Cisco ASA での VPN フィルタの設定例

内容

概要

このドキュメントでは、VPNフィルタについて詳細に説明し、LAN-to-LAN(L2L)、Cisco VPN Client、およびCisco AnyConnectセキュアモビリティクライアントに適用されます。

フィルタは、セキュリティ アプライアンスを経由して着信したトンネリングされたデータ パケットを、送信元アドレス、宛先アドレス、プロトコルなどの基準によって、許可するか拒否するかを決定するルールで構成されます。さまざまなタイプのトラフィックを許可または拒否するには、アクセスコントロールリスト(ACL)を設定します。フィルタは、グループポリシー、ユーザ名属性、またはダイナミックアクセスポリシー(DAP)で設定できます。

DAPは、ユーザ名属性とグループポリシーの両方で設定された値よりも優先されます。DAPがフィルタを割り当てない場合、ユーザ名属性値がグループポリシー値よりも優先されます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- L2L VPNトンネルの設定
- VPN Client Remote Access(RA)の設定
- AnyConnect RAの設定

使用するコンポーネント

このドキュメントの情報は、Cisco 5500-Xシリーズ適応型セキュリティアプライアンス(ASA)バージョン9.1(2)に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

sysopt connection permit-vpnコマンドを使用すると、VPNトンネル経由でセキュリティアプライアンスに入るすべてのトラフィックがインターフェイスアクセスリストをバイパスできるようになります。グループ ポリシーおよびユーザ単位の認可アクセス リストは、引き続きトラフィックに適用されます。

vpn-filterは、トンネルを出た後の復号後のトラフィックと、トンネルに入る前の暗号化前のトラフィックに適用されます。VPNフィルタに使用されるACLは、インターフェイスアクセスグループにも使用しないでください。

リモートアクセスVPNクライアント接続を制御するグループポリシーにvpn-filterを適用する場合、ACLは、クライアントによって割り当てられたIPアドレスをACLのsrc_ip位置に、ローカルネットワークをACLのdest_ip位置に設定して設定する必要があります。L2L VPN接続を制御するグループポリシーにvpn-filterを適用する場合、ACLは、ACLのsrc_ip位置のリモートネットワークと、ACLのdest_ip位置のローカルネットワークで設定する必要があります。

設定

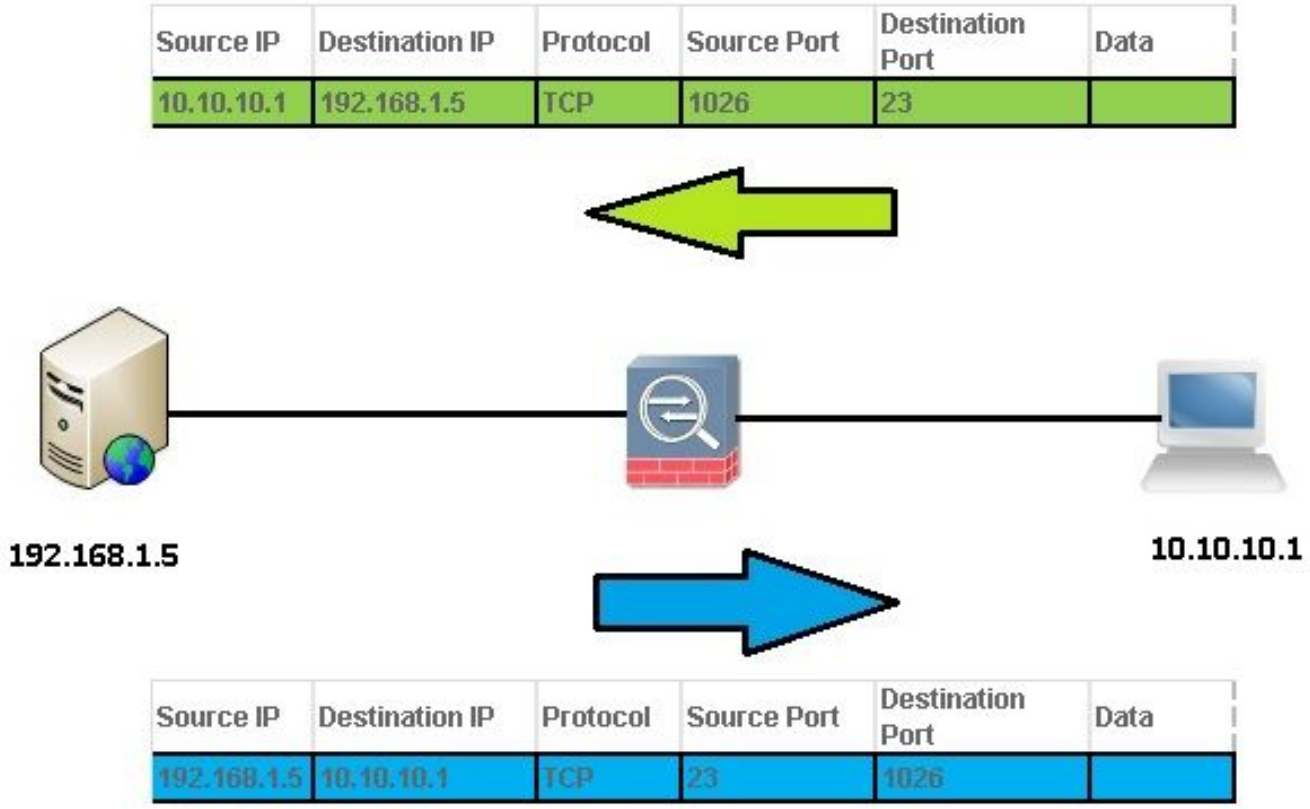
VPNフィルタはインバウンド方向で設定する必要がありますが、ルールは双方向に適用されます。単方向ルールをサポートするために拡張CSCsf99428が公開されましたが、実装のスケジュール設定やコミットは行われていません。

