INFORMATION SECURITY

UNIT-III

Planning for Security: Security policy, Standards and practices, Security blue print, Security education, Continuity strategies.

Security Technology: Firewalls and VPNs: Physical design, firewalls, protects remote connections.

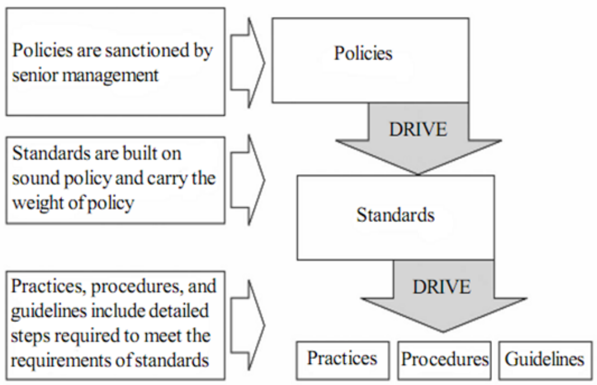
Introduction

- Creation of an information security program begins with creation and/or review of an organization's information security policies, standards, and practices
- Without policy, blueprints, and planning, an organization is unable to meet information security needs of various communities of interest

Key terms covered in this unit are:

- **Policy**: course of action used by organization to convey instructions from management to those who perform duties
- **Policies** are organizational laws
- **Standards**: more detailed statements of what must be done to comply with policy
- **Practices, procedures, and guidelines** effectively explain how to comply with policy
- For a policy to be effective, it must be properly disseminated, read, understood, and agreed to by all members of organization and uniformly enforced

The below diagram shows the relation between security policies, standards and practices


Policies are sanctioned by senior management
Policies
DRIVE
Standards are built on sound policy and carry the weight of policy
Standards
DRIVE
Practices, procedures, and guidelines include detailed steps required to meet the requirements of standards
Practices
Procedures
Guidelines

INFORMATION SECURITY GOVERNANCE

Information governance, or **IG**, is an emerging term used to encompass the set of multi-disciplinary structures, policies, procedures, processes and controls implemented to manage information at an enterprise level, supporting an organization's immediate and future regulatory, legal, risk, environmental and operational requirements.

Steps in IG are shown in the below given figure:

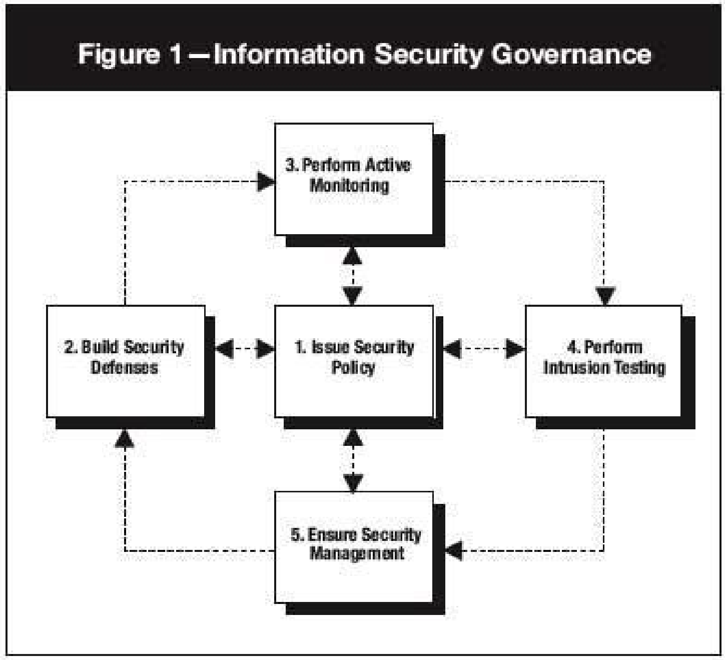


Figure 1 — Information Security Governance
3. Perform Active Monitoring
2. Build Security Defenses
1. Issue Security Policy
4. Perform Intrusion Testing
5. Ensure Security Management

SECURITY POLICIES

Management should define 3 types of security policy, according to the National Institute of Standards and Technology’s special publication 800-14. They are:

1. Enterprise Information Security Policy (EISP)
2. Issue-Specific Security Policy (ISSP)
3. Systems-Specific Policy (SysSP)

For policy to be more effective it must satisfy the following criteria:

1. Dissemination (Distribution)
2. Review (Reading)
3. Comprehension (Understanding)
4. Compliance (Agreement)
5. Uniform Enforcement

1. **Dissemination (Distribution):** the organization must be able to demonstrate that the policy has been made readily available for review by the employee. Commonly used Dissemination techniques are hard copy and electronic distribution.

2. **Review (Reading):** the organization must be able to demonstrate that the disseminated document is in proper format that is understood by all levels of employees of organization. Commonly used techniques for reading are recording the policy in English and other languages

3. **Comprehension (Understanding):** the organization must be able to demonstrate that the employee has understood the requirements and content of the policy. Commonly used techniques are quiz and assessment.

4. **Compliance (Agreement):** the organization must be able to demonstrate that the employee agrees to comply with the policy through act or affirmation. Commonly used techniques are logon banners which require a specific action (mouse click) to acknowledge agreement or a signed document.

5. **Uniform Enforcement:** the organization must be able to demonstrate that the policy has been uniformly enforced, regardless of employee status or assignment.

Enterprise Information Security Policy (EISP)

EISP is also called as information security policy or IT security policy or general security policy.
EISP is based on and directly involved in organizations mission, vision and direction.
It set the strategic direction, scope and tone for all security efforts within the organization.

It is an executive level document, usually prepared with the contribution of chief Information officer (CIO) of an organization.

This document is about 2 to 10 pages long which only focus on security of IT in an organizations environment.

According to National institute of standard, two set principles are involved in EISP such as,

- General compliance to ensure meeting the requirements to establish a program and the responsibilities assigned there in to various organizational components.
- The use of specified penalties and disciplinary actions.

Components of EISP are:

- Statement of purpose: This document will
  - Identify elements of good IS policy
  - Explain need of IS
  - Specify various categories of IS
  - Identify IS responsibility and roles
  - Identify appropriate levels of security through standards and guidelines
- Information security elements: this section will layout security definitions to give a clarity on the IS policy.
- Need for information security: it specifies importance of IS policy in the organization to protect critical information regarding customers, employees and markets.
- Information security roles and responsibilities : defines the organizational structure designed to support IS within organization, identifies categories of individuals with responsibility for information security.
- Reference to other information standards and guidelines : specifies the list of standards That are influenced by policy document perhaps including relevant laws.

Issue Specific Security Policy (ISSP)

In an organization different technologies and processes are use to perform their work, so employees are needed some instructions or guidelines to use effectively .The ISSP,

Indicate specific area of technology.
Needs of latest development and updates.
Focus on organization's positions on specific issues.

Different types of techniques are involved to create and manage ISSP within the organization. Following are the three techniques used,

Create a number of independent ISSP documents for each and every issue.
Create a single and simple ISSP document which include all issues.

Create a modular ISSP documents that distinct the policies when created and administrate the issues.

Components of ISSP are:

- Statement of policy
- Authorized access and usage of equipment
- Prohibited usage of equipment
- Systems management
- Violations of policy
- Policy review and modification
- Limitation of liability

Systems -Specific Policies (SysSP)

SysSp frequently function according to standards procedures used when system are going to configure or maintain.

Types of SysSP :

SysSp falls into two groups,

Managerial Guidance SysSp : These are created by management .The basic aim is to guide the implementation and configuration of the technology and also the employees working behavior in a firm

Technical Specifications SysSP : These are technical policy or set of configuration to implement managerial policy .

Technical SysSP are divided into other sub groups.

- **Access Control List (ACLs)**: It consist of list, matrices and capability tables that provide rights and benefits to the user for its specific system.
- **Configuration Rules**: It comprise the specific configuration codes, which are entered into security system .The objective is to guide the user for the execution of the system.

Policy Management

Policy are generally known as plan with a document of principles which should managed accordingly to the changes.

Special consideration should be made for organizations which involve the mergers, takeover and partnership.

For an effective security policy ,the consideration should be involve,

- **Responsible individual:** As per the companies information and security policy, a manager is required who has complete knowledge of both as a professional (technical) or policy requirement. He is called as policy administrator. He link as middleman between superior and low-level employees. He should poses their work according to implementation of policy to guide , educate and provide valuable suggestions.
- **Schedule review**: Today every business operations are change according to changing environment .So, the policy should be changing according to requirements inorder to reach the set objectives of a firm . A proper schedule can be prepare in the form of printed document which helps for an effective control operations.
- **Review Procedure and Practices**: To make the effective implementation of policy, a manager should develop a procedure or structure by taking a various recommendations and feedbacks from others. Different methods such as email, drop-box etc., can be use for revision of policy . The involvement and guidance from sub employees makes the policy to practice in a possible way.
- **Policy and revision date**: whenever the policy prepared it should include the various dates , if not the confusion may arise. Some policies may include expiration date i.e., *sunset clause* and short-term business agencies or associates should involve to make the policy an effective implementation.
- **Automated Policy Management**: Due to change and improvement in information technology policy, softwares are developed according to requirement . These softwares are automated in nature to tackle the problem or workflow of approved policy, a computer based information techniques are needed such as training and testing, which improves knowledge among employees for its implementation.

Information Security Blueprint

- Basis for design, selection, and implementation of all security policies, education and training programs, and technological controls
- More detailed version of security framework (outline of overall information security strategy for organization)
- Should specify tasks to be accomplished and the order in which they are to be realized
- Should also serve as scalable, upgradeable, and comprehensive plan for information security needs for coming years

BS 7799 Part 1

One of the most widely referenced and often discussed security models is Information Technology – Code of Practice for Information Security Management, which was originally published as British Standard BS 7799.

The purpose of ISO/IEC 17799 is to “give recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization.

It is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings.”

Volume 2 provides information on how to implement Volume 1 (17799) and how to set up an Information Security Management Structure (ISMS).

ISO 27000 Series

The ISO 27000 series of standards have been specifically reserved by ISO for information security matters. This of course, aligns with a number of other topics, including ISO 9000 (quality management) and ISO 14000 (environmental management).

As with the above topics, the 27000 series will be populated with a range of individual standards and documents. A number of these are already well known, and indeed, have been published. Others are scheduled for publication, with final numbering and publication details yet to be determined.
The following matrix reflects the current known position for the major operational standards in the series:

The following matrix reflects the current known position for the major operational standards in the series:

ISO 27001 This is the specification for an information security management system (an ISMS) which replaced the old BS7799-2 standard	**ISO 27002** This is the 27000 series standard number of what was originally the ISO 17799 standard (which itself was formerly known as BS7799-1)..
ISO 27003 This will be the official number of a new standard intended to offer guidance for the implementation of an ISMS (IS Management System) .	**ISO 27004** This standard covers information security system management measurement and metrics, including suggested ISO27002 aligned controls..

ISO 27005 This is the methodology independent ISO standard for information security risk management..	**ISO 27006** This standard provides guidelines for the accreditation of organizations offering ISMS certification.

The position of course is currently fairly fluid, but we will update this site as new information emerges. Please see our news page for the latest position.

The **ISO 27001** standard was published in October 2005, essentially replacing the old BS7799-2 standard. It is the specification for an ISMS, an Information Security Management System. BS7799 itself was a long standing standard, first published in the nineties as a code of practice. As this matured, a second part emerged to cover management systems. It is this against which certification is granted. Today in excess of a thousand certificates are in place, across the world.

ISO 27001 enhanced the content of BS7799-2 and harmonized it with other standards. A scheme has been introduced by various certification bodies for conversion from BS7799 certification to ISO27001 certification

THE CONTENTS OF ISO 27001

The content sections of the standard are:

- Management Responsibility
- Internal Audits
- ISMS Improvement
- Annex A - Control objectives and controls
- Annex B - OECD principles and this international standard

- Annex C - Correspondence between ISO 9001, ISO 14001 and this standard

The **ISO 27002** standard is the rename of the ISO 17799 standard, and is a code of practice for information security. It basically outlines hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided within ISO 27001.

The standard "established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization". The actual controls listed in the standard are intended to address the specific requirements identified via a formal risk assessment. The standard is also intended to provide a guide for the development of "organizational security standards and effective security management practices and to help build confidence in inter-organizational activities".

The basis of the standard was originally a document published by the UK government, which became a standard 'proper' in 1995, when it was re-published by BSI as BS7799. In 2000 it was again re-published, this time by ISO ,as ISO 17799. A new version of this appeared in 2005, along with a new publication, ISO 27001. These two documents are intended to be used together, with one complimenting the other.

ISO's future plans for this standard are focused largely around the development and publication of industry specific versions (for example: health sector, manufacturing, and so on). Note that this is a lengthy process, so the new standards will take some time to appear.

THE CONTENTS OF ISO 17799 / 27002

The content sections are:

- Structure
- Risk Assessment and Treatment
- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical Security
- Communications and Ops Management
- Access Control

PLAN-DO-CHECK-ACT

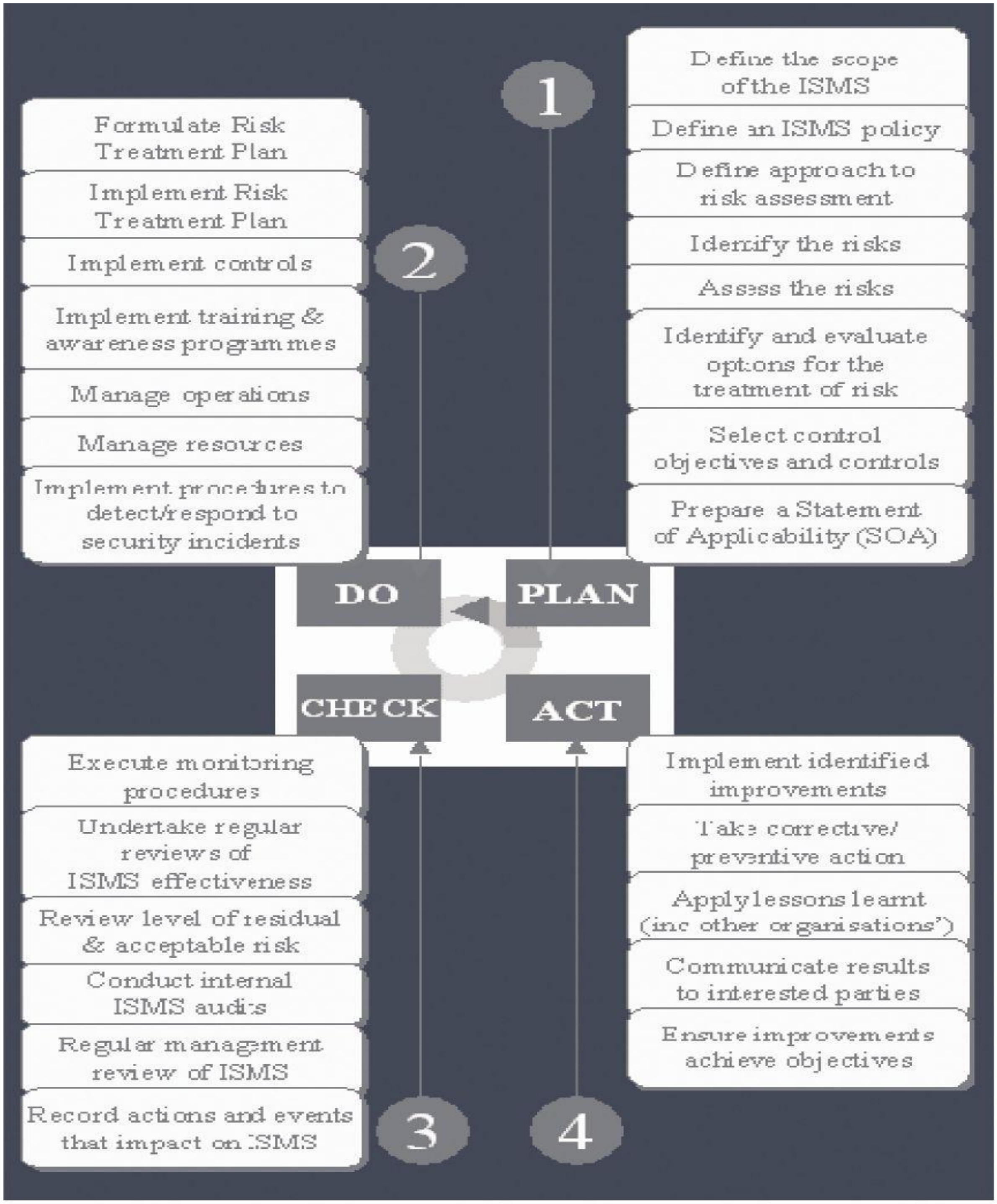

1
Define the scope of the ISMS
Define an ISMS policy
Define approach to risk assessment
Identify the risks
Assess the risks
Identify and evaluate options for the treatment of risk
Select control objectives and controls
Prepare a Statement of Applicability (SOA)
2
Formulate Risk Treatment Plan
Implement Risk Treatment Plan
Implement controls
Implement training & awareness programmes
Manage operations
Manage resources
Implement procedures to detect/respond to security incidents
DO
PLAN
CHECK
ACT
3
Execute monitoring procedures
Undertake regular reviews of ISMS effectiveness
Review level of residual & acceptable risk
Conduct internal ISMS audits
Regular management review of ISMS
Record actions and events that impact on ISMS
4
Implement identified improvements
Take corrective/ preventive action
Apply lessons learnt (inc other organisations')
Communicate results to interested parties
Ensure improvements achieve objectives

FIGURE 6-2 Plan-Do-Check-Act Cycle from BS 7799:2

ISO/IEC 17799 Drawbacks

The global information security community has not defined any justification for a code of practice as identified in the ISO/IEC 17799

ISO/IEC 17799 lacks “the necessary measurement precision of a technical standard”

There is no reason to believe that ISO/IEC 17799 is more useful than any other approach

ISO/IEC 17799 is not as complete as other frameworks

ISO/IEC 17799 is perceived to have been hurriedly prepared, given the tremendous impact its adoption could have on industry information security controls

The Ten Sections of ISO/IEC 17799

1. **Organizational Security Policy is needed to provide management direction and support for information security.**

2. **Organizational Security Infrastructure objectives include:**

Manage information security within the company

Maintain the security of organizational information processing facilities and information assets accessed by third parties

Maintain the security of information when the responsibility for information processing has been outsourced to another organization

3. **Asset Classification and Control is needed to maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection**.

