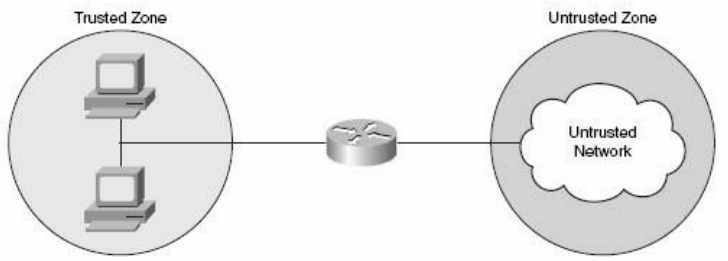
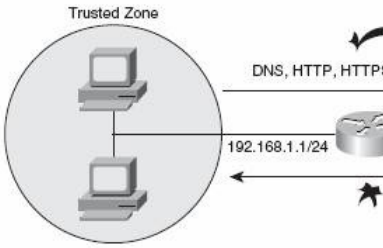
How to configure IOS Zone-Based Firewall

Cisco introduced IOS Zone-Based Firewalling (ZFW) in Cisco IOS 12.4(6)T. Cisco announced that their strategic direction for IOS firewalling is going to be with Zone-Based Firewalling. They will continue to support Classic IOS Firewall, but all the new developments will be through Zone-Based Firewalling. Zone-Based Firewall changes the IOS stateful inspection model from Classic Firewall's interface-based model to a more flexible, easier-understood zone-based configuration model. Router interfaces are assigned to security zones, and a firewall inspection policy is applied to traffic moving between the zones. Zone-Based Firewall enforces a secure interzone policy by default, such that a given interface cannot pass traffic to interfaces in other security zones until an explicit policy allowing traffic is defined. Firewall policies are configured using Cisco Common Classification Policy Language (C3PL), which uses a hierarchical structure to define inspection for network protocols and the groups of hosts' traffic to which inspection will be applied. Interzone policies offer considerable flexibility and granularity, so different inspection policies can be applied to hosts, host groups, or subnets connected to the same router interface. Figure 3 shows a sample network with two security zones.



After zones have been configured, interfaces are placed into these zones. Remember a few important rules when working with zones: - Traffic flows freely between interfaces that are not in configured zones. This is the same as normal router operation. - Traffic will never flow between an interface in a zone and an interface not in a zone. - Traffic will flow between interfaces in different zones as long as the configured policy allows it. The default is to deny all. We are now going to look at the configuration of Zone-Based Firewalls. Zone-Based Firewall configuration uses the familiar class map and policy map framework similar to quality of service (QoS) and network protection framework configuration. Cisco are migrating a lot of their technologies fit this configuration framework. We are going to use a simple network topology, as shown in Figure 4.



You can see from Figure 4 that we have a router with two security zones. The inside (trusted zone) IP address is 192.168.1.1/24. The outside (untrusted zone) IP address is 10.0.0.1/24. The untrusted zone would normally be the Internet or any other public and untrusted network that you may connect to. The trusted zone wants to access services that exist in the untrusted zone. These are general Internet type services, so we need to allow access for DNS, HTTP, HTTPS, SMTP, and ICMP. We are not allowing any services from the untrusted zone to access the trusted zone. There are four required steps to configure a Zone-Based Firewall: STEP 1 Define class maps that permit traffic between zones. STEP 2 Configure a policy map to inspect the traffic on the class map. STEP 3 Configure the required zones and assign interfaces to the required zones. STEP 4 Configure the zone pair and apply the policy map. Step 1: Define Class Maps That Permit Traffic Between zones The first step is the most important step because it is here you have to do the work to decide the policy you are going to configure in the later steps. You need to decide which interfaces are going to be in which zones and what traffic is required between these zones. For our example, we want to permit DNS, HTTP, HTTPS, SMTP, and ICMP from the trusted to the untrusted zone. We define this in a class map that we will call trusted-allowed: Router(config)# **class-map type inspect match-any TRUSTED-ALLOWED** Router(config-cmap)# **match protocol http** Router(config-cmap)# **match protocol https** Router(config-cmap)# **match protocol dns** Router(config-cmap)# **match protocol smtp** Router(config-cmap)# **match protocol icmp** We now have configured a class map called trusted-allowed that defines the list of services in the firewall policy. Step 2: Configure a Policy Map to Inspect the Traffic on the Class Map After we have configured

the class map, the next action is to configure the policy map to inspect the traffic we have just defined in the class map. We are going to create a policy map called trusted-policy: Router(config)# **policy-map type inspect TRUSTED-POLICY** Router(config-pmap)# **class type inspect TRUSTED-ALLOWED** Router(config-pmap-c)# **inspect** We have now tied the trusted-allowed class map to the trusted-policy policy map. The next step is to create the zones to use in the configuration. Step 3: Configure the Required Zones and Assign Interfaces to the Required Zones Now that the class map has been applied to the policy map, the next step it to configure the security zones and place the required interfaces into the correct zones. Let's start by creating two security zones: one called trusted and one called untrusted. We are going to give each a meaningful description: Router(config)# **zone security trusted** Router(config-sec-zone)# **description trusted inside security zone** Router(config-sec-zone)# **exit** Router(config)# **zone security untrusted** Router(config-sec-zone)# **description untrusted outside security zone** We now have two security zones, trusted and untrusted, configured on the router. The next step is to put the correct interfaces into the correct security zones. Refer to Figure 4. You can see that fa0/0 is the untrusted interface and fa0/1 is the trusted interface. The configuration is as follows: Router(config)# **interface fa0/0** Router(config-if)# **zone-member security untrusted** Router(config-if)# **exit** Router(config)# **interface fa0/1** Router(config-if)# **zone-member security trusted** We have now configured the two security zones and placed interface fa0/0 into the untrusted security zone and interface fa0/1 into the trusted security zone. Step 4: Configure the Zone Pair and Apply the Policy Map The last configuration step for Zone-Based Firewalls is to configure the zone pair. The zone pair defines the flow of traffic and the policy map to apply to the flow. This is the final step that brings together the previous configuration steps to enable Zone-Based Firewalling: Router(config)# **zone-pair security trusted-untrusted source trusted destination untrusted** Router(config-sec-zone-pair)# **service-policy type inspect trusted-policy** The first line of the configuration creates a zone pair called trusted-untrusted. This name has been given to it because it defines the actions from the trusted to the untrusted security zone. We define the source and the destination. The source is the trusted network, and the destination is the untrusted network. The second line of the configuration ties in the policy map called trusted-policy that we created at Step 2 with the zone pair. The configuration of the Zone-Based Firewall is now complete. To verify the Zone-Based Firewall, you can use the following commands in addition to the usual commands for displaying class map and policy map information: **show zone security** Shows information about the configured security zones **show zone-pair security** Shows information about the configured zone pairs