

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 értelemeszerűen a pre-shared-key egyezzen mindkét oldalon pl.

Nem is nagyon részletezem, a konfiguráció:

SRX oldal:

[edit security ike]

```
proposal pre-g2-3des-shal {
  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-shal;
  pre-shared-key ascii-text #####; ## SECRET-DATA
}

gateway gw_DRAYTEKVPN {
  ike-policy ike_DRAYTEKVPN;
  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:

IKE advanced settings

IKE phase 1 mode	<input type="radio"/> Main mode	<input checked="" type="radio"/> Aggressive mode
IKE phase 1 proposal	DES_MD5_G2/DES_SHA1_G2/3DES_MD5_G2/3DES_SHA1_G2 ▾	
IKE phase 1 key lifetime	<input type="text" value="28800"/>	(900 ~ 86400)
IKE phase 2 key lifetime	<input type="text" value="3600"/>	(600 ~ 86400)
Perfect Forward Secret	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable
Local ID	<input type="text" value="DYNAMICVPN"/>	

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> ISDN <input type="radio"/> PPTP <input checked="" type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy <input type="text" value="None"/>	Link Type <input type="text" value="64k bps"/> Username <input type="text" value="???"/> Password <input type="text"/> PPP Authentication <input type="text" value="PAP/CHAP"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <input type="text" value="ip_of_SRX_untrust"/>	<input type="text" value="IKE Pre-Shared Key"/> <input type="text" value="....."/> IPsec Security Method <input type="radio"/> Medium(AH) <input checked="" type="radio"/> High(ESP) <input type="text" value="3DES with Authentication"/> <input type="button" value="Advance"/>
	Scheduler (1-15) <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>
	Callback Function (CBCP) <input type="checkbox"/> Require Remote to Callback <input type="checkbox"/> Provide ISDN Number to Remote

4. TCP/IP Network Settings

My WAN IP <input type="text" value="0.0.0.0"/>	RIP Direction <input type="text" value="TX/RX Both"/>
Remote Gateway IP <input type="text" value="0.0.0.0"/>	RIP Version <input type="text" value="Ver. 2"/>
Remote Network IP <input type="text" value="remote_trust_net"/>	For NAT operation, treat remote sub-net as <input type="text" value="Private IP"/>
Remote Network Mask <input type="text" value="255.255.255.0"/> <input type="button" value="More"/>	<input type="checkbox"/> Change default route to this VPN tunnel

(c) 2011. pingtomi

Kérdés, kérés esetén: pingtomi@pingtomi.hu