INTERNATIONAL STANDARD

ISO/IEC 27033-4

First edition
2014-03-01

Information technology — Security techniques — Network security —

Part 4: Securing communications between networks using security gateways

Technologies de l'information — Techniques de sécurité - Sécurité de réseau —

Partie 4: Sécurisation des communications entre réseaux en utilisant des portails de sécurité

Reference number
ISO/IEC 27033-4:2014(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 27033-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This first edition of ISO/IEC 27033-4 cancels and replaces ISO/IEC 18028-3:2005, which has been technically revised.

ISO/IEC 27033 consists of the following parts, under the general title *Information technology — Security techniques — Network security*:

— *Part 1: Overview and concepts*

— *Part 2: Guidelines for the design and implementation of network security*

— *Part 3: Reference networking scenarios – Threats, design techniques and control issues*

— *Part 4: Securing communications between networks using security gateways*

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

— *Part 6: Securing wireless IP network access*

(Note that there may be other Parts. Examples of possible topics to be covered by Parts include local area networks, wide area networks, broadband networks, web hosting, Internet email, and routed access to third party organizations. The main clauses of all such Parts should be Risks, Design Techniques and Control Issues.)

Introduction

The majority of both commercial and government organizations have their information systems connected by networks, with the network connections being one or more of the following:

— within the organization.

— between different organizations.

— between the organization and the general public.

Further, with the rapid developments in publicly available network technology (in particular with the Internet) offering significant business opportunities, organizations are increasingly conducting electronic business on a global scale and providing online public services. The opportunities include the provision of lower cost data communications, using the Internet simply as a global connection medium, through to more sophisticated services provided by Internet Service Providers (ISPs). This can mean the use of relatively low cost local attachment points at each end of a circuit to full scale online electronic trading and service delivery systems, using web-based applications and services. Further, the new technology (including the integration of data, voice and video) increases the opportunities for remote working (also known as teleworking or telecommuting). Telecommuters are able to keep in contact through the use of remote facilities to access organization and community networks and related business support information and services.

However, while this environment does facilitate significant business benefits, there are new security threats to be managed. With organizations relying heavily on the use of information and associated networks to conduct their business, the loss of confidentiality, integrity, and availability of information and services could have significant adverse impacts on business operations. Thus, there is a major need to properly protect networks and their related information systems and information. In other words, implementing and maintaining adequate network security is critical to the success of any organization's business operations.

In this context, the telecommunications and information technology industries are seeking cost-effective comprehensive security solutions, aimed at protecting networks against malicious attacks and inadvertent incorrect actions, thereby meeting the business requirements for confidentiality, integrity, and availability of information and services. Securing a network is also essential to achieve accurate billing for network usage. 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 security solution.

The purpose of ISO/IEC 27033-4, Securing communications between networks using security gateways, is to provide guidance on how to identify and analyse network security threats associated with security gateways, define the network security requirements for security gateways based on threat analysis, introduce design techniques to achieve a network technical security architecture to address the threats and control aspects associated with typical network scenarios, and address the issues associated with implementing, operating, monitoring and reviewing network security controls with security gateways.

It is emphasized that the ISO/IEC 27033-4 is relevant to all personnel who are involved in the detailed planning, design and implementation of security gateways (for example network architects and designers, network managers, and network security officers).

Information technology — Security techniques — Network security —

Part 4: Securing communications between networks using security gateways

1 Scope

This part of ISO/IEC 27033 gives guidance for securing communications between networks using security gateways (firewall, application firewall, Intrusion Protection System, etc.) in accordance with a documented information security policy of the security gateways, including:

a) identifying and analysing network security threats associated with security gateways;

b) defining network security requirements for security gateways based on threat analysis;

c) using techniques for design and implementation to address the threats and control aspects associated with typical network scenarios; and

d) addressing issues associated with implementing, operating, monitoring and reviewing network security gateway controls.

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 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27033-1 and the following apply.

3.1
bastion host
specific host with hardened operation system that is used to intercept packets entering or leaving a network and the system that any outsider must normally connect with to access a service or a system that lies within an organization's firewall

3.2
end-point software-based firewall
software application running on a single machine, protecting network traffic into and out of that machine to permit or deny communications based on an end user-defined security policy

3.3
hardened operating system
operating system which has been configured or designed specifically to minimize the potential for comprise or attack

Note 1 to entry: This may be a general OS, such as Linux, which has been configured for this environment or may be a more custom built solution.

3.4
Internet gateway
entry point to access the internet

3.5
packet
entity comprising a well-defined block of bytes consisting of 'header', 'data' and optional 'trailer' which can be transmitted across networks or over telephone lines

Note 1 to entry: The format of a packet depends on the protocol that created it. Various communications standards and protocols use special purpose packets to monitor and control a communications session. For example the X.25 standard uses diagnostic, call clear and reset packets (among others), as well as data packets (or) a unit of data that is transmitted over the network.

