

# Virtual Private Networks

## Improving network security for a diverse user community

---

- VPN's Role
- How IPSec VPN Works
- How SSL VPN Works
- Security Strengths and Weaknesses
- Choosing Between IPSec and SSL

Virtual Private Networks (VPNs) have become a critical security tool for higher education institutions as an increasing number of professors, staffers and students require access to the campus data network over the Internet.

VPNs allow IT departments to create a private tunnel over the Internet, so remote users or users in satellite campuses can securely connect and transmit data to the main campus' local area network (LAN). VPNs authenticate users and then encrypt the traffic between their computers and the college network.

The two dominant VPN technologies — IPSec (Internet Protocol Security) and SSL (Secure Sockets Layer) VPNs — have their strengths and weaknesses. Some educational institutions have deployed one or the other, while other colleges are choosing to take advantage of both, giving their diverse community of users multiple ways to connect to the campus network.

To help you determine which VPN works best for your campus, this white paper will explain the different VPNs available, their advantages and disadvantages, and the latest technological advances.

### VPN's Role

VPNs have two common uses: remote access for users and site-to-site connectivity. There are two types of site-to-site connections. An intranet VPN links users from satellite offices to the main network, while an extranet VPN connects outsiders, such as partners, contractors or suppliers, to the LAN.

In the past, before the Internet explosion, universities and colleges had limited ways to extend their LANs beyond their campus' boundaries, and those methods were either difficult to manage or cost prohibitive. Colleges, for example, subscribed to costly leased

Higher  
Education

Sponsored by



## Layers of Security

Some SSL vendors offer the following layers of security:

- Check for malware and keyloggers before log-in.
- Encrypt all data on the hard disk and in memory using AES encryption during the session to render any local snooping during or after the session futile.
- Delete the cache, temporary files, usernames and passwords when the session ends with a Department of Defense-approved cleaning algorithm.

Ultimately, it's not wise to try to determine whether IPSec or SSL VPNs are more secure because it all depends on an IT department's implementation, says Lisa Phifer, vice president of Core Competence Inc., a network and security consulting firm in Chester Springs, Pa.

"You really need to access a particular product, the policies configured into that product and the way users use the product," she says. "It's possible to implement a weak IPSec VPN or a weak SSL VPN – or to deploy either type with sufficiently strong security."

lines to connect different sites together. They also installed remote access servers, featuring modems that users dialed into to connect to the LAN.

But the Internet's growth has changed everything. In the 1990s, the technology industry introduced VPN technology using IPSec as a more cost-effective way to connect offices in different locations. Enterprises also began using IPSec for remote access for individual users.

An IPSec VPN requires users to download, install and configure a software client onto their computers before they can establish a secure connection with their campus networks. Today, IPSec VPNs have the largest installed base because it was the only VPN technology available for the longest time.

In recent years, a new VPN technology that uses the SSL protocol has captured the limelight and seen its market share skyrocket. The biggest benefit of SSL VPNs is ease of use. Instead of requiring users to install a separate software client, SSL VPNs allow users to connect through standard Web browsers. SSL is an encryption technology that is embedded in browsers, such as Internet Explorer and Firefox.

With VPNs, students can get secure remote access to their e-mail and also get personal files from their departments' file servers and library servers. They can even send print jobs to campus printers. Likewise, staffers can connect to critical business applications and data, while faculty can access online gradebooks and other educational applications.

VPNs can also bolster security for open-campus Wi-Fi networks. They can protect voice traffic for colleges that have deployed Voice over Internet Protocol (VoIP) and allow professors and staffers to access their office phone numbers from home or while traveling. VoIP transmits digitized voice as a stream of data, so it's protected by encryption like other data packets.

### IPSec VPN: How It Works

IPSec VPNs, which authenticate and encrypt at a network layer, excel at securing site-to-site tunnels, applying a consistent security policy at the network edge and supporting high-speed bulk encryption for IP traffic exchanged between networks, such as a satellite campus network to a main campus network, says Lisa Phifer, vice

president of Core Competence Inc., a network and security consulting firm in Chester Springs, Pa.

IPSec can provide one "big tunnel" to support all users between a branch and a central site, says Nortel engineer Bob Gaughan. In contrast, SSL VPNs operate at the application layer. If organizations want to do site-to-site connectivity with SSL VPNs, every user would have to establish individual SSL connections.

