

# CORPORATE REMOTE ACCESS

LAHTI UNIVERSITY OF APPLIED SCIENCES  
Faculty of Technology  
Telecommunications Technology  
Bachelor's Thesis  
Spring 2009  
Erpo Eronen

Lahti University of Applied Sciences  
Degree Programme in Technology

ERONEN, ERPO:

Corporate remote access

Bachelor's Thesis in Telecommunications, 68 pages, 0 appendixes

Spring 2009

## ABSTRACT

---

The objective of this thesis was to find a suitable, cost efficient and easy-to-use secure remote access solution for the Andritz Group. Currently these secure remote connections are provided using Check Point IPsec VPN connections. However, there is a need for more precise access restriction and a cut in management costs. Because of these reasons Andritz Group piloted products of the Juniper Networks Secure Access series. Secondary reasons for choosing Juniper SSL VPN were the market leading technology offered by Juniper and previous co-operation with Juniper Networks.

There are several ways to provide users with secure remote connection to the company network. One way could be a leased line between the home office and the company network. However, leased lines are expensive and if users are required to work in different locations leased line connections are useless. Two other ways to create secure remote connection are IPsec VPN and SSL VPN solutions. These two use shared media, normally Internet, to create a connection between the client and the company network. Traffic is normally tunnelled or used via a device which acts as a gateway to the company network. IPsec VPN and SSL VPN solutions are far more cost efficient than leased lines and also multi-user capable.

The main requirements for the Andritz Group remote connections are high security, data integrity with strong user and device authentication. Because of this, certificates and virus protection software checks are used for connecting devices. If the client computer does not pass these tests, only limited access to the company's resources is granted. In addition to ensuring users identity, AD authentication and one-time-password are used for two-factor authentication.

SSL VPN was selected as a new secure remote access solution for the Andritz Group. The decision to change the functional IPsec VPN solution to SSL VPN was done mainly because of monetary, as well as administrative reasons. Check Point VPN requires client software to be installed to each computer that might need secure remote connection. Juniper SSL VPN, on the other hand, works by using a number of logged-in users. Because no installation of client software is required, administrative overhead is also reduced.

The Current AD structure and variety of applications used by the Andritz Group caused the biggest challenges in this project. However, these problems were solved in co-operation between the workstation, network and application departments. As a final outcome the company acquired a functional, strictly controllable and redundant remote access environment.

Key words: SSL VPN, Juniper Networks Secure Access, Check Point IPsec VPN

Tietoliikennetekniikan opinnäytetyö 68 sivua, 0 liitesivua

Kevät 2009

## TIIVISTELMÄ

---

Tämän opinnäytetyön tarkoitus on saada aikaan kustannustehokas, helppokäyttöinen ja Andritz Groupin tarpeisiin soveltuva turvallinen etäkäyttöratkaisu. Tähän asti etäkäyttöyhteydet on toteutettu käyttämällä Check Pointin IPsec VPN-ratkaisua, joka muodostaa suoran VPN-tunnelin asiakastietokoneen ja yritysverkon välille. Andritzin yritysverkossa on kuitenkin viime aikoina ilmennyt tarvetta tarkempaan verkkoresurssien rajoitukseen ja hallinnointikustannusten leikkaukseen. Näiden uusien tarpeiden ja onnistuneen aikaisemman yhteistyön johdosta Andritz Group pilotoi Juniperin Networksin Secure Access tuoteperheen laitteita, jotka valittiin Andritz Groupin SSL VPN -ratkaisuksi.

Turvallinen etäkäyttöyhteys voidaan toteuttaa usealla eri tavalla. Näihin kuuluvat kiinteät verkkoyhteydet yrityksen konttorin ja kotikonttorin välille sekä erilaiset VPN-yhteydet käyttäjän ja yrityksen verkon välillä. Koska kiinteät linjat ovat kalliita eivätkä palvele liikkuvaa toimistoa, on yritykselle hyödyllisempää toteuttaa etäkäyttö VPN-yhteyksillä. VPN-yhteydet käyttävät hyväkseen olemassa olevia verkkoja, kuten internetiä, luodakseen yhteyden työntekijän ja yrityksen verkon välille. VPN-yhteydet mahdollistavat koko liikenteen tunnelointiin, tai vain tietyn palvelun käytön välittäjä laitteen kautta. Lisäksi IPsec- ja SSL VPN-sovellukset ovat kiinteitä linjoja halvempia ja mahdollistavat mobiilin etäyhteyden usealla käyttäjälle samanaikaisesti.

Tärkeimmät vaatimukset Andritz Groupin etäkäyttöratkaisulle ovat korkea tietoturva, tiedon eheys sekä vahva käyttäjän ja päätelaitteen autentikointi. Tästä johtuen Andritzin etäkäyttö sovellus tarkistaa käyttäjän koneelta sertifikaatin ja virusten torjunta ohjelman ajantasaisuuden ja testien vaillinaisen läpäisy rajoittaa käyttäjälle annetuja oikeuksia. Tämän lisäksi käyttäjät tunnistetaan käyttäen kahta eri tunnistusmenetelmää; AD-tunnistusta ja kertakäyttösalasanaa, jolloin varmistetaan käyttäjän oikeellisuudesta.

SSL VPN valittiin Andritzin uudeksi etäkäyttöstandardiksi sekä kustannusten, että hallinnollisten syiden takia. Kustannussäästöjä tuo erityisesti Juniperin yhtäaikaisten käyttäjien määrään perustuva laskutus, kun taas Check Pointin VPN-ratkaisussa kaikkiin Andritz Groupin kannettaviin tietokoneisiin olisi tarvinnut ostaa erillinen VPN-lisenssi. Hallinnoinnin määrää voidaan vähentää, koska SSL VPN:n ei vaadi erillisen ohjelman asennusta.

Projektin suurimmat ongelmat aiheutuivat Andritzin AD rakenteesta ja yrityksen käytössä olevien eri ohjelmien yhteensopivuudesta SSL VPN:n laitteiston kanssa. Nämä ongelmat on kuitenkin pääosin ratkaistu, ja nyt meillä on käytössämme toimiva, helposti hallittava ja redundanttinen etäkäyttö ratkaisu.

Avainsanat: SSL VPN, Juniper Networks Secure Access, Check Point IPsec VPN

## CONTENTS

1	INTRODUCTION	1
2	VIRTUAL PRIVATE NETWORK	2
2.1	Virtual Private Networks in general	2
2.2	VPN topologies	3
2.3	Data encryption and decryption	5
2.4	Integrity of the data	7
3	VIRTUAL PRIVATE NETWORKING TECHNIQUES	9
3.1	OSI layer 1 VPN solutions	9
3.2	Public Switched Telephone Networks	10
3.3	Packet Switched Networks	11
3.4	IPsec	13
3.4.1	IPsec authentication header	14
3.4.2	Encapsulating Security Payload	15
3.4.3	Security association	17
3.4.4	IPsec Keying	18
3.4.5	IPsec VPN	19
3.5	SSL/TLS	21
3.5.1	SSL/TLS Handshake Layer	22
3.5.2	SSL/TLS Record	23
3.5.3	SSL/ TLS session	23
3.5.4	SSL VPN	25
4	AUTHENTICATION	30
4.1	Authentication in general	30
4.2	Certificates	30
4.2.1	Trusted certificates	31
4.2.2	Certificate Authority	32
4.2.3	Revoking certificates	33
4.2.4	Self-signed certificates	34
4.3	One time password	34
4.4	Digital fingerprint	35
4.5	Biometric authentication	36

4.6	Password authentication	38
4.7	Comparing authentication solutions	38
5	ANDRITZ GROUP AND ITS LINE OF INDUSTRY	40
5.1	History of the Andritz Group	40
5.2	Andritz Group today	41
5.3	Andritz Oy	42
5.4	Line of business	44
5.4.1	Pulp and Paper industry	44
5.4.2	Hydropower industry	44
6	COMPARISON OF VPN SOLUTIONS	45
6.1	Check Point VPN	45
6.1.1	Enhanced IPsec VPN Security	45
6.1.2	Check Point VPN remote access	46
6.2	Nortel SSL VPN	47
6.3	Checkpoint VPN vs. Juniper SSL VPN	48
6.4	Check Point VPN vs. Nortel SSL VPN / IPsec VPN	49
6.5	Juniper SSL VPN vs. Nortel SSL VPN / IPsec VPN	51
6.6	Result of comparison	52
7	REMOTE ACCESS SOLUTION FOR ANDRITZ GROUP CORPORATE NETWORK	53
7.1	Andritz Group's network environment	53
7.2	Andritz Group's original VPN solution	54
7.3	Juniper Networks SSL VPN – Secure Access	55
7.3.1	Juniper SSL VPN requirements	55
7.3.2	Accessing Juniper SSL VPN	56
7.3.3	Juniper Networks IVE	56
7.3.4	Juniper Networks Host checker	57
7.3.5	Juniper SSL VPN levels of access	57
7.4	Juniper SSL VPN solution for Andritz Group	58
7.5	Using Juniper SSL VPN	60
7.5.1	Configuration and administration of Juniper SSL VPN	61
7.5.2	Using Juniper Networks SSL VPN – Secure Access	63
7.6	Goals to be achieved by changing remote access method	65

8	PROJECT OVERVIEW AND RESULTS	66
8.1	Finding a suitable secure remote access solution	66
8.2	Requirements for the remote access solution	66
8.3	Results of the project	67
8.4	Future of the project	68
	SOURCES	69
	ATTACHMENTS	75

## ABBREVIATION LIST

AD	Active Directory is technology created by Microsoft, which provides variety of network services including: LDAP, Kerberos authentication and DNS-based naming
ADSL	Asymmetric Digital Subscriber Line, is network connection method that uses phonelines for transferring data
AES	Advanced Encryption Standard, is one of many block cipher methods
AH	Authentication Header, is authentication header of IPsec protocol
ARPANET	Advanced Research Projects Agency Network, is network used by United States Department of Defense
ATM	Asynchronous Transfer Mode, is an electronic digital data transmission technology
CA	Certificate Authority, usually some trusted third party who grants the certificate for requester
CPE	Customer Premises Equipment, device used to connect to the network e.g. ADSL modem
CRL	Certificate Revocation List, list of certificates no longer valid
CSU/DSU	Channel Service Unit/Data Service Unit, device used to connecting router to the T1 or E1 connector
DCE	Data Communications Equipment, e.g. ADSL modem

DES	Data Encryption Standard, a symmetric block cipher method
DHCP	Dynamic Host Configuration Protocol, network protocol which is used to hand out IP addresses
DMZ	Demilitarized Zone, part of communications network, which allows logical connections from the internet
DoS	Denial of Service, network attack which aims in paralyzing the network
DTE	Data Terminal Equipment, end point device which is trying to connect the network
ESP	Encapsulating Security Payload, used to encrypt IPsec protocol information
HMAC	Hashed Message Authentication Code, one of many keyed hash functions
HTTP	Hypertext Transfer Protocol, networking protocol used by web browsers
HTTPS	Hypertext Transfer Protocol Secure, combination of HTTP and network security protocol
ICV	Integrity check value, a fixed size block of data which is used to ensure data integrity
IETF	Internet Engineering Task Force, group of people responsible for standards used in internetworks
IKE	Internet Key Exchange, secure key exchange protocol used to create security associations in the IPsec protocol suite



IP	Internet Protocol, networking protocol used in TCP/IP networks
IPsec	Internet Protocol Security, tunneling protocol commonly used in internetworks
ISAKMP	Internet Key Exchange and Key Management Protocol, commonly used key exchange protocol
ISP	Internet Service Provider
IVE	Instant Virtual Extranet, operating system used by Juniper Networks Secure Access product family
L2TP	Layer 2 Tunneling Protocol, tunneling protocol used to support Virtual Private Networks
LAN	Local Area Network, computer network covering a small physical area
LDAP	Lightweight Directory Access Protocol, application protocol for querying and modifying directory services running over TCP/IP
MAC	Message Authentication Code, a short piece of information used to authenticate a message
MD5	Message-Digest algorithm 5, widely used cryptographic hash function
MPLS	Multiprotocol Label Switching, highly scalable, protocol agnostic, data-carrying mechanism

NAC	Network Access Control, an approach to computer network security that attempts to unify endpoint security
NAT	Network Address Translation, address translation technique
NTLM	NT LAN Manager, Microsoft authentication protocol used with the SMB protocol
OSI	Open System Interconnection Reference Model, layered model of networking protocols
OTP	One-Time-Password, secure password method used for more secure user authentication
PC	Personal Computer
PKI	Public Key Infrastructure, set of hardware, software, people and policies and procedures needed to create, manage, store, distribute, and revoke digital certificates
PPP	Point-to-Point Protocol, data link protocol, commonly used to establish a direct connection between two networking nodes
PSE	Packet Switching Exchange, device used to connect DCEs and DTEs inside a X.25 network
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuits
RA	Registration Authority, authority who receives an application for a certificate, works as a middle man between certificate requester and CA

RADIUS	Remote Authentication Dial In User Service, protocol used to authenticate the users
RC4	Rivest Cipher 4, most widely known stream cipher, it is used in popular protocols such as SSL, designed by Ron Rivest
RFC	Request For Comments, collection of internet standard published by IETF
SA	Secure Access, Juniper Networks SSL VPN product family
SA	Security Accosiation, trust relationship generated between two systems
SAM	Secure Application Manager, solution used by Juniper Networks SSL VPN, to allow user to connect and operate a single application
SMS	System Management Server, centralized management software developed by Microsoft
SMTP	Simple Mail Transfer Protocol, mail transfer protocol that uses the TCP protocol
SPI	Security Parameter Index
SSL	Secure Sockets Layer, data encryption protocol
SVC	Switched Virtual Circuit, temporary route in X.25 network
TCP	Transmission Control Protocol, connection oriented data transfer protocol

TLS	Transport Layer Security, data encryption protocol offspring of SSL
TTP	Trusted Third Party, external agent trusted by both parties
UI	User Interface
VA	Validation Authority, authority used to check authenticity of used certificates
WAN	Wide Area Network, geographically significant network
VC	Virtual Circuit, technique used by X.25, Frame Relay and ATM networks
VPN	Virtual Private Network
XOR	Exclusive OR, a type of logical disjunction on two operands that results in a value of true if and only if exactly one of the operands has a value of true

## 1 INTRODUCTION

Working from home or outside of the office has become more common since high speed internet connections have become more popular. Users are able to connect to their company's network and receive all the services like they would be able to inside the office. Due to increased popularity of high speed internet connections it makes sense to perform some of the required tasks from home, without the need to travel to the office in the middle of the night or early in the morning if something urgent is needed to be done.

The Andritz Group has a growing need for more restricted secure remote connection. Because of this need the original IPsec VPN (Internet Protocol secure Virtual Private Network) remote access solutions must be replaced with SSL VPN (Secure Sockets Layer Virtual Private Network) connections, which will allow the company to perform more detailed access restriction. Although there are several ways to provide secure remote access for a single user, none of these have the level of access control or ease of access that an SSL VPN solution provides.

The main goal of this thesis is to find and configure a scalable and cost efficient secure remote connection environment for the Andritz Group global network to replace the Check Point secure client solution they already have. A secondary goal is to find suitable host check requirements for the Andritz Group's internal users, subcontractors and business partners, in order to block insecure computers from accessing the company network.

Due to the highly classified nature of data used by remote users in the Andritz Group, this thesis also looks into strong user authentication solutions to be used in the Andritz Group SSL VPN. As users have different habits there should be at least a couple of different ways to perform the strong authentication. Since end users are not always that familiar with these kinds of applications it is crucial that the SSL VPN environment is easy for the end user to understand and use.

## 2 VIRTUAL PRIVATE NETWORK

### 2.1 Virtual Private Networks in general

VPN (Virtual Private Network) is described as a telecommunications network built for a company's personal use which overlays on a public network infrastructure, in most cases the Internet, as shown in FIGURE 1. The Public network infrastructure can also be physical leased line or a VC network (Virtual Circuit). VPN has two main topologies, site-to-site VPN and remote access VPN. (Perlmutter & Zarkower 2001, 10).

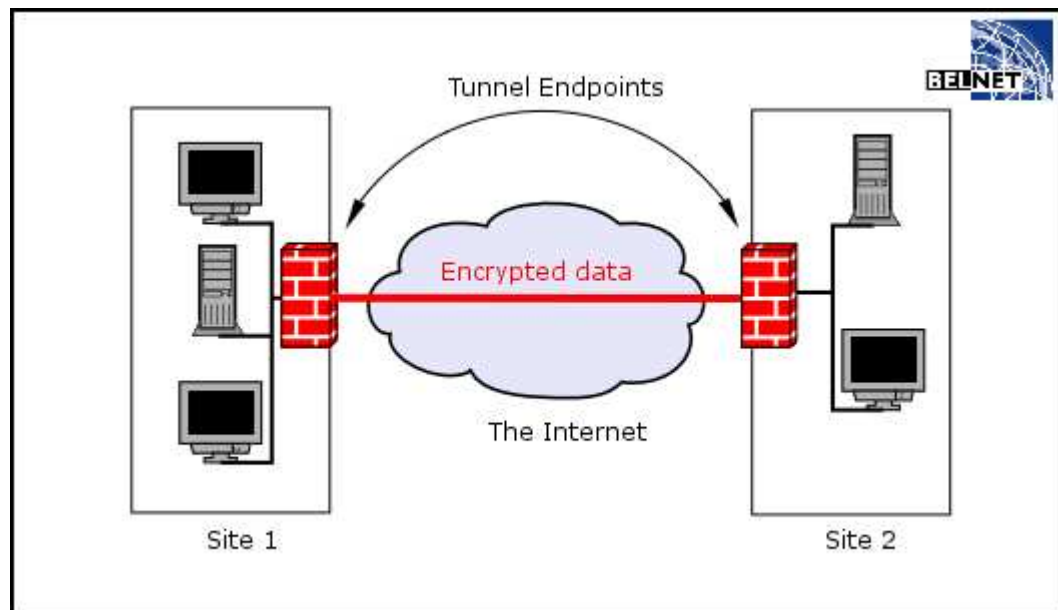


FIGURE 1. VPN over the Internet (Advanced technologies : VPN 2005).

