settings MY Team - Starlink Labs

MY Team - Starlink Labs

Online 3 device(s)

Total 3 device(s)

Devices

Search devices... Loading... InTouch

Status Device Name Tags Wi-Fi Config Online WAN Cellular Firmware

Balance C570 - - Balance 20X 4 days - -

MAX_HD2_7D39 EssentialCare expired - - MAX HD2 3 hours - -

MBX-Mini B93F - - MAX MBX Mini a month - -

Compact View Add Devices

WAN Configurations

Outbound Policy

Firewall Rules

Grouped Networks

Grouped MAC Addresses

VLAN Networks

LAN Network Settings

Route Advertisement

LLDP

Captive Portals

Connection Tests

Step 2. Enable **WAN Configurations**.

InControl²

Group Level Pismo Research-MY6 MY Team - Starlink Labs Network Settings WAN Configurations

Dashboard Reports SpeedFusion VPN Wi-Fi AP Network Settings Clients Settings MY Team - Starlink Labs

WAN Configurations

☒ Manage WAN configurations on Balance and MAX devices

Save

New Profile

Search:

WAN configuration profile	Applied on	Creation Date	Modified Date
No data available			

Note: WAN configurations of devices that receive no configuration profile will be kept unchanged.

Step 3. Click **New Profile**.

InControl²

Group Level Pismo Research-MY6 MY Team - Starlink Labs Network Settings WAN Configurations

Dashboard Reports SpeedFusion VPN Wi-Fi AP Network Settings Clients Settings MY Team - Starlink Labs

WAN Configurations

☒ Manage WAN configurations on Balance and MAX devices

Save

New Profile

Search:

WAN configuration profile	Applied on	Creation Date	Modified Date
No data available			

Step 4. Name the Profile. Click **Add**.

Step 5. Enter **WAN Name to Match**.

Step 6. Enable **Bandwidth Allowance**. Select the billing cycle start day and set the bandwidth allowance. **Save** the WAN setting.

Step 7. Select which devices this profile applies to. Any WAN with the specified name across the selected devices will follow this profile.

SpeedFusion Bonding Configuration

This is the core step. You will create a SpeedFusion profile that bonds all Starlink WANs into a single tunnel. Choose your deployment path below, using SpeedFusion Connect, FusionHub, or another Peplink device as the second endpoint.

PATH A - PEPLINK-HOSTED CLOUD BONDING

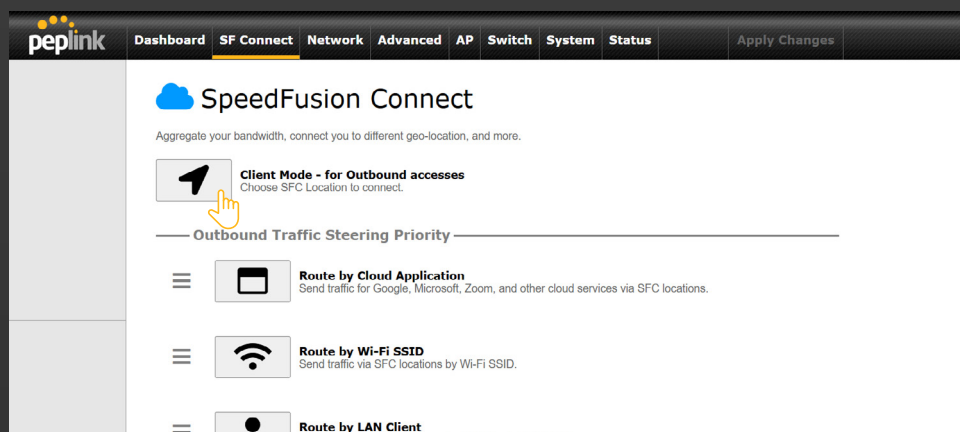
SpeedFusion Connect



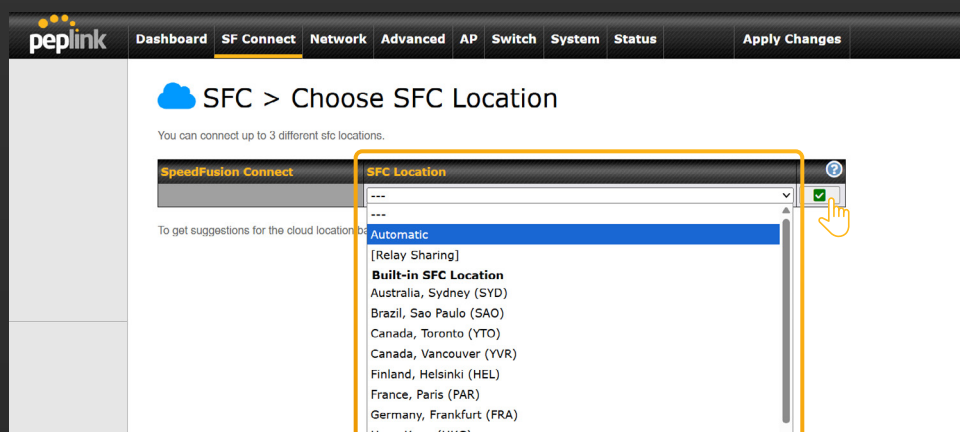
SpeedFusion Connect uses Peplink's managed cloud infrastructure as the tunnel endpoint. No external infrastructure required.

Configuration Steps:

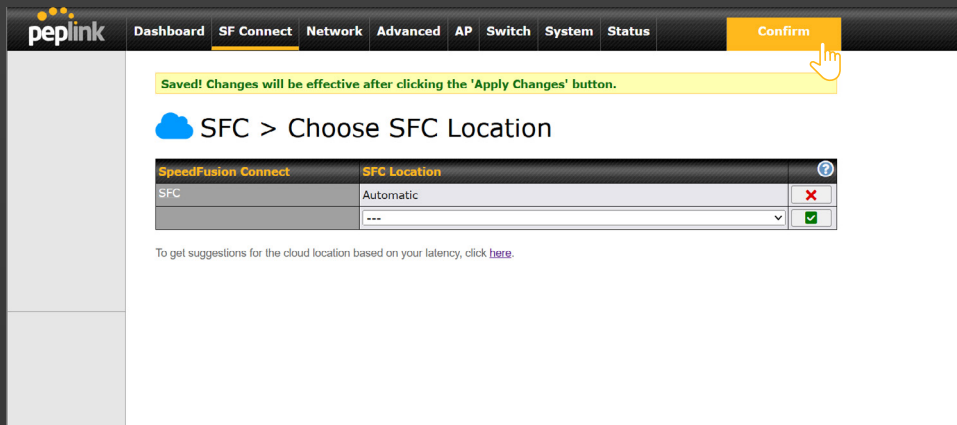
Step 1. Navigate to **SpeedFusion Connect** in Web Admin. Click **Client Mode**.



