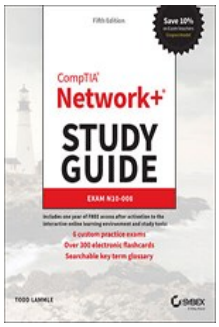

CompTIA Network+ Study Guide: Exam N10-008, 5th Edition

by Todd Lammle

Chapter 14: Organizational Documents and Policies

The following Comptia Network+ Exam Objectives are Covered in This Chapter

- **3.2 Explain the purpose of organizational documents and policies.**
  - Plans and procedures
    - Change management
    - Incident response plan
    - Disaster recovery plan
    - Business continuity plan
    - System life cycle
    - Standard operating procedures
  - Hardening and security policies
    - Acceptable use policy
    - Password policy
    - Bring your own device (BYOD) policy
    - Remote access policy
    - Onboarding and offboarding policy
    - Security policy
    - Data loss prevention
  - Common documentation
    - Physical network diagram
      - Floor plan
      - Rack diagram
      - Intermediate distribution frame (IDF)/main distribution frame (MDF) documentation
    - Logical network diagram
    - Wiring diagram
    - Site survey report
    - Audit and assessment report
    - Baseline configurations
  - Common agreements
    - Non-disclosure agreement (NDA)
    - Service-level agreement (SLA)
    - Memorandum of understanding (MOU)

It's up to us, individually and corporately, to nail down exactly what solid guidelines there should be for policies and procedures for network installation and operation. Some organizations are bound by regulations that also affect how they conduct their business,

and that kind of thing clearly needs to be involved in their choices.

One of the most important aspects of any policy or procedure is that it's given high-level management support. This is because neither will be very effective if there aren't any consequences for not following the rules!

Note To find Todd Lammle CompTIA videos and practice questions, please see `www.lammle.com`.

Plans and Procedures

Let’s take some time to examine the difference between policies and procedures.

Policies govern how the network is configured and operated as well as how people are expected to behave on it. They're in place to direct things like how users access resources and which employees and groups get various types of network access and/or privileges. Basically, policies give people guidelines as to what they are expected to do. Procedures are precise descriptions of the appropriate steps to follow in a given situation, such as what to do when an employee is terminated or what to do in the event of a natural disaster. They often dictate precisely how to execute policies as well.

Procedures are the actions to be taken in specific situations:

- Disciplinary action to be taken if a policy is broken
- What to do during an audit
- How issues are reported to management
- What to do when someone has locked themselves out of their account
- How to properly install or remove software on servers
- What to do if files on the servers suddenly appear to be "missing" or altered
- How to respond when a network computer has a virus
- What actions to take if it appears that a hacker has broken into the network
- What actions to take if there is a physical emergency like a fire or flood

So you get the idea, right? For every policy on your network, there should be a credible related procedure that clearly dictates the steps to take in order to fulfill it. And you know that policies and procedures are as unique as the wide array of companies and organizations that create and employ them. But all this doesn't mean you can't borrow good ideas and plans from others and tweak them a bit to meet your requirements.

Note An example of a network access policy is a time-of-day restriction on logging into the network.

Change Management

Change should be introduced in a managed fashion. For this to occur, an organization must have a formal change management process in place. The purpose of this process is to ensure that all changes are approved by the proper personnel and are implemented in a safe and logical manner. Let's look at some of the key items that should be included in these procedures.

Document Reason for a Change

Clearly, every change should be made for a reason, and before the change is even discussed, that reason should be documented. During all stages of the approval process (discussed later), this information should be clearly communicated and attached to the change under consideration.

Change Request

A change should start its life as a change request. This request will move through various stages of the approval process and should include certain pieces of information that will guide those tasked with approving or denying it.

Configuration Procedures

The exact steps required to implement the change and the exact devices involved should be clearly detailed. Complete documentation should be produced and submitted with a formal report to the change management board.

Rollback Process

Changes always carry a risk. Before any changes are implemented, plans for reversing changes and recovering from any adverse effects from them should be identified. Those making the changes should be completely briefed in these rollback procedures, and they should exhibit a clear understanding of them prior to implementing the changes.

Potential Impact

While unexpected adverse effects of a change can't always be anticipated, a good-faith effort should be made to identity all possible systems that could be impacted by the change. One of the benefits of performing this exercise is that it can identify systems that may need to be more closely monitored for their reaction to the change as the change is being implemented.

Notification

When all systems and departments that may be impacted by the change are identified, system owners and department heads should be notified of all changes that could potentially affect them. One of the associated benefits of this is that it creates additional monitors for problems during the change process.

Approval Process

Requests for changes should be fully vetted by a cross section of users, IT personnel, management, and security experts. In many cases, it's wise to form a change control board to complete the following tasks:

- Assure that changes made are approved, tested, documented, and implemented correctly.
- Meet periodically to discuss change status accounting reports.
- Maintain responsibility for assuring that changes made do not jeopardize the soundness of the verification system.

Maintenance Window

A maintenance window is an amount of time a system will be down or unavailable during the implementation of changes. Before this window of time is specified, all affected systems should be examined to identify how essential they are in supporting mission-critical operations. It may be that the time required to make the change may exceed the allowable downtime a system can suffer during normal business hours, and the change may need to be implemented during a weekend or in the evening.

Authorized Downtime

Once the time required to make the change has been compared to the maximum allowable downtime a system can suffer and the optimum time for the change is identified, the authorized downtime can be specified. This amounts to a final decision on when the change will be made.

Notification of Change

When the change has been successfully completed and a sufficient amount of time has elapsed for issues to manifest themselves, all stakeholders should be notified that the change is complete. At that time, the stakeholders (those possibly affected by the change) can continue to monitor the situation for any residual problems.

Documentation

The job isn't complete until the paperwork is complete. In this case, the following should be updated to reflect the changed state of the network:

- Network configurations

- Additions to network
- Physical location changes

Incident Response Plan

Often, when an attack or security breach occurs in the network, valuable time and information are lost in the critical first minutes and hours after the incident occurs. In some cases, evidence is inadvertently destroyed, making prosecution of the offending party impossible. In other cases, attacks that could have been interrupted and prevented before damage occurs are allowed to continue.

An incident response plan or policy is designed to prevent this by establishing in advance the procedures that should be followed when an attack occurs. It may categorize incidents in such a way that certain event types (such as an active port scan) may require a response (such as disabling certain services) within 10 minutes while other events (such as an attempt to access a file without proper credentials) may only require a notation and follow-up in the next few days. The point is to establish these rules ahead of time to ensure that events are handled in a way that minimizes damage and preserves evidence.

Disaster Recovery Plan

A disaster is an emergency that goes beyond the normal response of resources. The causes of disasters are categorized into three main areas according to origin:

- Technological disasters (device failures)
- Manmade disasters (arson, terrorism, sabotage)
- Natural disasters (hurricanes, floods, earthquakes)

The severity of financial and reputational damage to an organization is largely determined by the amount of time it takes the organization to recover from the disaster. A properly designed disaster recovery plan (DRP) minimizes the effect of a disaster. The DRP is implemented when the emergency occurs and includes the steps to restore systems so the organization can resume normal operations. The goal of a DRP is to minimize or prevent property damage and prevent loss of life.

Business Continuity Plan

One of the parts of a DRP is a plan to keep the business operational while the organization recovers from the disaster; this is known as a business continuity plan (BCP). Continuity planning deals with identifying the impact of any disaster and ensuring that a viable recovery plan for each function and system is implemented. By prioritizing each process and its supporting technologies, the company can ensure that mission-critical systems are recovered first and systems that are considered luxuries can be recovered as time allows.

One document that should be created to drive this prioritization is the business impact analysis (BIA). In this document, the impact each system has on the ability of the organization to stay operational is determined. The results list the critical and necessary business functions, their resource dependencies, and their level of criticality to the overall organization.