3.6
perimeter network
physical or logical subnetwork that contains and exposes an organization's external services to a public network

3.7
remote office
branch office
office externally connected to the organization's main office through remote networks to provide users with services (e.g. file, print and the other service) required to maintain their daily business routine

3.8
single point of failure
type of failure that if a part of a system fails, the entire system does not work

3.9
SIP gateway
perimeter device that sits between the internal VoIP network and an external network such as the public telephone network

Note 1 to entry: Often a router is used to perform the role. Where VoIP is in use to external IP networks it is important to ensure that the gateway contains sufficient security measures especially dynamic rule base changes to all call setup to take place securely.

4 Abbreviated terms

ACL	Access Control List
API	Application Programming Interface
ASIC	Application Specific Integrated Circuit
BGP	Border Gateway Protocol
CPU	Central Processing Unit
DDoS	Distributed Denial-of-Service

DLL	Dynamic Link Library
DMZ	Demilitarized Zone
DNS	Domain Name Server
DoS	Denial-of-Service
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
ISP	Internet Service Provider
MIME	Multipurpose Internet Mail Extensions
NAT	Network Address Translation
NFS	Network File System
NIS	Network Information System
NNTP	Network News Transport Protocol
NTP	Network Time Protocol
OS	Operating System
OSI	Open System Interconnection
OSPF	Open Shortest Path First
RIP	Routing Information Protocol
RPC	Remote Procedure Call
SIP	Session Initiation Protocol
SMS	Short Message Service
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SPA	Switched Port Analyzer
SPOF	Single Point Of Failure
SQL	Structured Query Language

SSL	Secure Sockets Layer protocol
SYN	Synchronous
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAIS	Wide-area Information Servers or Service
WLAN	Wireless Local Area Network
XML	Extensible Markup Language

5 Structure

The structure of ISO/IEC 27033-4 comprises:

— an overview of security gateway (see Clause 6);

— security threats associated with security gateway (see Clause 7);

— security requirements based on an analysis for security gateways (see Clause 8);

— security controls associated with typical network scenarios and network technology areas using security gateway (see Clause 9);

— various design techniques for security gateways (see Clause 10); and

— guidelines for product selection (see Clause 11).

6 Overview

A security gateway is placed at the boundary between two or more network segments, for example, between the organization's internal network and a public network, to filter the traffic flowing across the boundary in accordance with the documented security gateway service access policy for that boundary. Another use of security gateways is to separate segments of the network when using services that may have multiple tenants, for example when using cloud services a security gateway would protect an organization's information by applying the organization's security policy.

An example network environment is shown in Figure 1 below which is only for illustrative purposes in this overview. The DMZ, referred to as a perimeter network, is a physical or logical subnetwork that contains and exposes an organization's external services to a public network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's internal network; an external attacker only has access to services in the DMZ, rather than any other part of the internal network. All external connections to services should terminate inside the DMZ and DMZ systems should have little or no access to internal systems. Designing a network in this way does not eliminate the risk of an internal network compromise, it merely makes it more difficult. Any intruder which can subvert a service inside a perimeter network may then have the opportunity to identify another vulnerability

which could allow access to the internal network. For this reason, amongst others, the internal network should still be made as secure as possible.

