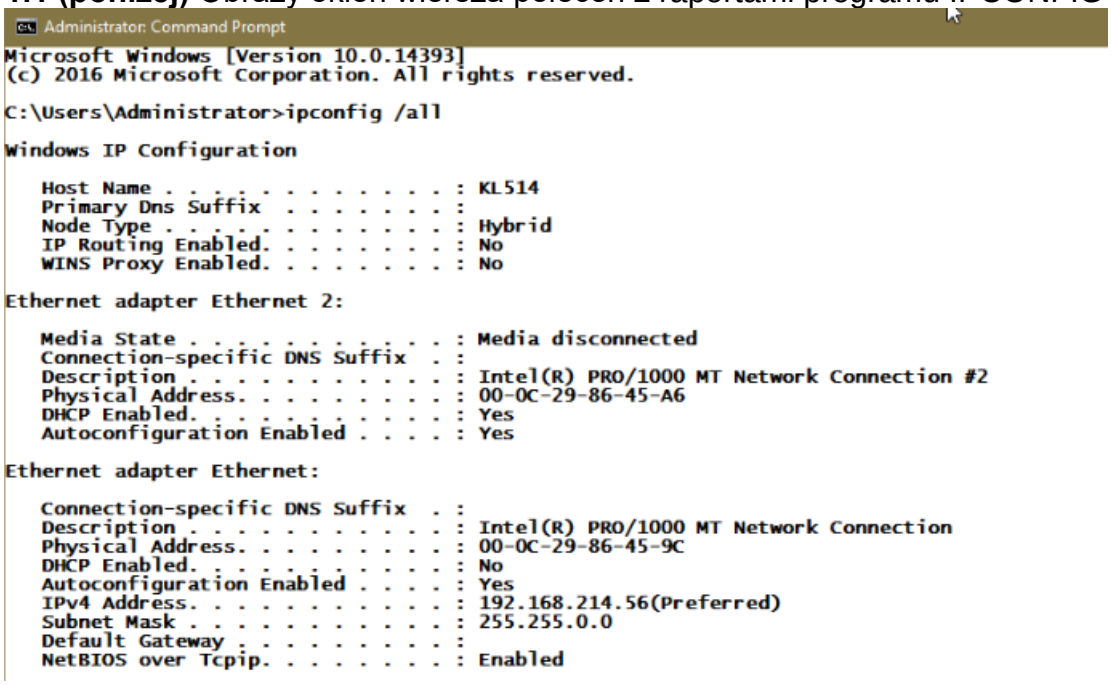
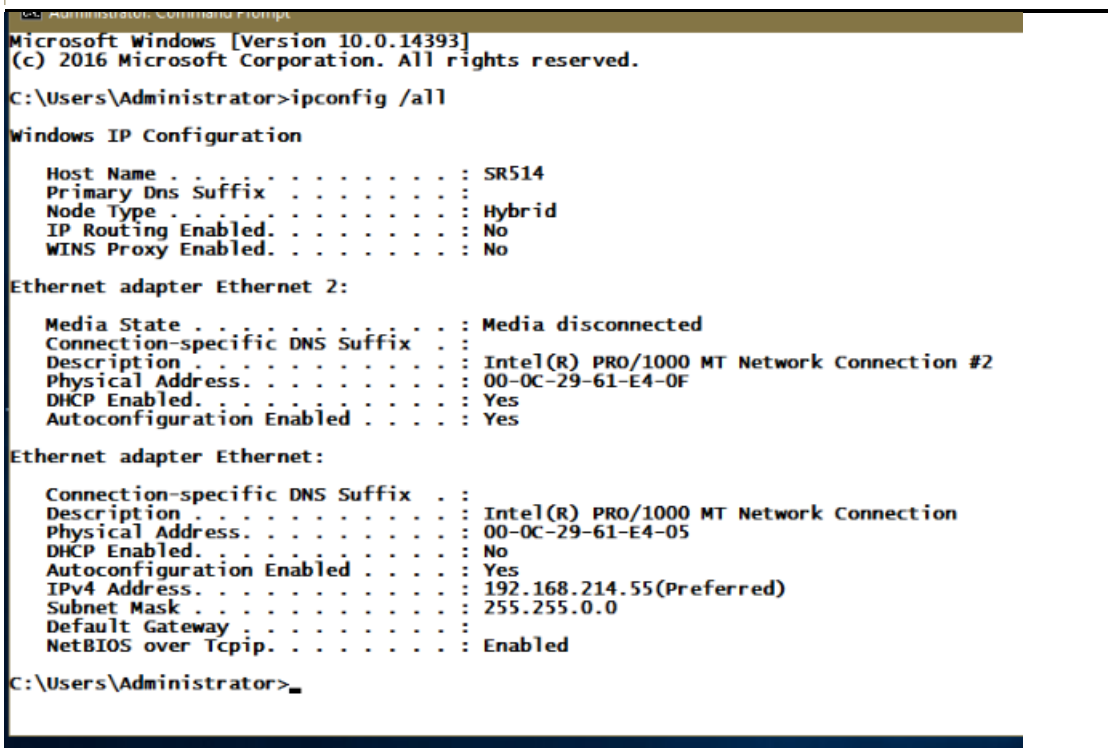
Temat 08a.2 Konfigurowanie i testowanie kanałów IPSec

Wykonał(a):Bartosz Miazga
Stanowisko: 14

Zadanie 1 - Weryfikacja poprawności komunikacji

1.1 (poniżej) Obrazy okien wiersza poleceń z raportami programu IPCONFIG /ALL (z obu maszyn)



