Unidade VI

6 VPN, VLANS, WLANS E IPSEC

Um administrador de rede deve utilizar as tecnologias existentes sempre com a segurança da informação em mente. Isso talvez lhe permita descobrir que ferramentas desenvolvidas para facilitar o tráfego da informação também podem favorecer a segurança da informação, desde que configuradas de maneira adequada.

6.1 VPN

Moraes (2010) afirma que podemos definir uma VPN de diferentes formas:

- Uma rede de circuitos virtuais que transporta tráfego privado.
- Uma conexão segura baseada em criptografia, que tem por objetivo transportar informação sensível através de uma rede insegura (internet). As VPNs combinam tecnologias de criptografia, autenticação e tunelamento, o que é interessante para interligar pontos distantes de uma organização através da internet.
- Uma rede na qual a conectividade entre múltiplos usuários e/ou sites é estabelecida sobre uma infraestrutura compartilhada, mas com as mesmas políticas de acesso e segurança de uma rede privada.

A figura a seguir apresenta a visão simplificada de uma VPN.

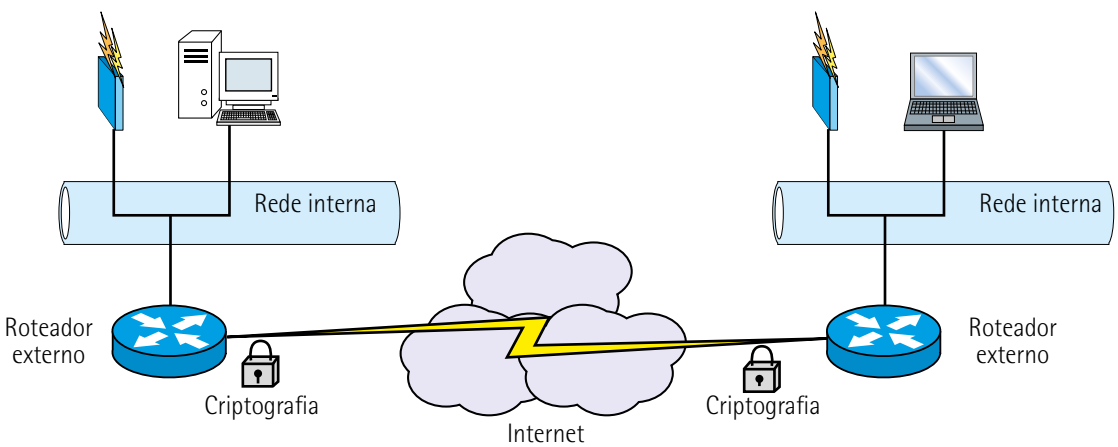

Figura 23 – Conexão segura entre redes internas via rede externa (VPN)

Segundo Ramos (2008), as redes públicas de comunicação sempre estiveram disponíveis, e há muitos anos existem tecnologias que permitem estabelecer conexões ponto a ponto sobre elas. Um bom exemplo é o PPP (point-to-point protocol), muito usado no começo da internet para conectar computadores que se comunicavam pela rede de telefonia. As tecnologias que permitem estabelecer um túnel privado em cima de uma rede pública são as redes virtuais privadas ou VPNs.

Com a popularização da internet, um novo nicho de possibilidades se abriu para essas tecnologias, pois elas permitiam que empresas em locais diferentes do globo se comunicassem sem gastar fortunas com links diretos internacionais. Por conta dos problemas de segurança, difundiram-se as tecnologias VPN que utilizam criptografia.

Apesar de tecnicamente não implicar o uso de segurança, a palavra VPN é hoje quase sinônima de VPN segura, ou seja, que usa mecanismos de criptografia e proteção.

A figura a seguir ilustra a comunicação entre escritórios localizados em distintas cidades do mundo. Para isso, usou-se nada mais do que uma VPN sobre a internet.

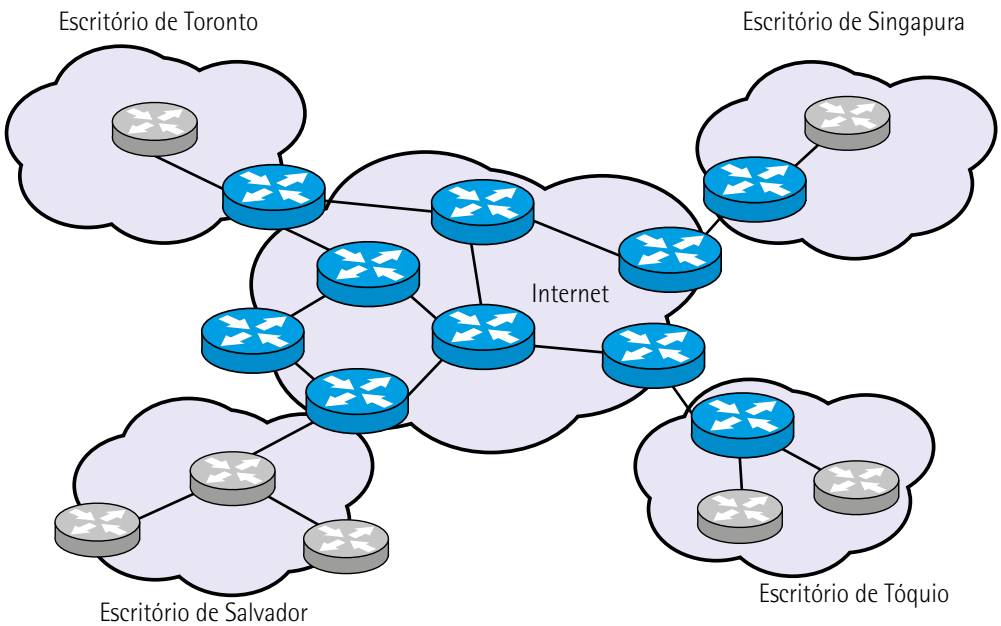

Figura 24 – Interligação entre redes através de uma VPN

Nessa solução, circuitos de acesso dedicados foram substituídos por conexões lógicas sobre a internet. Essas conexões podem ser realizadas entre nós, roteadores, firewalls e outros dispositivos.

