

# Virtual Private Network Workgroup Report

March 2006

## *Executive Summary*

Students, staff and faculty increasingly connect to the campus data network via the Internet. The need to access university resources is likely to increase dramatically with the implementation of projects such as Sakai, and VPN services appear to offer solutions to related remote access requirements. Additionally, VPN services provide a secure method of improving remote access to licensed material and other university resources restricted to systems assigned a campus IP address.

The workgroup examined available VPN technology and believes that SSL VPN solutions reflect a cost-effective and capable VPN solution for UC Davis. The workgroup recommends Information and Educational Technology prepare a Request for Information for an SSL VPN solution. As part of the RFI process, the workgroup further recommends that IET perform a pilot test using SSL VPN solution(s) that meet RFI specifications to ensure product conformity with our requirements for infrastructure and campus unit services and performance.

The result of examination and successful testing should be a Request for Quote that permits a phased implementation based on campus size, but that does not make a commitment beyond an initial implementation level that includes current library proxy users and those users who are denied access to university resources due to network source address restrictions.

## *Project Background*

In December 2005, the Interim Vice Provost, Information and Educational Technology, appointed a workgroup to review Virtual Private Network (VPN) technology and suggest if this technology should be applied to serve UC Davis. The workgroup was also requested to address the following tasks:

1. Identify the security problem(s) that are resolved by a VPN service.
2. Review the campus remote access connectivity requirements.
3. Discuss how VPN services are able to meet such requirements.
4. Provide recommendations regarding VPN use at UC Davis, operational and policy prerequisites for establishing a campus VPN service, protocol use, network integration and an estimate of the financial, program and personnel resources required to implement and support any recommended campus VPN service.

The workgroup included representatives from the College of Agricultural and Environmental Sciences, College of Letters and Science, Desktop Enterprise Solutions, Network Operations Center, Office of the Vice Provost, Information and Education Technology, Plant Sciences and University Library (See Appendix A for participant listing).

### ***Use of VPN Services***

Institutions have an obvious need to link their satellite sites, individual home users and travelers securely to centrally located services on the institutional intranet. Security was once achieved by creating and using actual private networks. Leased circuits connected dispersed installations. Modem pools economically linked home users in the immediate area and were available at long distance rates to commuters and travelers. When public Internet Service Providers began offering broadband connections, institutions realized significant cost savings with one significant disadvantage: a loss of the security that derives from controlling the physical network. The industry solution was to create “virtual” rather than actual private networks that operate over the public Internet.

The most common applications of VPN technology involve linking dispersed institutional sites to institutional headquarters, extending the institutional intranet to the extranet of partners, business customers, or suppliers, and providing remote access to the institutional intranet. This report focuses on remote access to the institutional intranet, noting that extranet extension can be treated as a special case of remote access.

### ***How Remote Access VPN Works***

All VPN technologies establish a trust relationship based on an authentication procedure. VPN traffic can be encrypted and hidden instead of being passed as clear text. A distinguishing characteristic of VPN technologies is whether or not a network layer tunnel is created for the traffic. This report will compare the advantages and disadvantages of two alternative VPN technologies, IPSec and SSL with only brief remarks on the other available VPN solutions. The workgroup chose to focus on IPSec and SSL VPNs due to broad marketplace acceptance and adoption of this VPN technology.

#### ***IP Security (IPSec):***

IPSec is a peer-negotiated network layer protocol that can be implemented in one of two modes, transport mode or tunnel mode. Tunnel mode protects not only the payload of the IP datagram, but also the entire IP datagram by, optionally, employing Encapsulating Security Payload protocol on the original IP datagram and by adding an Authentication Header. A number of encryption

standards and authentication methods can be employed. Transport mode protects only the IP packet payload.

IPSec can conveniently be used to link dispersed institutional sites using router-based transport mode, but VPN implementations for individual computers require installation of a client program on the end-user machine. Client software can only be installed on machines that are controlled by the University or machines on which the end-user has administrator rights. This restriction renders IPSec of limited use to travelers using kiosks or guest access on other networks. Client software is specific to operating system and computing platform and clients have to be configured for specific ISPs and network configurations. The client software configuration can be confusing to end-users and, accordingly, help desk support costs can become elevated. IPSec uses the IP source and destination addresses and can be incompatible with many NAT (Network Address Translation) implementations. Moreover, IPSec trouble-shooting time may increase, as end-users often have no knowledge of whether NAT is in use at their remote location.

