Contents

CAPITOLUL 4. SECURE DEVICE ACCESS

4.0 Introduction

4.0.1 - Scope

Securizarea accesului la dispozitiv este o sarcină critică pentru un profesionist în securitatea rețelei.

- *Cui ar trebui să i se permită accesul ?*
- *Cum se securizeaza routerul edge ?*
- *Ce pași trebuie facuti pentru a configura accesul administrativ securizat ?*
- *Cum se poate configura securitatea îmbunătățită pentru autentificarea virtuală ?*

4.0.2- Obiective

Configurarea accesului administrativ securizat.

Secure the Edge Router – Explicarea modului pentru securizarea unui perimetru de rețea.

Configure Secure Administrative Access - Utilizarea comenzilor corecte pentru a configura parolele pe un dispozitiv Cisco IOS.

Configure Enhanced Security for Virtual Logins - Utilizarea comenzilor corecte pentru a configura securitatea îmbunătățită pentru autentificarea virtuală.

Configure SSH - Configurarea unui daemon SSH pentru gestionarea securizată de la distanță.

4.1 Secure the Edge Router

4.1.1 - Secure the Network Infrastructure

Securizarea infrastructurii de rețea este esențială pentru securitatea generală a rețelei. Infrastructura de rețea include routere, comutatoare, servere, puncte finale și alte dispozitive.

Daca luam în considerare un angajat nemulțumit care se uită cu ochiul peste umărul unui administrator de rețea în timp ce administratorul se conectează la un router edge, putem spune ca este o modalitate surprinzător de ușoară pentru un atacator de a obține acces neautorizat.

Dacă un atacator obține acces la un router, securitatea și gestionarea întregii rețele pot fi compromise. De exemplu, un atacator poate șterge configurația de pornire și face ca routerul să se reîncarce în cinci minute. Când routerul repornește, nu va avea o configurație de pornire.

Pentru a preveni accesul neautorizat la toate dispozitivele de infrastructură, trebuie implementate politici și controale de securitate adecvate. Routerele sunt o țintă principală

pentru atacuri, deoarece aceste dispozitive acționează ca poliție rutieră, care direcționează traficul în, din și între rețele.

Routerul de margine prezentat în figură este ultimul router dintre rețeaua internă și o rețea de neîncredere, cum ar fi internetul. Tot traficul de internet al unei organizații trece printr-un router de margine, care funcționează adesea ca prima și ultima linie de apărare pentru o rețea. Routerul edge ajută la securizarea perimetrului unei rețele protejate și implementează acțiuni de securitate care se bazează pe politicile de securitate ale organizației. Din aceste motive, securizarea routerelor de rețea este imperativă.

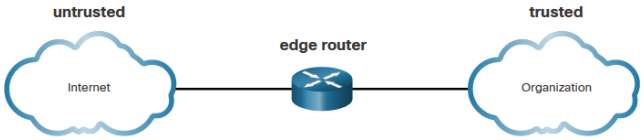

Fig. 4.1. Router de granita.
Figura arată routerul de margine între rețeaua internă și o rețea de neîncredere.

4.1.2 - Edge Router Security Approaches

Implementarea routerului edge variază în funcție de dimensiunea organizației și de complexitatea designului de rețea necesar. Implementările de router pot include un singur router care protejează o întreagă rețea internă sau un router care funcționează ca prima linie de apărare într-o abordare de apărare în profunzime. Topologiile simplificate pentru cele trei abordări sunt prezentate în figură.

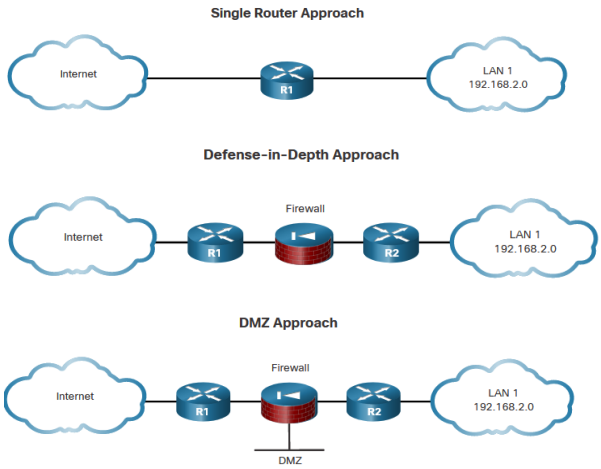

Fig. 4.2 Cele trei tipuri de topologii bazate pe aparare.

Abordare cu un singur router - Single Router Approach - În figură, un singur router conectează rețeaua protejată sau rețeaua locală internă (LAN) la internet. Toate politicile de

securitate sunt configurate pe acest dispozitiv. Acest lucru este mai frecvent implementat în implementări de siteuri mai mici, cum ar fi site-urile de sucursale și birouri mici, birouri de acasă (SOHO). În rețelele mai mici, caracteristicile de securitate necesare pot fi susținute de ruterele de servicii integrate (ISR) fără a împiedica capabilitățile de performanță ale routerului.

Abordare de apărare în profunzime - Defense-in-Depth Approach - O abordare de apărare în profunzime este mai sigură decât abordarea cu un singur router. Utilizează mai multe niveluri de securitate înainte ca traficul să intre în LAN protejat. Există trei niveluri primare de apărare: routerul edge, firewall-ul și un router intern care se conectează la LAN protejat. Routerul de margine acționează ca prima linie de apărare și este cunoscut sub numele de router de screening. După ce a efectuat filtrarea inițială a traficului, routerul de margine trece toate conexiunile care sunt destinate rețelei LAN interne către a doua linie de apărare, care este firewall-ul.

Firewall-ul reia de obicei de unde se oprește routerul de margine și efectuează filtrare suplimentară. Oferă control suplimentar al accesului prin urmărirea stării conexiunilor și acționează ca un dispozitiv de control. Implicit, firewall-ul interzice inițierea conexiunilor din rețelele exterioare (neîncredere) la rețeaua interioară (de încredere). Cu toate acestea, permite utilizatorilor interni să stabilească conexiuni la rețelele care nu sunt de încredere și permite răspunsurilor să revină prin firewall. De asemenea, poate efectua autentificarea utilizatorului (proxy de autentificare) în care utilizatorii trebuie să fie autentificați pentru a obține acces la resursele rețelei.

Routerele nu sunt singurele dispozitive care pot fi utilizate într-o abordare de apărare în profunzime. Pot fi implementate și alte instrumente de securitate, cum ar fi sistemele de prevenire a intruziunilor (IPS), dispozitivele de securitate web (servere proxy) și dispozitivele de securitate pentru e-mail (filtrarea spamului).

Abordarea DMZ - DMZ Approach - O variație a abordării apărării în profunzime este prezentată în figură. Această abordare include o zonă intermediară, adesea numită zonă demilitarizată (DMZ). DMZ poate fi folosit pentru servere care trebuie să fie accesibile de pe internet sau din altă rețea externă. DMZ poate fi configurat între două routere, cu un router intern care se conectează la rețeaua protejată și un router extern care se conectează la rețeaua neprotejată. Alternativ, DMZ poate fi pur și simplu un port suplimentar de pe un singur router. Firewall-ul este situat între rețelele protejate și cele neprotejate. Firewall-ul este configurat

pentru a permite conexiunile necesare, cum ar fi HTTP, din rețelele exterioare (neîncredere) la serverele publice din DMZ. Firewall-ul servește drept protecție principală pentru toate dispozitivele din DMZ.

