

## SEGURANÇA / SECURITY

TP1

Configure a Network Security Scenario

### Descrição

O primeiro trabalho prático pretende promover a aplicação dos conhecimentos adquiridos nas aulas de modo a criar uma rede funcional e ativar todos os mecanismos de segurança discutidos até ao momento.

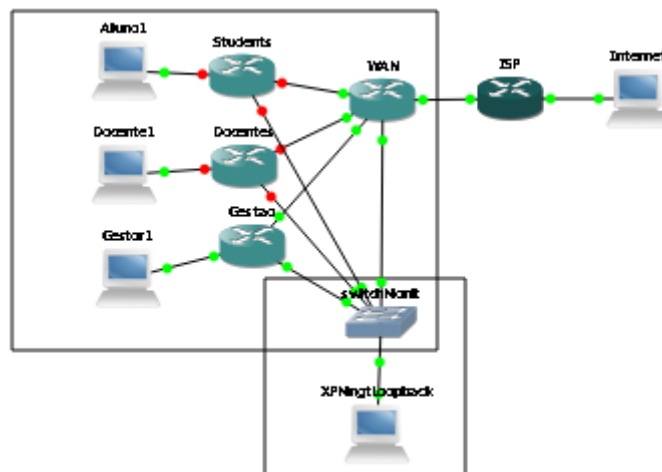
É objetivo que os alunos entreguem um ambiente GNS3 funcional ao docente, contendo todos os equipamentos configurados de modo a responder ao solicitado na descrição do *cenário de rede*.

### Equipas

Para executar o trabalho prático pretende-se que sejam criados grupos constituídos por um máximo de 4 elementos, sendo o mínimo aceitável de 2 elementos. É desejável que os alunos de Erasmus sejam parte integrante com outros alunos nacionais, promovendo a partilha cultural. No caso de ocorrerem alterações de grupos, no decorrer dos trabalhos, deverão informar de imediato, indicando o motivo para a alteração.

### Cenário de rede

O cenário de rede que se pretende é o que se apresenta na figura seguinte:



As configurações que devem obrigatoriamente ter são:

- ISP
  - Router 7200, slot 0 with C7200-IO-2FE
  - F0/1: 172.16.0.1/24
- WAN
  - Router 7200, slot 0 with C7200-IO-FE, slot 1 with PA-4E
  - E1/3: 192.168.200.10/24
- Student
  - Router 2600, slot 0 with CISCO2600-MB-2FE, slot 1 with NM-4E
  - E1/3: 192.168.200.11
- Docentes
  - Router 2600, slot 0 with CISCO2600-MB-2FE, slot 1 with NM-4E
  - E1/3: 192.168.200.12
- Gestão
  - Router 7200, slot 0 with C7200-IO-FE, slot 1 with PA-4E
  - E1/3: 192.168.200.13
- Internet
  - VPCS 1
  - 172.16.0.2/24
- Aluno1
  - VPCS 2
  - 192.168.10.2/24
- Docente1

- VPCS 3
- 192.168.11.2/24
- Gestor1
  - VPCS XP Soft Loopback
  - 192.168.12.2/24
- XPMngtLoopback
  - VPCS XP Mngt Loopback
  - 192.168.200.1/24

## Segurança do equipamento

---

As implementações de segurança em todos os equipamentos, excepto o ISP (cujos usernames criados não devem poder aceder) devem cumprir com:

- **Segurança do equipamento**
  - Fecho de serviços e servidores não necessários
  - Configuração de username/passwords locais
    - enable/myenable
    - operator/myop
    - manager/myman
  - Configuração dos banners contendo
    - Quando faz telnet: nomes dos elementos do grupo e aviso de acesso
    - Quando insere password com sucesso: Nome do equipamento, âmbito a que se destina o equipamento e relação Interface/IPs utilizados
  - Medidas anti acesso
    - Bloqueio por 10 minutos se falhar 3 vezes no prazo de 1 minuto
    - Registo de acessos com sucesso e falhados
  - Configuração do SSH permitindo apenas acesso via SSH aos equipamentos
- **Configuração de privilégios**
  - Operador
    - Apenas pode visualizar, tanto quanto possível, as informações dos interfaces
    - Apenas pode alterar, tanto quanto possível, nos interfaces de acesso local
    - Nestes, apenas pode mexer no endereço IP e descritivo, tanto quanto possível
    - No router WAN e uplinks dos restantes routers deve poder alterar e visualizar o descritivo, apenas
  - Gestor pode realizar todas as operações em todos os interfaces, exceptando fazer shutdown nos interfaces de uplink
  - Deverão, obrigatoriamente, utilizar privilege ou role-based cli (view e superview) nos equipamentos que permitam. Note-se que no 2600 apenas suporta o privilege pelo que devem usar este método, enquanto que o 7200 deve-se usar o role-based cli
  - Os operador e manager devem entrar automaticamente no seu nível de privilégio correto
- **Configurações AAA e Logging**
  - Deve-se configurar todos os routers para fazer logging no servidor de log 192.168.200.1
  - Deve-se permitir acesso AAA, com accounting, no servidor RADIUS 192.168.200.1, auth port 1812 e acct port 1813

## Avaliação

---

A avaliação do trabalho prático contemplará os seguintes components:

- Configuração da rede (10%)
- Segurança do equipamento (30%)
- Configuração de privilégios (Privilege e Role-based CLI) (30%)
- AAA e Logging (30%)

## Datas de entrega e entregáveis

---

A data de entrega é a que consta no moodle.

No que respeita a entrega do trabalho prático é esperado que cada grupo criem e configurem um ambiente virtual GNS3 que permita responder ao cenário descrito anteriormente. A entrega deve ser realizada no dia de entrega, ao professor, num ficheiro zipado contendo os seguintes componentes:

- Ficheiros GNS3
- Ficheiros VPCS

Considerando que foi dada a máquina virtual original e igual à do docente, considera-se que estão reunidas todas as condições para que o trabalho entregue pelos alunos funcione sem erros. É da responsabilidade do aluno garantir que o ambiente está corretamente funcional e que executa no estado original do .ova entregue.



**Instituto Superior de Engenharia de Coimbra**  
**Departamento de Engenharia Informática e de Sistema**

---

Todo o ambiente deve ser dado ao professor numa PEN que será usada para transferir a informação para o computador do docente. Para evitar atrasos, pede-se o favor de terem tudo pronto na PEN no momento da avaliação.

### **Esclarecimentos**

---

Esclarecimentos sobre o trabalho prático devem ser endereçados via moodle, mail ou durante as aulas práticas dedicadas a esclarecimento de dúvidas..