ADOT Uses for Virtual Private Networking Technology: Phase 1 – Pre-Pilot Test Report

Final Report 502(1)

Prepared by:
Mark Merkow, CCP
1216 East Commodore
Tempe, Arizona 85283

February 2001

Prepared for:
Arizona Department of Transportation
206 South 17th Avenue, MD 075R
Phoenix, Arizona 85007
in cooperation with
U.S. Department of Transportation
Federal Highway Administration

METRIC (SI*) CONVERSION FACTORS

APPROXIMATE CONVERSIONS TO SI UNITS

Symbol	When You Know	Multiply By	To Find	Symbol
	LENGTH			
in	inches	2.54	centimeters	cm
ft	feet	0.3048	meters	m
yd	yards	0.914	meters	m
mi	miles	1.61	kilometers	km
	AREA			
in^2	square inches	6.452	centimeters squared	cm^2
ft^2	square feet	0.0929	meters squared	m^2
yd^2	square yards	0.836	meters squared	m^2
mi^2	square miles	2.59	kilometers squared	km^2
ac	acres	0.395	hectares	ha
	MASS (weight)			
oz	ounces	28.35	grams	g
lb	pounds	0.454	kilograms	kg
T	short tons (2000 lb)	0.907	megagrams	Mg
	VOLUME			
fl oz	fluid ounces	29.57	milliliters	mL
gal	gallons	3.785	liters	L
ft^3	cubic feet	0.0328	meters cubed	m^3
yd^3	cubic yards	0.765	meters cubed	m^3

Note: Volumes greater than 1000 L shall be shown in m^3.

	TEMPERATURE (exact)			
°F	Fahrenheit temperature	5/9 (after subtracting 32)	Celsius temperature	°C

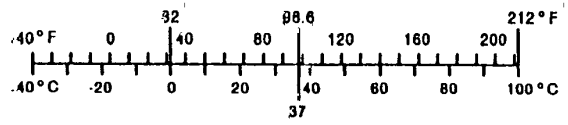
APPROXIMATE CONVERSIONS TO SI UNITS

Symbol	When You Know	Multiply By	To Find	Symbol
	LENGTH			
mm	millimeters	0.039	inches	in
m	meters	3.28	feet	ft
yd	meters	1.09	yards	yd
km	kilometers	0.621	miles	mi
	AREA			
mm^2	millimeters squared	0.0016	square inches	in^2
m^2	meters squared	10.764	square feet	ft^2
yd^2	kilometers squared	0.39	square miles	mi^2
ha	hectares (10,000 m^2)	2.53	acres	ac
	MASS (weight)			
g	grams	0.0353	ounces	oz
kg	kilograms	2.205	pounds	lb
Mg	megagrams (1000 kg)	1.103	short tons	T
	VOLUME			
mL	milliliters	0.034	fluid ounces	fl oz
L	liters	0.264	gallons	gal
m^3	meters cubed	35.315	cubic feet	ft^3
m^3	meters cubed	1.308	cubic yards	yd^3

	TEMPERATURE (exact)			
°C	Celsius temperature	9/5 (then add 32)	Fahrenheit temperature	°F

These factors conform to the requirement of FHWA Order 5190.1A

*SI is the symbol for the International System of Measurements



Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-AZ-01-502(1)		

4. Title and Subtitle	5. Report Date
ADOT Uses for Virtual Private Networking Technology: Phase 1 – Pre-Pilot Test Report	February 2001
	6. Performing Organization Code

7. Authors	8. Performing Organization Report No.
Mark Merkow, CCP	

9. Performing Organization Name and Address	10. Work Unit No.
Merkow Consulting 1216 East Commodore Tempe, Arizona 85283	11. Contract or Grant No. SPR-PL-1-(57) 502

12. Sponsoring Agency Name and Address	13.Type of Report & Period Covered
ARIZONA DEPARTMENT OF TRANSPORTATION **206 S. 17TH AVENUE** **PHOENIX, ARIZONA 85007** Project Manager: John Semmens	14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

This phase of the project includes the feasibility study for the use of Virtual Private Network technology by ADOT, and especially by the Motor Vehicles Division (MVD) of ADOT. Following the feasibility study period, preliminary analysis was conducted to determine potential users of VPNs for access to MVD records in cases where no other connectivity is possible or the costs of such connectivity are prohibitive.

A final report will be issued to embody the results of preliminary testing by third-parties and external government agencies to help assess the viability of the technology as a general-purpose utility for MVD records access.

17. Key Words	18. Distribution Statement	23. Registrant's Seal
Virtual Private Networks, Public Key Infrastructure(PKI),	Document is available to the U.S. public through the National Technical Information Service, Springfield, Virginia 22161	

19. Security Classification	20. Security Classification	21. No. of Pages	22. Price
Unclassified	Unclassified	60	

TABLE OF CONTENTS

List of Tables

List of Figures

EXECUTIVE SUMMARY

This project was initiated to assess the possibility of using modern Virtual Private Networking technology as an additional means for access into ADOT user-based services for records retrieval and management. Two phases of the project were defined early in the planning stage.

Phase 1 began on April 5, 2000 with a kick-off meeting at ADOT facilities to assess internal current projects related to VPNs and to combine efforts. Several follow-on meetings were held throughout the Summer of 2000, and have led to a concrete plan for rolling-out VPN technology across a variety of third-party private and government users.

Phase 2 will conclude after sufficient testing time has elapsed and sufficient data is collected for meaningful analysis. Once this analysis is complete, a final report will be published containing the test results and recommendations for the future.

This project is unlike many of the other ADOT-initiated research projects in that the technology being researched is primarily for external users and not ADOT employees themselves. VPNs, as a potential option for connectivity into the ADOT WAN, benefit outside users through (potentially) reduced network charges or new connectivity that's not possible through traditional network links.

Field interviews and observations will offer the insights needed to help determine if VPNs are a viable option to offer organizations wishing to access ADOT systems and resources.

1.Introduction and Objectives

1.1. Objectives of the Study

The goal of this study is to determine the effectiveness, security, and potential cost reductions that are traditionally shown through the use of Virtual Private Networking technology and services.

ADOT network security polices prohibit direct connections with outside constituents unless a VPN is used. The ADOT network did not provide the sufficient level of firewall security desired but ADOT network administrators and managers began to explore some options using the technology with internal trials and vendor-supplied trial equipment. Discussions ensued about the varied landscape of VPNs and ADOT's readiness to adopt leading-edge systems in light of a technology that re-invents itself on a near daily basis.

Through the collection of sufficient data across multiple types of MVD third-party customers, this study will help to fill in the gaps due to a lack of experience with the technology and help to assess its viability for long-term uses.

2. Virtual Private Networks Technology Basics

2.1 Introduction

In the pre-Internet days of computing, costly leased communication lines from the telcos (telephone companies) or dial-up modem-to-modem connections over analog telephone lines were the only viable options available to those who wanted to communicate with others in the outside world.

- Often, these communication links could only carry the traffic for a single network protocol (such as IBM's SNA and TTY traffic), necessitating additional lines for each new protocol.
- These links were point-to-point. A dedicated connection could only be used from Point A to Point B. If Point A needed to communicate with Point C, another line was mandatory. As complexity increased, networks grew among multiple external companies and expenses began to soar. Beside inter-company communications, businesses created branch offices, remote factories, and far-flung sales sites. These isolated facilities had their own communication needs
- Wide Area Network (WAN) development and support required additional dedicated links or satellite communications to attain the high availability that's required.
- As organizations began to encourage remote employee access to internal networks (LANs), huge banks of modems became prevalent -- requiring additional capital investments and support costs that were already becoming unmanageable.

Over time, the symptoms that companies experienced with difficult-to-manage networked connections began to include never-before-witnessed problems, such as

- Unreasonably long lead times to install and test new communication links
- Finger pointing among users, telcos, and equipment providers as communication problems arose
- Skyrocketing support and management costs
- Increased complexity in all aspects of hardware, software, and dependence on multiple service providers
- Difficulties in scaling up as needs dictated

2.2 The Evolution of VPN Technologies

Once the Internet was deemed a viable alternative to dedicated and dial-up computer links, organizations began to hop on the bandwagon, hoping to drive down the costs of operation. Without effective security and reliability in place, however, any hopes of migrating to the Internet were quickly dashed. To serve these aspiring business users, new technologies entered the scene.

2.2.1. Early VPN protocols

To answer some of the security requirements that became mandatory as Internet demand increased, certain vendors of networking systems responded with proprietary solutions to tunnel private traffic over the public network. Some of these earlier solutions included

- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Forwarding (L2F)
- Layer 2 Tunneling Protocol (L2TP; combining PPTP and L2F)
- SOCKS protocol

2.2.1.1 PPTP

PPTP is a tunneling protocol that supports other protocols by encrypting their traffic before submitting them to the Internet for transport. PPTP is intended for use over dial-up connections to the Internet.

- LAN protocols such as Novell's IPX and Microsoft's NetBEUI are encapsulated (wrapped-up) using PPTP and unwrapped on the receiving end before being routed to their destination.
- PPTP is built into Microsoft Windows NT and Windows 2000; client software for PPTP is available as a free add-on for Windows 95 users and is included with Windows 98 and Windows 2000.
- PPTP has received industry criticism that it lacks scalability and was found to contain several flaws in earlier implementations, making it vulnerable to attacks.

2.2.1.2 L2F

L2F's essential technical difference from PPTP is L2F's ability to use protocols at Layer 2 of the TCP/IP network protocol stack (described later), for tunneling purposes, including

- Asynchronous Transfer Mode (ATM)
- Frame Relay

2.2.1.3 L2TP

Combining the best features of PPTP and L2F, Layer 2 Tunneling Protocol (L2TP) merges the two as an evolutionary protocol that's supported by commonly used network routing devices.

2.2.1.4 SOCKS

SOCKS is an authenticated firewall traversal protocol. It is designed to permit traffic to pass through only after the user who sent it has been authenticated to the system. SOCKS doesn't rely upon any specific characteristics of an IP packet to decide whether access is permitted.
Some of SOCKS' greatest advantages are

- Support for both UNIX and NT systems
- Application-specific tunnels for programs that are tied to specific TCP/IP server ports

SOCKS is an Internet Engineering Task Force (IETF) standard described in RFC1928, RFC1929, and RFC1961. SOCKS Version 5 includes support for negotiating encryption uses between communicating parties.

2.2.1.5 IP Security (IPSec)

Today's modern VPN solutions are increasingly relying on IP Security (IPSec), IPSec was developed by the IETF as RFC1825-9, based on the work conducted in the Automotive Network eXchange (ANX) project from the Big 3 automakers. IPSec is designed to:

- Perform both encryption and authentication to address the inherent lack of security on IP-based networks.
- Support the security goals of:
  - Sender authentication
  - Message integrity
  - Data confidentiality

Figure 2.1 below shows how VPN protocols are related to the TCP/IP protocol stack.

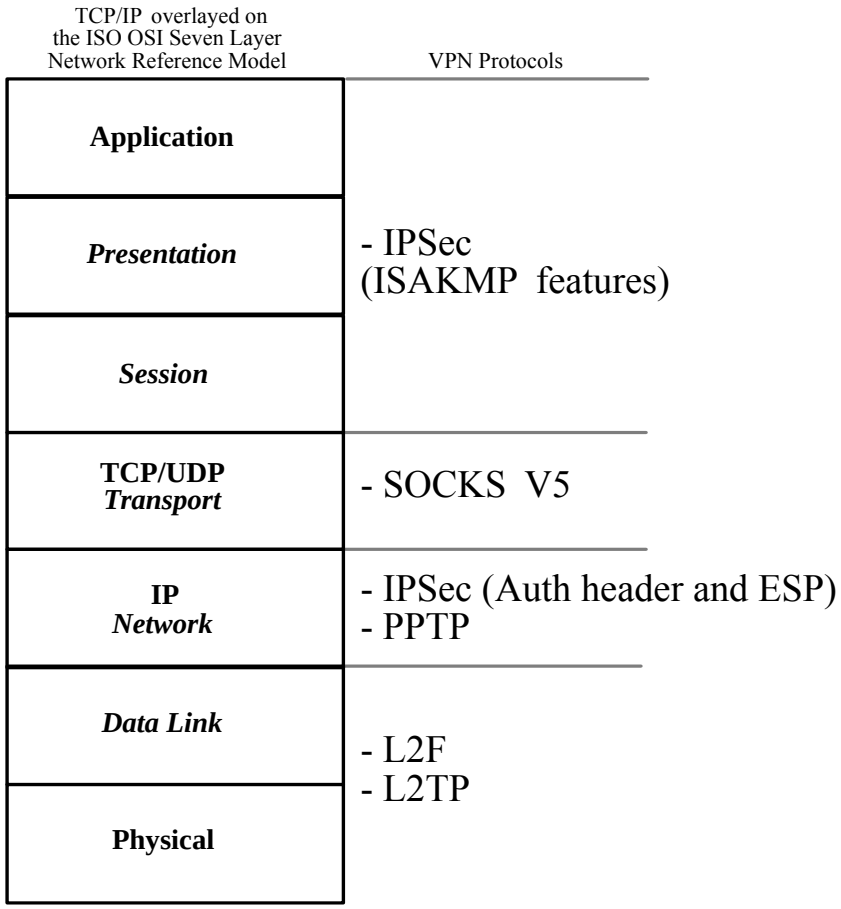


Figure 2-1: VPN protocols mapped onto TCP/IP

2.3 Components Needed With VPNs

Because of system requirements to assure high levels of security, VPNs are naturally complicated. To help assemble a VPN it's helpful to know what the VPN puzzle looks like. Typical components that you'll find needed for an effective VPN include

- Gateway devices (routers, dedicated servers, and firewalls)
- Client software
- Hardware-based encryption accelerators
- Load balancing, fail-over, and redundant critical servers
- Network transport communication mechanisms

2.3 Typical VPN Configurations

VPNs have found their way into three primary classes of use:

- Remote access computing to eliminate dial-up modem banks and long distance toll calls by remote employees needing to access back office resources (e-mail, user directories, specialized application software, etc.)
- Branch office networks to eliminate the costs associated with dedicated leased-lines and to build new branch office connections ad-hoc if needed.
- Extranets to connect partners, suppliers, users, and providers without the expensive overhead of leased lines or controlled modem access.

2.3.1 Remote Access Computing

Figure 2-2 below is one possible VPN configuration for remote access, employing statewide or national Internet Service Provider services to route from the end user location to the target VPN gateway.

