



The Right Technology. Right Away.™

# Network Security

Reference Guide

[CDWG.com/securityguide](http://CDWG.com/securityguide) | 888.510.4239

# Network Security

## Reference Guide

Chapter 1:	Introduction .....	3
Chapter 2:	Gateway Security .....	5
	• Firewalls	
	• Intrusion Prevention Systems/Intrusion Detection Systems	
	• Network Access Control	
Chapter 3:	Server Security .....	9
	• Authentication and Authorization	
	• IP Security	
	• Content Filters	
Chapter 4:	Client Security.....	13
	• Malware	
	• What to Do About Malware	
Chapter 5:	Mobile and Wireless Security .....	26
	• Unsecured Wireless Networks	
	• Remote Access to Institutional Networks	
	• Breaking the Security Boundaries	
Chapter 6:	Physical Security .....	29
	• Securing Data Centers, Property, Staff and Students	
	• Securing Notebook PCs and Portable Devices	
Chapter 7:	Summary .....	31
Glossary:	.....	33
Index:	.....	35

## What is a CDW•G Reference Guide?

At CDW•G, we're committed to getting you everything you need to make the right purchasing decisions — from products and services to information about the latest technology. Our Reference Guides are designed to provide you with an in-depth look at topics that relate directly to the IT challenges you face. Consider them an extension of your account manager's knowledge and expertise, to help your organization succeed. We hope you find this guide to be a useful resource.

Keep an eye on your mailbox for the **CDW•G IT Investment Guide**. It has even more products and information to help with your security objectives.



The Right Technology. Right Away.™

# Introduction

The IT profession is acutely aware of the need for information security. The seemingly constant stream of new viruses, worms, rootkits, Denial of Service (DoS) attacks and other threats is well publicized.

According to the 2006 Computer Security Institute (CSI)/FBI Computer Crime and Security Survey:

- 52 percent of respondents reported unauthorized use of computer systems
- 313 respondents reported total losses of \$52 million due to computer incidents
- 59 percent of respondents reported more than 10 Web site security incidents over a year's time, and 36 percent of respondents did not know how many Web site security incidents had occurred
- Virus incidents were the greatest cause of financial loss

Source:

[http://www.gocsi.com/forms/fbi/csi\\_fbi\\_survey.jhtml](http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml)

To neutralize these threats, most organizations are spending significant money on countermeasures. Although organizations are taking precautions, the threats continue to proliferate and evolve. As existing technology becomes more mature and well known,

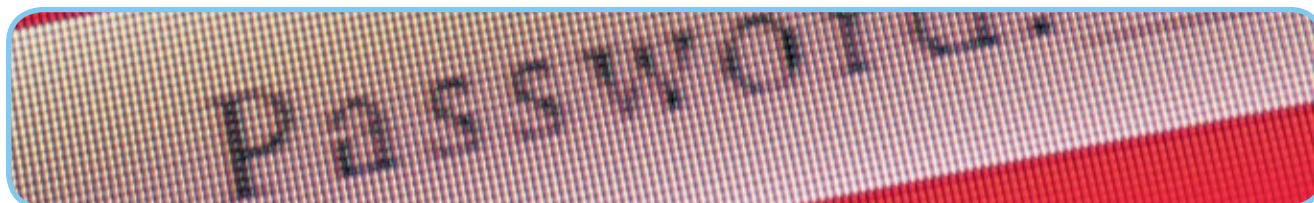
more sophisticated attacks occur. These attacks often take into account today's security measures and seek ways to work around them. For example, rootkits are designed to avoid virus scanners completely, thereby bypassing a very common and otherwise effective security control.

→ Industry analysts and security experts agree that the key to striking a balance between tight network security and network access is a layered security solution.

This guide examines five areas of network security designed to offer a layered approach.

- Gateway Security
- Server Security
- Client Security
- Mobile and Wireless Security
- Physical Security

For each security threat, we'll examine the various security vulnerabilities that are unique to that area. We'll then examine the most effective methods to mitigate the vulnerabilities. Where appropriate, multiple methods will be described, and you will be provided with decision-making criteria to help determine which method or methods would be best for your environment.



# Today, stopping threats goes way beyond virus protection.

Good thing, so do we.



There are more threats to your network and your critical data than ever. Fortunately, CDW•G has the leading security products to help you fight back. Not to mention security specialists who have worked with organizations of all sizes. So you're sure to get the right protection for your needs. And a lot less to worry about.

Protect your network from the unexpected. Call 800.808.4239 or visit [CDWG.com/security](http://CDWG.com/security)

The Right Technology. Right Away.™

CDW®, CDW•G®, CDW@work®, CDWG@work® and The Right Technology. Right Away.™ are trademarks of CDW Corporation.

# Gateway Security

### IN THIS CHAPTER:

- Firewalls
- Intrusion Prevention Systems/Intrusion Detection Systems
- Network Access Control

The idea of a solid security foundation hasn't changed much in modern computer networks from medieval Europe — keeping citizens safe from invaders with moats, solid walls and armed fortifications. You still want to keep the attacker on the outside of the wall. Although you have limited control over what happens outside the network, you can put up an effective series of barriers to help ensure that as few attackers as possible get inside. Because this defense begins at the network's gateway, we often refer to it as gateway defense.

- Gateway security is critically important and extremely complex. Organizations need complete solutions that integrate content filtering, intrusion detection and prevention, firewall and virtual private network (VPN) services, antivirus, antispam and protection against Denial of Service (DoS) attacks.

At the network gateway, there are several common defense tools and techniques. These defenses include:

- Firewalls
- Intrusion Prevention Systems (IPS)/Intrusion Detection Systems (IDS)
- Network Access Control (NAC)

The most common of these is the firewall, either dedicated or as part of a larger network access system. Many organizations

feel that a single firewall is all the protection they need at their gateway. However, there are a number of gateway defense tools that can be used. Each serves a purpose and all should be examined when deciding which defenses are the best for your network perimeter.

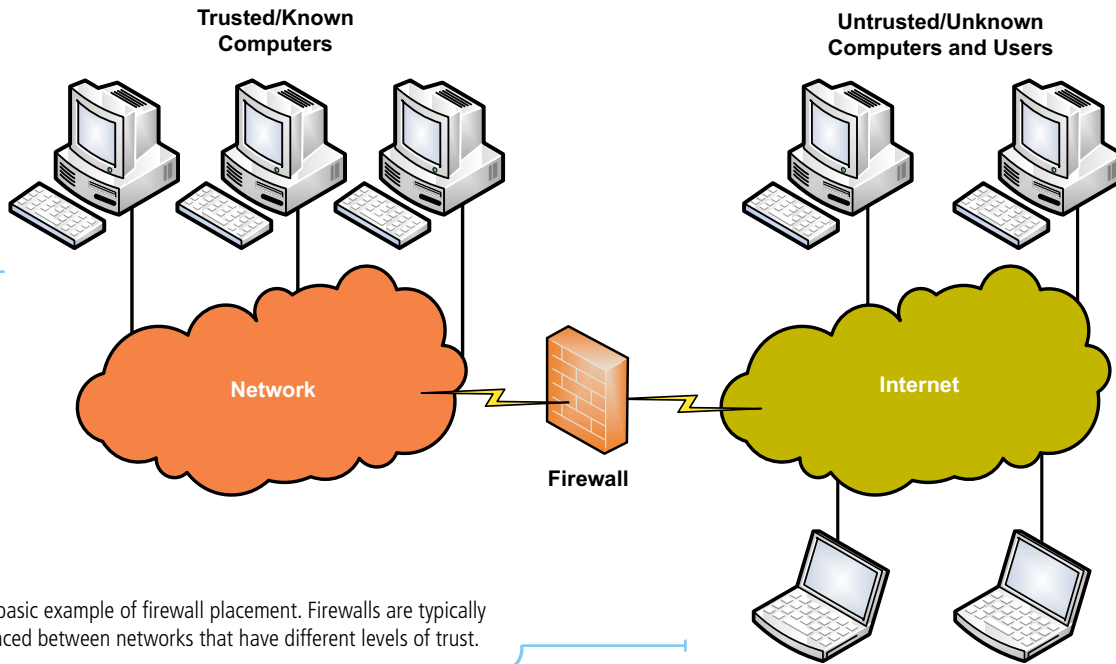
## Firewalls

At a basic level, a firewall sits between a private network and a public network (such as the Internet) and examines network traffic to determine whether the traffic should be allowed through. It's essentially a traffic cop. For example, a firewall might allow a client computer to open an outbound network connection to a Web site. But it might not allow an unsolicited inbound connection access to that computer. In this way, it helps prevent network attacks by blocking some types of traffic.

### How Firewalls Work

Firewalls are always placed between network boundaries. Their intention is to block some network traffic while allowing other traffic to flow. A basic example of firewall placement is illustrated on the following page.

This is virtually always the placement for a firewall. Note that there may be more firewalls on the internal network if there are separate zones of different trust levels. An example might be a highly restrictive firewall that separates a research-based network from the institutional network. There may also be additional firewalls placed on the untrusted side, such as those implemented by an Internet Service Provider (ISP).



Firewalls are semi-intelligent devices. They examine all network traffic that needs to pass between networks and determine whether to allow or block the traffic. They make this decision based on a set of rules.

Firewall rules can be as varied as any other decision-making system. Some older firewalls have preconfigured, unchanging rules that block common attacks. Most modern firewalls, however, start with a basic set of rules but allow the administrator to further configure and refine them to provide the desired level of security.

## Types of Firewalls

There are two main types of firewalls available today. The difference between these types is mostly a matter of how deeply they inspect the network traffic, and, as a result, how complex their rules can be. More detailed examination of network traffic consumes more time on the firewall while allowing more specific and rich rules to be enforced.

### Network-Layer Firewall

The most basic type of firewall is the network-layer firewall. This firewall examines Transmission Control Protocol/Internet Protocol (TCP/IP) packets at the protocol level. It allows examination and rules based on information found at the protocol level such as source or destination address, port number, Media Access Control (MAC) address and domain name.

This information, contained in the TCP/IP header for each packet, is easily and quickly scanned by the firewall, and the appropriate

rules can be enforced with little delay. In many cases, network-layer firewalls are powerful enough to block the majority of undesired network traffic while still allowing permitted communications to flow unhindered.

### Application-Layer Firewall

Application-layer firewalls examine the network traffic at a deeper level. Typically an application-layer firewall incorporates the functionality of a network-layer firewall and extends it by examining the data within the packet. This extended examination can enable firewall rules that are based on the content, such as allowing Web browsing (regardless of port or domain name) but blocking multimedia content. Because this examination is more thorough and more complex, it is a bit slower (depending on the rules enabled) than a network-layer firewall.

