

# Defense in Depth

Peplink Security White Paper

Version 2.0 - December 2021



[www.peplink.com](http://www.peplink.com)

# Overview



## 1. Client Layer

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

## 2. Router Layer

These features can also be virtualized on the cloud layer. Having them both on the cloud and on 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 on this layer.

## 4. Cloud Layer

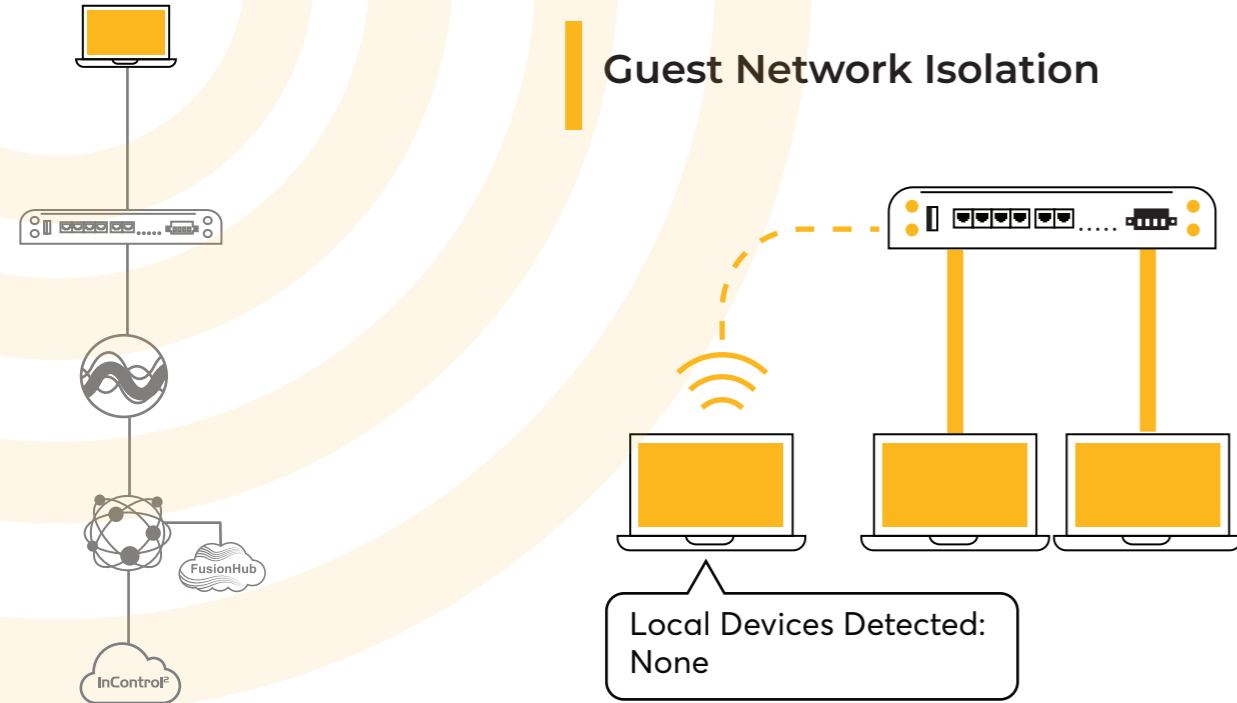
FusionHub can be installed on cloud services for cloud-based security. Combined with a Peplink router, and you can secure both organizational VPN traffic as well as branch office Internet breakout.

## 5. Administrative Layer

The human layer covers credentials that are carried by an organization's team members. Countermeasures protect passwords and minimize the potential harm done by a breach.

