INTERNATIONAL STANDARD

ISO/IEC 27033-5

First edition
2013-08-01

Information technology — Security techniques — Network security —

Part 5:
Securing communications across networks using Virtual Private Networks (VPNs)

Technologies de l'information — Techniques de sécurité - Sécurité de réseau —

Partie 5: Sécurité des communications au travers des réseaux utilisant des réseaux privés virtuels (VPNs)

Reference number
ISO/IEC 27033-5:2013(E)

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 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT security techniques*.

This first edition cancels and replaces ISO/IEC 18028-5:2006, 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.)

Information technology — Security techniques — Network security —

Part 5: Securing communications across networks using Virtual Private Networks (VPNs)

1 Scope

This part of ISO/IEC 27033 gives guidelines for the selection, implementation, and monitoring of the technical controls necessary to provide network security using Virtual Private Network (VPN) connections to interconnect networks and connect remote users to networks.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

ISO/IEC 27005:2011, *Information technology — Security techniques — Information security risk management*

ISO/IEC 27033-1:2009, *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 7498 (all parts), ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, and ISO/IEC 27033-1 apply.

4 Abbreviations

For the purposes of this document, the abbreviated terms given in ISO/IEC 27033-1 and the following apply.

AH	Authentication Header
ESP	Encapsulating Security Payload
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
L2F	Layer Two Forwarding (Protocol)
LDP	Label Distribution Protocol
MPPE	Microsoft Point-to-Point Encryption
MPLS	Multi-protocol Label Switching
NAS	Network Area Storage
OSI	Open Systems Interconnection
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
WAN	Wide Area Network

5 Document structure

The structure of ISO/IEC 27033-5 comprises:

— an overview of VPNs (see clause 6),

— security threats associated with VPNs (see clause 7),

— security requirements derived from threat analysis for VPNs (see clause 8),

— security controls associated with typical network scenarios and network technology areas using VPNs (see clause 9),

— various design techniques for VPNs (see clause 10).

6 Overview

6.1 Introduction

VPNs have developed rapidly as a means of inter-connecting networks and as a method of connecting remote users to networks.

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.

An example representation of a VPN, with the secure data channel connecting an end user to a gateway across a public network and a secure data channel connecting two gateways across a public network, is shown in Figure 1 below.

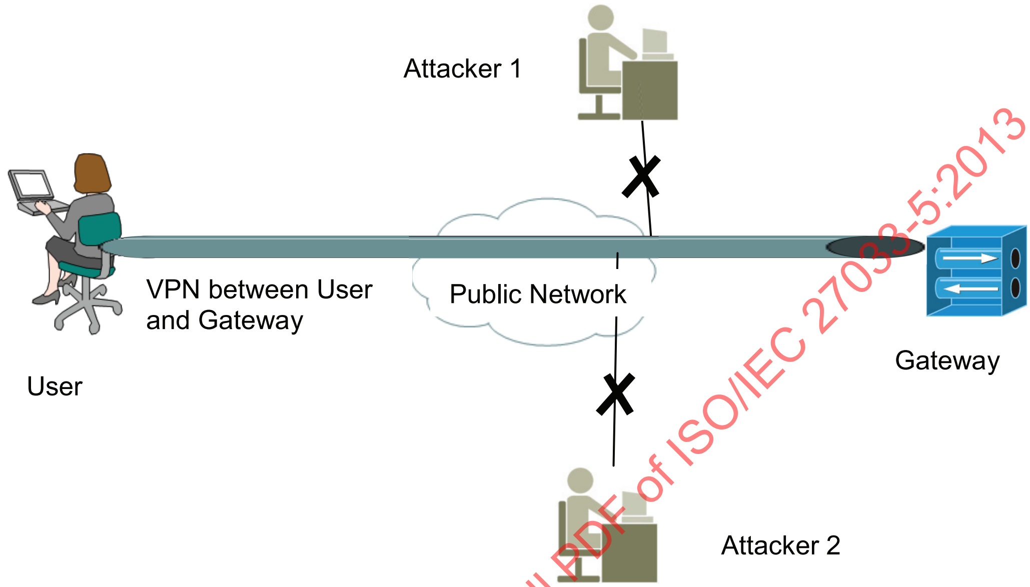

Figure 1 — Example representations of a VPN

Remote access using a VPN is implemented over the top of a normal point-to-point connection. The normal point-to-point connection between the local user and the remote locations is established first. 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.

