High Availability

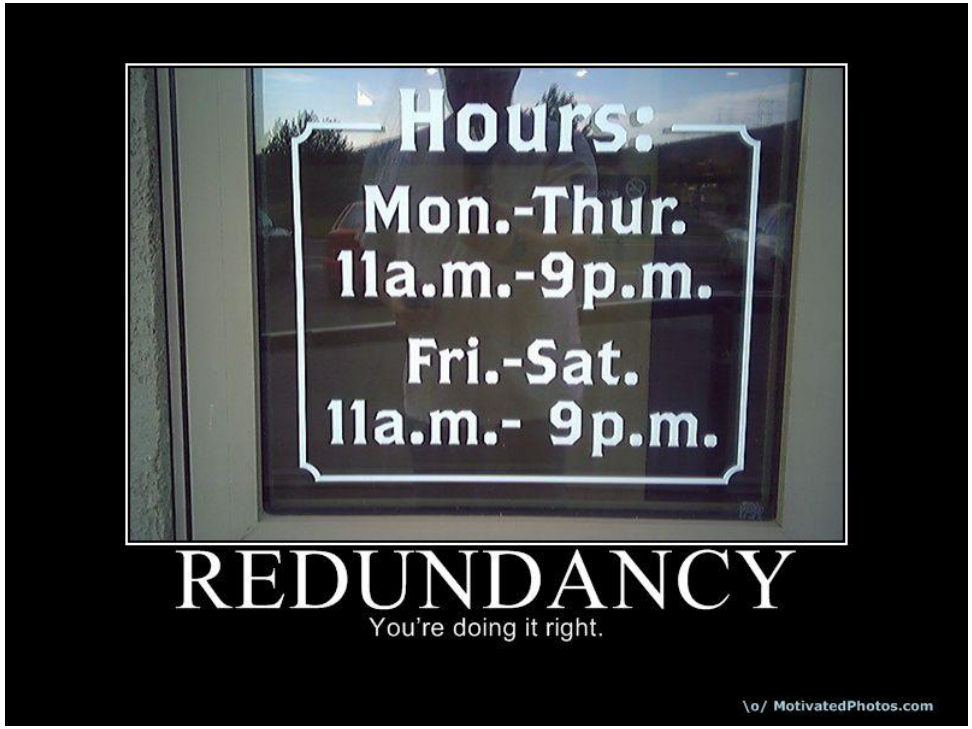
8 Mai 2014

Obiective

- Implementarea redundanței la nivel 2 și 3
- Implementarea redundanței la nivel de firewall
- Cisco ASA
  - Terminologie Cisco HA
  - Topologii HA
  - Condiții de failover
  - Alegerea Active/Standby
  - Configurarea HA și stateful failover
- Fortinet
  - Soluții de HA oferite de Fortinet
  - FGCP – sumar funcționalități
  - Configurarea de bază a unui cluster FGCP

Redundanța

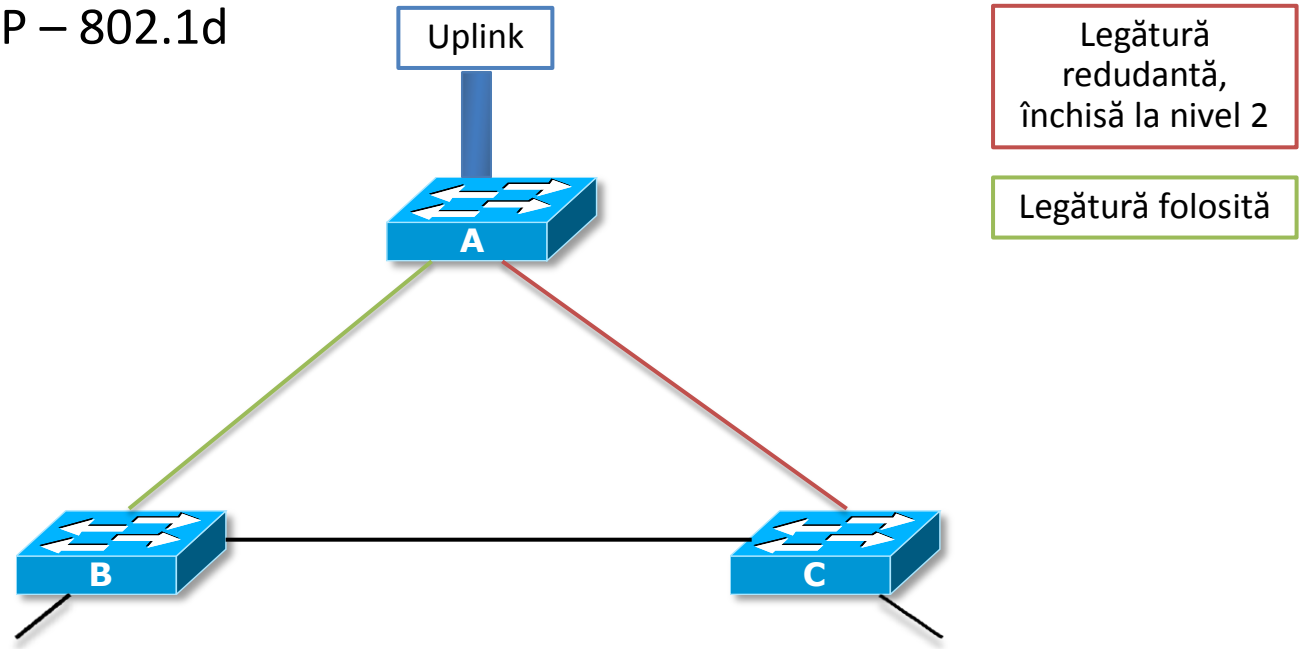
- Necesară la toate nivelele din stiva OSI
  - Nivel 2?
  - Nivel 3?
    - La nivel de rutare
    - La nivel de gateway



SRED

Redundanță la nivel 2

- Protocolul STP – 802.1d

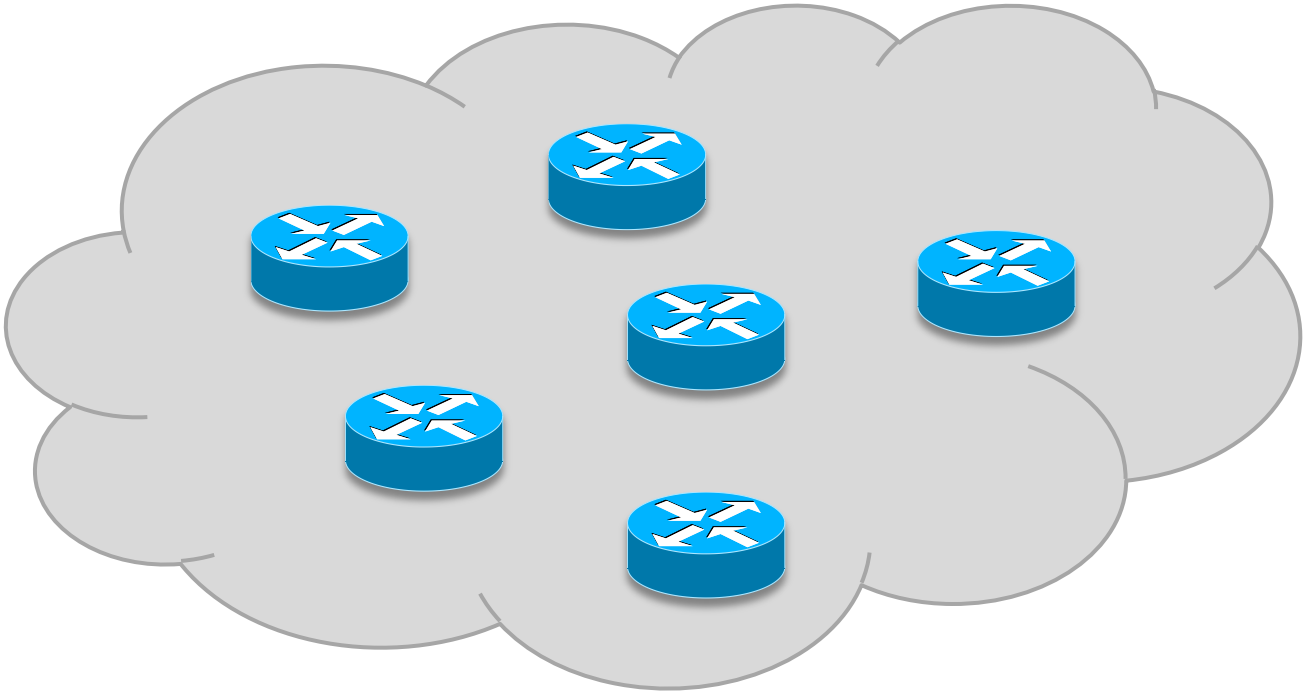


- Legăturile fizice redundante la nivel 2 pot cauza probleme serioase la nivel 2 (broadcast storms)
- Protocolul STP folosește un algoritm pentru a identifica și închide la nivel 2 legăturile redudante
- În caz că legătura principală pică, STP reactivează calea redundantă
- Reconvergență în 6 secunde folosind RSTP

