Introducere SRED
Administrarea cursului. Soluții de securitate

26 februarie 2015

Obiective

- Cuprinsul cursului
- Organizare laborator
- Notare
- Soluții de securitate
  - Cisco
  - Fortinet
- Device UI

Ce este SRED?

Curs avansat de securizare a infrastructurilor de rețea

- Continuare pentru SCR
- Utilizare de echipamente dedicate

Laborator provocator – inter-vendor

- Cisco
- Fortinet
- … în același timp

Posibilitatea de certificare

- Cisco CCNP Security - Firewall 1.0 (80%)
- Fortinet – FCNSA și FCNSP

SRED

Cuprinsul cursului

No.	Course Title	Date
1	Administrare curs. Soluții de securitate. Device UI.	26-feb-2015
2	Basic firewalling și mentenanță	12-mar-2015
3	ACL-uri și NAT	19-mar-2015
4	Advanced firewalling	26-mar-2015
5	Rutare și switching	2-apr-2015
6	Vacanță	9-apr-2015
7	Test grilă	16-apr-2015
8	Contexte de securitate	23-apr-2015
9	Basic VPNs	30-apr-2015
10	Advanced VPNs și IPS	7-mai-2015
11	High Availability	14-mai-2015
12	Fortinet Demo	21-mai-2015

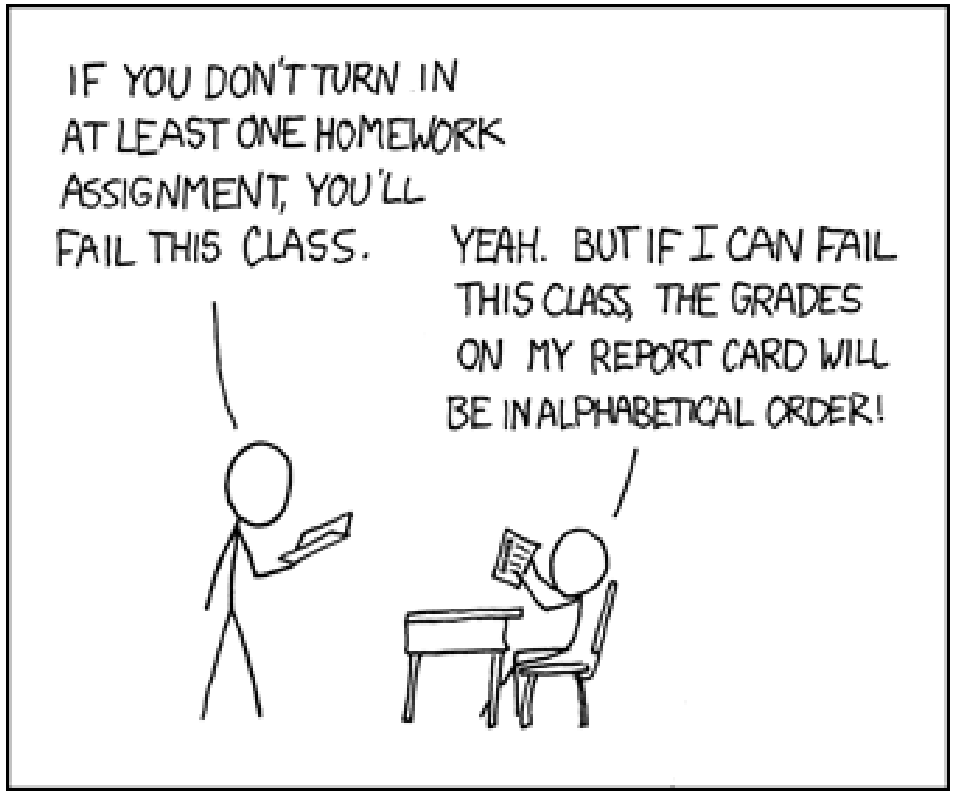
Laboratorul – hands-on

- 16 studenți la laborator
- 2 invervale orare
  - Joi 16:00 – 18:00
  - Joi 20:00 – 22:00
- Laborator dual
  - O oră pe echipamente Cisco, o oră pe echipamente Fortinet

SRED

Notare

- Activitate la curs: 1 pcte
- Laborator: 2.5 pcte
- Examen final practic: 2.5 pcte
  - 1.25 pcte Fortinet
  - 1.25 pcte Cisco
- Grilă 1 (parțial): 2.5 pcte
  - Cursul 1-6
- Grilă 2 (final teoretic): 2.5 pcte
  - Cursul 6-11
- Rezultat final
  - Maxim 11 puncte
  - Se trece cu nota 5



SRED

Soluții de securitate

Vendori - Cisco

- Companie fondată în 1984
- Deține 80% din piața de Routing and Switching
- În domeniul securității oferă:
  - ASA 5500 series – Firewall, VPN, IPS (lightweight – AIP/SSM)
  - VPN Concentrators – pentru hub-ul VPN
  - IPS/IDS 4200 series – soluție dedicată IPS
  - Ironport – Antispam, Data Leakage Prevention, Web filtering
  - ACE – Web Application Firewall
  - MARS – monitorizare
  - Cisco Security Manager – provisioning și management
  - Cisco Security Agent – HIPS
  - Cisco NAC

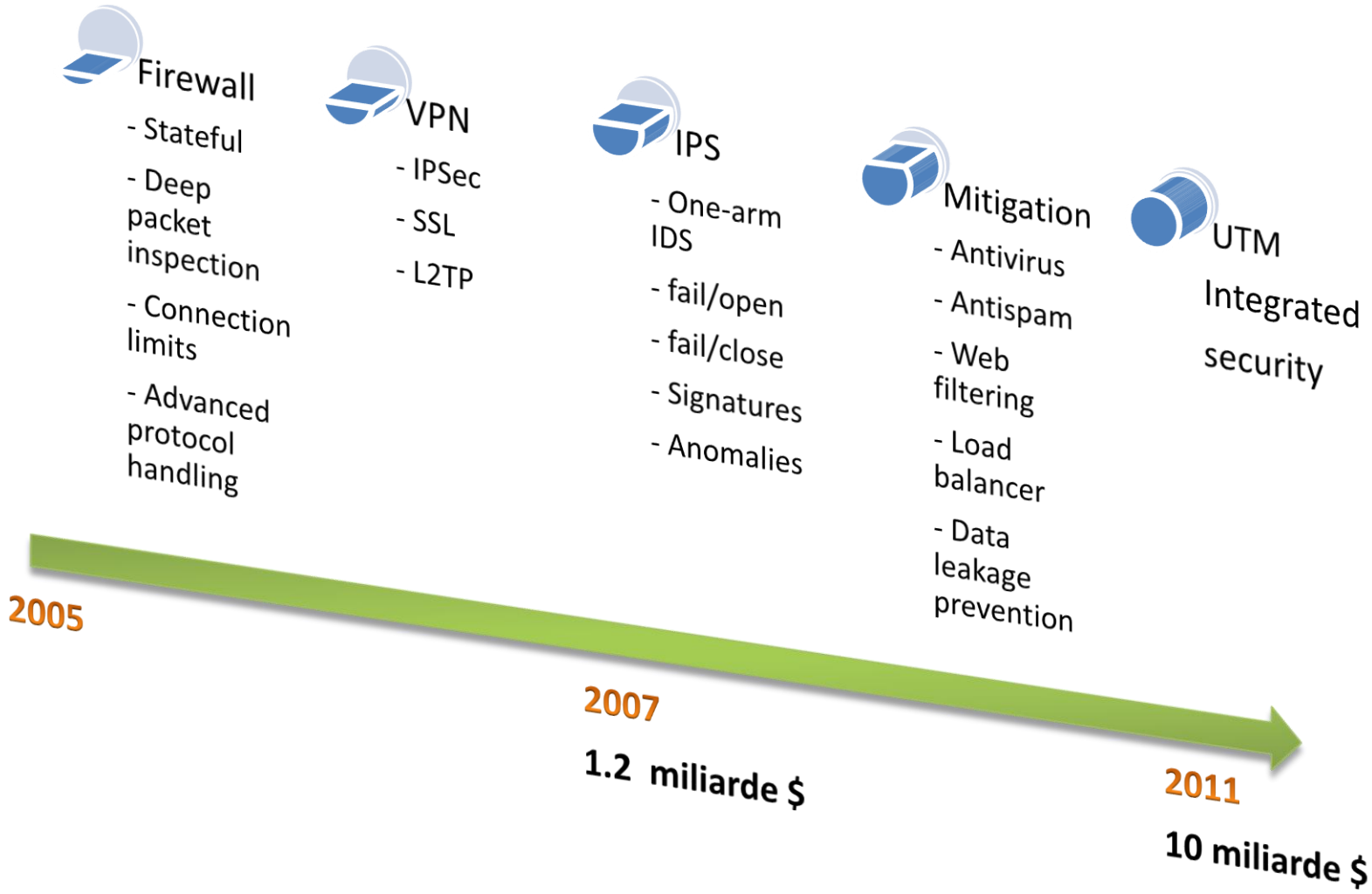
SRED

Vendori - Fortinet

- Companie fondată în 2000
- În domeniul securității oferă:
  - Fortigate – Unified Threat Management
  - FortiMail – pentru volum mare de spam
  - FortiWeb – Web Application Firewall
  - FortiDB – database security
  - FortiClient – HIPS, Antivirus, Firewall, VPN
  - FortiAnalyzer – monitorizare și rapoarte
  - FortiManager – management
  - FortiScan – soluție de management a vulnerabilităților

SRED

Mai multe despre UTM



SRED

Multe echipamente de studiat…

- ...pe ce lucrăm la SRED?

