「 GSR： 受信アクセス コントロール リスト

目次

概要

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

ギガビット スイッチ ルータ （ GSR) によって受け取ったデータは 2 つの広いカテゴリーに分けることができます:

- トラフィック フォワーディングパスでルータを通して通過させる。
- 更なる分析のための GRP にレシーブ パスによって送信 する必要があるトラフィック。

正常な動作では、大部分のトラフィックは他の宛先に GSR を単に途中でフローします。 ただし、GRP はリモートルータ アクセスおよびネットワーク管理トラフィック 特定タイプのデータを、とりわけルーティング プロトコル処理する、必要があります (Simple Network Management Protocol (SNMP) のような[SNMP]) 。 このトラフィックに加えて、他のレイヤ3 パケットは GRP の処理柔軟性を必要とするかもしれません。 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 に各複数のデータパスがトラフィックの保守異なる形式あります。 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 データパスに加えて、GSR にローカル 処理を必要とするトラフィックのための 2 つの他のパスがあります: LC への LC CPU および LC への GRP へのファブリックへの LC CPU。 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。

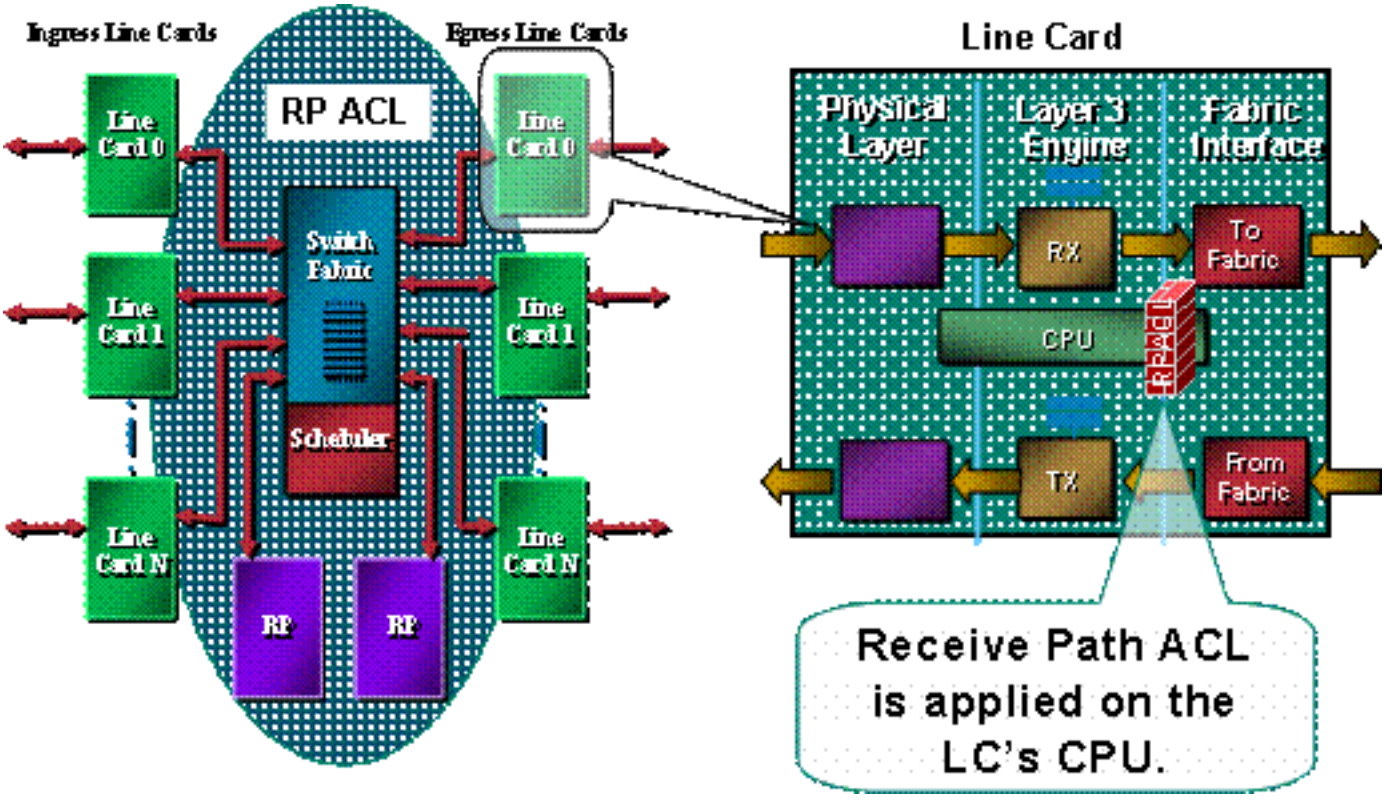
トラフィック タイプ	データパス
正常な (中継) トラフィック	LC へのファブリックへの LC
ルーティング プロトコル /SSH/SNMP	LC への GRP へのファブリックへの LC CPU
ICMPエコー (PING)	LC への LC CPU
ロギング	