SRED

Redundanță la nivel 3

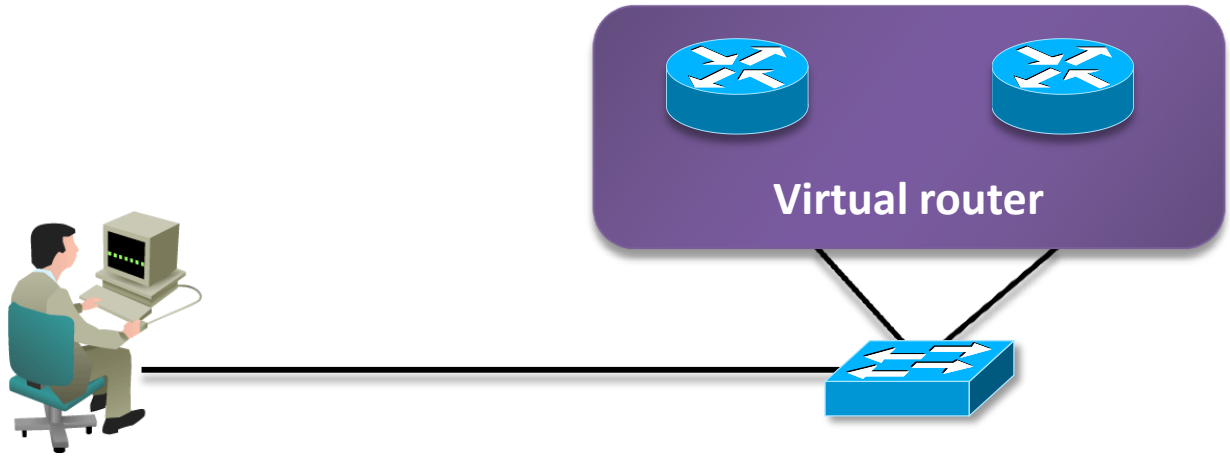
- Pentru determinarea căii prin rețea
  - Nevoie de nivel de redundanță ridicată (Internetul)
  - Protocoale de rutare link-state (Djkstra) sau distance-vector (Bellman-Ford)



- Reconvergență sub-second pentru protocoale link-state (depinde și de designul și configurația rețelei)

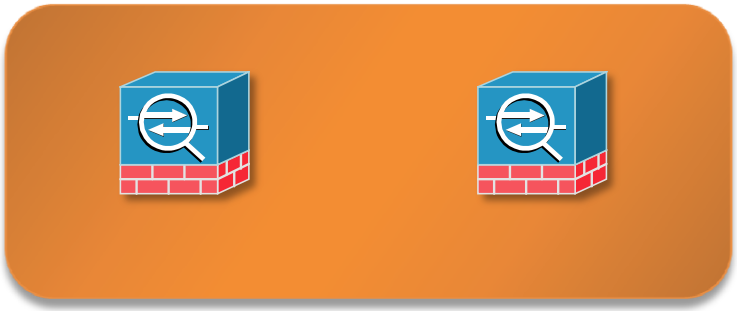
Redundanță la nivel de gateway

- Oferă failover în cazul în care gateway-ul fizic pică
  - Sunt folosite două sau mai multe rutere într-un cluster (ruter virtual)
  - Clusterul are un IP și un MAC virtual pe care fiecare ruter din cluster primește pachete
  - Funcție de protocolul folosit, toate ruterele pot fi active într-un moment de timp (load-balancing) sau doar unul dintre ele (Master/Slave failover)
  - Există și posibilitate de a face track pe statusul uplink-ului oferit de gateway și a face failover bazat pe disponibilitatea acestuia



SRED

Redundanță la nivel de firewall



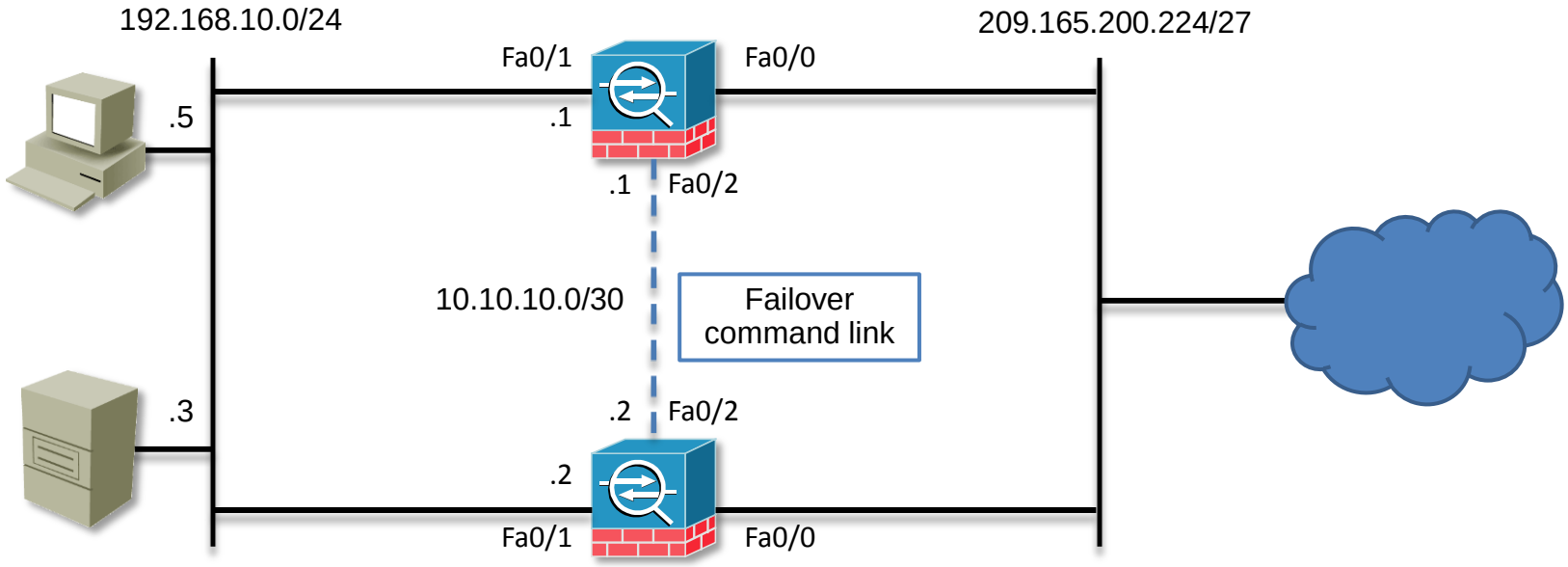
- În multe topologii securizate cu un firewall, acesta devine noul gateway al rețelei
- Funcționalități comune cu protocoalele de gateway high-availability (VRRP, HSRP, GLBP)
- Ce funcționalități suplimentare ar avea sens?
  - Sincronizarea configurațiilor de pe cele două firewall-uri
  - Sincronizarea tabelei stateful
  - Sincronizarea tabelei NAT

Cisco ASA - High Availability

ASA HA

- Soluția ASA HA este concetrată pe failover
- Unul din dispozitive este *active*, celălalt *standby*
- Sunt permise doar 2 ASA într-o configurație de HA
- Este nevoie de următoarele configurații hardware identice:
  - Modelul ASA
  - Versiunea de software (condiție ușor relaxată pentru ultimele OS-uri)
  - Dimensiunea memoriei flash
  - Dimensiunea RAM-ului
  - Existența aceluiași set de funcționalități (un base set nu va crea HA cu un VPM Premium set)
  - Numărul și tipul interfețelor să fie același

Topologie ASA HA

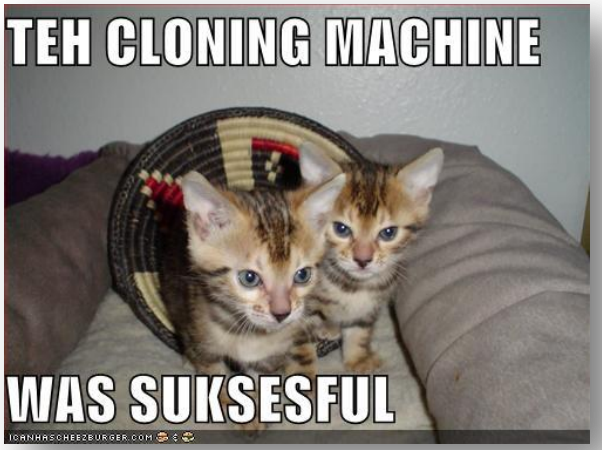


- Pentru funcționarea HA, este nevoie de un link dedicat de comandă peste care se transmit:
  - Starea ASA (Active sau Standby)
  - Mesaje de hello (o dată la 1 secundă pe ASA; o dată la 15 secunde la PIX)
  - Schimbul de adrese MAC
  - Sincronizarea de configurații

SRED

Replicarea configurațiilor

- Orice configurație, inclusiv cele inițiale trebuie realizate pe ASA Active
- Unitatea standby se sincronizează prin conexiunea de comandă cu unitatea activă:
  - Când ASA-ul standby bootează SO-ul
    - este recomandat ca în configurare, mai întâi să se configureze unitatea primară și apoi să fie pornită cea standby
  - Când se realizează o modificare pe ASA-ul Active în running-config
  - Când se dă comanda **`write standby`**
- Atenție, sincronizarea se face între RAM-uri
  - Comanda **`write memory`** e foarte importantă pe unitatea Activă



