GSR：受信アクセスコントロールリスト

内容

はじめに

この文書では、receive access control list（rACL; 受信アクセス コントロール リスト）1 と呼ばれる新しいセキュリティ機能について説明し、rACL の配備に関する推奨事項およびガイドラインを紹介します。受信 ACL は、弊害を含む可能性のある不必要なトラフィックからルータの Gigabit Route Processor（GRP; ギガビット ルート プロセッサ）を保護することにより、Cisco 12000 ルータのセキュリティを強化するために使用されます。受信 ACL は、Cisco IOS ® ソフトウェア リリース 12.0.21S2 では特別なメンテナンスとして追加されていましたが、Cisco IOS ソフトウェア リリース 12.0(22)S に統合されました。

GRP保護

Gigabit Switch Router（GSR；ギガビットスイッチルータ）で受信されるデータは、大きく2つのカテゴリに分類できます。

- 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.
- さらに分析するために、受信パスを介してGRPに送信する必要があるトラフィック。

通常の運用では、トラフィックの大部分は他の宛先へのルートでGSRを通過するだけです。ただし、GRPは特定のタイプのデータ(特にルーティングプロトコル、リモートルータアクセス、およびネットワーク管理トラフィック（Simple Network Management Protocol [SNMP]など）など)を処理する必要があります。このトラフィックに加えて、他のレイヤ3パケットではGRPの処理の柔軟性が必要になる場合があります。これには、特定の IP オプションや、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）パケットの特定の形式な

どが含まれますrACL に関するその他の詳細や、GSR での受信パスのトラフィックについては、「受信隣接関係とパケットのパント」の付録を参照してください。

GSRには複数のデータパスがあり、それぞれが異なる形式のトラフィックにサービスを提供します。通過トラフィックは、着信 line card (LC; ラインカード) からファブリックに転送され、その後、ネクストホップへ送出するために、出力カードへ転送されます。トランジットトラフィックのデータパスに加えて、GSRには、ローカル処理を必要とするトラフィック用に、LCからLCへのCPUと、LCからLCへのCPUからファブリックからGRPという2つのパスがあります。次の表では、一般的に使用される機能とプロトコルに対するパスを示しています。

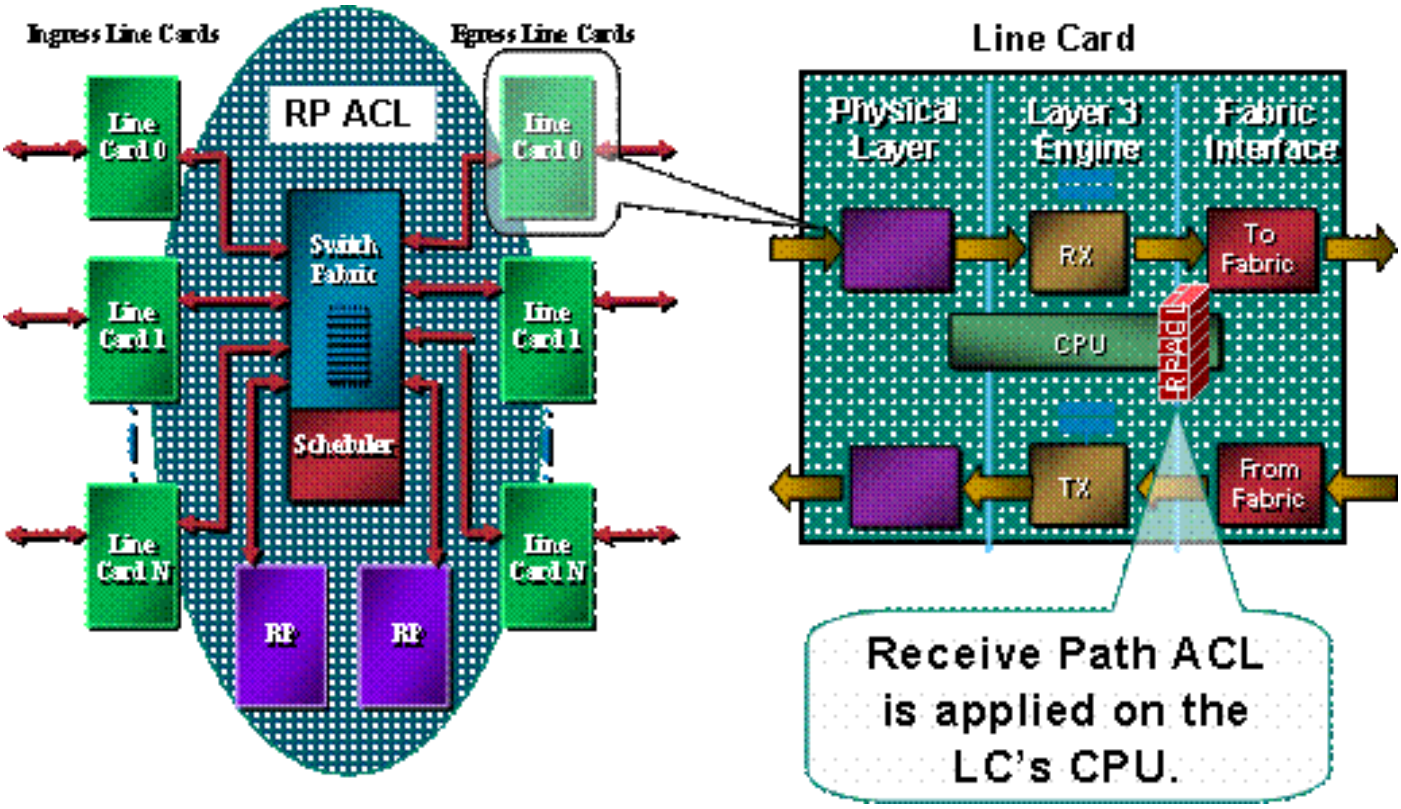
トラフィック タイプ	データパス
通常 (中継) トラフィック	LCからファブリックからLC
ルーティング プロトコル /SSH/SNMP	LCからLC、CPUからファブリックからGRP
ICMPエコー(ping)	LCからLCへのCPU
Logging	

