ADOT Uses for Virtual Private Networking Technology: Phase 2 – Final Test Report

Final Report 502(2)

Prepared by:
Mark Merkow, CCP, 1216 East Commodore, Tempe, Arizona 85283
Rich Nacinovich & Nicole Drew, Arizona Department of Transportation, 206 S. 17th Ave., Phoenix, AZ 85007

February 2002

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

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-AZ-00-502(2)		

4. Title and Subtitle	5. Report Date
ADOT Uses for Virtual Private Networking Technology: Phase 2 – Final Test Report	February 2002
	6. Performing Organization Code

7. Authors	8. Performing Organization Report No.
Mark Merkow, CCP, CISSP, Rich Nacinovich & Nicole Drew	

9. Performing Organization Name and Address	10. Work Unit No.
Merkow Consulting, 1216 East Commodore, Tempe, Arizona 85283 Rich Nacinovich & Nicole Drew, Arizona Department of Transportation, 206 S. 17th Ave., Phoenix, AZ 85007	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

Prepared in cooperation with the U.S. Department of Transportation, Federal Highway Administration

16. Abstract

This phase of the project includes the final report and recommendations following field-testing Virtual Private Network (VPN) technology by ADOT, and especially by the Motor Vehicles Division (MVD) of ADOT.

This final report embodies the results of preliminary and field testing by remote access ADOT employees, third-party and external government agencies to help assess the long-term 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	74	

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

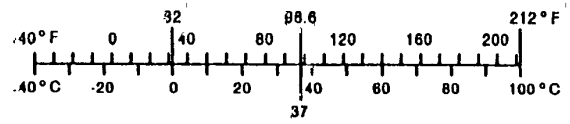


TABLE OF CONTENTS

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 to a variety of internal ADOT employees, third-party businesses and government entities who access ADOT systems remotely.

Phase 2 concluded after sufficient testing time elapsed and sufficient data was collected for meaningful analysis and for developing a recommendation.

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 specifically for 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. ADOT however, still benefits internally by using VPN technology to 1) reduce the expenses related to long-distance and toll calls; 2) simplify network architectures with smaller growth in establishing dedicated external links.

From the results gained by the study and from the levels of satisfaction expressed by the users, VPNs are a viable option for ADOT to offer both remote access and LAN-to-LAN connectivity to ADOT systems and information resources, and are recommended for full roll-out to all appropriate parties.

1.Introduction and Objectives

1.1. Objectives of the Study

The goal of this study is to determine the effectiveness, appropriateness of the security, and potential cost reductions that have proven themselves when Virtual Private Networking technology and services are in use.

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.

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 local telecommunications carriers 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. Due to Lata and facilities restriction telecomm carriers cannot always provide service to remote locations. ADOT customers that travel frequently and must connect to the ADOT network are incurring excessive long distance charges.

The solution should provide a reliable and secure connection to ADOT network using low cost public networks. This solution should support internal and external customers that have a business need. This project will analyze and test industry standards of VPN technology to determine best the solution for ADOT.

Expected Deliverables

- 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.

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 by MVD as well as throughout the ADOT agency.

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:

1. Wide Area Network (WAN) development and support required additional dedicated links or satellite communications to attain the high availability that's required.
2. 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

1. Unreasonably long lead times to install and test new communication links
2. Finger pointing among users, telcos, and equipment providers as communication problems arose
3. Skyrocketing support and management costs
4. Increased complexity in all aspects of hardware, software, and dependence on multiple service providers
5. 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

1. Point-to-Point Tunneling Protocol (PPTP)
2. Layer 2 Forwarding (L2F)
3. Layer 2 Tunneling Protocol (L2TP; combining PPTP and L2F)
4. 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, leaving it vulnerable to attacks. These concerns were later remedied, and today's Windows 2000 Server Edition offer an off-the-shelf implementation of PPTP that's proven and reliable.

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

1. Asynchronous Transfer Mode (ATM)
2. 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

1. Support for both UNIX and NT systems
2. 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:

1. 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.) ADOT has tested this method during field-testing.

2. Branch office networks to eliminate the costs associated with dedicated leased-lines and to build new branch office connections ad-hoc if needed. ADOT has also tested this method on a limited rollout basis using the Phoenix City Prosecutors Office.
3. Extranets to connect partners, suppliers, users, and providers without the expensive overhead of leased lines or controlled modem access. This method would prove useful to ADOT for converting or accelerating the rollout of 3rd party processors who offer MVD services to the public but are not staffed using ADOT personnel.

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:

1) Uses low-cost ISPs instead of long-distance phone access and costs
2) Reduces network complexity and support costs
3) Network help desk calls are serviced by managed ISP rather than internal support channels
4) 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:

3. Elimination of 56KB and other dedicated leased lines
4. Elimination of SNA coax controllers by replacing them with pooled Logical Units (LUs) as needed by users.
5. Replacement of PCs using thin client technology
6. Bridge between departmental or organizational Intranets
7. 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:

1. Motor Vehicle Records
2. Mandatory insurance
3. Court convictions and warrants
4. Abandoned vehicles and towed vehicle records
5. Fleet processing at the point of information origination
6. License plate processing
7. Emissions data
8. Financing and insurance records
9. Electronic vehicle tittles and liens
10. 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 or directly on the MVD Web site. Some of these functions include:

1. MVD policies and procedures available via the Internet
2. Ordering special plates
3. Access to motor vehicle records for both drivers and vehicles
4. Ordering duplicate copies of registration information
5. Sold notices
6. Applications and other common forms
7. Personalized license plate inquiries for availability
8. 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.

4. **Internal ADOT Customers**

All internal customers located outside of the Phoenix metro area where dedicated connections are not available must incur long distance charges to connect to the ADOT network. VPN is also a great solution for traveling employees. VPN allows customers to connect through a local ISP provider at a much lower rate.

In June 2000, Craig Stender, CIO of Information Technology Group at ADOT, chose to pilot the VPN first with third-party providers and employee remote-access users of MVD systems following a successful internal pilot testing period with Information Technology Group (ITG) 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, 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 ITG 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 ITG 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 ITG 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:

1. Bizillion
2. USWest/Qwest
3. COX@Home
4. AOL
5. 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 ITG 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 is indicating that IP Security (IPSec) is becoming the dominant standard for VPNs. In the 3rd Quarter of 2001 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:

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

ITG 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 for field-testing is shown in Figure 3-1 below, and the PIJ is shown in Appendix B of this document.

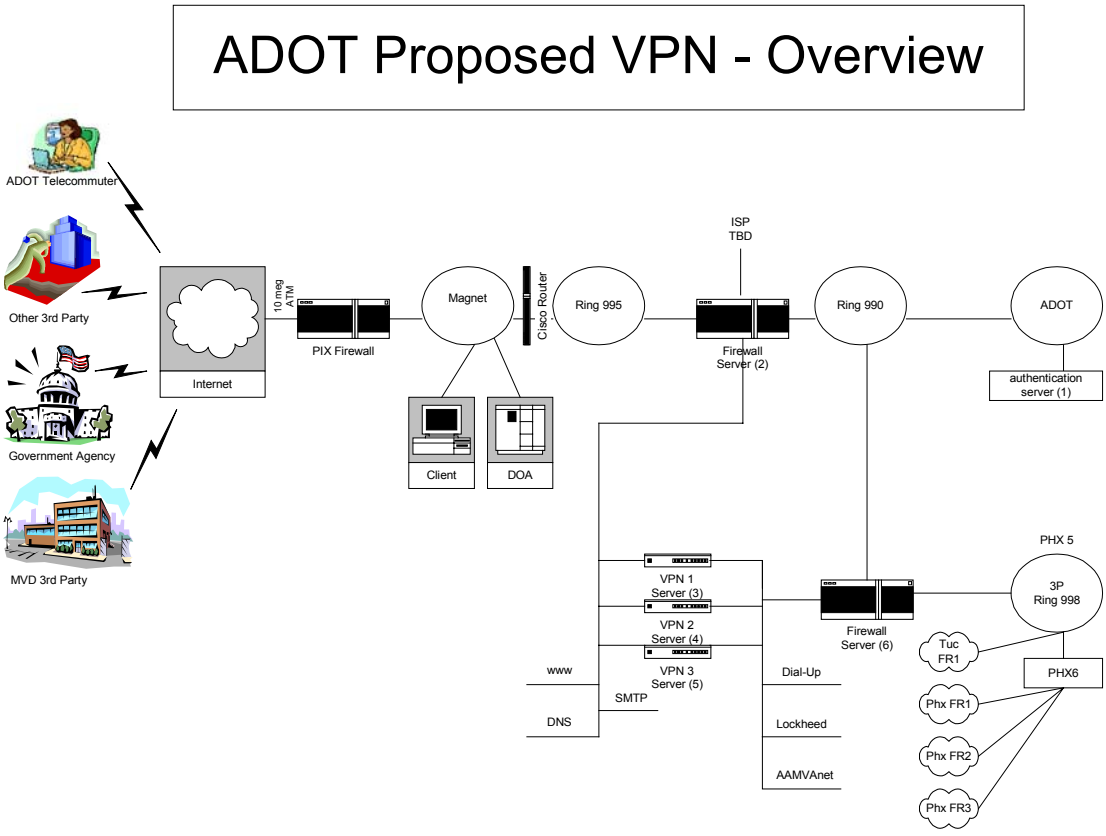


Figure 3-1 Proposed VPN Architecture

3.2 External Testing of the ADOT VPN Solution

Beginning in August 2000, 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 ITG with the appropriate approvals, 5 organizations were participants:

- City of Phoenix Prosecutors Office
- Federal Bureau of Investigation
- Scottsdale Police Department
- RRRobertson Investigations
- Kolb, Stewart & Associates Investigations

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 ITG staff enough! A follow-up in September 2001 later reinforced her initial opinion.

