パブリッククラウドでの仮想ルーター自動化例

Shogo Katsurada
@shogokatsurada
2018 Apr 20th

はじめに

- パブリッククラウドで仮想ルータ(ネットワークアプライアンス)を動作させてネットワーク構築する企業も増えてきています

- ネットワーク運用自動化というと構成管理ツールやスクリプティングを中心とした話題になりますが、クラウドでの仮想ルータでは、クラウドで提供されるツールセットも使えます

- ここでは、パブリッククラウドでの自動化の一例をご紹介します

パブリッククラウドで利用できる
仮想ルータ(ネットワークアプライアンス) は様々

AWS

https://www.slideshare.net/AmazonWebServices/networking-state-of-the-union-net205-reinvent-2017

Azure

https://azure.microsoft.com/en-us/blog/new-networking-capabilities-for-a-consistent-connected-and-hybrid-cloud/

ツールセットも…

	オンプレミス
機器セットアップ	• PXE • ZTP
構成管理	• Ansible • Chef • Puppet
スクリプティング	• APIライブラリ(YDK, PyEz,NAPALM..etc)
状態監視	• SNMP • Telemetry
その他	• Cron

… 他にも多数

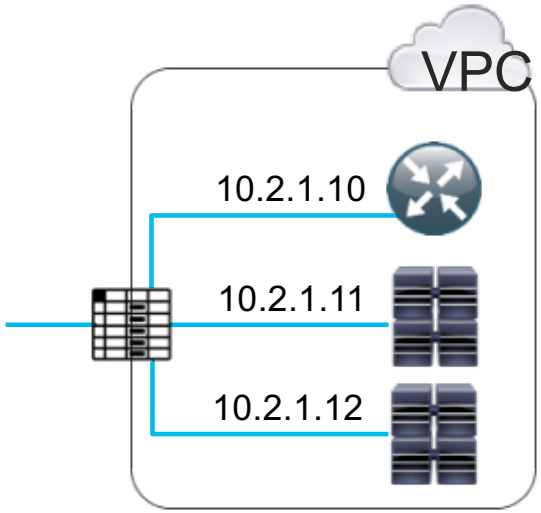
ツールセットも…

	オンプレミス	クラウド環境
機器セットアップ	• PXE • ZTP	• Terraform • AWS CloudFormation • Azure ARM Template
構成管理	• Ansible • Chef • Puppet	
スクリプティング	• APIライブラリ(YDK, PyEz,NAPALM..etc)	• AWS Lambda • Azure Functions
状態監視	• SNMP • Telemetry	• AWS Cloudwatch • Azure monitor
その他	• Cron	• オブジェクトストレージ (AWS S3) • KMS