## Proper Use of Firewalls

Firewalls are useful when properly planned and implemented. A properly configured firewall can thwart the majority of attackers before they have a chance to attack any other part of the network. They are almost always the network's first line of defense against unwelcome visitors. The vast majority of organizations use them, with the 2006 CSI/FBI Computer Crime and Security Survey reporting 98 percent of respondents having a firewall in place.

Consider placing a firewall between any two networks that have a different level of trust. For many organizations, this simply means between the primary network and the Internet. But for other



organizations that have networks with differing levels of trust, you might want to implement firewalls at the boundaries of each network with different rules to help protect each network from attack. Because firewalls have become less expensive and easier to manage over the past few years, the current thinking is that having multiple firewalls is a perfectly acceptable network configuration.

## → Firewall Performance

While we describe firewalls as slower or faster, the speed differences can actually be very slight and barely measurable. Firewalls are designed to examine traffic and apply their rules as quickly as possible. So when you're deciding which firewall solution to implement, consider running tests or crunching the numbers to determine whether your specific rules will have a significant effect on throughput.

Firewalls can also be a dangerous crutch when not used properly. All too often, an administrator will purchase a hardware or software firewall, accept the default configuration and install it in the network with no further configuration or maintenance plan. In some ways, this is more dangerous than having no firewall at all. It provides the perception of absolute, rock-solid security. But the reality is that firewalls are specialized devices that must be installed and configured properly.

As with all security controls, ongoing maintenance is critical to continue the same level of security. As new exploits or organizational needs arise, the firewall administrator must maintain the systems to ensure they continue to function as desired. Although the need to regularly update the configuration is common knowledge and a regularly performed practice with malware scanning software (described later in this guide), it is also important to do so for firewalls and other security controls.

Don't leave your network security to an administrative assistant who claims to be network savvy. Small organizations with little IT support may simply use a router as a perimeter protection because they simply cannot afford an enterprise-class security solution. A router is designed to segment the network to help optimize network bandwidth and traffic control. A router is not intended to protect against attacks, although some attacks are more difficult to execute across a routed network. Employing a router in place of a firewall is a dangerous configuration, because any determined attacker or sufficiently complex automated attack can traverse the router and successfully compromise your network.

Implementing a standalone firewall device, therefore, is the preferred security configuration. Which type of implementation (software vs. hardware), location (at the ISP, on your network and so on), and how strictly to configure the firewall are all questions that you should consider when purchasing and implementing your firewall.

In addition, consider the cost of long-term ownership. Does the firewall update itself regularly? Does the firewall notify you when there is a problem? These may be features that you're looking for to simplify administration and lower the cost of the firewall.

## Reasons for Unsecured Network Access

Believe it or not, there are a number of organizations that do not implement any perimeter defenses. This probably seems absurd, as you've read over and over again that a good network defense starts with a good firewall. And that's a rule that you should not discount. But there are cases in which perimeter defenses aren't used.

One such example is at a growing number of American universities. Students are notorious for finding and exploiting network weaknesses. When you have 50,000 students looking for a way to pirate music and three network security experts to support that entire user base, this may be a losing battle.

Taking a different approach, some universities do not block ports or filter for content at the perimeter. Instead, they educate students that they have an uncontrolled, undefended Internet connection.

Students learn how to defend their own systems using local firewalls, limiting software installation and so on. The students effectively become responsible for their own security, with support from the university when requested. (Most universities embracing this type of policy provide free security software.)

Another example of a type of organization without a perimeter defense would be the Web content/development department. Many of these departments cannot activate content blocking, as their organization depends on unrestricted connectivity to function properly. There are certainly mitigations for this, such as having a separate network for sensitive data such as human resource, student/staff and payroll information. Again, these organizations inform and educate their users to ensure that they get the best security they can while still enabling them to do their jobs.

# Intrusion Prevention Systems/Intrusion Detection Systems

Although firewalls are a great foundation for preventing intrusion, their abilities are somewhat limited by the scope of their design. Firewall rules are simple and easily implemented, and the decision-making criteria utilized are very basic. Although these criteria are often sufficient to provide the desired level of gateway security, sometimes there is a need for a more advanced set of decision-making criteria. This is where an IPS/IDS comes in.

## How an IPS/IDS Works

An IPS/IDS is similar to a firewall in that they both inspect network traffic and based on a set of rules, then allow or block the traffic. An IPS/IDS, however, is far more complex than a firewall. Most IPS/IDS implementations include features such as content inspection to examine the data portion of the network traffic for certain types of data. The benefit of this type of deep inspection requires a bit of explanation.

Many common attacks have certain things in common. For example, a DoS attack may contain code that creates a specific type of network traffic. An IPS/IDS can detect this common element in otherwise normal-appearing network traffic. They can potentially defeat attacks that would otherwise circumvent firewalls and other perimeter defenses. This detection, called pattern analysis, is similar to how virus scanners work. They identify a pattern common to a category of threat (or a specific, known threat) and when such an element is identified, it is mitigated.

A significant feature of pattern analysis-based IPS/IDS is that it can protect against zero-day attacks. This is where a previously unknown vulnerability is identified and exploited before a mitigation is available. If the zero-day attack follows an identified pattern (as many do), the IPS/IDS will block the attack, even if that specific vulnerability has not yet been identified. This has been seen in the corporate security setting over and over again. The benefit of such adaptive, preemptive defenses cannot be understated.

At its heart, an IPS/IDS is a combination of a firewall and a network monitor. It not only contains firewall-like rules and permissions but is also capable of monitoring a network for traffic abnormalities such as a broadcast storm or a DoS attack. Although this may make it seem like the IPS/IDS may replace the firewall in the future, the IPS/IDS isn't designed for widespread use. It is slower than a comparable firewall because of the examination it must perform. It is also more difficult to maintain and configure due to its complexity. Thus, although having an IPS/IDS is helpful and can help mitigate many attacks, it's not for every organization.

## Proper Use of IPS/IDS

The location of an IPS/IDS is similar to the location of a standard firewall. Most organizations implement only one or a handful of IPS/IDS devices at the perimeter between the network and the Internet. This more limited implementation is largely due to the cost of obtaining, implementing and maintaining the IPS/IDS, which is more costly than a basic firewall. In addition, there is often little need for the more detailed IPS-specific examination of network traffic within some organizations.

As with a firewall, proper installation and maintenance of an IPS/IDS is critical to having it provide the proper functionality and security. Alternatively, consider identifying IPS/IDS specialists within the IT organization and training them so that they have the skill set necessary to perform these tasks in-house. This expertise can often help improve security by proactively securing the network and responding quickly to zero-day attacks.

## Network Access Control

Network access control products are similar to firewalls and IPS/IDS in that they allow or disallow network access. However, NAC differs from these other security devices because it provides user-focused access control: it grants or denies network access based on who the user is. The identity of or the "who" of an end user is determined by more than merely a username.

## Determining the "Who" of Access Control

Determining access control under NAC, or "who" an end user is, has three parts: authentication, endpoint-security assessment and network environmental information. Access-control policies are set using a combination of these three elements.

First, NAC authentication is identical to that used with other applications. As covered in Chapter 3, authentication is the process through which the user asserts his or her identity, which is then validated by the server.

Second, endpoint-security assessment is the foundation of NAC deployment and also the most complex component of NAC. Basically, endpoint-security assessment calls for the security postures of all connecting systems (servers, desktop and notebook PCs) to be part of the access control policies. For instance, if a connecting PC is not equipped with the required antimalware software, a different access control policy should be applied to that user than that applied to a PC running updated antimalware software.

Third, network environmental information dictates access based on a user's location. For instance, if a user is connecting via a wireless network, access may be more limited than it would be if the connection was being made from within the building.





## Chapter 3

# Server Security

### IN THIS CHAPTER:

- Authentication and Authorization
- IP Security
- Content Filters

In most organizations, a server infrastructure exists as a collection of server-based computers. These computers host a variety of functions that support users and the infrastructure, including (but certainly not limited to) these functions:

- Network Functionality (for example, Domain Name System [DNS] and Dynamic Host Configuration Protocol [DHCP])
- Data Repositories
- E-mail Servers
- Web Servers
- Authentication and Authorization Servers
- Remote-Access Servers

Many of these functions are critical and their loss would cause lost productivity, legal liability or a variety of other negative ramifications. That's why most IT organizations protect their servers so carefully.

Server infrastructures can be a double-edged sword. On the one hand, IT professionals can identify those servers that provide critical business functions and maintain them as such. They may employ regular online updates, online backup systems and constant security updates.

On the other hand, attackers know that servers are the keys to the kingdom. Attackers usually target servers as their most coveted prize because servers either have the information they're looking for or can access it. So although gateways are certainly the first place an attacker has to fight through, servers are usually their first target.

Luckily, there are a number of defenses that can be implemented on servers that not only protect the server but, by proxy, the entire organization.

→ Servers can usually run client-oriented software, for example, Windows Server 2003, running software such as Microsoft Office 2007. As a result, you should consider most client security controls (discussed in Chapter 4) as appropriate for your servers as well. For instance, implementing a self-updating malware scanner is not mentioned in this section. But it's just as important on servers as it is on clients.

## Authentication and Authorization

Usually we take for granted that people are who they say they are. If you meet someone at a party and he introduces himself as Mike, you assume that person is Mike. Why would he lie? Social interaction and computer-based security controls are, in this regard, completely opposite. When a user claims he is Mike, that claim must be validated before access can be granted. Without validation, Mike has access to virtually nothing.

### Authentication

This is the process through which the user asserts his or her identity and the server validates that identity. A user must supply some

information along with the user's identity assertion that a server can use to positively identify the user. Historically, we use a secret password with the user name. Although modern authentication systems can use other information such as smart cards, fingerprints and retinal scans, the basic process of authentication is the same.

## Authorization

This is closely tied to authentication. Once the user proves her or his identity, the next step in the access control process is determining whether the user has permission to access whatever it is they're trying to access. That process of comparing the authenticated user's identity with the permissions for an object is called authorization. Together, authentication and authorization make a complete access control model.

Virtually all authentication and authorization data is kept on servers. In Windows, for example, this data is kept on a domain controller that is part of the Windows authentication structure known as Active Directory (AD). Whenever an authentication or authorization request is received by any computer within the AD infrastructure, the request is passed to a domain controller for trusted verification.



Therefore, keeping those domain-controller servers secure is critical to ensuring the security of the network. Compromise of a domain controller, whether logical or physical, allows the attacker to impersonate any user or computer on the network and effectively grants the attacker access to any data or object.

To help prevent this type of attack, domain-controller servers should be protected both logically and physically. Physical security is described in Chapter 6 of this guide. Logical security controls such as firewalls, malware scanners and gateways are discussed throughout this guide. The important thing to remember specifically about servers is that they will almost always be the primary target of an attacker. They should receive the appropriate amount of protection to ensure that they are resilient to as many attacks as possible.

