



システムのテスト

すべてのセットアップが適切であることを確認するために、アクセスコントロールポリシーを作成してすべてのトラフィックを許可し、クライアントを内部ネットワークに接続し、クライアントがインターネットに接続できることを確認します。最後に、管理対象デバイス上のトラフィックを直接モニタし、Firepower Management Center 上のトラフィックもモニタします。

- [アクセスコントロールポリシーの編集 \(1 ページ\)](#)
- [システムのテスト \(3 ページ\)](#)
- [システムのトラブルシューティング \(6 ページ\)](#)


アクセスコントロールポリシーの編集

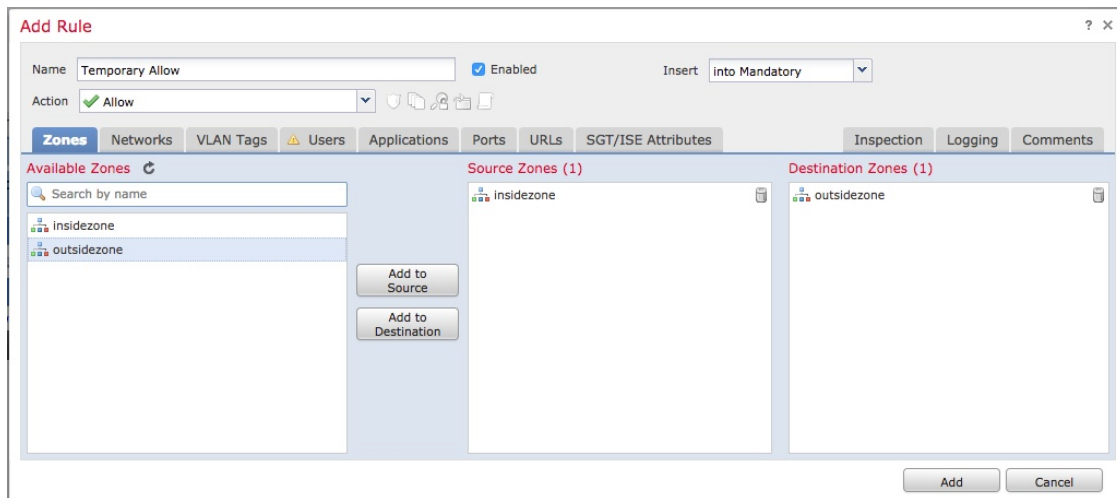
内部ネットワークから外部ネットワークへのすべてのトラフィックを許可するインスペクションなしの一時的なアクセスコントロールポリシーを作成して、以下をテストします。


- 内部ネットワークに接続しているクライアントがインターネットに接続できる。
- Firepower Threat Defense デバイスを介してトラフィックがフィルタリングされている。(管理対象デバイスは、トラフィックがフィルタリングされていなくても、すべてのトラフィックを確認する必要があります)

始める前に

続行する前に、このガイドで説明した他のすべてのタスクを完了していることを確認してください。

-
- ステップ 1** Firepower Management Center で、**[Policies] > [Access Control] > [Access Control]** を選択します。
 - ステップ 2** [Initial Policy] の横にある  (編集) をクリックします。
 - ステップ 3** [ルール追加 (Add Rule)] をクリックします。
 - ステップ 4** [Add Rule] ダイアログボックスで、次の情報を入力します。



- ステップ 5** [ロギング (Logging)] タブをクリックします。
- ステップ 6** [Log at End of Connection] をオンにします。
- ステップ 7** [追加 (Add)] をクリックします。
ポリシーのページが表示されます。
- ステップ 8** [Initial Policy] ページの [Default Action] リストで、[Intrusion Prevention: Balanced Security and Connectivity] をクリックします。
- ステップ 9** リストの横にある  (ロギング) をクリックします。
- ステップ 10** [接続の終了時にロギングする (Log at End of Connection)] をオンにします。
- ステップ 11** [OK] をクリックします。
- ステップ 12** ページの上部にある [保存 (Save)] をクリックします。
- ステップ 13** 変更を展開します。
- a) ページの上部にある [展開 (Deploy)] をクリックします。
 - b) オプションデバイスを展開して、変更する内容を表示します。
 - c) デバイスの左にあるチェックボックスをオンにします。
次の図は例を示しています。



