INTERNATIONAL STANDARD

ISO/IEC 18028-5

First edition
2006-07-01

Information technology — Security techniques — IT network security —

Part 5: Securing communications across networks using virtual private networks

Technologies de l'information — Techniques de sécurité — Sécurité de réseaux TI —

Partie 5: Communications sûres à travers les réseaux utilisant les réseaux privés virtuels

Reference number
ISO/IEC 18028-5:2006(E)

© ISO/IEC 2006

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

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/IEC 2006

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

© ISO/IEC 2006 – All rights reserved

Not for Resale

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 2
3.1 Terms defined in other International Standards 2
3.2 Terms defined in this part of ISO/IEC 18028 2

4 Abbreviated terms 3

5 Overview of VPNs 3
5.1 Introduction 3
5.2 Types of VPN 4
5.3 VPN techniques 5
5.4 Security aspects 6

6 VPN security objectives 7

7 VPN security requirements 7
7.1 Confidentiality 8
7.2 Integrity 8
7.3 Authentication 8
7.4 Authorization 8
7.5 Availability 8
7.6 Tunnel Endpoints 8

8 Guidelines for the selection of secure VPNs 9
8.1 Regulatory and legislative aspects 9
8.2 VPN management aspects 9
8.3 VPN architectural aspects 9

9 Guidelines for the implementation of secure VPNs 12
9.1 VPN management considerations 12
9.2 VPN technical considerations 12

Annex A (informative) **Technologies and protocols used to implement VPNs** 15
A.1 Introduction 15
A.2 Layer 2 VPNs 15
A.3 Layer 3 VPNs 17
A.4 Higher Layer VPNs 17
A.5 Comparison of typical VPN protocol security features 19

Bibliography 20

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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 should not be held responsible for identifying any or all such patent rights.

ISO/IEC 18028-5 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 1: Network security management*

— *Part 2: Network security architecture*

— *Part 3: Securing communications between networks using security gateways*

— *Part 4: Securing remote access*

— *Part 5: Securing communications across networks using virtual private networks*

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

© ISO/IEC 2006 – All rights reserved

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 information system networks, and their inter-connections. Those individuals within an organization that are responsible for information security in general, and 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 analyze 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 (VPNs).

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 and/or network security, network operation, or who are responsible for an organization's overall security program 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 network managers, administrators, engineers, and 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 network managers, administrators, engineers and 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 network managers, administrators, engineers, and 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 network managers, administrators, engineers, and network security officers).

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Information technology — Security techniques — IT network security —

Part 5: Securing communications across networks using virtual private networks

1 Scope

This part of ISO/IEC 18028 provides detailed direction with respect to the security aspects of using Virtual Private Network (VPN) connections to inter-connect networks, and also to connect remote users to networks. It builds upon the network management direction provided in ISO/IEC 18028-1.

It is aimed at those individuals responsible for the selection and implementation of the technical controls necessary to provide network security when using VPN connections, and for the subsequent network monitoring of VPN security thereafter.

This part of ISO/IEC 18028 provides an overview of VPNs, presents VPN security objectives, and summarizes VPN security requirements. It gives guidance on the selection of secure VPNs, on the implementation of secure VPNs, and on the network monitoring of VPN security. It also provides information on typical technologies and protocols used by VPNs.

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 7498 (all parts), *Information technology — Open Systems Interconnection — Basic Reference Model*

ISO/IEC 13335-1:2004, *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*

ISO/IEC 17799:2005, *Information technology — Security techniques — Code of practice for information security management*

ISO/IEC 18028-1:2006, *Information technology — Security techniques — IT network security — Part 1: Network security management*

ISO/IEC 18028-2:2006, *Information technology — Security techniques — IT network security — Part 2: Network security architecture*

ISO/IEC 18028-3:2005, *Information technology — Security techniques — IT network security — Part 3: Securing communications between networks using security gateways*

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ISO/IEC 18028-4:2005, *Information technology — Security techniques — IT network security — Part 4: Securing remote access*

3 Terms and definitions

3.1 Terms defined in other International Standards

For the purposes of this document, the terms and definitions given in ISO/IEC 7498 (all parts) and ISO/IEC 18028-1 apply, as do the following terms defined in ISO/IEC 13335-1: accountability, asset, authenticity, availability, baseline controls, confidentiality, data integrity, impact, integrity, security policy, non-repudiation, reliability, risk, risk analysis, risk management, safeguard, threat, and vulnerability.

3.2 Terms defined in this part of ISO/IEC 18028

For the purposes of this document, the following terms and definitions apply.

3.2.1
layer 2 switching
technology that uses internal switching mechanisms to establish and control connections between devices using layer 2 protocols

NOTE It is typically used to simulate a LAN environment to upper layer protocols.

3.2.2
layer 2 VPN
virtual private network used to provide a simulated LAN environment over a network infrastructure

NOTE Sites linked by a layer 2 VPN can operate as though they are on the same LAN.

3.2.3
layer 3 switching
technology that uses internal switching mechanisms in combination with standard routing mechanisms, or which employs MPLS techniques, in order to establish and control connections between networks

3.2.4
layer 3 VPN
virtual private network used to provide a simulated WAN environment over a network infrastructure

NOTE Sites linked by a layer 3 VPN can operate as though they are on a private WAN.

3.2.5
private
restricted to members of an authorized group: in the context of VPNs, it refers to the traffic flowing in a VPN connection

3.2.6
private network
network that is subject to access controls which are intended to restrict use to members of an authorized group

3.2.7
protocol encapsulation
enveloping one data flow inside another by transporting protocol data units wrapped inside another protocol

NOTE This is one method which can be used to establish tunnels in VPN technology.

