amazon web services

Conectividade com AWS utilizando VPC

Conectividade com AWS utilizando VPC

Julho 2016

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Sumário

Introdução

O movimento de adoção de computação em nuvem vem tornando cada vez mais crescente nas corporações e isso faz com que, dependendo da arquitetura utilizada, tem-se a necessidade de conectividade entre infraestrutura on-premises com a AWS.
Através do serviço Amazon VPC (Virtual Private Cloud), que implementa isolamento lógico de rede, é possível realizar essa conexão, provendo assim uma infraestrutura hibrida.

Abaixo as possibilidade de conectividade:

- Hardware VPN – Serviço em alta disponibilidade, gerenciado pela AWS, que permite conexão através de tuneis IPSec;
- AWS Direct Connect – Serviço de conectividade física, através de links privados com a AWS;
- Software VPN – Possibilidade de interconexão de redes, através de softwares/appliance de VPN, os quais estão disponibilizados em sua VPC;

Conceitos

O intuito desse tópico é expor conceitos, os quais serão utilizados no decorrer desse documento.

VPC

Forma de segregação/isolamento de rede na AWS. Permite você criar redes privadas e públicas, assim como segregação de subredes(subnets).

CIDR

Método de alocação de IPs utilizado em VPC.

BGP

Protocolo de roteamento dinâmico, utilizado para roteamento interdominios.

VGW

Serviço que permite interconexão, com ambientes externos/remoto a AWS.

CGW

Representação virtual do dispositivo lado do ambiente on-premises que representa firewall/roteador.

NACL

Camada de segurança opcional para a sua VPC que age como firewall para controle de trafego de entrada de saída. Esse tipo de controle é no nível de subnet, equivalente a firewall stateless.

Security Group

Atua como firewall virtual, o qual controla tráfego de entrada e saída no nível de instâncias, equivalente a um firewall stateful.

VPC Peering Connection

Serviço que permite comunicação/conexão de rede entre VPCs.

Conectividade do seu ambiente on-premises com AWS

Nessa seção será exposto arquiteturas e boas práticas de conexão entre ambientes on-premises e AWS.
Através dessa conectividade, a AWS pode ser entendida como extensão do seu datacenter e com isso seus utilizadores, consumirão os serviços de forma transparente, como se estivesse em rede local.
Um ponto de bastante atenção que deve ser levado em consideração na escolha do range de ip da sua VPC é que não exista sobreposição/conflito nos ranges, para evitar problemas com roteamento de pacotes.

Hardware VPN

Esse serviço de VPN gerenciado pela AWS, consiste em fornecer em alta disponibilidade serviço de tuneis IPSec de VPN, os quais permitem estabelecer conexão com seu ambiente on-premises através da Internet.
Com a utilização desse serviço, surgirão mais acrônimos que são CGW(Customer Gateway) – Representação do ponto de intercomunicação do seu ambiente on-premises e VGW (Virtual Private Gateway) – Representação do serviço do lado da AWS, conforme pode ser observado na Figura 1.

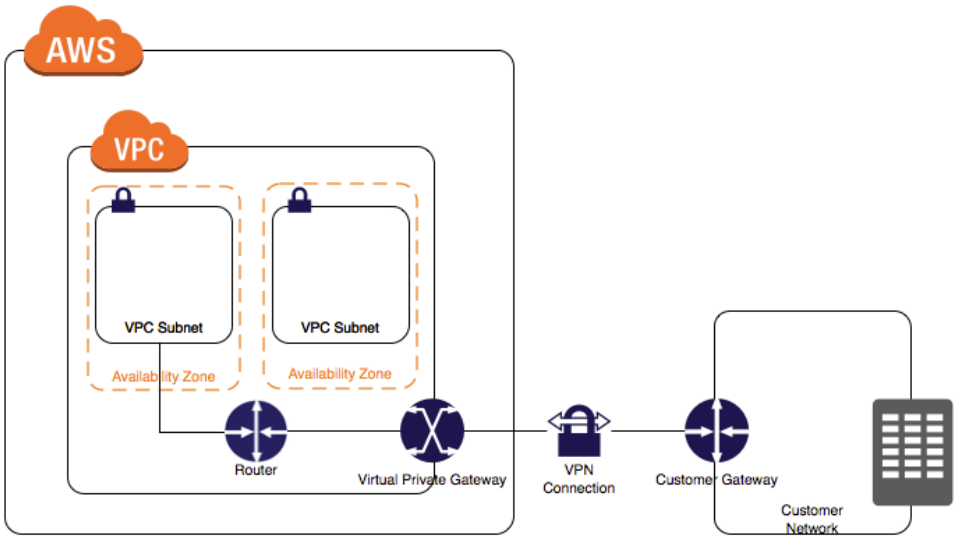

Figura 1: Diagrama básico representação CGW e VGW.

