

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.

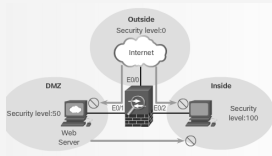
VPN med isakmp og ipsec opsætning

```
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 209.165.200.226
Branch(config)#
Branch(config)# crypto ipsec transform-set HQ-VPN esp-aha-hmac esp-3des
Branch(config-crypto-set)# exit
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)#
Branch(config)# crypto map HQ-VPN 10 ipsec-isakmp
! NOTE: This new crypto map will remain 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)# set 40/1/1
Branch(config-if)# crypto map HQ-VPN
Branch(config-if)# *
Branch#
```

- ISAKMP Policy**
Specifies the initial VPN security details
- IPsec Details**
Specifies how the IPsec packet will be encapsulated
- Crypto ACL**
Specifies the traffic that will trigger the VPN to activate
- VPN Tunnel Information**
Creates the crypto map that combines the ISAKMP policy, IPsec transform set, VPN peer address, and crypto ACL
- Apply the Crypto Map**
Identifies which interface is actively looking to create a VPN

se bilag for kildehenvisning

acl



ACL 2

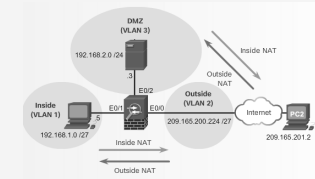
```
CRSAS-ASA(config)# object-group protocol TCP
CRSAS-ASA(config-protocol)# description 0G identifies TCP as the protocol
CRSAS-ASA(config-protocol)# protocol-object top
CRSAS-ASA(config)#
CRSAS-ASA(config)# object-group network Internet-Routers
CRSAS-ASA(config-network)# description 0G matches PC-A and PC-B
CRSAS-ASA(config-network)# network-object host 209.165.201.1
CRSAS-ASA(config-network)# network-object host 209.165.201.2
CRSAS-ASA(config-network)# exit
CRSAS-ASA(config)# object-group network Internal-Servers
CRSAS-ASA(config-network)# description 0G matches Web and email servers
CRSAS-ASA(config-network)# network-object host 209.165.202.131
CRSAS-ASA(config-network)# network-object host 209.165.202.132
CRSAS-ASA(config-network)# exit
CRSAS-ASA(config)#
CRSAS-ASA(config)# object-group service HTTP-HTTPS tcp
CRSAS-ASA(config-service)# description 0G matches SMTP and HTTP/HTTPS traffic
```

Opsætning af vlan interfaces

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 0.0.0.0 209.165.2-00.225	

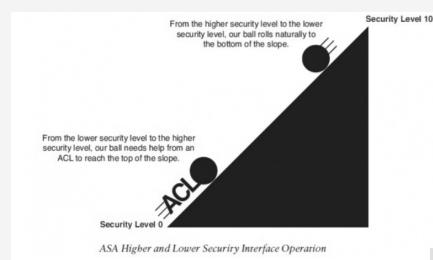
Nat in ASA 2



ASDM

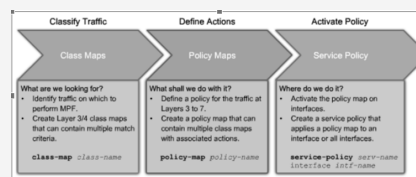
```
CRSAS-ASA(config)# http server enable
CRSAS-ASA(config)# http 192.168.1.1 255.255.255.255 inside
CRSAS-ASA(config)#
```

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

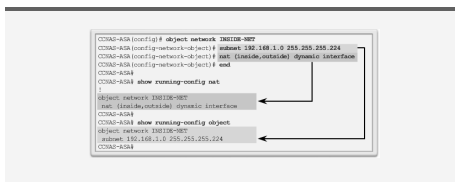
Nat in ASA

```
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
```



By **Unlocked**
cheatography.com/unlocked/

Published 10th January, 2016.

Last updated 13th May, 2016.

Page 1 of 2.

Sponsored by **Readable.com**

Measure your website readability!

<https://readable.com>