



Configuring and Managing Cisco FirePOWER Devices

Cisco FirePOWER Next-Generation IPS

Ahmed Sultan
Senior Network Security Engineer
ahmedsultan.me/about

Registration Configuration on the Management Center

Add Device ? X

Host:

Registration Key:

Group: ▼

Access Control Policy: ▼

Licensing

Protection: ☐

Control: ☐

Malware: ☐

URL Filtering: ☐

VPN: ☐

SSL: ☐

▲ **Advanced**

Unique NAT ID:

Transfer Packets: ☒

Host or NAT ID is required.

Register Cancel

Registration Configuration on the Management Center (Cont.)

Name	License Type	Health Policy	System Policy	Access Control Policy	
4 📁 Ungrouped (2)					
✓ 192.168.111.10 192.168.111.10 - Virtual Device 64bit - v5.4.0	Protection, Control, M...	None	Initial System Policy 2015-01	Default Intrusion Prevention	✓ ✎ 📄
✓ 192.168.111.40 192.168.111.40 - 3D8140 - v5.4.0	Protection, Control, M...	None	Initial System Policy 2015-01	Default Intrusion Prevention	✓ ✎ 📄

Interfaces Tab

192.168.111.40

3D8140

Apply Changes

Device

Interfaces



Inline Sets

Virtual Switches

Virtual Routers

Add...



Name	Security Zone	Used By	MAC Add...	IP Addresses	
 s1p1	Internal	Default Inline Set			
 s1p2	External	Default Inline Set			
 s1p3		Vswitch	2e:42:44:75:		
 s1p4		Vswitch	5a:f5:ea:2b:		

Aggregate Interfaces



Adding Aggregate Interfaces

Add Interface

? X

None

Switched

Routed

Name

lag0

Mode:

Autonegotiation

▼

MDI/MDIX:

Auto-MDIX

▼

Link Aggregation

Available Interfaces:

s1p2

s1p3

s1p4

→

←

Load-Balancing Algorithm:

Destination IP

▼

Link Selection Policy:

Highest Port Count

▼

Tunnel Level:

Inner

▼

LACP

Enabled:

☒

Rate:

☒ Slow

☐ Fast

Mode:







☒ Active

☐ Passive

Save

Cancel

Adding Aggregate Interfaces (Cont.)

Name	Security Zone	Used By	MAC Address	IP Addresses	
 lag0		Vswitch	3e:ef:71:7e:cc		  
Physical					
 s1p2					
 s1p3					
 s1p4					
 s1p1		Vswitch	9e:d6:4c:68:d7		

Adding Logical Interfaces

Add Interface

? X

Switched Routed Hybrid

Interface:	s1p1	▼
VLAN Tag:	1	
Security Zone:	None	▼
Virtual Switch:	None	▼
Enabled:	<input checked="" type="checkbox"/>	
MTU:	1518	

Save Cancel

Configuring Passive Interfaces

Edit Interface ? X

None Passive Inline Switched Routed HA Link

Security Zone:

None

▼

Enabled:

☒

Mode:

Autonegotiation

▼

MDI/MDIX:

Auto-MDIX

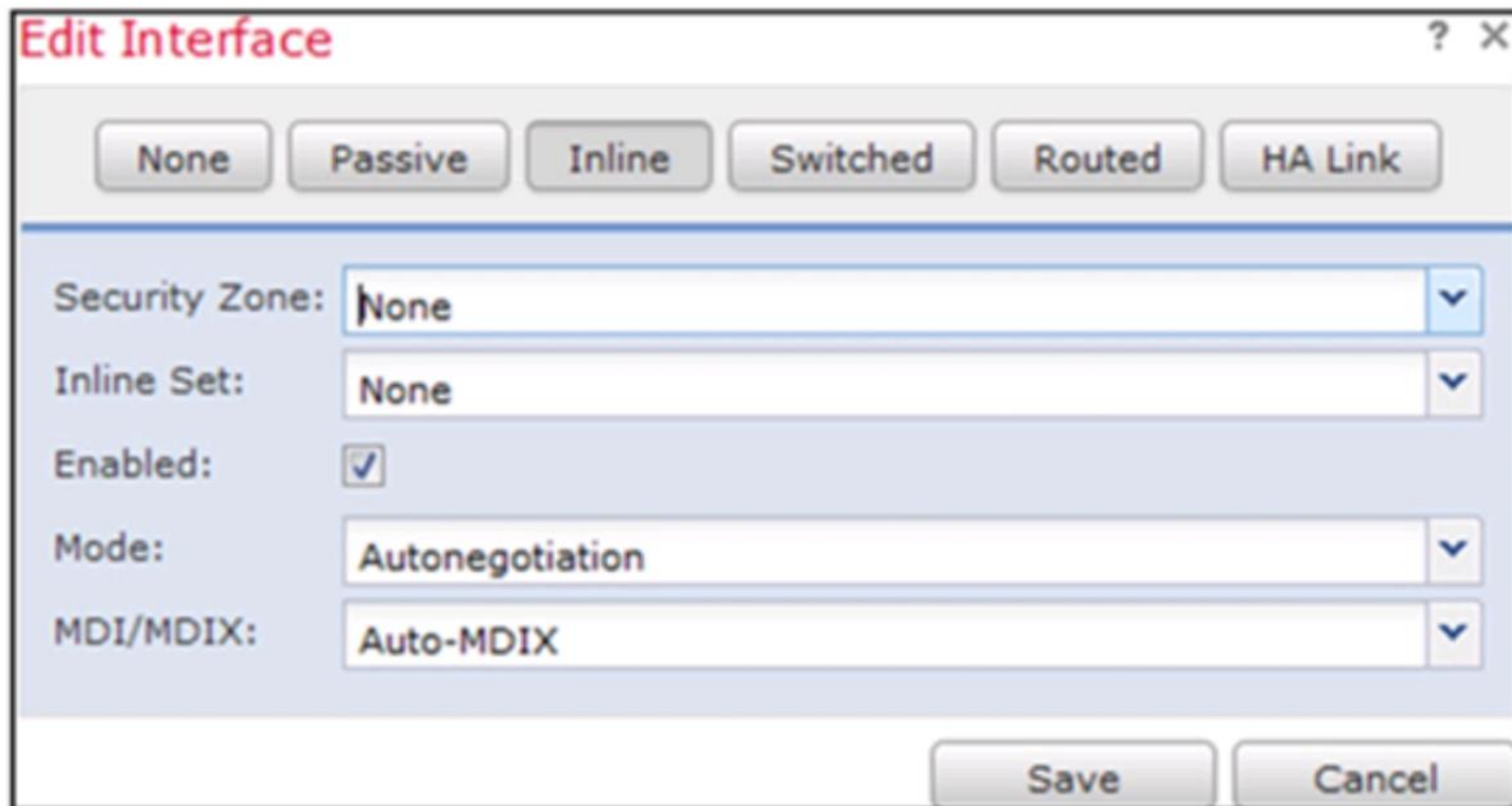
▼

MTU:

1518

Save Cancel

Configuring Inline Interfaces



The image shows a screenshot of the 'Edit Interface' configuration window in a network management system. The window has a title bar with a question mark and a close button. Below the title bar is a row of six buttons: 'None', 'Passive', 'Inline', 'Switched', 'Routed', and 'HA Link'. The 'Inline' button is highlighted. Below this row are five configuration fields: 'Security Zone' with a dropdown menu showing 'None', 'Inline Set' with a dropdown menu showing 'None', 'Enabled' with a checked checkbox, 'Mode' with a dropdown menu showing 'Autonegotiation', and 'MDI/MDIX' with a dropdown menu showing 'Auto-MDIX'. At the bottom right of the window are two buttons: 'Save' and 'Cancel'.

Edit Interface ? X

None Passive **Inline** Switched Routed HA Link

Security Zone: None

Inline Set: None

Enabled: ☒

Mode: Autonegotiation

MDI/MDIX: Auto-MDIX

Save Cancel

Configuring Physical Switched Interfaces

Edit Interface



None Passive Inline **Switched** Routed HA Link

Security Zone:

Virtual Switch:

Enabled: ☒

Mode:

MDI/MDIX:

MTU:

Save Cancel

Configuring Physical Routed Interfaces

Edit Interface ? x

None Passive Inline Switched **Routed** HA Link

Security Zone:

Virtual Router:

Enabled: ☒

Mode:

MDI/MDIX:

MTU:

ICMP: ☒ Enable Responses

IPv6 NDP: ☒ Enable Router Advertisement

IP Addresses:

Address	Type
---------	------

Static ARP Entries:

IP Address	MAC Address
------------	-------------

Configuring High-Availability Link Interfaces

Edit Interface

? X

<div>None Passive Inline Switched Routed HA Link</div>	
Enabled:	<input checked="" type="checkbox"/>
Mode:	Autonegotiation ▼
MDI/MDIX:	Auto-MDIX ▼
MTU:	9922
<div>Save Cancel</div>	

Inline Set Tab

Add Inline Set

? X

General Advanced

Name:

Interfaces:

→

→

←

←

MTU:

Failsafe: ☐

Bypass Mode: ☒ Bypass ☐ Non-Bypass

OK Cancel

Add Inline Set

? X

General **Advanced**

Tap Mode: ☐

Propagate Link State: ☐

Transparent Inline Mode: ☒

Strict TCP Enforcement: ☐

OK Cancel

Virtual Switches Tab

Add Virtual Switch



General Advanced

Name:

Available

Selected

Add

Hybrid Interface:

Save Cancel

Add Virtual Switch



General **Advanced**

Static Mac Entries

MAC Address	Interface
-------------	-----------

Enable Spanning Tree Protocol: ☐

Strict TCP Enforcement: ☐

Drop BPDUs: ☐

Save Cancel

Virtual Routers Tab

Add Virtual Router

? X

GeneralStaticDynamic RoutingFilterAuthentication Profile

General:

Name:

IPv6 Support:☒

Strict TCP Enforcement:☐

Interfaces:

Available

Selected

Add

DHCP Relay:

☐ DHCPv4☐ DHCPv6

SaveCancel

A valid virtual router name is required.

Static Route Configuration

Add Static Route



Route Name:	<input type="text"/>
Enabled:	<input checked="" type="checkbox"/>
Preference:	<input type="text" value="210"/>
Type:	<input type="text" value="IP"/>
Destination:	<input type="text"/>
Gateway:	<input type="text"/>

OK

Cancel

Working With Variable Sets

- Variables represent values that are commonly used in intrusion rules to identify source and destination IP addresses and ports.
- Variable sets are used to manage, customize, and group your variables.



Working With File Lists

Filter

Network

Individual Objects

Object Groups

Security Intelligence

Port

Individual Objects

Object Groups

VLAN Tag

Individual Objects

Object Groups

URL

Individual Objects

Object Groups



Application Filters

Variable Set

File List

Security Zones

Geolocation

Name	Number of Entries	
Clean List	0	 
Custom Detection List	0	