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3.2.8
virtual circuit
data path between network devices established using a packet or cell switching technology such as X.25, ATM or Frame Relay

4 Abbreviated terms

For the purposes of this document, the abbreviated terms given in ISO/IEC 18028-1 and the following apply.

AH	Authentication Header
ESP	Encapsulating Security Payload
IKE	Internet Key Exchange
IPX	Internetwork Packet Exchange
ISAKMP	Internet Security Association and Key Management Protocol
L2F	Layer Two Forwarding (Protocol)
L2TP	Layer 2 Tunneling Protocol
LDP	Label Distribution Protocol
MPPE	Microsoft Point-to-Point Encryption
NAS	Network Area Storage
NCP	Point-to-Point Protocol
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
SSL	Secure Sockets Layer
VPLS	Virtual Private LAN Service
VPWS	Virtual Private Wire Service

5 Overview of VPNs

5.1 Introduction

VPNs have developed rapidly as a means of inter-connecting networks, and as a method of connecting remote users to networks. A VPN is an example of a type of technology that can implement the Communication Flow Security Dimension described in ISO/IEC 18028-2, the security for which is considered as part of the Services Security Layer (as defined in ISO/IEC 18028-2).

There exists a broad range of definitions for VPNs. In their simplest form, they provide a mechanism for establishing a secure data channel or channels over an existing network or point-to-point connection. They are assigned to the exclusive use of a restricted user group, and can be established and removed dynamically, as needed. The hosting network may be private or public.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

An example representation of a VPN, with the secure data channel connecting the two endpoints across an insecure public network, is shown in Figure 1 below.

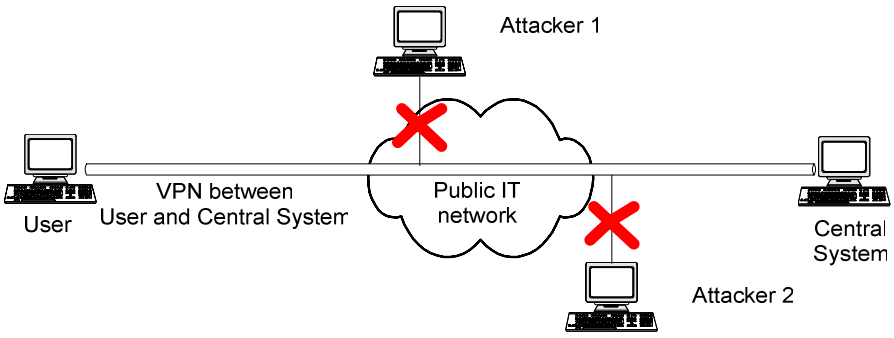

Figure 1 — Example representation of a VPN

Remote access using a VPN is implemented over the top of a normal point-to-point connection, which should first be established between the local user and the remote location in line with ISO/IEC 18028-4. The connection could take the form of wired or wireless network technology.

Some VPNs are provided as a managed service, in which secure, reliable connectivity, management and addressing, equivalent to that on a private network, are provided on a shared infrastructure. Additional security controls, as indicated in this standard, may therefore need to be taken into account to strengthen the VPN.

The data and code transiting a VPN should be restricted to the organization using the VPN and should be kept separate from other users of the underlying network. It should not be possible for data and code belonging to other users to access the same VPN channel. The level of trust in the confidentiality and other security aspects of the organization owning or providing the VPN should be taken into consideration when evaluating the extent of additional security controls that may be required.

5.2 Types of VPN

As stated above, there are multiple ways of expressing types of VPN.

Architecturally, VPNs comprise either:

— a single point-to-point connection (e.g. client device remotely accessing an organization's network via a site gateway, or a site gateway connecting to another site gateway), or

— a point-to-cloud connection (e.g. implemented by MPLS technology).

From an OSI Basic Reference Model perspective, there are three main types of VPN:

— Layer 2 VPNs offer a simulated LAN facility, using VPN connections running over a hosting network (e.g. a provider's network) to link sites of an organization or to provide a remote connection to an organization. Typical provider offerings in this area include Virtual Private Wire Service (VPWS), which provides a simulated "wires only connection", or Virtual Private LAN Service (VPLS), which provides a more complete simulated LAN service.

— Layer 3 VPNs offer a simulated WAN facility, again using VPNs running over a network infrastructure. These offerings provide sites with simulated "OSI Network Layer" connectivity. A basic attraction here is the ability to use private IP addressing schemes over a public infrastructure, a practice that would not be permitted over a "normal" public IP connection. Whilst private addresses can be used over public networks via NAT (Network Address Translation), this can complicate IPsec VPN establishment and use, although there are work-arounds available.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO/IEC 2006 – All rights reserved
Not for Resale

— Higher Layer VPNs are used for securing transactions across public networks. They typically provide a secure channel between communicating applications, thus ensuring data confidentiality and integrity during the transaction. This type may also be known as a Layer 4 VPN because the VPN connection is usually established over TCP which is a Layer 4 protocol.

Specific technologies and protocols typically used by types of VPN are further described in Annex A.

5.3 VPN techniques

VPNs are 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.

VPNs can be implemented entirely within a private network under the control of the owning organization, they can be implemented across networks in the public domain, or they can be implemented across combinations of the two. (Whilst it is perfectly possible for VPNs to be built over existing private WANs, the general availability of relatively low cost access to the Internet has made this public network system appear to be a cost effective vehicle for supporting wide area VPNs and remote access VPNs, in many applications.) Alternatively, the channels may be established employing secure channels built using tunnels running through Internet Service provider networks. In this case the public Internet is effectively the underlying transport system. This implies a greater degree of uncertainty as to the confidentiality of the VPN.

A tunnel is a data path between networked devices, which is established across an existing network infrastructure. It is transparent to normal network operations and, for most practical purposes, can be used similar to normal network connections. It can easily be switched on or off as required without any change to the underlying physical network infrastructure. A VPN created with tunnels is therefore more flexible then a network based on physical links.

