Basic VPNs

17 aprilie 2014

Obiective

- Clasificarea VPN-urilor
  - Overlay vs. Point-to-point
  - Site-to-Site vs Remote-access
  - Criptografie – elemente esențiale
- IPSec Site-to-Site VPNs
  - Servicii IPSec: criptare, autentificare, integritate
  - Protocoale IPSec
  - Funcționarea IPSec
- Cisco ASA
  - Implementarea Site-to-Site IPSec
- Fortinet
  - Implementarea Site-to-Site IPSec

Ce sunt VPN-urile?

- O soluție de creare a unei conexiuni end-to-end privată peste o infrastructură publică și nesigură precum Internetul
- Există și soluții WAN ce oferă aceleași servicii precum un VPN: linii închiriate.
- Care este diferența dintre un VPN și a avea o linie închiriată?
  - costul

SRED

Clasificarea soluțiilor VPN în funcție de SP

- Funcție de SP:
  - Overlay
  - Point-to-point

- Modelul overlay face rețeaua ISP-ului invizibilă pentru clienți
- Ruterele ISP-ului nu ajung să cunoască rețelele clienților
- Modele de VPN-uri overlay: PPTP, L2TP, IPSec

SRED

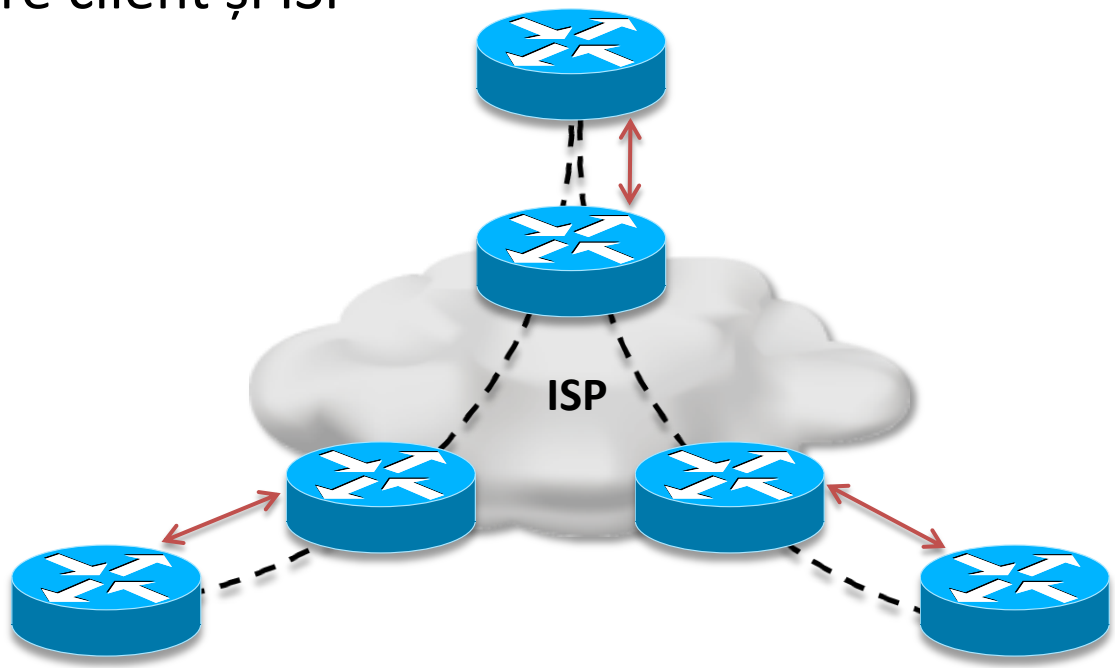
Modele Overlay VPN

Tehnologie VPN	Avantaje	Dezavantaje
PPTP	• suport extins pe platforme Microsoft • oferă criptare (MPPE) • oferă compresie (MPPC)	• schemă slabă de autentificare și criptare • sistem proprietar de key management • nescalabil pe partea de server din cauza unei limite de sesiuni
L2TP	• independent de L2 • poate asigura confidențialitate folosind IPSec	• nu a fost niciodată adoptat la o scară foarte mare
IPSec	• scheme puternice de criptare și autentificare • este open și extensibil	• funcționalitatea ridicată aduce complexitate ridicată • interoperabilitate scăzută între vendori • posibile probleme cu Firewall/NAT

SRED

Point-to-point VPNs

- În modelul point-to-point ISP-ul participă în procesul de rutare
- Adiacența se face între client și ISP

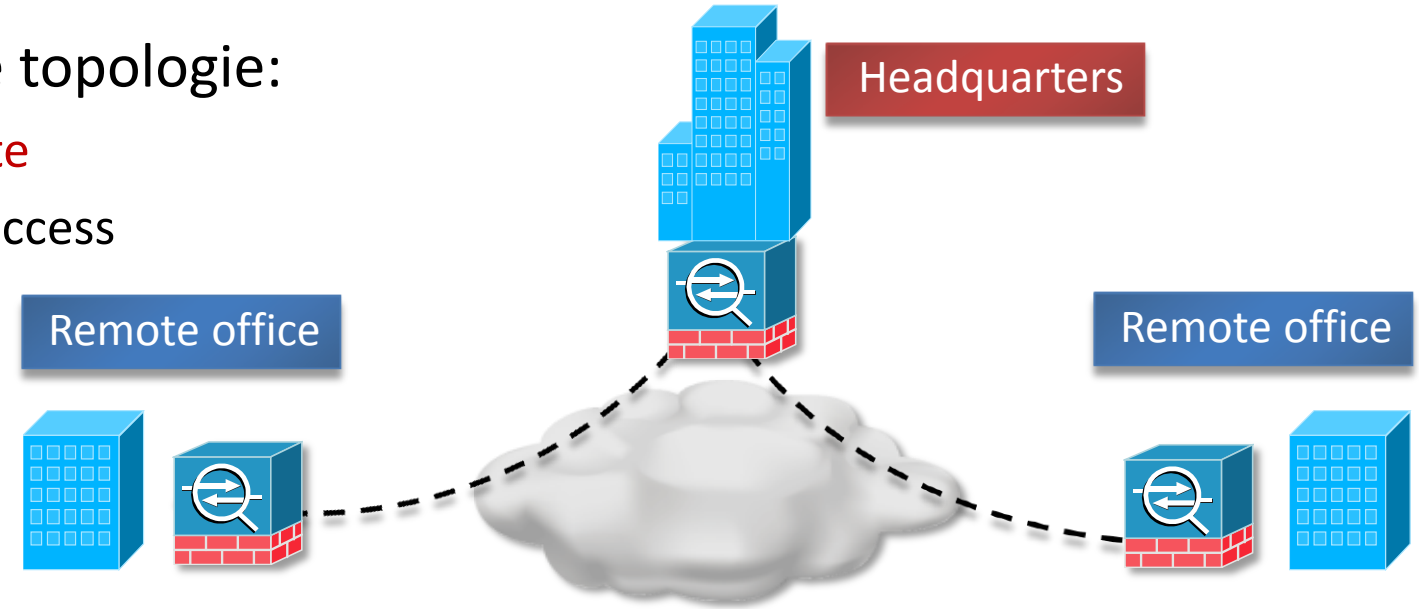


- Modele overlay constituiau 90% din implementări până la apariția protocolului MPLS
- Totuși MPLS nu oferă nici o schemă de confidențialitate

SRED

Clasificarea soluțiilor VPN în funcție de topologie

- Funcție de topologie:
  - Site-to-Site
  - Remote-access

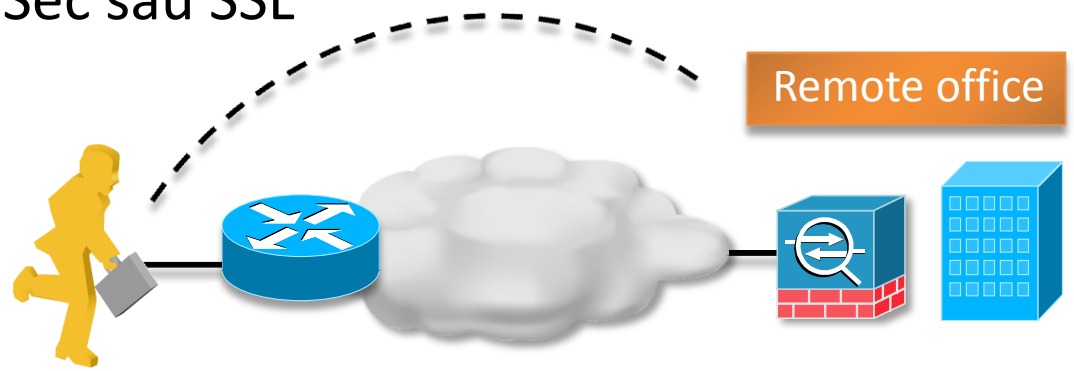


- O topologie Site-to-Site leagă mai multe locații peste Internet
- Configurațiile nu trebuie făcute decât pe firewall-uri/rutere
- Nu necesită un client pentru conectare
  - Toți angajații de la locația respectivă folosesc ca gateway firewall-ul /ruterul configurat pentru conexiunea VPN

SRED

VPN-uri Remote-access

- O topologie Remote-access oferă posibilitatea conectării la VPN pentru un teleworker
- Gateway-ul teleworkerului nu este un gateway VPN
- Oferă o conexiuni securizată până la resursele interne ale companiei
- Folosește un client de VPN pentru conectarea la serverul aflat la remote office
- În general IPSec sau SSL



SRED

Tunelare: încapsulare

- Orice tehnologie de VPN se bazează pe tunelare
- Tunelarea presupune încapsularea cu încâ un antet la nivelul la care se contruiește tunelul

- Exemplu: tunel IPIP
  - Folosit când rețeaua sursă sau destinație nu este cunoscută în tabela de rutare a unui ruter intermediar

- Antetul IP original este ascuns tuturor ruterelor dintre cele 2 capete ale tunelului

