Defense in Depth

Peplink Security White Paper

Version 2.0 - December 2021

www.peplink.com

Overview

1. Client Layer

The client layer covers devices that end users interact with directly, as well as APs that deliver Wi-Fi to such devices.

2. Router Layer

These features can also be virtualized on the cloud layer. Having them on both the cloud and the router makes it possible to secure local internet breakout as well as VPN traffic.

3. SD-WAN Layer

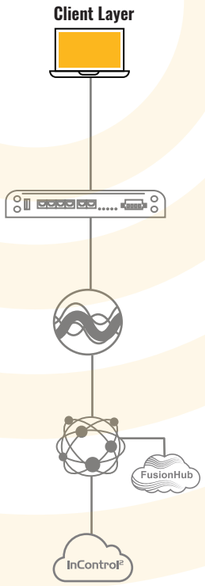
The SD-WAN layer covers the security of the data as it travels across WAN links. Peplink's patented SpeedFusion technology provides a significant advantage at this layer.

4. Cloud Layer

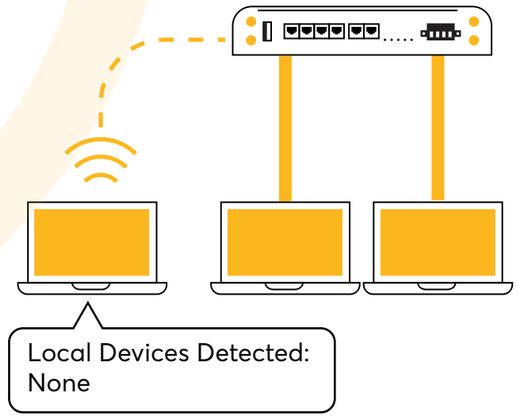
FusionHub can be installed on cloud services for cloud-based security. Combined with a Peplink router, it can secure both organizational VPN traffic and branch office internet breakout.

5. Administrative Layer

The human layer covers credentials used by an organization's team members. Countermeasures protect passwords and minimize the potential harm caused by a breach.

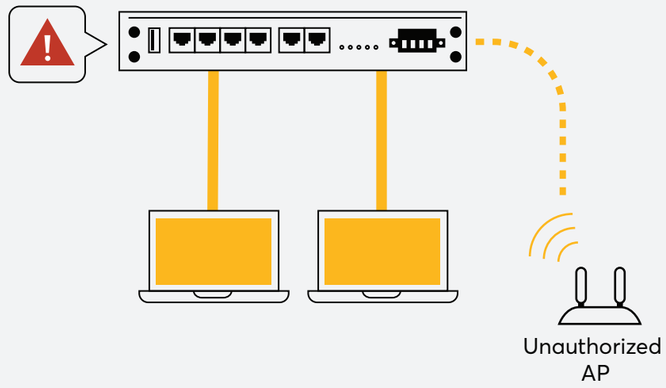


Guest Network Isolation



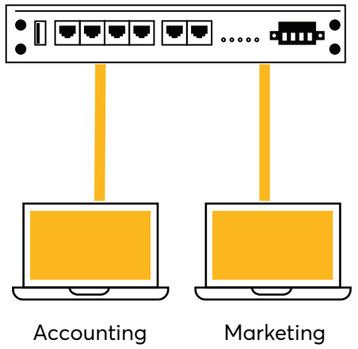
Peplink devices are capable of creating networks where guest users can only access the internet. This ensures complete isolation from any other devices connected to the router. Additionally, any devices on the guest network will be unable to access the router's WebUI.

Centralized VLAN Management



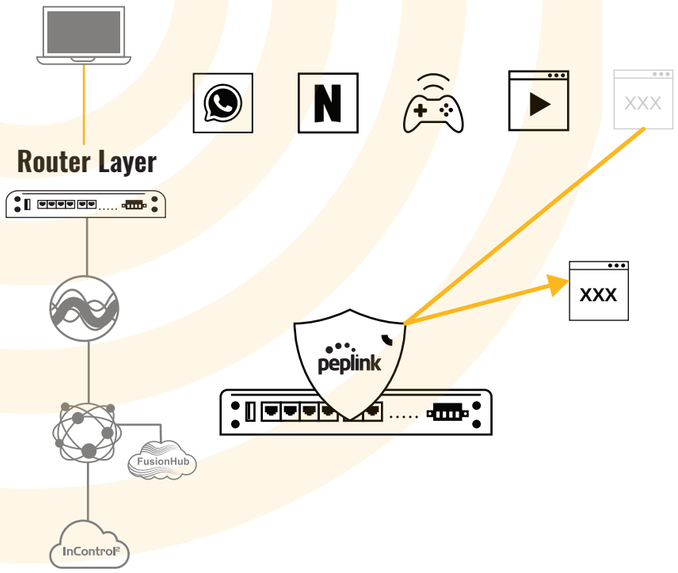
By isolating the local network, VLANs can significantly reduce the attack surfaces available to potential intruders. With InControl, you can centralize your VLAN policies across all devices at multiple locations.