## IP Security

When data is transmitted across any network, it is usually broadcast only on the appropriate network segments. This data, at its basic level, takes the form of electrical signals sent along a cable. If you're familiar with the behavior of electricity, you know that these signals can be observed anywhere along the cable (with or without tampering).

The potential for data eavesdropping or tampering is enormous. For example, consider a bank with one headquarters and ten remote branches, all in Miami. An attacker can tap into the network cable at the headquarters by any of the following means:

- Finding an available network jack in an empty cubicle
- Finding an available network jack in the unsecured lobby
- Accessing the wireless network from outside the building
- Renting space within the building and cutting a small hole in a common wall
- Accessing the building's wiring closet (from inside or outside)

By default, data is not protected in transit from one computer to another. That's because computer networking was not designed with security in mind. The original designers of Ethernet and TCP/IP did not consider that their inventions would carry financial data, medical information and nuclear weapons secrets.

Fortunately, there are solutions available today to help protect data in transit. The most common and frequently used solution is IP Security (IPSec). IPSec offers several options:

- Encrypt the data portion of network packets
- Digitally sign the entire network packet (including the header)
- Encrypt the data and sign the entire packet

IPSec is extremely flexible in its implementation. It can be used to protect traffic between remote locations, encrypting traffic while transmitting over unsecured networks. This is often implemented as router-to-router IPSec.

It can also be enforced on a server-by-server basis, with many current operating systems (OS) such as Windows Server 2003 and Windows Server 2000 fully supporting IPSec communication. In this way, you can protect both client-server and network-network communications.

Like most security controls, IPSec comes with a price. The price is primarily network performance. The act of encrypting and decrypting network traffic, plus the associated administrative tasks such as establishing secret keys and negotiating cryptographic protocols, can seriously affect network performance.

One large organization recently decided, without examining performance implications, to use IPSec throughout its network to protect all communications. It took less than 24 hours for them to reverse their position and back IPSec out of its systems before conducting an appropriate feasibility study.

- One common myth about IPSec is that it creates a large amount of additional network traffic. Nothing could be further from the truth. The initial IPSec connection requires some communication between the two computers, but this is minimal (often less than 30 packets). Once the connection is established, the additional data sent when using IPSec is just a few bytes per packet.

Another cost of IPSec is the result of its design. IPSec encrypts data so that only the sender and recipient can read it. So what happens if you have content filters or stateful inspection firewalls that are designed to examine the content of these network packets? They fail. Because they don't have the private key, these intermediate systems cannot thoroughly inspect the traffic. Although this isn't necessarily a reason to avoid IPSec, it is a consideration.

## Proper Use of IP Security

As a general rule, consider using IPSec to protect important traffic on your network and between physical locations where the intermediate connection may not be secure. If performance is a concern, use IPSec-enabled network cards or routers to offload the encryption and decryption tasks to these dedicated devices. Doing so allows you to implement IPSec without having to upgrade every component in your infrastructure. When implemented appropriately, IPSec is a strong security control that is difficult to defeat.

## Content Filters

Most organizations today have their own internal e-mail infrastructure. Many of them also implement other communications systems such as Instant Messaging (IM) and peer-to-peer (P2P) collaboration software such as Microsoft Groove. These technologies have had a tremendous impact in recent years, greatly simplifying collaboration and globalization efforts. But they come with a price, which is not limited to the price of lost productivity.

E-mail, IM and P2P communications are all popular replication systems for malicious software or malware. They can also enable other security threats such as phishing and social engineering. This is the reason that many organizations have disallowed P2P and IM systems. But that's not always possible and can sometimes cause more harm in lost productivity.

Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. In most cases the attacker never comes face-to-face with the victim.

- Attacks that previously targeted organizations' e-mail systems are rapidly shifting to IM and other collaboration platforms. Organizations need integrated security solutions for all e-mail and messaging applications and for all client devices.

Content filters examine network traffic as it flows to determine whether it contains an attack. Today there are a number of content filters designed specifically for different types of communication including e-mail, IM and P2P collaboration systems. These content filters are able to prevent malicious use of systems while still enabling the rich work environment that helps boost the productivity of today's tech-savvy user.

If you only use e-mail for communication, consider an e-mail-specific content filter. Often these systems come with malware scanners and phishing scanners, as well as flexible rules that help you enforce security policies on e-mail with little performance impact.

## 3 CHAPTER

Threats to  
network security  
are increasing.  
Fortunately, so are  
the number of ways  
CDW•G can help.



The Right Technology.  
Right Away.™

# And this is just the first network task of the day.



At CDW•G, we understand how messy supporting your networking environment can be. We also know that you need a way to protect all of the equipment involved. For some peace of mind, look to CDW•G to help solve your networking woes. We offer warranty contracts to keep your software and support options current — and the experts to help you figure out how to best reinforce your networking environment.

Support your network. Call 800.808.4239  
or visit [CDWG.com](http://CDWG.com)

The Right Technology. Right Away.™

CDW®, CDW•G®, CDW@work®, CDWG@work® and The Right Technology. Right Away.™ are trademarks of CDW Corporation.



## Chapter 4

# Client Security

### IN THIS CHAPTER:

- Malware
- What to Do About Malware

In early computing, virtually no importance was placed on client security. All security efforts were focused on server hardening, such as domain infrastructure, server-based data encryption and role-specific security such as database storage. Only 10 years ago, most client computers didn't have a virus scanner installed.

Today virtually every computer has a virus or malware scanner installed. This change from past behavior is due in part to the behavior of attackers. They now see that unsecured client computers can provide leverage to conduct further and more successful attacks against the rest of an organization.

Consider that an administrator may configure servers and access sensitive server-based data from his or her client computer. Rather than attacking the well-protected servers, an attacker can compromise the client computer and install software that monitors and reports on the administrator's activity. This can lead to an unwanted server compromise simply by attacking the right client.

## Malware

Computer viruses have been around for decades. They are the most common form of malicious software (or malware). Originally written and distributed as proof-of-concept code, today they take on much more sinister motives. Some virus writers are paid to spread their code. Others conduct attacks against opposing political or religious organizations. And some attack for no other reason than the challenge. Malware attacks clients in a variety of forms: viruses and worms, Trojan horses, spyware and rootkits.

## Viruses and Worms

Viruses are autonomous software packages that have several characteristics: They spread from computer to computer, they often mutate themselves as they spread, and they usually cause some harm to the computer or the user when they execute their payload (or bomb). Most viruses infect systems by copying their code into other files and then continuing to spread, both on the local host and throughout any network that is reachable by the host.

Worms are, in today's security context, nearly analogous with viruses. Their infection and propagation methods are nearly identical, with the exception that most worms spread by copying their own files without mutation or infection of other files. Their distribution methods and payloads can be the same as viruses.

Although worms are sometimes considered less dangerous because their payloads tend to be less destructive, they are not. Because viruses and worms are so similar, for the remainder of this section, the definition of worm also includes virus.

Virus behavior and countermeasures are well understood in today's computing environment. Through years of study, experimentation and development, effective virus scanners are available. Virus scanners can be installed at several points in your network: host, internal network, perimeter network or server (for example, an e-mail server).

Most virus scanners require a signature file to help them identify all known viruses. But with current implementations, most virus scanners periodically download and install new signature files

Continued on page 24



# Stop hackers at the door. Protect your network's gateway.

**A FIREWALL INSTALLED AT YOUR NETWORK'S GATEWAY** is your first and foremost line of defense against viruses, worms and other programs that cause data loss, downtime and bandwidth consumption.

Your firewall options might require more technical knowledge to secure your network properly, depending on the needs of your organization.

What else do firewalls do besides screen e-mail and Web requests? A general firewall appliance should have the following minimum functions:

- **Stateful Packet Inspection (SPI)** — SPI inspects packets of network headers and blocks any claiming to be a solicited response.
- **Network Address Translation (NAT)** — NAT is a technique that hides the IP address of your internal systems by replacing them with a single IP address.
- **Monitoring and Logging** — Keeping records of attacks is important. It will help you analyze your security needs and provide you with feedback on the performance of your firewall.

Your firewall options might require more technical knowledge to secure your network properly, depending on the needs of your organization. More sophisticated firewalls offer antivirus, antispam, antispyware, content filtering and Virtual Private Network (VPN) services.

This is where CDW•G security specialists can assist you in choosing and configuring your firewall. Working together with your dedicated CDW•G account manager, our vendor-certified security specialists can help you get the right gateway security solution. Call your account manager or visit [CDWG.com/securityguide](http://CDWG.com/securityguide) for more details.



The next step in protecting your network's endpoints and clients, an intrusion prevention system (IPS) combines the capabilities of a firewall with the deep packet inspection of intrusion detection.



## CALL FOR PRICING

### Cisco® IPS 4200 Series

Cisco® IPS 4200 Series sensors offer significant protection to your network by helping to detect, classify and stop threats, including worms, spyware/adware, network viruses and application abuse. Using Cisco IPS Sensor Software Version 5.1, the Cisco Intrusion Prevention System (IPS) combines inline intrusion prevention services with innovative technologies that improve accuracy. As a result, more threats can be stopped without the risk of dropping legitimate network traffic. The new software release includes enhanced detection capabilities, as well as improved scalability, resiliency, and performance features.

The Cisco IPS solution helps organizations stop more threats with greater confidence through the use of the following:

- **Accurate online prevention technologies** — provides unparalleled confidence to take preventive action against a broader range of threats
- **Multi-vector threat identification** — protects your network from policy violations, and anomalous activity through detailed inspection of traffic in Layers 2 through 7
- **Unique network collaboration** — enhances scalability and resiliency through network collaboration, including efficient traffic-capture techniques, load-balancing capabilities and visibility into encrypted traffic

CDWG 741806



888.510.4239  
[CDWG.com/securityguide](http://CDWG.com/securityguide)





Information system breaches are a major concern — often affecting Web, e-mail and database servers — which can result in millions of dollars lost, stolen data or information otherwise unaccounted for.

### **The challenge: securing the virtual private network (VPN)**

It is paramount to ensure that the VPN does not become a conduit for network attacks such as worms, viruses, spyware, keyloggers, Trojan horses, rootkits or hacking. Secure Socket Layer (SSL) VPN deployments enable universal access from both secure and non-network-managed endpoints, as well as the ability to extend network resources to diverse user communities.

With additional remote-access and remote-office VPN users, come more open common security points. All too often, VPNs are deployed without proper inspection and threat mitigation applied at the tunnel termination point at the main office location, thereby allowing malware from remote users to infiltrate the network and spread.

Cisco Systems® offers unique integrated security solutions that allow an organization to protect itself against information theft from both external and internal sources. A Cisco Self-Defending Network integrates security intelligence into the network, protecting valuable information while using the existing network infrastructure and containing the total cost of ownership.

