

Cheatography

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 bådbredde 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.

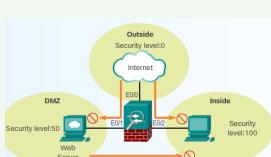
VPN med isakmp og ipsec opsætning

```
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)# crypto ipsec transform-set HQ-VPN esp-sha-hmac esp-3des
Branch(config)# crypto ipsec transform-set HQ-VPN esp-aes esp-sha-hmac
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-MP 10 ipsec-isakmp
NOTE: This new crypto map will remain disabled until a peer configures its own crypto map.
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 s0/0/1
Branch(config-if)# crypto map HQ-MP
Branch(config-if)# ^Z
Branch#
```

① ISAKMP Policy
Specifies the initial VPN security details
② IPsec Details
Specifies how the IPsec packet will be encapsulated
③ Crypto ACL
Specifies the traffic that will trigger the VPN
④ VPN Tunnel Information
Creates the crypto map that combines the ISAKMP policy, IPsec transform set, VPN peer address, and crypto ACL
⑤ Apply the Crypto Map
Specifies which interface is actively looking to create a VPN

se bilag for kildehenvisning

acl



ACL 2

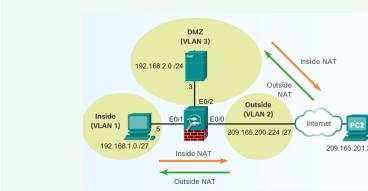
```
ASA# config t
ASA(config)# object-group protocol TCP
ASA(config-object)# description OG identifies TCP as the protocol
ASA(config-object)# exit
ASA(config)# object-group network Internal-Hosts
ASA(config-object)# description OG identifies Internal PC-S
ASA(config-object)# network-object host 209.165.202.1
ASA(config-object)# network-object host 209.165.201.1
ASA(config-object)# network-object host 209.165.201.2
ASA(config-object)# exit
ASA(config)# object-group network Internal-Servers
ASA(config-object)# network-object 0G matches Web and email Servers
ASA(config-object)# exit
ASA(config)# network-object host 209.165.202.131
ASA(config)# network-object host 209.165.202.132
ASA(config)# exit
ASA(config)# exit
ASA(config)# object-group service HTTP-HTTPS http
ASA(config-object)# description OG matches HTTP and HTTPS traffic
```

Opsætning af vlan interfaces

Nytte 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 0.0.0.0 209.165.2-0.0.225 | |

Nat in ASA 2

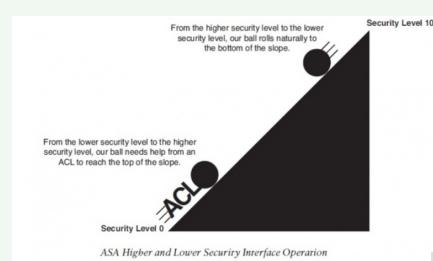


ASDM

```
CCNA-ASA (config)# http server enable
CCNA-ASA (config)# http 192.168.1.3 255.255.255.255 inside
CCNA-ASA (config)#

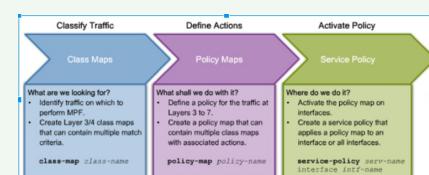
```

Security-level



Jo højere security-level jo mere sikker 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)#
```

```
CCNAS-ASA(config)# object network INSIDE-SW1
CCNAS-ASA(config#) nat (inside,outside) dynamic interface
CCNAS-ASA(config#) exit
CCNAS-ASA(config)# show running-config nat
object network INSIDE-SW1
nat (inside,outside) dynamic interface
CCNAS-ASA(config)# show running-config object
object network INSIDE-SW1
nat (inside,outside) dynamic interface
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>