CONCURSO PÚBLICO – SDS/PE

CARGO 11: PERITO CRIMINAL
ÁREA 7: CIÊNCIA DA COMPUTAÇÃO, ENGENHARIA DA COMPUTAÇÃO OU SISTEMAS DE INFORMAÇÃO

PROVA DISCURSIVA – ESTUDO DE CASO
Aplicação: 19/6/2016

PADRÃO DE RESPOSTA

Espera-se que, para resolver o caso, o candidato contemple em seu texto, em linhas gerais, as informações a seguir.

O *firewall* da rede de computadores da organização deveria estar configurado de maneira restritiva para permitir que o acesso externo à rede fosse realizado somente por meio das portas respectivas para os serviços SMTP (*mail*) e SMTPS (*mail* seguro). Os clientes de correio eletrônico deveriam utilizar o protocolo POP3S ou IMAPS para receber suas mensagens, garantindo-se, assim, que as mensagens, ao serem trafegadas na rede, estivessem protegidas por criptografia. O *firewall* deveria ficar restrito a esses clientes e às portas para POP3S e IMAPS.

Já que o ambiente possui servidor Windows 2012 R2, deveria existir um serviço de Active Directory (AD) nesse ambiente, o que permitiria que tanto os usuários quanto os computadores da rede pudessem ser autenticados no serviço AD. Para a atualização de segurança, o serviço Windows Update deveria estar configurado nas estações Windows 7 e nos servidores de rede. Como função mais avançada, poderia ser utilizado o serviço WSUS para atualizações de redes corporativas.

O OpenLDAP, que é um serviço de autenticação de usuários, pode ser removido da rede se for instalado o serviço de AD no Windows 2012 R2, porque se torna redundante na rede, gerando dois serviços com a mesma finalidade. Assim, por questões de integração de soluções de rede, já que o AD é integrado nativamente ao Windows 2012 R2 e o Windows 7 é compatível com esse serviço, o OpenLDAP pode ser removido, sem prejuízo para a autenticação dos usuários.

Como o *switch* é gerenciável, poderiam ser criados três segmentos de rede, conforme a necessidade de uma DMZ. Nesse caso, o *firewall* deveria ter três interfaces de rede para serem ligadas a três VLANs distintas, que devem ser criadas, sendo cada interface do *firewall* ligada em uma VLAN diferente para roteamento entre as VLANs. A título de exemplo, poderia ser criada uma VLAN externa (Internet), uma VLAN interna (rede local com computadores clientes e serviços de autenticação) e uma VLAN para serviços de Internet (DMZ/*email*, no caso em questão).