

realtimepublishers.com<sup>tm</sup>

# *The Definitive Guide<sup>tm</sup> To*

# Security Inside the Perimeter

**Apani**

*Rebecca Herold*

Chapter 4: The Value of Zoning .....	77
Regulatory Implications for Zoning.....	77
Why Network Security Zones?.....	80
Original Zoning Simply Protected the Enterprise Network.....	80
Security Zones Should Now Be Built to Fit the Business .....	81
Enterprise Management Implications for Zoning .....	82
Zoning Streamlines Business Processes .....	82
Zoning Mitigates Risk Within the Network Perimeter .....	83
Zones Lessen the Impact of Zero-Day Attacks.....	83
Zones Lessen the Impact of Insider Attacks .....	83
Zoning Saves Organizations Time, Money, and Human Resources .....	83
Security Zoning Reduces Operational Risk.....	85
Zoning Protects Against Viruses and Malicious Code .....	85
Zoning Improves Systems Maintenance.....	85
Zoning Improves Network Management .....	85
Zoning Enables Secure Exchange of Information and Software .....	86
Zoning Makes Reporting Security Incidents More Efficient.....	86
Zones Physically Protect Information Assets .....	86
Start to Think About Zoning.....	89
Identify Critical Enterprise Information and Network Assets .....	89
Create an Asset Inventory .....	90
Identify Security Zones by Grouping Assets .....	91
Zone Development and Production Environments .....	92
Zone Business Partners .....	92
Zone by Business Units .....	92
Create a Road Map to Implement Security Zones .....	93
Implement Zone-Specific Protections.....	93
Integrate Security Zones Within Your Layered Security Strategy .....	95
Summary .....	97

## Copyright Statement

© 2005 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at [info@realtimepublishers.com](mailto:info@realtimepublishers.com).

[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library. All leading technology guides from Realtimepublishers can be found at <http://nexus.realtimepublishers.com>.]

## Chapter 4: The Value of Zoning

Zoning to secure valuable resources is nothing new. The concept of creating security zones has been around for centuries. For example, countries have divided their lands into regions and applied military security protection to each region based upon the regional characteristics, value, population, and other various factors.

Security zones are also used to help protect valuable resources against acts of terrorism or other targeted violence. For example, airports mitigate their risks through the use of security zones. They divide the airport grounds, airspace, and facilities into specific zones in order to protect the critical sections of the airport from unlawful interference and to more easily manage the zone areas. Certain security controls apply within each zone. These may include actions such as establishing and maintaining barriers to protect the zoned area, restrictions on entry, and so on. Typically, an airport has an airside area and a landside area. The critical aviation operations are generally included in the airside area, where security is more tightly regulated. These zones may be established for a range of reasons, including the control of people movement, prevention of interference with aircraft, and restriction of access to critical facilities.

Using security zones in these ways not only makes management of security more effective and efficient but also helps to decrease the overall cost of security by creating scalable protection for zones based upon the risks of each zone. Organizations can learn from these practices and apply these same concepts of creating security zones to their own enterprises to protect their information and network resources more efficiently, effectively, and economically. As discussed in earlier chapters, securing only the perimeter will not provide defense against new attack methods and threats such as:

- Social engineering
- Zero-day vulnerabilities
- Malicious email and Trojan horses
- Worms
- Insider attack and fraud
- Rogue wireless and modem connections

### Regulatory Implications for Zoning

Recent surveys reveal that most customers still do not trust companies to handle their personal information responsibly. An October 2005 Ponemon Privacy Survey indicates the customer and opportunity losses associated with information breach events cost a company significantly more than the actual breach events themselves. A March 2005 Ponemon Privacy Trust Survey of more than 2300 adult Internet users in the United States reveals that customers who have a high level of trust in their banks are more likely to do online banking tasks and to remain loyal to the bank they trust. Fifty-seven percent indicated that they would stop using online services if a single privacy breach occurred.

Reflecting consumer mistrust, several governmental regulations have emerged that legislate security and build consumer trust. The laws are complex and failure to follow regulation can result in huge fines, penalties, and even prison time for offending executives. Business leaders must not only be aware of but also strive to be in compliance with the multitude of regulations that are applicable to their companies. This complexity can be made more manageable and companies can more clearly provide demonstration of due diligence by tackling the requirements in zoned chunks across the enterprise. Table 4.1 highlights a few of the regulations and high-level requirements as well as the implications for zoning to make compliance with multiple regulations more manageable.

Regulation	General Requirements	Implications of Zone Security
United States Gramm-Leach-Bliley Act	Administrative, technical, and physical safeguards to protect personal information Privacy notices and opt-out provisions Safeguards and monitoring against future threats Responsibility for ensuring secure outsourced security solutions	Increased storage volume and secure backup storage as well as increased network and storage security Data encryption at source Company-wide policies, risk assessments, and reports Enterprise-wide monitoring
United States California Senate Bill 1386	Disclosure of security breaches in which unencrypted (clear text) personal information may have been accessed by an unauthorized person Procedures to identify and contact persons affected Due diligence in protecting customer information from unauthorized access	Data encryption at source and throughout data life cycle Network and storage security at information repositories Quick and comprehensive identification of personal information storage locations Intrusion detection for access to personal information storage locations
United States Sarbanes-Oxley Act	All documentation used for financial reports and audits as well as all transactions and meeting minutes must be saved Data must be retained for 5 years Ability to locate and recover documents in a few days	Increased storage volumes and distributed storage locations Indexed document retrieval from primary and backup media Secured Write-Once, Read-Many (WORM) storage Restricted access for only personnel with a business need Disaster recovery including geographically dispersed and/or isolated synchronized storage
United States SEC Rule 17a (Books and Records Rules)	Non-rewritable, non-erasable, time-stamped, duplicate message storage Third-party download and storage service Fully indexed and searchable messages Data retention for 6 years, with the first 2 years being in faster storage Ability to provide a copy of any message upon SEC request Collect certain account records and customer information and verify the information with customers	Increased primary and WORM storage volumes Improved indexed message retrieval from primary and backup media, with query/report tools Third-party security Customer access to their corresponding information

