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

概要

この文書では、使用しているネットワークの入り口での通過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、ガイドラインと推奨する配備方法を説明します。 トランジット access control list (ACL; アクセス コントロール リスト) は、ネットワークに必要なトラフィックだけを明示的に許可することで、ネットワークのセキュリティを高めるために使用されます。

トランジット フィルタ

典型的な設定

ほとんどのエッジネットワーク環境では、典型的なエンタープライズ ネットワーク インターネット Point of Presence のような、入力フィルタリングがネットワークのエッジで不正 な トラフィックを廃棄するのに使用する必要があります。 ある特定のサービスプロバイダー配備では、またエッジまたはトランジットトラフィック フィルタリングのこの形式が仕様によって許可されるプロトコルだけに顧客に出入してトランジットトラフィックのフローを制限するのに効果的に使用することができます。 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。

この例は典型的な企業 インターネット接続 設計を描写したものです。 2 台のエッジ ルータ、IR1 と IR2 が、インターネットに直接接続しています。 これら二つのルータの後ろで、ファイアウォ

ール（この例の Cisco PIX）のペアは内部ネットワークおよび非武装地帯両方（DMZ）にステートフル 点検機能およびアクセスを提供します。 DMZ は DNS および Web のようなサービスにパブリック直面することが含まれています; これは公衆インターネットから直接アクセス可能な唯一のネットワークです。 内部ネットワークはインターネットから直接アクセスすることはできませんが、内部ネットワークを発信元とするトラフィックは、インターネット上のサイトへ到達することが可能です。

エッジ ルータは、着信 ACL を使用して、セキュリティの第一段階を構築できるよう設定されている必要があります。 この ACL では、DMZ 宛ての特別に許可されたトラフィックだけを許可します。また、インターネットへアクセスしている内部ユーザに返されるリターン トラフィックも許可します。 すべての nonauthorized トラフィックは入力 インターフェイスで廃棄する必要があります。

トランジット ACL のセクション

一般に、中継 ACL は 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。不正な発信元またはパケットが、使用しているネットワークに属する発信元アドレスを使用して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 は アンチスプーフィング ガイドラインを提供します。
- インターネットへの内部接続のための明示的に許可されたリターントラフィック
- 保護された内部アドレスに向かう明示的に許可された外部にソースをたどられたトラフィック
- 明示的 な **Deny ステートメント注:** すべての ACL が暗黙の deny 文が含まれているが、Cisco は明示的 な**拒否** statemen の使用を、たとえば、**deny ip any any** 推奨します。 ほとんどのプラットフォームでは、このような文によって、拒否されたパケットの数が記録され、show access-list コマンドで表示することができます。

中継 ACL を開発する方法

中継 ACL の開発の第一歩がネットワークの内で必要なプロトコルを判別することです。 各サイトに特定の必要条件があるが、ある特定のプロトコルおよびアプリケーションは広く利用されて、最も頻繁に割り当てられます。 たとえば、DMZ セグメントがパブリックにアクセスできる Webサーバに接続を提供すれば、インターネットからのポート 80 の DMZ サーバアドレスへの TCP が必要となります。 インターネットに同様に、内部接続は確認応答（ACK）ビットが設定がある ACL 割り当て戻りが TCPトラフィックを–トラフィック確立したことを必要とします。

必須プロトコルを確認して下さい

必須プロトコルのこのリストの開発は非常に困難な課題である場合もありますが使用できる複数の手法が必須トラフィックの識別を助けるために必要に応じて、あります。

- **ローカルのセキュリティ ポリシーとサービス ポリシーの検討。**ローカル サイトのポリシーは、サービスの許可および拒否の基準の決定に役立ちます。
- **ファイアウォール設定の検討および監査。**現在のファイアウォール設定には、許可するサービスに対する明示的な permit 文が含まれている必要があります。 多くの場合、ACL 形式に

この設定を変換し、ACL エントリのバルクを作成するのにそれを使用できます。**注:** ステートフルなファイアウォールでは、承認されている接続へのリターン トラフィックに対しては、通常は明示的なルールを定義していません。 ルータ ACL はステートフルではないため、リターン トラフィックは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および監査。**DMZ 内でホストされるアプリケーションと、内部的に使用されるアプリケーションは、フィルタリング要求の判別に役立ちます。 フィルタリング 設計についての必要な詳細を提供するためにアプリケー– ション使用要件を検討して下さい。
- **分類 ACLの使用。**分類 ACL は内部ネットワークに向かうことができるさまざまなプロトコルのための**割り当て**文で構成されます。（広く使われたプロトコルおよびアプリケーションのリストについては付録 A を参照して下さい。）access control entry（ACE; アクセス コントロール エントリ）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。 予想外プロトコルのための明示的 な**割り当て**文を作成する前に疑わしくか意外な結果を調査し、理解して下さい。
- **Netflow スイッチング機能の使用。**Netflow は場合有効に された詳しいフロー情報を提供する切り替え機能です。 Netflow がエッジルータで有効に なる場合、**show ip cache flow コマンドは** Netflow によって記録 されるプロトコルのリストを提示します。 Netflow はすべてのプロトコルを確認できません従ってこの手法は他と共に使用する必要があります。

