STUK

STUK-YTO-TR 174 January 2001

# SECURE TRANSFER OF SURVEILLANCE DATA OVER INTERNET USING VIRTUAL PRIVATE NETWORK TECHNOLOGY

## Field trial between STUK and IAEA

Report on Task FIN A929
of the Finnish Support Program
to IAEA Safeguards

**H. Smartt, R. Martinez, S. Caskey**
Sandia National Laboratories
**T. Honkamaa, T. Ilander, R. Pöllänen**
STUK
**N. Jeremica, G. Ford**
Nokia

STUK • SÄTEILYTURVAKESKUS • STRÅLSÄKERHETSCENTRALEN
RADIATION AND NUCLEAR SAFETY AUTHORITY

The conclusions presented in the STUK report series are those of the authors and do not necessarily represent the official position of STUK.

ISBN 951-712-430-9
ISSN 0785-9325

Oy Edita Ab, Helsinki 2001

*SMARTT Heidi, MARTINEZ Robert, CASKEY Susan (Sandia National Laboratories), HONKAMAA Tapani, ILANDER Tarja , PÖLLÄNEN Roy (STUK), JEREMICA Nick , FORD Gary (Nokia).*
*Secure transfer of surveillance data over Internet using Virtual Private Network technology. Field trial between STUK and IAEA. Report on Task FIN A929 of the Finnish Support Program to IAEA Safeguards. STUK-YTO-TR 174. Helsinki 2001. 14 pp. + Appendix 1 pp.*

**ISBN** 951-712-430-9
**ISSN** 0785-9325

**Keywords**: safeguards, remote monitoring, virtual private network, VPN

# ABSTRACT

One of the primary concerns of employing remote monitoring technologies for IAEA safeguards applications is the high cost of data transmission. Transmitting data over the Internet has been shown often to be less expensive than other data transmission methods. However, data security of the Internet is often considered to be at a low level. Virtual Private Networks has emerged as a solution to this problem.

A field demonstration was implemented to evaluate the use of Virtual Private Networks (via the Internet) as a means for data transmission. Evaluation points included security, reliability and cost. The existing Finnish Remote Environmental Monitoring System, located at the STUK facility in Helsinki, Finland, served as the field demonstration system. Sandia National Laboratories (SNL) established a Virtual Private Network between STUK Headquarters in Helsinki, Finland, and IAEA Headquarters in Vienna, Austria. Data from the existing STUK Remote Monitoring System was viewed at the IAEA via this network.

The Virtual Private Network link was established in a proper manner, which guarantees the data security. Encryption was verified using a network sniffer. No problems were encountered during the test.

In the test system, fixed costs were higher than in the previous system, which utilized telephone lines. On the other hand transmission and operating costs are very low. Therefore, with low data amounts, the test system is not cost-effective, but if the data amount is tens of Megabytes per day the use of Virtual Private Networks and Internet will be economically justifiable. A cost-benefit analysis should be performed for each site due to significant variables.

*SMARTT Heidi, MARTINEZ Robert, CASKEY Susan (Sandia National Laboratories), HONKAMAA Tapani, ILANDER Tarja , PÖLLÄNEN Roy (STUK), JEREMICA Nick , FORD Gary (Nokia). Valvontatiedon turvallinen siirto Internetissä virtuaalisen erillisverkon avulla. Kenttäkoe STUKin ja IAEA:n välillä. Raportti tehtävässä FIN A929 Suomen IAEA-Safeguards-tukiohjelmassa. STUK-YTO-TR 174. Helsinki 2001. 14 s. + liite 1 s.*

**ISBN** 951-712-430-9
**ISSN** 0785-9325

**Avainsanat:** safeguards, kaukovalvonta, virtuaalinen erillisverkko, VPN

# TIIVISTELMÄ

Tiedonsiirtokustannukset ovat merkittävin yksittäinen menoerä, kun Kansainvälinen Atomienergiajärjestö IAEA suunnittelee kaukovalvontasovelluksen käyttöönottoa. Tiedon siirtäminen Internetin kautta on usein edullisinta, mutta tietoturva koetaan usein puutteelliseksi. Virtuaalinen erillisverkko (Virtual Private Network, VPN) on ratkaisu, joka parantaa Internetin tietoturvallisuutta.