<p>Canada Personal Information Protection and Electronic Documents Act (PIPEDA)</p>	<p>Consent before disclosing personal information Well-planned and documented privacy policies made known within the company Information sensitivity and security levels Data retrieval on demand by customer or law enforcement Data retention only as long as required by law</p>	<p>Company-wide policies, risk assessments, and reports Procedures for gaining customer permission to disclose private information Increased secure storage volume Indexed document retrieval from primary and backup media Security based on levels of sensitivity</p>
<p>European Union Data Protection Directive</p>	<p>Personal data must be processed fairly and lawfully and obtained only for specified purposes Data subjects must be told how their personal information will be used and with whom it will be shared Personal data must be accurate, adequate, relevant, and not excessive for the purposes for which it was collected, and not be kept for longer than is necessary Appropriate technological measures must be taken to stop personal data being hacked, lost, damaged, or stolen Personal data cannot be transferred outside the European Economic Area unless the country to where it is transferred provides an adequate level of protection</p>	<p>Company-wide policies, risk assessments, and reports Information and network intrusion detection and prevention Improved indexed message retrieval from primary and backup media with query/report tools Provide access to individual's information upon their request Isolate personal data within only approved countries</p>
<p>Japan Personal Information Protection Law</p>	<p>Take measures to prevent personal data from being accessed or stolen Provide consumers with specific notices, obtain consent, provide information regarding their corresponding information in a timely manner, and allow information subjects to request corrections Cannot handle personal information beyond the stated scope Controlling access of personal information to third parties except as specifically indicated and allowed by the information subject</p>	<p>Company-wide policies, risk assessments, and reports Information and network intrusion detection and prevention Improved indexed message retrieval from primary and backup media with query/report tools</p>
<p>United States Health Insurance Portability and Accountability Act (HIPAA)</p>	<p>Administrative, technical, and physical safeguards to protect health information Privacy notices Safeguards and monitoring against threats Responsibility for ensuring security with third parties</p>	<p>Information and network intrusion detection and prevention Increased storage volume and secure backup storage Increased distributed network and storage security with internal firewalls Data encryption throughout life cycle Company-wide policies, risk assessments, and reports Enterprise-wide monitoring</p>

**Table 4.1: Regulations with zoning implications.**

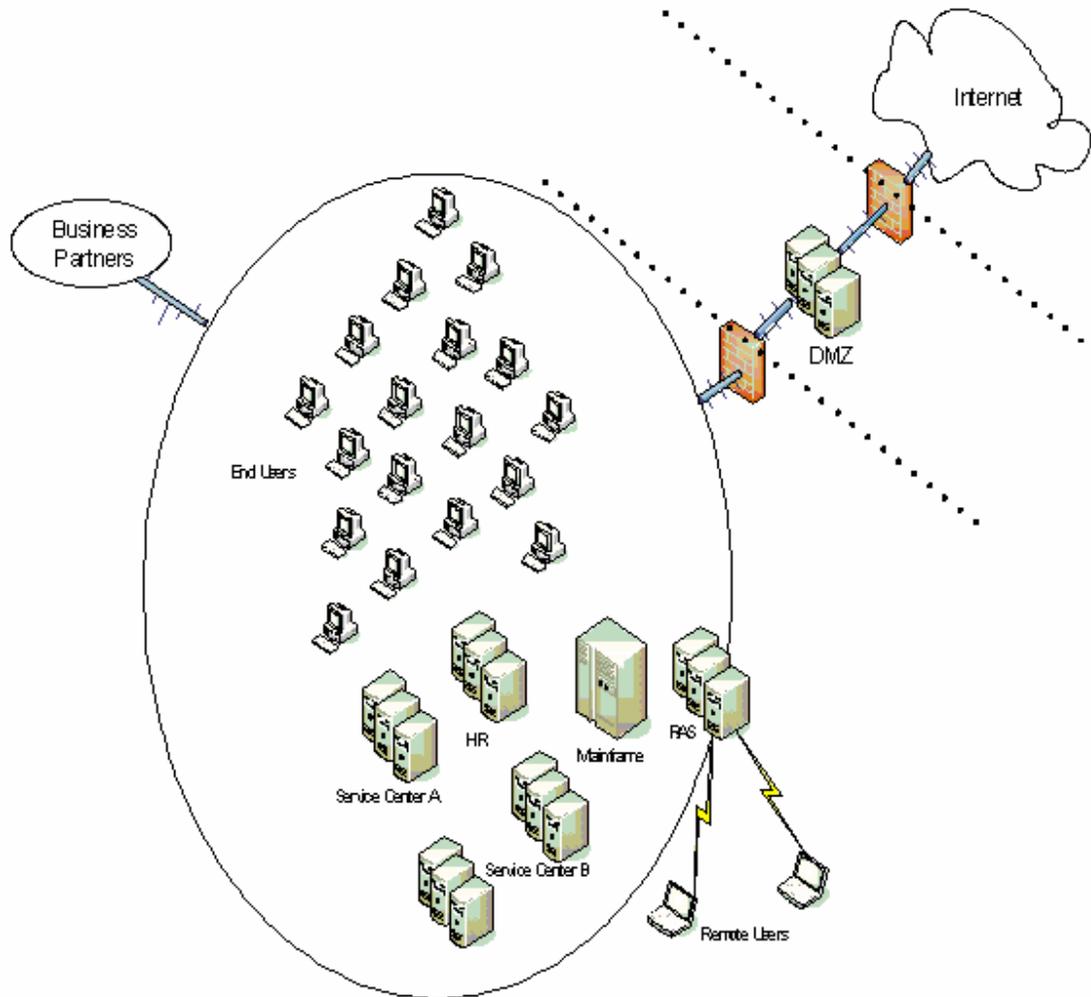
## Why Network Security Zones?