The City of Phoenix Prosecutors Office is an example of a Server-to-server (or LAN-to-LAN) VPN as opposed to a desktop to VPN server configuration, as with the other third-party pilot testers and remote access users.

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 relived that the time savings and travel reduction are helping the FBI offices tremendously.

3.2.3 City of Scottsdale Police Department

Mike Rosenberger of the Scottsdale Police Department began using the VPN in 2001 to pull MVD records. Initially, there was a hold up in processing the paperwork for Scottsdale in gaining access, and a change in personnel over there further delayed setup, but today the system is performing flawlessly.

3.2.4 RR Robertson Private Investigations

Rich Robertson requested access to the VPN for himself and 2 other users in his private investigations office to pull MVD drivers license and license plate records rather than drive down to MVD offices, fill out paperwork, and wait for ADOT personnel to fulfill the requests.

3.2.5 Kolb, Stewart & Associates Private Investigations

3 users from Kolb, Stewart & Associates requested access to the VPN to pull MVD drivers license and license plate records rather than drive down to MVD offices, fill out paperwork, and wait for ADOT personnel to fulfill the requests.

3.3 Testing Conducted

The VPN field-testing that took place from August 2000 through October 2001 for both types of access to the ADOT VPN -- server-to-server and remote client to server -- showed great promise and indicated that VPNs should be made an ADOT offering for a wider audience of potential users.

ADOT's enterprise network is run almost exclusively on the Microsoft family of client, server and network operating systems. Because of this architecture, the Information Technology Group adopted Microsoft's Point-to-Point Tunneling Protocol (PPTP) as the best fit for a VPN solution for acceptance and field testing. Under the ADOT / Microsoft Enterprise Agreement, the VPN software could be deployed at no additional cost to the Department. After careful research and analysis, the necessary hardware to support this configuration was purchased, installed and used in testing the VPN.

A year prior to the inception of the VPN project, ITG's Data Security Group was championing a task to strengthen remote, dial-up networking security via the use of a portable challenge / response token card devices.
VPN security was not a concern to the Token Card plan at the time because:

- The principal focus was Dial-up clients.
- The VPN process had not yet been born.

After the challenge / response server, clients and VPN solution were implemented, ITG received a directive from the Office of the CIO, that all remote users be required to use the CRYPTOCard for remote network access as a *two-factor authentication device* (something a person has -- a token, plus something a person knows -- a password). PC/LAN's Server Team and Systems Architecture began testing the Token Card logon process with the field-testing Microsoft VPN. **It was concluded from these tests that the two systems were incompatible.**

Because of the obstacles described above, ITG decided that a new, compatible VPN solution should be engineered, and the details of the new system may be found in Appendix F of this report (Courtesy of Rich Nacinovich of ITG)

4. Results of VPN field-testing

"It's almost too easy!"
-- Rich Robertson's commentary on the ADOT VPN

At the end of the testing period, 72 people were set-up to use the VPN for remote access and for LAN-to-LAN connectivity within the Phoenix Prosecutors Office. In September 2001, an online survey was developed by the researcher and sent out to the user base of 72 people. A number of questions related to system configurations from remote access workstations and usability questions were asked using the Likert Scale (e.g. 1-easy, 3-moderate, 5-difficult) for developing survey questions. The surveying period was open for two weeks and survey recipients were requested to complete the survey two times, but only 22 responses were eventually received. All 22 survey responses may be found in Appendix A of this document.

4.1 User Survey

The survey sent to users was developed as a Web form (shown below in Figure 4-1 below), placed on a publicly-accessible Web site, and a link was sent to all e-mail addresses of the users conducting VPN testing. Anonymous survey responses were automatically e-mailed to the researcher for collection and analysis.

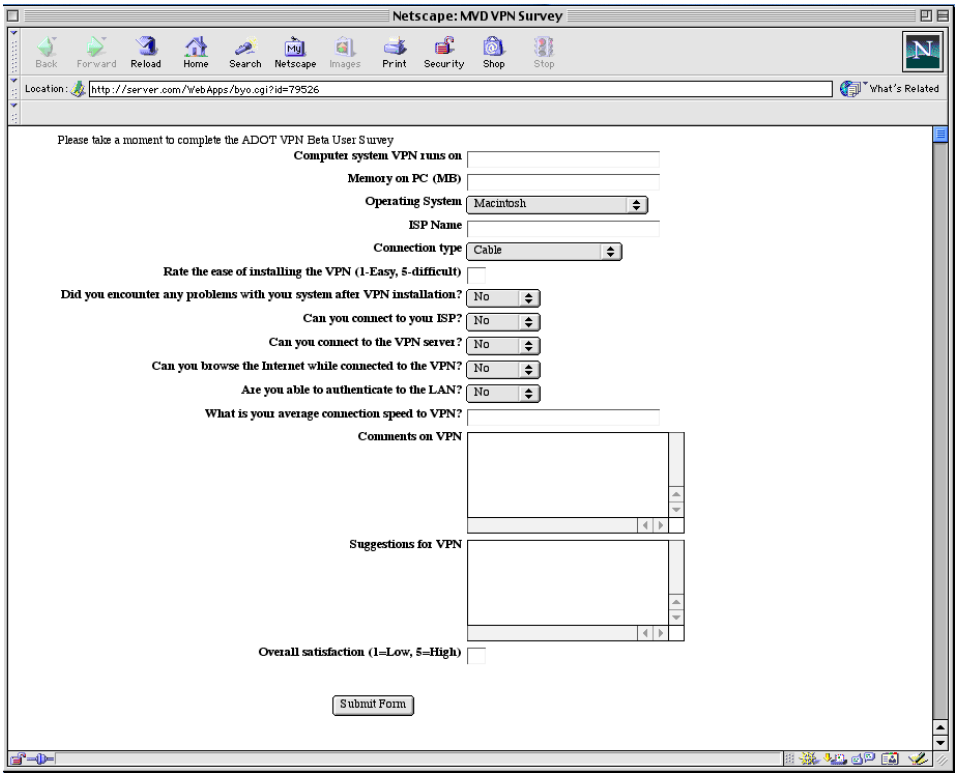


Figure 4-1 MVD VPN User Survey Form

4.2 Analysis

A number of selected items from the survey were tabulated and graphed, including:

1 - Rating of the ease of installing the requisite VPN software and configuring the system

2- Types of ISP services in use for connecting via the VPN

3- Overall satisfaction with the system

These graphs are shown below in Figures 4-2. 4-3. And 4-4 respectively.

