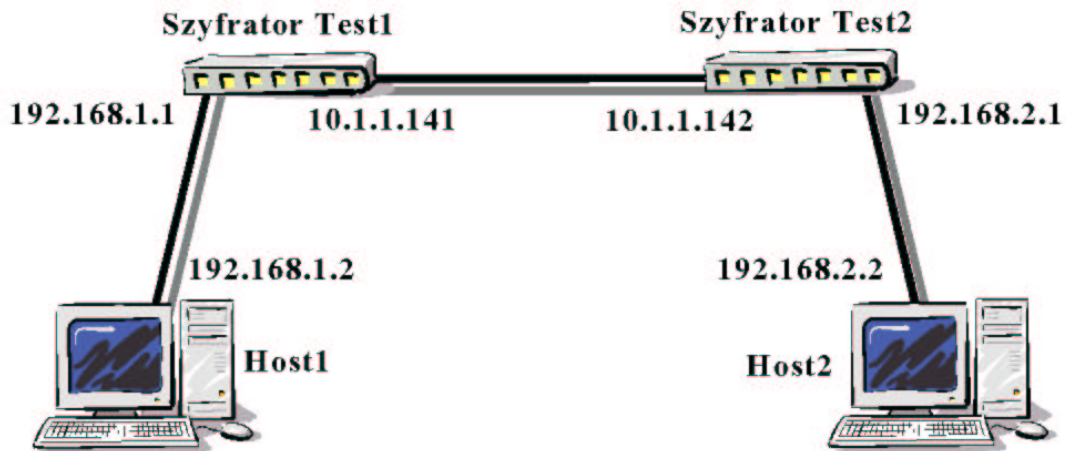


Testy wydajnościowe szyfratorów IPsec Gate

Konfiguracja testowa



Konfiguracja szyfratorów

Szyfrator TEST1

```
interface eth0 10.1.1.141/24
interface eth1 192.168.1.1/24
```

Szyfrator TEST2

```
interface eth0 10.1.1.142/24
interface eth1 192.168.2.1/24
```

1. Transmisja poprzez szyfratory bez szyfrowania - nie jest zestawiany tunel, ruch poprzez szyfratory jest przekazywany niezmienny

1.1. Konfiguracja szyfratorów

Szyfrator TEST1

```
route default 10.1.1.142
```

Szyfrator TEST2

```
route default 10.1.1.141
```

Host1

```
route add -net 192.168.2.0 netmask 255.255.255.0 gw 192.168.1.1
```

Host1

```
route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.2.1
```

1.2. Testy wydajności

Lp.	Transfer [Mbit/sec]
1	89,58
2	89,55
3	89,66

2. Tunel AH: tryb tunelowy VPN

2.1. Konfiguracja szyfratorów

Szyfrator TEST1

```
route del default 10.1.1.142
peer test2 10.1.1.142
peer test2 secret test1234
peer test2 ah
peer test2 noesp
peer test2 route 192.168.2.0/24
peer test2 lroute 192.168.1.0/24
peer test2 enable
```

Szyfrator TEST2

```
route del default 10.1.1.141
peer test1 10.1.1.141
peer test1 secret test1234
peer test1 ah
peer test1 noesp
peer test1 route 192.168.1.0/24
peer test1 lroute 192.168.2.0/24
peer test1 enable
```

Host1

```
route del -net 192.168.2.0 netmask 255.255.255.0 gw 192.168.1.1
```

Host1

```
route del -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.2.1
```

2.2. Konfiguracja parametrów szyfrowania

Obydwa szyfratory w ten sam sposób

Modyfikacja parametrów IPsec IKE:

```
ipsec ikecipher aes-md5-modp1536
```

Modyfikacja parametrów IPsec ESP:

```
ipsec espcipher aes128-md5
```

2.3. Testy wydajności

Lp.	Opcje IPsec IKE	Opcje IPsec ESP	Transfer [Mbit/sec]
	3des-md5-modp1536	3des-md5	
1.			85,01
2.			85,71
3.			85,12
	3des-sha1-modp1536	3des-md5	
1.			84,93
2.			85,24
3.			85,31
	3des-sha2_256-modp1536	3des-md5	
1.			85,19
2.			85,33
3.			85,21
	3des-sha2_512-modp1536	3des-md5	
1.			85,16
2.			85,27
3.			85,63
	3des-sha2_512-modp3072	3des-md5	
1.			85,11
2.			85,67
3.			85,20
	3des-sha2_512-modp4096	3des-md5	
1.			84,74
2.			85,20
3.			85,32
	aes-sha2_512-modp4096	3des-md5	
1.			84,98
2.			85,69
3.			85,35
	aes-md5-modp4096	3des-md5	
1.			85,31
2.			85,38
3.			85,48
	aes-md5-modp1536	3des-md5	
1.			85,04
2.			85,50
3.			85,32
	aes-md5-modp1536	3des-sha1	
1.			84,94
2.			85,68
3.			85,27
	aes-md5-modp1536	3des-sha2_512	
1.			85,56
2.			85,21
3.			85,68

Lp.	Opcje IPsec IKE	Opcje IPsec ESP	Transfer [Mbit/sec]
	aes-md5-modp1536	aes128-sha2_512	
1.			84,78
2.			85,67
3.			85,29
	aes-md5-modp1536	aes128-md5	
1.			85,34
2.			85,49
3.			85,38
	aes-md5-modp1536	aes192-md5	
1.			85,08
2.			85,76
3.			85,34
	aes-md5-modp1536	aes192-sha2_512	
1.			85,43
2.			85,10
3.			85,37
	aes-md5-modp1536	aes256-sha2_512	
1.			84,94
2.			85,57
3.			85,42
	aes-md5-modp1536	aes256-md5	
1.			85,42
2.			85,28
3.			85,48

3. Tunel ESP: tryb tunelowy VPN

3.1. Konfiguracja szyfratorów

Szyfrator TEST1

```
peer test2 esp
peer test2 noah
peer test2 enable
```

Szyfrator TEST2

```
peer test1 esp
peer test1 noah
peer test1 enable
```

3.2. Konfiguracja parametrów szyfrowania

Obydwa szyfratory w ten sam sposób

Modyfikacja parametrów IPsec IKE:

```
ipsec ikecipher aes-md5-modp1536
```

Modyfikacja parametrów IPsec ESP:

```
ipsec espcipher aes128-md5
```

3.3. Testy wydajności

Lp.	Opcje IPsec IKE	Opcje IPsec ESP	Transfer [Mbit/sec]
	3des-md5-modp1536	3des-md5	
1.			65,86
2.			65,36
3.			65,55
	Aes-md5-modp1536	aes128-md5	
1.			73,33
2.			73,30
3.			73,45
	aes-md5-modp1536	aes192-md5	
1.			72,47
2.			72,76
3.			72,33
	aes-md5-modp1536	aes256-md5	
1.			65,32
2.			65,68
3.			65,54
	aes-md5-modp1536	aes128-sha1	
1.			64,66
2.			66,25
3.			66,81
	aes-md5-modp1536	aes128-sha2_256	
1.			48,18
2.			48,62
3.			48,25

Lp.	Opcje IPsec IKE	Opcje IPsec ESP	Transfer [Mbit/sec]
	aes-md5-modp1536	aes128-sha2_512	
1.			31,20
2.			31,23
3.			31,32
	aes-sha1-modp1536	aes128-md5	
1.			70,78
2.			70,86
3.			71,47
	aes-sha2_256-modp1536	aes128-md5	
1.			70,32
2.			71,59
3.			70,98
	aes-sha2_512-modp1536	aes128-md5	
1.			71,21
2.			71,59
3.			70,98
	aes-md5-modp1024	aes128-md5	
1.			72,75
2.			73,00
3.			73,01
	aes-md5-modp2048	aes128-md5	
1.			71,05
2.			71,16
3.			71,24
	aes-md5-modp4096	aes128-md5	
1.			71,28
2.			71,30
3.			71,20
	aes-sha2_512-modp4096	aes128-md5	
1.			71,89
2.			72,73
3.			72,55
	3des-sha2_512-modp4096	aes128-md5	
1.			72,31
2.			72,52
3.			72,64
	3des-sha2_512-modp4096	3des-md5	
1.			65,77
2.			65,64
3.			65,73
	3des-sha2_512-modp4096	aes192-md5	
1.			69,29
2.			69,24
3.			69,05

Lp.	Opcje IPsec IKE	Opcje IPsec ESP	Transfer [Mbit/sec]
	3des-sha2_512-modp4096	aes256-md5	
1.			65,42
2.			66,06
3.			66,12
	3des-sha2_512-modp4096	aes256-sha1	
1.			61,26
2.			61,70
3.			61,15
	3des-sha2_512-modp4096	aes256-sha2_256	
1.			45,79
2.			46,04
3.			46,02
	3des-sha2_512-modp4096	aes256-sha2_512	
1.			30,20
2.			30,38
3.			30,38
	3des-sha2_512-modp4096	3des-sha1	
1.			66,02
2.			66,18
3.			65,59
	3des-sha2_512-modp4096	3des-sha2_256	
1.			65,90
2.			65,77
3.			66,47
	3des-sha2_512-modp4096	3des-sha2_512	
1.			64,92
2.			66,16
3.			65,67

4. Konfiguracja sprzętu użytego do testów

Szyfratory

Procesor: Intel Celeron 900 MHz

RAM: 128 MB

Karty sieciowe: Intel EtherExpres 100/Pro

Host1

Procesor: Intel Celeron 633 MHz

RAM: 128 MB

Karta sieciowa: Intel EtherExpres 100/Pro

Host2

Procesor: Intel Pentium III 933 MHz

RAM: 512 MB

Karta sieciowa: Realtek RLT-8139