***Section 1: Creating and Modifying a Class Map for Web Traffic Inspection***

These commands define a **class-map** to match **HTTP, HTTPS, and DNS protocols** for firewall inspection using Cisco's ZPF (Zone-Based Policy Firewall).

|  |  |
| --- | --- |
| **Router(config)#** | **class-map type inspect match-any Web-Traffic** |
| **Router(config-cmap)#** | **match protocol http** |
| **Router(config-cmap)#** | **match protocol https** |
| **Router(config-cmap)#** | **match protocol dns** |
| **Router(config-cmap)#** | **exit** |

***Section 2: Creating a Policy Map and Assigning a Class***

This section defines a **policy-map** named PRIV-PUB-POLICY and binds it to the previously created class Web-Traffic.

|  |  |
| --- | --- |
| **Router(config)#** | **policy-map type inspect PRIV-PUB-POLICY** |
| **Router(config-pmap)#** | **class type inspect Web-Traffic** |
| **Router(config-pmap-c)#** | **inspect** |
| **Router(config-pmap)#** | **exit** |
| **Router(config)#** | **exit** |

***Section 3: Creating Zone Pairs and Binding Policy***

This section configures a **zone-pair** from a Private zone to a Public zone and applies the policy map to it.

|  |  |
| --- | --- |
| **Router(config)#** | **zone-pair security Private-to-Public-Traffic** |
| **Router(config-sec-zone-pair)#** | **source Private** |
| **Router(config-sec-zone-pair)#** | **destination Public** |
| **Router(config-sec-zone-pair)#** | **service-policy type inspect PRIV-PUB-POLICY** |
| **Router(config-sec-zone-pair)#** | **exit** |

***Section 4: Assigning Interfaces to Zones***

This section assigns physical interfaces to the Private and Public zones.

|  |  |
| --- | --- |
| **Router(config)#** | **interface GigabitEthernet0/0** |
| **Router(config-if)#** | **zone-member security Private** |
| **Router(config)#** | **interface GigabitEthernet0/1** |
| **Router(config-if)#** | **zone-member security Public** |

***Section 5: Cleaning Up Existing Configurations***

This part removes previously created firewall class-maps, policy-maps, zones, and zone-pairs. It’s typically done when **restarting or troubleshooting** a ZPF setup.

|  |  |
| --- | --- |
| **Router(config)#** | **no class-map type inspect match-any Web-Traffic** |
| **Router(config)#** | **no policy-map type inspect PRIV-PUB-POLICY** |
| **Router(config)#** | **no zone security Private** |
| **Router(config)#** | **no zone security Public** |
| **Router(config)#** | **no zone-pair security Private-to-Public-Traffic source Private destination Public** |
| **Router(config)#** | **no zone-member security Private** |
| **Router(config)#** | **no zone-member security Public** |

***Section 6: Recreating Class Map from Scratch***

These commands show how to **redefine the class map** again after cleanup.

|  |  |
| --- | --- |
| **Router(config)#** | **class-map type inspect match-any Web-Traffic** |
| **Router(config-cmap)#** | **match protocol http** |
| **Router(config-cmap)#** | **match protocol https** |
| **Router(config-cmap)#** | **match protocol dns** |
| **Router(config-cmap)#** | **exit** |

***Section 7: Rebuilding Policy Map and Interface Bindings***

This continues the process by **recreating the policy**, reassigning it to **interfaces**, and adjusting **interface settings** like IP address, duplex, and speed.

|  |  |
| --- | --- |
| **Router(config)#** | **policy-map type inspect PRIV-PUB-POLICY** |
| **Router(config-pmap)#** | **class type inspect Web-Traffic** |
| **Router(config-pmap-c)#** | **inspect** |
| **Router(config-if)#** | **duplex auto** |
| **Router(config-if)#** | **speed auto** |
| **Router(config)#** | **interface GigabitEthernet0/0/1** |
| **Router(config-if)#** | **ip address 10.1.1.1 255.255.255.0** |

***Section 8: Configuring an Extended Access List and Matching It in a Class Map***

This part defines a **named access list** allowing specific traffic from 10.1.1.4 to 192.168.1.100, then creates a **class-map** that matches this access group.

|  |  |
| --- | --- |
| **Router(config)#** | **ip access-list extended ext-int** |
| **Router(config-ext-nacl)#** | **permit tcp host 10.1.1.4 host 192.168.1.100 eq 80** |
| **Router(config-ext-nacl)#** | **permit tcp host 10.1.1.4 host 192.168.1.100 eq 443** |
| **Router(config-ext-nacl)#** | **permit tcp host 10.1.1.4 host 192.168.1.100 eq ftp** |
| **Router(config-ext-nacl)#** | **permit icmp host 10.1.1.4 host 192.168.1.100** |
| **Router(config)#** | **class-map type inspect match-all 10-1-1-4** |
| **Router(config-cmap)#** | **match access-group name ext-int** |

***Section 9: Defining a Policy Map to Inspect Access-List-Based Traffic***

Now we define a **policy-map** named pub-priv that inspects traffic matching the access-list-based class-map.

|  |  |
| --- | --- |
| **Router(config)#** | **policy-map type inspect pub-priv** |
| **Router(config-pmap)#** | **class type inspect 10-1-1-4** |
| **Router(config-pmap-c)#** | **inspect** |

***Section 10: Creating Zone-Pair PUBLIC-PRIVATE and Applying Policy***

Creates a zone-pair named PUBLIC-PRIVATE, linking the policy to it.

|  |  |
| --- | --- |
| **Router(config)#** | **zone-pair security PUBLIC-PRIVATE source Public destination Private** |
| **Router(config-sec-zone-pair)#** | **service-policy type inspect pub-priv** |