



## 統合

次のセクションでは、Cisco ISE 機能をサポートするためにスイッチおよびワイヤレスコントローラに必要な構成について説明します。

- [スイッチでの標準 Web 認証のサポートの有効化 \(2 ページ\)](#)
- [代理 RADIUS トランザクション用のローカルユーザー名とパスワードの定義 \(2 ページ\)](#)
- [ログとアカウンティングのタイムスタンプの正確性を保証するための NTP サーバー設定 \(2 ページ\)](#)
- [AAA 機能を有効にするコマンド \(2 ページ\)](#)
- [スイッチ上の RADIUS サーバーの設定 \(3 ページ\)](#)
- [RADIUS 認可変更 \(CoA\) を処理するスイッチの有効化 \(4 ページ\)](#)
- [スイッチポートでのデバイストラッキングと DHCP スヌーピングの有効化 \(4 ページ\)](#)
- [スイッチポート用 802.1X ポートベースの認証の有効化 \(5 ページ\)](#)
- [クリティカルな認証に対する EAP の有効化 \(5 ページ\)](#)
- [リカバリの遅延を使用した AAA 要求のスロットリング \(5 ページ\)](#)
- [適用状態に基づく VLAN の定義 \(5 ページ\)](#)
- [スイッチでのローカル \(デフォルト\) アクセスリスト \(ACL\) の定義 \(6 ページ\)](#)
- [802.1X および MAB のスイッチ ポートの有効化 \(7 ページ\)](#)
- [Identity-Based Network Services に基づいて 802.1X を有効にするコマンド \(9 ページ\)](#)
- [EPM ロギングの有効化 \(10 ページ\)](#)
- [SNMP トラップを受信するためのスイッチの有効化 \(11 ページ\)](#)
- [プロファイリング用の SNMP v3 クエリーの有効化 \(11 ページ\)](#)
- [プロファイラによる収集を可能にするための MAC 通知トラップの有効化 \(11 ページ\)](#)
- [スイッチ上での RADIUS アイドルタイムアウトの設定 \(12 ページ\)](#)
- [iOS サブリカントのプロビジョニング用のワイヤレスコントローラの構成 \(12 ページ\)](#)
- [MDM 相互運用性のためのワイヤレス LAN コントローラでの ACL の設定 \(13 ページ\)](#)

## スイッチでの標準 Web 認証のサポートの有効化

認証時の URL リダイレクションのプロビジョニングなど、Cisco ISE 用の標準 Web 認証機能を有効にするには、次のコマンドをスイッチの構成に含めます。

```
ip classless
```

```
ip route 0.0.0.0 0.0.0.0 10.1.2.3
```

```
ip http server
```

```
! Must enable HTTP/HTTPS for URL-redirectation on port 80/443
```

```
ip http secure-server
```

## 代理 RADIUS トランザクション用のローカルユーザー名とパスワードの定義

スイッチがこのネットワーク セグメントの RADIUS サーバーであるかのように Cisco ISE ノードと通信するには、次のコマンドを入力します。

```
username test-radius password 0 abcde123
```

## ログとアカウントिंगのタイムスタンプの正確性を保証するための NTP サーバー設定

次のコマンドを入力して、Cisco ISE で設定したのと同じ NTP サーバーをスイッチ上に指定していることを確認します。

```
ntp server <IP_address>|<domain_name>
```

## AAA 機能を有効にするコマンド

802.1X および MAB 認証機能など、スイッチと Cisco ISE との間でさまざまな AAA 機能を有効にするには、スイッチ上で次のコマンドを入力します。

```
aaa new-model
```

```
! Creates an 802.1X port-based authentication method list
```

```
aaa authentication dot1x default group radius
```

```
! Required for VLAN/ACL assignment

aaa authorization network default group radius

! Authentication & authorization for webauth transactions

aaa authorization auth-proxy default group radius

! Enables accounting for 802.1X and MAB authentications

aaa accounting dot1x default start-stop group radius

!

aaa session-id common

!

aaa accounting update periodic 1440

! Update AAA accounting information periodically every 1440 minutes

aaa accounting system default start-stop group radius

!
```

