Revised: October 30, 2026

Firewall for Cisco 8000 Series Secure Routers using Cisco Meraki Dashboard

Feature history for firewall

Table 1: Feature history: Firewall

Feature Name	Release	Feature Information
Firewall	Cisco IOS XE 26.2.1 Release	This feature provides the ability to configure Layer 3 outbound and inbound firewall rules, as well as Layer 7 firewall rules, to allow, inspect or deny traffic based on traffic type. From this release, Cisco 8000 Series Secure Routers can be configured for firewall feature using Cisco Meraki Dashboard.

Firewall

On IOS-XE networks, firewall rules are mapped to Zone-Based Firewall (ZBFW).

- ZBFW uses zones, zone pairs, class maps, and policy maps.
- The Cisco Meraki Dashboard does not expose zones to customers.
- IOS-XE places interfaces into built-in zones and applies the generated security policy to the appropriate zone pair.

Firewall supports L3 and L7 rule enforcement.

L3 firewall rules

- Outbound firewall rules
- Inbound firewall rules when No NAT is enabled
- Policy: Deny or Allow
- Protocol: TCP, UDP, ICMPv4, or Any
- Source address: IPv4 CIDR and port
- Destination address: IPv4 CIDR, port, and FQDN for outbound rules only
- Syslog per rule
- Rule description

L7 firewall rules

- Blocking destination traffic based on NBAR ID
- Traffic to or from a list of countries
- Traffic not to or from a list of countries

Benefits of firewall

- You can configure L3 outbound, L3 inbound, and L7 firewall rules from the Dashboard.
- Rules can enforce traffic based on 5-tuple values: source IP, destination IP, source port, destination port, and protocol.
- Rules can also enforce traffic based on application using NBAR.
- The reserved `any` zone reduces the number of generated zone pairs needed to represent Dashboard firewall intent on IOS-XE.

Prerequisites for firewall

- Firewall is enabled by default.

Restrictions for firewall

- Firewall refers to L3 and L7 rules, not IPS or IDS.
- Inbound firewall rules are supported when No NAT is enabled.
- FQDN is supported on the destination field for outbound firewall rules only.
- FQDN ZBFW rules are not supported.
- Custom applications are not supported.
- Cellular failover rulesets and cellular inbound firewall rulesets are blocked on XE networks.
- Policy object and VLAN object features are blocked on XE networks.
- Firewall logging is not supported.

Configure firewall

Use one of these methods to configure firewall:

- Firewall configurations using Cisco Meraki Dashboard
- Firewall configurations on Cisco Secure Routers

Configure firewall from Cisco Meraki Dashboard

For information on firewall settings on Cisco Meraki Dashboard, refer to MX Firewall Settings.

From the Cisco Meraki Dashboard, choose **Security & SD-WAN** > **Configure** > **Firewall**.

On this page you can configure Layer 3 and Layer 7 outbound firewall rules.

Firewall configuration on Cisco Secure Routers

Note

The router configurations are not manually set on the router, instead, all the configurations are automatically pushed from the Cisco Meraki cloud.

Security zones and zone pairs

```
zone security zone-lan-cloud-default-vrf
zone security zone-wan
zone security zone-vpn
interface Vlan10
 zone-member security zone-lan-cloud-default-vrf
!
interface GigabitEthernet0/0/2
 zone-member security zone-wan
!
interface Virtual-Template1
 zone-member security zone-vpn
zone-pair security ZP_LAN_TO_ANY \
 source zone-lan-cloud-default-vrf destination any
 service-policy type inspect OUTBOUND-FW-POLICY
zone-pair security ZP_VPN_TO_ANY \
 source zone-vpn destination any
 service-policy type inspect OUTBOUND-FW-POLICY
```

Inbound firewall objects

```
! !inbound firewall rules
INBOUND_FIREWALL_OBJ_GRP-<UUID>
INBOUND-FW-ACL-RULE-<UUID>
INBOUND-FW-RULE-CLASS-MAP-1
INBOUND-FW-POLICY
ZP_WAN_TO_ANY
```

L3 rule translation

!allow tcp src 20.1.0.0/16 dst 10.0.0.0/24

!deny udp any dst 1.1.1.0/24 logging enabled

!default allow any

Generated object groups and ACLs:

```
!! Generated address and protocol object groups
!
object-group network FIREWALL_OBJ_GRP-<SRC-RULE1-UUID>
 description Generated source addresses object-group
 20.1.0.0 255.255.0.0
!
object-group network FIREWALL_OBJ_GRP-<DST-RULE1-UUID>
 description Generated destination addresses object-group
 10.0.0.0 255.255.255.0
!
object-group network FIREWALL_OBJ_GRP-<DST-RULE2-UUID>
 description Generated destination addresses object-group
 1.1.1.0 255.255.255.0
```

```
!
object-group service FIREWALL_OBJ_GRP-<UDP-UUID>
 description Generated source port object-group
 udp
!
! Rule 1 classification ACLs
!
ip access-list extended FIREWALL-ACL-<RULE1-NETWORK-UUID>
 10 permit ip object-group FIREWALL_OBJ_GRP-<SRC-RULE1-UUID> \
  object-group FIREWALL_OBJ_GRP-<DST-RULE1-UUID>
!
! Rule 2 classification ACLs
!
ip access-list extended FIREWALL-ACL-<RULE2-PROTOCOL-UUID>
 10 permit object-group FIREWALL_OBJ_GRP-<UDP-UUID> any any
!
ip access-list extended FIREWALL-ACL-<RULE2-NETWORK-UUID>
 10 permit ip any object-group FIREWALL_OBJ_GRP-<DST-RULE2-UUID>
!
! Automatically appended outbound default-allow classification
!
ip access-list extended FIREWALL-ACL-<DEFAULT-UUID>
 10 permit ip any any
!
```

Class maps and policy map

```
! One ordered class map per Dashboard rule
!
class-map type inspect match-all OUTBOUND-FW-RULE-CLASS-MAP-1
 match access-group name FIREWALL-ACL-<RULE1-PROTOCOL-UUID>
 match access-group name FIREWALL-ACL-<RULE1-NETWORK-UUID>
!
class-map type inspect match-all OUTBOUND-FW-RULE-CLASS-MAP-2
 match access-group name FIREWALL-ACL-<RULE2-PROTOCOL-UUID>
 match access-group name FIREWALL-ACL-<RULE2-NETWORK-UUID>
!
class-map type inspect match-all OUTBOUND-FW-RULE-CLASS-MAP-3
 match access-group name FIREWALL-ACL-<DEFAULT-UUID>
!
! Dashboard allow becomes inspect; deny becomes drop
!
policy-map type inspect optimized OUTBOUND-FW-POLICY
 class type inspect OUTBOUND-FW-RULE-CLASS-MAP-1
  inspect
 class type inspect OUTBOUND-FW-RULE-CLASS-MAP-2
  drop log
 class type inspect OUTBOUND-FW-RULE-CLASS-MAP-3
  inspect
!
```

L7 configuration

```
!L7 Firewall rules
class-map type inspect match-any L7-FW-CLASS-MAP-1
 match protocol <application-1>
 ...
 match protocol <application-32>
!
class-map type inspect match-any L7-FW-CLASS-MAP-2
 match protocol <application-33>
 match protocol <application-34>
policy-map type inspect OUTBOUND-FW-POLICY
```

```
 class type inspect L7-FW-CLASS-MAP-1
  drop
 class type inspect OUTBOUND-FW-RULE-CLASS-MAP-1
  inspect
 class type inspect OUTBOUND-FW-RULE-CLASS-MAP-2
  drop log
 class type inspect OUTBOUND-FW-RULE-CLASS-MAP-3
  inspect
```

Verify firewall

Use the following commands to verify zone, zone-pair, policy-map, session, ACL, and logging state:

Verify security zones

```
Device# show zone security
zone VPN_2_zone 1
 Member Interfaces:
    TenGigabitEthernet0/0/2
```

Verify zone pairs

```
Device# show zone-pair security
Zone-pair name lananyzone 5
    Source-Zone VPN_2_zone  Destination-Zone any
    service-policy LANANYPOLICY
```

Verify access lists

```
Device# show access-lists ACL-NEG-DST-ONLY
Extended IP access list ACL-NEG-DST-ONLY
    10 permit icmp any any (14 matches)
    15 permit tcp 10.20.24.0 0.0.0.255 any eq www (13 matches)
    21 permit tcp host 10.20.25.16 object-group OG-NEG-DST-ONLY eq 22
    35 permit object-group zbfw_newtest object-group OUTBOUND-FW-SRC-NETWORK-OBJ-GRP-1 any
```

Verify policy-map inspection

```
Device# show policy-map type inspect zone-pair
 Zone-pair: lananyzone
 Service-policy inspect : LANANYPOLICY
    Class-map: CM-NEG-DST-ONLY (match-all)
      Match: access-group name ACL-NEG-DST-ONLY
      Inspect
        Packet inspection statistics [process switch:fast switch]
        icmp packets: [0:42]
        http packets: [0:160]
        Session creations since subsystem startup or last reset 81
        Current session counts (estab/half-open/terminating) [1:0:0]
        Maxever session counts (estab/half-open/terminating) [1:0:0]
        Last session created 00:00:21
        Last statistic reset 00:04:46
        Last session creation rate 12
        Last half-open session total 0
    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
```

Verify sessions

Session verification output:

```
Device# show policy-map type inspect zone-pair sessions
  Zone-pair: lananyzone
  Service-policy inspect : LANANYPOLICY
    Class-map: CM-NEG-DST-ONLY (match-all)
      Match: access-group name ACL-NEG-DST-ONLY
      Inspect
        Established Sessions
         Session ID 0x0000006D (10.20.24.150:8)=>(10.1.15.254:22074) icmp/ping SIS_OPEN
          Created 00:00:11, Last heard 00
          Bytes sent (initiator:responder) [616:616]
    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
```