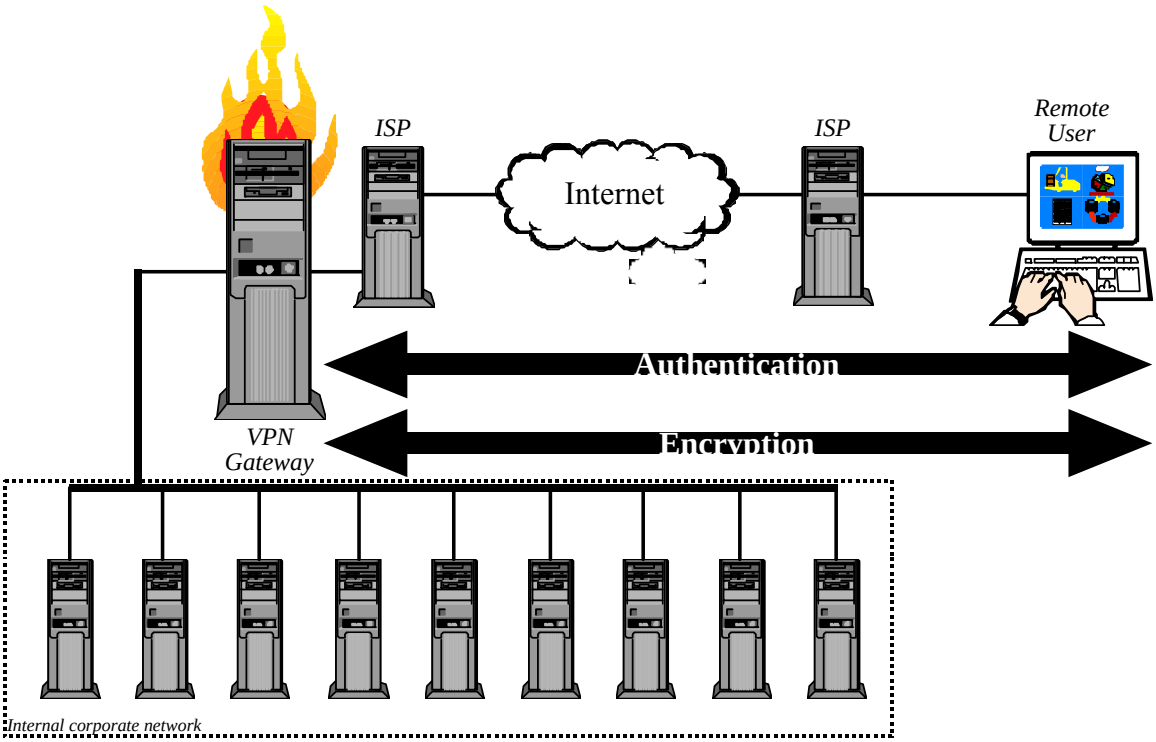


Figure 2-2 Remote Access VPN

Some of the benefits from using Remote Access VPNs include:

- Uses low-cost ISPs instead of long-distance phone access and costs
- Reduces network complexity and support costs
- Network help desk calls are serviced by managed ISP rather than internal support channels
- Helps with IT chargeback accounting and management

2.3.2 Branch Office Networks

Figure 2-3 below illustrates one possible configuration to bridge a branch office with a home office

network. It too uses statewide or national ISP services for the connections to the 'last mile' between locations.

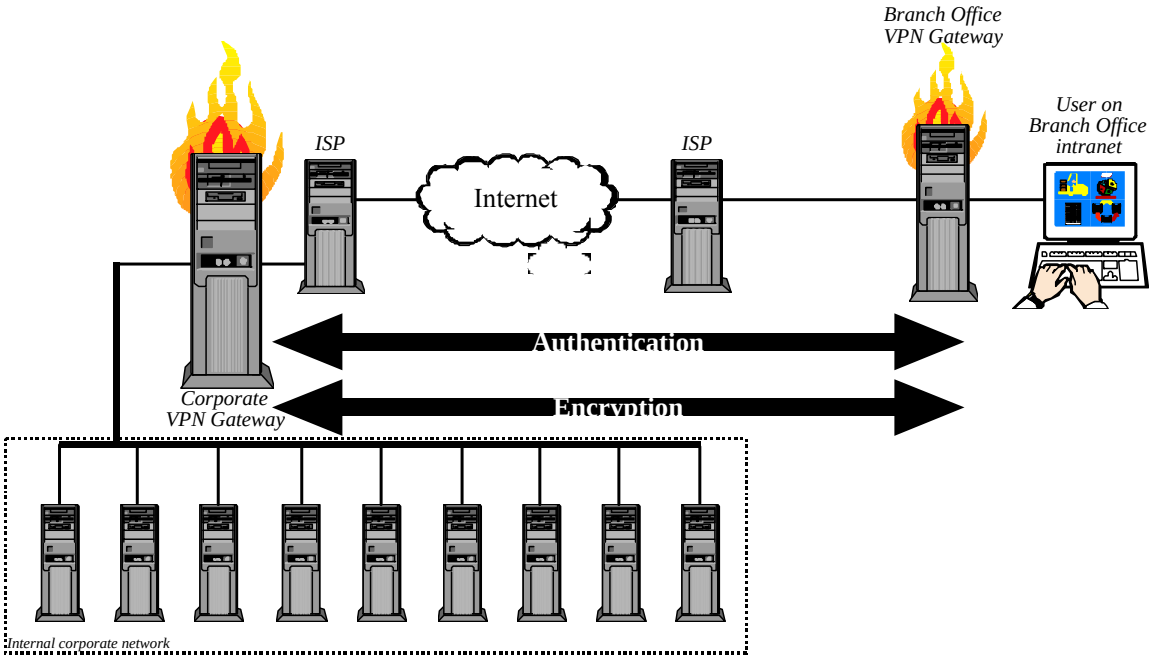


Figure 2-3 Branch Office VPN

Some of the benefits from using Branch Office VPNs include:

- Elimination of 56KB and other dedicated leased lines
- Elimination of SNA coax controllers using pooled services
- Replacement of PCs using thin client technology
- Bridge between departmental or organizational intranets
- Reduced software licensing costs

2.3.3 Extranets for Business Partners and Suppliers

Figure 2-4 shows the typical VPN connection for extranet users, employing a Certificate Authority for the management of digital certificates for access controls to the network. A public directory (LDAP) is used to enable locating the users of the system, along with their public key certificates, to facilitate private communications and to manage the VPN user base.

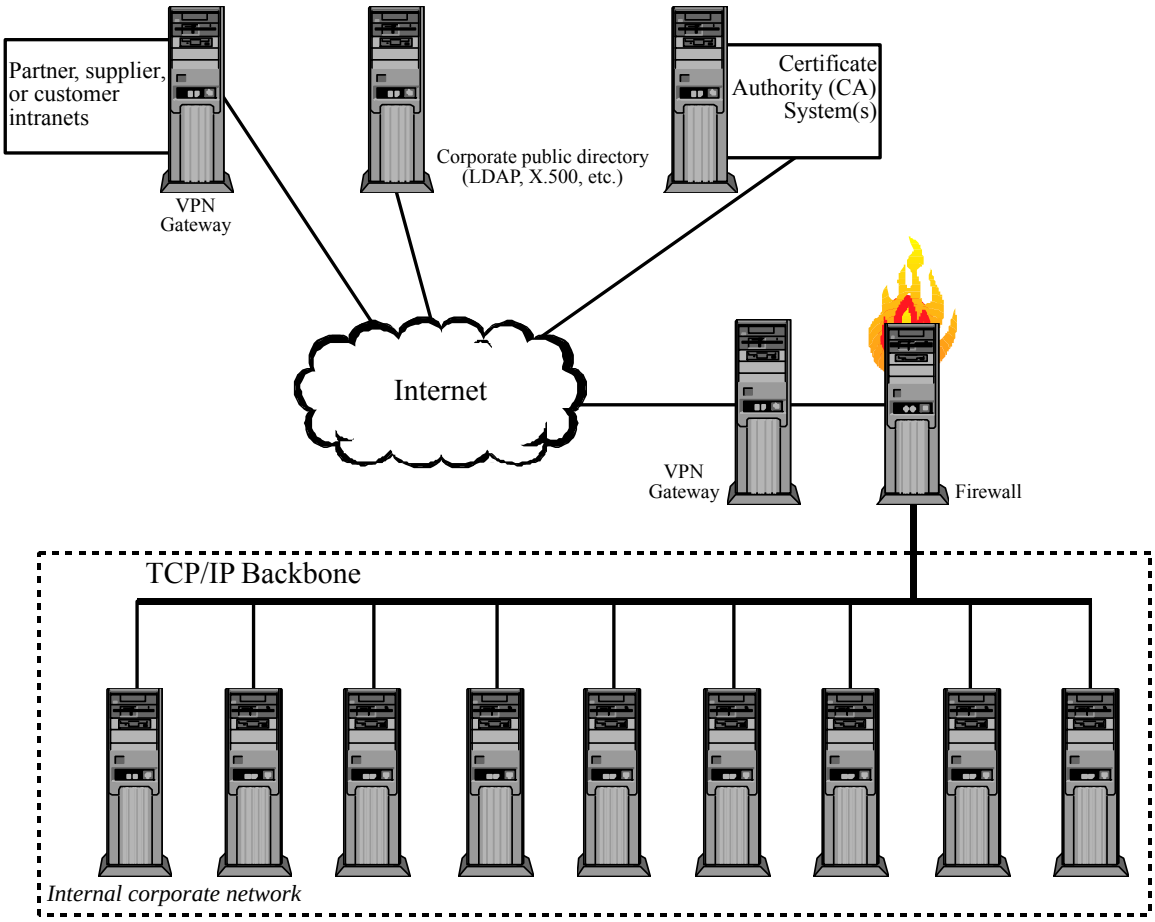


Figure 2-4 An Extranet VPN Configuration

2.4 ADOT Directives for VPN Pilot Uses

ADOT has identified a wide variety of potential uses for a VPN, primarily for users of Motor Vehicle Division (MVD) networks. The three types of businesses MVD wishes to explore VPNs with include:
1. **Third-party access**
With the additional network connectivity provided by a VPN, MVD wishes to extend network access to areas where leased lines are unavailable or cost prohibitive to operate, as well as open up access to those who don't need dedicated connections into ADOT.

Third-parties are defined by ADOT as:
"Any external agent who performs MVD work or has access to MVD data"

Some of the third-party customers identified are:

- **Automated Transaction Third Party** who are external agents performing MVD work online. These include AADA, AMTA, Hertz, and Academy. Services provided include title, registration, MVRs, and driver license processing.
- **Electronic Delivery Transaction Third-party** as external agents doing online work through alternative electronic delivery methods, such as Service Arizona and Vector (E-titles).
- **Non-automated third-parties** who perform off-line MVD work such as offline dealers and TSS who provide title and registration paperwork processing, vehicle inspections, driver license

training and testing.

- **Automated government customers** who are non-ADOT government agencies that access MVD systems for updates. Examples here include county assessors, DOR, ATAA, etc. Some of these services include mobile home taxes, Watch Your Car, placing stops, and legislated record updates.

Other Records Customers Only are another identified group of users within the Third-party definition. Included here are:

- **Automated records customers** who are external agents that access MVD records in read-only mode. Examples include government agencies, insurance companies, private investigators, photo radar administrators, and R.L. Polk.
- **Mandated Records Update customers** are external agents who transmit data to MVD for purposes of updating MVD databases. Examples include Gordon Darby, insurance companies, and Arizona courts. Information being provided includes conviction processing, emission testing updates, etc.

2. **Electronic Data Interchange (EDI) and File Exchange Services**

MVD has identified the need for secure File Transfers to move sensitive information between providers and users without expensive infrastructure changes or management. Some of the records identified for these types of transfers include:

- Motor Vehicle Records
- Mandatory insurance
- Court convictions and warrants
- Abandoned vehicles and towed vehicle records
- Fleet processing at the point of information origination
- License plate processing
- Emissions data
- Financing and insurance records
- Electronic vehicle tittles and liens
- Replacement of magnetic tape processing that's currently being conducted between batch systems

3. **Internet transactions**

MVD hopes to expand online services either through third-party providers of directly on the MVD Web site. Some of these functions include:

- MVD policies and procedures available via the Internet
- Ordering special plates
- Access to motor vehicle records for both drivers and vehicles
- Ordering duplicate copies of registration information
- Sold notices
- Applications and other common forms
- Personalized license plate inquiries for availability
- Ordering replacement license plates, tabs, and title records

Other potential uses identified for an ADOT VPN for the MVD includes remote viewing and management of the *Q-Matic System* at MVD offices for service improvement opportunities or early warning of queuing problems being experienced, thus jeopardizing the service level promises

established by MVD administrators.

A number of Government-to-Government (G2G) potential uses were also identified, including Electronic Funds Transfers (EFT) and credit card payment processing, and broader access to the Driver Record Information Verification System.

In June 2000, Craig Stender, CIO of ADOT, chose to pilot the VPN first with third-party providers and users of MVD systems following a successful internal pilot testing period with Technical Information Resources (TIR) and other ADOT employees.

2.5 Security Classification of MVD Data

To best gauge the levels of security required on MVD records, it was necessary to obtain a guiding principle for how much security on the VPN is deemed sufficient. After a discussion with Craig Stender, CIO of ADOT, it was determined that the data is considered **sensitive** -- needing strong access controls, but otherwise *not treated* the same as data deemed confidential or proprietary in nature. This point is critical for understanding the rationale behind the VPN architecture slated for MVD pilot testing.

3. ADOT Testing of VPN Technology

Employees in the ADOT TIR Department initiated evaluation and testing VPN technology early in the first phase of this project using equipment and software that ADOT already owned. The intent was for TIR to make a recommendation to ADOT for a system was deemed both reliable and secure. Two systems were tested:
1. Microsoft Windows 2000 VPN
2. Checkpoint VPN1

3.1 Internal testing

These products were tested in the laboratory using one Compaq Proliant server and 3 Compaq workstations, including one laptop computer. These were attached using 100MB Ethernet.

Problems with the Checkpoint firewall appeared early and with any ability to troubleshoot the interaction between the Checkpoint system and Windows NT, further efforts at testing were abandoned. The results of testing the Checkpoint VPN are summarized below in Table 3.1

Application	Pass/Fail	Reliability and comments
Telnet	Pass	Good
FTP	Pass	Good
MS Outlook (e-mail)	Fail	50% reliability - unknown causes
MS Networking (file access)	Fail	50 reliability - unknown causes

Table 3.1 Results of Checkpoint VPN1 Testing

Concentrating on the Windows 2000 VPN solution, using Microsoft's implementation of PPTP, the team was able to successfully install and access the suite of applications that remote users of ADOT systems would normally access.

The results of the Windows 2000 VPN using 128-bit encryption are shown in Table 3.2.

Application	Pass/Fail	Reliability and comments
Telnet	Pass	Good
FTP	Pass	Good
MS Outlook (e-mail)	Pass	Good
MS Networking (file access)	Pass	Good
SMS 1.2	Pass	Good
HEAT (OBDC)	Pass	Good
MS Terminal Server	Pass	Good
MS SQL Server	Pass	Good

Table 3.2 Results of MS Windows 2000 VPN Testing

Notes from the evaluation report indicate that all applications tested successfully without any connectivity or performance problems. Network bandwidth never exceeded 50% utilization.

