Cisco IOS Firewall Common Deployment Scenarios

http://www.cisco.com/go/iosfirewall

Cisco IOS Firewall

Feature Overview

Stateful firewall: Full Layer 3 through 7 deep packet inspection

Flexible embedded application layer gateway (ALG): Dynamic protocol and application engines for seamless granular control

Application inspection and control (AIC): Visibility into both control and data channels to help ensure protocol and application conformance

Virtual firewall: Separation between virtual contexts, addressing overlapping IP addresses

Transparent (Layer 2) firewall: Deploy in existing network without changing the statically defined IP addresses

Intuitive GUI management: Easy policy setup and refinement with CCP and CSM

Resiliency: High availability for users and applications with stateful firewall failover

Interfaces: Most WAN and LAN interfaces

Selected List of Recognized Protocols

- HTTP, HTTPS, and JAVA
- E-mail: POP, SMTP, ESMTP, IMAP
- P2P and IM (AIM, MSN, and Yahoo!)
- FTP, TFTP, and Telnet
- Voice: H.323, SIP, and SCCP
- Database: Oracle, SQL, and MYSQL
- Citrix: ICA and CitrixImaClient
- Multimedia: Apple and RealAudio
- IPSec VPN: GDOI and ISAKMP
- Microsoft: MSSQL and NetBIOS
- Tunneling: L2TP and PPTP

Cisco IOS Firewall

Common Deployments Scenarios

- **Internal firewall: branch or small office**

  Example: Retail outlet

  IOS Firewall segments the network for compliance requirements in transparent or routed environments, wireless to wired segments

- **Internet connected location: branch or small office**

  Example: Retail store with wi-fi hotspot

  IOS Firewall separates VPN traffic to corporate headquarters and Internet traffic

- **Virtual firewall: location with co-located partners**

  Example: retail location with co-located photo kiosk or pharmacy

  IOS Firewall supports partners' overlapping IP addresses and secures the shared WAN connection between business partners

- **Transparent firewall: large to medium sized branch office**

  Example: branch office with many existing network nodes

  IOS Firewall provides network protection without disrupting the existing network scheme

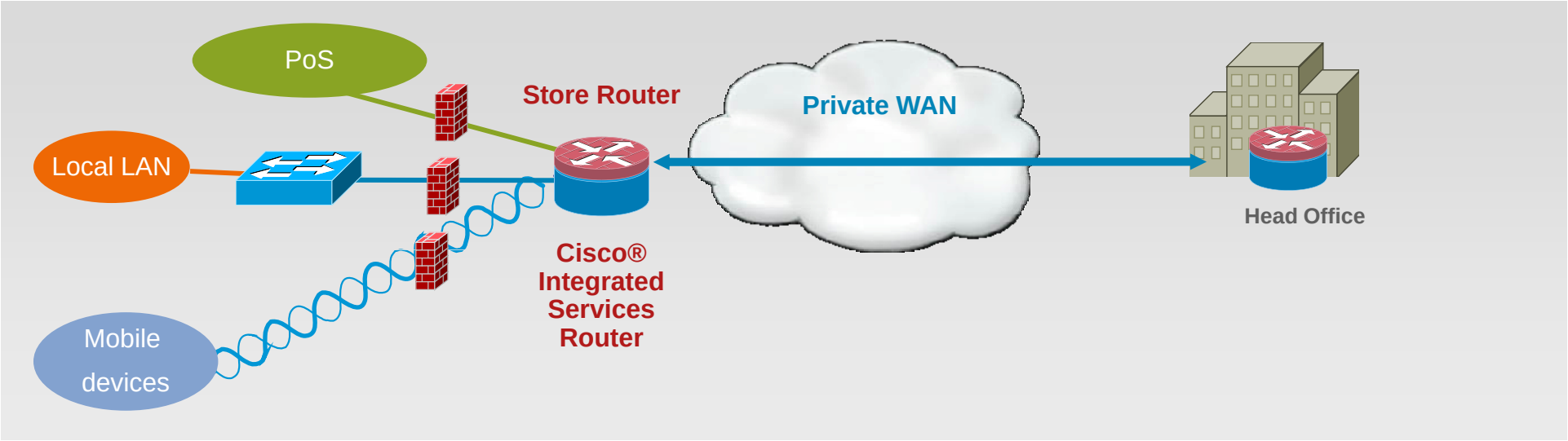
- **Securing Unified Communications: branch location with unified communications**

