SVENSK STANDARD
SS-ISO/IEC 27033-4:2016

Fastställd/Approved: 2016-12-16
Publicerad/Published: 2016-12-20
Utgåva/Edition: 1
Språk/Language: engelska/English
ICS: 35.030; 35.040.01

Informationsteknik – Säkerhetstekniker – Nätverkssäkerhet – Del 4: Säkerställande av kommunikation mellan nätverk med användning av säkerhets ”gateways” (ISO/IEC 27033-4:2014, IDT)

Information technology – Security techniques – Network security – Part 4: Securing communications between networks using security gateways (ISO/IEC 27033-4:2014, IDT)

Standarder får världen att fungera

SIS (Swedish Standards Institute) är en fristående ideell förening med medlemmar från både privat och offentlig sektor. Vi är en del av det europeiska och globala nätverk som utarbetar internationella standarder. Standarder är dokumenterad kunskap utvecklad av framstående aktörer inom industri, näringsliv och samhälle och befrämjar handel över gränser, bidrar till att processer och produkter blir säkrare samt effektiviserar din verksamhet.

Delta och påverka
Som medlem i SIS har du möjlighet att påverka framtida standarder inom ditt område på nationell, europeisk och global nivå. Du får samtidigt tillgång till tidig information om utvecklingen inom din bransch.

Ta del av det färdiga arbetet
Vi erbjuder våra kunder allt som rör standarder och deras tillämpning. Hos oss kan du köpa alla publikationer du behöver – allt från enskilda standarder, tekniska rapporter och standardpaket till handböcker och onlinetjänster. Genom vår webbtjänst e-nav får du tillgång till ett lättnavigerat bibliotek där alla standarder som är aktuella för ditt företag finns tillgängliga. Standarder och handböcker är källor till kunskap. Vi säljer dem.

Utveckla din kompetens och lyckas bättre i ditt arbete
Hos SIS kan du gå öppna eller företagsinterna utbildningar kring innehåll och tillämpning av standarder. Genom vår närhet till den internationella utvecklingen och ISO får du rätt kunskap i rätt tid, direkt från källan. Med vår kunskap om standarders möjligheter hjälper vi våra kunder att skapa verklig nytta och lönsamhet i sina verksamheter.

Vill du veta mer om SIS eller hur standarder kan effektivisera din verksamhet är du välkommen in på www.sis.se eller ta kontakt med oss på tel 08-555 523 00.

Standards make the world go round

SIS (Swedish Standards Institute) is an independent non-profit organisation with members from both the private and public sectors. We are part of the European and global network that draws up international standards. Standards consist of documented knowledge developed by prominent actors within the industry, business world and society. They promote cross-border trade, they help to make processes and products safer and they streamline your organisation.

Take part and have influence
As a member of SIS you will have the possibility to participate in standardization activities on national, European and global level. The membership in SIS will give you the opportunity to influence future standards and gain access to early stage information about developments within your field.

Get to know the finished work
We offer our customers everything in connection with standards and their application. You can purchase all the publications you need from us - everything from individual standards, technical reports and standard packages through to manuals and online services. Our web service e-nav gives you access to an easy-to-navigate library where all standards that are relevant to your company are available. Standards and manuals are sources of knowledge. We sell them.

Increase understanding and improve perception
With SIS you can undergo either shared or in-house training in the content and application of standards. Thanks to our proximity to international development and ISO you receive the right knowledge at the right time, direct from the source. With our knowledge about the potential of standards, we assist our customers in creating tangible benefit and profitability in their organisations.

If you want to know more about SIS, or how standards can streamline your organisation, please visit www.sis.se or contact us on phone +46 (0)8-555 523 00

Den internationella standarden ISO/IEC 27033-4:2014 gäller som svensk standard. Detta dokument innehåller den officiella engelska versionen av ISO/IEC 27033-4:2014.

The International Standard ISO/IEC 27033-4:2014 has the status of a Swedish Standard. This document contains the official English version of ISO/IEC 27033-4:2014.

Upplysningar om sakinnehållet i standarden lämnas av SIS, Swedish Standards Institute, telefon 08-555 520 00. Standarder kan beställas hos SIS Förlag AB som även lämnar allmänna upplysningar om svensk och utländsk standard.

Information about the content of the standard is available from the Swedish Standards Institute (SIS), telephone +46 8 555 520 00. Standards may be ordered from SIS Förlag AB, who can also provide general information about Swedish and foreign standards.

Denna standard är framtagen av kommittén för Säkerhetsåtgärder och tjänster, SIS/TK 318/AG 41.

Har du synpunkter på innehållet i den här standarden, vill du delta i ett kommande revideringsarbete eller vara med och ta fram andra standarder inom området? Gå in på www.sis.se - där hittar du mer information.

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