Aalto University

Network Security: VPN

Tuomas Aura

CS-E4300 Network security
Aalto University

Virtual private network (VPN)

- Site-to-site VPN (gateway-to-gateway)
  - Connecting two networks, e.g., branch office to main office
- Remote access VPN (host-to-gateway)
  - Connecting a mobile or remote computer to the office network
- Cloud VPN (on-premised gateway to cloud)
  - Outsourcing previously local services to cloud
- Provider-provisioned VPN: the above as outsourced service
- Multi-cloud VPN
- Commercial VPN: host to internet

VPN components

- VPN software for managing authentication credentials
- Secure tunnel
  - Tunnel for IP packets (L3) or Ethernet frames (L2)
  - Must define encapsulation of packets/frames to the tunnel
  - Security with TLS, SSH, IPsec, DTLS, or proprietary algorithms
  - Authentication with certificates, shared key, or password
  - Policy for which packets/frames are sent to the tunnel
- VPN gateway terminates connections at a site
  - Gateway may implement DHCP and NAT for clients

VPN tunnel interface

Implementation at each gateway or host:

- Virtual network interface
  - Linux TUN interface for L3 tunnel
  - Linux TAP interface for L2 tunnel
- Routing rules determine which traffic goes to the tunnel

```
ip -d a
ip tuntap list
```

- Firewall, routing, NAT, and VPN rules are often entangled; need to get them all right
- This architecture used by OpenVPN, WireGuard
  - IPsec VPN is typically not implemented as a virtual interface (although it could) but as an IPsec policy on an existing interface

OpenVPN

- VPN tunnel based on the OpenSSL library

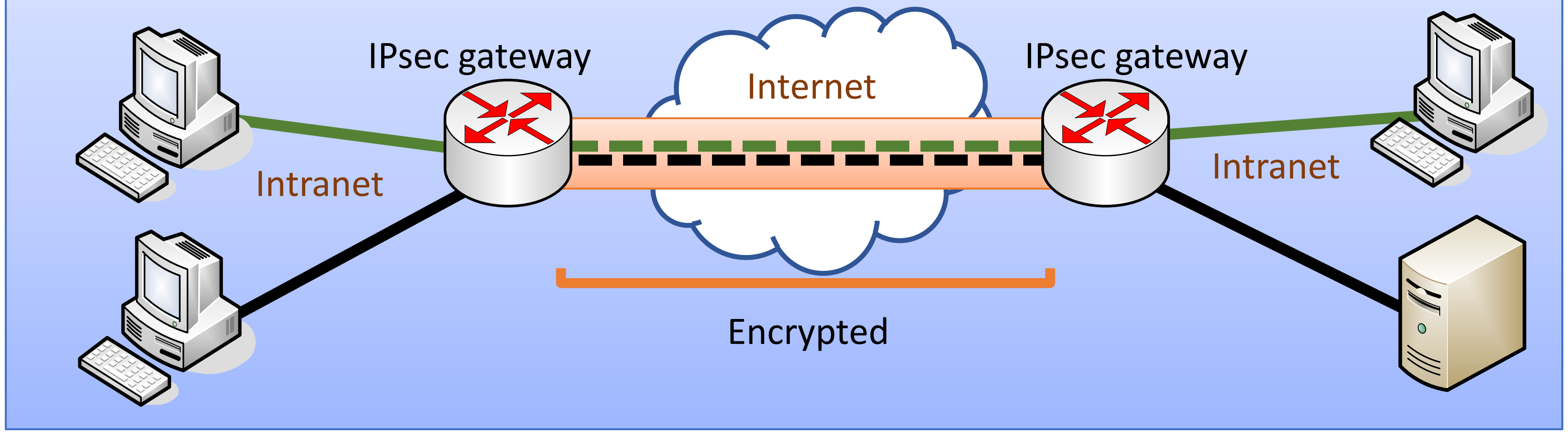
  https://openvpn.net/index.php/open-source/documentation.html

- TLS handshake for authenticated key exchange
  - Static key or certificates
- Custom session protocol:
  - Tunnel IP packets or Ethernet frames in UDP: packets/frames are protected with cryptography and encapsulated in UDP
  - Why not DTLS? Because OpenVPN is older
- TUN or TAP interface on client and server

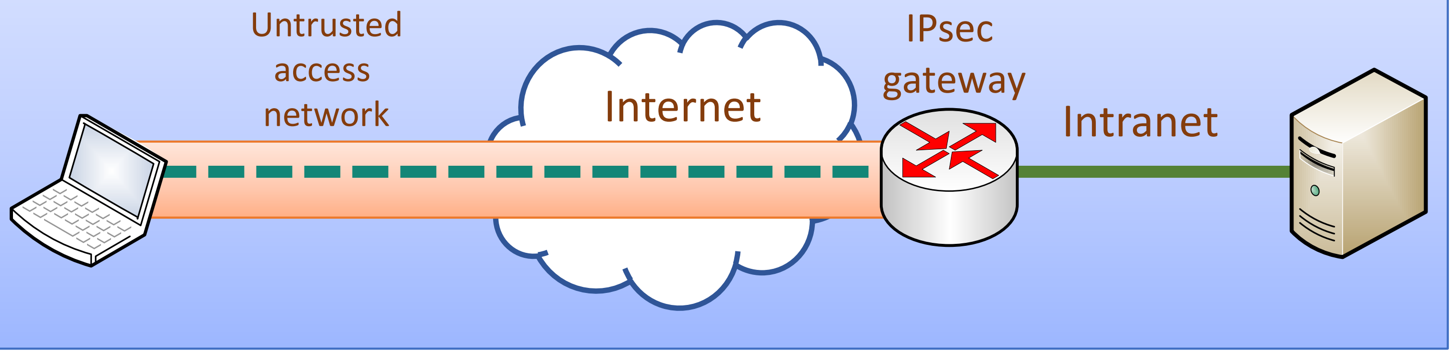
IPsec VPN (recall)

Tunnel mode

Encryption and/or authentication between two gateways (VPN)



Tunnel mode between a host and a gateway (typical VPN connection)



IPsec VPN in Linux

- VPN software configures the IPsec policy
  - Common software: strongSwan, Libreswan
  - https://libreswan.org/wiki/Configuration_examples
  - https://www.strongswan.org/test-scenarios/

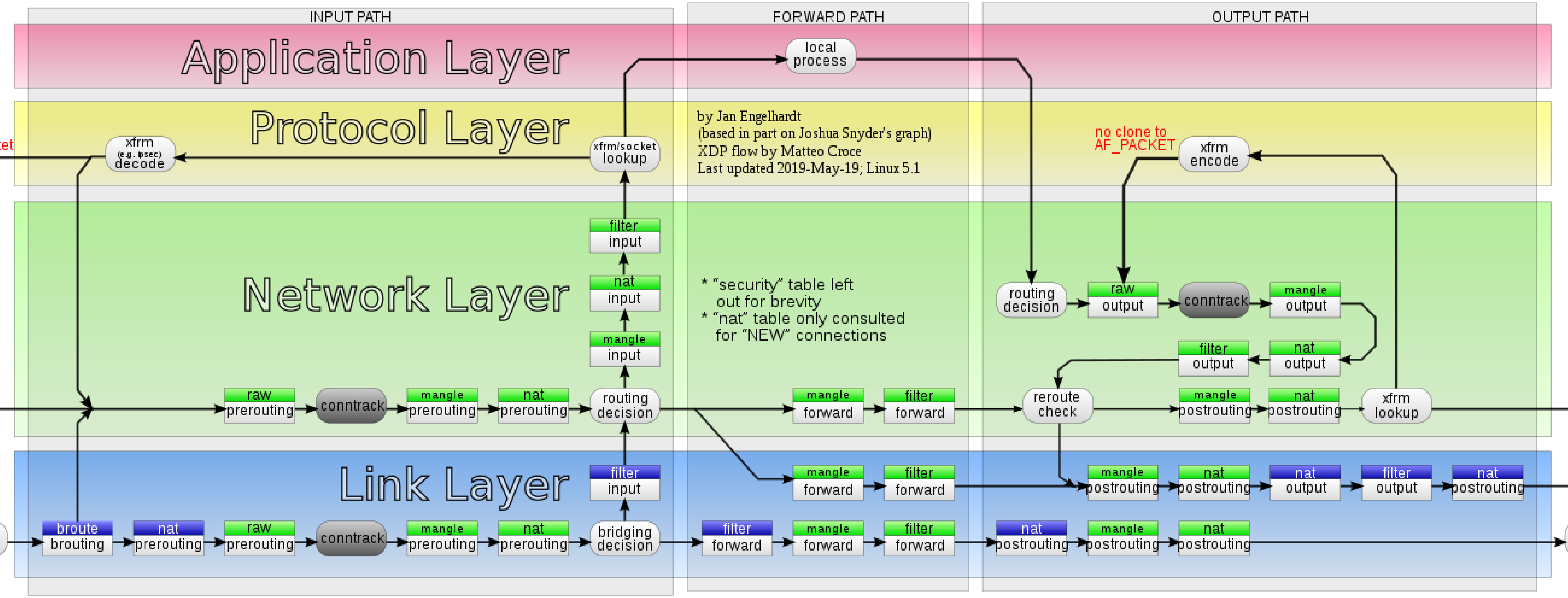
```
ipsec
/etc/ipsec.conf
/etc/ipsec.d/*
```

- XFRM in Linux kernel implements IPsec policy and tunnels

```
ip xfrm policy
ip xfrm state
```

Linux Netfilter architecture

- How does IPsec integrate with firewall filtering and NAT?



by Jan Engelhardt
(based in part on Joshua Snyder's graph)
XDP flow by Matteo Croce
Last updated 2019-May-19; Linux 5.1

- "security" table left out for brevity
- "nat" table only consulted for "NEW" connections

https://en.wikipedia.org/wiki/Netfilter#/media/File:Netfilter-packet-flow.svg

L2TP VPN

- Layer 2 tunneling protocol (L2TP)
  - Encapsulation of Ethernet frames to UDP
  - Used as client-to-server VPN, or for connecting LANs over the Internet
- Protected with IPsec and pre-shared keys or certificates
- Point-to-Point Protocol (PPP) is used on top of L2TP for creating tunnel interfaces, assigning addresses, multiplexing
  - Optional user or client application authentication with MS-CHAPv2 or EAP (separate from IPsec authentication)

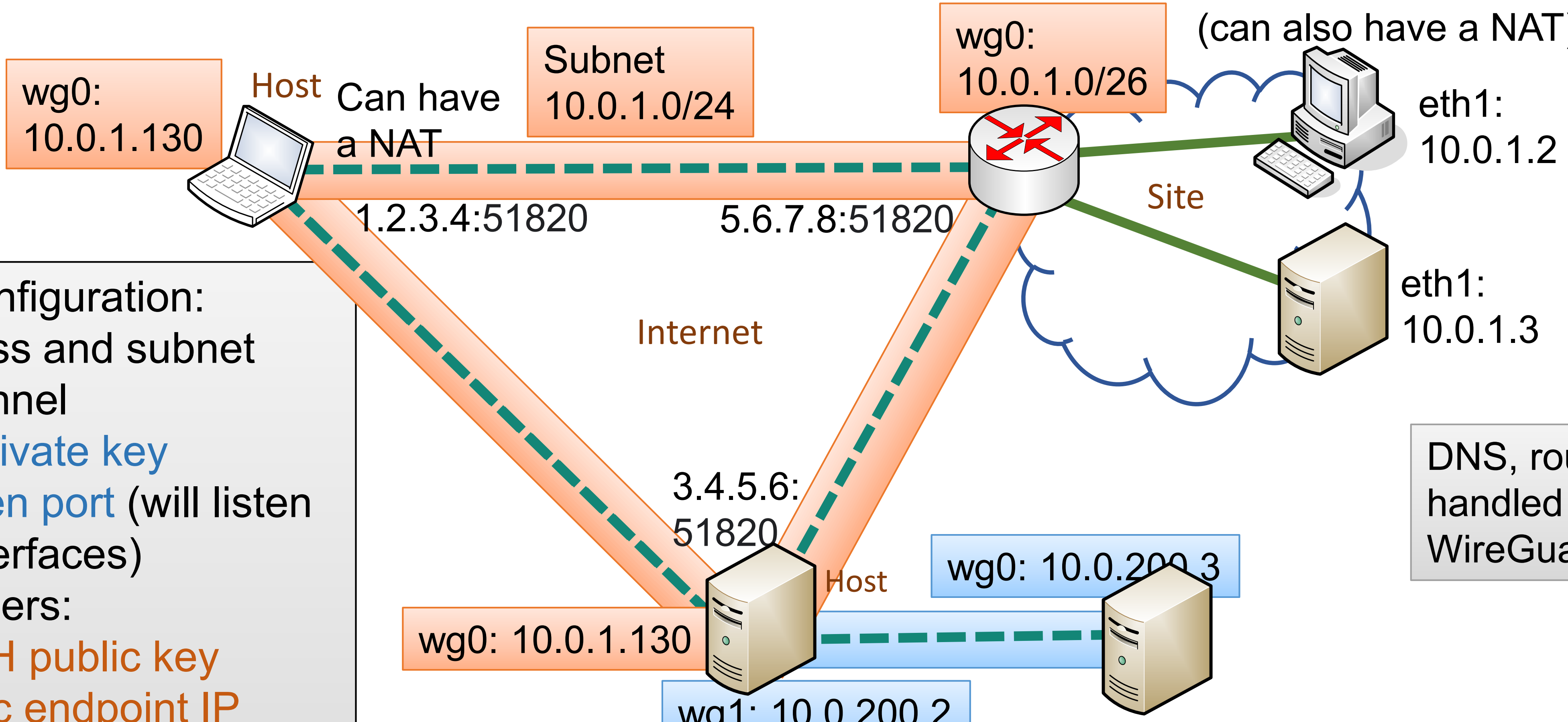
WireGuard

- Secure virtual networks with private IP address spaces
  - Virtual TUN interface for connecting host or gateway to the virtual network
  - Can implement site-to-site, host-to-site, or peer-to-peer VPN
- Authenticated ECDH handshake with preshared static ECHD keys
- IP packets are encapsulated in UDP and WireGuard header
- Focus on small codebase, auditability
  - No crypto-agility: only one set of cryptographic algorithms

```
/etc/wireguard/*
wg-quick
wg
```

https://www.wireguard.com/talks/inria2017-slides.pdf

WireGuard architecture



Router connects the site to the WireGuard subnet (can also have a NAT)

Node may belong to multiple WireGuard subnets

DNS, routing, NAT handled outside WireGuard

Interface configuration:

- IP address and subnet inside tunnel
- ECDH private key
- UDP listen port (will listen on all interfaces)
- List of peers:
  - ECDH public key
