SSL VPN overview and architecture

Overview

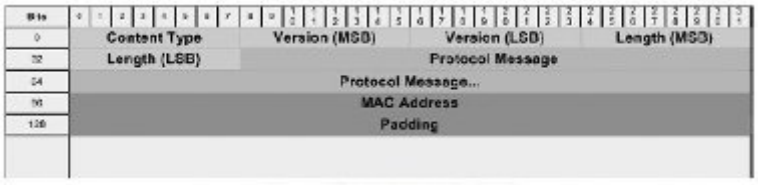
SSL VPN technology has grown in popularity in recent years and like its IPSec counterpart allows users to connect remotely back to their home organisation, obtaining access to restricted network resources. There are several different variants of SSL VPN architecture and an increasing number of vendors and Open Source projects providing solutions.

IPSec VPN technology is used for both end user and site-to-site connectivity. SSL VPN technology is used exclusively for user connectivity where it provides an ideal solution for creating a VPN tunnel through restricted networks back to the home site.

When SSL VPN clients negotiate a connection, they connect using TLS. TLS provides connection-oriented communication as a shim between the application layer and the transport layer to be used over a TCP connection. Since the IETF took over the development of SSL, the terms SSL and TLS are often used interchangeably.

Clients can also negotiate a simultaneous DTLS (Datagram Transport Layer Security) connection to avoid possible latency with time sensitive applications like video and voice. DTLS is a modified version of TLS which provides the same security and protection; however is designed to work with UDP. This may be beneficial where time sensitive applications are required to function over a VPN connection; for example a soft phone on a remote laptop.

DTLS does not provide any reliability, oversize or re-sequencing technology: it is a simple connectionless protocol implementation with security features matching TLS (Figure 13).



[1]

Figure 13. TLS Record Protocol.

The single largest advantage SSL VPN technology has over traditional IPSec is the accessibility of the SSL library and access to port 443 TCP. Whilst IPSec uses a known protocol and associated port, this is often blocked on public access networks along with other tunnelling protocols. Unfortunately it is through these public access networks where users' need for VPN technology is at its greatest. SSL VPN technology will work wherever one can gain access to HTTPS websites such as Internet Banking, Secure WebMail or Intranet sites.

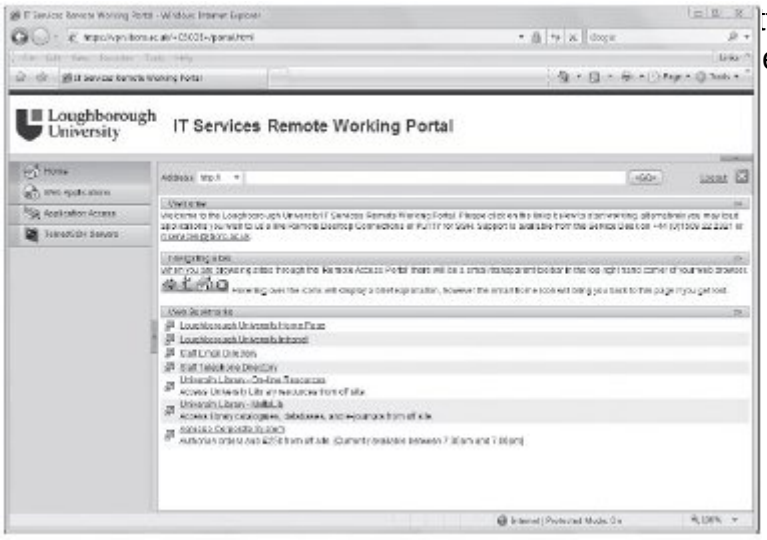
SSL VPN technology is seen by many as easier to configure and administer than IPSec. It also has the distinct advantage that it runs in user space rather than via the close ties IPSec has with the kernel layer.

As SSL VPN technology is relatively new in the market place, whilst clients are available for a large number of desktop operating systems, they are only available for a small number of mobile devices.

Web-Based Portals

Web-based portals allow the user to connect to the SSL VPN concentrator through a web-based interface using simply a web browser and the SSL protocol. This does not require preinstalled client software. All that is required is a web browser. Portals can therefore be accesed from centrally-managed computers and those not managed by the organisation, as well as from kiosk computers.

As organisations strive to make their IT provision more user focused, remote access through form for the remote delivery of services ent configuration (Figure 14).



[2]

Figure 14. SSL VPN web-based portal.

The security of communications is guaranteed by the SSL protocol, achieving privacy, authentication, data integrity and anti replay through functionality already included in the majority of web browsers.

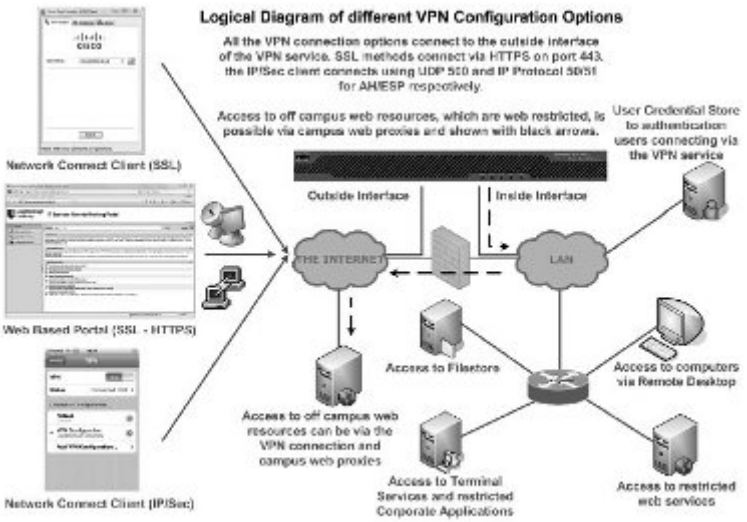
The SSL technology relies on certificates and the public key infrastructure. It is important to ensure that a correctly issued certificate is used for the SSL VPN concentrator, otherwise the user experience will be degraded through multiple certificate errors. Janet can provide appropriate certificates through our agreement with TERENA. Further details are available at:

http://community.ja.net/library/janet-services-documentation/janet-certificate-service [3]

Organisations may want to consider the use of Extended Validation certificates which are becoming popular for e-commerce and financial sites. These certificates are a subset of the

traditional X.509 certificate which requires the issuing organisation to validate the registering organisation more thoroughly before issuing the certificate. The effectiveness of Extended Validation certificates is often debated; however end-user confidence is higher when seeing the green URL bar in recent browsers when one of these certificates is used. This could be a

urces in the web-based portal are the web interface (Figure 15).

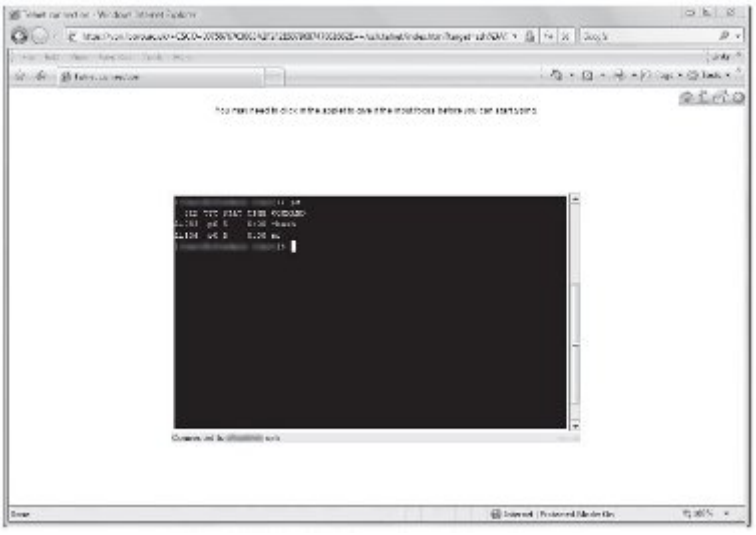


[4]

Figure 15. Logical diagram of different VPN configuration options.

Other applications can be accessed through web-based portals using a combination of modules: SSH, Telnet, RDP, VNC and Citrix are primary examples. These protocols are typically implemented as Java applets for cross-platform compatibility. Not all functionality is

SH Key support is often missing (Figure



[5]

Figure 16 Using SSH through a web-based portal.

As requests for web content through the web-based portal are seen by the web server to come from the internal interface of the SSL VPN concentrator, this will allow access to be given to IP restricted resources on campus. However, since requests from all users will

originate from the same interface address, services cannot distinguish users based on their IP address. Should access be required to off-campus resources that are restricted to an organisational IP netblock, web requests through the portal can be directed through a local web cache/proxy. In the long term it is hoped these cases will diminish as more organisations enrol in the UK Access Management Federation.

Access to filestore can be achieved through a web-based interface to SMB/CIFS shares on servers located in the organisation. The files located on the share are presented as a set of hyperlinks in the web browser which can be used to download and upload content and perform basic file management operations. One noticeable omission from many vendors is the rename a file function.

The majority of web-based portals also include an option to provide either a full network connection or a limited network connection for a number of specific applications on their computer. In the latter case an Active X or Java control creates specific routes on the remote computer to the user's organisation. For example, a connection can be opened to a remote license manager, to use remote printing services or the full Outlook client, without requiring a VPN client to be installed. The functionality of this element is limited and varies greatly between vendors of this software. This shortlived VPN connection is often implemented using what is known as a dissolving client, due to the disappearance of the client once the connection has been terminated, or may be referred to as a smart client or smart tunnel.

Network Connect

Network connect software provides a full VPN client which connects back to the home organisation over SSL TCP port 443. Depending on the software chosen and configuration policy, this can support split tunnel configuration or all traffic from the remote computer can be sent via the home organisation. A lot of the functionality contained within IPSec clients is available in SSL clients as well, offering a full network tunnel with the ease of the SSL client (Figure 17).

[6]

Figure 17. SSL VPN Network Connect process.

The majority of Network Connect full VPN software works in the same way. A TCP connection is made to the SSL VPN concentrator in the first instance to allow an SSL protocol handshake where the SSL certificate for the VPN concentrator is checked for validity. If the certificate has been revoked the connection will be torn down, otherwise minor errors are reported to the user and a correct certificate allows the exchange of user credentials before the tunnel is established. Many vendors also allow automated client updates at this stage. It is important to establish what local rights are required for a client upgrade as this is different from vendor to vendor.

The Network Connect method of SSL VPN is not intended to replace traditional IPSec VPN [illegible] will typically be used for point-to-point hardware links, for example [illegible]re devices cannot support SSL VPN, for example the iPhone

[7]

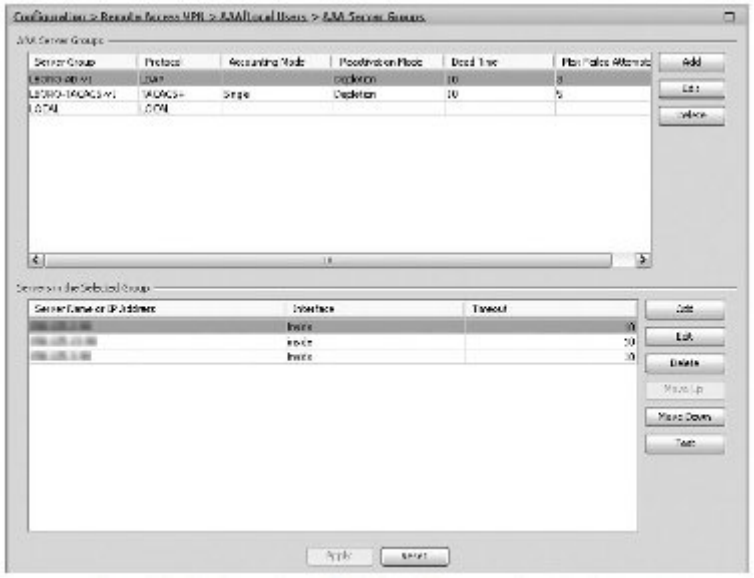
Figure 18. IPSec VPN being used on an Apple iPhone.

Virtual Desktop

An alternative solution to providing a secure desktop environment is to provide a virtual desktop for remote users to access. In a similar fashion to Microsoft Terminal Services and Citrix a remote desktop session is provided on the SSL VPN Concentrator with no traffic passing directly onto the organisational network. Once connected, users interact with the desktop that is sandboxed from the remote computer so no viruses or malicious code can be transferred. The Virtual Desktop provision can also be subject to posture checking (see Section 8.5.1), so that without certain prerequisites the remote user will not be able to gain access.

Additional SSL VPN Security

The primary method of authentication to the VPN concentrator will be via user credentials, typically a username and password. Other methods of authentication can be supported depending on the vendor; this may include two factor authentication supported by biometrics, one-time pass code, RSA key fob and hieroglyphics (Figure 19).



[8]

Figure 19. Configuration of VPN for different authentication methods.

