# Gestão e Segurança de Redes

LETI 2017/18

## Projeto 2


Grupo: 7 Membros do grupo:

Nº: 84611 Nome: Margarida Simões

Nº: 84613 Nome: Miguel Gonçalves

Nº: 84618 Nome: Pedro Maria


Respondam às seguintes questões sobre o projeto implementado pelo grupo:

| | |
|---|---|
| O projeto é baseado no projeto 1 do grupo ou na resolução de referência fornecida pelos docentes da cadeira? | Baseado no projecto 1 do grupo |
| Criou uma conta *admin* nos dois servidores da LAN de serviços? | Sim |
| Configurou o OpenSSH? | Sim |
| É possível fazer *ssh* e *scp* do PC da Internet para os servidores da LAN de serviços? | Sim |
| É possível fazer *ssh* e *scp* dos PCs dos engenheiros para os dois servidores da LAN de serviços? | Sim |
| Ao fazer *ssh* e *scp,* a autenticação é baseada em criptografia de chave pública? | Sim |
| Configurou as VPNs usando o pacote OpenVPN? Funcionam? | Sim e funcionam. |
| Configurou o *netfilter / iptables* no *router* do edifício central? | Sim |
| Esse *router* bloqueia a maior parte dos acessos da Internet à ICI? | Sim |
| Esse *router* bloqueia a maior parte dos acessos da DMZ às outras subredes da ICI? | Sim |
| Criou um novo nó para instalar o *snort* na rede da DMZ? | Sim |
| Instalou o *snort* na rede DMZ? | Sim |
| Instalou o *snort* na subrede *corporate?* | Sim |
| Indique o conteúdo do 1º pedido HTTP usado para testar o *snort.* | http://www.ici.pt/bin/ps |
| Qual das regras do ficheiro *web-attacks.rules* é activada por esse pedido? | 1ª (uricontent:"bin/ps") |
| Indique o conteúdo do 2º pedido HTTP usado para testar o *snort.* | http://www.ici.pt/bin/chmod |
| Qual das regras do ficheiro *web-attacks.rules* é activada por esse pedido? | 9ª (content:"bin/chmod") |

# SSH

Usou-se o software OpenSSH de modo a implementar as ligações SSH entre os clientes e servidores indicados no enunciado. Os clientes SSH consistem nos 2 PCs dos engenheiros (pcCorporate1 e pcCorporate2), situados na LAN Corporate, assim como o pcInternet situado na Internet.

Os servidores SSH consistem no servidor de DNS da ICI, dnsici, e também no servidor web da ICI, servidorWWW, ambos na LAN de serviços.

## Passos realizados na implementação do SSH:

Começou-se por activar o protocolo SSH em todas as máquinas pretendidas e, tendo todas as ligações sido activadas e testadas, seguidamente passou-se à geração das chaves públicas e privadas com recurso ao algoritmo de criptografia RSA.

Mais uma vez estabeleceu-se ligação entre todos os servidores SSH e todos os clientes SSH de modo a que estes últimos pudessem adicionar ao seu ficheiro *Known_Hosts* a fingerprint dos servidores. Por último foram metidas as chaves públicas de cada cliente SSH em cada servidor SSH, de modo a assegurar uma ligação SSH com segurança por encriptação de chave pública em vez de password.

# VPNs

Usando o software OpenVPN foram implementadas duas VPNs, onde o servidor é o router da LAN SCADA, e os clientes são os routers das subestações. Os endereços IP das VPNs pertencem à rede 200.200.200.0/25.

## Passos realizados na criação da VPN:

Primeiro criaram-se as chaves e certificado da CA, de seguida criaram-se as chaves e certificados para o servidor VPN (server) e os dois clientes VPN (client1 e client2, que correspondem ao router da Subestação1 e ao router da Subestação2 respectivamente).

As chaves e certificados correspondentes a cada cliente (*ca.crt*, *client1.crt*, *client1.key* para o client1 e *ca.crt*, *client2.crt*, *client.2key* para o client2) encontram-se na pasta root dos mesmos, bem como o ficheiro *client.conf*. O servidor VPN contém na pasta */etc/openvpn/* os ficheiros *ca.crt*, *dh1024.pem*, *server.key*, *server.crt* e *server.conf*.

## Routing na VPN:

Após a criação da VPN verificou-se que, para que os PCs das subestações pudessem comunicar com o PC da LAN SCADA e vice-versa, era necessária uma configuração adicional. No ficheiro *server.conf* foram feitas as modificações necessárias de modo a que a subrede da LAN SCADA (10.20.64.128/26) ficasse acessível aos clientes VPN e de modo a que os PCs das subestações pudessem comunicar com as máquinas da LAN SCADA através da VPN.

Além das alterações no ficheiro *server.conf* foi criada a pasta ccd na directoria onde se encontra esse mesmo ficheiro. Dentro da pasta estão dois ficheiros (client1 e client2) que informam o servidor VPN da rede para onde deve ser feito o encaminhamento, para cada um dos clientes VPN.

# Firewalls

De modo a se obter a filtragem de pacotes obtida utilizou-se o software de *netfilter / iptables* no router central e no router da LAN SCADA. Foram criadas ao todo 63 regras *iptables*, das quais 29 no router central e 34 no router da LAN SCADA, que em conjunto asseguram todos os requisitos do enunciado assim como o correcto funcionamento do SSH, das VPNs e do *snort*. Seguem-se por ordem as regras *iptables* do router central:

```
iptables -A FORWARD -s 10.20.64.100 -d ! 10.20.64.0/21 -p tcp --sport 80 --dport ! 1:1023 -j ACCEPT
iptables -A FORWARD -s ! 10.20.64.0/21 -d 10.20.64.100 -p tcp --sport ! 1:1023 --dport 80 -j ACCEPT
```
Permitem que do exterior da ICI se consiga comunicar por HTTP com o servidor www da ICI.

```
iptables -A FORWARD -s 10.20.64.80 -p udp --sport 53 --dport ! 1:1023 -j ACCEPT
iptables -A FORWARD -d 10.20.64.80 -p udp --sport ! 1:1023 --dport 53 -j ACCEPT
```
Permitem o livre acesso ao serviço de DNS do servidor de DNS da ICI por parte de qualquer máquina.

```
iptables -A FORWARD -s 10.20.64.0/21 -d 10.20.64.0/21 -p icmp --icmp-type 0 -j ACCEPT
iptables -A FORWARD -s 10.20.64.0/21 -d 10.20.64.0/21 -p icmp --icmp-type 8 -j ACCEPT
iptables -A INPUT -s 10.20.64.0/21 -p icmp --icmp-type 0 -j ACCEPT
iptables -A INPUT -s 10.20.64.0/21 -p icmp --icmp-type 8 -j ACCEPT
iptables -A OUTPUT -d 10.20.64.0/21 -p icmp --icmp-type 0 -j ACCEPT
iptables -A OUTPUT -d 10.20.64.0/21 -p icmp --icmp-type 8 -j ACCEPT
```
Permitem fazer ping de, para e através do router central e obter a resposta aos mesmos, dentro da ICI.

```
iptables -A FORWARD -s 10.20.64.2 -d ! 10.20.64.0/21 -p icmp --icmp-type 8 -j ACCEPT
iptables -A FORWARD -s 10.20.64.3 -d ! 10.20.64.0/21 -p icmp --icmp-type 8 -j ACCEPT
iptables -A FORWARD -s ! 10.20.64.0/21 -d 10.20.64.2 -p icmp --icmp-type 0 -j ACCEPT
iptables -A FORWARD -s ! 10.20.64.0/21 -d 10.20.64.3 -p icmp --icmp-type 0 -j ACCEPT
```
Permitem aos PCs da LAN Corporate fazer ping para o exterior da ICI e obter resposta aos mesmos.

```
iptables -A FORWARD -s 10.20.64.2 -d 10.20.64.100 -p tcp --dport 22 -j ACCEPT
iptables -A FORWARD -s 10.20.64.100 -d 10.20.64.2 -p tcp --sport 22 -j ACCEPT
iptables -A FORWARD -s 10.20.64.2 -d 10.20.64.80 -p tcp --dport 22 -j ACCEPT
iptables -A FORWARD -s 10.20.64.80 -d 10.20.64.2 -p tcp --sport 22 -j ACCEPT
iptables -A FORWARD -s 10.20.64.3 -d 10.20.64.100 -p tcp --dport 22 -j ACCEPT
iptables -A FORWARD -s 10.20.64.100 -d 10.20.64.3 -p tcp --sport 22 -j ACCEPT
iptables -A FORWARD -s 10.20.64.3 -d 10.20.64.80 -p tcp --dport 22 -j ACCEPT
iptables -A FORWARD -s 10.20.64.80 -d 10.20.64.3 -p tcp --sport 22 -j ACCEPT
iptables -A FORWARD -s 30.40.0.100 -d 10.20.64.100 -p tcp --dport 22 -j ACCEPT
iptables -A FORWARD -s 10.20.64.100 -d 30.40.0.100 -p tcp --sport 22 -j ACCEPT
iptables -A FORWARD -s 30.40.0.100 -d 10.20.64.80 -p tcp --dport 22 -j ACCEPT
iptables -A FORWARD -s 10.20.64.80 -d 30.40.0.100 -p tcp --sport 22 -j ACCEPT
```
Permitem o funcionamento do SSH conforme descrito acima, estando limitado unicamente às 5 máquinas indicadas.

```
iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP
```
Estabelecem a default policy da firewall, neste caso todo o pacote que não cumpra as regras acima é descartado.