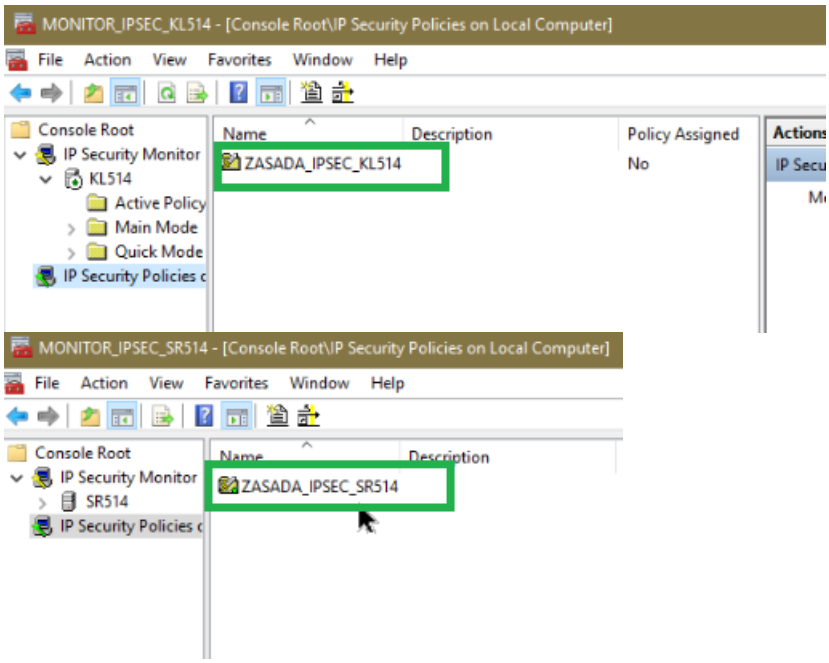


1.2 (poniżej) Obraz okna snifera z jednej z maszyn, z zaznaczonymi pakietami związanymi z testowaniem komunikacji między maszynami przy pomocy programu PING (krok 4 zadania)

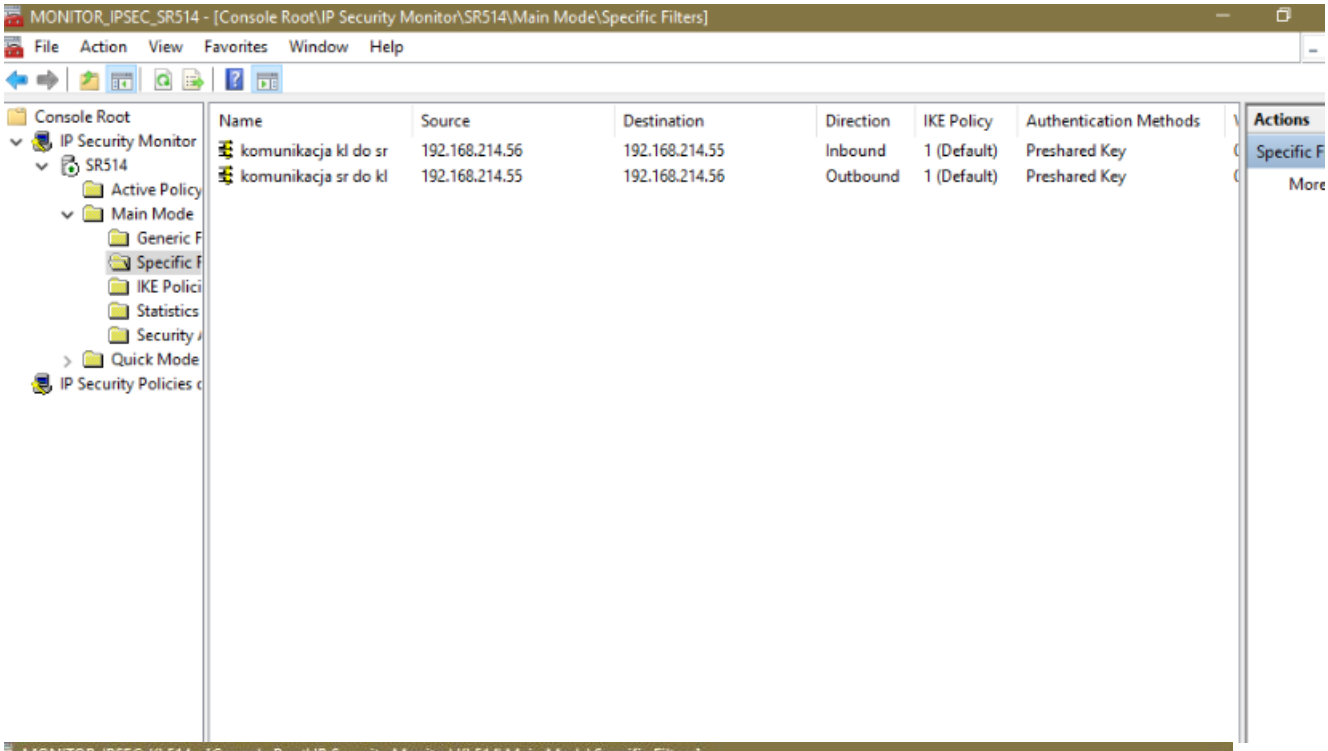
	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Vmware_61:e4:05	Broadcast	ARP	60	Who has 192.168.214.56? Tell 192.168.214.55
2	0.000019	Vmware_86:45:9c	Vmware_61:e4:05	ARP	42	192.168.214.56 is at 00:0c:29:86:45:9c
3	0.000132	192.168.214.55	192.168.214.56	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=1
4	0.000156	192.168.214.56	192.168.214.55	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=1
5	1.009535	192.168.214.55	192.168.214.56	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=1
6	1.009563	192.168.214.56	192.168.214.55	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=1
7	2.025201	192.168.214.55	192.168.214.56	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=1
8	2.025228	192.168.214.56	192.168.214.55	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=1
9	3.040861	192.168.214.55	192.168.214.56	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=
10	3.040905	192.168.214.56	192.168.214.55	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=
11	4.512458	Vmware_86:45:9c	Vmware_61:e4:05	ARP	42	Who has 192.168.214.55? Tell 192.168.214.56
12	4.512931	Vmware_61:e4:05	Vmware_86:45:9c	ARP	60	192.168.214.55 is at 00:0c:29:61:e4:05

