Juniper SRX – Draytek Vigor IPSec VPN

Feladat: összelőni IPSEC VPN-t Juniper SRX (Junos-t futtató) eszközzel. Miért is? Mert elképzelhető (sőt, életképes) egy olyan környezet, ahol van egy központi SRX, és sok-sok telephely, melyek célszerűen olcsó Draytek Vigor routereken keresztül csatlakoznak be.

Fenti környezet működőképes, de abszolút nem támogatott ☺ Talán emiatt van, hogy nekem csak 3DES titkosítású VPN-t sikerült összehoznom (na jó, a DES-t nem próbáltam). De az AES sajna nekem nem ment, a tunnel összeállt, de nem ment benne egy bit se át. Nem térek ki olyan apróságokra, hogy értelemszerűen a pre-shared-key egyezzen mindkét oldalon pl.

Nem is nagyon részletezem, a konfig:

SRX oldal:

[edit security ike]

```
proposal pre-g2-3des-sha1 {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 28800;
}

policy ike_DRAYTEKVPN {
    mode aggressive;
    proposals pre-g2-3des-sha1;
    pre-shared-key ascii-text #####"; ## SECRET-DATA
}

gateway gw_DRAYTEKVPN {
    ike-policy ike_DRAYTEKVON;
    dynamic hostname DRAYTEKVPN;
    dead-peer-detection interval 30;
    nat-keepalive 30;
    external-interface fe-0/0/0;
}
```

[edit security ipsec]

```
proposal g2-esp-3des-md5 {
    protocol esp;
    authentication-algorithm hmac-md5-96;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 3600;
}

policy ipsec_DRAYTEKVPN {
    perfect-forward-secrecy {
        keys group2;
    }
    proposals g2-esp-3des-md5;
}

vpn DRAYTEKVPN {
    bind-interface st0.2;
    vpn-monitor {
        optimized;
    }
    ike {
```

```
        gateway gw_DRAYTEKVPN;
        ipsec-policy ipsec_DRAYTEKVPN;
    }
    establish-tunnels immediately;
}
```

[edit interfaces st0]

```
unit 2 {
    family inet;
}
```

```
[edit security zones security-zone DRAYTEK-VPN]

address-book {
        address site_DRAYTEKVPN 192.168.75.0/24;
    address HQ_2 172.21.50.0/24;
}
interfaces {
    st0.2;
}
```

[edit security policies from-zone DRAYTEK-VPN to-zone trust]

```
policy SITE_DRAYTEKVPN {
    match {
        source-address site_DRAYTEKVPN;
        destination-address HQ;
        application any;
    }
    then {
        permit;
    }
}
```

[edit security policies from-zone trust to-zone DRAYTEK-VPN]

```
policy SITE_DRAYTEKVPN {
    match {
        source-address HQ;
        destination-address site_DRAYTEKVPN;
        application any;
    }
    then {
        permit;
    }
}
```

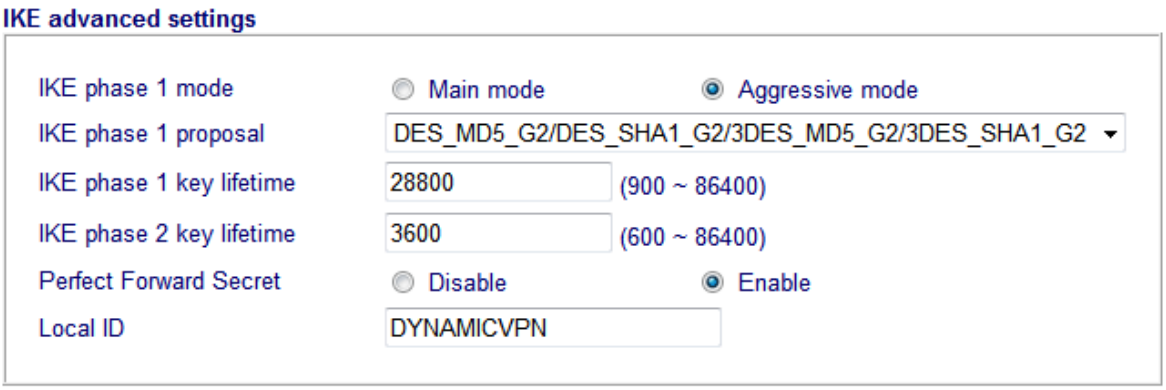
[edit security zones security-zone untrust]