Dentro desse conceito, a internet tornou-se um backbone virtual, gerando uma redução potencial de custos com a substituição de linhas privativas. Essa solução permite conexão em banda larga entre matriz e filiais, além de conexão via xDSL ou cable modem para home office. Outras aplicações de VPN incluem acesso para pessoal que trabalha em campo e conexões entre empresas parceiras.

As figuras a seguir mostram alguns cenários de uso de VPN.

Figura 25 – VPN para conexão home office

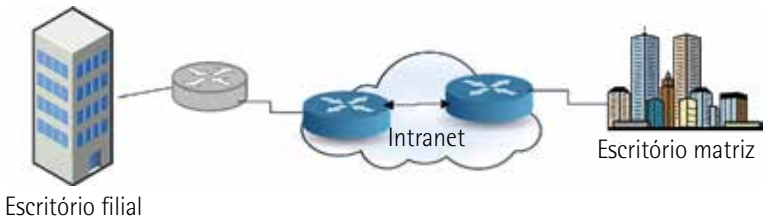

Figura 26 – VPN para conexão de intranet

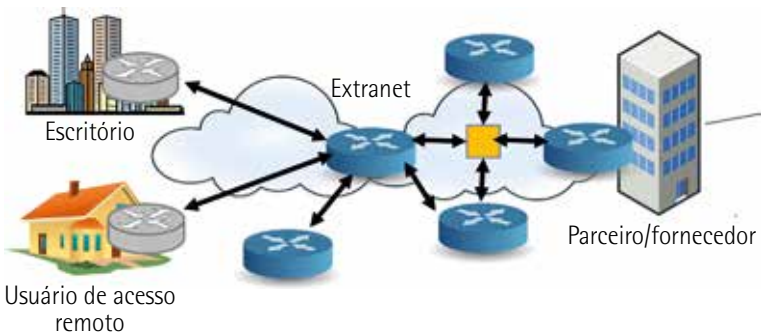

Figura 27 – VPN para conexão de extranet

Embora a demanda por home office já existisse antes da disponibilidade dos serviços xDSL, os meios existentes, isto é, as conexões discadas, não tinham performance suficiente (dial-up assíncrono) ou não estavam disponíveis na quantidade necessária (rede digital de serviços integrados).

Os serviços xDSL oferecem banda passante mais do que suficiente para atender à demanda de escritórios remotos individuais (home office), e mesmo de escritórios remotos de maior porte.

As conexões LAN to LAN (local area network to local area network) através da internet permitem que as organizações não necessitem mais de frame relay ou de linhas privadas para conexões privadas. Além disso, garantem conexões seguras com empresas parceiras (extranet). Podemos listar algumas vantagens do uso de VPN:

- escalabilidade;
- facilidade de gerenciamento;

- menor chance de falha;
- necessidade de menos equipamentos;
- pagamento apenas do uso (em algumas modalidades);
- menor custo em relação à linha privada (mais de 50% de redução).

As VPNs podem ser usadas para substituir ou ampliar redes privadas, incluir novas aplicações sem interromper as atuais e inserir novas unidades. Os ganhos são maiores quanto mais geograficamente espalhada estiver a empresa.

Contudo, as VPNs não são recomendadas quando a performance não é tão vital ao negócio, quando existem aplicações não IP na rede que não podem ser tuneladas e para tráfego de voz, vídeo ou outro tráfego isócrono.

O problema com as aplicações isócronas é que não existe controle de congestão e acesso. Além disso, a latência, o jitter (variância da latência), a perda de pacotes e a vazão (especialmente numa rede IP/frame relay) são muito grandes, o que afeta diretamente a qualidade do serviço.

Outro ponto importante que deve ser observado é a segurança. Algumas características presentes na VPN:

- **Autenticação**: identifica com quem se está comunicando.
- **Tunelamento**: encapsula dados roteados através da rede pública.
- **Criptografia**: garante a segurança.

As VPNs podem ser implementadas por hardware ou software. Todas as soluções de VPN envolvem a aplicação de diversos algoritmos, e nenhum deles é interoperável.

Uma vantagem da implementação por hardware é a velocidade: o uso de hardware criptográfico com chips dedicados torna a VPN muito rápida e não sobrecarrega a CPU de roteadores, firewalls ou gateways.

Essa é uma solução do tipo black box, ou seja, um hardware dedicado. Existem vários appliances com essa finalidade e vários fabricantes que fornecem essa solução (como Cisco e Nortel Networks).

Entre as vantagens do uso de software, estão: facilidade de implementação, que pode ser massificada; facilidade de distribuição de updates e patches por e-mail e web; gerenciamento centralizado; e menor possibilidade de erros.

A implementação de VPN usando a internet obriga a pensar em segurança. Devem ser instalados mecanismos de autenticação, que permitam saber com quem se está comunicando; de integridade, de modo que os dados não sejam alterados no trânsito; e de acesso, para que pessoas não desejadas não consigam acessar sistemas, softwares e dados.

Cada maneira de implementar uma VPN usa diferentes protocolos em diferentes camadas do modelo OSI. Existem os seguintes tipos de configuração:

- **Camada 2 (camada de enlace)**: PPTP (point-to-point tunneling protocol), L2F (layer 2 forwarding), L2TP (layer 2 tunneling protocol), além de VPNs criadas com frame relay e ATM (asynchronous transfer mode).

- **Camada 3 (camada de rede)**: MPLS (multiprotocol label switching) e IPSec.

- **Camadas 4–7 (da camada de transporte à de aplicação)**: SSL/TLS (secure socket layer/transport layer security), S/Mime (secure/multipurpose internet mail extensions) e SSH (secure shell).

Segundo Moraes (2010), apesar de pouco utilizadas, também há VPNs discadas, conhecidas como VPDNs (virtual private dial-up networks).

