CHAPTER 14

Attack Response Controller でのブロッキングおよびレート制限の設定

（注） 現在、Cisco IPS 7.1 をサポートしているプラットフォームは、IPS SSP を搭載した Cisco ASA 5585-X のみです。それ以外の Cisco IPS センサーは、IPS 7.1 を現在サポートしていません。

（注） IPS SSP を搭載した Cisco ASA 5585-X は、ASA 8.2(4.4) 以降および ASA 8.4(2) 以降でサポートされています。ASA 8.3(*x*) ではサポートされていません。

（注） ARC は、以前は Network Access Controller と呼ばれていました。名前は変更されましたが、IDM、IME、および CLI には Network Access Controller、**nac**、および **network-access** などの記述が含まれています。

この章では、センサーでブロッキングおよびレート制限を実行するための ARC の設定について説明します。次のような構成になっています。

ブロッキングについて

（注）　ARC は、以前は Network Access Controller と呼ばれていました。名前は変更されましたが、IDM、IME、および CLI には Network Access Controller、**nac**、および **network-access** などの記述が含まれています。

ARC は、攻撃側のホストおよびネットワークからのアクセスをブロックすることで、疑わしいイベントに対応し、ネットワーク デバイスを管理します。ARC は、管理しているデバイスの IP アドレスをブロックします。他のマスター ブロッキング センサーを含め、管理しているすべてのデバイスに同じブロックを送信します。ARC は、ブロックの時間をモニタし、時間の経過後にブロックを削除します。

ARC は、新しいブロックでのアクション応答を 7 秒以内に完了します。ほとんどの場合は、より短い時間でアクション応答を完了します。このパフォーマンス目標を達成するために、センサーでのブロックの実行レートが高すぎたり、管理するブロッキング デバイスおよびインターフェイスが多すぎたりしないように設定してください。最大ブロック数は 250 以下にし、最大ブロッキング項目数は 10 以下にすることを推奨します。ブロッキング項目の最大数を計算するために、セキュリティ アプライアンスはブロッキング コンテキストあたり 1 つのブロッキング項目としてカウントします。ルータは、ブロッキング インターフェイス / 方向あたり 1 つのブロッキング項目としてカウントします。Catalyst ソフトウェアを実行しているスイッチは、ブロッキング VLAN あたり 1 つのブロッキング項目としてカウントします。推奨される制限を超えると、ARC がブロックをタイミングよく適用しなかったり、ブロックをまったく適用できなかったりする場合があります。

注意　マルチモード管理コンテキストの FWSM では、ブロッキングはサポートされません。

セキュリティ アプライアンスがマルチモードで設定されている場合、Cisco IPS はブロック要求に VLAN 情報を挿入しません。したがって、ブロックされる IP アドレスが各セキュリティ アプライアンスに対して正しいことを確認する必要があります。たとえば、センサーは、VLAN A に対して設定されているセキュリティ アプライアンス カスタマー コンテキストでパケットをモニタし、VLAN B に対して設定されている別のセキュリティ アプライアンス カスタマー コンテキストでブロッキングしている場合があります。VLAN A でブロックをトリガーするアドレスは、VLAN B 上の別のホストを指している可能性があります。

ブロックには次の 3 種類があります。

- ホスト ブロック：特定の IP アドレスからのすべてのトラフィックをブロックします。
- 接続ブロック：特定の送信元 IP アドレスから特定の宛先 IP アドレスおよび宛先ポートへのトラフィックをブロックします。同じ送信元 IP アドレスから異なる宛先 IP アドレスまたは宛先ポートへの複数の接続ブロックによって、接続ブロックからホスト ブロックにブロックが自動的に切り替えられます。
- ネットワーク ブロック：特定のネットワークからのトラフィックをすべてブロックします。ホスト ブロックと接続ブロックは、手動で開始するか、シグニチャがトリガーされたときに自動的に開始できます。ネットワーク ブロックは手動でだけ開始できます。

（注）　適応型セキュリティ アプライアンスでは、接続ブロックとネットワーク ブロックはサポートされません。適応型セキュリティ アプライアンスでは、接続情報が追加されたホスト ブロックだけがサポートされます。

注意　ブロッキングとセンサーのパケット ドロップ機能を混同しないでください。センサーでは、インライン モードのセンサーに対してパケットのインライン拒否、接続のインライン拒否、および攻撃者のインライン拒否のアクションが設定されている場合にパケットをドロップできます。

自動ブロックの場合は、特定のシグニチャに対するイベント アクションとして [request-block-host] または [request-block-connection] チェック ボックスをオンにし、それらのアクションを設定済みの任意のイベント アクション オーバーライドに追加する必要があります。これによって、そのシグニチャがトリガーされたとき、SensorApp は ARC にブロック要求を送信することができます。SensorApp からブロック要求を受信すると、ARC はホストまたは接続をブロックするようにデバイス コンフィギュレーションを更新します。

Cisco ルータおよび Catalyst 6500 シリーズ スイッチでは、ARC は ACL または VACL を適用してブロックを作成します。ACL および VACL は、インターフェイス方向または VLAN 上のデータ パケットの経路を許可または拒否します。各 ACL または VACL には、IP アドレスに適用される許可条件と拒否条件が含まれます。セキュリティ アプライアンスでは、ACL または VACL は使用されません。組み込みの **shun** および **no shun** コマンドが使用されます。

注意　ARC が作成する ACL を、ユーザまたは他のシステムが変更してはいけません。これらの ACL は一時的なものであり、センサーによって新しい ACL が絶えず作成されています。Pre-Block ACL および Post-Block ACL にのみ変更を加えることができます。

ARC でデバイスを管理するには、次の情報が必要です。

- ログイン ユーザ ID（デバイスに AAA が設定されている場合）。
- ログイン パスワード。
- イネーブル パスワード（イネーブル特権を持つユーザは不要）。
- 管理対象のインターフェイス（ethernet0、vlan100 など）。
- 作成される ACL または VACL の先頭（Pre-Block ACL または VACL）または末尾（Post-Block ACL または VACL）に適用する既存の ACL または VACL 情報。セキュリティ アプライアンスはブロッキングに ACL を使用しないため、この情報はセキュリティ アプライアンスには適用されません。
- デバイスとの通信に Telnet と SSH のどちらを使用しているか。
- ブロックしない IP アドレス（ホストまたはホストの範囲）。
- ブロックの継続時間。

ヒント　ARC のステータスを確認するには、`sensor#` に **show statistics network-access** と入力します。管理下にあるデバイス、アクティブなブロックとレート制限、すべてのデバイスのステータスが出力に表示されます。

（注）　IPv6 トラフィックに対するレート制限およびブロッキングはサポートされていません。シグニチャにブロックまたはレート制限イベント アクションが設定されている場合、IPv6 トラフィックによってそのシグニチャがトリガーされると、アラートは生成されますがアクションは実行されません。

詳細情報

- request-block-host または request-block-connection イベント アクションをシグニチャに追加する手順については、「シグニチャへのアクションの割り当て」（P.7-16）を参照してください。
- 特定のリスク レーティングのアラートに request-block-host または request-block-connection イベント アクションを追加するオーバーライドの設定手順については、「イベント アクション オーバーライドの追加、編集、イネーブル化、およびディセーブル化」（P.8-17）を参照してください。
- Pre-Block ACL および Post-Block ACL の詳細については、「センサーによるデバイスの管理方法」（P.14-22）を参照してください。

レート制限について

ARC は、保護されているネットワーク内のトラフィックに対してレート制限を行います。レート制限により、センサーはネットワーク デバイス上の指定したトラフィック クラスのレートを制限できます。レート制限応答は、Host Flood エンジンと Net Flood エンジン、および TCP ハーフオープン SYN シグニチャに対してサポートされます。ARC では、Cisco IOS 12.3 以降を実行しているネットワーク デバイスにレート制限を設定できます。マスター ブロッキング センサーは、レート制限要求をブロッキング転送センサーに転送することもできます。

