Virtual Private Networks

Tamás Holczer and Gergő Ládi
Laboratory of Cryptography and System Security
Department of Networked Systems and Services
{Holczer,Gergo.Ladi}@CrySyS.hu

Outline

- Introduction
- Typical protocols employed by VPN solutions
- VPN protocols and implementations

Virtual Private Networks – Definition

- A **V**irtual **P**rivate **N**etwork extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network

  (Definition in *Cisco Secure Virtual Private Networks*, 2002)

- Simplified: VPNs make it possible for a remote party (or parties) to become part of a private network over the internet

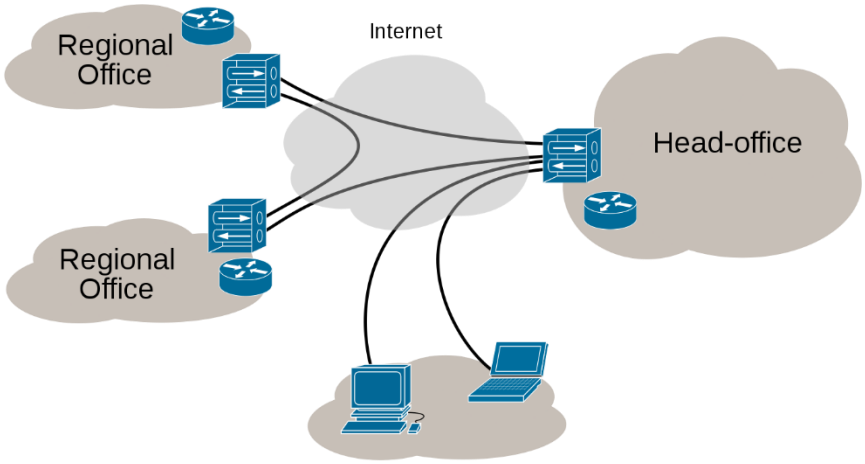
VPN Goals

- L3 connection between participants
- L2 connection only in special cases
- CIA triad
  - Confidentiality
  - Integrity
  - Availability
- AAA triad
  - Authentication
  - Authorization
  - Accounting(?)

Virtual Private Networks – The two kinds

- Remote access VPN
  - Lets remote users join a private network
  - Example: a laptop user at home, connecting to the internal network of his workplace

- Site-to-site VPN
  - Connects two or more sites (offices) of a company
  - Example: a company with offices in Budapest, Miskolc, and Szeged may connect these with site-to-site VPNs to make it seem like there is only one, big internal network



Source: Wikipedia

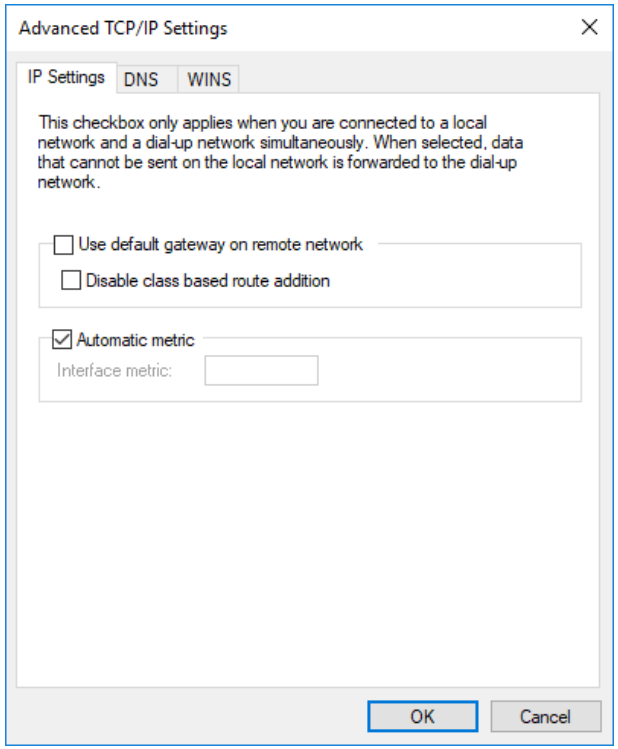
Virtual Private Networks – Split tunneling

- Depending on the network's (and the client's) settings, packets that are not addressed to hosts on the private network may be routed differently

- Without split tunneling
  - Packets to all non-local networks are sent through the VPN gateway
    - » The gateway server has to route these packets
  - The gateway operator can see all non-encrypted traffic and may also filter traffic
  - Needs a gateway with high bandwidth in case of many clients (or performance issues will occur)
  - External hosts will see the company gateway's IP as the source
    - » This might not be the same IP as that of the VPN gateway!

