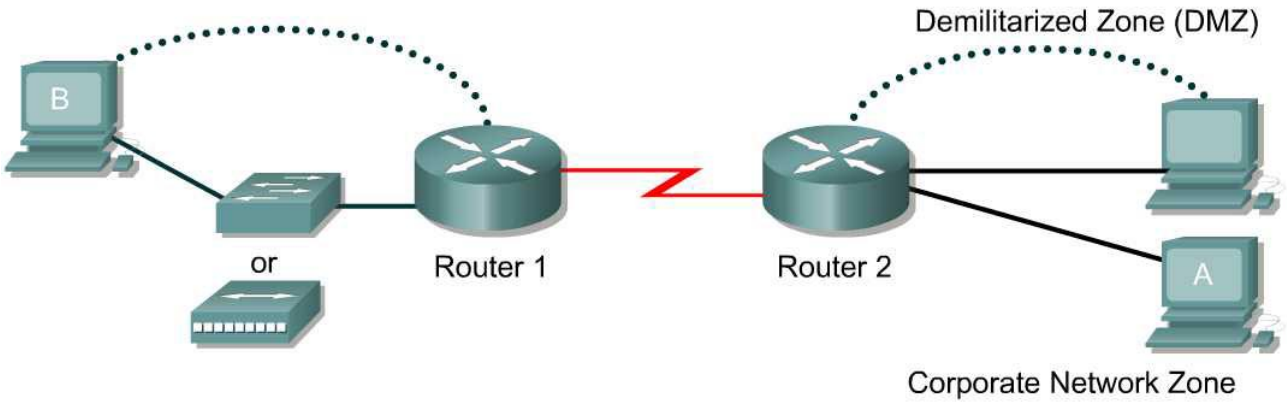
Simple DMZ Extended Access Lists



Straight-through cable	
Serial cable	
Console (Rollover)	
Crossover cable	

Router Designation	Router Name	Enable secret password	Enable, VTY and console password	Routing protocol	RIP network statements
Router 1	ISP	class	cisco	RIP	172.16.0.0
Router 2	GAD	class	cisco	RIP	10.0.0.0 172.16.0.0

Router Designation	IP host names	Fast Ethernet 0 Address	Interface type Serial 0	Serial 0 Address	Fast Ethernet 1 Address
Router 1	ISP	172.16.2.1/24	DTE	172.16.1.1/24	10.10.10.1 /24
Router 2	GAD	10.1.1.1 /24	DCE	172.16.1.2/24	

Host	IP Address	Subnet Mask	Gateway
Web Server	10.1.1.10	255.255.255.0	10.1.1.1
A	10.10.10.10	255.255.255.0	10.10.10.1
B	172.16.2.10	255.255.255.0	172.16.2.1

Objective

In this lab, the use extended access lists to create a simple DeMilitarized Zone (DMZ) will be learned.

Scenario

The BMTC is a small manufacturing company located in Gadsden. They have decided that they would like to create an awareness of their products over the Internet. Therefore their immediate requirement is to promote their products to potential customers by providing product overviews, reports, and testimonials. Future requirements could include e-mail, FTP, DNS, and online e-commerce services.

They have contracted you to design and configure a secure infrastructure to support their internal and external network requirements while maintaining fiscal responsibility which means “make it secure but keep costs down”.

After careful analysis, it is proposed to create a two-tier security architecture consisting of a corporate network zone and a DeMilitarized Zone (DMZ). The corporate network zone would house private servers and internal clients. The DMZ would house only one external server that would provide World Wide Web services. Although the one server creates a single point of failure, the service is only informational and not considered mission critical.

They liked the proposal and have signed a contract with to proceed.

Step 1 (Basic Router and Host Configurations)

a. Interconnect the routers and hosts as shown in the diagram. Configure all router basics such as hostname, router interfaces, and routing protocol. Use the preceding diagram and tables for reference.

The configurations on each router should similar to the following:

```
GAD#show running-config

<Output Omitted>

!
hostname GAD
!
interface FastEthernet0
 ip address 10.1.1.1 255.255.255.0
!
interface Serial0
 ip address 172.16.1.2 255.255.255.0
!
interface FastEthernet1
 ip address 10.10.10.1 255.255.255.0
!
router rip
 network 10.0.0.0
 network 172.16.0.0
!
GAD#


ISP#show running-config

<Output Omitted>

!
hostname ISP
!
interface FastEthernet0
 ip address 172.16.2.1 255.255.255.0
!
interface Serial0
 ip address 172.16.1.1 255.255.255.0
!
router rip
```

```
 network 172.16.0.0
!

ISP#
```

b. Configure the hosts with the appropriate information using the information previously defined.

c. To make the lab more realistic, web server software should be installed on the web server host. Examples include Microsoft IIS or Microsoft Personal Web Server (Windows 98). A third-party software such as TinyWeb Server (http://www.ritlabs.com/tinyweb/) can be used. If TinyWeb Server is used, it is recommended that TinyBox (http://people.freenet.de/ralph.becker/tinybox/) also be installed, which is a GUI front-end for TinyWeb Server.

