tilb
Távközlés-
Informatika
Laboratórium

IP alapú kommunikáció

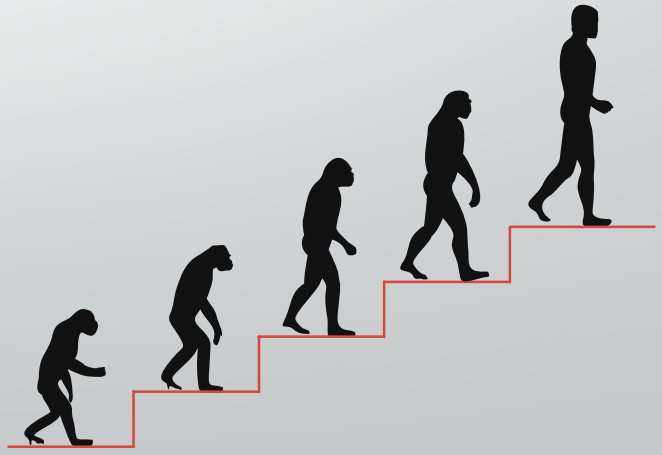
10. Előadás Cybersecurity I. NGFW

Kovács Ákos

paloalto NETWORKS
CYBERSECURITY ACADEMY

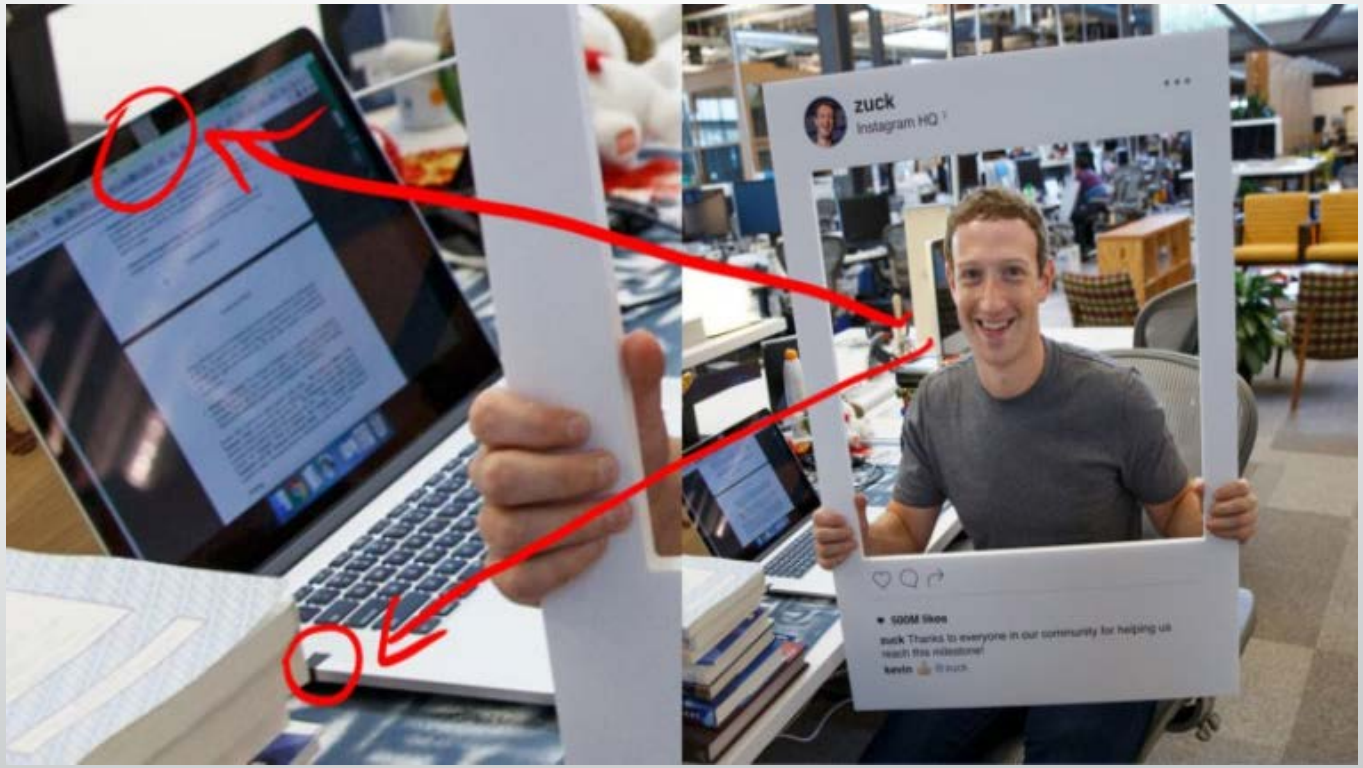
Támadások az internet felől

- A hekkerek evolúciója
- A kiberbűnözés manapság 600+ milliárd dolláros üzlet
- Több mint 100 ország építi a kiber támadások elleni védelmet



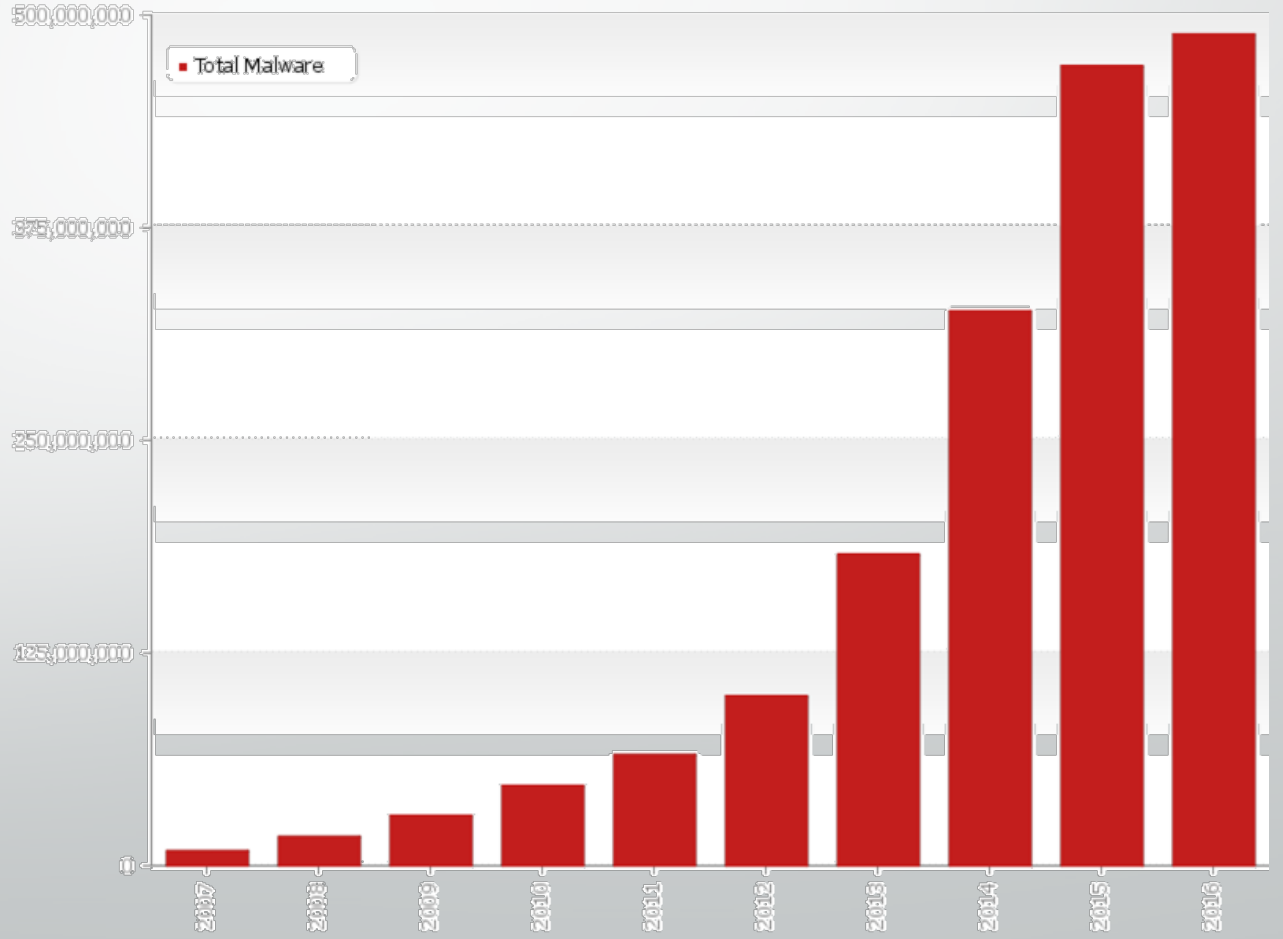
Támadások az internet felől

The FBI Director Puts Tape Over His Webcam, Should You? Apr 18, 2016 OSXdaily.com



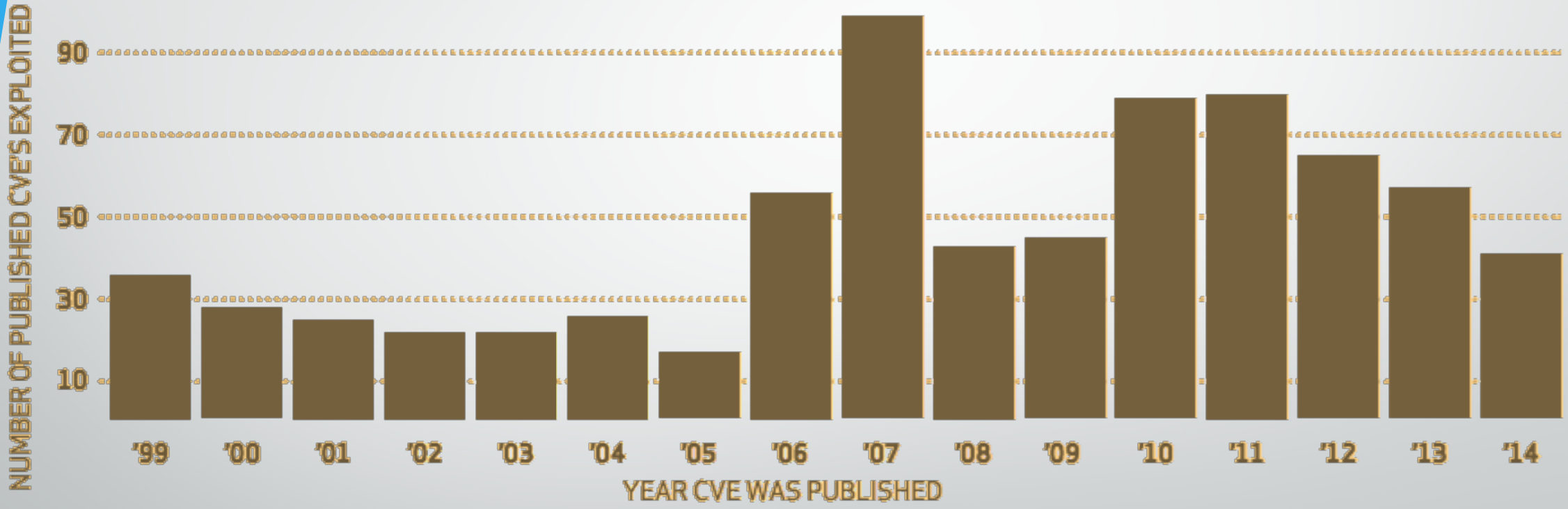
Malware-ek

A malware-ek (kártékony szoftver) száma drasztikusan megnőtt, több mint 500 millió már ma is ismert



tilb
Távközlés-
Informatika
Laboratórium

Nem csak a oday veszélyes



paloalto NETWORKS
CYBERSECURITY ACADEMY

tilb
Távközlés-
Informatika
Laboratórium

A támadások evolúciója

paloalto NETWORKS
CYBERSECURITY ACADEMY

Egy kiber támadás élete – The kill-chain

A megelőzés a kulcs

Információ gyűjtés	Elterjeszti Az exploitot	Futtatni az exploitot	Csatornát nyitni kifelé	Elérni a célunkat
A támadás megtervezése	Csendben megfertőz	A kártékony kód aktiválódik	A kártékony kód Kommunikál támadóval	Adatlopás Szabotázs rombolás

