

誰でも使える サーバーサイド Open NAT64実証実験報告 (Open NAT64 Experience Report)

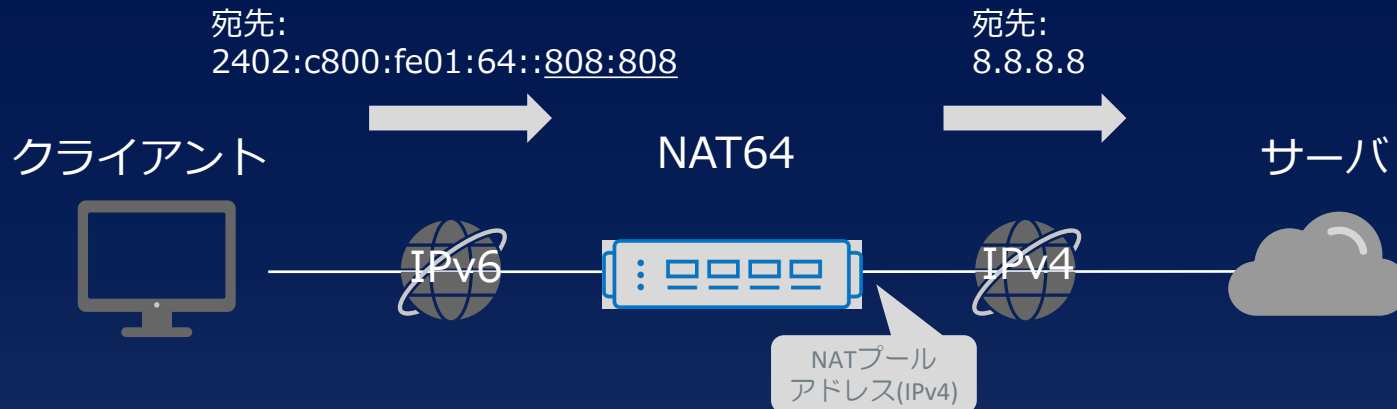
JANOG46 Okinawa 2020 8/27
Kaname NISHIZUKA, NTT Communications
@__kaname__

NAT64が活躍するユースケース



[復習]NAT64とは？

IPv6空間のクライアントから、IPv4空間のサーバへの通信を可能にする仕組み



- NAT64 prefix(/96) と IPv4アドレスを組み合わせたIPv6合成アドレス(IPv6 Synthesis address)を宛先とする
- IPv4パケットの送信元アドレスはNAT64に設定されたプールアドレスになる
- IPv6合成アドレスがAAAAレコードに設定されていればIPv6クライアントは通信可能
 - DNS64は、AAAAレコードが存在しないときに、AレコードからIPv6合成アドレスを生成して返してくれるフルリゾルバ

NAT64 prefix:

2402:c800:fe01:64::/96

Pool IPv4:

163.138.237.48/28

DNS64:

2402:c800:fe01:a10::53

解説記事:

秒でサイトのIPv6対応ができる！サーバサイド Open NAT64を
公開した話

https://qiita.com/__kaname__/items/0c77fb3b5fb01a796a4b

NAT64が活躍するユースケース



対象:

