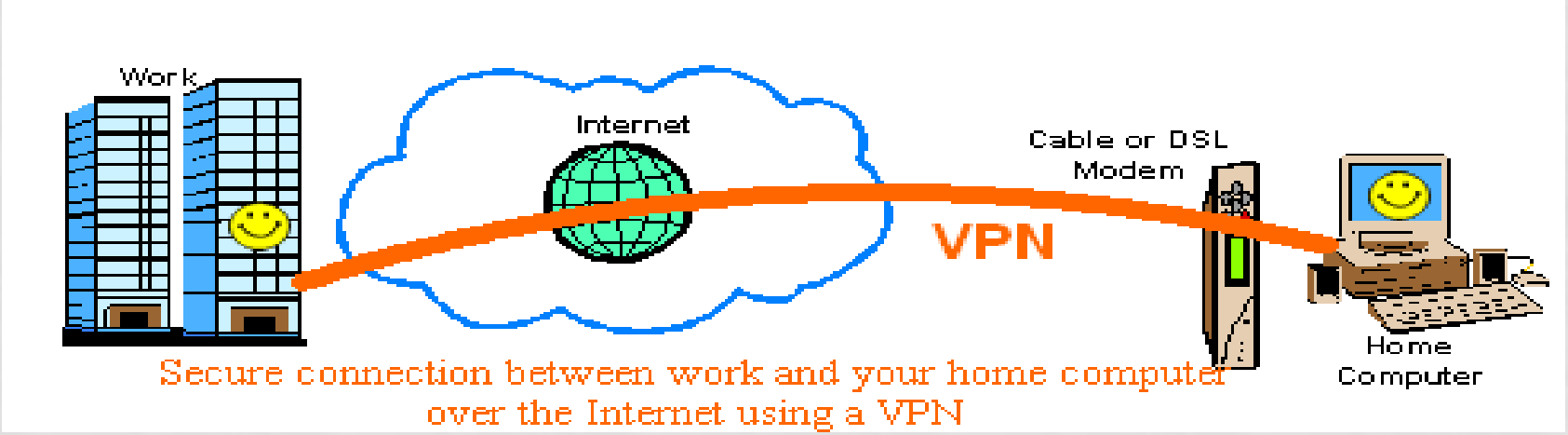
Institucioni i Arsimit
UNIVERSITAR AAB
PRISHTINË

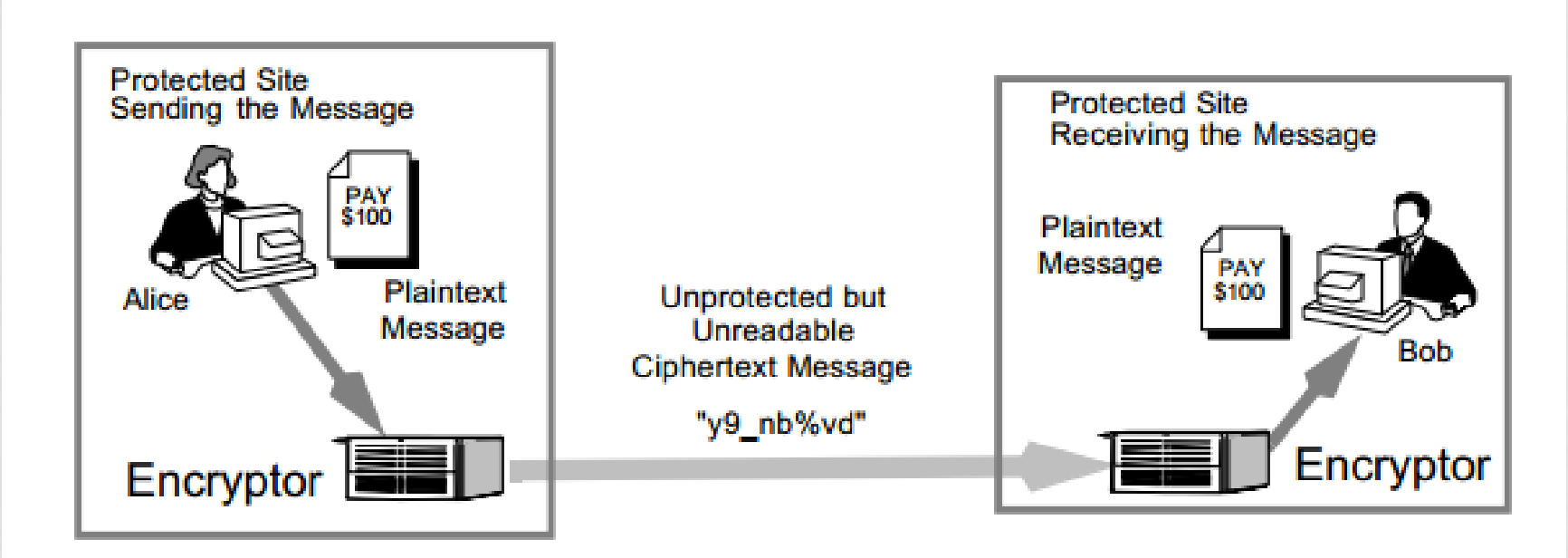
FAKULTETI I SHKENCAVE KOMPJUTERIKE

CFARË ËSHTË (VPN)

- VPN - lejon 2 ose më shumë rrjete private të lidhen mes tyre
- VPN - është një tunel komunikimi i sigurtë dhe privat
- VPN - perdor rrjetin publik (internetin) në vend të linjave të dedikuara
- VPN – Perdorin rrjetin publik me te dhena te enkriptuara



KODIMI I MESAZHIT PERMES VPN



- Mbron fjalekalimet nga nderhyrjet e sistemit
- Bllokon perdoruesit e jashtem (lejon vetem mesazhet e koduara)

SI FUNKSIONON VPN???

- VPN Klient dhe VPN Server (hardware ose software)

1. Lejon tunelet VPN të konfigurohen
2. Authentifikon nyjen tjetër të një lidhjeje VPN
3. Ruton të dhënat e marra nga rrjeti i vet lokal tek tuneli VPN
4. Kodon të dhënat në tunelin VPN dhe i enkapsulon ato në paketë IPSec

5. Bën de - kodimin paketës IPSec e marrë nga tuneli VPN dhe bën dekodimin e të dhënave
6. Ruton të gjitha të dhënat e marra nga tuneli në rrjetin lokal(LAN)
7. Lejon tunelet VPN të menaxhohen