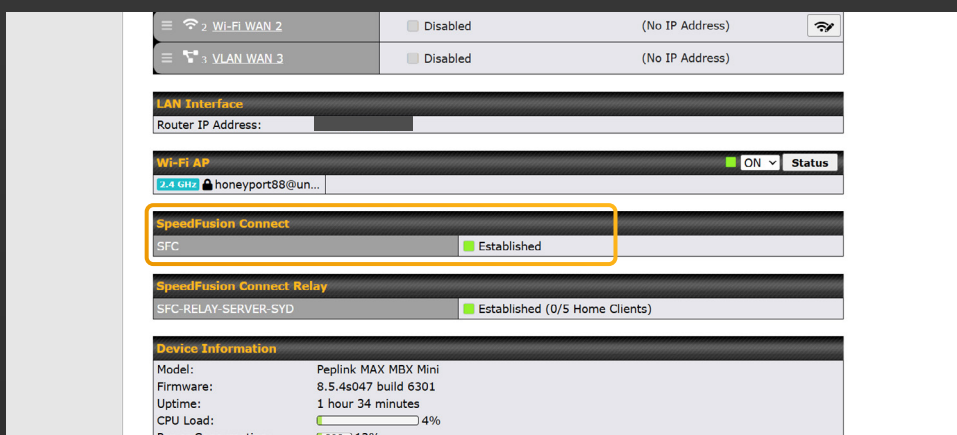
Step 2. Select **Automatic** to connect to the server location in the closest region. You can select another location as needed. Click on the green checkmark to confirm "SFC Location".



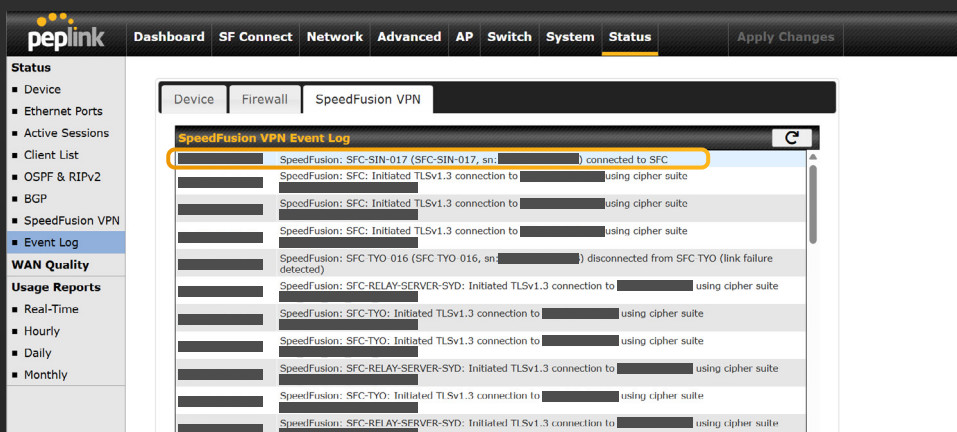
Step 3. Click **Apply Changes**.



Step 4. Check that SpeedFusion Connect is established by navigating to the **Dashboard**.



Optional. To check which server location is connected, go to **Status > Event Log > SpeedFusion VPN**.



PATH B - CUSTOMER-CONTROLLED CLOUD APPLIANCE

FusionHub



FusionHub is a virtual SpeedFusion appliance you deploy on your own cloud infrastructure.

You must first deploy the FusionHub instance, then configure the site router to connect to it. For AWS, Azure, or Vultr, follow the configuration steps up to Chapter 7.2 of [FusionHub Deployment Guide](#).

Note. Use the FusionHub instance's public IP address.

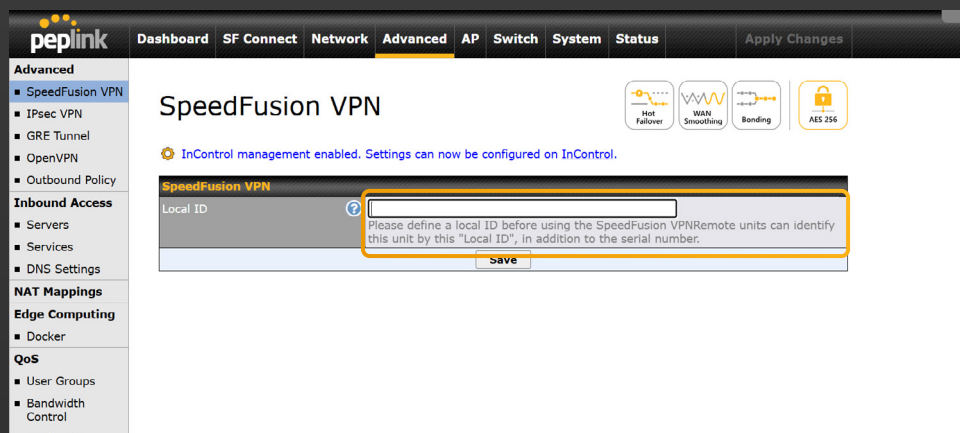
PATH C - CUSTOMER-OWNED PHYSICAL ENDPOINT

Peplink Router

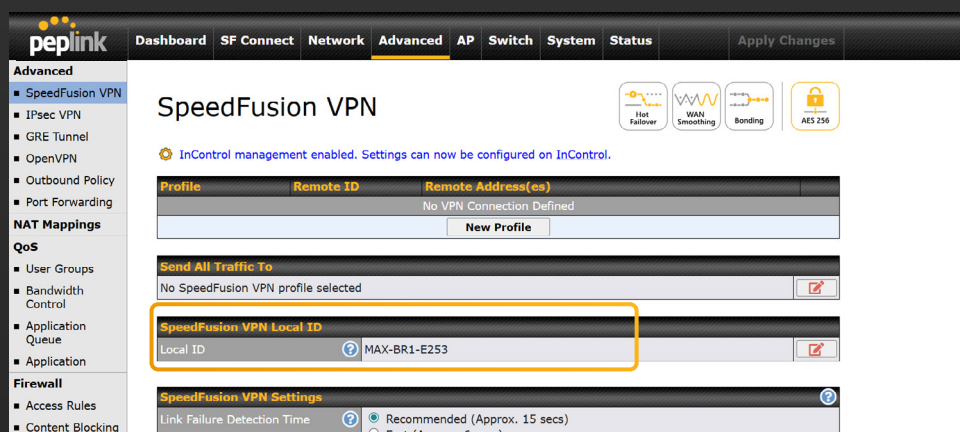


Using a Peplink router as the tunnel endpoint provides a subscription-free, customer-owned hardware solution for high-throughput enterprise connectivity. This requires two Peplink devices with SpeedFusion capability, with a public IP on at least one WAN connection.

Step 1. Open a separate tab for both routers and navigate to **Advanced > SpeedFusion VPN**. Assign a **Local ID** to each device.



Step 2. Ensure each router has been assigned its own **Local ID**. You will need these Local IDs in later steps.



