

SEGURANÇA

Trabalho Prático

Configuração avançada de um equipamento

Introdução

Neste trabalho prático, o objetivo principal é conseguir estimular a aplicação prática dos conhecimentos adquiridos no âmbito das aulas de segurança, assim como promover a pesquisa de soluções técnicas que promovam as melhores práticas de segurança em redes.

A implementação do cenário, análise dos componentes que o compõem e a avaliação das questões de segurança que possam estar envolvidas na implementação das melhores regras e soluções serão tidas em consideração para a nota final.

Equipas

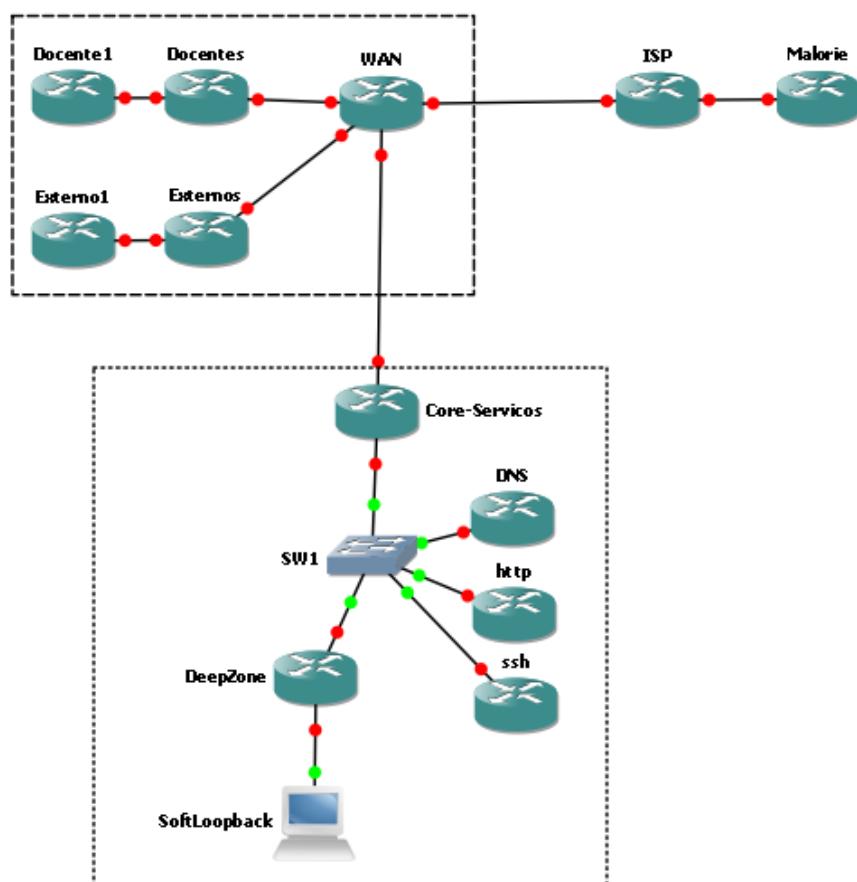
Para executar o trabalho prático pretende-se que sejam criados grupos constituídos por um máximo de 4 elementos, sendo o mínimo aceitável de 2 elementos. É desejável que os alunos de Erasmus sejam parte integrante com outros alunos nacionais, promovendo a partilha cultural. No caso de ocorrerem alterações de grupos, no decorrer dos trabalhos, deverão informar de imediato, indicando o motivo para a alteração. Os elementos que não tenham grupo definido ou que não constem na lista de grupos disponível no moodle não serão objeto de avaliação, não tendo classificação no trabalho prático.

Assim, reforça-se que é imperativo que todos os elementos que pretendam ser alvo de avaliação neste trabalho devem pertencer a um grupo, validar se o seu nome consta na lista de grupos criado no moodle.

O momento de avaliação de cada grupo vai ser definido pelo docente, sendo a lista publicada em endereço a ser disponibilizado posteriormente.

Cenário do trabalho prático

O cenário de trabalho é o que se apresenta a seguir.



Este cenário possui 3 ambientes distintos: a Internet (ISP e Malorie), Rede Interna (WAN, Docentes e Externos) e DMZ (Core-Servicos e restantes equipamentos).

