Poszt-kvantum kriptográfia megvalósítása hálózati és alkalmazás oldalról

NMHH-EIVOK szakmai-tudományos konferencia
2026. április 23.

Poór Gergely
Rendszermérnök
https://relnet.hu

GYÁRTÓINK, AMELYEKET KÉPVISELÜNK

Stratégiai gyártóink

EXTRAHOP
HEQA SECURITY
ManageEngine
PENTERA
STORMSHIELD
ZTE

Kiemelt gyártóink

algosec
censys
exabeam
GARLAND TECHNOLOGY See every bit, byte, and packet
Greenbone
Progress Flowmon
Progress Kemp
SecuPi
SSH.COM
wallix
I4P

Gyártóink

Acronis
allot See. Control. Secure.
CTS CONNECTION TECHNOLOGY SYSTEMS
CYREBRO
Extreme networks
FORTINET
HPE
HPE JUNIPER networking
Microsemi a MICROCHIP company
netwrix
PacketLight NETWORKS
PROFITAP
PROGET
radware
STARVIEW TECHNOLOGIES
TELTONIKA
Tenda
XM Cyber

Bemutatkozás: RelNet = Reliable Networks

- 2004-ben alakult VAD (Value Added Distributor)
- ISO 9001:2015 és ISO 14001:2015 szerinti működés
- 32 gyártó megoldását kínáljuk
- **„Szakmai műhely vagyunk”** – ~50 esemény /év
  - tréningek,
  - előadások,
  - workshopok,
  - konferenciák
  - eLearning program
- **Szolgáltatásaink**
  - RelNet Silver és RelNet Gold támogatások
  - szakértői tanácsadás
  - demoeszköz kölcsönzés + POC
  - helpdesken keresztül 7/24 magyar nyelvű support felár nélkül (már 1 licenc vásárlásától)

Bemutatkozás

- Poór Gergely (27)
  Rendszermérnök

  MTCRE, JNCIS-SP, JNCIS-ENT
  SSH Certified, HEQA Certified

  Szakterület:
  Linux/BSD, PQC, Hálózatbiztonság,
  Erősáramú és strukturált kábelezési installációk

  Hobbik:
  MikroTik, FreeBSD, beágyazott rendszerek

A kvantum-fenyegetés

- Kvantumszámítógépen futtatható kvantumalgoritmusok
- Shor algoritmusa
  - **Az aszimmetrikus kulcscsere sérülékenysége**
- Grover algoritmusa
  - **Szimmetrikus** kriptografikus algoritmusok feltörésének megkönnyítése (brute-force)
  - **Megoldás: AES-256 és SHA-512 használata**

- „Harvest now, decrypt later” jelenség

Jogi szabályozások (a teljesség igénye nélkül)

- 2024/LXIX(69) tv. Magyarország kiberbiztonságáról
  - kritikus/állami szektorok: energetika, közigazgatás, digitális szolgáltatók, pénzintézetek, DNS, hírközlés, TLD szolgáltató stb.
- 2024/2853 EU termékfelelősségi irányelv
  - kiberbiztonsági előírásoknak meg nem felelés, mint hiba
- 2024/2393 EU ajánlás (PQC-re átállás)
- 2023/20 EU JOIN rendelet (kvantumtechnológia kockázat értékelés)
- 2022/2555 EU irányelv (NIS2)
- 2022/2554 EU rendelet (DORA)

A megoldás aszimmetrikus titkosításra

- QKD: kvantum-kulcselosztás
  - A fizika törvényein alapuló biztonság
    - BB84, E91, SKIP, ETSI GS QKD 014

- PQC: poszt-kvantum kriptográfia
  - Matematikai biztonság
    - FIPS 203, 204, 205 (ML-KEM, ML-DSA, SLH-DSA)