### **Cisco® ASA 5540 VPN Edition Adaptive Security Appliance**

**For 1000 concurrent SSL VPN users**

The Cisco® ASA 5540 VPN Edition Adaptive Security Appliance enables organizations to gain the connectivity and cost benefits of Internet transport without compromising the integrity of operational security policies. By converging IPSec and SSL VPN (Cisco WebVPN) services with comprehensive threat defense technologies, this appliance delivers highly customizable network access tailored to meet the requirements of diverse deployment environments, while providing a fully secured VPN with complete endpoint and network-level security.

CDWG 1013737

Cisco ASA 5500 Series Content Security and Control Services Module (CSC-SSM) CDWG 984452

**CONTACT YOUR  
SECURITY  
SPECIALIST  
FOR A QUOTE**

### **Cisco ASA 5510 Adaptive Security Appliance with CSC-SSM-10 Module powered by Trend Micro™**

**With 50-user Antivirus, Antispyware and 1-year Subscription Service**

The Cisco ASA 5510 Adaptive Security Appliance with CSC-SSM-10 Module powered by Trend Micro™ combines comprehensive malware protection with advanced traffic and message compliance for Cisco ASA multifunction security appliances. The result is a powerful solution that provides strong protection and control, stops network threats including viruses, worms, spyware, spam and phishing, controls unwanted visitors and Web content while reducing the operational costs and complexity of deploying and managing multiple point solutions.

- Combines comprehensive malware protection with advanced traffic and message
- Delivers threat protection and content control at the Internet edge providing comprehensive antivirus, antispyware, file blocking, antispam, antiphishing, URL blocking and filtering, and content filtering — all available in a comprehensive easy-to-manage solution

CDWG 941654



# Keep your network safe — your organization depends on it.

## THREATS TO THE NETWORK

have increased since the introduction of the Internet and multiplication of personal PCs. Nowadays, any computer or network that is connected to the Internet is at risk.

Web servers and e-mail servers are particularly appealing targets of attackers. This is because e-mail and Web servers must allow a certain amount of traffic through in order to perform their functions. These "open doors" to traffic can often be exploited. In addition, Web and e-mail servers are very complex, and the more complex the code is, the more bugs it will have. It is therefore important that organizations take steps to secure them.

Protect your servers:

- Install a firewall in addition to your router to protect from unwarranted intrusion
- Modify and lock down a standard default installation of an operating system
- Be sure to only authorize valid users to access the system
- Ensure that all computers and notebooks are kept up to date with the latest patches and updates

Working together with your dedicated CDW•G account manager, our vendor-certified security and VSL specialists can help you get the right server security solution that is appropriate to your size organization. Call your account manager or visit [CDWG.com/securityguide](http://CDWG.com/securityguide) for more details.

Organizations are always looking for ways to both protect their users and ensure the confidentiality of their networked resources. As IT staffs research options, they are learning why 3Com® secure converged networks are praised for their high-performance and high-value solutions.

CONTACT YOUR  
SECURITY SPECIALIST  
FOR A QUOTE



3COM

## 3Com® X5 Unified Security Platform

The 3Com® X5 Unified Security Platform is built on best-of-breed Intrusion Prevention System (IPS) technology with the added functionality of firewall, VPN, bandwidth shaping and Web content filtering. It is the only integrated security platform with true IPS protection providing preemptive vulnerability protection and zero day threat prevention through the Digital Vaccine® service.

In addition to the IPS functionality, the 3Com X5 Unified Security Platform includes IPsec VPN, a stateful packet inspection firewall, Web content filtering and policy-based traffic shaping, which provides fine grain bandwidth usage and control for both inbound and outbound traffic streams.

25-user CDWG 1116673

Unlimited-user CDWG 1116674



888.510.4239  
[CDWG.com/securityguide](http://CDWG.com/securityguide)

## 3Com® Switch 4500G 10/100/1000BASE-T switches

The 3Com® Switch 4500G family delivers voice-optimized quad-speed performance with advanced features and PoE for organizations seeking a secure, converged network. Layer 2 switching with dynamic Layer 3 routing make the 3Com Switch 4500G ideal both for wiring-closet workgroup connectivity and as the core for medium-size enterprises.

- Supports clustered stacking in any combination up to 32 units for simplified administration
- Four of the ports are dual-personality, operating either as 10/100/1000Mbps or SFP-based fiber
- Accommodates up to four extra optional 10GbE high-speed links, enabling connectivity to a core network or to high-performance servers
- Security features include IEEE 802.1X network login, SSH/SSL encrypted device login and Access Control Lists (ACLs)
- Lifetime warranty

24-port **\$2271.30** CDWG 1090632    48-port **\$3491.24** CDWG 1090635



SSH/SSL encrypted device login



CDWG 1090635



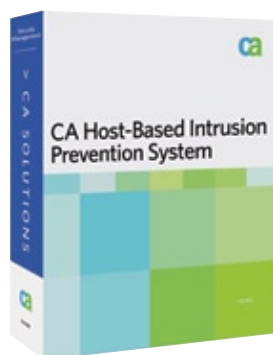
## APC® Smart-UPS® 1000VA USB and Serial RM 2U 120V

Performance power protection for servers and voice and data networks

- 1000VA, 670-watt, six outlets
- Up to 30 minutes at half-load<sup>1</sup>
- Hot-swappable battery
- AVR

**\$548.62** CDWG 469105

<sup>1</sup>Runtime may vary due to load and battery conditions



## CA Host-based Intrusion Prevention System

CA HIPS blends standalone firewall and intrusion detection and prevention capabilities to provide centralized, proactive threat protection to counter online threats. This combination offers superior security access control policy enforcement, easy intrusion prevention management and deployment from a central location via a single, intuitive console to enhance your endpoint protection.

- Reduces the risk of downtime
- Improves cost and operational efficiencies
- Ensures service continuity and helps keep your critical IT assets up and running
- Protects assets
- Facilitates compliance, monitoring and investigations

**100-249 users**

1-year License<sup>2</sup> **\$23.18** CDWG 1151024    3-year License<sup>3</sup> **\$41.99** CDWG 1151025



<sup>1</sup>Includes one-year Enterprise Maintenance (24 x 7 technical phone support and upgrade protection) <sup>2</sup>Includes three-year Enterprise Maintenance (24 x 7 technical phone support and upgrade protection)

# Layered Lockdown

Organizations keep information safe by implementing security measures for mobile technology.

Staking out a drug deal, a police officer inputs intelligence into the database on his notebook as his partner steers the cruiser. The database produces a list of potential suspects. The cruiser pulls into a parking lot and the officers show a mugshot to a witness. Bingo. The witness identifies him, and around the corner, the officers find the suspect and make the arrest.

No, it's not an upcoming episode of *Law & Order*, but rather a real-life case handled by Daytona Beach police officers, who, like their peers around the country, have woven mobile technology into the very fabric of police work.

"An officer without a laptop is like an officer without a gun," says Grady Meeks, IT director for the city of Daytona Beach, Fla.

In fact, mobile technology has become indispensable throughout government agencies and educational institutions. Firemen race to emergency scenes checking maps and floor plans on GPS (Global Positioning System)-equipped tablet computers and students give PowerPoint presentations with notebook PCs from their school's mobile technology carts. But, with the new possibilities offered by mobile technology come significant risks.

"Nowadays, we're carrying around a lot of information," says William Pelgrin, director of New York State's Office of Cyber Security and Critical Infrastructure Coordination. "We have devices that have gotten smaller and smaller. The challenge is how do you make sure they don't fall into the wrong hands?"

There's no such thing as a foolproof security measure. But, says Pelgrin and other security professionals around the nation, organizations can go a long way toward keeping their mobile devices safe by employing a combination of precautions.

"Security in layers, in depth, is much better than flatline," Pelgrin says. "You don't want to put all of your eggs in one basket."

## Get Smart

In a recent six-month period, 85,619 mobile phones, 21,460 PDAs and 4,425 notebooks were left behind in Chicago taxis. And that's at just one taxi cab company.

Those figures — from a study by mobile data security firm Pointsec Mobile Technologies — shine a spotlight on the biggest threats to portable technology: careless users.

To combat that threat, organizations need strong mobile technology policies and user education, Pelgrin insists. His office holds monthly workshops with agency information security officers from throughout New York state to review policies and share best practices.

Step one of any mobile security policy should be to determine what types of portable devices can be permitted, who can use them and for what purposes. If a wireless user doesn't need a PDA to do his job, he shouldn't be given one, Pelgrin says. "More is not always better."

The staff at the city of Daytona Beach have a personal stake in security because if their user names are attached to a security breach on a city network, they're held responsible.

"The biggest issue you have is with folks not wanting to comply, but when you hold them accountable, it makes it a lot easier," Meeks says.

Once usage policies are established, organizations need to take an inventory of the equipment they have.


New York policy dictates that state staff members must either carry their mobile devices with them or store them securely. For instance, notebooks should be carried onto airplanes rather than checked in with luggage, and they should be stored in a safe or fastened with a security cable when left in hotel rooms.

While security policies should err on the side of caution, organizations shouldn't go overboard, warns Pelgrin. If security prevents users from doing their jobs, it defeats its purpose. Security policies, he says, need to be flexible and account for workplace realities. "I'm not a big believer that security wins in every case," he says.

## Strong Passwords

New York's cybersecurity office sets the example for secure network practice. Whenever notebook computers are used outside of the network, they must be scanned to ensure they're as safe as the other devices on the network before they're allowed back in.





What may seem an obvious security measure is actually one that many organizations struggle to keep under control. There are still plenty of people who use their children's names or "password" as passwords or write them on notes stuck to their computers.

Many organizations require wireless users to use a combination of capital and lowercase letters and digits for their passwords, explains Mark Williams, CEO of Lilburn, Ga.-based Access Anyplace, a wireless Internet access provider. Others employ double authentication, using a secure key or some other physical component that only works with a password.

### VPN Value

With desktop computers, the focus is on keeping the network secure. But when devices leave the office and connect to the Internet using other networks, those computers are literally out in the wild.

One of the best defenses, other than a firewall, is for organizations to require that remote users connect to the network using a virtual private network (VPN). Information traveling over that connection can be encrypted using Internet Protocol Security (IPSec), which must be installed on each device, or Secure Sockets Layer (SSL), which is built directly into Web browsers.

Mobile telephones and PDAs, which are even more portable than notebooks, also need strong security. Different wireless carriers employ an array of security solutions to protect their devices as they access the Internet.

For instance, Sprint Nextel offers a Sprint Mobile Security package, which contains a VPN, password protection, encryption for individual files or an entire device, antivirus, a firewall and central management capabilities. Sprint Mobile Security can also lock and delete data if a device is lost or stolen.

"With Sprint Mobile Security, organizations have access to the highest level of security expertise, tools and customer service to ensure complete protection for their unique and evolving enterprise security needs," says Barry Tishgart, director of product marketing for Sprint.