Step 3. On the first router, add a **New Profile**.

Step 4. Name the profile, enter the Local ID of the second router as the **Remote ID**, and create a **Pre-shared Key**.

Step 5. Click **Apply Changes**.

Step 6. On the second router, add a **New Profile**.

Step 7. Enter the **Name** and **Pre-shared Key** created on the first router (Step 4). Enter the Local ID of the first router as the **Remote ID**.

peplink Dashboard SF Connect Network **Advanced** AP Switch System Status Apply Changes

SpeedFusion VPN Profile

Name: Demo

Enable: ☒

Encryption: ☒ 256-bit AES ☐ OFF

Authentication: ☒ Remote ID / Pre-shared Key ☐ X.509

Remote ID / Pre-shared Key: Remote ID: MAX-BR1-E253, Pre-shared Key: [Masked]

Allow shared Remote ID: ☐

NAT Mode: ☐

Remote IP Address / Host Names (Optional): [Empty]

Cost: 10

Data Port: ☒ Auto ☐ Custom

Step 8. Navigate to **Dashboard > General**. Copy the **WAN IP Address** of the first router.

peplink Dashboard **General** SF Connect Network Advanced AP Switch System Status Apply Changes

WAN Connection Status

Priority 1 (Highest):

- WAN: Connected via Starlink, IP: 10.8.10.2
- Wi-Fi WAN on 5 GHz: Connected to PLHQ_Marketing_11a, IP: 10.10.15.109

Priority 2:

- Cellular: Standby

Priority 3:

Drag desired (Priority 3) connections here

Disabled:

- Wi-Fi WAN on 2.4 GHz: Disabled (No IP Address)
- VLAN WAN 1: Disabled (No IP Address)

LAN Interface

Router IP Address: [Empty]

Wi-Fi AP OFF Status

Step 9. Paste the first router's IP address into the **Remote IP Address** field on the second router. Click **Save** and **Apply Changes**.

peplink Dashboard SF Connect Network **Advanced** AP Switch System Status Apply Changes

SpeedFusion VPN Profile

Name: Demo

Enable: ☒

Encryption: ☒ 256-bit AES ☐ OFF

Authentication: ☒ Remote ID / Pre-shared Key ☐ X.509

Remote ID / Pre-shared Key: Remote ID: MAX-BR1-E253, Pre-shared Key: [Masked]

Allow shared Remote ID: ☐

NAT Mode: ☐

Remote IP Address / Host Names (Optional): 10.8.10.2

Cost: 10

Data Port: ☒ Auto ☐ Custom

Step 10. Check that SpeedFusion VPN is established by navigating to the **Dashboard**.

peplink Dashboard **General** SF Connect Network Advanced AP Switch System Status Apply Changes

SpeedFusion VPN

Demo: Established

SpeedFusion Connect

SFC: Established

Data usage allowance: 1.00 TB (Expiry date: Dec 30, 2026)

ALL PATHS

SpeedFusion Boost

SpeedFusion Boost is a single on/off setting. When enabled, it automatically optimizes all traffic flowing through the bonded tunnel, making connections faster, cleaner, and more responsive for real-time applications.

Boost scales with the number of Starlinks in the architecture. The more you add, the better Boost performance and aggregate throughput become. There is no additional configuration or tuning required.

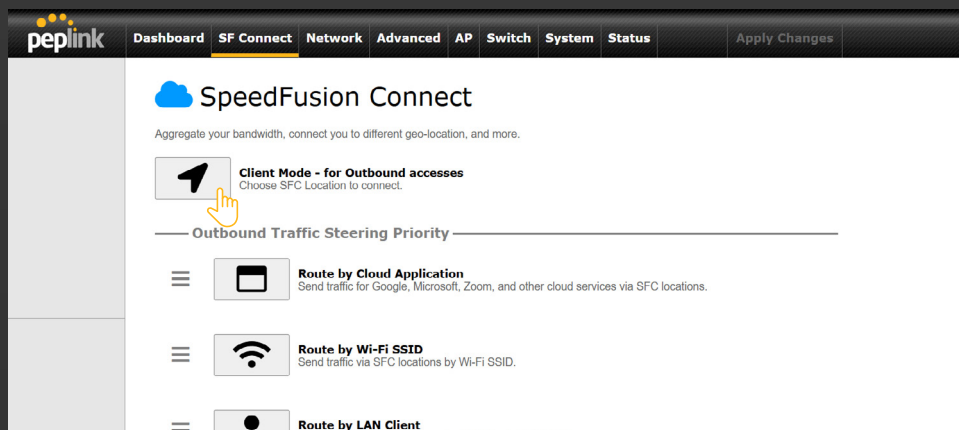
Note. SpeedFusion Boost requires firmware version 8.6.0. Please be aware that version 8.6.0 has not yet been officially released.



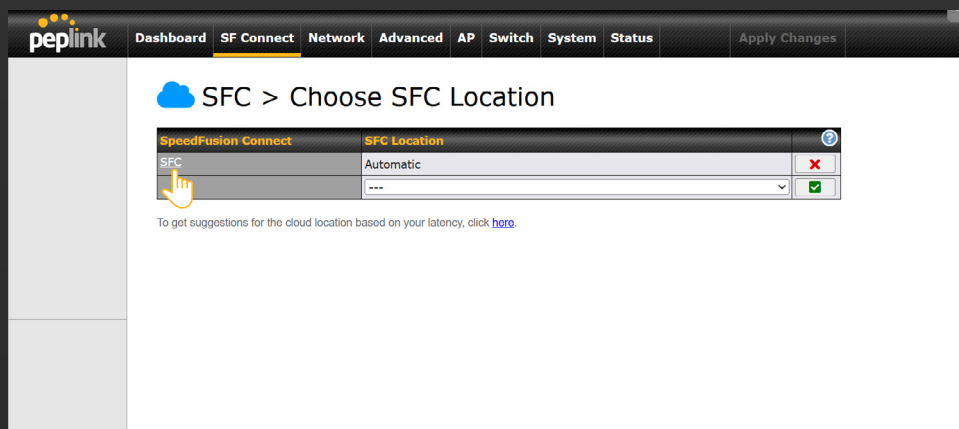
Recommendation

Enable SpeedFusion Boost on every multi-Starlink bonded deployment.

Step 1. Navigate to **SpeedFusion Connect > Client Mode**.



Step 2. Click **SFC**.



Step 3. Enable SpeedFusion Boost.

SpeedFusion Connect Profile

Enable ☒

SFC Location: Automatic

Tunnel Options

Local / Remote Tunnel ID: 1 (default tunnel)

Tunnel Name:

Data Port: ☒ Auto ☐ Custom

Bandwidth Limit: ☐

SpeedFusion Boost: ☒ (hand icon clicking)

TCP Ramp Up:

WAN Smoothing: Off



Step 1. Navigate to **Advanced** > **SpeedFusion VPN**.

SpeedFusion VPN

InControl management enabled. Settings can now be configured on InControl.