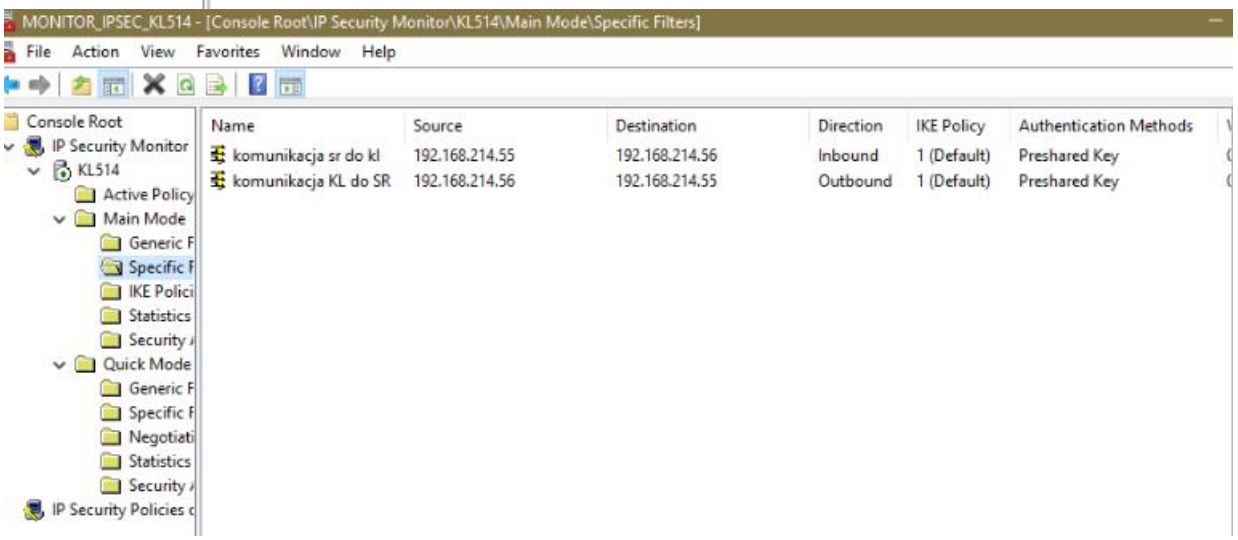
Zadanie 2 - Konfigurowanie kanału IPSec.

2.1 (poniżej) Obrazy okien konsol MONITOR_IPSEC_nazwa (z obu maszyn partnerskich) z zaznaczonymi, uaktywnionymi zasadami, które zostały skonfigurowane podczas realizacji tego zadania.



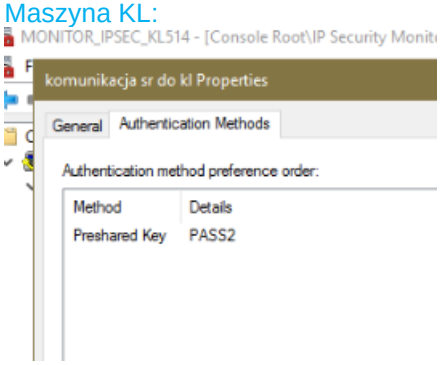
2.2 (poniżej) Obrazy okien właściwości zdefiniowanych zasad (z obu maszyn partnerskich), które zostały skonfigurowane podczas realizacji niniejszego zadania - podkontener *Specific Filters*, kontenera *Main Mode*, konsili MONITOR_IPSEC_~~nazwa~~. W pełni powinny być widoczne kolumny: *Name*, *Source*, *Destination*,*Direction*, *Authentication Methods*.

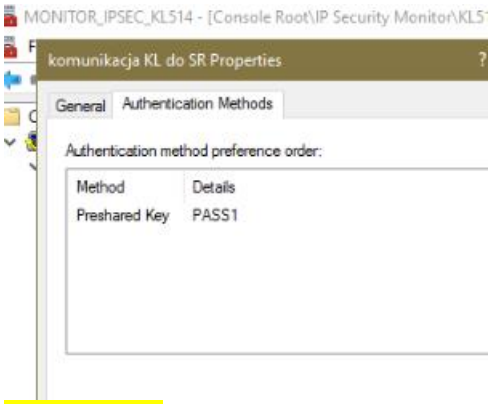




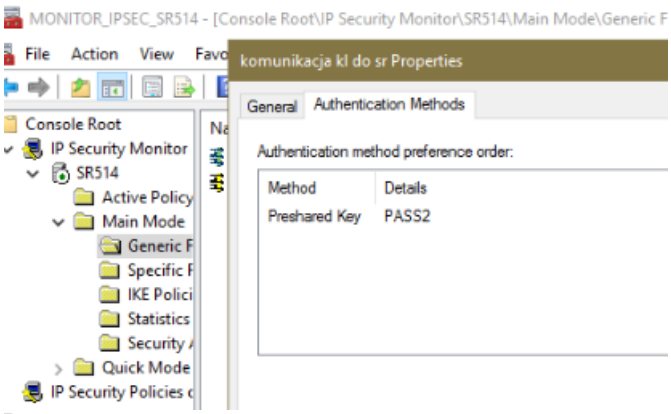
2.3 (poniżej) Obrazy okien prezentujących wybrane metody uwierzytelniania i ustalone hasła dostępu (dla wszystkich zdefiniowanych reguł) – uzyskane poprzez wybranie funkcji właściwości (*Properties*) reguł prezentowanych oknach w punkcie 2.2

