



Test the System

To make sure everything is set up properly, you'll create an access control policy to allow all traffic, connect a client to the inside network, and make sure the client can connect to the internet. Finally, you'll monitor traffic on the managed device directly as well as on the Firepower Management Center.

- [Edit the Access Control Policy, on page 1](#)
- [Test the System, on page 3](#)
- [Troubleshoot the System, on page 6](#)


Edit the Access Control Policy

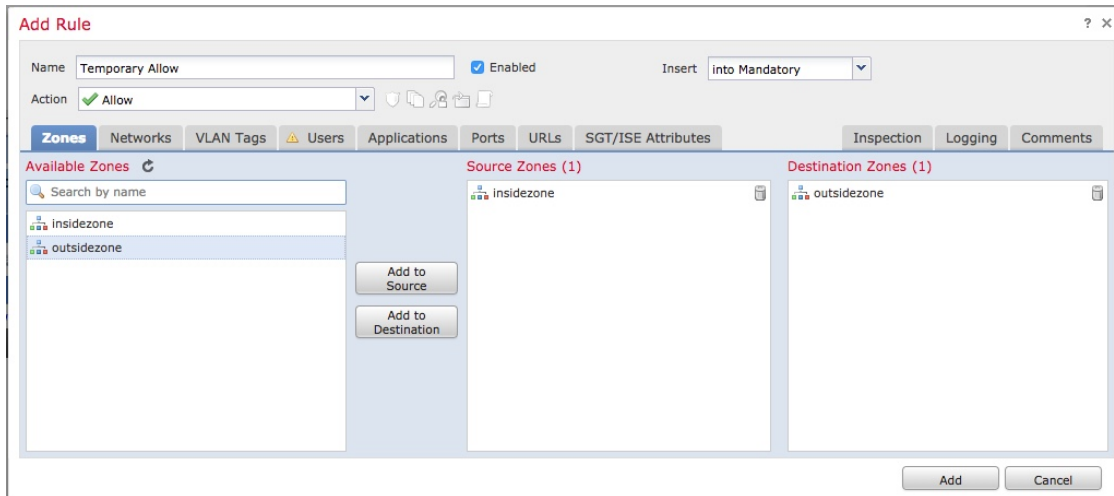
You'll create a temporary access control policy to allow all traffic, with no inspection, from the inside network to the outside network to test the following:


- A client connected to the inside network can connect to the internet.
- Traffic is being filtered through the Firepower Threat Defense device. (The managed device should "see" all the traffic even if it's not being filtered.)

Before you begin

Make sure you have completed all other tasks discussed in this guide before continuing.

-
- Step 1** In the Firepower Management Center, click **Policies > Access Control > Access Control**.
 - Step 2** Click  (edit) next to **Initial Policy**.
 - Step 3** Click **Add Rule**.
 - Step 4** Enter the following information in the Add Rule dialog box:



- Step 5** Click the **Logging** tab.
- Step 6** Check **Log at end of connection**.
- Step 7** Click **Add**.
The policy page is displayed.
- Step 8** On the Initial Policy page, from the **Default Action** list, click **Intrusion Prevention: Balanced Security and Connectivity**.
- Step 9** Next to the list, click  (logging).
- Step 10** Check **Log at end of connection**.
- Step 11** Click **OK**.
- Step 12** At the top of the page, click **Save**.
- Step 13** Deploy the changes:
- At the top of the page, click **Deploy**.
 - Optional. Expand the device to display the changes you're about to make.
 - Check the box to the left of the device.
The following figure shows an example.



- d) Click **Deploy**.
- e) Wait while the changes are deployed; deployment can take several minutes. Messages are displayed to indicate the progress of the deployment.

What to do next

See [Test the System, on page 3](#).

Test the System

To make sure the system is operating normally, connect a client to the inside network and make sure it can reach the internet. While the client is connecting to the internet, use diagnostics in the Firepower Management Center to make sure traffic is passing through it. You can also view connection events.

Before you begin

See [Edit the Access Control Policy, on page 1](#).

Step 1

Connect a client to the managed device's inside network.

The client can run any operating system: Windows, Mac, UNIX, and so on. The details of how to connect the client depend on how your network is set up and are beyond the scope of this guide. If you have access to the network rack in which the managed device is installed, you can directly connect a client to the device's GigabitEthernet 0/1 port.

Step 2

Set up the client with a static IP address of 10.10.1.50 , a default gateway of 10.10.1.1, and any accessible DNS server.

The default gateway should be the IP address of the inside interface. The client contacts this gateway first before sending any traffic to inside or outside addresses.

Step 3 Log in to the Firepower Management Center.