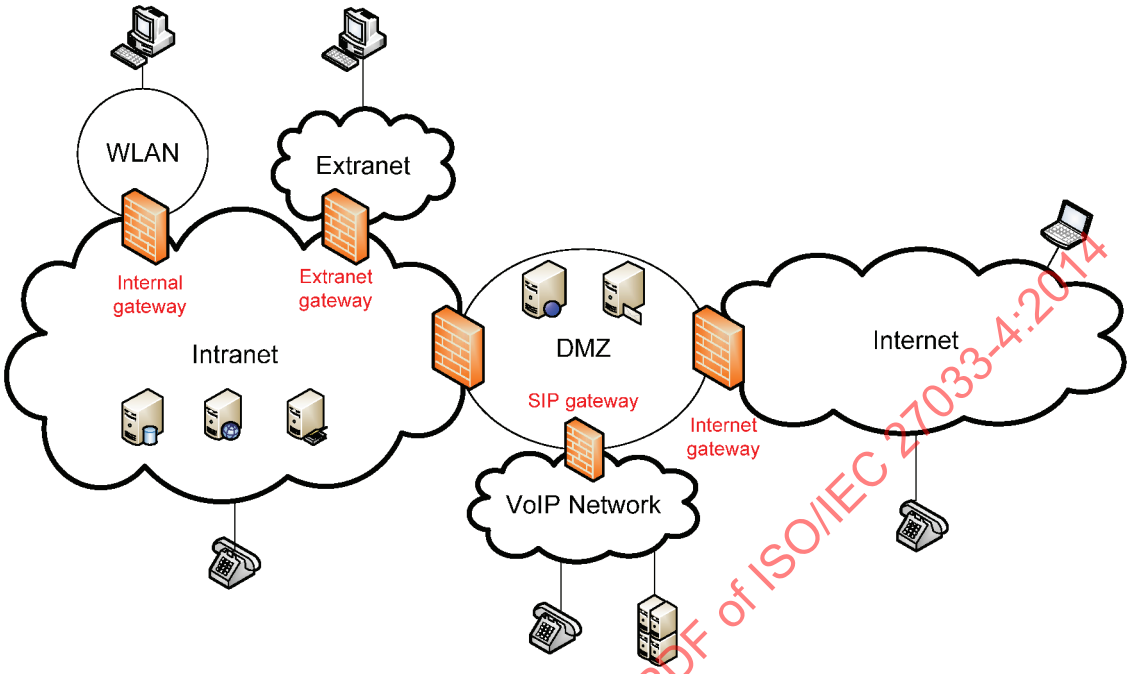

Figure 1 — Example Network Environment

Most organizations may have multiple "zones" or DMZ areas for web, application and database layers and for meeting some compliance/regulatory requirements.

The "hybrid" solutions now exist which incorporate multiple areas of functionality. Many packet filtering firewalls now have proxies for certain services and include more controls for context such as role, time of day, etc.

The Intranet owned by the organization is managed and maintained by those authorized by the organization. An organization of any significant size should have separate network segments between which internal security gateways will control the traffic flow. Separate infrastructure may be used for special purposes within the Intranet. For instance, if a WLAN is used as part of the intranet, it should be isolated and require further authentication as it introduces additional risks. The internal security gateway can be used to protect the organization's assets against attacks from this segmentation.

The organization communicates and exchanges data with trusted third parties in a way extending the Intranet towards the network of the partner's network through the so-called Extranet. The extranet security gateway can be used to address the threats induced from this extension. When using services such as cloud computing the security gateway is used to restrict access and apply an organization's security policy to logical networks. The business of the organization necessitates communications and data exchange with business partners, customers, and general public through the public network, of which the Internet is the most common example. Since trust level of the public network is relatively low, security gateways, so called Internet gateways, are needed to address risks induced from the public network.

7 Security threats

For the foreseeable future, organizations can expect increasingly sophisticated attacks to be mounted against their systems. Attempts at unauthorized access can be malicious, for example, leading to a Denial-of-Service (DoS) attack, the misuse of resources, or the unauthorized access to valuable information. Organizations should protect their internal network or assets from various threats, such as intentional

misuse of the assets, misconfiguration of the systems, unauthorized traffic transversal from different trusted domains within the organization, or other threats from Internet application services.

The security gateway needs to protect the organization from intrusions from unauthorized users accessing the network from the internal network, the Internet, or third party networks. Unmonitored content leaving the organization may introduce legal issues and a potential loss of intellectual property. In addition, as more organizations are connecting to the Internet to meet their organizational requirements, they are faced with the need to control access to inappropriate or objectionable websites or web applications and services. Without control, organizations face the threat of productivity losses, liability exposure and misallocation of bandwidth due to non-productive web surfing. Thus, the key security threats to be addressed include those associated with:

— Denial-of-Service to authorized users;

— unauthorized modification of data;

— unauthorized disclosure of data;

— unauthorized system re-configuration;

— unauthorized use of resources and assets of organization;

— unauthorized transversal of content e.g. virus and malware;

— violation of virtualization; and

— Denial-of-Service and Distributed Denial-of-Service attack against security gateway.

8 Security requirements

Security gateways control access to a network (OSI model layer 2, 3, and 4), or to an application (OSI model layers 5 to 7) depicted in Figure 2.

