

IPsec

Instalacja oprogramowania

Zainstalować ipsec-tools oraz strongswan

Polecenia do instalacji ipsec:

```
wget http://launchpadlibrarian.net/234435245/ipsec-  
tools_0.8.2+20140711-5_amd64.deb  
sudo apt install ./ipsec-tools_0.8.2+20140711-5_amd64.deb
```

Polecenie do instalacji strongswan:

```
sudo apt install strongswan
```

Konfiguracja IPSec za pomocą setkey

Modyfikacja plików konfiguracyjnych

[setkey.conf_a_](#)

```
#!/usr/sbin/setkey -f  
  
## konfiguracja dla maszyny A  
  
## flush SAD and SPD  
flush;  
spdflush;  
  
## add SAs in SAD  
add 172.20.253.237 172.20.252.198 esp 0x1000 -E aes-cbc  
0xaa223344556677889900aabbccddeeff;  
add 172.20.252.198 172.20.253.237 esp 0x2000 -E aes-cbc  
0xbb223344556677889900aabbccddeeff;  
  
## add SPs in SPD  
spdadd 172.20.253.237 172.20.252.198 any -P out ipsec  
esp/transport//require;  
spdadd 172.20.252.198 172.20.253.237 any -P in ipsec  
esp/transport//require;
```

[setkey.conf_b_](#)

```
#!/usr/sbin/setkey -f

## konfiguracja dla maszyny B

## flush SAD i SPD
flush;
spdflush;

## add SAs in SAD
add 172.20.253.237 172.20.252.198 esp 0x1000 -E aes-cbc
0xaa223344556677889900aabbccddeeff;
add 172.20.252.198 172.20.253.237 esp 0x2000 -E aes-cbc
0xbb223344556677889900aabbccddeeff;

## add SPs in SPD
spdadd 172.20.253.237 172.20.252.198 any -P in ipsec
esp/transport//require;
spdadd 172.20.252.198 172.20.253.237 any -P out ipsec
esp/transport//require;
```

Załadowanie konfiguracji

Na maszynie a:

```
administrator@ipsec-A:~$ sudo setkey -f setkey.conf_a_
administrator@ipsec-A:~$ sudo setkey -D
172.20.252.198 172.20.253.237
    esp mode=transport spi=8192(0x00002000) reqid=0(0x00000000)
    E: aes-cbc bb223344 55667788 9900aabb ccddeeff
    seq=0x00000000 replay=0 flags=0x00000000 state=mature
    created: Jun 14 19:29:57 2025    current: Jun 14 19:30:01 2025
    diff: 4(s)    hard: 0(s)    soft: 0(s)
    last:
    current: 0(bytes)    hard: 0(bytes)    soft: 0(bytes)
    allocated: 0    hard: 0 soft: 0
    sadb_seq=1 pid=13464 refcnt=0
172.20.253.237 172.20.252.198
    esp mode=transport spi=4096(0x00001000) reqid=0(0x00000000)
    E: aes-cbc aa223344 55667788 9900aabb ccddeeff
    seq=0x00000000 replay=0 flags=0x00000000 state=mature
    created: Jun 14 19:29:57 2025    current: Jun 14 19:30:01 2025
    diff: 4(s)    hard: 0(s)    soft: 0(s)
    last:
    current: 0(bytes)    hard: 0(bytes)    soft: 0(bytes)
    allocated: 0    hard: 0 soft: 0
    sadb_seq=0 pid=13464 refcnt=0
administrator@ipsec-A:~$ sudo setkey -DP
172.20.252.198[any] 172.20.253.237[any] 255
```

```
fwd prio def ipsec
esp/transport//require
created: Jun 14 19:29:57 2025  lastused:
lifetime: 0(s) validtime: 0(s)
spid=82 seq=1 pid=13511
refcnt=1
172.20.252.198[any] 172.20.253.237[any] 255
in prio def ipsec
esp/transport//require
created: Jun 14 19:29:57 2025  lastused:
lifetime: 0(s) validtime: 0(s)
spid=72 seq=2 pid=13511
refcnt=1
172.20.253.237[any] 172.20.252.198[any] 255
out prio def ipsec
esp/transport//require
created: Jun 14 19:29:57 2025  lastused:
lifetime: 0(s) validtime: 0(s)
spid=65 seq=3 pid=13511
refcnt=1
(per-socket policy)
in(socket) none
created: Jun 14 19:18:30 2025  lastused:
lifetime: 0(s) validtime: 0(s)
spid=59 seq=4 pid=13511
refcnt=1
(per-socket policy)
out(socket) none
created: Jun 14 19:18:30 2025  lastused:
lifetime: 0(s) validtime: 0(s)
spid=52 seq=5 pid=13511
refcnt=1
(per-socket policy)
in(socket) none
created: Jun 14 19:18:30 2025  lastused:
lifetime: 0(s) validtime: 0(s)
spid=43 seq=6 pid=13511
refcnt=1
(per-socket policy)
out(socket) none
created: Jun 14 19:18:30 2025  lastused:
lifetime: 0(s) validtime: 0(s)
spid=36 seq=7 pid=13511
refcnt=1
(per-socket policy)
in(socket) none
created: Jun 14 19:18:30 2025  lastused:
lifetime: 0(s) validtime: 0(s)
spid=27 seq=8 pid=13511
refcnt=1
(per-socket policy)
```

```

    out(socket) none
    created: Jun 14 19:18:30 2025  lastused:
    lifetime: 0(s) validtime: 0(s)
    spid=20 seq=9 pid=13511
    refcnt=1
(per-socket policy)
    in(socket) none
    created: Jun 14 19:18:30 2025  lastused:
    lifetime: 0(s) validtime: 0(s)
    spid=11 seq=10 pid=13511
    refcnt=1
(per-socket policy)
    out(socket) none
    created: Jun 14 19:18:30 2025  lastused:
    lifetime: 0(s) validtime: 0(s)
    spid=4 seq=0 pid=13511
    refcnt=1
administrator@ipsec-A:~$

```

Na maszynie b:

```

administrator@ipsec-B:~$ sudo setkey -f setkey.conf_b_
administrator@ipsec-B:~$ sudo setkey -D
172.20.252.198 172.20.253.237
    esp mode=transport spi=8192(0x00002000) reqid=0(0x00000000)
    E: aes-cbc bb223344 55667788 9900aabb ccddeeff
    seq=0x00000000 replay=0 flags=0x00000000 state=mature
    created: Jun 14 19:31:00 2025  current: Jun 14 19:31:15 2025
    diff: 15(s)  hard: 0(s)  soft: 0(s)
    last:
    current: 0(bytes)  hard: 0(bytes)  soft: 0(bytes)
    allocated: 0  hard: 0  soft: 0
    sadb_seq=1 pid=32009 refcnt=0
172.20.253.237 172.20.252.198
    esp mode=transport spi=4096(0x00001000) reqid=0(0x00000000)
    E: aes-cbc aa223344 55667788 9900aabb ccddeeff
    seq=0x00000000 replay=0 flags=0x00000000 state=mature
    created: Jun 14 19:31:00 2025  current: Jun 14 19:31:15 2025
    diff: 15(s)  hard: 0(s)  soft: 0(s)
    last:
    current: 0(bytes)  hard: 0(bytes)  soft: 0(bytes)
    allocated: 0  hard: 0  soft: 0
    sadb_seq=0 pid=32009 refcnt=0
administrator@ipsec-B:~$ sudo setkey -DP
172.20.252.198[any] 172.20.253.237[any] 255
    out prio def ipsec
    esp/transport//require
    created: Jun 14 19:31:00 2025  lastused:
    lifetime: 0(s) validtime: 0(s)
    spid=17 seq=1 pid=32078
    refcnt=1

```

```

172.20.253.237[any] 172.20.252.198[any] 255
  fwd prio def ipsec
  esp/transport//require
  created: Jun 14 19:31:00 2025  lastused:
  lifetime: 0(s) validtime: 0(s)
  spid=10 seq=2 pid=32078
  refcnt=1
172.20.253.237[any] 172.20.252.198[any] 255
  in prio def ipsec
  esp/transport//require
  created: Jun 14 19:31:00 2025  lastused:
  lifetime: 0(s) validtime: 0(s)
  spid=8 seq=0 pid=32078
  refcnt=1
administrator@ipsec-B:~$

```

Test Działania tunelu

Wykonanie ping z maszyny A do B i obserwacja nagłówka ESP

Wireshark capture on interface eth0. The packet list shows several SSH and TCP packets, followed by two ESP packets (SPI=0x00001000 and SPI=0x00002000). The packet details for the first ESP packet show it's an Encapsulating Security Payload with SPI 0x00001000 and sequence 45. The packet bytes show the raw data of the ESP packet.

No.	Time	Source	Destination	Protocol	Length	Info
242	16.080055036	172.20.240.1	172.20.253.237	SSH	150	Client: Encrypted packet (len=96)
243	16.080125936	172.20.253.237	172.20.240.1	SSH	102	Server: Encrypted packet (len=48)
244	16.080407953	172.20.253.237	172.20.240.1	SSH	118	Server: Encrypted packet (len=64)
245	16.080497397	172.20.253.237	172.20.240.1	SSH	102	Server: Encrypted packet (len=48)
246	16.080497475	172.20.240.1	172.20.253.237	TCP	54	58100 → 22 [ACK] Seq=385 Ack=8897 Win=251 Len=
247	16.080919364	172.20.253.237	172.20.240.1	SSH	102	Server: Encrypted packet (len=48)
248	16.081001536	172.20.240.1	172.20.253.237	TCP	54	58100 → 22 [ACK] Seq=385 Ack=8993 Win=250 Len=
249	16.081047702	172.20.253.237	172.20.240.1	SSH	102	Server: Encrypted packet (len=48)
250	16.123220824	172.20.240.1	172.20.253.237	TCP	54	58100 → 22 [ACK] Seq=385 Ack=9041 Win=250 Len=
251	16.414761906	172.20.253.237	172.20.252.198	ESP	138	ESP (SPI=0x00001000)
252	16.415066422	172.20.252.198	172.20.253.237	ESP	138	ESP (SPI=0x00002000)

Frame 251: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface eth0, id 0
 Ethernet II, Src: Microsof_38:01:3f (00:15:5d:38:01:3f), Dst: Microsof_38:01:40 (00:15:5d:38:01:40)
 Internet Protocol Version 4, Src: 172.20.253.237, Dst: 172.20.252.198
 Encapsulating Security Payload
 ESP SPI: 0x00001000 (4096)
 ESP Sequence: 45

0000 00 15 5d 38 01 40 00 15 5d 38 01 3f 08 00 45 00 ..8.0...]8.?..E.
 0010 00 7c f1 b3 40 00 40 32 f5 be ac 14 fd ed ac 14 |..0.02
 0020 fc c6 00 00 10 00 00 00 00 2d 03 de 3b 39 e5 a69..
 0030 2d cf 07 8d 7a f5 8b e8 77 fc f4 e6 7b 22 52 7az...w...{"Rz
 0040 87 32 3b 89 b6 6e 47 e0 d6 02 8a 62 5a 24 e3 63 ..2;..nG...bZ\$.c
 0050 ad ff 34 18 85 89 17 20 d6 d9 b6 3d e5 0a ba 9e ..4.....=.....
 0060 82 f2 78 14 70 f2 58 43 bd 0b 45 0e 04 08 f9 9c ..x.p.XC..E.....
 0070 9b 2f 14 49 49 71 dc 13 c7 89 65 ef 4e ed 0b 25 ../.IIq...e.N...%
 0080 8c 12 1c 37 c0 29 43 f6 ba 077.)C... ..

Pytania

Jaki ruch zabezpieczony jest tunelem IPsec?

Ruch IP pomiędzy maszynami A (172.20.253.237) i B (172.20.252.198) – każdy protokół (any) zdefiniowany w SPD.

Jaki protokół IPsec jest używany? Jakie algorytmy?

- Protokół: ESP
- Algorytm szyfrowania: AES-CBC
- Usługi: Szyfrowanie (brak autentykacji w tym przykładzie)

Rola SAD i SPD:

- SAD: Przechowuje parametry SA (klucze, algorytmy, SPI)
- SPD: Przechowuje polityki bezpieczeństwa (który ruch ma być zabezpieczony i jak)

Które komendy są przetwarzane dla ruchu wychodzącego/ przychodzącego?

- Dla pakietów wychodzących – `spdadd ... -P out`
- Dla pakietów przychodzących – `spdadd ... -P in`

Dlaczego potrzebne są dwie SA?

SA są jednokierunkowe – jedna dla $A \rightarrow B$, druga dla $B \rightarrow A$, aby zabezpieczyć dwukierunkowy kanał.

Znaczenie komend "setkey -D" i "setkey -DP"

- -D – pokazuje aktywne asocjacje bezpieczeństwa (SA)
- -DP – pokazuje aktywne polityki bezpieczeństwa (SPD)

Jakie jest przeznaczenie pola SPI w nagłówku IPsec?

SPI (Security Parameter Index) to unikalny identyfikator asocjacji bezpieczeństwa (SA), który pozwala odbiorcy zidentyfikować, jakich parametrów użyć do odszyfrowania i uwierzytelnienia pakietu.

Jakie jest przeznaczenie pola Sequence Number w nagłówku IPsec?

Sequence Number służy do zapobiegania atakom typu replay. Numer rośnie monotonicznie dla każdego pakietu, co pozwala sprawdzić, czy pakiety nie zostały powtórzone.

