

O co chodzi z tym APN?

APN prywatny/publiczny - wady/zalety

O mnie

- w branży ICT od 2006,
- najpierw telekomunikacja (analogowa -> cyfrowa -> VoIPowa),
- później doszły sieci komputerowe,
- z mikrotika korzystam od 2017r (MTCNA, MTCRE)
- na co dzień pracuje dla operatora sieci komórkowej,
- równolegle - wdrażam rozwiązania sieciowe i telekomunikacyjne w przedsiębiorstwach,

Hobby branżowe: VoIP (SIP) <- polecam się ;-)

Hobby prywatne: różne ;-)



Karol Skibiński



[https://www.linkedin.com/
in/karolskibinski/](https://www.linkedin.com/in/karolskibinski/)

Wstęp

Co to APN (Access Point Name)?

- duże uproszczenie - nazwa bramy pomiędzy siecią komórkową 2G/3G/4G/5G, a inną siecią komputerową (np. Internet),
- nieco dokładniej - zestaw parametrów sieci komputerowej z którą łączy się urządzenie z kartą SIM,

Przykładowe APN z których używamy na co dzień:

- internet - kieruje do Internetu
- MMS - kieruje do "bramki MMS"

A czy mogę mieć APN kierujący do mojego routera brzegowego?
Ktoś może zapytać "po co?". Ktoś inny zapyta "jakie to ma wady/zalety?".

O tym w dalszej części spotkania/prezentacji.

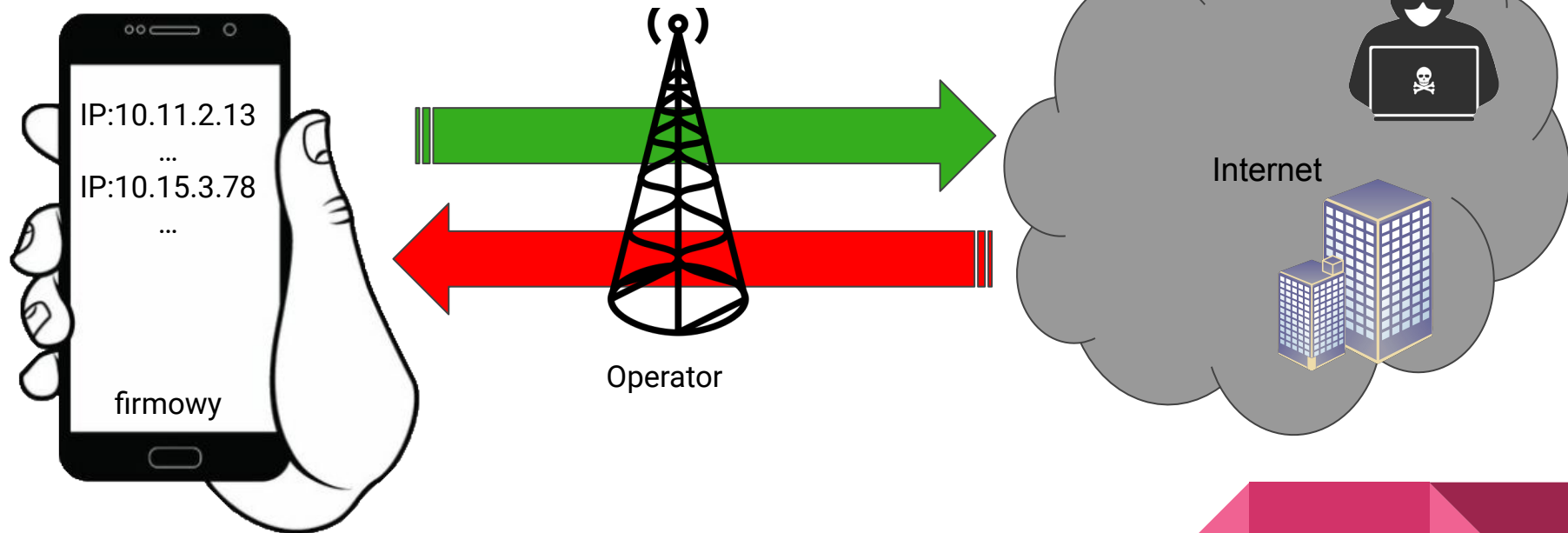


Rodzaje APN?:

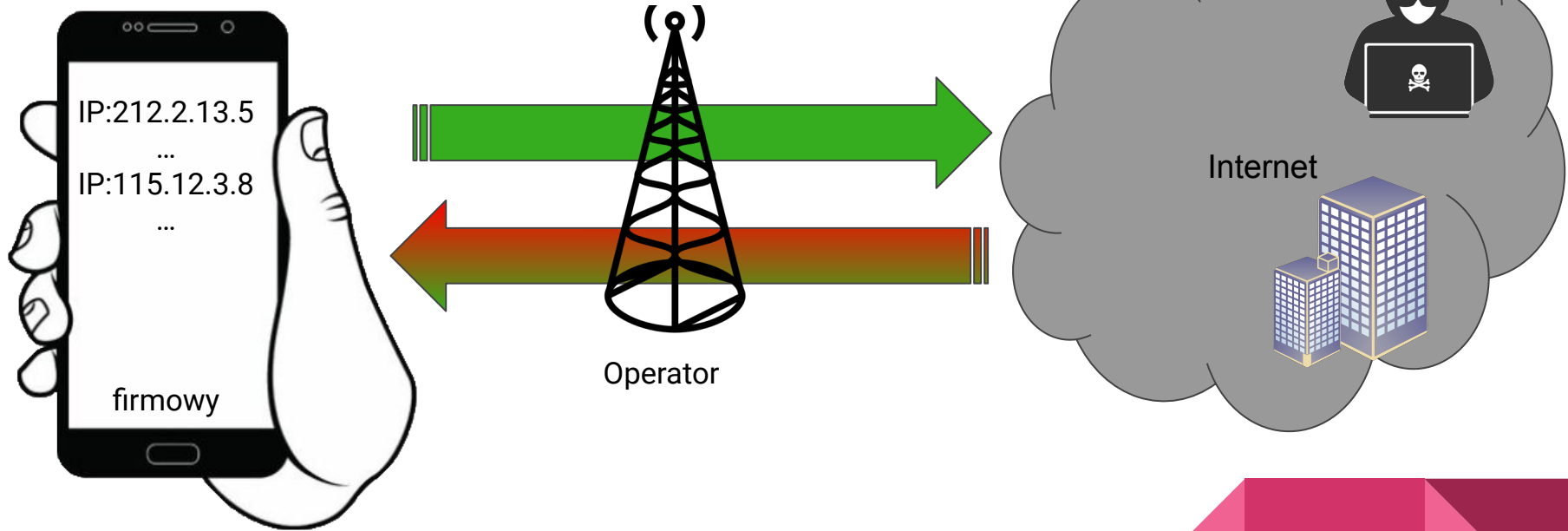
- publiczny
 - z adresem prywatnym
 - z adresem publicznym dynamicznym
 - z adresem publicznym statyczny
- prywatny
 - intermobile/standard/zamknięty
 - intranet/premium/otwarty



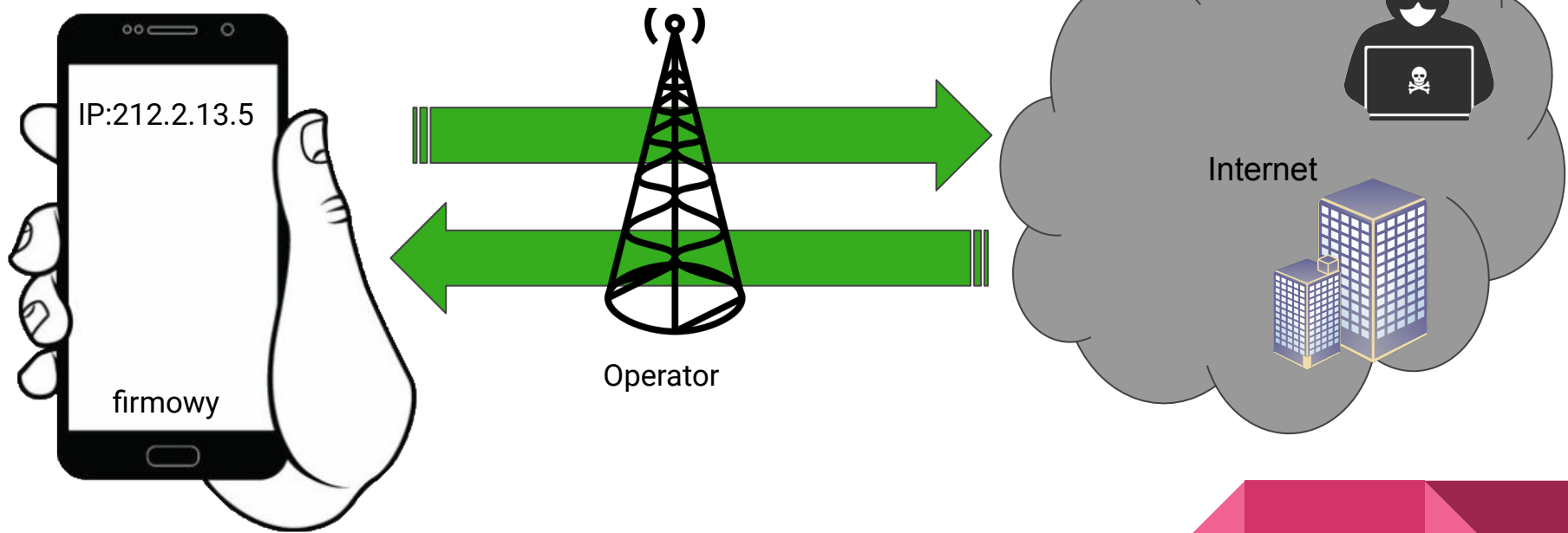
Rodzaj APN - publiczny (internet)



