

# **Configure a Basic Policy**

Configure a basic security policy with the following settings:

- Inside and outside interfaces—Assign a static IP address to the inside interface, and use DHCP for the outside interface.
- DHCP server—Use a DHCP server on the inside interface for clients.
- Default route—Add a default route through the outside interface.
- NAT—Use interface PAT on the outside interface.
- Access control—Allow traffic from inside to outside.

You can also ccustomize your security policy to include more advanced inspections.

- Configure Interfaces, on page 1
- Configure the DHCP Server, on page 6
- Configure NAT, on page 7
- Configure an Access Control Rule, on page 10
- Enable SSH on the Outside Interface, on page 13
- Deploy the Configuration, on page 14

## **Configure Interfaces**

When you use zero-touch provisioning or the device manager for initial setup instead of using the CLI, the following interfaces are preconfigured:

- Ethernet 1/1—outside, IP address from DHCP, IPv6 autoconfiguration
- VLAN1— inside, 192.168.95.1/24
- Default route—Obtained through DHCP on the outside interface

If you performed additional interface-specific configuration within device manager before registering with the management center, then that configuration is preserved.

If you used the CLI for initial setup, there is no preconfiguration of your device.

In both cases, you need to perform additional interface configuration after you register the device. For CLI initial setup, you must add the VLAN1 interface for the inside switch ports. Additional configuration includes

converting switch ports to firewall interfaces as desired, assigning interfaces to security zones, and changing IP addresses.

The following example configures a routed-mode inside interface (VLAN1) with a static address and a routed-mode outside interface using DHCP (Ethernet1/1). It also adds a DMZ interface for an internal web server.

**Step 1** Choose **Devices** > **Device Management**, and click **Edit** ( $\Diamond$ ) for the device.

### Step 2 Click Interfaces.

### Figure 1: Interfaces

rice Routing Interface	es Inline Sets D	DHCP VTE	P SNMP				२ Search by na	ne	Syn	c Device Add I	nterfac
Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby) IP /	Address	Path Monitori	n: Port Mode	VLAN Usage	SwitchPo	o Virtual Router	
Management1/1	management	Physical				Disabled				Global	Q
Ethernet1/1	outside	Physical	outside	10.	89.5.29/255.255.255.192(	Disabled				Global	Ø
Ethernet1/2		Physical				Disabled	Access	1			Ø
Ethernet1/3		Physical				Disabled	Access	1			O
Ethernet1/4		Physical				Disabled	Access	1			0

- **Step 3** If you used the CLI for initial setup, enable the switch ports.
  - a) Click **Edit** ( $\Diamond$ ) for the switch port.

Figure 2: Enable Switch Port

Edit Physical Interface				
General	Hardware Configuration			
Interface ID				
Enabled Description				
Port Mode:				
Access	~			
VLAN ID:				
(1 - 4070) Protected:				

- b) Enable the interface by checking the **Enabled** check box.
- c) (Optional) Change the VLAN ID; the default is 1. You will next add a VLAN interface to match this ID.
- d) Click OK.

r

L

- **Step 4** Add (or edit) the **inside** VLAN interface.
  - a) Click Add Interfaces > VLAN Interface, or if this interface already exists, click Edit (2) for the interface. Figure 3: Add VLAN Interface

Add VLAN Interface	0
General IPv4 IPv6 Advanced	
Name: inside Enabled Description: Mode:	
None   Security Zone: inside_zone  MTU: 1500	
VLAN ID *:	(0 - 65535)
(1 - 4070) Disable Forwarding on Interface Vlan: None ~	Port Mo
	cords to display

- b) From the Security Zone drop-down list, choose an existing inside security zone or add a new one by clicking New.
   For example, add a zone called inside\_zone. You apply your security policy based on zones or groups.
   If VLAN1 was preconfigured, the rest of these fields are optional.
- c) Enter a Name up to 48 characters in length.

For example, name the interface inside.

- d) Check the **Enabled** check box.
- e) Leave the Mode set to None.
- f) Set the VLAN ID to 1.

By default, all of the switchports are set to VLAN 1; if you choose a different VLAN ID here, you need to also edit each switchport to be on the new VLAN ID.

