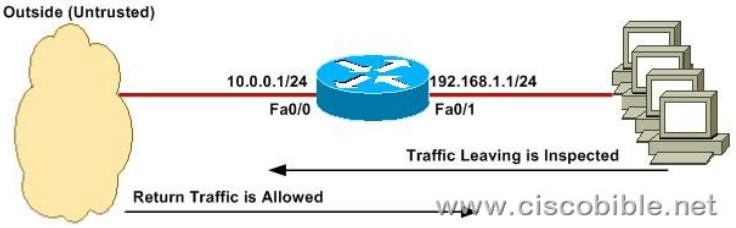
How to Configure the IOS Classic Firewall

The Cisco IOS Classic Firewall implements stateful inspection of traffic flow through the router. The router intercepts packets that it has been configured to intercept, and tracks the state of the packets and compares them against patterns of normal behavior. The IOS code understands the way that specific protocols operate, and IOS provides support for more than just TCP and User Datagram Protocol (UDP) packets. Cisco IOS Firewall offers services that operate at the application layer of the OSI model. The following application layer features are shown in Table 1, along with related configuration keywords that are implemented for the following protocols with IOS 12.4. We can split the configuration of the IOS Classic Firewall into three steps: **STEP 1** Configure the ACL to block traffic from the unsecure network. **STEP 2** Create the inspection rules. **STEP 3** Apply the ACL and inspection rule to an interface. We are going to base this configuration on below topogoly.



You can see from the topo that we have a router with the inside (trusted) IP address of 192.168.1.1/24. The outside (untrusted) IP address is 10.0.0.1/24. We are going to configure IOS Classic Firewall to protect the inside network from the outside network. Under this default configuration, traffic originating from the inside is inspected and return traffic allowed. No traffic originating from the outside will be allowed to access the inside. **Step 1: Configure the ACL to Block Traffic from the Unsecure Network** The first step is to configure an access list on the router to block all traffic from the outside (untrusted) network. In this example, we are not advertising any services to the outside network. Therefore, we can use a single ACL rule to deny all traffic Router(config)# access-list 120 deny ip any any The preceding syntax creates access list 120 that will deny all IP traffic from any source to any destination. We will apply this to the outside interface in Step 3. **Step 2: Create the Inspection Rules** Now that we have created the access list, the next step is to configure the inspection rules. Because we are using general Internet traffic through the router, we will enable protocol inspection for TCP, UDP, and ICMP. To achieve this, we have to create an inspection rule and configure it to inspect TCP, UDP, and ICMP: Router(config)# ip inspect name MYFW tcp Router(config)# ip inspect name MYFW udp Router(config)# ip inspect name MYFW icmp These three lines of configuration create an inspection rule called MYFW and configure TCP, UDP, and ICMP inspection. **Step 3: Apply the Inspection Rules to an Interface** Now that the access list and inspection rule has been configured, we need to apply them to an interface for the IOS Firewall to be effective. The general rule when applying access lists is to place the access list as near to the traffic as possible. This is also the same for the inspection rule. So, we need to apply the access list inbound on the outside (untrusted) network so that traffic is prevented from entering the interface. We also need to apply the inspection rule outbound on the inside (trusted) network so that the traffic destined for the outside network will be inspected. The following configuration applies the access list to the outside, fa0/0 interface: Router(config)# **interface fa0/0** Router(config-if)# ip access-group 120 out The following configuration applies the inspection rule we created in Step 2 to the inside, fa0/1 interface: Router(config)# interface fa0/1 Router(config-if)# ip inspect MYFW out The IOS Classic Firewall is now configured and will be operational. The IOS Firewall dynamically creates access list entries to access list 120. Use the following commands to verify and show the IOS Classic Firewall in operation: **show ip access-lists**   Shows a list of the ACL entries for the configured ACLs on the router **show ip inspect name** inspection-name   Displays information about the configured inspection rule **show ip inspect config**   Shows all IOS Classic Firewall configuration items **show ip inspect all**   Shows all IOS Classic Firewall configuration items and the existing state of the firewall and connections