レート制限を追加するには以下を指定します。

- レート制限の送信元アドレスまたは宛先アドレス（あるいはその両方）
- TCP または UDP プロトコルを使用するレート制限の送信元ポートまたは宛先ポート（あるいはその両方）

レート制限シグニチャをチューニングすることもできます。また、アクションを request-rate-limit に設定し、これらのシグニチャの比率を設定する必要があります。

（注） IPv6 トラフィックに対するレート制限およびブロッキングはサポートされていません。シグニチャにブロックまたはレート制限イベント アクションが設定されている場合、IPv6 トラフィックによってそのシグニチャがトリガーされると、アラートは生成されますがアクションは実行されません。

表 14-1 に、サポートされるレート制限シグニチャとパラメータを示します。

表 14-1　レート制限シグニチャ

シグニチャ ID	シグニチャ名	プロトコル	許可される宛先 IP アドレス	データ
2152	ICMP Flood Host	ICMP	Yes	echo-request
2153	ICMP Smurf Attack	ICMP	Yes	echo-reply
4002	UDP Flood Host	UDP	Yes	なし
6901	Net Flood ICMP Reply	ICMP	No	echo-reply
6902	Net Flood ICMP Request	ICMP	No	echo-request
6903	Net Flood ICMP Any	ICMP	No	なし
6910	Net Flood UDP	UDP	No	なし
6920	Net Flood TCP	TCP	No	なし
3050	TCP HalfOpenSyn	TCP	No	halfOpenSyn

ヒント　ARC のステータスを確認するには、sensor# に **show statistics network-access** と入力します。管理下にあるデバイス、アクティブなブロックとレート制限、すべてのデバイスのステータスが出力に表示されます。

詳細情報

- ルータにレート制限を設定する手順については、「ブロッキングおよびレート制限デバイスの設定」（P.14-22）を参照してください。
- センサーをマスター ブロッキング センサーとして設定する手順については、「センサーをマスター ブロッキング センサーにする設定」（P.14-29）を参照してください。

レート制限のサービス ポリシーについて

レート制限が設定されているインターフェイス/方向にはサービス ポリシーを適用しないでください。適用した場合は、レート制限アクションが失敗します。レート制限を設定する前に、インターフェイス/方向にサービス ポリシーがないことを確認し、存在する場合には削除します。ARC では、ARC が以前に追加したものでないかぎり、既存のレート制限は削除されません。

レート制限では ACL が使用されますが、ブロックと同じ方法では使用されません。レート制限では、**acls** および **class-map** エントリを使用してトラフィックを識別し、**policy-map** および **service-policy** エントリを使用してトラフィックをポリシングします。

ARC を設定する前に

注意　2 つのセンサーが同じデバイスでブロッキングまたはレート制限を制御することはできません。この状況が必要な場合は、一方のセンサーをデバイス管理用のマスター ブロッキング センサーとして設定すると、もう一方のセンサーからマスター ブロッキング センサーに要求を転送できます。

（注）　マスター ブロッキング センサーを追加する場合は、センサーあたりのブロッキング デバイス数を減らします。たとえば、それぞれ 1 つのブロッキング インターフェイス/方向を持つ 10 個のセキュリティ アプライアンスと 10 台のルータでブロッキングを行う場合、センサーに 10 個を割り当て、マスター ブロッキング センサーに残りの 10 個を割り当てることができます。

ARC でブロッキングまたはレート制限を設定する前に、必ず次の作業を実行してください。

- ネットワーク トポロジを解析し、どのデバイスをどのセンサーによってブロックするか、ブロックしてはならないアドレスはどれかを確認します。
- 各デバイスへのログインに必要なユーザ名、デバイスのパスワード、イネーブル パスワード、および接続タイプ（Telnet または SSH）の情報を収集します。
- デバイスのインターフェイス名を確認します。
- Pre-Block ACL または VACL、および Post-Block ACL または VACL が必要な場合は、その名前を確認します。

- ブロックするインターフェイス、ブロックしないインターフェイス、およびそれらの方向（インまたはアウト）を確認します。誤ってネットワーク全体をシャットダウンすることは避けなければなりません。

詳細情報

マスター ブロッキング センサーの設定手順については、「センサーをマスター ブロッキング センサーにする設定」（P.14-29）を参照してください。

サポートされるデバイス数

注意　推奨される制限を超えると、ARC がブロックをタイミングよく適用しなかったり、ブロックをまったく適用できなかったりする場合があります。

デフォルトでは、ARC は任意の組み合わせで 250 までのデバイスをサポートします。ARC によるブロッキングでは、次のデバイスがサポートされます。

- Cisco IOS 11.2 以降（ACL）を使用する Cisco シリーズ ルータ
  - Cisco 1600 シリーズ ルータ
  - Cisco 1700 シリーズ ルータ
  - Cisco 2500 シリーズ ルータ
  - Cisco 2600 シリーズ ルータ
  - Cisco 2800 シリーズ ルータ
  - Cisco 3600 シリーズ ルータ
  - Cisco 3800 シリーズ ルータ
  - Cisco 7200 シリーズ ルータ
  - Cisco 7500 シリーズ ルータ
- Catalyst 5000 スイッチ、RSM 搭載、IOS 11.2(9)P 以降（ACL）
- Catalyst 6500 スイッチおよび 7600 ルータ、IOS 12.1(13)E 以降（ACL）
- Catalyst 6500 スイッチおよび 7600 ルータ、Catalyst ソフトウェア バージョン 7.5(1) 以降（VACL）
  - Supervisor Engine 1A（PFC 搭載）
  - Supervisor Engine 1A（MSFC1 搭載）
  - Supervisor Engine 1A（MFSC2 搭載）
  - Supervisor Engine 2（MSFC2 搭載）
  - Supervisor Engine 720（MSFC3 搭載）

（注）　Supervisor Engine での VACL ブロッキングと MSFC での ACL ブロッキングがサポートされます。

- PIX Firewall、バージョン 6.0 以降（**shun** コマンド）
  - 501
  - 506E
  - 515E
  - 525
  - 535
- ASA バージョン 7.0 以降（**shun** コマンド）
  - ASA-5510
  - ASA-5520
  - ASA-5540
- FWSM 1.1 以降（**shun** コマンド）

ブロッキングを設定するには、ACL、VACLS、または **shun** コマンドのいずれかを使用します。すべてのファイアウォールおよび ASA モデルで **shun** コマンドがサポートされます。

ARC によるレート制限では、次のデバイスがサポートされます。

- Cisco IOS 12.3 以降を使用する Cisco シリーズ ルータ
  - Cisco 1700 シリーズ ルータ
  - Cisco 2500 シリーズ ルータ
  - Cisco 2600 シリーズ ルータ
  - Cisco 2800 シリーズ ルータ
  - Cisco 3600 シリーズ ルータ
  - Cisco 3800 シリーズ ルータ
  - Cisco 7200 シリーズ ルータ
  - Cisco 7500 シリーズ ルータ

注意　ARC は、VIP を使用する 7500 ルータでのレート制限はできません。ARC はエラーを報告しますが、レート制限は実行できません。

ブロッキング プロパティの設定

デフォルトのブロッキング プロパティは変更可能です。デフォルトのプロパティを使用することを推奨しますが、変更する必要がある場合は、次の手順を使用します。

- 「センサー自体のブロックの許可」（P.14-8）
- 「ブロッキングのディセーブル」（P.14-9）
- 「最大ブロックエントリ数の指定」（P.14-11）
- 「ブロック時間の指定」（P.14-13）
- 「ACL ロギングのイネーブル化」（P.14-14）
- 「NVRAM への書き込みのイネーブル化」（P.14-15）
- 「すべてのブロッキング イベントおよびエラーのロギング」（P.14-17）

- 「ブロッキング インターフェイスの最大数の設定」（P.14-18）
- 「絶対にブロックしないアドレスの設定」（P.14-19）

センサー自体のブロックの許可

サービス ネットワーク アクセス サブモードで **allow-sensor-block {true | false}** コマンドを使用して、センサーがそれ自体をブロックするように設定します。