4. **Personnel Security objectives are:**

Reduce risks of human error, theft, fraud or misuse of facilities

Ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work

Minimize the damage from security incidents and malfunctions and learn from such incidents

5. **Physical and Environmental Security objectives include:**

Prevent unauthorized access, damage and interference to business premises and information

Prevent loss, damage or compromise of assets and interruption to business activities

Prevent compromise or theft of information and information processing facilities

6. **Communications and Operations Management objectives are:**

Ensure the correct and secure operation of information processing facilities

Minimize the risk of systems failures

Protect the integrity of software and information

Maintain the integrity and availability of information processing and communication

Ensure the safeguarding of information in networks and the protection of the supporting infrastructure

Prevent damage to assets and interruptions to business activities

Prevent loss, modification or misuse of information exchanged between organizations

7. **System Access Control objectives in this area include:**

Control access to information

Prevent unauthorized access to information systems

Ensure the protection of networked services

Prevent unauthorized computer access

Detect unauthorized activities

Ensure information security when using mobile computing and telecommunication networks

8**. System Development and Maintenance objectives include:**

Ensure security is built into operational systems

Prevent loss, modification or misuse of user data in application systems

Protect the confidentiality, authenticity and integrity of information

Ensure IT projects and support activities are conducted in a secure manner

Maintain the security of application system software and data

9. **Business Continuity Planning to counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.**

10. **Compliance objectives include:**

Avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements .Ensure compliance of systems with organizational security policies and standards.Maximize the effectiveness of and minimize interference to/from the system audit process

NIST SP 800-12

SP 800-12 is entitled The Computer Security Handbook, and is an excellent reference and guide for the routine management of information security.

It provides little guidance, however, on design and implementation of new security systems; use it as a supplement to gain a deeper understanding in the background and terminology.

800-12 also lays out the NIST philosophy on security management by identifying 17 controls organized into three categories:

The Management Controls section addresses security topics that can be characterized as managerial.

The Operational Controls section addresses security controls that focus on controls that are, broadly speaking, implemented and executed by people (as opposed to systems).

The Technical Controls section focuses on security controls that the computer system executes.

NIST Special Publication 800-14

NIST SP800-14, subtitled Generally Accepted Principles and Practices for Securing Information Technology Systems, describes best practices and provides information on commonly accepted information security principles that can direct the security team in the development of a security blueprint.

It also describes the philosophical principles that the security team should integrate into the entire information security process, expanding upon the components of SP 800-12.

The more significant points made in NIST SP 800-14 are as follows:

1) Security Supports the Mission of the Organization.

2) Security is an Integral Element of Sound Management.

3) Security Should Be Cost-Effective

4) Systems Owners Have Security Responsibilities Outside Their Own Organizations.

5) Security Responsibilities and Accountability Should Be Made Explicit.

6) Security Requires a Comprehensive and Integrated Approach.

7) Security Should Be Periodically Reassessed.

8) Security is Constrained by Societal Factors.

Principle 1. Establish a sound security policy as the “foundation” for design.

Principle 2. Treat security as an integral part of the overall system design.

Principle 3. Clearly delineate the physical and logical security boundaries governed by associated security policies.

Principle 4. Reduce risk to an acceptable level.

Principle 5. Assume that external systems are insecure.

Principle 6. Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.

Principle 7. Implement layered security (Ensure no single point of vulnerability).

Principle 8. Implement tailored system security measures to meet organizational security goals.

Principle 9. Strive for simplicity.

Principle 10. Design and operate an IT system to limit vulnerability and to be resilient in response.

Principle 11. Minimize the system elements to be trusted.

Principle 12. Implement security through a combination of measures distributed physically and logically.

Principle 13. Provide assurance that the system is, and continues to be, resilient in the face of expected threats.

Principle 14. Limit or contain vulnerabilities.

Principle 15. Formulate security measures to address multiple overlapping information domains.

Principle 16. Isolate public access systems from mission critical resources.

Principle 17. Use boundary mechanisms to separate computing systems and network infrastructures.

Principle 18. Where possible, base security on open standards for portability and interoperability.

Principle 19. Use common language in developing security requirements.

Principle 20. Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.

Principle 21. Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.

Principle 22. Authenticate users and processes to ensure appropriate access control decisions both within and across domains.

Principle 23. Use unique identities to ensure accountability.

Principle 24. Implement least privilege.

Principle 25. Do not implement unnecessary security mechanisms.

Principle 26. Protect information while being processed, in transit, and in storage.

Principle 27. Strive for operational ease of use.

Principle 28. Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.

Principle 29. Consider custom products to achieve adequate security.

Principle 30. Ensure proper security in the shutdown or disposal of a system.

Principle 31. Protect against all likely classes of "attacks."

Principle 32. Identify and prevent common errors and vulnerabilities.

Principle 33. Ensure that developers are trained in how to develop secure software.

NIST Special Publication 800-18

NIST SP 800-18 - A Guide for Developing Security Plans for Information Technology Systems, provides detailed methods for assessing, designing, and implementing controls and plans for various sized applications.

SP 800-18 serves as a guide for the activities described in this chapter, and for the overall information security planning process.

It includes templates for major application security plans.

NIST Special Publication 800-26

Management Controls

1. Risk Management

2. Review of Security Controls

3. Life Cycle Maintenance

4. Authorization of Processing (Certification and Accreditation)

5. System Security Plan

Operational Controls

6. Personnel Security

7. Physical Security

8. Production, Input/Output Controls

9. Contingency Planning

10. Hardware and Systems Software

11. Data Integrity

12. Documentation

13. Security Awareness, Training, and Education

14. Incident Response Capability

Technical Controls

15. Identification and Authentication

16. Logical Access Controls

17. Audit Trails

These 17 areas are the core of the NIST security management structure.

NIST Special Publication 800-30

NIST SP 800-30 - Risk Management Guide for Information Technology Systems provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems.

The ultimate goal is to help organizations to better manage IT-related mission risks.

Security Management Practices

In information security, two categories of benchmarks are used: standards of due care/due diligence, and best practices.

Best practices include a sub-category of practices—called the gold standard—that are general regarded as "the best of the best."

Standards of Due Care/Due Diligence

When organizations adopt minimum levels of security for a legal defense, they may need to show that they have done what any prudent organization would do in similar circumstances; this is known as a standard of due care.

Implementing controls at this minimum standard, and maintaining them, demonstrates that an organization has performed due diligence.

Due diligence requires that an organization ensure that the implemented standards continue to provide the required level of protection.

Failure to support a standard of due care or due diligence can expose an organization to legal liability, provided it can be shown that the organization was negligent in its application or lack of application of information protection.

When organizations adopt minimum levels of security for a legal defense, they may need to show that they have done what any prudent organization would do in similar circumstances; this is known as a standard of due care.

Implementing controls at this minimum standard, and maintaining them, demonstrates that an organization has performed due diligence.

Due diligence requires that an organization ensure that the implemented standards continue to provide the required level of protection.

Failure to support a standard of due care or due diligence can expose an organization to legal liability, provided it can be shown that the organization was negligent in its application or lack of application of information protection.

Best Security Practices

Security efforts that seek to provide a superior level of performance in the protection of information are referred to as best business practices or simply best practices.

Some organizations refer to these as recommended practices.

Security efforts that are among the best in the industry are referred to as best security practices

These practices balance the need for information access with the need for adequate protection. Best practices seek to provide as much security as possible for information and information systems while demonstrating fiscal responsibility and ensuring information access.

Companies with best practices may not be the best in every area; they may only have established an extremely high quality or successful security effort in one area.

Security efforts that seek to provide a superior level of performance in the protection of information are referred to as best business practices or simply best practices.

Some organizations refer to these as recommended practices.

Security efforts that are among the best in the industry are referred to as best security practices

These practices balance the need for information access with the need for adequate protection. Best practices seek to provide as much security as possible for information and information systems while demonstrating fiscal responsibility and ensuring information access.

Companies with best practices may not be the best in every area; they may only have established an extremely high quality or successful security effort in one area.

VISA International Security Model

Another example of best practices is the VISA International™ Security Model.

VISA has developed two important documents that improve and regulate its information systems:

The “Security Assessment Process” document contains a series of recommendations for the detailed examination of an organization’s systems with the eventual goal of integration into the VISA systems.

The “Agreed Upon Procedures” document outlines the policies and technologies used to safeguard security systems that carry the sensitive cardholder information to and from VISA systems.

Selecting Best Practices

Choosing which recommended practices to implement can pose a challenge for some organizations.

In industries that are regulated by governmental agencies, government guidelines are often requirements.

For other organizations, government guidelines are excellent sources of information about what other organizations are required to do to control information security risks, and can inform their selection of best practices.

When considering best practices for your organization, consider the following:

Does your organization resemble the identified target organization of the best practice?

Are you in a similar industry as the target?

Do you face similar challenges as the target?

Is your organizational structure similar to the target?

Are the resources you can expend similar to those called for by the best practice?

Are you in a similar threat environment as the one assumed by the best practice?

Best Practices

- Microsoft has published a set of best practices in security at its Web site:
- Use antivirus software
- Use strong passwords
- Verify your software security settings
- Update product security
- Build personal firewalls
- Back up early and often
- Protect against power surges and loss

Benchmarking and Best Practices Limitations

The biggest problem with benchmarking in information security is that organizations don't talk to each other; a successful attack is viewed as an organizational failure, and is kept secret, insofar as possible.

However, more and more security administrators are joining professional associations and societies like ISSA and sharing their stories and lessons learned.

An alternative to this direct dialogue is the publication of lessons learned.

Base Lining

A baseline is a "value or profile of a performance metric against which changes in the performance metric can be usefully compared."

Baselining is the process of measuring against established standards. In InfoSec, baselining is the comparison of security activities and events against the organization's future performance.

Baselining can provide the foundation for internal benchmarking, as information gathered for an organization's first risk assessment becomes the baseline for future comparisons.

The Gartner group offers twelve questions as a self assessment for best security practices.

People:

1) "Do you perform background checks on all employees with access to sensitive data, areas, or access points?

2) "Would the average employee recognize a security issue?

3) "Would they choose to report it?

4) "Would they know how to report it to the right people?

Processes:

5) "Are enterprise security policies updated on at least an annual basis, employees educated on changes, and consistently enforced?

6) "Does your enterprise follow a patch/update management and evaluation process to prioritize and mediate new security vulnerabilities?

7) "Are the user accounts of former employees immediately removed on termination?

8) “Are security group representatives involved in all stages of the project life cycle for new projects?

Technology:

9) “Is every possible route to the Internet protected by a properly configured firewall?

10) “Is sensitive data on laptops and remote systems encrypted?

11) “Do you regularly scan your systems and networks, using a vulnerability analysis tool, for security exposures?

12) “Are malicious software scanning tools deployed on all workstations and servers?”

Emerging Trends in Certification and Accreditation

In security management, accreditation is the authorization of an IT system to process, store, or transmit information.

It is issued by a management official and serves as a means of assuring that systems are of adequate quality.

It also challenges managers and technical staff to find the best methods to assure security, given technical constraints, operational constraints, and mission requirements.

Certification is “the comprehensive evaluation of the technical and non-technical security controls of an IT system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.”

Organizations pursue accreditation or certification to gain a competitive advantage, or to provide assurance or confidence to customers.

DESIGN OF SECURITY ARCHITECTURE

- Defense in depth
    - Implementation of security in layers
    - Requires that organization establish sufficient security controls and safeguards so that an intruder faces multiple layers of controls
- Security perimeter

- Point at which an organization’s security protection ends and outside world begins
- Does not apply to internal attacks from employee threats or on-site physical threats

- Firewall: device that selectively discriminates against information flowing into or out of organization
- Demilitarized zone (DMZ): no-man’s land between inside and outside networks where some organizations place Web servers
- Proxy servers: performs actions on behalf of another system
- Intrusion detection systems (IDSs): in effort to detect unauthorized activity within inner network, or on individual machines, organization may wish to implement an IDS

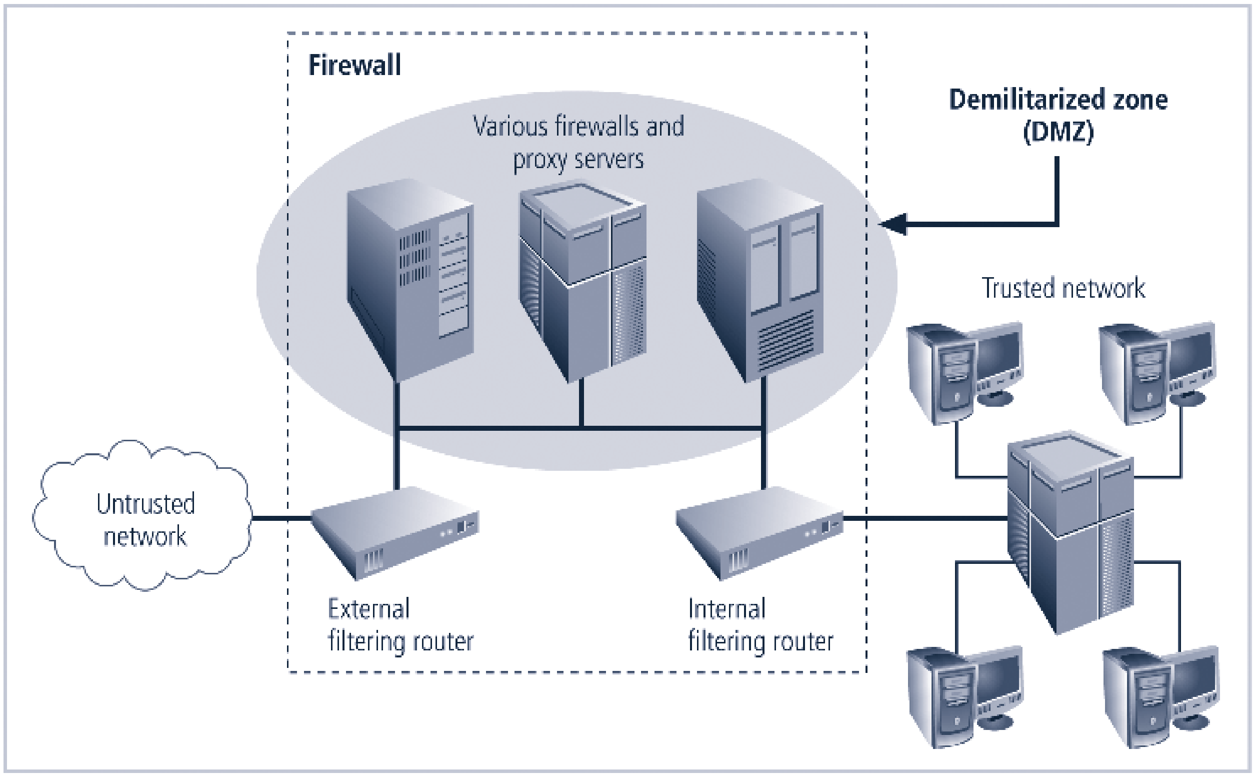
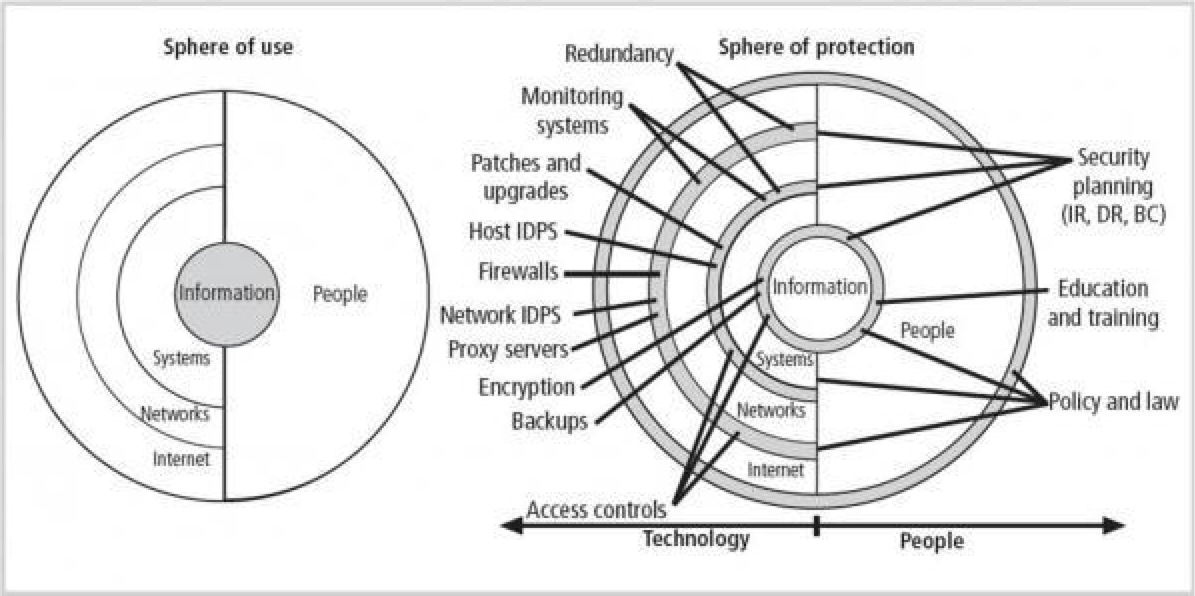
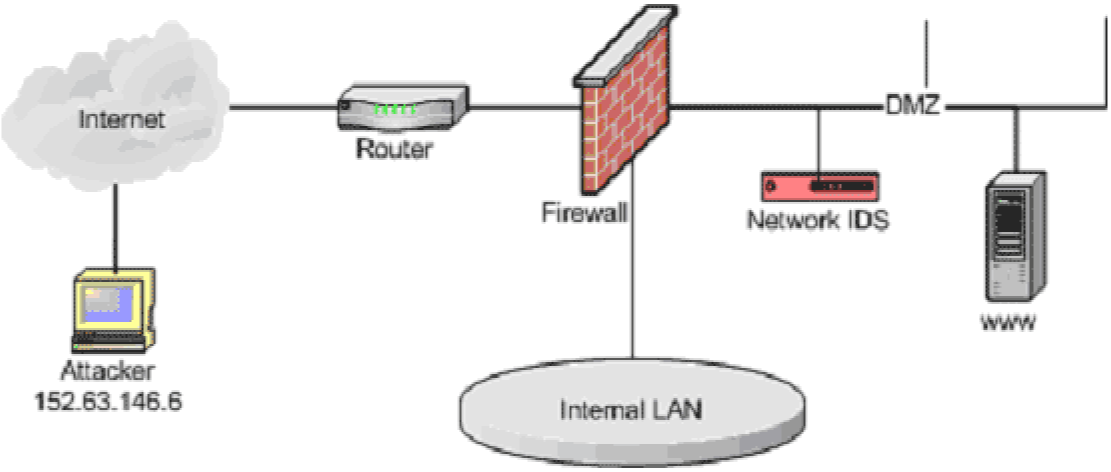

Firewall
Various firewalls and proxy servers
Demilitarized zone (DMZ)
Trusted network
Untrusted network
External filtering router
Internal filtering router

FIGURE 5-18 Firewalls, Proxy Servers, and DMZs

Spheres of security



Intrusion detection system



An **intrusion detection system** (**IDS**) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system**. Intrusion detection and prevention systems** (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.

