Virtual Firewalling

27 martie 2014

Obiective

- Conceptul de Virtual Firewalling
- Cisco ASA
  - Arhitectura multiple-context
  - Implementarea multiple-context
  - Studiu de caz
- FortiGate
  - Arhitectura VDOM
  - Comunicarea Inter-VDOM
  - Implementarea VDOM și Inter-VDOM Links

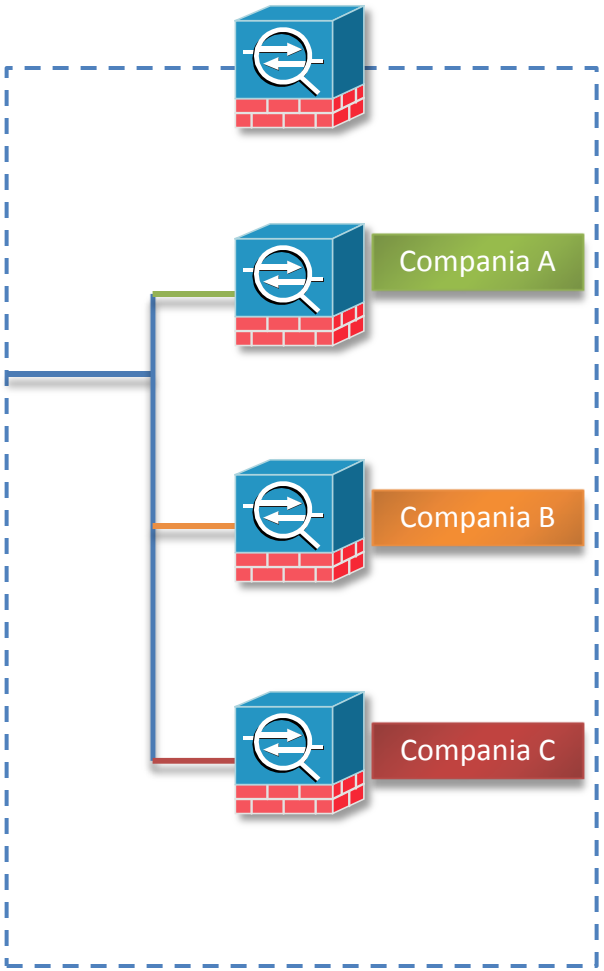
Virtualizare

- Posibilitatea de partiționare a unui singur firewall fizic în mai multe instanțe virtuale ale acestuia
- Fiecare firewall virtual are propriile fișiere de configurare independente și proprii administratori
- Există un super_admin care poate controla întreg dispozitivul
- Numărul/posibilitatea de instanțe virtuale este controlat de obicei prin licențiere

SRED

De ce virtualizare?

- Un ISP trebuie să ofere servicii mai multor clienți dar nu vrea să cumpere un firewall pentru fiecare client (Managed Security Service Provider)
- O facultate dorește să aibă o instanță pentru traficul realizat de studenți și altă instanță pentru traficul realizat de cadre didactice
- O companie are mai multe departamente împărțite pe VLAN-uri și dorește inspectarea diferită a traficului funcție de VLAN/departament
- Se dorește asigurarea serviciilor de firewalling într-o rețea cu spații de adrese overlapping



SRED

Cisco ASA – Contexte de securitate

Arhitectură

ASA – Contexte de securitate

- În mod implicit este în modul “single”

```
Waters# sh mode
Security context mode: single
```

- La trecerea în modul “multiple”, din punct de vedere funcțional ASA va cuprinde 3 componente

System Execution Space

- Configurat de super_admin

Admin Context

- Configurat de super_admin

Customer Context

- Configurat de admin-ul fiecărui context sau de super_admin

SRED

System execution space (SES)

- Este componenta de unde admin-ul “regizează” dispozitivul ASA în multiple-mode
- Numit și **System context**
  - Nu este practic un context – nu se pot aloca interfețe către SES și nici nu conține L3 data-plane
- Din SES se configurează parametrii multi-context:
  - Crearea de contexte
  - Apartenența fiecărei interfețe/subinterfețe la contexte
  - Locația fișierului de configurare pentru fiecare context
- … și parametrii globali ce nu țin de L3 data-plane:
  - Activation-key
  - Banner
  - Parametrii de nivel 1 și 2 pentru o interfață/subinterfață

SRED

Admin context

- La trecerea din single-mode în multiple-mode toate configurațiile L3 sunt salvate în contextul admin
- Contextul admin ar trebui folosit pentru:
  - Trafic de management
  - Trafic de logging și autentificare pentru acces remote
  - Descărcarea fișierelor de configurare ale altor contexte de pe locații remote (SES definește aceste locații dar poate descărca fișierele pentru ca nu are capacități L3 data-plane)
  - Din admin context se poate ajunge în SES
- Contextul admin nu ar trebui folosit pentru
  - Trafic de date al utilizatorilor
    - În afară de relația specială între contextul admin și SES, acesta poate fi folosit ca un context normal, dar acest lucru nu este recomandat (Analogie: este ca un fel de VLAN de management)

SRED

Customer context (1)

- Instanțele virtuale efective ce sunt folosite pentru a trata diferit traficul, din motive explicate în slide-ul “De ce virtualizare?”
- Pot fi definiți administratori diferiți pentru fiecare context
- Dintr-un context customer nu se poate ajunge în contextul admin sau în SES

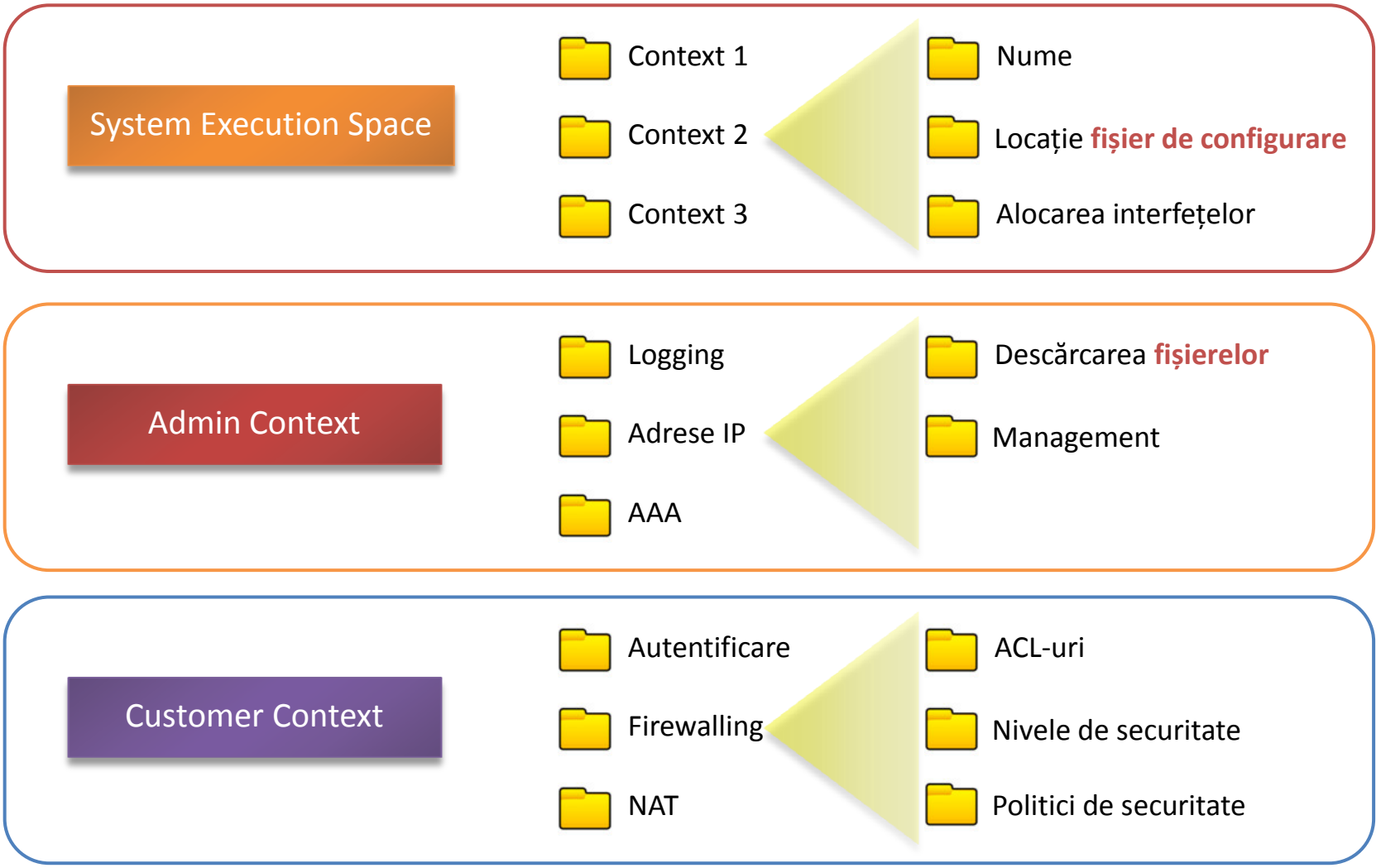
SRED

Customer context (2)