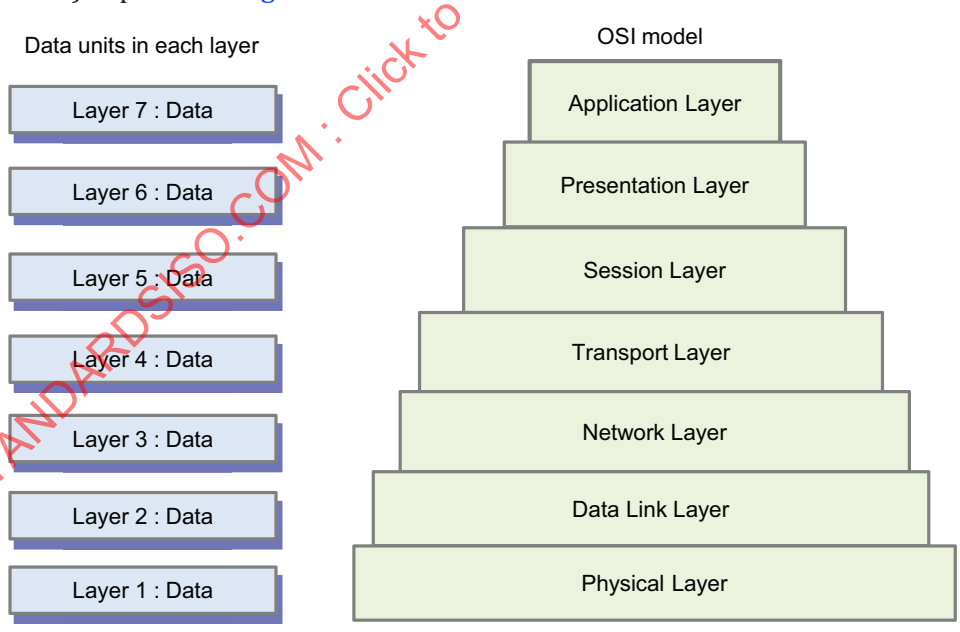

Figure 2 — OSI seven layers

Security gateways are used to fulfil the following security requirements:

— provide logical network segmentation;

— restrict and analyse the traffic which passes between the logical networks;

— control access to and from the organization´s network, by inspection of connections or by proxy operations on selected applications;

— enforce an organization´s network security policy;

— log traffic for subsequent audit;

— hide internal network, host and application architecture; or

— provide the capability for facilitating network management functions, e.g. DoS or DDoS mitigation.

Table 1 illustrates the relationship between the threats in Clause 7 and the security requirements in this clause.

Table 1 — Relationship between the threats and the requirements

Threats	Requirement						
	Provide logical network segmentation	Restrict and analyse the traffic which passes between the logical networks	Control access to and from the organization's network, by inspection of connections or by proxy operations on selected applications	Enforce an organization's network security policy	Log traffic for subsequent audit	Hide internal network, host and application architecture	Provide the capability for facilitating network management functions
Denial of Service to authorized users		X		X	X		X
Unauthorized modification of data	X	X	X	X	X		X
Unauthorized disclosure of data	X	X	X	X	X		X
Unauthorized system re-configuration			X	X	X	X	X
Unauthorized use of resources and assets of organization	X	X	X	X	X	X	X
Unauthorized transversal of content e.g. virus and malware	X	X	X	X	X	X	X
Violation of virtualization	X	X	X	X	X		X
Denial-of-Service and Distributed DoS attack against security gateway.		X		X	X		X

9 Security controls

9.1 Overview

For each security gateway, a separate service access (security) policy document should be developed and the content implemented to ensure that only the authorized traffic is allowed to pass. This document should contain the details of the ruleset that the gateway is required to administer and the configuration of the gateway. It needs to be ensured that the policy hierarchy is put into force: an organization of any significant size is likely to have generic policy across the whole organization, possibly augmented by a generic policy towards a whole class of security devices, possibly further augmented by a specific policy for a particular device. Thus, in order to ensure that only valid users and traffic gain access from communications connections, the policy should define and record in detail the constraints and rules applied to traffic passing into and out of the security gateway and the parameters for its management and configuration. With all security gateways, appropriate use should be made of available identification and authentication, logical access control and audit facilities. In addition, they should be checked regularly for unauthorized software and/or data and, if such is found, incident reports should be produced in accordance with the organization and/or community's information security incident management scheme (see ISO/IEC 27035). A security patch is a change applied to a security gateway to correct the weakness expressed by a vulnerability, in order to prevent successful exploitation and removes or mitigates a threat's capability in a gateway. Hence, security gateways should be regularly updated with the latest patches and versions to ensure that they are effective against the latest vulnerabilities.

A security gateway should not be connected to an organization's network until it has been established that its configuration satisfies the requirements of its governing policies.

A firewall is a good example of a security gateway. Firewalls should normally be those that have achieved an appropriate assurance level commensurate with the assessed threats, with the standard firewall ruleset having an implicit deny all for any traffic between networks and adding explicit rules to satisfy only the required communications paths.

The policies governing a security gateway used to protect a remote system may not warrant the expense and specialist skills to support a dedicated hardware device. Instead, an end-point software-based firewall, so-called a personal firewall, can be used, which controls the flow of traffic between the remote computer and the network to which it is attached. As with any other security gateway, the organization must be satisfied that the configuration of the ruleset in the end-point software-based firewall satisfies the requirements of the governing policies.

There are many types of security gateways; including a packet filtering, a proxy firewall, a stateful packet inspection, a content filtering and application firewall. The details of each type of security gateway will be described in the following sub-clauses.

Security gateway may employ a virtualization technology to implement necessary functions. Virtual machines should be well-isolated when sharing memory, CPU and storage capacities.

