コアの保護：インフラストラクチャ保護 ACL

内容

概要

この文書では、インフラストラクチャ保護 access control list (ACL; アクセス コントロール リスト) についてのガイドラインと、推奨する配備方法について説明します。 インフラストラクチャ ACL は、インフラストラクチャ機器への認証されたトラフィックだけを明示的に許可し、他の一時通過トラフィックはすべて許可することで、直接的なインフラストラクチャ攻撃の危険性と影響を最小限に抑えるために使用されます。

インフラストラクチャ保護

背景

ルータをさまざまなリスク (偶発的または作為的を問わず) から保護するために、ネットワークの入口にはインフラストラクチャ保護 ACL を導入してください。IPv4 ACL および IPv6 ACL により、外部ソースからのすべてのインフラストラクチャ アドレス (ルータ インターフェイスなど) へのアクセスが拒否されます。同時に、ACLは定期的なトランジットトラフィックのフローを中断なく許可し、基本的なRFC 1918 、RFC 3330、およびアンチスプーフィングフィルタリングを提供しま す。

ルータで受信されるデータは、次の 2 つのカテゴリに大別できます。

- フォワーディング パスを経由してルータを通過するトラフィック
- ルート プロセッサの処理のために受信パスを経由してこのルータを宛先とするトラフィック

通常の動作では、ほとんどのトラフィックはルータからルータを通過して最終的な宛先に到達します。

ただし、ルーティング プロトコル、リモート ルータ アクセス（セキュア シェル（SSHS）など）、ネットワーク管理トラフィック（Simple Network Management Protocol（SNMP）など）をはじめとする特定のタイプのデータについては、ルート プロセッサ（RP）が直接処理しなければなりません。 さらに、Internet Control Message Protocol（ICMP）などのプロトコルや IP オプションも、RP で直接処理する必要があります。通常、インフラストラクチャ ルータへのダイレクト アクセスが必要になるのは、内部発信元からの場合だけです。少数の注目すべき例外としては、外部 Border Gateway Protocol（BGP）のピア、実際のルータを終端とするプロトコル（Generic Routing Encapsulation（GRE）や IPv6 over IPv4 トンネルなど）、そして場合によっては接続テスト用（エコー要求または ICMP 到達不能など）およびトレースルートに対するパケット存続時間（TTL）満了メッセージのための ICMP パケットの一部が挙げられます。

注：ICMPは単純なサービス拒否(DoS)攻撃によく使用され、必要に応じて外部ソースからのみ許可する必要があることに注意してください。

すべての RP にはパフォーマンス枠があり、その枠内で動作します。RP 宛ての過剰なトラフィックによってルータが過負荷状態になる可能性があります。その場合、CPU 使用率が増加し、最終的にはパケットおよびルーティング プロトコルがドロップされて DoS 攻撃が発生することになります。外部送信元からのインフラストラクチャ ルータへのアクセスをフィルタリングすることにより、ルータが直接攻撃されることになる外的リスクの多くが軽減されます。こうすれば、外部からの攻撃はインフラストラクチャ機器を使用できなくなります。攻撃は自律システム（AS）への入力インターフェイスでドロップされます。

この文書で説明するフィルタリング方式は、ネットワーク インフラストラクチャ機器宛てのデータのフィルタリングが目的です。インフラストラクチャフィルタリングを汎用フィルタリングと混同しないでください。インフラストラクチャ保護 ACL の唯一の目的は、極めて重要なインフラストラクチャ機器へのアクセスを許可するプロトコルと送信元をより細かいレベルで制限することです。

ネットワーク インフラストラクチャ機器には、次の領域が含まれます。

- すべてのルータおよびスイッチ管理アドレス（ループバック インターフェイスを含む）
- すべての内部リンク アドレス：ルータ間リンク（ポイントツーポイントおよび多重アクセス）
- 外部発信元からアクセスすべきでない内部サーバまたはサービス

