Site-to-Site VPN Encryption and Authentication

https://campus.barracuda.com/doc/43846964/

Connection Establishment

Establishing an IPsec tunnel usually consists of the following steps:

1. The "active" IPsec peer establishes a UDP port 500 connection to the "passive" peer. Then both peers negotiate a main mode security association using their preshared secret. This is done in order to verify data integrity and confidentiality.
2. Various quick-mode security associations are established on top of the existing phase 1 (main mode) security association. These provide keying and configuration material for the next step.
3. Any IP packet matching a security association that was established prior to it will be encrypted and authenticated using the keying and configuration material found in the corresponding phase 2 security association.

Encryption Specifications

The IPsec suite of protocols is used to provide encryption and authentication at the IP layer. The authentication of data origin and integrity, just like data content confidentiality and replay protection, are transparent to any application operating on a higher layer than IP. IPsec consists of three standards:

- **Encapsulating Security Payload (ESP)**
- **Authentication Header (AH)**
- **Internet Security Association and Key Management Protocol(ISAKMP)** - ISAKMP consists of two steps: Phase 1 (Main-Mode), Phase 2 (Quick-Mode).

Authentication

There are several different possible authentication methods for site-to-site VPN tunnels:

- **Pre-shared RSA Public Key**
- **External Root-signed x.509 Certificate** - This method is capable of many restrictive configurations (match on one root certificate, match on all root certificates, additional pattern check for subject/subject alternative name, policy match, and generic v3 OID match).
- **Explicit x.509 Certificate** (e.g. self-signed) - This method is used if no

CA/Public Key Infrastructure (PKI) is available.