

# Мрежова сигурност

VPN

Боян Кроснов

[boyan@krosnov.org](mailto:boyan@krosnov.org)

Мариян Маринов

[mm@yuhu.biz](mailto:mm@yuhu.biz)

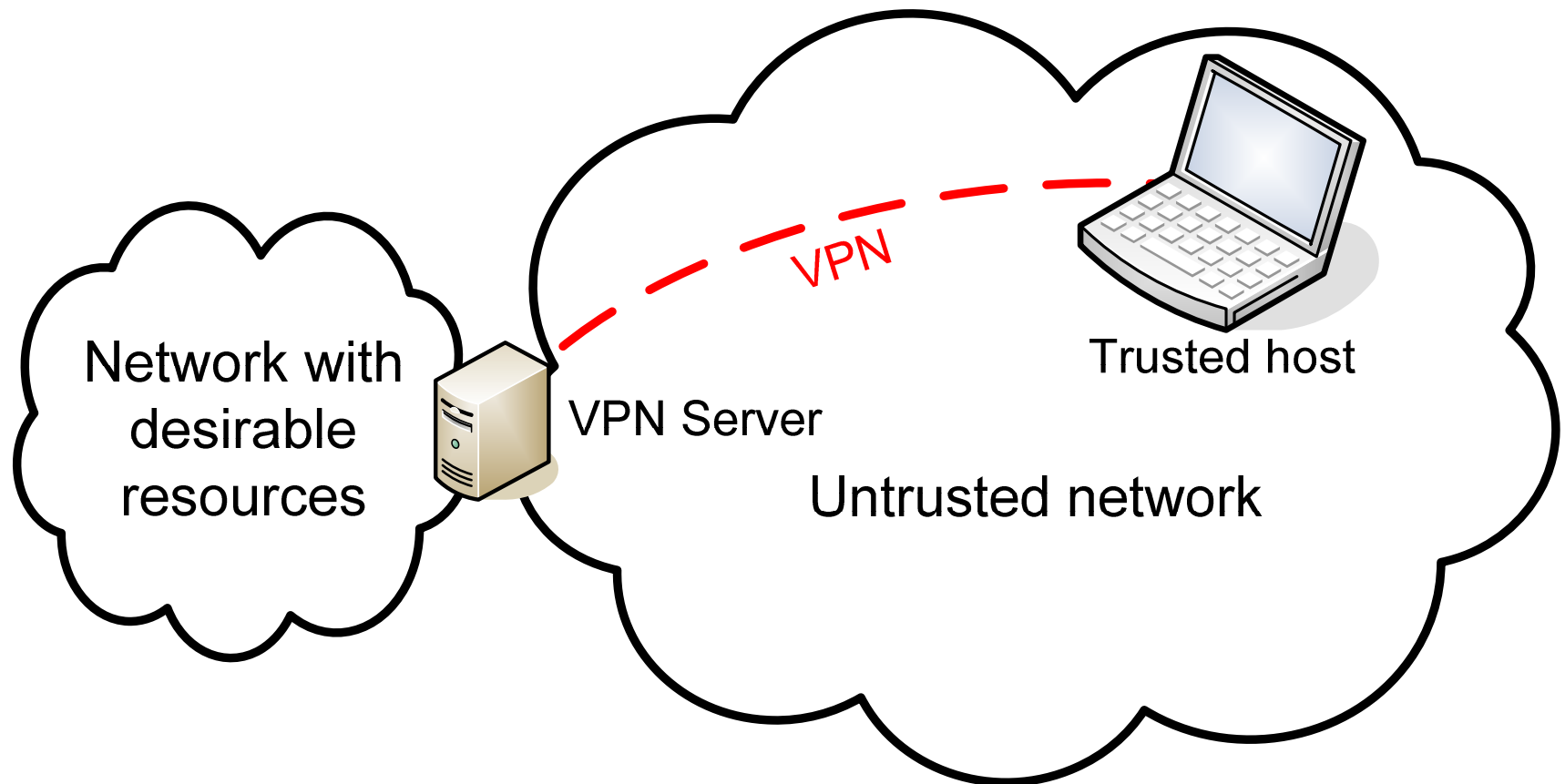
# Лекцията

- Видове VPN
- VPN технологии
