xSPのルータにおいて設定を推奨するフィルタの項目について(IPv6版)

KDDI 石原

パワードコム　向井

DTI 馬渡

はじめに

- 「xSPのルータにおいて設定を推奨するフィルタの項目について」のIPv6版
  - 「最低限、設定することが推奨されるフィルタ」について、まず議論したい
- 接続形態に変化はないので、IPv6対応をメインに
- IETF draft、RIRでproposal進行中のものについては今回の検討外としたい

登場するアドレス

- default
  - ::/0
- ループバックアドレス
  - ::1/128
- 未指定アドレス
  - ::/128
- IPv4互換アドレス
  - ::ffff:/96
  - ::ffff:a.b.c.d
- IPv4射影アドレス
  - ::/96
  - ::a.b.c.d
- リンクローカルアドレス
  - fe80::/10
- サイトローカルアドレス
  - fec0::/10
  - もう使われないアドレスだけど
- ユニークローカルアドレス
  - fec0::/7 **New!**
  - RFC4193
- マルチキャストアドレス
  - ff00::/8
- ドキュメントアドレス
  - 2001:db8::/32
- 自ASのprefix
  - まさに2001:db8::/32の出番☺
- 6to4
  - 2002::/16

フィルタリングをするところ

- ピア接続
- トランジット接続
- 顧客接続
- ルーター自身へのアクセス

ピア接続 パケットフィルタリング

- Ingress
  - source addressが、ループバック、サイトローカル、ユニークローカル、ドキュメント、マルチキャストのパケットは、reject
  - source addressが、リンクローカルのパケットはaccept
  - 自ASのprefixをreject
- Egress
  - 特に必要なし

ピア接続 経路フィルタリング

- Ingress
  - default、ループバック、リンクローカル、サイトローカル、ユニークローカル、ドキュメント、マルチキャスト、自ASのprefixをor longerでreject
  - as-path filterは特になし
- Egress
  - 自ASのprefixは集約してaccept
  - private ASNをreject

トランジット接続 パケットフィルタリング

- Ingress
  - source addressが、ループバック、サイトローカル、ユニークローカル、ドキュメント、マルチキャストのパケットは、reject
  - source addressが、リンクローカルのパケットはaccept
  - 自ASのprefixをreject
- Egress
  - 特に必要なし

トランジット接続 経路フィルタリング

- Ingress
  - default、ループバック、リンクローカル、サイトローカル、ユニークローカル、ドキュメント、マルチキャスト、自ASのprefixをor longerでreject
  - as-path filterは特になし
- Egress
  - default、ループバック、リンクローカル、ドキュメント、マルチキャストをor longerでreject
  - 自ASのprefixは集約してpermit
  - private ASNをreject

顧客接続 パケットフィルタリング

- Ingress
  - source addressが、ループバック、サイトローカル、ユニークローカル、ドキュメント、マルチキャストのパケットをreject
  - source addressが、リンクローカルのパケットはaccept
  - トランジット顧客の場合、自ASのprefixがsource addressのパケットをreject
- Egress
  - 特に必要なし

顧客接続 経路フィルタリング

- BGP接続顧客を対象
- Ingress
  - 顧客に割り当てたprefixをexactでaccept
  - 顧客からアナウンスされる可能性のあるprefixをaccept
  - as-path filterは特になし
- Egress
  - default、ループバック、リンクローカル、サイトローカル、ユニークローカル、ドキュメント、マルチキャストをor longerでreject
  - 自ASのprefixは集約してaccept
  - private ASNをreject

ルータ自身へのアクセス パケットフィルタリング

- Ingress
  - ルータで動かしているサービスのうち、アクセス可能なsource addressを限定してaccept
    - TELNET / SSH / SNMP / FTP/ TFTP / NTP
  - 利用しないサービスはもちろんdisable
  - eBGP / iBGPのneighbor addressのみ179/tcpでaccept
  - 接続リンクにおいて、source addressがリンクローカルのパケットはaccept
- Egress
  - 特に必要なし

経路フィルタリング (bogons routes)

- IANAからRIRに割り振られたprefixのみacceptする経路フィルターについては、運用ポリシー次第？
  - 例:
    - 2003::/16 prefix-length-range /19-/32 accept
    - 2600::/12 prefix-length-range /19-/32 accept
    - 2a00::/16 prefix-length-range /19-/32 accept
    - 他はreject
- ちなみに、各RIRのポリシーにより、IX、critical internet infraに対する割り当て長が違うので、気をつける必要があります
    - ARINだと/48がroot serverなどに割り当てられています
    - APNIC、RIPE/NCCは、/32
    - でも、全部追従できるか不安。☹

IPv6で考慮されるもの

6to4

::/8

/48 or longer

6bone

6to4

- RFC3068で定義されている
- 6to4のglobalなリレールータのprefix
  - 日本なら、KDDI labさんがoriginateしてる模様
  - 2002::/16 192.88.99.0/24でアナウンスされています。
  - 6to4 relay anycast address
    - 192.88.99.1
    - 2002:c058:6301::
  - rejectしないでね。☺
- ピア、トランジット、顧客向けの経路フィルタリングでの扱いどうしましょう？

::/8

- IPv6への移行を目的としたアドレス
  - IPv4互換アドレス
    - ::/96　　自動設定トンネリングで利用(RFC2893)
  - IPv4射影アドレス
    - ::ffff:/96　IPv6ノードがIPv4ノードと通信する際にIPv6ノード内部で利用
- 特殊なUnicast address(RFC3513)
  - 未指定アドレス(unspecified address)
    - ::/128　　neighbor discoveryで利用
    - IPv6ルータは転送すべきでないと書かれている
  - ループバックアドレス
    - ::1/128
    - IPv6ノードはsrc / dstにループバックアドレスが設定されている場合、そのノードから送信すべきではないと書かれている
- これら::/8のパケットフィルタリング、経路フィルタリングはどうしましょう？

/48 or longerのprefix

- 今のところ、/48より長いprefixはsiteに割り当てはされない
- accept？reject？運用ポリシー次第でどちらでもOK？

6bone

- RFC2471で定義
  - 3ffe::/16
  - 2006年6月6日に終了予定とRFC3701で書かれている
- 6bone終了後は、パケットフィルタリング、経路フィルタリングともにreject?

参考資料

- xSPのルータにおいて設定を推奨するフィルタの項目について, http://www.bugest.net/irs/
- IPv6 BGP filter recommendations, http://www.space.net/~gert/RIPE/ipv6-filters.html

参考資料

- **IANA**
  - IPv6 Address Space, http://www.iana.org/assignments/ipv6-address-space
- **RFC**
  - IPv6 Testing Address Allocation, RFC2471
  - Transition Mechanisms for IPv6 Hosts and Routers, RFC2893
  - An Anycast Prefix for 6to4 Relay Routers, RFC3068
  - Internet Protocol Version 6 (IPv6) Addressing Architecture, RFC3513
  - Unique Local IPv6 Unicast Addresses, RFC4193