Série de Certificação GCP: 3.5 Implantando e implementando recursos de rede.

Prashanta Paudel

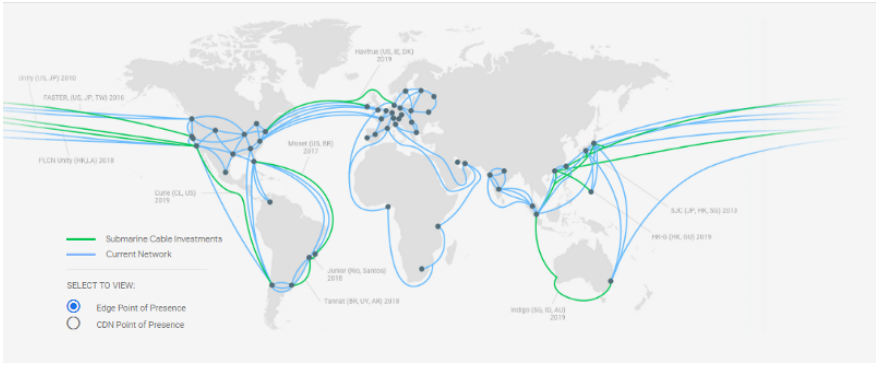
5 de novembro de 2018 · 28 min de leitura

Se olharmos de perto, a parte mais importante da plataforma Cloud é sua infraestrutura de rede, como tudo, desde instâncias até o trabalho da API, porque existe uma rede entre elas.

Cloud é basicamente uma rede remota de dispositivos ou instâncias de computação fornecidos ao usuário através da rede que os conecta ao usuário.

Nós já temos alguns conceitos básicos de quão vasta é a rede do Google em todo o mundo e como eles estão conectados, mas vamos rever os principais pontos da rede.

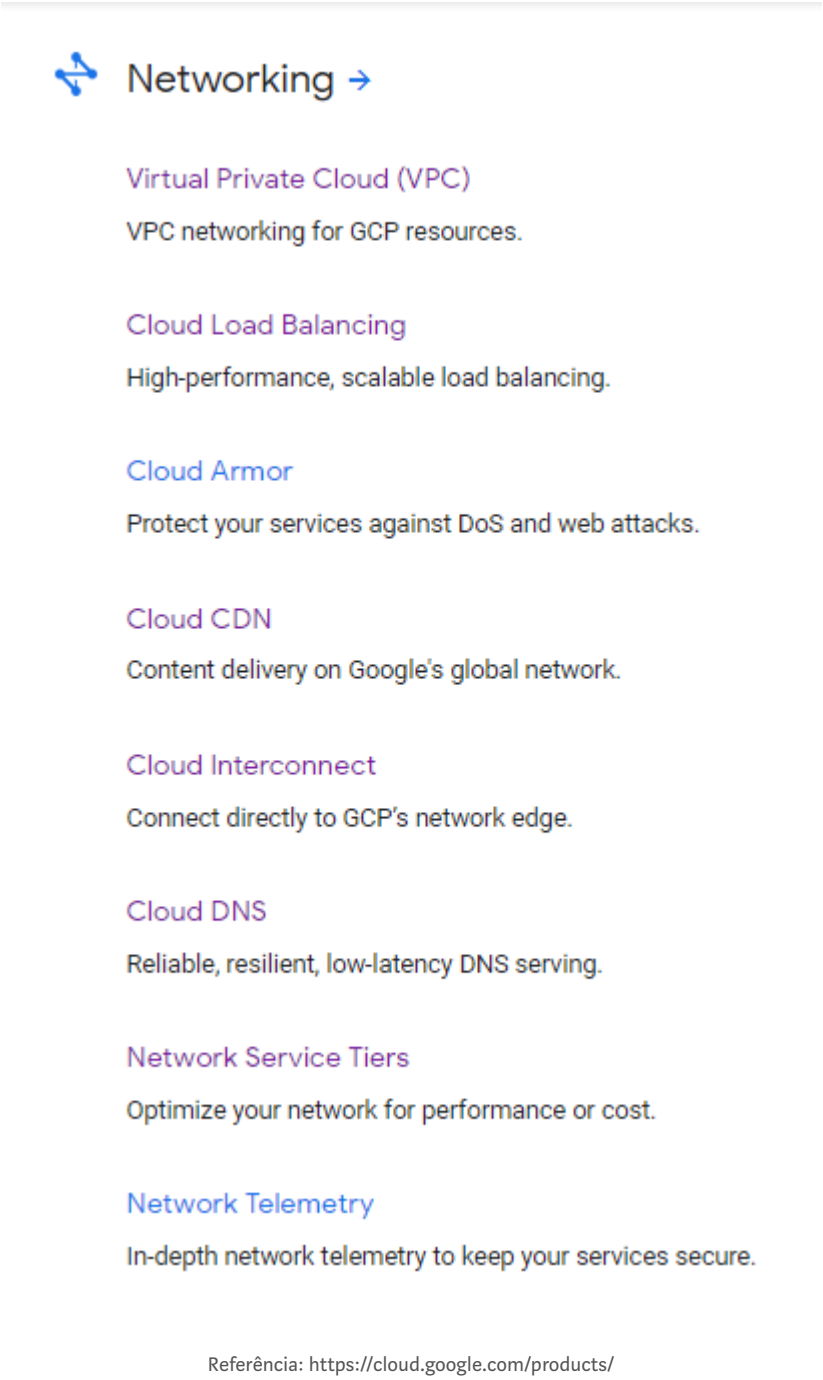
O Google é provavelmente um provedor de rede de nível 1 ou 2, mas como eles só transferem tráfego na rede do Google, não são considerados como ISP. O Google tem uma rede global privada que conecta muitos data centers e POP (ponto de presença). Eles têm



referência: https://cloud.google.com/about/locations/#network-tab

A rede privada do Google conecta seus locais regionais a mais de 100 pontos de presença (POP). O Google Cloud Platform usa tecnologias de sistemas distribuídos e redes definidas por software para hospedar e fornecer serviços em todo o mundo. Como o Google tem uma rede privada global, isso ajudará a tornar seu produto global, vinculando todas as regiões pela rede de alta velocidade.

Os elementos de rede do Google na nuvem são:



Referência: https://cloud.google.com/products/

Regiões e Zonas

Ao desenvolver seu aplicativo no GCP, é muito importante entender regiões e zonas,

Os recursos também são regionais e zonais, portanto você também deve ter uma ideia sobre qual recurso é o que antes de entrar em detalhes.

Uma região é uma localização geográfica subdividida em zonas.

Embora alguns dos recursos do GCP sejam globais, outros podem estar restritos por região ou zona.

Recursos regionais podem ser usados em qualquer lugar dentro da mesma região, enquanto recursos zonais podem ser usados em qualquer lugar dentro da mesma zona. Alguns exemplos disso são:

Recursos Globais:

- Imagens
- Instantâneos
- Rede VPC
- Firewalls
- Rotas

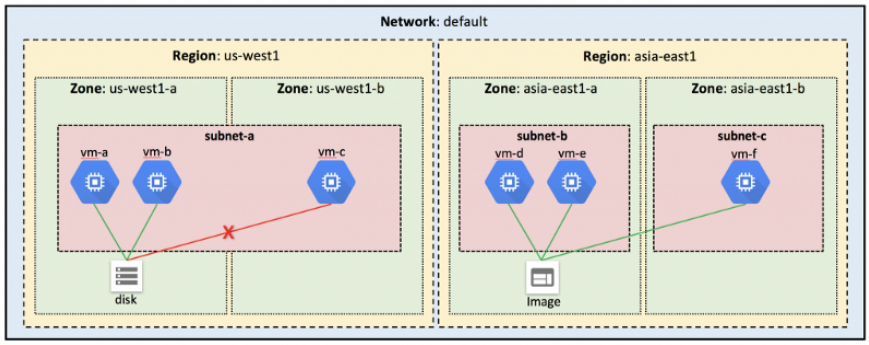
Recursos regionais:

- Endereços IP externos estáticos
- Sub-redes

Recursos Zonais:

- Instâncias (VMs)
- Discos Persistentes

Por exemplo, posso anexar um disco de uma instância a outra dentro da mesma zona, mas não posso fazer isso entre zonas. No entanto, como imagens e instantâneos são recursos globais, posso usá-los em várias zonas da mesma região.



referência: https://www.networkmanagementsoftware.com/google-cloud-platform-gcp-networking-fundamentals/

Nuvem privada virtual

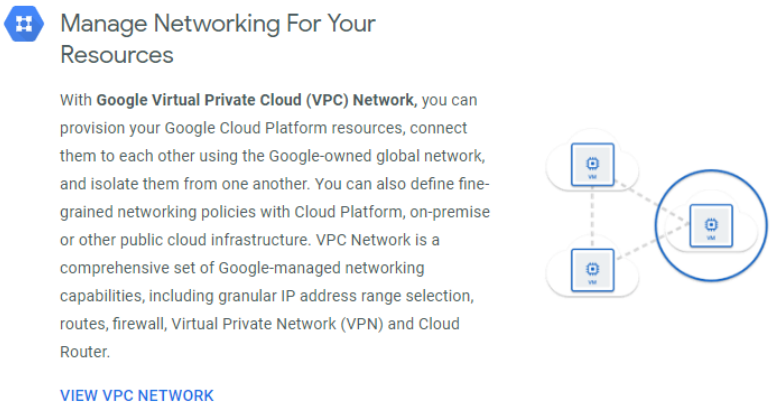
Com a ajuda da nuvem privada do Google Virtual (VPC), você pode

- provisionamento de recursos do GCP
- conectar recursos

- isolar recursos
- fazer políticas refinadas para acessar recursos e rede

VPC consiste em

- Endereço de IP
- firewall
- VPN
- roteador de nuvem



Referência: https://cloud.google.com/products/networking/

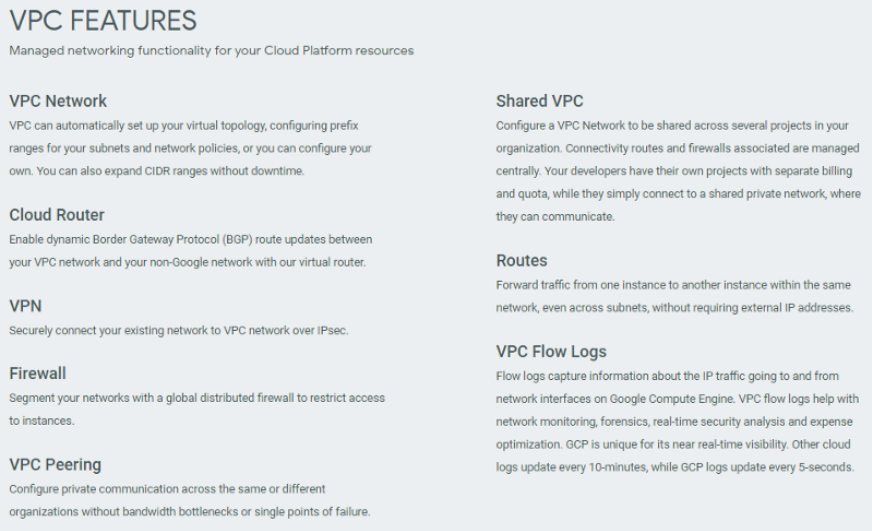
Um espaço privado no Google Cloud Platform

A Virtual Private Cloud (VPC) oferece flexibilidade para dimensionar e controlar como as cargas de trabalho se conectam regional e globalmente. Quando você conecta seus recursos locais ou remotos ao GCP, você terá acesso global às suas VPCs sem precisar replicar políticas administrativas ou de conectividade em cada região.

