

## At-A-Glance

### What is Cisco® Secure WAN?

Cisco Secure WAN is a program that helps you take advantage of Cisco router security features with your initial router purchase. The program:

- Saves you money by providing comprehensive, affordable protection in a single network device.
- Provides bundled features at substantial discounts.
- Offers compelling return on investment (ROI), allowing you to add security upfront.
- Helps future-proof your router purchases with security-ready and voice-ready implementations.

### Cisco Secure WAN Overview

Networks today run mission-critical business services that need protection from external and internal threats. Cisco Secure WAN bundles add valuable security functions in a simple, manageable, single-box solution to your Cisco router—for considerably less cost and effort than adding these features later.

### What is a Cisco Secure WAN Bundle?

A Cisco Secure WAN bundle is a Cisco IOS® security image that you purchase in conjunction with routers. It may also be an add-on for a previously deployed Cisco router. A Cisco Secure WAN bundle includes:

- A stateful firewall
- Site-to-site VPN (Dynamic Multipoint VPN [DMVPN], Easy VPN, IPSec generic routing encapsulation [GRE])
- Remote-access VPN (Easy VPN, SSL VPN)
- Intrusion prevention system (IPS)
- URL filtering
- WAN (and dynamic) routing
- Network Admission Control (NAC)
- Cisco Router and Security Device Manager (SDM)
- Added memory (when needed)

There are four Cisco Secure WAN bundles for Cisco integrated services routers: Baseline Security for basic security, High Performance for added performance and growth, Secure Voice for combined security and IP Communications, and Secure Wireless for integrated security and wireless LAN access

### How do Cisco Secure WAN Bundles Benefit my Company?

#### Cisco Secure WAN bundles:

- Increase protection against network security threats by helping to ensure that branch offices are as secure as a headquarter location.
- Provide comprehensive, affordable protection in a single device that can be managed centrally, for reduced cost of ownership.
- Enable you to take advantage of VPNs, one of the fastest-growing forms of networking that can help you save money and increase productivity.
- Maximize ROI by greatly increasing the capabilities of your Cisco router, including VPN, firewall, IPS, URL filtering, secure WAN routing or secure infrastructure for voice.
- Simplify branch security—secure WANs are the easiest, most cost-effective way to implement comprehensive branch security.
- Facilitate compliance with data and network privacy laws such as Sarbanes-Oxley, Gramm-Leach-Bliley Act, HIPAA, and The Personal Information Protection and Electronic Documents Act.

### What Issues Should I Consider in my Decision to Purchase a Secure WAN Bundle for my Cisco Router?

#### A. Secure Connectivity

##### Are you considering migrating to VPNs?

Many companies are migrating from leased lines or Frame Relay for cost savings and increased performance. They often see a 100-percent ROI within a year. As a backup link, VPN over DSL is cheaper and quicker to deploy than ISDN, and is faster and more reliable. Many companies also use VPNs within their LANs to add encryption protection between segments, buildings, or groups where information security and uptime are critical.

##### Are you facing challenges complying with information privacy legislation?

Healthcare, finance, retail, and government sectors are now required by law to encrypt data. In order to comply, companies must use authentication standards and solutions (such as NAC and 802.1x) and auditing practices, and are advised to encrypt over their existing WANs. More industries are affected every year by federal and state legislation. Adding these capabilities with initial router purchases will make it easier and far less expensive than adding the required security tomorrow.

##### Are you planning to offer secure remote access to employees or partners?

Many companies have sales staff and telecommuters that need remote access to networked applications (e-mail, sales tools, shared folders, etc.). Some organizations have outsourced staffs or remote partners that need limited and secured network access. Cisco Secure WAN bundles are an ideal solution for these applications.

#### B. Data and Identity Protection

##### Do you need protection against worms, viruses, and Trojans?

Most of today's worms and viruses use the network to spread throughout an organization. With a Cisco Secure WAN bundle, your network can drop malicious traffic at the perimeter and contain the spread of infections.

##### Are you concerned with unauthorized access and the security posture of laptops and PCs connecting to your network?

Cisco integrated services routers are the fundamental component of the Cisco Network Admissions Control (NAC) Framework. Cisco NAC allows IT administrators to centrally control the admission policy for laptops and PCs, including guest systems.

##### Have you integrated Internet use policy and Web filtering into your network, from headquarters out to your branch offices?

URL filtering is one way to implement and enforce an Internet usage policy—it helps protect an organization from possible legal issues. Cisco Secure WAN bundles offer URL filtering within Cisco IOS Software. Adding a Cisco Content Engine Network Module to an integrated services router increases URL filtering capabilities.

##### What is your current overall security architecture, from headquarters out to your branch offices?

An initial understanding of the differences between how you have secured headquarters and branch office locations will help you identify needs in both areas—needs that can be met with Cisco integrated services routers.

##### Are your remote offices as secure as your headquarters?

Security threats at the WAN level may quickly spread to your LAN. You need an in-depth defense policy at all network locations to prevent worm and virus outbreaks, distributed denial of service (DDoS) attacks, and unauthorized traffic.

#### C. Secure Voice and Wireless

##### Are you looking to reduce costs by combining your voice and data services onto one secure network?

A secure network is the foundation for a secure Cisco IP Communications infrastructure. If you have plans to implement Voice over IP (VoIP), it is cost-effective to build a network that securely implements voice- and video-enabled VPN (V3PN) and Secure Real-Time Transport Protocol (SRTP).

##### Are you considering IP Communications applications at your campus or branch office?

Many businesses are implementing IP Communications solutions for improved employee productivity and significantly reduced operational costs.

## At-A-Glance

**Table 1.** Cisco Secure WAN Bundle Overview

	Baseline Security Bundles	High Performance Bundles	Secure Voice Bundles	Secure Wireless Bundles
<b>Secure Connectivity</b>				
Site-to-Site VPN	X	X	X	X
Remote-Access VPN	X	X	X	X
High-Performance VPN		X	X	
<b>Data and Identity Protection</b>				
Perimeter Defense	X	X	X	X
Outbreak Prevention	X	X	X	X
NAC	X	X	X	X
<b>Voice and Wireless</b>				
Voice Gateway, Cisco CallManager Express			X	
Wireless				X
<b>Business Continuity</b>				
WAN Backup	X	X	X	X
Network Foundation Protection	X	X	X	X

### D. Business Continuity

**Do you have a disaster recovery plan that includes your business-critical network services?**

Network downtime due to disasters affects uninterrupted access to mission-critical business applications. WAN link backups and secured remote access are typically core components of a business continuity plan. Many customers use IP VPN as a WAN backup for its flexibility and cost-effectiveness. Some businesses continue to invest in ISDN and dial-up to keep them as backup links.

**Do you have a plan to protect your network infrastructure from DDoS attacks, targeted attacks?**

The unique network foundation features in Cisco integrated services routers provide the first line of defense against such attacks.

**What are the business benefits of the incremental upfront cost?**

To answer this question, you need to consider current and pending regulations (encryption, for example) in your industry that may affect your company. In today's environment, it often makes sense to deploy security capabilities to ensure that they are available when needed. Purchasing a Cisco Secure WAN bundle with your Cisco router prepares you to activate features as you need them without the cost and effort of upgrading later—and to do so with substantial bundle discounts.

**Why would I add security to my routers if I am already using a security appliance?**

Adding security to your routers does not replace the security you already have. It gives you the flexibility to deploy security throughout the network where different levels of security are needed. Cisco provides both appliance-based security and security integrated into routing and switching solutions so you can optimize security and minimize costs across your entire network—headquarters to branch offices.

**Why should I choose Cisco for my security solution?**

Cisco offers the industry's only integrated, end-to-end security solution that extends from individual desktops through the LAN and across the WAN to protect businesses from worm and virus outbreaks, information theft, DDoS attacks, and increasingly common insider and application abuse. A truly end-to-end security solution results in lower total cost of ownership over the life of your network.

### Additional Resources

#### Cisco Secure WAN Bundles

<http://www.cisco.com/go/securitybundles>

#### Cisco Security and VPN Products

<http://www.cisco.com/go/routersecurity>

#### Cisco Self-Defending Network

<http://www.cisco.com/go/selfdefend>

#### Cisco Integrated Services Routers

<http://www.cisco.com/go/isr>