# Global Information Assurance Certification Paper

**Securing remote users VPN access to your Company LAN**

Klavs Klavsen

July 29, 2001

Denmark

## Introduction

This paper is intended to be an introduction to the Security issues you face and the solutions you can choose between, when you want to give your remote users access to your Company Network via VPN. This topic is very broad, and has many aspects. This paper only focuses on the security aspects of the remote users pc, not including the security of different VPN-solutions, encryption techniques or other aspects related to the VPN-tunnel itself. It assumes a basic understanding of VPNs, IDS technology and common Industry terms and acronyms. See Virtual Private Network (VPN) Security by Gregory J. Ciolek, January 4, 2001 <http://www.sans.org/infosecFAQ/encryption/VPN_sec.htm> for more information on VPNs and IDS Terminology, part one A-H, by A. Cliff, July 19, 2001 <http://www.securityfocus.com/frames/?focus=ids&content=/focus/ids/articles/idsterms.html> and IDS Terminology, part two H-Z, by A. Cliff, July 19, 2001 <http://www.securityfocus.com/frames/?focus=ids&content=/focus/ids/articles/idsterms2.html> for more information on IDS technology.

## The VPN-tunnel is secure – what's the problem?

If you want to secure a building, you don't just put up a big fat metal door to protect your front entrance. you also ensure, that your windows are not easily penetrable, and you do not have a backdoor, that is easily kicked in. This also goes for your company network – the old saying ”The chain is only as strong as the weakest link” very much applies to network security.

It's not enough to ensure the front entrance to your network, you also have to ensure all other entrances to your network – such as the remote users pc, which often has the same access to your network, as their office pc – once the VPN-tunnel is open, and therefore is a very dangerous backdoor to your network.As company's networks gets more and more secure, by ways of enterprise firewalls, Intrusion Detection Systems etc., hackers turn to the remote users pc, and if you don't protect your backdoors – you are greatly at risk.

Unfortunately many people implementing VPN's for remote users, tend to focus on the security of the VPN-tunnel itself and often forget, that the VPN tunnel, is only half the job of implementing a secure remote user

VPN. The VPN-tunnel can only ensure the integrity and confidentiality of the data, while in transit from the pc to the company network and ensure reliable authentication of the user logging on. It can NOT protect the users pc against misuse by hackers:

- either by obtaining information from the harddrive, keyboard or any other part of the pc (eg.. the login for the users InternetBank or your network or, the local copy (even if only in Windows swap-file) of your business documents)
- or by using it as a staging point of an attack at the company network – through the VPN-tunnel.

This misuse by hackers, is made possible through program bugs or misconfigurations, viruses and/or trojans and different rogue programs like the gnutella file-share programs.. (why it can pose a security risk is shown in the article Gnutelle defeats many perimeter defenses by Meredith Lynes, June 19, 2000 <http://www.sans.org/infosecFAQ/firewall/gnutella.htm>). These programs can make it onto the home users computer (any computer, actually) through the means of two factors:

- Un-educated users of the pc

  (usually kids or a spouse that unintentionally opens an e-mail attachment or something else with a virus or trojan embedded in it or installs programs like the gnutella clients – because they have not been educated in what to do and not to do, in regards to these things)

- Program bugs/misconfigurations

  (an example could be, the bug in the Microsoft Outlook mail program – which enabled a buffer overflow attack, so that anyone who could craft an e-mail with a special mail-header – for example by using programs readily available on the internet - and sent it to this user, would make outlook crash and enable the person who crafted the e-mail to execute whatever he wanted on the pc – the unsuspecting user wouldn't even have to open the mail! See <http://www.securityfocus.com/frames/?content=/vdb/bottom.html%3Fsection%3Ddiscussion%26vid%3D1481> for details).

Both factors, are valid on all computers, and you really should consider the solutions I will describe later on, for your office computers also, even if you have Intrusion Detection systems, that monitor outgoing traffic also and regular port-scannings of your users pc's – just to add that extra layer of protection.

Remember, that no matter how good your products are, if your costumers/users find out that their personal information are at risk, because of your bad security – many will most likely find some other provider to fill their need – thus leaving you out of business.