ASA all-in-one security solution

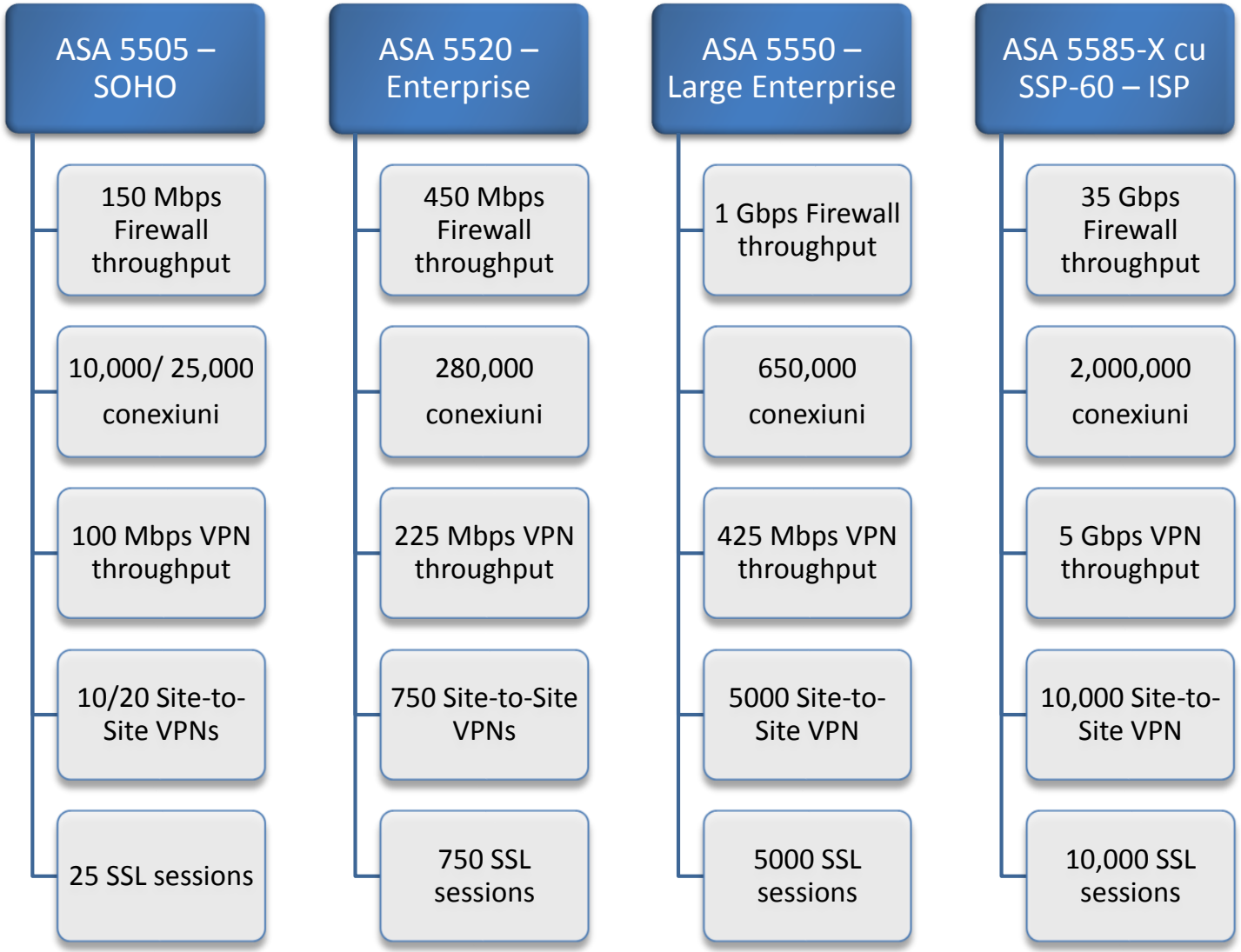
- Firewall
- IPS/IDS (module)
- VPN
- Web Filtering
- AAA
- Antispam/Antivirus (module)
- Content Filtering (module)

FortiGate - UTM

- Firewall
- IPS/IDS
- VPN
- Antispam/Antivirus
- Data Leakage Prevention
- Content/Web Filtering
- WAN Optimization

