



Solution Overview

Cisco Smart Business Roadmap—Security

EXECUTIVE SUMMARY

The Cisco Smart Business Roadmap helps small and medium sized businesses (SMBs) ensure regulatory compliance, protect corporate assets, and maintain customer confidence by bringing business planning and technology planning together to enable secure business growth.

The Cisco Smart Business Roadmap Enables Small and Medium Businesses to Protect their Business and Their Customers

CHALLENGE

A security breach can cost a company millions of dollars in lost productivity and confidential or competitive data. But the cost in damage to the firm's reputation or public image can be even greater. In addition to the need to guard against such losses, government regulations are also accelerating the need to document and secure business information and technology assets more effectively than ever before.

To keep pace with evolving security threats and ensure that the business survives and grows securely, organizations need to:

- Protect their business from internal and external network threats
- Provide secure network connectivity for employees either working in the office or remotely
- Secure physical surroundings to protect company assets
- Make sure company and customer data is properly stored

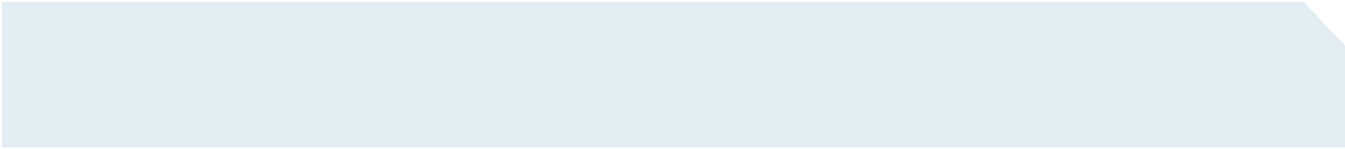
CISCO SMART BUSINESS ROADMAP

The Cisco Smart Business Roadmap provides a structured, planned evolution path to help businesses make smart technology decisions and keep pace with everchanging security challenges. This roadmap shows how Cisco security solutions can help businesses thrive by effectively addressing current security threats and evolving to meet new ones.

Cisco Systems® has identified three major phases of business and technology evolution: foundation, growth, and optimized. No two companies are identical in their current needs or plans for the future. These flexible phases are planning guidelines to implement technology in an incremental and structured way that will best optimize the business. It's not uncommon for a company to be in multiple phases at the same time. These phases are just a starting point for planning.

Foundation

Businesses in the foundation phase (Figure 1) are looking to implement a secure network over which employees, customers, and suppliers can communicate effectively. While they recognize the need to provide employees and customers with tools that allow easier access to information, such as e-mail, scheduling systems, and the Web, businesses are concerned with keeping sensitive information secure.



The following are typical security challenges encountered at the foundation phase:

- Connected computers are at risk from viruses, spam, and spyware
- Unauthorized access puts business at risk
- Business reputation and regulatory compliance will falter if customer and business data is compromised or stolen

Growth

Companies in the growth phase (Figure 2) have secured their core business processes and are focused on enabling growth without compromising information security. They are beginning to give workers the ability to work from home or from the road which presents new security challenges. They also want to continue to improve communications between employees, customers, and suppliers, but they need to maintain effective control over network access.

The following are typical security challenges encountered at the growth phase:

- Need for layered security protection that detects and prevents network intrusion, controls network activity, and monitors application traffic
- Need for protection from unauthorized network access to keep confidential company information safe
- Concern for secure connectivity for remote and mobile employees
- Need to protect and monitor physical assets

Optimized

In the optimized phase (Figure 3), businesses are often focused on offering customers, suppliers and employees the type of relationship that sets them apart from their competitors. Customer relationship management, sales force automation, and call center applications can improve information sharing and efficiency across the company. Ensuring the integrity and security of application data, as well as that of the network itself, requires optimized security measures.

