

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 5
- Configure NAT, on page 6
- Configure an Access Control Rule, on page 9
- Enable SSH on the Outside Interface, on page 12
- Deploy the Configuration, on page 13

Configure Interfaces

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

Procedure

Step 1 Choose Devices > Device Management,	, and click Edit ($ otin)$ for the firewall.
--	---

Step 2 Click Interfaces.

Figure 1: Interfaces

Device Routing Interfaces	Inline Sets DHCP	VTEP							
						Q Search by name	Sync D	Add Int	erfaces 🔻
Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby)	IP Ad	Idress	Path Monitorin	virtual Router	
Management0/0	management	Physical					Disabled	Global	QC
GigabitEthernet0/0		Physical					Disabled		/
GigabitEthernet0/1		Physical					Disabled		/
GigabitEthernet0/2		Physical					Disabled		/
GigabitEthernet0/3		Physical					Disabled		1
GigabitEthernet0/4		Physical					Disabled		1
GigabitEthernet0/5		Physical					Disabled		/
GigabitEthernet0/6		Physical					Disabled		/
GigabitEthernet0/7		Physical					Disabled		1

Step 3 To create breakout ports from a 40-Gb or larger interface, click the **Break** icon for the interface.

If you already used the full interface in your configuration, you will have to remove the configuration before you can proceed with the breakout.

Step 4 Click **Edit** (\mathcal{O}) for the interface that you want to use for inside.

Figure 2: General Tab

General	IPv4	IPv6	Path I	Monitoring	ł
Name:					
inside					
Enabled					
Managem	nent Only				
Description:					
Mode:					
None			•		
Security Zone	:				
inside_zone)		•		
Interface ID:					
MTU:					
1500					
(64 - 9000)					
Priority:					
0				(0 - 655	35)
Propagate Se	ourity Gr	oup Tage			

a) 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. For example, configure your access control policy to enable traffic to go from the inside zone to the outside zone, but not from outside to inside.

b) Enter a Name up to 48 characters in length.

For example, name the interface inside.

- c) Check the **Enabled** check box.
- d) Leave the Mode set to None.
- e) 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 192.168.1.1/24

Figure 3: IPv4 Tab

General	IPv4	IPv6	Path Mo	onitoring
IP Type:				
Use Static	IP		•	
IP Address:				
192.168.1	1/24			

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

Figure 4: IPv6 Tab

Edit Physical Interface

General	IPv4	IPv6	Pat	h Monitoring	Hardware Configu
Basic	Address	Prefixe	es	Settings	DHCP
	Enab	le IPV6:			
	Enforce	EUI 64:			
	Link-Local a	ddress:			
	Autoconfig	uration:			
0	btain Default	Route:			

f) Click OK.

Step 5 Click Edit (\mathcal{O}) for the interface that you want to use for outside.

Figure 5: General Tab

Edit Physical Interface

General	IPv4	IPv6	Path Monitoring	Hardware
Name:				
outside				
Enabled				
Manager	nent Only			
Description:				
Mode:				
None			•	
Security Zone	e:			
outside_zo	ne		•	
Interface ID:				
MTU:				
1500				
(64 - 9000)				
Priority:				
0			(0 - 655	35)
Propagate Se	ecurity Gr	oup Tag:		
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) Click **Edit** (\Diamond) for the interface you want to use.
 - b) 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.
 - c) Enter a Name up to 48 characters in length.

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

- d) Check the Enabled check box.
- e) Leave the Mode set to None.
- f) Click the IPv4 and/or IPv6 tab and configure the IP address as desired.
- g) 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.

Procedure

Step 1 Step 2

Device Routing Interfation	Ping Timeout 50 (10 - 10000 ms)	
DHCP Relay		
DHCP Relay		
-		
	Lease Length	
DDNS	(300 - 10,48,575 sec)	
	Auto-Configuration	
	Interface	
	\sim	
	Override Auto Configured Settings:	
	Domain Name	
	Primary DNS Server Primary WINS Server	
	· · · · · · · · · · · · · · · · · · ·	
	Secondary DNS Server Secondary WINS Server	
	· · · · · · · · · · · · · · · · · · ·	
	Server Advanced	
		+ 4

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

Figure	7: Add	Server
--------	--------	--------

Add Server	(?)
Interface*		
inside v		
Address Pool*		
192.168.1.2-192.168.1.55		
(2.2.2.10-2.2.2.20)		
🗹 Enable DHCP Server		
	Cancel OK	

- 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)*.

Procedure

- **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 a	nd Templates	
Q Search by name or value	J	192.168.0.124		Ū
192.168.0.124		192.168.0.155		Ū
192.168.0.155	'			
	Add to Policy			
	J			
			Cancel	Save

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							N	IAT Exemptions	Policy Ass	ignments (1)
Filter by Device	₽ Filter Rules								\otimes	Add Rule
				Original Packet			Translated Packet			
# Direction	Source Type Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
✓ NAT Rules Before										
 Auto NAT Rules 										
 NAT Rules After 										

Step 3 Click Add Rule.

Step 4 Configure the basic rule options:

Figure 10: Basic Rule Options

Add NAT Rule	
NAT Rule:	
Auto NAT Rule	\sim
Туре:	
Dynamic	~
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 Trans	slation PAT Pool	Advanced		
Available Interface Objects 🛛 📿		Source Interface Objects (0) Destination Interface Objects	(1)
Q Search by name		any	3 outside	ō)
	Add to Source			
inside				
1 outside	Add to 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	~ +		Translated Source: Destination Interface IP The values selected for
Original Port: TCP	~		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 (0.0.0.0/0).

Figure 13: New Network Object

New Network Object		0
Name all-ipv4		
Description		
Network Host Range Network	O FQDN	
0.0.0.0/0		
Allow Overrides		
	Cancel	Save
X		

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.

Procedure

Step 1 Choose Policy > Access Policy > Access Policy, and click Edit (𝔊) for the access control policy assigned to the device.
 Step 2 Click Add Rule, and set the following parameters.

Figure 14: Source Zone Add Rule inside-to-outside Action 🔁 Allow 🖹 Lc Name into Mandatory 🗸 🗸 Intrusion Policy Insert None Zones (1) Networks Ports Applications URLs **Dynamic Attributes** VLAN Tags A Users Q Clear Selections Q Search Security Zone Objects Selected Sources: 0 Showing 2 out of 2 Selected 1 tinside (Routed Security Zone) dia outside (Routed Security Zone) Anv + Create Security Zone Object Add Source Zon

- 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 S Allow	✓ V De Logging OFF K Time Range None V
Insert Into Mandatory ~	Intrusion Policy	None Variable Set Variable Set None
Q Zones (2) Networks Ports Applications 🛕 Users U	JRLs Dynamic Attributes VLAN Tags	S
Clear Selections Q Search Security Zone Objects Showing 2 of	ut of 2 Selected 1 Selected Sources:	1 Selected Destinations and Applications: 0
E inside (Routed Security Zone)	Collapse All	Remove All
4 distinct (Routed Security Zone)	ZONE V 1 Obje	ect
	🚠 ins	side
		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 🔸	Ø	Prefilter Rules	→	Ο	Decryption	→	0	Security Intelligence	-	С) Identity →	0	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 A
igs		System-Provided Policies
Selected	d Sources: 1	Balanced Security and Conne
Collaps	e All	Connectivity Over Security
ZONE	🗸 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 [⊅]	

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.

Procedure

Step 1	Choose Devices > Platform Settings and create or edit the threat defense politication of the set of the se	icy.
--------	--	------

- 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 Cor	nfiguration	?
IP Address* any-ipv4 ~	+	
Available Zones/Interfaces	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.

Procedure

Step 1Click 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
1010-2	Ready for Deployment
1120-3	Ready for Deployment

Or click Deploy All to deploy to all devices.

Figure 22: Deploy All

2	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

nding Changes Reports									
	Device	Modified by	Inspect Interru	Туре	Group	Last Deploy Time	Preview		
	ftd1	rboersma, Syste	m	FTD		Feb 26, 2024 11:09	đ	Ready for Deployment	
	ftd-cluster1	rboersma, Syste	m	FTD		Feb 22, 2024 10:36	đ	Ready for Deployment	
 Image: A start of the start of	1010-2	rboersma, Syste	m	FTD		Feb 22, 2024 11:09	đ	Ready for Deployment	
ў́= @	Access Control Group Access Control Group Access Control Policy: In-out Intrusion Policy: No Rules Active Network Analysis Policy: Balanced Securi Device Configurations Interface Policy Flex Configuration Templete Policy: Unassigned NAT Group Manual NAT Rules: Interface_PAT Security Updates Rule Ucdate: (8p-ref-20240311-2013)	ty and Connectivity	Q rboersma, System Q System Q System Q rboersma Q rboersma Q rboersma						

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 Search		Deploy	· _ · · · · ·			
Deployments	Upgrades 🔺 Health	Tasks	⊻	Show Pop-	up Notifications 🥫		
7 total	1 running 6 success	0 warnings	0 failures	Q Filter	·		
🔑 1010-2	Deployment - Policy and object collection 10% complete.						
1120-3	Deployment to devi	ce successful.			2m 39s		
1120-4	Deployment to devi	ce successful.			2m 43s		
3110-1	Deployment to devi	ce successful.			1m 38s		

I