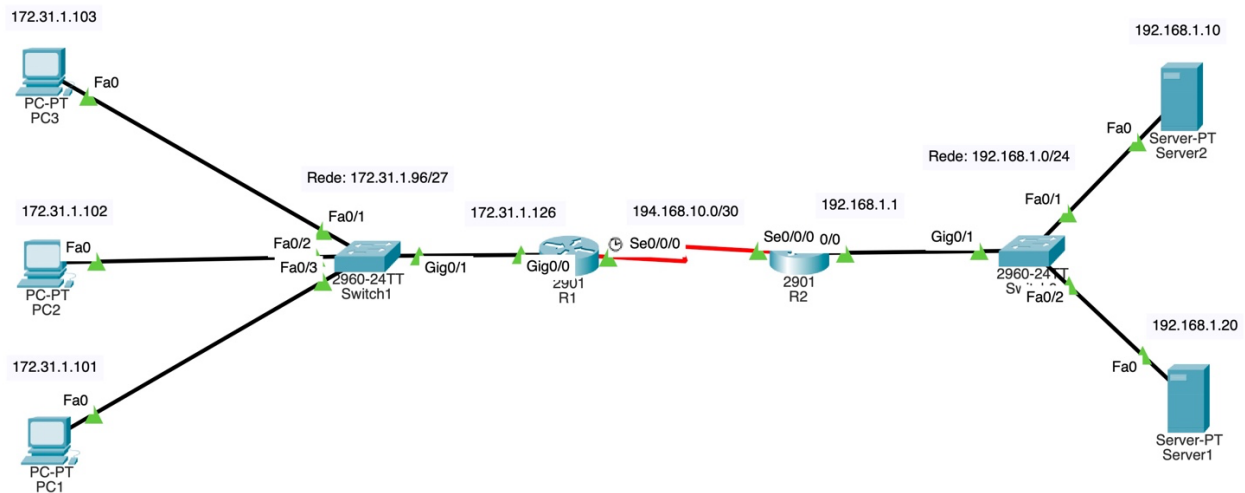


Redes de Dados II

Trabalho Prático Nº8 – ACLs

Considere o seguinte cenário de rede:



PARTE I

1.1 - Implemente o cenário e configure os equipamentos, seguindo os seguintes passos (para cada um dos passos registre os comandos necessários):

- a. Entre em modo de execução privilegiada.
- b. Entre em modo de configuração.
- c. Altere o nome dos equipamentos.
- d. Ative as passwords de consola dos *routers* e *switches*. Utilize a password 'cisco'.

Redes de Dados II

- e. Ative também a password de *enable*. Utilize 'class'.
- f. Desabilite a pesquisa DNS.
- g. Configure a senha cisco para as conexões vty.
- h. Desligue todas as portas que não estão a ser utilizadas no *Switch0*.
- i. Configure as interfaces dos equipamentos com os IPs adequados.
- j. Configure a Clock rate 56000 em ambos os *routers*.
- k. Configure a segurança de porta no *Switch0* da camada de acesso. Configure as portas Fa0/1 e Fa0/2 para que elas permitam apenas um host único e aprendam o endereço MAC do host dinamicamente. Caso seja identificado um evento de segurança a porta deve ser deligada.
- l. Verifique que a segurança das portas está a funcionar corretamente.
- m. Configure R1 e R2 para utilizar o protocolo RIPv2.
- n. Verifique as configurações e teste a conectividade entre todos os PCs e Servidores.

Redes de Dados II

- o. Configure e teste ACLs de modo a que o PC3 não consiga comunicar com os Servidores. Aplique a lista construída à interface mais adequada.

- p. Configure e teste ACLs de modo a que o PC1 não consiga efectuar TELNET para a interface série do R1, mas permita que o PC1 o faça para a interface Gig0/0 de R1. Aplique a ACL no local mais adequado.

- q. Configure e teste ACLs de modo a que a sub-rede dos Servidores não recebam *pings* de outras sub-redes mas sim da própria sub-rede.

- r. Configure e teste ACLs de modo a que apenas seja possível a saída de tráfego proveniente dos Servidores 1 e 2 da sub-rede onde eles se encontram.

- s. Configure e teste ACLs de modo a bloquear o acesso HTTP e HTTPS do PC1 ao Servidor 2.

- t. Configure e teste ACLs de modo a permitir tráfego UDP do PC2 ao Servidor 2 mas não do PC1.

- u. Configure e teste ACLs de modo a permitir o acesso FTP ao Servidor 1 do PC1 mas não do PC2.

- v. Configure e teste ACLs de modo a bloquear tráfego TCP do PC1 ao Servidor 1.

- w. Continua a conseguir utilizar o FTP do Servidor 1 a partir do PC1? Porque?

Redes de Dados II

- x. Configure e teste ACLs de modo a negar todo o tráfego de entrada e saída da sub-rede dos servidor relativo ao TELNET e permita o tráfego relativo ao SSH, efetuando o log.