VPC é

- **Global**
- **Compartilhável**
- **Expansível**
- **Privado**

- **Transparente**

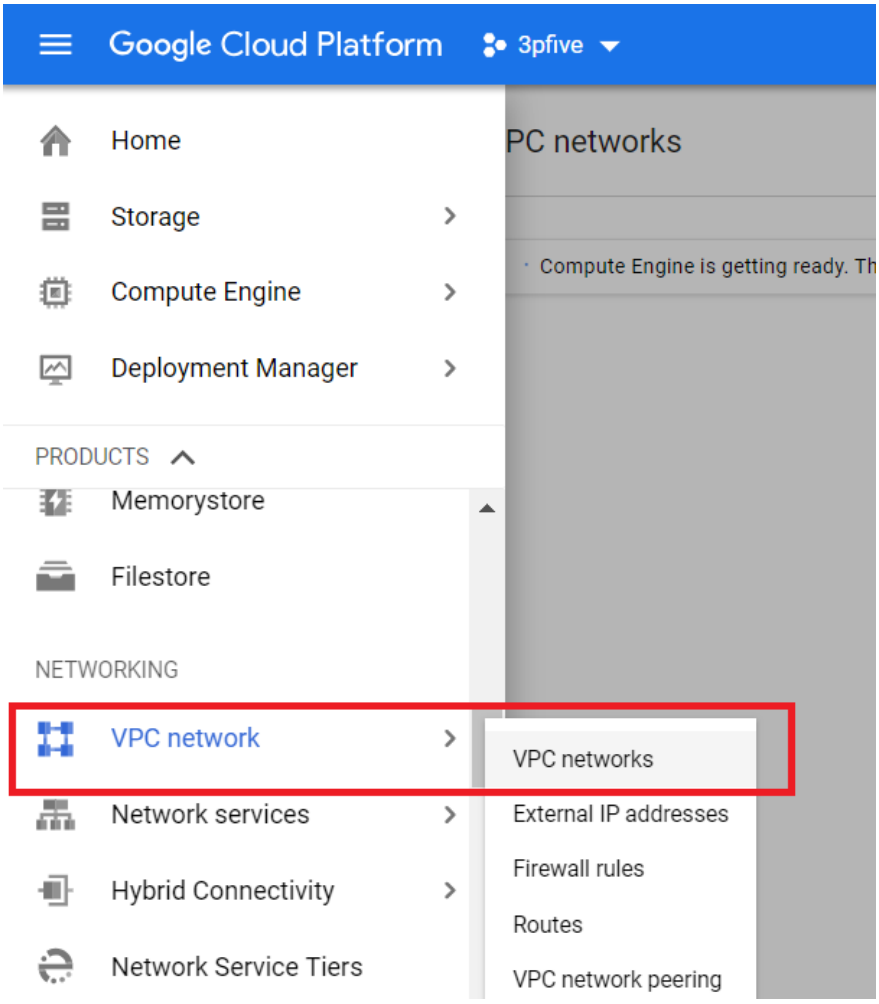


Referência: https://cloud.google.com/vpc/

Criando um VPC com sub-redes. (por exemplo, VPC de modo personalizado, VPC compartilhado)

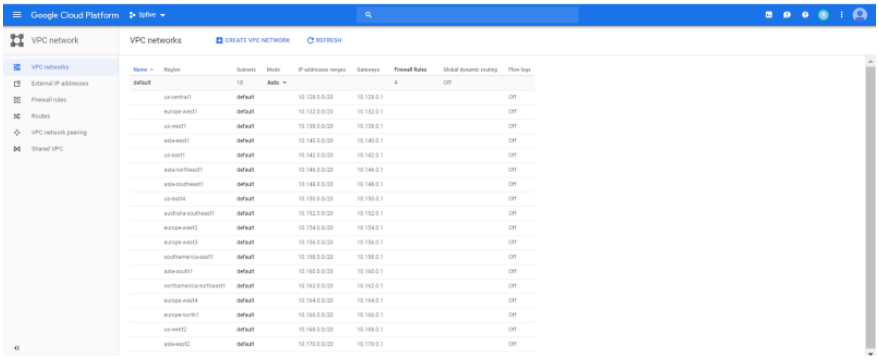
Para criar uma nuvem privada virtual, primeiro você deve ter uma configuração de projeto feita. Por favor, siga meus blogs anteriores para configurar um projeto no GCP.

Depois de criar um projeto, clique na rede VPC em NETWORKING e vá para o Dashboard



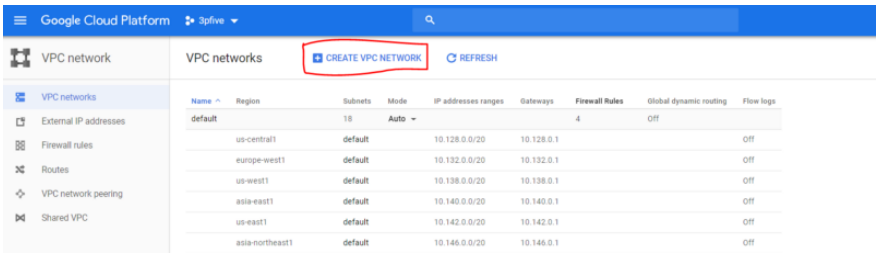
Redes VPC

Então você verá um intervalo de rede VPC padrão.

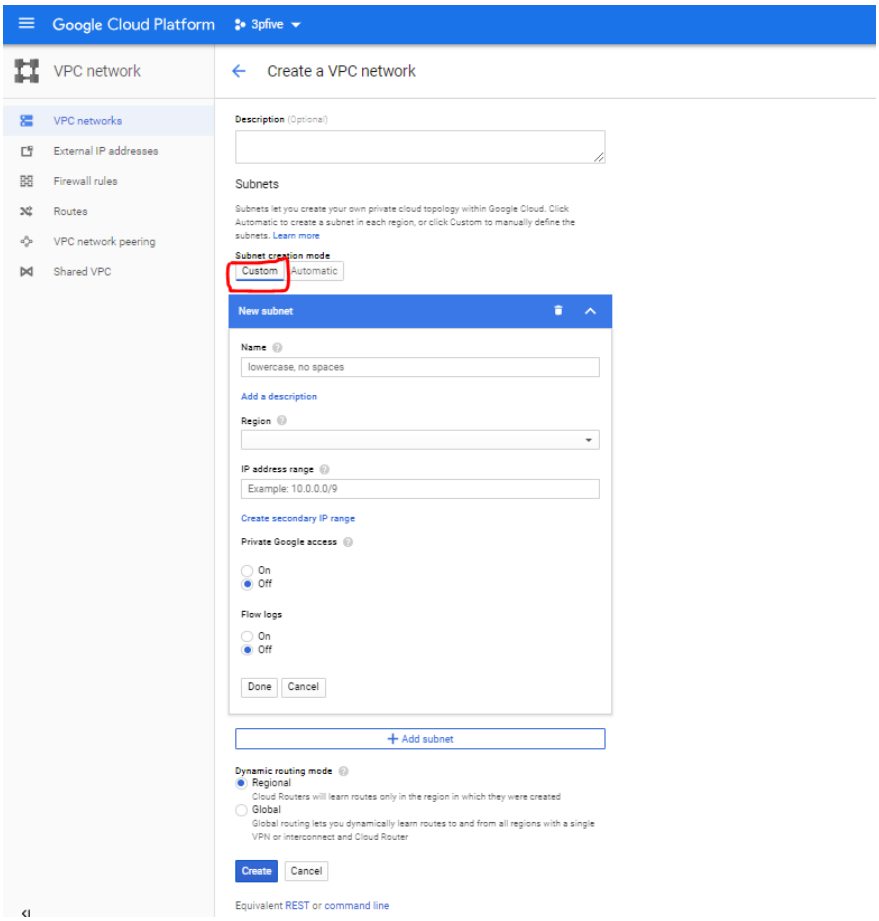


Redes VPC padrão

Agora clique em CREATE VPC NETWORK no topo da página



Então você será presenteado com uma página de configuração VPC



Configuração VPC

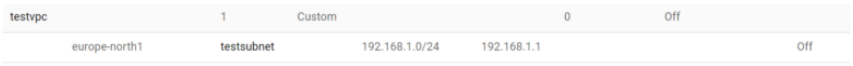
Na descrição, você pode nomear tudo o que puder lembrar facilmente.

Agora você tem duas opções,

- **Sub-rede automática**
- **Sub-rede personalizada**

A sub-rede automática criará uma sub-rede em cada região, enquanto o personalizado criará apenas nessas regiões e, com o IP, você declarará explicitamente.

Vamos para o **costume** no momento e definir a rede 192.168.0.1/24



sub-rede personalizada

Visão geral da rede Virtual Private Cloud (VPC)

Uma rede VPC, às vezes chamada apenas de "rede", é uma versão virtual de uma rede física, como uma rede de data center. Ele fornece conectividade para sua máquina virtual Compute Engine instâncias (VM) , aglomerados Kubernetes Motor , casos App Engine Flex e outros recursos em seu projeto .

Os projetos podem conter várias redes VPC. **Novos projetos começam com uma `default` rede que possui uma sub-rede em cada região (uma rede de modo automático).**

Especificações

As redes VPC têm as seguintes propriedades:

- Redes VPC, incluindo suas rotas associadas e regras de firewall, são recursos globais . Eles *não* estão associados a nenhuma região ou zona específica.
- *As sub-redes* são recursos regionais. Cada sub-rede define um intervalo de endereços IP. Para mais informações sobre redes e sub-redes, consulte redes e sub-redes .
- O tráfego para e de instâncias pode ser controlado com regras de firewall de rede .
- Os recursos dentro de uma rede VPC podem se comunicar uns com os outros usando endereços IPv4 internos (privados), sujeitos às

regras de firewall de rede aplicáveis. Para mais informações, consulte a comunicação dentro da rede .

- Instâncias com endereços IP internos podem se comunicar com APIs e serviços do Google . Para mais informações, consulte Opções de acesso privado .
- Administração de rede pode ser protegida usando funções de gerenciamento de identidade e acesso (IAM) .
- Uma organização pode usar o Shared VPC para manter uma rede VPC em um projeto host comum. Os membros autorizados do IAM de outros projetos na mesma organização podem criar recursos que usam sub-redes da rede compartilhada VPC.
- As redes VPC podem ser conectadas a outras redes VPC em diferentes projetos ou organizações usando Peering de Rede VPC .
- As redes VPC podem ser conectadas com segurança em ambientes híbridos usando o Cloud VPN ou o Cloud Interconnect .
- As redes VPC suportam apenas tráfego unicast IPv4 . Eles **não** suportam tráfego broadcast , multicast ou IPv6 *na* rede. No entanto, o IPv6 pode ser usado para *alcançar* recursos na rede. Por exemplo, os endereços IPv6 podem ser atribuídos a um balanceador de carga global e o ambiente padrão do App Engine oferece suporte a IPv6.

Redes e sub-redes

Cada rede VPC consiste em uma ou mais partições de intervalo IP úteis chamadas *sub - redes* ou *sub - redes* . Cada sub-rede está associada a uma região . As redes podem conter uma ou mais sub-redes em qualquer região. Redes de modo automático criam sub-redes em cada região automaticamente. Redes de modo personalizado iniciam sem sub-redes, dando a você controle total sobre a criação de sub-redes. Para obter informações sobre as diferenças entre as redes de modo automático e personalizado, consulte os tipos de redes VPC .