Tunnels can be created by using:

— virtual circuits,

— label switching, or

— protocol encapsulation.

Tunnels created as virtual circuits are typically established in conventional WAN facilities as leased lines using packet switching technologies (e.g. Frame Relay or ATM). These technologies assure that data flows between tunnels are separated.

Label switching is another way of creating tunnels. All data packets flowing in one tunnel are assigned with one identifying label. This label ensures that every packet with a different label will be excluded from the specified path through the network.

Although the techniques used for tunneling do assure that data flows between tunnels and the underlying networks are properly separated, they do not fulfill general confidentiality requirements. If confidentiality is needed, encryption technologies need to be used to provide the required security level.

Tunnels can also be created by using a protocol encapsulation technique whereby one protocol's data unit is wrapped and carried in another protocol. For example, an IP packet is wrapped using the IPsec ESP protocol’s tunnel mode. An additional IP header is inserted, and the packet is then transmitted over an IP network.

VPN tunnels can be created on different layers of the OSI model. Virtual circuits form tunnels on Layer 2. Label switching techniques allows tunnels to be created at Layer 2 or 3. Protocol encapsulation can be used on all layers except the Physical Layer (most implementations are on Layer 3 and above).

Encryption may be used to provide an additional level of security for tunnels based on virtual circuits, protocol encapsulation and label switching.

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

5.4 Security aspects

Although tunnels are hidden from normal network users, they are not invisible, and therefore not inherently secure. The basic partitioning (into virtual circuits or label-switched paths) or encapsulation process used to construct a tunnel is not protected from determined inspection by attackers using network analyzers or interceptors. If the tunnel is not implemented using encryption, then the attacker would be able to access the traffic, and even if encryption is utilized, the existence of the tunnel and its endpoints would still not be hidden. In addition, the end-points of the tunnel may also not be necessarily protected from unauthorized logical and/or physical access. In order to achieve secure VPN implementations, it is therefore necessary to apply security controls to tunnels depending on the organizational security policy and risk acceptance levels.

It will depend on the organizational security policy whether such vulnerabilities are acceptable or not.

5.4.1 Virtual circuits

The security controls which establish the underlying secure channels may use virtual circuits in conventional wide area telecommunications facilities, e.g. leased lines, using technologies such as Frame Relay or ATM. In these technologies the underlying networks are also essentially secure, to the extent that the telecommunications operators maintain separation between leased line facilities for private subscribers, and provision of public access Internet services. The technology used in virtual circuits inherently confers a degree of confidentiality, but not absolute security, to the channel. A VPN built over such traditional virtual circuits is considered relatively unlikely to be compromised, as security breaches or attacks would typically need to originate within the provider's core network.

5.4.2 Label switching

Security issues for label switched VPNs include:

— address space and routing separation between VPNs carried over the label switched network:

— ensuring that the internal structure of the label switched network core is not visible to outside networks (e.g. to limit information available to a potential attacker);

— providing resistance to denial of service attacks;

— providing resistance to unauthorized access attacks;

— protecting against label spoofing (although whilst it may be possible to insert wrong labels into a label switched network from the outside, because of address separation the spoofed packet would only harm the VPN from which the spoofed packet originated).

5.4.3 Protocol encapsulation

The level of confidentiality sustained using protocol encapsulation is dependent on the property of the encapsulating protocol. For example, if an IPsec tunnel with only AH protocol is used to create a tunnel; it does not provide confidentiality because any data intercepted by third party will be clearly visible. This is because the AH protocol provides only authentication for the communicating parties.

5.4.4 Encryption

Guidance on the general security aspects of cryptography are provided in ISO/IEC 18028-1, ISO/IEC 11770-1 and ISO/IEC 17799. Information on specific algorithms and protocols are addressed in other publications and should be considered as part of the secure VPN selection (see Clause 8).

5.4.5 Integrity protection

Encrypted packets without integrity protection can be subject to tampering. For that reason, traffic that is susceptible to alteration, whether or not it is encrypted, should also be integrity-protected.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6 VPN security objectives

The primary security objective of a VPN is protection from unauthorized access. VPNs could therefore be used to fulfill wider network security objectives:

— to safeguard information in networks, in systems connected to networks, and the services used by them,

— to protect the supporting network infrastructure,

— to protect network management systems.

ISO/IEC 18028-1 discusses the key security risks associated with VPNs.

7 VPN security requirements

To achieve the objectives outlined in Clause 6 above, VPNs should be implemented in a way that ensures the:

— confidentiality of data and code in transit between VPN end-points,

— integrity of data and code in transit between VPN end-points,

— authenticity of VPN users and administrators,

— authorization of VPN users and administrators,

— availability of VPN end-points and network infrastructure.

This in turn implies that the underlying tunnels used to construct the VPN should be implemented in such a way that the security objectives are met. These objectives are summarized in Figure 2.

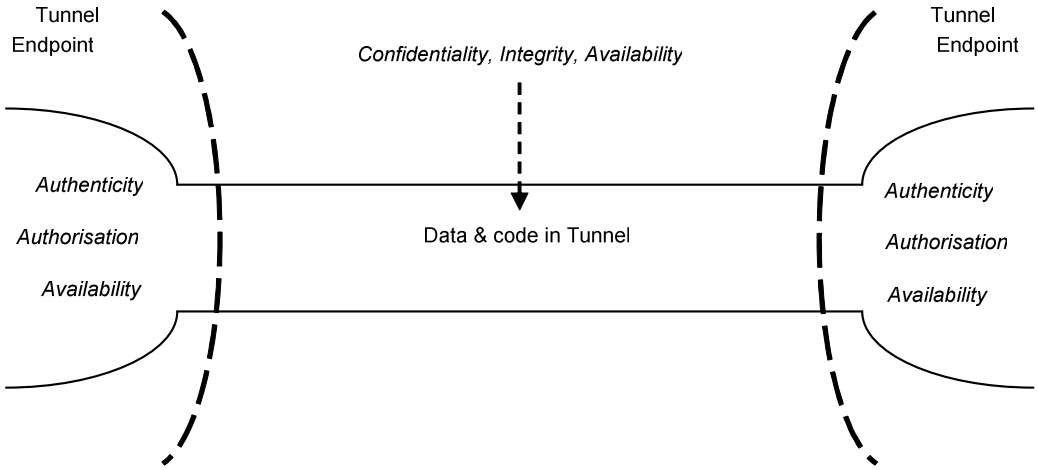

Figure 2 — Generic security requirements of VPNs mapped onto the underlying tunnel

Each of these requirements is discussed in detail below.

