INTERNATIONAL STANDARD

ISO/IEC 18028-3

First edition
2005-12-15

Information technology — Security techniques — IT network security —

Part 3: Securing communications between networks using security gateways

Technologies de l'information — Techniques de sécurité — Sécurité de réseaux TI —

Partie 3: Communications de sécurité entre réseaux utilisant des portails de sécurité

Reference number
ISO/IEC 18028-3:2005(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 18028-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 18028 consists of the following parts, under the general title *Information technology — Security techniques — IT network security*:

— *Part 2: Network security architecture*

— *Part 3*: *Securing communications between networks using security gateways*

— *Part 4: Securing remote access*

The following parts are under preparation:

— *Part 1: Network security management*

— *Part 5: Securing communications across networks using Virtual Private Networks*

Introduction

The telecommunications and information technology industries are seeking cost-effective comprehensive security solutions. A secure network should be protected against malicious and inadvertent attacks, and should meet the business requirements for confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability of information and services. Securing a network is also essential for maintaining the accuracy of billing or usage information as appropriate. Security capabilities in products are crucial to overall network security (including applications and services). However, as more products are combined to provide total solutions, the interoperability, or the lack thereof, will define the success of the solution. Security must not only be a thread of concern for each product or service, but must be developed in a manner that promotes the interweaving of security capabilities in the overall end-to-end security solution. Thus, the purpose of ISO/IEC 18028 is to provide detailed guidance on the security aspects of the management, operation and use of IT networks, and their inter-connections. Those individuals within an organization that are responsible for IT security in general, and IT network security in particular, should be able to adapt the material in ISO/IEC 18028 to meet their specific requirements. Its main objectives are as follows:

— in ISO/IEC 18028-1, to define and describe the concepts associated with, and provide management guidance on, network security – including on how to identify and analyse the communications-related factors to be taken into account to establish network security requirements, with an introduction to the possible control areas and the specific technical areas (dealt with in subsequent parts of ISO/IEC 18028);

— in ISO/IEC 18028-2, to define a standard security architecture, which describes a consistent framework to support the planning, design and implementation of network security;

— in ISO/IEC 18028-3, to define techniques for securing information flows between networks using security gateways;

— in ISO/IEC 18028-4, to define techniques for securing remote access;

— in ISO/IEC 18028-5, to define techniques for securing inter-network connections that are established using virtual private networks (VPN).

ISO/IEC 18028-1 is relevant to anyone involved in owning, operating or using a network. This includes senior managers and other non-technical managers or users, in addition to managers and administrators who have specific responsibilities for Information Security (IS) and/or network security, network operation, or who are responsible for an organization's overall security programme and security policy development.

ISO/IEC 18028-2 is relevant to all personnel who are involved in the planning, design and implementation of the architectural aspects of network security (for example IT network managers, administrators, engineers, and IT network security officers).

ISO/IEC 18028-3 is relevant to all personnel who are involved in the detailed planning, design and implementation of security gateways (for example IT network managers, administrators, engineers and IT network security officers).

ISO/IEC 18028-4 is relevant to all personnel who are involved in the detailed planning, design and implementation of remote access security (for example IT network managers, administrators, engineers, and IT network security officers).

ISO/IEC 18028-5 is relevant to all personnel who are involved in the detailed planning, design and implementation of VPN security (for example IT network managers, administrators, engineers, and IT network security officers).

Information technology — Security techniques — IT network security —

Part 3:
Securing communications between networks using security gateways

1 Scope

This part of ISO/IEC 18028 provides an overview of different techniques of security gateways, of components and of different types of security gateway architectures. It also provides guidelines for selection and configuration of security gateways.

Although Personal Firewalls make use of similar techniques, they are outside the scope of this part of ISO/IEC 18028 because they do not serve as security gateways.

The intended audiences for this part of ISO/IEC 18028 are technical and managerial personnel, e.g. IT managers, system administrators, network administrators and IT security personnel. It provides guidance in helping the user choose the right type of architecture for a security gateway which best meets their security requirements.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 18028-4:2005, *Information technology — Security techniques — IT network security — Part 4: Securing remote access*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
alert
'instant' indication that an information system and network may be under attack, or in danger because of accident, failure or people error

3.2
attacker
any person deliberately exploiting vulnerabilities in technical and non-technical security controls in order to steal or compromise information systems and networks, or to compromise availability to legitimate users of information system and network resources

3.3
audit
formal inquiry, formal examination, or verification of facts against expectations, for compliance and conformity

3.4
audit logging
gathering of data on information security events for the purpose of review and analysis, and ongoing monitoring

3.5
Demilitarised Zone
DMZ
security host or small network (also known as a screened sub-net or a perimeter network) inserted as a 'neutral zone' between networks

NOTE It forms a security buffer zone.

cf. **security host**

3.6
filtering
process of accepting or rejecting data flows through a network, according to specified criteria

3.7
firewall
type of security barrier placed between network environments – consisting of a dedicated device or of a composite of several components and techniques – through which all traffic from one network environment to another, and vice versa, traverses and only authorized traffic, as defined by the local security policy, is allowed to pass

3.8
Information Security Incident
single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

NOTE See ISO/IEC 18044.

3.9
Information Security Incident Management
formal process of responding to and dealing with information security events and incidents

NOTE See ISO/IEC 18044.

3.10
Intrusion
unauthorized access to a network or a network-connected system, i.e. deliberate or accidental unauthorized access to an information system, to include malicious activity against an information system, or unauthorized use of resources within an information system

3.11
Intrusion Detection
formal process of detecting intrusions, generally characterized by gathering knowledge about abnormal usage patterns as well as what, how, and which vulnerability has been exploited to include how and when it occurred

3.12
Intrusion Detection System
IDS
technical system that is used to identify that an intrusion has been attempted, is occurring or has occurred, and possibly to respond to intrusions in IT systems and networks

3.13
port(1)
endpoint to a connection

3.14
port(2)
⟨internet protocol⟩ logical channel endpoint of a TCP or UDP connection

NOTE Application protocols which are based on TCP or UDP have typically assigned default port numbers, e.g. port 80 for the HTTP protocol.