サービスのIPv6化を検討しているコンテンツ事業者

サーバ自体へのIPv6アドレス付与をしない場合

- CDN事業者を利用したIPv6化
- ロードバランサ(SLB64)を利用したIPv6化

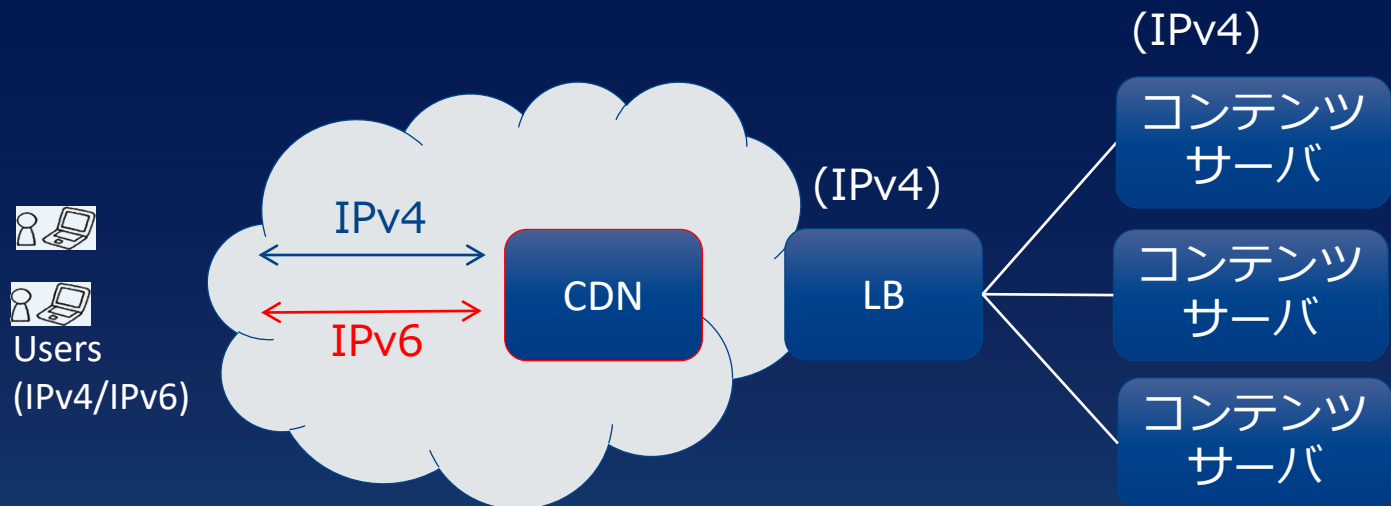
※SLB64: Server Load Balancer 64

IPv6でのアクセスをIPv4サーバに振り分けるロードバランサ

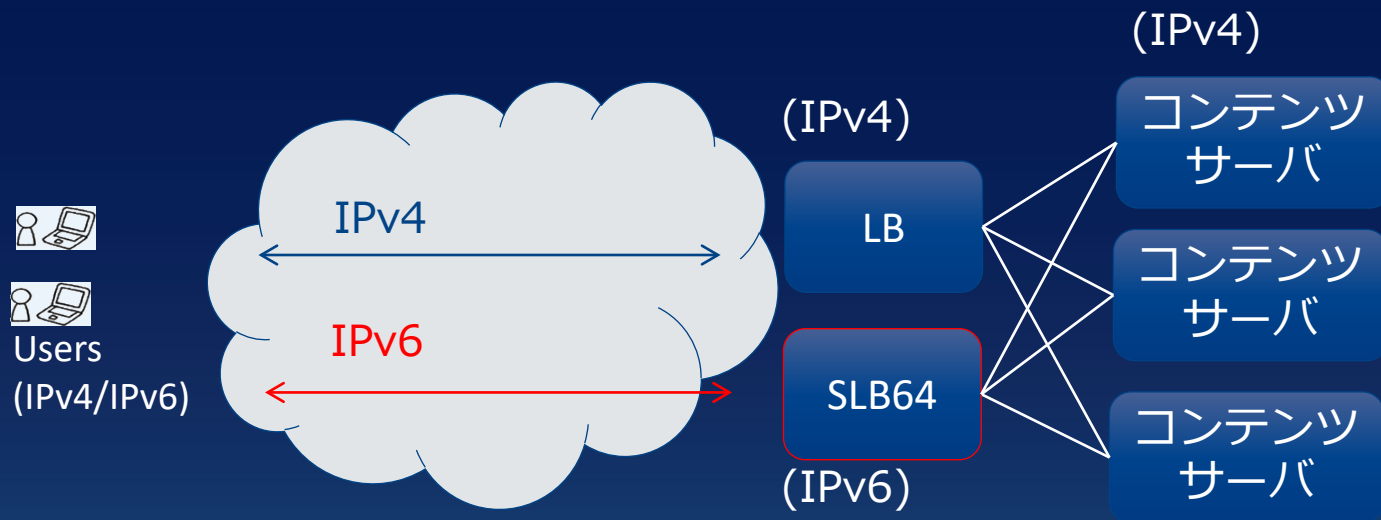


Open NAT64/SLB64を使うのはどうか？

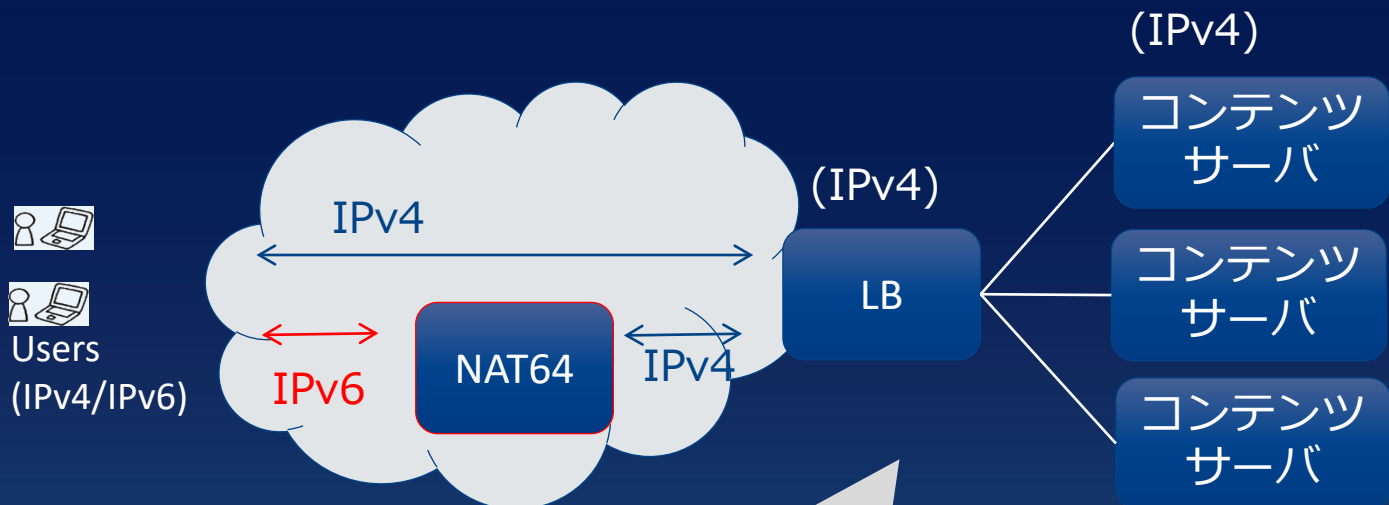
CDN型



slb64型(パブリッククラウドなど)

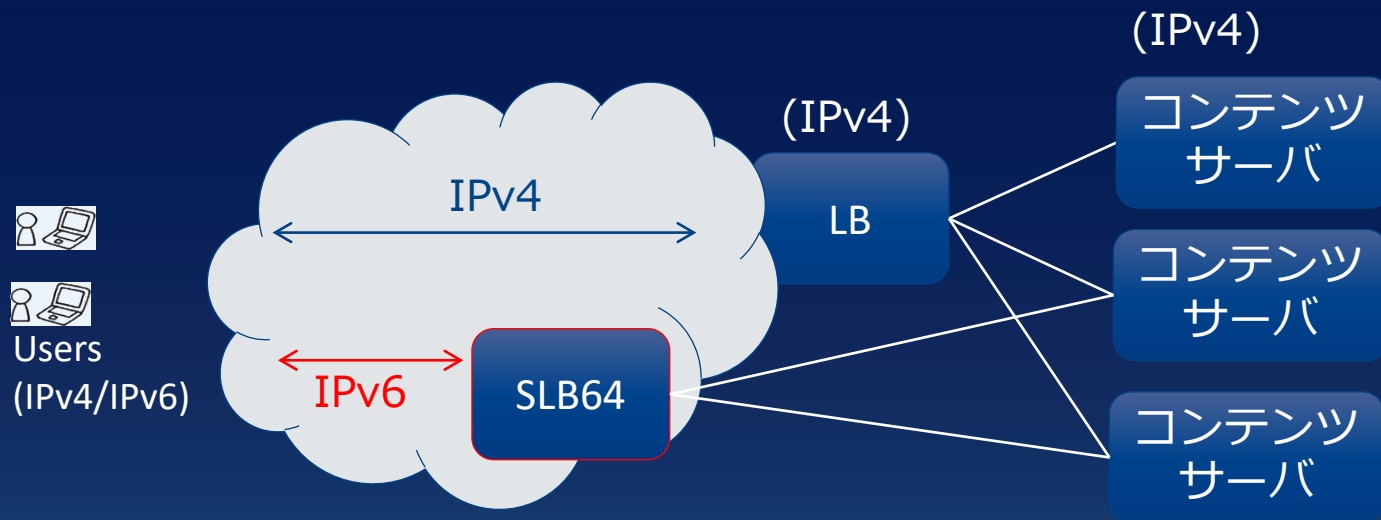


Open NAT64型(New)