Once the technology was proven sufficient for TIR requirements, the pilot test was expanded to other internal ADOT employees who used a variety of workstations, including MS Windows 2000, Microsoft NT Workstation, and Microsoft Windows 95/98. Connection types also varied. Users accessed the Internet using Digital Subscriber Line (DSL), Cable modems, traditional dial-up, and even 2-way wireless technology. A number of different ISPs were used by the testers as well, including:

- Bizillion
- USWest/Qwest
- COX@Home
- AOL
- Sprint broadband

The pilot ran from April 2000 through August 2000 when it was determined that the Windows 2000 VPN met the criteria for a TIR recommendation to ADOT to proceed with expanding the pilot to select MVD third-parties.

3.1.1 Short-term recommendations and plans

Due to ADOT's commitment to the Microsoft product line for both infrastructure (networks and OSs) and application programs (terminal server, Outlook, etc.), using VPNs other than Microsoft's was thought to lead to support and reliability problems. Marketplace research supports this theory. Since many of the protocols used within the Microsoft family of products are atypical of the protocols most often found on the Internet. The support that vendors other than Microsoft are providing on their VPN products often do not work well with Microsoft protocols, but this will not always be the case. As VPN technology matures and standards shake themselves out, in the future VPN products should become fungible. However in today's marketplace reality they're not quite there yet and organizations simply cannot wait.

As a participant in the standards process, Microsoft pledges support on future products for whatever the industry standard calls for and has provided a migration path for users. Despite the criticisms of Microsoft's implementation of PPTP, what's important is that the system *does operate* as needed and still provides the sufficient layer of security needed to protect MVD records.

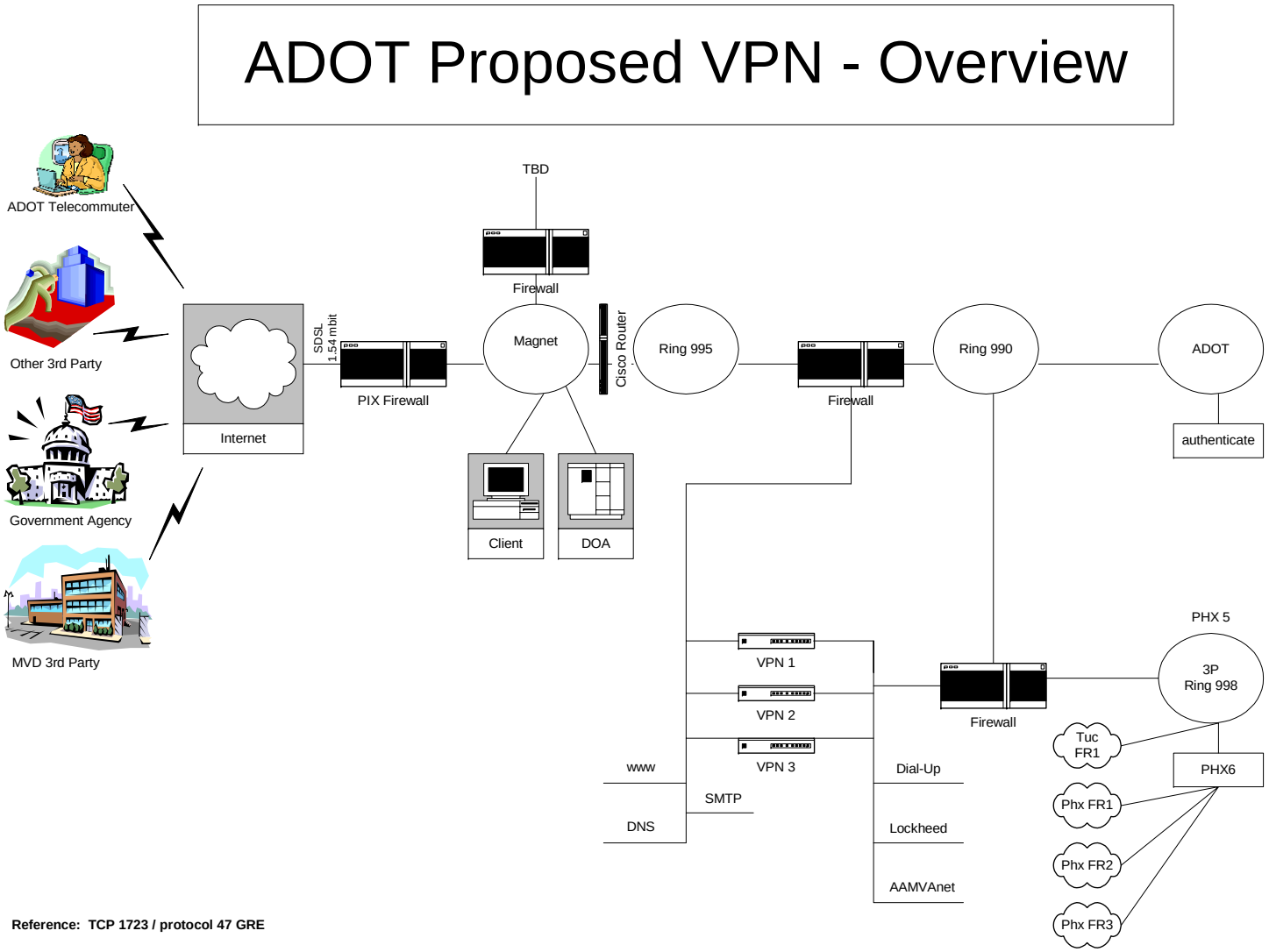
Research indicates that IP Security (IPSec) will become the dominant standard for VPNs. In today's environment however, implementing an IPSec VPN and expecting full interoperability and reliability is still too premature. For those organizations who operate their systems based only on the 'purist' protocols upon which the Internet was built, IPSec-based VPNs are likely to work well. On the other hand, those who use other types proprietary protocols (like Microsoft) are given two basic choices:

- Wait until the standards shake themselves out, then invest in the technology
- Tip-toe slowly into the technology by adopting 'what works today' with an eye to a point of arrival migration (wherever that may be).

TIR opted for the second choice.

In late-October 2000, a Project and Investment Justification (PIJ) was prepared to use the research dollars tied to capital investments to purchase the hardware and needed to offer load-balancing, fail-over, and improved reliability. The proposed network architecture is shown in Figure 3-1 below.

Figure 3-1 Proposed VPN Architecture



3.2 External Testing of the ADOT VPN Solution

ADOT business partners began recruiting efforts to locate potential testing organizations with an understanding that they were participating in an experiment. Once the paperwork found its way back to TIR with the appropriate approvals, 3 organizations were participants:

- City of Phoenix Prosecutors Office
- Federal Bureau of Investigation
- Scottsdale Police Department

3.2.1 City of Phoenix Prosecutor's Office

The City of Phoenix Prosecutors Office already had access to MVD records through a dated Wang terminal server to gain access to the MVD mainframe. This connection was over a private link into the ADOT back office network. The Prosecutors Office elected to try the VPN to replace the Wang since support and maintenance costs far exceeded its value to the organization. Gail Piceno of the Prosecutor's Office claimed that she was spending $100,000 annually for a maintenance contract (Wang has long since been bankrupt), and an additional $40,000 annually for a contract programmer to keep the system active for users. The eventual elimination of the Wang will save the City of Phoenix close to $150,000 per year in maintenance costs.

In a telephone interview with Ms. Piceno in October 2000, she exhibited near elation with the VPN system and could not thank the TIR staff enough! A follow-up several weeks later reinforced her initial opinion.

The City of Phoenix Prosecutors Office is an example of a Server-to-server VPN as opposed to a desktop to VPN server configuration, as with the other third-party pilot testers.

3.2.2 Federal Bureau of Investigation

The Phoenix FBI Office needs access to drivers license images to help the Fugitive Task Force and the FBI arrest squads in properly identifying criminals prior to their arrest. Prior to gaining access to imaging records via the VPN, the FBI sent a staffer to the basement of the MVD office several times a day to retrieve driver license images. All requests were submitted and processed manually. Five people on the FBI Investigative Assistance Team (the former MVD runners) now access image records via the ADOT Pilot VPN. Ten people have been set up for access from the FBI, planned for future uses. Shawna Watson, system administrator for the FBI's network is relieved that the time savings and travel reduction are helping the FBI offices tremendously. She claims that the system was highly reliable when it was first installed, but lately some changes within ADOT are causing sluggishness and downtime. The FBI has re-arranged some working schedules to try and pull images at those times that have proven the most reliable for VPN access. While she'd like to see 100% reliability, she's still grateful for the system and hopes to roll-out access to all who need it within the Phoenix FBI office.

It should be pointed out that the reliability issue has nothing to do with VPN. The application they are accessing has the problem and the vendor responsible is working on it. The VPN connection has never had a problem. The VPN server has never experienced any technical problems. There have been a few problems, but all of them have turned out to be either client or network related.

3.2.3 City of Scottsdale Police Department

As of October 2000, paperwork was holding up the access to the VPN from the City of Scottsdale Police Department, and follow-up calls in November 2000 to Captain Burl Haenel went unanswered. Another round of follow-up calls will be conducted early in 2001 to determine progress and satisfaction.

To aid in research for the entire pilot period (expected to end around May 2001), 2 questionnaires were prepared for the testing third-party organizations. The two surveys are shown in Appendix A and Appendix B respectively. As information is collected and analyzed, and as new participants come online, the data will be summarized and prepared for reporting in the final version of this report, expected in the Summer of 2001.

3.3 Tests Conducted and Preliminary Results

The testing that's currently underway for both types of access to the ADOT VPN -- server-to-server and remote client to server -- appears promising and should indicate that the system is successful and should be made an ADOT offering in the future. Once the proposed hardware configuration is installed, tested, and rolled-out, expansion of the system to other third-parties should become routine. As new participants enter the mix, their experiences will be incorporated into the final report.

3.4 Lessons Learned from the Tests

The detailed information on the lessons learned will appear in the Phase II report.

4. Analysis of VPN Survey Questionnaire

This portion of the report will be completed in the final report for the project in Summer 2001.

4.1 Survey Sample Information

See Appendix A and B for sample surveys.

4.2 Analysis Summary

The analysis summary will appear in the Phase II report.

5. Conclusions

The efforts to field-test a VPN for access to MVD records are increasingly successful as the system is rolled-out to new prospective users. Field data contained in the Phase II report will be used to support the project's final recommendations and conclusions.

Appendix A: Survey form for Third-party System Administrators

Arizona Department of Transportation
VPN Questionnaire For Remote Site Administrators

SA Name:	Number of users who will connect to the VPN pilot?
Organization Name:	Number of users who will connect to the VPN at full rollout?
E-mail ID:	Types of users: □ Internal employees □ Remote employees (at home, on road, etc.) □ Contract employees □ Customers □ Suppliers
Job title:	VPN primary use: □ LAN-to-LAN □ User to network □ Both
Ease of installation/set-up/configuration (1=easy,5=difficult)	Comments about your installation:
Have you had prior experience with a VPN? □ Yes □ No	
Did you encounter any problems with your system after installation? □ Yes □ No	
Describe:	

Are you able to successfully access the following:		COMMENTS
Network Files/Drives (MS Networking)	□ Yes □ No □ Do not usually access	
Email (MAPI)	□ Yes □ No □ Do not usually access	
MS Terminal Server	□ Yes □ No □ Do not usually access	
NT Administration Tools	□ Yes □ No □ Do not usually access	
File Transfer Protocol (FTP)	□ Yes □ No □ Do not usually access	Record average file transfer speeds here: _____Kbytes/sec.
MS SQL Server	□ Yes □ No □ Do not usually access	
Mainframe	□ Yes □ No □ Do not usually access	

Appendix B: Survey form for Third-party VPN Users

Arizona Department of Transportation
VPN Questionnaire For Users

User Name:	Operating System:
Organization:	ISP Name:
Date:	Connection Type/Speed
Job title:	Ease of installation/configuration (1=easy,5=difficult)
Computer Manufacturer/Model:	Memory on PC: _____ MB
Comments about your installation:	
Have you had prior experience with a VPN? □ Yes □ No	
Did you encounter any problems with your system after installation? □ Yes □ No	
Describe:	
Can you connect to your ISP?	□ Yes □ No
Can you connect to the VPN server?	□ Yes □ No
What is your connection speed?	Bytes/second
Are you able to authenticate to the LAN?	□ Yes □ No
What forms of authentication to the VPN do you use?	□ Hardware token □ Software token □ Static password □ Static IP address □ Other:

Are you able to successfully access the following:		COMMENTS
Network Files/Drives (MS Networking)	□ Yes □ No □ Do not usually access	
Email (MAPI)	□ Yes □ No □ Do not usually access	
MS Terminal Server	□ Yes □ No □ Do not usually access	
NT Administration Tools	□ Yes □ No □ Do not usually access	
File Transfer Protocol (FTP)	□ Yes □ No □ Do not usually access	Record average file transfer speeds here: _____Kbytes/sec.
MS SQL Server	□ Yes □ No □ Do not usually access	
Mainframe	□ Yes □ No □ Do not usually access	

ADOT VPN User Questionnaire - Page II

Name: _____

What's on your wishlist for future uses of the ADOT VPN?
What are your security concerns regarding your network or access to the ADOT VPN?
What are your overall comments about your experience with the ADOT VPN?
What are your overall recommendations for the ADOT VPN?

Appendix C: Project and Investment Justification

Project and Investment Justification

A Statewide Standard
Document for Information Technology Projects

Project Title: **Virtual Private Networks**

Version 3.0 Revised 01/01/99

Prepared by:

Name	**Diane Ohde, Project Manager**
Agency	**AZ Dept. of Transportation, Technical Information Resources**
Date	**October 25, 2000**

Table of Contents

Section I. Business and Technology Assessment

Agency Name and Address	*Contact Name, Phone, FAX*
AZ Department of Transportation Technical Information Resources Project Management 206 S. 17th Avenue, Room 119A Phoenix, AZ 85007	Debra Stroops 602/712-6723 602/712-8105

Project Investment Name	*Date*
Virtual Private Networks	October 25, 2000

A. Management Summary

ADOT customers are faced with soaring communications costs. External customers such as MVD Third Parties and other Government entities access the ADOT network by either dialing in or paying QWest for dedicated lines. All customers that are located outside of the Phoenix metro area must incur long distance charges to connect to the ADOT network. This may impede potential customers from providing ADOT services or doing ADOT business. QWest does not provide dedicated connections to several remote locations.

