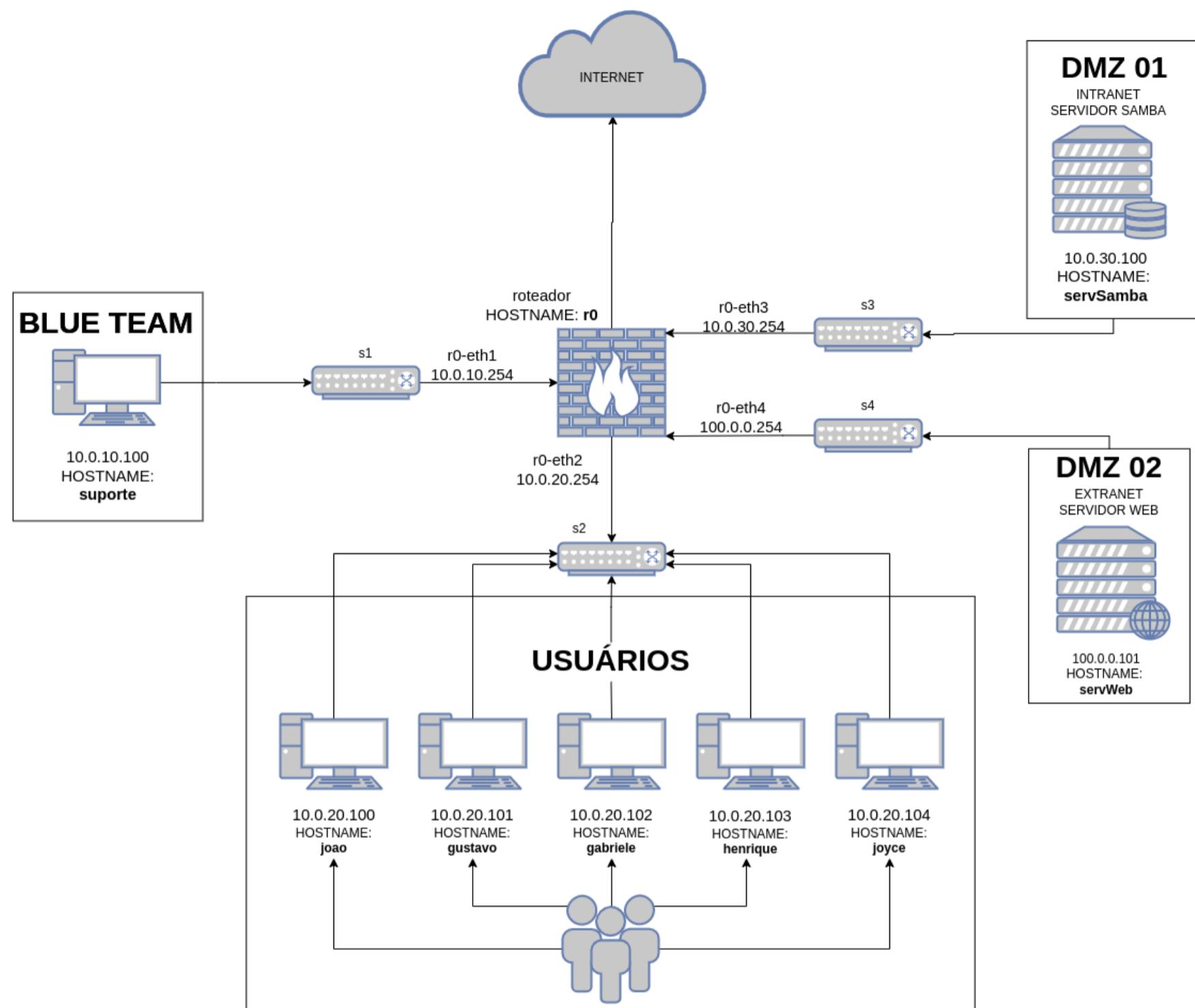


Questão 1

Tentativas restantes: 3

Vale 1,0 ponto(s).



📌 O usuário João reportou que não estava conseguindo acessar suas pastas compartilhadas no Servidor Samba. Você, como membro da equipe de suporte, ficou encarregado de identificar a causa e resolver o problema. Vamos começar!

📝 Utilitários:

Container:

Server Samba

Comando:

`ifconfig`

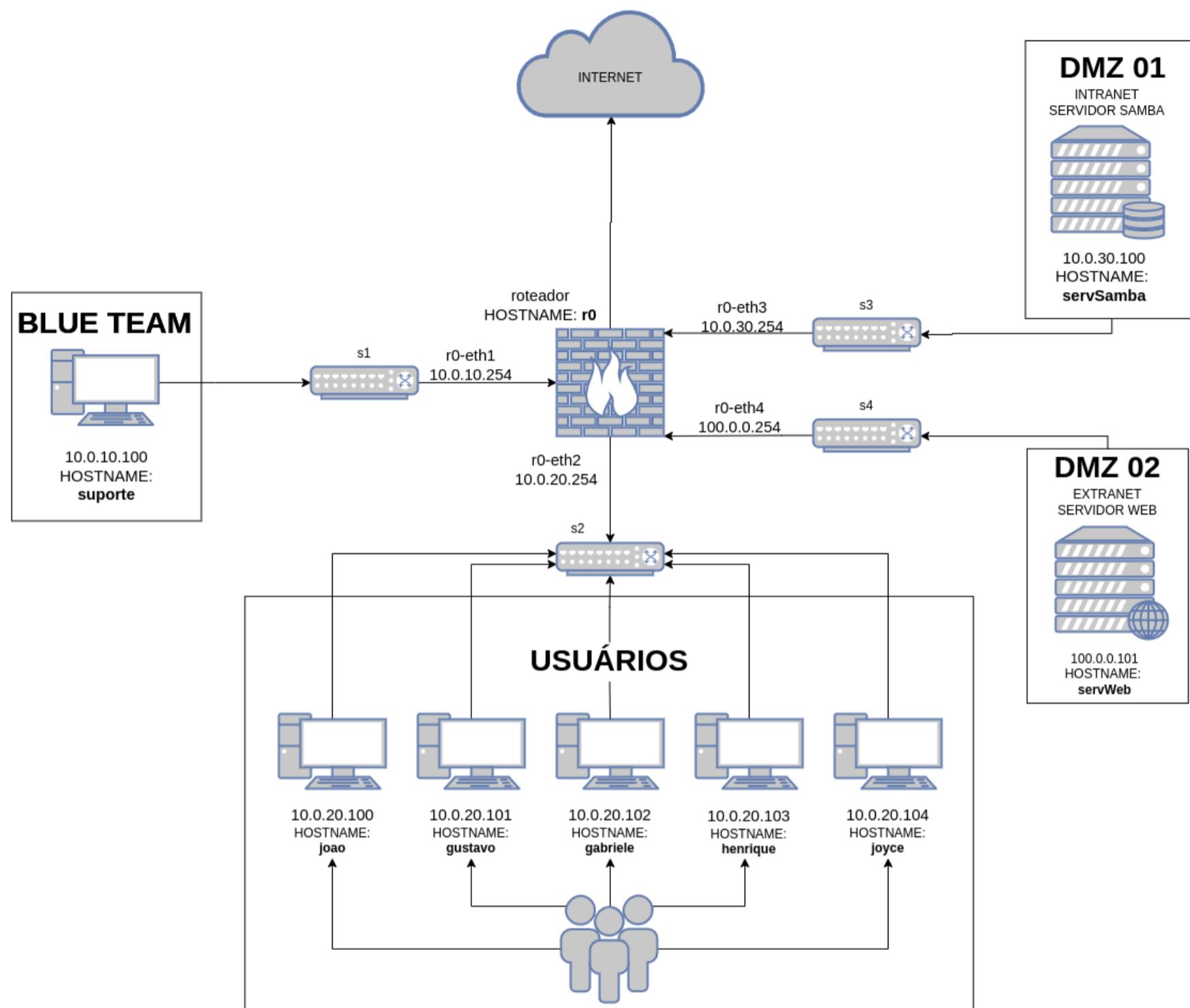
❓ Qual o endereço IP do Servidor Samba?

Resposta:

Questão 2

Tentativas restantes: 3

Vale 1,0 ponto(s).



💡 Suponha que você tenha um usuário e um diretório remoto no servidor Samba. Com isso, podemos verificar se o serviço do Samba está realmente acessível remotamente através da execução de um comando **smbclient**. Para tanto, é necessário executar esse comando juntamente com algumas informações de usuário pelo **Supporte**.

📌 Utilitários:

Container:

Suporte

Informações do usuário:

Usuário: suporte

Senha: badpass

Diretório remoto: suporte

Comando:

```
smbclient //10.0.30.100/suporte -U "suporte"
```

Aviso: Depois de executar o comando acima, responda o que se pede.

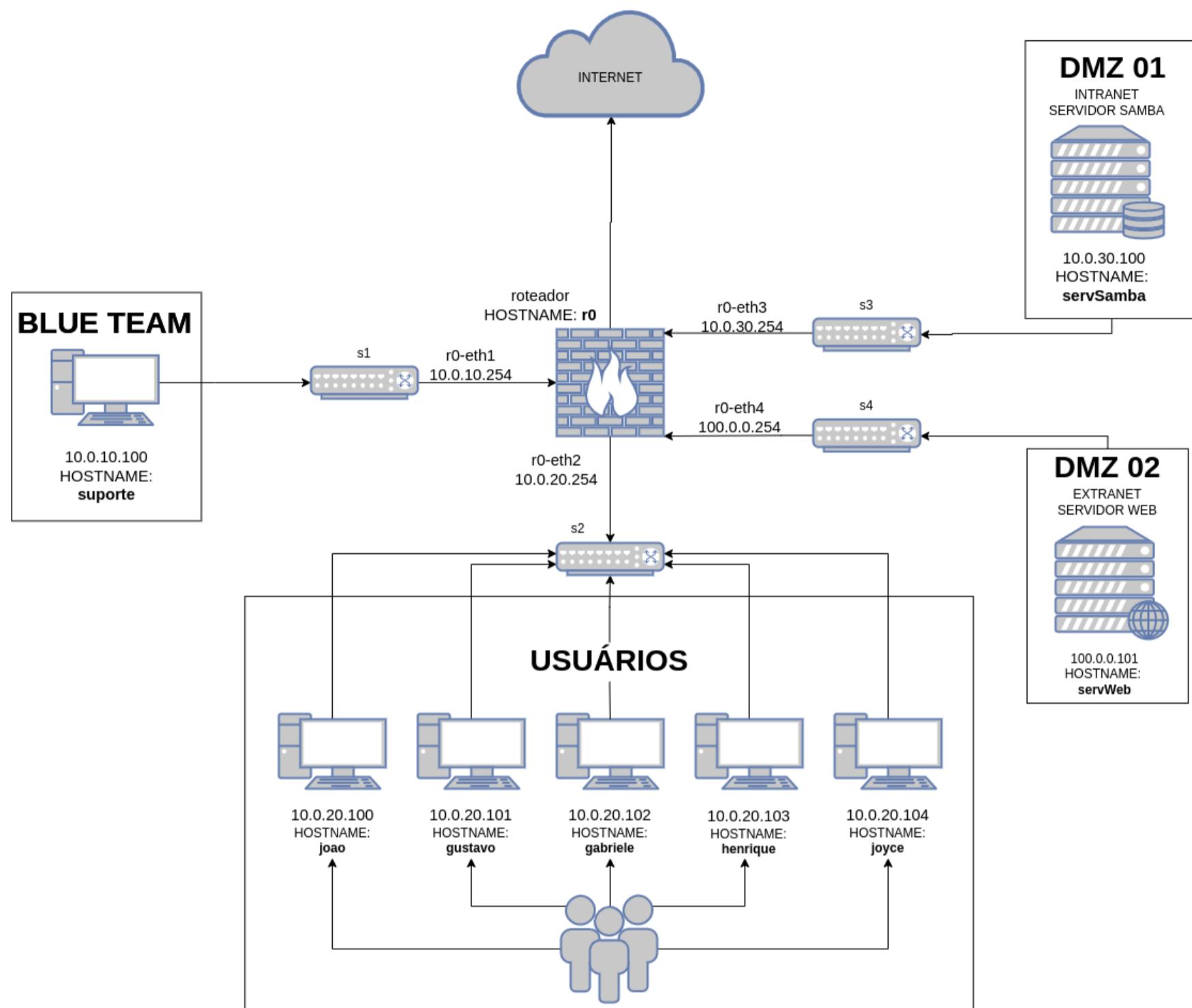
❓ Foi possível se conectar ao servidor? Responda sim ou não

Resposta:

Questão 3

Tentativas restantes: 3

Vale 1,0 ponto(s).



📌 Utilizando o container **Supporte**, com o protocolo *Internet Control Management Protocol (ICMP)* verifique se a interface do **Servidor Samba** está alcançável na rede.

📝 Utilitários:

Comando:

`ping -c4 <ip_server_samba>`

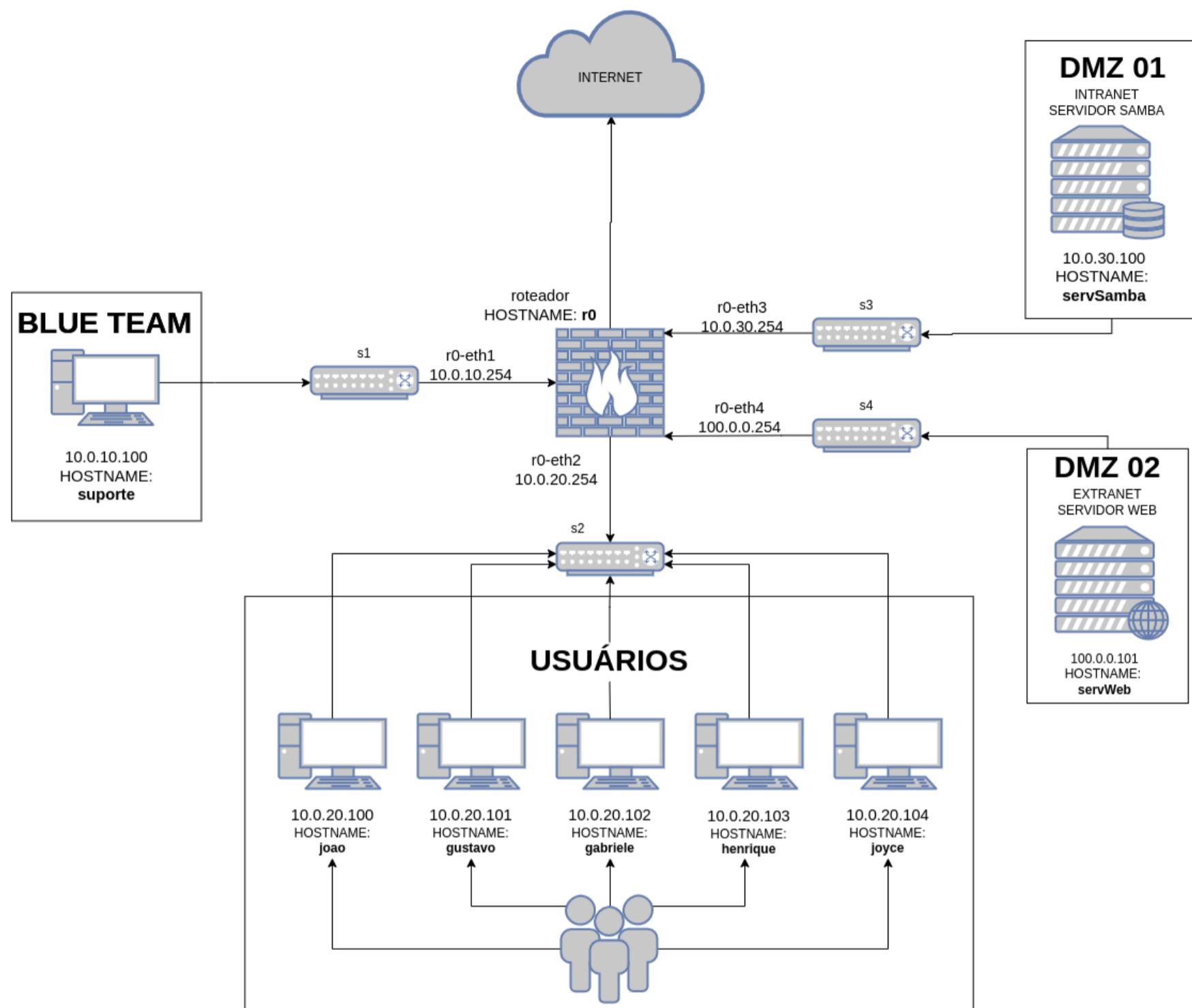
❓ O servidor está alcançável? Responda "sim" ou "não".

Resposta:

Questão 4

Tentativas restantes: 3

Vale 1,0 ponto(s).



★ Agora, a partir do **Server Samba**, liste os processos em execução no sistema.

Utilitários:

Comando:

```
timeout 1s top | grep smbd
```

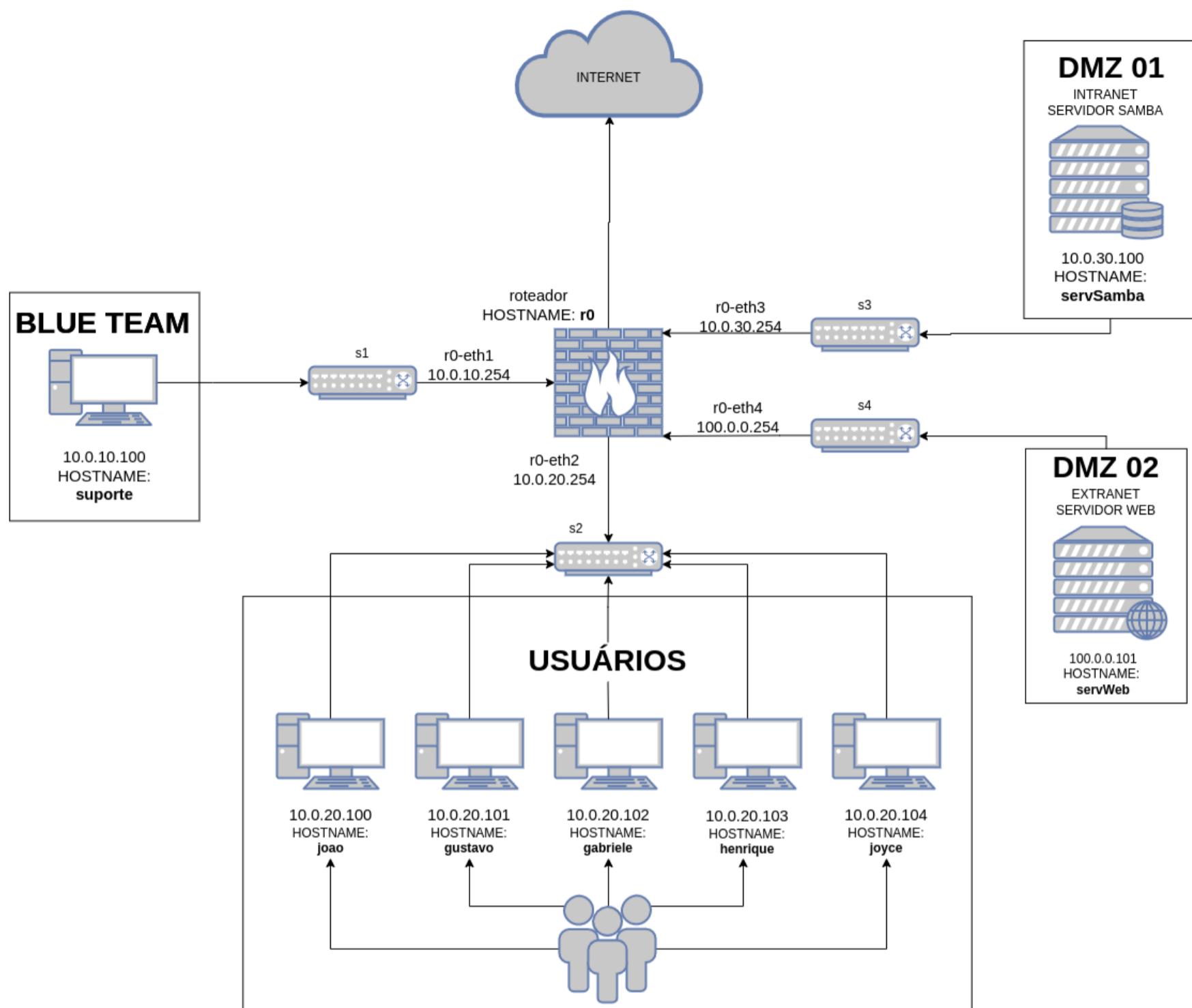
? O serviço do **Samba** (**smbd**) está em execução? Responda "sim" ou "não".

Resposta:

Questão 5

Tentativas restantes: 3

Vale 1,0 ponto(s).



📌 Ainda no **Server Samba**, utilize o comando **netstat** para verificar se existem conexões TCP ativas com o serviço **Samba**.

📄 Utilitários:

Comando:

`timeout 20s netstat`

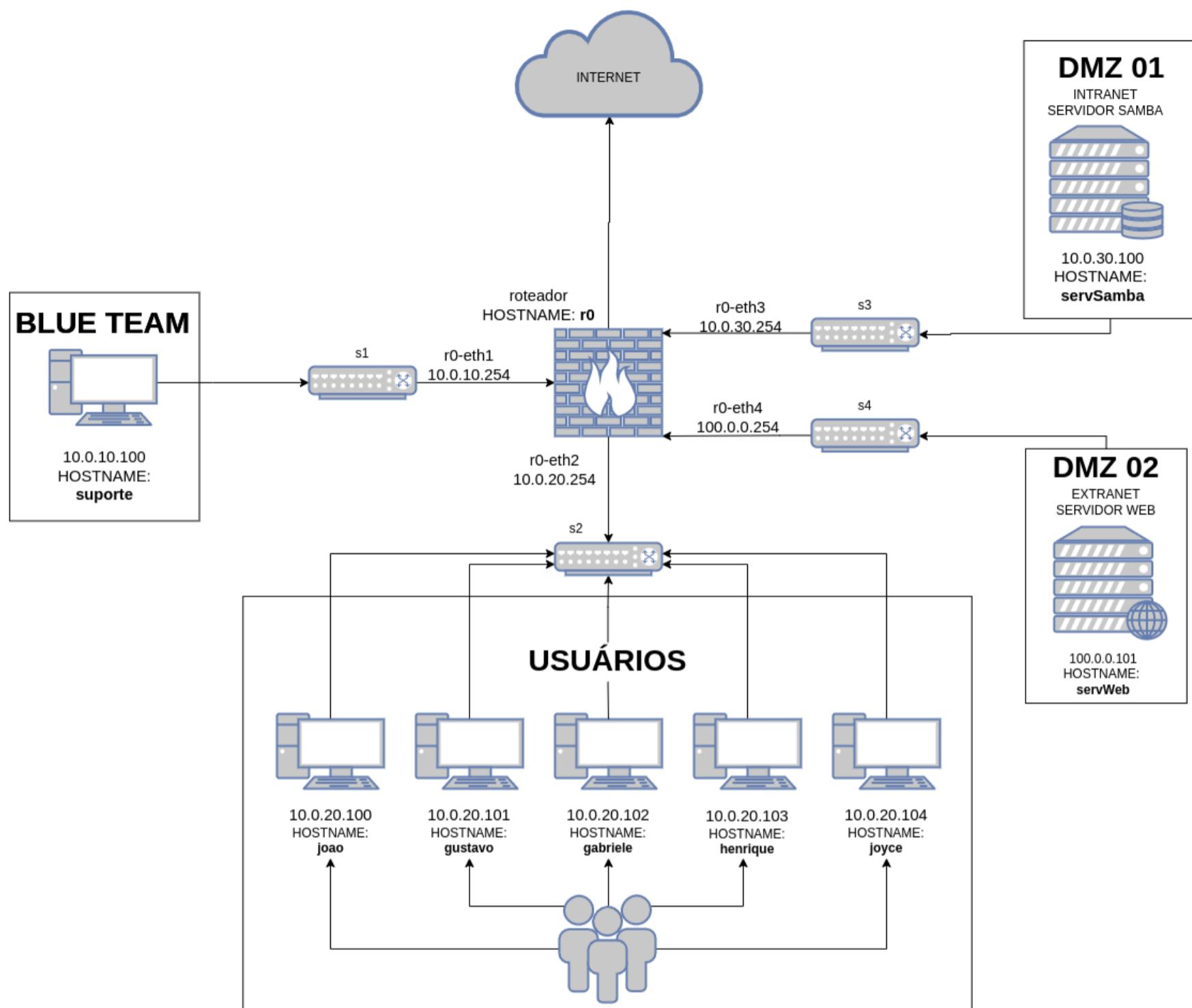
❓ Existem conexões com o serviço **Samba**? Responda "sim" ou "não".

Resposta:

Questão 6

Tentativas restantes: 3

Vale 1,0 ponto(s).



📌 Ainda no **Server Samba**, através do comando **ifconfig**, verifique se está chegando muitos ou poucos dados na interface ethernet.

Utilitários:

Comando:

`ifconfig servSamba-eth0`

Análise:

- Número total de bytes transmitidos (TX bytes)
- Número total de bytes recebidos (RX bytes)

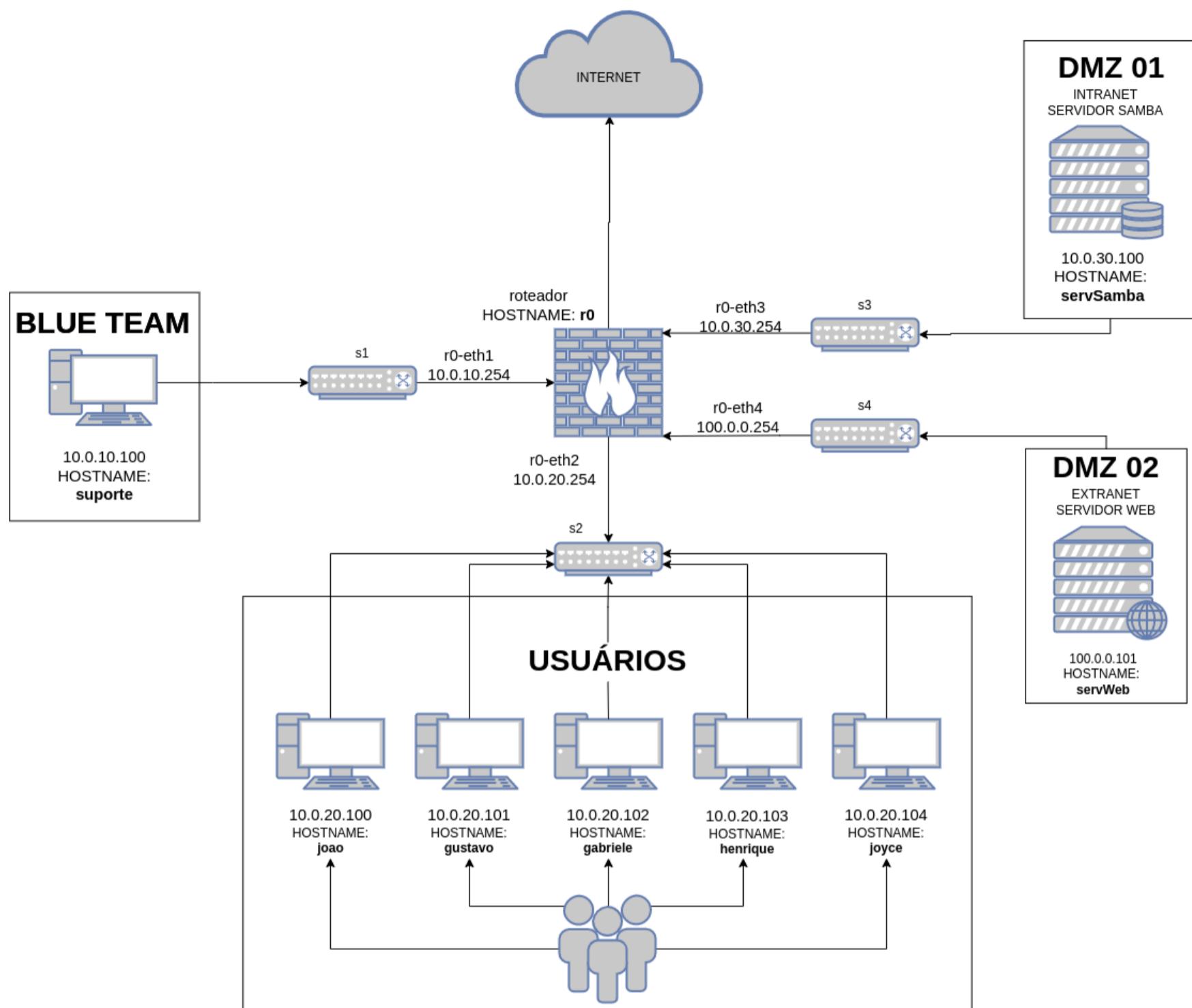
❓ Como está o tráfego no servidor? Responda muito tráfego ou pouco tráfego.

Resposta:

Questão 7

Tentativas restantes: 3

Vale 1,0 ponto(s).



💡 De acordo com a questão anterior, o alto tráfego na interface ethernet do **Server Samba** está indisponibilizando o serviço Samba para novos acessos. Isso pode ou não ser classificado como um ataque. Vamos analisar isso!

💡 O **tshark** é uma ferramenta de linha de comando para análise de tráfego de rede, sendo uma alternativa ao **Wireshark**. Sabe-se que o roteador **r0** possui o **tshark** instalado.

💡 A partir do **r0**, é possível usar o **tshark** para capturar e salvar (.pcap) o tráfego na interface correspondente a VLAN **DMZ 01**. Mas antes, faça o que se pede abaixo:

Utilitários

Apenas **observe** esse comando:

```
r0 tshark -i <interface_name> -w saida.pcap -a duration:5 -d tcp.port==445,nbss
```

Aviso: Observe a conexão com o Switch (s3), que por sua vez, se conecta em uma outra interface com IP 10.0.30.254, referente ao roteador principal (r0).

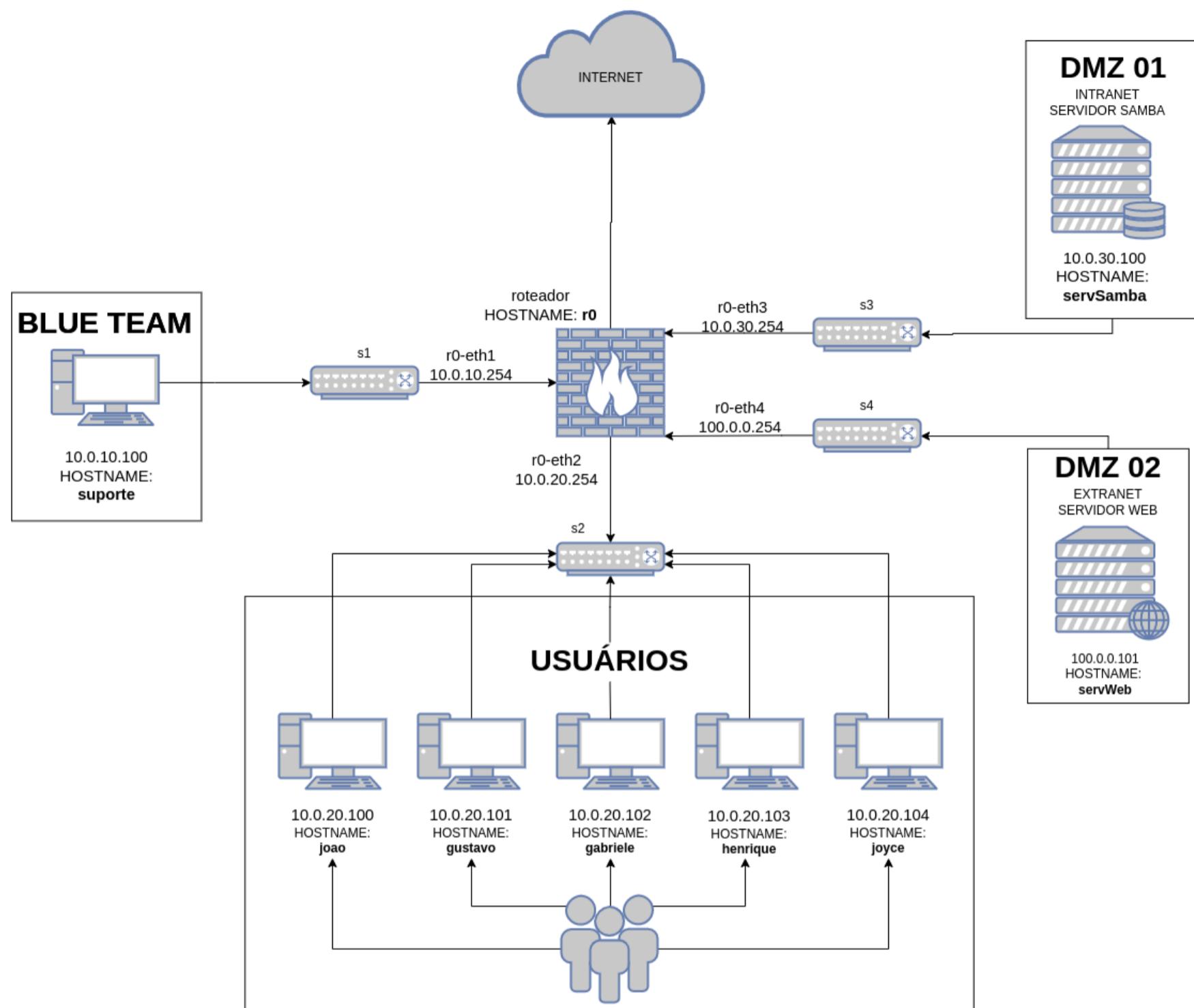
❓ Feito a análise do cenário anteriormente. Qual o **nome da interface** do roteador principal (**r0**) onde o tráfego deverá ser capturado?

Resposta:

Questão 8

Tentativas restantes: 3

Vale 1,0 ponto(s).



💡 Agora precisamos analisar o tráfego para buscar possíveis anormalidades. Utilizando o **Tshark** execute a captura por 5 segundos e filtre na porta e serviço específico.

💡 Dito isso, esteja conectado ao **Containernet** e identifique quais endereços IP estão enviando tráfego para o Servidor Samba.

Utilitários

Comandos:

```
r0 tshark -i r0-eth3 -w saida.pcap -a duration:5 -d tcp.port==445,nbss  
r0 tshark -r saida.pcap
```

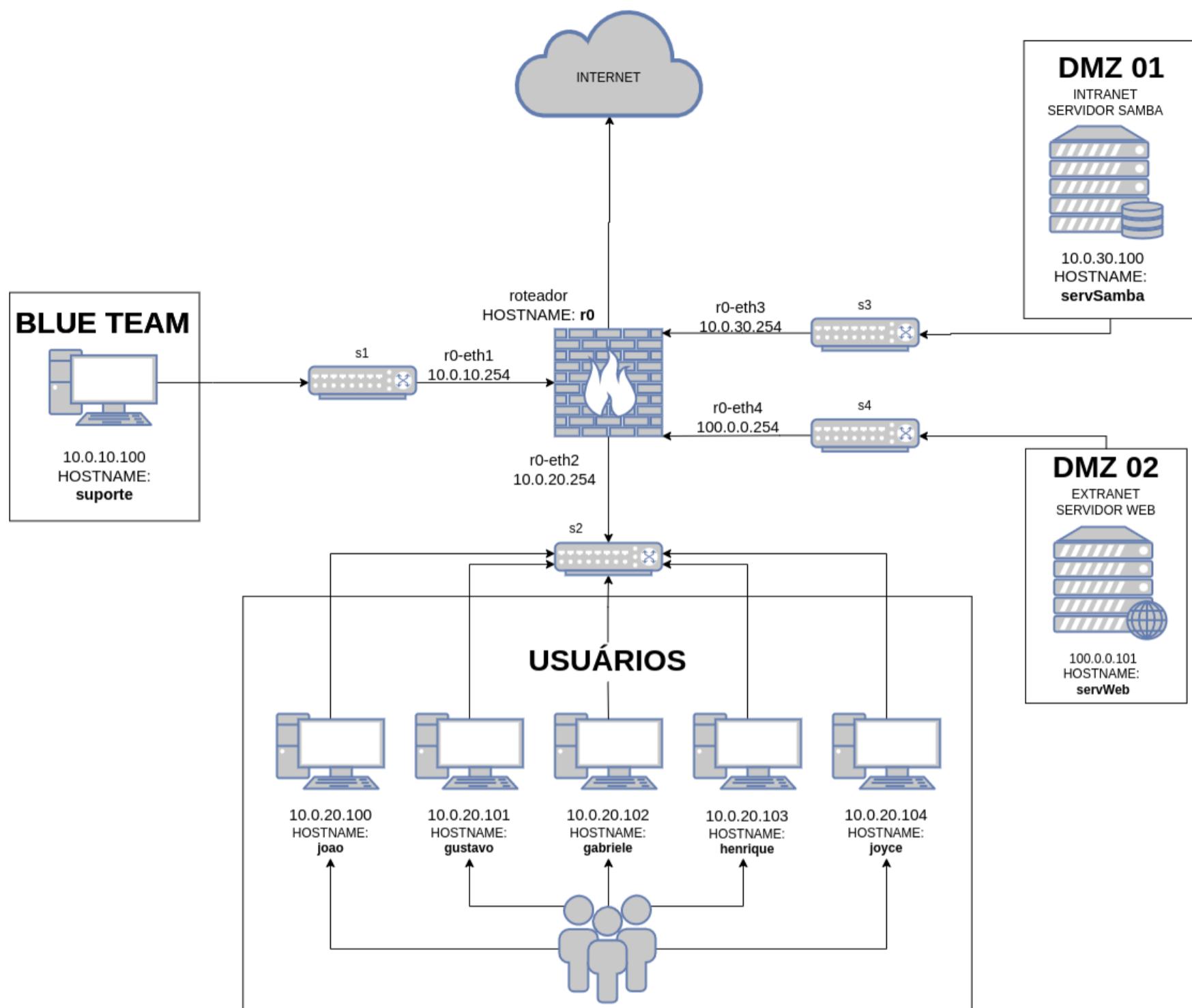
❓ Dentre os IP's capturados, existe algum endereço IP que esteja enviando muito tráfego? Se existir, responda qual o endereço IP. Se não, responda simplesmente "não".

Resposta:

Questão 9

Tentativas restantes: 3

Vale 1,0 ponto(s).



💡 Com a análise de tráfego da questão anterior, você conseguiu identificar um alto tráfego gerado pelo IP **10.0.20.103** do User **Henrique**, pertencente a VLAN **USUÁRIOS**. Além disso, você descobriu que ele não está acessando o serviço Samba neste momento. Ou seja, provavelmente é um **ataque** sendo disparado pelo PC de **Henrique**.

💡 Portanto, é necessário realizar a mitigação deste ataque. Inicialmente você poderá realizar o bloqueio deste tráfego no roteador **r0**. Para tanto, você pode usar o ***iptables*** que consiste em um firewall com a funcionalidade de bloquear e liberar o tráfego. Lembre-se de ainda estar conectado ao **Containernet**!

💡 Utilitários

Comandos:

```
r0 iptables -I FORWARD -s <ip_atacante> -j DROP
r0 tshark -i r0-eth3 -w saida.pcap -a duration:5 -d tcp.port==445,nbss
r0 tshark -r saida.pcap
```

Análise:

Verifique se o fluxo diminuiu na interface correspondente a VLAN **DMZ 01**! Em caso positivo, você teve sucesso no bloqueio!

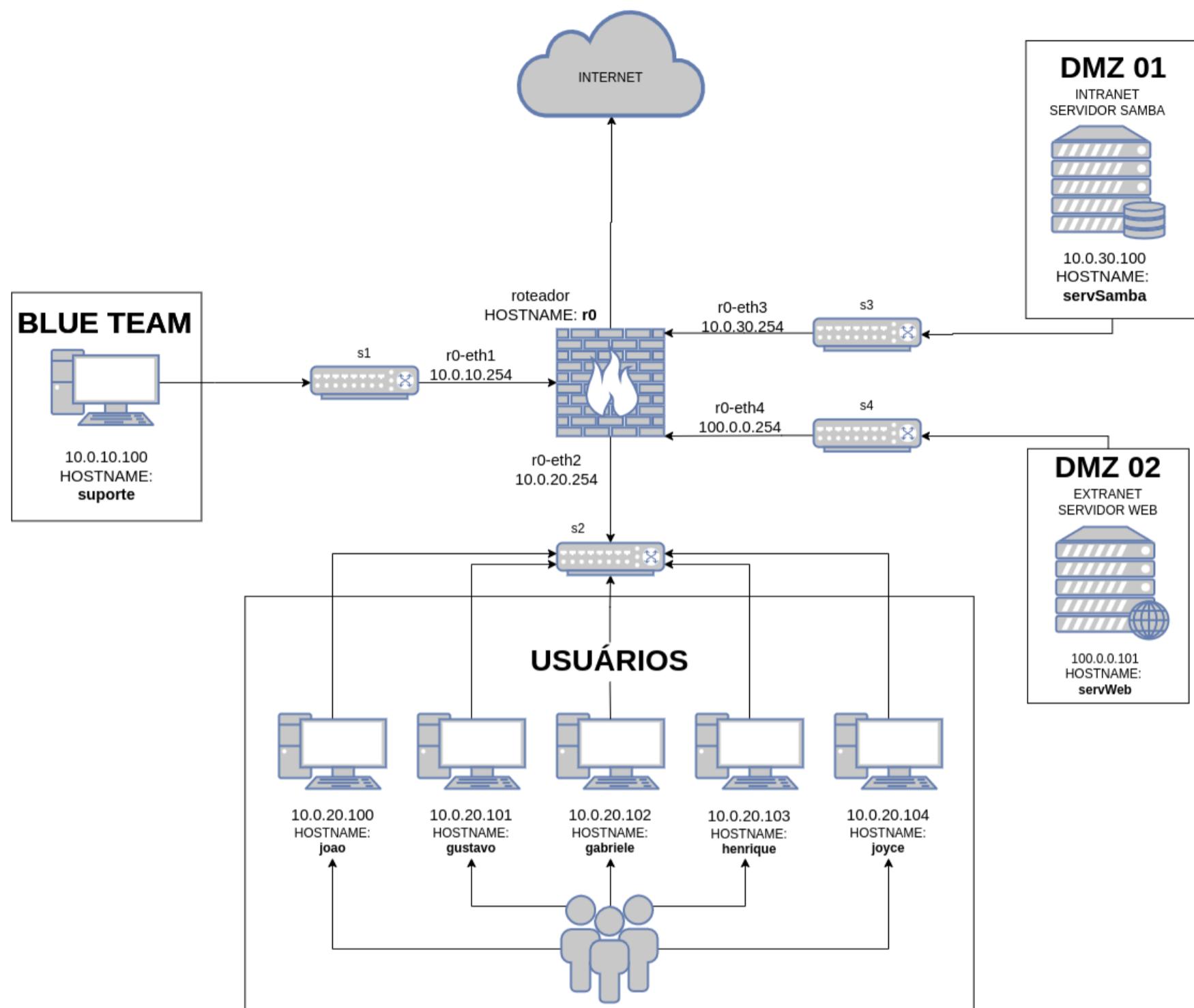
❓ Foi possível bloquear o ataque? Responda **sim** ou **não**.

Resposta:

Questão 10

Tentativas restantes: 3

Vale 1,0 ponto(s).



✖ Você já bloqueou o tráfego com o *iptables*, impossibilitando o atacante de prosseguir. Contudo, as conexões TCP previamente estabelecidas ainda se encontram ativas. Nesse caso, é necessário que desconecte o User Henrique do switch que faz parte da VLAN USUÁRIOS. Lembre-se de ainda estar conectado ao ContainerNet!

✖ Para realizar esse procedimento puxe o cabo do host que está afetando o serviço.

Utilitários

Comando:

```
r0 link henrique <switch_name> down
```

Aviso: Em caso o comando acima retornar alguma mensagem de erro, não se preocupe.

Após ter realizado o processo anterior, verifique se ainda está ocorrendo o ataque!

```
r0 tshark -i r0-eth3 -w saida.pcap -a duration:5 -d tcp.port==445,nbss
r0 tshark -r saida.pcap
```

❓ O servidor Samba ainda está sofrendo o ataque do User Henrique? e qual o nome do switch ao qual ele estava conectado?

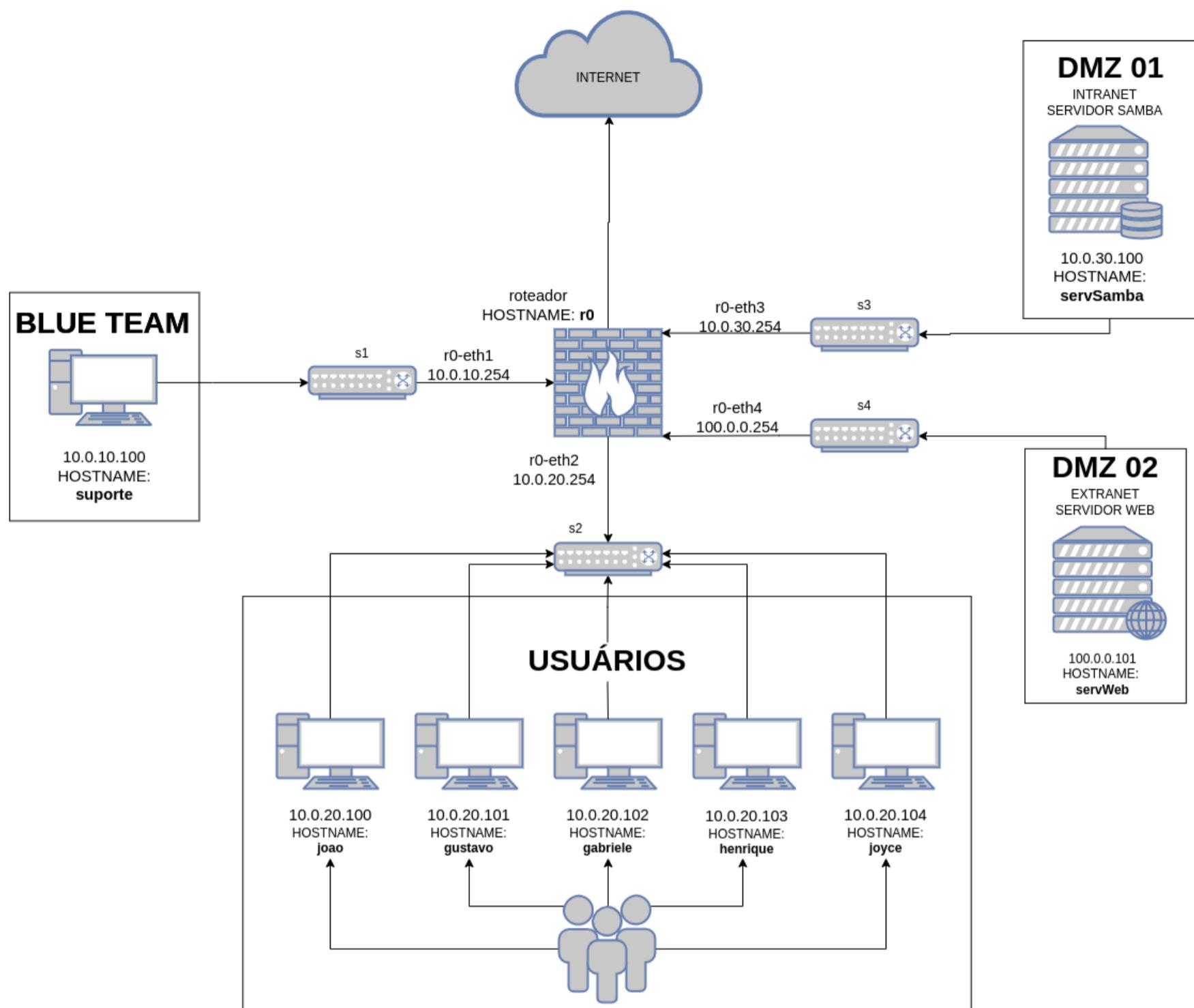
Responda no seguinte formato: sim,switch_name ou não,switch_name

Resposta:

Questão 11

Tentativas restantes: 3

Vale 1,0 ponto(s).