Por si só, as redes VPC não possuem intervalos de endereços IP associados a elas. Ao criar uma sub-rede, você deve definir um intervalo de endereços IP primário. Você pode, opcionalmente, definir um ou mais *intervalos secundários* :

- **Intervalo principal** : você pode escolher qualquer bloco RFC 1918 CIDR privado para o intervalo de endereços IP principal da sub-rede, sujeito a essas regras . Suas sub-redes não precisam formar um bloco CIDR contíguo predefinido, mas você pode fazer isso se desejar. Por exemplo, as redes de modo automático criam sub-redes que se encaixam em um intervalo de IP de modo automático predefinido .
- **Intervalos secundários** : você pode definir até cinco intervalos de endereços IP secundários para uso com o alias de IP .

Quando você cria um recurso no GCP, escolhe uma rede e uma sub-rede. Para recursos que não sejam modelos de instância, você também seleciona uma zona ou região . Selecionar uma zona seleciona implicitamente sua região pai. Como as sub-redes são objetos regionais, a região selecionada para um recurso determina as sub-redes que podem ser usadas:

- O processo de criação de uma instância envolve a seleção de uma zona, uma rede e uma sub-rede. As sub-redes disponíveis para seleção são restritas àquelas na região selecionada. O GCP atribui à instância um endereço IP do intervalo de endereços disponíveis na sub-rede.
- O processo de criação de um grupo de instâncias gerenciadas envolve a seleção de uma zona ou região, dependendo do tipo de grupo e de um modelo de instância. Os modelos de instância disponíveis para seleção são restritos àqueles cujas sub-redes definidas estão na mesma região selecionada para o grupo de instâncias gerenciadas.
- Modelos de instância são recursos globais. O processo de criação de um modelo de instância envolve a seleção de uma rede e uma sub-rede. Se você selecionar uma rede de modo automático, poderá escolher "sub-rede automática" para adiar a seleção de sub-rede a uma disponível na região selecionada de qualquer grupo de instâncias gerenciadas que usaria o modelo, porque as redes de modo automático têm uma sub-rede em cada região definição.
- O processo de criação de um cluster de contêiner do Kubernetes envolve a seleção de uma zona ou região (dependendo do tipo de cluster), uma rede e uma sub-rede. As sub-redes disponíveis para seleção são restritas àquelas na região selecionada.

Terminologia de rede e sub-rede

Os termos "sub-rede" e "sub-rede" são sinônimos. Eles são usados de forma intercambiável no console do GCP, nos `gcloud` comandos e na documentação da API.

Nota: Uma sub-rede ou sub-rede **não** é a mesma coisa que uma rede (VPC). **Redes e sub-redes (sub-redes) são *tipos diferentes* de objetos no GCP.**

Tipos de redes VPC

Existem dois tipos de redes VPC:

- Quando uma rede de **modo automático** é criada, uma sub-rede de cada região é criada automaticamente dentro dela. Essas sub-redes criadas automaticamente usam um conjunto de intervalos IP predefinidos que se encaixam no `10.128.0.0/9` bloco CIDR. À medida que novas regiões do GCP se tornam disponíveis, novas sub-redes nessas regiões são automaticamente adicionadas às redes do modo automático usando um intervalo de IPs desse bloco. Além das sub-redes criadas automaticamente, você pode adicionar mais sub-redes manualmente às redes de modo automático, nas regiões escolhidas, usando intervalos de IP fora de `10.128.0.0/9` .
- Quando uma rede de **modo personalizado** é criada, nenhuma sub-rede é criada automaticamente. Esse tipo de rede fornece controle total sobre suas sub-redes e intervalos de IP. Você decide quais sub-redes criar, nas regiões escolhidas e usando os intervalos de IP especificados .

Cada projeto começa com uma `default` rede de modo automático.

Você pode alternar uma rede do modo automático para o modo personalizado . Essa conversão é unidirecional; redes de modo personalizado não podem ser alteradas para redes de modo automático. Analise com atenção as considerações sobre as redes de modo automático para ajudá-lo a decidir que tipo de rede atende às suas necessidades.

Considerações para redes de modo automático

Redes de modo automático são fáceis de configurar e usar, e são adequadas para casos de uso com esses atributos:

- Ter sub-redes criadas automaticamente em cada região é útil.
- Os intervalos de IP predefinidos das sub-redes não se sobrepõem aos intervalos de IP que você utilizaria para finalidades diferentes (por exemplo, conexões VPN de nuvem com recursos locais).

No entanto, as redes de modo personalizado são mais flexíveis e são mais adequadas à produção. Os atributos a seguir destacam casos de uso em que as redes de modo personalizado são recomendadas ou necessárias:

- Ter uma sub-rede criada automaticamente em cada região não é necessária.
- Novas sub-redes criadas automaticamente à medida que novas regiões se tornam disponíveis podem se sobrepor a endereços IP usados por sub-redes criadas manualmente ou por rotas estáticas, ou podem interferir no planejamento geral da rede.
- Você precisa ter controle total sobre as sub-redes criadas em sua rede VPC, incluindo regiões e intervalos de endereços IP usados.
- Você planeja conectar redes VPC usando Peering de Rede VPC ou Cloud VPN . Como as sub-redes de cada rede de modo automático usam o mesmo intervalo predefinido de endereços IP , você não pode conectar redes de modo automático entre si.

Importante: As redes de produção devem ser planejadas com antecedência. É recomendado que você use redes de modo personalizado em produção.

Sub-redes e intervalos de IP

Os intervalos de IP podem ser atribuídos a sub-redes que você cria de acordo com estas regras:

- Cada sub-rede deve ter um intervalo de endereços principal, que é um bloco CIDR RFC 1918 válido .
- As sub-redes na mesma rede devem usar intervalos de IP exclusivos. As sub-redes em redes *diferentes* , mesmo no mesmo projeto, podem reutilizar os mesmos intervalos de endereços IP.
- Ao criar uma sub-rede manualmente, você pode usar qualquer intervalo CIDR RFC 1918 sujeito a estas restrições:
- As sub-redes na mesma rede do GCP devem ter intervalos de IP exclusivos.
- Os intervalos de IP para todas as sub-redes devem ser exclusivos entre as redes VPC conectadas entre si pela Peering de Rede VPC ou VPN Cloud.
- Os intervalos de IP para redes locais conectadas por meio do Cloud VPN ou do Cloud Interconnect não devem entrar em conflito com os intervalos de IP de qualquer sub-rede. As rotas de sub-rede devem ter o destino mais específico.
- Os intervalos de IP usados pelas sub-redes não podem entrar em conflito com os referenciados por uma rota estática.
- Ao criar sub-redes adicionais em uma rede de modo automático , suas sub-redes criadas manualmente **devem** usar um intervalo de IP *fora* do `10.128.0.0/9` bloco CIDR. Esse bloco é reservado para os principais intervalos IP de sub-redes criadas automaticamente.
- Você pode atribuir um ou mais intervalos de IP secundários a uma sub-rede. Esses intervalos secundários são reservados para instâncias de VM na sub-rede configuradas com aliases de IP . Os intervalos secundários podem ser qualquer bloco CIDR RFC 1918 sujeito às mesmas restrições discutidas no ponto anterior.
- Os intervalos de IP **não** precisam ser contíguos de sub-rede para sub-rede na mesma rede.
- Intervalos de IP para sub-redes na mesma rede **não** precisam ser membros de um bloco CIDR contíguo maior. Por exemplo, uma sub-rede pode usar `10.0.0.0/8` enquanto outra sub-rede na mesma rede pode usar `192.168.0.0/16` .
- O tamanho mínimo do CIDR para uma sub-rede é `/29` .

IPs reservados

Cada sub-rede tem quatro endereços IP reservados em seu intervalo de IP primário:

Endereço ReservedDescriptionExampleNetworkPrimeiro endereço no intervalo de IP principal da sub-rede `10.1.2.0` no `10.1.2.0/24` endereço GatewaySecond padrão no intervalo de IP principal da sub - rede `10.1.2.1` na `10.1.2.0/24` segunda à última reserva Endereço de penúltimo endereço na faixa de IP principal da sub-rede `10.1.2.254` no `10.1.2.0/24` endereço BroadcastLast na primária Faixa de IP para a sub-rede `10.1.2.255` em `10.1.2.0/24`

Nota: Não há endereços IP reservados nos intervalos de IP secundários .

Intervalos de IP do modo automático

Esta tabela lista os intervalos de IP para as sub-redes criadas automaticamente em uma rede de modo automático . Intervalos IP para essas sub-redes cabem dentro do `10.128.0.0/9` bloco CIDR. Redes de modo automático são criadas com uma sub-rede por região no momento da criação e receberão automaticamente novas sub-redes em novas regiões. Portanto, partes não utilizadas de `10.128.0.0/9` são reservadas para uso futuro do GCP.

Intervalo IP de Região (CIDR) Gateway Padrão Utilizadores Úteis (Inclusivo) asia-east110.140.0.0 / 2010.140.0.110.140.0.2 a 10.140.15.253asia-east210.170.0.0 / 2010.170.0.110.170.0.2 a 10.170.15.253asia -northeast110.146.0.0 / 2010.146.0.110.146.0.2 a 10.146.15.253asia-south110.160.0.0 / 2010.160.0.110.160.0.2 a 10.160.15.253asia-southeast110.148.0.0 / 2010.148.0.110.148.0 .2 a 10.148.15.253australia-sudeste110.152.0.0 / 2010.152.0.110.152.0.2 a 10.152.15.253europe-north110.166.0.0 / 2010.166.0.110.166.0.2 a 10.166.15.253europe-west110.132.0. 0 / 2010.132.0.110.132.0.2 a 10.132.15.253europe-west210.154.0.0 / 2010.154.0.110.154.0.2 a 10.154.15.253europe-west310.156.0.0 / 2010.156.0.110.156.0.2 a 10.156. 15.253europe-west410.164.0.0 / 2010.164.0.110.164.0.2 a 10.164.15.253northamerica-northeast110.162.0.0 / 2010.162.0.110.162.0.2 a 10.162.15.253southamerica-east110.158.0.0 / 2010.158.0.110.158.0.2 a 10.158.15.253us-central110.128.0.0 / 2010.128.0.110.128.0.2 a 10.128.15.253us-

east110.142.0.0 / 2010.142.0.110.142.0.2 a 10.142. 15.253us-east410.150.0.0 / 2010.150.0.110.150.0.2 a 10.150.15.253us-west110.138.0.0 / 2010.138.0.110.138.0.2 a 10.138.15.253us-west210.168.0.0 / 2010.168.0.110 .168.0.2 a 10.168.15.253

Rotas e regras de firewall

Rotas

Rotas definem caminhos para pacotes que saem de instâncias (tráfego de saída). As rotas no GCP são divididas em duas categorias: geradas pelo sistema e personalizadas. Esta seção descreve brevemente os dois tipos de rotas geradas pelo sistema. Você também pode criar rotas personalizadas na sua rede. Veja a visão geral das rotas para obter detalhes completos sobre o roteamento no GCP.

Cada nova rede começa com dois tipos de rotas geradas pelo sistema:

- A rota padrão define um caminho para o tráfego deixar a rede VPC. Ele fornece acesso geral à Internet para VMs que atendem aos requisitos de acesso à Internet . Ele também fornece o caminho típico para o Google Private Access .
- Uma rota de sub-rede é criada para cada um dos intervalos de IP associados a uma sub-rede. Cada sub-rede tem pelo menos uma rota de sub-rede para seu intervalo de IP principal e rotas de sub-rede adicionais são criadas para uma sub-rede se você adicionar intervalos de IP secundários a ela. Rotas de sub-rede definem caminhos para o tráfego atingir as VMs que usam as sub-redes.