Profile	Remote ID	Remote Address(es)
Demo	MAX-BR1-E253	1

Send All Traffic To

No SpeedFusion VPN profile selected

SpeedFusion VPN Local ID

Local ID: Balance-B580X-7105

SpeedFusion VPN Settings

Link Failure Detection Time: Recommended (Approx. 15 secs)

Step 2. Enable SpeedFusion Boost.

SpeedFusion VPN Settings

Encryption: ☒ 256-bit AES ☐ OFF

Authentication: ☒ Remote ID / Pre-shared Key ☐ X.509

Remote ID / Pre-shared Key: Remote ID: MAX-BR1-E253, Pre-shared Key:

Allow shared Remote ID: ☐

NAT Mode: ☐

Remote IP Address / Host Names (Optional):

Cost: 10

Data Port: ☒ Auto ☐ Custom

Bandwidth Limit: ☐

SpeedFusion Boost: ☒ (hand icon clicking)

TCP Ramp Up:

WAN Smoothing: Off

Forward Error Correction: Off

Receive Buffer: 0 ms

Outbound Policy (Traffic Steering)

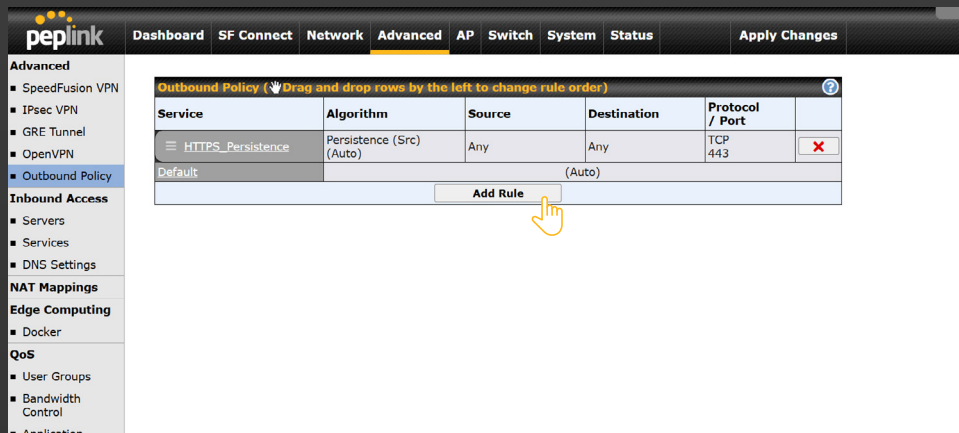
Once a SpeedFusion tunnel is established, traffic must be explicitly routed through it via outbound policies. This section covers how to route all traffic through the SpeedFusion tunnel, and split policies for deployments that require separating critical from non-critical traffic.

OPTION 1

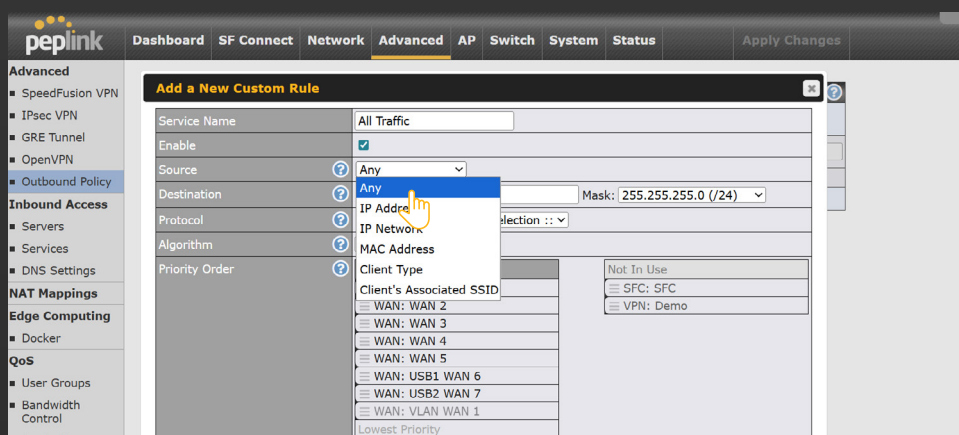
Sending All Traffic Through the SpeedFusion Tunnel

For deployments where all traffic is considered critical, an outbound policy can be configured to route all traffic through the SpeedFusion tunnel. If no outbound policy is configured, the router automatically sends traffic through the WAN connection with the lowest latency.

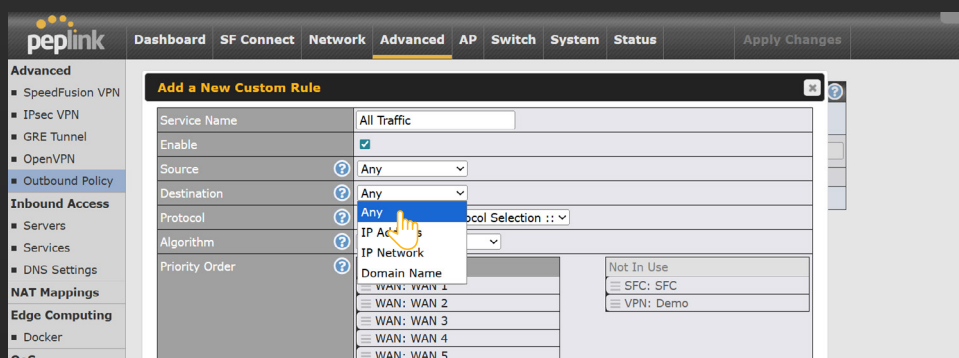
Step 1. Navigate to **Advanced > Outbound Policy > Add Rule**.



Step 2. Set **Source** to **Any**.



Step 3. Set **Destination** to **Any**.



Step 4. Set **Algorithm** to **Priority**. Drag **Speedusion Connect** or **SpeedFusion VPN** to **Highest Priority** on the left.

Add a New Custom Rule

Service Name: All Traffic

Enable: ☒

Source: Any

Destination: Any

Protocol: Any

Algorithm: Priority

Priority Order: Highest Priority, WAN: WAN 1, WAN: WAN 2, WAN: WAN 3, WAN: WAN 4, WAN: WAN 5, WAN: USB1 WAN 6, WAN: USB2 WAN 7, WAN: VLAN WAN 1, Lowest Priority

Not In Use: SFC: SFC, VPN: Demo

Step 5. Save the rule and click **Apply Changes**.

Outbound Policy (Drag and drop rows by the left to change rule order)

Service	Algorithm	Source	Destination	Protocol / Port
All Traffic	Priority SFC: SFC ...	Any	Any	Any
HTTPS_Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443
Default	(Auto)	(Auto)	(Auto)	(Auto)

Add Rule

Apply Changes

OPTION 2

Split Policy: Define Critical Traffic, Catch-All the Rest

This approach avoids the need to enumerate every non-critical destination. Define what matters, and let everything else fall through to the standard WAN path.