## スイッチ上の RADIUS サーバーの設定

Cisco ISE とやり取りし、RADIUS ソース サーバーとして動作するようスイッチを設定するには、次のコマンドを入力します。

```
!
radius-server <ISE Name>

! ISE Name is the name of the ISE PSN

address ipv4 <ip address> auth-port 1812 acct-port 1813

! IP address is the address of the PSN. This example uses the standard RADIUS ports.

key <passwd>

! passwd is the secret password configured in Cisco ISE

exit
```



(注) 3回の再試行を含む30秒のデッド基準時間を設定し、Active Directoryを認証に使用するRADIUS要求に対して、より長い応答時間を提供することを推奨します。

## RADIUS 認可変更 (CoA) を処理するスイッチの有効化

スイッチが Cisco ISE で RADIUS CoA の動作と関連するポスチャ機能を適切に処理できるように設定を指定するには、次のコマンドを入力します。

```
aaa server radius dynamic-author client <ISE-IP> server-key 0 abcde123
```



- (注)
- Cisco ISE では、RFC の CoA 用デフォルトポート 3799 に対して、ポート 1700 (Cisco IOS ソフトウェアのデフォルト) を使用します。既存の Cisco Secure ACS 5.x ユーザーは、既存の ACS の実装の一部として CoA を使用している場合、すでにこれをポート 3799 に設定している可能性があります。
  - 秘密キーは、ネットワークデバイスの追加時に Cisco ISE で設定したものと同一である必要があります、IP アドレスは PSN IP アドレスである必要があります。

## スイッチポートでのデバイストラッキングと DHCP スヌーピングの有効化

セキュリティに関連する Cisco ISE のオプション機能を提供できるようにするには、次のコマンドを入力することによって、スイッチポートのダイナミック ACL 内での IP 置換に関して、デバイストラッキングと DHCP スヌーピングを有効化します。

```
! Optional
```

```
ip dhcp snooping
```

```
! Required!
```

```
! Configure Device Tracking Policy!device-tracking policy <DT_POLICY_NAME>no protocol ndp tracking enable
```

```
! Bind it to interface!interface <interface_id>device-tracking attach-policy<DT_POLICY_NAME>
```

RADIUS アカウンティングでは、DHCP スヌーピングが有効になっていても、DHCP 属性は IOS センサーによって Cisco ISE に送信されません。このような場合、DHCP スヌーピングを VLAN で有効にして DHCP をアクティブにする必要があります。

VLAN で DHCP スヌーピングを有効にするには、次のコマンドを使用します。

```
ip dhcp snooping
```

```
ip dhcp snooping vlan 1-100
```

## スイッチポート用 802.1X ポートベースの認証の有効化

スイッチポートに対してグローバルに 802.1X 認証を有効にするには、次のコマンドを入力します。

```
dot1x system-auth-control
```

## クリティカルな認証に対する EAP の有効化

サブリカントによる LAN 経由での認証要求をサポートするには、次のコマンドを入力することによって、EAP をクリティカルな認証（アクセスできない認証バイパス）に対して有効にします。

```
dot1x critical eapol
```

## リカバリの遅延を使用した AAA 要求のスロットリング

クリティカルな認証リカバリの場合は、自動的に認証遅延（秒単位）を発生させるようにスイッチを設定し、リカバリ後に Cisco ISE が再びサービスを開始できるようにします。次のコマンドを使用します。

```
authentication critical recovery delay 1000
```

## 適用状態に基づく VLAN の定義

ネットワーク内の既知の適用状態に基づいて VLAN 名、番号、およびスイッチ仮想インターフェイス（SVI）を定義するには、次のコマンドを入力します。ネットワーク間のルーティングを有効にするには、それぞれの VLAN インターフェイスを作成します。これは特に、エンドポイントがネットワークに接続するときに経由するエンドポイント（PC やラップトップ）と IP 電話の両方からの同じネットワークセグメントを経由して渡される複数のソースからのトラフィックを処理する場合に役立ちます。次に例を示します。

```
vlan <VLAN_number>
name ACCESS!
vlan <VLAN_number>
name VOICE

!
interface <VLAN_number>
description ACCESS
ip address 10.1.2.3 255.255.255.0
ip helper-address <DHCP_Server_IP_address>
ip helper-address <Cisco_ISE_IP_address>
```

```
!  
interface <VLAN_number>  
description VOICE  
ip address 10.2.3.4 255.255.255.0  
ip helper-address <DHCP_Server_IP_address>
```

