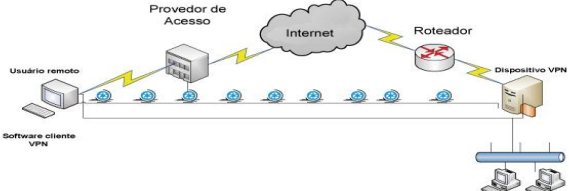
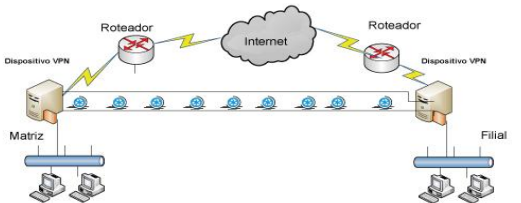
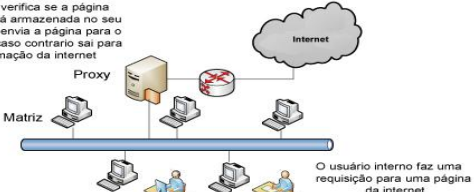


AGENTES DE SEGURANÇA	AGENTES DE SEGURANÇA
O que são os <b>Agentes de Segurança</b> ?	<b>Agentes de Segurança:</b> são os elementos de um sistema de segurança da informação que são reponsáveis por combater as ameaças aos sistemas de informação. Dentre eles vamos ter softwares, ferramentas e métodos de serviço que nos ajudam a manter a segurança do nosso sistema informático.
Quais são <b>alguns Agentes de Segurança</b> ?	Eles são:  <div><div>- <b>Antivírus;</b></div><div>- <b>Anti-Malware;</b></div><div>- <b>Firewall;</b></div><div>- <b>IDS</b></div><div>- <b>IPS;</b></div><div>- <b>Honeypot;</b></div><div>- <b>AntiSPAM;</b></div><div>- <b>VPN;</b></div><div>- <b>VLAN;</b></div><div>- <b>PROXY;</b></div><div>- <b>DMZ;</b></div></div>
Como funciona o Agente de Segurança <b>Anti-Vírus</b> ?	<b>Anti-Vírus:</b> São programas de computador instalados no computador que <b>detectam e eliminam rotinas virais que entram nos computadores por através de mensagens, dowloads e etc.</b> Os anti-vírus ficam constantemente ativos no computador, assim que este é iniciado, e fazem varreduras periódicas no sistema em busca de aplicativos virais, além de atuarem instantaneamente sobre qualquer dispositivo ou arquivo que adentre no sistema. Alguns exemplos de Anti-Vírus são: Norton, Panda, McAfee, BitDefender, BullGuard, Avast.
Como funciona o Agente de Segurança <b>Anti-Malware</b> ?	<b>Anti-Malware:</b> Assim como os Anti-Vírus, são programas de computador instalados para <b>detectar e eliminam todo tipo de malware que entrar nos computadores por através de mensagens, dowloads e etc.</b> Os Anti-Malware vão além dos Anti-Vírus, enquanto os Anti-Vírus são especialistas em rotinas virais, os Anti-Malware lidam com todo e qualquer tipo de malware. Alguns exemplos de Anti-Malware são: Malwarebytes, Exeddb, McAfee Rootkit Detective, IObit Security 360, Ad-Aware Free, Ashampoo, Avira Free, ComboFix.
Como os Anti-Vírus e Anti-Malware <b>conseguem detectar os malwares que adentraram um sistema</b> ?	Por meio da <b>comparação entre o arquivo que chegou e uma biblioteca de informações que contém informações sobre como as rotinas dos malwares se comportam e quais são as suas Assinaturas</b> - Assinaturas são: uma sequência de caracteres que representam o vírus e que podem ser encontradas pelo processo de escaneamento do sistema. Achando uma rotina suspeita o Anti-Vírus ou Anti-Malware pode bloquear o arquivo, colocá-lo em quarentena, apagá-lo e etc.