Importante: Você não pode remover rotas de sub-rede manualmente. Consulte a seção de rotas de sub - rede da visão geral de rotas para obter detalhes sobre como as rotas de sub-rede são criadas ou excluídas.

Modo de roteamento dinâmico

Cada rede VPC possui um *modo de roteamento dinâmico* associado que controla o comportamento de todos, se for o Cloud Routers . Os Cloud Routers compartilham rotas com sua rede VPC e aprendem rotas

dinâmicas personalizadas de redes conectadas quando você conecta sua rede VPC a outra rede com um túnel VPN de Nuvem usando roteamento dinâmico , Interconexão Dedicada ou Interconexão de Parceiro .

- **O roteamento dinâmico regional** é o padrão. Nesse modo, as rotas para os recursos locais aprendidos por um determinado Cloud Router na rede VPC se aplicam apenas às sub-redes na mesma região que o Cloud Router. A menos que modificados por anúncios personalizados, cada Cloud Router compartilha apenas as rotas para sub-redes em sua região com sua contraparte local.
- **O roteamento dinâmico global** altera o comportamento de todos os Cloud Routers na rede, de modo que as rotas para os recursos locais que eles aprendem estejam disponíveis em todas as sub-redes da rede VPC, independentemente da região. A menos que modificados por anúncios personalizados, cada Cloud Router compartilha rotas para todas as sub-redes da rede VPC com sua contraparte local.

Veja anúncios personalizados para obter informações sobre como o conjunto de rotas compartilhadas por um Cloud Router pode ser personalizado.

O modo de roteamento dinâmico pode ser definido quando você cria uma rede VPC ou a modifica. Você pode alterar o modo de roteamento dinâmico de regional para global e vice-versa sem restrições. Consulte usando redes VPC para obter instruções.

Cuidado: Alterar o modo de roteamento dinâmico tem o potencial de interromper o tráfego dentro da rede ou ativar ou desativar rotas de maneiras inesperadas. Revise cuidadosamente a função de cada Cloud Router antes de alterar o modo de roteamento dinâmico.

Regras de firewall

As regras de firewall aplicam-se ao tráfego de saída (saída) e de entrada (entrada) na rede. As regras de firewall controlam o tráfego, mesmo que estejam totalmente dentro da rede, como a comunicação de instância para instância.

Toda rede VPC possui duas regras de firewall implícitas . Uma regra implícita permite a maior parte do tráfego de saída e a outra nega todo o tráfego de entrada. Você não pode excluir as regras implícitas, mas pode substituí-las pelas suas. O GCP sempre bloqueia algum tráfego, independentemente das regras de firewall. Para mais informações, consulte tráfego bloqueado .

Veja a visão geral das regras de firewall para mais informações.

Você pode monitorar qual regra de firewall permitiu ou negou uma conexão específica. Veja Registro de Regras de Firewall para mais informações.

Comunicação dentro da rede

As rotas de sub-rede geradas pelo sistema definem os caminhos para o envio de tráfego entre instâncias dentro da rede usando endereços IP internos (privados). Para que uma instância possa se comunicar com outra, as regras de firewall apropriadas também devem ser configuradas, pois toda rede tem uma regra de firewall de negação implícita para o tráfego de ingresso .

Exceto para a `default` rede, você deve criar explicitamente regras de firewall de entrada de prioridade mais alta para permitir que as instâncias se comuniquem umas com as outras. A `default` rede inclui várias regras de firewall, além das implícitas , incluindo a `default-allow-internal` regra, que permite a comunicação de instância para instância na rede. A `default` rede também vem com regras de entrada permitindo protocolos como RDP e SSH.

As regras que acompanham a `default` rede também são apresentadas como opções para você aplicar a novas redes no modo automático criadas usando o Console do GCP.

Requisitos de acesso à Internet

Os critérios a seguir devem ser satisfeitos para que uma instância tenha acesso à Internet de saída:

- A rede deve ter uma rota de *gateway de Internet padrão* válida ou uma rota personalizada cujo intervalo de IP de destino seja o mais

geral (`0.0.0.0/0`). Esta rota simplesmente define o caminho para a Internet. Veja Rotas para mais informações sobre rotas.

- As regras de firewall devem permitir o tráfego de saída da instância. A menos que seja substituído por uma regra de prioridade mais alta, a regra de permissão implícita para o tráfego de saída permite o tráfego de saída de todas as instâncias.
- Um dos seguintes itens deve ser verdadeiro:
- A instância deve ter um endereço IP externo. Um IP externo pode ser atribuído a uma instância quando ela é criada ou depois de criada .
- Outra instância na rede deve servir como um gateway NAT .

Exemplo de rede VPC

O exemplo a seguir ilustra uma rede de modo personalizado com três sub-redes em duas regiões:

- **Subnet1** é definido como `10.240.0.0/24` na região us-west1.
- Duas instâncias de VM na zona us-west1-a estão nesta sub-rede. Seus endereços IP vêm da faixa disponível de endereços na *subnet1* .
- **A sub** - **rede2** é definida como `192.168.1.0/24` na região us-east1.
- Duas instâncias de VM na zona us-east1-a estão nesta sub-rede. Seus endereços IP vêm da faixa disponível de endereços na *subnet2* .
- **A sub** - **rede3** é definida como `10.2.0.0/16` também na região us-east1.
- Uma instância de VM na zona us-east1-a e uma segunda instância na zona us-east1-b estão na *sub-rede3* , cada uma recebendo endereços IP de seu intervalo disponível. Como as sub-redes são recursos regionais, as instâncias podem ter suas interfaces de rede associadas a qualquer sub-rede na mesma região que contém suas zonas.

Visão geral compartilhada do VPC

A VPC compartilhada permite que uma organização conecte recursos de vários projetos a uma rede VPC comum , para que eles possam se comunicar de maneira segura e eficiente usando IPs internos dessa rede. Quando você usa o Shared VPC, designa um projeto como um *projeto de host* e anexa um ou mais outros *projetos de serviço* a ele. As redes VPC no projeto host são chamadas de *redes compartilhadas VPC* . Recursos elegíveis de projetos de serviço podem usar sub-redes na rede VPC compartilhada.

A VPC compartilhada permite que os administradores da organização deleguem responsabilidades administrativas, como a criação eo gerenciamento de instâncias, para os Administradores de Projetos de Serviços, enquanto mantêm o controle centralizado dos recursos da rede, como sub-redes, rotas e firewalls. Este modelo permite que as organizações:

- Implemente uma prática recomendada de segurança de menor privilégio para administração de rede, auditoria e controle de acesso. Os Administradores de VPCs compartilhados podem delegar tarefas de administração de rede a Administradores de Rede e Segurança na rede de VPC Compartilhada, sem permitir que os Administradores de Projetos de Serviços façam alterações com impacto na rede. Os administradores de projetos de serviços só têm a capacidade de criar e gerenciar instâncias que usam a rede VPC compartilhada. Consulte os administradores e a seção do IAM para obter mais detalhes.
- Aplique e imponha políticas de controle de acesso consistentes no nível da rede para vários projetos de serviço na organização enquanto delega responsabilidades administrativas. Por exemplo, os administradores de projeto de serviço podem ser administradores de instância de computação em seus projetos, criando e excluindo instâncias que usam sub-redes aprovadas no projeto de host de VPC compartilhada.
- Use projetos de serviço para separar os centros de orçamento ou de custo interno. Consulte a seção de faturamento para mais detalhes.

Conceitos

Organizações e Projetos

A VPC compartilhada conecta projetos dentro da mesma organização . Os projetos de host e de serviço participantes não podem pertencer a organizações diferentes. Consulte a hierarquia de recursos do GCP para obter mais informações sobre organizações e projetos.

Um projeto que participa do Shared VPC é um *projeto de host* ou um *projeto de serviço* :

- Um **projeto de host** contém uma ou mais redes VPC compartilhadas . Um administrador de VPC compartilhado deve primeiro habilitar um projeto como um projeto de host. Depois disso, um Administrador de VPC Compartilhado pode anexar um ou mais *projetos de serviço* a ele.
- Um **projeto de serviço** é qualquer projeto que tenha sido anexado a um projeto de host por um Administrador de VPC Compartilhado. Este anexo permite que ele participe do VPC compartilhado. É uma prática comum ter vários projetos de serviço operados e administrados por diferentes departamentos ou equipes em sua organização.
- Um projeto não pode ser simultaneamente um host e um projeto de serviço. Assim, um projeto de serviço não pode ser um projeto de host para futuros projetos de serviço.
- Você pode criar e usar vários projetos de host; no entanto, cada projeto de serviço só pode ser anexado a um único projeto de host. Veja o exemplo de vários projetos de host para uma ilustração.

Para maior clareza, um projeto que não participa do Shared VPC é chamado de **projeto autônomo** . Isso enfatiza que não é um projeto hospedeiro nem um projeto de serviço.

Redes

Uma **rede VPC compartilhada** é uma rede VPC definida em um projeto de host e disponibilizada como uma rede compartilhada centralmente para recursos elegíveis em projetos de serviço. As redes VPC compartilhadas podem ser automáticas ou personalizadas , mas as redes herdadas não são suportadas.

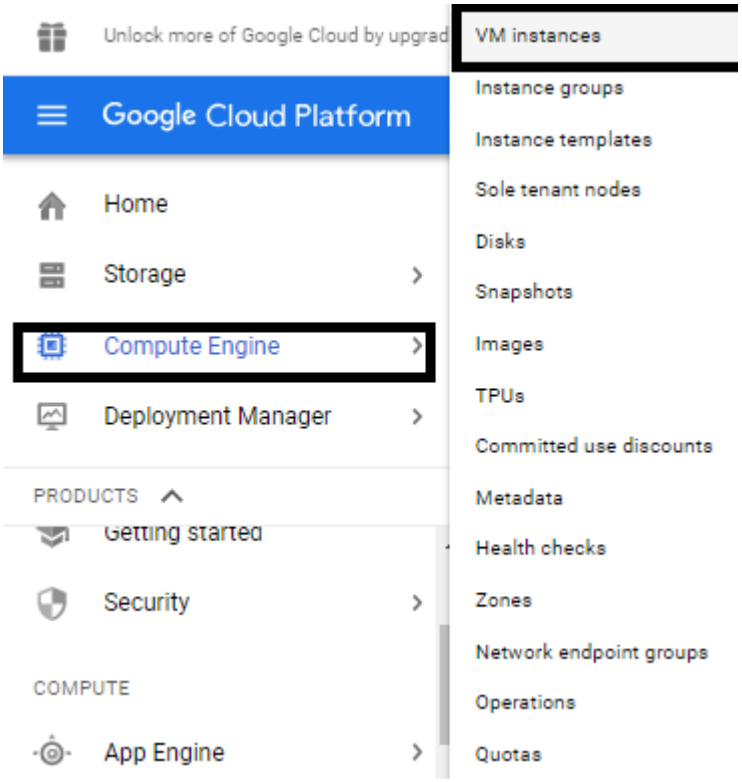
Quando um projeto de host é habilitado, **todas as suas redes VPC existentes se tornam redes VPC compartilhadas, e qualquer nova rede criada nele também será automaticamente uma rede compartilhada VPC** . Assim, um único projeto de host pode ter mais de uma rede compartilhada VPC.