O PPTP foi o primeiro protocolo para o tunelamento. Ele é usado em máquinas com sistemas operacionais Microsoft e faz VPN ponto a ponto. O PPTP permite implementar criptografia na camada de enlace com o protocolo RC4-RSA. Basicamente, é uma extensão do PPP.

A integridade do PPTP, baseada no algoritmo MD4 (message digest 4), é fraca; há programas de crackers que conseguem descobrir o tráfego de uma VPN PPTP. Mesmo assim, é um dos protocolos mais difundidos porque foi um dos primeiros disponíveis.

Além de VPN ponto a ponto, faz fim a fim. Necessita de servidores Microsoft para implementar os túneis e encapsula NetBEUI (NetBIOS extended user interface), IPX (internetwork packet exchange) e AppleTalk.

O PPTP tem algumas restrições, como especificar o gerenciamento proprietário das chaves (ou seja, tem que ser adquirido), não existir criptografia quando usado em acesso remoto e permitir uma única conexão no túnel.

O L2F é um protocolo proprietário Cisco. Sua implementação baseou-se no uso tanto do PPP como do PPTP para a autenticação do usuário. O L2F trabalha com Radius e Tacacs+ (terminal access controller access-control system plus). Não suporta criptografia, porém é mais poderoso que o PPTP, pois permite várias conexões no mesmo túnel.

O L2TP, que combina o L2F com o PPTP, também é uma extensão do PPP. Só pode ser usado em VPN nó a nó devido à aplicação na camada de enlace. Para funcionar fim a fim, todos os nós da rede (roteadores) precisam suportar L2TP.

O L2TP trabalha e interopera com o IPSec, garantindo confidencialidade com a criptografia e tornando-se a melhor solução para o acesso remoto.

Também funciona com redes baseadas em quadros, como frame relay e X.25, e encapsula protocolos como NetBEUI, IPX e AppleTalk. A autenticação é garantida pelo PAP (password authentication protocol) ou pelo Chap (challange handshake authentication protocol). Suporta Radius e Tacacs.

A solução VPN frame relay faz a separação de tráfego por circuitos virtuais, os DLCIs (data link connection identifiers). Numa VPN frame relay, não existe encriptação, o que não é necessário, pois o protocolo atua apenas na camada 2 do modelo OSI, sendo uma solução segura para o acesso. O frame relay é suportado para velocidades baixas.

O MPLS, de acordo com Moraes (2010, p. 111),

> [...] é uma novidade no mercado e promete, além de uma infraestrutura de VPN segura, a garantia da qualidade de serviço, assegurando resolver problemas como congestionamentos, atrasos e jitters encontrados nas VPNs tradicionais. Uma rede MPLS comuta pacotes baseados no label, e não no endereço IP. É flexível, pois não exige provisionamento complexo de PVC ou gestão dos túneis. Os problemas encontrados nas VPNs MPLS estão relacionados a não padronização e baixa interoperabilidade entre diferentes fabricantes.

A utilização de VPN com IPSec também é uma tendência. O IPSec foi constituído para operar tanto em ambiente de estação do usuário como em gateway (roteador, concentrador etc.), garantindo a segurança do tráfego IP. A proteção oferecida é baseada nas necessidades da política de segurança estabelecida e mantida pelo usuário ou administrador do sistema.

O IPSec é um protocolo de tunelamento desenhado tanto para IPv4 como para IPv6 e oferece mecanismos de segurança fim a fim e criptografia na camada IP.

Basicamente, os serviços disponibilizados são:

- **Integridade**: os pacotes são protegidos contra modificação acidental ou deliberada.
- **Autenticação**: a origem de um pacote IP é autenticada criptograficamente.
- **Confidencialidade**: a parte útil de um pacote IP ou o próprio pacote IP podem ser criptografados.
- **Antirreplay**: o tráfego IP é protegido por um número de sequência que pode ser usado pelo destino para prevenir ataques do tipo replay (que repetem a sequência antes enviada).

O IPSec permite a interoperabilidade de implementações de diferentes fabricantes e é uma solução de segurança fim a fim entre roteadores, firewalls, estações de trabalho e servidores. Ele se integra com a pilha TCP/IP existente, sendo transparente para todos os usos, ou seja, não há necessidade de executar nenhuma alteração nos sistemas existentes para a aplicação do IPSec.

O IPSec utiliza criptografia simétrica, pela rapidez do mecanismo para encriptar dados, e criptografia assimétrica, por meio de mecanismos de troca de chaves criptográficas. Os algoritmos de hashing no IPSec geram hashs de tamanho de 128 ou 160 bits.

Os algoritmos suportados pelo IPSec são:

- **Para a criptografia**: AES, DES, 3DES, RC5 (Rivest cipher 5), Idea (international data encryption algorithm), Cast (Carlisle Adams and Stafford Tavares) e blowfish.
- **Para o hashing**: MD5 (message digest 5), SHA-1 (secure hash algorithm 1) e tiger.
- **Para a autenticação**: assinaturas digitais RSA e DSS (digital signature standard).

A associação de segurança é um acordo estabelecido entre os dois pontos da comunicação para a negociação de parâmetros do túnel IPSec. Deve-se estabelecer esse acordo antes da criação do túnel IPSec. Entre os mesmos dois pontos, podem existir múltiplas associações de segurança.

Essas associações ficam armazenadas na SPD (security policy database) e na SAD (security association database). Cada uma tem seu identificador único no SPI (security parameter index).

Na associação de segurança, são negociados os seguintes mecanismos de segurança:

- modo do túnel IPSec – AH (authentication header) ou ESP (encapsulating security payload);
- algoritmo de criptografia;
- método de autenticação;
- função de hashing;
- método de autenticação do usuário (Radius, SecurID);
- escolha de chaves criptográficas e chaves de autenticação.

Saiba mais

Para conhecer mais sobre a resolução de problemas de segurança em redes VPN, acesse:

BRADLEY, S. 4 passos para não ter problemas de segurança com redes VPN. *ComputerWorld*, 27 jun. 2018. Disponível em: <http://computerworld.com.br/4-passos-para-nao-ter-problemas-de-seguranca-com-redes-vpn>. Acesso em: 5 jul. 2018.