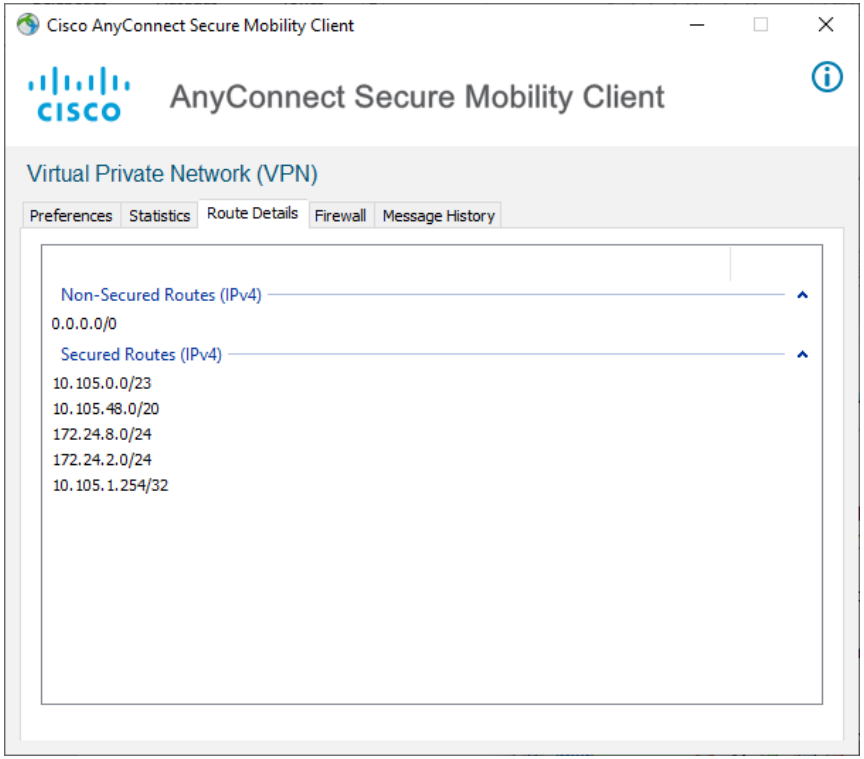
Virtual Private Networks – Split tunneling

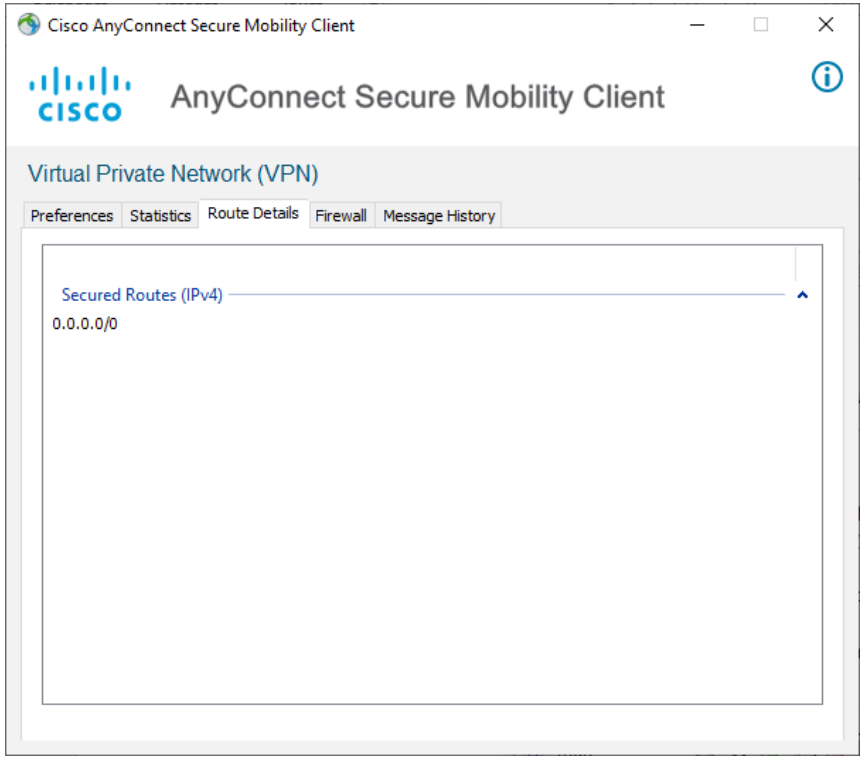
- With split tunneling
  - Only packets addressed to internal hosts are sent through the VPN connection
  - External hosts will see the client's ISP-assigned IP



Virtual Private Networks – Split tunneling

- Split tunneling: rate limit by IP
  - Similar problems with NAT
- No split tunnel: authorization based on IP
  - Company has subscription





Virtual Private Networks – Other uses

- Commercial VPN services
  - Some companies offer VPNs that don't let you access their internal network, but will route packets for you (split tunneling has to be disabled)
  - Typical uses
    - » Hiding your traffic from the ISP/company
      - But you have to trust the VPN provider!
    - » Bypassing restrictive firewalls
      - Typical in hotels, airports, etc.
      - The VPN traffic must be able to pass through
    - » Bypassing geo-blocking
      - Needs a provider with servers in many different countries