Modyfikacja polityk IPsec i SA

ESP z AES-CBC + HMAC-SHA1

[setkey.conf_a_](#)

```
#!/usr/sbin/setkey -f

## konfiguracja dla maszyny A

## flush SAD and SPD
flush;
spdflush;

## add SAs in SAD
add 172.20.253.237 172.20.252.198 esp 0x1000 -E aes-cbc
0xaa223344556677889900aabbccddeeff -A hmac-sha1
0xaa223344556677889900aabbccddeeff;
add 172.20.252.198 172.20.253.237 esp 0x2000 -E aes-cbc
0xbb223344556677889900aabbccddeeff -A hmac-sha1
0xbb223344556677889900aabbccddeeff;

## add SPs in SPD
spdadd 172.20.253.237 172.20.252.198 any -P out ipsec
esp/transport//require;
spdadd 172.20.252.198 172.20.253.237 any -P in ipsec
esp/transport//require;
```

[setkey.conf_b_](#)

```
#!/usr/sbin/setkey -f

## konfiguracja dla maszyny B

## flush SAD i SPD
flush;
spdflush;

## add SAs in SAD
add 172.20.253.237 172.20.252.198 esp 0x1000 -E aes-cbc
0xaa223344556677889900aabbccddeeff -A hmac-sha1
0xaa223344556677889900aabbccddeeff;
add 172.20.252.198 172.20.253.237 esp 0x2000 -E aes-cbc
0xbb223344556677889900aabbccddeeff -A hmac-sha1
0xbb223344556677889900aabbccddeeff;

## add SPs in SPD
spdadd 172.20.253.237 172.20.252.198 any -P in ipsec
```

```
esp/transport//require;  
spdadd 172.20.252.198 172.20.253.237 any -P out ipsec  
esp/transport//require;
```

AH z HMAC-SHA1

[setkey.conf_a_](#)

```
#!/usr/sbin/setkey -f  
  
## konfiguracja dla maszyny A  
  
## flush SAD and SPD  
flush;  
spdflush;  
  
## add SAs in SAD  
add 172.20.253.237 172.20.252.198 ah 0x1000 -E hmac-sha1  
0xaa223344556677889900aabbccddeeff;  
add 172.20.252.198 172.20.253.237 ah 0x2000 -E hmac-sha1  
0xbb223344556677889900aabbccddeeff;  
  
## add SPs in SPD  
spdadd 172.20.253.237 172.20.252.198 any -P out ipsec  
esp/transport//require;  
spdadd 172.20.252.198 172.20.253.237 any -P in ipsec  
esp/transport//require;
```

[setkey.conf_b_](#)

```
#!/usr/sbin/setkey -f  
  
## konfiguracja dla maszyny B  
  
## flush SAD i SPD  
flush;  
spdflush;  
  
## add SAs in SAD  
add 172.20.253.237 172.20.252.198 ah 0x1000 -E hmac-sha1  
0xaa223344556677889900aabbccddeeff;  
add 172.20.252.198 172.20.253.237 ah 0x2000 -E hmac-sha1  
0xbb223344556677889900aabbccddeeff;  
  
## add SPs in SPD  
spdadd 172.20.253.237 172.20.252.198 any -P in ipsec  
esp/transport//require;
```



```
spdadd 172.20.252.198 172.20.253.237 any -P out ipsec  
esp/transport//require;
```

ESP (AES-CBC) + AH (HMAC-SHA1)

[setkey.conf_a_](#)

```
#!/usr/sbin/setkey -f  
  
## konfiguracja dla maszyny A  
  
## flush SAD and SPD  
flush;  
spdflush;  
  
## add SAs in SAD  
add 172.20.253.237 172.20.252.198 esp 0x1000 -E aes-cbc  
0xaa223344556677889900aabbccddeeff;  
add 172.20.252.198 172.20.253.237 esp 0x2000 -E aes-cbc  
0xbb223344556677889900aabbccddeeff;  
  
## add SAs in SAD  
add 172.20.253.237 172.20.252.198 ah 0x1001 -E hmac-sha1  
0xaa223344556677889900aabbccddeeff;  
add 172.20.252.198 172.20.253.237 ah 0x2001 -E hmac-sha1  
0xbb223344556677889900aabbccddeeff;  
  
## add SPs in SPD  
spdadd 172.20.253.237 172.20.252.198 any -P out ipsec  
esp/transport//require;  
spdadd 172.20.252.198 172.20.253.237 any -P in ipsec  
esp/transport//require;
```

[setkey.conf_b_](#)

```
#!/usr/sbin/setkey -f  
  
## konfiguracja dla maszyny B  
  
## flush SAD i SPD  
flush;  
spdflush;  
  
## add SAs in SAD  
add 172.20.253.237 172.20.252.198 ah 0x1000 -E hmac-sha1  
0xaa223344556677889900aabbccddeeff;  
add 172.20.252.198 172.20.253.237 ah 0x2000 -E hmac-sha1
```

```
0xbb223344556677889900aabbccddeeff;
```

```
## add SPs in SPD
```

```
spdadd 172.20.253.237 172.20.252.198 any -P in ipsec  
esp/transport//require;
```

```
spdadd 172.20.252.198 172.20.253.237 any -P out ipsec  
esp/transport//require;
```

Nagłówek