- Clasificarea traficului funcție de contextul destinație folosind:
  - (Sub)Interfețe unice per context
    - dacă toate contextele de pe ASA folosesc (sub)interfețe unice, clasificarea se face după (sub)interfața sursă
  - Interfețe shared
    - Oferă posibilitatea apartenenței unei interfețe la mai multe contexte
    - În fiecare context, interfața va avea un IP diferit, însă din aceeași rețea
    - Permite adrese suprapuse
    - Clasificarea se face folosind NAT și generând/configurând o adresă MAC unică pentru fiecare IP diferit din fiecare context diferit

SRED

Structură generală



SRED

Fișiere de configurare

- În multi-mode există următoarele fișiere de configurare
  - **Old_running.cfg**
    - snapshot realizat configurației din RAM în momentul trecerii de la single-mode la multi-mode
  - **Admin.cfg**
    - fișier de configurare al contextului admin
    - Trebuie păstrat neapărat în flash
  - **Context.cfg**
    - fișier de configurare pentru fiecare context
    - Poate fi păstrat pe:
      - Disk - flash
      - TFTP
      - FTP
      - HTTP(S)
    - Locația unde este stocat este configurată din: System execution space

SRED

Fișiere de configurare

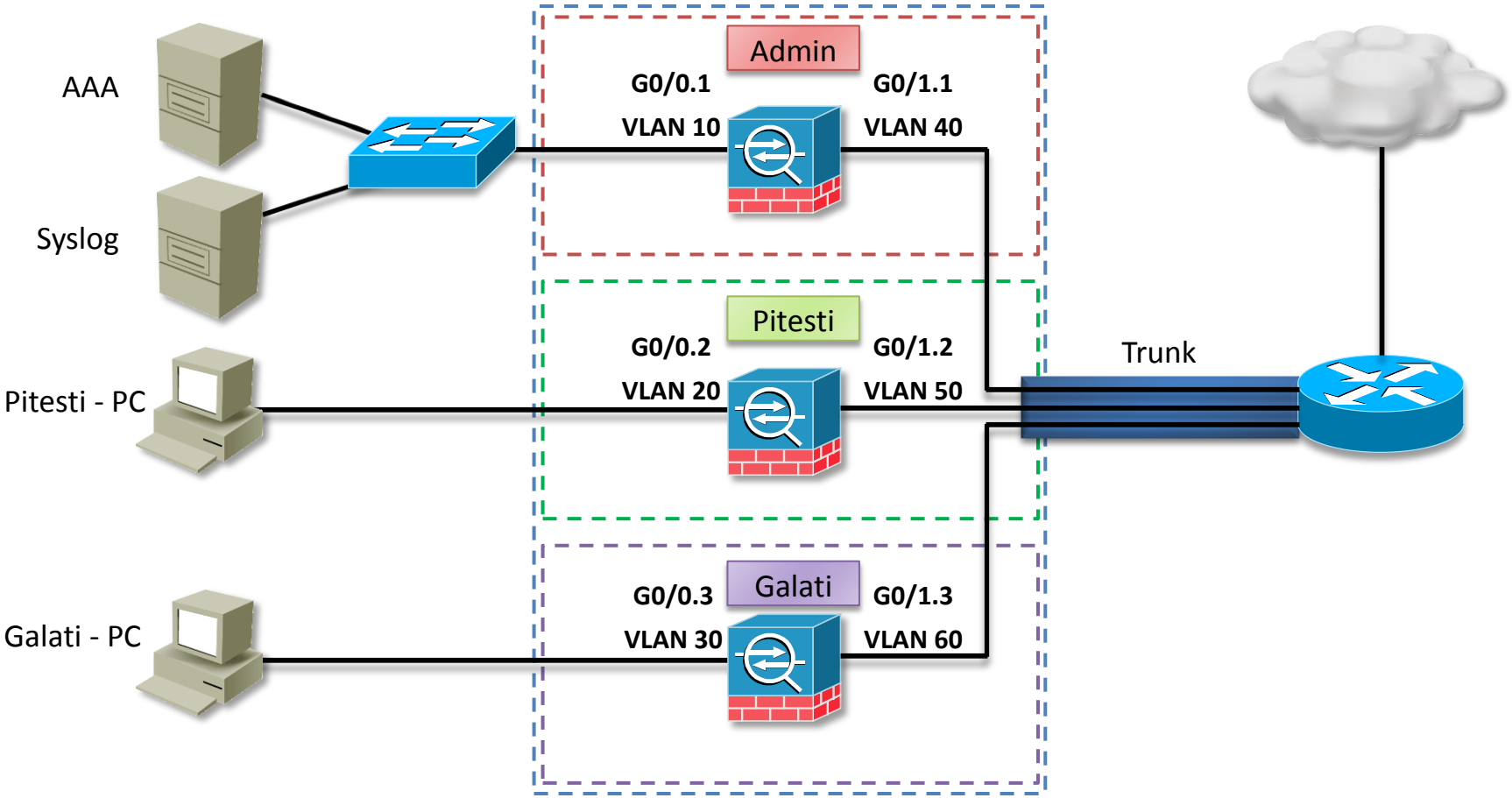
- SES-ul nu este salvat în flash, ci în NVRAM
- În SES se află configurația pentru modul în care funcționează ASA (single/multiple)
- La trecerea din multiple-mode în single-mode trebuie:
  - Șterse toate contextele customer
  - Șters contextul admin
  - Șters RAM-ul
    - copierea old_running.cfg în RAM folosește *merge*, nu *replace*
  - Configurat modul ASA la single
  - Copiat old_running.cfg în RAM

Costul multiple-mode

- ASA 5510-5540 suportă în mod implicit 2 contexte customer și 1 context admin, fără licență.
- Din păcate, odată cu activarea multiple-mode pe ASA se pierd funcționalități din ASA OS
  - Posibilitatea de a face QoS
  - Posibilitatea de a folosi multicast
  - Posibilitatea de a rula protocoale de rutare (este permisă doar rutarea statică)
  - Posibilitatea de a avea VPN-uri de date (VPN-urile de management sunt încă permise)

Comunicarea între contexte sau cu exteriorul (1)

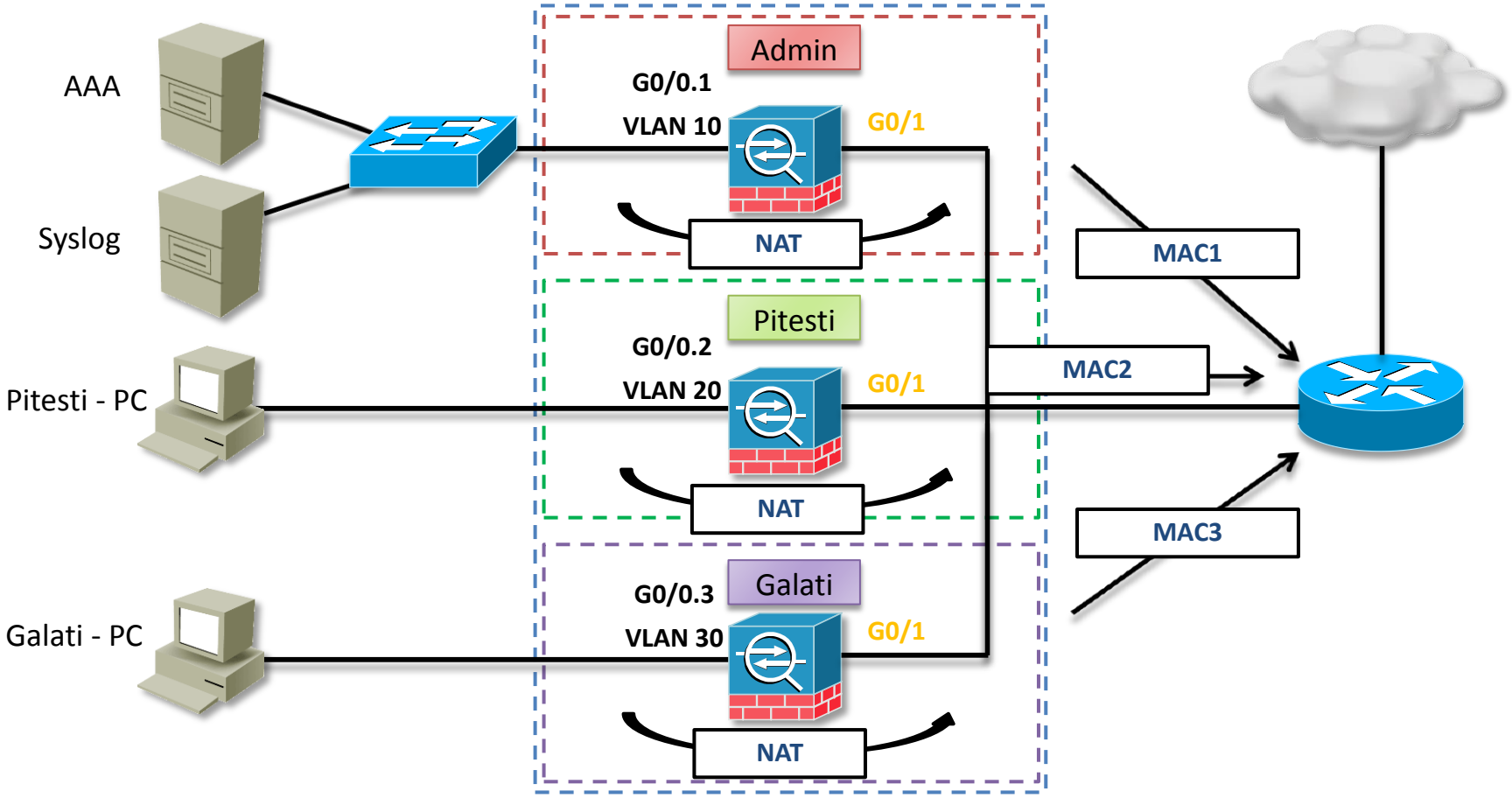
- Folosind (sub)interfețe unice (slide 9)