6.2 Types of VPNs

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

Architecturally, VPNs comprise of 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.

— 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.

7 Security Threats

For the foreseeable future, organizations can expect increasingly sophisticated attacks to be mounted against their systems. Attempts at unauthorized access can be malicious, for example leading to a Denial-of-Service attack, the misuse of resources, or the access to valuable information.

Generally speaking threats against a VPN can be in the form of Intrusions or Denial of Service (DoS).

Intrusions happen when an outsider or malicious perpetrator takes control over part of your network; this can be a computer or other networking device (including mobile devices).

Intrusions may come from any location that has connectivity to your/the network. These attacks can come from other VPNs, the internet or the service provider core itself. The protection against these types of attacks comes from the ability to filter unwanted traffic from unwanted sources on network's ingress points. One of the typical examples of intrusion is the unauthorized access to the secure tunnel by an unauthorized entity.

This can be difficult in some VPN design models which lack centralization as all sites connect to each other without traffic control.

DoS attacks are another type of threat against a VPN. Both DoS attacks and intrusions can come from another VPN, the internet or the service provider core.. The main difference between the two types of attacks is that for DoS attacks the attacker needs to get access or have control over one of your pieces of equipment.

DoS attacks against the service provider devices can also cause a denial of service to some parts of your VPN. Although it might be hard to sometimes protect your network against DoS attacks, the main protection against them lies in the good network design of the VPN.

Security issues for 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).

8 Security Requirements

8.1 Overview

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.

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

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

— integrity of data 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.

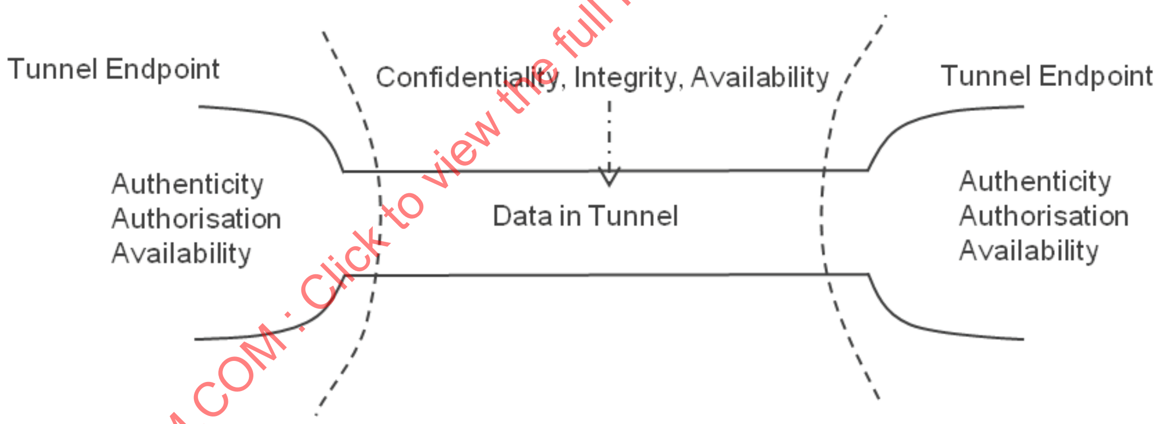

Figure 2 — Generic security requirements of VPNs mapped onto the underlying tunnel

Each of these requirements is discussed in detail below.

Clause 9 also discusses the types of security controls used to implement secure VPNs.

8.2 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 27033-1 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 endpoints should also not be neglected (see 8.7).