NAT64のIPv6合成アドレスを
AAAAレコードに登録するだけ！

Open slb64型(New)



NAT64が活躍するユースケース



対象:

サーバをIPv6 Onlyにしたいコンテンツ事業者

- (大規模で、IPv4アドレスが枯渇しており)DC内のIPv6化を検討している

❖ IPv4空間に接続するために、IPv6 Onlyのサーバインフラは、NAT64/DNS64を利用する必要がある。

※インターネット上のOS/パッケージの取得や、IPv6対応していないミドルウェア(例:Hadoop)など

コンテンツ事業者のIPv6 onlyへの移行シナリオには
NAT64が出てくるのではないかな？

- コンテンツ事業者は、「コンテンツのIPv6化」の後、
「IPv6 Onlyインフラ」に向かう
- 2つのユースケースは同じNAT64のプラットフォーム
で提供できるのではないかな？

Open な誰でも使えるNAT64を公開する

コンテンツのIPv6対応のシナリオを検証する

実験結果についてコミュニティに広くフィードバックする

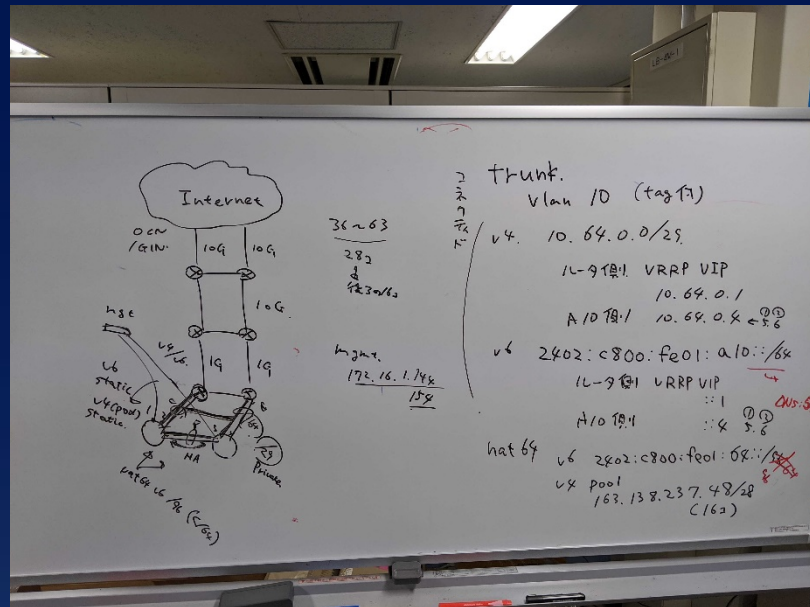
Open NAT64実験概要

- 帯域1G

- NTT大手町本館

機器提供：A10ネットワークス様

- TH4430S * 2台(冗長)



ささっと設計して半日で構築

眞野さん(A10)ありがとうございます！

1. ロケーション
2. Path MTU Blackhole問題
3. NATログ
4. SLB機能をONにするAPIを公開するアイデア
5. Abuse/アクセス制限/DDoS対策

本実験(大手町)

- 都内からの遅延: 10ms程度

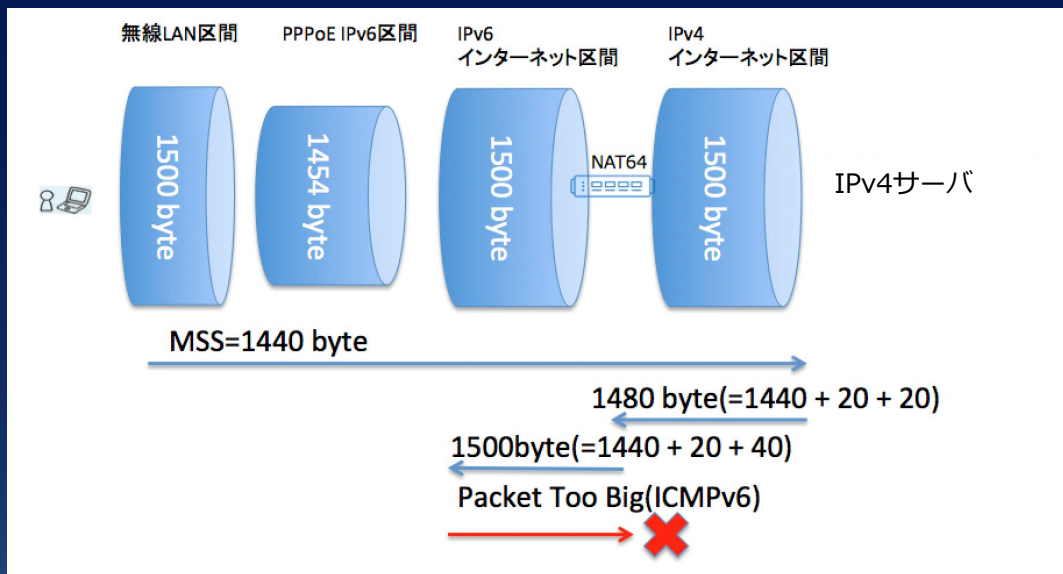
NAT64/DNS64 public test by go6lab (Slovenia)