SRED

Condiții care provoacă failover

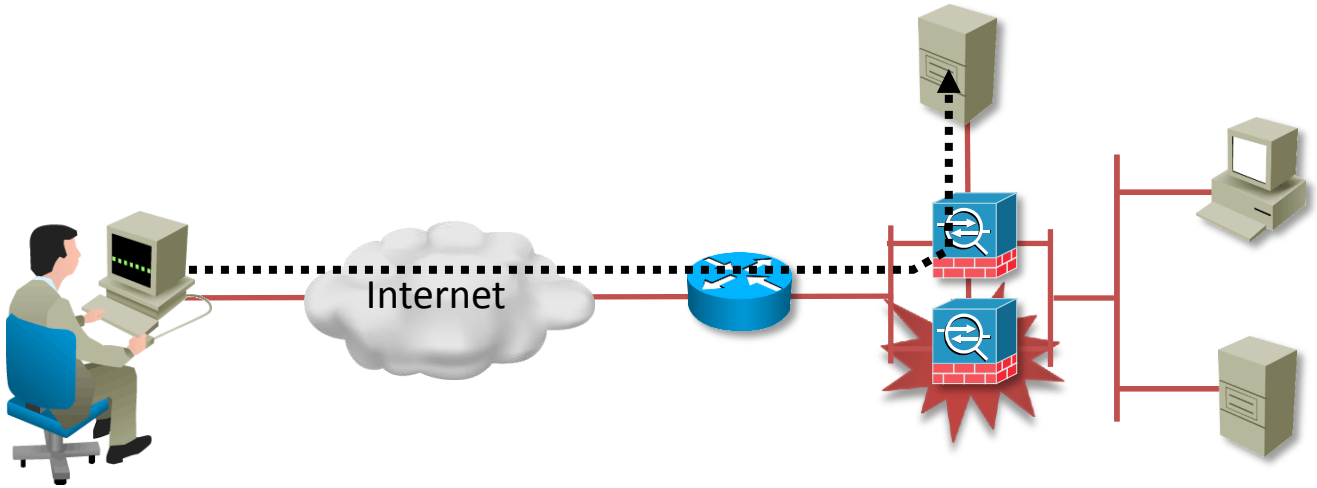
- 1: când un administrator trece manual un ASA din modul active în standby
- 2: pierderea de curent electric pe ASA activ
- 3: network/hardware failure
  - Dacă unitatea standby nu primește răspuns la 2 hello-uri consecutive sau pentru un maxim de 30 secunde, începe o serie de teste pentru a verifica dacă există conectivitate pe alte interfețe cu ASA-ul vecin în afară de cea de comandă

SRED

Teste de failover

- Pentru a detecta pierderea de conectivitate, ASA execută o serie de teste pentru a fi sigur că există un failure
  - Link up/down test: se verifică dacă portul remote este UP folosindu-se niște mesaje de tip Probe. Dacă portul este UP și nu este vorba de un failure de nivel 1, se trece la următorul test.
  - Network activity test: în acest test ASA numără toate pachetele primite timp de 5 secunde. Dacă nu a primit nici un răspuns, trece la testul următor.
  - ARP test: ASA citește ultimele 10 intrări din tabela ARP și trimite pentru fiecare dintre ele un ARP Requst, așteptând 5 secunde pentru un răspuns. Dacă nu s-a primit nici un răspuns, se trece la următorul test.
  - Broadcast ping: se trimite un broadcast ping pe interfețele active pentru a primi răspunsuri.
- Dacă oricare din testele de mai sus sunt trecute, interfața este marcată ca operațională și ASA ia următoarea acțiune:
  - Dacă este active, rămâne în active
  - Dacă este standby, trece în active și încearcă să trimită un mesaj HA pe interfața operațională în care să indice vecinului să intre în standby

Tipuri de failover



- Hardware failover
  - Conexiunile sunt pierdute odată cu picarea echipamentului Activ
  - Aplicațiile client trebuie să se reconecteze
  - Este oferită redundanță la nivel hardware
- Stateful failover
  - Conexiunile TCP rămân active
  - Aplicațiile client nu trebuie să facă reconectare
  - Oferă redundanță hardware dar și redundanța conexiunilor stateful
  - Necesită o conexiune fizică între cele 2 ASA-uri folosită pentru sincronizarea informațiilor stateful

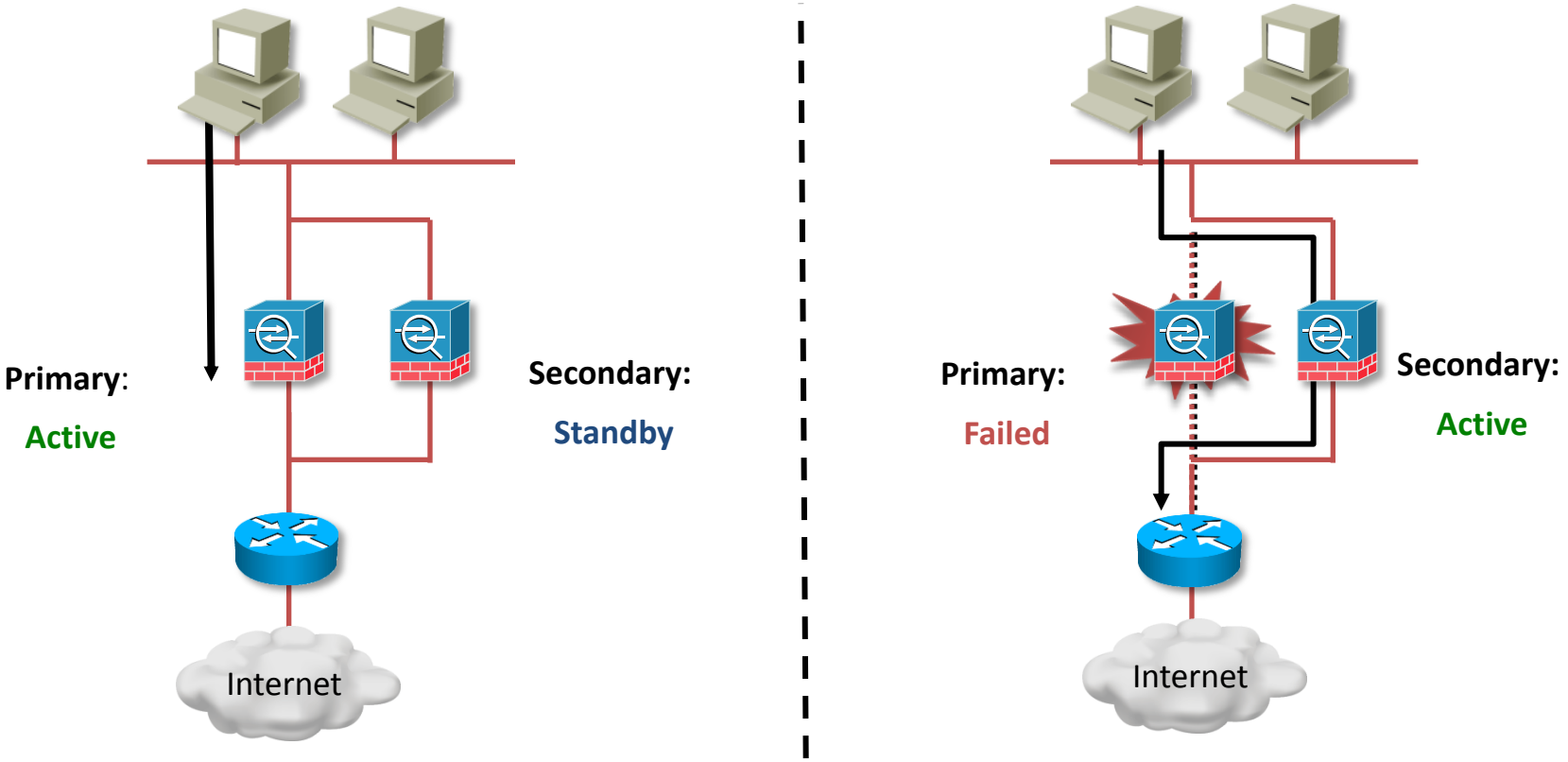
SRED

Stateful failover

- Prin stateful failover, cele 2 ASA-uri își sincronizează:
  - Tabela de conexiuni TCP cu toate informațiile din aceasta
  - Tabela xlate
  - H.323 UDP, SIP și MGCP UDP
  - HTTP replication – by default nu se copiază și conexiunile HTTP pentru că sunt foarte scurte ca life-time și în număr foarte mare
  - IPSec SA – doar în funcționarea Active/Standby
- Necesită configurarea unei legături pentru realizarea transferului de informație
  - Poate fi aceeași interfață ca cea de comandă
  - De obicei volumul de trafic pentru stateful failover este foarte mare și se recomandă folosirea unei interfețe dedicate
- Tabela de rutare sau conexiuni ICMP și UDP (în afară de cele de mai sus) nu sunt replicate