Preventív szakasz **Reaktív szakasz**

Ransomware az új generációs malware

- A végpontokat fertőzi meg
  - Elterjeszteni lehet pl. adat halászat, Social Media, rosszindulatú linkek, bit.ly stb.
- Titkosítja a merevlemezt, vagy a **hálózati megosztást**
  - Az első indításnál megkeresi a lokális vagy hálózati erőforrásokat
  - Vállalati környezetben nagyon veszélyes
  - Nagyon komoly titkosításokat használnak
  - Nincs mód visszafejtésre, vagy feltörésre a kulcs nélkül
- Lezárja a számítógépünket, és kéri a váltságdíjat
  - Az áldozatnak limitált ideje van bitcoinban fizetni
  - A feloldáshoz szükséges kulcs egy anonym szerveren
  - Vagy működik, vagy nem

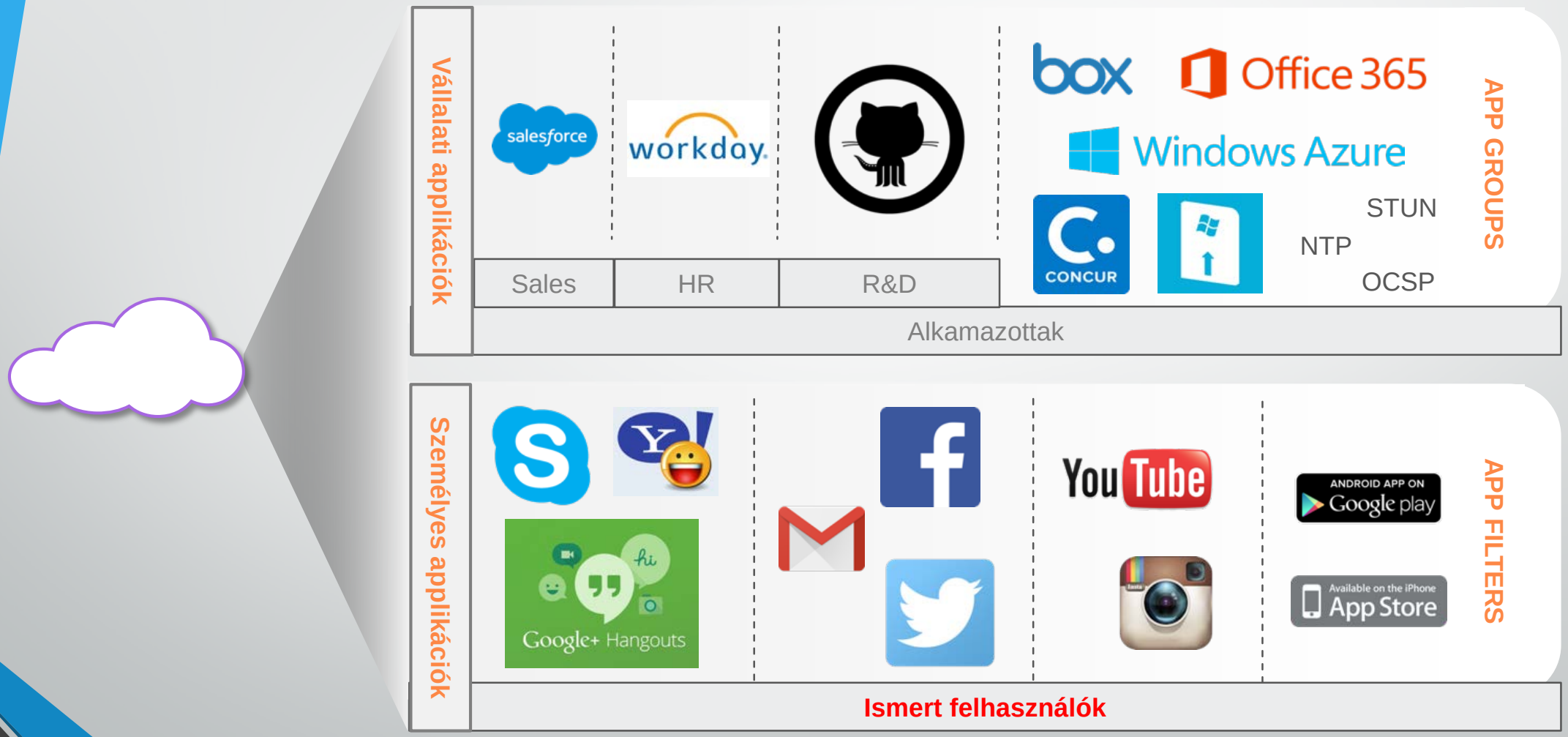
Következő generációs tűzfalak II.

- NGFW különböző biztonsági előírások alapján egy döntést hoz meg
- Mindent egy helyen
- A feltétel lehet a szokásos IP/port vagy applikáció vagy akár user ID is
- A különböző szoftveropciók lassíthatják a tűzfalat
  - Ha az IP/port döntés megszületett a forgalom már a tűzfalon belül van
  - További filterek tovább lassíthatják a tűzfalat -> egy csomagot többször néz meg
  - Az új generációs tűzfalak gyorsabbak mivel egy natív megoldás mindig gyorsabb mint több sorosan kapcsolt szoftver

Zero trust hálózati koncepció

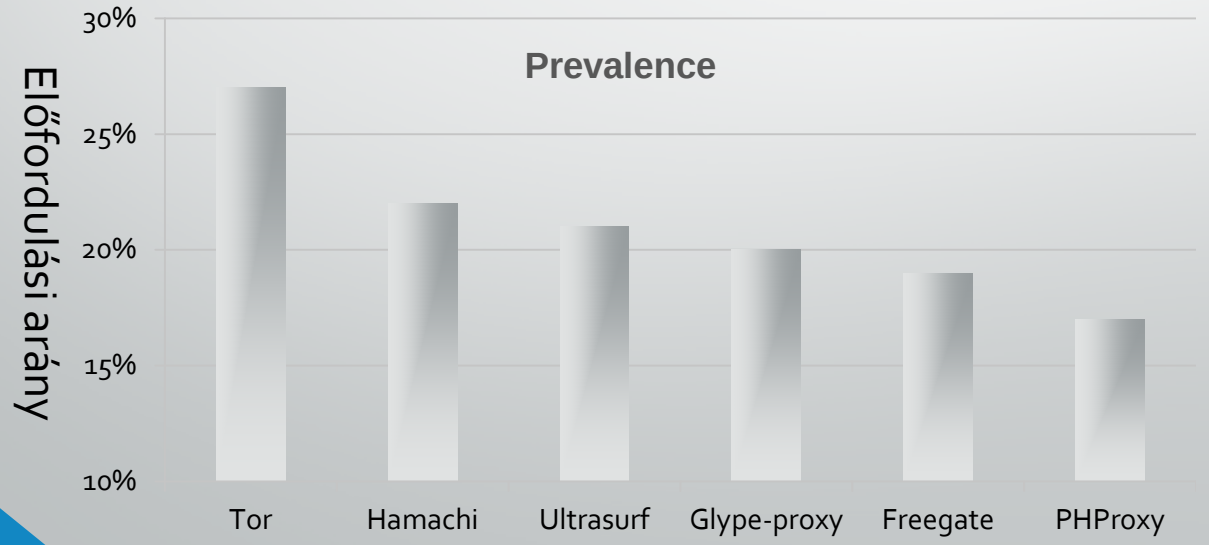
- Minden erőforrást a tűzfalon keresztül érhetünk el
- A hozzáférések az egész rendszerben láthatóak
- A hálózati szegmentáció igen fontos
- A szegmensek mindig az NGFW az átjárója
- A forgalom és a naplófájlok folyamatos figyelése tovább növelheti a biztonságot

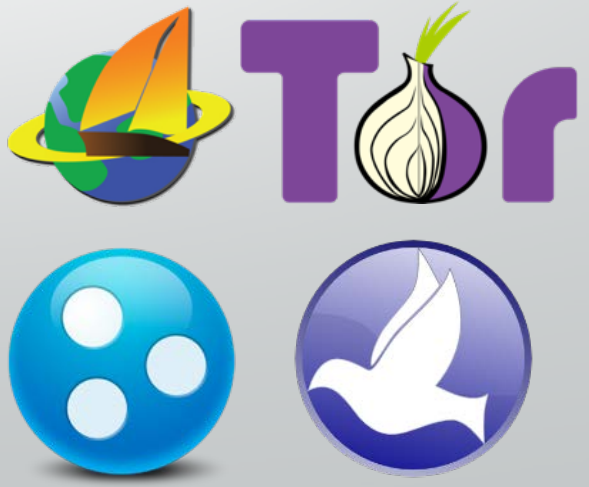
Fehérlisták



Fekete listák

- Ha a „mindent engedünk kivéve amit nem” szabályt alkalmazzuk akkor explicit módon ki kell tiltani a nem kívánt hálózati forgalmat
- Fekete listás applikációk:
  - UltraSurf, Tor, P2P, Proxy applikációk
- A támadok által használt de hasznos protokollok:
  - Távoli hozzáférés, fájlmegosztók, tunneling protokollok, DNS



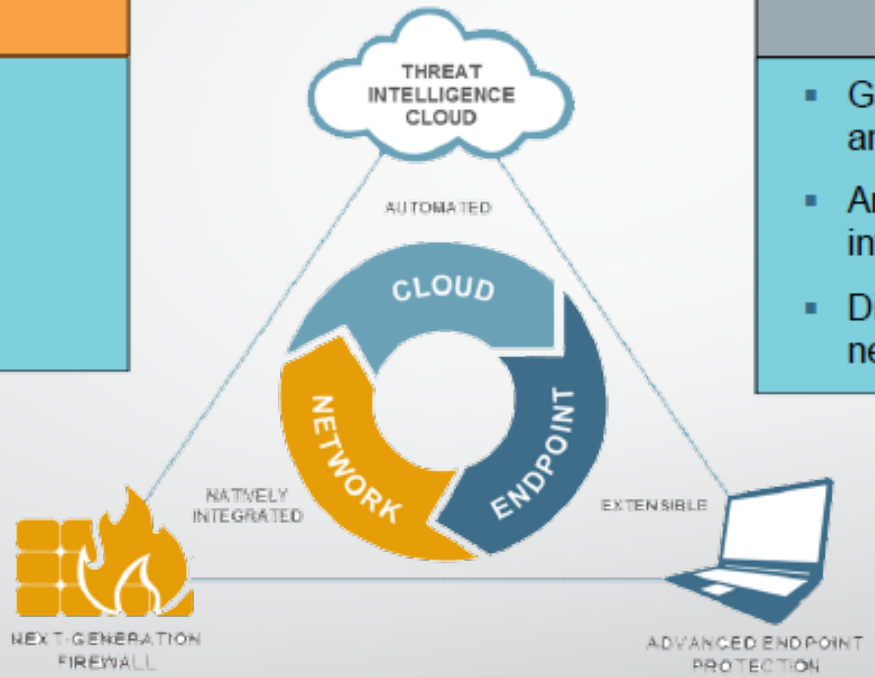


tilb
Távközlés-
Informatika
Laboratórium

Next-Generation Security Platform

Next-Generation Firewall

- Identifies and inspects all traffic
- Blocks known threats
- Sends unknown to cloud
- Extensible to mobile and virtual networks