The hypervisor, also called virtual machine manager, should provide protection for itself and for hosted VMs, e.g. by moving antivirus and anti-spam processing from VM to hypervisors.

Virtualization security protects both the hypervisor and its VMs. It protects the hypervisor from attacks and enables VM isolation. This function also includes the protection of the VM images and suspended VM instances in storage and during migration, and overall VM security life-cycle management.

9.2 Stateless packet filtering

A packet filter judges each packet in isolation from any other packet. The decision as to whether to allow or deny its progress is based entirely on data within the packet itself. There is no attempt to associate the packet with any preceding packets that may have been presented to the packet filter. The decision is therefore based on factors such as:

— Source and/or destination IP address;

— Payload the packet is carrying (e.g. TCP, UDP, ICMP);

— Source and/or destination port for a TCP or UDP payload;

— Time/date of packet arrival/departure; and

— Network interface card of arrival/departure.

Packet filtering gateways are fast but do not track the significance of any packet within an overall communication stream.

9.3 Stateful packet inspection

Stateful packet inspection extends (stateless) packet filtering by recording key events in the life cycle of a communications exchange, typically tracking the state of transport layer protocols. Based upon packet filtering technology, the stateful packet inspection approach intended and implemented in some firewall products 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 determine the state of the attempted connection on upper layers. When deciding the fate of a packet, a stateful packet filter will consider the packet in the context of other packets it has already seen. This allows the filter, for example, to distinguish between a packet which is part of an established TCP connection and a similar packet which has arrived on its own. A stateful packet filter can therefore make more subtle decisions than a packet filter without state. This, however, requires more resource (memory and processing power) to achieve the same packet throughput.

9.4 Application firewall

An application firewall analyses communications exchange at the application level protocol. For example, a web application firewall would be configured with rules that represented the correct operation of HTTP. The decision as to whether to allow an HTTP request or HTTP response can be based both on the state of the HTTP conversation (for example, is this an appropriate response for a previously seen request?) or some particular pattern in the data (for example, are characters present which indicate an SQL injection attack?).

If an application firewall is to function on encrypted communication such as SSL /TLS, then end-to-end encryption must be broken at the application firewall so that it can filter application data in the clear. In these circumstances, the application firewall should operate a pair of back-to-back encrypted communication channels between the source and destination. Should the integrity of such an application firewall be compromised, then the consequences are especially severe due to the trust that users might have had in the protection of end to end encryption.

Firewalls mask some of the threats described in Clause 7, for example, unauthorized use of resources and assets of an organization, by limiting the access to an application or a computer system to a finite set of identifiable tasks within the proxy itself.

The application firewall 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. The application firewall can be implemented in part of the application proxy which can improve responsiveness and reduce duplicate traffic. The application proxy service has full visibility at the application layer and can accordingly 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 attackers on the outside to exploit vulnerabilities on systems internally. The encrypted end-to-end communications cannot directly traverse an application firewall but instead exist as two back-to-back encrypted streams with the message in the clear within the application firewall. This makes the application firewall particularly attractive as an attack target from which to launch man-in-the-middle attacks against encrypted connections.

Many firewalls now offer both the traditional proxy services, along with transparent proxy capabilities, often referred to as “deep packet inspection” or application control. They are application aware and are able to allow only certain functions within an application or to apply additional controls (for example, anti-virus scanning of files transferred within an application or blocking video call within Instant Messaging clients.).

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.

9.5 Content filtering

Security gateways with application level proxies often implement content filtering. Content filtering is a key protection against malicious or inappropriate code. It can help to defend against threats delivered as application downloads or executed in the browser. This can range from Trojan horses to inappropriate ActiveX controls. As most of this malicious code is distributed over the Internet via email or HTTP-based communication (e.g. downloads from a website 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 services such as SMTP-based email traffic and the HTTP-based communication are routed to the content filtering scanner.

The predominant technologies for content analysis are as follows:

— protocol analysis;

— Signature-based scanning (searching for known patterns);

— Investigative analysis (analysing code for functions and behaviour known to be associated with malicious code); and

— 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.

NOTE Selection, deployment and operations of intrusion detection or prevention systems form the subject of an International Standard, ISO/IEC 27039.

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 is decrypted and re-encrypted again on the firewall. This could pose security threats such as “man in the middle” attacks.

There may be legal implications regarding content scanning and filtering, especially where a strong data protection legislation is in effect. In such a scenario, only automatic scanning for malicious code may be allowed, but not the scanning for specific content of an email because this may infringe upon the privacy of the sender and of the recipient.

