Uwierzytelnianie w Cisco IOS – hasła lokalne

O tym jak ważne jest zabezpieczenie urządzeń przed dostępem osób nieuprawnionych wie zapewne każdy. Jeżeli weźmiemy pod uwagę urządzenia sieciowe to zagrożenie staje się jeszcze bardziej realne, bo logować możemy się zdalnie, a to w znacznym stopniu zwiększa grono potencjalnych użytkowników. Dlatego pierwsze co powinniśmy zrobić po wypakowaniu urządzenia z pudełka i podłączeniu do sieci to odpowiednio skonfigurować hasła i metody logowania.

W urządzeniach Cisco zarządzanych przez IOS mamy do wyboru autentykację poprzez lokalne hasła zapisane w pamięci urządzenia bądź poprzez serwer z wykorzystaniem Radius'a lub TACACS'a.

Pamiętajcie, że w IOS'ie mamy standardowo dwa tryby dostępu: tryb użytkownika (user mode) i tryb uprzywilejowany(privileged mode). Pierwszy jest mało użyteczny i pozwala na podejrzenie kilku mniej ważnych parametrów urządzenia, drugi natomiast pozwala na nieograniczony dostęp do przeglądania i edytowania. Dodatkowo IOS zapewnia 16 poziomów dostępu – od level 0 do level 15. Odpowiednie poziomy możemy przypisać konkretnym użytkownikom, aby pozwolić lub zabronić dostępu do ważniejszych poleceń systemu.

Aktywując hasło pozwalające na dostęp do urządzenia pierwszym krokiem jest wybranie interfejsu, który chcemy konfigurować.

Konsola Zacznijmy od najbardziej powszechnego i dostępnego w niemal każdym switchu i routerze Cisco czyli portu konsolowego. Wykorzystujemy go podczas pierwszej konfiguracji i w przypadkach gdy straciliśmy dostęp za pośrednictwem innych interfejsów np. przez przypadek wyłączyliśmy port trunk. Ustawienie hasła w tym miejscu uniemożliwi podłączanie się niepowołanym osobom poprzez kabel konsolowy. Chociaż, jeżeli ktoś już ma fizyczny dostęp do urządzenia to może z nim zrobić prawie wszystko.

```
Switch# config t
Switch(config)# line console 0
Switch(config-line)# password Cisco123
Switch(config-line)# login
```

Aux

W niektórych urządzeniach dostępny jest również port pomocniczy, dzięki któremu można podłączyć się fizycznie. Hasło ustawiamy analogicznie jak w przypadku portu konsolowego.

```
Switch# config t
Switch(config)# line aux 0
Switch(config-line)#password Cisco123
Switch(config-line)# login
```

VTY Virtual tty reprezentuje zdalne połączenia do urządzenia, może to być telnet lub SSH. Liczba dostępnych wirtualnych linii może być różna w zależności od urządzenia, maksymalnie 16. Poniższy przykład pokazuje konfiguracje linii od 0 do 4. Umożliwia to nawiązanie jednocześnie pięciu połączeń zdalnych, w większości przypadków jest to wystarczająca ilość.

```
Switch# config t
Switch(config)#line vty 0 4
Switch(config-line)#password Cisco123
Switch(config-line)# login
```

Czasem mamy potrzebę przygotowania uniwersalnej konfiguracji dla różnych urządzeń. Jeżeli chcemy mieć możliwość podłączenia do wszystkich dostępnych na maszynie wirtualnych interfejsów, warto konfiguracje rozdzielić na dwie części. Zapobiegnie to odrzuceniu polecenia w przypadku gdy konfigurujemy linie od 0 do 15, a urządzenie udostępnia mniejszą ich ilość.

```
Switch# config t
Switch(config)#line vty 0 4
Switch(config-line)#password Cisco123
Switch(config-line)# login
Switch(config)#line vty 5 15
Switch(config-line)#password Cisco123
Switch(config-line)# login
```

Tryb uprzywilejowany

Logując się do IOSa zazwyczaj zaczynamy od trybu użytkownika, aby podnieść swoje uprawnienia używamy komendy enable. Do ustawiania hasła dostępu tego trybu możemy użyć polecenie enable password lub enable secret. Zalecane jest stosowanie tego drugiego ze względu na to, że jest szyfrowane MD5. Enable secret wpisane jest w konfiguracji jawnym tekstem.

```
Switch# config t
Switch(config)# enable secret Cisco321
```