Create one or more rules for traffic that needs bonding and boost optimization.

Rule 1: Critical Source → Priority

Identify critical traffic and prioritize sending it through the SpeedFusion tunnel above all other connections.

Step 1. Navigate to **Network > Network Settings > New LAN**.

Network Settings

InControl management enabled. Settings can now be configured on InControl.

LAN

Untagged LAN

VLAN: [1]

IP Address / Network: []

New LAN

Static Route Settings

Static Route	Destination Network	Subnet Mask	Gateway
		255.255.255.0 (/24)	

Virtual Network Mapping

One-to-One NAT	Local Network	Virtual Network

Step 2. Set **IP Settings** and **Network Settings** as follows:

LAN

IP Settings

IP Address: 192.168.10.1 Subnet Mask: 255.255.255.0 (/24)

Network Settings

Name: Important_Traffic

VLAN ID: 10

Inter-VLAN routing: ☒

Captive Portal: ☐

DHCP Server

DHCP Server: ☒ Enable

DHCP Server Logging: ☐

IP Range: 192.168.10.10 - 192.168.10.200 Subnet Mask: 255.255.255.0 (/24)

Lease Time: 1 Days 0 Hours 0 Mins

DNS Servers: ☒ Assign DNS server automatically

Step 3. Set the **IP Range** to any valid private subnet. Save the LAN settings.

LAN

IP Settings

IP Address: 192.168.10.1 Subnet Mask: 255.255.255.0 (/24)

Network Settings

Name: Important_Traffic

VLAN ID: 10

Inter-VLAN routing: ☒

Captive Portal: ☐

DHCP Server

DHCP Server: ☒ Enable

DHCP Server Logging: ☐

IP Range: 192.168.10.10 - 192.168.10.200 Subnet Mask: 255.255.255.0 (/24)

Lease Time: 1 Days 0 Hours 0 Mins

DNS Servers: ☒ Assign DNS server automatically

Private IP Address Ranges

These ranges are used by LANs and are not accessible from the public internet without a router using NAT.

- Class A** for large networks
 - 10.0.0.0 - 10.255.255.255
- Class B** for medium networks
 - 172.16.0.0 - 172.31.255.255
- Class C** for small/home networks
 - 192.168.0.0 - 192.168.255.255

Step 4. Click **Apply Changes**.

LAN

Saved! Changes will be effective after clicking the 'Apply Changes' button.

InControl management enabled. Settings can now be configured on InControl.

LAN	VLAN	IP Address / Network
Untagged LAN	[1]	
Important_Traffic	10	192.168.10.1/24

Static Route Settings

Static Route	Destination Network	Subnet Mask	Gateway
		255.255.255.0 (/24)	

Virtual Network Mapping

One-to-One NAT	Local Network	Virtual Network

Many-to-One NAT	Local Network	Virtual IP Address

Step 5. Navigate to **Advanced > Outbound Policy > Add Rule**.

Advanced

Outbound Policy

Drag and drop rows by the left to change rule order

Service	Algorithm	Source	Destination	Protocol / Port
HTTPS_Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443
Default			(Auto)	

Add Rule

Step 6. Set **Source** to **IP Network** and enter the configured IP network to use with the SpeedFusion tunnel.

The screenshot shows the 'Add a New Custom Rule' dialog in the Peplink Advanced configuration page. The 'Source' dropdown is set to 'IP Network' and the 'Destination' dropdown is set to 'Any'. A hand cursor is pointing at the 'IP Network' option in the 'Source' dropdown menu.

Step 7. Set **Destination** to **Any**.

The screenshot shows the 'Add a New Custom Rule' dialog in the Peplink Advanced configuration page. The 'Destination' dropdown is set to 'Any'. A hand cursor is pointing at the 'Any' option in the 'Destination' dropdown menu.

Step 8. Set **Algorithm** to **Priority**. Drag **Speedusion Connect** or **SpeedFusion VPN** to **Highest Priority** on the left.

The screenshot shows the 'Add a New Custom Rule' dialog in the Peplink Advanced configuration page. The 'Algorithm' dropdown is set to 'Priority'. The 'Priority Order' list shows 'WAN: WAN 1' at the top, followed by 'WAN: WAN 2' through 'WAN: WAN 7'. A hand cursor is pointing at the 'WAN: WAN 1' entry in the 'Priority Order' list.

Step 9. Save the rule and click **Apply Changes**.

The screenshot shows the 'Outbound Policy' table in the Peplink Advanced configuration page. The table has columns for Service, Algorithm, Source, Destination, and Protocol / Port. The 'Priority' rule is listed with 'SFC: SFC' as the algorithm and 'IP Network' as the source. The 'Apply Changes' button is highlighted with a hand cursor.

Service	Algorithm	Source	Destination	Protocol / Port
Priority	Priority SFC: SFC ...	IP Network	Any	Any
HTTP Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443
Default			(Auto)	

Rule 2: Catch-All → Weighted Balance

After configuring all critical traffic rules, add a catch-all rule at the bottom. All remaining traffic (e.g. OS updates, app store downloads, general web browsing, non-critical backups) routes directly across the Starlink WANs without consuming tunnel capacity.

Step 1. Navigate to **Network > Network Settings > New LAN**.

The screenshot shows the Peplink web interface with the 'Network' tab selected. Under 'LAN', the 'New LAN' button is highlighted with a yellow circle and a hand icon. The interface also shows 'Static Route Settings', 'Virtual Network Mapping', and 'WINS Server Settings'.

Step 2. Set **IP Settings** and **Network Settings** as follows:

The screenshot shows the 'IP Settings' and 'Network Settings' for a new LAN. The 'IP Address' is set to 192.168.20.1 and the 'Subnet Mask' is 255.255.255.0 (/24). The 'Network Settings' section shows 'Name' as General_Traffic, 'VLAN ID' as 20, and 'Inter-VLAN routing' checked. The 'DHCP Server' section shows 'Enable' checked, 'IP Range' as 192.168.20.10 - 192.168.20.200, and 'Assign DNS server automatically' checked.

Step 3. Set the **IP Range** to any valid private subnet, ensuring it does not overlap with "Important_Traffic". Save the LAN settings.

The screenshot shows the 'IP Range' for a new LAN. The 'IP Range' is set to 192.168.20.10 - 192.168.20.200. The 'DHCP Server' section shows 'Enable' checked, 'IP Range' as 192.168.20.10 - 192.168.20.200, and 'Assign DNS server automatically' checked.

Step 4. Click **Apply Changes**.