You cannot change the VLAN ID after you save the interface; the VLAN ID is both the VLAN tag used, and the interface ID in your configuration.

- g) Click the IPv4 and/or IPv6 tab.
  - IPv4—Choose Use Static IP from the drop-down list, and enter an IP address and subnet mask in slash notation.

For example, enter 192.168.1.56/24

Figure 4: Set Inside IP Address

### Add VLAN Interface

General	IPv4	IPv6	Advanced
IP Type:			
Use Stat	ic IP		~
IP Address	:		
192.168.1	.56/24		
ea. 192.0.2.1	1/255.255.2	255.128 or	192.0.2.1/25

• IPv6—Check the Autoconfiguration check box for stateless autoconfiguration.

- h) Click OK.
- **Step 5** Click Edit ( $\Diamond$ ) for Ethernet1/1 that you want to use for **outside**.

The **General** page appears.

Figure 5: General

### **Edit Physical Interface**

General IPv4	IPv6	Path Monitor	ing Harc
Name: outside			
Enabled			
Management	Only		
Description:			
Mode:			
None		~	
Security Zone:			
outside_zone		~	
Interface ID:			
Ethernet1/1			
MTU:			
1500			
(64 - 9198)			
Priority:			
0			(0 - 65535)
Propagate Securit	y Group T	ag: 🗌	
NVE Only:			

a) From the Security Zone drop-down list, choose an existing outside security zone or add a new one by clicking New.
 For example, add a zone called outside\_zone.

You should not alter any other basic settings because doing so will disrupt the management center management connection.

- b) Click OK.
- **Step 6** Configure a DMZ interface to host a web server, for example.
  - a) Disable switch-port mode for the switch port you want to use for the DMZ by clicking the slider in the **SwitchPort** column so it shows as disabled (.....).
  - b) Click **Edit** ( $\Diamond$ ) for the interface.
  - c) From the Security Zone drop-down list, choose an existing DMZ security zone or add a new one by clicking New.
     For example, add a zone called dmz\_zone.
  - d) Enter a Name up to 48 characters in length.

For example, name the interface **dmz**.

e) Check the **Enabled** check box.

- f) Leave the **Mode** set to **None**.
- g) Click the IPv4 and/or IPv6 tab and configure the IP address as desired.
- h) Click **OK**.

```
Step 7 Click Save.
```

# **Configure the DHCP Server**

Enable the DHCP server if you want clients to use DHCP to obtain IP addresses from the firewall.

**Step 1** Choose **Devices** > **Device Management**, and click **Edit** ( $\Diamond$ ) for the device.

### **Step 2** Choose **DHCP** > **DHCP** Server.

### Figure 6: DHCP Server

Device Routing Interfaces	s Inline Sets DHCP VTEP	SNMP	
	Ping Timeout		
DHCP Server	50	(10 - 10000 ms)	
DHCP Relay	Lease Length		
DDNS	3600	(300 - 10,48,575 sec)	
	Auto-Configuration		
	Interface		
	Override Auto Configured Settin	ngs:	
	Domain Name		
	Primary DNS Server	Primary WINS Server	
	[ ~ ]	+ ( ~ ) +	
	Secondary DNS Server	Secondary WINS Server	
	[ · · · ]	+ ( ~ ) +	
r	Server Advanced		
			+ Add
	Interface	Address Pool	Enable DHCP Server
		No records to display	

**Step 3** In the Server area, click Add and configure the following options.

Figure 7: Add Server

Add Server			?
Interface*			
inside	~		
Address Pool*			
192.168.1.2-192.168.1.55			
(2.2.2.10-2.2.2.20)			
Enable DHCP Server			
		Cancel	ок

- Interface—Choose the interface name from the drop-down list.
- Address Pool—Set the range of IP addresses. The IP addresses must be on the same subnet as the selected interface and cannot include the IP address of the interface itself.
- Enable DHCP Server—Enable the DHCP server on the selected interface.

Step 4Click OK.Step 5Click Save.

# **Configure NAT**

This procedure creates a NAT rule for internal clients to convert the internal addresses to a port on the outside interface IP address. This type of NAT rule is called *interface Port Address Translation (PAT)*.

- **Step 1** Choose **Devices** > **NAT**, and click **New Policy**.
- **Step 2** Name the policy, select the devices that you want to use the policy, and click **Save**.