3.15
privacy
the right of every individual that his/her private and family life, home and correspondence are treated confidentially, without interference by an authority except where it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, the protection of health or morals, or for the protection of the rights and freedoms of others

3.16
remote access
process of accessing network resources from another network, or from a terminal device which is not permanently connected to the network it is accessing

3.17
router
network device that is used to establish and control the flow of data between different networks, which themselves can be based on different network protocols, by selecting paths or routes based upon routing protocol mechanisms and algorithms

NOTE The routing information is kept in a routing table.

3.18
security dimension
set of security controls designed to address a particular aspect of network security

NOTE The detailed description of security dimensions is given in ISO/IEC 18028-2.

3.19
security domain
set of assets and resources subject to a common security policy

3.20
security gateway
point of connection between networks, or between subgroups within networks, or between software applications within different security domains intended to protect a network according to a given security policy

NOTE A security gateway comprises more than only firewalls; the term includes routers and switches which provide the functionality of access control and optionally encryption.

3.21
spoofing
impersonating a legitimate resource or user

3.22
switch
device which provides connectivity between networked devices by means of internal switching mechanisms

NOTE 1 Switches are distinct from other local area network interconnection devices (e.g. a hub) as the technology used in switches sets up connections on a point to point basis. This ensures the network traffic is only seen by the addressed network devices and enables several connections to exist simultaneously.

NOTE 2 Switching technology can be implemented at either layer 2 or layer 3 of the OSI reference model (ISO/IEC 7498-1)

3.23
Virtual Private Network
restricted-use logical computer network that is constructed from the system resources of a physical network, e.g. by using encryption and/or by tunneling links of the virtual network across the real network

4 Abbreviated terms

API	Application Program Interface
BGP	Border Gateway Protocol
DLL	Dynamic Link Library
ICMP	Internet Control Message Protocol
IDP	Intrusion Detection Prevention
NFS	Network File Transfer
NIS	Network Information System
NNTP	Network News Transfer Protocol
NTP	Network Time Protocol
OSPF	Open Shortest Path First
RIP	Routing Information Protocol
RPC	Remote Procedure Call
SHTTP	Secure Hypertext Transfer Protocol
SOAP	Simple Object Access Protocol
S/MIME	Secure Multipurpose Internet Mail Extensions protocol
SPAN	Switched Port Analyzer
TCP-SYN	Transmission Control Protocol, SYNchronisation
V.35	high-speed synchronous data exchange protocol
WAIS	Wide Area Information Service
X.11	graphical user interface protocol
XML	Extensible Mark-up Language

5 Security requirements

A suitable security gateway arrangement should protect the organization´s internal systems and securely manage and control the traffic flowing across it, in accordance with a documented security policy.

Security gateways control access to a network (OSI model layer 2, 3, and 4), or to an application (OSI model layers 5 to 7). Examples include firewalls being used to protect:

- an internal organizational network from the Internet,
- two internal organizational networks from each other, or
- an internal organizational network from an external organisation's network.

Security gateways are used to fulfil the following security requirements:

- separate logical networks,
- provide restricting and analysing functions on the information which passes between the logical networks,
- provide means of controlling access to and from the organization´s network, by inspection of connections or by proxy operations on selected applications,
- provide a controlled and manageable single point of entry to a network,
- enforce an organization´s security policy, regarding network connections,
- provide a single point for logging,
- provide network address translation to hide internal networks,
- provide port mapping (including dynamic port opening), and application-level attack detection and protection (including content filtering).

6 Techniques for security gateways

Beginning with simple packet filtering, further technical approaches used within security gateways have evolved including such things as application proxy and stateful packet inspection. Additionally, network address translation as well as content filtering are introduced in this chapter, since these techniques are often used in combination with security gateways.

6.1 Packet filtering

Packet filtering means that network traffic is blocked or passed by comparing the information found in the header of each incoming or outgoing packet against a table of access control rules. The filtering device looks at the header of each packet individually as it enters and compares the IP address and port of the source and destination against its rule base. If the address and port information are permitted, the packet proceeds through the firewall directly to its destination. If a packet fails this test, it is dropped.

The IP packets can be checked selectively as to whether the data flow between two hosts or networks should be allowed or not. Criteria upon which the decision to allow or deny this data flow is taken can include:

- IP source address;
- IP destination address;
- Protocol (e.g., TCP, UDP, ICMP);
- Source port;
- Destination port;
- Direction of the communication (incoming, outgoing).

Packet filtering gateways are fast because they operate at the network and transport layer and make only cursory checks into the validity of a given connection.

6.2 Stateful packet inspection

Based upon packet filtering technology, the stateful packet inspection approach adds more security checks in an attempt to simulate the secure checks of an application proxy firewall. Instead of simply looking at the address of each incoming packet individually, the stateful packet inspection firewall intercepts incoming packets at the network layer until it has enough information to make some determination as to the state of the attempted connection on upper layers. These packets are then inspected in a proprietary inspection module inside the operating system kernel. State-related information required for the security decision is examined in this inspection module, then maintained in dynamic state tables for evaluating subsequent connection attempts. Packets that are cleared are then forwarded inside the firewall, allowing direct contact between the internal and external systems.

Because most of the examination occurs in the kernel, stateful packet inspection firewalls are often faster than application proxy firewalls. Although the stateful packet inspection approach has significantly enhanced the security of simple packet filtering firewalls, it will fail security checks that require collecting packets into larger units like URLs or files. Above that it must make security decisions without information of the application layer of the protocol stack in the same way that an application proxy handles this.

Packet filters with stateful inspection still allow external users direct access to business applications and systems that may very well have poorly configured operating systems with well-known security vulnerabilities. Application proxies mask these same vulnerabilities by limiting the access to an application or a computer system to a finite set of identifiable tasks within the proxy itself.

6.3 Application proxy

The application proxy approach offers superior security control because it provides application-level awareness of attempted connections by examining everything at the highest layer of the protocol stack. Because it has full visibility at the application layer, an application proxy service can easily see the granular details of each attempted connection up front and implement security policies accordingly. Application proxy services also feature a built-in proxy function – terminating the client connection at the application gateway and initiating a new connection to the internal protected network. The proxy mechanism provides added security because it separates the external and internal systems and makes it more difficult for hackers on the outside to exploit vulnerabilities on systems inside.

Secure gateways using the application proxies provide the strongest security with the only drawback being that the added security can negatively impact the performance. Furthermore, for new services it often takes time before the proxy for this service becomes available.