The screenshot shows the Peplink web interface with the 'Network' tab selected. The 'Apply Changes' button is highlighted with a hand icon. A yellow banner at the top states: "Saved! Changes will be effective after clicking the 'Apply Changes' button." Below this, a message indicates: "InControl management enabled. Settings can now be configured on InControl." The 'LAN' section shows a table with columns: LAN, VLAN, IP Address / Network, and a status column. The table contains three rows: 'Untagged LAN' with VLAN [1], 'Important_Traffic' with VLAN 10 and IP 192.168.10.1/24, and 'General_Traffic' with VLAN 20 and IP 192.168.20.1/24. Below the table is a 'New LAN' button. The 'Static Route Settings' section shows a table with columns: Destination Network, Subnet Mask, and Gateway. The 'Virtual Network Mapping' section shows a table with columns: Local Network, Virtual Network, and Virtual IP Address.

Step 5. Navigate to **Advanced > Outbound Policy > Add Rule**.

The screenshot shows the Peplink web interface with the 'Advanced' tab selected. The 'Outbound Policy' section is active, showing a table with columns: Service, Algorithm, Source, Destination, Protocol / Port, and a status column. The table contains three rows: 'Priority' with Algorithm 'Priority SFC: SFC...', 'HTTPS_Persistence' with Algorithm 'Persistence (Src) (Auto)', and 'Default' with Algorithm '(Auto)'. The 'Add Rule' button is highlighted with a hand icon.

Step 6. Set **Source** and **Destination** to **Any**.

The screenshot shows the 'Add a New Custom Rule' dialog box in the Peplink web interface. The 'Source' and 'Destination' fields are highlighted with a yellow box and set to 'Any'. Other fields include 'Service Name' (Weighted Balance), 'Enable' (checked), 'Protocol' (Any), 'Algorithm' (Weighted Balance), 'Connection Type' (WAN), and 'Load Distribution Weight' (sliders for WAN 1-7 and USB1-2).

Step 7. Set **Algorithm** to **Weighted Balance**, WAN Selection: All Starlink WANs (equal weight). Save the rule.

The screenshot shows the 'Add a New Custom Rule' dialog box with the 'Algorithm' set to 'Weighted Balance'. The 'Load Distribution Weight' section shows sliders for WAN 1-7 and USB1-2. A yellow box highlights the 'Algorithm' and 'Load Distribution Weight' sections. A 'Note' box on the right explains the 10:5:10 ratio for WAN 1, 2, and 3.

Note

For example, WAN 1 and 3 are both Starlink WANs, set at 10. This means they are equal weighted.

10:5:10 means:
 WAN 1 handles 10 out of 25 sessions (10/25)
 WAN 2 handles 5 out of 25 sessions (5/25)
 WAN 3 handles 10 out of 25 sessions (10/25)
 The remaining WANs handle 0 sessions.

Step 8. Set **When No Connections are Available** to **Fall-through to Next Rule** and enable **Terminate Sessions on Connection Recovery**. Save the rule.

The screenshot shows the Peplink configuration interface. On the left, a sidebar lists various settings categories: Edge Computing, QoS, User Groups, Bandwidth Control, Application Queue, Application, Firewall, Access Rules, Content Blocking, Routing Protocols, Remote User Access, Misc. Settings, High Availability, RADIUS Server, and 802.1X. The main area displays a list of WAN connections: WAN: WAN 3 10, WAN: WAN 4 0, WAN: WAN 5 0, WAN: USB1 WAN 6 0, and WAN: USB2 WAN 7 0. Below this list, a configuration box for 'When No Connections are Available' is highlighted with an orange border. It contains a dropdown menu set to 'Fall-through to Next Rule' and a checkbox for 'Terminate Sessions on Connection Recovery' which is checked and labeled 'Enable'.



Note

When all WAN connections with weight > 0 are unavailable (down or failed health check):

Option 1) **Drop the Traffic**

- Traffic is dropped.

Option 2) **Use Any Available Connections**

- Traffic is routed through any available WAN with weight = 0.

Option 3) **Fall-through to Next Rule**

- This rule is skipped, and traffic follows the next outbound policy rule.

Step 9. Drag "Weighted Balance" below "Priority". Click **Apply Changes**.

The screenshot shows the Peplink configuration interface with the 'Advanced' tab selected. A yellow banner at the top states: 'Saved! Changes will be effective after clicking the 'Apply Changes' button.' Below this is the 'Outbound Policy' section with a header that says 'Drag and drop rows by the left to change rule order'. A table lists the policies: Priority, Weighted Balance, and Persistence (Src). The 'Weighted Balance' row is highlighted in blue, and a hand icon is shown dragging it to a position below the 'Priority' row. The table has columns for Service, Algorithm, Source, Destination, and Protocol / Port. The 'Priority' row has 'Priority SFC: SFC ...' as the algorithm and 'IP Network' as the source. The 'Weighted Balance' row has 'Weighted Balance WAN: ...' as the algorithm and 'Any' as the source. The 'Persistence (Src)' row has 'Persistence (Src) (Auto)' as the algorithm and 'Any' as the source. The 'Protocol / Port' column shows 'Any' for the first two rows and 'TCP 443' for the third. An 'Add Rule' button is at the bottom right of the table.

OPTIONAL

Cellular Failover Priority

If the Peplink router has an integrated cellular modem (e.g. BR2 Pro 5G, SDX Pro), configure cellular as a lower-priority WAN within the SpeedFusion tunnel. Cellular activates only if all Starlink WANs become unavailable, maintaining tunnel continuity.

The screenshot shows the Peplink configuration interface with a list of WAN connections. The list includes: GRE WAN 1, GRE WAN 2, HD1 Dome - Ethernet..., HD2 Dome - Ethernet..., HD1 Dome Pro - Ethe..., Ethernet 1/4, Ethernet 1/5, Ethernet 1/6 HD1 Do..., Ethernet 1/7, Ethernet 1/8, Starlink 1, Starlink 2, Cellular 1/1, Cellular 1 1/1, Cellular 2 1/2, Cellular 1/1, Wi-Fi WAN on 2.4 GH..., and Wi-Fi WAN on 5 GHz ... Each entry has a 'Priority' dropdown menu. The 'Starlink 1' and 'Starlink 2' entries are set to 'Priority: 1 (Highest)'. The 'Cellular 1/1' and 'Cellular 1 1/1' entries are set to 'Priority: 2'. These four entries are highlighted with an orange border.

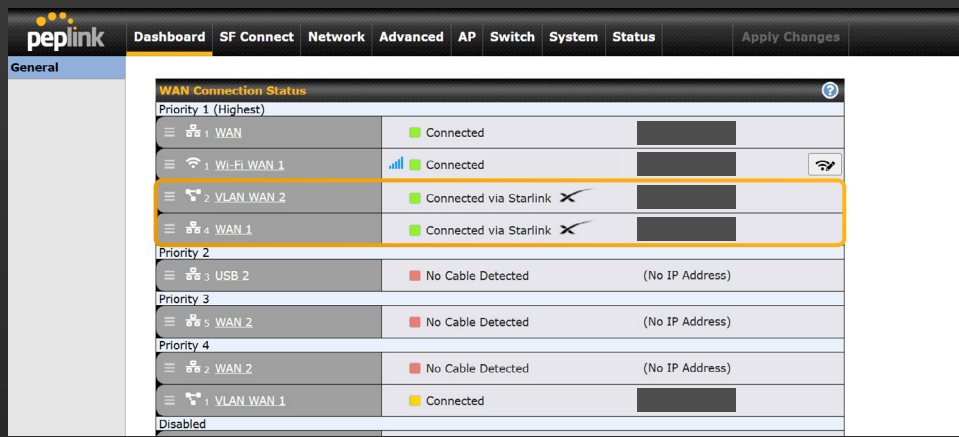
Verification and Testing

After completing configuration, verify that all components are functioning correctly before handing the deployment over to operations.