Access control is also critical for mobile devices, Pelgrin says. Workers should only be able to access the applications that are necessary to do their jobs, he explains. Mobile users should be taught to stick to trusted secure wireless networks when they're not in the office.

Intrusion prevention/detection systems (IPS/IDS) can go a long way toward helping organizations keep unwanted visitors off their networks. Daytona Beach uses Web-filtering software to limit users' exposure to viruses and other threats on the Internet. And the city monitors its networks so that if anything unusual appears, IT can shut it down immediately. "We keep a pretty tight grip on it," Meeks says.

### Ready for Attack

Organizations can build layers of security around themselves and their equipment, but Andrew Krcik, vice president of marketing for PGP Corp., a Palo Alto, Calif.-based data encryption firm, warns, "There's never been a fence built that somebody couldn't penetrate."

Even if mobile equipment is lost or stolen, or a network penetrated, data can't get into the wrong hands if it's encrypted. Some operating systems have begun to include varying degrees of built-in encryption.

Another defense for devices or networks that have been compromised is to automatically configure them so that after a certain number of failed log-in attempts, all the data is erased and the hard drive is reimaged, explains Williams.

Important data stored on portable devices should be regularly backed up onto password-protected or biometric external hard drives, disks, USB (Universal Serial Bus) drives or a network-based backup system. Those devices should always be kept separate from the equipment they're backing up.

Essentially, says Pelgrin, "Security is a process. It consists of layers. We can't ever sit back and say we're secure, because the landscape is constantly changing."

## The Importance of Physical Security

"For medium-sized organizations, buying notebooks ranging from \$1000 to \$2000 each can be a big expense and they want to protect it," says Jeremy Weiss, network security specialist at CDW•G.

Sturdy computer bags and carrying cases will help protect notebooks from being banged into, dropped or knocked about. APC, Kensington, Targus, Tripp Lite and others offer a variety of options, including some as stylish as they are functional.

Basically, employees should treat notebooks like they would any valuable property. "Don't leave your notebook in plain sight in public places, especially the front seat of your car," comments Michael Day, chief technical officer at IT consultancy Currid & Company.

Alarms and cable locks are available from such vendors as APC, Kensington, PC Guardian and Targus. While these won't stop the determined thief, they'll deter casual opportunists. Newer locks that fit in the video port will make it hard to take the computer without damaging it.

To help recover computers that go astray accidentally, consider "Reward For Return" label services, such as StuffBak. "We recommend a 'PC low-jack' service that helps mitigate the risk if the unit is lost or stolen," says Weiss.

# The best time to think about the security of your network is before it's breached.

## TODAY, NETWORK SECURITY IS CHANGING.

Threats can come from any direction — allowing guests to access the network, accessing personal e-mail on network servers or even letting your teenager do homework on your organizational notebook. Each of these represents a risk that could compromise your network's security.

Client security is a key component in an overall defense strategy. Simply put, client security should incorporate a software and hardware strategy to protect all endpoints (desktops, notebooks and mobile devices) from a variety of threats. Best-practice organizations place an emphasis on standards, conduct a thorough and ongoing analysis of systems, and invest in tools and policies that provide maximum protection.

Protect your clients:

- Keep antivirus, antispyware and antispam up-to-date
- Train employees to use systems effectively and safely
- Consider installing an intrusion detection/intrusion prevention system
- Adopt a strict security policy

CLIENT SECURITY SHOULD  
INCORPORATE A SOFTWARE  
AND HARDWARE STRATEGY TO  
PROTECT ALL ENDPOINTS.

Working together with your dedicated CDW•G account manager, our vendor-certified security and VSL specialists can help you get the client security solution that is appropriate for your organization. Call your CDW•G account manager or visit [CDWG.com/securityguide](http://CDWG.com/securityguide) for more details.



888.510.4239  
[CDWG.com/securityguide](http://CDWG.com/securityguide)

## McAfee



### McAfee® Total Protection for Enterprise — Advanced

A single solution with a single console, McAfee Total Protection for Enterprise — Advanced has been engineered from the ground up to reduce the complexity of managing enterprise security.

Includes:

- Network access control
- Host intrusion prevention
- Antispyware
- Antispam
- Antiphishing
- Antivirus
- Firewall

101-250 user license<sup>1</sup> **\$55.99** CDWG 970155

<sup>1</sup>Licensing starts at 5 nodes; Maintenance includes 24 x 7 technical support, upgrade protection and virus definition updates; call your CDW•G account manager for details



### CALL FOR PRICING

#### PGP® Whole Disk Encryption for Enterprises

Comprehensive mobile security for notebooks, desktops, external drives and USB Flash drives

- Provides secure, comprehensive disk encryption that is nonstop and user-transparent
- Encrypts everything on the hard disk, including data files, system files, temporary files and applications data
- Enables you to quickly and cost effectively provide powerful data security, immediately safeguarding sensitive information from unauthorized access
- Complies with existing and emerging industry and government regulations for information security and partner data protection requirements





[Contact your security specialist  
for a quote]

### Juniper Networks Secure Access 2000 SSL VPN security appliance

The Juniper Networks SA 2000 enables medium-sized organizations to deploy cost-effective remote and extranet access, as well as intranet security. From several different access methods, it enables everything from Web application to high performance network-layer access. Administrators can restrict access to different users, based on the resources they require. The SA 2000 requires no client software, server changes, or DMZ build-out and minimal ongoing support. CDWG 846060



[Contact your security specialist  
for a quote]

**Stops spam, viruses and phishing attacks**



### SonicWALL Email Security 400<sup>1</sup>

Stop e-mail threats at the SMTP gateway

- Powerful, easy-to-use inbound and outbound e-mail threat management
- Stops spam, viruses and phishing attacks
- Prevents leaks in confidential information
- Stops violation of regulatory compliance laws
- Ideal for medium- or large-sized networks

750-user license CDWG 1044154

<sup>1</sup>SonicWALL Email Protection Subscription required; call your CDW•G account manager for details



**Includes one-year antivirus, antispam  
and content filtering services**



### WatchGuard® Firebox® Core™ X750e UTM Bundle

A complete Unified Threat Management Solution for medium-sized organizations

- Delivers a comprehensive upgradeable security solution, integrating multiple security functions including proactive true zero-day protection
- Includes an intuitive management interface with real-time monitoring and reporting
- Bundles the appliance and one-year subscriptions to Gateway AntiVirus, spamBlocker, WebBlocker and LiveSecurity® Service

**\$4612.43** CDWG 973449

# Travel with confidence.

## Your wireless network is secure.

**AS WORKERS BECOME MORE MOBILE**, organizations must be aware of emerging threats that target notebooks, cell phones, BlackBerry handhelds and other mobile devices. Common security threats include data leakage, productivity loss and liability. According to the Privacy Rights Clearinghouse, 56 potential breaches of personal information that involve mobile devices — typically stolen or lost — from Jan. 1 to Oct. 24, 2006, involve the personal data of at least 31.68 million people. And that doesn't count breaches of organizational information.

Protect your mobile workforce and your network:

- A VPN appliance doesn't supply enough security on its own. Be sure to install a firewall with an Intrusion Prevention System (IPS).
- Install client antivirus or personal firewall software on mobile devices.

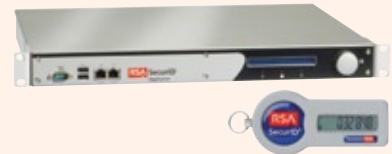
Common security threats include data leakage, productivity loss and liability.

- Do not store important company data on mobile devices. Keep data stored on servers in a safe, secure location.
- Encrypt the data on each device as well as connections back to the main network.
- Ensure that each device is password protected as well as encrypted.
- Develop and enforce a security policy for remote devices.

Working together with your dedicated CDW•G account manager, our vendor-certified security specialists can help you get the right mobile security solution that is appropriate to your organizational size. Call your CDW•G account manager or visit [CDWG.com/securityguide](http://CDWG.com/securityguide) for more details.

**RSA**

The Security Division of EMC



### CALL FOR PRICING

#### **RSA® SecurID® Appliance with 10 Tokens<sup>1</sup>**

- Offers strong two-factor authentication for secure remote access
- Scalable from 10 to 50,000 users to meet your organization's needs
- Delivered as a streamlined, purpose-built rack-mountable hardware appliance, preloaded with award-winning RSA® Authentication Manager software

RSA SecurID Appliance Bundle 10-user  
CDWG 854205

**ca**



#### **CA Integrated Threat Management r8**

The CA Integrated Threat Management r8 solution combines best of breed eTrust® PestPatrol® Anti-Spyware with eTrust Antivirus and extends the functionality with a single integrated management console.

100-249 user upgrade license<sup>1</sup>

**\$27.00** CDWG 922434

100-249 user license<sup>1</sup>

**\$38.00** CDWG 922428

<sup>1</sup>Includes 1-year Value Maintenance (technical phone support and upgrade protection)



888.510.4239  
[CDWG.com/securityguide](http://CDWG.com/securityguide)



More and more, organizations are relying on increased productivity from their mobile workforce as a key component of the growth/production strategy. As this reliance increases, so does the need to provide mobile and remote users with access to operational resources such as e-mail, files, intranets and applications — without compromising network security.

Now there's a secure, clientless remote access solution that allows your mobile users to be more productive wherever they go. The SonicWALL SSL-VPN 2000 is simple to deploy and easy to manage.

### SonicWALL SSL-VPN 2000

- Securely access confidential information and other network data utilizing a standard Web browser
- Clientless, secure remote access — no fat client to pre-install and maintain
- No per-seat license fee
- Integrates alongside almost any existing firewall

**\$1759.58** CDWG 840778



### McAfee® ePolicy Orchestrator®

#### Centrally manage system security

Coordinate your defense against malicious threats and attacks with McAfee® ePolicy Orchestrator®. As your central security management hub, it helps you keep protection up-to-date, configure and enforce protection policies and monitor security status. Do it all from one centralized console.

101-250 user license<sup>1</sup> **\$12.99** CDWG 694653

<sup>1</sup>Call your CDW•G account manager for McAfee licensing details



### CALL FOR PRICING

#### Websense® Web Security Suite

Websense provides a content filtering and security solution that safeguards organizations from bots, spyware, malicious code, phishing and crimeware. Websense software integrates with leading security and networking solutions to leverage existing IT investments and provide comprehensive security.



without interaction, saving maintenance costs and helping provide the best security possible.

Because the space is so well understood and the countermeasures so effective, most organizations easily mitigate the threat of viruses. The solutions are relatively inexpensive and simple. But virus countermeasures should never be taken for granted. Any risk analysis should take viruses into consideration.

## Trojan Horses

Trojan horses (or Trojans) are another form of malware. They masquerade as legitimate or desired software, tempting users to run them. Many Trojan horses even provide some limited functionality, such as a basic Tetris game. But this software hides malicious code as its payload. The payload can do anything that a virus can, such as delete data, convert the computer into a network zombie or install software to allow an attacker to remotely gather data.