Tämä kenttäkoe oli IAEAn, Sandia National Laboratory:n (SNL) ja Säteilyturvakeskuksen (STUK) yhteishanke. Kenttäkokeella esiteltiin ja arvioitiin VPN-tekniikan mahdollisuuksia IAEAn kaukovalvontasovelluksiin. Arvioitavia asioita olivat turvallisuus, luotettavuus ja kustannukset. Koepaikkana oli Säteilyturvakeskuksen toimitilan katolla sijaitseva laboratorio, jonka SNL oli varustanut kaukovalvontalaitteilla. Kokeen aikana kaukovalvontalaitteiden välittämät tiedot välitettiin Internetin kautta Kansainvälisen Atomienergiajärjestön IAEAn päämajaan Wieniin. VPN-laitteisto ja -ohjelmisto suojasi kaiken välitetyn tiedon.

Tiedossa olevan kokemuksen mukaan VPN-tekniikka on turvallista ja luotettavaa, kun laitteet ja ohjelmistot asennetaan hyvin. Kokeessa tiedon salaus varmistettiin valvomalla verkossa siirtyvää tietoa. Testin aikana ei havaittu teknisiä ongelmia.

Testijärjestelmän laitteisto- ja asennuskustannukset ovat suurempia kuin käytettäessä modeemia ja puhelinlinjoja. Toisaalta lähetys-, ja käyttökulut lähes olemattomia. Hyvin pienen tietomäärän siirtäminen Internetin kautta ei ole taloudellisesti järkevää. Jos siirrettävä tietomäärä on kymmeniä megatavuja päivässä VPN-tekniikan ja Internetin käyttö on taloudellisesti perusteltavissa. Kustannusanalyysi on tehtävä jokaiselle sovellukselle ja sijoituspaikalle erikseen.

# ACKNOWLEDGEMENTS

On the Finnish side this project is financed under the umbrella task FIN A 929 of the Finnish support programme to the IAEA safeguards.

On the U.S. side this project is financed by the Department of Energy.

# CONTENTS

# 1 INTRODUCTION

Operating remote monitoring systems requires data connections from the sites under IAEA safeguards to the IAEA offices. These sites exist globally, and the traditional method for remote data transmission are leased lines from the site to the IAEA. These leased lines are typically priced by distance, which can get expensive in an international deployment. Therefore the high cost of data transmission has become an obstacle to operating existing, or implementing new remote monitoring systems.

An alternative to a leased line is a shared public network, such as the Internet. Transmitting data over the Internet can be less expensive than other data transmission methods since the backbone is shared with many users. The major cost of implementing an Internet-based network solution becomes connecting to the Internet; this is known as the "last mile". The connection to the Internet can be accomplished via ISDN, wireless, DSL (Digital Subscriber Line), satellite, leased line (the distance from the site to an Internet Service Provider (ISP)), or phone line based on individual site geography and current infrastructure.

The Internet has other advantages beyond cost-effectiveness, such as scalability. With a leased line, both sites will require hardware and configuration, as well as a dedicated point-to-point connection, possibly over a long distance (Figure 1). However, by using the Internet, only the new site requires any additional hardware and configuration. Each site only has to connect to the nearest ISP thus utilizing the already-in-place infrastructure (Figure 2).

Another benefit of the Internet is reliability. If a link in the Internet backbone fails during a communications session, the packets of data will automatically be re-routed and the session will not terminate. With a leased line, new routes can be defined in the event of a link failure, but the amount of time to accomplish this is too long to maintain most sessions.

The well-publicized drawback of the Internet has been the lack of data security. Data can be intercepted, deleted, or modified by parties with ill intent. Leased lines can also be insecure since the network is also shared, albeit with less users than Internet. Therefore, a customer must rely on the reliability and security of the leased line operator. Virtual Private Networks (VPNs) have emerged as a solution to data security problems, thus allowing the Internet to be a viable data transmission method for remote monitoring.

The present report describes the field trial, where remote monitoring data is transferred securely via Internet from STUK, Helsinki, Finland to IAEA, Vienna, Austria. This field trial took place in May–November 2000. The focus in this project is on Internet data transfer. The concept of remote monitoring has been successfully demonstrated earlier at the same site in the first field trial in February–August 1998 between STUK, SNL and IAEA. At that time phone lines and modems were used as a transmission path.

