POLICY BASED ROUTING

SONYA LAO
CCNP P1/2

Purpose

The purpose of this lab is to explore the functions of policy based routing in a large network. We solidified our understanding of web servers and routing protocols, and learned a new method for routing traffic.

Background Information

Imagine you work in the airport control tower. It is your job to direct aircrafts on where to land in the airport. You have a set of protocols to follow based on the type of aircraft and type of flight that is landing. For example, if a cargo plane is landing, you will direct them to land in Area 3, close to the airport warehouse. However, if it is a commercial flight with many passengers, you will direct the plane to land in Area 1, closest to the terminal for the passenger's ease of access. All the planes have the same destination, but you have control over what path they take to enter the airport. The same is true with route maps. The access lists configured on the router give certain protocols for what type of traffic is permitted, but it is through the route map that the next hop, or landing area is set. The route map directs traffic flow to go through different routes depending on the type of traffic, just like the airport control tower.

Lab Summary

First, I created my topology. I have one router (R3) connected to PC-0 to give the PC a default gateway. R3 is connected to R4. R4 is connected to R5 and R7, which are connected to R8. The HTTP and HTTPS servers are located on R8. The goal of this lab is to redirect all HTTP traffic to go through R7, and all HTTPS traffic through R5. After I created my topology, I configured each interface on the corresponding routers with the correct IP address and subnet masks. I also set up EIGRP, with all routers in the same autonomous system. After the network is set up, I created 2 access lists on R4. The first access list permits HTTP traffic from host PC0 to the IP address of R8. The second access list permits HTTPS traffic from PC0 to the IP address of R8. Next, I created the route map. Every route map has a match and set command. For the first layer of the route map, I matched the HTTP access list to the route map. Then I set the default IP route destination to the IP address on Router 7. Similarly, I matched the HTTPS access list to the 2nd layer of the route map and set the default IP route destination to the IP address of Router 5. Then I applied the route map to the interface connected to R3. To test the success of the route map, I generated HTTP traffic on PC0, and confirmed that the packets

Lab Commands

```
R1(config)#ip http server
```

This command enables the IP HTTP server on the router.

```
R1(config)#ip http secure-server
```

This command activates the HTTPS server on the router and generates an rsa certificate that is self-signed for the server. The standard HTTP server and the HTTPS server can run on the router at the same time.

```
R1(config)#username [name] privilege [1-15] [password/secret] [your password]
```

This command creates a user and sets the privilege level for that user on the router. 15 is the highest level of privilege. Secret encrypts the password when shown on the running configuration.

```
R1(config)#ip http authentication local
```

This command keeps the authentication local to the server, using the username and password set on the router.

```
R1(config)#ip access-list extended [name]
```

This command is used to create a named extended access list. Extended access lists allow for more specification of the source and destination addresses and the specific port permissions.