## スイッチでのローカル（デフォルト）アクセスリスト（ACL）の定義

このような機能を古いバージョンのスイッチ（Cisco IOS ソフトウェア リリースのバージョンが 12.2(55)SE よりも前）で有効にし、Cisco ISE が認証と許可に必要なダイナミック ACL の更新を実行できるようにするには、次のコマンドを入力します。

```
ip access-list extended ACL-ALLOW  
  
    permit ip any any  
  
!  
  
ip access-list extended ACL-DEFAULT  
  
    remark DHCP  
  
    permit udp any eq bootpc any eq bootps  
  
    remark DNS  
  
    permit udp any any eq domain  
  
    remark Ping  
  
    permit icmp any any  
  
    remark Ping  
  
    permit icmp any any  
  
    remark PXE / TFTP  
  
    permit udp any any eq tftp  
  
    remark Allow HTTP/S to ISE and WebAuth portal  
    permit tcp any host <Cisco_ISE_IP_address> eq www  
  
    permit tcp any host <Cisco_ISE_IP_address> eq 443  
  
    permit tcp any host <Cisco_ISE_IP_address> eq 8443
```

```
permit tcp any host <Cisco_ISE_IP_address> eq 8905
permit udp any host <Cisco_ISE_IP_address> eq 8905
permit udp any host <Cisco_ISE_IP_address> eq 8906
permit tcp any host <Cisco_ISE_IP_address> eq 8080
permit udp any host <Cisco_ISE_IP_address> eq 9996

remark Drop all the rest

deny ip any any log

!

! The ACL to allow URL-redirection for WebAuth
ip access-list extended ACL-WEBAUTH-REDIRECT

permit tcp any any eq www

permit tcp any any eq 443
```



(注) ワイヤレスコントローラでこの設定を行うと、CPU使用率が増加し、システムが不安定になるリスクが高まります。これは IOS の問題で、Cisco ISE は悪影響を受けません。

## 802.1X および MAB のスイッチ ポートの有効化

802.1X および MAB のスイッチ ポートを有効にするには、以下の手順を実行します。

- ステップ 1 すべてのアクセススイッチポートのインターフェイス コンフィギュレーション モードを開始します。  
**interface range FastEthernet0/1-8**
- ステップ 2 次のように、（トランク モードではなく）アクセス モードのスイッチ ポートを有効にします。  
**switchport mode access**
- ステップ 3 静的にアクセス VLAN を設定します。アクセス VLAN のローカル プロビジョニングを提供するこの手順は、オープンモード認証に必要となります。  
**switchport access vlan <VLAN\_number>**
- ステップ 4 静的に音声 VLAN を設定します。  
**switchport voice vlan <VLAN\_number>**
- ステップ 5 オープン モード認証を有効にします。オープンモードを使用すると、認証が完了する前に、トラフィックをデータおよび音声 VLAN 上にブリッジングできます。実稼働環境では、ポートベースの ACL を使用して不正アクセスを防ぐことを強く推奨します。

オープンモード認証を有効にすると、ポート ACL に従って AAA サーバー応答の前に事前認証アクセスも可能になります。

#### **authentication open**

**ステップ 6** ポートベースの ACL を適用して、認証されていないエンドポイントからアクセス VLAN 上にデフォルトでどのトラフィックをブリッジングするかを決定します。最初にすべてのアクセスを許可してからポリシーを適用する必要があるため、ACL-ALLOW を適用して、スイッチポートを通過するすべてのトラフィックを許可する必要があります。すでに現時点のすべてのトラフィックを許可するデフォルトの Cisco ISE 許可を作成しましたが、この理由は、完全な可視性を実現し、既存のエンドユーザー環境にはまだ影響を与えないようにするためです。

ACL は AAA サーバーから動的 ACL の前に追加されるように設定する必要があります。

#### **ip access-group ACL-ALLOW in**

(注) DSBU スイッチ上に Cisco IOS Release 12.2(55)SE ソフトウェアを用意する前に、RADIUS AAA サーバーからのダイナミック ACL を適用するためのポート ACL が必要です。デフォルトの ACL を用意できなかった場合、割り当てられた動的 ACL はスイッチによって無視されます。Cisco IOS ソフトウェアのリリース 12.2(55)SE では、デフォルトの ACL が自動的に生成および適用されます。

(注) テストの現段階では、ポートベースの 802.1X 認証を有効にし、さらに既存のネットワークに対する影響を避けるために、ACL-ALLOW を使用しています。今後のテストでは、実稼働環境に必要なトラフィックをブロックする、異なる ACL-DEFAULT を適用する予定です。

**ステップ 7** マルチ認証ホストモードを有効にします。マルチ認証は、基本的には複数ドメイン認証 (MDA) のスーパーセットです。MDA では、データドメイン内の単一のエンドポイントだけが許可されます。マルチ認証を設定すると、音声ドメイン内では認証された単一の電話が (MDA の場合と同じように) 許可されますが、データドメイン内では認証できるデータデバイスの数に制限がありません。

同じ物理アクセスポート上の音声と複数のエンドポイントが許可されます。

#### **authentication host-mode multi-auth**

(注) IP 電話の背後で複数のデータデバイス (仮想デバイスであるかハブに接続されている物理デバイスであるかにかかわらず) を使用すると、アクセスポートの物理リンクステータス認識度が低下する可能性があります。

**ステップ 8** 次のコマンドを使用して、さまざまな認証方式オプションを有効にします。

次のように、再認証を有効にします。

#### **authentication periodic**

次のように、RADIUS セッションタイムアウトを介して再認証を有効にします。

#### **authentication timer reauthenticate server**

#### **authentication event fail action next-method**

デッドサーバーの場合は、次のようにクリティカル認証 VLAN 方式を設定します。

#### **authentication event server dead action reinitialize vlan <VLAN\_number>**

#### **authentication event server alive action reinitialize**

次のように、802.1X と MAB の IOS Flex-Auth 認証を設定します。



```
authentication order dot1x mab
authentication priority dot1x mab
```

ステップ 9 次のように、スイッチ ポートで 802.1X ポート制御を有効にします。

```
authentication port-control auto
authentication violation restrict
```

ステップ 10 次のように、MAC 認証バイパス (MAB) を有効にします。

```
mab
```

ステップ 11 次のように、スイッチポート上で 802.1X を有効にします。

```
dot1x pae authenticator
```

ステップ 12 次のように、再送信時間を 10 秒に設定します。

```
dot1x timeout tx-period 10
```

(注) 802.1X tx-period のタイムアウトは 10 秒に設定する必要があります。この値を変更する場合は、その影響を理解したうえで行ってください。

ステップ 13 次のように、PortFast 機能を有効にします。

```
spanning-tree portfast
```

---

## Identity-Based Network Services に基づいて 802.1X を有効にするコマンド

次の例は、802.1X、MAB、および Web 認証を使用する連続認証方式を許可するように設定されている制御ポリシーを示しています。

```
class-map type control subscriber match-all DOT1X
  match method dot1x
  !
class-map type control subscriber match-all DOT1X_FAILED
  match method dot1x
  match result-type method dot1x authoritative
  !
class-map type control subscriber match-all DOT1X_NO_RESP
  match method dot1x
  match result-type method dot1x agent-not-found
  !
class-map type control subscriber match-all MAB
  match method mab
  !
class-map type control subscriber match-all MAB_FAILED
  match method mab
  match result-type method mab authoritative
  !
  !

policy-map type control subscriber DOT1XMAB
  event session-started match-all
```

```

10 class always do-until-failure
  10 authenticate using dot1x retries 2 retry-time 0 priority 10
event authentication-failure match-first
10 class DOT1X_NO_RESP do-until-failure
  10 terminate dot1x
  20 authenticate using mab priority 20
20 class DOT1X_FAILED do-until-failure
  10 terminate dot1x
  20 authenticate using mab priority 20
  30 authorize
40 class always do-until-failure
  10 terminate dot1x
  20 terminate mab
  30 authentication-restart 60
event agent-found match-all
  10 class always do-until-failure
  10 terminate mab
  20 authenticate using dot1x retries 2 retry-time 0 priority 10
!

```

次の例は、MAB、802.1X、および Web 認証を使用する連続認証方式を許可するように設定されている制御ポリシーを示しています。

```

policy-map type control subscriber MABDOT1X
event session-started match-all
  10 class always do-until-failure
  10 authenticate using mab priority 20
  20 authenticate using dot1x priority 10
event authentication-failure match-first
  10 class ALL_FAILED do-until-failure
  10 authentication-restart 60
event authentication-success match-all
  10 class DOT1X do-until-failure
  10 terminate mab
event agent-found match-all
  10 class always do-until-failure
  10 authenticate using dot1x priority 10

```

サービスポリシーをインターフェイスに適用します。

```

interface GigabitEthernet1/0/4
switchport mode access
device-tracking attach-policy poll
ip access-group sample in
authentication timer reauthenticate server
access-session port-control auto
mab
dot1x pae authenticator
dot1x timeout tx-period 10
dot1x timeout auth-period 10
spanning-tree portfast
service-policy type control subscriber DOT1XMAB

```

## EPM ログイングの有効化

Cisco ISE の機能について発生する可能性があるトラブルシューティングや記録をサポートするには、スイッチに標準のログイング機能を次のように設定します。

**epm logging**

## SNMP トラップを受信するためのスイッチの有効化

次のように、スイッチがこのネットワークセグメント内の適切な VLAN を経由して、Cisco ISE から SNMP トラップ送信を受信できるようにします。

```
snmp-server community public RO
snmp-server trap-source <VLAN_number>
```

## プロファイリング用の SNMP v3 クエリーの有効化

SNMP v3 ポーリングが正常に実行され、Cisco ISE プロファイリングサービスがサポートされるように、次のコマンドを使用してスイッチを設定します。その前に、SNMP 設定を Cisco ISE の GUI の [SNMP 設定 (SNMP Settings)] ウィンドウで設定します。このウィンドウを表示するには、[メニュー (Menu)] アイコン (☰) をクリックして次を選択します。[管理 (Administration)] > [ネットワークリソース (Network Resources)] > [ネットワークデバイス (Network Devices)] > [追加 | 編集 (Add | Edit)] > [SNMP 設定 (SNMP Settings)]。

```
Snmp-server user <name> <group> v3 auth md5 <string> priv des <string>
snmp-server group <group> v3 priv
snmp-server group <group> v3 priv context vlan-1
```



- (注) `snmp-server group <group> v3 priv context vlan-1` コマンドは、コンテキストごとに設定する必要があります。`snmp show context` コマンドでは、すべてのコンテキスト情報がリストされません。

SNMP 要求がタイムアウトになり、接続の問題が発生していない場合は、タイムアウト値を増加させることができます。

## プロファイラによる収集を可能にするための MAC 通知トラップの有効化

次のように、適切な MAC 通知トラップを送信するようスイッチを設定し、Cisco ISE のプロファイラ機能がネットワークエンドポイントで情報を収集できるようにします。

```
mac address-table notification change
mac address-table notification mac-move
snmp trap mac-notification change added
snmp trap mac-notification change removed
```

## スイッチ上での RADIUS アイドルタイムアウトの設定

スイッチに RADIUS Idle-timeout を設定するには、次のコマンドを使用します。

```
Switch(config-if)# authentication timer inactivity
```

ここで、*inactivity* は、クライアントアクティビティが不正と見なされるまでの非アクティブ間隔を秒単位で表したものです。

Cisco ISE では、そのようなセッション非アクティブタイマーを適用する認証ポリシーに対してこのオプションを有効にできます。[ポリシー (Policy)]>[ポリシー要素 (Policy Elements)]>[結果 (Authorization)]>[承認 (Authorization)]>[認証プロファイル (Authorization Profiles)] Cisco ISE GUI で [メニュー (Menu)] アイコン (☰) をクリックして次を選択します。[ポリシー (Policy)]>[ポリシー要素 (Policy Policy Elements)]>[結果 (Authorization)]>[承認 (Authorization)]>[認証プロファイル (Authorization Profiles)] を選択します。