Virtual Private Networks – Other uses

- Home VPNs
  - Some home routers offer you to set up a VPN server
  - Typical uses
    - » Using your home IP as a source when abroad
    - » Access to devices on your home network (NAS, media server, …)
    - » Making unsecure channels (e.g. open WiFi) more secure

VPN BUILDING BLOCKS

Typical protocols employed in VPN solutions

- Secure Sockets Layer (SSL) / Transport Layer Security (TLS)
  - Discussed on *Cryptographic Protocols*
  - UDP in TCP: not efficient
  - TCP meltdown possible
    - » inner and outer connection packet loss -> resend -> more loss
- Datagram TLS (DTLS)
  - Very similar to TLS
  - Uses UDP instead of TCP as a transport layer protocol
    - » No ACKing => no inherent reliability but better throughput and latency
- Typical examples: OpenVPN, Cisco AnyConnect

Point-to-Point Protocol (PPP)

- RFC 1661, 1994
- An OSI Layer 2 protocol that is used to establish a direct connection between two endpoints
- Three components
  - Encapsulation: multiplexing several upper-layer protocols to the same link
  - Link Control Protocol (LCP): parameter agreement, authentication, compression, error detection, multilink negotiation
  - Network Control Protocols: manage the establishment of L3 protocols
- Example:
  - ADSL PPPoE (slowly disappearing)
  - Serial connection between routers (disappeared)
  - Home PON (widely used)

Internet Protocol Security (IPSec)

- First appearance in 1995 (Naval Research Labs, RFCs 1825-7)
- A suite of protocols which aims to provide security-related guarantees for IP traffic
- Originally, all IPv6 stacks were required to support IPSec
  - MUST was changed to SHOULD in RFC 6434 (2011)

- IPSec is not a VPN solution on its own
- IPSec is not exclusively used for VPNs

IPSec – Services

- Authentication Header (AH) – RFC 1826 (and later versions)
  - Message integrity
  - Message authentication (easier behind NAT)
  - Optionally, protection against replay attacks (using sequence numbering)
  - Protects both the header and the payload
    - » Mutable fields (TTL, fragmentation-related fields, …) are excluded, of course
    - » IP/port is included in the integrity checksum -> does not work with NAT!
  - Provides no confidentiality!

IPSec – Services

- Encapsulating Security Payload (ESP) – RFC 1827 (and later vers.)
  - Optional message integrity and authentication
    - » Only the payload is protected
  - Replay attack protection
  - Confidentiality of data
  - Traffic flow confidentiality (limited, against pattern based attacks)

- AH and ESP can be combined to achieve message integrity and authentication for both the header and the payload

IPSec – Modes

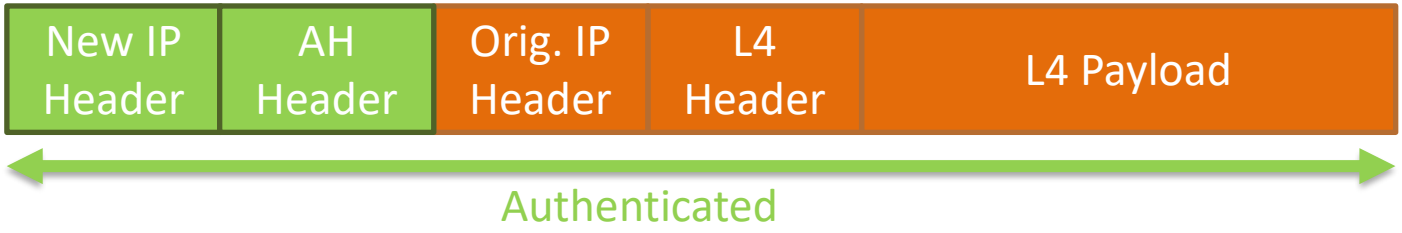
- Transport Mode
  - Used between end-to-end devices or a host and a gateway
  - Both parties must support IPSec
- Tunnel Mode
  - Used between gateways (s2s setup)
  - AH/ESP headers are added/removed by the gateways
    - » The other devices need not support IPSec (or even know that it's used)