- 都内からの遅延: 250ms程度

❗ 今までは気軽に試せるOpen NAT64は海外にしかなかったが、遅延が問題だった
→国内にNAT64を配置することで利便性が向上

<https://go6lab.si/current-ipv6-tests/nat64dns64-public-test/>

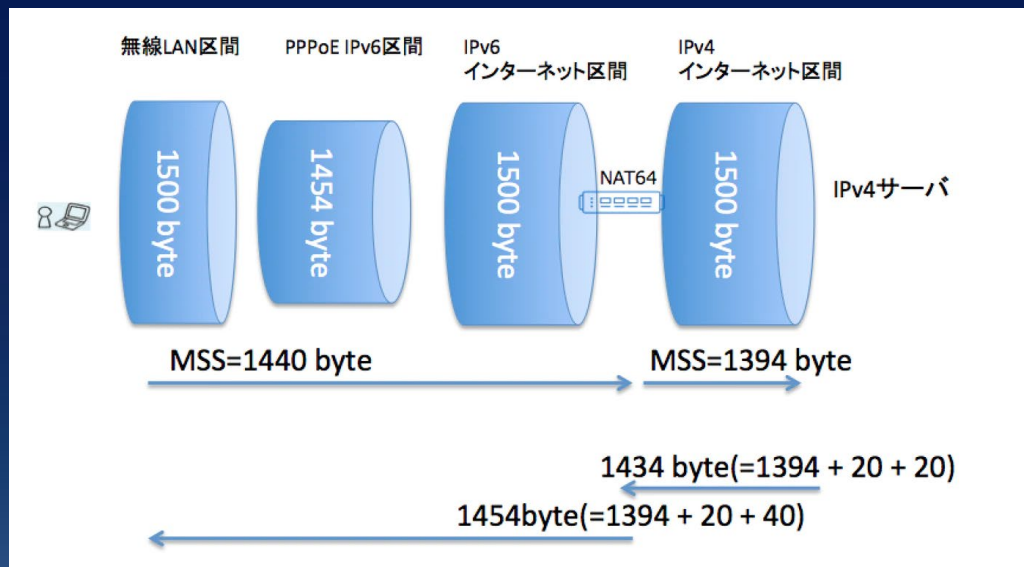
Packet Too BigメッセージがIPv4空間に変換されないため、Path MTU Blackhole問題が発生する



[参考]Path MTU Blackhole で阿部寛様のご尊顔が表示されない！
https://qiita.com/__kaname__/items/f1e9d1da965c003c7669

対策: NAT64装置でMSS-clampingを実施

- PPPoE IPv6に対応可能なMSS=1394に固定
- `cgnv6 nat64 tcp mss-clamp fixed 1394`

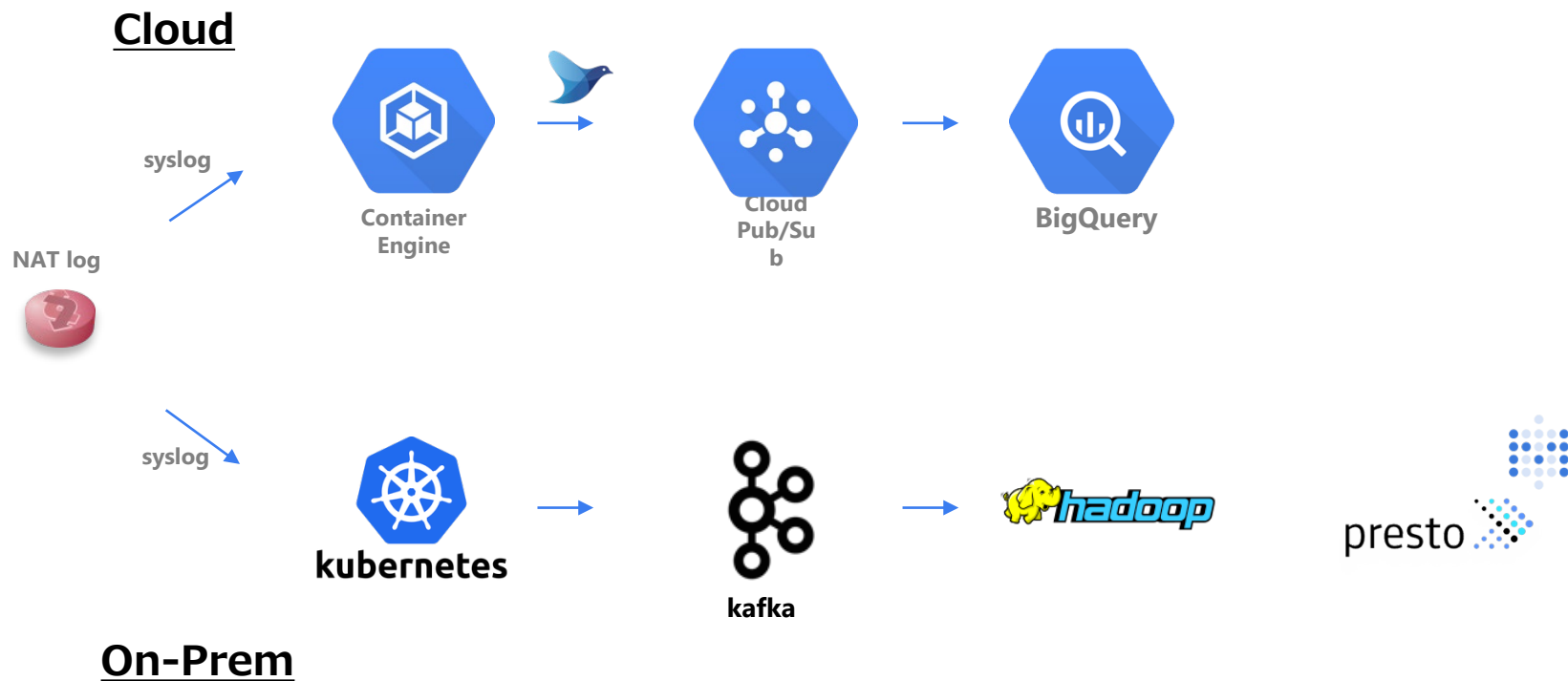


NATサービスにおけるログ保存の重要性

- 発信者情報開示請求への対応

ログ提供の重要性

- コンテンツサーバからは、NATプールアドレスからのアクセスにしか見えない
- ユーザアクセス分析のために(CDN事業者のような)分析情報の提供が求められると想定される

