



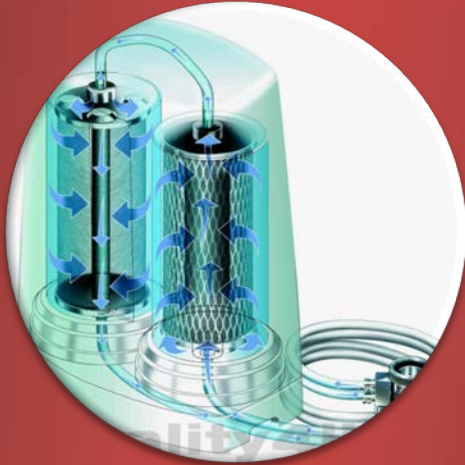
Basic firewalling

12 Martie 2015

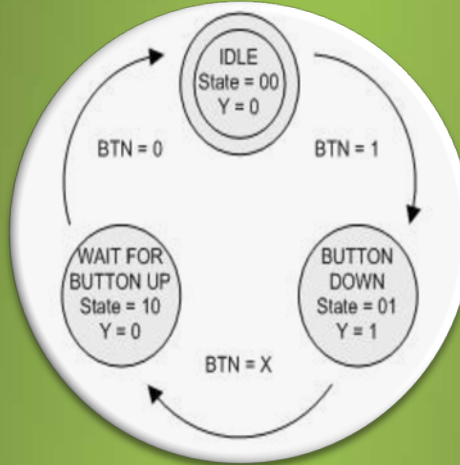
Obiective

- ▶ Tipuri de firewall-uri
- ▶ Funcționalități avansate ale unui firewall
- ▶ Cisco ASA
 - ❑ Tratarea conexiunilor
 - ❑ ACL-uri
 - ❑ Metode de troubleshooting
- ▶ Fortinet FortiGate
 - ❑ Tratarea conexiunilor
 - ❑ Politici de firewall
 - ❑ Autentificarea prin politică de firewall (cut-through proxy)
 - ❑ Politici DoS
 - ❑ Explicit WEB proxy

Tipuri de firewall-uri



Packet filtering
firewall
(stateless)



Stateful
firewall

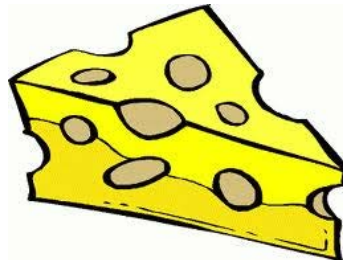


Proxy firewall

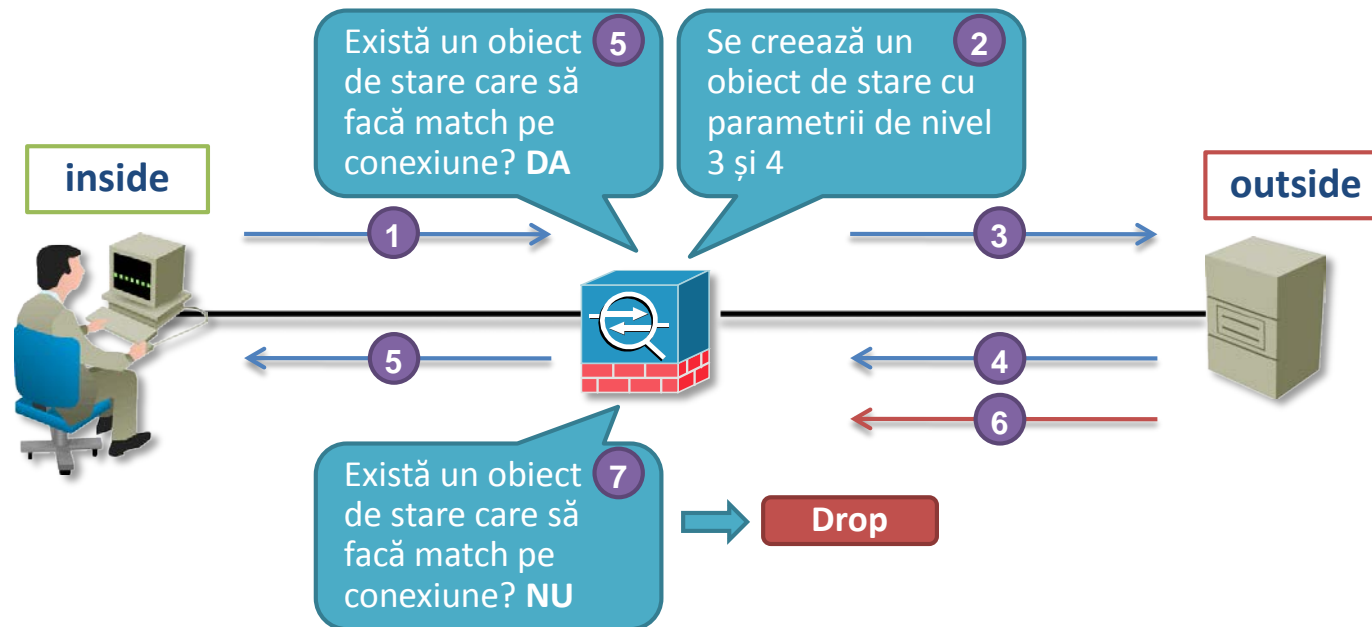


Packet-filtering firewall

- ▶ Nu menține nici o stare internă despre conexiunile realizate
- ▶ Funcționează pe baza unor reguli statice
- ▶ Identificarea traficului blocat sau permis se face de obicei cu ACL-uri
- ▶ ACL-urile pot identifica adrese L2/L3/L4 și câmpuri specifice din antetele de la aceste niveluri (SYN, numărul de protocol 89, 0x806)
- ▶ Din păcate regulile sunt statice
 - ❑ Adăugarea de ACL-uri va crea găuri permanente în firewall
 - ❑ În curând...