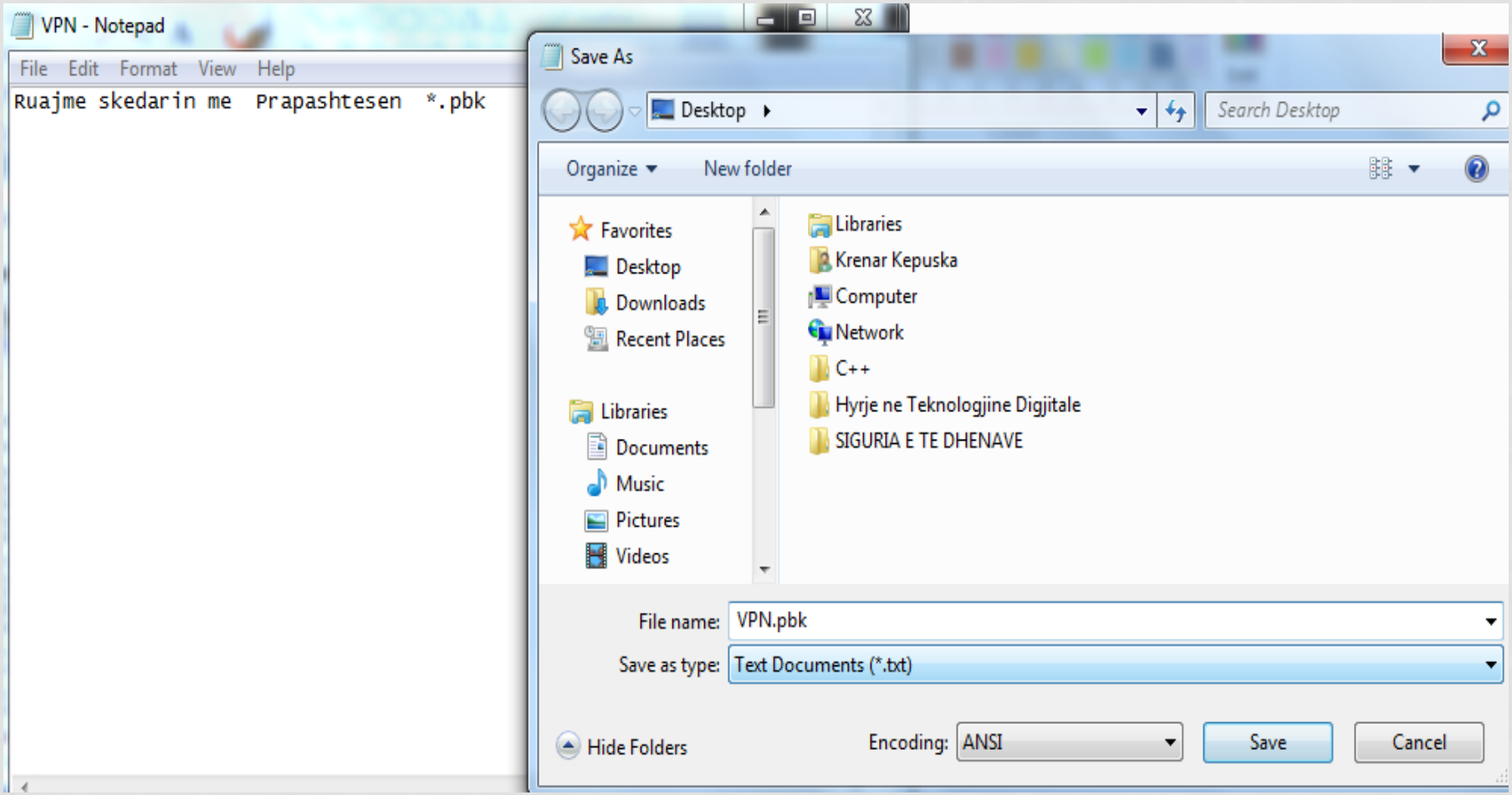
KOMUNIKIMI ME VPN

1. Network-Network - dy subnete janë lidhur me njëri-tjetrin duke përdorur tunel VPN, ku cdo subnet duhet të konsistojë në një gateway/router dhe një host.

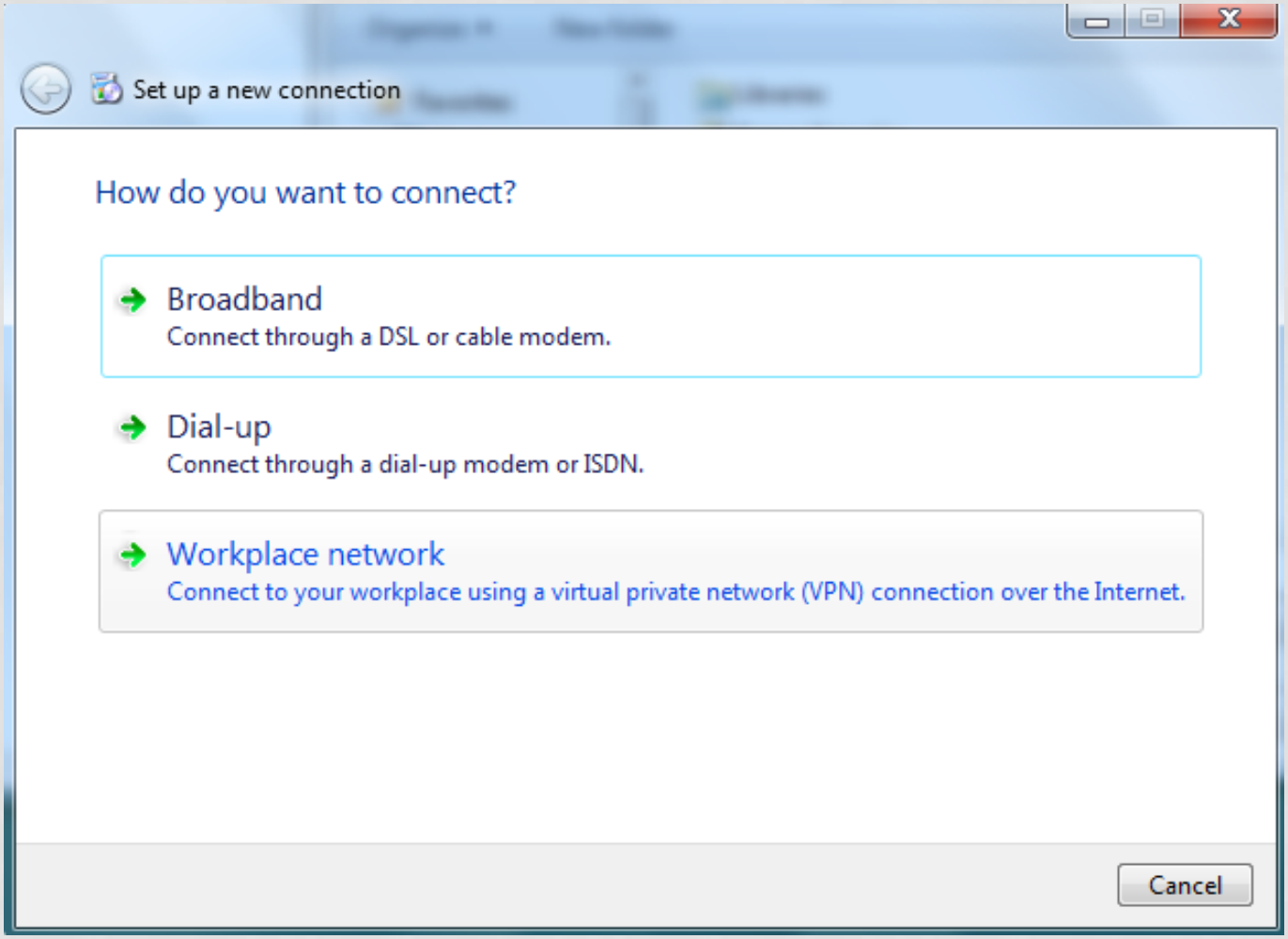
2. Host-Network - përdoret kur një nga subnetet që do të lidhet konsiston në nje host të vetëm.

3. Host – Host – përdoret kur ne duam të vendosim një tunel të sigurtë ndërmjet dy hosteve që i takojnë dy rrjeteve të ndryshme.