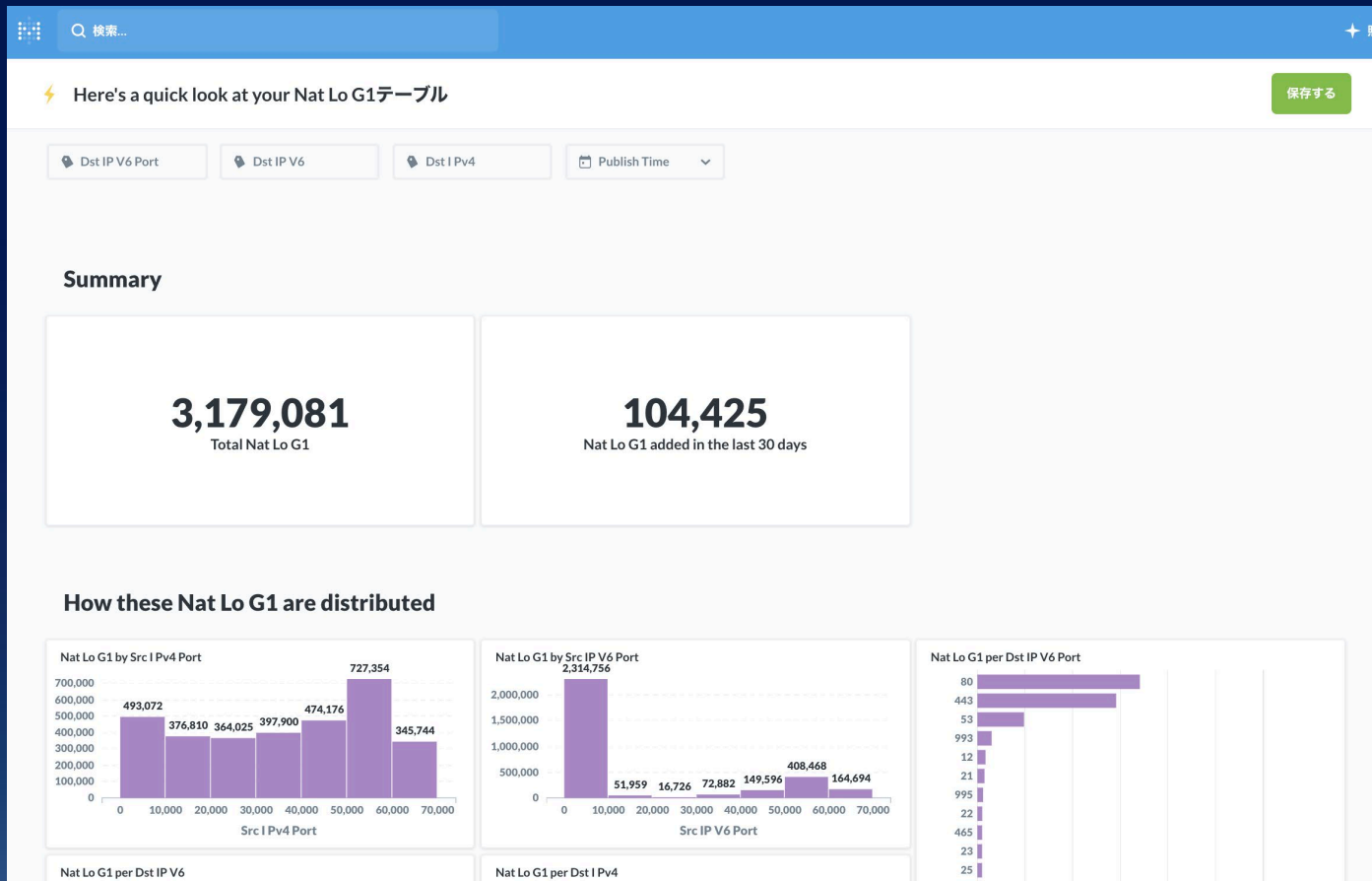


検索...

bigquery-test • Nat Lo G1

Publish Time	Host	Ident	Dst I Pv4	Dst IP V6	Dst IP V6 Port	Src I Pv4	Src I Pv4 Port	Src IP V6	Src IP V6 Port	Time Rs Y Slog
6月 14, 2020, 2:19 午後	TH01	NAT-TCP-C		2402:c800:fe01:64::	31	163.138.237.48	9,118		9,118	Jun 14 14:18:07
6月 15, 2020, 3:51 午前	TH01	NAT-TCP-C		2402:c800:fe01:64::	23456	163.138.237.48	45,100		45,100	Jun 15 03:50:08
6月 15, 2020, 6:36 午前	TH01	NAT-TCP-C		2402:c800:fe01:64::	8443	163.138.237.48	53,614		53,614	Jun 15 06:34:55
6月 15, 2020, 2:25 午前	TH01	NAT-TCP-C		2402:c800:fe01:64::	443	163.138.237.48	37,520		37,520	Jun 15 02:23:10
6月 14, 2020, 9:33 午前	TH01	NAT-TCP-C		2402:c800:fe01:64::	8885	163.138.237.48	48,235		48,235	Jun 14 09:32:02
6月 14, 2020, 2:47 午後	TH01	NAT-TCP-C		2402:c800:fe01:64::	9600	163.138.237.48	33,721		33,721	Jun 14 14:45:40
6月 14, 2020, 6:24 午後	TH01	NAT-TCP-C		2402:c800:fe01:64::	8008	163.138.237.48	50,092		50,092	Jun 14 18:22:51
6月 14, 2020, 5:54 午後	TH01	NAT-TCP-C		2402:c800:fe01:64::	26470	163.138.237.48	55,182		55,182	Jun 14 17:52:29
6月 14, 2020, 8:15 午後	TH01	NAT-TCP-C		2402:c800:fe01:64::	3520	163.138.237.48	37,827		37,827	Jun 14 20:13:17
6月 14, 2020, 10:35 午後	TH01	NAT-TCP-C		2402:c800:fe01:64::	1400	163.138.237.48	46,943		46,943	Jun 14 22:33:50
6月 15, 2020, 12:03 午前	TH01	NAT-TCP-C		2402:c800:fe01:64::	36	163.138.237.48	36,407		36,407	Jun 15 00:01:14
6月 14, 2020, 3:36 午後	TH01	NAT-TCP-C		2402:c800:fe01:64::	443	163.138.237.48	54,580		54,580	Jun 14 15:34:38
6月 14, 2020, 3:36 午後	TH01	NAT-TCP-C		2402:c800:fe01:64::	443	163.138.237.48	53,108		53,108	Jun 14 15:34:34
6月 14, 2020, 10:21 午前	TH01	NAT-TCP-C		2402:c800:fe01:64::	443	163.138.237.48	60,700		60,700	Jun 14 10:19:45
6月 14, 2020, 10:21 午前	TH01	NAT-TCP-C		2402:c800:fe01:64::	443	163.138.237.48	60,698		60,698	Jun 14 10:19:45
6月 14, 2020, 10:21 午前	TH01	NAT-TCP-C		2402:c800:fe01:64::	443	163.138.237.48	60,924		60,924	Jun 14 10:19:46
6月 14, 2020, 12:08 午後	TH01	NAT-ICM-C		2402:c800:fe01:64::	0	163.138.237.48	60,014		60,014	Jun 14 12:06:40
6月 15, 2020, 12:31 午前	TH01	NAT-TCP-C		2402:c800:fe01:64::	443	163.138.237.48	45,310		45,310	Jun 15 00:30:05
6月 14, 2020, 8:01 午後	TH01	NAT-TCP-C		2402:c800:fe01:64::	443	163.138.237.48	49,568		49,568	Jun 14 19:59:37