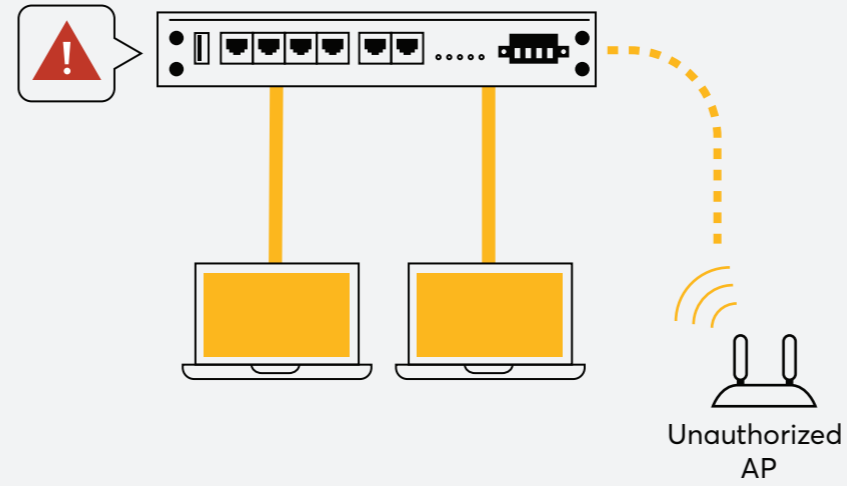
Client Layer

### Guest Network Isolation



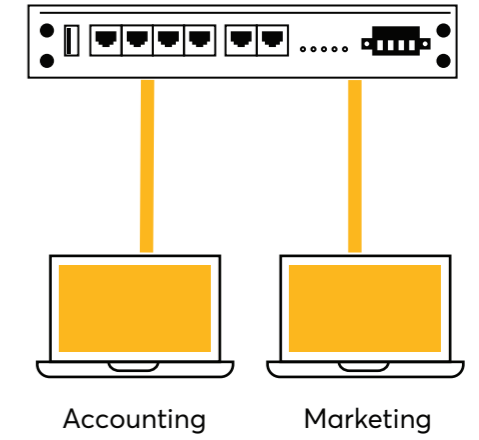
Peplink devices are capable of creating networks where guest users can only see the Internet. This means complete isolation from any other devices connected to the router. Also, any devices on the great network will be unable to access the router's WebUI.