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。 データの高いボリュームが GRP にパントを必要とする場合、そのトラフィックは GRP を圧倒できます。 これは有効なサービス拒絶 (DoS) 攻撃という結果に終ります。 GRP の CPU はパケット チェックに遅れずについていくために努力し、パケットを廃棄し始めま入力保持および Selective Packet Discard (SPD; 選択パケット廃棄) キューにあふれます。 [2] GSR はルータの GRP で指示される DoS攻撃に起因する場合がある 3 つのシナリオから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
- normal-priority フラッドからの管理 セッション (Telnet、セキュアシェル[SSH]、SNMP) パケットロス
- 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。 そのような保護を提供するために normal-priority データが廃棄されるしきい値を下げて normal-priority フラッドからのマネジメントトラフィックの損失だけを悪化させます。

このイメージが示すと同時に、rACL は各 LC でパケットが GRP に送信される前に実行されます。



GRP のための保護メカニズムが必要となります。 rACL 影響トラフィック レシーブ 隣接関係が理由で GRP に送信 される。 レシーブ 隣接関係は Cisco Express Forwarding（CEF）ルータのインターフェイスで設定されるブロードキャスト アドレスまたはアドレスのようなルータの IP アドレスに、向かうトラフィックのための隣接関係です。[3] レシーブ 隣接関係およびパントされたパケットの付録 セクションを詳細については参照して下さい。

トラフィックは LC の LC を入力する GRP によって処理を必要とするローカル CPU、およびパケットにルートプロセッサへの転送のために最初に並べられます送信 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、トラフィックは rACL と比較されます。 許可された場合、トラフィックは GRP に他のトラフィックはすべて拒否されるが、通じます。 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。 今後 の 作業は rACL にレートリミット コンポーネントが含まれています。

パフォーマンスへの影響

メモリは単一の設定 エントリおよび定義されたアクセス リスト自体を保持するのに必要なそれ以外消費されません。 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。

Receive ACL は転送されたトラフィックのパフォーマンスに影響を及ぼしません。 rACL はただ隣接関係 トラフィックを受信するために適用します。 転送されたトラフィックは rACL に応じて決してありません。 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「規則的な」ACL は指定された方向のインターフェイスに適用されます。 トラフィックは rACL 処理以前 ACL処理に応じてあります、従ってインターフェイス 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。 しかしこの増大したCPU 利用は GRP に送信されるトラフィックの高いボリューム引き起こされます; rACL 保護の GRP の利点はずっと LC の増大したCPU 利用を上回ります。 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、同じ攻撃を与えられて、エンジン 3 LC にエンジンより低い CPU稼働率が 0 LC あります。

ターボ ACL を有効に することは非常に能率的な一連のルックアップテーブル エントリに (**access-list compiled コマンドの**使用によって) ACL を変換します。 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。 すなわち、処理速度は ACL のエントリの数の依存しないです。 rACL が短い場合、ターボ ACL はパフォーマンスを大幅に向上しませんが、ためにメモリを消費して下さい; 短い rACL を使うと、コンパイルされた ACL は本当らしい必要です。