ダッシュボード(BigQuery+metabase)



SLB64も同一の機器構成で提供可能

SLB64の設定(IPv6アドレス→IPv4サーバプールの設定)をAPI公開することで、サーバのIPv6対応を自動化できるのではないかな？

❗ アイデアはあったものの実験協力者が現れなかったため、検討のみ

Openであることの引き換えにAbuseの可能性

- 送信元の隠蔽
- 日本国内からのアクセスへの偽装

対策:

- NATログ/トラフィックの監視
- 問題が発生した際には、実験協力者の宛先IPv4向けの通信のみ許可するようにアクセス制限を検討

DDoS対策:

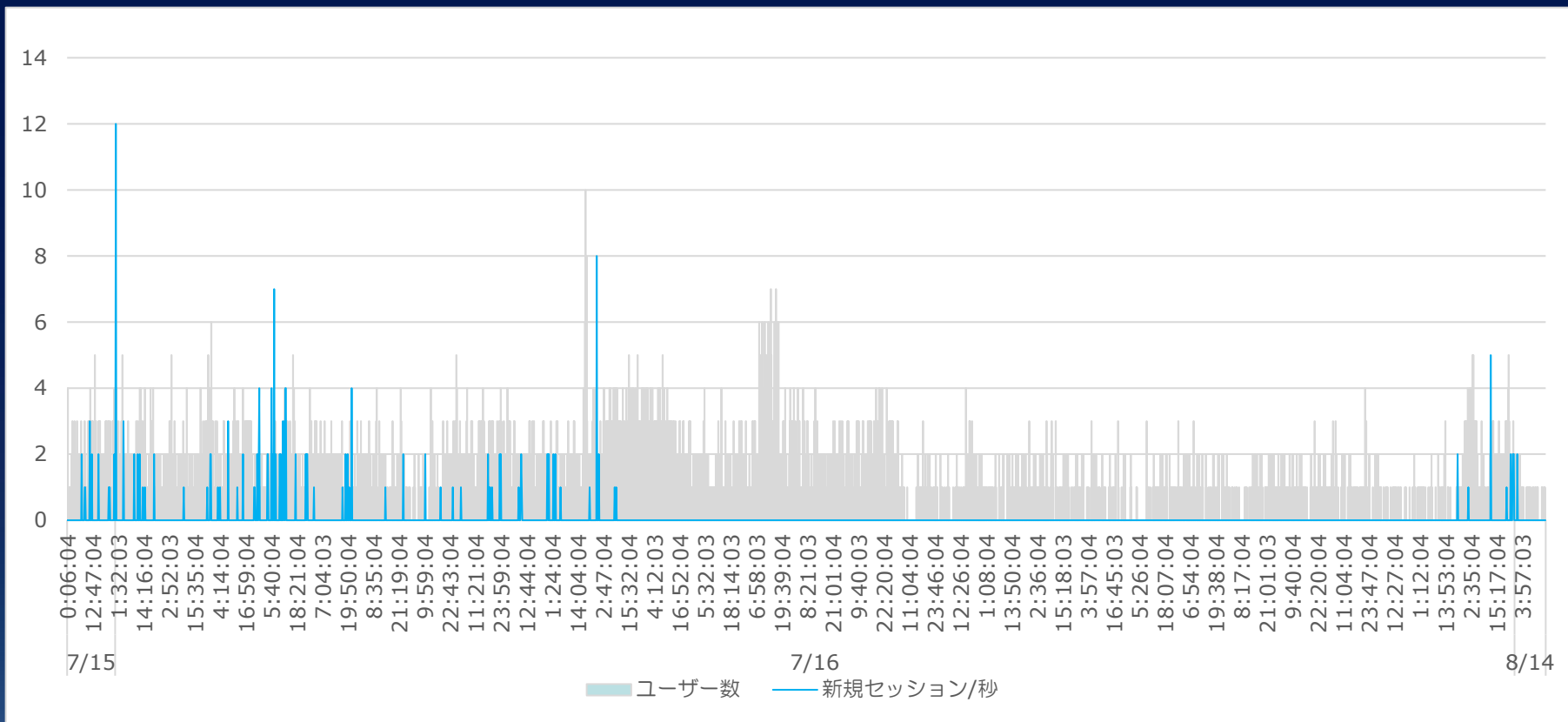
- 今回は実施せず



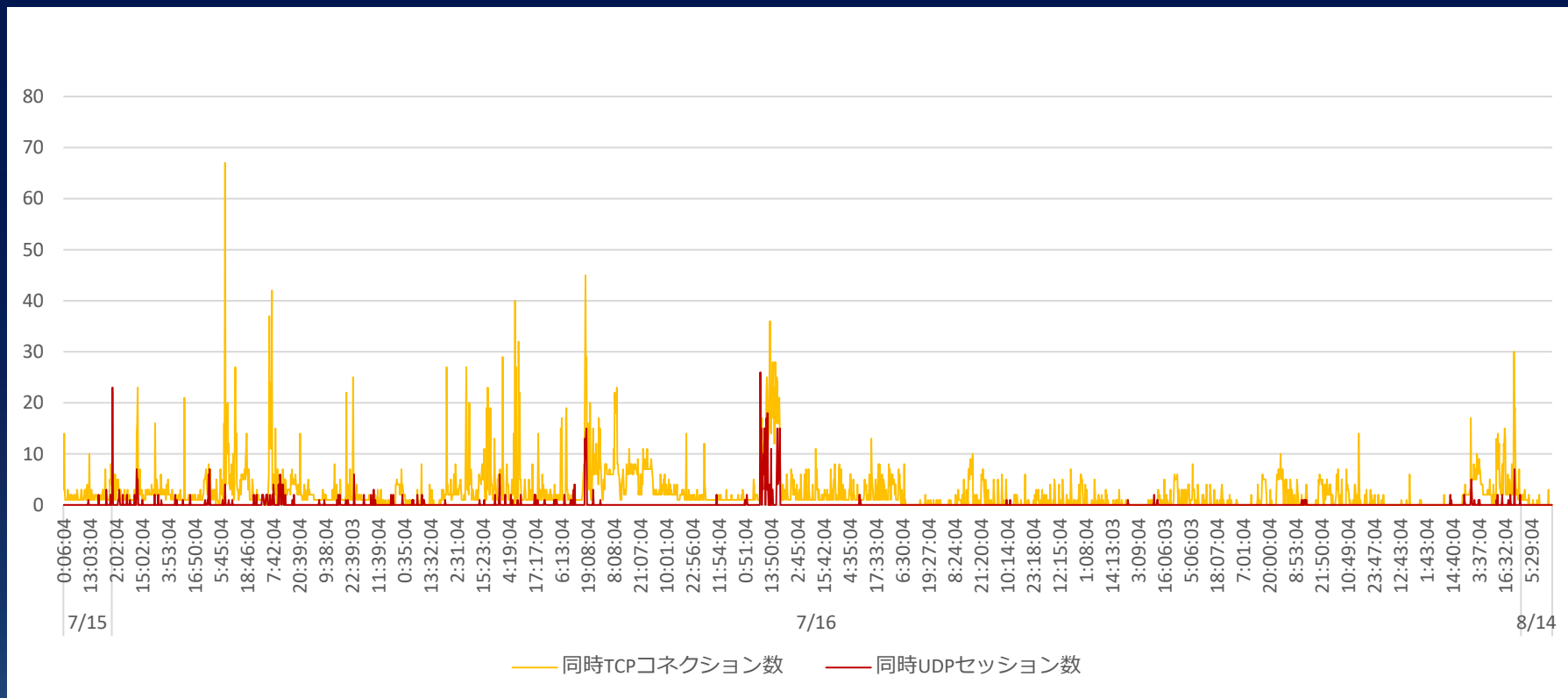
今回の実験期間では問題は発生しなかった

統計情報

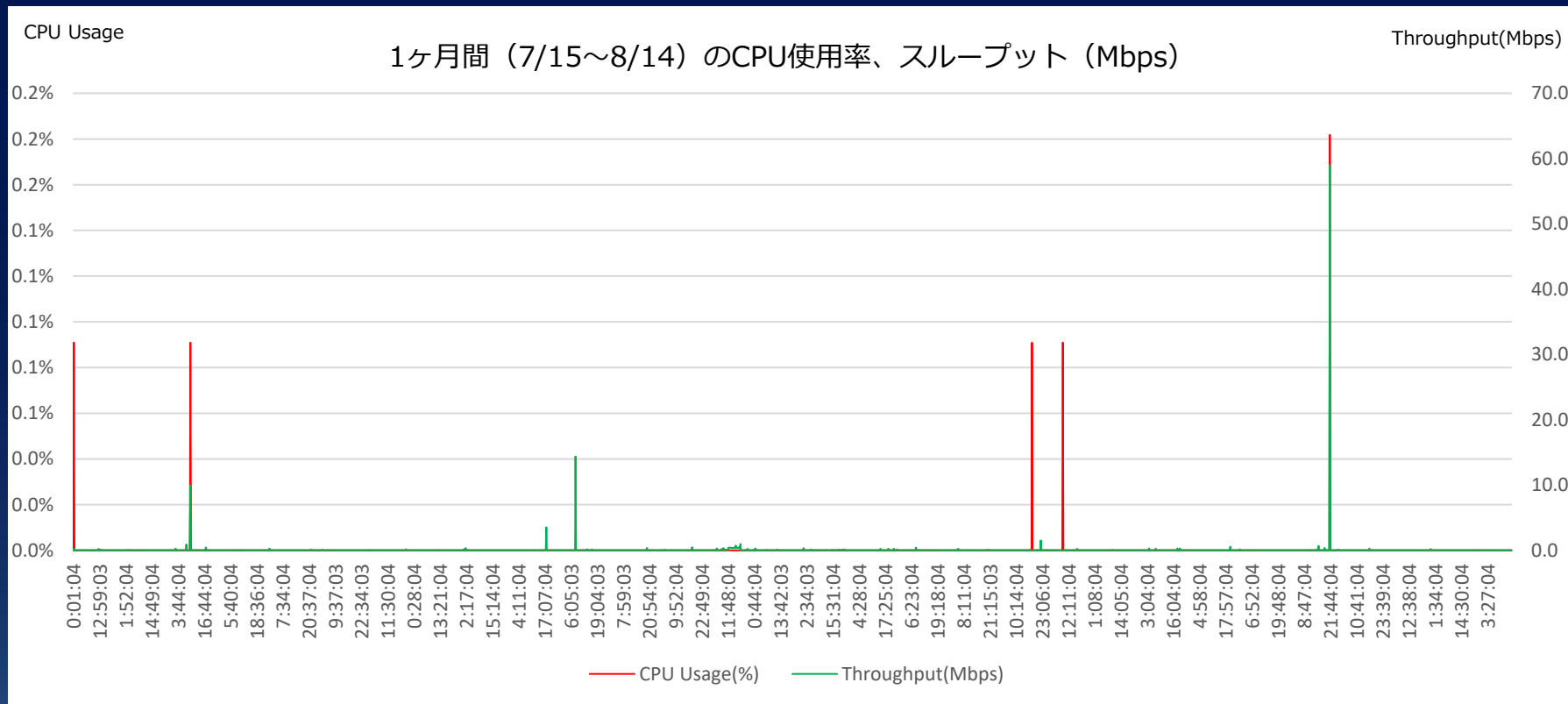
グラフ①ユーザー数・新規コネクション数/秒



グラフ②同時TCPコネクション数・UDPフロー数



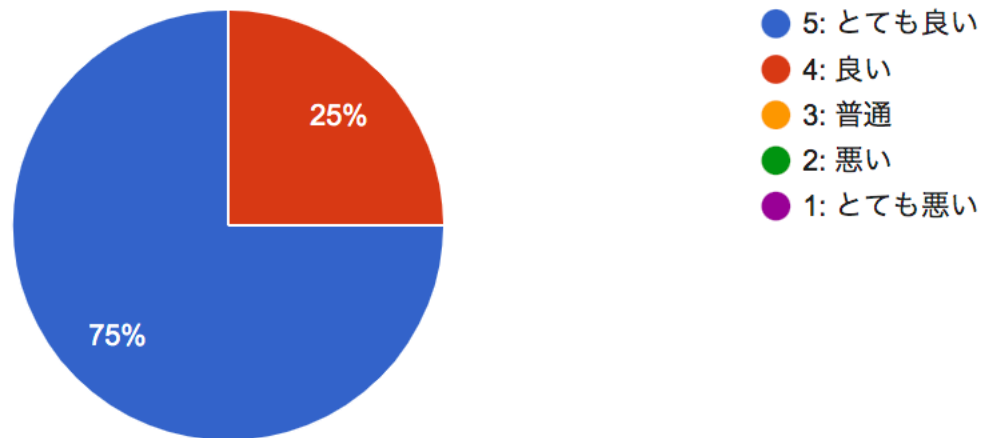
グラフ③CPU使用率、スループット (Mbps)



アンケート結果

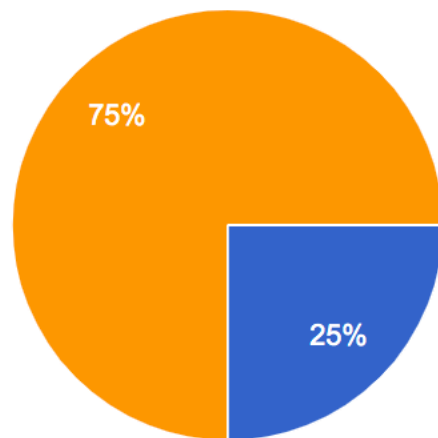
実験の有用性について教えてください(5段階評価)

4 件の回答



Open NAT64/SLB64によるIPv6化をサービスとして評価したとき、どのくらいの価格に値するか感触を教えてください