  - Public endpoint IP address and port
  - Allowed IP addresses inside tunnel

WireGuard handshake

- 1-RTT handshake based on Noise-IK and ECHD
- Pre-distributed static ECDH parameters of A and B: $Q_A = d_A \cdot G$ and $Q_B = d_B \cdot G$
- A and B generate ephemeral ECDH parameters: $Q'_A = d'_B \cdot G$ and $Q'_A = d'_B \cdot G$

1. $A \rightarrow B$: $A, Q'_A, AEAD_{h(K1)}(Q_A), AEAD_{h(K1,K4)}(T), f(Q_B)$
2. $B \rightarrow A$: $A, Q'_A, AEAD_{h(K1,K4,K3,K2)}$ (_)

T = timestamp (used as monotonic counter)

$K1 = d'_A \cdot Q_B = d_B \cdot Q'_A$ $\quad$ $K2 = d_A \cdot Q'_B = d'_B \cdot Q_A$

$K3 = d'_A \cdot Q'_B = d'_B \cdot Q'_A$ $\quad$ $K4 = d_A \cdot Q_B = d_B \cdot Q_A$

$AEAD_K(M)$ = authenticated encryption (AE) additional data (AD), where the AD is a transcript of all relevant information until there

$SK = h(K1, K4, K3, K2)$ Initiator keys = h(K1,K4) Responder keys = h(K3,K1)

$f(Q_B)$ = function of responder public key or DoS cookie

https://www.wireguard.com/protocol

VPN and IP addresses

- VPN tunnel has inner and outer IP address for each endpoint
- NAT and firewall traversal:
  - Tunnel must be TCP or UDP
  - One tunnel endpoint must have public IP address (no NAT or firewall); or use NAT traversal techniques (STUN or ICE)

- Which inner IP addresses in the tunnel?
  - Private IPv4 addresses may overlap (conflict) between sites
  - Dynamic addresses are not good for specifying long-term policy
- Solutions:
  - Site-to-site: VPN administrators may coordinate address allocation between sites
  - Host-to-site: VPN gateway assigns client a dynamic IP address from the site:
    - PPP IP-Address configuration option (RFC 1332 section 3.3)
    - IKEv2 CGF_REQUEST for virtual address in remote network (RFC 5996 section 2.19)
    - DHCP over L2 VPN
  - NAT at both gateways and separate address range for the inner tunnel addresses