Como funciona o Agente de Segurança <b>Firewall</b> ?	<b>Firewall:</b> Do inglês " <b>Muralha de Fogo</b> ", faz referência as parede anti-chamas de um edifício, feitas de um material especial para não propagar as chamas. Da mesma forma, os Firewall são um " <b>ponto de proteção em local de grande risco em uma rede Ethernet</b> ", geralmente os firewalls fazem frente ao Switch que é a porta de entrada entre a rede local e a internet. Os Firewalls aplicam políticas de segurança predeterminadas pelo usuário, ou por um especialista em segurança, <b>para proteger a rede de ataques maliciosos.</b> Os Firewalls podem ser tanto Hardwares quanto softwares, eles <b>atuam sobre as portas de rede, protegendo diretamente a rede ou um computador específico.</b>
Como funciona o Agente de Segurança <b>IDS</b> ?	<b>IDS:</b> Do inglês " <b>Intrusion Detection System</b> " ( <b>Sistema de Detecção de Intruso</b> ), é um aplicativo que pode ser instalado nos computadores da rede. A função o IDS é <b>funcionar como um Sniffer, escutando a rede a todo tempo na procura por atividades que possam ser maliciosas ou procedentes de uma invasão, ao encontrar uma atividade maliciosa ele ALERTA os computadores da rede que algo está acontecendo em tal lugar.</b> Ele <b>NÃO IRÁ BARRAR UMA INVASÃO</b> , mas ele vai alertar á todos que alguma coisa suspeita está acontecendo. Por isso podemos dizer que o IDS funciona no <b>modo PASSIVO</b> , escutando a rede e só toma providências se vê algo suspeito.
Como funciona o Agente de Segurança <b>IPS</b> ?	<b>IPS:</b> Do inglês " <b>Intrusion Prevention System</b> " ( <b>Sistema de Prevenção de Intruso</b> ), é a evolução do sistema IDS, enquanto o IDS ficaria escutando a rede passivamente esperando que algo suspeito acontecesse para soar um alerta, o IPS não, ele <b>funciona INLINE analisando diretamente o tráfego de rede, e ao detectar um comportamento inseguro na rede ele INTERROMPE AS COMUNICAÇÕES CONSIDERADAS INSEGURAS instantaneamente</b> , ou seja, ele funciona totalmente no modo ATIVO. Um detalhe importante é que o <b>IPS trabalha em conjunto com o Firewall</b> , ele que alerta o Firewall que as comunicações "naquela determinada porta" devem ser interrompidas.
Como funciona o Agente de Segurança <b>Honeypot</b> ?	<b>Honeypot:</b> Do inglês " <b>Pote de Mel</b> ", o Honeypot não é uma aplicação, nem hardware, na verdade é um <b>método de verificação das ferramentas de segurança, para ver se elas estão funcionando ou não.</b> O Honeypot é como chamamos um computador vulnerável, deixamos um computador vulnerável a ataques de propósito - claro que sem nenhum dado ou informações importantes nele. Esse computador geralmente é usado em conjunto com o IDS para disparar alertas de possíveis invasões. Isso vai nos mostrar onde estão as brechas do nosso sistema e vai dar aos Crackers a falsa impressão de que é fácil invadir o nosso sistema.