Por ser um serviço em alta disponibilidade, o VGW fornece dois ip para conexão, sendo assim, você pode utilizar dois CGW para que possa ter 4 tuneis IPSec controlados por eBGP em alta disponibilidade, conforme pode ser observado na Figura 2.

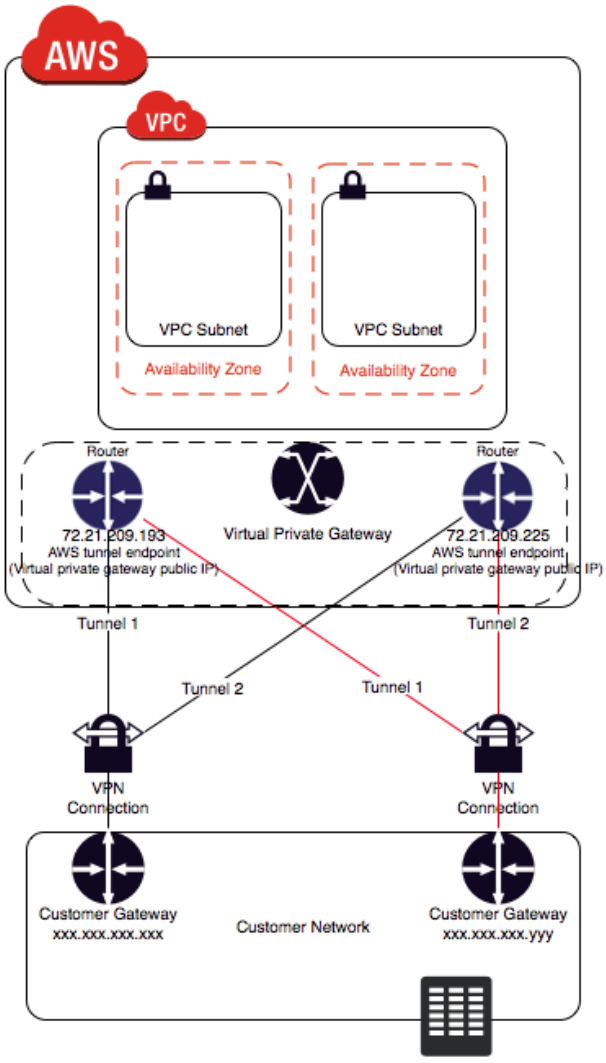

Figura 2: VPN em alta disponibilidade utilizando protocolo de roteamento.

Esse serviço permite ainda que você utilize utilizando rotas estáticas e dinâmicas (utilizando BGP).
Existe uma documentação, o qual expõe passo a passo, como construir esse serviço na AWS, http://bit.ly/2akrj2X.

Caso de Uso
- Serviço de conectividade em alta disponibilidade VPN com a AWS.

Vantagens
- Serviço em alta disponibilidade;
- Reutilização de possível infraestrutura já existente;
- Utilização de conectividade com Internet já existente;
- Suporta BGP e Rotas Estáticas;
- Rápida (em minutos) e fácil adesão e configuração;

Pontos de Atenção
- Variações de latência, velocidade e conectividade, dependentes da Internet;
- Necessidade de possuir dois ativos de rede para possuir alta disponibilidade no túnel.