4件の回答

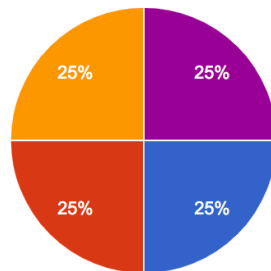


- オンプレ(NAT64/SLB64機器などを自社購入する場合)よりも安ければ使う
- CDNと同程度であれば使う
- CDNよりも安ければ使う

アンケートを実施(4件の回答)

望ましい課金方式について

4 件の回答



- トラフィック課金
- セッション数課金
- AAAAレコード数に応じた課金
- NATログ提供に対して課金(利用は無料だが、NATログの提供は有料)
- ワンショット課金(実験用途など)

具体的な価格感について教えてください

4 件の回答

個人だと年間1000円/AAAAレコードといったところでしょうか...

出来れば、利用自体はRouter53やGoogle cloud DNS程度、ログ利用やそれ以外のオプションについては都度オプション料金などだとありがたい。

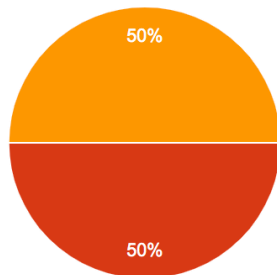
実験目的に使用したいのでただNAT64を使用するだけならワンコイン、一定数のAAAAレコードにつき追加料金、ログ提供で追加料金のようにしてほしい

トラフィック課金としましたが、上限ナシだと怖いですね。ちょっと予測が出来ないです。

アンケートを実施(4件の回答)

1. クラウド型のNAT64/SLB64サービスによるコンテンツのIPv6化について

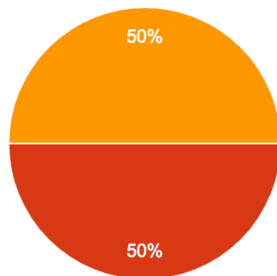
4件の回答



- 実験用途の一時的な構成である