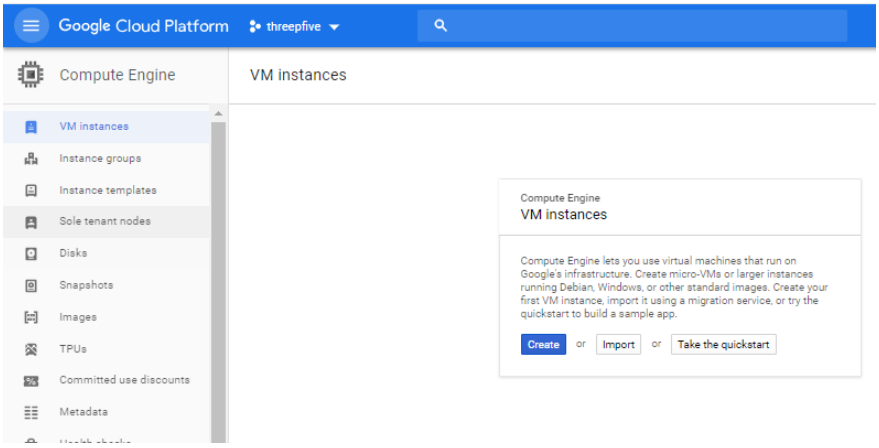
Projetos de host e serviço são conectados por anexos **no nível do projeto** . As sub-redes das redes de VPC compartilhadas no projeto de host podem ser acessadas pelos administradores do projeto de serviço, conforme descrito na próxima seção, administradores e IAM .

- -

Lançamento de uma instância do Compute Engine com configuração de rede personalizada (por exemplo, endereço IP somente interno, acesso privado do Google, endereço IP externo e privado estático, tags de rede)

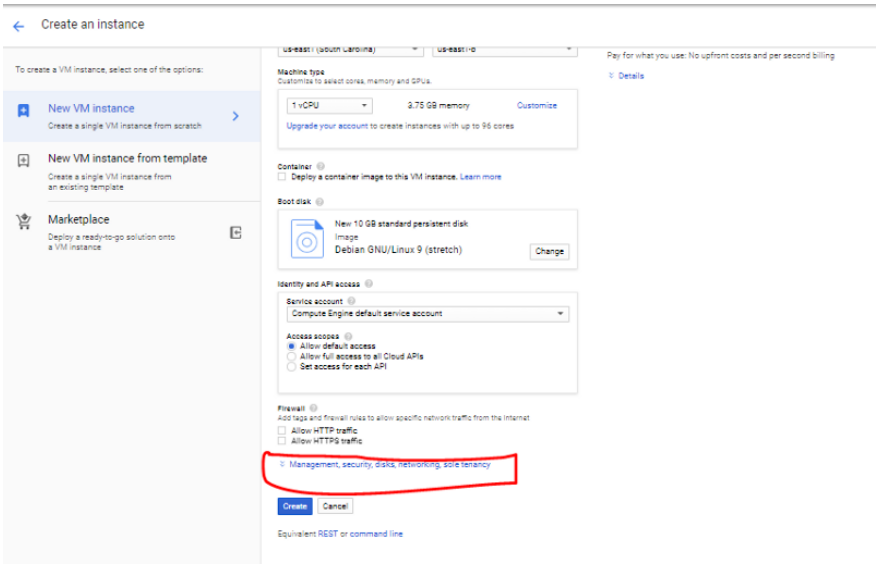
Primeiro, crie uma VM indo para a página principal> compute Engine>





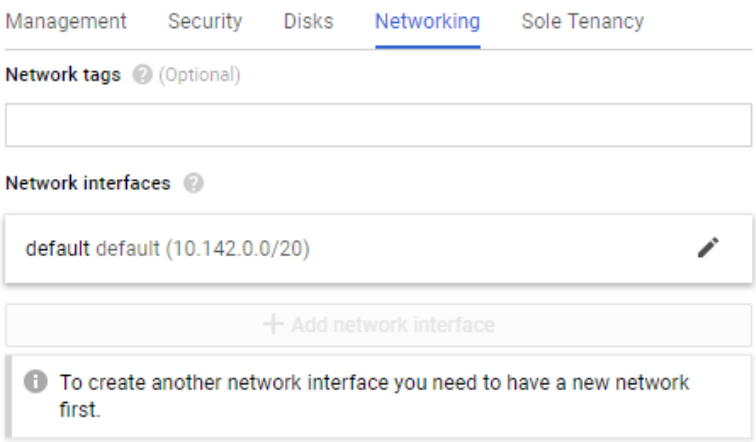
criar VM

Agora, depois de fornecer o sistema operacional, a memória e o espaço HD, na parte inferior da página, você verá a rede. Clique na seta para baixo

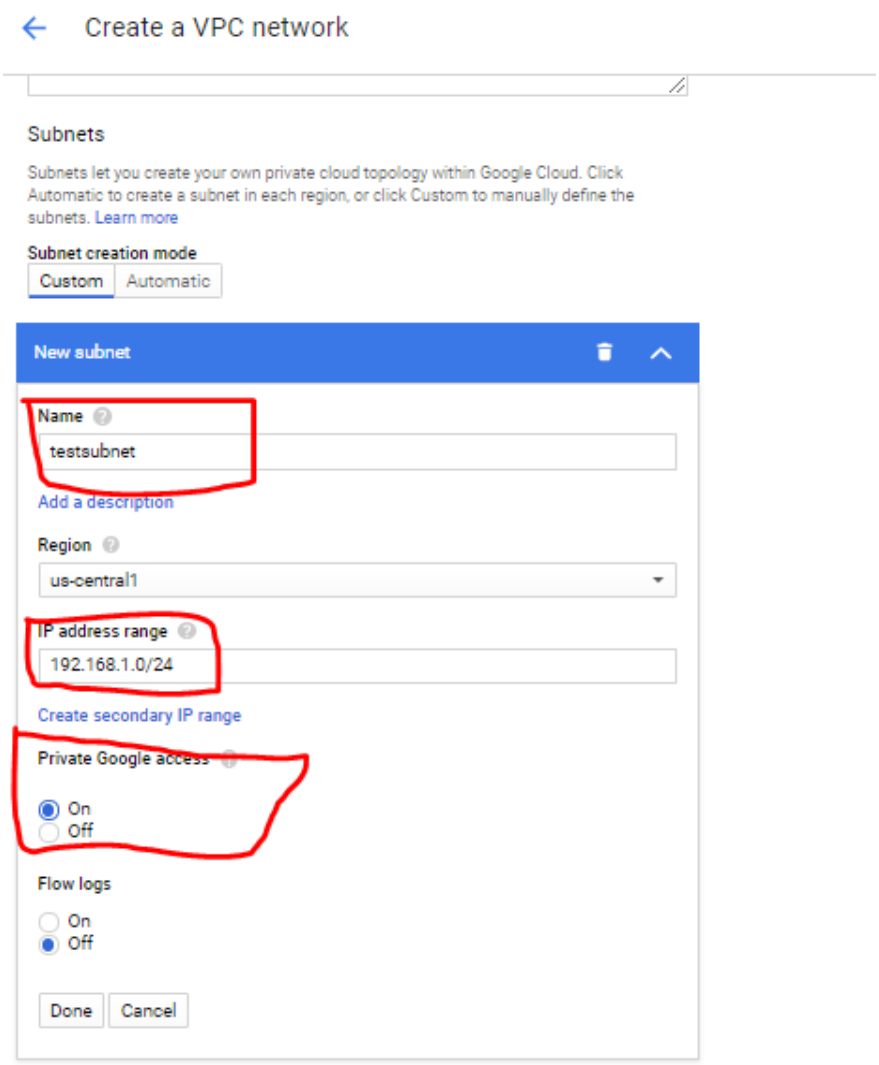


opções personalizadas

Na tag Network, escreva algo que defina essa rede e que você possa lembrar facilmente. Em seguida, selecione a interface de rede e clique em custom



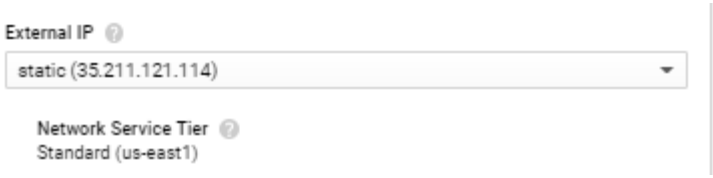
Para disponibilizar a rede personalizada, você precisa adicionar uma rede personalizada em redes VPC que fizemos anteriormente nesta postagem.



VPC personalizado com informações de sub-rede

As regiões devem ser as mesmas para a VM e a rede personalizada para aparecer na lista.

Você também pode especificar o IP externo estático durante a configuração



I.P. estático

- -

Visão geral das regras de firewall

As regras de firewall do Google Cloud Platform (GCP) permitem que você permita ou negue o tráfego de e para suas instâncias de máquina virtual (VM) com base em uma configuração especificada por você. As regras de firewall do GCP são aplicadas no nível de rede virtual, de modo que fornecem proteção eficaz e controle de tráfego, independentemente do sistema operacional usado por suas instâncias.

Toda rede VPC funciona como um firewall distribuído. Embora as regras de firewall sejam definidas no nível da rede, as conexões são permitidas ou negadas por instância. Você pode pensar nas regras de firewall do GCP como existentes não apenas entre suas instâncias e outras redes, mas entre instâncias individuais na mesma rede.

Regras de firewall no GCP

As regras de firewall do GCP são específicas de uma rede VPC. Cada regra permite ou nega o tráfego quando suas condições são atendidas. Suas condições permitem que você especifique o tipo de tráfego, como portas e protocolos, e a origem ou o destino do tráfego, incluindo endereços IP, sub-redes e instâncias. Consulte os componentes da regra de firewall para obter descrições dos componentes que definem uma regra de firewall.

Toda rede tem duas regras de firewall implícitas permanentes que permitem conexões de saída e bloqueiam conexões de entrada. Consulte a seção de regras de firewall padrão e implícita para obter mais informações sobre sua aplicabilidade e como elas interagem com as regras definidas por você. Além disso, a `default` rede é pré-preenchida com algumas regras editáveis adicionais .

Você cria ou modifica as regras de firewall do GCP por meio do console do Google Cloud Platform , da `gcloud` ferramenta de linha de comando e da API REST . Quando você cria ou modifica uma regra de firewall, é possível especificar as instâncias às quais se pretende aplicar usando o componente de destino da regra.

Especificações

As regras de firewall têm as seguintes características:

- As regras de firewall são definidas no nível da rede VPC e são específicas da rede na qual elas são definidas. As regras em si não podem ser compartilhadas entre redes.
- As regras de firewall suportam apenas o tráfego IPv4. Ao especificar uma origem para uma regra de entrada ou um destino para uma regra de saída por endereço, você pode usar apenas um endereço IPv4 ou um bloco IPv4 na notação CIDR.
- A ação executada por uma regra de firewall é `allow` ou `deny` . A regra não pode simplesmente registrar como uma ação. Consulte a ação no componente de correspondência de uma regra de firewall para obter mais informações.
- Cada regra de firewall é definida para se aplicar a tráfego incoming (`ingress`) ou outgoing (`egress`), não ambos. Consulte a direção do componente de tráfego de uma regra de firewall para obter mais informações.
- As regras de firewall do GCP são stateful . Se uma conexão for permitida entre uma origem e um destino ou um destino e um destino, todo o tráfego subseqüente em qualquer direção será permitido, desde que a conexão esteja ativa. Em outras palavras, as regras de firewall permitem a comunicação bidirecional quando uma sessão é estabelecida. A conexão é considerada ativa se pelo menos um pacote for enviado a cada 10 minutos. *As regras de firewall não podem permitir tráfego em uma direção enquanto negam o tráfego de retorno associado.*
- As regras de firewall do GCP não remontam pacotes TCP fragmentados. Conseqüentemente, *uma regra de firewall aplicada ao protocolo TCP só pode ser aplicada ao primeiro fragmento* porque contém o cabeçalho TCP. As regras de firewall aplicáveis ao protocolo TCP não se aplicam aos fragmentos TCP subsequentes.
- O número máximo de conexões controladas na tabela de regras de firewall depende do número de conexões com informações de estado suportadas pelo tipo de máquina da instância:

Direção de tráfego

A direção de uma regra de firewall pode ser `ingress` ou `egress` . A direção é sempre definida a partir da perspectiva do alvo .