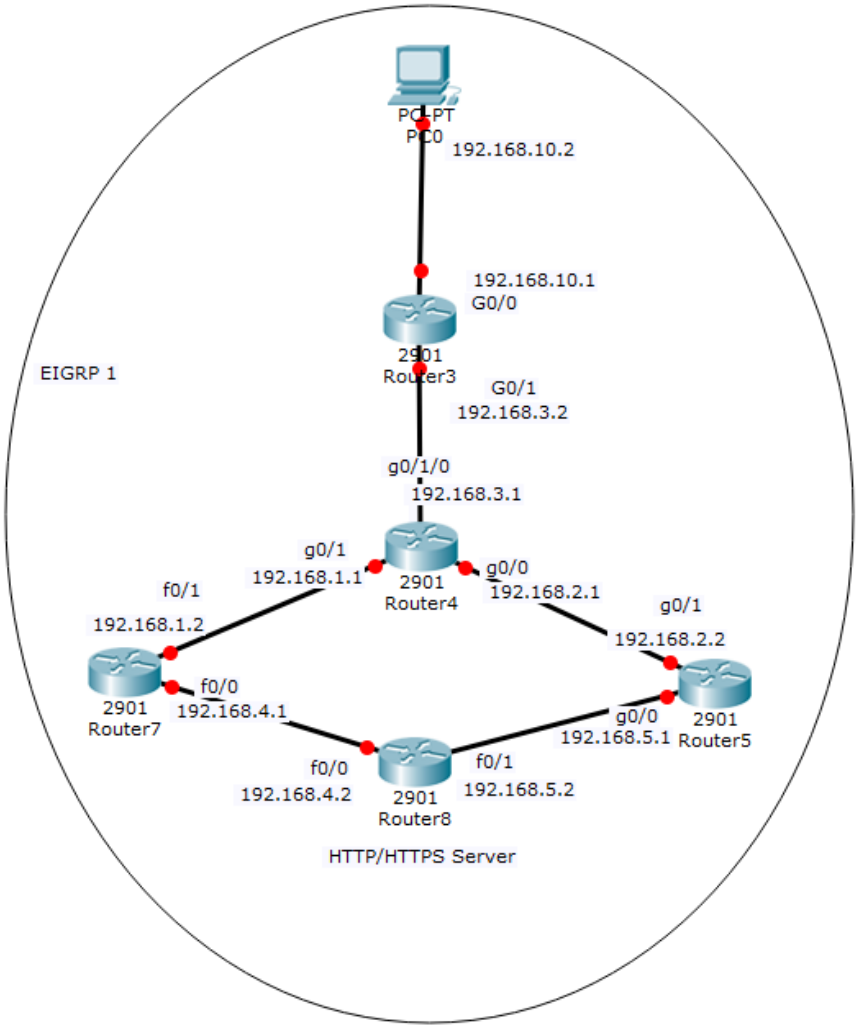
```
R1(config-nacl)#[permit/deny] [ip/tcp/udp/icmp] [source address] [source
subnet] [destination address] [destination subnet] eq [protocol/port #]
```

This command is issued within the named access list. You can permit or deny a source address, specify the type of protocol (IP, TCP, UDP, and more), specify the destination address, and the port number of the protocol involved.

```
R1(config)#route-map [name] [permit/deny] [number]
 match ip address HTTP
 set ip next-hop 192.168.1.2
```

The route map is used to define which routes, in this case, access lists are allowed to be redistributed into the routing process. You begin by giving the route map a name and setting it as either a permit or deny. Then you match the IP address to the named access list, and set the next hop IP address to decide where the specified traffic will flow.

Lab Diagram


PC-PT
PC0
192.168.10.2
192.168.10.1
G0/0
2901
Router3
EIGRP 1
G0/1
192.168.3.2
g0/1/0
192.168.3.1
g0/1
192.168.1.1
2901
Router4
g0/0
192.168.2.1
f0/1
192.168.1.2
g0/1
192.168.2.2
2901
Router7
f0/0
192.168.4.1
g0/0
192.168.5.1
2901
Router5
f0/0
192.168.4.2
2901
Router8
f0/1
192.168.5.2
HTTP/HTTPS Server

Configurations

R3#show run

```
Building configuration...
Current configuration : 1494 bytes
version 15.2
no service password-encryption
hostname R3
no ip domain lookup
no ipv6 cef
interface GigabitEthernet0/0
 ip address 192.168.10.1
255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 192.168.3.2
255.255.255.0
 duplex auto
 speed auto
router eigrp 1
 network 192.168.3.0
 network 192.168.10.0
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

R4#show run

```
Building configuration…
Current configuration: 1995 bytes
Last configuration change at
18:31:41 UTC Thu May 18 2017
no service password-encryption
hostname R4
no ip domain lookup
no ipv6 cef
interface GigabitEthernet0/0
 ip address 192.168.2.1
255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 192.168.1.1
255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1/0
 ip address 192.168.3.1
255.255.255.0
 ip policy route-map PBR
 duplex auto
 speed auto
router eigrp 1
 network 192.168.1.0
 network 192.168.2.0
 network 192.168.3.0
no ip http server
no ip http secure-server
ip access-list extended HTTP
 permit tcp host 192.168.10.3 host
192.168.4.2 eq www
ip access-list extended HTTPS
 permit tcp host 192.168.10.3 host
192.168.5.2 eq 443
route-map PBR permit 10
 match ip address HTTP
 set ip next-hop 192.168.1.2
route-map PBR permit 20
 set ip next-hop 192.168.2.2
control-plane
end
```

R5#show run