**How to remedy the problem**

If you want to maximize your chances of avoiding unwanted intrusions, you need to ensure the integrity, confidentiality and reliability of all the links to your network and data – by protecting every computer it can reside on and the network in between. When talking about remote users, connected via VPN, you are protected against the network in between as long as the VPN-tunnel is safe. This leaves the computers on each end.

The company computers is not the focus of this article, so I will merely state that they also need to be properly protected.

The remote users pc, you need to ensure that it has and will not be, tampered with in any unwanted way. In short you need to ensure that the pc contains no viruses, trojans or any other programs – that you can not fully thrust (due to bugs or misconfigurations) and you need a way to protect it against infection from these.

First rule of thumb in security, is protection-in-depth. If you do not have at least 2 layers of protection, what happens if one layer fails open (eg. fails without closing down the avenue of attack)? – you have a potential backdoor into your network, as this computer is no longer protected against misuse by hackers – and still connected to the Internet.

With home users you can get at least one extra layer, by choosing the correct Internet Connection for the user. If the user is connected via a properly configured router – preferrably with NAT – you have a packet filter firewall which provides an extra layer of protection, that the Cable modems, ordinary modems and other devices without firewalling capabilities do not provide. This also means that your home users may not run any services accessible from the outside, such as a webserver on their home network, if it's accessible from their company pc at home – without going through the router as this would defeat the routers protection if the webserver is compromised.

With travelling users – connecting from many different places around the world, you can not ensure that there will be a firewall in front of the users pc, so instead of merely trusting a personal firewall, you should consider getting an extra layer of protection by using a VPN-client , that can route all traffic – including http-trafic – through the VPN-tunnel, and hereby in effect, putting the user behind your company firewall. This way, you can add an extra layer of protection to the users pc, by means of your company security systems. Be aware of drawbacks, such as slower internet surfing for the user and a greater load on your internet connection and encryption Hardware/Software.

Securing the remote users pc, is a complex issue. First you need to choose between two main strategies.

1. Making the employee sign some legalese saying that he will not install none-work related software, and he will adhere to the company policy in regards to use of computers (if you have one) and so on – to ensure that the pc will not be subjected to any actions that the office pc wouldn't. And then setting up the remote users pc, as if it were an office pc without it's own protective measures, beyond anti-virus software. This strategy relies on the home user not breaking the agreement, and aims to make the pc just as secure (or insecure) as the office pc. As I've stated earlier, this is not a strategy I would recommend – because of several factors which makes it a worse security risk, than the office pc (see prior section “The VPN tunnel is secure – what's the problem”). I would choose the 2. strategy, and implement it on the office pc's also.

2. Realising that you can not trust the security of the OS or any programs installed on the pc and therefore installing software such as personal firewalls and other Intrusion Detection Software to prevent or at least detect when the pc has been compromised. To quote a security principle, that is emphasized on during SANS training ”Prevention is ideal, but detection is a must”.

If you choose the 2. strategy, just keep reading and I will tell you what features in the solution you should be looking fore.

To be as secure as possible you need software, that incorporates and combines features from several Intrusion Detection Areas – preferrably into one software package, to more easily ensure that all your security measures are in place at all times and to increase manageability.

**Personal Firewall**

You need the firewalling feature, to ensure that no services (open ports) on the pc, are accessible from the network, from unallowed hosts. For instance only your own remote-clients should be able to connect to any services installed on the remote users pc, and it is not sufficient that the program service ensures this only by user/password measures – because what if there is found a program bug, in that particular code, or what if someone succeeds in a brute force attack (user/password guessing).

**Network-based IDS**

The Network-based IDS features you need are, recognition and identification of the signature of network attack patterns. This helps the IT staff identify the severity of the incident, so they don't get alarmed by

some unwilling ”scanning” by some user with no bad intentions – but still recognizes serious hacking attempts. Another essential part of Network-based IDS's you need, are the logging of all incidents to a central server. This ensures that your IT staff gets wind of any incidents on the remote users pc, so that a hacker who penetrates your defences and compromises the pc – can't just delete the logs and ”trojan” your security measures, so you think everything is alright.