IDPSes typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content.

Security Education, Training, and Awareness Program

- As soon as general security policy exists, policies to implement security education, training, and awareness (SETA) program should follow
- SETA is a control measure designed to reduce accidental security breaches
- Security education and training builds on the general knowledge the employees must possess to do their jobs, familiarizing them with the way to do their jobs securely
- The SETA program consists of three elements: security education; security training; and security awareness.

Security awareness training in most organizations focuses on familiarizing the employees with the organizational security policy. The security awareness focus for users may include:

- educating users on the creation of good passwords
- do's and don'ts for maintaining workstations
- informing users of email and Internet access policies
- employee responsibility for computer security
- reporting procedures
- emergency procedures
- The focus for security awareness for system administrators may include:
- training on how to configure systems securely
- education on user account management policies

- secure remote access for support of systems

Continuity Strategies

- Incident response plans (IRPs); disaster recovery plans (DRPs); business continuity plans (BCPs)
- Primary functions of above plans
    - IRP focuses on immediate response; if attack escalates or is disastrous, process changes to disaster recovery and BCP
    - DRP typically focuses on restoring systems after disasters occur; as such, is closely associated with BCP
    - BCP occurs concurrently with DRP when damage is major or long term, requiring more than simple restoration of information and information resources

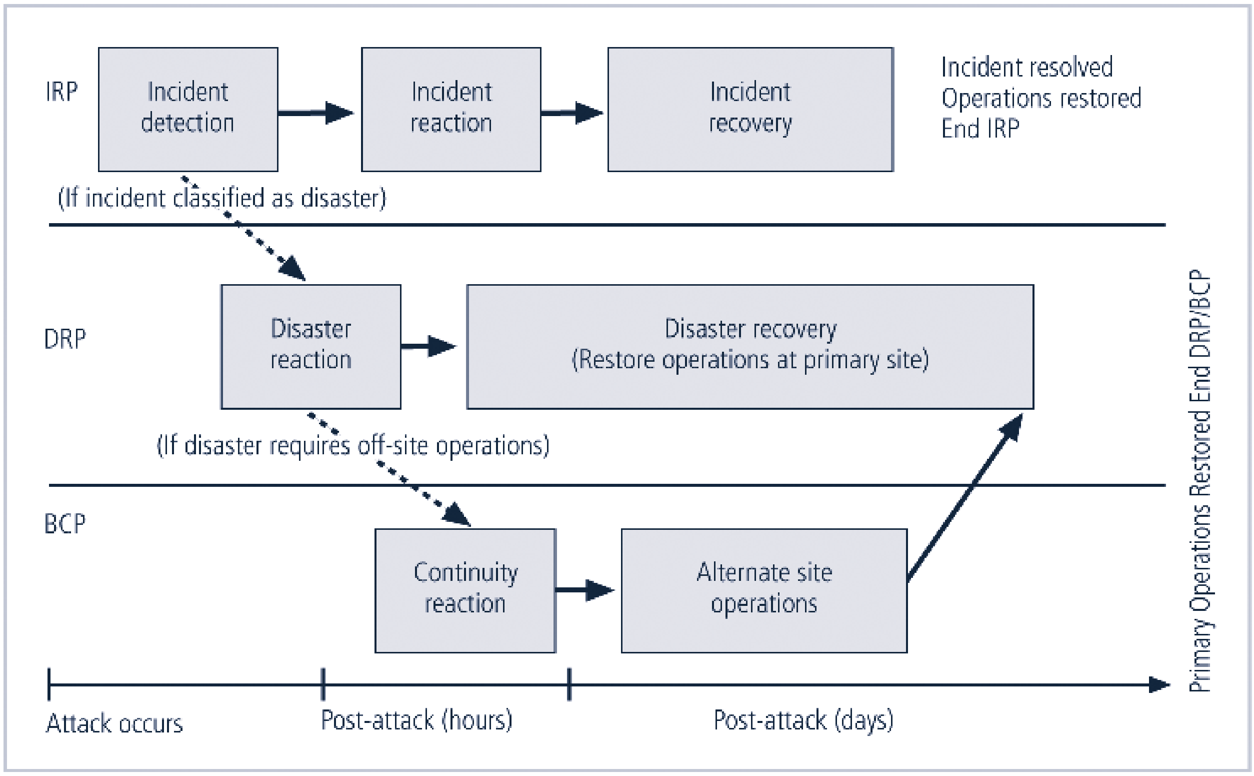


FIGURE 5-22 Contingency Planning Timeline

Major steps in contingency planning

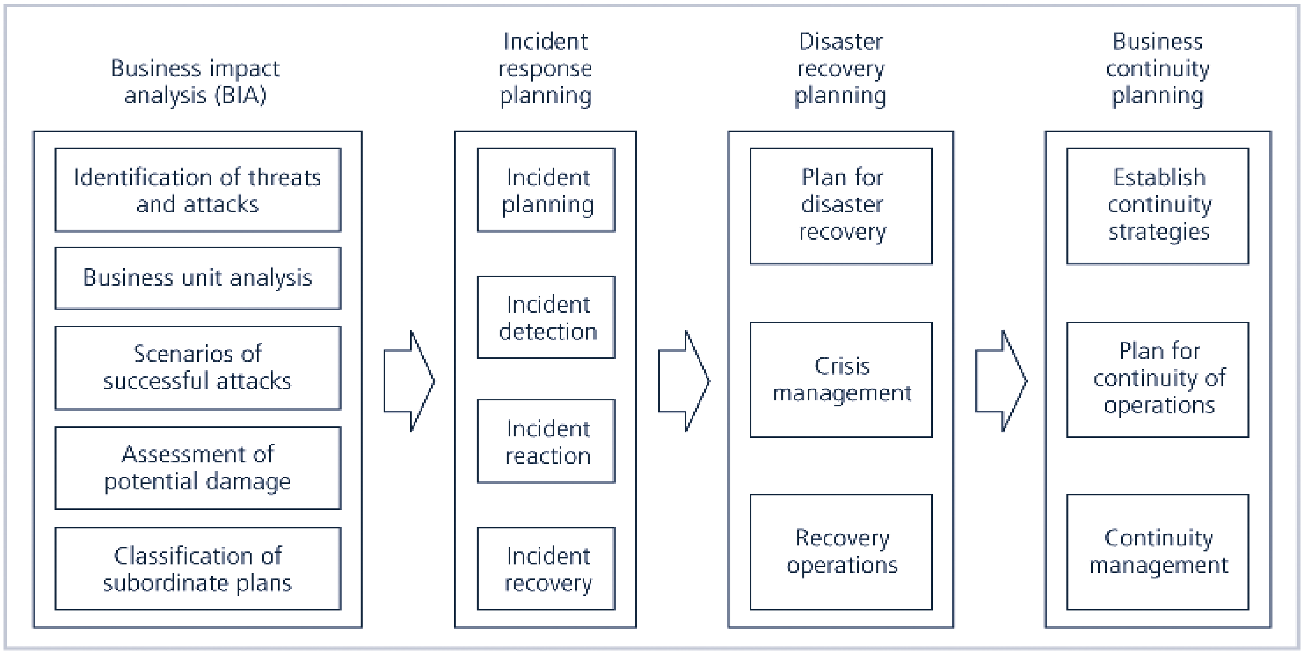

Business impact analysis (BIA)
Identification of threats and attacks
Business unit analysis
Scenarios of successful attacks
Assessment of potential damage
Classification of subordinate plans
Incident response planning
Incident planning
Incident detection
Incident reaction
Incident recovery
Disaster recovery planning
Plan for disaster recovery
Crisis management
Recovery operations
Business continuity planning
Establish continuity strategies
Plan for continuity of operations
Continuity management

FIGURE 5-23 Major Steps in Contingency Planning

Incident Response Planning

- Incident response planning covers identification of, classification of, and response to an incident
- Attacks classified as incidents if they:
    - Are directed against information assets
    - Have a realistic chance of success
    - Could threaten confidentiality, integrity, or availability of information resources
- Incident response (IR) is more reactive than proactive, with the exception of planning that must occur to prepare IR teams to be ready to react to an incident

Incident Detection

- Most common occurrence is complaint about technology support, often delivered to help desk
- Careful training needed to quickly identify and classify an incident

- Once attack is properly identified, organization can respond

Incident Reaction

- Consists of actions that guide organization to stop incident, mitigate impact of incident, and provide information for recovery from incident
- In reacting to an incident, there are actions that must occur quickly:
  - Notification of key personnel
  - Documentation of incident

Incident Containment Strategies

- Before incident can be contained, areas affected must be determined
- Organization can stop incident and attempt to recover control through a number or strategies

Incident Recovery

- Once incident has been contained and control of systems regained, the next stage is recovery
- First task is to identify human resources needed and launch them into action
- Full extent of the damage must be assessed
- Organization repairs vulnerabilities, addresses any shortcomings in safeguards, and restores data and services of the systems

Damage Assessment

- Several sources of information on damage, including system logs; intrusion detection logs; configuration logs and documents; documentation from incident response; and results of detailed assessment of systems and data storage

- Computer evidence must be carefully collected, documented, and maintained to be acceptable in formal or informal proceedings
- Individuals who assess damage need special training

Automated Response

- New systems can respond to incident threat autonomously
- Downsides of current automated response systems may outweigh benefits
- Entrapment is luring an individual into committing a crime to get a conviction
- Enticement is legal and ethical, while entrapment is not

Disaster Recovery Planning

- Disaster recovery planning (DRP) is planning the preparation for and recovery from a disaster
- The contingency planning team must decide which actions constitute disasters and which constitute incidents
- When situations are classified as disasters, plans change as to how to respond; take action to secure most valuable assets to preserve value for the longer term
- DRP strives to reestablish operations at the primary site

Business Continuity Planning

- Outlines reestablishment of critical business operations during a disaster that impacts operations
- If disaster has rendered the business unusable for continued operations, there must be a plan to allow business to continue functioning
- Development of BCP is somewhat simpler than IRP or DRP; consists primarily of selecting a continuity strategy and integrating off-site data storage and recovery functions into this strategy

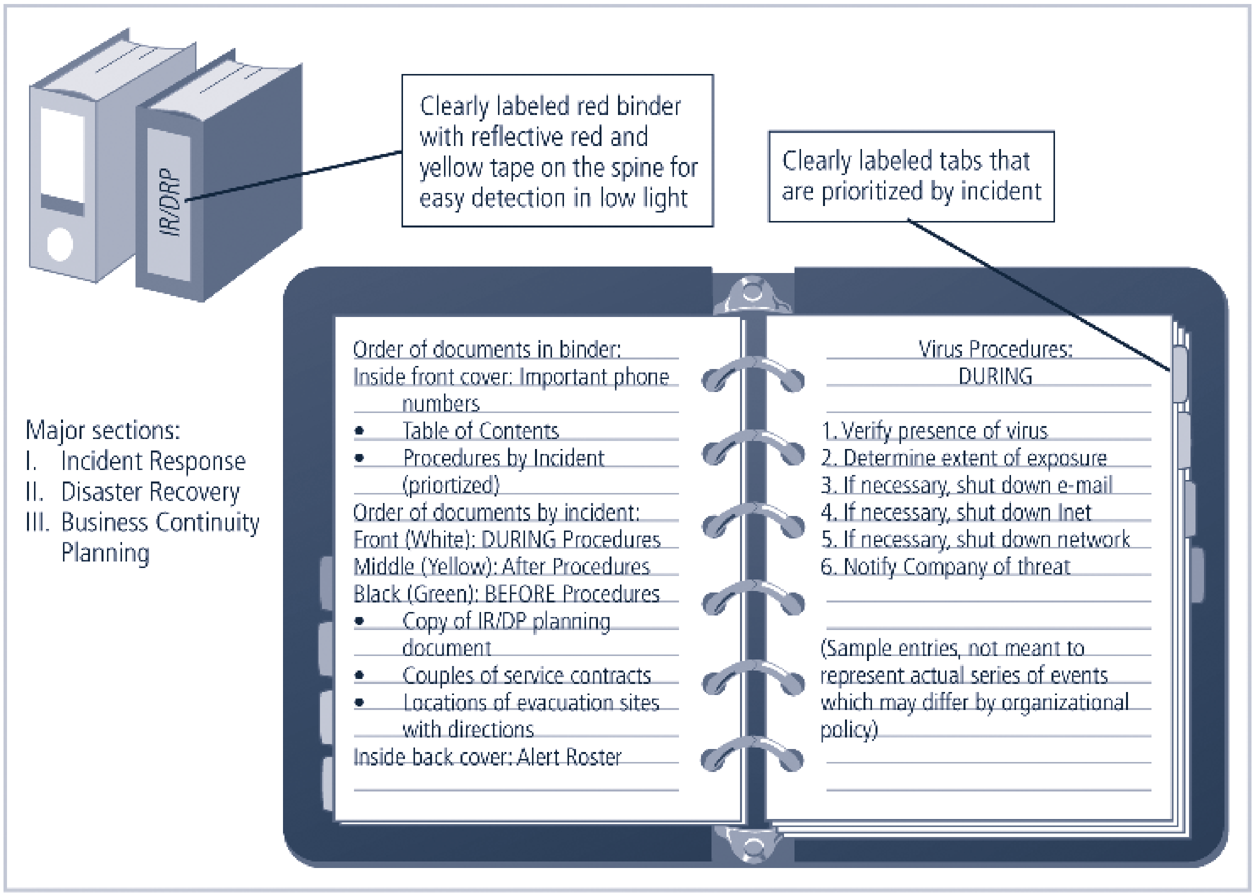
Continuity Strategies

- There are a number of strategies for planning for business continuity
- Determining factor in selecting between options is usually cost

- In general there are three exclusive options: hot sites, warm sites, and cold sites
- Three shared functions: time-share, service bureaus, and mutual agreements

Off-Site Disaster Data Storage

- To get sites up and running quickly, an organization must have the ability to port data into new site's systems
- Options for getting operations up and running include:
  - Electronic vaulting
  - Remote journaling
  - Database shadowing



Clearly labeled red binder with reflective red and yellow tape on the spine for easy detection in low light

Clearly labeled tabs that are prioritized by incident

Major sections:
I. Incident Response
II. Disaster Recovery
III. Business Continuity Planning

Order of documents in binder:
Inside front cover: Important phone numbers
- Table of Contents
- Procedures by Incident (priortized)

Order of documents by incident:
Front (White): DURING Procedures
Middle (Yellow): After Procedures
Black (Green): BEFORE Procedures
- Copy of IR/DP planning document
- Couples of service contracts
- Locations of evacuation sites with directions

Inside back cover: Alert Roster

Virus Procedures:
DURING

1. Verify presence of virus
2. Determine extent of exposure
3. If necessary, shut down e-mail
4. If necessary, shut down Inet
5. If necessary, shut down network
6. Notify Company of threat

(Sample entries, not meant to represent actual series of events which may differ by organizational policy)

FIGURE 5-24 Contingency Plan Format

Law Enforcement Involvement

- When incident at hand constitutes a violation of law, organization may determine involving law enforcement is necessary
- Questions:
  - When should organization get law enforcement involved?
  - What level of law enforcement agency should be involved (local, state, federal)?
  - What happens when law enforcement agency is involved?
- Some questions are best answered by organization's legal department

Benefits and Drawbacks of Law Enforcement Involvement

- Involving law enforcement agencies has **advantages:**
  - Agencies may be better equipped at processing evidence
  - Organization may be less effective in convicting suspects
  - Law enforcement agencies are prepared to handle any necessary warrants and subpoenas
  - Law enforcement is skilled at obtaining witness statements and other information collection
- Involving law enforcement agencies has **disadvantages:**
  - Once a law enforcement agency takes over case, organization loses complete control over chain of events
  - Organization may not hear about case for weeks or months
  - Equipment vital to the organization's business may be tagged as evidence
  - If organization detects a criminal act, it is legally obligated to involve appropriate law enforcement officials

SECURITY TECHNOLOGY

Introduction

As one of the methods of control that go into a well-planned information security program, technical controls are essential in enforcing policy for many IT functions that do not involve direct human control.