8.3 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.

8.4 Authenticity

Authenticity of information crossing public IP networks should be provided between participating peers in a VPN. 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 received has originated from the correct authorized source.

8.5 Authorization

The tunnel establishment and operating process should be supported by authorisation controls and should include ACLs. This ensures that each end of the tunnel that it is communicating with is an authorised partner end-point, which may be a remote-access system, and that data and code received have originated from an authorized source.

8.6 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.

8.7 Tunnel Endpoint Security

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 the use of packet filter or firewall technology. See 10.4.2 (Endpoint security) and 10.4.3 (Termination security) for further details.

9 Security Controls

9.1 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.

NOTE Even if data is encrypted the presence of data flow might be just as important as the data which is communicated. For instance if the endpoints of the VPN can be determined the individual user's location can also be determined. This poses a risk to the individual's privacy and in the case of law enforcement or military it might compromise their mission.

9.2 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.

10 Design Techniques

10.1 Overview

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 ensure that data flowing between tunnels and the underlying networks is 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.

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

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.

10.2 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.

10.3 VPN management aspects

When considering the use of VPNs all those with 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.

10.4 VPN architectural aspects

10.4.1 Overview

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

— endpoint security,

— termination security,

— malicious software protection,

— authentication,

— intrusion detection and prevention system,

— security gateways (including firewalls),

— network design,

— other connectivity,

— split tunneling,

— audit logging and network monitoring,

— technical vulnerability management,

— public network route encryption

Each of these aspects is summarized below.

10.4.2 Endpoint security

The function of a VPN is to provide a secure communication channel across some network medium. 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.

In order to smoothly operate endpoint security control, the number of aggregating endpoints should be minimized.

Some endpoint user devices (e.g. mobile/teleworking computing equipment) used for remote access may not be under the same management control as 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 27002 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.

10.4.3 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 method for VPN termination is deployment of dedicated VPN endpoints in perimeter networks, 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.

NOTE Intermediate zone will be discussed as perimeter networks or DMZ in ISO/IEC 27033-4

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.

10.4.4 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 that is executed by the receiver (such as code). Many programs allow code (script) embedded in data that looks inconspicuous. 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 27002.

NOTE Provision should be made for "duress codes" for end-point security, especially when particularly sensitive information could be involved. The duress code should possibly still allow access in order to protect the compromised end-user; however it could trigger additional logging and tracking, and alert the relevant management to the situation.

10.4.5 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 11770-1 and ISO/IEC 27002.

10.4.6 Intrusion Prevention and detection system (IPDS)

The need for Intrusion Detection and Prevention System (IPDS) technology should be considered. An IDPS 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. It should be noted 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 27039.

10.4.7 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 27033-4.

10.4.8 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 DMZ.

10.4.9 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.

10.4.10 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 by attacks 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.

10.4.11 Audit logging and network monitoring

In common with all other security technologies, the chosen VPN solution should maintain 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.

10.4.12 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.

10.4.13 Public network route encryption

Routing through a 3rd party/untrusted network over a static tunnel makes the VPN susceptible to network analysis. As mentioned in 9.1, even if data encryption is utilized, the existence of the tunnel and its endpoints would still not be hidden.

In VPN architectures where endpoint obfuscation is a requirement, controls are required to mask source and destination locations of VPN users. Implementing these controls would be challenging in itself seeing as the VPN operator is not in control of 3rd party/untrusted network. Certain technologies exist which might provide obfuscation of source and destination IP within 3rd party network e.g. Virtual Proxies and The Onion Router Project. The legal implications of running such tools will need to be discussed and approved by 3rd party network providers prior to utilizing these tools.

10.5 VPN technical considerations

10.5.1 Background

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,

— VPN device management, and

— VPN security monitoring.

Each of these aspects is discussed below.

10.5.2 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.

10.5.3 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.

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.

11 Guidelines for Product Selection

11.1 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.

11.2 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