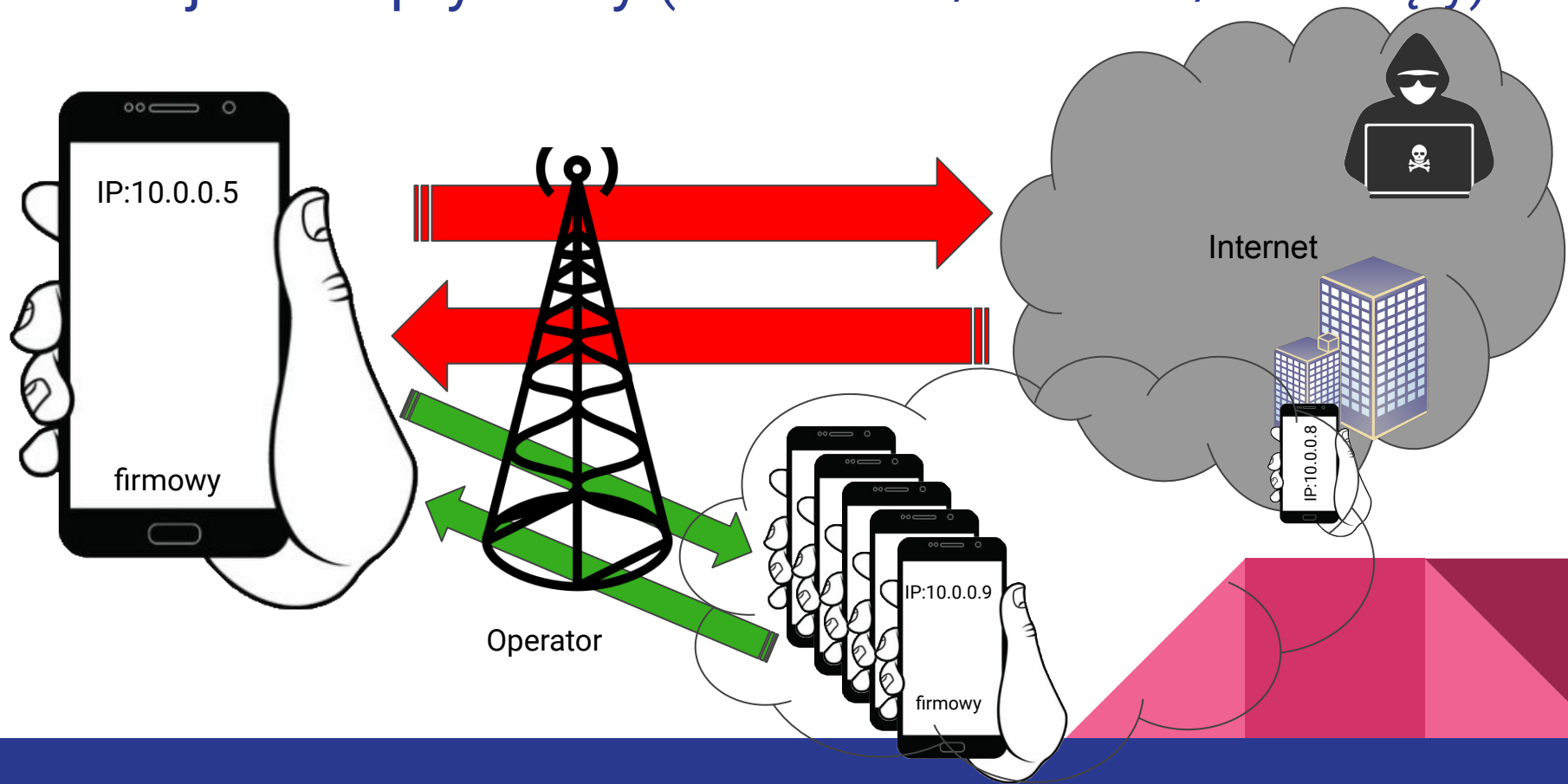
Rodzaj APN - dynamic (zmiennie publiczne IP)



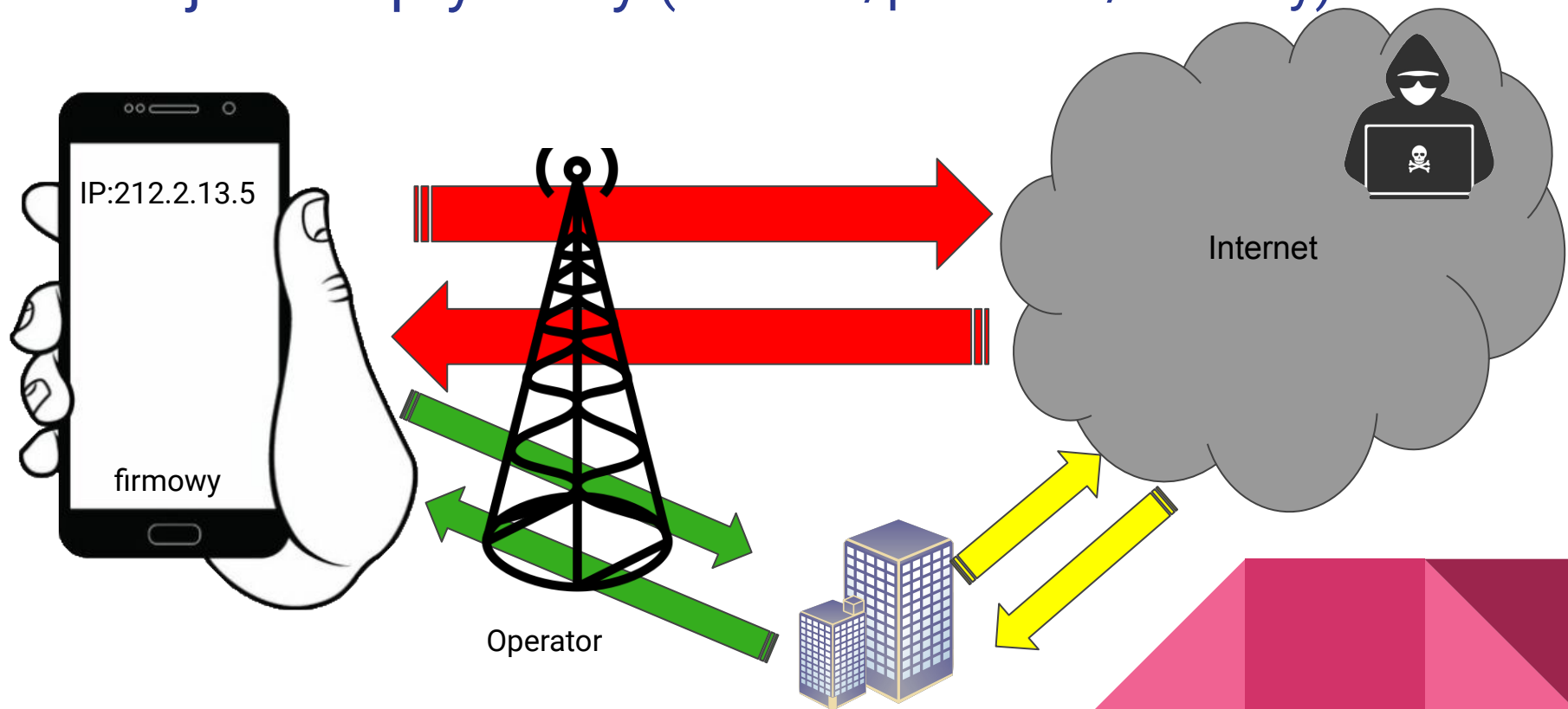
Rodzaj APN - static (stałe publiczne IP)