6.4 Network Address Translation (NAT)

One of the features that Network Address Translation (NAT) technology provides is to enable the “hiding” of the network-addressing schema behind a firewall environment. With network address translation, the IP address of a system on the internal network is mapped to a different corresponding external, routable IP address. It is also possible that many systems behind a firewall share the same external IP address. Resources behind a firewall are still accessible to external users by forwarding inbound connections on certain port numbers.

Network address translation can be implemented on most network devices (switches, routers as well as bastion hosts or firewalls).

6.5 Content analyzing and filtering

Security gateways with application level proxies often implement content analyzing and filtering too. Content filtering comprises the protection against malicious code (like viruses, worms and Trojan horses) and also mobile code (like Java, JavaScript, ActiveX, or any other executable code) which can cause damage to networks, applications, and data.

As most of this malicious code is distributed over the Internet via email or HTTP-based communication (e.g. downloads from a web site or a FTP site), the protection should start at the point where the security gateway interfaces to the Internet. Therefore a virus scanner or more generally, a content scanner is added to the screened subnet or the demilitarized zone (DMZ). In most of the installations, the content scanner is linked directly to the firewall with a network interface so that the SMTP-based email traffic and the HTTP-based communication is routed to the content filtering scanner.

The predominant technologies for content analyzing are as follows:

- Signature-based scanning (searching for known patterns);
- Investigative analysis (analyzing code for functions and behavior known to be associated with malicious code)
- Sandbox technology (essentially a content monitoring program, which quarantines suspect code in a “sandbox”).

As the difference between content scanning and intrusion detection is small, especially regarding network-based intrusion detection, an intrusion detection system (IDS) can also be combined with the firewall by implementing an IDS agent on the firewall device. See ISO/IEC TR 15947:2002, *Information technology — Security techniques — IT intrusion detection framework.*

NOTE Selection, deployment and operations of intrusion detection systems will form the subject of a future International Standard (ISO/IEC 18043).

Content filtering technology also has some limitations. If data is encrypted on the transport or application layer (e.g., SSL/TLS or S/MIME), content screening is no longer possible unless the encrypted data are decrypted and re-encrypted again on the firewall. N.B. this could pose security threats such as “man in the middle” attacks.

There are legal implications regarding content scanning and filtering, especially where a strong data protection legislation is required. In such a scenario, only automatic scanning for malicious code is allowed, but not the scanning for specific content of an email because this would influence the privacy of the sender and of the recipient.

7 Security gateway components

The section provides an overview of four distinct categories of security gateways by component, e.g., switches, routers, and firewalls.

7.1 Switches

Switches are used to allow high-speed communications delivering full network bandwidth to each physical port. Generally switches are layer 2 devices which are extensively used to segment local area networks. Further, they can provide subnet isolation when VLAN techniques are implemented.

Through the use of access control lists (ACLs) applied to different OSI model layers 2, 3 and 4, the traffic between a switch and the nodes connected to that switch can be controlled. Access control functionality provided by switches makes them useful for inclusion as components of security gateway architectures, especially for the implementation and structuring of any screened subnets’ respective demilitarized zones.

Switches used in a security gateway environment should not be connected directly to a public network, due to various threats, e.g., denial-of service-like attacks that can cause the exposed switch to flood connected networks with packets.

7.2 Routers

Routers are normally designed to connect different networks by supporting multiple network protocols and to optimize the network traffic and the routes between communicating hosts. In addition, routers can be used as components for security gateways as they are able to filter the respective data communication data packets based on packet filtering techniques.

A router that utilizes this checking of packet information to control network traffic is often referred to as a screening router (see 8.1.1). Routers normally work on the layer 3 of the OSI model, the network layer, where only a control of the low level information of the data packets is possible in so far that no check of the user data is performed.

Routers can perform NAT and packet filtering.

7.3 Application Level Gateway

An application level gateway is a hardware and software based device or set of devices. Application level gateways are specifically designed to restrict access between two separate networks.

Primarily two techniques are used for implementing application level gateways:

- Stateful Packet Inspection;
- Application Proxy.

Combinations and variations (e.g., circuit-level firewalls) of these techniques may also be used. In addition NAT can be performed by application level gateways.

7.4 Security Appliances

Network devices (routers, switches, modems etc.) equipped with hardened operating systems, all dedicated to security purposes are called Security Appliances. These devices can be a base for security software (firewall, IDS/IDP, anti-virus protection etc).

Security appliances are offered on a wide range of platforms to meet diverse security needs, from the smallest remote locations to large corporate networks, and data centres as well. Appliances dedicated to protect remote locations or single computers are called Personal Firewall Appliances although they may include other security functions, e.g. anti-virus protection.

All techniques mentioned in Clause 6 can be implemented by using security appliances.

8 Security Gateway Architectures

To adequately protect an internal network from exposure to attacks from external networks, such as the Internet, an effective architecture for a security gateway should be selected.

Two different approaches can be considered in creating security gateways, the structured and the staged approach.

The structured approach is based on network design principles and security options set by the Internet protocol. The staged approach relates to security domains and safeguards to be implemented on the domains' perimeters in accordance with the security requirements defined in an organization's security policy.

Both approaches are discussed below.

8.1 Structured approach

The structured approach can be implemented by four different architectures, driven by the different specific security needs a company may have. These are:

- Packet filter firewall;
- Dual-homed gateway;
- Screened host;
- Screened subnet.

The protection should include safeguards against malicious code, viruses, crackers, denial of service attacks, and other unauthorized activities.

8.1.1 Packet filter firewall architecture

The most basic type of firewall architecture is called a packet filter. Packet filter firewalls are essentially routing devices that include access control functionality for system addresses and communication sessions. They are often referred to as screening routers. In their most basic form, packet filters operate at layer 3 of the OSI model.

The access control functionality of a packet filter firewall is governed by a set of directives collectively referred to as a rule set. They provide network access control and can for example, be based upon the source address of a packet, the destination address of a packet, the type of traffic, some characteristics of the layer 4 communication sessions, such as source and destination ports of the session, as well as (sometimes) information pertaining to which interface of the router the packet came from and which interface of the router the packet is destined for.

Packet filter firewalls have two main strengths: These are speed and flexibility. Since packet filters do not usually examine data above layer 3 of the OSI model, they can operate very quickly. The simplicity allows packet filter firewalls to be deployed as an exterior router in front of a screened host or screened subnet. The reason for this placement is their capability to block denial of service and related attacks as well.