Threat Intelligence Cloud

- Gathers potential threats from network and endpoints
- Analyzes and correlates threat intelligence
- Disseminates threat intelligence to network and endpoints

Advanced Endpoint Protection

- Inspects all processes and files
- Prevents both known and unknown exploits
- Integrates with cloud to prevent known and unknown malware

paloalto NETWORKS
CYBERSECURITY ACADEMY

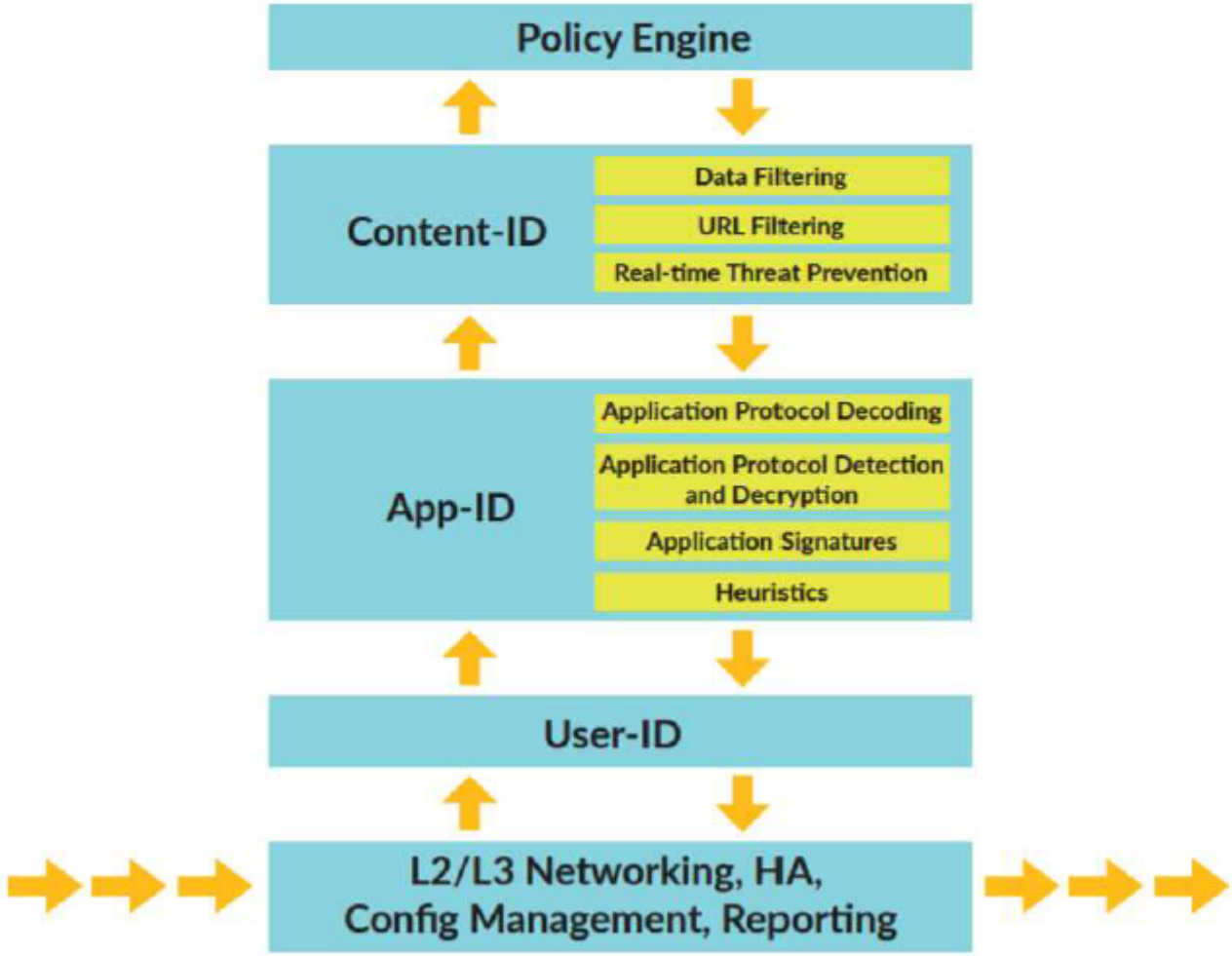
Palo Alto Single Pass Architektúra

Single pass:

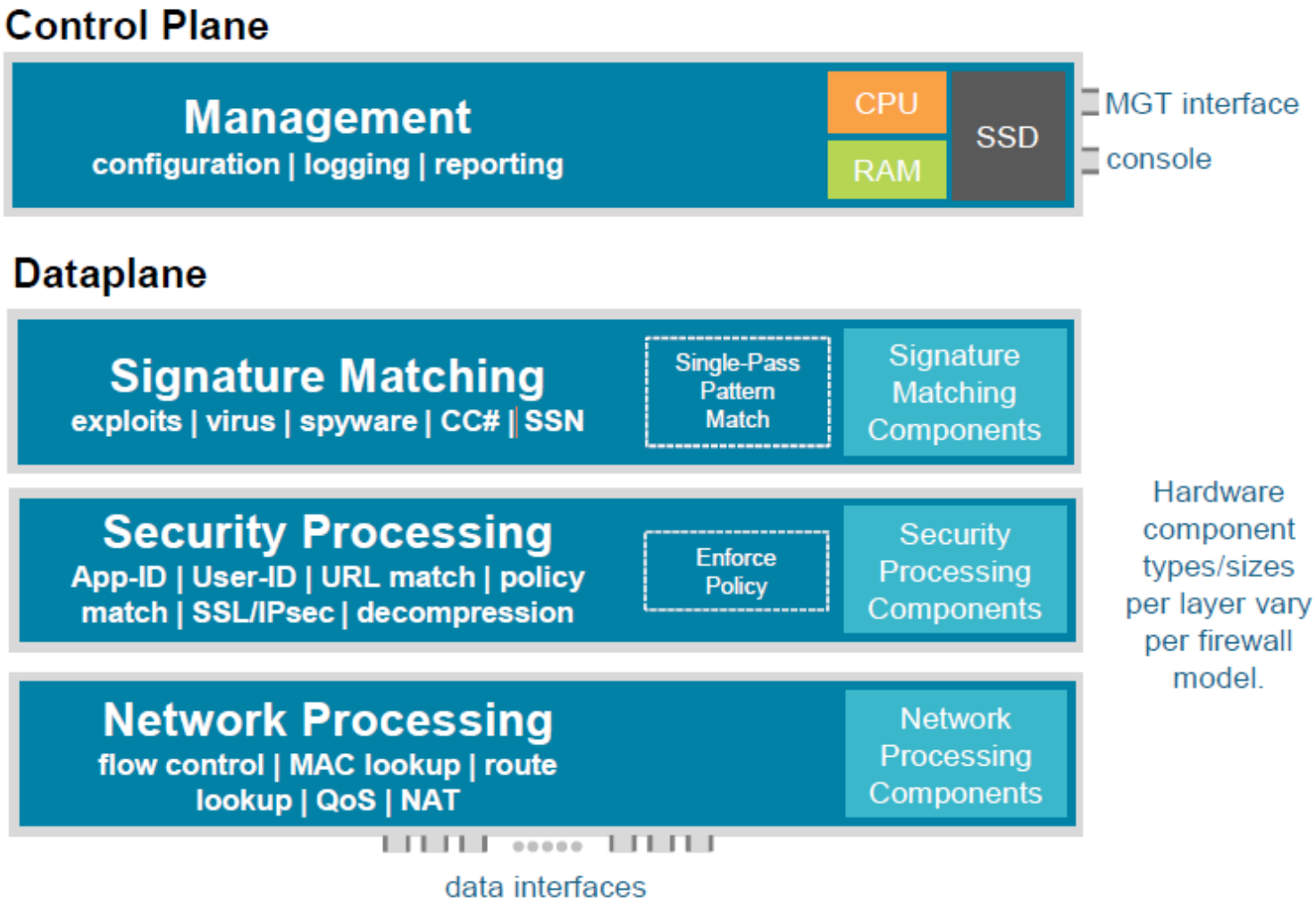
- Operations per packet:
  - Traffic classification with App-ID technology
  - User/group mapping
  - Content scanning – threats, URLs, confidential data
- One single policy (per type)

Parallel processing:

- Function-specific parallel processing hardware engines
- Separate data/control planes



Palo Alto Architektúra



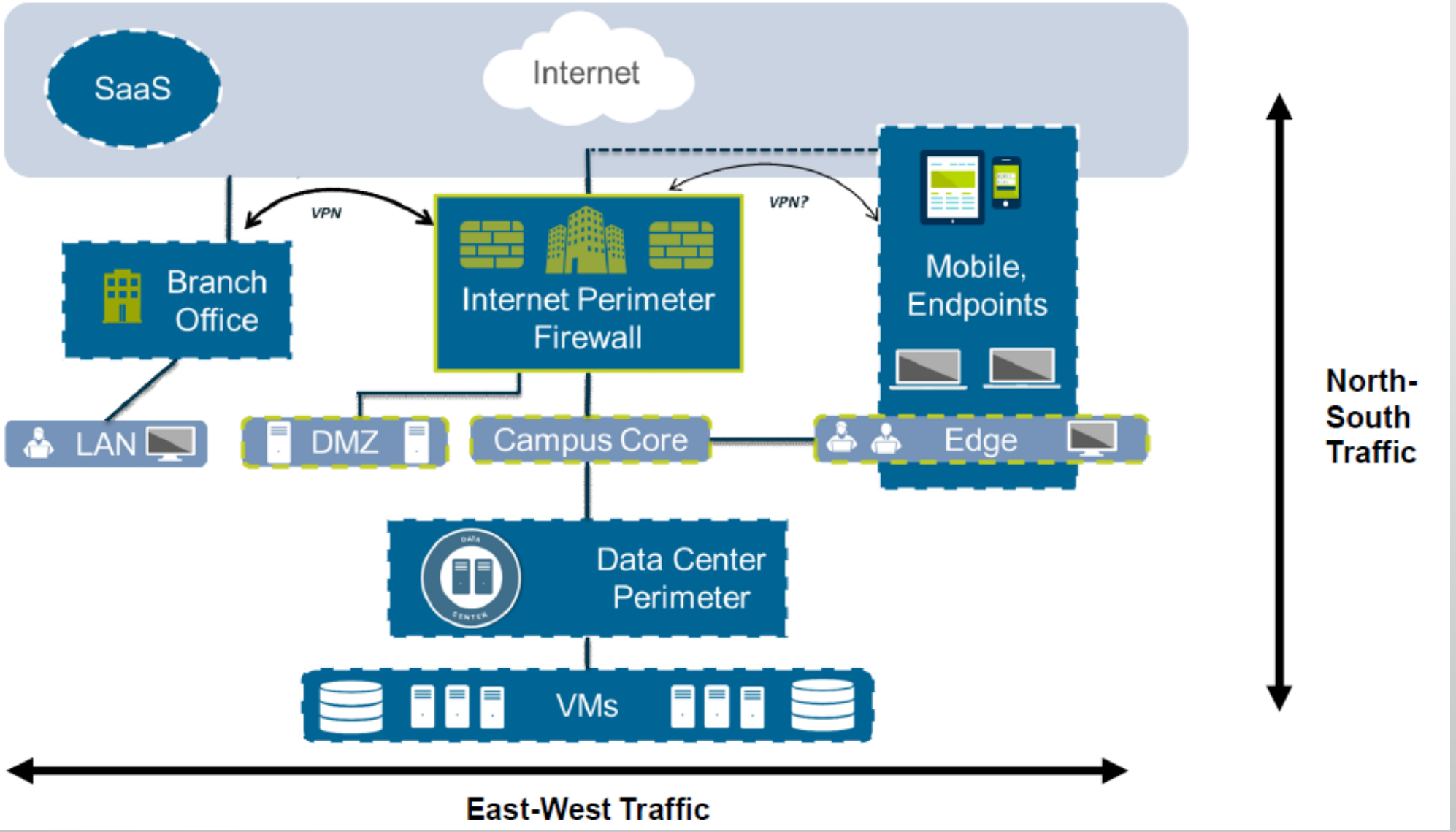
Control Plane | Management
Provides configuration, logging, and report functions on a separate processor, RAM, and hard drive