- d) [展開 (Deploy)]をクリックします。
- e) 変更内容が展開されるのを待機します。展開には数分かかることがあります。展開の進行状況を示すメッセージが表示されます。

次のタスク

[システムのテスト \(3 ページ\)](#) を参照してください。

システムのテスト


システムが正常に動作していることを確認するには、クライアントを内部ネットワークに接続してインターネットに到達できることを確認します。クライアントがインターネットに接続しているときに、Firepower Management Center の診断を使用して、トラフィックが通過していることを確認します。接続イベントを表示することもできます。

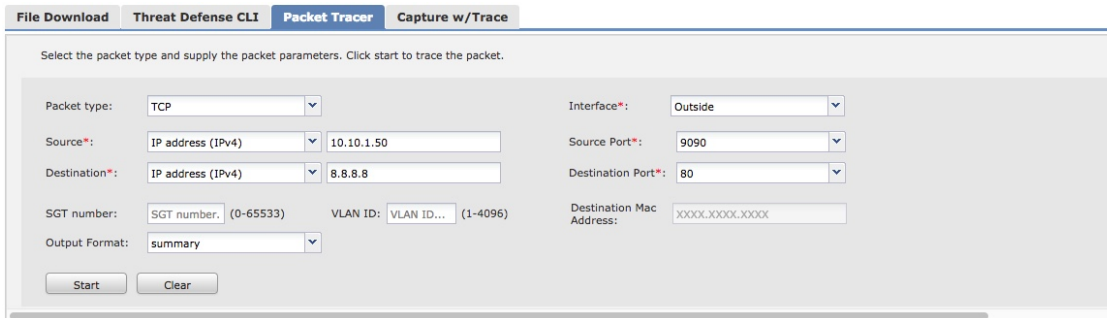
始める前に

[アクセス コントロール ポリシーの編集 \(1 ページ\)](#) を参照してください。

ステップ 1 管理対象デバイスの内部ネットワークにクライアントを接続します。

クライアントは、Windows、Mac、UNIX、など、実行しているオペレーティングシステムを問いません。クライアントを接続する方法の詳細はネットワークのセットアップ方法に応じて異なり、このガイドの対象外です。管理対象デバイスがインストールされているネットワークラックに手が届く状態であれば、デバイスの GigabitEthernet 0/1 ポートにクライアントを直接接続できます。

- ステップ 2** クライアントに静的 IP アドレス 10.10.1.50、デフォルトゲートウェイ 10.10.1.1、およびアクセス可能な任意の DNS サーバをセットアップします。
デフォルトゲートウェイは、内部インターフェイスの IP アドレスである必要があります。クライアントは、初めにこのゲートウェイに接続してから、トラフィックを内部または外部アドレスに送信します。
- ステップ 3** Firepower Management Center にログインします。
- ステップ 4** [デバイス (Devices)] > [デバイス管理 (Device Management)] をクリックします。
- ステップ 5** 管理対象デバイスの横にある  (トラブルシューティング) をクリックします。
- ステップ 6** [高度なトラブルシューティング (Advanced Troubleshooting)] をクリックします。
- ステップ 7** [パケットトレーサ (Packet Tracer)] タブをクリックします。
- ステップ 8** [Packet Tracer] タブ ページで、次の情報を入力します。



The screenshot shows the Packet Tracer configuration page. The 'Packet type' is set to TCP. The 'Source' is an IP address (IPv4) of 10.10.1.50. The 'Destination' is an IP address (IPv4) of 8.8.8.8. The 'Interface' is set to Outside. The 'Source Port' is 9090 and the 'Destination Port' is 80. The 'SGT number' is 0-65533 and the 'VLAN ID' is 1-4096. The 'Destination Mac Address' is XXXX.XXXX.XXXX. There are 'Start' and 'Clear' buttons at the bottom.

