

**Introduction**—The specialised nature of information systems (IS) auditing and the skills necessary to perform such audits require standards that apply specifically to IS auditing. One of the goals of the Information Systems Audit and Control Association® (ISACA®) is to advance globally applicable standards to meet this need. The development and dissemination of the IS Auditing Standards are a cornerstone of the ISACA professional contribution to the audit community.

**Objectives**—The objectives of the ISACA IS Auditing Standards are to inform:

- IS auditors of the minimum level of acceptable performance required to meet the professional responsibilities set out in the *ISACA Code of Professional Ethics* for IS auditors
  - Management and other interested parties of the profession's expectations concerning the work of practitioners
- The objective of the IS Auditing Procedures is to provide further information on how to comply with the IS Auditing Standards.

**Scope and Authority of IS Auditing Standards**—The framework for the IS Auditing Standards provides multiple levels of guidance:

- **Standards** define mandatory requirements for IS auditing and reporting.
- **Guidelines** provide guidance in applying IS Auditing Standards. The IS auditor should consider them in determining how to achieve implementation of the standards, use professional judgment in their application and be prepared to justify any departure.
- **Procedures** provide examples of procedures an IS auditor might follow in an audit engagement. Procedures should not be considered inclusive of any proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtain the same results. In determining the appropriateness of any specific procedure, group of procedures or test, the IS auditor should apply their own professional judgment to the specific circumstances presented by the particular information systems or technology environment. The procedure documents provide information on how to meet the standards when performing IS auditing work, but do not set requirements.

The words audit and review are used interchangeably. A full glossary of terms can be found on the ISACA web site at [www.isaca.org/glossary.htm](http://www.isaca.org/glossary.htm).

Holders of the Certified Information Systems Auditor™ (CISA®) designation are to comply with the IS Auditing Standards adopted by ISACA. Failure to comply with these standards may result in an investigation into the CISA holder's conduct by the ISACA Board of Directors or appropriate ISACA committee and, ultimately, in disciplinary action.

#### Development of Standards, Guidelines and Procedures

The ISACA Standards Board is committed to wide consultation in the preparation of the IS Auditing Standards, Guidelines and Procedures. Prior to issuing any documents, the Standards Board issues exposure drafts internationally for general public comment. The Standards Board also seeks out those with a special expertise or interest in the topic under consideration for consultation where necessary.

The following COBIT® resources should be used as a source of best practice guidance:

- *Control Objectives*—High-level and detailed generic statements of minimum good control
- *Control Practices*—Practical rationales and how-to-implement guidance for the control objectives
- *Audit Guidelines*—Guidance for each control area on how to: obtain an understanding, evaluate each control, assess compliance, and substantiate the risk of controls not being met
- *Management Guidelines*—Guidance on how to assess and improve IT process performance, using maturity models, metrics and critical success factors

Each of these is organised by the IT management process, as defined in the *COBIT Framework*. COBIT is intended for use by businesses and IT management as well as IS auditors. Its usage allows for the understanding of business objectives and for the communication of best practices and recommendations around a commonly understood and well-respected standard reference.

The Standards Board has an ongoing development programme and welcomes the input of ISACA members and other interested parties to help identify emerging issues requiring new standards. Any suggestions should be e-mailed ([research@isaca.org](mailto:research@isaca.org)), faxed (+1.847.253.1443) or mailed (address at the end of this guideline) to ISACA International Headquarters, for the attention of the director of research standards and academic relations.

This material was issued on 1 May 2003.

#### Information Systems Audit and Control Association 2002-2003 Standards Board

Chair, Claudio Cilli, CISA, CISM, Ph.D., CIA, CISSP KPMG, Italy  
Claude Carter, CISA, CA Nova Scotia Auditor General's Office, Canada  
Sergio Fleginsky, CISA PricewaterhouseCoopers, Uruguay  
Alonso Hernandez, CISA, ROAC Colegio Economistas, Spain  
Marcelo Hector Gonzalez, CISA Central Bank of Argentina Republic, Argentina  
Andrew MacLeod, CISA, FCPA, MACS, PCP, CIABrisbane City Council, Australia  
Peter Niblett, CISA, CA, MIIA, FCPA Day Neilson, Australia  
John G. Ott, CISA, CPA Aetna, Inc., USA  
Venkatakrishnan Vatsaraman, CISA, ACA, AICWA, CISSPEmirates Airlines, United Arab Emirates

#### 1. BACKGROUND

## **1.1 Linkage to Standards**

- 1.1.1** Standard S6 Performance of Audit Work states, "IS audit staff should be supervised to provide reasonable assurance that audit objectives are accomplished and applicable professional auditing standards are met."
- 1.1.2** Standard S6 Performance of Audit Work states, "During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence."
- 1.1.3** G25 Review of Virtual Private Networks provides guidance.
- 1.1.4** P3 Intrusion Detection Systems (IDS) Review provides guidance.

## **1.2 Linkage to COBIT**

- 1.2.1** The COBIT *Framework* states, "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility, as well as to achieve its expectations, management must establish an adequate system of internal control."
- 1.2.2** The COBIT *Management Guidelines* provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:
  - Performance measurement—How well is the IT function supporting business requirements?
  - IT control profiling—What IT processes are important? What are the critical success factors for control?
  - Awareness—What are the risks of not achieving the objectives?
  - Benchmarking—What do others do? How can results be measured and compared?
- 1.2.3** The *Management Guidelines* provide example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes, and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.
- 1.2.4** The *Management Guidelines* can be used to support self-assessment workshops, and they also can be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.
- 1.2.5** COBIT provides a detailed set of controls and control techniques for the information systems management environment. Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's information criteria.
- 1.2.6** Refer to the COBIT reference located in the appendix of this document for the specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance.

## **1.3 Need for Procedure**

- 1.3.1** Primarily intended for IS auditors—internal as well as external—this document can be used by other IS security professionals with responsibilities in firewall configuration.
- 1.3.2** Modern businesses are organised as a set of core processes operating within supply and demand networks. Almost every organisation in the world is faced with increasing pressure for effectiveness and efficiency (i.e., higher quality requirements for products and services, increased revenue, cost reduction, new product development), a pressure for better, faster and cheaper processes. These increasingly complex operating networks are supported by available communication technologies (mainly the Internet), allowing businesses to focus on their core competencies and partner with others to deliver enhanced value to customers.
- 1.3.3** The transformation of the old processes is enabled by new communication channels. These channels provide new linking possibilities among different systems and networks, making them available to more people and letting the entities and their processes interact, such as, e-procurement and e-sourcing.
- 1.3.4** These new processes have shown the necessity for new techniques to allow authorised access to an organisation's data and programs and protect them from unauthorised (and mostly malicious) access through the new channels that interconnect the existing networks with external sources. In light of this, equipment has been developed with special kinds of functionality (firewalls) that help to minimise the previously mentioned risks.
- 1.3.5** There are various types of firewalls and they are used in several different configurations, each one suited for a specific protection need.
- 1.3.6** This document gives some guidance for IS auditors who are being increasingly faced with having to audit or review new processes that interconnect different entities through means such as the Internet, direct connections and leased networks, and thus evaluate the strength of the protection barriers to provide reasonable assurance of information integrity, availability and confidentiality.

