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)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

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

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).