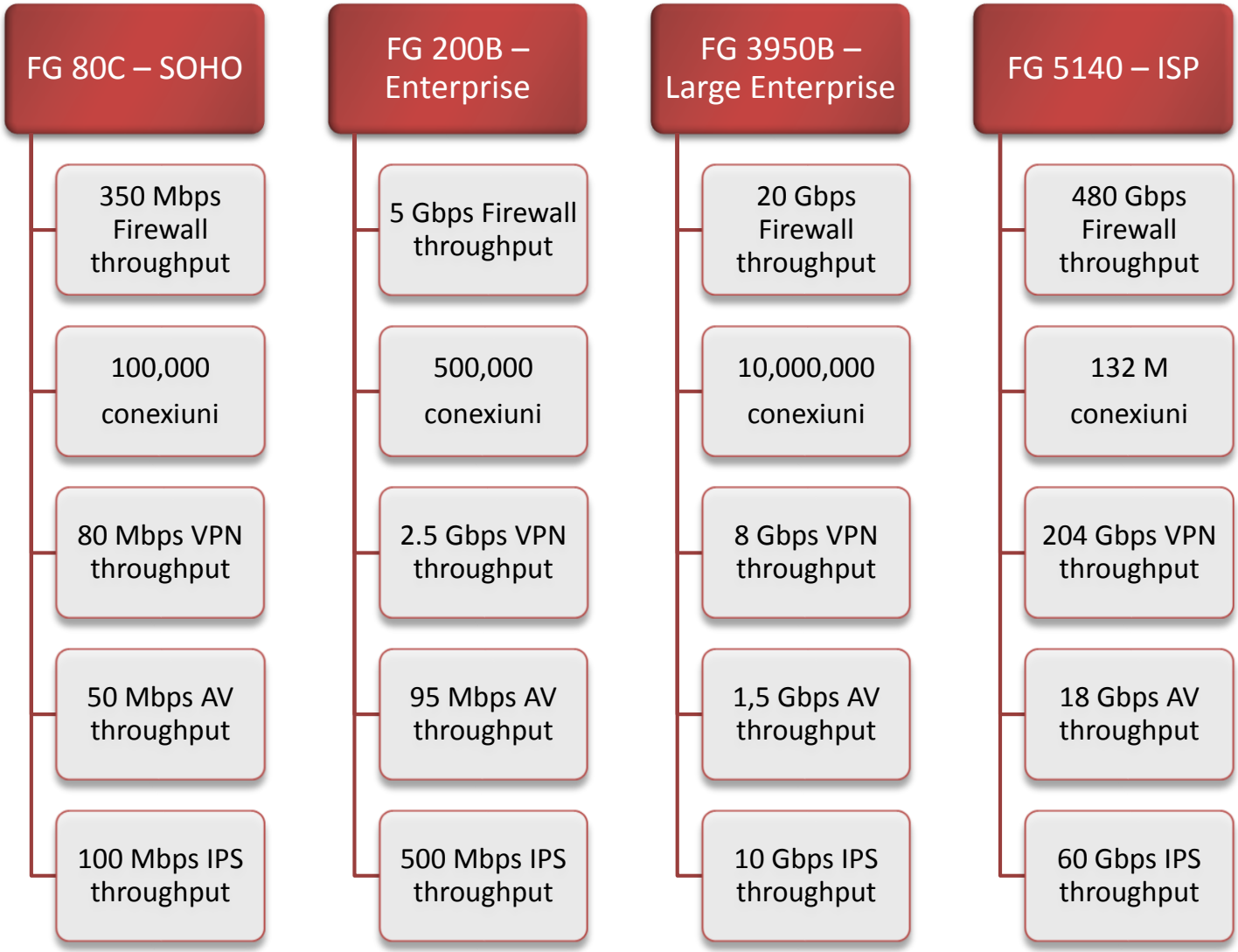
SRED

Cisco ASA – Product range



SRED

Fortinet FortiGate – Product range



SRED

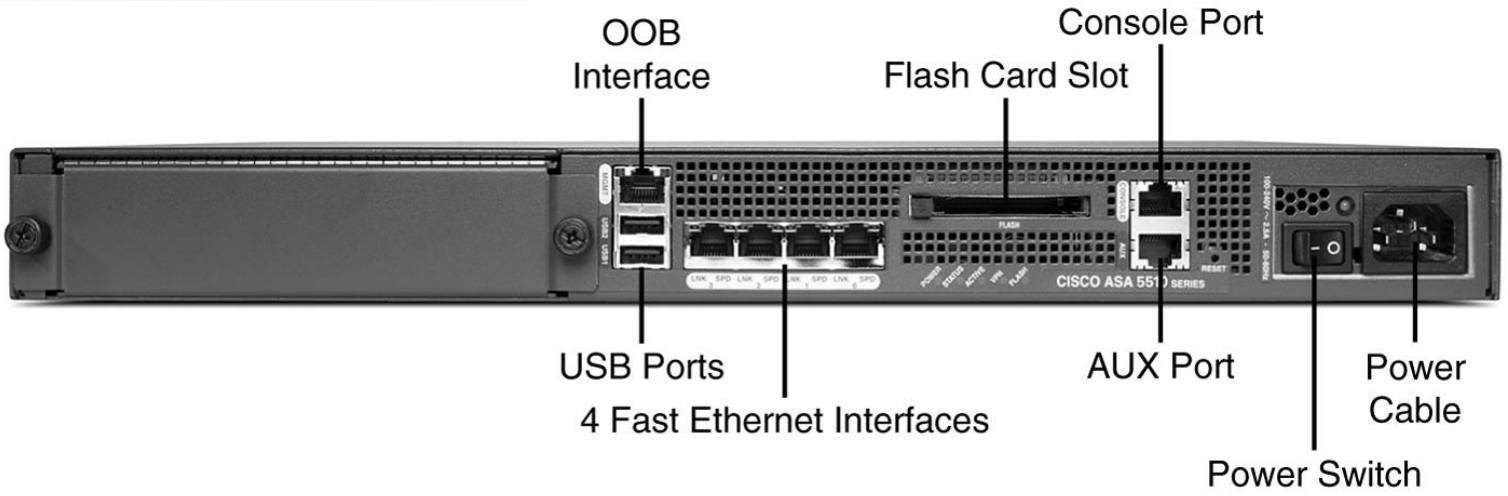
Cu ce lucrăm noi?

- Cisco ASA 5510
- Tech specs
  - 1.6 Ghz Celeron CPU
  - 256 RAM
  - 5 interfețe 10/100 Mbps
  - 64 MB flash
  - 50,000/130,000 conexiuni
  - 2/250 SSL VPNs
  - De ce se folosește CPU general-purpose?
  - De ce frecvența procesului este una mare?
- Module suportate
  - AIP-SSM-10/20 – 150/300 IPS throughput
  - CSC-SSM – adaugă suport Antivirus
  - Modul 4 Gigabit Ethernet

SRED

Cisco ASA 5510 -

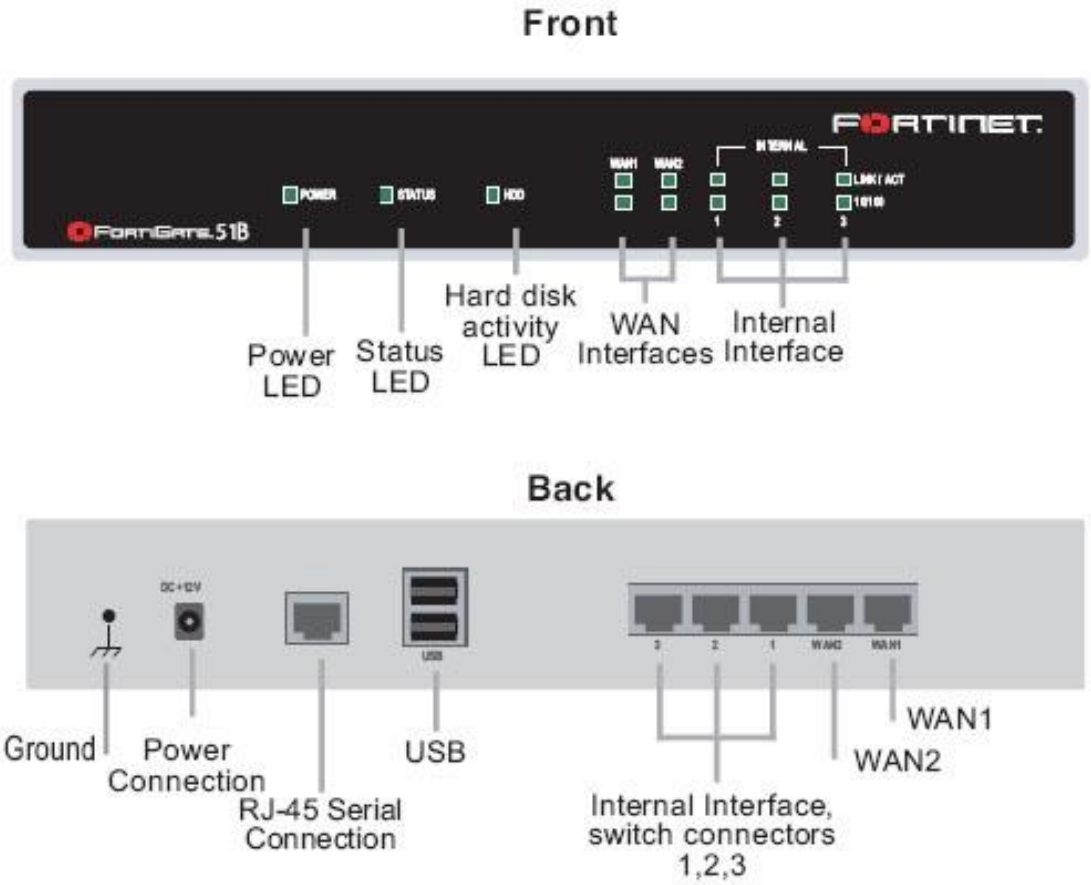
- Portul OOB poate fi configurat ca port normal
- Modulul de Fa poate fi înlocuit cu unul de GB
- Porturile USB sunt “reserved for future use”



SRED

Fortinet

- FortiGate 50/51B
- Tech specs
  - 50 Mbps FW throughput
  - 48 Mbps VPN throughput
  - 19 Mbps AV throughput
  - 30 Mbps IPS throughput
  - 25,000 conexiuni
  - 35 GB SSD
- FortiAnalyzer 100C
  - 200 loguri/sec
- Denumire: A/B/C
  - Cât de nouă este generația dispozitivului din punct de vedere hardware și software



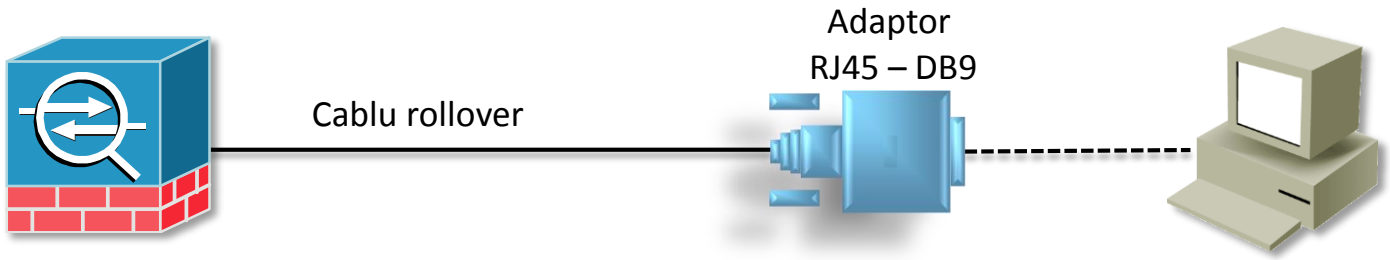
SRED

Device UI – Cisco ASA

ASA 5510

- Accesul la ASA se poate face prin:
  - CLI
  - GUI (ASDM)
- Accesul se poate realiza prin:
  - Consolă
  - Telnet/SSH
  - HTTPS (ASDM)

Parametri consolă	Valoare
Baud rate	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	Hardware

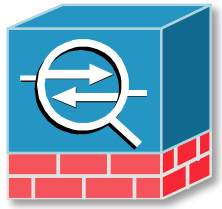


- Echipamentul nu are IP în mod implicit astfel încât prima configurare trebuie făcută prin consolă

SRED

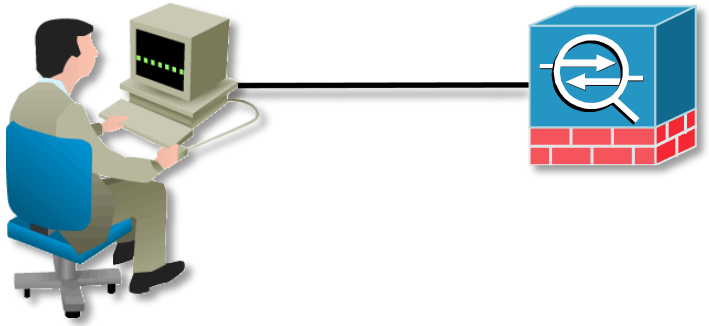
ASA OS

- Laborator se va concentra pe CLI
- Cisco încearcă să uniformizeze OS-ul
  - Vă amintiți Catalyst OS?
  - Cunoștințele de IOS or să fie utile
- Aceeași structură modulară a IOS
  - Unprivileged mode
    - Drepturi limitate
  - Privileged mode
    - Utilizat în general pentru comenzi “show”
  - Global configuration
    - Utilizat pentru configurații “generale” (e.g parolă pentru modul priviledged, rute statice, bannere, configurare hostname)
  - Submoduri de configurare
    - Utilizate pentru configurări avansate (firewall, VPN, protocoale de rutare)



```
ciscoasa>
ciscoasa#
ciscoasa(config)#
Ciscoasa(config-if)#
```

