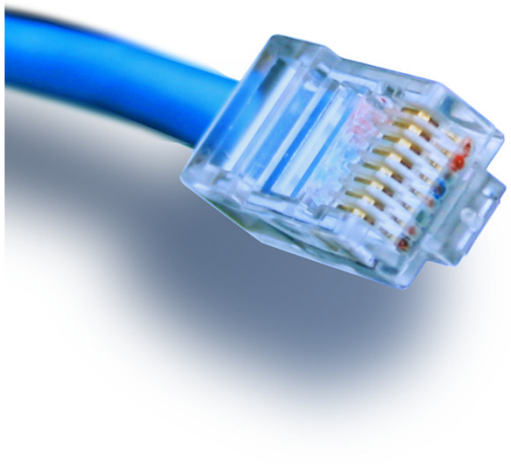
HOUSE OF TECHNOLOGY

– en del af mercantec



Cisco ASA 5505

Vejledning

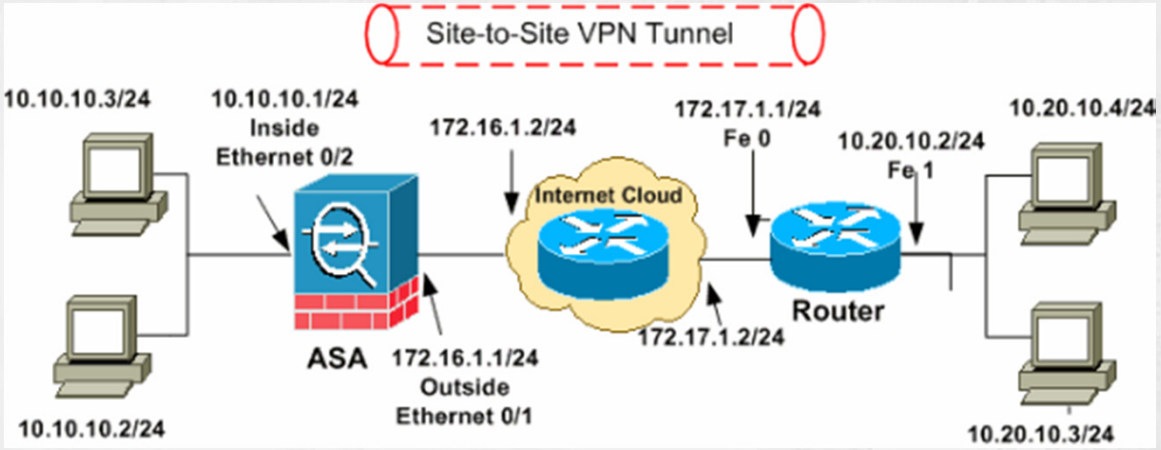
Opsætning af Site-to-Site VPN

Hvad er et Site-to-Site VPN???

HOUSE OF TECHNOLOGY

– en del af mercantec

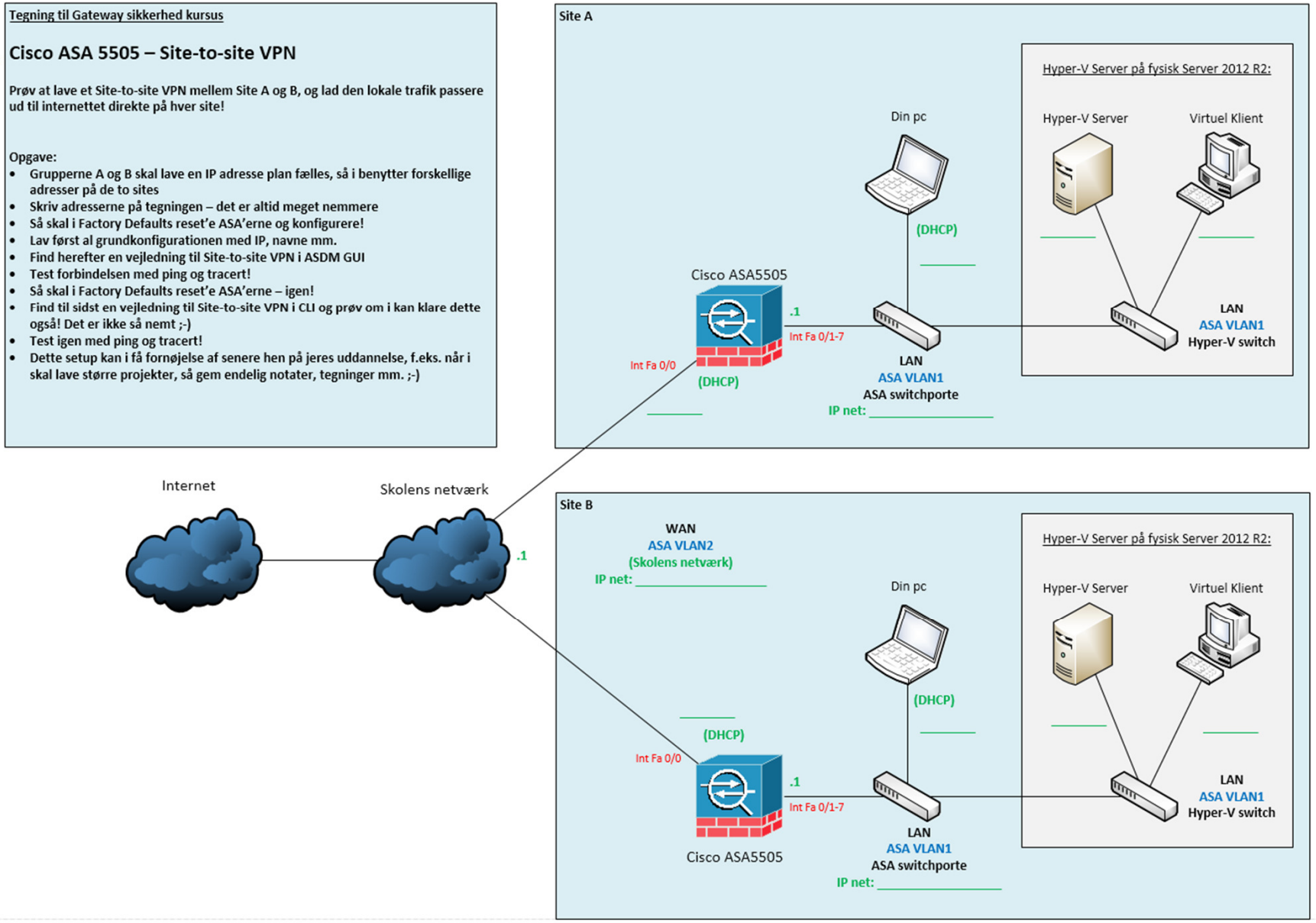
- En sikker, krypteret tunnel til IP pakkerne hen over et usikkert netværk mellem to firma netværk! ☺
- Eksempel fra Cisco:



- http://www.cisco.com/c/en/us/support/docs/cloud-systems-management/configuration-professional/112153-ccp-vpn-asa-router-config-00.html#

Målet for vores ASA netværk:

HOUSE OF TECHNOLOGY



Kapiteloversigt - klik her …

Bemærk!

HOUSE OF TECHNOLOGY

– en del af mercantec

- ASA5505 er ingen almindelig Cisco router!
  - Den kører med sit eget og helt specielle software.
  - Man kan som udgangspunkt IKKE pinge igennem en ASA!
    - Se vejledningen der åbner for ping på de næste sider ☺
  - Det er vigtigt at 'Google' dokumenter til korrekt ASA software version for at finde de rette vejledninger ;-)
  - Udskift IP adresserne i denne vejledning med jeres egne efter behov!
  - Held og lykke ;-)

Lidt om ASA: Factory defaults!

HOUSE OF TECHNOLOGY

– en del af mercantec

- I lab-opsætninger er det altid godt at starte forfra!
- Factory defaults reset procedure:
  - asa>en
  - asa#conf t
  - asa(config)#config factory-default
  - Vent på at konfigurationen er færdig og lav så en reload
    - Svar ja (Yes) til spørgsmålet om at gemme konfigurationen
  - Vent på at ASA'en er klar igen

Grundkonfiguration af en ASA

HOUSE OF TECHNOLOGY

– en del af mercantec

- En grundkonfiguration på en ASA5505 omfatter f.eks.:
  - Setting the Login Password
  - Changing the Enable Password
  - Setting the Hostname
  - Setting the Domain Name
  - Feature History for the Hostname, Domain Name, and Passwords
  - Se vejledning hos Cisco til ASA version 9.x her:
    - http://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/basic_hostname_pw.html#pgfId-1045399

Konfiguration af SSH access

HOUSE OF TECHNOLOGY

– en del af mercantec

- En konfiguration af SSH adgang på en ASA5505:
  - Metode 1 - med lokal brugerdatabase i brug:
    - ASA(config)#username *username* password *password*
    - ASA(config)#aaa authentication ssh console LOCAL
  - Metode 2 - er at bruge default værdierne (ikke optimalt!):
    - ASA(config)#passwd password
      - Brugernavnet er **ASA** og password er **cisco**
  - Fortsættes næste side …

Konfiguration af SSH access

HOUSE OF TECHNOLOGY

– en del af mercantec

- En konfiguration af SSH adgang på en ASA5505 (fortsat):
  - Opret nu RSA kryptonøglene til SSH:
    - ASA(config)#crypto key generate rsa modulus *1024*
  - Justér hvilke IP adresser som må bruge SSH på LAN og WAN:
    - ASA(config)#ssh 192.168.x.x 255.255.255.x inside
    - ASA(config)#ssh *192.168.63.x* 255.255.255.x outside
  - Fortsætte på næste side …

Konfiguration af SSH access

HOUSE OF TECHNOLOGY

– en del af mercantec

- En konfiguration af SSH adgang på en ASA5505 (fortsat):
  - Sæt eventuelt versionsnummer (1 eller 2) og timeout i minutter:
    - ASA(config)# ssh version *version_number*
    - ASA(config)#ssh timeout *minutes*
  - Exit & write mem!
  - Forbind fra en klient via f.eks. PuTTY og SSH. Virker det?
  - Se vejledning hos Cisco til ASA version 9.x her:
    - http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118075-configure-asa-00.html

Tillad ‘ping’ (ICMP) gennem ASA

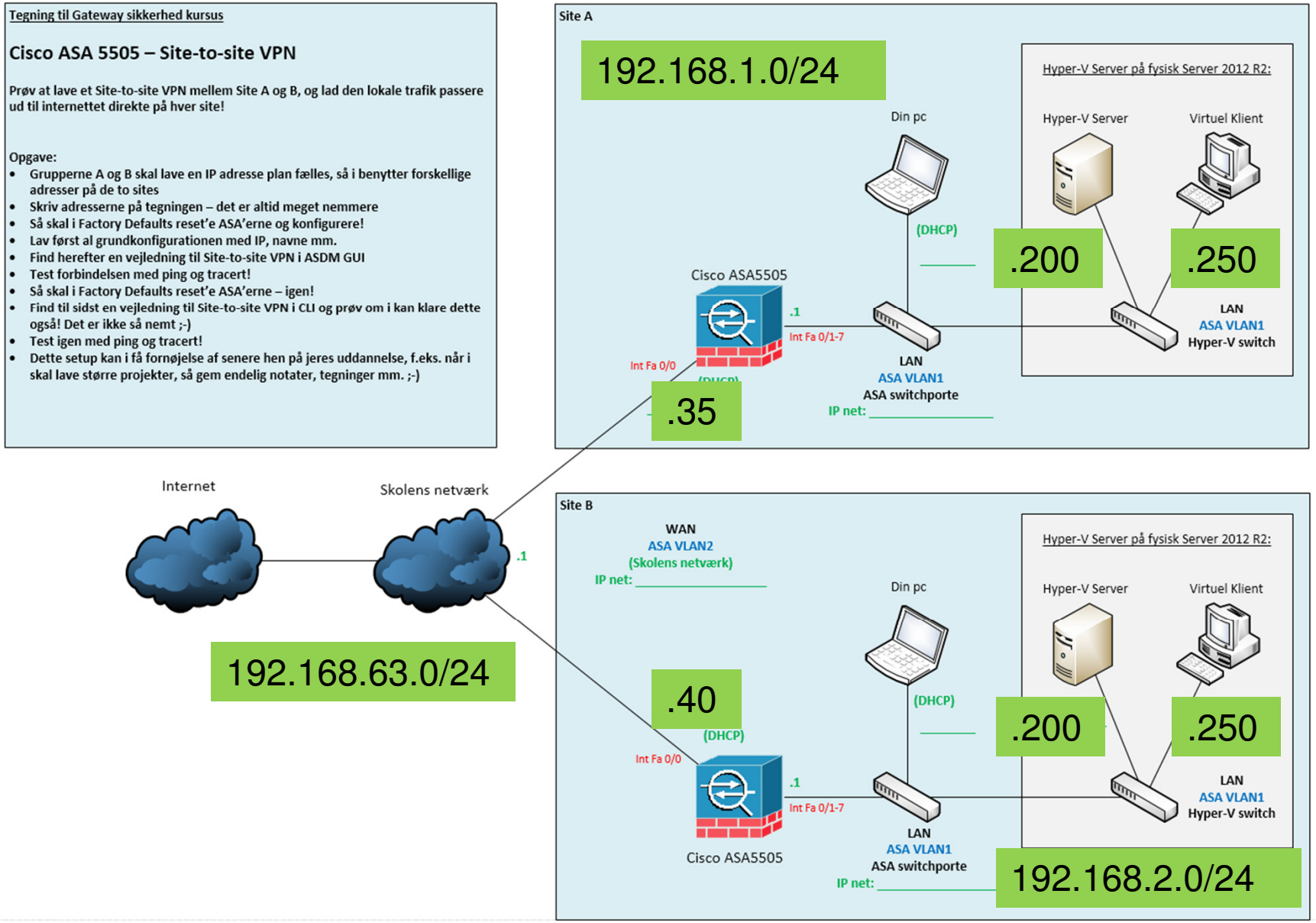
HOUSE OF TECHNOLOGY

– en del af mercantec

- Konfiguration af tillad ‘ping’-policy på ASA5505:
  - ASA(config)# class-map icmp-class
  - ASA(config-cmap)# match default-inspection-traffic
  - ASA(config-cmap)# exit
  - ASA(config)# policy-map icmp_policy
  - ASA(config-pmap)# class icmp-class
  - ASA(config-pmap-c)# inspect icmp
  - ASA(config-pmap-c)# exit
  - ASA(config-pmap)# exit
  - ASA(config)# service-policy icmp_policy interface outside
- Exit & write mem!

Målet for vores ASA netværk:

HOUSE OF TECHNOLOGY



Kapiteloversigt - klik her …

Tilpasning af Inside IP mm.

HOUSE OF TECHNOLOGY

– en del af mercantec

- **Bemærk:** ASA på **Site B** er vist i denne serie!
- Eksempel på ny statisk IP adresse til VLAN1 (Inside):
  - asa(config)#int vlan1
  - asa(config-if)#ip address **192.168.2.1** 255.255.255.0
  - asa(config-if)#exit
- Husk at tilpasse DHCP på Inside samt Inside-Outside Dynamisk NAT – se de næste sider.

Opsætning af DHCP i Inside

HOUSE OF TECHNOLOGY

– en del af mercantec

- Konfiguration af DHCP i Inside-zonen:
  - asa(config)#dhcpd address 192.168.2.100-192.168.2.131 inside
  - asa(config)#dhcpd dns 192.168.63.1 interface inside
  - asa(config)#dhcpd enable inside
- Tips: Husk at gemme running-config indimellem:
  - asa(config)exit
  - asa#write

Opsætning af Dynamisk PAT

HOUSE OF TECHNOLOGY

– en del af mercantec

- Konfiguration af LAN mod Internet Dynamisk PAT:
  - asa(config)#object network inside-subnet
  - asa(config-network-object)#subnet 192.168.2.0 255.255.255.0
  - asa(config-network-object)#nat (inside,outside) dynamic interface

Tilpasning af Outside IP mm.

HOUSE OF TECHNOLOGY

– en del af mercantec

- Eksempel på ny statisk IP adresse til VLAN2 (Outside):
  - asa(config)#int vlan2
  - asa(config-if)#ip address 192.168.63.35 255.255.255.0
  - asa(config-if)#exit
- Eksempel på ny statisk route til gateway of last resort:
  - asa(config)#route outside 0.0.0.0 0.0.0.0 192.168.63.1
- Slet den gamle object network obj_any:
  - asa(config)#no object network obj_any

Lidt om tunneling protokoller

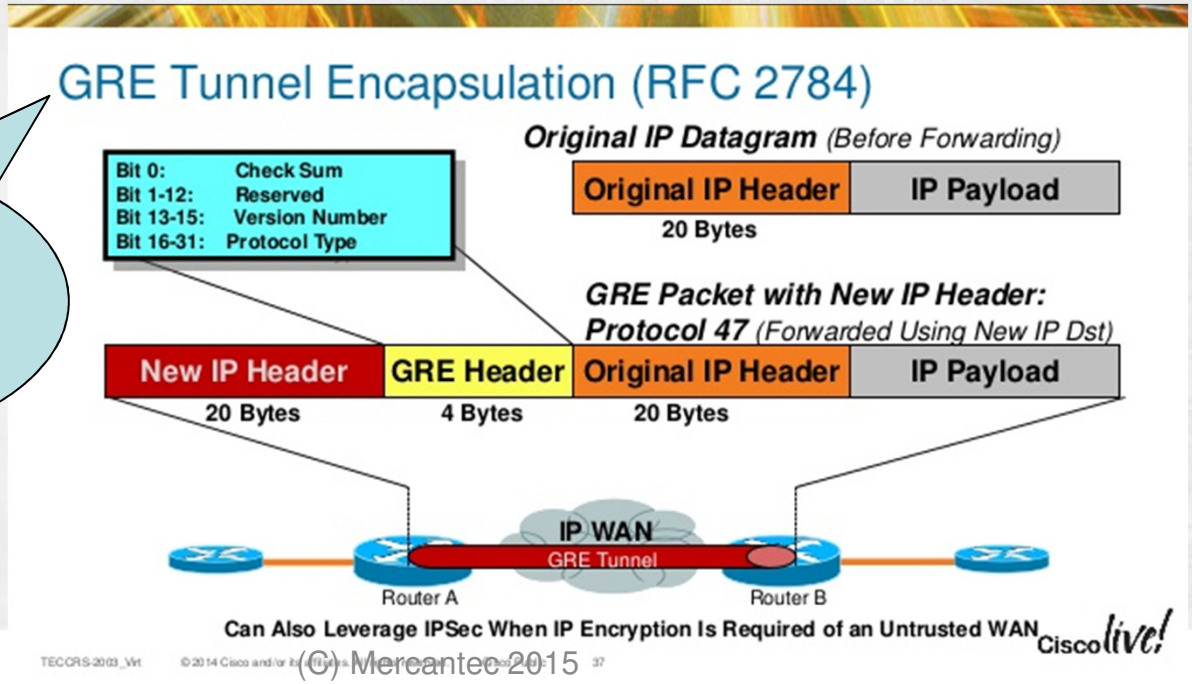
HOUSE OF TECHNOLOGY

– en del af mercantec

- Tunneling (uden kryptering) kræver 3 forskellige protokoller:
  - En passager protokol – dvs. de **originale data** (**IP**, NetBEUI, IPX) som overføres
  - Encapsulation (indpakning) protokol – Protokollen som de originale data er pakket ind i (fx **GRE**, IPSec, L2F, PPTP, L2TP)
  - En bærer protokol (fx. **IP**) som anvendes til at transportere informationen

Cisco ASA bokse understøtter IKKE GRE tunneler ;-)

Brug i stedet IPsec!



Tunneling protokoller

HOUSE OF TECHNOLOGY

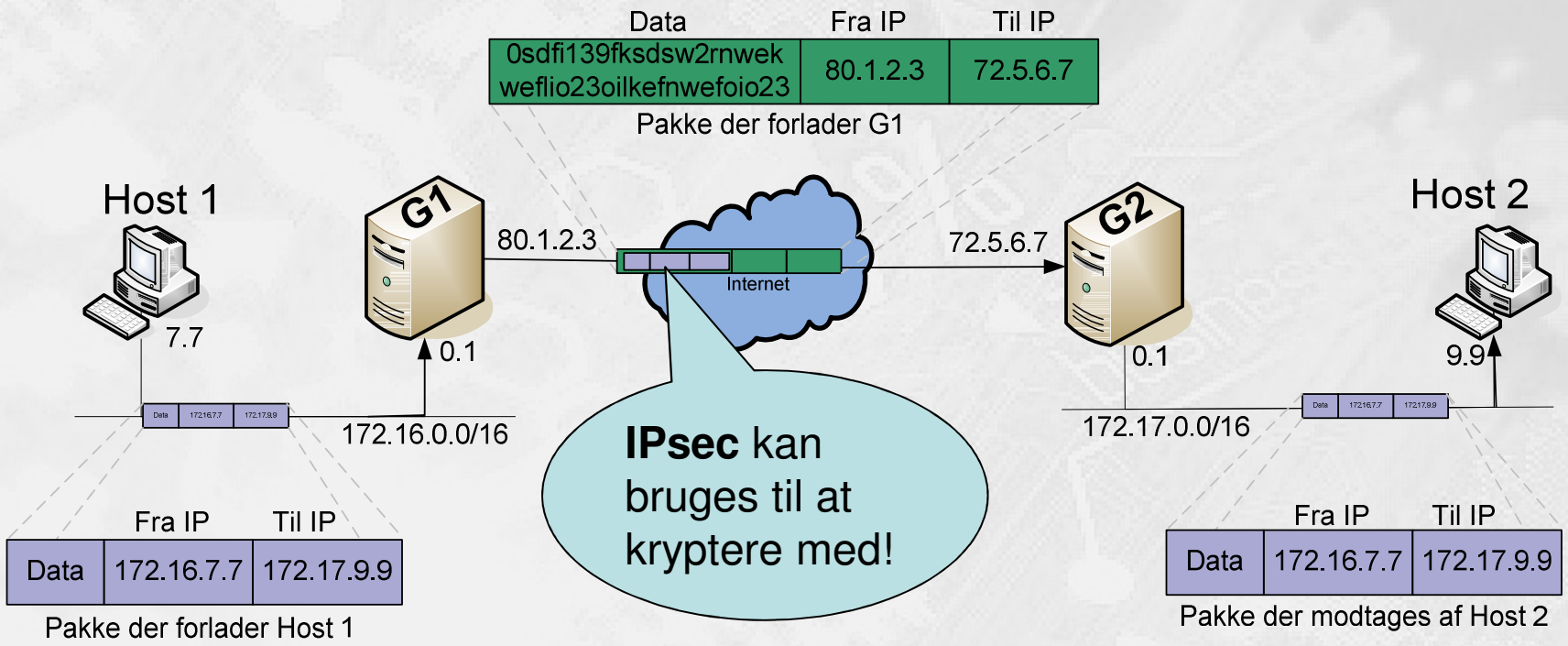
– en del af mercantec

- Et eksempel på en '**netværks lag over netværks lag**' tunnel:
  - **GRE** (generic routing encapsulation)
    - Traditionel tunneling - beskrevet i RFC1701 og 1702.
- Et eksempel på en '**datalink lag over netværk lag**' tunnel:
  - **L2TP** (layer 2 tunneling protocol)
    - Client-Server protokol som kombinerer mange faciliteter fra PPTP og L2F (layer 2 forwarding)
  - **PPTP** (point to point tunneling protocol)
    - Client-Server protokol som er meget benyttet i forbindelse med Microsoft klienter
    - Understøttes af næsten alle Windows operativ- og filsystemer
    - Benytter Microsoft MPPE kryptering
  - **L2F** (Layer 2 Forwarding)
    - Udviklet af Cisco og L2F kan bruge alle type authentication som understøttes i PPP

Kryptering og Tunneling

HOUSE OF TECHNOLOGY

– en del af mercantec



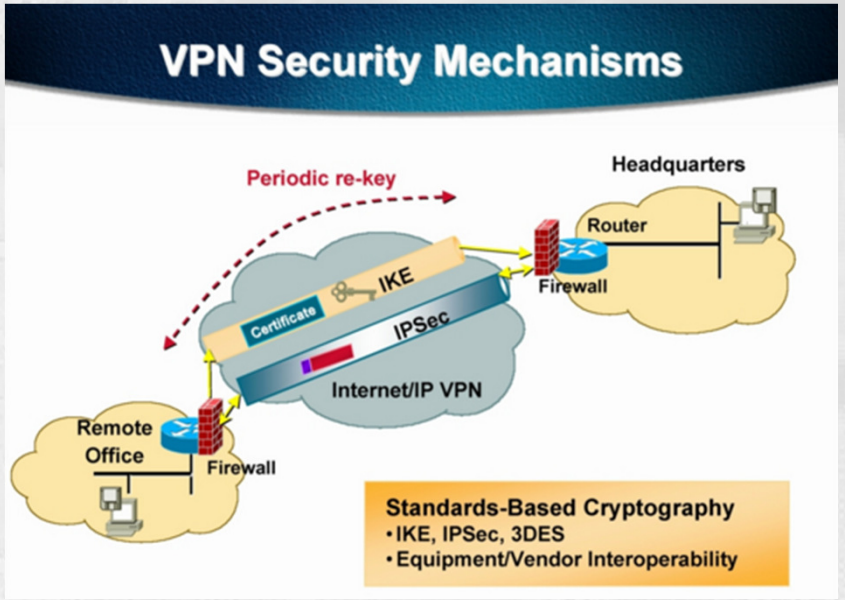
- Kryptering sikrer at uvedkommende ikke tyder data
- Kryptering af hele IP pakken sikrer hemmeligholdelse af identitet på afsender og modtager (Originale IP adresser)

IPsec - Internet Protocol Security

HOUSE OF TECHNOLOGY

– en del af mercantec

- IPsec er:
  - **Ikke** en transportprotokol, men en **sikkerheds protokol suite** …
  - En **tilføjelse til IPv4**
    - **Suiten installeres separat**
  - **Indbygget i IPv6** som standard
- IPsec giver:
  - 'Per IP pakke' beskyttelse
  - **Authentication** og **Encryption** på forbindelserne, dvs. fra:
    - IP host til IP host
    - Netværk til netværk
      - Mellem to **Security gateways**
    - IP host til netværk
      - F.eks. en software-VPN

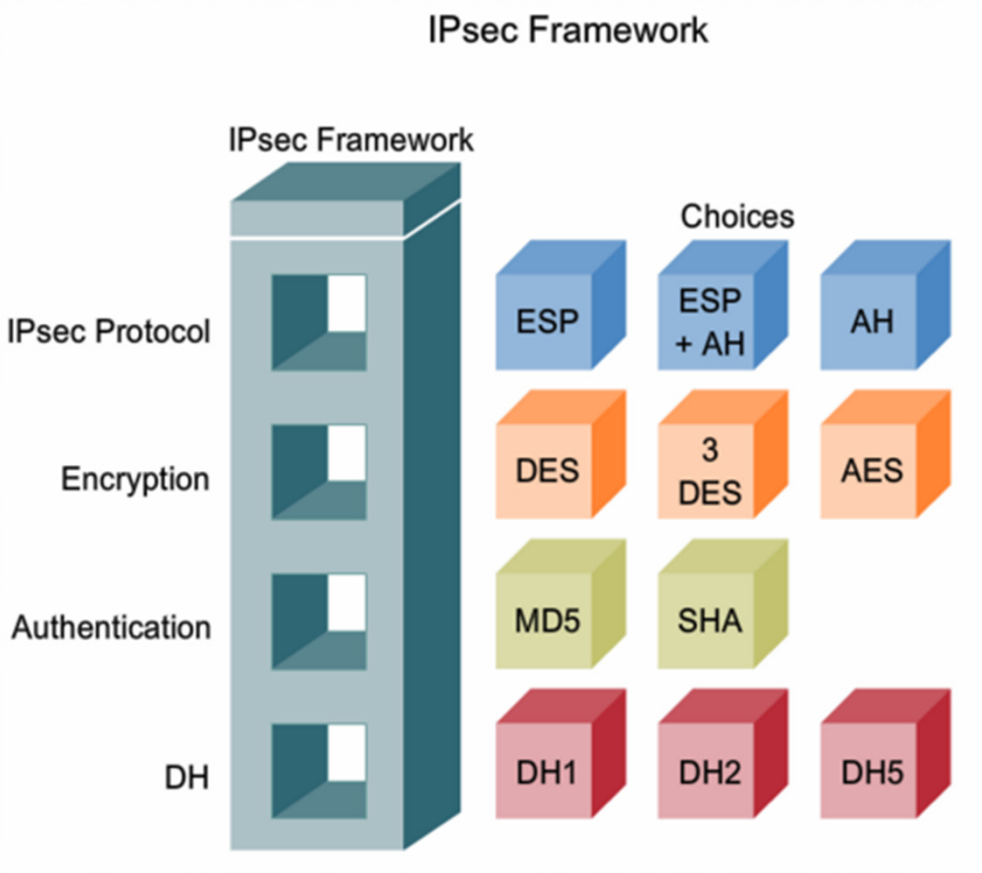


- IPsec **opererer på netværkslaget**, hvilket giver højere sikkerhed end systemer på de højere lag, f.eks. SSH, TLS eller SSL systemerne

IPsec - Internet Protocol Security

HOUSE OF TECHNOLOGY

– en del af mercantec



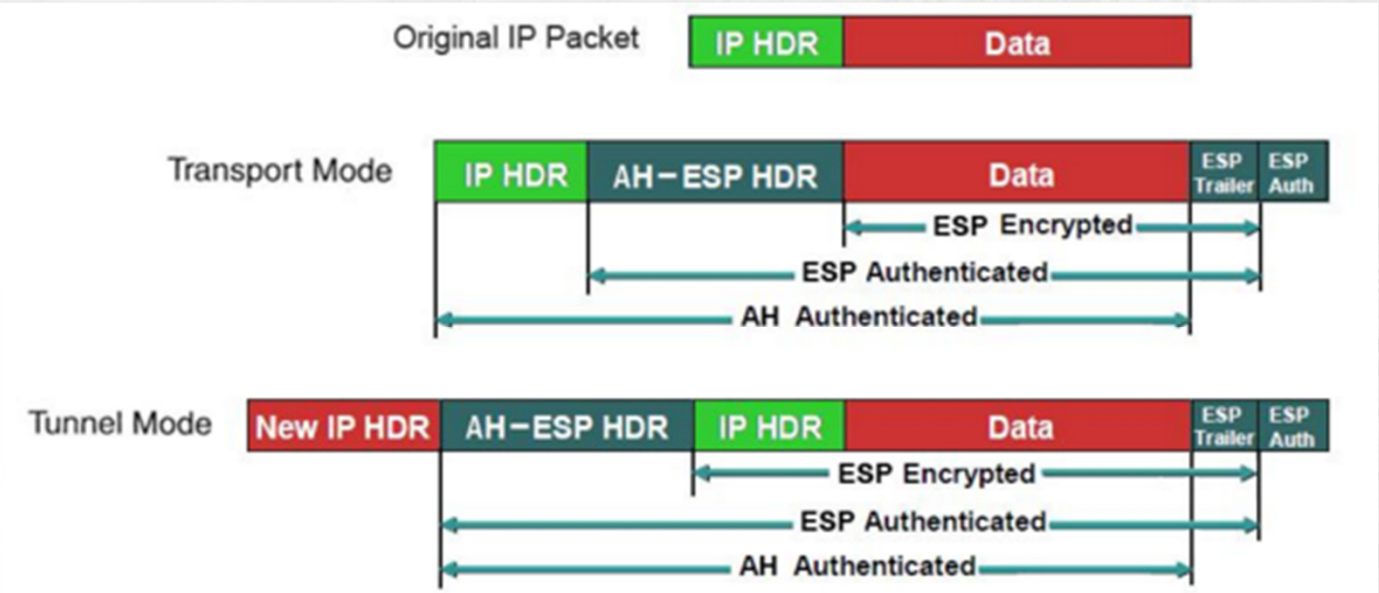
- **IPsec modulerne:**
  - **Protokollerne AH og ESP** giver authentication og integritet
    - AH er ukrypteret
    - ESP benytter kryptering
  - **Krypteringen DES, 3DES og AES** giver confidentiality på dataudvekslingen
  - **Authentication MD5 og SHA** giver via en sikker HASH funktionalitet både integrity protection og authenticity
  - **Diffie-Hellman** giver mulighed for at udveksle kryptonøgler sikkert over et usikkert netværk

IPsec – de to 'modes'

HOUSE OF TECHNOLOGY

– en del af mercantec

- IPsec kan benyttes i to 'modes':
  - **Transport mode –** IPsec headeren lægges ind i den originale pakke
    - Bruges ofte til **Remote access VPN løsninger**
  - **Tunnel mode –** hele pakken krypteres og bliver en del af en ny, større pakke
    - Bruges ofte til **Site-to-site VPN**



IPSec Architecture

Site-to-Site VPN: **ISAKMP**

HOUSE OF TECHNOLOGY

- **ISAKMP** (Internet Security Association and Key Management Protocol) håndterer **sikkerheden på Ipsec tunnelen:**
  - Internet Key Exchange, **IKE**, skal bruges til at **håndtere kryptonøgler** og at **forhandle tunellen på plads**.
  - Brug **IKEv2** – den er bedst
  - Vælg kryptering, hash, authentication, DH, Lifetime og PRF
  - Defaults: 3DES, SHA-1, Preshared keys, Group 2, 86400 sec. og SHA-1

IKE Version	Attribute	Possible Value	Default Value
IKEv1	Encryption	DES 56-bit 3DES 168-bit* AES 128-, 192-, 256-bit*	3DES 168-bit, or DES 56-bit if 3DES feature is not active
	Hashing	MD5 or SHA-1	SHA-1
	Authentication method	Preshared keys RSA signature CRACK**	Preshared keys
	D-H group	Group 1 768-bit field Group 2 1024-bit field Group 5 1536-bit field Group 7 ECC 163-bit field***	Group 2 1024-bit field
	Lifetime	120 to 2,147,483,647 seconds	86,400 seconds
IKEv2	Encryption	DES 56-bit 3DES 168-bit* AES 128, 192, 256-bit* AES-GCM 128-, 192-, 256-bit*	3DES 168-bit, or DES 56-bit if 3DES feature is not active
	Hashing	MD5 SHA-1 SHA-2 256-, 384-, 512-bit	SHA-1
	Authentication method	Preshared keys RSA signature CRACK**	Preshared keys
	D-H group	Group 1 768-bit field Group 2 1024-bit field Group 5 1536-bit field Group 7 ECC 163-bit field*** Group 14 2048-bit field Group 19 ECC 256-bit field Group 20 ECC 384-bit field Group 21 ECC 521-bit field Group 24 2048-bit with 256-bit prime order	Group 2 1024-bit field
	Lifetime	120 to 2,147,483,647 seconds	86,400 seconds
	PRF	MD5 SHA-1 SHA-2 256-, 384-, 512-bit	SHA-1

(Kilde: SafariBooks Online)

Site-to-Site VPN: **Konfiguration**

HOUSE OF TECHNOLOGY

– en del af mercantec

- Her er et eksempel på en konfigurationsplan:
  1. Enable ISAKMP.
  2. Create ISAKMP policy.
  3. Set the tunnel type.
  4. Define the IPsec policy.
  5. Configure the crypto map.
  6. Configure traffic filtering (optional).
  7. Bypass NAT (optional).
  8. Enable Perfect Forward Secrecy (optional).

(Kilde: SafariBooks Online)

Enable ISAKMP & create policy

HOUSE OF TECHNOLOGY

– en del af mercantec

- Gå I ciscoasa(config)# mode og udfør kommandoerne:

  crypto ikev2 enable outside

  crypto ikev2 policy 1

  encryption aes-256

  integrity sha

  group 5

  prf sha

  lifetime seconds 86400

(Kilde: SafariBooks Online)

Set up tunnel groups

HOUSE OF TECHNOLOGY

– en del af mercantec

- Gå I ciscoasa(config)# mode og udfør kommandoerne:

tunnel-group 192.168.63.35 type ipsec-l2l

tunnel-group 192.168.63.35 ipsec-attributes

ikev2 remote-authentication pre-shared-key *Cisco123*

ikev2 local-authentication pre-shared-key *Cisco123*

(Kilde: SafariBooks Online)

Define IPsec policy

HOUSE OF TECHNOLOGY

– en del af mercantec

- Gå I ciscoasa(config)# mode og udfør kommandoerne:

  crypto ipsec ikev2 ipsec-proposal TEST-AES256SHA1

  protocol esp encryption aes-256

  protocol esp integrity sha-1

(Kilde: SafariBooks Online)

Create crypto map

HOUSE OF TECHNOLOGY

– en del af mercantec

- Gå I ciscoasa(config)# mode og udfør kommandoerne:

```
access-list outside_cryptomap line 1 remark ACL to encrypt traffic from Site A to B
access-list outside_cryptomap line 2 extended permit ip 192.168.1.0 255.255.255.0
192.168.2.0 255.255.255.0
crypto map outside_map 1 match address outside_cryptomap
crypto map outside_map 1 set  peer  192.168.63.35
crypto map outside_map 1 set  ikev2 ipsec-proposal  TEST-AES256SHA1
crypto map outside_map interface outside
```

(Kilde: SafariBooks Online)

Traffic Filtering (Optional)

HOUSE OF TECHNOLOGY

– en del af mercantec+

- Et eksempel på at tillade telnet mellem to hosts samt at deaktivere interface accesslists på VPN trafikken:

- Gå I ciscoasa(config)# mode og udfør kommandoerne:

```
access-list outside_acl extended permit tcp host 192.168.2.10 host 192.168.1.10 eq 23
access-group outside_acl in interface outside
no sysopt connection permit-vpn
```

(Kilde: SafariBooks Online)

Bypass NAT (Optional)

HOUSE OF TECHNOLOGY

– en del af mercantec

- Et eksempel på at undlade NAT'ning af VPN trafikken:
- Gå I ciscoasa(config)# mode og udfør kommandoerne:

```
object network 192.168.1-Net
subnet 192.168.1.0 255.255.255.0
object network 192.168.2-Net
subnet 192.168.2.0 255.255.255.0
exit
nat (inside,outside) source static 192.168.2-Net 192.168.2-Net destination static
192.168.1-Net 192.168.1-Net
```

(Kilde: SafariBooks Online)

Perfect Forward Secrecy (Optional)

HOUSE OF TECHNOLOGY

– en del af mercantec

- Et eksempel på at aktivere PFS teknologi, som tvinger ASA'en til at udskifte kryptonøglerne I fase 2:
- Gå I ciscoasa(config)# mode og udfør kommandoerne:

```
crypto map outside_map 10 set pfs group5
```

(Kilde: SafariBooks Online)

Attributes & Features

HOUSE OF TECHNOLOGY

– en del af mercantec

- Eksempler på diverse features der kan fungere hen over en Site-to-Site VPN tunnel:
  - Image OSPF updates over IPsec
  - Image Reverse route injection
  - Image NAT Traversal (NAT-T)
  - Image Tunnel default gateway
  - Image Management access
  - Image Fragmentation policies

(Kilde: SafariBooks Online)

Test med packet-tracer i ASA

HOUSE OF TECHNOLOGY

– en del af mercantec

- Test (simulering) af Internet forbindelse fra LAN på ASA:
  - Cisco ASA IOS indeholder en packet-tracer feature, som kan simulere en pakketransmission gennem maskinen med de nuværende regler.
  - Prøv engang følgende tests fra Site A mod Site B og se om det hele virker:
    - asa# packet-tracer input inside tcp 192.168.1.100 12345 192.168.2.100 80
  - Sæt jeres egne IP adresser på ;-)
  - Husk at ethvert interface involveret I pakketransporten skal være tilsluttet et kabel og være oppe for at det vil virke ;-)