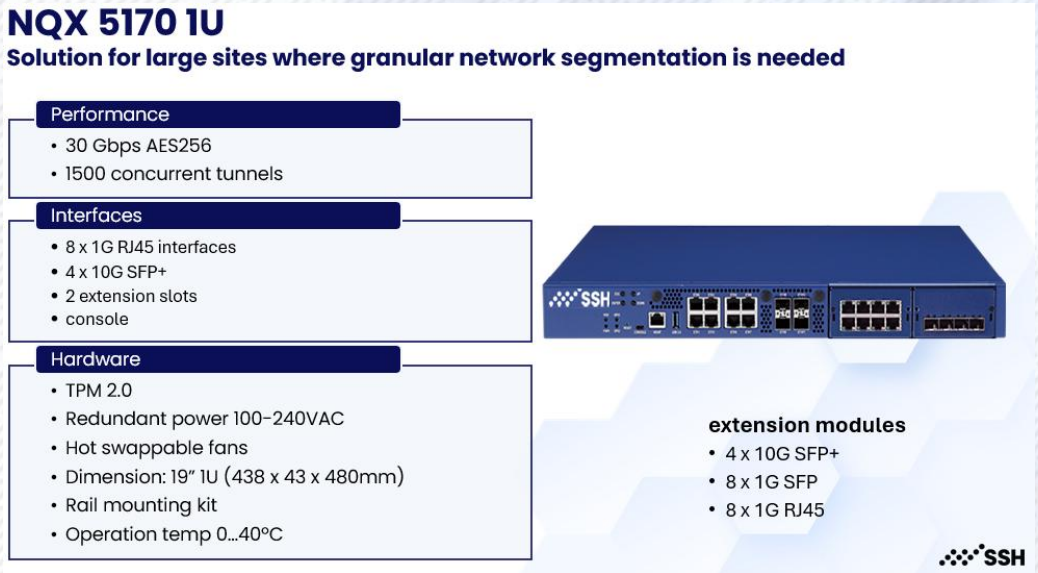
QKD

- Kulcsgenerálás
  - Fotonok manipulációja a kvantumfizika törvényei alapján
- MITM érzékelése
- DWDM/optika/műhold
- HEQA Sceptre termékcsalád
  - BB84 csali állapottal (decoy-state)

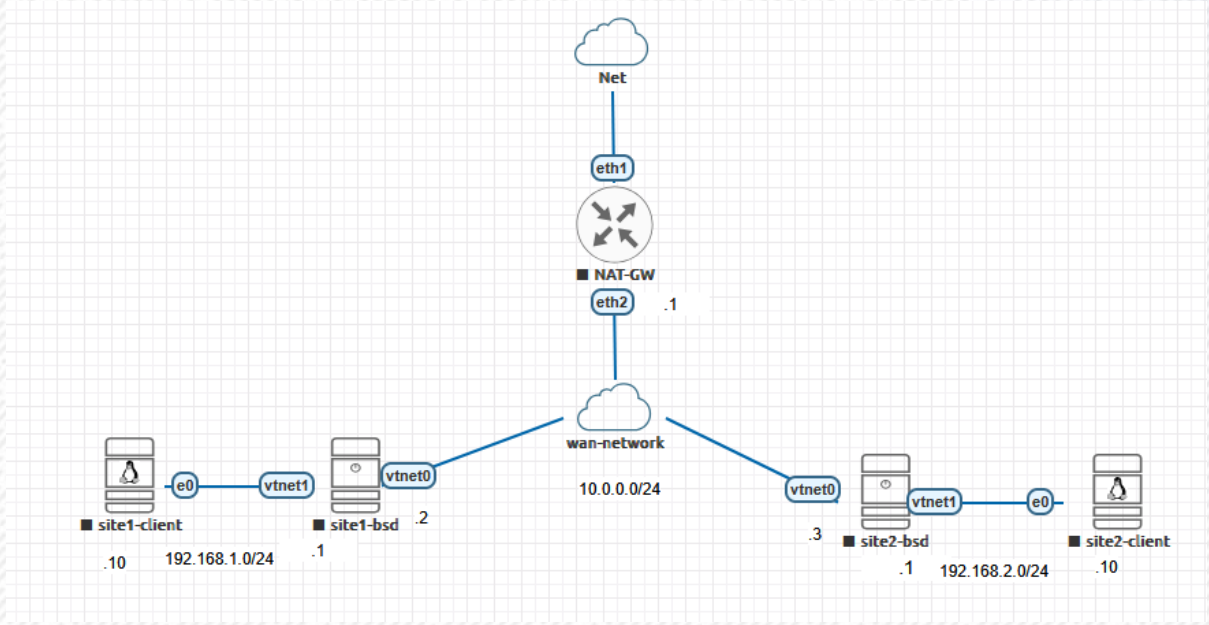
Nagyvállalati PQC megoldás – SSH NQX

Kvantumbiztos hálózati titkosító platform

- Kvantumbiztos IPSec VPN akár dinamikusan is
  - L2, L3
- Felhasználóbarát webes felület
- Verziókezelt házirendek
- Központi felügyeleti rendszer
- HA (magas rendelkezésreállás)
- L2-L4 tűzfal, router funkcionalitás
- PAM integráció (SSH PrivX)
- RFC8784 (PPK) támogatás
- Könnyű életciklus-kezelés
- **Európai, NATO által jóváhagyott** gyártó
  - Az SSHv2 protokoll megalkotója
- **Nagyvállalati szintű támogatás**



Nyílt forráskódú PQC megoldások: IPSec VPN




```
root@site1-bsd:~ # swanctl --list-sas
site2site: #1, ESTABLISHED, IKEv2, 928e1b816c566952_i* 16b7820121e44798_r
  local  '10.0.0.2' @ 10.0.0.2[4500]
  remote '10.0.0.3' @ 10.0.0.3[4500]
  AES_CBC-256/HMAC_SHA2_384_192/PRF_HMAC_SHA2_384/ECP_384/KE1_ML_KEM_768
  established 257s ago, rekeying in 12760s
  net-net: #2, reqid 1, INSTALLED, TUNNEL, ESP:AES_GCM_16-256
    installed 257s ago, rekeying in 3056s, expires in 3703s
    in  c692e079,     816 bytes,    10 packets,     10s ago
    out cc15e722,    1356 bytes,    10 packets,     10s ago
    local  192.168.1.0/24
    remote 192.168.2.0/24
root@site1-bsd:~ #
```