KONFIGURIMI I VPN

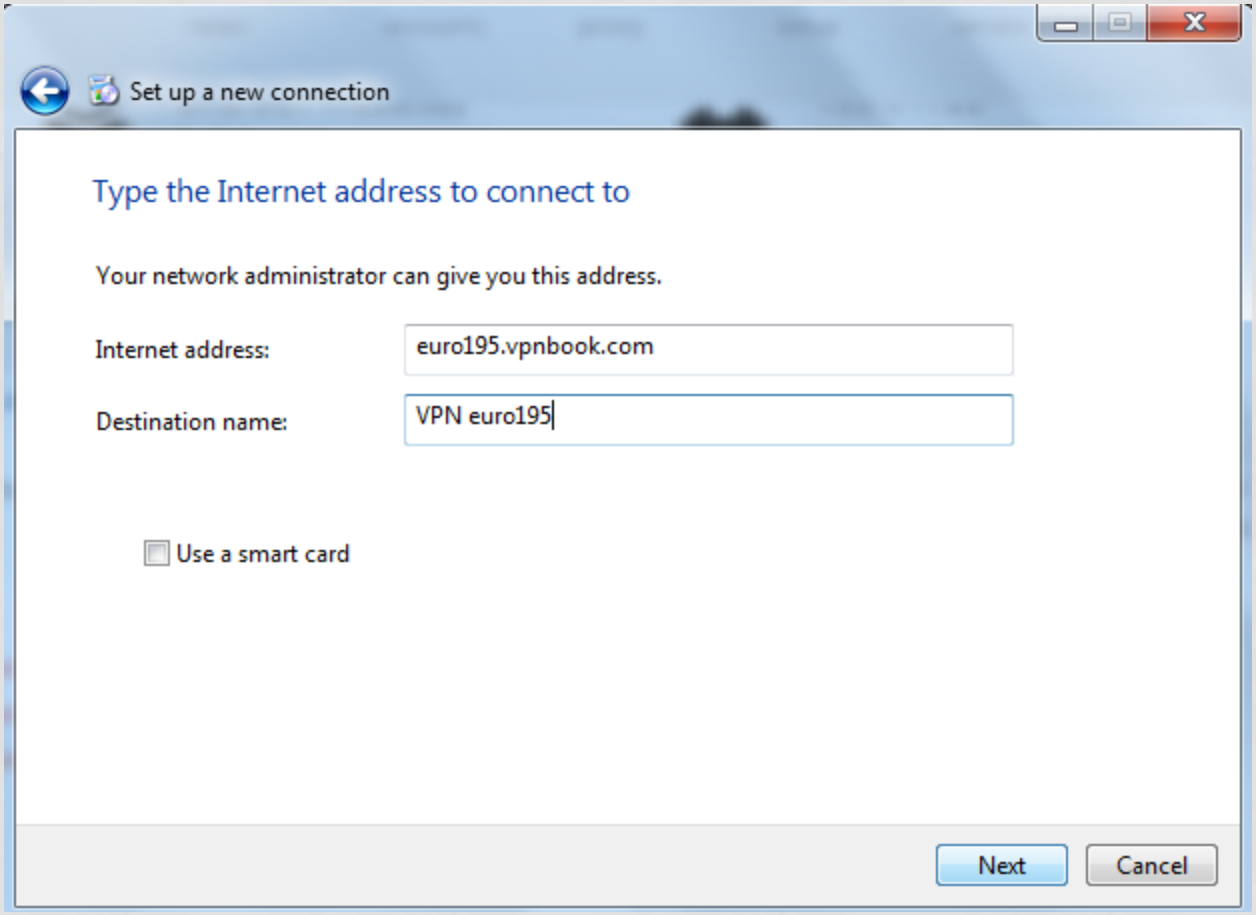


KONFIGURIMI I VPN

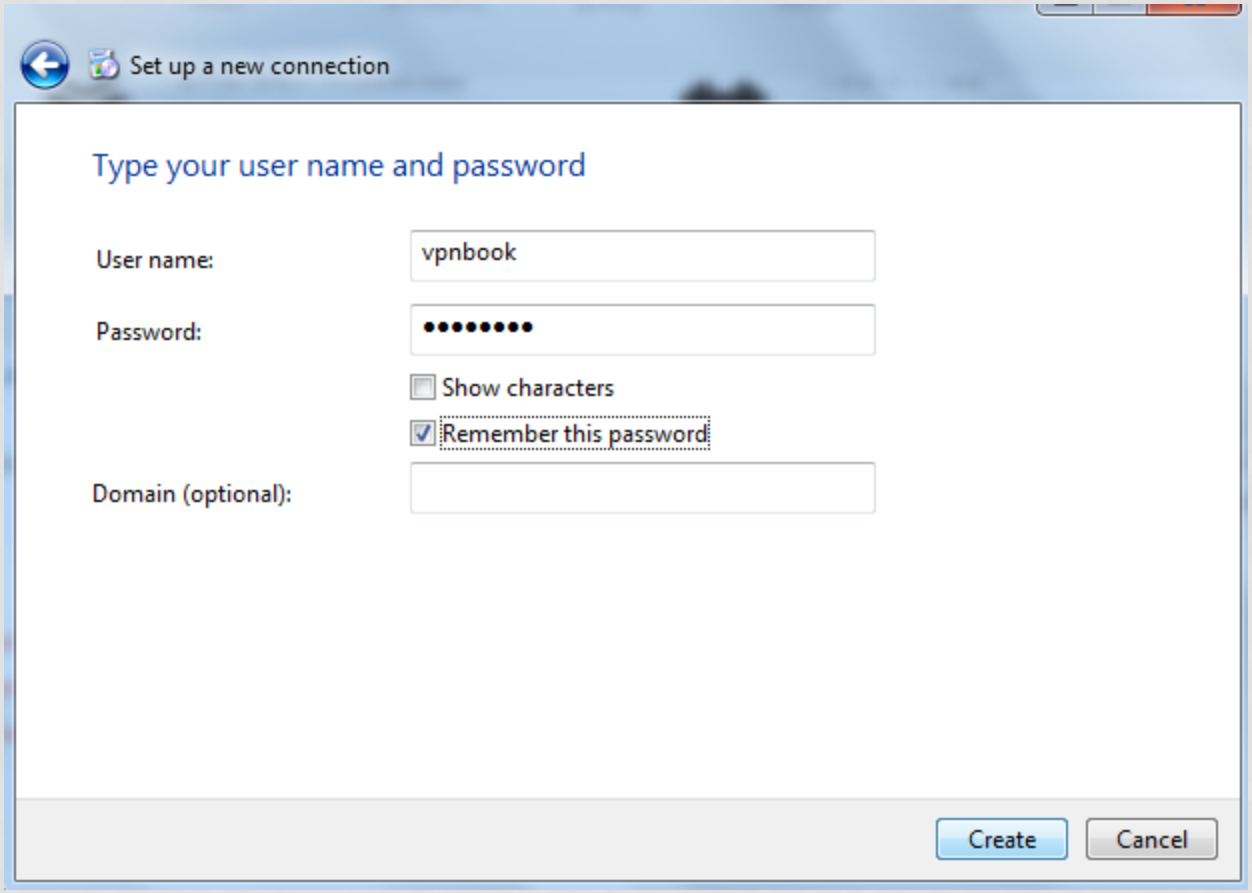


KONFIGURIMI I VPN

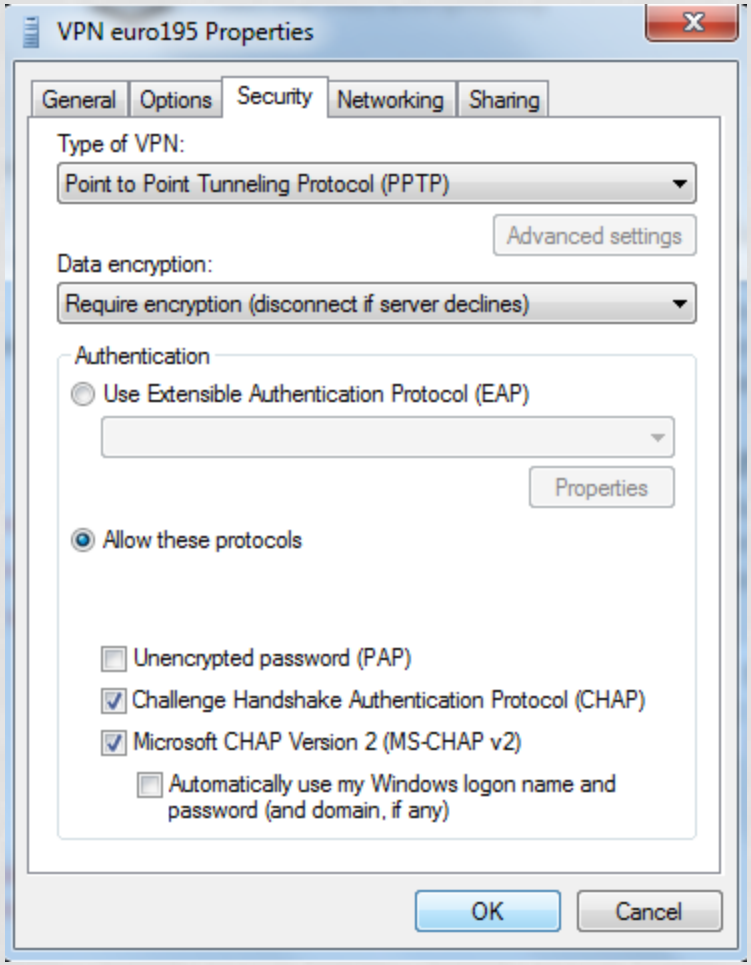
KONFIGURIMI I VPN

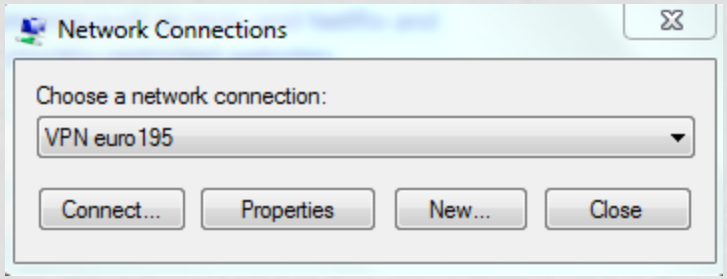


KONFIGURIMI I VPN

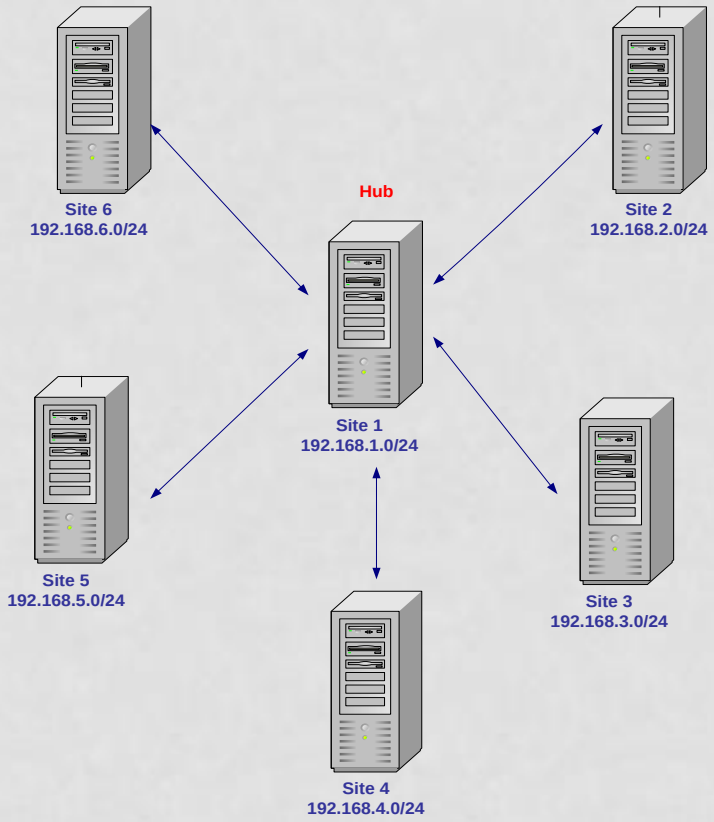


KONFIGURIMI I VPN





TOPOLOGJIA YLL