このドキュメントでは、インフラストラクチャを宛先としないすべてのトラフィックを中継トラフィックと呼びます。

方法

インフラストラクチャ保護は、次のさまざまな方法で実現できます。

- **受信 ACL（rACL）** Cisco 12000 および 7500 プラットフォームでは、RP 宛てのすべてのトラフィックをフィルタリングし、中継トラフィックには影響を与えない rACL をサポートします。認証済みトラフィックを明示的に許可し、rACL をすべてのルータに導入する必要があります。デバイスへの正当なトラフィックを識別して許可を与え、望ましくないパケットをすべて拒否するには、『GSR：受信アクセス コントロール リストを参照してください。
- **ホップバイホップ ルータ ACL**ルータのインターフェイスで認証済みのトラフィックだけを許可し、中継トラフィックを除くその他のすべてのトラフィックを拒否する ACL を定義することでも、ルータを保護できます。中継トラフィックは明示的に許可する必要があります。この ACL は、論理的に rACL と似ていますが、中継トラフィックに影響が及びます。したがって、ルータの転送レートに悪影響を与える可能性があります。

- **インフラストラクチャ ACL によるエッジ フィルタリング**ACL は、ネットワークのエッジに適用できます。サービス プロバイダー（SP）の場合は、AS のエッジに適用できます。この ACL では、インフラストラクチャのアドレス空間宛てのトラフィックを明示的にフィルタリングします。エッジ インフラストラクチャ ACL を導入するには、インフラストラクチャ空間と、この空間にアクセスする必要があるプロトコルおよび認証済みプロトコルを明確に定義する必要があります。この ACL は、ネットワークの入口で、外部に対するすべての接続（ピア接続、顧客向け接続など）に適用します。この文書では、エッジ インフラストラクチャ保護 ACL の作成と配備に重点を置いて説明します。

ACL の例

次の IPv4 および IPv6 アクセス リストでは、保護 ACL に必要な一般的なエントリの簡単で実際的な例を示しています。これら基本的な ACL は、ローカルなサイト特有の設定事項を反映するようにカスタマイズする必要があります。デュアル IPv4/IPv6 環境では、以下のアクセス リストを両方とも導入します。

IPv4 の例

```
!--- Anti-spoofing entries are shown here. !--- Deny special-use address sources. !--- Refer to
RFC 3330 for additional special use addresses. access-list 110 deny ip host 0.0.0.0 any access-
list 110 deny ip 127.0.0.0 0.255.255.255 any access-list 110 deny ip 192.0.2.0 0.0.0.255 any
access-list 110 deny ip 224.0.0.0 31.255.255.255 any !--- Filter RFC 1918 space. access-list 110
deny ip 10.0.0.0 0.255.255.255 any access-list 110 deny ip 172.16.0.0 0.15.255.255 any access-
list 110 deny ip 192.168.0.0 0.0.255.255 any !--- Deny your space as source from entering your
AS. !--- Deploy only at the AS edge. access-list 110 deny ip YOUR_CIDR_BLOCK any !--- Permit
BGP. access-list 110 permit tcp host bgp_peer host router_ip eq bgp access-list 110 permit tcp
host bgp_peer eq bgp host router_ip !--- Deny access to internal infrastructure addresses.
access-list 110 deny ip any INTERNAL_INFRASTRUCTURE_ADDRESSES !--- Permit transit traffic.
access-list 110 permit ip any any
```

IPv6 の例

IPv6 アクセスリストは、拡張および名前付きアクセスリストとして適用する必要があります。

```
!--- Configure the access-list. ipv6 access-list iacl !--- Deny your space as source from
entering your AS. !--- Deploy only at the AS edge. deny ipv6 YOUR_CIDR_BLOCK_IPV6 any !---
Permit multiprotocol BGP. permit tcp host bgp_peer_ipv6 host router_ipv6 eq bgp permit tcp host
bgp_peer_ipv6 eq bgp host router_ipv6 !--- Deny access to internal infrastructure addresses.
deny ipv6 any INTERNAL_INFRASTRUCTURE_ADDRESSES_IPV6 !--- Permit transit traffic. permit ipv6
any any
```

注： キーワード log は、あるプロトコルの発信元と宛先に関する詳細を表示するために使用できます。このキーワードは ACL ヒットに関する有益な詳細情報を提供しますが、**log キーワードを使用した ACL エントリとのヒット数が多すぎると、CPU 使用率が高くなります。**ロギングに関連したパフォーマンスへの影響は、プラットフォームによって異なります。また、log キーワードを使用すると、アクセス リスト ステートメントに一致するパケットの Cisco Express Forwarding（CEF）スイッチングが無効になります。これらのパケットは、代わりにファースト スイッチングされます。

