IPv6 CPE Balanced Security

draft-v6ops-vyncke-balanced-ipv6-security

Shishio Tsuchiya

shtsuchi@cisco.com

何が問題か？

- 既存のIPv4ではNAPTが提供され、それによりInboudトラフィックのセキュリティが担保されてきた。
- 一方エンドツーエンドのコミュニケーションには問題があるケースがあった。
- そこでIPv6ではエンドツーエンドのコミュニケーションが重点される様になった。

今までのIPv6セキュリティ

- RFC 6092: Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service
  - すべての入力トラフィック許可かすべてをDenyかいずれか
  - 多くのベンダーでインプリ済み
- draft-vyncke-advanced-ipv6-security-03
  - IPSやレピュテーションなど最新セキュリティ技術を導入
  - CPEでのインプリ無し

Balanced Security?

Balanced Security?

- SwissCommが適用したモデル
- 基本的にRFC6092のAll Openモードで動作
- ただしWell-knownな例外を除く

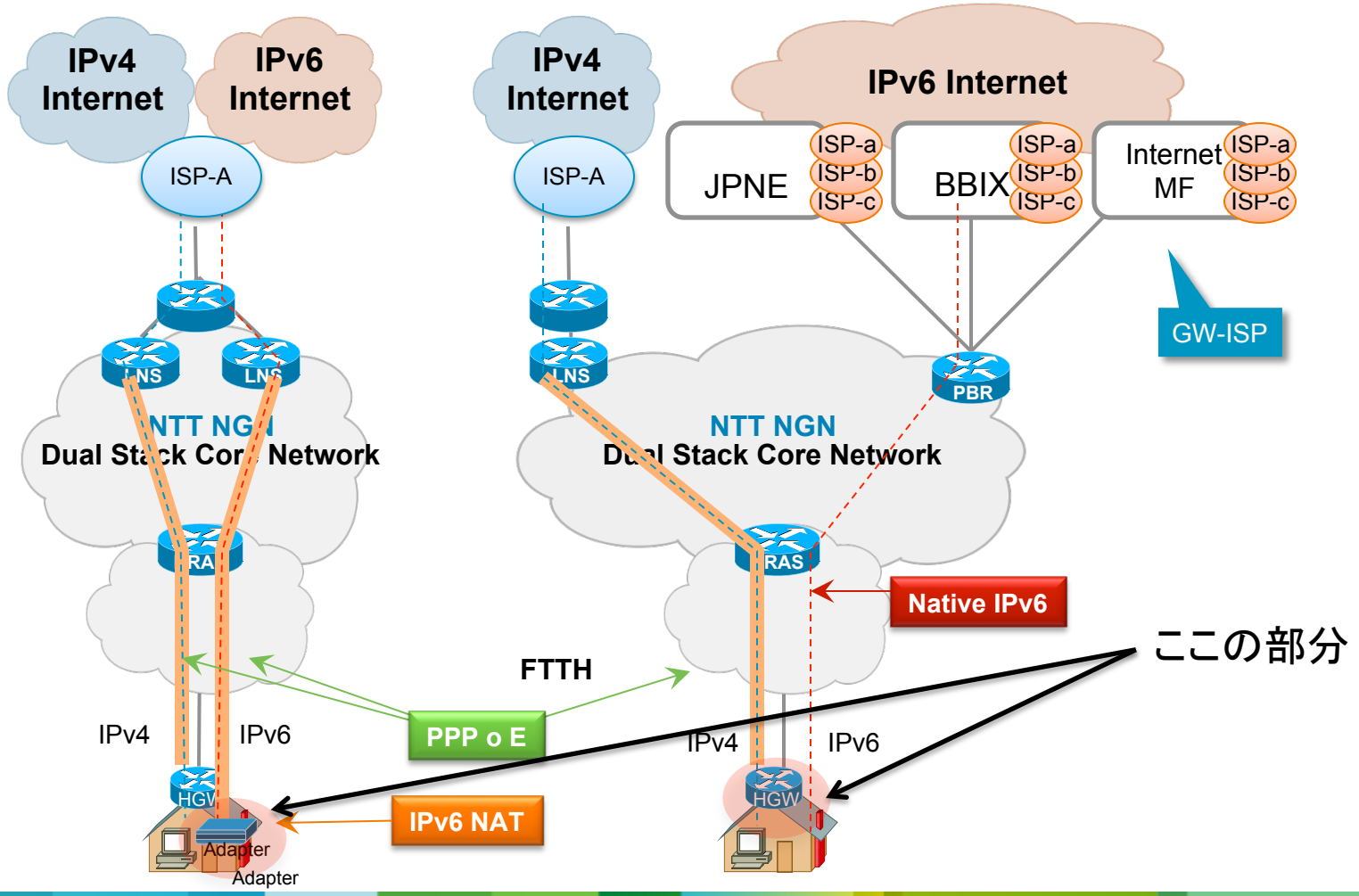
Well-knownな例外
その1 Drop inbound

トランスポート	ポート番号	プロトコル
TCP	22	Secure Shell (SSH)
TCP	23	Telnet
TCP	80	HTTP
TCP	3389	マイクロソフト リモートデスクトップ
TCP	5900	VNC リモートデスクトップ