## **2. FIREWALLS**

### **2.1 Types of firewalls**

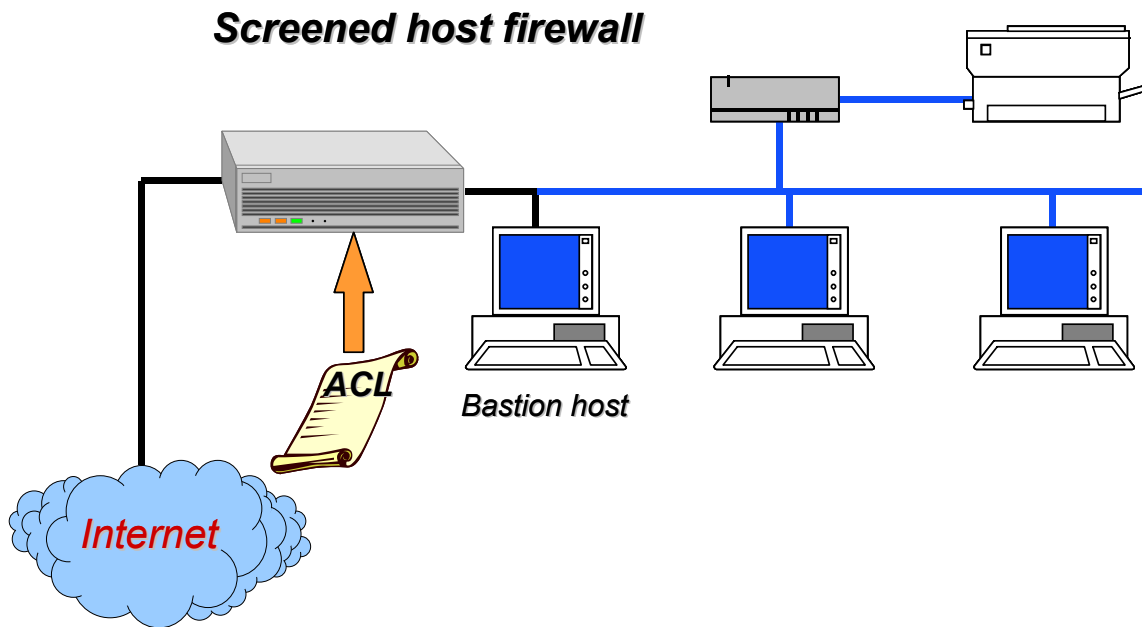
Note: OSI is an acronym for open standards interconnection.

OSI layer/ firewall type	7 Application	6 Presentation	5 Session	4 Transport	3 Network	2 Data Link	1 Physical
Routers used as a firewall							
Packet filter				(not always supported)			
Stateful inspection							
Hybrid firewall technologies							
Application-proxy gateway				(covered as a result of the functions on layer 7)			

**2.1.1** Network layer firewalls generally make their decisions based on the source, on destination addresses and in individual IP packets. A simple router is the “traditional” network layer firewall, since it is not able to make particularly sophisticated decisions about what a packet is actually talking to or from where it actually came. Modern network layer firewalls have become increasingly sophisticated and now maintain internal information about the state of connections passing through them, the contents of some of the data streams, and so on. An important distinction about many network layer firewalls is that they route traffic directly through them, so to use one you either need to have a validly assigned IP address block or to use a “private Internet” address block. Network layer firewalls tend to be very fast and tend to be very transparent to users.

**2.1.2** Screened host firewalls control access to and from a single host by means of a router operating at the network layer. The single host is typically a bastion host—a highly defended and secured strong-point that can resist attack.

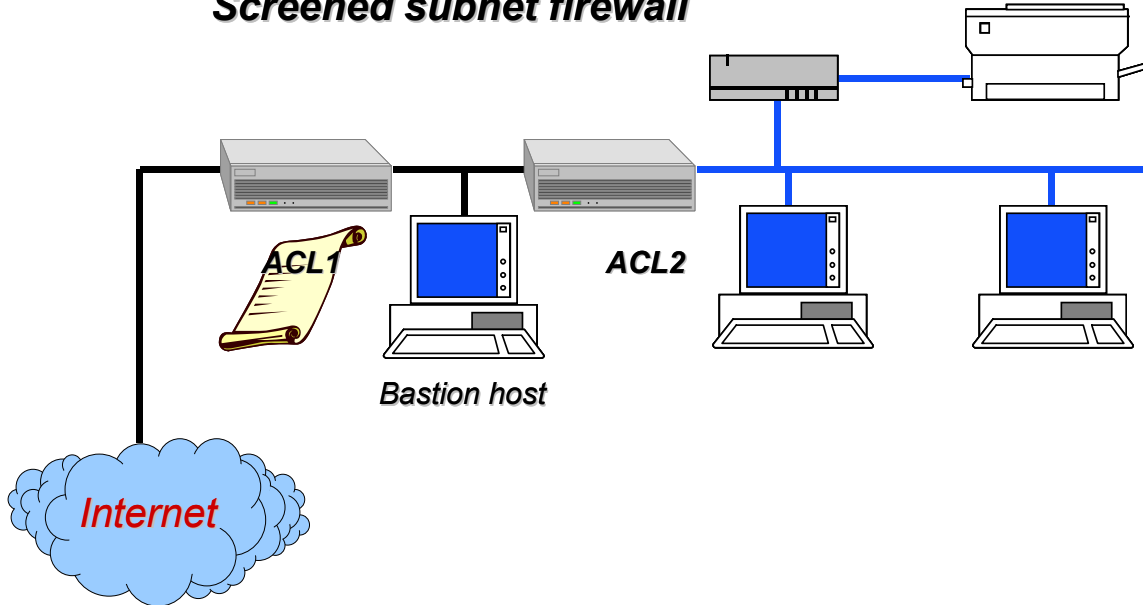
The Internet	Exterior Router	Bastion Host	Internal Network	Trusted Devices
traffic →	traffic → ←	traffic → ←	traffic → ←	traffic ←



**2.1.3** Screened subnet firewalls control access to and from a whole network by means of a router operating at a network layer. It is similar to a screened host, except that it is, effectively, a network of screened hosts.