4.1.3 - Three Areas of Router Security

Securizarea routerului edge este un prim pas critic în securizarea rețelei. Dacă există și alte routere interne, acestea trebuie să fie configurate în siguranță. Trei zone de securitate a routerului trebuie menținute.

1. ***Siguranță fizică - Physical Security -*** Asigurarea securitatii fizice pentru routere:

- *Așezarea routerului și dispozitivele fizice care se conectează la acesta într-o cameră încuiată securizată, care este accesibilă numai personalului autorizat, nu are interferențe electrostatice sau magnetice, are mechanism de stingere a incendiilor și are control pentru temperatură și umiditate.*
- *Instalarea unei surse de alimentare neîntreruptibilă (UPS) sau un generator de energie de rezervă diesel. Utilizarea surselor de alimentare redundante în dispozitivele de rețea, dacă este posibil. Acest lucru reduce posibilitatea unei întreruperi de rețea din cauza pierderii de energie sau a echipamentelor de alimentare defectuoase.*

2. ***Securitatea sistemului de operare - Operating System Security -*** Există câteva proceduri implicate în securizarea caracteristicilor și performanței sistemelor de operare a routerului:

Echiparea routerelor cu cantitatea maximă de memorie posibilă. Disponibilitatea memoriei poate ajuta la atenuarea riscurilor pentru rețea de la unele atacuri de tip denial of service (DoS), susținând în același timp cea mai largă gamă de servicii de securitate.

Utilizarea celei mai recente versiuni (stabilă) a sistemului de operare care îndeplinește specificațiile caracteristicilor routerului sau dispozitivului de rețea. Caracteristicile de securitate și criptare dintr-un sistem de operare sunt îmbunătățite și actualizate în timp, ceea ce face esențială să fie instalata cea mai actualizată versiune.

Păstrarea unei o copii sigure a imaginilor sistemului de operare a routerului și a fișierelor de configurare a routerului ca copii de rezervă.

3. ***Întărirea routerului - Router Hardening*** - Eliminarea potențialului abuz al porturilor și serviciilor neutilizate:

Control administrativ sigur. Asigurarea faptului că numai personalul autorizat are acces și că nivelul lor de acces este controlat.

Dezactivarea porturilor și interfețelor neutilizate. Reducerea numărului de moduri în care un dispozitiv poate fi accesat.

Dezactivarea serviciilor inutile. Similar multor computere, un router are servicii care sunt activate implicit. Unele dintre aceste servicii sunt inutile și pot fi folosite de un atacator pentru a aduna informații despre router și rețea. Aceste informații pot fi apoi utilizate într-un atac de exploatare.

4.1.4 - Secure Administrative Access

Securizarea accesului administrativ este o sarcină de securitate extrem de importantă. Dacă o persoană neautorizată obține acces administrativ la un router, acea persoană poate modifica parametrii de rutare, poate dezactiva funcțiile de rutare sau poate descoperi și obține acces la alte sisteme din rețea.

Mai multe sarcini importante sunt implicate în securizarea accesului administrativ la un dispozitiv de infrastructură:

- *Restricționarea accesibilitatii dispozitivului* – Limitarea numarului de porturi accesibile, restricționarea comunicatorilor permisi și restricționarea metodelor de acces permise.
- *Înregistrarea și conectari pentru tot accesul* – Sa se înregistreze pe oricine accesează un dispozitiv, ce s-a întâmplat în timpul accesului și când a avut loc accesul în scopuri de audit.
- *Acces autentificat* – Asigurarea faptului că accesul este acordat numai utilizatorilor, grupurilor și serviciilor autentificate. Limitarea numărului de încercări eșuate de conectare și timpul permis între conectări.
- *Autorizarea acțiunilor* - Restricționarea acțiunilor și vizualizărilor permise de un anumit utilizator, grup sau serviciu.
- *Prezentarea notificarilor legale* – Afișarea unei notificari legale, care ar trebui dezvoltată împreună cu consilierul juridic al companiei, pentru diferite tipuri de acces la dispozitiv.
- *Asigurarea confidențialitatii da*telor - Protejarea datele stocate local și sensibile de a fi vizualizate și copiate. Luarea în considerare a vulnerabilitatii datelor în tranzit

printr-un canal de comunicație la atacurile de tip sniffing, deturnarea sesiunii și atacurile „man-in-the-middle” (MITM).

4.1.5 - Secure Local and Remote Access

Un router poate fi accesat în scopuri administrative local sau de la distanță:

1. ***Acces local -*** Toate dispozitivele de infrastructură de rețea pot fi accesate local. Accesul local la un router necesită de obicei o conexiune directă la un port de consolă de pe routerul Cisco și utilizarea unui computer care rulează software de emulare a terminalului, așa cum se arată în figură. Administratorul trebuie să aibă acces fizic la router și să folosească un cablu de consolă pentru a se conecta la portul de consolă. Accesul local este de obicei utilizat pentru configurarea inițială a dispozitivului.

Fig. 4.3. Access Local.

2. ***Acces de la distanță*** - Administratorii pot accesa și dispozitivele de infrastructură de la distanță, așa cum se arată în figură. Deși opțiunea de port aux este disponibilă, cea mai comună metodă de acces la distanță implică permiterea conexiunilor Telnet, SSH, HTTP, HTTPS sau SNMP la router de pe un computer. Computerul poate fi în rețeaua locală sau la distanță. Cu toate acestea, dacă conexiunea la rețea la dispozitiv este întreruptă, singura modalitate de a o accesa ar putea fi prin linii telefonice.

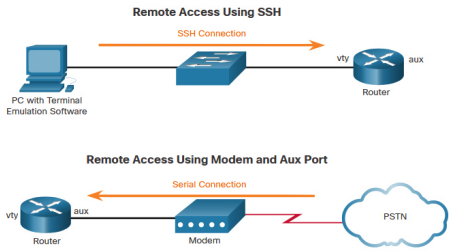

Fig. 4.4. Access de la distanta.

Figura arată metoda de acces de la distanță folosind metoda SSH și accesul de la distanță folosind metoda modemului și portului auxiliar folosind o conexiune serială prin linii telefonice.

