OPPORTUNISTIC IPSEC USING DNSSEC

ICANN 58, Copenhagen, March 2017

Presented by Paul Wouters,
RHEL Security

THE LIBRESWAN PROJECT

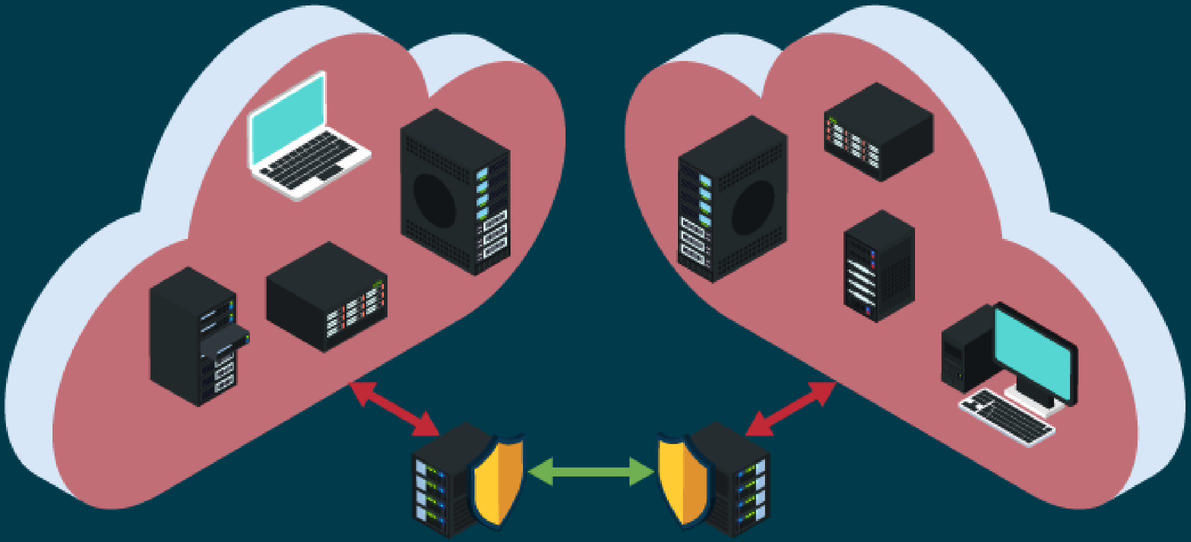
An Internet Key Exchange (“IKE”) daemon for IPsec

- Enterprise IPsec based VPN solution
- Make encryption the default mode of communication

- Certifications (FIPS, Common Criteria, USGv6, etc.)
- Contributing to IETF Standards for IKE and IPsec