The Internet	Exterior Router	Bastion Host	Perimeter Network	Interior Router	Internal Network	Trusted Devices
traffic →	traffic → ←	traffic → ←		traffic → ←	traffic → ←	traffic ←

### Screened subnet firewall



**2.1.4** Packet filter firewalls (perimeter solutions) examine all the packets they see, then forward or drop them based on predefined rules. Packet filtering uses source/destination, protocol and port information from the packet header to restrict the flow of traffic. The packet filtering firewall is perhaps the most common and easiest to employ for small, uncomplicated sites. However, it suffers from a number of disadvantages and is less desirable than the other firewalls. Basically, a packet filtering router is installed at the Internet (or any subnet) gateway and then the packet filtering rules are configured in the router to block or filter protocols and addresses. The site systems ordinarily have direct access to the Internet while all or most access to site systems from the Internet is blocked. However, the router could allow selective access to systems and services, depending on the policy. Ordinarily, inherently dangerous services such as NIS, NFS, and X Windows are blocked. Packet filter firewalls can be found on TCP/IP based networks but also on other networks using layer 3 addressing (for example, IPX). Some routers also can provide some basic functions over layer 4, becoming a simple implementation of a stateful inspection firewall. As the filtering rules they use are very simple, they allow fast processing speeds, but at the same time, this feature makes them very susceptible to misconfiguration by defining a set of rules that does not comply with the organisation's security policy. As they do not examine higher layers of data, they are not suited to protect against attacks made using application function, nor can they protect effectively against spoofing attacks. They also have a limited logging capability. This type of firewall is used in environments that require high processing speeds, but no complex logging or authentication functions. This functionality can be included as the only firewalling feature (for example in a router) or may be one among others that operate at higher layers.

The Internet	Firewall	Internal Network	Trusted Devices
traffic →	traffic → ←	traffic → ←	traffic ←

**2.1.5** Stateful inspection (or dynamic packet filtering) is a firewall architecture that works at the network layer. Unlike static packet filtering, which examines a packet based on the information in its header, stateful inspection examines not just the header information but also the contents of the packet to determine more about the packet than just information about its source and destination. It uses a combination of packet filtering, stateful inspection and proxy servers. SI/DPF uses state tables and programmed instructions to analyse information from the packet header and from the contents of the packet (application state), up through the application layer. The information is processed and stored to provide the firewall with a context for classifying traffic. The principal objective is to identify packets that are part of an established connection and to open and close specific ports for that traffic. A stateful inspection firewall also monitors the state of the connection and compiles the information in a state table. These devices examine the packets, remember which connections use which port numbers, and shut down access to those ports after the connection closes. The expressions that define the filters have to be written under the vendor syntax. Stateful inspection/dynamic packet filtering is an extension of the firewall operating system that stores application state and packet header information in a table. That table is used to classify traffic and to apply different processing rules to established connections and to manage opening and closing specific ports.

**2.1.6** Hybrid firewalls combine aspects of packet filtering and application-level filtering. Like packet filtering, these firewalls operate at the network layer of the OSI model, filtering all incoming packets based on source and destination IP addresses and port numbers, and determine whether the packets in a session are appropriate. They also can act like application-level firewalls in that they can review the contents of each packet up through the application layer. Ordinarily they employ some combination of security characteristics of both packet filtering and application filtering products. A hybrid firewall uses a combination of packet filtering, stateful inspection and proxy servers. The objective is to process different types of traffic according to the risk they present and to balance processing time against throughput. In a hybrid implementation, some hosts are behind a traditional firewall, while other hosts live on the outside. An IPSec gateway at the central site provides connectivity to the outside machines. This configuration is common at organisations with a major central site and some number of telecommuters. As in ordinary virtual private networks (VPNs), remote hosts have full access to the inside by virtue of the IPSec tunnel. Traffic from inside machines to the remote nodes is similarly protected. What is distinct is that traffic from remote nodes to the rest of the Internet is governed by the central site's security policy. That is, the firewall administrator distributes a security policy to the remote nodes. Ideally, of course, this same policy statement is used to control the traditional firewall, thus ensuring a consistent security policy.

**2.1.7** Proxy server firewalls run special software written to allow specific programs to function and to enforce authentication, filtering and logging policies. For example, an HTTP proxy is written to specifically allow HTTP access, and only HTTP access, through it. It also requires special action to be taken at the user level. For example, in Netscape, the user must edit the properties dialog—specifically, go into "Advanced," then go into "Proxies," and make the appropriate entries there. As they have no firewall capabilities, they have to be placed behind a firewall. A user who needs to access external resources should use the proxy server that can enforce user authentication, log user activities and can scan, for example, web and e-mail contents. Additional supported functions are content scanning, service blocking, virus removal, etc. Proxy server firewalls typically act as an intermediary for user requests, they set up a second connection to the desired resource either at the application layer via application proxy or at the session or transport layer via circuit relay. They intercept all messages entering and leaving the network. The firewall only allows external systems to communicate with the proxy server. The proxy server effectively hides the true network addresses.

External Host	The Internet	Firewall	Dedicated Proxy Server	Internal Network	Trusted Devices
traffic →	traffic →	traffic → ←	traffic → ←	traffic → ←	traffic ←

Advantages of proxy server firewalls:

- The proxy ordinarily is highly aware of the data format it handles, and can look for many inconsistencies, and provide protection from them.
- Only specific protocols that are to be supported are allowed.

Disadvantages of proxy server firewalls:

- For any new protocol(s) that are allowed, a proxy that is specifically aware of that protocol is necessary.
- If an existing protocol is extended, proxy software will probably need to be updated.

Proxy server firewall provides a controlled network connection between internal and external systems. A virtual circuit exists between the internal client and the proxy server. Internet requests go through this circuit to the proxy server, and the proxy server delivers those requests to the Internet after changing the IP address. External users only see the IP address of the proxy server. Responses are then received by the proxy server and sent back through the circuit to the client. While traffic is allowed through, external systems never see the internal systems. This type of connection is often used to connect "trusted" internal users to the Internet. Used most often for outgoing connections that relay TCP connections and are transparent to the user. During a call, the gateway's relay programs copy bytes back and forth; the gateway acts as a wire.

Auto-connect capability, i.e., external hosts outside the gateway, need access to a printer on the inside. Restrictions on port designation and access control are implemented. Auto-connect assists with connection control, if a hole in the external host is created. Manual servicing is a protocol for the connection service that needs to be implemented to define the desired destination. Either a proxy (destination hostname) or SOCKS (IP address) is implemented. The logs store the bytes and TCP destination but do not examine them.

Advantages of auto-connect proxy firewall servers:

- More secure than a packet level gateway, although not as secure as an application gateway
- Replay TCP connections
- Permissions granted by port address
- Is capable of understanding the contents of the packet

Disadvantages of auto-connect proxy firewall servers:

- Inbound connections are inherently risky. They relay packets without inspection, have limited audit capabilities and no application specific controls
- No application-level checking

**2.1.8** Transparent firewalls are amalgams of proxy server firewalls and network address translation (NAT) (see 4.1.1). An internal machine only has to know where to send packets to reach the outside, similar to a NAT firewall. However, the firewall may transparently invoke proxy-like mechanisms on certain traffic, for security purposes, rather than just blindly forwarding them through. The internal machines may or may not have a private IP address range.

Advantages of transparent firewalls:

- No special configuration on the client side, just like a NAT firewall
- Allows for finer control and protection for well-known services

Disadvantage of transparent firewalls:

- Shares most of the disadvantages of a NAT firewall. If a particular application protocol is being used on a non-standard port, all "special" protections are lost. Depending on the rules allowed, it may not even happen at all.

