EESTI STANDARD EVS-ISO/IEC 27033-4:2015

INFOTEHNOLOOGIA
Turbemeetodid
Võrguturve
Osa 4: Võrkudevahelise side turve turvalüüside abil

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

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA	NATIONAL FOREWORD
See Eesti standard EVS-ISO/IEC 27033-4:2015 „Infotehnoloogia. Turbemeetodid. Võrguturve. Osa 4: Võrkudevahelise side turve turvalüüside abil“ sisaldab rahvusvahelise standardi ISO/IEC 27033-4:2014 „Information technology. Security techniques. Network security. Part 4: Securing communications between networks using security gateways“ identset ingliskeelset teksti.	This Estonian Standard EVS-ISO/IEC 27033-4:2015 consists of the identical English text of the International Standard ISO/IEC 27033-4:2014 „Information technology. Security techniques. Network security. Part 4: Securing communications between networks using security gateways“.
Ettepaneku rahvusvahelise standardi ümbertrüki meetodil ülevõtuks on esitanud EVS/TK 4, standardi avaldamist on korraldanud Eesti Standardikeskus.	Proposal to adopt the International Standard by reprint method has been presented by EVS/TK 4, the Estonian standard has been published by the Estonian Centre for Standardisation.
Standard EVS-ISO/IEC 27033-4:2015 on jõustunud sellekohase teate avaldamisega EVS Teataja 2015. aasta veebruarikuu numbris.	Standard EVS-ISO/IEC 27033-4:2015 has been endorsed with a notification published in the February 2015 issue of the official bulletin of the Estonian Centre for Standardisation .
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Käsitlusala

ISO/IEC 27033 see osa annab juhiseid võrkudevahelise side turbeks turvalüüside (tulemüüride, rakenduste tulemüüride, sissetungi tuvastuse süsteemi vm) abil vastavalt turvalüüside dokumenteeritud infoturvapoliitikale, sealhulgas selle kohta, kuidas

a) tuvastada ja analüüsida võrgu turvaohte, mis on seotud turvalüüsidega;

b) ohtude analüüsi põhjal määratleda võrguturbe nõudeid turvalüüsidele;

c) kasutada kavandamis- ja teostamismeetodeid tüüpiliste võrgustsenaariumidega seotud ohtude ja meetmeaspektide käsitlemiseks;

d) käsitleda probleeme, mis on seotud võrgu turvalüüsi turvameetmete evitamise, käigushoiu, seire ja läbivaatusega.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.040

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