### Centralized VLAN Management



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

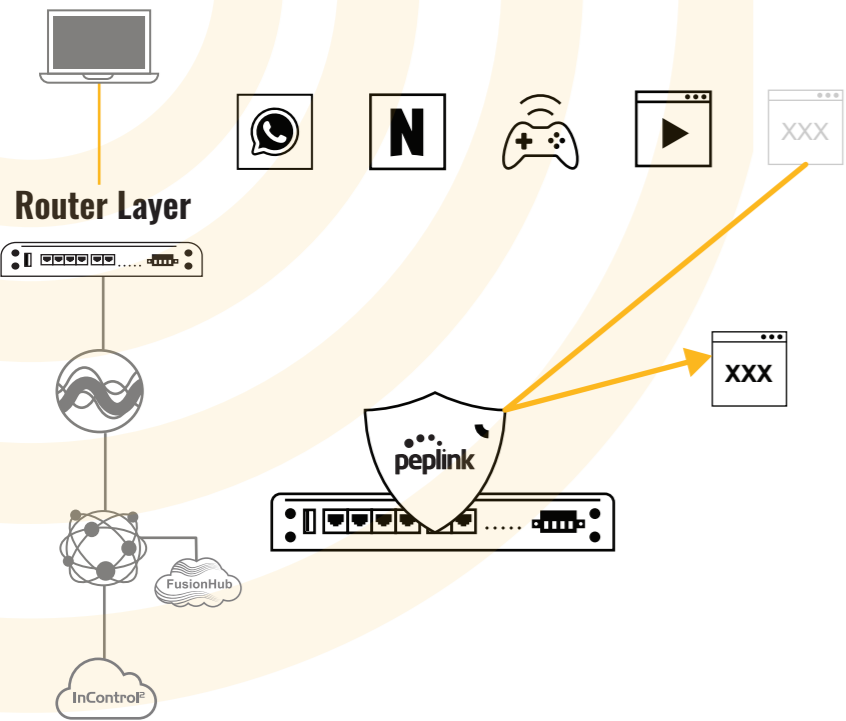
### Rogue AP Detection



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

Client Layer





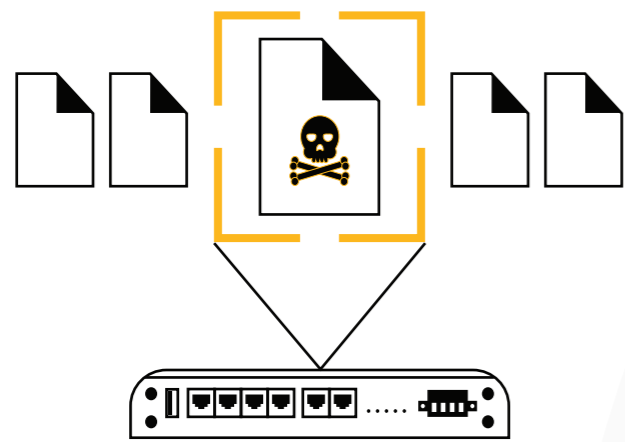
### Web Blocking

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



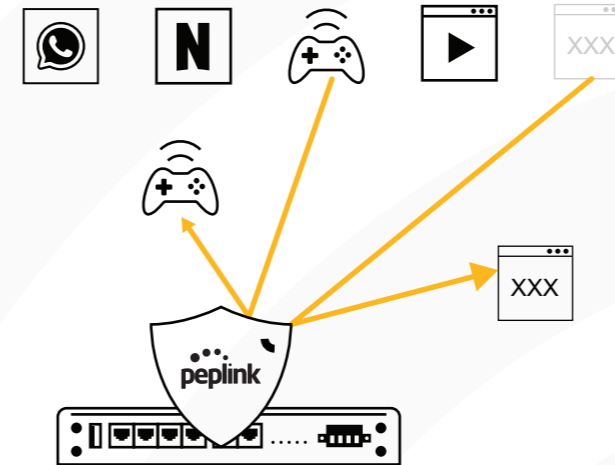
### Intrusion Detection & DoS Protection

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.



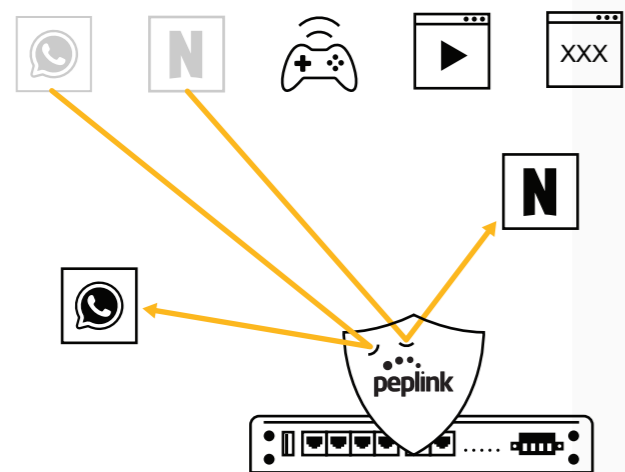
### Security Patches

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



### Scalable Firewall & Outbound Policy

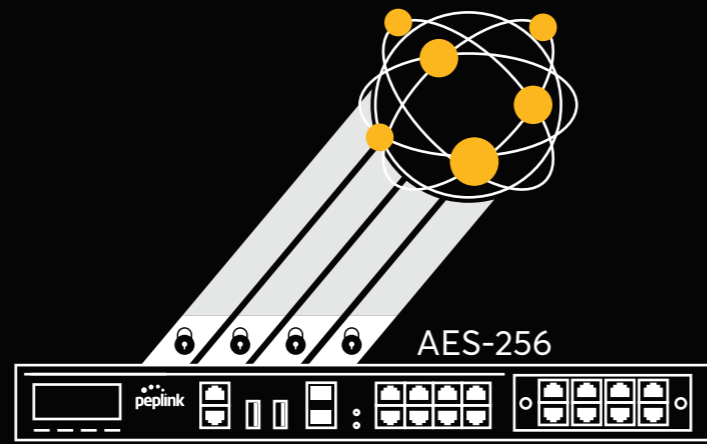
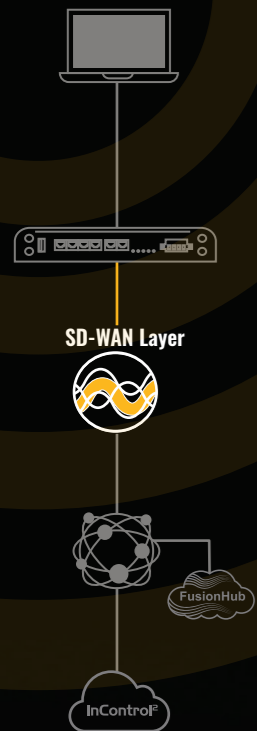
Outbound policy and firewall rules are only effective if they are usable. With Peplink gear, you can set firewall rules based on application and even by country. With InControl, you can also centralize firewall rules and outbound policies for multiple devices.