注意　センサーがそれ自体をブロックすることを許可すると、ブロッキング デバイスとの通信ができなくなる可能性があるため、推奨しません。センサーでそれ自体の IP アドレスをブロックするルールが作成されても、センサーからブロッキング デバイスへのアクセスが妨げられないことが確認された場合は、このオプションを設定できます。

センサーがそれ自体をブロックすることを許可するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
```

ステップ 3　一般サブモードを開始します。

```
ips-ssp(config-net)# general
```

ステップ 4　センサーがそれ自体をブロックするように設定します。デフォルトでは、この値は false です。

```
ips-ssp(config-net-gen)# allow-sensor-block true
```

ステップ 5　設定を確認できます。

```
ips-ssp(config-net-gen)# show settings
   general
   ------------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: true default: false
      block-enable: true default: true
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      ------------------------------------------------
         ip-address: 192.0.2.1
         ------------------------------------------------
      ------------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      ------------------------------------------------
         ip-address: 209.165.200.224/27
         ------------------------------------------------
      ------------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
--MORE--
```

ステップ 6　センサーがそれ自体をブロックしないように設定します。

```
ips-ssp(config-net-gen)# allow-sensor-block false
```

ステップ 7　設定を確認します。

```
ips-ssp(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false default: false
      block-enable: true default: true
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
      -----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      -----------------------------------------------
         ip-address: 192.0.2.1
         -------------------------------------------
      -----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      -----------------------------------------------
         ip-address: 209.165.200.224/27
         -------------------------------------------
      -----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      -----------------------------------------------
--MORE--
```

ステップ 8　ネットワーク アクセス サブモードを終了します。

```
ips-ssp(config-net-gen)# exit
ips-ssp(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

ブロッキングのディセーブル

サービス ネットワーク アクセス サブモードで **block-enable {true | false}** コマンドを使用して、センサーでのブロッキングをイネーブルまたはディセーブルにします。

（注）　ブロッキングが機能するには、デバイスがブロッキングを実行するように設定する必要があります。

デフォルトでは、センサーのブロッキングはイネーブルになっています。デバイスが ARC によって管理されており、そのデバイスを手動で設定する必要がある場合、まずブロッキングをディセーブルにする必要があります。ユーザと ARC の両方が同じデバイスで同時に変更を加える状況を回避する必要があります。デバイスや ARC がクラッシュする可能性があるためです。

注意　デバイスのメンテナンスを目的としてブロッキングをディセーブルにする場合は、メンテナンスの完了後、必ずブロッキングをイネーブルにしてください。そうでないと、本来ブロック可能な攻撃に対してネットワークが脆弱になります。

（注）　ブロッキングがディセーブルの間も、ARC は引き続きブロックを受信し、アクティブなブロックの時間を追跡します。ただし、管理下にあるデバイスで新しいブロックの追加や削除は行いません。ブロッキングが再度イネーブルになると、デバイスのブロックは更新されます。

ブロッキングまたはレート制限をディセーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)#
```

ステップ 3　一般サブモードを開始します。

```
ips-ssp(config-net)# general
```

ステップ 4　センサーでブロッキングをディセーブルにします。デフォルトでは、この値は true に設定されています。

```
ips-ssp(config-net-gen)# block-enable false
```

ステップ 5　設定を確認できます。

```
ips-ssp(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false default: false
      block-enable: false default: true
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
      -----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      -----------------------------------------------
         ip-address: 192.0.2.1
         -----------------------------------------------
      -----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      -----------------------------------------------
         ip-address: 209.165.200.224/27
         -----------------------------------------------
      -----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      -----------------------------------------------
--MORE--
```

ステップ 6　センサーでブロッキングをイネーブルにします。

```
ips-ssp(config-net-gen)# block-enable true
```

ステップ 7　設定がデフォルトに戻ったことを確認します。

```
ips-ssp(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false default: false
      block-enable: true default: true
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
      -----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      -----------------------------------------------
         ip-address: 192.0.2.1
         -----------------------------------------------
      -----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      -----------------------------------------------
         ip-address: 209.165.200.224/27
         -----------------------------------------------
      -----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      -----------------------------------------------
--MORE--
```

ステップ 8　ネットワーク アクセス サブモードを終了します。

```
ips-ssp(config-net-gen)# exit
ips-ssp(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

- センサーで Cisco ルータの管理を設定する手順については、「センサーで Cisco ルータを管理するための設定」（P.14-23）を参照してください。
- センサーで Cisco ルータおよびスイッチの管理を設定する手順については、「センサーで Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータを管理するための設定」（P.14-26）を参照してください。

最大ブロックエントリ数の指定

サービス ネットワーク アクセス サブモードで **block-max-entries** コマンドを使用して、最大ブロック エントリ数を設定します。同時に維持するブロックの数を指定できます（1 ～ 65535）。デフォルト値は 250 です。

注意　250 を超える最大ブロック エントリ数を設定することは推奨できません。ACL または shun エントリ数が多いと、一部のデバイスで問題が発生する場合があります。エントリ数を増やす前に、各デバイスのマニュアルでその制限を確認してください。

（注） ブロック数が最大ブロック エントリ数を超えることはありません。最大数に達すると、既存のブロックがタイムアウトするか削除されるまで新しいブロックは発生しません。

最大ブロック エントリ数を変更するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)#
```

ステップ 3　一般サブモードを開始します。

```
ips-ssp(config-net)# general
```

ステップ 4　ブロック エントリの最大数を変更します。

```
ips-ssp(config-net-gen)# block-max-entries 100
```

ステップ 5　設定を確認します。

```
ips-ssp(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false default: false
      block-enable: true <defaulted>
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
      -----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      -----------------------------------------------
         ip-address: 192.0.2.1
         ---------------------------------------------
      -----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      -----------------------------------------------
         ip-address: 209.165.200.224/27
         ---------------------------------------------
      -----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      -----------------------------------------------
--MORE--
```

ステップ 6　ブロック数をデフォルト値の 250 に戻します。

```
ips-ssp(config-net-gen)# default block-max-entries
```

ステップ 7　設定を確認します。

```
ips-ssp(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
```

```
        allow-sensor-block: false default: false
        block-enable: true <defaulted>
        block-max-entries: 250 <defaulted>
        max-interfaces: 250 <defaulted>
        master-blocking-sensors (min: 0, max: 100, current: 0
        -----------------------------------------------
        -----------------------------------------------
        never-block-hosts (min: 0, max: 250, current: 1)
        -----------------------------------------------
           ip-address: 192.0.2.1
           -------------------------------------------
        -----------------------------------------------
        never-block-networks (min: 0, max: 250, current: 1)
        -----------------------------------------------
           ip-address: 209.165.200.224/27
           -------------------------------------------
        -----------------------------------------------
        block-hosts (min: 0, max: 250, current: 0)
        -----------------------------------------------
--MORE--
```

ステップ 8　ネットワーク アクセス サブモードを終了します。

```
ips-ssp(config-net-gen)# exit
ips-ssp(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

ブロック時間の指定

サービス イベント アクション ルール サブモードで **global-block-timeout** コマンドを使用して、自動ブロックが継続される時間を変更します。デフォルトは 30 分です。

（注）　デフォルトのブロック時間の変更は、すべてのシグニチャに影響するシグニチャ パラメータを変更することによって行います。

（注）　手動ブロックの時間は、そのブロックの要求時に設定されます。

デフォルトのブロック時間を変更するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント アクション ルール サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service event-action-rules rules0
ips-ssp(config-rul)#
```

ステップ 3　一般サブモードを開始します。

```
ips-ssp(config-rul)# general
```

ステップ 4　ブロック時間を指定します。この値は、ブロック イベントの継続時間を分単位で示しています（0 ～ 10000000）。