保護 ACL の作成

一般に、インフラストラクチャ ACL は次の 4 つのセクションで構成されます。

- 特定用途のアドレスとアンチスプーフィングのエントリで、これは不正な発信元や、自身の AS に属する発信元アドレスを持ったパケットが、外部発信元から AS 内に入ることを拒否します。**注：**RFC 3330では、フィルタリングが必要な可能性のあるIPv4の特殊用途アドレスを定義しています。RFC 1918 では、インターネット上で無効とするソース アドレスを IPv4 予約アドレスとして定義しています。RFC 3513 では、IPv6 アドレッシング アーキテクチャを定義しています。RFC 2827では、入力フィルタリングのガイドラインを提供しています 。
- 明示的に許可する、外部送信元からのインフラストラクチャ アドレス宛てトラフィック
- **他のすべての外部発信元からのインフラストラクチャ アドレスへのトラフィックを拒否する deny 文**
- **インフラストラクチャ以外の宛先へ向かう途中の、通常のバックボーン トラフィック宛ての他のすべてのトラフィックに対する permit 文**

インフラストラクチャ ACL の最後の行では、中継トラフィックを明示的に許可します。**permit ip any any** for IPv4**とpermit ipv6 any any any for IPv6。このエントリにより、すべてのIPプロトコルがコアを通じて許可され、顧客は問題なくアプリケーションを実行し続けることができます。**

インフラストラクチャ保護 ACL を作成する最初のステップは、必要なプロトコルを理解することです。それぞれのサイトによって固有の要件がありますが、一般的に導入する特定のプロトコルについて理解する必要があります。たとえば、外部ピアに対する外部 BGP は明示的に許可する必要があります。インフラストラクチャ ルータへのダイレクト アクセスが必要なその他のすべてのプロトコルについても、同じく明示的に許可する必要があります。たとえば、GRE トンネルをコア インフラストラクチャ ルータで終端する場合は、プロトコル 47（GRE）も明示的に許可する必要があります。同様に、IPv6 over IPv4 トンネルをコア インフラストラクチャ ルータで終端する場合は、プロトコル 41（IPv6 over IPv4）も明示的に許可する必要があります。

分類 ACL を利用して、必要なプロトコルを特定できます。分類 ACL は、インフラストラクチャ ルータ宛てに使用される可能性のある各種のプロトコルに対する **permit 文で構成されます。**詳細なリストについては、Cisco IOS®ソフトウェアでサポートされているプロトコルの付録を参照してください。アクセス コントロール エントリ（ACE）のヒット数を表示する **show access-list コマンドを使用すると、必要なプロトコルを判別できます。**疑わしい、あるいは意外な結果が出た場合は、予期しないプロトコルに対して **permit 文を作成する前に、調査してその結果を理解してください。**

たとえば、GRE、IPsec（ESP）および IPv6 トンネリング（IP プロトコル 41）を許可する必要があるかどうかを判別するには、以下の IPv4 ACL が参考になります。

```
access-list 101 permit GRE any infrastructure_ips
access-list 101 permit ESP any infrastructure_ips
access-list 101 permit 41 any infrastructure_ips
access-list 101 permit ip any infrastructure_ips log
!--- The log keyword provides more details !--- about other protocols that are not explicitly
permitted.

access-list 101 permit ip any any

interface <int>
 ip access-group 101 in
```