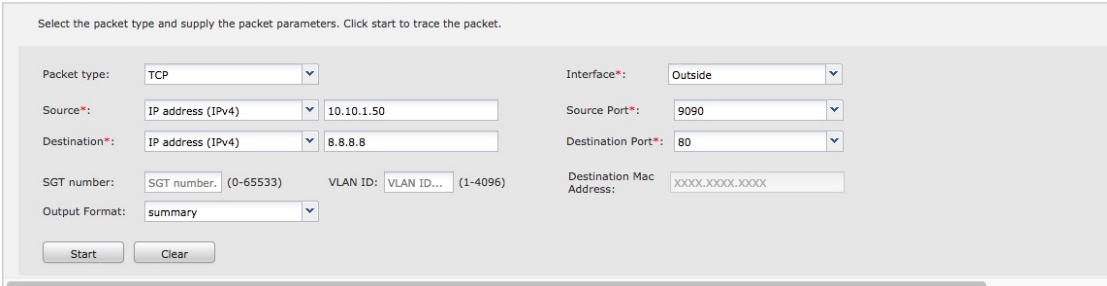
Step 4 Click **Devices > Device Management**.

Step 5 Next to your managed device, click  (Troubleshoot).

Step 6 Click **Advanced Troubleshooting**.

Step 7 Click the **Packet Tracer** tab.

Step 8 Enter the following information in the Packet Tracer tab page.



Select the packet type and supply the packet parameters. Click start to trace the packet.

Packet type: TCP

Source*: IP address (IPv4) 10.10.1.50

Destination*: IP address (IPv4) 8.8.8.8

Interface*: Outside

Source Port*: 9090

Destination Port*: 80

SGT number: SGT number (0-65533)

VLAN ID: VLAN ID... (1-4096)

Destination Mac Address: XXXX.XXXX.XXXX

Output Format: summary

Start Clear

The values for **Source IP address** and **Source Port** can be anything. What's being tested is whether or not traffic is forwarded from the inside interface to the outside interface. Only the **Destination IP address** and **Destination Port** values are used in this example.

Step 9 On your client, ping or browse to an internet site.

Step 10 On the Packet Tracer tab page, click **Start**.

For information about interpreting the results, see [Interpret the Results, on page 7](#).

Step 11 Click the **Capture w/ Trace** tab.

Step 12 Check **Enable Auto-Refresh** and change the refresh interval if desired.

Step 13 Click **Add Capture**.

Step 14 Enter the following information in the Add Capture dialog box.

Step 15 Click **Save**.

Step 16 On your client, ping or browse to an internet site.

Step 17 In the bottom pane, click  (Refresh).

The Firepower Management Center bottom pane displays results of the packet capture and trace. Look for messages like the following, which confirms traffic from the managed device's inside interface is matching your access control policy:

```
Phase: 5
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, ACK, seq 2101701398, ack 3091508482
AppID: service HTTP (676), application Adobe Analytics (2846), out-of-order
Firewall: allow rule, 'Temporary Allow Policy', allow
Snort id 1, NAP id 1, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet
```

For additional information about interpreting the results, see [Interpret the Results, on page 7](#).

For more information about the packet tracer, see [Packet Tracer Overview](#).

Step 18 Click **Analysis > Connections > Events**.

Step 19 In the upper right corner, click  to adjust the frequency of page updates.

Step 20 Click the **Preferences** tab.

Step 21 In the **Refresh Interval (minutes)** field, enter **1**.

Step 22 Click **Apply**.

Step 23 Navigate away from the page and come back to the Connection Events page.

Step 24 Wait for the page to refresh.

Connection events similar to the following should be displayed.

Connection Events (switch workflow)
 Connections with Application Details > Table View of Connection Events 2018-04-20 08:35:00 - 2018-04-20 09:56:23 Expanding

No Search Constraints (Edit Search)

Jump to	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL	URL Category	URL Reputation	Device	
\$	2018-04-20 08:40:18	2018-04-20 08:40:22	Allow		10.10.1.50	USA	13.78.213.133	USA	insidezone	outsidezone	49328 / tcp	443 / https	/ tcp							10.10.2.45
\$	2018-04-20 08:39:57	2018-04-20 08:40:06	Allow		10.10.1.50	USA	13.78.213.133	USA	insidezone	outsidezone	49327 / tcp	443 / https	/ tcp							10.10.2.45
\$	2018-04-20 08:39:36	2018-04-20 08:39:45	Allow		10.10.1.50	USA	13.78.213.133	USA	insidezone	outsidezone	49326 / tcp	443 / https	/ tcp							10.10.2.45
\$	2018-04-20 08:39:15	2018-04-20 08:39:24	Allow		10.10.1.50	USA	13.78.213.133	USA	insidezone	outsidezone	49325 / tcp	443 / https	/ tcp							10.10.2.45
\$	2018-04-20 08:38:54	2018-04-20 08:39:03	Allow		10.10.1.50	USA	13.78.213.133	USA	insidezone	outsidezone	49324 / tcp	443 / https	/ tcp							10.10.2.45
\$	2018-04-20 08:38:33	2018-04-20 08:38:42	Allow		10.10.1.50	USA	13.78.213.133	USA	insidezone	outsidezone	49323 / tcp	443 / https	/ tcp							10.10.2.45
\$	2018-04-20 08:38:33	2018-04-20 08:38:33	Allow		10.10.1.50	USA	8.8.8.8	USA	insidezone	outsidezone	53 / domain	53 / domain	/ udp	<input type="checkbox"/> DNS	<input type="checkbox"/> DNS client					10.10.2.45
\$	2018-04-20 08:38:33	2018-04-20 08:38:33	Allow		10.10.1.50	USA	8.8.8.8	USA	insidezone	outsidezone	53 / domain	53 / domain	/ udp	<input type="checkbox"/> DNS	<input type="checkbox"/> DNS client					10.10.2.45
\$	2018-04-20 08:38:12	2018-04-20 08:38:21	Allow		10.10.1.50	USA	52.165.21.19	USA	insidezone	outsidezone	49322 / tcp	443 / https	/ tcp							10.10.2.45