**2.1.9** Application-level (gateway) firewalls have all the functionality of the dedicated proxy servers, plus the functionality of a firewall (i.e., each proxy application can access the firewall rule base to permit or deny packets). They are generally hosts running proxy servers, which permit no traffic directly between networks, and which perform elaborate logging and auditing of traffic passing through them, as they can inspect all the packets (destination address, ports and packet contents). They can implement enhanced authentication methods, as they can combine more information (they can consider additional information than packet filter and stateful inspection packet filter firewalls, that authenticate users based on the network layer address that it is easily spoofed). Since the proxy applications are software components running on the firewall, it is a good place to do lots of logging and access control. Application layer firewalls can be used as network address translators, since traffic goes in one side and out the other, after having passed through an application that effectively masks the origin of the initiating connection. Having an application in the way in some cases may effect performance and may make the firewall less transparent (in high-bandwidth applications a dedicated proxy server behind a firewall is often a preferred solution). An application-layer firewall, called a dual-homed gateway, is a highly secured host that runs the proxy software. It has two network interfaces, one on each network, and blocks all traffic passing through it.

The Internet	Firewall (Dual Homed Host)	Internal Network	Trusted Devices
traffic →	traffic → ←	traffic → ←	traffic ←

Advantages of application-level (gateway) firewalls:

- Easier to log and control all incoming and outgoing traffic
- Application layer firewalls can incorporate encryption to protect traffic transmissions

Disadvantages of application-level (gateway) firewalls:

- Administratively intensive—each networked service requires separate configuration (i.e., HTTP, telnet, mail, news)
- Inside users must use proxy-aware clients for most services
- Without further modifications to a service client, the user would have to connect to firewall. Modifications can be applied to make this connection transparent to the user

### 3. COMMON FUNCTIONS AND FEATURES RELATED TO FIREWALLS

#### 3.1 Network Address Translation

##### 3.1.1

NAT is a tool for "hiding" the network-addressing schema present behind a firewall environment. It allows a chosen addressing schema to be deployed behind a firewall, while still maintaining the ability to connect to external resources through the firewall. It also allows the mapping of nonroutable IP addresses to a smaller set of legal addresses. Network address translation can have three modes:

- Static NAT—Each internal system on the private network has a corresponding external, routable IP address associated with it. With this technique, it is possible to maintain the ability to provide selective access to external users (an external system could access an internal server and the firewall would perform mappings in either direction, outbound or inbound).
- Hiding NAT—All internal IP addresses are hidden behind a single IP address. The main weakness of this configuration is that it is not possible to make resources available to external users once they are placed behind a firewall, as mapping in reverse from outside systems to internal systems is not possible, so systems that must be accessible to external systems must not have their addresses mapped. In this type of implementation, the firewall must use its own external interface address as the substitute or translated address, impairing the flexibility of the configuration.
- Port address translation (PAT)—Similar to hiding network address translation, but with some differences. That is, it does not require use of the IP address of the external firewall interface, and the access to resources behind a firewall system can be granted selectively by forwarding inbound connections on certain port numbers to specific hosts.

##### 3.1.2

Advantage of NAT:

- Requires no special configuration on the client side, except for normal routing configuration. Clients just have to know their default gateway.

##### 3.1.3

Disadvantages of NAT:

- There is no additional security beyond selecting "allow this type of traffic." Once an internal client connects via an allowed protocol, anything can happen within the bounds of that protocol.
- There is no way to allow for special protocols that require a return connection to be made.

##### 3.1.4

If certain types of protocols are to be restricted, access can be limited to certain ports. On the one hand, this is too restrictive, because internal users may not be able to access web servers on nonstandard ports. And at the same time, this is too permissive,

because there may be a disallowed service running on a nonstandard port on the outside, and internal users will be able to access it in this case.

## **3.2 Intrusion Detection Systems (IDS)**

**4.2.1** These systems are designed to notify and prevent unauthorised access to a networked system or resource. Often they interact with firewalls to generate an automatic response against a perceived threat (e.g., blocking the source of the attack).

**3.2.2** Attack recognition and response software works by continually monitoring network traffic and looking for known patterns of attack. When the software detects unauthorised activity, it responds automatically with some form of defined action configured by the administrator.

**3.2.3** Requirements for a good intrusion detection system are:

- Installable throughout the overall network to ensure enterprisewide security
- Monitor incoming and outgoing traffic
- Provide protection for LANs, Internet, intranet and dial-up access
- Generate alarms in real time to appropriate personnel, such as administrators and security officers
- Configurable to automatically eliminate the intruder and block the intruder's reentry
- Selectively log session data
- Provide audit trails to help reconstruct the attack, for post-investigative analysis
- Can be administered remotely, and can encrypt the administration sessions for security purposes (if required by the client organisation)

**3.2.4** Intrusion detection systems are not able to assist in:

- Compensating weaknesses in network protocols
- Analysing all the traffic on a busy network
- Dealing with some of the modern network hardware and related features
- Compensating for weak identification and authentication mechanism(s)
- Compensating for problems in the quality or integrity of information the system provides
- Conducting investigations of attacks without human intervention

**3.2.5** The installation of an IDS should be made first by establishing the network perimeter and identifying all possible points of entry. Once identified, IDS sensors can be put in place, configured to report to a central management console. Possible placements are suggested as follows:

- Between the network and extranet
- In the DMZ (demilitarised zone, see section 5.2) before the firewall to identify the attacks on servers in the DMZ
- Between the firewall and the network, to identify a threat in case of the firewall penetration
- In the remote access environment
- If possible between the servers and the user community, to identify the attacks from the inside
- On the intranet, FTP and database environments

**3.2.6** Intrusion detection systems can be classified in two categories, host-based and network-based. The effectiveness of network-based intrusion detection is ordinarily greater than host-based intrusion detection, due to its ability to monitor multiple systems and resources. These types of systems ordinarily generate false attack identification, needing human intervention to determine the real attacks. Definitions of the two categories of IDS are as follows:

- Host-based intrusion detection—Highly integrated with the operating system, it should be installed on each individual computer system that is to be protected. There are some issues that arise from the use of this type of system:
  - They have a negative effect on system performance.
  - They do not provide effective detection over network-based (for example, denial of service).
  - They can affect system stability.
- Network-based intrusion detection—Analyses protocols, monitoring network traffic looking for specific strings that could indicate certain types of attacks. The issues that arise from the use of this type of systems are:
  - In most cases, they can not effectively detect signatures that are distributed among several packets.
  - They ordinarily require special equipment configurations (feature sometimes not supported) to establish promiscuous mode network interface.
  - They can be detected by identifying promiscuous mode network interface.
  - Sometimes it is difficult to predict the signature that identifies an attack.