Navigare în OS



```
ciscoasa>enable 15
Password:
ciscoasa#configure terminal
ciscoasa(config)#interface fa0/1
ciscoasa(config-if)#exit
ciscoasa(config)#exit
ciscoasa#exit
ciscoasa>
```

- Parola default este …?
  - CR + LF

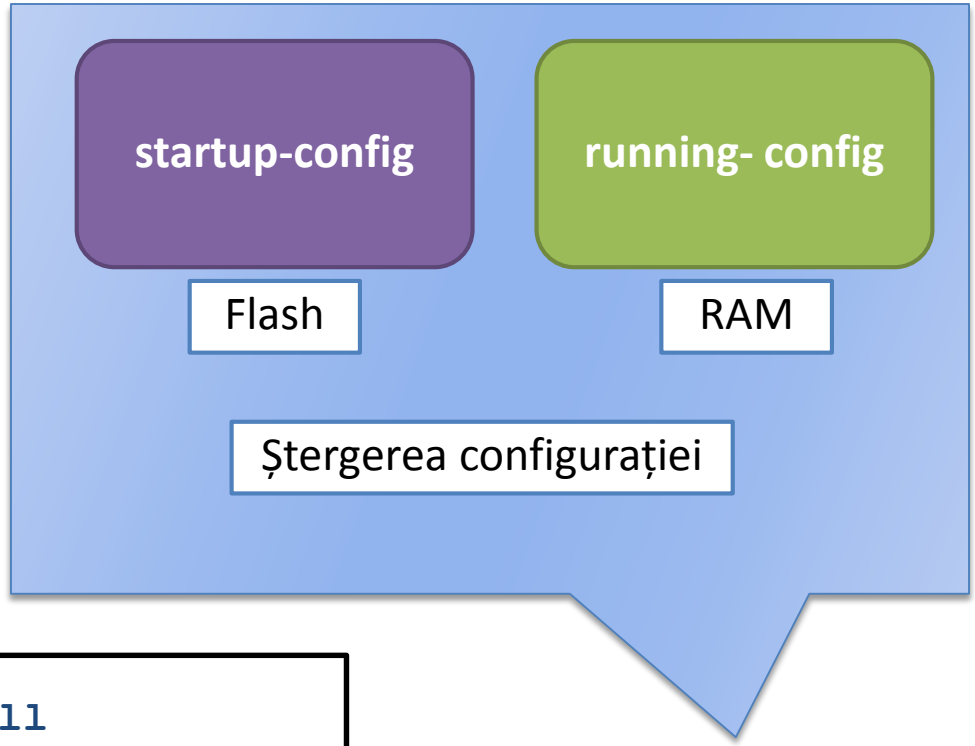
Help în ASA OS


```
ciscoasa > ?
  enable    Turn on privileged commands
  exit      Exit the current command mode
  login     Log in as a particular user
  logout    Exit from current user profile to unprivileged mode
  perfmon   Change or view performance monitoring options
  ping      Test connectivity from specified interface to an IP
            address
  quit      Exit the current command mode

ciscoasa > help enable
  USAGE:
        enable [<priv_level>]

  DESCRIPTION:
  enable            Turn on privileged commands
```


SRED

Lucrul cu sistemul de fișiere

- Mai întâi ștergem… 😐




```
ciscoasa# clear configure all
```

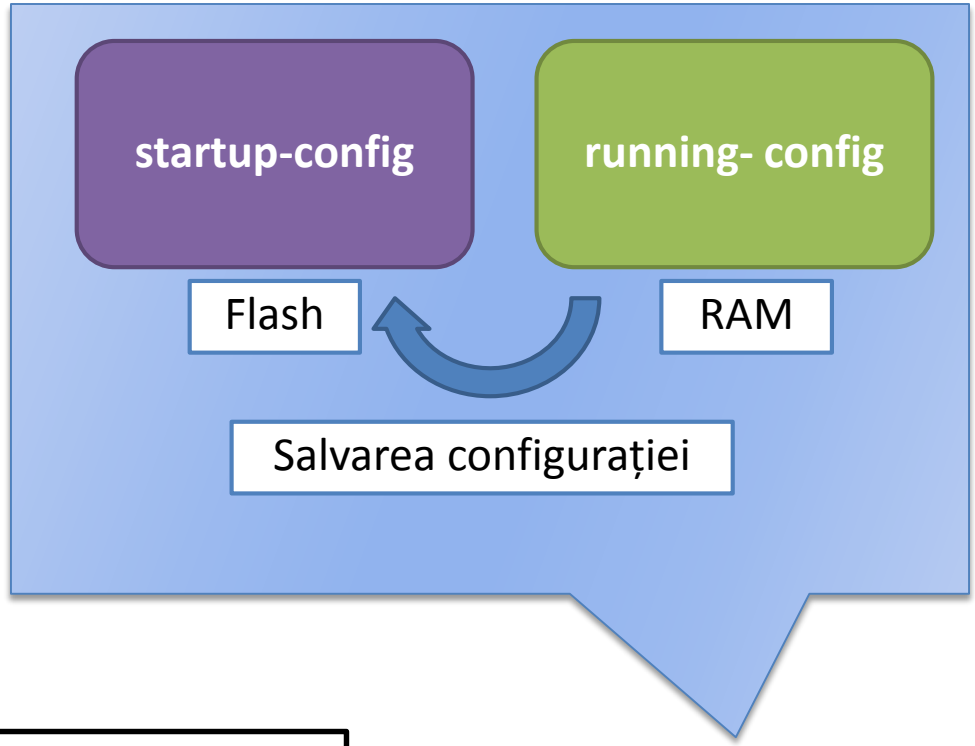
```
ciscoasa# write erase
```


SRED

Lucrul cu sistemul de fișiere (2)

- Apoi salvăm ☺

```
ciscoasa# show running
ciscoasa# show startup
```




```
ciscoasa# copy running startup
ciscoasa# write mem
ciscoasa# wr
```


SRED

Comanda `clear configure`

- Nu există în IOS (pe rutere)
- Permite inclusiv ștergerea granulară a configurațiilor din RAM

```
ciscoasa(config)# show running-config | include isakmp
isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400

ciscoasa(config)# clear configure isakmp
ciscoasa(config)# show running-config | include isakmp
```

Alte comenzi utile

- Configurarea hostname-ului

```
ciscoasa(config)# hostname sredasa
sredasa(config)#
```

- Configurarea unei parole pentru linia de telnet

```
sredasa(config)# passwd cisco
```

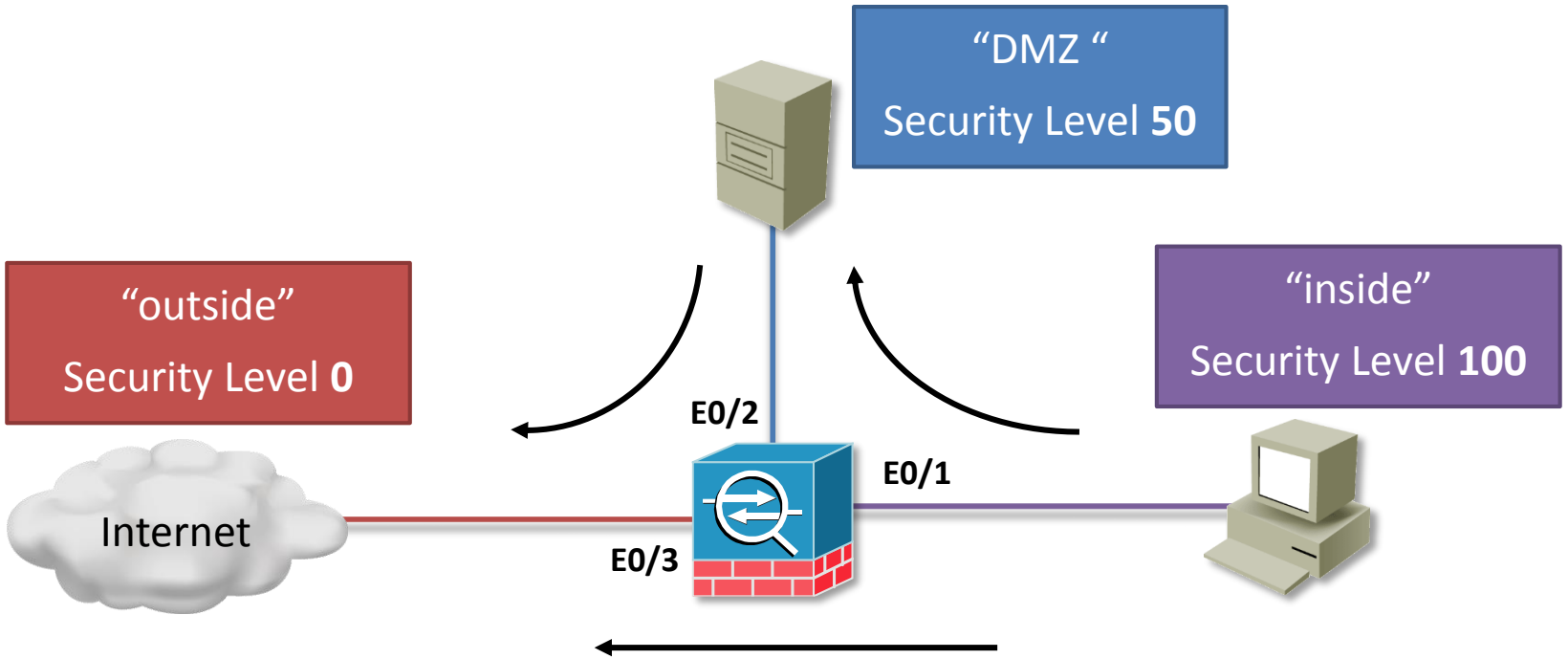
- Configurarea unei parole pentru modul privileged. Cum se configura aceasta pe rutere?

```
sredasa(config)# enable password cisco
sredasa# sh run | i pass
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
```