System Life Cycle

The steps in the system life cycle are defined, including acquisition, implementation, maintenance, and decommissioning. The life cycle specifies certain due diligence activities to be performed in each phase.

Asset disposal is usually a subset of the system life cycle and prescribes methods of ensuring that sensitive data is removed from devices before disposal.

Standard Operating Procedures

Once your business is launched, each department leader will need to develop practical methods to implement their assigned tasks using the specific part of the business model's blueprint that relates to their branch. These practical methods, or protocols, must be compiled into a standard operating procedures manual and followed closely. The procedures in your manual will have been included for different reasons and have varying degrees of importance and implementation. If you form a partnership or acquire another company, it will be crucial for its business protocols to either match or be compatible with yours.

Hardening and Security Policies

One of the ongoing goals of operations security is to ensure that all systems have been hardened to the extent that is possible and still provide functionality. The hardening can be accomplished on both a physical and logical basis. From a logical perspective:

- Remove unnecessary applications.
- Disable unnecessary services.
- Block unrequired ports.
- Tightly control the connecting of external storage devices and media if it's allowed at all.

But hardening is only a part of the picture. There needs to be a set of security policies that are enforced through the use of security profiles, sometimes also called baselines. Let's look at some of the more important policies that should be implemented.

Acceptable Use Policy

Acceptable use policies should be as comprehensive as possible and should outline every action that is allowed in addition to those that are not allowed. They should also specify the devices and websites that are allowed and the proper use of company equipment.

Real World Scenario

Implement the appropriate policies or procedures.

You operate a mid-sized network for Acme Inc. Recently a rogue access point was discovered in the network, which constituted a security breach. While the original fear was that it was installed as an evil twin, further investigation revealed it was placed there by an employee so his department could have wireless access. It has now been removed.

- **Question:** What two actions do you need to take and what security policy document do you need to access?
- **Answer:** Remind/inform the employee of the security policy prohibiting this activity and discipline the employee. This will require access to an acceptable use policy, specifically the one that the employee signed when hired.

To prevent this in the future, you should schedule a training session for employees that reinforces the rules contained in the acceptable use policy and explains the motivation behind each of these rules.

Password Policy

The password policy defines the requirements for all passwords, including length, complexity, and age. Password management considerations include, but may not be limited to, the following:

- **Password life**: How long a password will be valid. For most organizations, passwords are valid for 60 to 90 days.
- **Password history**: How long before a password can be reused. Password policies usually remember a certain number of previously used passwords.
- **Authentication period**: How long a user can remain logged in. If a user remains logged in for the specified period without activity, the user will be automatically logged out.
- **Password complexity:** How the password will be structured. Most organizations require upper- and lowercase letters, numbers, and special characters.

  The following are some recommendations:

  - Passwords shouldn't contain the username or parts of the user's full name, such as their first name.
  - Passwords should use at least three of the four available character types: lowercase letters, uppercase letters, numbers, and symbols.
- **Password length**: How long the password must be. Most organizations require 8 to 12 characters.

Bring Your Own Device (BYOD) Policy

Increasingly, users are doing work on their mobile devices that they once performed on laptops and desktop computers. Moreover, they are demanding that they be able to use their personal devices to work on the company network. This presents a huge security issue for the IT department because they have to secure these devices while simultaneously exercising much less control over them.

The security team must have a way to prevent these personal devices from introducing malware and other security issues to the network. Bring your own device (BYOD) initiatives can be successful if implemented correctly. The key is to implement control over personal devices that leave the safety of your network and return later after potentially being exposed to environments that are out of your control.

Educating users on the risks related to mobile devices and ensuring that they implement appropriate security measures can help protect against threats involved with these devices. Some of the guidelines that should be provided to mobile device users include implementing a device locking PIN, using device encryption, implementing GPS location services, and implementing remote wipe. Also, users should be cautioned on downloading apps without ensuring that they are coming from a reputable source. In recent years, mobile device management (MDM) and mobile application management (MAM) systems have become popular in enterprises. They are implemented to ensure that an organization can control mobile device settings, applications, and other parameters when those devices are attached to the enterprise.

Remote Access Policy

Remote access policies define the requirements for all remote access connections to the enterprise. This may cover VPN, dial-up, and wireless access methods. One method of securing remote access connections is through the use of Network Access Control (NAC), which you will learn about in Chapter 19.

Onboarding and Offboarding Policy

Every new user that is hired undergoes what is called an onboarding process that should be guided by a consistent onboarding policy. This policy prescribes the way in which users are assigned accounts and access to resources as well as the issuance of equipment to them. The following items should be defined and standardized by the onboarding policy:

- Required training
- Account creation
- Resource access

Also, several documents should be executed and signed prior to starting work:

- Acceptable use agreement
- Nondisclosure agreement

There also should be an offboarding policy that defines what actions take place when a user leaves the organization. Special items of concern are as follows:

- Proper recovery of all equipment
- Secure removal of all resource access
- Deletion or disablement of account

Security Policy

So what, exactly, is a security policy? Ideally, it should precisely define how security is to be implemented within an organization and include physical security, document security, and network security. Plus, you have to make sure these forms of security are implemented completely and solidly because if they aren't, your security policy will be a lot like a block of Swiss cheese—some areas are covered, but others are full of holes.

Before a network can be truly secure, the network support staff should post the part of the security policy that applies to employee conduct on bulletin boards. It should, for example, forbid posting any company and/or employee information that's not absolutely necessary—like, believe it or not, sticking Post-its with usernames and passwords on computer screens. Really clean desks, audits, and recordings of email communications and, in some cases, phone calls should also be requirements. And don't forget to also post the consequences of not complying with the security policy.

Security Audit

Let’s examine each of these aspects of security policy a little more closely, beginning with security audits. A *security audit* is a thorough examination of your network that includes testing all its components to make sure everything is secure. You can do this internally, but you can also contract an audit with a third party if you want the level of security to be certified. A valid and verified consultant's audit is a good follow-up to an internal audit. One reason for having your network's security certified like this is that government agencies usually require it before they'll grant you contract work, especially if that work is considered confidential, secret, or top secret.

Clean-Desk Policy

That clean-desk policy doesn't just end with "get rid of the crumbs from your last snack." It means requiring that all potentially important documents like books, schematics, confidential letters, notes to self, and so on aren't left out in the open when someone's away from their desk. Instead, they're locked away, securely out of sight. And make sure it's clear that this rule applies to users' PC desktops too. Policies like this apply to offices, laboratories, and workbenches as well as desks, and it's really important for employees who share workspaces and/or workstations.

It's super easy to nick something off someone's desk or screen. Because most security problems involve people on the inside, implementing and enforcing a clean-desk policy is a simple way to guard against security breaches.

It might sound really nitpicky, but for a clean-desk policy to be effective, users have to clean up their desks every time they walk away from them—without exception. The day someone doesn't will be the very day when some prospective tenant is being shown the building's layout and a sensitive document suddenly disappears. You should make sure workstations are locked to desks and do random spot checks once in a while to help enforce the policy. For obvious reasons, before company picnics and parties and before "bring your child to work day" are good times to do this.

Tip The ICSA is a vendor-neutral organization that certifies the functionality of security products as well as makes recommendations on security in general.

Recording Equipment

Recording equipment—such as tape recorders, cell phones, and small memory devices like USB flash memory keychains—can contain sensitive, confidential information, so a good security policy should prohibit their unauthorized presence and use.

Just walk into almost any large technology company and you'll be immediately confronted with signs. A really common one is a camera with a circle surrounding it and a slash through the center of the circle. Read the text below the sign and you'll be informed that you can't bring any recording devices onto the premises.

Here's a good example. The National Security Agency (NSA) has updated its policy to include prohibiting Furby dolls on government premises because they have reasonably sophisticated computers inside them, complete with a digital recording device. The doll repeats what it hears at a certain interval of time, which is either cute or creepy but pretty much harmless—maybe even protective—in a children's daycare center. Not so much at the NSA, though—no recording conversations there. Maybe, at least in some locations, it's not such a good idea for your company either.