Rogue AP Detection



Peplink routers can quickly identify any unauthorized APs that are connecting to your secure network, enabling prompt detection and removal.

Client Layer

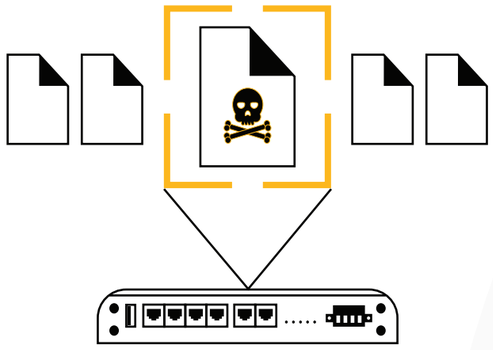


Web Blocking

Each Peplink router has a dynamically updated web-blocking tool that filters traffic into several categories. Users simply need to select the categories they wish to block, and the router will take care of the rest.

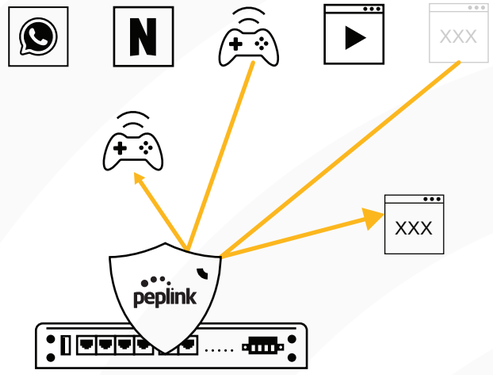
Intrusion Detection & DoS Protection

Each Peplink router has a built-in DoS protection feature. Once enabled, it can detect and block abnormal packets, as well as suspicious traffic typical of intrusion and denial-of-service attacks.



Security Patches

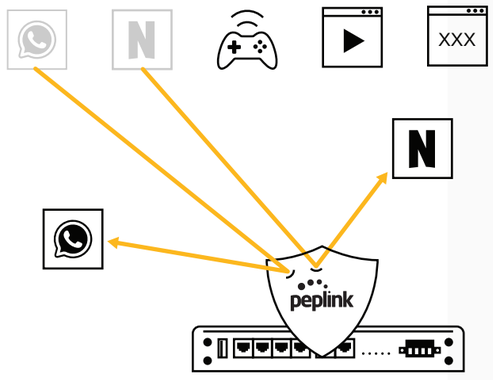
There are always new threats and vulnerabilities to be discovered. When one emerges, Peplink quickly develops and deploys new firmware to address the threats. We continue to update firmware for our products years after they have been launched.



Scalable Firewall & Outbound Policy

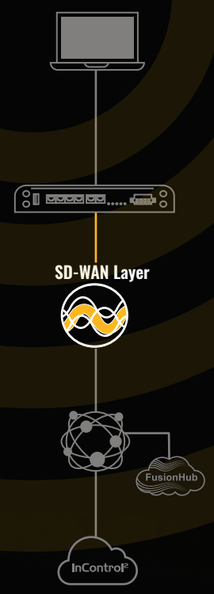
Outbound policies and firewall rules are only effective if they are usable. With Peplink gear, you can set firewall rules based on applications and even by country. With InControl, you can also centralize firewall rules and outbound policies for multiple devices.

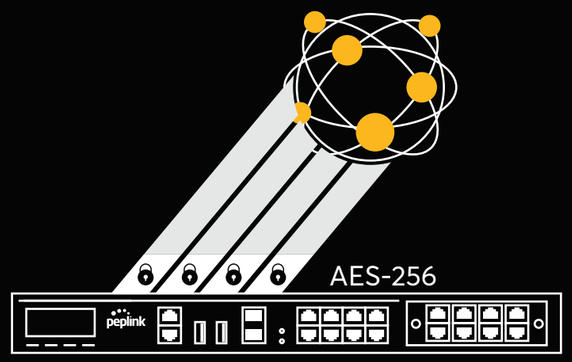
Router Layer



DPI Application Filtering

For applications that cannot be recognized by First Packet Inspection, there is Deep Packet Inspection. It allows you to block popular distractions such as streaming sites, social media platforms, and instant messengers.