The quality of a network's security is an essential component of the security posture; it connects applications, systems, and users. The network should provide a solid first layer of defense against outside attacks, complementing operating system (OS) and application-level security. Separating the network into virtual compartments, or zones, allows security managers to consolidate resources in a cost-effective manner and control user access to each application and related information. The network then creates a secure environment not only at the perimeter but also in security zones throughout the enterprise.

 Security zones can contain the spread of an attack and provide strong access controls.

### ***Original Zoning Simply Protected the Enterprise Network***

The concept of network security zoning really became widely critical in the 1990s when exploding numbers of organizations began connecting to the Internet. In doing so, they realized, sometimes through brutal business-impacting results of security incidents, that security was needed between the corporate network and the wild and untamed Internet. This realization resulted in the widespread use of demilitarized zones (DMZs) at most security-conscious organizations. The DMZ protected the organization's information and network assets by connecting through them through a firewall. Basically, the network became one large security zone, and the DMZ became another, less-trusted filtering security zone, as demonstrated in Figure 4.1. The connections to business partners largely were made without any additional security applied, creating huge vulnerabilities that were by-and-large unbeknownst and/or unconsidered within the organization.



**Figure 4.1:** Typical early zoning with the internal network all in one zone.

### **Security Zones Should Now Be Built to Fit the Business**

As zoning has evolved, it is increasingly used for creating security defenses between departments or other logical divisions of services and products. For example, the marketing department typically has hosts and subnets with many security and access controls in common. These hosts and networks can logically be grouped into their own zone simply called Marketing.

When there is a need for exceptions or other special cases, perhaps when one or more hosts belonging to the zone needs specific or more restricted access, explicit policy rules can be created within the host or subnet level, again without compromising security. Security zones allow for easy consolidation of environments in which multiple distributed security defenses are currently used for security segmentation. This consolidation offers significant cost savings, reduced administrative burden, policy enforcement, and clearly defined trust domains—all of which are the primary drivers behind consolidation.

 So why isn't network security zoning more widely embraced if it is such a good idea? The most common reason IT analysts give is that up until recently the only way to employ security zoning was with hardware—by either installing firewalls or VLANs and subnets throughout the network. These methods alone were cumbersome to manage and created a certain level of inflexibility. As the internal threats, risks, and vulnerabilities were not fully understood, they felt that as long as the perimeter was secure, the inflexibility wasn't worth the perceived gains. However, with an increasingly porous perimeter, and more knowledge and understanding of insider threats, the value of establishing internal network security zones is being recognized as valuable. There are also many new and emerging products to allow the network to be zoned from a software point of view instead of just a hardware standpoint, effectively addressing the inflexibility of the older hardware-only solutions.

## Enterprise Management Implications for Zoning

Over the years, within the typical organization, the network grows and security is deployed within various departments as it is needed. This network growth often accompanies rapid company growth, disparate geographies, and numerous new technologies, usually with no combined effort to consolidate the varying security components and layers into a single enterprise strategy. Dependence on the network along with functional enhancements to the business systems increases the importance of security and dependable accessibility to information. This uncoordinated application of security whenever it is needed, without any forethought to support or management, results in extremely costly and difficult-to-manage systems with gaps in security throughout the network. Implementing network security zones can help organizations achieve their goals of scalability, availability, security, manageability, performance, supportability, and geographic distribution, while realizing savings at many levels throughout the enterprise.

### ***Zoning Streamlines Business Processes***

Creating effective security zones throughout the enterprise will not only decrease the total cost of ownership (TCO) for the IT infrastructure by eliminating wasteful redundancies and establishing consistent standards but also has the added benefit of creating an efficient management layer of protection through thoughtful and effective network and systems segmentation.

Security zones enable organizations to:

- Allow for more efficient audits and compliance reviews
- Decrease operating costs
- Ease the challenges for security policy enforcement
- Enable better geographic security distribution
- Improve network security manageability
- Improve network security scalability
- Improve physical security defenses and management
- Increase network performance
- Increase overall network availability
- Optimize resource allocation
- Provide more efficient security systems supportability
- Reduce software and hardware requirements for security tools and systems
- Respond more quickly to network and systems threats

### **Zoning Mitigates Risk Within the Network Perimeter**

Providing compartmentalized security throughout the enterprise through the use of security zones is a tried and true way to mitigate risks within the perimeter. Security zones proactively defend against vulnerabilities, minimizing unauthorized access, intentional and unintentional.

### **Zones Lessen the Impact of Zero-Day Attacks**

Consider the impact of “zero-day” malicious code attacks. “Zero day” refers to an attack, usually through a malicious code exploit, such as a worm or a virus, that makes use of previously unknown vulnerabilities. Zero-day exploits typically start attacking systems at the same time as, or even before, the public announcement of a vulnerability in a computer system. Reactive defenses, such as signature-based virus scanners and automated patching systems, are still necessary, but they are ineffective against zero-day attacks.

By using security zones, such zero-day attacks can be more successfully contained within the zone of origination, isolating the attacks and the compromised device. Confining an attack to one or a few zones allow other network security zones to continue to support business as usual.

### **Zones Lessen the Impact of Insider Attacks**

As discussed earlier in this guide, there is great threat to information resources from insiders who have authorized access. Insiders may threaten an organization’s interests by disclosing sensitive or classified information, making decisions that have a negative impact on the business, or exacting a network attack. Establishing security zones throughout the enterprise can help to contain the impact of any insider attack to only the zone within which they are located.