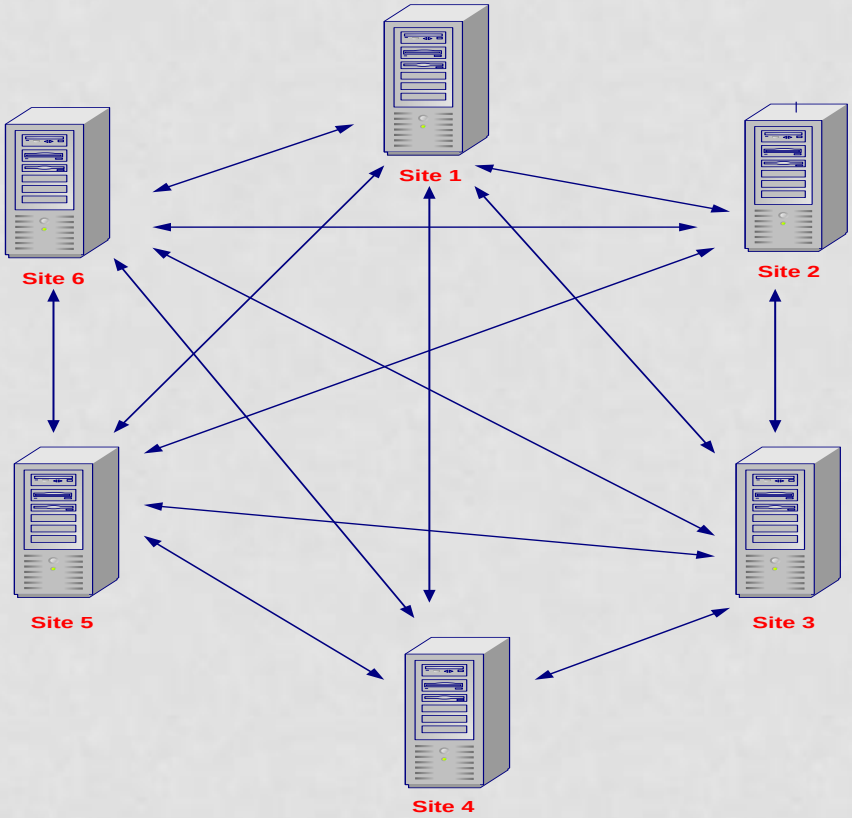


- Ka një pikë të vetme dështimi - nëse hub-i bie, atëherë të gjithë sitet nuk komunikojnë dot më me njëri-tjetrin.

- Nëse performanca e hub- it është e ulet atëherë edhe performanca e të gjithë lidhjeve VPN do të jetë e tillë.

- Dy nyje që gjeografikisht mund të jenë shumë afër njera-tjetrës sërisht duhet të komunikojnë përmes hub -it.