The following are typical security challenges encountered at the optimized phase:

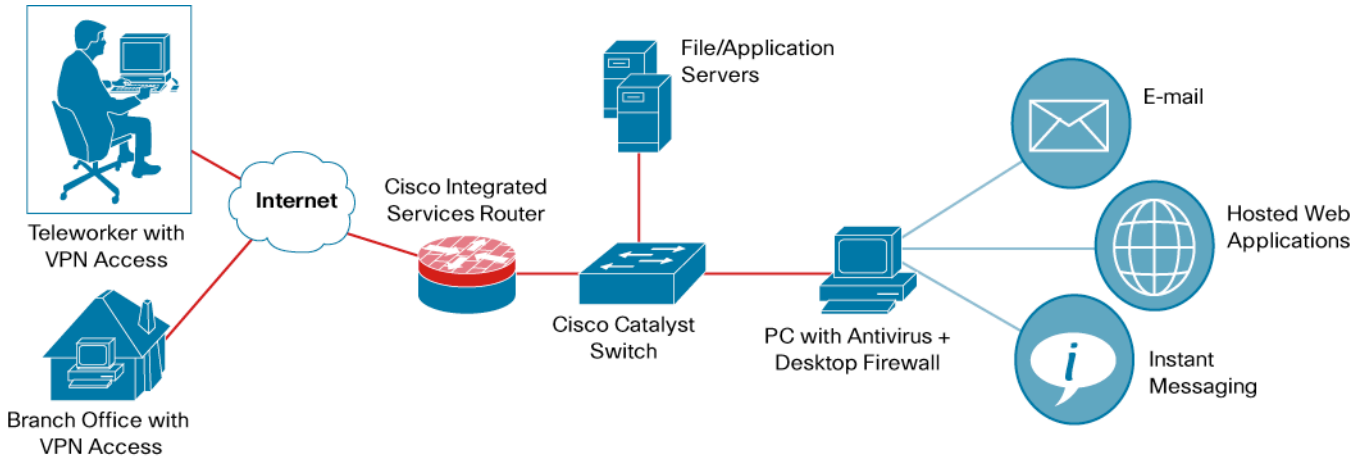
- Data-sharing across the company, and with other agencies can be compromised
- Must be able to properly store company and customer data to safeguard information and comply with government regulations
- Need for physical security surveillance technology, including on-demand access to archived video feeds
- Online Ordering capabilities

SOLUTION

Using the Cisco® Smart Business Roadmap, customers can align a flexible network technology plan with their top business priorities. The roadmap shows how organizations can use Cisco technology solutions to optimize the business by effectively addressing current security challenges and preparing to meet new ones. SMBs can work with their Cisco specialized partner to implement the roadmap at a pace that is right for them. Each phase of the roadmap creates a base for the next phase and makes adoption of new technologies easier and securing business data as the business needs or internal/external threats change? Security concerns are constantly evolving as new threats are constantly emerging. It's important to keep a security plan up to date to keep your company resources secure.