例1:AnyConnectまたはVPN Clientでのvpn-filter

クライアントに割り当てられたIPアドレスが10.10.10.1/24で、ローカルネットワークが192.168.1.0/24であるとします。

このアクセスコントロールエントリ(ACE)により、AnyConnectクライアントはローカルネットワークにTelnet接続できます。

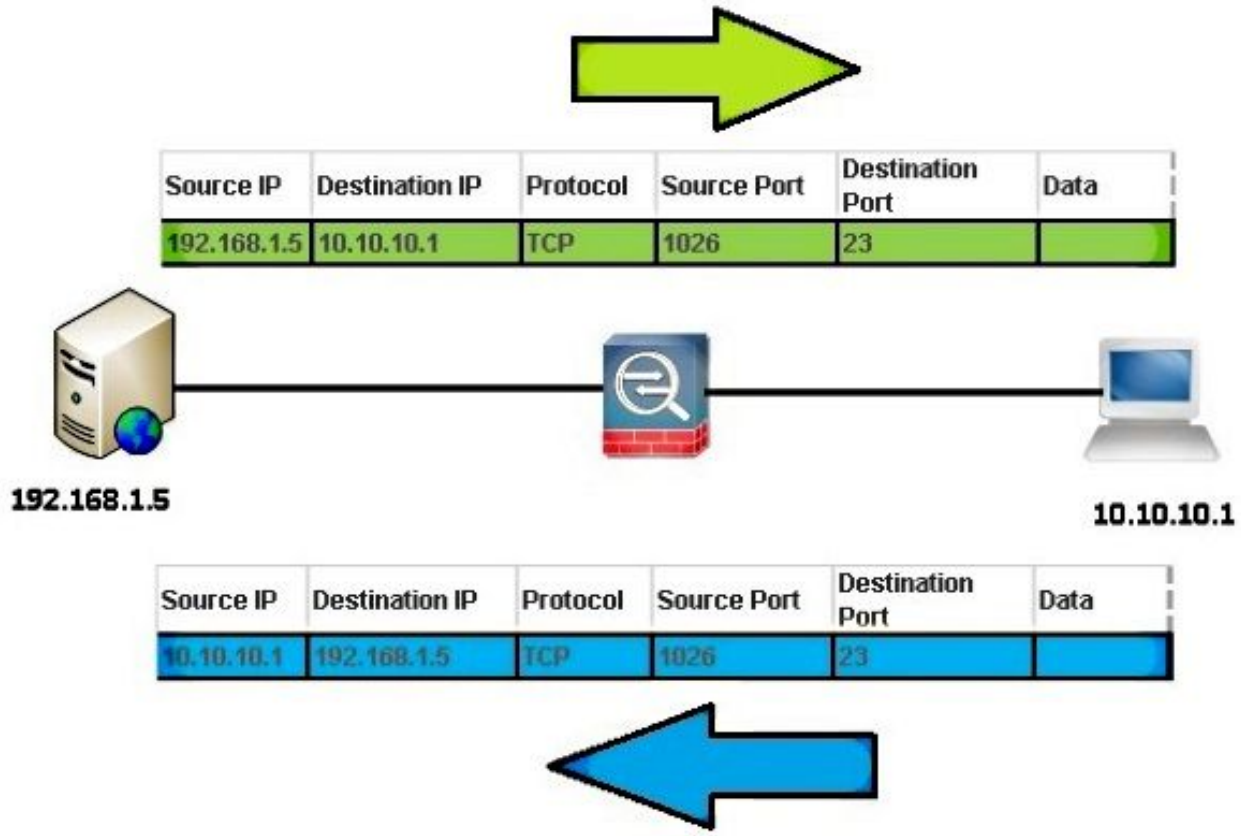
```
access-list vpnfilt-ra permit tcp
10.10.10.1 255.255.255.255 192.168.1.0 255.255.255.0 eq 23
```