Unele protocoale de acces la distanță trimit date, inclusiv nume de utilizator și parole, către router în text simplu. Dacă un atacator poate colecta trafic de rețea în timp ce un administrator se conectează de la distanță la un router, atacatorul poate captura parole sau informații de

configurare a routerului. Din acest motiv, este de preferat să se permita doar accesul local la router. Cu toate acestea, în unele situații, accesul de la distanță poate fi în continuare necesar. Trebuie luate măsuri de precauție atunci când se permite accesul rețelei de la distanță:

- *Criptarea intergului trafic dintre computerul administratorului și router. De exemplu, în loc să fie utilizat Telnet, se utilizeaza SSH versiunea 2; sau în loc să se utilizeze HTTP, se poate folosi HTTPS.*
- *Stabilirea unei rețele de management dedicată. Rețeaua de management ar trebui să includă doar gazde de administrare identificate și conexiuni la o interfață dedicată pe router. Accesul la această rețea poate fi strict controlat.*
- *Configurarea unui filtru de pachete pentru a permite doar gazdelor de administrare identificate și protocoalelor preferate să acceseze routerul. De exemplu, permiterea numai a cererilor SSH de la adresa IP a unei gazde de administrare care să inițieze o conexiune la routerele din rețea.*
- *Configurarea și stabilirea unei conexiuni VPN la rețeaua locală înainte de conectarea la o interfață de gestionare a routerului.*

Aceste măsuri de precauție sunt valoroase, dar nu protejează complet rețeaua. Trebuie implementate și alte metode de apărare. Una dintre cele mai de bază și importante metode este utilizarea parolelor securizate.

4.2 Configure Secure Administrative Access

4.2.1 - Passwords

Pentru a proteja dispozitivele din rețea, este important să fie folosite parole puternice. Iată liniile directoare standard de urmat:

Utilizarea unei lungimi a parolei de cel puțin opt caractere, de preferință 10 sau mai multe caractere. O parolă mai lungă este o parolă mai sigură.

Crearea de parolele complexe. Includere unui amestec de litere mari și mici, numere, simboluri și spații, dacă este permis.

Evitarea parolelor bazate pe repetare, cuvinte uzuale din dicționar, secvențe de litere sau numere, nume de utilizator, nume de rude sau animale de companie, informații biografice, cum ar fi datele de naștere, numerele de identificare, numele strămoșilor sau alte informații ușor de identificat.

Scrierea greșita în mod deliberat a parolei. De exemplu, Smith = Smyth = 5mYth sau Security = 5ecur1ty.

Schimbarea frecventa a parolelor. Dacă o parolă este compromisă fără să se știe, fereastra de oportunitate pentru ca actorul amenințării să utilizeze parola este limitată.

A nu se nota parolele și a nu se lăsa în locuri vizibile, cum ar fi pe birou sau pe monitor.

Tabelele prezintă exemple de parole puternice și slabe.

Weak Password	**Why it is Weak**
secret	Parolă simplă de dicționar
smith	Numele de fată al mamei
toyota	Numele masinii
bob1967	Numele și ziua de naștere a utilizatorului
Blueleaf23	Cuvinte și numere simple
Strong Password	**Why it is Strong**
b67n42d39c	Combină caractere alfanumerice
12^h u4@1p7	Combină caractere alfanumerice, simboluri și include un spațiu

Pe routerele Cisco, spațiile de început sunt ignorate pentru parole, dar spațiile de după primul caracter nu sunt. Prin urmare, o metodă de a crea o parolă puternică este să fie utilizata bara de spațiu și să se creeze o expresie formată din mai multe cuvinte. Aceasta se numește expresie de acces. O expresie de acces este adesea mai ușor de reținut decât o simplă parolă. De asemenea, este mai lunga și mai greu de ghicit.

Managerii de parole - Utilizarea unui manager de parole pentru a securiza parolele pentru activitatea online pe internet. Considerat a fi cea mai bună practică pentru a securiza parolele, managerul de parole generează automat parole complexe pentru utilizator și le va introduce automat când sunt accesate acele site-uri. Trebuie doar să se introduca o parolă principală pentru a activa această funcție.

Autentificare cu mai mulți factori - Utilizarea autentificarii cu mai mulți factori atunci când este disponibilă. Aceasta înseamnă că autentificarea necesită două sau mai multe mijloace independente de verificare. De exemplu, atunci când este introdusa o parolă, ar trebui să se introduca și un cod care poate fi trimis prin e-mail sau mesaj text.

4.2.2 - Configure Passwords

Când se face conectarea inițiala la un dispozitiv, se realizeaza în modul EXEC utilizator. Acest mod este securizat folosind consola.

Pentru a asigura accesul utilizatorului în modul EXEC, se intra în modul de configurare a consolei de linie folosind comanda de configurare globală a consolei de linie 0, așa cum se arată în secventa de cod de mai jos. Zero este folosit pentru a reprezenta prima (și în cele mai multe cazuri singura) interfață de consolă. Apoi, se specifica parola modului EXEC utilizator utilizând comanda parolă. În cele din urmă, se activeaza accesul EXEC utilizator folosind comanda de conectare.

```
Sw-FMI-1# configure terminal
Sw-FMI-1(config)# line console 0
Sw-FMI-1(config-line)# password cisco
Sw-FMI-1(config-line)# login
Sw-FMI-1(config-line)# end
```

Accesul la consolă va necesita acum o parolă înainte de a permite accesul la modul EXEC utilizator. Pentru a avea acces de administrator la toate comenzile IOS, inclusiv configurarea unui dispozitiv, trebuie să se obțina acces privilegiat în modul EXEC. Este cea mai importantă metodă de acces deoarece oferă acces complet la dispozitiv.

Pentru a asigura accesul EXEC privilegiat, se utilizaeazacomanda enable secret password global config, așa cum se arată în exemplu.

```
Sw-FMI-1# configure terminal
Sw-FMI-1(config)# enable secret class
Sw-FMI-1(config)# exit
```

Liniile de terminale virtuale (VTY) permit accesul de la distanță utilizând serviciile Telnet sau SSH la dispozitiv. Multe switch-uri Cisco acceptă până la 16 linii VTY care sunt numerotate de la 0 la 15. Cele mai multe routere acceptă 5 linii VTY cu numerele de la 0 la 4. În exemplu, este configurat un comutator de nivel de acces.

Pentru a securiza liniile VTY, se intra în modul linie VTY utilizând comanda line vty 0 15 din global config. Apoi, se specifica parola VTY utilizând comanda parolă ***parolă***. În sfârșit, se activeaza accesul VTY utilizând comanda de conectare.

Este prezentat un exemplu de securizare a liniilor VTY pe un comutator.

```
Sw-FMI-1# configure terminal
Sw-FMI-1(config)# line vty 0 15
Sw-FMI-1(config-line)# password cisco
Sw-FMI-1(config-line)# login
Sw-FMI-1(config-line)# end
Sw-FMI-1#
```

4.2.3 - Encrypt Passwords

Parolele puternice sunt utile doar dacă sunt secrete. Există mai mulți pași care pot fi luați pentru a asigura faptul că parolele rămân secrete pe un router și un comutator Cisco, inclusiv aceștia:

- *Criptarea tuturor parolelor text simplu*
- *Setarea unei lungimi minime acceptabile a parolei*
- *Descurajarea atacurilor de ghicire a parolelor cu forță brută*
- *Dezactivarea unui acces inactiv în modul EXEC privilegiat după o anumită perioadă de timp.*

Fișierele startup-config și running-config afișează majoritatea parolelor în text simplu. Aceasta este o amenințare de securitate deoarece oricine poate descoperi parolele dacă are acces la aceste fișiere.

Pentru a cripta toate parolele text simplu, se utilizeaza comanda ***service password-encryption*** din global config, așa cum se arată în exemplu.

```
Sw-FMI-1# configure terminal
Sw-FMI-1(config)# service password-encryption
Sw-FMI-1(config)#
```

Comanda aplică o criptare slabă tuturor parolelor necriptate. Această criptare se aplică numai parolelor din fișierul de configurare. Scopul acestei comenzi este de a împiedica persoanele neautorizate să vadă parolele în fișierul de configurare.

Se utilizeaza comanda ***show running-config*** pentru a verifica dacă parolele sunt criptate.

```
Sw-FMI-1(config)# end
Sw-FMI-1# show running-config
!
(Output omitted)
!
line con 0
password 7 094F471A1A0A
login
!
line vty 0 4
 password 7 094F471A1A0A
 login
line vty 5 15
 password 7 094F471A1A0A
 login
!
!
End
```

4.2.4 - Additional Password Security

După cum se arată în configurația din exemplu, comanda de configurare globală a serviciului de criptare a parolei împiedică persoanele neautorizate să vadă parolele cu text simplu în fișierul de configurare. Această comandă criptează toate parolele text simplu. Se poate observa în exemplu că parola „cisco” a fost criptată ca „094F471A1A0A”.

Pentru a asigura faptul că toate parolele configurate au o lungime minimă specificată, se utilizeaza comanda ***security passwords min-length length*** în modul de configurare globală, doar pe router, pe switch nu poate fi configurata.

Actorii amenințărilor pot folosi software de spargere a parolelor pentru a efectua un atac cu forță brută asupra unui dispozitiv de rețea. Acest atac încearcă continuu să ghicească parolele valide până când una funcționează. Utilizarea comenzii de configurare globală a blocului de conectare pentru numărul de încercări în câteva secunde pentru a descuraja acest tip de atac.

Administratorii de rețea pot deveni distrași și pot lăsa accidental deschisă o sesiune privilegiată în mod EXEC pe un terminal. Acest lucru ar putea permite unui actor intern de amenințare să modifice sau să șteargă configurația dispozitivului. În mod implicit, routerele Cisco vor deconecta o sesiune EXEC după 10 minute de inactivitate. Cu toate acestea, se poate reduce această setare folosind comanda de configurare a liniei exec-timeout minute secunde. Această comandă poate fi aplicată în consolă online, linii auxiliare și vty.

De exemplu, următoarele comenzi configurează:

Toate parolele text simplu sunt criptate.

Noile parole configurate trebuie să aibă opt caractere sau mai mult.

Dacă există mai mult de trei încercări eșuate de conectare la VTY în 60 de secunde, atunci se blocheaza liniile VTY timp de 120 de secunde.

Setarea routerului ca să deconecteze automat un utilizator inactiv pe o linie VTY dacă linia a fost inactivă timp de 5 minute și 30 de secunde.

```
R1-FMI(config)# service password-encryption
R1-FMI(config)# security passwords min-length 8
R1-FMI(config)# login block-for 120 attempts 3 within 60
R1-FMI(config)# line vty 0 4
R1-FMI(config-line)# password cisco123
R1-FMI(config-line)# exec-timeout 5 30
R1-FMI(config-line)# transport input ssh
R1-FMI(config-line)# end
R1-FMI#
R1-FMI# show running-config | section line vty
line vty 0 4
```

```
 password 7 094F471A1A0A
 exec-timeout 5 30
 login
 transport input ssh
R1-FMI#
```

4.2.5 - Secret Password Algorithms

Hash-urile MD5 nu mai sunt considerate sigure, deoarece atacatorii pot reconstrui certificate valide. Acest lucru poate permite atacatorilor să falsifice orice site web. Comanda de activare a parolei secrete prezentată în figură utilizează un hash MD5 în mod implicit. Prin urmare, acum este recomandat să fie configurate toate parolele secrete folosind fie parole de tip 8, fie de tip 9. Tipul 8 și tipul 9 au fost introduse în Cisco IOS 15.3(3)M. Tipul 8 și tipul 9 folosesc criptarea SHA. Deoarece tipul 9 este puțin mai puternic decât tipul 8, acesta va fi folosit pe tot parcursul acestui curs ori de câte ori este permis de Cisco IOS.

```
R1-FMI(config)# enable secret cisco12345
R1-FMI(config)# do show run | include enable
enable secret 5 $1$cam7$99EfzkvmJ5h1gEbryLVRy.
R1-FMI(config)# enable secret ?
  0      Specifies an UNENCRYPTED password will follow
  5      Specifies a MD5 HASHED secret will follow
  8      Specifies a PBKDF2 HASHED secret will follow
  9      Specifies a SCRYPT HASHED secret will follow
  LINE   The UNENCRYPTED (cleartext) 'enable' secret
  level  Set exec level password

R1-FMI(config)# line con 0
R1-FMI(config-line)# password ?
  0     Specifies an UNENCRYPTED password will follow
  7     Specifies a HIDDEN password will follow
  LINE  The UNENCRYPTED (cleartext) line password
R1-FMI(config-line)#
```

Figura arată că pentru configurarea criptării de tip 9 nu este atât de ușoară pe cât pare. Nu se poate introduce pur și simplu enable secret 9 și parola necriptată. Pentru a utiliza această formă a comenzii, trebuie să lipeasca parola criptată, care poate fi copiată dintr-o altă configurație de router.

```
R1-FMI(config)# enable secret 9 cisco12345
ERROR: The secret you entered is not a valid encrypted secret.
To enter an UNENCRYPTED secret, do not specify type 9 encryption.
When you properly enter an UNENCRYPTED secret, it will be encrypted.
R1-FMI(config)# enable secret 9
$9$HZWdzLHwhPtZ3U$D9OlUDSGvBy.m8Tf9vCGDJRcYy8zIMbyRJgtxgRkwzY
R1-FMI(config)#
```

Pentru a introduce o parolă necriptată, se utilizeaza sintaxa comenzii de tip algoritm de activare:

Algorithm Keyword	Descriere
md5	Tip 5; selectează algoritmul de tip digest mesaj 5 (MD5) ca algoritm de hashing.
scrypt	Tip 9; selectează scrypt ca algoritm de hashing.
sha256	Tip 8; selectează Funcția 2 de derivare a cheilor bazată pe parolă (PBKDF2) cu algoritm de hașare securizat, 256 de biți (SHA-256) ca algoritm de hashing.

Un exemplu de configurație este prezentat în figură. Se poate observa că acest tip de configurație de rulare arată acum o parolă secretă de activare de tip 9.

```
R1-FMI(config)# enable algorithm-type ?
  md5     Encode the password using the MD5 algorithm
  scrypt  Encode the password using the SCRYPT hashing algorithm
  sha256  Encode the password using the PBKDF2 hashing algorithm
R1-FMI(config)# enable algorithm-type scrypt ?
secret  Assign the privileged level secret (MAX of 25 characters)

R1-FMI(config)# enable algorithm-type scrypt secret cisco12345
R1-FMI(config)# do show run | include enable
enable secret 9 $9$Gyk9x3Ve4c0n5k$8.cR3yReBduzHymEyCOcErgPKW8MSKokRN
9KjEg4WQA
R1-FMI(config)#
```

Criptarea tip 8 și tip 9 a fost, de asemenea, introdusă în Cisco IOS 15.3(3)M pentru comanda secretă a numelui de utilizator. Similar cu comanda enable secret, dacă pur și simplu se introduce un utilizator cu comanda secret username, criptarea implicită va fi MD5. Se utilizeaza comanda nume de utilizator algorithm-type pentru a specifica criptarea de tip 9. Sintaxa este prezentată urmată de un exemplu.

```
R1-FMI(config)# username Bob secret cisco54321
R1-FMI(config)# do show run | include username
username Bob privilege 15 secret 5 $1$lmBB$UjOC6JA4f1WgI3/La8wGz/
R1-FMI(config)#
R1-FMI(config)# username Bob algorithm-type scrypt secret cisco54321
R1-FMI(config)# do show run | include username
username Bob privilege 15 secret 9 $9$9FkS.zTuLs89pk$v5P2y.M6reR18lS
92moKHdFauk8joK0xHICXxGDuurs
R1-FMI(config)#
```

Din motive de compatibilitate inversă, comenzile de activare a parolei, a numelui de utilizator și a parolei de linie sunt disponibile în Cisco IOS. Aceste comenzi nu folosesc criptare în mod implicit. În cel mai bun caz, pot folosi doar criptarea de tip 7, așa cum se arată în figură.

```
R1-FMI(config)# enable password ?
  0      Specifies an UNENCRYPTED password will follow
  7      Specifies a HIDDEN password will follow
  LINE   The UNENCRYPTED (cleartext) 'enable' password
```

```
  level  Set exec level password

R1-FMI(config)# username Bob password ?
  0     Specifies an UNENCRYPTED password will follow
  7     Specifies a HIDDEN password will follow
  LINE  The UNENCRYPTED (cleartext) user password

R1-FMI(config)# line con 0
R1-FMI(config-line)# password ?
  0     Specifies an UNENCRYPTED password will follow
  7     Specifies a HIDDEN password will follow
  LINE  The UNENCRYPTED (cleartext) line password
```

4.3 Configure Enhanced Security for Virtual Logins

4.3.1 - Enhance the Login Process

Atribuirea parolelor și autentificarea locală nu împiedică un dispozitiv să fie vizat pentru atac. Îmbunătățirile de conectare oferite de Cisco IOS oferă mai multă securitate prin încetinirea atacurilor, cum ar fi atacurile de dicționar și atacurile DoS. Activarea unui profil de detectare permite configurarea unui dispozitiv de rețea care să reacționeze la încercările de conectare eșuate repetate, refuzând solicitările de conectare ulterioare (sau blocarea autentificarii). Acest bloc poate fi configurat pentru o perioadă de timp, care se numește o perioadă de liniște. Listele de control al accesului (ACL) pot fi utilizate pentru a permite conexiuni legitime de la adresele administratorilor de sistem cunoscuți.

Bannerele sunt dezactivate în mod implicit și trebuie activate în mod explicit, de aceea se utilizeaza comanda modului de configurare globală ***banner*** pentru a specifica mesajele adecvate.

```
R1-FMI(config)# banner { motd | exec | login } delimiter message delimiter
```

Bannerele protejează organizația din perspectivă legală. Alegerea formulării adecvate pentru a fi plasate în mesajele banner este importantă și ar trebui revizuită de consilierul juridic înainte de a fi plasată pe routerele de rețea. A nu se folosi niciodată cuvântul bun venit sau orice alt salut familiar care ar putea fi interpretat greșit ca o invitație de a utiliza rețeaua. Următorul este un exemplu de banner adecvat.

```
"This equipment is privately owned and access is logged. Disconnect
immediately if you are not an authorized user. Violators will be prosecuted
to the fullest extent of the law."
  User Access Verification:
  Username:
```

4.3.2 - Configure Login Enhancement Features

Secventa de cod de mai jos prezintă un exemplu de configurare. Comanda login block-for poate apăra împotriva atacurilor DoS prin dezactivarea autentificărilor după un anumit număr de încercări eșuate de conectare. Comanda de conectare în modul silențios se mapează la un ACL care identifică gazdele permise. Acest lucru asigură că numai gazdele autorizate pot încerca să se autentifice la router. Comanda de întârziere de conectare specifică un număr de secunde pe care utilizatorul trebuie să le aștepte între încercările de conectare nereușite. Comenzile de conectare cu succes și de conectare eșuate înregistrează încercările de conectare reușite și nereușite.

Aceste îmbunătățiri de conectare nu se aplică conexiunilor la consolă. Când se configureaza cu conexiunile la consolă, se presupune că numai personalul autorizat are acces fizic la dispozitive.

Notă: Aceste îmbunătățiri de conectare pot fi activate numai dacă baza de date locală este utilizată pentru autentificare pentru acces local și de la distanță. Dacă liniile sunt configurate numai pentru autentificarea cu parolă, atunci funcțiile de conectare îmbunătățite nu sunt activate.

```
R1-FMI(config)# login block-for 15 attempts 5 within 60
R1-FMI(config)# ip access-list standard PERMIT-ADMIN
R1-FMI(config-std-nacl)# remark Permit only Administrative hosts
R1-FMI(config-std-nacl)# permit 192.168.10.10
R1-FMI(config-std-nacl)# permit 192.168.11.10
R1-FMI(config-std-nacl)# exit
R1-FMI(config)# login quiet-mode access-class PERMIT-ADMIN
R1-FMI(config)# login delay 10
R1-FMI(config)# login on-success log
R1-FMI(config)# login on-failure log
R1-FMI(config)#
```

4.3.3 - Enable Login Enhancements

Pentru a ajuta un dispozitiv Cisco IOS să ofere detectarea DoS, se poate utiliza comanda login block-for. Toate celelalte funcții de îmbunătățire a autentificării sunt dezactivate până când comanda de blocare pentru autentificare este configurată.

Mai exact, comanda de blocare pentru autentificare monitorizează activitatea dispozitivului de conectare și funcționează în două moduri:

Modul normal - Acesta este cunoscut și sub denumirea de modul ceas. Routerul ține contorizarea numărului de încercări eșuate de conectare într-un interval de timp identificat.

Modul silențios - Acesta este cunoscut și sub denumirea de perioadă de liniște. Dacă numărul de autentificări eșuate depășește pragul configurat, toate încercările de conectare folosind Telnet, SSH și HTTP sunt refuzate pentru perioada specificată în comanda login block-for.

Când modul silențios este activat, toate încercările de conectare, inclusiv accesul administrativ valid, nu sunt permise. Cu toate acestea, pentru a oferi access la gazde critice, cum ar fi accesul la anumite gazde administrative în orice moment, acest comportament poate fi suprascris folosind un ACL. ACL-ul este creat și identificat utilizând comanda ***login quiet-mode access-class***. Doar gazdele identificate în ACL au acces la dispozitiv în modul silențios.

Exemplul din figură arată o configurație care utilizează un ACL numit PERMIT-ADMIN. Gazdele care îndeplinesc condițiile din ACL- PERMIT-ADMIN sunt scutite de modul silențios.

```
R1-FMI(config)# ip access-list standard PERMIT-ADMIN
R1-FMI(config-std-nacl)# remark Permit only Administrative hosts
R1-FMI(config-std-nacl)# permit 192.168.10.10
R1-FMI(config-std-nacl)# permit 192.168.11.10
R1-FMI(config-std-nacl)# exit
R1-FMI(config)# login quiet-mode access-class  PERMIT-ADMIN
```

Când se implementează comanda login block-for, este invocată automat o întârziere de o secundă între încercările de conectare. Pentru a face mai dificil pentru un atacator, timpul de întârziere dintre încercările de conectare poate fi mărit utilizând comanda login delay seconds, așa cum se arată în figură. Comanda introduce o întârziere uniformă între încercările succesive de conectare. Întârzierea are loc pentru toate încercările de conectare, inclusiv încercările eșuate sau reușite. Exemplul configurează o întârziere de trei secunde între încercările succesive de conectare.

Această comandă ajută la atenuarea atacurilor de dicționar. Este o comandă opțională. Dacă nu este setat, o întârziere implicită de o secundă este impusă după configurarea comenzii de blocare pentru autentificare.

Comenzile de blocare pentru autentificare, clasa de acces în modul silențios de conectare și comenzile de întârziere de conectare ajută la blocarea încercărilor de conectare eșuate pentru o perioadă limitată de timp. Cu toate acestea, nu pot împiedica un atacator să încerce din nou. Cum poate un administrator să știe când cineva încearcă să obțină acces la rețea ghicind parola

4.3.4 - Log Failed Attempts

Există trei comenzi care pot fi configurate pentru a ajuta un administrator să detecteze un atac cu parolă, așa cum se arată în figură. Fiecare comandă permite unui dispozitiv să genereze mesaje syslog pentru încercările de conectare eșuate sau reușite.

Primele două comenzi, login on-succes log și login on-failure log, generează mesaje syslog pentru încercările de conectare reușite și nereușite. Numărul de încercări de conectare înainte ca un mesaj de înregistrare să fie generat poate fi specificat utilizând sintaxa [every login], unde valoarea implicită de conectare este 1 încercare. Intervalul valid este de la 1 la 65.535.

```
Router(config)# login on-success log [every login]
Router(config)# login on-failure log [every login]
```

Ca alternativă la comanda login on-failure log, comanda security authentication failure rate poate fi configurată pentru a genera un mesaj de jurnal atunci când rata de eșec de conectare este depășită.

```
Router(config)# security authentication failure rate threshold-rate log
```

Se utilizeaza comanda ***show login*** pentru a verifica blocarea autentificarii pentru setările comenzii și modul curent. În figură, R1-FMI a fost configurat să blocheze gazdele de conectare timp de 120 de secunde dacă mai mult de cinci solicitări de conectare eșuează în 60 de secunde. R1-FMI confirmă, de asemenea, că modul curent este normal și că au existat patru erori de conectare în ultimele 55 de secunde, deoarece au mai rămas cinci secunde în modul normal.

```
R1-FMI# show login
    A login delay for 10 sec is applied.
    Quiet-Mode access list PERMIT-ADMIN is applied.

    Router enabled to watch for login Attacks.
    If more than 5 login failures occur in 60 sec or less,
    login will be disabled for 120 secs.

    Router presently in Normal-Mode.
    Current Watch Window
        Time remaining: 5 seconds.
        Login failures for current window: 4.
    Total login failures:4.
```

Următoarele două figuri arată exemple de ceea ce se întâmplă atunci când pragul de încercare eșuată este depășit.

Fig. 4.5. Încercări de conectare eșuate.

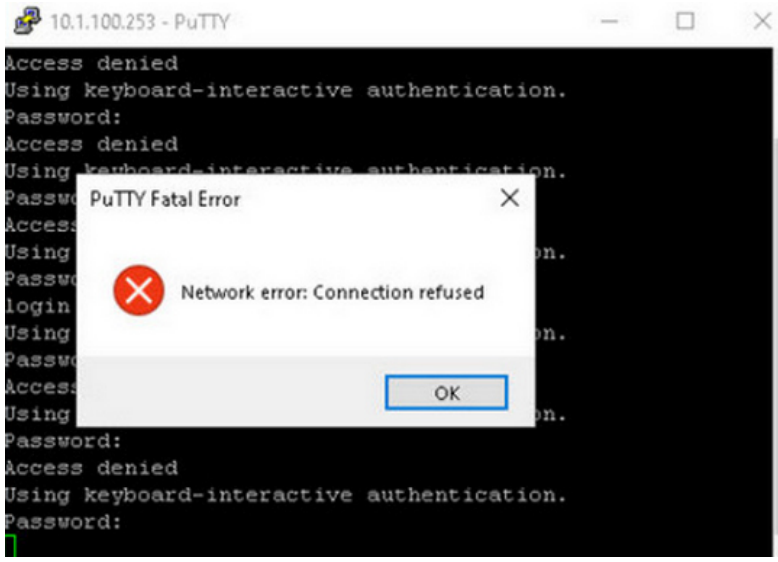

Fig. 4.6. Depășirea pragului de tentativă eșuată.

Următoarea ieșire a comenzii afișează starea rezultată folosind comanda show login. Se poate observa că acum este în modul silențios și va rămâne în modul silențios pentru încă 105 secunde. R1-FMI identifică, de asemenea, că ACL-ul PERMIT-ADMIN conține o listă de gazde permise să se conecteze în modul silențios.

```
  R1-FMI#
  *Dec  10  15:38:54.455:  %SEC_LOGIN-1-QUIET_MODE_ON:  Still  timeleft  for
watching failures
  is 12 secs, [user: admin] [Source: 10.10.10.10] [localport: 23] [Reason:
Login
  Authentication Failed - BadUser] [ACL: PERMIT-ADMIN] at 15:38:54 UTC Wed
Dec 10 2008

  R1-FMI# show login
       A login delay of 3 seconds is applied.
       Quiet-Mode access list PERMIT-ADMIN is applied.
```

```
     Router enabled to watch for login Attacks.
     If more than 5 login failures occur in 60 seconds or
     less,logins will be disabled for 120 seconds.
     Router presently in Quiet-Mode.
Will remain in Quiet-Mode for 105 seconds.
Restricted logins filtered by applied ACL PERMIT-ADMIN.
R1-FMI#
```

Comanda ***show login failures*** afișează informații suplimentare cu privire la încercările eșuate, cum ar fi adresa IP de la care au provenit încercările eșuate de conectare. Figura afișează exemplu de rezultat al comenzii show login failures.

```
R1-FMI# show login failures
Total failed logins: 22
Detailed information about last 50 failures
Username     SourceIPAddr     lPort Count TimeStamp
admin        1.1.2.1          23    5     15:38:54 UTC Wed Dec 10 2008
Admin        10.10.10.10      23    13    15:58:43 UTC Wed Dec 10 2008
admin        10.10.10.10      23    3     15:57:14 UTC Wed Dec 10 2008
cisco        10.10.10.10      23    1     15:57:21 UTC Wed Dec 10 2008
R1-FMI#
```

4.4 Configure SSH

4.4.2 - Enable SSH

Fig. 4.7. Enable SSH

Telnet simplifică accesul la dispozitiv de la distanță, dar nu este sigur. Datele conținute într-un pachet Telnet sunt transmise necriptate. Din acest motiv, este foarte recomandat să fie activat Secure Shell (SSH) pe dispozitive pentru acces securizat de la distanță.

Este posibil să se configureze un dispozitiv Cisco să accepte SSH utilizând următorii șase pași:

Pasul 1. Configurarea unui nume de gazdă unic pentru dispozitiv. Un dispozitiv trebuie să aibă un nume de gazdă unic, altul decât cel implicit.

Pasul 2. Configurarea numelui domeniului IP. Configurarea numelui domeniului IP al rețelei utilizând comanda modului de configurare global ip domain name name. În exemplu, routerul R1 este configurat în domeniul security.com. Această informație este utilizată împreună cu valoarea de bit specificată în comanda de criptare generare rsa general-keys modulus pentru a crea o cheie de criptare

Pasul 3. Generarea unei cheie pentru a cripta traficul SSH. SSH criptează traficul dintre sursă și destinație. Cu toate acestea, pentru a face acest lucru, o cheie de autentificare unică trebuie să fie generată prin utilizarea comenzii de configurare globală crypto key generate rsa general-keys modulus bits. Biții de modul determină dimensiunea cheii și pot fi configurați de la 360 de biți la 2048 de biți. Cu cât valoarea biților este mai mare, cu atât cheia este mai sigură. Cu toate acestea, valorile de biți mai mari durează, de asemenea, mai mult pentru a cripta și decripta informațiile. Lungimea minimă recomandată a modulului este de 1024 de biți.

Pasul 4. Verificarea sau crearea unei intrari locale în baza de date. Se ceeaza o intrare cu nume de utilizator în baza de date locală folosind comanda de configurare globală a numelui de utilizator. În exemplu, parametrul secret este folosit astfel încât parola să fie criptată folosind MD5.

Pasul 5. Autentificarea în baza de date locală. Se poate utilizațcomanda de configurare a liniei locale de conectare pentru a autentifica linia vty în baza de date locală.

Pasul 6. Activarea sesiunilor SSH de intrare vty. În mod implicit, nu este permisă nicio sesiune de intrare pe liniile vty. Se pot specifica mai multe protocoale de intrare, inclusiv Telnet și SSH utilizând intrarea de transport {ssh | comanda telnet}.

```
Router# configure terminal
Router(config)# hostname R1
R1(config)# ip domain name security.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: Rl.security.com % The key modulus size is
1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
R1(config)#
```

Pentru a verifica SSH și a afișa cheile generate, se foloseste comanda ***show crypto key mypubkey rsa*** în modul EXEC privilegiat. Dacă există perechi de chei existente, se recomandă ca acestea să fie suprascrise folosind comanda ***crypto key zeroize rsa***. Dacă există perechi de chei existente, se recomandă să fie eliminate folosind comanda ***cripto key zeroize rsa***. Secventa de cod de mai jos oferă un exemplu de verificare a cheilor criptografice SSH și de eliminare a cheilor vechi.

```
R1# show crypto key mypubkey rsa
% Key pair was generated at: 21:18:41 UTC Feb 16 2015
Key name: R1.security.com
Key type: RSA KEYS
 Storage Device: not specified
 Usage: General Purpose Key
 Key is not exportable.
 Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00CF35DB
  A58A1BDB F7C7E600 F189C2F3 2EC6E584 D923EE5B 71841D98 B5472A03 D19CD620
  ED125825 5A58412B B7F29234 DE2A1809 6C421AC3 07F298E6 80BE149D 2A262E13
  74888DAF CAC8F187 B11111AF A413E76F 6C157CDF DFEF0D82 2961B58C BE1CAD21
  176E82B9 6D81F893 06E66C93 94E1C508 887462F6 90AC63CE 5E169845 C1020301
0001
% Key pair was generated at: 21:18:42 UTC Feb 16 2015
Key name: R1.security.com.server
Key type: RSA KEYS
Temporary key
 Usage: Encryption Key
 Key is not exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00AB914D 8172DFBE
  DE57ACA9 7B844239 1F3B5942 3943AC0D F54E7746 3895CF54 606C3961 8A44FEB3
  1A019F27 D9E71AAE FC73F423 A59CB8F5 50289272 3392CEBC 4C3CBD6D DB9233DE
  9DDD9DAD 79D56165 4293AA62 FD1CBAB2 7AB859DC 2890C795 ED020301 0001
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# crypto key zeroize rsa
% All keys will be removed.
% All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no]: yes
R1(config)#
```

4.4.3 - Enhance SSH Login Security

Pentru a verifica setările opționale ale comenzii SSH, exista comanda ***show ip ssh***, așa cum se arată în figură. De asemenea, se poate modifica intervalul de timeout SSH implicit și numărul de încercări de autentificare. Se utilizeaza comanda ***ip ssh time-out seconds*** global configuration mode pentru a modifica intervalul implicit de timeout de 120 de secunde. Aceasta configurează numărul de secunde pe care SSH le poate folosi pentru a autentifica un

utilizator. După ce este autentificat, începe o sesiune EXEC și se aplică exec-timeout-ul standard configurat pentru vty.

În mod implicit, un utilizator care se conectează are trei încercări de a introduce parola corectă înainte de a fi deconectat. Pentru a configura un număr diferit de reîncercări SSH consecutive, se folosesete comanda ***ip ssh authentication-retries*** integer global configuration mode.

```
R1# show ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Authentication timeout: 120 secs; Authentication retries: 3
(output omitted)

R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip ssh time-out 60
R1(config)# ip ssh authentication-retries 2
R1(config)# ^Z
R1#
*Feb 16 21:23:51.237: %SYS-5-CONFIG_I: Configured from console by console
R1# show ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Authentication timeout: 60 secs; Authentication retries: 2
(output omitted)
```

4.4.4 - Connect a Router to an SSH-Enabled Router

Pentru a verifica starea conexiunilor client, exista comanda ***show ssh.*** Există două moduri diferite de a face conectarea la un router compatibil SSH.

În mod implicit, când SSH este activat, un router Cisco poate acționa ca server SSH sau client SSH. Ca server, un router poate accepta conexiuni client SSH. În calitate de client, un router se poate conecta prin SSH la un alt router compatibil SSH, prezentat în următorii trei pași.

Figura prezintă două routere conectate printr-o legătură serială. De asemenea, fiecare router se conectează la o rețea printr-un port gigabit Ethernet.

Fig. 4.8. SSH de la router la router

În următoarele exemple, administratorul de pe R1 utilizează comanda show ssh pentru a verifica conexiunile SSH curente. Apoi un alt administrator se conectează la R1 de la R2. Administratorul de pe R1 verifică din nou conexiunile SSH curente.

```
R1# show ssh
%No SSHv2 server connections running.
%No SSHv1 server connections running.
R1#
R2# ssh -l Bob 192.168.2.101
Password:
 R1>
R1# show ssh
Connection Version Mode Encryption  Hmac       State               Username
0          2.0     IN   aes128-cbc  hmac-sha1  Session started     Bob
0          2.0     OUT  aes128-cbc  hmac-sha1  Session started     Bob
%No SSHv1 server connections running.
R1#
```

4.4.6 - Connect a Host to an SSH-Enabled Router

Conectarea folosind un client SSH care rulează pe o gazdă, așa cum se arată în următoarele patru figuri. Exemple de acești clienți includ PuTTY, OpenSSH și TeraTerm.

Procedura de conectare la un router Cisco variază în funcție de aplicația client SSH utilizată. În general, clientul SSH inițiază o conexiune SSH la router. Serviciul SSH al routerului solicită combinația corectă de nume de utilizator și parolă. După ce autentificarea este verificată, routerul poate fi gestionat ca și cum administratorul ar folosi o sesiune standard Telnet.

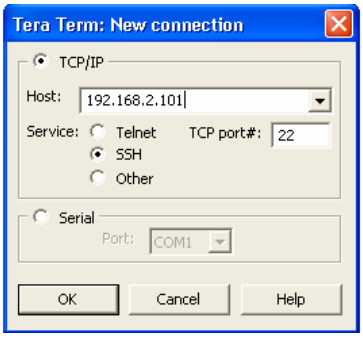

Fig. 4.9.SSH de la gazdă la router

4.5 SUMMARY

Securizați routerul Edge

Routerele sunt o țintă principală pentru atacuri, deoarece aceste dispozitive acționează ca poliție rutieră, care direcționează traficul în, din și între rețele. Routerul edge este ultimul router dintre rețeaua internă și o rețea nede încredere, cum ar fi internetul. Securizarea

routerului este imperativă. Cele trei abordări ale acestui lucru sunt abordarea cu un singur router, abordarea apărării în profunzime și abordarea DMZ. În abordarea cu un singur router, toată securitatea este configurată pe acest router. Acest lucru este comun pentru site-urile mai mici, cum ar fi site-urile SOHO. O abordare de apărare în profunzime este mai sigură decât abordarea cu un singur router. Utilizează mai multe nivele de securitate înainte ca traficul să intre în LAN protejat. Există trei nivele primare de apărare: routerul edge, firewall-ul și un router intern care se conectează la LAN protejat. Pot fi implementate și alte instrumente de securitate, cum ar fi sistemele de prevenire a intruziunilor (IPS), dispozitivele de securitate web (servere proxy) și dispozitivele de securitate pentru e-mail (filtrarea spamului). Abordarea DMZ include o zonă intermediară, adesea numită zonă demilitarizată (DMZ). DMZ poate fi configurat între două routere, cu un router intern care se conectează la rețeaua protejată și un router extern care se conectează la rețeaua neprotejată. Alternativ, DMZ poate fi pur și simplu un port suplimentar de pe un singur router. Firewall-ul servește drept protecție principală pentru toate dispozitivele din DMZ. Cele trei domenii de securitate a routerului care trebuie menținute sunt securitatea fizică, securitatea sistemului de operare și întărirea routerului. Securizarea accesului administrativ pentru a împiedica o persoană neautorizată să obțină acces la un dispozitiv de infrastructură include restricționarea accesibilității dispozitivului, înregistrarea și contabilizarea tuturor accesului, autentificarea accesului, autorizarea acțiunilor, prezentarea notificărilor legale și asigurarea confidențialității datelor. Un router poate fi accesat în scopuri administrative local sau de la distanță. Trebuie luate măsuri de precauție suplimentare atunci când accesați rețeaua de la distanță.

Configurare accesul administrativ securizat

Pentru a proteja dispozitivele din rețea, este important să folosiți parole puternice. Îndrumările standard de urmat sunt folosirea parolelor mai lungi (10 sau mai multe caractere), parole complexe, evitarea cuvintelor comune din dicționar, schimbarea frecventă a parolelor și păstrarea confidențialității parolelor. Parolele și liniile VTY ar trebui să fie securizate. Pentru a cripta toate parolele text simplu, se utilizează comanda service password-encryption global config. Se utilizează comanda show running-config pentru a verifica dacă parolele sunt acum criptate. Comanda de configurare globală a serviciului de criptare a parolei împiedică persoanele neautorizate să vadă parolele cu text simplu în fișierul de configurare. Hashe-urile MD5 nu mai sunt considerate sigure, deoarece atacatorii pot reconstrui certificate valide.

Acum este recomandat să configurați toate parolele secrete folosind fie parole de tip 8, fie de tip 9.

Configurare securitatea îmbunătățită pentru autentificarea virtuală

Îmbunătățirile de conectare Cisco IOS oferă mai multă securitate prin încetinirea atacurilor, cum ar fi atacurile de dicționar și atacurile DoS. Activarea unui profil de detectare vă permite să configurați un dispozitiv de rețea să reacționeze la încercările de conectare eșuate repetate, refuzând solicitările de conectare ulterioare (sau blocarea autentificarii). Acest bloc poate fi configurat pentru o perioadă de timp, care se numește o perioadă de liniște. Listele de control al accesului (ACL) pot fi utilizate pentru a permite conexiunea legitimă de la adresele administratorilor de sistem cunoscuți. Bannerele protejează organizația din perspectivă legală. Comenzile de îmbunătățiri de conectare Cisco IOS cresc securitatea conexiunilor de conectare virtuale. Comanda login block-for se poate apăra împotriva atacurilor DoS prin dezactivarea autentificărilor după un anumit număr de încercări eșuate de conectare. Comanda de conectare în modul silențios se mapează la un ACL care identifică gazdele permise. Acest lucru asigură că numai gazdele autorizate pot încerca să se autentifice la router. Comanda de întârziere de conectare specifică un număr de secunde pe care utilizatorul trebuie să aștepte între încercările de conectare nereușite. Comenzile de conectare la succes și de conectare la eșec înregistrează încercările de conectare reușite și nereușite. Pentru a spori securitatea, puteți modifica, de asemenea, intervalul de timeout SSH implicit și numărul de încercări de autentificare. Se utilizează comanda ip ssh time-out seconds global configuration mode pentru a modifica intervalul implicit de timeout de 120 de secunde. Există două moduri diferite de a vă conecta la un router compatibil SSH. În mod implicit, când SSH este activat, un router Cisco poate acționa ca server SSH sau client SSH. Ca server, un router poate accepta conexiuni client SSH. Ca client, un router se poate conecta prin SSH la un alt router compatibil SSH

Configurare SSH

Telnet simplifică accesul la dispozitiv la distanță, dar nu este sigur. Datele conținute într-un pachet Telnet sunt transmise necriptate. Din acest motiv, este foarte recomandat să activați Secure Shell (SSH) pe dispozitive pentru acces securizat de la distanță.