### Figure 8: New Policy

New Policy				?
Name: FTD_policy				
Description:				
Targeted Devices Select devices to which you want to apply t	his policy.			_
Available Devices and Templates		Selected Devices an	nd Templates	ā
192.168.0.124		192.168.0.124		Ū
192.168.0.155				
	Add to Policy			
			Cancel	ave

The policy is added the management center. You still have to add rules to the policy.

### Figure 9: NAT Policy

FTD_Policy							Show Warning	s Save	Cancel
Enter Description									
Rules						Ν	NAT Exemptions	Policy Ass	ignments (1)
Filter by Device								$\otimes$	Add Rule
			Original Packet			Translated Packet			
Source # Direction Type Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
<ul> <li>NAT Rules Before</li> </ul>									
<ul> <li>Auto NAT Rules</li> </ul>									
<ul> <li>NAT Rules After</li> </ul>									

Step 3 Click Add Rule.

**Step 4** Configure the basic rule options:

Figure 10: Basic Rule Options

Add NAT Rule	9
NAT Rule:	
Auto NAT Rule	$\sim$
Туре:	
Dynamic	$\sim$
Enable	
Interface Objects	Translation

- NAT Rule—Choose Auto NAT Rule.
- Type—Choose Dynamic.
- **Step 5** On the **Interface Objects** page, add the outside zone from the **Available Interface Objects** area to the **Destination Interface Objects** area.

Figure 11: Interface Objects

Interface Objects	Translation	PAT Pool	Advanced			
Available Interface Objects	e C'		Source Interface Objects	(0)	Destination Interface Objects	(1)
Q Search by name			any		3 outside	ō)
inside	Ad	d to Source				
1 outside	Add t	o Destination				
T	2		,			
	-					

**Step 6** On the **Translation** page, configure the following options:

### Figure 12: Translation

Interface Objects	Translation	PAT Pool	Advanced
Original Packet			Translated Packet
Original Source:* all-ipv4 Original Port: TCP	× +		Translated Source: Destination Interface IP The values selected for Destination Interface Objects in 'Interface Objects' tab will be used Translated Port:

• Original Source—Click Add (+) to add a network object for all IPv4 traffic (0.0.0/0).

#### Figure 13: New Network Object

New Network Object		?
Name all-ipv4		
Description		
Network Host Range Network	O FQDN	
0.0.0/0		
Allow Overrides		
	Cancel	Save

- **Note** You cannot use the system-defined **any-ipv4** object, because Auto NAT rules add NAT as part of the object definition, and you cannot edit system-defined objects.
- Translated Source—Choose Destination Interface IP.
- **Step 7** Click **Save** to add the rule.

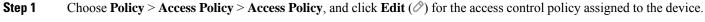
The rule is saved to the **Rules** table.

**Step 8** Click **Save** on the **NAT** page to save your changes.

## **Configure an Access Control Rule**

If you created a basic **Block all traffic** access control policy when you registered the device, then you need to add rules to the policy to allow traffic through the device. The access control policy can include multiple rules that are evaluated in order.

This procedure creates an access control rule to allow all traffic from the inside zone to the outside zone.



Step 2 Click Add Rule, and set the following parameters.

L

#### Figure 14: Source Zone

1	0 Add Rule	•							
Name	inside-to-outside							Action 📀 Allow	✓ ■ Lo
Insert	into Mandatory	~						Intrusion Policy	None
Q	Zones (1)	Networks	Ports	Applications	🛕 Users	URLs	Dynamic Attribute	s VLAN Tags	
Clea	ar Selections Q S	earch Security Zo	ne Objects		Showing	g 2 out of 2	Selected 1	Selected Sources: 0	
2 2	♣ inside (Routed) ♣ outside (Routed)								
									Any
+ C	reate Security Zone	Object						3	Add Source Zone

- 1. Name this rule, for example, inside-to-outside.
- 2. Select the inside zone from Zones

### 3. Click Add Source Zone.

Figure 15: Destination Zone

1 🗘 Add Rule	
Name Inside-to-outside	Action 😂 Allow 💙 🖻 Logging OFF 🛛 🕏 Time Range None 🗸 Ru
Insert Into Mandatory V	Intrusion Policy None     Variable Set     Set     File Policy None
Q Zones (2) Networks Ports Applications 🛕 Users URLs Dynamic Attribu	tes VLAN Tags
Clear Selections Q Search Security Zone Objects Showing 2 out of 2 Selected 1	Selected Sources: 1 Selected Destinations and Applications: 0
E inside (Routed Security Zone)	Collapse All Remove All
4 outside (Routed Security Zone)	ZONE v 1 Object
	🚓 inside
	Any
+ Create Security Zone Object	Add Source Zone 5 Add Destination Zone

4. Select the outside zone from Zones.

### 5. Click Add Destination Zone.

Leave the other settings as is.

**Step 3** (Optional) Customize associated policies by clicking on the policy type in the packet flow diagram.

Prefilter, Decryption, Security Intelligence, and Identity policies are applied before an access control rule. Customizing these policies is not required, but after you know your network's needs, they let you improve network performance by either fastpathing trusted traffic (bypassing processing) or blocking traffic so no further processing is required.

Figure 16: Policies Applied Before Access Control

₽ Packets →	0	<b>Prefilter Rules</b>	→ C	Decryption →	Ø	Security Intelligence	→ (	🔵 ldentity → 🄇	Access Control
-------------	---	------------------------	-----	--------------	---	-----------------------	-----	----------------	----------------

• **Prefilter Rules**—The Default Prefilter Policy passes all traffic for the other rules to act on (analyzes). The only change to the default policy you can make is to **block** tunnel traffic. Otherwise, you can create a new prefilter policy to associate with the access control policy that can analyze (pass on), fastpath (bypass further checks) or block.

Prefiltering lets you improve performance by dealing with traffic before it gets any further, by either blocking or fastpathing. In a new policy, you can add *tunnel* rules and *prefilter* rules. A tunnel rule lets you fastpath, block, or rezone plaintext (non-encrypted), passthrough tunnels. A prefilter rule lets you fastpath or block non-tunneled traffic identified by IP address, port, and protocol.

For example, if you know you want to block all FTP traffic on your network, but fastpath SSH traffic from an administrator, you can add a new prefilter policy.

- **Decryption**—Decryption is not applied by default. Decryption is a way to expose network traffic to deep inspection. In most cases, you don't want to decrypt traffic, and can only do so if it is legally allowed. For maximum network protection, a decryption policy might be a good idea for traffic going to critical servers or coming from untrusted network segments.
- Security Intelligence—(Requires the IPS license) Security Intelligence is enabled by default. Security Intelligence is another early defense against malicious activity applied before passing connections to the access control policy for further processing. Security Intelligence uses reputation intelligence to quickly block connections to or from IP addresses, URLs, and domain names provided by Talos, the threat intelligence organization at Cisco. You can add or delete additional IP addresses, URLs, or domains if desired.
- **Note** If you do not have the IPS license, this policy will not be deployed even though it shows in your access control policy as enabled.
- **Identity**—Identity is not applied by default. You can require a user to authenticate before allowing traffic to be processed by the access control policy.
- **Step 4** (Optional) Add an Intrusion policy that is applied after the access control rule.

The Intrusion policy is a defined set of intrusion detection and prevention configurations that inspects traffic for security violations. The management center includes many system-provided policies you can enable as-is or that you can customize. This step enables a system-provided policy.

a) Click the Intrusion Policy drop-down list.

Figure 17: System-Provided Intrusion Policies

Int	rusion Policy	None ^
ags		System-Provided Policies
Selected	Sources: 1	Balanced Security and Conne
Collapse	e All	Connectivity Over Security
ZONE V 1 Object		Maximum Detection
	📫 inside_	Security Over Connectivity
		User-Created Policies

- b) Choose one of the system-provided policies from the list.
- **Step 5** (Optional) Add a File policy that is applied after the access control rule.

a) Click the **File Policy** drop-down list and choose either an existing policy or add one by choosing the **Open File Policy** List.

Figure 18: File Policy

🖶 File Policy	None	^
	No options	
ns and Applicatio	Open File Policy List $^{7}$	

For a new policy, the **Policies** > **Malware & File** page opens in a separate tab.

- b) See the Cisco Secure Firewall Device Manager Configuration Guide for details on creating the policy.
- c) Return to the Add Rule page and select the newly created policy from the drop-down list.

### Step 6 Click Apply.

The rule is added to the **Rules** table.

Step 7 Click Save.

## Enable SSH on the Outside Interface

This section describes how to enable SSH connections to the outside interface.

By default, you can use the admin user for which you configured the password during initial setup.

- **Step 1** Choose **Devices** > **Platform Settings** and create or edit the threat defense policy.
- Step 2 Select SSH Access.
- **Step 3** Identify the outside interface and IP addresses that allow SSH connections.
  - a) Click Add to add a new rule, or click Edit to edit an existing rule.
  - b) Configure the rule properties:
    - **IP** Address—The network object or group that identifies the hosts or networks you are allowing to make SSH connections. Choose an object from the drop-down menu, or click + to add a new network object.
    - Available Zones/Interfaces—Add the outside zone or type the outside interface name into the field below the Selected Zones/Interfaces list and click Add.

Figure 19: Enable SSH on the Outside Interface

Edit Secure Shell	Configuration	?
IP Address* any-ipv4	~ +	
Available Zones/Interfaces	C <sup>™</sup> Selected Zones/Interfaces	
Q Search	Add	
DMZ		
inside		
outside		
	outside	Add
	Cancel	ок

c) Click **OK**.

### Step 4 Click Save.

You can now go to **Deploy > Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

# **Deploy the Configuration**

Deploy the configuration changes to the device; none of your changes are active on the device until you deploy them.

**Step 1** Click **Deploy** in the upper right.

Figure 20: Deploy



**Step 2** For a quick deployment, check specific devices and then click **Deploy**.

### Figure 21: Deploy Selected

Q	Advanced Deploy   Ignore warnings  Deploy
1010-2	Ready for Deployment
1120-3	Ready for Deployment

Or click **Deploy All** to deploy to all devices.

### Figure 22: Deploy All

Q	Advanced Deploy
1010-2	Ready for Deployment
1120-3	Ready for Deployment
1120-4	Ready for Deployment
ftd-cluster1	Ready for Deployment
ftd1	Ready for Deployment

🔋 5 devices are available for deployment 📴 🐁

Otherwise, for additional deployment options, click Advanced Deploy.

### Figure 23: Advanced Deployment

	Q s	Search using device name, user name, type								Deploy time: Estimate
nd	ing Ch	anges Reports								
		Device	Modified by	Inspect In	terru	Туре	Group	Last Deploy Time	Preview	
>		ftd1	rboersma, Syster	n		FTD		Feb 26, 2024 11:09	đ	Ready for Deployment
>		ftd-cluster1 rboersma, System		n	FTD			Feb 22, 2024 10:36	a	Ready for Deployment
~	<ul> <li></li> </ul>	1010-2	rboersma, Syster	n		FTD		Feb 22, 2024 11:09	a	Ready for Deployment
y.		✓ Access Control Group								
		Access Control Policy: in-out		A rboersma, System						
0		Intrusion Policy: No Rules Active		Q System						
۶	2	Network Analysis Policy: Balanced Security	y and Connectivity	Q System						
		<ul> <li>Device Configurations</li> </ul>								
		Interface Policy		Q rboersma						
		<ul> <li>Flex Configuration</li> </ul>								
		Template Policy: Unassigned		Q rboersma						
		✓ NAT Group								
		Manual NAT Rules: interface_PAT		A rboersma						
		<ul> <li>Security Updates</li> </ul>								
		Rule Update: (Isp-rel-20240311-2013)								

**Step 3** Ensure that the deployment succeeds. Click the icon to the right of the **Deploy** button in the menu bar to see status for deployments.

### Figure 24: Deployment Status

	Q s	earch		Deploy	<b>@</b>	@   ~	
Deployments	Upgrades	A Health	Tasks	$\checkmark$	Show	Pop-up Notifications 🥫	
7 total	1 running	6 success	0 warnings	0 failures	Q	Filter	
😜 1010-2	Deployment - Policy and object collection 10%						
1120-3	D-3 Deployment to device successful.						
1120-4	Deployment to device successful.						
3110-1	Deploy	ment to devic	e successful.			1m 38s	

Configure a Basic Policy