注：ACE access-list vpnfilt-ra permit tcp 10.10.1 255.255.255.255 192.168.1.0 255.255.255.0 eq 23では、送信元ポート23を使用する場合、ローカルネットワークは任意のTCPポートでRAクライアントへの接続を開始できます。

このACEにより、ローカルネットワークからAnyConnectクライアントにTelnet接続できます。

```
access-list vpnfilt-ra permit tcp 10.10.10.1 255.255.255.255
eq 23 192.168.1.0 255.255.255.0
```



注：ACE access-list vpnfilt-ra permit tcp 10.10.1 255.255.255.255 eq 23 192.168.1.0 255.255.255.0では、送信元ポート23を使用する場合、RAクライアントは任意のTCPポートでローカルネットワークへの接続を開始できます。

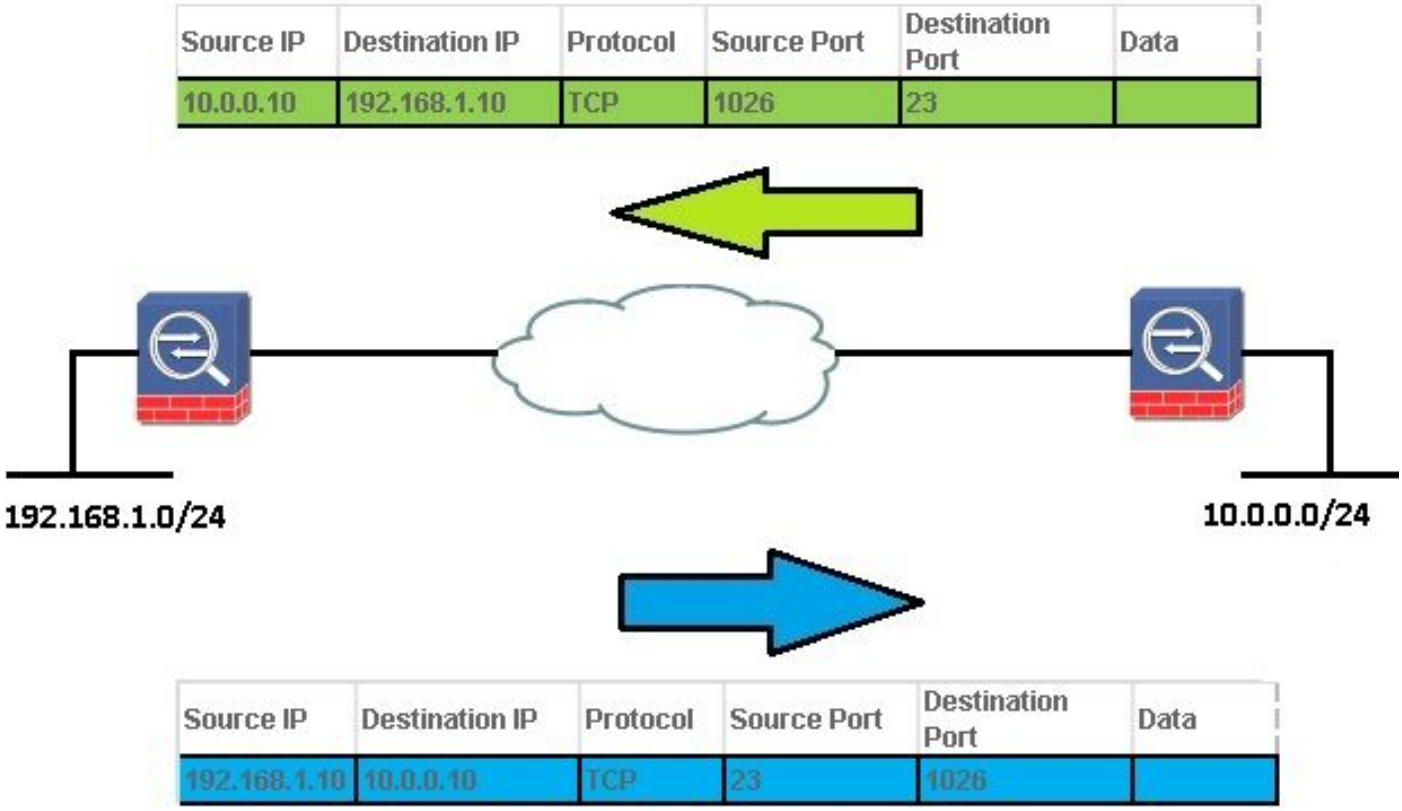
注意：vpn-filter機能を使用すると、トラフィックをインバウンド方向でのみフィルタリングでき、アウトバウンドルールが自動的にコンパイルされます。したがって、インターネット制御メッセージプロトコル(ICMP)アクセスリストを作成する際に、指向性フィルタが必要な場合は、アクセスリスト形式でICMPタイプを指定しないでください。