9.6 Intrusion prevention system and intrusion detection system

An intrusion is an unauthorized access to a network or a network-connected system, i.e. deliberate or accidental unauthorized access to an information system, malicious activity against an information system, or unauthorized use of resources within an information system. Intrusion prevention is a formal process of actively responding to prevent intrusions. The intrusion prevention system is a variant on intrusion detection systems that are specifically designed to provide an active response capability, while

intrusion detection systems simply detect possible intrusions that have been attempted, are occurring, or have occurred and possibly notify the administrators of the intrusions.

9.7 Security management API

A centralized management function allows proper and efficient management of security gateways deployed in the organization network.

The security management API should be provided by the security gateway for this remote centralized management in an organization. This centralized management function should help remote management of security gateways in terms of operation and configuration.

The remote security administrator should be identified and authenticated by the security gateway. This remote management API should provide a network administrator with tools to administer, monitor, and troubleshoot the security gateway.

10 Design techniques

10.1 Security gateway components

10.1.1 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. The traffic between a switch and the nodes connected to that switch can be controlled through the use of Access Control Lists (ACLs). These can be applied to the OSI model layers 2, 3 and 4. 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-attacks that can cause the exposed switch to flood connected networks with packets.

There may be load-balanced switches that operate at layer 7. These are used to provide availability of both firewalls and servers (though not layer 7 for firewalls usually).

10.1.2 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. Routers normally work on layer 3 of the OSI model (the network layer). At this level only packet level information, such as source and destination ports, can be analysed. Routers can perform NAT and packet filtering.

There may be load-balanced switches that operate at layer 7. These are used to provide availability of both firewalls and servers (though not layer 7 for firewalls usually).

10.1.3 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. An application level gateway understands the applications and protocols being used by applications to be able to determine if the requests are legitimate responses. For example when using such applications as VoIP an application level gateway would need to understand the Session Initiation Protocol(SIP) to allow the appropriate information between connections.

When employing VoIP technology to provide telephone service, the organization network should be protected by attacks against the SIP using a so-called SIP-aware firewall, a typical example of application level gateway.

10.1.4 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/IPS, 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. An appliance dedicated to a single machine called a personal firewall appliance, is a software application running on that machine to protect traffic into and out of that machine. An appliance dedicated to protect a remote location is termed a branch/home or Remote office and branch office security appliances. The Remote office and branch office security appliance generally protects traffic into and out of remote/branch office or home office. All techniques mentioned in Clause 9 can be implemented by using security appliances.

10.1.5 Monitoring function

A centralized monitoring/auditing function allows proper and efficient auditing and/or monitoring of security gateways deployed in the organization network. The communication between the monitoring/auditing function and the security gateway should be secured, which is used to exchange necessary information for proper auditing and monitoring function.

In addition, each security gateway should provide an interface to communicate with the centralized monitoring/auditing function. This centralized monitoring/auditing function may help capture any abnormal status of security gateways and/or any trials and actions that can trigger a security breach to the gateways and/or internal systems and further track the user accountability of actions performed, and records security policy violations.

Comprehensive monitoring of security gateway's operation and the audit trails are facilitated by this centralized monitoring/auditing function. In addition, it may offer a descriptive, efficient and readily-available dashboard for management decision-making.

10.2 Deploying security gateway controls

10.2.1 Packet filter firewall architecture

There are two types of packet filter firewalls: stateful or non-stateful. A stateless packet firewall is appropriate to remove malformed packets, packets arriving from the "wrong" source, or heading towards the "wrong" destination. The source or destination may be identified by the direction of flow through the firewall, the network address of the packet, or the port of the transport-layer content of the packet. Each packet is considered in isolation from all other packets. The packet filter firewall does not break end to end connectivity. The most basic type of firewall architecture is called a packet filter depicted in Figure 3. 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.

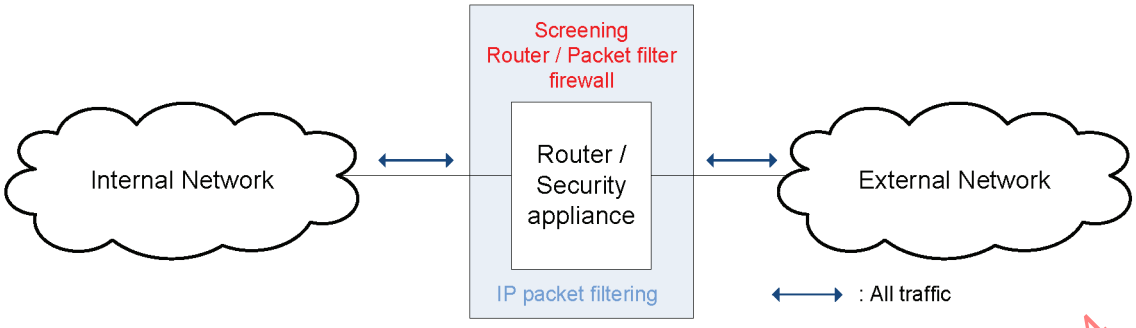

Figure 3 — Packet filter firewall/screening router

The access control functionality of a packet filter firewall is governed by a set of directives collectively referred to as a rule set. Rule sets are commonly referred to as Access Control Lists (ACLs). 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, such as source and destination ports, as well as 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: speed and flexibility. Since packet filters do not usually examine data above layer 4 of the OSI model, they can operate very quickly. This 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). The limited information available to the firewall results in limited logging functionality in packet filter firewalls. Due to the large numbers of variables used in access control decisions, they are susceptible to security breaches caused by improper configurations.