SRED

Comunicarea între contexte sau cu exteriorul (2)

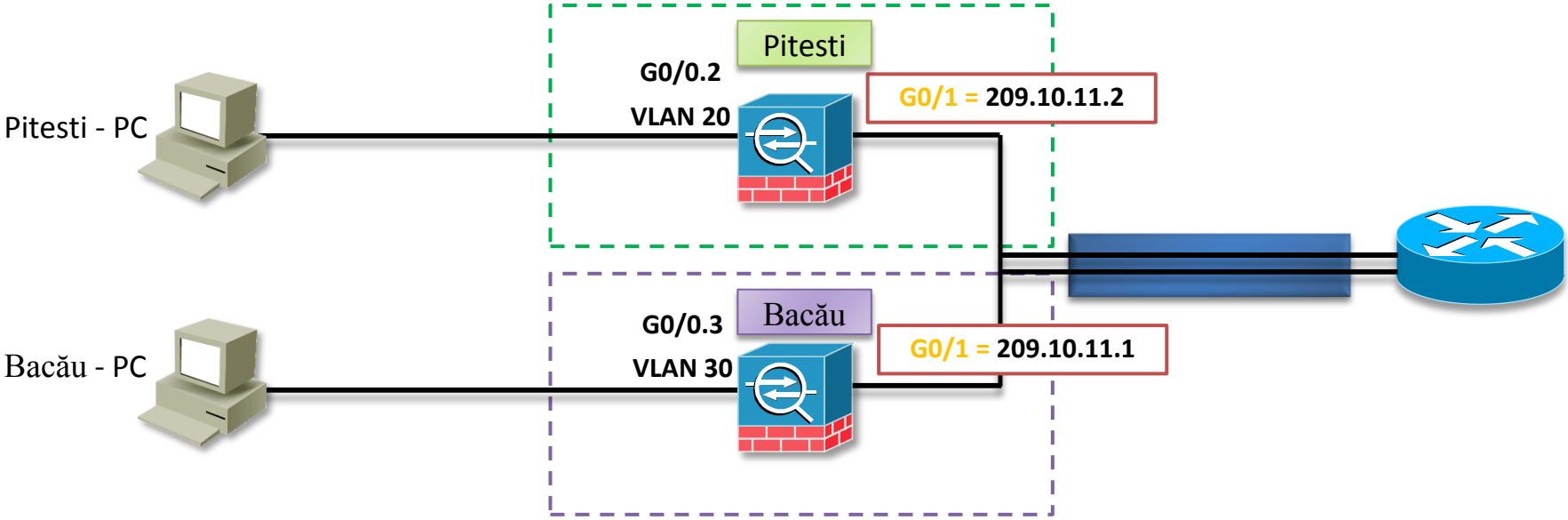
- Folosind o interfață shared cu IP diferit în fiecare context



SRED

Comunicarea între contexte sau cu exteriorul (3)

- Utilizarea unei interfețe shared face comunicația dintre contexte mult mai ușoară



SRED

Cisco ASA – Contexte de securitate

Implementare

Configurare modului

- La schimbarea modului ASA face reboot

```
Waters# configure terminal
Waters(config)# mode ?
  multiple Multiple mode; mode with security contexts
  single   Single mode; mode without security contexts
Waters(config)# mode multiple

WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]

   Convert the system configuration? [confirm]
The old running configuration file will be written to disk0
The admin context configuration will be written to disk0
The new running configuration file was written to disk0
Security context mode: multiple
***
*** --- SHUTDOWN NOW ---
***
Waters>
```


SRED

Configurarea unui context

- Configurarea unui context presupune
  - Crearea contextului
  - Alocarea (sub)interfețelor membre
  - Definirea locației fișierului de configurare

- Crearea contextului

```
Waters(config)# context Pitesti
Creating context 'Pitesti'... Done. (2)
Waters(config-ctx)# description Client Premium
Waters(config)# context Galati
Creating context 'Galati'... Done. (3)
Waters(config-ctx)# description Client Silver
```

Alocarea interfețelor

- Alocarea interfețelor trebuie făcută mereu înainte de definirea locației fișierului de configurare
  - La definirea locației fișierului de configurare, ASA va încerca imediat să descarce acel fișier și nu va putea dacă interfețele nu au fost mai întâi alocate
  - Descărcarea fișierelor de configurare este făcută de contextul admin – de aceea acest context trebuie definit înainte de oricare altul

```
Waters(config)# context Pitesti
Waters(config-ctx)# allocate-interface GigabitEthernet0/0 A_inside invisible
Waters(config-ctx)# allocate-interface GigabitEthernet0/1 A_outside invisible
Waters(config-ctx)# exit
Waters(config)# context Galati
Waters(config-ctx)# allocate-interface GigabitEthernet0/2 B_inside invisible
Waters(config-ctx)# allocate-interface GigabitEthernet0/3 B_outside invisible
```

- Pentru orice interfață alocată, se poate mapa un nume
- Cuvântul cheie invisible face astfel încât administratorul contextului să nu poată vedea numele adevărat al interfeței

SRED

Locația fișierelor de configurare

- Se configurează tot din SES
- Dacă se folosesc servere externe, contextul admin trebuie să aibă acces la Internet

```
Waters(config)# context admin
Waters(config-ctx)# config-url disk0:/admin.cfg
Waters(config-ctx)# context Pitesti
Waters(config-ctx)# config-url tftp://192.168.10.50/Pitesti.cfg
Waters(config-ctx)# context Galati
Waters(config-ctx)# config-url ftp://cisco:cisco123@192.168.20.50/Galati.cfg
```

- La modificarea URL-ului, se descarcă noul fișier de configurare și se face *merge* în RAM
  - Trebuie șters RAM-ul înainte de schimbarea URL-ului

Alte operații pe contexte

- Vizualizarea modului de operare ASA

```
Waters# show mode
   Security context mode: multiple
```