[Source] の IP アドレスと [Source Port] には、任意の値を指定できます。ここでテストするのは、トラフィックが内部インターフェイスから外部インターフェイスに転送されるかどうかです。この例では、[Destination] IP アドレスと [Destination Port] の値のみが使用されます。

- ステップ 9** クライアントで、ping を実行するかインターネットサイトを閲覧します。
- ステップ 10** [Packet Tracer] タブ ページで [Start] をクリックします。
結果の解釈については[結果の解釈 \(7 ページ\)](#) を参照してください。
- ステップ 11** [Capture w/Trace] タブをクリックします。
- ステップ 12** [Enable Auto-Refresh] をオンにして、必要に応じて更新間隔を変更します。
- ステップ 13** [キャプチャの追加 (Add Capture)] をクリックします。
- ステップ 14** [Add Capture] ダイアログボックスで、次の情報を入力します。

ステップ 15 [保存 (Save)]をクリックします。

ステップ 16 クライアントで、ping を実行するかインターネット サイトを参照します。

ステップ 17 下部のペインで  (更新) をクリックします。

Firepower Management Center の下部ペインに、パケットのキャプチャとトレースの結果が表示されます。次のようなメッセージを見つけます。このメッセージは、管理対象デバイスの内部インターフェイスからのトラフィックがアクセス コントロール ポリシーと一致していることを裏付けています。

```
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
```

結果の解釈についてのその他の情報は[結果の解釈 \(7 ページ\)](#) を参照してください。

パケット トレーサの詳細については、「[Packet Tracer Overview \(パケット トレーサの概要\)](#)」を参照してください。

ステップ 18 [Analysis] > [Connections] > [Events] をクリックします。

ステップ 19 右上隅の  をクリックしてページの更新頻度を調整します。

ステップ 20 [Preferences] タブをクリックします。

ステップ 21 [Refresh Interval (minutes)] フィールドに 1 を入力します。

ステップ 22 [適用 (Apply)] をクリックします。

ステップ 23 ページから移動して、[Connection Events] ページに戻ります。

ステップ 24 ページが更新されるまで待機します。
次のような接続イベントが表示されます。

Connection Events (switch, workflow)
Connections with Application Details | Table View of Connection Events
No Search Constraints (Edit Search) 2018-04-20 08:34:00 - 2018-04-20 09:46:23 Expanding

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 Category	URL Reputation	Device	
\$	2018-04-20 08:40:18	2018-04-20 08:40:22	Allow		10.10.1.50	USA	13.78.233.133	USA	insidezone	outsidezone	49228 / tcp	443 / https							10.10.2.45
\$	2018-04-20 08:39:57	2018-04-20 08:40:06	Allow		10.10.1.50	USA	13.78.233.133	USA	insidezone	outsidezone	49227 / tcp	443 / https							10.10.2.45
\$	2018-04-20 08:39:36	2018-04-20 08:39:45	Allow		10.10.1.50	USA	13.78.233.133	USA	insidezone	outsidezone	49226 / tcp	443 / https							10.10.2.45
\$	2018-04-20 08:39:15	2018-04-20 08:39:24	Allow		10.10.1.50	USA	13.78.233.133	USA	insidezone	outsidezone	49225 / tcp	443 / https							10.10.2.45
\$	2018-04-20 08:38:54	2018-04-20 08:39:03	Allow		10.10.1.50	USA	13.78.233.133	USA	insidezone	outsidezone	49224 / tcp	443 / https							10.10.2.45
\$	2018-04-20 08:38:33	2018-04-20 08:38:42	Allow		10.10.1.50	USA	13.78.233.133	USA	insidezone	outsidezone	49223 / tcp	443 / https							10.10.2.45
\$	2018-04-20 08:38:12	2018-04-20 08:38:21	Allow		10.10.1.50	USA	8.8.8.8	USA	insidezone	outsidezone	51253 / udp	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	8.8.8.8	USA	insidezone	outsidezone	51253 / udp	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	52.165.21.12	USA	insidezone	outsidezone	49222 / tcp	443 / https							10.10.2.45