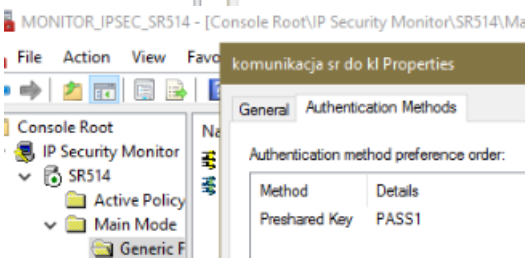
Maszyna KL:





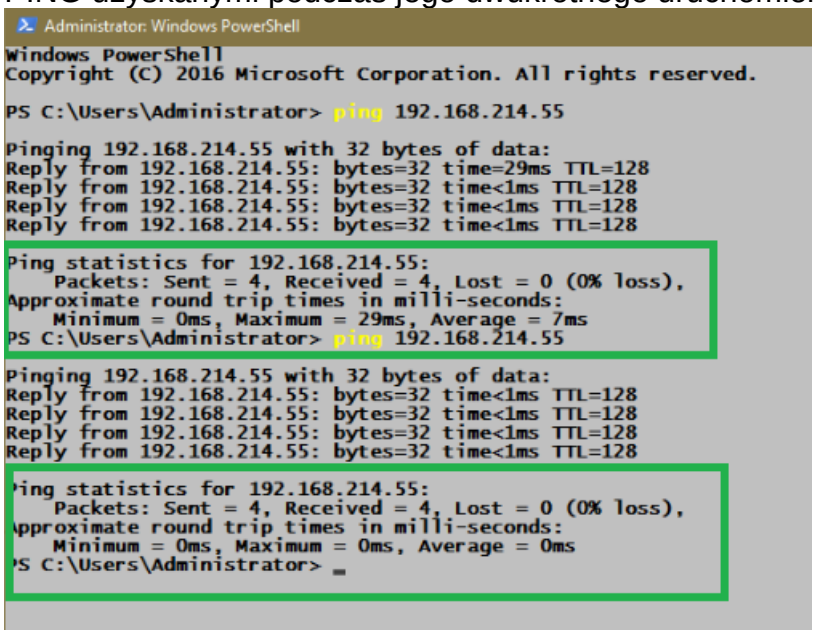
Maszyna SR:





Zadanie 3 - Testowanie poprawności pracy kanału IPSec.

3.1 (poniżej) Obraz okna programu *PowerShell* z zaznaczonymi raportami wynikowymi programu PING uzyskanymi podczas jego dwukrotnego uruchomienia (krok 1)



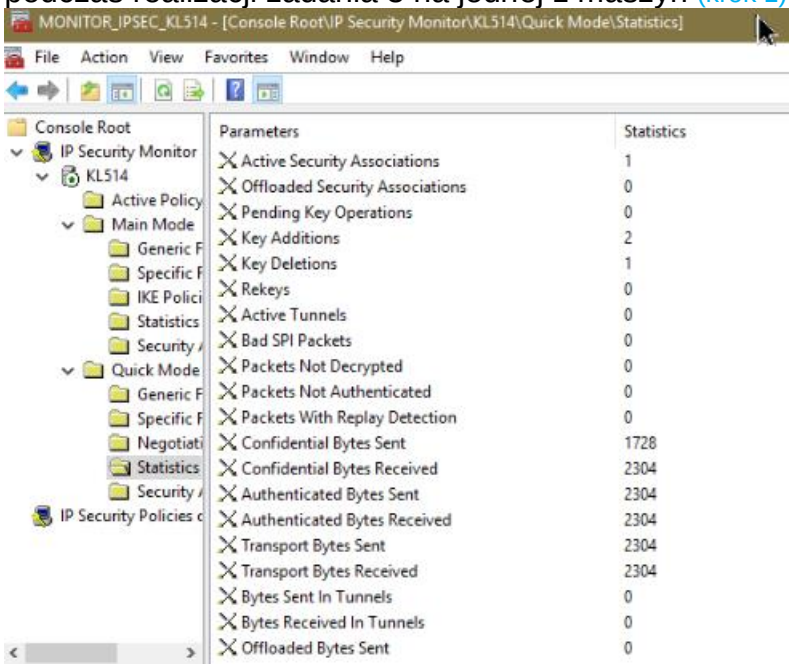
3.2 (poniżej) Obraz okna snifera z zaznaczonymi pakietami fazy negocjacji (krok 1)

