ISG ポートバンドル ホスト キーの設定

Intelligent Services Gateway（ISG）は、エッジ デバイスが柔軟で拡張性の高いサービスを加入者に提供できる、構造化フレームワークを提供する Cisco IOS ソフトウェアの機能セットです。このモジュールでは、加入者からの TCP パケットを、ISG ゲートウェイのローカル IP アドレスおよび一定範囲のポートにマッピングする、ISG Port-Bundle Host Key 機能の設定方法について説明します。このマッピングにより、外部ポータルで、セッションが開始された ISG ゲートウェイを識別できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「ISG Port-Bundle Host Key の機能情報」（P.139）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

目次

ISG Port-Bundle Host Key 機能の前提条件

リリースおよびプラットフォームの要件の詳細については、「ISG Port-Bundle Host Key の機能情報」（P.139）を参照してください。

外部のポータルは、ポートバンドル ホスト キーをサポートし、同じポートバンドル ホスト キー パラメータが設定されている必要があります。

ISG Port-Bundle Host Key 機能の制約事項

- ISG Port-Bundle Host Key は、ポータル、および接続されているすべての ISG で個別にイネーブルにしておく必要があります。
- **source** コマンドで設定されたすべての ISG 発信元 IP アドレスは、ポータルが存在する管理ネットワーク内でルーティング可能になっている必要があります。
- 各ポータル サーバでは、接続されているすべての ISG のポートバンドル長を同じにする必要があります。
- ISG Port-Bundle Host Key 機能では TCP が使用されます。パケットは、TCP トラフィックを送信していない加入者に対してはマップされません。
- ユーザ プロファイルで Port-Bundle Host Key 機能を指定した場合は、そのユーザ プロファイルが IP パケットの到着前に有効になっていたときだけ機能します。たとえば、PPP セッションや、透過的な自動ログイン機能を備えた Dynamic Host Configuration Protocol（DHCP）で開始される IP セッションなどです。
- Cisco 7600 ルータでは、Port-Bundle Host Key 機能をセッションに適用できますが、フロー レベルでは適用できません。
- Cisco 7600 ルータでは、レイヤ 4 リダイレクトと Port-Bundle Host Key を、最大 150 の並列セッションで同時にイネーブルにできます。

ISG Port-Bundle Host Key に関する情報

ISG Port-Bundle Host Key の概要

ISG Port-Bundle Host Key 機能は、外部ポータルにおいて、セッションを識別するためのインバンド シグナリング メカニズムとして機能します。加入者からの TCP パケットは、ISG ゲートウェイのローカル IP アドレスと一定範囲のポートにマッピングされます。このマッピングにより、ポータルはセッションが開始された ISG ゲートウェイを識別できるようになります。また、このマッピングにより、加入者が重複する IP アドレスを持っている場合でも、セッションを一意に識別できます。ISG Port-Bundle Host Key 機能では、重複する IP アドレスを持つ加入者がいる場合でも、複数の Virtual Routing and Forwarding（VRF）に対して 1 つのポータルを展開できます。

Port-Bundle Host Key のメカニズム

ISG Port-Bundle Host Key 機能を使用して、ISG は、加入者とポータルの間の TCP トラフィックにおいて、Port-Address Translation（PAT; ポート アドレス変換）および Network Address Translation（NAT; ネットワーク アドレス変換）を実行します。加入者の TCP 接続が設定されていると、ISG はポート マッピングを作成します。このマッピングでは、発信元 IP アドレスを設定済みの ISG IP アドレスに変更し、発信元 TCP ポートを ISG から割り当てられたポートに変更します。Web ページにアクセスしている場合は、1 人の加入者が同時に複数の TCP セッションを持つことができるため、ISG はポートのバンドルを各加入者に割り当てます。割り当てられたポートバンドル ホスト キー、またはポート バンドルと ISG 発信元 IP アドレスの組み合わせにより、各加入者は一意に識別されます。ホスト キーは、ポータル サーバと ISG 間で送信される RADIUS パケット内の、Subscriber IP の Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）で伝達されます。表 10 に、Subscriber IP VSA を示します。ポータル サーバが加入者に応答を送信すると、ISG は変換テーブルを使用して、宛先 IP アドレスおよび宛先 TCP ポートを識別します。

表 10　Subscriber IP VSA の説明

アトリビュート（ID）	ベンダー ID	サブアトリビュート ID とタイプ	アトリビュート名	アトリビュート データ
26	9	250 Account-Info	Subscriber IP	S *subscriber-ip-address* [:*port-bundle-number*] • S：加入者 IP の Account-Info コード。 • *subscriber-ip-address* [:*port-bundle-number*]：port-bundle number は、ISG Port-Bundle Host Key 機能が設定されている場合のみ使用されます。