GSR 用のルート プロセッサには、LC から GRP 自体に宛てて送られたトラフィックを処理する容量に限界があります。大量のデータをGRPにパントする必要がある場合は、そのトラフィックがGRPを圧迫する可能性があります。その結果、効果的なサービス拒否(DoS)攻撃が発生します。GRPのCPUでは、パケットの検査についていくのに苦労し、パケットの廃棄が始まり、入力保留キューと選択パケット廃棄(SPD)キューがフラッディングします。[2] GSRは、ルータのGRPに対するDoS攻撃によって発生する可能性がある3つのシナリオに対して保護する必要があります。

- 通常の優先順位のフラッディングによるルーティング プロトコル パケットの喪失
- 通常の優先順位のフラッドによる管理セッション(Telnet、Secure Shell [SSH]、SNMP)のパケット損失
- スプーフィングされた高優先順位のフラッディングによるパケットの喪失

通常の優先順位のフラッディングの際に発生し得るルーティング プロトコルのデータ喪失は、現在はスタティックな分類と、LC から GRP に送られるトラフィックにレート制限をかけることによって緩和されています。しかし、残念ながらこの方法には限界があります。GRP 宛ての通常の優先順位のトラフィックに対するレート制限では、複数の LC 経由での攻撃があった場合の、高優先順位のルーティング プロトコル データの保護には不十分です。このような保護を提供するために、通常の優先順位のデータが廃棄されるしきい値を下げても、通常の優先順位のフラッドによる管理トラフィックの損失が悪化するだけです。

次の図に示すように、rACLは、パケットがGRPに送信される前に各LCで実行されます。



GRPの保護メカニズムが必要です。rACLは、受信隣接関係のためにGRPに送信されるトラフィックに影響を与えます。受信隣接関係とは、ルータのIPアドレスを宛先とするトラフィックのCisco Express Forwarding(CEF)隣接関係のことです。ブロードキャストアドレスや、ルータのインターフェイスで設定されたアドレスなどがあります。[3] 受信隣接関係とパントされたパケットの詳細については、「付録」の項を参照してください。

LCに入るトラフィックは、最初にLCのローカルCPUに送信され、GRPによる処理が必要なパケットはルートプロセッサに転送するためにキューイングされます。受信 ACL は GRP 上で作成され、さまざまな LC の CPU に送出されます。トラフィックがLC CPUからGRPに送信される前に、トラフィックがrACLと比較されます。許可されている場合、トラフィックはGRPに渡されますが、他のすべてのトラフィックは拒否されます。LC から GRP へのレート制限機能よりも先に、rACL が調べられます。rACL はすべての受信隣接関係に対して使用されるので、LC の CPU によって処理される一部のパケット（エコー要求など）も rACL フィルタリングの対象になります。rACL のエントリを決める際には、この点を考慮する必要があります。