SRED

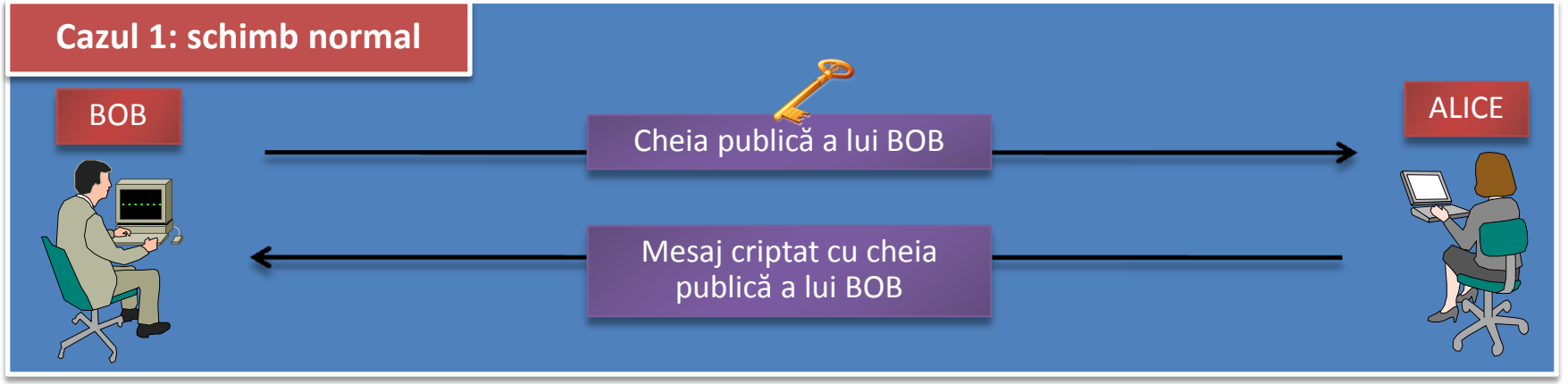
Cryptography trivia – Round 1

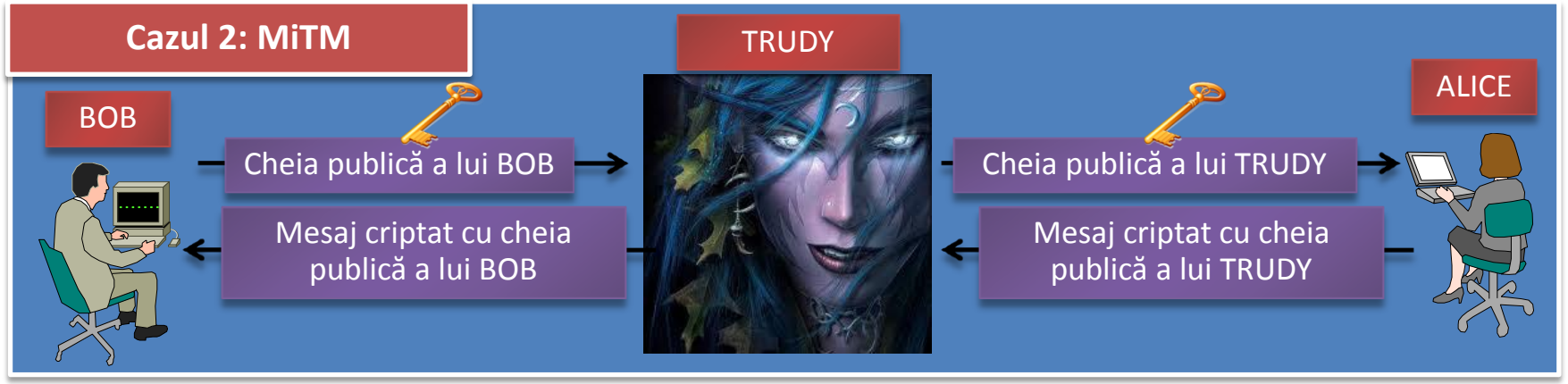
- Care sunt cele 2 tipuri de criptografie?
  - Simetrică
  - Asimetrică
- Ce presupune criptografia simetrică?
  - Folosirea aceleiași chei atât pentru criptare cât și pentru decriptare
- Ce presupune criptografia asimetrică?
  - Folosirea de chei diferite pentru criptare și decriptare
- Care dintre cele două variante pot fi realizate în hardware?
  - Ambele
- Care dintre cele două variante este mai rapidă?
  - Simetrică
- Care este problema criptografiei simetrice?
  - Schimbul inițial al cheii de criptare între două entități remote
- Rezolvă criptografia asimetrică această problemă?
  - Depinde

SRED

Public key infrastructure

- Ce este PKI?
- De ce avem nevoie de PKI în criptare asimetrică?

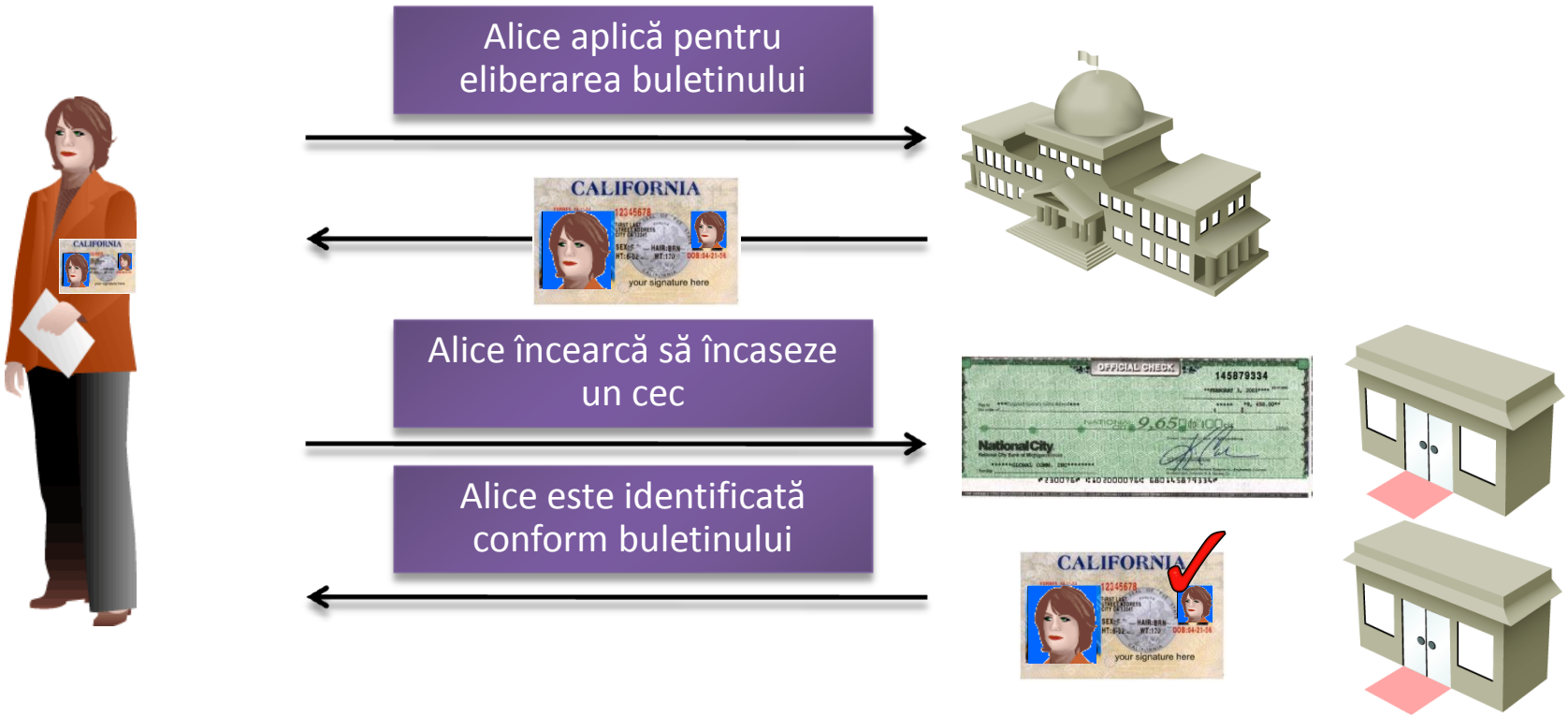




SRED

Public key infrastructure – Funcționare

- Criptare asimetrică fără PKI nu rezolvă problema distribuției unei chei inițiale între cele două entități
- Funcționarea PKI este asemănătoare funcționării certificatelor de identitate



SRED

Public key infrastructure – Funcționare

- Analogia de mai devreme funcționează pentru că atât Alice cât și banca au încredere în aceeași autoritate comună (statul care a eliberat buletinul)
- În PKI o autoritate eliberează un certificat digital ce conține:
  - Informație despre deținătorul certificatului (nume, vârstă etc)
  - Cheia publică a deținătorului certificatului
- … și este semnat cu cheia privată a autorității
- Însă și o autoritate poate fi atacată MiTM
  - dar mult mai greu
- Concluzie: nu există un mod perfect de a schimba o informație în mod securizat; schema finala se bazează pe încredere.

Cryptography trivia – Round 2

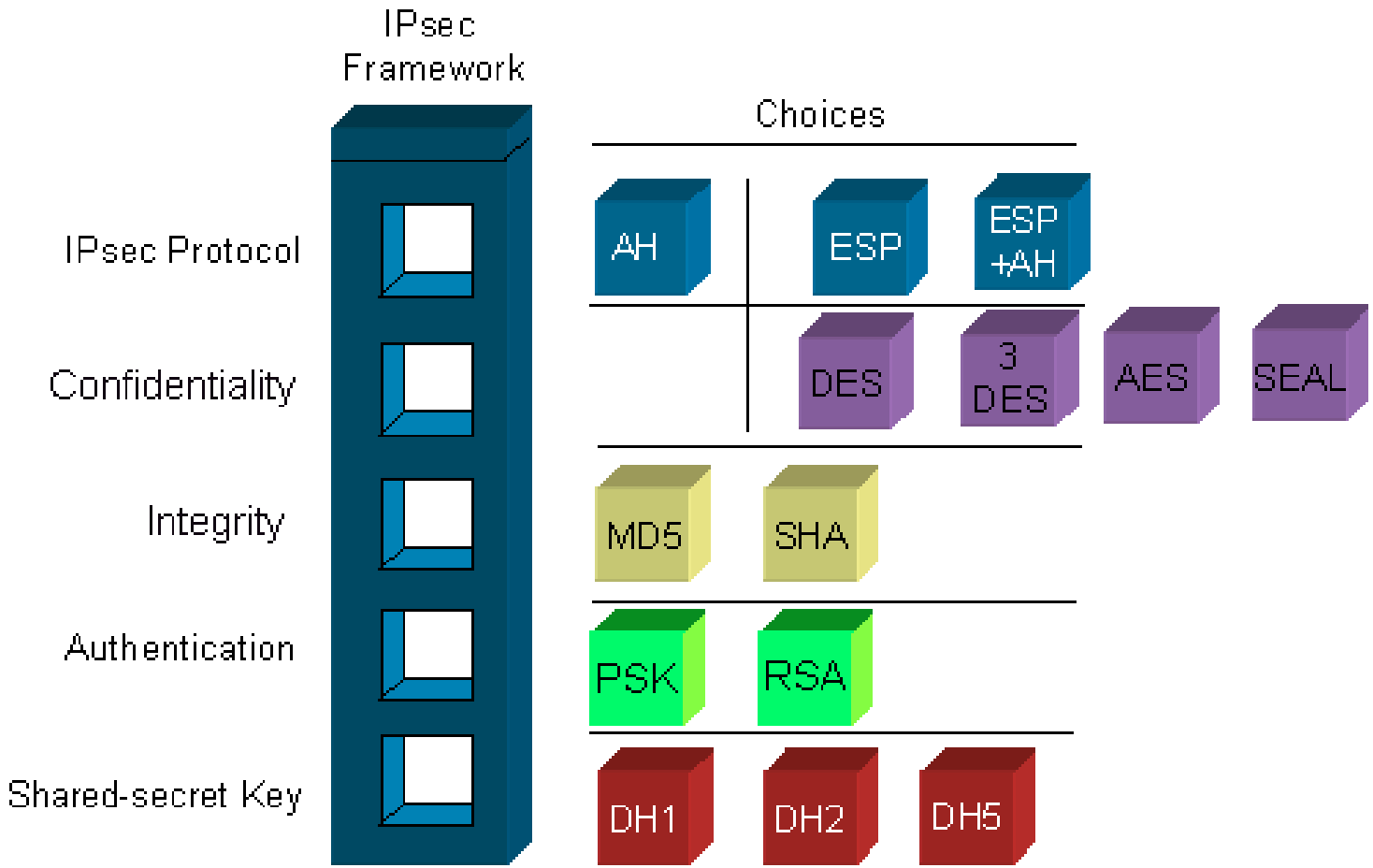
- Care din cele de mai jos poate fi folosită ca o schemă de autentificare?
  - Pre-shared key
  - RSA
  - DES