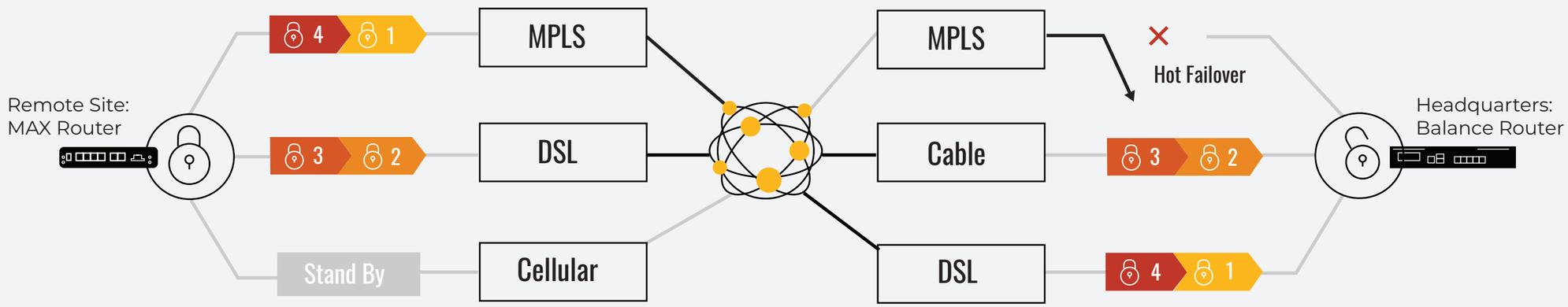
256-Bit AES Encryption

Each secure WAN-to-WAN link is established through a Diffie-Hellman key exchange, which produces randomly changing data encryption keys to protect data with a 256-bit AES cryptographic algorithm. A 256-bit AES encryption would take the world's fastest supercomputer millions of years to crack.

Packet Separation

Once the SpeedFusion tunnel is formed, sessions are broken down into packets and sent separately across available WAN-to-WAN connections. Because each connection is encrypted separately, potential hackers would need to obtain the key for every connection.

SD-WAN Layer



2 Packets are sent through each WAN link via the SpeedFusion tunnel.

3 VPN traffic can fail over in under 1 second, ensuring that session-persistent apps stay up.

4 3 2 1

Session

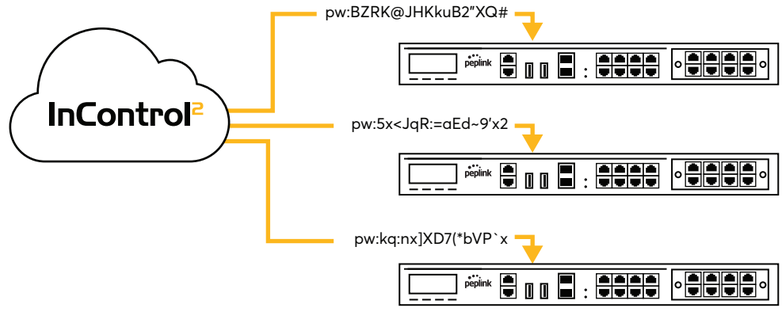
1 Each session is broken down into packets, and each packet is encrypted with 256-bit AES.

4 3 2 1

Session

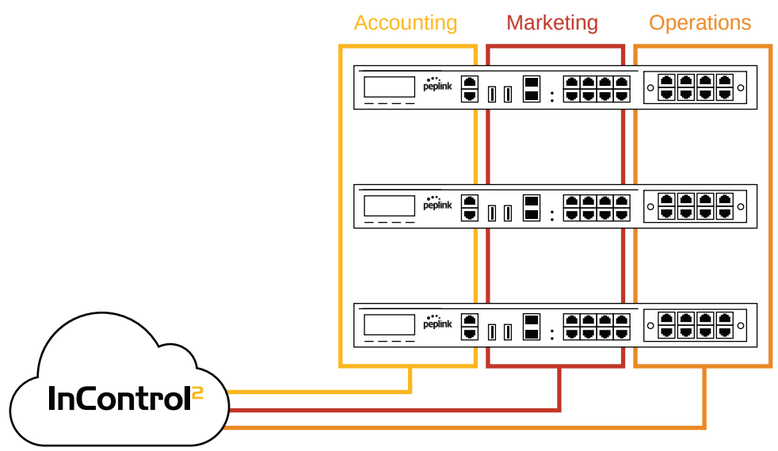
4 Packets are unencrypted and reassembled into the original sessions.

