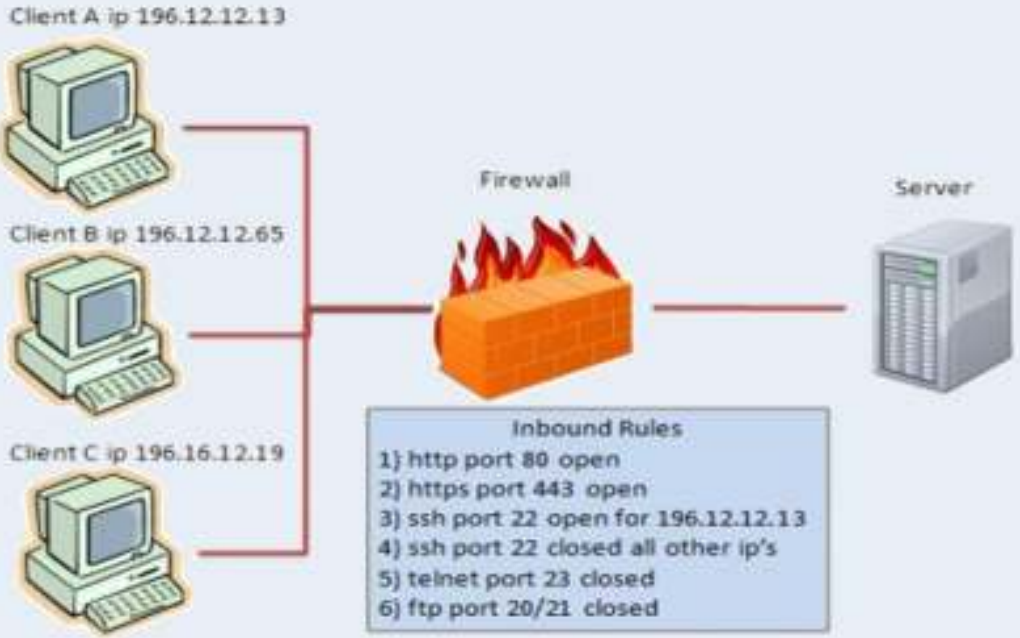
Biztonsági eszközök

- Tűzfalak
- Proxyk
- Honeypot
- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- Log szerver
- Log elemző
- Időszerver
- Hitelesítő (Authentikációs) szerver

Tűzfalak

- Access Control List (ACL)
- Firewall
- Állapotmentes (stateless)
- Állapottartó (stateful)
- Host alapú
- Hálózat alapú
- Demilitarizált zóna, DMZ, Perimeter network, Screened subnet
- Proxyk
- Kapcsolat szintű
- Alkalmazás szintű
- Web Application Firewall
- Database Access Management

Firewall, Tűzfal

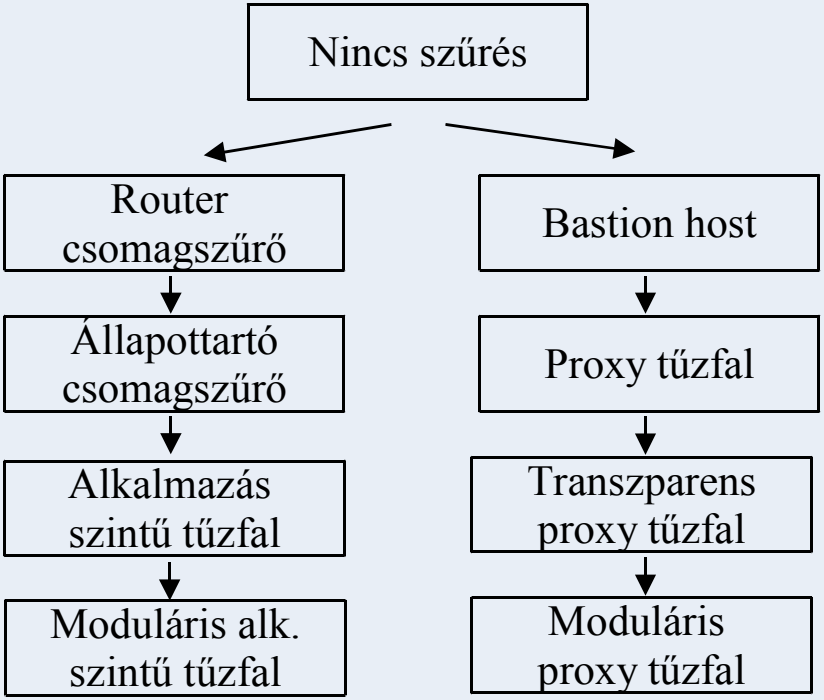


Forgalomszabályzó eszköz két, vagy több eltérő biztonsági szintű hálózat közt.

