VPN şi IPsec

29 martie 2010

IPSec – concepte

- Proces de tunelare folosit pentru protejarea datelor dintr-un pachet
- Defineşte mai mult un concept, şi nu o implementare
- Asigură autentificarea, integritatea şi confidenţialitatea datelor
- Datele pot fi securizate începând cu nivelul 3
- Poate fi folosit în două moduri
  - tunelare
  - transport

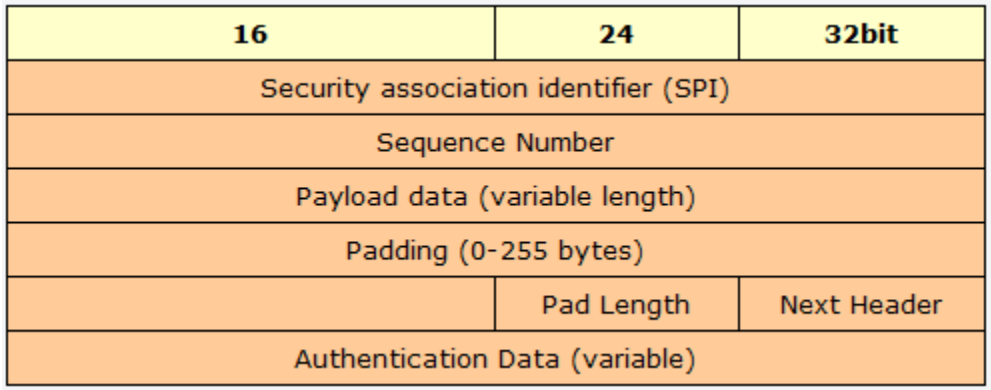
AH – Authentication Header

- Asigură autentificarea şi integritatea datelor la nivel aplicaţie
- Foloseşte chei simetrice pentru autentificare
- Nu funcţionează cu NAT

8	16	32bit
Next Header	Payload Length	Reserved
Security parameters index (SPI)		
Sequence Number Field		
Authentication data (variable)		

ESP – Encapsulating Security Payload

- Folosit pentru autentificare şi criptare
- Asigură criptarea la nivel aplicaţie
- Foloseşte chei simetrice pentru autentificare
- Poate proteja traficul de replicare prin numere de secvenţă
- Poate funcţiona împreună cu serviciul de NAT



IKE – Internet Key Exchange

- Protocol folosit pentru negocierea conexiunii
- Pentru fiecare conexiune IPSec este necesară crearea unei asocieri de securitate "security association" (SA)
- Fiecare SA este salvat într-o bază de date locală numită Security Paramater Index (SPI)
- ISAKMP – Internet Security Association Key Management Protocol
  - un framework folosit pentru negocierea parametrilor
  - Oakley este un protocol ce foloseşte Diffie-Hellman pentru generarea de key simetrice ce vor fi folosite

IKE – Main mode

- Pasul 1
  - Iniţiatorul IPSec propune o suită de protocoale ce vor fi folosite
  - Pentru asigurarea folosirii celui mai bun pachet acestea trebuie definite în ordine

Criptarea datelor	DES, 3DES
Integritatea datelor	MD5, SHA1
Metode de autentificare	Kerberos, preshared, certificat
Diffie-Hellman	Group 1/2/5

- Pasul 2
  - Se generează o pereche de chei Diffie-Hellman
- Pasul 3
  - Autentificarea

IKE – Quick mode

- Mesajele trimise în acest mod sunt protejate de către Security Association din Main mode
- În această etapă se crează două alte SA pentru traficul inbound şi outbound
- Propune protocoale folosite pentru IPSec (AH vs. ESP, MD5 vs. SHA, DES vs. 3DES)
- La finalul acestei etape se stabilesc 3 SA
  - Pentru trafic de control
  - Pentru trafic inbound
  - Pentru trafic outbount

Windows Firewall with Advanced Security

- Folosit pentru definirea de noi reguli IPSec pentru o conexiune
- Există mai multe tipuri de reguli predefinite
  - isolation
  - authentication exemption
  - server-to-server
  - tunnel
  - custom
- Acestă metodă nu este foarte des folosită