Services based on VCs such as X.25, Frame Relay and ATM (Asynchronous Transfer Mode) are different from VPN over the Internet because in these solutions data has been made invisible to others in the Data Link layer and Network

layer of the OSI model (Open System Interconnection) a firewall is not necessarily required. (Perlmutter & Zarkower 2001, 11).

Another way of transferring data which covers all the definitions of Virtual Private Networking is leased line. A single leased line that is used to connect the remote office to the company network. These kinds of connections, as well as previously mentioned X.25, Frame Relay and ATM connections, are expensive compared to a VPN tunnel built over the Internet. (Perlmutter & Zarkower 2001, 11).

VPN connections use different layers of the OSI model to provide secure networking. For example leased physical lines are located on the first layer of the OSI model (also called physical layer), packet switched connections, such as Frame Relay and X.25 use data link layer of the OSI model. IPsec (Internet Protocol security) VPN uses an Internet layer of the Internet protocol suite which is roughly the same as the Network layer of the OSI model. VPN solutions like SSL VPN (Secure Sockets Layer VPN) use OSI layers from four till seven. (Wikipedia – SSL VPN 2009) (Wikipedia - Frame Relay 2009).

VPN traffic between CPE devices (Customer Premises Equipment) is tunneled. In its simplest form tunneling is encapsulating data packets inside each other. It is also possible to add features like encryption, integrity check, sender verification, address translation or packing of data when encapsulating data packets. (Perlmutter & Zarkower 2001, 11, 12).

## 2.2 VPN topologies

Virtual private networking has two main applications: Site-to-Site VPN and VPN remote access. Remote access VPN users connect to the company network via VPN remote access as shown in FIGURE 2. VPN remote access requires the VPN device, normally a firewall or router, and some software or VPN key on the client's computer to handle user authentication and to create the secure tunnel over the public network. (Perlmutter & Zarkower 2001, 12, 48).

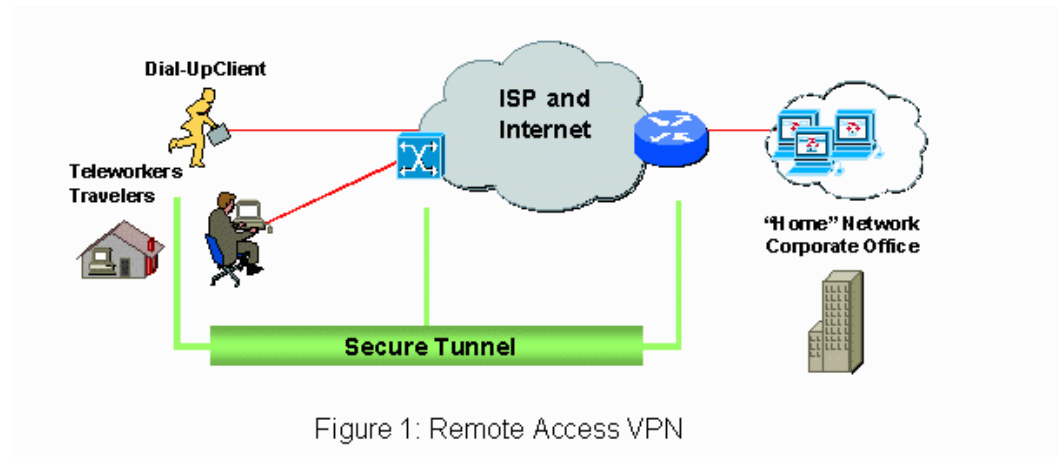


FIGURE 2. VPN remote access (Phifer 2001).

Another quite common VPN application is Site-to-Site VPN. In Site-to-Site VPN a secure tunnel is created for transferring files and other forms of data securely between two or more corporate LANs (Local Area Network), as shown in FIGURE 3. (Phifer 2001).

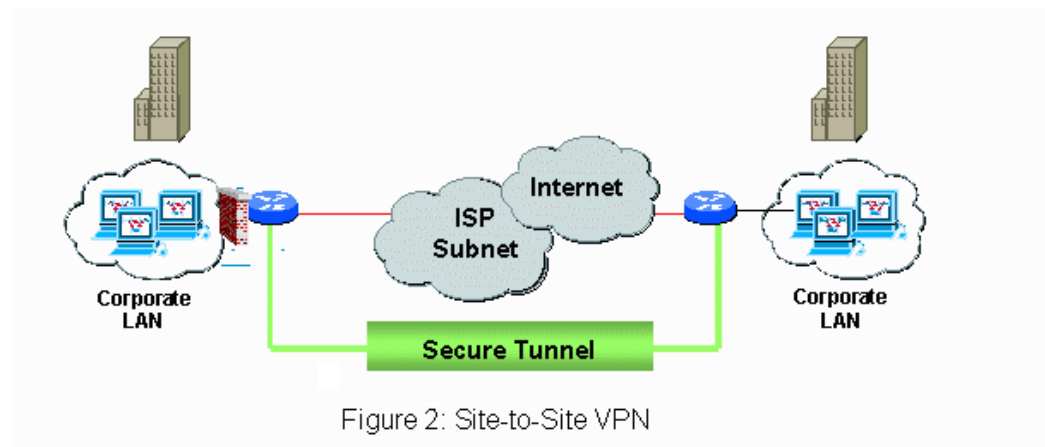


FIGURE 3. Site-to-Site VPN (Phifer 2001).

Point-to-Point connections between different offices are normally provided by a network layer of the OSI model. Generally Point-to-Point connections are created between firewalls or routers; encryption of traffic is done by a secret key or certificate. Certificates are a less complicated way of encryption and generally con-



sidered more secure than applying the same password for all the routers and firewalls of the network. In order for VPN to work, it is required to provide subnets used for VPN connections to the router or firewall responsible for the VPN connection. (Perlmutter & Zarkower 2001, 12; Phifer 2001).

It is common to have to authenticate both the user and the computer used for a VPN connection before a person is granted access to a virtual private network. User authentication is most commonly done by checking user credentials from the authentication server. For this process the RADIUS protocol is normally used. There are also many other ways to perform user authentication, many of which are more secure than password authentication. These methods are covered more thoroughly in chapter 4. (Wikipedia – Authentication 2009).

### 2.3 Data encryption and decryption

The main concerns of virtual private networking are encryption of outbound traffic, user authentication and authentication of devices used to remotely access company's resources. Authentication is used to verify the identity of people and devices participating in the secure remote connection session. If authentication is done properly it reduces the possibility of data theft. Well encrypted VPN traffic is worthless if the person who tries to interpret it does not possess the key required to decrypt the message. There are two generally used ways of encrypting the data: symmetric and asymmetric keying. (Perlmutter & Zarkower 2001, 12,106).

Symmetric key algorithms are a class of algorithms for cryptography that use trivially related, often identical cryptographic keys for both encryption and decryption. In order to successfully encrypt and decrypt data using symmetric key algorithms, both sender and receiver need to have knowledge of the keys to be used. Symmetric key algorithms can be divided into two groups, the one being stream ciphers and the other being block ciphers. (Wikipedia – Symmetric-key algorithm 2009).

Stream cipher techniques encrypt bits of the message one at a time and therefore stream cipher is executed faster and with lower hardware complexity than block cipher. Stream cipher typically uses XOR operation (Exclusive-OR) to mix plain text message with cipher bit stream, which may appear random but actually is not. Stream cipher is normally used in applications where the length of the plain text is not known beforehand, such as secure wireless connections. The most commonly used software planted stream cipher is the RC4 (Rivest Cipher 4) designed by Ron Rivest in the late 1980s while he was working for RSA Security. (Wikipedia - Stream cipher 2009).

In block cipher, data is encrypted as fixed-length blocks, for example 128 bits at a time. These blocks are encrypted one by one using a secret key and sent to the receiver. After data has been transferred, the receiver can decrypt the data using a secret key. The most widely known block ciphers are DES (Data Encryption Standard), Blowfish and AES (Advanced Encryption Standard). AES 256-bit is the most commonly used block cipher today. (Connected: An Internet Encyclopedia 2009).

Asymmetric key cryptography also known as public key cryptography uses two types of keys. Each person creates a public key that can be used to send encrypted information to this person, and also a private key which can be used to decrypt messages encrypted by the person's public key. Information encrypted with a public key must be decrypted with the corresponding private key, which makes it impossible for an unauthorized third party to decipher private messages sent to the possessor of the private key. Many companies have tried to create superior asymmetric keying techniques that would become a standard of asymmetric keying but so far no such technique has been released. Probably the best-known application of asymmetric cryptography is RSA keys. For more information, see chapter 4.3 one-time-password. (Wikipedia - Public-key cryptography 2009).

## 2.4 Integrity of the data

Cryptographic hash functions can be used in many applications. They work as a checksum for sent data. Hash functions can be used in authentication and they can work as digital fingerprints for detecting duplicate data files. In networking, hash functions are commonly used to assure data integrity. A cryptographic hash function takes an arbitrary block of data and returns a fixed-size bit string called the hash value. A cryptographic hash function is based on the hash value of a data block and an assumption that if data has been tampered during the transfer its hash value has also changed. The sending device calculates the hash value and adds it to the package. After transfer has completed receiving, the device checks that the value of the hash has not changed during the transfer. If hash values do not match, information is discarded. (Wikipedia - Cryptographic hash function 2009).

The fact that hash functions are fixed-length sometimes causes collisions. This happens when hash values generated for two strings of data are identical. Superiority of cryptographic hash functions is determined by comparing the amount of collisions generated. A hash function that is less likely to cause collisions is better than one which causes more collisions. The most commonly used cryptographic hash functions are SHA-1 and MD5 (Message-Digest algorithm 5). (Wikipedia - Cryptographic hash function 2009).

There are also keyed hash functions, where only a person who knows the key can count the hash value. Keyed hash functions create hash values based on data and a secret key provided by the user, as shown in FIGURE 4. (Wikipedia - Cryptographic hash function 2009).

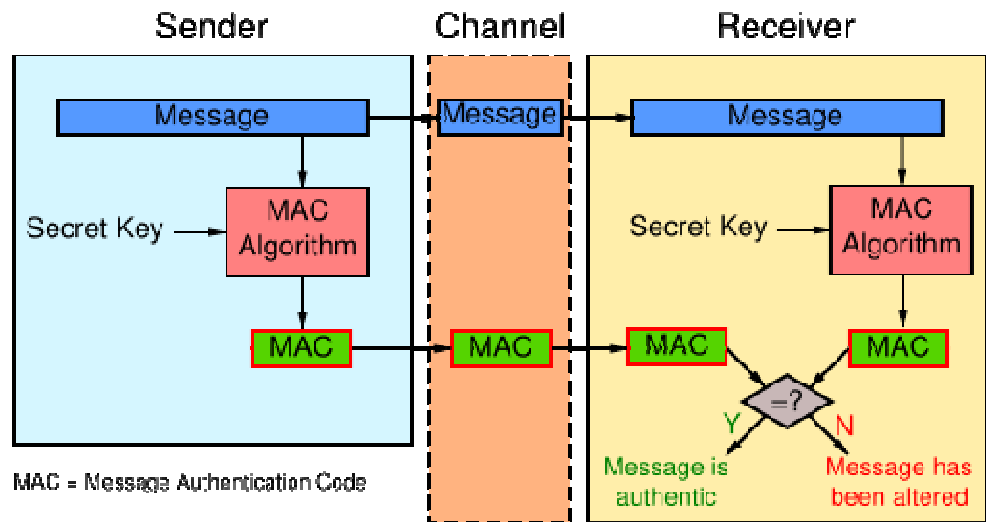


FIGURE 4. Keyed hash function (Wikipedia - Message authentication code 2007).

After a message is sent and received, the person who opens the message is prompted for the secret key used to generate the hash. After the key is provided, the system compares two MACs (Message Authentication Code) to each other and if they match, the message is successfully authenticated. HMAC is a commonly used keyed hash function, which is based on MAC, but because HMAC encryption is harder to crack it is more commonly used than its predecessor. (Wikipedia - Cryptographic hash function 2009).

### 3 VIRTUAL PRIVATE NETWORKING TECHNIQUES

#### 3.1 OSI layer 1 VPN solutions

The physical layer of the OSI model provides a VPN solution that is considered the golden standard of Virtual Private Networking, a physical network line between two places. Physical lines presented in FIGURE 5 are normally leased from the local phone company to connect two offices or an office and a home office. Client companies are able to choose between the clear channel T1 connection with transfer rate of 1.544Mbit/s and channeled E1 connection with transfer rate of 2.048Mbit/s. These days there are many more transfer rates available. These solutions also provide the invariable bandwidth and latency which are also definitions for the golden standard of Virtual Private Networking. (Perlmutter & Zarkower 2001, 35).

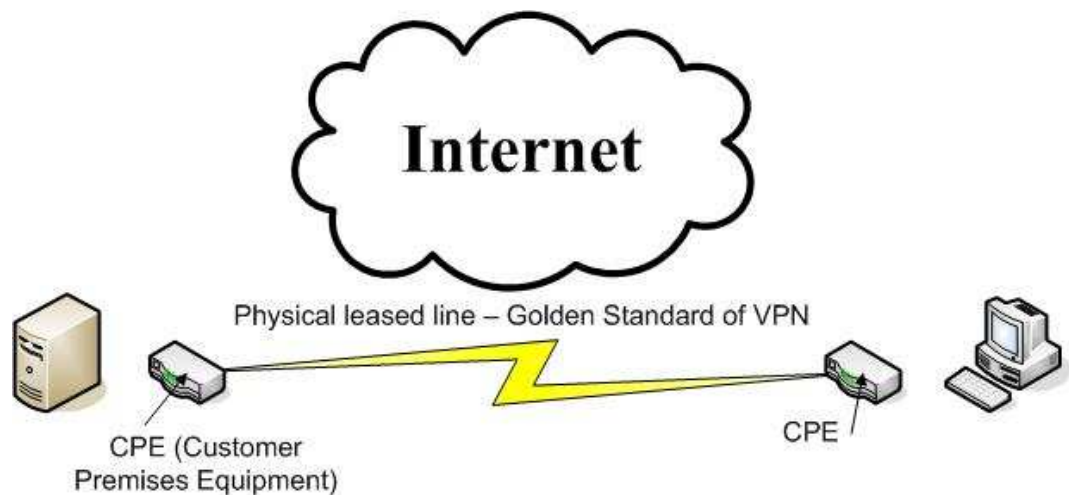


FIGURE 5. Physical leased line

While using a clear channel T1 connection, two physical connections, two CSU/DSU devices (Channel Service Unit/Data Service Unit) and two ports from the network router are required. A CSU/DSU device provides time synchronization, framing and signal to data conversion services of leased T1/E1 lines. When a channeled E1 connection is used, one physical connection, one CSU/DSU device and one port from network a router are required. The type of connection is dependant from the ISP's (Internet Service Provider) way of delivering network connection. ISPs in North America, Korea and Japan provide leased lines using T-carriers whereas E-carriers are commonly used in Europe. (Perlmutter & Zarkower 2001, 38).

Lately, leased physical lines have lost their standing on markets against VPN over thr Internet solutions, which is mainly because VPN solutions over the internet are more cost efficient and easy to set up. In rural areas such as China, it can take up to two months for a company to get a physical line or MPLS connectivity between two places whereas VPN over the Internet can be operational the next day. (Perlmutter & Zarkower 2001, 40; China Telecom 2008).

### 3.2 Public Switched Telephone Networks

Public switched telephone networks, also known as PSTNs are a commonly used solution for a remote user to access the company network. In PSTNs the connection is made between the client's modem and the modem in the company network. The modems are used to transform a digital signal into analog form, so it can be transmited via an analog telephone network. To create this connection either a Dial-up networking or Point-to-Point Protocol, later referred to as PPP, is used. (Perlmutter & Zarkower 2001, 49).

In Dial-up networking packets are transferred using the Internet Protocol, later referred to as IP. In PPP the user gets to choose which data transfer protocol will be used, after the connection has been established. PPP can also provide connection authentication, transmission encryption and data compression, which makes it

more secure than Dial-up Networking. PSTN is extremely suitable for rural areas, since the only requirement for the connection is finding a phone line, which should be possible almost anywhere in the world. (Wikipedia - Public Switched Telephone Network 2009).

### 3.3 Packet Switched Networks

ARPANET, also known as Advanced Research Projects Agency Network, developed by the United States Department of Defence was the first packet switched network and it became operational in 1969. However, the first widely used packet switched network standard X.25 was not released until 1973. X.25 is an ITU-T standard network layer protocol for packet switched wide area network communication. (Wikipedia - Packet Switched Network 2009).

The X.25 standard defines the interface between a subscriber DTE (Data terminal Equipment) and an X.25 network DCE (Data Communications Equipment). In X.25 networks the DCE is normally a router and the DTE is normally a client PC. Routing between the DCEs is done via a group of PSE (Packet switching exchange) devices, as shown in FIGURE 6. (Perlmutter & Zarkower 2001, 41).