GRP の保護によって、rACL ヘルプは攻撃の間にルータおよび、最終的に、ネットワーク 安定性を確保します。 上記のように、rACL は LC CPU で処理されます、従って大きいデータ量がルータで指示される場合各 LC の CPU稼働率は増加します。 E0/E1 およびいくつかの E2 バンドルで、100+% の CPU稼働率はルーティング プロトコルおよび link-layer ドロップの原因となるかもしれません。 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。 絞有効に された マイクロコード [5] アクティブ化スロットリング モードでの E2 カード場合のルーティング プロトコルへの重負荷および前方優位だけ 6 および 7 トラフィックの下で。 他のエンジンタイプに複数のキュー アーキテクチャがあります; たとえば、E3 カードにルーティングプロトコルパケット (優位 6/7) との CPU に別途で 3 つのキューが、高優先度キューあります。 高優先度パケットによりそれを引き起こさなければ、高い LC CPU はルーティング プロトコル ドロップという結果に終りません。 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。 最終的には、E4-based カードにルーティングプロトコルパケットに専用されて 1 つが CPU に 8 つのキューが、あります。

構文

Receive ACL はルータの各 LC に rACL を配る次のグローバル 設定 コマンドで適用されます。

[no] ip receive access-list *<num>*
この構文では、*<num> は*次の通り定義されます。

```
<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および ACL 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 に関しては、ループバック アドレスは宛先として使用されます。 ルーティング プロトコルに関しては、実際のインターフェイス アドレスは使用されます。 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。 たとえばループバックがすべての BGP ピアリングセッションのために使用されれば、そして BGP のための**割り当て**文で許可されるそれらのループバック必要だけ。

```
!--- 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 been
exceeded (type 11, code 3); !--- the final destination returns a message that !--- the ICMP port
is unreachable (type 3, code 0). 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、ACL のエントリを否定される一致する アクセス リストの端に暗黙の deny 文が、そうあらゆるトラフィックあります。

注: キーワード log は、許可されていない GRP 宛てのトラフィックを分類するために使用できます。 **log キーワードが** ACL ヒットの詳細にこのキーワードを使用する貴重な洞察を提供するが、ACL項目への余分なヒットは LC CPU稼働率を増加します。 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。 一般に、記録はエンジン 0/1/2 で必要な場合だけだけ使用する必要があります。 エンジン 3/4/4+ に関しては、記録はより少し増大したCPU パフォーマンスおよび複数のキュー アーキテクチャが理由で影響のずっと起因します。

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 には、特化した断片化パケット処理動作を有効にする、**fragments** というキーワードがあります。 一般に、ACL の L3 文を（L4 情報に関係なく）一致する 先頭 以外 の フラグメントは一致されたエントリの**許可**か **Deny ステートメント**から影響を受けます。 **フラグメント** キーワードの使用がより多くの細かさの拒否または割り当て先頭 以外 の フラグメントに ACL を強制できることに注目して下さい。

rACL 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は先頭 以外 の フラグメントだけ使用する DoS攻撃に対して保護の追加層を追加します（のような FO > 0）。 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、下記に示されている部分的な ACL を考慮して下さい。

```
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>
```

rACL の始まりへこれらのエントリを追加することは GRP に非断片化パケットか先頭フラグメントは**拒否フラグメント**文を変化しない rACL の次の行に通るが、先頭 以外 の フラグメント アクセスを拒否します。 上記の rACL 断片はまた各プロトコル以来の攻撃の分類を– Universal Datagram Protocol （ UDP ）、TCP および ICMP –増分分けます ACL のカウンターを促進します。

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 がルータにルーティング プロトコルまたはインタラクティブアクセスのような極めて重要なトラフィックをフィルタリングしないようにして下さい。 従って必要なトラフィックをフィルタリングすることはルータにリモートアクセスする不可能という結果に終る可能性がありまコンソール接続を必要とします。 従って、ラボ コンフィギュレーションは実際の配備をできるだけ密接にまねる必要があります。

常にとして、Cisco は配備前にラボのこの機能をテストすることを推奨します。

付録およびメモ

受信隣接関係とパケットのパント

先にこの資料に説明があられるように、いくつかのパケットは GRP処理を必要とします。 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。 これはレイヤ3 データのよくあるフォームのリストです GRP アクセスを必要とする。

- 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、ホットスタンバイ ルータ プロトコル[HSRP]、タグ配布プロトコル[TDP]、Protocol Independent Multicast [PIM]、およびそのような物 ）
- フラグメンテーションを必要とするマルチプロトコル 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 ストリームの最初パケット
- 再組立てを必要とするフラグメント化された ICMPパケット
- ルータ自体に向かう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。 ルータへの ICMPエコー要求 誘導は LC CPU によって処理されます; 要求がレシーブ 隣接関係であるので、また rACL によって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。

```
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

シスコでは保守的な導入プラクティスを推奨しています。 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。 いくつかのネットワークでは、フィルタリング リストを作成するのに必要とされる正確なトラフィック プロファイルを判別することは困難であるかもしれません。 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 を使用して、ネットワークで使用されているプロトコルを識別する。**その rACL を割り当て GRP にアクセスするすべての既知のプロトコル展開して下さい。 この" discovery " rACL は設定 されるへの両方の送信元 および 宛先アドレスがあるはずです。 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**割り当て**文に加えて、**割り当てが** rACL の終わりに**あらゆるあらゆる測程線**フィルタリングされる rACL によって GRP にアクセスを必要とし、他のプロトコルを確認するのに使用することができます。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。 」ルータと伝えるかもしれませんか他に何を「判別するのに分析にロギングが使用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した ACL エントリとのヒット数が多すぎると、ログのエントリ数が大量になりルータの CPU 使用率が高くなることがあります。 **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、171.68.0.0/16 ネットワークのための割り当てられたら、そしてちょうど 171.68.0.0/16 からの割り当て送信元アドレス。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。 それはまた機器にアクセスするかもしれない CIDRブロックの外からのデバイス/個人のデータ点を提供します。すべての外部アドレスは廃棄されます。External BGP 同位はセッションのための許可 された ソース ソース・ アドレスが CIDRブロックの外部にあるので、例外を必要とします。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. **認識されていた承認された送信元アドレスしか許可しないために rACL 割り当て文を狭くして下さい。**次第に GRP と通信する割り当て出典だけへの送信元アドレスを制限して下さい。
5. **rACL の宛先アドレスを制限して下さい。((*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]

配備例

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。

この情報を与えられて、最初の Receive ACL は下記の例のよう何かである可能性があります。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。 以降はルータへのアクセスを必要とするすべてのデバイスのために特定 の アドレスとして、より詳しいアクセス制御エントリ（ACE）得られます追加されます。

```
!
no access-list 110
!
!--- This ACL is an explicit permit ACL. !--- The only traffic permitted will be packets that !--- match an explicit permit ACE. ! ! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 1 – Explicit Permit !--- Permit only applications whose destination address !--- is the loopback and whose source addresses !--- come from an valid host. ! !--- Note: This template must be tuned to the network's !--- specific source address environment. Variables in !--- the template need to be changed. ! !--- 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 (type 11, code 3); !--- the final destination returns a message that !--- the ICMP port is unreachable (type 3, code 0). ! 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 the phase !--- where you use ACEs with counters to track and classify attacks. ! !--- SQL WORM Example – Watch the rate of this worm. !--- Deny traffic destined to UDP ports 1434 and 1433. !--- from being sent to the GRP. This is the SQL worm. ! 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（CEF）および隣接関係に関する詳細については、外観を Cisco Express Forwarding（CEF）参照して下さい。
3. のために ACL 配置 の ガイドラインおよび関連のコマンドの詳しい議論は、ACL 12000 シリーズ インターネット ルータを on Cisco 設定することを示します。
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