CE0973a - Issues in Network Security
6: IPSEC & VPNs

James A Sutherland

Abertay University

Monday, 15th February 2016

Why VPNs?

- Privacy for remote access
- Authentication for non-public resources
- Smaller attack surface for internal servers
- Connect isolated sites together into one
- Can be done physically - private circuits - expensive!

Why VPNs?

- Privacy for remote access
- Authentication for non-public resources
- Smaller attack surface for internal servers
- Connect isolated sites together into one
- Can be done physically - private circuits - expensive!

Why VPNs?

- Privacy for remote access
- Authentication for non-public resources
- Smaller attack surface for internal servers
- Connect isolated sites together into one
- Can be done physically - private circuits - expensive!

Why VPNs?

- Privacy for remote access
- Authentication for non-public resources
- Smaller attack surface for internal servers
- Connect isolated sites together into one
- Can be done physically - private circuits - expensive!

Why VPNs?

- Privacy for remote access
- Authentication for non-public resources
- Smaller attack surface for internal servers
- Connect isolated sites together into one
- Can be done physically - private circuits - expensive!

Types of VPN

Three main kinds:

- Site to site
  - e.g. link London office to Edinburgh
- Client to site
  - Remote worker connecting back to HQ
- Client to Internet
  - Done for privacy: protect local segment
  - Or bypass censorship

Types of VPN

Three main kinds:

- Site to site
  - e.g. link London office to Edinburgh
- Client to site
  - Remote worker connecting back to HQ
- Client to Internet
  - Done for privacy: protect local segment
  - Or bypass censorship

Types of VPN

Three main kinds:

- Site to site
  - e.g. link London office to Edinburgh
- Client to site
  - Remote worker connecting back to HQ
- Client to Internet
  - Done for privacy: protect local segment
  - Or bypass censorship

Types of VPN

Three main kinds:

- Site to site
  - e.g. link London office to Edinburgh
- Client to site
  - Remote worker connecting back to HQ
- Client to Internet
  - Done for privacy: protect local segment
  - Or bypass censorship

Types of VPN

Three main kinds:

- Site to site
  - e.g. link London office to Edinburgh
- Client to site
  - Remote worker connecting back to HQ
- Client to Internet
  - Done for privacy: protect local segment
  - Or bypass censorship

Types of VPN

Three main kinds:

- Site to site
  - e.g. link London office to Edinburgh
- Client to site
  - Remote worker connecting back to HQ
- Client to Internet
  - Done for privacy: protect local segment
  - Or bypass censorship

Types of VPN

Three main kinds:

- Site to site
  - e.g. link London office to Edinburgh
- Client to site
  - Remote worker connecting back to HQ
- Client to Internet
  - Done for privacy: protect local segment
  - Or bypass censorship

IPSEC Protocol

Mainly RFC 4301 and 6071

- AH: Authentication Header (IA, no C)
- ESP: Encapsulation Security Payload (CIA)

ESP (IP protocol 50) more widely used and preferable, comparable to SSL.
AH (proto 51) is not obsolete though: why?

Security Associations

Point to point IPSEC sessions. One-way, unlike SSL.

- 32 bit ID (Security Parameter Index)
- Endpoints
- Encryption algorithm and key
- Integrity check (signing algorithm)
- Authentication signing key

Note: Much the same as SSL, but one way only.

Transport v Tunnel mode

Transport mode just changes the packet slightly: does not conceal source/destination.
Tunnel mode creates a whole new packet header. So, for example, you could have two sites both using private (RFC1918) address blocks, linked over the Internet using such a tunnel with just two 'proper' IP addresses.

Internet Key Exchange

IPSEC itself defines encrypting and signing the packets to protect the privacy and integrity of that data, using pre-established keys and algorithms.
IKE uses X.509 certificates (remember those?) to negotiate and establish SA pairs, in conjunction with some manual configuration. (Unlike SSL, for public use and reliant on CAs, IPSEC can use self-signed certificates without problems: why?)

Other VPN protocols

Of course, not all VPNs use IPSEC: there are SSL versions, PPTP versions (sometimes transferring the PPTP traffic over IPSEC)...
In particular, really all you can rely on with "Internet access" these days is UDP and TCP ... sometimes not even all of that.
Protocols 50 and 51 often get blocked!
So OpenVPN runs a VPN over TCP port 443; as long as your Internet connection doesn't block HTTPS you should get a working link.

Lab Work

Study both the similarities and differences in each component between IPSEC/IKE and SSL.

- Packet loss handling
- Flow control of payload
- Intended audience

In your example organisation, how would you link two server farms together? What about a teleworker needing to 'dial' in from Starbucks or hotels?