例2:L2L VPN接続でのvpn-filter

リモートネットワークが10.0.0.0/24で、ローカルネットワークが192.168.1.0/24であるとします。

このACEにより、リモートネットワークからローカルネットワークにTelnet接続できます。

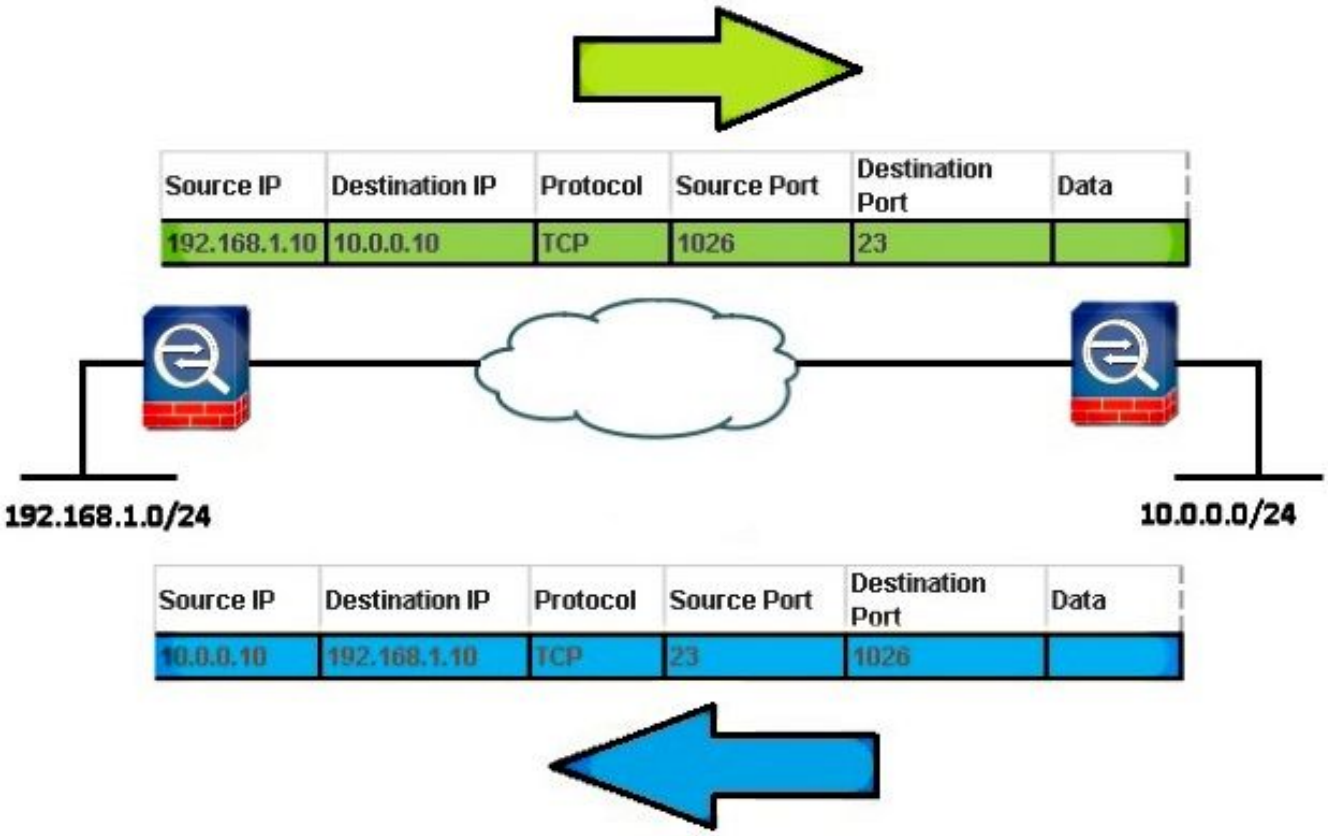
```
access-list vpnfilt-l2l permit tcp 10.0.0.0 255.255.255.0 192.168.1.0
255.255.255.0 eq 23
```