加入者とポータルの間の各 TCP セッションでは、ISG は、ポート バンドルの 1 つのポートをポート マップとして使用します。個々のポート マッピングは、非アクティブ タイマーに基づいて、再使用が可能であるというフラグを設定されますが、いったん割り当てられると明示的には削除されません。ポート バンドルの数は、ISG アドレスごとに制限されていますが、ポート バンドルの使用に対して設定できる ISG IP アドレスの数には制限がありません。

ポートバンドル長

ポートバンドル長は、1 つのバンドル内のポート数を決定するために使用されます。デフォルトでは、ポートバンドル長は 4 ビットです。ポートバンドルの最大長は 10 ビットです。使用できるポートバンドル長の値、およびそれに対応するバンドルごとのポート、およびグループごとのバンドルの値については、表 11 を参照してください。ポート バンドルでポートを使い切ってしまったことを示すエラー メッセージが頻繁に発生する場合は、ポートバンドル長を増やすことがあります。

表 11　ポートバンドル長と、対応するバンドルごとのポート数およびグループごとのバンドル数の値

ポートバンドル長（ビット）	バンドルごとのポート数	グループごと（および ISG 発信元 IP アドレスごと）のバンドル数
0	1	64512
1	2	32256
2	4	16128
3	8	8064
4（デフォルト）	16	4032

表 11　ポートバンドル長と、対応するバンドルごとのポート数およびグループごとのバンドル数の値 （続き）

ポートバンドル長（ビット）	バンドルごとのポート数	グループごと（および ISG 発信元 IP アドレスごと）のバンドル数
5	32	2016
6	64	1008
7	128	504
8	256	252
9	512	126
10	1024	63

（注）　ポータル サーバごとに、接続されているすべての ISG のポートバンドル長を同じにする必要があります。これは、ポータル サーバの BUNDLE_LENGTH 引数で指定されている設定済みの値に対応しています。ある ISG でポートバンドル長を変える場合は、ポータル上の設定において、必ず対応する値を変更してください。

ISG Port-Bundle Host Key の利点

外部ポータル使用のために拡張された加入者の重複 IP アドレスのサポート

ISG の Port-Bundle Host Key 機能を使用すると、加入者の IP アドレスまたは VRF メンバシップに関係なく、外部ポータルのアクセスが可能になります。ポートバンドル ホスト キーを使用しない場合、単一の外部ポータルにアクセスするすべての加入者は、一意の IP アドレスを持つ必要があります。また、ポートバンドル ホスト キーでは、ポータルが存在するドメインから VRF 特有のアドレスが分離されるため、ルーティング上の注意点が単純化されます。

加入者および ISG IP アドレスに対するポータル プロビジョニングが不要

ISG Port-Bundle Host Key 機能を使用しない場合に、ポータルで ISG に RADIUS パケットを送信したり、加入者に HTTP パケットを送信するには、事前に加入者および ISG IP アドレスに対してポータルをプロビジョニングしておく必要があります。ISG Port-Bundle Host Key 機能により、1 つのポータル サーバが複数の ISG に対応できるようにしたり、1 つの ISG が複数のポータル サーバに対応できるようにするためのポータルのプロビジョニングが不要になります。

ISG Port-Bundle Host Key の設定方法

サービス ポリシー マップでの ISG Port-Bundle Host Key 機能のイネーブル化

サービス ポリシー マップで ISG Port-Bundle Host Key 機能をイネーブルにするには、この作業を実行します。ISG Port-Bundle Host Key 機能は、このサービス ポリシー マップを使用しているすべての加入者に適用されます。

（注） この機能に対して 1 つの専用サービス ポリシーを使用することを推奨します。他の ISG 機能とポリシーを共有しないでください。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-name*
4. **ip portbundle**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type service** *policy-name* **例：** `Router(config)# policy-map type service service1`	ISG サービスの定義に使用する、サービス ポリシー マップを作成または定義します。
ステップ 4	**ip portbundle** **例：** `Router(config-service-policymap)# ip portbundle`	サービスに対して、ISG Port-Bundle Host Key 機能をイネーブルにします。
ステップ 5	**end** **例：** `Router(config-service-policymap)# end`	（任意）特権 EXEC モードに戻ります。

次の作業

サービス ポリシー マップまたはサービス プロファイルのアクティブ化の方法を設定できます。たとえば、サービスのアクティブ化に制御ポリシーを使用できます。サービスのアクティブ化方法の詳細については、「Configuring ISG Subscriber Services」モジュールを参照してください。

AAA サーバのユーザ プロファイルまたはサービス プロファイルでの Port-Bundle Host Key 機能のイネーブル化

Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバのユーザ プロファイルまたはサービス プロファイルで ISG Port-Bundle Host Key 機能をイネーブルにするには、この作業を実行します。

手順の概要

1. ユーザ プロファイルまたはサービス プロファイルに Port-Bundle Host Key アトリビュートを追加します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	ユーザ プロファイルまたはサービス プロファイルに Port-Bundle Host Key アトリビュートを追加します。 26,9,1 = "ip:portbundle=enable"	ユーザ プロファイルまたはサービス プロファイで ISG Port-Bundle Host Key アトリビュートをイネーブルにします。

次の作業

サービス プロファイルで ISG Port-Bundle Host Key 機能をイネーブルにした場合、制御ポリシーを使用してサービスをアクティブにするなど、サービス プロファイルをアクティブにする方法を設定することがあります。サービスのアクティブ化方法の詳細については、「Configuring ISG Subscriber Services」モジュールを参照してください。

Port-Bundle Host Key パラメータの設定

ISG Port-Bundle Host Key パラメータを設定し、ISG が、ダウンストリーム トラフィックに対する IP アドレスおよびポート番号を検出するために変換表を使用するインターフェイスを指定するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip portbundle**
4. **match access-list** *access-list-number*
5. **length** *bits*

6. **source** *interface-type interface-number*
7. **exit**
8. **interface** *type number*
9. **ip portbundle outside**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip portbundle** 例： `Router(config)# ip portbundle`	IP ポートバンドル コンフィギュレーション モードを開始します。
ステップ 4	**match access-list** *access-list-number* 例： `Router(config-portbundle)# match access-list 101`	加入者のトラフィックと比較するためのアクセス リストを指定して、ポート マッピング用のパケットを指定します。
ステップ 5	**length** *bits* 例： `Router(config-portbundle)# length 5`	ISG ポートバンドル長を指定します。この長さは、バンドルあたりのポート数、およびグループあたりのバンドル数を決定します。 • デフォルトのビット数は 4 です。 • 詳細については、「ポートバンドル長」を参照してください。
ステップ 6	**source** *interface-type interface-number* 例： `Router(config-portbundle)# source loopback 0`	メイン IP アドレスが、ISG によって加入者トラフィックの宛先 IP アドレスへマップされるインターフェイスを指定します。 • 発信元インターフェイスとしてループバック インターフェイスを使用することを推奨します。
ステップ 7	**exit** 例： `Router(config-portbundle)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface** *type number* 例： `Router(config)# interface ethernet 0/0`	設定用のインターフェイスを指定します。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。
ステップ 9	**ip portbundle outside** 例： `Router(config-if)# ip portbundle outside`	設定中のインターフェイスについて、ポータルから加入者へ向かっているトラフィックの場合は、宛先 IP アドレスと TCP ポートを、実際の加入者 IP アドレスと TCP ポートに逆変換するよう ISG を設定します。

ISG Port-Bundle Host Key の設定の確認

ISG Port-Bundle Host Key の設定に関する情報を表示するには、この作業を実行します。

手順の概要

1. **enable**
2. **show ip portbundle status** [**free** | **inuse**]
3. **show ip portbundle ip** *portbundle-ip-address* **bundle** *port-bundle-number*
4. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id* | **username** *name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show ip portbundle status** [**free** | **inuse**] 例： `Router# show ip portbundle status free`	ISG ポートバンドル グループの情報を表示します。
ステップ 3	**show ip portbundle ip** *portbundle-ip-address* **bundle** *port-bundle-number* 例： `Router# show ip portbundle ip 10.10.10.10 bundle 65`	特定の ISG ポート バンドルの情報を表示します。
ステップ 4	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id* | **username** *name*] 例： `Router# show subscriber session detailed`	ISG 加入者のセッション情報を表示します。

ISG Port-Bundle Host Key の設定例

ISG Port-Bundle Host Key の設定：例

次に、すべてのセッションに適用するために、ISG Port-Bundle Host Key 機能を設定する方法の例を示します。

```
policy-map type service ISGPBHKService
 ip portbundle
!
policy-map type control PBHKRule
 class type control always event session-start
  1 service-policy type service ISGPBHKService
!
service-policy type control PBHKRule

interface ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip portbundle outside
!
ip portbundle
 match access-list 101
 length 5
 source loopback 0
```

その他の参考資料

関連資料

内容	参照先
ISG コマンド	『*Cisco IOS Intelligent Services Gateway Command Reference*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ISG Port-Bundle Host Key の機能情報

表 12 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

プラットフォームおよびソフトウェア イメージのサポート情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どの Cisco IOS および Catalyst OS ソフトウェア イメージが特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 12 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連のソフトウェア リリースの以降のリリースでもサポートされます。

表 12　ISG Port-Bundle Host Key の機能情報

機能名	リリース	機能情報
ISG：セッション：Auth：PBHK	12.2(28)SB 12.2(33)SRC 15.0(1)S	ISG Port-Bundle Host Key 機能は、外部ポータルにおいて、セッションを識別するためのインバンド シグナリング メカニズムとして機能します。加入者からの TCP パケットは、ISG ゲートウェイのローカル IP アドレスと一定範囲のポートにマッピングされます。このマッピングにより、ポータルはセッションが開始された ISG ゲートウェイを識別できるようになります。 このモジュールでは、ISG Port-Bundle Host Key 機能の設定方法について説明します。 Cisco IOS Release 12.2(33)SRC では、サポートには Cisco 7600 ルータのサポートが追加されました。