   Be sure to create a default index.html page. The web page should include a message such as "Hello World". Save the page as instructed by the Web Server software.

d. Before applying any type of access list, it is important to verify reachability between systems.

   [ ] Verify reachability by pinging all systems and routers from each system.

   Can Host A ping Host B? _____

   Can Host A ping the Web Server? _____

   Can Host B ping Host A? _____

   Can Host B ping the Web Server? _____

   All hosts should be able to ping each other. Troubleshoot may have to be preformed if ping is not successful to some interfaces. Always verify the Physical layer connections, as they seem to be the more common source of connectivity problems. Next, verify the router interfaces. Make sure they are not shutdown, improperly configured, and that RIP is correctly configured. Finally, remember that along with valid IP addresses, hosts must also have default gateways specified.

e. On Host A, open a Web browser such as Windows Explorer or Netscape Navigator and enter the address of the Web Server in the address location.

   [ ] Verify that each Host has Web access to the Web Server.

   Can Host A view the index.html page? _____

   Can Host B view the index.html page? _____

   Both hosts should be able to view the index.html page in the Web Browser. Troubleshoot as necessary.

f. Now that the infrastructure is in place, it is time to begin securing the internetwork.

Step 2 Protect the Corporate Network

a. The corporate network zone houses private servers and internal clients. No other network should be able to access it.

b. Configure an extended access list to protect the corporate network. Protecting a corporate network begins by specifying which traffic can exit out the network. Although this may initially sound strange, it becomes clearer when it is known that most hackers are internal employees. The first access list will specify which network can exit out of the network.

   Enter the following:

```
GAD#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
GAD(config)#access-list 101 permit ip 10.10.10.0 0.0.0.255 any
GAD(config)#access-list 101 deny ip any any
```

The first line defines of access list “101” will only let valid corporate users on network 10.10.10.0 into the router. The second line is not really required because of the implicit deny all, but has been added for readability.

a. Now we need to apply the access list to corporate network interface.

   Enter the following:

```
GAD(config)#interface fa1
GAD(config-if)#ip access-group 101 in
```

b. Now it is necessary to test the access lists.

   [ ] Verify reachability by pinging all systems and routers from each system.

   Can Host A ping the Web Server? _____

   Can Host A ping Host B? _____

   Can Host B ping the Web Server? _____

   Can Host B ping Host A? _____

   All hosts should be able to ping any location.

c. Next, configure an outbound extended access list on the corporate network interface. Traffic entering the corporate network will be coming from either the Internet or the DMZ. For this reason which traffic can be allowed into the corporate network must be limited.

d. The first issue to address is to make sure that only traffic that originated from the corporate network can be allowed back into that network. Enter the following:

```
GAD(config)#access-list 102 permit tcp any any established
```

   The keyword **established** in this line only permits TCP traffic that originated from the 10.10.10.0 network.

e. To make network management and troubleshooting easier, it is also decided to permit ICMP into the network. This will allow the internal hosts to receive ICMP messages (e.g., ping messages).

   Enter the following:

```
GAD(config)#access-list 102 permit icmp any any echo-reply
GAD(config)#access-list 102 permit icmp any any unreachable
```

   The first line only allows successful pings back into the corporate network. The second line allows unsuccessful ping messages to be displayed.

f. At this time no other traffic is desired into the corporate network. Therefore enter the following:

```
GAD(config)#access-list 102 deny ip any any
```

g. Finally the access-list need to be applied to the corporate network Fast Ethernet port.

```
GAD(config)#interface fa 1
GAD(config-if)#ip access-group 102 out
```

h. Remember that an interface can support one incoming and one outgoing access list.

i. Use the **show access-lists** command to verify the syntax of the access lists. The output should be similar to the following:

```
GAD#show access-lists
Extended IP access list 101
    permit ip 10.10.10.0 0.0.0.255 any
    deny ip any any
Extended IP access list 102
    permit tcp any any established
    permit icmp any any echo-reply
    permit icmp any any unreachable
    deny ip any any
```

Access lists may have to deleted and re-entered if there is any discrepancy between the preceding output and the configuration.

j. Now access lists. Need to be tested.

