CHAPTER 15

SBC ファイアウォール トラバーサルおよび NAT の実装

Session Border Controller（SBC; セッション ボーダ コントローラ）では、Voice over IP（VoIP）シグナリングとメディアを、隣接ネットワークの境界にあるファイアウォールと Network Address Translation（NAT; ネットワーク アドレス変換）の背後のデバイスから受信したり、デバイスに誘導したりできます。デバイスまたはファイアウォールをアップグレードする必要はありません。つまり、SBC は、コール シグナリング ヘッダー内の IP アドレスとポート、およびこれらのメッセージに添付された Session Description Protocol（SDP）ブロックを書き換えることにより、この処理を行います。SBC は、ピンホールをオープン状態に保つオプションをサポートしていません。その代わりに、SBC は、シグナリング ピンホール メンテナンスのメッセージとメディアの Real-Time Protocol（RTP）パケットを登録します。

SBC は、対称応答ルーティングのための Session Initiation Protocol（SIP）拡張子（RFC 3581）をサポートしています （現在、H.323 はサポートしていません）。

（注） ACE SBC Release 3.0.0 以降では、この機能は統合モデルと分散モデルの両方でサポートされます。

この章で使用されているコマンドの詳細については、第 39 章「Cisco セッション ボーダ コントローラ コマンド」を参照してください。この章に記載されたその他のコマンドのマニュアルを特定するには、コマンド リファレンスのマスター インデックスを使用するか、またはオンラインで検索してください。

SBC ファイアウォール トラバーサルおよび NAT の実装機能の履歴

リリース	変更内容
ACE SBC Release 3.1.00	SIP PING メッセージのサポートが追加されました。
ACE SBC Release 3.0.00	この機能は、SBC 統合モデルのサポートとともに Cisco 7600 シリーズ ルータに追加されました。

この章の構成

この章で説明する内容は、次のとおりです。

ファイアウォール トラバーサルおよび NAT の実装の前提条件

次に、SBC ファイアウォール トラバーサルおよび NAT を実装するための前提条件を示します。

- Application Control Engine（ACE）モジュールで SBC コマンドを入力するには、Admin ユーザである必要があります。詳細については、次の URL にある『*Application Control Engine Module Administration Guide*』を参照してください。
  http://www.cisco.com/en/US/products/hw/modules/ps2706/products_configuration_guide_book09186a00806838f4.html
- ファイアウォール トラバーサルおよび NAT を実装する前に、SBC を作成しておく必要があります。第 2 章「SBC の ACE を設定するための前提条件」に記載された手順に従ってください。
- ファイアウォール トラバーサルおよび NAT を実装する前に、隣接を設定する必要があります。「SBC 隣接の実装」に記載された手順に従ってください。

ファイアウォール トラバーサルおよび NAT に関する情報

SBC では、VoIP シグナリングとメディアを、隣接ネットワークの境界にあるファイアウォールと NAT の背後のデバイスから受信したり、デバイスに誘導したりできます。デバイスまたはファイアウォールをアップグレードする必要はありません。つまり、SBC は、コール シグナリング ヘッダー内の IP アドレスとポート、およびこれらのメッセージに添付された SDP ブロックを書き換えることにより、この処理を行います。

ファイアウォールは、基本的なパケット フィルタリングを行うことにより、不要なトラフィックがネットワークを出入りするのを防ぎます。パケットのヘッダーを完全に検査することによりパケットのフィルタリングを行い、パケットのペイロードの解析や認識は行いません。したがって、すべてのタイプの不要なトラフィックをフィルタリングするわけではありません。たとえば、ファイアウォールは Call Admission Control（CAC; コール アドミッション制御）を行いません（SBC アプリケーションが行う）。

しかし、ファイアウォールは、広範なカテゴリの不要なトラフィックを効率的にフィルタリングし、SBC などのアプリケーション認識デバイスに処理をほとんど任せないため、有益です。外部ファイアウォールは、外部ネットワークからのパケットをフィルタリングしますが、内部ネットワークからのすべてのパケットがフィルタリングされずにパススルーします。内部ファイアウォールは、内部ネットワークからのパケットをフィルタリングしますが、外部ネットワークからのすべてのパケットがフィルタリングされずにパススルーします（すでに外部ファイアウォールをパススルーしているため）。

ファイアウォールは、デフォルトではネットワークからのパケットを受け入れませんが、特定のパケットを選択して受け入れるようにする規則が設定されます。したがって、パケットは、デフォルトのコンフィギュレーションではなく、*明示的なコンフィギュレーション*に基づいてネットワークへの出入りを許可されます。