- Schimbarea contextului

```
Waters# changeto context admin
Waters/admin#
```

- Vizualizarea contextelor

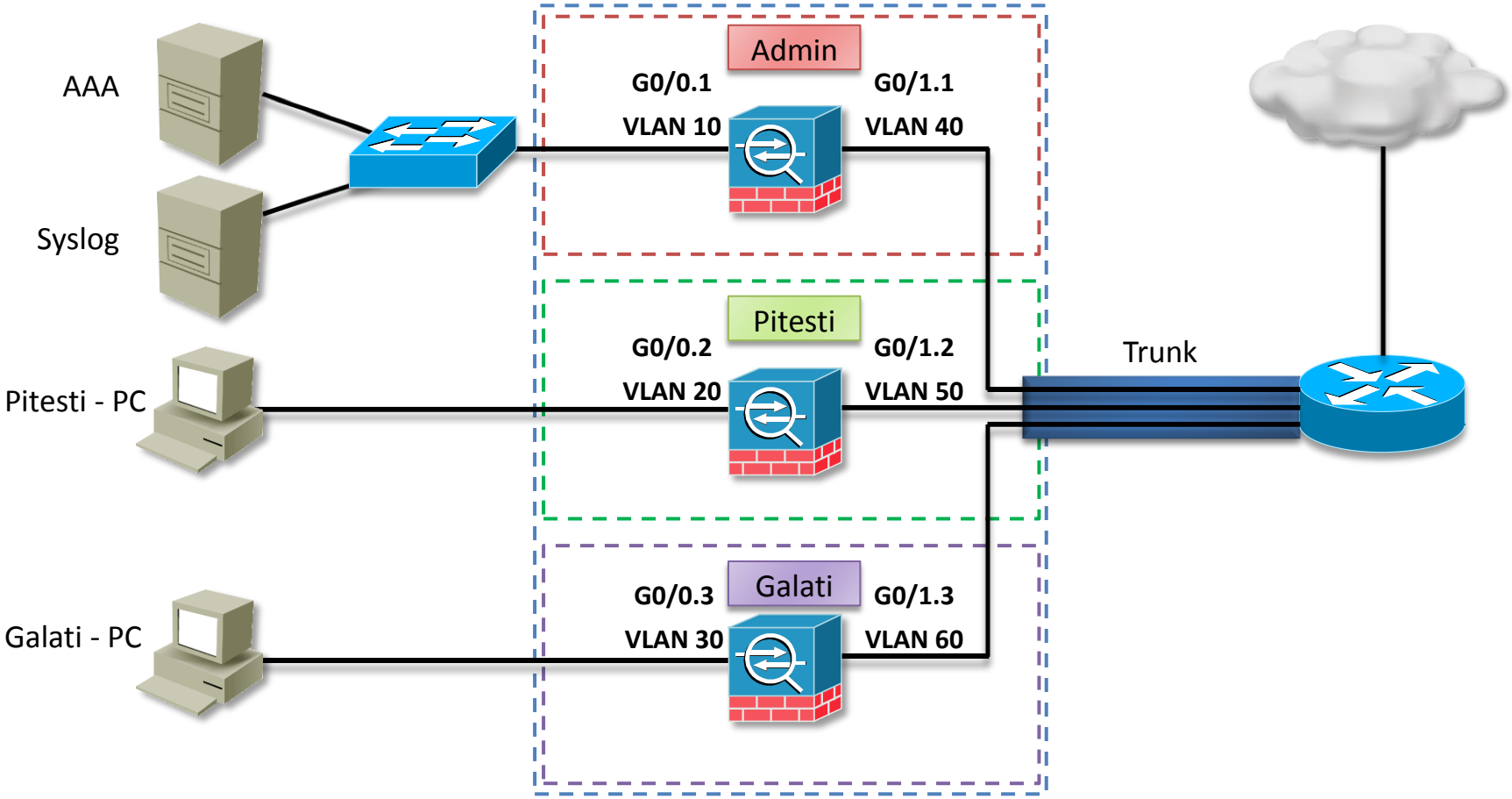
```
Waters(config)# show context
Context Name      Class      Interfaces            URL
*admin            default                        disk0:/admin.cfg
 Pitesti          default                        (not entered)
 Bacau            default                        (not entered)
```

Cisco ASA – Contexte de securitate

Studiu de caz

Studiu de caz

- Comunicarea între contexte sau cu exteriorul folosind interfețe unice



SRED

Configurații ASA - SES

```
Waters# show run
interface GigabitEthernet0/0
interface GigabitEthernet0/0.1
 vlan 10
interface GigabitEthernet0/0.2
 vlan 20
interface GigabitEthernet0/0.3
 vlan 30
interface GigabitEthernet0/1
interface GigabitEthernet0/1.1
 vlan 40
interface GigabitEthernet0/1.2
 vlan 50
interface GigabitEthernet0/1.3
 vlan 60
hostname Waters
admin_context admin
```


SRED

Configurații ASA - SES

```
context admin
  description admin Context for admin purposes
  allocate-interface GigabitEthernet0/0.1
  allocate-interface GigabitEthernet0/1.1
  config-url disk0:/admin.cfg
context Pitesti
  description Pitesti Customer Context
  allocate-interface GigabitEthernet0/0.2
  allocate-interface GigabitEthernet0/1.2
  config-url disk0:/Pitesti.cfg
context Galati
  description Galati Customer Context
  allocate-interface GigabitEthernet0/0.3
  allocate-interface GigabitEthernet0/1.3
  config-url disk0:/Galati.cfg
```


SRED

Configurații ASA – Admin Context

```
Waters/admin# show running
interface GigabitEthernet0/0.1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
interface GigabitEthernet0/1.1
 nameif outside
 security-level 0
 ip address 209.165.202.130 255.255.255.248
!
hostname admin
logging enable
logging timestamp
logging trap emergencies
logging host inside 192.168.1.10
!
route outside 0.0.0.0 0.0.0.0 209.165.202.129 1
telnet 192.168.1.0 255.255.255.0 inside
telnet timeout 5
ssh 0.0.0.0 0.0.0.0 outside
ssh timeout 5
```

Configurații ASA – Pitesti Context

```
waters/Pitesti# show running
interface GigabitEthernet0/0.2
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
interface GigabitEthernet0/1.2
 nameif outside
 security-level 0
 ip address 209.165.200.225 255.255.255.248

hostname Pitesti

!Configurație NAT pentru rețeaua Pitesti
global (outside) 1 209.165.200.230
nat (inside) 1 192.168.10.0 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 209.165.200.226 1
```


SRED

Configurații ASA – Galati Context

```
Waters/Galati# show running

interface GigabitEthernet0/0.3
 nameif inside
 security-level 100
 ip address 192.168.20.1 255.255.255.0

interface GigabitEthernet0/1.3
 nameif outside
 security-level 0
 ip address 209.165.201.2 255.255.255.224

hostname Galati

!Configurație NAT pentru Galati
global (outside) 1 interface
nat (inside) 1 192.168.20.0 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 209.165.201.1 1
```


SRED

FortiGate – VDOM-uri

Arhitectură

VDOM-uri

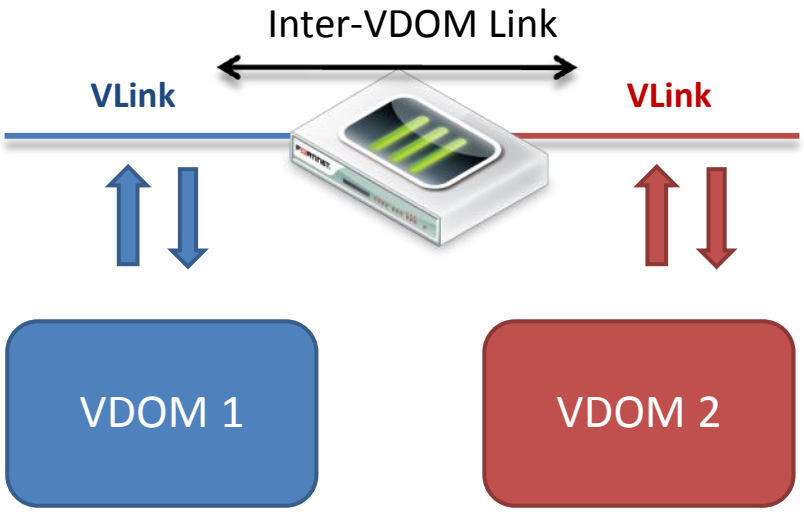
- Pe FortiOS implementarea de virtual firewalling poartă numele de Virtual Domains
- Aceeași arhitectură
  - Global – echivalent SES
  - Root VDOM – echivalent admin_context
  - VDOM X – echivalent customer_context
- Se pot crea 10 VDOM-uri implicit
  - Este nevoie de licență pentru mai multe
  - Doar FortiGate-urile de la seria 3000 în sus au posibilitatea de a aplica o licență pentru mărirea numărului de VDOM-uri
- Față de Cisco, în FortiOS nu există nici o limitare de funcționalități la trecerea în multiple-mode
  - În continuare funcționeaza VPN, protocoale de rutare etc.

Comunicare între VDOM-uri

- Se poate configura același model de comunicație ca și în cazul ASA în care fiecare (sub)interfață face parte dintr-un VLAN și comunicarea se face prin intermediului unui dispozitiv L3
- Dar există limitări
  - Dacă FortiGate are 8 interfețe, atunci pentru a putea comunica cu Internetul și între VDOM-uri pot face maxim 4 VDOM-uri (în licența de bază există 10)
  - Numărul de VDOM-uri ajunge să depindă de numărul de interfețe
  - Se pierde bandwidth și capacitate de comutare și CPU (procesare politici)
- InterVDOM Links
  - Posibilitatea de a configura o legătura software cu o politică atașată între oricare 2 VDOM-uri