Screening routers cannot prevent attacks that employ application specific vulnerabilities or functions because they do not examine upper-layer data (layer 5 – 7). Because of the limited information available to the firewall, the logging functionality in packet filter firewalls is also limited. Due to the large numbers of variables used in access control decisions, they are susceptible to security breaches caused by improper configurations.

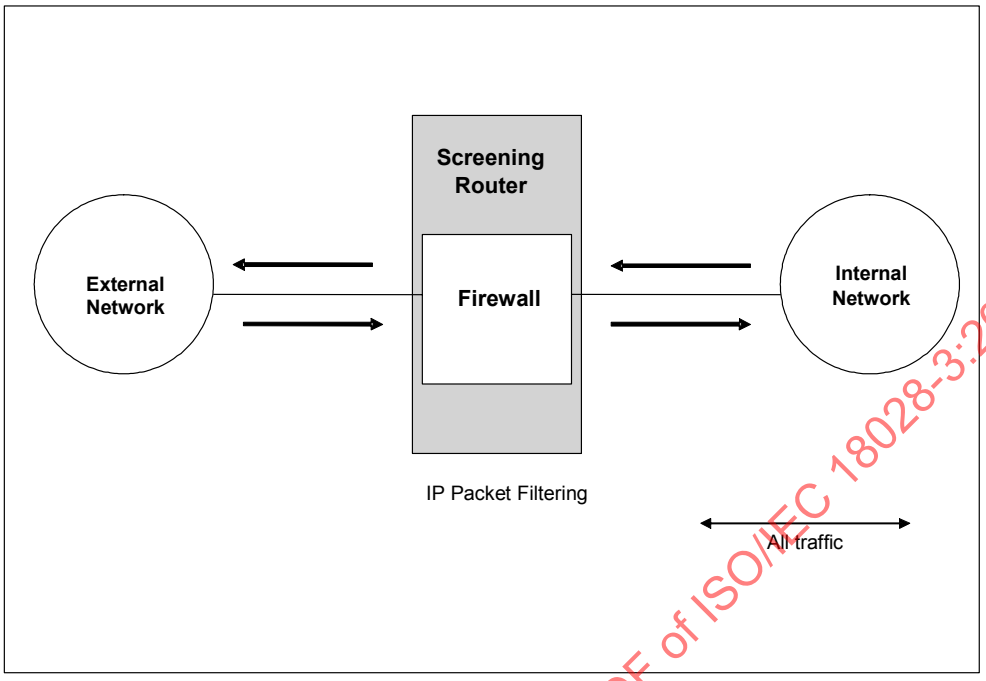

Figure 1 — Packet filter firewall/screening router

8.1.2 Dual-homed gateway architecture

The dual-homed gateway consists of a host system with two network interfaces A and B, and with the host's IP forwarding capability disabled. Thus, IP packets from one network (e.g., the Internet) are not directly routed to the other network (e.g., internal network). Systems of the internal network can communicate with the dual-homed host, and systems outside the firewall on external networks can communicate with the dual-homed host, but these systems cannot communicate directly with each other.

There are variations of this configuration if the host is equipped with several network cards, e.g., to the Internet for separate connections to Internet service providers, or to the internal network to different servers such as email servers or log servers. In this case it is referred to as a multi-homed gateway.

Optionally, a router can be placed at the connection to external networks to provide additional protection by filtering network packets. The dual-homed gateway blocks all direct IP traffic between external networks and the protected site. Service and access is provided by proxy services on the application level on the firewall.

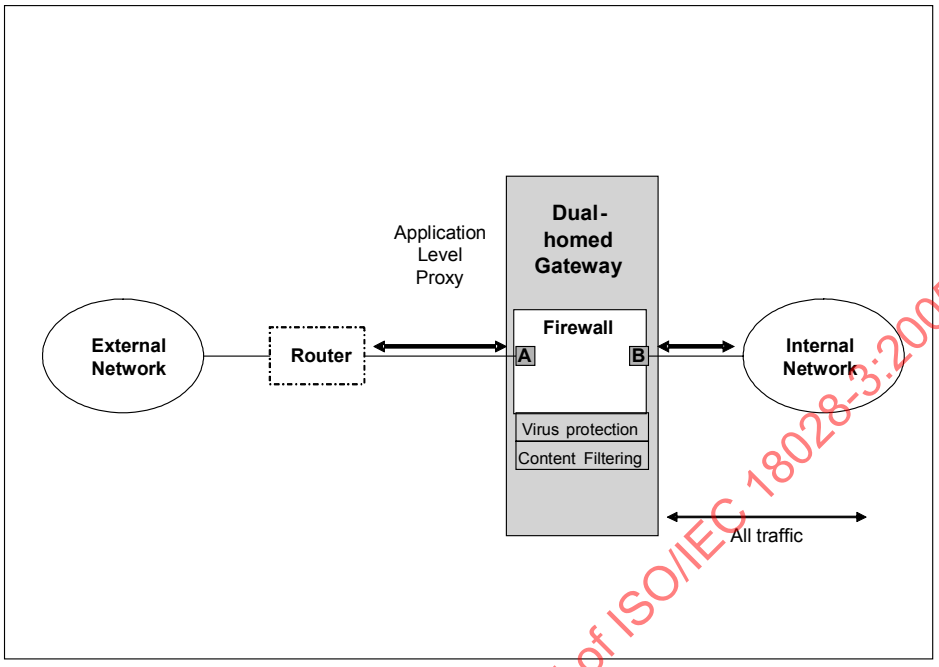

Figure 2 — Dual-homed gateway

The dual-homed gateway represents a more qualified type of security gateway because it hides internal IP addresses from systems of external networks and it provides logging capability which can be used in conjunction with an Intrusion Detection System (IDS) to detect possible intruder activities. The limited flexibility – only such services can be passed for which proxy services exist – could be a disadvantage to some sites. An additional router can solve this problem if in this case a trusted communication can be established as a by-pass to the security gateway. The security of the host system used for the firewall is crucial for the whole protection because if the firewall is compromised an intruder could gain access to the internal systems.