ISO/IEC 18028-1 also discusses the types of security controls used to implement secure VPNs.

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.1 Confidentiality

The confidentiality of data and code in transit in the tunnel should not be compromised. Use of tunnel technologies may imply that data and code in transit are not visible to other users of the network. However this does not mean that the traffic is kept confidential. In particular data and code flowing in tunnels are not protected from determined inspection using data analyzers or interceptors. The preservation of confidentiality of data and code whilst in transit in tunnels is therefore crucially dependent upon the likelihood of such inspection occurring. This in turn is a factor of the degree of trust that exists in the underlying network(s) supporting the VPN(s), which will vary depending upon the ownership of the transit network. If the transit network is not in a trusted domain (see ISO/IEC 18028-1 for more information on domains of trust), or if the data and code to be transmitted are considered sensitive, additional security controls may need to be taken to further protect confidentiality. In such cases, the tunnel mechanism(s) employed should support encryption, or items to be sent should be encrypted off-line before transmission over the VPN. The security of the tunnel end-points should also not be neglected (see Clause 7.6),

7.2 Integrity

The integrity of data and code in transit in the tunnel should not be compromised. The mechanisms used to implement the VPN tunnel should support integrity checking of data and code in transit, using techniques such as message verification codes, message authentication codes and anti-replay mechanisms. If such protection is not available from the tunnel implementation, or if the data or code to be transmitted is particularly sensitive, then integrity protection controls should be implemented in the end-systems, such that integrity protection is provided end-to-end.

7.3 Authentication

The tunnel establishment and operating process should be supported by authentication controls such that each end of the tunnel can be sure that it is communicating with the correct partner end-point, which may be a remote-access system, and that data and code received have originated from the correct authorized source. These security controls include, for example, password protection, password challenge protection, security certificate-based systems, secure key-exchange procedures, data origin authentication codes, and anti-replay mechanisms.

7.4 Authorization

The tunnel establishment and operating process should be supported by access control controls, such as ACLs, so that each end of the tunnel can be sure that it is communicating with an authorized partner end-point, which may be a remote-access system, and that data and code received have originated from an authorized source. Controlling access to the data path(s) existing through established tunnels is outside the scope of the tunnel mechanism(s), and should be addressed by adequate access controls in the end-systems.

7.5 Availability

The availability of tunnels, and hence of VPNs, is a function of the availability of the supporting network infrastructure and the end-point systems, but security controls to counter denial of service attacks which are specific to tunnel mechanisms should be incorporated wherever possible.

For specific service level agreements, diverse and resilient tunneling should be examined as alternatives.

7.6 Tunnel Endpoints

The security requirements for the VPN endpoints should also be considered. Typically each VPN endpoint should ensure that there is only controlled network traffic between the hosting network and the VPN. This usually implies disabling of routing, and also at least use of packet filter or firewall technology. See clauses 8.3.1 (Endpoint security) and 8.3.2 (Termination security) for further details.

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8 Guidelines for the selection of secure VPNs

8.1 Regulatory and legislative aspects

Consideration should be given to any regulatory or legislative security requirements relating to network connections and the use of VPNs as defined by the respective regulatory or legislative body (including national government agencies) in the countries where VPNs are to be used.

This includes regulations and/or legislation concerning:

— privacy/data protection,

— use of cryptographic technology, and

— operational risk management/governance.

8.2 VPN management aspects

When considering the use of VPNs and their impact across the Management, Control and End-User Security Planes, all those persons in the organization who have responsibilities associated with the VPN should be clear about the business requirements and benefits. In addition, they, and all other users of the VPN, should be aware of the security risks to, and related control areas for, such a connection. The business requirements and benefits are likely to influence many decisions and actions taken in the process of considering VPN connections, identifying potential control areas, and then eventually selecting, designing, implementing and maintaining security controls. Thus, these business requirements and benefits need to be kept in mind throughout the selection process.

Detailed guidance on secure service management frameworks and overall network security management is provided in ISO/IEC 18028-1, and addressed as part of the Management Security Plane described in ISO/IEC 18028-2.

8.3 VPN architectural aspects

In selecting VPNs, the following architectural aspects should be addressed:

— endpoint security,

— termination security,

— malicious software protection,

— authentication,

— intrusion detection system,

— security gateways (including firewalls),

— network design,

— other connectivity,

— split tunneling,

— audit logging and network monitoring,

— technical vulnerability management.

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Each of these aspects is summarized below.

8.3.1 Endpoint security

The function of a VPN is to provide a secure communication channel across some network medium. Unfortunately, while the VPN is established it is impossible to monitor what the data stream contains. If either of the endpoints is compromised, the compromise may spread to the session across the VPN.

Endpoint security not only applies to the device itself, but also the applications on these devices and procedural/physical aspects surrounding their use.

