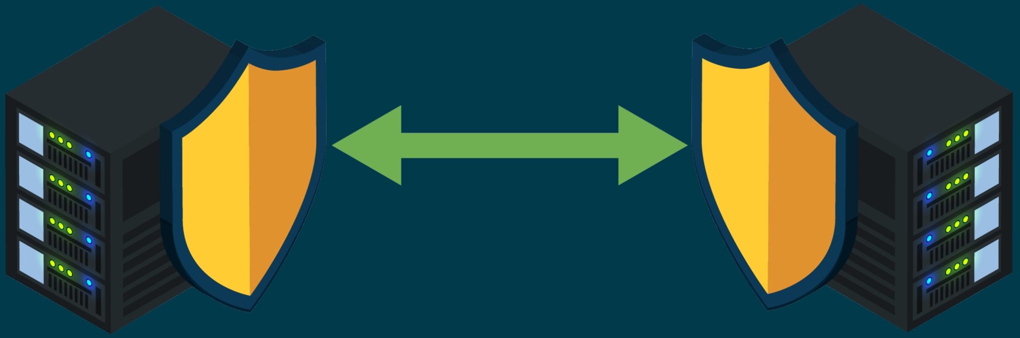
IPSEC VPN DEPLOYMENTS

I2NSF interim, IETF
September 6, 2017

Paul Wouters,
RHEL Security

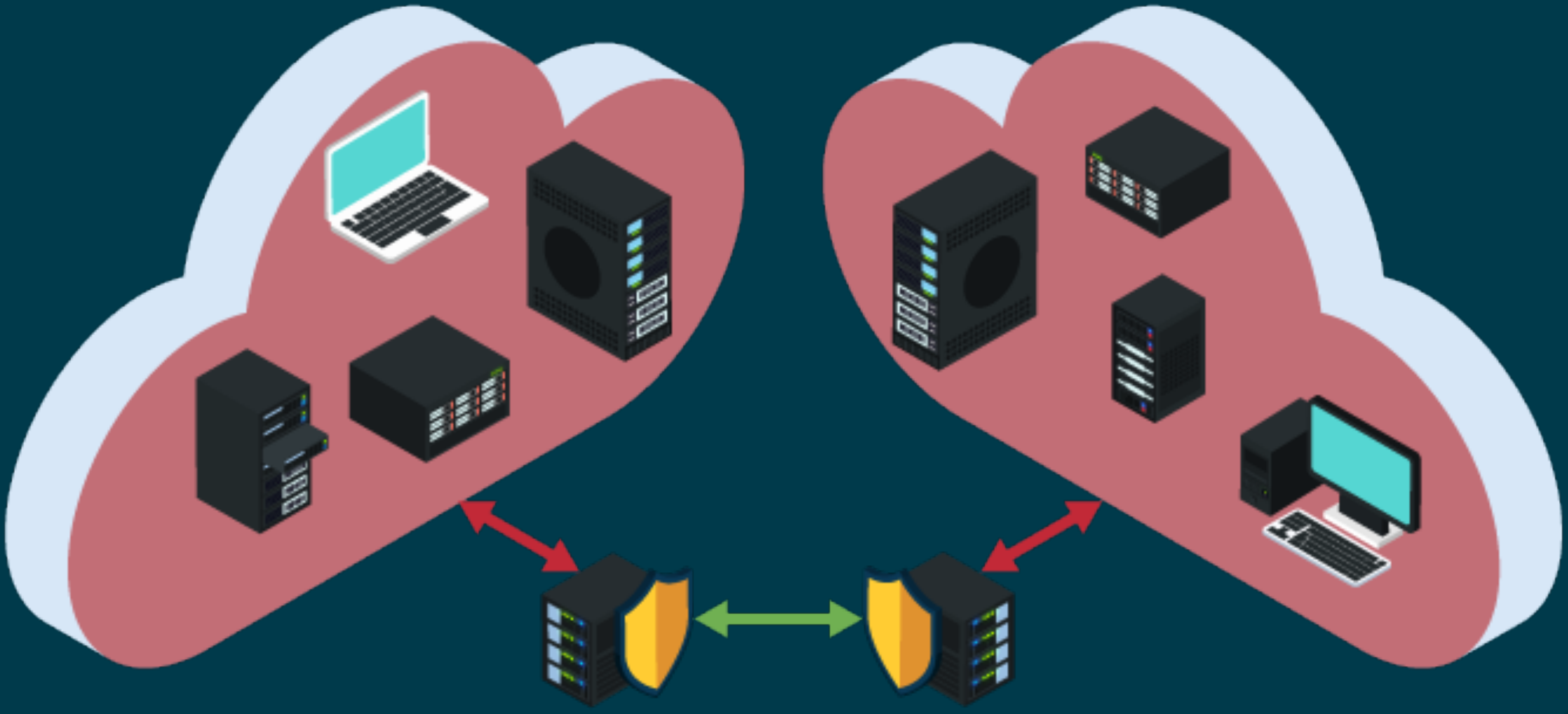
HOST TO HOST VPN

One device communicates to one other device using encryption



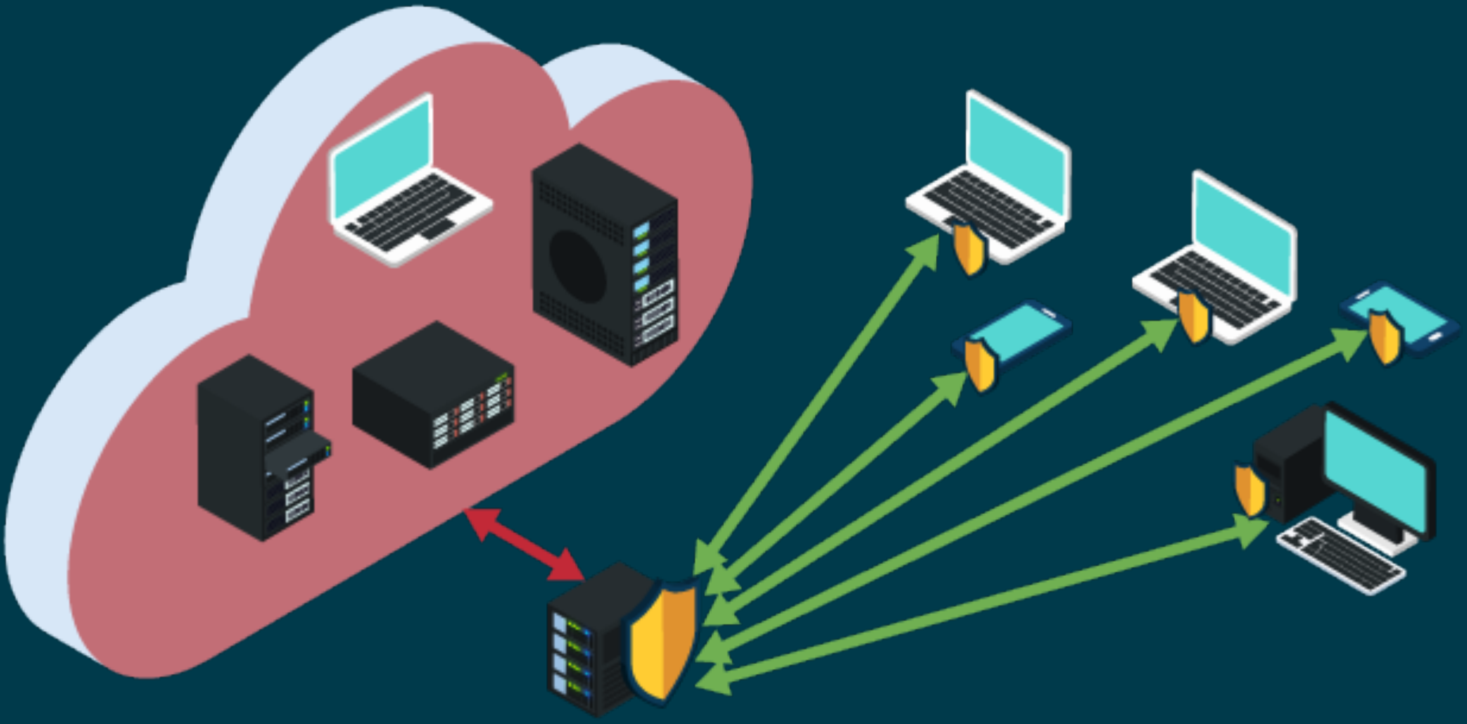
SITE TO SITE VPN

Individual networks are unencrypted, only the interconnect is encrypted.
Individuals devices are unaware of the encryption.



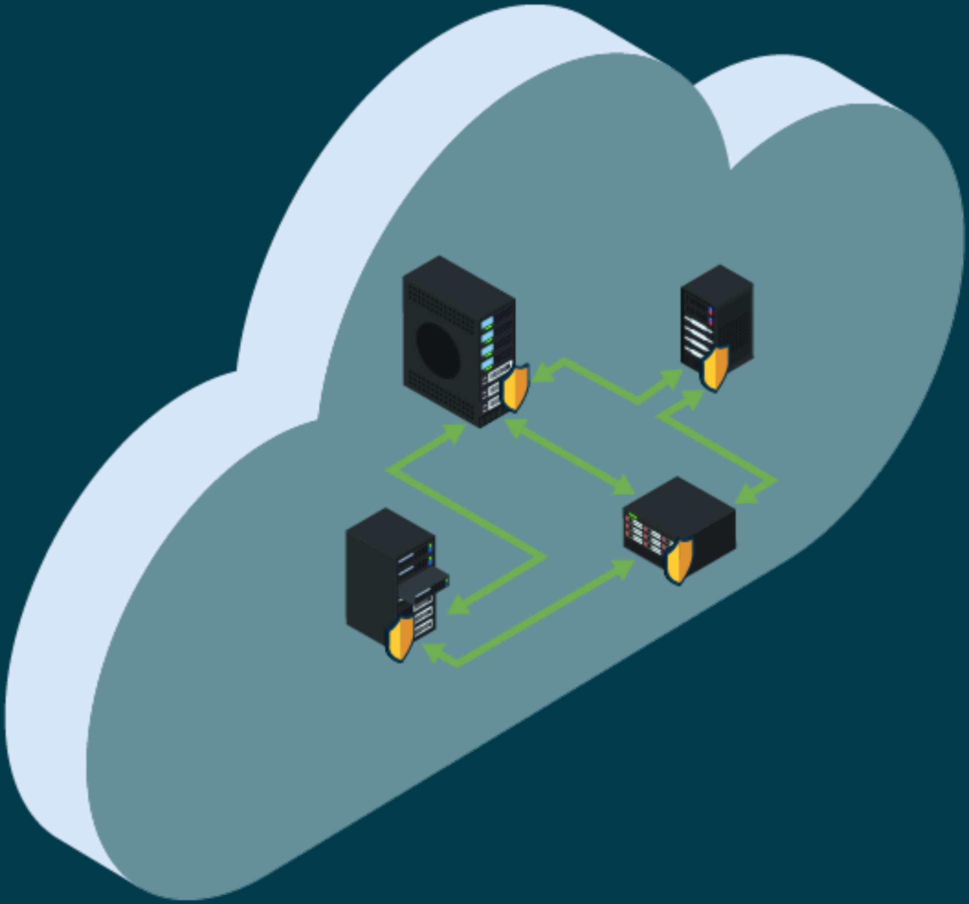
REMOTE ACCESS VPN

End device to site network access point encrypted – LAN still unencrypted. Remote devices are usually assigned an IP address to appear to be located inside the LAN.



FULL MESH ENCRYPTION

Each device communicates with IPsec to all other (capable) devices



IPsec PRIMER [RFC 6071]

IKE + IPsec = VPN

Internet Key Exchange (IKE)

ISAKMP, IKE SA, Parent SA, Phase 1

Command Channel

- ~~Internet Key Exchange v1 [RFC 2409]~~
- Internet Key Exchange v2 [RFC 7296]
  - also: Minimal IKEv2 [RFC 7815]
- Uses UDP port 500 and 4500
- Peer authentication and authorization
- Connection parameter negotiation (algorithms, IP address, ports, etc)
- Generate IPsec keys (KEYMAT)
- Responsible for key rollover (PFS)
- Communicates encryption keys, modes, parameters, etc to kernel
- Lots of “plugin RFCs”
- IKE itself is encrypted
- IKE does not encrypt IP data traffic