Unlike viruses, Trojan horses cannot spread on their own. They use a combination of social engineering and technical exploits to succeed. For example, an attacker might determine that there are three administrators in your IT organization. The attacker might send these administrators a “free trial software package” that appears to be legitimate.

In fact, the software package is exactly what the attacker described, with the unmentioned addition of a silent Trojan horse that logs all keystrokes and sends them back to the attacker’s computer. The trick is that the attacker must persuade the target to run his software.

Countering Trojans is not difficult. Most virus scanners identify and remove Trojans, but you should also counter them by educating your users not to download or open any software that they have not verified as authentic. This is especially true when they receive an attachment via e-mail or instant messaging. When in doubt, they should consult the help desk or IT staff.

## Spyware

One current and nasty malware threat is spyware, which is browser-based software that installs on a computer, usually without permission, and performs some covert activity that benefits a third party. Spyware differs from viruses in that the payload does not usually destroy data on the host computer. But it does compromise security and privacy. Some characteristics of various spyware packages include:

- Reporting all Web sites visited to the infector
- Reporting all key strokes to the infector
- Displaying advertisements without permission
- Redirecting Web and search requests to a specific Web site

- Changing a Web browser’s home page
- Sending spam e-mail on behalf of the infector

Spyware can infect a host in nearly infinite ways. It can be contained within the installation package of other software, similar to a Trojan horse. It often infects a host through the Web browser when the user visits a malicious Web site. Sometimes the spyware is able to infect the host silently with no interaction (known as a drive-by installation).

Usually the spyware requires some explicit action such as permission to install a browser extension. Sometimes creators of the spyware even attempt to legally protect themselves by providing an end-user license agreement or some form of informed consent.

Once spyware is on a host, it often installs other companion spyware. Many of these packages attempt to hide and protect themselves against tampering and removal, even from an authorized administrator. In addition, spyware frequently mutates to protect itself. And many users do not notice or care about spyware as it is usually nondestructive. As a result, spyware identification and removal can be difficult.

There are specialty spyware scanners and removers available to combat this threat. They work like virus scanners, identifying patterns and using signature files to remove spyware. When considering a method to combat spyware, keep in mind that most spyware programs are browser-based and require an Internet connection to spread. You should ensure that your risk analysis considers viruses and spyware separately, as they are different threats with different controls.

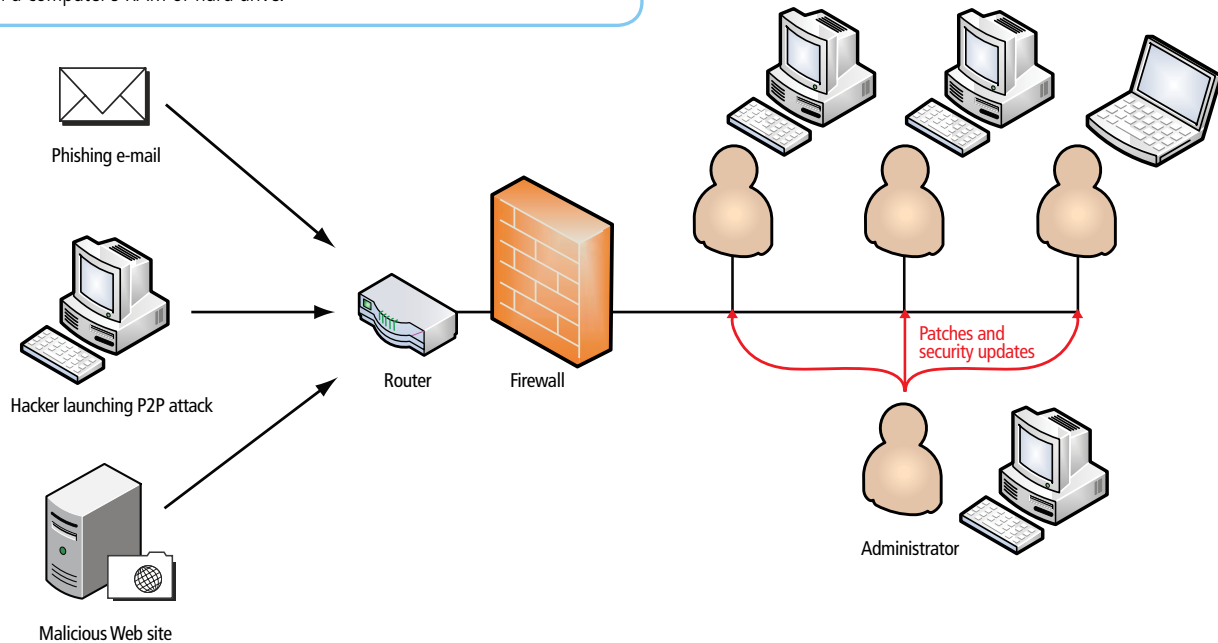
## Rootkits

Rootkits are a special class of malware. They do not harm the host computer. They do not display pop-up ads, delete files or monitor user activity. They do not self-propagate, have no knowledge of attack vectors and must be installed manually. Rootkits hide things such as files, running programs and open network ports. This hiding characteristic is what makes rootkits different.

A dedicated attacker will often use a rootkit to hide malware such as a keystroke logger or a password stealer. If the malware were simply installed on the system by itself, a virus scanner might detect it. But rootkits have the ability to hide software from such scanners and from user scrutiny. The software continues to run indefinitely in the background, immune to detection.

Only a few specialized tools currently exist to effectively detect and remove rootkits. Most of those tools have limited effectiveness because of the difficulty in detecting rootkits from within the affected OS. None of these tools today are deployable and very few even claim to remove the rootkits.

A malware scanner at the client level is used to detect malicious software in a computer's RAM or hard drive.



Because rootkits are not widespread and often other attacks can be detected when a rootkit is present, you do not need to make rootkit mitigation a top priority. However, you should consider rootkits as part of your overall malware control plan.

## What to Do About Malware

Fortunately for all of us, malware is relatively easy to control with a proactive approach. Malware must be stopped before it gets on a system. Stopping it from getting on a system is not difficult. But once it gets on a system, getting it off can be excruciating.

Install a malware scanner on every computer system on your network. This includes client and server computers in every role and every location. There are solid reasons for installing these scanners. Servers get infected often enough, even when access is controlled, to make them a source for malware outbreaks. And client computers are constantly exposed to malware sources including e-mail, IM, file sharing, files on USB drives, or MP3 players and notebooks connecting to unsecured networks.

When evaluating which malware scanner to use, consider these questions:

- Does it work on all OSs that I currently have in service?
- Can it update and maintain itself?
- Does it report infection information?
- Is it inexpensive enough for me to deploy across the entire organization, both today and in the future?

- Is the vendor reputable and trustworthy? Do I trust my network security to them?

Once you've considered these questions, obtain sample versions of the malware scanners that most closely meet your needs. Consider a test deployment to a small set of users to ensure that they are adequately protected. Once you've settled on a product, plan and deploy the solution.



Ask your  
CDW•G account  
manager for  
assistance in choosing  
a complete malware  
protection system.

The Right Technology.  
Right Away.™

# Mobile and Wireless Security

## IN THIS CHAPTER:

- Unsecured Wireless Networks
- Remote Access to Institutional Networks
- Breaking the Security Boundaries

When computers and users are contained within the well-defined boundaries of a physical and logical environment (for example, accessing an organization-owned computer on-premises), IT has an enormous amount of control over that experience. The recent engagement of a mobile workforce and telecommuting has challenged IT departments.

Chief among these changes is the proliferation of wireless networking. Today, virtually all notebook and mobile computers, and even many desktop computers, come equipped with wireless network cards. You can easily buy a wireless network access point for less than \$50 and deploy wireless access to your network within an hour.

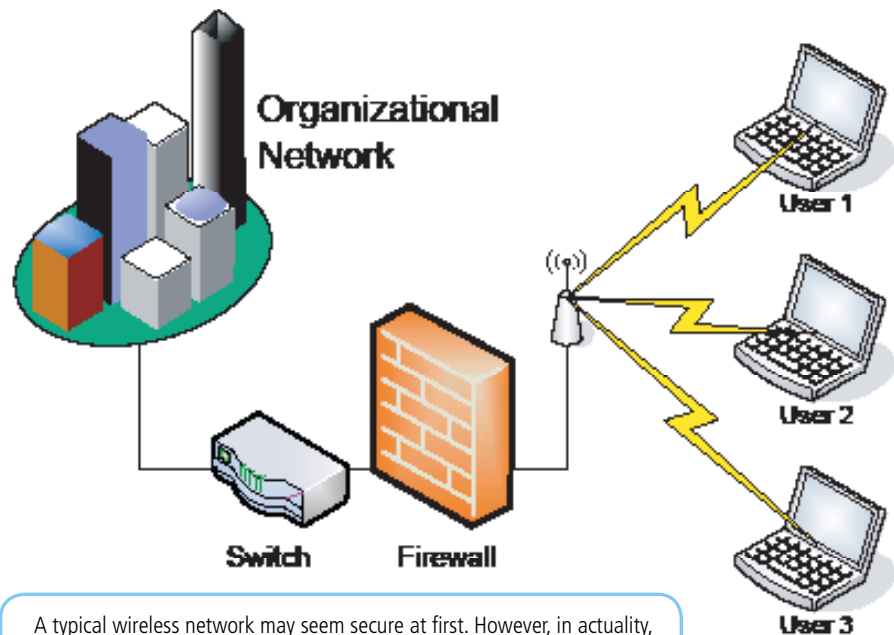
Another change is the adoption of remote access to organizational networks. A globalized economy means that people from all parts of the world might be working on a single project as a team. These users may not have the ability to travel to a centralized location or relocate to a desired site. So instead, remote access is provided so that these people can connect to the network from wherever they are.

These changes bring a wealth of benefits. But, as with most benefits, come some risks. This chapter will examine the risks and discuss potential remedies.

## Unsecured Wireless Networks

The biggest issue is controlling who has access to your network. When only copper cable connects computers, an attacker must perform a direct physical attack (such as splicing into a network cable) to access your systems.