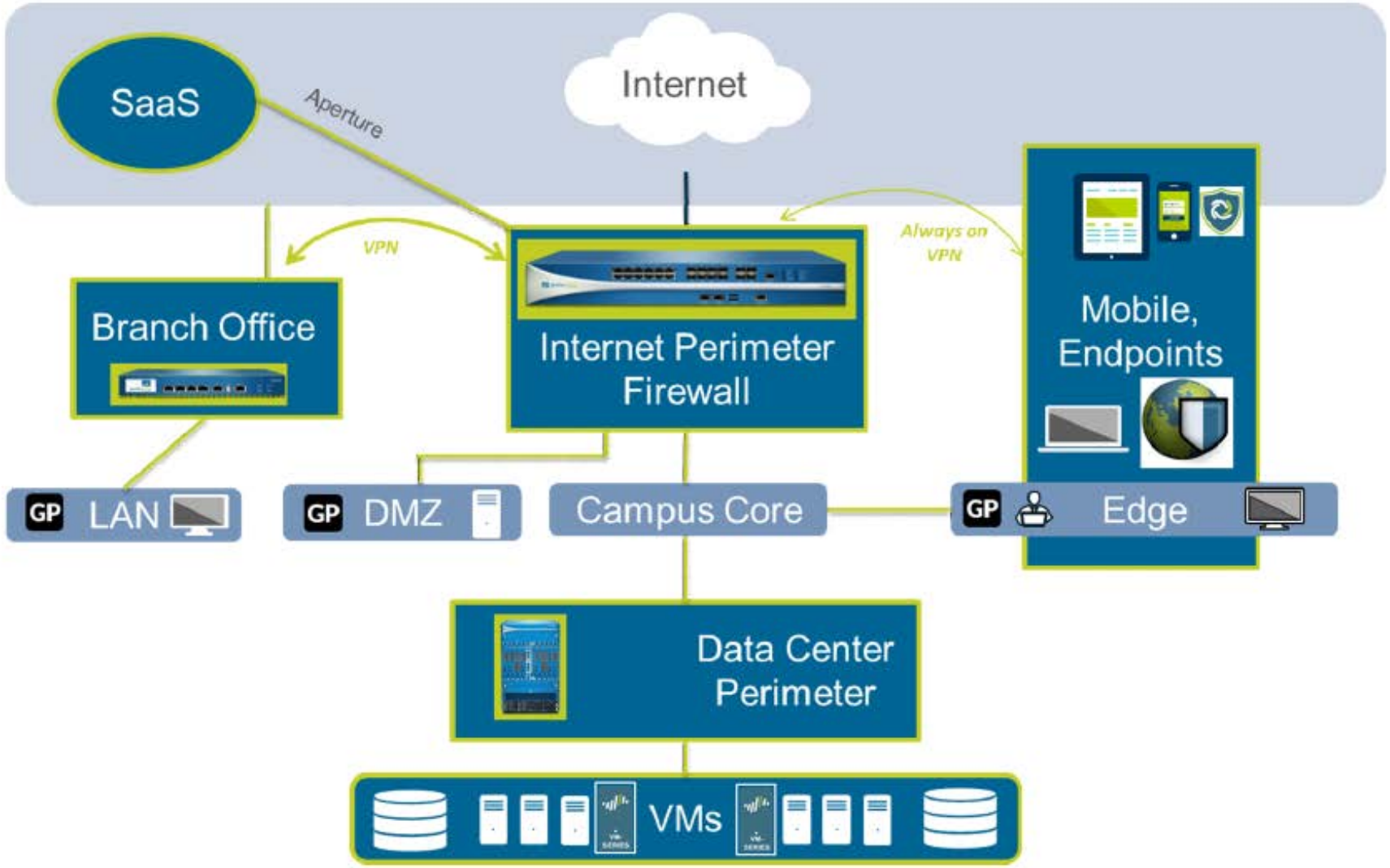
Signature Matching
Stream-based, uniform signature match including vulnerability exploits (IPS), virus, spyware, CC#, and SSN

Security Processing
High-density parallel processing for flexible hardware acceleration for standardized complex functions

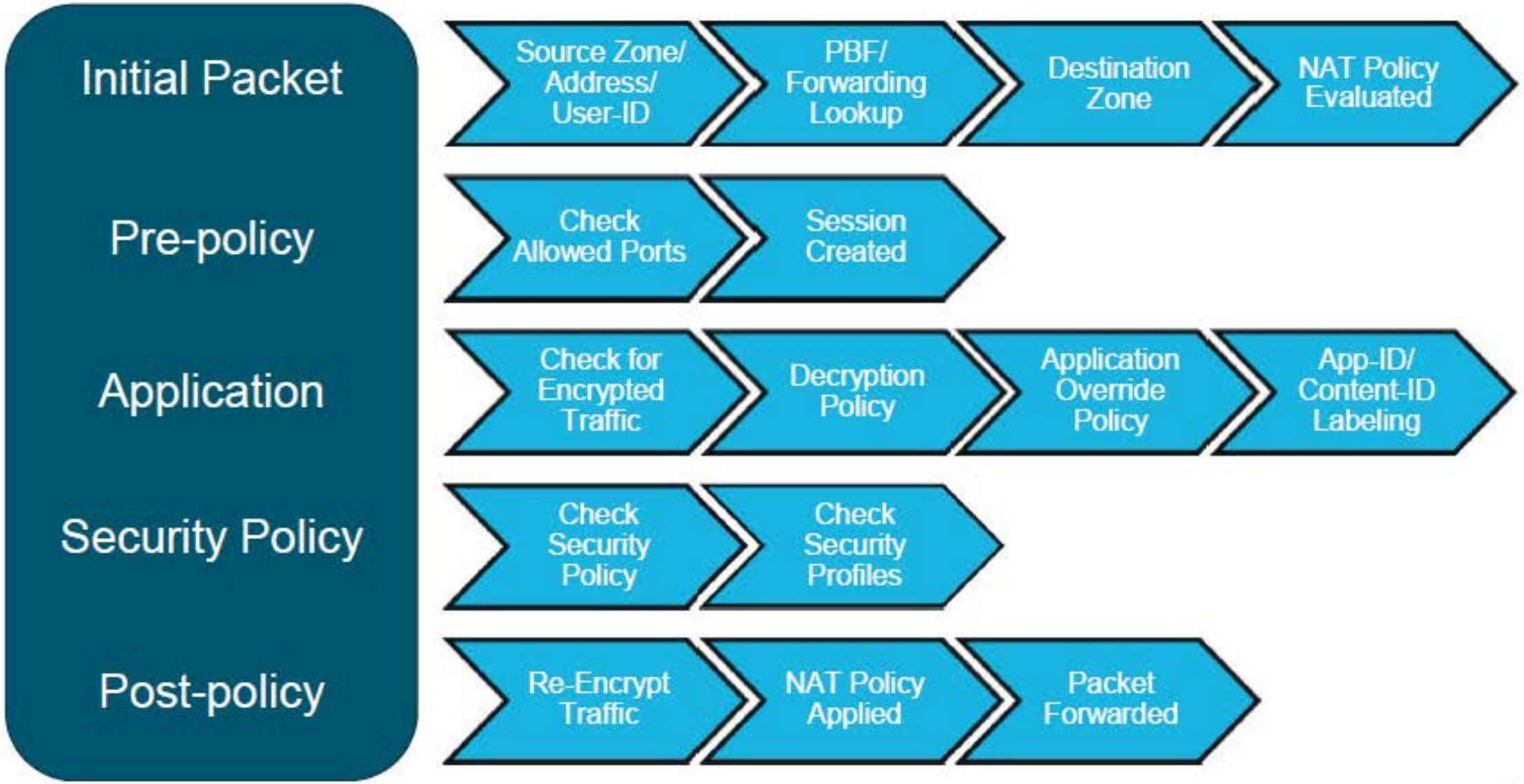
Network Processing
Front-end network processing, hardware-accelerated per-packet route lookup, MAC lookup, and NAT

Adatfolyamok a hálózatokban



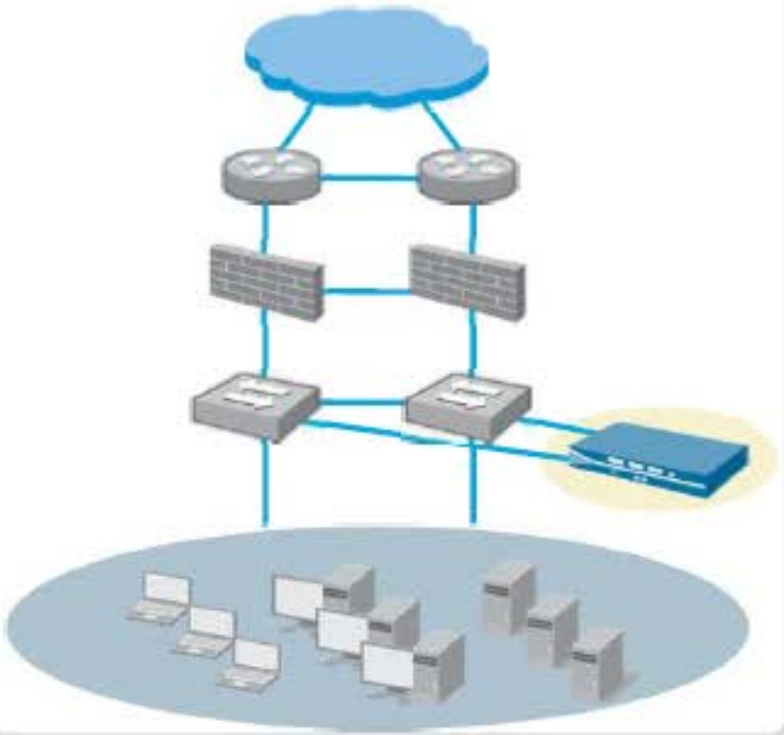

SaaS
Aperture
Internet
VPN
Always on
VPN
Branch Office
Internet Perimeter
Firewall
Mobile,
Endpoints
GP LAN
GP DMZ
Campus Core
GP Edge
Data Center
Perimeter
VMs