#### *Secure Socket Layer (SSL) VPN:*

In contrast, an SSL VPN uses the familiar SSL/TLS application layer security protocol. This protocol was originally designed to enhance the security of web traffic by encryption and authentication. SSL is implemented through every web browser without the need for additional client software. Because of SSL's focus on securing streams of data between web client and server, sophisticated vendor VPN implementations let administrators assign remote users to different authorization zones that can be used to determine the host and application access for remote users. Non-web applications can be made available through agents (commonly Active-X controls or Java applets) that are downloaded to the end-user computer. A similar approach is deployed by many SSL VPN vendors for endpoint security verification (security patch and anti-virus update checks on a remote computer). The most advanced vendor implementations offer VM (virtual machine) technology to enhance remote computer security.

The advantages of IPsec versus SSL VPN technology is compared below in Figure 1.

Figure 1  
Remote Access VPN Technology Summary

	IPsec VPN	SSL VPN
Advantages	<ul style="list-style-type: none"> <li>Existing Juniper firewalls support IPsec VPN services</li> <li>Transparent access to institutional network</li> <li>Supports endpoint security function</li> </ul>	<ul style="list-style-type: none"> <li>Only a web browser is needed to initiate a VPN session</li> <li>Poor connections will not cause VPN to fail</li> <li>Transparent access to applications</li> <li>Lower support costs</li> <li>Compatible with most ISPs, home networks and remote locations</li> <li>Supports endpoint security function, for OS, browser cache clean-up, malicious code scan, anti-virus scan, host firewall rules</li> <li>Supports zone-based authorization</li> </ul>
Disadvantages	<ul style="list-style-type: none"> <li>Client software required on end-user computer</li> <li>Higher support costs</li> <li>May not work with all ISPs, home networks and/or NAT firewalls</li> <li>May not work from remote locations</li> </ul>	<ul style="list-style-type: none"> <li>Additional hardware and training costs.</li> <li>Not as mature of a technology</li> </ul>

*Other options:*

The workgroup chose not to consider PPTP (Point-to-Point Tunneling Protocol) and L2TP (Layer 2 Tunneling Protocol), server-intensive Microsoft-centric technologies that are not well adapted to the current campus infrastructure. Individual departments may find them easy to economically implement within their limited trust domains using existing servers. These solutions may not be easily scalable or present a number of support challenges. While a small number of departments have implemented such VPNs, the workgroup recommends that

campus units carefully evaluate whether such solutions support the desired VPN features listed further in this report.

### ***Potential VPN Problems***

A simple tunnel between a client computer and an intranet brings all client traffic to the institutional network. The client computer receives an institutional IP address for the client traffic as it passes from the institutional network onto the greater Internet. Assigning a campus IP address to a remote computer can be beneficial. This network assignment permits the remote VPN system to access campus resources, such as library resources and patch management services, that are traditionally limited to computing systems connected to the campus network. However, this assignment also increases commercial bandwidth costs to the University, lengthens network transit times for users and presents other implications.

VPN connections rely implicitly on “trust” between the server and the end-user machine established through an authentication procedure. While there may be reason to trust the individual’s identity, there is no guarantee that the user’s computer is worthy of trust. Allowing the machine transparent access to the university network may expose the institution to viruses or malicious intrusions by individuals controlling the compromised remote machine through backdoor exploits. Allowing a compromised remote computer to use a campus IP address to access Internet sites could appear to the Internet community that the university network is hosting malicious network traffic. As a means to ensure the remote computer meets specific security standards, a number of VPN solutions now employ a service that evaluates the security of a remote computer before permitting the computer to establish a VPN connection. Such measures are often referred to as “end-point” security services.

It is often more desirable to use a “split tunnel” to separate traffic from a remote computer between the campus and the Internet. This function permits campus-bound encrypted traffic to appear with a university network address and all other traffic to use the computer’s local network interface. It should be noted that VPN traffic split in this fashion may fail to provide transparent access to university-licensed e-journals, a powerful incentive to use VPN, and, without an end-point security service, does nothing in itself to secure the campus network against virus transmission or backdoor exploits.