Some endpoint user devices (e.g. mobile/teleworking computing equipment) used for remote access may not be under the same management control as that for the VPN. These devices may be connected to different networks, e.g. to gain access to the Internet and the organization's private network at different times. These networks may pose additional risk and consideration should be given to ensure that appropriate security controls are applied. The security controls from ISO/IEC 17799 should be taken into account when considering the security of such endpoint devices, including those relating to:

— equipment security,

— protection against malicious and mobile code,

— information security awareness, education and training of those personnel using the devices,

— technical vulnerability management of the devices and related VPN technology.

Other controls should be taken into account, for example a packet filter or personal firewall.

8.3.2 Termination security

One of the key factors influencing the security of a VPN is how it is terminated at each end. If the termination is directly into the core of the endpoint (for example, into the secure zone of a network), security is directly dependent on the security of the remote partner. If the termination point is somewhere in the insecure zone, it is likely that communications may be readily spoofed.

The standard methods for VPN termination are:

— termination on an external firewall, using the firewall termination facility: suitable for point-to-point connectivity (e.g. between two networks). (Firewalls are further discussed in ISO/IEC 18028-3);

— deployment of a dedicated VPN endpoint in an intermediate zone, allowing the ability to further process information from the VPN (e.g. in deciding whether to grant access to applications/systems in the secure zone). Potentially, intermediate zone termination allows greater control over the VPN and its users.

In any case, the VPN endpoint should authenticate the entity (e.g. user or device) before allowing access. This is in addition to the authentication performed between endpoints to set up the VPN link. For example, for users, this typically involves a user name and password, and may also require the use of an additional form of authentication (so-called 'strong authentication'), e.g. token, card or biometric technology.

8.3.3 Malicious software protection

Once information systems are shown to be free of malicious software, the only route for such code to be introduced is via data (or executable code). VPN endpoints offer good control points for the implementation of malicious software protection to control the transmission of such code.

Further information on protection against malicious code, including viruses, worms and Trojans, is provided in ISO/IEC 17799.

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8.3.4 Authentication

Authentication is one of the key stages in the establishment of a VPN. Of necessity, each end should authenticate to its intended session partner (in other words, mutual authentication is required). This can be achieved by a number of methods:

— pre-shared keys, which may offer convenience because, once set up, no further management is required. However, these may be subject to abuse (e.g. for man-in-the-middle attacks) if they are compromised;

— certificates, which offer more flexibility and scalability, especially if deployed with PKI backing to simplify key management, revocation and re-issue.

Further information on authentication and use of cryptographic based services for authentication is provided in ISO/IEC 18028-1, ISO/IEC 11770-1 and ISO/IEC 17799.

8.3.5 Intrusion detection system (IDS)

The need for Intrusion Detection System (IDS) technology should be considered, An IDS can be implemented on both sides of the VPN to detect possible intrusions. IDS alerts can then be raised by any appropriate mechanism, as well as being logged (and managed) as part of an audit trail. Note that some personal firewalls even have the capacity to act as a simple intrusion prevention system (IPS), barring network access to unauthorized applications.

Further information on IDS is provided in ISO/IEC 18028-1, ISO/IEC TR 15947 and ISO/IEC 18043.

8.3.6 Security gateways

Careful consideration should be given to the selection of appropriate security gateway (including firewall) technology to support a VPN deployment.

Information on secure gateways (including firewalls) is provided in ISO/IEC 18028-3.

8.3.7 Network design

The network design at either end of the VPN should support the aims of termination security, discussed above. In particular, the VPN should normally be terminated either on an outer firewall (e.g. at the network perimeter) or within its own intermediate zone.

Further information on this is provided in ISO/IEC 18028-1, ISO/IEC 18028-2, ISO/IEC 18028-3 and ISO/IEC 18028-4.

8.3.8 Other connectivity

Consideration should be given to any further connectivity from a VPN endpoint. If other connectivity exists at either of the VPN endpoints, it is possible that a security compromise initiated from that channel may attack both the local systems and, via the VPN, the remote systems. This possibility can be mitigated by correct network design and use of firewalls. However, the most effective control is not to have any unnecessary connectivity. This consideration is particularly acute for the presence of modems on remote/home-based systems.

Special attention should be given to connectivity between organizational networks and third party organizations providing services such as support and troubleshooting. Security controls for the service provider environment should be established as part of the contractual arrangements. Such controls should ensure a physically and logically segregated environment from the service provider's other operations and customer environments. Further information is provided in ISO/IEC 17799:2005 (Clause 6.2).

Further information on this is provided in ISO/IEC 18028-3.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8.3.9 Split tunneling

Split tunneling should be avoided where practical. Split tunneling refers to the ability of a single connection (usually the Internet) to support the VPN and another connection (VPN or otherwise). In this situation, there is a risk that the security of the remote network is compromised because of attack coming through the other tunnel; analogous to a personal computer with two network cards routing between the two networks. In general, split tunneling can be avoided by the VPN products 'taking over' the network connection.

8.3.10 Audit logging and network monitoring

In common with all other security technologies, the chosen VPN solution should maintain an appropriate audit logs for the analysis of all actions at that endpoint. Like the other audit logs generated by the network, it should be reviewed for indications of security incidents.

Care should be taken to ensure that audit logs are themselves protected, commensurate with the assessed risks, against corruption and misuse. Where audit logs are to be used in legal prosecutions then their integrity should be provable beyond reasonable doubt.

Further information on audit logging and network monitoring is provided in ISO/IEC 18028-1 and ISO/IEC 17799.

8.3.11 Technical vulnerability management

Network environments, as other complex systems, are not free of errors. Technical vulnerabilities are present in, and are published for, components frequently used in networks such as VPNs. The exploitation of these technical vulnerabilities can have a severe impact on the security of the VPN, most often observed in the areas of availability and confidentiality. Thus technical vulnerability management should be present for all VPN devices.