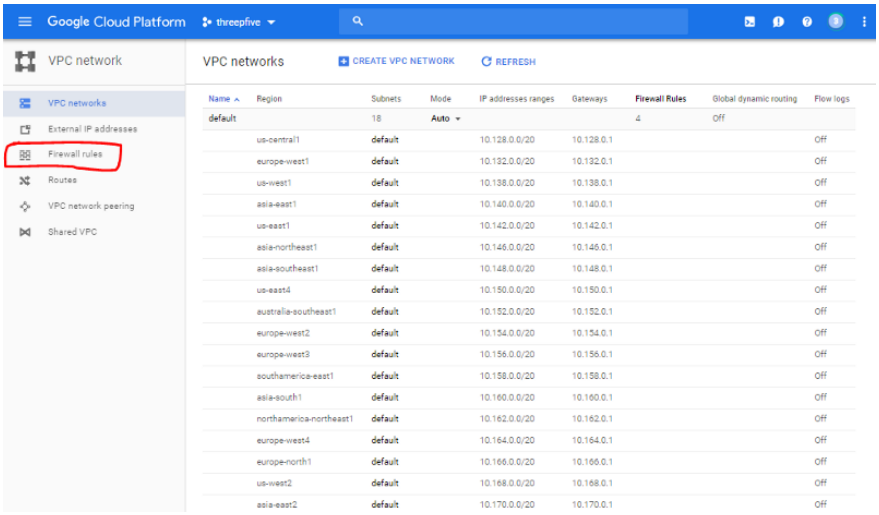
- A `ingress` direção descreve o tráfego enviado de uma fonte para um destino. Regras de entrada se aplicam a pacotes para novas sessões em que o destino do pacote é o destino.
- A `egress` direção descreve o tráfego enviado de um destino para um destino . Regras de saída se aplicam a pacotes para novas sessões em que a origem do pacote é o destino.
- Se você não especificar uma direção, o GCP usará `ingress` .

Considere um exemplo de conexão entre duas VMs na mesma rede. O tráfego da VM1 para a VM2 pode ser controlado usando uma dessas regras de firewall:

- Uma `ingress` regra com um destino de VM2 e uma origem de VM1.
- Uma `egress` regra com um destino de VM1 e um destino de VM2.

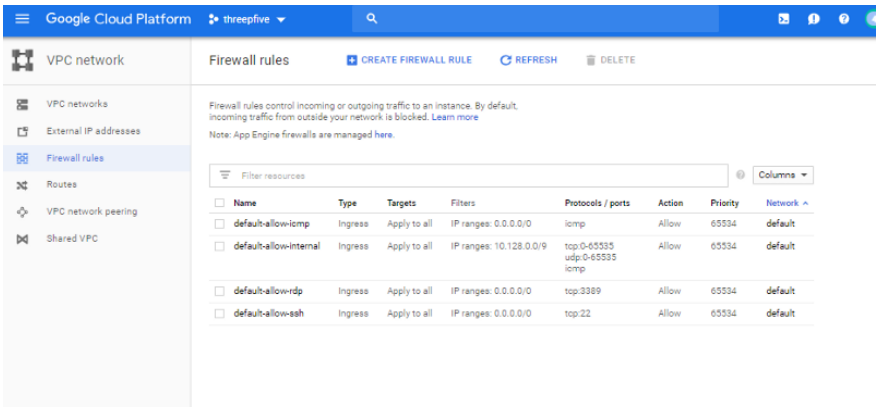
Criando regras de firewall de entrada e saída para uma VPC (por exemplo, sub-redes IP, Tags, contas de serviço)

Da Rede VPC do último post, vá para as regras do Firewall.



Regras de firewall

Por padrão, as regras a seguir são permitidas na VPC durante a criação do projeto.



Regras padrão.

Visão geral do Cloud VPN

Introdução

O Cloud VPN **conecta sua rede local com** segurança à **sua rede virtual privada (VPC) do Google Cloud Platform (GCP)** por meio de uma conexão VPN IPsec. O tráfego viajando entre as duas redes é criptografado por um gateway de VPN e, em seguida, descriptografado pelo outro gateway de VPN. Isso protege seus dados enquanto eles viajam pela Internet.

Características

O Cloud VPN inclui os seguintes recursos:

- **Fornece um SLA de 99,9% de disponibilidade de serviço** .
- **Suporta VPN site a site** como uma topologia simples ou com redundância.
- **Suporta rotas dinâmicas** que usam o Cloud Router e rotas estáticas para gerenciar o tráfego entre suas instâncias de máquina virtual do Compute Engine (VM) e sua infraestrutura existente.

- **Suporta IKEv1 e IKEv2** usando um segredo compartilhado (chave pré-compartilhada IKE). Suporta essas cifras IKE.
- **Usa ESP no modo de túnel com autenticação.** O Cloud VPN não suporta AH ou ESP no modo de transporte. Observe que o Cloud VPN não realiza filtragem relacionada à política em pacotes de autenticação de entrada. Os pacotes de saída são filtrados com base no intervalo de IP configurado no gateway do Cloud VPN.

Topologia VPN

Este diagrama mostra uma conexão VPN simples entre seu gateway do Cloud VPN e seu gateway de VPN no local.

Com o Cloud VPN, seus hosts locais se comunicam por meio de um ou mais túneis VPN IPsec para as instâncias da Máquina Virtual do Compute Engine (VM) nas redes VPC do seu projeto.

Escolhendo VPN para rede híbrida

Consulte Como escolher um tipo de interconexão para determinar se deve usar o Cloud VPN, o Cloud Interconnect - Dedicated ou o Cloud Interconnect - Partner como sua conexão de rede híbrida com o GCP. Esta página também abrange o tipo de cenários de VPN que o Cloud VPN suporta.

Terminologia

Os termos a seguir são usados em toda a documentação da VPN:

ID do projetoO ID do seu projeto do GCP. Este não é o nome do projeto, que é o nome amigável criado pelo usuário do seu projeto. Para encontrar o ID, consulte a coluna " **ID** do **projeto**" no console do GCP. Para mais informações, consulte Identificação de projetos . Internet Key Exchange (IKE) O IKE é o protocolo usado para autenticação e para negociar uma chave de sessão para criptografar o tráfego. **Nota:**O Cloud VPN sempre inicia o IKE. Se dois gateways do Cloud VPN estiverem envolvidos, eles podem atuar como o iniciador do IKE. Gateway de VPN virtual do gateway de VPN em nuvem executado no GCP gerenciado pelo Google, usando uma configuração especificada em seu projeto. Cada gateway do Cloud VPN é um recurso regional que usa um endereço IP externo regional. Um gateway de VPN na nuvem

pode se conectar a um gateway de VPN local ou outro gateway de VPN de nuvem.Local de VPN no localO gateway de VPN que não está no GCP, conectado a um gateway de VPN de nuvem, pode ser um dispositivo físico em seu datacenter ou oferta de VPN baseada em software na rede de outro provedor de nuvem. Instruções nuvem VPN são escritos do ponto de vista da sua rede VPC, de modo a "porta de entrada no local" é a porta de conexão *para*O túnel Cloud VPN.VPN conecta dois gateways VPN e serve como um meio virtual através do qual o tráfego criptografado é passado. Dois túneis VPN devem ser estabelecidos para criar uma conexão entre dois gateways VPN: Cada túnel define a conexão a partir da perspectiva de seu gateway, e o tráfego só pode passar quando o par de túneis é estabelecido.

Opções de roteamento de túnel

O Cloud VPN oferece três métodos de roteamento diferentes para túneis de VPN:

Roteamento dinâmico (BGP) Um Cloud Router pode gerenciar rotas para um túnel de VPN na nuvem usando o Border Gateway Protocol (BGP), se o gateway VPN correspondente ou local o suportar. Esse método de roteamento permite que as rotas sejam atualizadas e trocadas sem alterar a configuração do túnel. Rotas para sub-redes do GCP são exportadas para o gateway de VPN local e as rotas para sub-redes locais aprendidas do gateway de VPN local são aplicadas à sua rede VPC, ambas de acordo com a opção de roteamento dinâmico da rede. O roteamento dinâmico é recomendado porque não exige que os túneis sejam recriados quando as rotas são alteradas. Roteamento baseado em políticaCom esta opção de roteamento, você especifica *intervalos de IP de rede remota* e *sub-redes locais*ao criar o túnel VPN na nuvem. Do ponto de vista do Cloud VPN, os intervalos de IP da rede remota são o "lado direito" e as sub-redes locais são o "lado esquerdo" do túnel VPN. O GCP cria automaticamente rotas estáticas para cada um dos intervalos da rede remota quando o túnel é criado. Ao criar o túnel correspondente no gateway de VPN local, os intervalos do lado direito e esquerdo são invertidos. VPN baseada em rota com essa opção de roteamento, você especifica apenas os *intervalos de IP da rede remota* (lado direito). Todo o tráfego de entrada é aceito através do túnel, sujeito às rotas que você cria manualmente. **Nota:** Algumas literaturas referem-se aos intervalos de sub-rede do lado esquerdo e direito como *domínios de criptografia* .

Para obter mais detalhes sobre tipos de rede e opções de roteamento, consulte a página Escolhendo um tipo de rede VPC e opções de roteamento.

Especificações

O Cloud VPN tem as seguintes especificações:

- O Cloud VPN pode ser usado com redes VPC e redes legadas . Para o VPC, um modo personalizado é recomendado para que você tenha controle total sobre os intervalos de endereços IP usados pelas sub-redes na rede.
- Se os intervalos de endereços IP para sub-redes locais se sobrepuserem a endereços IP usados por sub-redes em sua rede VPC, consulte Ordem de rotas para determinar como os conflitos de roteamento são resolvidos.
- Cada gateway do Cloud VPN deve estar conectado a outro gateway do Cloud VPN ou a um gateway de VPN local .
- O gateway de VPN local deve ter um endereço IP externo estático. Você precisará saber seu endereço IP para configurar o Cloud VPN.
- Se o seu gateway VPN no local estiver protegido por um firewall, você deverá configurar o firewall para passar o protocolo ESP (IPSec) e o tráfego IKE (UDP 500 e UDP 4500) para ele. Se o firewall fornecer conversão de endereços de rede (NAT), consulte encapsulamento UDP e NAT-T .
- O Cloud VPN suporta apenas uma chave pré-compartilhada (segredo compartilhado) para autenticação. Você deve especificar um segredo compartilhado ao criar o túnel da VPN na nuvem. Esse mesmo segredo deve ser especificado ao criar o encapsulamento no gateway local. Consulte estas diretrizes para criar um segredo compartilhado forte .
- O Cloud VPN usa uma unidade máxima de transmissão (MTU) de 1460 bytes. Os gateways VPN locais devem ser configurados para usar uma MTU de no máximo 1460 bytes.
- Para compensar a sobrecarga de ESP, talvez seja necessário definir os valores de MTU para os **sistemas que** enviam tráfego pelo túnel

para valores mais baixos. Consulte as Considerações da MTU para uma discussão detalhada e recomendações.