  Example: any branch office with Voice over IP

  IOS Firewall enables trusted media control and helps to prevent impersonation attacks

Cisco IOS Firewall Deployment Scenario 1

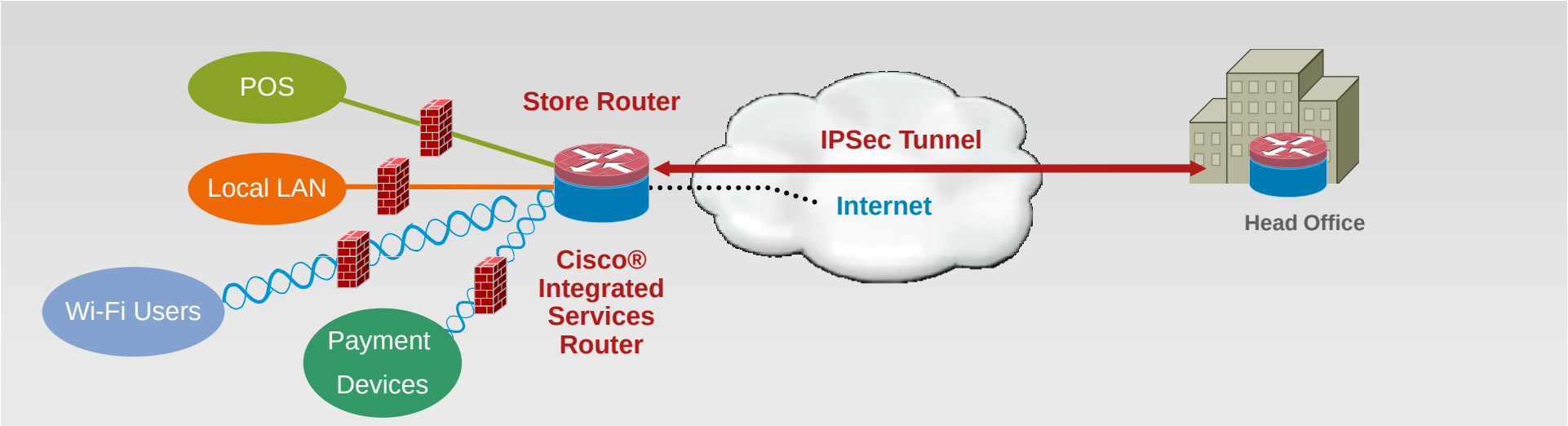
Retail Outlet



- PCI compliance requires firewalling of Point-of-Sale systems, wired and wireless network segments
- Cisco IOS Firewall creates separate security zones for Point-of-Sale (Server/Electronic Cash register), LAN and wireless LAN network segments
- Cisco has its retail design guide certified through a third party (CyberTrust)