## **3.3 Virtual Private Networks (VPN)**

**3.3.1** A virtual network is constructed in an encrypted or unencrypted form on top of existing network media, to establish secure network links across networks that are not trusted (for example the Internet). This technology can be used to provide secure remote access to corporate networks or link networks between different organisations. The most common protocols used are:

- IPSec
- PPTP (Microsoft Point-to-Point Tunneling Protocol)
- L2TP (Layer 2 Tunneling Protocol)

## **4. COMMON FIREWALL CONFIGURATIONS**

### **4.1 Common Firewall Configurations Uses**

**4.1.1** Most common uses of firewalls are:

- Control access for internal and external networks (perimeter firewalls)

- Control access among public accessible and public inaccessible servers (DMZ firewalls)
- Control access among internal networks with different access and security requirements
- Control access thru pools of modems and private dial-up networks
- Control access to and from third party administered hosts and networks
- Encrypt internal and external networks that transmit sensitive data
- Hide internal network addresses from external networks (NAT)

## 4.2 Demilitarised Zone (DMZ)

**4.2.1** A DMZ greatly increases the security of a network, protecting any computer that needs to be available from an external network behind one firewall and adding a layer of protection between the shared machine and the internal network. If appropriately configured, there are two protection layers for an attacker to compromise to get to anything valuable.

**4.2.2** This type of configuration greatly increases the skills required by an external hacker to compromise the internal network and thus lowers the threat of the internal network being compromised. To further reduce risk, usage of different compatible technologies reduces the chances of exposure.

**4.2.3** In a DMZ network, the untrusted host is brought "inside" the firewall, but placed on a network by itself (the firewall host then interconnects three networks). This increases the security, reliability, and availability of the untrusted host, but it does not increase the level of trust that other "inside" hosts can afford. Other untrustworthy hosts for other purposes, such as a public web site or FTP server, can easily be placed on the DMZ network, creating a public services network.

**4.2.4** Sometimes a single firewall with three network interface cards is used to implement a DMZ. One of the cards is attached to the external network, the second to the internal network, and the third to the DMZ network. This configuration does not prevent against service degradation effectively during a denial-of-service attack.

The Internet	Firewall	DMZ (dual-homed) eth0/eth1 (SMTP/WWW/DNS, etc.)	Internal Network	Trusted Devices
traffic →	traffic → ←	traffic → ←	traffic → ←	traffic ←

**4.2.5** Advantages and considerations of DMZs:

- Price of the hardware and software of the extra machines needed to implement a DMZ
- Slight decrease in performance
- Cost of the time to implement the DMZ
- Cost of down time the system suffers from adding on the DMZ
- Lowered level of accessibility to an attacker

## 4.3 DMZ with Dual Firewall Configuration

**4.3.1** The organisation's internal network is further isolated from the untrustworthy network by adding a second firewall host. By connecting the untrustworthy network to one firewall host, the organisation's internal network to the other, and the DMZ between, traffic between the internal network and the Internet must traverse two firewalls and the DMZ.

**4.3.2** In a more comprehensive definition, consider an Internet protocol (IP)-based infrastructure between an external network (the exterior) and an internal network (the interior). Such an infrastructure typically contains different types of machines: network devices (i.e., routers); systems (i.e., servers running applications, such as e-mail or a web service), and, of course, security appliances (i.e., firewalls). Each firewall interface is considered to represent a different segment of the infrastructure, which is called the DMZ network.

**4.3.3** In each of these architectures, firewalls are used to control access at the border of the network mainly for the purpose of protecting the network from an untrusted network. Firewalls deployed entirely within the network can also be used to provide mutual protection among subnets of the network. Controlling access between internal subnets is no different than controlling access between a network and the Internet, so all of the above architectures can be used as internal firewall architectures as well.

**4.3.4** In a multiple-layer architecture the firewall functions are distributed among a small number of hosts, typically connected in series, with DMZ networks between them. This approach is more difficult to design and operate, but can provide substantially greater security by diversifying the defences being implemented. Although more costly, it is prudent to use different technologies in each of these firewall hosts. This reduces the risk that the same implementation flaws or configuration errors may exist in every layer. This approach will reduce the chance of redundancy and greater possibility of compromise. The most common design approach for this type of architecture is an Internet firewall composed of two hosts interconnected with one DMZ network.

## 4.4 Proxy Server

**4.4.1** Proxy servers are used in environments that require stronger authentication methods and good logging functions, as each proxy agent is able to require authentication of each individual network user. On the other side, these enhanced security capabilities require more processing power, and thus makes them unsuitable for environments with high-bandwidth requirements. A special agent for the traffic of each application is required on the firewall. They can analyse e-mail and web content by:

- Java applet, ActiveX control, JavaScript filtering
- Blocking some MIME types
- Virus, and macro virus scanning
- Application command blocking
- User-defined blocking functions

## 5. RISKS CONTROLLED BY FIREWALLS

### 5.1 Attacks Based on Software Weaknesses

- 5.1.1** The objective of this type of attack is to put the server on a virtual offline condition (denial of service attack, DoS), but unauthorised access could also occur.
- 5.1.2** Buffer overflow is probably one of the most effective types of attack. It is not associated with a particular application and it uses publicly known bugs or weaknesses of the software to generate an error condition in the program used to handle a service. The most common origin of the problem is when portions of memory used by the program are rewritten by an overflow condition. An example of an attack using this weakness is the one made by the virus Code Red.
- 5.1.3** Directory transversal attack is directed against web servers, trying to access the file systems outside the authorised pages. This can result in unauthorised access to data, or execution of unauthorised code. In some of the oldest versions of the software, using an URL in the form of `http://server/../../../../` was enough. An example of an attack using this weakness is the one made by the virus NIMDA.
- 5.1.4** Source disclosure attack is directed against web servers that process dynamic pages. They try to access their source code that can include installation information, such as user IDs and passwords to access databases. This form of attack can be made issuing a special URL that the server processes incorrectly, or makes the server execute some software components that can contain errors or bugs.
- 5.1.5** MIME exploit attack is directed against mail clients and services and, in some cases, against browsers. The attack consists of the modification of headers to provoke certain situations, such as DOS, program executions. Some of the controls that can be in place are:
- Continuous follow-up of published bugs and weaknesses, and installation of patches and software updates
  - Procedures to control system and application logs to detect attacks

### 5.2 Attacks Based on Processing Power

- 5.2.1** SYN floods are intended to generate an error in the program used to handle the service. In their simplest form, they overwrite memory used by data or program code and thus generate the error. In more dangerous forms, the attacks manage to execute program code provided by the attacker. As the services are ordinarily executed at a high level of privilege, these types of attacks are high risk. Ordinarily, packets include false origination addresses. SYN floods generate two basic problems—bandwidth shortage and growth of the connection table on the server. Controls that can be put in place against this type of attack (although they cannot have a total effectiveness) include:
- Configuring firewalls to detect and filter spoofed addresses
  - Adjusting connection parameters, such as number of waiting connections and timeouts, to avoid excessive growth of connection table
- 5.2.2** UDP flooding is similar to the previous case. The main difference is that UDP does not use the concept of connections. The attack is based on the occupied bandwidth and, eventually, in the resources used by the server to answer the packets.
- 5.2.3** ICMP floods have been some of the most effective past attacks. They use the configuration problems to enhance the attacks. One of the most well-known applications, Smurf, is based on using other networks to attack the final target.
- 5.2.4** DDoS attacks intend to flood the target site with one or more attacks of DoS. It does not use software bugs or configuration errors. The attack ID is based on a massive use of bandwidth and requires that many previously affected nodes of the network (hundreds) participate in the attack. There are not so many options to prevent this type of attack. Some of the controls that can be in place are:
- Packet filtering
  - Providing reasonable assurance that weaknesses of interconnected sites are as well controlled as they can be
  - Adjusting parameters to control excessive connection table growth

