Zone-based policy firewall (also known as “Zone-Policy Firewall” or “ZPF”) changes the firewall from the older interface-based model to a more flexible, more easily understood zone-based configuration model. Interfaces are assigned to zones, and an inspection policy is applied to traffic moving between the zones. Inter-zone policies offer considerable flexibility and granularity, so different inspection policies can be applied to multiple host groups connected to the same router interface.

Firewall policies are configured with the Cisco Common Classification Policy Language (C3PL), which employs a hierarchical structure to define inspection for network protocols and the groups of hosts to which the inspection will be applied.

For a good description of how Zone-Based Policy Firewall can be implemented, read The Zone-Based Policy Firewall Design Guide available on cisco.com by going to Support > Product Support > Cisco IOS Software > Cisco IOS Software Releases 12.4 Mainline > Configure > Feature Guides and clicking Zone-Based Policy Firewall Design Guide. This document may also be available at the following link:


Configuration Task Order

The following task order can be followed to configure a Zone-Based Policy Firewall:

1. Define zones.
2. Define zone-pairs.
3. Define class-maps that describe traffic that must have policy applied as it crosses a zone-pair.

4. Define policy-maps to apply action to your class-map’s traffic.

5. Apply policy-maps to zone-pairs.

6. Assign interfaces to zones.

The sequence of tasks is not important, but some events must be completed in order. For instance, you must configure a class-map before you assign a class-map to a policy-map. Similarly, you cannot assign a policy-map to a zone-pair until you have configured the policy. If you try to complete a task that relies on another portion of the configuration that you have not configured, SDM does not allow you to do so.

## Zone Window

A zone, or security zone, is a group of interfaces to which a security policy can be applied. The interfaces in a zone should share common functions or features. For example, two interfaces that are connected to the local LAN might be placed in one security zone, and the interfaces connected to the Internet might be placed in another security zone.

For traffic to flow among all the interfaces in a router, all the interfaces must be a member of one security zone or another. It is not necessary for all router interfaces to be members of security zones.

Zone-based Policy General Rules describes the rules governing interface behavior and the flow of traffic between zone-member interfaces.

This window displays the name of each security zone, the interfaces that it contains, and any associated zone pairs that the zone is a member of. A zone can be a member of multiple zone pairs.

Click **Add** to create a new zone.

Click **Edit** to choose different interfaces for an existing zone.

Click **Delete** to remove a zone. A zone that is a member of a zone pair cannot be deleted.
Add or Edit a Zone

To add a new zone, also called a security zone, enter a zone name, and choose the interfaces that are to be included in the zone. The Interface list displays the names of available interfaces. Because physical interfaces can be placed in only one zone, they do not appear in the list if they have already been placed in a zone. Virtual interfaces, such as Dialer interfaces or Virtual Template interfaces can be placed in multiple zones and will always appear in the list.

- Traffic flowing to or from this interface is governed by the policy map associated with the zone.
- An interface that you associate with this zone may be used for a site-to-site VPN, DMVPN, Easy VPN, SSL VPN or other type of connection whose traffic might be blocked by a firewall. When you associate an interface with a zone in this dialog, SDM does not create any passthrough ACL to permit such traffic. You can configure the necessary passthrough for the policy map two ways.
  - Go to Configure > Firewall and ACL > Edit Firewall Policy > Rule for New Traffic. In the displayed dialog, provide the source and destination IP address information, and the type of traffic that must be allowed to pass through the firewall. In the Action field, select Permit ACL.
  - Go to Configure > C3PL > Policy Map > Protocol Inspection. Provide a protocol inspection policy map that will allow the necessary traffic to pass through the firewall.

After a zone has been created, you can change the interfaces associated with the zone, but you cannot change the name of the zone.

Zone-Based Policy General Rules

Router network interfaces’ membership in zones is subject to several rules governing interface behavior, as is the traffic moving between zone member interfaces:

- A zone must be configured before interfaces can be assigned to the zone.
An interface can be assigned to only one security zone.

All traffic to/from a given interface is implicitly blocked when the interface is assigned to a zone, excepting traffic to/from other interfaces in the same zone, and traffic to any interface on the router.

Traffic is implicitly allowed to flow by default among interfaces that are members of the same zone.

To permit traffic to/from a zone member interface, a policy allowing or inspecting traffic must be configured between that zone and any other zone.

The self zone is the only exception to the default deny-all policy. All traffic to any router interface is allowed until traffic is explicitly denied.

Traffic cannot flow between a zone member interface and any interface that is not a zone member.

Pass, inspect, and drop actions can only be applied between two zones.

Interfaces that have not been assigned to a zone function as classical router ports and might still use classical stateful inspection/CBAC configuration.

If it is required that an interface on the box not be part of the zoning/firewall policy, it might still be necessary to put that interface in a zone and configure a pass all policy (sort of a dummy policy) between that zone and any other zone to which traffic flow is desired.

From the preceding it follows that, if traffic is to flow among all the interfaces in a router, all the interfaces must be part of the zoning model (each interface must be a member of one zone or another).

The only exception to the preceding deny by default approach is the traffic to/from the router, which will be permitted by default. An explicit policy can be configured to restrict such traffic.

This set of rules was taken from *The Zone-Based Policy Firewall Design Guide* available at the following link:

Zone Pairs

A zone-pair allows you to specify a unidirectional firewall policy between two security zones. The direction of the traffic is specified by specifying a source and destination security zone. The same zone cannot be defined as both the source and the destination.

If you want traffic to flow in both directions between two zones, you must create a zone pair for each direction. If you want traffic to flow freely among all interfaces, each interface must be configured in a zone.

The following table shows an example of four zone-pairs.

<table>
<thead>
<tr>
<th>Zone Pair</th>
<th>Source</th>
<th>Destination</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN-out</td>
<td>zone-VLAN1</td>
<td>zone-FE1</td>
<td>inspection-policymap-a</td>
</tr>
<tr>
<td>LAN-in</td>
<td>zone-FE1</td>
<td>zone-VLAN1</td>
<td>inspection-policymap-b</td>
</tr>
<tr>
<td>Bkup-out</td>
<td>self</td>
<td>zone-BRI0</td>
<td>inspection-policymap-c</td>
</tr>
<tr>
<td>Bkup-in</td>
<td>zone-BRI0</td>
<td>self</td>
<td>inspection-policymap-c</td>
</tr>
</tbody>
</table>

LAN-out and LAN-in are zone-pairs configured for traffic flowing between the LAN interface, VLAN1, and the FastEthernet 1 interface. Each zone-pair is controlled by a separate policy. Bkup-out and Bkup-in are configured for traffic generated by the router. The same policy controls traffic sent from zone-BRI0 as traffic sent by the router, represented by the self zone.

Click Add to create a zone-pair.

Click Edit to change the policy associated with a zone pair.

Click Delete to remove a zone pair.

Add or Edit a Zone Pair

To configure a new zone pair, provide a name for the zone pair, a source zone from which traffic will originate, a destination zone to which traffic is to be sent, and the policy that is to determine which traffic can be sent across the zones. The source zone and destination zone lists contain the zones configured on the router and the self zone. The self zone can be used when you are configuring zone pairs.
for traffic originating from the router itself, or destined for the router itself, such as a zone pair configured for SNMP traffic. The Policy list contains the name of each policy map configured on the router.

If you are editing a zone pair, you can change the policy map, but you cannot change the name or the source or destination zones.

**Add a Zone**

You can configure an interface as a member of a security zone from the Interfaces and Connections Association tab. The zone that you add will include the interface that you are editing as a zone member.

- **Note**

  - Traffic flowing to or from this interface is governed by the policy map associated with the zone.

  - An interface that you associate with this zone may be used for a site-to-site VPN, DMVPN, Easy VPN, SSL VPN or other type of connection whose traffic might be blocked by a firewall. When you associate an interface with a zone in this dialog, SDM does not create any passthrough ACL to permit such traffic. You can configure the necessary passthrough for the policy map two ways.

    - Go to Configure > Firewall and ACL > Edit Firewall Policy > Rule for New Traffic. In the displayed dialog, provide the source and destination IP address information, and the type of traffic that must be allowed to pass through the firewall. In the Action field, select Permit ACL.

    - Go to Configure > C3PL > Policy Map > Protocol Inspection. Provide a protocol inspection policy map that will allow the necessary traffic to pass through the firewall.

**Zone Name**

Enter the name of the zone that you want to add.
Select a Zone

If a security zone has been configured on the router, you can add the interface that you are configuring as a member of that zone.

Select a Zone for the Interface

Select the zone that you want to include the interface in, and click OK.