Cisco: Context-based access control (CBAC)

CBAC (Context-Based Access Control) is a stateful firewall feature available on Cisco routers that analyses traffic passing through the router, creating dynamic ACLs based on detected sessions. It allows traffic to be filtered based on the state of the connection, not just addresses and ports.

How CBAC works

- CBAC monitors Layer 4 sessions (TCP, UDP, ICMP).
- Analyses and tracks connection status in both directions.
- Dynamically adds entries to ACLs to allow return traffic (e.g. replies to queries).
- Protects against unauthorised access and certain types of attacks (e.g. DoS)

Advantages of

- Dynamic port opening only for active connections
- Better control than standard ACLs
- Logging and alerting capability

Basic CBAC configuration

1. define protocol inspection

```
ip inspect name CBAC_INSPECT http
ip inspect name CBAC_INSPECT ftp
ip inspect name CBAC_INSPECT tcp
ip inspect name CBAC_INSPECT udp
```

2. assign the inspection to an interface

Outgoing traffic (where connections are initiated).

```
interface FastEthernet0/0
 ip inspect CBAC_INSPECT out
```

3. configure ACLs on the inbound interface (e.g. from the Internet)

```
access-list 100 permit tcp any any established
access-list 100 permit icmp any any echo-reply
access-list 100 deny ip any any
```

```
interface FastEthernet0/1
 ip access-group 100 in
```

4. (Optional) Enable CBAC logging

```
ip inspect audit-trail
ip inspect log drop-pkt
ip inspect log tcp syn
```

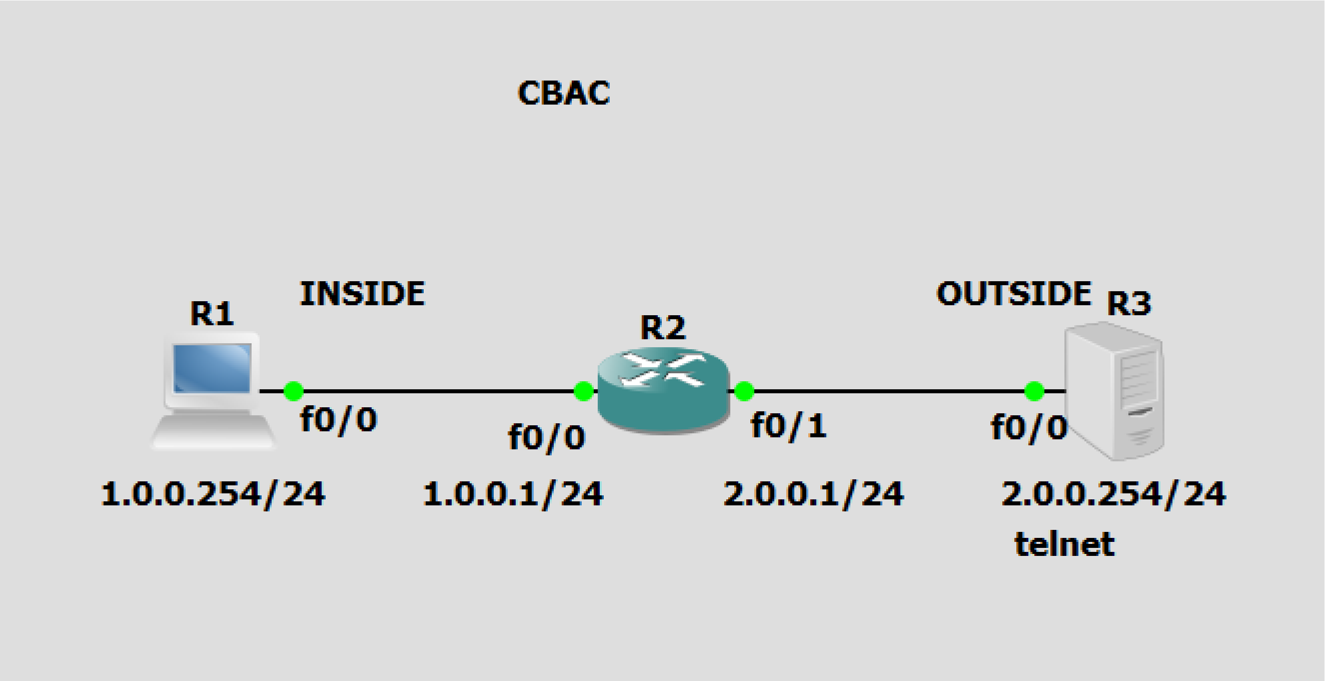
Useful commands for diagnostics

```
show ip inspect sessions
show ip inspect config
debug ip inspect
```

Concluding remarks

- CBAC works best on traffic initiated from within the network.
- Can overload the router with heavy traffic - worth monitoring performance
- Often replaced in modern configurations by a Zone-Based Firewall (ZBF). **Zone-Based Firewall (ZBF)**

Example



test:

```
R1#ping 2.0.0.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.0.0.254, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#telnet 2.0.0.254
Trying 2.0.0.254 ... Open


User Access Verification

Password:
R3>
```

R1 configuration:

```
Building configuration...

Current configuration : 1303 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
```

```
!
!
!
!
!
!
!
!
!
!
!
!
!
archive
 log config
  hidekeys
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
 ip address 1.0.0.254 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/2
 no ip address
 shutdown
 clock rate 2000000
!
```

```
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 1.0.0.1
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```

R2 configuration:

```
Building configuration...

Current configuration : 1445 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
ip inspect name TELNET_ONLY telnet
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
archive
```

```
 log config
  hidekeys
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
 ip address 1.0.0.1 255.255.255.0
 ip inspect TELNET_ONLY out
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet0/1
 ip address 2.0.0.1 255.255.255.0
 ip access-group 100 in
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/2
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
```

```
!
!
no ip http server
no ip http secure-server
!
access-list 100 permit tcp any any established
access-list 100 deny   ip any any
no cdp log mismatch duplex
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```

R3 configuration:

```
Building configuration...

Current configuration : 1342 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
```

```
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
archive
 log config
  hidekeys
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
```

```
 ip address 2.0.0.254 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/2
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 2.0.0.1
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
!
!
!
!
!
```

```
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 password cisco
 login
!
!
end
```