IT administrators can encrypt IPSec traffic using two modes: transport and tunnel. In transport mode, only the data portion of the traffic is encrypted and the IP header is untouched. Tunnel mode is more secure because it encrypts both the data packet and the IP headers.

When remote users are connected via an IPSec VPN, the data is encrypted and transferred over the Internet, and once it's received by the VPN gateway device on campus, the data is decrypted and routed to the correct server destination.

In an IPSec solution, the network handles traffic from the VPN gateway as if it came from any other user connected directly on the LAN. As a result, remote users can access everything they normally could access when they are on campus. IPSec is ideal for users such as IT administrators, faculty and staff members, who regularly need full access to their applications and data.

The technology does present some challenges. Because it requires a client installed and configured on users' computers, managing and troubleshooting IPSec VPNs can become expensive and a time-consuming task for the help desk, particularly in college campuses where the number of users can reach 20,000 to 30,000 people. "The diversity of student-owned systems makes it very challenging, if not impossible, to provide every student with IPSec access," Phifer says.

In addition, IPSec doesn't work if students need to connect through a public computer, such as at a public library, because they won't be allowed to download the client.

Colleges would also need to ensure that their IPSec VPN vendors support a myriad of computers and operating systems, including Windows, Macintosh and Linux. "They require installation, configuration and maintenance, increasing total cost of ownership in direct

proportion to the size of the remote-user work force," Phifer says.

## SSL VPN: How It Works

SSL VPNs, which first came to market four to five years ago, allow users to simply launch their Web browsers to securely connect to the campus LAN. As noted earlier, IPSec VPNs operate on the network layer, while SSL VPNs work on the application layer, giving IT administrators the ability to more easily manage application and data access. SSL VPN appliances are usually installed within the DMZ (demilitarized zone) and behind a perimeter firewall.

Today, some Internet service providers block IPSec connections, and subsequently users who need to connect via an IPSec VPN. SSL VPN users have no such problems because SSL VPNs use commonly used Web ports, 80 or 443, for communication, says Jon Kuhn, SonicWall's director of product management.

SSL VPNs are much easier to deploy than IPSec VPNs, particularly in environments where IT departments have little or no control of client devices — a category that students fall into, Phifer says. SSL VPNs reduce help-desk costs because users don't have to download, install, configure — or update — software clients.

SSL VPNs also provide good management tools that allow IT administrators to easily configure access to applications. For example, IT staffers can give employees full access to applications if they have to work from home or on the road, while limiting students to a few specific applications. The level of granular control makes the technology easier for IT administrators and safer for the campus as a whole.

Some SSL VPNs allow IT administrators to develop portal sites. So once users are connected through a VPN, they are directed to a portal that shows all the applications and data that they access, says Forrester Research analyst Robert Whiteley. "You can give each their own tailored look and grant them different authorization policies," he says.

SSL VPN's primary weakness is its breadth of application support, Phifer says. While simple Web-based applications can be supported by an ordinary Web browser, support for more complex applications requires other techniques, which make SSL VPNs more complicated.

SSL VPN vendors support access to client-server applications, Citrix and Microsoft Terminal Services, but it requires SSL VPN users to download ActiveX or Java applets to access those applications. The applets are removed from the computer at the end of the session.

For users who need network-layer-like access, some SSL VPN vendors allow users to download from their Web browsers a full client similar to those used for IPSec VPNs to give users full application access.

## Equal Encryption Strength

When it comes to VPN encryption technology, IPSec and SSL are both flexible in the security standards they support, from the Triple DES (Data Encryption Standard) algorithm to the stronger AES (Advanced Encryption Standard). From an integrity standpoint, the encryption strength of both is equal.

Both types of VPNs also allow IT departments to bolster authentication beyond usernames and passwords by using key fobs, such as RSA SecurID tokens.

In some colleges, VPNs are configured to permit the use of "split tunneling," which separates traffic when remote users are connected to the campus LAN. In this scenario, data traffic that is campus bound is encrypted, while all other traffic — such as general Web surfing — goes through users' ISPs.

Split-tunnel connections can save campus bandwidth, but leave the campus network vulnerable against virus transmissions and backdoor exploits. IT administrators need to secure split tunneling by using "endpoint" securities, such as firewalls. Some SSL VPN vendors, for example, build in a firewall to specifically protect split tunnels.