- O Cloud VPN requer que o gateway de VPN no local esteja configurado para suportar a fragmentação. Os pacotes devem ser fragmentados *antes de* serem encapsulados.
- O Cloud VPN usa a detecção de reprodução com uma janela de 4096 pacotes. Você não pode desligar isso.
- Consulte as IPS Ciphers Suportadas para cifras e parâmetros de configuração suportados pelo Cloud VPN.

Manutenção e disponibilidade

O Cloud VPN é submetido a manutenção periódica. Durante a manutenção, os túneis do Cloud VPN são colocados off-line, resultando em breves quedas no tráfego da rede. Quando a manutenção é concluída, os túneis do Cloud VPN são restabelecidos automaticamente.

A manutenção do Cloud VPN é uma tarefa normal e operacional que pode acontecer a qualquer momento sem aviso prévio. Os períodos de manutenção são projetados para serem curtos o suficiente para que o SLA do Cloud VPN não seja afetado.

Você pode criar configurações de VPN altamente disponíveis usando vários túneis. Algumas estratégias para fazer isso são discutidas na página Redundant and High-throughput VPNs .

Encapsulamento UDP e NAT-T

O Cloud VPN **só** suporta NAT um-para-um através de encapsulamento UDP para NAT-Traversal (NAT-T). A conversão de endereço baseada em NAT e porta a um **não** é suportada. Em outras palavras, o Cloud VPN **não pode se conectar** a vários gateways VPN locais ou de mesmo nível que compartilham um único endereço IP público.

Ao usar NAT de um para um, um gateway de VPN local **deve** ser configurado para se identificar usando um endereço IP público, não seu endereço interno (privado). Quando você configura um túnel do Cloud VPN para se conectar a um gateway de VPN local, você especifica um

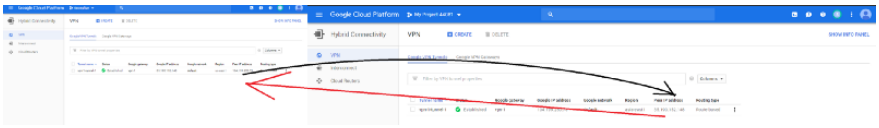
endereço IP externo. O Cloud VPN espera que um gateway de VPN local use seu endereço IP externo para sua identidade.

Para mais detalhes sobre os gateways VPN atrás do NAT one-to-one, consulte a página de solução de problemas .

Melhores práticas

Use essas práticas recomendadas para criar seu Cloud VPN da maneira mais eficaz.

Criação de uma VPN entre um Google VPC e uma rede externa usando o Cloud VPN

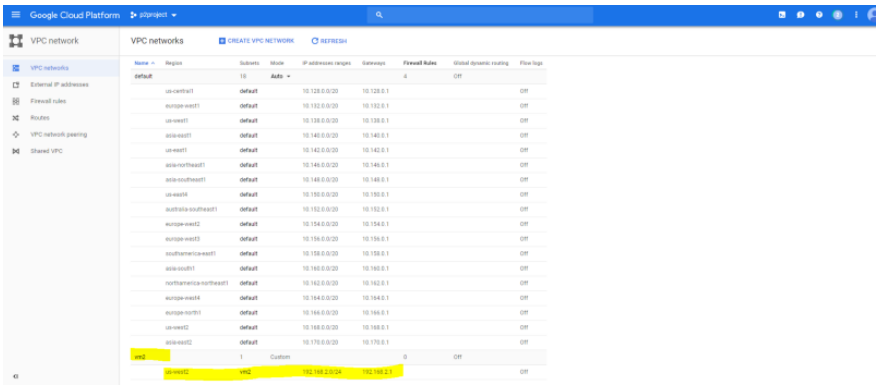


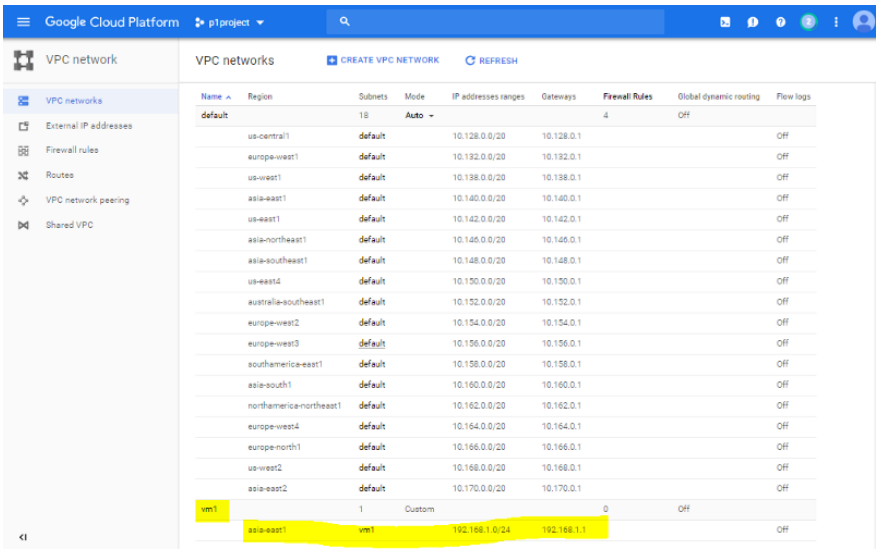
Conexão VPN

Criar uma conexão VPN entre duas redes é um objetivo básico de uma conexão VPN. Vamos tentar conectar duas redes usando VPN na nuvem.

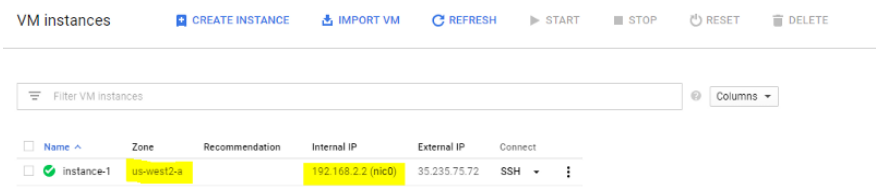
1. Rede VPC padrão com sub-rede personalizada com uma VM
2. VPC personalizada com sub-rede personalizada com uma VM

Primeiro de tudo, crie uma sub-rede dentro do VPC

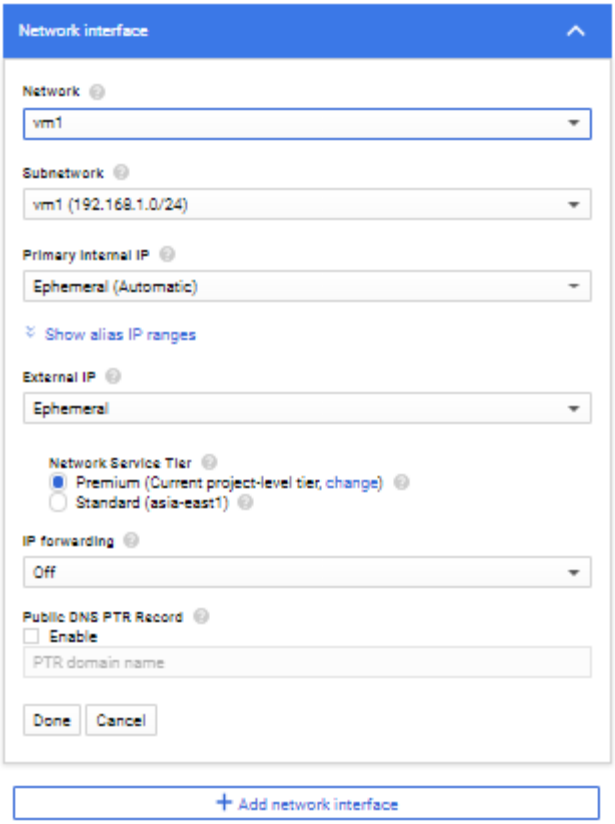




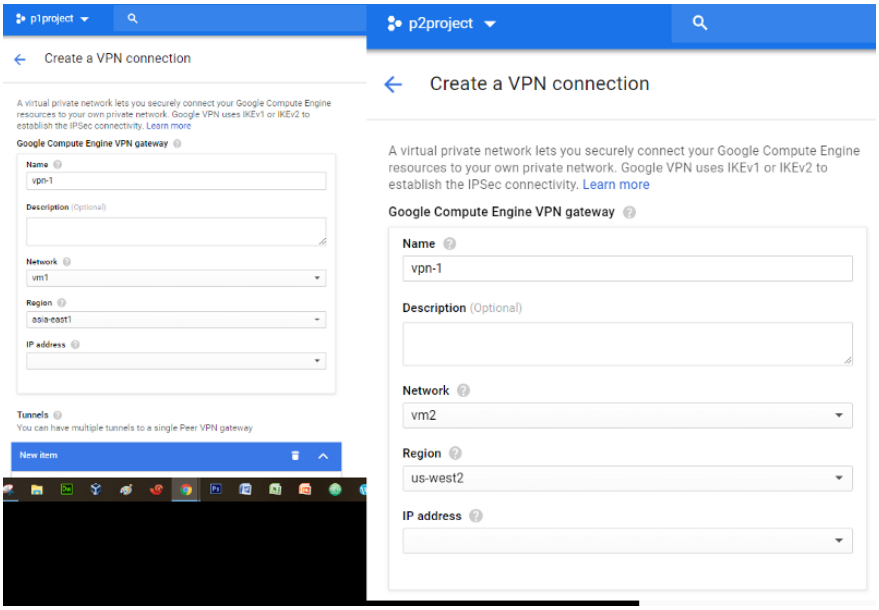
Agora crie uma VM dentro da VPC

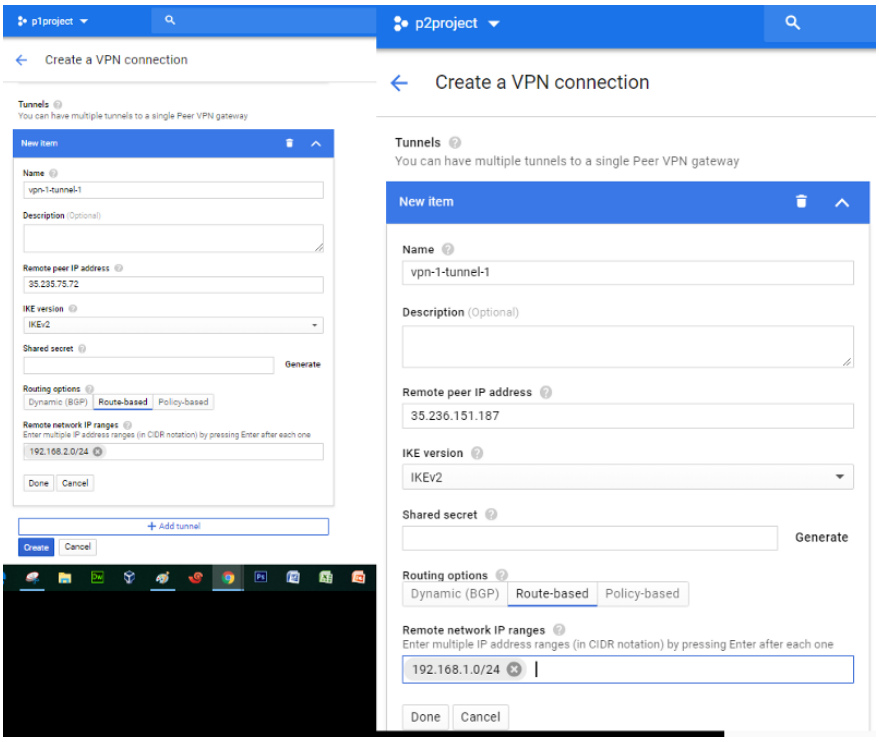


Ao criar a VM, selecione a rede e o IP durante a configuração.