### DPI Application Filtering

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





## 256-Bit AES Encryption

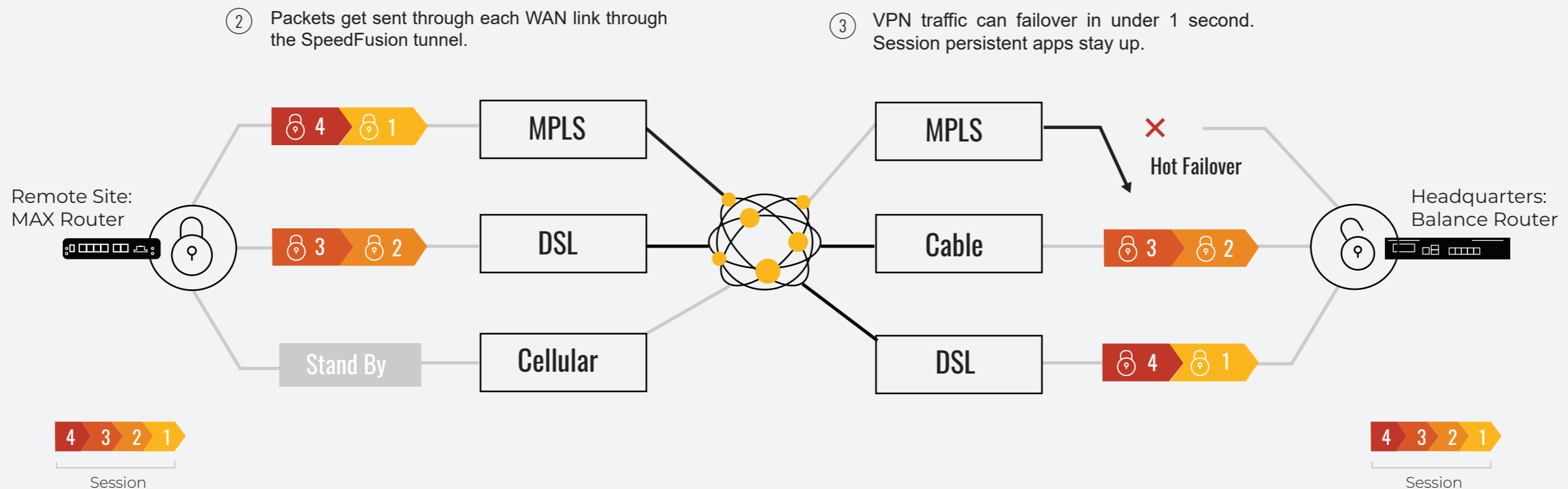
Each secure WAN-to-WAN link is established through a Diffie-Hellman key exchange. This produces randomly changing data encryption keys to protect data with a 256-bit AES cryptographic algorithm. 256-bit AES would take the world's fastest supercomputer millions of year to crack.



## Packet Separation

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

SD-WAN Layer



① Each session gets broken down into packets. Each packet gets 256-bit AES encryption.

② Packets get sent through each WAN link through the SpeedFusion tunnel.

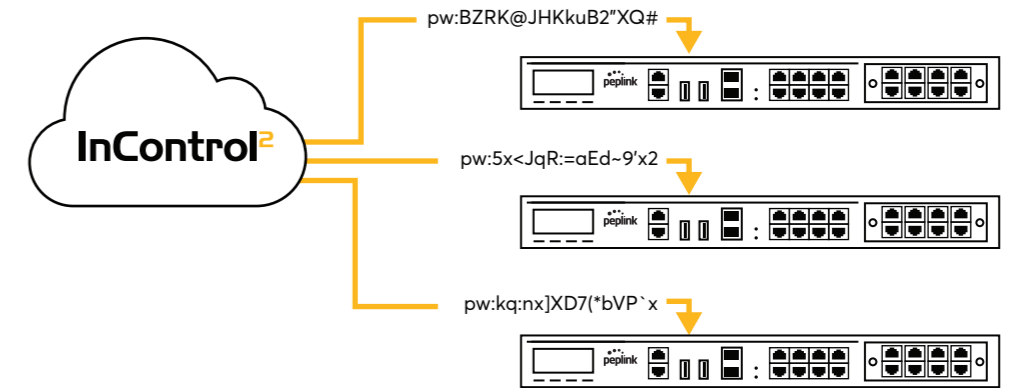
③ VPN traffic can failover in under 1 second. Session persistent apps stay up.