## IPSec Security

Both technologies have their strengths and weaknesses when it comes to security. Because IPSec operates at a lower layer, it is inherently more resistant to Denial-of-Service (DoS) attacks, Phifer says. But IPSec access to an unmanaged student device raises security concerns. Colleges don't want to give network-layer access to a device that has been infected.

## SSL VPN Drivers

Increase security: 80 percent

Decrease network downtime: 51 percent

Enable clientless VPNs: 46 percent

Increase network capacity/performance: 41 percent

Decrease operating cost: 41 percent

Collaboration with remote users: 41 percent

Extend the life of the network: 38 percent

Support a wide variety of client platforms: 38 percent

Enable a new application: 30 percent

Enable employee access from handheld devices: 29 percent

Enable employee access from kiosks and guest computers: 23 percent

Add extranets: 20 percent

Source: Infonetics Research

---

To protect the campus network, IT departments need to have security layers, such as firewalls, antivirus software and intrusion detection and prevention systems deployed. And because IPSec VPNs grant full access to networked resources, IT administrators need to pare down access to some users through Access Control Lists (ACLs) or by segmenting the networks.

## SSL Security

SSL VPNs are the opposite. Users only get access to applications that IT administrators give them rights to. While SSL VPNs offer more convenience, they have their own security risks because users can connect from any machine. Students, for example, can connect from computers in public libraries or at their friend's houses. Security on these computers is not assured. In addition, if students' usernames and passwords are stolen, people can hack into their accounts.

To protect remote access, SSL VPN vendors offer additional security by allowing administrators to control user access depending on the users' need for access to applications, the device they are coming from, their location, as well as whether the device they are using meets campus security guidelines.

For example, SSL vendors offer management software that makes it easy for IT administrators to develop policies on the specific types of applications and data that students, faculty and staff can access while connected to a VPN.

SSL VPNs offer "host checking," which can lead to "granular access control," meaning the VPN inspects the security of users' computers, such as whether they are running firewalls or have updated antivirus signatures, says Charles Goldberg, product marketing manager at Juniper

Networks. If computers are missing security software or patches, the IT department can direct the VPN user to download the latest signatures or patches before they can connect to the campus network.

SSL VPNs also can check if employees are on their known campus-owned notebook computers, on their home computers or at airport kiosks. IT administrators can create policies that give users full access if they are connecting from their school-owned notebook computers and perhaps limit access to applications if they are on a public computer, Goldberg says.

## Choosing Between IPSec and SSL

Today, about 80 percent of large enterprises have deployed IPSec VPNs and another 45 to 50 percent have installed SSL VPNs, meaning some enterprises are deploying both, says Forrester analyst Whiteley.

"We're in a transition period because the awareness of SSL is not real high," he says. "In the next few years, we will see colleges support both, but most universities I've talked to are phasing out IPSec and switching to SSL."

While IPSec has the market share, SSL has the momentum as vendors continually add new features into their SSL VPN products, such as granular access control and endpoint securities. Recent advances include support for mobile devices, such as personal digital assistants and smart phones.

Analysts and security experts say IPSec is best for site-to-site connectivity, while SSL is best for remote user access. In a university scenario, SSL VPNs make more sense because IT administrators can more easily restrict network and application access, says Tony Bradley, a security consultant

and owner of Internet and network security firm S3KUR3 Inc., in Houston.

"I would picture professors and students needing access to particular applications and not having a situation where you want to give people carte blanche access to a network," Bradley says.

"If you're using IPSec, you can segregate off parts of the network, but it seems like it would result in more overhead than SSL without any added benefit."

SonicWall's Kuhn says it makes sense for colleges to offer both options to users, depending on their computing needs. For example, administrators or faculty members who are outfitted with notebook computers, and need full network access, can connect through IPSec. Students should connect through SSL because they are typically less secure as a user group.

## Summary

Today, institutions of higher education house tremendous amounts of sensitive and private information, from students' financial and educational records and faculty research data to employees' Social Security numbers. IT administrators face a difficult task in securing the network, while simultaneously providing the remote access that its diverse community of users need.

For optimal security, IT departments must deploy layers of security throughout their technology infrastructure, and VPNs play a huge role through their ability to create secure tunnels between users' computing devices and campus servers. Whether you choose IPSec, SSL or both, the result is secured data transmissions for remote users. ■