受信 ACL は、ルータ内のリソースを保護する方式のさまざまな部分で構成されるプログラムの一部分です。将来の作業には、rACLへのレート制限コンポーネントが含まれます。

パフォーマンスへの影響

単一のコンフィギュレーションエントリと定義されたアクセスリスト自体を保持するために必要なメモリ以外は消費されません。rACL は各 LC にコピーされますが、各 LC では、ごくわずかなメモリが使用されるだけです。特に rACL を配備することによって得られるメリットと比較すると、全体として、使用するリソースはきわめて少ないものです。

受信ACLは、転送されるトラフィックのパフォーマンスには影響しません。rACLは、受信隣接関係トラフィックにのみ適用されます。転送されたトラフィックはrACLの対象になりません。通過

トラフィックをフィルタリングするのは、インターフェイス ACL です。これらの「通常の」ACLは、指定された方向でインターフェイスに適用されます。トラフィックはrACL処理よりも先にACL処理の対象になるため、インターフェイスACLによって拒否されたトラフィックはrACLによって受信されません。[4]

実際にフィルタリングを実行する LC (言い換えれば、rACL でフィルタされるトラフィックを受信する LC) では、rACL の処理により、CPU の使用率が上がります。ただし、このCPU使用率の増加は、GRP宛ての大量のトラフィックによって引き起こされます。rACL保護によるGRPの利点は、LCでのCPU使用率の増加をはるかに上回っています。LC での CPU 利用率は、LC エンジンのタイプによって異なります。たとえば、同じ攻撃を受けた場合、エンジン3のLCのCPU使用率はエンジン0のLCよりも低くなります。

ターボACLをイネーブルにすると(access-list compiledコマンドを使用)、ACLが非常に効率的なルックアップテーブルエントリのシリーズに変換されます。ターボ ACL を有効にすると、rACL の深さによりパフォーマンスが影響を受けることがなくなります。つまり、処理速度はACLのエントリ数に依存しません。rACLが短い場合、ターボACLはパフォーマンスを大幅に向上させませんが、メモリを消費します。rACLが短い場合、コンパイルされたACLは必要ない可能性が高くなります。

rACLはGRPを保護することで、攻撃中のルータと最終的にはネットワークの安定性を確保します。前述のように、rACLはLCのCPUで処理されるため、ルータに大量のデータが向けられると、各LCのCPU使用率が増加します。E0/E1および一部のE2バンドルでは、CPU使用率が100 %を超えると、ルーティングプロトコルとリンクレイヤのドロップが発生する可能性があります。このような廃棄はカードだけに限定され、GRP のルーティング プロセスは保護されるため、安定性は維持されます。スロットリングが有効なマイクロコード[5]が搭載されたE2カードは、負荷が高いときにスロットリングモードをアクティブにし、優先順位6および7のトラフィックのみをルーティングプロトコルに転送します。他のエンジンタイプにはマルチキューアーキテクチャがあります。たとえば、E3カードにはCPUへのキューが3つあり、ルーティングプロトコルパケット (優先順位6/7) は個別の高優先度キューにあります。LCのCPU使用率が高い場合は、優先順位の高いパケットが原因でない限り、ルーティングプロトコルの廃棄は発生しません。低優先キューに送られたパケットには、テール ドロップが適用されます。最後に、E4ベースのカードにはCPUへの8つのキューがあり、1つはルーティングプロトコルパケット専用です。

構文

rACLをルータの各LCに配布するために、次のグローバルコンフィギュレーションコマンドを使用して受信ACLが適用されます。

<#root>

[no] ip receive access-list

この構文では、<num>は次のように定義されます。

```
<1-199> IP access list (standard or extended)
<1300-2699> IP expanded access list (standard or extended)
```

基本的なテンプレートとACLの例

このコマンドを使用できるようにするには、ルータとの対話を許可するトラフィックを識別するアクセスリストを定義する必要があります。アクセスリストには、ルーティング プロトコルと管理トラフィック（Border Gateway Protocol（BGP; ボーダーゲートウェイ プロトコル）、Open Shortest Path First（OSPF）、SNMP、SSH、Telnet）の両方を含める必要があります。詳細については、「配備のためのガイドライン」のセクションを参照してください。