Technical control solutions, properly implemented, can improve an organization’s ability to balance the often conflicting objectives of making information more readily and widely available against increasing the information’s levels of confidentiality and integrity.

Physical Design

Selects specific technologies to support the information security blueprint

Identifies complete technical solutions based on these technologies, including deployment, operations, and maintenance elements, to improve the security of the environment

Designs physical security measures to support the technical solution

Prepares project plans for the implementation phase that follows

Firewalls

A firewall prevents specific types of information from moving between the outside world, known as the untrusted network, and the inside world, known as the trusted network.

The firewall may be a separate computer system, a software service running on an existing router or server, or a separate network containing a number of supporting devices.

Firewall Categorization Methods

Firewalls can be categorized by:

- Processing mode
- Development era
- Intended structure

Five processing modes that firewalls can be categorized by are:

- Packet filtering
- Application gateways
- Circuit gateways
- MAC layer firewalls
- Hybrids

Packet Filtering

Packet filtering firewalls examine the header information of data packets that come into a network.

The restrictions most commonly implemented are based on a combination of:

- Internet Protocol (IP) source and destination address
- Direction (inbound or outbound)
- Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source and destination port requests

Simple firewall models examine one aspect of the packet header: the destination and source address. They enforce address restrictions, rules designed to prohibit packets with certain addresses or partial addresses from passing through the device.

They accomplish this through access control lists (ACLs), which are created and modified by the firewall administrators.

There are three subsets of packet filtering firewalls:

- Static filtering
- Dynamic filtering
- Stateful inspection

Static filtering requires that the filtering rules governing how the firewall decides which packets are allowed and which are denied are developed and installed.

Dynamic filtering allows the firewall to react to an emergent event and update or create rules to deal with the event.

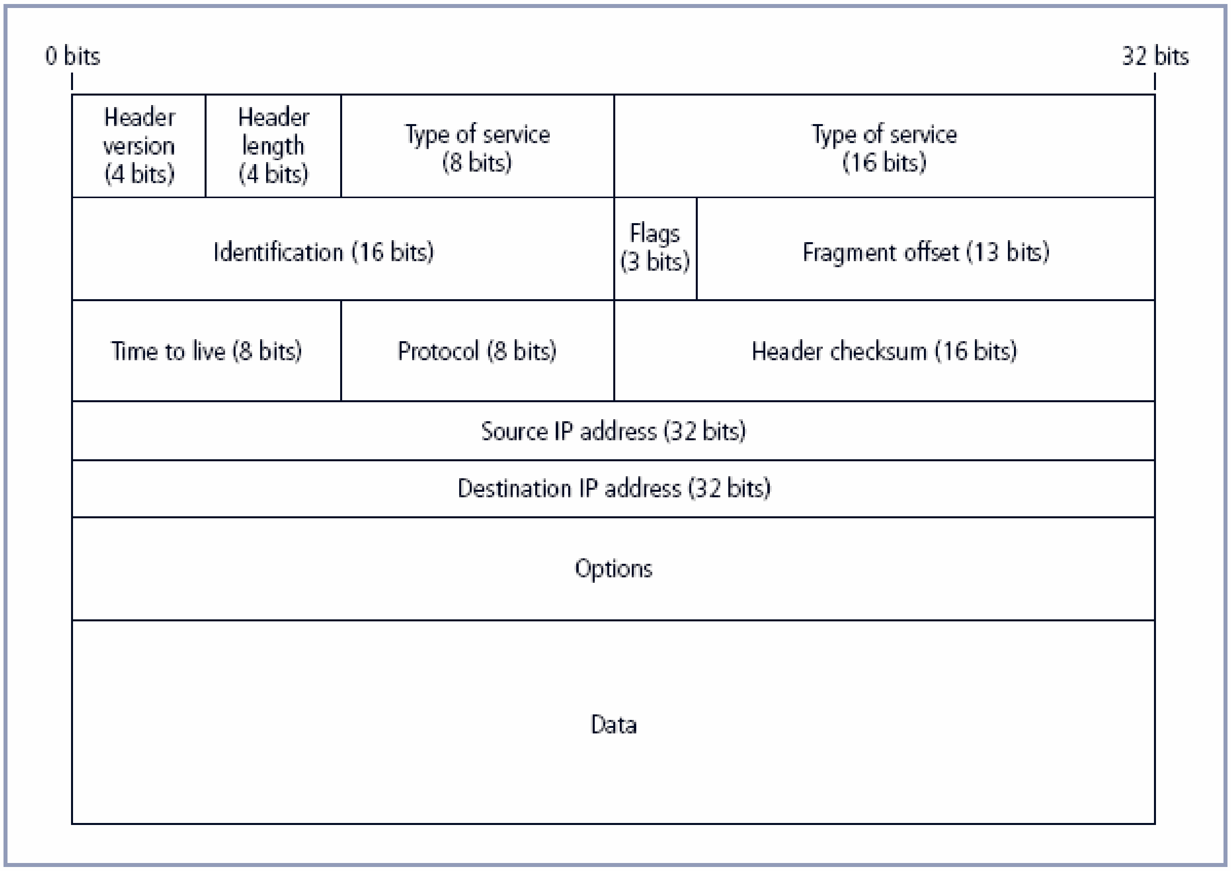
While static filtering firewalls allow entire sets of one type of packet to enter in response to authorized requests, the dynamic packet filtering firewall allows only a particular packet with a particular source, destination, and port address to enter through the firewall.

Stateful inspection firewalls, or stateful firewalls, keep track of each network connection between internal and external systems using a state table, which tracks the state and context of each packet in the conversation by recording which station sent what packet and when.

Whereas simple packet filtering firewalls only allow or deny certain packets based on their address, a stateful firewall can block incoming packets that are not responses to internal requests.

The primary disadvantage of this type of firewall is the additional processing required to manage and verify packets against the state table, which can leave the system vulnerable to a DoS or DDoS attack.

IP packet structure is shown below



<table>
<tr><td>Header version (4 bits)</td><td>Header length (4 bits)</td><td>Type of service (8 bits)</td><td colspan="2">Type of service (16 bits)</td></tr>
<tr><td colspan="3">Identification (16 bits)</td><td>Flags (3 bits)</td><td>Fragment offset (13 bits)</td></tr>
<tr><td colspan="2">Time to live (8 bits)</td><td>Protocol (8 bits)</td><td colspan="2">Header checksum (16 bits)</td></tr>
<tr><td colspan="5">Source IP address (32 bits)</td></tr>
<tr><td colspan="5">Destination IP address (32 bits)</td></tr>
<tr><td colspan="5">Options</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

FIGURE 6-1 IP Packet Structure

TCP packet and UDP datagram structure is shown below:

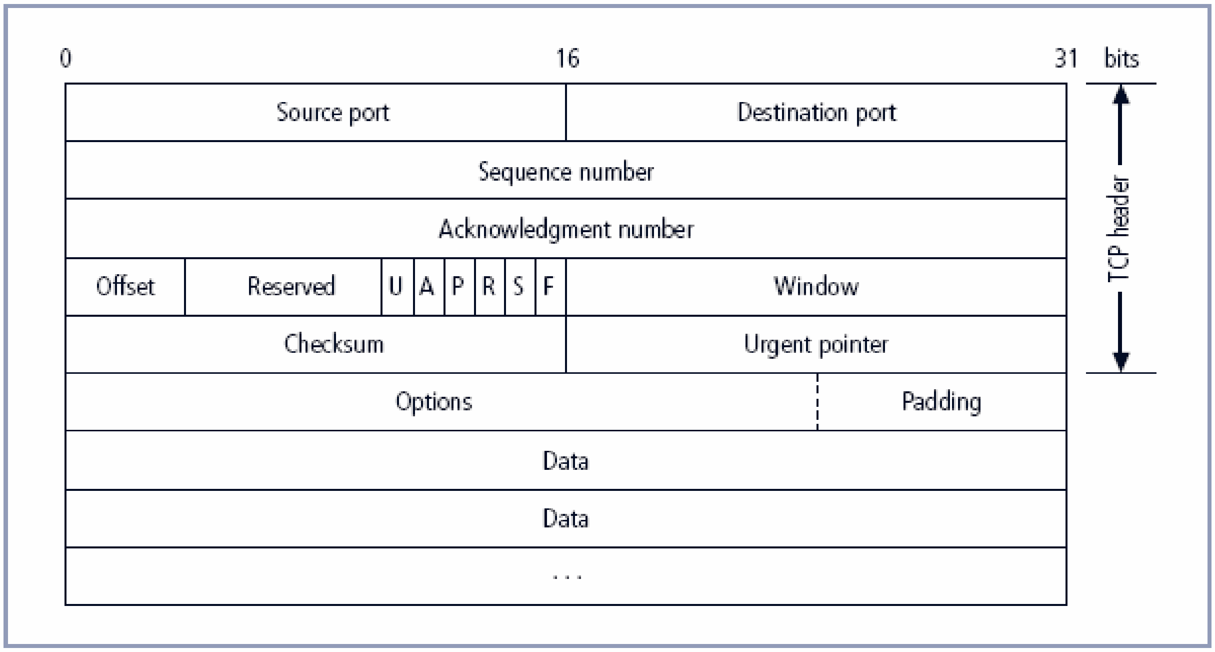


FIGURE 6-2 TCP Packet Structure

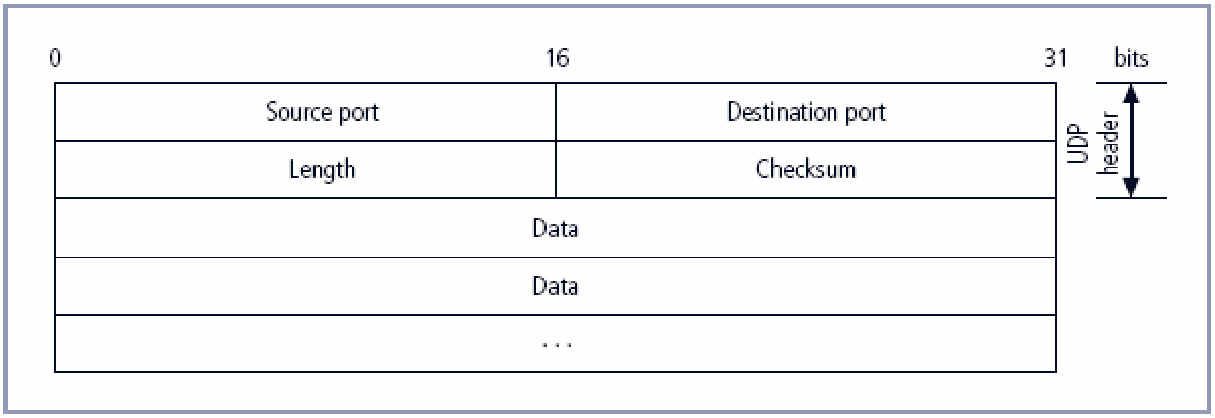


FIGURE 6-3 UDP Datagram Structure

Packet filtering router is shown below:

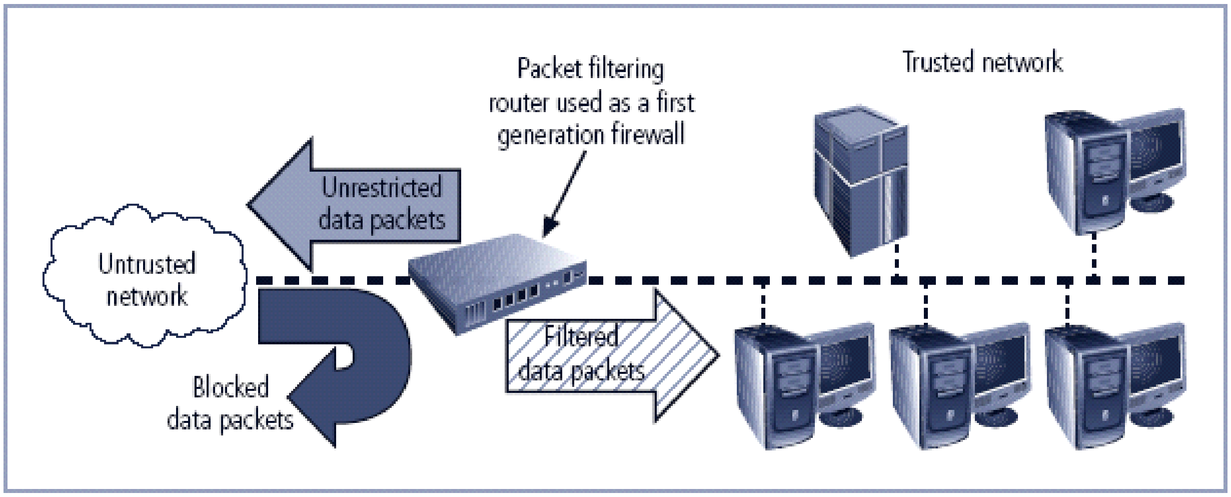


FIGURE 6-4 Packet Filtering Router

Simple firewall format

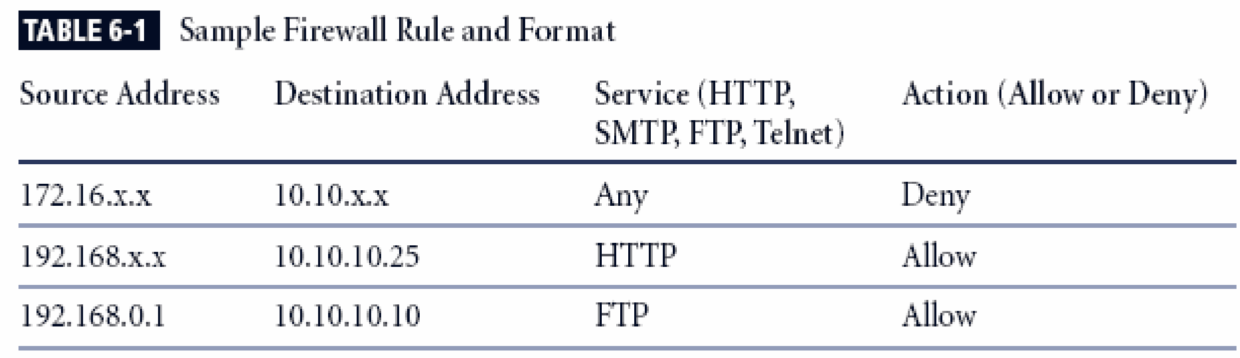


TABLE 6-1 Sample Firewall Rule and Format

Source Address	Destination Address	Service (HTTP, SMTP, FTP, Telnet)	Action (Allow or Deny)
172.16.x.x	10.10.x.x	Any	Deny
192.168.x.x	10.10.10.25	HTTP	Allow
192.168.0.1	10.10.10.10	FTP	Allow

Application Gateways

The application gateway, application-level firewall, or application firewall is frequently installed on a dedicated computer, separate from the filtering router, but it is commonly used in conjunction with a filtering router.

The application firewall is also known as a proxy server, since it runs special software that acts as a proxy for a service request.

Since the proxy server is often placed in an unsecured area of the network or is placed in the DMZ, it, rather than the Web server, is exposed to the higher levels of risk from the less trusted networks.

Additional filtering routers can be implemented behind the proxy server, limiting access to the more secure internal system and thereby further protecting internal systems.

Circuit Gateways

The circuit gateway firewall operates at the transport layer.

Connections are authorized based on addresses.

Like filtering firewalls, circuit gateway firewalls do not usually look at data traffic flowing between one network and another, but they do prevent direct connections between one network and another.

They accomplish this by creating tunnels connecting specific processes or systems on each side of the firewall, and then they allow only authorized traffic, such as a specific type of TCP connection for only authorized users, in these tunnels.

MAC Layer Firewalls

While not as well known or widely referenced as the firewall approaches above, MAC layer firewalls are designed to operate at the media access control layer of the OSI network model.

This gives these firewalls the ability to consider the specific host computer’s identity in its filtering decisions.

Using this approach, the MAC addresses of specific host computers are linked to ACL entries that identify the specific types of packets that can be sent to each host, and all other traffic is blocked.