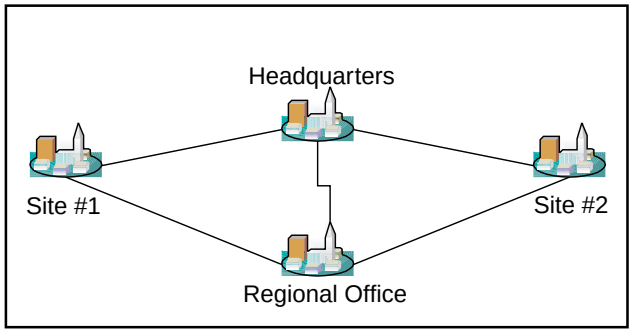


***Figure 1.*** *Leased-line Wide Area Network.*

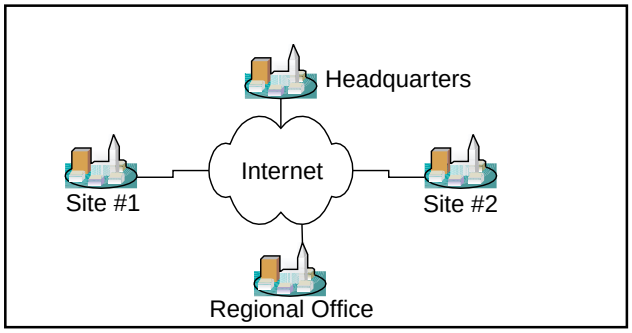


***Figure 2.*** *Internet-based Wide Area Network.*

# 2 DESCRIPTION OF VPN

A VPN allows secure data transmission over an untrusted public network, such as the Internet. VPN users can define encrypted and/or authenticated tunnels through the Internet. Encryption converts data from a readable format to cipher text that only the intended recipient can decipher. Most VPNs include encryption algorithms such as 3DES, DES, RC5, Blowfish, CAST, or IDEA. Authentication verifies that the data has not been altered. It does this by creating a unique signature based on the data. If the data were altered, a re-authentication would show mismatched signatures. VPN authentication can use a number of algorithms including MD5 and SHA-1.

VPNs can be implemented in either software or hardware, and each solution has benefits and drawbacks. Software VPN solutions allows for encryption and/or authentication at each computer, rather than the hardware "gateways", which are located within the local area network. Hardware has better performance, especially if using strong encryption, such as 3DES. However, the data behind the hardware will not be encrypted and thus should be in a trusted environment.

Many VPN solutions are based on IPSec. IPSec is a draft standard being developed by the Internet Engineering Task Force (IETF) than runs on TCP/IP. The goal of IPSec is to provide a set of standards for Internet Security. Different VPN vendors are able to interoperate using IPSec.

In a non-VPN solution, a key management policy for encryption and authentication is typically manually implemented. However, with almost all IPSec-based VPNs, key management is handled by the Internet Key Exchange Protocol (IKE) and is automatic.

In an example site-to-site VPN configuration, a computer at Site A wants to send encrypted and authenticated data to a computer at Site B. The data from Site A is first fragmented into IP (Internet Protocol) packets that contain both the data and an IP header. This IP header contains the IP address of the source (computer at Site A) and destination (computer at Site B) as well as other protocol information. The IP packet is then routed through the internal network to the VPN hardware, or "gateway", which encrypts and authenticates the intercepted packet and adds a new IP header (Figure 3). The new IP header contains the IP address of the VPN gateways at both Site A and B, rather than the actual computers at each site. This can be an advantage, since the IP addresses of the source and destination are now hidden. The new packet is routed to the Internet, where it finds its way to the VPN gateway at Site B. The packet is now authenticated, decrypted, and sent to the appropriate destination computer at Site B.