AWS Direct Connect

O serviço de Direct Connect consiste em você estabelecer conectividade com a AWS, através de links de conexão privados e dedicados. Com a utilização desse tipo de conectividade, você possui benefícios como aumento na velocidade e qualidade da sua conexão.
Atualmente as velocidades de conexões disponíveis, 50, 100, 200, 300, 400 e 500 Mbps, essas conexões são realizadas necessariamente através dos nossos parceiros de Direct Connect (http://amzn.to/29ZQ4Cn), o qual provisionará toda a infraestrutura de conectividade. Existem também as velocidades de 1 ou 10 Gbps, as quais você contacta qualquer fornecedor de conectividade que possui chegada em nosso datacenter para provê essa conexão. Um exemplo de conexão, pode ser observado na Figura 3

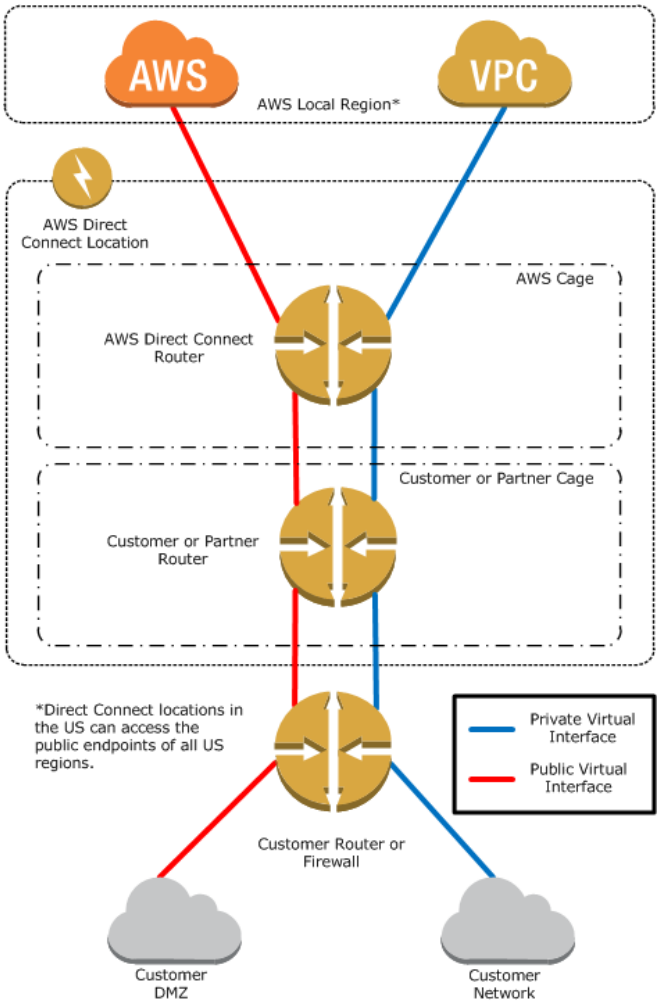

Figura 3: Disposição componentes Direct Connect.

Em diversas regiões, possuímos dois ou mais pontos de conectividade (http://amzn.to/2a2YZCB) dessa forma, você pode possuir alta disponibilidade, utilizando dois links para duas localidades distintas ou ainda utilizando uma VPN.

Caso de Uso

- Conexão direta com AWS, com latências e velocidades controladas.

Vantagens

- Serviço te permite ter alta disponibilidade de conectividade direta;

- Redução de custos com “transfer out”;
- Suporte a BGP peering e politicas de roteamento;
- Velocidade e latência mais controladas;

Pontos de Atenção
- Faz-se necessário o provisionamento de novos links/circuitos de dados;

Software VPN

Na AWS também provê a flexibilidade de você gerenciar os dois pontos da VPN(origem e destino).
Essa opção é recomendada caso possua algum requisito específico que não possua em nosso hardware de VPN ou caso precise gerenciar as duas pontas do túnel.
Possuímos um ecossistema muito vasto de UTMs/Firewall em nosso marketplace (http://amzn.to/29ZQwkj), o qual pode ser utilizado nessa solução.
Lembrando que toda a responsabilidade do gerenciamento desse componente, desde de atualizações e alta disponibilidade fica por conta do cliente.

Caso de Uso
- Conexão com AWS, via Internet, gerenciando as duas pontas da conexão

Vantagens
- Flexibilidade de utilizar alguma tecnologia que já está acostumado a trabalhar;
- Gerenciamento de toda conectividade;

Pontos de Atenção
- Gerenciamento do appliance utilizado na conectividade, desde as atualizações e alta disponibilidade.

Contribuidores

O contribuidor para a construção desse documento é:

- Cláudio Freire Júnior, Arquiteto de Soluções, Amazon Web Services

Conclusão

A Amazon Web Services provê uma plataforma bastante flexível, a qual permite também que você possua diversas opções de conectividade.
No que tange a escolha de qual a conexão ideal, vai depender do caso de uso e da necessidade da arquitetura especifica.