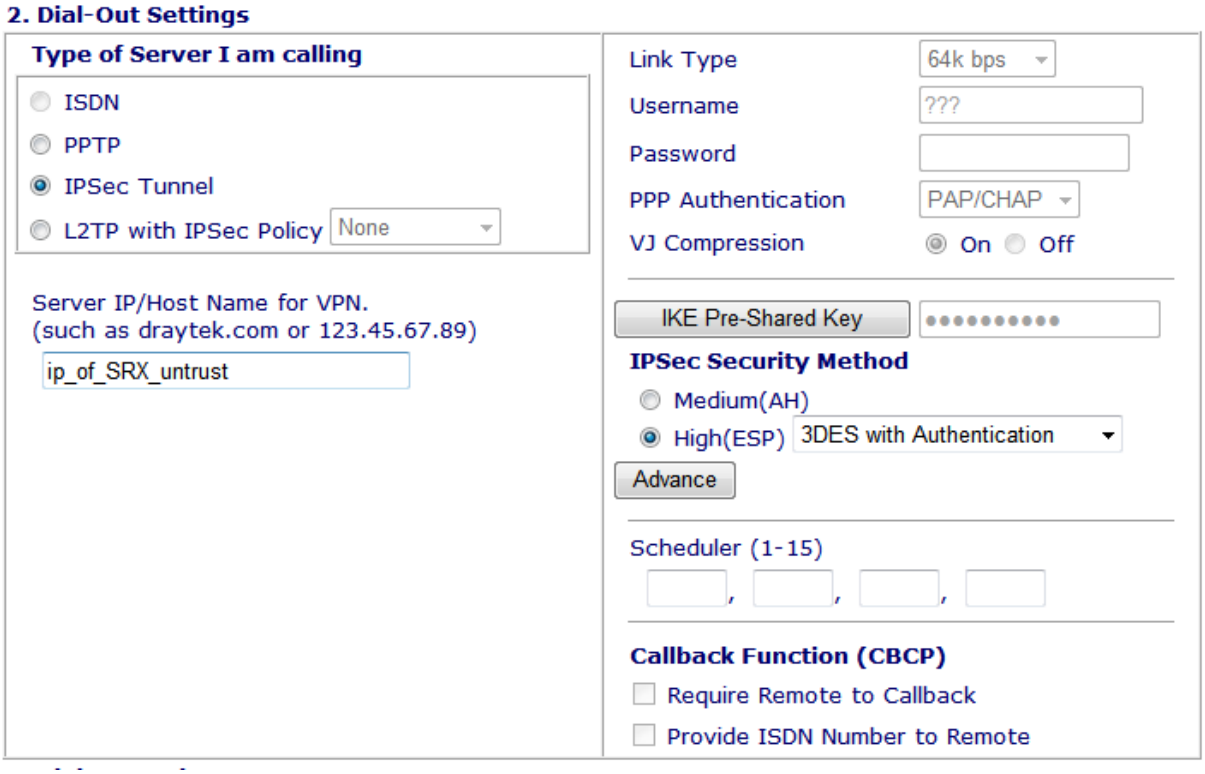
```
screen untrust-screen;
interfaces {
    fe-0/0/0.0 {
        host-inbound-traffic {
            system-services {
                ping;
                https;
                ssh;
                ike;
            }
        }
    }
}
```

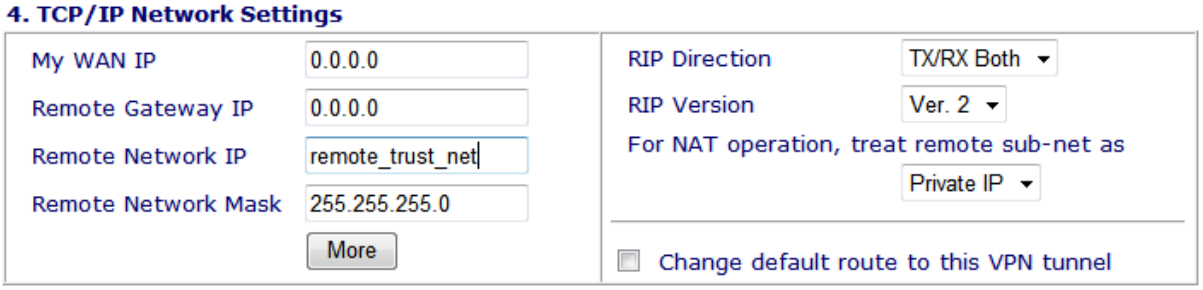
[edit routing-options]

```
static {
    route 192.168.75.0/24 next-hop st0.2;
}
```

Draytek oldal:







Kérdés, kérés esetén: pingtomi@pingtomi.hu