IPSec – Services and modes

- The original IP packet

- Transport mode with AH

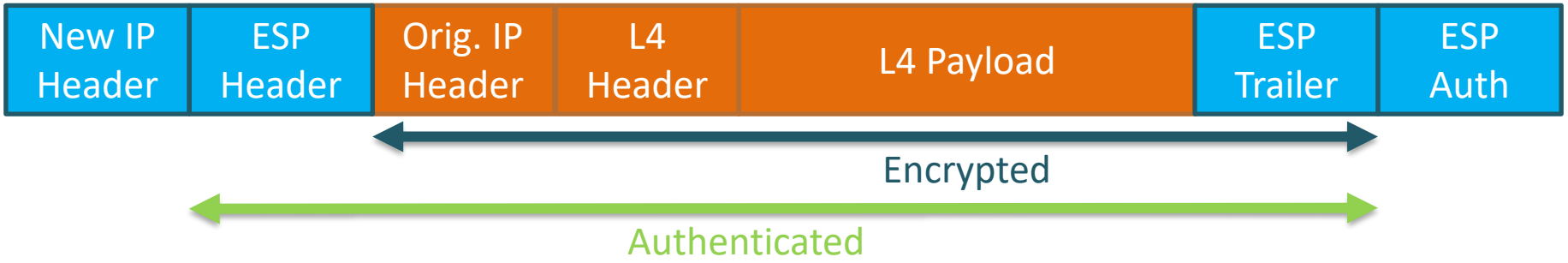
- Tunnel mode with AH



IPSec – Services and modes

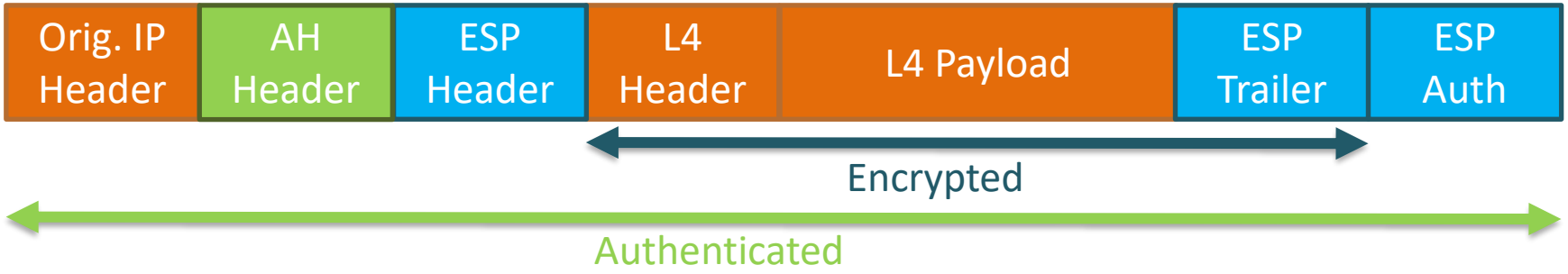
- Transport mode with ESP

- Tunnel mode with ESP

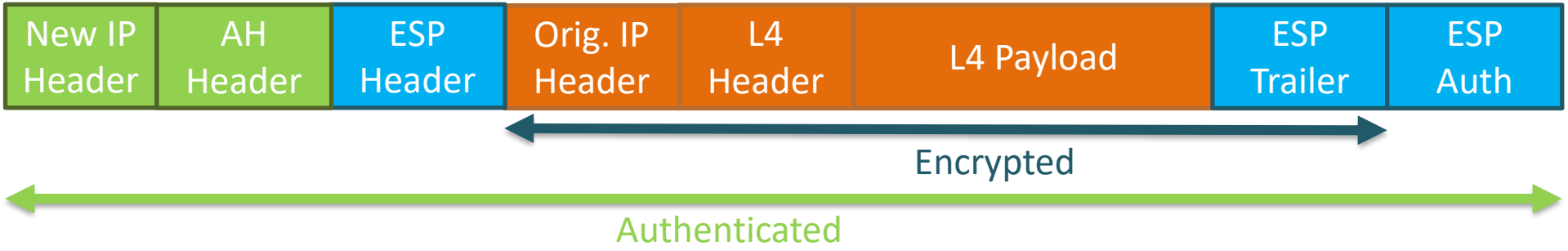


IPSec – Services and modes

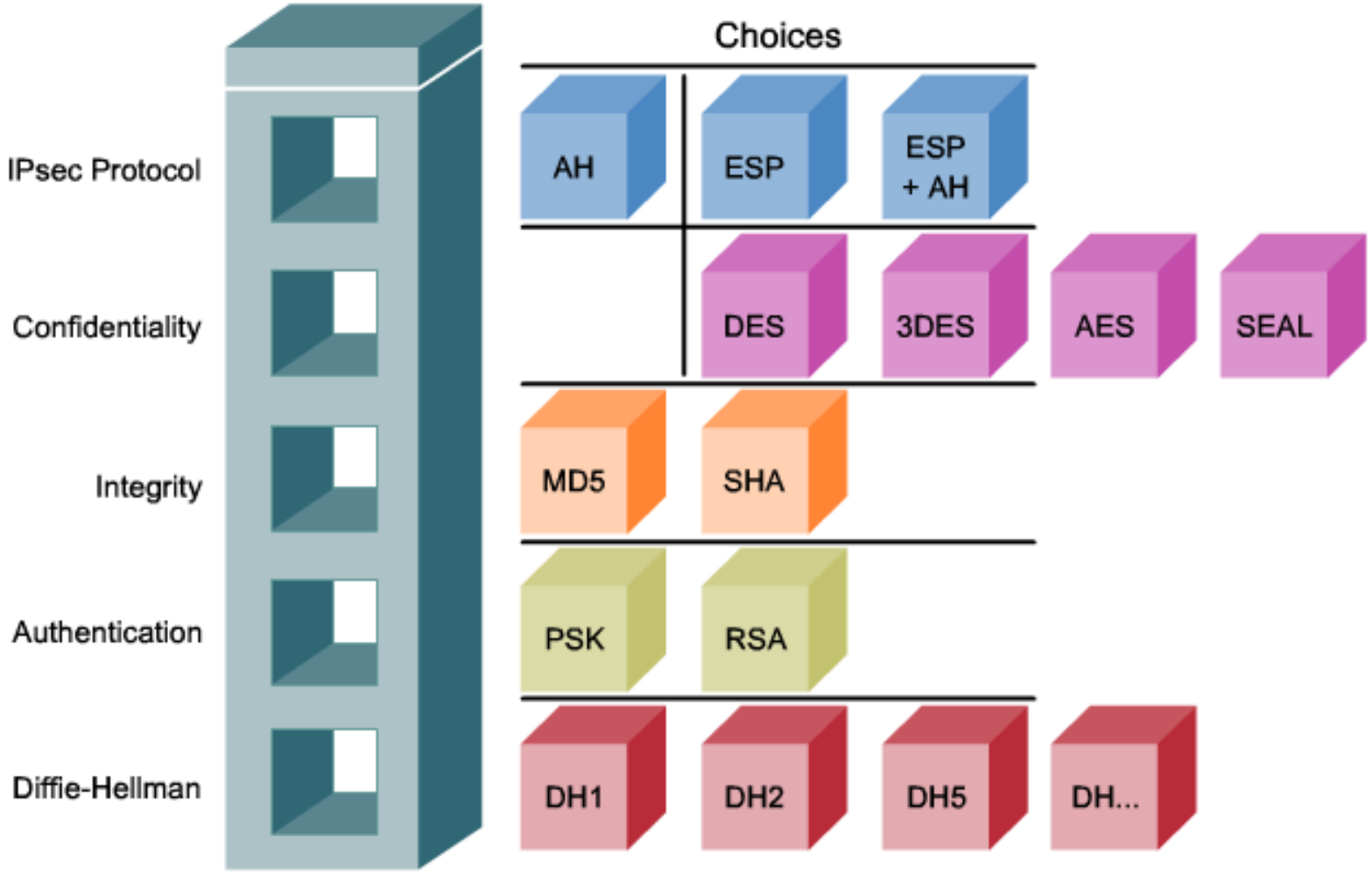
- Transport mode with AH and ESP



- Tunnel mode with AH and ESP



IPSec – The Framework



Source: Cisco CCNA Security

IPSec – Security Associations

- In order to make use of IPSec services, both parties need to know
  - The IP address and port of the other party
  - The services to be used and the mode of usage
  - Algorithms to use
  - Secrets and other parameters of the algorithms
  - …

- A collection of the above connection-specific parameters is called a Security Association (SA), stored in the SADB (SA database)
  - Each SA is assigned a unique identifier, the Security Parameters Index (SPI)
  - The SPI is sent in each AH/ESP packet
  - SAs are uni-directional, meaning there has to be one for each direction
    - » Moreover, when combining AH and ESP, a total of 4 SAs are created

IPSec – Internet Key Exchange (IKE)

- Internet Key Exchange is a group of protocols that are used to set up Security Associations automatically
  - Internet Security Association and Key Management Protocol (ISAKMP)
    - » A framework on its own: authentication, key exchange, policy negotiation
  - Oakley
    - » Diffie-Hellman-based key agreement for authenticated peers
  - SKEME
    - » Key refreshment, perfect forward secrecy, etc.
- 1998, RFCs 2407-9 (and later versions)

- Typical implementations use an X.509 certificate or pre-shared key for peer authentication
- Uses UDP port 500

IPSec – Internet Key Exchange (IKE) – v1

- Parts of it are too complicated
- Not enough automatisms

- SA creation takes two phases
- Phase 1: authentication and keying
  - Main mode: 6 messages, secure
  - Aggressive mode: 3 messages, but less secure
    - » Peer identity is not always protected
    - » PSK may be brute-forced offline
- Phase 2: IPSec parameter establishment
  - Quick mode: 3 messages