TOPOLOGJIA FULL MESH



- Nuk ka më vetëm një pikë dështimi. Site-t nuk kounikojnë më me një hub qëndror për të vendosur lidhjen me një site tjetër
- E gjithë performanca e sistemit nuk është e varur vetëm nga një pikë
- Site që ndodhen gjeografikisht pranë njëri-tjetrit mund të komunikojnë direkt

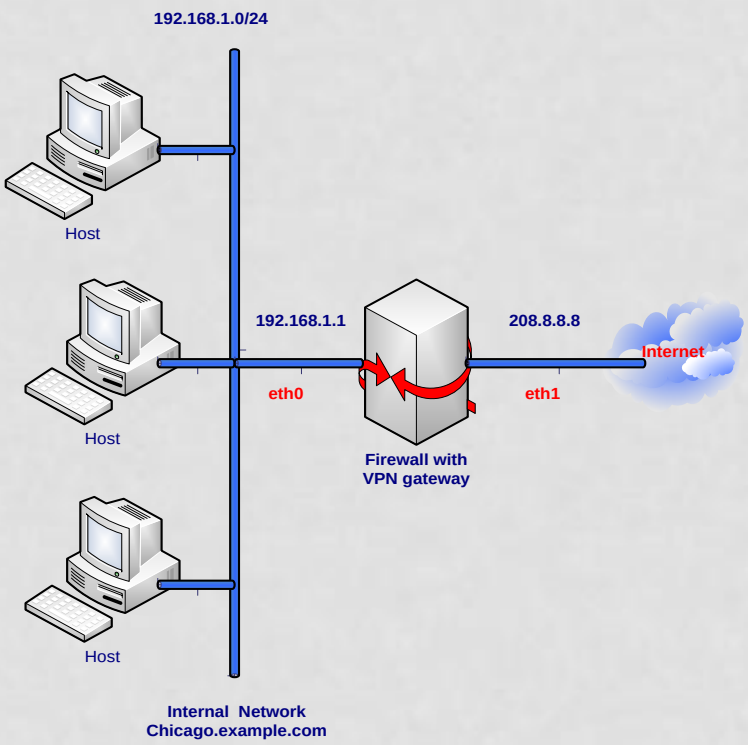
PROTOKOLLET VPN PER KODIM

- **IPSec** - siguron algoritma të fuqishëm enkriptimi dhe më shumë autentifikim. IPSec ka dy modele enkriptimi:tunel dhe transport. Tunel enkripton kokën dhe payload-in e cdo pakete ndërkohë që transporti enkripton vetëm payload-in.

- **PPTP/MPPE** - PPTP suporton multi-protocol VPN me enkriptim 40 bit dhe 128 bit duke përdorur një protokoll të quajtur MPPE (Microsoft Point-to-Point Encryption)

- **L2TP/IPSec**–zakonisht i quajtur L2TP mbi IPSec,kjo siguron sigurinë e protokollit IPSec në tunelimin e shtresës se dytë të protokollit të tunelimit(L2TP).

VPN SERVER NË NJË FIREWALL

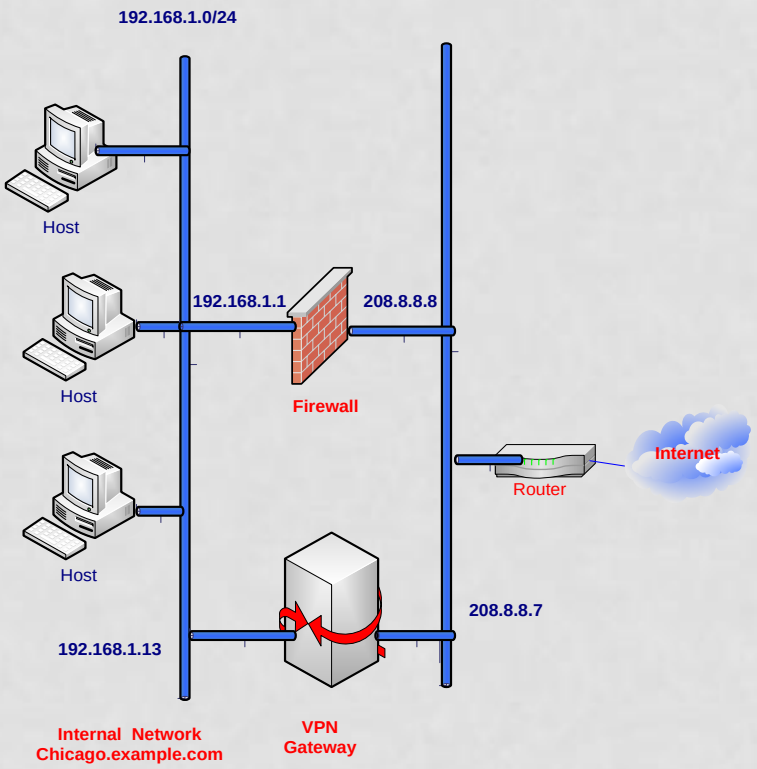


- Firewall-i lejon akses të jashtëm për në internet dhe pengon akses te brendshëm nga interneti
- Shërbimi i VPN-së enkripton trafikun për klientin ose rrjetin nëlargësi

- Ne kemi vetëm një pikë për të kontrolluar sigurinë tonë, që do të thotë me pak makina për të manaxhuar.

- Duke qenë se ne kemi vetëm një pikë nga ku mund të kontrollojmë sigurinë tonë duhet të sigurohemi që kjo makinë është në një siguri maksimale.

LIDHJA E VPN SERVER PARALEL ME FIREWALL-IN



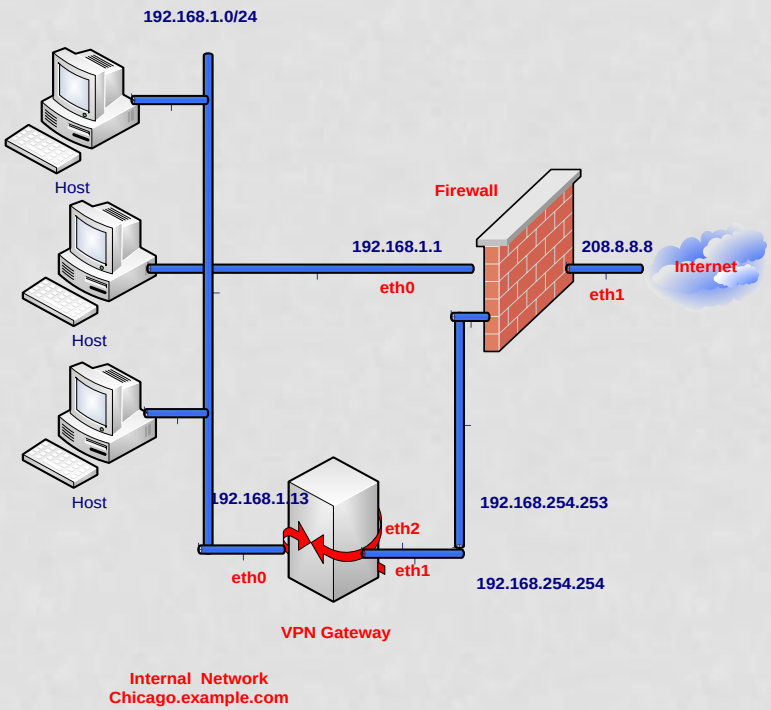
Tafiku VPN nuk do të kalojë përmes firewall-it kështu që nuk është e nevojshme të konfigurohet firewall-i për të suportuar paketat VPN.

Nëse një server VPN është shumë i ngarkuar ne mund të shtojmë makina të tjera dhe të shpërndajmë lidhjet VPN që mund të vendosen.

Serveri ynë VPN është i lidhur direkt me interntin, kështu që ne duhet të sigurohemi që kjo makinë është e siguruar, përndryshe një sulmues mund të aksesojë rrjetin tonë të brendshëm.

Vendosja e një serveri tjetër dhe e të gjithë stafit të lidhur metë rrit shumë koston

VENDOSJA E SERVERIT VPN PAS FIREWALL-IT



Avantazhet:

VPN është e gjitha e mbrojtur nga internti nëpërmjet firewall-it

Është vetëm një makinë për të kontrolluar të gjithë aksesimin nga dhe për në internet

Të gjithë kufizimet për trafikun VPN janë lokalizuar vetëm tek serveri VPN i cili e bën më të thjeshtë shkrimin e rregullavea

AVANTAZHET VPN

- Siguria : të gjitha të dhënat janë enkriptuar duke përdorur një celes prej 168 bitesh

- Kostoja : zëvendësimi i linjave të dedikuara të cilat janë shumë të shtrenjta e ul shumë koston.

- Shkallezueshmeria : kostoja e një organizate që përdor linja të dedikuara fillimisht mund të jetë e arsyeshme por mund të rritet në mënyrë eksponenciale me rritjen e organizatës.

- VPN-ja që përdor internetin mund ta evitojë këtë problem. Duke e krahasuar me linjat e dedikuara VPN-ja ofron një hapsire globale më të madhe.

- Fleksibiliteti : pothuajse i gjithë trafiku IP mund të rutohet përmes VPN-së.

DISAVANTAZHET E VPN-SË

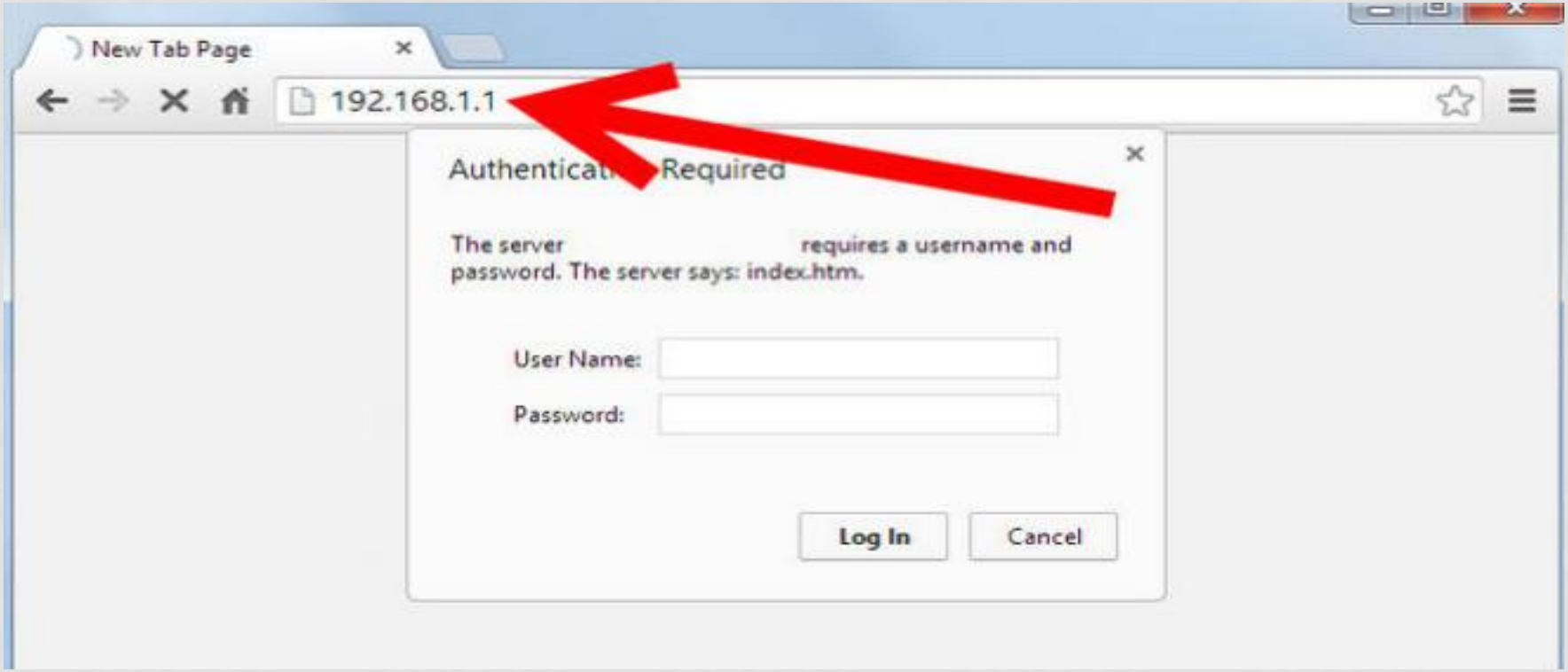
- VPN-të kërkojnë që ceshtjet e sigurisë së rrjetit publik, internetit të kuptohen në detaje dhe në brendësi.

- Disponueshmëria dhe performanca e një organizate wide-area VPN varet nga faktorë qe janë shume larg kontrollit të organizatës.

- Teknologjitë VPN nga prodhues të ndryshëm mund të mos punojnë dot mirë së bashku.

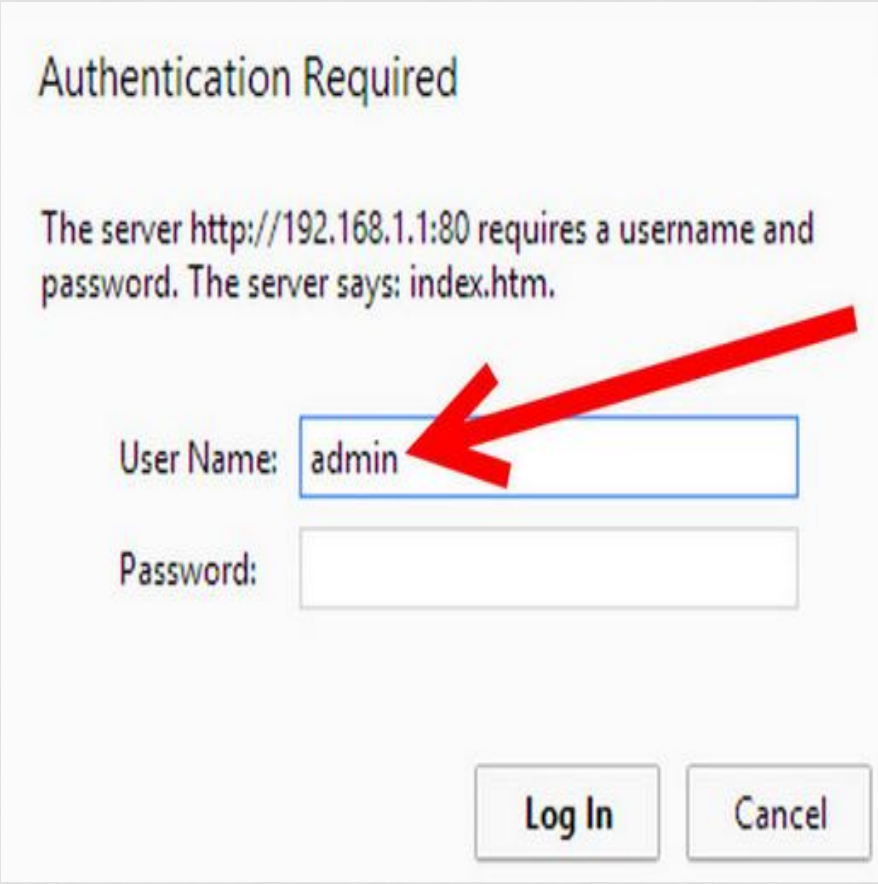
- VPN-ja ka nevojë për protokolle të tjerë përvec protokollit IP.

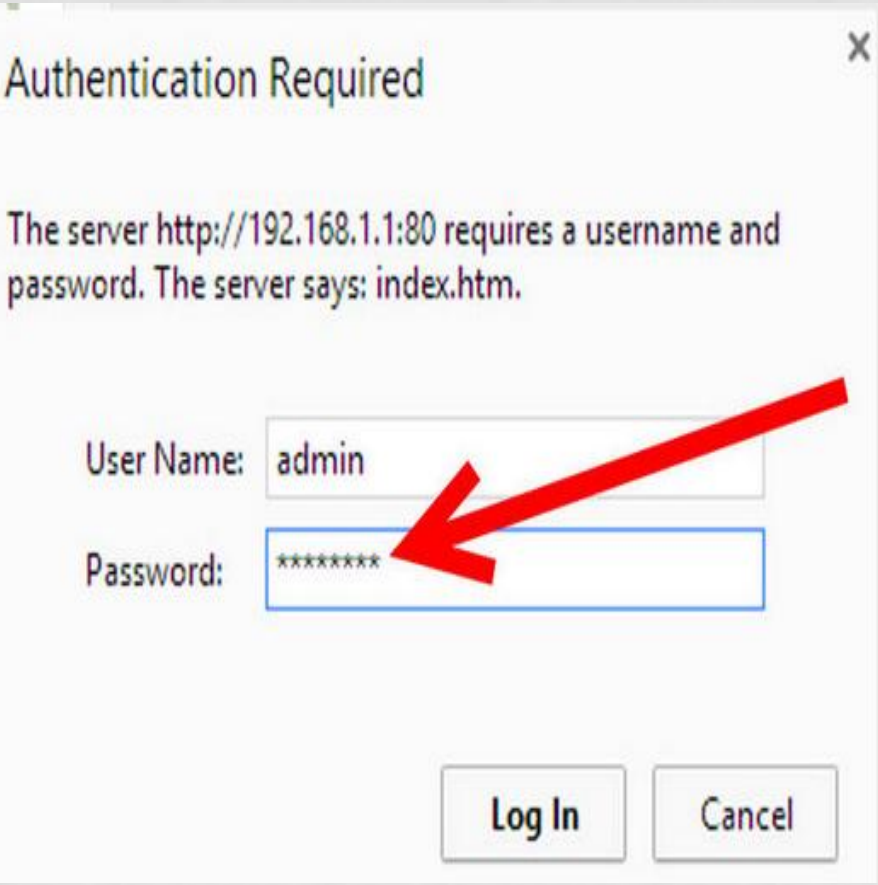
KONFIGURIMI I WIRELESS ROUTER



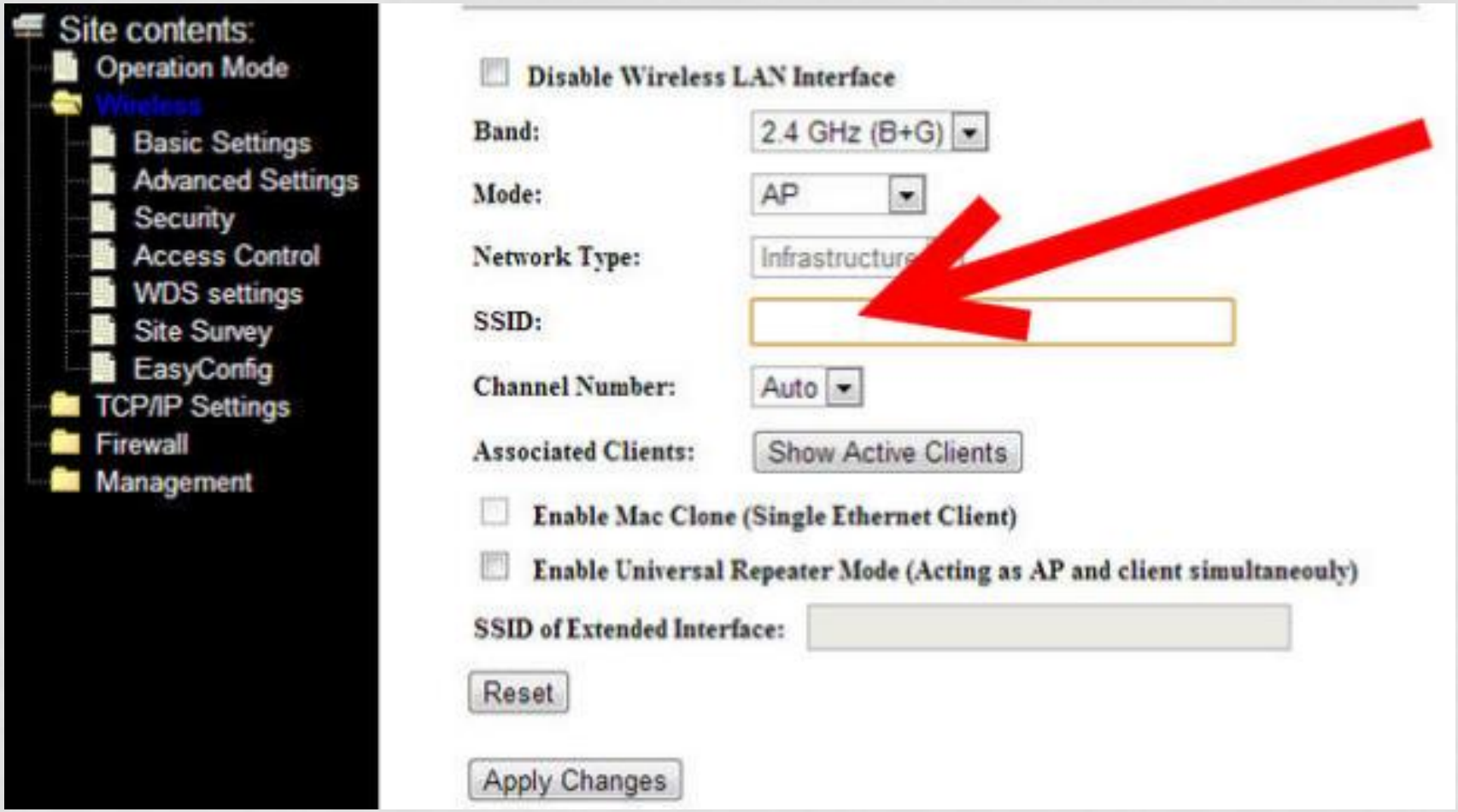
192.168.1.1 \\ 192.168.0.1 \\ 192.168.2.1

KONFIGURIMI I WIRELESS ROUTER

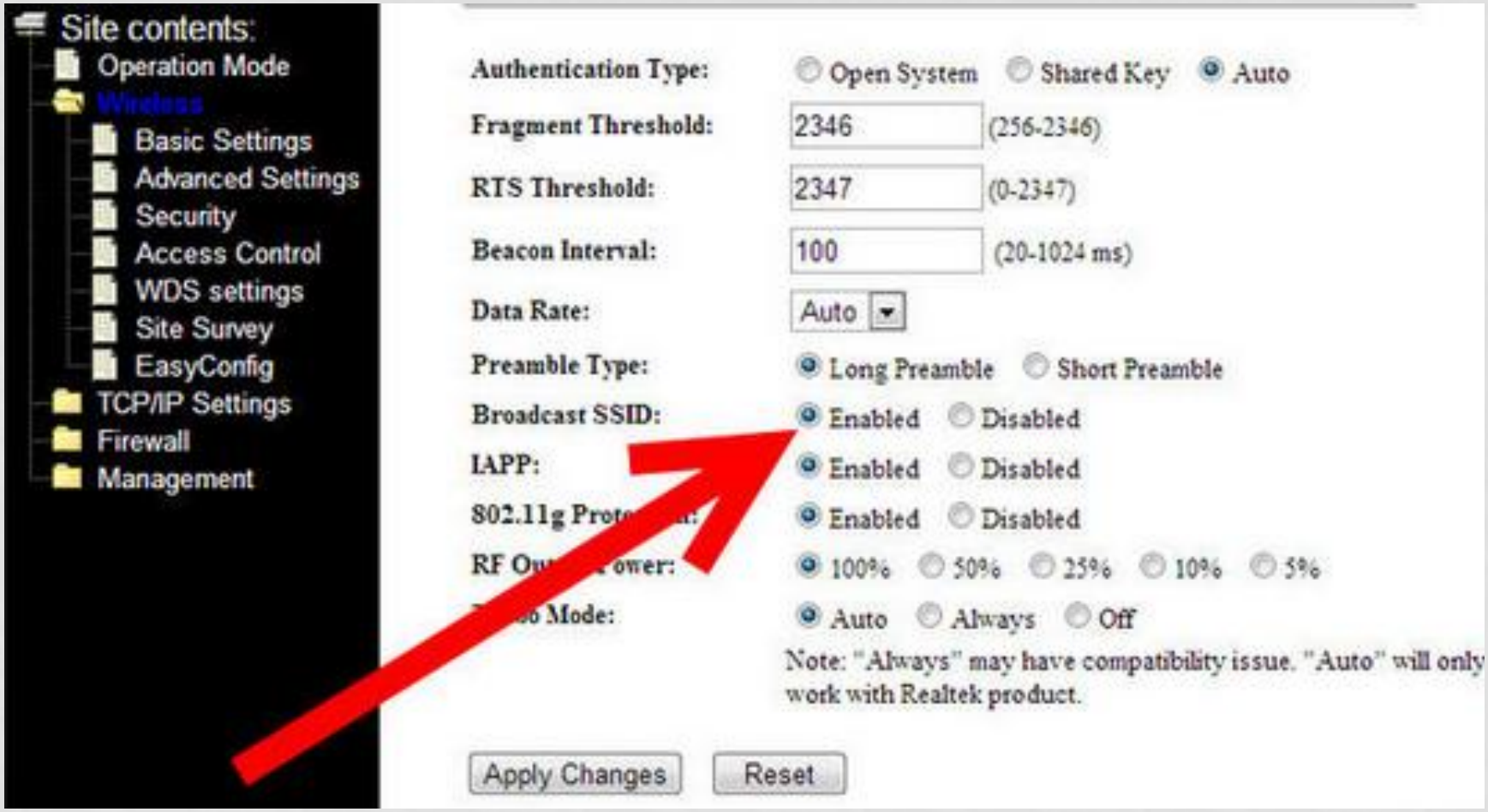




KONFIGURIMI I WIRELESS ROUTER



KONFIGURIMI I WIRELESS ROUTER

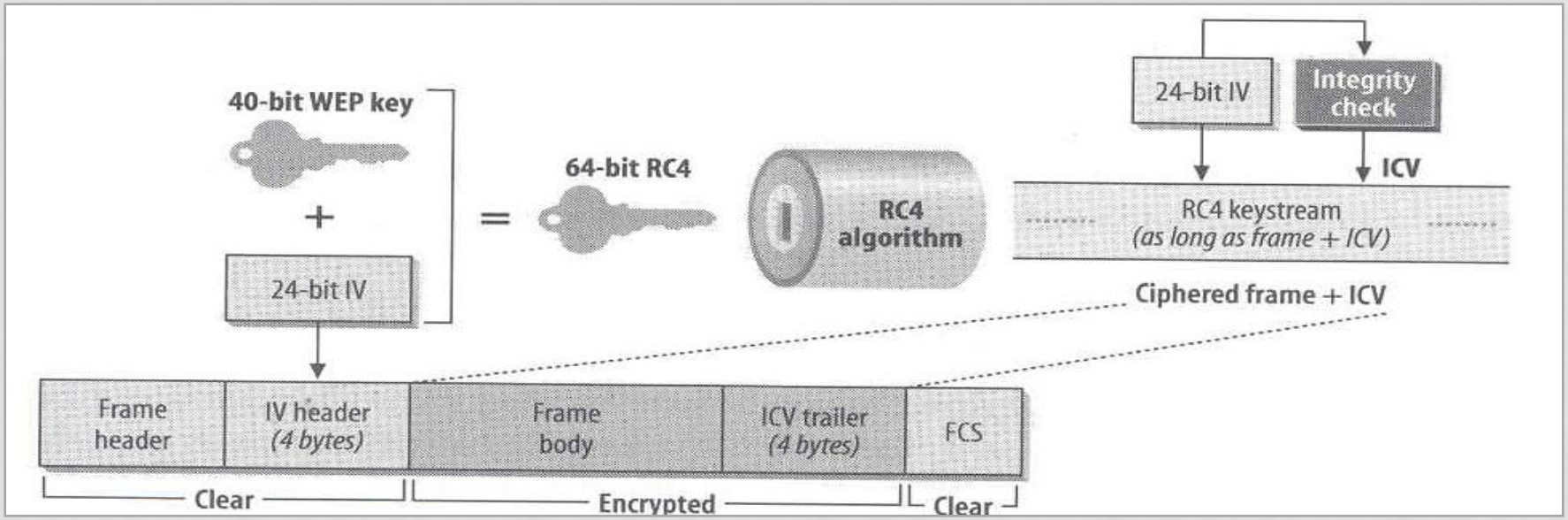


KONFIGURIMI I WIRELESS ROUTER

KONFIGURIMI I WIRELESS ROUTER

KONFIGURIMI I WIRELESS ROUTER

SFONDI KRIPTOGRAFIKE WEP



•Qëllimi i një IV, i cili transmetohet si plain text, është që të parandalojë përsëritjet, por një IV 24 bit nuk është i gjatë mjafteshëm për ta siguruar këtë në një rrjet të ngarkuar

•Për një IV 24 bit, ka 50% mundësi që e njëjta IV të përsëritet pas 5000 paketash

KARAKTERISTIKAT E WEP

- Qëllimi kryesor i standartit WEP ishte ti bënte rrjetat wireless po aq të sigurt sa rrjetat me tela.
- Çelësat e sigrisë që përdoren aktalisht nga WEP janë 128 dhe 256 bit.
- WEP përdor shifrat
- RC4 për sigurimin e konfidencialitetit dhe metoden checksum CRC-32 për integritetin
- Standarti WEP 64 bit përdor një çelës 40 bit, i cili është i lidhur me një vektor inicializues 24 bit (IV) për të formar çelësin e trafikut RC4

STANDARTI WPA (WI – FI PROTECTED ACCESS)

Për tu dhënë zgjidhje këtyre problemeve, WPA përdor dy protokolle të standartit 802.11i.

Temporal Key Integrity Protocol (TKIP)
Ky protokoll u dha zgjidhje problemeve në lidhje me enkriptimin dhe integritetin e frame-it në WEP. Protokolli TKIP përdor algoritmin fillestar të enkriptimit RC4 por i shton një funksion i cili krijon një çelës për çdo frame, për të shmangur sulmet ndaj çelësave të dobët në WEP

802.1x Port Based Authentication
Ky protokoll ishte dizenjuar për të siguruar një framework i cili lejon pajisjet e lidhura në një rrjet që fillimisht të autentikohen para se tu jepet e drejta e aksesit.

FALEMNDERIT

Pyetje?