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.

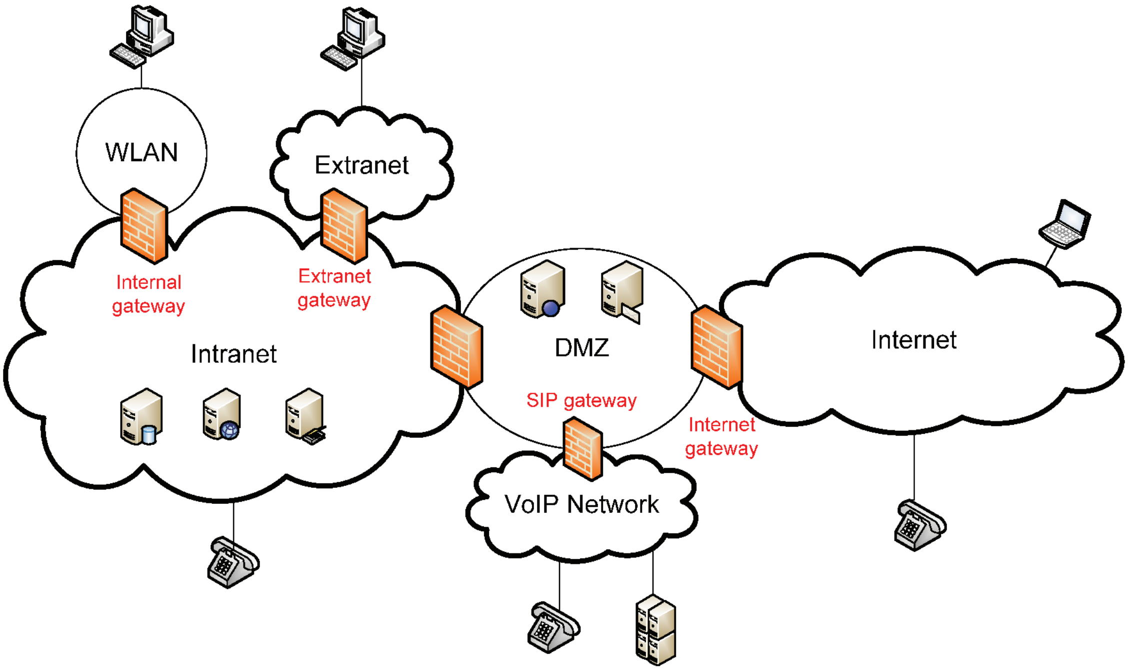

Figure 1 — Example Network Environment

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.

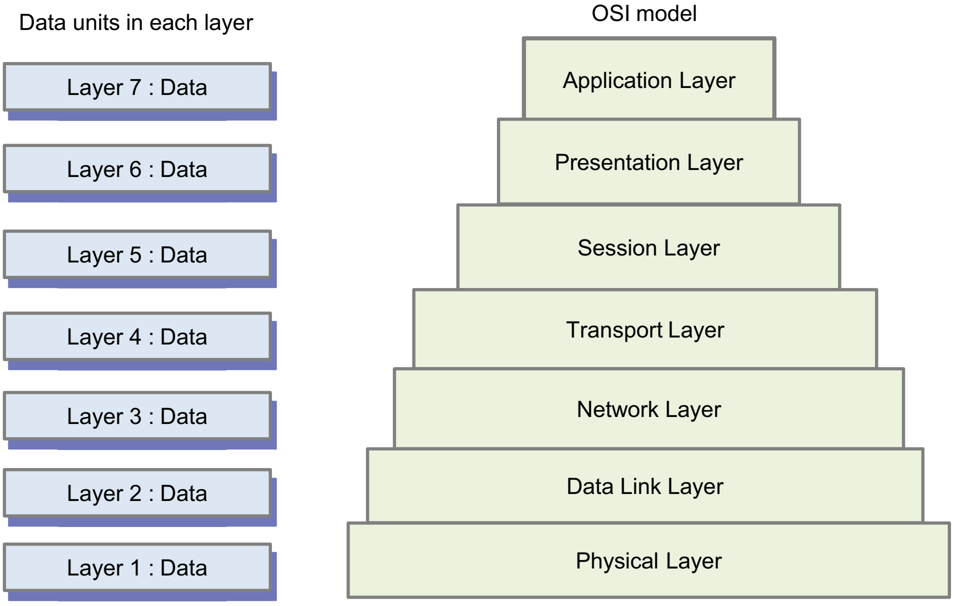

Figure 2 — OSI seven layers

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;