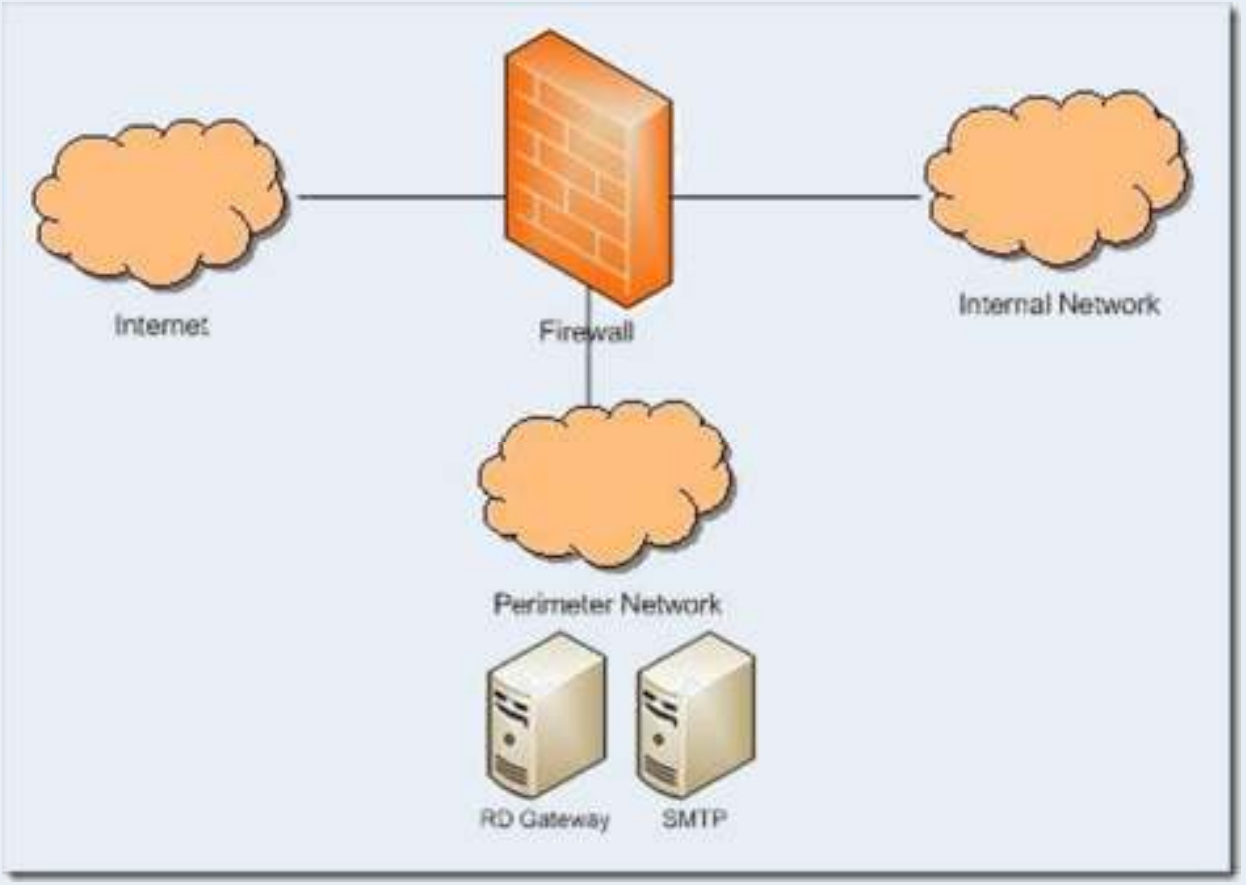
Típusok

- Állapotmentes (stateless)
- Állapottartó (stateful)
- Host alapú
- Hálózat alapú