IPSec – Internet Key Exchange (IKE) – v2

- RFC 4306, 2005

- Fixes most of the issues of IKEv1
- No phases: SA creation requires 4 messages

- Actively used today

VPN PROTOCOLS

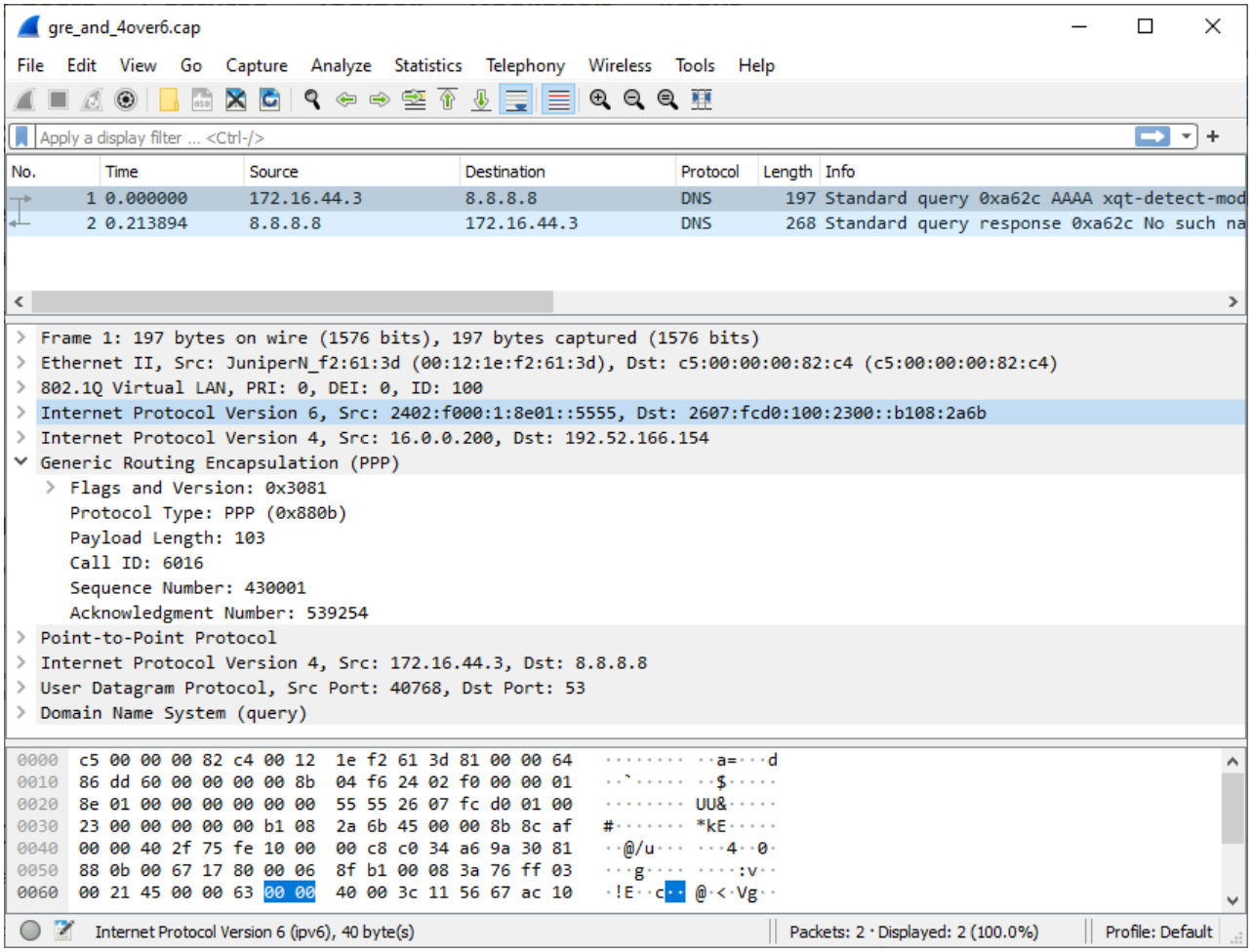
Point-to-Point Tunneling Protocol (PPTP)

- RFC 2637, 1999
- Widely supported, although not considered secure anymore
  - Linux/Android
  - Windows
  - ~~MacOS~~ (no longer supported since Sierra, 2016)
  - Mid-end SOHO routers and above

- Out-of-band protocol
  - Uses a TCP control channel (port 1723)
  - And a Generic Routing Encapsulation tunnel to forward PPP packets
- Microsoft extensions
  - Microsoft Point-to-Point Encryption (MPPE, RFC 3078, 2001): 40-bit/128-bit RC4 encryption for data packets
  - Microsoft Point-to-Point Compression (MPPC): compresses packets using LZV

GRE

- Tunneling protocol
- Encapsulate network layer protocols
- Can be used with e.g.:
  - PPTP
  - IPsec
- Simple header, no encryption
- Can be used for bcast/mcast traffic



Layer 2 Tunneling Protocol (L2TP)

- RFC 2261, 2000
- Widely supported
  - Linux/Android
  - Windows
  - MacOS
  - Mid-end SOHO routers and above
- Tunnels PPP packets over UDP port 1701
- L2TP does not support authentication or encryption
  - It is almost always combined with IPSec

Secure Socket Tunneling Protocol (SSTP)

- Once it was Microsoft's proprietary protocol, now its specifications are openly accessible
- Available on
  - Windows
  - Linux (e.g. via the SoftEther VPN client)

- Tunnels PPP packets over TCP port 443 (over SSL/TLS)
  - This provides confidentiality and integrity
  - Although it is not undetectable, the use of TCP port 443 makes it pass through even some of the strictest firewalls

IKEv2-based VPNs

- Available on
  - Linux
  - Windows
  - MacOS
- As expected, it relies on IPSec to protect packets
- Similar to L2TP, but there is no PPP encapsulation

AnyConnect / OpenConnect

- Cisco proprietary, but an open source implementation exists (OpenConnect)
  - There is also an open implementation of the server
- Uses DTLS (UDP port 443), but can fall back to TCP if UDP is blocked

- OpenConnect also supports
  - Pulse Secure SSL VPN (formerly Juniper Networks)
  - GlobalProtect SSL VPN (Palo Alto Networks)

Anyconnect server config excerpt

```
tunnel-group ANYCONNECT-TUNNEL-GROUP type remote-access
tunnel-group ANYCONNECT-TUNNEL-GROUP general-attributes
 address-pool ANYCONNECT-POOL
 authentication-server-group LDAP
 default-group-policy GROUPPOLICY-ANYCONNECT
tunnel-group ANYCONNECT-TUNNEL-GROUP webvpn-attributes
 customization ModCustomization
 group-alias CRYSYS-INTERNAL enable
```

```
group-policy GROUPPOLICY-ANYCONNECT internal
group-policy GROUPPOLICY-ANYCONNECT attributes
 dns-server value 10.105.1.254
 vpn-simultaneous-logins 20
 vpn-tunnel-protocol ssl-client ssl-clientless
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value SPLIT-LIST
 default-domain value crysys.hu
```

```
access-list SPLIT-LIST standard permit 10.105.0.0 255.255.254.0
access-list SPLIT-LIST standard permit 10.105.48.0 255.255.240.0
access-list SPLIT-LIST standard permit 172.24.8.0 255.255.255.0
access-list SPLIT-LIST standard permit 172.24.2.0 255.255.255.0
```

VPN vs client-side validation

- Why we should not validate inputs on the client side?
- Routing entries are client side input
  - User can inject new routing entry towards the VPN interface
- Controlling the routing table is not a good idea
  - Race condition
- Using custom client may NOT control the routing table
  - E.g., Openconnect
- Result
  - User uses custom client (not envisioned by developers)
  - User inject new routing entry
  - Unwanted traffic is routed towards the VPN endpoint
  - If the VPN endpoint can route it, it will route it!
- Solution:
  - Server-side input validation (e.g., vpnfilter command)

OpenVPN

- Open source VPN client/server
- Widely available, the "de facto" standard
- By default, it uses its own port (UDP 1194), but it may be set to use any port, even TCP
- Uses TLS for transport
  - May be configured to look like regular HTTPS traffic, but advanced DPI will most likely realize that it's not legit HTTPS

OpenVPN – Interface types

- TAP
  - Transports L2 frames
  - Supports non-IP protocols
  - Extra overhead (broadcasts, extra headers)
- TUN
  - Transports L3 IP packets
  - Supports only IP (and IPv6 in later versions)
  - Lower overhead