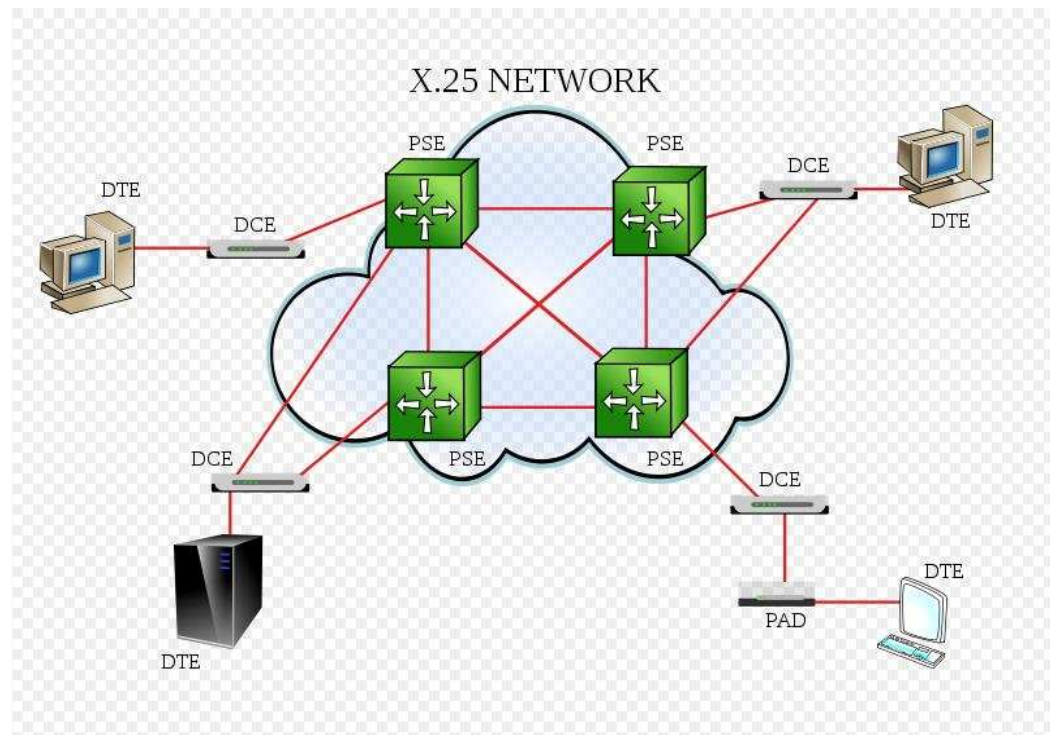


FIGURE 6. X.25 Wide area network topology (Wikipedia – X.25 2009).

A physical X.25 network is the same for all users, but inside the network VCs are used to create VPN type tunnels between the client networks. This way the clients only have an access to their own data. There are two types of VCs: SVCs (Switched virtual circuits) which are temporary, and PVCs (Permanent virtual circuits) which are permanent. Companies normally have one so-called virtual circuit end point, to which all other virtual circuits terminate. (Perlmutter & Zarkower 2001, 42).

The price of X.25, Frame Relay, and ATM connections is considerably lower than the cost of leased lines, because in these networks the costs can be divided between different users. However, in VC networks such as X.25, Frame Relay, and ATM the Internet Service Provider, also known as ISP, is responsible for routing the information inside the PSE field, and has to make sure that the data is not routed to a wrong network. (Perlmutter & Zarkower 2001, 43).



### 3.4 IPsec

IPsec (Internet Protocol security) is a framework of open standards for protecting communications over IP (Internet Protocol) networks through the use of cryptographic security services. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality, and replay protection. IPsec is dual a mode, end-to-end security scheme operating at the Internet layer of the Internet Protocol Suite. IPsec is a modern standard which does not require any measures from users after the initial sign-in process. After the IPsec connection has been formed, network traffic will be tunneled securely over the IP network. (Perlmutter & Zarkower 2001, 42; Wikipedia – IPsec 2009).

IPsec was first announced by IETF (Internet Engineering Task Force) in August of 1995 in the RFC document (Request for Comments) 1825 called Security Architecture for the Internet Protocol. Defining the IPsec made it possible for different vendors to start producing hardware independent solutions for secure networking. IPsec is based on three basic factors: authentication, encryption and key management. Even though many application and device manufacturers have their own solutions for the IPsec key management, it is most commonly based on the IKE protocol (Internet Key Exchange). Key management is a procedure where used encryption keys are negotiated or determined by the connecting parties. IPsec is designed to only authenticate devices used in connection, not the users. (Perlmutter & Zarkower 2001, 106).

IPsec has two modes of operation: the transport mode and the tunnel mode. In transport mode, only the payload of the IP packet is authenticated and/or encrypted. The routing of the packet stays the same, since the IP header is not modified or encrypted; however, while using the AH (Authentication Header), the IP addresses cannot be translated because this would invalidate the hash value. In transport mode the transport and application layers are always secured by hash, and therefore they cannot be modified. The transport mode is used for host-to-host communications. In a tunnel mode, the whole IP packet is authenticated and/or encrypted. Afterwards, the IP packet is encapsulated into a new IP packet with a

new header. To create virtual private networks for site-to-site, remote access connections and host-to-host communications a tunnel mode is used. (Wikipedia – IPsec 2009).

IPsec works as a framework for secure connection. Inside the frame different types of algorithms and parameters can be selected. In order to set up a functional IPsec connection between two places, it is required that corresponding parameters and algorithms are used in both ends of the connection. (Perlmutter & Zarkower 2001, 106).

### 3.4.1 IPsec authentication header

IPsec adds an AH field to a normal IP message, as shown in FIGURE 7. IPsec also changes the value of the frame's IP header to 51, which indicates that IPsec AH is used. The purpose of the AH is to guarantee connectionless integrity and data origin authentication of the IP packets. AHs can also be used to protect the connection against the replay attacks. This is done by using the sliding window technique and discarding old packets. The sliding window protocol works on a data link and transport layers of the OSI model. It is used to keep a record of the frame sequences sent and the respective acknowledgements received by both users. (RFC 2402 – Kent & Atkinson 1998, 1, 2).

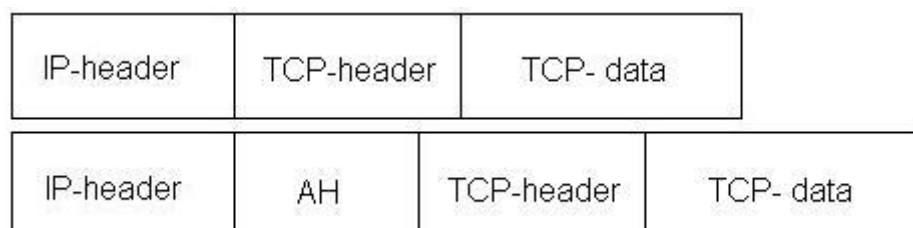


FIGURE 7. IP message without and with Authentication Header

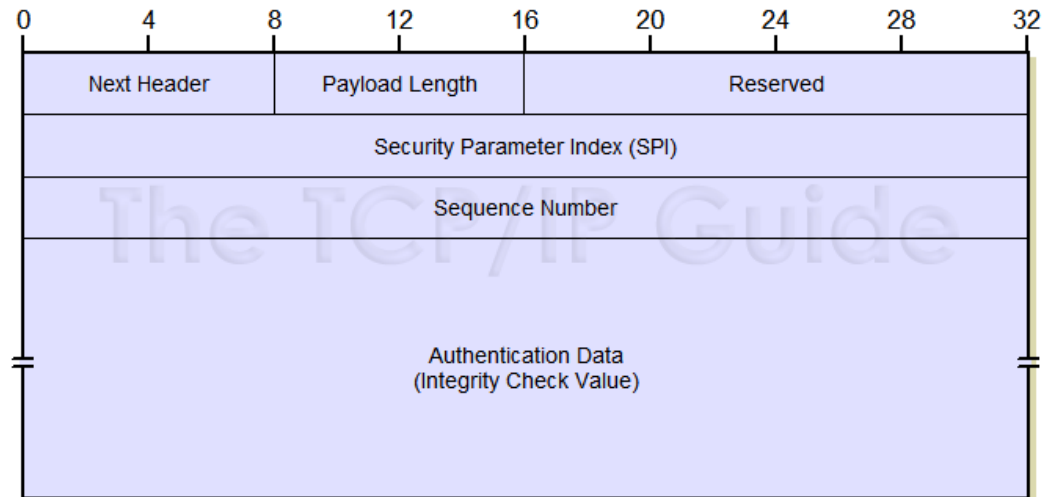


FIGURE 8. Authentication header (The TCP/IP guide 2005).

The structure of AH is presented above in FIGURE 8. Authentication data field is the main component of an AH and it has variable length containing the ICV (Integrity Check Value) that is used to authenticate the packet. It may also contain padding. Authentication Data field, as well as the whole AH must be a multiple of 32bits while using the IPv4 (Internet protocol version 4). When using IPv6 (Internet Protocol version 6) the length of the AH must be a multiple of 64 bits. (The TCP/IP guide 2005).

### 3.4.2 Encapsulating Security Payload

Another member of the IPsec protocol suite is ESP. ESP offers origin authenticity, integrity, and confidentiality protection of packets. ESP supports both encryption-only and authentication-only configurations, but using both encryption and authentication is recommended in order to achieve maximum security. IP packet header protection included in AH is not on the ESP's feature list. In a tunneled mode the whole inner packet is encapsulated, including the IP packet header, while the outer most header stays unprotected. Using ESP gives the IP packets a protocol number 50. (Wikipedia – Encapsulating Security Payload 2009).

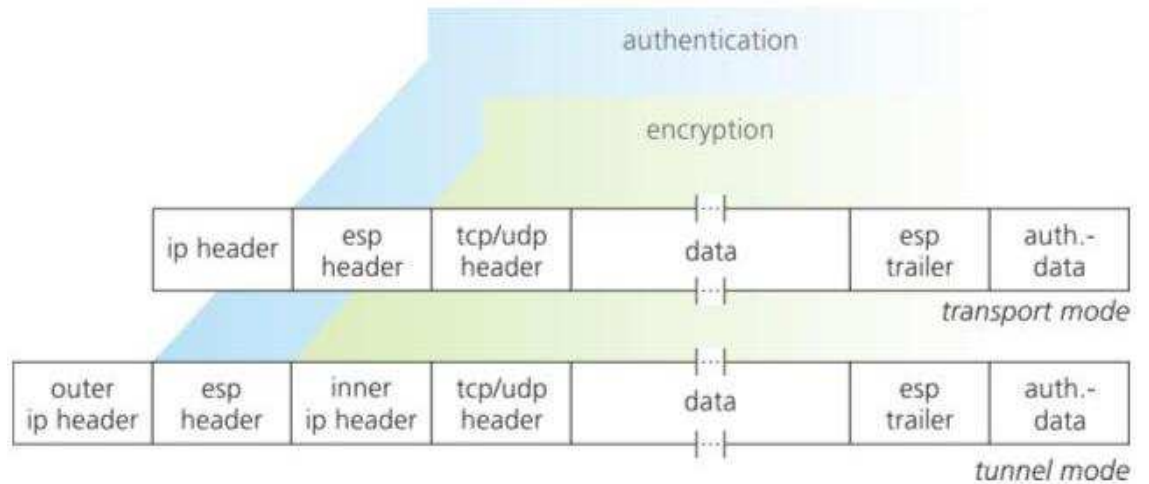


FIGURE 9. IP message with and without ESP (FIDIS – internet layer protocols 2007).

Using an ESP extends the IP-message frame by three additional fields as shown in FIGURE 9. Information between the ESP header and the ESP trailer is encrypted. In addition, the ESP performs integrity check for sent messages. The structure of an ESP packet is presented in FIGURE 10. (RFC 2406 – Kent & Atkinson 1998, 3).

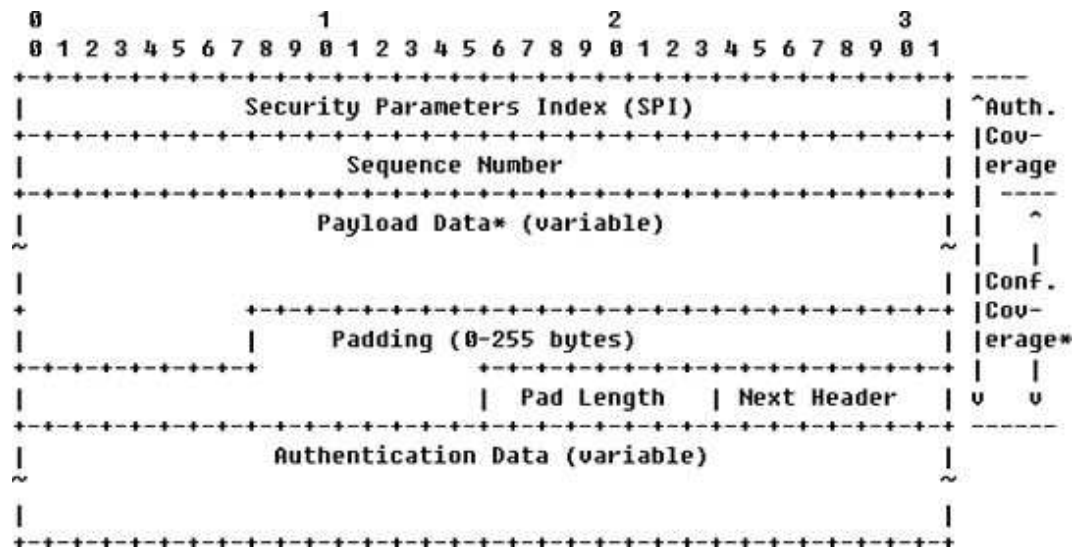


FIGURE 10. ESP packet diagram (RFC 2406 – Kent & Atkinson 1998, 2).

### 3.4.3 Security association

SA (security association) is the establishment of shared security information between two network entities to support secure communication; it is the core of an IPsec connection. SA may include cryptographic keys, initialization vectors or digital certificates. SAs are defined by a set of three parameters, called a triple. These three are: an SPI (Security Parameter Index), an IP destination address and a security protocol identifier. An IP destination address is the IP address of the device whose SA is established. (Wikipedia – Security Association 2008).

An SPI is a 32-bit number chosen to uniquely identify an SA for any connected device. The SPI is located inside the AH or ESP datagram and thus links each secure datagram to the SA. The SPI determines the integrity check of algorithm, encryption algorithm, algorithm key(s), and lease time for created key(s), algorithm lifetime and list of the IP addresses allowed to connect to the system. SPI services used can be personalized for each case, which makes it possible to exclude services that are not required. After an SPI is created it is saved to the SPI field of the packet. (RFC 2401 – Kent & Atkinson 1998, 20).

A functional IPsec connection requires exchange of SPI information between connecting devices. SA is normally a one-way channel, but if the connecting devices are required to change information between each other and two-way channels are used, both devices need to have a unique SPI in order to successfully complete the process. If the connecting devices use different protocols, for example AH and ESP, additional SPIs are required, which gives a total number of four SPIs. (RFC 2401 – Kent & Atkinson 1998, 20, 21).

#### 3.4.4 IPsec Keying

IPsec key management is normally done using the IKE protocol, but there are also other solutions developed by device and application manufacturers. Failure to integrate IPsec key management solutions as one has slowed down the spread of IPsec. The IKE protocol is the latest step in the evolution of IPsec key management, succeeding the Oakley and ISAKMP protocols. IKEv1 was developed because of the complexity of ISAKMP, but it too remained rather complex. Complexity of protocol was not solved until in IKEv2 which was much more, straightforward than its predecessor. The purpose of the IKE protocol is to negotiate, and provide authenticated keying material for security associations in a protected manner. IKE is a hybrid protocol combining ISAKMP, Oakley and SKME protocols previously used for internet key exchange. The medium which IPsec connections are built on are normally insecure (e.g. Internet), therefore extra caution should be taken to ensure secure key exchange. In order to provide the secure key exchange, IKE uses the asymmetric Diffie-Hellman protocol, which allows connected parties to negotiate a symmetric key used for encrypting the messages. IKE also supports certificate based authentication for connecting devices. (RFC 2409 – Harkins & Carrel 1998, 1, 4).

IKEv2 was released in December of 2005 in order to improve support for mobile devices and to provide general upgrades for the protocol. The biggest improvements compared to IKEv1 included improved resilience towards DOS (Denial of Service) attacks, reliability and state management, and standard mobility support. Standard mobility support is an extension for IKEv2 called MOBIKE, which provides IKEv2 and IPsec services for mobile and multihomed users. In IKEv1 there was a possibility of a dead state situation; this is encountered when both parties expected the other to initiate an action, which never eventuated. Reliability and state management service were added to IKEv2 to prevent dead state problems. Only the most important fixes and new features introduced by IKEv2 were covered in this chapter. (Wikipedia – Internet Key Exchange 2009).

### 3.4.5 IPsec VPN

An IPsec connection always has two parties: sender and receiver. The relationship between sender and receiver is called Security association (SA). SA is created by allocating sender and receiver the keys used for protecting the connection. These keys can be generated either statically or dynamically, by using one of the IPsec key exchange protocols. After both parties receive keys the SA is created. Connection between the parties involved in security association is always provided by the network layer of the OSI model. (Perlmutter & Zarkower 2001, 109).

When information is sent using an AH, the sender signs information with a private key created during the security association process. Security associated packets can be opened with the receiver's secret key. If ESP is used, the whole message is encrypted using an algorithm decided by connecting parties. After the encrypted message has been received, it will be decrypted using a reversal algorithm to the one it was encrypted with. As a result a clear text packet is received. Using AH prevents IPsec VPN traffic passing through NAT (Network address translation), because AH performs integrity check for IP addresses as well as data. (Perlmutter & Zarkower 2001, 109, 110).

IPsec VPN solutions normally combine VPN devices and VPN applications, between which the VPN connection is established. The VPN device is normally a server or a firewall that is located in the company's own premises. VPN application on the other hand is a piece of software running in a remote computer which is trying to connect to the corporate network. Site-to-Site VPN connections are normally done using a VPN device in both ends of the line. VPN remote connect favors application-based on VPN solution with VPN device at the other end. Hosting several simultaneous IPsec connections can be consuming for the VPN device, because it is required to calculate and keep track of many different keys and algorithms. (Perlmutter & Zarkower 2001, 112).