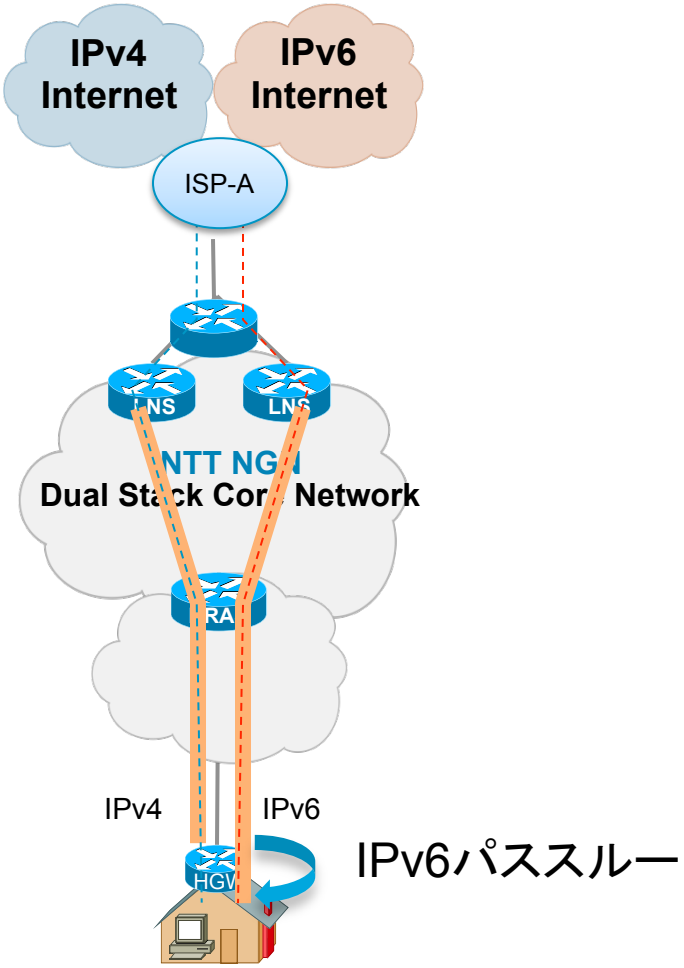
Well-knownな例外
その2 inbound/outbound ドロップ

トランスポート	ポート番号	プロトコル
TCP/UDP	88	Kerberos
TCP	111	SUN Remote Procedure Call
TCP	135	Microsoft EPMAP (End Point Mapper)
TCP	139	NetBIOS Session Service
TCP	445	Microsoft SMB Domain Server
TCP	513	Login
TCP	514	Shell
TCP	548	Apple Filing Protocol over TCP
TCP	631	Internet Printing Protocol
UDP	1900	Simple Service Discovery Protocol
TCP	2689	Simple Service Discovery Protocol
UDP	3702	Web Services Dynamic Discovery
UDP	5353	Multicast DNS
UDP	5355	Link-Local Multicast Name Resolution

さて、日本ってどうだっけ？



閉域網ではあるけど、パススルー（All open）



このドラフトは

- Swisscomのみ/Managed CPEのみでは無く色々な例が追加される予定です。
- カテゴリはInformationalになり、強制権はもちろん無いでしょう。

- ただし、業界スタンダードの手法と日本のやり方が分かれるのは色々不具合があるはずです。
- 日本でのパターン・実情をインプットしませんか？

Thank you.