Flow Logic of the Next-Generation Firewall



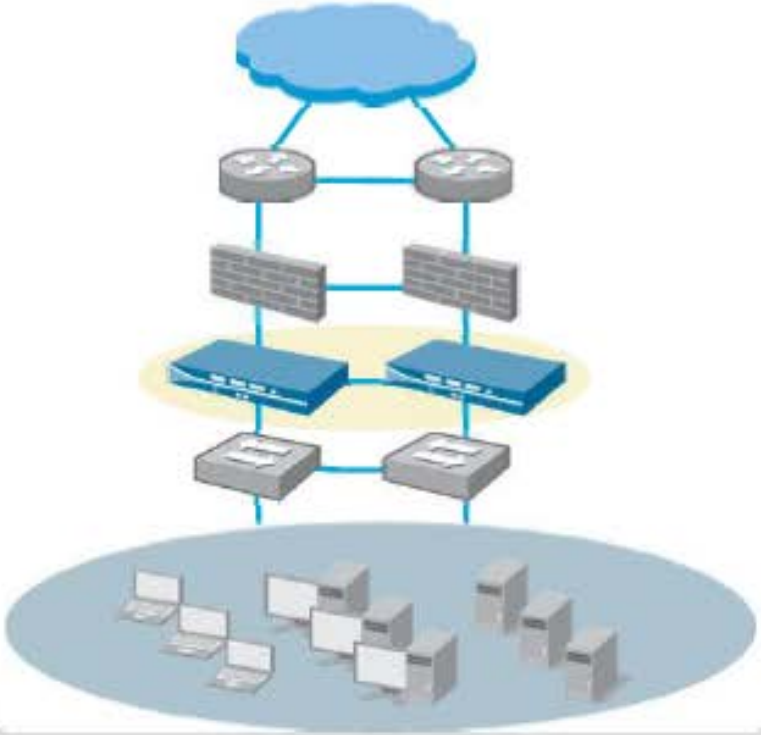
Flexible Deployment Options for Ethernet Interfaces

Tap



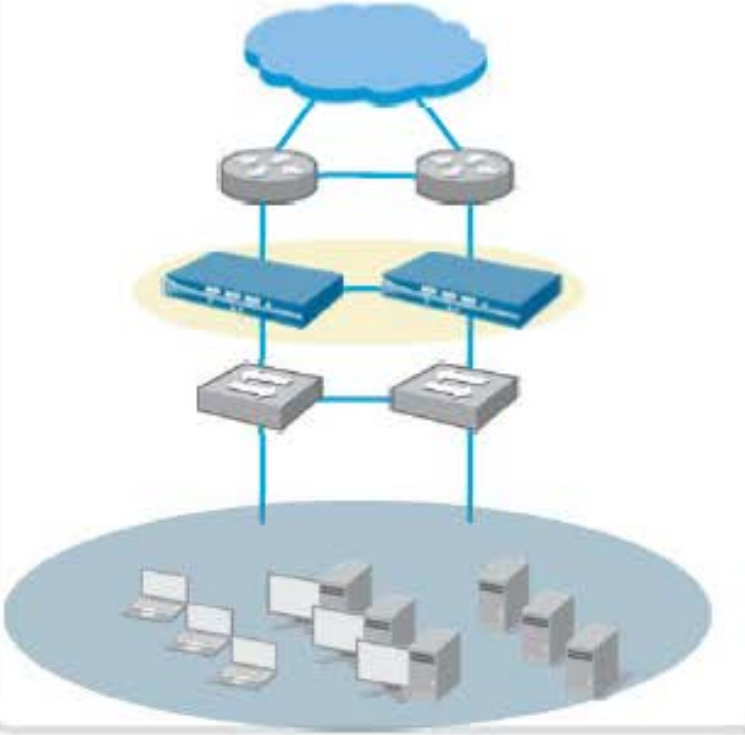
- Application, user, and content visibility without inline deployment
- Evaluation and audit of existing networks

Virtual Wire



- App-ID, Content-ID, User-ID, and SSL decryption
- Includes NAT capability

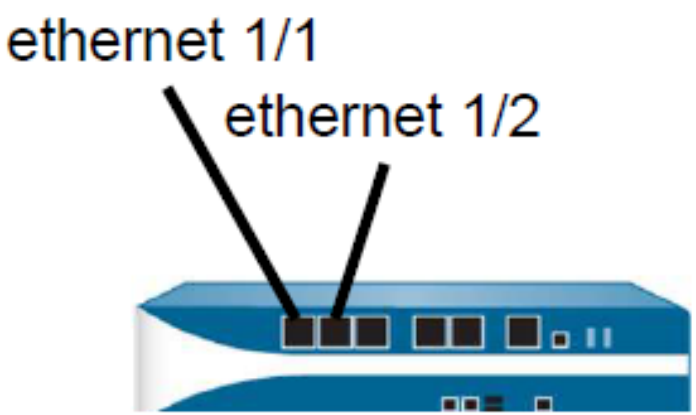
Layer 3



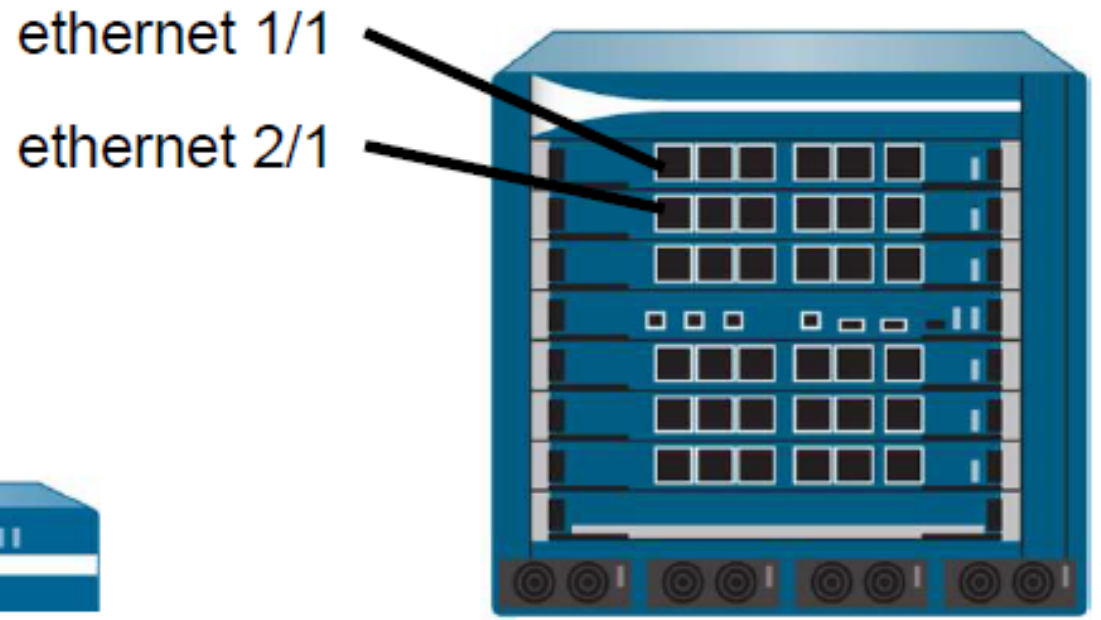
- All of the Virtual Wire mode capabilities with the addition of Layer 3 services: virtual routers, VPN, and routing protocols

In-Band Network Interfaces

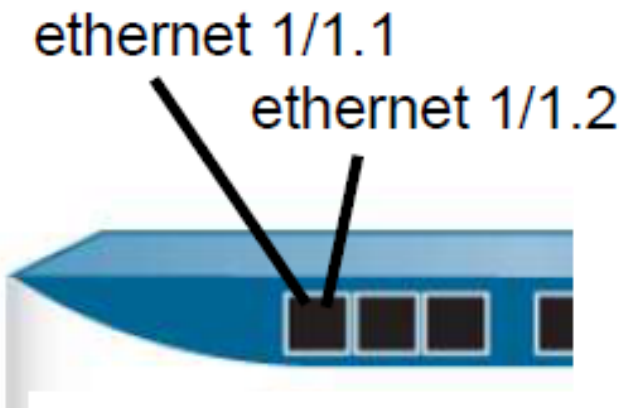
- Each interface is assigned to a single zone.
- A zone can include multiple physical or logical interfaces.