Step 25 To customize the view, click **Table View of Connection Events**.

For more information, see [Connection and Security Intelligence Event Fields](#) and [Using Connection and Security Intelligence Event Tables](#).

Step 26 If you see packet capture messages and connection events, congratulations! You have set up your system successfully.

What to do next

If errors are displayed or if your client cannot connect to the internet, see [Troubleshoot the System, on page 6](#).

Troubleshoot the System

This topic discusses solutions to problems you might encounter with your system; typically, no internet access for your network client.

Check the Static Route and Default Gateway

Check the static route and default gateway by pinging an internet site from your managed device as follows:

1. Using an SSH client or a virtual device's management console, log in to your managed device.
2. If required by your managed device, enter **connect ftd**
3. Enter **ping 8.8.8.8**

Successful results are displayed as follows:

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/av/max = 60/62/70 ms
```

If you *cannot* ping an internet IP address, make sure the managed device interfaces are connected properly. Make sure the link and activity LEDs on both ends of the cable are on (activity LED should flash).

Connection Events Not Displayed

The most likely reason connection events are not displayed is that you didn't enable logging in your access control rule or access control policy. See [Edit the Access Control Policy, on page 1](#).

Interpret the Results

This topic discusses how to interpret the results of the packet capture and `tracert` command.

Interpret Packet Tracer

The following excerpts from the packet tracer show the significant information and decisions made in forwarding traffic from the inside interface to the outside interface. Some of the configuration information discussed in this guide is highlighted. Note the following:

- Phase 3 resolves the outside gateway to 209.165.200.254
- Phase 4 shows the first time the Temporary Allow Policy is invoked
- Phase 6 shows the NAT policy forwarding from the inside client to the outside interface
- Phase 16 shows the inspection engine (Snort) allowing the traffic according to the Temporary Allow Policy

A failure at any of these phases could result in traffic being rejected or dropped, depending on whether policies were configured incorrectly or configured to block the traffic.

```
Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 209.165.200.254 using egress ifc Outside
```

```
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_global
access-list CSM_FW_ACL_advanced permit ip ifc Inside any ifc Outside any rule-id 268434433

access-list CSM_FW_ACL_remark rule-id 268434433: ACCESS POLICY: Initial Policy - Mandatory
access-list CSM_FW_ACL_remark rule-id 268434433: L7 RULE: Temporary Allow Policy
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached
```

```
Phase: 6
Type: NAT
Subtype:
Result: ALLOW
Config:
object network insidesubnet
 nat (Inside,Outside) dynamic interface
Additional Information:
Dynamic translate 10.10.1.50/52177 to 209.165.200.225/52177
```

```
Phase: 15
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'
```

```
Phase: 16
```

```
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: UDP
Session: new snort session
AppID: service DNS (617), application unknown (0)
Firewall: allow rule, 'Temporary Allow Policy', allow
Snort id 1, NAP id 1, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet
```



Note Packet Tracker and Capture w/ Trace might display different phase numbers but the information displayed in each phase should be very similar.



Note If there is no final SNORT phase, look for errors in the ROUTE-LOOKUP phase. For example, the following could indicate there is a problem with your outside interface. Verify its IP address and the IP address of the outside gateway.

```
Phase: 15
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 209.165.200.254 using egress ifc outside

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: drop
Drop-reason: (no-adjacency) No valid adjacency
```

Symptom: No Network Translation

If your packet capture does *not* have a line similar to the following, it likely means NAT is set up incorrectly.

```
Dynamic translate 10.10.1.50/65413 to 209.165.200.225/65413
```

Solution: Set up dynamic NAT as discussed in [Add a NAT Policy](#).

Symptom: Access Control Policy is Blocking Traffic

If your access control policy is configured to block traffic instead of allowing it, your packet capture contains the following line:

```
Drop-reason: (acl-drop) Flow is denied by configured rule
```

You can confirm this is the case by looking at connection events: **Analysis > Connections > Events**.

Solution: Configure your access control policy to allow traffic as discussed in [Edit the Access Control Policy, on page 1](#).

