

Table of Contents

- IPSec Firewall AIX** 3
- Filter only one IP and one port 3
- References 4

IPSec Firewall AIX

Chek if it's installed:

```
lsllpp -l | grep ipsec
```

Start:

```
smit ipsec4
Start/Stop IP Security
Start IP Security
Start IP Security [Now and After Reboot]
```

Filter only one IP and one port

Specific network interface:

```
genfilt -v4 -a D -s 10.149.128.122 -m 255.255.255.0 -d 10.149.128.123 -M
255.255.255.0 -g N -c tcp -o eq -p 80 -r L -w I -l N -f Y -i en0
```

All interfaces:

```
genfilt -v4 -a D -s 10.149.128.122 -m 255.255.255.0 -d 10.149.128.123 -M
255.255.255.0 -g N -c tcp -o eq -p 80 -r L -w I -l N -f Y -i all
```

The same but locally:

```
genfilt -v4 -a D -s 10.149.128.122 -m 255.255.255.0 -d 10.149.128.123 -M
255.255.255.0 -g N -c tcp -O eq -P 80 -r L -w 0 -l N -f Y -i en0
```

The same but locally with all interfaces:

```
genfilt -v4 -a D -s 10.149.128.122 -m 255.255.255.0 -d 10.149.128.123 -M
255.255.255.0 -g N -c tcp -O eq -P 80 -r L -w 0 -l N -f Y -i all
```

¿What meaning the above?

- -v4: use IPv4 rules
- -a D: action Deny
- -s 10.149.128.122: source address
- -m 255.255.255.0: source subnet mask
- -d 10.149.128.123: destination address
- -M 255.255.255.0: destination subnet mask
- -g N: use source routing No
- -c tcp: apply to tcp protocol
- -O eq: destination port condition (lt, le, gt, ge, eq, neq, and any)
- -P: destination port
- -r L: apply the rule for destined and local packets

- -w O: apply the rule for outbound packets
- -l N: no log
- -f Y: Control all packets fragmented or no
- -i all: all interfaces

Apply changes:

```
mkfilt -g start  
mkfilt -u
```

List rules:

```
lsfilt -a -v4
```

Restart IPsec:

```
smit ipsec4
```

Remove rules

Remove all rules:

```
rmfilt -v4 -n all  
mkfilt -g start  
mkfilt -u
```

References

- https://www.ibm.com/support/knowledgecenter/en/ssw_aix_71/com.ibm.aix.cmds2/genfilt.htm

From:
<https://www.estebanmonge.site/> - **Esteban Monge**

Permanent link:
https://www.estebanmonge.site/doku.php?id=ipsec_aix

Last update: **2019/07/08 16:04**