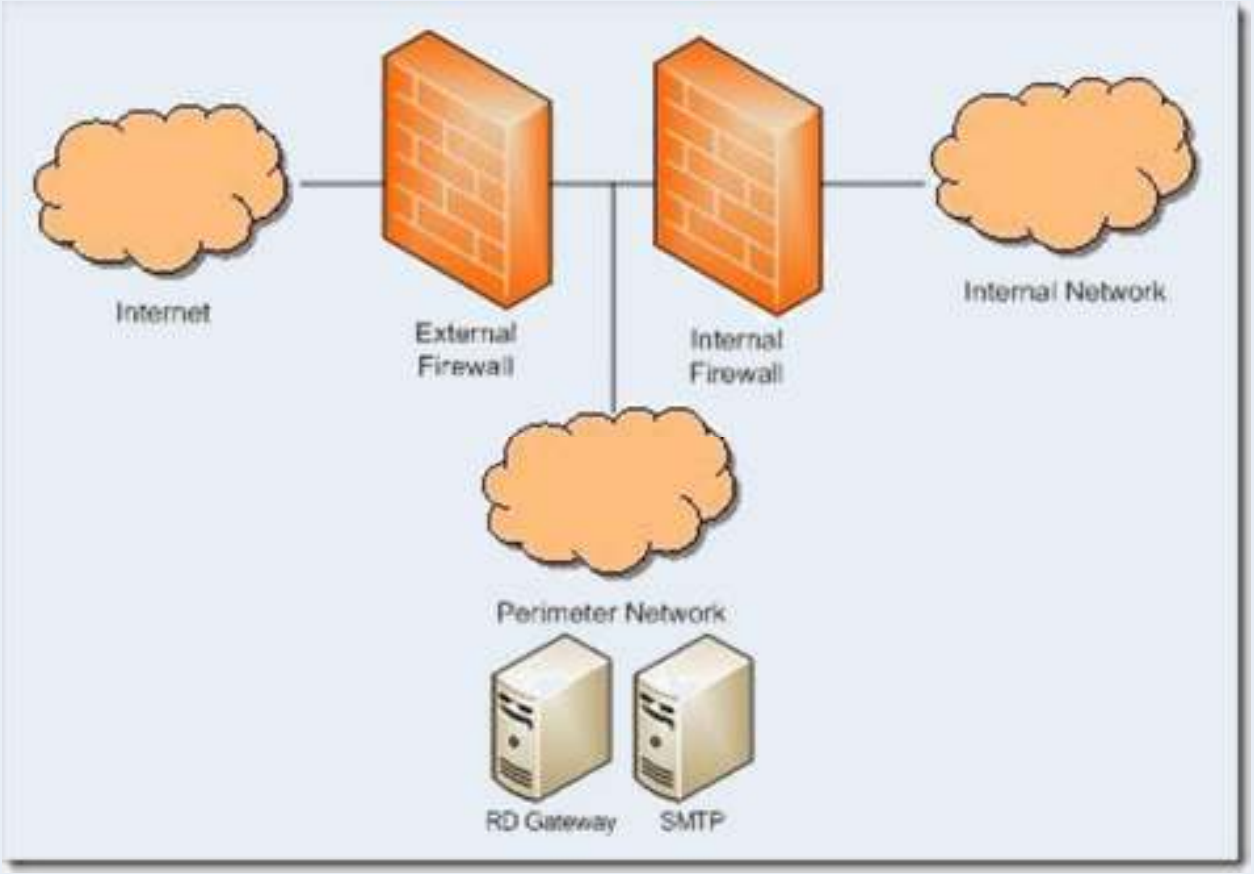
Tűzfalak fejlődése



Single Firewall DMZ



Dual Firewall DMZ



Proxy

- Kapcsolat szintű
- Alkalmazás szintű
- Reverse proxy
- Web Application Firewall (Apache, URLScan, Zero day)
- Database Access Management

Egyéb eszközök

- Honeypot
- Intrusion Detection System (IDS)
- Host
- Hálózat
- Intrusion Prevention System (IPS)
- Host
- Hálózat
- Log szerver
- Log elemző szerver
- Időszerver
- Authentikációs szerver (LDAP, RADIUS, TACACS)

Management Plane Security

- Enforce password policy
  - Use Cisco IOS login enhancements
- Implement RBAC
  - CLI views
- Deploy AAA services for central device management
- Use NTP
  - Consistent logging timestamps
  - Digital certificate validation
- Use strong authentication when required for device management
  - Example: SNMPv3
- Restrict access to management protocols
  - Use access control lists
  - Use management plane protection feature

ACL Filtering

- Block unwanted traffic or users
- Reduce the chance of DoS attacks
- Mitigate IP spoofing attacks
- Provide bandwidth control
- Classify traffic to protect other planes
  - Control access to vty (for management plane)
  - Restrict the content of routing updates (for control plane)