💡 Pronto, possivelmente mitigamos o ataque que estava sendo realizado pelo **User Henrique**. Nesse caso, vamos testar o acesso ao serviço **Samba** novamente.

💡 A partir da conexão com **Suporte**, verifique se o diretório remoto do usuário **Suporte** no servidor **Samba** está acessível via **smbclient**. Seguem os dados novamente:

📝 Utilitários:

Container:

Suporte

Informações do usuário:

Usuário: suporte

Senha: badpass

Diretório remoto: suporte

Comando:

`smbclient //10.0.30.100/suporte -U "suporte"`

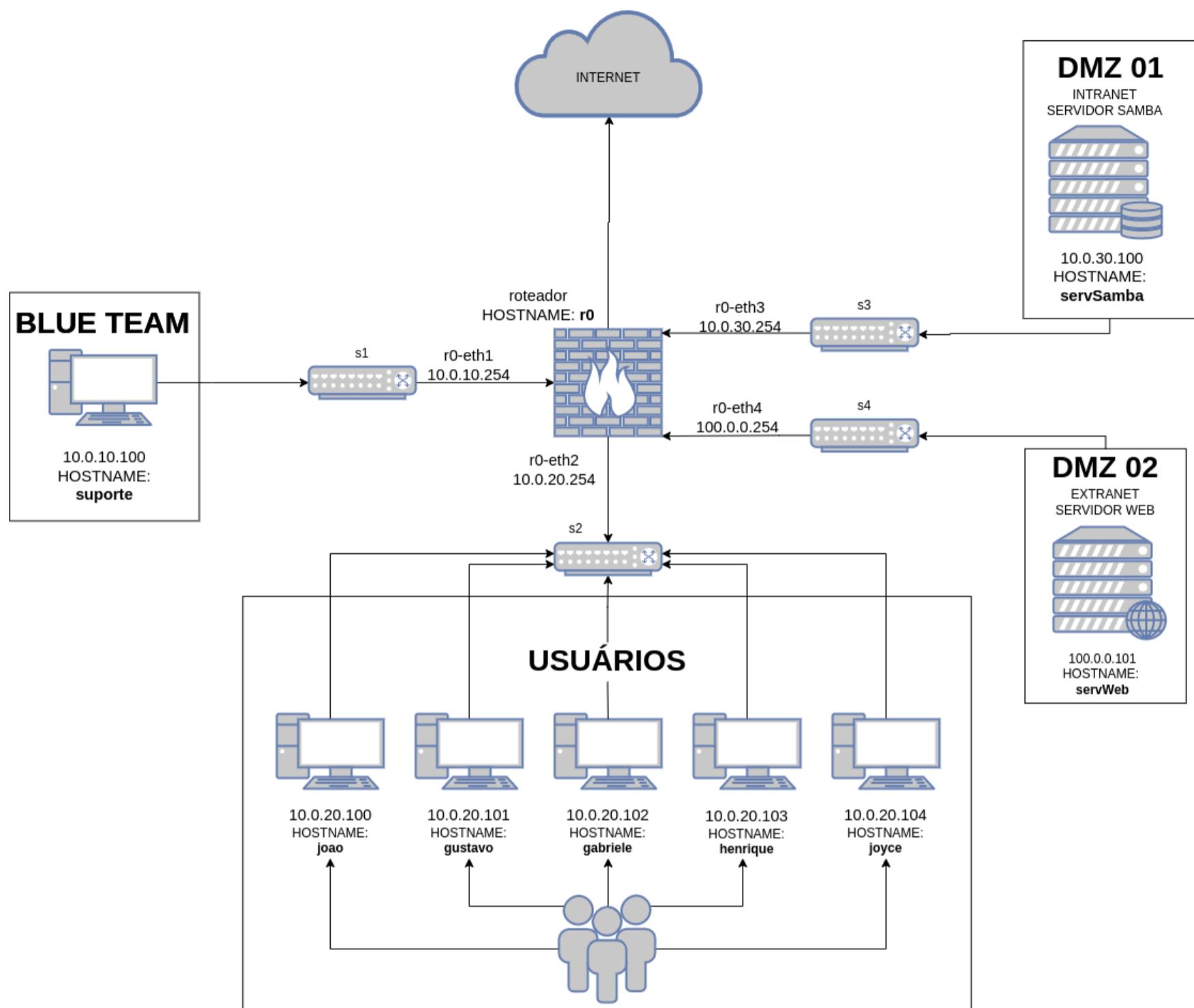
❓ Consegue obter acesso? Responda com "sim" ou "não".

Resposta:

Questão 12

Tentativas restantes: 3

Vale 1,0 ponto(s).



✿ Na questão anterior ainda não foi possível o **Suporte** obter acesso ao serviço **Samba**. Nesse caso, provavelmente qualquer outro usuário também não está conseguindo! Como isso é possível? Você como suporte realizou várias atividades até encontrar o atacante e fez a mitigação do ataque. Que problemão!

✿ Uma das possibilidades seria que o **Server Samba** ainda está sendo atacado, mas agora por outro dispositivo. Para verificar, realize o mesmo procedimento que fez com o **User Henrique**.

✿ Capture e análise o tráfego novamente. Caso seja preciso, filtre para verificar se há um novo atacante. Em caso positivo, faço o bloqueio do tráfego de origem e desconecte o atacante da rede. Finalmente, tente conectar ao **Server Samba** novamente para verificar se possui acesso!

Utilitários

Passo a passo conectado ao *Containernet*:

1º) Use o seguinte comando para capturar o tráfego

```
r0 tshark -i r0-eth3 -w saida.pcap -a duration:5 -d tcp.port==445,nbss
```

2º) Use o seguinte comando ler o tráfego capturado

```
r0 tshark -r saida.pcap
```

3º) Filtre o ip do atacante

```
r0 tshark -r saida.pcap | awk '$4 ~ /04$/ {print $4; exit}'
```

4º) Use o seguinte comando para bloquear o tráfego

```
r0 iptables -I FORWARD -s <ip_atacante> -j DROP
```

5º) Use o seguinte comando para desconectar do switch:

```
r0 link <hostname> <switch_name> down
```

Agora estando conectado ao *Suporte*:

1º) Conectar ao servidor samba via smbclient com a máquina do suporte

```
smbclient //10.0.30.100/suporte -U "suporte"
```

Informações de Usuário:

Usuário: suporte

Senha: badpass

Diretório remoto: suporte

? Conseguiu identificar algum novo atacante? Se sim, qual o nome (hostname) do atacante? Foi possível acessar com *smbclient*?

Responda com o seguinte formato:

Se tiver atacante: sim,hostname_atacante,sim ou sim,hostname_atacante,não

Se não tive atacante: não

Resposta:

©2020 - Universidade Federal do Ceará - Campus Quixadá.

Todos os direitos reservados.

Av. José de Freitas Queiroz, 5003

Cedro – Quixadá – Ceará CEP: 63902-580

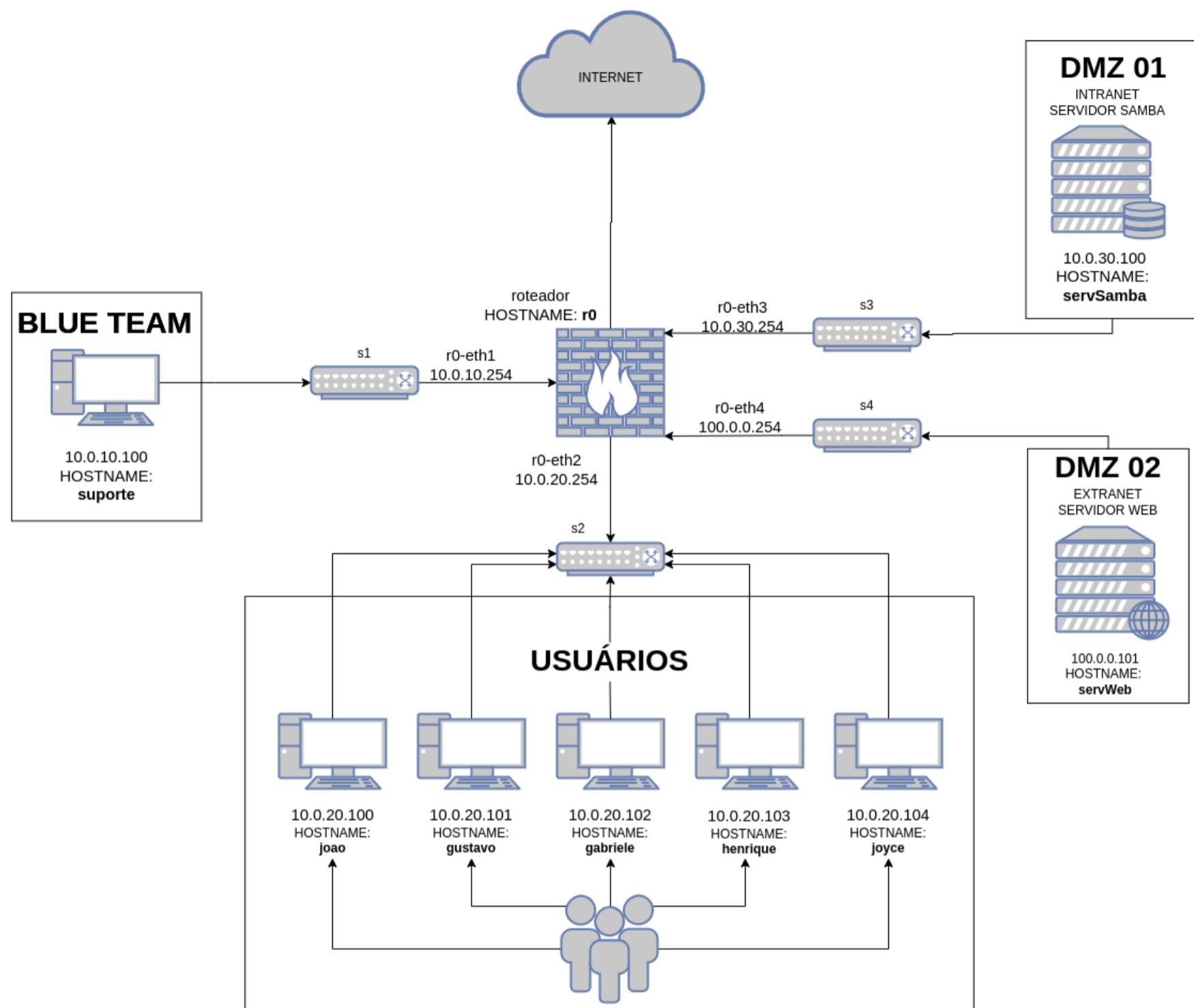
Secretaria do Campus: (88) 3411-9422

 [Obter o aplicativo para dispositivos móveis](#)

Questão 13

Tentativas restantes: 3

Vale 1,0 ponto(s).



📌 Após várias análises, você mitigou os ataques que estavam indisponibilizando o serviço **Samba**. Agora estes serviços estão normalizados!

❓ Quais eram os endereços dos atacantes? Responda exatamente nesse formato: <IP do primeiro atacante> e <IP do segundo atacante>

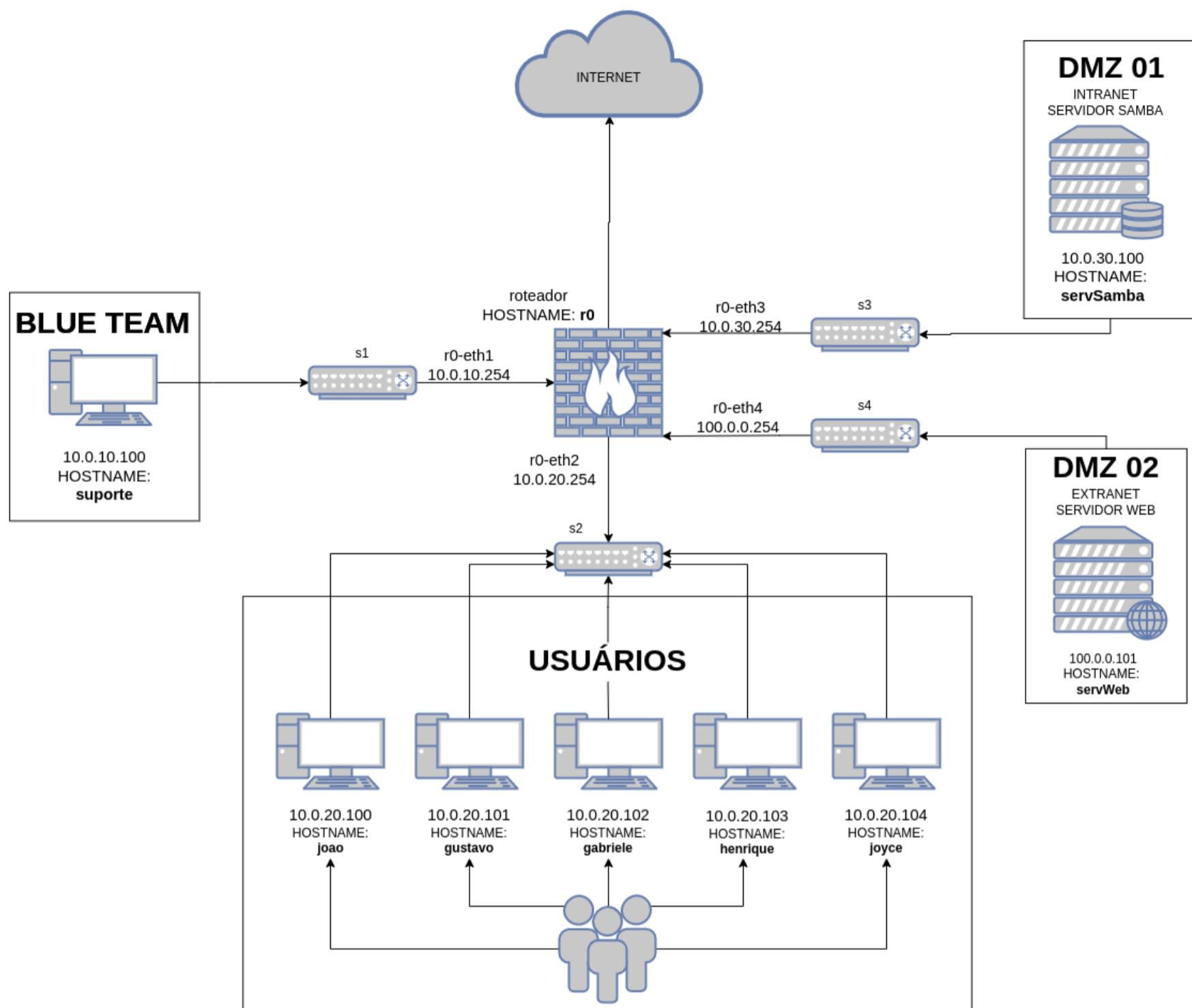
Dica: Verifique a ilustração do cenário logo acima e observe a VLAN USUÁRIOS.

Resposta:

Questão 14

Tentativas restantes: 3

Vale 1,0 ponto(s).



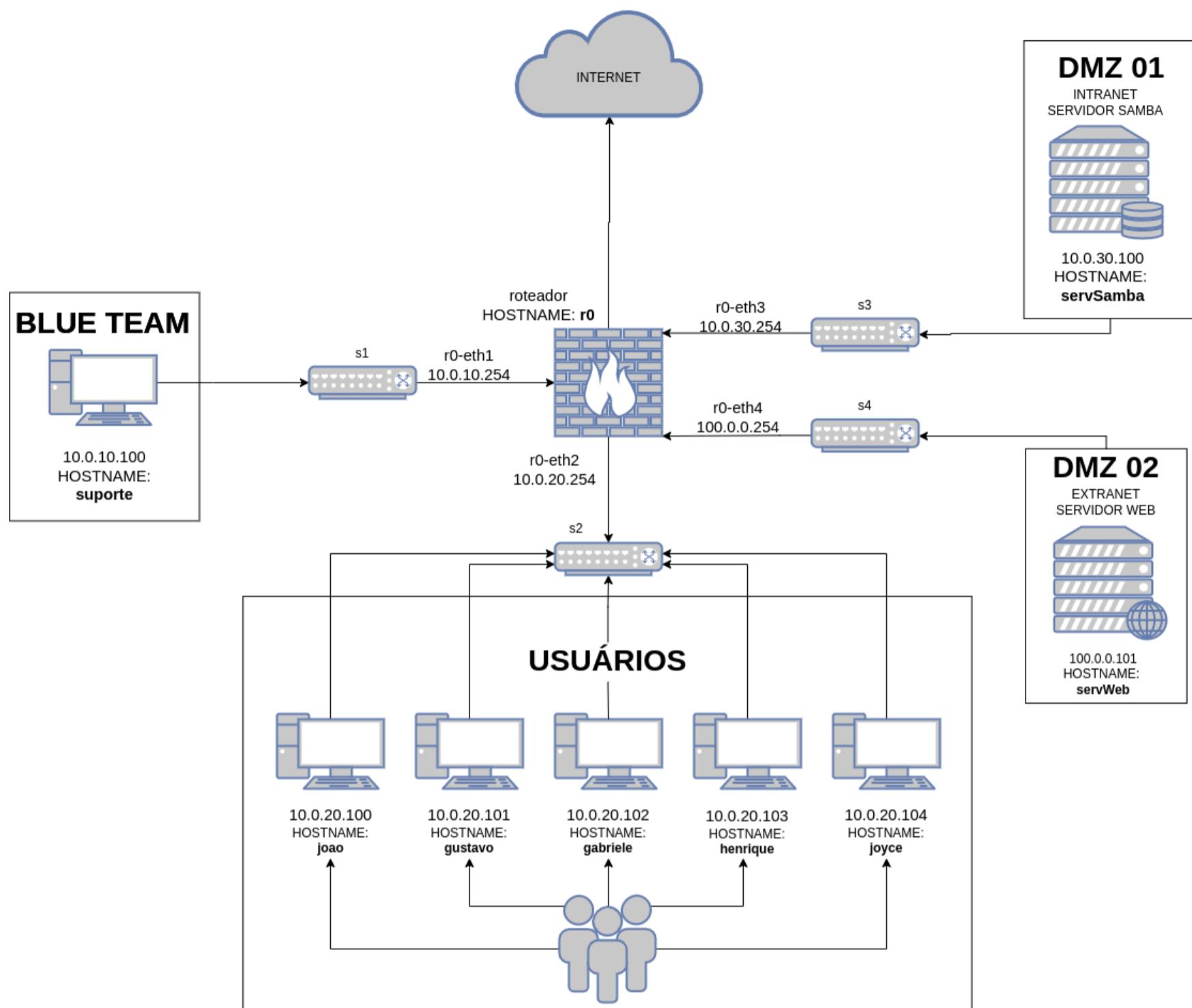
? Os ataques foram originados na **rede externa** ou na **rede interna** da empresa?

Resposta:

Questão 15

Tentativas restantes: 3

Vale 1,0 ponto(s).



? Quais eram os nomes dos *hostnames* dos atacantes? Responda nesse formato: <hostname do atacante 1> e <hostname do atacante 2>

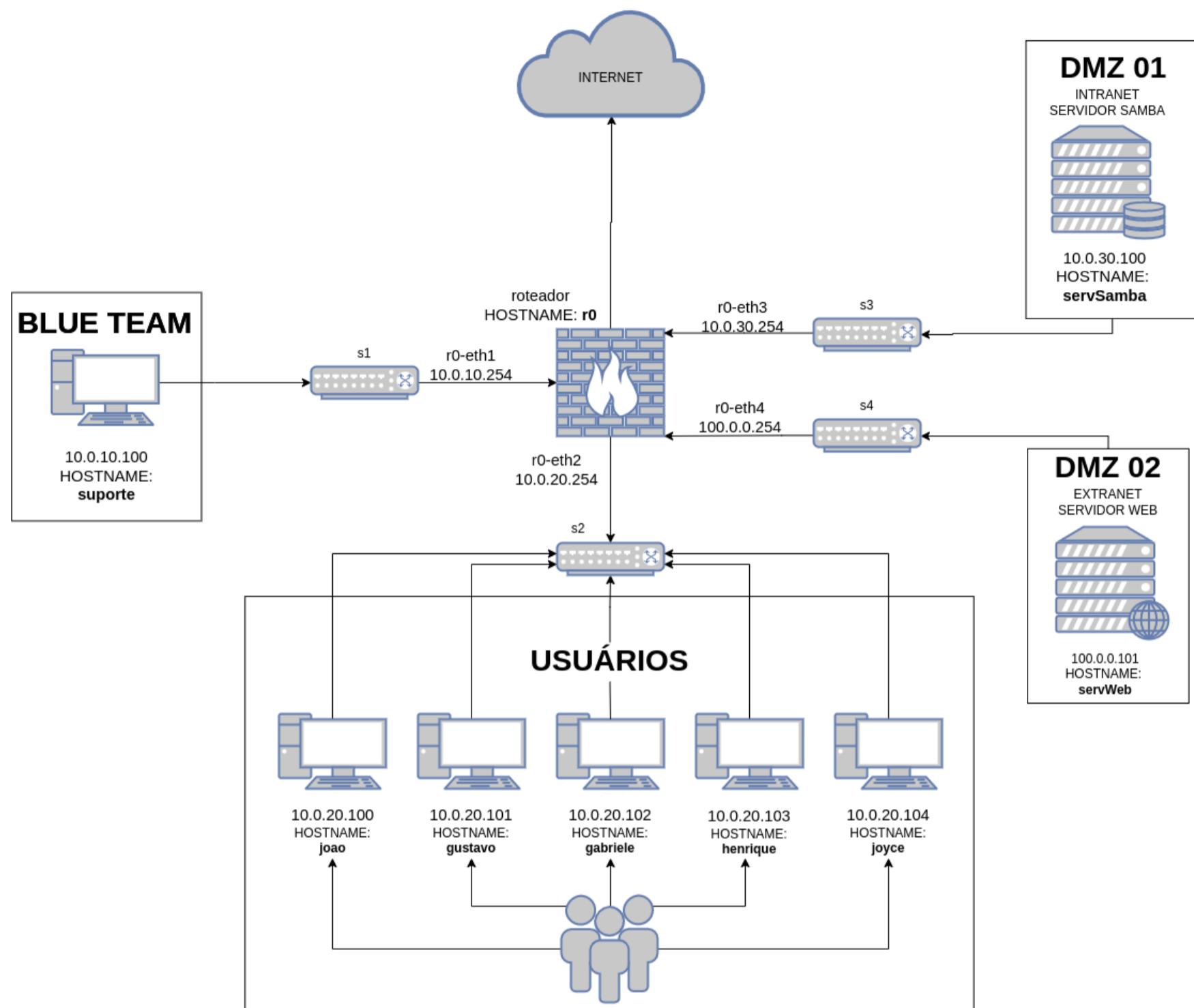
Dica: Verifique a ilustração do cenário logo acima e observe a VLAN USUÁRIOS.

Resposta:

Questão 16

Tentativas restantes: 3

Vale 1,0 ponto(s).



► No mundo da tecnologia há vários tipos de ataques, cada um com seu devido propósito. No ataque mitigado, observamos que a indisponibilidade do serviço Samba foi provocada por uma inundação de pacotes disparado por dois atacantes.

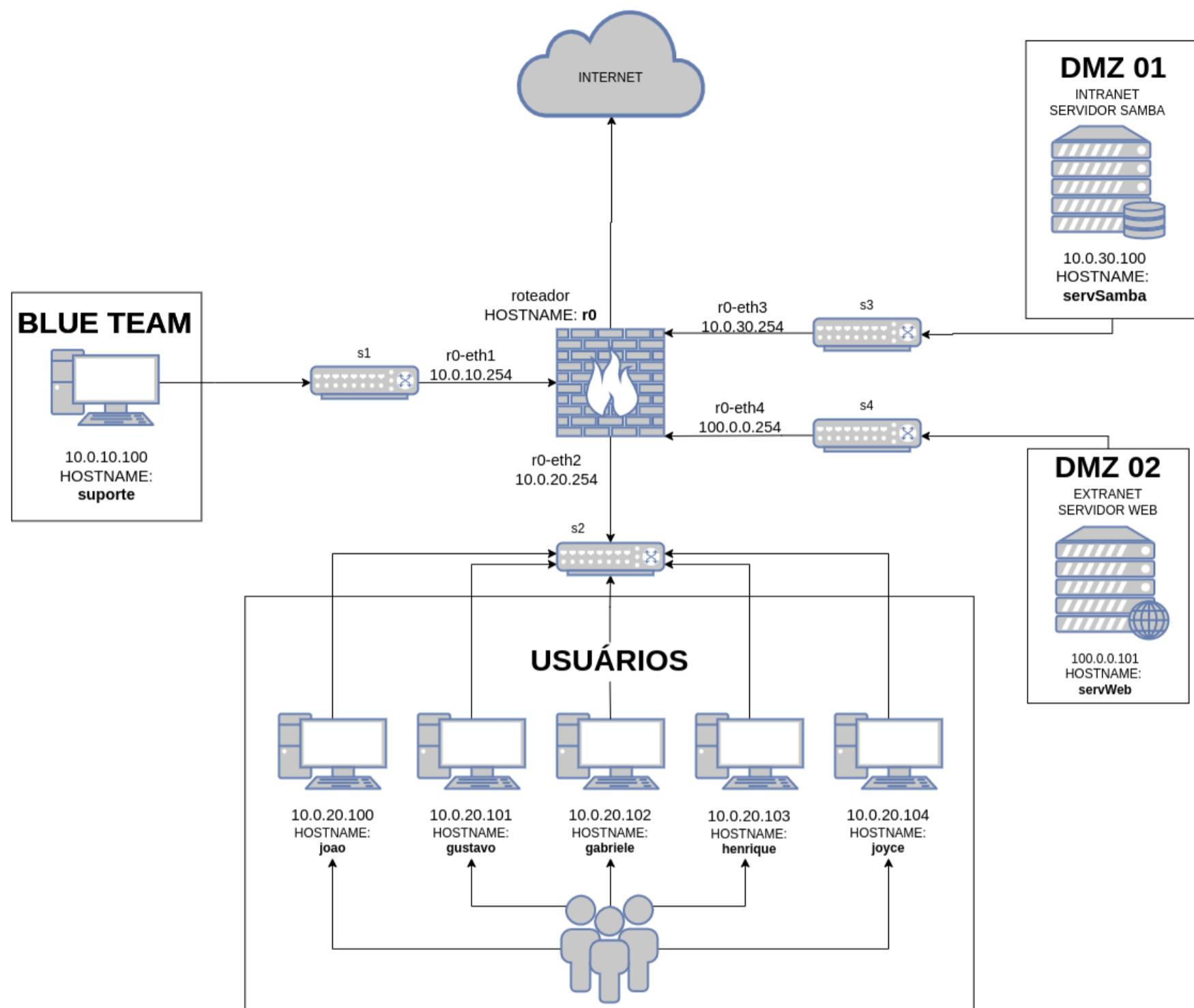
? Como é o nome desse ataque? Responda em letra minúscula!

Resposta:

Questão 17

Tentativas restantes: 3

Vale 1,0 ponto(s).



📌 De modo que seja possível realizar a proteção dos dados contra ameaças internas e externas, é importante que haja a garantia de alguns princípios básicos da segurança da informação.

Confidencialidade que garante que os dados sejam acessíveis e somente pessoas autorizadas possam usufruir desses dados.

Integridade é o pilar que garante que a informação trafegada não foi deletada ou corrompida.

Disponibilidade garante que a informação esteja sempre disponível e acessível para os usuários.

Há outros que também são muito importantes, como a **Autenticidade** e a **Irretratabilidade** (Não-Repúdio).

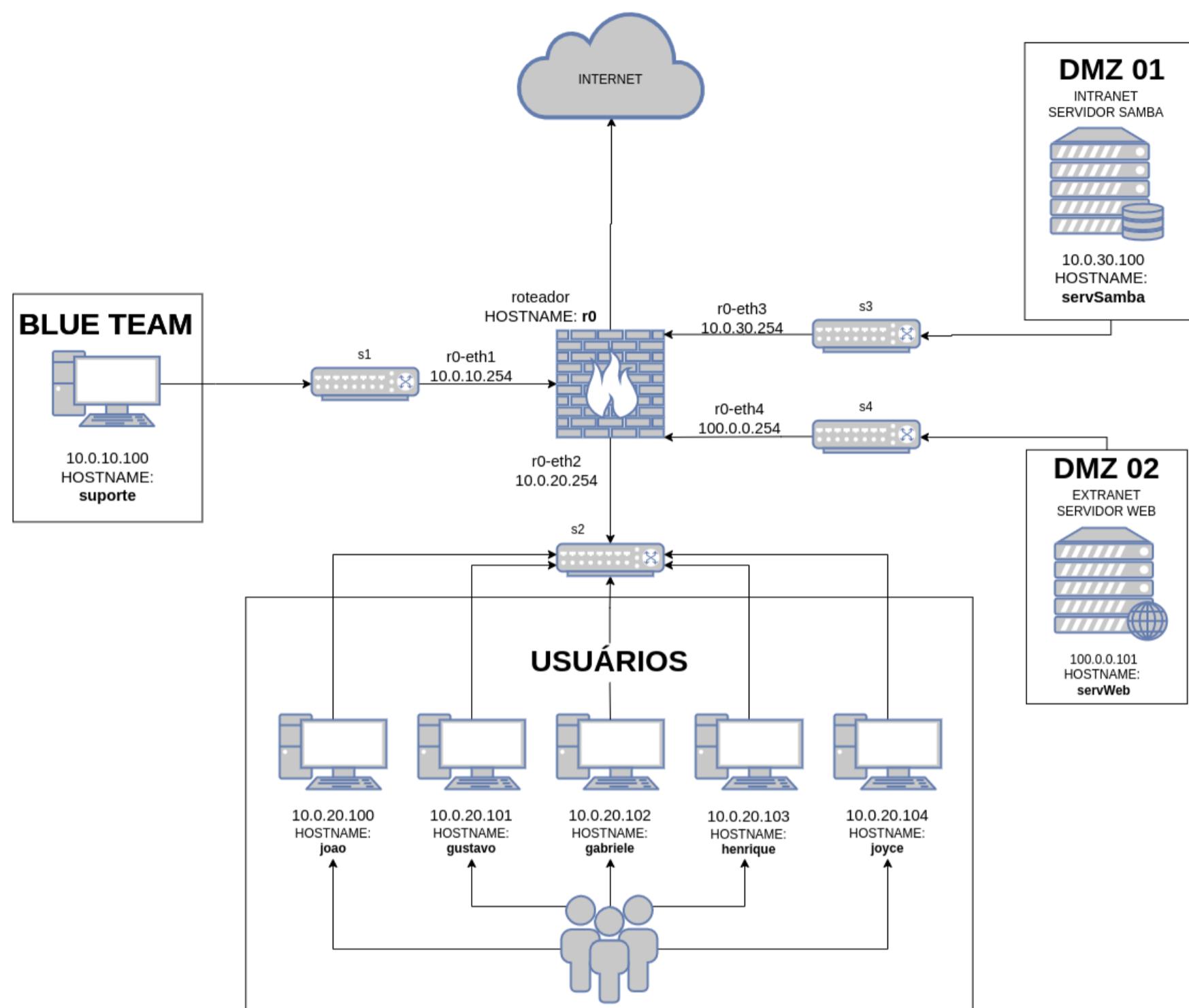
❓ Qual princípio da segurança da informação que o ataque **DDoS** violou? Digite a resposta em minúsculo.

Resposta:

Questão 18

Tentativas restantes: 3

Vale 1,0 ponto(s).



💡 Você, como suporte, analisou o servidor **Samba**, pois o mesmo estava inacessível, e com essas análises chegou a conclusão que o serviço estava sofrendo um ataque **DDoS (Distributed Denial of Service)**. Em seguida, você realizou a mitigação, bloqueando e desconectando o acesso dos atacantes, solucionando assim o problema!

💡 O CEO da corporação está preocupado com a segurança dos dados sigilosos da empresa após um incidente e pediu que você avaliasse o **Servidor Web**. O objetivo é garantir que o serviço funcione sem interrupções e que seja protegido contra cibercriminosos. Além disso, o servidor permite o acesso remoto via SSH, mas somente a equipe de suporte tem acesso às credenciais.

Utilitários

Nota:

Utilizando a máquina **Suporte**, com o protocolo *Internet Control Management Protocol (ICMP)* verifique se a interface do **Server Web** está alcançável na rede.

Comando:

```
ping -c4 <ip_server_web>
```

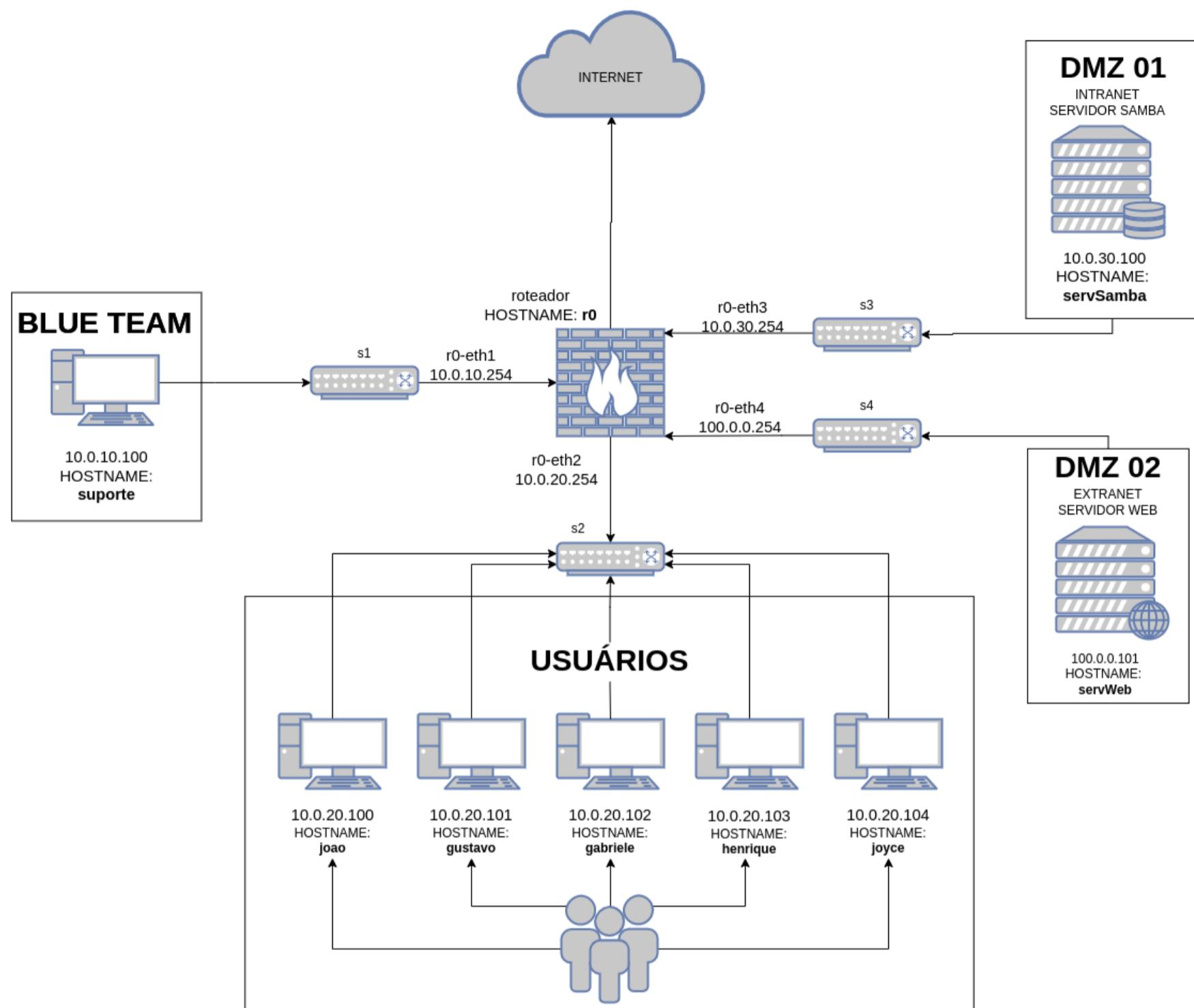
❓ O servidor está alcançável? Responda "sim" ou "não".

Resposta:

Questão 19

Tentativas restantes: 3

Vale 1,0 ponto(s).



💡 Agora, vamos testar se a partir do **Supor te** é possível acessar remotamente o **Server Web** via SSH na porta 22.

Utilitários

Informações de acesso:

Usuário: root

Senha: 123456

Comando:

`ssh <usuario>@<ip_server_web>`

Nota:

Salve o comando usado para efetuar o SSH no **Server Web**, ele será necessário para responder à questão em caso de sucesso.

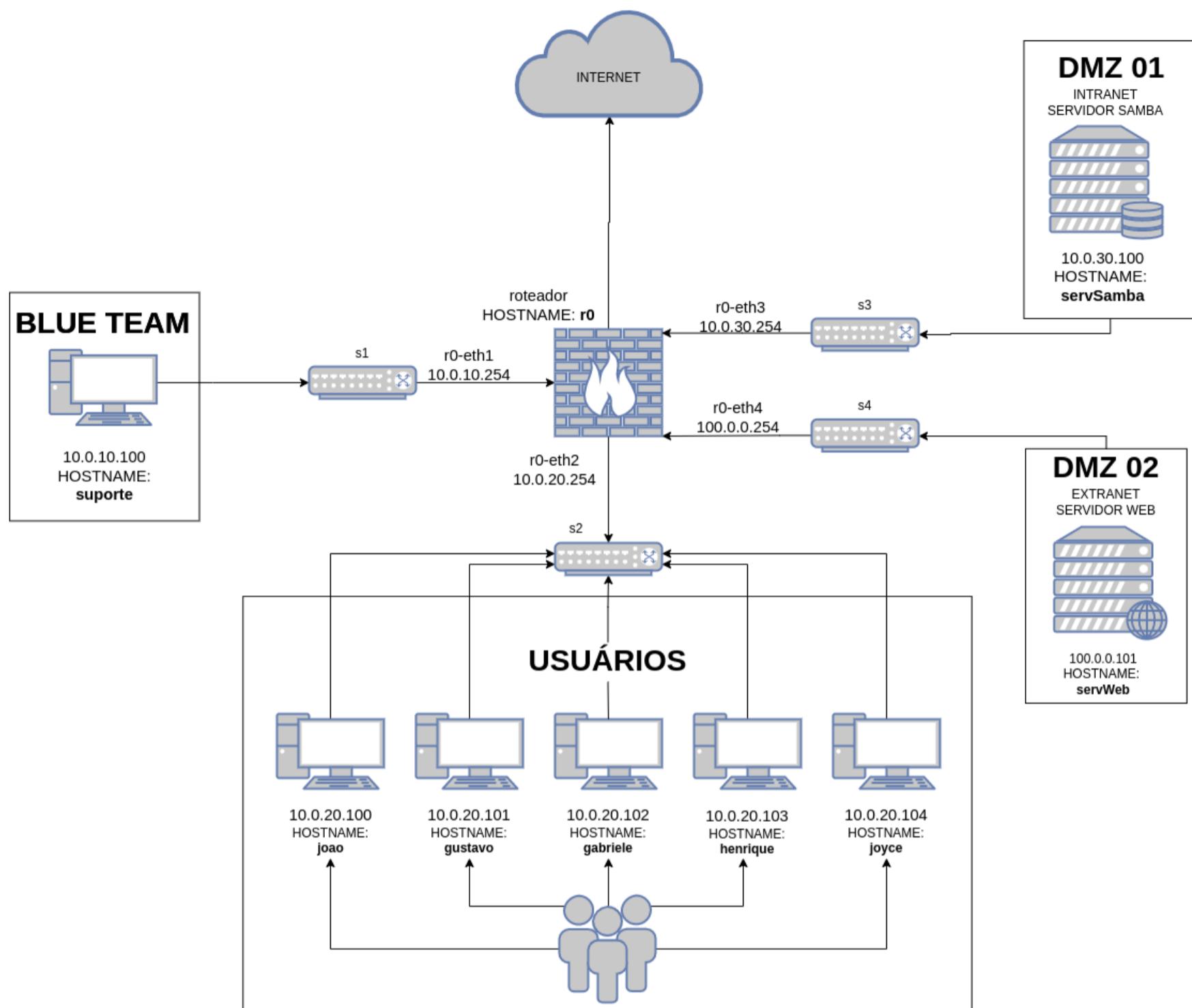
❓ Conseguiu acessar? Responda da seguinte forma: sim,comando ou não

Resposta:

Questão 20

Tentativas restantes: 3

Vale 1,0 ponto(s).



📌 Agora que você verificou que o suporte consegue acessar remotamente o **Server Web**, vamos fazer algumas análises para ter certeza de que todos os serviços do servidor web estão funcionando corretamente.

Utilitários

Mantendo a conexão SSH a partir do **Suporte** para o **Server Web**, utilize o comando **netstat** para verificar as conexões TCP ativas.

Comando:

```
timeout 20s netstat
```

? Existe alguma anormalidade? **sim** ou **não**. Em qual protocolo (não é tcp)? Qual o *state* das conexões com anormalidade? Qual o IP *Foreign Address*? É um IP da rede interna ou externa?

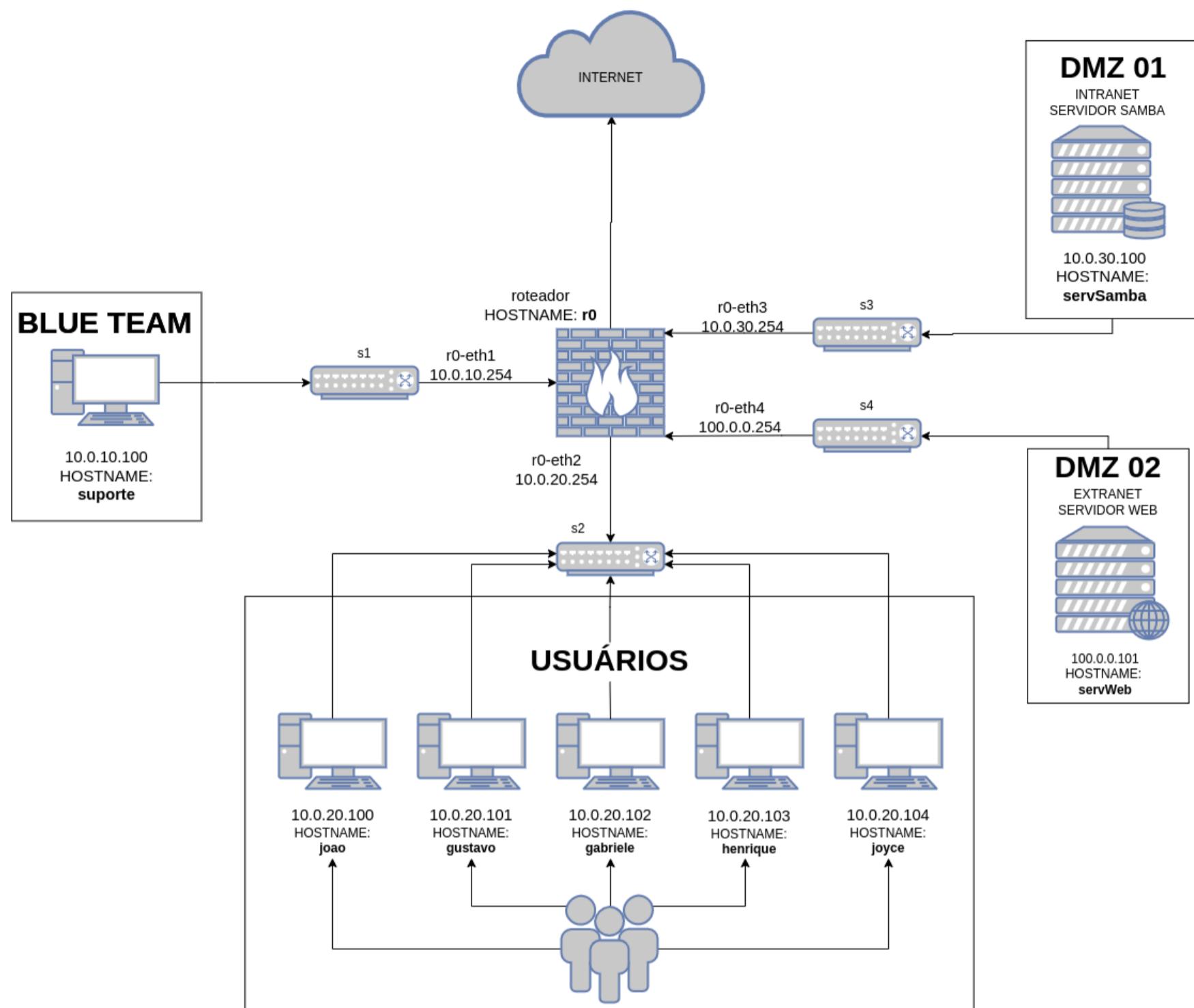
OBSERVAÇÃO: Responda somente com **letras minúsculas**. Separe as respostas por vírgula e sem espaço.

Resposta:

Questão 21

Tentativas restantes: 3

Vale 1,0 ponto(s).



📌 De acordo com a questão anterior, descobrimos que o IP externo **1.178.218.56** está tentando acessar o serviço SSH no **Server Web**. Contudo, somente o **Supor te** tem autorização para isso. Portanto, vamos investigar mais a fundo.

📌 Vale ressaltar que o serviço **SSH** está acessível, logo pode não ser um ataque **DDoS**. Contudo, ainda existem chances de ser um ataque. Nos sistemas operacionais *Linux* existem vários arquivos de **logs** para determinada funcionalidade, todos armazenados na pasta **/var/log**.

📌 Portanto, o próximo passo seria verificar o arquivo de log do serviço **SSH** que trata das tentativas de login, pois precisamos verificar se o suposto atacante está testando pares de login/senha aleatórios para acertar as credenciais verdadeiras e usufruir do **Servidor Web**.

📄 Utilitários

Nota:

Saia da sessão **SSH** com o **Server Web** usando o comando: **exit**. Feito isso, se conecte ao **Server Web**.

Agora, leia o arquivo log de autenticação que possua as tentativas de conexão no servidor.

Comando:

```
cd ..;/var/log  
ls  
tail -n 20 <nome_arquivo>.log
```

Análise:

Verifique a quantidade de tentativas de conexão, senhas inválidas e o tempo entre cada tentativa de conexão.

? Qual o nome do arquivo que armazena os logs de tentativas de login? Realmente possui múltiplas tentativas de conexão partindo de um IP suspeito?

Responda neste formato: <nome do arquivo>,sim ou <nome do arquivo>,não.

Resposta:

[Verificar](#)

©2020 - Universidade Federal do Ceará - Campus Quixadá.

Todos os direitos reservados.

Av. José de Freitas Queiroz, 5003

Cedro – Quixadá – Ceará CEP: 63902-580

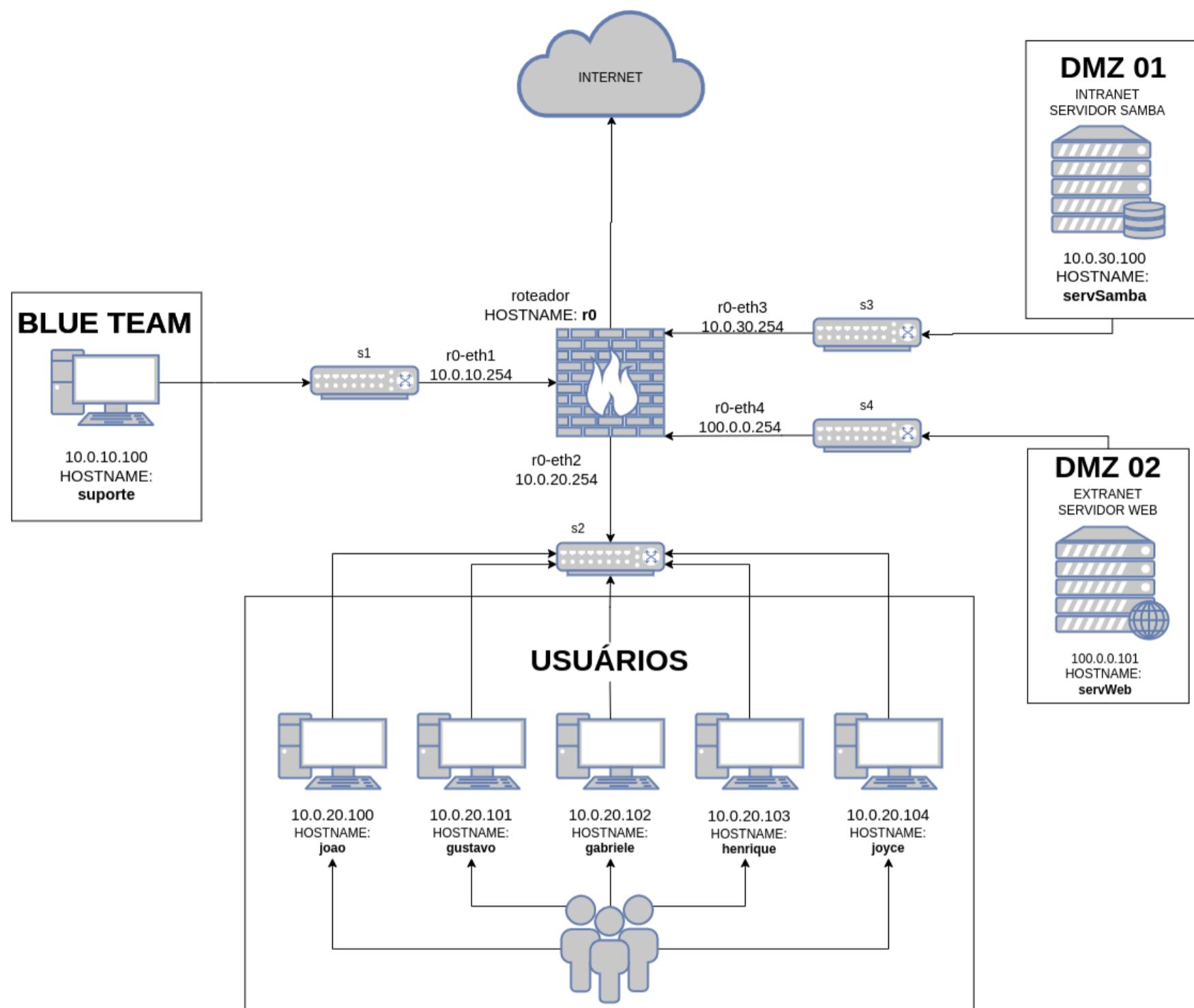
Secretaria do Campus: (88) 3411-9422

[!\[\]\(868cd8bec65c3e41dda30683af45e20b_img.jpg\) Obter o aplicativo para dispositivos móveis](#)

Questão 22

Tentativas restantes: 3

Vale 1,0 ponto(s).



💡 Com a checagem do arquivo de **auth.log**, você conseguiu diagnosticar o problema: o endereço IP **1.178.218.56** está tentando um acesso não autorizado ao **Server Web**, através de múltiplas tentativas de conexão. Isso é um ataque!

💡 Portanto, é necessário realizar a mitigação deste ataque. Inicialmente, você poderá realizar o bloqueio deste tráfego no roteador **r0**. Para tanto, você pode usar o **iptables**, que consiste em um firewall com a funcionalidade de bloquear e liberar o tráfego. Vamos então fazer o bloqueio do tráfego!

📄 Utilitários

Nota:

Esteja conectado no **Containernet**

Comando:

```
r0 iptables -I FORWARD -s 1.178.218.56 -j DROP  
r0 iptables -L
```

Análise:

Agora conecte-se ao **Server Web** e verifique o arquivo **auth.log** novamente, observe os horários dos ataques e se estão surgindo novas tentativas de conexão.

```
tail -n 20 /var/log/auth.log
```

❓ As tentativas de conexão cessaram? Responda **sim** ou **não**.

Resposta:

[Verificar](#)

©2020 - Universidade Federal do Ceará - Campus Quixadá.

Todos os direitos reservados.

Av. José de Freitas Queiroz, 5003

Cedro – Quixadá – Ceará CEP: 63902-580

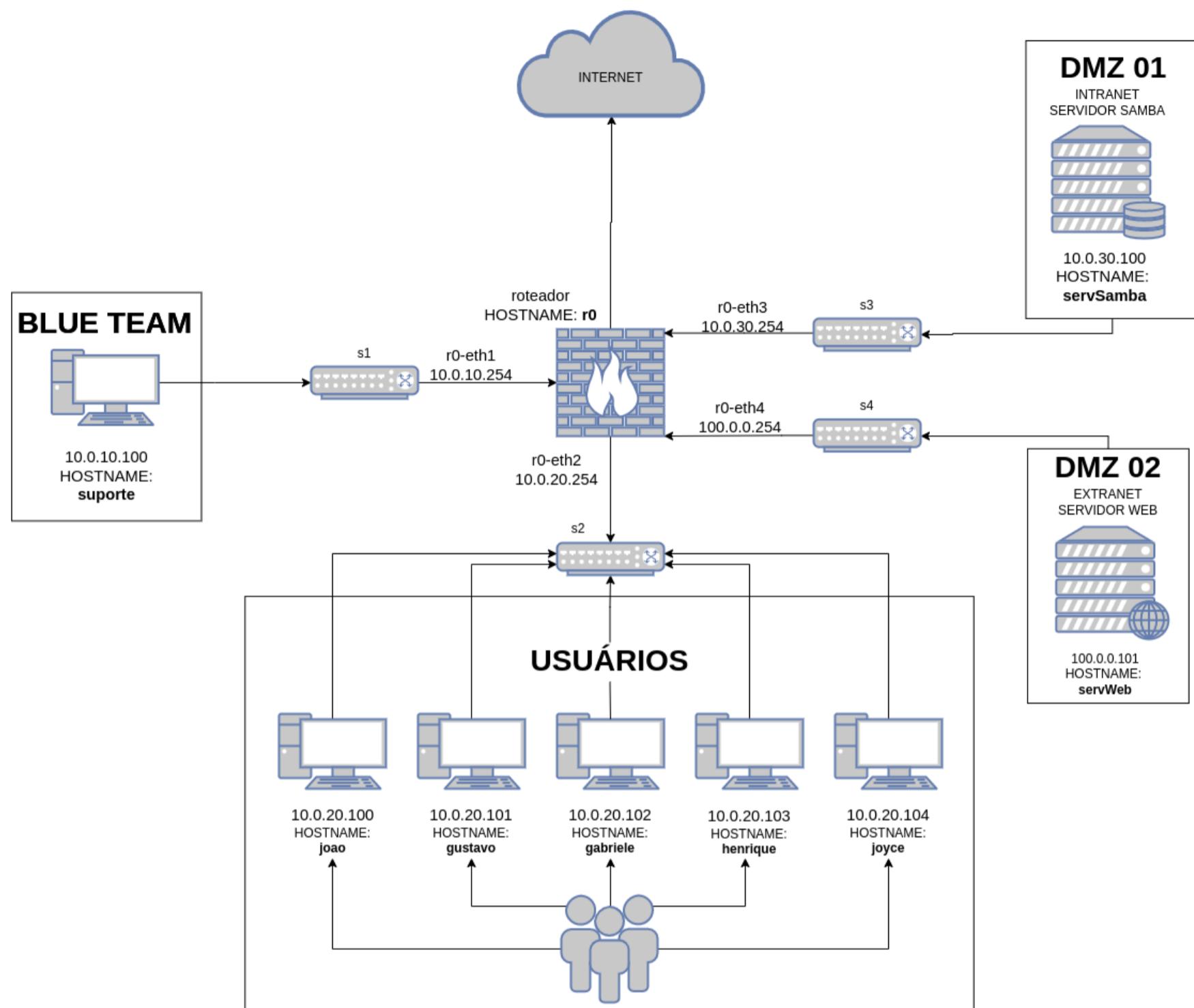
Secretaria do Campus: (88) 3411-9422

 [Obter o aplicativo para dispositivos móveis](#)

Questão 23

Tentativas restantes: 3

Vale 1,0 ponto(s).



💡 Com o passo realizado na questão anterior, foi possível bloquear o tráfego originado pelo IP do atacante. Contudo, outros ataques podem surgir provenientes de outros IP's. Nesse caso, a nossa atividade de mitigação ainda está incompleta.

💡 Um ponto que facilita a execução de ataques em serviços na Internet é o uso da porta padrão. No caso do nosso serviço SSH, estamos usando a porta padrão 22. Portanto, vamos dificultar a vida de futuros atacantes alterando a porta padrão para outra completamente diferente. Seguem os passos necessários que dever ser executados diretamente no **Server Web**:

Utilitários

Passo a Passo:

1º) Liste os processos no **Server Web** e identifique o PID do serviço SSH

```
ps aux
```

Exemplo do pid que deverá ser encerrado:

```
19 root 0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
```

2º) Matar o processo SSH no **Server Web**

```
kill pid <id_do_processo>
```

3º) Verifique novamente se o serviço SSH realmente foi encerrado

```
ps aux
```

4º) Initialize o serviço SSH na porta 40157

```
/usr/sbin/sshd -D -p 40157 2>&1 &
```

5º) Verifique se o serviço SSH realmente está em execução e na porta 40157

```
ps aux
```

Nota:

Para testar se realmente trocou a porta corretamente, entre em **Supporte** e acesse remotamente o **Server Web**, utilizando a nova porta.

? Conseguiu acessar? **sim** ou **não**. Qual comando você usou para acessar?

OBSERVAÇÃO: respostas separadas por vírgulas e sem espaço.

Resposta:

Verificar

©2020 – Universidade Federal do Ceará – Campus Quixadá.

Todos os direitos reservados.

Av. José de Freitas Queiroz, 5003

Cedro – Quixadá – Ceará CEP: 63902-580

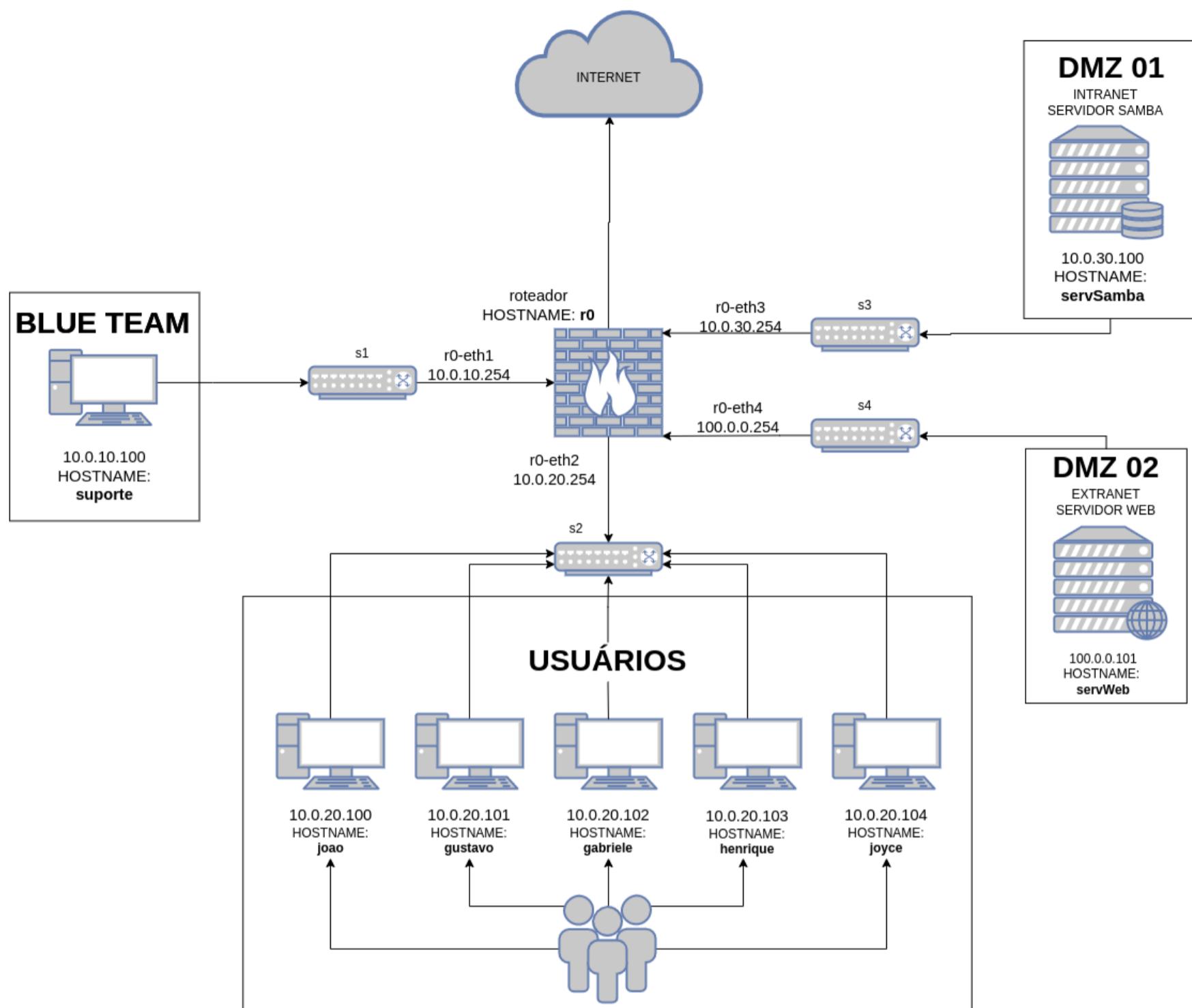
Secretaria do Campus: (88) 3411-9422

 [Obter o aplicativo para dispositivos móveis](#)

Questão 24

Tentativas restantes: 3

Vale 1,0 ponto(s).