注:ACE access-list vpnfilt-l2l permit tcp 10.0.0.0 255.255.255.0 192.168.1.0 255.255.255.0 eq 23では、送信元ポート23を使用する場合、ローカルネットワークが任意のTCPポートでリモートネットワークへの接続を開始することもできます。

このACEにより、ローカルネットワークからリモートネットワークにTelnet接続できます。

```
access-list vpnfilt-l2l permit tcp 10.0.0.0 255.255.255.0 eq 23
192.168.1.0 255.255.255.0
```



注:ACEアクセスリストvpnfilt-l2l permit tcp 10.0.0.0 255.255.255.0 eq 23 192.168.1.0 255.255.255.0では、送信元ポート23を使用する場合、リモートネットワークによる任意のTCPポートでのローカルネットワークへの接続の開始も許可されます。

注意：vpn-filter機能を使用すると、トラフィックをインバウンド方向でのみフィルタリングでき、アウトバウンドルールが自動的にコンパイルされます。したがって、ICMPアクセスリストを作成する際に、指向性フィルタが必要な場合は、アクセスリスト形式でICMPタイプを指定しないでください。

VPNフィルタおよびユーザごとの上書きアクセスグループ

VPNトラフィックはインターフェイスACLによってフィルタリングされません。デフォルトの動作を変更するには、コマンド**no sysopt connection permit-vpn**を使用できます。この場合、ユーザトラフィックに次の2つのACLを適用できます。最初にインターフェイスACLがチェックされ、次にvpn-filterがチェックされます。

per-user-overrideキーワード（インバウンドACLのみ）を使用すると、ユーザ許可のためにダウンロードされたダイナミックユーザACLによって、インターフェイスに割り当てられたACLが上書きされます。たとえば、インターフェイスACLで10.0.0.0からのトラフィックはすべて拒否されるが、ダイナミックACLで10.0.0.0からのトラフィックはすべて許可される場合、ダイナミックACLはそのユーザのインターフェイスACLを上書きし、トラフィックは許可されます。

例(**no sysopt connection permit-vpn**が設定されている場合):

- no per-user-override, no vpn-filter：トラフィックがインターフェイスACLと照合されます。
- no per-user-override, vpn-filter：トラフィックはまずインターフェイスACLと照合され、次に

vpn-filterと照合されます。

- per-user-override、vpn-filter：トラフィックはvpn-filterのみに対して照合されます。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