8.1.3 Screened host architecture

The screened host architecture combines a packet filtering router with a bastion host using application proxies. The bastion host is placed on the protected subnet side of the router. In this architecture, the primary security is provided by a packet filtering router, e.g., to prevent people from going around proxy servers to establish direct connections to the internal network.

The packet filtering on the screening router is set up in such a way that the bastion host is the only system that hosts of external networks can open connections to. Such a bastion host as an application-level firewall consists of proxy services that pass or block the services according to the site's policy. The router filters inherently dangerous protocols from reaching the firewall and site systems.

Application traffic from external networks to the bastion host gets routed; all other traffic from external sites gets rejected. The router rejects any application traffic originating from internal networks unless it came from the bastion host.

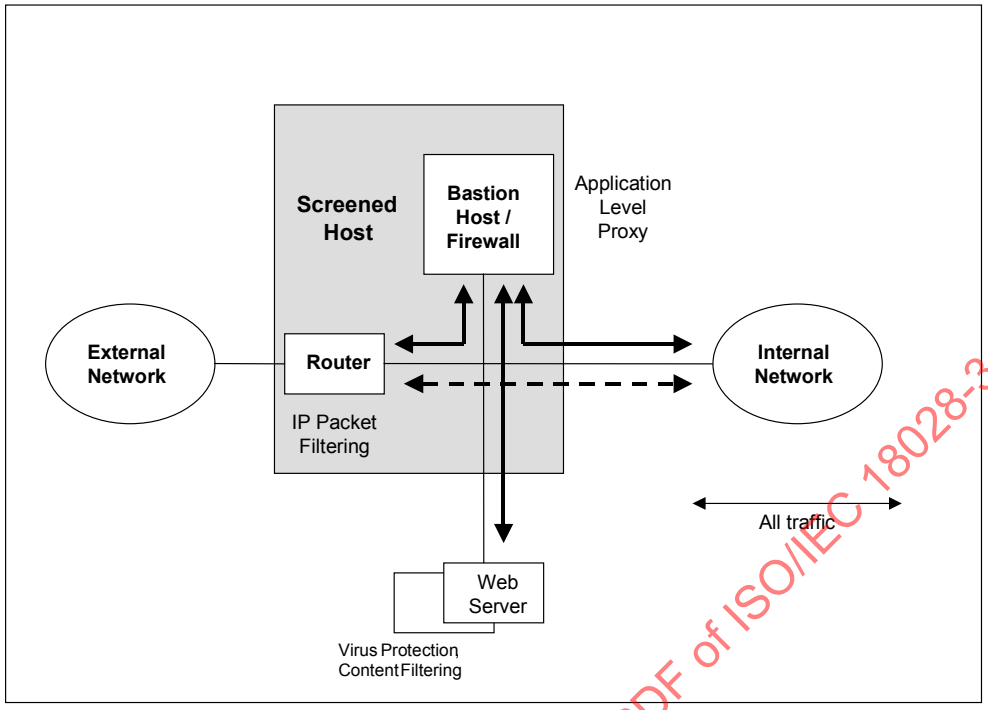

Figure 3 — Screened host

This architecture is more flexible because the bastion host needs only one network interface and does not require a separate subnet between the bastion host and the router. Furthermore, the router can pass trusted services "around" the bastion host directly to internal systems.

This flexibility can be interpreted as being less secure overall because it is easier to violate the established security policy. The major disadvantage is that if an attacker manages to break in to the bastion host, there is nothing left in the way of network security between the bastion host and the internal network. The router also presents a single point of failure; if the router is compromised, the entire network is available for an attacker. Another disadvantage is that you have two systems, which have to be configured carefully. The packet filtering rules of the router can get very complex and difficult to maintain.

8.1.4 Screened subnet architecture

The screened subnet architecture is a variation of the dual-homed gateway and screened host architectures. It adds an extra layer of protection to the screened host architecture by adding a perimeter network that further isolates the internal network from external networks like the Internet.

Two routers are used to create an inner, screened subnet. This subnet, sometimes referred to as the demilitarized zone (DMZ) or a perimeter network, houses the bastion host or application-level firewall, however, it could also house web server(s), email server(s) or DNS server(s) and other systems that require carefully controlled access. The external router restricts access from external networks to specific systems on the screened subnet (e.g., routing e-mail traffic from Internet sites to the e-mail server), and blocks all other traffic to external networks originating from systems that should not be originating connections (e.g., NFS mounts to external systems). The interior router passes traffic to and from systems on the screened subnet according to existing rules (e.g., routing e-mail traffic from site systems to the e-mail server and vice versa).

