



UNIVERSIDADE DO SUL DE SANTA CATARINA

AUTORIA DO TRABALHO

TOPOLOGIA EMPRESA NOLIMITS2

Tubarão

2022

**ANDRÉ MENDES NUNES
DIOGO SCHMITZ MARTINS
GUSTAVO BERTI DA SILVA
MATHEUS SOUZA MENDES**

TOPOLOGIA EMPRESA NOLIMITS2

Trabalho de Conclusão de UC Sistemas
Computacionais e Conectividade.

Orientador: Ms. Marcos Tonon Alcantara

LISTA DE FIGURAS

Figura 1 - Logo representativa	5
Figura 2 - Topologia logica.....	9
Figura 3 - Exemplo de VLAN configuradas	10
Figura 4 - Configuração pool DHCP	11
Figura 5 - Protocolo RIP.....	12
Figura 6 - Lista de acesso.....	13
Figura 7 - AWS	14
Figura 8 - Zonas de Disponibilidade	14
Figura 9 - Grupo de segurança service publico	15
Figura 10 - Requisição porta 80 service publico	15
Figura 11 - Requisição porta 8080 servidor interno	16
Figura 12 - Conexão bastion host via SSH	17

LISTA DE TABELAS

Tabela 1 - Setor P&D	6
Tabela 2 - Setor qualidade	6
Tabela 3 - Setor compras.....	7
Tabela 4 - Setor logística	7
Tabela 5 - Rede roteador	8

SUMÁRIO

1	INTRODUÇÃO	5
2	DIVISÃO DAS REDES	6
2.1	SETOR P&D	6
2.2	SETOR QUALIDADE	6
2.3	SETOR COMPRAS.....	7
2.4	SETOR LOGISTICA.....	7
2.5	REDE ROTEADOR.....	7
3	CONFIGURAÇÃO DE REDES.....	9
3.1	CONFIGURAÇÃO VLAN	9
3.2	CONFIGURAÇÃO DHCP.....	10
3.3	PROTOCOLO RIP	11
3.4	LISTA DE ACESSOS (UCL)	12
4	UTILIZAÇÃO DA NUVEM	14
4.1	ZONAS DE DISPONIBILIDADE	14
4.2	WEBSERVICE LINUX.....	15
4.3	SERVICE LINUX PRIVADO	16
4.4	BASTION HOST.....	16
5	ORÇAMENTO DOS DISPOSITIVOS	18

1 INTRODUÇÃO

Nesta topologia da empresa Nolimits2 foi construída com base em dois prédios separados a 500 metros de distância. Um prédio seria usado para produção e outro para logística. Para produção estão previstos 195 computadores, separados por setores, P&D irá conter 63 dispositivos, qualidade 102 dispositivos e compras 30 dispositivos. O setor P&D deverá ser isolado dos demais setores para garantir a confiabilidade do mesmo. Para a logística contará apenas 1 setor, com 82 dispositivos.

Será apresentada nesta topologia modelo lógico, físico e também a possibilidade do escalonamento de serviços para empresa utilizando a nuvem, neste caso o serviço escolhido para fornecer a estrutura foi a AWS (amazon).



Figura 1 - Logo representativa

2 DIVISÃO DAS REDES

Foram divididas as redes com base no número de hosts de cada setor, ao todo foram utilizados 14 switches e 2 roteadores, cada setor e suas respectivas redes serão descritas abaixo.

2.1 SETOR P&D

Neste setor foram utilizados 3 switches, cada switch com 24 portas, totalizando 72 portas disponíveis. Cada switch utilizara uma subdivisão do endereço de IP 192.168.1.0/26 com a máscara 255.255.255.192, cada sub rede poderá conter 62 hosts.

	Network	Broadcast
Switch 1 – VLAN 10	192.168.1.0	192.168.1.63
Switch 2 – VLAN 20	192.168.1.64	192.168.1.127
Switch 3 – VLAN 30	192.168.1.128	192.168.1.191

Tabela 1 - Setor P&D

2.2 SETOR QUALIDADE

Neste setor foram utilizados 5 switches, cada switch com 24 portas, totalizando 120 portas disponíveis. Cada switch utilizara uma subdivisão do endereço de IP 192.162.2.0/27 com a máscara 255.255.255.224, cada sub rede poderá conter 30 hosts.