Single-Slot Firewall



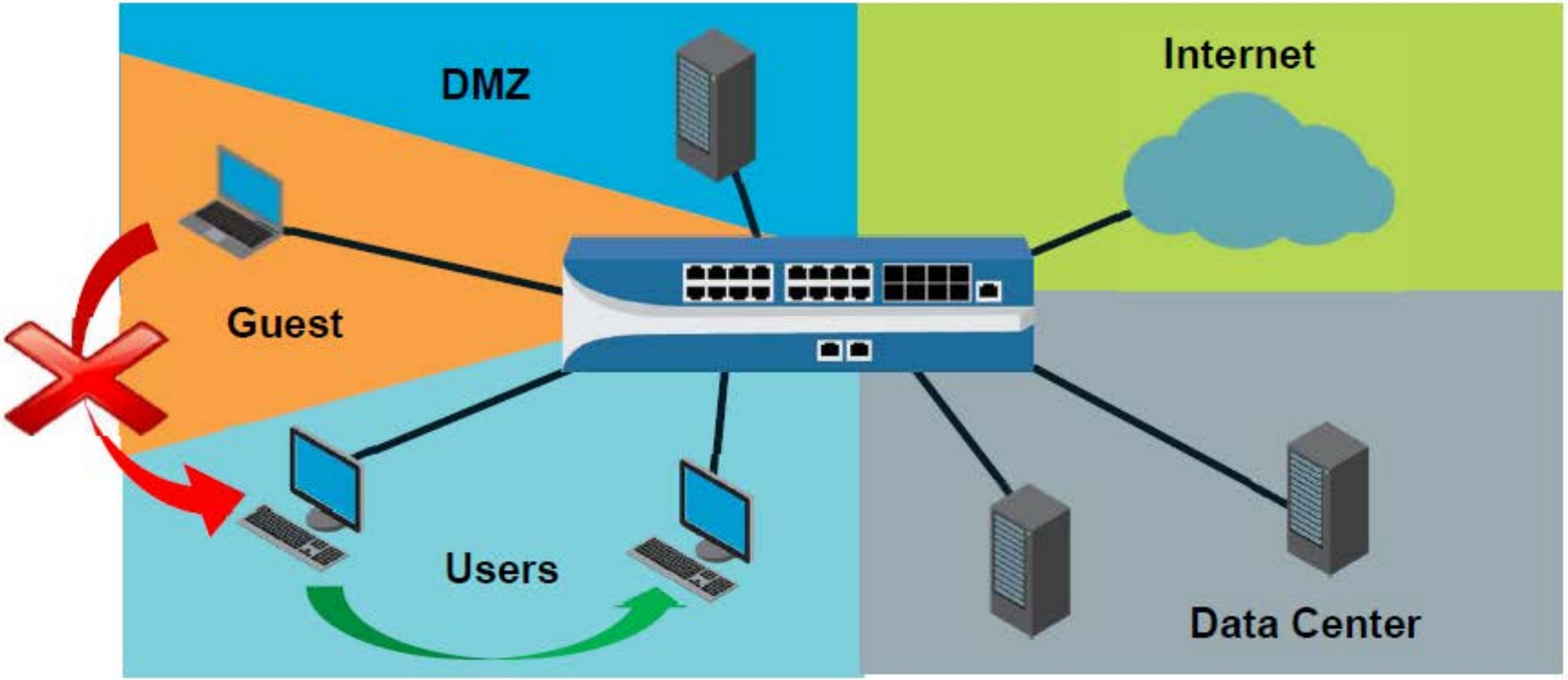
Multi-Slot Firewall



Logical Interfaces

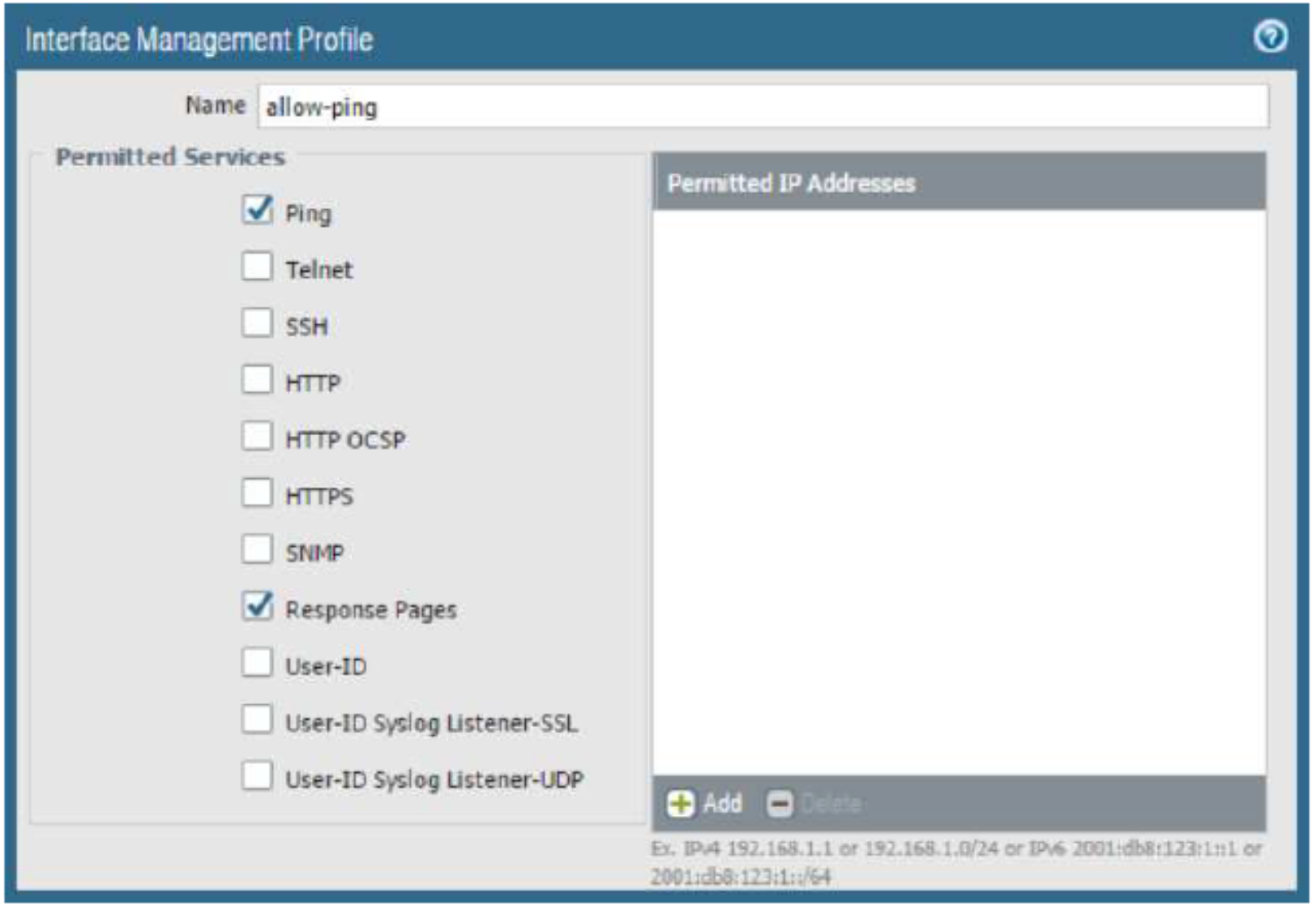
Security Zones and Security Policy Rules

- Traffic within a zone is *allowed* by default.
- Traffic between zones is *denied* by default.



Interface Management Profile

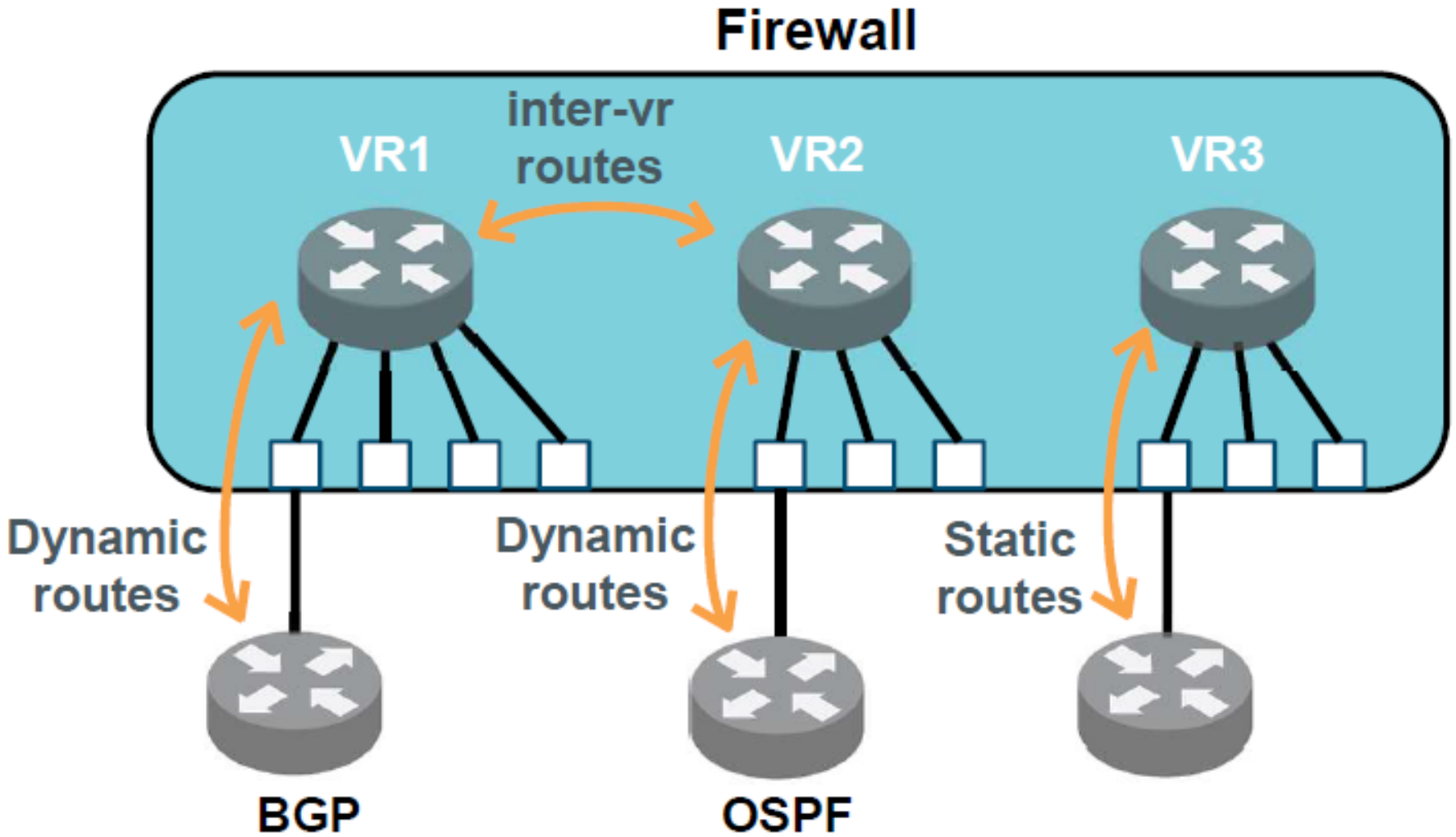
Network > Network Profiles > Interface Mgmt > Add



- Defines which firewall management services are accessible from a traffic interface
- Can be applied to Layer 3, loopback, and tunnel interfaces

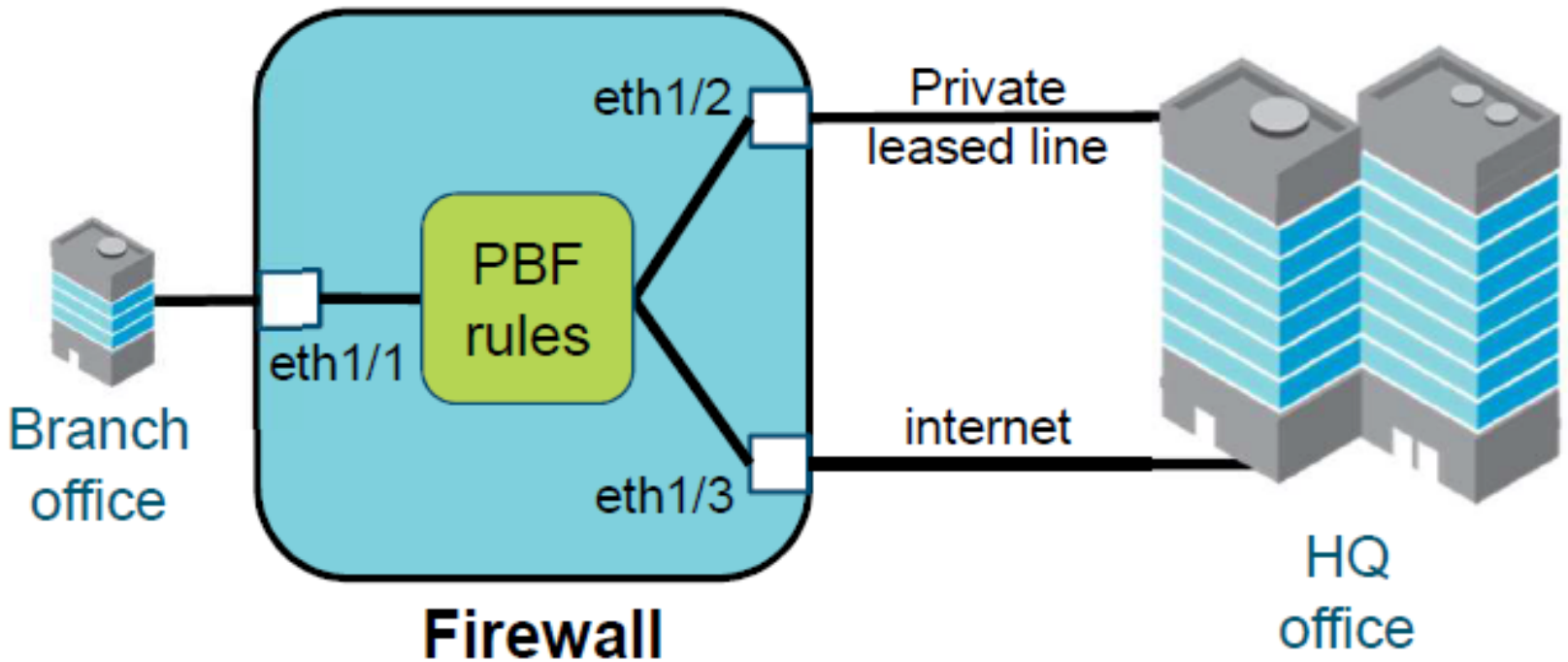
Virtual Routers

- Support one or more static routes
- Support dynamic routing:
  - RIPv2
  - OSPFv2
  - OSPFv3
  - BGPv4
- Support multicast routing
  - PIM-SM
  - PIM-SSM