**Host-based IDS**

The Host-based IDS features you need, are it's capability to ensure that programs allowed a network connection has been uniquely identified in a 100% secure manner, so only approved programs - that has NOT been altered (eg. Trojaned/virus infected), are allowed. The program must verify the hash of the program as a part of the identification process. You should know that many programs out there, claims to do this, but in fact only checks the port it accesses, and the name of the executable file. See Personal Firewalls: not enough, by Vincent Wallace, February 12, 2001 <http://www.sans.org/infosecFAQ/firewall/not_enough.htm>.

**Anti-Virus**

You need an Anti-Virus program to protect the pc against virus attacks, including scanning of email-attachments. If you have a server-side virus-scanning (such as an email-scanner) also, you should use a different brand of virus-scanner for the client pc. This increases the layers of protection, because different brands of virus scanners, actually do catch different viruses/trojans.

**Manageable security**

All this may sound as if you would need to double your IT-staff to keep remote users pc's safe. This does not have to be the case, if you make sure to find programs that assists your IT-staff greatly in the daily work. To decrease your TCO (Total Cost of Ownership) and make the solution more scaleable, in terms of manpower needed to manage it, you need the following features:

- The security configuration has to be protected 100% against tampering from the user, as it is impossible to ensure the security of a home users pc, if you can not be certain it keeps the

configuration you give it.

- It must enable your IT-staff, to ensure the anti-virus definitions, IDS signatures etc. are kept up to date – by enabling them to manage it from the company network.
- It must have the ability to disconnect the VPN-tunnel – and preferrably disconnect the network entirely, if any incidents occur.
- It must as a minimum, ensure that all the relevant security software are running and correctly configured, while the VPN-tunnel is open. Optimally, it should protect the pc at all times, so the user can thrust his pc at all times, and to avoid locally accessible company documents and the likes, from exposure while the VPN-tunnel is closed.
- It should be remotely configurable, by your IT-staff. Centralized management is much more effective when dealing with remote users pc's (otherwise they would have to bring the pc to the office for each needed change – and if the need arises for a quick configuration change, while the user and his pc is away on travel, you have a problem).

**Finding the right programs**

When finding programs that implements these features, be sure to not just trust the product sales pitch – as they are often a very glamour like view of the product, that might not hold water in real life. Verify the stated features, by reviewing different product reviews made by un-biased professionals – and if possible, ask the reseller of the product to put you in contact with other users of the product, so you can talk to their IT-staff, and get their experiences with the program, and confirm that it works as needed.

Most commonly you can find one program that is a hybrid of all these IDS types, and implements exactly what you need. If you can't or perhaps prefer a seperate Anti-Virus program, make sure you are able to ensure that they are all running at all times.

You can find many vendors, products and reviews by searching the Internet with www.google.com (the swizz knife of the Internet) and www.metacrawler.com. Try searching for ”personal firewall review” or if you have a specific product in mind search for ”productname review”. That's guaranteed to give you some relevant hits. I've given the links to a selected few at the bottom of this article.

**Conclusion**

As you should have realised by now, a remote pc is not just another company pc – mainly due to the fact,

that it is not protected by enterprise firewalls and IDS's. It needs some special attention in securing it, but then it can be almost as safe as your office pc's, and once you have setup a security system with the features I've described for you, it can easily be rolled out and maintained on all your remote users's pc's.

**References**


Intrusion Detection, Theory and Practice by David "del" Elson, 27. march, 2000 <http://www.securityfocus.com/focus/ids/articles/davidelson.html>

Personal Firewalls: not enough, by Vincent Wallace, February 12, 2001 <http://www.sans.org/infosecFAQ/firewall/not_enough.htm>

IDS Terminology, part one A-H, by A. Cliff, July 19, 2001 <http://www.securityfocus.com/frames/?focus=ids&content=/focus/ids/articles/idsterms.html>

IDS Terminology, part two H-Z, by A. Cliff, July 19, 2001 <http://www.securityfocus.com/frames/?focus=ids&content=/focus/ids/articles/idsterms2.html>

Protecting your corporate laptops, while they are on the road, by Darrel Keller, May 2001 <http://www.sans.org/infosecFAQ/firewall/corp_laptops.htm>

Personal Firewalls: What are they, how do they work? By Tina Zych, August 2000 <http://www.sans.org/infosecFAQ/homeoffice/personal_fw.htm>


**Links to a few Products, reviews and vendors of personal firewalls.**

Notice! This list is in no way conclusive.