④ Packets get unencrypted and reassembled into the original sessions.



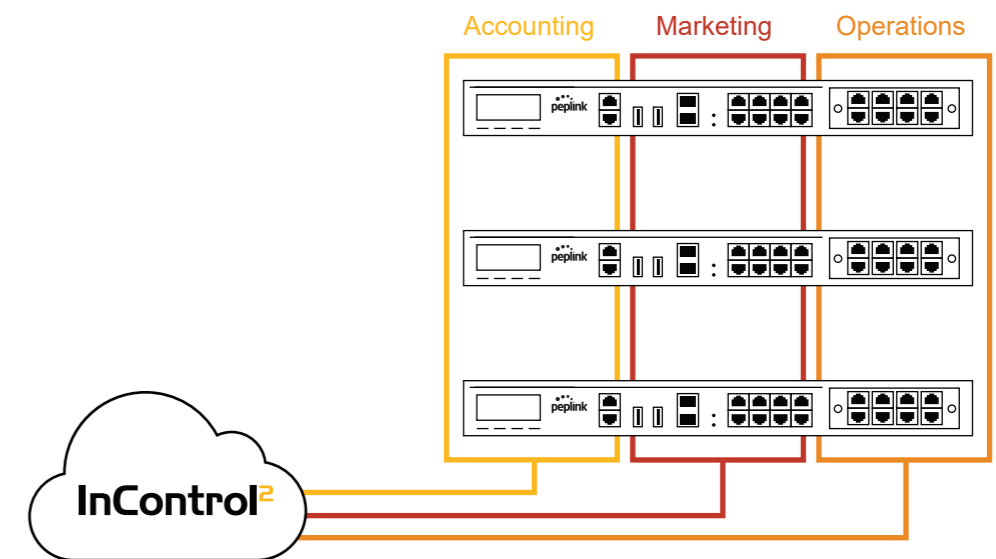
Cloud Layer

## Admin Password Management

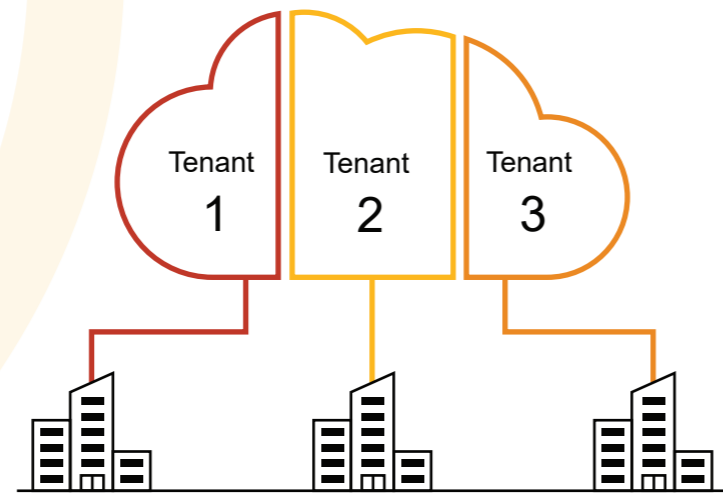
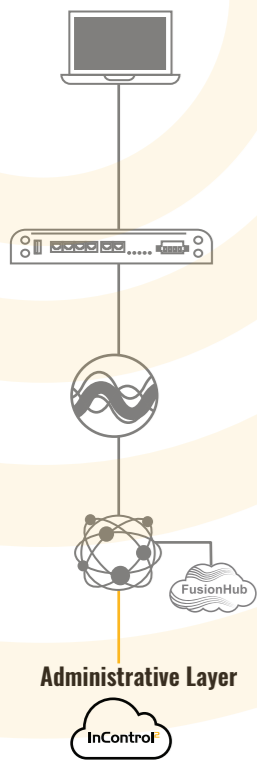


Separating your network into different trust boundaries will minimize the damage caused by a compromised credential. Use VLANs to separate the networks for different teams, each with a separate login gateway. Use InControl to set up different access levels for each administrator.