10.2.2 Dual-homed gateway architecture

The dual-homed gateway is an application proxy / application gateway that breaks end to end connectivity. The dual-homed gateway depicted in Figure 4 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 acting as a packet filter 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.

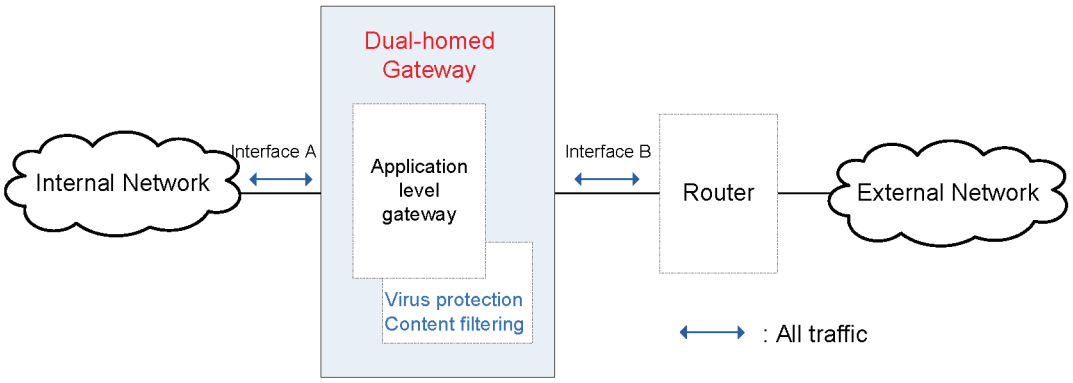

Figure 4 — Dual-homed gateway

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 a 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 bypass to the security gateway. The security of the host system used for the firewall is crucial for the overall protection because if the firewall is compromised an intruder could gain access to the internal systems.

10.2.3 Screened host architecture

The screened host architecture depicted in Figure 5 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.

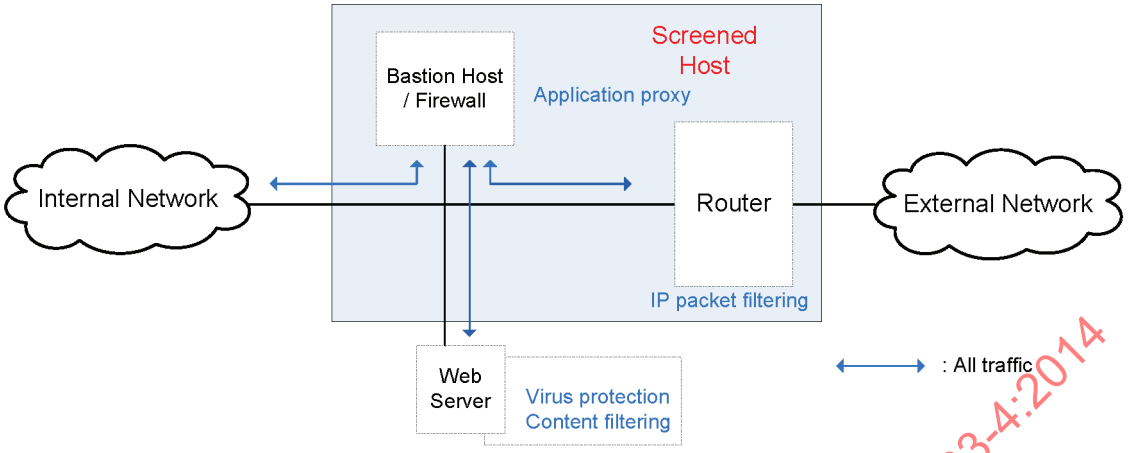

Figure 5 — Screened host

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.