The authentication at the VPN concentrator can be handed off to central authentication repositories: LDAP, Active Directory, e-Directory or RADIUS. For LDAP authentication a Kerberos principal needs to be created for the system to use. This account does not require any special privileges as the VPN concentrator will re-authenticate as the end-user in order to read the user's Active Directory object attributes. This could be implemented using a role-based account for the initial LDAP connection, or access allowable from the VPN concentrator boxes to the LDAP servers. Administration access via TACACS+ (Terminal Access Controller Access-Control System) can be configured to differentiate between using the system and administration.

Any attribute or combination of attributes in the Active Directory can be used to control the ACLs that are applied to Network Connect VPN access and Web portal access. The latter is referred to as 'webtype' for the Cisco ASA. For example Active Directory group membership can be checked (e.g. "memberOf=staff") and ACLs applied accordingly.

As with any VPN technology, the organisational network is extended to the end-user PC. This is dangerous unless managed correctly and the relative ease by which this can be achieved increases the risk. Whilst it is trivial to connect to a web-based portal from any Internet connected computer with a browser, what prevents a user revealing their credentials via a key logger installed on a kiosk PC at a conference or airport lounge? Extend this scenario with the use of a full Network Connect client and there is a possibility that any worm present on the end-user PC will not be attacking hosts internally on your network without that perimeter firewall defence that usually protects the site from Internet-based threats.

Split tunnel functionality is provided by the majority of SSL VPN vendors and provides a method of only routing traffic that is destined for the home site back to the home site. All other traffic goes via the ISP Internet connection. Whilst split tunnelling appears to be an ideal solution, preventing the bandwidth bottleneck of passing all traffic back to the home site, configuration is this way will allow a computer to have a connection to both the Internet and the home site simultaneously, allowing the possible routing of traffic between the two.

If users of the SSL VPN are working with sensitive documents, traces of these will remain on the computer once the VPN connection has been closed. Temporary files, cookies, spooler directories and application data can still be retained on the computer for a long time. User education is still paramount as there are many other methods of information disclosure that are far more likely to occur; for example editing sensitive documents on a train, or leaving sensitive data on an unencrypted USB stick.

With any technology of this nature, security is of concern; however a fine balance between usability and security needs to be achieved. Thankfully there is a raft of additional security measures that may help to mitigate risk in these scenarios.

Posture Checking

Checking the current status of the end-user PC is known by several terms: Posture Checking, Endpoint Security or Client-Side Security. This allows facets of the end-user PC, such as whether its patching and anti-virus measures are up-to-date, to be checked against a central security policy before a connection is allowed to continue.

VPN software can also clean the PC after the tunnel has been torn down; data can be securely removed from temporary files, cookies, spooler directories and application data. One area that cannot be securely erased is any swap space used during the use of the VPN tunnel; however policies can require the paging file to be disabled before a tunnel can be established.

Integrated Network Protection

Some solutions offer integrated network protection technologies. The Cisco ASA product family offers the option of additional modules providing an inline Intrusion Prevention System (IDS (*sic*)) or Anti-X protection.

Inline IDS allows the monitoring of all network traffic passing through the VPN tunnel and mitigation of risk. This could be the prevention of worms propagating through the VPN tunnel or spotting rogue traffic from misconfiguration. Anti-X inspects HTTP protocols looking for malware, viruses or malicious code contained in the traffic traversing the VPN tunnel. This can be intercepted and replaced with benign content or the stream blocked.

When these modules are enabled, the Layer 7 inspection required for the functionality results in increased latency and throughput performance.

Roles and Policies

The SSL VPN concentrator can be configured to provide choices for a number of different configurations, depending upon the user connecting, and which groups they are a member of in the underlying directory system. It is possible therefore to provide access only to central services and the home department, or users of financial systems may be required to use dual factor authentication at login, otherwise they are only able to use a base level of services.

FIPS 140-2 Compliance

Many organisations are now required to install systems which comply with approved security accreditation to obtain research grants. One example of this is the cryptography standards specified in FIPS140-2. It is important to ensure that only certified protocols are enabled on the device, otherwise compliance will be invalid.

Links
[1] http://community.ja.net/system/files/images/tg-vpn-13.jpg
[2] http://community.ja.net/system/files/images/tg-vpn-14.jpg
[3] https://community.ja.net/library/janet-services-documentation/janet-certificate-service
[4] http://community.ja.net/system/files/images/tg-vpn-15.jpg
[5] http://community.ja.net/system/files/images/tg-vpn-16.jpg
[6] http://community.ja.net/system/files/images/tg-vpn-17.jpg
[7] http://community.ja.net/system/files/images/tg-vpn-18.jpg
[8] http://community.ja.net/system/files/images/tg-vpn-19.jpg