- Видове атаки
  
- Заключение и дискусия

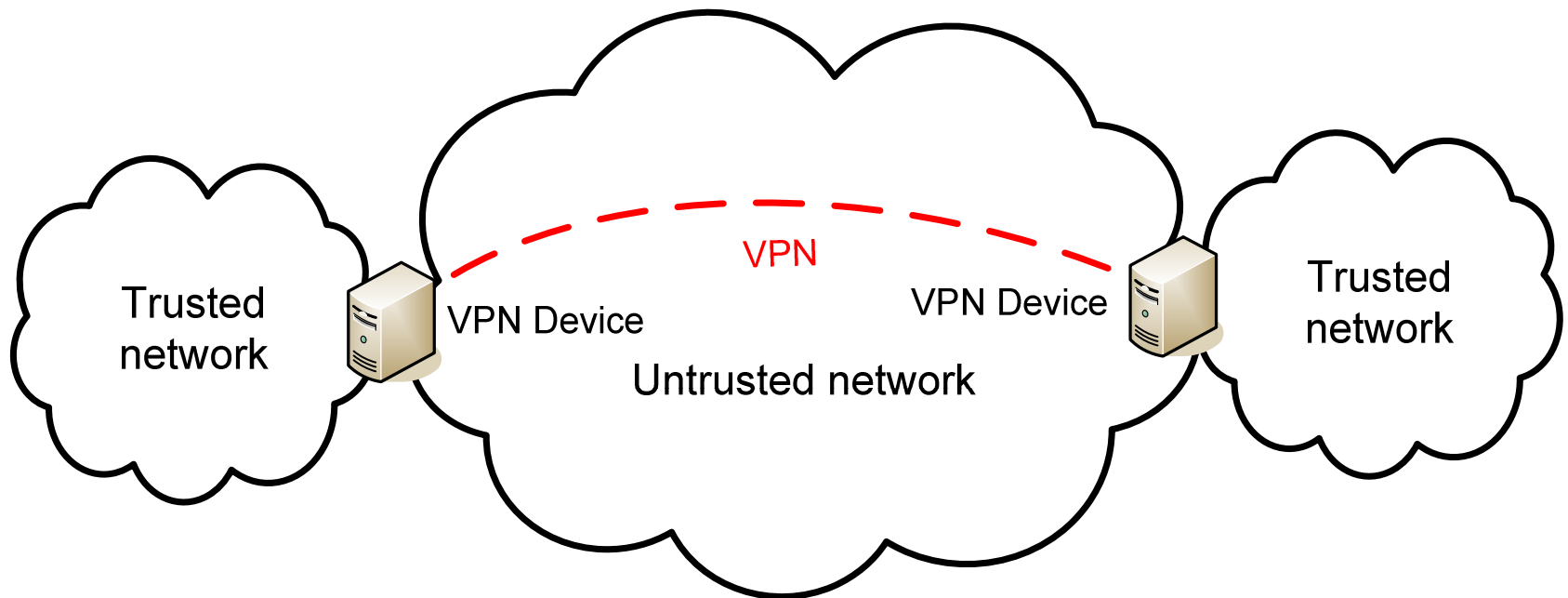
# VPN - дефиниция

- Виртуална
- Частна
- Мрежа
  
- Използва се за гарантиране на
  - Контрол на достъпа
  - Конфиденциалност
  - Достоверност
  
- Няколко различни методи, технологии, понятия под едно име

# Remote access VPN

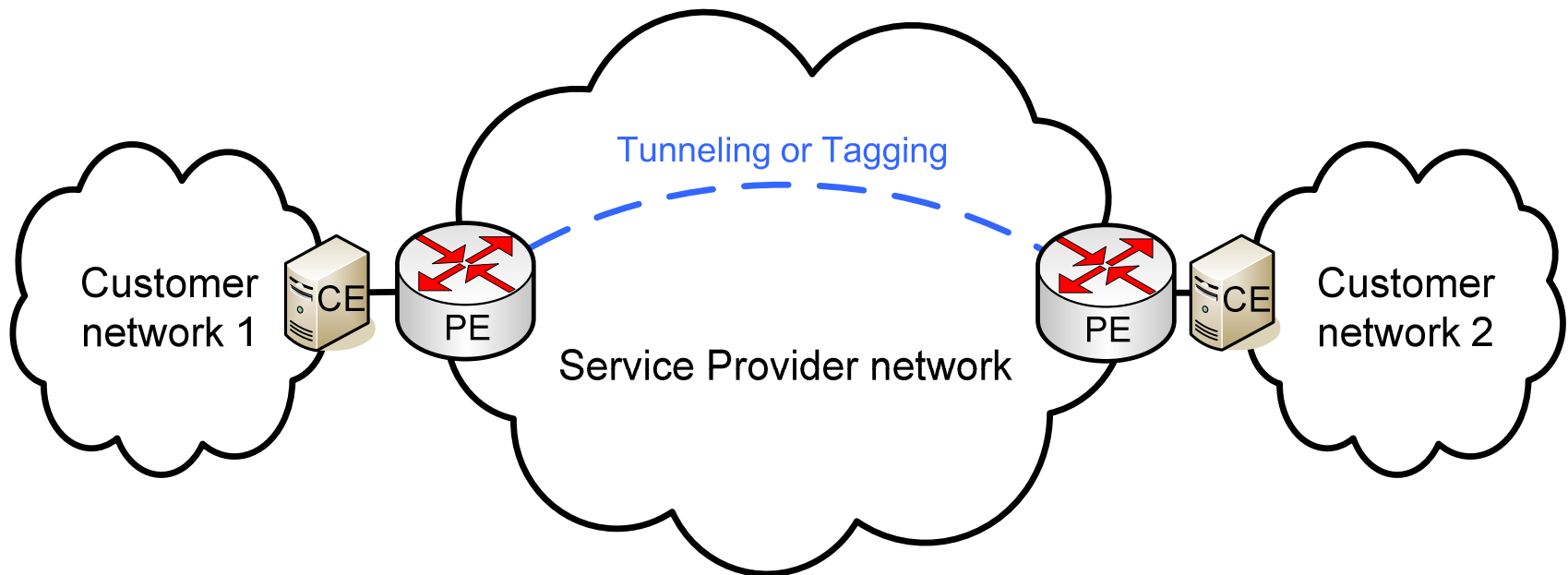


# Site to site VPN



# VPN Service

- aka Network Based VPN



# Видове VPN

- Remote access VPN
- Site to Site VPN
- VPN Service
  
- Layer 2 (прозрачни) vs. Layer 3 (не-прозрачни)
- Point-to-point vs. Multipoint
- Tunneling vs. Tagging

# VPN протоколи

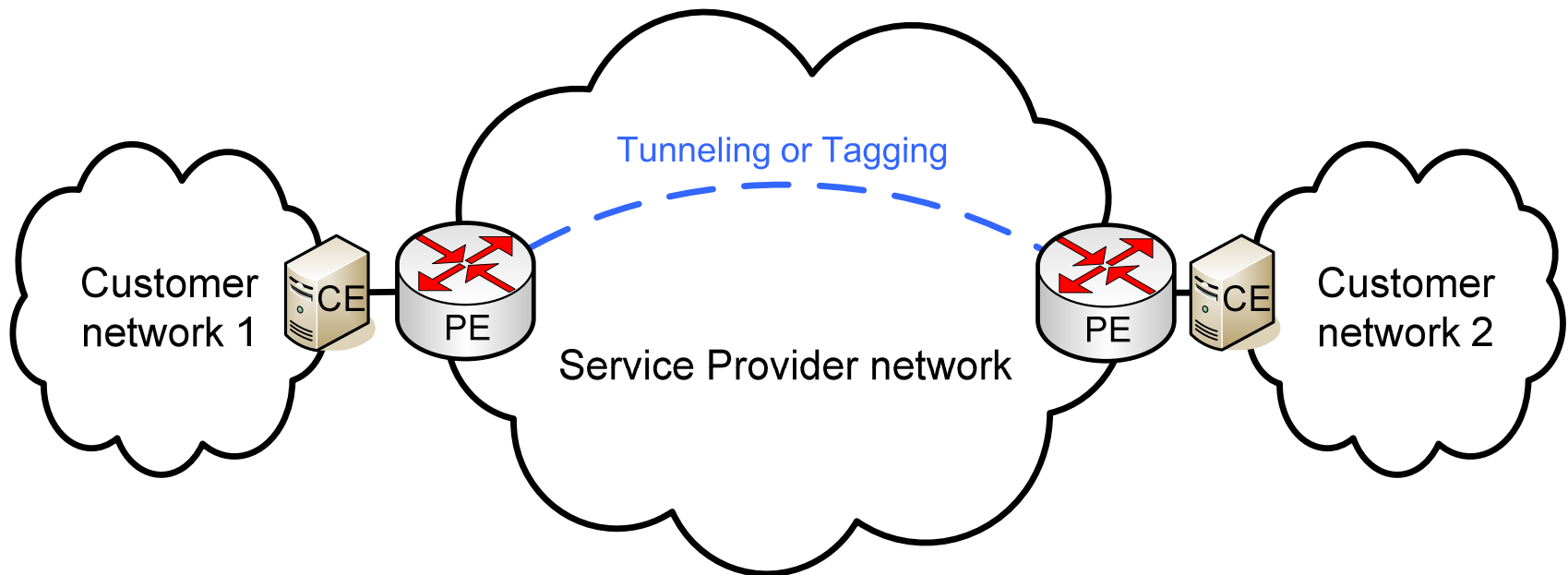
- Layer 2 tagging
  - 802.1q, q-in-q
  - ATM, Frame Relay, X.25 и т.н.
  - MPLS (L3 VPN, AToM, VPLS)
- Layer 2 tunneling
  - PPPoEverything (Ethernet, ATM, GRE, SSH)
  - L2TP, L2TPv3
- IPSec
- SSL VPN
  - OpenVPN
  - SSL Web proxy

# VPN и слоестия модел

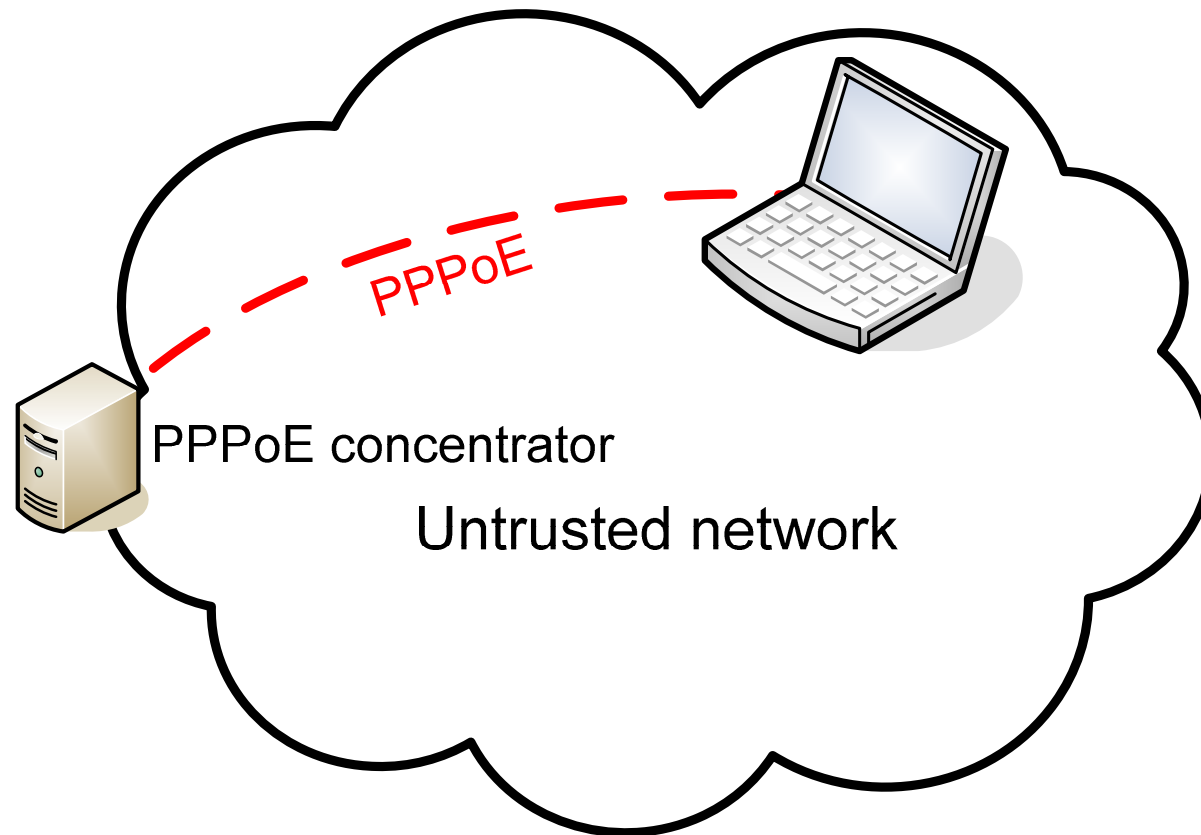
|                 |                  |  |
|-----------------|------------------|--|
| 7. Application  | HTTP, Mail suite | ← PPPoSSH (c. L2, L3)                        |
| 6. Presentation | SSL / TLS        | ← OpenVPN (c. L2, L3), SSL Web Proxy (c. L7) |
| 5. Session      |                  | ← PPTP, L2TP (c. L2, L3)                     |
| 4. Transport    | TCP, UDP         |  |
| 3. Network      | IP               | ← IPSec (c. L3, L4)                          |
| 2. Datalink     | Ethernet, PPP    | ← PPPoE, PPPoA (c. L2, L3); MPLS (c. L2, L3) |
|                 |                  | ← 802.1q, ATM, FR, X.25 (c. L3)              |
| 1. Physical     | 100Base-TX, V.34 |  |

# Layer 2 tagging

- Layer 2 tagging
  - 802.1q, q-in-q
  - ATM, Frame Relay, X.25 и т.н.
  - MPLS (L3 VPN, AToM, VPLS)



# PPPoE technology



- PPTP on Layer 4
- PPPoE/PPPoA on Layer 2

# PPPoE technology

- RFC 2616 (PPPoE), RFC 2684 (PPPoA)
- Client/Server
- PPP layer authentication (EAP, PAP, CHAP, etc.)
- PPP layer encryption (ECP)
  - PADI (Active Discovery Initiation)
  - PADO (Active Discovery Offer)
  - PADR (Active Discovery Request)
  - PADS (Active Discovery Session-confirmation)
  - PADT (Active Discovery Termination)

# PPTP technology

- RFC 2637
- Client/Server
- PPP layer authentication (EAP, PAP, CHAP, etc.)
- PPP layer encryption (ECP)
  
- TCP port 1723 (session control)
- PPP over GRE

# PPTP attacks

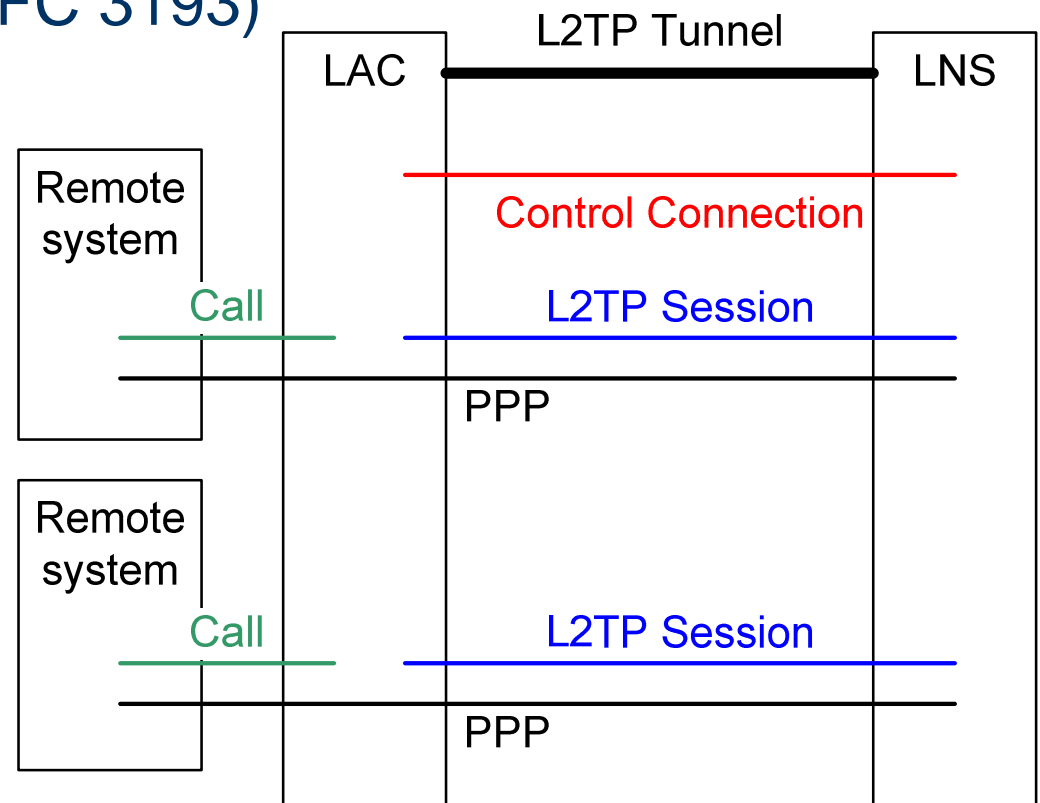
- Flood

- asleep

"... we do not have any plans for proactive communication at this point beyond the best practice guidance we already have out there." // Microsoft 2004

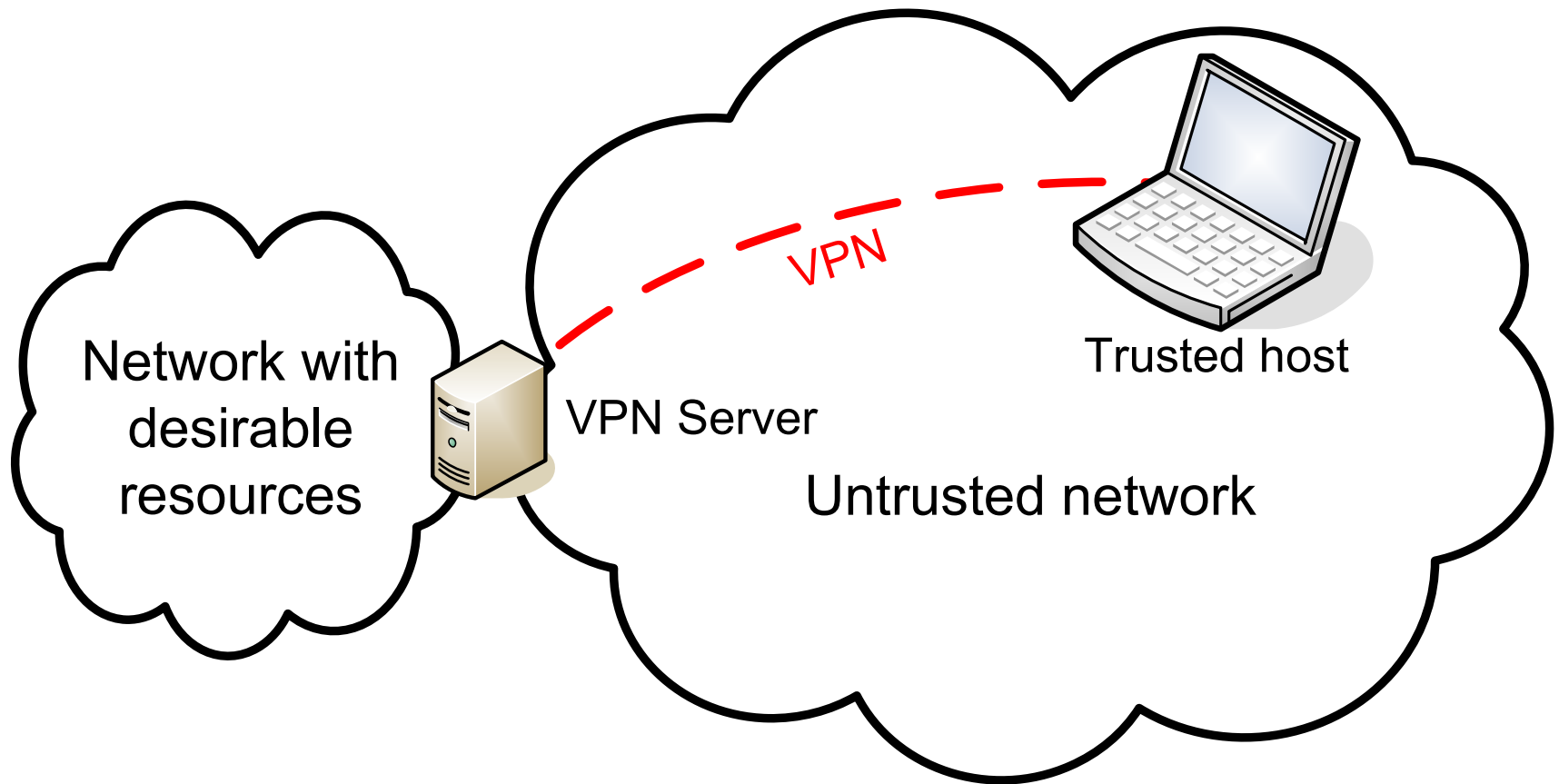
# L2TP

- IETF RFC 2661
- PPP layer security
- L2TP over IPSec (RFC 3193)



# L2TP

- L2TP over IPSec (RFC 3193)



# IPSec

- RFC 4301 “Security Architecture for the Internet Protocol”
- Tunnel mode
- Transport mode

Unprotected

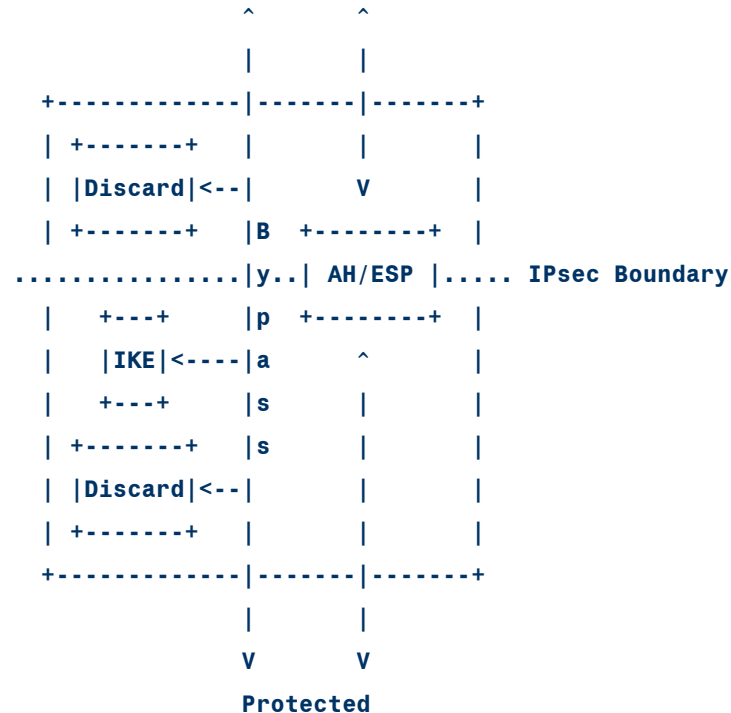


Figure 1. Top Level IPsec Processing Model

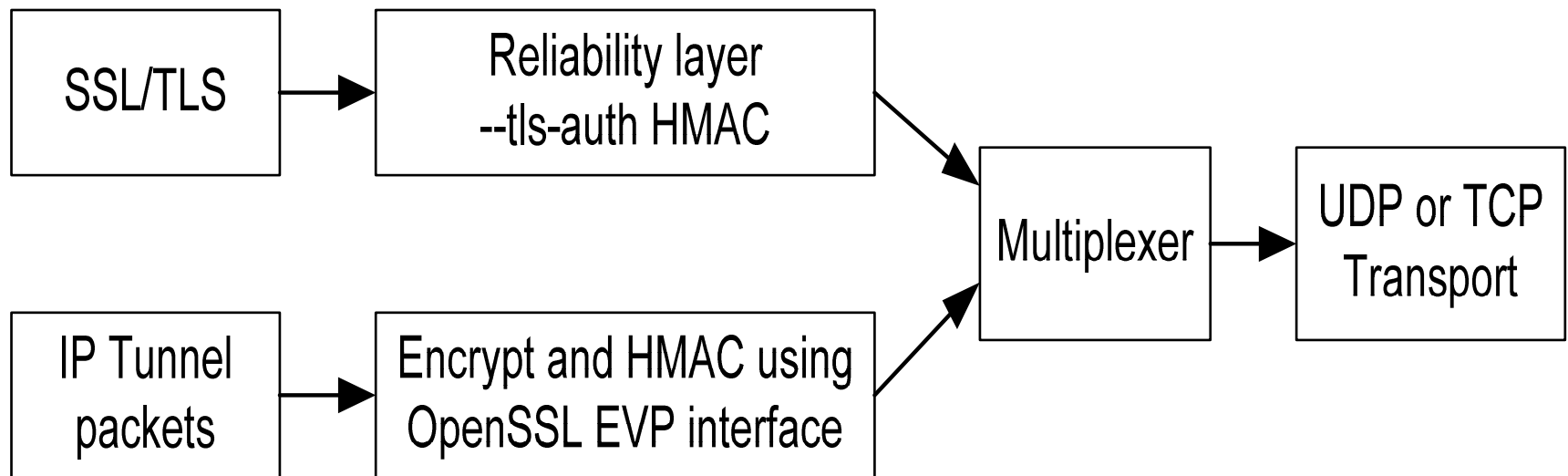
# IPSec

- ESP (Encapsulating Security Payload)
- AH (Authentication Header)
- IKE, ISAKMP (RFC2407, 2408, 2409)
- IKEv2 (RFC 4306)
- NAT-T (IPSec in UDP) (RFC 3947, 3948)

# IKEv2

- IKEv2 (RFC 4306)
  - Fewer RFCs
  - Simpler message exchange
  - Fewer crypto mechanisms
  - Reliability and State management
  - DoS attack resilience
  - OpenIKE, strongSwan 4.0 and other opensource implementations
  - 8) To fix cryptographic weaknesses such as the problem with symmetries in hashes used for authentication documented by Tero Kivinen;

# OpenVPN technology



- Uses OpenSSLv3 / OpenTLSv1

# OpenVPN technology

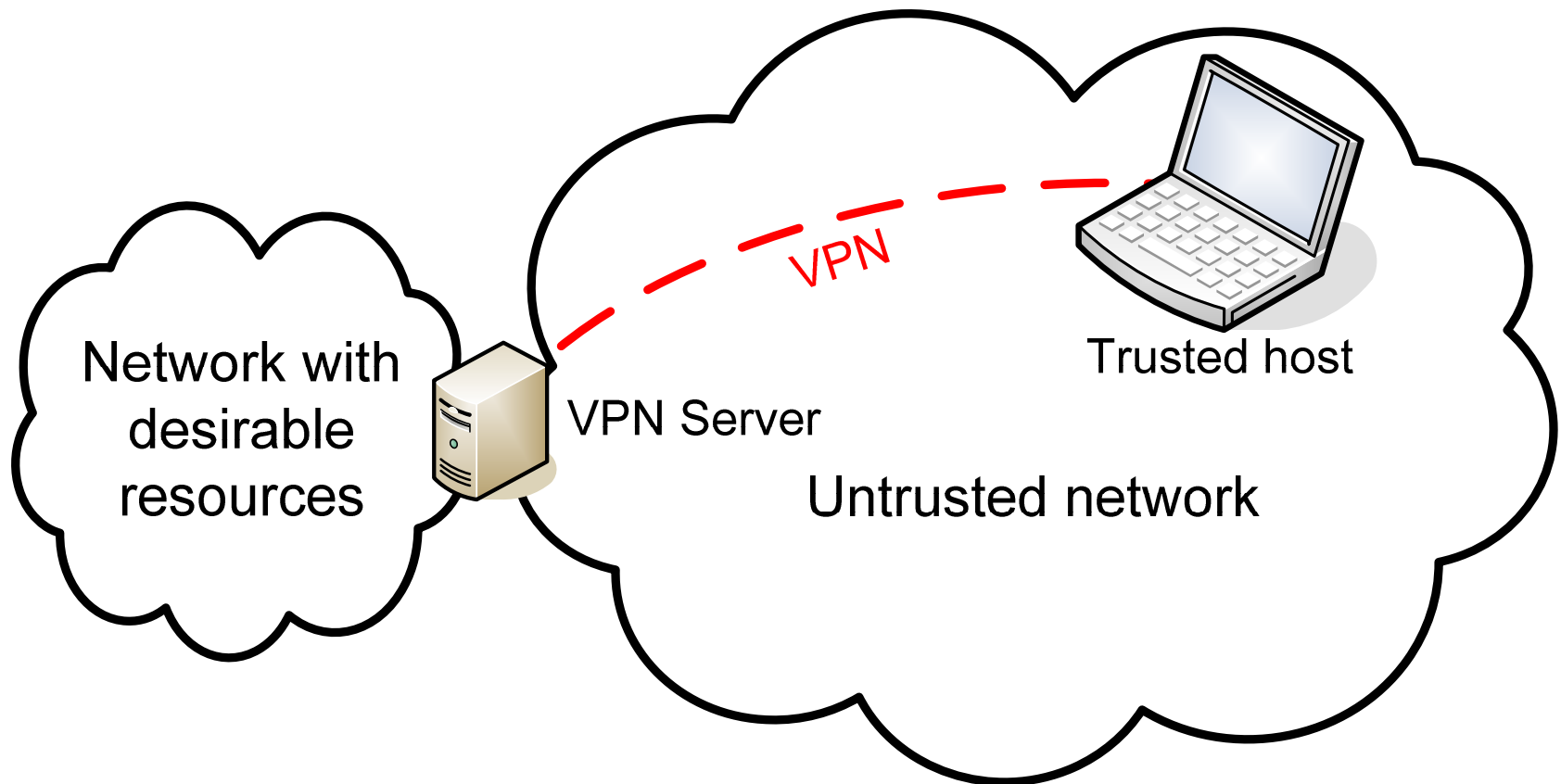
- Authentication
  - pre-shared secret
  - certificate based
  - username / password based (PAM)
- Security
  - runs as normal user
  - chroot
  - supports smart cards

# OpenVPN technology

- Network
  - over TCP or UDP
  - through HTTP proxy and NAT
  - LZO compression
  - Provides TUN (L3) or TAP (L2) interface
  - Client-server and Client-to-client
  - site-to-site and remote access VPN

# SSL Web proxy

- SSL session to a proxy server
- Web resource remains hidden in trusted network



# References

- <http://www.ietf.org/rfc.html>
  - 2561 (PPPoE), 2684(PPPoA), 2637(PPTP)
  - 2661 (L2TP), 3193 (L2TP over IPSec)
  - 4301-4309 (IPSec)
- <http://asleap.sf.net/> (PPTP cracker)
- Wikipedia
- Google