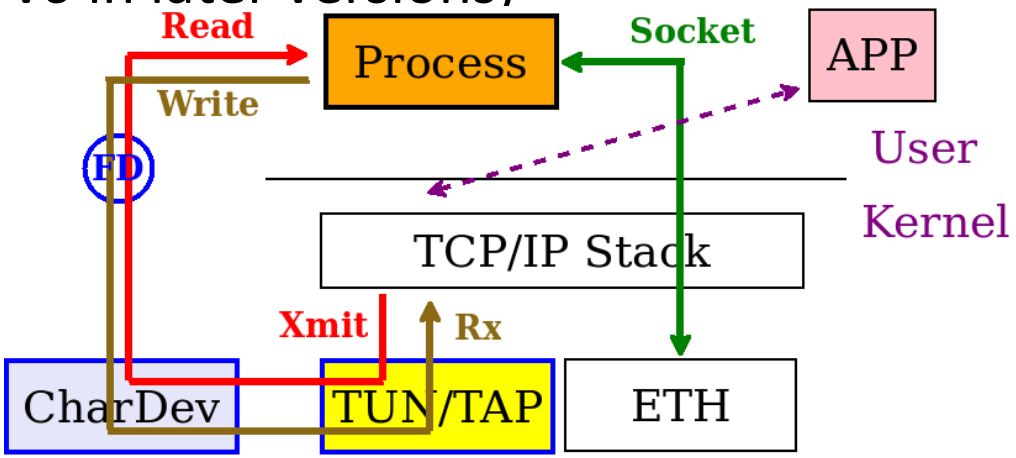


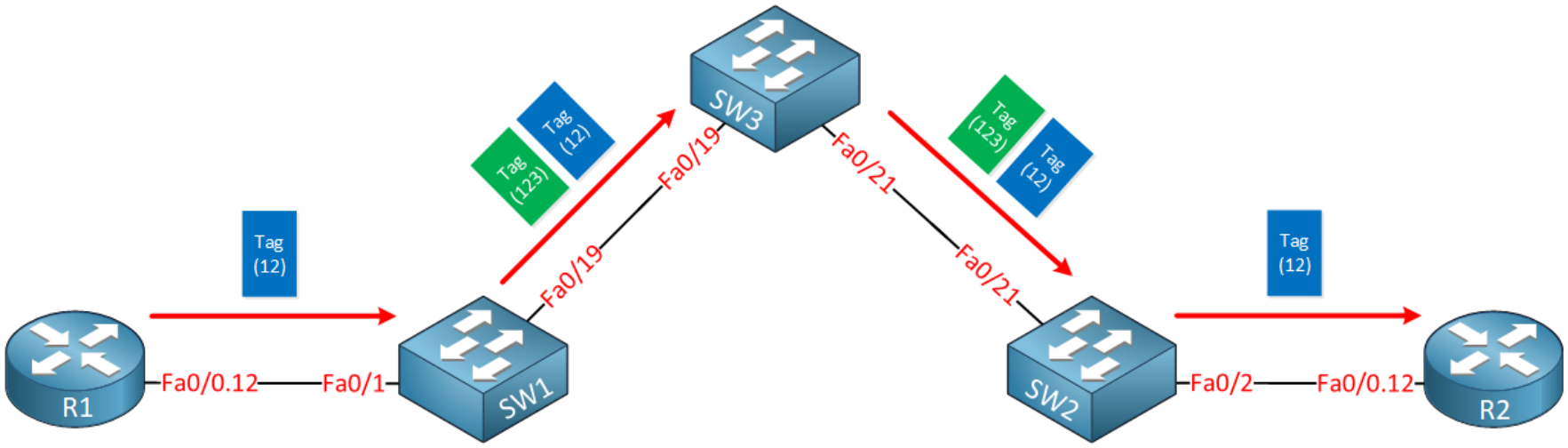
image source: recolog.blogspot.com
example code: http://recolog.blogspot.com/2016/06/tuntap-devices-on-linux.html

OpenVPN example config

```
client

;dev tap
dev tun

;proto tcp
proto udp

remote bl1lgw.hit.bme.hu 1194
;remote my-server-2 1194


# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
ca "C:\\Program Files\\OpenVPN\\config\\..."
cert "C:\\Program Files\\OpenVPN\\config\\..."
key "C:\\Program Files\\OpenVPN\\config\\..."

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
;cipher x
cipher AES-256-CBC
;keysize 256
;link-mtu 1557
```

q-in-q tunnel

- Layer 2 VPN (metro ethernet)
- Customers differentiated by outer VLAN tag
- No cryptographic protection
- No routing protocol needed



Source: networklessons.com

MISCELLANEOUS

Control Questions

- Give a definition of a VPN
- Name two largely different scenarios where VPNs might be used
- What is split tunneling?
- What is DTLS?
- What are the two basic services offered by IPSec?
- What is the purpose of the IPSec AH?
- What is the purpose of the IPSec ESP?
- Does it make any sense to use AH and ESP at the same time? Why (not)?
- In what modes can IPSec operate?

Control Questions

- Explain what a packet protected by IPSec AH in transport mode looks like
- Explain what a packet protected by IPSec ESP in transport mode looks like
- Explain what a packet protected by IPSec AH in tunnel mode looks like
- Explain what a packet protected by IPSec ESP in tunnel mode looks like
- What is a Security Association?
- What is the purpose of the IKE protocol suite?
- You are staying in a hotel where the WiFi only lets you access services on ports UDP 53, TCP 80, and TCP 443. Which of the following VPN methods would work?: PPTP, SSTP, OpenVPN
- Name at least 3 different VPN access methods

Further Reading, Sources

- [MS-SSTP]: Secure Socket Tunneling Protocol (SSTP)
  - https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-sstp
- SKEME: A Versatile Secure Key Exchange Mechanism for Internet
  - http://www.di-srv.unisa.it/~ads/corso-security/www/CORSO-9900/oracle/skeme.pdf
- Naganand Doraswamy, Dan Harkins: IPSec - The New Security Standard for the Internet, Intranets, and Virtual Private Networks
- CCIE or Null! - IKE main mode, aggressive mode, & phase 2
  - https://ccie-or-null.net/2012/03/26/ike-main-mode-aggressive-mode-phase-2/

THANK YOU FOR YOUR ATTENTION!