無効なトラフィックを識別して下さい

直接保護に加えて、中継 ACL はまたインターネットで特定タイプの無効なトラフィックに対して最初の防衛線を提供する必要があります。

- RFC 1918 スペースを否定して下さい。
- RFC 3330 で定義されたように special-use アドレス スペースの下で落ちる送信元アドレスのパケットを拒否して下さい。
- RFC 2827 に従って anti-spoof フィルタを、加えて下さい; アドレス スペースは決して自律システム（AS）の外からのパケットの出典ではないはずです。

考慮するべき他のトラフィック の 種類は下記のものを含んでいます:

- **エッジルータと通信する必要がある IP アドレスおよび外部プロトコル**サービスプロバイダー IP アドレスからの ICMPルーティング プロトコルエッジルータが終了として使用される場合、IPSec VPN
- **インターネットへの内部接続のための明示的に許可されたリターントラフィック**特定のインターネット制御メッセージ プロトコル（ICMP）のタイプ発信用ドメイン 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）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
- **保護された内部アドレスに向かう明示的に許可された外部にソースをたどられたトラフィック**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）走査専用のカプセル化方法 Encapsulating Security Payload（ESP）認証ヘッダー（AH）Webサーバへの HTTPWeb サーバに対するセキュア ソケット レイヤ（SSL）FTP サーバへの FTPFTP 受信 データ接続受信 FTP 受動態（**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受信 DNS クエリ受信 DNSゾーン転送

ACL を適用して下さい

この新しく構築された ACL は、エッジ ルータのインターネット向けインターフェイスへの着信に適用する必要があります。 典型的なセットアップセクションで説明された例では ACL は IR1 および IR2 のインターネット向き インターフェイスで isapplied。

配置 の ガイドラインおよび配備例のセクションを詳細については参照して下さい。

ACL 例

このアクセス リストが中継 ACL で必要な典型的なエントリの簡単でけれども現実的な例を提供します。 この基本的な ACL は、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。

```
!--- 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: 中継 ACL を適用するときこれらの推奨事項に留意して下さい。

- **log キーワードは**ある特定のプロトコルに送信元および宛先についての追加詳細を提供するために使用することができます。 このキーワードが ACL ヒットの詳細に **log キーワード**増加 CPU稼働率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。 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。
- ICMP 到達不能 メッセージは ACL によって管理上拒否されるパケットのために生成されます。 これはルータおよび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。 中継（エッ

ジ）ACL が展開されるインターフェイスの Ip unreachables をディセーブルにするために **no ip unreachables コマンド**の使用を考慮して下さい。
- この ACL はすべての**割り当て**文とビジネス 正当なトラフィックが拒否されないようにするために最初に展開することができます。 正当なビジネス用のトラフィックを特定できたら、対象となる要素に対して deny 文を設定してください。

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。 一般に、— ACL のレイヤ4 情報に関係なくレイヤ3 文（プロトコル、送信元アドレスおよび宛先アドレス）を一致する非初期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非初期フラグメントに ACL を強制できることに注目して下さい。

フラグメントをフィルタリングすることはサービス拒絶（DoS）攻撃に対して保護の追加層を追加します非初期フラグメントだけ使用する（のような FO > 0）。 ACL の始めに非初期フラグメントのための **Deny ステートメント**の使用はルータのアクセスからのすべての非初期フラグメントを否定します。 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、そのために ACL に deny fragment 文がある場合にフィルタされることがあります。 フラグメンテーションの原因となるかもしれない条件は ISAKMP 認証のためのデジタル証明書の使用および IPSec NAT 走査の使用が含まれています。

たとえば、ここ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 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>
```

ACL の始まりへこれらのエントリを追加することはネットワーク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 ACL の次の行に通るが、非初期フラグメント アクセスを拒否します。 前の ACL 断片はまたそれぞれ以来の攻撃の分類を UDP、TCP protocol —促進し、icmp —増分は ACL のカウンターを分けます。

攻撃の多くは、断片化パケットによってフラッディングを起こすこと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、ある程度の保護を追加し、単にトランジット ACL のレイヤ 3 ルールに一致させることだけでフラグメントを送信する攻撃ができないようにすることができます。

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

トランジットトラフィック 保護 ACL を展開するとき、リスクの 2 つの重要 な 地域を考慮して下さい。

- 適切な **permit/deny** 文が設定されていることを確認します。 有効である ACL に関しては割り当て必要なすべてのプロトコルなります。
- 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、ハードウェアの性能特性を検討して下さい。

Cisco は配備前にラボのこの設計をテストすることを推奨します。

付録

広く使われたプロトコルおよびアプリケーション

TCP のポート名

TCPポート名前のこのリストはポート番号の代りに Cisco IOS ® ソフトウェアの ACL を設定するとき使用することができます。 これらのプロトコルへの参照を見つけるために現在の割り当て番号の RFC を参照して下さい。 これらのプロトコルに対応するポート番号はまた a の入力によって ACL を設定する間、によって見つけることができますか。 ポート番号の代わり。

bgp	kshell
chargen	ログイン
cmd	lpd
daytime	nntp
discard	pim
domain	pop2
echo	pop3
Exec	SMTP
finger	sunrpc
ftp	syslog
ftp-data	tacacstalk
gopher	Telnet
hostname	時刻
ident	uucp
irc	whois
klogin	www

UDP のポート名

UDP ポート名のこのリストはポート番号の代りに Cisco IOSソフトウェアの ACL を設定するとき使用することができます。 これらのプロトコルへの参照を見つけるために現在の割り当て番号の RFC を参照して下さい。 これらのプロトコルに対応するポート番号はまた a の入力によって ACL を設定する間、によって見つけることができますか。 ポート番号の代わり。

biff	ntp
bootpc	pim-auto-rp
bootps	RIP
discard	SNMP
dnsix	snmptrap
domain	sunrpc
echo	syslog
isakmp	tacacs

mobile-ip	talk
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。 順調に中継 ACL を展開するために必須プロトコルの確実な理解を持たなければなりません。 反復的なアプローチを利用するこれらのガイドラインは保護 ACL の配備のための非常に保守的な方式を記述します。

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 ACL を割り当てネットワークで使用するすべての既知のプロトコル展開して下さい。 このディスカバリ、か分類は、ACL の送信元アドレスおよび IP アドレスまたは全体のインターネットのルーティング可能なIP サブネットの宛先があるはずです。 許可する必要がある追加プロトコルの確認を助けるように最後のエントリをこと割り当て **IP あらゆるあらゆるログイン**順序設定して下さい。目的は、ネットワーク上で使用されている必要なすべてのプロトコルを判別することです。 通信するかもしれませんか他に何がルータと判別するために分析のためにロギングを使用して下さい。**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。 必要な場合だけだけトラフィックの分類を助けるために **log キーワードを**短い間使用すれば。ネットワークは攻撃の危険がある状態にすべての**割り当て**文で構成されている ACL が間、以下の事項に注意して下さい:あります。 分類処理をなるべく早く実行し、正しいアクセス制御を配備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、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 で設定した ACL でフィルタされたパケットの識別と確認ができたら、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のための Add ACL エントリ。 要求に応じて、分類 ACL の**割り当て**文の特定の**拒否**エントリを代わりにして下さい。 また、show access-list コマンドを使用して、特定の deny エントリを監視すると、ヒット カウントを調べることができます。 この方法では、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 アクセスの試行の詳細を調べることができます。 ACL の最後の行は、deny ip any any とします。 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行に関する情報を得ることができます。
3. **ACL を監視し、アップデートして下さい。**新規に導入されす必須プロトコルが制御された方法で追加されるようにするために完了された ACL を監視して下さい。 ACL を監視する場合、また切迫した不正侵入についての情報を提供する可能性がある禁止されたネットワークアクセス試みについての情報を提供します。

配備例

この例はこのアドレッシングに基づいてネットワークを保護する中継 ACL を示したものです。

- ISP ルータ の IP アドレスは 10.1.1.1 です。エッジルータ インターネット向き IP アドレスは 10.1.1.2 です。インターネットにルーティング可能なサブネットは 192.168.201.0

255.255.255.0 です。VPN ヘッドエンドは、192.168.201.100 です。Web サーバのアドレスは 192.168.201.101 です。FTP サーバのアドレスは 192.168.201.102 です。SMTP サーバのアドレスは 192.168.201.103 です。プライマリ DNS サーバのアドレスは 192.168.201.104 です。セカンダリ DNS サーバのアドレスは 172.16.201.50 です。

中継保護 ACL はこの情報に基づいて開発されました。 この ACL では、ISP のルータへの eBGP ピアリングを許可し、アンチスプーフィング フィルタを備え、特定のリターン トラフィックと特定の着信トラフィックを許可し、他のすべてのトラフィックを拒否します。

```
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 コマンドレファレンス、リリース 12.2 -コマンド: ip cef による access-list レート制限
- Requests for Comments (RFC)
- テクニカルサポートとドキュメント - Cisco Systems