Nivele de securitate ASA

- Pentru a putea trece trafic între 2 interfețe ale unui ASA, trebuie să fie definite nivelele de securitate pentru fiecare din acestea.
- Nivelele de securitate reprezintă cel mai simplu model de stateful firewall pe care ASA îl oferă.
- Pachetele sunt inspectate atunci când traversează dispozitivul de la o interfață cu nivel de securitate mare, la o interfață cu nivel de securitate mic
- Pachetele ce încearcă să treacă de la un nivel de securitate mic la un nivel de securitate mare sunt blocate în mod implicit
- În afară de nivele de securitare, orice interfață are nevoie de un “nume” care este ulterior referit în orice altă comandă

Exemplu nivele de securitate

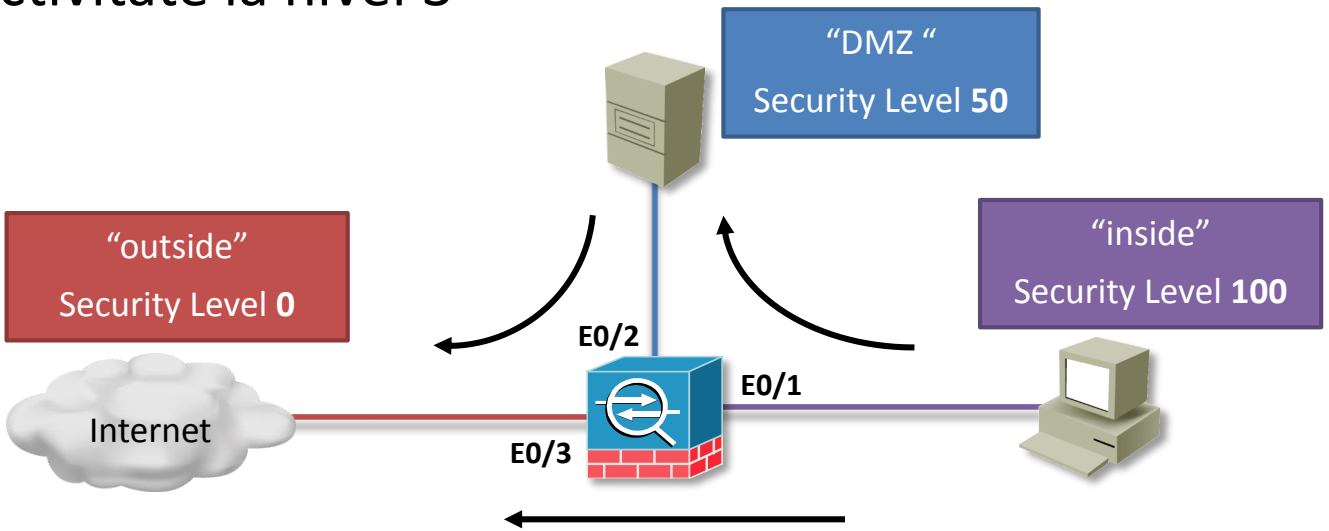


- Configurarea nivelului de securitate are loc în modul de configurare al interfeței

SRED

Configurarea numelor interfețelor

- O interfață ASA fără nume și nivel de securitare configurat nu are conectivitate la nivel 3

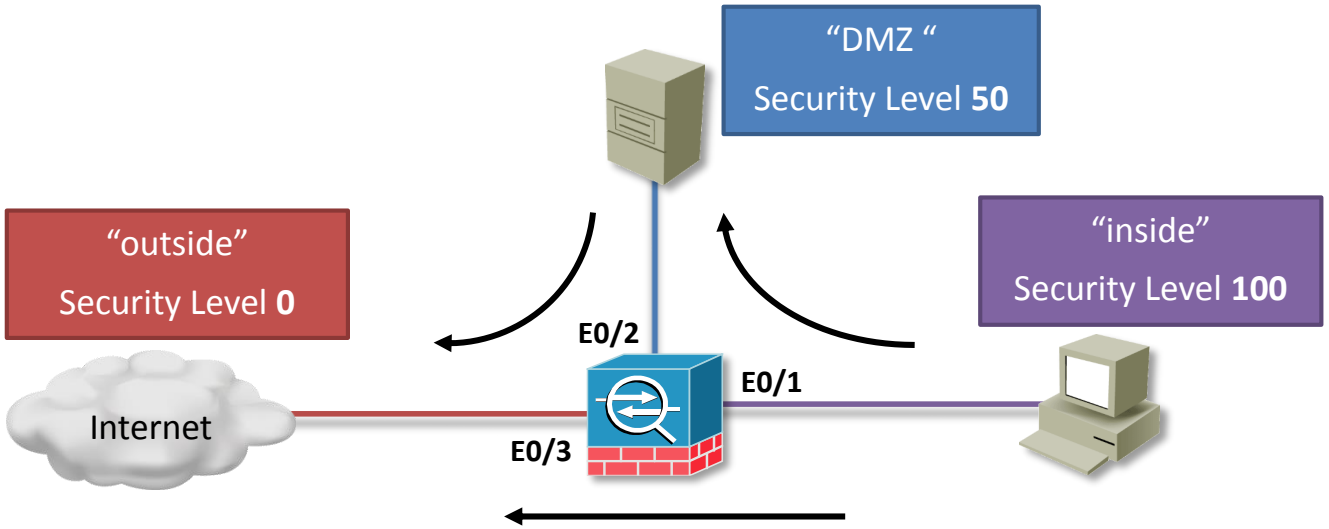



```
ciscoasa(config)#interface e0/1
ciscoasa(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)#ip address 192.168.1.1 255.255.255.0
```


SRED

Configurarea nivelelor de securitare

- Se poate customiza folosind comanda **`security-level`**




```
ciscoasa(config)#interface e0/1
ciscoasa(config-if)#nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
ciscoasa(config-if)#security-level 50
ciscoasa(config-if)#ip address 192.168.2.1 255.255.255.0
ciscoasa(config-if)#no shutdown
```


SRED

ASA – acces de la distanță prin telnet

- În mod implicit accesul este restricționat

```
sredasa(config)# telnet 10.10.0.0 255.255.255.0 inside
sredasa(config)# telnet timeout 10
sredasa(config)# passwd sred!@#
```

- Dacă nu se setează o parolă, implicit este "**cisco**"
- Accesul prin telnet pe interfața outside (security-level 0) nu este permis decât dacă conexiunea telnet vine printr-un tunel IPSec
- Monitorizarea conexiunilor

```
sredasa# who
0: 10.10.0.132
sredasa# kill 0
sredasa# who
```

ASA – acces de la distanță prin SSH

- Permis pe orice interfață
- Pasul 1: generarea cheilor

```
sredasa(config)# crypto key generate rsa  modulus 1024
WARNING: You have a RSA keypair already defined named
<Default-RSA-Key>.
Do you really want to replace them? [yes/no]: yes
Keypair generation process begin. Please wait...
```

- Pasul 2: activare SSH

```
sredasa(config)# ssh 141.85.37.0 255.255.255.0 outside
sredasa(config)# ssh version 2
sredasa(config)# ssh timeout 10
```

- Utilizatorul implicit este “pix” și parola sunt configurați cu comanda **`passwd`**

Comenzi **show**

- Configurația unei anumite interfețe


```
asa1# show run interface E0/3
 interface Ethernet0/3
 speed 10
 duplex full
 nameif outside
 security-level 0
 ip address 192.168.3.1 255.255.255.0
```

- Numele și nivelele de securitate

```
asa1# show nameif
Interface                      Name                      Security
GigabitEthernet0/0             outside                      0
GigabitEthernet0/1             inside                     100
GigabitEthernet0/2             dmz                         50
```


SRED

Comenzi **show** (2)

- Toți parametrii unei interfețe

```
asa1# show interface
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
        Full-Duplex(Full-duplex), 100 Mbps(100 Mbps)
        MAC address 0013.c482.2e4c, MTU 1500
        IP address 192.168.1.2, subnet mask 255.255.255.0
        8 packets input, 1078 bytes, 0 no buffer
        Received 8 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (8/0) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
  Traffic Statistics for "outside":
        8 packets input, 934 bytes
        0 packets output, 0 bytes
        8 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
```


SRED

Comenzi **show** (3)

- Ce comandă IOS se folosea pentru a vedea rapid statusul interfețelor și adresele IP?
  - **show ip interface brief**

- La ASA e ușor asemănătoare
  - **show interface ip brief**

```
sredasa(config)# sh int ip br
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                192.168.1.1     YES manual up                    up
Ethernet0/1                10.10.1.1       YES manual up                    up
```


SRED

Lucrul avansat cu comanda show

- IOS Q: se putea da o comandă show în modul global de configurare?
  - A: da, folosind argumentul “do” în fața comenzii

```
normal_cisco_router(config)#do show clock
*15:08:07.867 UTC Thu Feb 17 2011
```