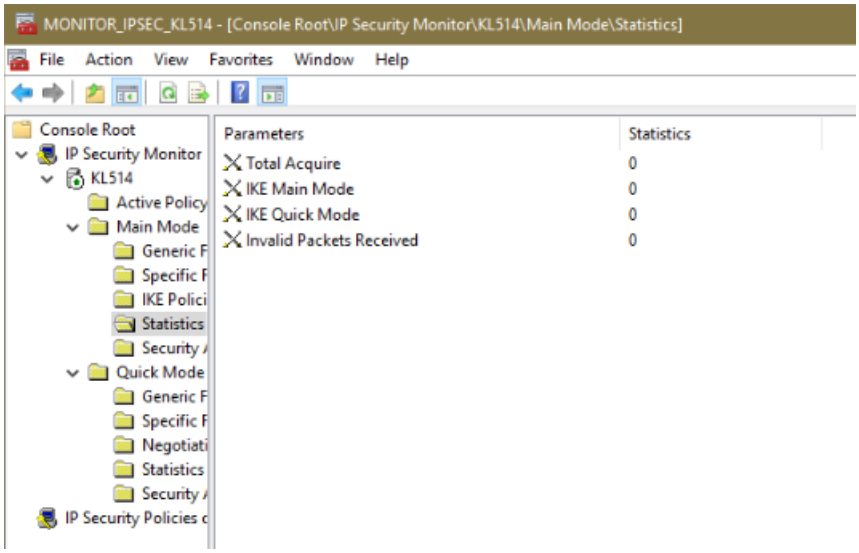
	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.214.56	192.168.214.55	ISAKMP	294	Identity Protection (Main Mode)
2	0.000845	192.168.214.55	192.168.214.56	ISAKMP	250	Identity Protection (Main Mode)
3	0.001631	192.168.214.56	192.168.214.55	ISAKMP	302	Identity Protection (Main Mode)
4	0.002944	192.168.214.55	192.168.214.56	ISAKMP	302	Identity Protection (Main Mode)
5	0.003659	192.168.214.56	192.168.214.55	ISAKMP	110	Identity Protection (Main Mode)
6	0.003920	192.168.214.55	192.168.214.56	ISAKMP	110	Identity Protection (Main Mode)
7	0.004296	192.168.214.56	192.168.214.55	ISAKMP	214	Quick Mode
8	0.005036	192.168.214.55	192.168.214.56	ISAKMP	214	Quick Mode
9	0.005238	192.168.214.56	192.168.214.55	ISAKMP	102	Quick Mode
10	0.005741	192.168.214.55	192.168.214.56	ISAKMP	118	Quick Mode
11	[illegible]	[illegible]	[illegible]	ESP	110	ESP (SPI=0x6e8c26a4)
12	0.006186	192.168.214.55	192.168.214.56	ESP	110	ESP (SPI=0xc3cb8e56)
13	1.009966	192.168.214.56	192.168.214.55	ESP	110	ESP (SPI=0x6e8c26a4)
14	1.010399	192.168.214.55	192.168.214.56	ESP	110	ESP (SPI=0xc3cb8e56)
15	2.025405	192.168.214.56	192.168.214.55	ESP	110	ESP (SPI=0x6e8c26a4)
16	2.025729	192.168.214.55	192.168.214.56	ESP	110	ESP (SPI=0xc3cb8e56)
17	3.040938	192.168.214.56	192.168.214.55	ESP	110	ESP (SPI=0x6e8c26a4)
18	3.041186	192.168.214.55	192.168.214.56	ESP	110	ESP (SPI=0xc3cb8e56)
19	4.947104	Vmware_86:45:9c	Vmware_61:e4:05	ARP	42	Who has 192.168.214.55? Tell 192.168.214.56
20	4.947296	Vmware_61:e4:05	Vmware_86:45:9c	ARP	60	192.168.214.55 is at 00:0c:29:61:e4:05
21	4.976479	Vmware_61:e4:05	Vmware_86:45:9c	ARP	60	Who has 192.168.214.56? Tell 192.168.214.55
22	4.976492	Vmware_86:45:9c	Vmware_61:e4:05	ARP	42	192.168.214.56 is at 00:0c:29:86:45:9c

3.3 (poniżej) Obraz okna snifera z zaznaczonymi pakietami fazy zabezpieczonej transmisji (krok 1)

	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.214.56	192.168.214.55	ISAKMP	294	Identity Protection (Main Mode)
2	0.000845	192.168.214.55	192.168.214.56	ISAKMP	250	Identity Protection (Main Mode)
3	0.001631	192.168.214.56	192.168.214.55	ISAKMP	302	Identity Protection (Main Mode)
4	0.002944	192.168.214.55	192.168.214.56	ISAKMP	302	Identity Protection (Main Mode)
5	0.003659	192.168.214.56	192.168.214.55	ISAKMP	110	Identity Protection (Main Mode)
6	0.003920	192.168.214.55	192.168.214.56	ISAKMP	110	Identity Protection (Main Mode)
7	0.004296	192.168.214.56	192.168.214.55	ISAKMP	214	Quick Mode
8	0.005036	192.168.214.55	192.168.214.56	ISAKMP	214	Quick Mode
9	0.005238	192.168.214.56	192.168.214.55	ISAKMP	102	Quick Mode
10	0.005741	192.168.214.55	192.168.214.56	ISAKMP	118	Quick Mode
11	0.005988	192.168.214.56	192.168.214.55	ESP	110	ESP (SPI=0x6e8c26a4)
12	0.006186	192.168.214.55	192.168.214.56	ESP	110	ESP (SPI=0xc3cb8e56)
13	1.009966	192.168.214.56	192.168.214.55	ESP	110	ESP (SPI=0x6e8c26a4)
14	1.010399	192.168.214.55	192.168.214.56	ESP	110	ESP (SPI=0xc3cb8e56)
15	2.025405	192.168.214.56	192.168.214.55	ESP	110	ESP (SPI=0x6e8c26a4)
16	2.025729	192.168.214.55	192.168.214.56	ESP	110	ESP (SPI=0xc3cb8e56)
17	3.040938	192.168.214.56	192.168.214.55	ESP	110	ESP (SPI=0x6e8c26a4)
18	3.041186	192.168.214.55	192.168.214.56	ESP	110	ESP (SPI=0xc3cb8e56)
19	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible] 192.168.214.56
20	4.947296	Vmware_61:e4:05	Vmware_86:45:9c	ARP	60	192.168.214.55 is at 00:0c:29:61:e4:05
21	4.976479	Vmware_61:e4:05	Vmware_86:45:9c	ARP	60	Who has 192.168.214.56? Tell 192.168.214.55
22	4.976492	Vmware_86:45:9c	Vmware_61:e4:05	ARP	42	192.168.214.56 is at 00:0c:29:86:45:9c