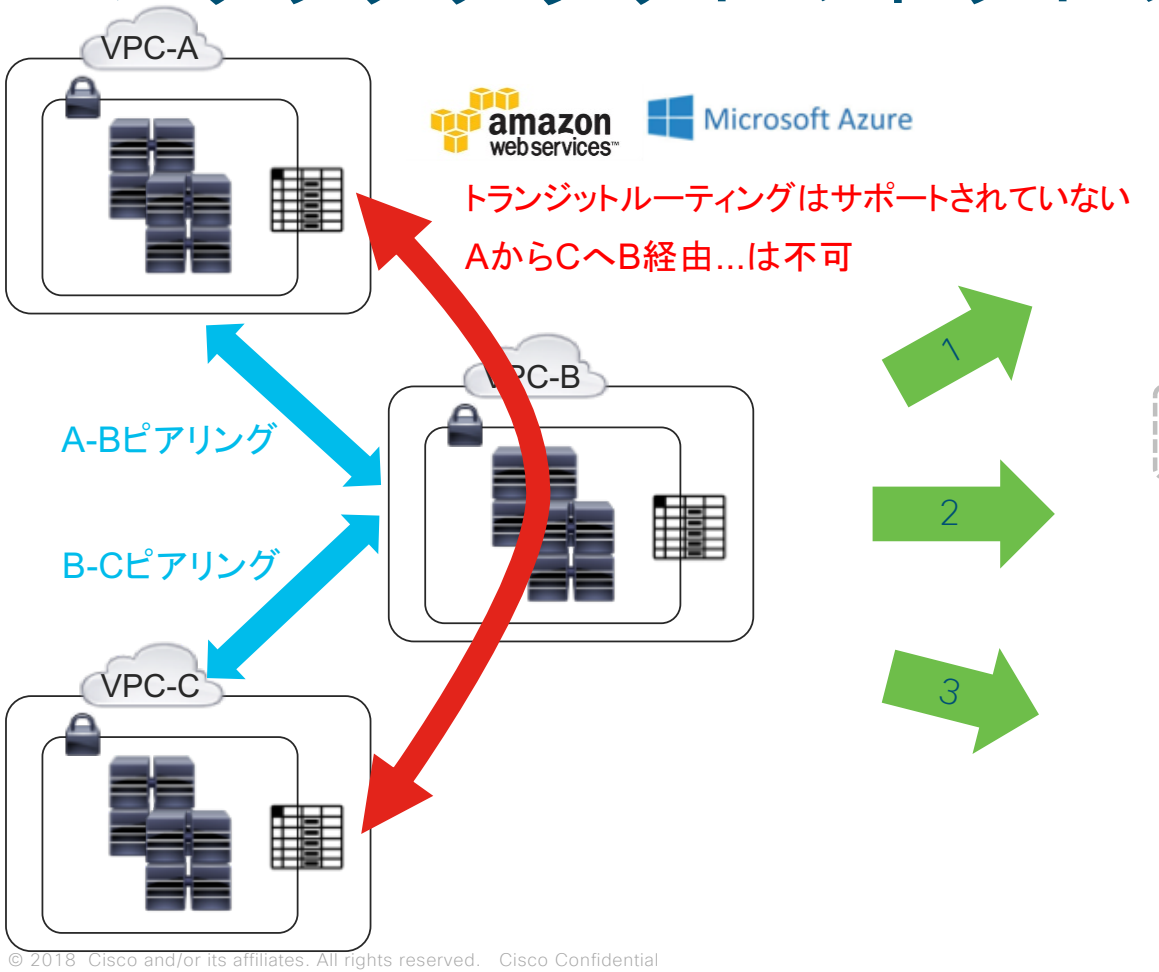
… 他にも多数

パブリッククラウドのネットワーク

- さまざまなお作法・ネットワークの制限がある
  - VPC(Virtual Private Cloud)/ VNET
  - AZ (Availability Zone) / AS(Availability Set)
  - マルチキャスト, ブロードキャストが通らない
    - 使えないプロトコル・機能が…
      - IGP(OSPF..etc)
      - HSRP/VRRP
      - BFD
      - Proxy ARP, Gratuitous ARP
    - GREを使うことで回避できるケースもある



パブリッククラウドのネットワーク – cont.