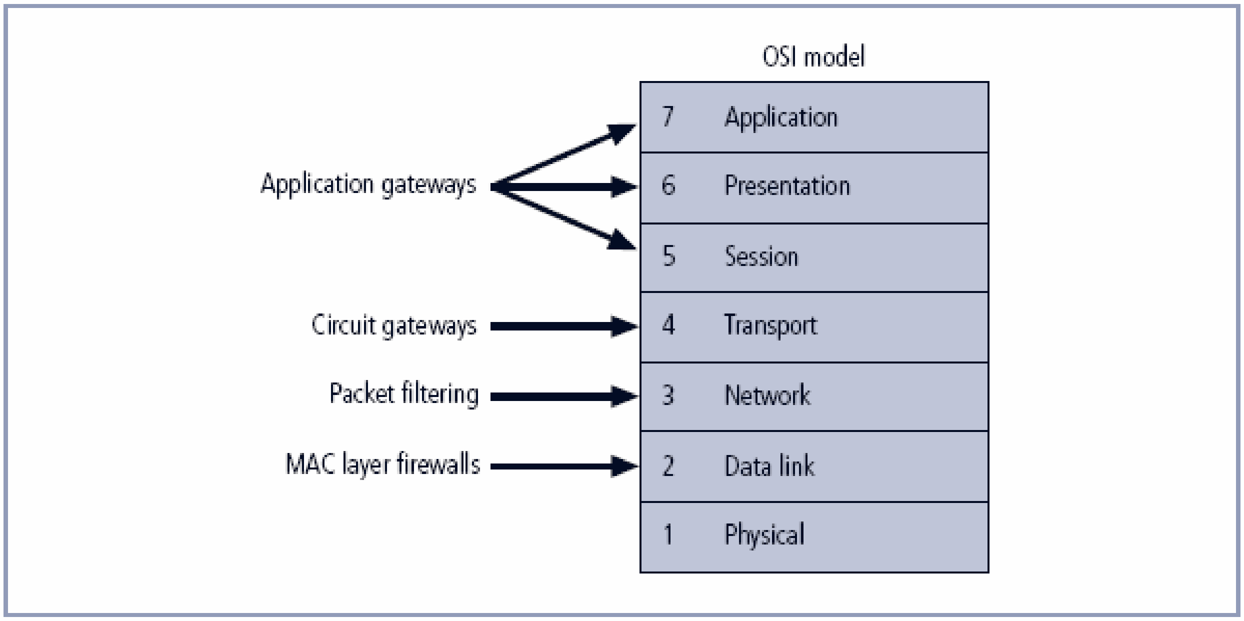


FIGURE 6-5 Firewall Types and the OSI Model

Hybrid Firewalls

Hybrid firewalls combine the elements of other types of firewalls—that is, the elements of packet filtering and proxy services or of packet filtering and circuit gateways.

Alternately, a hybrid firewall system may actually consist of two separate firewall devices; each is a separate firewall system, but they are connected so that they work in tandem.

Division of firewalls according to generations

First generation firewalls are static packet filtering firewalls—simple networking devices that filter packets according to their headers as the packets travel to and from the organization’s networks.

Second generation firewalls are application-level firewalls or proxy servers— dedicated systems that are separate from the filtering router and that provide intermediate services for requestors.

Third generation firewalls are stateful inspection firewalls and monitor network connections between internal and external systems using state tables.

Fourth generation firewalls are dynamic packet filtering firewalls and allow only a particular packet with a particular source, destination, and port address to enter.

Fifth generation firewalls are kernel proxy and are a specialized form that works under the Windows NT Executive, which is the kernel of Windows NT.

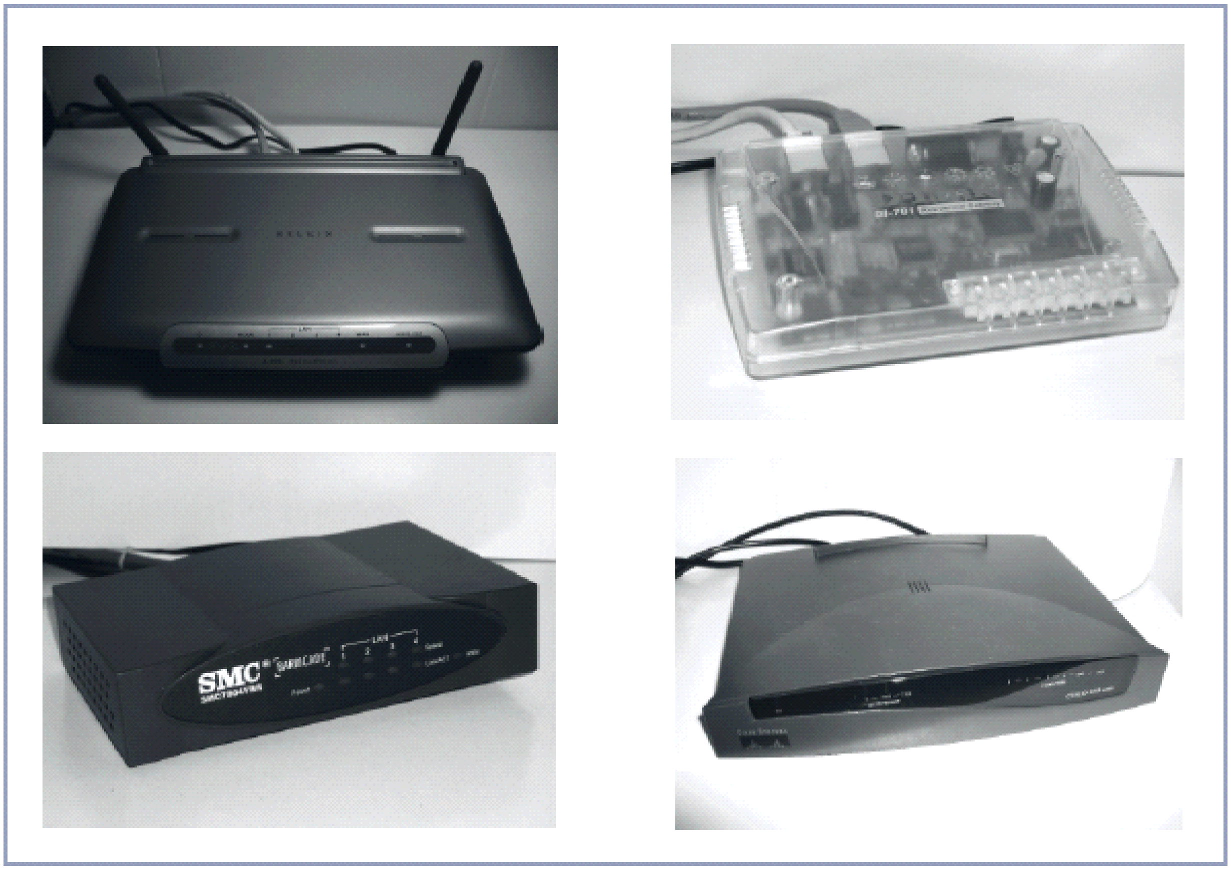


FIGURE 6-6 SOHO Firewall Devices

Software vs. Hardware: The SOHO Firewall Debate

So which type of firewall should the residential user implement?

Where would you rather defend against a hacker?

With the software option, the hacker is inside your computer, battling with a piece of software that may not have been correctly installed, configured, patched, upgraded, or designed. If the software happens to have a known vulnerability, the hacker could bypass it and then have unrestricted access to your system. With the hardware device, even if the hacker manages to crash the firewall system, your computer and information are still safely behind the now disabled connection, which is assigned a nonroutable IP address, making it virtually impossible to reach from the outside.

Firewall Architectures

Each of the firewall devices noted earlier can be configured in a number of network connection architectures.

The firewall configuration that works best for a particular organization depends on three factors: the objectives of the network, the organization’s ability to develop and implement the architectures, and the budget available for the function.

Although literally hundreds of variations exist, there are four common architectural implementations of firewalls:

- Packet filtering routers
- Screened host firewalls
- Dual-homed firewalls
- Screened subnet firewalls

Packet Filtering Routers

- Most organizations with an Internet connection have a router as the interface to the Internet at the perimeter. Many of these routers can be configured to reject packets that the organization does not allow into the network.
- The drawbacks to this type of system include a lack of auditing and strong authentication, and the complexity of the access control lists used to filter the packets can grow and degrade network performance.

Screened Host Firewalls

- This architecture combines the packet filtering router with a separate, dedicated firewall, such as an application proxy server, allowing the router to prescreen packets to minimize the network traffic and load on the internal proxy.

- The application proxy examines an application layer protocol and performs the proxy services.
- This separate host is often referred to as a bastion host or sacrificial host; it can be a rich target for external attacks and should be very thoroughly secured.

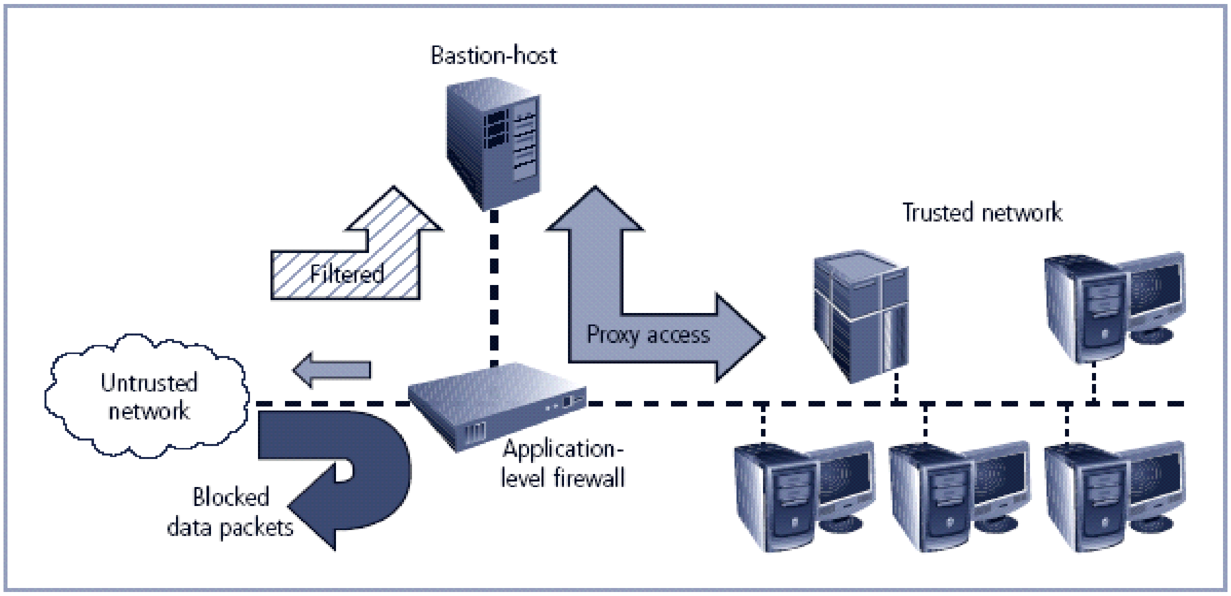


FIGURE 6-11 Screened Host Firewall

Dual-Homed Host Firewalls

With this approach, the bastion host contains two NICs: one connected to the external network and one connected to the internal network, providing an additional layer of protection by requiring all traffic to go through the firewall to move between the internal and external networks.

Implementation of this architecture often makes use of NAT mapping—assigned IP addresses to special ranges of nonroutable internal IP addresses, creating yet another barrier to intrusion from external attackers.

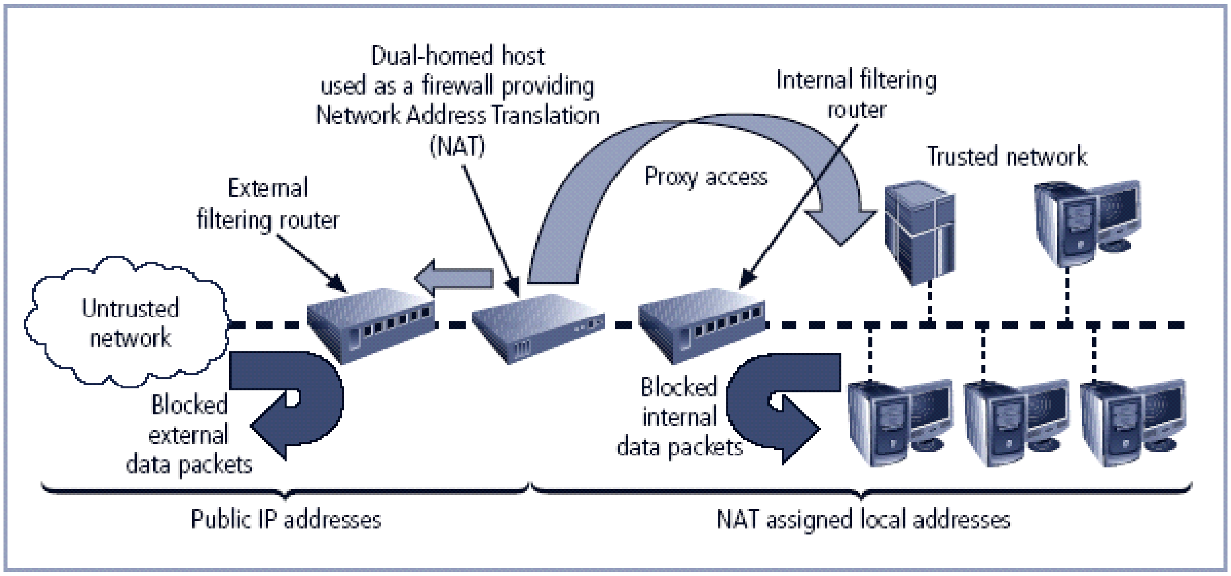

Dual-homed host used as a firewall providing Network Address Translation (NAT)
Internal filtering router
Trusted network
Proxy access
External filtering router
Untrusted network
Blocked external data packets
Blocked internal data packets
Public IP addresses
NAT assigned local addresses

FIGURE 6-12 Dual-Homed Host Firewall

Screened Subnet Firewalls (with DMZ)

The dominant architecture used today, the screened subnet firewall, provides a DMZ, which can be a dedicated port on the firewall device linking a single bastion host or it can be connected to a screened subnet.

A common arrangement finds the subnet firewall consisting of two or more internal bastion hosts behind a packet filtering router, with each host protecting the trusted network:

- Connections from the outside or untrusted network are routed through an external filtering router.
- Connections from the outside or untrusted network are routed into—and then out of—a routing firewall to the separate network segment known as the DMZ.
- Connections into the trusted internal network are allowed only from the DMZ bastion host servers.

The screened subnet is an entire network segment that performs two functions:

- It protects the DMZ systems and information from outside threats by providing a network of intermediate security.
- It protects the internal networks by limiting how external connections can gain access to internal systems.

DMZs can also create extranets—segments of the DMZ where additional authentication and authorization controls are put into place to provide services that are not available to the general public.

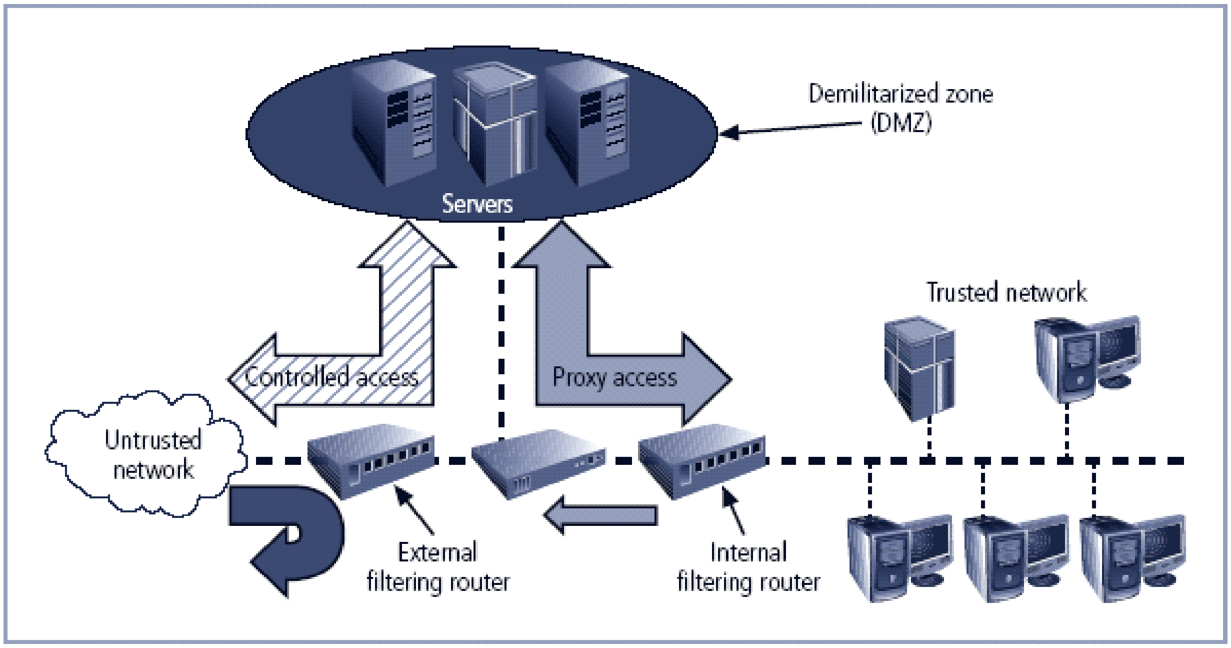


FIGURE 6-13 Screened Subnet (DMZ)

Selecting the Right Firewall

When selecting the best firewall for an organization, you should consider a number of factors. The most important of these is the extent to which the firewall design provides the desired protection:

- What type of firewall technology offers the right balance between protection and cost for the needs of the organization?
- What features are included in the base price? What features are available at extra cost? Are all cost factors known?
- How easy is it to set up and configure the firewall? How accessible are the staff technicians who can competently configure the firewall?
- Can the candidate firewall adapt to the growing network in the target organization?

The second most important issue is cost.

Configuring and Managing Firewalls

Good policy and practice dictates that each firewall device, whether a filtering router, bastion host, or other firewall implementation, must have its own set of configuration rules that regulate its actions.