- Care este diferența între autentificare și autentificare_cu_nonrepudiere?
  - Autentificarea simplă autentifică un grup de persoane fără a oferi posibilitatea de a identifica o persoană în grupul respectiv
  - Autentificarea cu nonrepudiere identifică unic o persoană ce nu își poate repudia juridic identitatea
- Exemplu:
  - Autentificarea simplă poate fi considerată accesarea unui share Windows cu aceeași parolă pentru toți utilizatorii
  - Autentificarea cu nonrepudiere poate fi considerată PIN-ul unui card de credit

SRED

IPSec – Framework

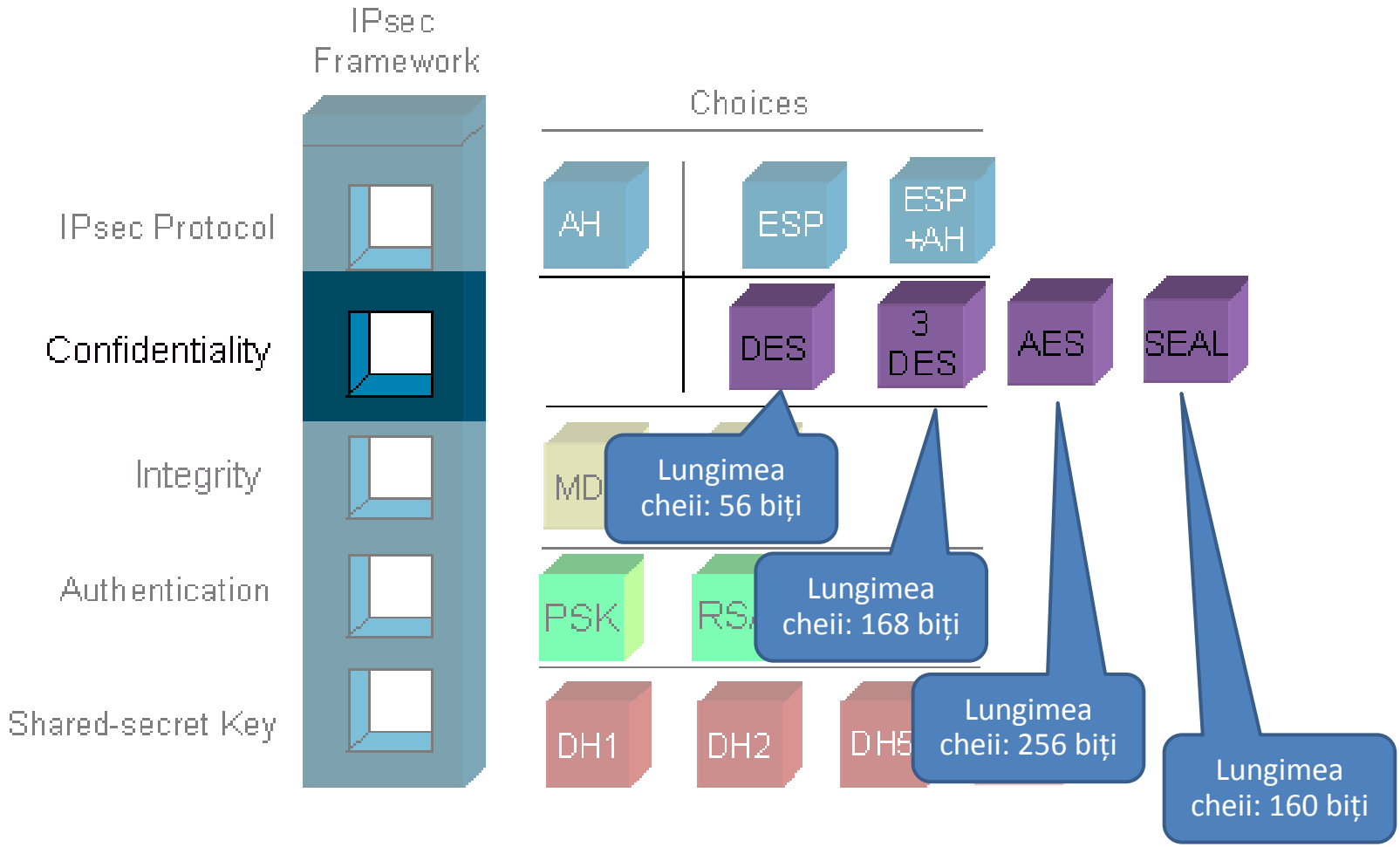
- IPSec este un framework de protocoale



SRED

IPSec – Framework

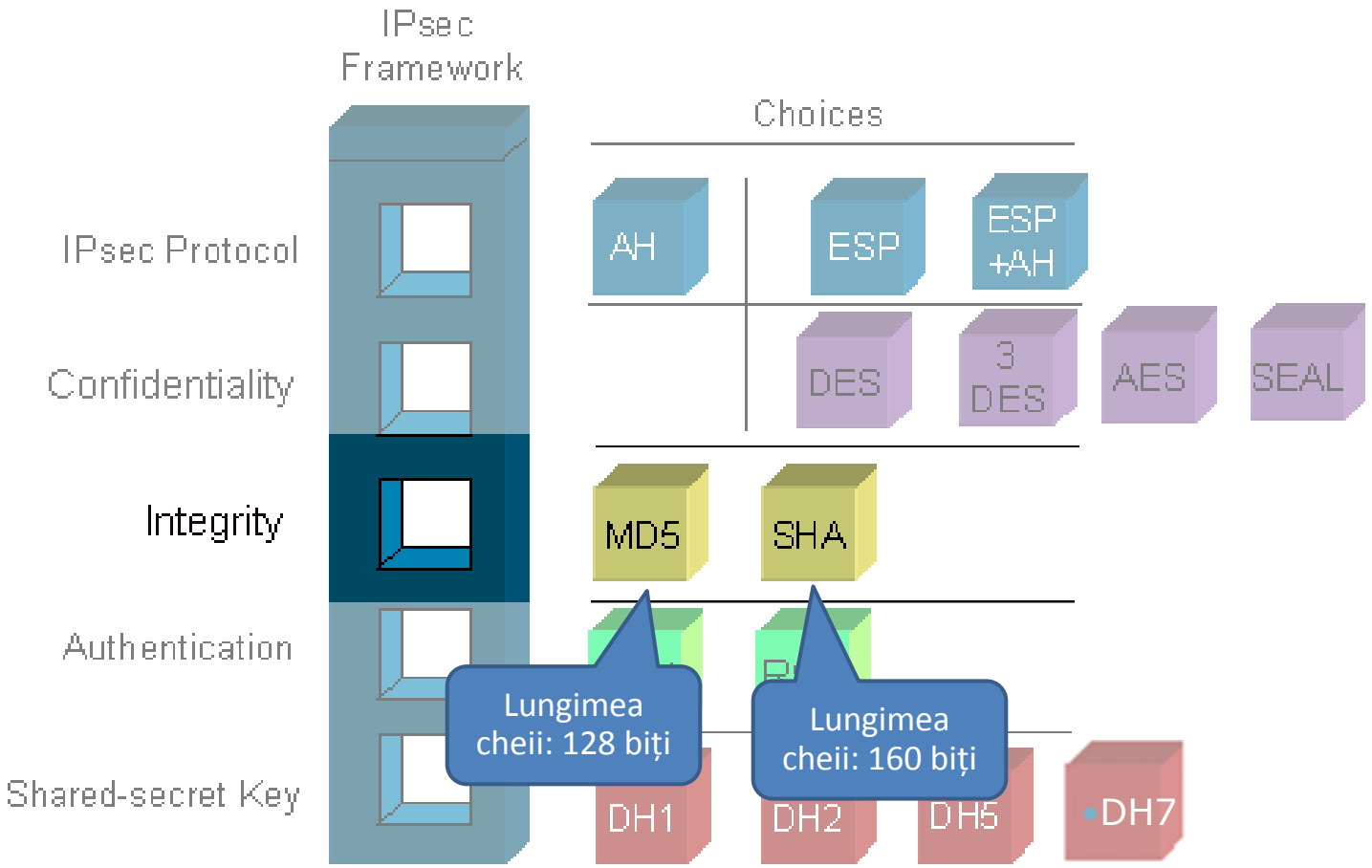
- IPSec: Confidențialitate



SRED

IPSec – Framework

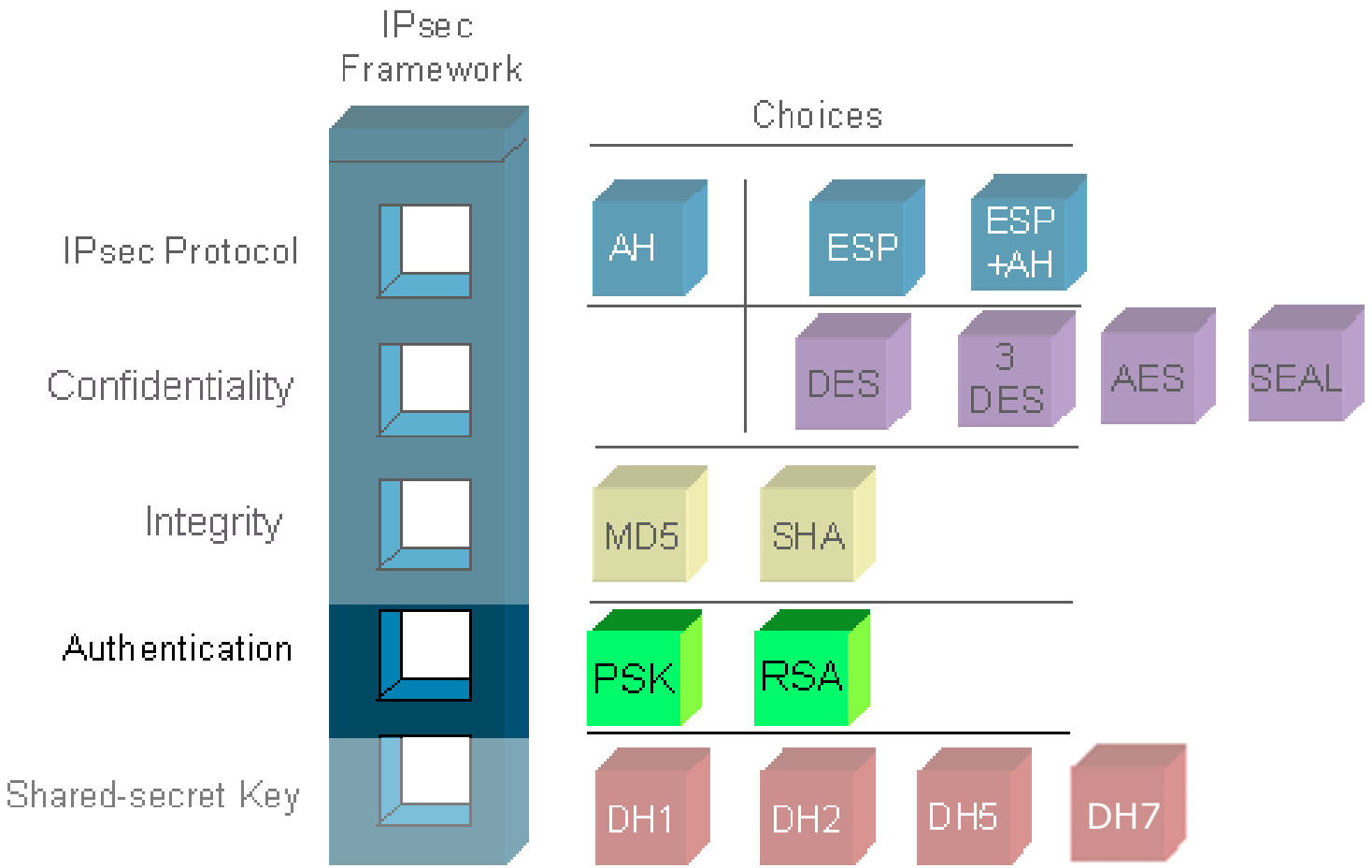
- IPSec: integritate



SRED

IPSec – Framework

- IPSec: autentificare cu non-repudiere



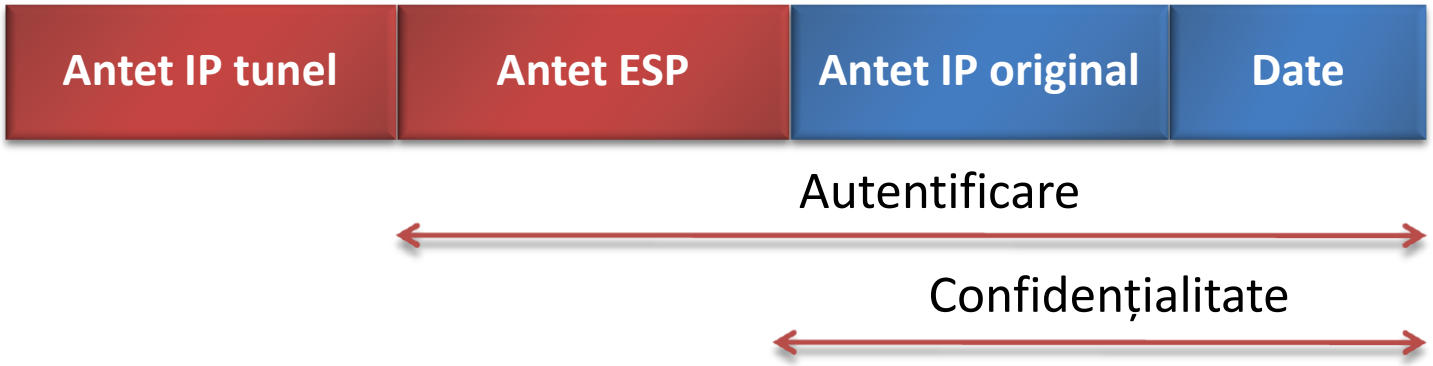
SRED

IPSec – Protocoale folosite

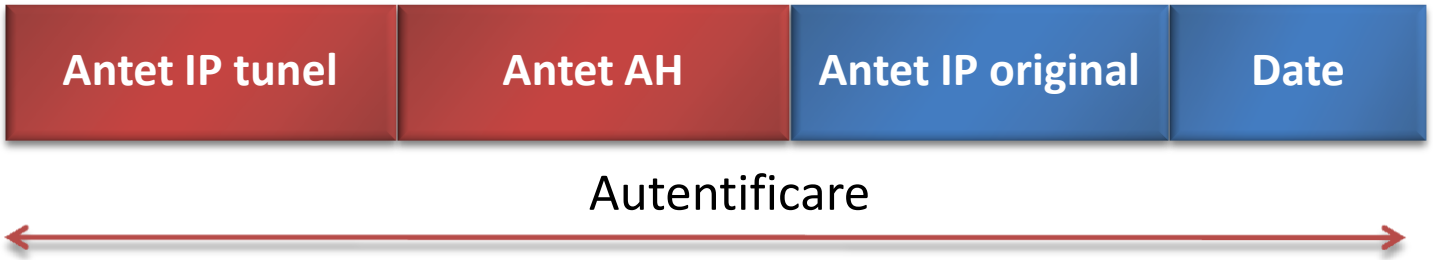
- IPSec definește în standard următoarele protocoale
  - ESP – protocol folosit pentru încapsulare ce oferă suport pentru toate serviciile IPSec
  - AH – protocol folosit pentru încapsulare ce nu oferă suport pentru confidențialitate
  - IKE – protocol folosit pentru a negocia serviciile IPSec între două capete ale unui tunel
- Structurile de date interne ce definesc ce protocoale folosește IPSec pentru confidențialitate, integritate etc se numesc SA-uri (Security Associations)
- IKE este folosit pentru a negocia SA-urile IPSec

IPSec – ESP vs. AH