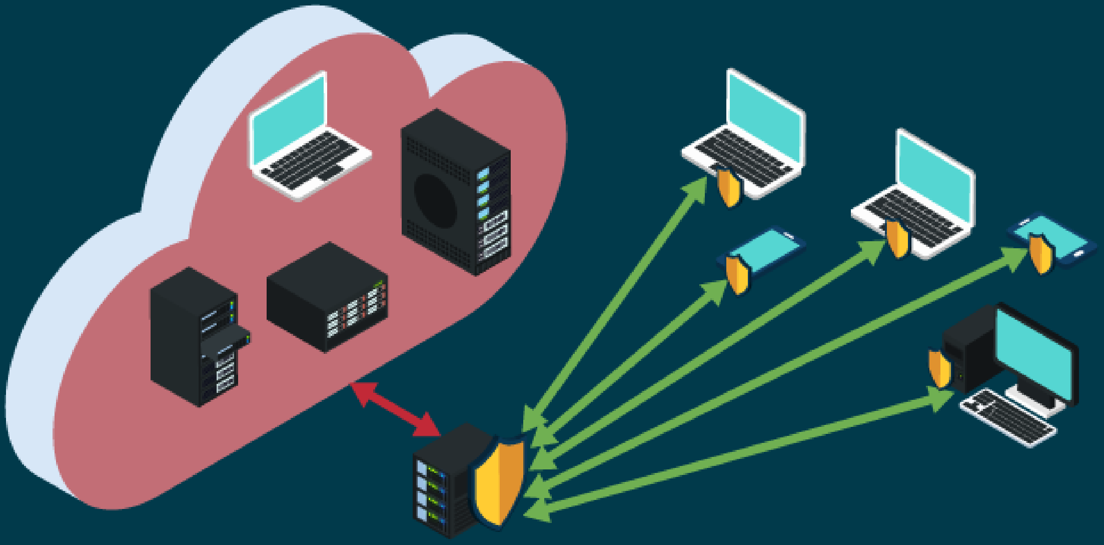
TYPICAL SITE TO SITE VPN

Individual networks are unencrypyed, only the interconnect is encrypted



TYPICAL REMOTE ACCESS VPN

End device to site network access point encrypted – LAN still unencrypted



OPPORTUNISTIC IPSEC USING DNSSEC

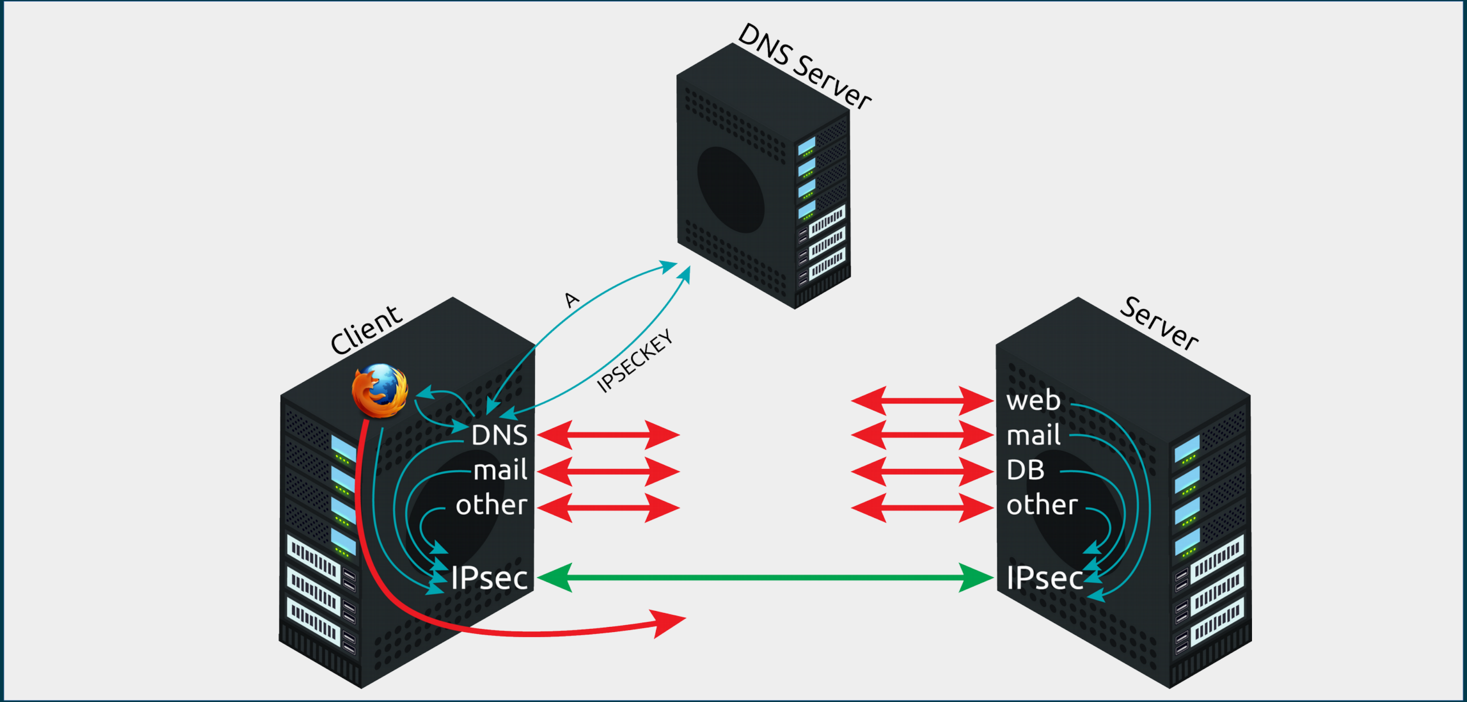
- IKEv2 allows asymmetric AUTH for IPsec (like SSL/TLS)
- DNSSEC resolving on the end node (eg unbound DNS server)
- Allows DNSSEC based triggers for Opportunistic Encryption

- Linux conntrack and IKEv2 addresspool to resolve NAT problem
- IKEv2 allows assigning IP addresses natively (for NAT support)
- Linux conntrack vastly improved (for NAT support)

ESTABLISHING IPSEC TUNNELS USING DNSSEC

1. Application performs a DNS lookup (eg for “oe1.libreswan.org”)
2. Local DNS server (eg unbound or knot) receives request from application:
   a) DNS server resolves and validates A record (eg for “oe1.libreswan.org”)
   b) DNS server resolves and validates IPSECKEY record (eg for “oe1.libreswan.org”)
   c) If DNSSEC signed IPSECKEY found, send QNAME + A + IPSECKEY to IKE daemon
      i. IKE daemon (eg libreswan) negotiates IPsec tunnel to IP address using pubkey from IPSECKEY record
   d) DNS server returns A record to application
3. Application receives A record and sends data to remote server
4. kernel encrypts all application traffic using IPsec.

ESTABLISHING IPSEC TUNNELS USING DNSSEC



OPPORTUNISTIC IPSEC DEPLOYMENT

End-to-end encryption using IPsec where possible