	Network	Broadcast
Switch 4 – VLAN 50	192.168.2.0	192.168.2.31
Switch 5 – VLAN 60	192.168.2.32	192.168.2.63
Switch 6 – VLAN 70	192.168.2.64	192.168.2.95
Switch 7 – VLAN 80	192.168.2.96	192.168.2.127
Switch 8 – VLAN 90	192.168.2.128	192.168.2.159

Tabela 2 - Setor qualidade

2.3 SETOR COMPRAS

Neste setor foram utilizados 2 switchs, cada switch com 24 portas, totalizando 48 portas disponíveis. Cada switch utilizara uma subdivisão do endereço de IP 192.168.3.0/25 com a máscara 255.255.255.128, cada sub rede poderá conter 126 hosts.

	Network	Broadcast
Switch 9 – VLAN 130	192.168.3.0	192.168.3.127
Switch 10 – VLAN 140	192.168.3.128	192.168.3.255

Tabela 3 - Setor compras

2.4 SETOR LOGISTICA

Neste setor foram utilizados 4 switchs, cada switch com 24 portas, totalizando 96 portas disponíveis. Cada switch utilizara uma subdivisão do endereço de IP 192.162.4.0/26 com a máscara 255.255.255.192, cada sub rede poderá conter 62 hosts.

	Network	Broadcast
Switch 11 – VLAN 150	192.168.4.0	192.168.4.63
Switch 12 – VLAN 160	192.168.4.64	192.168.4.127
Switch 13 – VLAN 170	192.168.4.128	192.168.4.191
Switch 14 – VLAN 180	192.168.4.192	192.168.4.255

Tabela 4 - Setor logística

2.5 REDE ROTEADOR

Neste setor foram utilizados 2 roteadores para comunicação entre os prédios, utilizando cabeamento de fibra, configurado uma sub rede apenas para comunicação entre os roteadores, rede 192.168.5.0/30 com apenas 2 host para utilização.

	Network	Broadcast
Roteador	192.168.5.0	192.168.5.3

Tabela 5 - Rede roteador

3 CONFIGURAÇÃO DE REDES

Será demonstrado abaixo o processo de configuração para criação de VLANS, encapsulamento das sub redes, configuração de DHCP, a utilização de UCL (lista de acessos) para o isolamento do setor P&D dos outros setores e também será utilizado o protocolo RIP para a divulgação das redes entre os roteadores, a figura 1 demonstra o projeto logico.