### ***Survey of Higher Education Implementers:***

Other UC campuses have implemented IPsec VPNs and their instruction pages reflect a variety of encountered problems. These problems included the lack of a working IPsec software client for specific operating system platforms, difficulty in performing client software updates, the need to purchase home routers to

respond to predominant local ISP's broadband technology, VPN reconfiguration for specific ISPs and the inability to use the technology at all in some environments.

The workgroup contacted two universities that were early adopters of IPsec VPN technology, Oregon State University and the University of Miami. Their experience provides anecdotal evidence that IPsec implementation may be peaking and SSL VPN implementation growing. Both OSU and Miami substantially reduced help desk utilization with the introduction of SSL VPN. Both cited a particular SSL VPN feature, the ability to place end-users in security zones appropriate to their level of authorization. At Miami, a minimum authorization zone was employed to provide a campus IP address with which licensed resources on the Internet could be accessed without the use of a proxy server.

### ***Potential UC Davis use of a VPN***

The workgroup identified two desirable uses of a UC Davis VPN for remote users. First, there is a campus unit need for VPN services. Faculty and staff working at home or other remote locations need secure access to departmental servers to access departmental and personal files. In the conduct of University business, they need to send email to campus or elsewhere from their departmental server account rather than from an account elsewhere. Encryption of their traffic would be desirable.

Second, VPN services provide remote user access to institutional resources. A campus VPN would enable remote access to sites that cannot be reached using the existing library proxy service. For example important, expensive chemistry and art databases require special client software and some prestigious e-journals are inaccessible using the library proxy servers. SSL VPNs should permit remote access to these restricted sites.

### ***Desired VPN Features***

The workgroup found that the following characteristics are necessary for a successful UC Davis VPN implementation:

- 1. Available to all CyberSafe remote computers.* Every vendor supported end-user platform should be able to use the VPN service, but VPN access from computing systems that are or can be compromised should be denied.
- 2. Easily supportable.* VPN implementation must not substantially increase help desk utilization or costs.

3. *Integrate with existing authentication/authorization infrastructure.* The log-in procedure should be simpler and less confusing than current proxy login.

4. *Security that is not “one size fits all”.* The ability to assign remote users to security zones based on authorization groups is highly desirable in many circumstances. For example, SSL VPN technology could be used to enhance campus wireless security through the assignment of users to trusted and untrusted zones depending on their affiliation.

5. *Granular administration.* A VPN implementation that permits administrative delegation in an environment of central control would be highly desirable. A vendor solution that permits departmental participation through independent purchase of compatible equipment may also be acceptable.

6. *Split tunnel services.* Split tunnel services should be supported by a campus VPN implementation.

7. *Browser support.* The SSL VPN solution must be compatible with current Internet Web browsers, including Internet Explorer, Safari, Netscape, Opera and Firefox.

8. *Monitoring and logging.* Monitoring should go beyond the indispensable network utilization and error reporting level. Any VPN solution has to provide logging that is integrated with syslog services. In the case of DMCA violations, the University must be able to remove access to infringing files upon notification. For resources licensed by the UC Office of the President and the Davis campus, the University is obligated by contract to remedy abuses or suffer penalties that could include denial to future resource access for all campus users. For those reasons, it is necessary to associate user identity and activity. The obligation to remedy abuse is a requirement for departments even if they manage VPNs independently.

9. *Scalability.* It should be possible to begin small and economically increase capacity without degrading performance. Technical details relating to interoperation with the existing VLAN infrastructure may contribute significantly in this respect.

10. *Hardened.* The VPN platform should have a hardened operating system and firmware that provide no opportunities for exploits.

11. *Operation 24x7x365.* Every hour of the night and day, some UC Davis affiliate uses campus resources remotely, so we require a high availability platform. An active/passive configuration would provide fail-safe operation if a load balancing active/active configuration was unaffordable.

12. *Supported.* As a core service, VPN would require 24x7 vendor telephone support and 24x7 hardware maintenance availability.

The workgroup identified one feature, *Endpoint Security Integration*, which will require further analysis. While end-point security is a highly desirable function for entry to the campus network, the ability to check an operating system version, application of security patches or the currency of anti-virus detection files would likely benefit the campus as part of a broader offering, integrated into network access for wired, wireless and VPN services. Nonetheless, some SSL VPN products are capable of using the endpoint security services to check for specific programs and files needed for interoperation with particular servers and services.