Tipuri de failover

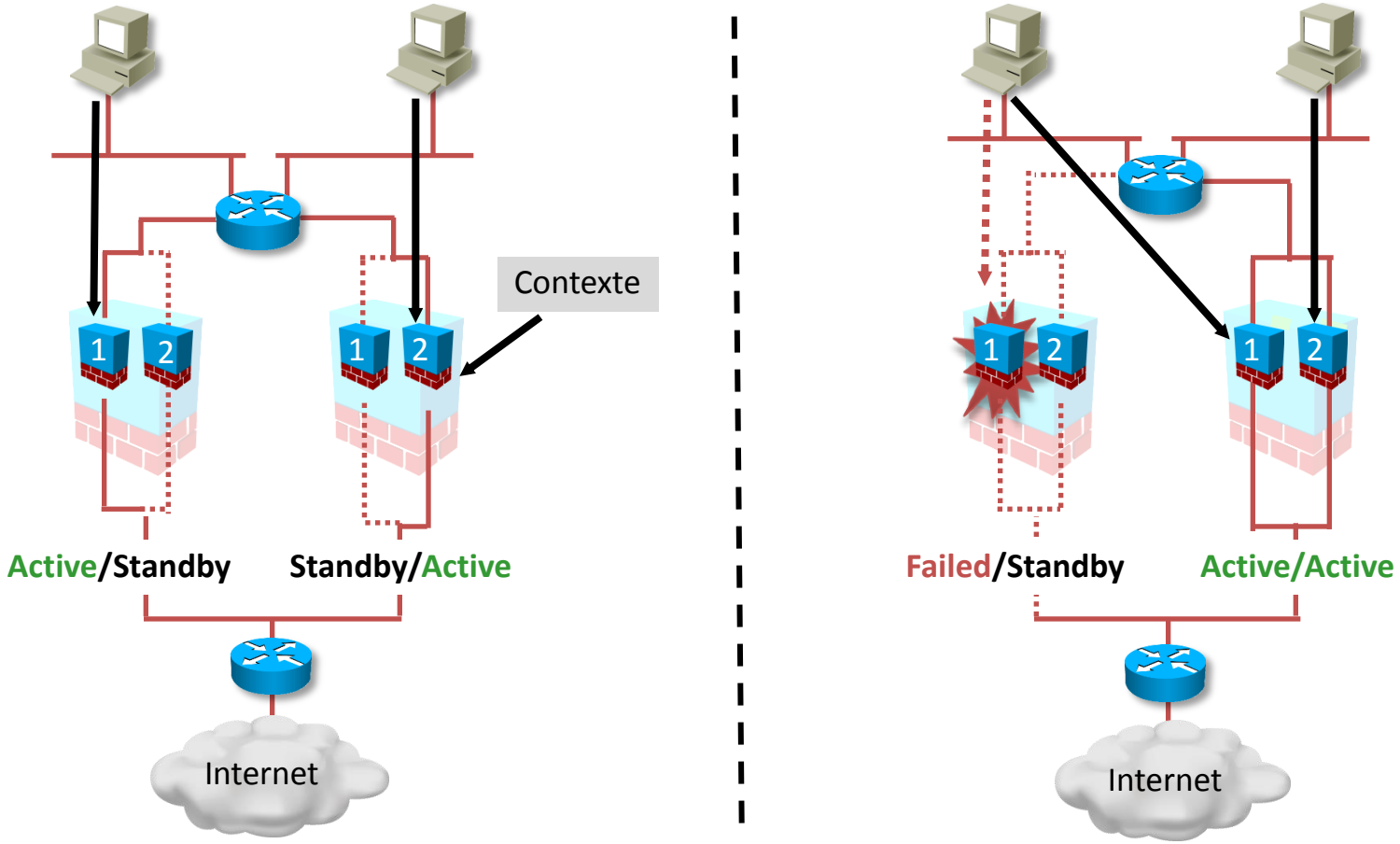
- Active/Standby
  - Doar un singur ASA face forwarding de trafic
  - În caz de picarea ASA-ului **Activ**, cel **Standby** îi ia locul



SRED

Tipuri de failover

- Active/Active – poate fi configurat doar în multiple context
  - Contexte diferite de pe ASA-uri diferite sunt în același cluster de failover
  - Ex: contextul 1 de pe ASA 1 e activ în timp ce Contextul 1 de pe ASA 2 e standby



SRED

Alegerea Active/Standby

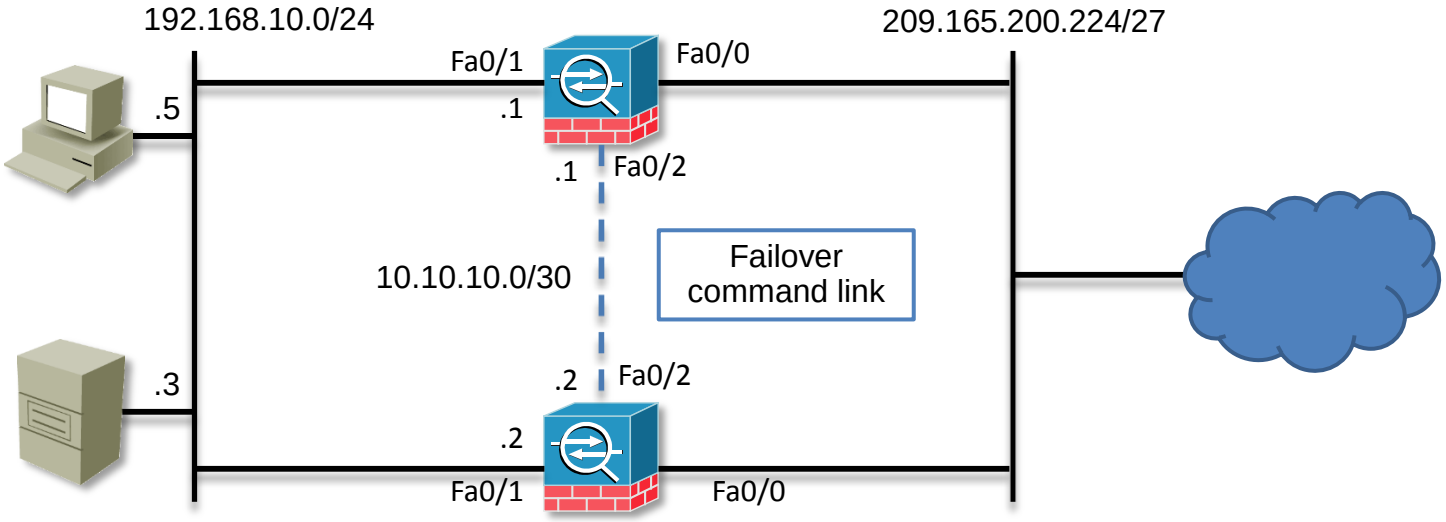
- La nivel de comenzi, administratorul de rețea va configura un ASA ca primary și altul ca secondary.
- Funcție de această configurație, alegerea active/standby se face astfel:
  - Dacă un ASA bootează mai rapid și nu detectează o unitate active, devine activă indiferent de configurație (primary sau secondary)
  - Dacă un ASA bootează mai rapid și detectează o unitate active, devine standby indiferent de configurație
  - Dacă ambele dispozitive bootează în același timp, cel primar ia rolul de active în timp ce cel secundar ia rolul de standby

Pași de configurare HA pe ASA

- Pasul 1: selectarea link-ul folosit pentru failover
- Pasul 2: configurarea de adrese IP pentru failover
- Pasul 3 (Opțional): configurarea autentificării pentru link-ul de failover
- Pasul 4: configurarea modului primary/secondary
- Pasul 5 (Opțional): configurarea stateful failover
- Pasul 6: activarea failover la nivel global
- Pasul 7: configurarea failover pe dispozitivul secundar

SRED

Configurarea link-ului de failover



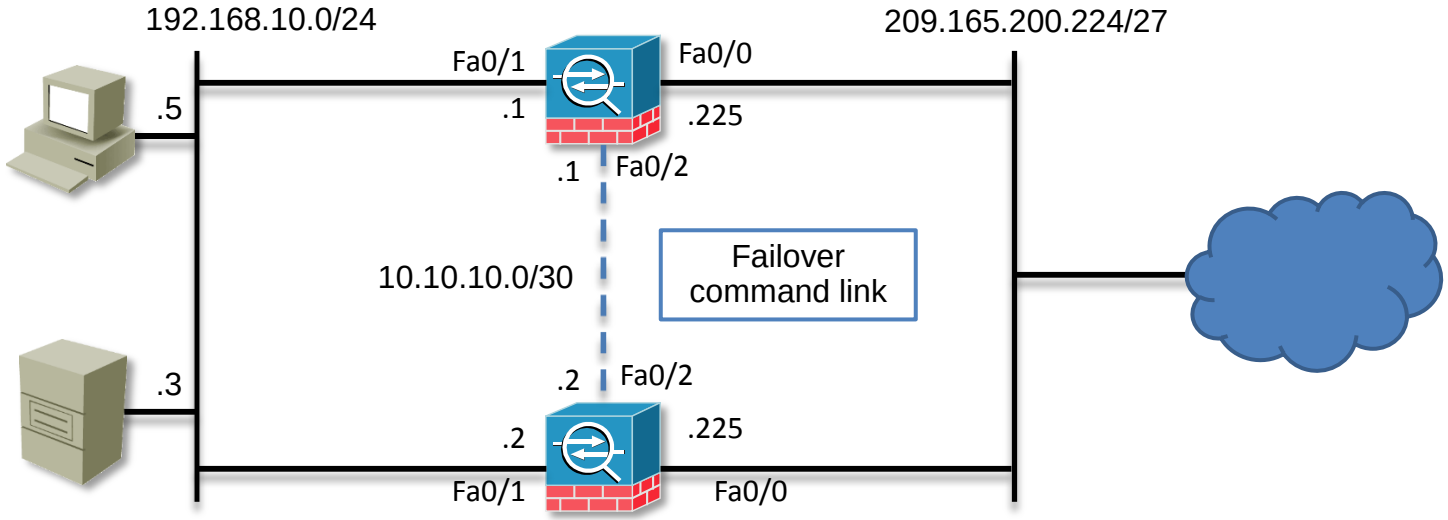
- Comanda permite specificarea unui nume pentru interfață (același efect ca și **`nameif)`**

```
Waters(config)# failover lan interface Ctrl Fa0/2
```

```
Waters(config)# interface Fa0/1
Waters(config-if)# nameif Ctrl
Waters(config)# failover lan interface Ctrl Fa0/2
Interface already in use
```