 Authorized users with privileged access may attempt to access unauthorized resources, perform Denial of Service (DoS) attacks on shared resources, or delete or modify shared data sets. Establishing security zones throughout your enterprise network will prevent such attempts from going beyond the security zone into another where the user has no authorization.

The situation is particularly dangerous when a legitimate user’s authentication credentials (password or keys) are stolen, allowing an attacker to masquerade as a legitimate user. Such masquerade attacks can lead to further damage beyond the initial compromised account and there is little indication of a problem to security systems administrators. Establishing security zones will help to limit the damage to only one zone within the enterprise and save the rest of the enterprise zones from the destructive impacts.

### **Zoning Saves Organizations Time, Money, and Human Resources**

When considering the deployment of security zones, wise business leaders must consider how the implementation of what at the onset seems to be a huge investment, in reality will save the organization time, money, and human resources in the long run.

 According to a 2005 Gartner Group study, the average downtime cost for businesses across all industries is more than \$1 million per hour. In addition, according to a 2005 Wall Street Journal report, more than 83 percent of all critical data lost is due to some form of human error, 64 percent from human mistakes and 19 percent from internal sabotage within an organization.

So where can savings be realized? Measure the gains in IT staff and user productivity from deploying the solution as well as the revenue recaptured from reduced downtime, the cost savings from increased IT staff efficiency, fewer security incidents and associated response costs, and lower capital and operating expenses. The following list provides examples of ways in which network zoning will save organizations time and money resources:

- **IT productivity savings**—Zoning can help improve IT staff productivity by allowing security to be managed and addressed on a zone-by-zone basis as opposed to the common way of managing on a server-by-server and node-by-node basis. Besides reducing operations costs, gains in IT productivity can free up staff to implement new initiatives more rapidly, helping to create a competitive edge.
- **User productivity**—When users are unable to access network resources, their productivity is likely to be severely impaired. Users often are able to move to other business applications when service interruptions or performance degradations occur. Zoning will improve system uptime and user productivity by confining problems to as few zones as possible while allowing other zones to remain in full production mode, providing areas for those affected in one zone to continue their work in another unaffected zone.
- **Recaptured revenue**—Higher system availability contributes to businesses' top lines because less revenue is lost due to downtime and potential service penalties are avoided. Downtime can also be costly in terms of diminished customer satisfaction and possible loss of a customers' business. Security zoning can contribute to recaptured revenue by isolating security problems to one part of the enterprise to more efficiently be responded to while allowing the other zones within the enterprise to continue providing service and products.
- **IT efficiency**—IT staff efficiency can be described as a measure of how well the IT management organization can achieve economies of scale and scope of work with its people, tools, and practices. Companies must be able to grow their systems and networks at a faster rate than the IT staffs required supporting them in order to remain competitive. Experienced and knowledgeable IT professionals continue to be scarce, resulting in existing staff taking on more work and responsibilities, including more and more security management activities. Establishing security zones helps IT departments to achieve economies of scale and scope to better manage with fewer staff and resources, while at the same time gaining a competitive advantage.
- **Other cost savings**—Additional cost savings may be realized by eliminating other security management tools that have historically be used on a server-by-server and system-by-system basis, and instead use tools designed to effectively manage security within established security zones.

### **Security Zoning Reduces Operational Risk**

Security controls must be in place to safeguard all operations of enterprise information facilities and systems. Operational security controls must ensure that risks to information integrity, availability, and confidentiality are minimized in the operational environment, in online service delivery, and in exchanging information by any means in the internal or external information environment. Zoning can enhance and improve the efficiency of security and risk reduction for these operations. The following sections provide examples of operational activities that can be enhanced by security zones.

### **Zoning Protects Against Viruses and Malicious Code**

Organizations must ensure that security controls are in place for the protection of information and systems against viruses and other malicious code. Controls must include prevention, detection, removal, and reporting of attacks of malicious code on the information environment. Incorporating zone-based virus and malicious code prevention can help improve the effectiveness of the controls and help protect zones when outbreaks occur in other zones on the network.

### **Zoning Improves Systems Maintenance**

Organizations must develop processes to ensure the availability of information and information systems, networks, and applications in the event of failure or unforeseen loss of information. Processes must be established that include comprehensive information backup procedures. Operator and fault logs must be implemented to monitor the integrity and availability of information, information systems, networks, and applications. Efficiency is improved by implementing logs and maintenance within zones. This task is accomplished by limiting the scope of the logs and, as a result, making maintenance less labor intensive, allowing multiple groups to focus just on their areas of responsibility.

### **Zoning Improves Network Management**

Organizations must establish security controls to protect networks and infrastructures from unauthorized access and to safeguard information confidentiality and integrity. To ensure the integrity of networks, privately owned devices (for example, home computers) must not connect to enterprise networks unless detailed risk assessments are conducted to determine all security impacts and any additional security measures are in place to ensure the highest level of information security. Assessment must include all aspects of information security (for example, authentication measures, access controls, virus and malicious code protection, physical and personnel security). Establishing such measures and controls and performing such assessments within identified security zones helps to streamline the security process and limit the scope to only the area of the network for the management process.

## **Zoning Enables Secure Exchange of Information and Software**

Methods for exchanging information between an organization and business partners or third parties must be consistent and secure to meet legal and regulatory requirements. When network information is exchanged, it must be protected according to the level of classification. By creating security zones, an organization can more easily and efficiently manage the information within each zone as well as ensure each piece of information is appropriately classified. This setup then enables the information to be shared with third parties and business partners in the most appropriate way. For example, a zone can be established to exchange information with a high-risk third party so that the accompanying risks to rest of the network will be minimized as much as possible.