```
ips-ssp(config-rul-gen)# global-block-timeout 60
```

ステップ 5　設定を確認します。

```
ips-ssp(config-rul-gen)# show settings
   general
   -----------------------------------------------
      global-overrides-status: Enabled <defaulted>
      global-filters-status: Enabled <defaulted>
      global-summarization-status: Enabled <defaulted>
      global-metaevent-status: Enabled <defaulted>
      global-deny-timeout: 3600 <defaulted>
      global-block-timeout: 60 default: 30
      max-denied-attackers: 10000 <defaulted>
   -----------------------------------------------
ips-ssp(config-rul-gen)#
```

ステップ 6　イベント アクション ルール サブモードを終了します。

```
ips-ssp(config-rul-gen)# exit
ips-ssp(config-rul)# exit
Apply Changes:?[yes]:
```

ステップ 7　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

（注）　シグニチャがアップデートされるまで、少し時間がかかります。

ACL ロギングのイネーブル化

サービス ネットワーク アクセス サブモードで **enable-acl-logging {true | false}** コマンドを使用します。ACL ロギングをイネーブルにすると、ARC はログ パラメータを ACL または VACL のブロック エントリに追加します。これにより、デバイスはパケットがフィルタ処理されるときに syslog イベントを生成します。ACL ロギングのイネーブル化は、ルータとスイッチだけに適用されます。デフォルトではディセーブルになっています。

ACL ロギングをイネーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)#
```

ステップ 3　一般サブモードを開始します。

```
ips-ssp(config-net)# general
```

ステップ 4　ACL ロギングをイネーブルにします。

```
ips-ssp(config-net-gen)# enable-acl-logging true
```

ステップ 5　ACL ロギングがイネーブルになったことを確認します。

```
ips-ssp(config-net-gen)# show settings
   general
   ------------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: true default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ------------------------------------------------
```

ステップ 6　**false** キーワードを使用して ACL ロギングをディセーブルにします。

```
ips-ssp(config-net-gen)# enable-acl-logging false
```

ステップ 7　ACL ログングがディセーブルに設定されたことを確認します。

```
ips-ssp(config-net-gen)# show settings
   general
   ------------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ------------------------------------------------
```

ステップ 8　ネットワーク アクセス モードを終了します。

```
ips-ssp(config-net-gen)# exit
ips-ssp(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

NVRAM への書き込みのイネーブル化

enable-nvram-write {true | false} コマンドを使用して、ARC が最初に接続したときにルータが NVRAM に書き込みを実行するようにセンサーを設定します。enable-nvram-write をイネーブルにすると、ACL が更新されるたびに NVRAM への書き込みが実行されます。デフォルトではディセーブルになっています。

NVRAM 書き込みをイネーブルにすると、ブロッキングに関するすべての変更が NVRAM に書き込まれます。ルータが再起動されても、適切なブロックがアクティブな状態で維持されます。NVRAM 書き込みをディセーブルにすると、ルータの再起動後、ブロッキングが実行されない期間が短時間発生します。NVRAM 書き込みをイネーブルにしない場合は、NVRAM の寿命が長くなり、新しいブロックを設定する時間が短縮されます。

NVRAM 書き込みをイネーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)#
```

ステップ 3　一般サブモードを開始します。

```
ips-ssp(config-net)# general
```

ステップ 4　NVRAM への書き込みをイネーブルにします。

```
ips-ssp(config-net-gen)# enable-nvram-write true
```

ステップ 5　NVRAM への書き込みがイネーブルになったことを確認します。

```
ips-ssp(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: true default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
```

ステップ 6　NVRAM への書き込みをディセーブルにします。

```
ips-ssp(config-net-gen)# enable-nvram-write false
```

ステップ 7　NVRAM への書き込みがディセーブルになったことを確認します。

```
ips-ssp(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
```

ステップ 8　ネットワーク アクセス サブモードを終了します。

```
ips-ssp(config-net-gen)# exit
ips-ssp(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

すべてのブロッキング イベントおよびエラーのロギング

サービス ネットワーク アクセス サブモードで **log-all-block-events-and-errors {true | false}** コマンドを使用して、ブロックの後に続くイベントを最初から最後までログに記録するようにセンサーを設定します。たとえば、ブロックがデバイスに追加されるかデバイスから削除されると、イベントがログに記録されます。これらすべてのイベントおよびエラーをログに記録する必要はない可能性があります。**log-all-block-events-and-errors** をディセーブルにすると、新しいイベントとエラーは抑止されます。デフォルトはイネーブルです。

ブロッキング イベントとエラーのロギングをディセーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス モードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)#
```

ステップ 3　一般サブモードを開始します。

```
ips-ssp(config-net)# general
```

ステップ 4　ブロッキング イベントとエラーのロギングをディセーブルにします。

```
ips-ssp(config-net-gen)# log-all-block-events-and-errors false
```

ステップ 5　ロギングがディセーブルになったことを確認します。

```
ips-ssp(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: false default: true
      enable-nvram-write: false default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
```

ステップ 6　ブロッキング イベントとエラーのロギングをイネーブルにします。

```
ips-ssp(config-net-gen)# log-all-block-events-and-errors true
```

ステップ 7　ロギングがイネーブルになったことを確認します。

```
ips-ssp(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true default: true
      enable-nvram-write: false default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
```

ステップ 8　ネットワーク アクセス モードを終了します。

```
ips-ssp(config-net-gen)# exit
ips-ssp(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

ブロッキング インターフェイスの最大数の設定

max-interfaces コマンドを使用して、ブロックを実行するためのインターフェイスの最大数を設定します。たとえば、PIX Firewall は 1 つのインターフェイスとしてカウントされます。1 つのインターフェイスを持つルータは 1 つとしてカウントされますが、2 つのインターフェイスを持つルータは 2 つとしてカウントされます。1 つのルータ、スイッチ、またはファイアウォールに、最大 250 のブロッキング インターフェイスを設定できます。最大 250 の Catalyst 6K スイッチ、ルータ、およびファイアウォールを設定できます。

max-interfaces コマンドでは、すべてのインターフェイスとデバイスの合計数の制限を設定します。インターフェイスとデバイスの合計数の制限を設定できる一方、デバイス単位で設定できるブロッキング インターフェイスには、固定の制限値があります。ネットワーク アクセス モードで **show settings** コマンドを使用すると、デバイスごとに固有の最大制限値が表示されます。

ブロッキング インターフェイスの最大数を設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス モードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)#
```

ステップ 3　一般サブモードを開始します。

```
ips-ssp(config-net)# general
```

ステップ 4　インターフェイスの最大数を指定します。

```
ips-ssp(config-net-gen)# max-interfaces 50
```

ステップ 5　インターフェイスの最大数を確認します。

```
ips-ssp(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true default: true
      enable-nvram-write: false default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 50 default: 250
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
```

ステップ 6　設定をデフォルトの 250 に戻します。

```
ips-ssp(config-net-gen)# default max-interfaces
```

ステップ 7　デフォルト設定を確認します。

```
ips-ssp(config-net-gen)# show settings

   general
   ------------------------------------------------
      log-all-block-events-and-errors: true default: true
      enable-nvram-write: false default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ------------------------------------------------
```

ステップ 8　ネットワーク アクセス モードを終了します。

```
ips-ssp(config-net-gen)# exit
ips-ssp(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

絶対にブロックしないアドレスの設定

サービス ネットワーク アクセス サブモードで **never-block-hosts** および **never-block-networks** コマンドを使用して、ブロックしないホストとネットワークを設定します。

オプション

次のオプションが適用されます。

- *ip_address*：ブロックしないデバイスの IP アドレス。
- *ip_address/netmask*：ブロックしないネットワークの IP アドレス。形式は A.B.C.D/nn です。

信頼できるネットワーク デバイスによる通常の予期可能な動作が攻撃と見なされることも考えられるため、手動でも絶対にブロックしてはならないホストおよびネットワークをセンサーが識別するように調整する必要があります。そのようなデバイスは絶対にブロックしてはなりません。また、信頼できる内部のネットワークも絶対にブロックしてはなりません。単一のホストを指定することも、ネットワーク全体を指定することもできます。

（注）　**never-block-hosts** および **never-block-networks** コマンドは、Request Block Host および Request Block Connection イベント アクションだけに適用されます。Deny Attacker Inline、Deny Connection Inline、または Deny Packet Inline イベント アクションには適用されません。ブロック、拒否、またはドロップ対象から除外するホストをフィルタリングするには、イベント アクション ルールを使用します。

ブロックしないアドレスの設定

アドレスがブロッキング デバイスでブロックされないように設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)#
```

ステップ 3　一般サブモードを開始します。

```
ips-ssp(config-net)# general
```

ステップ 4　ブロックしないアドレスを指定します。

- シングル ホスト

```
ips-ssp(config-net-gen)# never-block-hosts 192.0.2.1
```

- ネットワーク

```
ips-ssp(config-net-gen)# never-block-networks 209.165.200.224/27
```

ステップ 5　設定を確認できます。

```
ips-ssp(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false default: false
      block-enable: true default: true
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
      -----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 2)
      -----------------------------------------------
         ip-address: 192.0.2.1
         -----------------------------------------------
      -----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 2)
      -----------------------------------------------
         ip-address: 209.165.200.224/27
--MORE--
```

ステップ 6　ネットワーク アクセス サブモードを終了します。

```
ips-ssp(config-net-gen)# exit
ips-ssp(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 7　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

イベント アクション フィルタの設定手順については、「イベント アクション フィルタの設定」（P.8-21）を参照してください。

ユーザ プロファイルの設定

サービス ネットワーク アクセス サブモードで **user-profiles** *profile_name* コマンドを使用して、センサーが管理する他のデバイスにユーザ プロファイルを設定します。ユーザ プロファイルには、ユーザ ID、パスワード、およびイネーブル パスワードの情報が含まれます。たとえば、同一のパスワードとユーザ名を共有するすべてのルータを、1 つのユーザ プロファイルにまとめることができます。

（注） デバイスへのログインにユーザ名またはパスワードが必要ない場合は、その値を設定しないでください。

（注） ユーザ プロファイルは、ブロッキング デバイスを設定する前に作成する必要があります。

ユーザ プロファイルを作成するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス モードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)#
```

ステップ 3　ユーザ プロファイル名を作成します。

```
ips-ssp(config-net)# user-profiles PROFILE1
```

ステップ 4　そのユーザ プロファイルに対応するユーザ名を入力します。

```
ips-ssp(config-net-use)# username username
```

ステップ 5　このユーザのパスワードを指定します。

```
ips-ssp(config-net-use)# password
Enter password[]: ********
Re-enter password ********
```

ステップ 6　このユーザのイネーブル パスワードを指定します。

```
ips-ssp(config-net-use)# enable-password
Enter enable-password[]: ********
Re-enter enable-password ********
```

ステップ 7　設定を確認できます。

```
ips-ssp(config-net-use)# show settings
   profile-name: PROFILE1
   -----------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: jsmith default:
   -----------------------------------------------
ips-ssp(config-net-use)#
```

ステップ 8　ネットワーク アクセス サブモードを終了します。

```
ips-ssp(config-net-use)# exit
ips-ssp(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

ブロッキングおよびレート制限デバイスの設定

ここでは、センサーがブロッキングまたはレート制限の実行に使用するデバイスの設定方法について説明します。次のような構成になっています。

- 「センサーによるデバイスの管理方法」（P.14-22）
- 「センサーで Cisco ルータを管理するための設定」（P.14-23）
- 「センサーで Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータを管理するための設定」（P.14-26）
- 「センサーで Cisco ファイアウォールを管理するための設定」（P.14-28）

センサーによるデバイスの管理方法

（注）　ACL はレート制限デバイスには適用されません。

ARC は Cisco ルータおよびスイッチ上の ACL を使用して、これらのデバイスを管理します。ACL は、次のように作成されます。

1. センサーの IP アドレスまたは NAT アドレス（指定されている場合）が記述された **permit** 行

   （注）　センサーのブロックを許可している場合、この行は ACL に含まれません。

2. Pre-Block ACL（指定されている場合）

   この ACL は、すでにデバイスに存在している必要があります。

   （注）　ARC は ACL 内の行を読み取り、それらの行を ACL の先頭にコピーします。

3. アクティブなブロックがある場合、そのブロック
4. 次のいずれか
   - Post-Block ACL（指定されている場合）

     この ACL は、すでにデバイスに存在している必要があります。

     （注）　ARC は ACL 内の行を読み取り、それらの行を ACL の末尾にコピーします。

（注）　一致しないすべてのパケットを許可するには、ACL の最終行を **permit ip any any** にしてください。

- **permit ip any any**（Post-Block ACL を指定した場合は使用されません）

ARC は 2 つの ACL を使用してデバイスを管理します。アクティブな ACL は一度に 1 つだけです。オフラインの ACL 名を使用して新しい ACL が作成され、それがインターフェイスに適用されます。次のサイクルでは、ARC はこのプロセスを逆順で実行します。

注意　ARC が作成する ACL を、ユーザまたは他のシステムが変更してはいけません。これらの ACL は一時的なものであり、センサーによって新しい ACL が絶えず作成されています。Pre-Block ACL および Post-Block ACL にのみ変更を加えることができます。

Pre-Block ACL または Post-Block ACL を修正する必要がある場合は、次の手順を実行します。

1. センサーでブロッキングをディセーブルにします。
2. デバイスの設定に変更を加えます。
3. センサーでブロッキングを再びイネーブルにします。

ブロッキングが再度イネーブルになると、センサーは新しいデバイス コンフィギュレーションを読み取ります。

注意　1 つのセンサーで複数のデバイスを管理できますが、1 つのデバイスに対して複数のセンサーは使用できません。その場合は、マスター ブロッキング センサーを使用してください。

詳細情報

- ブロッキングをイネーブルにする手順については、「ブロッキング プロパティの設定」（P.14-7）を参照してください。
- センサーをマスター ブロッキング センサーとして設定する手順については、「センサーをマスター ブロッキング センサーにする設定」（P.14-29）を参照してください。

センサーで Cisco ルータを管理するための設定

ここでは、Cisco ルータを管理できるようにセンサーを設定する方法について説明します。次のような構成になっています。

ルータと ACL

（注）　Pre-Block ACL と Post-Block ACLS は、レート制限には適用されません。

Pre-Block ACL と Post-Block ACL は、ルータのコンフィギュレーション内に作成し、保存します。これらの ACL は名前付きまたは番号付きの拡張 IP ACL にする必要があります。ACL の作成の詳細については、ルータのマニュアルを参照してください。[Pre-Block ACL] と [Post-Block ACL] の各フィールドに、ルータですでに設定されているこれら ACL の名前を入力します。

Pre-Block ACL は、主にブロック対象外のものを許可するために使用されます。この ACL を使用してパケットがチェックされるとき、最初に一致する行によってアクションが決まります。最初に一致する行が Pre-Block ACL の許可の行である場合、ACL の後の方に（自動ブロックの）拒否の行があっても、そのパケットは許可されます。Pre-Block ACL は、ブロックによって生じる拒否の行よりも優先されます。

Post-Block ACL は、同じインターフェイスまたは方向に対して、追加的にブロッキングまたは許可を行う場合に最適です。センサーが管理するインターフェイスまたは方向に既存の ACL がある場合、その ACL を Post-Block ACL として使用できます。Post-Block ACL がない場合、センサーは新しい ACL の末尾に **permit ip any any** を挿入します。

センサーが起動すると、2 つの ACL の内容が読み込まれます。そして、次のエントリを持った 3 つ目の ACL が作成されます。

- センサーの IP アドレスに対応する **permit** 行
- Pre-Block ACL のすべての設定行のコピー
- センサーによってブロックされている各アドレスの **deny** 行
- Post-Block ACL のすべての設定行のコピー

センサーは新しい ACL を、指定したインターフェイスと方向に適用します。

（注） 新しい ACL がルータのインターフェイスまたは方向に適用されると、そのインターフェイスまたは方向に対する他の ACL が適用されなくなります。

センサーで Cisco ルータを管理するための設定

Cisco ルータを管理できるようにセンサーを設定し、ブロッキングおよびレート制限を実行するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)#
```

ステップ 3　ARC によって制御されるルータの IP アドレスを設定します。

```
ips-ssp(config-net)# router-devices ip_address
```

ステップ 4　ユーザ プロファイルの設定時に作成した論理デバイス名を入力します。

```
ips-ssp(config-net-rou)# profile-name user_profile_name
```

ARC はどのような入力内容も受け入れます。そのユーザ プロファイルが存在するかどうかは確認されません。

ステップ 5　センサーへのアクセスに使用する方法を指定します。指定しないと、SSH 3DES が使用されます。

```
ips-ssp(config-net-rou)# communication {telnet | ssh-3des}
```

（注）　3DES を使用している場合は、**ssh host-key** *ip_address* コマンドを使用してキーを受け入れる必要があります。そうでないと、ARC はデバイスに接続できません。

ステップ 6　センサーの NAT アドレスを指定します。

```
ips-ssp(config-net-rou)# nat-address nat_address
```

（注）　これによって ACL の 1 行目の IP アドレスが、センサーのアドレスから NAT アドレスに変更されます。このアドレスは、管理対象のデバイスに設定された NAT アドレスではありません。これはセンサーが中間デバイスによって変換されたアドレス、つまり、センサーと管理対象デバイスの間にあるアドレスです。

ステップ 7　ルータがブロッキングまたはレート制限、あるいはその両方を実行するかどうかを指定します。

（注）　デフォルトはブロッキングです。ルータでブロッキングだけを実行する場合、応答機能を設定する必要はありません。

a.　レート制限のみの場合

```
ips-ssp(config-net-rou)# response-capabilities rate-limit
```

b.　ブロッキングとレート制限の場合

```
ips-ssp(config-net-rou)# response-capabilities block|rate-limit
```

ステップ 8　インターフェイス名と方向を指定します。

```
ips-ssp(config-net-rou)# block-interfaces interface_name {in | out}
```

注意　インターフェイス名はインターフェイスの完全な名前か、ルータが **interface** コマンドを使用して認識できる省略名のいずれかでなければなりません。

ステップ 9　（任意）pre-ACL 名を追加します（ブロッキングのみ）。

```
ips-ssp(config-net-rou-blo)# pre-acl-name pre_acl_name
```

ステップ 10　（任意）post-ACL 名を追加します（ブロッキングのみ）。

```
ips-ssp(config-net-rou-blo)# post-acl-name post_acl_name
```

ステップ 11　設定を確認できます。

```
ips-ssp(config-net-rou-blo)# exit
ips-ssp(config-net-rou)# show settings
   ip-address: 192.0.2.1
   -----------------------------------------------
      communication: ssh-3des default: ssh-3des
      nat-address: 19.89.149.219 default: 0.0.0.0
      profile-name: PROFILE1
      block-interfaces (min: 0, max: 100, current: 1)
      -----------------------------------------------
         interface-name: GigabitEthernet0/1
         direction: in
         -----------------------------------------------
            pre-acl-name: <defaulted>
```

```
            post-acl-name: <defaulted>
          ------------------------------------------------
        ------------------------------------------------
        response-capabilities: block|rate-limit default: block
      ------------------------------------------------
ips-ssp(config-net-rou)#
```

ステップ 12　ネットワーク アクセス サブモードを終了します。

```
ips-ssp(config-net-rou)# exit
ips-ssp(config-net)# exit
ips-ssp(config)# exit
Apply Changes:?[yes]:
```

ステップ 13　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

- ユーザ プロファイルの設定手順については、「ユーザ プロファイルの設定」（P.14-21）を参照してください。
- 既知のホスト リストにデバイスを追加する手順については、「SSH 既知ホスト リストへのホストの追加」（P.4-35）を参照してください。

センサーで Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータを管理するための設定

ここでは、Cisco スイッチを管理できるようにセンサーを設定する方法について説明します。次のような構成になっています。

スイッチと VACL

ARC を設定して、Cisco Catalyst ソフトウェアの実行時にスイッチ自体の VACL を使用してブロッキングするか、あるいは Cisco IOS ソフトウェアの実行時に MSFC またはスイッチ自体のルータ ACL を使用してブロッキングすることができます。ここでは、VACL を使用したブロッキングについて説明します。VACL を使用するスイッチがレート制限を実行するように設定することはできません。Catalyst 6500 シリーズ スイッチでブロッキング インターフェイスを設定し、ブロックするトラフィックの VLAN を指定する必要があります。

スイッチのコンフィギュレーション内に Pre-Block VACL と Post-Block VACL を作成し、保存します。これらの VACL は、名前付きまたは番号付きの拡張 IP VACL にする必要があります。VACL の作成の詳細については、スイッチのマニュアルを参照してください。[Pre-Block VACL] と [Post-Block VACL] の各フィールドに、スイッチですでに設定されている VACL の名前を入力します。

Pre-Block VACL は、主としてセンサーでブロックの対象外とするものを許可するために使用されます。VACL でパケットが確認されると、最初に一致した行によってアクションが決定されます。最初に一致した行が Pre-Block VACL の permit 行の場合、VACL の後の部分に（自動ブロックの）deny 行があっても、そのパケットは許可されます。Pre-Block VACL は、ブロックによって生じる deny 行をオーバーライドできます。

Post-Block VACL は、同じ LAN 上で追加のブロッキングまたは許可を行う場合に最適です。センサーが管理する VLAN 上に既存の VACL がある場合、その既存 VACL を Post-Block VACL として使用することができます。Post-Block VACL がない場合、センサーは新しい VACL の末尾に **permit ip any any** を挿入します。

センサーは、起動すると 2 つの VACL の内容を読み込みます。そして、次のエントリが含まれた 3 つ目の VACL を作成します。

- センサーの IP アドレスに対応する **permit** 行
- Pre-Block VACL のすべての設定行のコピー
- センサーによってブロックされている各アドレスの **deny** 行
- Post-Block VACL のすべての設定行のコピー

センサーは、指定された VLAN に新しい VACL を適用します。

（注） 新しい VACL がスイッチの VLAN に適用されると、その VLAN に対して他の VACL は適用されなくなります。

詳細情報

ルータ ACL を使用したブロッキングの設定手順については、「ブロッキングおよびレート制限デバイスの設定」（P.14-22）を参照してください。

センサーで Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータを管理するための設定

Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータを管理できるようにセンサーを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)#
```

ステップ 3　ARC によって制御されるルータの IP アドレスを設定します。

```
ips-ssp(config-net)# cat6k-devices ip_address
```

ステップ 4　ユーザ プロファイルの設定時に作成したユーザ プロファイル名を入力します。

```
ips-ssp(config-net-cat)# profile-name user_profile_name
```

（注） ARC はどのような入力内容も受け入れます。論理デバイスが存在するかどうかのチェックは行いません。

ステップ 5　センサーへのアクセスに使用する方法を指定します。指定しないと、SSH 3DES が使用されます。

```
ips-ssp(config-net-cat)# communication {telnet | ssh-3des}
```

（注） 3DES を使用している場合は、**ssh host-key** *ip_address* コマンドを使用してキーを受け入れる必要があります。そうでないと、ARC はデバイスに接続できません。

ステップ 6　センサーの NAT アドレスを指定します。

```
ips-ssp(config-net-cat)# nat-address nat_address
```

（注） これによって ACL の 1 行目の IP アドレスが、センサーの IP アドレスから NAT のアドレスに変更されます。このアドレスは、管理対象のデバイスに設定された NAT アドレスではありません。これはセンサーが中間デバイスによって変換されたアドレス、つまり、センサーと管理対象デバイスの間にあるアドレスです。

ステップ 7　VLAN 番号を指定します。

```
ips-ssp(config-net-cat)# block-vlans vlan_number
```

ステップ 8　（任意）pre-VACL 名を追加します。

```
ips-ssp(config-net-cat-blo)# pre-vacl-name pre_vacl_name
```

ステップ 9　（任意）post-VACL 名を追加します。

```
ips-ssp(config-net-cat-blo)# post-vacl-name post_vacl_name
```

ステップ 10　ネットワーク アクセス サブモードを終了します。

```
ips-ssp(config-net-cat-blo)# exit
ips-ssp(config-net-cat)# exit
ips-ssp(config-net)# exit
ips-ssp(config)# exit
Apply Changes:?[yes]:
```

ステップ 11　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

- ユーザ プロファイルの設定手順については、「ユーザ プロファイルの設定」（P.14-21）を参照してください。
- 既知のホスト リストにデバイスを追加する手順については、「SSH 既知ホスト リストへのホストの追加」（P.4-35）を参照してください。

センサーで Cisco ファイアウォールを管理するための設定

Cisco ファイアウォールを管理できるようにセンサーを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)#
```

ステップ 3　ARC によって制御されるファイアウォールの IP アドレスを指定します。

```
ips-ssp(config-net)# firewall-devices ip_address
```

ステップ 4　ユーザ プロファイルの設定時に作成したユーザ プロファイル名を入力します。ARC はどのような入力内容も受け入れます。ARC は入力を受け入れず、論理デバイスが存在するかどうか確認します。

```
ips-ssp(config-net-fir)# profile-name user_profile_name
```

ステップ 5　センサーへのアクセスに使用する方法を指定します。指定しないと、SSH 3DES が使用されます。

```
ips-ssp(config-net-fir)# communication {telnet | ssh-3des}
```

（注） 3DES を使用している場合は、**ssh host-key** *ip_address* コマンドを使用してキーを受け入れる必要があります。そうでないと、ARC はデバイスに接続できません。

ステップ 6　センサーの NAT アドレスを指定します。

```
ips-ssp(config-net-fir)# nat-address nat_address
```

（注） これによって ACL の 1 行目の IP アドレスが、センサーの IP アドレスから NAT のアドレスに変更されます。このアドレスは、管理対象のデバイスに設定された NAT アドレスではありません。これはセンサーが中間デバイスによって変換されたアドレス、つまり、センサーと管理対象デバイスの間にあるアドレスです。

ステップ 7　ネットワーク アクセス サブモードを終了します。

```
ips-ssp(config-net-fir)# exit
ips-ssp(config-net)# exit
ips-ssp(config)# exit
Apply Changes:?[yes]:
```

ステップ 8　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

- ユーザ プロファイルの設定手順については、「ユーザ プロファイルの設定」（P.14-21）を参照してください。
- 既知のホスト リストにデバイスを追加する手順については、「SSH 既知ホスト リストへのホストの追加」（P.4-35）を参照してください。

センサーをマスター ブロッキング センサーにする設定

複数のセンサー（ブロッキング転送センサー）が、1 つ以上のデバイスを制御する、指定したマスター ブロッキング センサーに、ブロッキング要求を転送できます。マスター ブロッキング センサーは、他の 1 つ以上のセンサーに代わって 1 つ以上のデバイスでブロッキングを制御するセンサーで実行されている ARC です。マスター ブロッキング センサーの ARC は、他のセンサーで動作している ARC の要求に応じてデバイスでのブロッキングを制御します。マスター ブロッキング センサーは、レート制限を転送することもできます。

注意　2 つのセンサーが同じデバイスでブロッキングまたはレート制限を制御することはできません。この状況が必要な場合は、一方のセンサーをデバイス管理用のマスター ブロッキング センサーとして設定すると、もう一方のセンサーからマスター ブロッキング センサーに要求を転送できます。

マスター ブロッキング センサーを追加する場合は、センサーあたりのブロッキング デバイス数を減らします。たとえば、それぞれ 1 つのブロッキング インターフェイス/方向を持つ 10 個のファイア ウォールと 10 台のルータでブロックする場合は、センサーに 10 個を割り当て、マスター ブロッキング センサーに残りの 10 個を割り当てることができます。

ブロッキング転送センサーで、マスター ブロッキング センサーとして機能するリモート ホストを特定します。マスター ブロッキング センサーでは、ブロッキング転送センサーをアクセス リストに追加する必要があります。

マスター ブロッキング センサーが Web 接続に TLS を必要とする場合は、マスター ブロッキング センサー リモート ホストの X.509 証明書を受け入れるようにブロッキング転送センサーの ARC を設定する必要があります。センサーでは TLS がデフォルトでイネーブルになりますが、このオプションは変更できます。

（注）　通常、マスター ブロッキング センサーはネットワーク デバイスを管理するように設定します。ブロッキング転送センサーは、通常は他のネットワーク デバイスを管理するようには設定されていませんが、これを行うことは可能です。

ブロッキングまたはレート制限用に設定されたデバイスがなくても、ブロッキングまたはレート制限用に設定されたセンサーは、ブロッキングおよびレート制限要求をマスター ブロッキング センサーに転送することができます。ブロッキングまたはレート制限要求がイベント アクションとして設定されているシグニチャが起動した場合、センサーはブロック要求またはレート制限要求をマスター ブロッキング センサーに転送し、そのセンサーがブロックまたはレート制限を実行します。

注意　1 つのセンサーだけがデバイス上のすべてのブロッキング インターフェイスを制御する必要があります。

サービス ネットワーク アクセス サブモードで **master-blocking-sensors** *mbs_ip_address* コマンドを使用して、マスター ブロッキング センサーを設定します。

オプション

次のオプションが適用されます。

- *master_blocking_sensor_ip_address*：ブロック要求を転送するセンサーの IP アドレスを指定します。
- **password**：ブロック要求を転送するセンサーのアカウント パスワードを指定します。
- **port**：ブロック要求を転送するセンサーのポートを指定します。
- **tls {true | false}**：リモート センサーに TLS が必要な場合は true、それ以外の場合は false に設定します。
- **password**：ブロック要求を転送するセンサーのアカウント名を指定します。

マスター ブロッキング センサーの設定

センサーの ARC がマスター ブロッキング センサーにブロックを転送するように設定するには、次の手順を実行します。

ステップ 1　マスター ブロッキング センサーとブロッキング転送センサーの両方で、管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　両方のセンサーでコンフィギュレーション モードを開始します。

```
ips-ssp# configure terminal
```

ステップ 3　必要に応じて TLS を設定します。

a. マスター ブロッキング センサーで TLS が必要かどうかと、使用されるポート番号を確認します。`enable-tls` が true の場合はステップ b に進みます。

```
ips-ssp(config)# service web-server
ips-ssp(config-web)# show settings
   enable-tls: true <defaulted>
   port: 443 <defaulted>
   server-id: HTTP/1.1 compliant <defaulted>
ips-ssp(config-web)#
```

b. ブロッキング転送センサーで、マスター ブロッキング センサーの X.509 証明書を受け入れるように設定します。

```
ips-ssp(config-web)# exit
ips-ssp(config)# tls trusted-host ip-address master_blocking_sensor_ip_address port
port_number
```

例

```
ips-ssp(config)# tls trusted-host ip-address 192.0.2.1 port 8080
Certificate MD5 fingerprint is
F4:4A:14:BA:84:F4:51:D0:A4:E2:15:38:7E:77:96:D8Certificate SHA1 fingerprint is
84:09:B6:85:C5:43:60:5B:37:1E:6D:31:6A:30:5F:7E:4D:4D:E8:B2
Would you like to add this to the trusted certificate table for this host?[yes]:
```

（注） 証明書のフィンガープリントに基づいて証明書を受け入れるよう求めるプロンプトが表示されます。センサーが提供するのは、自己署名証明書（認識された認証局の署名がある証明書ではなく）だけです。マスター ブロッキング センサーのホスト センサーの証明書を確認するには、そのホスト センサーにログインし、**show tls fingerprint** コマンドを入力して、ホスト証明書のフィンガープリントと一致することを確認します。