Local Policy

- Se crează o regula care specifică
  - Listă de filtrare pentru care se aplică
  - Acţiunea care defineşte modul în care este prelucrat traficul
    - dacă se cere securizarea traficului atunci trebuie specificate şi metodele de securizare
    - traficul se poate bloca sau permite (similar firewall)
- Ordinea de prelucrare a listelor este bazată pe calculul "greutăţii" listei de filtrare
- Acest calcul se pe baza
  - adresa IP sursă şi destinaţie
  - masca de reţea pentru sursă şi destinaţie
  - valoarea protocolului IP
  - valoarea porturilor UDP / TCP sursă sau destinaţie

Local Policy

- "Greutatea" unei regulii de filtrare este cu atât mai mare cu cât parametrii definiţi sunt mai specifici
- O regulă cu o greutate mai mare este preferată
- În cazul în care două reguli sunt identice dar acţiunea specificată este diferită ordinea este
  - block > securizarea traficului > permiterea

IPSec – HowTo

- Configurarea unei noi politici IPSec pentru winXP

1. *[start]→[run] →[secpol.msc] →[IP Security Policies on Local Computer] →[⇪][Create IP Security Policy] →[No default response rule]*
2. *[start] →[run] →[secpol.msc] →[IP Security Policies on Local Computer] →[policy name] →[⇪][Properties] →[Add]*
   - folosim cheie preshared key
   - *[add new filter rule] →[adăugăm un nou filtru pentru acestă listă] →[selectăm tipul de trafic interesant]*
   - *[add new filter action] →[selectăm metodele de criptare pentru ipsec]*
3. *[start] →[run] →[secpol.msc] →[IP Security Policies on Local Computer] →[policy name] →[⇪][Assign]*

- Configurarea tipurilor de metode de securitate folosite pentru IKE Main mode

1. *[start] →[run] →[secpol.msc] →[IP Security Policies on Local Computer] →[policy name] →[⇪][Properties] →[General] →[Advanced] →[Methods]*
   - ordinea în care aceste metode vor fi folosite este importantă

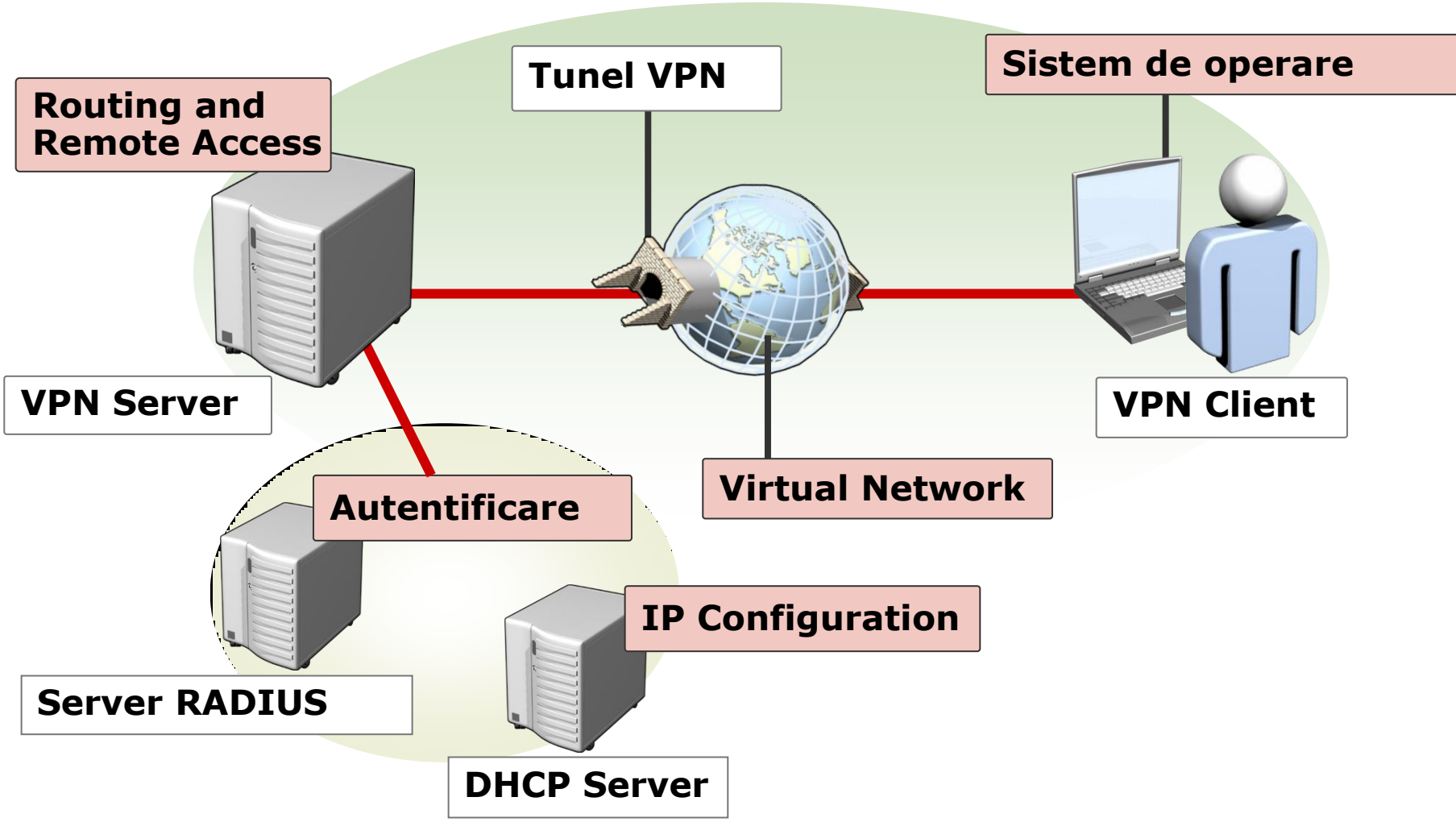
IPSec – HowTo for a router (remember SRS)