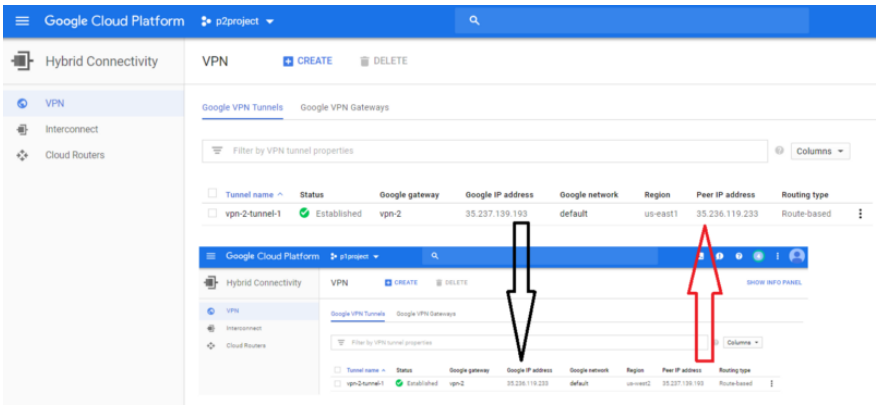


Use os detalhes da VM e do IP do VPC para se conectar usando a VPN na nuvem.





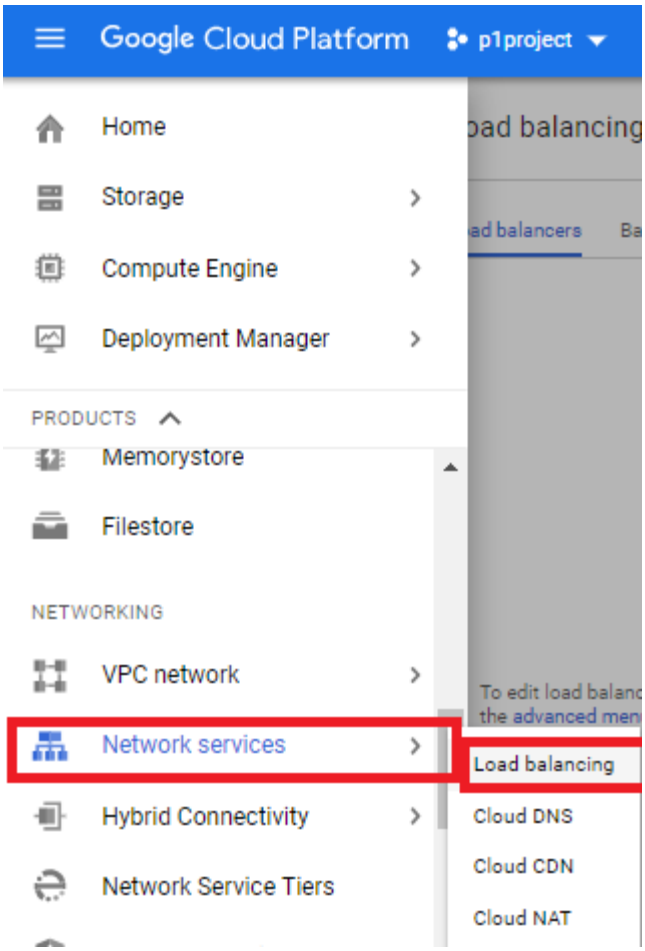
Depois que a VPN for conectada com sucesso, uma marca de verificação verde será mostrada e poderemos fazer ping entre duas VMs.



- -

Criando um balanceador de carga para distribuir o tráfego da rede de aplicativos para um aplicativo (por exemplo, balanceador de carga HTTP Global, balanceador de carga Global SSL Proxy, balanceador de carga Global TCP Proxy, balanceador de carga de rede regional, balanceador de carga interno regional)

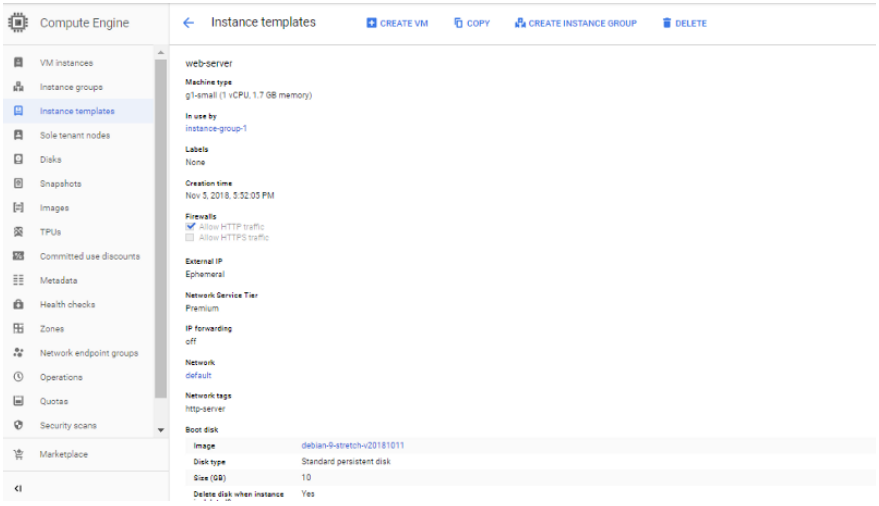
Para ir para a configuração do balanceador de carga, clique em Serviços de rede e, em seguida, em balanceamento de carga



balanceamento de carga

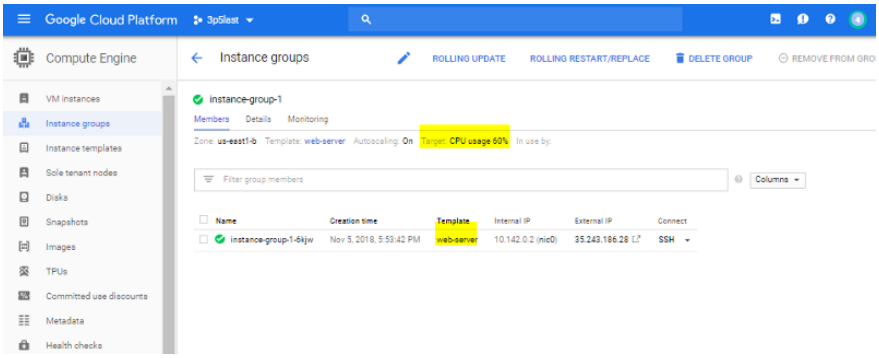
Isso levará a outra página com várias opções.

Antes de ir para lá, criarei um modelo de instância e um grupo de instâncias.



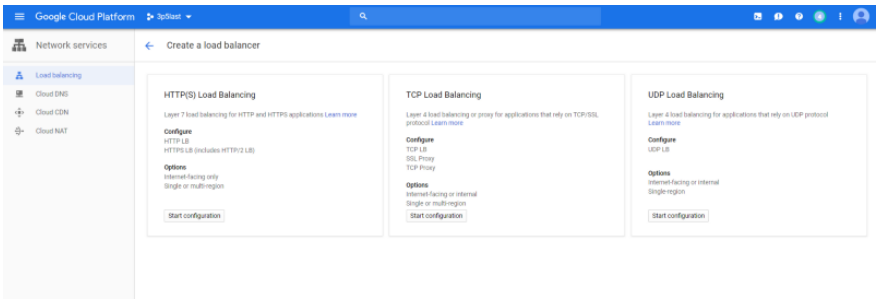
modelo de instância

Com base no modelo de instância, criei o grupo de instâncias



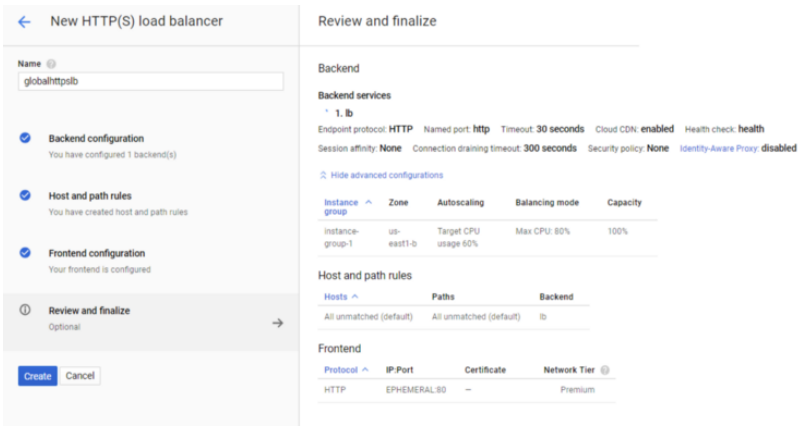
grupo de instâncias

Agora, quando você vai para a página de balanceamento de carga, você verá essas opções.

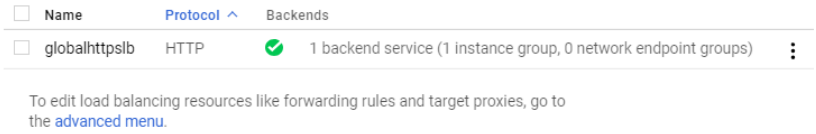


opções de balanceamento de carga

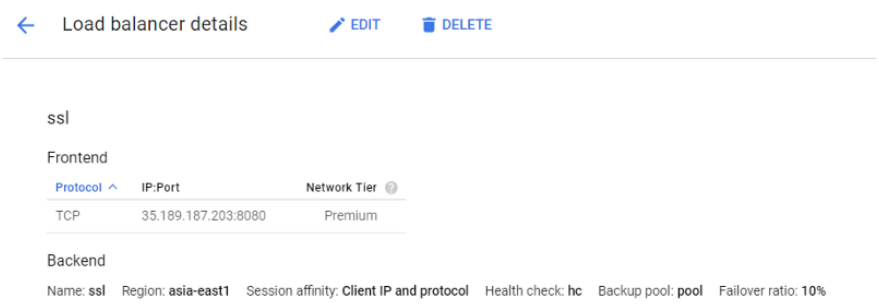
Balanceador de carga HTTPS global



Depois de um tempo, ele será ativado.

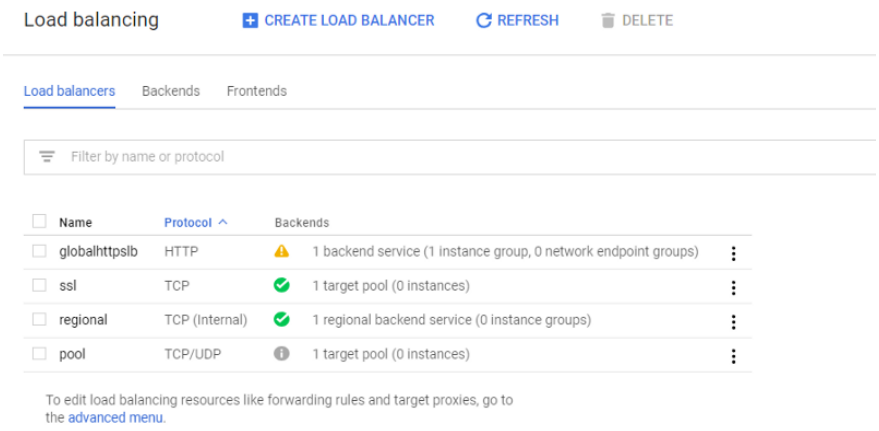


Balanceador de carga proxy global SSL



SSL LB

Dessa maneira, vários balanceadores de carga podem ser configurados facilmente no console.



vários LBs