IPsec is a protocol which has built-in encryption tools, but it does not use a specific encryption algorithm, which makes it more flexible to use, since the user can choose the algorithm used to encrypt the data. Only the form of the encryption algorithm is determined by the IPsec protocol. This characteristic makes the IPsec protocol suite an easy base for creating new applications and devices, since there is no problem with compatibility. The IPsec protocol being well integrated into the IP protocol makes IPsec solutions easy to implement and use. (Perlmutter & Zarkower 2001, 113).

The fact that IPsec is integrated to IP protocol makes it incompatible with most of the other network protocols, which may in some situations cause extra work for the network administrator. However, this can be solved by tunneling the traffic first inside the IP packet and afterwards for IPsec. Even though IPsec is well standardized there are still some compliance issues between IPsec solutions provided by different vendors. IPsec only provides tools for authenticating the devices used to connect, for user authentication separate authentication methods must be used. (Perlmutter & Zarkower 2001, 113).

IPsec VPN applications normally require installing a piece of software to the client computer. In corporate networks where there might be hundreds or thousands of remote users, this means lots of work. IPsec is not fully compatible with Network Address Translation, also known as NAT, which adds some more problems to the equation. Since IPsec connections are always created on a network layer, it is a prominent platform for viruses and worms to infiltrate to the company network. (Perlmutter & Zarkower 2001, 115).



### 3.5 SSL/TLS

The Secure Sockets Layer protocol, later referred to as SSL, was created by Netscape Communications Corporation in 1994. It was first planned to be used for securing HTTP (Hypertext Transfer Protocol) connections between HTTP servers and Internet browsers. The SSL protocol was built to operate on the fourth layer of the OSI model called the Transport Layer. Because of this feature, SSL can be used to secure all TCP protocol based network traffic; these include many commonly used protocols such as Simple Mail Transfer Protocol, also known as SMTP, and Lightweight Directory Access Protocol, better known as LDAP. (Microsoft Technet 2009).

In 1999, the IETF (Internet Engineering Task Force) released a new standard Transport Layer Security version 1.0, later referred as TLS. The TLS protocol was based on the SSL version 3.0, which is why differences between these two protocols are minimal. The biggest difference between these two standards is the algorithm used to check data integrity; SSL uses the MAC algorithm, and TLS uses the HMAC algorithm. Even though differences between these two protocols are miniscule, they are not compatible. (Microsoft Technet 2009).

The TLS protocol is based on four sub-protocols called handshake protocol, change cipher spec, alert and record protocol, presented in FIGURE 11. TLS relies on lower level protocols like TCP to provide reliable data transport. The handshake layer is used to create and maintain the connection between end-point devices. The Record protocol is responsible for data encryption and fragmenting. (Microsoft Technet 2009).

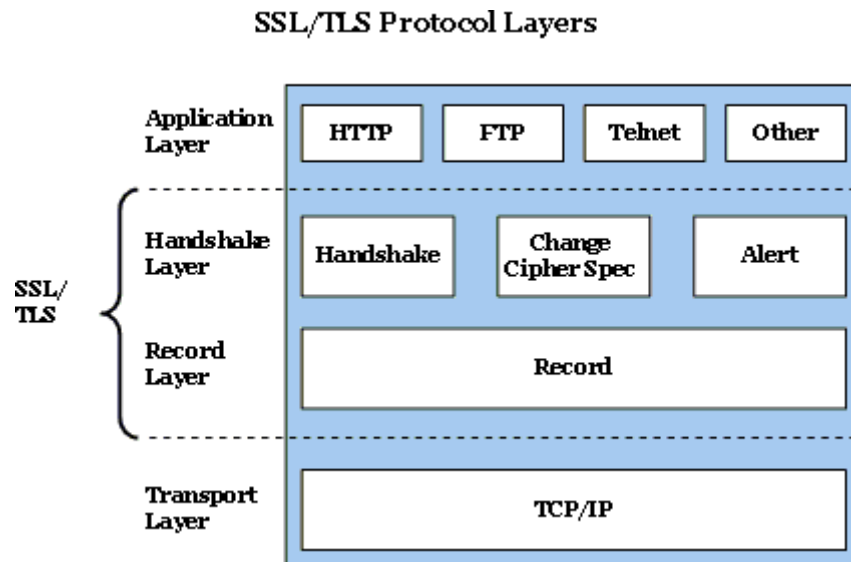


FIGURE 11. SSL/TLS protocol layers (Microsoft Technet 2009).

### 3.5.1 SSL/TLS Handshake Layer

The Handshake Layer consists of three sub-protocols: the handshake, change cipher spec, and alert protocols. Functions of these protocols are explained more thoroughly in following chapters. (Microsoft Technet 2009).

The handshake sub-protocol is used to negotiate session information between the client and the server. The session information includes a session ID, peer certificates, the cipher spec to be used, the compression algorithm to be used, and also a shared secret used to generate keys. The handshake sub-protocol also provides a number of important security functions. It performs a set of exchanges that starts authentication and negotiates encryption, hash and compression algorithms. (Microsoft Technet 2009).

The second sub-protocol is Change Cipher Spec, which is used to change the keying material used for encryption between the client and the server. Keying material is raw data, from which the cryptographic keys are formed. The Change Cipher Spec sub-protocol is used to send messages to the receiving party of the TLS ses-

sion, saying that the sender wants to change to a new set of keys. New keys are computed from the information exchanged by the handshake sub-protocol. (Microsoft Technet 2009).

The alert sub-protocol is used to send alert messages indicating a change in the status of the peer or error in the condition of the peer. The alert sub-protocol includes a wide variety of alerts to notify the peer of both normal and abnormal conditions. Alerts are commonly sent when the connection is closed. If the message cannot be decrypted, or if operation is cancelled by the user, an invalid message is received. Depending on severity of the error, the connection might be disconnected immediately or the user might simply be notified of the problem. (Microsoft Technet 2009).

### 3.5.2 SSL/TLS Record

The TLS Record protocol has two main objectives: it checks the data integrity and makes sure the data is encrypted. Neither one of these objectives is mandatory, both are however recommended to be used. (RFC 2246 – Dierks & Allen 1999, 3).

SSL/TLS Records allow the user to choose whether to use symmetric or asymmetric encryption algorithm. For each TLS session a new unique set of keys is created by the handshake layer. In addition, the Record protocol is used to fragment the data received from the upper layer protocols. (RFC 2246 – Dierks & Allen 1999, 3).

### 3.5.3 SSL/ TLS session

At the beginning of each SSL/TLS session, handshaking between connecting parties, illustrated in FIGURE 12, takes place. The Handshake protocol is used to perform this action. Creating the connection between the client and the server is divided into states, which all include changing messages between the client device

and the server. After handshaking is completed all traffic will be encrypted, and the connection is secure. (Microsoft Technet 2009).

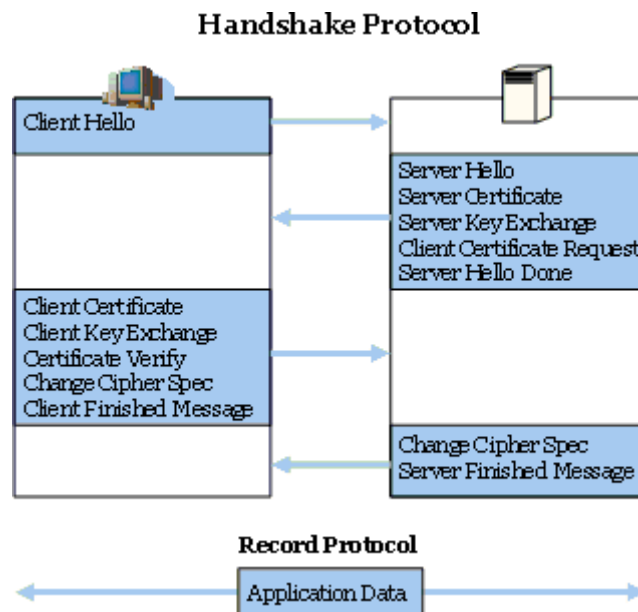


FIGURE 12. Handshake protocol messages (Microsoft Technet 2009).

The client initiates the handshake by using a Client Hello message, after which the server replies to this message with a Server Hello message. If this is not done the connection will time out. The Client Hello message includes information on supported protocols and versions of the SSL/TLS, supported encryption algorithms, supported compression algorithms, session ID, and some random information which is used to generate encryption keys. Session ID for a new session is 0. (Microsoft Technet 2009).

After the Client Hello packet is received, the server sends the Server Hello packet, which includes information regarding the protocol, encryption algorithm, compression algorithm, and the session ID which will be used. The Server Hello packet also contains random information that is used to generate encryption keys. The Server may also send a Server Certificate to a client; this however is optional. Server Key Exchange is only required if a Server Certificate is not used. The Server Key Exchange message includes the server's public key, which can be used

to encrypt and decrypt the messages sent to and from the server. The server also sends a request for the client certificate and Server Hello Done messages to the client. (Microsoft Technet 2009).

After the client receives information from the server it, sends its Client Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, and Client Finished messages to the server. The Client Certificate is compulsory and when used it is verified by using a Certificate Verify message used by the client. In the Certificate Verify message the client certificate is encrypted with the client's private key and opened by the server with the client's public key, in order to verify the integrity of the certificate. The Client Key Exchange message is mandatory; it uses either Diffie-Hellman or RSA key exchange in order to provide secure exchange of the symmetric key used to encrypt the connection between the client and the server. A Change Cipher spec message is used to notify the server that the client will start using previously negotiated security measures. After the Change Cipher Spec message the client sends an encrypted Client Finished Message. After this the server sends its own Change Cipher Spec message to the client and encrypted Server Finished message. After this all data will be encrypted with negotiated parameters. (Microsoft Technet 2009).

#### 3.5.4 SSL VPN

SSL VPN solutions are manufacturer specified systems based on the SSL/TLS protocol. In SSL VPN solutions services and resources are normally provided to a customer via an Internet browser, so separate client software is not required. This gives SSL VPN a leverage compared to IPsec VPN, since in SSL VPN the connection can be made from anywhere in the world, the only requirement for a SSL VPN connection is an Internet connection. SSL VPN is normally used for remote connections rather than Site-to-Site VPN connections. (Steinberg & Speed 2005, 33).

The SSL VPN solutions currently available on the market provide a much more sophisticated and overall security solution than a simple SSL/TLS connection. SSL VPN combines the advantages of the SSL/TLS protocol with subsystems that allow the user to create a secure session to a single program, rather than the whole internal network of a company. Most SSL VPN solutions also provide a wide range of security checks, including checking the antivirus program used by the client computer, as well as checking if the used antivirus program is up to date. Many other checks can also be performed. It is also possible to order a client computer to delete cache files after the session has ended. Because the SSL VPN connection allows the security association of devices over the Internet, it is important that the client computer has up to date data security software. Services provided by SSL VPN can be granted and/or denied based on information gathered from the remote computer, as shown in FIGURE 13. This procedure is called host checking. The SSL VPN administrator has to decide if the client computer which did not pass the host check is trusted with any services or if an “unsecure host message” is shown to the user. In order for the SSL VPN device to perform a host check, installation of the host checker software might be required. It should be noted that; installation of this software requires administrative privileges to the computer. (Steinberg & Speed 2005, 70, 71, 74).

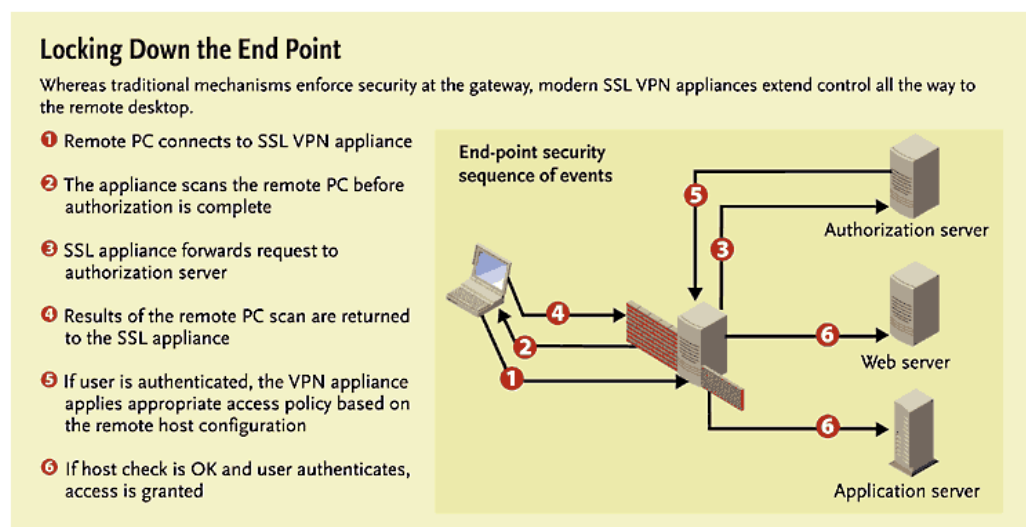


FIGURE 13. SSL VPN host check procedure (IT World Canada – SSL VPN 2005).

In addition to network connect, which is an IPsec VPN type secure tunnel between the client and the corporate network, SSL VPN also provides a possibility to create application based secure connections. Before network connect or application based secure connection is formed, the user might be required to install a piece of software to their computer. Administrative privileges are usually required to install software on the client computer, which may cause some problems for users trying to access applications from kiosk computers. It is possible to install a piece of software to the client computer, which uses administrative privileges in order to install components required for the SSL VPN connection, even if the user does not possess sufficient rights. (Steinberg & Speed 2005, 41).

Application based secure connections are normally done by using port forwarding software installed to the client computer by a SSL VPN device. The software installed to the client's computer monitors ports and destination addresses used by the client. When the software detects that the client is trying to connect the defined address and port it sends the information through the SSL/TLS tunnel to the corresponding address located in the internal network of the company. (Steinberg & Speed 2005, 47).

In order for SSL VPN to provide HTTP and HTTPS based applications located in the intranet of the company, reverse proxying is used. Placement of a reverse proxy server in DMZ, also known as demilitarized zone of the network topology, is presented in FIGURE 14. A reverse proxy server catches the packets that are trying to access the corporate network, and re-routes them to their designated addresses. (IBM – Secure Remote data access 2003).

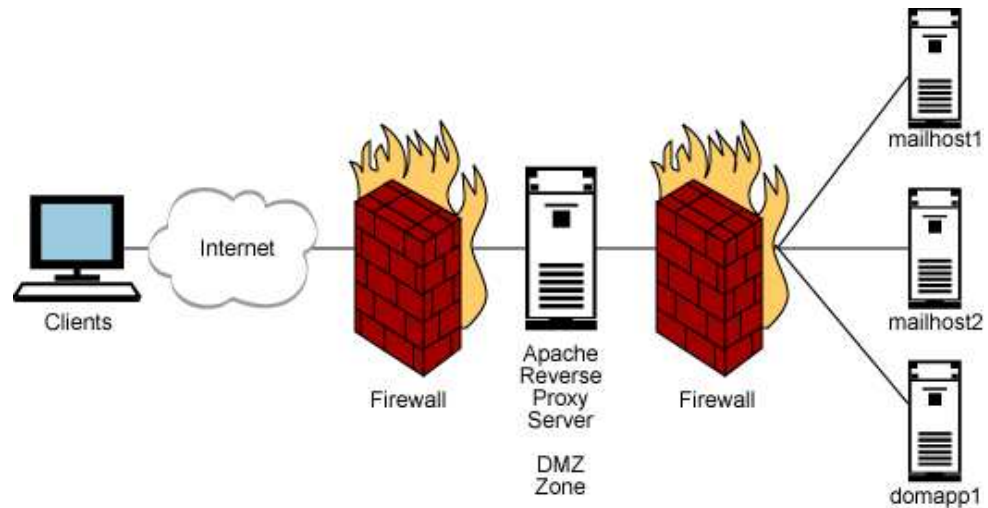


FIGURE 14. Placement of reverse proxy server in network topology (IBM – Secure Remote data access 2003).

SSL VPN solutions provide two ways of creating network connect between the client workstation and the internal network. These ways are called full tunneling and split tunneling. While full tunneling is used all the traffic from the client computer is routed through the SSL VPN device. In the split tunneling state only traffic from defined addresses is routed through the SSL VPN device. (Steinberg & Speed 2005, 48).

An IPsec-like VPN connection is also one of the many features of SSL VPN. In order to achieve this kind of connection SSL VPN device must have named the DHCP server which it uses to hand out IP addresses used in VPN connections, or use an IP pool definition tool built-in to the SSL VPN device. To make a firewall believe that SSL VPN clients are actually clients of the internal network, virtual network cards and routing table modification are used. (Steinberg & Speed 2005, 48).

There are also risks in using SSL VPN connections. The main concerns are insecure client computers used for accessing confidential information on internal servers. SSL VPN connections are also vulnerable for Denial of Service, also known as DoS attacks. This is because SSL/TLS protocols work in upper layers of the



OSI model, which makes it impossible to drop packets to lower levels of the OSI model. (Wikipedia – Virtual Private Network 2009).

SSL VPN provides many improvements to old IPsec VPN networks. With the SSL VPN the user is not bound to the computer or place; SSL VPN can be connected anywhere where there is internet. It also allows the possibility to provide only required services to the users, whereas IPsec VPN gives users access to the whole company network. SSL VPN is also a PC support friendly solution, because it does not require pre-installed client software. It is possible to install client computers with a piece of software that will use administrator privileges to install all applications required by SSL VPN. In addition, SSL VPN provides excellent tools for checking security of client devices. SSL VPN allows several other security features, such as the possibility to use one-time passwords and checking clients for certificate. (Steinberg & Speed 2005, 74, 75).

## 4 AUTHENTICATION

### 4.1 Authentication in general

There are different levels of authentication. Weak authentication uses only one type of weak authentication method: password, digital fingerprint, onetime password or certificate. These are considered weak authentication methods because they are easy to crack, copy, or duplicate. (Wikipedia – Authentication 2009).

Biometric authentication is considered strong authentication because most biometrics used in authentication are unique and quite hard to counterfeit. When multiple authentication methods are used it is also considered strong authentication. (Wikipedia – Authentication 2009).

