SITE-TO-SITE VPNS PART I: THEORY.

A VPN uses encryption and hashing: encryption so no outsider can capture useful data, and hashing to verify that the sender the data is who he says he is and no alteration of data was done in transit.

First encryption. Important to understand here is that no encryption is truly unbreakable. Any key or encryption can be broken with brute-forcing: just trying all possible combinations until the right one is found. The encryption standards just have a massive amount of combinations, making this nearly impossible, e.g. 128-bit keys yield $3.4*10^{38}$ possibilities.

There are many possible encryption schemes, but these two are used the most:

- 3DES, uses 168-bit keys to encrypt data. It's been around since 1998 and some weaknesses have been found, but none that bad that encryption can be broken in a reasonable amount of time.
- AES, which uses 128, 192 or 256-bit keys. One weakness has been found so far, now requiring four times less computational power to break AES, but still well beyond any reasonable time frame (modern-day computers would still need millennia).

Blowfish encryption is an open standard, but not widely supported in vendor products so rarely seen in production environments. Most devices do support DES encryption (yes, 3DES is derived from it), but DES is considered breakable and insecure.

Hashing, the other main VPN parameter, also comes in two widely used flavors:

- MD5, while using 128-bit hashes, is considered insecure. A modern-day multi-core computer can break the encryption in less than a minute.
- SHA. SHA-1 uses a 160-bit hash, but has weaknesses and just like MD5 is supposedly cracked in less than a minute. SHA-2 however uses several different key lengths and has as of this article's date not yet been broken, which makes it the only safe hash with support on many platforms.

SHA-3 is a new standard that was announced just this month, and has no practical implementations yet.

While most of these hashing methods by themselves are insecure, they are still widely used in VPNs because the encryption provides sufficient protection already (the hash is also encrypted). Adding to the confusion, some platforms mention 'SHA' without indication about the version.

A third important parameter is the Diffe-Hellman (DH) group used. DH is a method of key exchange, since during the initial setup of a VPN, the VPN peers must exchange encryption keys. If these keys are captured by an outsider, the entire VPN can still be decrypted. DH solves this problem mathematically so peers can derive each others keys without sending them unmodified. The DH group means the length of the algorithm:

- DH Group 1: 768-bit group
- DH Group 2: 1024-bit group
- DH Group 5: 1536-bit group
- DH Group 7: 163 bits elliptical curve field

While most implementations simply ask the group, some ask for bit-length. Group 2 and 5 are used widely, and generally group 1 is not recommended because it's suspected to be breakable in a reasonable amount of time with realistic computational power. DH Group 7 is a special one: it's made for devices with low processing power, like PDAs. I couldn't find any objective source claiming this encryption is better or worse than group 5, but most seem to agree it's less secure.

Another important parameter is the mode used to connect: main mode or aggressive mode. Cisco also supports quick mode, see their site for a brief explanation. Quick mode is rarely used.

And last but not least: the timers. The VPN will renegotiate from time to time. Unlike the previous parameters, if these timers do not match on both ends, the VPN might come up, but will become unstable and disconnect from time to time.

Now that all important parameters are listed, one more thing: a VPN connection consists of two phases. Phase 1 is the initial setup of a secure tunnel, using a common encryption, hashing, renegotiation timer and DH group. Inside that secure tunnel, parameters for the actual

encrypted tunnel for data are negotiated: again encryption, hashing, a timer and optionally a maximum data limit before renegotiation. This is Phase 2. Also optionally, during Phase 2, you can use ‘Perfect Forwarding Secrecy’ (PFS), which means Diffie-Hellman key exchange will be used again inside the secure tunnel.

Note that the parameters (encryption, hashing, timers and optionally DH group) do not have to match between Phase 1 and Phase 2: you can use AES-256 SHA-2, DH group 5 for Phase 1, and a less resource-intensive 3DES MD5 DH group 2 for Phase 2, for example. Obviously, they have to match between the two connecting devices.

Edit 28/10/2012: looks like I forgot two important facts:

1) The Phase 2 also needs to list the traffic to encrypt, usually in a ‘from subnet x to subnet y’ form. Sometimes referred to as ‘encryption domain’.

2) How do the VPN peers actually exchange policy information? Through the exchange of IKE packets on UDP port 500, containing the Phase 1 information.

That concludes the theory. In the following articles, I’ll explain how to set up a VPN connection on different platforms. Stay tuned!

Source : http://reggle.wordpress.com/2012/10/25/site-to-site-vpns-part-i-theory/