

## Terminology

### Security Zone

A group of interfaces which share a common level of security

### Zone Pair

A unidirectional pairing of source and destination zones to which a security policy is applied

### Inspection Policy

An inspect-type policy map used to statefully filter traffic by matching one or more inspect-type class maps

### Parameter Map

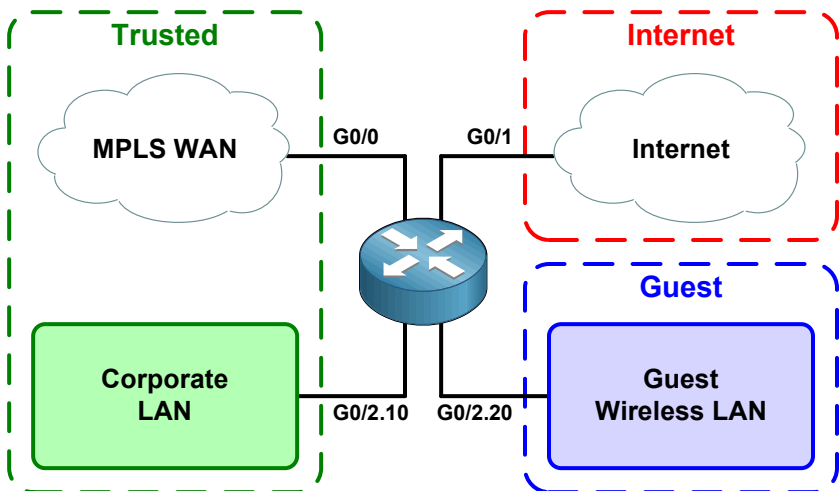
An optional configuration of protocol-specific parameters referenced by an inspection policy

## Inspection Class Configuration

```
! Match by protocol
class-map type inspect match-any ByProtocol
match protocol tcp
match protocol udp
match protocol icmp
```

```
! Match by access list
ip access-list extended MyACL
permit ip 10.0.0.0 255.255.0.0 any
!
class-map type inspect match-all ByAccessList
match access-group name MyACL
```

## Security Zones



## Parameter Map Configuration

```
parameter-map type inspect MyParameterMap
alert on
audit-trail off
dns-timeout 5
max-incomplete low 20000
max-incomplete high 25000
icmp idle-time 3
tcp synwait-time 3
```

## Inspection Policy Actions

- Drop** Traffic is prevented from passing
- Pass** Traffic is permitted to pass without stateful inspection
- Inspect** Traffic is subjected to stateful inspection; legitimate return traffic is permitted in the opposite direction

## Inspection Policy Configuration

```
policy-map type inspect MyInspectionPolicy
! Pass permitted stateless traffic
class VPN-Tunnel
pass
! Inspect permitted stateful traffic
class Allowed-Traffic1
inspect
! Stateful inspection with a parameter map
class Allowed-Traffic2
inspect MyParameterMap
! Drop and log unpermitted traffic
class class-default
drop log
```

! Defining security zones

```
zone security Trusted
zone security Guest
zone security Internet
```

! Assigning interfaces to security zones

```
interface GigabitEthernet0/0
zone-member security Trusted
!
interface GigabitEthernet0/1
zone-member security Internet
!
interface GigabitEthernet0/2.10
zone-member security Trusted
!
interface GigabitEthernet0/2.20
zone-member security Guest
```

## Zone Pair Configuration

```
! Service policies are applied to zone pairs
zone-pair security T2I source Trusted destination Internet
service-policy type inspect Trusted2Internet
```

```
zone-pair security G2I source Guest destination Internet
service-policy type inspect Guest2Internet
```

```
zone-pair security I2T source Internet destination Trusted
service-policy type inspect Internet2Trusted
```

## Troubleshooting

- show zone security
- show zone-pair security
- show policy-map type inspect
- show class-map type inspect
- show parameter-map type inspect
- debug zone security events