### 4.2 Certificates

Certificates are documents used to verify the origin of the messages. In telecommunication networks certificates are normally signed by a third party, who validates the identity of a sender or the source of data. This third party is called certificate authority, and its actions are explained in following chapters. (Wikipedia – Public key infrastructure 2009).

There are two kinds of certificates: trusted certificates that are signed by a third party or self-signed certificates. Self-signed certificates are free but they are less secure than trusted certificates. How certificates work and advantages and disadvantages of trusted and self-signed certificates are explained more thoroughly in following chapters. (Wikipedia – Public key infrastructure 2009).

#### 4.2.1 Trusted certificates

Public key certificates used in computing are electronic documents incorporated to a digital signature which is used to bind a public key and a person's identity together. Public key certificates are managed by Public Key Infrastructure, later referred to as PKI, which is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates. A person in need of certificate applies for the certificate from Registration Authority, here on known as RA, who delivers the application to Certificate Authority, later referred to as CA, which is usually some Trusted Third Party (TTP). CA grants the certificate and also notifies Validation Authority (VA) from this new certificate, and when a certificate is used VA is prompted to verify authenticity of the certificate. PKI is presented below in FIGURE 15. The concept of CA is explained more thoroughly in chapter 4.2.2. (Wikipedia – Public key infrastructure 2009).

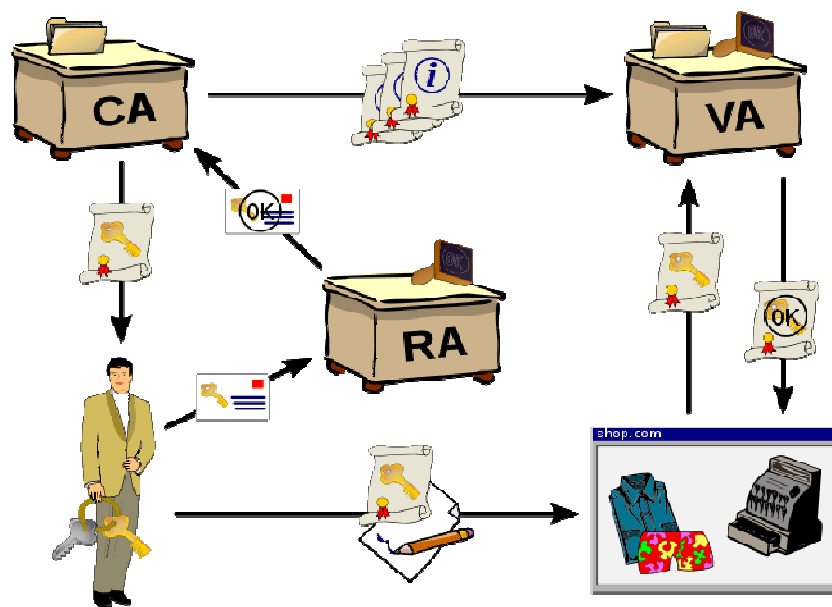


FIGURE 15. Public Key Infrastructure. (Wikipedia – Public key infrastructure 2009).

One of the most commonly used PKI applications is the ITU-T standard X.509. Amongst other things, X.509 specifies standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm. The structure of X.509 is tree-like, and it uses digital certificates to create SAs between the root certificate and users. The system is based on private and public keys, and each certificate holder should have one of each. A private key can be used to sign or encrypt information and it can only be decrypted or opened by a corresponding public key. Information signed with a public key can only be opened with a corresponding private key. In order to verify the source of the message, private keys should be used to sign messages. (Wikipedia – Public key infrastructure 2009; Wikipedia – X.509 2009).

#### 4.2.2 Certificate Authority

Certificate Authority, also known as CA, is a trusted third party. CA verifies the righteousness of its certificates with a digital signature. CA uses a private key of the root certificate to sign certificates that are created. Root certificate can be signed by CA. CA's public root certificate can be used to verify the righteousness of the certificates signed by CA. (Wikipedia – Certificate Authority 2009).

Certificates signed by CA include the following items: a private key used to sign certificates, a public key used to verify documents signed with a private key, acknowledgement of the owner of the certificate, and information about who granted the certificate. Also information about the certificate's best before date is included. CAs have a wide variety of different types of certificates, which are suitable for different situations. All certificates are used for authenticating a person, organization, or other entity. However, certificates used for signing legal documents are bound by different regulations than certificates used for verifying a server name. (Wikipedia – Certificate Authority 2009).

The CA business is fragmented, with local providers dominating the home markets, because many uses of digital signature are bound by local laws, regulations and accreditation schemes. The market for the SSL certificates, used for website security, is held by a small number of multinational companies, VeriSign being the biggest with over 50% share of the markets. (Wikipedia – Certificate Authority 2009).

#### 4.2.3 Revoking certificates

The most common reason for revoking certificates is compromised security of the private key. A certificate revocation list later, known as CRL, is a list of the certificates already revoked. Users should never accept certificates mentioned on this list. If the security of CA's root certificate is compromised, all certificates granted by the CA should be revoked and renewed. (Wikipedia – Certificate Revocation List 2009).

Certificates on CRL have two status options: certificates can be either revoked or held. Revoked certificates cannot be re-validated, but certificates on hold can be. Certificates with hold status are the ones about which the user is unsure whether or not the private key has been compromised. A list of revoked certificates is released and normally also signed by CA. Signing revocation lists is normally done to prevent spoofing or denial-of-service attacks. Even though CRLs are only valid for a certain period of time, which is normally less than 24 hours, there are many people trying to take advantage of CRLs, which is why it is important for lists to be digitally signed. (Wikipedia – Certificate Revocation List 2009).

#### 4.2.4 Self-signed certificates

A self-signed certificate is an identity certificate that is signed by its own creator. Since self-signed certificates are not signed by TTP, there might be some trust issues with using them. For this reason self-signed certificates are mainly used in small implementations where people know each other. (Wikipedia – Self-signed certificate 2009).

Self-signed certificates offer a secure and free way of authenticating an individual, but there are also security risks related to self-signed certificates. The only major problem with self-signed certificates is that they cannot be revoked, like certificates created by CA, so if the security of person's private key is compromised, someone else can use their identity as their own. (Wikipedia – Self-signed certificate 2009).

#### 4.3 One time password

The purpose of OTP (One Time Password) is to reduce the risk of unauthorized access to restricted resources. This is done by altering the password or part of the password every time a person authenticates. There are five types of OTPs that are commonly used. The first solution uses mathematical algorithms to generate a new password based on the previous. The second OTP solution is based on time-synchronization between the authentication server and the client. Time-synchronized OTP solutions normally require some form of a physical hardware token such as RSA SecurID key seen in FIGURE 16. (Wikipedia – One-time password 2009).



FIGURE 16. RSA SecurID token.

The third OTP type uses mathematical algorithms as well, but is based on a challenge sent to the user rather than the previous password. The fourth OTP type uses password lists printed on a piece of paper or card. These types of OTPs are very common in internet banking. The fifth OTP type is also based on challenge and response and uses cell phones for delivering passwords for users and then the user can authenticate himself by using this password. (Wikipedia – One-time password 2009).

#### 4.4 Digital fingerprint

Digital fingerprints are a weak authentication method for devices such as laptops. The most common type of digital fingerprint is certificates, but there are also other forms of digital fingerprints. A digital fingerprint can be as simple as a windows registry value or a file with a certain name stored in certain location. (Juniper Networks 2008).

Digital fingerprints such as registry values or files can be added by an administrator and then checked by an authenticating device. If values match then authentication has been successful. Digital fingerprints are generally used to authenticate devices rather than people. (Juniper Networks 2008).

#### 4.5 Biometric authentication

Biometric authentication is considered to be the most secure way of authenticating people, even though some applications are more secure than the others. In principle, biometric samples can be used to recognize individuals quickly, anywhere and at any time throughout their entire life. If biometrics were to be used in everyday life it would open the possibility to link all the political, economic and social roles and behaviours of a person. For example how one behaves as a customer or a tenant could have consequences on his treatment as a seeker of a loan. (Bleumer 1999, 2, 3).

There are, however, a few issues regarding biometric authentication. Firstly people in some cultures can think their soul is stolen if a photo of them was taken for biometric authentication. Many people also feel that biometric authentication is intrusive, which has prevented biometric technology becoming widely deployed. Not surprisingly, the biggest users of biometric authentication are physical access control, law enforcement, health care and banking. Computer security and telecommunications have also increased the use of biometric authentication methods, even though these are not the most common places to use biometric authentication. (Bleumer 1999, 2, 3).

The problem with biometric technology is that it tends to cost more than password or token-based systems. However, almost all business laptops sold these days have fingerprint scanners installed on them, so it would not be impossible to think that using biometric authentication in computers and telecommunications security would become more popular. The only question that remains is whether to trust the quality of built-in fingerprint scanners of the laptops or not. When applied to



the use of VPN or SSL VPN it would also require a company to have a database where all the fingerprints would be stored. (Bleumer 1999, 3, 4).

It is possible to understand if a human characteristic can be used for biometrics in terms of the following parameters:

- Universality - each person should have the characteristic
- Uniqueness - is how well the biometric separates an individual from another.
- Permanence - measures how well a biometric resists aging.
- Collectability - ease of acquisition for measurement.
- Performance - accuracy, speed, and robustness of technology used.
- Acceptability - degree of approval of a technology.
- Circumvention - ease of use of a substitute.

Table 1 shows a comparison of existing biometric systems in terms of parameters listed above. (Wikipedia – Biometric authentication 2009).

Table 1. Comparison of existing biometric systems (Wikipedia – Biometric authentication 2009).

Comparison of various biometric technologies, modified from Jain et al., 2004  
(H=High, M=Medium, L=Low)

Biometrics:	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention*
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand geometry	M	M	M	H	M	M	M
Keystrokes	L	L	L	M	L	M	M
Hand veins	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retinal scan	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial thermograph	H	H	L	H	M	H	H
Odor	H	H	H	L	L	M	L
DNA	H	H	H	L	H	L	L
Gait	M	L	L	H	L	H	M
Ear Canal	M	M	H	M	M	H	M

#### 4.6 Password authentication

Password authentication is the simplest way of authenticating users. In password authentication the user is prompted to provide the username and password given to him. Password authentication is among the least secure ways of authenticating people. This is because many users do not consider it as a security risk if they hand their password to husband, child, or even some guy over the phone. Passwords are also highly susceptible to hacking, cracking, keyloggers, and other attacks. (Aladdin – VPN Authentication 2009).

Password authentication can be done by adding a static password and username to a system, which are then used to authenticate the person. Another way of password authentication is comparing user credentials with a password database such as the Microsoft active directory or the Novell eDirectory. In VPN communications both types of user passwords are used. Statically generated passwords are normally more vulnerable to brute force attacks where a password is attempted to be cracked by going through all possible password character combinations in order to hack into a system. Password database solutions normally lock the password after three to five false positives, after which the administrator might be needed to unlock the password. (Aladdin – VPN Authentication 2009).

#### 4.7 Comparing authentication solutions

Selecting suitable authentication methods for secure remote networking is not easy, because users are required to perform strong authentication in order to get access to the required software and services. Because of the high cost and possible invasiveness of the technology biometrics is out of the question. Digital fingerprints were tried as authentication method, but they were soon decided to be too insecure for enterprise use.

Because of the functional AD authentication infrastructure and possibility to use existing AD as authentication method for SSL VPN, AD was made the primary authentication method to be used while signing in to a SSL VPN portal. Insecurity of password authentication requires two-factor authentication to be used in order to receive full access to the company network. Because of this, a one-time password solution was also implemented to Andritz Group SSL VPN remote access. The OTP solution used gives the user the possibility to choose from four different OTP technologies. These technologies are password list, time synchronized password, and mobile token.

In addition to authentication methods, the Andritz Group SSL VPN solution uses certificates to authenticate the devices accessing the company network. Certificate is checked before authentication and will be used to restrict access to network resources.

Table 2. Comparison of authentication methods

<b>Comparison of various authentication technologies</b> ( <b>H=High, M=Medium, L=Low</b> )						
<b>Techniques:</b>	<b>Ease of use</b>	<b>Collectability</b>	<b>Cost</b>	<b>Performance</b>	<b>Security</b>	<b>Acceptability</b>
<b>Certificates</b>	<b>H</b>	<b>H</b>	<b>M</b>	<b>H</b>	<b>H</b>	<b>H</b>
<b>Self-signed Certificates</b>	<b>H</b>	<b>H</b>	<b>L</b>	<b>M</b>	<b>L</b>	<b>H</b>
<b>Password</b>	<b>H</b>	<b>H</b>	<b>L</b>	<b>H</b>	<b>L</b>	<b>H</b>
<b>Biometrics</b>	<b>M</b>	<b>M</b>	<b>H</b>	<b>M</b>	<b>H</b>	<b>M</b>
<b>One-time-password</b>	<b>M</b>	<b>H</b>	<b>L</b>	<b>H</b>	<b>H</b>	<b>H</b>
<b>Digital finger-print</b>	<b>H</b>	<b>H</b>	<b>L</b>	<b>M</b>	<b>L</b>	<b>H</b>

## 5 ANDRITZ GROUP AND ITS LINE OF INDUSTRY

### 5.1 History of the Andritz Group

Andritz AG was first founded in 1852 by Hungarian entrepreneur Josef Körösi as a foundry and machine works. In a couple of years time Andritz had extended its product range to cranes, pumps and water turbines. Later also bridges, steam vessels, steam engines and mining equipment became part of Andritz's product range. By the 1870s Andritz employed over 1300 people. In the late 1800s Andritz got into trouble because important markets and customers were lost, which in the end resulted in Andritz being sold to a group of Austrian iron and steel companies. (Andritz 2009b).

In 1900 Andritz was sold to the Gutmann Banking Group and transformed into a stock holding company. The new owner managed to gain a large railway tunnel contract, and at the same time the company was very successful in building high-pressure centrifugal pumps and cranes. The bank crisis of 1932 made Andritz close its gates, but in the end the company survived the crisis that made so many other companies declare a bankruptcy. (Andritz 2009b).

After the bank crisis Andritz changed owners twice before World War II. In the end of WWII Andritz's production machinery was taken away by occupying authorities. This was the second time it looked that the story of Andritz might have ended, but instead current owners managed to borrow some second hand machinery and started producing small and medium size pumps and turbines in the old buildings. From the 1940s till the start of the 1980s Andritz grew and extended its product range to cover electro-chemical and metallurgical plants as well as coolant pumps for nuclear reactors. At the beginning of the 1980s Andritz was hit by the oil crisis and its effects on the world economy. Over 700 people were dismissed. Since 1987 when the company became profitable again it has steadily increased its

knowledge and revenue by acquisitions that support the company's structure. In 1999 Andritz was sold to a group of investors consisting of President and CEO Andritz Wolfgang Leitner and the management. (Andritz 2009b).

## 5.2 Andritz Group today

The Andritz Group is a publicly listed company in the Austrian stock exchange. The headquarters are located in Graz, Austria. The Andritz Group is a global market leader for customized plants, systems, and services for the pulp and paper, hydropower, steel, and other specialized industries such as solid/liquid separation, feed and biofuel technology. (Andritz 2009a).

Since 1999 the Andritz Group has been making acquisitions around the world to support its goal to be a global market leader in areas of pulp & paper, hydro, metals, environment & process, and feed & biofuel. The Andritz Group's main business areas are pulp & paper technology with 37% share of the sales in 2008, and hydro power business with 33% of the sales in 2008. Today the Andritz Group employs approximately 13,700 people worldwide, in previously named areas of business. As a publicly listed company another important goal of Andritz AG is continuation of profitable growth, which is done by acquiring rising companies with good visions and solid economy. (Andritz 2009c).

The Andritz Group's overall strategy is to be a globally leading supplier of customized plants, process technologies, and services with full-line capabilities in all of its business areas. Being one of the few players in this field who are able to offer this full line of capabilities, the Andritz Group is a strong and respected competitor in its market areas. (Andritz 2009c).

### 5.3 Andritz Oy

Andritz Oy covers the Andritz Group's operations in Finland. Andritz Oy's head office is in Helsinki and side offices are in Hollola, Kotka, Savonlinna, Tampere and Varkaus. Currently over 1,000 people in Finland are directly employed by Andritz Oy, and combined with indirect employment, the numbers are closer to 2,000. Andritz Oy's chairman of the board is Wolfgang Leitner (Andritz AG) and the President and CEO is Harry Rickman, who reports to the members of the executive board of Andritz Group. Andritz Oy's sister company is Finnish Savonlinna Works Oy, which is located in Savonlinna. Total sales of Andritz Oy is approximately EUR 500 million annually. (Andritz 2009a).

Andritz Oy consists of 13 divisions and its business is divided to five regions, which are North America, South America, North Europe, Central Europe and Asia. Following chapters will introduce four of the biggest divisions in Andritz Oy. (Andritz 2009a).

The Wood Processing Division is the world's leading supplier of systems, equipment and processes for all steps required in a woodyard - from the arrival of the logs to their subsequent preparation into wood chips – all the way to the production of chemical and mechanical pulps. The headquarters of the Wood Processing Divisions is located in Hollola, Finland. In addition, it has sites in USA, Canada and Brazil. (Andritz 2009d).

The Pulp Mill Services Division covers the service activities for the Wood Processing and Kraft Mill Systems Divisions. Primary emphasis is on production efficiency and availability, services (engineered wear parts, replacement parts, equipment rebuilds, shutdown services, service contracts and upgrades) to kraft pulp mills and woodyards supplied either by Andritz or other manufacturers. Apart from the traditional service business, the division works with its customers to maximize reliability and overall production efficiency, by providing added value

services and innovative solutions. The Pulp Mill Services Division serves the large installed base of Andritz equipment all over the world. The main sites are located in North America and Europe, but there are local service centers in more than 30 countries worldwide. The headquarters for the Pulp Mill Services is located in Savonlinna, Finland. The Division has approximately 285 employees, from whom roughly 50 % in the USA, 40 % in Europe and 10 % in the rest of the world. The production facilities for rebuilds and parts are located in Finland and in the USA. In addition, the division has local rebuilt partner shops in New Zealand, Indonesia, South Africa, Brazil, and Portugal. (Andritz 2009d).