SBC アプリケーションには、NAT 機能も組み込まれています。NAT はネットワークを異なるアドレス レンジに分離します。SBC の NAT コンポーネントは、内部ネットワークのアドレス レンジを外部ネットワークのアドレス レンジから分離します。NAT は {external address, port} から {internal address, port} へのマッピングおよびその逆のマッピングのテーブルを維持します。このテーブルはデュアル インデックス テーブルであるため、特定のマッピングは、内部または外部のアドレス指定情報により検索できます。NAT はこのテーブルを使用して、転送する IP パケットのヘッダーを書き換えます。

NAT は、外部ネットワークから IP パケットを受信すると、テーブル内でパケットの宛先アドレスとポート（外部アドレス レンジからのアドレスになる）を検索します。マッピングが検出された場合、IP パケットの宛先アドレス ヘッダーは、テーブルからの対応する内部アドレスおよびポートを含むように変更され、パケットは内部ネットワークに転送されます。マッピングが検出されない場合、パケットは破棄されます。

NAT は、内部ネットワークから IP パケットを受信すると、テーブル内でパケットの送信元アドレスとポート（内部アドレス レンジからのアドレスになる）を検索します。マッピングが検出された場合、IP パケットの送信元アドレス ヘッダーは、テーブルからの対応する外部アドレスおよびポートを含むように変更され、パケットは外部ネットワークに転送されます。マッピングが検出されない場合、新しいマッピングが作成されます。NAT は、外部アドレス レンジからの新しい外部アドレスおよびポートを、パケット（およびこの送信元アドレスおよびポート タプルからのすべての将来のパケット）にダイナミックに割り当てます。

SBC は、ピンホールをオープン状態に保つオプションをサポートしていません。その代わりに、SBC は、シグナリング ピンホール メンテナンスのメッセージとメディアの RTP パケットを登録します。この問題を解決するには、カスタマーの NAT がピンホールをオープンし、IP Phone がシグナリング パケットおよびメディア パケットをパブリック ネットワークに送信できるようにし、カスタマーのファイアウォールがこれらのパケットを通過させる必要があります。

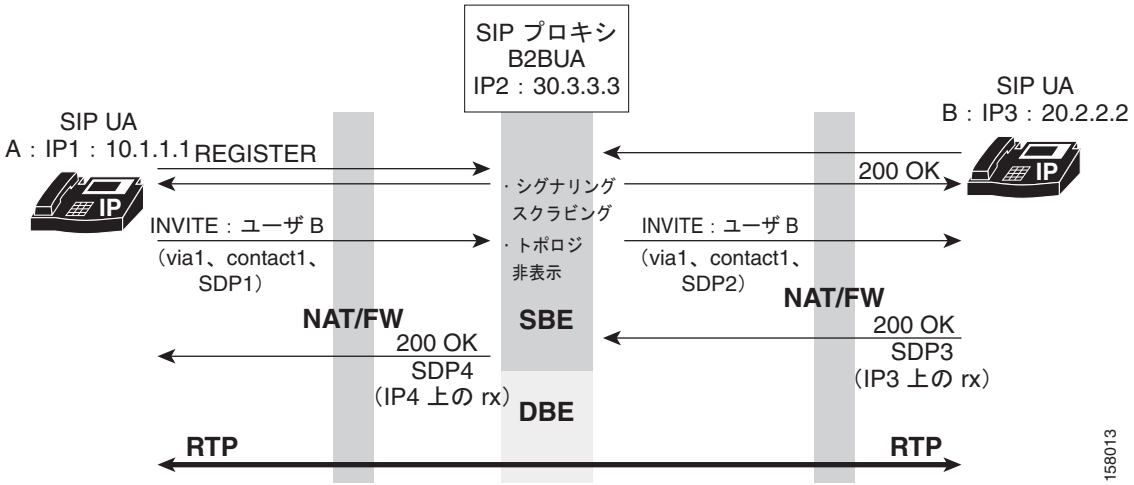
したがって、パブリック ネットワークからの着信シグナリングおよびメディアは、カスタマーの NAT のパブリック ネットワーク側にあるピンホールのアドレスとポートに誘導することにより、カスタマーのファイアウォールと NAT をトラバースできます。シグナリングとメディアでは、ピンホールのライフタイムが異なります。

- シグナリング ピンホールは、いったん作成されると、すべてのコール シグナリングで再利用されます。
- メディア ストリームの送信元および宛先ポートはコール単位でダイナミックに割り当てられるため、メディア ピンホールは各メディア ストリームに対して新しく作成されます。

シグナリング ピンホールは、IP Phone が最初にオンラインになったときに完全に作成され、IP Phone が再びオフラインになるまでオープン状態のままです。メディア ピンホールは、SIP invite が SBC に到達したときに作成されます。

図 15-1 に、SBC によるファイアウォール トラバーサルと NAT のサポートのためのデータ パスを示します。

図 15-1　ファイアウォール トラバーサルおよび NAT



ファイアウォール トラバーサルおよび NAT の実装

次に示すタスクは、ファイアウォール トラバーサルおよび NAT を実装します。

手順概要

（注）　隣接がすでに接続されている場合は、**nat-enable** の前に **no attach** コマンドを発行する必要があります。

1. **configure**
2. **sbc** *service-name*
3. **sbe**
4. **adjacency sip** *adjacency-name*
5. **nat force-on**
6. **signaling-address ipv4** *ipv4_IP_address*
7. **signaling-port** *port_num*
8. **remote-address ipv4** *ipv4_IP_address/prefix*
9. **signaling-peer** [**gk**] *peer_name*
10. **signaling-peer-port** *port_num*
11. **attach**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `host1/Admin# configure`	グローバル コンフィギュレーション モードをイネーブルにします。
ステップ 2	**sbc** *service-name* **例：** `host1/Admin(config)# sbc mysbc`	SBC サービス モードを開始します。 サービス名を定義するには、*service-name* 引数を使用します。
ステップ 3	**sbe** **例：** `host1/Admin(config-sbc)# sbe`	SBC サービス内で SBE エンティティ モードを開始します。
ステップ 4	**adjacency sip** *adjacency-name* **例：** `host1/Admin(config-sbc-sbe)# adjacency sip SIP_7301_1`	SBE SIP 隣接モードを開始します。 • サービス名を定義するには、*adjacency-name* 引数を使用します。

	コマンドまたはアクション	目的
ステップ 5	**nat force-on** **例：** `host1/Admin(config-sbc-sbe-adj-sip)# nat force-on`	すべてのエンドポイントが NAT デバイスの背後にあると見なすように SIP 隣接を設定します。
ステップ 6	**signaling-address ipv4** *ipv4_IP_address* **例：** `host1/Admin(config-sbc-sbe-adj-sip)# signaling-address ipv4 10.1.0.2`	SIP 隣接のローカル IPv4 シグナリング アドレスを指定します。
ステップ 7	**signaling-port** *port_num* **例：** `host1/Admin(config-sbc-sbe-adj-sip)# signaling-port 5000`	SIP 隣接のローカル シグナリング ポートを指定します。
ステップ 8	**remote-address ipv4** *ipv4_IP_address/prefix* **例：** `host1/Admin(config-sbc-sbe--adj-sip)# remote-address ipv4 1.2.3.0/24`	隣接経由で通信するリモート シグナリング ピアのセットを、指定の IP アドレス プレフィクスを持つピアに制限します。
ステップ 9	**signaling-peer** [**gk**] *peer_name* **例：** `host1/Admin(config-sbc-sbe-adj-sip)# signaling-peer athene`	SIP 隣接が使用するリモート シグナリング ピアを指定します。
ステップ 10	**signaling-peer-port** *port_num* **例：** `host1/Admin(config-sbc-sbe--adj-sip)# signaling-peer-port 123`	隣接が使用するリモート シグナリング ピア ポートを指定します。
ステップ 11	**attach** **例：** `host1/Admin(config-sbc-sbe-adj-sip)# attach`	隣接を接続します。

NAT ステータスの変更

NAT ステータスを変更しても、その変更はすぐには有効になりません。このタスクに示すように、隣接を切断してから接続し直す必要があります。

手順概要

1. **configure**
2. **sbc** *service-name*
3. **sbe**
4. **adjacency sip** *adjacency-name*
5. **no attach**

6. **nat force-off**
7. **attach**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `host1/Admin# configure`	グローバル コンフィギュレーション モードをイネーブルにします。
ステップ 2	**sbc** *service-name* **例：** `host1/Admin(config)# sbc mysbc`	SBC サービス モードを開始します。 サービス名を定義するには、*service-name* 引数を使用します。
ステップ 3	**sbe** **例：** `host1/Admin(config-sbc)# sbe`	SBC サービス内で SBE エンティティ モードを開始します。
ステップ 4	**adjacency sip** *adjacency-name* **例：** `host1/Admin(config-sbc-sbe)# adjacency sip SIP_7301_1`	SBE SIP 隣接モードを開始します。 • サービス名を定義するには、*adjacency-name* 引数を使用します。
ステップ 5	**no attach** **例：** `host1/Admin(config-sbc-sbe-adj-sip)# no attach`	SBE 上のアカウントから隣接を切断します。
ステップ 6	**nat force-off** **例：** `host1/Admin(config-sbc-sbe-adj-sip)# nat force-on`	エンドポイントは NAT デバイスの背後にはないと見なすように SIP 隣接を設定します。
ステップ 7	**attach** **例：** `host1/Admin(config-sbc-sbe-adj-sip)# attach`	隣接を接続します。

SIP PING メッセージのサポート

Release 3.1.0 では、Midcom 非対応 NAT/ファイアウォール トラバーサルに関する IETF ドラフトで定義された SIP PING メッセージのサポートが追加されました。

sip ping-support コマンドで SIP PING メッセージのサポートをイネーブルにすると、SBC は 2 つのヘッダー（Via ヘッダーと Contact ヘッダー）を含む 200 OK 応答を返します。これらのヘッダーは、送信側の NAT コンフィギュレーションを検出するために使用されます。

どちらのヘッダーにも、PING メッセージを受信した IP アドレスとポートの情報が含まれています。次に、PING メッセージとそれに対応する 200 OK 応答の例を示します。

```
PING sip:7075160418@lgdacom.net SIP/2.0
From: <sip:7075160418@lgdacom.net>;tag=db2000-647ba8c0-13c4-386d43b7-42d6ea8a-386d43b7
To: <sip:7075160418@lgdacom.net>
Call-ID: db2000-647ba8c0-13c4-386d43b7-6769ff65-386d43b7@lgdacom.net
CSeq: 1 PING
Via: SIP/2.0/UDP 192.168.123.100:5060;branch=z9hG4bK-386d43b7-6ad08603-2972814
Max-Forwards: 70
Supported: replaces, 100rel
Proxy-Require: com.nortelnetworks.firewall
Contact: <sip:7075160418@192.168.123.100>
Content-Length: 0

SIP/2.0 200 OK
Via: SIP/2.0/UDP
192.168.123.100:5060;branch=z9hG4bK-386d43b7-6ad08603-2972814;received=10.0.200.111;rport=
5060
From: <sip:7075160418@lgdacom.net>;tag=db2000-647ba8c0-13c4-386d43b7-42d6ea8a-386d43b7
To: <sip:7075160418@lgdacom.net>;tag=sbc-zfgjyuts-4935681
Call-ID: db2000-647ba8c0-13c4-386d43b7-6769ff65-386d43b7@lgdacom.net
CSeq: 1 PING
Contact: <sip:pong@10.0.200.111:5060;transport=UDP>
Content-Length: 0
```

PING メッセージのサポートの設定

NAT ステータスを変更すると、その変更が即座に有効になります。次に示すように、PING メッセージのサポートを設定します。

手順概要

1. **configure**
2. **sbc** *service-name*
3. **sbe**
4. **sip ping-support**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** host1/Admin# configure	グローバル コンフィギュレーション モードをイネーブルにします。
ステップ 2	**sbc** *service-name* **例：** host1/Admin(config)# sbc mysbc	SBC サービス モードを開始します。 サービス名を定義するには、*service-name* 引数を使用します。
ステップ 3	**sbe** **例：** host1/Admin(config-sbc)# sbe	SBC サービス内で SBE エンティティ モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**sip ping-support** **例：** host1/Admin(config-sbc-sbe)# sip ping-support	SIP ping サポートを設定します。

設定例

次に、ファイアウォール トラバーサルおよび NAT を実装する例を示します。

```
host1/Admin# configure
host1/Admin(config)# sbc mySbc
host1/Admin(config-sbc)# sbe
Router/Admin(config-sbc-sbe)# adjacency sip SIP_7301_1
Router/Admin(config-sbc-sbe-adj-sip)# nat force-on
Router/Admin(config-sbc-sbe-adj-sip)# signaling-address ipv4 88.88.121.102
Router/Admin(config-sbc-sbe-adj-sip)# signaling-port 5060
Router/Admin(config-sbc-sbe-adj-sip)# remote-address ipv4 10.10.111.0/24
Router/Admin(config-sbc-sbe-adj-sip)# signaling-peer 10.10.111.41
Router/Admin(config-sbc-sbe-adj-sip)# signaling-peer-port 5060
Router/Admin(config-sbc-sbe-adj-sip)# attach
```

次に、NAT ステータスを変更する例を示します。

```
host1/Admin# configure
host1/Admin(config)# sbc mySbc
host1/Admin(config-sbc)# sbe
Router/Admin(config-sbc-sbe)# adjacency sip SIP_7301_1
Router/Admin(config-sbc-sbe-adj-sip)# no attach
Router/Admin(config-sbc-sbe-adj-sip)# nat force-off
Router/Admin(config-sbc-sbe-adj-sip)# attach
```

次に、SIP ping サポートを設定する例を示します。

```
host1/Admin# config
host1/Admin(config)# sbc mySbc
host1/Admin(config-sbc)# sbe
host1/Admin(config-sbc-sbe)# sip ping-support
```