- ESP oferă confidențialitate și autentificare + integritate pentru antetul IP original, pentru antetul ESP și pentru payload



- AH oferă autentificare+integritate pentru întreg pachetul



- Se pot folosi ambele protocoale în același timp. De ce s-ar dori acest lucru?

SRED

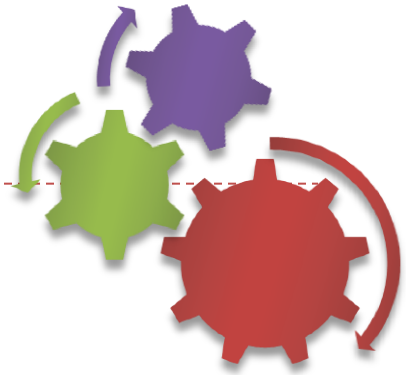
IPSec – Moduri de operare

- IPSec are două moduri de operare:
  - Transport
  - Tunel
- Modul **tunel** adaugă un nou antet IP pe lângă antetul AH sau ESP
  - Mărește pachetul cu 20 bytes

- Modul **transport** inserează antetul ESP/AH între antetul IP original și antetul de nivel 4
  - Nu se adaugă un antet IP nou
  - Util pentru situațiile în care pachetele sunt foarte mici

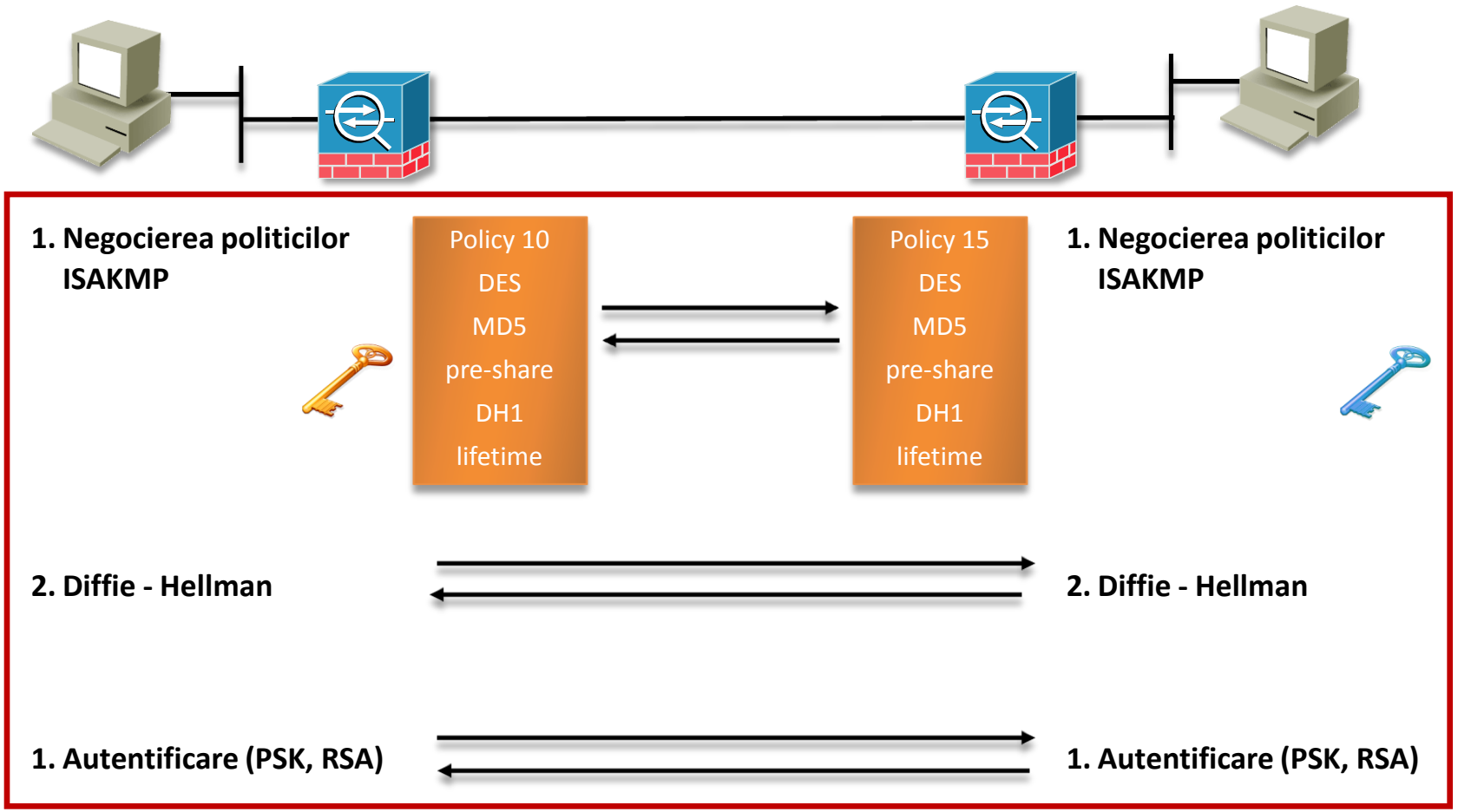
SRED

IPSec – Funcționare IKE



- Toți parametrii SA-urilor sunt negociați folosind IKE
- IKE are 2 faze
  - IKE phase 1 – prima fază a IKE este gestionată de protocolul ISAKMP
  - IKE phase 2 – numită și IPSec phase
- IKE phase 1 (ISAKMP)
  - Are rolul de a negocia SA-uri ce vor fi folosite pentru a securiza negocierea SA-urilor din faza a doua
  - Folosește protocolul de criptare asimetrică Diffie-Hellman pentru a negocia o cheie simetrică cu care se vor cripta propunerile de SA-uri din faza a doua
  - Autentifică cele 2 capete ale tunelului
- IKE phase 2
  - Se negociază SA-uri peste tunelul sigur creat de ISAKMP pentru a fi folosite la criptarea traficului de date

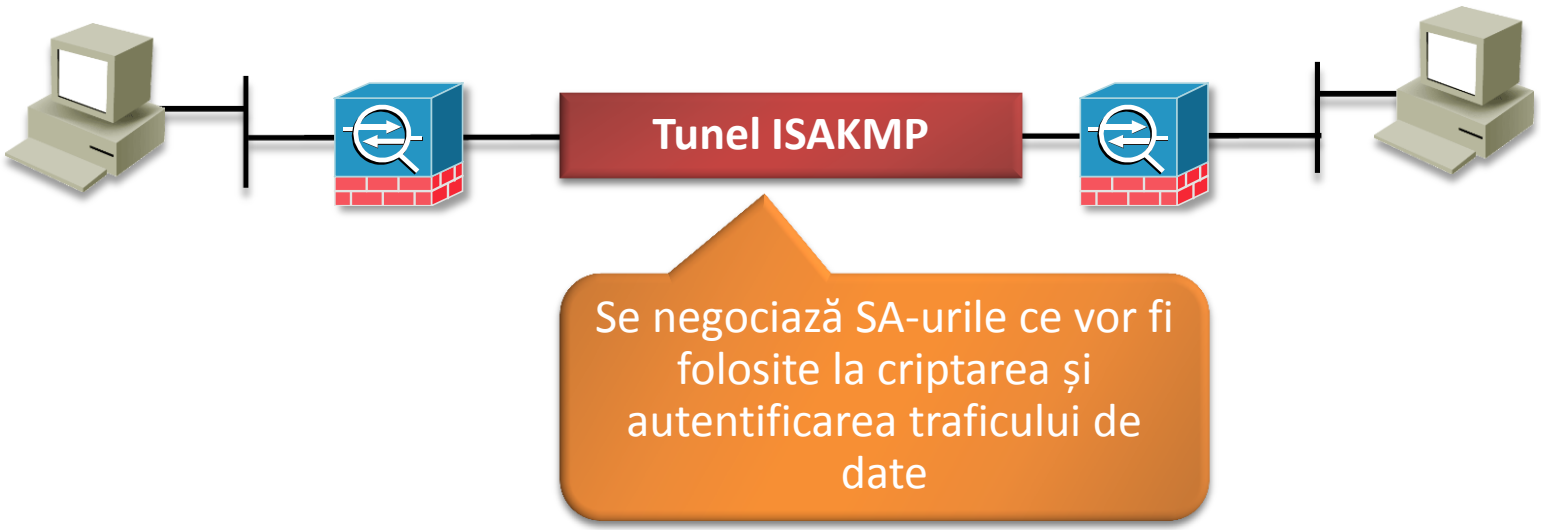
IKE phase 1 - ISAKMP



- În urma acestei faze fiecare firewall va avea un SA pe care îl va folosi atât pentru transmisie cât și recepție în faza a doua