Admin Password Management

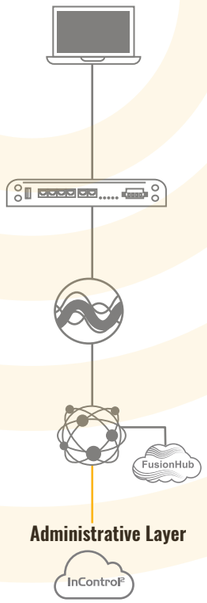


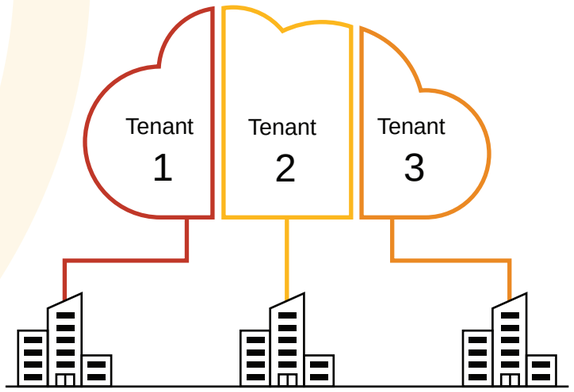
Separating your network into different trust boundaries minimizes the damage caused by compromised credentials. Use VLANs to separate networks for different teams, each with a separate login gateway. Use InControl to set up different access levels for each administrator.

Trust Boundary Management



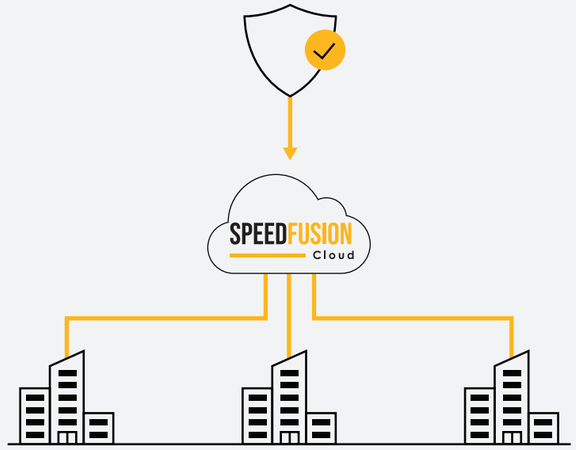
One of a router's simplest attack vectors is the admin password. With InControl, you can change the admin password for multiple devices at the same time. Doing so at regular intervals will significantly increase the network's level of security.





Tenant Segmentation

Our cloud appliance supports VRF, which divides the appliance into groups and maintains a separate routing table for each group. The result: one cloud appliance can host several tenants, each completely isolated from the others.

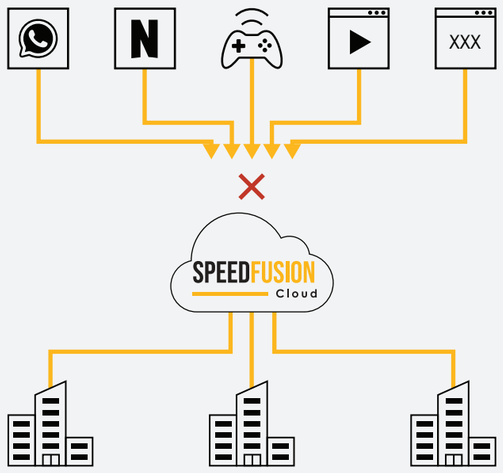


Security Patches

When vulnerabilities appear, we swiftly develop patches and make them available to our users. These patches are provided through our cloud services as well as our routers, securing your entire network.

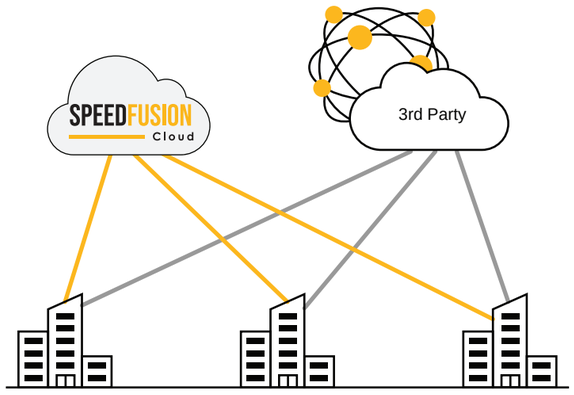
Administrative Layer

InControl²



Comprehensive Traffic Security

Use web blocking, firewall, outbound policies, DPI, and application filtering to control the type of traffic that can access your network. Protect your entire network with Intrusion Detection and DoS Protection. Any security feature available on our routers can also be applied to the cloud.



3rd-Party Security Integration

Works seamlessly with your 3rd-party cloud-based security solution. Secure organizational traffic with our security features, and protect public internet traffic with the 3rd-party solution of your choice using IPsec or OpenVPN.