トランジット アクセス コントロール リスト：エッジでのフィルタリング

目次

はじめに

このドキュメントでは、ネットワークの入口での中継トラフィックとエッジ トラフィックのフィルタリングについて、ガイドラインおよび推奨する展開方法を示します。 アクセス コントロール リスト（ACL）を使用して、ネットワークへの必要なトラフィックのみを明示的に許可して、ネットワークのセキュリティを向上させます。

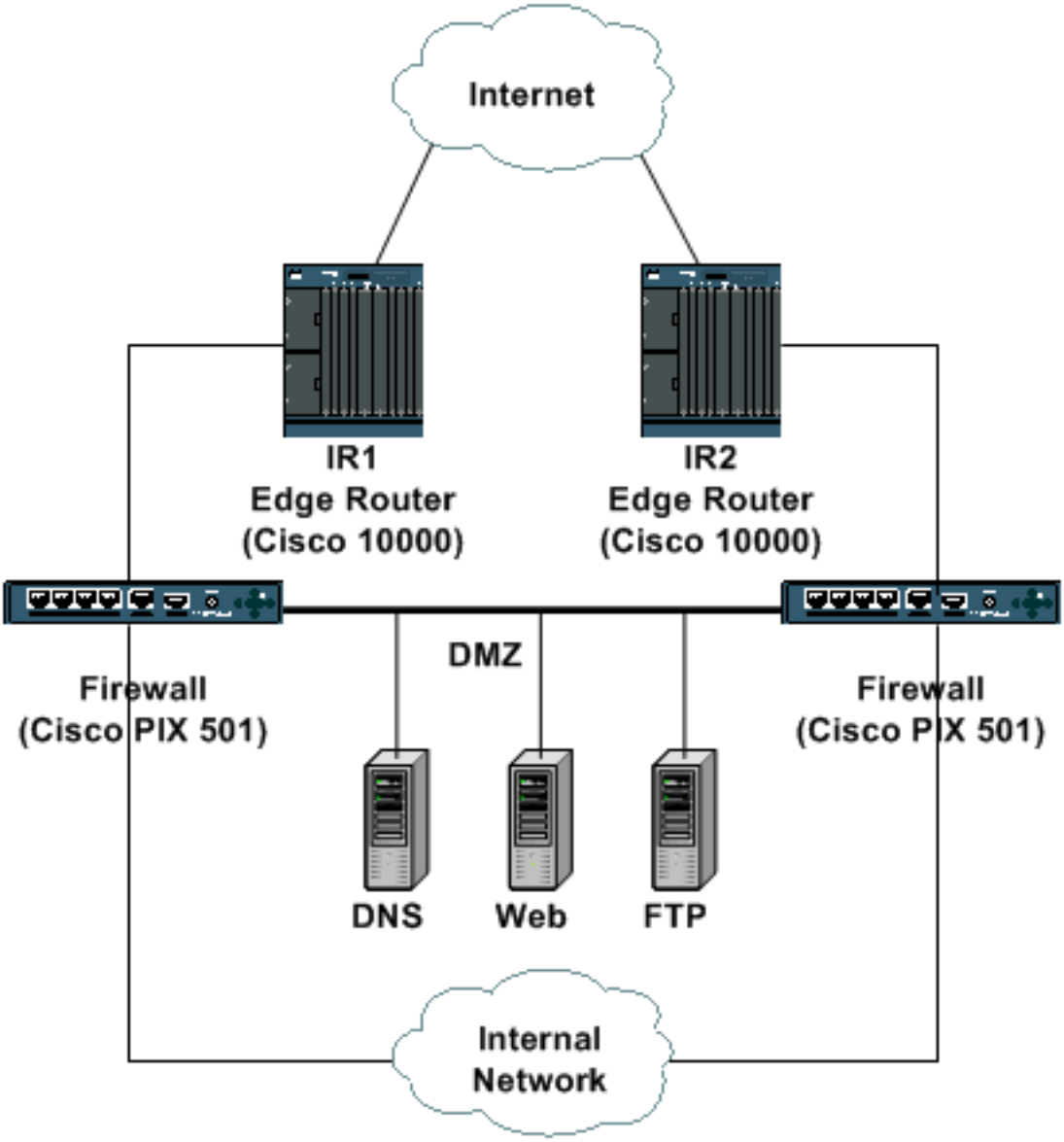
中継フィルタ

一般的なセットアップ

一般的な企業ネットワークのインターネット接続点（Point of Presence）など、大部分のエッジ ネットワーク環境では、入力フィルタリングを使用して無許可トラフィックをネットワークのエッジで廃棄する必要があります。 一部のサービス プロバイダーの展開では、この形式による エッジ トラフィックや中継トラフィックのフィルタリングを効果的に使用して、顧客に出入りする中継トラフィックの流れを特定の許可されたプロトコルだけに制限できます。 この文書では、企業への配備モデルに焦点を絞って説明します。