以下の IPv6 ACL は、GRE および IPsec（ESP）を許可する必要があるかどうかを判別するために使用できます。

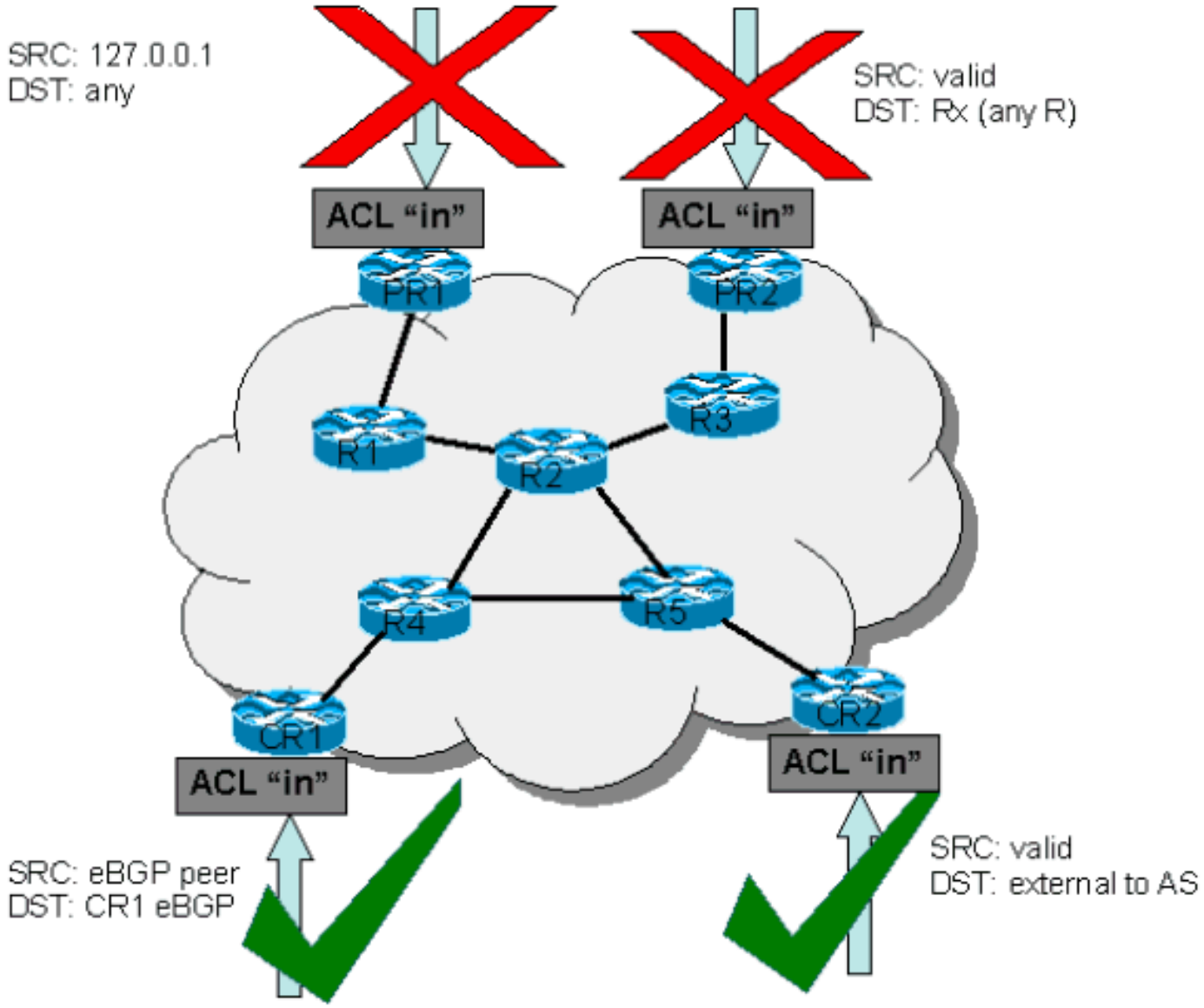
```
ipv6 access-list determine_protocols
 permit GRE any infrastructure_ips_ipv6
 permit ESP any infrastructure_ips_ipv6
 permit ipv6 any infrastructure_ips_ipv6 log
!--- The log keyword provides more details !--- about other protocols that are not explicitly
permitted. permit ipv6 any any interface <int> ipv6 traffic-filter determine_protocols in
```

必要なプロトコルに加え、ACL が保護する対象のインフラストラクチャ アドレス空間も識別しなければなりません。インフラストラクチャ アドレス空間には、内部ネットワークで使用され、外部送信元はほとんどアクセスすることのないアドレスがすべて含まれます（たとえば、ルータ インターフェイス、ポイントツーポイント リンク アドレッシング、重要なインフラストラクチャ サービスなど）。これらのアドレスは、インフラストラクチャ ACL の宛先部分として使用されるため、要約が重要です。可能であれば、これらのアドレスをクラスレス ドメイン間ルーティング（CIDR）ブロックにグループ化してください。

識別されたプロトコルとアドレスを使用すると、インフラストラクチャ ACL を作成して、これらのプロトコルを許可しアドレスを保護できるようになります。ACL は直接的な保護手段になるだけでなく、インターネット上の特定タイプの無効なトラフィックに対する防御の最前線にもなります。

- RFC 1918 空間は拒否する必要があります。
- RFC 3330 で定義されているような特殊用途のアドレス空間の範疇にある発信元アドレスを持つパケットは拒否する必要があります。
- アンチスプーフィング フィルタを適用しなければなりません。（自分のアドレス空間が、AS 外部からのパケットの送信元になることは許されない事態です）。

