

FW CNaas IPsec

Description

IPsec is used to open an encrypted tunnel between 2 nodes.
We use it for remote offices access over unsecure networks.

Useful commands

Ike SA

```
#> show security ike security-associations
node0:
```

```
-----
Index State Initiator cookie Responder cookie Mode Remote Address
3844846 UP 8dbd93d0cc99fd49 b100412715f614eb Main 10.20.54.255
```

IPsec

```
#> show security ipsec security-associations
node0:
```

```
-----
Total active tunnels: 1 Total Ipsec sas: 2
ID Algorithm SPI Life:sec/kb Mon lsys Port Gateway
<131073 ESP:aes-cbc-256/sha256 4ec70ecf 3184/ unlim - root 500 10.20.54.255
>131073 ESP:aes-cbc-256/sha256 19cad505 3184/ unlim - root 500 10.20.54.255
<131073 ESP:aes-cbc-256/sha256 663c944f 3192/ unlim - root 500 10.20.54.255
>131073 ESP:aes-cbc-256/sha256 3e638bf3 3192/ unlim - root 500 10.20.54.255
```

```
#> show security ipsec statistics
node0:
```

```
-----
ESP Statistics:
Encrypted bytes: 64366130192
Decrypted bytes: 22801202965
Encrypted packets: 114170364
Decrypted packets: 54108301
AH Statistics:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0
Errors:
AH authentication failures: 0, Replay errors: 0
ESP authentication failures: 0, ESP decryption failures: 0
Bad headers: 0, Bad trailers: 0
```

```
node1:
```

```
-----
ESP Statistics:
Encrypted bytes: 502632
Decrypted bytes: 221067
Encrypted packets: 1770
Decrypted packets: 779
AH Statistics:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0
Errors:
AH authentication failures: 0, Replay errors: 0
ESP authentication failures: 0, ESP decryption failures: 0
Bad headers: 0, Bad trailers: 0
```