次の例は、一般的な企業のインターネット接続形態を示しています。 2 台のエッジ ルータ（IR1 と IR2）によってインターネットに直接接続しています。 2 台のルータの背後にある 1 対のファ

イアウォール（この例では Cisco PIX）は、ステートフル インスペクション機能を備えており、内部ネットワークと緩衝地帯（DMZ）の両方へのアクセスを許可します。 DMZ には、DNS や Web などの一般向けサービスが含まれています。 DMZ はパブリック インターネットから直接アクセスできる唯一のネットワークです。 インターネットから内部ネットワークに直接アクセスすることはできませんが、内部ネットワークから送信されたトラフィックはインターネット上のサイトに到達できます。



着信 ACL を使用して一次レベルのセキュリティを確保するように、エッジ ルータを設定する必要があります。 この ACL によって、特別に許可されたトラフィックだけを DMZ にアクセスさせ、インターネットにアクセスしている内部ユーザに返されるリターン トラフィックを許可します。 無許可トラフィックはすべて、入力インターフェイスで廃棄されます。

トランジット ACL のセクション

一般的に、トランジット ACL は次の 4 つのセクションから構成されます。

- 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。ネットワーク内のアドレスを送信元とするパケットや不正な送信元が、外部ソースからネットワーク内に入ることを拒否します。**注:** RFC 1918 では、インターネット上で無効とする発信元アドレスを予約アドレスとして定義しています。 RFC 3330 では、フィルタリングが必要となる可能性のある特定用途ア

ドレスを定義しています。 RFC 2827 では、アンチスプーフィングのガイドラインを提供しています。
- インターネットへの内部接続に対して明示的に許可されたリターン トラフィック
- 保護されている内部アドレスを宛先とする、明示的に許可された外部ソース トラフィック
- 明示的な **deny** 文**注:** すべての ACL には暗黙的な **deny** 文が含まれていますが、明示的な **deny** 文（**deny ip any any** など）を使用することを推奨します。 大部分のプラットフォームでは、拒否されたパケットの数をそのような文によって記録し、**show access-list** コマンドで表示することができます。

トランジット ACL の作成方法

トランジット ACL を作成する第一歩は、自身のネットワークに必要なプロトコルを決定することです。 各サイトには固有の要件がありますが、ある種のプロトコルやアプリケーションは広く使用されており、ほとんどの場合、許可されています。 たとえば、パブリック アクセス可能な Web サーバへの接続を DMZ セグメントによって提供する場合は、ポート 80 でインターネットから DMZ サーバ アドレスへの TCP を使用する必要があります。 同様に、インターネットへの内部接続の場合は、確立された TCP のリターン トラフィック（確認応答（ACK）ビットが設定されているトラフィック）を ACL で許可する必要があります。

必要なプロトコルの識別

必要なプロトコルのリストの作成は大変な作業になることもありますが、必要なトラフィックの識別に役立ついくつかのテクニックを必要に応じて使用できます。

- **ローカルのセキュリティ ポリシー/サービス ポリシーの検討。**ローカル サイトのポリシーは、サービスを許可または拒否する基準を策定する上で役立つものでなければなりません。
- **ファイアウォール設定の検討/監査。**現在のファイアウォール設定に、許可するサービスに対する明示的な **permit** 文を含める必要があります。 多くの場合、この設定を ACL 形式に変換して使用することで、ACL の大部分のエントリを作成できます。**注:** ステートフルなファイアウォールでは通常、認可された接続へのリターン トラフィックに対する明示的なルールは定義されていません。 ルータ ACL はステートフルではないため、リターン トラフィックを明示的に許可する必要があります。
- **使用するアプリケーションの検討/監査。**DMZ にホストされているアプリケーションと内部で使用されるアプリケーションは、フィルタリング要件の決定に役立ちます。 アプリケーションの要件を検討することで、フィルタリングの設計に不可欠な詳細事項を把握できます。
- **分類 ACL の使用。**分類 ACL は、内部ネットワーク宛てに使用される可能性がある各種プロトコル向けの **permit** 文から構成されます（一般的に使用されるプロトコルとアプリケーションのリストについては、「付録 A」を参照）。 **show access-list** コマンドを使用してアクセス コントロール エントリ（ACE）のヒット数を表示すると、必要なプロトコルを識別できます。 疑わしい結果や予期しない結果を調査して把握してから、予想外のプロトコルに対する明示的な **permit** 文を作成してください。
- **Netflow スイッチング機能の使用。**Netflow は一種のスイッチング機能であり、有効にすると詳細なフロー情報を得ることができます。 エッジ ルータで Netflow が有効になっている場合、**show ip cache flow command** を使用すると、Netflow により記録されたプロトコルの一覧が表示されます。 Netflow であらゆるプロトコルを識別できるわけではないので、このテクニックは他のテクニックと組み合わせて使用する必要があります。