The Fiber Preparation Systems Division is a global supplier of systems, equipment and services for all papermaking processes such as recycled fiber processing, fiber stock preparation, paper machine approach systems, broke handling as well as paper mill internal water loop handling, sludge and reject handling. The division has its headquarters in Graz, Austria and Kotka, Finland, with significant operations in Foshan, China, Glens Falls, New York, USA and Tokyo, Japan. (Andritz 2009d).

The Fiberline Division is one of the world's leading suppliers of systems, equipment, and processes for the production of chemical pulp. The products include continuous cooking systems, washers, screens, MC equipment, bleaching systems and related equipment. The division is headquartered in Kotka and has operations in Savonlinna, Finland; Roswell, GA and Glens Falls, NY, both in the USA; Tokyo, Japan, Curitiba, Brazil and Karlstad, Sweden. (Andritz 2009d).

Like all the major companies, Andritz Oy has had mergers, in order to develop its business and grow as a company. Within 15 years Andritz Oy has merged two times, first with Konewood, and then with GE Hydro Finland in 2006. These mergers have made Andritz Oy a considerable employer in Finland with over 1,000 people employed directly and almost 1,000 people employed indirectly. (Andritz 2009a).

## 5.4 Line of business

### 5.4.1 Pulp and Paper industry

The global pulp and paper industry is dominated by North American, northern European and East Asian countries. Australia and Latin America have also some significant pulp and paper industries. India and China are believed to be the key to the pulp and paper industry's growth in the next few years. Andritz Group has made some strong investments in previously mentioned regions. (Wikipedia – Pulp and paper industry 2009).

The pulp and paper industry has grown to be a big multinational market, valued over \$150 billion annually, when in the late 1980s it was worth around \$14 billion. While markets are growing, and even more advanced technology is required in order to receive better quality chips, Andritz must be ready to accept the challenge to meet these new requirements. (Minnes 2009, 1).

### 5.4.2 Hydropower industry

Hydropower provides around 19% of world electricity, and it is one of the few renewable energy sources. The main source of hydropower are dams built to utilize the huge amount of energy released by water when it runs through a water turbine. New more sophisticated and powerful turbines are planned, in order to utilize even bigger amounts of the energy released by the flowing water. (Wikipedia - Hydropower 2009).

Andritz Group has made several acquisitions to support its goal to be the market leader in the branch of hydropower and turbine technology. Andritz Group's full line of capabilities in this area gives Andritz an advantage to provide everything from upgrading the old turbine systems to building whole new systems. (Wikipedia - Hydropower 2009).



## 6 COMPARISON OF VPN SOLUTIONS

### 6.1 Check Point VPN

Check Point VPN is an integrated software solution that provides secure connectivity to the corporate network, remote and mobile users, branch offices and business partners. Check Point VPN provides access control, authentication, and data encryption in order to provide users with a secure connection over the public internet. In addition, Check Point VPN offers a unified method for creating and managing complex VPNs. (Check Point 2009).

In order to define the participating gateways, and to perform other administrative tasks, an easy to use administration tool called the SmartDashboard is used. Check Point VPN also includes support for third party gateways as well as their own products. Check Point VPN supports gateways configured for both star and mesh topologies, and configuration of topologies can be done in minutes with an integrated certificate authority to manage keys. (Check Point 2009).

A Check Point VPN connection can be created based on either the routes or the domain used by the client. In route-based VPNs, the administrator defines the traffic to be encrypted by VPN rules, which enables the creation of complex large-scale site-to-site VPNs in a dynamic environment. Multicast communities across VPNs and the extension of dynamic routing are also supported in route-based VPNs. (Check Point 2009).

#### 6.1.1 Enhanced IPsec VPN Security

Check Point VPNs are built to provide VPN connectivity solutions matched with a high level of security. Check Point's IPsec VPN provides secure connectivity between remote users, sites, and partners. It also gives an administrator the ability to choose what kind of traffic will be affected by the Check Point VPN security policy. This can either be encrypted traffic, a specified subset of traffic, or all VPN

traffic can also be allowed to enter the company network uninspected. (Check Point 2009).

Check Point's solution also includes strong security against DoS attacks, such as ones directed against the IKE mechanism. Preventing the DoS attacks is done by asking unknown connecting gateways to solve a computationally intensive problem before allocating resources. (Check Point 2009).

### 6.1.2 Check Point VPN remote access

Since almost every company has their own unique requirements for the remote access, Check Point provides a flexible solution, which allows the customer to design a solution to meet their personal needs. Underneath there are some service examples provided by Check Point's IPsec VPN suite. (Check Point 2009).

- Check Point Endpoint Security—Check Point Endpoint Security is the first single agent for total endpoint security that combines a remote access VPN with the highest-rated firewall, NAC (network access control), program control, antivirus, anti-spyware, and data security features.
- SecuRemote—SecuRemote is a basic VPN client that offers IPsec connectivity for remote users.
- SecureClient—SecureClient is an advanced VPN client that offers IPsec connectivity for remote users.
- SecureClient Mobile—SecureClient Mobile delivers firewall protection and secure, uninterrupted remote access for wireless devices such as mobile phones.
- L2TP (Layer 2 Tunneling protocol) for iPhone—Support for iPhone's built-in L2TP VPN client.

In addition, Check Point VPN offers several ways to avoid the most common routing and connectivity issues faced by remote users. Check Point's solution to these problems is the use of connectivity modes, such as office mode, visitor mode, and hub mode. In office mode IP packets are encapsulated by using the remote user's original IP address, thereby making users to appear as if they were in the office, even if this is not the case. In office mode enhanced anti-spoofing is also provided.

Visitor mode allows the user to establish IPsec VPN connection in locations where Internet connectivity may be limited to HTTP and HTTPS traffic. Hub mode provides strict and centralized inspection of all client traffic, while removing the need to deploy security functions to multiple offices. Hub mode also provides users with the possibility to use secure client-to-client communications and Internet conferencing services, which may require the use of a third party software. (Check Point 2009).

## 6.2 Nortel SSL VPN

Nortel's VPN Gateway 3000 series is designed to offer both SSL VPN and IPsec VPN services for medium and large enterprises rather than small businesses. The Nortel VPN Gateway family has two members. Smaller VPN Gateway 3050 is designed to provide services for up to 2,000 concurrent users and bigger VPN Gateway 3070 supports up to 5,000 concurrent users. Both of these products are designed to provide flexible access options including browser-based, on demand and installed SSL clients, and IPsec client support. (Nortel 2009).

The Nortel VPN Gateway offers services quite similar to Juniper Networks SA. The Nortel VPN Gateways come with integrated traffic management and content-based load balancing. Also included in Nortel's VPN Gateways is improved filtering technology, which allows users to be blocked based on IP address, requested URL, application type, or even cookie information. The VPN Gateways perform authentication based on local user database, LDAP, RADIUS, NTLM, Active Directory, or Netegrity. The Nortel VPN Gateways also support using digital certificates, token-based systems or two-factor authentication as a strong authentication method. (Nortel 2009).

In addition, Nortel VPN Gateway products should integrate seamlessly into any network, which makes it easy to implement the Nortel VPN Gateway to an existing network, even if the company had not used Nortel products before. The Nortel Web management interface provides easy to use configuration wizards and de-

tailed help screens, which will guide the administrator in setting up client connections. Both VPN Gateway products have built-in acceleration features, which provide better performance and flexibility. (Nortel 2009).

All in all, the Nortel VPN Gateway 3000 series offers combined SSL VPN and IPsec VPN solutions for a cheap price and are packed with features. However, Nortel have not quite made it to the big league of SSL VPN manufacturers, and solutions introduced by Nortel VPN Gateway products have normally been introduced by some of the bigger SSL VPN players before. (Nortel 2009).

### 6.3 Checkpoint VPN vs. Juniper SSL VPN

Both Check Point Secure Client and Juniper Networks SSL VPN provide the user with an access to the internal network of the company. There are, however, huge differences. With Check Point Secure client, connection is made using the client software which requires installation. The competitor SSL VPN on the other hand is always ready to go, wherever, and on whatever computer. In order to use all features offered by SSL VPN, installation of ActiveX components or Java applets might be required. Installation of these files requires administrator privileges. As a solution to this Juniper Networks have created software which uses administrative privileges to install these components on the client computer, even if the user had logged in with an account that does not have administrative privileges.

Both Check Point Secure Client and Juniper SSL VPN support use of one-time-passwords, AD authentication, and a static user authentication. When it comes to device authentication, Check Point Secure Client relies on pre-installed software and security of the corporate computers, while SSL VPN provides a wide range of authentication methods and security checks, including antivirus check, certificate check, checking for corresponding registry entries and many more.

The biggest improvement provided by Juniper SSL VPN is, however, the possibility to grant the user with limited access to the company's resources. While Check Point Secure Client always provides full VPN access for each user, in most cases this is unnecessary and can lead to compromised network security. Table 3 presented below gives a more comprehensive view of the differences between Check Point VPN and Juniper SSL VPN.

Table 3. Comparison of Check Point VPN and Juniper SSL VPN

<b>Features</b>	<b>Check Point VPN</b>	<b>Juniper SSL VPN</b>
Price	Existing system (Firewall and management), expensive secure client licences	Price is determined by the number of concurrent users and the platform
Configuration	Command line and SmartDashboard	Configuration is done via web browser based GUI
Operation	Requires installed client software	Service can be used via web browser, some features may require installing ActiveX or Java components
Encryption Algorithm	Depends on used configuration	Encryption algorithm is dependant from used web browser
User authentication	Several ways, supports two factor authentication	Several ways, supports two factor Authentication
Device Authentication	Pre-installed software required	Host checker allows SSL VPN administrator to define which security features are required before client is allowed to access any services or applications
User groups	Each client is treated as an individual	Clients can be assigned to user groups which can be then assigned with services and applications required
Applications	Full VPN connection is created	Client can be allowed to connect network resources, web based applications, use a single program via SAM, or create Network Connect session which can be compared to end-to-end VPN connection.
Troubleshooting	Logs	Juniper SSL VPN has several tools for Troubleshooting

#### 6.4 Check Point VPN vs. Nortel SSL VPN / IPsec VPN

Because both Check Point and Nortel are major suppliers in the IPsec VPN markets. They are able to provide competitive pricing and worldwide support network for their remote access products. The main differences between these two products are the Nortel VPN Gateway's ability to combine the best of both IPsec and SSL VPN, while Check Point's product only provides IPsec VPN. The target of this

comparison is to see if combining both IPsec VPN and SSL VPN has forced Nortel to make some changes to the traditional IPsec VPN connectivity. Differences between these two are presented in Table 4.

Table 4. Comparison of Check Point IPsec VPN and Nortel IPsec / SSL VPN

<b>Features</b>	<b>Check Point VPN</b>	<b>Nortel VPN Gateway 3000 series</b>
Price	Existing system (Firewall and management), expensive secure client licences	New equipment is needed, however Nortel's VPN Gateway 3000 series appliances are among the cheapest on the market
Configuration	Command line and SmartDashboard	Configuration is done via web browser based GUI
Operation	Requires installed client software	Service can be used via web browser, some features may require installing ActiveX or Java components, Nortel VPN Gateway 3000 series also provides opportunity to install VPN client software to the client computer.
Encryption Algorithm	Depends on used configuration	Encryption algorithm is dependant from used web browser
User authentication	Several ways, supports two factor authentication	Several ways, supports two factor authentication
Device Authentication	Pre-installed software required	Administrator can decide whether to use pre-installed client software or do SSL VPN type authentication of the client device.
User groups	Each client is treated as an individual	Clients can be assigned to user groups which can be then assigned with services and applications required
Applications	Full VPN connection is created	Client access to network resources can be limited by SSL VPN, but full VPN connection is also possible.
Troubleshooting	Logs	Nortel VPN Gateway offers several tools for troubleshooting

In Nortel's case combining an IPsec VPN and SSL VPN into one has not affected functionality of the IPsec VPN, but SSL VPN has been used to correct the flaws and imperfection of IPsec VPN. This makes the Nortel VPN Gateway 3000 series a device worth considering for companies trying to combine the best of both IPsec VPN and SSL VPN.

## 6.5 Juniper SSL VPN vs. Nortel SSL VPN / IPsec VPN

This chapter compares SSL VPN solutions of Juniper Networks Secure Access and Nortel VPN Gateway 3000 series. Solutions are compared mainly on SSL VPN level and IPsec features are ignored.

Table 5. Comparison of Juniper SSL VPN and Nortel VPN gateway

<b>Features</b>	<b>Juniper SSL VPN</b>	<b>Nortel VPN Gateway 3000 series</b>
Price	Price is determined by the number of concurrent users and the platform	New equipment is needed, however Nortel's VPN Gateway 3000 series appliances are among the cheapest ones on the market
Configuration	Configuration is done via web browser based GUI	Configuration is done via web browser based GUI
Operation	Service can be used via web browser, some features may require installing ActiveX or Java components	Service can be used via web browser, some features may require installing ActiveX or Java components, Nortel VPN Gateway 3000 series also provides opportunity to install VPN client software to the client computer.
Encryption Algorithm	Encryption algorithm is dependant from used web browser	Encryption algorithm is dependant from used web browser
User authentication	Several ways, supports two factor authentication	Several ways, supports two factor authentication
Device Authentication	Host checker allows SSL VPN administrator to define which security features are required before client is allowed to access any services or applications	Administrator can decide whether to use pre-installed client software or do SSL VPN type authentication of the client device.
User groups	Clients can be assigned to user groups which can be then assigned with services and applications required	Clients can be assigned to user groups which can be then assigned with services and applications required
Applications	Client can be allowed to connect network resources, web based applications, use a single program via SAM, or create Network Connect session which can be compared to end-to-end VPN connection.	Client access to network resources can be limited by SSL VPN, but full VPN connection is also possible.
Troubleshooting	Juniper SSL VPN has several tools for troubleshooting	Nortel VPN Gateway offers several tools for troubleshooting

For corporate SSL VPN solutions both Juniper Networks SA and the Nortel VPN Gateway 3000 series offer suitable and fully functional applications that can be easily deployed to the existing company network. Both Nortel and Juniper products offer a wide variety of services and clear restrictions to access control.

Nortel is a big player on IPsec VPN markets, but for some reason its SSL VPN products have not sold as well as its competitors' solutions. Because of this Nortel might give up providing SSL VPN solutions, which would be problematic if a company is using Nortel's SSL VPN solution.(Girard 2007).

## 6.6 Result of comparison

SSL VPN provides superior cost efficiency compared to the old IPsec VPN solution. Also, it allows more precise user access control required to prevent unauthorized access. SSL VPN also allows users to connect the company network to read e-mail and check information from the company's internal network, from any computer with internet connection. Implementing SSL VPN also reduces administrative overhead caused by supporting the remote users.

The Andritz Group selected Juniper Networks Secure Access product family for its new remote access solution. Even though there are several other competitive products on the markets besides Juniper's SSL VPN solution, the decision was quite easy. This is because previous co-operation with Juniper Networks has been successful, and Juniper Networks were able to provide a complete SSL VPN solution with required services and worldwide support.

The Andritz Group also used independent research carried out by Gratner to decide which SSL VPN solution would be selected as the Andritz Group SSL VPN standard. Based on the independent research Juniper Networks Secure Access would be the best solution as the enterprise's SSL VPN solution, and also based on good experiences in the past, Juniper Networks Secure Access was selected as the new remote access solution.



## 7 REMOTE ACCESS SOLUTION FOR ANDRITZ GROUP CORPORATE NETWORK

### 7.1 Andritz Group's network environment

The Andritz group corporate network is a global full mesh network, which has several MPLS (Multiprotocol Label Switching) clouds with up to 30 sites connected to each cloud. These clouds are connected to each other via MPLS or Check Point's IPsec VPN connections. Globally the Andritz group corporate network has eight main sites which have local MPLS connections between different offices in each region. In addition, these sites are connected to each other via MPLS and/or site-to-site VPN connections. In total, there are seven long distance MPLS connections used to connect the sites. On top of that, there are also over 70 VPN connections, some of which work as primary lines and some of which are back up lines. FIGURE 17, presented below, is a picture of the Andritz Group's global WAN (wide area network). Updates, however, have been made since this picture was released.

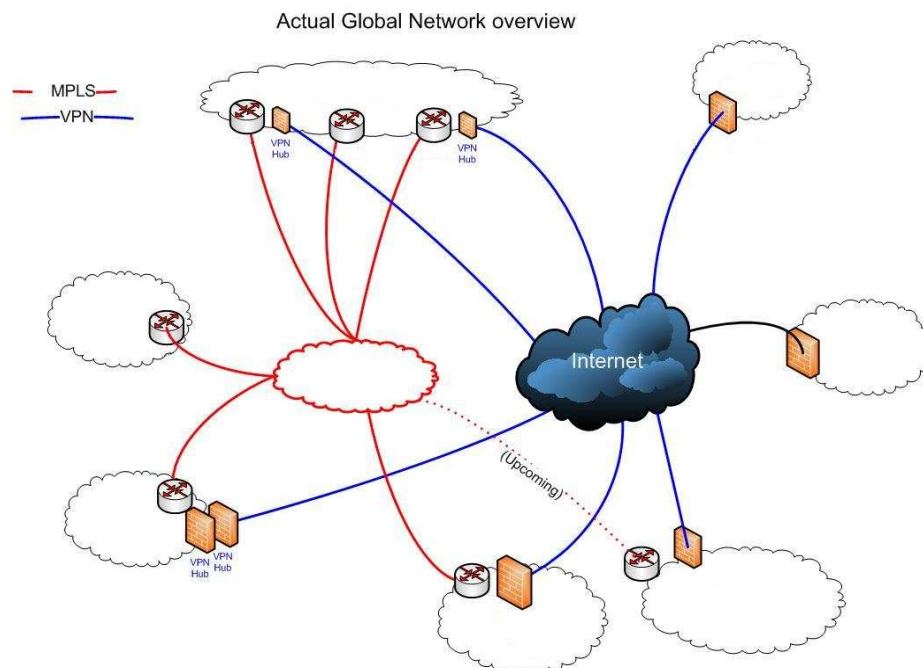


FIGURE 17. Andritz Group WAN modified

In addition to site-to-site connections, the Andritz Group has a need to provide mobile users with access to the corporate network. To ensure security of the remote access connection, an IPsec VPN or SSL VPN connection is used.