## iOS サプリカントのプロビジョニング用のワイヤレスコントローラの構成

### シングル SSID の場合

同じワイヤレスアクセスポイントで、Apple iOS ベースのデバイス (iPhone または iPad) が、ある SSID から別の SSID に切り替えることができるようにするには、**FAST SSID change** 機能を有効にするようワイヤレスコントローラを設定します。この機能によって、iOS ベースのデバイスが SSID 間の切り替えを迅速に行えるようにします。

### デュアル SSID BYOD の場合

デュアル SSID BYOD をサポートするには、Fast SSID が有効になっている必要があります。ワイヤレスコントローラで Fast SSID Change が有効になっている場合、クライアントは SSID 間を高速で移動できます。高速 SSID が有効になっている場合、クライアントエントリがクリアされず、遅延は適用されません。シスコワイヤレスコントローラでの高速 SSID の構成に関する詳細については、『[Cisco Wireless Controller Configuration Guide](#)』を参照してください。

### ワイヤレスコントローラの構成例

```
WLC (config)# FAST SSID change
```

一部の Apple iOS ベースのデバイスでは、ワイヤレスネットワークに接続しようとする時、次のエラーメッセージが表示される場合があります。

```
Could not scan for Wireless Networks.
```

デバイス認証に影響しないため、このエラーメッセージは無視できます。

# MDM 相互運用性のためのワイヤレス LAN コントローラでの ACL の設定

未登録のデバイスおよび証明書プロビジョニングをリダイレクトするために認証ポリシーで使用する ACL をワイヤレスコントローラで設定します。ACL は次の順序にする必要があります。

- 
- ステップ 1 サーバーからクライアントへのすべての発信トラフィックを許可します。
  - ステップ 2 (任意) トラブルシューティングのためにクライアントからサーバーへの ICMP 着信トラフィックを許可します。
  - ステップ 3 未登録および非準拠のデバイスが MDM エージェントをダウンロードし、コンプライアンスチェックに進むように MDM サーバーへのアクセスを許可します。
  - ステップ 4 Web ポータルおよびサブリカント用 Cisco ISE、および証明書プロビジョニングフローに対するクライアントからサーバーへのすべての着信トラフィックを許可します。
  - ステップ 5 名前解決のためにクライアントからサーバーへの着信ドメインネームシステム (DNS) トラフィックを許可します。
  - ステップ 6 IP アドレスのためにクライアントからサーバーへの着信 DHCP トラフィックを許可します。
  - ステップ 7 Cisco ISE へのリダイレクションのための、クライアントからサーバーへの企業リソースに対するすべての着信トラフィックを (会社のポリシーに応じて) 拒否します。
  - ステップ 8 (任意) 残りのトラフィックを許可します。
- 

## 例

次の例では、未登録のデバイスを BYOD フローにリダイレクトするための ACL を示しています。この例では、Cisco ISE IP アドレスは 10.35.50.165 で、企業のネットワークの IP アドレスは 192.168.0.0 および 172.16.0.0 (リダイレクト用) で、MDM サーバーサブネットは 204.8.168.0 です。

図 1: 登録されていないデバイスをリダイレクトするための ACL

**General**

Access List Name: NSP-ACL

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720	<input checked="" type="checkbox"/>
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227	<input checked="" type="checkbox"/>
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626	<input checked="" type="checkbox"/>
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505	<input checked="" type="checkbox"/>
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864	<input checked="" type="checkbox"/>
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0	<input checked="" type="checkbox"/>
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0	<input checked="" type="checkbox"/>
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4	<input checked="" type="checkbox"/>
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457	<input checked="" type="checkbox"/>
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256	<input checked="" type="checkbox"/>
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310	<input checked="" type="checkbox"/>
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0	<input checked="" type="checkbox"/>
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819	<input checked="" type="checkbox"/>

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。