ASA Cheat Sheet

by Unlocked via cheatography.com/25347/cs/6603/

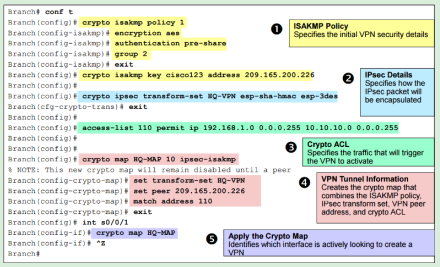
Forkortelser

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

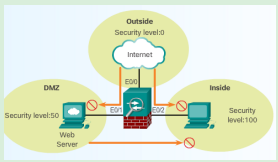
IKEv2 bruger ikke så meget båndbredde som IKEv1.
IKEv2 supportere EAP authentication hvor at IKEv1 ikke gør.
IKEv2 supportere MOBIKE hvor at IKEv1 ikke gør.
IKEv2 har indbygget NAT gennemgåelse(traversal?), som IKEv1 ikke har.
IKEv2 kan opdage når en IPsec tunnel går ned, altså den kan se om den er i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

VPN med isakmp og ipsec opsætning

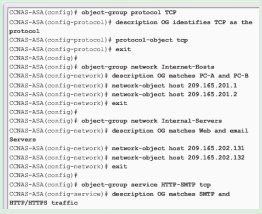


se bilag for kildehenvisning

acl



ACL 2



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

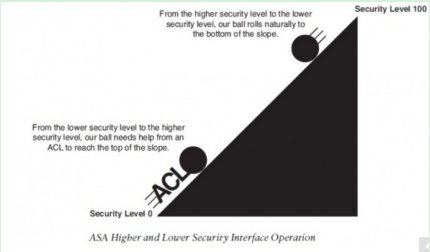
For at vores netværk skal kunne tilgå informationer ude på internettet, skal en default route laves på ASA:

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

Nyttige commands

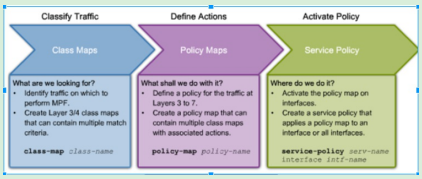
Command	Note
Show running-config crypto	
show crypto isakmp sa	
show crypto ipsec sa	
show crypto key mypubkey rsa	
show running-config object network	
show running-config tunnel	
show acces-list	For at se HIT counter
show run acces-list	Nemmere output af ^
more system:running-config	Viser pre-shared 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



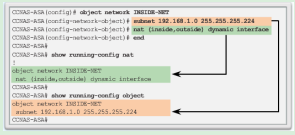
Jo højere security-level jo mere sikkert er netværket. Det højeste er inside, det laveste er som real outside. For at komme ind fra outside skal der bruges ACL'er.

Class-,Policy- og Service-map

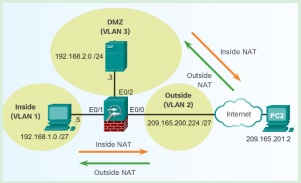


Se bilag for kildehenvisning

Nat in ASA



Nat in ASA 2



ASDM