SRED

IKE phase 2



- SA-urile din aceasta fază sunt unidirecționale
  - Există un SA folosit pentru transmisie și altul pentru recepție
  - Totuși, dacă SA-urile diferă, tunelul nu este realizat
- În standardul oficial se specifică posibilitatea de a avea nivele de securitate diferite pentru transmisie și recepție, dar nici un vendor nu implementează această opțiune.

SRED

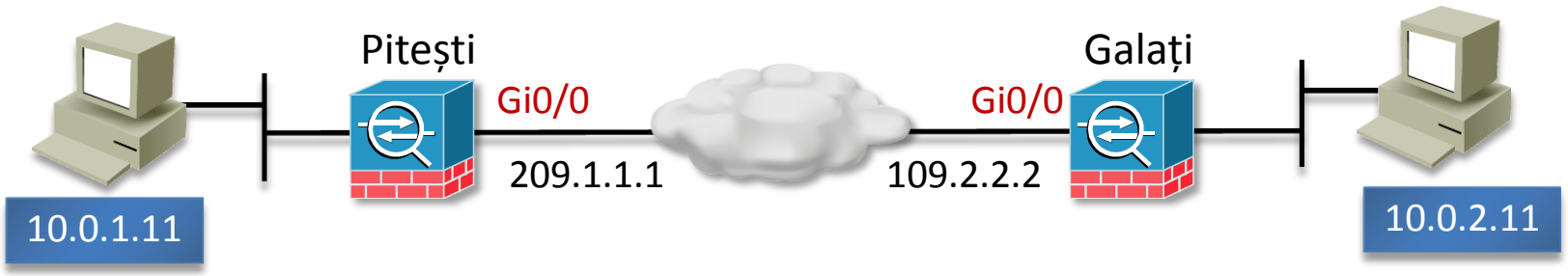
Cisco ASA
Configurarea IPSec Site-to-Site VPN

Pași de configurare parametri ISAKMP

- Pasul 1: activarea ISAKMP
- Pasul 2: definirea politicilor ISAKMP
- Pasul 3: definirea unui tunnel-group
- Pasul 4: definirea PSK pentru autentificare

SRED

Activare ISAKMP



- Activarea ISAKMP pe interfață

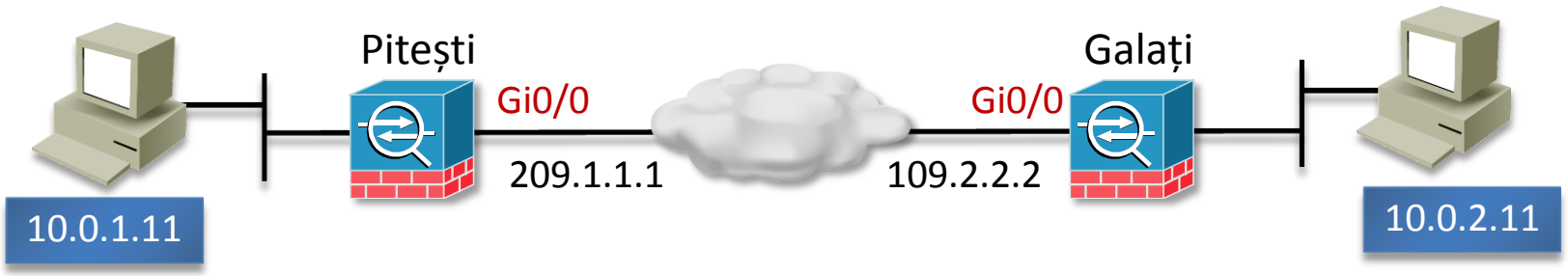
```
Pitești(config)# isakmp enable outside
```

- Opțional (pentru ASA OS 7.0, 7.1): Activarea posibilității de a termina un tunel pe ASA

```
# Pentru 7.0
Pitești(config)# sysopt connection permit-ipsec
# Pentru 7.1
Pitești(config)# sysopt connection permit-vpn
```


SRED

Configurarea unei politici ISAKMP

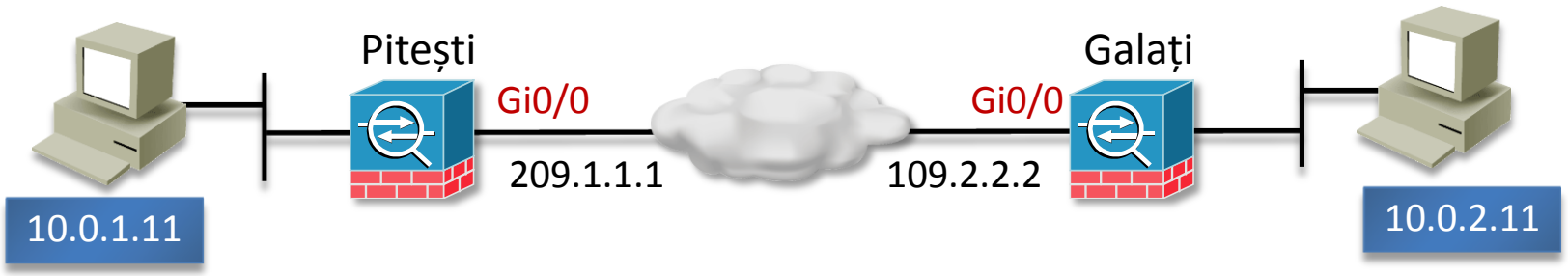


- Politicile ISAKMP sunt parcurse în ordinea indexului configurat până la găsirea unei compatibilități perfecte între cele două capete ale tunelului

```
Pitesti#(config)# isakmp policy 10
Pitesti#(config-isakmp-policy)# encryption des
Pitesti#(config-isakmp-policy)# hash sha
Pitesti#(config-isakmp-policy)# authentication pre-share
Pitesti#(config-isakmp-policy)# group 1
Pitesti#(config-isakmp-policy)# lifetime 86400
```


SRED

Configurarea unui tunnel-group

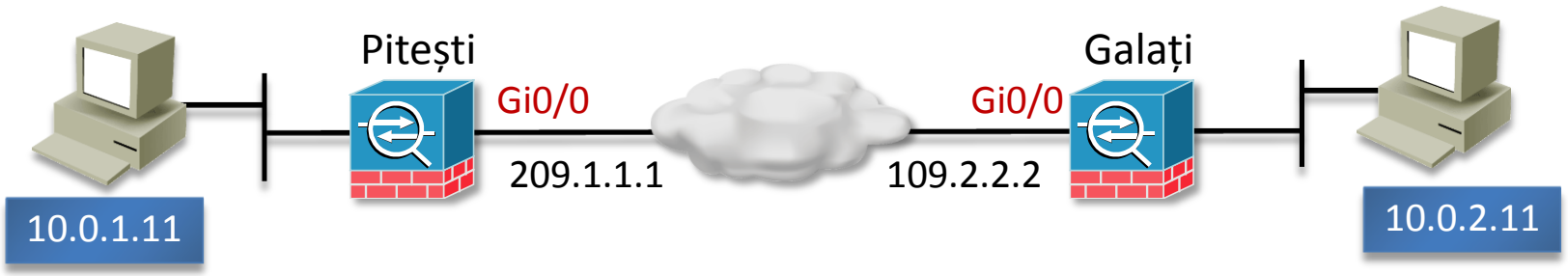


- Conceptul de tunnel-group a fost preluat de la VPN 3000 Concentrators
- Definește tipul de tunel folosit (Site-to-Site/Remote-access) și peer-ul cu care se va construi tunelul
- Atenție: deși primul argument al comenzii este un string, trebuie introdus IP-ul celuilalt capăt al VPN-ului

```
Pitesti(config)# tunnel-group 109.2.2.2 type ipsec-l2l
```


SRED

Configurarea PSK



- Tot în tunnel-group se definește și pre-shared key-ul folosit pentru autentificare

```
Pitesti(config)# tunnel-group 109.2.2.2 ipsec-attributes
Pitesti(config-ipsec)# pre-shared-key cisco123
Pitesti(config-ipsec)# show run crypto isakmp
isakmp enable outside
isakmp policy 10
   authentication pre-share
   encryption 3des
   hash sha
   group 2
   lifetime 86400
```

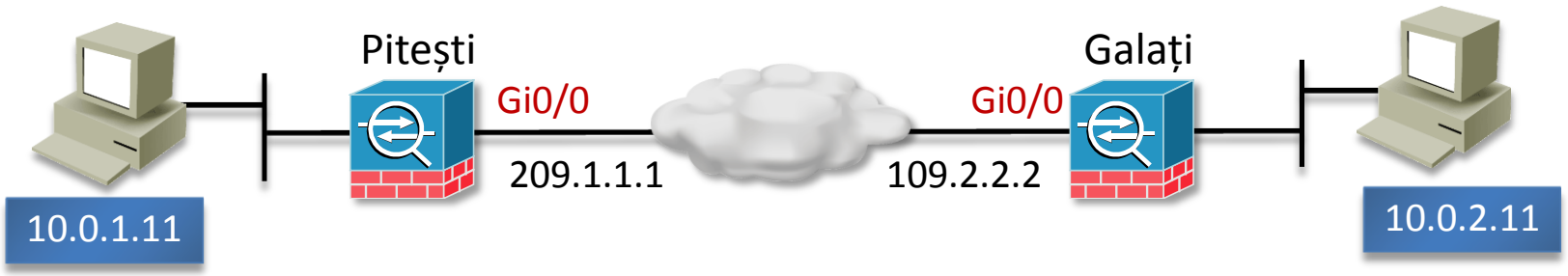

SRED

Pași de configurare parametri IPSec (IKE phase 2)

- Pasul 1: definirea traficului interesant
- Pasul 2: definirea NAT Exemption pentru traficul IPSec
- Pasul 3: configurarea IPSec transform-set
- Pasul 4: configurarea unui crypto-map
- Pasul 5: aplicarea crypto-map

SRED

Definirea traficului interesant și NAT Exemption

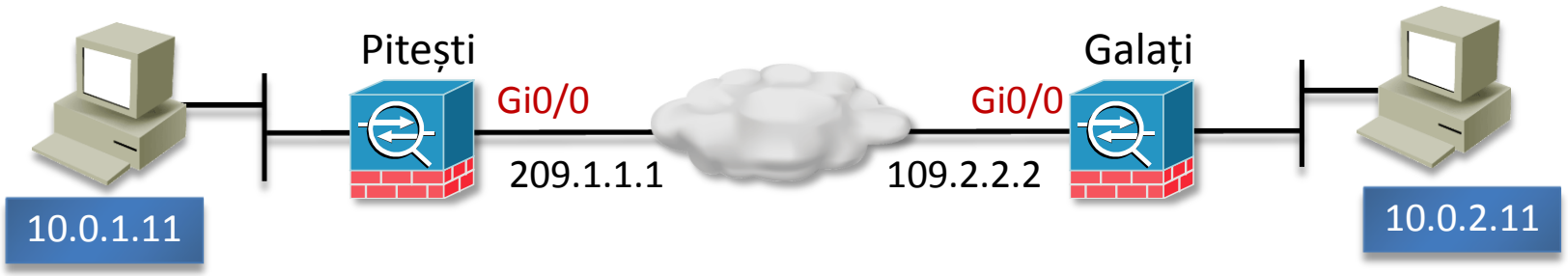


- Cele două liste de acces trebuie să fie simetrice
  - Acțiunea permit = encrypt

```
Pitesti(config)# access-list 101 permit ip 10.0.1.0
  255.255.255.0 10.0.2.0 255.255.255.0
Pitesti(config)# nat 0 (inside) 101
Galati(config)# access-list 101 permit ip 10.0.2.0
  255.255.255.0 10.0.1.0 255.255.255.0
Galati(config)# nat 0 (inside) 101
```


SRED

Configurarea unui transform-set

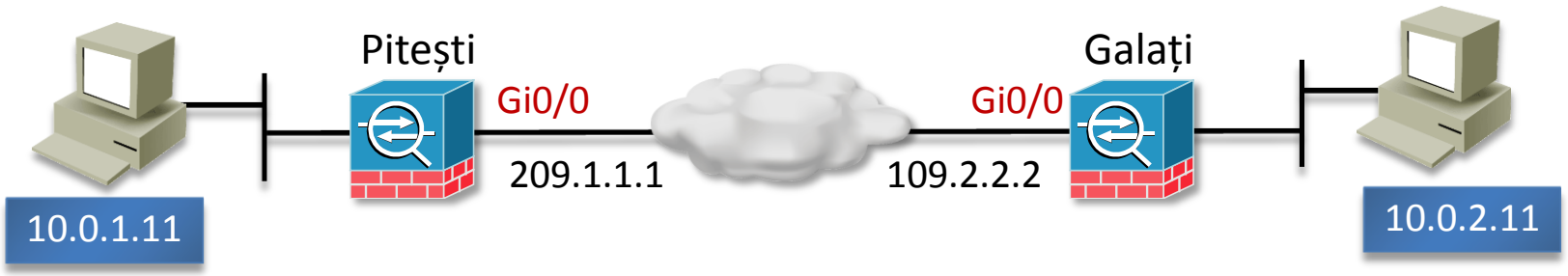


- Doar ESP este suportat pe ASA în acest moment
- Se pot defini maxim 2 intrări în fiecare set
- Modul implicit este *tunnel*

```
Pitesti(config)# crypto ipsec transform-set Galati esp-des esp-
  md5-hmac
```


SRED

Configurarea și aplicarea unui crypto-map



- Structura de date care reunește toate configurațiile IPSec

```
Pitesti(config)# crypto map Pitesti 10 match address 101
Pitesti(config)# crypto map Pitesti 10 set peer 109.2.2.2
Pitesti(config)# crypto map Pitesti 10 set transform-set Galati
Pitesti(config)# crypto map Pitesti 10 set security-association
  lifetime seconds 28800
```

- Aplicarea unui crypto-map

```
Pitesti(config)# crypto map Pitesti interface outside
```


SRED

Testarea și verificarea configurației VPN

- Verificarea ACL-urilor
  - `show run access-list`
- Verificarea configurației corecte de ISAKMP
  - `show run isakmp`
  - `show run tunnel-group`
- Verificarea configurației corecte IPSec
  - `show run ipsec`
- Verificarea IPSec și ISAKMP SA
  - `show crypto ipsec sa`
  - `show crypto isakmp sa`

Testarea și verificarea configurației VPN

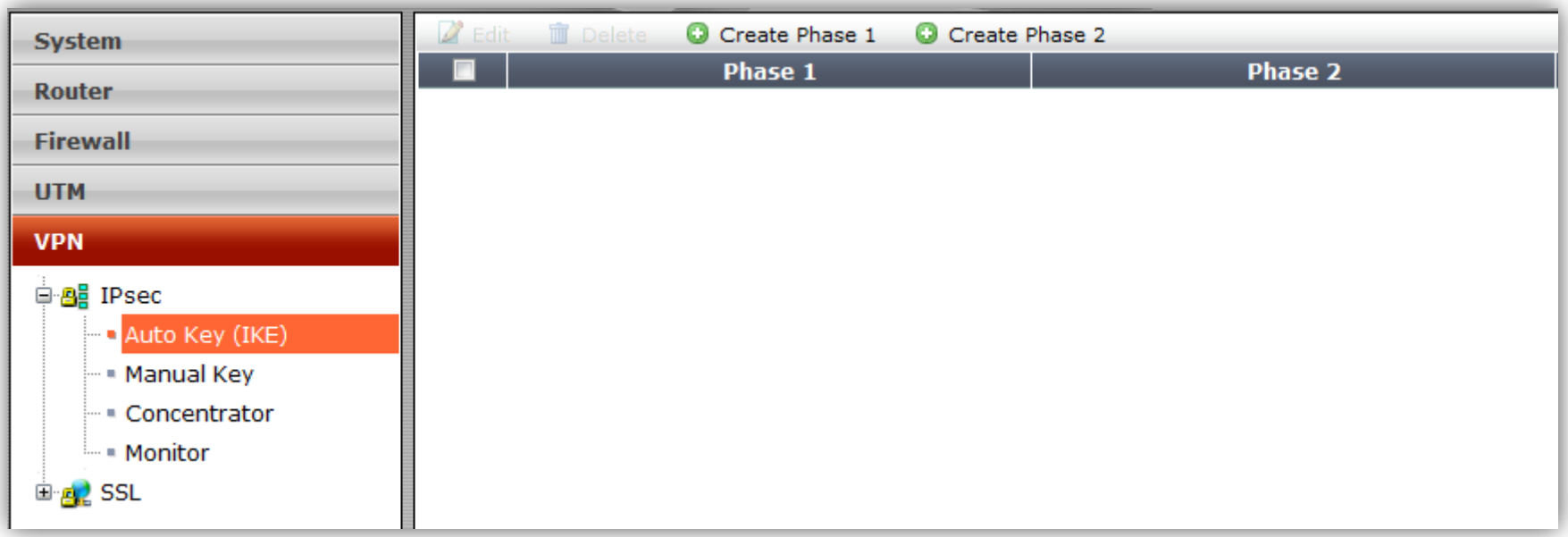
- Verificarea configurației crypto-map
  - `show run crypto-map`
- Ștergerea SA-urilor IPSec
  - `clear crypto ipsec sa`
- Ștergerea SA-urilor ISAKMP
  - `clear crypto isakmp sa`
- Debug pentru IPSec și ISAKMP
  - `debug crypto ipsec`
  - `debug crypto isakmp`

Fortinet
Implementarea IPSec Site-to-Site VPN

Tipuri de configurație IPSec

- În FortiOS, IPSec se poate configura în două moduri de operare
  - Policy-based – se implementează prin definirea unei politici cu acțiunea **IPSEC** între două interfețe și asocierea acesteia cu un tunel VPN
  - Route-based – la crearea tunelului VPN se creează o interfață virtuală pentru acest tunel; definirea politicii se face între interfața fizice și cea virtuală cu acțiunea **ACCEPT**
- Se recomandă utilizarea Route-based cât de des posibil din cauza flexibilității pe care o oferă
- Policy-based nu suportă GRE-over-IPSec sau L2TP cu IPSec
- Când folosim Policy-based?
  - Dacă UTM-ul este configurat în modul transparent, nu se poate folosi decât policy-based

Configurare IPSec

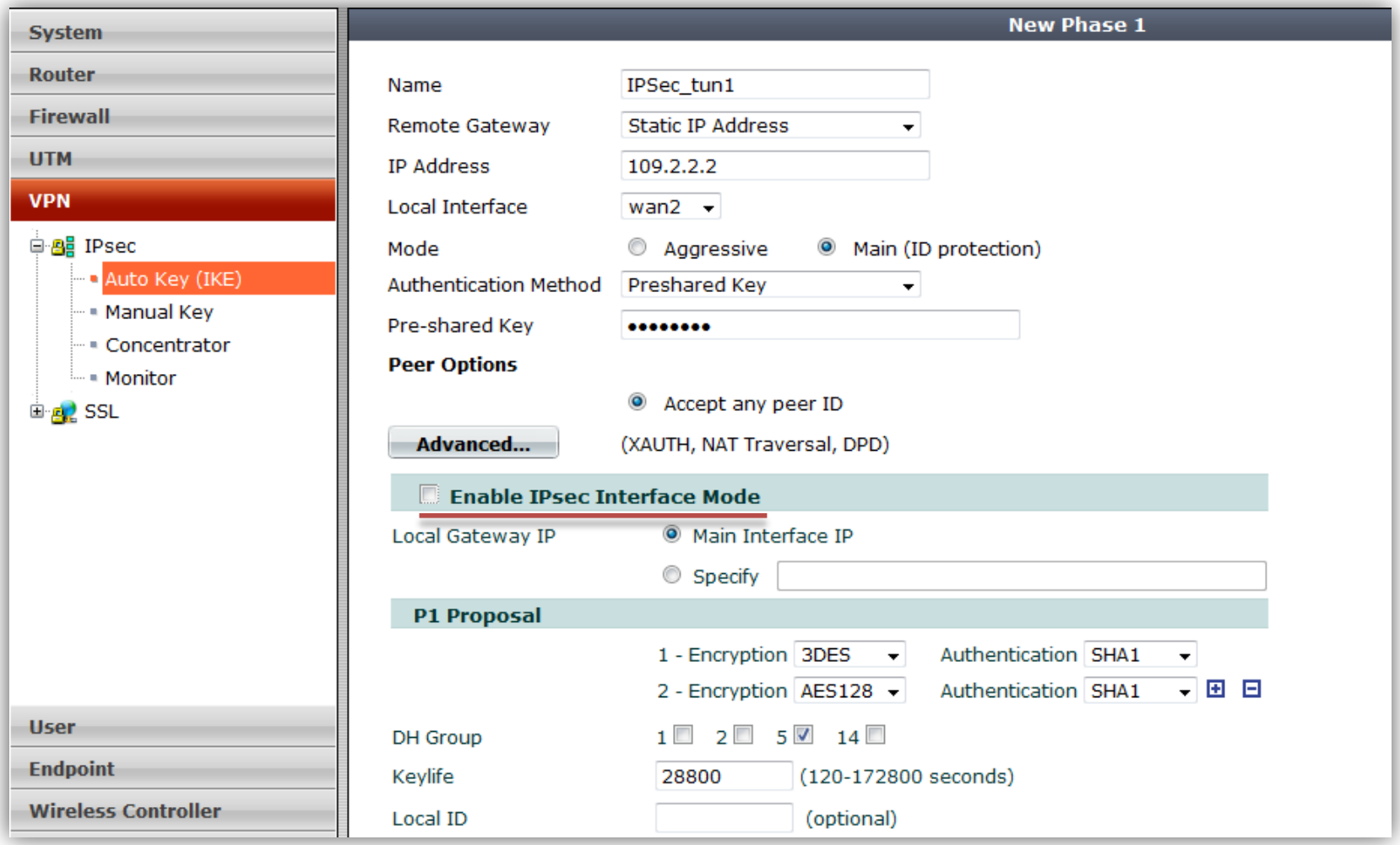


- Pași de configurare IPSec:
  - Definirea Phase 1
  - Definirea Phase 2
  - Definirea unei politici de firewall pentru direcționarea prin tunel (diferită funcție de tipul configurației tunelului – route-based/policy-based)

SRED

Definirea phase 1 – Policy-based

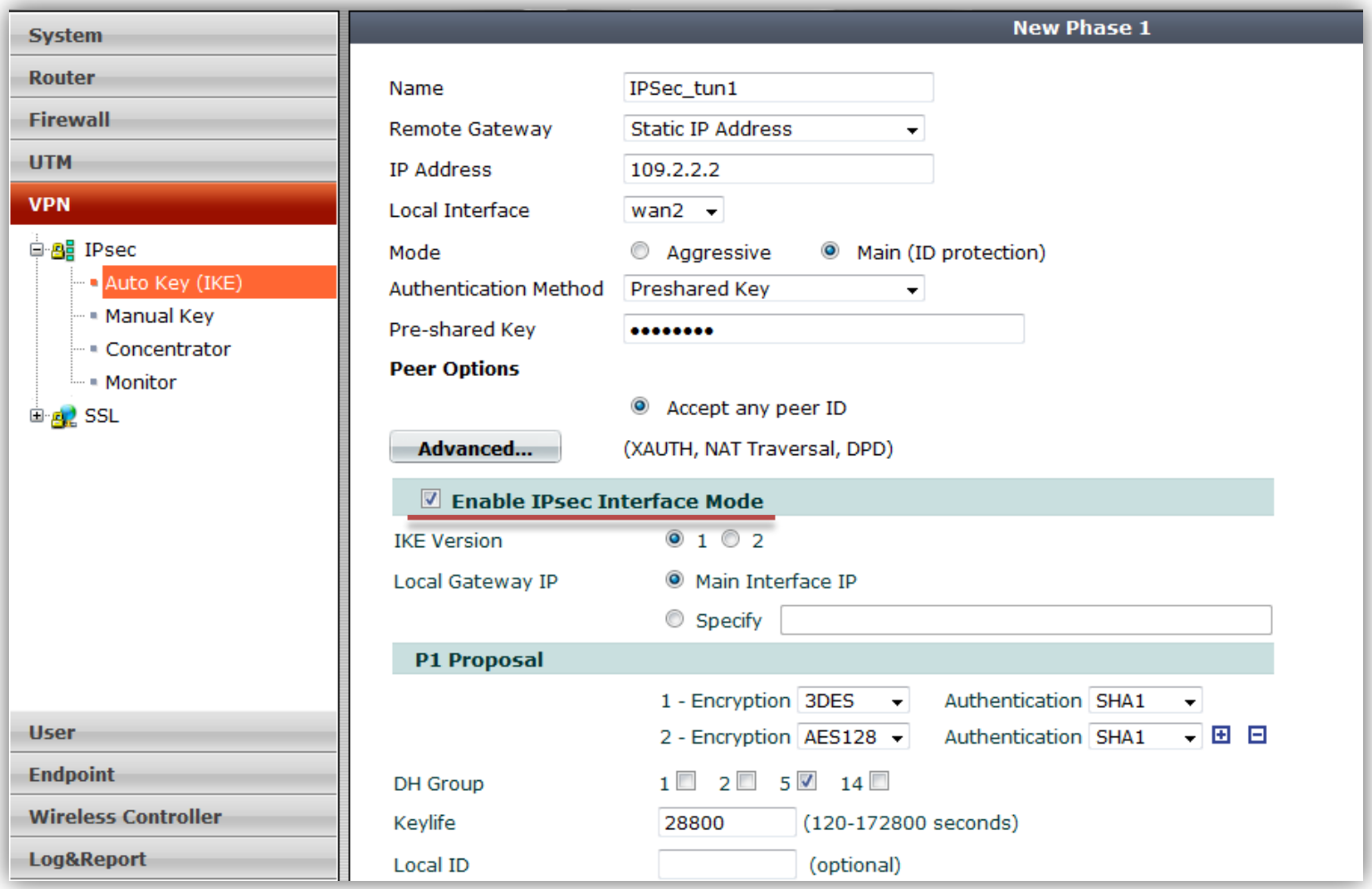
- În phase 1 se alege modul route-based sau policy-based



SRED

Definirea phase 1 – Route-based mode

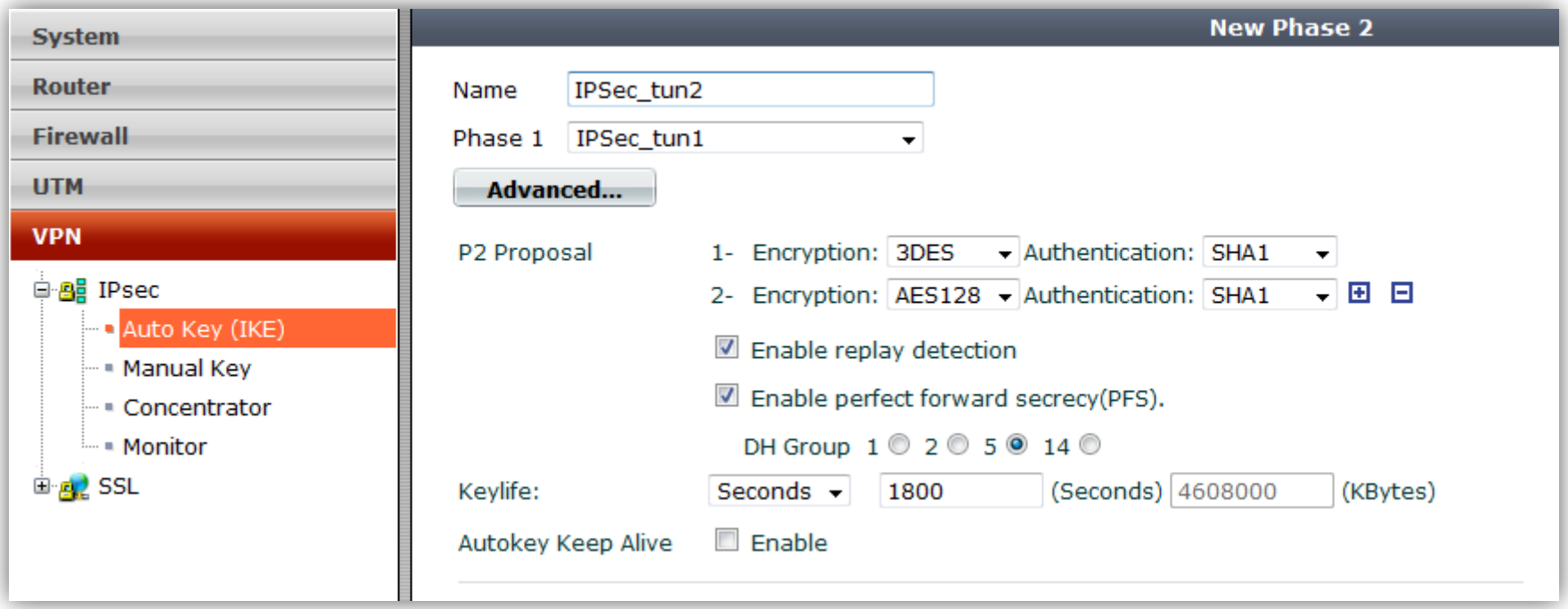
- Route-based permite alegerea IKE v2



SRED

Definirea phase 2

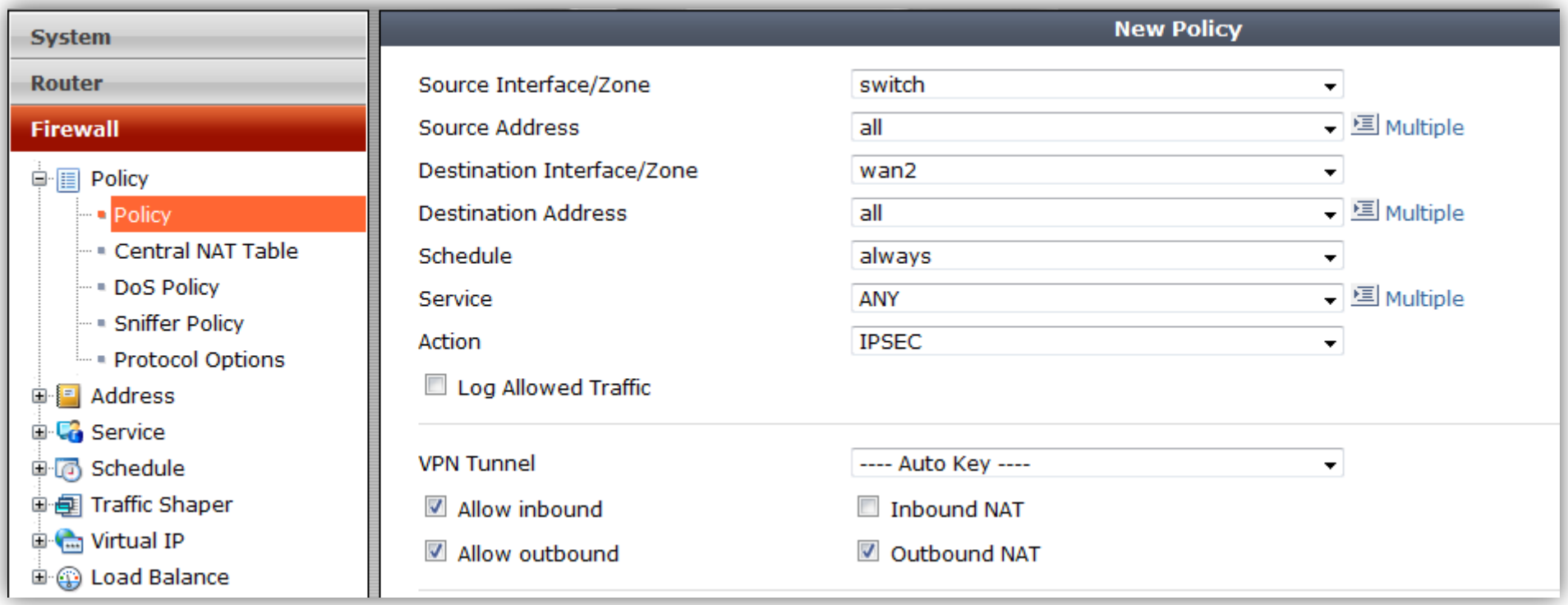
- Necesită:
  - Nume
  - Asocierea cu un obiect phase 1
  - Definirea transform-setului



SRED

Definirea unei politici policy-based

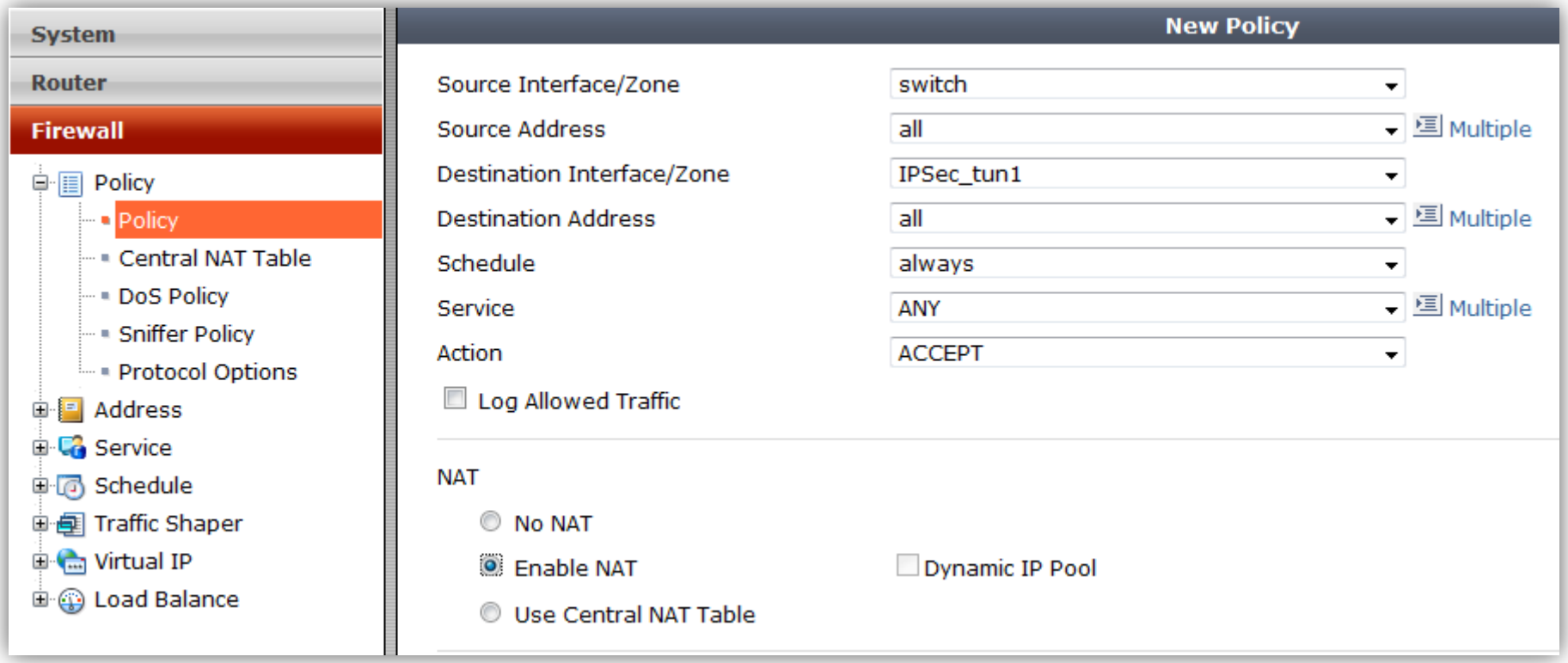
- Acțiunea trebuie să fie **IPSec**
- Odată cu politica de firewall pot fi definite și politicile de NAT pentru tunel
  - Inbound NAT activează Outside NAT pentru pachetele ce vin criptate prin tunel
  - Outbound NAT activează Inside NAT pentru pachetele clear text ce intră în tunel



SRED

Definirea unei politici route-based

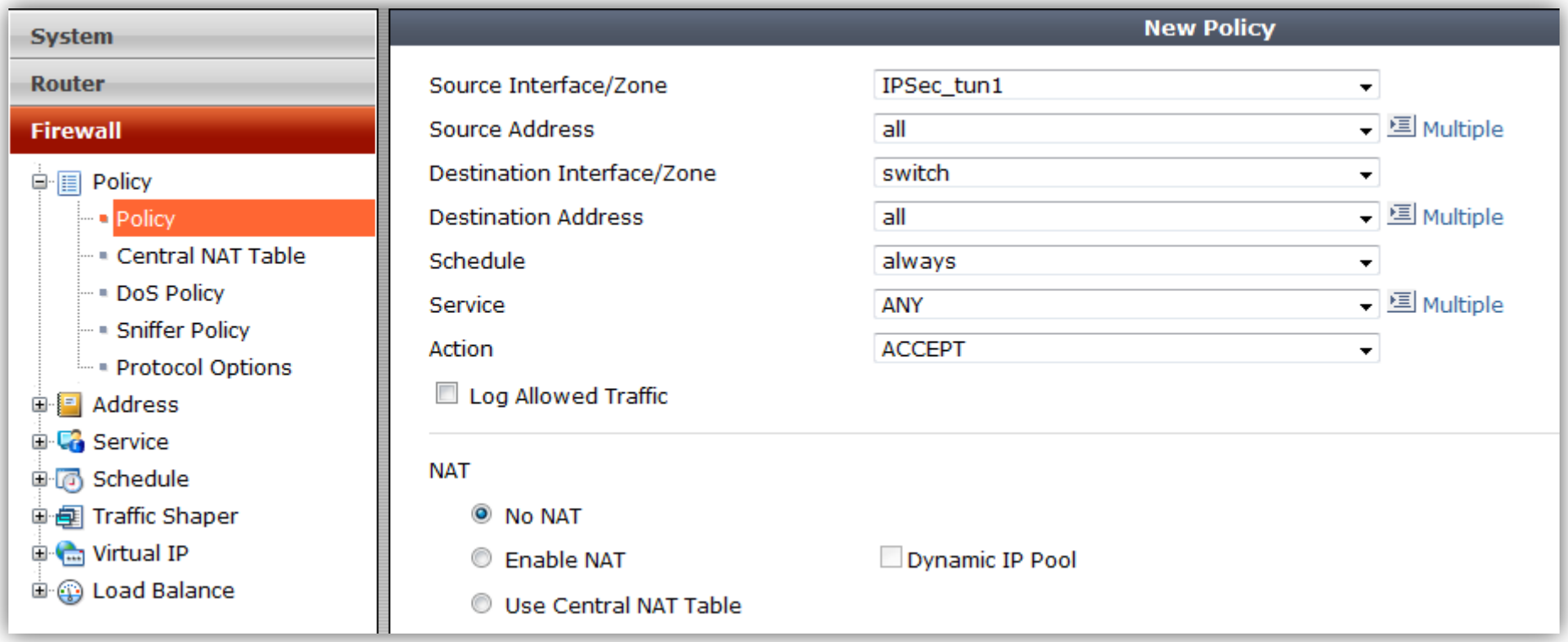
- În route-based se creează o interfață virtuală cu numele dat IKE Phase 1
- Pentru a permite traficul inițiat din LAN prin tunel trebuie creată o politică ACCEPT între interfața internă și interfața virtuală



SRED

Definirea unei politici route-mode bidirecționale

- În route-mode trebuie definite 2 politici ACCEPT astfel încât tunelul să poată fi inițiat din orice direcție

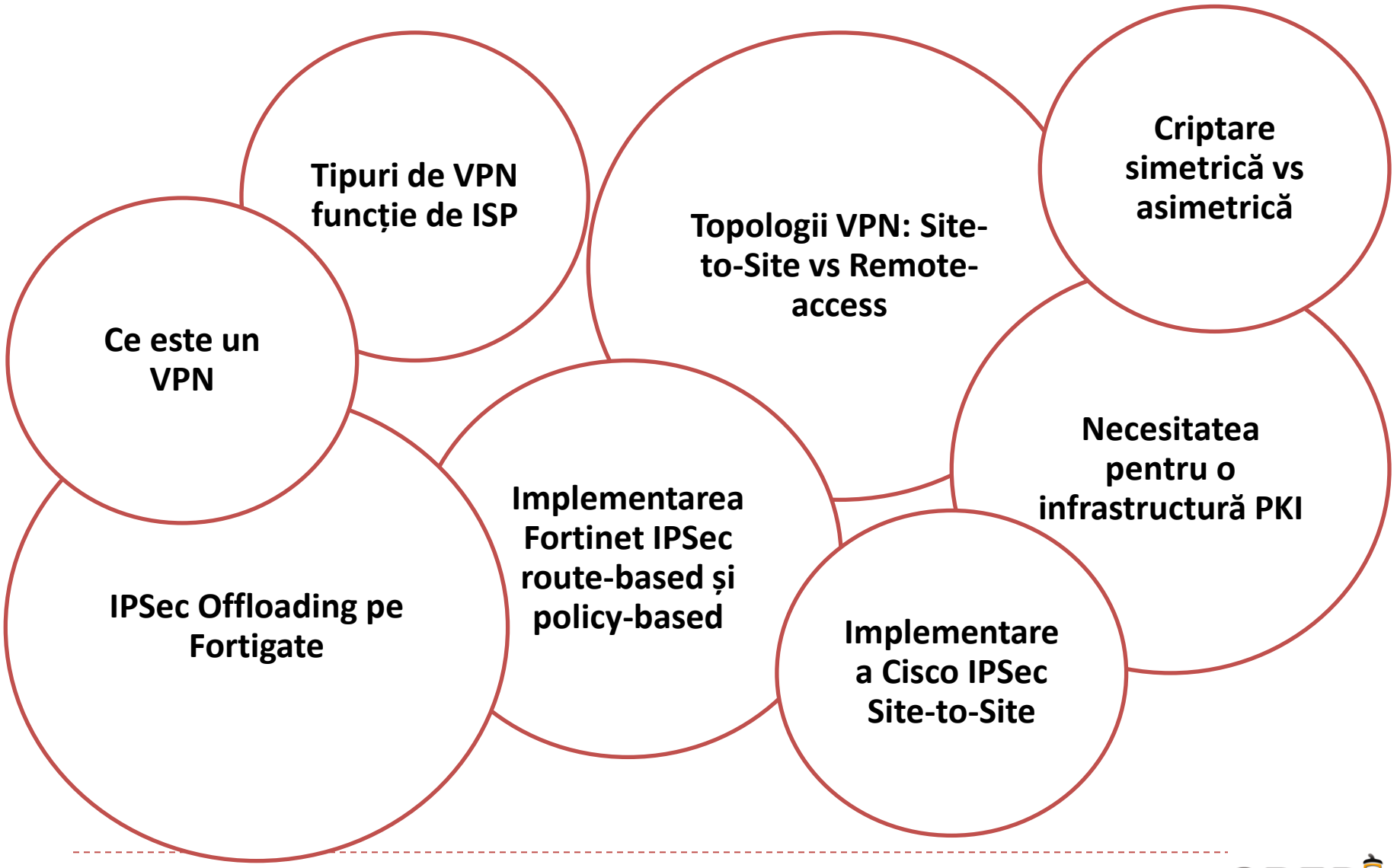


SRED

Offload și accelerare IPSec

- Unele FortiGate-uri au procesor specializat pentru criptarea IPSec: FortiASIC NP2
- Astfel se face offloading de pe procesorul principal
- Există anumite cerințe de trafic pentru utilizarea sa
  - Pachetele trebuie să fie IPv4
  - Nivelul 4 trebuie să fie TCP, UDP, ICMP
  - Politica de firewall nu trebuie să conțină IPS sau antivirus
  - Interfața de ieșire și de intrare trebuie să fie pe același network processor
  - Pachetele incoming nu trebuie să fie fragmentate
  - MTU-ul pentru pachetele outgoing trebuie să fie minim 385 bytes

Overview



SRED

Cursul viitor…

- Teleworking
  - Remote-access VPN
  - Topologii de remote-access
  - Internet-browsing prin SSL

- Intrusion Prevention Systems
  - Strategii IPS
  - Semnături IPS
  - Implementări IPS

SRED