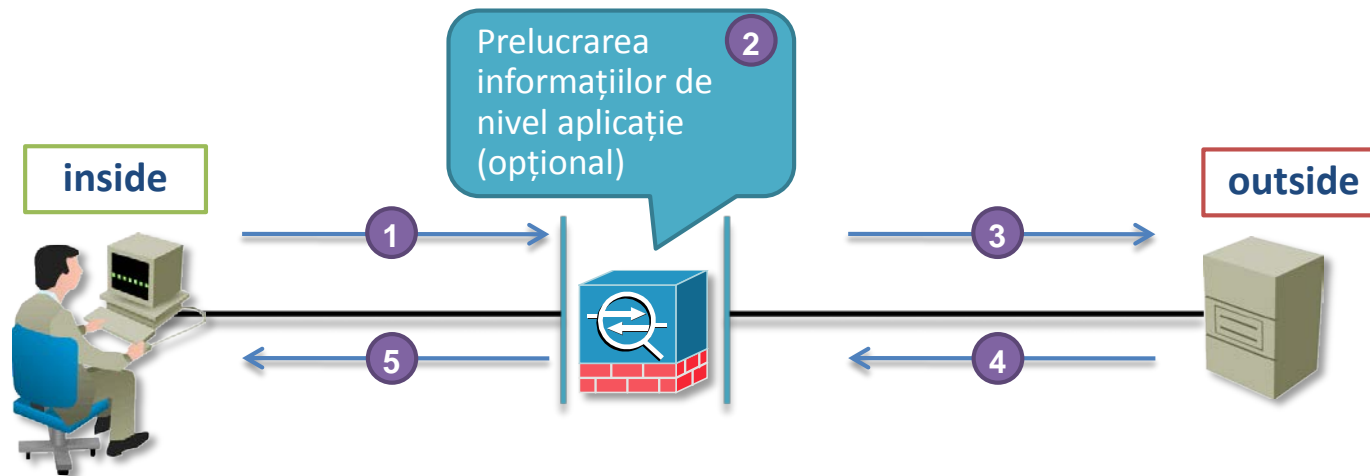


Stateful firewall



- ▶ Modul în care zona inside și outside sunt marcate depinde de vendor
 - ❑ Cisco – nivele de securitate
 - ❑ Fortinet – politici de firewall
- ▶ Pentru protocoale neorientate conexiune (UDP, ICMP etc) firewall-ul păstrează variabile interne alături de informațiile de nivel 3 și 4 pentru a determina validitatea unui pachet ce se întoarce în zona “inside”

Proxy firewall



- ▶ Față de modelul stateful, într-un proxy firewall, stația din zona “inside” nu contactează niciodată direct serverul din “outside”
- ▶ Stația realizează o conexiuni direct către firewall
 - ❑ Adresa firewall-ului este configurată ca proxy în browser/aplicație
- ▶ Firewall-ul realizează conexiunea către server folosind propria adresă sursă
- ▶ Firewall-ul poate opțional să analizeze pachetele la nivel superior sau să logheze anumite informații
- ▶ Proxy nu este NAT!

Firewall – moduri de funcționare

- ▶ Majoritatea firewall-urilor dedicate de rețea
 - ❑ sunt implicit stateful
 - ❑ Pot funcționa în 2 moduri diferite
 - NAT/Routed mode - firewall-ul este un hop de nivel 3 și realizează rutare
 - Transparent mode – firewall-ul este invizibil din punct de vedere al nivelului 3 și face switching funcție de tabela CAM pentru a trimite pachetele
- ▶ Modul transparent de obicei limitează funcționalitățile firewall-ului din cauza pierderii capacității de nivel 3
 - ❑ Ex: Cisco ASA, în transparent mode, nu suportă:
 - NAT
 - Protocoale de rutare
 - IPv6
 - VPN-uri folosite pentru transfer de date (doar VPN-urile pentru management sunt permise)



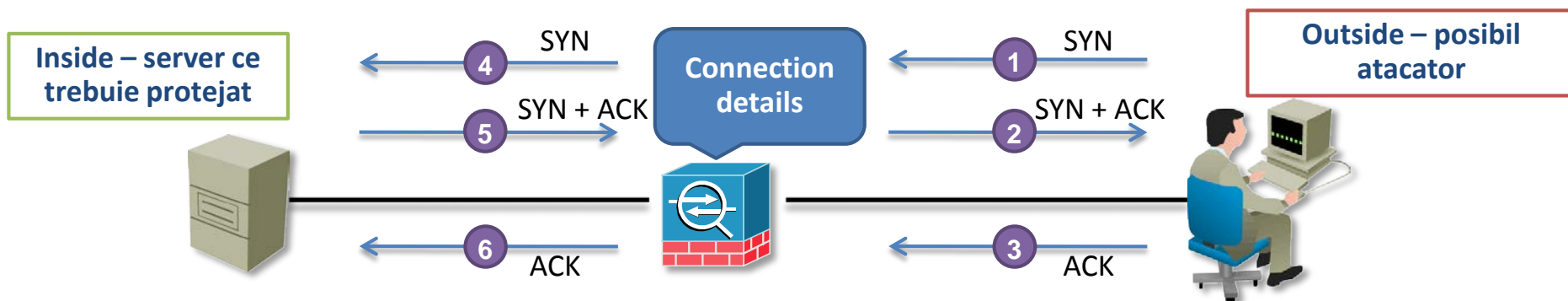
Funcționalități avansate ale unui firewall

Limitarea conexiunilor

- ▶ În general se limitează:
 - ❑ Embryonic connections – numărul de conexiuni care nu au completat 3-way handshake (doar pentru TCP)
 - ❑ TCP connections – numărul total de conexiuni TCP
 - ❑ UDP connections – numărul total de conexiuni UDP
- ▶ Dar cu ICMP ce facem?
 1. Îl blocăm
 2. De obicei avem nevoie de el pentru anumite funcționalități (Path MTU discovery, traceroute) → ne protejăm cu tehnici anti-DoS (DoS senzor)
- ▶ Toate limitele de mai sus se pot configura
 - ❑ Per host
 - ❑ Global la nivelul dispozitivului

Dacă limitele sunt depășite?

- ▶ Două soluții
- ▶ TCP Intercept
- ▶ SYN cookies
- ▶ TCP Intercept – modul de funcționare

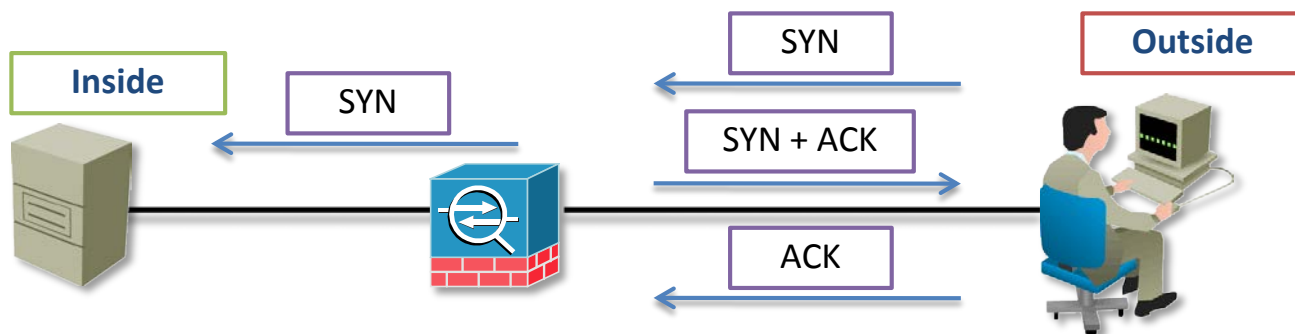


- ▶ Problema cu modelul TCP Intercept?
 - ❑ Firewall-ul trebuie să rețină în memorie parametrii fiecărei conexiuni

SYN Cookies



- ▶ Metoda SYN Cookies nu păstrează nici o informație de stare pe firewall



- ▶ O cerere de conectare este transmisă către firewall
- ▶ Firewall-ul calculează un hash din informațiile de L3/L4 și câmpuri TCP (ISN etc) primite în pachetul SYN
- ▶ Firewall-ul ia hash-ul și îl pune în câmpul de ISN al său din pachetul de SYN+ACK pe care îl trimite clientului
- ▶ Când firewall-ul primește ACK-ul, recalculează hash-ul din informațiile de L3/L4 știind că în 3-way handshake $ACKnr = SN+1$ și îl compară cu hash-ul din câmpul de ACKnr
- ▶ Dacă hash-urile se potrivesc, conexiune este trimisă proxy către server
- ▶ De ce nu se aplică algoritmul SYN Cookies de la primul pachet?

Alte funcționalități avansate



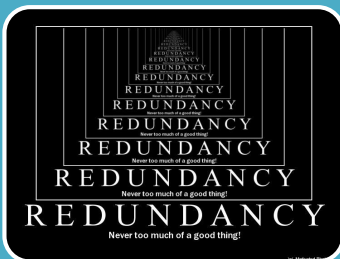
Inspecție la nivel aplicație

- Necesară pentru protocoalele ce deschid porturi dinamice prin firewall (utorrent, Active FTP)
- CPU intensive



Virtual Firewall

- Posibilitatea de a crea mai multe instanțe virtuale ale aceluiași firewall
- Oferă practic mai multe firewall-uri într-un singur device fizic



Redundanță

- Oferă posibilitatea de fallback a conexiunilor și traficului dacă unul din 2 firewall-uri cedează
- Configurațiile se mențin sincronizate



Cisco ASA – funcționalități de firewall

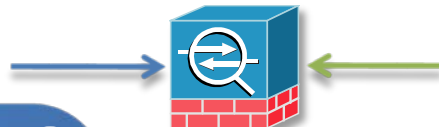
Cisco ASA – TCP flow

Pachetul este primit pe interfața inside 1

- se aplică ACL-uri în direcția inbound
- dacă NAT este configurat, se realizează inside NAT

- ASA randomizează numărul inițial de secvență al conexiunii 2

- se creează un obiect de stare în memorie cu informații de nivel 3 și 4 folosite pentru a identifica sesiunea
- conexiunea este marcată ca *embryonic*



Pachetul se întoarce pe interfața outside 3

- se aplică ACL-urile în direcția inbound → dacă pachetul este permis de un ACL, tabela de stări nu mai este verificată
- se verifică tabela de stare pentru informațiile din pachetul primit
- dacă nu se găsește un obiect de stare matching pachetul este aruncat

- ASA verifică numărul ACK din pachet funcție de SN-ul suprascris de dispozitiv la pasul anterior 4

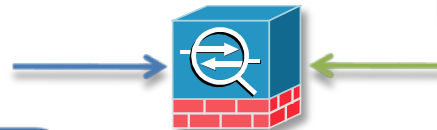
- Dacă pachetul e legitim, acesta e transmis către stația internă cu un număr de ACK care să reflecte ISN-ul inițial +1

- Stația internă răspunde cu ACK 5

- Numărul de ACK nu este randomizat
- Conexiunea este trecută în starea *active-established* și *counter-ul* de conexiuni în starea *embryonic* este resetat

Cisco ASA – UDP flow

- ▶ UDP nu este orientat conexiune și deci mult mai ușor de spoofat



Pachetul este primit pe interfața inside 1

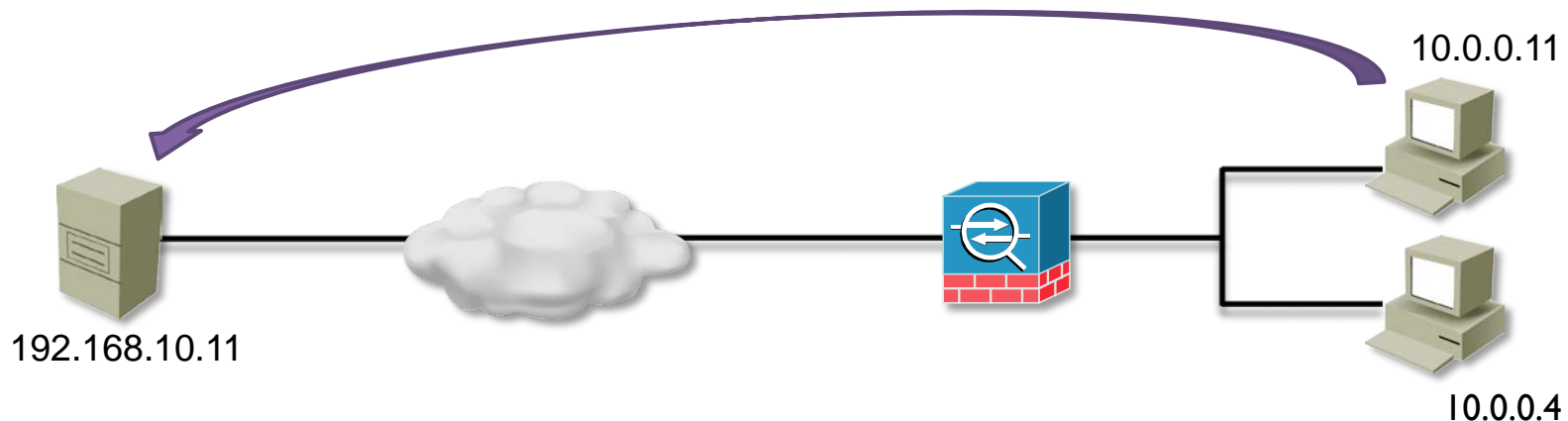
- se aplică ACL-uri în direcția inbound
- dacă NAT este configurat, se realizează inside NAT

- se creează un obiect de stare în memorie cu informații de nivel 3 și 4 folosite pentru a identifica sesiunea 2
- se trimite pachetul pe interfața “outside”
- se pornește un timeout de 2 minute pentru așteptarea pachetului de întoarcere

Pachetul se întoarce pe interfața outside 3

- se aplică ACL-urile în direcția inbound → dacă pachetul este permis de un ACL, tabela de stări nu mai este verificată
- se verifică tabela de stare pentru informațiile din pachetul primit
- dacă nu se găsește un obiect de stare matching pachetul este aruncat

Verificarea stării conexiunilor



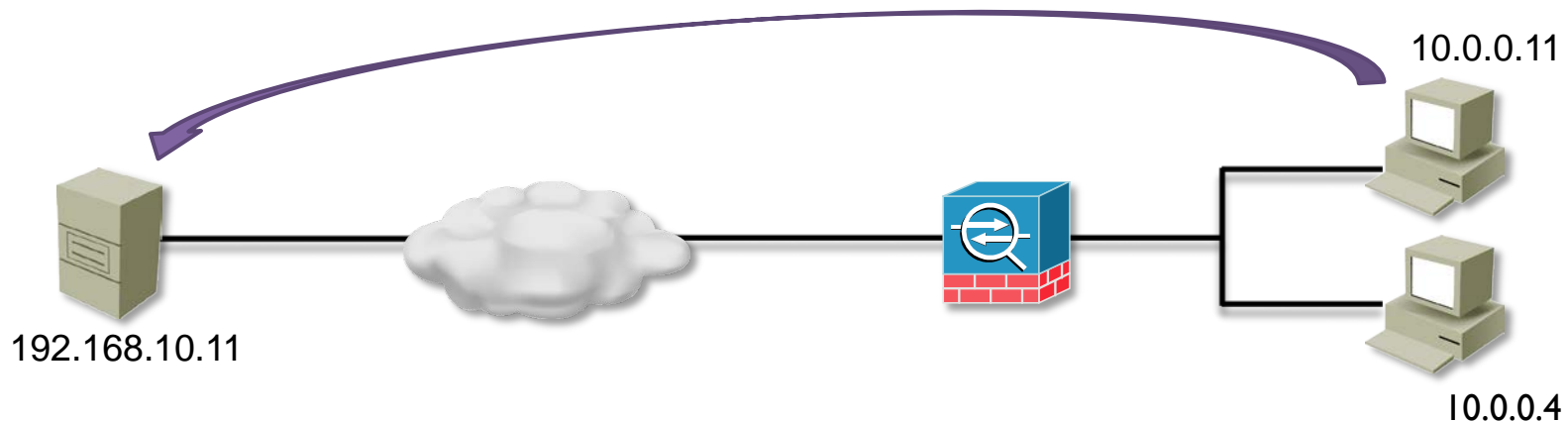
```
asal# show conn
```

```
2 in use, 9 most used
```

```
TCP out 192.168.10.11:80 in 10.0.0.11:2824 idle 0:00:03 bytes  
2320 flags UIO
```

```
TCP out 192.168.10.11:80 in 10.0.0.11:2823 idle 0:00:03 bytes  
3236 flags UIO
```


Verificarea stării conexiunilor



```
asa1# show local-host
Interface dmz: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 5 maximum active, 0 denied
local host: < 10.0.0.11 >,
  TCP flow count/limit = 2/300
  TCP embryonic count to host = 0
  TCP intercept watermark = 25
  UDP flow count/limit = 0/unlimited
Conn:
  TCP out 192.168.10.11 :80 in 10.0.0.11 :2824 idle 0:00:05 bytes 466 flags UIO
  TCP out 192.168.10.11 :80 in 10.0.0.11 :2823 idle 0:00:05 bytes 1402 flags UIO
```

Inspecția de protocoale



- ▶ ASA inspectează în mod implicit un set limitat de protocoale
- ▶ Class-map-ul identifică protocoalele
- ▶ Policy-map-ul identifică acțiunea (în mod implicit *inspect*)
- ▶ Dacă se dorește permiterea oricărui alt protocol prin dispozitiv trebuie editată politica implicită
- ▶ Mai multe la laborator...

```
ASA1# sh run
--- output omis ---
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
--- output omis ---
```

Liste de acces

▶ ASA suportă 5 tipuri de ACL-uri

❑ Standard

- Nu pot filtra pachete!
- Se folosesc în scenarii de split-tunneling și redistribuire de rute

❑ Extinse

- Clasificare L3/L4

❑ EtherType

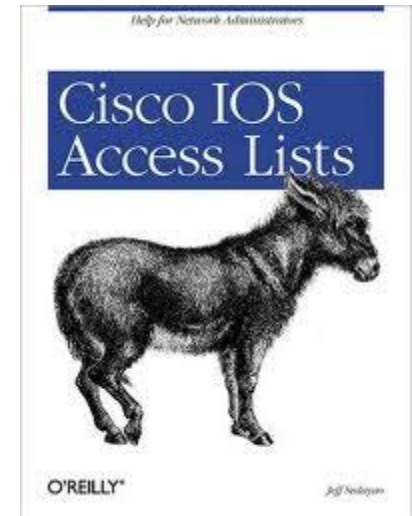
- Folosite pentru filtrarea de trafic non-IP

❑ WebVPN

- Folosite pentru a restricționa traficul ce vine printr-un WebVPN

❑ IPv6 ACLs

- Take a guess...



The power of an ACL!

- ▶ Ce se întâmplă dacă dorim să permitem unei stații din exterior să inițieze o conexiune către o stație din interior?
- ▶ Nu putem modifica nivelul de securitate al interfețelor căci stricăm modelul stateful



- ▶ Soluție: se poate configura un ACL extins pe interfața outside care să permită anumite conexiuni din exterior
 - ▶ Dacă se face match pe o intrare din acest ACL, nu se mai analizează tabela de obiecte de stare

Liste de acces extinse

- ▶ Exercițiu: creați un ACL extins în Cisco IOS care să blocheze doar trafic tcp www de la rețeaua sursă 192.168.1.0/24 către orice destinație.

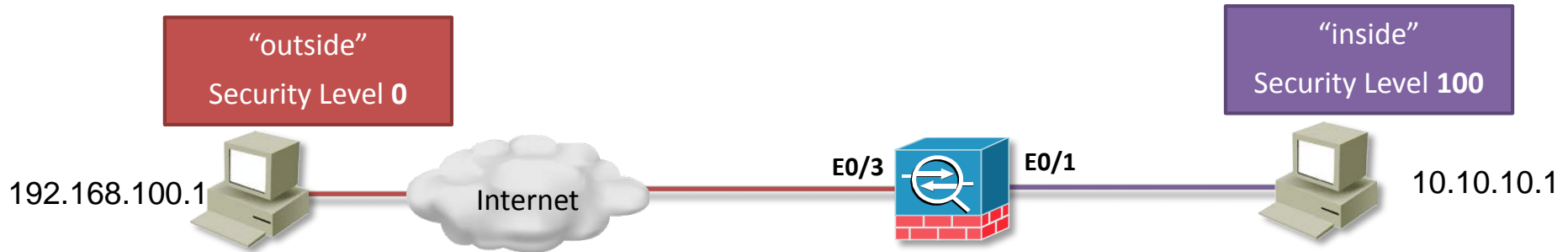
```
R1(config)#access-list 101 deny tcp 192.168.1.0 0.0.0.255 any eq 80
R1(config)#access-list 101 permit ip any any
```

- ▶ Să transpunem acest ACL în ASA OS:

```
asa1(config)#access-list test1 line 1 extended deny tcp 192.168.1.0
255.255.255.0 any eq 80
asa1(config)# access-list test1 line 10 extended permit ip any any
```

- ▶ Care sunt diferențele?
- ▶ Cursul viitor (ACL&NAT) va avea mult mai multe detalii

Exemplu



- ▶ Dorim să permitem traficul IP inițiat de la stația din “outside” la stația din “inside”

```
ASA1(config)# access-list permit_outside line 10 extended permit ip host
192.168.100.1 host 10.10.10.1
ASA1(config)# access-group permit_outside in interface outside
ASA1(config)# sh access-1
access-list permit_outside; 1 elements
access-list permit_outside line 1 extended permit ip host 192.168.100.1
host 10.10.10.1 (hitcnt=0) 0x8c400363
```

- ▶ Dacă am avea și NAT ar trebui să facem și port-forwarding sau static-nat

Permiterea ICMP către ASA

- ▶ Traficul ICMP către ASA nu este controlat de nivelele de securitate sau clasele de protocoale inspectate...
- ▶ ... ci de comanda “icmp”
- ▶ În mod implicit ASA acceptă mesaje ICMP pe toate interfețele
- ▶ Exemplu: filtrarea mesajelor ICMP de la stația 10.10.10.1 din rețeaua “inside”



```
ASA1(config)# icmp deny 10.10.10.1 255.255.255.255 inside
```

Metode de troubleshooting

- ▶ Cisco ASA are mecanisme de troubleshooting extrem de utile
 - ❑ Logging
 - În memorie sau către dispozitive externe
 - ❑ Capturi de pachete
 - În memorie sau către dispozitive externe
 - Suport real-time
 - Trafic IP sau după codul EtherType
 - Filtrarea traficului capturat prin specificarea unui ACL
 - ❑ Packet-tracer (nu cel de la SCR 😊)
 - Poate simula un flow tcp/udp/icmp de la o sursă la o destinație și arata fiecare proces intern ASA și decizia sa
 - Poate ajuta administratorul să descopere motivul pentru care traficul său este negat de ASA
 - Motive posibile: inspecția nu a fost activată pentru protocolul respectiv, nu există rută, trafic blocat de un ACL etc.

Comanda capture

```
ciscoasa(config)# ciscoasa(config)#access-list inside_test permit ip
host 192.168.1.50 any
ciscoasa(config)#capture inside_interface access-list inside_test
interface inside
```

```
ciscoasa(config)#show capture inside_interface
1: 15:59:42.749152 192.168.1.50.1107 > 172.22.1.1.80:
S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK>
2: 15:59:45.659145 192.168.1.50.1107 > 172.22.1.1.80:
S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK>
3: 15:59:51.668742 192.168.1.50.1107 > 172.22.1.1.80:
S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK>
```

```
ciscoasa(config)#clear capture inside_interface
ciscoasa#show capture inside_interface
0 packet captured
0 packet shown
```

Packet tracer

```
ASA1(config)# packet-tracer input  inside icmp 10.10.10.1 8 0 192.168.1.100
```

```
Phase: 1
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: FLOW-LOOKUP
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
Found no matching flow, creating a new flow
```

```
Result:
```

```
input-interface: inside
```

```
input-status: up
```

```
input-line-status: up
```

```
Action: drop
```

```
Drop-reason: (no-route) No route to host
```



FortiGate – funcționalități de firewall

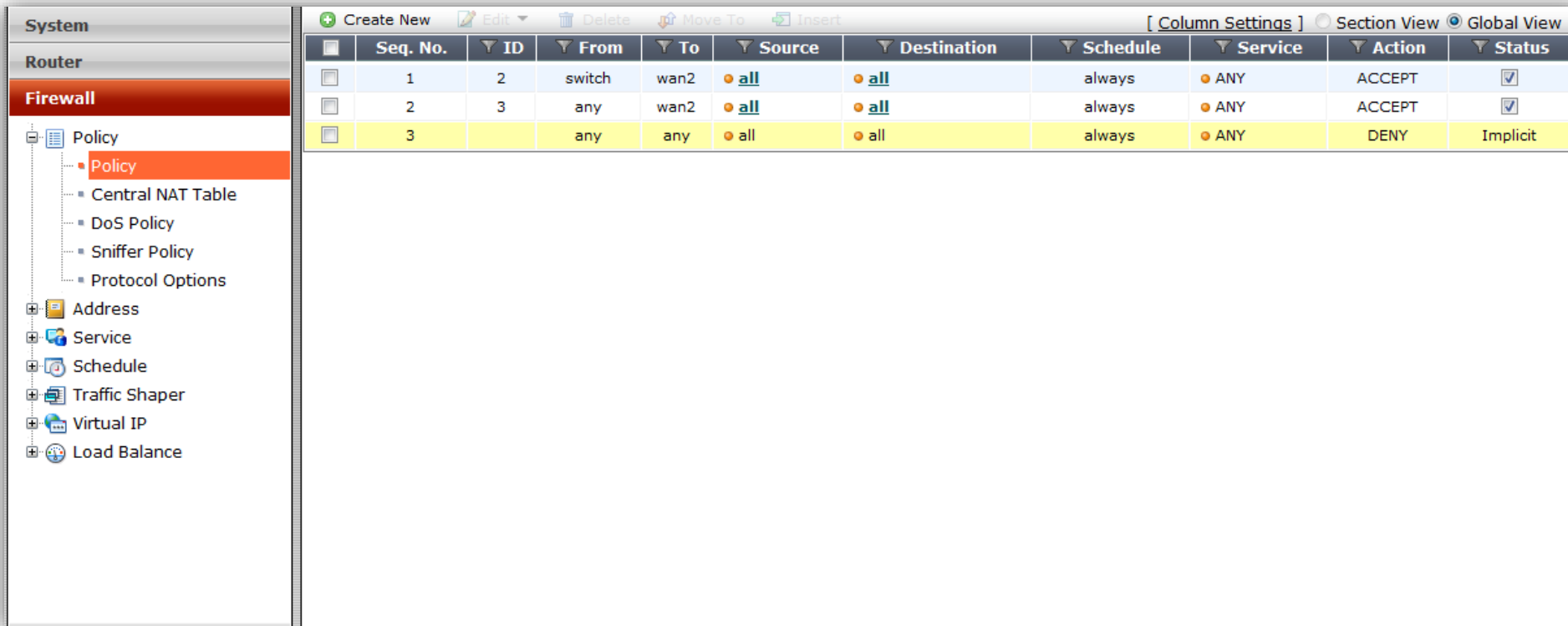
Fortigate – inspecția stateful



- ▶ Mecanismele stateful funcționează la fel ca în cazul ASA
- ▶ În mod implicit FortiGate nu inspectează nimic
 - ❑ Fiecare politică de firewall definește trafic ce va fi inspectat funcție de:
 - Interfață de intrare
 - Interfață de ieșire
 - Adrese L3/L4 sursă
 - Adrese L3/L4 destinație
 - Politici de autentificare
- ▶ Sunt adăugate optimizări de UTM
- ▶ FortiGate aplică următoarele tipuri de inspecție
 - ❑ Stateful
 - ❑ Flow-based
 - ❑ Proxy

Fortigate – tipuri de inspecție: stateful

- ▶ Stateful – prin intermediul unei politici de firewall



The screenshot displays the FortiGate configuration interface for Firewall Policies. The left sidebar shows the navigation tree with 'Firewall' selected. The main area shows a table of three policies. The table has columns for Seq. No., ID, From, To, Source, Destination, Schedule, Service, Action, and Status. The first two policies are 'ACCEPT' and the third is 'DENY'.

Seq. No.	ID	From	To	Source	Destination	Schedule	Service	Action	Status
1	2	switch	wan2	all	all	always	ANY	ACCEPT	<input checked="" type="checkbox"/>
2	3	any	wan2	all	all	always	ANY	ACCEPT	<input checked="" type="checkbox"/>
3		any	any	all	all	always	ANY	DENY	Implicit

Fortigate – tipuri de inspecție: flow-based

- ▶ Pentru funcționalități avansate de firewall și UTM
- ▶ Inspecția mai multor pachete odată funcție de anumite pattern-uri
 - ❑ Se stochează/inspectează un maxim de X pachete cât timp pachetele ce intră în dispozitiv se potrivesc cu patternul predefinit
- ▶ De ce exista nevoia pentru flow based inspection?
 - ❑ Pentru că puțini viruși/troieni sau puține aplicații_dinamice pot fi identificate doar printr-un singur pachet
- ▶ Fortinet definește patternul prin
 - ❑ Session helpers – în cazul application inspection
 - ❑ Antivirus profile – în cazul scanării antivirus
 - ❑ IPS senzor – în cazul detecției atacurilor de rețea

Fortigate – tipuri de inspecție: proxy

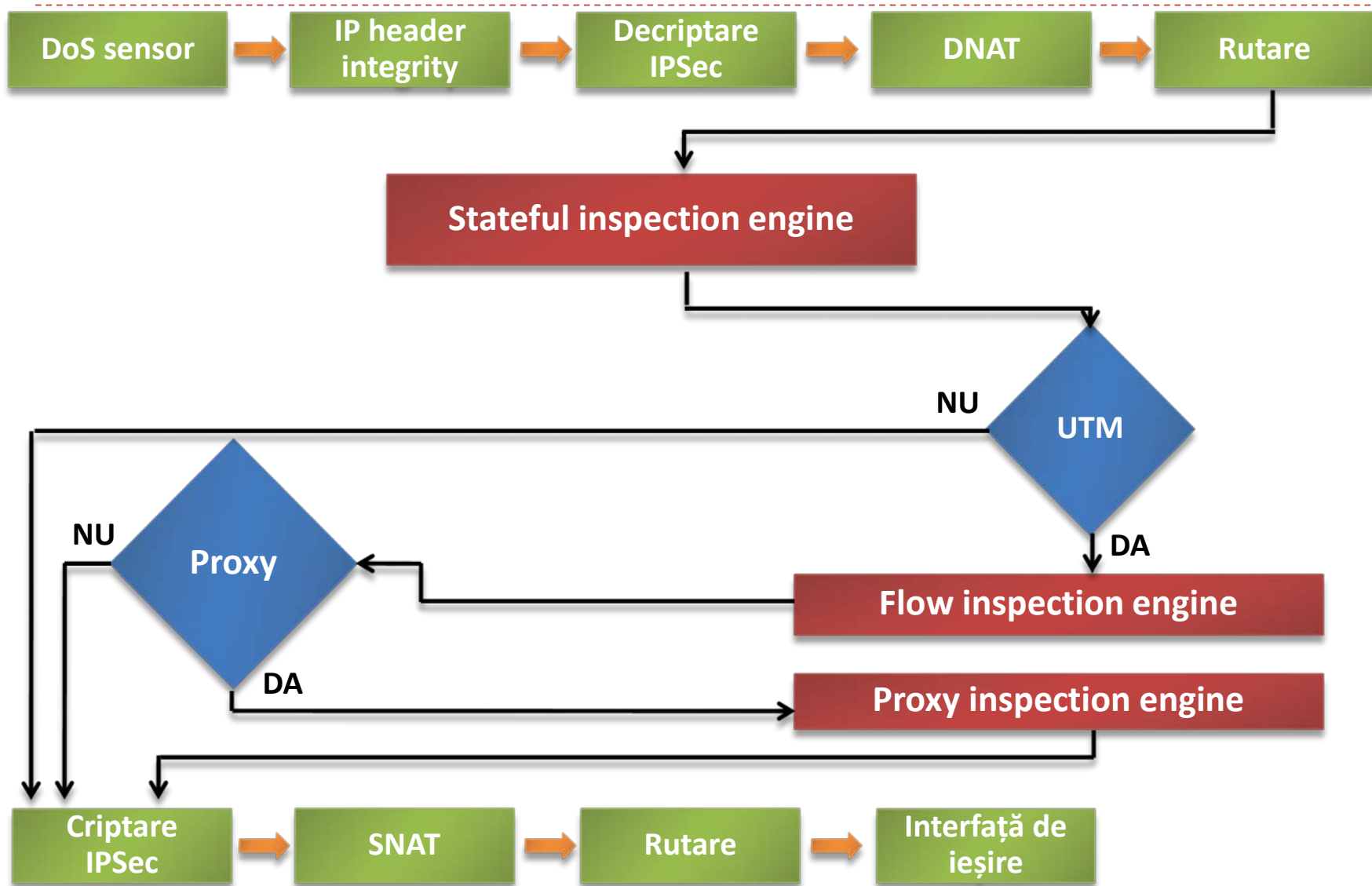
- ▶ UTM-ul stochează întreaga conversație în memorie și reconstruiește informația până la nivel aplicație
 - ❑ Atașamente de e-mail
 - ❑ Conversații de IM
- ▶ După ce informația e reconstruită, este scanată și trimisă spre destinație în cazul în care nu se detectează nimic malițios
- ▶ Tipul de inspecție proxy este cea mai sigură dar are cerințe mari de procesor și memorie

**40 times
stronger than
pure vitamin c**

Când se aplică fiecare tip de inspecție?

Security Function	Stateful	Flow-based	Proxy
Firewall	X		
IPSec VPN	X		
Traffic Shaping	X		
User Authentication	X		
Management traffic	X		
SSL VPN	X		
Intrusion Prevention		X	
Flow-based Antivirus		X	
Application Control		X	
VoIP Inspection		X	
Proxy Antivirus			X
Email filtering			X
WEB Filtering (Antispam)			X
Data Leak Prevention			X

Ordinea de procesare în UTM



Politici de firewall

- ▶ Orice politică de firewall are următoarele componente
 - ❑ Criterii de match
 - ❑ Acțiunea firewall-ului
 - ❑ Funcționalități suplimentare activate de politică
- ▶ Criterii de match:
 - ❑ Interfață sursă/Zonă sursă
 - ❑ Adresă IP sursă
 - ❑ Interfață destinație/Zonă destinație
 - ❑ Adresă IP destinație
 - ❑ Schedule – momentul de timp în care politica e validă
 - ❑ Adrese de nivel 4



Politici de firewall

▶ Acțiuni

- Permit
- Deny
- IPSec

▶ Funcționalități suplimentare atașate politicii

- NAT
- Identity-based policy – autentificarea utilizatorilor care au voie să folosească politica
- UTM (Protocol Options, Antivirus, IPS, Web Filter, Email Filter, DLP Sensor, Application Control, VoIP)
- Traffic-shaping
- Endpoint NAC

See it to believe it

System

Router

Firewall

- Policy
 - Policy
 - Central NAT Table
 - DoS Policy
 - Sniffer Policy
 - Protocol Options
- Address
- Service
- Schedule
- Traffic Shaper
- Virtual IP
- Load Balance

UTM

VPN

User

Endpoint

Wireless Controller

Log&Report

New Policy

Source Interface/Zone: switch

Source Address: all [Multiple](#)

Destination Interface/Zone: wan1

Destination Address: all [Multiple](#)

Schedule: always

Service: ANY [Multiple](#)

Action: ACCEPT

Log Allowed Traffic

NAT

No NAT

Enable NAT Dynamic IP Pool

Use Central NAT Table

Enable Identity Based Policy

UTM

Traffic Shaping: [Please Select]

Reverse Direction Traffic Shaping: [Please Select]

Per-IP Traffic Shaping: [Please Select]

Enable Endpoint NAC: [Please Select]

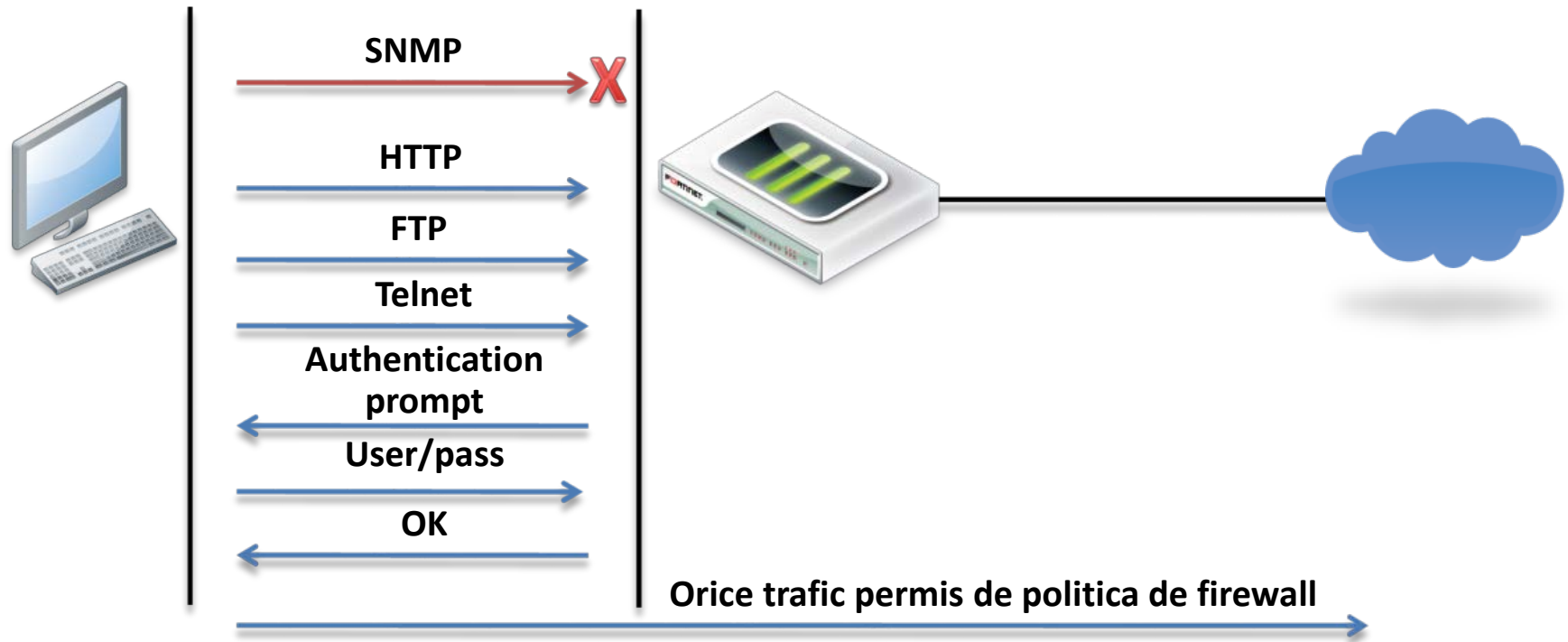
Comments (maximum 63 characters)

Autentificare prin politica de firewall

- ▶ Este activată din interiorul politicii
 - ❑ Se numește “Identity-based policy”
- ▶ Hostul nu are nevoie de configurare proxy
- ▶ Se poate face prin:
 - ❑ Certificate – trebuie instalate atât pe FortiGate cât și pe hosturi (browsere)
 - ❑ User și parolă
- ▶ Autentificarea cu user și parolă se poate face doar prin generare de trafic:
 - ❑ HTTP
 - ❑ FTP
 - ❑ telnet

Autentificare prin politica de firewall

- ▶ Utilizatorul trebuie să se autentifice mai întâi la firewall prin generare de trafic care este are suport de autentificare din partea firewall-ului
- ▶ După autentificare, utilizatorul poate genera orice trafic permis de politica de firewall



Politici DoS

- ▶ Prima procesare realizată asupra unui pachet ingress
 - ❑ Avantajul este ca pachete aparținând unui atac DoS nu mai sunt procesate de firewall, AV, IPS etc
- ▶ În mod implicit, FortiGate oferă 2 senzori
 - ❑ All-default – lasă tot traficul să treacă
 - ❑ Block-dos – preconfigurat de Fortinet pentru a bloca:
 - tcp_syn_flood
 - udp_flood
 - icmp_flood
 - ❑ Se pot crea senzori custom pentru detecția mai multor tipuri de atacuri DoS
- ▶ Activarea unei politici de DoS se face separat de politica de firewall

Exemplu: DoS policy

System

- Router
 - Firewall**
 - Policy
 - Policy
 - Central NAT Table
 - DoS Policy**
 - Sniffer Policy
 - Protocol Options
 - Address
 - Service
 - Schedule
 - Traffic Shaper
 - Virtual IP
 - Load Balance
- UTM
- VPN
- User
- Endpoint
- Wireless Controller
- Log&Report

New Policy

Source Interface/Zone: wan2

Source Address: all Multiple

Destination Address: all Multiple

Service: ANY Multiple

DoS Sensor: [Please Select] (dropdown menu open)

- [Please Select]
- [Please Select]
- [Create New...]
- all_default
- block_flood

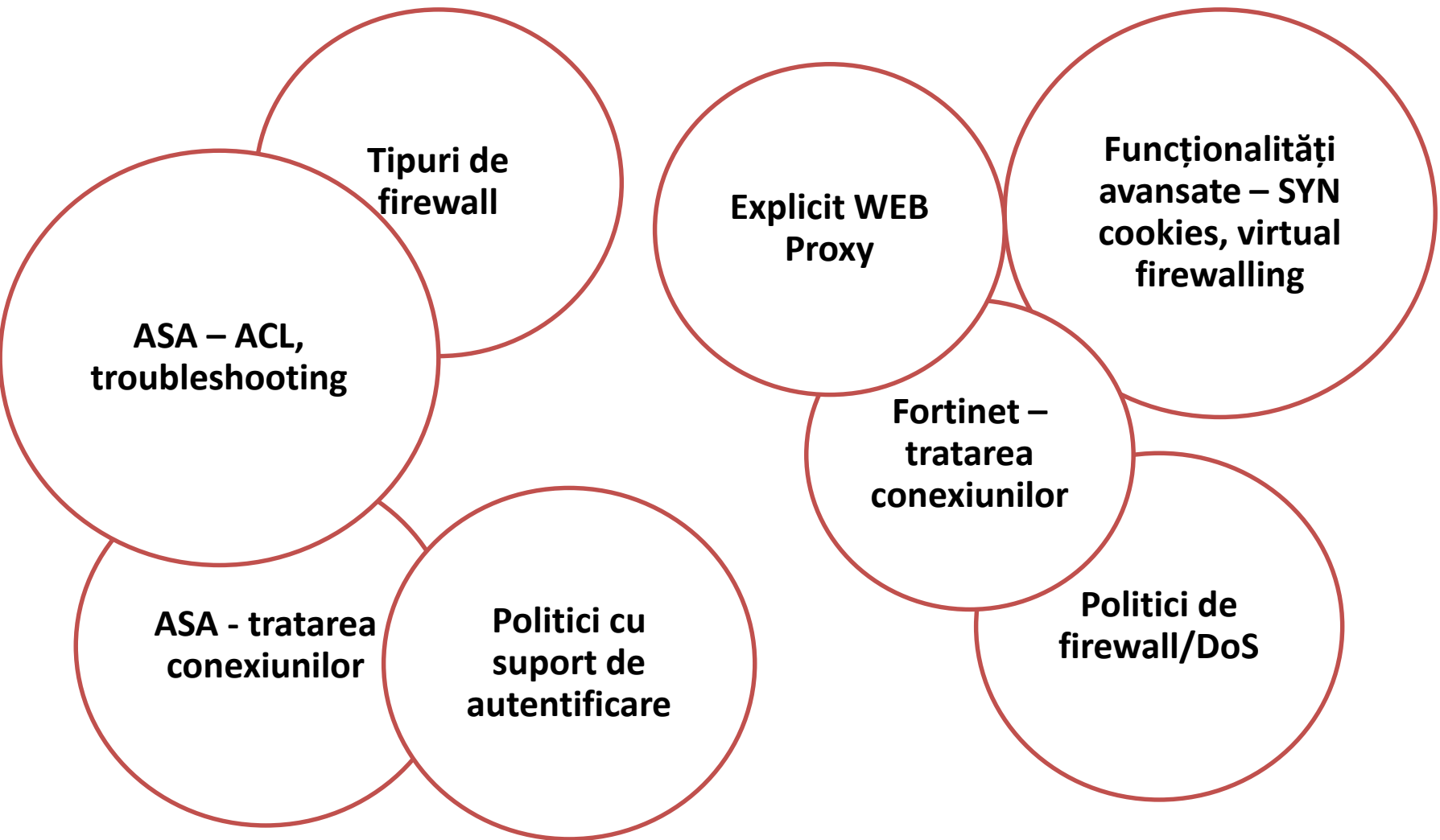
Cancel

Explicit WEB Proxy

- ▶ Util pentru caching/logging
- ▶ Poate fi activat pentru HTTP/FTP proxying
- ▶ Browserul clienților trebuie configurat explicit pentru proxy

- ▶ Atenție: configurarea proxy trebuie făcută doar pe interfața de intrare
 - ❑ Activarea pe interfața de WAN permite oricărui host de pe Internet să folosească firewallul ca proxy
- ▶ Nu se pot configura tunele IPSec, SSL sau traffic shaping pentru proxy-ul web

Overview



Cursul viitor...

- ▶ Se va concentra ceva mai mult pe ASA
- ▶ NAT/PAT
 - ❑ “What do you mean no more IPv4 addresses? We’ll just put the entire Internet behind a NAT!”
- ▶ Become an ASA ACL wizard!
- ▶ Reducerea complexității configurațiilor de politici:
 - ❑ ASA object-grouping
 - ❑ Fortinet service/address grouping