Layer 2 Data Plane Protection

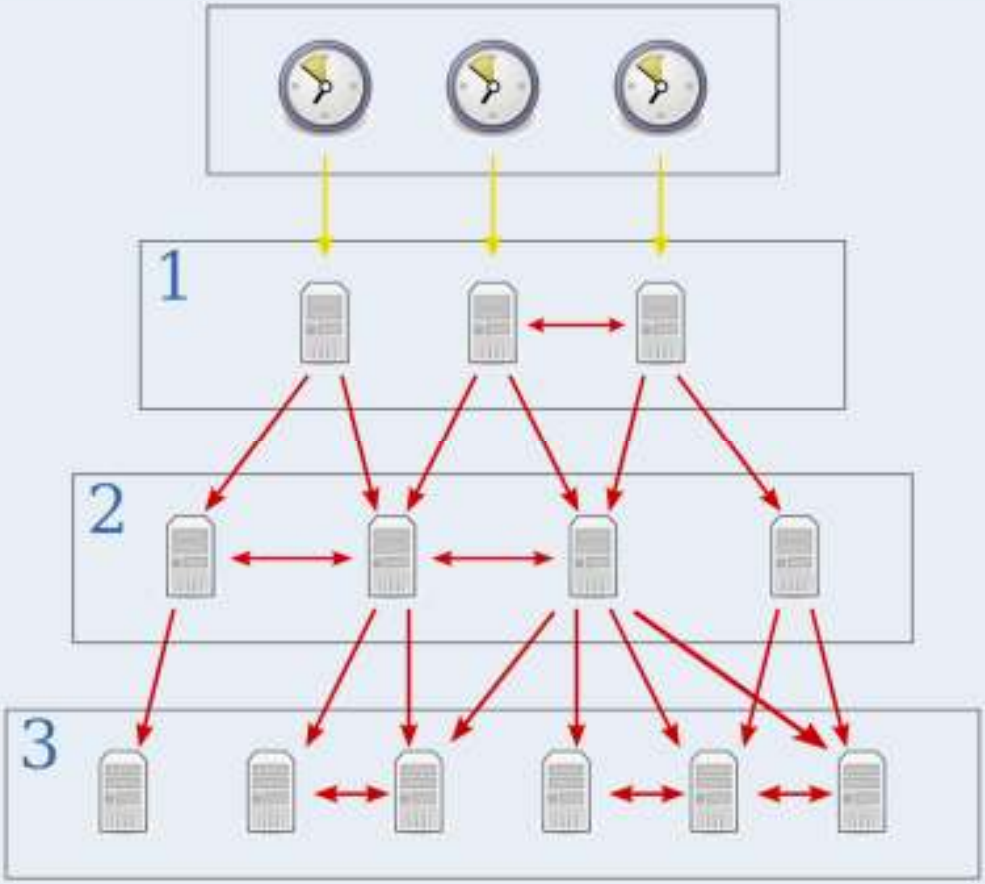
Secure Management and Reporting Guidelines

- Management guidelines
  - Keep clocks on hosts and network devices synchronized.
  - Record changes and archive configurations.
  - Enforce a password policy.
- OOB management guidelines
  - Provide the highest level of security and mitigate the risk of passing insecure management protocols over the production network.
- In-band management guidelines
  - Guidelines apply only to devices that need to be managed or monitored.
  - Use IPsec, SSH, or SSL when possible.
  - Decide whether the management channel needs to be open at all times.

Network Time Protocol

- NTP is a protocol for secure synchronization of clocks in computer systems.
- NTP uses UDP port 123.
- SNTP is a simpler, less secure version of NTP.
- You can configure your own master clock source or use a public NTP server from the Internet.
- NTPv3 is defined in RFC 1305 and supports cryptographic authentication between peers.

Network Time Protocol Stratum



AAA

- Authentication
  - Who are you?
  - "I am user student and my password validateme proves it."
- Authorization
  - What can you do? What can you access?
  - "User student can access host serverXYZ using Telnet."
- Accounting
  - What did you do? How long did you do it? How often did you do it?
  - "User student accessed host serverXYZ using Telnet for 15 minutes."

Implementing Log Messaging for Security

- Routers should be configured to send log messages to one or more of these items:
  - Console
  - Terminal lines
  - Buffered logging
  - SNMP traps
  - Syslog
- Syslog logging is an essential security policy component.

Community Strings

- Read-only community strings can get information but cannot set information in an agent.
- Read-write community strings can get and set information in an agent.
- Set access is equivalent to having the enable password for a device.

TACACS+ Overview

- Is not compatible with its predecessors TACACS and XTACACS
- Separates authentication and authorization
- Supports a large number of features
- Encrypts all communication
- Utilizes TCP port 49

RADIUS Overview

- RADIUS was developed by Livingston Enterprises.
- RADIUS proxy servers are used for scalability.
- RADIUS combines authentication and authorization as one process.
- DIAMETER is the planned replacement.
- Technologies that use RADIUS include the following:
  - Remote access (such as dialup and DSL)
  - 802.1X
  - SIP

Egyéb módszerek

- Routing protocolok
- Switching tábla telítés
- MAC Address Spoofing

Backup

- Nem elég a RAID? (Off-line!)
- Mennyit ér az adat?
- Mit, mikor, hogyan mentsünk?
- Mennyi idő szükséges a helyreállításhoz?

Backup types

Backup típus	**Mit ment**	**Archiv attr.**	**Tárhely**
Full	Mindent	Törli	Sok
Incremental	Ami Arch.	Törli	Minimális
Differential	Ami Arch.	Marad	Kevés
Daily copy	Napi módosításokat	Marad	Minimális

Restore

- A Backup stratégiától függ
- Példák