==========
4th Inter-Domain Routing Security Workshop

日 時： 2005/04/08 14:00-18:00
場 所： Cisco赤坂オフィス 14F
参加者： 50名
議事録： 白畑さん（編集：近藤）
==========

1. Agenda

1) Generalized Filtering Policy Proposal
DTI 馬渡氏
2) Generalized Router Configuration in IX
JPIX 平尾氏

2. 議事

2.1 Generalized Filtering Policy Proposal

※質疑応答を中心に記録しています。

■トランジット接続部分
□非対称なルーティングについて

Q:どのようにして非対称なルーティングを発見したか？

A:トラフィックのパターンをみていたところ、不思議な箇所があったため、tracerouteを行ったところ、ループ箇所を発見した。

C:フィルタを実施するとお客さんが使っているのが発覚する、といったケースなどを想像していた。アドレススプーフィングを防ぐという面では、フィルタするのが望ましいので、メリットとデメリットを記述してはどうか。

Q:最初からフィルタを適用していた？

A:あまり顧客のエッジではフィルタをかけていなかった。フィルタをかけて通信が止まった結果、見つかったというわけではない。顧客へは、地域の公共IP網というか、他のISPから割り当てられているIPアドレスの顧客に通信するという形になっており、地域あての通信トラフィックはそこに流す形になっている。

incomingのトラフィックにそのようなIPアドレスからのパケットがきているが、アドレスリストの管理がされていない。地域のネットワークの内部はOSPF、外部へのデフォルトはこちらに向いている。

□ルータ自身へのingress フィルタ

Q:資料の方では、ルータ自身のingressフィルタということで、eBGPへのneighbor のアドレスのフィルタは、ルータ自身をまもるフィルタではないか。

A:トランジットの部分でフィルタしてしまうと、トランジットの下流でeBGP multihop をやっているケースにひっかかってしまう場合があるのではないか。フィルタを書くルータ自身以外のものはいじらないほうが無難なのではないか。

2-1-1 の [1]: 自分のルータにくるBGPセッションを保護する、ではルータ自身のところに、eBGP と iBGP を同時に書いた方がよいのではないか。

Q:[3] の部分にこだわっているが、理由は？

A:自分のアドレスをspoofされることを防止したい

Q:自分の定義とは？
A:自分のカスタマーの持っているIPアドレス

Q:一カ所でやろうとすると楽に思えるが、目的を分けて考えるべき。カスタマーのアドレスなら、カスタマーのエッジでやるべき。カスタマーが別のカスタマーにアタックする可能性もある。

UDLRやマルチホーム、地域IX（マルチホームの一種）では、小細工をするケースなどもある。ソースIPアドレスを自社のバックボーンに限定するべきではないか？

A:アドレスの設計をきちんとやっているところでは楽だが、設計がきちんとしていないところでは厳しいかもしれない。

Q:バックボーンのアドレスが散らばっているところは？
A:数名挙手

□非対称ルーティングについて

Q:非対称ルーティングをやっているのは特殊な例か。

A:ASとらずに複数のISPに広報できないかという問い合わせが年に3,4件ある。やってもよいかは悩むが、昔はOKといっていた。

□punching-hole について

Q:punching-hole な経路は日本ではどのぐらいあるのか？自分の CIDR から二本ぐらい切り出して、ほかにアナウンスしているケースがUSではあるが、日本でもあるか？

A:国内のISPの経路をpunchするケースはないが、外資系のお客さんで/16を本国で使っていて、/24を支社で使っているケースなど。

C:設定内容を淡々と書くと、意図が伝わらないので、意図を書くようにしてほしい。

□Egressフィルタ

Q:Egress フィルタはなぜいらないのか。Private IPアドレスを source に持つものはどれぐらいあるのか。

A:前回、とある大手ISPではバックボーンにPrivate IPアドレスを使っているため、フィルタを適用できないので、推奨にはいれなくてもよいのではないかという意見があった。

C:source が Private、destination がグローバルなら届く。

Q:他のISPが ingress でかけるなら、結局は届かないので、ingress でかけるなら、egress で書いてもよいのではないか。

C:自分で利用している IP アドレス以外は通さないという書き方はどうか。内部でPrivate IP アドレスを利用しているケースは通す。

C:トランジットISPでは許さざるを得ない。

C:アナウンスしている prefix について書いた方がよいのではないか。

C:RFCの3330がでている
->RFC3330 で提示されている prefix を全部 reject する事は出来

ないTeam Cymru で出しているドキュメントも参考にしている

□Private AS を含む AS_PATH の扱いについて

基本方針：AS_PATH から Private AS は除去する。

Q:トランジットで通している ingress の AS_PATH に Private AS がはいっている経路は落とした方がよいのではないか？

A:フィルタしたがために、full route が full route でなくなってしまうのではないか。Private AS origin ではなければ良いのではないか。

C:問題の経路はAS hop数が長い。だいたい他のhopでbackupされているので、99.9%ぐらい大丈夫。

C:もしお客さんが使っていれば、お客さんにトランジットを提供している場合には、full routeがfull routeでなくなってしまうのはいや。

C:当該AS管理者に contact しても返事をくれない。

□Private AS の除去について

- IANA 的には 65535 が Reserve AS で Private AS ではない。IETF 的ではPrivate AS。Juniper は reserve は通る、Ciscoは落とす。