The configuration of firewall policies can be complex and difficult.

Configuring firewall policies is as much an art as a science. Each configuration rule must be carefully crafted, debugged, tested, and sorted.

When configuring firewalls, keep one thing in mind: when security rules conflict with the performance of business, security often loses.

Best Practices for Firewalls

- All traffic from the trusted network is allowed out.

- The firewall device is never directly accessible from the public network.
- SMTP data is allowed to pass through the firewall but should be routed to a well-configured SMTP gateway to filter and route messaging traffic securely.
- All ICMP data should be denied.
- Telnet access to all internal servers from the public networks should be blocked.
- When Web services are offered outside the firewall, HTTP traffic should be denied from reaching your internal networks through the use of some form of proxy access or DMZ architecture.

Firewall Rules

Firewalls operate by examining a data packet and performing a comparison with some predetermined logical rules.

This logical set is most commonly referred to as firewall rules, rule base, or firewall logic.

Most firewalls use packet header information to determine whether a specific packet should be allowed to pass through or should be dropped.

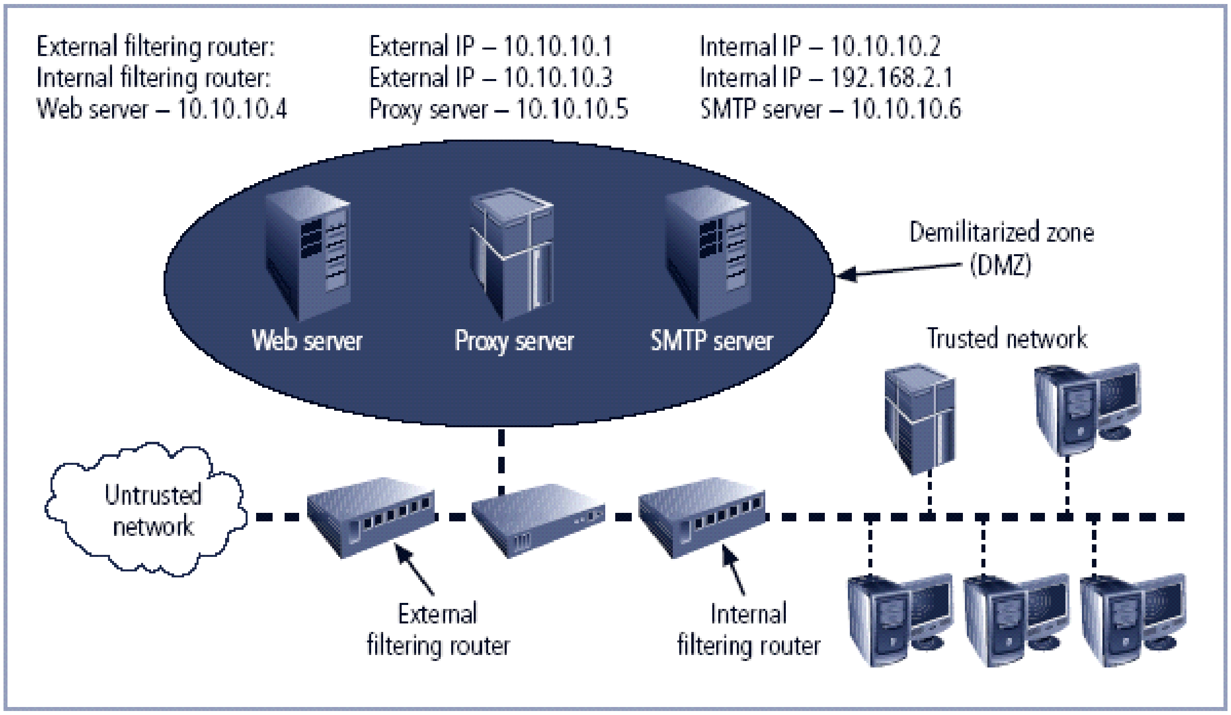


FIGURE 6-14 Example Network Configuration

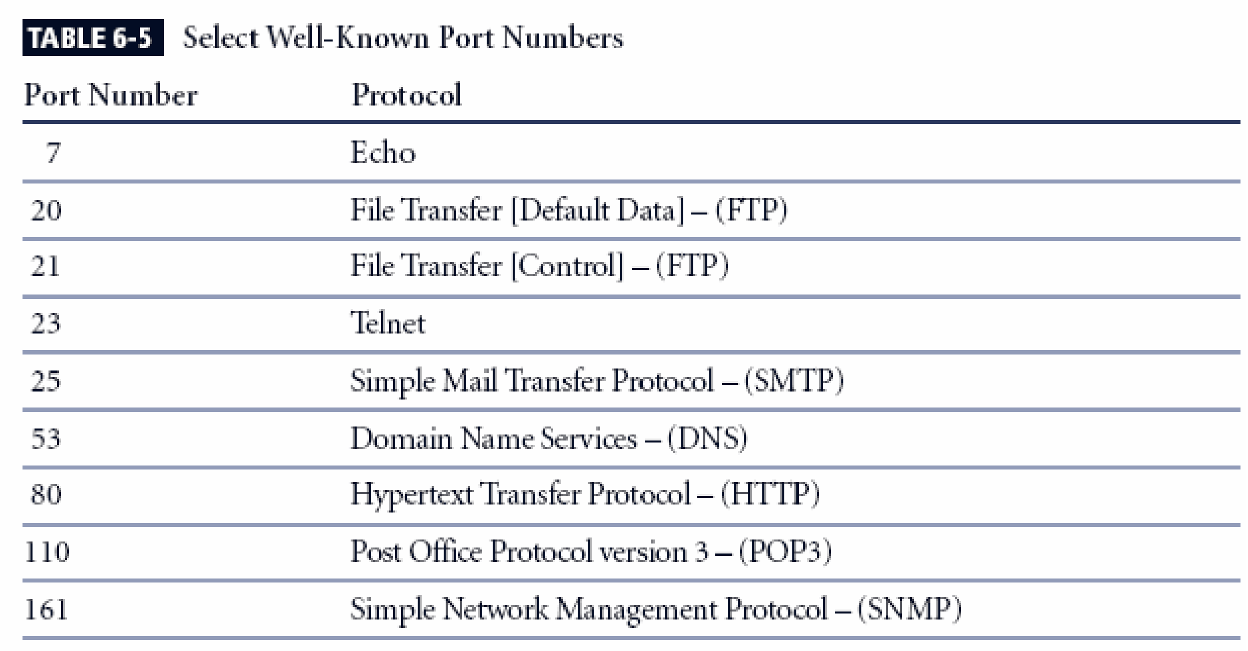


TABLE 6-5 Select Well-Known Port Numbers

Port Number	Protocol
7	Echo
20	File Transfer [Default Data] – (FTP)
21	File Transfer [Control] – (FTP)
23	Telnet
25	Simple Mail Transfer Protocol – (SMTP)
53	Domain Name Services – (DNS)
80	Hypertext Transfer Protocol – (HTTP)
110	Post Office Protocol version 3 – (POP3)
161	Simple Network Management Protocol – (SNMP)

All traffic from the trusted network is allowed out. As a general rule it is wise not to restrict outgoing traffic, unless a separate router is configured to handle this traffic. Assuming most of the potentially dangerous traffic is inbound, screening outgoing traffic is just more work for the firewalls. This level of trust is fine for most organizations. If the organization wants control over outbound traffic, it should use a separate router. The rule shown in Table 6-8 allows internal communications out.

(NOTES)Why should rule set 3 come after rule sets 1 and 2? It makes sense to allow the rules that unambiguously impact the most traffic to be earlier in the list. The more rules a firewall must process to find one that applies to the current packet, the slower the firewall will run. Therefore, most widely applicable rules should come first since the first rule that applies to any given packet will be applied.

The rule set for the Simple Mail Transport Protocol (SMTP) data is shown in Table 6-9. As shown, the packets governed by this rule are allowed to pass through the firewall, but are all routed to a well-configured SMTP gateway. It is important that e-mail traffic reach your e-mail server, and *only* your e-mail server. Some hackers try to disguise dangerous packets as e-mail traffic to fool a firewall. If such packets can reach only the e-mail server and the e-mail server has been properly configured, the rest of the network should be safe.

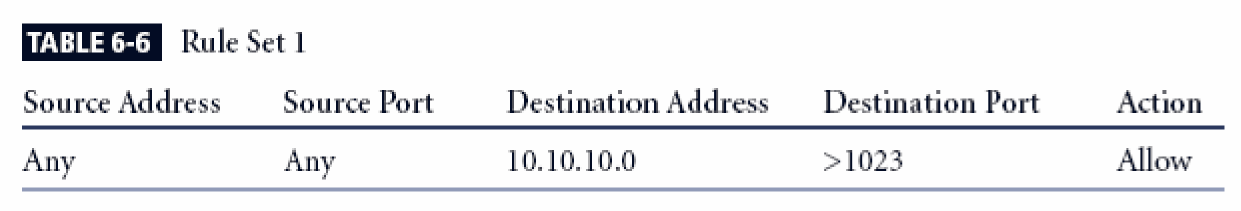


TABLE 6-6 Rule Set 1

Source Address	Source Port	Destination Address	Destination Port	Action
Any	Any	10.10.10.0	>1023	Allow

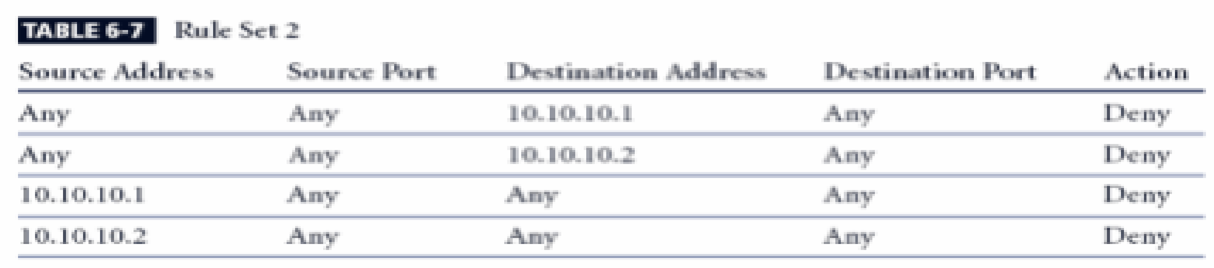


TABLE 6-7 Rule Set 2

Source Address	Source Port	Destination Address	Destination Port	Action
Any	Any	10.10.10.1	Any	Deny
Any	Any	10.10.10.2	Any	Deny
10.10.10.1	Any	Any	Any	Deny
10.10.10.2	Any	Any	Any	Deny

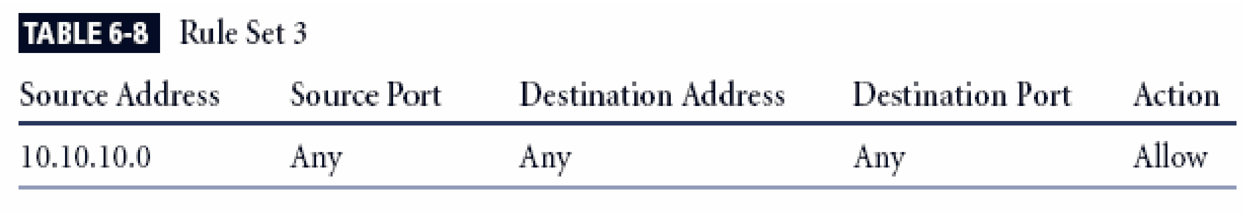


TABLE 6-8 Rule Set 3

Source Address	Source Port	Destination Address	Destination Port	Action
10.10.10.0	Any	Any	Any	Allow

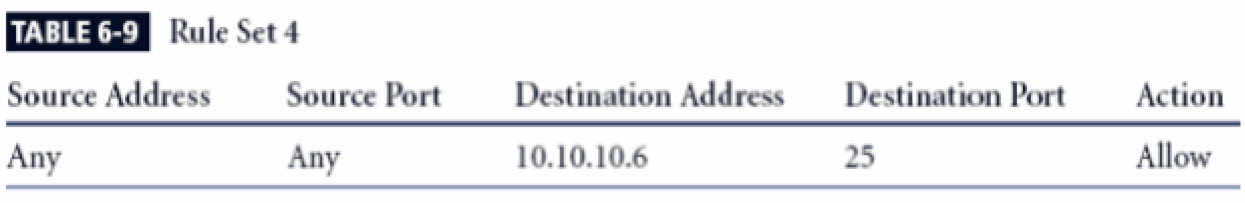


TABLE 6-9 Rule Set 4

Source Address	Source Port	Destination Address	Destination Port	Action
Any	Any	10.10.10.6	25	Allow

All traffic from the trusted network is allowed out. As a general rule it is wise not to restrict outgoing traffic, unless a separate router is configured to handle this traffic. Assuming most of the potentially dangerous traffic is inbound, screening outgoing traffic is just more work for the firewalls. This level of trust is fine for most organizations. If the organization wants control over outbound traffic, it should use a separate router. The rule shown in Table 6-8 allows internal communications out.

(NOTES)Why should rule set 3 come after rule sets 1 and 2? It makes sense to allow the rules that unambiguously impact the most traffic to be earlier in the list. The more rules a firewall must process to find one that applies to the current packet, the slower the firewall will run. Therefore, most widely applicable rules should come first since the first rule that applies to any given packet will be applied.

The rule set for the Simple Mail Transport Protocol (SMTP) data is shown in Table 6-9. As shown, the packets governed by this rule are allowed to pass through the firewall, but are all routed to a well-configured SMTP gateway. It is important that e-mail traffic reach your e-mail server, and *only* your e-mail server. Some hackers try to disguise dangerous packets as e-mail traffic to fool a firewall. If such packets can reach only the e-mail server and the e-mail server has been properly configured, the rest of the network should be safe.

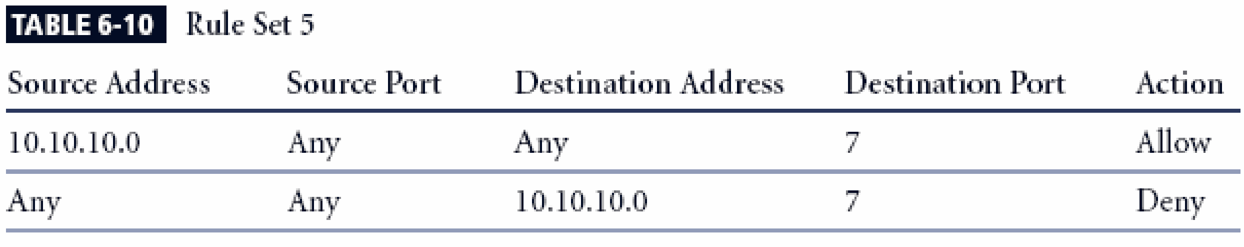


TABLE 6-10 Rule Set 5

Source Address	Source Port	Destination Address	Destination Port	Action
10.10.10.0	Any	Any	7	Allow
Any	Any	10.10.10.0	7	Deny

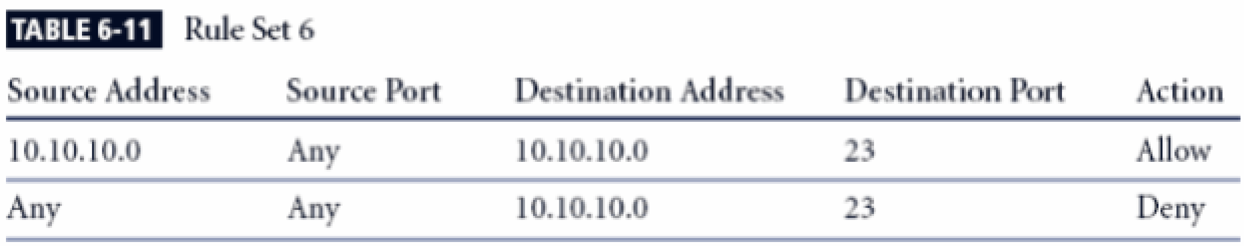


TABLE 6-11 Rule Set 6

Source Address	Source Port	Destination Address	Destination Port	Action
10.10.10.0	Any	10.10.10.0	23	Allow
Any	Any	10.10.10.0	23	Deny

All Internet Control Message Protocol (ICMP) data should be denied. Pings, formally known as ICMP Echo requests, are used by internal systems administrators to ensure that clients and servers can reach and communicate. There is virtually no legitimate use for ICMP outside the network, except to test the perimeter routers. ICMP uses port 7 to request a response to a query (e.g., “Are you there?”) and can be the first indicator of a malicious attack. It’s best to make all directly connected networking devices “black holes” to external probes. Traceroute uses a variation on the ICMP Echo requests, so restricting this one port provides protection against two types of probes.

Allowing internal users to use ICMP requires configuring two rules, as shown in Table 6-10.

(NOTES)

The first of these two rules allows internal administrators (and users) to use Ping. Note that this rule is unnecessary if internal permissions rules like those in rule set 2 are used. The second rule in Table 6-10 does not allow anyone else to use Ping. Remember that rules are processed in order. If an internal user needs to Ping an internal or external address, the firewall allows the packet and stops processing the rules. If the request does not come from an internal source, then it bypasses the first rule and moves to the second.

Telnet (terminal emulation) access to all internal servers from the public networks should be blocked. Though not used much in Windows environments, Telnet is still useful to systems administrators on Unix/Linux systems. But the presence of external requests for Telnet services can indicate a potential attack. Allowing internal use of Telnet requires the same type of initial permission rule you use with Ping. See Table 6-11. Note that this rule is unnecessary if internal permissions rules like those in rule set 2 are used.