10.2.4 Screen subnet architecture

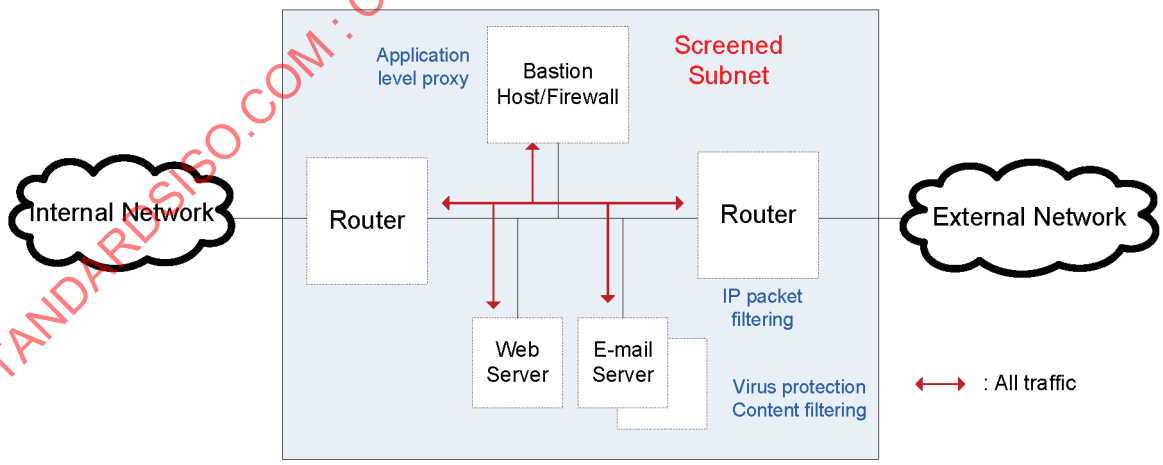

Figure 6 — Screened subnet

The screened subnet architecture depicted in Figure 6 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 such as 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).

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.

11 Guidelines for product selection

11.1 Overview

It is assumed that if the organization is connected to the Internet, then its networks are already protected by some form of packet filtering firewall. If this is not the case, then a perimeter firewall needs to be put into place and configured according to security policy set by an organization as a matter of utmost urgency.

It is assumed that hosts on the same subnet carry similar levels of trust. For example it is assumed that the organization's outward-facing servers (web, email, DNS etc.) are segregated onto their own subnet, distinct from the subnet for the organization's internal hosts. If hosts with significantly different levels of trust share the same subnet, the network design needs refactoring so that boundaries between different trust domains are clear. It is at these boundaries that network security gateway appliances will be positioned.

To ensure that the requirements as outlined in Clause 8 are fulfilled, a structured approach for selecting and configuring security gateways is necessary. This clause gives some guidance for this process, particularly in the areas of:

— Selecting a security gateway architecture and appropriate components;

— Selecting hardware and software platform;

— Configuration;

— Security features and settings;

— Administration;

— Logging;

— Audit; and

— Training/Education.

As a general guidance, the following principles should be applied:

— 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; and

— Use components or devices in their designated functionality and configuration.

11.2 Selection of a security gateway architecture and appropriate components

Based on the business and security requirements for the security gateway (see Clause 8 for further reference), an appropriate security gateway architecture should be selected and adapted (see 10.2 for an overview of possible security gateway architectures).

Once an architecture is defined, each component of this architecture needs to be further specified and their functionality need to be evaluated, refer to 10.2 for an overview of possible components and to 10.1 for a detailed description of the provided functions. In the practice multiple layers of gateways are often used.

The following sub-clauses provide some further guidance on selecting the right components with appropriate architecture.

11.3 Hardware and software platform

While selecting a hardware platform the performance, efficiency, reliability and applicability should particularly be considered, 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.

11.4 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;

— Ensure ports are not enabled by default;

— Ensure Switched Port Analyzer (SPA) ports are not enabled unless the use of intrusion detection systems is needed;

— Ensure passwords are implemented on device interfaces;

— Rejection of the Routing Information Protocol (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;

— Ensure "logging" of all administration events and of all traffic;

— Platform hardening regarding the operating system.

11.5 Security features and settings

As a minimum, an application firewall should provide the following:

— 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 HTTPS correctly;

— Rejection of the Border Gateway Protocol (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;

— Support of identifying applications running within the protocol stream (office productivity applications, embedded video, instant messaging etc.);

— Support of filtering incoming traffic for malware etc., in case of VPN connection;

— Possibility of allowing, denying, or dropping connections or packets.

As minimum, packet filtering device should be able to:

— Support packet filtering on the basis of (packet);

— IP source and destination address;

— Source and destination port (for TCP, UDP);

— Direction of the connection (inbound, outbound).

As a minimum both a packet filtering and stateful filtering device should be able to:

— 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;

— Limit the length of the fragments of IP packets and define a minimum fragment offset;

— Filter the ICMP messages ”destination unreachable” and ”redirect”;

— Prevent spoofing of internal IP addresses if they come from the Internet (due to IP Spoofing).

In addition, as a minimum, stateful 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;

— Detect certain Denial-of-Service attacks such as TCP-SYN flooding;

— Prevent TCP sequence number guessing;

— Resist ping-of-death attacks (a kind of denial of service attack);

