SearchSecurity.com

Choosing between an SSL/TLS VPN vs. IPsec VPN

By Lisa Phifer

If your organization struggles with managing its IPsec VPN, going clientless can sound compelling -- SSL/TLS-based VPNs can be much easier to deploy and manage. The key is deciding when to use IPsec and when to use SSL/TLS. There isn't necessarily a right or wrong answer. In fact, in many enterprises, it isn't an SSL/TLS VPN vs. IPsec VPN; it's an SSL/TLS VPN *and* IPsec VPN.

Both IPsec and SSL/TLS VPNs can provide enterprise-level secure remote access, but they do so in fundamentally different ways. These differences directly affect both application and security services and should drive deployment decisions.

IPsec VPNs protect IP packets exchanged between remote networks or hosts and an IPsec gateway located at the edge of your private network. SSL/TLS VPN products protect application traffic streams from remote users to an SSL/TLS gateway. In other words, IPsec VPNs connect hosts or networks to a protected private network, while SSL/TLS VPNs securely connect a user's application session to services inside a protected network.

IPsec VPNs can support all IP-based applications. To an application, an IPsec VPN looks just like any other IP network. SSL/TLS VPNs can only support browser-based applications, absent custom development to support other kinds.

Before you choose to deploy either or both, you'll want to know how SSL/TLS and IPsec VPNs stack up in terms of security and what price you have to pay for that security in administrative overhead. Let's compare how IPsec and SSL/TLS VPNs address authentication and access control, defense against attack and client security, and then look at what it takes to configure and administer both IPsec and SSL/TLS VPNs, including client vs. clientless pros and cons and fitting VPN gateways into your network and your app servers.

Authentication and access control

Accepted security best practice is to only allow access that is expressly permitted, denying everything else. This encompasses both **authentication**, making sure the entity communicating -- be it person, application or device -- is what it claims to be, and **access control**, mapping an identity to allowable actions and enforcing those limitations.

Authentication
Both SSL/TLS and IPsec VPNs support a range of user authentication methods. IPsec employs Internet Key Exchange (IKE) version 1 or version 2, using digital certificates or preshared secrets for two-way authentication. Preshared secrets is the single most secure way to handle secure communications but is also the most management-intensive. SSL/TLS web servers always authenticate with digital certificates, no matter what method is used to authenticate the user. Both SSL/TLS and IPsec systems support certificate-based user authentication, though each offers less expensive options through individual vendor extensions. Most SSL/TLS vendors support passwords and tokens as extensions.

SSL/TLS is better suited for scenarios where access to systems is tightly controlled or where installed certificates are infeasible, as with business partner desktops, public kiosk PCs and personal home computers.

Access control
Once past authentication, an IPsec VPN relies on protections in the destination network, including firewalls and applications for access control, rather than in the VPN itself. IPsec standards do, however, support selectors -- packet filters that permit, encrypt or block traffic to individual destinations or applications. As a practical matter, most organizations grant hosts access to entire subnets, rather than keep up with the headaches of creating and modifying selectors for each IP address change or new app.

SSL/TLS VPNs tend to be deployed with more granular access controls enforced at the gateway, which affords another layer of protection but which also means admins spend more time configuring and maintaining policies there. Because they operate at the session layer, SSL/TLS VPNs can filter on and make decisions about user or group access to individual applications (ports), selected URLs, embedded objects, application commands and even content.

If you really need per-user, per-application access control at the gateway, go SSL/TLS. If you need to give trusted user groups homogenous access to entire private network segments or need the highest level of security available with shared secret encryption, go IPsec.

Defense against attacks

Both SSL/TLS and IPsec support block encryption algorithms, such as Triple DES, which are commonly used in VPNs. SSL/TLS VPNs also support stream encryption algorithms that are often used for web browsing. Given comparable key lengths, block encryption is less vulnerable to traffic analysis than stream encryption.

If you're implementing an SSL/TLS VPN, choose products that support the current version of TLS, which is stronger than the older SSL. Among other benefits, TLS eliminates older SSL key exchange and message integrity options that made it vulnerable to key cracking and forgery.

Beyond encryption, there are some important differences between IPsec VPNs and TLS VPNs that can impact security, performance and operability. They include the following:

- **Handling man in the middle (MitM) attacks.** Using shared secrets for IPsec authentication and encryption completely prevents MitM attacks. In addition, IPsec detects and rejects packet modification, which also thwarts MitM attacks, even when not using shared secrets. It can cause problems if there is a Network Address Translation system between the endpoints because a NAT gateway modifies packets by its nature, substituting public IP addresses for private ones and fiddling with port numbers. However, nearly all IPsec products support NAT traversal extensions.

TLS has some protections against lightweight MitM attacks (those not hijacking the encryption); it carries sequence numbers inside encrypted packets to prevent packet injection, for example, and uses message authentication to detect payload changes.

- **Thwarting message replay.** Both IPsec and TLS use sequencing to detect and resist message replay attacks. IPsec is more efficient because it discards out-of-order packets lower in the stack in system code. In SSL/TLS VPNs, out-of-order packets are detected by the TCP session engine or the TLS proxy engine, consuming more resources before they are discarded. This is one reason why IPsec is broadly used for site-to-site VPNs, where raw horsepower is critical to accommodate high-volume, low-latency needs.
- **Resisting denial of service (DoS).** IPsec is more resistant to DoS attacks because it works at a lower layer of the network. TLS uses TCP, making it vulnerable to TCP SYN floods, which fill session tables and cripple many off-the-shelf network stacks. Business-grade IPsec VPN appliances have been hardened against DoS attacks; some IPsec vendors even publish DoS test results.

Look carefully at individual products and published third-party test results, including International Computer Security Association certifications for IPsec, IKE and SSL/TLS, to assess DoS vulnerability in each implementation.

Client security

Your VPN -- IPsec or SSL/TLS -- is only as secure as the laptops, PCs or mobile devices connected to it. Without precautions, any client device can be used to attack your network. Therefore, companies implementing any kind of VPN should mandate complementary client security measures, such as personal firewalls, malware scanning, intrusion prevention, OS authentication and file encryption.

This is easier with IPsec since IPsec requires a software client. Some IPsec VPN clients include integrated desktop security products so that only systems that conform to organizational security policies can use the VPN.

SSL/TLS client devices present more of a challenge on this score because SSL/TLS VPNs can be reached by computers outside a company's control -- public computers are a particular challenge. Vendors address this in several ways -- for example:

- An SSL/TLS VPN can attempt to ensure there is no carryover of sensitive information from session to session on a shared computer by wiping information such as cached credentials, cached webpages, temporary files and cookies.
- An SSL/VPN can have the browser run an applet locally that looks for open ports and verifies antimalware presence before the gateway accepts remote access.
- Some SSL/TLS VPNs combine client security with access rules. For example, the gateway can filter individual application commands -- e.g., FTP GET but not PUT; no retrieving HTTP objects ending in .exe -- to narrow the scope of activity of those using unsecured computers.

Session state is a dimension of usability more than security, but it's worth noting that both IPsec and SSL/TLS VPN products often run configurable keepalives that detect when the tunnel has gone away. Both kinds of tunnels are disconnected if the client loses network connectivity or the tunnel times out due to inactivity. Different methodologies are used based on different locations in the protocol stack, but they have the same net effect on users.

Client vs. clientless

The primary allure of SSL/TLS VPNs is their use of standard browsers as clients for access to secure systems rather than having to install client software, but there are a number of factors to consider.

SSL/TLS VPNs do a great job making browser-based apps available to remote devices. However, generally speaking, the more diverse the application mix, the more attractive IPsec can become. It boils down to a tradeoff between IPsec client installation and SSL/TLS VPN customization.

Of course, not all applications are browser-accessible. If key applications aren't, the gateway would have to push a desktop agent, such as a Java applet, to provide access -- e.g., to a legacy client or server application. If the environment is rich in such applications, you may spend more time and effort developing or deploying add-ons than you would have supporting an IPsec VPN. The use of such plugins may conflict with other security policies for desktops. Most organizations block unsigned Java, for example, since it can be used to install Trojans, retrieve or delete files and so forth. Some organizations block all active content to be on the safe side. As a result, you may have to reconfigure some browser clients to use an SSL/TLS VPN, which puts you back in the business of fiddling with client configurations.

Most client platforms, including Windows, Mac OS X, Android and Apple iOS, have native support for IPsec. Some gateways may still require third-party client software for advanced functionality, and older clients may not have the native solution. So, be sure to evaluate potential VPNs with this in mind. Installing third-party clients is time-consuming and requires access to the users' devices.

Some vendors offer hardware IPsec VPN clients for organizations that must deal with diverse OS platforms. These small appliances sit between a worker's home PC and cable or DSL (Digital Subscriber Line) modem, acting like an IPsec VPN client. The idea is to invest in hardware upfront to enable administering VPN access via an enterprise-controlled device rather than every client device behind it. Organizations can instead use IPsec-enabled single office/home office firewalls to incorporate teleworkers' LANs into their site-to-site VPN topology.

Policy distribution and maintenance are often hamstrung by user mobility and intermittent connectivity. This is a significant issue for IPsec VPNs. IPsec administrators must create security policies for each authorized network connection, identifying critical information, such as IKE identity, Diffie-Hellman group, crypto-algorithms and security association lifetimes. IPsec vendors provide centralized policy management systems to ease and automate policy distribution, though not always in a way that integrates cleanly with other network security policies and policy domains.

For the most part, security policy for SSL/TLS VPNs is implemented and enforced at the gateway -- SSL/TLS proxy. Thus, there's no user or device involved and no remote management.

Integrating VPN gateways

Server-side issues tend to get lost amid the buzz about clientless savings, but understanding what's involved is essential in VPN product selection, secure system design and cost-effective deployment.

Whether you choose IPsec or SSL/TLS, your VPN gateway will be where the rubber meets the road. Server-side VPN administration is required for both. Network configurations are the main issue for IPsec, and app server management is the problem for SSL/TLS.

IPsec remote hosts become part of your private network, so IT must sort out the following:

- **Address assignment.** IPsec tunnels have two addresses. Outer addresses come from the network where the tunnel starts -- e.g., the remote client. Inner addresses, for the protected network, are assigned at the gateway. IT has to use its Dynamic Host Configuration Protocol or other IP address management tools to provide ranges for the gateway to use and has to ensure any internal firewalls or other security systems allow those addresses access to the desired services.
- **Traffic classification.** SSL/TLS systems enable granular control of access to services at the gateway. Deciding what to protect and then setting selectors to protect it takes time to configure and time to maintain. For example, "HR clients should be able to reach the HR server" must be mapped into the right set of users and destination subnets, servers, ports and URLs and maintained over time as the services change.
- **Routing.** Adding an IPsec VPN gateway changes network routes. You'll spend time deciding how client traffic should be routed to and from the VPN gateway.

SSL/TLS VPNs don't require client address assignment or changes to routing inside your network because they work higher in the network stack. Typically, though, SSL/TLS VPN gateways are deployed behind a perimeter firewall, which must be configured to deliver SSL/TLS traffic to the gateway. By contrast, a perimeter firewall is often the IPsec VPN gateway.

SSL/TLS VPN gateways can have a positive impact on the application servers inside your private network. Should IT staff need to restrict access at a finer-than-firewall granularity -- e.g., user-aware access to a directory on a web server -- they may need to apply OS-level access controls, such as Windows NTFS, and per-user or per-application authentication on the servers themselves. This would control access for staff coming in from company endpoints or via an IPsec or SSL/TLS VPN.

By applying the same granular access controls at SSL/TLS VPN gateways, organizations can offload that security from the application servers. It also enables an organization to enforce uniform policy at the gateway and across internal systems, even if the gateway is redirecting traffic to an external target, like a SaaS service. Citrix NetScaler, for example, can provide a uniform security policy environment for all sanctioned enterprise applications, whether on premises or cloud-delivered.

This fine-grained access control comes at a price: More planning, configuration and verification translates into overhead. And it doesn't eliminate the need for controls on the servers unless all traffic passes through the gateways, so keeping policies in sync is another ongoing task.

The test of time

Will it always be SSL/TLS VPN vs. IPsec VPN? It's quite likely that IPsec will remain attractive for groups needing the highest degree of security, requiring broader access to IT systems or to rich sets of legacy applications, and, of course, for site-to-site connectivity -- now often under the control of an software-defined WAN rather than a VPN. SSL/TLS will continue to be attractive for lower-security deployments or those requiring a single place to control a lot of fine-grained differentiation of access rights for users across multiple systems or those unable to enforce or control use of IPsec.

IT departments should assess the specific needs of different groups of users to decide whether a VPN is right for them, as opposed to a newer kind of system, such as a software-defined perimeter tool; which kind of VPN will best serve their needs; and whether to provide it themselves or contract a VPN service, such as Palo Alto Prisma or Cisco Umbrella.

08 Oct 2019