CHECK 1

Dashboard: All WANs Active

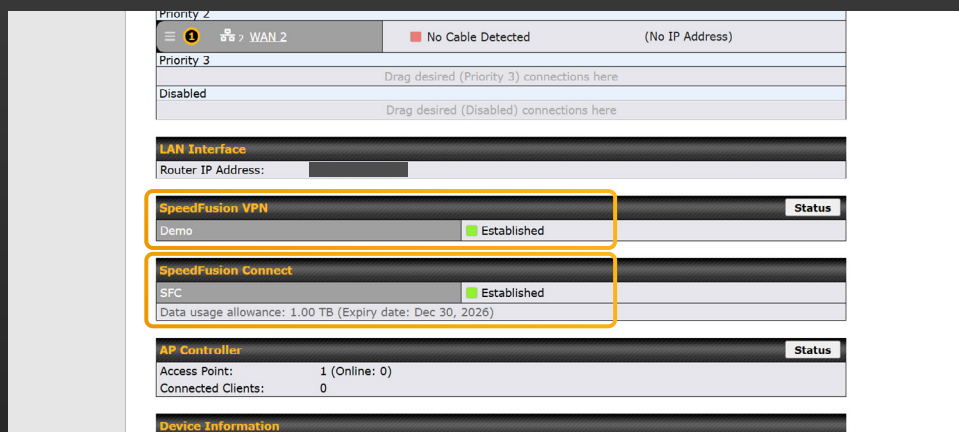
Navigate to **Dashboard**. Confirm every Starlink WAN shows a **green "Connected" status**. If any WAN shows red or amber, troubleshoot that connection before proceeding.



CHECK 2

SpeedFusion Status: Tunnel Established

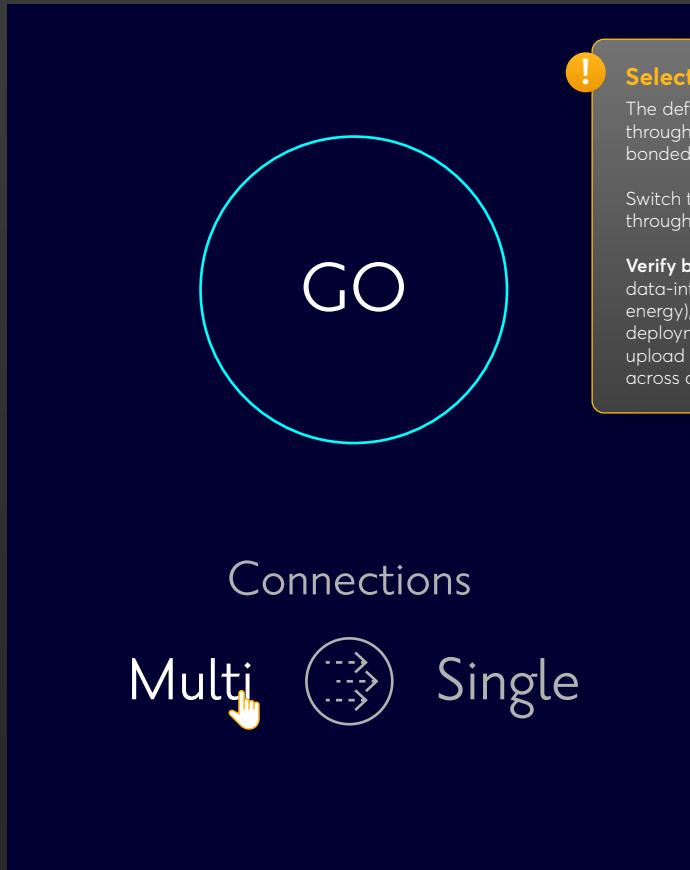
Navigate to **Dashboard > General**. Confirm that the tunnel shows a green status and all Starlink WANs are listed as active within the tunnel. SpeedFusion VPN refers to FusionHub. Note the reported bonded throughput capacity of SpeedFusion Connect.



CHECK 3

Speed Test: Use Multi-Connection Mode

Connect a test device to a LAN port on the Peplink router via CAT-6 Ethernet. Run a speed test at speedtest.net



Select "Multi" Connection Mode

The default "Single" connection test restricts throughput to a single WAN, which will not reflect bonded performance.

Switch to **"Multi"** connection mode to see aggregate throughput across all bonded Starlink connections.

Verify both download and upload. For data-intensive verticals (e.g. mining, research, energy), bonded upload throughput is often the deployment acceptance criteria. Confirm that upload results reflect the combined throughput across all units, not a single-unit upload speed.