次に示す ACL のサンプルでは、簡単なアウトラインを提供し、特定用途に応用できる設定例を紹介しています。また、この ACL では、一般的に必要とされるいくつかのサービスやプロトコルのために必要な設定を説明しています。SSH、Telnet、およびSNMPの場合、宛先としてループバックアドレスが使用されます。ルーティングプロトコルでは、実際のインターフェイスアドレスが使用されます。rACL で使用するルータ インターフェイスの選択は、ローカル サイトのポリシーと運用によって決定します。たとえば、すべてのBGPピアリングセッションにループバックが使用される場合、BGPのpermit文で許可する必要があるのは、そのループバックだけです。

```
!--- Permit BGP.

access-list 110 permit tcp host bgp_peer host loopback eq bgp

!--- Permit OSPF.

access-list 110 permit ospf host ospf_neighbor host 224.0.0.5

!--- Permit designated router multicast address, if needed.

access-list 110 permit ospf host ospf_neighbor host 224.0.0.6
access-list 110 permit ospf host ospf_neighbor host local_ip

!--- Permit Enhanced Interior Gateway Routing Protocol (EIGRP).

access-list 110 permit eigrp host eigrp_neighbor host 224.0.0.10
access-list 110 permit eigrp host eigrp_neighbor host local_ip

!--- Permit remote access by Telnet and SSH.

access-list 110 permit tcp management_addresses host loopback eq 22
access-list 110 permit tcp management_addresses host loopback eq telnet

!--- Permit SNMP.

access-list 110 permit udp host NMS_stations host loopback eq snmp

!--- Permit Network Time Protocol (NTP).
```

```
access-list 110 permit udp host ntp_server host loopback eq ntp

!--- Router-originated traceroute: !--- Each hop returns a message that time to live (ttl) !--- has bee

access-list 110 permit icmp any any ttl-exceeded
access-list 110 permit icmp any any port-unreachable

!--- Permit TACACS for router authentication.

access-list 110 permit tcp host tacacs_server router_src established

!--- Permit RADIUS.

access-list 110 permit udp host radius_server router_src log

!--- Permit FTP for IOS upgrades.

access-list 110 permit tcp host image_server eq ftp host router_ip_address
access-list 110 permit tcp host image_sever eq ftp-data host router_ip_address
```

すべてのCisco ACLと同様に、アクセスリストの最後には暗黙のdenyステートメントが存在するため、ACLのエントリに一致しないトラフィックはすべて拒否されます。

注：logキーワードは、許可されていないGRP宛てのトラフィックを分類するのに役立ちます。log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、このキーワードを使用したACLエントリへのヒット数が多すぎると、LCのCPU使用率が増加します。ロギングに関連するパフォーマンスへの影響は、LC エンジンのタイプによって異なります。一般的に、ロギングはエンジン0/1/2で必要な場合にのみ使用する必要があります。エンジン3/4/4+では、CPUパフォーマンスの向上とマルチキューアーキテクチャにより、ロギングによる影響ははるかに小さくなります。

アクセスリストの詳細さのレベルは、ローカルのセキュリティ ポリシーによって決定します（たとえば、OSPF 隣接ルータに必要なフィルタリングのレベルなど）。

rACLS 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。一般に、ACL内のL3ステートメント（L4情報とは無関係）に一致する先頭以外のフラグメントは、一致したエントリのpermitまたはdenyステートメントの影響を受けます。fragmentsキーワードを使用すると、ACLによる先頭以外のフラグメントの拒否または許可をより詳細に制御できます。

rACLのコンテキストでは、フラグメントをフィルタリングすることにより、先頭以外のフラグメント（FO > 0など）だけを使用するDoS攻撃に対する保護が追加されます。rACL の先頭で非先頭フラグメントに対する 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が拒否されます。特殊な環境下では、有効なセッションに断片化が必要とされています、rACL に deny fragment 文があると、これがフィルタされてしまう場合があります。

たとえば、次に示すACLの一部を取り上げます。

<#root>

```
access-list 110 deny tcp any any fragments
access-list 110 deny udp any any fragments
access-list 110 deny icmp any any fragments

<rest of ACL>
```

これらのエントリをrACLの先頭に追加すると、すべての非先頭フラグメントのGRPへのアクセスが拒否されますが、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rACLの次の行に渡されます。上記のrACLのスニペットでは、各プロトコル(Universal Datagram Protocol(UDP)、TCP、およびICMP)がACLの個別のカウンタを増分するため、攻撃の分類も容易になります。