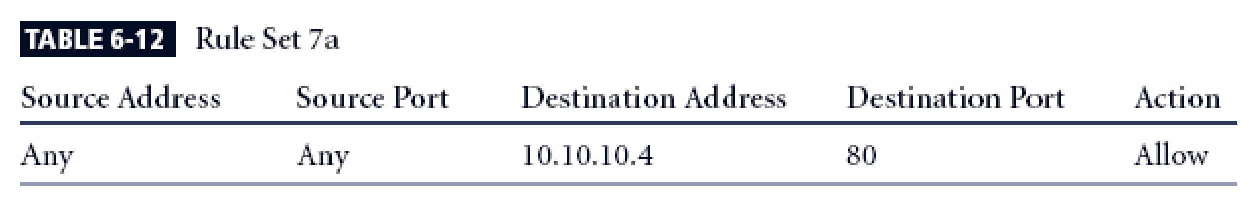


TABLE 6-12 Rule Set 7a

Source Address	Source Port	Destination Address	Destination Port	Action
Any	Any	10.10.10.4	80	Allow

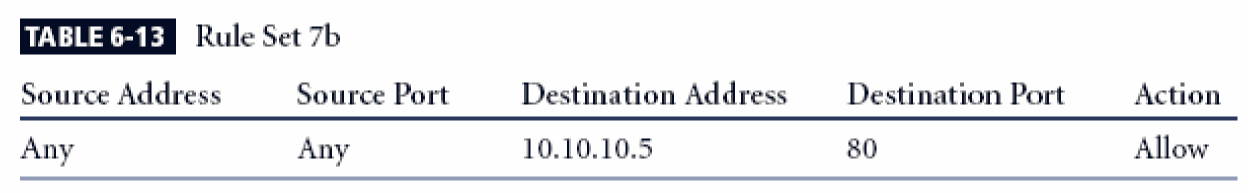


TABLE 6-13 Rule Set 7b

Source Address	Source Port	Destination Address	Destination Port	Action
Any	Any	10.10.10.5	80	Allow

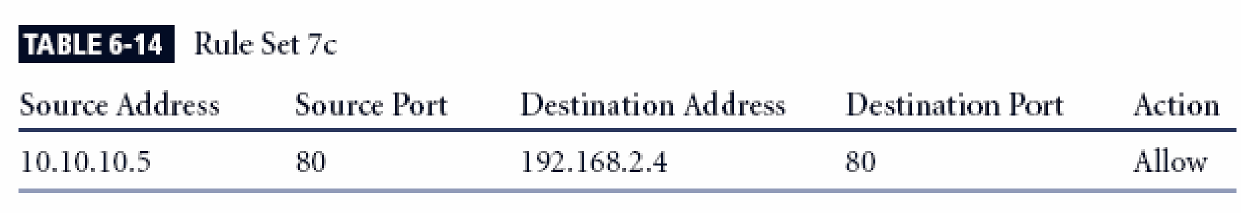


TABLE 6-14 Rule Set 7c

Source Address	Source Port	Destination Address	Destination Port	Action
10.10.10.5	80	192.168.2.4	80	Allow

When Web services are offered outside the firewall, HTTP traffic should be denied from reaching the internal networks through the use of some form of proxy access or DMZ architecture. With a Web server in the DMZ, you simply allow HTTP to access the Web server, and use rule set 8, the Cleanup rule, (which will be described shortly) to prevent any other access. In order to keep the Web server inside the internal network, direct all HTTP requests to the proxy server and configure the internal filtering router/firewall only to allow the proxy server to access the internal Web server.

This rule accomplishes two things: it allows HTTP traffic to reach the Web server and it prevents non-HTTP traffic from reaching the Web server. It does the latter through the Cleanup rule (Rule 8). If someone tries to access the Web server with non-HTTP traffic (other than port 80), then the firewall skips this rule and goes to the next. Proxy server rules allow an organization to restrict all access to a device. The external firewall would be configured as shown.

The effective use of a proxy server of course requires the DNS entries to be configured as if the proxy server was the Web server. The proxy server would then be configured to repackage any HTTP request packets into a new packet and retransmit to the Web server inside the firewall. Allowing for the retransmission of the repackaged request requires the rule shown to enable the proxy server at 10.10.10.5 to send to the internal router, presuming the IP address for the internal Web server is 192.168.2.4.

The restriction on the source address then prevents anyone else from accessing the Web server from outside the internal filtering router/firewall.

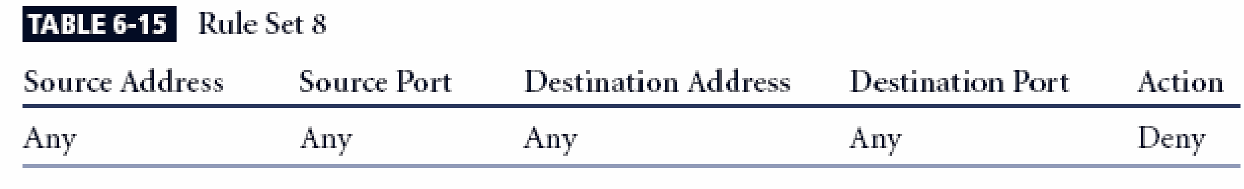


TABLE 6-15 Rule Set 8

Source Address	Source Port	Destination Address	Destination Port	Action
Any	Any	Any	Any	Deny

The Cleanup Rule

As a general practice in firewall rule construction, if a request for a service is not explicitly allowed by policy, that request should be denied by a rule

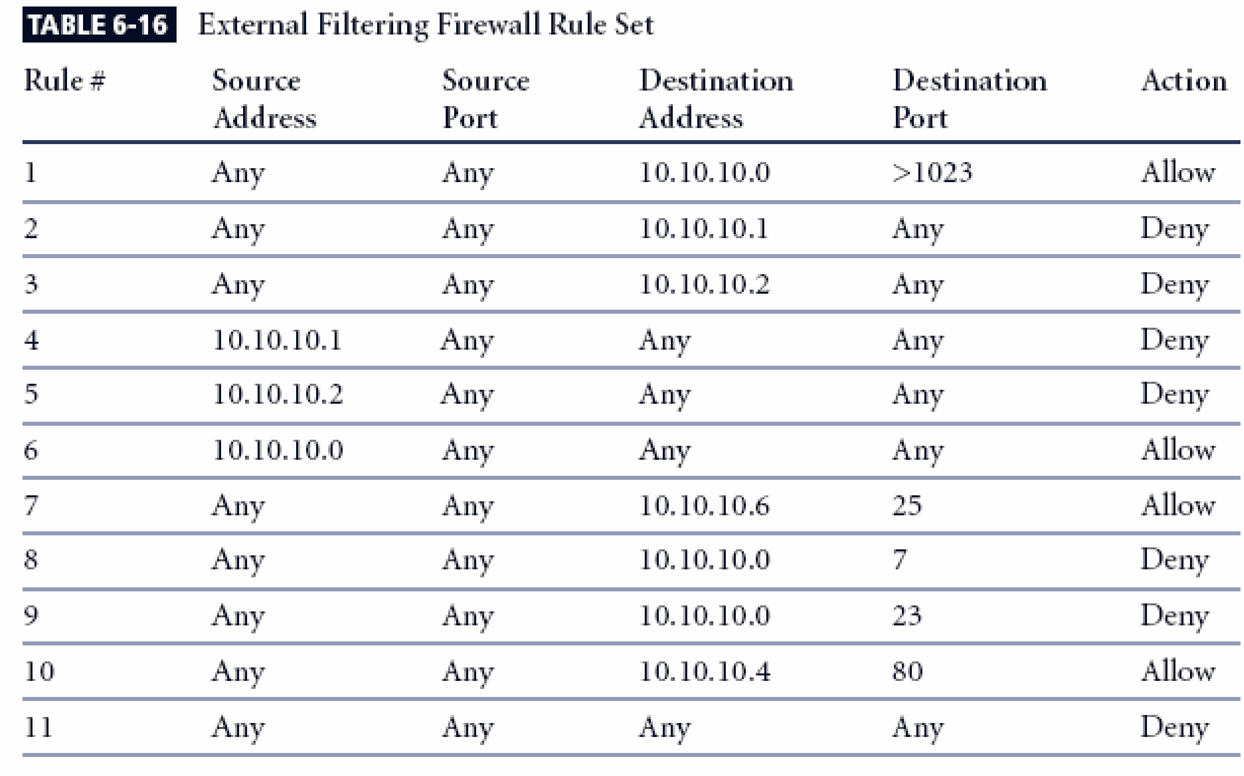


TABLE 6-16 External Filtering Firewall Rule Set

Rule #	Source Address	Source Port	Destination Address	Destination Port	Action
1	Any	Any	10.10.10.0	>1023	Allow
2	Any	Any	10.10.10.1	Any	Deny
3	Any	Any	10.10.10.2	Any	Deny
4	10.10.10.1	Any	Any	Any	Deny
5	10.10.10.2	Any	Any	Any	Deny
6	10.10.10.0	Any	Any	Any	Allow
7	Any	Any	10.10.10.6	25	Allow
8	Any	Any	10.10.10.0	7	Deny
9	Any	Any	10.10.10.0	23	Deny
10	Any	Any	10.10.10.4	80	Allow
11	Any	Any	Any	Any	Deny

Note that the rule allowing responses to internal communications comes first (appearing in Table 6-16 as Rule #1), followed by the four rules prohibiting direct communications to or from the firewall (Rules #2 through 5 in Table 6-16). After this comes the rule stating that all outgoing internal communications are allowed, followed by the rules governing access to the SMTP server and denial of Ping, Telnet access, and access to the HTTP server. If heavy traffic to the HTTP server is expected, move the HTTP server rule closer to the top (for example, into the position of Rule #2), which would expedite rule processing for external communications. The final rule in Table 6-16 denies any other types of communications.

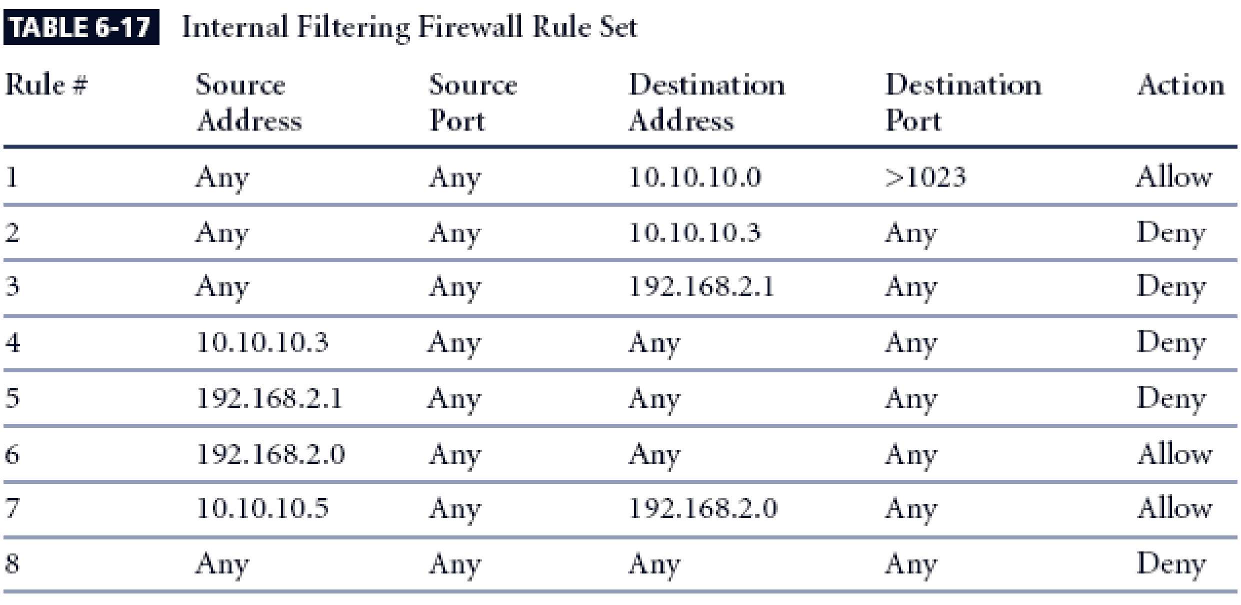


TABLE 6-17 Internal Filtering Firewall Rule Set

Rule #	Source Address	Source Port	Destination Address	Destination Port	Action
1	Any	Any	10.10.10.0	>1023	Allow
2	Any	Any	10.10.10.3	Any	Deny
3	Any	Any	192.168.2.1	Any	Deny
4	10.10.10.3	Any	Any	Any	Deny
5	192.168.2.1	Any	Any	Any	Deny
6	192.168.2.0	Any	Any	Any	Allow
7	10.10.10.5	Any	192.168.2.0	Any	Allow
8	Any	Any	Any	Any	Deny

Note the similarities and differences in the two rule sets. The internal filtering router/firewall rule set, shown in Table 6-17, has to both protect against traffic and allow traffic from the internal network (192.168.2.0). Most of the rules in Table 6-17 are similar to those in Table 6-16: allowing responses to internal communications (Rule #1); denying communications to/from the firewall itself (Rules #2 through 5); and allowing all outbound internal traffic (Rule #6). Note that there is no permissible traffic from the DMZ systems, except as in Rule #1. Why isn't there a comparable rule for the 192.168.2.1 subnet? Because this is an unrouteable network, external communications are handled by the NAT server, which maps internal (192.168.2.0) addresses to external (10.10.10.0) addresses. This prevents a hacker from compromising one of the internal boxes and accessing the internal network with it. The exception is the proxy server (Rule #7 in Table 6-17), which should be very carefully configured. If the organization does not need the proxy server, as in cases where all externally accessible services are provided from machines in the DMZ, then Rule #7 is not needed.

Note that there are no Ping and Telnet rules in Table 6-17. This is because the external firewall filters these external requests out. The last rule, Rule #8, provides cleanup.

Content Filters

A content filter is a software filter—technically not a firewall—that allows administrators to restrict access to content from within a network.

It is essentially a set of scripts or programs that restricts user access to certain networking protocols and Internet locations or restricts users from receiving general types or specific examples of Internet content. Some refer to content filters as reverse firewalls, as their primary focus is to restrict internal access to external material.

In most common implementation models, the content filter has two components: rating and filtering.

The rating is like a set of firewall rules for Web sites and is common in residential content filters.

The filtering is a method used to restrict specific access requests to the identified resources, which may be Web sites, servers, or whatever resources the content filter administrator configures.

The most common content filters restrict users from accessing Web sites with obvious non-business related material, such as pornography, or deny incoming spam e-mail.

Protecting Remote Connections

Installing Internetwork connections requires using leased lines or other data channels provided by common carriers, and therefore these connections are usually permanent and secured under the requirements of a formal service agreement.

In the past, organizations provided remote connections exclusively through dial-up services like Remote Authentication Service (RAS).

Since the Internet has become more widespread in recent years, other options such as virtual private networks (VPNs) have become more popular.

Dial-Up

It is a widely held view that these unsecured, dial-up connection points represent a substantial exposure to attack.

An attacker who suspects that an organization has dial-up lines can use a device called a war dialer to locate the connection points.

A war dialer is an automatic phone-dialing program that dials every number in a configured range and checks to see if a person, answering machine, or modem picks up.

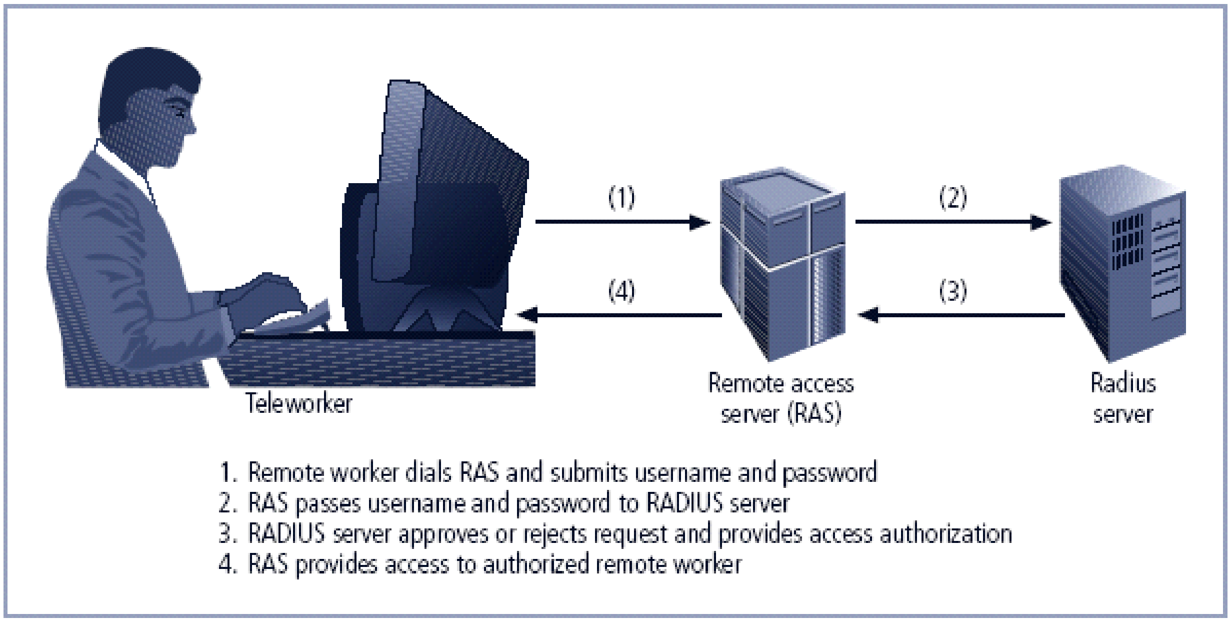
Some technologies, such as RADIUS systems, TACACS, and CHAP password systems, have improved the authentication process.