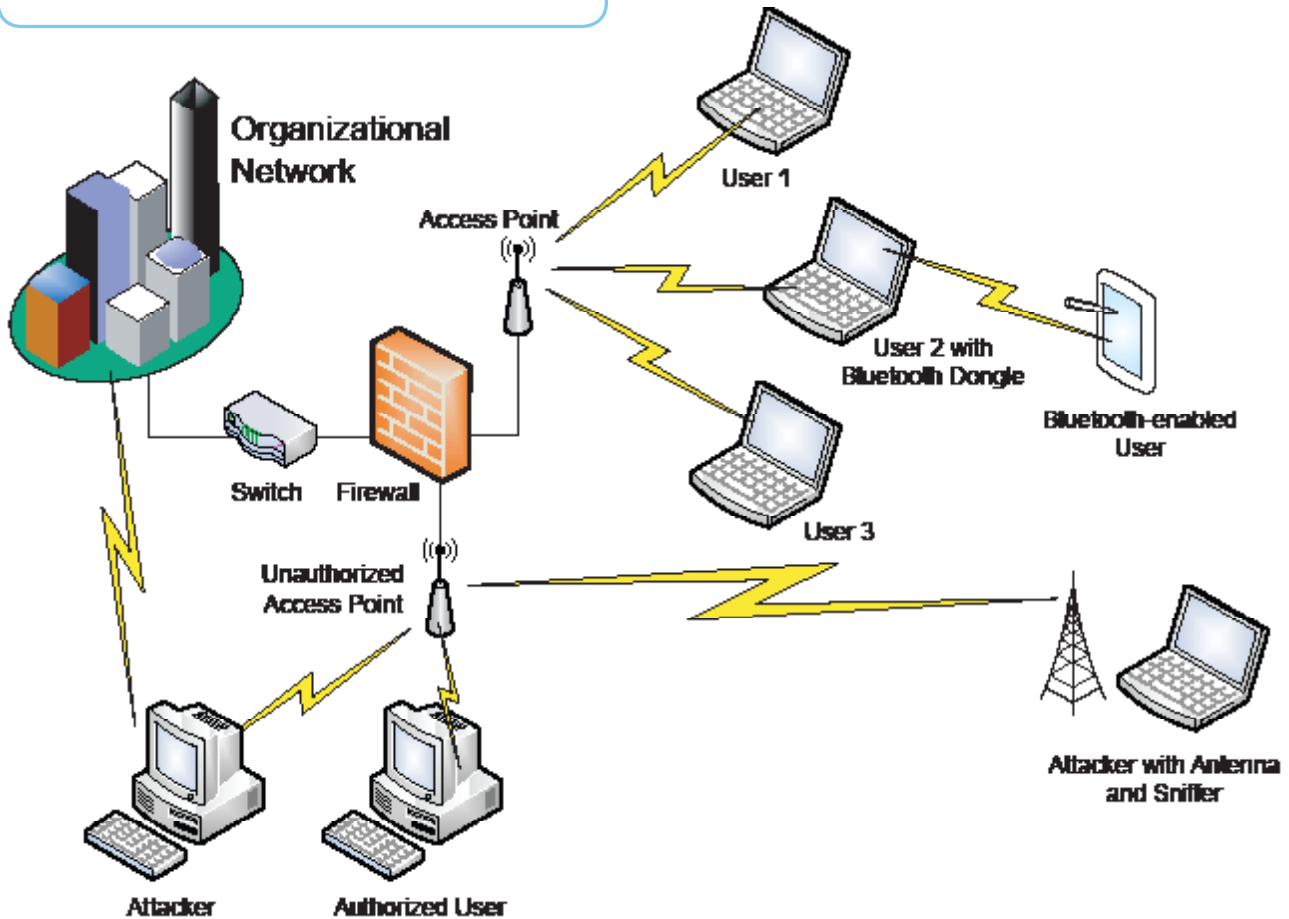
However, once you've deployed a wireless network, virtually anyone can access your system. Consider the following diagram, which represents what most school network administrators consider an accurate picture of their wireless network:



A typical wireless network may seem secure at first. However, in actuality, it may be riddled with security threats as noted in the next illustration.



Now consider a more accurate layout of the same network:



Although this image depicts a somewhat extreme example, it is far closer to reality than the perceived image shown on page 26.

Luckily, there are a number of very effective ways to enhance the security of your wireless network. And most of these can be contained within one device: the wireless access point.

Before you deploy any portion of a wireless network, you should spend some time considering which wireless access point you want to use. From a security perspective, you should look for the following features:

- Support for Wi-Fi Protected Access (WPA) and WPA2 to protect the wireless traffic
- Support for Remote Authentication Dial-In User Service (RADIUS) authentication so that you can use your centralized authentication system to provide strong, integrated authentication
- Support for MAC address filtering to limit which clients can access your network (great for smaller networks)

## Remote Access to Institutional Networks

Current changes in workforce composition have made today's IT professional consider permitting remote access to organizational resources. Like wireless networking, permitting remote access extends the boundary of your network. Virtually any attacker is now provided with the means to attempt to break into your network. Whether your remote access is provided via dial-up modem, Internet-based VPN or some other method, attackers will find and attempt to exploit this access.

There are a number of effective security controls that can help prevent attackers from accessing your network, while allowing simple and fast access to authorized users. These include RADIUS server support and built-in attack detection and prevention (much like an IPS specifically designed for remote access security).

## Breaking the Security Boundaries

Many networks support the concept of a roaming user. This user often spends extended periods outside the organization's network but periodically returns and directly connects to the network. Governments might see this embodied in a field agent or inspector, and in educational institutions the roaming student-user is often the most common type of user.

For example, let's assume you have a roaming user named Fred. Fred is issued a notebook computer. This notebook is configured with appropriate security controls such as a malware scanner, a firewall and a remote access client. Fred connects to the department network when he's at the administrative office. But the majority of the time, Fred accesses network resources from outside locations.

While traveling, Fred's computer is infected by malware when it attaches to an unsecured wireless network. Fred has no idea this has happened because his notebook behaves normally. The malware is designed to attack only organizational resources such as domain controllers and file servers, so it remains dormant until the next time Fred connects to the network. At that point, the malware is able to access department assets from within the security perimeter. Fred has unwittingly brought the malware inside with his notebook.

As another example, consider Sally, who attends a local university. Throughout a typical week, Sally uses her notebook computer in various locations, which provide free wireless access for notebook PC users. Each time Sally connects to one of these networks, she exposes her computer to attack. These attacks can come not only from wireless users at that location but also from any wireless computer within range of her notebook PC. And when she takes

the notebook from one network to the other, she is most likely spreading whatever malware is on her computer from the old network to the new. This spread will likely continue until Sally cleans the malware from her notebook.

This happens every day. Often called a Typhoid Mary attack because of the apparently healthy yet very dangerous state of the computer, the notebook computer is being increasingly used to get around strong gateway security and attack systems from the inside. This is one reason why relying solely on gateway security is insufficient to properly protect your network.

Mitigating this threat is both simple and difficult. The concepts are very easy, as there are only two necessary controls:

- Implement adequate client computer protection to avoid infection
- Only allow authorized client computers to access your network

The first item was discussed in Chapter 4. The second, only allowing authorized client computers to access resources, is difficult to implement. There are several emerging technologies that allow you to authenticate and quarantine computers before they are granted access to your network, even when plugged directly into the network. However, these technologies often require significant investments in router hardware, network routing changes and some client software installation.

An easier way to help ensure that only authorized client computers connect to your network is to implement a written administrative policy and educate users about this policy. Often, users connect their own notebooks or mobile devices because they think it's acceptable to do so without any malicious intent. They may only require a bit of awareness to understand that their actions are putting the organization (and their jobs) at risk. Although this doesn't seem like a true security control, it is often very effective.

### Working with a team of experts: CDW•G Security Specialists

Network security has two goals: protecting your organization and ensuring your peace of mind. At CDW•G, security begins with solutions — not products. Our industry-certified security specialists take a vendor-neutral approach, working with you to recommend the best mix of solutions to plug any current security gaps or prevent future ones.

CDW•G's security specialists are familiar with the latest security products, standards and policies. That's why they can deliver effective solutions based upon your evolving needs and challenges:

- Protecting your network from viruses, spyware and spam
- Keeping your servers secure
- Applying intrusion prevention and detection
- Monitoring physical environments

- Providing a safe network for your mobile/remote users
- Staying compliant to security policies and procedures

The most critical commodity in technology is neither hardware nor software. It's the expertise behind the technology — a commodity CDW•G offers in abundance. As your technology provider, our security specialists can help you make the right security decision with in-depth expertise across the technological board.

The CDW•G difference: Armed with technological expertise, a breadth of products, skilled technicians and your dedicated CDW•G account manager, our security specialists are able to provide you with solutions built for your needs today with the ability to evolve for the demands of tomorrow.



The Right Technology.  
Right Away.™

# Physical Security

## IN THIS CHAPTER:

- Securing Data Centers, Property, Staff and Students
- Securing Notebook PCs and Portable Devices

Often overlooked, physical security is the foundation for all computer security. The adage is, “No physical security equals no security.” Although there are arguable exceptions to this rule, it is virtually always true. Without strong physical security, no computer security control should be considered adequate.

If an attacker has logical (network) or even keyboard/mouse access to a computer, their interactions are limited by the OS and other security controls that are probably in place. Factors such as configuration management, malware scanners and access control can continue to hinder this attacker.

But once the attacker has access to the physical computer (not just the keyboard and mouse, but the entire computer system), the situation changes. He can now compromise data on the hard drive, replacing the OS or application software with his own software. He can manipulate the configuration of the OS or security applications. The attacker can even install hardware-based keystroke loggers or other security-defeating mechanisms.



It is crucial to the security of your assets that you protect them from an attacker's physical access. This is true for all of your assets such as servers, clients and mobile computers, as well as other assets such as employees and buildings. However, the level of risk varies for each of those categories. The following sections describe the categories and their unique physical security requirements.

→ A frequent mistake made by computer security specialists happens during risk analysis. A critical part of any risk analysis procedure is the identification and ranking of assets. Most security specialists include physical computers, data centers, computer data and even the access to that data as assets. However, they fail to identify one critical asset: employees. Without employees, most systems are useless. And attacks against students and employees are very real. There are a variety of successful attacks, ranging from the obvious physical attack to less tangible attacks such as phishing, malware and social engineering. You should ensure that any risk analysis you perform considers the people portion of the system.

## Securing Data Centers, Property, Staff and Students

Depending upon the configuration of an organization's facilities, a number of physical safeguards may be used to prevent unauthorized access and protect property and people. One of the most widely used physical site security tools is the IP-surveillance or network camera.

IP surveillance facilitates monitoring and recording of video over an IP network. It allows users to gather information and view it in real-time, which makes it perfectly suited for monitoring equipment, people and places locally or remotely. Installation costs are usually minimal since IP surveillance systems can often be run on existing wired as well as wireless networks.

IP surveillance is gaining popularity in the education sector. It is used to monitor and secure building perimeters, hallways, classrooms, campuses and school playgrounds, and ensure the safety of staff and students. In some cases, it is also used to facilitate remote learning.

Governments at all levels (federal, state and local) are embracing IP surveillance to ensure the safety of citizens, staff and assets. In addition to being a crime and vandalism deterrent, IP surveillance is key in helping emergency response teams locate an emergency and adequately handle it.