Foundation

Figure 1. Typical Foundation Phase Network to Improve Security

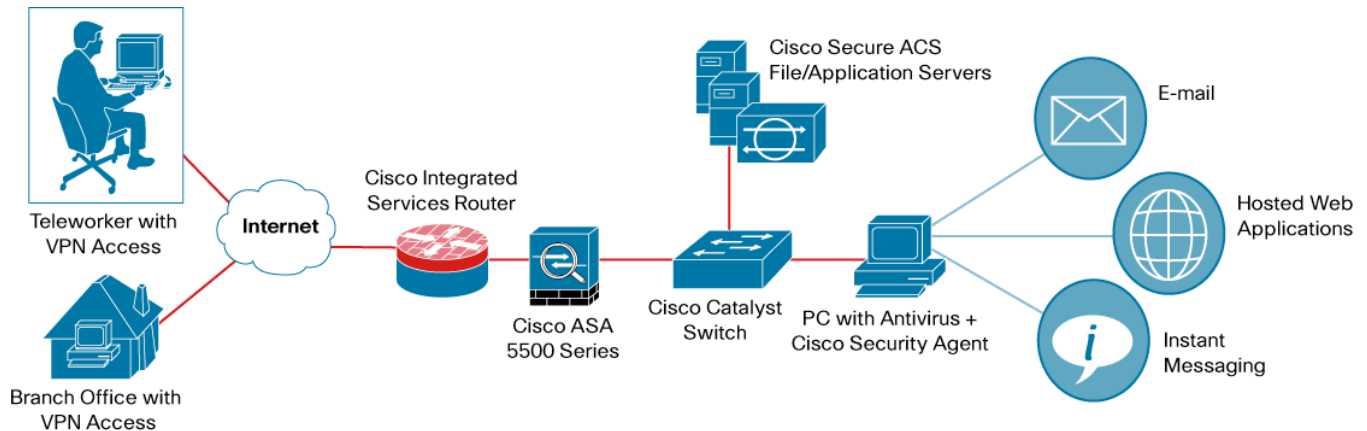


Protecting against security breaches and network intrusions, such as viruses, spam, spyware, and unauthorized access to company and customer data, is a priority for most businesses. Companies often resort to a mixture of specialized applications that protect against specific threats, but each of these applications is independent, and must be configured, managed, and maintained separately. This scenario is inefficient and can lead to gaps in a company's security framework. The Cisco Smart Business Roadmap recommends the following integrated, easy-to-manage solutions that help SMBs maximize security:

- Cisco integrated services routers have integrated security services capabilities such as Cisco IOS[®] Software, firewall, intrusion prevention systems (IPS), and VPN, which provide the basic security functions necessary for preventing network intrusion and a flexible platform for adding new technologies as the business evolves. Dedicated security appliances such as the Cisco ASA 5500 Series Adaptive Security Appliances offer enhanced performance and security controls that allow businesses to protect their network from a variety of security risks.
- Integrated security capability functionality in the Cisco Catalyst[®] switches includes access lists, 802.1x, and other technologies. Integration of security services into the switches facilitates the implementation and enforcement of a comprehensive network security policy for control of network traffic and support for business needs.

Growth

Figure 2. Typical Growth Phase Network to Improve Security

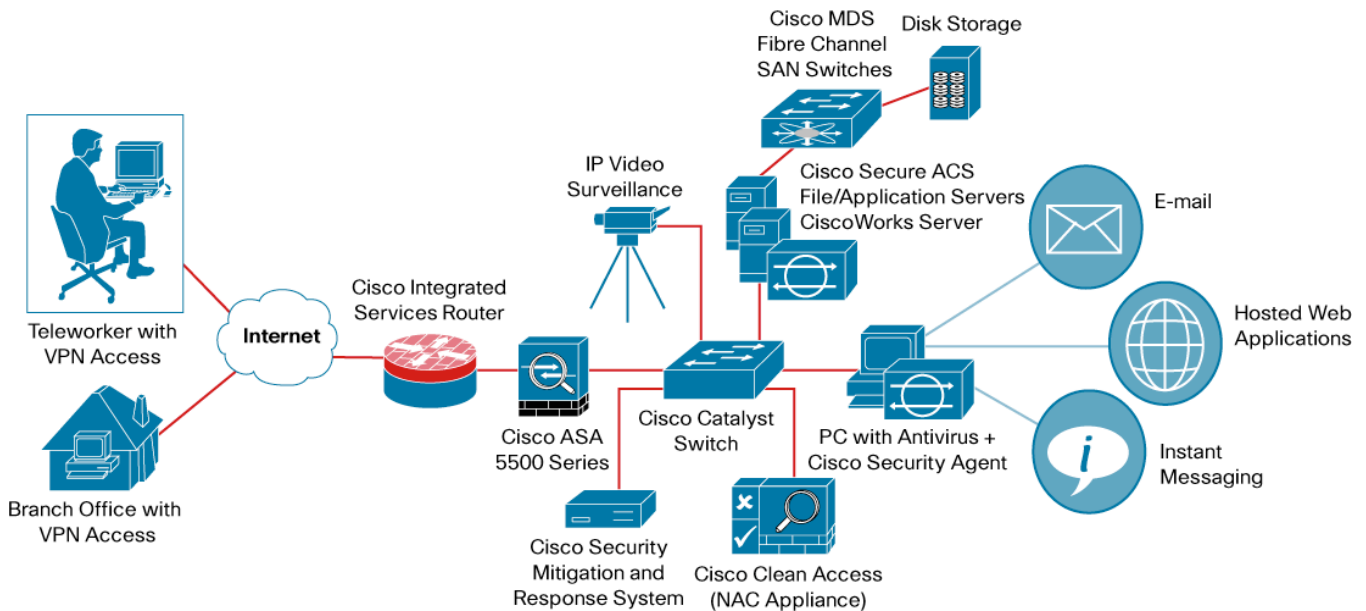


As they advance beyond the foundation phase, businesses often consider implementing a layered, end-to-end security policy. A comprehensive approach to security can protect the business by detecting network intrusion, preventing unauthorized access to the network, providing secure connectivity for mobile and remote employees, and monitoring traffic flows.

- Cisco Security Agent provides threat protection for server and desktop computing systems. Cisco Security Agent addresses network security of businesses by identifying, preventing, and eliminating known and unknown security threats. Cisco Security Agent consolidates endpoint security functions into a single agent, providing host intrusion prevention, spyware/adware protection, as well as protection against buffer overflow attacks, distributed firewall capabilities, malicious mobile code protection, OS integrity assurance, application inventory, and audit-log consolidation.
- The Cisco ASA 5500 Series is a high-performance, multifunction security device, delivering converged firewall, IPS, and network antivirus and VPN services. The Cisco ASA 5500 Series appliances stop attacks before they spread through the network, control network activity and application traffic, and deliver flexible VPN connectivity while remaining cost-effective and easy to manage.
- Cisco Secure Access Control Server (ACS) provides a centralized identity networking solution that simplifies the user and security management experience across the entire network. Cisco Secure ACS helps to ensure enforcement of assigned policies by allowing network administrators to control security matters, including who can log onto the network, user privileges, and recorded security audit information. With Cisco Secure ACS, businesses can manage and administer user access for many Cisco network devices.
- Cisco Clean Access (Network Admission Control Appliance) can automatically detect, isolate, and clean infected or vulnerable devices that attempt to access an organization's network, regardless of the access method. It identifies whether networked devices such as laptops and personal digital assistants (PDAs) are compliant with network security policies and repairs any vulnerability before permitting access to the network.

Optimized

Figure 3. Typical Optimized Phase Network to Improve Security



Businesses in the optimized phase often focus on differentiating themselves from their competitors by enhancing the efficiency of their organizations. To optimize interaction with customers and suppliers, and among colleagues and branches, businesses consider implementing applications to enable secure information sharing. In addition to focusing on meeting data storage security requirements, companies in this phase are also seeking solutions for physical security, such as visual surveillance of visitors and sensitive areas of buildings.

- Cisco site-to-site VPN functionality, which is built into Cisco integrated services routers and Cisco ASA 5500 Series security appliances, facilitates safe and secure transport of business communications between office sites and remote or mobile employees. While Cisco VPN technology safeguards data between endpoints, Cisco Security Agent helps ensure that the endpoints themselves are secure and able to defend against viruses or other malicious attacks.
- IP-based video surveillance solutions offer many benefits over older solutions. Anytime, anywhere access to live camera feeds or archived video is just one of these benefits. A solid Cisco network foundation that supports quality of service (QoS) and other security-related features allows businesses to obtain the greatest benefit from IP-based video surveillance solutions.
- Many businesses use storage area networks (SANs) to facilitate data storage and archiving across all business locations. Fast, QoS-enabled network links are critical to ensuring that data storage and recovery mechanisms work when needed and minimize risks to the business. Cisco offers SMBs a range of SAN solutions. The Cisco SN 5400 Series Storage Routers reduce management and infrastructure costs while improving availability and data protection. This entry-level solution deploys SANs with a low initial investment in capital and staffing and reduces total cost of ownership (TCO) with increased storage resource efficiency.

BUSINESS BENEFITS

The Cisco® Smart Business Roadmap brings together tailored technology solutions, world-class service and support delivered through local specialized partners, and flexible financing options—all designed specifically for SMBs. The roadmap is designed to be implemented over time in incremental stages, according to the company's needs and schedule. Following are examples of some of the potential security benefits at each phase:

Foundation

- Reduced downtime because Cisco Secure Network Foundation provides basic security functions and safeguards against unauthorized network access.
- Customers and employees are confident in data integrity and availability.
- Integrated security capability ensures regulatory compliance

Growth

- Business is conducted with a high degree of confidence because layered security protection detects and prevents network intrusion and monitors network activity.
- Secure network protects against unauthorized network access, reduces costs associated with security policy management, and keeps confidential company information safe.
- Secure access to company information allows remote and mobile employees easy connectivity.