```
Building configuration...
Current configuration : 1823 bytes
Last configuration change at
18:27:44 UTC Thu May 18 2017
version 15.2
no service password-encryption
hostname R5
no ip domain lookup
interface GigabitEthernet0/0
 ip address 192.168.5.1
255.255.255.0
 ip broadcast-address 192.168.5.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 192.168.2.2
255.255.255.0
 ip broadcast-address 192.168.2.0
 duplex auto
 speed auto
router eigrp 1
 network 192.168.2.0
 network 192.168.5.0
no ip http server
no ip http secure-server
line con 0
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
End
```

R7#show run

```
Building configuration...
Current configuration : 2992 bytes
Last configuration change at
19:48:23 UTC Thu May 18 2017
version 15.1
no service password-encryption
hostname R7
interface FastEthernet0/0
 ip address 192.168.4.1
255.255.255.0
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 192.168.1.2
255.255.255.0
 duplex auto
 speed auto
router eigrp 1
 network 192.168.1.0
 network 192.169.4.0
line con 0
line aux 0
line vty 0 4
 login
 transport input all
end
```

R8#show run

```
Building configuration...
Current configuration : 3034 bytes
Last configuration change at
20:29:54 UTC Thu May 18 2017
version 15.1
service timestamps debug datetime
msec
service timestamps log datetime
msec
no service password-encryption
hostname R8
ip source-route
no ip domain lookup
no ipv6 cef
crypto pki token default removal
timeout 0
crypto pki trustpoint TP-self-
signed-2354516119
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-
Certificate-2354516119
 revocation-check none
 rsakeypair TP-self-signed-
2354516119
crypto pki certificate chain TP-
self-signed-2354516119
 certificate self-signed 01
  3082022B 30820194 A0030201
02020101 300D0609 2A864886 F70D0101
05050030
```

```
  31312F30 2D060355 04031326
494F532D 53656C66 2D536967 6E65642D
43657274
  69666963 6174652D 32333534
35313631 3139301E 170D3137 30353138
32303139
  32385A17 0D323030 31303130
30303030 305A3031 312F302D 06035504
03132649
  4F532D53 656C662D 5369676E
65642D43 65727469 66696361 74652D32
33353435
  31363131 3930819F 300D0609
2A864886 F70D0101 01050003 818D0030
81890281
  8100A7C1 153A5D52 8987BAE7
943400D3 2CADC853 755F8F17 6302C75E
BAD5D96F
  DE1564D7 EA4E8B6A 6F274185
FC1EFB9D A711FCAA 3FBDE301 637D53F7
F12C9F6E
  D5000A03 C329DE68 7ECA5E00
A98951BE F5C07C4D 7B28BF95 9E051A43
13A0E4FB
  43F5A3DD 8F1C9F76 EE34D448
B68D721A 9626434B 97D9BC3C 36D7E733
6A3BF715
  96B30203 010001A3 53305130
0F060355 1D130101 FF040530 030101FF
301F0603
  551D2304 18301680 14330F97
59BE79E7 1D3E6DB4 68981C8C 28E41777
73301D06
  03551D0E 04160414 330F9759
BE79E71D 3E6DB468 981C8C28 E4177773
300D0609
  2A864886 F70D0101 05050003
81810023 C1A4E178 3544D870 56995078
514D351E
  502EB785 412FAADE 1A825D75
B3D8CBCE 15F3E94E 3E1AF03E 82A2CFC0
DAA75DC3
  A66B8F8C 8B1636AE 680B7FDC
D690B2DC 69A88DFF B7EB8A56 499708EC
4BF7656E
  C29B7EC2 5648B7BF 7F93E4CD
6D9450D5 0B9AEA2C CCB60435 5A826A8E
83E29379
  CC13DDDE AB34B6AC 7B4B88A8 794BCA
       quit
license udi pid CISCO2811 sn
FTX1233A58A
license accept end user agreement
username sonya privilege 15 secret
5 $1$pxCm$NGJYHF9vWhk4eXHaUAgpE1
interface FastEthernet0/0
 ip address 192.168.4.2
255.255.255.0
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 192.168.5.2
255.255.255.0
 duplex auto
 speed auto
router eigrp 1
 network 192.168.4.0
 network 192.168.5.0
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
line con 0
line aux 0
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

R3#show ip route

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
Gateway of last resort is not set

D     192.168.1.0/24 [90/28416] via 192.168.3.1, 00:04:57, GigabitEthernet0/1
D     192.168.2.0/24 [90/3072] via 192.168.3.1, 00:05:36, GigabitEthernet0/1
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, GigabitEthernet0/1
L        192.168.3.2/32 is directly connected, GigabitEthernet0/1
D     192.168.4.0/24 [90/31232] via 192.168.3.1, 00:04:13, GigabitEthernet0/1
D     192.168.5.0/24 [90/28672] via 192.168.3.1, 00:04:17, GigabitEthernet0/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0
```

R3#show ip eigrp neighbors

```
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface              Hold Uptime   SRTT   RTO
Q  Seq
                                                   (sec)         (ms)
Cnt Num
0   192.168.3.1             Gi0/1                    13 00:11:09    1   100
0  24
```

R4#show ip route

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
Gateway of last resort is not set
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/1
L        192.168.1.1/32 is directly connected, GigabitEthernet0/1
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, GigabitEthernet0/0
L        192.168.2.1/32 is directly connected, GigabitEthernet0/0
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, GigabitEthernet0/1/0
L        192.168.3.1/32 is directly connected, GigabitEthernet0/1/0
D     192.168.4.0/24 [90/30976] via 192.168.2.2, 00:53:37, GigabitEthernet0/0
D     192.168.5.0/24 [90/28416] via 192.168.2.2, 00:53:42, GigabitEthernet0/0
D     192.168.10.0/24
           [90/3072] via 192.168.3.2, 00:55:44, GigabitEthernet0/1/0
```

R4#show ip eigrp neighbors

```
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
2   192.168.1.2             Gi0/1                    13 00:54:51    1   100  0  5
1   192.168.2.2             Gi0/0                    10 00:55:33  416  2496  0  11
0   192.168.3.2             Gi0/1/0                  11 00:56:19  265  1590  0  11
```

R4#show route-map

```
route-map PBR, permit, sequence 10
  Match clauses:
    ip address (access-lists): HTTP
  Set clauses:
    ip next-hop 192.168.1.2
  Policy routing matches: 6 packets, 677 bytes
route-map PBR, permit, sequence 20
  Match clauses:
  Set clauses:
    ip next-hop 192.168.2.2
  Policy routing matches: 42 packets, 4504 bytes
```

R5#show ip route

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

D     192.168.1.0/24 [90/28416] via 192.168.2.1, 00:55:50, GigabitEthernet0/1
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, GigabitEthernet0/1
L        192.168.2.2/32 is directly connected, GigabitEthernet0/1
D     192.168.3.0/24 [90/3072] via 192.168.2.1, 00:56:27, GigabitEthernet0/1
D     192.168.4.0/24 [90/30720] via 192.168.5.2, 00:55:06, GigabitEthernet0/0
      192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.5.0/24 is directly connected, GigabitEthernet0/0
L        192.168.5.1/32 is directly connected, GigabitEthernet0/0
D     192.168.10.0/24 [90/3328] via 192.168.2.1, 00:56:27, GigabitEthernet0/1
```

R5#show ip eigrp neighbors

```
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface              Hold Uptime   SRTT   RTO
Q  Seq
                                                   (sec)         (ms)
Cnt Num
1   192.168.5.2             Gi0/0                    14 00:55:29 1596  5000
0  3
0   192.168.2.1             Gi0/1                    14 00:56:50    1   100
0  25
```

R7#show ip route

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, FastEthernet0/1
L        192.168.1.2/32 is directly connected, FastEthernet0/1
D     192.168.2.0/24 [90/28416] via 192.168.1.1, 00:56:53, FastEthernet0/1
D     192.168.3.0/24 [90/28416] via 192.168.1.1, 00:56:53, FastEthernet0/1
      192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.4.0/24 is directly connected, FastEthernet0/0
L        192.168.4.1/32 is directly connected, FastEthernet0/0
D     192.168.5.0/24 [90/30976] via 192.168.1.1, 00:56:18, FastEthernet0/1
D     192.168.10.0/24 [90/28672] via 192.168.1.1, 00:56:53, FastEthernet0/1
```

R7#show ip eigrp neighbors

```
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface              Hold Uptime   SRTT   RTO
Q  Seq
                                                   (sec)         (ms)
Cnt Num
1   192.168.4.2             f0/0                    14 00:55:29 1596  5000  0
3
0   192.168.1.1             f0/1                    14 00:56:50    1   100  0
25
```

R8#show ip route

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

D     192.168.1.0/24 [90/30976] via 192.168.5.1, 00:58:09, FastEthernet0/1
D     192.168.2.0/24 [90/28416] via 192.168.5.1, 00:58:09, FastEthernet0/1
D     192.168.3.0/24 [90/28672] via 192.168.5.1, 00:58:09, FastEthernet0/1
      192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.4.0/24 is directly connected, FastEthernet0/0
L        192.168.4.2/32 is directly connected, FastEthernet0/0
      192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.5.0/24 is directly connected, FastEthernet0/1
L        192.168.5.2/32 is directly connected, FastEthernet0/1
D     192.168.10.0/24 [90/28928] via 192.168.5.1, 00:58:09, FastEthernet0/1
```

R8#show ip eigrp neighbors

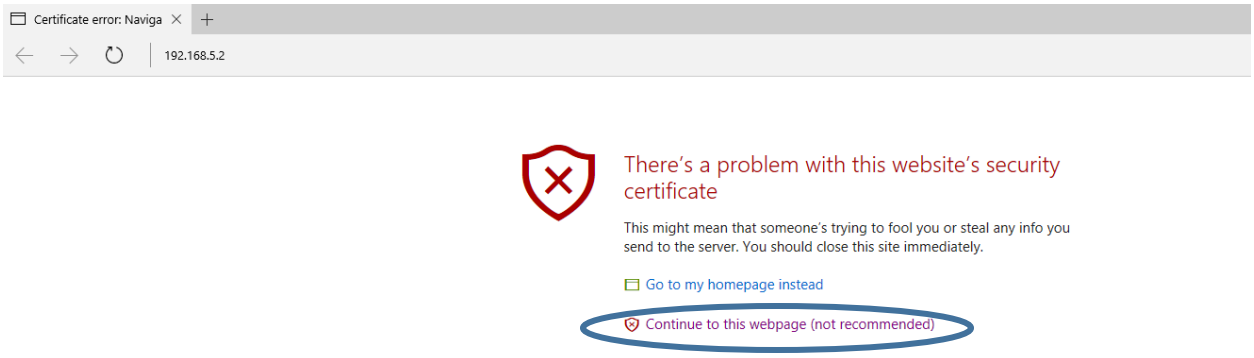
```
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.5.1             Fa0/1             10 00:58:24    1   200  0  12
```

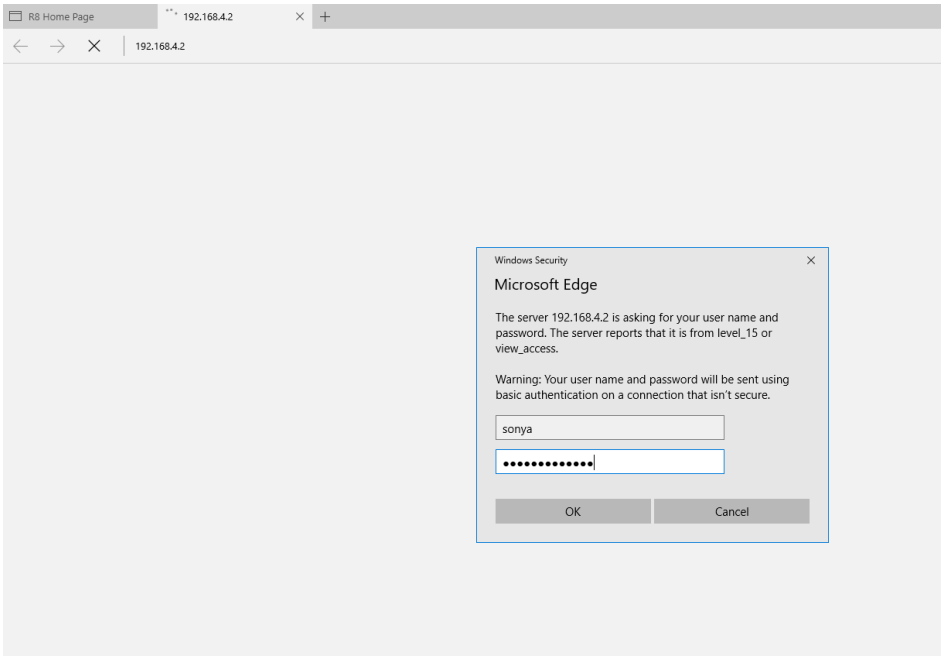
R8#show ip http server status

```
HTTP server status: Enabled
HTTP server port: 80
HTTP server active supplementary listener ports:
HTTP server authentication method: local
HTTP server digest algorithm: md5
HTTP server access class: 0
HTTP server base path:
HTTP server help root:
Maximum number of concurrent server connections allowed: 5
Server idle time-out: 180 seconds
Server life time-out: 180 seconds
Maximum number of requests allowed on a connection: 1
HTTP server active session modules: ALL
HTTP secure server capability: Present
HTTP secure server status: Enabled
```

```
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-128-sha
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:
HTTP secure server active session modules: ALL
```

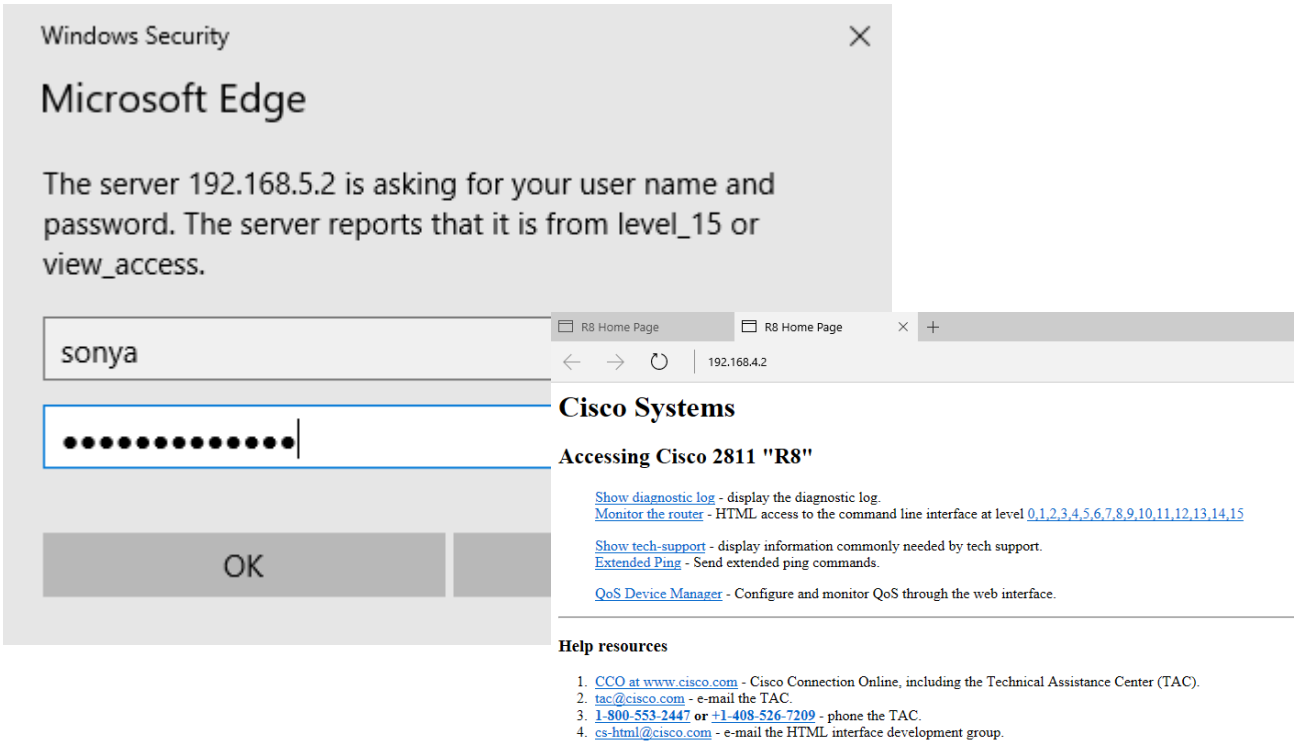
To test the HTTPS server, enter the IP address of the router, preceded by https://. A Certificate error message should pop up (see below)





After authenticating using the username and password configured on the router, you should be able to access the web page of the router.

Similarly, to check that the HTTP server is running, enter the IP address of the router in the web browser. The security login window should pop up right away, without the certificate error page. After logging in, you should see the homepage of the router.



To check that the packets are routed based on the type of web traffic (HTTP/HTTPS), use the `show route-map` command and notice the difference in packets.

```
R4#show route-map
route-map PBR, permit, sequence 10
  Match clauses:
    ip address (access-lists): HTTP
  Set clauses:
    ip next-hop 192.168.1.2
  Policy routing matches: 6 packets, 677 bytes
route-map PBR, permit, sequence 20
  Match clauses:
  Set clauses:
    ip next-hop 192.168.2.2
  Policy routing matches: 42 packets, 4504 bytes
```

Problems

When I first started the lab, I had issues with the basic setup of the HTTPS Server. I was able to successfully view the HTTP server after issuing the `ip http server` command on the router, but after issuing the `ip http secure-server` command, I couldn't access the HTTPS server. The syslog error message that was returned was that an rsa key could not be generated because the clock was not set up, so only a temporary certificate was generated. So I tried searching online for a solution based on the error message, and I tried various commands to install the clock. However, that did not work, so then I tried to reload the router. After a reload, the router was still unable to generate the certificate. Then I tried the `write memory` command, as prompted by the router, thinking that the command would save the temporary certificate to the router memory, but that did not work either. Finally, I tried the exact set of commands on a different router, and I was able to access the HTTP and HTTPS servers. So, I concluded that the original router had an issue with the ability to generate certificates, which I could not solve.

Another issue that I had involved creating the access lists. I did not remember the distinction between named access lists and extended access lists, and was confused as to which type of access list to use. In the end, I settled on a named extended access list so that I could more easily distinguish each access list. In addition, it had to be an extended access list so that I could specify the port number of HTTP and HTTP, 80 and 443 respectively.

Conclusion

This lab was a good way to review CCNA concepts (access lists, routing protocols), and apply them to new routing methods (route maps). I see the value that policy-based routing has for a large network, as it gives the network administrator the freedom to direct traffic based on the needs of the network.