Inter-VDOM links – Funcționare

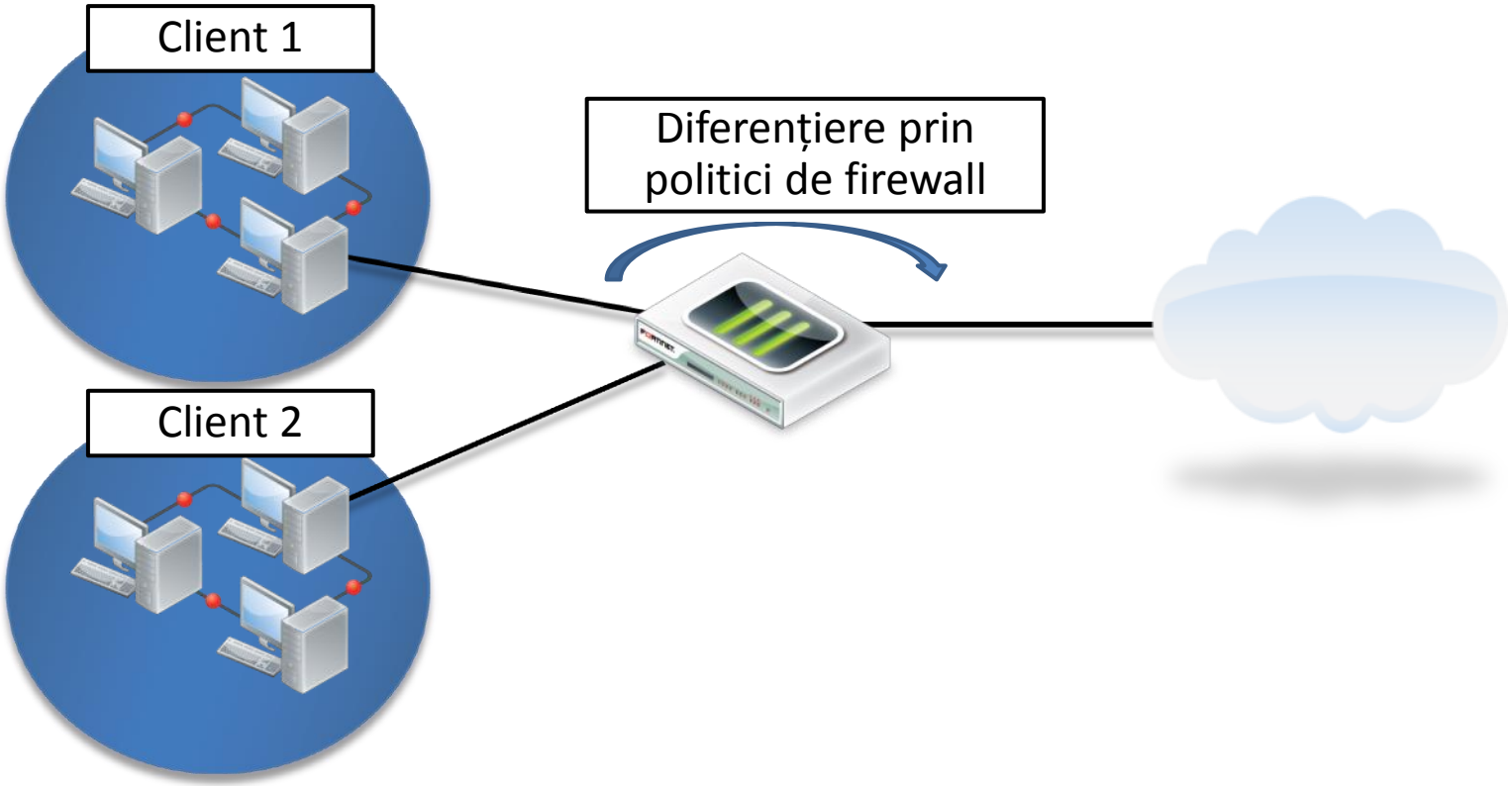
- La definirea unui Inter-VDOM link se creează 2 interfețe virtuale, fiecare alocată automat în unul din cele 2 VDOM-uri
- Administratorul fiecărui VDOM poate defini apoi politici între interfețele din VDOM-ul său și interfața sa virtuală din Inter-VDOM link
- Astfel fiecare administrator controlează precis ce poate părăsi sau intra în VDOM-ul său



SRED

Topologii – Standalone VDOM

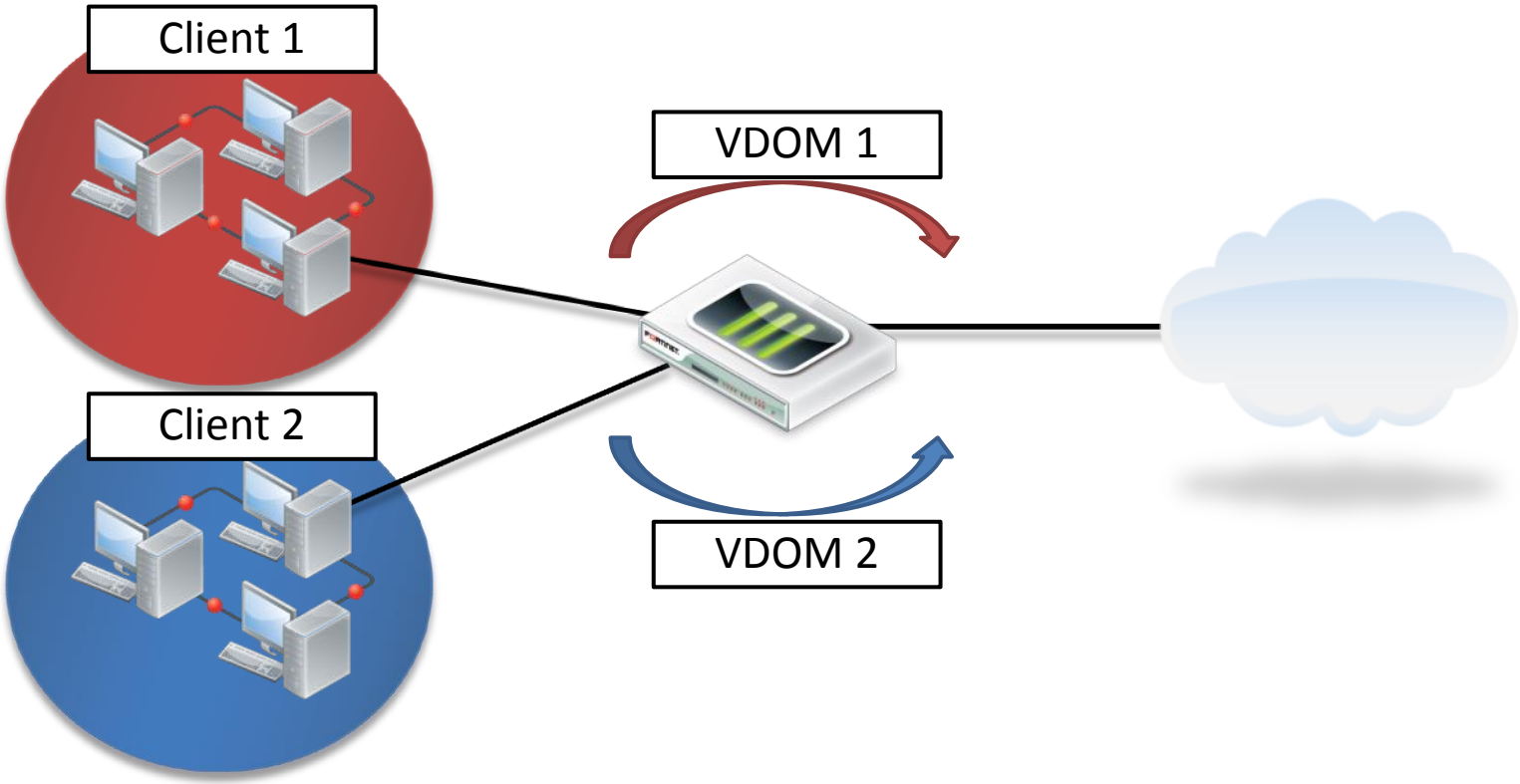
- Dacă nu se activează contextul multiplu există implicit VDOM-ul Root, invizibil pentru utilizator, în care se definesc toate politicile
- La migrarea către multiple-mode, Root VDOM-ul păstrează toate configurațiile



SRED

Topologii – Independent VDOM

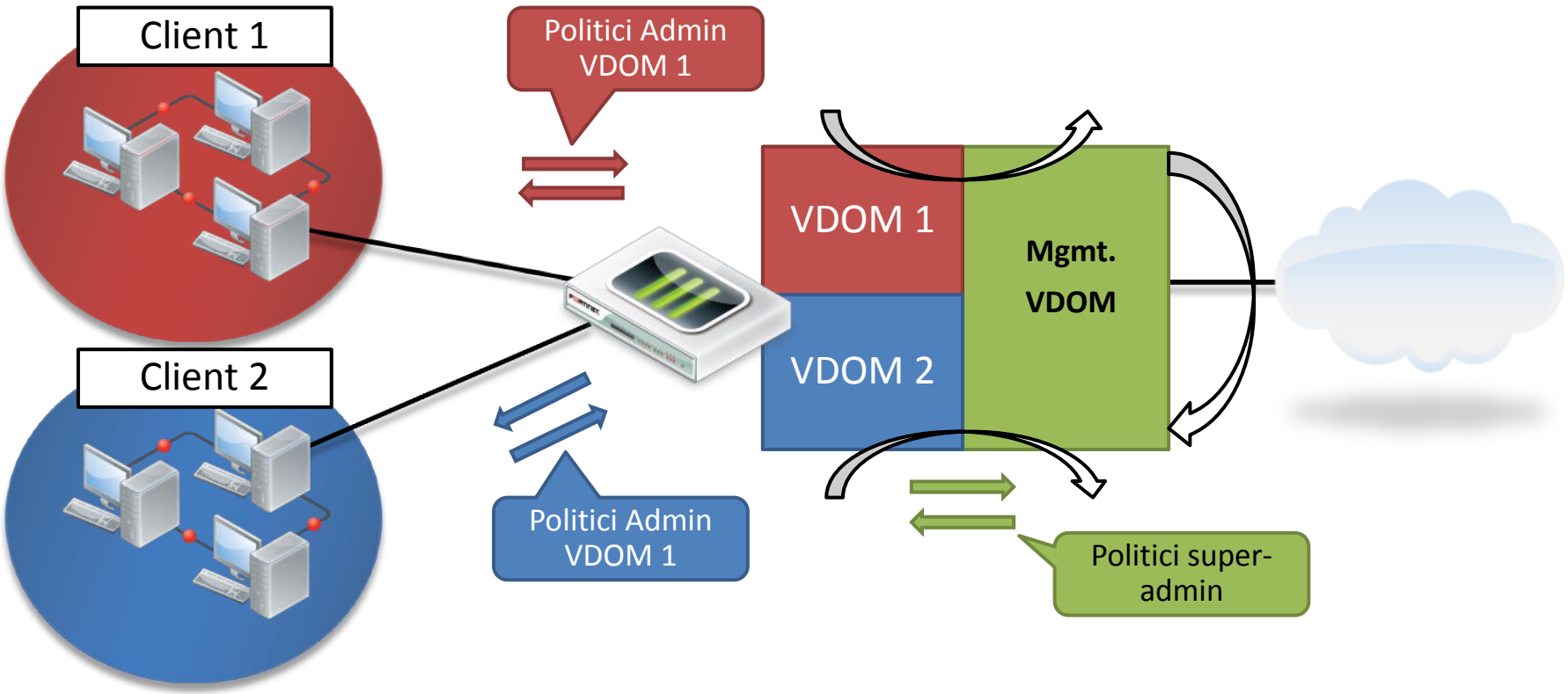
- Fiecare client are VDOM-ul său și este conectat la Internet
- Nu există comunicație între VDOM-uri
- Nu există interfețe conectate la Management VDOM – dezavanteje în funcționalite și control



SRED

Topologii – Partial mesh Management VDOM

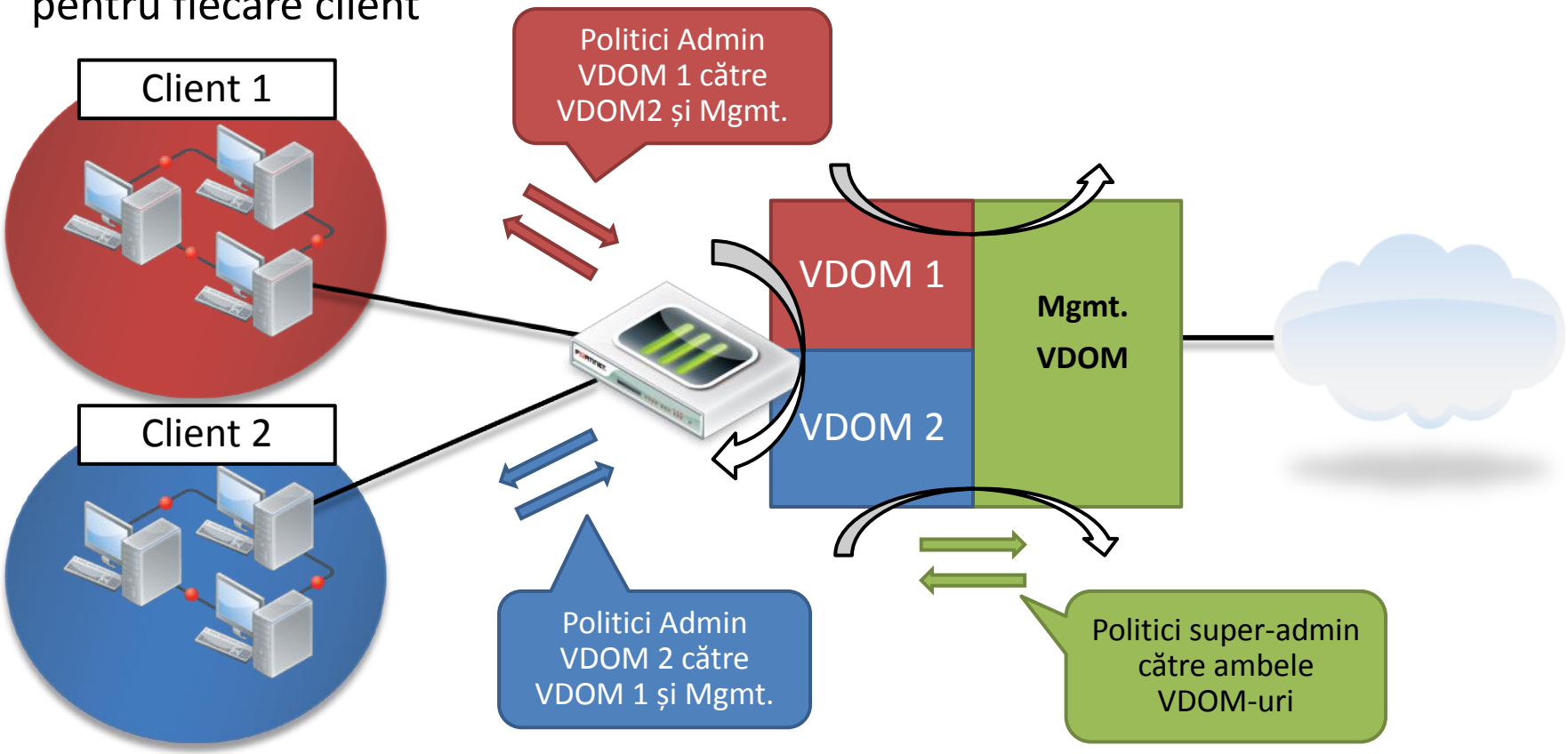
- Comunicarea dintre **VDOM1** și **VDOM2** se face prin **Mgmt**
- Super_admin-ul are grad complet de control față de traficul dintre cele 2 VDOM-uri
  - Poate fi un lucru bun sau rău depinzând de scenariu



SRED

Topologii – Full-mesh Management VDOM

- Permite un control granular asupra oricări direcții de trafic pentru fiecare VDOM_admin
- Permite super_adminului să aibă politici de Internet comune, sau specifice pentru fiecare client