- 1,2年使える繋ぎの技術である(他の構成・技術へ移行すると考える)
- 3年以上使える技術である
- 使えるところはない

2. IPv6 Only インフラに向けたクラウド型のNAT64/DNS64サービスについて

4件の回答



- 実験用途の一時的な構成である
- 1,2年使える繋ぎの技術である(他の構成・技術へ移行すると考える)
- 3年以上使える技術である
- 使えるところはない

IPv4しか提供していないサービスのIPv6対応がこれでできます。たいへんありがたいです。

IPv6利用に制限あるサービスでも利用出来てありがたいです。

できれば今後も負担にならない程度にサービスを継続していただけるとありがたいです。

可能であれば高速な回線へと切り替えて欲しい。

頭では理解していましたが、実際に試すことが出来て、楽しかったです。商用化されても実験ベースで利用できるとありがたいと思いました。

商用化の予定はありますか？



ありません！



最後に

快く機材を提供いただいたA10ネットワークス様に深く感謝します。

A10

Always Secure. Always Available.

今の設備で200万円/月の収益を目指す
AAAAレコード課金の場合

- 今回のAAAAレコード：約10
- NAT64装置の本来の収容能力：10000倍
→20円/月/AAAA 程度？

(トラフィック量の多いAAAAレコードが無い前提)

セッション数課金の場合

- 今回のセッション数：10万セッション/月
- NAT64装置の本来の収容能力：10000倍
→200円/月/10万セッション 程度？