Cisco IOS Security Hardening & Best Practices

Date: 8 July 2021

Table of Contents

Best Practices & Tools

```
# Cisco Auditor Tool
https://github.com/cisco-config-analysis-tool/ccat

# How to use CCAT
https://www.blackhillsinfosec.com/how-to-use-ccat-an-analysis-tool-for-cisco-configuration-files/

# Cisco Security Best Practices
https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html
```

Hardening

Create Local User Admin Account

```
username netadmin privilege 15 secret 1111
enable secret 2222
service password-encryption
aaa new-model
aaa authentication login enable
aaa local authentication attempts max-fail 10
aaa session-id common
```

Configure Management IP

```
# Loopback interfaces are always up so use loopback interface for SSH remote mgmt access
int lo0
    ip add 10.10.100.250 255.255.255.255
```

Restrict and Secure Remote Mgmt Access

```
ip access-list extended SSHAccess
 permit tcp host 192.168.20.48 any eq 22 log
 permit tcp host 192.168.20.2 any eq 22 log
 deny tcp any any log
!
line vty 0 4
 access-class SSHAccess in
 transport input ssh
 exec-timeout 15
```

OR

```
ip access-list standard 1
        remark SSH ACCESS
        permit x.x.x.x
        permit x.x.x.x
!
line vty 0 4
 access-class 1 in
 transport input ssh
 exec-timeout 15 0
```

Restrict Console Access

```
line con 0
   exec-timeout 15
   no privilege level 15
```

Configure SSH Options

```
ip domain-name 1.com
crypto key generate rsa modulus 2048
ip ssh version 2
ip ssh time-out 30
ip ssh logging events
ip ssh maxstartups 10
ip ssh authentication-retries 5
ip ssh server algorithm encryption aes256-ctr  (sets aes256-ctr as the only SSH cipher to be used)
ip ssh server algorithm mac hmac-sha1  (sets hmac-sha1 as the only SSH integrity cipher to be used)
```

Enable Secure Login Checking

```
# Helps prevent dictionary attack/brute force
login block-for 300 attempts 5 within 120
login delay 2
login on-failure log
login on-success log
```

Enable Logging

```
logging buffered 16000 informational
logging 10.10.10.5  (note: syslog server IP)
logging source-interface Loopback 0
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

Enable Configuration Change Notification & Logging

#Enables configuration management and history of changes on the device

```
archive
   log config
   logging enable
   logging size 200
   hidekeys
   notify syslog
```

```
sh archive log config all
         (OUTPUT)
         idx sess user@line Logged command
         1 1 console@console |access-list 199 permit icmp host 10.10.10.10 host 20.20.20.20
         2 1 console@console |crypto map NiStTeSt1 10 ipsec-manual
         3 1 console@console |match address 199
         4 1 console@console |set peer 20.20.20.20
         5 1 console@console |exit
         6 1 console@console |no access-list 199
         7 1 console@console |no crypto map NiStTeSt1
         8 2 netadmin@console |crypto key generate rsa modulus *****
         9 0 netadmin@vty0 |!exec: enable
```

Disable Log to Console or Monitor Sessions

```
no logging console
no logging monitor
```

Enable NTP Server

```
clock timezone CST -6 0
clock summer-time CDT recurring
ntp server x.x.x.x
```

NTP Authentication

```
#On the switch/router that will be the master NTP server
ntp master 3
ntp authenticate
ntp authentication-key 1 md5 <password>

#On the client switches/routers to receive NTP from the NTP server
ntp server x.x.x.x  key 1
ntp authenticate
ntp authentication-key 1 md5 <password>
ntp trusted-key 1
```

Restrict SNMP Access

```
ip access-list standard ACL-SNMP
   permit 10.10.100.6
   deny any log
snmp-server community T@s9aMon RO ACL-SNMP
snmp-server location AL
snmp-server contact tater@1.com
```

Disable Unused Services

```
no ip http server
no ip http secure-server
no service dhcp
no cdp run

no lldp run global

no ip bootp server

no ip domain-lookup

no ip source-route
```

Enable Login Banner

#Change this banner message to reflect your organization’s preferred warning banner

```
banner login #

 UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED! You must have explicit
permission to access or configure this system.

 All activities performed on this system may be logged, and violations of this policy may result in
disciplinary action and may be reported to law enforcement.

 Use of this system shall constitute consent to monitoring.

 #

banner motd #

 AUTHORIZED ACCESS ONLY! If you are not an authorized user, disconnect IMMEDIATELY!
All connections are monitored and recorded.

 #
```

Enable Keepalives TCP Sessions

```
service tcp-keepalives-in

service tcp-keepalives-out
```

Enable Memory & CPU Threshold Notifications

```
memory free low-watermark processor 204800

memory free low-watermark io 204800
memory reserve critical 20480

process cpu threshold type total rising 80 interval 60 falling 70 interval 60
process cpu statistics limit entry-percentage 80 size 60

memory reserve console 4096

exception memory ignore overflow io
exception memory ignore overflow processor

exception crashinfo maximum files 32
```

Enable Secure Copy & IOS Software Resilient

```
ip scp server enable
copy scp://usernam@10.10.100.250/home/tater/file.txt flash:

configuration mode exclusive auto

secure boot-image
secure boot-config
```

Disable Unused Ports & Apply Port Security

```
# global command to recovery from port security violation
errdisable recovery cause psecure-violation

int range fa0/1 - 48
   switchport port-security maximum 2
   switchport port-security mac-address sticky
   switchport port-security violation shutdown
   switchport port-security port-security aging time 15
   shut
```

Secure STP operation

#Enable BPDU guard on access ports

```
spanning-tree bpduguard enable
```

Prevent VLAN Hopping

# OPTION 1: Change the Native VLAN and then Prune the Native VLAN (CDP, PAgp and DTP will still function)

```
switchport trunk encapsulation dot1q
switchport trunk native vlan 800
switchport trunk allowed vlan remove 800
switchport mode trunk
```

# OPTION 2: Force the switch to tag the native VLAN (global cmd, must be done on all switches)

```
vlan dot1q tag native
```

OSPF Authentication

#Interface that OSPF is enabled on

```
interface FastEthernet0/1
        description to KeyWest
        ip address 200.120.45.253 255.255.255.252
        no ip directed-broadcast
        bandwidth 512
        ip ospf authentication message-digest
        ip ospf message-digest-key 1 md5 <password>
```

```
#The other router interface that peers with Key West
interface FastEthernet0/1
        description to Miami
        ip address 200.120.45.254 255.255.255.252
        no ip directed-broadcast
        bandwidth 512
        ip ospf authentication message-digest
        ip ospf message-digest-key 1 md5 <password>
```

Bogon Address ACL

```
#Denies invalid IP address space from being routed by core switch
#Apply ACL to egress port of the core switch connecting to the perimeter router/firewall

ip access-list extended 102
        remark BOGON ADDRESSES
        deny ip 0.0.0.0 0.255.255.255 any
        deny ip 10.0.0.0 0.255.255.255 any
        deny ip 100.64.0.0 0.63.255.255 any
        deny ip 127.0.0.0 0.255.255.255 any
        deny ip 169.254.0.0 0.0.255.255 any
        deny ip 172.16.0.0 0.15.255.255 any
        deny ip 192.0.0.0 0.0.0.255 any
        deny ip 192.0.2.0 0.0.0.255 any
        deny ip 192.168.0.0 0.0.255.255 any
        deny ip 198.18.0.0 0.1.255.255 any
        deny ip 198.51.100.0 0.0.0.255 any
        deny ip 203.0.113.0 0.0.0.255 any
        deny ip 224.0.0.0 31.255.255.255 any
        permit ip any any
```

RADIUS Authentication

```
#Configure AAA lines
aaa authentication login default local enable
aaa authentication login aaa_login group radius local
aaa authorization exec default local
aaa authorization network default group radius local

#Create Local Device User Accounts
#Accounts must match how the user account is created within LDAP (e.g., LDAP account tater.tot must be tater.tot on the device)
username mr.robot privilege 15 secret 9
username tater.tot privilege 15 secret 9

#Setup Radius Server
radius server DUO-Radius
 address ipv4 x.x.x.x auth-port 1812 acct-port 1813
 non-standard
 key 7

#Configure VTY Lines
line vty 0 4
 access-class 101 in
 login authentication aaa_login
 length 0
 transport input ssh
 transport output ssh
```

Dynamic Trunking Protocol (DTP)

```
#Disable DTP on access ports

#Add “switchport nonegotiate” to disable DTP on the interface

# Haven’t found a global command to disable yet


int range gig 0/1 - 48

  switchport mode access

  switchport nonegotiate

  spanning-tree portfast edge
```