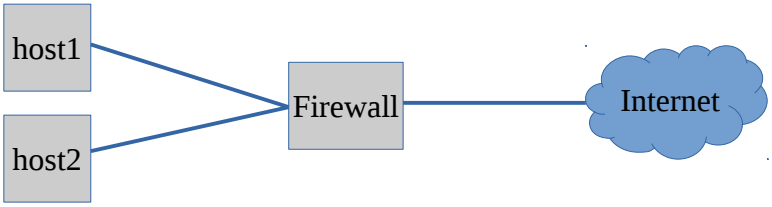
APS – Segurança

Valor 2,0 (média final)
Equipe: dupla
Data de entrega e apresentação 05/12/2016

Criar e configurar o seguinte cenário de rede:

- Dois hosts em uma rede local (LAN) ligados a um firewall que dá acesso à Internet (tal como figura a seguir):



Tal cenário deverá ser replicado no laboratório E105 da UTFPR e por isso deverá ter os seguintes IPs e configurações de rede:

- O firewall terá um IP do laboratório E105, por exemplo 172.16.2.**160** na interface eth0, e outro IP em na interface eth0:1 10.255.**160**.1/24 (os nomes das interfaces podem ser diferentes nos hosts do laboratório).
- O host 1 terá o IP 10.255.**160**.2/24 e o seu gateway padrão e servidor DNS é o firewall.
- O host 2 terá o IP 10.255.**160**.3/24 e o seu gateway padrão e servidor DNS é o firewall.
  Obs. note que o terceiro octeto do IP da rede local leva o número do último octeto do IP da UTFPR – isso é obrigatório. Nesse exemplo foi utilizado o IP 172.16.2.160 no IP da UTFPR, mas a equipe deve utilizar o IP que estiver no host que eles estiverem utilizando no laboratório e não o 172.16.2.160.

Quando as configurações do firewall as equipes podem escolher um dos seguintes cenários de configuração:

1. **Cenário A**
   a) Deverá ser configurado no firewall um NIDS que monitore todo o tráfego de rede;
   b) Deverá ser utilizada a política de permitir tudo em todas as situações do firewall;
   c) O firewall não deve permitir que os hosts da LAN utilizem outro DNS que não o próprio firewall.
   d) O firewall não deve permitir que os hosts que cruzam o firewall utilizem o serviço de telnet;
   e) O firewall não deve permitir que os hosts da LAN acessem o host 172.217.29.35;
   f) O firewall não deve permitir que os hosts da LAN utilizem serviços de SMTP e POP3;
   g) O firewall deve utilizar uma configuração de LAN screened na tabela *filter* para os hosts da LAN;
   h) Somente o host 1 pode acessar o firewall via SSH e isso deve ser feito através de controle de MAC;
   i) Ninguém pode acessar o firewall via Telnet e FTP;
   j) O firewall deve mascarar os IPs da LAN para a Internet.

2. **Cenário B**
   a) Deverá ser configurado no firewall uma VPN utilizando OpenVPN entre o host 1 e outro host dentro da rede da UTFPR (exemplo do IP 172.16.2.X e não do IP 10.255.X.2).
   b) O firewall deverá trabalhar com a política de negar tudo em todas as situações;
   c) O firewall deve permitir a comunicação via VPN;

d) Os hosts da LAN devem acessar o firewall via SSH;
e) Os hosts da LAN devem acessar os serviços de HTTP, HTTPS, FTP e DNS na Internet;
f) Os hosts da LAN devem poder pingar o Firewall e hosts da Internet, mas não podem ser "pingados" - contudo qualquer ping não deve exceder o número de 10 pacotes;
g) Os pacotes da LAN destinados ao servidor DNS do firewall devem ser redirecionados para o IP 8.8.8.8;
h) O firewall deve mascarar os IPs da LAN para a Internet.
i) Os firewall deve acessar os serviços de HTTP, HTTPS, FTP e DNS na Internet;
j) Os pacotes administrativos (SSH) devem ter mais prioridade no firewall/LAN do que os pacotes demais pacotes.

3. **Cenário C**
   a) Deverá ser configurado um Proxy no firewall;
   b) Deve ser utilizado a política de liberar tudo para os pacotes roteados pelo firewall e de negar tudo aos pacotes destinados/originados para o firewall;
   c) O firewall não deve permitir que os usuários da LAN acessem a Internet sem utilizar o proxy.
   d) Não deve ser permitido o uso de SSH e Telnet entre as redes que cruzam o firewall;
   e) Deve ser dado o direito de acesso ao firewall via SSH apenas pela rede local;
   f) O firewall deve poder acessar como cliente os serviços de SSH, HTTP, HTTPS e DNS;
   g) O firewall deve mascarar os IPs da LAN para a Internet.

4. **Cenário D**
   a) Deverá ser configurado um Proxy e um HIDS no firewall;
   b) O firewall deve permitir que os hosts da Internet acessem o host 1 e host 2 via HTTP;
   c) Os hosts da LAN devem utilizar o proxy para acessar sites HTTP e essa configuração deve ser transparente (proxy transparente).
   d) Somente o firewall pode acessar os hosts da LAN via SSH.
   e) Somente um host da rede da UTFPR (exemplo do IP 172.16.2.X e não do IP 10.255.X.2) poderá acessar o firewall via SSH.

Cada cenário só poderá ser implementado por duas equipes, ou seja, um mesmo cenário não pode ser implementado por três equipes ou mais. Portanto assim, que a equipe escolher um cenário essa deve enviar um e-mail para o professor (luizsantos@utfpr.edu.br), informando qual cenário escolheu. As duas primeiras equipes a enviar o e-mail ganham o direito sobre a implementação do cenário. A lista com os cenários e as equipes ficará disponível no Moodle da disciplina.

Além de implementar o cenário no laboratório e apresentar para o professor no dia 05/12/2016 cada equipe deve entregar um texto impresso contendo:

1. Introdução;
2. Apresentação do ambiente de rede;
3. Apresentação da tecnologia utilizada;
4. Configuração de rede (incluindo comandos e opções) para cada host e serviço utilizado para montar o cenário de rede proposto. Descrever configuração, apresentar arquivos de configuração utilizados e comandos com opções e parâmetros;
5. Configuração de NIDS/HIDS/VPN/PROXY conforme cada cenário. Descrever configuração, apresentar arquivos de configuração utilizados e comandos com opções e parâmetros;
6. Configuração do firewall. Descrever configuração, apresentar arquivos de configuração utilizados e comandos com opções e parâmetros;
7. Conclusão. Descreva também dificuldades e/ou facilidades encontradas durante o desenvolvimento do cenário proposto.

Observação: Em caso de plágio o trabalho receberá nota ZERO.