Redes a serem usadas:

- Malorie: 193.137.2.2
- ISP: 193.137.1.1
- WAN: 193.137.1.2
- Docentes: 193.136.1.2
- Externos: 193.136.2.2
- Docente1: 192.168.100.2
- Externos1: 192.168.101.2
- Core-Servicos: 193.136.5.2
- DNS: 193.136.6.2
- HTTP: 193.136.6.3
- SSH: 193.136.6.4
- DeepZone: 193.136.6.5
- SoftLoopback: 192.168.200.2

Tipo de equipamentos:

- Deve ser usado o router Cisco modelo 7200 em todos os equipamentos excetuando o Externos
- O Externos deve ter um router Cisco modelo 2600

Definições que devem ser cumpridas:

- Configuração Radius:
 - IP 192.168.200.2
 - Secret: myradiuspwd
- Configuração Syslog:
 - IP 192.168.200.2
- Configurações de acessos em todos os routers:
 - enable: myenapwd
 - oper: operpwd
 - adm: admpwd
 - manager: manpwd
- Configurações em todos os equipamentos finais:
 - Enable: myenapwd
 - oper: operpwd

Configurações básicas de segurança que devem ser realizadas:

- Fecho de serviços desnecessários
- Criação de banners
 - No acesso inicial: indicação de grupo, nomes elementos e avisos de segurança básicos
 - Após autenticação: informação sobre o router, informação da rede, informação sobre destino do router a que acedemos, informação sobre interfaces existentes e sua função
- Aplicação de medidas que limitem tentativas de acesso indevidas (bloqueio por 10 mins se falhar 3 tentativas de acesso no prazo de 1 minuto; bloqueio de acesso ao serviço de ssh por redes não autorizadas, outras medidas que considerem importantes)
- Registo de eventos e acessos (com sucesso ou falhados) ao sistema no servidor de logging central definido
- Configuração do servidor de ssh e limitação a apenas este protocolo para os equipamentos que o permitam

Privilégios de administração:

- Operador (username: oper):
 - Apenas pode visualizar todas as informações sobre os interfaces finais dos routers (excluir acessos *upper-link*)
 - Apenas pode alterar o descriptivo dos interfaces a que tem direito a aceder
- Administrador (username adm):
 - Deve poder ver todos os interfaces
 - Pode fazer todas as ações nos interfaces exceptuando o *shutdown*
- Gestor (username: manager):
 - Terá privilégios totais sobre o equipamento
- Todos os utilizadores deverão entrar no sistema com a permissão adequada, sem necessidade de partilha da password de *enable*

AAA e Logging:

- Todos os equipamentos devem poder fazer autenticação via AAA centralizado no servidor indicado, com accounting
- Deverão realizar logging no servidor de syslog central definido para o efeito

Firewall:

- Não deve ser permitido spoofing a partir da Internet
- Não se deve permitir o spoofing ou RFC1918 para a Internet
- Não deve ser possível fazer telnet ou ssh para qualquer router interno, exceto se indicado explicitamente em contrário
- Rede Docentes e Externos:
 - Não deve ser permitido qualquer ligação do exterior para estas redes
 - Os equipamentos internos deverão poder realizar ligações tcp, udp e icmp sem restrição
- Core-Servicos
 - Deve permitir acesso aos diversos serviços internos (DNS, HTTP, ...)
 - Se se realizar um telnet ao Core-Servicos, e se autenticar com sucesso como utilizador *myaccess* (pwd: *mypwd*), a partir do Malorie, então deve-se permitir realizar pings para o servidor DNS a partir do Malorie
- DeepZone:
 - Deve ser configurado de modo a permitir acesso aos serviços que possui (Radius e Syslog)
 - Deve ser possível realizar telnet ou ssh, conforme o caso, aos diversos equipamentos da rede interna a partir desta zona
 - Deve ser possível pingar todos os equipamentos internos
- Deve haver um bloqueio que não permita os utilizadores docentes e externos de acederem à Internet ao fim-de-semana
- Nota adicional:
 - é obrigatório a utilização, no decorrer deste trabalho, de todos os tipos de firewall ensinados nas aulas (**standard, extended, dynamic, reflexive, time-based**, CBAC e Zone-based Policy Firewall)
 - a aplicação de cada uma das possíveis soluções de firewall a cada equipamento e situação será alvo de avaliação, sendo que deve ser tida em consideração a melhor adequação da solução existente a cada caso
 - Deve-se utilizar o NAT para garantir o acesso ao exterior das redes docentes e externos

Prazos e Entregáveis

O prazo de entrega encontra-se definido na página do moodle.

Os entregáveis do trabalho são:

- Um relatório onde seja explicado de forma sucinta, mas completa, os seguintes pontos
 - Configuração das firewalls
 - Configuração de logging
 - Configuração da autenticação
 - Configuração do NAT
- Todos os ficheiros do ambiente GNS3

Os ficheiros devem ser entregues num ficheiro comprimido (.zip, .rar, ...).

O relatório produzido deve permitir que uma pessoa externa à cadeira, com conhecimentos básicos de GNS3 e CISCO; assim como sendo possuidor da imagem de WindowsXP disponibilizada aos alunos, possa executar todo o trabalho apresentado.

Esclarecimentos

Esclarecimentos relativos ao trabalho prático podem ser discutidos durante as aulas destinadas para o efeito, via email para o docente (vapi@isec.pt) ou via moodle.