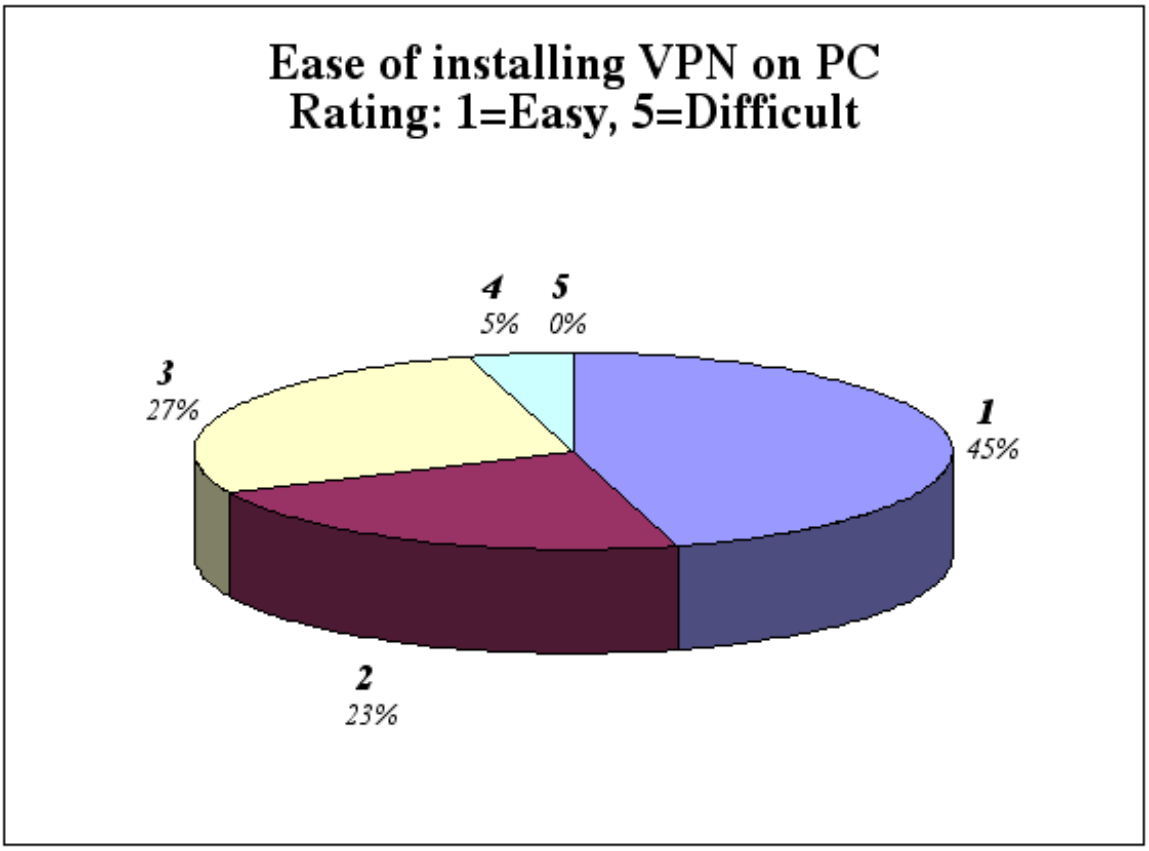


Figure 4-2 Ratings of VPN ease of use

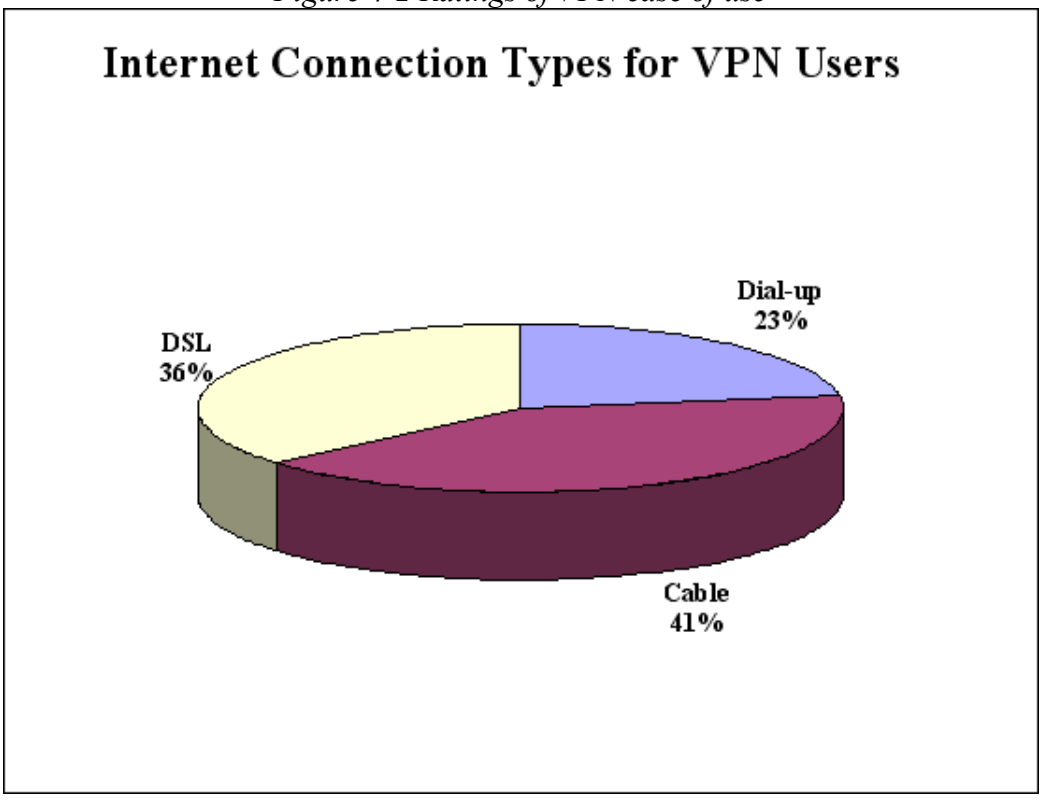


Figure 4-3 ISP connectivity methods by VPN users

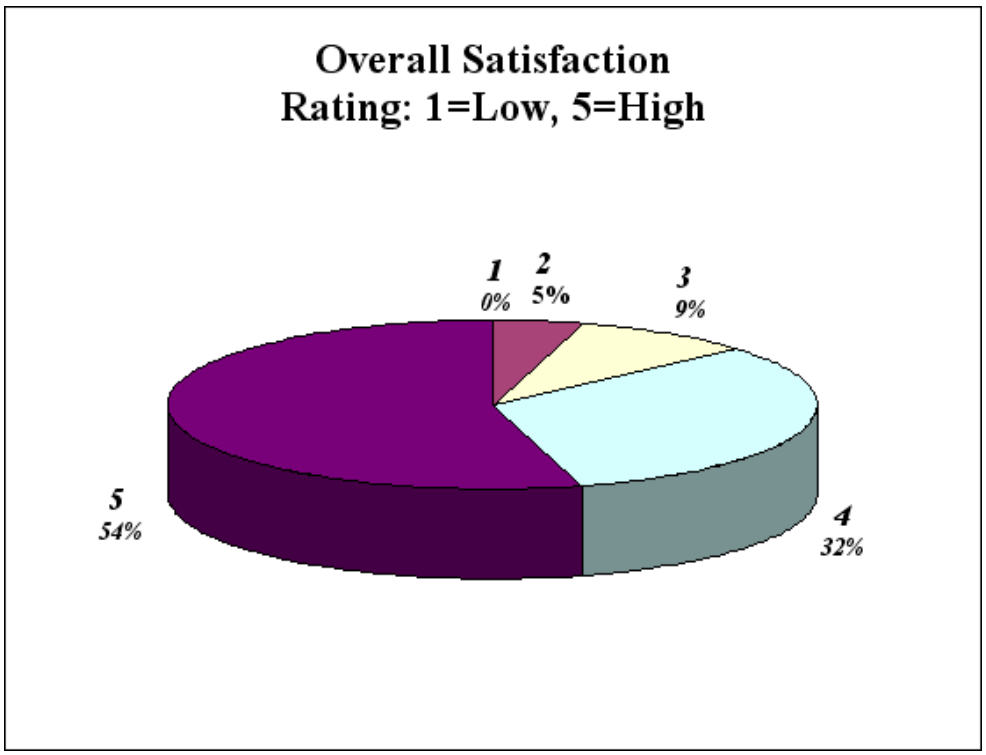


Figure 4-4 Overall VPN User satisfaction

4.3 Comments from ADOT VPN users

Below are some selected comments and recommendations from the survey forms received.

" I hope you intend to take it to the next stage (CryptoCard authentication or ??). If possible, it should be opened up, especially to those who telecommute on a regular basis."

" It is wonderful and normally a very reliable connection"

" Worked very nicely with a High Speed Wireless Modem. Even a Slow Connection was not too bad, for critical times I needed access to files."

" Wonderful. I use it often; when I telecommute on Thursday & at other times. It's useful in that I have access to all my files on the network regardless of where I'm working"

" I have been using the VPN since approximately March 2001. The reliability of the system is outstanding. I think there have only been two/three times when my connection was dropped. I was able to log back in right away."

" Faster than speeding bullet!"

" Very convenient and useful, lived the flexibility when I didn't have to dial in, like not having my phone line tied up."

"I absolutely LOVE it! Makes my job so much easier and I'm more efficient."

4.4 ADOT's VPN Recognized by IT Industry

In an April 10, 2001, Internetweek In-depth article, entitled "Will Web Services Do The Trick?", columnist John Webster wrote about CSE Insurance Company who are trying to expand internal processing and servicing using the Internet. An excerpt from the article follows:

"For example, when the company sells an auto insurance policy, it has to retrieve a customer's driving record from a state department of motor vehicles, a process that can take days. A Web services app could retrieve the DMV information electronically, Pierson says.

CSE now retrieves DMV data using batch-oriented electronic data interchange (EDI), which can take three business days to process. A few states, **including Arizona**, have the technology in place to post DMV information on the Internet. As more states do this, CSE will be able to retrieve DMV information in seconds."

The complete article may be found at:
http://www.internetweek.com/indepth01/indepth041001.htm

5. Conclusions

ADOT's system has proven that VPN technology is suitable for remote access by employees and for LAN-to-LAN connectivity to other government agencies with a need for high-volume processing and retrieval of ADOT records.

The system should be deployed in a full roll-out once a solution that's compatible with ADOT's two-factor authentication mechanisms is in place and fully integrated into ADOT's production network.

ADOT should also consider using the VPN to further expand connectivity into 3rd party processing offices for MVD.

Appendix A: Survey Responses

Following are the 22 responses received over a two-week survey period for MVD users:

Computer system VPN runs on: Compaq
Memory on PC (MB): 312
Operating System: Windows 9x/NT/2K
ISP Name: Qwest
Connection type: DSL
Rate the ease of installing the VPN (1-Easy, 5-difficult): 1
Did you encounter any problems with your system after VPN installation?: No
Can you connect to your ISP?: No
Can you connect to the VPN server?: Yes
Can you browse the Internet while connected to the VPN?: No
Are you able to authenticate to the LAN?: Yes
What is your average connection speed to VPN?:
Comments on VPN: Works very well unless I receive an e-mail with an Intranet address. Do not know how to connect to the ADOT Intranet while operating on VPN.
Suggestions for VPN: Comment on Survey - As a non-technical person, I am uncertain what you are seeking in response.
Example: "What is your average connection speed to VPN?" Are you asking for a time?
Overall satisfaction (1=Low, 5=High): 5

Computer system VPN runs on: Compaq Deskpro EN
Memory on PC (MB): 256
Operating System: Windows 9x/NT/2K
ISP Name: ADOT?
Connection type: Other
Rate the ease of installing the VPN (1-Easy, 5-difficult): 3
Did you encounter any problems with your system after VPN installation?: No
Can you connect to your ISP?: Yes
Can you connect to the VPN server?: Yes
Can you browse the Internet while connected to the VPN?: Yes
Are you able to authenticate to the LAN?: Yes
What is your average connection speed to VPN?:
Comments on VPN:
Suggestions for VPN:
Overall satisfaction (1=Low, 5=High): 4

Computer system VPN runs on: Various
Memory on PC (MB): 256 MB
Operating System: Windows 9x/NT/2K

ISP Name: COX
Connection type: Cable
Rate the ease of installing the VPN (1-Easy, 5-difficult): 1
Did you encounter any problems with your system after VPN installation?: No
Can you connect to your ISP?: Yes
Can you connect to the VPN server?: No
Can you browse the Internet while connected to the VPN?: Yes
Are you able to authenticate to the LAN?: Yes
What is your average connection speed to VPN?: 10 meg
Comments on VPN:
Suggestions for VPN:
Overall satisfaction (1=Low, 5=High): 5