[ ] Verify reachability by pinging all systems and routers from each system.

Can Host A ping the Web Server? _____

Can Host A ping Host B? _____

Can Host B ping the Web Server? _____

Can Host B ping Host A? _____

Host A should be able to ping all locations. However, no other host should be able to ping Host A.

k. On Host A, open a Web browser such as Windows Explorer or Netscape Navigator and enter the address of the Web Server in the address location.

[ ] Verify that Host A still has Web access to the Web Server.

Can Host A view the index.html page? _____

l. Host A should still be able to view the index.html page in the Web Browser. Troubleshoot as necessary.

m. The internal corporate network is now secure. Next we need to secure the DMZ network.

Step 3 Protect the DMZ Network

a. The internal corporate network is now secure. Next we need to secure the DMZ network.

b. The DMZ network will house only one external server that will provide World Wide Web services. Other services such as E-mail, FTP, and DNS will be implemented at a later time. Although the one server creates a single point of failure, the service is only informational and not considered mission critical.

c. Configure an extended access list to protect the DMZ network. Again, as with the corporate network, specify which traffic can exit the network and apply it to the interface.

Enter the following:

```
GAD#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
GAD(config)#access-list 111 permit ip 10.1.1.0 0.0.0.255 any
GAD(config)#access-list 111 deny ip any any

GAD(config)#interface f0
GAD(config-if)#ip access-group 111 in
```

d. Now test the new access lists.

[ ] Verify reachability by pinging all systems and routers from each system.

Can Host A ping the Web Server? _____

Can Host A ping Host B? _____

Can Host B ping the Web Server? _____

Can Host B ping Host A? _____

Host A should be able to ping all locations. However, no other host should be able to ping Host A

e. Next, an outbound extended access list is required to specify which traffic can enter the DMZ network. Traffic entering the DMZ network will be coming from either the Internet or the corporate network requesting World Wide Web services.

f. Configure an outbound extended access-list specifying that World Wide Web requests be allowed into the network. Enter the following:

```
GAD(config)#access-list 112 permit tcp any host 10.1.1.10 eq www
```

This line will allow World Wide Web services destined for the Web server into the DMZ network.

What command would be entered to allow DNS requests into the DMZ?

_____

What command would be entered to allow E-mail requests into the DMZ?

_____

What command would be entered to allow FTP requests into the DMZ?

_____

g. For management purposes, it would be useful to let corporate users **ping** the Web Server. However, Internet users should not be provided the same privilege. Add a line to the access list to allow only corporate users ICMP access into the DMZ network.

Enter the following:

```
GAD(config)#access-list 112 permit icmp 10.10.10.0 0.0.0.255 host
10.1.1.10
```

This line only allows hosts on the Corporate network to **ping** the Web Server. Although the configuration could be more restrictive with the ICMP options, it is not viewed as being necessary.

h. Other services could be permitted into the DMZ network in the future. However, at this time, no other traffic is to be permitted into the DMZ network. Therefore enter the following:

```
GAD(config)#access-list 112 deny ip any any
```

i. Apply the outbound access-list to the DMZ network Fast Ethernet port.

```
GAD(config)#interface fa 0
GAD(config-if)#ip access-group 112 out
```

j. To verify the syntax of the access lists, use the **show-access-lists** command. The output should be similar to the following:

```
GAD#show access-lists
```

```
Extended IP access list 101
    permit ip 10.10.10.0 0.0.0.255 any (70 matches)
    deny ip any any
Extended IP access list 102
    permit tcp any any established (8 matches)
    permit icmp any any echo-reply (12 matches)
    permit icmp any any unreachable
    deny ip any any (4 matches)
Extended IP access list 111
    permit ip 10.1.1.0 0.0.0.255 any (59 matches)
    deny ip any any
Extended IP access list 112
    permit tcp any host 10.1.1.10 eq www (29 matches)
    permit icmp 10.10.10.0 0.0.0.255 host 10.1.1.10 (4 matches)
    deny ip any any (14 matches)
```

The access lists may have to be deleted and re-entered if there is any discrepancy between the preceding output and the configuration.

k. The access lists now need to be tested.

[ ] Verify reachability by pinging all systems and routers from each system.

Can Host A ping the Web Server? _____

Can Host A ping Host B? _____

Can Host B ping the Web Server? _____

Can Host B ping Host A? _____

l. Only Host A should be able to ping all locations.

Use a Web browser such as Windows Explorer or Netscape Navigator on each host and enter the address of the Web Server in the address location.

[ ] Verify that the hosts still have Web access to the Web Server.

Can Host A view the index.html page? _____

Can Host B view the index.html page? _____

Both hosts should still be able to view the index.html page in the Web Browser. However, host B should not be able to ping the web server. Troubleshoot if necessary.

m. The DMZ network is now secure. Next, we need to configure our external interface to deter spoofing and hacking practices.

Step 4 Deter Spoofing

a. Networks are becoming increasingly prone to attacks from outside users. Hackers, crackers, and script kiddies are titles used to describe various individuals who maliciously try to break into networks or render networks incapable of responding to legitimate requests (Denial of Service (DoS) attacks). This has proven to be a troublesome for the Internet community.

b. You are well aware of the practices used by some of these hackers. A common method that they employ is to attempt to forge a valid internal source IP addresses. This practice is commonly known as “spoofing”.

c. To deter spoofing, it is decided to configure an access list so that Internet hosts cannot easily spoof an internal network addresses. Three common source IP addresses that hackers attempt to forge are valid internal addresses (e.g., 10.10.10.0), loopback addresses (i.e., 127.x.x.x), and multicast addresses (i.e., 224.x.x.x – 239.x.x.x).

d. Configure an inbound access list that will make it difficult for outside users to spoof internal addresses and apply it to the Serial 0 interface.

Enter the following:

```
GAD(config)#access-list 121 deny ip 10.10.10.0 0.0.0.255 any
GAD(config)#access-list 121 deny ip 127.0.0.0 0.255.255.255 any
GAD(config)#access-list 121 deny ip 224.0.0.0 31.255.255.255 any
GAD(config)#access-list 121 permit ip any any

GAD(config)#interface serial 0
GAD(config-if)#ip access-group 121 in
```

The first line will stop outside users from forging a valid source IP address. The second line stops them from using the loopback address range. The third line stops the practice of hackers using the multicast range of addresses (i.e., 224.0.0.0 – 239.255.255.255) to create unnecessary internal traffic.

e. Verify the syntax of the access lists with the **show-access-lists** command. The output should be similar to the following:

```
GAD#show access-lists
GAD#show access-lists
Extended IP access list 101
    permit ip 10.10.10.0 0.0.0.255 any (168 matches)
    deny ip any any
Extended IP access list 102
    permit tcp any any established (24 matches)
    permit icmp any any echo-reply (28 matches)
    permit icmp any any unreachable
    deny ip any any (12 matches)
Extended IP access list 111
    permit ip 10.1.1.0 0.0.0.255 any (122 matches)
    deny ip any any
Extended IP access list 112
    permit tcp any host 10.1.1.10 eq www (69 matches)
    permit icmp 10.10.10.0 0.0.0.255 host 10.1.1.10 (12 matches)
    deny ip any any (22 matches)
Extended IP access list 121
    deny ip 10.10.10.0 0.0.0.255 any
    deny ip 127.0.0.0 0.255.255.255 any
    deny ip 224.0.0.0 31.255.255.255 any
    permit ip any any (47 matches)
```

The access lists may have to be deleted and re-entered if there is any discrepancy between the preceding output and the configuration.

f. Finally, test if connectivity still exists.

[ ] Verify reachability by pinging all systems and routers from each system.

Can Host A ping the Web Server? _____

Can Host A ping Host B? _____

Can Host B ping the Web Server? _____

Can Host B ping Host A? _____

Only Host A should be able to ping all locations.

g. Use a Web browser such as Windows Explorer or Netscape Navigator on each host and enter the address of the Web Server in the address location.

[ ] Verify that the hosts still have Web access to the Web Server.

Can Host A view the index.html page? _____

Can Host B view the index.html page? _____

Both hosts should still be able to view the index.html page in the Web Browser. Troubleshoot as necessary.

h. The BMTC network is now secure.

Note: The preceding lab is a basic solution to providing a secure network. It is by no means intended to be a complete solution.

To properly protect enterprise networks, dedicated network devices such as Cisco PIX devices should be implemented. As well, advanced features such as Network Address Translation and advanced access lists options such as Reflexive access lists, Content Based Access Lists (CBAC), are strongly recommended and well beyond the scope of CCNA certification.

Finally, it is recommended that network administrators maintain strong relationships with their service providers to help when network security is compromised.

Step 7 Document the ACL

a. As a part of all network management, documentation needs to be created. Using the text file created for the configuration, add additional comments. This file should also contain output from the **`show access-list`** and the **`show ip interface`** commands.

b. The file should be saved with other network documentation. The file naming convention should reflect the function of the file and the date of implementation.

c. That should complete this extended ACL lab.

d. Once finished, erase the start-up configuration on routers, remove and store the cables and adapter. Also logoff and turn the router off.