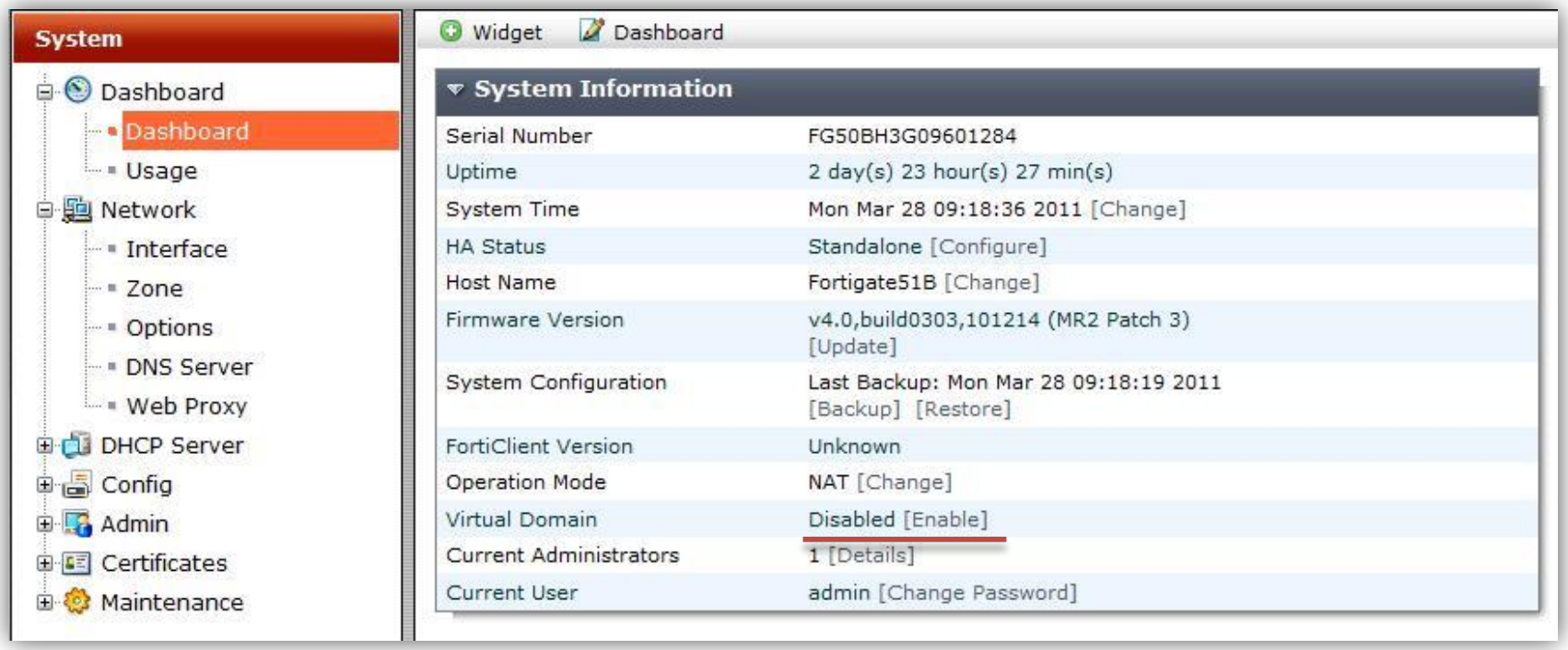
SRED

FortiGate – VDOM-uri

Implementare

Activarea multiple-mode

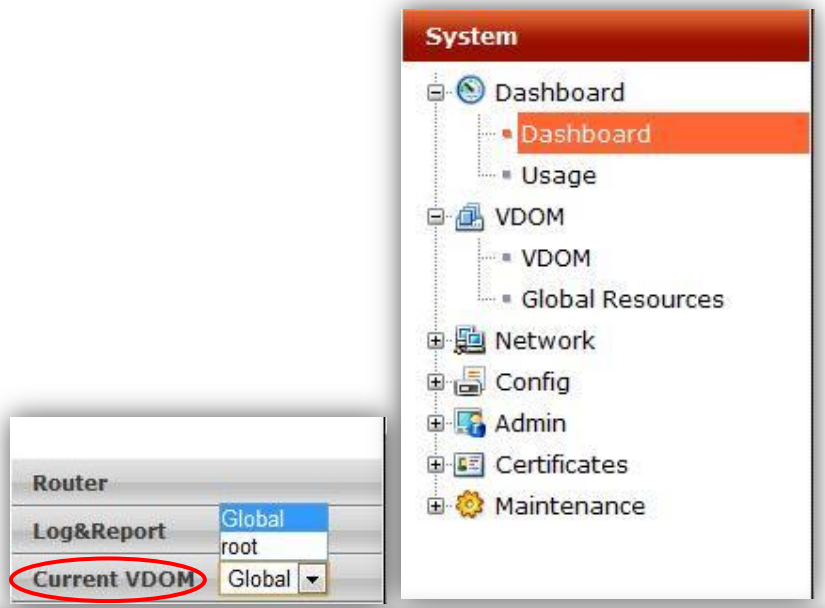
- Se face din Dashboard
  - Widgetul de System Information

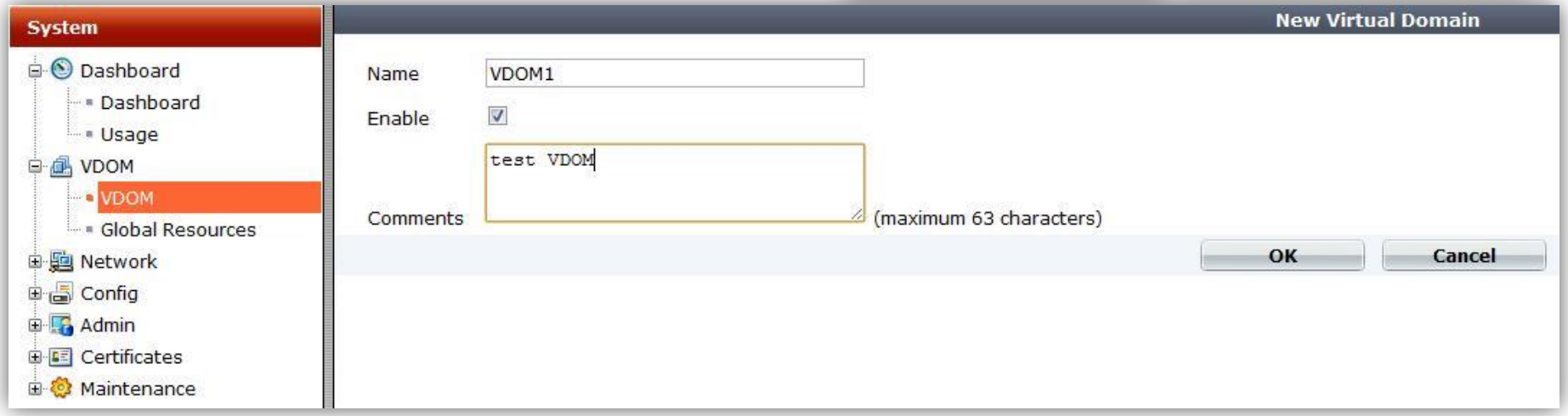


SRED

Navigare VDOM

- După activarea multiple-mode:
  - Apare un meniu de VDOM în System din care se pot crea VDOM-uri
  - Apare un drop-down din care se poate naviga dintr-un VDOM în altul



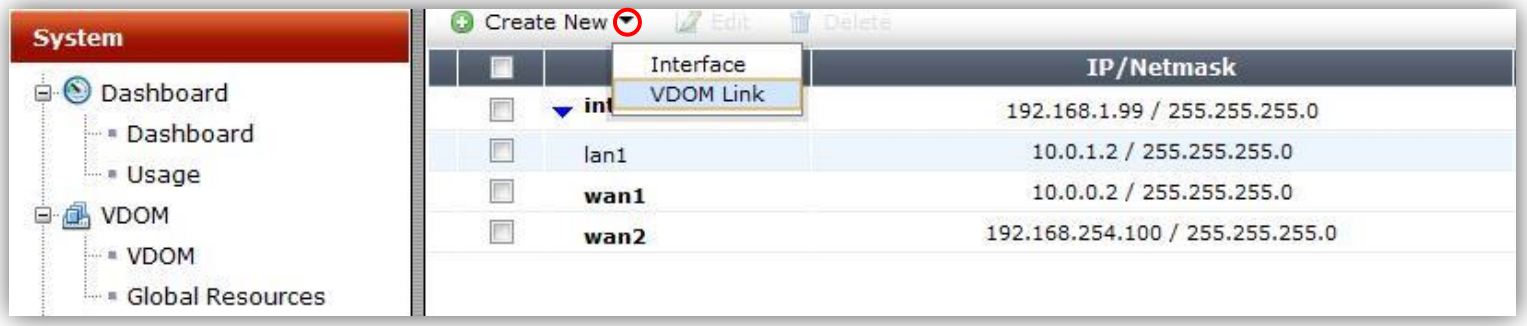


SRED

Asocierea interfețelor cu VDOMuri

- Se face din modul de configurare al interfeței

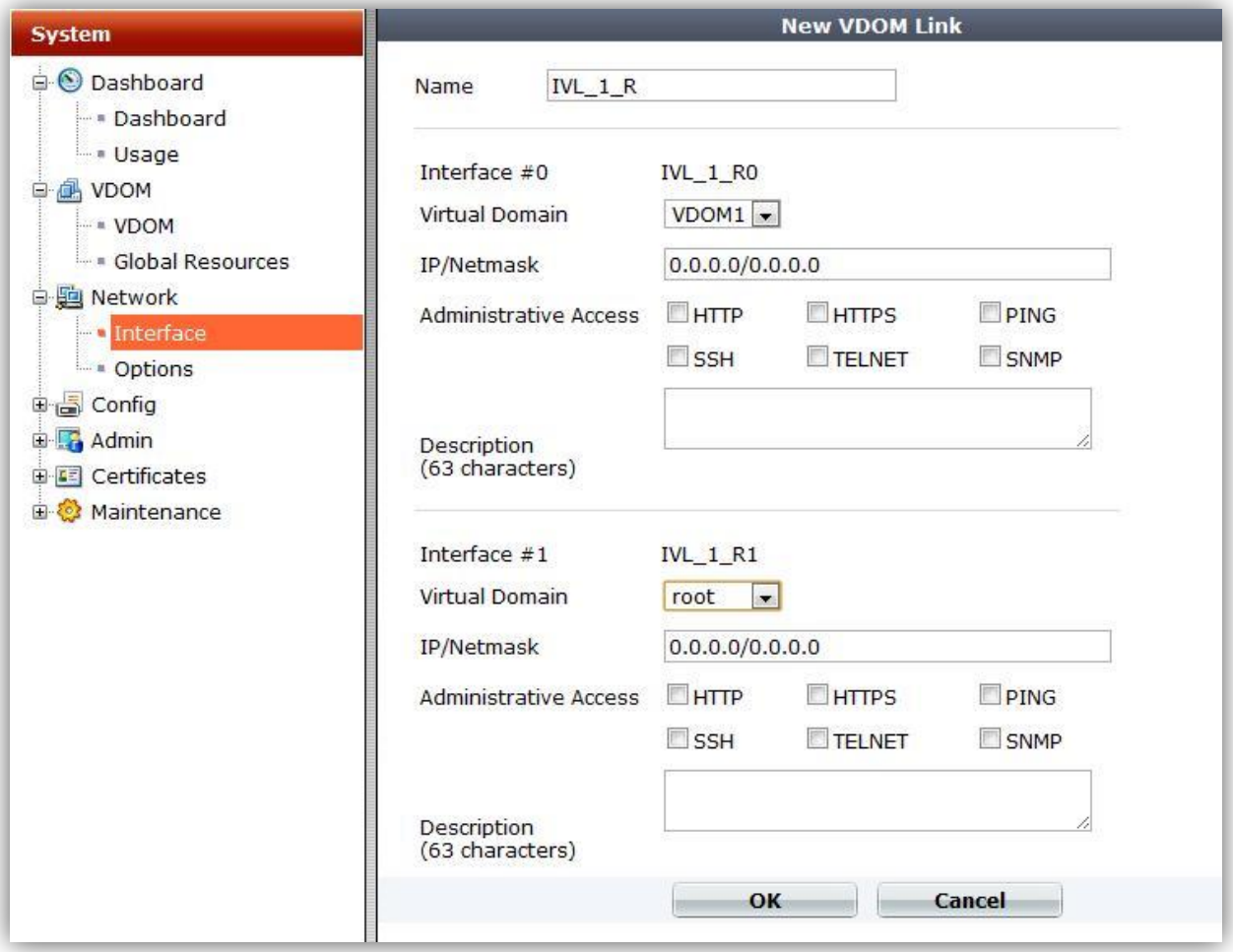
- Tot din același meniu se creează un Inter-VDOM link