Further information on technical vulnerability management is provided in ISO/IEC 18028-1 and ISO/IEC 17799.

9 Guidelines for the implementation of secure VPNs

9.1 VPN management considerations

Detailed guidance on implementing secure service management frameworks and network security management is addressed in detail in ISO/IEC 18028-1. This part also discusses the high level security risks to VPNs and security control groups relevant to mitigating those risks. ISO/IEC 18028-2 discusses the network security activities necessary across the Management, Control and End-User Security Planes.

9.2 VPN technical considerations

Achieving a secure VPN implementation requires a systematic consideration of the elements identified in the objectives. In particular, the following implementation aspects should be considered:

— carrier protocol selection,

— hardware versus software, and

— VPN device management.

Each of these aspects is discussed below.

Annex A provides further information regarding specific technologies and protocols typically used by types of VPN.

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9.2.1 Carrier protocol selection

A suitably secure carrier protocol should be selected on the basis of:

— business need,

— interoperability (formal international standard or proprietorial standard),

— market perception,

— known weaknesses, and

— robustness.

9.2.2 VPN appliances

Use of VPN appliances should be considered. While in small-scale VPNs (e.g. single user to central system), the implementation of the VPN functionality by a software solutions is adequate, in many situations the use of appliances providing VPN functionalities may have significant advantages, e.g. in terms of simplified management and typically operating on a more security-hardened platform. There is also likely to be some form of authentication platform required (e.g. directory, PKI or RADIUS), which would, for example, allow only authorized users to connect into the central location.

9.2.3 VPN device management

VPN devices should be correctly managed. VPN device management is the generic term for the processes required to set up and monitor VPN devices. Setting up a VPN device consists of configuring it to the network configuration and port/application access required, installation of certificates (e.g. for Higher Layer VPNs), and the continuing network monitoring of the VPN device as for any other network device.

VPN deployment using portable media such as CD-ROMs, diskettes, etc. should be controlled, e.g. by creating delivery and receipt log(s) and by implementing restrictions on re-use of media such as a date/time expiration or limitation on the number of times an execution can be performed.

9.2.4 VPN security monitoring

VPNs, particularly when used as remote access channels into corporate networks, can present particular challenges to network security management, if not carefully managed and controlled.

Consideration should be given to the tunnel itself, its end-points, and also to the data and code flowing through the tunnel, to prevent a secure path into the network being provided as a convenience to attackers.

In order that network security controls remain effective, it is essential that systematic network monitoring of security implementations, including VPNs, be conducted, and that network managers or administrators are able to detect and respond to actual or suspected information security incidents.

In addition, one or more of the following should be implemented:

— intrusion detection system(s),

— security/incident alarms,

— security/audit logs,

— routine inspections,

— users trained to identify and report information security incidents.

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

It is also important to recognize that network security is a dynamic concept. It is therefore essential that security staff are keep up to date with developments in the field and that the VPN and supporting technologies are working with the most current security patches and fixes available from vendors.

Further information on all of the above is provided in ISO/IEC 18028-1, ISO/IEC TR 15947, ISO/IEC 18043, ISO/IEC TR 18044 and ISO/IEC 17799.

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex A
(informative)

Technologies and protocols used to implement VPNs

A.1 Introduction

This informative annex presents examples of the typical technologies and protocols used to implement VPNs. It is not intended to present an exhaustive list, or to promote one particular technology or protocol over another.

Clause A.5 presents a summary comparison of the security features of VPN protocols.

A.2 Layer 2 VPNs

A.2.1 Frame Relay

Frame Relay is based on X.25 packet switching technology. In Frame Relay, the frames used for data transactions are of variable size. In addition, any error-control mechanism is the responsibility of only the sender and the recipient end, which results in high-speed data transmissions. It uses two types of circuits for transmitting data: Permanent Virtual Circuits (PVCs) and Switched Virtual Circuits (SVCs). PVCs are virtual paths through a private network (e.g. owned by the network service provider) in which the end points of the connections are defined by the network administrator. SVCs are more transient virtual paths (typically through an extranet) in which the end points of the connections are defined by the network users at the time of their call initiations.

A.2.2 Asynchronous Transfer Mode (ATM)

ATM is a PVC-based digital switching technology that can support audio, video, and data signals. It uses frames or packets of fixed size for this purpose. These packets (or 'cells') are queued before transmission and processed asynchronously irrespective of other related cells, which makes the ATM transmission faster than other switching technologies.

A.2.3 Multi Protocol Label Switching (MPLS)

MPLS is a technology, developed for use in inter-network routing, whereby labels are assigned to individual data paths or flows, and used to switch connections, overriding normal routing protocol mechanisms. It typically enables IP-based VPNs to be deployed across ATM-based networks. During a transmission, the initial MPLS device that receives an IP packet encapsulates it using an assigned MPLS label. Subsequently, this MPLS label, rather than the actual IP header, is used for routing the packets across the WAN. On the edge of the ATM-based network, when the packet is about to access the external IP-based infrastructure (e.g., the Internet) the MPLS label is then stripped off.

MPLS supports Class of Service (CoS) and Quality of Service (QoS), enabling different types of traffic (e.g. voice, video, messaging) to be prioritized in its transition over a network.

A major risk when using MPLS technology for high bandwidth traffic such as voice/video is the potential for poor quality of signal due to end-to-end latency delays, particularly where different network bearers and translation is employed.

MPLS is defined in a series of IETF RFCs, including RFC 3031 (Multiprotocol Label Switching Architecture), RFC 3032 (MPLS Label Stack Encoding) and RFC 3036 (Label Distribution Protocol (LDP) Specification).

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.2.4 Point-to-Point Protocol (PPP)

PPP was designed to send data across dial-up or dedicated point-to-point connections. PPP encapsulates IP, IPX (Internet Packet Exchange Protocol), and NetBEUI packets within PPP frames, and then transmits the PPP-encapsulated packets across a point-to-point link. PPP is typically used as the dial-up protocol between a client device and a remote access server.