3.4 (poniżej) Obrazy okien konsoli MONITOR_IPSEC_nazwa (oba kontenery *Statystyka*) uzyskany podczas realizacji zadania 3 na jednej z maszyn (krok 1)





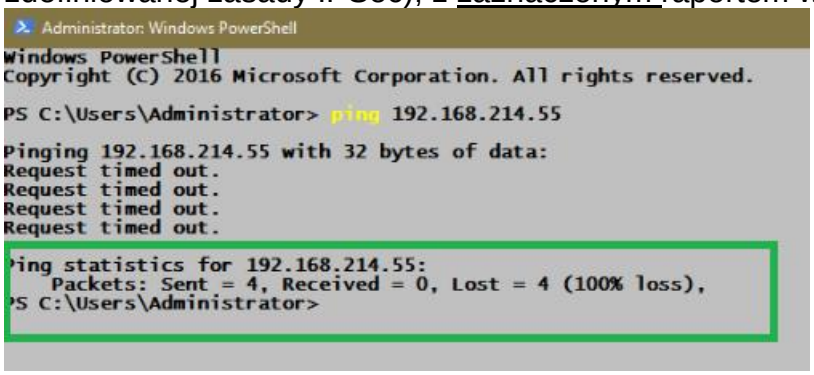
3.5. Spostrzeżenia i wnioski dotyczące zadania 3

Podczas wykonywania pierwszego podpunktu można zaobserwować następujący ruch sieciowy pomiędzy maszynami: na początku obserwuję negocjację klucza i parametrów połączenia – w czasie tych negocjacji wykorzystywany jest protokół **ISAKMP** - najpierw protokół ISAKMP działa w trybie głównym ,podczas którego ustanawiany jest bezpieczny, uwierzytelniony kanał komunikacyjny pomiędzy komputerami wykorzystywany w dalszych negocjacjach
Podczas działania trybu głównego uzgadniane są algorytmy szyfrujące , haszujące, metody uwierzytelniania oraz tzw. Grupa Fiffie -Hellmana. Generowana jest również para kluczy- prywatny i publiczny na podstawie grupy D-H oraz tzw. Materiał klucza, służący potem do generowania kluczy w trybie szybkim.
Następnie po trybie głownym protokół przechodzi w tryb szybki, podczas którego wykorzystywany jest bezpieczny kanał utworzony przez tryb główny, negocjowane są SA wykorzystywane do zabezpieczenia transmisji danych.
Po zakończeniu działania protokołu ISAKMP następuje bezpieczna transmisja pakietów pomiędzy użytkownikami. W fazie zabezpieczonej transmisji (po negocjacjach) wykorzystywany jest protokół **ESP**.
W kontenerach prezentujących statystyki ruchu sieciowego można zaobserwować następujące zmiany:
W „Quick Mode/Statistics” zwiększyła się wartość:
„Key Additions”
„Key Deletions”
„Confidential Bytes Sent”
„Confidential Bytes Received”
„Authenticated Bytes Sent”
„Authenticated Bytes Received”
„Transport Bytes Sent”
„Transport Bytes Received”

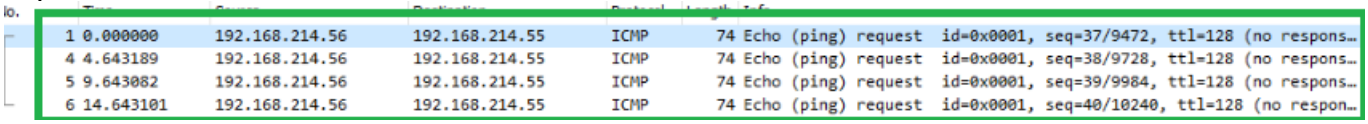
Podczas wykonywania czwartego podpunktu **nie zaobserwowałem różnic** w stosunku do obrazów uzyskanych podczas realizacji kroku 1.

Zadanie 4 - Wyłączanie zabezpieczeń IPSec.

4.1 (poniżej) Obraz okna wiersza poleceń z maszyny KLxxx (na której dokonano deaktywacji zdefiniowanej zasady IPSec), z zaznaczonym raportem wynikowym programu PING (krok 2).

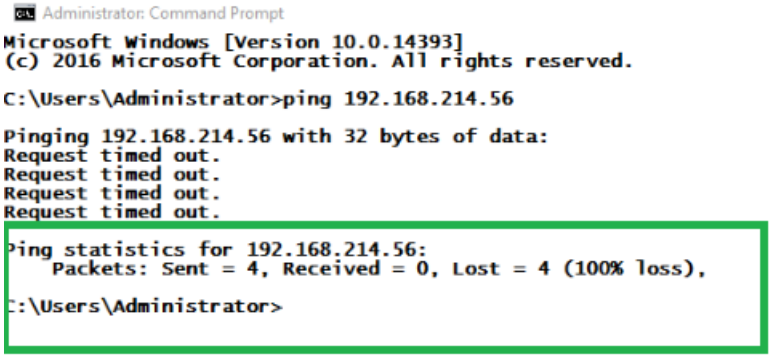


4.2 (poniżej) Obraz okna snifera z zaznaczonymi pakietami związanymi z raportem przedstawionym w punkcie 4.1.