Cisco CLI アナライザ（登録ユーザ専用）は、特定の show コマンドをサポートします。show コマンド出力の分析を表示するには、Cisco CLI アナライザを使用します。

- **show asp table filter [access-list <*acl-name*>] [hits]**

  Accelerated Security Path(ASP)フィルタテーブルをデバッグするには、特権EXECモードで**show asp table filter**コマンドを使用します。フィルタがVPNトンネルに適用されると、フィルタルールがフィルタテーブルにインストールされます。トンネルにフィルタが指定されている場合は、内部パケットを許可するか拒否するかを決定するために、暗号化前と復号化後にフィルタテーブルがチェックされます。

```
 USAGE
 show asp table filter [access-list
```

```
 SYNTAX <acl-name>      Show installed filter for access-list <acl-name>
hits Show filter rules which have non-zero hits values
```

- **clear asp table filter [access-list <*acl-name*>]**

  このコマンドは、ASPフィルタテーブルエントリのヒットカウンタをクリアします。

```
 USAGE
clear asp table filter [access-list
```

```
 SYNTAX
<acl-name> Clear hit counters only for specified access-list <acl-name>
```

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

Cisco CLI アナライザ（登録ユーザ専用）は、特定の show コマンドをサポートします。show コマンド出力の分析を表示するには、Cisco CLI アナライザを使用します。

> **注：debug コマンドを使用する前に、「デバッグ コマンドの重要な情報」を参照してください。**

- **debug acl filter**

  このコマンドは、VPNフィルタのデバッグを有効にします。ASPフィルタテーブルへのVPNフィルタのインストール/削除のトラブルシューティングに使用できます。例1:AnyConnectまたはVPN Clientを使用したvpn-filterの場合。

  user1の接続時のデバッグ出力：

```
 ACL FILTER INFO: first reference to inbound filter vpnfilt-ra(2): Installing
rule into NP.
ACL FILTER INFO: first reference to outbound filter vpnfilt-ra(2): Installing
rule into NP.
```

  user2の接続時のデバッグ出力（user1と同じフィルタの後）：

```
 ACL FILTER INFO: adding another reference to outbound filter vpnfilt-ra(2): refCnt=2
ACL FILTER INFO: adding another reference to inbound filter vpnfilt-ra(2): refCnt=2
```

  user2の接続解除時のデバッグ出力：

```
 ACL FILTER INFO: removing a reference from inbound filter vpnfilt-ra(2): remaining
refCnt=1
ACL FILTER INFO: removing a reference from outbound filter vpnfilt-ra(2): remaining
refCnt=1
```

  user1の接続解除時のデバッグ出力：

```
 ACL FILTER INFO: releasing last reference from inbound filter vpnfilt-ra(2): Removing
rule into NP.
ACL FILTER INFO: releasing last reference from outbound filter vpnfilt-ra(2): Removing
rule into NP.
```

- **show asp table**

  user1が接続する前の**show asp table filter**の出力を次に示します。IPv4とIPv6に対して、イン方向とアウト方向の両方に暗黙の拒否ルールだけがインストールされます。

```
 Global Filter Table:
in id=0xd616ef20, priority=11, domain=vpn-user, deny=true
hits=0, user_data=0xd613ea60, filter_id=0x0(-implicit deny-), protocol=0
src ip=0.0.0.0, mask=0.0.0.0, port=0
dst ip=0.0.0.0, mask=0.0.0.0, port=0
in id=0xd616f420, priority=11, domain=vpn-user, deny=true
hits=0, user_data=0xd615ef70, filter_id=0x0(-implicit deny-), protocol=0
src ip=::/0, port=0
dst ip=::/0, port=0
out id=0xd616f1a0, priority=11, domain=vpn-user, deny=true
hits=0, user_data=0xd614d900, filter_id=0x0(-implicit deny-), protocol=0
src ip=0.0.0.0, mask=0.0.0.0, port=0
dst ip=0.0.0.0, mask=0.0.0.0, port=0
out id=0xd616f6d0, priority=11, domain=vpn-user, deny=true
hits=0, user_data=0xd6161638, filter_id=0x0(-implicit deny-), protocol=0
src ip=::/0, port=0
dst ip=::/0, port=0
```

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。