Computer system VPN runs on: 1.1GH AMD Thunderbird
Memory on PC (MB): 640
Operating System: Windows 9x/NT/2K
ISP Name: QWEST
Connection type: DSL
Rate the ease of installing the VPN (1-Easy, 5-difficult): 3
Did you encounter any problems with your system after VPN installation?: No
Can you connect to your ISP?: Yes
Can you connect to the VPN server?: Yes
Can you browse the Internet while connected to the VPN?: Yes
Are you able to authenticate to the LAN?: Yes
What is your average connection speed to VPN?: It says 1000000000. Can't be!
Comments on VPN: Excellent! When I must work from home, it's almost like being on a LAN attached machine. The mainframe access is not much different from being there and Email is fast enough to be efficient.
Suggestions for VPN: I hope you intend to take it to the next stage (CryptoCard authentication or??). If possible, it should be opened up, especially to those who telecommute on a regular basis. Of course the DSL or Cable connection is not possible for some.
Overall satisfaction (1=Low, 5=High): 4

Computer system VPN runs on: HP670Z Pentium II 400
Memory on PC (MB): 96
Operating System: Windows 9x/NT/2K
ISP Name: Earthlink
Connection type: Other
Rate the ease of installing the VPN (1-Easy, 5-difficult): 2
Did you encounter any problems with your system after VPN installation?: Yes
Can you connect to your ISP?: Yes
Can you connect to the VPN server?: Yes
Can you browse the Internet while connected to the VPN?: Yes
Are you able to authenticate to the LAN?: Yes

What is your average connection speed to VPN?: 10,000,000 bps
Comments on VPN: Was getting knocked off several times a day and sometimes could not get re-connected until late afternoon. This has not happened lately.
Suggestions for VPN: Need help desk trained for VPN problem resolution. Sometimes when I had problems, I had to sign onto dial-up to send email requesting problem resolution.
Overall satisfaction (1=Low, 5=High): 3

Computer system VPN runs on: P IV 1.4g Intell
Memory on PC (MB): 256
Operating System: Windows 9x/NT/2K
ISP Name: Cox @ Home
Connection type: Cable
Rate the ease of installing the VPN (1-Easy, 5-difficult): 4
Did you encounter any problems with your system after VPN installation?: No
Can you connect to your ISP?: Yes
Can you connect to the VPN server?: Yes
Can you browse the Internet while connected to the VPN?: Yes
Are you able to authenticate to the LAN?: Yes
What is your average connection speed to VPN?: Faster than 56K Slower than c
Comments on VPN:
Suggestions for VPN:
Overall satisfaction (1=Low, 5=High): 3

Computer system VPN runs on: P2 400 mghz
Memory on PC (MB): 256
Operating System: Windows 9x/NT/2K
ISP Name: cox @ home
Connection type: Cable
Rate the ease of installing the VPN (1-Easy, 5-difficult): 3
Did you encounter any problems with your system after VPN installation?: No
Can you connect to your ISP?: Yes
Can you connect to the VPN server?: Yes
Can you browse the Internet while connected to the VPN?: Yes
Are you able to authenticate to the LAN?: Yes
What is your average connection speed to VPN?: 10000
Comments on VPN: Runs great!!
Suggestions for VPN:
Overall satisfaction (1=Low, 5=High): 5

Computer system VPN runs on: 400 Mhz Pentium II
Memory on PC (MB): 128 MB
Operating System: Windows 9x/NT/2K
ISP Name: Qwest
Connection type: DSL

Rate the ease of installing the VPN (1-Easy, 5-difficult): 1
Did you encounter any problems with your system after VPN installation?: No
Can you connect to your ISP?: Yes
Can you connect to the VPN server?: Yes
Can you browse the Internet while connected to the VPN?: Yes
Are you able to authenticate to the LAN?: Yes
What is your average connection speed to VPN?: 1 Meg
Comments on VPN: Works for me.
Suggestions for VPN: Make telecommuting manditory.
Overall satisfaction (1=Low, 5=High): 4

Computer system VPN runs on: ACT
Memory on PC (MB): 384
Operating System: Windows 9x/NT/2K
ISP Name: Cox@Home
Connection type: Cable
Rate the ease of installing the VPN (1-Easy, 5-difficult): 1
Did you encounter any problems with your system after VPN installation?: No
Can you connect to your ISP?: Yes
Can you connect to the VPN server?: Yes
Can you browse the Internet while connected to the VPN?: Yes
Are you able to authenticate to the LAN?: Yes
What is your average connection speed to VPN?:
Comments on VPN:
Suggestions for VPN:
Overall satisfaction (1=Low, 5=High): 5

Computer system VPN runs on: PC - Windows 98
Memory on PC (MB): 128 Mb
Operating System: Windows 9x/NT/2K
ISP Name: Cox @ Home
Connection type: Cable
Rate the ease of installing the VPN (1-Easy, 5-difficult): 2
Did you encounter any problems with your system after VPN installation?: No
Can you connect to your ISP?: Yes
Can you connect to the VPN server?: Yes
Can you browse the Internet while connected to the VPN?: No
Are you able to authenticate to the LAN?: Yes
What is your average connection speed to VPN?:
Comments on VPN: It is wonderful and normally a very reliable connection.
Suggestions for VPN: Provide means, if possible, to allow connection to Internet or Servers outside firewall while logged into network via VPN.
Overall satisfaction (1=Low, 5=High): 5

Computer system VPN runs on: Compaq Armada M700
Memory on PC (MB): 392mb
Operating System: Windows 9x/NT/2K
ISP Name:
Connection type: Dial-up
Rate the ease of installing the VPN (1-Easy, 5-difficult): 1
Did you encounter any problems with your system after VPN installation?: No
Can you connect to your ISP?: Yes
Can you connect to the VPN server?: Yes
Can you browse the Internet while connected to the VPN?: Yes
Are you able to authenticate to the LAN?: Yes
What is your average connection speed to VPN?: 128
Comments on VPN: I has worked very well for me until the wireless modem company went bankrupt. I do not use VPN at this time.
Suggestions for VPN:
Overall satisfaction (1=Low, 5=High): 5

Computer system VPN runs on: Window 95 & 98 SE
Memory on PC (MB): 32 & 192
Operating System: Windows 9x/NT/2K
ISP Name: MCI World Com & Qwest.net
Connection type: Other
Rate the ease of installing the VPN (1-Easy, 5-difficult): 3
Did you encounter any problems with your system after VPN installation?: No
Can you connect to your ISP?: Yes
Can you connect to the VPN server?: Yes
Can you browse the Internet while connected to the VPN?: No
Are you able to authenticate to the LAN?: Yes
What is your average connection speed to VPN?: 100k & 50k
Comments on VPN: Worked very nicely with a High Speed Wireless Modem. Even a Slow Connection was not too bad, for critical times I needed access to files.
Suggestions for VPN: Maybe make some easy to access files that tell folks how to map their drive and set up e-mail. These would be accessed through some simple share & instruction. Maybe something like \\VPNHELP\ on the Intranet.
Overall satisfaction (1=Low, 5=High): 4

Computer system VPN runs on: Compaq Armada E7000
Memory on PC (MB): 128
Operating System: Windows 9x/NT/2K
ISP Name: Cox
Connection type: Cable
Rate the ease of installing the VPN (1-Easy, 5-difficult): 2
Did you encounter any problems with your system after VPN installation?: No
Can you connect to your ISP?: Yes
Can you connect to the VPN server?: Yes

Can you browse the Internet while connected to the VPN?: Yes
Are you able to authenticate to the LAN?: Yes
What is your average connection speed to VPN?: ?? Don't know how to tell??
Comments on VPN: Wonderful. I use it often; when I telecommute on Thursday & at other times. It's useful in that I have access to all my files on the network regardless of where I'm working
Suggestions for VPN: * I would like my password to reset automatically after 30 days so that I can keep in sync with my others.

* As for ease of install, I don't recall the specific issue with install but, I didn't get it right the first time. But, I think it had to do with my router config. I have a netgear RT314 because I have a home system & the work system sharing the cable line. I had some trouble initially connecting the work system into the network but worked with Rich & Roger to resolve. Also, I recall that when I initally loaded the VPN files off the ADOTNet, one of the files was for zone alarm software. I don't think anything loaded and that was a bit confusing.

* I have been using the VPN since apx March 2001. The reliability of the system is outstanding. I think there have only been two/three times when my connection was dropped. I was able to log back in right away.

The only other problem I encountered had to do with my LAN password. Something to do with it expiring and not being in cache. Rich advised what to do to remedy.
Overall satisfaction (1=Low, 5=High): 5

Computer system VPN runs on: Gateway 700 mhz
Memory on PC (MB): 128
Operating System: Windows 9x/NT/2K
ISP Name: Qwest
Connection type: DSL
Rate the ease of installing the VPN (1-Easy, 5-difficult): 2
Did you encounter any problems with your system after VPN installation?: No
Can you connect to your ISP?: Yes
Can you connect to the VPN server?: Yes
Can you browse the Internet while connected to the VPN?: Yes
Are you able to authenticate to the LAN?: Yes
What is your average connection speed to VPN?: Faster than speeding bullet
Comments on VPN: Very happy with the VPN. It's fast and reliable. Once in, the forms and commands are not user-friendly, but that's not a VPN issue I don't think.
Suggestions for VPN: Photos???
Overall satisfaction (1=Low, 5=High): 5

Computer system VPN runs on: Intel Pentium III 750
Memory on PC (MB): 128
Operating System: Windows 9x/NT/2K
ISP Name: Cox@Home
Connection type: Cable
Rate the ease of installing the VPN (1-Easy, 5-difficult): 1
Did you encounter any problems with your system after VPN installation?: No
Can you connect to your ISP?: No
Can you connect to the VPN server?: Yes
Can you browse the Internet while connected to the VPN?: No
Are you able to authenticate to the LAN?: Yes
What is your average connection speed to VPN?:
Comments on VPN: Easy to set up.
Suggestions for VPN:
Overall satisfaction (1=Low, 5=High): 4