ステップ 25 ビューをカスタマイズするには、[Table View of Connection Events] をクリックします。

詳細については、「[Connection and Security Intelligence Event Fields \(接続およびセキュリティインテリジェンス イベントフィールド\)](#)」および「[Using Connection and Security Intelligence Event Tables \(接続およびセキュリティインテリジェンスのイベントテーブルの使用\)](#)」を参照してください。

ステップ 26 パケットキャプチャメッセージと接続イベントが表示されれば成功です。システムは正常にセットアップされています。

次のタスク

エラーが表示される場合、またはクライアントがインターネットに接続できない場合は、[システムのトラブルシューティング \(6 ページ\)](#) を参照してください。

システムのトラブルシューティング

このトピックでは、システムで発生する可能性がある問題に対する解決策について説明します。多くは、ネットワーク クライアントがインターネットにアクセスできない問題です。

スタティック ルートとデフォルト ゲートウェイを確認する

次のように管理対象デバイスからインターネット サイトの ping を実行して、スタティック ルートとデフォルト ゲートウェイをチェックします。

1. SSH クライアントまたは仮想デバイスの管理コンソールを使用して、管理対象デバイスにログインします。
2. 管理対象デバイスで必要な場合は、次を入力します。 **connect ftd**
3. Enter **ping 8.8.8.8**

成功した場合、結果は次のように表示されます。

```
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
```

インターネット IP アドレスに対する ping が成功しない場合は、管理対象デバイスのインターフェイスが正しく接続されていることを確認してください。ケーブル両端のリンクとアクティビティの LED が点灯（アクティビティ LED は点滅）していることを確認してください。

接続イベントが表示されない

接続イベントが表示されない最も可能性が高い理由は、アクセス コントロールルールまたはアクセスコントロールポリシーでロギングを有効にしていないことです。[アクセスコントロールポリシーの編集 \(1 ページ\)](#) を参照してください。

結果の解釈

このトピックでは、パケット キャプチャおよび traceroute コマンドの結果を解釈する方法について説明します。

パケット トレーサの解釈

以下のパケット トレーサからの抜粋は、重要な情報および内部インターフェイスから外部インターフェイスへのトラフィック転送における判断が示されています。このガイドで説明した設定情報の一部が強調表示されています。次の点に注意してください。

- Phase 3 は、外部ゲートウェイを 209.165.200.254 に解決しています。
- Phase 4 は、一時的な許可ポリシー（Temporary Allow Policy）の初回の呼び出しを示しています。
- Phase 6 は、内部のクライアントから外部インターフェイスへ転送する NAT ポリシーを示しています。
- Phase 16 は、一時的な許可ポリシーに基づいてトラフィックを許可する、インスペクションエンジン（Snort）を示しています。

これらのいずれかのフェーズでのエラーは、ポリシーが誤って設定されているかどうか、またはトラフィックをブロックするように設定されているかどうかに応じて、トラフィックの拒否またはドロップの原因となり得ます。

```
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
```



(注) [Packet Tracker]と [Capture w/Trace] には異なるフェーズ番号が表示されますが、各フェーズで表示される情報はほぼ同一です。



- (注) 最終的な SNORT フェーズがない場合は、ROUTE-LOOKUP フェーズでエラーを探します。たとえば、次は外部インターフェイスに問題があることを示している場合があります。該当インターフェイスの IP アドレスと外部ゲートウェイの IP アドレスを確認してください。

```
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
```

症状：ネットワークが変換されない

パケットキャプチャに次のような行が存在しない場合、多くの場合 NAT が正しくセットアップされていないことを意味します。

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

解決策： [NAT ポリシーの追加](#)の説明に従ってダイナミック NAT を設定します。

症状：アクセスコントロールポリシーがトラフィックをブロックする

アクセスコントロールポリシーがトラフィックを許可するのではなくトラフィックをブロックするように設定されている場合、パケットキャプチャには次の行が含まれます。

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

これに該当するかどうかは、**[Analysis]** > **[Connections]** > **[Events]** で接続イベントを調べて確認できます。

解決策： [アクセスコントロールポリシーの編集 \(1 ページ\)](#)の説明に従って、トラフィックを許可するようにアクセスコントロールポリシーを設定します。