SRED

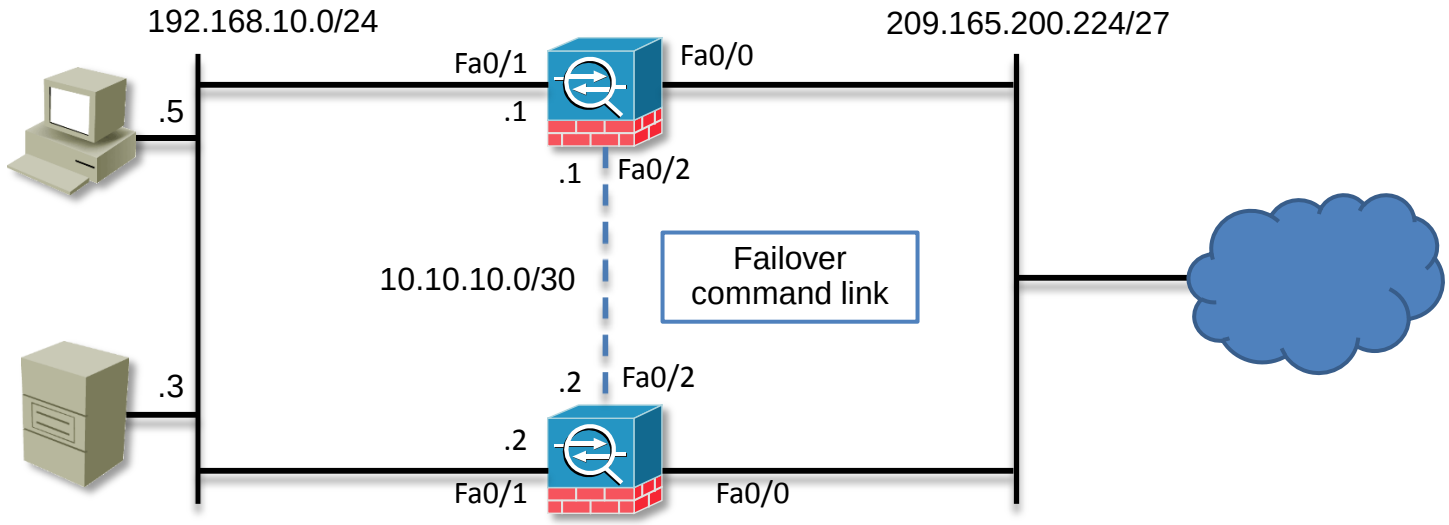
Configurarea adreselor de standby




```
Waters(config)# interface Fa0/0
Waters(config-if)# nameif outside
Waters(config-if)# security-level 0
Waters(config-if)# ip address 209.165.200.225 255.255.255.224 standby 209.165.200.226
Waters(config)# interface Fa0/1
Waters(config-if)# nameif inside
Waters(config-if)# security-level 100
Waters(config-if)# ip address 192.168.10.1 255.255.255.0 standby 192.168.10.2
```


SRED

Configurarea IP pe interfața de comandă

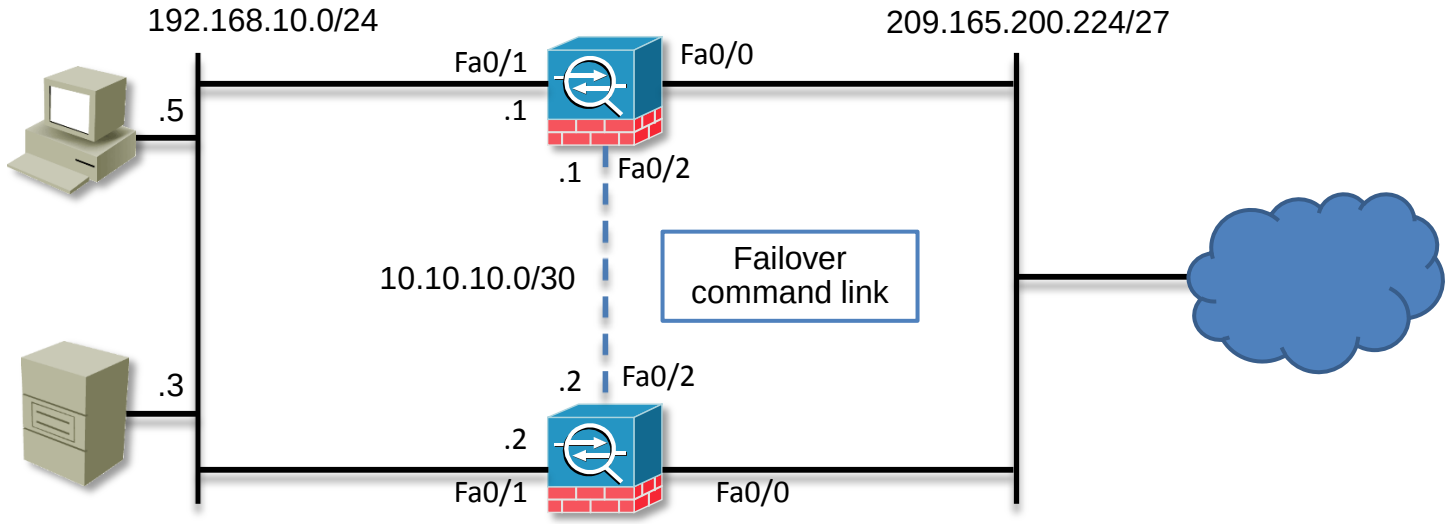


- Funcție de licența instalată, ASA folosește DES/AES pentru criptare și o schemă bazată pe hashing pentru autentificare

```
Waters# configure terminal
Waters(config)# failover interface ip Ctrl 10.10.10.1 255.255.255.252
  standby 10.10.10.2
Waters(config)# failover key cisco123
Waters(config)# failover lan unit primary
```


SRED

Configurarea stateful failover

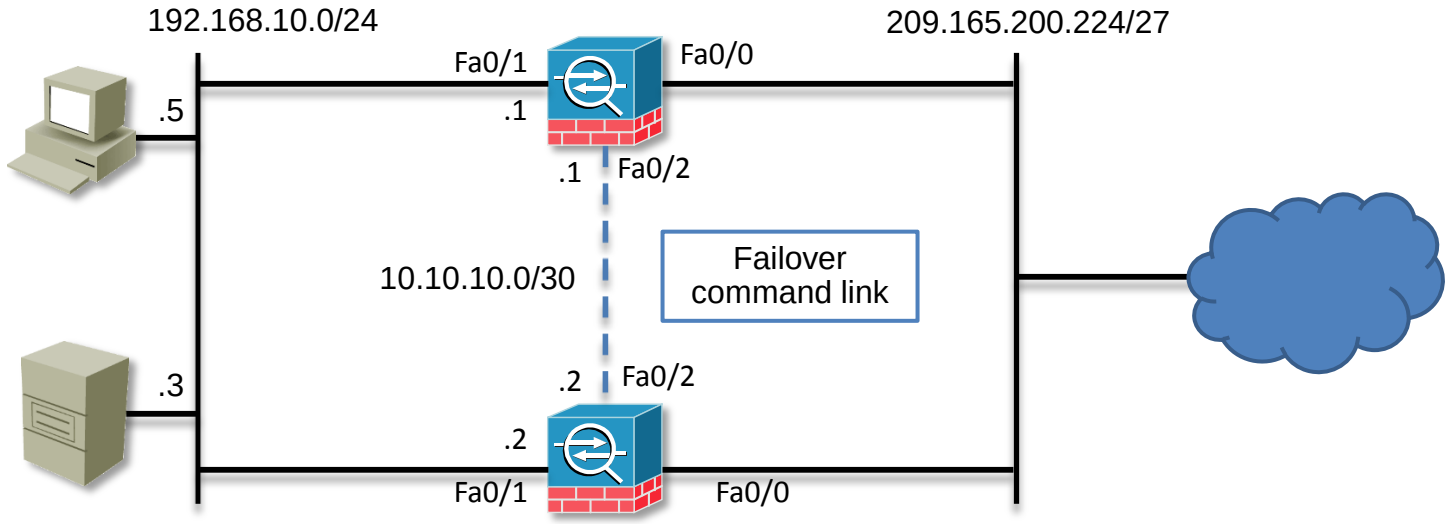


- Opțional se poate activa și replicarea HTTP

```
Waters(config)# failover link statefullink Fa0/2
Waters(config)# failover interface ip statefullink 10.10.10.5 255.255.255.252
  standby 10.10.10.6
Waters(config)# failover replication http
# Activarea HA la nivel global
Waters(config)# failover
```