Como funciona o Agente de Segurança <b>Anti-SPAM</b> ?	<b>Anti-SPAM:</b> É uma ferramenta usada geralmente nos servidores de e-mail para minimizar os SPAMs enviados pelas redes. Elas fazem isso por bloquear remetentes de SPAMs e identificar comportamentos suspeitos nos e-mails. O foco dessa ferramenta de rede é <b>minimizar a quantidade de mensagens indesejadas e o congestionamento de tráfego por causa da grande quantidade de SPAMs.</b>

AGENTES DE SEGURANÇA	AGENTES DE SEGURANÇA
<p>Como funciona o Agente de Segurança <b>VPN</b>?</p>	<p><b>VPN:</b> ou Virtual Private Network (Rede Privada Virtual), é um protocolo que permite a uma organização a criação de uma Extranet - Uma espécie de ethernet que pode ser acessada remotamente sem a necessidade do computador estar diretamente conectado a um access point ou switch. Isso é possível graças aos métodos de tunelamento do protocolo VPN, que cria um acesso criptografado a todos os computadores conectados a VPN, esse acesso pode ser feito pelo método "voluntário" ou "compulsório". Diferente da Ethernet que não precisaria de Internet para manter a conexão entre os hosts, na VPN a internet é essencial, sem ela o tunelamento não funciona.</p>
<p>Como se dá os <b>tunelamentos Voluntário e Compulsório</b> do protocolo VPN? E que <b>segurança</b> eles oferecem?</p>	<p><b>Tunelamento Voluntário:</b> O tunelamento voluntário é feito por através de software instalado no computador do usuário remoto, que gera comunicação direta com o servidor VPN da empresa; <b>Tunelamento Compulsório:</b> Nesse esquema de tunelamento, <b>NÃO É NECESSÁRIO SOFTWARE</b> para ligar o servidor VPN principal a uma máquina cliente que se tornará uma espécie de servidor VPN secundário;</p> <p>Esses métodos de tunelamento permitem que somente os computadores conectados a VPN criptograficamente possam adentrar o sistema, tornando a transferência de dados via internet muito mais segura.</p>
<p><b>Ilustre como acontece o tunelamento VPN voluntário</b> (Perceba que esse é o caso do usuário comum que acessa a rede remota da empresa, sem o auxílio de um servidor VPN na sua casa que faça o acesso ao servidor VPN da empresa)</p>	
<p><b>Ilustre como acontece o tunelamento VPN Compulsório</b> (Perceba que esse é o caso de usuários de uma matriz que acessam a rede remota do servidor VPN principal que se encontra na filial da empresa, é uma comunicação Servidor VPN á Servidor VPN)</p>	
<p>Como funciona o Agente de Segurança <b>VLAN</b>?</p>	<p><b>VLAN:</b> ou Virtual LAN, é uma rede virtual criada dentro de um switch para segregar um determinado número de portas do switch a trocarem informações somente dentro a rede interna delegada para isso. Esse é um aumento na segurança da rede, impedindo que mesmo funcionários internos tenham acesso a informações que não são para o seu setor de aplicação e adicionando uma camada á mais de dificuldade para um invasor que adentre a rede principal.</p> <p><b>OBS: somente switches L3 são capazes de fazer isso!</b></p>
<p>Como funciona o Agente de Segurança <b>PROXY</b>?</p>	<p><b>PROXY:</b> ou "Procurador", é uma espécie de servidor utilizado somente para fazer buscas no lugar do cliente ou trazer respostas no lugar do servidor. Ele evita o acesso direto de uma aplicação ao cliente ou ao servidor, protegendo os dispositivos tanto cliente quanto servidor de ataques diretos, em vez disso, o PROXY fica com toda a carga de ataque. Além disso, eles trabalham com o esquema de cache, armazenando as buscas e requisições mais procuradas, diminuindo o congestionamento na internet.</p>
<p><b>Ilustre como se dá o uso de PROXYS</b></p>	<p>O servidor proxy verifica se a página requisitada não está armazenada no seu cache. Se estiver, envia a página para o cliente solicitante, caso contrario sai para buscar a informação da internet</p> 
<p>Como funciona o Agente de Segurança <b>DMZ</b>?</p>	<p><b>DMZ:</b> ou Demilitarized Zone (Zona Desmilitarizada), assim como existe as Zonas Desmilitarizadas entre a fronteira dos países onde temos um terreno "neutro" para a troca de informações, podemos criar uma DMZ entre a nossa Ethernet ou Intranet e a Internet Global, nessa zona podemos colocar 1 ou 2 firewalls fazendo a defesa á nossa rede, tendo entre eles servidores como o VPN, onde conseguimos acessar informações remotamente. Somente os dispositivos que têm a chave criptográfica para passar pelo firewall conseguem acessar a rede interna e externa da empresa.</p>
<p><b>Ilustre como se dá o uso de DMZ</b></p>	