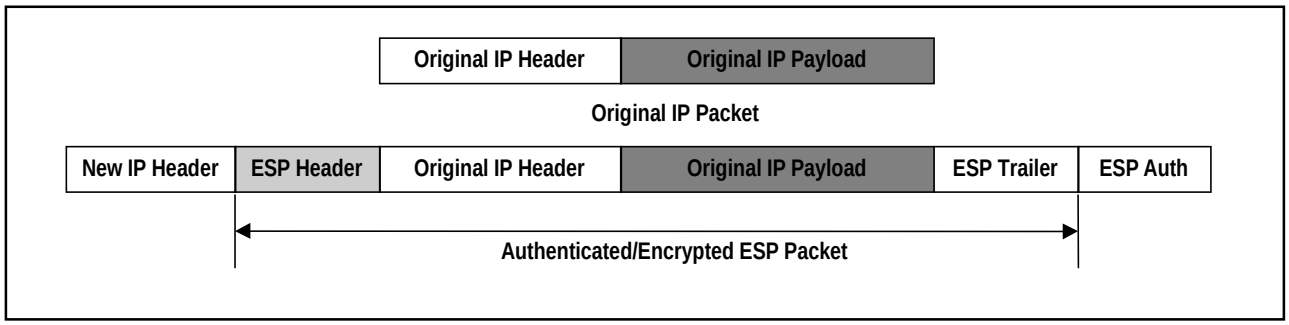


***Figure 3.*** *To convert an IP packet into an IPSec-compliant ESP packet, or Encapsulated Security Payload packet, the IP packet is encapsulated, encrypted, and authenticated.*

# 3 DESCRIPTION OF THE TEST SITE

Environmental monitoring laboratory located at a laboratory on the roof of STUK's headquarters was selected as a test site. The laboratory is equipped with an automatic aerosol sampler, known as CINDERELLA.STUK, which performs aerosol sampling, sample preparation and sample measurement without any need of human intervention. Reporting the results is also done automatically using Internet technology in STUK's intranet.

The schematic drawing of the test site is in Figure 4. The station and automatic sampler have thoroughly been reported in Toivonen et al., 1998 and Pöllänen et al, 1999. After these reports no major updates have been done in the sampling system.

Equipping a fully automated sampler with remote monitoring equipment is of particular interest, since it enables leaving the sampling station unattended for long periods of time. The first field trial of the International Remote Monitoring Project between STUK, SNL and IAEA took place in February–August 1998, where the laboratory was equipped with different types of door sensors, limit switches, motion sensors and a camera. In the first project the concept of remote monitoring has been successfully demonstrated. At that time telephone lines and modems were used as a transmission path.

The test site had existing Internet connections. All the traffic is routed via the firewall computer.

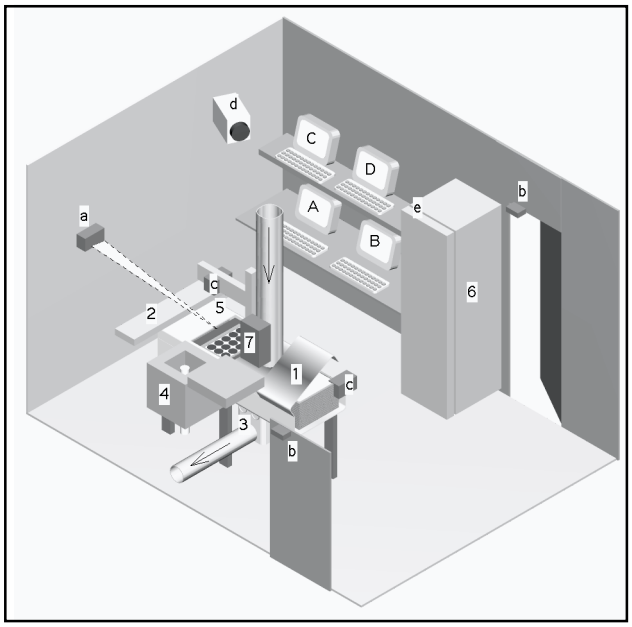


***Figure 4.*** *Automated air sampling station. This figure is adopted from Pöllänen et al, 1999. The equipment consists of 1) air sampling unit, 2) sample preparation unit, 3) real-time monitoring and alarm unit, 4) counting unit, 5) sample storage, 6) cabinet for remote monitoring site collection equipment and 7) aerosol authentication apparatus. The remote monitoring system has a break beam sensor (a), door sensors (b), air sampler door sensors (c), a video camera (d) and cabinet door sensors (e). Computers are for real-time monitoring (A), process monitoring and HPGe data acquisition and presentation (B), weather data measurements (C) and intranet / internet connections (D).*

# 4 INSTALLATION OF VPNs AT STUK AND IAEA

## 4.1 STUK Headquarters, Helsinki, Finland

The purpose of this installation and demonstration was to evaluate the cost-effectiveness, security, and reliability of VPN as a means for transmitting data over the Internet. In the process, the existing "Finnish Remote Monitoring System" software was also upgraded to the Sandia National Laboratories developed Material Monitoring Software (MMS). This was required to allow the remote monitoring data (sensors and video) to be displayed as Internet web pages.