The OSI Layer 2 protocols depend heavily on the features originally specified for PPP.

Detail is provided in IETF RFC 1661 (Point-to-Point Protocol).

A.2.5 Layer 2 Forwarding (L2F) Protocol

L2F is a transmission protocol that allows dial-up access servers to frame dial-up traffic in PPP and transmit it over WAN links to an L2F server (a router). The L2F server then unwraps the packets and injects them into the network. Unlike L2TP, L2F has no defined client. Note that L2F functions in compulsory tunnels only. L2F does not provide data confidentiality; traffic transits as clear text. L2F will eventually be replaced by L2TP.

Detail is provided in IETF RFC 2341 (Cisco Layer Two Forwarding (Protocol) "L2F").

A.2.6 Layer 2 Tunneling Protocol (L2TP)

L2TP allows IP, IPX, or NetBEUI traffic to be encrypted and then sent over any medium that supports point-to-point datagram delivery, such as IP, X.25, Frame Relay, or ATM.

It is a network protocol that encapsulates PPP frames to be sent over IP, X.25, Frame Relay, or Asynchronous Transfer Mode (ATM) networks. When configured to use IP as its datagram transport, L2TP can be used as a tunneling protocol over the Internet. L2TP can also be used directly over various WAN media (such as Frame Relay) without an IP transport layer. L2TP over IP internets uses UDP and a series of L2TP messages for tunnel maintenance. L2TP also uses UDP to send L2TP-encapsulated PPP frames as the tunneled data. The payloads of encapsulated PPP frames can be encrypted and/or compressed.

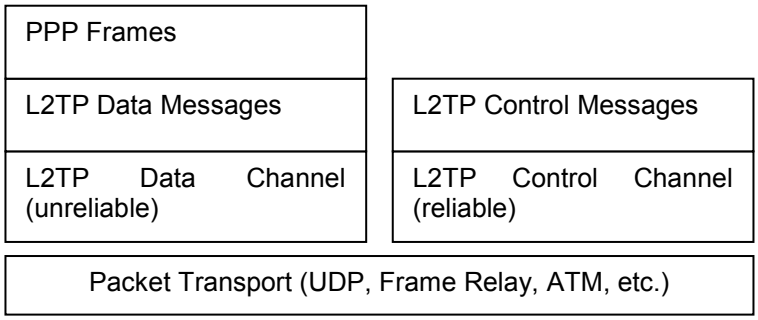

Figure 3 — Layer 2 Tunneling Protocol structure

Figure 3 depicts the relationship of PPP frames and Control Messages over the L2TP Control and Data Channels. L2TP utilizes two types of messages, control messages and data messages. Control messages are used in the establishment, maintenance and clearing of tunnels and calls. Data messages are used to encapsulate PPP frames being carried over the tunnel. Control messages utilize a reliable Control Channel within L2TP to guarantee delivery. Data messages are not retransmitted when packet loss occurs. PPP Frames are passed over an unreliable Data Channel encapsulated first by an L2TP header and then a Packet Transport such as UDP, Frame Relay, ATM, etc. Control messages are sent over a reliable L2TP Control Channel which transmits packets in-band over the same Packet Transport.

Traditionally, secure VPNs were set up using specialized hardware and proprietary protocols such as L2TP. There are known security vulnerabilities with this and many secure VPN implementations are instead built on IPsec or SSL.

Detail is provided in IETF RFC 2661 (Layer 2 Tunneling Protocol).

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.3 Layer 3 VPNs

A.3.1 IPsec

IPsec is a framework designed by the IETF as an end-to-end mechanism for ensuring data security in IP-based communications. IPsec defines OSI Layer 3 protocol standards that support the secure transfer of information across an IP internetwork. IPsec can be envisioned as providing an alternative layer to IP below the TCP layer. The IPsec layer is controlled by a security policy on each hardware device and a negotiated security association between the sender and receiver.

IPsec provides two separate protocols that ensure data confidentiality and data integrity. The Authentication Header (AH) protocol provides source authentication and integrity without encryption, and the Encapsulating Security Payload (ESP) protocol provides authentication; it also provides integrity and/or encryption. Either protocol can be implemented in transport mode, in which for ESP the OSI transport layer data only is protected, or in tunnel mode, in which an entire IP packet is encapsulated. The AH protocol protects the entire IP packet. Both AH and ESP protocols can provide replay protection.

An IPsec tunnel consists of a tunnel client and tunnel server, which are both configured to use IPsec tunneling and a negotiated encryption mechanism. Use of the IPsec ESP Tunnel Mode allows IP datagrams to be encrypted and then encapsulated inside another IP datagram, which can then be sent across a private or public IP internetwork such as the Internet. Upon receipt, the tunnel server processes the plain text IP header, verifies the integrity of the encapsulated datagram, and decrypts the encapsulated datagram to retrieve the original payload IP packet. IPsec Tunnel Mode has the following features and limitations:

— It supports IP traffic only;

— It is controlled by a security policy — a set of filter-matching rules. This security policy establishes the encryption and tunneling mechanisms available in order of preference and the authentication methods available, also in order of preference. As soon as there is traffic, the two machines perform mutual authentication, and then negotiate the encryption methods to be used. Thereafter, all traffic is encrypted using the negotiated encryption mechanism, and then wrapped in a tunnel header.

IPsec also contains a component to support authentication, authorization, security association negotiation, key establishment and management.

The IPsec protocol covers all aspects of VPN setup, from initial key negotiation to final tunnel setup, and will allow the choice of a large number of encryption and integrity solutions. The complexity of IPsec has lead to a large number of ambiguities, contradictions, inefficiencies and weaknesses (e.g. the vulnerability of the session setup to man-in-the-middle and spoofing attacks where a pre-shared key is shared across a group of endpoints). Common problems typically result from weak configurations caused by the complexity of IPsec.