Seguem-se por ordem as regras *iptables* do router da LAN SCADA:

```
iptables -A FORWARD -s 10.20.64.128/26 -d 10.20.65.128/26 -j ACCEPT
```

iptables -A FORWARD -s 10.20.64.128/26 -d 10.20.65.192/26 -j ACCEPT
iptables -A FORWARD -s 10.20.64.128/26 -d 10.20.65.2 -j ACCEPT
iptables -A FORWARD -s 10.20.64.128/26 -d 10.20.65.66 -j ACCEPT
iptables -A OUTPUT -d 10.20.65.128/26 -j ACCEPT
iptables -A OUTPUT -d 10.20.65.192/26 -j ACCEPT
iptables -A OUTPUT -d 10.20.65.2 -j ACCEPT
iptables -A OUTPUT -d 10.20.65.66 -j ACCEPT
Permitem a livre comunicação da LAN SCADA para qualquer endereço IP das 2 subestações.

iptables -A FORWARD -s 10.20.65.128/26 -d 10.20.64.128/26 -j ACCEPT
iptables -A FORWARD -s 10.20.65.192/26 -d 10.20.64.128/26 -j ACCEPT
iptables -A FORWARD -s 10.20.65.2 -d 10.20.64.128/26 -j ACCEPT
iptables -A FORWARD -s 10.20.65.66 -d 10.20.64.128/26 -j ACCEPT
iptables -A INPUT -s 10.20.65.128/26 -j ACCEPT
iptables -A INPUT -s 10.20.65.192/26 -j ACCEPT
iptables -A INPUT -s 10.20.65.2 -j ACCEPT
iptables -A INPUT -s 10.20.65.66 -j ACCEPT
Permitem a livre comunicação das 2 subestações para qualquer endereço IP da LAN SCADA.

iptables -A FORWARD -s 10.20.64.128/26 -d 200.200.200.0/25 -j ACCEPT
iptables -A FORWARD -s 200.200.200.0/25 -d 10.20.64.128/26 -j ACCEPT
iptables -A INPUT -s 10.20.64.128/26 -j ACCEPT
iptables -A OUTPUT -d 10.20.64.128/26 -j ACCEPT
iptables -A FORWARD -s 200.200.200.0/25 -d 200.200.200.0/25 -j ACCEPT
iptables -A INPUT -s 200.200.200.0/25 -j ACCEPT
iptables -A OUTPUT -d 200.200.200.0/25 -j ACCEPT
Permitem o funcionamento das VPNs conforme descrito acima, estando limitado unicamente às 3 máquinas indicadas.

iptables -A FORWARD -s 10.20.64.80 -d 10.20.64.128/26 -p udp --sport 53 --dport ! 1:1023 -j ACCEPT
iptables -A FORWARD -s 10.20.64.128/26 -d 10.20.64.80 -p udp --sport ! 1:1023 --dport 53 -j ACCEPT
Permitem o acesso ao serviço de DNS do servidor de DNS da ICI por parte da LAN SCADA.

iptables -A FORWARD -s 10.20.64.0/21 -d 10.20.64.0/21 -p icmp --icmp-type 0 -j ACCEPT
iptables -A FORWARD -s 10.20.64.0/21 -d 10.20.64.0/21 -p icmp --icmp-type 8 -j ACCEPT
iptables -A INPUT -s 10.20.64.0/21 -p icmp --icmp-type 0 -j ACCEPT
iptables -A INPUT -s 10.20.64.0/21 -p icmp --icmp-type 8 -j ACCEPT
iptables -A OUTPUT -d 10.20.64.0/21 -p icmp --icmp-type 0 -j ACCEPT
iptables -A OUTPUT -d 10.20.64.0/21 -p icmp --icmp-type 8 -j ACCEPT
Permitem fazer ping de, para e através do router da LAN SCADA e obter a resposta aos mesmos, dentro da ICI.

iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP
Estabelecem a default policy da firewall, neste caso todo o pacote que não cumpra as regras acima é descartado.

Em resumo, as máquinas de fora da ICI apenas podem utilizar os serviços de DNS e WWW da ICI. Todas as máquinas da ICI podem fazer ping entre elas, e apenas os PCs da LAN Corporate podem fazer ping para o exterior. As máquinas da DMZ têm comunicação muito limitada com o resto da ICI, para além de pings dentro da ICI apenas podem servir de servidores SSH para os PCs da LAN Corporate. As máquinas da LAN SCADA comunicam livremente com as subestações e vice-versa, sem que as subestações tenham comunicação livre entre elas e sem que mais nenhuma máquina tenha comunicação livre com as subestações. Todas as máquinas da ICI excepto as das subestações têm livre acesso ao serviço de DNS da ICI. Por último, todo o tráfego que não cumpra estas condições é descartado.

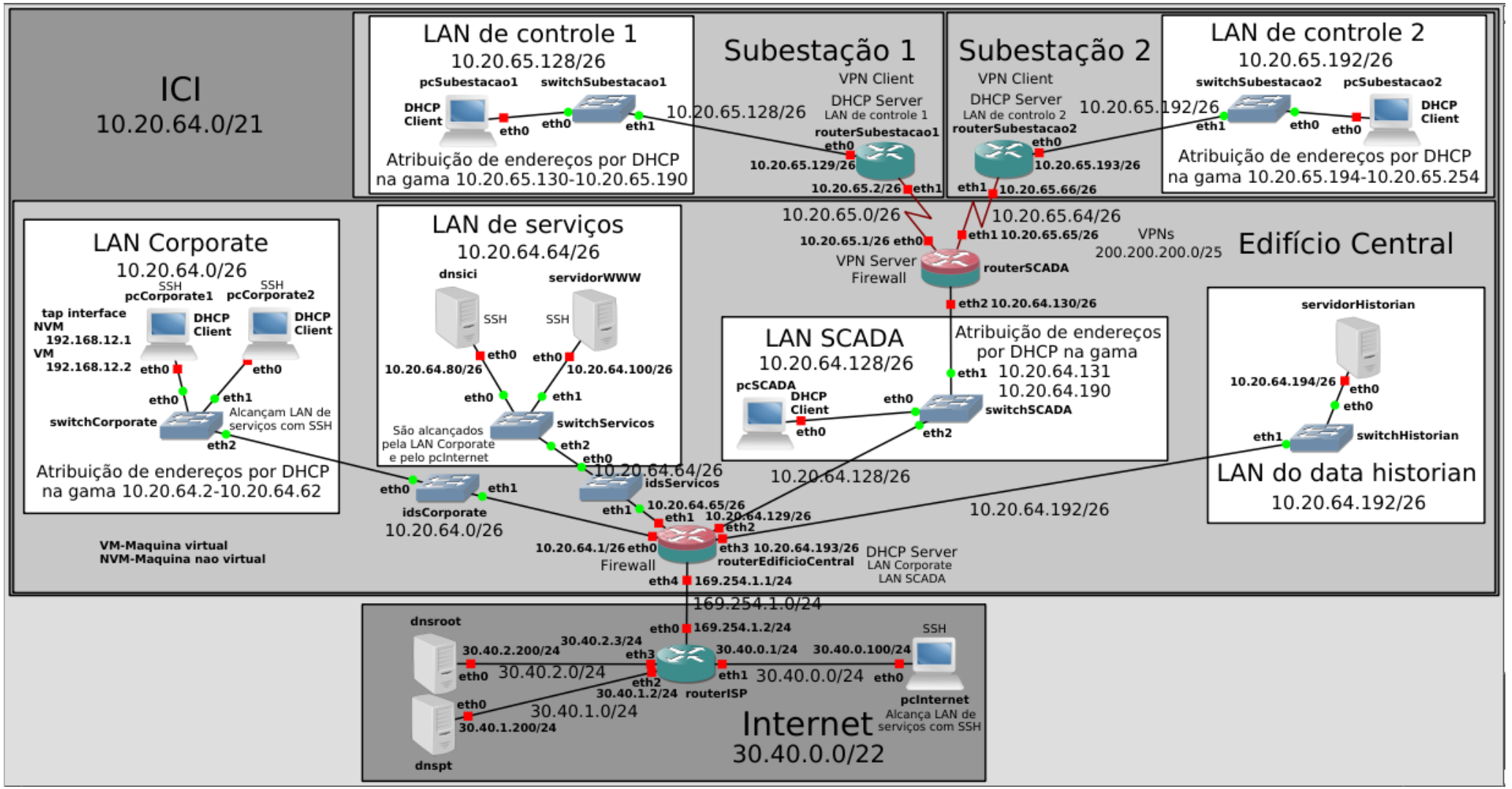
## Snort

Foram instalados 2 IDSs na ICI configurados para detectarem ataques e intrusões na rede, ou seja, 2 PCs configurados como switches a correr o *snort*. Um foi colocado entre o switch da LAN Corporate e o router central, enquanto o outro foi colocado entre o switch da LAN de serviços e o router central. Nos 2 IDSs o *snort* foi colocado a correr em modo *daemon*. De modo a se configurar o *snort*, na directoria de cada IDS no projecto foi criada uma pasta */etc/snort* e nela foi colocado um ficheiro de configuração base *snort.conf*. Apenas foi necessário alterar a variável HOME_NET para ter o endereço da sub-rede do IDS, e a variável EXTERNAL_NET para ser o inverso da variável HOME_NET.

Com o *snort* devidamente configurado, foram enviados do pcInternet para o servidorWWW da ICI dois pedidos HTTP, http://www.ici.pt/bin/ps e http://www.ici.pt/bin/chmod, que respectivamente violaram a 1ª e 9ª regras do ficheiro *web-attacks.rules* e causaram assim a geração de um alarme.

A 1ª regra consiste no seguinte: “alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:”WEB-ATTACKS /bin/ps command attempt”; flow:to_server,estabilished; uricontent:”/bin/ps”; nocase; classtype:web-application-attack; sid:1328; ver:6;)”

A 9ª regra consiste no seguinte:”alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:”WEB-ATTACKS chmod command attempt”; flow:to_server,estabilished; content:”/bin/chmod”; nocase; classtype:web-application-attack; sid:1336; rev:5;)”


ICI
10.20.64.0/21
LAN de controle 1
10.20.65.128/26
pcSubestacao1
switchSubestacao1
DHCP Client
eth0
eth0
eth1
Atribuição de endereços por DHCP na gama 10.20.65.130-10.20.65.190
Subestação 1
VPN Client
DHCP Server
LAN de controle 1
routerSubestacao1
eth0
10.20.65.129/26
10.20.65.2/26
eth1
10.20.65.128/26
Subestação 2
VPN Client
DHCP Server
LAN de controlo 2
routerSubestacao2
eth0
10.20.65.193/26
eth1
10.20.65.66/26
10.20.65.192/26
LAN de controle 2
10.20.65.192/26
switchSubestacao2
pcSubestacao2
eth1
eth0
eth0
DHCP Client
Atribuição de endereços por DHCP na gama 10.20.65.194-10.20.65.254
10.20.65.0/26
10.20.65.1/26 eth0
eth1 10.20.65.65/26
10.20.65.64/26
VPNs
200.200.200.0/25
Edifício Central
VPN Server
Firewall
routerSCADA
eth2 10.20.64.130/26
LAN Corporate
10.20.64.0/26
SSH
pcCorporate1
SSH
pcCorporate2
tap interface
NVM
192.168.12.1
VM
192.168.12.2
DHCP Client
DHCP Client
eth0
eth0
eth0
eth1
switchCorporate
Alcançam LAN de serviços com SSH
eth2
Atribuição de endereços por DHCP na gama 10.20.64.2-10.20.64.62
LAN de serviços
10.20.64.64/26
dnsici
servidorWWW
SSH
SSH
eth0
eth0
10.20.64.80/26
10.20.64.100/26
eth0
eth1
switchServicos
São alcançados pela LAN Corporate e pelo pcInternet
eth2
eth0
10.20.64.64/26
idsServicos
LAN SCADA
10.20.64.128/26
pcSCADA
DHCP Client
eth0
eth0
switchSCADA
eth2
eth1
Atribuição de endereços por DHCP na gama 10.20.64.131 10.20.64.190
10.20.64.128/26
servidorHistorian
10.20.64.194/26
eth0
eth0
eth1
switchHistorian
LAN do data historian
10.20.64.192/26
10.20.64.192/26
eth0
eth1
idsCorporate
10.20.64.0/26
eth1
10.20.64.65/26
eth1
10.20.64.129/26
eth2
10.20.64.1/26 eth0
Firewall
eth3 10.20.64.193/26
routerEdificioCentral
DHCP Server
LAN Corporate
LAN SCADA
eth4
169.254.1.1/24
169.254.1.0/24
VM-Maquina virtual
NVM-Maquina nao virtual
dnsroot
eth0
169.254.1.2/24
30.40.2.200/24
30.40.2.3/24
eth3
30.40.0.1/24
30.40.0.100/24
SSH
eth0
30.40.2.0/24
eth2
30.40.1.2/24
routerISP
eth1
30.40.0.0/24
eth0
pcInternet
Alcança LAN de serviços com SSH
eth0
30.40.1.200/24
30.40.1.0/24
dnspt
Internet
30.40.0.0/22