Cisco: Context-based access control (CBAC)

CBAC (Context-Based Access Control) to funkcja zapory stanu (stateful firewall) dostępna na routerach Cisco, która analizuje ruch przechodzący przez router, tworząc dynamiczne listy ACL na podstawie wykrytych sesji. Umożliwia filtrowanie ruchu na podstawie stanu połączenia, a nie tylko adresów i portów.

Jak działa CBAC

- CBAC monitoruje sesje warstwy 4 (TCP, UDP, ICMP)
- Analizuje i śledzi stan połączeń w obu kierunkach
- Dynamicznie dodaje wpisy do list ACL, aby umożliwić ruch powrotny (np. odpowiedzi na zapytania)
- Chroni przed nieautoryzowanym dostępem i niektórymi typami ataków (np. DoS)

Zalety

- Dynamiczne otwieranie portów tylko dla aktywnych połączeń
- Lepsza kontrola niż standardowe ACL
- Możliwość logowania i alertowania

Podstawowa konfiguracja CBAC

1. Zdefiniuj inspekcję protokołów

```
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. Przypisz inspekcję do interfejsu

Ruch wychodzący (gdzie inicjowane są połączenia)

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

3. Skonfiguruj ACL na interfejsie wejściowym (np. od strony Internetu)

```
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. (Opcjonalnie) Włącz logowanie CBAC

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

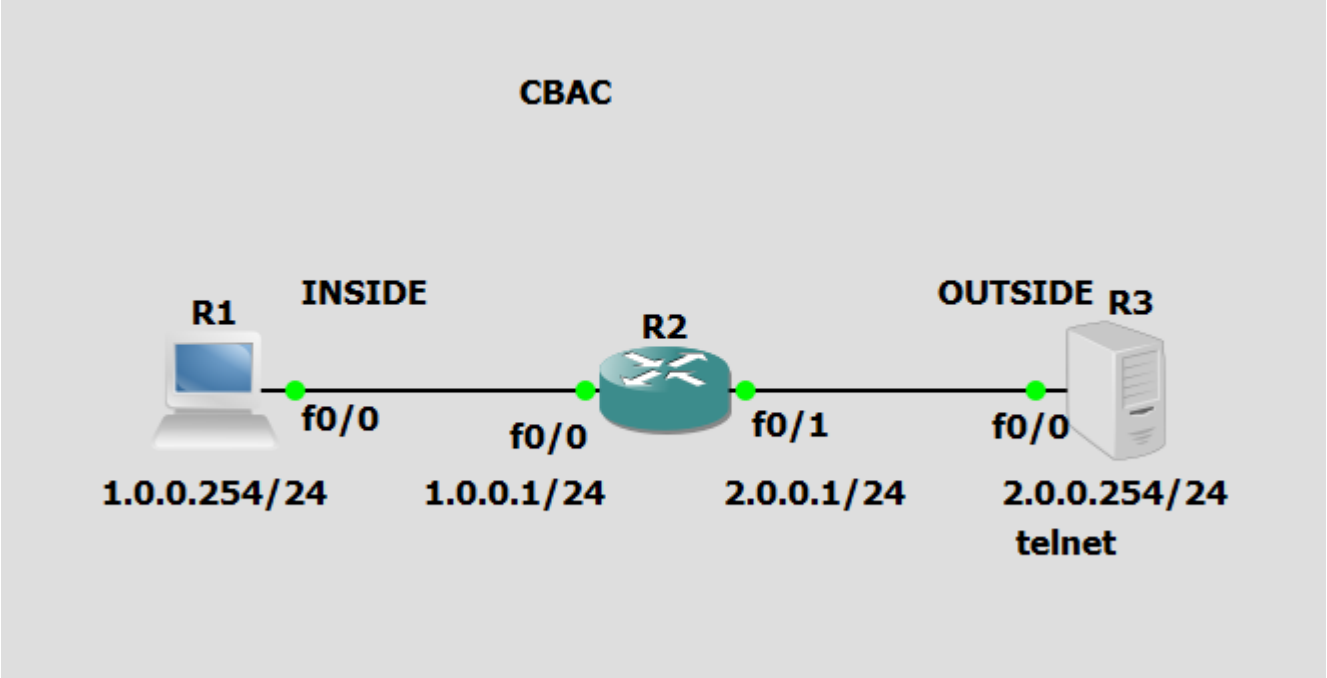
Przydatne polecenia do diagnostyki

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

Uwagi końcowe

- CBAC działa najlepiej na ruchu inicjowanym z wewnątrz sieci
- Może obciążać router przy dużym ruchu – warto monitorować wydajność
- W nowoczesnych konfiguracjach zastępowany często przez **Zone-Based Firewall (ZBF)**

Przykład



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>
```

konfiguracja R1:

```
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
```

konfiguracja R2:

```
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
```

konfiguracja R3:

```
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
```