Computer system VPN runs on: Windows 98
Memory on PC (MB): 32 mgs
Operating System: Windows 9x/NT/2K
ISP Name: Qwest.net
Connection type: DSL
Rate the ease of installing the VPN (1-Easy, 5-difficult): 1
Did you encounter any problems with your system after VPN installation?: No
Can you connect to your ISP?: Yes
Can you connect to the VPN server?: Yes
Can you browse the Internet while connected to the VPN?: No
Are you able to authenticate to the LAN?: Yes
What is your average connection speed to VPN?: n/a
Comments on VPN: It would be nice to be able to log into VPN while connected to Internet. I also believe that an actual training class should be mandated before access to the system-not just a training packet.
Suggestions for VPN: None. We are actually very satisfied with the system.
Overall satisfaction (1=Low, 5=High): 4

Computer system VPN runs on: Compaq M700 laptop
Memory on PC (MB): 384
Operating System: Windows 9x/NT/2K
ISP Name: Qwest
Connection type: DSL
Rate the ease of installing the VPN (1-Easy, 5-difficult): 1
Did you encounter any problems with your system after VPN installation?: Yes
Can you connect to your ISP?: Yes
Can you connect to the VPN server?: Yes
Can you browse the Internet while connected to the VPN?: Yes

Are you able to authenticate to the LAN?: Yes
What is your average connection speed to VPN?: 256
Comments on VPN: Seems to work well for the most part. The MS Outlook many times
does not connect properly, and hangs up (freezes) quite a bit.
Suggestions for VPN: Look into interface with MS outlook.
Overall satisfaction (1=Low, 5=High): 5

Computer system VPN runs on: Intel Chassis & Motherboard
Memory on PC (MB): 256
Operating System: Windows 9x/NT/2K
ISP Name: SNET(SBC)
Connection type: DSL
Rate the ease of installing the VPN (1-Easy, 5-difficult): 1
Did you encounter any problems with your system after VPN installation?: No
Can you connect to your ISP?: Yes
Can you connect to the VPN server?: Yes
Can you browse the Internet while connected to the VPN?: Yes
Are you able to authenticate to the LAN?: Yes
What is your average connection speed to VPN?: 1.5
Comments on VPN: No special software was installed, only that which came with various versions of Windows NT and 2K.
Suggestions for VPN:
Overall satisfaction (1=Low, 5=High): 5

Computer system VPN runs on: Compaq
Memory on PC (MB): 256
Operating System: Windows 9x/NT/2K
ISP Name: MCI World Com
Connection type: Other
Rate the ease of installing the VPN (1-Easy, 5-difficult): 3
Did you encounter any problems with your system after VPN installation?: No
Can you connect to your ISP?: Yes
Can you connect to the VPN server?: Yes
Can you browse the Internet while connected to the VPN?: Yes
Are you able to authenticate to the LAN?: Yes
What is your average connection speed to VPN?: 100
Comments on VPN: Very convienent and useful, lved the flexibility when I didn't have to dial in, like not having my phone line tied up.
Suggestions for VPN: Available in more parts of Arizona, like east Mesa.
Overall satisfaction (1=Low, 5=High): 5

Computer system VPN runs on: Windows 98/Packard Bell 166
Memory on PC (MB): 24
Operating System: Windows 9x/NT/2K
ISP Name: Cox
Connection type: Cable
Rate the ease of installing the VPN (1-Easy, 5-difficult): 3
Did you encounter any problems with your system after VPN installation?: No
Can you connect to your ISP?: Yes
Can you connect to the VPN server?: Yes
Can you browse the Internet while connected to the VPN?: Yes
Are you able to authenticate to the LAN?: No
What is your average connection speed to VPN?: Same as at work
Comments on VPN: I did not install the VPN. I am not able to access other drives, intranet through VPN. It operates as a fast email link.
Suggestions for VPN:
Overall satisfaction (1=Low, 5=High): 4

Computer system VPN runs on: Compaq Armada
Memory on PC (MB): 6.04
Operating System: Windows 9x/NT/2K
ISP Name:
Connection type: Cable
Rate the ease of installing the VPN (1-Easy, 5-difficult): 1
Did you encounter any problems with your system after VPN installation?: No
Can you connect to your ISP?: Yes
Can you connect to the VPN server?: Yes
Can you browse the Internet while connected to the VPN?: Yes
Are you able to authenticate to the LAN?: Yes
What is your average connection speed to VPN?: 10.0
Comments on VPN: I absolutely LOVE it! Makes my job so much easier and I'm more effient.
Suggestions for VPN: I don't honestly have any suggestions. It is great
Overall satisfaction (1=Low, 5=High): 5

Computer system VPN runs on: Has been tried on two "clones"
Memory on PC (MB): 128 and 256
Operating System: Windows 9x/NT/2K
ISP Name: Earthlink thru sprint broadban
Connection type: Other
Rate the ease of installing the VPN (1-Easy, 5-difficult): 2
Did you encounter any problems with your system after VPN installation?: Yes
Can you connect to your ISP?: Yes
Can you connect to the VPN server?: Yes
Can you browse the Internet while connected to the VPN?: Yes

Are you able to authenticate to the LAN?: Yes
What is your average connection speed to VPN?: extremely slow, about modem sp
Comments on VPN: I have tried running ADOT VPN on two different "clone" machines at home over the past year. The first installation worked but was very slow, no better then just using RAS and every single time I exited the VPN it would cause my computer to reboot about 30 seconds after exiting. For the second installation it installed with some confusion due to trying to juggle the broadband connection settings and the VPN settings. Once it was installed I was able to connect and get my email and browse the network. However, it only worked that one initial time. And it was very slow, again, it seemed about the speed of a modem. The second time I tried to use VPN it would not work at all and continually crashed the computer.
Suggestions for VPN:
Overall satisfaction (1=Low, 5=High): 2

Appendix B: Project and Investment Justification

(insert PIJ document here)

Appendix C: 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 D: 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 E: 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:

1. Authentication
2. Cryptography
3. General security
4. Malicious code
5. Network security
6. Physical security
7. Policies
8. 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 F: Proposed Solution For Production Rollout VPN Compatible With CRYPTOCard (Token) Authentication Mechanisms

by
Rich Nacinovich and Nicole Drew

ARIZONA DEPARTMENT OF TRANSPORTATION

Information Technology Group

A comprehensive VPN / Extranet overview

Executive Summary

ADOT has selected a VPN / Extranet system that will accommodate its growing telecommuter workforce as well as the ever evolving site-to-site B2G (Business-to-Government) and G2G (Government-to-Government) customer base. Before selecting Nortel's Contivity 2600 hardware, several vendors' Extranet / VPN offerings were evaluated.

- *Note: For a complete review of the equipment evaluation, please refer to the test results document, found below.*

In the past, RAS (remote access service) over dial-up was an acceptable form of off-site connectivity. As applications advance in complexity and size, so does the demand for bandwidth requirements. With the proliferation of broadband services for home users and the implementation of a pure IP remote access solution, the perfect combination of remote access, convenience and throughput performance is obtained. Telecommuters now have the option of reaching the remote network many times faster and more secure than dialing up over the PSTN (public switched telephone network).

Although a benefit, high-speed connections are certainly not a prerequisite of VPN usage. In fact, once deployed, the VPN could viably support all of ADOT's remote user access needs. Ultimately, direct-dial long distance sessions and the accompanying server side, channelized leased lines that support those sessions could eventually be reduced in number or completely eliminated.

The alternative? A local or toll-free dial-up Internet connection to an IPSec compliant ISP (Internet service provider). The result? A significantly lower TCO for secure, remote user accommodations.

MVD third parties access ADOT's network resources to carry out their contractual obligations while representing the Department both proficiently and professionally. Traditionally, these connections required the purchase of expensive leased carrier lines and enterprise grade CPE (customer premise equipment). Now, the partnering business need only an Internet connection and a low cost Contivity 100 switch or compatible firewall that supports IPSec branch office tunnels to carry out those data transactions.

Intergovernmental agencies also query ADOT's Driver's Database and Central Image Server for assistance with law enforcement activities and court proceedings, to name a few. Most, if not all of these agencies are already subscribing to dedicated Internet access via a local ISP, making extranet communications the simple and smart way to use an existing, publicly established IP infrastructure.

With a solid VPN / extranet solution in place, ADOT is ready to accommodate its remote employees, governmental peers and business partners today. Moreover, the Contivity 2600's built in scalability primes ADOT to meet the predictable remote access demands of the future.

Tunnels

Using a combination of time tested and cutting-edge technologies, the Nortel Contivity 2600s'

dedicated purpose is to establish and maintain strongly encrypted “tunnels” over the PDN (public data network).

Tunneling is a technology that enables one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network. For example, Microsoft's PPTP technology enables organizations to use the Internet to transmit data across a virtual private network (VPN). It does this by embedding its own network protocol within the TCP/IP packets carried by the Internet.[1]
ADOT incorporates a much more secure 3DES (triple data security standard), IPSec tunnel.
Two types of tunnels will be available for use:

- The most common is the single user to switch category.
    - This arrangement allows a single user (client) to access the enterprise network from a remote location.
    - Single session supports a single user.
    - Similar in function to dial-up service.
- Secondly, branch office tunnels (switch-to-switch) are configurable.
    - A connection like this creates a virtual wide area network.
    - In a remote office, many computers’ WAN needs can be supported in this way.
    - Single session supports one or many users, simultaneously, at the remote site.

Contivity 2600 Switch

Hardware Specifications

Each Nortel Contivity 2600 switch is capable of supporting up to 1,000 concurrent connections. The rack mounted 3U component system is essentially an Intel x86 based server equipped with 256MB of SDRAM (128 MB standard plus an optional 128 MB module) and dual 100Mb/s Ethernet controllers.
One Ethernet card interfaces the PDN and the other connects the switch to the private, internal ADOT Network.