IPsec has been defined in a series of IETF RFCs, notably RFCs 2401, 2402 and 2406.

A.4 Higher Layer VPNs

A.4.1 Secure Socket Layer (SSL)

SSL is typically used for securing transactions across networks and has been commonly utilized in web browser/server technology. It runs as a layer inserted between the application and TCP/IP and is widely used with HyperText Transfer Protocol (HTTP) where it is known as HyperText Transfer Protocol Secure (HTTPS).

The SSL protocol used for VPN traffic is the same as that used to secure browser datastreams. A Public Key Infrastructure (PKI, either private or public) will issue certificates for distribution to each VPN endpoint. Where an SSL endpoint sends its certificate, the receiver may use PKI facilities to authenticate the authenticity of the certificate and its sender. If mutual authentication is performed, these certificates will allow the exclusion of a man-in-the-middle attack, but may still be susceptible to spoofing where a single SSL endpoint certificate is shared across a number of devices.

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

As part of the SSL session setup, the two endpoints negotiate a ‘crypto-suite’ which is a predefined combination of encryption, hash, and key exchange methods which will define the actual level of protection for confidentiality and integrity of the exchanged data.

A.4.2 Secure Shell

Secure Shell is historically associated with Unix systems, where it is used as to gain secure access to the command interface and other running applications by its use to create and maintain secure VPNs. It relies on each participating system generating an asymmetric key pair, keeping the private key secure locally, and sharing the public key with systems which have a requirement to send data to the first system.

Unlike SSL and IPsec, public keys are not authenticated in a formal PKI. Instead, the public key is used to ‘sign’ information used to authenticate the sender and to create a generated shared secret on both systems. At this time, a symmetric encryption algorithm is selected and a key generated for use in data transfer. Other authentication mechanisms also exist e.g. for password authentication. Secure Shell may also be used between computer systems to create a secure tunnel through which other protocols may be directed.

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.5 Comparison of typical VPN protocol security features

The following table presents a comparison of typical VPN protocol security features.

VPN Type	Technology/ Protocols	User Authentication	Data Encryption	Key Management	Integrity Checking
Layer 2 VPNs	Frame Relay	-	-	-	-
	ATM	-	-	-	-
	MPLS	-	-	-	-
	PPP	-	-	-	-
	L2F	-	-	-	-
	L2TP	Simple CHAP-like	-	-	-
Layer 3 VPN	IPsec	Certificate based (packet) Pre-shared secret keys	Negotiable Several algorithms (packet)	IKE	Negotiable
	IPsec with L2TP	Certificate based (packet) Pre-shared secret keys	Negotiable Several algorithms (packet)	IKE	Negotiable
	MPLS	-	-	-	-
Higher Layer VPNs	SSL	Certificate-based	Negotiable	Negotiable	Negotiable
	Secure Shell	System-generated key pair (not certificated)	Negotiable	Exchange of public keys to data sender	Negotiable

Table 1 —VPN Basic Protocols and VPN Functional Areas

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Bibliography

[1] ISO/IEC 10181-1:1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview* (ITU-T X.810)

[2] ISO/IEC 11770-1:1996, *Information technology — Security techniques — Key management — Part 1: Framework*

[3] ISO/IEC 27005:— [1)], *Information technology — Information security risk management*

[4] ISO/IEC 13888-1:2004, *IT security techniques — Non-repudiation — Part 1: General*

[5] ISO/IEC TR 14516:2002, *Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services*

[6] ISO/IEC TR 15947, *Information technology — Security techniques — IT intrusion detection framework*

[7] ISO/IEC 18043, *Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems*

[8] ISO/IEC TR 18044:2004, *Information technology — Security techniques — Information security incident management*

[9] NIST-800, NIST Special Publications 800 series on Computer Security, USA

[10] RFC 1352, *SNMP Security Protocols*, IETF, July 1992

[11] RFC 1661, *Point-to-Point Protocol*, IETF, July 1994

[12] RFC 1918, *Address Allocation for Private Internets*, IETF, February 1996

[13] RFC 2196, *Site Security Handbook*, IETF, September 1997

[14] RFC 2341, *Cisco Layer Two Forwarding (Protocol) "L2F" (historic)*, IETF, May 1998

[15] RFC 2401, *Security Architecture for the Internet Protocol*, IETF, November 1998

[16] RFC 2402, *Authentication Header*, IETF, November 1998

[17] RFC 2406, *Encapsulating Security Protocol*, IETF, November 1998

[18] RFC 2407, *IPsec Domain of Interpretation (IPsec DoI)*, IETF, November 1998

[19] RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*, IETF, November 1998

[20] RFC 2409, *Internet Key Exchange (IKE)*, IETF, November 1998

[21] RFC 2411, *IP Security Document Roadmap*, IETF, November 1998

[22] RFC 2637, *Point-to-Point Tunneling Protocol (informational)*, IETF, July 1999

1) To be published. (Revision of ISO/IEC TR 13335-3:1998 and ISO/IEC TR 13335-4:2000.)

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

[23] RFC 2661, *Layer 2 Tunneling Protocol*, IETF, August 1999

[24] RFC 2828, *Internet Security Glossary*, IETF, May 2000

[25] RFC 3031, *Multi-Protocol Label Switching Architecture*, IETF, January 2001

[26] RFC 3032, *MPLS Label Stack Encoding*, IETF, January 2001

[27] RFC 3036, *Label Distribution Protocol (LDP) Specification*, IETF, January 2001

[28] X.25, *Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit*, ITU-T, October 1996

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ICS 35.040

Price based on 21 pages

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale