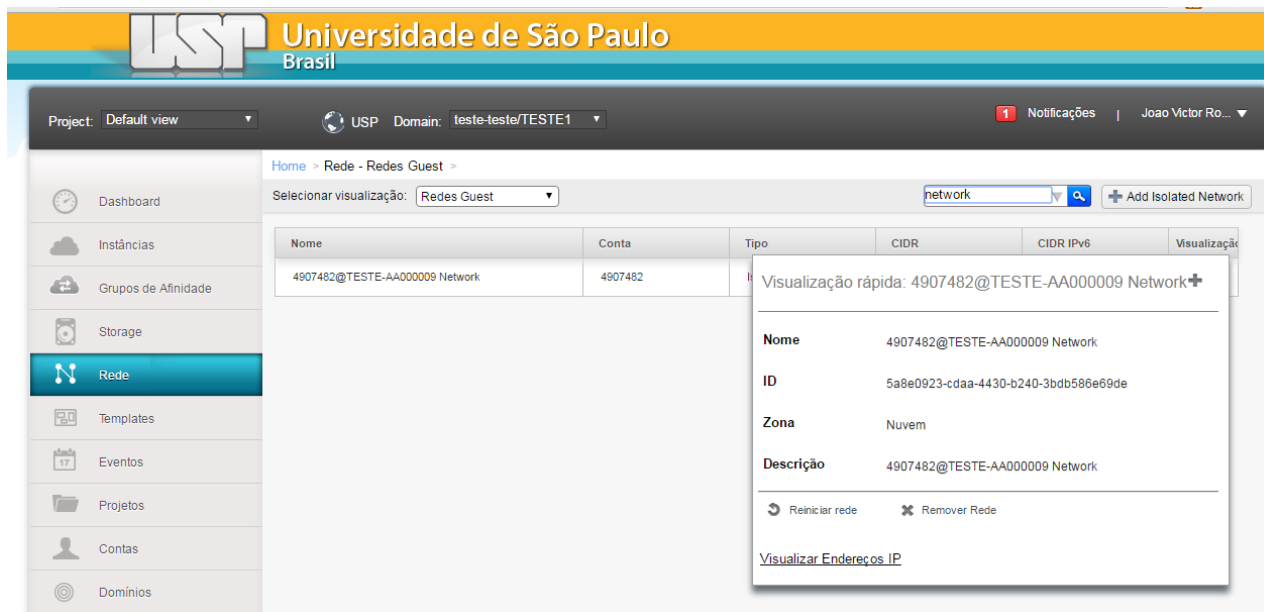


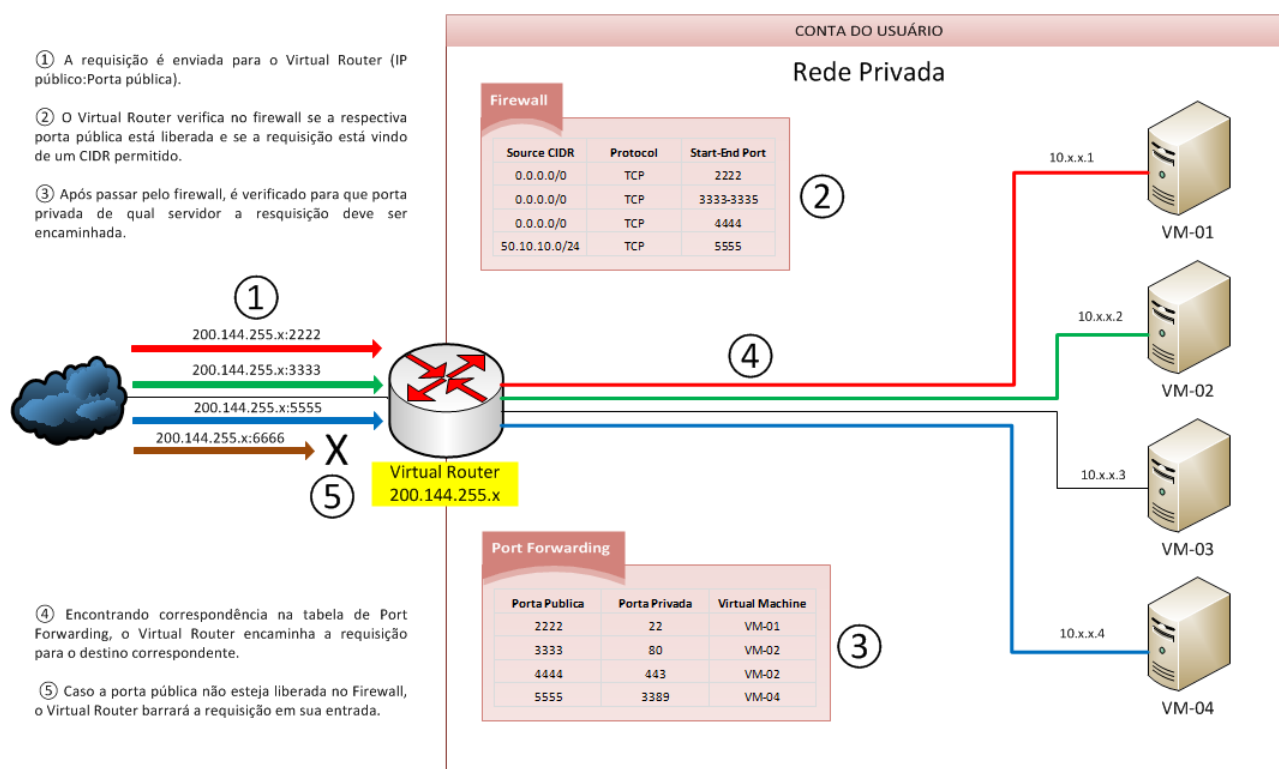
# CONFIGURANDO ACESSO EXTERNO (FIREWALL E PORT FORWARDING)

No console clique em Rede → Visualização “+” → Visualizar Endereços IP



Na tela que abrir, clique no IP de **Source NAT**.

## SOURCE NAT



Nesta configuração, você terá várias VMs sendo acessadas através de um único endereço IP, utilizando para isso portas públicas de acesso distintas para cada uma delas.

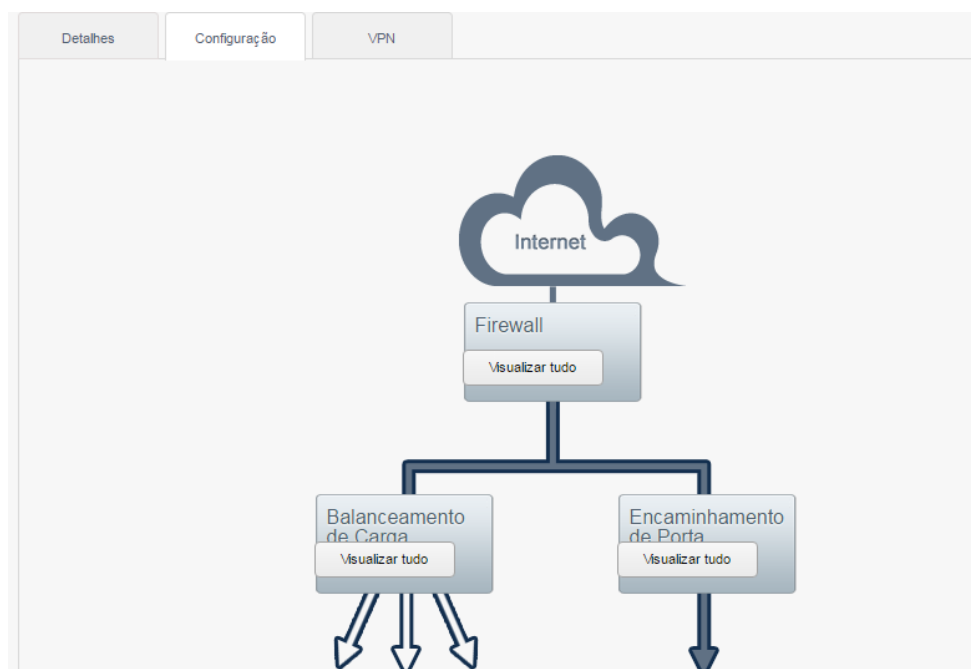
| IPs                         | Zona  | Nome da VM | Estado    | Visualização |
|-----------------------------|-------|------------|-----------|--------------|
| 200.144.255.31 [Source NAT] | Nuvem |            | Allocated | +            |
| 200.144.254.64              | Nuvem | web-proxy  | Allocated | +            |

Clique na aba Configurações:



Para liberação de acesso externo, será necessária a configuração de Firewall e Encaminhamento de Porta.

Clique em Encaminhamento de Porta:



Configure a Porta Privada da VM e a Porta Pública a qual será utilizada para acesso externo.

Abaixo, a configuração permitirá o acesso ao serviço SSH da VM (porta 22) através da porta externa 2222. Nós recomendamos sempre que possível não utilizar o mesmo valor de porta privada e porta pública a fim de evitar ataques em portas previsíveis (salvo casos de serviços pontuais: http, https, etc).

Home > Rede - Redes Guest > Endereços IP > 200.144.255.31 [Source NAT] > Encaminhamento de Porta >

Atualizar

Encaminhamento de Porta

| Porta Privada | Porta Pública | Protocolo | Estado | Adicionar VM | Ações |
|---------------|---------------|-----------|--------|--------------|-------|
| 22            | 2222          | TCP       |        | Adicionar    |       |

Clique em “Adicionar” para associar a configuração a uma VM.

+ Adicionar VMs

| Nome               | Nome de exibição   | Endereço IP | Nome da zona | Estado  | Select |
|--------------------|--------------------|-------------|--------------|---------|--------|
| web-proxy          | web-proxy          |             | Nuvem        | Running |        |
| teste-upgrade-ac s | teste-upgrade-ac s |             | Nuvem        | Running |        |

Após a configuração, a nova regra será mostrada no painel.

Encaminhamento de Porta

| Porta Privada | Porta Pública | Protocolo | Estado | Adicionar VM                   | Ações |
|---------------|---------------|-----------|--------|--------------------------------|-------|
|               |               | TCP       |        | Adicionar                      |       |
| 22 - 22       | 2222 - 2222   | TCP       | Active | VM: web-proxy<br>IP: 10.2.2.74 |       |

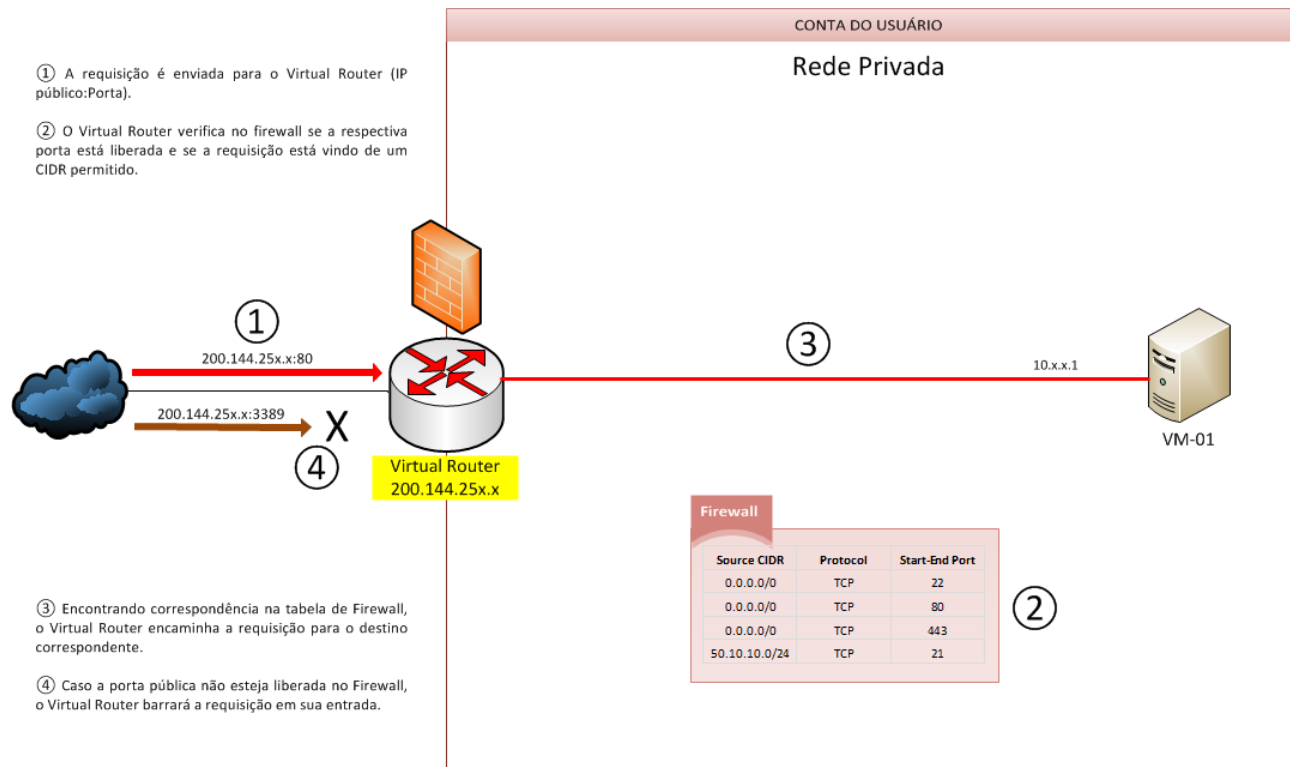
Para configurar o firewall, é necessário informar o CIDR a partir do qual o acesso estará liberado. O CIDR “0.0.0.0/0” significa que o acesso estará liberado para qualquer IP externo, enquanto um CIDR “200.144.252.5/32” significa que o acesso estará liberado apenas a partir deste endereço IP de origem.

Firewall

| CIDR de Origem | Protocolo | Porta de Início | Porta Final | Tipo ICMP | Código ICMP | Adicionar regra | Estado | Ações |
|----------------|-----------|-----------------|-------------|-----------|-------------|-----------------|--------|-------|
| 0.0.0.0/0      | TCP       | 2222            | 2222        |           |             | Adicionar       |        |       |

Para um acesso direto (porta pública 80 → porta privada 80), é necessário utilizar a configuração de **Static NAT**.

## STATIC NAT



Na configuração de Static NAT, é necessária apenas a configuração de Firewall