- *Note: Please refer to the included Logical RAS Schematic below for details on hardware and communication link logistics.*

The Contivity 2600s each came equipped with an optional PCI encryption accelerator board. These specialized, internal modules perform bulk encryption and algorithms for all tunnel traffic, dramatically improving performance. During times of high system demand, this extra hardware makes short work of the complicated data encryption and decryption processes[2]. Unlike software VPNs, the Contivity is dedicated to maintaining multiple, encrypted tunnels. No unrelated, unnecessary services, peripherals or drivers are required, making it adept at this function alone.

Features

User Administration

With the issuance of a valid challenge-response token card and the appropriate client connection software, remote access is effortlessly obtained. Previously, adding a new user was a tedious process of creating, managing and deleting individual user accounts. Now, all user administration is conducted on the challenge-response authentication server. For credential verification purposes, the switches simply act as a conduit by passing the encrypted logon process on to ADOT's RADIUS server and the token authentication server. This streamlined procedure is a boon for ADOT system administrators.

Administration Interfaces

Initial administration is carried out via a serial cable and terminal emulation software. Alternatively, preliminary TCP/IP data can be entered using Nortel's included ExNetIP.exe utility. This program will automatically search the local subnet for any Contivity equipment, return the respective serial number and provide a space for directly editing the management IP address, subnet mask, and default gateway.

Subsequent programming is best performed over HTTP, with any current web browser.
Support for telnet sessions is also provided.

Load Balancing

The VPN device carefully monitors session volume and traffic flow. Automatic activation of load balancing occurs between the two switches in the event that the number of connections or throughput threshold approaches equipment limitations. The hardware accelerator card detects the impending overload and automatically begins to divert connection attempts to the secondary switch.

Automatic Failover

Another useful feature is automatic failover. Upon initial logon, the switch silently saves pertinent configuration information to the client operating system's registry. These instructions specify what to do in the unlikely event that the primary switch is unavailable.

For example, clients routinely connect to VPN A. A hardware failure has occurred with this unit and as a result, it is no longer answering connection attempts. The client connection software automatically tries VPN B. If it is responding, a session is established with the specified back-up (VPN B). Subsequent logon attempts will repeat this process until VPN A becomes available again.

Contivity Client Software

System Requirements

Minimum Hardware Requirements

- 233 MHz Pentium
- 64 MB RAM
- 20 MB Free HDD space

OR

- Hardware requirements of the loaded operating system +
    - 8 MB RAM
    - 20 MB Free HDD space

Note: The strong encryption algorithms used to secure data may cause lower-end systems to perform more slowly.

Supported Operating Systems

The ADOT / Contivity client is supported by the following operating systems:

- Windows 98
- Windows Me*
- Windows NT 4.0
- Windows 2000 Professional
- Windows XP Home and Professional Editions

*Windows Millennium edition is not listed in Nortel's documentation as a supported operating system; however, the client has been tested successfully on this platform by the Systems Architecture team.

Note: While all of the operating systems listed above are compatible with Nortel's Contivity client software, ADOT will only provide technical support and assistance with Windows 98SE and Windows NT 4.0. All other operating systems above may receive limited support.

Customized ADOT Program

Nortel includes a basic client connection application that is functionally adequate; however, distributed in its default format requires arduous user interaction and input. Additionally, if the settings are not accurately configured, there will inevitably be problems. These problems generate unnecessary support calls and in turn, increase the demand for administrator troubleshooting and intervention.

Building on the basic client with custom setup and configuration files, the ITG VPN Team has created a unique, convenient installation executable tailored exclusively for ADOT's authorized telecommuters and non-ADOT individuals. Three versions were created to support the client's appropriate group association.

Packed inside the setup program(s) are customized files, which provide instructions on what the client application does as it is being loaded and how it functions after installation.
Once the program has been set up on the user's computer and launched, client interaction is limited to a simple UID (user ID) and password logon process. All program attributes have been preset and cannot be altered. In fact, option menus have been disabled and are "grayed-out" to the client.

While taking the "keep it simple" approach, the ITG team has effectively reduced the administration of a complicated process and increased security.

- *Note: Detailed information on security can be found under the Security heading, below.*

The switch maintains the following complimentary client functions, allowing for unique and highly customizable session attributes.

- Split tunneling – Disabled for all client connections as a security precaution. When allowed, this option permits the initiating party to retain its ISP's default gateway settings. If enabled, the user still has a valid route to all outside Internet resources while simultaneously connected to the remote enterprise network. Clearly, this configuration could cause serious problems if a rogue program were to use the telecommuter's computer as a spring- board to the internal ADOT network. Disabling split tunneling in effect completely eliminates external attacks. Virus threats such as Trojan viruses and DoS / DDoS (Denial of Service / Distributed Denial of Service) attacks cannot launch properly, thanks to inherent programming features that prevent external exposure. Once connected, the client machine is fitted with virtual "blinders" disallowing both outgoing and incoming traffic to and from the Internet. While a tunnel is up, all IP traffic is restricted to the group defined internal subnets. *see Security; User Groups*
- Third party IPSec clients – Again, for security purposes, third-party IPSec clients are not allowed. The customized software package described above was configured to serve the needs of every foreseeable remote client.
- Forced logout – This policy will not be enabled rather; an idle timeout period has been set in the switches' group policies.
- Client fail-over - Client fail-over uses small packets to check and maintain, or keep alive, the session between the user computer and the switch. See Contivity 2600 Switch; Features; Automatic Fail over
- Client auto connect – A great feature for organizations providing Internet access to their employees. Establishing a tunnel requires that an Internet connection be present. The client application can be pre-set with those phone numbers and credentials so that the both the Internet connection and tunnel are formed with a single mouse click. This feature has not been deployed because employees are free to choose their own ISP and no external Internet service is provided by the Department.

- Banner: A window that appears upon successful logon. It has been customized to include Support Desk contact information and important legal and security compliance data.
- Password storage – When enabled, allows the remote user to save their user ID and password for convenience. This option is disabled, since the hardware token card and server use a random, synchronized password.
- Client screen saver – If set, the client must password protect his / her screen saver. If the user leaves the system while connected to a tunnel, the system would effectively be locked out of the tunnel when the screen saver became active.[3] Option is disabled for all ADOT groups.
- Domain name – Domain access via the logon process is not provided. NT authentication occurs by logging on to an ADOT computer that is a member of an NT domain using cached credentials or by providing UID, password and domain for individual network resources (exchange, shares, etc…). The Contivity switch does not partake in client / domain authentication.
- Client policy – Used in concert with split tunneling (when enabled). These administrator created policies help prevent potential security violations with simple protocol filters.
    - For instance, a filter is applied to group #1's policy, effectively allowing only HTTP traffic to pass. A rogue program attempts to connect from the Internet through the active tunnel, into ADOT's network using Telnet. The attempt would be unsuccessful because only HTTP traffic is permitted.

Security

Security is, of course, the chief concern of any IT organization's remote connectivity solution. With a combination of inherent switch and client software qualities and ITG ingenuity, the Contivity solution provides extremely secure access.

From the first connection attempt, until logoff all data is transmitted using strong 3DES, IPSec tunnels.

While connected, the client software is actively monitoring its session, listening for any direct or indirect changes to the user's local IP stack. If such a change is detected, the silent monitor immediately forces a session disconnect.

IPSec Tunneling

The Contivity 2600 provides support for the following, popular tunneling protocols:
IPSec, PPTP, L2TP, and L2F.

IP Sec was chosen exclusively, as previously stated, for its hardened encryption algorithms (3DES) and diverse customization capabilities. This protocol can be difficult to manage; however, the client software and switch automatically run the necessary PKI (public key infrastructure) operations in the background, without administrator or user input.

For a more in depth description of IPSec and its capabilities and limitations, please visit the IETF (Internet Engineering Task Force) website. http://www.ietf.cnri.reston.va.us/home.html A working group exists for IPSec under the Security heading.

DES

Short for Data Encryption Standard, a popular symmetric-key encryption method developed in 1975 and standardized by ANSI in 1981 as ANSI X.3.92. DES uses a 56-bit key and is illegal to export out of the U.S. or Canada.[4]

The deployed 3DES variant applies a 168-bit key to all data. While 3DES is only one third as fast as DES, it provides protection billions of times greater than that of DES.[5] (56-bit x 3 = 168-bit)

More information on DES and other data encryption methods can be found by visiting the FIPS (Federal Information Processing Standards Publications) website.
http://www.itl.nist.gov/fipspubs/index.htm
DES specific information is available here: http://www.itl.nist.gov/fipspubs/fip46-2.htm

Contivity User Groups

User-centric groups provide the foundation for the Contivity's security and permissions scheme. Based on a need-to-know methodology, three separate groups have been pre-programmed within the switches, to accommodate ADOT's specific requirements.

1. An ADOT group was created to accommodate those employees requiring access to all network resources. A successful connection as a member of this group garners the same rights and privileges, as though the client were working from the office.
2. Mainframe & DDL Extranet CIS (Central Image Server) access will be granted to local law enforcement organizations and courts. The additional access is necessary to provide these government entities with valuable, yet sensitive positive identification data.
3. Lastly, a member of the Mainframe only group is restricted to all network resources except, as the name implies, the mainframe computer. MVD Third-Party firms will make up the bulk of this group's membership.

Extremely flexible, groups can be easily created and edited to fit the needs of any remote user situation.

Three corresponding client connection packages were also produced, each with different group attributes, to enforce the respective access policies. These inherent group properties, which are transparent to the user, dictate which private subnets are accessible.

In conjunction with the group guidelines, separate IP pools were created on ADOT's RADIUS Server, *RADIUS1*, for each of the three groups. Depending on membership and upon successful logon, an IP address is assigned to the user, which dictates the specific, accessible networks.
A firewall is responsible for enforcing the following security policies:

- ADOT Group has access to all hosts on these subnets:
    - ADOT All
    - Extranet

    - DMZ
- Mainframe only & DDL Extranet only Group has access to hosts:
    - ADOT Mainframe
    - Internal, DDL Extranet Imageserver
- Mainframe only Group has access to host:
    - ADOT Mainframe

Logon Process

From the Contivity VPN client, the user simply supplies their UID (User ID), current token (password) and clicks the connect button.