## **Zoning Makes Reporting Security Incidents More Efficient**

Formal processes must be in place to report security incidents and weaknesses as quickly as possible to appropriate positions, such as the corporate information security officer and/or corporate privacy officer. Dividing the enterprise network into security zones can allow for more efficient and timely monitoring of security incidents on a zone-by-zone basis and report to the most appropriate position based upon the zone within which the incident occurs.

## **Zones Physically Protect Information Assets**

Physical and environmental controls are also an important component to protecting enterprise information and systems. Without sufficient physical and environmental controls, you could experience a complete network failure. To help prevent network interruptions and inappropriate access to information resources you need to:

- Ensure adequate climate control, such as monitoring temperatures and humidity of information systems equipment
- Store all backup media at a secure offsite location
- Protect network equipment and information media from water, fire, and other environmental hazards
- Use power interruption controls to ensure continuous, consistent electricity
- Control physical access to computing equipment
- Ensure only authorized persons can enter areas in which sensitive information and network components are located

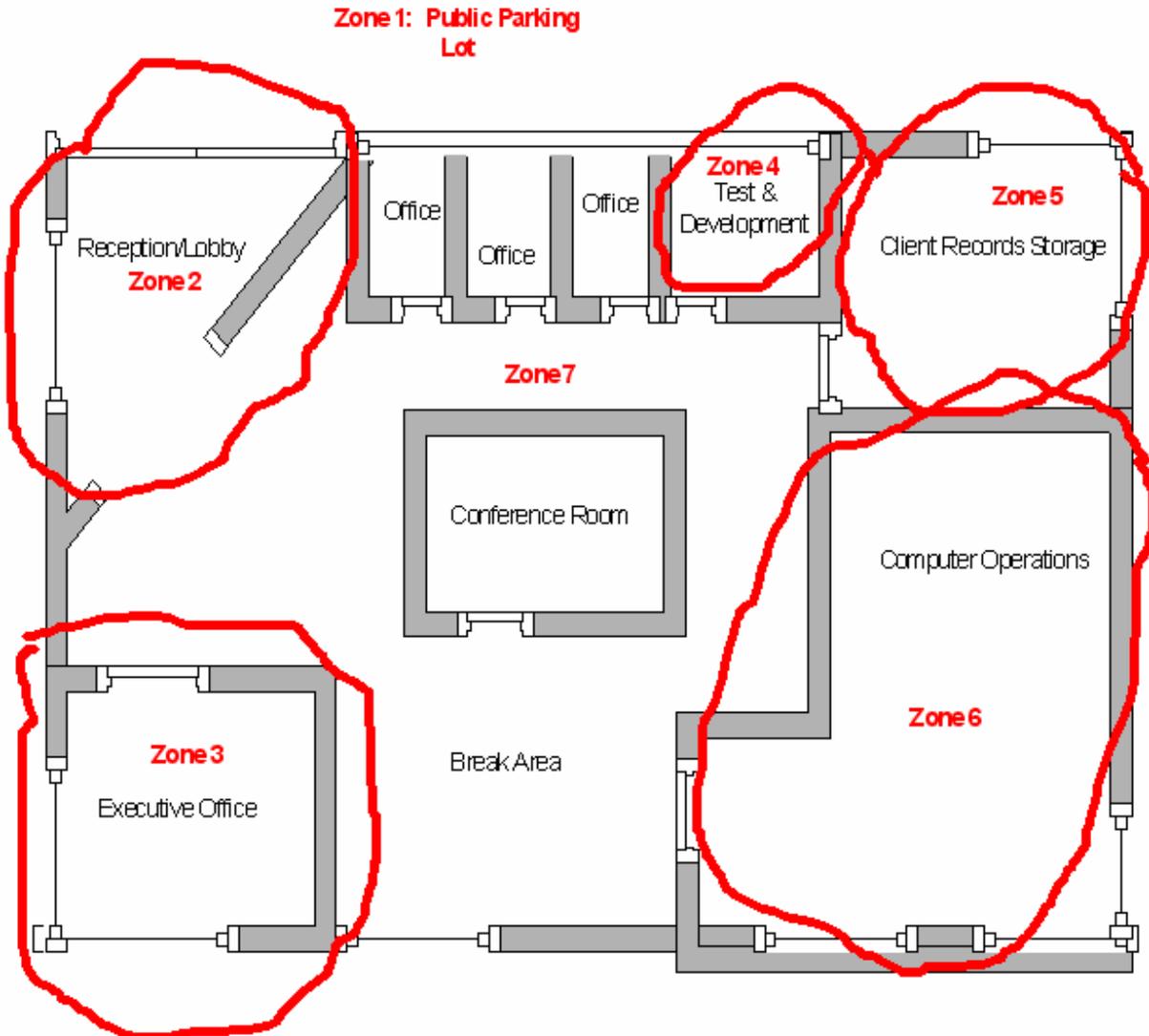
Environmental failures and physical events can cause considerable damage to information systems and business processing. Such threats can be natural or man-made. Mitigating the risks from these threats can be approached using zoning techniques in the same way that zones can be established within the network.

Implementing a strategy for physical protection is an important step to include within any effective enterprise information security plan. Zoning can be used to establish efficient and effective physical information protection.

Traditionally, organizations considered zoning to basically consist of installing fire alarms and fire suppression systems within each room. However, physical zoning to complement network security zoning efforts goes beyond this. Physical zoning can facilitate the simplest to the most detailed security model. The components of security devices implemented within each identified security zone may include:

- Smoke and fire alarms
- Motion detectors
- Physical intrusion detection alarms
- Closed circuit television (CCTV) systems
- Physical barriers
- Locks and safes
- Break-proof glass
- Temperature and humidity control
- Halon and other waterless fire suppression systems

Physical security zones can be based upon similar requirements as network-based zones. For example, physical zones can be role-based. In such a plan, users are assigned to access physical areas, systems, data, and other components based upon their job responsibilities and assigned roles. Figure 4.2 provides a basic example of using role-based physical security zoning for access control. In this example, the zones are labeled 1 through 7. Each zone has unique threats, risks, and vulnerabilities. Zone 1 is the least restrictive, being open to the public. Zones 5 and 6 are the most restrictive, containing the operations equipment and all the customer data. Everyone within the building has access to the areas within Zone 7. Only authorized personnel have access to Zone 3, the executive office. Zone 4 is restricted to only personnel performing test and development activities.



**Figure 4.2: Example of physical security zoning.**

Conduct a risk analysis to understand the physical threats, vulnerabilities, and risks, then use this information to build a risk mitigation strategy that includes identification for where physical security zones are needed. Once you have decided where your physical security zones should be located and how restrictive access to each should be, you then need to determine the controls to support the security zones.

👉 The more restrictive the zone, the stronger and more reliable the controls should be.

By combining physical zones with network security zones, organizations can create an effective centrally managed defense to protect information and assets.

## Start to Think About Zoning

Business leaders can translate the broad concept of using security zones as discussed within enterprises at a very high level by:

- Identifying relationships between departments and determining how they share information and how they trust each other
- Identifying critical enterprise information and network assets
- Creating an inventory of these assets
- Identifying security zones by grouping the assets and identifying key processing areas
- Creating a road map to implement the security zones, based upon criticality, over a practical period of time
- Determining and implementing zone-specific protections

The following sections explore at a high level the concepts of creating and implementing security zones to help guide enterprise leaders in overseeing such activities within their organizations.

### ***Identify Critical Enterprise Information and Network Assets***

Create a list of critical enterprise information and network assets, then document the ones essential to the reliable and necessary operation of the enterprise. Follow a documented, risk-based process for your identification methodology. Establish risk-based criteria that correspond to the unique environment, requirements, services, and products of your organization.

 Most organizations have a control center and backup control center that are considered critical enterprise assets.

The computers and networks that provide the data and information to drive decisions made in the control center will typically be considered critical assets. Some organizations will have a very long list of critical assets. They will often be based within business units and critical corporate activity centers.

 Identifying critical information and network assets will require the participation of personnel from all facets of the organization.

The following list highlights examples of critical information and network assets:

- Customer information
- Web servers
- E-commerce applications
- Firewalls, routers, and other network security components
- Employee data
- Business transaction logs

 As of September 2005, the North American Electric Reliability Council (NERC) is currently drafting wide-ranging cyber-security guidelines to replace their temporary precautions adopted as NERC Cyber Security Standard 1200 in 2003, renamed NERC Cyber Security Standard 1300 in 2004. This new set of guidelines, NERC CIP, will be finalized in Spring 2006 and establishes standards in eight key areas:

- Provisions for identifying critical cyber assets
- Developing security management controls
- Implementing training
- Identifying and implementing perimeter security
- Implementing a physical security program for the protection of critical cyber assets
- Protecting assets and information within the perimeter
- Conducting incident reporting and response planning
- Crafting and implementing recovery plans

### **Create an Asset Inventory**

Creating an inventory and corresponding classification of critical enterprise information and network assets is a critical step in creating security zones. It is also an activity that should have been done already to facilitate business continuity processes and comply with various regulatory requirements for identifying and protecting certain types of information.

 Typically, such an inventory and classification of criticality is created during a business impact analysis during the creation or update of a business continuity plan.

The types of resources typically included within a business impact analysis include:

- Personnel
- Facilities and associated specific locations
- Technological platforms, including traditional, e-commerce-related and network management systems
- Applications and systems software
- Data networks and equipment
- Voice networks and equipment
- Wireless networks and equipment
- Vital records
- Personally identifiable information
- Supply chain partners and associated data and network components
- Business processing outsourced vendors and associated data and network components

 The 2004 TechRepublic State of IT Asset Management study of 497 organizational responses revealed:

- 10 percent do not have an IT asset inventory
- 51 percent use the most rudimentary asset management tools (spreadsheets and discovery tools) to maintain an IT asset inventory
- 19 percent use a repository integrated with discovery tools to manage inventory
- 13 percent manage the IT asset life cycle with defined processes, automated workflow, and integration
- 7 percent use a mature IT asset management model

Asset inventory and categorization will also help auditors and compliance regulators to better understand how the security threats on a low-priority system or zone are different and require different levels of security than the security threats on a high-priority system or zone. Not only will such an inventory and categorization improve the reviewers' understanding, it will also help to reduce the time necessary for the review, which will then result in a positive impact on your organization's bottom-line.

 The information within a zoned area of the enterprise network for development systems will likely be lower priority than the customer information located within the zoned area of the enterprise network for production ecommerce systems.

### ***Identify Security Zones by Grouping Assets***

Divide the data center into areas that are logically separated from one another based upon their associated critical assets and revenue areas to contain an attack at minimal impact to the overall business. Zones can support individual applications or application tiers, groups of servers, database servers, Web servers, e-commerce zones, and storage resources.

 Examples of security zones created through grouping assets include limiting user access to Web servers, such as through the use of a Web front-end, protecting the application and database tiers from accidental or malicious damage. In addition, communication between applications can be limited to specific traffic required for application integration, data warehousing, and Web services.

Security zones can provide logical separation of each application's storage environment across a scalable, consolidated storage network. To achieve this setup efficiently, firewalls can be integrated and virtualized to provide secure connectivity between application and server environments

## Zone Development and Production Environments

Segregate business-critical development and production facilities to reduce the risk of accidental changes or unauthorized access to production software and business data. Development and testing activities can cause unintended changes to software and data sharing the same computing environment. Use zoning to manage these risks.

When creating zones take into consideration that

- Development and production applications should run on different processors or in separate domains or directories \
- Development and test work should be separated at a logical level
- There are (or should be) rules governing the transfer of software from development to production
- Software version controls may reside in different zones
- System utilities (such as compilers and editors) should not be accessible from production systems

## Zone Business Partners

The risks of using external service providers, connecting to business partners, and otherwise sharing information and network resources with third parties should be assessed and documented. Connecting to or using third parties for managing or processing computer or network facilities increases the risks to an organization's information security. Just look at the number of incidents that have occurred through third parties in just the past 12 months, as described in previous chapters.

Appropriate information security measures, both technical and non-technical, should be incorporated into contracts before a third party connects to an organization's network or starts processing an organization's information. Use this contract information to create security zones for the business partners that address the unique risks presented by each.

## Zone by Business Units

Many organizations find after identifying critical information and network assets that it is most advantageous and efficient for security management to create security zones based upon business unit services and products.

### **Create a Road Map to Implement Security Zones**

After the security zones are identified, a road map needs to be created to ensure the efficient and effective implementation of the security zones into the enterprise, based upon criticality, over a reasonable period of time. Integrate the security zones into the existing enterprise network. Define the access and security requirements for every service so that the network can be divided into security zones with clearly identified security and access levels.

Work with each security zone separately. It is likely each zone will have a different security model necessary to address the identified risks. Security controls should be implemented so that security breaches and incidents can be confined to a particular zone or part of the network as much as possible.

 Implement security zones in such a way so that they will limit the damage a security breach or incident has on the entire network.

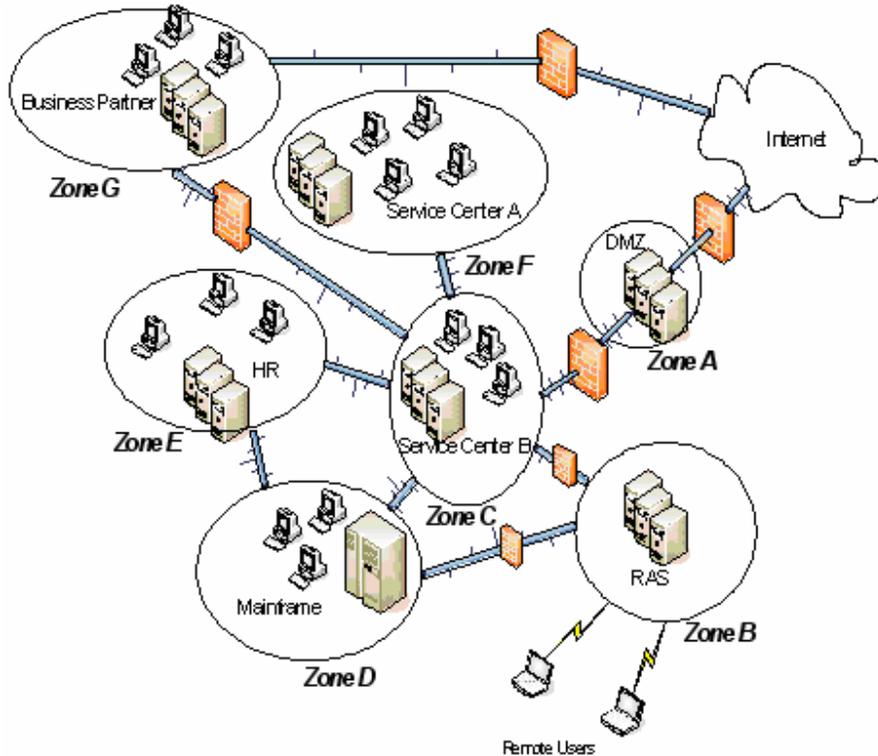
In addition, security zones should take into consideration the network security architecture defining common security services that are implemented across the network. The following list highlights typical services:

- Password authentication, command authorization, and accounting
- Virtual private networks (VPNs)
- Access control systems
- Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs)
- Encryption systems
- Third-party application service providers (ASPs)

Recognize the optimal varying levels of control within the security zones to identify clients and zone users, protect your zone perimeters as well as network perimeters, protect confidential information from eavesdropping or tampering during transmission, and ensure the integrity of your system and applications. Such decision making will involve not only IT staff but also information security, business unit contacts, and internal audit. After you have made the difficult decisions for the types of security to deploy within the zones based upon the risks within each of the zones, deploy the security architecture in phases, addressing the most critical zone areas first.

### **Implement Zone-Specific Protections**

The road map for establishing and maintaining security zones will likely include a diagram representing the zones. For example, Figure 4.1 from earlier in this chapter may now look like Figure 4.3 after the decisions have been made about where to establish the zones.



**Figure 4.3: Example of zoning within the network.**

Each of the identified security zones need to have controls and protections implemented based upon the risks specific to that zone. It is likely all zones will have similar protections, such as virus control systems. However, it is also likely that zones will have unique controls that no other zones may have, such as a zone with a remote access server (RAS) or a zone that houses a credit card processing system. There will probably be zones that have firewalls protecting them, and other zones that have no firewalls.

Steps to building a security zone include:

- Asset identification and classification
- Business impact analysis
- Asset prioritization
- Creation of manageable security zones (compartmentalization)
- Hardened security zones based on criticality using firewalls, filters, and access controls
- Deployment of in-depth and diverse defenses
- Security zones monitoring
- Assessment then remediation of vulnerabilities

☞ The key to successful zoning is thoughtful analysis of the risks within and to each zone, then the application of the most appropriate security controls for each zone's risk.

## Integrate Security Zones Within Your Layered Security Strategy

By implementing security zones, an organization will shift reliance from perimeter security to an asset-centric model that protects the enterprise assets from the most likely threats with the most efficient measures. Security zones allow assets of greater organizational criticality and value to be held to higher security standards and protected by additional layers of defense. If possible, they should be compartmentalized, or zoned, into their own networks and segments. By doing so, the perimeter will be considered an asset.

Do not stop at just zoning alone, though. Zoning is just one of the layers to use within an organizational security strategy. To successfully defend against the multiple and varied types of threats and address the numerous and diverse vulnerabilities, organizations need to create and implement a layered security strategy. Perimeters, infrastructure devices, OSs, applications, and data must be assessed and appropriately fortified to mitigate the risks that threaten your organization. Use multiple complementary approaches for security enforcement and defense at various points in the network, which will remove single points of security failure.

Chapter 5 will discuss the need for a layered security strategy in detail. For now, the following list outlines at a high level a layered security strategy, including security zones:

- Obtain executive management support—An information security program must have the visible backing of upper management to be successful. Personnel follow the example of their leaders; if they clearly see upper management supporting information security efforts, they will also do so.
- Address legal and contractual requirements—An information security program must include activities that support privacy and information assurance requirements that exist within the wide range of enterprise contracts and are required by applicable laws and regulations throughout all the locations where the organization has offices and does business with partners and customers.
- Include personnel and processes into enterprise security planning—Effective security policies and procedures, security awareness and training, and consistent policy enforcement ensures a stronger, more efficient security program. You cannot expect security policies and procedures to be followed effectively, efficiently, or consistently unless the people using information resources have been told what they are and truly understand how to follow them.
- Clearly define user roles within security zones—Use both technical and non-technical security tools and control mechanisms—such as firewalls, IDSs, filters, access control capabilities, physical barriers, and alarms—to enforce access policies between security zones, giving only those with a business need access.
- Implement strong authentication methods to protect network and physical zones from unauthorized access and entry.

- Implement processes to maintain the integrity of the resources located on the network, servers, and end-user systems by doing such activities as
  - Hardening the OSs within the enterprise network and implementing ways to harden mobile computing devices
  - Disabling unused services
  - Applying patches as soon as possible, but only after testing and waiting for a timeframe when the risk of the change is reduced
  - Continuously protecting against malicious code, such as viruses, worms, Trojan horses, and spyware
- Secure endpoint computing devices that are connected, or sometimes connected, to the enterprise network—Create an inventory to account for all end-user computing devices, including wired and wireless. For instance:
  - Securing WLAN/Wi-Fi or Wireless Mesh communications using VPNs and WPA2
  - Securing devices that are often forgotten with regard to security, such as handheld computing devices (PDAs, Blackberries, and so on), smart phones, and mobile storage devices, such as USB thumb drives; such devices can contain a huge amount of personal information, intellectual property, and sensitive data, and are highly prone to loss or theft
- Protect the network administration and management information—Establish virtual LANs (VLANs) in conjunction with other security tools (such as IPsec, SNMPv3, SSH, TLS, and so on) to separate traffic between zones, allow only authorized access, and protect network resources, devices and applications, management and systems components. Be sure to implement backup processes for systems and device configurations and use a change management process to ensure only appropriate changes are implemented, in addition to tracking changes.
- Stay aware of your network traffic trends and the corresponding threats, risks, and vulnerabilities within each of the security zones—Monitor for threats, both outside of the perimeter and within the perimeter. Block invalid network activity and traffic using a variety of tools, such as DoS prevention, anti-spoofing, and logon blocking implemented at the security zone perimeters.
- Implement a wide range of security tools to create a blanket of protection against threats and protect mission-critical systems and applications—Keep your firewalls up to date to support new systems, applications, and protocols, such as SIP and H.323.
- Monitor the network security health by creating appropriate and sufficient logs—Analyze the logs and associate them with audited events to help ensure the most effective security management based upon current and relevant information. Summarize logs and events to create a network security health report with identified threat activity.
- Evaluate all established security zones to ensure they are still effective—Update the zones whenever necessary to improve upon security by addressing new threats, risks, and vulnerabilities.

## Summary

Organizations should use security zones to more effectively and efficiently help protect valuable information and network resources against the multitude of threats within the perimeter as well as the increasing amount of threats from outside. The following checklist identifies considerations for security zone implementation:

- Identify critical assets and create an inventory to know and understand where necessary information and network resources are located.
- Perform a security assessment to identify vulnerabilities and risks, with specific breakdown by host, OS, application, data, network devices, and links. The assessment will provide information necessary for determining appropriate risk levels for each asset and the requirements for maintaining each one to the desired security level; this information should be incorporated into the security policy.
- Define security zones and set security levels for each zone. Use security zones to divide the network as well as the data center into areas that are logically separated from one another to contain an attack at minimal impact.
- Employ zones that support individual applications or application tiers, groups of servers, database servers, Web servers, e-commerce zones, and storage resources.
- Limit user access to and within security zones to specific servers, protecting the application and database tiers from accidental or malicious damage.
- Limit communication between applications to specific traffic required for application integration, data warehousing, Web services, and so on.
- Use security zones to provide logical separation of each application's storage environment across a scalable, consolidated storage network.
- Implement endpoint protection for critical servers and hosts. This protection can be used to discover attacks in progress, protecting not only the zone being attacked but also the OS and applications and sending alarms to the management console when an exploit is detected. Implement network IDSs for critical network segments and zones, analyzing traffic streams to identify DDoS and other attacks as well as hacker activity. Implement IPSs to stop attacks, but do so thoughtfully so that you reduce the risks that false-positives will kill a legitimate session.
- Control access between zones with firewalls and routers. Firewalls provide control for outbound connections from a zone and allow legitimate responses from the remote host.
- Implement VLANs to enable containment within security zones. When each host or segment has its own VLAN, security managers can quarantine attacks and prevent their spread to other hosts; hosts on each VLAN can communicate only with the default gateway, not with other hosts.

## Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.