Rodzaj APN - prywatny (intermobile/standard/zamknięty)



Rodzaj APN - prywatny (intranet/premium/otwarty)

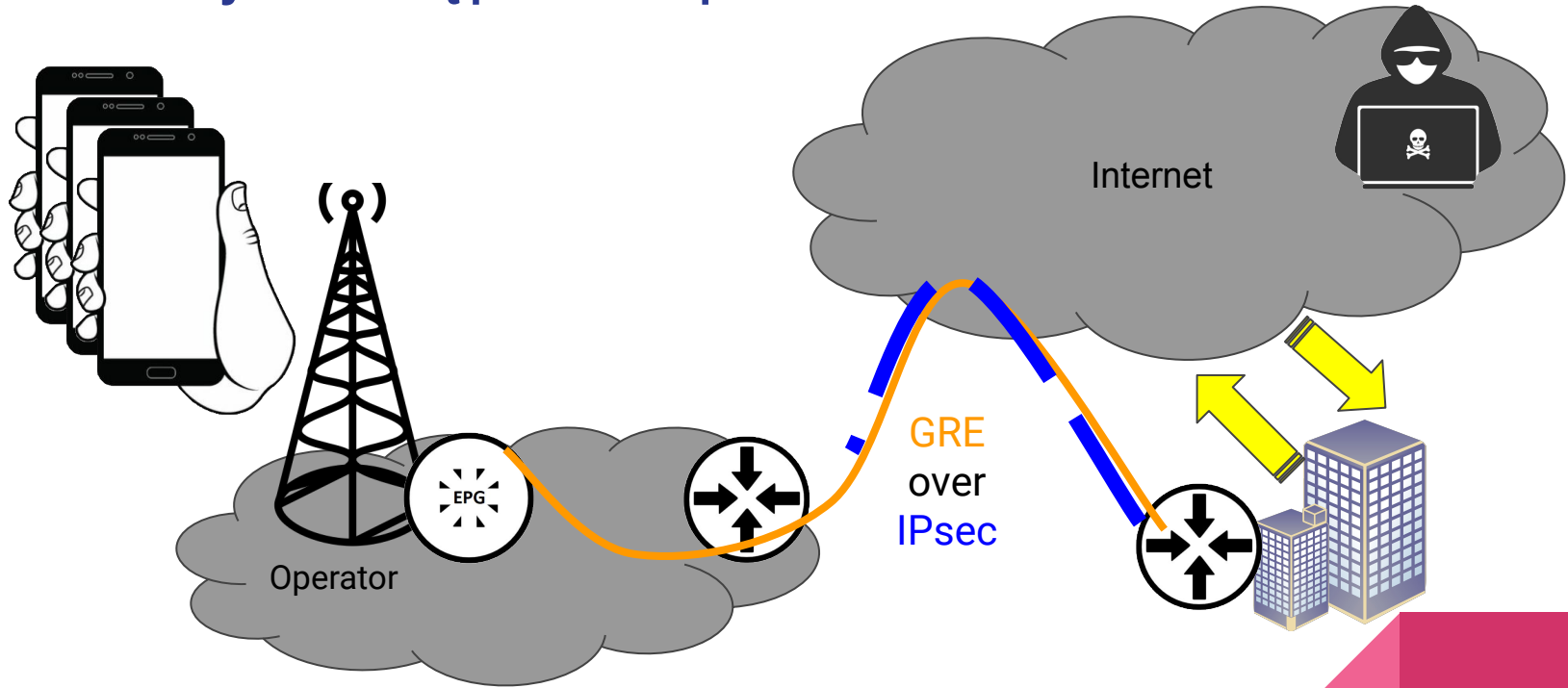


Podsumowanie

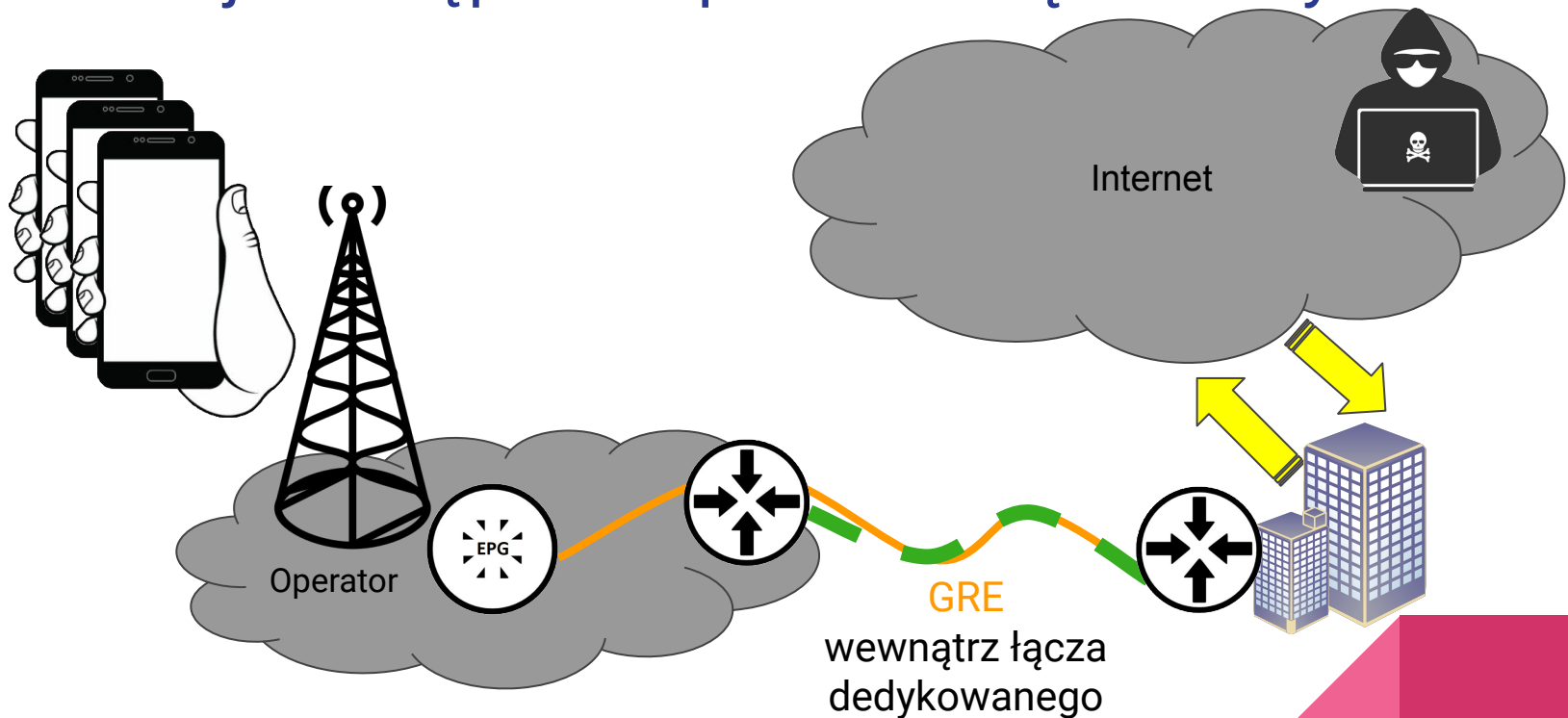
	publiczny	dynamic [x zł]*	static [xx zł]*	prywatny intermobile [xxx zł]*	prywatny intranet [xxx zł]*
adres IP	zmienny, prywatny lub CGNAT	zmienny, publiczny	stały, publiczny	stały, prywatny	stały, prywatny
dostęp do Internetu	tak	tak	tak	nie	konfigurowalne
dostęp z Internetu	nie	tak	tak	nie	konfigurowalne

* orientacyjny koszt (rzęd wielkości)

Rodzaje dostępu do operatora - tunel



Rodzaje dostępu do operatora - łącze dedykowane



Końcówka teorii teraz warsztaty.

Jak to wygląda i co jeszcze z tym możemy zrobić w routerze Mikrotik?

- konfiguracja wcześniej wymienionych APN w Mikrotiku
- multi APN
- passthrough
- routing przez konkretny APN



Opis LABu

Testy/doświadczenia prowadzimy na:

- hAP ac³ LTE (ROSv7.5) - konfiguracja bezpośrednio po przywróceniu ustawienia fabrycznych.
- karta SIM (Plus) z zaprovisionowanym po stronie operatora APNami:
 - publiczny
 - z adresem prywatnym (internet)
 - z adresem publicznym dynamicznym (pro.plusgsm.pl)
 - z adresem publicznym statyczny (m2m.plusgsm.pl)
 - prywatny
 - ~~intermobile/standard/zamknięty~~
 - intranet/premium/otwarty (twoja-firma.pl)

nazwa do ustalenia indywidualnie z operatorem

Scenariusz testowy #01

Mikrotik ma mieć dostęp do Internetu i znajdować się za NATem realizowanym przez operatora komórkowego.

Realizujemy to poprzez połączenie z APN publicznym o nazwie "internet"



Realizacja #01

Konfiguracja domyślna jest wystarczająca, aby połączyć się do publicznego APN “internet”. Dla porządku zmieniliśmy tylko nazwę profilu z “default” na “public”.

```
[admin@MikroTik] > interface lte apn
set [ find default=yes ] name=public
```

```
[admin@MikroTik] > ip address print
Flags: D - DYNAMIC
Columns: ADDRESS, NETWORK, INTERFACE
# ADDRESS NETWORK INTERFACE
;;; defconf
0 192.168.88.1/24 192.168.88.0 bridge
1 D 100.111.93.112/32 100.111.93.112 lte1
```

Po połączeniu z siecią widzimy, że interfejs sieciowy lte1 otrzymuje adres prywatny lub CGNAT

Scenariusz testowy #02

Mikrotik ma mieć dostęp do Internetu bez NAT i być dostępny pod publicznym adresem IP. Adres ten może się zmieniać przy kolejnych zestawieniach połączenia do operatora komórkowego.

Realizujemy to poprzez połączenie z APN publicznym dynamicznym o nazwie "pro.plusgsm.pl". Oczywiście wymaga to jeszcze dodania reguły w firewallu na chain=input, która zezwala na dostęp na konkretny port. Ten fragment z firewallem pomijamy podczas warsztatów.



Realizacja #02

Najpierw dodajemy nowy profil APN:

```
[admin@MikroTik] > interface lte apn add name=dynamic apn=pro.plusgsm.pl
```

Następnie ustawiamy go w konfiguracji interfejsu lte1:

```
[admin@MikroTik] > interface lte set apn-profiles=dynamic lte1
```

```
[admin@MikroTik] > ip address print
Flags: D - DYNAMIC
Columns: ADDRESS, NETWORK, INTERFACE
# ADDRESS NETWORK INTERFACE
;;; defconf
0 192.168.88.1/24 192.168.88.0 bridge
1 D 46.77.89.248/32 46.77.89.248 lte1
```

adres zmienny

Po połączeniu z siecią widzimy, że interfejs sieciowy lte1 ma adres publiczny.

Scenariusz testowy #03

Mikrotik ma mieć dostęp do Internetu bez NAT i być dostępny pod publicznym adresem IP. Adres ten **nie** może się zmieniać przy kolejnych zestawieniach połączenia do operatora komórkowego.

Realizujemy to poprzez połączenie z APN publicznym dynamicznym o nazwie "m2m.plusgsm.pl". Podobnie jak w poprzednim scenariuszu pomijamy konfigurację firewalla.



Realizacja #03

Najpierw dodajemy nowy profil APN:

```
[admin@MikroTik] > interface lte apn add name=static apn=m2m.plusgsm.pl
```

Następnie ustawiamy go w konfiguracji interfejsu lte1:

```
[admin@MikroTik] > interface lte set apn-profiles=static lte1
```

```
[admin@MikroTik] > ip address print
Flags: D - DYNAMIC
Columns: ADDRESS, NETWORK, INTERFACE
#  ADDRESS          NETWORK  INTERFACE
;;; defconf
0  192.168.88.1/24   192.168.88.0  bridge
1  D 31.0.237.104/32 31.0.237.104  lte1
```

adres stały

Po połączeniu z siecią widzimy, że interfejs sieciowy lte1 ma adres publiczny.

Scenariusz testowy #04

Mikrotik ma mieć adres prywatny z naszej sieci firmowej. Połączenie do/z niego realizowane jest tylko przy użyciu routera brzegowego w naszej firmie.

Realizujemy to poprzez połączenie z APN prywatnym o nazwie “twoja-firma.pl” (indywidualnie do ustalenia z operatorem po zawarciu umowy). Zakładamy, że łącze pomiędzy operatorem, a naszą firmą już jest zestawione np. w oparciu o GRE over IPsec.