この新しく作成した ACL を、すべての入力インターフェイスでの着信に適用する必要があります。詳細については、導入ガイドラインおよび導入例に関するセクションを参照してください。



ACLS と断片化パケット

ACLに特殊な**フラグメント化されたパケット処理の動作をイネーブルにするfragmentsキーワードがあります。**この **fragments キーワードが指定されていない場合、（レイヤ 4 の情報とは関係なく）ACL のレイヤ 3 ステートメントと一致する非先頭フラグメントには、一致したエントリの permit または deny 文が適用されます。**ただし、**fragments キーワードを追加すれば、非先頭フラグメントの拒否または許可を ACL により細かく制御させられます。**この動作は、IPv4 アクセス リストと IPv6 アクセス リストの両方で同じです。ただし唯一の例外として、IPv4 ACL では fragments キーワードをレイヤ 3 およびレイヤ 4 ステートメントで使用できるのに対し、IPv6 ACL では fragments キーワードをレイヤ 3 ステートメントでしか使用できません。

フラグメントをフィルタリングすると、非先頭フラグメント（つまり、FO > 0）を使用するサービス妨害（DoS）攻撃に対するもう 1 つの保護層が追加されます。 非先頭フラグメントに対して ACL の先頭で deny 文を使用すると、すべての非先頭フラグメントのルータへの着信を拒否します。特殊な環境下では、断片化を必要とする有効なセッションが、ACL に **deny fragment 文があるためにフィルタリングされる場合があります。**

例として、次の IPv4ACL の抜粋を検討します。

```
access-list 110 deny tcp any infrastructure_IP fragments
access-list 110 deny udp any infrastructure_IP fragments
access-list 110 deny icmp any infrastructure_IP fragments
<rest of ACL>
```

上記のエントリを ACL の先頭に追加すると、コア ルータへの非先頭フラグメントのアクセスは拒否されますが、断片化されていないパケットまたは先頭フラグメントは **deny fragment 文の影響を受けずに ACL の次の行に渡されます。**前述の ACL コマンドは、各プロトコル (Universal Datagram Protocol (UDP) 、TCP、および ICMP) が ACL の別個のカウンタを増分させることから、攻撃を分類しやすくします。

以下に、上記の例に相当する IPv6 の例を示します。

```
ipv6 access-list iacl
   deny ipv6 any infrastructure_IP fragments
```

上記のエントリを IPv6 ACL の先頭に追加すると、ACL により非先頭フラグメントはコア ルータにアクセスできなくなります。前述のとおり、IPv6 アクセス リストでは fragments キーワードをレイヤ 3 ステートメントでしか使用できません。

攻撃の多くは、断片化パケットによってコア ルータをフラッディングさせることに依存しているため、コア インフラストラクチャ宛てに着信するフラグメントをフィルタリングすることにより、保護手段が追加され、単にインフラストラクチャ ACL のレイヤ 3 ルールと照合するだけでフラグメントを送信する攻撃が阻止されます。

この方法の詳細な説明については、「アクセス コントロール リストと IP 断片化」を参照してください。

リスク評価

インフラストラクチャ保護 ACL を導入する際は、次の 2 つ領域の主要なリスクについて検討してください。

- 適切な許可/**拒否ステートメントが設定されていることを確認します。**ACL を有効にするには、必要なすべてのプロトコルを許可し、正しいアドレス空間を **deny 文で保護する必要があります。**
- ACLパフォーマンスはプラットフォームによって異なります。ACL を導入する前に、ハードウェアのパフォーマンス特性を確認してください。

いつものことながら、導入する前に、この設計をラボでテストすることが推奨されます。

付録

Cisco IOS ソフトウェアでサポートされている IP プロトコル

Cisco IOS ソフトウェアでサポートされている IP プロトコルは、次のとおりです。

- 1 – ICMP
- 2 – IGMP
- 3 – GGP

- 4 – IP-in-IP カプセル化
- 6 – TCP
- 8 – EGP
- 9 – IGRP
- 17 – UDP
- 20 – HMP
- 27 – RDP
- 41:IPv6のIPv4トンネリング
- 46 – RSVP
- 47 – GRE
- 50 – ESP
- 51 – AH
- 53 – SWIPE
- 54 – NARP
- 55 – IP モビリティ
- 63 – 任意のローカル ネットワーク
- 77 – Sun ND
- 80 – ISO IP
- 88 – EIGRP
- 89 – OSPF
- 90 – Sprite RPC
- 91 – LARP
- 94:KA9Q/NOS互換IP over IP
- 103 – PIM
- 108 – IP 圧縮
- 112 – VRRP
- 113 – PGM
- 115:L2TP
- 120 – UTI
- 132 – SCTP