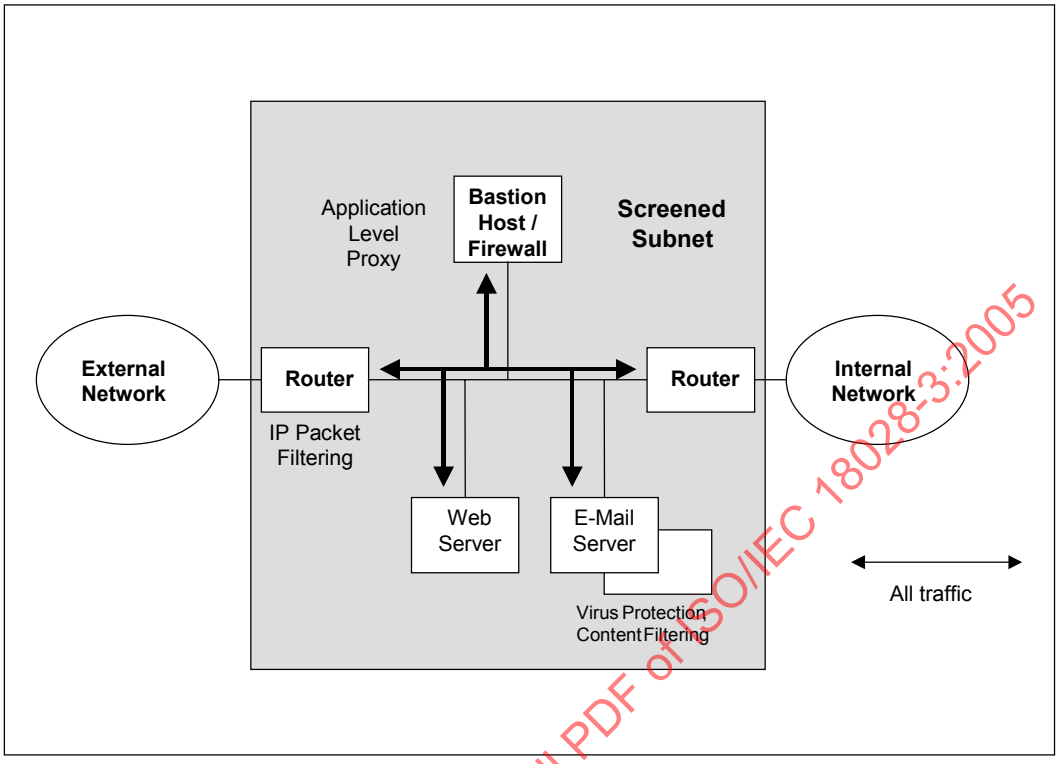

Figure 4 — Screened subnet

It is important with the dual-homed and often also the multi-homed gateway, that no internal system is directly reachable from external networks and vice versa. With the screened subnet architecture, there is no absolute necessity for implementing the application-level gateway's respective bastion host as a dual-homed system.

The screened subnet architecture may be more appropriate for sites with large amounts of traffic or sites that need very high-speed traffic.

8.2 Staged approach

A protection stage comprises different security dimensions of the security domain covering the security requirements. For example, a password prompt from an operating system is a protection stage for access control. External users can access the security domain if authenticated properly on the protection stage with a valid ID and password. If the authentication mechanism is strong enough to meet the access authentication requirement, it can be implemented to protect the domain from unauthorized access.

Requirements of protection stages can be expressed in terms of confidentiality, integrity, availability, accountability, authenticity and reliability of critical data and services placed in the security domain. A protection stage can be comprised of security controls such as:

a) authentication,
b) packet filtering,
c) intrusion detection,
d) logging.

Protection stages can be implemented separately in different devices, or can be grouped if possible in one or more devices. This is the point where structured and staged approaches meet each other, e.g. if all stages can be placed in one device, the packet filtering or dual-homed gateway architecture can be formed.

This approach creates Defence in Depth through implementation of many protection stages placed where they are needed and providing sufficient security controls to satisfy security requirements of protected security domains.

8.2.1 Single and multi-staged security gateway architecture

Single stage architecture is the simplest staged approach. It can be applied if only one security requirement is to be met e.g. user authentication before access to the domain. Typically the router is then implemented performing only one security task – user authentication.

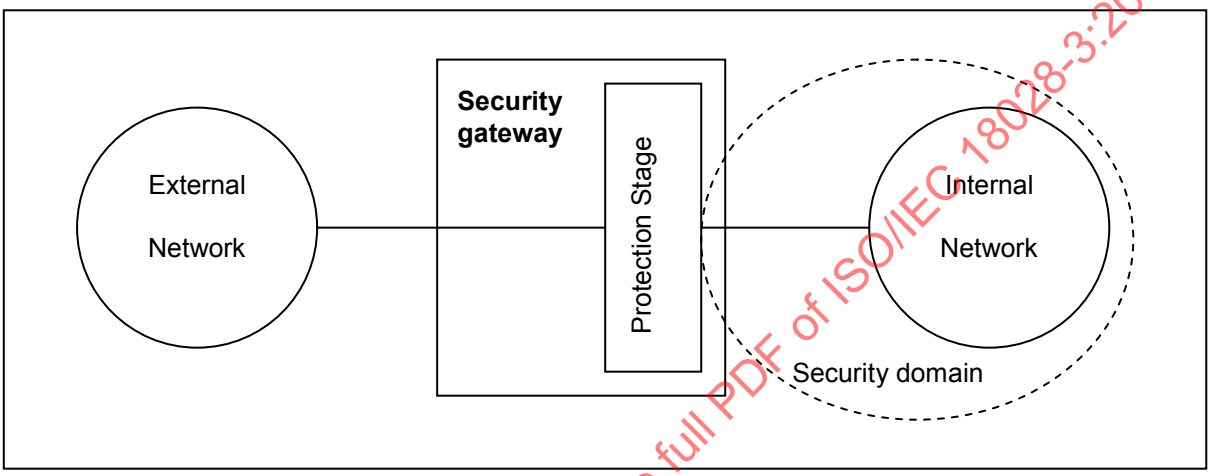

Figure 5 — Single stage security gateway

Usually the security domain should fulfil more security requirements, and the security gateway becomes more complex, e.g. a specified set of protocols is allowed and authentication before access to the domain is to be performed. In that case two security stages are needed – packet filtering stage and authentication stage. Both can be implemented with a router performing packet filtering and authentication.

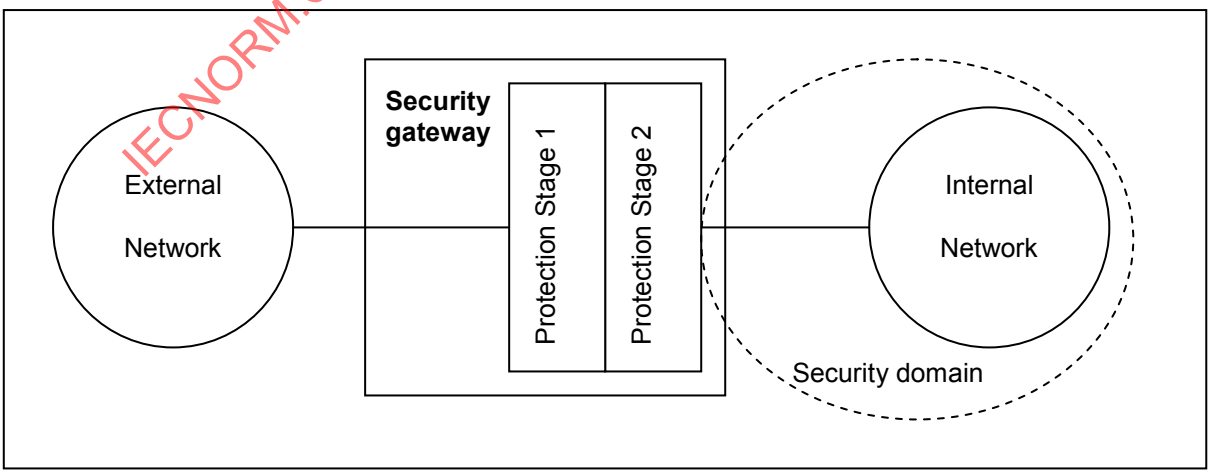

Figure 6 — Multi-staged security gateway

Most organizations have more than one security domain in their networks. If there is another domain in the organization with similar security requirements it may happen that the security gateway can protect both domains simultaneously. In that case a Demilitarized Zone (DMZ) or a perimeter network can be formed. If the security policy of the first domain allows the traffic to pass through the second domain, the DMZ is similar to a DMZ in a screened subnet architecture (see Figure 7).