SRED

Creare Inter-VDOM Link

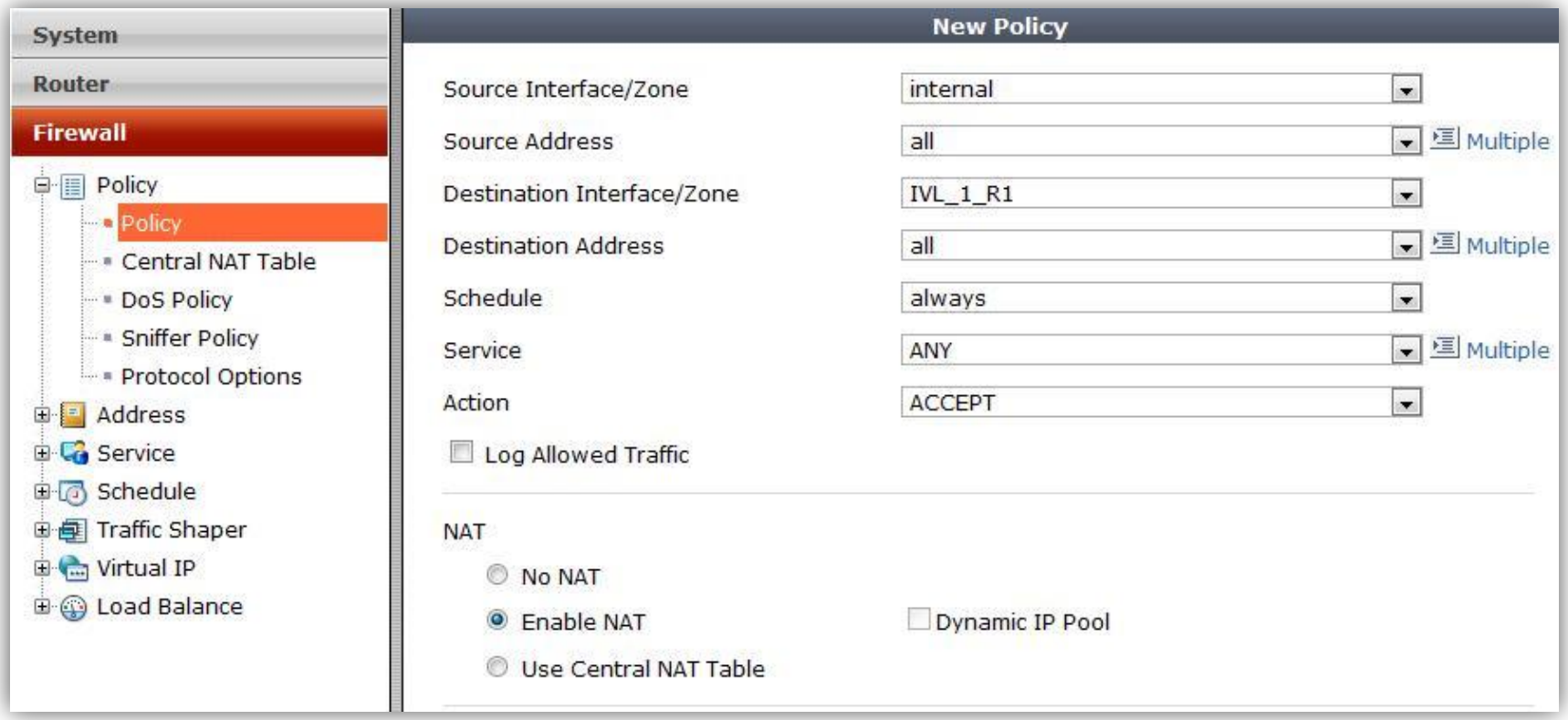
- Din modul global
- La creare se alege numele link-ului și VDOM-urile între care se face legătura
- Opțional se pot asigna adrese IP celor 2 interfețe virtuale create



SRED

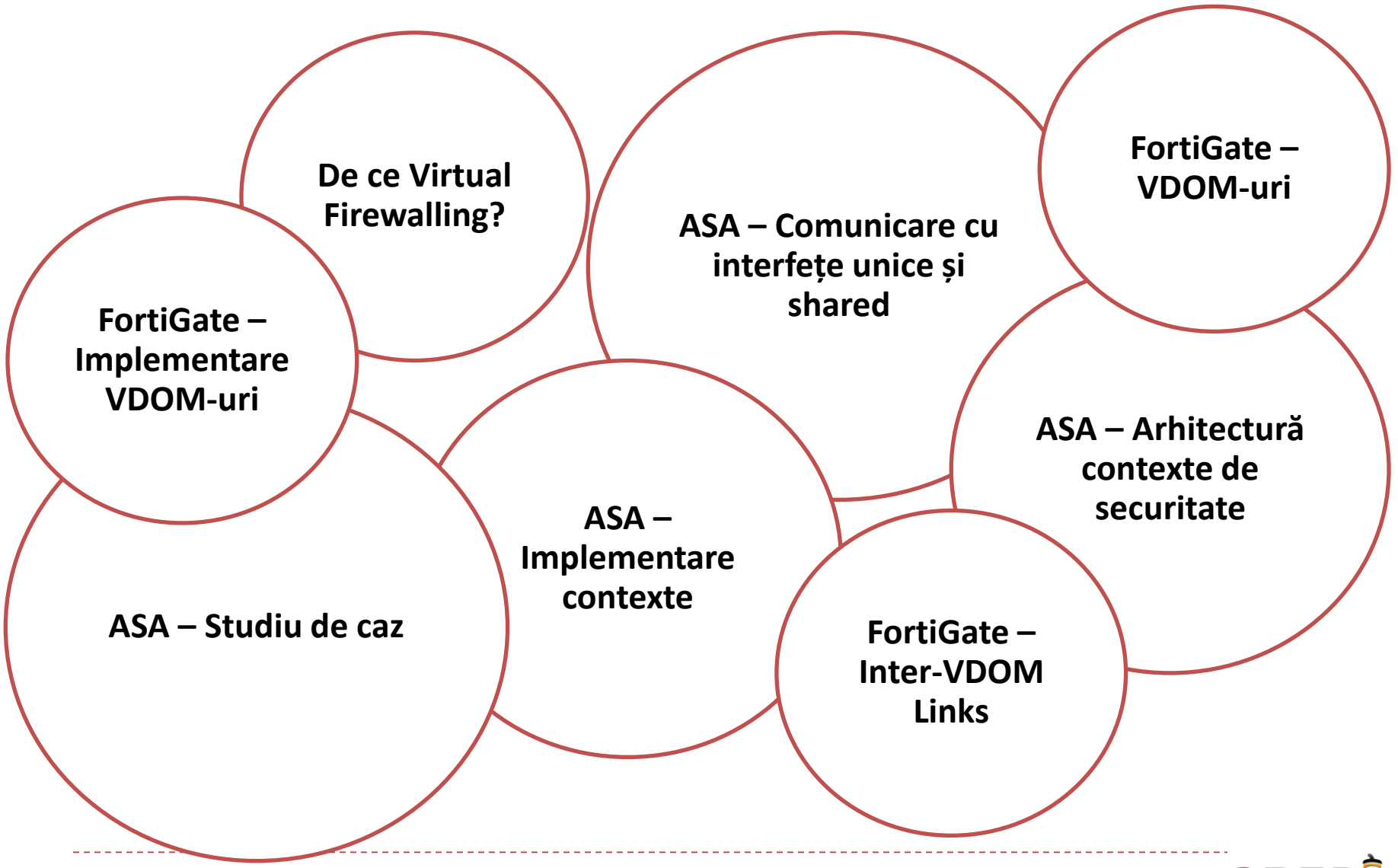
Comunicare între VDOM-uri

- Din modul global nu se pot crea politici de firewall
- Fiecare administrator trebuie să își configureze propriile politici între interfața fizică și cea virtuală și propriile rute prin interfața virtuală



SRED

Overview



SRED

Cursul viitor…

- Test grilă
  - Primele 5 cursuri
  - 9.04.2013, 19:00

- Curs 7: Basic VPNs
  - 16.04.2013

SRED