SRED

Configurarea echipamentului secundar




```
(Waters2-config)# failover lan unit secondary
(Waters2-config)# failover lan interface FOCtrlIntf Fa0/2
(Waters2-config)# failover key cisco123
(Waters2-config)# failover interface ip Ctrl 10.10.10.1 255.255.255.252 standby
  10.10.10.2
(Waters2-config)# failover
```

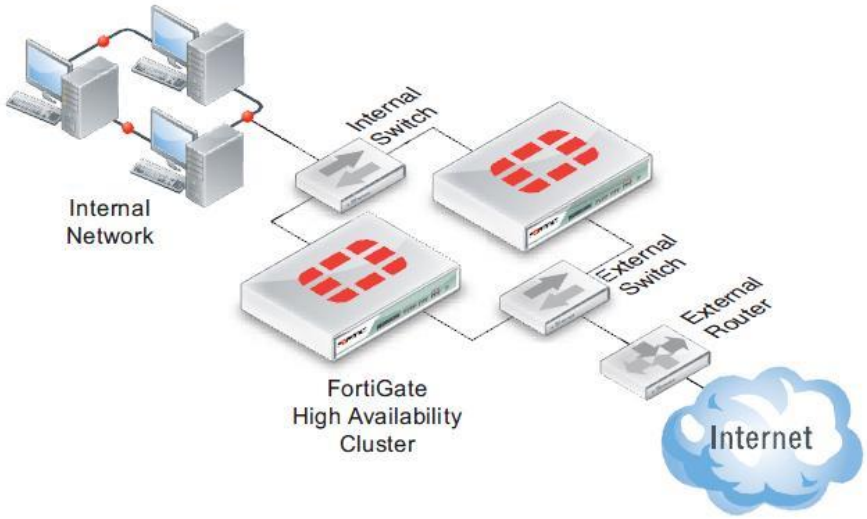
- În acest moment cele două dispozitive sunt sincronizate

SRED

Fortinet- High Availability

Soluții de HA

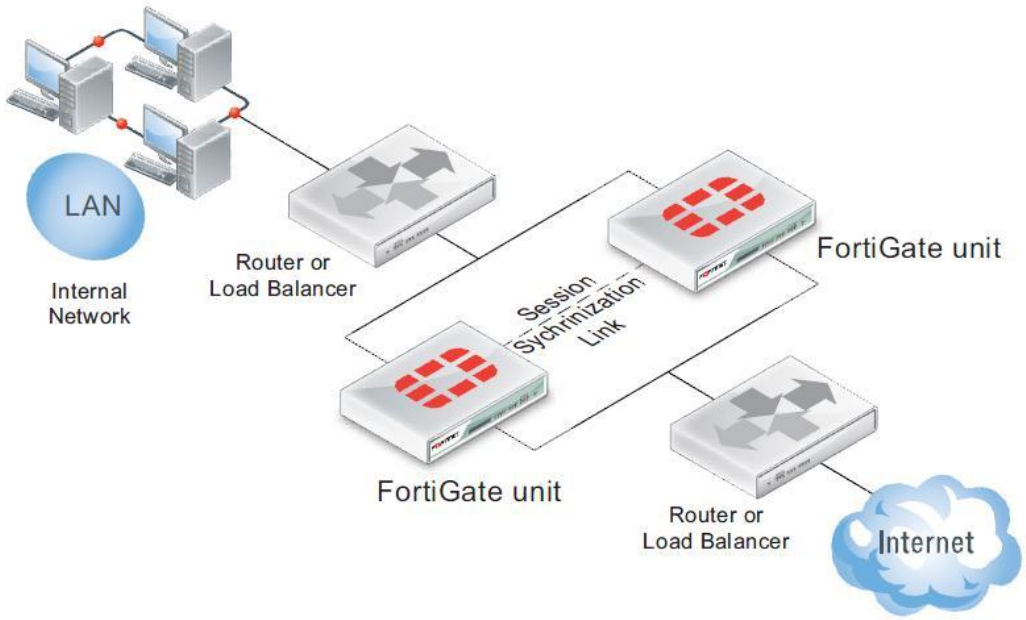
- Fortinet prezintă mai multe soluții de HA
  - FortiGate Cluster Protocol (FGCP) - soluție complexă de HA proprietară Fortinet
    - Oferă modul Active/Active cu și fără VDOM-uri
    - Oferă device failover, link failover și remote failover protection (oferă un sistem de monitorizare și tracking asemănător VRRP)
    - Oferă configurații avansate de full-mesh HA și virtual clustering



SRED

Soluții de HA

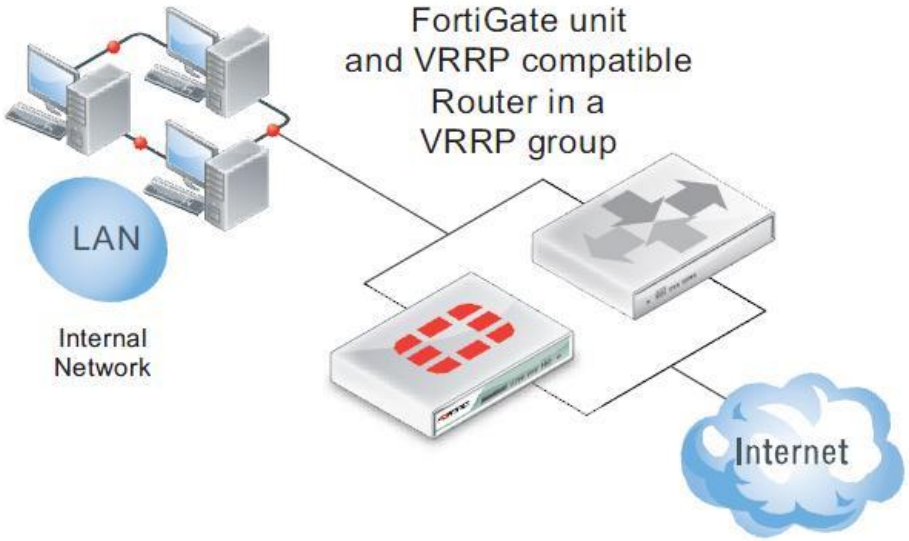
- Fortinet prezintă mai multe soluții de HA
  - TCP session sync
    - Soluția presupune că schema de load-balancing e deja adresată prin load-balancere sau rutere și cele 2 FortiGate-uri doar își sincronizează sesiunile TCP
    - Configurațiile nu sunt sincronizate



SRED

Soluții de HA

- Fortinet prezintă mai multe soluții de HA
  - VRRP
    - Oferă o soluție open de gateway load-balancing
    - Poate fi folosit atât între FG-uri cât și între un FG și ruterul altui vendor care implementează VRRP



SRED

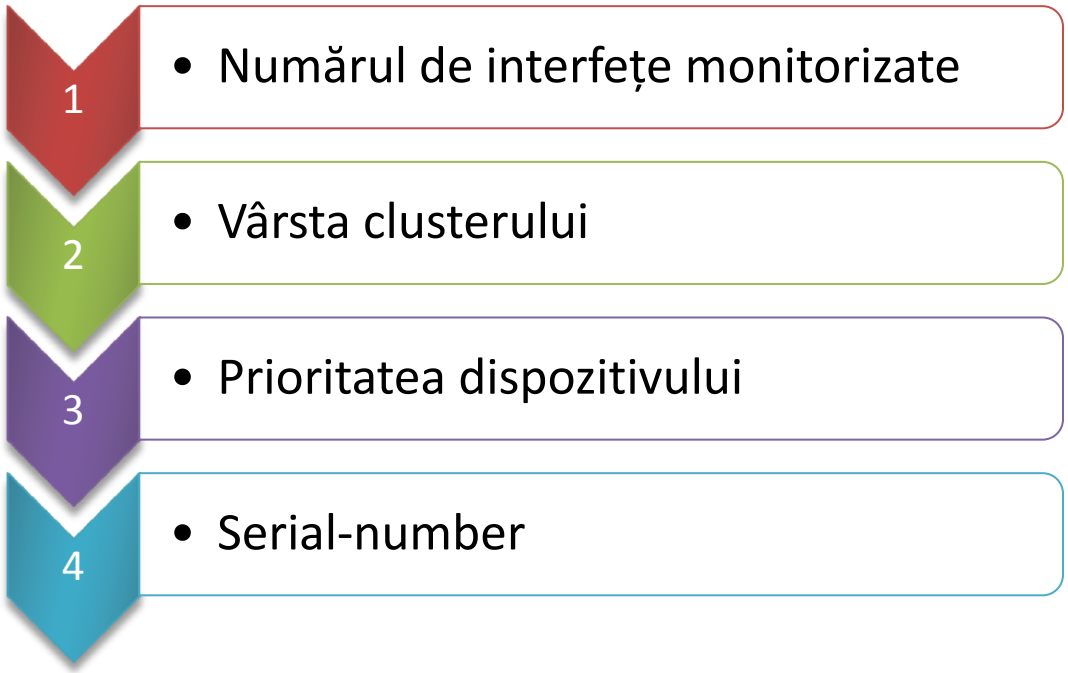
FGCP Facts

- FGCP grupează mai multe FortiGate-uri în *clustere*
- Într-un cluster se pot două sau mai multe FortiGate-uri
- Toate FortiGate-urile trebuie să aibă același firmware și configurație hardware
- Odată configurat, FGCP caută FortiGate-uri din același cluster cu care să realizeze sincronizarea de configurații și de informații de sesiune
- Toate schimburile de configurații se realizează prin mesaje *Heartbeats*
- FGCP are modul Active/Passive (Failover) sau Active/Active (Load-balancing)