The installation team included participants from SNL, Nokia, and STUK. The process commenced with a meeting to discuss and agree on the installation plan that was generated by SNL. The installation plan required that the necessary work at STUK be completed within three days.

The existing computer and camera were removed and prepared for shipment back toSNL . Nokia verified that the STUK local area network (LAN) was prepared for the VPN installation. This required the STUK network administrator to configure the network firewall to allow ESP (Encapsulation Security Payload) and IKE (Internet Key Exchange) protocols to pass through the firewall.

A new computer, a new camera , and VPN hardware were then installed. A power cable was assembled so that the VPN hardware could receive power from the existing Echelon sensor network power supply. The VPN hardware was configured, and the VPN "client" software was installed on a laptop so that a local test could be performed. The encrypted/authenticated (VPN) tunnel was tested using the software client to hardware configuration. During the test, the client was unable to connect to the VPN hardware. A setting on the STUK LAN was changed and the test was successful.

The new MMS software for data collection, storage, and dissemination was installed and configured to operate with the existing Echelon (sensor) network. The sensors included two balanced magnetic switches (BMS), one on each room door, an infra-red motion sensor, a photo-electric breakbeam sensor, tamper switches on the system equipment rack, and tamper switches on the STUK air sampler instrumentation. The integration of the existing Echelon sensors with the MMS software was successfully completed without any anomalies. The sensor network and camera were configured such that whenever the breakbeam sensor detected the movement of the air sampler's robotic arm an image was captured. The camera was also programmed to capture an image every twelve hours.

SNL next performed an end-to-end test of the entire system using a test plan. The system worked successfully and STUK and SNL signed the test plan, signifying acceptance of the system. Backups of the MMS and VPN databases were copied onto disks and passwords were distributed to proper individuals.

## 4.2 IAEA Headquarters, Vienna, Austria

The following week, SNL and Nokia installed the VPN client software on a training computer (containing a CompuServe Internet Account and Internet Explorer Software) provided by the IAEA.

The remote monitoring data from STUK was then accessed via the Internet using the encrypted/authenticated VPN tunnel. The data was displayed on web pages using an Internet Browser. A second demonstration was set up at the IAEA

involving all VPN hardware connecting two separate computers. Approximately ten IAEA employees attended each demonstration.

After the demonstrations, SNL and Nokia relocated the VPN hardware demonstration to the systems infrastructure department at the IAEA, uninstalled the VPN client from the training room computer, and trained the IAEA on installing the VPN client on a more permanent computer for the duration of the field demonstration.

A software client connection, rather than a direct hardware connection between two VPN modules, was established between IAEA and STUK because of internal security issues on the IAEA LAN. STUK/IAEA Virtual Private Network Diagram is shown in Figure 5.

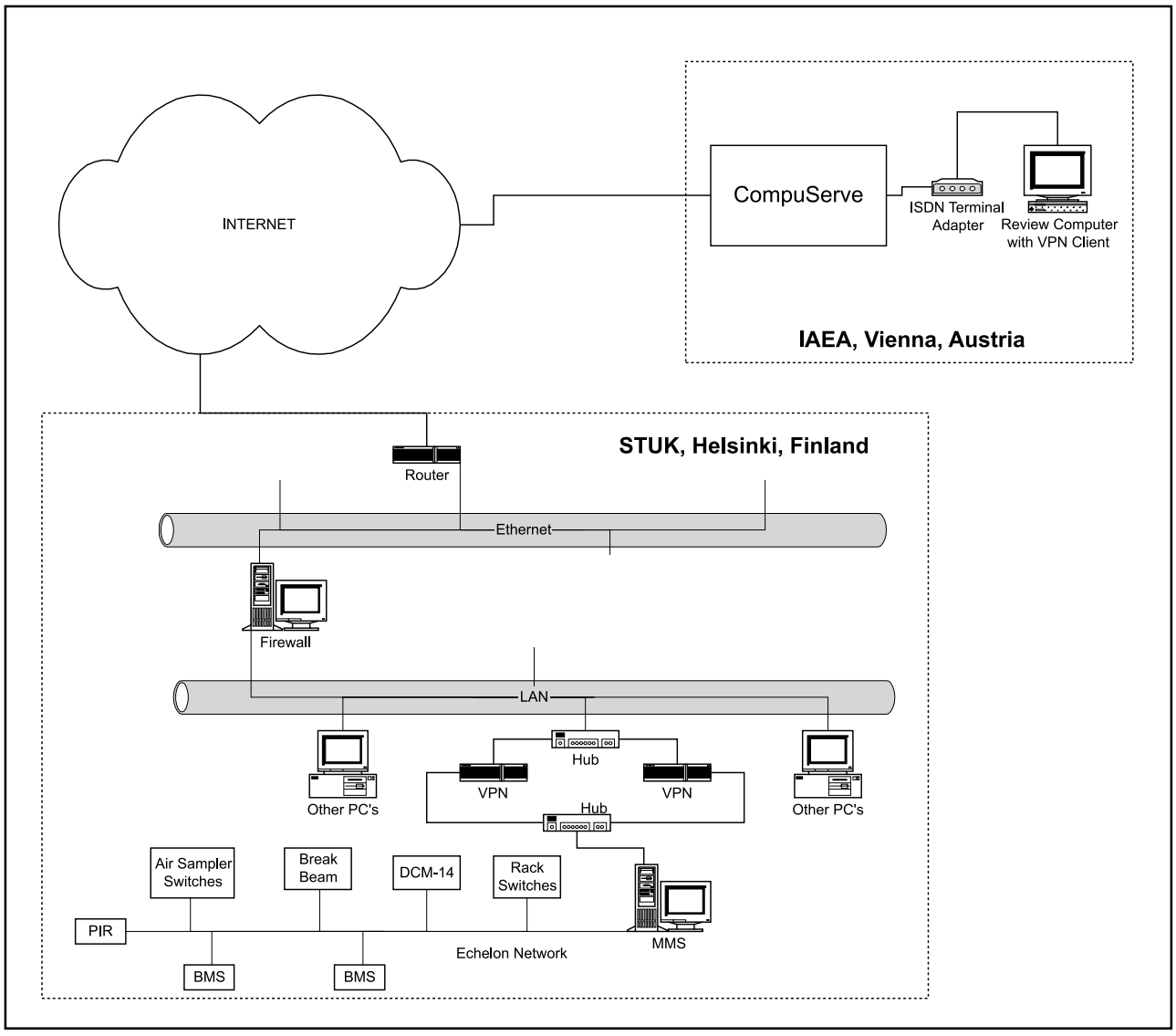


***Figure 5.*** *STUK/IAEA Virtual Private Network Diagram.*

# 5 RESULTS AND EXPERIENCES OF THE FIELD TRIAL

During the test the VPN hardware operated continuously. The VPN software client established connections with the VPN hardware on a consistent basis. The VPN connection was checked several times per week from SNL. The IAEA did not initially have the VPN client permanently installed, and thus was connecting to the STUK system only during this trial. IAEA had no problems establishing the connection to STUK and viewing data.

No security problems were discovered. The VPN hardware and software was configured for 3DES encryption, HMAC SHA-1 integrity (data authentication), and certificates for source authentication. Encryption re-keying occurs every hour, and authentication re-keying occurs every 8 hours. Encryption can be verified using a network sniffer.

In a VPN solution, every access point on each end must be secure. It is possible for an attacker to install a program on one of the end point systems, which would allow them to use the VPN to access the system on the other end without detection. In the current demonstration system, the MMS computer at STUK is only connected to the VPNs, and the IAEA is using a "stand-alone" computer to dial-out to CompuServe, thus both end point systems are secure.

Cost estimate analysis (APPENDIX 1) for this case show that installing VPN technology is not beneficial, because the dataflow from STUK to IAEA is low (25 kbytes per day). However, an increase in the amount of data, or the number of VPN applications (such as remote access for e-mail or protecting other computers or networks), would significantly change the cost-benefit. For example, increasing the amount of data to 25 Mbytes per day and keeping all other factors constant, the payback period would be 16 months.

# 6 CONCLUSIONS

A VPN solution across the Internet increases security when compared to a leased line because data cannot be accessed except by the intended users. With a leased line, the Phone Company as well as other customers must be trusted. The Internet can allow cost-effective, scalable, and reliable communication methods between two or more sites.

Technology described in this report can provide substantial savings in data transmission costs. It should be emphasized that a cost-benefit analysis should be performed for each site due to significant variables. Typically fixed cost are high, but transmission and operating costs are very low.

The combination of ensured data security and potential low operating costs make VPNs an attractive alternative for both intra-site and inter-site data transmission. That, in turn, makes remote monitoring a much more effective and efficient tool for accomplishing the IAEA mission of International Safeguards.

# REFERENCES

Toivonen H, Honkamaa T, Ilander T, Leppänen A, Nikkinen M, Pöllänen R, Ylätalo S: Automated high-volume aerosol samplig station for environmental radiation monitoring, STUK-A153 July 1998.

Pöllänen R, Ilander T, Lehtinen J, Leppänen A, Nikkinen M, Toivonen H, Ylätalo S, Smartt H, Garcia R, Martinez R, Glidewell D, Krantz K. Remote monitoring field trial. Application to automatic air sampling. Report on Task FIN-E935 of the Finnish Support Programme to IAEA Safeguards. STUK-YTO-TR 154, January 1999.

# APPENDIX 1 COST-BENEFIT ANALYSIS

*Data transfer from STUK to IAEA using phone lines and modems vs. client-to-site VPN.*

| DATA TRANSMISSION VIA VPN | | | | |
|---|---|---|---|---|
| **Operating Costs (Internet Access)** | | | | |
| STUK* | | | | $0.00 |
| IAEA (CompuServe Account)** | | | | $0.00 |
| **Total Operating Cost Per Month** | | | | **$0.00** |
| **Capital Equipment** | **Quantity** | **Cost** | | **Total** |
| Nokia VPN Hardware (Model 500) | 2 | $1,995.00 | | $3,990 |
| Ethernet Hubs | 2 | $171.75 | | $343.50 |
| Ethernet Card for PC | 1 | $200.00 | | $200.00 |
| Miscellaneous Cables | 10 | $3.95 | | $39.50 |
| VPN Client Software Licence | 1 | Inc. w/ HW | | $0.00 |
| CompuServe Software | 1 | Free | | $0.00 |
| ISDN Terminal Adapter | 1 | IAEA | | $0.00 |
| **Total Equipment Cost** | | | | **$4,573.00** |
| **Implementation Costs (Labor)** | **Days** | **Persons** | **Cost/Day** | **Total** |
| Network Information Gathering | 1.5 | 1 | $1,000.00 | $1,500.00 |
| VPN Installation Planning | 2 | 2 | $1,000.00 | $4,000.00 |
| Simulate in Lab (Sandia) | 2 | 2 | $1,000.00 | $4,000.00 |
| VPN Installation (Hardware – at STUK) | 1.5 | 1 | $1,000.00 | $1,500.00 |
| VPN Installation (Client/CompuServe at IAEA) | 1 | 1 | $1,000.00 | $1,000.00 |
| Training (Two Sandia employees) | 5 | 2 | $1,000.00 | $10,000.00 |
| **Total Labor** | | | | **$22,000.00** |
| **Total Capital Costs (Labor + Equipment)** | | | | **$26,573.00** |

| DATA TRANSMISSION VIA TELEPHONE | Low Data Amount | High Data Amount |
|---|---|---|
| Bytes/Day of Data | 250,000 | 25,000,000 |
| Lowest Modem Connection Data Rate (bps) | 33,000 | 33,000 |
| Time to Download/Day (in minutes) | 1.01 | 101.01 |
| Cost/Minute | $0.52 | $0.52 |
| Total Operator Charges $0.08 per 7 minutes | $0.01 | $1.15 |
| Cost Per Day to Download Data | $0.54 | $53.68 |
| **Monthly Operating Costs (30 days)** | **$16.10** | **$1,610.39** |

| | | |
|---|---|---|
| **Payback Period (in Months)** | **1,650.1** | **16.5** |
| **Return on Investment** | **–99.27%** | **–27.28%** |

* STUK already has Internet access and doesn't anticipate additional costs from VPNs.
**IAEA has a CompuServe account for the Safeguards Department and doesn't anticipate additional costs from VPNs.