Policy-Based Forwarding

- Specifies different egress interface from that specified in route table
- Possible use for performance or security reasons



Specify egress interface for:

- Bandwidth sensitive applications
- Unencrypted applications

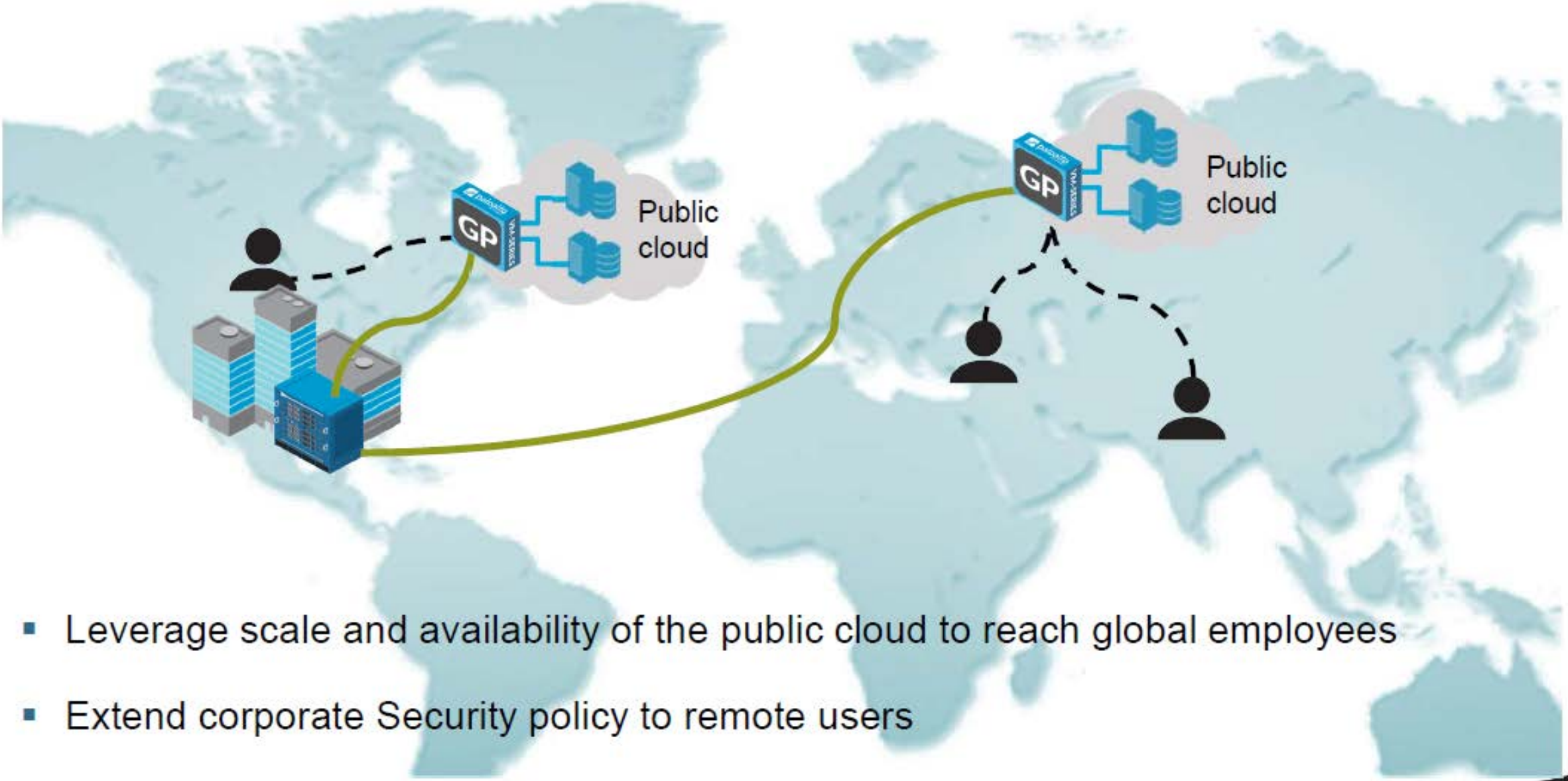
Specify egress interface for:

- Non-bandwidth sensitive applications
- Encrypted applications

Integrated Approach to Threat Prevention

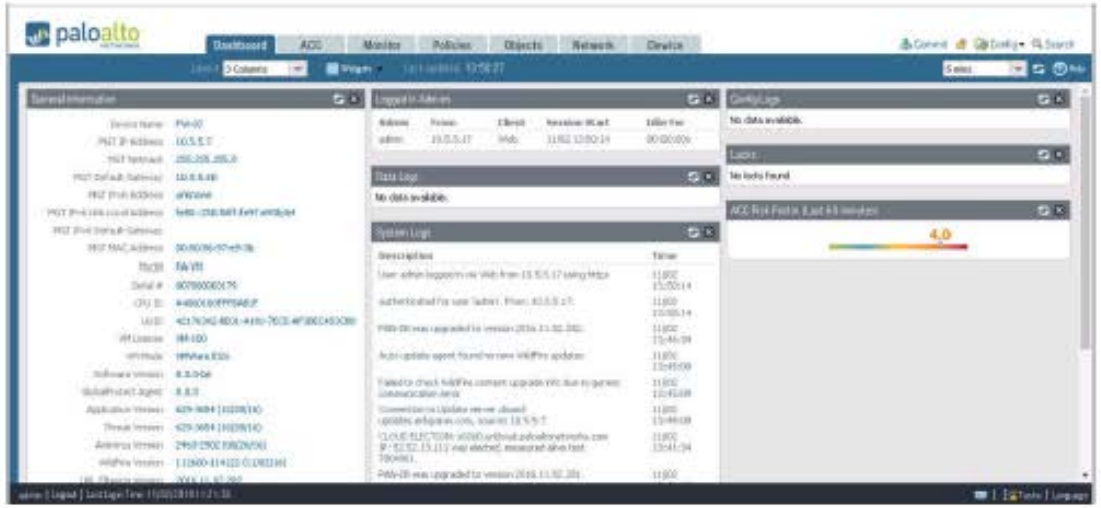
	Delivery	Exploitation	Installation	C2	Act on Objective
App-ID	Block high risk applications			Block C2 on non-standard ports	Prevent exfiltration and lateral movement
URL Filtering	Block known malware sites			Block malware, fast-flux domains	
Vulnerability		Block the exploit			Prevent lateral movement
Anti-spyware				Block spyware, C2 traffic	
AV			Block malware		Prevent lateral movement
Traps	Monitor allowed processes and executables	Prevent the exploit	Prevent malicious .exe from running		
File Blocking			Prevent drive-by downloads		Prevent exfiltration and lateral movement
DoS/Zone		Prevent evasions			Prevent DoS attacks
WildFire	Identify malware		Detect unknown malware	Detect new C2 traffic	

GlobalProtect: Extend Security to All Users/Devices

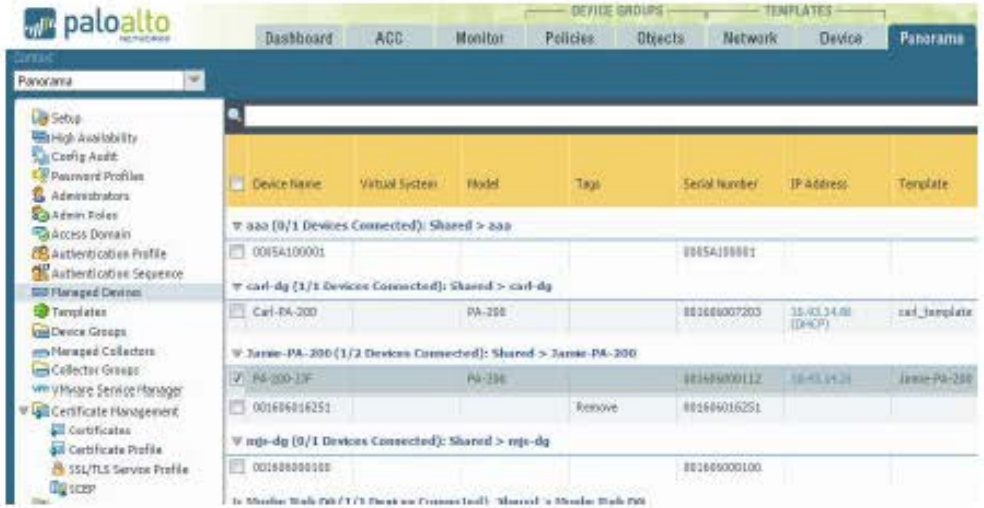


- Leverage scale and availability of the public cloud to reach global employees
- Extend corporate Security policy to remote users