Realizacja #04

Najpierw dodajemy nowy profil APN:

```
[admin@MikroTik] > interface lte apn add name=private apn=twoja-firma.pl
```

nazwa do ustalenia indywidualnie z operatorem

Następnie ustawiamy go w konfiguracji interfejsu lte1:

```
[admin@MikroTik] > interface lte set apn-profiles=private lte1
```

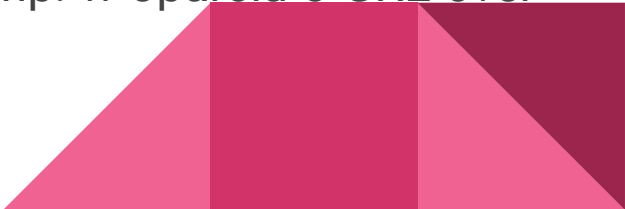
```
[admin@MikroTik] > ip address print
Flags: D - DYNAMIC
Columns: ADDRESS, NETWORK, INTERFACE
# ADDRESS NETWORK INTERFACE
;;; defconf
0 192.168.88.1/24 192.168.88.0 bridge
1 D 172.21.2.40/32 172.21.2.40 lte1
```

Po połączeniu z siecią widzimy, że interfejs sieciowy lte1 ma adres prywatny z naszej sieci firmowej.

Scenariusz testowy #05

Mikrotik ma mieć dostęp do Internetu poprzez APN publiczny oraz dostęp do zasobów firmowych poprzez APN prywatny. Cały ruch z Mikrotika wychodzi przez APN publiczny, jedynie ruch pod adresacją firmową 172.21.0.0/16 oraz np. 195.78.67.62 ma wychodzić przez APN prywatny.

Realizujemy to poprzez połączenie z APN publicznym i prywatnym oraz konfigurację NATa. To od konfiguracji NAT zależy poprzez który APN realizowany jest ruch wyjściowy. Podobnie jak w poprzednim scenariuszu zakładamy, że łącze pomiędzy operatorem, a naszą firmą już jest zestawione np. w oparciu o GRE over IPsec.



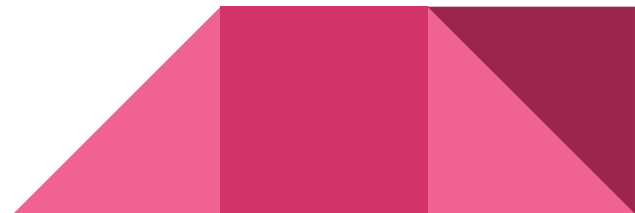
Realizacja #05

Profile APN private i public mamy już dodane w poprzednich scenariuszach. Konfigurujemy więc od razu interfejsu lte1 dodając dwa w/w profile:

```
[admin@MikroTik] > interface lte set apn-profiles=public,private lte1
```

Następnie konfigurujemy NAT wskazując na adres lte1 w APN private:

```
[admin@MikroTik] > ip firewall nat add chain=srcnat dst-address=172.21.0.0/16 out-interface-list=WAN  
action=src-nat to-addresses=172.21.2.40 place-before=0  
[admin@MikroTik] > ip firewall nat add chain=srcnat dst-address=195.78.67.62/32 out-interface-list=WAN  
action=src-nat to-addresses=172.21.2.40 place-before=0
```



Scenariusz testowy #06

Poprzedni scenariusz rozbudowujemy o przeźroczyste przepuszczenie przez Mikrotika APN static na urządzenie podłączone do ether5. W efekcie urządzenie podpięte do tego interfejsu 5. otrzyma adres publiczny prosto z konfiguracji APN i pod tym adresem publicznym jest dostępne.

Realizujemy to poprzez połączenie z APN publicznym, prywatnym i statycznym oraz usunięcie ether5 z bridge'a. Podobnie jak w poprzednim scenariuszu zakładamy, że łącze pomiędzy operatorem, a naszą firmą już jest zestawione np. w oparciu o GRE over IPsec.



Realizacja #06

Na początek usuwamy ether5 z bridge:

```
[admin@MikroTik] > interface bridge port remove [ find interface=ether5 ]
```

Profile APN private, public i static mamy już dodane w poprzednich scenariuszach. Ten trzeci musimy zmodyfikować. Należy wskazać interfejs passthrough. Następnie na interfejsie lte1 dodajemy 3 w/w profile.

```
[admin@MikroTik] > interface lte apn set passthrough-interface=ether5 [ find name=static ]  
[admin@MikroTik] > interface lte set apn-profiles=public,private,static lte1
```



Koniec

No chyba, że jednak jakieś pytania jeszcze są ;-)