

## Számonkérés anyaga

Dr. Lencse Gábor: Hálózatok biztonsága

1-81, 83-90, 99-111, 119-150. oldal

<http://en.wikipedia.org/wiki/RAID>

Szintek: 0,1,4,5,6,10(1+0)

Dr. Berta István Zsolt: Nagy e-szignó könyv

1.2, 1.3, 2.3, 2.4, 2.6.1 (jellemzői, alapok), 2.7, 3.1, 3.4, 3.6.8, 3.6.9, 4.1.1, 4.1.5.1, 5.1, 5.2.1, 9.

Figyelem! A megadott pontok alfejezetei is kellenek!

[http://en.wikipedia.org/wiki/Sender\\_Policy\\_Framework](http://en.wikipedia.org/wiki/Sender_Policy_Framework)

Működése, egy SPF rekord összeállítása, értelmezése.

[http://en.wikipedia.org/wiki/DomainKeys\\_Identified\\_Mail](http://en.wikipedia.org/wiki/DomainKeys_Identified_Mail)

Működése.

Amavis: célja.

<http://spamassassin.apache.org/>

Működése, bayesian (tanulás alapvető működése).

<http://www.greylisting.org/>

Működése.

[http://www.cisco.com/c/en/us/td/docs/net\\_mgmt/vpn\\_solutions\\_center/2-0/ip\\_security/provisioning/guide/IPsecPG1.html](http://www.cisco.com/c/en/us/td/docs/net_mgmt/vpn_solutions_center/2-0/ip_security/provisioning/guide/IPsecPG1.html)

<https://technet.microsoft.com/en-us/library/cc779919%28v=ws.10%29.aspx>

<https://www.bestvpn.com/blog/4147/pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/>

Tunneling protocol	Firewall access	Description
PPTP	TCP port 1723	Provides data confidentiality but not data integrity or data authentication.

L2TP/IPsec	UDP port 500, UDP port 1701, UDP port 4500, and IP protocol ID 50	Uses either certificates or preshared keys for authentication. Certificate authentication is recommended.
SSTP	TCP port 443	Uses SSL to provide data confidentiality, data integrity, and data authentication.
IKEv2	UDP port 500	Supports the latest IPsec encryption algorithms to provide data confidentiality, data integrity, and data authentication.
OpenVPN	UDP port 1194, TCP port 443	Uses either certificates or preshared keys for authentication. Certificate authentication is recommended.

- Password
  - PAP
  - CHAP
  - Preshared key
- one-time pad (OTP):
  - HOTP
  - TOTP
  - OCRA
  - (Software)
- Certificate:
  - File
  - Smartcard
  - USB Token

VPN működése.

VPN fajták: Site-to-site és Remote Access VPN.

VPN protokollok.

Horváth Tamás: Vezeték nélküli hálózatok biztonsági kérdései

<https://www.tilb.sze.hu/tilb/targyak/ta83/wifisec.pdf>

5,8,18-27,30,36. diák.

[https://www.tilb.sze.hu/tilb/targyak/NGB\\_TA0028\\_1/ZH2-prezi.pdf](https://www.tilb.sze.hu/tilb/targyak/NGB_TA0028_1/ZH2-prezi.pdf)

[http://en.wikipedia.org/wiki/VLAN\\_hopping](http://en.wikipedia.org/wiki/VLAN_hopping)

<http://itsecurity.telelink.com/stp-manipulation/>

[http://en.wikipedia.org/wiki/Network\\_Access\\_Protection](http://en.wikipedia.org/wiki/Network_Access_Protection)

<https://technet.microsoft.com/en-us/magazine/ff741764.aspx>

Tűzfalak, Proxyk, IDS, IPS, WAF fogalmak, fajtáik, működésük, alkalmazásuk.

NTP, SYSLOG, RADIUS jellemzői, működésük.

VLAN hopping módszerek működése, védekezés.

STP manipulációs módszer, védekezés.

Mentés, archiválás fogalma/különbség.

Mentési típusok fajtái, működésük, visszaállítás.

UAC, NAP fogalma, működése.

Password policy beállítási lehetőségek, ajánlások.