Optimized

- Secure data-sharing capabilities across the company, and with customers and suppliers, promotes customer confidence in data integrity and security.
- Proper storage of company and customer data supports regulatory compliance and minimizes risk exposure at justified costs.
- Up-to-date security surveillance technology helps provide a secure work environment and safeguards company assets.

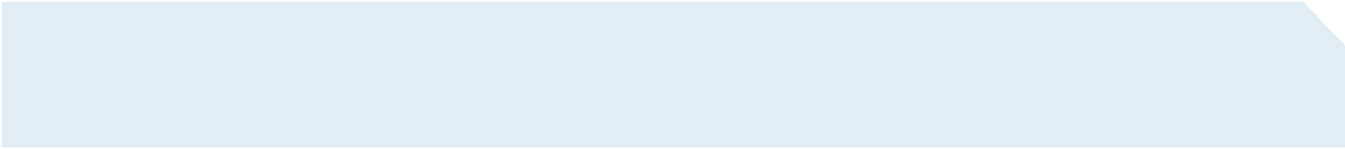
WHY CISCO

Cisco Systems provides a complete solution that addresses the unique challenges faced by SMBs. Cisco offers a wide array of industry-tailored solutions and applications that are proven and tested to meet specific business needs. Acting as trusted advisors, Cisco and its partners work closely with customers to identify the state of their business and network and provide a solution that most closely aligns with their immediate requirements. The Cisco Smart Business Roadmap also provides a framework to help ensure that the immediate solution scales to optimize the business over time.

The Cisco Smart Business Roadmap provides networking solutions, services and support, and financing—as well as specialized local partners and service providers—to design and deliver the right solution that will evolve with individual business needs. Only Cisco offers a whole solution in which the components work better together to produce optimal business results.

Cisco Systems Capital® financing and leasing options provide SMBs worldwide with innovative, flexible leasing and financing programs at competitive rates. SMBs have the flexibility to use revenue derived from enhanced network performance to pay for equipment.

Cisco specialized partners and service providers are experts in the technologies that support the Smart Business Roadmap, providing a high level of localized, in-depth expertise in solutions that can help your company move to the next level. To ensure that your network remains robust and supports critical business operations, service and support options such as Cisco SMB Support Assistant can help you maximize network availability.



Cisco understands that a better way of doing business begins at the business level—not the technology level. Cisco, its channel partners, and service providers work closely with businesses to ensure that their network supports and optimizes the business. Companies can implement a networking technology solution over time in small, incremental steps, at the pace they choose, with lower risk and a lower total cost of ownership. For businesses that are looking for an alternative to purchasing and operating their equipment and services in-house, Cisco has global partnerships with proven service providers to deliver and manage these services. With this flexible roadmap approach, any business can take its first step toward meeting changing business needs today and in the years to come.

ABOUT CISCO

Cisco Systems is the worldwide leader in networking for the Internet. Today, networks are an essential part of business, education, government, and home communications, and Cisco IP-based networking solutions are the foundation of these networks. Cisco hardware, software, and service offerings are used to create Internet solutions that allow individuals, companies, and countries to increase productivity, improve customer satisfaction, and strengthen competitive advantage. The Cisco name has become synonymous with the Internet, as well as with the productivity improvements that Internet business solutions provide. At Cisco, our vision is to change the way people work, live, play, and learn.

Cisco's innovation continues with industry-leading products in the core areas of routing and switching, as well as advanced technologies in areas such as home networking, IP Communications, optical solutions, network security, storage networking, and wireless LAN technology.

Today, Cisco remains committed to creating secure networks that are smarter, faster, and more durable, with a generational approach to an evolutionary infrastructure.

FOR MORE INFORMATION

To learn more about the Cisco Smart Business Roadmap, visit <http://www.cisco.com/go/sbr> or contact your Cisco channel partner. For more information on finding a Cisco partner, visit <http://www.cisco.com/go/partnerlocator>.



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic
Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy
Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)