Schemat komunikacji z oddziałami RPWiK Tychy S. A.
IPSec – AES 256

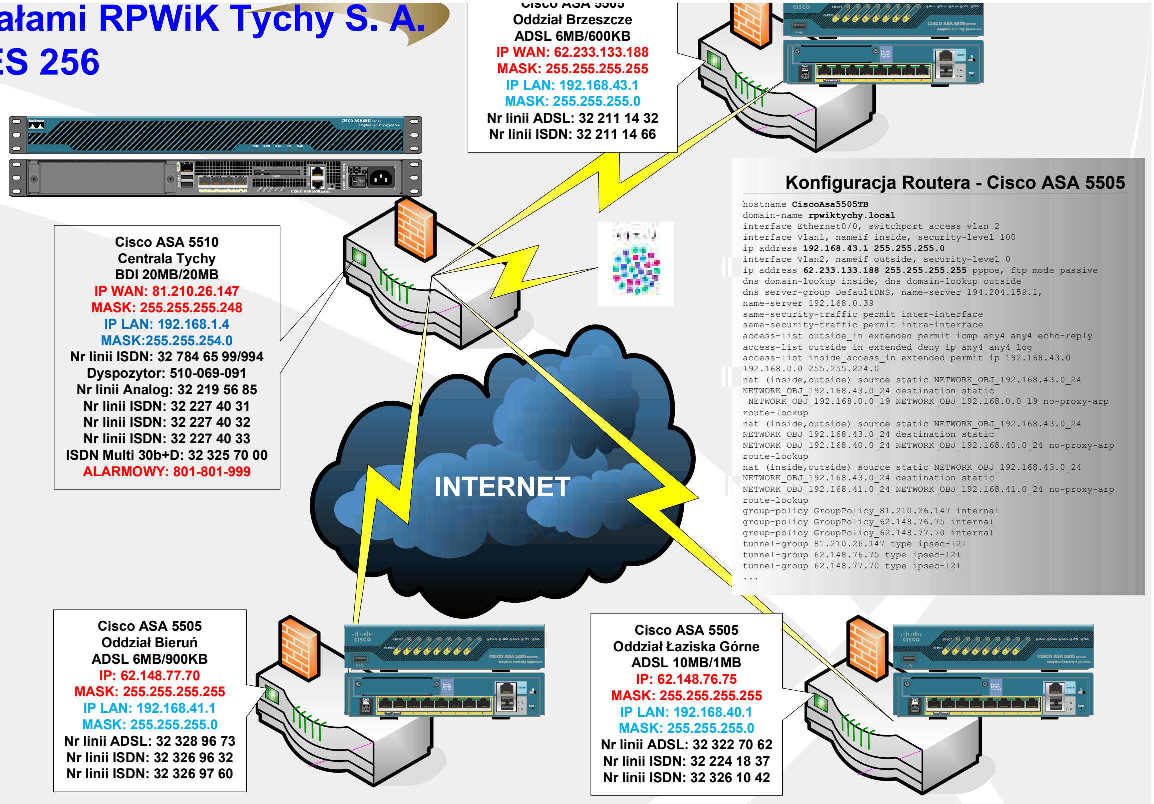
Konfiguracja Routera - Cisco ASA 5510 Firewall

```
hostname CiscoAsa5510TY
domain-name rpwiktychy.local

interface Ethernet0/0                    nameif outside, security-level 0, ip address 81.210.26.147 255.255.255.248
interface Ethernet0/1                    nameif inside, security-level 100, ip address 192.168.1.4 255.255.224.0
interface Management0/0                  nameif management security-level 100 ip address 192.168.10.1 255.255.255.0

ftp mode passive, clock timezone CEST 1, dns domain-lookup outside, dns domain-lookup inside
dns server-group DefaultDNS - name-server 192.168.0.39, name-server 194.204.159.1
same-security-traffic permit inter-interface, same-security-traffic permit intra-interface

object network INTERNET subnet 0.0.0.0 0.0.0.0
object network NETWORK_OBJ_192.168.0.0_19, subnet 192.168.0.0 255.255.224.0
object network NETWORK_OBJ_192.168.41.0_24, subnet 192.168.41.0 255.255.255.0
object network NETWORK_OBJ_192.168.40.0_24, subnet 192.168.40.0 255.255.255.0
object network NETWORK_OBJ_192.168.43.0_24, subnet 192.168.43.0 255.255.255.0
object-group service DM_INLINE_TCP_1 tcp, port-object eq www, port-object eq https

access-list outside_in extended permit icmp any any echo-reply
access-list outside_in extended deny ip any any log
access-list inside_access_in extended permit ip 192.168.0.0 255.255.224.0 192.168.40.0 255.255.255.0
access-list inside_access_in extended permit ip 192.168.0.0 255.255.224.0 192.168.41.0 255.255.255.0
access-list inside_access_in extended permit ip 192.168.0.0 255.255.224.0 192.168.43.0 255.255.255.0
access-list outside_cryptomap extended permit ip 192.168.0.0 255.255.224.0 192.168.41.0 255.255.255.0
access-list outside_cryptomap_1 extended permit ip 192.168.0.0 255.255.224.0 192.168.40.0 255.255.255.0
access-list outside_cryptomap_3 extended permit ip 192.168.0.0 255.255.224.0 192.168.43.0 255.255.255.0

icmp unreachable rate-limit 1 burst-size 1
icmp deny any echo outside
icmp permit any echo inside
arp timeout 14400
nat (inside,outside) source static NETWORK_OBJ_192.168.0.0_19

NETWORK_OBJ_192.168.0.0_19 destination static NETWORK_OBJ_192.168.41.0_24 NETWORK_OBJ_192.168.41.0_24 no-proxy-arp route-lookup
nat (inside,outside) source static NETWORK_OBJ_192.168.0.0_19 NETWORK_OBJ_192.168.0.0_19 destination static
NETWORK_OBJ_192.168.43.0_24 NETWORK_OBJ_192.168.43.0_24 no-proxy-arp route-lookup nat (inside,outside) source static
NETWORK_OBJ_192.168.0.0_19 NETWORK_OBJ_192.168.0.0_19 destination static NETWORK_OBJ_192.168.40.0_24
NETWORK_OBJ_192.168.40.0_24 no-proxy-arp route-lookup

object network INTERNET, nat (inside,outside) dynamic interface
access-group outside_in in interface outside
access-group inside_access_in in interface inside
route outside 0.0.0.0 0.0.0.0 81.210.26.145 1
aaa-server rpwiktychy.local protocol ldap
aaa-server rpwiktychy.local (inside) host 192.168.0.39
http server enable

crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto map outside_map 1 match address outside_cryptomap
crypto map outside_map 1 set pfs
crypto map outside_map 1 set peer 62.148.77.70
crypto map outside_map 1 set ikev1 transform-set ESP-AES-256-SHA
crypto map outside_map 1 set ikev2 ipsec-proposal AES256
crypto map outside_map 2 match address outside_cryptomap_1
crypto map outside_map 2 set pfs
crypto map outside_map 2 set peer 62.148.76.75
crypto map outside_map 2 set ikev1 transform-set ESP-AES-256-SHA
crypto map outside_map 2 set ikev2 ipsec-proposal AES256
crypto map outside_map 4 match address outside_cryptomap_3
crypto map outside_map 4 set pfs
crypto map outside_map 4 set peer 62.233.133.188
crypto map outside_map 4 set ikev1 transform-set ESP-AES-256-SHA
crypto map outside_map 4 set ikev2 ipsec-proposal AES256
crypto map outside_map interface outside

group-policy GroupPolicy_62.233.133.188 internal
group-policy GroupPolicy_62.148.76.75 internal
group-policy GroupPolicy_62.148.77.70 internal

tunnel-group 62.148.76.75 type ipsec-l2l
tunnel-group 62.233.133.188 type ipsec-l2l
...
```