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

rACLが、ルーティングプロトコルやルータへのインタラクティブアクセスなどの重要なトラフィックをフィルタリングしないことを確認します。必要なトラフィックをフィルタリングすると、ルータにリモートアクセスできなくなり、コンソール接続が必要になる可能性があります。このため、ラボの設定は、可能な限り実際の導入に近い設定にする必要があります。

シスコでは、通常どおり、導入前にラボでこの機能をテストすることを推奨しています。

付録と注意事項

受信隣接関係とパケットのパント

このドキュメントで前述したように、一部のパケットにはGRP処理が必要です。これらのパケットは、データ転送プレーンから GRP へパントされます。これは、GRPアクセスを必要とするレイヤ3データの一般的な形式のリストです。

- ルーティング プロトコル
- マルチキャスト制御トラフィック（OSPF、Hot Standby Router Protocol [HSRP]、Tag Distribution Protocol [TDP]、Protocol Independent Multicast [PIM]など）
- フラグメンテーションが必要なマルチプロトコルラベルスイッチング(MPLS)パケット
- ルータのアラートなどの IP オプションを持つパケット
- マルチキャストストリームの最初のパケット
- 再構成が必要なフラグメント化ICMPパケット
- ルータ自体を宛先とするすべてのトラフィック（LCで処理されるトラフィックを除く）

rACL は受信隣接関係に適用されるため、rACL は、GRP にパントされない、受信隣接関係のトラフィックをフィルタリングします。最も一般的な例は、ICMP エコー要求（ping）です。ルータ宛てのICMPエコー要求はLC CPUで処理されます。この要求は受信隣接関係であるため、rACLでもフィルタリングされます。したがって、ルータのインターフェイス（またはループバック）への ping を許可するためには、rACL で明示的にエコー要求を許可する必要があります。

受信隣接関係は、show ip cef コマンドで表示できます。

```
<#root>

12000-1#

show ip cef

Prefix              Next Hop            Interface
0.0.0.0/0           drop                Null0 (default route handler entry)
1.1.1.1/32          attached            Null0

2.2.2.2/32          receive

64.0.0.0/30         attached            ATM4/3.300
...
```

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。rACL の配備を成功させるには、既存のコントロール プレーンや管理プレーンのアクセス要件をよく理解する必要があります。一部のネットワークでは、フィルタリングリストの構築に必要な正確なトラフィックプロファイルを特定することが困難な場合があります。以下のガイドラインでは、トラフィックの識別とフィルタリングのための rACL の設定を段階的に行う、rACL の堅実な配備方法を説明します。

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。

   GRPにアクセスするすべての既知のプロトコルを許可するrACLを展開します。この「ディスカバリ」rACLでは、送信元アドレスと宛先アドレスの両方をanyに設定する必要があります。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。プロトコルのpermit文に加えて、rACLの最後にあるpermit any log行を使用すると、rACLによってフィルタリングされる可能性があり、GRPへのアクセスを必要とする可能性がある他のプロトコルを識別できます。

   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、「他に何が」ルータと通信しているかを判断する必要があります。

   注：log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、このキーワードを使用するACLエントリへのヒットが多すぎると、ログのエントリ数が膨大になり、ルータのCPU使用率が高くなる可能性があります。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、GRP 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 の rACL によってフィルタリングされたパケットを判別および検査が終ったら、permit any any 文を含む rACL を、許可されているプロトコルに対して配備します。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 any log を使用すると、GRP 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 rACL では、基本的な保護を行い、ネットワーク エンジニアが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るようになっています。

目的は、発信元と宛先の IP アドレスの範囲を明示的に指定しないで、ルータとの通信に必要なプロトコルの範囲をテストすることです。

3. 発信元アドレスの大きな範囲を制限します。

   割り当てられた classless interdomain routing (CIDR; クラスレス ドメイン間ルーティング) ブロックの範囲全体が、発信元アドレスとして許可されるようにします。たとえば、ネットワークに171.68.0.0/16が割り当てられている場合、171.68.0.0/16からの送信元アドレスだけを許可します。

   このステップにより、サービスを中断することなく、リスクを緩和できます。また、CIDRブロックの外部から機器にアクセスする可能性のあるデバイス/人のデータポイントも提供します。すべての外部アドレスが廃棄される

   セッションに対して許可された送信元アドレスはCIDRブロックの外部にあるため、外部BGP(eBGP)ピアには例外が必要です。

   rACL を絞り込む次のフェーズのためのデータを収集するために、このフェーズで数日間そのままにしておきます。

4. rACLのpermit文を絞り込み、既知の承認済み送信元アドレスだけを許可します。

   送信元アドレスを、GRPと通信する送信元だけを許可するように制限するケースが増えています。

5. rACLの宛先アドレスを制限します(オプション)。

   Internet service provider (ISP; インターネット サービス プロバイダー) 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、あるプロトコルに対するトラフィックを受け入れる宛先アドレスの範囲を制限します。[6]

展開例

次の例では、次のアドレスに基づいて、ルータを保護する受信 ACL を示しています。

- この ISP のアドレス ブロックは、169.223.0.0/16 です。
- この 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。

- このルータはコア バックボーン ルータであるため、内部 BGP セッションだけがアクティブになっています。

この情報から、最初の受信ACLは次の例のようになります。インフラストラクチャ アドレスのブロックが分かっているため、まずブロック全体を許可します。その後、ルータへのアクセスを必要とするすべてのデバイスの特定のアドレスを取得するため、より詳細なアクセスコントロールエントリ(ACE)が追加されます。

<#root>

```
!
no access-list 110
!

!--- This ACL is an explicit permit ACL. !--- The only traffic permitted will be packets that !--- matc

permit

 ACE.

!
! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!---

Phase 1 - Explicit Permit

 !--- Permit only applications whose destination address !--- is the loopback and whose source addresse

!

!---

Note

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

!

!--- Permit BGP.

!
access-list 110 permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq bgp
!

!--- Permit OSPF.

!
access-list 110 permit ospf 169.223.252.0 0.0.3.255 host 224.0.0.5
!

!--- Permit designated router multicast address, if needed.

!
access-list 110 permit ospf 169.223.252.0 0.0.3.255 host 224.0.0.6
access-list 110 permit ospf 169.223.252.0 0.0.3.255 host 169.223.253.1
!

!--- Permit EIGRP.
```

```
!
access-list 110 permit eigrp 169.223.252.0 0.0.3.255 host 224.0.0.10
access-list 110 permit eigrp 169.223.252.0 0.0.3.255 host 169.223.253.1
!

!--- Permit remote access by Telnet and SSH.

!
access-list 110 permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq 22
access-list 110 permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq telnet
!

!--- Permit SNMP.

!
access-list 110 permit udp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq snmp
!

!--- Permit NTP.

!
access-list 110 permit udp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq ntp
!

!--- Router-originated traceroute: !--- Each hop returns a message that ttl !--- has been exceeded (typ

!
access-list 110 permit icmp any 169.223.253.1 ttl-exceeded
access-list 110 permit icmp any 169.223.253.1 port-unreachable
!

!--- Permit TACACS for router authentication.

!
access-list 110 permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 established
!

!--- Permit RADIUS.
!
!
access-list 110 permit udp 169.223.252.0 0.0.3.255 169.223.253.1 log
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!


!--- Phase 2 - Explicit Deny and Reaction

 !--- Add ACEs to stop and track specific packet types !--- that are destined for the router. This is t

!

!--- SQL WORM Example - Watch the rate of this worm. !--- Deny traffic destined to UDP ports 1434 and 1

!
access-list 110 deny udp any any eq 1433
access-list 110 deny udp any any eq 1434
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!---

Phase 3 - Explicit Denies for Tracking
```

```
 !--- Deny all other traffic, but count it for tracking.

!
access-list 110 deny udp any any
access-list 110 deny tcp any any range 0 65535
access-list 110 deny ip any any
```

注意事項

1. DoS への抵抗力を向上するための SPD とホールド キューのガイドラインについては、『選択パケット廃棄（SPD）について』を参照してください。
2. Cisco Express Forwardingと隣接関係の詳細については、『Cisco Express Forwardingの概要』を参照してください。
3. ACLの導入ガイドラインと関連コマンドの詳細については、『Cisco 12000シリーズインターネットルータでのACLの実装』を参照してください。
4. これは、Vanilla、Border Gateway Protocol Policy Accounting（BGPPA）、Per Interface Rate Control（PIRC）、および Frame Relay Traffic Policing（FRTP）のバンドルに言及するものです。
5. 受信パス保護のフェーズ II では、管理インターフェイスの作成と、着信パケットを受信する IP アドレスの自動的な制限などが行えます。

関連情報

- アクセス リストに関するサポートページ
- テクニカルサポート - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。