CyberArmour from www.infoexpress.com

Information Security <http://www.infosecuritymag.com/articles/march01/departments_products2.shtml>

Internet Week

Product Review <http://www.internetweek.com/reviews00/rev110600-4.htm>

Summary <http://www.internetweek.com/reviews00/rev110600-5.htm>

Personal Firewall from www.tinysoftware.com

Internet Week

Product description <http://www.internetweek.com/reviews01/rev051401-2.htm>

Product summary <http://www.internetweek.com/reviews01/rev051401-3.htm>

Zone Alarm Pro from www.zonelabs.com

links to reviews

Product reviews<http://www.zonelabs.com/pressroom/news/10.html>

Checkpoint Systems www.checkpoint.com , has a VPN client with built-in personal firewall and IDS features.

Find the rest with Google.

Last Updated: May 28th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANS Stockholm 2017 | Stockholm, Sweden | May 29, 2017 - Jun 03, 2017 | Live Event |
| SANS San Francisco Summer 2017 | San Francisco, CA | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| Security Operations Center Summit & Training | Washington, DC | Jun 05, 2017 - Jun 12, 2017 | Live Event |
| SANS Houston 2017 | Houston, TX | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| Community SANS Ottawa SEC401 | Ottawa, ON | Jun 05, 2017 - Jun 10, 2017 | Community SANS |
| SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | vLive |
| SANS Secure Europe 2017 | Amsterdam, Netherlands | Jun 12, 2017 - Jun 20, 2017 | Live Event |
| Community SANS Portland SEC401 | Portland, OR | Jun 12, 2017 - Jun 17, 2017 | Community SANS |
| SANS Rocky Mountain 2017 | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Charlotte 2017 | Charlotte, NC | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Minneapolis 2017 | Minneapolis, MN | Jun 19, 2017 - Jun 24, 2017 | Live Event |
| SANS Columbia, MD 2017 | Columbia, MD | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Cyber Defence Canberra 2017 | Canberra, Australia | Jun 26, 2017 - Jul 08, 2017 | Live Event |
| SANS Paris 2017 | Paris, France | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS London July 2017 | London, United Kingdom | Jul 03, 2017 - Jul 08, 2017 | Live Event |
| Cyber Defence Japan 2017 | Tokyo, Japan | Jul 05, 2017 - Jul 15, 2017 | Live Event |
| SANS Cyber Defence Singapore 2017 | Singapore, Singapore | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Minneapolis SEC401 | Minneapolis, MN | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Los Angeles - Long Beach 2017 | Long Beach, CA | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Phoenix SEC401 | Phoenix, AZ | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Munich Summer 2017 | Munich, Germany | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Mentor Session - SEC401 | Macon, GA | Jul 12, 2017 - Aug 23, 2017 | Mentor |
| Mentor Session - SEC401 | Ventura, CA | Jul 12, 2017 - Sep 13, 2017 | Mentor |
| Community SANS Atlanta SEC401 | Atlanta, GA | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| Community SANS Colorado Springs SEC401 | Colorado Springs, CO | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| SANSFIRE 2017 | Washington, DC | Jul 22, 2017 - Jul 29, 2017 | Live Event |
| SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style | Washington, DC | Jul 24, 2017 - Jul 29, 2017 | vLive |
| Community SANS Charleston SEC401 | Charleston, SC | Jul 24, 2017 - Jul 29, 2017 | Community SANS |
| Community SANS Fort Lauderdale SEC401 | Fort Lauderdale, FL | Jul 31, 2017 - Aug 05, 2017 | Community SANS |
| SANS San Antonio 2017 | San Antonio, TX | Aug 06, 2017 - Aug 11, 2017 | Live Event |
| SANS Prague 2017 | Prague, Czech Republic | Aug 07, 2017 - Aug 12, 2017 | Live Event |