# **BONUS Packet Tracer 8.1.1 lab 20**

Last Updated: Monday, 21 February 2022 07:30

Written by PacketTracerNetwork

<https://www.packettracernetwork.com/labs/packettracerlabs.html>

## **Cisco Packet Tracer labs for your reference**

Download free Cisco Packet Tracer 8.0.1 activity files (pka) designed by our team for CCNAand CCNP ENTERPRISE certification exams training. Perform LAB 20 for 10 point bonus mark.

[**Lab 1** : Basic switch setup](https://www.packettracernetwork.com/labs/lab1-basicswitchsetup.html)

[**Lab 2** : Configuring switch interfaces](https://www.packettracernetwork.com/labs/lab2-switchinterfacesconfig.html)

[**Lab 3** : VLAN and VTP configuration](https://www.packettracernetwork.com/labs/lab3-vlanvtpconfig.html)

[**Lab 4** : Port security](https://www.packettracernetwork.com/labs/lab4-portsecurity.html)

[**Lab 6** : Basic router setup](https://www.packettracernetwork.com/labs/lab6-basicroutersetup.html)

[**Lab 16** : ASA 5505 SSL WebVPN](https://www.packettracernetwork.com/labs/lab16-asa-webvpn.html)

[**Lab 17** : ASA 5505 IPSEC VPN](https://www.packettracernetwork.com/labs/lab17-asa-ipsec-vpn.html)

[**Lab 18** : ASA 5505 DMZ configuration](https://www.packettracernetwork.com/labs/lab18-asa-dmz.html)

[**Lab 19** : ASA 5505 traffic inspection](https://www.packettracernetwork.com/labs/lab-19-deep-packet-inspection-with-asa-5505.html)

[**Lab 20** : CBAC traffic Inspection with ISR router](https://www.packettracernetwork.com/labs/lab-20-cbac-inspection-with-isr.html)

# **BONUS Lab - CBAC traffic Inspection with ISR router**

Last Updated: Tuesday, 16 July 2019 20:58

Written by PacketTracerNetwork

## **What is Cisco Context-Based Access Control ?**

**Cisco's Context-Based Access Control (CBAC)** is a security component similar to **reflexive ACL** available in ISR routers. This feature has been implemented in Packet Tracer since version 5.3

CBAC enables dynamic modification of inbound access lists to allow some incoming flows even if a "**deny any any**" ACL has been implemented by first inspecting and recording flows initiated from the protected internal network. **The main difference with reflexive ACLs is that whereas reflexive ACLs act solely on L2-L4 protocol attributes, CBAC is able to inspect all the way to the application layer (layer 7)**, taking into consideration characteristics of a flow on a per-protocol (or context) basis.

Diagram

Description automatically generated

[Download Cisco Packet Tracer 7.2 CBAC lab](https://www.packettracernetwork.com/pktlabs/lab20-CBAC.pka)

## **Lab instructions**

Aim of this lab is to configure CBAC traffic inspection on ISR 2911 "Router1" connecting the branch office to the Internet. An inbound DENY ANY ANY access list is configured on the Gi0/2 interface of the router to deny all incoming flows from the internet. Despite this access list, the branch office laptops have to be able to access the 46.20.150.2 web server.

1. Activate security license on ISR 2911 router

2. Configure DHCP for the 192.168.1.0/24 LAN network. Gateway is 192.168.1.1 on Router 1. The first 8 IP addresses are reserved for network use and don't have to be used by LAN clients.

3. Configure NAT on Router 1 to allow branch laptops to access the Internet. Use the first standard access list to configure the source network and the Gi 0/2 interface for outgoing traffic to the internet

4. Configure a named accesslist to deny all the inbound traffic from the internet and apply it on the internet facing network interface. The access-list will be named DENY\_ANY

5. Configure CBAC to allow outbound HTTP traffic

6. Verify CBAC configuration by accessing http://46.20.150.2 from a laptop's web browser. CBAC inspection policy will be named ALLOWED\_TRAFIC

## **Lab Solution**

### Step 1 : Activate security license on ISR 2911 routers

**Firewalling and other security-functions like VPN are only available with the Security-License on Cisco ISR 2900 routers.** **Activate the evaluation of the securityk9 license on the router, save the configuration, and reload the ISR router before continuing.**

Router>enable

Router#configure terminal

Router(config)#license boot module c2900 technology-package securityk9

PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR

LICENSE KEY PROVIDED FOR ANY CISCO PRODUCT FEATURE OR USING SUCH

PRODUCT FEATURE CONSTITUTES YOUR FULL ACCEPTANCE OF THE FOLLOWING

TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO BE BOUND

BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires an additional license from Cisco,

together with an additional payment. You may use this product feature

on an evaluation basis, without payment to Cisco, for 60 days. Your use

of the product, including during the 60-day evaluation period, is

subject to the Cisco end user license agreement

http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN\_.html

If you use the product feature beyond the 60 day evaluation period, you

must submit the appropriate payment to Cisco for the license. After the

60 day evaluation period, your use of the product feature will be

governed solely by the Cisco end user license agreement (link above),

together with any supplements relating to such product feature. The

above applies even if the evaluation license is not automatically

terminated and you do not receive any notice of the expiration of the

evaluation period. It is your responsibility to determine when the

evaluation period is complete and you are required to make payment to

Cisco for your use of the product feature beyond the evaluation period.

Your acceptance of this agreement for the software features on one

product shall be deemed your acceptance with respect to all such

software on all Cisco products you purchase which includes the same

software. (The foregoing notwithstanding, you must purchase a license

for each software feature you use past the 60 days evaluation period,

so that if you enable a software feature on 1000 devices, you must

purchase 1000 licenses for use past the 60 day evaluation period.)

Activation of the software command line interface will be evidence of

your acceptance of this agreement.

ACCEPT? [yes/no]: yes

% use 'write' command to make license boot config take effect on next boot

%IOS\_LICENSE\_IMAGE\_APPLICATION-6-LICENSE\_LEVEL: Module name = C2900 Next reboot level = securityk9 and License = securityk9

%LICENSE-6-EULA\_ACCEPTED: EULA for feature securityk9 1.0 has been accepted. UDI=CISCO2911/K9:FTX1524PCPQ; StoreIndex=0:Evaluation License Storage

Router(config)#exit

Router#

%SYS-5-CONFIG\_I: Configured from console by console

Router#write

Building configuration...

[OK]

Router#reload

After router reload, check activation of the securityk9 license

Router>enable

Router#show license feature

Feature name Enforcement Evaluation Subscription Enabled RightToUse

ipbasek9 no no no yes no

securityk9 yes yes no yes yes

datak9 yes no no no yes

uck9 yes yes no no yes

Router#

Note the "yes" in the evaluation column of the securityk9 license : the router doesn't have a valid license file but allows an evaluation period. Be careful in a production environmnent !

### Step 2 : Configure DHCP and NAT on Router 1

Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.9

Router(config)#ip dhcp pool LAN

Router(dhcp-config)#network 192.168.1.0 255.255.255.0

Router(dhcp-config)#default-router 192.168.1.1

Router(config)#interface GigabitEthernet0/0

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Router(config-if)#ip nat inside

Router(config)#interface GigabitEthernet0/2

Router(config-if)#ip address 46.20.146.1 255.255.255.252

Router(config-if)#ip nat outside

Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255

Router(config)#ip nat inside source list 1 interface GigabitEthernet0/2 overload

### Step 3 : Configure inbound ACL and CBAC on outbound traffic

**Configure and apply inbound ACL**

Router(config)#ip access-list extended DENY\_ANY

Router(config-ext-nacl)#deny ip any any

Router(config-ext-nacl)#exit

Router(config)#int gigabitEthernet 0/2

Router(config-if)#ip access-group DENY\_ANY in

**Configure CBAC to allow HTTP traffic**

Router(config)#ip inspect name ALLOWED\_TRAFIC http audit-trail on

Router(config)#interface gigabitEthernet 0/2

Router(config-if)#ip inspect ALLOWED\_TRAFIC out

**Verify CBAC (ip inspect) configuration**

Router#show ip inspect all

Session audit trail is enabled

Session alert is enabled

one-minute (sampling period) thresholds are [unlimited : unlimited] connections

max-incomplete sessions thresholds are [unlimited : unlimited]

max-incomplete tcp connections per host is unlimited. Block-time 0 minute.

tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec

tcp idle-time is 3600 sec -- udp idle-time is 30 sec

tcp reassembly queue length 16; timeout 5 sec; memory-limit 1024 kilo bytes

dns-timeout is 5 sec

Inspection Rule Configuration

Inspection name ALLOWED\_TRAFIC

http alert is on audit-trail is on timeout 3600

Interface Configuration

Interface GigabitEthernet0/2

Inbound inspection rule is not set

Outgoing inspection rule is ALLOWED\_TRAFIC

http alert is on audit-trail is on timeout 3600

Inbound access list is DENY\_ANY

Outgoing access list is not set

Router#