amazon web services　Microsoft Azure

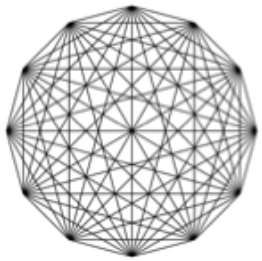
トランジットルーティングはサポートされていない

AからCへB経由…は不可

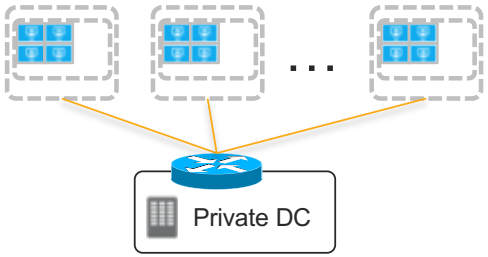
1

2

3



フルメッシュ？

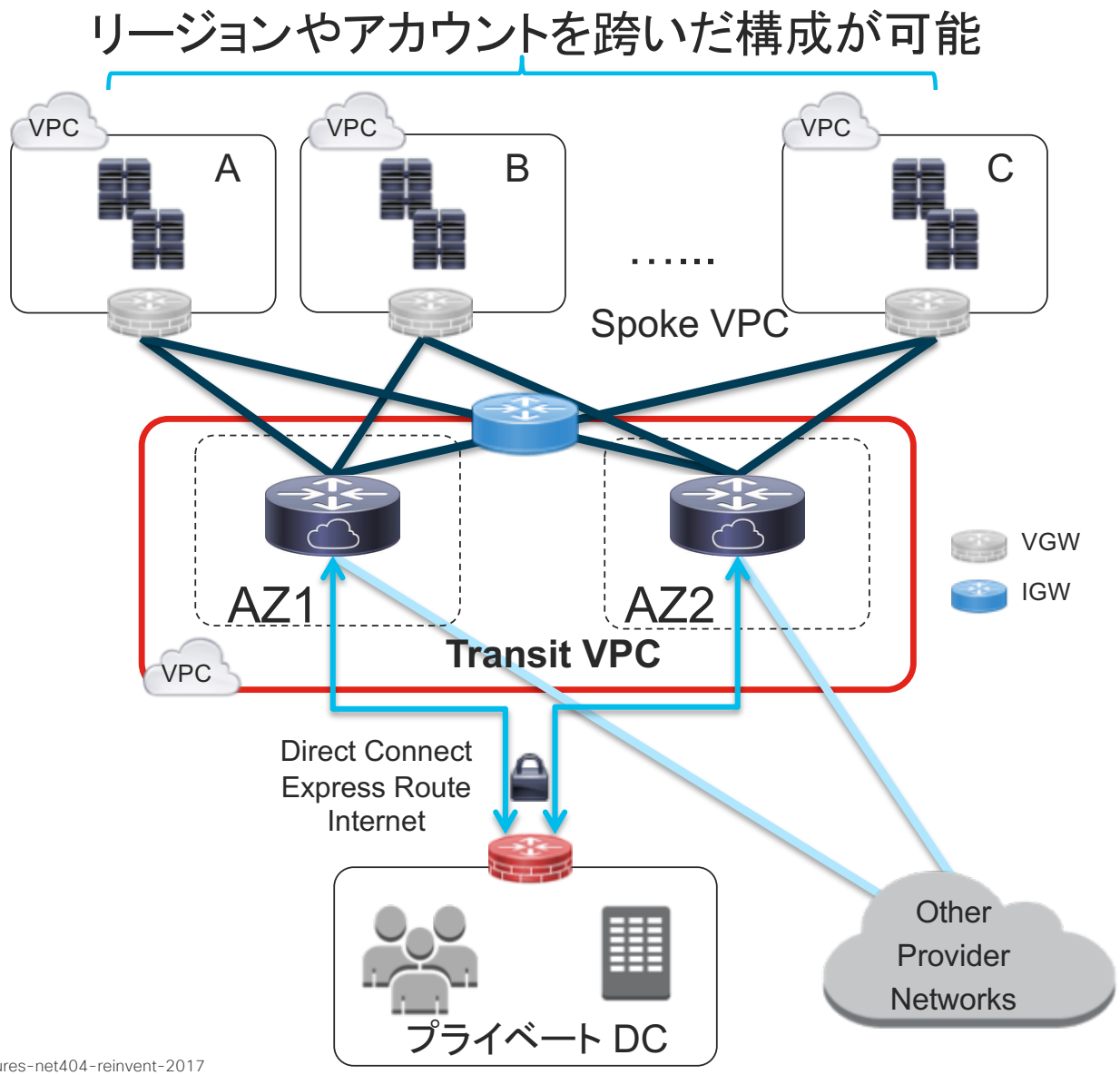


DCでルーティング?

Transit VPC

Transit VPC 構成

- 転送専用のVPC を用意することでVPC間のトランジットルーティングをサポート
- Cisco や Juniper の仮想アプライアンスでドキュメント化されている