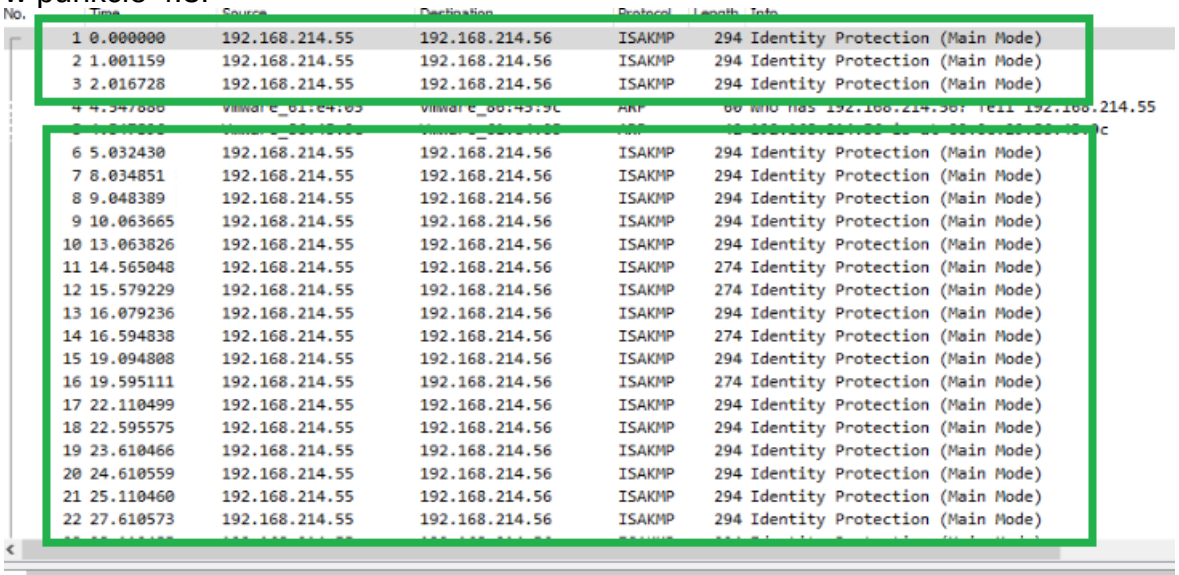


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.214.56	192.168.214.55	ICMP	74	Echo (ping) request id=0x0001, seq=37/9472, ttl=128 (no respons…
4	4.643189	192.168.214.56	192.168.214.55	ICMP	74	Echo (ping) request id=0x0001, seq=38/9728, ttl=128 (no respons…
5	9.643082	192.168.214.56	192.168.214.55	ICMP	74	Echo (ping) request id=0x0001, seq=39/9984, ttl=128 (no respons…
6	14.643101	192.168.214.56	192.168.214.55	ICMP	74	Echo (ping) request id=0x0001, seq=40/10240, ttl=128 (no respon…

4.3 (poniżej) Obraz okna wiersza poleceń z maszyny SRxxx (na której nie wyłączono zdefiniowanej zasady IPSec), z zaznaczonym raportem wynikowym programu PING (krok 2).



4.4 (poniżej) Obraz okna snifera z zaznaczonymi pakietami związanymi z raportem przedstawionym w punkcie 4.3.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.214.55	192.168.214.56	ISAKMP	294	Identity Protection (Main Mode)
2	1.001159	192.168.214.55	192.168.214.56	ISAKMP	294	Identity Protection (Main Mode)
3	2.016728	192.168.214.55	192.168.214.56	ISAKMP	294	Identity Protection (Main Mode)
6	5.032430	192.168.214.55	192.168.214.56	ISAKMP	294	Identity Protection (Main Mode)
7	8.034851	192.168.214.55	192.168.214.56	ISAKMP	294	Identity Protection (Main Mode)
8	9.048389	192.168.214.55	192.168.214.56	ISAKMP	294	Identity Protection (Main Mode)
9	10.063665	192.168.214.55	192.168.214.56	ISAKMP	294	Identity Protection (Main Mode)
10	13.063826	192.168.214.55	192.168.214.56	ISAKMP	294	Identity Protection (Main Mode)
11	14.565048	192.168.214.55	192.168.214.56	ISAKMP	274	Identity Protection (Main Mode)
12	15.579229	192.168.214.55	192.168.214.56	ISAKMP	274	Identity Protection (Main Mode)
13	16.079236	192.168.214.55	192.168.214.56	ISAKMP	294	Identity Protection (Main Mode)
14	16.594838	192.168.214.55	192.168.214.56	ISAKMP	274	Identity Protection (Main Mode)
15	19.094808	192.168.214.55	192.168.214.56	ISAKMP	294	Identity Protection (Main Mode)
16	19.595111	192.168.214.55	192.168.214.56	ISAKMP	274	Identity Protection (Main Mode)
17	22.110499	192.168.214.55	192.168.214.56	ISAKMP	294	Identity Protection (Main Mode)
18	22.595575	192.168.214.55	192.168.214.56	ISAKMP	294	Identity Protection (Main Mode)
19	23.610466	192.168.214.55	192.168.214.56	ISAKMP	294	Identity Protection (Main Mode)
20	24.610559	192.168.214.55	192.168.214.56	ISAKMP	294	Identity Protection (Main Mode)
21	25.110460	192.168.214.55	192.168.214.56	ISAKMP	294	Identity Protection (Main Mode)
22	27.610573	192.168.214.55	192.168.214.56	ISAKMP	294	Identity Protection (Main Mode)