- În ASA OS nu există “do” dar…
  - … se pot da comenzi show de oriunde (deocamdată)

```
sredasa(config-if)# sh clock
15:54:01.139 UTC Thu Feb 17 2011
```

- Există posibilitatea filtrării outputului folosind “|” și argumentele “i”, “b”, “grep” (mai multe la laborator…)

Device UI – Fortinet FortiGate

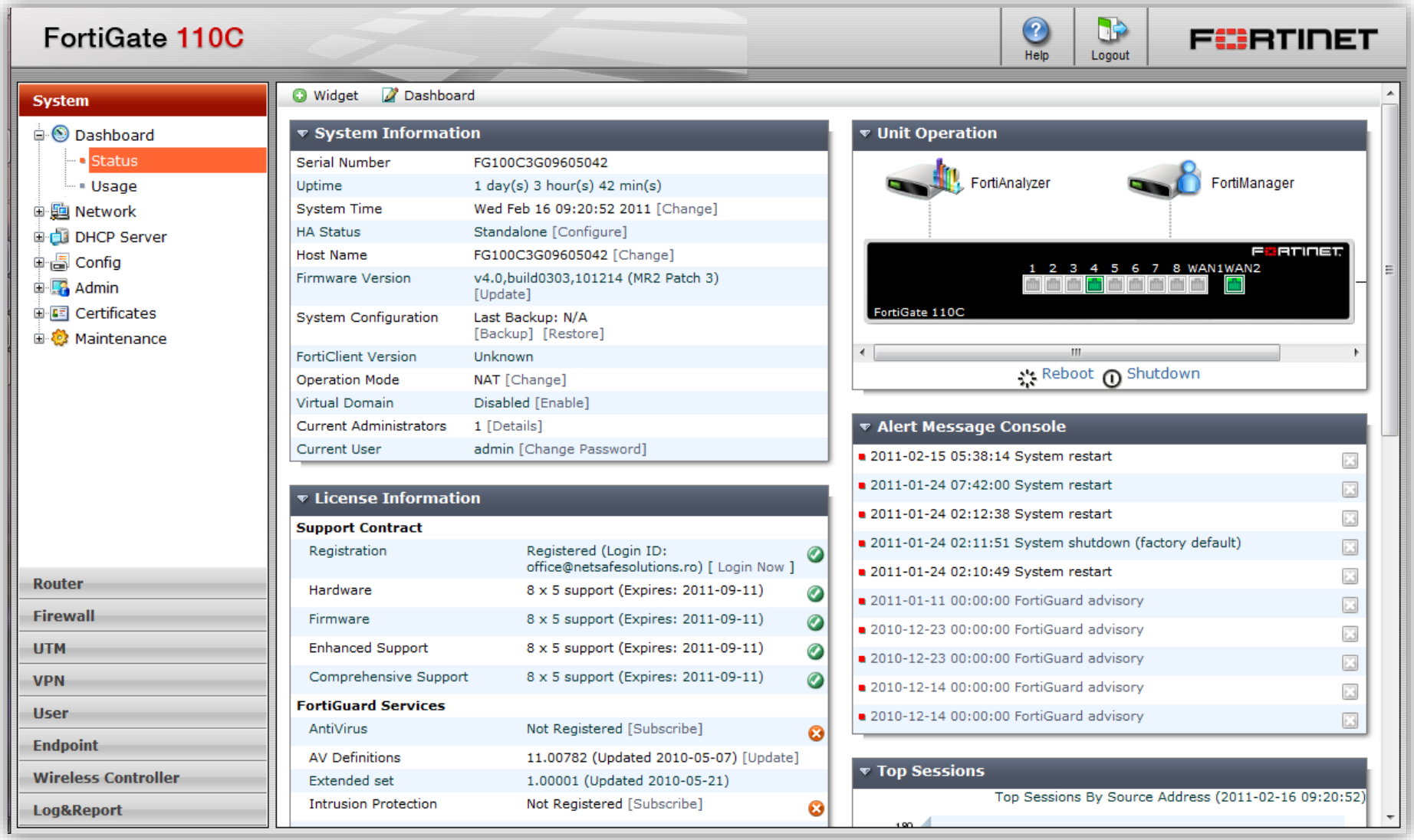
Fortigate - FortiOS

- Construite pentru a fi 90% configurabile prin interfața Web
  - Interfață dinamică, ergonomică și intuitivă
  - Construită în AJAX
- CLI pentru debug și configurații avansate
- Versiunea curentă 5.01 patch release 1
  - MR – versiuni minore ce apar anul și intermediază un release major
  - Include atât bug-fixuri cât și funcționalități noi
- Configurate deja cu un IP de management pentru interfețele LAN (inside)
  - 192.168.1.99
- Port de consolă pentru … momentele dulci de lockout

Fortigate - firewall

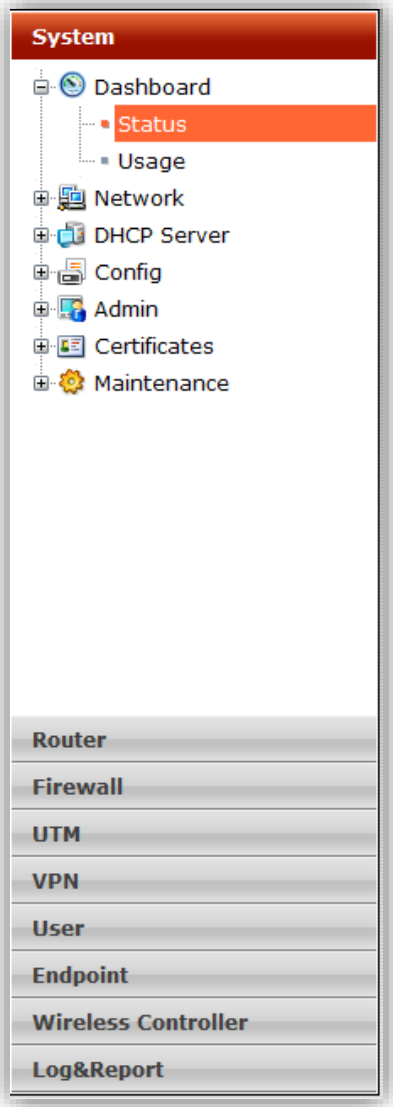
- Firewall-ul de pe Fortigate este foarte asemănător conceptual cu ZPF din IOS
- Pentru ca traficul sa poată traversa dispozitivul, este nevoie de o politică de firewall de la o zonă/interfață sursă la o zonă/interfață destinație
  - O zonă poate fi compusă din una sau mai multe interfețe
- Orice altă funcționalitate a UTM-ului este atașată politicii (senzor IPS, profil AV, tunel IPSec)
- Acțiunile posibile ale unui politici de firewall:
  - Accept (se creează un obiect de stare pentru conexiuni)
  - Deny
  - IPSec

Interfața WEB



SRED

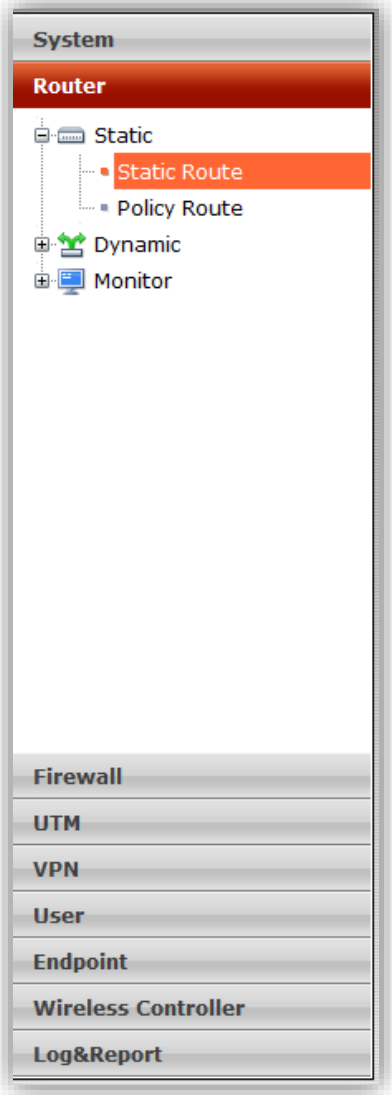
Structura UI – System



- System
  - Status și informații legate de UTM (widgets)
  - Configurarea interfețelor
  - Configurarea zonelor de securitate (remember ZPF?)
  - Web Proxy
  - DHCP/DNS Server
  - High-availability
  - SNMP Agent
  - Definirea conturilor de administratori
  - Certificate digitale
  - Licențiere (FortiGuard push updates)