💡 Estamos melhorando a segurança do servidor, mas podemos fazer ainda mais. Percebeu que a senha de acesso ao **SSH** é 123456? Não acha muito fácil? Utilizar senhas mais complexas irá dificultar a atividade de novos atacantes. A Cartilha de Segurança da Internet, no Fascículo [Senhas](#), possui boas práticas para a escolha, uso e armazenamento de senhas de forma segura.

💡 Portanto, você deve fazer a troca da senha de acesso. Para tanto, atualize a senha atual para outra encontrada no arquivo `/root/pass.txt` do **Server Web**. Para a troca de senha do usuário **root** utilize os seguintes comandos:

💡 Utilitários

Comando:

```
cat /root/pass.txt
```

Aviso: Salve a senha acima em alguma local, você irá precisar dela para o próximo passo!

```
passwd root
```

Nota:

Vai pedir a nova senha (introduza a senha que estava guardada no arquivo `/root/pass.txt`)

Vai pedir para repetir a senha digitada (introduza a senha novamente)

Agora para verificar se o procedimento teve sucesso, se conecte em **Suporte** e faça um acesso SSH ao **Server Web** usando a nova senha.

❓ Foi possível trocar a senha do usuário **root** e fazer o SSH utilizando a nova senha? **sim** ou **não**.

Resposta:

[Verificar](#)

©2020 - Universidade Federal do Ceará - Campus Quixadá.

Todos os direitos reservados.

Av. José de Freitas Queiroz, 5003

Cedro – Quixadá – Ceará CEP: 63902-580

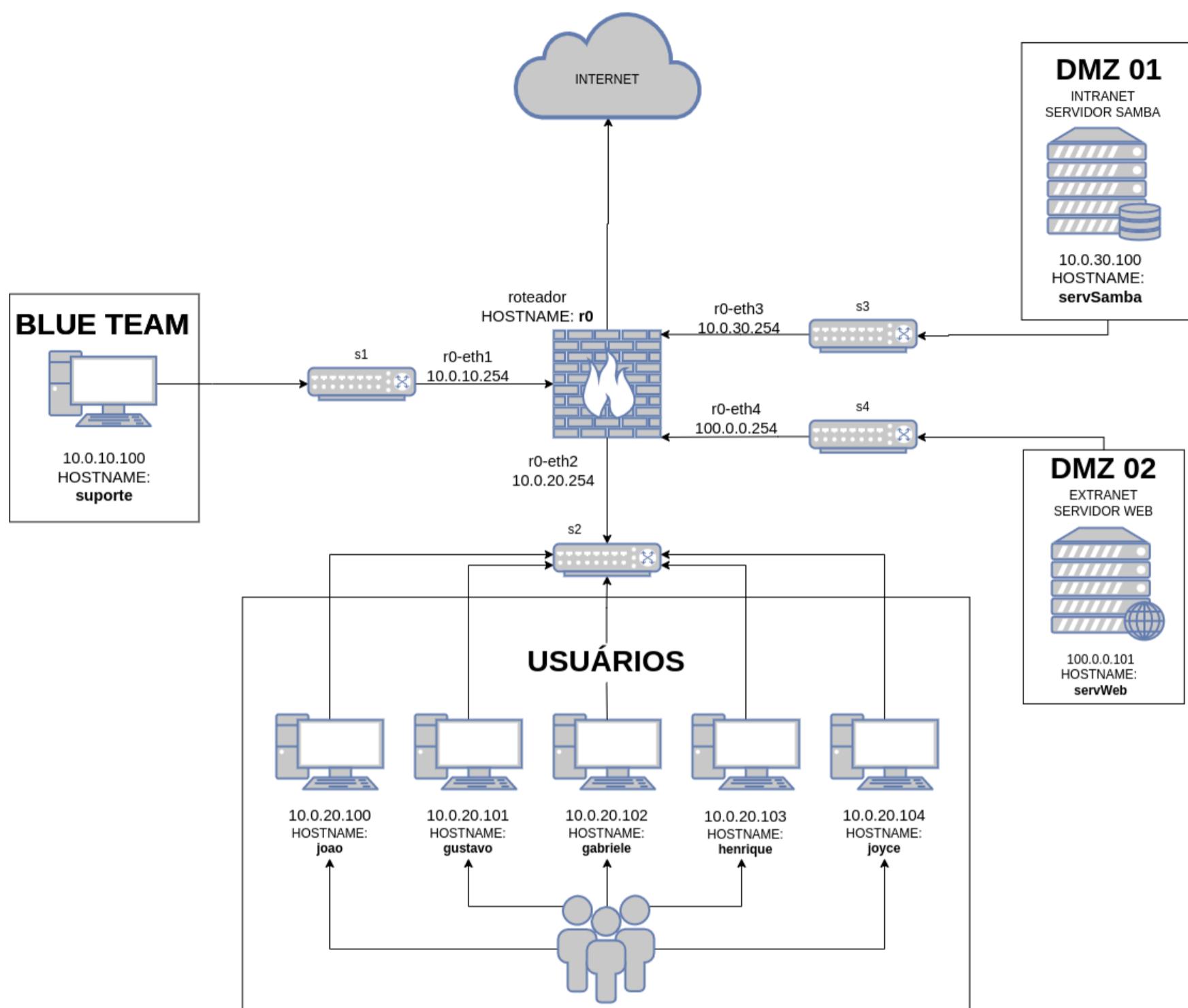
Secretaria do Campus: (88) 3411-9422

 [Obter o aplicativo para dispositivos móveis](#)

Questão 25

Tentativas restantes: 3

Vale 1,0 ponto(s).



💡 Com a mitigação completa e as configurações do servidor mais seguras, o CEO da empresa pode ficar mais tranquilo!

💡 Agora, sabendo qual é o IP do atacante, vamos verificar de qual país que o ataque se originou. Para tanto, a ferramenta **geoiplookup** possui a finalidade de identificar qual o país de origem.

💡 Utilitários

Nota:

Tenha certeza de estar conectado em **Suporte**

Comando:

```
geoiplookup 1.178.218.56
```

❓ Qual o nome de país? Responda a primeira letra em caixa alta. Como neste exemplo: **China**

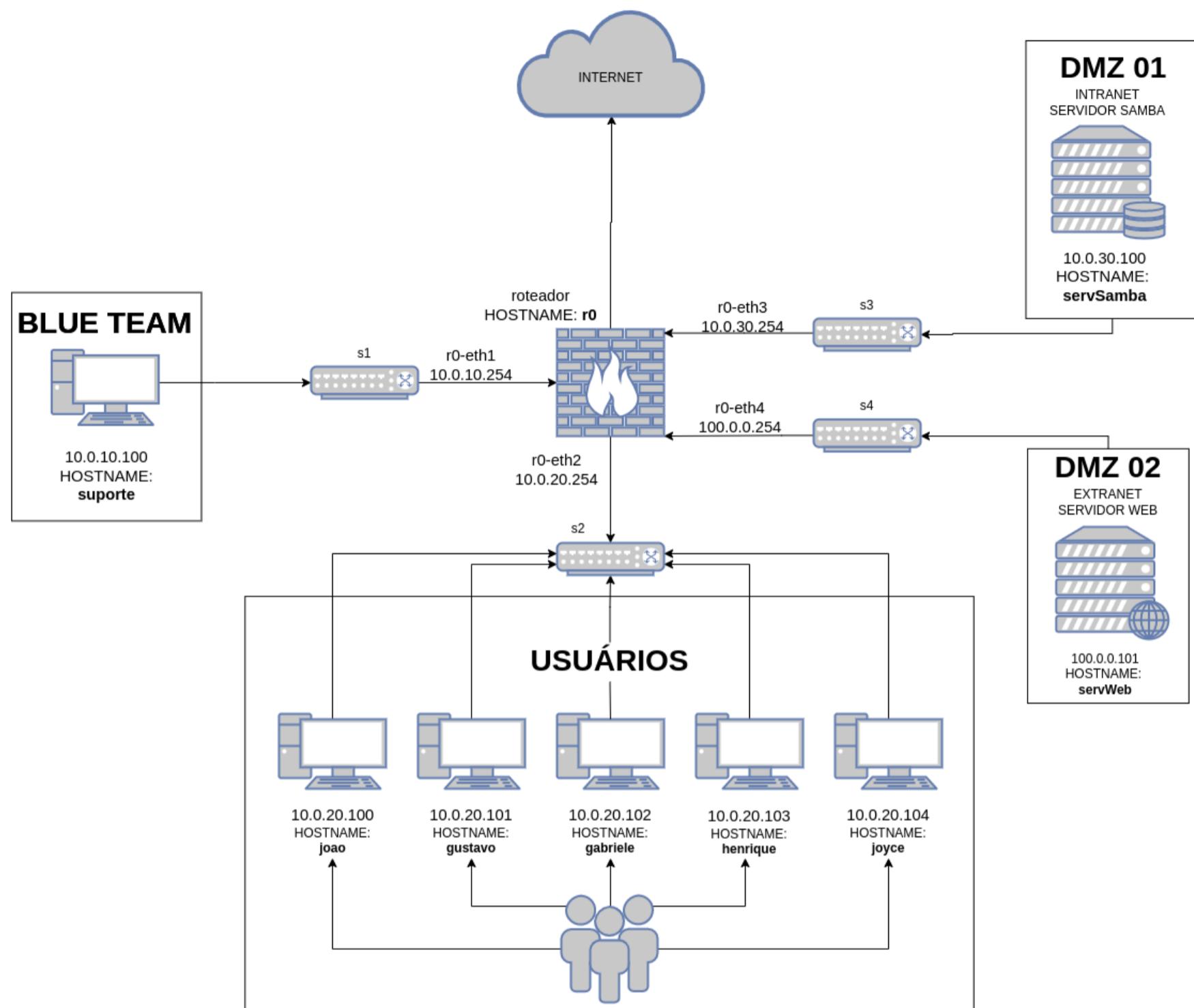
Resposta:

Verificar

Questão 26

Tentativas restantes: 3

Vale 1,0 ponto(s).



✿ Na atualidade da tecnologia que vivemos, há vários tipos de ataques, cada um com seu devido propósito. Podendo observar que o atacante utilizou dicionários contendo logins e senhas com o propósito de acertar as credenciais verdadeiras, a fim de obter acesso ao serviço para possivelmente roubar e alterar informações.

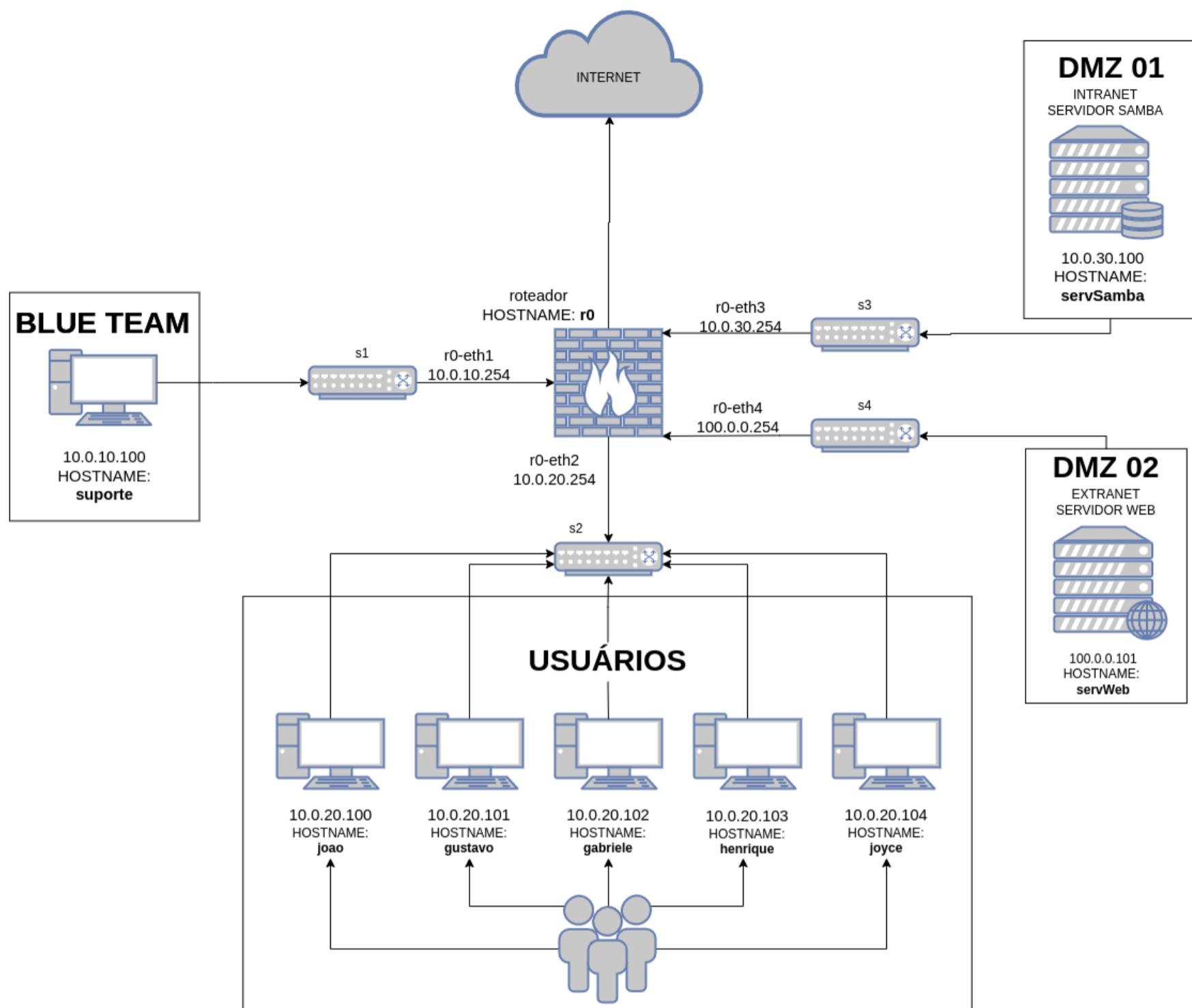
? Qual nome do ataque descrito anteriormente? Responda em letra minúscula!

Resposta:

Questão 27

Tentativas restantes: 3

Vale 1,0 ponto(s).



De modo que seja possível realizar a proteção dos dados contra ameaças internas e externas, é importante que haja a garantia de alguns princípios básicos da segurança da informação.

Confidencialidade que garante que os dados sejam acessíveis e somente pessoas autorizadas possam usufruir desses dados.

Integridade é o pilar que garante que a informação trafegada não foi deletada ou corrompida.

Disponibilidade garante que a informação esteja sempre disponível e acessível para os usuários.

Há outros que também são muito importantes, como a **Autenticidade** e a **Irretratabilidade** (Não-Repúdio).

? Qual princípio da segurança da informação o ataque de **força bruta** poderia ter violado, caso tivesse sucesso?
Digite a resposta em minúsculo.

Resposta: