

Forkortelser

ISAKMP(Internet Security Association and Management Protocol)	Framework til udveksling af keys og authentication gennem SA(Security Appliances)
IKE(Internet Key Exchange)	Framework til oprettelse af IPsec gennem SA(Security Appliances)

IKEv1 VS IKEv2 - Forskellen

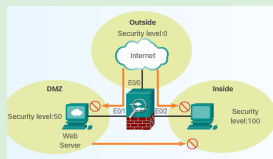
IKEv2 bruger ikke så meget båndbredde som IKEv1.
 IKEv2 supporterer EAP authentication hvor at IKEv1 ikke gør.
 IKEv2 supporterer MOBIKE hvor at IKEv1 ikke gør.
 IKEv2 har indbygget NAT gennemgåelse(traversal?), som IKEv1 ikke har.
 IKEv2 kan opdage når en IPsec tunnel går ned, altså den kan se om den er i live, det kan IKEv1 ikke.

VPN med isakmp og ipsec opsætning

```
Branch# conf t
Branch(config)# crypto isakmp policy 1
Branch(config-isakmp)# encryption aes
Branch(config-isakmp)# authentication pre-share
Branch(config-isakmp)# group 2
Branch(config-isakmp)# exit
Branch(config)# crypto isakmp key cisco123 address 209.165.200.225
Branch(config)# crypto ipsec transform-set HQ-VPN esp-sha-hmac esp-3des
Branch(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 10.10.10.0 0.0.0.255
Branch(config)# crypto map HQ-MAP 10 ipsec-isakmp
! NOTE: This new crypto map will come in disabled until a peer
Branch(config-crypto-map)# set transform-set HQ-VPN
Branch(config-crypto-map)# set peer 209.165.200.226
Branch(config-crypto-map)# match address 110
Branch(config-crypto-map)# exit
Branch(config)# int e0/0/1
Branch(config-if)# crypto map HQ-MAP
Branch(config-if)# *S
Branch#
```

se bilag for kildehenvisning

acl



ACL 2

```
CCNAS-ASA(config)# object-group protocol TCP
CCNAS-ASA(config-protocol)# description 00 Identify TCP as the protocol
CCNAS-ASA(config-protocol)# protocol-object tcp
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group network Internal-Hosts
CCNAS-ASA(config-network)# description 00 matches PCA and PC-B
CCNAS-ASA(config-network)# network-object host 209.145.201.1
CCNAS-ASA(config-network)# network-object host 209.145.201.2
CCNAS-ASA(config-network)# exit
CCNAS-ASA(config)# object-group network Internal-Servers
CCNAS-ASA(config-network)# description 00 matches Web and email servers
CCNAS-ASA(config-network)# network-object host 209.145.202.131
CCNAS-ASA(config-network)# network-object host 209.145.200.130
CCNAS-ASA(config-network)# exit
CCNAS-ASA(config)# object-group service HTTP-HTTPS top
CCNAS-ASA(config-service)# description 00 matches HTTP and HTTPS/HTTPS traffic
```

Opsætning af vlan interfaces

```
CCNAS-ASA(config)# interface vlan 1
CCNAS-ASA(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
CCNAS-ASA(config-if)# security-level 100
CCNAS-ASA(config-if)# ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)# interface e0/1
CCNAS-ASA(config-if)# switchport access vlan 1
CCNAS-ASA(config-if)# no shut
CCNAS-ASA(config-if)# exit
CCNAS-ASA(config)# interface vlan 2
CCNAS-ASA(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
CCNAS-ASA(config-if)# security-level 0
CCNAS-ASA(config-if)# ip address 209.165.200.226 255.255.255.248
CCNAS-ASA(config-if)# interface e0/0
CCNAS-ASA(config-if)# switchport access vlan 2
CCNAS-ASA(config-if)# no shut
CCNAS-ASA(config-if)# exit
CCNAS-ASA(config)#
```

Static default route

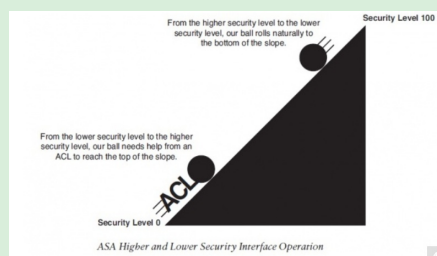
For at vores netværk skal kunne tilgå informationer ude på internettet, skal en default route laves på ASA:

```
CCNAS-ASA(config)# route outside 0.0.0.0 0.0.0.0 209.165.200.225
```

Nyttige commands

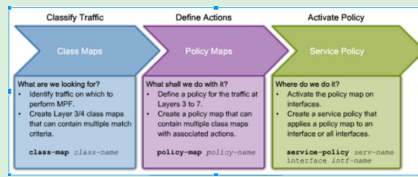
Command	Note
Show running-config crypto	
show crypto isakmp sa	
show crypto ipsec sa	
show crypto key mypubkey rsa	
show running-config object network	
show running-config tunnel	
show acces-list	For at se HIT counter
show run acces-list	Nemmere output af ^
more system:running-config	Viser pre-shared key
show run crypto map	viser maps via vpn
show route	viser ruter
show activation-key	
show password encryption	
show switch vlan	
route outside 0.0.0.0 0.0.0.0 209.165.200.225	

Security-level



Jo højere security-level jo mere sikkert er netværket. Det højeste er inside, det laveste er som real outside. For at komme ind fra outside skal der bruges ACL'er.

Class-, Policy- og Service-map



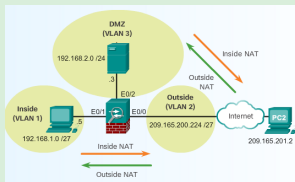
Se bilag for kildehenvisning

Nat in ASA

```

ASA>ASA (config) # object network 192.168.0/24
ASA>ASA (config-network-object) # subnet 192.168.1.0 255.255.255.224
ASA>ASA (config-network-object) # dns (inside,outside) gwipsec Internet
ASA>ASA (config-network-object) # end
ASA>ASA
ASA>ASA show running-config nat
1
nat (inside,outside) gwipsec interface
ASA>ASA
ASA>ASA show running-config object
object network 192.168.0/24
subnet 192.168.1.0 255.255.255.224
ASA>ASA
  
```

Nat in ASA 2



ASDM

```

ASA>ASA (config) # http server enable
ASA>ASA (config) # http 192.168.1.3 255.255.255.255 Inside
ASA>ASA (config) #
  
```