導入ガイドライン

シスコは控えめな導入プラクティスを推奨します。インフラストラクチャ ACL の導入を成功させるには、必要なプロトコルについて十分に理解し、アドレス空間を明確に識別し、定義する必要があります。以降のガイドラインで、反復的な方法を使用して保護 ACL を導入する非常に保守的な方法について説明します。

1. **分類ACLネットワークで使用されるプロトコルを指定します。**インフラストラクチャ デバイスにアクセスすることが既知のすべてのプロトコルを許可する ACL を導入します。このディスカバリ ACL には、発信元アドレスとして **any を指定し、インフラストラクチャの IP 空間を包含する宛先を指定します。**ロギングを使用して、プロトコルの **permit 文と一致する発信元アドレスのリストを作成できます。**トラフィック フローを許可するために、最後の行では **ip any any（IPv4）または ipv6 any any（IPv6）を許可する必要があります。**目標は、特定のネットワークで使用しているプロトコルを判別することです。ロギングを分析に使用して、ルータと通信しているその他すべてのものを特定します。**注：logキーワード**は、ACLヒットの詳細に関する有益な情報を提供しますが、このキーワードを使用するACLエントリへの過剰なヒットは、ログエントリの数が多くなり、ルータのCPU使用率が高くなる可

能性があります。また、**log キーワードを使用すると、アクセス リスト ステートメントに一致するパケットの Cisco Express Forwarding（CEF）スイッチングが無効になります。**これらのパケットは、代わりにファースト スイッチングされます。log キーワードの使用は短時間にとどめ、トラフィックの分類に必要な場合にのみ使用するようにしてください。

2. **判別したパケットをよく調べ、ルート プロセッサ RP へのアクセスのフィルタリングを開始します。**ステップ 1 で ACL によってフィルタリングされたパケットの判別と検査が終ったら、permit any source という指定を含む ACL を、許可されたプロトコルについてインフラストラクチャ アドレスに配備します。ステップ 1 と同様に、**log キーワードを使用すると、permit エントリに一致するパケットに関する詳細情報を取得できます。**最後に deny any を使用すると、ルータ宛てに送られた予期しないパケットの判別に役立てることができます。この ACL の最後の行は、**permit ip any any（IPv4）または permit ipv6 any any（IPv6）という文にして、通過トラフィックのフローを許可するようにする必要があります。**この ACL によって基本的な保護手段が講じられ、ネットワーク エンジニアは、必要なトラフィックがすべて許可されていることを確認できます。
3. **発信元アドレスを制限します。**許可する必要のあるプロトコルが明らかになったら、さらにフィルタリングを実行して、それらのプロトコルについて承認された発信元だけを許可できます。たとえば、外部 BGP ネイバーまたは特定の GRE ピア アドレスを明示的に許可できます。このステップにより、サービスを停止させずにリスクを軽減でき、また、インフラストラクチャ機器にアクセスする発信元を細かく制御できるようになります。
4. **ACLの宛先アドレスを制限します(オプション)。**インターネット サービス プロバイダー（ISP）によっては、ルータ上で特定のプロトコルによる特定の宛先アドレスの使用を許可することが必要になります。この最後の段階では、あるプロトコルのトラフィックの受け入れを許可する宛先アドレスの範囲を制限します。

導入例

IPv4 の例

以下の IPv4 の例では、次のアドレスに基づいて、ルータを保護するインフラストラクチャ ACL を示しています。

- ISP のアドレス ブロックは、169.223.0.0/16 です。
- ISP のインフラストラクチャ ブロックは、169.223.252.0/22 です。
- ルータのループバックは 169.223.253.1/32 です。
- このルータはピアリング ルータであり、169.254.254.1 とピア関係を結んでいます（アドレス 169.223.252.1）。