### ***Preliminary Cost Examination***

The workgroup invited two leading SSL VPN solution vendors to provide presentations about their offerings with particular attention to general design, deployment issues, maintenance issues, support requirements and both initial and on-going costs.

The vendors were selected based on the Gartner Group's designation of companies falling in its magic quadrant. The magic quadrant's x-axis is labeled "completeness of vision" and its y-axis is designated "ability to execute". The four resulting quadrants are 1) niche players (lower left), 2) challengers (upper left), 3) visionaries (lower right), and 4) leaders (upper right). Our invited vendors were the "leaders" in the SSL VPN field.

From workgroup discussion, it was clear that existing products could fill our needs and provide the granular administrative flexibility needed for overall control without losing the ability for departments to be the ultimate arbiters of their own server security.

Rather than base our cost estimates on vendor-suggested percentages for a fully-implemented system based on campus population, we attempted to determine the scale of an initial, basic implementation, using modem line usage and the library proxy service. After years of not being able to provide sufficient modem lines to meet demand for dial-up access to the central campus network, figures show very significant declines in modem lines without evidence of unsatisfied demand. Students and faculty have found alternatives to campus-provided modem service, recognizing increased value in higher bandwidth despite its higher cost. Using statistics for the proxy server from Fall 2005 to date, we found the highest number of unique users per hour was 169 and the average was 51. Hourly utilization of departmental VPN connections remains a significant unknown, but we concluded that hardware for 500 concurrent users (\$94,000 one-time costs and \$40,000 annual costs) should be sufficient initially for a centralized campus service. Counterbalancing any VPN expenditure would be the possibility of reducing or outsourcing campus modem pool service after the VPN service moved into production.

It should be noted that there is an open source SSL VPN solution, OpenVPN. OpenVPN was first released in 2001 and is available for Windows, Mac OSX, Solaris and BSD operating systems.

***Recommendations:***

The workgroup recommends Information and Educational Technology prepare a Request for Information for an SSL VPN solution. As part of the RFI process, the workgroup further recommends that IET perform a pilot test using SSL VPN solution(s) that meet RFI specifications to ensure product conformity with our requirements. The pilot would permit testing of extending SSL VPN services to a campus unit participant for local file sharing and service access needs.

The result of examination and testing should be a Request for Quote that permits a phased implementation based on campus size, but that does not make a commitment beyond an initial implementation level.

A basic initial implementation would allow IET and selected departments to design, test, and document procedures necessary for the delegation of departmental security to departmental staff. By including as initial users those unable to use the existing proxy service, campus technical staff would be confronted with the most difficult problems to be surmounted and documented prior to a general rollout and user instructions could be created that will minimize the need for assistance by typical users.

In the report, we note that there is existing departmental usage we cannot estimate as well as existing unmet needs that a VPN service would accommodate. We suspect future campus requirements to grow as additional departments take advantage of a campus service they are not now providing themselves. The development of Sakai and its use in instruction may increase further the need for VPN services. Whatever future needs may be, VPN offers the possibility of increased security now.

The use of the Internet by students, staff and faculty to connect to the campus data network continues to grow. The establishment of a campus virtual private network (VPN) service would provide a secure method by which to access the campus network from the Internet. VPN services could also improve remote access to licensed resources and other university resources restricted to systems assigned a campus IP address.

## Appendix 1: List of Workgroup Participants

Tom Arons, Office of the Vice Provost, Information and Educational Technology

Adam Getchell, College of Agricultural and Environmental Sciences

Kevin Kawaguichi, Network Operations Center, Information and Educational Technology

Rob Kerner, Plant Sciences

Karl Kocher, University Library

Minh Nguyen, College of Letters and Science

Robert Ono, Office of the Vice Provost, Information and Educational Technology

Dan Rackerby, Data Center and Client Services, Information and Educational Technology

## Appendix 2: Additional References

IPSec VPN Use at Carnegie Mellon University

<http://www.cmu.edu/computing/documentation/VPN/>

SSL VPN Central

<http://www.sslvpn.breakawaymg.com/index.php>

SSL VPNs Dissected

<http://www.networkworld.com/reviews/2005/121905-ssl-test-intro.html>

VPN Decision Guide, IPSec or SSL VPN Decision Criteria, Juniper Networks

[http://www.juniper.net/solutions/literature/white\\_papers/350037.pdf](http://www.juniper.net/solutions/literature/white_papers/350037.pdf)