## Trust Boundary Management

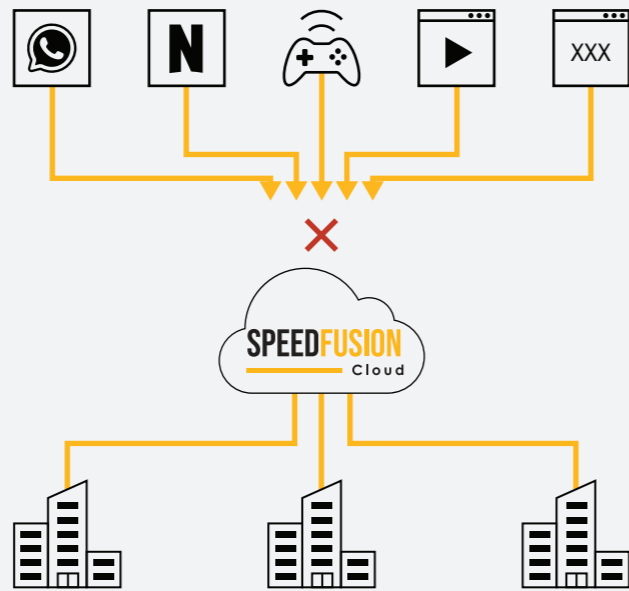


One of a router's simplest attack vectors is the admin password. With InControl, you can change the admin password for multiple devices at the same time. Doing so at regular intervals will significantly increase the network's level of security.



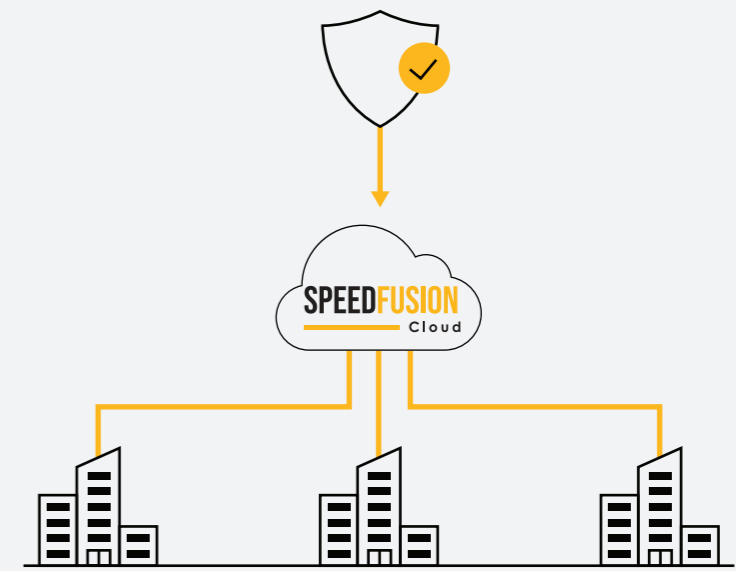
### Tenant Segmentation

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



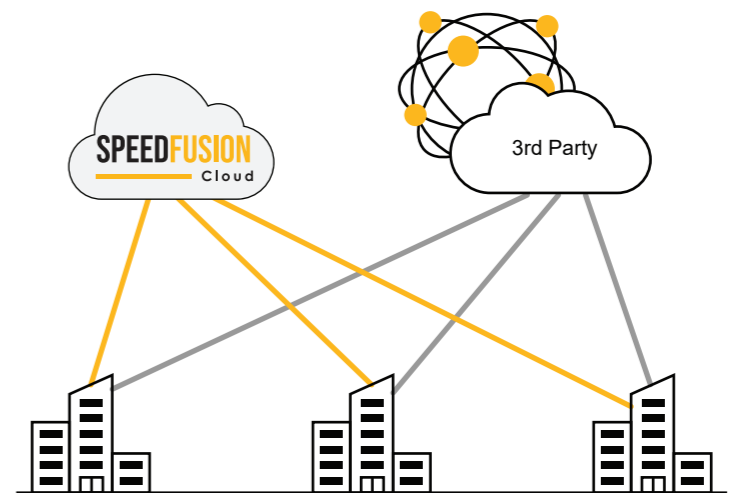
### Comprehensive Traffic Security

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



### Security Patches

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



### 3rd-Party Security Integration

Works together with your 3rd-party cloud-based security solution. Secure organization traffic with our security features, and secure public Internet traffic with the 3rd-party solution of your choice using IPsec or OpenVPN.