## 6. PROCEDURES TO REVIEW FIREWALLS

	Suggested Procedures	√	
<b>Gather preliminary information</b> —These are examples of information that can be obtained to plan the audit work.	Obtain security policies.		
	Obtain the firewall security policy.		
	Identify the services that the firewall is intended to protect and perform a high-level risk assessment of their sensitivity considering the seven information criteria defined by COBIT.		
	Identify the risk assessment process in place to identify the main sources of threats and the probability of their occurrence.		
	Develop an understanding of how the technology is being used, including the security measures in place, such as authentication methods, security administration and hardware maintenance.		
	<b>Gather preliminary information</b> continued	Identify procedures used in the systems development life cycle, for the set of applications used from the outer network (those accessed directly and the ones they use thru interfaces) and for the system software of the firewall.	
		Determine the logging functionality in place.	
		Identify the procedures used for rule base maintenance.	
		Identify the procedures used to monitor new bugs or weaknesses of the software used.	
		Identify the procedures used to review systems and application logs to detect attacks.	
	Identify the procedures to share technical and security incident related information with neighbor sites.		
	Identify the configuration management procedures.		
<b>Risk assessment</b>	Adjust the scope of the review using the information on sensitivity of the services that the firewall is		

	<b>Suggested Procedures</b>	√
	intended to protect, the identified risks, and the likelihood of their occurrence.	
<p><b>Detailed planning—</b> All the control objectives that can be identified as a result of selecting COBIT processes can be reviewed by usual installation reviews. This section includes some special procedures that can be included as a part of a firewall installation review. These are examples of areas to include in the review.</p>	For the IDS installation, review the analysis made to evaluate the existing network, the identification of entry points, the types of traffic allowed by firewalls, the analysis rules introduced, and the alarms and notification schema set.	
	Review each DMZ on an individual basis, while considering the others as a different network or computer as applicable. In this approach, the configuration and rules should be considered against all the types of traffic of the networks related to the DMZ.	
	Review the procedures used to monitor security-related sources of information (mainly web sites and specialised sources) and identify new types of attack, such as software bugs; consider verification of whether all available security patches have been applied.	
	Review the systems development life cycle controls in place over the code executed as part of the firewall software and the applications published to the outer side of the network, such as segregation of duties, initiation and testing.	
	Review the authentication controls used to control access from the outer network.	
	Review the procedures used for device administration (including at least physical access and administrators' passwords, for example, to reduce the risk of tampering the connections thru unauthorised access.	
	Review the procedures used to control remote access for administering network devices (by administrators or vendors).	
	Review the procedures to review the logs in an effective and timely manner and to deal with potential harmful traffic.	
	Review the procedures for dealing with potential or effective attacks.	
	Review the procedures for rule-base maintenance, such as reviewing access to maintenance functions, request procedures, new or modified rules testing, transfer to production and documentation. Determine if there is a formal and controlled process in place to request, review, approve and elevate firewall addition and changes into the production environment. Specifically:	
	<ol style="list-style-type: none"> <li>1. Determine if the formal request includes the business purpose and sponsor, date it is requested and how long (in time duration) the rule will be needed.</li> <li>2. Determine if the review is completed by technically competent individual who understands the risk associated with the rule. The reviewer should document the risk in relation to the protection of the entire information infrastructure.</li> <li>3. Determine if the approval includes both the head or supervisor of the firewall administrator and the appropriate business manager. The approval of the firewall rule request must be done formally.</li> <li>4. Determine if the firewall rule is formally tested first in a test environment prior to elevation into the production processing environment.</li> </ol>	
	Where possible, test for outage of services (for example identifying unusual amounts of off-hours made by the unit where the change was requested).	
	Review risk management procedures.	
	Identify the existence of single points of failure.	
	Review virtual private network in place (see guidance on Virtual Private Networks from ISACA).	
	Review the plan for conducting penetration tests and the criteria for re-performing the tests when changes are made. Coverage of the risks identified by the tests.	
	Identify the filtering rules in place (to determine if they address all the issues included in the security policy and other applicable threats identified during the risk analysis). Verify that the overall firewall rule restrict access, unless specifically allowed by the rules.	
	Review the procedures to test revised rules prior to the transfer to production environment.	
	Review physical access controls to firewall and network equipment that connects it to the networks.	
	Review the procedures used to test new software and configure its security to accomplish defined security policies.	
Review disaster recovery and contingency procedures. The existence of a fail-over device to back up the processing functions of the firewall should be considered (as its services ordinarily have high-availability requirements).		
Review configuration management processes.		
<p><b>Stateful inspection/ dynamic packet filtering (SI/DPF)</b></p>	Document how SI/DPF will affect the controls provided by the other firewall when the SI/DPF is used as the border firewall and there is another firewall behind it.	
	Confirm that program change controls (specially testing controls) are applied to any API if APIs in SI/DPF are used (to execute code written by the organisation by the firewall operating system).	
	SI/DFP uses state tables and programmed instructions. It uses information from the packet header and from the contents of the packet, up through the application layer. The information is processed and stored to provide the firewall with a context for classifying traffic. The principal objective is to identify packets that are part of an established connection and to open and close specific ports for that traffic. Design and perform testing of traffic that will be affected by SI/DPF, to verify its proper functioning.	