## 7.2 Andritz Group's original VPN solution

Originally the Andritz Group was using Check Point's IPsec VPN and MPLS lines for its secure remote connections. A Check Point VPN is used to provide most of the global Site-to-Site connections, and for secure remote connections a Check Point secure client is used. Remote users are mainly personnel of the Andritz Group, though there are some subcontractors and other business partners who are provided with Check Point secure clients so they can connect to the Andritz Group intranet. However, granting external users with a full VPN connection can compromise the security of the entire internal network, and therefore a new secure remote access solution was required.

Since Check Point VPN 1 has proven to be a reliable and easily configurable solution for site-to-site VPN connections, it will remain as the Andritz Group's site-to-site VPN solution. Increased security requirements for company data have created a need for new more restricted secure remote access solutions. To find the best possible SSL VPN solution for the Andritz Group, several products were tested. However, after thorough review one proved to be better than the rest. Therefore, the Andritz Group selected a Juniper Networks SA (Secure Access) SSL VPN solution, which was easily manageable, allowed restriction of access and provided the required level of security for both user and device authentication. Changing the secure remote connection method will also bring considerable savings, because SSL VPN licence fees are based on the number of concurrent users, whereas Check Point secure client must be installed to each computer that uses secure remote connections, no matter how random this use might be.

### 7.3 Juniper Networks SSL VPN – Secure Access

Juniper Networks SA products offer a complete SSL VPN solution to everyone from small businesses to large enterprises. Their products offer a full range of SSL VPN services from intranet access to network connect.

The SSL VPN solutions of Juniper Networks SA series introduce several new features essential for improving productivity, cost efficiency, and for the mobility of remote users. Some of these features are introduced in this chapter. Also covered in this chapter are Juniper SSL VPN solutions used in the Andritz Group global network.

#### 7.3.1 Juniper SSL VPN requirements

Implementing a Juniper Networks SA device to a company network requires no changes to the existing servers or other appliances of the network. Since all required applications are stored to Juniper SSL VPN's harddrive, they can be downloaded and installed from there over the Internet when the required application is used for the first time; therefore no preinstallation of the client software is required.

In order to install some of the applications required by Juniper SSL VPN, administrative privileges are needed. Because of this, Juniper Networks have created software which grants the user with temporary administrative privileges to install an application required by the SSL VPN device. This software is preinstalled to all Andritz Group computers via Microsoft's software distribution software called SMS (System Management Server).

### 7.3.2 Accessing Juniper SSL VPN

Juniper Networks SA appliances provide SSL VPN connectivity over a web browser, and therefore no installation of client software is required. Juniper SSL VPN is also operating system independent, which makes it easier for companies using several operating systems to provide an identical VPN solution for all users regardless of the platform.

Since all major web browsers these days are embedded with SSL/TLS support, it makes no difference which browser is used to make the connection. Both administrative web UI (User Interface) and end-user web UI are presented in chapters 7.5.1 and 7.5.2.

### 7.3.3 Juniper Networks IVE

The Juniper Networks Instant Virtual Extranet, later referred to as IVE, is a platform that serves as the underlying hardware and software for the Juniper Networks SSL VPN appliances. The appliances of the Juniper Networks SA series allow administrators to set restrictions to control from which IP addresses users can access an IVE sign-in page, be mapped to a role, or access a resource. Restrictions set for accessing the IVE sign-in page are monitored by the host checker, the functions of which will be explained in chapter 7.3.4.

The IVE is a hardened network operating system and it is used as the platform for all products of the Juniper Networks SA series. In order to access IVE, the users must have authenticated successfully, and passed the host check procedure. After this, the IVE works as a gateway between the client and the internal network. As an exception to this, the network connect creates a direct tunnel between the client and the internal network. To provide secure connectivity between the SSL VPN device, the client, and the internal network, SSL/TLS protocol is used.

#### 7.3.4 Juniper Networks Host checker

Because SSL VPN makes it possible for users to access confidential and classified information resided on the company's internal servers, via any device with internet connection and appropriate web browser, additional security measures are required. Juniper has solved this problem by adding a host checker feature to all appliances of the SA family.

Host checker is a piece of software which is automatically installed on the computer when it is used for the first time. Host checker is used to perform tests, based on which client device can be categorized as safe or unsafe. These tests may include checking client for up-to-date antivirus software, certificates, registry entries, and other security features. After categorization is done, it can be used to determine which resources the client will be given access to. This way it is possible to restrict permissions given to the client who is accessing the company network from an unsafe source.

#### 7.3.5 Juniper SSL VPN levels of access

The biggest difference between Juniper SSL VPN and traditional IPsec VPN is the possibility to limit access given to the user. Juniper SSL VPN offers three layers of connection. The first layer is called core access, which allows the user to connect to internal web based resources and fileshares. After installing an activeX component, core access can also provide terminal services, SSH and Telnet connections. The second layer provides a Secure Application Manager, later referred as SAM. There are two ways of creating a SAM connection, Java-based and Windows-based. These two can be used together or as separate applications to create a SAM session. The third connection option provided by Juniper SSL VPN is network connect, which offers full end-to-end VPN connectivity between the client and the company network.

The first two layers use a Juniper SSL VPN device as a proxy-like service. This means that a connection from the client is established to the Juniper SSL VPN device. After the connection has been established, Juniper SSL VPN acts as a connecting gateway between the client and the dedicated server residing in the company's internal network. This provides enhanced security, since the client is not allowed to connect directly to the company's internal network.

#### 7.4 Juniper SSL VPN solution for Andritz Group

The Juniper SSL VPN was implemented as a part of the Andritz Group global network in 2008, in order to get more restricted access control and easier access to the company network. Currently there are two SSL VPNs deployed, one in Finland and one in Austria. These devices are administrated separately, yet the configurations of these devices should be similar, in order to provide the end-user with an identical portal page view no matter which SSL VPN device the user connects to. Since the current version of Juniper SSL VPN does not provide the centralized management feature, it is hard to keep the pages similar and to do so, lots of work is required. A centralized management feature should, however, be introduced in future releases.

Implementing the Juniper SSL VPN to the Andritz Group network environment allows resources to be shared based on AD groups. Sharing resources based on AD groups has proved its efficiency in the Andritz Group corporate network. The use of AD groups reduces the amount of administrative work, compared to maintaining static user databases locally. Together with Juniper SSL VPN's built-in SSO (single sign on) feature, users will receive a smooth and flexible end user experience while operating Juniper SSL VPN. Since the Andritz AD groups are defined based on divisions and locations of people rather than software used by people, it has been difficult to find suitable AD groups to determine specific roles which provide resources (concepts of roles and resources are explained in chapter 7.4.1). In order to provide users with required resources, several new AD groups have been created. To gain a functional and secure remote access solution, co-

operation with experts from different fields is required. In the Andritz Group corporate network this means interaction between the network, AD, security, and workstation teams.

A high level of security is one of the main requirements for the Andritz Group remote access connection. In order to enforce the high level of security a host check feature is used on all sign-in realms. In addition, user access to resources on internal servers has been reduced from the old days, when IPsec VPN was used. The Andritz Group is using a host check to ensure the user is running up-to-date antivirus software and device certificates. Without a valid device certificate or up-to-date antivirus software the user receives only limited resources.

An external user, who does not have the Andritz AD account, will be added to the Juniper SSL VPN's local user database or external one-time-password authentication server. In addition, all external users are host checked for up-to-date antivirus software, to prevent virus outbreaks in the company's internal network.

To prevent unauthorized access to the Andritz Group internal network, the SSL VPNs are configured to require users to provide two factor authentication. Firstly users are prompted for their AD username and password, and after successful AD authentication the user has to provide either a mobile token sent to their cell phone, a password from the password list or a time synchronized password created by Mobile Authentication Code Creator application.

Because Juniper SSL VPN is used to support the remote access needs of the Andritz Group production network, it is important that systems are redundant and backed up in case of hardware malfunction. The Andritz Group's Juniper SSL VPN environment is backed up to a designated server using the archiving feature of Juniper Networks SA devices. The archiving feature gives SSL VPN administrators the possibility to choose which configurations are backed up and how often this backup job occurs. Restoring the saved configurations from the backup file is an easy and fast procedure. In simulated backup restore situations Juniper SSL VPN has been fully operational in less than five minutes. The system snapshot

feature offered by Juniper Networks SA appliances is a less thorough backup of the system config. System snapshot is mainly used for troubleshooting purposes, but in some cases it can be used for backing up the system as well.

The complexity of the Andritz Group global network and AD structure provides a good testing ground for the Juniper SSL VPN administrator to test the troubleshooting tools provided by appliances of Juniper Networks SA series. Policy trace is a feature which allows the administrator to track login information, applications and services used by single users on single realms. It also offers detailed information on how the accessed applications have worked. In addition, Juniper SSL VPN offers tools for the administrator to simulate problems experienced by the users. Session recording tools can be used to gain detailed information regarding the SSL VPN session of the user. Session recording can be done based on username used for IVE authentication. Juniper Networks SA appliances also have an interface to perform basic network tests such as ping, tracert, and tcp dump to name but a few. The administrator can also print out debug logs, to help with troubleshooting of the system.

## 7.5 Using Juniper SSL VPN

Juniper Networks SA devices are based on the IVE operating system developed by Juniper Networks. After a successful user authentication, IVE is launched. Juniper Networks IVE is a clear and easy to use operating system and it is used for both administrative and end-user interfaces.

The following chapters will introduce configuring and using of the Juniper Networks IVE operating system. Both configuring and using the Juniper SSL VPN are covered from both end-user and administrative points of view.



### 7.5.1 Configuration and administration of Juniper SSL VPN

Start up configuration of Juniper Networks SA series SSL VPN is done via the console port situated in the front panel of the Juniper SSL VPN device. After initial configuration is done administration of the Juniper SSL VPN is done via web browser. As shown in FIGURE 18, administrative interface is clear and it provides the administrator with plenty of information regarding the system.

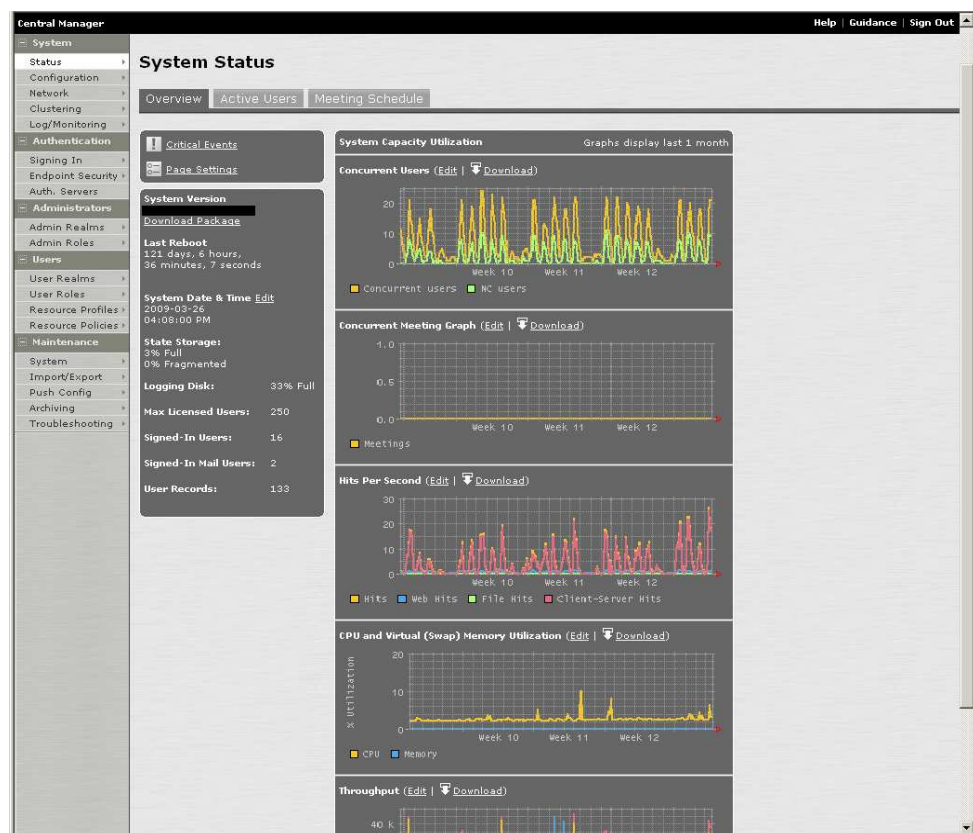


FIGURE 18. Juniper SSL VPN administrative web interface

The web browser based management interface is easy to access, from anywhere in the network, but it is also a security risk. The devices of the Juniper Networks SA series offer a wide variety of solutions in order to prevent unauthorized access to the administrative interface. It is possible for the administrator to define an IP ad-

dress or a group of IP addresses which are allowed to connect with administrative privileges. Another way of preventing unauthorized access to the administrative IVE is configuring the Juniper SSL VPN host checker feature with strict requirements.

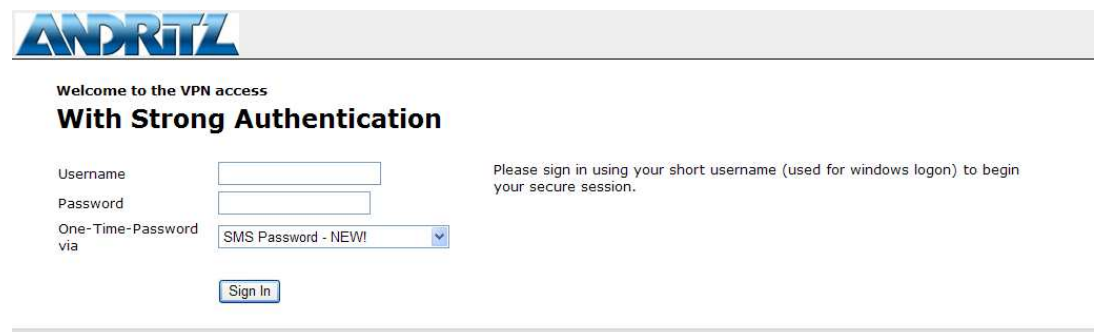
Juniper SSL VPN allows separation of users to realms and roles. Realms are selected while the user is logging into the system. This can be done by creating separate sign-in pages for different authentication methods. For example `www.something.com/ad` could be a realm for AD authentication. A single person can be listed as the user for several realms, but cannot be signed into more than one realm at the time. Even if the user had successfully authenticated to a realm it does not mean he would get any resources, since in order to receive resources the user must be assigned to a role. Roles can be assigned for a single user or a group of users inside the realm. The administrator can choose if the user has to select between roles assigned to him, or if resources granted by different roles are merged into one bigger set of resources for the user to access. The user can have different roles in different realms; this is, however, for the SSL VPN administrator to choose.

The SSL VPN administrator can easily add and remove resources and realms for each user via a system panel located on the left side of the web UI. This makes assigning users to roles and realms and configuring access rights inside these areas simple and clear.

In addition, there are several tools for troubleshooting problems encountered with SSL VPN. These tools include session simulation, session recording, detailed debug logs, and system snapshots. Each of these can be useful for different kinds of debug operations.

## 7.5.2 Using Juniper Networks SSL VPN – Secure Access

Using SSL VPN services is done via a web browser. Since almost every web browser available today has built-in support for the SSL/TLS protocol, it does not matter which browser is used. SSL VPN login pages can have different naming patterns depending on which authentication method will be used, for example SSL VPN connection using RSA tokens could be called `www.something.com/RSA`. After connection to a dedicated site has been established, the user is prompted to give his username and password. The SSL VPN login page is shown in FIGURE 19.



The screenshot shows a web page for ANDRITZ. At the top left is the ANDRITZ logo. Below it, the text reads "Welcome to the VPN access" followed by "With Strong Authentication" in bold. There are three input fields: "Username" (a text box), "Password" (a text box), and "One-Time-Password via" (a dropdown menu). The dropdown menu is currently set to "SMS Password - NEW!". To the right of these fields, a note says "Please sign in using your short username (used for windows logon) to begin your secure session." At the bottom of the form is a "Sign In" button.

FIGURE 19. SSL VPN login page with two factor authentication

When two-factor authentication is used, the user is required to provide his username and password, after which the user is prompted for a unique one-time-password (see FIGURE 20). The user has the possibility to choose a desired one-time-password option from the dropdown list.

The screenshot shows a web page for Andritz VPN access. At the top left is the Andritz logo. Below it, the text reads "Welcome to the VPN access" followed by "With Strong Authentication". A yellow box contains the "Challenge / Response" section. It asks the user to "Challenge: Please enter SMS password:" and provides instructions: "Enter the challenge string above into your token, and then enter the one-time response in the field below." There is a text input field labeled "Response:" and two buttons: "Sign In" and "Cancel".

FIGURE 20. Challenge/response one-time password via text message

After the user has been authenticated successfully, he will be provided with a web browser view of the services and applications available for him. A web browser view after successful authentication is presented in FIGURE 21. Accessing the resources and applications provided via SSL VPN is simple: single clicking the link on the main page opens a new web page or starts the application.

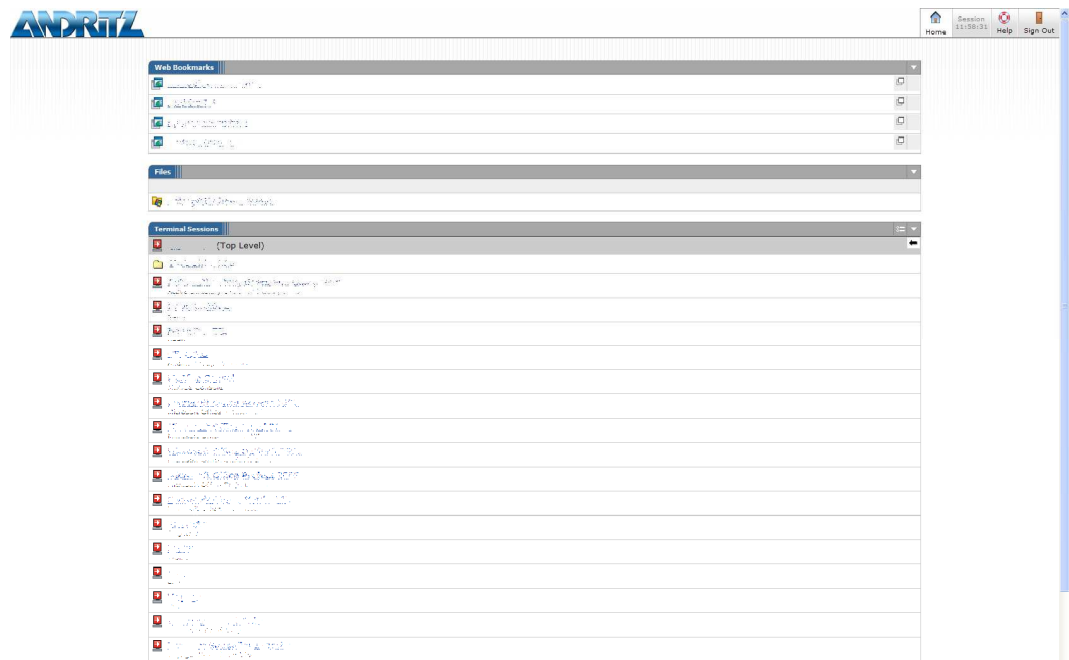


FIGURE 21. Andritz Group SSL VPN main page with strong authentication

After the user has successfully authenticated the following services (software, websites, fileshares and full network connect) are all just one click away from the main page. In addition, the mainpage view is clear and easy to use, which was one of the main criteria when the SSL VPN solution was selected.

#### 7.6 Goals to be achieved by changing remote access method

The primary goal in implementing a SSL VPN solution as part of the Andritz Group remote access environment was to limit user access to company resources so that only required resources and programs would be provided. Since this kind of access limitation could not be done by using traditional IPsec VPNs, new technology had to be introduced. In addition to access limitation, SSL VPN technology reduces administrative overhead caused by installing and maintaining the VPN software. In a big multinational company with over a thousand sales representatives worldwide, the possibility of accessing data easily over Internet almost anywhere in the world was also one of the key features, which gave the SSL VPN an edge compared to the original IPsec VPN.

Since the SSL VPN system will be used by Andritz personnel worldwide, it is important that systems are redundant and the system can be used on different platforms. Additional requirements for the system included the possibility to use authentication methods configured to the current IPsec solution and a clear, easy-to-use management interface.

## 8 PROJECT OVERVIEW AND RESULTS

### 8.1 Finding a suitable secure remote access solution

Like any other similar project, in order to find a suitable secure remote access solution for the needs of the Andritz Group, comparing different solutions and devices was required. In this project three solutions were compared: Check Point IPsec VPN, Nortel VPN Gateway 3000 series and Juniper Networks Secure Access – SSL VPN.

After thorough investigation the Juniper Networks Secure Access – SSL VPN solution was selected as the new secure remote access solution for the Andritz Group. This was because previous co-operation with Juniper Networks has been successful, and because Juniper Networks Secure Access – SSL VPN devices were able to provide a complete SSL VPN solution with required services and worldwide support, but also because Juniper has superior client based service development.

### 8.2 Requirements for the remote access solution

The primary goal in implementing the SSL VPN solution as part of the Andritz Group remote access environment was to limit user access to company resources so that only required resources and programs would be provided. In addition to access limitation, SSL VPN technology is used to reduce administrative overhead caused by installing and maintaining the VPN client software. In a big multinational company with over a thousand sales representatives worldwide, the possibility of accessing data easily over Internet almost anywhere in the world was also one of the key features, which gave the SSL VPN an edge compared to the original IPsec VPN. Since the SSL VPN system will be used by Andritz personnel worldwide, it is important that systems are redundant and system can be used on

different platforms. Additional requirements for the system included possibility to use authentication methods configured to the current IPsec solution and a clear, easy-to-use management interface.

In addition, frequent changes in used software and the network environment require the remote access solution to be easily updatable. Changes in the network environment are something the company has to prepare for, and downtime caused by the change of the network environment can usually be avoided by having a redundant SSL VPN system. Problems with incompatible software are to be solved in co-operation between the company and the supplier. Providing frequent security and service updates is to be done by Juniper Networks.

### 8.3 Results of the project

More precise access control provided by Juniper SSL VPN has drastically improved the security of remote networking in the Andritz Group. In addition, there is no longer fear of infected remote hosts contaminating the whole company network, because of the additional security provided by the host check feature of Juniper SSL VPN. Clients are already reporting about improved connectivity, which is most likely because the traffic between the client and the SSL VPN device is compressed. Also, the possibility to access personal e-mails from any computer with internet connectivity has received a lot of positive feedback from the clients.

So far the project has been successful, and users have been satisfied with the new remote access solution provided by the Andritz Group. In addition, the workstation team has been pleased with reduced workload, since no new VPN client installations have been required. Now it is also possible to perform more precise checks for access and user control. Using SSL VPN also provides tools for enforcing security of the client devices. All in all, Juniper Networks Secure Access products have found their place in the Andritz Group corporate network.

#### 8.4 Future of the project

In the future the Andritz Group is planning to implement centralized management for the Secure Access products provided by Juniper Networks. However, this centralized management software is still under development (by Juniper Networks). The centralized management software Juniper Networks is going to release will work with all products of Juniper Networks, which makes it easier for the Andritz Group to expand the usage of services provided by Juniper. The future will bring several challenges independent from the Andritz Group or Juniper networks, like new versions of Windows, requirement for more secure networking and software that is not fully compatible with Juniper SSL VPN devices. However, these issues can be solved in co-operation with different parties. This allows Juniper to develop their products and the Andritz Group to expand its knowledge of SSL VPN solutions.

Because no client software is required, computers consume less energy, which allows them to perform longer with a single charging. Reduced energy consumption of Andritz Group computers will help saving natural resources and fight back the global warming, possibly saving the world along the way.



## SOURCES

Advanced technologies: VPN, 2005. BELNET the network of knowledge [network publishing]. 2005 BELNET [referred 10.1.2009] Available:

<http://www.belnet.be/en/index2.php?upnr=165>

Aladdin, 2009. VPN Authentication [network publishing] 2009 Aladdin knowledge system ltd. [referred 12.3.2009] Available:

<http://www.aladdin.com/etoken/solutions/secure-vpn-access.aspx>

Andritz, 2009a. Andritz Oy general information [network publishing]. 2009 Andritz Oy [referred 28.3.2009] Available:

[http://finland.andritz.com/aboutus/aboutus\\_perustiedot.cfm](http://finland.andritz.com/aboutus/aboutus_perustiedot.cfm)

Andritz, 2009b. History of Andritz Group [network publishing]. 2009 Andritz Oy [referred 28.3.2009] Available:

[http://finland.andritz.com/aboutus/aboutus\\_historia-1999.cfm](http://finland.andritz.com/aboutus/aboutus_historia-1999.cfm)

Andritz, 2009c. History of Andritz Group [network publishing]. 2009 Andritz Oy [referred 28.3.2009] Available:

[http://finland.andritz.com/aboutus/aboutus\\_historia1999-2008.cfm](http://finland.andritz.com/aboutus/aboutus_historia1999-2008.cfm)

Andritz, 2009d. Divisionaprofiilit [network publishing]. 2009 Andritz Oy [referred 28.3.2009] Available:

[http://finland.andritz.com/aboutus/aboutus\\_division\\_profiles.cfm](http://finland.andritz.com/aboutus/aboutus_division_profiles.cfm)

Authentication, 2009. [network publishing] 2009 Wikipedia [referred 22.2.2009]

Available: <http://en.wikipedia.org/wiki/authentication>

Biometric Authentication, 2009. [network publishing] 2009 Wikipedia [referred

22.2.2009] Available: [http://en.wikipedia.org/wiki/Biometric\\_authentication](http://en.wikipedia.org/wiki/Biometric_authentication)

Bleumer G. 1999. Biometric authentication and multilateral security [network publishing]. 1999 AT&T Labs-Research [referred 20.2.2009] Available: <http://www.semper.org/sirene/people/gerrit/papers/bioauth.pdf>

Certificate Authority, 2009. [network publishing] 2009 Wikipedia [referred 22.2.2009] Available: [http://en.wikipedia.org/wiki/Certificate\\_Authority](http://en.wikipedia.org/wiki/Certificate_Authority)

Certificate Revocation List, 2009. [network publishing] 2009 Wikipedia [referred 22.2.2009] Available: [http://en.wikipedia.org/wiki/Certificate\\_Revocation\\_List](http://en.wikipedia.org/wiki/Certificate_Revocation_List)

Check Point, 2009. IPsec VPN software blade[network publishing]. 2009 Check Point Software Technologies Limited [referred 15.3.2009] Available: <http://www.checkpoint.com/products/softwareblades/ipsec-virtual-private-network.html>

China Telecom, 2008. [report] 2008 China Telecom [referred 15.3.2009]

Connected: An Internet Encyclopedia, 2009. Block ciphers [network publishing] 2009 Connected: An Internet Encyclopedia [referred 26.2.2009] Available: <http://www.lincoln.edu/math/rmyrick/ComputerNetworks/InetReference/143.htm>

Cryptographic hash function, 2009. [network publishing] 2009 Wikipedia [referred 20.3.2009] Available: [http://en.wikipedia.org/wiki/Cryptographic\\_hash\\_function](http://en.wikipedia.org/wiki/Cryptographic_hash_function)

Dierks T. & Allen C. 1999. RFC 2246[network publishing] 1999 IETF [referred 22.2.2009] Available: <http://www.ietf.org/rfc/rfc2246.txt>

Encapsulating Security Payload, 2009. [network publishing] 2009 Wikipedia [referred 22.3.2009] Available: [http://en.wikipedia.org/wiki/Encapsulating\\_Security\\_Payload#Encapsulating\\_Security\\_Payload\\_.28ESP.29](http://en.wikipedia.org/wiki/Encapsulating_Security_Payload#Encapsulating_Security_Payload_.28ESP.29)

Future of Identity in the Information Society, 2007. [network publishing] 2009

FIDIS [referred 16.2.2009] Available:

[http://www.fidis.net/typo3temp/tx\\_rlmpofficelib\\_2cc6359f5b.jpg](http://www.fidis.net/typo3temp/tx_rlmpofficelib_2cc6359f5b.jpg)

Girard John, 2007. Magic quadrant for SSL VPN [report] 2007 Gartner [referred

20.3.2009] Available: PDF document

Harkins D. & Carrel D. 1998. RFC 2409 [network publishing] 1998 IETF Avail-

able: <http://www.ietf.org/rfc/rfc2409.txt>

Hydropower, 2009. [network publishing] 2009 Wikipedia [referred 29.3.2009]

Available: <http://en.wikipedia.org/wiki/Hydropower>

Internet Key Exchange, 2009. [network publishing] 2009 Wikipedia [referred

21.3.2009] Available: [http://en.wikipedia.org/wiki/Internet\\_Key\\_Exchange](http://en.wikipedia.org/wiki/Internet_Key_Exchange)

IPsec, 2009. [network publishing] 2009 Wikipedia [referred 21.3.2009] Available:

<http://en.wikipedia.org/wiki/IPsec>

Juniper Networks, 2008. [conversation 21.10.2008] 2008 Juniper Networks [re-

ferred 10.11.2008]

Keith Schultz, 2005. SSL VPN come of age [review] 2005 IT World Canada [re-

ferred 21.3.2009] Available: <http://www.itworldcanada.com/product/2/53978.html>

Kent S. & Atkinson R. 1998. RFC 2401 [network publishing] 1998 IETF [referred

20.2.2009] Available: <http://www.ietf.org/rfc/rfc2401.txt>

Kent S. & Atkinson R. 1998. RFC 2402 [network publishing] 1998 IETF [referred

20.2.2009] Available: <http://www.ietf.org/rfc/rfc2402.txt>

Kent S. & Atkinson R. 1998. RFC 2406 [network publishing] 1998 IETF [referred 20.2.2009] Available: <http://www.ietf.org/rfc/rfc2406.txt>

Kozierok C. M, 2005. IPsec Authentication Header [network publishing] 2005 The TCP/IP Guide [referred 21.3.2009] Available: [http://www.tcpipguide.com/free/t\\_IPSecAuthenticationHeaderAH-4.htm](http://www.tcpipguide.com/free/t_IPSecAuthenticationHeaderAH-4.htm)

Message authentication code, 2007. [network publishing] 2009 Wikipedia [referred 20.3.2009] Available: [http://en.wikipedia.org/wiki/Message\\_authentication\\_code](http://en.wikipedia.org/wiki/Message_authentication_code)

Microsoft Technet, 2009. SSL/TLS in detail [network publishing] 2009 Microsoft [referred 1.3.2009] Available: <http://technet.microsoft.com/en-us/library/cc785811.aspx>

Minnes G. 2009. Pulp and Paper Industry [network publishing] 2009 The Canadian Encyclopedia [referred 28.3.2009] Available: <http://www.thecanadianencyclopedia.com/index.cfm?PgNm=TCE&Params=A1ART0006564>

Nortel, 2009. Nortel Secure gateway 3000 series [network publishing] 2009 Nortel networks [referred 7.4.2009] Available: [http://products.nortel.com/go/product\\_content.jsp?parId=0&segId=0&prod\\_id=53021](http://products.nortel.com/go/product_content.jsp?parId=0&segId=0&prod_id=53021)

One-time password, 2009. [network publishing] 2009 Wikipedia [referred 22.2.2009] Available: [http://en.wikipedia.org/wiki/One-time\\_password](http://en.wikipedia.org/wiki/One-time_password)

Packet Switched Network, 2009. [network publishing] 2009 Wikipedia [referred 10.2.2009] Available: [http://en.wikipedia.org/wiki/Packet\\_switched\\_network](http://en.wikipedia.org/wiki/Packet_switched_network)

Perlmutter B. & Zarkower J. 2001. Virtuaaliset yksityisverkot. Helsinki: Edita.

Phifer Lisa A. 2001. VPNs: Virtually Anything? [network publishing] 2001 Core Competence Inc. [referred 27.1.2009] Available:

<http://www.corecom.com/html/vpn.html>

Public-key cryptography, 2009. [network publishing] 2009 Wikipedia [referred 22.3.2009] Available: [http://en.wikipedia.org/wiki/Public-key\\_cryptography](http://en.wikipedia.org/wiki/Public-key_cryptography)

Public key infrastructure, 2009. [network publishing] 2009 Wikipedia [referred 22.2.2009] Available: [http://en.wikipedia.org/wiki/Public\\_key\\_infrastructure](http://en.wikipedia.org/wiki/Public_key_infrastructure)

Public Switched Telephone Network, 2009. [network publishing] 2009 Wikipedia [referred 10.2.2009] Available:

[http://en.wikipedia.org/wiki/Public\\_Switched\\_Telephone\\_Network](http://en.wikipedia.org/wiki/Public_Switched_Telephone_Network)

Pulp and paper industry, 2009. [network publishing] 2009 Wikipedia [referred 29.3.2009] Available: [http://en.wikipedia.org/wiki/Pulp\\_and\\_paper](http://en.wikipedia.org/wiki/Pulp_and_paper)

Security Association, 2009. [network publishing] 2009 Wikipedia [referred 21.3.2009] Available: [http://en.wikipedia.org/wiki/Security\\_Association](http://en.wikipedia.org/wiki/Security_Association)

Self-signed certificate, 2009. [network publishing] 2009 Wikipedia [referred 22.2.2009] Available: [http://en.wikipedia.org/wiki/Self-signed\\_certificate](http://en.wikipedia.org/wiki/Self-signed_certificate)

Steinberg J. & Speed T. 2005. Understanding SSL VPN [eBook] 2005 Packt Publishing Ltd.

Stream cipher, 2009. [network publishing] 2009 Wikipedia [referred 20.3.2009] Available: [http://en.wikipedia.org/wiki/Stream\\_cipher](http://en.wikipedia.org/wiki/Stream_cipher)

Symmetric-key algorithm, 2009. [network publishing] 2009 Wikipedia [referred 20.3.2009] Available: [http://en.wikipedia.org/wiki/Symmetric-key\\_algorithm](http://en.wikipedia.org/wiki/Symmetric-key_algorithm)

Virtual Private Network, 2009. [network publishing] 2009 Wikipedia [referred 22.3.2009] Available: [http://en.wikipedia.org/wiki/Virtual\\_Private\\_Network](http://en.wikipedia.org/wiki/Virtual_Private_Network)

X.25, 2009. [network publishing] 2009 Wikipedia [referred 9.2.2009] Available: <http://en.wikipedia.org/wiki/X.25>

X.509, 2009. [network publishing] 2009 Wikipedia [referred 22.2.2009] Available: <http://en.wikipedia.org/wiki/X.509>

Yao-An Liao J, 2003. Secure Remote data access [network publishing] 2003 IBM [referred 21.3.2009] Available: <http://www.ibm.com/developerworks/web/library/wa-secdomdat/>

## ATTACHMENTS