ステップ 4　**yes** を入力して、マスター ブロッキング センサーの証明書を受け入れます。

ステップ 5　ネットワーク アクセス モードを開始します。

```
ips-ssp(config)# service network-access
```

ステップ 6　一般サブモードを開始します。

```
ips-ssp(config-net)# general
```

ステップ 7　マスター ブロッキング センサーのエントリを追加します。

```
ips-ssp(config-net-gen)# master-blocking-sensors master_blocking_sensor_ip_address
```

ステップ 8　マスター ブロッキング センサー ホストの管理アカウントのユーザ名を指定します。

```
ips-ssp(config-net-gen-mas)# username username
```

ステップ 9　このユーザのパスワードを指定します。

```
ips-ssp(config-net-gen-mas)# password
Enter password []: *****
Re-enter mbs-password []: *****
ips-ssp(config-net-gen-mas)#
```

ステップ 10　ホストの HTTP 通信用のポート番号を指定します。

```
ips-ssp(config-net-gen-mas)# port port_number
```

指定しない場合のデフォルトは 80/443 です。

ステップ 11　ホストが TLS/SSL を使用するかどうかを指定します。

```
ips-ssp(config-net-gen-mas)# tls {true | false}
ips-ssp(config-net-gen-mas)
```

（注）　値を true に設定する場合は、**tls trusted-host ip-address** *master_blocking_sens0r_ip_address* コマンドを使用する必要があります。

ステップ 12　ネットワーク アクセス サブモードを終了します。

```
ips-ssp(config-net-gen-mas)# exit
ips-ssp(config-net-gen)# exit
ips-ssp(config-net)# exit
ips-ssp(config)# exit
Apply Changes:?[yes]:
```

ステップ 13　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

ステップ 14　マスター ブロッキング センサーで、ブロック転送センサーの IP アドレスをアクセス リストに追加します。

詳細情報

ブロッキング転送センサーの IP アドレスをアクセス リストに追加する手順については、「アクセス リストの変更」（P.4-5）を参照してください。

ホスト ブロッキングの設定

特権 EXEC モードで **block host** *ip-address* [**timeout** *minutes*] コマンドを使用して、ホストをブロックします。ホストのブロックを削除するには、このコマンドの **no** 形式を使用します。ブロッキングの設定は、ホスト ブロックの設定前に行う必要があります。ブロックされているホストのリストを表示することもできます。

（注）　ホスト ブロックの時間を設定しない場合、そのブロックは永続的に実行されます。

（注）　適応型セキュリティ アプライアンスでは、接続ブロックとネットワーク ブロックはサポートされません。適応型セキュリティ アプライアンスでは、接続情報が追加されたホスト ブロックだけがサポートされます。

オプション

次のオプションが適用されます。

- *ip-address*：ブロックするホストの IP アドレスを指定します。
- *minutes*：（任意）ホスト ブロックの時間を分単位で指定します。指定できる範囲は 0 ～ 70560 分です。

ホストのブロッキング

ホストをブロックするには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　たとえば、15 分間のホスト ブロックを設定します。このホスト ブロックは 15 分で終了します。

```
ips-ssp# block host 192.0.2.1 timeout 15
```

ステップ 3　ホスト ブロックを開始します。このホスト ブロックは削除されるまで継続されます。

```
ips-ssp# block host 192.0.2.1
```

ステップ 4　ホスト ブロックを終了します。

```
ips-ssp# no block host 192.0.2.1
ips-ssp#
```

ネットワーク ブロッキングの設定

特権 EXEC モードで **block network** *ip-address/netmask* [**timeout** *minutes*] コマンドを使用して、ネットワークをブロックします。ネットワークのブロックを削除するには、このコマンドの **no** 形式を使用します。ブロッキングの設定は、ネットワーク ブロックの設定前に行う必要があります。ブロックされているネットワークのリストを表示することもできます。

（注）　ネットワーク ブロックの時間を設定しない場合、そのブロックは永続的に実行されます。

（注）　適応型セキュリティ アプライアンスでは、接続ブロックとネットワーク ブロックはサポートされません。適応型セキュリティ アプライアンスでは、接続情報が追加されたホスト ブロックだけがサポートされます。

オプション

次のオプションが適用されます。

- *ip-address/netmask*：ブロックするネットワークのサブネットを *X.X.X.X/nn* 形式で指定します。*X.X.X.X* はセンサーの IP アドレスで、ピリオドで区切られた 4 オクテットで記述される 32 ビット アドレスです。*X* は 0 ～ 255、*nn* はネットマスクのビット数（1032）を示します。
- *minutes*：（任意）ネットワーク ブロックの時間を分単位で指定します。指定できる範囲は 0 ～ 70560 分です。

ネットワークのブロッキング

ネットワークをブロックするには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　たとえば、15 分間のネットワーク ブロックを設定します。このネットワーク ブロックは 15 分で終了します。

```
ips-ssp# block network 192.0.2.0/24 timeout 15
```

ステップ 3　ネットワーク ブロックを開始します。このネットワーク ブロックは削除されるまで継続されます。

```
ips-ssp# block network 192.0.2.0/24
```

ステップ 4　ネットワーク ブロックを終了します。

```
ips-ssp# no block network 192.0.2.0/24
ips-ssp#
```

接続ブロッキングの設定

特権 EXEC モードで **block connection** *source-ip-address destination-ip-address* [**port** *port-number*] [**protocol** *type*] [**timeout** *minutes*] コマンドを使用して、2 つの IP アドレス間の接続をブロックします。接続ブロックを削除するには、このコマンドの **no** 形式を使用します。ブロッキングの設定は、接続ブロックの設定前に行う必要があります。ブロックされている接続のリストを表示することもできます。

（注）　接続ブロックの時間を設定しない場合、そのブロックは永続的に実行されます。

（注）　適応型セキュリティ アプライアンスでは、接続ブロックとネットワーク ブロックはサポートされません。適応型セキュリティ アプライアンスでは、接続情報が追加されたホスト ブロックだけがサポートされます。

オプション

次のオプションが適用されます。

- *source-ip-address*：接続ブロックでの送信元 IP アドレスを指定します。
- *destination-ip-address*：接続ブロックでの宛先 IP アドレスを指定します。
- *port-number*：（任意）宛先ポート番号を指定します。有効な範囲は 0 ～ 65535 です。
- *type*：（任意）プロトコル タイプを指定します。有効なタイプは **tcp** または **udp** です。
- *minutes*：（任意）接続ブロックの時間を分単位で指定します。指定できる範囲は 0 ～ 70560 分です。

接続のブロッキング

接続をブロックするには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　たとえば、ポート、プロトコル、時間を指定して、送信元 IP アドレスと宛先 IP アドレス間の接続ブロックを設定します。この接続ブロックは 30 分で終了します。

```
ips-ssp# block connection 10.0.0.0 172.16.0.0 port 80 protocol tcp timeout 30
```

ステップ 3　接続ブロックを開始します。この接続ブロックは削除されるまで継続されます。

```
ips-ssp# block connection 10.0.0.0 172.16.0.0
```

ステップ 4　接続ブロックを終了します。

```
ips-ssp# no block connection 10.0.0.0
ips-ssp#
```

ブロックされているホストおよび接続のリストの取得

show statistics コマンドを使用して、ブロックされているホストと接続のリストを取得します。

ブロックされているホストおよび接続のリストを取得するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　ARC の統計情報を確認します。`Host` エントリは、ブロックされているホストと、ブロックの時間を示しています。

```
ips-ssp# show statistics network-access
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = false
   BlockMaxEntries = 250
   MaxDeviceInterfaces = 250
   NetDevice
      Type = Cisco
      IP = 10.1.1.1
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = fa0/0
```

```
         InterfaceDirection = in
State
   BlockEnable = true
   NetDevice
      IP = 10.1.1.1
      AclSupport = uses Named ACLs
      Version = 12.2
      State = Active
   BlockedAddr
      Host
         IP = 192.168.1.1
         Vlan =
         ActualIp =
         BlockMinutes = 80
         MinutesRemaining = 76
```