SRED

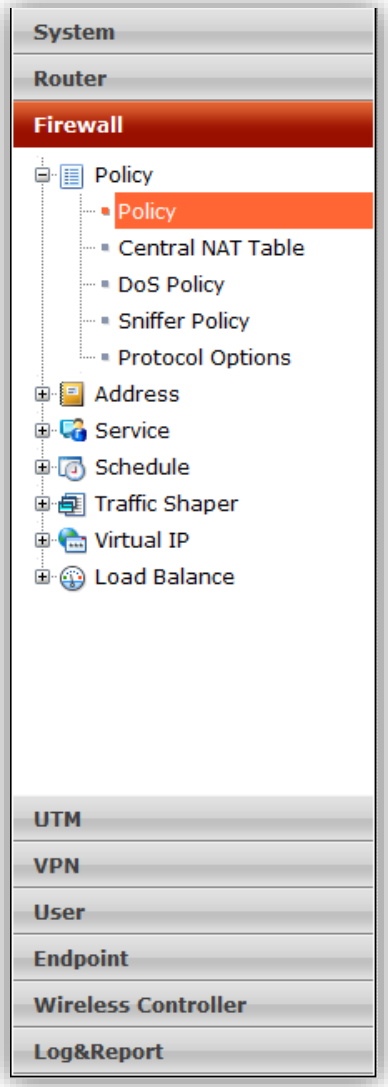
Structura UI – Router



- Router
  - Rute statice
  - Policy based routing
  - Protocoale de rutare
    - RIP
    - OSPF
    - Full-BGP
    - IPv4/v6 Multicast

SRED

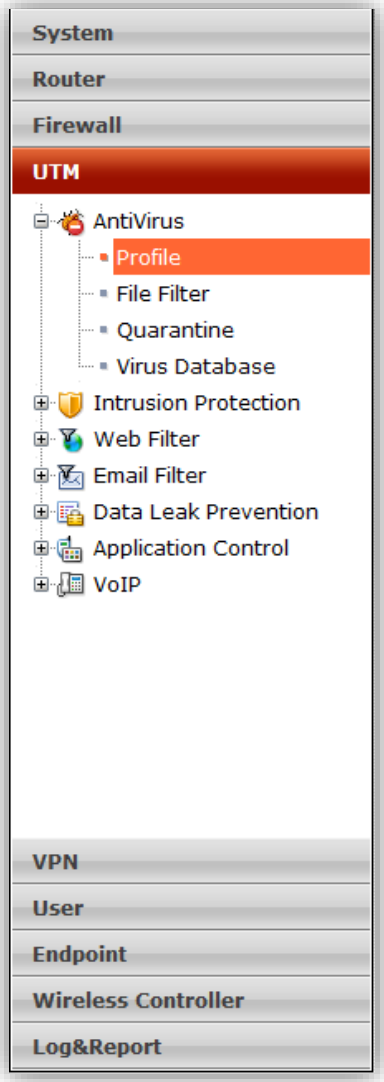
Structura UI – Firewall



- Firewall
  - Politici de firewall
    - Foarte importante – toate celelalte funcții se activează în jurul acestor politici
  - Configurarea senzorului DoS
  - Configurare liste de adrese/servicii (object grouping la ASA)
  - Traffic shaping
  - Virtual IP
    - Ce reprezintă acest concept?
    - Port forwarding
  - Load balancing
    - Către servere din interiorul rețelei
    - Mapare Virtual server <-> Real servers

SRED

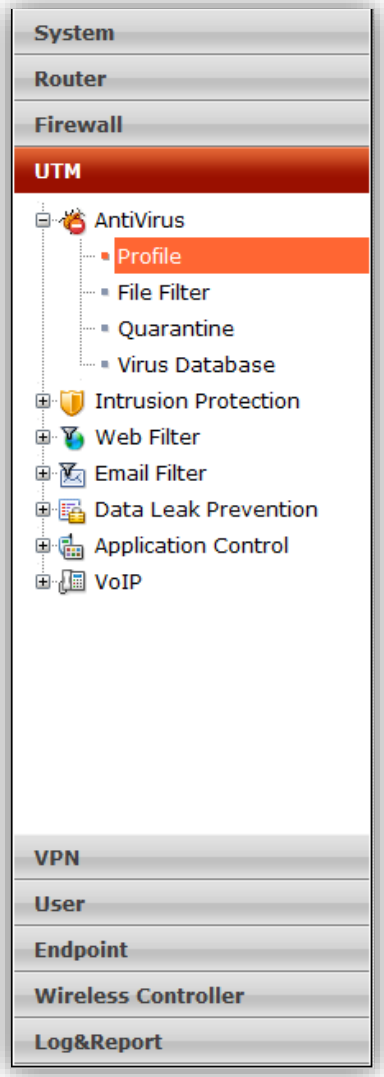
Structura UI – UTM



- UTM
  - Antivirus
    - Profile de scanare
    - Filtrarea fișierelor după extensie sau cu recunoaștere automată a tipului
    - Updatare a bazei de date prin push (Fortiguard)
  - IPS
    - One-arm IDS – funcționare cu un port SPAN al unui switch
    - Definirea de senzori IPS
      - Protocoale
      - Acțiuni
      - Severitate

SRED

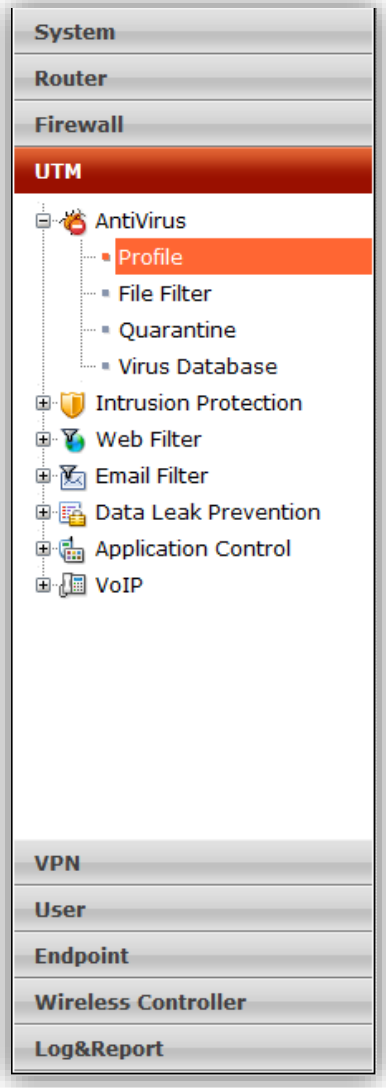
Structura UI – UTM (2)



- UTM
  - Web Filter
    - Bază de date internă
      - Limitată
      - Suport pentru expresii regulate
    - Bază de date externă
      - Varianta recomandată (there are a lot of xxx URLs out there)
  - Email Filter
  - Data Leak Prevention
    - Numere de card
    - String-uri custom (Example: “my boss sucks”)
    - Se poate loga toata informația din rețea – CPU intensive

SRED

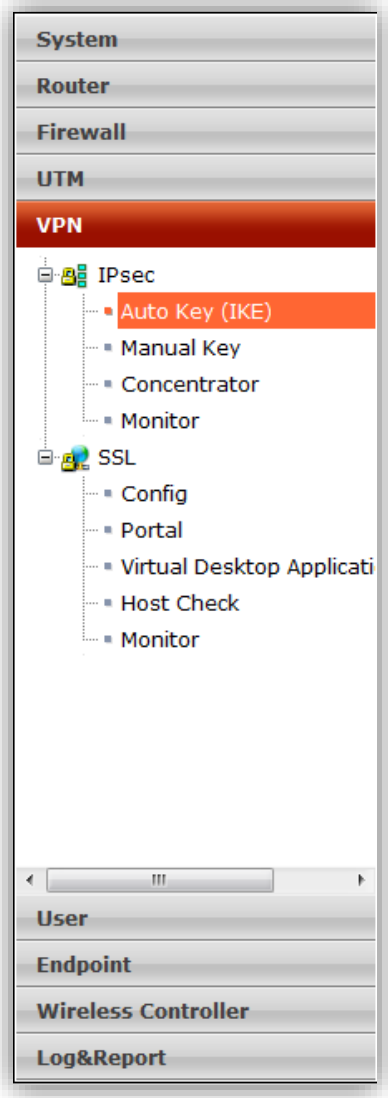
Structura UI – UTM (3)



- UTM
  - Application Control
    - Inspecție la nivel aplicație pentru a recunoaște protocoale p2p, torrent ,etc.
  - VoIP
    - SIP: limitarea cererilor de înregistrare
    - SIP: limitarea cererilor de invite
    - SCCP: limitarea procesului de Call Setup (Calls/min/client)

SRED

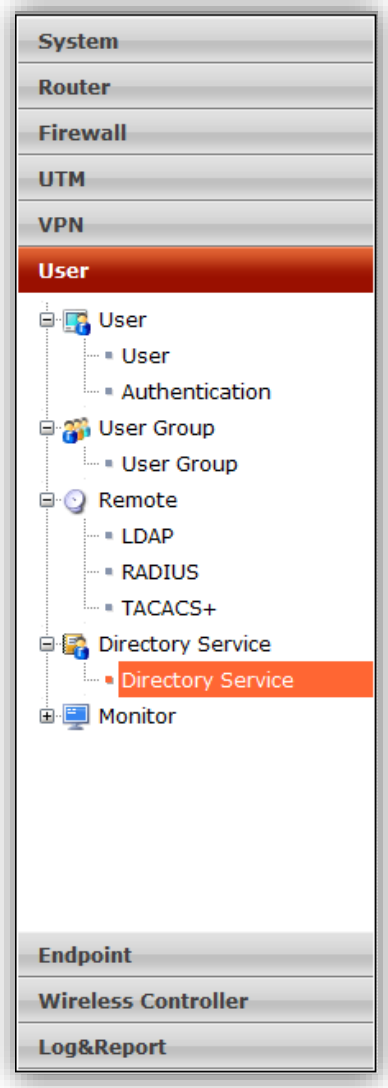
Structura UI – VPN



- VPN
  - IPsec
    - Suport pentru transmiterea de trafic multicast peste tunel
    - Interface mode și routed mode
  - SSL
    - Portal customizabil de administrator și de fiecare client în parte
    - SSL Offloading – Fortigate-ul poate decripta traficul SSL și să îl trimită în rețeaua locală decriptat
    - Avantaje SSL Offloading
      - economisirea puterii de procesare pe server
      - Posibilitatea de a inspecta traficul SSL