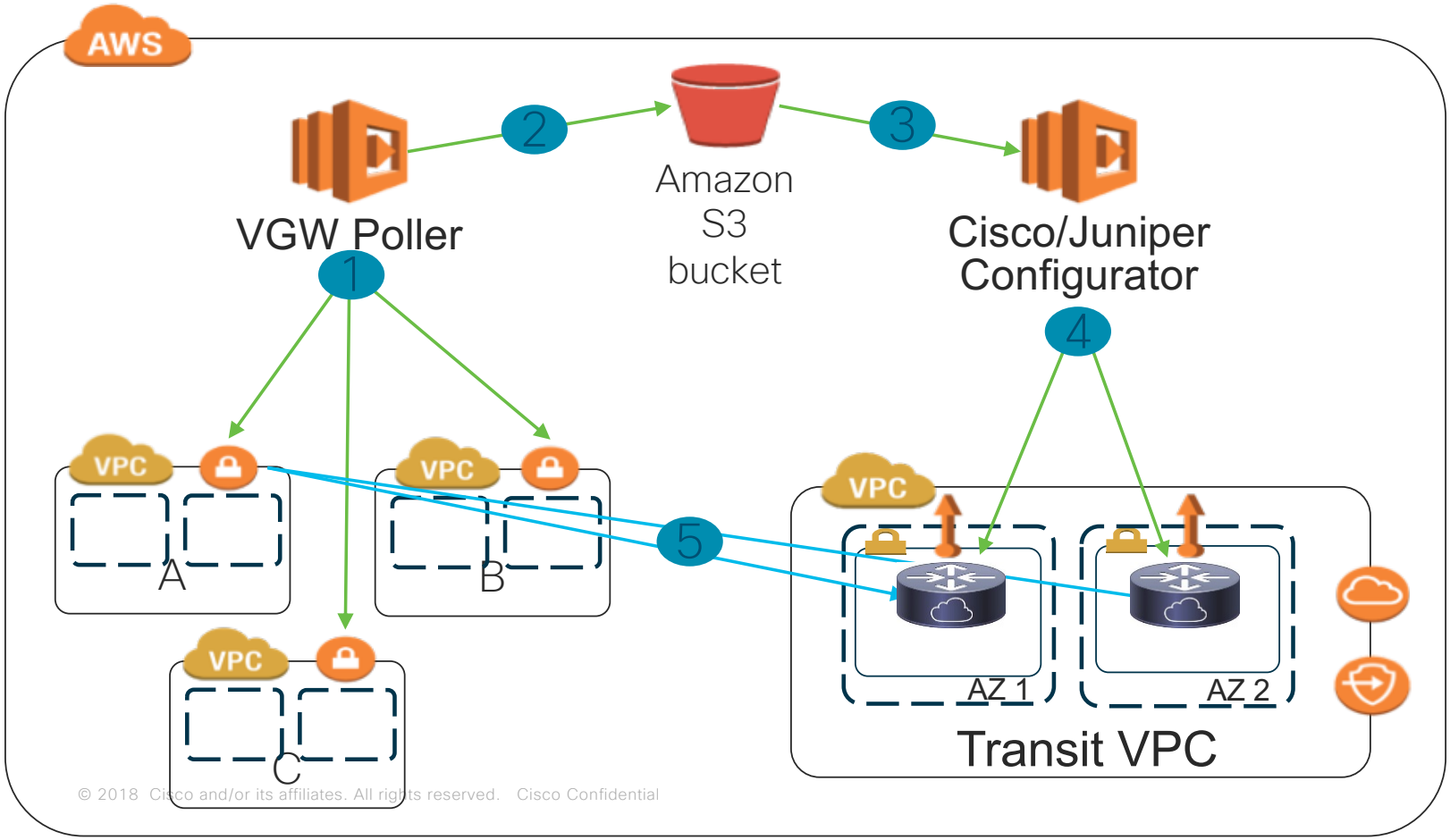
参考: https://www.slideshare.net/AmazonWebServices/networking-many-vpcs-transit-and-shared-architectures-net404-reinvent-2017

Transit VPC の自動化 – 実現できること

- HUBルータ デプロイの自動化
  - トランジットVPCの仮想ルータを立ち上げ
  - 初期設定
    - AZを分けた配置
    - HA構成
- スポークVPCの追加の自動化
  - 手順の自動化
    - 追加したいVPC のVGW で任意の Tag を記載することで自動的に トランジットVPCへ接続設定が完了

次頁

スポークVPC追加 自動化の仕組み



2つのLambdaファンクション

VGW Poller

1) 1分毎に(予め指定した) Tag がついているVGWがあるか確認。あればVPNに必要な設定をクラウド側に投入
2) その後、設定情報を S3 に格納

C/J Configurator

3) S3に格納された情報から、BGP, VPN, インターフェイス等のパラメタからConfigを作成
4) SSH で仮想アプライアンスにConfig 投入

まとめ

- クラウドのツールセットを活用して完成度の高い自動化を実現している例のご紹介
  - スクリプト・テンプレートは公開されているので、カスタマイズも可能

- Ansible は元はサーバ構成管理ツール → ネットワークへの応用
- クラウドサービスの進化は早いのでツールをうまく活用できると自動化が捗るケースも

参考情報

- Transit Network VPC
  https://docs.aws.amazon.com/solutions/latest/cisco-based-transit-vpc/overview.html
- Github
  https://github.com/awslabs/aws-transit-vpc
- CSR1000v Deployment Videos for Public Cloud
  http://cs.co/csr1000v
- vSRX Virtual Firewall-BasedAWS Transit VPC
  https://www.juniper.net/assets/us/en/local/pdf/implementation-guides/8010096-en.pdf


CISCO