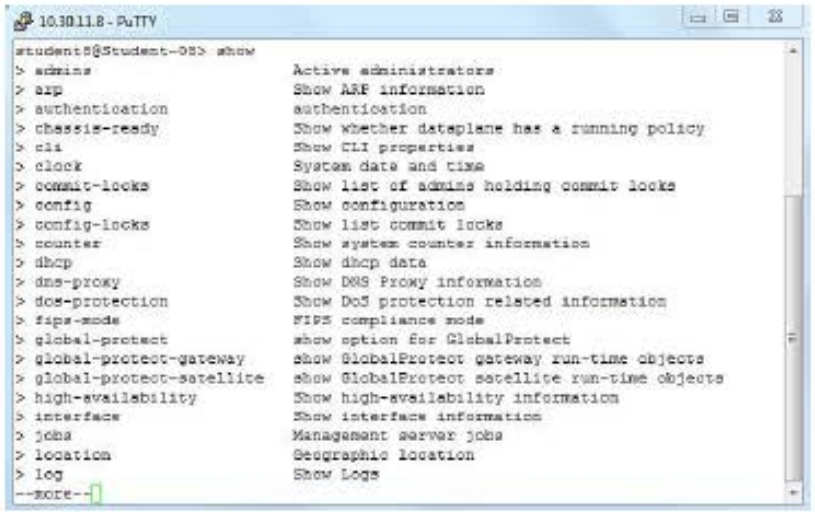
Administrative Access



WebUI



Panorama

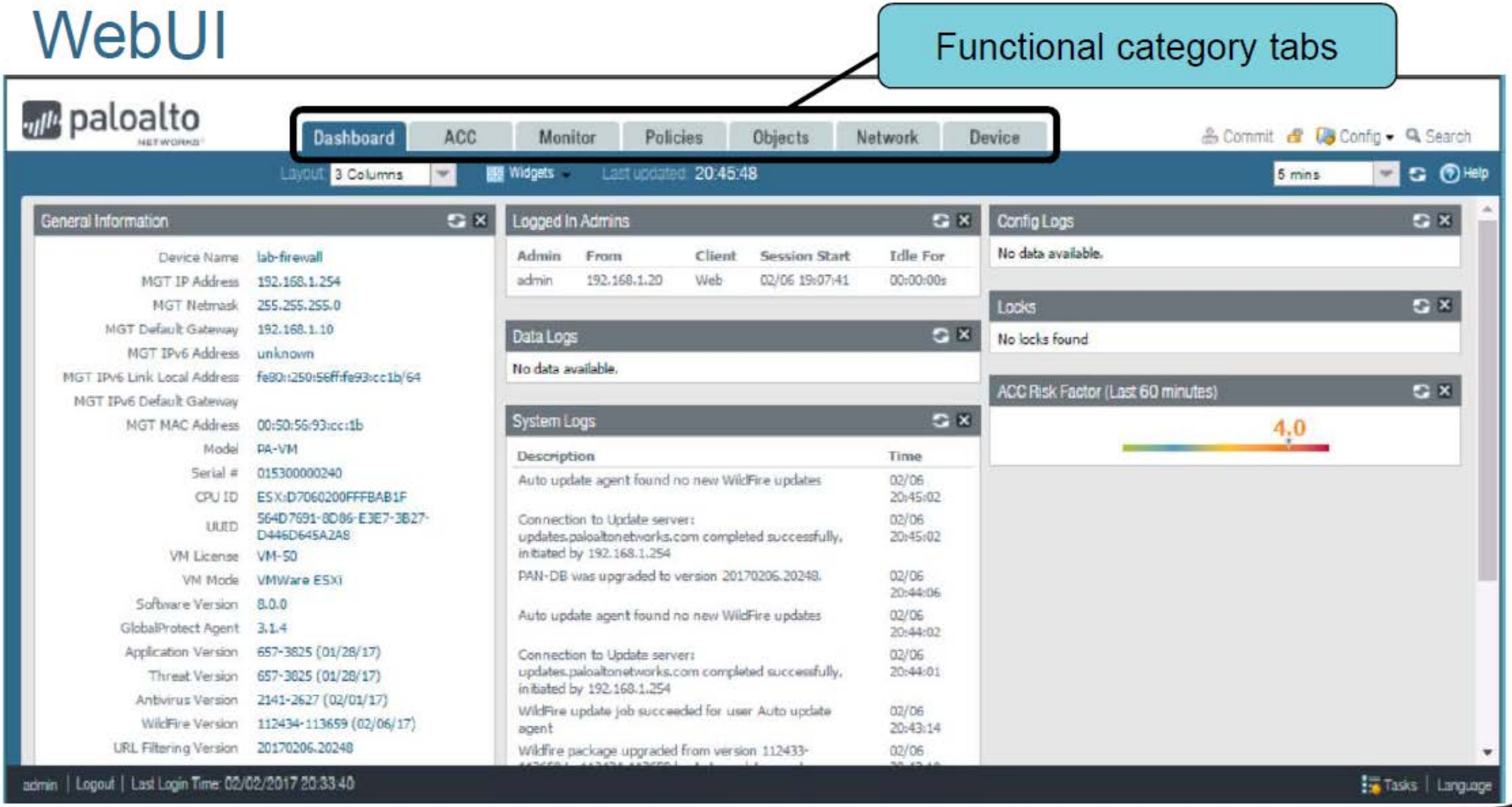


SSH/console CLI

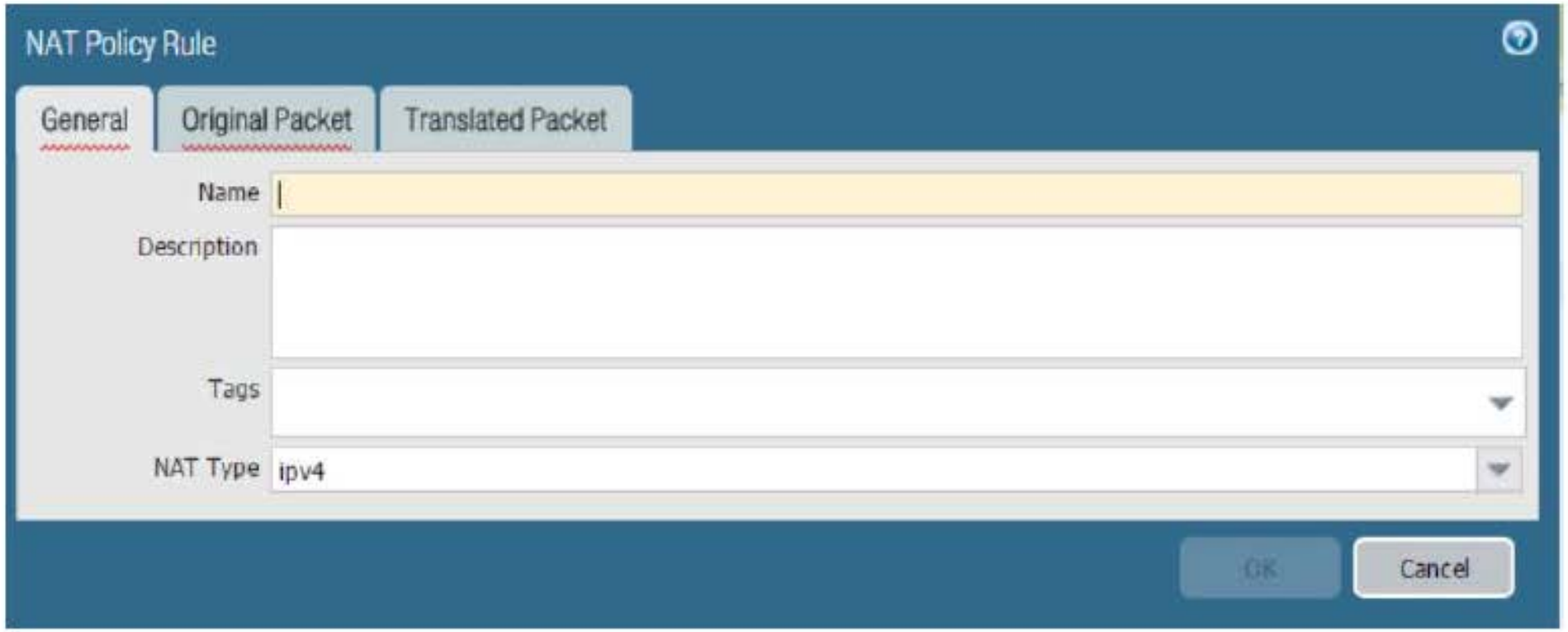
```
▼<response status="success" code="19">
  ▼<result>
    ▼<msg>
        <line>Commit job enqueued with jobid 17</line>
      </msg>
      <job>17</job>
    </result>
  </response>
```

REST XML API

WebUI


Functional category tabs
paloalto NETWORKS
Dashboard
ACC
Monitor
Policies
Objects
Network
Device
Commit
Config
Search
Layout 3 Columns
Widgets
Last updated 20:45:48
5 mins
Help
General Information
Device Name lab-firewall
MGT IP Address 192.168.1.254
MGT Netmask 255.255.255.0
MGT Default Gateway 192.168.1.10
MGT IPv6 Address unknown
MGT IPv6 Link Local Address fe80::250:56ff:fe93:cc1b/64
MGT IPv6 Default Gateway
MGT MAC Address 00:50:56:93:cc:1b
Model PA-VM
Serial # 015300000240
CPU ID ESX:D7060200FFFBAB1F
UUID 564D7691-8D86-E3E7-3B27-D446D645A2A8
VM License VM-50
VM Mode VMWare ESXi
Software Version 8.0.0
GlobalProtect Agent 3.1.4
Application Version 657-3825 (01/28/17)
Threat Version 657-3825 (01/28/17)
Antivirus Version 2141-2627 (02/01/17)
WildFire Version 112434-113659 (02/06/17)
URL Filtering Version 20170206.20248
Logged In Admins
Admin From Client Session Start Idle For
admin 192.168.1.20 Web 02/06 19:07:41 00:00:00s
Data Logs
No data available.
System Logs
Description Time
Auto update agent found no new WildFire updates 02/06 20:45:02
Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254 02/06 20:45:02
PAN-DB was upgraded to version 20170206.20248. 02/06 20:44:06
Auto update agent found no new WildFire updates 02/06 20:44:02
Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254 02/06 20:44:01
WildFire update job succeeded for user Auto update agent 02/06 20:43:14
Wildfire package upgraded from version 112433- 02/06
Config Logs
No data available.
Locks
No locks found
ACC Risk Factor (Last 60 minutes)
4.0
admin | Logout | Last Login Time: 02/02/2017 20:33:40
Tasks | Language

WebUI Editing Guidance

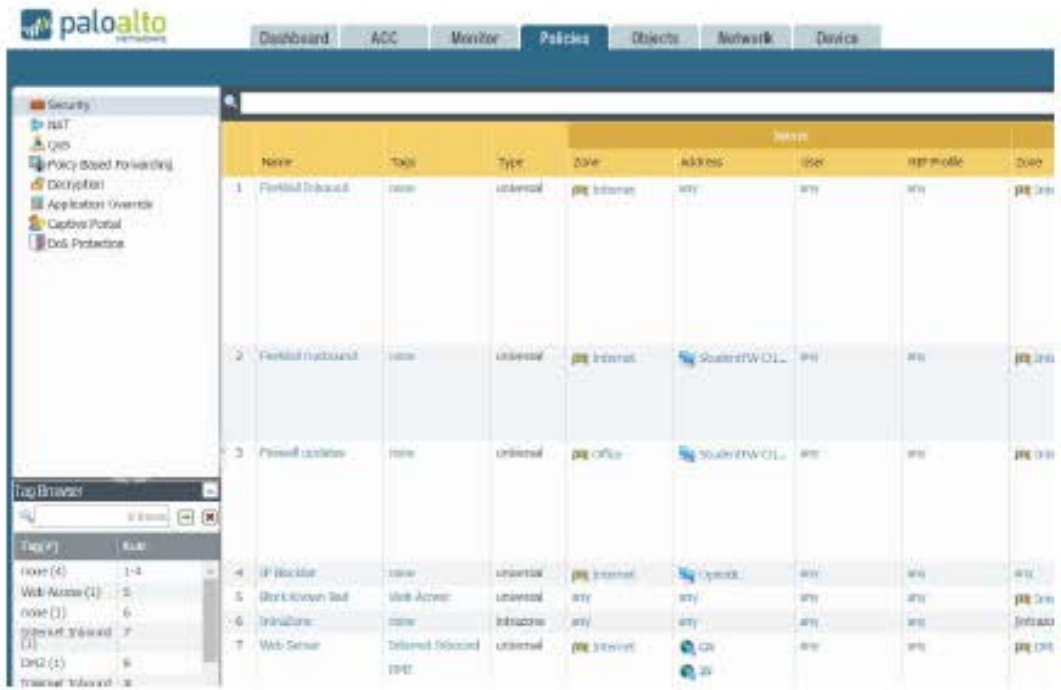


- Red underline:
  - Information required
- Yellow text box:
  - Required field
- OK button:
  - Unavailable if information missing

Configuration Types

Candidate Configuration

- Configuration changes made but not committed



Running Configuration

- Configuration settings currently active on the firewall