SRED

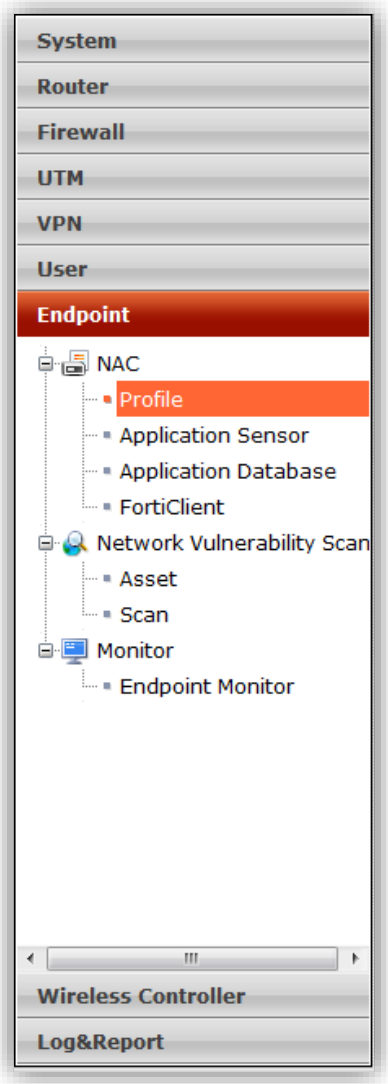
Structura UI – User



- User
  - Definirea de utilizatori
  - Definirea de grupuri de utilizatori
  - Definirea de servere remote folosite pentru autentificare (LDAP, RADIUS, TACACS+)
  - Directory Service – SSO
    - Se poate implementa Single Sign-on pentru orice utilizator din Windows Active Directory folosind un server Microsoft FSAE
    - Odată autentificați în FSAE, utilizatorii sunt autentificați pentru orice serviciu de pe firewall (Ex: cut-through proxy)

SRED

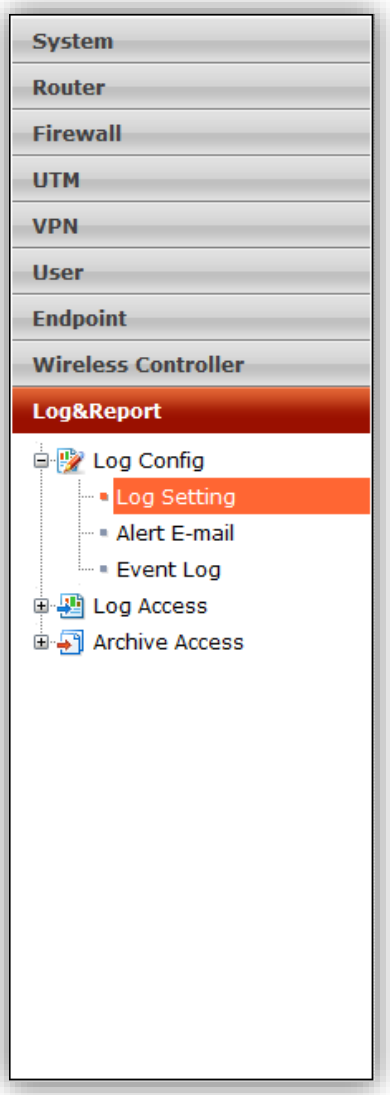
Structura UI – Endpoint



- Endpoint
  - Network Access Control
    - Recomandat împreună cu autentificare la nivel 2 folosind 802.1x și un server Radius
    - NAC controlează drepturile pe care un utilizator le are în rețea odată ce a fost autentificat funcție de profilul stației cu care accesează rețeaua
    - Profilul stației este definit de aplicații (prezența unui AV), funcționalități ale OS-ului (firewall activat) și versiuni ale programelor(patch-uri, update-uri etc)
    - Este nevoie de FortiClient pe fiecare stație
  - Scanare de vulnerabilități
    - Dispozitivul FortiScan complementează funcția aceasta adăugând și push automat de update-uri și patch-uri de securitate prin FortiClient

SRED

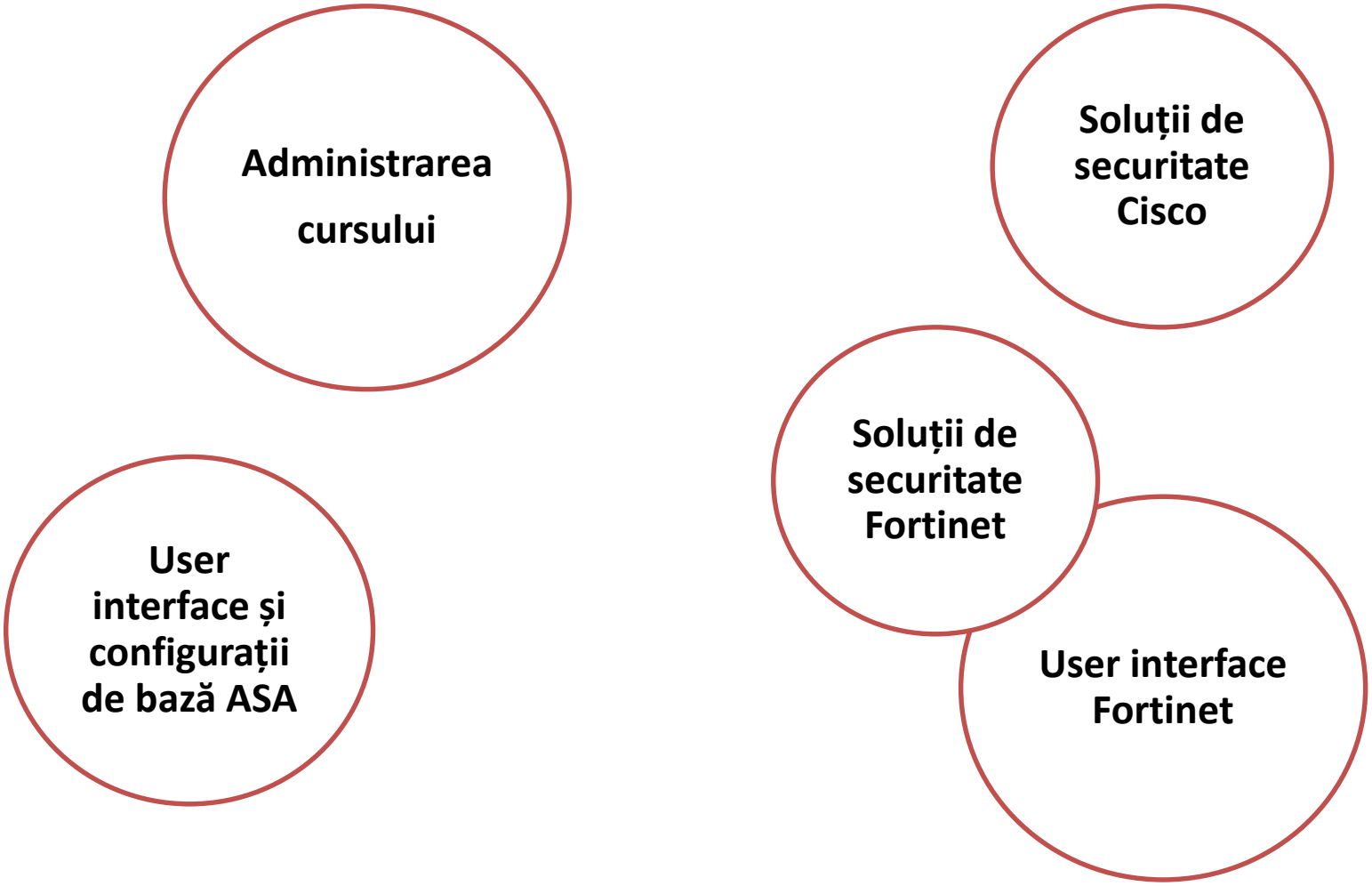
Structura UI – Log & Report



- Log & Report
  - Orice proces de pe firewall poate fi logat
  - Logurile se pot:
    - păstra local pe echipament
      - În memoria flash – spațiu limitat
      - Pe HDD – dacă echipamentul are o unitate de stocare
    - Trimite la un dispozitiv FortiAnalyzer dedicat pentru analiza de log-uri și evenimente și generare de rapoarte

SRED

Overview



SRED

Cursul viitor…

- Firewalls – tipuri, concepte și optimizări de platformă
  - Oh my god it's on fire!!!
- Identity Based Authentication

```
Login:yes
Password:  I don't have one
password is incorrect
Login: yes
Password: incorrect
```

- ASA ACLs
  - deny ip any any; and you're safe.
- Fortigate firewall policies

SRED