SRED

Alegerea rolurilor într-un cluster

- Orice cluster, indiferent de modul de operare, va avea un dispozitiv primar și mai multe secundare
- Dispozitivul primar este coordonatorul clusterului



- În mod implicit alegerea nu este preemptivă, dar poate fi configurată pentru a fi din modul CLI (HA override)

SRED

Funcționalități FGCP

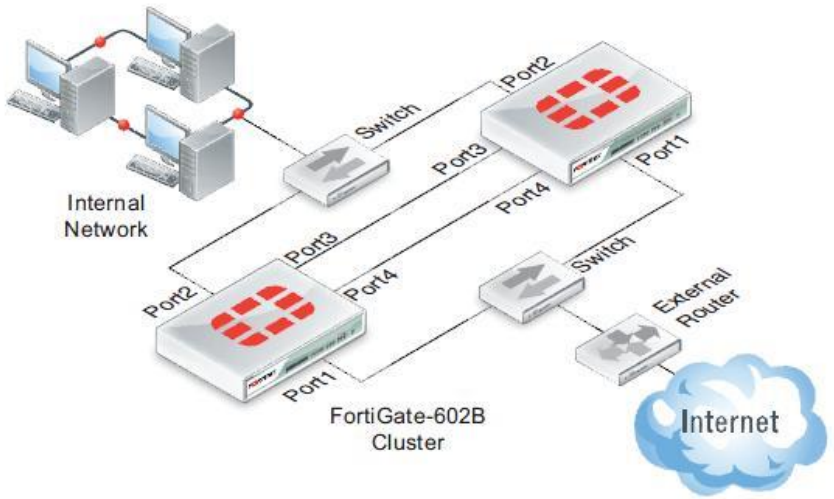
- FGCP Failover protection
  - Toate FG-urile din cluster răspund la aceeași pereche de IP-MAC virtuale
  - Failover < 1 secundă
  - Când un FG pică, celalalte preiau în mod dinamic sesiunile și procesarea
  - Este suportată monitorizarea la nivel de interfață
- Session failover
  - FGCP face failover pentru TCP, SIP și IPSec VPN
  - Nu sunt suportate UDP, multicast, ICMP sau SSL VPN
- Load balancing
  - În modul Active-Active un cluster poate balansa trafic UTM și trafic TCP (în mod implicit doar UTM)
- Virtual Clustering
  - Presupune un cluster de 2 FG între mai multe VDOM-uri
- Full Mesh HA
  - Folosește 802.3ad pentru link-aggregation și introduce switch-uri redundante în topologie pentru eliminarea unui single-point of failure în cluster

Moduri de funcționare FGCP

- Active/Passive
  - Oferă funcționalitatea de failover transparent în cluster
  - Doar dispozitivul primar realizează operații de firewalling sau UTM
  - Dispozitivele secundare monitorizează dispozitivul principal pentru failover
- Active/Active
  - Toate dispozitivele din cluster fac implicit load-balancing UTM
  - Dispozitivul primar este coordonator și “servește” conexiunile celorlalte dispozitive
  - Se poate activa și balansarea de TCP
- Virtual Clustering
  - Creează clustere între VDOM-urile e 2 dispozitive
  - Poate face load-balancing pentru orice tip de trafic

Configurarea unui cluster

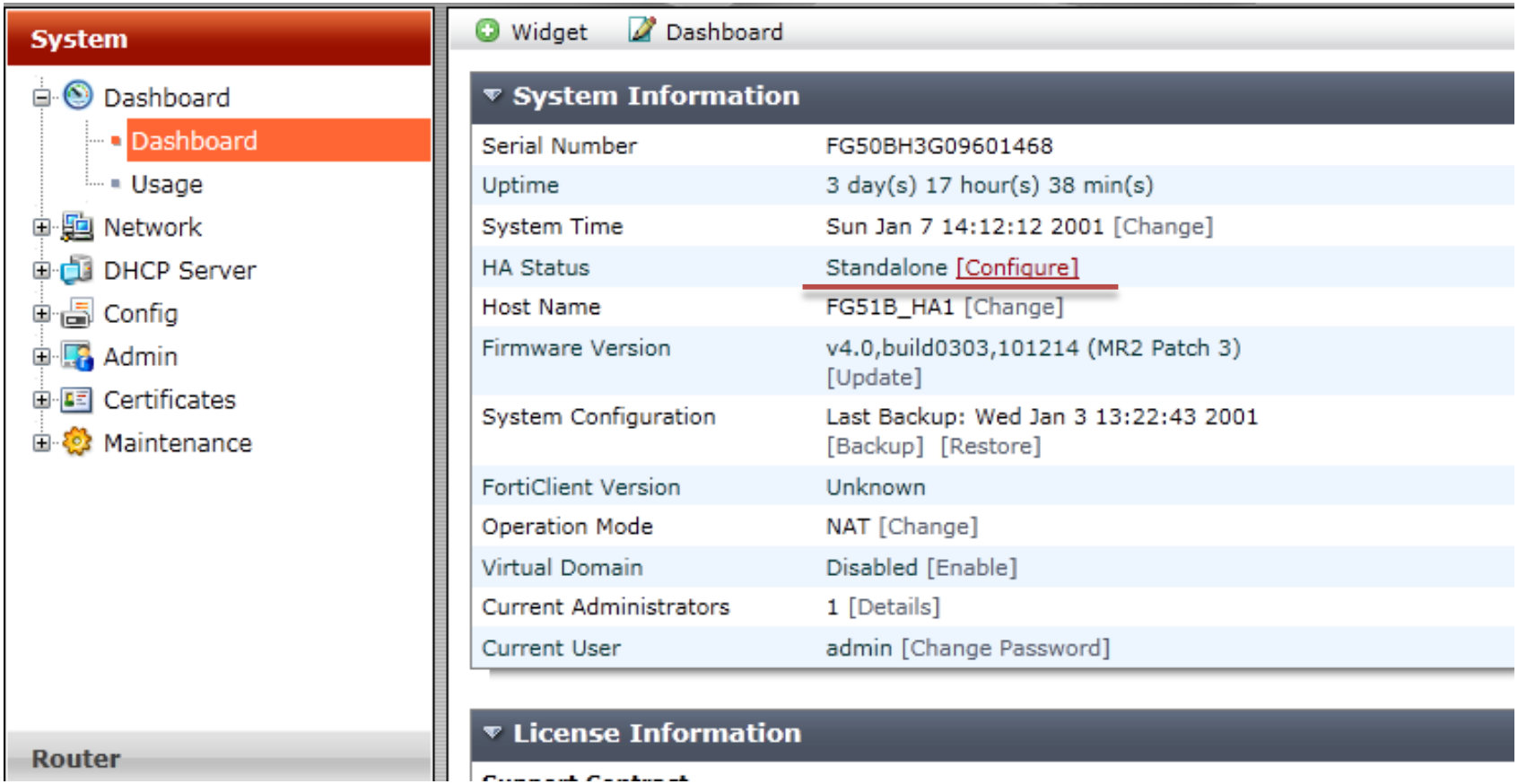
- Pasul 1: Fiecare dispozitiv trebuie configurat separat pentru clusterul din care face parte
  - Modul de funcționare
  - Numele clusterului
  - Cheia de autentificare folosită
- Pasul 2:
  - Conectarea fiecărui FG la cluster
  - Interfețele trebuie să fie matching
  - În timpul configurării clusterului acesta nu va forwarda trafic
  - După configurarea clusterului trebuie ca intrarea ARP să expire