Cisco IOS Firewall Deployment Scenario 2

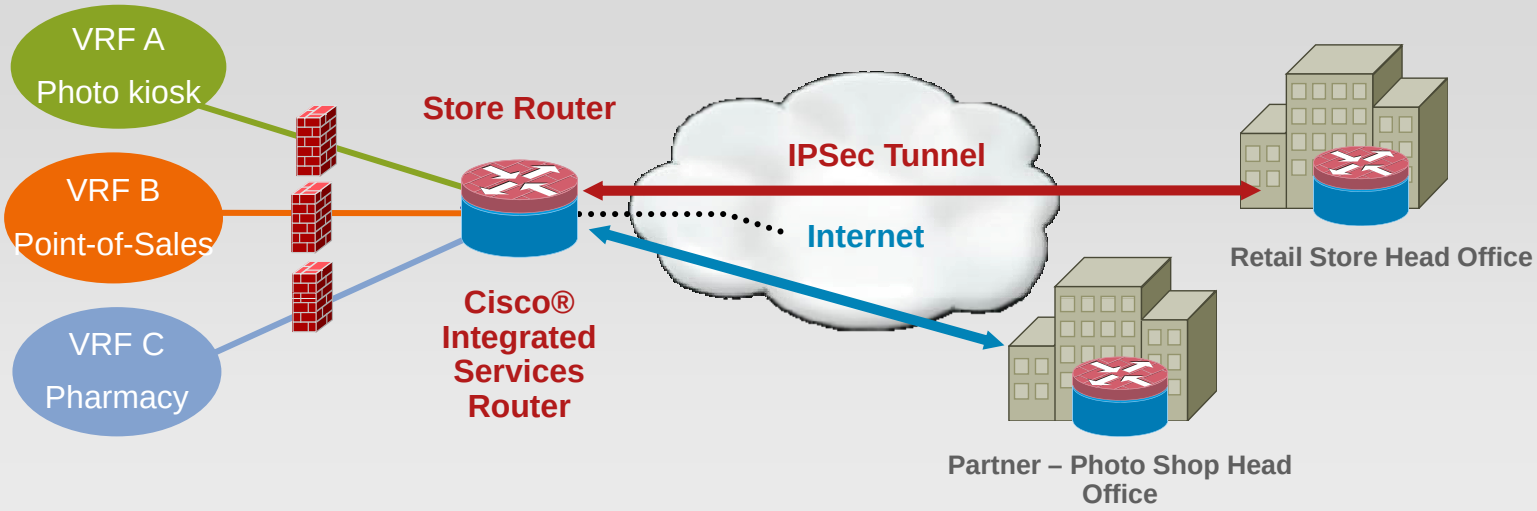
Retail Outlet with Internet Hotspot



- Internet Hotspot (Wi-Fi) services opens the network to additional risk
- Cisco IOS Firewall creates separate security zones for Point of Sale (Server/Electronic Cash register), LAN and wireless LAN
- Firewall policies segregate and protect the corporate vlans and the Internet Wi-Fi vlans

Cisco IOS Firewall Deployment Scenario 3

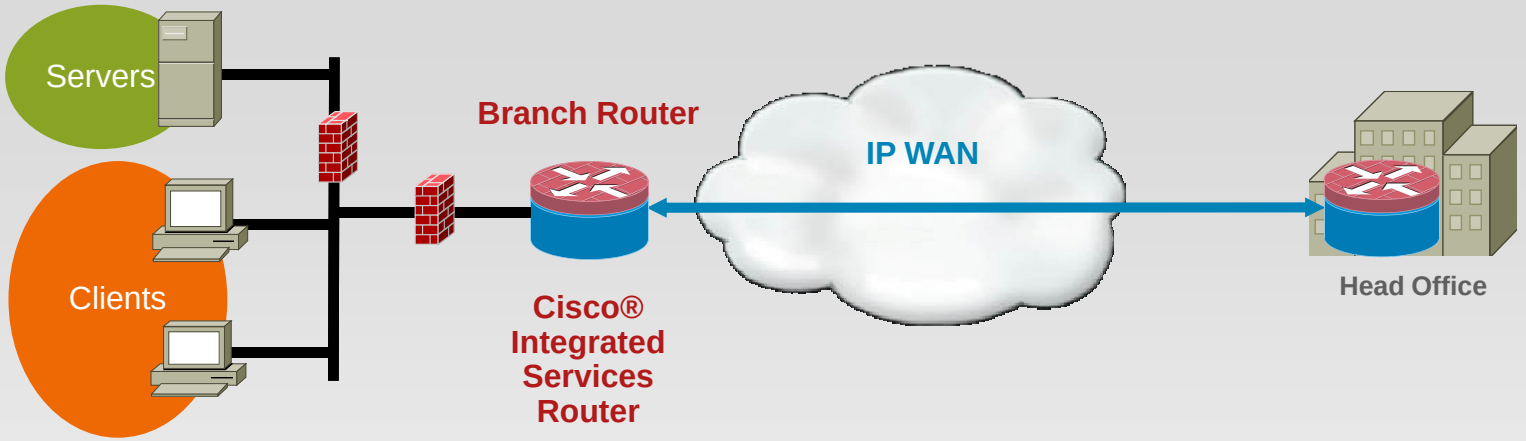
Virtual Firewall (VRF-aware Firewall)



- Cisco IOS Firewall separates network segments and supports overlapping address space in environments where partners share the same physical location
- Each virtual firewall helps secure a partner's Internet access and isolates risk factors such as a photo kiosk with media card slots
- PCI compliance requires retail stores to firewall wired and wireless network segments as well as Point-of-Sales (PoS) segments

Cisco IOS Firewall Deployment Scenario 4

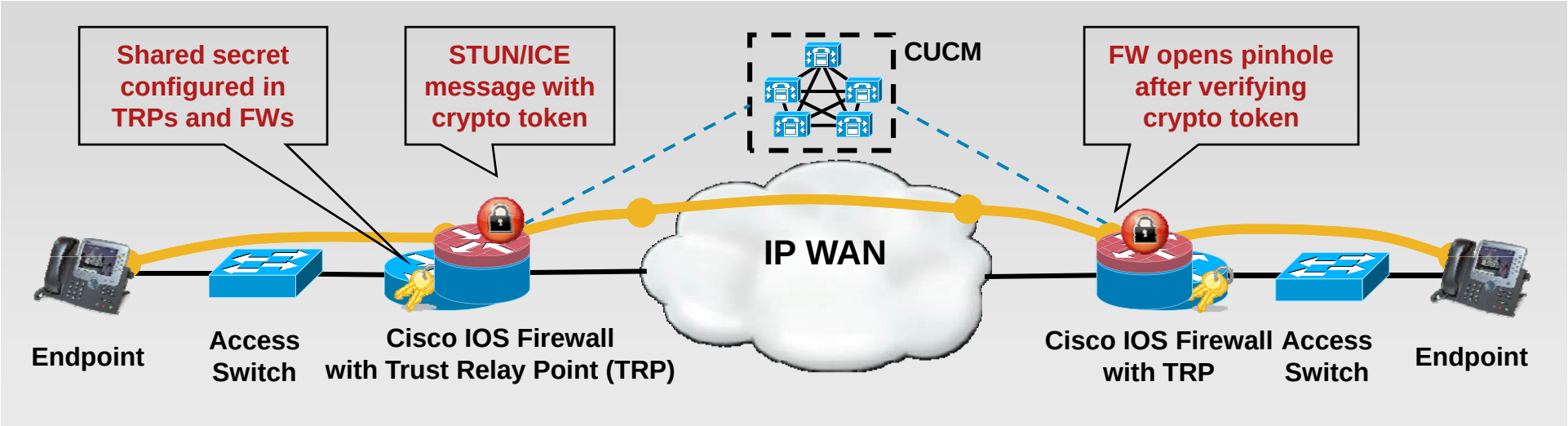
Transparent Firewall



- The Transparent Cisco IOS Firewall feature allows users to "drop" a Cisco IOS Firewall in front of their existing network without changing the statically defined IP addresses of their network-connected devices
- The tedious and costly overhead that is required to renumber devices on the trusted network is eliminated

Cisco IOS Firewall Deployment Scenario 5

Unified Communications Trusted Firewall



- Cisco IOS Firewall enables trusted media control and helps to prevent impersonation attacks
- Trusted Firewall authenticates/authorizes calls to ensure pinholes are only opened for legitimate calls
- Trusted Firewall is voice protocol version independent and it secures
  - encrypted signaling paths
  - asymmetric signaling and media paths

Cisco IOS Firewall
Summary

Cisco IOS Firewall

- Helps meet PCI requirements by segmenting and protecting Point of Sale systems
- Segregates and defends corporate networks from Wi-Fi hotspots connected to the Internet
- Supports overlapping address space in environments where partners share the same physical location
- Provides network protection without disrupting the existing network scheme
- Secures Unified Communications