CHECK 4

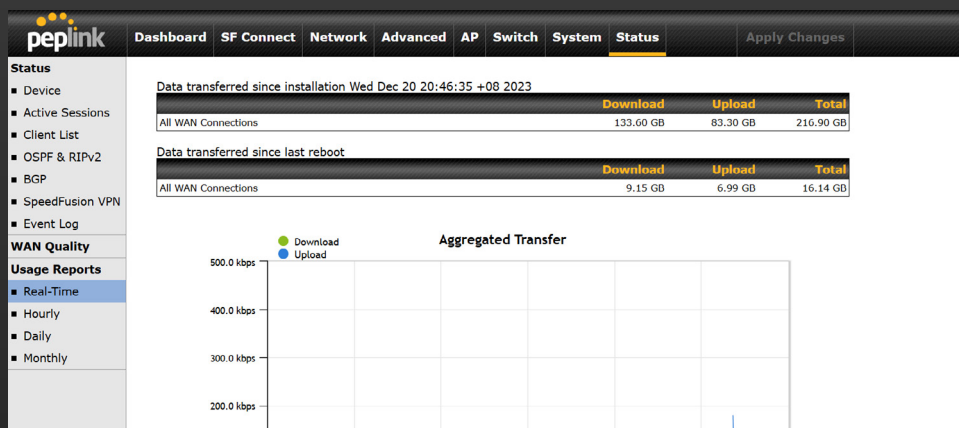
Real-Time Bandwidth Monitoring

Web Admin

InControl

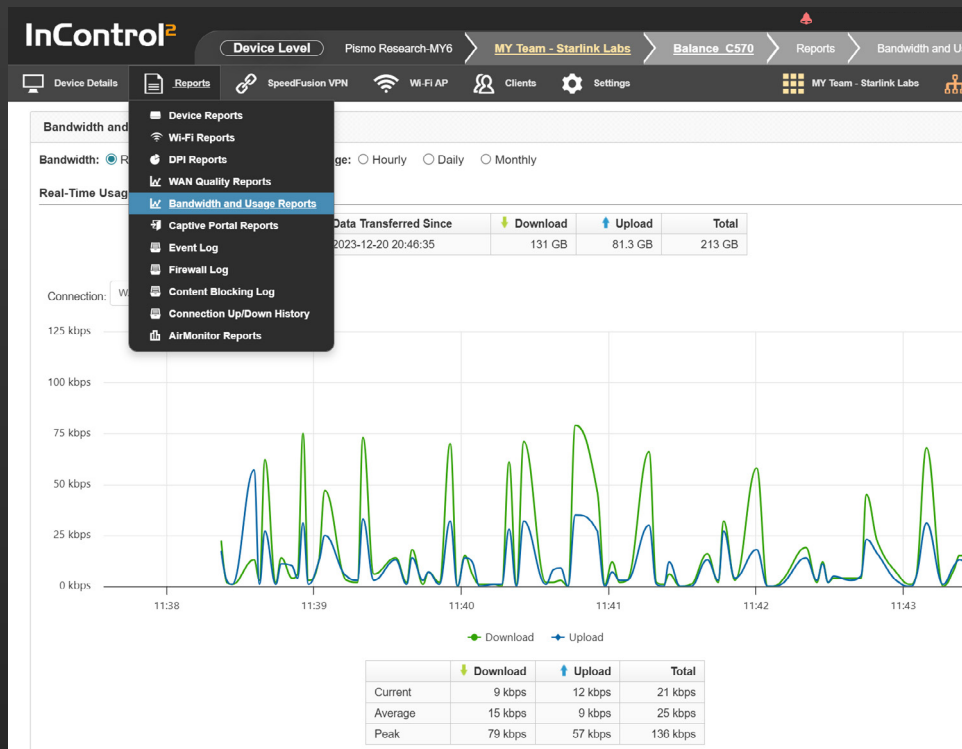
Web Admin

Navigate to **Status > Real-Time**. Confirm that traffic is distributed across all active Starlink WANs. Uneven distribution may indicate a health check or bonding configuration issue.



InControl

Select the router. Navigate to **Reports > Bandwidth and Usage Reports**. Confirm that traffic is distributed across all active Starlink WANs. Uneven distribution may indicate a health check or bonding configuration issue.



Optimization and Troubleshooting

Common issues and tuning recommendations for multi-Starlink bonded deployments.

SpeedFusion tunnel won't establish

Likely Cause: Starlink router not in bypass mode, causing double-NAT

Resolution: Verify bypass mode is enabled on every Starlink's router. Re-test tunnel after enabling.

Tunnel is established but throughput is slow

Likely Cause: MTU mismatch or exceeded router SpeedFusion throughput ceiling

Resolution: Confirm WAN MTU is set to 1500 (Starlink recommended) and SpeedFusion Boost is enabled. Verify the router's SpeedFusion throughput capacity is not the bottleneck (see [🔗 Hardware Sizing in the Starlink Solution Page](#)).

WAN flapping (frequent up/down)

Likely Cause: Health check settings modified from recommended values, or PING target is unreliable

Resolution: Confirm health check is set to PING, interval 10 seconds, retries 5, targeting 8.8.8.8 or 1.1.1.1. These values are optimized for satellite connections where SpeedFusion bonding handles brief interruptions transparently.

One WAN not carrying traffic

Likely Cause: WAN not selected in SpeedFusion profile

Resolution: Edit the SpeedFusion profile and confirm all Starlink WANs are checked.

Speed test shows single-link speed

Likely Cause: Speed test set to "Single" connection mode

Resolution: Switch to "Multi" connection mode on speedtest.net.

VoIP or video quality issues

Likely Cause: SpeedFusion Boost not enabled

Resolution: Enable SpeedFusion Boost in the SpeedFusion profile. Boost optimizes real-time traffic automatically and scales with the number of bonded units.



Keep Boost enabled at all times.

Use the split outbound policy (Step 4) to route non-critical traffic outside the tunnel if you need to maximize tunnel capacity for critical applications.

TUNING RECOMMENDATIONS

SpeedFusion Boost and Scaling

SpeedFusion Boost is either on or off. There are no levels to tune. When enabled, it optimizes all bonded traffic automatically.

Boost scales with the number of Starlinks in the deployment. Adding more increases both aggregate throughput and Boost effectiveness. If real-time application performance is not meeting expectations, adding another Starlink to the architecture is a more effective path than adjusting configuration settings.

TUNING RECOMMENDATIONS

Health Check Settings

The recommended PING health check settings (10 seconds, 5 retries) are optimized for multi-Starlink bonded deployments. PING targets should be reliable public services such as Google DNS (8.8.8.8) or Cloudflare DNS (1.1.1.1). These conservative values prevent the router from marking a WAN as down during brief interruptions that SpeedFusion bonding is already handling transparently at the packet level. With bonding active, a formally "down" WAN declaration matters less than it would on a single-WAN setup, so the slower detection (10s × 5 retries = 50 seconds) has minimal practical impact while eliminating unnecessary WAN flapping.

TUNING RECOMMENDATIONS

InControl Alerts

Configure alerts in InControl to notify your NOC when a WAN goes offline or when SpeedFusion tunnel status changes. Navigate to **InControl > [Device Group] > Settings > Notifications**. Set alerts for WAN disconnection and SpeedFusion tunnel down events.

Enabled ☒

Device Online / Offline ☐

All Devices Offline ☐

Device Starts Up ☐

HA Transitions ☐

WAN Up / Down ☒

Recipients
All group admins

Alert delay: 0 minutes

☐ Notify for priority 1 WANs only
(Require firmware 8.2 or above)

Starlink ☐

High System Temperature ☐

SpeedFusion Up / Down ☒

Recipients
All group admins

Alert delay: 0 minutes

Scaling with InControl

For deployments with multiple sites (e.g. fleet, multi-site operations, service provider networks), InControl enables centralized configuration management and monitoring.

CONFIGURE

Bulk Configuration

Remotely configure multiple Peplink devices at once through InControl. Apply settings across sites for various applications, ensuring consistent deployment while reducing manual setup time.

[!\[\]\(2c23357b2ce30e79d586a996e0cfa785_img.jpg\) Elevate Your Network Management: The Power of InControl](#)

MONITOR

GPS Services

Leverage built-in GPS capabilities in InControl to support tracking and location-based applications. Enable features such as Dead Reckoning, Geo-Fencing, Fleet Tracking, Map & Tag, and GPS Time Source, or forward GPS data to external systems for real-time visibility and control.

[!\[\]\(14909700a73c96358a74751a485059a6_img.jpg\) Exploring Peplink's GPS Capabilities](#)