

امن سازک تجهیزات سیسکو

برای محدود کردن دسترسی به Telnet و SSH از یک رنج IP خاص در سویچ

در راستای اعمال تنظیمات سیسکو ۳۸۵۰، باید از Access Control Lists (ACLs) استفاده کنید. در زیر مراحل که باید طی کنید آورده شده است:

۱. ایجاد ACL: ابتدا باید یک Access Control List بسازید که فقط به رنج IP خاص اجازه دسترسی به Telnet/SSH بدهد.

```
Switch(config)# ip access-list standard TELNET_SSH_ACL
```

```
Switch(config-std-nacl)# permit <IP_Range>
```

```
<Wildcard_Mask>
```

```
Switch(config-std-nacl)# deny any
```

```
Switch(config-std-nacl)# exit
```

در اینجا <IP_Range> رنج IP مورد نظر شما و <Wildcard_Mask> معادل

ماسک وارون (inverted mask) برای رنج IP است.

به عنوان مثال، برای اجازه دسترسی فقط به رنج: ۱۹۲، ۱۶۸، ۱، ۰/۲۴ IP

```
Switch(config)# ip access-list standard TELNET_SSH_ACL
```

```
Switch(config-std-nacl)# permit ۱۹۲,۱۶۸,۱,۰۰,۰,۰,۲۵۵
```

```
Switch(config-std-nacl)# deny any
```

```
Switch(config-std-nacl)# exit
```

۱۲. اعمال ACL به خطوط vty: حالا باید ACL ی که ساخته اید را به خطوط vty

سویچ اعمال کنید تا فقط IP های مجاز بتوانند Telnet یا SSH کنند.

```
Switch(config)# line vty
```

```
Switch(config-line)# access-class TELNET_SSH_ACL in
```

```
Switch(config-line)# exit
```

اگر سویچ شما تعداد بیشتری خطوط vty دارد، ممکن است نیاز باشد این

تنظیم را برای بقیه خطوط نیز تکرار کنید:

```
Switch(config)# line vty ۵ ۱۵
```

```
Switch(config-line)# access-class TELNET_SSH_ACL in
```

```
Switch(config-line)# exit
```

۳. ذخیره پیکربندی: برای ذخیره تنظیمات انجام شده، دستور زیر را اجرا کنید:

Switch# write memory

این مراحل باعث می شود که تنظیمات IPهای مشخص شده در ACL به Telnet و

SSH دسترسی داشته باشند و سایر IPها دسترسی نداشته باشند.

دو دستور زیر رو هم باید داشته باشید روی سوئیچ هاتون وارد مد کانفیگ

سوئیچ بشید و بنویسید

no ip http server

no ip http secure-server

گام اول

باید دو رنج آی پی رو در این قسمت معرفی کنید

جهت دسترسی از دیتاسنتر به سوئیچ های شما که در زیر مشخص شده (۱-۲)

(جهت جهت دسترسی خودتون به سوئیچ ها)

ip access-list standard TELNET_SSH_ACL

permit ۱۹۲,۱۶۸,۲۵۰,۰۰,۰,۰,۲۵۵

Permit ip range,wildcard-mask

مربوط به رنج آی پی قسمت کاری خودتون در (ip range,wildcard-mask

(محل کارتتون)

deny any

exit

برای تنظیم این قسمت به تنظیمات کارت شبکه سیستم خودتون در محل کار وارد شدید و با توجه به رنج آی پی اون این قسمت رو کامل کنید
توجه: در صورت نیاز برای بدست آوردن رنج شبکه و wildcard-mask واحد کاری خودتون با توجه به ip ,subnet کارت شبکه سیستم خودتون میتونید از این لینک استفاده کنید/ <https://www.subnet-calculator.com/>

گام دوم

line vty 0 10

access-class TELNET_SSH_ACL in

exit

گام سوم

Switch#write memory