1. configurarea politicilor isakmp (pentru ike main mode)
2. configurarea ipsec transform set (pentru ike quick mode)
3. definirea traficului interesant
4. configurarea unui crypto map
5. asignarea unui crypto map pe interfata

VPN – Virtual Private Connection

- Reprezintă o conexiune punct-la-punct realizată peste un mediu de transmisie de obicei public
- Tehnologiile VPN diferă prin
  - protocolul de tunelare folosit
  - prin punctul de terminare (la client sau la ISP)
  - site-to-site sau acces de la distanţă
  - nivelul de securitate oferit
  - prin nivelul din stiva OSI la care este implementat

VPN - componente

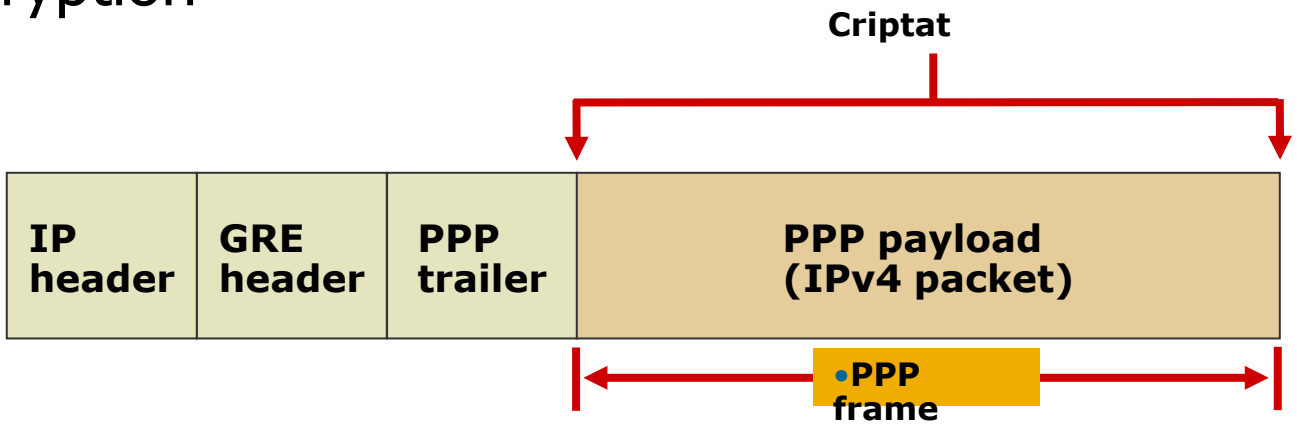


VPN – concepte

- Encapsularea datelor
  - Datele utilizatorului sunt reîncapsulate pentru a fi transportate peste reţeaua publică
- Autentificarea
  - folosită pentru a determina dacă un client are acces la reţea
  - poate fi folosită şi pentru autentificarea serverului
- Autorizarea
  - asigură un anumit nivel de acces pentru clienţi

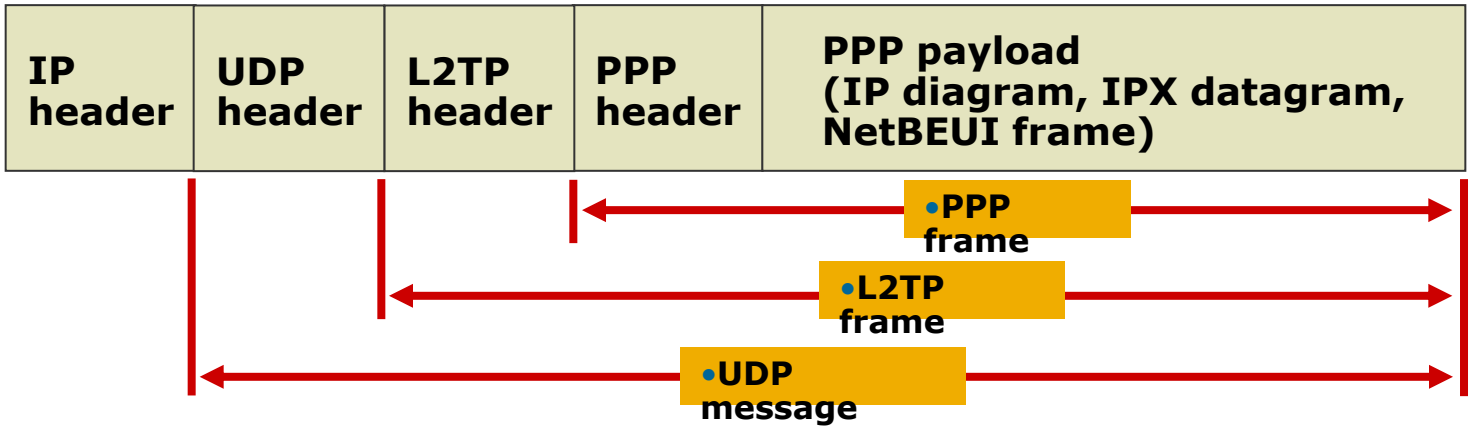
Protocoale de tunelare – PPTP

- Permite encapsularea multiprotocol
- Foloseşte conexiuni TCP portul 1723
- Deschide peste conexiunea TCP un tunel GRE (versiune non-standard)
- Peste tunelul format sunt încapsulate alte protocoale
- Criptarea se realizează folosind Microsoft Point-to-Point Encryption



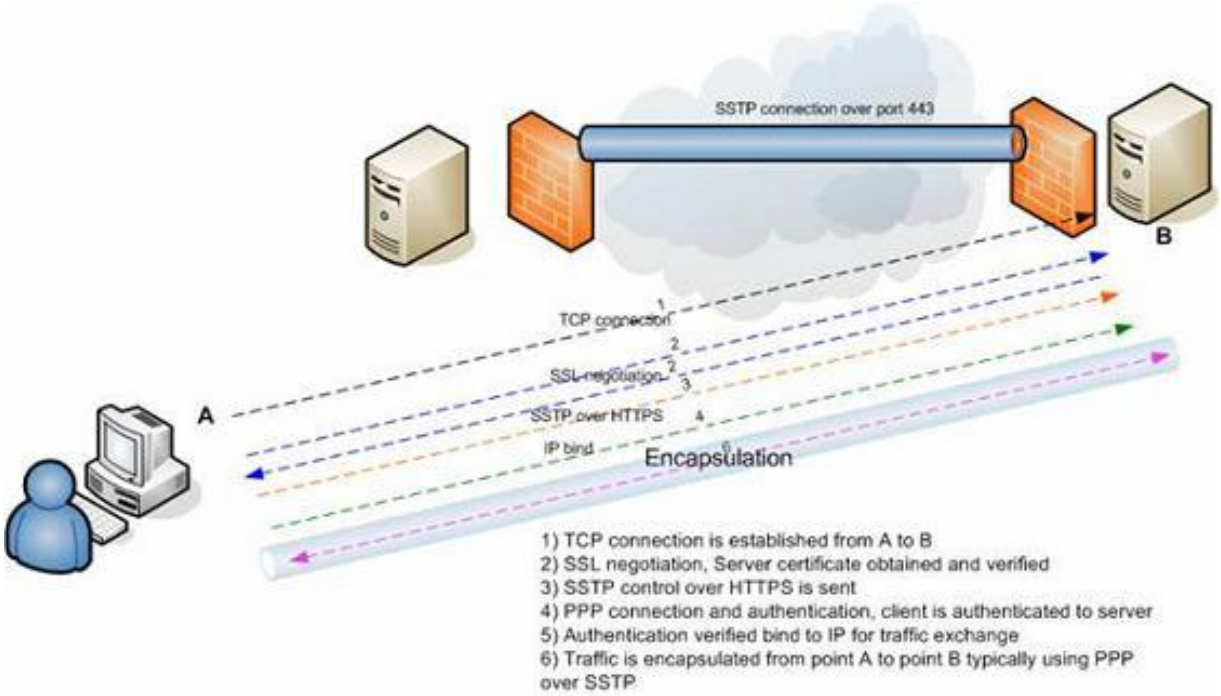
Protocoale de tunelare – L2TP/IPSec

- L2TP nu oferă criptare sau confidenţialitate
- Se negociază întâi IPSec SA
- Datele sunt tranportate folosind IPSec ESP
- Ultimul pas este de negociere a parametrilor L2TP



Protocoale de tunelare – SSTP

- Protocol de tunelare ce foloseşte HTTPS
- Foloseşte portul 443 pentru trimiterea datelor dar şi a mesajelor de control
- Poate fi folosit cu uşurinţă peste orice tip de firewall



Protocoale de autentificare

Protocol	Descrierea	Nivel de securitate
PAP	Foloseşte parole în text clar. Folosit de obicei când clientul şi serverul remote nu pot negocia o formă mai sigură de validare.	Cel mai puţin sigur protocol de autentificare. Inutil în cazul atacurilor replay, impersonări ale clientului remote, sau impersonări ale serverului remote.
CHAP	Un protocol de autentificare challenge-response ce foloseşte schema hash MD5 pentru a cripta răspunsul.	O îmbunătăţire peste PAP a faptului că parola nu este trimisă pe link-ul PPP. Necesită o versiune în text clar a parolei pentru a valida răspunsul challenge. Nu protejează în cazul impersonării serverului remote.
MS-CHAPv2	Un upgrade al MS-CHAP. Autentificare mutuală. Clientul remote primeşte verificarea că serverul remote pe care-l accesează are acces la parola utilizatorului.	Oferă securitate mai bună decât CHAP.
EAP	Permite autentificarea arbitrară a unei conexiuni la distanţă folosind scheme de autentificare, cunoscute sub numele de tipuri EAP.	Oferă cea mai puternică securitate furnizând flexibilitate la tipurile de autentificare.

Metode de autentificare

- Folosind proprietăţile Dial-in ale unui utilizator
  - configurare manuală pentru fiecare utilizator
- Folosind un server de Network Policy Server
  - configurare pentru un anumit grup de utilizatori
  - un grup de utilizator se poate definii folosind diferite condiţii
- Folosind un server de RADIUS
  - autentificarea se face prin interogarea unui server de RADIUS

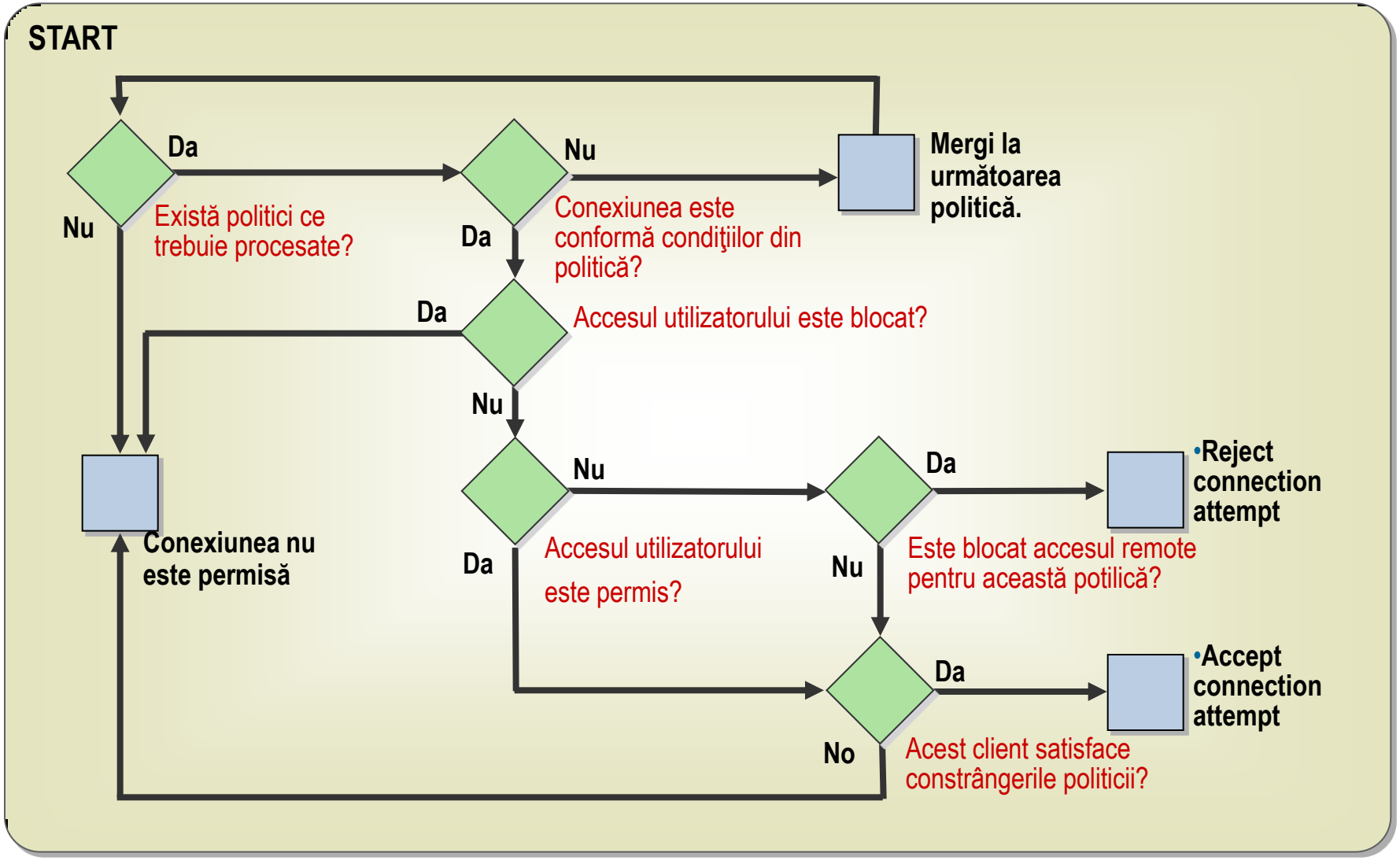
Autorizarea clienţilor

- Reprezintă procesul de permitere sau nu a accesului
- Pentru VPN se pot defini mai multe politici de acces folosind Network Policy Server
- Fiecare politică are asociată o prioritate
  - prioritate mai mică = politica va fi accesată prima

Politică de acces

- Condiţiile
  - pentru cine se aplică această politică
  - ex. interval de timp, utilizator, metoda de autentificare folosită de client
- Constrângerile
  - defineşte anumiţii parametri ce trebuie îndepliniţi de către clienţi
  - ex. idle timeout, session timeout, restricţii de timp
- Permisiunea
  - dacă acest client este acceptat sau nu
- Parametrii conexiunii
  - configurările pentru un client care a fost acceptat
  - ex. criptarea traficului PPP, filtrarea traficului primit

Ordinea de procesare a politicilor



Adresarea IP prin VPN

- Pentru fiecare client se poate configura o adresă IP statică ce îi va fi asignată
- Se poate folosi un server de DHCP intern serviciului de VPN
- Se poate folosi un DHCP Relay Agent pe serverul de VPN pentru a trimite cererile de DHCP unui server local

VPN – HowTo