Legenda

Elementy komunikacji z oddziałami RPWiK Tychy S. A.

Symbol	Liczba	Opis
⚡	4	Łącze komunikacyjne BDI oraz ADSL Netia



Cisco ASA 5505
Oddział Brzeszcze
ADSL 6MB/600KB
IP WAN: 62.233.133.188
MASK: 255.255.255.255
IP LAN: 192.168.43.1
MASK: 255.255.255.0
Nr linii ADSL: 32 211 14 32
Nr linii ISDN: 32 211 14 66

Cisco ASA 5510
Centrala Tychy
BDI 20MB/20MB
IP WAN: 81.210.26.147
MASK: 255.255.255.248
IP LAN: 192.168.1.4
MASK:255.255.254.0
Nr linii ISDN: 32 784 65 99/994
Dyspozytor: 510-069-091
Nr linii Analog: 32 219 56 85
Nr linii ISDN: 32 227 40 31
Nr linii ISDN: 32 227 40 32
Nr linii ISDN: 32 227 40 33
ISDN Multi 30b+D: 32 325 70 00
ALARMOWY: 801-801-999

Konfiguracja Routera - Cisco ASA 5505

```
hostname CiscoAsa5505TB
domain-name rpwiktychy.local
interface Ethernet0/0, switchport access vlan 2
interface Vlan1, nameif inside, security-level 100
ip address 192.168.43.1 255.255.255.0
interface Vlan2, nameif outside, security-level 0
ip address 62.233.133.188 255.255.255.255 pppoe, ftp mode passive
dns domain-lookup inside, dns domain-lookup outside
dns server-group DefaultDNS, name-server 194.204.159.1,
name-server 192.168.0.39
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
access-list outside_in extended permit icmp any4 any4 echo-reply
access-list outside_in extended deny ip any4 any4 log
access-list inside_access_in extended permit ip 192.168.43.0
192.168.0.0 255.255.224.0
nat (inside,outside) source static NETWORK_OBJ_192.168.43.0_24
NETWORK_OBJ_192.168.43.0_24 destination static
 NETWORK_OBJ_192.168.0.0_19 NETWORK_OBJ_192.168.0.0_19 no-proxy-arp
route-lookup
nat (inside,outside) source static NETWORK_OBJ_192.168.43.0_24
NETWORK_OBJ_192.168.43.0_24 destination static
NETWORK_OBJ_192.168.40.0_24 NETWORK_OBJ_192.168.40.0_24 no-proxy-arp
route-lookup
nat (inside,outside) source static NETWORK_OBJ_192.168.43.0_24
NETWORK_OBJ_192.168.43.0_24 destination static
NETWORK_OBJ_192.168.41.0_24 NETWORK_OBJ_192.168.41.0_24 no-proxy-arp
route-lookup
group-policy GroupPolicy_81.210.26.147 internal
group-policy GroupPolicy_62.148.76.75 internal
group-policy GroupPolicy_62.148.77.70 internal
tunnel-group 81.210.26.147 type ipsec-l2l
tunnel-group 62.148.76.75 type ipsec-l2l
tunnel-group 62.148.77.70 type ipsec-l2l
...
```

Cisco ASA 5505
Oddział Bieruń
ADSL 6MB/900KB
IP: 62.148.77.70
MASK: 255.255.255.255
IP LAN: 192.168.41.1
MASK: 255.255.255.0
Nr linii ADSL: 32 328 96 73
Nr linii ISDN: 32 326 96 32
Nr linii ISDN: 32 326 97 60

Cisco ASA 5505
Oddział Łaziska Górne
ADSL 10MB/1MB
IP: 62.148.76.75
MASK: 255.255.255.255
IP LAN: 192.168.40.1
MASK: 255.255.255.0
Nr linii ADSL: 32 322 70 62
Nr linii ISDN: 32 224 18 37
Nr linii ISDN: 32 326 10 42

Konfiguracja Routera - Cisco ASA 5505

```
hostname CiscoAsa5505TO
domain-name rpwiktychy.local
interface Ethernet0/0, switchport access vlan 2
interface Vlan1, nameif inside, security-level 100
ip address 192.168.41.1 255.255.255.0
interface Vlan2, nameif outside, security-level 0
ip address 62.148.77.70 255.255.255.255 pppoe. ftp mode passive
dns domain-lookup inside, dns domain-lookup outside
dns server-group DefaultDNS, name-server 194.204.159.1,name-server 192.168.0.39
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
access-list outside_in extended permit icmp any any echo-reply
access-list outside_in extended deny ip any any log
access-list inside_access_in extended permit ip 192.168.41.0
nat (inside,outside) source static NETWORK_OBJ_192.168.41.0_24
NETWORK_OBJ_192.168.41.0_24 destination static
NETWORK_OBJ_192.168.0.0_19 NETWORK_OBJ_192.168.0.0_19 no-proxy-arp route-lookup
nat (inside,outside) source static NETWORK_OBJ_192.168.41.0_24
NETWORK_OBJ_192.168.41.0_24 destination static NETWORK_OBJ_192.168.40.0_24
NETWORK_OBJ_192.168.41.0_24 destination static NETWORK_OBJ_192.168.43.0_24
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto map outside_map 1 match address outside_cryptomap
crypto map outside_map 1 set pfs
crypto map outside_map 1 set peer 81.210.26.147
```

Konfiguracja Routera - Cisco ASA 5505

```
hostname CiscoAsa5505TL
domain-name rpwiktychy.local
interface Ethernet0/0, switchport access vlan 2
interface Vlan1, nameif inside, security-level 100
ip address 192.168.40.1 255.255.255.0
interface Vlan2, nameif outside, security-level 0
ip address 62.148.76.75 255.255.255.255 pppoe, ftp mode passive
clock timezone CEST 1
dns domain-lookup inside, dns domain-lookup outside,
dns server-group DefaultDNS, name-server 192.168.0.39, 194.204.159.1
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
object network Gatway_Outside, host 81.210.100.137
object-group protocol TCPUDP, protocol-object udp, protocol-object tcp
access-list outside_in extended permit icmp any any echo-reply
access-list outside_in extended deny ip any any
access-list outside_cryptomap extended permit
ip 192.168.40.0 255.255.255.0 192.168.0.0 255.255.224.0
access-list inside_access_in extended permit
ip 192.168.40.0 255.255.255.0 192.168.0.0 255.255.224.0
logging enable, logging asdm informational, mtu inside 1500, mtu outside 1500
icmp unreachable rate-limit 1 burst-size 1
icmp permit any echo inside
asdm image disk0:/asdm-647.bin
arp timeout 14400
nat (inside,outside) source static NETWORK_OBJ_192.168.40.0_24
```