Minimum követelmény: strongSwan 6.0 vagy újabb

```
root@site1-bsd:~ # cat /usr/local/etc/swanctl/swanctl.conf
connections {
   site2site {
      version = 2
      proposals = aes256-aes128-sha384-sha256-ecp384-x25519-
ke1_mlkem768-ke1_mlkem1024-ke1_mlkem512-ke1_none
      remote_addrs  = 10.0.0.3
      local_addrs = 10.0.0.2
      local {
         auth = psk
         id = 10.0.0.2
      }
     remote {
         auth = psk
         id = 10.0.0.3
      }
      children {
         net-net {
            remote_ts  = 192.168.2.0/24
            local_ts = 192.168.1.0/24
            esp_proposals = aes256gcm128-aes128gcm128-ecp384-x25519-
ke1_mlkem768-ke1_mlkem1024-ke1_mlkem512-ke1_none
            start_action = trap
            dpd_action = restart
         }
      }
   }
}
secrets {
      ike-psk {
            id-1 = 10.0.0.2
            id-2 = 10.0.0.3
            secret = supersecret
      }
}
```

Nyílt forráskódú PQC megoldások: SSH

- Követelmények: OpenSSH 9.0 vagy újabb
  - OpenSSH 10.2 és felette:
    - Alapból poszt-kvantum algoritmusokat használ
    - Figyelmeztet, ha a másik fél nem ismeri ezeket
- Bármilyen TCP/UDP protokoll átvihető rajta, ezáltal kvantumbiztossá tehető!

```
openbsd# ssh admin@192.168.56.254
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
admin@192.168.56.254's password:
```

Nyílt forráskódú PQC megoldások: SSH

/etc/ssh/sshd_config

(...)

KexAlgorithms mlkem768x25519-sha256,sntrup761x25519-sha512,sntrup761x25519-sha512@openssh.com

- Támogatott PQC algoritmusok és minimum OpenSSH verzió: sntrup761x25519(9.0), mlkem768x25519(9.9)

- A fenti beállítással kvantumbiztossá tehetőek szervereink:

```
[gpoor@geri-rhel9-vm ~]$ ssh gpoor@192.168.56.10
Unable to negotiate with 192.168.56.10 port 22: no matching key exchange method found. Their offer: mlkem768x25519-sha256,
sntrup761x25519-sha512,sntrup761x25519-sha512@openssh.com,ext-info-s,kex-strict-s-v00@openssh.com
[gpoor@geri-rhel9-vm ~]$ ssh -V
OpenSSH_8.7p1, OpenSSL 3.2.2 4 Jun 2024
[gpoor@geri-rhel9-vm ~]$
```

Nyílt forráskódú PQC megoldások: HTTPS

- Szerveroldali követelmények:
  - OpenSSL 3.5 (vagy OpenSSL 3.2)
  - nginx
- Tesztelje Ön is!
  https://pq.relnet.hu
- A vonatkozó konfigurációs direktíva:

```
server{
        listen 443 ssl;
        ssl_protocols TLSv1.2 TLSv1.3;
        ssl_ecdh_curve X25519MLKEM768:X25519;
        (...)
}
```

Saját publikációm a témában

- **Implementing a Quantum-Safe Website on FreeBSD**
  - FreeBSD Journal 2025 Q3
- Megvalósítás lépésről-lépésre
- Az OpenSSL 3.5 óta egyszerűbb!

Table of Contents

(Now available in both HTML and PDF)


```
[oqsprovider_sect]
activate = 1
module = /usr/local/lib/ossl-modules/oqsprovider.so
…
```

Now we will compile nginx.

```
# cd /usr/ports/www/nginx
```

I will export some environmental variables to make nginx link against the newly installed OpenSSL 3.4.1

```
# export OPENSSL_BASE=/usr/local
# export OPENSSL_LIBS=”-L/usr/local/lib”
# export OPENSSL_CFLAGS=”-I/usr/local/include”
```

Then we will configure nginx to make sure that “HTTP_SSL” is supported (it should be enabled by default, but it’s always better to double-check). I will not adjust any other settings.

```
# make config
```

„Elvihető gondolatok”

- **A PQC és QKD nem zárja ki egymást**
  PQC + QKD = Defense in Depth
- **A PQC tisztán szakértői munkával is megvalósítható**
- **A fizetős (nagyvállalati) és az ingyenes megoldások jól kiegészítik egymást**

+1

A cél, hogy a macska mindig életben legyen!

Köszönöm a figyelmet!

Kérdések?

Poór Gergely

Rendszermérnök

https://relnet.hu