RADIUS and TACACS

RADIUS and TACACS are systems that authenticate the credentials of users who are trying to access an organization’s network via a dial-up connection.

The Remote Authentication Dial-In User Service system places the responsibility for authenticating each user in the central RADIUS server. When a remote access server receives a request for a network connection from a dial-up client, it passes the request along with the user’s credentials to the RADIUS server, which then validates the credentials and passes the resulting decision (accept or deny) back to the accepting RAS.

Similar in function to the RADIUS system is the Terminal Access Controller Access Control System (TACACS). TACACS, like RADIUS, is a centralized database and validates the user's credentials at this TACACS server.



1. Remote worker dials RAS and submits username and password
2. RAS passes username and password to RADIUS server
3. RADIUS server approves or rejects request and provides access authorization
4. RAS provides access to authorized remote worker

FIGURE 6-15 RADIUS Configuration

Securing Authentication with Kerberos

Kerberos uses symmetric key encryption to validate an individual user to various network resources. Kerberos keeps a database containing the private keys of clients and servers—in the case of a client, this key is simply the client's encrypted password.

The Kerberos system knows these private keys and can authenticate one network node (client or server) to another.

Kerberos consists of three interacting services, all of which use a database library:

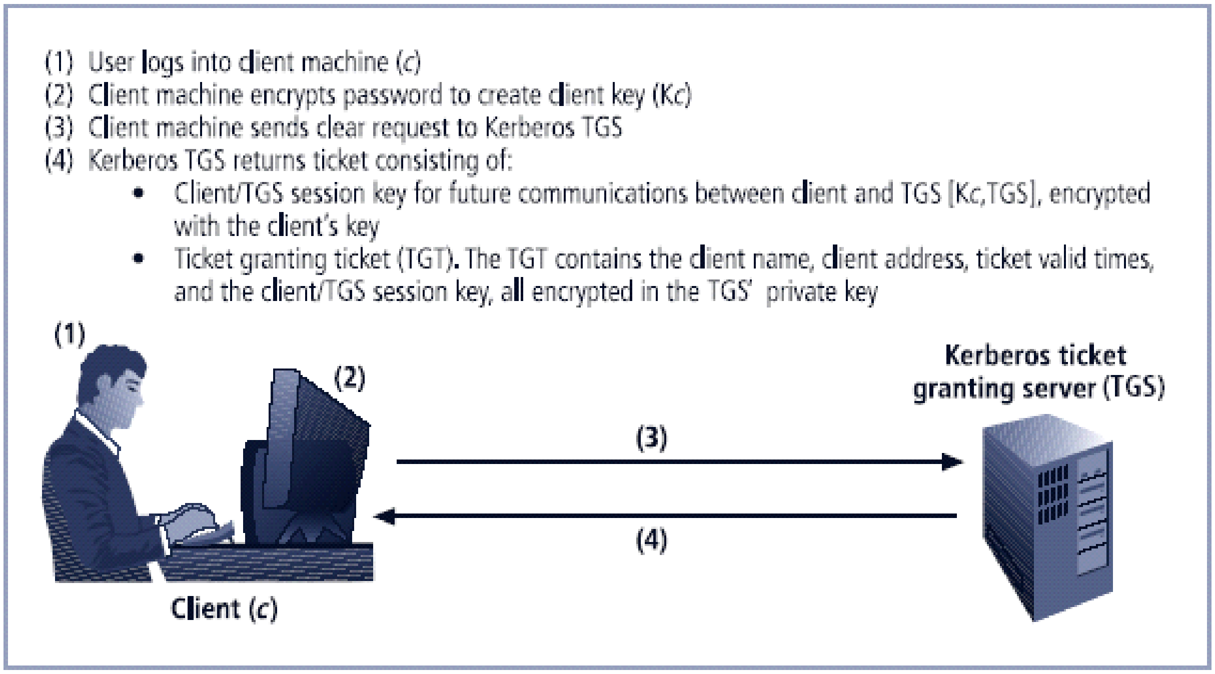
1. Authentication server (AS), which is a Kerberos server that authenticates clients and servers.

2. Key Distribution Center (KDC), which generates and issues session keys.

3. Kerberos ticket granting service (TGS), which provides tickets to clients who request services.

In Kerberos, a ticket is an identification card for a particular client that verifies to the server that the client is requesting services and that the client is a valid member of the Kerberos system and therefore authorized to receive services.

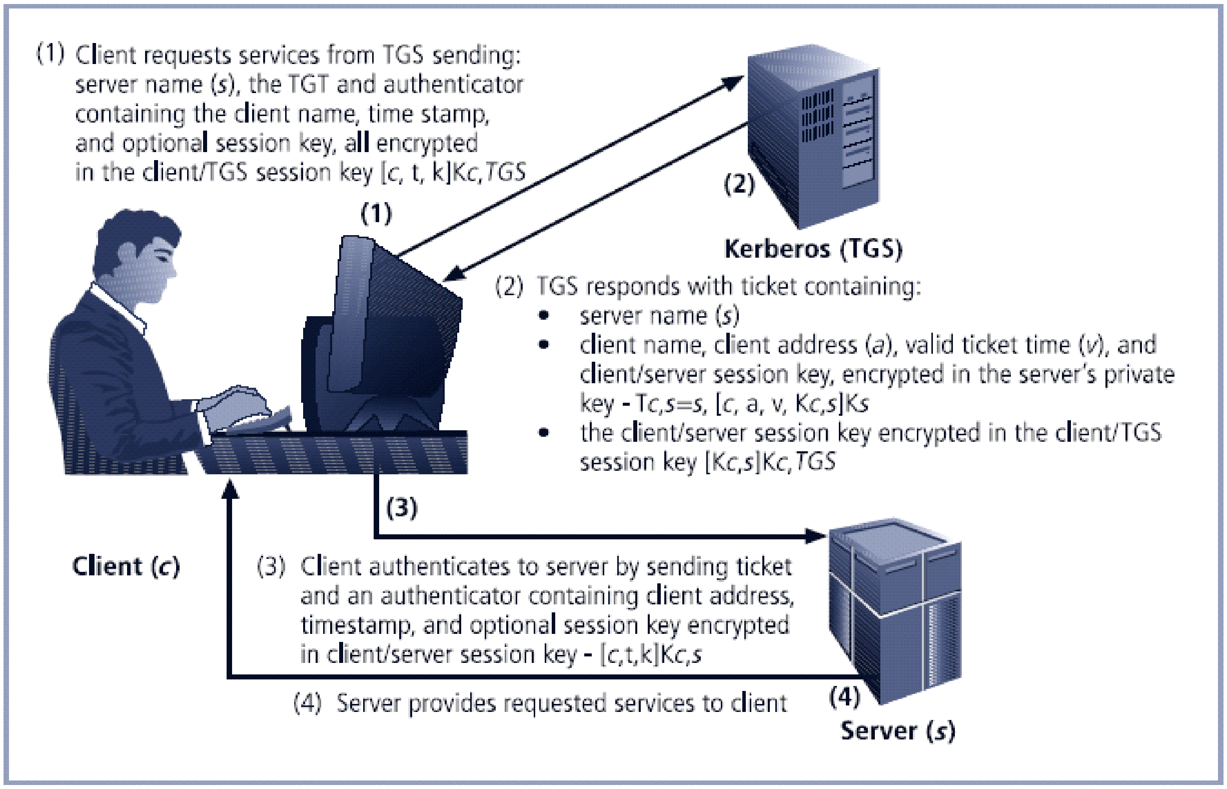
The ticket consists of the client’s name and network address, a ticket validation starting and ending time, and the session key, all encrypted in the private key of the server from which the client is requesting services.



(1) User logs into client machine (*c*)
(2) Client machine encrypts password to create client key (K*c*)
(3) Client machine sends clear request to Kerberos TGS
(4) Kerberos TGS returns ticket consisting of:

- Client/TGS session key for future communications between client and TGS [Kc,TGS], encrypted with the client’s key
- Ticket granting ticket (TGT). The TGT contains the client name, client address, ticket valid times, and the client/TGS session key, all encrypted in the TGS’ private key

FIGURE 6-16 Kerberos Login



(1) Client requests services from TGS sending: server name (*s*), the TGT and authenticator containing the client name, time stamp, and optional session key, all encrypted in the client/TGS session key [*c*, t, k]K*c*,*TGS*

(2) TGS responds with ticket containing:

- server name (*s*)
- client name, client address (*a*), valid ticket time (*v*), and client/server session key, encrypted in the server's private key - T*c*,*s*=*s*, [*c*, a, v, K*c*,*s*]K*s*
- the client/server session key encrypted in the client/TGS session key [K*c*,*s*]K*c*,*TGS*

(3) Client authenticates to server by sending ticket and an authenticator containing client address, timestamp, and optional session key encrypted in client/server session key - [*c*,t,k]K*c*,*s*

(4) Server provides requested services to client

FIGURE 6-17 Kerberos Request for Services

SESAME

The Secure European System for Applications in a Multivendor Environment (SESAME) is similar to Kerberos in that the user is first authenticated to an authentication server and receives a token.

The token is then presented to a privilege attribute server (instead of a ticket granting service as in Kerberos) as proof of identity to gain a privilege attribute certificate (PAC).

SESAME also builds on the Kerberos model by adding additional and more sophisticated access control features, more scalable encryption systems, as well as improved manageability, auditing features, and the delegation of responsibility for allowing access.

Virtual Private Networks (VPNs)

A VPN is a private and secure network connection between systems that uses the data communication capability of an unsecured and public network.

VPNs are commonly used to extend securely an organization’s internal network connections to remote locations beyond the trusted network.

The VPNC defines three VPN technologies:

- A trusted VPN, or VPN, uses leased circuits from a service provider and conducts packet switching over these leased circuits.
- Secure VPNs use security protocols and encrypt traffic transmitted across unsecured public networks like the Internet.
- A hybrid VPN combines the two, providing encrypted transmissions (as in secure VPN) over some or all of a trusted VPN network.

A VPN that proposes to offer a secure and reliable capability while relying on public networks must address:

- *Encapsulation* of incoming and outgoing data, wherein the native protocol of the client is embedded within the frames of a protocol that can be routed over the public network, as well as be usable by the server network environment.
- *Encryption* of incoming and outgoing data to keep the data contents private while in transit over the public network but usable by the client and server computers and/or the local networks on both ends of the VPN connection.
- *Authentication* of the remote computer and, perhaps, the remote user as well. Authentication and the subsequent authorization of the user to perform specific actions are

predicated on accurate and reliable identification of the remote system and/or user.

A VPN is a private and secure network connection between systems that uses the data communication capability of an unsecured and public network.

VPNs are commonly used to extend securely an organization’s internal network connections to remote locations beyond the trusted network.

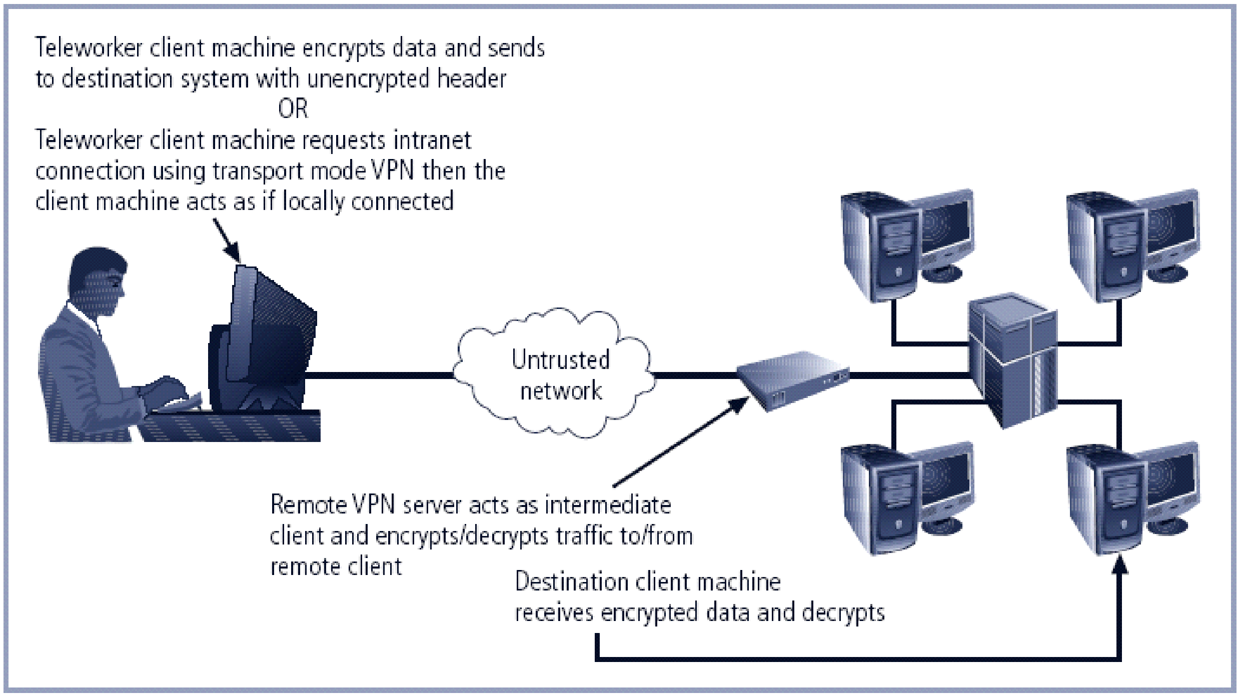
The VPNC defines three VPN technologies:

- A trusted VPN, or VPN, uses leased circuits from a service provider and conducts packet switching over these leased circuits.
- Secure VPNs use security protocols and encrypt traffic transmitted across unsecured public networks like the Internet.
- A hybrid VPN combines the two, providing encrypted transmissions (as in secure VPN) over some or all of a trusted VPN network.

Transport Mode

- In transport mode, the data within an IP packet is encrypted, but the header information is not. This allows the user to establish a secure link directly with the remote host, encrypting only the data contents of the packet.
- There are two popular uses for transport mode VPNs.
- The end-to-end transport of encrypted data. In this model, two end users can communicate directly, encrypting and decrypting their communications as needed. Each machine acts as the end node VPN server and client.

- A remote access worker or teleworker connects to an office network over the Internet by connecting to a VPN server on the perimeter.



Teleworker client machine encrypts data and sends to destination system with unencrypted header
OR
Teleworker client machine requests intranet connection using transport mode VPN then the client machine acts as if locally connected

Remote VPN server acts as intermediate client and encrypts/decrypts traffic to/from remote client

Destination client machine receives encrypted data and decrypts

FIGURE 6-18 Transport Mode VPN

Tunnel Mode

In tunnel mode, the organization establishes two perimeter tunnel servers. These servers serve as the encryption points, encrypting all traffic that will traverse an unsecured network.

In tunnel mode, the entire client packet is encrypted and added as the data portion of a packet addressed from one tunneling server and to another. The receiving server decrypts the packet and sends it to the final address.

The primary benefit to this model is that an intercepted packet reveals nothing about the true destination system.

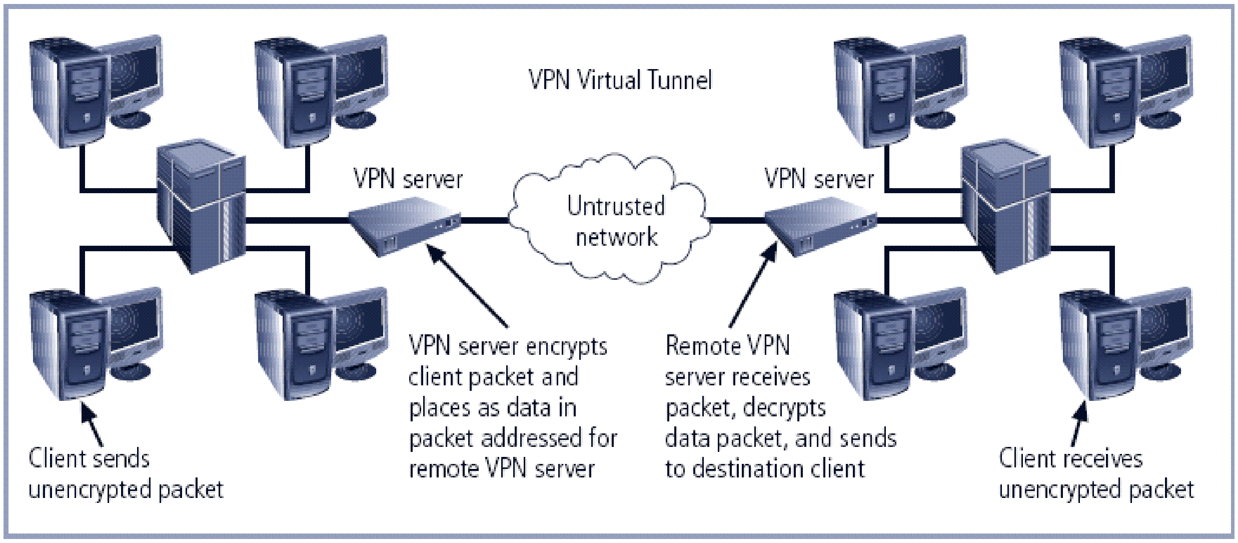

VPN Virtual Tunnel
VPN server
Untrusted network
VPN server
VPN server encrypts client packet and places as data in packet addressed for remote VPN server
Remote VPN server receives packet, decrypts data packet, and sends to destination client
Client sends unencrypted packet
Client receives unencrypted packet

FIGURE 6-19 Tunnel Mode VPN