## Securing Servers

Secure servers behind locked doors or in data centers, where you can monitor physical access. When in a shared environment, like a colocation center, you may have a choice between a locked rack or a cage you can walk into. The cage has the advantage that people can't poke at keyboards or power switches through the rack.

Even inside a secured area, you may still want to further secure your servers. One option for securing equipment within racks is APC's Rack Access PX, a locking appliance designed for use with the firm's InfraStruXure modular rack and power system. The Rack Access PX can be controlled either through a key-card or remotely through a Web browser, by administrators who can observe the facility via IP video cameras.

## Securing Notebook PCs and Portable Devices

Unfortunately, not all computers are easy to physically secure. Although you may be able to lock up desktop computers, that's not the case with notebook and mobile computers in use throughout your organization. These computers will invariably be used in potentially dangerous and unsecured areas.

Notebook PC and portable device theft continues to increase year after year. It is actually a source of profit for two types of attackers: the opportunist and the spy. Opportunists see a notebook PC as a quick source of income. They're not concerned with the data on the notebook or its value — in fact, they probably don't even know how to access the data.

The spy, however, is far more skilled. This person steals notebooks and mobile computers with the intention of compromising their data and making a profit from that stolen data. The computer hardware is of little value compared with the compromised information.

A number of innovations help to thwart such attackers. They include:

- Bitlocker Drive Encryption, a feature of Windows Vista™ that can encrypt an entire hard drive
- Encrypting File System, another Windows feature that encrypts individual files on a hard drive
- Content management systems that use public-key cryptography to protect data against unauthorized use
- Hardware-based hard drive encryption technologies
- Software-based file and whole-disk encryption applications
- Built-in hardware protection using the Trusted Platform Module (TPM)

There are other technologies available to help protect sensitive data — this is only a small sample of the available options. You should carefully consider all options when making a decision about which technology or technologies to use. This is especially important if you are subject to regulations requiring specific types of cryptography or key length. Be sure you implement a solution that provides the required level of security control for your organization.

# Shop

## CDWG.com

### for best-of-breed security solutions.



**The Right Technology.  
Right Away.™**



## Chapter 7

# Summary

Security can be considered one of the larger concerns for IT administrators today. This is due to the increased number and effectiveness of attackers. Given that attackers now have financial and political motivation to attack systems, they are often very aggressive and effective in thwarting poorly implemented defenses.

The defense strategies outlined in this guide are intended to represent the current best thinking for a balanced systemic defense. Balance between cost, usability and security is critical whenever planning defenses. Many system administrators make the mistake of saying, "I want the strongest defense possible," without realizing that implementing such a defense would block critical job functions or create a negative perception of IT security.



Instead of taking that approach, consider asking, "What are the most appropriate defenses that I can implement to block the attacks I'm worried about, while still providing necessary job functionality?" That question should be the one that guides you to the proper security balance.

### CDW•G's Capabilities

Against this backdrop of constant change and uncertainty, CDW•G can be of assistance to you — not only as a dependable and convenient source of products for your security needs, but also as an adviser. We provide you with a single point of access to a multitude of technology vendors.

We offer security resources far beyond just hardware and software. In addition to our own team of dedicated security specialists, we have full-time access to vendor-assigned system engineers, as well as service providers who offer a full range of IT services for our customers. We know today's operational demands are constantly changing, so we can also keep you aware of new capabilities and technologies.

Through planning, designing, migrating, building and implementing, we'll work with you to define key objectives, determine your technology goals and understand the purpose of your security initiative. And we continue supporting you after the project has been completed — with onsite assistance (when requested), 24 x 7 telephone tech support and your ongoing relationship with your CDW•G account manager. Because of our focus on providing the right technology, right away, you can enjoy the confidence of working with the premier experts for your security and other technology solutions.

At CDW•G, we've designed our company with you in mind. Our ultimate goal is to ensure your satisfaction over the long run.



CDW•G stocks  
a large assortment  
of security hardware  
and software to meet  
your network needs.

The Right Technology.  
Right Away.™

7  
CHAPTER



# Gigantinormous.

It's the only word we could come up with to describe our Configuration Center capabilities.



The CDW® Configuration Center can handle your configuration needs. Our A+ and vendor-certified technicians can custom configure, image and test hundreds of systems every day. And that's just the beginning. We handle everything from basic installation of hardware and software to high-end enterprise configuration services at one of our three Configuration Centers. We offer a variety of services to keep your organization up and running at optimum efficiency.

Get configured. Call 800.808.4239  
or visit [CDWG.com](http://CDWG.com)

The Right Technology. Right Away.™



CDW®, CDW•G®, CDW@work®, CDWG@work® and The Right Technology. Right Away.™ are trademarks of CDW Corporation.





# Glossary

## Attacker

An individual trying to compromise any element of your data security infrastructure

## Biometrics

Authentication process in which a user authenticates based on a personal characteristic, such as a fingerprint, voice, retina or writing pattern

## Cryptography

Conversion of data into a secret code for transmission over a public network and long-term data storage

## Decryption

Process of translating a coded sequence of bytes back into its original sequence

## Denial of Service (DoS) Attack

Attack that prevents legitimate users from accessing system resources

## Domain

Logically distinct segment of a network that is managed as a single security area

## Dynamic Host Configuration Protocol (DHCP)

Network protocol that automatically assigns IP addresses to clients logging onto a TCP/IP network

## Encryption

Process of coding, or "scrambling," a sequence of bytes so it cannot be understood without first unscrambling the code

## Firewall

Network device for limiting the flow of traffic into and out of a network

## Hacker

Term commonly misused in the security context, often actually meaning attacker

## Intrusion Detection System (IDS)

Monitors network activity, alerts personnel when suspicious activity occurs and shuts down suspect connections automatically

## Intrusion Prevention System (IPS)

Inline device, implementing a basic IDS that network traffic flows through; can block any traffic that appears to be an intrusion

## IP Security (IPSec)

Framework for establishing encrypted communications between two devices by using two protocols: AH and ESP

## Keystroke Logger

Software package or hardware device that records all keystrokes on a computer

## Malware

Any type of malicious program, such as a virus, worm, Trojan horse or blended threat

## Media Access Control (MAC) Address

Hardware address that uniquely identifies each node of a network

## Payload

Code portion of malware that damages a computer system

## Phishing

Form of online scam that attempts to mislead people into disclosing private information, such as credit card numbers; well-known brands are often used to lure subjects to spoofed Web sites or even hijacked domains that look legitimate, but will prompt subjects for personal information

## Policy

Formal document describing an organization's position on a particular aspect of enterprise security

## Private Key

Part of a two-part, public-key cryptography system that is kept secret and never transmitted over a network

## Procedure

Step-by-step description of tasks required under a security policy

## Public Key

Published part of a two-part, public-key cryptography system

## Rootkit

Tool that hides other software from detection; often used with malware

## Secure Sockets Layer (SSL)

Leading security protocol on the Internet; in a typical SSL session, the server sends its public key to the browser, which uses that public key to send a randomly generated secret key back to the original server in order to have a secret key exchange for that session

## Security Threat

Ability to exploit a computer or network vulnerability

## Social Engineering

Illegally entering a computer system by having persuaded an authorized person to reveal IDs, passwords and other confidential information

## Spy

An attacker intending to conduct espionage, usually in a corporate or government environment

## Spyware

Software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes

## Transmission Control Protocol (TCP)

Protocol within the TCP/IP protocol suite that is used when reliable packet delivery is essential; requires confirmation of packet delivery for all transmitted packets

## Virus

Malicious program that replicates and transmits itself by exploiting vulnerabilities in other programs

## Worm

Malicious program that replicates and transmits itself with dependency on other programs; typically exploits a single vulnerability, although newer worms are exploiting multiple vulnerabilities

## Zombie

Computer system that has been covertly taken over in order to transmit phony messages that slow down service and disrupt the network



# Index

Attacker .....	5-7, 9-11, 13, 24, 26-27, 29-31	Payload .....	13, 24
Biometrics .....	19	Phishing .....	11, 25, 29
Cryptography .....	30	Policy .....	7-8, 18, 28
Decryption .....	11	Private Key .....	11
Denial of Service (DoS) Attack .....	3, 5	Procedure .....	28-29
Domain .....	6, 9-10, 13, 28	Public Key .....	30
Dynamic Host Configuration Protocol (DHCP) .....	9	Rootkit .....	3, 13, 24-25
Encryption .....	3, 11, 13, 19, 25, 30	Secure Sockets Layer (SSL) .....	19
Firewall .....	5-8, 10-11, 19, 25-26, 28	Security Threat .....	3, 11
Hacker .....	25	Social Engineering .....	11, 24, 29
Intrusion Detection System (IDS) .....	5, 8	Spy .....	30
Intrusion Prevention System (IPS) .....	5, 8	Spyware .....	3, 13, 19, 24-25, 28
IP Security (IPSec) .....	9-11	Transmission Control Protocol (TCP) .....	6, 10
Keystroke Logger .....	24, 29	Virus .....	3, 8, 13, 18-19, 24-25, 28
Malware .....	3, 7-11, 13, 24-25, 28-29	Worm .....	3, 13
Media Access Control (MAC) Address .....	6, 27	Zombie .....	24

## Disclaimer

For all products, services and offers, CDW•G® reserves the right to make adjustments due to changing market conditions, product/service discontinuation, manufacturer price changes, errors in advertisements and other extenuating circumstances. All trademarks and registered trademarks are the sole property of their respective owners. CDW•G and the Circle of Service logo are registered trademarks of CDW Corporation. ©2007 CDW Corporation. All rights reserved. This document may not be reproduced or distributed for any reason. Federal law provides for severe and criminal penalties for the unauthorized reproduction and distribution of copyrighted materials. Criminal copyright infringement is investigated by the Federal Bureau of Investigation (FBI) and may constitute a felony with a maximum penalty of up to five (5) years in prison and/or a \$250,000 fine. Title 17 U.S.C. Sections 501 and 506. This reference guide is designed to provide readers with information regarding network security. CDW•G makes no warranty as to the accuracy or completeness of the information contained in this reference guide nor specific application by readers in making decisions regarding network security and/or related systems. Furthermore, CDW•G assumes no liability for compensatory, consequential or other damages arising out of or related to the use of this publication.

# Network Security

Reference Guide

## Look inside for more information on:

- The proliferation of network security threats
- The benefits of a layered-security strategy
- Security solutions for the five primary network pillars
- Gateway, server, client, mobile and physical security approaches
- Current best thinking for a balanced security response

CDWG.com | 888.510.4239

### CDW Government, Inc.

One CDW Way  
230 N. Milwaukee Avenue  
Vernon Hills, IL 60061



Your account number is

Key Code

PRSRT STD  
U.S. POSTAGE  
PAID  
MT. PROSPECT, IL  
PERMIT NO. 87