

Virtual Private Problems: The Broken Dream

A Comprehensive Guide to Circumventing Virtual Private Networks

Loki
Founder/Chief Research Scientist
Fate Research Labs
www.fatelabs.com
loki@fatelabs.com

Table of Contents

PREFACE	3
<i>Introduction</i>	3
THE FIRST GENERATION VPN	4
<i>In The Beginning</i>	4
INTRODUCTION TO VPNS	5
<i>Understanding a VPN</i>	5
FALSE HOPES	6
<i>The Great Lie</i>	6
IP 101, A BACKGROUND ON IP AND IPSEC	6
FALSE HOPES	7
VPN ENCRYPTION	8
<i>IPSec 101</i>	8
<i>The Encapsulating Security Payload (ESP)</i>	8
<i>The Attack</i>	8
VPN ENCRYPTION	9
CLOSING THOUGHTS	11
<i>Words From The Author</i>	11
APPENDIX	12

Introduction

As the mention of an acquisition sends arms raising for the air at a local Milpitas, based VPN vendor, the individual financial concerns and debts of the company are immediately lifted off the shoulders of its CEO, Board of Directors, and sales force world-wide. The company manufactures VPN appliances often spattering widely used marketing clichés such as “Industry Leading”, “IPSec compliant”, and “true interoperability with other devices.”

In a now much more grown-up world, matured far from the days of the first VPN, we now question whether the use of “IPSec Compliant” really holds any more weight. Where bastardized implementations of the IPSec protocol span vendor to vendor, where cumbersome heterogeneous networks are most often found than not, and many unsuccessful installations of time spent in vain to get two separate vendors to work harmoniously across the cloud, we find that long gone are the past and distant dreams of true vendor interoperability surrounded by scalable VPN products.

A new VPN solution must arise. The architecture on which VPN solutions have been built must be re-architected. New blueprints must now replace the old chicken scratch that the original idea once was.

This technical whitepaper shall serve as the guide to a much more intelligent suite of VPN products, the call for a new generation of redesigned VPNs that have learned from the misconfigurations and poor design flaws of its predecessor. Until that day arrives, this series of papers plans to prove the dire requisition for human intervention in this virtual private web of lies and misleading marketing campaigns.

The First Generation VPN

In The Beginning

In August of 1995 RFC 1825 was introduced that made way for a brand new, hybrid version of IPv4, a soon-to-be standard in IP Security as well as the building blocks for VPN technology to come; the IPSec protocol suite. This would be the technology on which Virtual Private Networks were built.

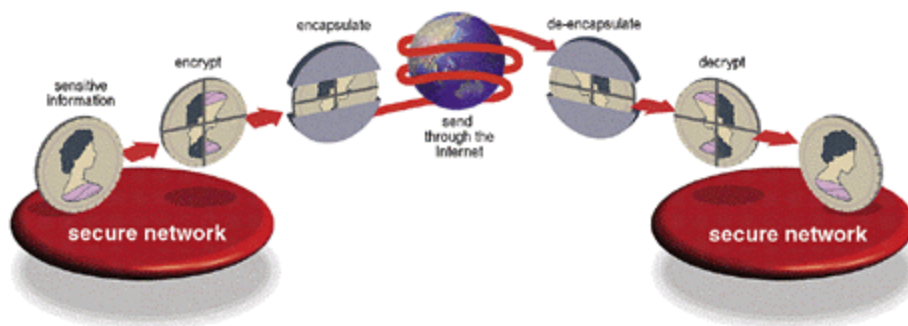
Once upon a time long distance bills were through the roof for remote dial-in users, modem pools were growing more and more tangled, and Remote Access Servers pretty much translated to “nightmare” in any language you spoke. It was the dawning of a new era in secure remote access. The question of how to transmit information via publicly shared network infrastructures was on the minds of every company on a global scale. The answer would soon change the way we do business today.

The answer was found in Virtual Private Networks. In the past few years alone, we have been charged with identifying a means to conduct business securely across publicly shared network infrastructures. Virtual Private Networks were our answer in establishing secure links with business partners and extend communications to regional and isolated offices, which significantly decreased the cost of communications for an increasingly mobile workforce.

The need for suppliers of this technology would soon spark the onslaught of a barrage of VPN vendors who claimed 100% IPSec compliance, 100% interoperability with other VPN vendors, and the “oh-so tickle my fancy statement” the “HACK PROOF VPN!”

The VPN products on the market today have implemented strong crypto solutions within their products. What should be pointed out is that this paper in no way is an attack on cryptography itself, as my belief has always been that the strength of the cryptography algorithms has never been a question, rather the implementation and architecture of the product.

Below is an example of an ideal VPN configuration. Notice the 2 “secure networks” on opposite sides of the Internet.



Understanding a VPN

The most frequent question posed is “what exactly defines a VPN?” What is it? The working definition of a VPN is the following: a combination of tunneling, encryption, authentication, and access control technologies, and services used to carry traffic over the Internet, a managed IP network, or a provider's backbone.

Basically, what this boils down to is nothing more than a means to extend a Local Area Network (LAN) within a corporation to an outside remote site or traveling employee. The VPN is an encrypted solution to secure remote access. The great and magical dream of extending your corporate network to anywhere in the world has evolved into a frightening reality.

There are many types of VPN implementations, each with its specific set of technology requirements. However, VPN deployments can be grouped into three categories:

1. Intranet VPN's
2. Remote Access VPN's
3. Extranet VPN's

The Intranet VPN is most often used to facilitate communications within a company's information structure and separate departments. Interlinking different offices in different cities or different buildings. The most important of the technologies requirements are strong data encryption to protect the information being transferred along the network. Other important factors of the Intranet VPN are to prioritize the crucial applications on the network such as, sales and customer database management, and document exchange. Scalable management of the VPN is also very important to ensure that the number of users applications and offices are easily accommodated.

Remote Access VPN's are usually used to link the remote network to mobile users. The users can connect to the VPN through any ISP if they have the proper access and technology. The most important thing to consider in a remote access VPN is to ensure strong authentication is applied to verify remote and mobile users identities in the most accurate and efficient manner possible. These VPN's can benefit companies with employees that travel on a regular basis.

The Extranet VPN implements multiple technologies to create a larger scale VPN with more flexibility and options to the users. It uses the Internet as the large backbone. For example you could have an extranet VPN that allows several branch offices, suppliers, and customers access to the VPN. The most used and accepted standard to the Internet based VPN is the Internet Security Protocol (IPSec).

False Hopes

The Great Lie

While the technologies are powerful, they are not foolproof. VPNs can be extremely difficult to configure properly, and even a small error can create a serious hole in a firewall. Even when configured properly, many of the protocols used in implementing VPNs have varying degrees of security problems and inherent implementation issues.

Case in point, in August of 2000, Fate Research Labs released its first VPN advisory, which targeted a local Sunnyvale VPN vendor called RapidStream. The problem outlined in this advisory focused on the company's implementation of SSH access for encrypted remote management. However, in a failed attempt to do so, it was discovered that RapidStream hard-coded the root account into the SSHD binary itself with a null passwd. Most likely, unaware of the ability to append command execution to the end of an ssh(exec) string in *nix, a string of `ssh -l rsadmin <ip of vpn> '/bin/sh -i'` would coincidentally spawn a root shell on the remote VPN's underlying OS.

What we have been faced with in the VPN industry is an influx of vendors attempting to convolute products with functionality that does not belong in a security device. Vendors that have added functionality such as archaic versions of Sendmail to turn your VPN into a combination VPN and Mail Server is one of many problems discovered in the past years since the first VPN came to market.

IP 101, A Background on IP and IPSec

The IPSec protocol suite provides answers to the inherent security flaws found in the design of the Internet Protocol (IP). The original design of IP raises the concern of three important questions. (1) Is the person we are communicating with really that person? (2) Is someone listening in on our "conversation" or session? (3) That the data sent between both parties is not altered in any way during transit. These (3) three questions are referred to as none other than (1) Authentication, (2) Confidentiality, and (3) Integrity. The architecture of the modern Internet Protocol makes all three of these concerns difficult to meet.

In order to understand IPSec, IP, and the many other protocols used to power the Internet, one must understand how the data is constructed and sent across a network. Below is a rudimentary diagram of a TCP/IP packet broken down into chunks. As a packet passes down the OSI model, individual layers append their own header to the packet for delivery. Each packet contains three vital pieces of information: (1) Data, (2) The IP address of the source, and (3) The IP address of the destination.



False Hopes

The inherent problems in this packet structure are several-fold. The Source IP address can be easily changed or crafted to be from a completely different machine than the one sending it, otherwise known as **spoofing**. Spoofing makes possible another serious type of attack called **Session Hijacking**, in which an attacker poses as a target system, sending an RST packet to the destination host, thereby ending the communication stream between the original two hosts. This allows the attacker to jump in on the session, masquerading as the destination machine.

Another type of attack that is vulnerable to Ethernet IP-based networks is sniffing. In most Ethernet LANs, packets are scattered across the network to every Ethernet node. Conventionally, each node's network card only listens and responds to packets specifically destined for its IP or MAC address. This is what gives a system the capability of sniffing out packets or communication between systems on a network.

The most obvious and apparent answers to the security flaws found on Ethernet IP networks is encryption technologies able to conceal and authenticate the data passed in IP packets.

IPSec 101

This is where IPSec has created its niche. IPSec employs a powerful suite of encryption technologies that make it possible to combat the numerous threats in traditional IP-based networks.

1. **Authentication Header (AH):** AH ties data in each packet to a verifiable signature that allows you to verify the sending party as well as the ability to ensure the data has not been altered during transit.
2. **Encapsulating Security Payload (ESP):** Using powerful encryption, ESP scrambles up the data or more properly referred to as the *payload* of the packet into unreadable chicken scratch that only the receiving party has the key to read. The encapsulation also conceals sensitive IP addresses of the sending and receiving party.
3. **Internet Key Exchange (IKE):** This is the protocol used in the negotiation between the two communicating hosts on what type of encryption algorithms to use, as well as the keys to use, and how long the keys will be valid before changing them. IKE also handles the responsibility required for the exchange of keys used to initiate and maintain the connection between the two hosts.

The Encapsulating Security Payload (ESP)

An IPSec packet is constructed in the following manner. ESP employs several technologies that allow sensitive IP information and the actual payload or data of the packet to be encrypted. Below is a diagram of how this compares to the traditional TCP/IP packet mentioned previously.



The Attack

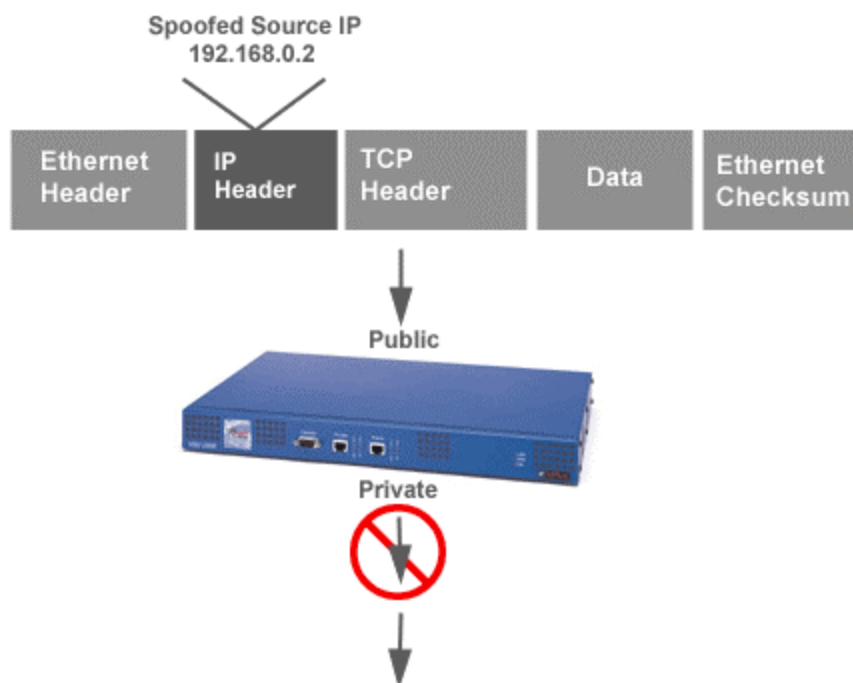
With respect to the aforementioned encryption implementations, the idea of attacking the actual encrypted session itself would be, for lack of a better word, insanity. Not to mention that the idea of cracking a (3) Triple DES Encryption stream would be a feat far from reality, at least with current technologies.

So, a new and different approach must be made to circumventing such a powerful encryption device. Instead of targeting the encryption itself, the fallen foe will have to be the improper implementation of such a technology from vendor to vendor. This paper is far from an attack on IPSec itself, moreover, it is in actuality an attack on the way each and every Vendor has architected their version of this great dream. With no standards set in place or blueprints to refer to, each vendor is faced with their own interpretation and ideology of what a VPN appliance should be. In the experience of Fate Labs, this has been nothing but a history of failed attempts.

In a second Fate Labs advisory targeting VPNet Technologies, now Avaya Corporation, particular problems were found in (2) two underlying areas of all VSU's in the company's line of VPN products. The first problem identified was an unknown flaw relating to how the VPN device handled packets. Due to a lack of

VPN Encryption

communication with the vendor (threats of lawsuits and being ignored by the company), a conclusion to what caused this problem was not reached. I had made an assumption that it was a problem somewhere in the NATing functions or bridging code of the VSU. This can be easily explained in the following diagram below using our original diagram of an IP packet.



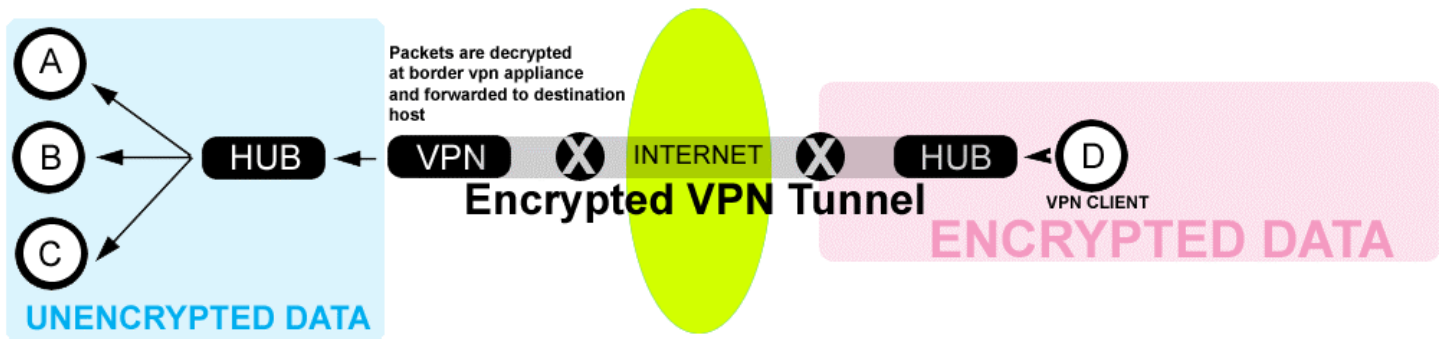
By modifying the source IP address to match the internal network of the VPN, it passes it over allowing us to initiate sessions with systems on the protected LAN.

The problem here is as one can see, not IPSec or the underlying protocols used by VPN's. It's the way, we as humans have integrated them all together into what we are marketing as a "complete solution". As budgets for security solutions within companies grow smaller and smaller, as the false sense of security is created by the purchase of a single firewall or even VPN, the loss caused by a single compromise heightens to unquantifiable amounts. Many Fortune 50 corporations have been discovered to be deploying VPN solutions without a firewall in order to cut deployment costs or even because of a lack of understanding and knowledge.

Several networks have been compromised in legitimate penetration tests that used a VPN as a "ride-free" ticket into the local protected LAN. During a recent study, Fate Research Labs conducted a global penetration test on networks containing different VPN vendor appliances. Several Fortune 5 Corporations that have asked to not be identified in this paper used a VPN vendor that stored the password of its Client software configuration in plain readable text.

A serious issue that has been brought to light by Loki and Fate Research Labs is the concerns regarding the implementation of VPN technology in general. Here we will diagram the flaws in VPN architecture that has undoubtedly been overlooked by several people we highlighted this to.

Where so much emphasis and encryption was placed into the tunnel created by a VPN in either a site to site or client configuration across the cloud, you have what I believe to be a serious oversight on the way the VPN was architected. I have provided a diagram below outlining the problem. Where over 95% of the compromises reported last year were caused by internal threats, such an expensive security solution should have been more meticulously designed.



Closing Thoughts

Words From The Author

It should be concluded that I am a very large advocate of the progression of Virtual Private Network technology. Many after hearing such a statement have asked me why I've chosen to brave such an evangelistic role in attacking VPN technology. The only thing I have to say regarding that question is that I am also dedicated to my convictions and belief in complete full disclosure.

I dream of a time when vendors will embrace open disclosure in a way to improve upon the technology and security of their product line. Instead of making enemies with lists such as Bugtraq, Fate Labs, and the many other groups active in releasing advisories on discovered vulnerabilities, Corporate America should utilize such resources and technical prowess in a way to fix such problems instead of associating us as being a part of them.

VPN Technology is indeed at a virgin and untested state. This should be taken into consideration in the deployment of any VPN solution, whether it's a VPNet VPN or even Checkpoint. Such VPN technologies can be implemented and aforementioned vulnerabilities prevented through conducting comprehensive and regular assessments of your VPN device and setup.

The advisories discovered and released by Fate Labs are not incredibly minute and convoluted discoveries. They are simple and logical issues that should not be allowed to cross a VPN. Things such as source routed packets, spoofed packets, or Unix daemons such as SSHD and Sendmail running on a device handling cryptographic sessions.

Loki
Founder, Chief Research Scientist
Fate Research Labs
<http://www.fatelabs.com>

Appendix

Fate Research Labs

<http://www.fatelabs.com>

VPN Consortium

<http://www.vpnc.org>

VPNet Technologies/Avaya Corporation

<http://www.avaya.com>