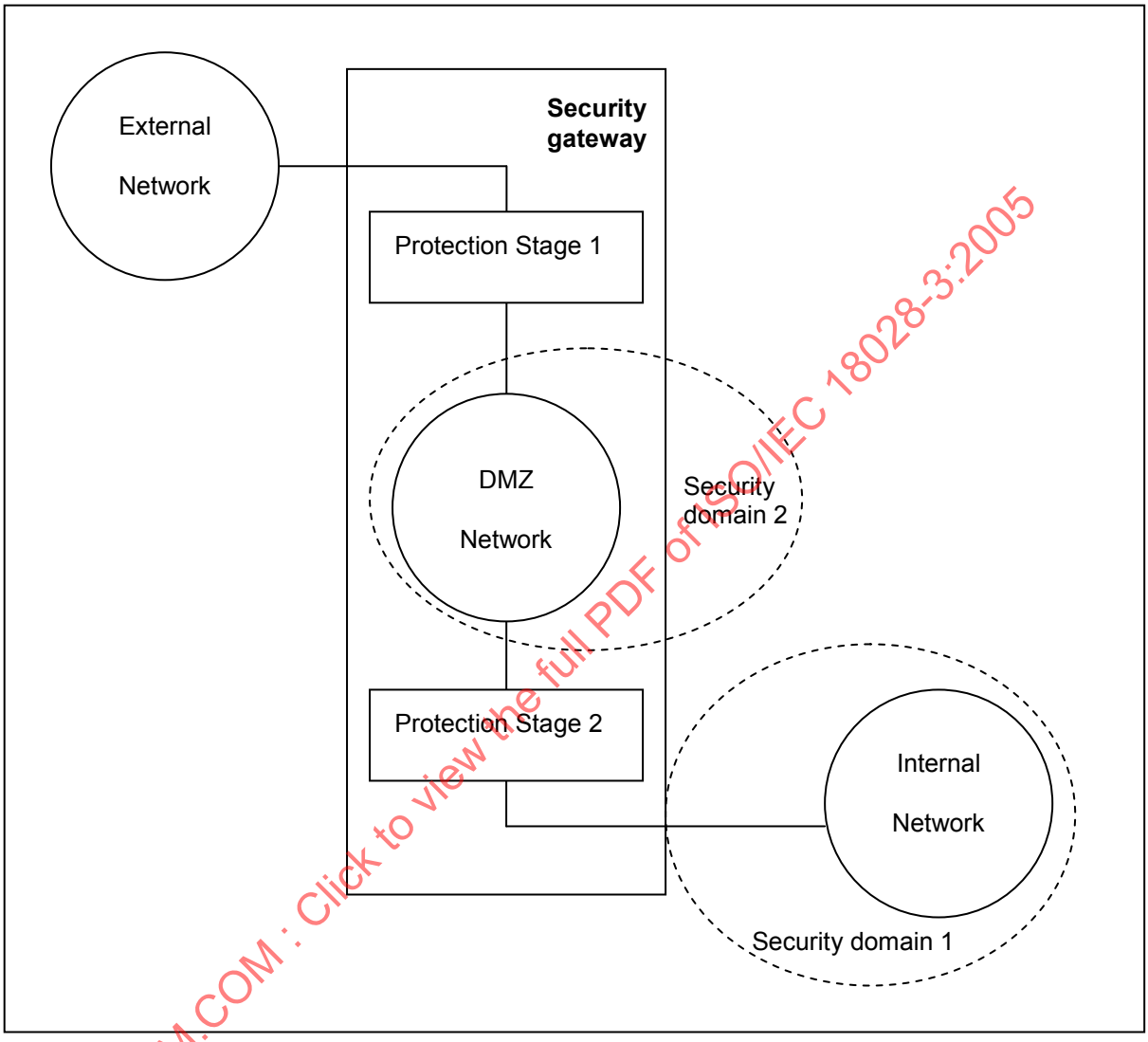

Figure 7 — DMZ in multi-staged security gateway

If the security policy of the first domain does not allow its traffic to pass through any other domain and the external stage can provide independent connection for the second domain, then this DMZ is called a Service Leg DMZ (see Figure 8).