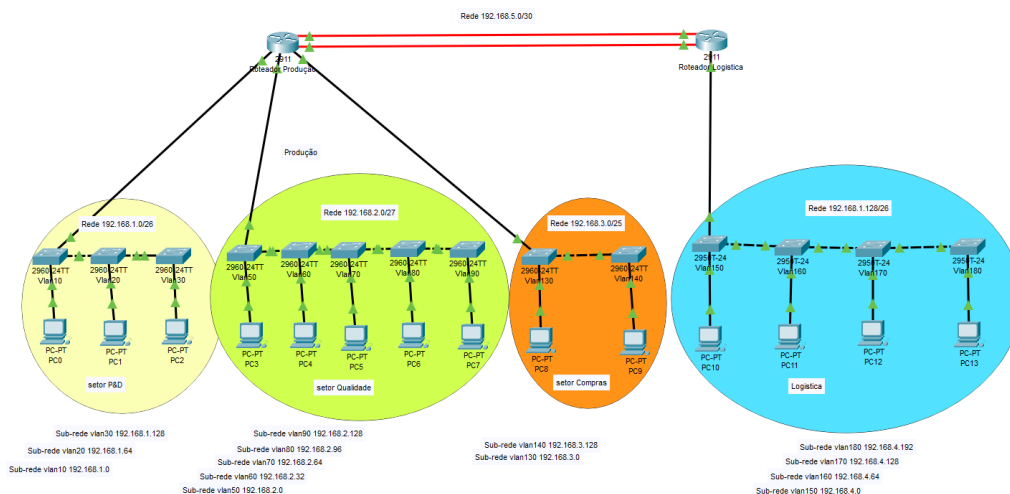


Figura 2 - Topologia logica

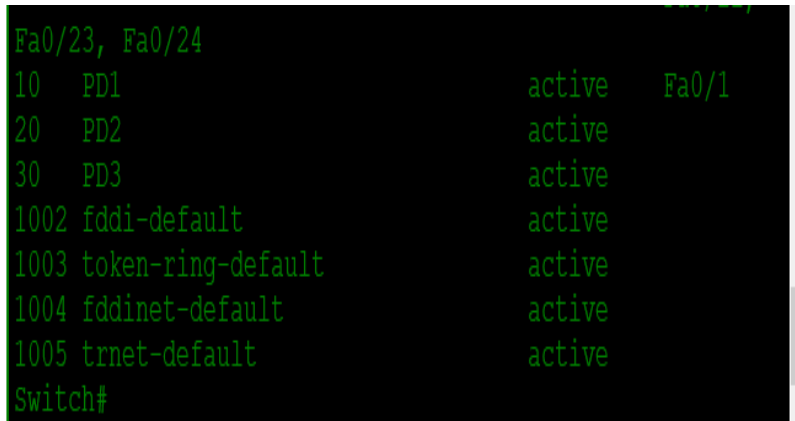
3.1 CONFIGURAÇÃO VLAN

Foram criadas VLANS para cada switch de um setor ocasionando assim a diminuição de protocolos broadcast percorrendo pela rede.

Habilitado o modo trunk em cada switch para permitir a comunicação entre VLANS, comandos utilizados:

- enable - modo privilegiado
- configure terminal - configurar o switch
- vlan 10 - configurar vlan 10
- name "" - nome da vlan 10 exemplo
- interface fastEthernet 0/3(exemplo)
- switchport mode trunk

show interfaces trunk - verificar as portas que estão em modo trunk



```
Fa0/23, Fa0/24
10 PD1 active Fa0/1
20 PD2 active
30 PD3 active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
Switch#
```

Figura 3 - Exemplo de VLAN configuradas

3.2 CONFIGURAÇÃO DHCP

Para configuração do servidor DHCP foi necessário a divisão em sub interfaces, cada sub interface foi encapsulada a uma VLAN específica, comandos utilizados para a divisão da interface e a criação do pool DHCP:

enable - modo privilegiado

configure terminal

interface fastEthernet 0/0.1(exemplo) - transforma em subrede

encapsulation dot1Q 10(vlan) - determina a vlan da subrede

ip address + ip + mascara - atribui o endereço ip para a subinterface

ip dhcp pool VLAN10 - entrar na pool da vlan

default-router 192.168.10.1(exemplo) - configurar o endereço da vlan

```

* - candidate default, U - per-user static route,
o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 8 subnets, 2
masks
C    192.168.1.0/26 is directly connected,
GigabitEthernet0/0.1
L    192.168.1.1/32 is directly connected,
GigabitEthernet0/0.1
C    192.168.1.64/26 is directly connected,
GigabitEthernet0/0.2
L    192.168.1.65/32 is directly connected,
GigabitEthernet0/0.2
C    192.168.1.128/26 is directly connected,
GigabitEthernet0/0.3
L    192.168.1.129/32 is directly connected,
GigabitEthernet0/0.3
C    192.168.1.192/26 is directly connected,
GigabitEthernet0/0.4
L    192.168.1.193/32 is directly connected,

```

Figura 4 - Configuração pool DHCP

3.3 PROTOCOLO RIP

É necessário habilitar o protocolo RIP versão 2 nos roteadores para a divulgação das redes e sub redes entre os edifícios, com isso cada rede privada pode se comunicar mesmo estando em outro local. Entre os roteadores foi configurado uma rede com apenas dois hosts, rede 192.168.5.1/30 mascara 255.255.255.252.

Comando utilizados:

configure terminal

router rip - habilita o protocolo rip

version 2 - utiliza mascaras de rede fora do "padrão"

no auto-summary - informa que existem duas sub-redes diferentes nas rotas

network 192.168.1.0 - informa para o roteador divulgar as redes conhecidas, no caso fazer isso para as redes que ele conhece

```

L      192.168.2.225/32 is directly connected,
GigabitEthernet0/1.8
      192.168.3.0/24 is variably subnetted, 4 subnets, 2
masks
C      192.168.3.0/25 is directly connected,
GigabitEthernet0/2.1
L      192.168.3.1/32 is directly connected,
GigabitEthernet0/2.1
C      192.168.3.128/25 is directly connected,
GigabitEthernet0/2.2
L      192.168.3.129/32 is directly connected,
GigabitEthernet0/2.2
      192.168.4.0/26 is subnetted, 4 subnets
R      192.168.4.0/26 [120/1] via 192.168.5.2, 00:00:25,
GigabitEthernet0/2/0
R      192.168.4.64/26 [120/1] via 192.168.5.2,
00:00:25, GigabitEthernet0/2/0
R      192.168.4.128/26 [120/1] via 192.168.5.2,
00:00:25, GigabitEthernet0/2/0
R      192.168.4.192/26 [120/1] via 192.168.5.2,
00:00:25, GigabitEthernet0/2/0
      192.168.5.0/24 is variably subnetted, 2 subnets, 2
masks

```

Figura 5 - Protocolo RIP

3.4 LISTA DE ACESSOS (UCL)

Para o isolamento do setor P&D dos demais foi configurado uma lista de acesso em que o roteador consiga bloquear a entrada de pacotes de outros setores.

Comando utilizado para configurar os acessos:

enable - entrar modo adm

configure terminal - configuração do terminal

ip access-list extended ACESSO-PD(nome) - criando a lista de acesso

deny tcp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 - negar acesso ao servidor

de todos os ips diferentes dos liberados

permit ip any any - permite todos os restantes de protocolos

interface fastEthernet 0/0.1 - entrar na interface da vlan 10

ip access-group ACESSO-PD in (quando entra ou out sai) - associando a lista a vlan10

```
Router>
Router>enable
Router#show ace
Router#show acc
Router#show access-lists
Extended IP access list ACESSO-PD
 10 deny ip 192.168.2.0 0.0.0.255 192.168.1.0
0.0.0.255
 20 deny ip 192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255
 30 deny ip 192.168.4.0 0.0.0.255 192.168.1.0
0.0.0.255
 40 permit ip any any (112 match(es))
Router#
```

Figura 6 - Lista de acesso

4 UTILIZAÇÃO DA NUVEM

Visando um projeto de reestruturação, a empresa pode utilizar alguns serviços de computação em nuvem, assim tendo uma maior flexibilidade para o seu crescimento, podendo utilizar ou aprimorar recursos de acordo com sua demanda.



Figura 7 - AWS

4.1 ZONAS DE DISPONIBILIDADE

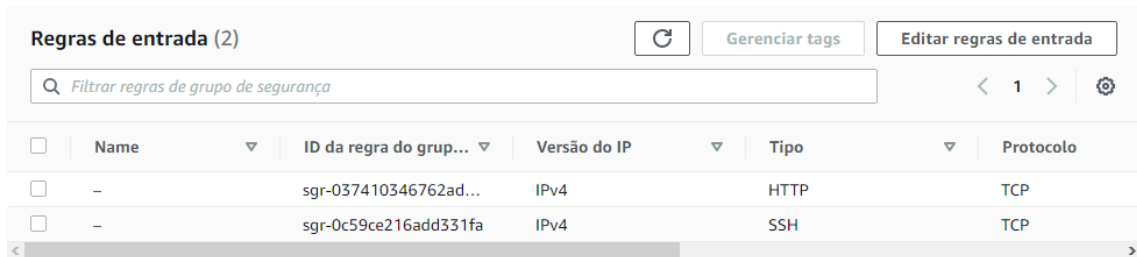
Neste caso optamos por utilizar o serviço da AWS, a proposta seria disponibilizar uma estrutura de redes, disposta em duas zonas de disponibilidade, serão duas subnets públicas e duas privadas, como demonstra a figura (8), utilizaremos a região leste dos EUA (Norte de Virgínia).

Sub-redes (4) Informações					Atualizar	Ações	Criar sub-rede
Filtrar sub-redes					< 1 > ⚙		
<input type="checkbox"/>	Name	ID da sub-rede	Estado	VPC			
<input type="checkbox"/>	nolimits2-subnet-public1-us-east-1a	subnet-030fc6bfd9e8d1fcf	✔ Available	vpc-0c348455241733dad nol...			
<input type="checkbox"/>	nolimits2-subnet-private1-us-east-1a	subnet-0e8c4f912d5b29bea	✔ Available	vpc-0c348455241733dad nol...			
<input type="checkbox"/>	nolimits2-subnet-public2-us-east-1b	subnet-0e3d5621ee749e282	✔ Available	vpc-0c348455241733dad nol...			
<input type="checkbox"/>	nolimits2-subnet-private2-us-east-1b	subnet-09815ed2e4cb91a92	✔ Available	vpc-0c348455241733dad nol...			

Figura 8 - Zonas de Disponibilidade

4.2 WEBSERVICE LINUX

Disponibilizado na subnet publica east-1b um servidor Linux, com apache respondendo externamente na porta 80 (Protocolo HTTP), e para conexão via SSH interno na porta 22, para isso foi configurado um grupo de segurança, onde permitia acesso apenas pelo IP privado.



The screenshot shows the AWS Management Console interface for a security group named 'service publico'. It displays two inbound rules:

<input type="checkbox"/>	Name	ID da regra do grup...	Versão do IP	Tipo	Protocolo
<input type="checkbox"/>	-	sgr-037410346762ad...	IPv4	HTTP	TCP
<input type="checkbox"/>	-	sgr-0c59ce216add331fa	IPv4	SSH	TCP

Figura 9 - Grupo de segurança service publico

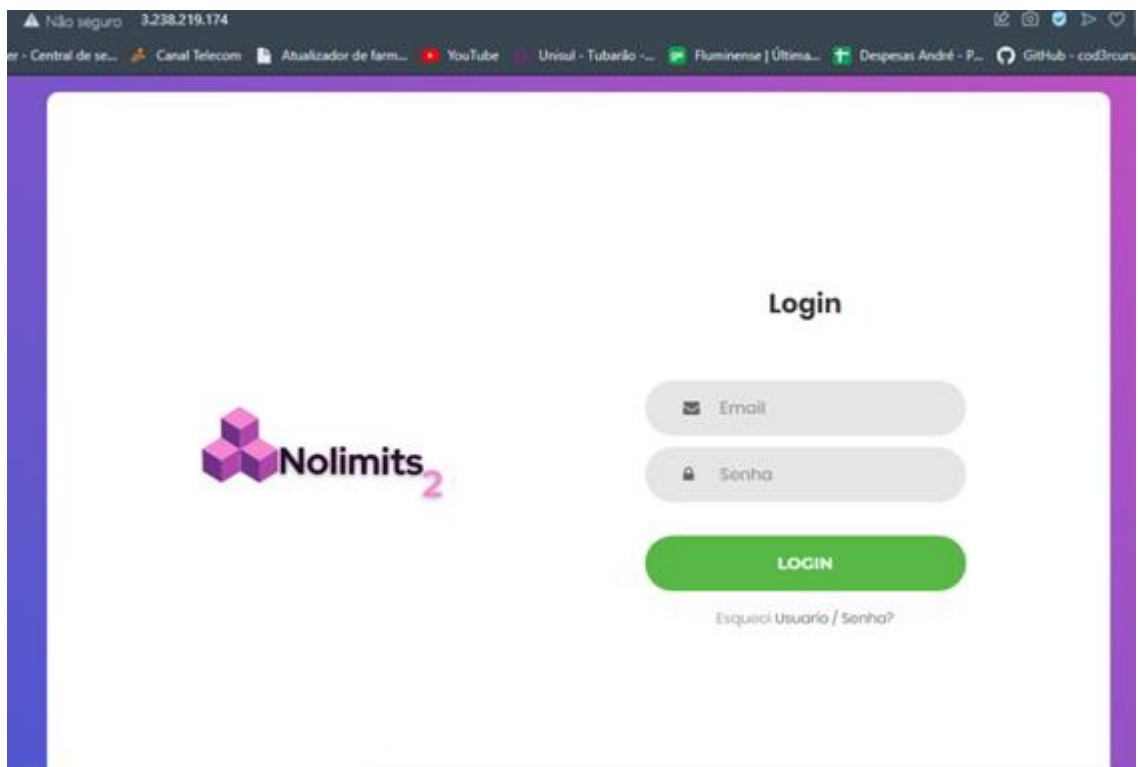
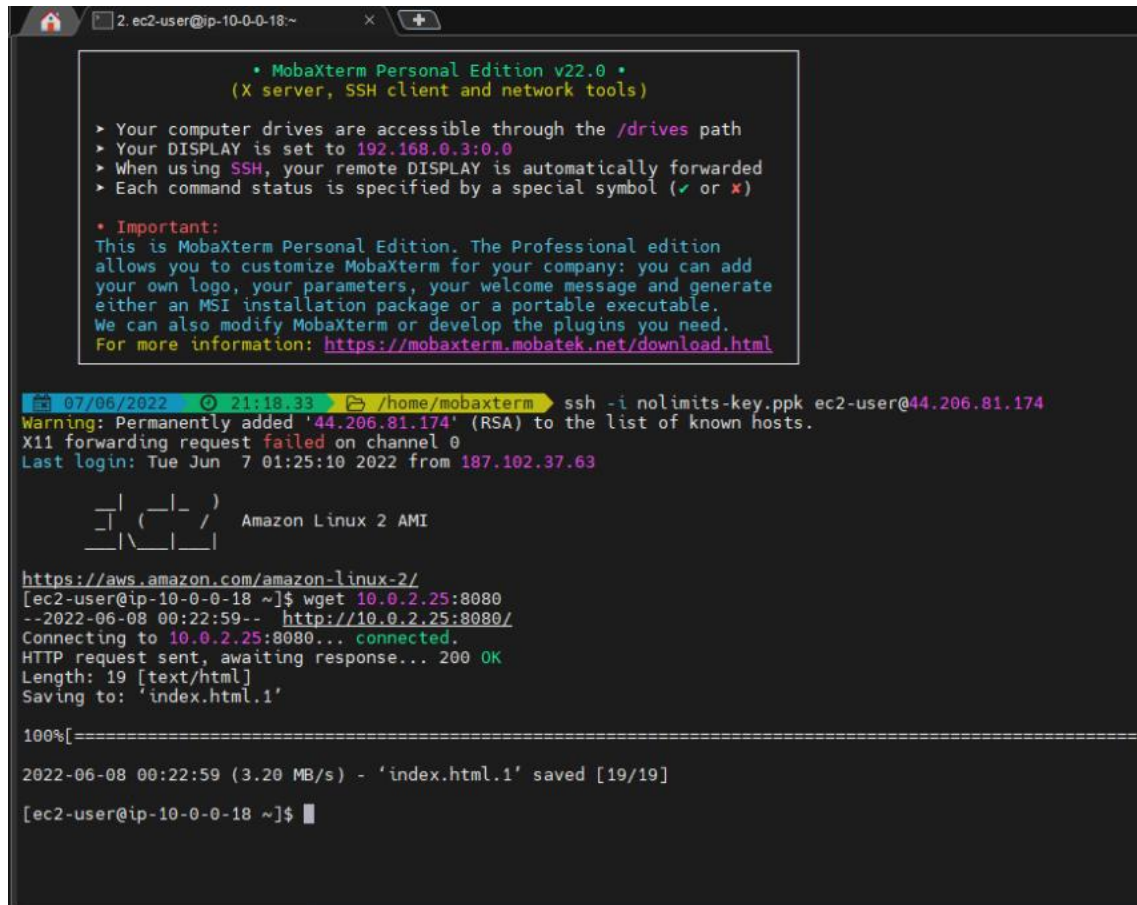


Figura 10 - Requisição porta 80 service publico

4.3 SERVICE LINUX PRIVADO

Instalado apache em uma subnet privada no qual se comunica pela porta 8080, e 22 para conexão SSH apenas interna, na figura 11 demonstra uma requisição na porta 8080 pelo bastion host.



```
2. ec2-user@ip-10-0-0-18:~  
• MobaXterm Personal Edition v22.0 •  
(X server, SSH client and network tools)  
» Your computer drives are accessible through the /drives path  
» Your DISPLAY is set to 192.168.0.3:0.0  
» When using SSH, your remote DISPLAY is automatically forwarded  
» Each command status is specified by a special symbol (✓ or ✗)  
  
• Important:  
This is MobaXterm Personal Edition. The Professional edition  
allows you to customize MobaXterm for your company: you can add  
your own logo, your parameters, your welcome message and generate  
either an MSI installation package or a portable executable.  
We can also modify MobaXterm or develop the plugins you need.  
For more information: https://mobaxterm.mobatek.net/download.html  
  
07/06/2022 21:18:33 /home/mobaxterm ssh -i nolimits-key.ppk ec2-user@44.206.81.174  
Warning: Permanently added '44.206.81.174' (RSA) to the list of known hosts.  
X11 forwarding request failed on channel 0  
Last login: Tue Jun 7 01:25:10 2022 from 187.102.37.63  
  
  _ | ( _ | - )  
  _ | \ _ | _ |  
Amazon Linux 2 AMI  
  
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-10-0-0-18 ~]$ wget 10.0.2.25:8080  
--2022-06-08 00:22:59-- http://10.0.2.25:8080/  
Connecting to 10.0.2.25:8080... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 19 [text/html]  
Saving to: 'index.html.1'  
  
100%[=====]  
  
2022-06-08 00:22:59 (3.20 MB/s) - 'index.html.1' saved [19/19]  
[ec2-user@ip-10-0-0-18 ~]$
```

Figura 11 - Requisição porta 8080 servidor interno

4.4 BASTION HOST

Disponibilizado um bastion host para a conexão via SSH de dispositivos externos, assim possibilitando acesso a rede privada dos demais servidores, figura 12 demonstra a conectividade do bastion host via SSH, com os servidores internos.

```

[ec2-user@ip-10-0-0-18 ~]$ ssh -i nolimits-key.pem ec2-user@10.0.0.72
Last login: Tue Jun  7 16:11:19 2022 from 187.102.37.63

  _|  _|  _|  _|  _|
 _| ( _|  /   Amazon Linux 2 AMI
 _| \ _|  _|  _|  _|

https://aws.amazon.com/amazon-linux-2/
13 package(s) needed for security, out of 21 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-0-72 ~]$ exit
logout
Connection to 10.0.0.72 closed.
[ec2-user@ip-10-0-0-18 ~]$ ssh -i nolimits-key.pem ec2-user@10.0.0.72
Last login: Wed Jun  8 00:28:16 2022 from ip-10-0-0-18.ec2.internal

  _|  _|  _|  _|  _|
 _| ( _|  /   Amazon Linux 2 AMI
 _| \ _|  _|  _|  _|

https://aws.amazon.com/amazon-linux-2/
13 package(s) needed for security, out of 21 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-0-72 ~]$ exit
logout
Connection to 10.0.0.72 closed.
[ec2-user@ip-10-0-0-18 ~]$ █

```

Figura 12 - Conexão bastion host via SSH

5 ORÇAMENTO DOS DISPOSITIVOS

14 switchs cisco SG350-28MP 28 portas

Valor R\$6.917,62 und

Total R\$96.846,68

<https://www.cnstore.com.br/switch-cisco-sg350-28mp-28-port-gigabit-poe#>

2 Roteadores cisco 2900 series 2911

Valor R\$ 1.200,00 und

Total 2.400,00

[https://www.mercadolivre.com.br/roteador-cisco-2900-series-2911-preto-e-aco-inoxidavel-](https://www.mercadolivre.com.br/roteador-cisco-2900-series-2911-preto-e-aco-inoxidavel-100v240v/p/MLB15910613?pdp_filters=category:MLB5867#searchVariation=MLB15910613&position=1&search_layout=grid&type=product&tracking_id=a5252257-9d71-42a1-8e11-5a84d366b0fb)

[100v240v/p/MLB15910613?pdp_filters=category:MLB5867#searchVariation=MLB15910613&position=1&search_layout=grid&type=product&tracking_id=a5252257-9d71-42a1-8e11-5a84d366b0fb](https://www.mercadolivre.com.br/roteador-cisco-2900-series-2911-preto-e-aco-inoxidavel-100v240v/p/MLB15910613?pdp_filters=category:MLB5867#searchVariation=MLB15910613&position=1&search_layout=grid&type=product&tracking_id=a5252257-9d71-42a1-8e11-5a84d366b0fb)