Welcome to

5. Virtual Private Network

Communication and Network Security 2020

Henrik Kramselund Jereminsen hkj@zencurity.com @kramse

Slides are available as PDF, kramse@Github

5-Virtual-Private-Network.tex in the repo security-courses

Goals for today

Todays goals:

- Introduce Virtual Private Networks
- Present the common protocols, and some tools used

Photo by Thomas Galler on Unsplash

Plan for today

Subjects

- IPsec and L2TP/IPsec
- TLS VPN with example OpenVPN
- Linux Wireguard VPN
- Microsoft DirectAccess and VPN (RAS)

Exercises

-

Time schedule

- 17:00 - 18:15
  Introduction and basics
- 30min break
- 18:45 - 19:30
- 15min break
- 19:45 -20:30 45min

Reading Summary, continued

The Zeek Network Security Monitor

ANSM chapter 7: Detection Mechanisms and Indicators of Compromise, and Signatures

- Indicators of Compromise (IOC) any piece of information that can be used to objectively describe a network intrusion, expressed in a platform-independent manner
- Background information, useful when we talk about Zeek (previously Bro) later
- Intrusion Detection Systems try to detect ... but what if we know that some domains, servers, IPs etc are signs of bad activity - even compromise
- IP reputation - some IPs are used for controlling malware command and control (C2) servers etc.
- A signature can contain one or more IOCs

Reading Summary, continued

ANSM chapter 8: Reputation-Based Detection

- The most basic form of intrusion detection is reputation-based detection
- Similar concept to blacklisting SMTP spam relays
- I often recommend `https://github.com/stamparm/maltrail` as a source of lists
- Other sources are lists like RIPE NCC delegated, which IP prefixes are handed out in different countries
  `https://ftp.ripe.net/pub/stats/ripencc/delegated-ripencc-extended-latest`
  `ripencc|DK|ipv4|185.129.60.0|1024|20151130|allocated|`
- Mentions SiLK `https://tools.netsa.cert.org/silk/`
  If we end up having time today, or another day, we should look into this tool chain also!

Reading Summary

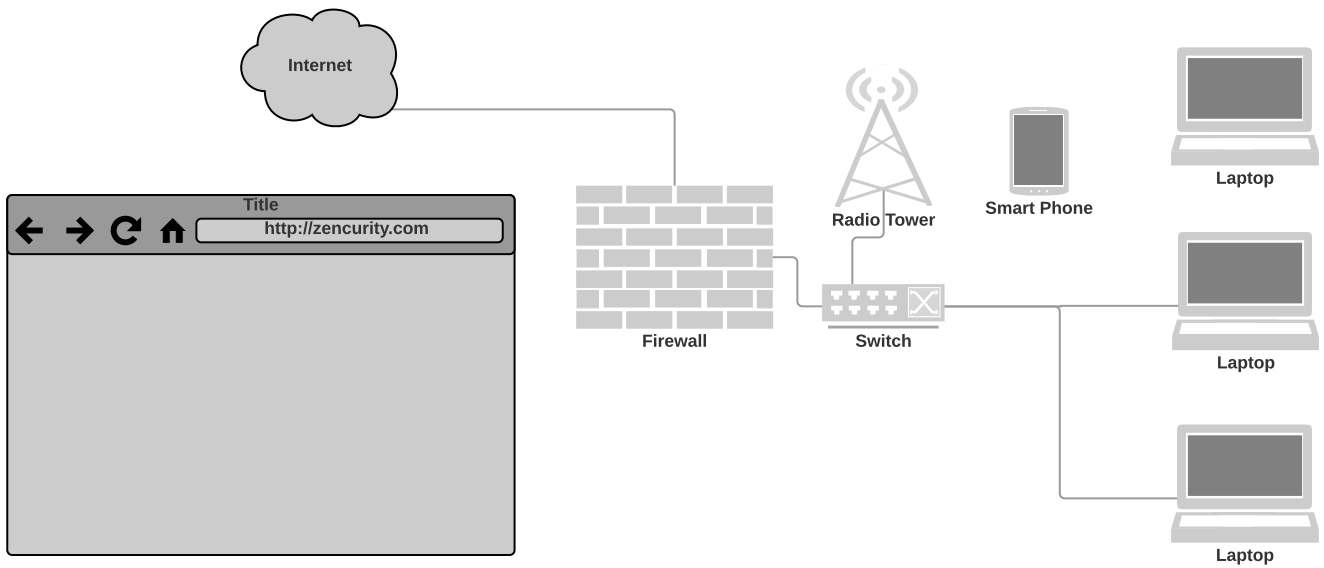
VPN are everywhere, but could be better!

https://en.wikipedia.org/wiki/Virtual_private_network
https://kb.juniper.net/InfoCenter/index?page=content&id=KB11104
IPSec VPN between JUNOS and Cisco IOS
Skim:
https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching
https://en.wikipedia.org/wiki/OpenVPN
https://en.wikipedia.org/wiki/IPsec
https://en.wikipedia.org/wiki/DirectAccess
https://www.wireguard.com/papers/wireguard.pdf

Fokus 2020: VPN alle steder

- VPN er relevant for alle der har data af værdi
- Sikrer data der flyttes
- Virtual Private Network dækker over klienter der kobler op, og site-2-site

Your Privacy



- Your data travels far
- Often crossing borders, virtually and literally

Data found in Network data

Lets take an example, DNS

Domain Name System DNS breadcrumbs

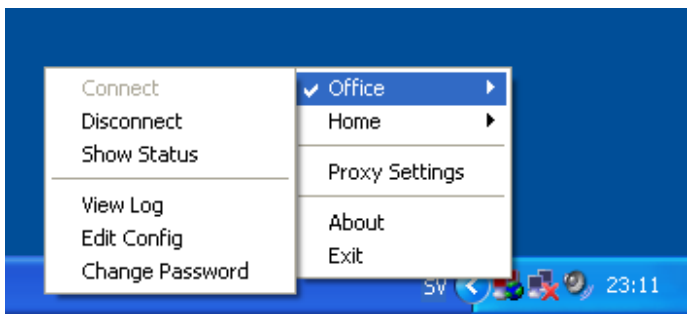
- Your company domain, mailservers, vpn servers
- Applications you use, checking for updates, sending back data
- Web sites you visit

Advice show your users,ask them to participate in a experiment

Join this Wireless network SSID and we will show you who you are on the internet

Maybe use VPN more - or always!

VPN



Virtual Private Networks are useful - or even required when travelling

VPN `http://en.wikipedia.org/wiki/Virtual_private_network`

SSL/TLS VPN - Multiple incompatible vendors: OpenVPN, Cisco, Juniper, F5 Big IP

IETF IPsec does work cross-vendors - sometimes, and is also increasingly becoming blocked or unusable due to NAT :-(

Recommended starting point OpenVPN - free and open, clients for "anything"

VPN without encryption

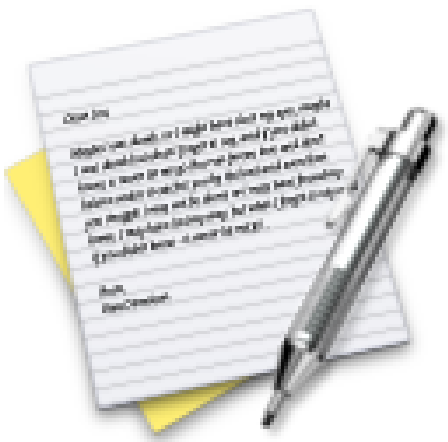
> Multiprotocol Label Switching (MPLS) is a routing technique in telecommunications networks that directs data from one node to the next based on short path labels rather than long network addresses, thus avoiding complex lookups in a routing table and speeding traffic flows.[
> ... MPLS works by prefixing packets with an MPLS header, containing one or more labels.

Source:

`https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching`

- The term VPN is also used in cases without encryption
- MPLS allows multiple customers to use the same IP prefixes, like 10/8
- MPLS is used in many provider networks
- Another example is Generic Routing Encapsulation (GRE), which is often then protected with IPsec
- People today also uses Virtual Extensible LAN (VXLAN) for cloud computing

Exercise

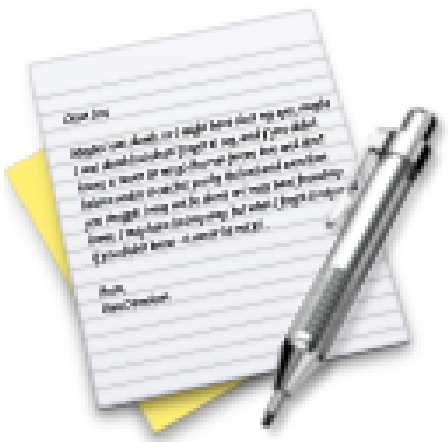


Now lets do the exercise

Frankenpacket - 20 min

which is number **34** in the exercise PDF.

Exercise



Now lets do the exercise

Bonus: Creating Frankenpackets - 15 min

which is number **35** in the exercise PDF.

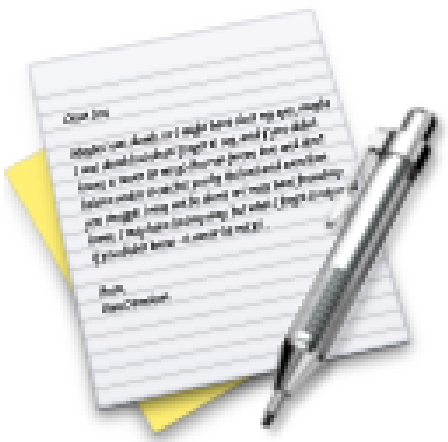
Linux Wireguard VPN

> WireGuard is a secure network tunnel, operating at layer 3, implemented as a kernel virtual network interface for Linux, which aims to replace both IPsec for most use cases, as well as popular user space and/or TLS-based solutions like OpenVPN, while being more secure, more performant, and easier to use.

Description from `https://www.wireguard.com/papers/wireguard.pdf`

- Going to be interesting!
- single round trip key exchange, based on NoiseIK
- Short pre-shared static keys—Curve25519
- strong perfect forward secrecy
- Transport speed is accomplished using ChaCha20Poly1305 authenticated-encryption
- encapsulation of packets in UDP
- WireGuard can be simply implemented for Linux in less than 4,000 lines of code, making it easily audited and verified

Exercise



Now lets do the exercise

Bonus: Wireguard - 60 min

which is number **36** in the exercise PDF.

IPsec

Sikkerhed i netværket

RFC-2401 Security Architecture for the Internet Protocol

RFC-2402 IP Authentication Header (AH)

RFC-2406 IP Encapsulating Security Payload (ESP)

RFC-2409 The Internet Key Exchange (IKE) - dynamisk keying

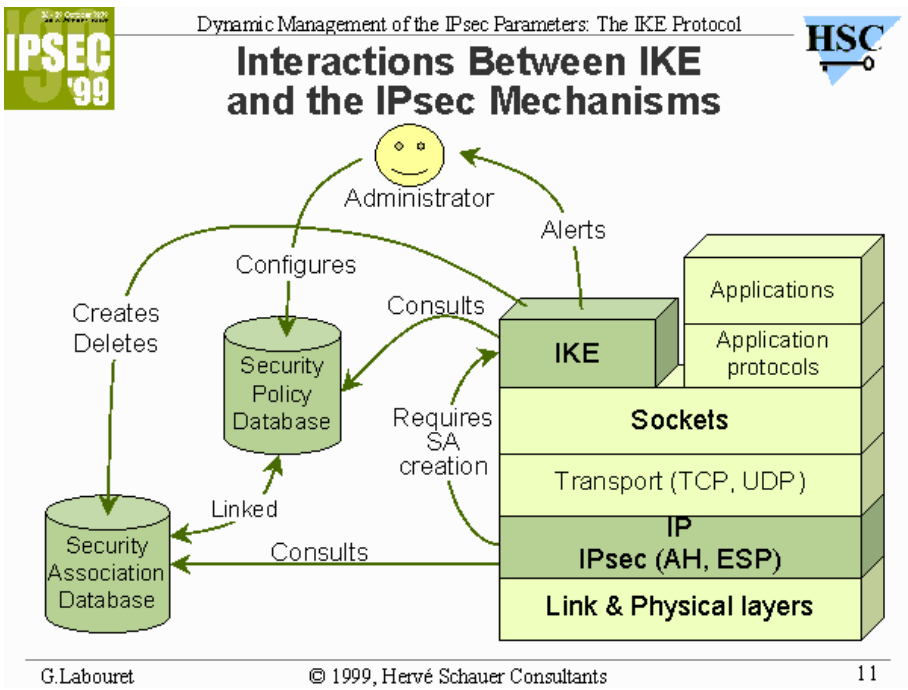
... IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap
`https://tools.ietf.org/html/rfc6071`

Både til IPv4 og IPv6

MANDATORY i IPv6! - et krav hvis man implementerer fuld IPv6 support

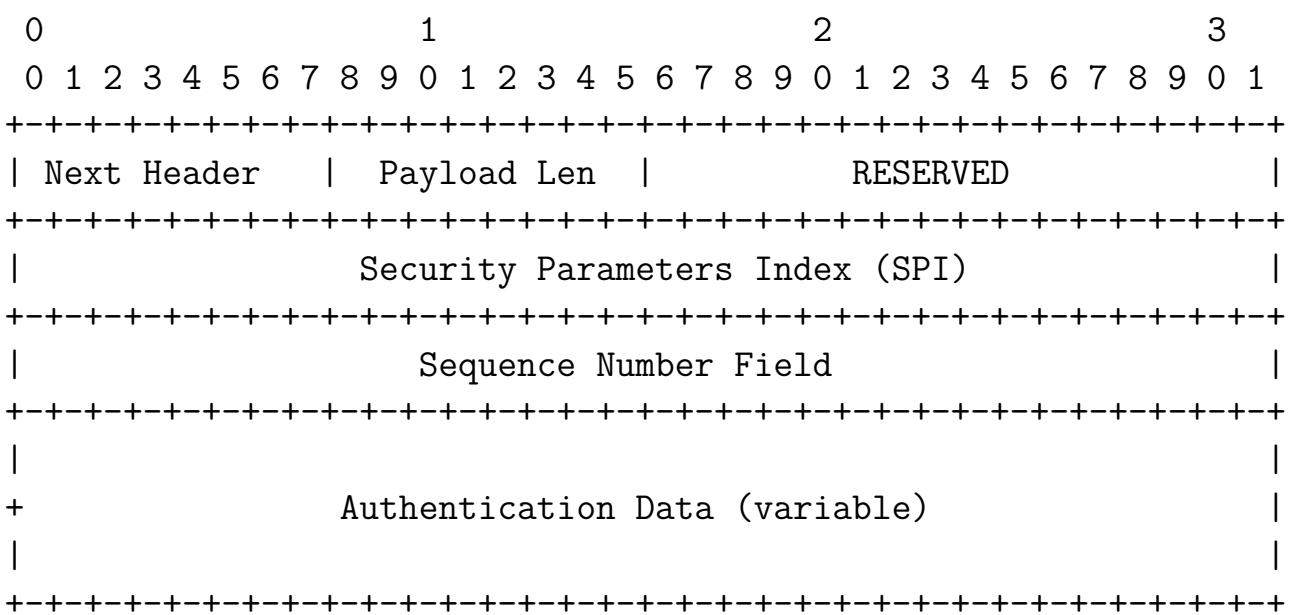
Der findes IKEscan til at scanne efter IKE porte/implementationer
`http://www.nta-monitor.com/ike-scan/index.htm`

IPsec er ikke simpelt!



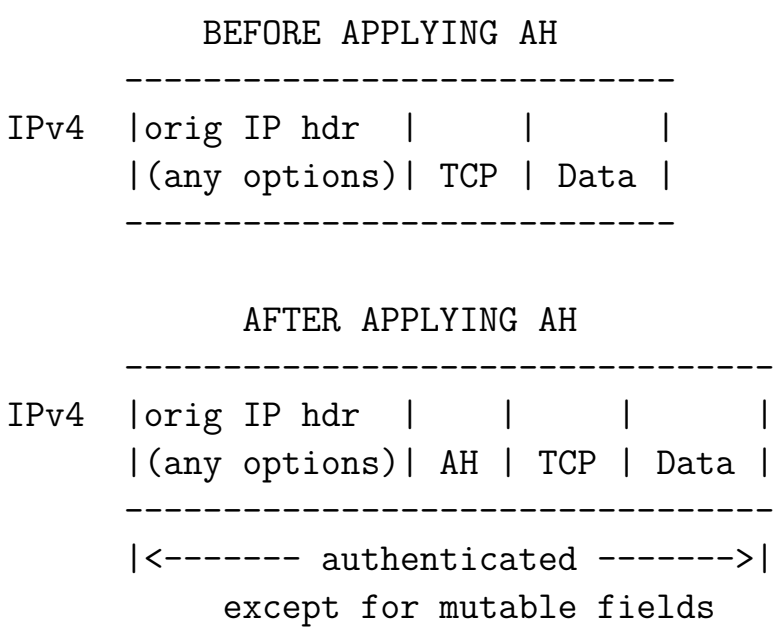
Kilde: `http://www.hsc.fr/presentations/ike/`

RFC-2402 IP Authentication Header AH

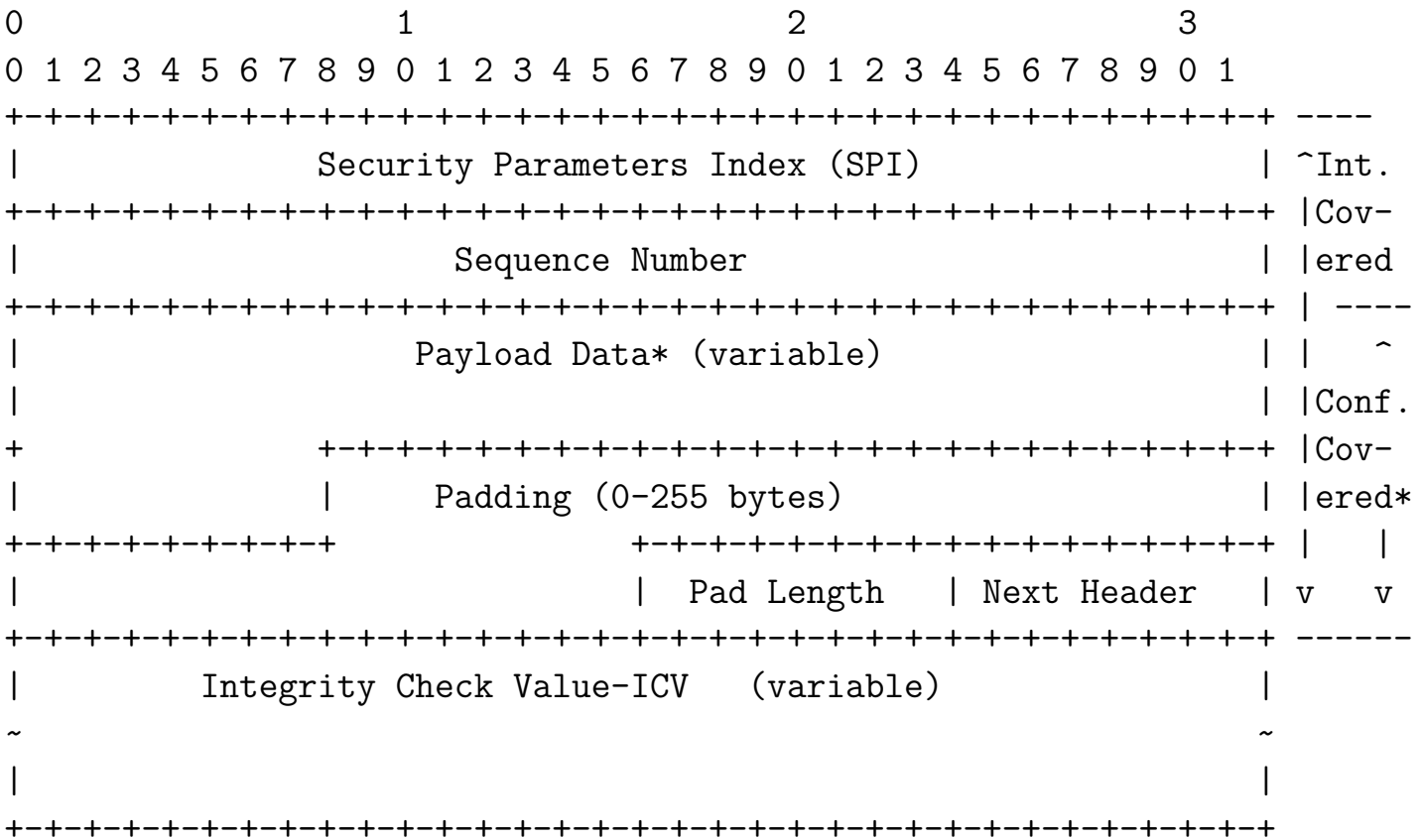


RFC-2402 IP Authentication Header AH

Indpakning - pakkerne før og efter Authentication Header:



RFC-2406 IP Encapsulating Security Payload ESP



RFC-2406 IP Encapsulating Security Payload ESP

Pakkerne før og efter:

```
              BEFORE APPLYING ESP
            ----------------------------------------
      IPv6  |              | ext hdrs |     |      |
            | orig IP hdr  |if present| TCP | Data |
            ----------------------------------------


              AFTER APPLYING ESP
            ------------------------------------------------------------
      IPv6  | orig |hop-by-hop,dest*,|   |dest|   |     | ESP   | ESP|
            |IP hdr|routing,fragment.|ESP|opt*|TCP|Data|Trailer|Auth|
            ------------------------------------------------------------
                                    |<---- encrypted ---->|
                                  |<---- authenticated ---->|
```

IPsec setup eksempel

Client: Mac OS X/NetBSD/FreeBSD - samme syntaks
`rc.ipsec.client`

Server: OpenBSD - bruger ipsecadm kommando
`rc.ipsec.server`

Dette setup når vi ikke at demonstrere

Vises for at trigge forundring over hvor kryptiske sådanne konfigurationer kan se ud!

rc.ipsec.client - client setup - adresser

```
#!/bin/sh
# /etc/rc.ipsec.client - IPsec client configuration
# built from http://rt.fm/~jcs/ipsec_wep.phtml
# FreeBSD/NetBSD syntaks! - used on Mac OS X
# IPv4
SECSERVER=10.0.42.1
SECCLIENT=10.0.42.53
# IPv6
#SECSERVER=2001:618:433:101::1
#SECCLIENT=2001:618:433:101::153
ESPKEY=`cat ipsec.esp.key`
AHKEY=`cat ipsec.ah.key`

# Flush IPsec SAs in case we get called more than once
setkey -F
setkey -F -P
```

rc.ipsec.client - client setup - SAs

```
# Establish Security Associations
# 1000 is from the server to the client
# 1001 is from the client to the server
setkey -c <<EOF

add $SECSERVER $SECCLIENT esp 0x1000  -m tunnel -E blowfish-cbc 0x$ESPKEY  -A hmac-sha1 0x$AHKEY;

add $SECCLIENT $SECSERVER esp 0x1001  -m tunnel -E blowfish-cbc 0x$ESPKEY -A hmac-sha1 0x$AHKEY;

spdadd $SECCLIENT $SECSERVER any -P out  ipsec esp/tunnel/$SECCLIENT-$SECSERVER/default;

spdadd $SECSERVER $SECCLIENT any -P in  ipsec esp/tunnel/$SECSERVER-$SECCLIENT/default;
EOF
```

rc.ipsec.server - server setup - adresser

```
#!/bin/sh
# /etc/rc.ipsec - IPsec server configuration
# built from http://rt.fm/~jcs/ipsec_wep.phtml
# OpenBSD syntaks!
SECSERVER=10.0.42.1
SECCLIENT=10.0.42.53
#SECSERVER6=2001:618:433:101::1
#SECCLIENT6=2001:618:433:101::153

ESPKEY=`cat ipsec.esp.key`
AHKEY=`cat ipsec.ah.key`

# Flush IPsec SAs in case we get called more than once
ipsecadm flush
```

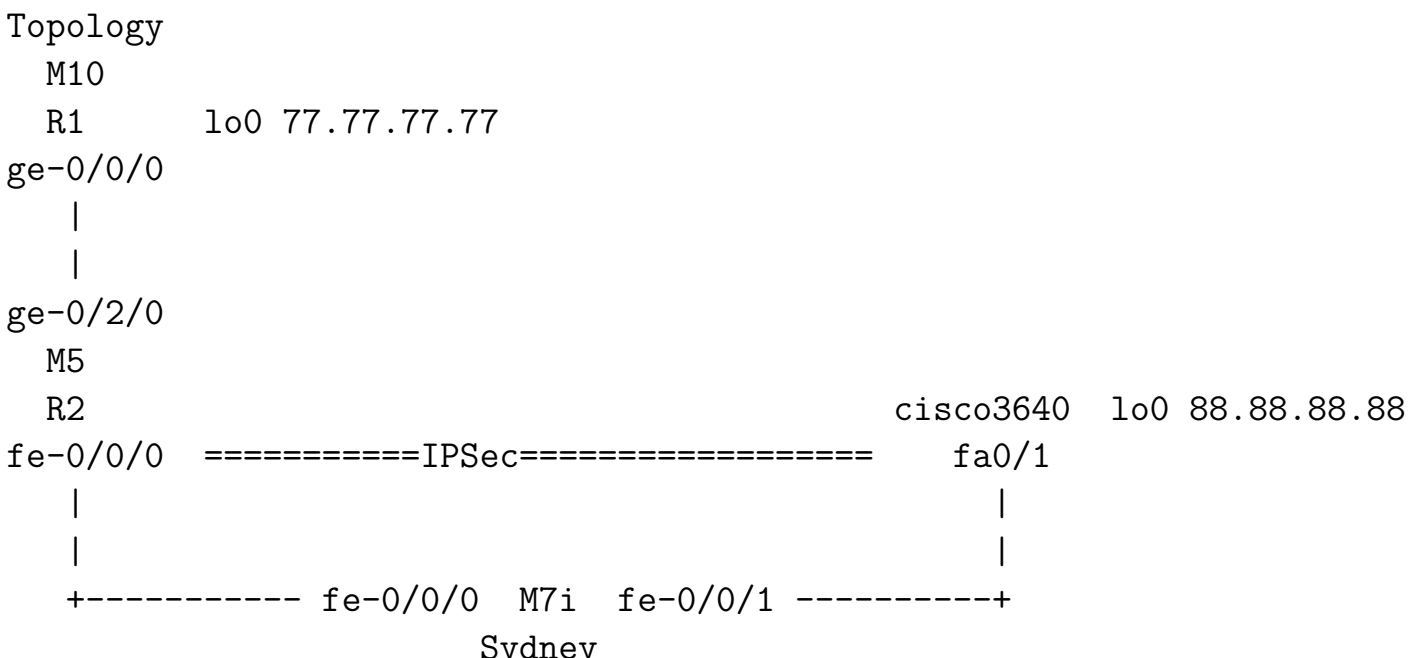
rc.ipsec.server - server setup - SAs

```
# Establish Security Associations
#
# 1000 is from the server to the client
ipsecadm new esp -spi 1000 -src $SECSERVER -dst $SECCLIENT  -forcetunnel -enc blf -key $ESPKEY  -auth sha1 -
authkey $AHKEY

# 1001 is from the client to the server
ipsecadm new esp -spi 1001 -src $SECCLIENT -dst $SECSERVER  -forcetunnel -enc blf -key $ESPKEY  -auth sha1 -
authkey $AHKEY
```

rc.ipsec.server - server setup - flows

```
# Create flows
# Data going from the outside to the client
ipsecadm flow -out -src $SECSERVER -dst $SECCLIENT -proto esp

-addr 0.0.0.0 0.0.0.0 $SECCLIENT 255.255.255.255 -dontacq
# IPv6
#ipsecadm flow -out -src $SECSERVER -dst $SECCLIENT -proto esp

#-addr :: :: $SECCLIENT ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff -dontacq

# Data going from the client to the outside
ipsecadm flow -in -src $SECSERVER -dst $SECCLIENT -proto esp

-addr $SECCLIENT 255.255.255.255 0.0.0.0 0.0.0.0 -dontacq
# IPv6
#ipsecadm flow -in -src $SECSERVER -dst $SECCLIENT -proto esp

#-addr :: :: $SECCLIENT ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff -dontacq
```

IPSec VPN between JUNOS and Cisco IOS



Source: https://kb.juniper.net/InfoCenter/index?page=content&id=KB11104

Cisco IOS crypto setup

```
cisco3640#sh run
crypto isakmp policy 10
 authentication pre-share
 group 2
 lifetime 3600
crypto isakmp key key123 address 11.0.0.1
!
!
crypto ipsec transform-set ts esp-3des esp-sha-hmac
crypto ipsec transform-set ts-man esp-des esp-md5-hmac
!
crypto map dyn 10 ipsec-isakmp
 set peer 11.0.0.1
 set transform-set ts
 match address 120
```

Not recommended settings! See later! People still use these examples!

Routing and addresses

```
interface Loopback1
 ip address 88.88.88.88 255.255.255.255
interface FastEthernet0/1
 ip address 12.0.0.1 255.255.255.252
 duplex auto
 speed auto
 no cdp enable
 crypto map dyn
!
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/1
ip route 11.0.0.0 255.255.255.252 12.0.0.2
ip route 77.77.77.77 255.255.255.255 FastEthernet0/1
ip route 99.99.99.0 255.255.255.0 FastEthernet0/1
!
access-list 120 permit ip host 88.88.88.88 host 77.77.77.77
end
```

Layer 2 Tunneling Protocol L2TP

Description from `https://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol`

> The entire L2TP packet, including payload and L2TP header, is sent within a User Datagram Protocol (UDP) datagram. A virtue of transmission over UDP (rather than TCP; c.f. SSTP) is that it avoids the "TCP meltdown problem".[3][4] It is common to carry PPP sessions within an L2TP tunnel. L2TP does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as L2TP/IPsec (discussed below).

Often used when crossing NAT, which everyone does ...

Configuration example for Cisco:

`https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14122-24.html`

OpenBSD L2TP IPsec

`https://www.exoscale.com/syslog/building-an-ipsec-gateway-with-openbsd/`

IPsec IKE-SCAN

Scan IPs for VPN endpoints with ike-scan:

```
root@kali:~# ike-scan 91.102.91.30
Starting ike-scan 1.9 with 1 hosts
(http://www.nta-monitor.com/tools/ike-scan/)
91.102.91.30 Notify message 14 (NO-PROPOSAL-CHOSEN)
HDR=(CKY-R=f0d6043badb2b7bc, msgid=f97a7508)

Ending ike-scan 1.9: 1 hosts scanned in 1.238 seconds (0.81 hosts/sec).
0 returned handshake; 1 returned notify
```

Source:

`http://www.nta-monitor.com/tools-resources/security-tools/ike-scan`

crack IKE psk?

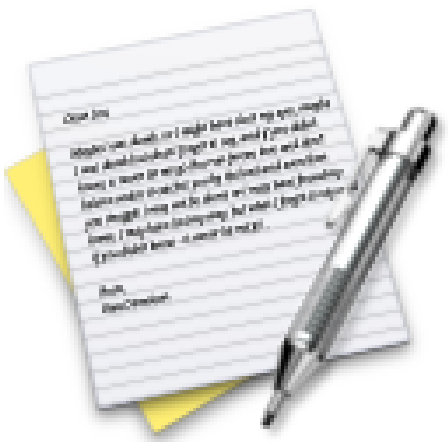
`http://ikecrack.sourceforge.net/`

`https://www.trustwave.com/Resources/SpiderLabs-Blog/Cracking-IKE-Mission-Improbable-(Part-1)/`

ike-scan network scanning

```
hlk@cornerstone03:~$ sudo ike-scan -M 91.102.91.0/24
Starting ike-scan 1.9 with 256 hosts
(http://www.nta-monitor.com/tools/ike-scan/)
91.102.91.14 Notify message 14 (NO-PROPOSAL-CHOSEN)
HDR=(CKY-R=94dd41cf44da082b, msgid=602c35c1)
91.102.91.30 Notify message 14 (NO-PROPOSAL-CHOSEN)
HDR=(CKY-R=e21e89d16f898aa5, msgid=ff41d51c)
91.102.91.70 Notify message 14 (NO-PROPOSAL-CHOSEN)
HDR=(CKY-R=e882d9b4477b847b, msgid=55be4339)
91.102.91.78 Notify message 14 (NO-PROPOSAL-CHOSEN)
HDR=(CKY-R=1fc54d8c3042daa3, msgid=ea705f39)
91.102.91.150 Notify message 14 (NO-PROPOSAL-CHOSEN)
HDR=(CKY-R=d5470f881de6d2d9, msgid=2bf5f5ef)
91.102.91.158 Notify message 14 (NO-PROPOSAL-CHOSEN)
HDR=(CKY-R=9f7af04bcb0152a9, msgid=44f26f01)

Ending ike-scan 1.9: 256 hosts scanned in 40.465 seconds (6.33 hosts/sec).
0 returned handshake; 6 returned notify
```

Exercise

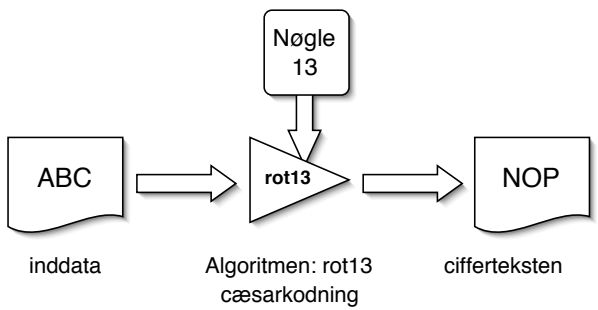


Now lets do the exercise

IPsec negotiation - 30-60 min

which is number **37** in the exercise PDF.

VPN indstillinger



Check hvert år:

- Certifikater/nøgler - ligesom TLS mange bits og skiftes indimellem
- Check algoritmerne, ingen 3DES!
- Check Diffie Helman groups
- Enable Perfect Forward Secrecy
- Check både client VPN og site-2-site

Forward Secrecy

In cryptography, forward secrecy (FS), also known as perfect forward secrecy (PFS), is a feature of specific key agreement protocols that gives assurances that session keys will not be compromised even if the private key of the server is compromised.[1] Forward secrecy protects past sessions against future compromises of secret keys or passwords.[2] By generating a unique session key for every session a user initiates, the compromise of a single session key will not affect any data other than that exchanged in the specific session protected by that particular key.

- `https://en.wikipedia.org/wiki/Forward_secrecy`

Anbefalinger til VPN

Use the following guidelines when configuring Internet Key Exchange (IKE) in VPN technologies:
Avoid IKE Groups 1, 2, and 5.
Use IKE Group 15 or 16 and employ 3072-bit and 4096-bit DH, respectively.
When possible, use IKE Group 19 or 20. They are the 256-bit and
384-bit ECDH groups, respectively.
Use AES for encryption.

Paper: `https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html`

- Certifikater/nøgler - ligesom TLS lange og rulles indimellem
- Algoritmer DES/3DES bye bye, husk både encryption og auth algoritmer
- DH-Group - +15 tak
- Check både client VPN og site-2-site
- Skift til IKEv2
- Selv disse råd er måske ikke tilstrækkelige nu!

OpenVPN / OpenSSL VPN

> OpenVPN is a full-featured SSL VPN solution which can accomodate a wide range of configurations, including remote access, site-to-site VPNs, WiFi security, and enterprise-scale remote access solutions with load balancing, failover, and fine-grained access-controls (articles) (examples) (security overview) (non-english languages).

Et andet populært VPN produkt er OpenVPN

Bemærk dog at hvis der benyttes TCP i TCP risikerer man at støde ind i et problem som kaldes *TCP in TCP meltdown*

Kilde: `http://openvpn.net/`

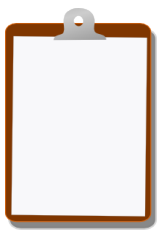
Microsoft DirectAccess and VPN (RAS)

Description from `https://en.wikipedia.org/wiki/DirectAccess`

> DirectAccess, also known as Unified Remote Access, is a VPN-like technology that provides intranet connectivity to client computers when they are connected to the Internet. Unlike many traditional VPN connections, which must be initiated and terminated by explicit user action, DirectAccess connections are designed to connect automatically as soon as the computer connects to the Internet. DirectAccess was introduced in Windows Server 2008 R2, providing this service to Windows 7 and Windows 8 "Enterprise"edition clients.

- DirectAccess establishes **IPsec tunnels** from the client to the DirectAccess server, and uses **IPv6** to reach intranet resources or other DirectAccess clients. This technology **encapsulates the IPv6 traffic over IPv4** to be able to reach the intranet over the Internet, which still (mostly) relies on IPv4 traffic. All traffic to the intranet is encrypted using IPsec and encapsulated in IPv4 packets, which means that in most cases, no configuration of firewalls or proxies should be required.

For Next Time



Think about the subjects from this time, write down questions

Check the plan for chapters to read in the books

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools