ZONES™
Connecting Business & Technology

What you need to know about network security

Now more than ever, you depend on your network for your most important business operations, such as communication, inventory, billing, sales, and trading with partners. Yet up to now, you might have held off on protecting your network, for several reasons:

- Network security might seem too complex, and tackling it might seem like too much work. But you can take a step-by-step approach and let Zones help you complete your security plan.
- You might think network security is an expense that won't help your business grow. Instead of thinking about network security as a technical concern, consider it a business continuity issue. Networks have become a basic part of doing business today, making security planning as important as sales and marketing.
- You may believe that small companies are less likely to be a target of attacks. But as large companies beef up their network security, hackers are increasingly focusing on small and medium-sized businesses.

Review these general security tips

The following tips can help you develop and win support for an effective network security plan:

- Consider the harm a network security breach could do to your business, such as lost revenue or even customer litigation.
- Never assume that network attacks will come only from outsiders. Your employees can accidentally create security vulnerabilities.
- Don't be tempted to take a piecemeal approach rather than a single, unified strategy that protects your whole network.
- Work with others in your company to develop and roll out security strategies, focusing on technology, training, and physical site security with tools like surveillance cameras.
- Find the right balance between security and usability. The more secure your network is, the more difficult it can be to use.

Know what should be in a security plan

Every business should have a written (and thoughtfully prepared) network security plan in place. A thorough policy will cover topics such as:

- Acceptable use policy, to specify what types of network activities are allowed and which ones are prohibited
- E-mail and communications activities, to help minimize problems from e-mails and attachments
- Antivirus policy, to help protect the network against threats like viruses, worms, and Trojan horses
- Identity policy, to help safeguard the network from access by unauthorized users
- Password policy, to help employees select strong passwords and protect them
- Remote access policy, to help employees safely access the network when working outside the office

Whether you need to update a plan you have in place or are looking for expert assistance with a new security plan, the Cisco certified experts at Zones can help.

Complete the network security self assessment on page 2.

cisco Gold Partner

THE ZONES DIFFERENCE IS YOUR ADVANTAGE

- Cisco Gold Certification
- Dedicated Cisco coverage across the United States
- Cisco product specialists and certified services team
- One source for all professional services: planning, design, procurement, installation and implementation
- Cisco DVAR with Direct Purchasing Relationship
- Specialization certifications from Cisco in Advanced Data Center, Advanced Borderless Network, and Advanced Collaboration
- Cisco Diversity Partner and certified Minority Business Enterprise (MBE)
- Cisco Customer Satisfaction Excellence (2013, 2014)

Network Security Planning and Cisco Solutions

ZONES™

Connecting Business and Technology

Complete this self assessment to protect against hackers, disasters and other threats

Inventory your current security technologies

Do you have any of the following?

- **Firewall**, to keep unauthorized users off your network.
- **Virtual private network (VPN)**, to give employees, customers, and partners secure access to your network.
- **Intrusion prevention**, to detect and stop threats before they harm your network.
- **Content security**, to protect your network from viruses, spam, spyware, and other attacks.
- **Secure wireless network**, to provide safe network access to visitors and employees on the go.
- **Identity management**, to give you control over who and what can access the network.
- **Compliance validation**, to make sure that any device accessing the network meets your security requirements.

Identify your most important digital assets and who uses them

- Exactly what are your company's digital assets (such as intellectual property and customer records)?
- What are they worth?
- Where do those assets reside?
- Who has access to these assets, and why? Can all employees access the same assets?
- Do you extend access to business partners and customers?
- How do you control that access?

What would a security breach do to your business?

- What is the potential financial impact of a network outage due to a security breach?
- Could a security breach disrupt your supply chain?
- What would happen if your Website went down?
- Do you have e-commerce features on your site? How long could the site be down before you lost money?
- Are you insured against Internet attacks, or against the misuse of your customers' data? Is this insurance adequate?
- Do you have backup and recovery capabilities to restore information if necessary after a security breach?

Consider your current and get a head start on future needs

- How do you expect your business plan to evolve over the next few years?
- How recently have you updated your network equipment? Software? Virus definitions?
- What type of security training do you provide to your employees?
- How will growth affect your digital assets and their value to your business as a whole?
- In the future, are you likely to have a greater need for remote employees, customers, or partners to access those digital assets?

Consult with a Zones security expert about your answers and how to put your network security plan into action.

Strengthen network security with proven Cisco solutions

cisco Gold Partner

Cisco ASA 5500-X Series Next-Generation Firewalls
With next-generation security services, ASA 5500-X firewalls protect your business, regardless of size, against multivector threats across the entire attack continuum.

FirePOWER Services
Cisco ASA with FirePOWER Services brings distinctive, threat-focused, next-generation security services to the ASA 5500-X Series and ASA 5585-X firewall products.

Cisco Email Security Appliance C170
Automate email security with the C170 that uses some of the industry's most advanced technology to automatically stop spam, viruses, and other anomalies.

Cisco 800 Series Routers
Get comprehensive and innovative services, including: Enterprise-grade security; Cisco unified voice, video and data communications; Built-in WAN optimization; Cloud-application connectivity.

Make Zones your technology partner. Visit zones.com or call 800.408.ZONES

2014041_SMB Ntwk Security_141023