- remove-private-as したとき、事故った際に自分の AS 番号になってしまうのではないか。Cisco は自分を origin にする以外は消さない。

- remove-private-as の実装: Juniper, Cisco以外だと、Foundry と Hitachi も remove-private-as に対応している。これらは IX で使われているルータを 99% カバーしている

□経路フィルタについて

- /6 or aggregate して /5 でアナウンスしているものがある

Q:/25 or longerでフィルタしたら到達性がなくなるのではないか？

A:intec netcoreでしらべると約100経路ひっかかる /0〜5,6 はない。一番短いのは/8で、59経路ほど。

■顧客接続部分

□プレフィックスフィルタについて

Q:多数のお客を持つ大きなトランジットISPでは、スケールでしないのではないか

A:NANOGで発表されている資料では、UUNET は exact に match している prefix のみ通している。
MCI は自分で IRR をたてている。Cable & Wireless は、自分でIRRをたて、そこに顧客に登録してもらっている。ルーズなアメリカでさえきちんとやっているので、きちんとやったほうがいいのではないか。

□ICMPのフィルタ方法について

- コメント: 3.1.1 (1)では、ICMPをコントロールするフィルタとして、優先度を低くする以外にも、512byte をこえる ICMP は落とすなどの対

策もあるのではないか。
ICMP をコントロールするフィルタを余力があるならやる、など。

- 優先度を低くした際の影響として、tracerouteで遅延が発生しているようにみえるケースもあるなど、断り書きをいれておいたほうがいいのではないか。

Q:BGP 接続を行っていない ISP 向けの記述は？
A:今回の文章のフォーカスとは違うので、他の文章をつくるならそれでまとめるのがよいのではないか。

Q:smurf みたいなアタックを考えた際、ルータ自身のアドレスだけではなく、broadcast アドレスあてのフィルタを書く必要はないのか。

A: no cdp enable をいれるかいれないかの議論に似ている。フィルタの記述ではないが、参考項目としてあげるのはどうか -> 次の発表でふれる。

Q:Max Prefix Limits でピアごとの経路数を制限するが、AS_PATH ホップ数の制限をするのはどうか。

A:わすれていた

Q:過去にAS_Path長が問題になり、ルータの障害を引き起こす事件があったため、いれているというが、どれくらいの長さをいれているのか？

A:100ぐらい。
ルータへの attack としてやってくる場合もあるので、ルータのパワーによる。ベンダに推奨値をだしてほしい。100という数字に根拠はない。

Q:50以上 - 挙手少々

A:50ぐらいにしてはどうか

C:potaroo.net によると、MAX AS_PATH は 12、
Prepend を考慮しても 32。

Q:2.1.1(1)のサービスリストに ntp を載せてほしい

A:のせます

2.2 Generalized Router Configuration in IX

□next-hop-self の利用

Q:next-hop-self を推奨するのはよいが、できない場合を書いたほうがよい。
IX 上に複数の複数ルータを導入する場合、ある AS に対してはトラフィックが偏ってしまいます。そこで、このセグメントを IGP に広報すると
OSPFの equal cost load balance を使うことができる。しかし、
next-hop-self をすると、どちらかの経路が優先できない。

A:やったことはないが、 eBGP multipath で解決できないか？最近はリンクがふといので、あまり困っていない。

Q:Cisco さんでは使えますか？

A:使えます。うろ覚えですが、6つまで。Source と Destination をハッシュにいれて分散するのだとおもいました。

Q:next-hop-self 派: 13人 / 出席者 約40人

Q:next-hop-self で、オペレーション上、ほかに困ったことはあったのか？

A:監視の際に ping が飛ばないと困る。border router 上からしか ping が飛ばない。

Netflow でどのルータから出て行くか見えるが、どのピアに出て行っているかが見えない。そのため、そのルータまでいって再度解析しないといけない。

あまりコミュニティがなかった際には、複数のルータとピアしているとき、区別してルーティングしたいといったニーズが以前あった。問題はないが、情報はほしい。

□BGPの脆弱性対策

- BGPの脆弱性対策の目的は、他からの不正なアクセスを防ぎたい。IX 上が一番あぶないといわれている BGP 脆弱性対策をしたい、というものである。

C:何を守りたいかという観点で、DoSの対策だと考えている。セッションを保護するにはMD5でとりあえず保護できる。そういう意味で、ルータの保護という意味ではありだと考えている。

C:このフィルタは、自分が幸せになるフィルタではないが、他の人が幸せになるフィルタである。オープンで DoS をする、相手のルータに DoS をするのと同様、BGP の脆弱性対策というのも、brute force attack のようにものを防げる。ただ、推奨というよりも、RFC でいえば shall 程度になるのだと思う。

Q:さきほどの馬渡さんのドキュメントでカバーされていないか？

A:かかれているが、意味がわかるとよいと思う。なぜそのような設定をするのか。

C:守ろうとするIXのセグメントは、AS内にしか広告されていない。AS内からIXセグメントへのBGPはふせげない。BGPのゾーンからでるときは、フィルタで落とせばよいのではないか。

C:趣旨は問題点の啓発。

□その他

- メーカーに推奨設定の config を出してもらうよう協力を依頼してはどうか。

- デフォルト設定の変更をお願いすることもしていかなくてはならない。

- APNIC の IX-Sig では似たようなことをやっているらしい。

以上