Cisco VPN Solutions

Easily use a Cisco VPN built into your router to:

- Securely connect enterprise branches and headquarters
- Give mobile workers secure access to your corporate network
- Run robust authentication that helps prevent man-in-the-middle attacks
- Comply with industry-specific data security mandates
- Add encryption and mutual authentication to your WAN link
- Protect sensitive Internet of Things (IoT) data in transit
- Secure data moving between data center sites

Protect Your Data in Transit with a Cisco VPN

Your branch offices and mobile workers need secure access to your corporate network 24 hours a day. You can safeguard their WAN connections and data using a secure virtual private network (VPN) solution built right into your Cisco® router.

A "secure" VPN is one that authenticates endpoints and encrypts data in transit. VPN helps thwart man-in-the-middle attacks, where a third party tries to intercept and steal or modify valuable data.

There are different types of secure VPN solutions, each using underlying technologies appropriate for certain network deployments. Cisco routers running Cisco IOS® Software or Cisco IOS XE Software support the industry's most robust array of VPN solutions. The VPNs are embedded directly in Cisco Integrated Services Routers (ISRs) for branch offices, Cisco Aggregation Services Routers (ASR 1000 Series) for data centers and other head-end locations, and Cisco Cloud Services Routers (CSR 1000V Series) for extending your WAN to off-premises cloud services.

Diverse Needs, Diverse VPN Solutions

How do you know what type of VPN you need? Table 1 shows the primary use cases that can be addressed by Cisco VPN solutions.

Cisco VPN solutions provide exceptional security through encryption and authentication technologies that protect data in transit from unauthorized access and attacks. A Cisco VPN helps you:

- Deliver highly secure communication, with access rights tailored to individual users
- Quickly add new sites or users with minimal configuration overhead
- Increase your data and network reliability by securing your corporate network
- Reduce WAN costs by using lower-cost Internet links that you can secure

Table 1. Applying Cisco Router-Based VPNs to Your Network

What to Secure	Recommended Cisco VPN Solution	Description
Internet or private WAN connections for cloud access and for direct communication among multiple corporate sites	Cisco Dynamic Multipoint VPN (DMVPN)	Creates private tunnels to connect to the headquarters and/or cloud and to interconnect multiple sites on demand. Offers the option to encrypt the tunnels using IPsec.
Your private WAN or Multiprotocol Label Switching (MPLS) VPN service	Cisco Group Encrypted Transport (GET) VPN	Encrypts data for secure “any-to-any” (mesh topology) transmissions.
Telecommuters and workers on the go	Cisco Secure Socket Layer VPN (SSL VPN)	Encrypts individual user connections to the corporate network with TLS-based tunnels using the Cisco AnyConnect® client running on mobile or desktop devices.
Access connections from remote sites and IoT sensor data in transit	Cisco FlexVPN	Encrypts connections from remote users or sites to the corporate network using IPsec-based tunnels.

If your network design calls for more than one type of VPN solution, you can simply turn on what you need in your Cisco IOS or IOS XE router. You can easily manage multiple Cisco VPN solutions using the Cisco Prime™ Infrastructure unified management application.

Next Steps

To learn more about Cisco VPN solutions, contact your Cisco sales rep and visit www.cisco.com/go/routervpn.