	<b>Suggested Procedures</b>	√
	<p>Examples of aspects to consider when reviewing filters—gateways, FTP sessions, X Windows, DNS, fixed addresses. Confirm that:</p> <ul style="list-style-type: none"> <li>■ It only allows access to those addresses intended to be accessed from the outside</li> <li>■ Does not allow use of unauthorised services, such as FTP and Telnet</li> <li>■ Does not allow to access certain ports</li> <li>■ Only allows packets that come from authorised sites from the outer network</li> <li>■ Discard all source-routed traffic</li> </ul>	
	Evaluate access control rules or other measures that are set up to drop packets representing undesirable communications such as denial of service attacks against the devices.	
	Confirm that there are rules in place to avoid IP spoofing.	
	Confirm that if NAT is used, only those packets that come from certain allowed IP addresses in the internal network are passed, and that incoming traffic is only allowed when a valid connection is established.	
<b>Packet filtering</b>	When the router is used as the border firewall and there is another firewall behind it, document how it will affect the controls provided by the other firewall.	
	Obtain (or create) an understanding of how packet filtering is being used to filter the packets in terms of the use of source/destination, protocol, and port information from the packet header.	
	Assess the effect on controls and identify the key areas of risks created by the use of packet filtering. Confirm that:	
	<ul style="list-style-type: none"> <li>■ It only allows access to those addresses intended to be accessed from the outside</li> <li>■ Does not allow use of unauthorised services, such as ftp and telnet</li> <li>■ Does not allow to access certain ports</li> <li>■ Only allows packets that come from authorised sites from the outer network</li> <li>■ Discard all source-routed traffic</li> </ul>	
	Design and perform testing of traffic that will be affected by packet filtering.	
	Evaluate rules that are set up to drop packets representing undesirable communications such as denial of service attacks against the devices.	
	Confirm that there are rules in place to avoid IP spoofing.	
	Confirm that if NAT is used, routing to internal IP addresses cannot be made directly.	
<b>Inherent risks of packet filtering</b>	There is little or no logging capability, thus an administrator may not determine easily whether the router has been comprised or is under attack	
	Packet filtering rules are often difficult to test thoroughly, which may leave a site open to untested vulnerabilities.	
	If complex filtering rules are required, the filtering rules may become unmanageable.	
	Each host directly accessible from the Internet will require its own copy of advanced authentication measures.	
<b>Hybrid firewalls</b>	Document how the use of the hybrid firewall will affect the controls over network traffic.	
	Obtain (or create) an understanding of how the three firewall approaches are being used (packet filtering, stateful inspection and proxy servers). Determine the logic for passing traffic into each of the firewall's processes.	
	Assess the effect on controls and identify the key areas of risks created by the use of a hybrid approach. Assess the decision logic applied to determine which firewall approach will be applied to each type of traffic.	
	Design and perform testing of traffic that will be affected by SI/DPF, considering the following rules:	
	<ul style="list-style-type: none"> <li>■ Confirm there is consistency in sending similar protocols to the same process within the hybrid.</li> <li>■ Confirm that any API's used in stateful inspection are controlled.</li> <li>■ Confirm the proxy process is maintaining the separation between the traffic and the application.</li> <li>■ Confirm the balance between throughput and control processing is appropriate.</li> </ul>	
	Evaluate access control rules or other measures that are set up to drop packets representing undesirable communications such as denial of service attacks against the devices.	
<b>Proxy firewalls</b>	The proxy firewall could be a separate device, or a service running on a multipurpose firewall device. Its purpose is to add special processing controls to one type of traffic.	
<b>Proxy firewalls continued</b>	Obtain (or create) an understanding of the use of the proxy—which traffic is being sent through the proxy and which devices are receiving the output.	
	Confirm that all traffic of the type being processed by the proxy must flow through the proxy firewall. For all devices on the inside of the proxy, confirm traffic of the type being proxied is only accepted from the proxy device address.	
	Design and perform testing of traffic that will be affected by the proxy, considering the following:	
	<ul style="list-style-type: none"> <li>■ Confirm all traffic is directed to the proxy</li> <li>■ Confirm that all traffic of the type being proxied is only processed from the address of the proxy.</li> </ul>	
	Evaluate the procedures for the review of logs from the proxy and the effectiveness of procedures to address potential problems identified from the logs.	
<b>DMZ—Consider a DMZ network with</b>	Verify the firewall is invisible to the exterior.	
	Verify systems on the DMZ segment are invisible to the exterior.	

	<b>Suggested Procedures</b>	√
<p>three segments: one embodies the connection to the exterior, one embodies the connection to the interior, and one, the DMZ segment, consists of the IP subnet on which reside systems that can be accessed from the exterior.</p> <p><b>DMZ</b> continued</p>	<p>If external service providers can troubleshoot devices at the edge of the DMZ network where connectivity with the service providers (and with the exterior in general) is made, confirm that:</p> <ul style="list-style-type: none"> <li>■ Tests have identified the precise extent to which what is in the DMZ network may be mapped and</li> <li>■ The potential exploitation effect is understood.</li> </ul>	
	<p>Review the DMZ network to provide reasonable assurance that external entities cannot administer or configure:</p> <ul style="list-style-type: none"> <li>■ The firewall</li> <li>■ Network devices and systems in the DMZ Network (If network devices on the external facing segment, such as routers that connect with service providers, can be accessed for any reason, such as troubleshooting, verify controls exist over who can administer/configure these devices.)</li> </ul>	
	<p>Verify access control rules are set up in network devices on the external facing segment for the purpose of denying packets that represent undesirable communications, such as denial-of-service attacks.</p>	
	<p>Review firewall rules to verify every packet is by default denied unless a specific rule exists to permit the packet to proceed but only to a destination system in the DMZ segment.</p>	
	<p>Confirm systems on the DMZ segment are set up so they cannot communicate with any other system outside the DMZ segment except through the firewall. If exceptions exist, evaluate the specific risks, the justification, and the compensating controls.</p>	
	<p>Confirm systems on the DMZ segment are set up so that they cannot initiate communications with the interior. Again, if exceptions exist, evaluate the specific risks, justification and compensating controls.</p>	
	<p>Confirm network devices, firewalls and systems on the DMZ network are configured so that routing between any possible combination of devices, firewalls and systems is well defined:</p> <ul style="list-style-type: none"> <li>■ All routes into, through and out of the DMZ network are easily identifiable.</li> <li>■ The routing set up is the minimum needed to support authorised communications flows. (If nonroutable communications protocols are used, confirm they have a purpose consistent with security policy requirements for the DMZ network.)</li> </ul>	
	<p>If NAT is used, provide reasonable assurance it works in a manner consistent with security policy requirements and that the configuration is periodically recertified by accountable individuals.</p>	
	<p>Confirm the firewall is set up:</p> <ul style="list-style-type: none"> <li>■ To deny all packets entering from the exterior with source IP addresses set up for internal networks.</li> <li>■ To deny all packets coming from the interior with source IP addresses not set up for the interior.</li> </ul>	
	<p>Confirm firewall rules discover external attempts to scan for commonly scanned ports (regardless of whether systems actually exist to listen on such ports).</p>	
	<p>Confirm the firewall is set up so that no message is returned in reply to any incoming packet that is denied.</p>	
	<p>Confirm the firewall has been tested by scanning every segment, including the DMZ segment, from every other segment to identify what packets can and cannot get through. Provide reasonable assurance the results are consistent with the overall security policy.</p>	
	<p>Confirm every rule in the firewall is consistent with the security policy. That is, provide reasonable assurance of consistency with policy is verifiable by examining the following components of potentially acceptable packets: protocol, source system IP address, destination system IP address, source port and destination port. For example, the destination system and port combination in a rule should make sense when the function of the destination system on the DMZ segment is considered. A rule should protect the firewall itself; should align with the functions provided by the systems on the DMZ segment; and should permit systems on internal networks to initiate communications with systems on the DMZ segment or allow systems on the DMZ segment respond to communications initiated from the interior. If the rule base has too many rules to be reviewed during the test, it may be an indicator of a poor security architecture design, making it very difficult to administer and to ensure proper coverage.</p>	
	<p>Confirm the rules in the firewall deny all packets that include TCP or UDP ports above port 1023 to provide reasonable assurance the application ports are being used as intended. If not, evaluate the specific risks, justification and compensating controls.</p>	
	<p>If multiple physical firewalls exist in the DMZ network for high-availability, redundancy or failover purposes, confirm the running configurations of the firewalls are equivalent.</p>	
<b>Additional key points to consider</b>		
<b>Configuration</b>	<p>DNS, e-mail, server load balancing services, or any software or services not related to firewall-specific functions should not be installed in or processed by the firewall.</p>	
	<p>Firewalls should be configured to hide internal restricted DNS information from external networks.</p>	
	<p>External firewalls should restrict incoming SNMP queries.</p>	
	<p>Router access control lists do not provide the protection level required for a firewall solution. A router should be used as part of a firewall solution (for example: initial Internet facing filter). This provides connection and removes some of the workload from the firewall by only passing those ports that are required, rather than having the firewall filter every single port. (However, there should still be rules in place to block unused ports on the firewall, just in case.)</p>	