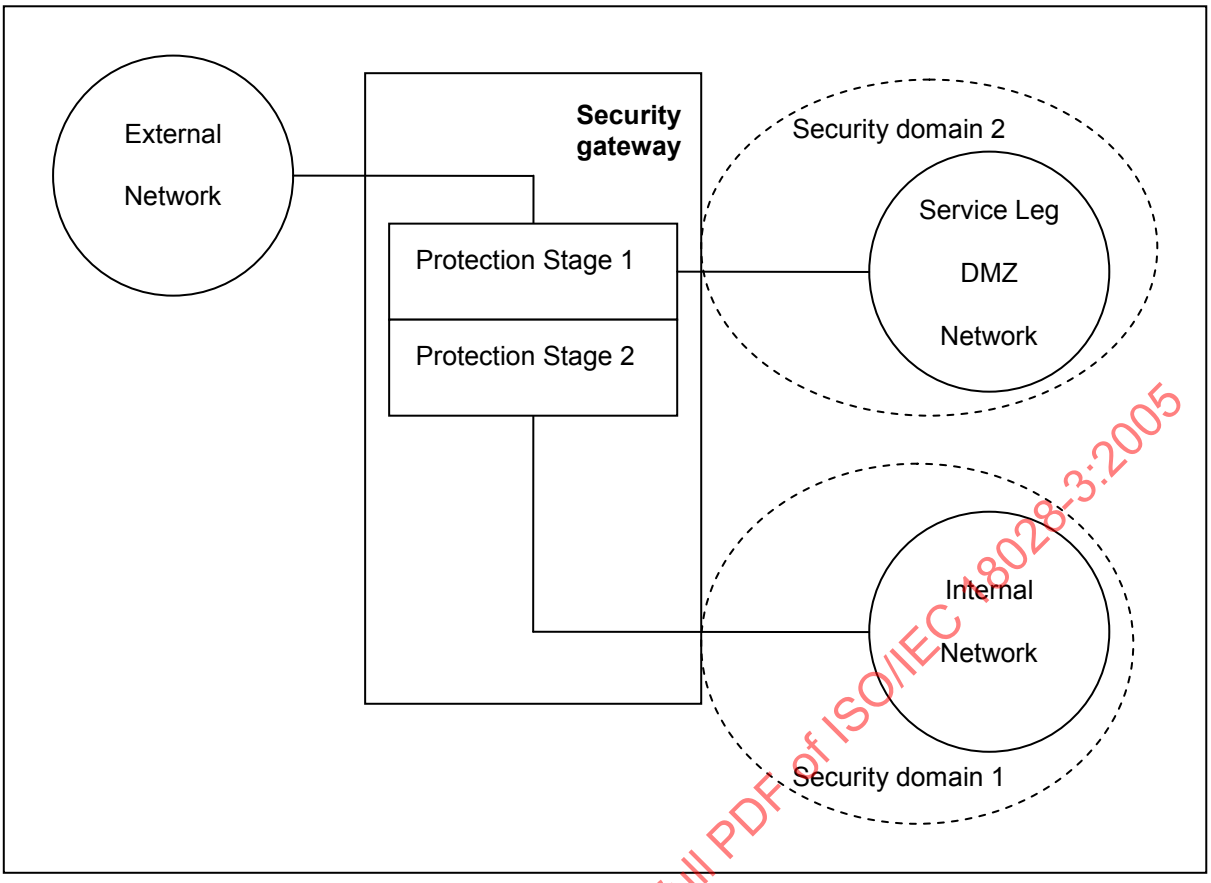

Figure 8 — Service Leg DMZ in multi-staged security gateway

9 Guidelines for selection and configuration

To ensure that the requirements as outlined in Clause 5 are fulfilled a structured approach for selecting and configuration of security gateways is necessary. This clause does give some guidance for this process, particularly in the areas of

- Selecting an security gateway architecture and appropriate components
- Selecting hardware and software platform
- Configuration
- Security features and settings
- Administration
- Logging
- Documentation
- Audit
- Training/Education

As a general guidance for the following four principles should be followed:

- Pay attention to all possible threats, which especially includes internal threats
- Pay attention to the human factor, e.g. in the areas of administration and education
- Keep it as simple as possible, although higher security requirements do typically also imply more complex architectures;
- Use components or devices in their designated functionality and configuration

9.1 Selection of a security gateway architecture and appropriate components

Based on the business and security requirements for the security gateway (see Clause 5 for further reference) an appropriate security gateway architecture should be selected and adapted (see Clause 8 for an overview of possible security gateway architectures).

NOTE Network security management will form the subject of a future International Standard (ISO/IEC 18028-1)

Once an architecture is defined, each components of this architecture needs to be further specified and their functionality need to be evaluated, refer to Clause 8 for an overview of possible components and to Clause 7 for a detailed description of the provided functions.

The following clauses do provide some further guidance on the selection for the right components with appropriate architecture.

9.2 Hardware and software platform

While selecting a hardware platform the performance, efficiency, reliability and applicability should be considered especially, e.g. if the platform has only Ethernet interfaces but Frame Relay on V.35 is required, then this platform is unusable.

Next the operating system of the hardware device should be looked at. For security purposes a hardened operating system should be used. It is also recommended to check it against known vulnerabilities. The software platform also needs to be verified according to its performance and reliability, e.g. a router with 10BaseT Ethernet interface cannot provide gigabit throughput.

9.3 Configuration

The following recommended settings for security gateway network devices should be considered during the configuration process:

- Switched network for the screened subnet architecture respective for the demilitarized zone;
- Static routing between the router(s) and the security gateway;
- Source routing information should not be accepted;
- Only software/programs on the security gateway, which are absolutely necessary for the operation ("platform hardening"), should be installed.
- Definition of rules in the case of packet filtering with the possibility to define that all that is not explicitly allowed is forbidden;
- Ensure ports are not enabled by default;
- Ensure SPAN ports are not enabled unless the use of intrusion detection systems is needed;
- Ensure passwords are implemented on device interfaces;
- Rejection of the RIP message "Loose-source-routing";
- Capability of network address translation as appropriate;
- Transparent operation of the security gateway;
- Access control on the security gateway (identification, authentication);
- In the case of a crash of the security gateway only administrative tasks should still be possible;
- Platform hardening regarding the operating system.

9.4 Security features and settings

As a minimum an application proxy should be able to:

- Support of the main Internet services (HTTP, FTP, Telnet, SMTP, NNTP);
- Support of further Internet services;
- Support of generic proxies (for new protocols or services);
- The HTTP proxy should be able to handle SHTTP correctly;
- Rejection of the BGP message ”notification” (e.g., by a generic proxy);
- Support of dynamic routing protocols;
- Support of web services (e.g., SOAP/XML);
- Support of proxies for packaged enterprise applications or other business applications;
- Possibility of allowing, denying, or dropping connections or packets.

As a minimum a packet filtering device should be able to:

- Support of the services NFS, NIS, RPC, RIP, OSPF, DNS, WAIS by an adequate protection through dynamic packet filters;
- Support packet filtering on the basis of:
  - IP source and destination address;
  - Source and destination port (for TCP, UDP);
  - Direction of the connection (inbound, outbound).
- Preserve filtering rules as inherently consistent;
- Filter packets for each network interface separately;
- Support of multicast packets if device clustering is needed;
- Preserve the order of the filtering rules by the security gateway;
- Detect denial-of-service attacks (e.g., TCP-SYN flooding);
- Prevent TCP sequence number guessing;
- Limit the length of the fragments of IP packets and define a minimum fragment offset;
- Re-assembling IP packets;
- Filter the ICMP messages ”destination unreachable” and ”redirect”;
- Resist ping-of-death attacks (a kind of denial of service attack);
- Prevent IP spoofing, that means internal IP addresses are refused if they come from the Internet;
- Couple usage of FTP commands with specific access rights;
- Enable context information to be stored, e.g. to check dynamically allocated port numbers;