E-fólio B | Folha de resolução para E-fólio

UNIDADE CURRICULAR: Segurança em redes e computadores

CÓDIGO: 21181

DOCENTE: Henrique São Mamede

A preencher pelo estudante

NOME: Vitor Manuel Metrogos Frango

N.º DE ESTUDANTE: 1802925

CURSO: Licenciatura em Engenharia Informática

DATA DE ENTREGA: 20 de dez. de 2022

TRABALHO / RESOLUÇÃO:

Q1 De forma a garantir uma distribuição segura de dados, neste caso especifico código-fonte, a minha sugestão passará pela implementação de uma VPN baseada no protocolo IPSec (Internet Protocol Security) em virtude do mesmo conjugar protocolos de rede seguros que autentica e criptografa pacotes de dados. Por outras palavras o IPSec tem a capacidade de proteger transmissão de dados através de LAN (Local Area Network) , WAN (Wide Area Network) privadas e publicas bem como pela Interne e que pode funcionar em **modo transporte** em que criptografa o trafego entre dois hosts sendo essa criptografia apenas para o pacote de dados e o **modo túne**l em que são criados tuneis virtuais entre as duas sub redes de forma a serem criptografados os dados bem como o cabeçalho IP (Internet Protocol)

Na figura abaixo (20.1) temos o exemplo de implementação de IPSec

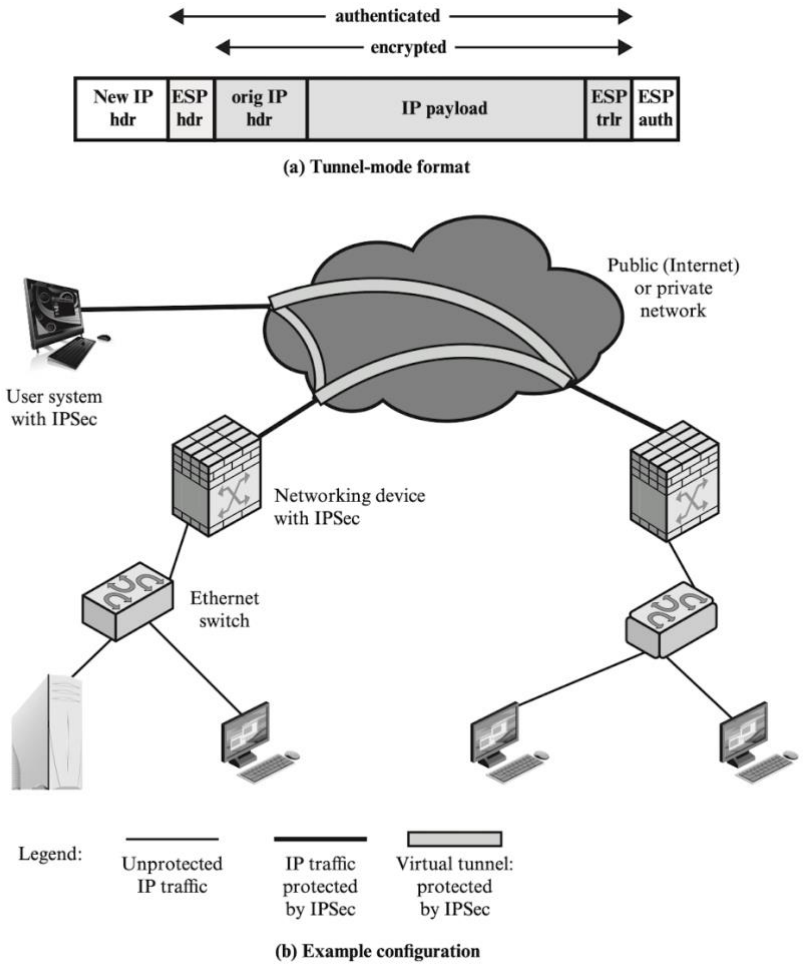
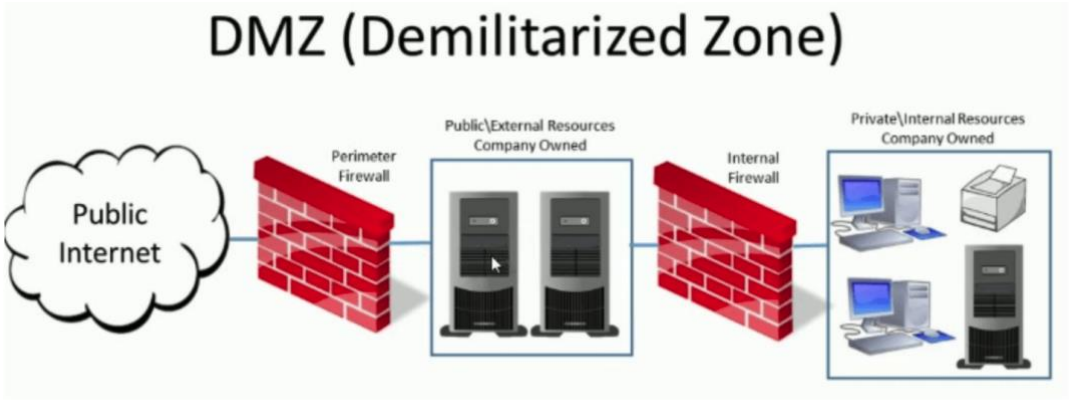


Figure 20.1 An IPSec VPN Scenario

Q2 Tendo em conta as características hibridas da infraestrutura em estudo, haverá a necessidade de se criar um perímetro de segurança que proteja a rede da infraestrutura central da rede externa onde se situam os trabalhadores, desta forma a sugestão passa pela implementação de uma rede DMZ (Demiliterized Zone) também ela conhecida por rede de perímetro ou sub-rede rastreada.

O objetivo da DMZ é criar uma camada extra de segurança à rede interna da empresa de forma a reduzir o risco de violação de dados, para isso implementa se uma arquitetura de firewall dupla ficando entre elas, a rede DMZ.



A primeira firewall ou firewall de perímetro é configurada para permitir trafego externo controlando o acesso entre a internet e a DMZ, a segunda firewall ou interna, apenas permite o trafego dentro da DMZ e a mesma controla todo o trafego interno ou entre recursos internos.

Visto a DMZ “dividir” a rede os seus controlos de segurança podem ser configurados especificamente para cada segmento, por exemplo um sistema de deteção de prevenção de intrusões. No entanto uma má configuração devido a sua complexa implementação poderá comprometer os recursos hospedados a ficarem expostos para o exterior.

Esta implementação DMZ deverá complementada com a configuração de uma VPN com protocolo IPSec, desta forma poderemos reforçar a redução de risco de intrusão.

Q3 Várias medidas podem ser implementadas, entre elas podemos destacar:

- **Autenticação forte** através de senhas seguras (utilização de mais de 10 caracteres alfanuméricos e símbolos) com periodicidade de renovação, tokens de acesso (renovação de código a cada 60seg), autenticação multi-fator e leitor biométrico
- **Atualização de software** manter os sistemas bem como os aplicativos atualizados com as mais recentes correções de segurança permite que a rede esteja protegida contra vulnerabilidades conhecidas
- **Controlo de acesso** implementação de medidas de controlo de acesso de forma a garantir que apenas utilizadores autorizados tenham acesso aos recursos da rede (inclui se acesso de pessoas as instalações da empresa)
- **Monitorização / auditorias** é importante a monitorização permanente da rede de forma a detetar atividades suspeitas ou ataques em potencial.

Q4 Para os computadores portáteis da empresa , e não só os home based, seria instalado um serviço SecaaS (Security as a Service) visto o mesmo possuir um vasto leque de serviços que se adequam as necessidades deste caso, como por exemplo e entre outras, monitorização continua, segurança de Email (onde se inclui anti SPAM e anti malware), gestão de anti vírus, proteção contra intrusão, avaliação de segurança e informações de segurança e gestão de eventos.

Alteração das permissões de acesso, deixando para tal de ser possível um trabalhador instalar software ou aceder as configurações do seu PC, isso evitará a instalação de software malware

Utilização de ferramentas de gestão de dispositivos moveis (MDM) ira colmatar os constrangimentos de quem possa estar longe da sede da empresa e necessite instalar/configurar um software.

Por fim e “fora” da componente técnica de forma a identificarem e agir perante as inúmeras ameaças de malware, pishing ou outras técnicas de engenharia social terá obrigatoriamente de haver uma aposta na formação e treino dos trabalhadores nos temas da segurança informática.

REFERÊNCIAS BIBLIOGRÁFICAS:

Stallings, William (2007) Cryptography and Network Security: Principles and Practice. 7th Edition (Global Edition), Prentice Hall.

https://www.okta.com

https://bobcares.com