IPsec

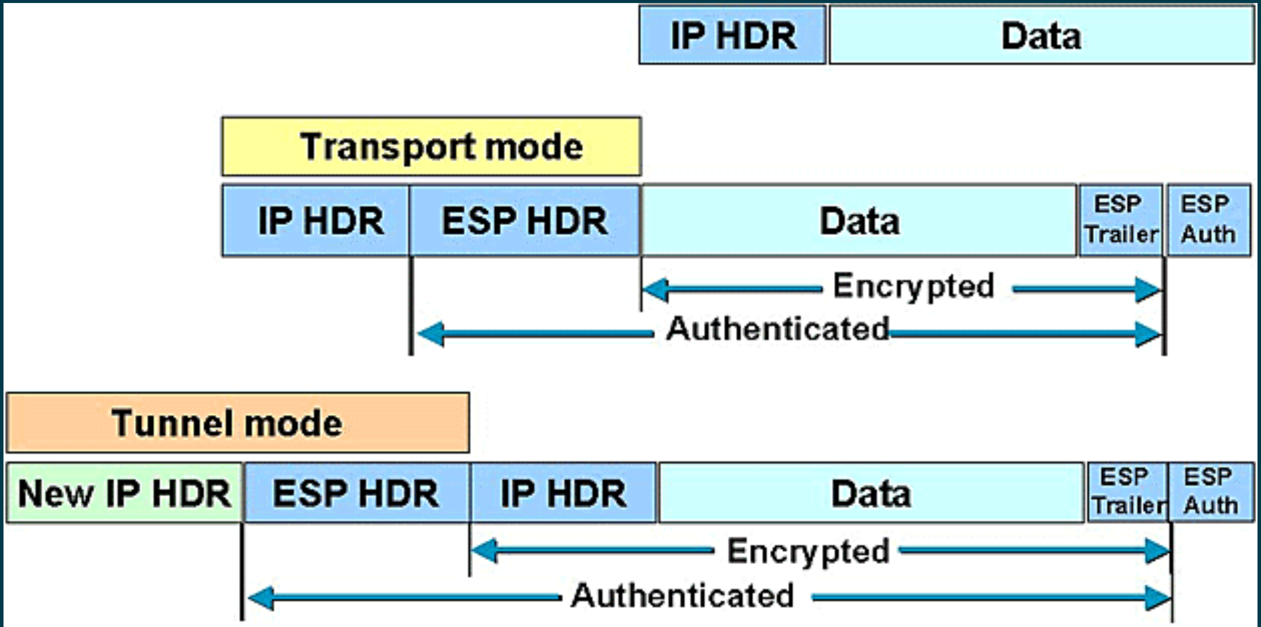
IPsec SA, Child SA, Phase 2

Data Channel

- ESP (protocol 50): Encapsulated Security Payload [RFC 4303]
  - Tunnel Mode [RFC 4301]
  - Transport Mode [RFC 4301]
  - ~~Beet Mode [expired draft]~~
- ESPinUDP [RFC 3948]
- ~~AH (protocol 51): Authenticated Header~~
  - Instead use ESP with NULL encryption [RFC 2410]
- ~~Wrapped ESP (WESP) [RFC 5840]~~
- NEW: ESPinTCP / ESPinTLS [RFC 8229]

TUNNEL MODE
VERSUS
TRANSPORT MODE

- Tunnel Mode places the entire packet (encrypted) inside a new packet
- Transport Mode encrypts native packet - it re-uses its own IP header



TUNNEL MODE
VERSUS
TRANSPORT MODE

- **Tunnel Mode**
  - Hides more information (source / destination IP address)
  - Can be used for host-to-host, site-to-site, NAT traversal deployments
  - Extra overhead takes a few extra bytes, decreases usable MTU
  - Very flexible deployments with slightly more complicated security policies
  - Swiss army knife: It can do everything but sometimes you cut yourself
- **Transport Mode**
  - Can only be used for host-to-host connections
  - Does not work well to traverse NAT's, leaks/clashes with pre-NAT IP
  - Very simple deployment with simple security policy
  - Butter knife: Works for plain bread, not fancy steaks
- In IKEv2, Transport Mode support is “optional” and dynamically negotiated