The purpose of this project is to research and develop a VPN technology to help ADOT reduce network cost structures, remove barriers to ADOT network connectivity, increase client connectivity capacity, and improve computer-based communications with ADOT's employees, suppliers, and business partners.

Is this project mandated by law, court case or rule? (Circle One)	**No**
However, ADOT operates under the Arizona Revised Statues, Title 28, Transportation, which regulates financial and licensing transactions of the state and the Virtual Private Network, as a tool of the agency, falls under this statue.	

The following table contains summary information taken from the other sections of the PIJ document.

Description	Section	Line	Significance
Value Rating	II. A. Value to the Public	10	21
Economic Benefits	II. B. Benefits to the State	8	$79.2k Annually
Total Development Cost	III. A. Development Costs	14	$99.8k

B. Proposed Changes and Objectives, "To Be"

The purpose of this project is to research and develop a VPN technology to help ADOT reduce network cost structures, remove barriers to ADOT network connectivity, increase client connectivity capacity, and improve computer-based communications with ADOT's employees, suppliers, and business partners. Customers that currently have high-speed access will notice a significant increase in performance. There will be a broader range of connectivity options, i.e. Lake Havasu, where leased lines are cost prohibitive. VPN limitation connections will not be an issue. VPN will enable more MVD 3rd Party entities to come on-line in remote areas which benefits the agency by decreasing the business impact and improves quality of service to the general public for remote and local areas.

The following criteria was used to select the VPN solution:

- Cost
- Connectivity
- Security
- Simplified Network Management
- Current Standards governing VPN technologies.

ADOT is proposing a dedicated ISP connection for VPN until DOA can guarantee QOS to ADOT for VPN. Cost cannot be provided at this time due to contract negotiations not being finalized.

Following is a high-level project plan on the phased implementation:

Phase I

Phase I will be research and analysis of VPN solutions.

Alternatives Researched:

- Microsoft VPN
- Checkpoint – VPN-1
- Nortel – Nonresponsive

Timeframe: March 2000 – June 2000

Phase II

Phase II will validate the Microsoft VPN alternative chosen from Phase I.

Testing included a small group of telecommuters. A select group of TIR technical staff started the initial testing, and then gradually grew to 20 ADOT personnel.

Current testing has shown that bandwidth has direct negative impact on the results of the VPN solution.

Start Acquisition for test servers to verify proof of concept.

Timeframe: June 2000 – August 2000

Phase III

Phase III will bring on a limited subset of ADOT customers for testing. This testing will validate larger customer implementation. ADOT will pursue a dedicated ISP connection for VPN.

Identified customers for this phase are:

- Government to Government (G2G)
  - ✓ To include larger customers (45 plus customers)
  - ✓ Validation of site to site connectivity and security

Timeframe: September 2000 – January 2001

Phase IV

Phase IV will initiate implementation thereby providing connectivity to government to business (G2B), other

G2G customers as well as ADOT telecommuters.

- Depending on business needs, additional infrastructure will be required
- Foreseeable support for up to 3,000 client connections
- Future performance is indicative of bandwidth constraints

Timeframe: January 2001 – On-going

C. Existing Situation and Problem, "As Is"

ADOT customers are faced with soaring communications costs. External customers such as MVD Third Parties and other Government entities access the ADOT network by either dialing in or paying QWest for dedicated lines. All customers that are located outside of the Phoenix metro area must incur long distance charges to connect to the ADOT network. This may impede potential customers from providing ADOT services or doing ADOT business. QWest does not provide dedicated connections to several remote locations. ADOT customers that travel frequently and must connect to the ADOT network are incurring excessive long distance charges.

ADOT is currently using a 10MB shared ATM link through DOA, which is being utilized by all State agencies. Quality of service from DOA cannot be guaranteed.

Internal and external customers that are currently RASing in are near capacity at 48 concurrent connections.

D. Proposed Technology

Microsoft VPN was the chosen alternative. There were many reasons for this. Some of the most predominant are:

- Compatibility with existing clients
- Current support contract covers solution
- Support personnel very familiar with solution
- Compatible with ADOT business applications
- Works with ADOT enterprise hardware
- Extremely scalable
- Minimal impact to infrastructure
- Fault tolerant
- Modular

Hardware

All Servers and Software Firewalls are rack-mountable Compaq ProLiant DL380R with:

- ProLiant DL380 275 Watt Redundant Power Supply Module
- Pentium III 733 Mhz Processors with 256Kb L2 Cache
- 133Mhz FSB
- 256 MB 133MHz SDRAM
- Four 9.1 GB Hot Pluggable Wide Ultra3 SCSI Universal 10K RPM Drives in a RAID 5 configuration with a hot stand by.
- Two Intel Pro 100S Fast Ethernet NIC Cards (Three in Firewalls)
- Compaq V700, 17" Color Monitor shared on an 8 port SVGA / PS/2 switch box

Software

- Microsoft Windows 2000 Advanced Server
- Microsoft Windows NT 4.x Server
- Microsoft ISA/Proxy Server
- Checkpoint Firewall-1

ADOT VPN Proposed Architecture

Refer to diagram in Appendix B for overview.

- Two firewalls are used to protect the integrity of the ADOT network.
- Two managed switches are used to provide traffic segregation and information flow.
- Windows 2000 is the primary Operating System used.
- The VPN traffic is segregated based on load and type of connection.
- IP addressing is provided by INTERNIC standard non-routable addresses used via NAT translation built in to the OS.
- The VPN servers provide Disaster Recovery through the use of MNLB technology built in to the OS
- multiple power sources including 2 UPS sources
- automated shutdowns
- The VPN servers also have internal Fault recovery.
- Redundant power supplies
- Hot Stand By Hard Drives
- RAID 5

Strategy

Hardware:

The VPN solution needed to address the majority of ADOT customer's hardware needs. In doing so the following were considered: Macintosh, Linux / UNIX, Windows 3.x, NT, 9x and 2000.

Transport Protocol:

There are many VPN protocols that can be used. Some examples are: PPTP, L2TP and IPSec. ADOT selected the Point-to-Point Tunneling Protocol (PPTP) for its VPN Solution. PPTP was chosen because of its:

- Low cost of implementation
- Ease of installation
- Accessible to dial-up users
- Ease of management
- High performance
- Low network overhead
- Compatibility with many Operating Systems and Hardware

PPTP is pervasive within the OS world and is predominant in the Microsoft OS's that ADOT has standardized on. This protocol encapsulates and encrypts the "private" data, allowing it to travel across public networks securely. PPTP supports many data encryption rates to rates to assure secure transmission of data.

Internet / Intranet Access Points:

Internet and Intranet access is accomplished through a combination of both client subscribed, ISP owned and internal ADOT Layer 3 hardware. All internal DNS requests to ADOT's Web server(s) are routed via ADOT owned equipment. While ADOT provides proxy service to its internal LAN and Dial-Up users, the VPN connection affords a completely separate connection to the Internet, via the user's ISP. The benefit is twofold, while security is increased, network traffic is reduced by eliminating standard Internet traffic such as web browsing and the occasional downloading and uploading of files.

E. Major Deliverables and Outcomes

Expected deliverables are:

- A cost effective and secure method for internal and external customers to access the ADOT Network.
- Solution will provide a secure connection to the ADOT Network in areas where point to point connection or Frame Relay are not available.
- Capability of providing bandwidth beyond dial-up speeds.
- Enables network to network connectivity, which is not available today.

- Current limitations on concurrent users will no longer be an issue.
- External customers will experience substantial savings by utilizing VPN technology.

Section II. Public Value and Benefits

A. Value to the Public

***Score:* 0=None, 1=Minor, 2=Moderate, 3=Considerable, 4=Substantial, 5=Extensive.**

Description	*Score*
Client Satisfaction: Applies to performance of the health and welfare services. How clients feel about the services they receive. This is closely associated with life safety functions.	**1**
Customer Service: Applies to improvements in internal and external customer service delivery by this project. Consideration should be given to imposing obligations from police departments, tax collectors, and environmental protection. It is important to distinguish citizen's evaluation from client's services.	**4**
Life Safety Functions: Applies to public protection, health, environment and safety. Consider how this project will reduce risk in these functions.	**4**
Public Service Functions: Applies to licensing, maintenance, payments and tax. Consider how this project will enhance services in these functions.	**4**
Legal Requirements: Consideration should be given to projects mandated by federal or state law. Other consideration could be given if there are interfaces with other federal, state, or local entities.	**4**
Product Quality: Applies to the information and services delivered to internal and external customers and the public.	**4**
Other: List any other applicable value or benefits.	
Total	**21**

Detail Description of Project Benefits
(Describe in detail any category in the *Value to the Public* with a score greater than 3) **Customer Service -** a) Enables connectivity that currently is not available. b) Cost effective for 3rd Party customers allowing smaller companies to participate. **Life Safety Functions -** a) Allows Law Enforcement to obtain information not currently available. b) Reduces Travel **Public Service Functions -** Enables citizens to more easily pay required licensing and taxes. **Legal Requirements -** Enables connectivity necessary for interagency communications. **Product Quality -** Service will be enhanced by more information being available.

B. Benefits to the State

Score: **0=None, 1=Minor, 2=Moderate, 3=Considerable, 4=Substantial, 5=Extensive.**

Savings: Enter the sum of measurable benefits for that category. The description and method of calculation are explained in the table labeled "Description of Savings."

Description	*Score*	*Savings*
Agency Performance: The extent to which duties and processes will improve or positively affect set business functions. Consider reduced redundancy and improved consistency for the agency.	**5**	
Productivity Increase: The improvements in quantity or timeliness of agency or division offerings and deliverables. Consider improved turnaround time or expanded capacity of key processes.	**5**	30k Annually
Operational Efficiency: The project is justified with a clearly defined payback and programmed period. Measure the agency's ability to adapt to change and remain resilient in the face of new requirements or expectations.	**5**	30k Annually
Accomplishment Probability: The extent to which this project is expected to have a high level of success in completing all requirements for the division or agency.	**5**	
Functional Integration: The impact the project will have in eliminating redundancy or improve consistency. Consider the practical means if the project functions in the proper or expected manner.	**5**	19.2k Annually
Technology Sensitive: The implementation of the right types of technology to meet clear and defined goals and to support key functions. Consider technologies and systems already proven within the agency, division or other, similar organizations.	**5**	
Other: List any other applicable benefit.		
Total	**30**	79.2k Annually

Additional Information on Savings
(Describe in detail the calculation for any item with a total greater than $50,000)

Currently, remote network access is attained via the client's POTS and two carrier-supplied, channelized T-1 circuits. Both circuits allow forty-eight total, simultaneous dial access sessions to the RAS Server. Data transfer rates are limited to the FCC mandated 56Kb/s, V.90 protocol. Once the forty-eight ports are in use, the next attempt results in a busy signal, denying entrance to the network. This ultimately results in production loss from the remote location. These conditions can be especially prevalent during end of month, when consultants and contractors are submitting construction payment estimates. Two circuits at $1600 each / month results in an overhead of $38,400 annually. The remote network access can be minimized due to the VPN alternative.

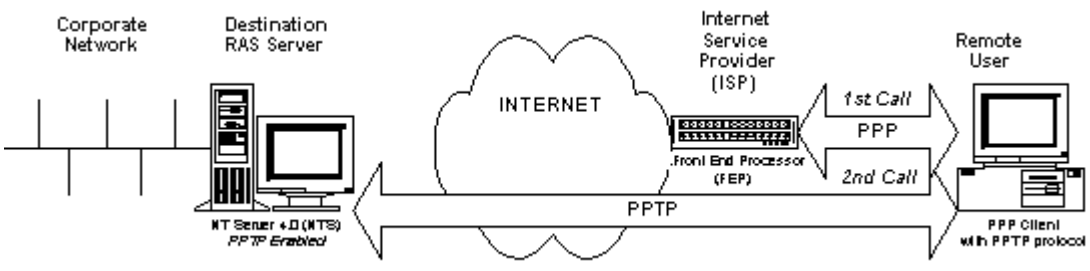
When connecting from outside of the home server's LATA, direct inward dialing to the enterprise network forces the user to incur toll charges. These charges are billed back not only by traveling employees but also by consultants in remote locations. In addition to the tolls, lodging establishments usually include a surcharge and / or inflated rates for long distance calling, which is reflected on the employee's expense report. Outlying offices without direct network connectivity dialing in for just two hours a day results in a monthly long distance bill of $216.00 per user. One hundred users dialing in for this length of time cumulatively, over the length of one year, cost the state $259,200. While 800 services may seem like an alternative, even a low rate such as $0.04 / min. still calculates to $155,200 annually, for the same hundred users.

The Clean Air Campaign promotes a 15% telecommuter guideline. With a 5,000+ ADOT computer base, 750 employees could be potential, remote users. As stated above, the infrastructure to support users of this volume is not in place and would be costly to retrofit ADOT's legacy RAS system.

Personal Internet Service Accounts are commonplace and free internet access is available to anyone with at least an analog phone line and a computer. Demographic restrictions are eliminated because most ISPs have a broad range of local access numbers to dial-in to. No matter where the user is or whether or not the ISP supports PPTP, they simply dial-up or connect directly to their individual Internet Service and "Tunnel" in to the remote ADOT network.

This is particularly effective for telecommuters and consultant offices using LEC offered broadband options such as @Home or xDSL. Network performance increases at least five-fold and some may realize as much as twenty-five times the speed of analog 56Kb/s, depending on subscribed speeds and varying Internet throughput.

Deploying VPN in the enterprise network ultimately lowers overall remote LAN access TCO. Given monthly leased circuit charges, limited user capacity, bandwidth constraints, long distance charges and more labor intensive administrative tasks, direct Dial-up connections are a thing of the past.



Section III. Financial Assessment

A. Development Costs

Fiscal Year						
Description	*FY 00-01*	*FY____*	*FY____*	*FY____*	*FY____*	*Total*
The number of FTE and third-party positions						
1. IT FTE Positions						**(Do not use)**
2. User FTE Positions						
3. Professional and Outside Positions	1					
4. Total Positions *	1					
The development costs in thousands ($000)						
5. IT FTE (Include ERE)						
6. User FTE (Include ERE)						
7. Professional and Outside Positions	$14					$14
8. Hardware	$73.8					$73.8
9. Software	$12					$12
10. Communications						
11. Facilities						
12. Licensing and Maintenance Fees						
13. Other- Services						
14. Total**	$99.8					$99.8

* Items 1 through 3 are be included in ***Section I.F Roles and Responsibilities***.

** Items 7 through 13 are be included in ***Appendices C. Itemized List with Costs.***

E. Funding

1. Timeline

Five Year Total ($000)						
Agency	*FY 00-01*	*FY____*	*FY____*	*FY____*	*FY____*	*Total*
1. Available Base Funding	$55.3					$55.3
2. Additional Appropriations						
3. Other Funding Source	$44.5					$44.5
4. GITA Special Funds						
5. Total Funding (*)	$99.8					$99.8

2. Source

Funding Source ($000)			
Name of Funding Source	***Base***	***Additional***	***Total***
1. General Fund	$55.3		$55.3
2. Transportation Research Fund	$44.5		$44.5
3.			
4.			
5.			
6.			
7. Federal Funding			
8. Funding Source Total (*)	$99.8		$99.8

(*) Equals the "Total Costs" from ***Section II. C. Summary of Costs by Year***, line 3.

Section V. Project Approvals

The appropriate signatures must be obtained from the Agency Sponsor and Agency CIO. The Agency Director or CEO's signature is required on projects over $1 million or on projects considered critical in nature to the Agency.

A. Project Approvals

Project Title: **Virtual Private Networks**

Responsibility	*Approval Signature and Title*	*Date*
Project Sponsor*:*		
Agency CIO*:*		
Agency Director:		
Comments:		

Appendices

A: Itemized List with Costs

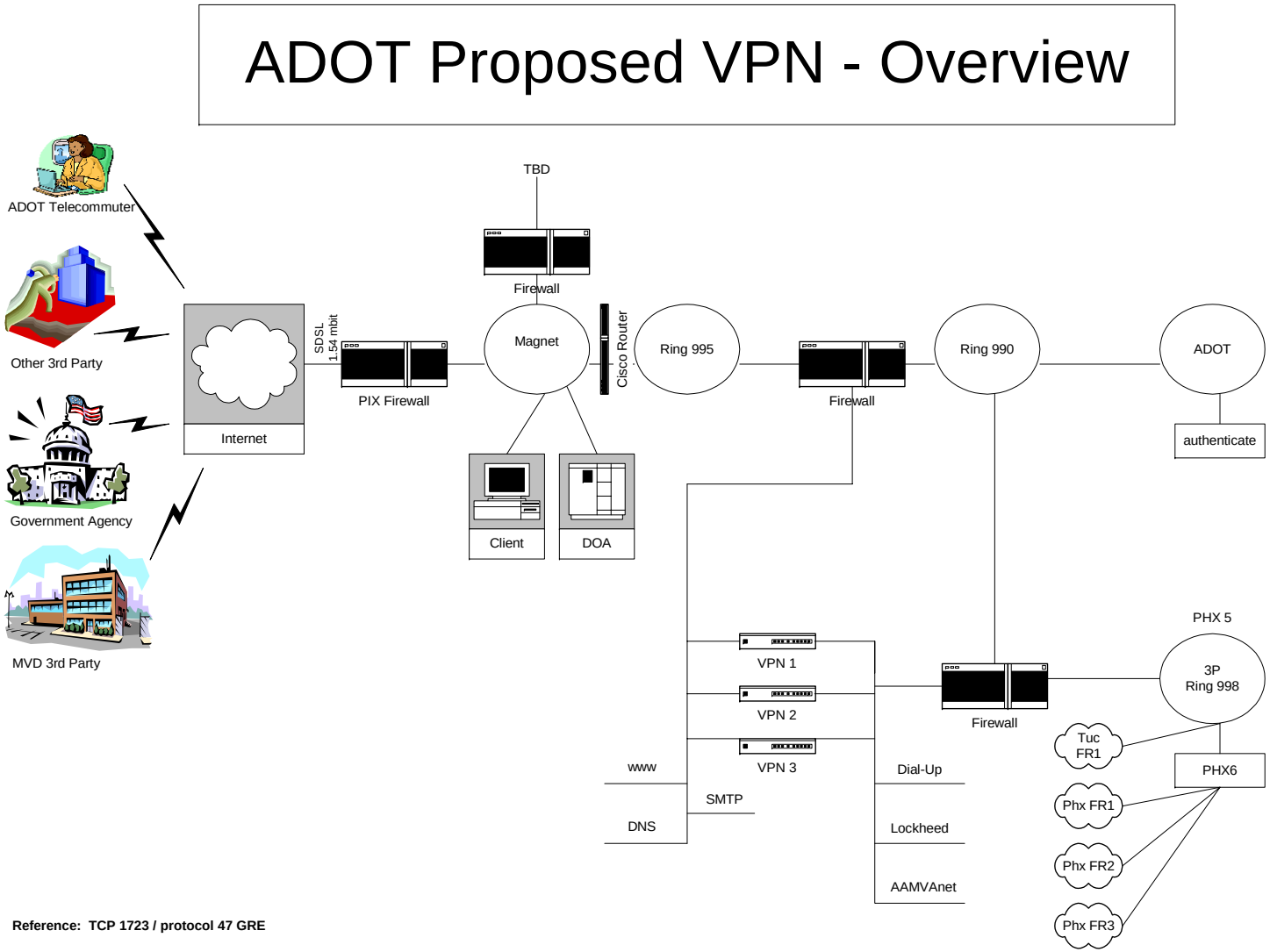
A. Development Costs -- Line 8 -- Year 00/01

Hardware		Unit Cost	Total
6	Compaq ProLiant DL380R	$4,816	$28,896
6	ProLiant DL380 275 Watt HP RPS Module	$324	$1,944
24	9.1 GB Pluggable Wide Ultra3 SCSI Universal 10K Drive	$561	$13,464
6	256 Reg 133MHz SDRAM DIMM	$896	$5,376
4	Pentium III 733/133-256K Processor Option Kit	$1,619	$6,476
20	Intel PRO 100 S	$121	$2,420
14	9' CPU-to-Switch Cable - Server	$71	$994
2	Catalyst 2924M XL autosensing Fast Ethernet switch with 24 switched 10BaseT/100BaseTX ports	$1,840	$3,680
1	8 port Switch Box	$1,142	$1,142
1	V700 Color Monitor	$342	$342
1	Monitor/Utility Shelf Kit	$111	$111
1	1U Keyboard Drawer	$235	$235
1	Rack Blanking Panel Kit (15U)	$45	$45
1	Compaq Rack Model 9142 (42U - Opal) - Flat Pallet	$1,332	$1,332
1	Side Panel Kit - 9142 Rack	$208	$208
1	Integrated Keyboard and Trackball (Opal)	$164	$164
4	APC MasterSwitch Plus	$525	$2,100
		SubTotal	**$68,929**
		Tax 7.1%	**$4,894**
		Total Hardware	**$73,823**

A. Development Costs -- Line 9 -- Year 00/01

Software		Unit Cost	Total
1	SmartStart 1-Year Subscription Service	$211	$211
6	Windows 2000 Advanced Server Licenses	$1,561	$9,366
2	Windows NT 4.x Server Licenses	$387	$774
2	VLA Proxy Server 2.0 License Microsoft	$455	$910
		SubTotal	**$11,261**
		Tax 7.1%	**$800**
		Total Software	**$12,060**

B. Connectivity Diagram



Appendix D: VPN Glossary

The following is a glossary of terms commonly found with Virtual Private Network technologies. It is provided for reference purposes only.

Address Hiding Refers to the firewall's practice of concealing the IP addresses of hosts behind the firewall. For outbound traffic the firewall, by default, substitutes its public IP address for the client's address in the source field of the packet. For inbound traffic the firewall, by default, substitutes its private IP address for the client's address in the source field of the packet.
Authentication Header (AH) Refers to a protocol, within the IPSec suite to authenticate IP data. The AH protocol is described in RFC 1826.
Application Program Interface (API) A standard method for programmers to access the features and functions of commercial software using custom-written routines that 'call' these services through the interfaces provided to the programmer.
Asymmetric key cryptography Defines the process where one key is used to encrypt a message and a second key is used to decrypt a message. The presence of key-pairs indicates the use of Asymmetric-key cryptography.
Authentication The process whereby a message recipient has confidence that the sender of a message is indeed whom the recipient believes they are. Authentication forces users to prove their identity before they can gain access to network resources.
Authorization (also called access control) The method of establishing access privileges for users. Access may be granted to all network resources, restricted to specific LAN segments, network servers, devices or applications.
Brute force attack Attempts to crack a cryptosystem by trying every combination of a key and subsequent inspection of the decryption process to determine if any sense can be made of it.
Certificate Authority (CA) Trusted parties who operate on the behalf of the corporation to manage the distribution and currency of X.509 digital certificates. Each layer in a Tree of Trust is represented by a well-defined Certificate Authority.
Certificate Chain An ordered group of digital certificates that are used to validate a specific certificate within the chain.
Certificate Practice Statement (CPS) A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.
Certificate Renewal The act of renewing certificates pending an expiration date to assure continued use for access.
Certificate Revocation The act of canceling a certificate in response to theft or suspected theft of the associated private key. Revocation is performed by the CA that issued the certificate, and once revoked, the serial number for the certificate will be placed on a Certificate Revocation list (CRL).
Certificate Revocation List (CRL) A mechanism that X.509 Public Key Infrastructures use to ensure that revoked certificates cannot be used for access or transacting.. CRLs contain revoked certificate serial numbers, their date of revocation, the date the CRL was generated, its

expiration date, issuer name, and serial number of the CA certificate used to sign it.
Certification The process of attesting to a person or resources proof of identity and right to use a X.509 certificate through the issuance of a signed certificate bearing the person's or resource's public key.
Ciphertext The output from an encryption algorithm after plaintext is passed through it.
Client A software program that requests the use of a network service. In this context, a browser is considered a client program. Often, client is used to refer to hosts (PCs, workstations) on which the client software runs.
Confidentiality Protecting private, personal, or sensitive information against attacks or disclosures.
Cryptanalysis The science (or art) of breaking a cryptosystem.
Cryptographic Key A series of data bits that are used to control a cryptographic process, such as encryption, decryption, or testing authentication of a message.
Cryptography The science (or art) or designing, building, and using cryptosystems.
Cryptology The umbrella study of cryptography and cryptanalysis.
Cryptoperiod The span of time where a given key is authorized for use or considered to be in effect.
Cryptosystem Refers to both the algorithm used in cryptography plus the means in which the algorithm is implemented.
Data Encryption Standard (DES) A 56-bit private-key algorithm that uses the block cipher method. Block cipher sends encrypted data to break the text into 64-bit blocks before transmitting it. DES is defined by the Federal Information Processing Standard (FIPS), 46-2 and published by the National Institute of Standards and Technology (NIST).
Dictionary Attack An attack on a cryptosystem using a dictionary of common possible keys. Brute force attacks on a key often start out with an attacker using the easiest keys first (English words and names, etc.).
Digital certificate A user's public key digitally signed by the certificate authority. The software sends the certificate with an encrypted message to verify the sender's identity. The recipient uses the CA's public key, which is widely publicized, to decrypt the sender's public key attached to the message. Then the sender's key is used to decrypt the message. Digital certificates bind a person’s identity with their public key, performed by a trusted party.
Digital Envelope When a digitally-signed message is further encrypted using the receiver’s public-key, the message is said to be contained in a digital envelope.
Digital Signature Created using PPK cryptography and message digests, encryption allows a message sender the ability to digitally sign messages, thus creating a digital signature for the message. When a message digest is computed then encrypted using the sender’s private key, and later appended to the message, the result is called the digital signature of the message.
Domain Name Service (DNS) The service that's used to translate Internet names, such as www.foo.com into IP addresses, and vice-versa.
Electronic Commerce Electronic forms of communication that permit the exchange of sale information related to goods and services purchasing between buyers and sellers.
Encapsulation Combines the uses of encryption and digital signatures to assure the highest degrees of message integrity and end entity authentication.
Encryption The hiding or masking of information through cryptography such that only those permitted can see through the disguise. Encryption assures that data in transit may only be read

by the intended recipient. Encryption uses a mathematical algorithm (cryptosystem) and a digital key to encode a message at one end of a transmission and then decode on at the other end.

Hash A mechanism to reduce a large domain of possible values into a smaller range of values. Hash values and message digests are created using hashing functions.

Internet Engineering Task Force (IETF) An open international community of network designers, operators, vendors and researchers concerned with the evolution of the Internet architecture and establishing Internet standards (RFCs)

Internet Key Exchange (IKE) Refers to the dynamic keying (Oakley) component of ISAKMP.

Integrity The function of ensuring the receiver that the data has not been tampered with by a third party en route. Integrity is also a quality metric that describes information and processes that are free of defects or errors

Interoperability The virtue of software products to work correctly with counterpart software produced by other developers with access to the same sets of specifications.

Internet Protocol (IP) is the standard protocol for sending information over the Internet. IP is also known as TCP/IP.

IP Security Protocol (IPSec) An IETF-developed security standard that defines data tunneling, authentication, and encryption using public networks, like the Internet. IPSec is detailed in Requests for Comments (RFCs) 1825-1829. Many vendors support the current version and plan to support the revised version when it is finalized.

Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley): is one of two public-key management schemes that the IPSec standard supports. ISAKMP/Oakley is actually a hybrid protocol, integrating ISAKMP with the Oakley key exchange scheme.

Internet Service Providers (ISP) deliver access to Internet resources for both remote users and enterprise servers via points of presence.(POPs)

Key-exchange certificate One type of digital certificate that's used to share the public key with those intending to send messages to the certificate owner. Contrast with Signature Certificate.

Layer 2 Forwarding (L2F) A tunneling protocol that Cisco Systems Inc. submitted to the IETF as a proposed standard. L2F transports link-layer frames such as Point-to-Point Protocol (PPP and operates at the data-link layer, which is layer 2 in the Open Systems Interconnection (OSI) model defined by the International Standards Organization (ISO). L2F is targeted at the ISP market.

Layer 2 Transport Protocol (L2TP) Combines the features of the L2F and PPTP protocols and permits tunneling of the link layer of PPP so that privately addressed IP, IPX and AppleTalk packets can be carried across the Internet. L2TP was put forward by Cisco Systems and Microsoft.

Layer 2 Tunneling Protocol (L2TP) Combines the features of the L2F and PPTP protocols and permits tunneling of the link layer of PPP so privately addressed IP, IPX and AppleTalk packets can be carried across the Internet. L2TP has been put forward by Cisco Systems and Microsoft, and it refers data security to the IPSEC Protocol.

MD5 authentication Verification of message integrity using Message Digest, Version 5, a hash function used to create digital signatures.

Message Authentication The process of authenticating that a message received came from the person whom the recipient believes to be the sender.

Message Digest A unique fingerprint of a message that's calculated based on the contents of the

message using a hashing algorithm. The original message cannot be recovered from the message digest, but is used to assure that no changes to the message took place while en route to the recipient.

Non-repudiation In the context of transactions, non repudiation is a legal term that dictates if a message is decryptable using a person's public key, the message MUST have originated with the holder of the private key. Under non-repudiation, a private key holder cannot deny that they signed the message if the decryption process succeeds.

Passwords The most basic security measure, which lacks the reliability of multi-factor authentication.

Plaintext The input to an encryption algorithm for the intent of producing ciphertext and the output from an decryption algorithm after ciphertext is passed through it.

Point of Presence (POP) Describes an ISP's premises, and provides access and egress for Internet traffic.

Point to Point Protocol (PPP) An implementation of TCP/IP that provides router-to-router and host-to-network connections.

Point-to-Point Tunneling Protocol (PPTP) Developed by Microsoft and several other remote access vendors to support tunneling of IP, IPX or NetBEUI protocols inside IP packets. PPTP was designed for PC-to-LAN remote access. PPTP is currently available for Windows NT servers and workstations and also for Windows 95 workstations through an upgrade.

Private Key The half of a key-pair that's retained on the computer, SmartCard, or token which generated the key pair. Private keys are used to encrypt messages that can be verified as legitimate if the associated public key is able to decrypt them.

Public Key Certificate See Digital Certificate.

Public Key Cryptography Standards (PKCS) A family of public-key cryptography standards used by SET which include:

• Certification request syntax describes the rules and sets of attributes needed for a certificate request from a Certificate Authority.

• Cryptographic message syntax describes how to apply cryptography to data, including digital signatures and digital envelopes

• Diffie-Hellman key agreements that define how two people, with no prior arrangements, can agree on a shared secret key that's known only between them and used for future encrypted communications.

• Extended certificate syntax permits the addition of extensions to standard X.509 digital certificates. These extensions add information such as certificate usage policies, other identifying information, etc.

• Password based encryption hides private keys when transferring them between computer systems, sometimes required under Public-Private Key Cryptography.

• Private-key information syntax describes how to include a private key along with algorithm information and a set of attributes to offer a simple way of establishing trust in information provided

• RSA encryption for the construction of digital signatures and digital envelopes.

Public key infrastructure (PKI) A policy that defines the uses of public key encryption for a specific organization. It describes the format of certificates and the functions of CAs in both the public and private sectors.

Public/private key pairs A required component for Public-Private Key (PPK) Cryptography

whereby two mathematically-related keys are used to encrypt and decrypt communications between two or more parties.
Quality of Service (QoS) The ability to define a level of performance in a network.
Random numbers Any number within a set of numbers that has an equal chance of being selected from the population, and its selection is considered unpredictable.
RC4 and RC5 encryption Algorithms developed by RSA Data Security that use a stream cipher method to encrypt a steady flow of data (bulk data).
Replay An attack in which a message is repeated over and over by either the true originator of the message or by an attacker posing as the originator.
Reserved Address Banks of IP addresses that are set aside for *intranet* uses. They are not registered to any network and are not routable across the Internet. RFC 1918 is the document that specifies the range of reserved addresses. Currently, this range is: 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 173.31.255.255, and 192.168.0.0 to 192.168.255.255.
Rivest, Shamir, Adelman (RSA) Cryptosystem A public-key cryptography system named after its inventors -- Rivest, Shamir, and Adelman.
Root Certificate The highest level in a Tree of Trust that's used to sign subordinate certificates..
Root Key Authority The managing organization that's responsible for the generation, maintenance, and distribution of root certificates.
Secondary DNS Server Refers to an authoritative DNS server that receives domain/zone information by requesting this information from the primary DNS server for the domain using a process known as a zone transfer.
Secret-key cryptography See Asymmetric Key Cryptography.
Secure Hash Algorithm (SHA-1) Used for hashing data (creating a message digest). It is defined by Federal Information Processing Standards 180-1.
Secure Socket Layer (SSL). A security protocol that sits on top of a reliable transport protocol to encapsulate other higher level protocols. The SSL Handshake Protocol authenticates the client and server to each other and enables them to decide upon an encryption algorithm and cryptographic keys before the higher level protocol sends or receives data.
Secure/Multipurpose Internet Mail Extensions (S/MIME) Based on technology from RSA Data Security, it offers another standard for electronic-mail encryption and digital signatures.
Security Association The IPSec mechanism for the management of authentication and encryption algorithms and their keys
Signature Certificate A type of a digital certificate that is used by the message recipient in authenticating the origin of a signed message. Contrasted with Key-Exchange Certificate.
Socks Version 5 An authenticated firewall traversal protocol that was designed to permit traffic to pass through only after the user who sent it has been authenticated to the system, rather than relying upon any specific characteristics of an IP packet to decide if access is permitted or not.
Security Parameter Index (SPI) Refers to the number that uniquely identifies an IPSec Security Association (SA). Specifically, the SPI is used to identify data integrity (authentication) and data privacy (encryption) algorithms, as well as the keys, used when handling IP traffic within the Security Association.
Symmetric key cryptography When the same shared, secret key is used to both encrypt and decrypt messages.
Token A credit card, keychain, or calculator sized computer or software program that has the

ability to authenticate users using a secret seed number that gives the token a uniqueness so it may be differentiated from other tokens.
Tree of Trust The hierarchy established to manage the issuance, maintenance, and currency of digital certificates.
Triple DES A procedure where the DES algorithm is used to encrypt the data three times.
Tunneling The process of encapsulating one data packet inside another. In a VPN, IP packets are encapsulated inside IPSec packets that are sent to gateways that are able to reconstruct them.
Virtual Address Used in describing service redirection, and refers to an additional IP address that is assigned to the firewall's outside network interface via routes on the Internet router
Virtual Private Network (VPN) A tunnel through the Internet that uses cryptography to hide the contents of messages as they traverse public networks. VPNs integrate private enterprise, semi-private extranet and public Internet access all over a single connection with less cost, greater capability and flexibility, and as much, if not more control than a private network.
X.509 Defines the most widely accepted format for digital certificates, as specified by the CCITT.

Appendix E: VPN Standards

The following is a list of pending IETF standards (RFCs), called Internet Drafts, that affect VPN- and PKI-related products, services, and protocols, as mentioned in Section 3 of this report.

These drafts are categorized as:

- Basic documents
- Authentication algorithms
- Cryptographic transforms
- Key management
- Other documents

The most current status of these documents are maintained in the libraries of the Internet Engineering Task Force (IETF) at:

http://www.ietf.org

IPSec Internet Drafts

The ESP Triple DES Transform

This document describes the 'Triple' DES-EDE3-CBC block cipher transform interface used with the IP Encapsulating Security Payload (ESP). It provides compatible migration from RFC-1851.

The ISAKMP Configuration Method

This document describes a new ISAKMP method that allows configuration items to be exchanged securely by using both push/acknowledge or request/reply paradigms.

The Use of HMAC-RIPEMD-160-96 within ESP and AH

This draft describes the use of the HMAC algorithm [RFC-2104] in conjunction with the RIPEMD-160 algorithm as an authentication mechanism within the revised IPSEC Encapsulating Security Payload and the revised IPSEC Authentication Header. HMAC with RIPEMD-160 provides data origin authentication and integrity protection

Dynamic configuration of IPSEC VPN host using DHCP

IPSEC is a protocol suite defined by IETF working group on IP security to secure communication at the network layer between communicating peers. Among many applications enabled by IPSEC, an interesting and useful application is connect a remote host (e.g., roaming user) to the intranet through SNG (or secure network gateway) using IPSEC tunnels. A remote host on the public internet would connect to a secure network gateway and then establish an IPSEC tunnel between itself and SNG.

Extended Authentication Within ISAKMP/Oakley

This document describes a method for using existing unidirectional authentication mechanisms such as RADIUS, SecurID, and OTP within IPSec's ISAKMP protocol.

A Hybrid Authentication Mode for IKE

This document describes a set of new authentication methods to be used within Phase 1 of the Internet Key Exchange (IKE). The proposed methods assume an asymmetry between the authenticating entities. One entity, typically an Edge Device (e.g. firewall), authenticates using standard public key techniques (in signature mode), while the other entity, typically a remote User, authenticates using challenge response techniques. These authentication methods are used to establish, at the end of Phase 1, an IKE SA which is unidirectional authenticated. To make this IKE bi-directional authenticated, this Phase 1 is immediately followed by an X-Auth Exchange. The X-Auth Exchange is used to authenticate the remote User. The use of these authentication methods is referred to as Hybrid mode. This proposal is designed to provide a solution for environments where a legacy authentication system exists, yet a full public key infrastructure is not deployed.

A Framework for Group Key Management for Multicast Security

This document provides a framework for group key management for multicast security, motivated by three main considerations, namely the multicast application, scalability and trust-relationships among entities. It introduces two planes corresponding to the network entities and functions important to multicasting and to security. The key management plane consists of two hierarchy-levels in the form of a single 'trunk region' (inter-region) and one or more 'leaf regions' (intra-region). The advantages of the framework among others are that it is scalable, it has reduced complexity and allows the independence in regions of group key management.

PKI Requirements for IP Security

The IP Security (IPsec) protocol set now being defined in the IETF uses public key cryptography for authentication in its key management protocol. This document defines the requirements that IPsec has for Public Key Infrastructure (PKI) protocols, formats, and services based on IETF PKIX (a/k/a X.509) certificate schemes.

Security Policy Specification Language

This document describes the Security Policy Specification Language (SPSL), a language designed to express security policies, security domains, and the entities that manage the policies and domains. The syntax and semantics of the language are presented here. SPSL currently supports policies for packet filtering, IP Security (IPSec), and ISAKMP exchanges, however, it may easily be extended to express other types of policies.

Intra-Domain Group Key Management Protocol

This document describes a protocol for intra-domain group key management for IP multicast security, based on the framework of [HCD98]. In order to support multicast groups, the domain is divided into a number of administratively-scoped 'areas'. A host-member of a multicast group is defined to reside within one (and only one) of these areas. The purpose of placing host-members in areas is to achieve flexible and efficient key management, particularly in the face of the problem of changes (joining, leaving, ejections) in the membership of a multicast group. A separate administratively-scoped area control-group is defined for each (data) multicast group, for the express purpose of key management and other control-message delivery.

Security Policy System

This document describes a distributed system that provides the mechanisms needed for discovering, accessing and processing security policy information of hosts, subnets or networks of a security domain. In this system policy clients and servers exchange information using the Security Policy Protocol. The protocol defines how the policy information is exchanged, processed, and protected by clients and servers. The system accommodates topology changes, hence policy changes, rather easily without the scalability constraints imposed by static reconfiguration of each client. The protocol is extensible and flexible. It allows the exchange of complex policy objects between clients and servers.

IPSec Monitoring MIB

This document defines low level monitoring and status MIBs for IPSec. It does not define MIBs that may be used for configuring IPSec implementations or for providing low-level diagnostic or debugging information. It assumes no specific use of IPSec. Further, it does not provide policy information. The purpose of the MIBs is to allow system administrators to determine operating conditions and perform system operational level monitoring of the IPSec portion of their network. Statistics are provided as well. Additionally, it may be used as the basis for application specific MIBs for specific uses of IPSec.

IPSec DOI Textual Conventions MIB

This memo defines textual conventions for use in monitoring, status, and configuration MIBs for IPSec. It includes a MIB module that defines those textual conventions.

Policy Framework for IP Security

As policy based networking has become a common place across the Internet with the advent of IPsec, firewalls and other initiatives, it is important for peering end nodes to understand where and why packets enroute are black-holed. End-to-end networking mandates that end nodes be cognizant of the impact policies along various points on the network will have on their packets. The objective of this document is to lay out a framework of policy requirements for end nodes. While the framework is focussed on IPSec based policies, it may be applicable across a wider policy base.

IPsec Interactions with ECN

IPsec supports secure communication over potentially insecure network components such as intermediate routers. Ipsec protocols support two operating modes, transport mode and tunnel mode. Explicit Congestion Notification (ECN) is an experimental addition to the IP architecture that provides indication of onset of congestion to delay- or loss- sensitive applications. ECN provides the congestion indication so as to enable adaptation to network conditions without the impact of dropped packets [RFC 2481]. Currently, the way ECN is specified does not conform to the manner in which IPsec tunnels are defined to be used. This document considers issues related to interactions between ECN and IPsec tunnel mode, and proposes two alternative solutions.

IKE Extensions Methods

This document describes the multiple extension methods of the ISAKMP [RFC 2408] and IKE [RFC-2409] protocols and how the older versions should respond when they receive such extensions. This document mainly tries to describe the best common practice of the extensions handling in ISAKMP [RFC-2408] and IKE [RFC-2409].

IPsec Policy Schema

This document presents an object-oriented model of IPsec policy in order to facilitate agreement about the content and semantics of IPsec policy and to enable derivations of task-specific representations of IPsec policy such as storage schema, distribution representations, and policy specification languages.

The Internet Key Exchange (IKE)

This memo describes a key exchange and security negotiation protocol which is intended to depricate [HC98]. As such it will not change the 'bits on the wire' for an implementation which is compiant with [HC98] but will clarify contentious issues with [HC98] and attempt to explain the protocol in a less haphazard manner. Due to advances in computer processing some mandatory-to-implement attributes have changed between this [HC98] and this document. In addition a new and optional exchange is introduced.

The ESP SKIPJACK-CBC Cipher Algorithm With Implicit IV

This protocol describes the SKIPJACK symmetric block cipher algorithm. The SKIPJACK algorithm is a confidentiality mechanism used, with other mechanisms, to provide secure messaging. This protocol describes the use of SKIPJACK in Cipher Block Chaining (CBC) mode with an Implicit IV within the context of the IP Encapsulating Security Payload [ESP].

Additional ECC Groups For IKE

This document describes new ECC groups for use in IKE [RFC2409] in addition to the Oakley groups included in RFC 2409. These groups are defined to align with other ECC implementations and standards, and in addition, some of them provide higher strength than the Oakley groups.

ISAKMP DOI-Independent Monitoring MIB

This document defines a DOI (domain of interpretation) independent monitoring MIB for ISAKMP. The purpose of this MIB is to be used as the basis for protocol specific MIBs that use ISAKMP as the basis for key exchanges or security association negotiation. As such, it has no DOI-dependent objects.

Content Requirements for ISAKMP Notify Messages

The ISAKMP and Domain Of Interpretation RFCs (RFC2408, RFC2407) specify error and status message types for use in ISAKMP NOTIFY messages, but in some cases do not specify that any additional clarifying data be carried in the messages. In these cases, it is difficult to determine which SA corresponds to the received NOTIFY message. While the DOI RFC specifies content and formats for additional data in the currently defined IPSEC status messages, no such requirements are currently specified for ISAKMP NOTIFY messages. This document provides content and format recommendations for those messages.

Security Policy Protocol

This document describes a protocol for discovering, accessing and processing security policy information of hosts, subnets or networks of a security domain. The Security Policy Protocol defines how the policy information is exchanged, processed, and protected by clients and servers. The protocol is extensible and flexible. It allows the exchange of complex policy objects between clients and servers.

IKE Base Mode

This document describes a new Phase I mode for IKE (RFC-2409) based on the ISAKMP (RFC-2408) Base Exchange. The purpose of this new exchange is to allow support of all authentication methods with fixed and non-fixed IP addresses, while offering protection against a denial of service attack aimed at costly operations. It also enables negotiation capabilities beyond those offered by Aggressive Mode. The exchange consists of only four messages and therefore is useful when performance is crucial.

X.509 Public Key Infrastructure Related Internet Drafts

Internet X.509 Public Key Infrastructure Representation of Elliptic Curve Digital Signature Algorithm (ECDSA) Keys and Signatures in Internet X.509 Public Key Infrastructure Certificates

This is the first draft of a profile for specification of Elliptic Curve Digital Signature Algorithm (ECDSA) keys in Internet Public Key Infrastructure X.509 certificates.

Certificate Management Messages over CMS

This document defines a Certificate Management protocol using CMS (CMC). This protocol addresses two immediate needs within the Internet PKI community: 1. The need for an interface to public key certification products and services based on [CMS] and [PKCS10], and 2. The need in [SMIMEV3] for a certificate enrollment protocol for DSA- signed certificates with Diffie-Hellman public keys. A small number of additional services are defined to supplement the core certificate request service. Throughout this specification the term CMS is used to refer to both [CMS] and [PKCS7]. For signedData the two specifications are equivalent. For envelopedData CMS is a superset of the PKCS7. In general, the use of PKCS7 in this document is aligned to the Cryptographic Message Syntax [CMS] that provides a superset of the PKCS7 syntax. The term CMC refers to this specification.

Internet X.509 Public Key Infrastructure Time Stamp Protocols

A time stamping service allows to prove that a datum existed before a particular time and can be used as a Trusted Third Party (TTP) as one component in building reliable non-repudiation services (see [ISONR]). This document describes the format of a request sent to a Time Stamping Authority (TSA) and of the response that is returned. An example on how to prove that a digital signature was generated during the validity period of the corresponding public key certificate is given in an annex. In order to get additional confidence about the information returned by the TSA, an optional Temporal Data Authority (TDA) can add data to the response that proves in addition that a datum existed before a particular unpredictable event.

Internet X.509 Public Key Infrastructure Data Certification Server Protocols

This document describes a general data certification service and the protocols to be used when communicating with it. The Data Certification Server is a Trusted Third Party (TTP) that can be used as one component in building reliable non-repudiation services (see [ISONR]). Useful Data Certification Server responsibilities in a PKI are to validate signatures and to provide up-to-date information regarding the status of public key certificates. We give examples of how to use the Data Certification Server to extend the lifetime of a signature beyond key expiry or revocation and to query the Data Certification Server regarding the status of a public key certificate.

Internet X.509 Public Key Infrastructure PKIX Roadmap

This document provides an overview or 'roadmap' of the work done by the IETF PKIX working group. It describes some of the terminology used in the working group's documents, and the theory behind an X.509-based PKI. It identifies each document developed by the PKIX working group, and describes the relationships among the various documents. It also provides advice to would-be PKIX implementors about some of the issues discussed at length during PKIX development, in hopes of making it easier to build implementations that will actually interoperate.

Internet X.509 Public Key Infrastructure Qualified Certificates

This Internet-Draft forms a certificate profile for Qualified Certificates, based on RFC 2459, for use in the Internet. The term Qualified Certificate is used to describe a certificate with a certain qualified status within applicable governing law. Further Qualified Certificates are issued exclusively to physical persons represented by a registered unmistakable identity. The goal of this document is to define a general syntax independent of local legal requirements. The profile is however designed to allow further profiling in order to meet specific local needs.

Diffie-Hellman Proof-of-Possession Algorithms

This document describes two methods for producing a signature from a Diffie-Hellman key pair. This behavior is needed for such operations as creating a signature of a PKCS #10 certification request. These algorithms are designed to provide a proof-of- possession rather than general purpose signing.

An Internet AttributeCertificate Profile for Authorization

Authorization support is required for various Internet protocols, for example, TLS, CMS and their consumers, and others. The X.509 AttributeCertificate provides a structure that can form the basis for such services. This specification defines two profiles (basic and proxiable) for the use of X.509 AttributeCertificates to provide such authorization services.

Basic Event Representation Token v1

More and more, standards agencies that use PKI technologies developed and promulgated through the efforts of the IETF have come to ask for a finite method of representing a discrete instant in time as a referable event. The present document establishes defined data structures for requesting a Basic Event Representation Token (BERT), after it has been issued by a Trusted Timebase provider.

Internet X.509 Public Key Infrastructure Extending Trust In Non-repudiation Tokens In Time

This document describes a way to maintain the trust in a token issued by a non-repudiation Trusted Third Party after the key initially used to establish trust in the token expires.

Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv3

This document describes the features of the Lightweight Directory Access Protocol v3 that are needed in order to support a public key infrastructure based on X.509 certificates and CRLs.

Simple Certificate Validation Protocol (SCVP)

The SCVP protocol allows a client to offload certificate handling to a server. The server can give a variety of valuable information about the certificate, such as whether or not the certificate is

valid, a chain to a trusted root, and so on.

Using HTTP as a Transport Protocol for CMP

This document describes how to layer [CMP] over [HTTP]. A simple method for doing so is described in section 5.4 of [CMP], but that method does not accommodate a polling mechanism, which may be required in some environments. This document specifies an alternative method which uses the polling protocol defined in section 5.2 of [CMP]. A new Content-Type for messages is also defined.

Appendix F: Internet References

Following a list of 10 Internet sites dedicated to supplying up-to-date information about Virtual Private Network technologies.

VPN Source Page at Internet Week Online

Internet Week, a CMP publication, is a trade journal for IT professionals. The Internet Week print edition has extensive coverage on VPN technologies, VPN uses, and late breaking news articles. The print edition has supplemental information at the Internet Week Web site (naturally), where they also offer the VPN Source Page. You can visit their site at:
`www.internetwk.com/VPN/default.html`

Once you're there, you'll find educational resources for people interested in VPNs and lots of on-going discussions about VPN issues.
The VPN Source Page features:

* Weekly summaries of VPN news
* VPN vendor sources page with links to vendor sites
* References to InternetWeek articles
* Links to VPN white papers
* VPN frequently asked questions
* Schedule of VPN-related events and trade shows

Network World Fusion VPN Information Site

Network World is a thorough resource for news and information on networking and data communications. The Network World Fusion Web site supplements the print edition and contains a section dedicated to VPNs. You'll need to register for the Fusion site before you're permitted to access it. You can find the registration form (it's free) at:
`www.networkworld.com/netresources/vpn.html`

Once you register, receive your acknowledgement, and log-in, you can visit the VPN information section at:
`www.nwfusion.com/xlogin.html`

Inside the site you'll find:

- VPN audio primer
- VPN roundtable
- Reviews and buyer's guides
- Building your own VPN

- Telecommunication carrier services

The NIST IPSec Project Home Page

Information about the IPSec project from the National Institute of Standards and Technology (NIST) to promote IPSec and help with interoperability testing using the IPSec-WIT tester. The NIST IPsec Project is concerned with providing authentication, integrity and confidentiality security services at the Internet (IP) Layer, for both the current IP protocol (IPv4) and the next generation IP protocol (IPv6). For additional information about the IPSec reference implementation for Linux (Cerberus), and the reference implementation of IPsec key negotiation and management specifications (PlutoPlus), as well as more detail about the IPSec-WIT tester, visit them at:

```
csrc.nist.gov/ipsec/
```

International Computer Security Association (ICSA) Library

Information about the International Computer Security Association (ICSA) services for IPSec product testing and certification. ICSA is also a popular source for information and security assurance services to IT professionals around the world. ICSA collects information from security product manufacturers, developers, security experts, academia and corporations to promote commercial computer security products, policies, techniques and procedures. To access the library of information they maintain, visit:

```
http://www.icsa.net/library/
```

Once you're at the ICSA Library, you'll find rich collections of information on multiple topic affecting computer security, including:

- Authentication
- Cryptography
- General security
- Malicious code
- Network security
- Physical security
- Policies
- White papers

ICSA IPSec Certification Program

For additional details about the IPSec Certification Programs visit their online section at:

```
www.icsa.net/services/product_cert/ipsec/
```

EarthWeb CrossNodes Technologies Information Resources

The EarthWeb family of Web sites are among the premiere sources of information for IT

professionals. Their CrossNodes Technologies Information Resource maintains terrific coverage of VPNs and related technology. You can visit CrossNodes at:
`www.crossnodes.com/tech/dir.tech.infr.vpn1.html`

Inside the site you'll find:
- Discussions
- Articles
- Events
- Software
- Books for Sale
- Training
- Hardware
- Online Books
- Job Listings
- Auctions

VPN Insider

The VPN Insider is another invaluable information resource on VPN products and services. You can visit their Web site at:
`http://www.vpninsider.com/`

At the site, you'll find useful collections that include:
- Forums dedicated to the VPN community.
- VPN-related hotlinks
- Updated VPN vendor information.
- VPN White Papers and tutorials.
- VPN job opportunities

VPDN.com

VPDN.com touts itself as a *one-stop shop* on the Web for all things VPN. They focus on Virtual Private Networking products and services, Internet security, directory services and networked applications. Their site is maintained by TeleChoice, Inc. and is updated daily with VPN news and commentary to help you stay current.
Access to the site requires registration. You can find them at:

```
www.vpdn.com/home.asp
```

The ISPortal

ISPortal was built from the feedback of vendors, ISP's, and corporate network managers across the world. Vendors supply information through sponsorship opportunities for the posting of white papers, press releases, inclusion of their products in an interactive buyers guide, and running banner ads. Their VPN information resources will help you to see VPNs from several different angles and points of view.
ISPortal primarily serves the interest of:

- ISP's
- IT Managers
- Systems Engineers
- Network Administrators

Visit their Web site at:

```
http://www.isportal.com/vpn/resources.htm
```

Electronic Privacy Information Center (EPIC)

The site for information about The Electronic Privacy Information Center (EPIC) study that finds international export restrictions on cryptography remains a major obstacle to the use of encryption. For more information about other studies on cryptography regulations, visit the EPIC Web site:

```
www.epic.org
```

Besides their reports, you'll also find links for:

- Latest News
- Resources
- Policy Archives
- About EPIC
- Search epic.org
- Visiting the EPIC Bookstore
- Subscribing to the EPIC Alert
- Supporting EPIC

VPN Operator's Home Page

This Web site from Japan is primarily of interest to operators of VPN and PKI-based systems. You can find the VPN Operator's Web site at:

```
sh.note.iri.co.jp/vpnops/index.en.html
```

Inside the site you'll find:

- VPN technical documents
- VPN service and solution links
- VPN hardware vendors
- VPN firewall vendors (Firewall)
- VPN client-server and software vendors
- VPN Operator Mailing List subscription form (it's free)

Appendix G: A VPN Reader's Guide

Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition

by Bruce Schneier
John Wiley & Sons
ISBN: 0471117099

Bruce Schneier's Applied Cryptography: Protocols, Algorithms, and Source Code in C offers an authoritative introduction to the field of cryptography, suitable for both the specialist and the general reader. The book adopts an encyclopedic approach to cryptographic systems throughout history, from ciphers to public key cryptography. Schneier also outlines cryptographic protocols--the steps required for secure encryption--with the precision of a chess master.

Readable, instructive, and truly exhaustive, this text is a must for anyone wanting a solid introduction to the field in a single volume. Applied Cryptography presents the source code for most algorithms and other procedures in C rather than using pure math. The book also includes source code for the Data Encryption Standard (DES) and other algorithms, but readers don't need to know programming to benefit from this text. With a truly comprehensive bibliography of over 1,600 entries, Applied Cryptography provides the reader with plenty of sources for more information.

Building Internet Firewalls

by D. Brent Chapman, Elizabeth D. Zwicky, Deborah Russell (Editor)
O'Reilly & Associates
ISBN: 1565921240
Building Internet Firewalls is a practical guide to building firewalls on the Internet. If your site is connected to the Internet, or if you're considering getting connected, you need this book. It describes a variety of firewall approaches and architectures and discusses how you can build packet filtering and proxying solutions at your site. It also contains a full discussion of how to configure Internet services (e.g., FTP, SMTP, Telnet) to work with a firewall. The book also includes a complete list of resources, including the location of many publicly available firewall construction tools.

Building SET Applications for Secure Transactions

by Mark S. Merkow, Jim Breithaupt, Ken Wheeler
John Wiley & Sons
ISBN: 0471283053

The authors of Building SET Applications for Secure Transactions show you why the Secure Electronic Transaction (SET) standard makes secure e-commerce a reality. This wide-ranging text informs Information Systems (IS) managers what SET is, how it works, and how to implement a secure commerce system on their Web sites. The book's strength is its wide-ranging perspective on e-commerce and how it fits into traditional business systems. Several chapters provide checklists for the IS manager considering the move toward the Web for commerce.

Analyzing and designing, planning for security, and testing are just some of the issues that must be faced when implementing a successful e-business. Clearly, SET is not a magic bullet against fraud, but the authors show why the future of electronic commerce is bright.

Computer Communications Security : Principles, Standard Protocols and Techniques

by Warwick Ford
Prentice Hall
ISBN: 0137994532

This book identifies and explains all the modern standardized methods of achieving network security in both TCP/IP and OSI environments -- with a focus on inter-system, as opposed to intra- system, security functions. Part I is a technical tutorial introduction to computer network security; Part II describes security standards, protocols and techniques. It covers such topics as cryptography, authentication, access control, and non-repudiation; describes a wide range of standard security protocols and techniques, drawn from international, national, government, and Internet standards; and considers areas such as network and transport layer security, local area network security, security management, and security for applications such as electronic mail, directory services, EDI, and banking.

Computer Networks: Protocols, Standards and Interface

by Uyless D. Black
Prentice Hall
ISBN: 0131756052

Offers a succinct tutorial on the major types of networks in use today for anyone involved in programming or purchasing. Each chapter describes a major computer network technology and covers the latest developments and specific protocols. Written for a wide audience; electronic engineering or math background is not necessary.

E-Commerce Security : Weak Links, Best Defenses

by Anup K. Ghosh
John Wiley & Sons
ISBN: 0471192236

Online security investigator and research scientist Anup Ghosh takes a realistic look at the state of security for electronic commerce. He is neither a Pollyanna believing that all is fine, nor a doomsayer predicting catastrophe for transactions lacking virtual plate armor. In fact, he feels that some levels of security are excessive. But he emphasizes that any security system is only as strong as its weakest point. If you're going to trust your money to online transactions, you need to know where your weaknesses lie and how to correct them.

To that end, Ghosh discusses real-life security failures, how they occurred, and how recurrences can be prevented. He then takes a systematic look at the areas of risk. One chapter deals with potential problems in active Web content, such as Java applets, ActiveX controls, and push

technology. He examines data protocols to secure transactions with the warning that the data can be vulnerable before and after the secure transmission. The weaknesses of server hardware and software come under scrutiny as well. Ghosh calls for greater attention to security as software is being developed and looks at what advances are likely to be coming down the road.

Hacking Exposed: Network Security Secrets and Solutions

by Stuart McClure, Joel Scambray, George Kurtz
Computing McGraw-Hill
ISBN: 0072121270

Whenever Hollywood does a movie in which someone breaks into a computer, the hacking scenes are completely laughable to anyone who knows the first thing about computer security. Think of Hacking Exposed: Network Security Secrets and Solutions as a computer thriller for people with a clue. This is a technical book, certainly--URLs, procedures, and bits of advice take the place of plot and characters--but the information about hackers' tools will leave you wondering exactly how vulnerable your system is. More to the point, the explicit instructions for stealing supposedly secure information (a Windows NT machine's Security Access Manager file, for example) will leave you absolutely certain that your computers have gaping holes in their armor.

The book describes the security characteristics of several computer-industry pillars, including Windows NT, Unix, Novell NetWare, and certain firewalls. It also explains what sorts of attacks against these systems are feasible, which are popular, and what tools exist to make them easier. The authors walk the reader through numerous attacks, explaining exactly what attackers want, how they defeat the relevant security features, and what they do once they've achieved their goal. In what might be called after-action reports, countermeasures that can help steer bad buys toward less-well-defended prey are explained.

ICSA Guide to Cryptography

by Randall K. Nichols
McGraw Hill Text
ISBN: 0079137598

Provides a survey of the principles and practice of cryptography with respect to business applications and, more specifically, commercial computer systems. The business value gained from implementation of cryptographic countermeasures is discussed. Other issues covered include processes, protocols, key management, implementation mistakes, and product certification. The CD-ROM contains a variety of papers and materials regarding cryptography and cryptographic products.

Intrusion Detection : Network Security Beyond the Firewall

by Terry Escamilla
John Wiley & Sons
ISBN: 0471290009

This superior text on computer security is extremely rich in information, based on experience, and a pleasure to read. In addition, the author is donating part of his royalties from this book to various charities--initially, a foundation that fights child abuse.

Escamilla begins by exploring intrusion prevention systems--firewalls, user authentication routines, and access controls--and telling how to properly set up such systems. He then describes mechanisms that identify and minimize damage caused by electronic break-ins once they occur. The author covers both system-level and network-level intrusion-detection systems, describing tools that attempt to catch not only outsiders who have broken in, but also legitimate system users who are up to no good.

Escamilla details several anti-intruder tools, including packet sniffers and vulnerability scanners. He describes a lot of Unix hacks and tells what you can do to prevent them from taking place on your systems. Other chapters focus on intrusions in Windows NT environments and what to do when your system is under attack. Escamilla closes with
references to other sources.

Maximum Security : A Hacker's Guide to Protecting Your Internet Site and Network

By: Anonymous
Sams Publishing
ISBN: 0672313413

This book is written for system administrators who need to know how to keep their systems secure from unauthorized use. The anonymous author takes a hacker's view of various systems, focusing on how the system can be cracked and how you can secure the vulnerable areas.

The book makes it clear from the outset that you cannot rely on commercial software for security. Some of it is flawed, and even the best of it has to be used correctly to provide even the most basic security measures. The author scrutinizes such operating systems as Microsoft Windows, Unix, Novell, and Macintosh. He details many of the tools crackers use to attack the system, including several that have legitimate uses for system administration. Rather than merely cataloging areas of risk and showing how various flaws can be exploited, the author makes every effort to show how security holes can be avoided and remedied. Maximum Security tells you which software to avoid and then details which security tools are invaluable, providing the URLs necessary to acquire them. An enclosed CD-ROM provides links to many of the tools and resources discussed in the book. The CD-ROM also leads you to several online documents where you can learn more about Internet security in general and specifics for securing your own site.

Security Issues for the Internet and the World Wide Web

by Debra Cameron
Computer Technology Research Corporation
ISBN: 156607973X

A report designed to assist management in deciding how to address the issue of Internet security

and to determine what security approaches are appropriate to a given organization. An executive summary is followed by chapters addressing Internet security risks, encryption technology, digital signatures and authentication, creating a shield for corporate systems (firewalls), security scanners and other approaches, transaction security for electronic commerce, security for the Web and other information services, and developing security policies and procedures. Includes several appendices, including Internet resources for security administrators and a CERT incident report form, a bibliography, and an extensive glossary of terms.

Virtual Private Networks for Dummies

By Mark Merkow
IDG Books Worldwide
ISBN: 0764505904

Virtual private networks let you create a secure business network over the Internet - and avoid the expense of dedicated access lines. This friendly guide walks you through this complex technology and leads you to a VPN solution that's just right for your business.

U.S. Department
of Transportation
**Federal Highway
Administration**

Memorandum

**6300 Georgetown Pike
McLean, VA 22101-2296**

Subject: ACTION: Commitment of SP&R Funds for FY2001
National Cooperative Highway Research Program
(Reply Due: February 28, 2001)

Date: January 16, 2001

From: Dennis C. Judycki /original signed by/
Director of Research, Development, and Technology

Reply to
Attn. of: HRPD-1

To: Division Administrators

I have attached a spreadsheet showing State Planning and Research (SP&R) apportionments and the National Highway Cooperative Research Program (NCHRP) contribution amounts for fiscal year 2001. Please work with your States to process the agreement for the authorization of funds. We would like all of the agreements (Form PR 2.1) signed, and the information entered into the Fiscal Management Information System (FMIS) by February 28, 2001. Be sure to use project number 0004201 for FMIS entries. The project number for the fiscal year 2001 NCHRP is SPR-4(201) and should be entered in space 2 of the Form PR 2.1.

It is important to note that once these funds are obligated, the project should not be closed in your State until formal notification has been received from the Office of Budget and Finance. We are having problems closing out several of the older NCHRP projects because several States withdrew funds prior to the projects being closed. If your State has prematurely closed one of the NCHRP projects, please try to get the project re-opened so we can pay the final invoices and formally close the projects. For our part, we will work to ensure that NCHRP invoices are paid promptly and projects can be closed on a timelier basis.

We will rely primarily on the data entered in FMIS for our information on the contributions made for NCHRP. However, since in the past some States have contributed by check or used other than SP&R funds for their contributions, we ask that you provide a copy of the Form PR 2.1 or an e-mail note to Mr. William Zaccagnino if your State uses funds other than appropriation codes Q55 or Q56.

Thank you and your staff in advance for your efforts in obligating the fiscal year 2001 NCHRP funds. You may contact Mr. Zaccagnino by e-mail or at 202-493-3183 if you have any questions.

2 Attachments

cc: Dr. Robert Reilly (TRB)
Directors of Field Services
Resource Center Managers

U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL HIGHWAY ADMINISTRATION
FEDERAL-AID PROJECT AGREEMENT
(National Cooperative Highway Research Program)

1. STATE

2. PROJECT NUMBER
SPR-4(201)

SECTION 1-AGREEMENT PROVISIONS

In conformance with arrangements for financing the National Cooperative Highway Research Program, hereinafter referred to as the "NCHRP," pursuant to the Memorandum Agreement effective October 1, 1988 as amended, between the Federal Highway Administration, hereinafter referred to as "FHWA," the American Association of State Highway and Transportation Officials, hereinafter referred to as "AASHTO," and the National Academies, hereinafter referred to as the "Academy"; the State formally consents to providing the funds stated in this agreement as its contribution towards financing expenditures incurred in conducting the NCHRP in accordance with the Memorandum Agreement.

In accordance with the action taken by AASHTO requesting the Academy, through its Transportation Research Board to administer the NCHRP, the State authorizes FHWA to charge the States=s pro rata share of the costs incurred against the funds stated in this agreement.

It is understood that FHWA will make payments to the Academy for the State=s share of the cost of the program pursuant to the State-Academy Agreement for the current fiscal year and the Fiscal Agreement entered into between the FHWA on July 1, 1962.

In the event the State=s contribution towards the cost of the NCHRP is to be financed with both Federal-aid funds and State-matching funds, the State agrees to advance the FHWA the State-matching funds for its share of the estimated cost.

SECTION IIBFUNDS

3. ESTIMATED TOTAL COST OF PROJECT	4. FEDERAL FUNDS	5. EFFECTIVE DATE OF AUTHORIZATION

SECTION IIIBAGREEMENT AND SIGNATURES

The State, through its Highway Agency, and the Federal Highway Administration agree to the above provisions.

_____
(Official Name of the Highway Agency)

U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL HIGHWAY ADMINISTRATION

BY _____
(Title)

BY _____
(Title)

BY _____
(Title)

_____
Date Executed

BY _____
(Title

Form PR 2.1

FISCAL YEAR 2001					
			Remaining Available		
State	SPR	25% RD&T2	For SPR	NCHRP	
Alabama	$10,270,562	$2,567,641	$7,702,922	$564,881	
Alaska	$6,760,406	$1,690,102	$5,070,305	$371,822	
Arizona	$9,989,102	$2,497,276	$7,491,827	$549,401	
Arkansas	$7,335,479	$1,833,870	$5,501,609	$403,451	
California	$50,286,824	$12,571,706	$37,715,118	$2,765,775	
Colorado	$6,713,666	$1,678,417	$5,035,250	$369,252	
Connecticut	$8,468,287	$2,117,072	$6,351,215	$465,756	
Delaware	$2,542,102	$635,526	$1,906,577	$139,816	
Dist. of Col.	$2,231,520	$557,880	$1,673,640	$122,734	
Florida	$27,302,997	$6,825,749	$20,477,248	$1,501,665	
Georgia	$19,640,764	$4,910,191	$14,730,573	$1,080,242	
Hawaii	$2,891,287	$722,822	$2,168,465	$159,021	
Idaho	$4,187,427	$1,046,857	$3,140,570	$230,308	
Illinois	$18,549,432	$4,637,358	$13,912,074	$1,020,219	
Indiana	$13,862,164	$3,465,541	$10,396,623	$762,419	
Iowa	$6,775,595	$1,693,899	$5,081,696	$372,658	
Kansas	$6,518,777	$1,629,694	$4,889,083	$358,533	
Kentucky	$9,325,003	$2,331,251	$6,993,752	$512,875	
Louisiana	$8,893,001	$2,223,250	$6,669,751	$489,115	
Maine	$2,989,547	$747,387	$2,242,160	$164,425	
Maryland	$8,816,395	$2,204,099	$6,612,296	$484,902	
Massachusetts	$10,186,705	$2,546,676	$7,640,029	$560,269	
Michigan	$18,153,944	$4,538,486	$13,615,458	$998,467	
Minnesota	$8,180,431	$2,045,108	$6,135,323	$449,924	
Mississippi	$6,620,582	$1,655,146	$4,965,437	$364,132	
Missouri	$13,286,108	$3,321,527	$9,964,581	$730,736	
Montana	$5,735,180	$1,433,795	$4,301,385	$315,435	
Nebraska	$4,460,672	$1,115,168	$3,345,504	$245,337	
Nevada	$4,168,312	$1,042,078	$3,126,234	$229,257	
New Hampshire	$2,838,185	$709,546	$2,128,639	$156,100	
New Jersey	$14,834,907	$3,708,727	$11,126,180	$815,920	
New Mexico	$5,485,853	$1,371,463	$4,114,390	$301,722	
New York	$27,991,939	$6,997,985	$20,993,954	$1,539,557	
North Carolina	$15,508,685	$3,877,171	$11,631,514	$852,978	
North Dakota	$3,782,193	$945,548	$2,836,645	$208,021	
Ohio	$18,536,527	$4,634,132	$13,902,395	$1,019,509	
Oklahoma	$8,482,865	$2,120,716	$6,362,149	$466,558	
Oregon	$6,671,822	$1,667,956	$5,003,867	$366,950	
Pennsylvania	$24,815,400	$6,203,850	$18,611,550	$1,364,847	
Rhode Island	$3,431,995	$857,999	$2,573,996	$188,760	
South Carolina	$9,617,917	$2,404,479	$7,213,438	$528,985	
South Dakota	$4,000,528	$1,000,132	$3,000,396	$220,029	
Tennessee	$11,664,961	$2,916,240	$8,748,721	$641,573	
Texas	$43,111,261	$10,777,815	$32,333,446	$2,371,119	
Utah	$4,359,588	$1,089,897	$3,269,691	$239,777	
Vermont	$2,587,234	$646,809	$1,940,426	$142,298	
Virginia	$14,369,987	$3,592,497	$10,777,490	$790,349	
Washington	$9,905,691	$2,476,423	$7,429,268	$544,813	
West Virginia	$4,661,921	$1,165,480	$3,496,441	$256,406	
Wisconsin	$11,162,733	$2,790,683	$8,372,050	$613,950	
Wyoming	$3,955,337	$988,834	$2,966,503	$217,544	
Subtotal	$556,919,800	$139,229,950	$417,689,850	$30,630,589	

John Semmens

From: Gabriel Roth [roths@earthlink.net]
Sent: Thursday, March 01, 2001 7:51 AM
To: Mr. John Semmens
Subject: Fwd: Re: Comments on Semmens investment chapter

John, herewith, for your information only, my first impressions of your investment chapter. Further response to follow.

G.

>Date: Thu, 1 Mar 2001 09:48:51 -0500
>To: Alex Tabarrok <ATabarrok@independent.org>
>From: Gabriel Roth <roths@earthlink.net>
>Subject: Re: Comments on Semmens investment chapter
>Cc:
>Bcc: "Ÿ: 2001 E-mails: Work:Book on roads"
>X-Attachments:
>
>Alex -
>
>I've now read the Semmens investment chapter and, on the whole, find
>it a good review of the weaknesses of present road financing
>systems, and of the case for privatization. I have some comments on
>minor matters with which I need not trouble you now, and I think
>there is some repetition that could be trimmed.
>
>His pricing regime is based on average costing for rural areas, with
>property owners having to bear the costs of little-used access
>roads. He mentions automated toll collection, and its use in
>congested areas. [Incidentally, my daughter, Diana Furchtgott-Roth,
>drafted much of the 1992 Executive Order mentioned on page 35.] John
>avoids complications such as "increasing" and "decreasing" returns
>in the provision of roads, but I expect that to be part of the
>Mohring chapter. Nor does he spend much time on political
>difficulties.
>
>It is noteworthy that Semmens goes straight for privatization,
>without dwelling on the intermediate stage of commercialization, as
>done by weaker souls.
>
>I think this could form an excellent first chapter - after my
>"Introduction" - and a good foil for some of the ones to follow,
>especially Levinson's, which tackle special problems.
>
>What do you think?
>
>Gabriel

--

****

Roths can also be reached at:

4815 Falstone Avenue
Chevy Chase, Maryland
USA 20815

Voice: 1 301 656 6094
Fax : 1 202 318 2431