	Suggested Procedures	√
	Configure firewalls as "fail closed."	
	Hide internal network information from external sources.	
	Configure firewalls to "deny all services, unless explicitly allowed."	
	Translate addresses of internal network nodes that are allowed to communicate with external networks.	
	Avoid UDP-based services when possible.	
	Scan, filter or block Java, JavaScript and ActiveX.	
	Limit NNTP to users that need it. This should be formally justified.	
	If possible, use static routing instead of routing protocols.	
	Apply strong security policies to the host where the firewall resides.	
	Restrict access to firewall generated logs to avoid its deletion or modification in an unauthorized manner.	
	Apply all security-related patches or similars to the components of the firewall system.	
	Determine procedures are in place to verify security policies (for example: penetration testing, manual reviews of rule base, OS security reviews, etc.).	
	Verify integrity monitoring tools for sensitive system files on the firewall system exist.	
<b>Monitor, audit and incident response</b>	Monitor firewall alerts on a continuous basis.	
	Log all the firewall activity.	
	Determine sensitive or high-risk connections have additional protection tools, such as intrusion detection systems.	
<b>Backup and recovery</b>	Verify continuity plans for firewalls are in accordance with those of other high-availability services, as firewalls ordinarily are components related to services with high-availability requirements.	

## 7. EFFECTIVE DATE

**7.1** This procedure is effective for all information systems audits beginning on or after 1 August 2003. A full glossary of terms can be found on the ISACA web site at [www.isaca.org/glossary.htm](http://www.isaca.org/glossary.htm).

## APPENDIX

### CobIT Reference

Selection of the most relevant material in CobIT applicable to the scope of the particular audit is based on the choice of specific CobIT IT processes and consideration of CobIT's information criteria.

This procedure links to the following primary CobIT processes:

- PO9 Assess risks
- DS4 Ensure continuous service
- DS5 Ensure systems security (5.20 is a specific control objective for firewalls)
- AI6 Manage changes

This procedure links to the following CobIT processes:

- AI2 Acquire and maintain application software
- AI3 Acquire and maintain technology infrastructure (3.4, 3.5, 3.6 and 3.7 control objectives)
- AI4 Develop and maintain IT procedures
- AI5 Install and Accredited Systems
- DS1 Define and manage service levels
- DS2 Manage third party services
- DS3 Manage performance and capacity
- DS10 Manage problems and incidents
- PO2 Define the information architecture
- M3 Obtain independent assurance

The information criteria most relevant to a firewall audit are:

- Primary: integrity, availability and confidentiality
- Secondary: effectiveness and reliability

### References

For reference purposes and only as an example some useful pages are listed:

CERT/CC (Computer Emergency Response Team/Coordination Center), [www.cert.org/tech\\_tips/packet\\_filtering.html](http://www.cert.org/tech_tips/packet_filtering.html)

Checkpoint FW1, [www.checkpoint.com/products/security/index.html](http://www.checkpoint.com/products/security/index.html)

Cisco Pix, [www.cisco.com/warp/public/cc/pd/fw/sqfw500/](http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/)

Digital Robotics (Internet Firewall 2000), [sysopt.earthweb.com/reviews/firewall/index3.html](http://sysopt.earthweb.com/reviews/firewall/index3.html)

Federal Computer Incident Response Center (FedCIRC) [www.fedcirc.gov/](http://www.fedcirc.gov/)

Firewall Options Chart, [www.networkbuyersguide.com/search/105242.htm](http://www.networkbuyersguide.com/search/105242.htm)

Guardian, [www.netguard.com/subpages/products.htm](http://www.netguard.com/subpages/products.htm)

National Infrastructure and Protection Center, [niap.nist.gov/](http://niap.nist.gov/)

NetScreen, [www.netscreen.com/products/](http://www.netscreen.com/products/)

Network Ice (Black Ice Defender), [www.networkice.com/products/soho\\_solutions.html](http://www.networkice.com/products/soho_solutions.html)  
NIST's Vulnerability Database, [icat.nist.gov](http://icat.nist.gov)  
Nokia, [www.nokia.com/securitysolutions/network/index.html](http://www.nokia.com/securitysolutions/network/index.html)  
SANS Institute, [www.sans.org/top20.htm](http://www.sans.org/top20.htm)  
Sonic FW, [www.rosser.com.au/products/Sonic/sonproducts.htm](http://www.rosser.com.au/products/Sonic/sonproducts.htm)  
Symantec/Axent, [enterprisesecurity.symantec.com/content/productlink.cfm#2](http://enterprisesecurity.symantec.com/content/productlink.cfm#2)  
SYN Flooding and IP Spoofing Attacks [www.cert.org/advisories/CA-1996-21.html](http://www.cert.org/advisories/CA-1996-21.html)  
UDP Port Denial-of-Service Attacks [www.cert.org/advisories/CA-1996-01.html](http://www.cert.org/advisories/CA-1996-01.html)

### **Freeware Firewall Products**

Sygate, [www.sygate.com/swat/products/default.htm](http://www.sygate.com/swat/products/default.htm)  
Tiny Personal Firewall, [www.tinysoftware.com/home/tiny?s=6007837888603234397A0&la=EN&va=aa&pg=prod\\_home](http://www.tinysoftware.com/home/tiny?s=6007837888603234397A0&la=EN&va=aa&pg=prod_home)  
ZoneAlarm, [www.rosser.com.au/products/Sonic/sonproducts.htm](http://www.rosser.com.au/products/Sonic/sonproducts.htm)

### **Firewall Reporting Products**

[www.stonylakesolutions.com/sls/insideout.jsp](http://www.stonylakesolutions.com/sls/insideout.jsp)

### **Hardware Platforms (commonly used configurations)**

Dell  
HP/Compaq  
HP-UX  
IBM  
Macintosh  
Sparc  
Sun

### **Operating Systems (commonly used configurations)**

Linux  
Macintosh  
Netware  
UNIX  
Windows

© Copyright 2003  
Information Systems Audit and Control Association  
3701 Algonquin Road, Suite 1010,  
Rolling Meadows, IL 60008 USA  
Telephone: +1.847.253.1545 Fax: +1.847.253.1443  
E-mail: [research@isaca.org](mailto:research@isaca.org)  
Web site: [www.isaca.org](http://www.isaca.org)