無効なトラフィックの識別

直接的に保護することに加え、トランジット ACL は、インターネット上の特定タイプの無効トラフィックに対する防御の最前線としても機能します。

- RFC 1918 空間を拒否。
- RFC 3330 で定義されている特殊用途のアドレス空間に該当する送信元アドレスを持つパケットを拒否。
- RFC 2827 に従って、アンチスプーフィング フィルタを適用。 自身のアドレス空間が自律システム（AS）外部からのパケットの送信元になることは、絶対にありません。

その他の考慮すべきトラフィック タイプは、以下のとおりです。

- **エッジ ルータとの通信に必要な外部プロトコルと IP アドレス**サービス プロバイダーの IP アドレスからの ICMPルーティング プロトコルIPSec VPN（エッジ ルータが終端として使用されている場合）
- **インターネットへの内部接続に対して明示的に許可されたリターン トラフィック**特定タイプのインターネット制御メッセージ プロトコル（ICMP）発信用ドメイン ネーム システム（DNS）クエリーの応答TCP establishedユーザ データグラム プロトコル（UDP）のリターン トラフィックFTP データ接続TFTP データ接続マルチメディア接続
- **保護されている内部アドレスを宛先とする、明示的に許可された外部ソース トラフィック** VPN トラフィックInternet Security Association and Key Management Protocol（ISAKMP）ネットワーク アドレス変換（NAT）トラバーサル独自のカプセル化 Encapsulating Security Payload（ESP）認証ヘッダー（AH）Web サーバに対する HTTPWeb サーバに対するセキュア ソケット レイヤ（SSL）FTP サーバに対する FTP着信 FTP データ接続着信 FTP パッシブ（**pasv**）データ接続SMTP（シンプル メール転送プロトコル）その他のアプリケーションとサーバ着信 DNS クエリー着信 DNS ゾーン転送

ACL の適用

新たに作成した ACL は、エッジ ルータのインターネット接続インターフェイスで着信に適用する必要があります。 「一般的なセットアップ」の項で示した図では、IR1 と IR2 のインターネット接続インターフェイスの「in」に ACL が適用されています。

詳細については、「導入ガイドライン」および「展開例」の項を参照してください。

ACL の例

次のアクセス リストは、トランジット ACL に必要な一般的エントリのシンプルかつ実用的な例を示しています。 この基本的な ACL は、ローカル サイト固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。

```
!--- Add anti-spoofing entries. !--- Deny special-use address sources. !--- Refer to RFC 3330
for additional special use addresses.

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
access-list 110 deny ip host 255.255.255.255 any
!--- The deny statement should not be configured !--- on Dynamic Host Configuration Protocol
(DHCP) relays.
```

```
access-list 110 deny ip host 0.0.0.0 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 !---
Permit Border Gateway Protocol (BGP) to the edge router. access-list 110 permit tcp host
bgp_peer gt 1023 host router_ip eq bgp access-list 110 permit tcp host bgp_peer eq bgp host
router_ip gt 1023 !--- Deny your space as source (as noted in RFC 2827). access-list 110 deny ip
your Internet-routable subnet any !--- Explicitly permit return traffic. !--- Allow specific
ICMP types.

access-list 110 permit icmp any any echo-reply
access-list 110 permit icmp any any unreachable
access-list 110 permit icmp any any time-exceeded
access-list 110 deny   icmp any any
!--- These are outgoing DNS queries. access-list 110 permit udp any eq 53 host primary DNS
server gt 1023 !--- Permit older DNS queries and replies to primary DNS server. access-list 110
permit udp any eq 53 host primary DNS server eq 53 !--- Permit legitimate business traffic.
access-list 110 permit tcp any Internet-routable subnet established access-list 110 permit udp
any range 1 1023 Internet-routable subnet gt 1023 !--- Allow ftp data connections. access-list
110 permit tcp any eq 20 Internet-routable subnet gt 1023 !--- Allow tftp data and multimedia
connections. access-list 110 permit udp any gt 1023 Internet-routable subnet gt 1023 !---
Explicitly permit externally sourced traffic. !--- These are incoming DNS queries.

access-list 110 permit udp any gt 1023 host <primary DNS server> eq 53
 !-- These are zone transfer DNS queries to primary DNS server. access-list 110 permit tcp host
secondary DNS server gt 1023 host primary DNS server eq 53 !--- Permit older DNS zone transfers.
access-list 110 permit tcp host secondary DNS server eq 53 host primary DNS server eq 53 !---
Deny all other DNS traffic. access-list 110 deny udp any any eq 53 access-list 110 deny tcp any
any eq 53 !--- Allow IPSec VPN traffic. access-list 110 permit udp any host IPSec headend device
eq 500 access-list 110 permit udp any host IPSec headend device eq 4500 access-list 110 permit
50 any host IPSec headend device access-list 110 permit 51 any host IPSec headend device access-
list 110 deny ip any host IPSec headend device !--- These are Internet-sourced connections to !-
-- publicly accessible servers. access-list 110 permit tcp any host public web server eq 80
access-list 110 permit tcp any host public web server eq 443 access-list 110 permit tcp any host
public FTP server eq 21 !--- Data connections to the FTP server are allowed !--- by the permit
established ACE. !--- Allow PASV data connections to the FTP server.

access-list 110 permit tcp any gt 1023 host public FTP server gt 1023 access-list 110 permit tcp
any host public SMTP server eq 25 !--- Explicitly deny all other traffic.

access-list 101 deny ip any any
```

注: トランジット ACL を適用する際は、次の推奨事項に留意してください。

- log キーワードを使用すると、所定のプロトコルの送信元と宛先に関する詳細を表示できます。 このキーワードによって ACL のヒットに関する有益な詳細情報を表示できますが、log キーワードを使用している ACL エントリへのヒットが多すぎると、CPU 使用率が増加してしまいます。 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。
- ACL によって管理上拒否されたパケットに対して、ICMP unreachable メッセージが生成されます。 これはルータとリンクのパフォーマンスに影響を与えることがあります。 トランジット (エッジ) ACL を展開するインターフェイスで IP unreachables を無効にするために、no ip unreachables コマンドを使用することを検討してください。
- ビジネス用の正当なトラフィックが拒否されないように、すべてが permit 文から成る ACL を初期展開できます。 その後、ビジネス用の正当なトラフィックを特定して把握してから、特定の deny 要素を設定できます。

ACLS 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。 一般的には、レイヤ 3 文（プロトコル、送信元アドレス、宛先アドレス）に一致した非初期フラグメントは、（ACL 内のレイヤ 4 情報とは関係なく）一致したエントリの **permit** や **deny** 文の影響を受けます。 ただし、**fragments** キーワードを使用することで、ACL による非初期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。

フラグメントをフィルタリングすることにより、非初期フラグメント（FO > 0 など）だけを使用するサービス拒否（DoS）攻撃に対する保護がさらに強化されます。 ACL の先頭で非初期フラグメントに対して **deny** 文を使用すると、すべての非初期フラグメントがルータにアクセスできなくなります。 まれな状況として、有効なセッションが断片化を必要とすることがあり、そのような場合に ACL に **deny fragment** 文があると、そのセッションはフィルタリングされてしまいます。 断片化が必要となる状況としては、ISAKMP 認証にデジタル認証を使用する場合や、IPSec NAT Traversal を使用する場合などがあります。

たとえば、次に示す部分的な ACL について考えてください。

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

これらのエントリを ACL の先頭に追加すると、すべての非初期フラグメントのネットワークへのアクセスが拒否されます。ただし、断片化されていないパケットや初期フラグメントは、**deny fragment** 文の影響を受けずに ACL の次の行に渡されます。 上記の部分的な ACL では、プロトコル（UDP、TCP、ICMP）ごとに ACL で個別のカウンタが増分されるので、攻撃の分類が容易になります。

攻撃の多くは断片化パケットによるフラッディングに依存しているため、内部ネットワーク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、防御を強化できます。また、トランジット 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を阻止できます。

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

中継トラフィックを保護する ACL を展開する際は、リスクに関する次の 2 つの主要事項を考慮してください。

- 適切な **permit/deny** 文が設定されていることを確認します。 ACL を効果的に使用するには、必要なプロトコルすべてを許可する必要があります。
- ACL の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 を展開する前に、使用しているハードウェアのパフォーマンス特性を検討してください。

展開する前にラボでテストすることを推奨します。

付録

一般的に使用されるプロトコルとアプリケーション

TCP のポート名

Cisco IOS® ソフトウェアで ACL を設定する際は、次のリストの TCP ポート名をポート番号の代わりに使用できます。 これらのプロトコルの参考情報については、現在割り当てられている番号の RFC を参照してください。 また、これらのプロトコルに対応するポート番号は、ACL の設定時に ? を ポート番号の代わりに入力することで判明します。

bgp	kshell
chargen	ログイン
cmd	lpd
日中	nntp
廃棄	pim
domain	pop2
echo	pop3
exec	SMTP
finger	sunrpc
ftp	syslog
ftp-data	tacacstalk
gopher	Telnet
ホスト名	時刻
ident	uucp
irc	whois
klogin	www

UDP のポート名

Cisco IOS ソフトウェアで ACL を設定する際は、次のリストの UDP ポート名をポート番号の代わりに使用できます。 これらのプロトコルの参考情報については、現在割り当てられている番号の RFC を参照してください。 また、これらのプロトコルに対応するポート番号は、ACL の設定時に ? を ポート番号の代わりに入力することで判明します。

biff	ntp
bootpc	pim-auto-rp
bootps	RIP
廃棄	snmp
dnsix	snmptrap
domain	sunrpc
echo	syslog
isakmp	tacacs
mobile-ip	トーク
nameserver	tftp
netbios-dgm	時刻
netbios-ns	who
netbios-ss	xdmcp

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。 トランジット ACL を適切に展開するには、必要なプロトコルを明確に把握しておく必要があります。 以降のガイドラインでは、反復的な方法を使用して保護 ACL を展開する非常に保守的な方法について説明します。

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。**ネットワークで使用される既知のプロトコルをすべて許可する ACL を展開します。 このディスカバリまたは分類では、ACL に送信元アドレス **any** と、宛先として IP アドレスまたはインターネット ルーティング可能な IP サブネット全体を設定する必要があります。 **ip any any log** を許可するように最後のエントリを設定すると、許可する必要があるその他のプロトコルの識別に役立ちます。目的は、ネットワークで使用されている必要なプロトコルをすべて特定することです。 分析のロギングを使用して、ルータと通信する可能性があるその他のプロトコルを判別します。**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。すべてが **permit** 文から成る ACL を使用している間は、ネットワークが攻撃のリスクにさらされていることに留意してください。 本来のアクセス制御を実施できるように、分類処理を可能な限り迅速に実行してください。
2. **識別したパケットを検討して、内部ネットワーク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 によりフィルタしたパケットを識別して検討したら、分類 ACL を更新して、新たに識別したプロトコルと IP アドレスを設定します。 アンチスプーフィングに関する ACL エントリを追加します。 必要に応じて、分類 ACL の **permit** 文を特定の **deny** エントリに置き換えます。 **show access-list** コマンドを使用して特定の **deny** エントリをモニタし、ヒット カウントを調べることができます。 この方法を使用すると、ACL エントリのロギングを有効にしなくても、禁止されているネットワーク アクセスの試みについて情報を得ることができます。 ACL の最後の行は、**deny ip any any** にする必要があります。 この最後のエントリに対するヒット カウントを調べることにより、禁止されているアクセスの試みについて情報を得ることができます。
3. **ACL をモニタして更新します。**完成した ACL をモニタして、新たに導入した必要なプロトコルが制御された方法で追加されていることを確認します。 ACL をモニタすることにより、禁止されているネットワーク アクセスの試みについて情報を得ることもできます。このような試みは攻撃の兆候を示していることがあります。

展開例

以下の例は、次のアドレスに基づいてネットワークを保護するトランジット ACL を示しています。

- ISP ルータの IP アドレス：10.1.1.1エッジ ルータのインターネット側の IP アドレス：10.1.1.2インターネット ルーティング可能なサブネット：192.168.201.0 255.255.255.0VPN ヘッドエンドは、192.168.201.100 です。Web サーバのアドレス：192.168.201.101FTP サーバのアドレスは 192.168.201.102 です。SMTP サーバのアドレス：192.168.201.103プライマリ DNS サーバのアドレス：192.168.201.104セカンダリ DNS サーバのアドレス：172.16.201.50

以下に示すトランジット保護 ACL は、これらの情報に基づいて作成されています。 この ACL は、ISP ルータへの eBGP ピアリングの許可、アンチスプーフィング フィルタの提供、特定のリターン トラフィックの許可、特定の着信トラフィックの許可を実施し、その他のトラフィックをすべて明示的に拒否します。

```
no access-list 110
!--- Phase 1 – Add anti-spoofing entries. !--- Deny special-use address sources. !--- See RFC
3330 for additional special-use addresses.

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
access-list 110 deny   ip host 255.255.255.255 any
!--- This deny statement should not be configured !--- on Dynamic Host Configuration Protocol
(DHCP) relays.

access-list 110 deny   ip host 0.0.0.0 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 !---
Permit BGP to the edge router. access-list 110 permit tcp host 10.1.1.1 gt 1023 host 10.1.1.2 eq
bgp access-list 110 permit tcp host 10.1.1.1 eq bgp host 10.1.1.2 gt 1023 !--- Deny your space
as source (as noted in RFC 2827). access-list 110 deny ip 192.168.201.0 0.0.0.255 any !--- Phase
2 – Explicitly permit return traffic. !--- Allow specific ICMP types.

access-list 110 permit icmp any any echo-reply
access-list 110 permit icmp any any unreachable
access-list 110 permit icmp any any time-exceeded
access-list 110 deny   icmp any any
!--- These are outgoing DNS queries. access-list 110 permit udp any eq domain host
192.168.201.104 gt 1023 !--- Permit older DNS queries and replies to primary DNS server. access-
list 110 permit udp any eq domain host 192.168.201.104 eq domain !--- Permit legitimate business
traffic. access-list 110 permit tcp any 192.168.201.0 0.0.0.255 established access-list 110
permit udp any range 1 1023 192.168.201.0 0.0.0.255 gt 1023 !--- Allow FTP data connections.
access-list 110 permit tcp any eq ftp-data 192.168.201.0 0.0.0.255 gt 1023 !--- Allow TFTP data
and multimedia connections. access-list 110 permit udp any gt 1023 192.168.201.0 0.0.0.255 gt
1023 !--- Phase 3 – Explicitly permit externally sourced traffic. !--- These are incoming DNS
queries.

access-list 110 permit udp any gt 1023 host 192.168.201.104 eq domain
!--- Zone transfer DNS queries to primary DNS server. access-list 110 permit tcp host
172.16.201.50 gt 1023 host 192.168.201.104 eq domain !--- Permit older DNS zone transfers.
access-list 110 permit tcp host 172.16.201.50 eq domain host 192.168.201.104 eq domain !--- Deny
all other DNS traffic. access-list 110 deny udp any any eq domain access-list 110 deny tcp any
any eq domain !--- Allow IPSec VPN traffic. access-list 110 permit udp any host 192.168.201.100
eq isakmp access-list 110 permit udp any host 192.168.201.100 eq non500-isakmp access-list 110
permit esp any host 192.168.201.100 access-list 110 permit ahp any host 192.168.201.100 access-
list 110 deny ip any host 192.168.201.100 !--- These are Internet-sourced connections to !---
publicly accessible servers. access-list 110 permit tcp any host 192.168.201.101 eq www access-
list 110 permit tcp any host 192.168.201.101 eq 443 access-list 110 permit tcp any host
192.168.201.102 eq ftp !--- Data connections to the FTP server are allowed !--- by the permit
established ACE in Phase 3. !--- Allow PASV data connections to the FTP server.

access-list 110 permit tcp any gt 1023 host 192.168.201.102 gt 1023
access-list 110 permit tcp any host 192.168.201.103 eq smtp

!--- Phase 4 – Add explicit deny statement.

access-list 110 deny   ip any any

Edge-router(config)#interface serial 2/0
Edge-router(config-if)#ip access-group 110 in
```

関連情報

- アクセス リストに関するサポートページ

- Cisco IOS スイッチング サービス コマンド リファレンス、リリース 12.2 - コマンド：access-list rate-limit through ip cef
- Requests for Comments（RFC）
- テクニカル サポートとドキュメント – Cisco Systems