SRED

Configurarea HA

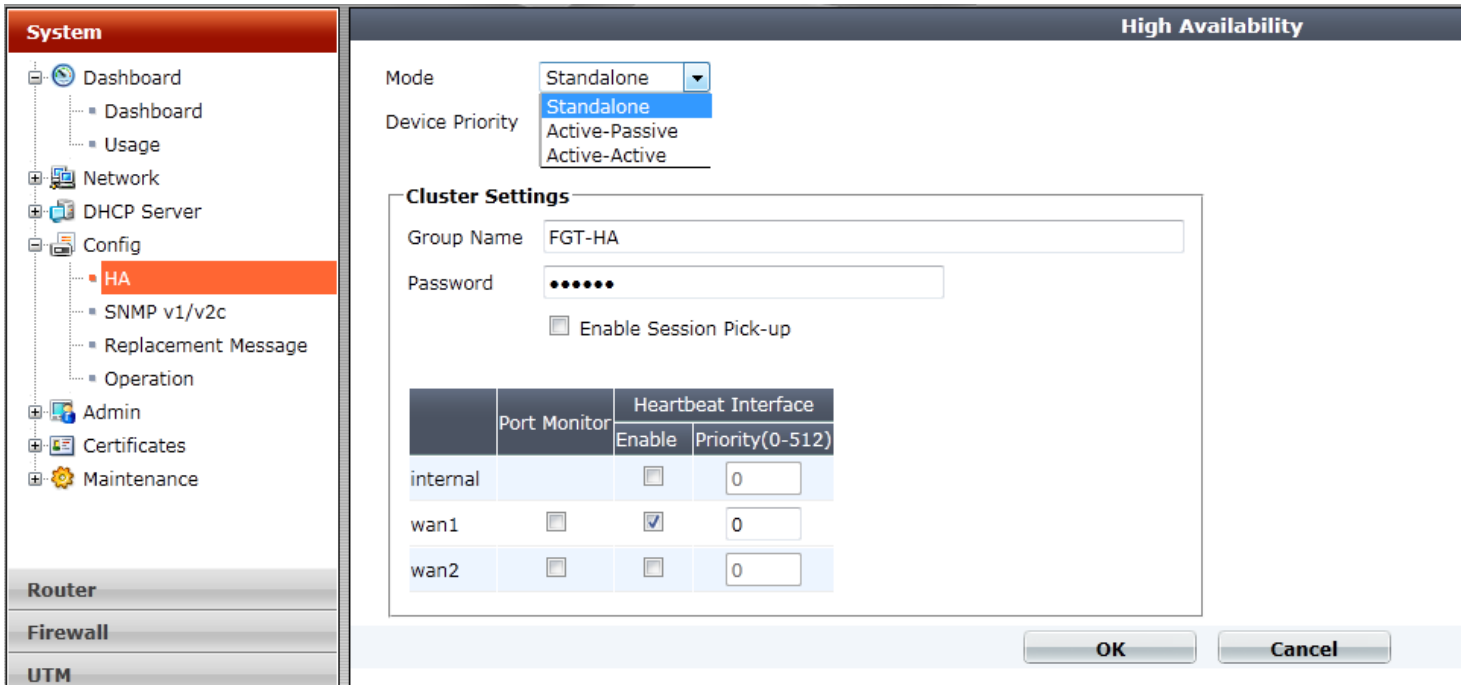
- Se pornește configurarea din meniul Dashboard



SRED

Configurarea HA

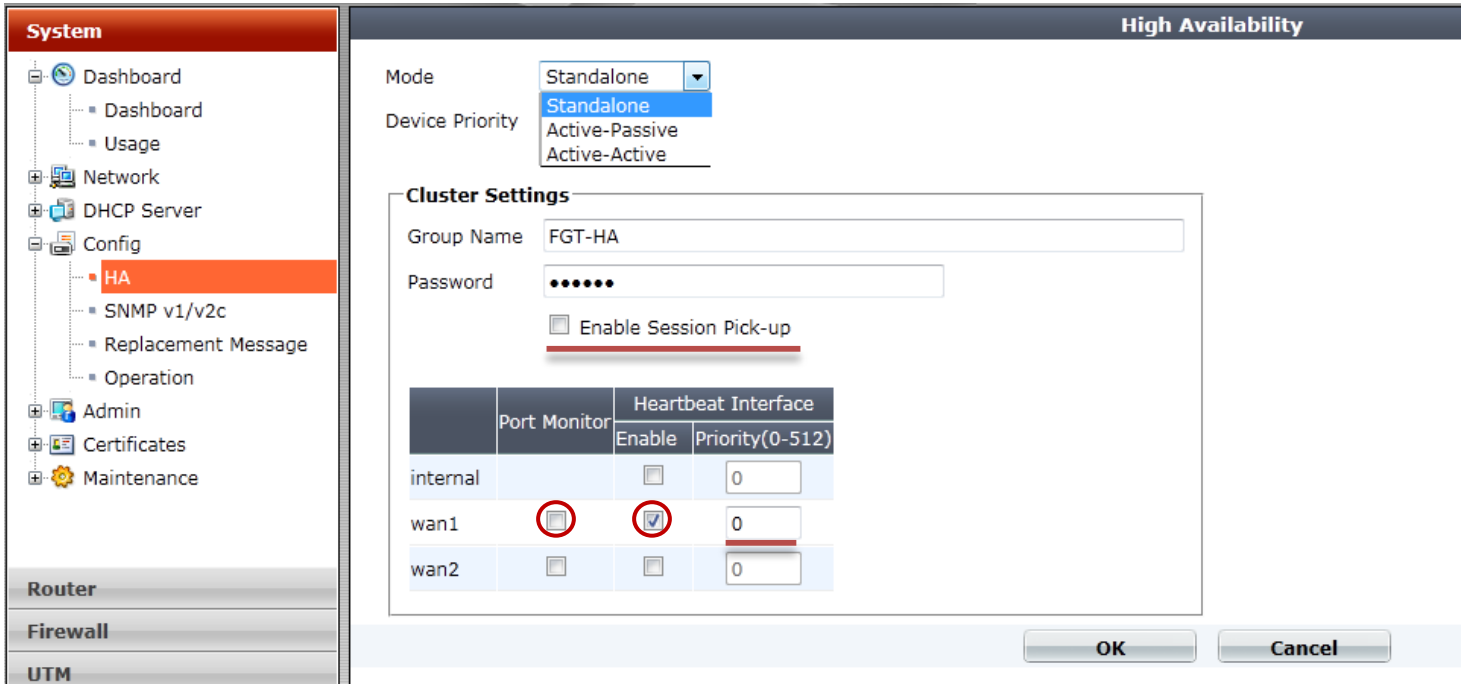
- Se configurează:
  - modul de operare
  - numele clusterului și parola



SRED

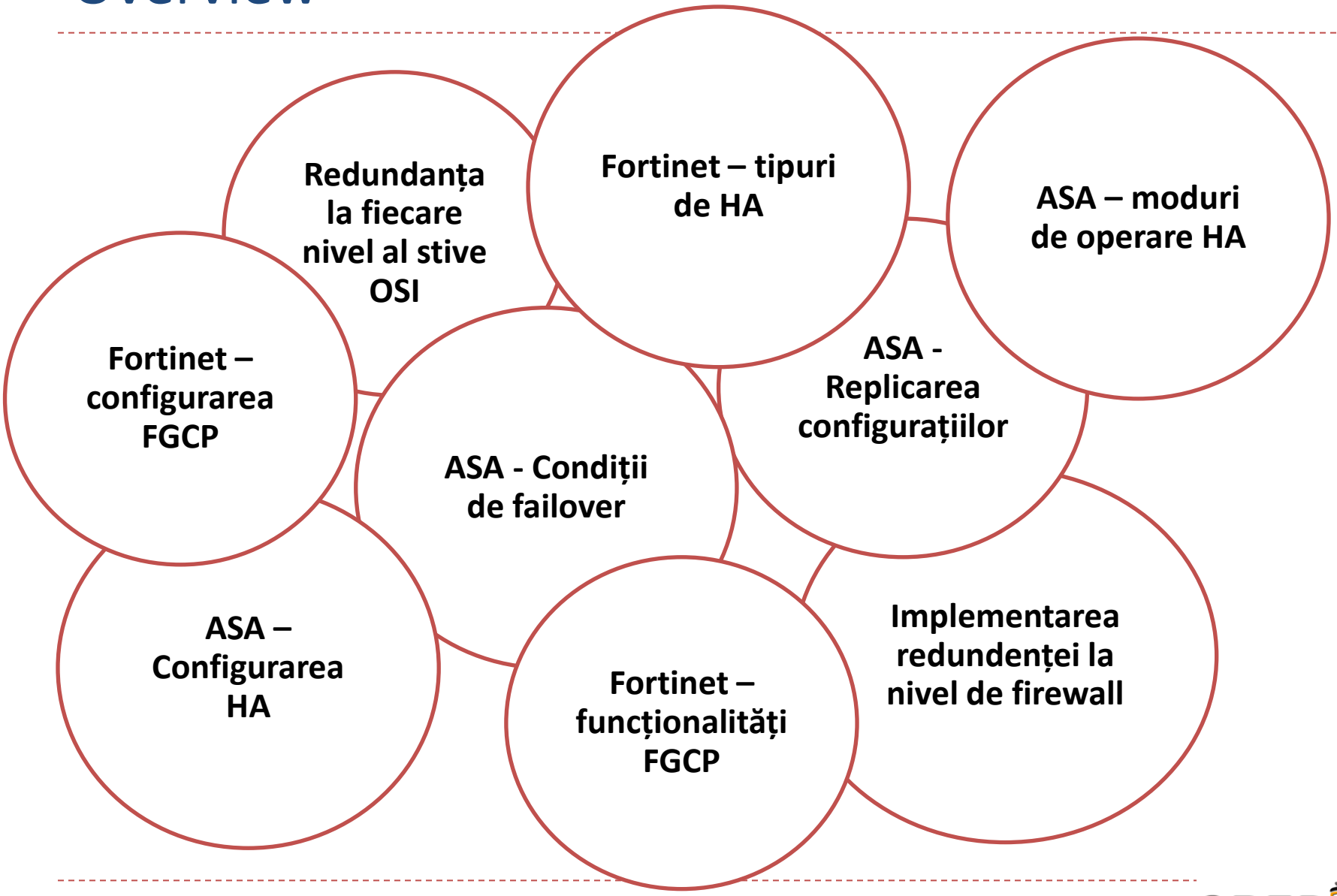
Configurații suplimentare

- Se poate activa sau dezactiva Session Pick-up (Stateful failover)
- Se poate activa sau dezactiva monitorizarea la nivel de interfață
  - O interfață monitorizată ce cade va scădea prioritatea dispozitivului cu valoarea configurată
  - Prioritatea este folosită pentru alegerea unui dispozitiv Primar în cluster (dacă opțiunea de HA Override este configurată)



SRED

Overview



SRED