以下に記載するインフラストラクチャ保護 ACL は、前述の情報に基づいて作成されています。この ACL では、外部ピアに対する外部 BGP ピアリングを許可し、アンチスプーフィング フィルタリングを実行し、インフラストラクチャを外部アクセスから保護しています。

```
!
no access-list 110
!
! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 – Anti-spoofing Denies !--- These ACEs deny fragments, RFC 1918 space, !--- invalid
source addresses, and spoofs of !--- internal space (space as an external source).

!
!--- Deny fragments to the infrastructure block. access-list 110 deny tcp any 169.223.252.0
0.0.3.255 fragments access-list 110 deny udp any 169.223.252.0 0.0.3.255 fragments access-list
```

```
110 deny icmp any 169.223.252.0 0.0.3.255 fragments !--- Deny special-use address sources. !---
See RFC 3330 for additional special-use addresses. access-list 110 deny ip host 0.0.0.0 any
access-list 110 deny ip 127.0.0.0 0.255.255.255 any access-list 110 deny ip 192.0.2.0 0.0.0.255
any access-list 110 deny ip 224.0.0.0 31.255.255.255 any !--- Filter RFC 1918 space. access-list
110 deny ip 10.0.0.0 0.255.255.255 any access-list 110 deny ip 172.16.0.0 0.15.255.255 any
access-list 110 deny ip 192.168.0.0 0.0.255.255 any !--- Deny our internal space as an external
source. !--- This is only deployed at the AS edge access-list 110 deny ip 169.223.0.0
0.0.255.255 any !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 2 - Explicit Permit !--
- Permit only applications/protocols whose destination !--- address is part of the
infrastructure IP block. !--- The source of the traffic should be known and authorized.

!
!--- Note: This template must be tuned to the network's !--- specific source address
environment. Variables in !--- the template need to be changed.

!--- Permit external BGP. access-list 110 permit tcp host 169.254.254.1 host 169.223.252.1 eq
bgp access-list 110 permit tcp host 169.254.254.1 eq bgp host 169.223.252.1 !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 - Explicit Deny to
Protect Infrastructure

access-list 110 deny ip any 169.223.252.0 0.0.3.255
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 4 - Explicit Permit for Transit Traffic

access-list 110 permit ip any any
```

IPv6 の例

以下の IPv6 の例では、次のアドレスに基づいて、ルータを保護するインフラストラクチャ ACL を示しています。

- ISP に割り当てられているプレフィックス ブロック全体は、2001:0DB8::/32 です。
- ISP がネットワーク インフラストラクチャ アドレスに使用している IPv6 プレフィックス ブロックは、2001:0DB8:C18::/48 です。
- 宛先 IPv6 アドレス 2001:0DB8:C19:2:1::F とピアになった発信元 IPv6 アドレス 2001:0DB8:C18:2:1::1 の BGP ピアリング ルータがあります。

以下に記載するインフラストラクチャ保護 ACL は、前述の情報に基づいて作成されています。この ACL では、外部ピアに対する外部マルチプロトコル BGP ピアリングを許可し、アンチスプーフィング フィルタリングを実行し、インフラストラクチャを外部アクセスから保護しています。

```
no ipv6 access-list iacl
ipv6 access-list iacl
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 - Anti-spoofing and Fragmentation Denies !--- These ACEs deny fragments and spoofs
of !--- internal space as an external source. !--- Deny fragments to the infrastructure block.
deny ipv6 any 2001:0DB8:C18::/48 fragments !--- Deny our internal space as an external source.
!--- This is only deployed at the AS edge. deny ipv6 2001:0DB8::/32 any
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 2 - Explicit Permit !--- Permit only
applications/protocols whose destination !--- address is part of the infrastructure IP block. !-
-- The source of the traffic should be known and authorized. !--- Note: This template must be
tuned to the !--- specific source address environment of the network. Variables in !--- the
template need to be changed. !--- Permit multiprotocol BGP. permit tcp host 2001:0DB8:C19:2:1::F
host 2001:0DB8:C18:2:1::1 eq bgp permit tcp host 2001:0DB8:C19:2:1::F eq bgp host
2001:0DB8:C18:2:1::1 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 -
Explicit Deny to Protect Infrastructure deny ipv6 any 2001:0DB8:C18::/48
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 4 - Explicit Permit for
Transit Traffic permit ipv6 any any
```

関連情報

- アクセス リストに関するサポートページ
- Requests for Comments (RFCs)
- テクニカル サポートとドキュメント – Cisco Systems