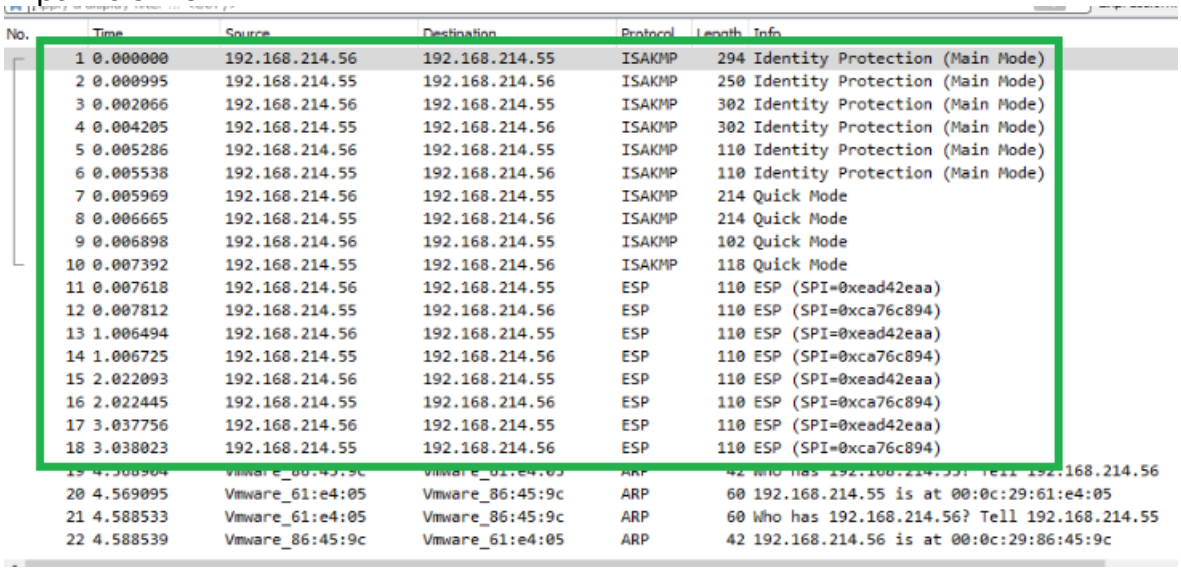
4.5 (poniżej) Obraz okna wiersza poleceń z maszyny KLxxx, na której ponownie przypisano zasadę IPSec, z zaznaczonym raportem wynikowym programu PING (krok 4).

```
PS C:\Users\Administrator> ping 192.168.214.55

Pinging 192.168.214.55 with 32 bytes of data:
Reply from 192.168.214.55: bytes=32 time=10ms TTL=128
Reply from 192.168.214.55: bytes=32 time<1ms TTL=128
Reply from 192.168.214.55: bytes=32 time<1ms TTL=128
Reply from 192.168.214.55: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.214.55:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
PS C:\Users\Administrator> _
```

4.6 (poniżej) Obraz okna snifera z zaznaczonymi pakietami związanymi z raportem przedstawionym w punkcie 4.5.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.214.56	192.168.214.55	ISAKMP	294	Identity Protection (Main Mode)
2	0.000995	192.168.214.55	192.168.214.56	ISAKMP	250	Identity Protection (Main Mode)
3	0.002066	192.168.214.56	192.168.214.55	ISAKMP	302	Identity Protection (Main Mode)
4	0.004205	192.168.214.55	192.168.214.56	ISAKMP	302	Identity Protection (Main Mode)
5	0.005286	192.168.214.56	192.168.214.55	ISAKMP	110	Identity Protection (Main Mode)
6	0.005538	192.168.214.55	192.168.214.56	ISAKMP	110	Identity Protection (Main Mode)
7	0.005969	192.168.214.56	192.168.214.55	ISAKMP	214	Quick Mode
8	0.006665	192.168.214.55	192.168.214.56	ISAKMP	214	Quick Mode
9	0.006898	192.168.214.56	192.168.214.55	ISAKMP	102	Quick Mode
10	0.007392	192.168.214.55	192.168.214.56	ISAKMP	118	Quick Mode
11	0.007618	192.168.214.56	192.168.214.55	ESP	110	ESP (SPI=0xead42eaa)
12	0.007812	192.168.214.55	192.168.214.56	ESP	110	ESP (SPI=0xca76c894)
13	1.006494	192.168.214.56	192.168.214.55	ESP	110	ESP (SPI=0xead42eaa)
14	1.006725	192.168.214.55	192.168.214.56	ESP	110	ESP (SPI=0xca76c894)
15	2.022093	192.168.214.56	192.168.214.55	ESP	110	ESP (SPI=0xead42eaa)
16	2.022445	192.168.214.55	192.168.214.56	ESP	110	ESP (SPI=0xca76c894)
17	3.037756	192.168.214.56	192.168.214.55	ESP	110	ESP (SPI=0xead42eaa)
18	3.038023	192.168.214.55	192.168.214.56	ESP	110	ESP (SPI=0xca76c894)
19	4.568984	Vmware_86:45:9c	Vmware_61:e4:05	ARP	42	Who has 192.168.214.55? Tell 192.168.214.56
20	4.569095	Vmware_61:e4:05	Vmware_86:45:9c	ARP	60	192.168.214.55 is at 00:0c:29:61:e4:05
21	4.588533	Vmware_61:e4:05	Vmware_86:45:9c	ARP	60	Who has 192.168.214.56? Tell 192.168.214.55
22	4.588539	Vmware_86:45:9c	Vmware_61:e4:05	ARP	42	192.168.214.56 is at 00:0c:29:86:45:9c

4.7 Spostrzeżenia i wnioski dotyczące zadania 4

(m.in. odpowiedzi na pytania i polecenia sformułowane w treści zadania)

W podpunkcie drugim ,po dezaktywacji zasady ZASADA_IPSEC_KL514 urządzenia próbują dokonać wymiany klucza i parametrów, jednakże wymiana nie jest w stanie zakończyć się powodzeniem. Nie ma komunikacji pomiędzy urządzeniami. Negocjacje nie mogą się zakończyć i nie dochodzi do bezpiecznej transmisji pakietów.

W podpunkcie czwartym ,po aktywacji zasady ZASADA_IPSEC_KL514 komunikacja między maszynami powraca do normy. Następuje wymiana kluczy i parametrów połączenia po czym dochodzi do bezpiecznej transmisji pakietów.

Własne uwagi, wnioski i propozycje dotyczące przebiegu ćwiczenia, mające na celu polepszenie procesu kształcenia:

.....

.....