Other Common Security Policies

So you get the idea—security policies can cover literally hundreds of items. Here are some common ones:

- **Notification** Security policies aren't much good if no one knows about them, right? So make sure you give users a copy of the security policy when you give them their usernames and passwords. It's also a good idea to have computers display a summarized version of the policy when any user attempts to connect. Here's an example: "Unauthorized access is prohibited and will be prosecuted to the fullest extent of the law." Remember—your goal is to close loopholes. One hacker actually argued that because a computer didn't tell him otherwise, anyone was free to connect to it and use the system!
- **Equipment Access** Disable all unused network ports so that any nonemployees who happen to be in the building can't connect a laptop to an unused port and gain access to the network. And don't forget to place all network equipment under lock and key.
- **Wiring** Your network's wires should never run along the floor where they can be easily accessed (or tripped over, getting you sued). Routers, switches, and concentrators should live in locked closets or rooms, with access to those rooms controlled by anything ranging from a good lock to a biometric access system, depending on the level of security your

specific network and data require.

- **Door Locks/Swipe Mechanisms** Be sure that only authorized people know the combination to the cipher lock on your data-center doors or that only the appropriate people have badges that allow access to the data center. Change lock combinations often, and never ever leave server room doors open or unlocked.
- **Badges** Require everyone to wear an ID badge, including contractors and visitors, and assign appropriate access levels to everyone.
- **Tracking** Require badge access to all entrances to buildings and internal computer rooms. Track and record all entry to and exits from these rooms.
- **Passwords** Reset passwords at least every month. Train everyone on how to create strong passwords. Set BIOS/UEFI passwords on every client and server computer to prevent BIOS/UEFI changes.
- **Monitor Viewing** Place computer monitors strategically so that visitors or people looking through windows can't see them, and make sure unauthorized users/persons can't see security-guard stations and server monitors. Use monitor privacy screens if necessary.
- **Accounts** Each user should have their own, unique user account, and employees should never share user accounts. Even temporary employees should have their own account. Otherwise, you won't be able to isolate a security breach.
- **Testing** Review and audit your network security at least once a year.
- **Background Checks** Do background checks on all network support staff. This may include calling their previous employers, verifying their college degrees, requiring a drug test, and checking for a criminal background.
- **Firewalls** Use a firewall to protect all Internet connections, and use the appropriate proxies and dynamic-packet-filtering equipment to control access to the network. Your firewall should provide as much security as your company requires and your budget allows.
- **Intrusion Detection** Use intrusion detection and logging software to discover security breaches, and be sure you're logging the events you want to monitor.
- **Cameras** Cameras should cover all entrances to the building and the entire parking lot. Be sure that cameras are in weatherproof and tamper-proof housings, and review the output at a security-monitoring office. Record everything on extended-length tape recorders.
- **Mail Servers** Provide each person with their own email mailbox, and attach an individual network account to each mailbox. If several people need to access a mailbox, don't give all of them the password to a single network account. Instead, assign individual privileges to each person's network account so you can track activity down to a single person, even with a generic address like `info@mycompany.com`.
- **DMZ** Use a demilitarized zone (DMZ) for all publicly viewable servers, including web servers, FTP servers, and email relay servers. Figure 14.1 shows a common DMZ setup.

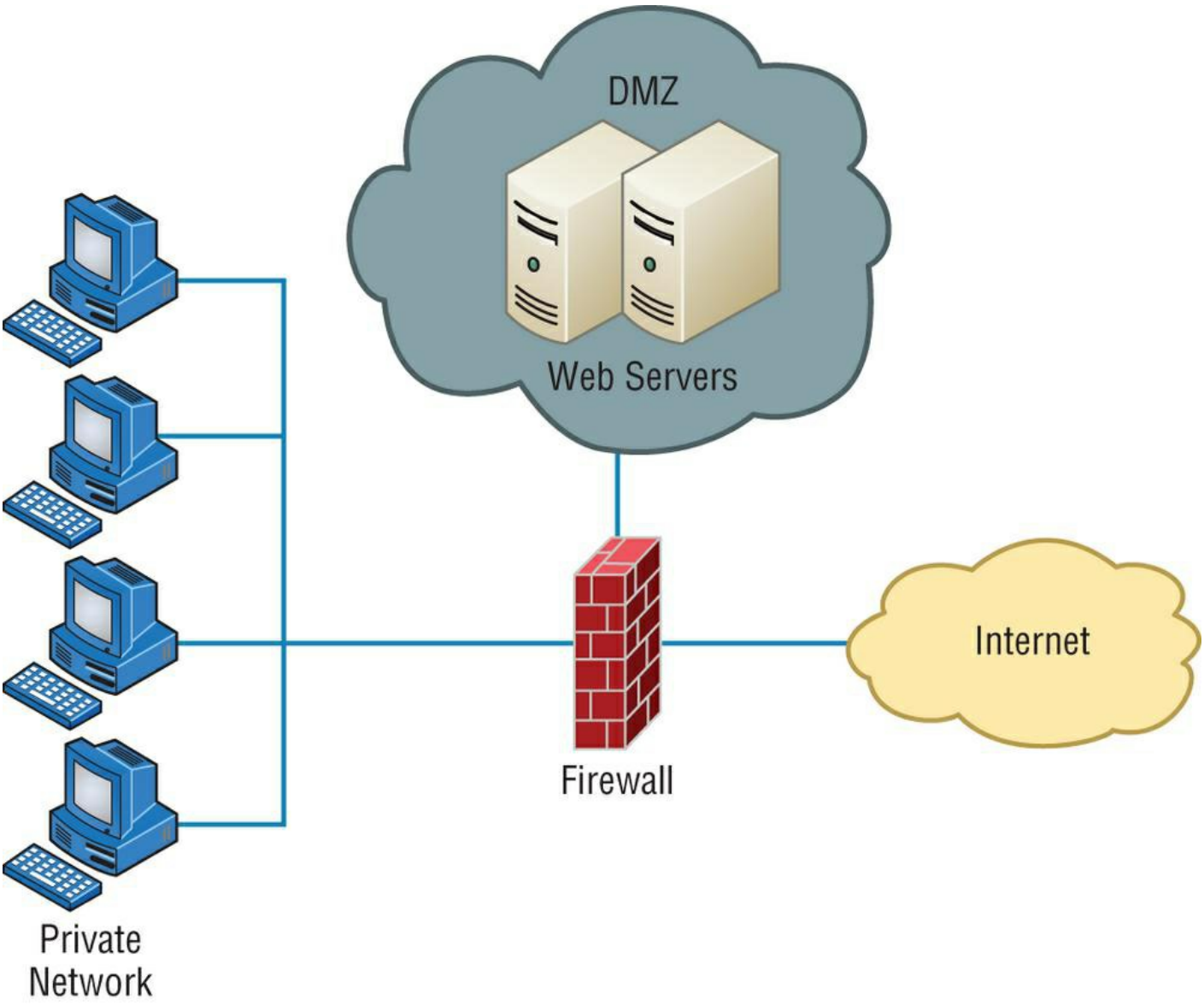

Figure 14.1: A common DMZ configuration

It is not advisable to put a DMZ outside the firewall because any servers outside your firewall defeat the whole purpose of having one. However, it is possible that you may see a DMZ outside the firewall in some networks. You will learn more about DMZs in Chapter 16.

- **Mail Relay** Mail servers relay to other email servers by design. When the email server relays from any server that requests it, it is called *open relay*. Hackers use this feature to forward spam. Modern email systems allow you to control which servers your email server will relay from which helps to prevent this.
- **Patches** Make sure the latest security updates are installed after being properly tested on a nonproduction computer.
- **Backups** Store backup tape cartridges securely, not on a shelf or table within reach of someone working at the server. Lock tapes in a waterproof, fireproof safe, and keep at least some of your backups off site.
- **Modems** Do not ever allow desktop modems because they can be used to get to the Internet without your knowledge. Restrict modem access to approved server-based modem pools.
- **Guards** If you need security guards, they shouldn't patrol the same station all the time. As people become familiar with an environment and situation, they tend to become less observant about that environment, so rotating guards to keep their focus at the highest possible level makes a lot of sense. Clearly, guards are people who need breaks to ensure alertness, but make sure that all patrol areas are covered during shift changes, rotations, and breaks. Guards should also receive periodic training and testing to make sure they can recognize a threat and take appropriate action.

Warning Believe it or not, covering all these bases still won't guarantee that your network or facility is secure. All of this is really just a starting point

that's meant to point you in the right direction.

Breaking Policy

You know that for your policy to be effective it has to be enforced consistently and completely. Nobody is so special that they don't have to adhere to it. And people have to understand the consequences of breaking policy too. Your network users need to have a clearly written document, called a *security policy*, that fully identifies and explains what's expected of them and what they can and can't do. Plus, people must be made completely aware of the consequences of breaking the rules, and penalties have to match the severity of the offense and be carried out quickly, if not immediately, to be effective.

Let's take a minute and talk about those penalties. As far back as the mid-1980s, employees were immediately terminated for major technology policy infractions. For example, one guy from a large computer company immediately got his pink slip when pornography was found on his computer's hard drive. The situation was handled decisively—his manager informed him that he was being immediately terminated and that he had one hour to vacate the premises. A security guard stood watch while he cleaned out his desk to make sure the employee only touched personal items—no computer equipment, including storage media—and when he had finished gathering his personal things, the guard then escorted him from the building.

Downloading and installing software from the Internet to your PC at work is not as major (depending on where you work), but from the things we've been over so far, you know that doing that can compromise security. Beta products, new software, and patches need to be tested by the IT department before anyone can use them, period! Here's an example: After an employee installed the untested beta release of a web browser and rebooted their PC, the production Windows server at a national telephone company crashed. The resulting action was to revoke that employee's Internet FTP privileges for three months.

Data Loss Prevention

The data loss prevention policy defines all procedures for preventing the egress of sensitive data from the network and may include references to the use of data loss prevention (DLP) software.

Data leakage occurs when sensitive data is disclosed to unauthorized personnel either intentionally or inadvertently. Data loss prevention (DLP) software attempts to prevent data leakage. It does this by maintaining awareness of actions that can and cannot be taken with respect to a document. For example, it might allow printing of a document but only at the company office. It might also disallow sending the document through email. DLP software uses ingress and egress filters to identify sensitive data that is leaving the organization and can prevent such leakage.

Another scenario might be the release of product plans that should be available only to the Sales group. A security professional could set a policy like the following for that document:

- It cannot be emailed to anyone other than Sales group members.
- It cannot be printed.
- It cannot be copied.

There are two locations where a DLP can be implemented:

- Network DLP: Installed at network egress points near the perimeter, network DLP analyzes network traffic.
- Endpoint DLP: Endpoint DLP runs on end-user workstations or servers in the organization.

Common Documentation

Building a great network requires some really solid planning before you buy even one device for it. And planning includes thoroughly analyzing your design for potential flaws and optimizing configurations everywhere you can to maximize the network's future throughput and performance. If you fail in this phase, trust me—you'll pay dearly later in bottom-line costs and countless hours consumed troubleshooting and putting out the fires of faulty design.

Start planning by creating an outline that precisely delimits all goals and business requirements for the network, and refer back to it often to ensure that you don't deliver a network that falls short of your client's present needs or fails to offer the scalability to grow with those needs. Drawing out your design and jotting down all the relevant information really helps in spotting weaknesses and faults. If you have a team, make sure everyone on it gets to examine the design and evaluate it, and keep that network plan up throughout the installation phase. Hang on to it after implementation has been completed because having it is like having the keys to the kingdom—it will enable you to efficiently troubleshoot any issues that could arise after everything is in place and up and running.

Physical Network Diagram

A physical network diagram contains all the physical devices and connectivity paths on your network and should accurately picture how your network physically fits together in glorious detail. Again, I know it seems like overkill, but ideally, your network diagram should list and map everything you would need to completely rebuild your network from scratch if you had to. This is actually what this type of diagram is designed for. But there's still another physical network diagram variety that includes the firmware revision on all the switches and access points in your network. Remember, besides having your physical network accurately detailed, you must also clearly understand the connections, types of hardware, and their firmware revisions. I'm going to say it again—you will be so happy you have this documentation when troubleshooting! It will prevent much suffering and enable you to fix whatever the problem is so much faster!

Real World Scenario: Avoiding Confusion

Naming your network devices is no big deal, but for some reason, coming up with systems for naming devices and numbering connections can really stress people out.

Let me ease the pain. Let's say your network has two racks of switches, creatively named Block A and Block B. (Sounds like a prison, I know, but it's just to keep things simple for this example. In the real world, you can come up with whatever naming system works for you.)

Anyway, I'm going to use the letters *FETH* for Fast Ethernet; and because each rack has six switches, I'm going to number them (surprise!) 1 through 6. Because we read from left to right, it's intuitive to number the ports on each switch that way too.

Having a solid naming system makes thing so much more efficient—even if it's a bit of a hassle to create. For instance, if you were the system administrator in this example and suddenly all computers connected to FETHB-3 couldn't access any network resources, you would have a pretty good idea of where to look first, right?

If you can't diagram everything, at least make sure all network devices are listed. As I said, physical network diagrams can run from simple, hand-drawn models to insanely complex monsters created by software packages like SmartDraw, Visio, and AutoCAD. Figure 14.2 shows a simple diagram that most of us could draw by hand.

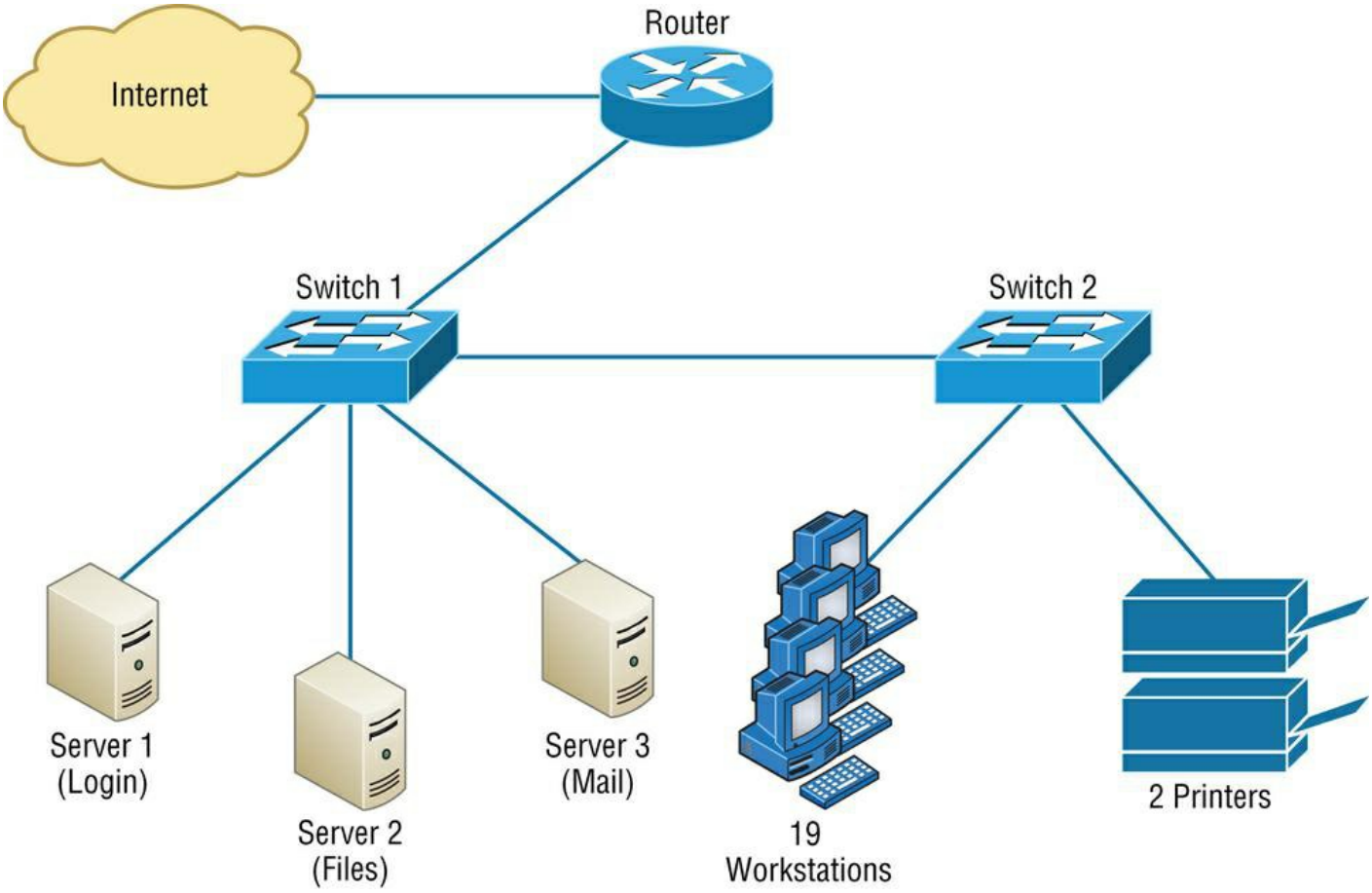

Figure 14.2: Simple network physical diagram

For the artistically impaired, or if you just want a flashier version, Figure 14.3 exhibits a more complex physical diagram. This is an actual sample of what SmartDraw can do for you, and you can get it at `www.smartdraw.com`. In addition, Microsoft Visio provides many or possibly more of these same functions.

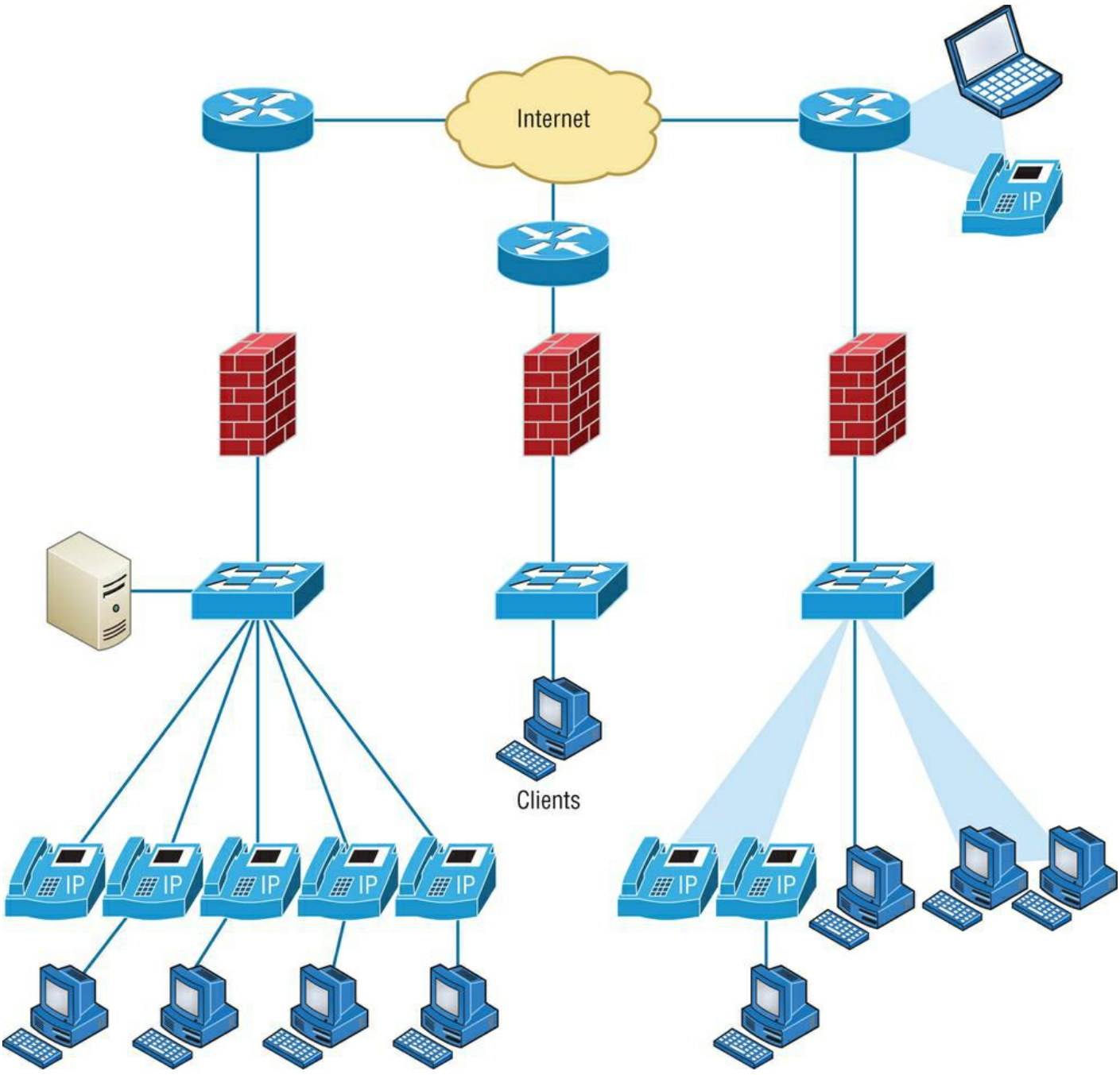

Figure 14.3: Network diagram with firewalls from SmartDraw

Don't throw anything at me, but I need to bring up one last thing: Never forget to mirror any changes you make to your actual network in the network's diagram. Think of it like an updated snapshot. If you give the authorities your college buddy's baby picture after he goes missing, will that really help people recognize him? Not without the help of some high-tech, age-progression software, that's for sure—and they don't make that for networks, so it's better to just keep things up-to-date.

Floor Plan

It's always helpful to have a floor diagram. One of the uses of this is when performing a WLAN site survey. When it's input to the survey software, you can indicate the types of materials found in all walls, doors, and so on, and the survey software can determine the best location for APs.

It can serve as a plotting bed if you have a wireless IPS that has at least three sensors. In that case, when the system sees a rogue AP or evil twin, the software can triangulate the location of the rogue AP and plot it on the floor plan, making it simple to physically locate it and remove it.

Rack Diagram

My next example, also courtesy of SmartDraw, includes diagrams of hardware racks, as revealed in Figure 14.4.

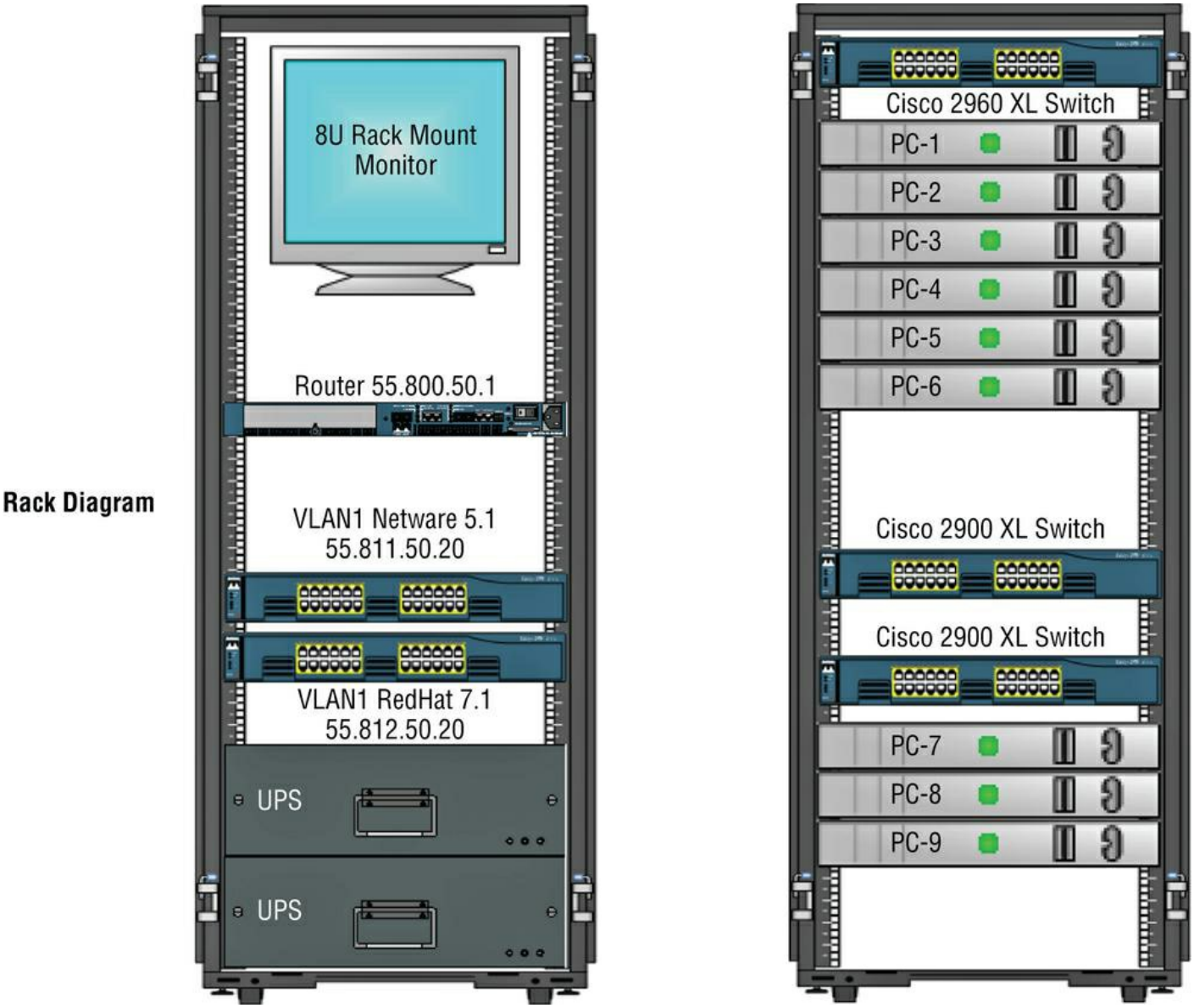

Figure 14.4: Hardware-rack diagram from SmartDraw

Intermediate Distribution Frame (IDF)/Main Distribution Frame (MDF) Documentation

The main distribution frame (MDF) connects equipment (inside plant) to cables and subscriber carrier equipment (outside plant). It also terminates cables that run to intermediate distribution frames distributed throughout the facility.

An intermediate distribution frame (IDF) serves as a distribution point for cables from the MDF to individual cables connected to equipment in areas remote from these frames. The relationship between the IDFs and the MDF is shown in Figure 14.5. This should also be clearly documented and continually updated.

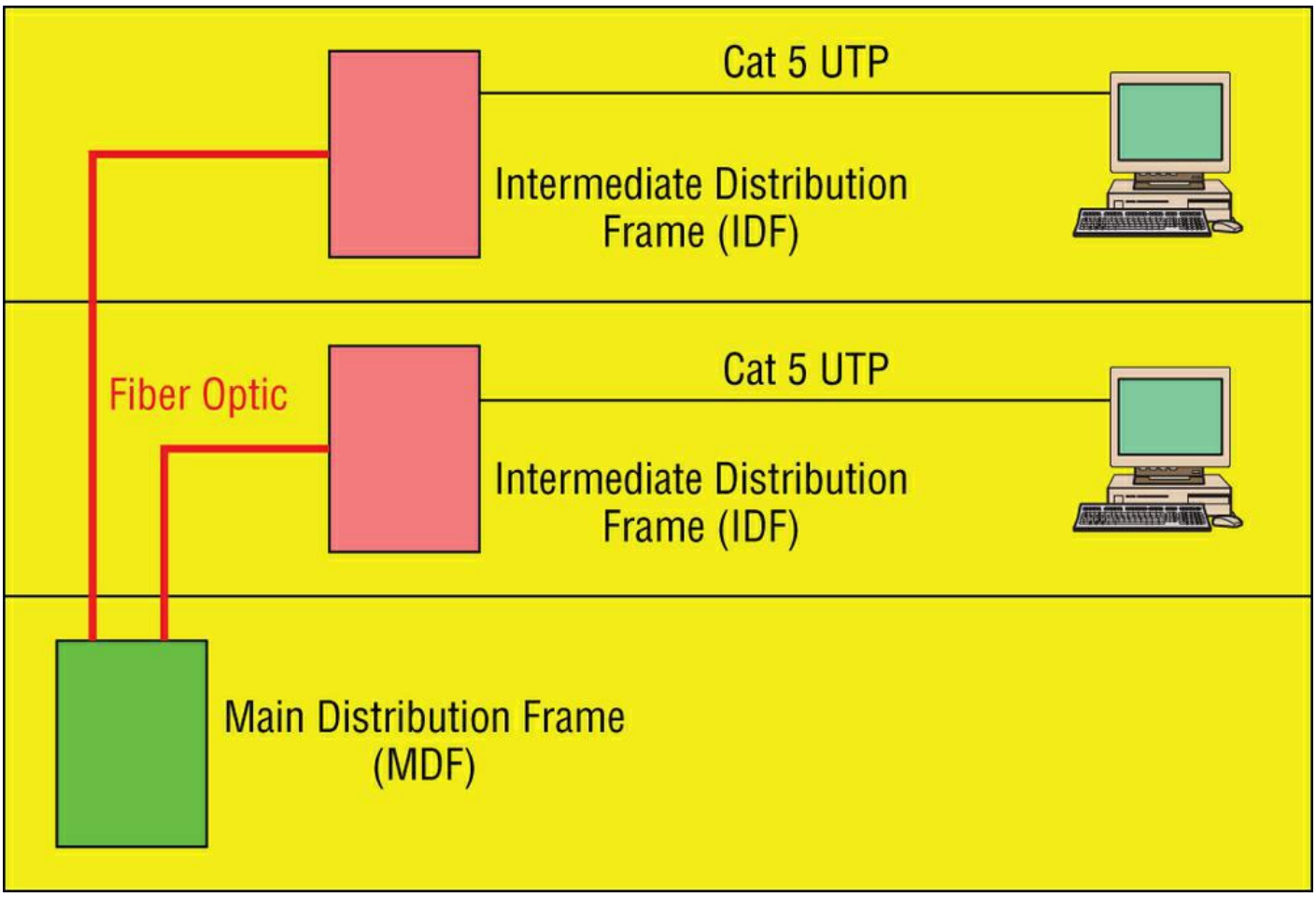

Figure 14.5: MDF and IDFs

Logical Network Diagram

Physical diagrams depict how data physically flows from one area of your network to the next, but a logical network diagram includes things like protocols, configurations, addressing schemes, access lists, firewalls, types of applications, and so on—all things that apply logically to your network. Figure 14.6 shows what a logical network diagram could look like.

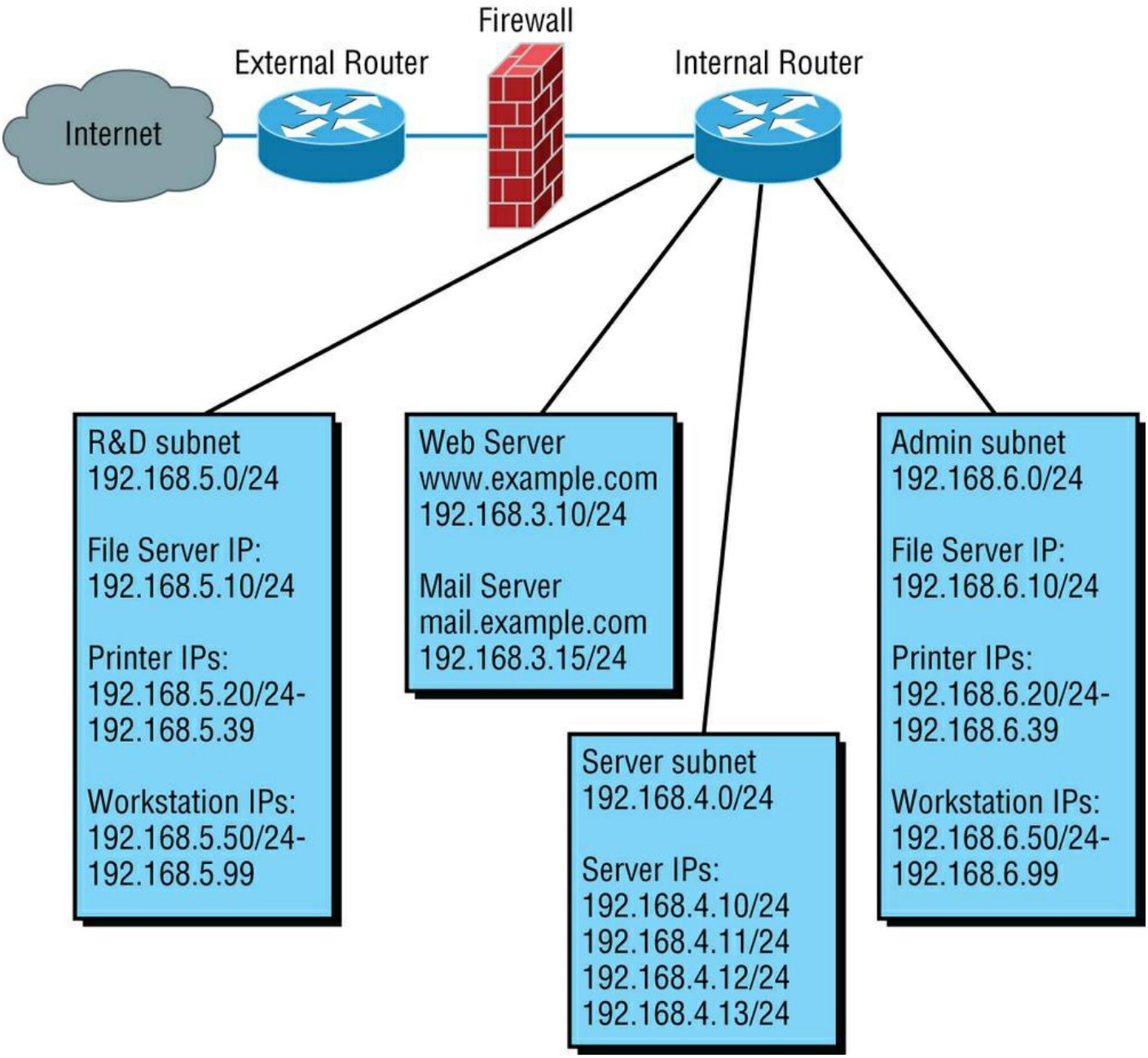

Figure 14.6: Logical network diagram

And just as you mirror any physical changes you make to the network (like adding devices or even just a cable) on your physical diagram, you map logical changes (like creating a new subnet, VLAN, or security zone) on your logical network diagram. It is important that you keep this oh-so-important document up-to-date.

Wiring Diagram

Wireless is definitely the wave of the future, but for now even the most extensive wireless networks have a wired backbone they rely on to connect them to the rest of humanity.

That skeleton is made up of cabled physical media like coax, fiber, and twisted pair. Surprisingly, it is the latter—specifically, unshielded twisted-pair (UTP)—that screams to be pictured in a diagram.

When you're troubleshooting a network, having a diagram is golden. Let's say you discover a connectivity problem between two hosts. Because you've got the map, you know the cable running between them is brand new and custom made. This should tell you to go directly to that new cable because it's likely it was poorly made and is therefore causing the snag.

Another reason it's so important to diagram all things wiring is that all wires have to plug into something somewhere, and it's really good to know what and where that is. Whether it's into a hub, a switch, a router, a workstation, or the wall, you positively need to know the who, what, where, when, and how of the way the wiring is attached.

Note After adding a new cable segment on your network, you need to update the wiring schematics.

Site Survey Report

Site surveys are covered extensively in Chapter 24. Please see that chapter for in-depth information.

Audit and Assessment Report

When audits and assessments are performed, there should be reports created that organize the collected information in a format that can be understood by those who are charged with making security decisions based on the reports. The language should be clear and all terms used should be defined. Keep in mind that decision makers do not always have the same security skills as those they manage.

Security Audit

As discussed earlier in this chapter's "Security Policy" section, a security audit is a thorough examination and testing of your network and all its components to make sure everything is secure. You can either do this internally or hire a third party to conduct an audit if you want the level of security to be certified. A valid and verified consultant's audit is a good follow-up to an internal audit. A number of government agencies usually require you to have your network's security certified in such a way before they'll grant you contract work, particularly if that work is considered confidential, secret, or top secret.

Results of security audits or assessments should be kept and used to perform gap analysis. The results of the latest audit are compared with those of the previous audit to determine if issues have been corrected or if there are still "gaps" to close.

Real World Scenario: Walk Your Beat

A great way to begin a basic security audit to get a feel for any potential threats to your network is to simply take a walk through the company's halls and offices. I've done this a lot, and it always pays off because invariably I happen upon some new and different way that people are trying to "beat the system" regarding security. This doesn't necessarily indicate that a given user is trying to cause damage on purpose; it's just that following the rules can be a little inconvenient—especially when it comes to adhering to strict password policies. Your average user just doesn't get how important their role is in maintaining the security of the network (maybe even their job security as well) by sticking to the network's security policy, so you have to make sure they do.

Think about it. If you can easily discover user passwords just by taking a little tour of the premises, so can a bad guy, and once someone has a username and a password, it's pretty easy to hack into resources. I wasn't kidding about people slapping sticky notes with their usernames and/or passwords right on their monitors—this happens a lot more than you would think. Some users, thinking they're actually being really careful, glue them to the back of their keyboards instead, but you don't have to be James Bond to think about looking there either, right? People wouldn't think of leaving their cars unlocked with the windows down and the keys in the ignition, but that's exactly what they're doing by leaving sensitive info anywhere on or near their workstations.

Even though it might not make you Mr. or Ms. Popularity when you search workspaces or even inside desks for notes with interesting or odd words written on them, do it anyway. People will try to hide these goodies anywhere. Or sometimes, not so much. I kid you not—I had a user who actually wrote his password on the border of his monitor with a Sharpie, and when his password expired, he just crossed it off and wrote the new one underneath it. Sheer genius! But my personal favorite was when I glanced at this one guy's keyboard and noticed that some of the letter keys had numbers written on them. All you had to do was follow the numbers that (surprise!) led straight to his password. Oh sure—he'd followed policy to the, ahem, letter by choosing random letters and numbers, but a lot of good that did—he had to draw himself a little map in plain sight on his keyboard to remember the password.

So, like it or not, you have to walk your beat to find out if users are managing their accounts properly. If you find someone doing things the right way, praise them for it openly. If not, it's time for more training—or maybe worse, termination.

Baseline Configurations

In networking, baseline can refer to the standard level of performance of a certain device or to the normal operating capacity for your whole network. For instance, a specific server's baseline describes norms for factors like how busy its processors are, how much of the memory it uses, and how much data usually goes through the NIC at a given time. A network baseline delimits when a bandwidth is available and the amount of that bandwidth. For networks and networked devices, baselines include information about four key components:

- Processor
- Memory
- Hard-disk (or other storage) subsystem
- Wired/wireless utilization

After everything is up and running, it's a good idea to establish performance baselines on all vital devices and your network in general. To do this, measure things like network usage at three different strategic times to get an accurate assessment. For instance, peak usage usually happens around 8:00 a.m. Monday through Friday, or whenever most people log in to the network in the morning. After hours or on weekends is often when usage is the lowest. Knowing these values can help you troubleshoot bottlenecks or determine why certain system resources are more limited than they should be. Knowing what your baseline is can even tell you if someone's complaints about the network running like a slug are really valid—nice!

It's good to know that you can use network-monitoring software to establish baselines. Even some server operating systems come with software to help with network monitoring, which can help find baselines, perform log management, and even do network graphing as well so you can compare the logs and graphs at a later period of time on your network.

In my experience, it's wise to re-baseline network performance at least once a year. And always pinpoint new performance baselines after any major upgrade to your network's infrastructure.

Common Agreements

In the course of supporting mergers and acquisitions, and in providing support to departments within the organization, it's always important to keep the details of agreements in writing to reduce the risk of misunderstandings. In the following sections, I'll discuss standard documents that are used in these situations. You should be familiar with the purpose of these documents.

Nondisclosure Agreement (NDA)

A nondisclosure agreement (NDA) is an agreement between two parties that defines what information is considered confidential and cannot be shared outside the two parties. An organization may implement NDAs with personnel regarding the intellectual property of the organization. NDAs can also be used when two organizations work together to develop a new product. Because certain information must be shared to make the partnership successful, NDAs are signed to ensure that each partner's data is protected.

While an NDA cannot ensure that confidential data is not shared, it usually provides details on the repercussions for the offending party, including but not limited to fines, jail time, and forfeiture of rights. For example, an organization should decide to implement an NDA when it wants to legally ensure that no sensitive information is compromised through a project with a third party or in a cloud-computing environment.

Service-Level Agreement (SLA)

This is an agreement that defines the allowable time in which a party must respond to issues on behalf of the other party. Most service contracts are accompanied by an SLA, which often include security priorities, responsibilities, guarantees, and warranties.

Memorandum of Understanding (MOU)

This is an agreement between two or more organizations that details a common line of action. It is often used in cases where parties do not have a legal commitment or in situations where the parties cannot create a legally enforceable agreement. In some cases, it is referred to as a letter of intent.

Summary

In this chapter you learned that plans and procedures should be developed to manage operational issues such as change management, incident response, disaster recovery, business continuity, and the system life cycle. You also learned that standard operating procedures should be developed to guide each of these processes.

We also discussed the hardening of systems and the use of security policies that help mitigate security issues such as acceptable use, password, bring your own device (BYOD), remote access. and onboarding and offboarding policies.

Finally, you learned about the importance of critical network documentation such as physical network diagrams, floor plans, rack diagrams, intermediate distribution frame (IDF)/main distribution frame (MDF) documentation, logical network diagrams, and wiring diagrams. We also covered common agreements such as nondisclosure agreements (NDA), service-level agreements (SLA), and

memorandums of understanding (MOUs).

Exam Essentials

Understand the importance of plans and procedures. These include change management, incident response, disaster recovery, business continuity, and the system life cycle.

Describe hardening and security policies. Among these are acceptable use, password, bring your own device (BYOD), remote access, and onboarding and offboarding policies.

Utilize common documentation. These include physical network diagrams, floor plans, rack diagrams, intermediate distribution frame (IDF)/main distribution frame (MDF) documentation, logical network diagrams, wiring diagrams, and site survey reports.

Identify common business agreements. These agreements include nondisclosure agreements (NDA), service-level agreements (SLA), and memorandums of understanding (MOUs).

Written Lab

1. Complete the table by filling in the appropriate plan of which the given step is a part. Choose from the following list: ?
   - Change management plan
   - Incident response plan
   - Disaster recovery plan
   - Business continuity plan
   - System life cycle plan

   You can find the answers in Appendix A.

Step	Plan
Utilization of three network interfaces on the DNS server	
Phased introductions of security patches	
Degaussing of all discarded hard drives	
Security issue escalation list	
System recovery priority chart	

Answers

1.

Step	Plan
Utilization of three network interfaces on the DNS server	Business continuity plan
Phased introductions of security patches	Change management plan
Degaussing of all discarded hard drives	System life cycle plan
Security issue escalation list	Incident response plan
System recovery priority chart	Disaster recovery plan

Review Questions

You can find the answers to the review questions in Appendix B.

1. The way to properly install or remove software on the servers is an example of which of the following? ?
   A. Plan
   B. Policy
   C. Procedure
   D. Code
2. Which of the following is a plan for reversing changes and recovering from any adverse effects from the changes? ?

A. Backup

B. Secondary

C. Rollback

D. Failover

3. Which of the following is the amount of time a system will be down or unavailable during the implementation of changes? ?

A. Downtime

B. Maintenance window

C. MTBF

D. Work factor

4. Which of the following is *not* a device hardening technique? ?

A. Remove unnecessary applications.

B. Deploy an access control vestibule.

C. Block unrequired ports.

D. Disable unnecessary services.

5. Which policy automatically logs a user out after a specified period without activity? ?

A. Password complexity

B. Password history

C. Password length

D. Authentication period

6. BYOD policies apply to what type of device? ?

A. Mobile

B. Desktop

C. Server

D. Firewall

7. Which tool can prevent the emailing of a document to anyone other than Sales group members? ?

A. SSS

B. STP

C. DLP

D. VBA

8. Which of the following connects equipment (inside plant) to cables and subscriber carrier equipment (outside plant)? ?

A. IDF

B. MDF

C. Plant rack

D. Access control vestibule

9. Which of the following is not part of the Information Gathering step of a site survey? ?

A. Determine the scope of the network with respect to applications in use.

B. Verify optimal distances between prospective AP locations.

C. Identify areas that must be covered.

D. Assess types of wireless devices that will need to be supported.

10. Device baselines include information about all but which of the following components? ?

A. CPU

B. Memory

C. Hard disk

D. Display

Answers

1. C. For every policy on your network, there should be a credible related procedure that clearly dictates the steps to take in order to fulfill it.
2. C. Those making the changes should be completely briefed in these rollback procedures, and they should exhibit a clear understanding of them prior to implementing the changes.
3. B. A maintenance window is an amount of time a system will be down or unavailable during the implementation of changes.
4. B. An access control vestibule is an access control solution, not a device hardening technique.
5. D. Authentication period controls how long a user can remain logged in. If a user remains logged in for the specified period without activity, the user will be automatically logged out.
6. A. Bring your qwn device (BYOD) initiatives can be successful if implemented correctly. The key is to implement control over these personal mobile devices that leave the safety of your network and return later after potentially being exposed to environments that are out of your control.
7. C. Data loss prevention (DLP) software attempts to prevent data leakage. It does this by maintaining awareness of actions that can and cannot be taken with respect to a document.
8. B. The main distribution frame (MDF) connects equipment (inside plant) to cables and subscriber carrier equipment (outside plant). It also terminates cables that run to intermediate distribution frames (IDFs) distributed throughout the facility.
9. B. Verifying optimal distances between prospective AP locations is part of the Predeployment Site Survey step.
10. D. For networks and networked devices, baselines include information about four key components: processor, memory, hard-disk (or other storage) subsystem, and wired/wireless utilization.