Unknown to that user though, many complex checks-and-balances are quickly happening behind the scenes.

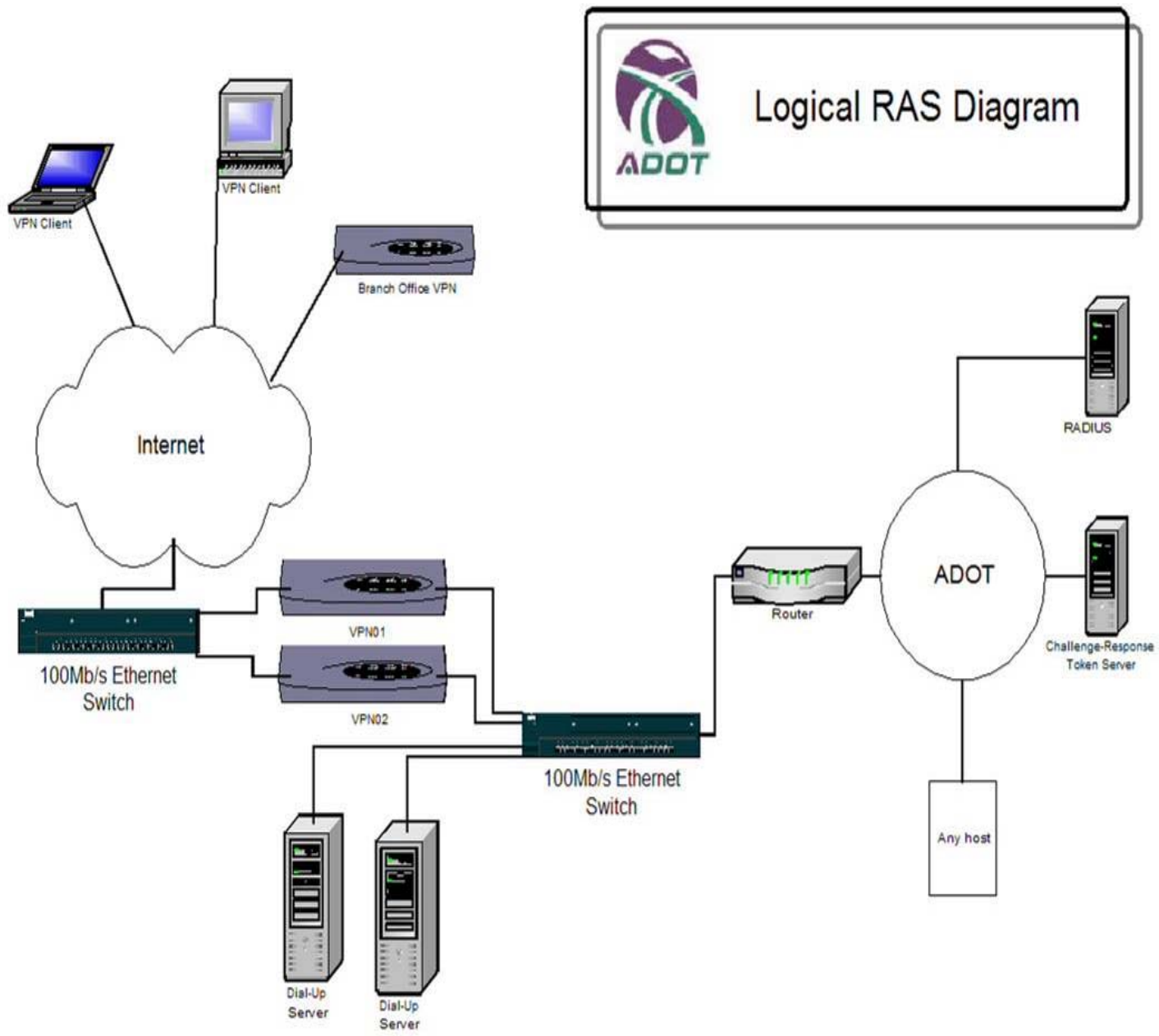
Although steps one through four follow industry "best practices" for remote access authentication, an additional layer has been added. Using ADOT's existing token authentication server and client hardware card strengthens security even further.

1. Static, group information from the preconfigured connection software and the individual username and token (password) are sent with 3DES encryption, via PAP (password authentication protocol) to the VPN switch via a temporary IPSec tunnel.
2. The group information is looked up in the VPN switches' LDAP (lightweight directory access protocol) table.
3. If any match is found in this table, the switch forwards its own, separate group shared secret to RADIUS.
4. If the Contivity's shared secret match RADIUS' LDAP database, RADIUS allows the *client* username and token to attempt several different validation methods, specified by the administrator.
5. These include, in order of attempt:
    a. 1st Attempt: Challenge-response credentials
        i. RADIUS forwards the individual's UID and token to the token authentication server. The first attempt in RADIUS' authentication order is token authentication, so if the UID or password match, the NT Domain and Native RADIUS method is not tried.
        ii. The token authentication server checks its database for the requesting UID and its corresponding valid password.
        iii. With a successful match, this server assigns its appropriate group attributes to the transaction and sends an accept challenge response and the group attribute to the RADIUS server.
        iv. RADIUS assigns the user an IP address from the specified group's IP pool.
        v. RADIUS informs the Contivity Switch of the successful logon process.
        vi. Finally, the tunnel negotiation process is complete and bi-directional, internal ADOT network access is established.
    b. 2nd Attempt: NT Domain(s) – Not used
    c. 3rd Attempt: Native (local) RADIUS accounts – Only used by administrators for diagnostic purposes.

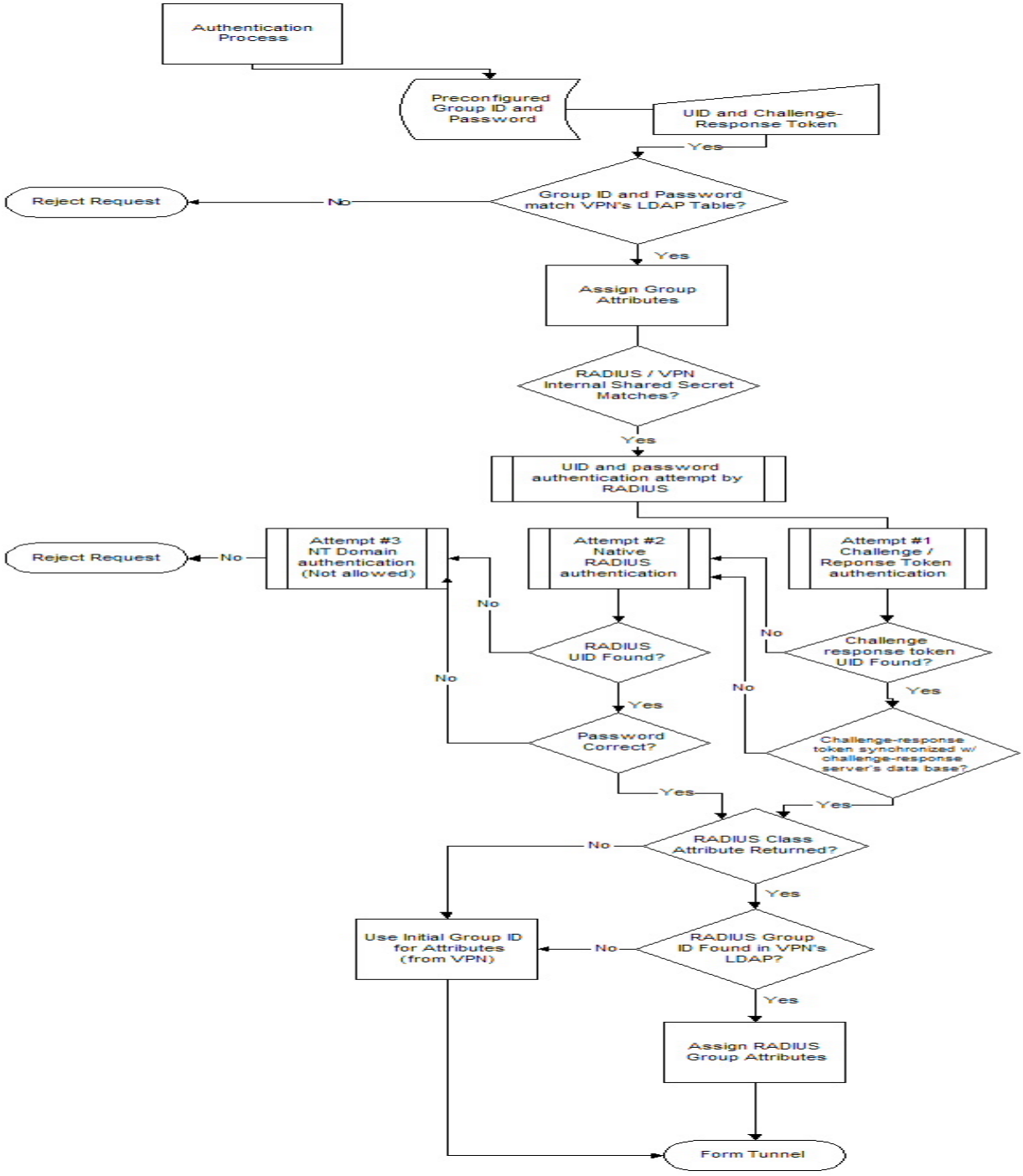
Of course, if any group name, username and / or passwords do not present an exact match, the logon request is terminated. A corresponding error message would then be displayed on the user's computer.

- Note: One inherent flaw of PAP is the method by which authentication information is transmitted. This process is carried out in clear text, completely unencrypted. Consequently, the transmitted data could be intercepted and possibly used for malicious purposes. This however, is not a concern. The Contivity's IPSec, 3DES tunnels are created using strong encryption, adding potency to the insecure PAP method of authentication. Furthermore, if the data were captured and successfully decoded, it could never be used again to complete another logon process. The random token method of authentication relies on a good-one-time-only password technology, which would render the intercepted password useless.

Logical RAS Schematic (VPN and Dial-up)


Logical RAS Diagram
ADOT
VPN Client
VPN Client
Branch Office VPN
Internet
RADIUS
ADOT
Challenge-Response
Token Server
Router
VPN01
VPN02
100Mb/s Ethernet
Switch
100Mb/s Ethernet
Switch
Any host
Dial-Up
Server
Dial-Up
Server

Authentication Server Validation Flowchart



Supporting Documentation

VPN Test Review

PURPOSE

Evaluate VPN hardware/software and make a recommendation based on reliability, capability and security.

EVALUTATION TEAM MEMBERS

Jamie Rybarczyk
Nicole Drew

OVERVIEW OF VIRTUAL PRIVATE NETWORKS

A Virtual Private Network (VPN) allows network connectivity by establishing a secure tunnel through the Internet or other private network. It allows single users as well as internal/external LAN-to-LAN connections. Some advantages of VPN's over traditional remote dial up access are:

- ⇒ Maintain security through use of encrypted tunnels
- ⇒ Enables the use of current technologies including DSL and cable modems
- ⇒ Higher than dial up connection rates
- ⇒ Reduce long distance charges
- ⇒ Higher availability / No busy signals
- ⇒ Uses the existing public telecommunication infrastructure.
- ⇒ A more scalable remote access infrastructure
- ⇒ Reduced cost of purchasing remote access ports

REQUIRED CAPABILITIES

The following capabilities are required in order for a VPN product to be considered for our production environment.

VPN Component

- ⇒ Employee/Business partner remote access
- ⇒ LAN to LAN access
- ⇒ High encryption
- ⇒ Ability to use challenge / response tokens in an encrypted tunnel
- ⇒ Allow IPSec through NAT
- ⇒ Ease of management and administration
- ⇒ Ease of installation to customer

⇒ Client compatibility (Windows 9x, ME, NT, and Windows 2000)
⇒ Support efficient number of concurrent connections

User Network/Application access:
⇒ Network Files/Drives (MS Networking)
⇒ Email (MAPI)
⇒ Mainframe
⇒ MS Terminal Server
⇒ NT Administration Tools
⇒ FTP
⇒ MS SQL Server

PRODUCTS COMPARED

The following products were chosen for testing and comparison:
⇒ MS Windows 2000 VPN
⇒ Cisco Altiga
⇒ Nortel Contivity Extranet

TEST ENVIRONMENT

Our testing was performed in the Research & Development lab. The hardware was configured on a virtual network separated from the ADOT production network. A Microsoft VPN was not configured in the lab as it is currently in use and we are familiar with its capabilities.

Representatives from both Cisco and Nortel gave on site presentations with an overview of their VPN products' configuration and capabilities. The VPN hardware was kept on site for several weeks for the purpose of evaluation and testing in our environment.

The VPNs were configured and evaluated using Windows ME, 98 and 2000 clients. They were both set-up to authenticate user accounts though a Steel Belted Radius server. Native Radius, NT Domain and challenge / response authentication were tested successfully.

TESTING RESULTS

The results of the *Required Capabilities* are as follows:

VPN Component	Microsoft	Cisco	Nortel
Employee/business partner remote access	Yes	Yes	Yes
LAN to LAN access	Yes	Yes	Yes
High encryption	Yes	Yes	Yes
Ability to use challenge / response tokens in an encrypted tunnel	No	Yes	Yes
Allow IPSec through NAT		Yes – UDP Encapsulation	UDP Encapsulation - available in July 2001 release
Ease of installation to customer	A manual process that involves several steps.	Ability to create a custom pre-configured, silent install.	Ability to create a pre-configured custom install where customer only needs to agree to licensing terms.
Administration	Routing and Remote Admin Easily configured Basic features Anyone with Admin rights to box can make changes	HTML Easily configured Detailed features Configurable levels of administration by user Good logging Networking tools	HTML/JAVA Easily configured Detailed features Configurable levels of administration by user Good diagnostics Good logging Networking tools
Client compatibility	Windows 9x, ME, NT 4.0, and 2000	Windows 9x, ME, NT 4.0, and 2000	Windows 9x, ME, NT 4.0, and 2000
Supported concurrent connections	256 tested	100 to 10,000 per unit depending on model	Up to 5,000 per unit depending on model

SUMMARY

User Network/Application access	Microsoft	Cisco	Nortel
Network Files/Drives (MS Networking)	Pass	Pass	Pass
Email (MAPI)	Pass	Pass	Pass
Mainframe	Pass	Pass	Pass
MS Terminal Server	Pass	Pass	Pass
NT Administration Tools	Pass	Pass	Pass
FTP	Pass	Pass	Pass
MS SQL Server	Pass	Pass	Pass

Microsoft 2000 VPN will not be considered, as it does not meet all of the required capabilities. It is not capable of passing a challenge / response hardware token's one time password through an encrypted tunnel.

Both Cisco and Nortel VPN products met all the capabilities required for our environment. They were both relatively easy to install and configure. They had many similar capabilities and functions that ease the administration, management and client configuration of the VPN.

VPN RECOMMENDATION

While both the Cisco Altiga and Nortel Contivity VPN's met all requirements for our environment, it is our recommendation that ADOT purchase and implement the Nortel Contivity Extranet VPN solution.

A deciding factor in this decision is simply that the Nortel VPN and Cisco VPN clients are incompatible and will not run properly when installed on the same client computer. The Department of Administration (DOA) currently uses the Nortel VPN product and there is a great potential that some users will need to access resources on both networks.

VPN System Change Notification

ADOT's enterprise network is run almost exclusively on the Microsoft family of client, server and network operating systems. Because of this architecture, the Information Technology Group adopted Microsoft's Point-to-Point Tunneling Protocol (PPTP) as the best fit for a VPN / Extranet solution.
Under the ADOT / Microsoft Enterprise Agreement, the VPN software could be deployed at no additional cost to the Department.
After careful research and analysis, the necessary hardware to support this configuration was purchased and installed.

A year prior to the inception of the aforementioned VPN project, ITG's Data Security Group was championing a task to strengthen remote, dial-up networking security via the use of a portable challenge / response token card devices.
VPN security was not a concern to the Token Card plan because:

1) The principal focus was Dial-up clients.
2) The VPN process had not yet been born.

After the challenge / response server, clients *and* VPN solution were implemented, ITG received a directive from the Office of the CIO, that all remote users be required to use the CRYPTOCard for network logon and authorization.

PC/LAN's Server Team and Systems Architecture began testing the Token Card logon process with Microsoft's VPN. It was concluded from these tests that the two systems were incompatible.

The hardware token card's method of logon uses an authentication process known as Password Authentication Protocol (PAP). With PAP, the username and password are transmitted over the network in clear, unencrypted text. Although this is usually the least secure logon process, the challenge / response server's rolling code technology and one-time password make the system extremely secure.

In contrast, the Point-to-Point Tunneling Protocol that Microsoft's VPN employs relies on MS-CHAP. Short for Challenge Handshake Authentication Protocol, this type of authentication requires an authentication agent (typically a network server) which sends the client program a key to be used to encrypt the username and password. Because the MS-CHAP logon process is encrypted in this way, the challenge / response authentication method of clear-text communication cannot be transmitted over the same, encrypted channel.

With the obstacles described above and for the reasons below, it was decided that a new, compatible VPN solution should be engineered.

1. The challenge / response token devices had already been widely distributed and in use for almost two years.
2. The Token Ring Network connecting the VPN server to the Internet was converted to an Ethernet Network. With a ubiquitous Ethernet interface available, the variety of VPN hardware options is much greater.
3. All of the hardware used in the Microsoft VPN solution will be entirely redeployed in other needed capacities. Three of the servers are already in use, serving ADOT's network as a platform for the firewall.

Research began in April of 2001 and multiple vendors' VPN / Extranet hardware devices were brought into the lab for evaluation and testing. The results of the testing have been included with this document, for review.

Microsoft VPN

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 auto sensing 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 Master Switch Plus	$525	$2,100
		Subtotal	**$68,929**
		Tax 7.5%	**$5,170**
		Total Hardware	**$74,099**

Software		Unit Cost	Total
1	Smart Start 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
		Subtotal	**$10,351**
		Tax 7.5%	**$776**
		Total Software	**$11,127**

Nortel VPN

Part Number	Description	Quantity	Retail Price	Discount	Extended
DM1401053	Contivity 2600, 1000 tunnels, 3 PCI Expansion Slots, Dual 10/100 Ethernet LAN Ports, Server S/W with (128-bit) Encryption, Unlimited license for IPsec Client S/W (Includes Documentation). No Power Cord Included. (See Note 1)	2	$20,000.00	30%	$28,000.00
DM0004003	128 MB RAM Upgrade (FACTORY INSTALL), for use/sale in the Contivity 2600 Only.	2	$1,250.00	30%	$1,750.00
DM0011051	Encryption Accelerator Card (FACTORY INSTALL) for use in the Contivity 2500/2600/4500 only. See Note 5 and 10.	2	$3,050.00	30%	$4,270.00
					$34,020
				Tax	$2,551.50
				Total	**$36,571.50**

References

[1] Internet.com Webopedia. 30 October 2001 <http://www.webopedia.com/TERM/t/tunneling.html>

[2] Configuring_VPN_Switch.pdf. Nortel Networks: 102

[3] Configuring_VPN_Switch.pdf. Nortel Networks: 150

[4] Internet.com Webopedia. 30 October 2001 <http://www.webopedia.com/TERM/D/DES.html>

[5] Netaction.org. 31 October 2001 <http://www.netaction.org/encrypt/appendixb.html>