6.2 VLANs

Uma forma básica de segregação de tráfego disponível na maioria dos switches é o uso de VLANs (virtual LANs), ferramenta a que se recorre extensivamente com o propósito de diminuir o impacto do tráfego de broadcast em redes de grande porte. Do ponto de vista da segurança, é possível utilizar essa funcionalidade em duas situações bastante comuns.

A VLAN para **uso externo** destina-se a usuários que acessam serviços internos através de meios externos. A técnica é muito empregada em data centers que alugam equipamentos de grande porte para diversos clientes pequenos, normalmente com o objetivo de compartilhar recursos e otimizar o custo. A fim de segregar o tráfego que os clientes são capazes de "ver", é possível inserir um servidor virtual para cada cliente, em VLANs separadas, garantindo assim que externamente eles tenham conectividade apenas com sua respectiva rede e que o tráfego não se misture com o de outros clientes. Fisicamente, somente um servidor e um segmento de rede existem.

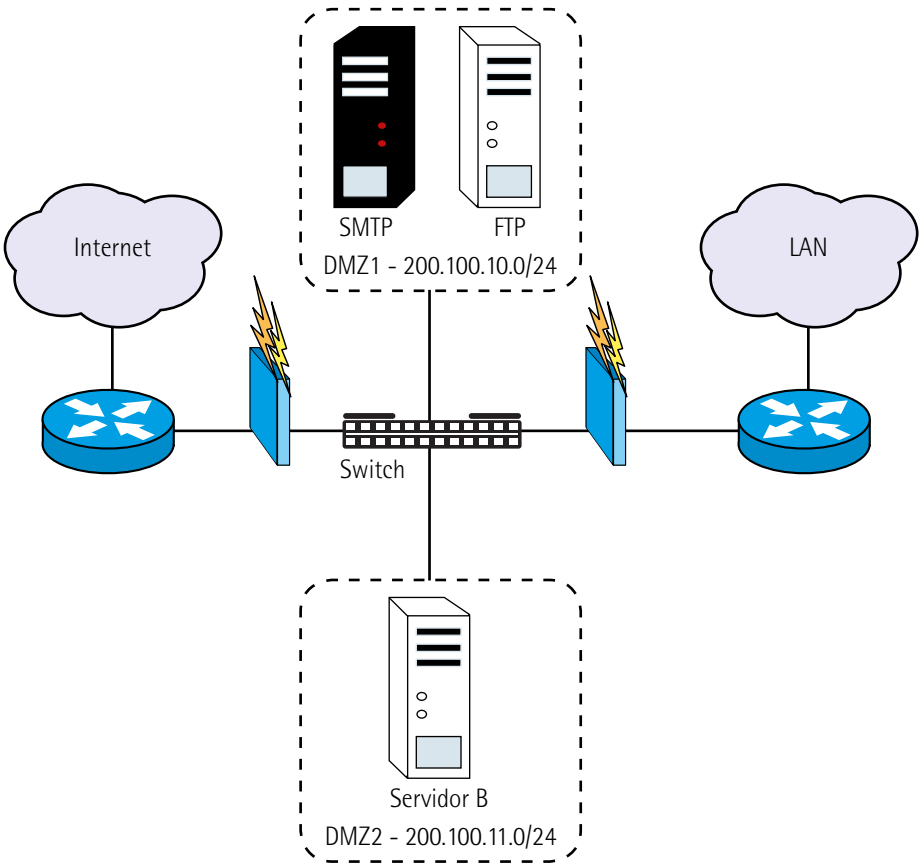

Figura 28 – Topologia para duas VLANs externas, usadas como DMZ

A VLAN para **uso interno**, como o próprio nome indica, é destinada a ambientes internos. Seu uso é mais frequente e tem aplicações mais comuns. A principal delas, do ponto de vista da segurança, é evitar que, dentro de um mesmo segmento de rede, o tráfego, cuja interceptação pode trazer problemas de segurança, seja segmentado daquele que normalmente é produzido pelos usuários. Um exemplo de tráfego com essas características é a comunicação de DMZ, que pode conter informações críticas, como o endereçamento de interfaces.

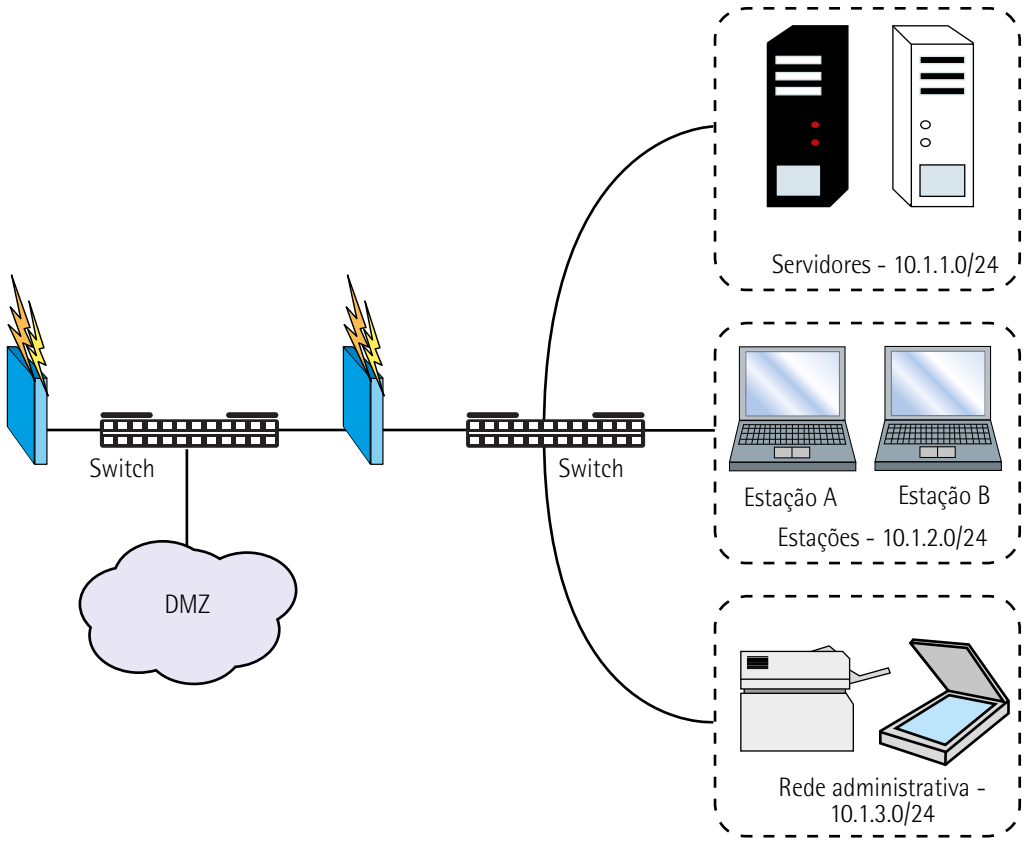

Figura 29 – Topologia para três VLANs internas

Um exemplo mais simples: imagine uma impressora que tem uma interface para administração remota. Todos os usuários desse recurso precisam conhecer o endereço de rede dele para despachar trabalhos de impressão. No entanto, no que diz respeito à administração, ela deve ficar confinada apenas ao grupo de administradores. Nem sempre a interface de administração remota trabalha com protocolos seguros. Por conta disso, é necessário impedir que os usuários comuns interceptem o tráfego de administração dessa impressora, o que lhes permitiria ter acesso a parâmetros críticos ou mesmo a senhas.

Uma solução possível, nesse caso, é criar duas VLANs, uma para a impressão e outra para a administração, garantindo que apenas os administradores façam parte da segunda. A impressora deverá ter dois endereços, participando de ambas as redes, e as funções de impressão deverão estar confinadas à rede apropriada, assim como as funções de administração. Com isso, usuários comuns não terão conectividade com a interface de administração, o que evitará muitos problemas de segurança.

Segundo Forouzan (2008), as principais vantagens de implantar VLANs são:

- **Aumento de performance**: a diminuição significativa de broadcast no tempo de resposta na rede auxilia a disponibilidade das informações.

- **Aumento da segurança**: a separação que as VLANs proporcionam entre as redes e os usuários possibilita a melhora nos quesitos de confidencialidade e integridade das informações.

- **Facilidade de gerenciamento**: com o uso das VLANs, o processo de rede é simplificado, além de ser mais rápido, prático e eficiente o processo de configuração através das plataformas de gerenciamento, o que contribui para o aumento da confidencialidade das informações.

- **Topologia de rede independente**: a disposição lógica da rede fica independente e segregada da topologia física, o que torna as modificações nessa rede mais flexíveis.

Nos switchs modernos, chamados de **multicamadas**, existe a possibilidade de desenvolver projetos de VLANs das mais variadas formas.

Quadro 26 – Tipos de configuração de VLANs em switchs multicamadas

Tipo	Descrição
VLANs por porta	Critério mais tradicional, também suportado por switches camada 2 comuns.
VLANs por endereço MAC (media access control)	Critério que apenas alguns switches suportam. Esse sistema baseia-se na configuração do endereço MAC da estação como política da VLAN. Assim que a estação se conecta à rede, independentemente do local físico em que esteja, automaticamente é conectada à VLAN. Essa solução é muito empregada por usuários de notebooks.
VLANs por endereço IP	O switch verifica o endereço de origem da máquina conectada a ele e realiza a ligação dessa máquina a sua VLAN correspondente.
VLANs por autenticação	Quando um usuário se conecta à rede, é solicitada uma autenticação. Feita a autenticação, o switch conecta o usuário a sua VLAN determinada.

Observação

Switchs multicamadas dispensam o uso de roteadores nas VLANs, uma vez que também têm a capacidade de realizar a função de roteamento.

6.3 WLANs

Ramos (2008, p. 237) afirma que, no atual cenário das tecnologias de rede,

> [...] a questão da mobilidade e da conectividade em qualquer ponto do planeta, a qualquer momento, vem se tornando uma verdadeira tendência de mercado. Todos desejam de maneira geral estar sempre conectados à internet, através de notebooks, celulares, PDAs etc.

Para isso ser possível, a tecnologia wireless (sem fio) tem se tornado fundamental. A quantidade crescente de aplicações e a facilidade de conexão à rede concorrem para que essa tecnologia seja vista com grande interesse por executivos e gestores de negócios e de TI.

De modo geral, todas as redes estão sujeitas à captura de informações por terceiros, desde que eles estejam conectados à mesma rede cabeada pela qual trafegam essas informações. Contudo, num

ambiente de rede cabeada, os acessos são mais controlados. É mais simples, por exemplo, detectar um intruso no ambiente interno da empresa.

Nas redes sem fio, por outro lado, a facilidade de furtar informações é enorme, pois o intruso pode estar em qualquer local da área de abrangência coberta pelo sinal dos APs (access points). Tudo o que for transmitido dentro dessa área poderá ser capturado e decodificado, "quebrando-se", portanto, a confidencialidade e a integridade da informação.

Um protocolo de comunicação desenvolvido com o objetivo de criar redes sem fio de alta velocidade não faz nada mais do que transferir dados por ondas de rádio em frequências não licenciadas.

A não obrigatoriedade de qualquer tipo de licença ou autorização do órgão regulador das comunicações para operar foi um dos fatores que levaram as empresas a adotar redes sem fio em alta escala, além, é claro, da grande vantagem da mobilidade dentro da área de cobertura do sinal.

A seguir, veremos as principais características das redes sem fio, também chamadas de WLANs (wireless local area networks), e de que maneira podem ser usadas mantendo-se seus riscos em patamares aceitáveis.

O padrão 802.1X fornece autenticação em nível de link, de estações móveis wireless com APs, através de dois tipos de sistema: **aberto**, em que qualquer estação wireless pode se conectar livremente, ou seja, não há autenticação do usuário da ponta, e **de chave compartilhada**, também conhecido como shared key.

APs são dispositivos que podem conectar uma rede cabeada – por exemplo, uma rede ethernet – à rede sem fio. Nada impede, porém, de utilizar um AP para conectar várias máquinas, sem conexão com a rede cabeada, e formar uma WLAN.

Um AP pode estender a distância da rede cabeada para além de cem metros, dependendo da potência do sinal e das interferências eletromagnéticas no raio de cobertura dele. Recorrer a outros APs pode expandir ainda mais a área de cobertura do sinal, com esses novos equipamentos funcionando como repetidores de sinal. No entanto, a cada vez que se aumenta a área de cobertura, cresce também a possibilidade de um intruso capturar as informações que trafegam pelo ar.

Os APs devem ser configurados para permitir apenas estações autorizadas a acessar a WLAN, ou seja, somente estações com o mesmo SSID (service set identifier), endereços MAC autorizados e chaves WEP (wired equivalent privacy) compartilhadas poderão acessá-la.

Qualquer tipo de tráfego sem criptografia deve ser descartado pelo AP, de modo que estações wireless ou outros dispositivos não se conectem a ele a menos que conheçam a chave WEP correta. O esquema de segurança para redes sem fio deve sempre levar em conta a criptografia das informações. Apesar de o protocolo WEP não ser o ideal, pois existem falhas em sua implementação, é melhor usá-lo a manter o texto em claro.

Enquanto a codificação WEP torna mais difícil para o atacante decifrar o tráfego, o desenho do WEP, independentemente do tamanho das chaves (64 ou 128 bits), torna o protocolo mais suscetível a ataques. O WEP é utilizado para criar uma string de caracteres binários pseudorrandômicos, e o tamanho total da chave consiste na soma de um vetor de inicialização (ou IV) com a chave WEP. O tamanho do IV é de 24 bits. Isso significa que, numa chave de 64 bits, somente 40 bits são fornecidos pelo usuário. O mesmo é verdadeiro para a chave de 128 bits: 24 bits são do IV e 104 bits são fornecidos pelo usuário.

O algoritmo RC4 empregado pelo WEP determina modificações periódicas nos 24 bits adicionais das chaves, dificultando a quebra destas por sniffers. Entretanto, a duração dessa modificação é limitada: como o IV tem apenas 24 bits, ele se repetirá periodicamente, o que dará margem para um atacante capturar dois ou mais IVs idênticos e realizar uma análise de frequência nos dados capturados, podendo chegar à quebra da confidencialidade da chave WEP.

Quando utilizamos o MAC filtering, adotamos a filtragem pelo endereço físico da placa de rede wireless (também conhecida como MAC address filtering). Isso permite inserir no AP uma lista de controle de acesso, a qual garante o acesso ao AP apenas de clientes que tiverem seus respectivos endereços MAC previamente cadastrados. Caso o AP não reconheça o endereço MAC, ele não vai repassar os pacotes. Endereços MAC desconhecidos são imediatamente descartados.

Como o mecanismo de proteção desse sistema é delicado, pois o endereço MAC da placa wireless pode ser forjado ou roubado, cuidados adicionais devem ser tomados para que o AP esteja acessível apenas a endereços MAC conhecidos, o que se pode fazer por meio de autenticação 802.1X, utilizando-se um servidor Radius, Tacacs+ ou Kerberos.

O SSID broadcast serve para identificar a rede sem fio, atribuindo a ela um nome, ou seja, somente estações que conheçam o nome correto da rede sem fio poderão fazer parte dela. Normalmente, todas as redes sem fio utilizam a divulgação continuada (broadcast) de seu SSID, o que, apesar de não recomendado nas boas práticas de segurança de redes sem fio, facilita a conectividade de usuários móveis, que podem detectar o SSID da rede e tentar a conexão, caso o AP empregue um sistema aberto de autenticação (sem autenticação). O SSID das redes sem fio é normalmente transmitido sem proteção criptográfica e pode ser capturado por qualquer estação que esteja no raio de cobertura do AP.

Quanto ao padrão de funcionamento da comunicação 802.1X, devemos pensar nele como um portão dentro de switches ethernet e APs, que começa na posição fechada, tratando somente de requisições 802.1X, até que uma permissão de entrada seja liberada para a estação requisitante; nesse ponto, o portão se abre e deixa passar todo o tráfego entre a estação autenticada e a rede. Eventualmente, a estação pode perder a conexão por time-out e o portão se fechar novamente para ela.

O 802.1X define o protocolo de gerenciamento a ser usado pelas estações para solicitar o acesso à rede. Ele utiliza o EAP (extensible authentication protocol), originalmente definido para dial-up, mas nesse caso enviado pela rede ethernet (EAPoL – EAP over LAN) ou pelas redes sem fio (EAPoW – EAP over wireless). A estação deve se conectar primeiramente ao meio físico, através da placa de rede, e então enviar uma mensagem EAP start. Essa mensagem desencadeia um fluxo de mensagens de gerenciamento, que deverá terminar com EAP success ou EAP failure.

O EAP pode ter diferentes tipos de autenticação, como desafio/resposta, OTP (one-time password), SecurID tokens e certificados digitais. O processo que ocorre entre EAP start e EAP success depende do tipo de autenticação utilizada.

Como qualquer usuário pode, teoricamente, conectar-se às WLANs, faz-se necessário utilizar um processo de autenticação para garantir o mínimo de segurança às redes sem fio. Essa autenticação emprega os protocolos abordados a seguir.

O **Peap** (protected extensible authentication protocol) usa um certificado digital a fim de autenticar uma estação wireless para o AP e transmitir a autenticação da estação através de um túnel criptografado. A autenticação para o cliente na ponta, porém, fica por conta de outras opções.

Com o Peap, as organizações podem evitar problemas relacionados à instalação de certificados digitais em cada cliente, como no EAP-TLS (discutido adiante). Em vez desse processo, mais trabalhoso, é possível selecionar métodos de autenticação como senhas de login ou OTP.

O **Leap** (lightweight extensible authentication protocol) foi criado pela Cisco em 2000. Esse algoritmo, que funciona como uma extensão do EAP, fornece suporte à autenticação mútua, tanto para o usuário da ponta como para o gerenciamento e a distribuição centralizada de chaves. As principais melhorias incorporadas ao Leap são:

- **Derivação segura de chave**: característica extremamente técnica e que demanda do profissional de segurança conhecimento prévio dos sistemas de autenticação do tipo desafio/resposta. O sistema original de derivação segura de chave secreta compartilhada é utilizado para gerar respostas ao sistema de autenticação mútua, o qual, por sua vez, resolve a questão de ataques de replay, que podiam ser realizados no sistema antigo. Os valores de base enviados pela rede são úteis apenas no início do processo de autenticação.

- **Chaves WEP dinâmicas**: alguns dos principais problemas de segurança do protocolo WEP são sua implementação (tamanho do vetor de inicialização), a chave única (estática) para a criptografia dos dados e o trabalho que essa limitação impõe aos administradores da WLAN. A utilização do Leap garante que as chaves de sessão sejam únicas para os usuários e que não sejam compartilhadas entre eles. Pela autenticação Leap, codifica-se o broadcast da chave WEP usando-se a chave de sessão antes de ela ser passada ao usuário da ponta. Com uma chave de sessão única para cada usuário, vinculada ao processo de login na rede, essa solução consegue minimizar a possibilidade de roubo ou perda da chave.

- **Políticas de reautenticação**: o Leap também permite aos administradores das WLANs configurar políticas de reautenticação no servidor Radius, o que força os usuários a se reautenticar mais frequentemente, recebendo assim novas chaves de sessão, a fim de minimizar ataques em que o tráfego é injetado.

O processo de autenticação 802.1X utiliza o **EAP-TLS** (extensible authentication protocol – transport layer security) entre estações wireless e um servidor de autenticação. O EAP possibilita o uso de diversos

protocolos de autenticação, como Radius e chaves assimétricas. Uma estação wireless solicita acesso ao AP; este repassa a solicitação a um servidor, que autentica ou não o usuário que está tentando se conectar; se a autenticação for bem-sucedida, o servidor enviará uma chave de criptografia ao AP, que utilizará essa chave para cifrar a chave de sessão e enviá-la à estação wireless. A possibilidade de transmissão da chave é uma opção do padrão 802.1X e permite o gerenciamento dinâmico da geração de chaves de criptografia. Isso não era possível no padrão 802.11; como consequência, o processo de distribuição manual de chaves para a criptografia era utilizado, o que inviabilizou a disseminação desse padrão.

Por meio do EAP-TLS, a estação wireless autenticada terá acesso à rede, e todas as transmissões entre o cliente e o AP estarão cifradas, ficando garantidas a integridade e a confidencialidade dos dados transmitidos.

Quando consideramos os princípios de confidencialidade, integridade e disponibilidade, obrigatoriamente devemos tratar dos protocolos comentados a seguir.

O **WEP**, protocolo de segurança especificado no padrão IEEE 802.11b, foi desenvolvido para garantir a segurança na transmissão de dados em WLANs através do uso de chaves simétricas de criptografia. É um protocolo de camada 2, suportado pela maioria dos fabricantes de dispositivos wireless. Baseia-se numa chave secreta, que deve ser compartilhada entre a estação móvel e o AP. A chave secreta é utilizada para cifrar os pacotes antes de sua transmissão para o AP.

Se um usuário ativar o WEP, sua placa cifrará o payload (conteúdo do pacote) de cada quadro 802.11 transmitido usando o algoritmo RC4. O AP decodificará o pacote com a mesma chave empregada para a codificação. É importante lembrar que, ao deixar o AP e entrar na rede cabeada, os pacotes não estarão mais cifrados.

O protocolo WEP, apesar de bastante difundido, é extremamente vulnerável a ataques de força bruta, bem como de dicionário. Se um atacante capturar uma quantidade suficiente de pacotes protegidos pelo protocolo WEP, não importando o tamanho da chave usada (64 ou 128 bits), ele conseguirá decifrá-los sem grande esforço, pois a chave usada para codificá-los é facilmente recuperada. Existem diversas ferramentas livremente disponíveis na internet para efetuar essa operação.

O **WPA** (Wi-Fi protected access), também denominado WEP2, surgiu de um de um esforço conjunto de membros da Wi-Fi Alliance e de membros do IEEE (Instituto de Engenheiros Eletricistas e Eletrônicos), os quais buscaram aumentar o nível de segurança das redes sem fio combatendo algumas vulnerabilidades do WEP.

A estrutura do WPA é a junção do sistema de autenticação 802.1X com o protocolo de rotação de chaves TKIP (temporal key integrity protocol), mais o protocolo de criptografia AES, sendo esse último opcional.

O WPA depende do 802.1X para autenticar os clientes wireless via servidor Radius e para gerar as chaves de sessão utilizadas na criação das chaves de criptografia dos dados, o que exige que ele utilize um método de autenticação que resulte na geração de uma chave de sessão (EAP-TLS, por exemplo). Devido a esse processo de autenticação ser exclusivo para cada cliente da WLAN, o AP com WPA lidará com múltiplas chaves e deverá ter uma quantidade de memória compatível com o tamanho da WLAN em número de usuários.

O **TKIP** é o protocolo responsável por geração da chave de criptografia, codificação dos dados e verificação de sua integridade.

As chaves do TKIP são mais longas (256 bits) que as do WEP (64 e 128 bits), e, portanto, mais difíceis de serem quebradas. Além disso, são geradas por um processo mais bem elaborado e consequentemente mais robusto.

O **WPA2** (Wi-Fi protected access 2), um novo padrão de segurança para redes sem fio, não é compatível com os protocolos anteriores, e sua arquitetura é definida pelo padrão IEEE 802.11i. Ele utiliza o protocolo CCMP (counter mode with cipher-block chaining message authentication code protocol), que faz uso extensivo do algoritmo AES, para confidencialidade, integridade e autenticação, estando assim em conformidade com os padrões de segurança definidos pelo governo norte-americano para a proteção de dados. Apesar de regionalizados, tais padrões servem de referência internacional e são seguidos em muitos países.

Em 2014, o padrão WPA2 teve sua integridade disponibilizada na internet, o que o tornou, da mesma maneira que seus antecessores (WEP e WPA), vulnerável a ataques – o mais recente, datado de 2017, foi um ataque chamado de Krack (key reinstallation attack) (MCGEE, 2017). A Wi-Fi Alliance, entidade responsável pelas certificações da conexão wireless, prometeu lançar o mais rápido possível equipamentos compatíveis com um novo padrão, o WPA3.

Saiba mais

Para conhecer mais sobre o padrão WPA3, acesse:

RIBEIRO, G. WPA3 deve chegar ainda em 2018 para tornar conexão Wi-Fi mais segura. *TechTudo*, 10 jan. 2018. Disponível em: <https://www.techtudo.com.br/noticias/2018/01/wpa3-deve-chegar-ainda-em-2018-para-tornar-conexao-wi-fi-mais-segura.ghtml>. Acesso em: 5 jul. 2018.

Diversos problemas de segurança estão associados ao uso dessas tecnologias. Apresentamos alguns a seguir.

O sinal das redes wireless, muitas vezes, cobre um perímetro físico maior do que o inicialmente previsto, o que facilita interceptá-lo. O risco de captura do sinal pode ser ainda maior se houver o uso de antenas. Esses fatores tornam a localização das redes uma tarefa bastante simples, aumentando a exposição aos problemas de segurança.

Uma vez que o sinal pode vazar para um perímetro físico grande, pessoas em localidades vizinhas ou mesmo na rua podem acessar a rede. Em geral, elas o fazem com o propósito de usar a internet de forma gratuita, utilizando indevidamente os links de comunicação de terceiros. São necessários mecanismos de autenticação e controle de acesso para impedir esse tipo de atividade.

Podemos destacar também alguns tipos de ataque:

- **Sniffing**: um usuário da rede wireless escuta e captura o tráfego que está passando por ela.
- **DoS**: um cracker causa interferências na faixa de frequência da rede wireless para derrubar o serviço.
- **Rogue access point**: um cracker adiciona um access point falso na rede, e os usuários, por não saberem, conectam-se a ele, pensando ser a rede desejada. É um ataque muito comum em redes públicas.
- **Wardriving ou warchalking**: consiste em dirigir ou andar pela cidade à procura de redes sem fio abertas, que possam ser invadidas. Nem sempre é necessário estar próximo à rede em questão. Existem relatos de ataques a redes com distância de até 8 km.

Além dos problemas anteriores, existe muita preocupação com o sigilo e a integridade dos dados que trafegam por essas redes, devido à grande exposição. Por isso, é necessário utilizar mecanismos que garantam a segurança das informações que trafegam por elas. Até hoje, porém, a maioria dos mecanismos projetados para o padrão 802.11 mostrou-se ineficiente.

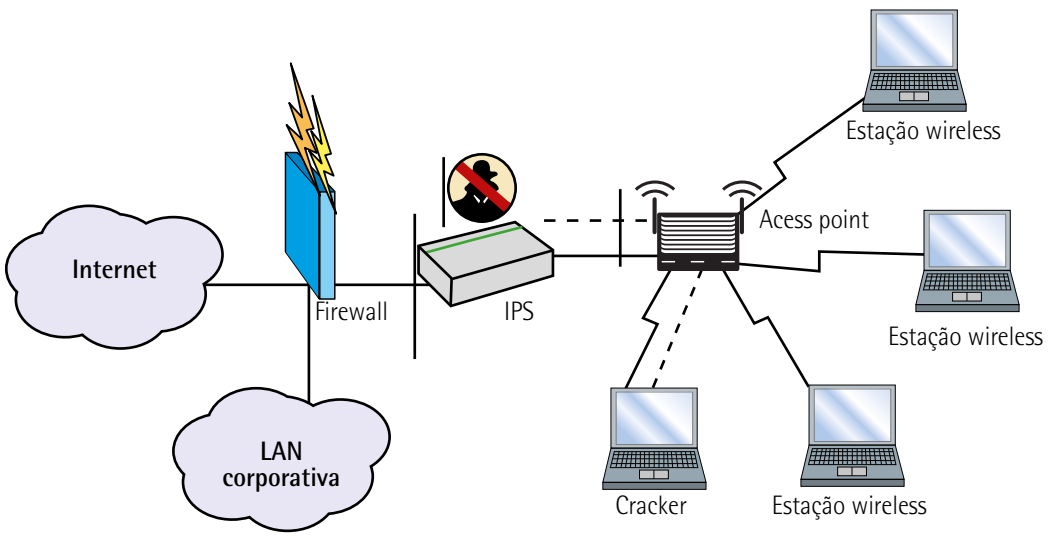

Figura 30 – Implementação de firewall e IPS para proteger uma rede sem fio

6.4 IPSec

O IPSec, projetado para garantir funcionalidades de segurança (confidencialidade, integridade e autenticação) ao protocolo IP, trabalha como um protocolo à parte no IPv4 e como parte nativa da especificação do protocolo IPv6. Enquanto no SSL/TLS há proteção apenas para protocolos que utilizem a comunicação via TCP, no IPSec pode-se prover segurança para qualquer protocolo que vá encapsulado diretamente em cima do IP, ou seja, praticamente todos os utilizados na internet. As especificações preveem dois modos de operação:

- **Tunnel mode**: todo o pacote original a ser codificado, incluindo a própria porção IP, é cifrado e colocado dentro de um novo pacote IP. Dessa forma, escondem-se até mesmo informações sobre as pontas da comunicação. Esse método, por manter mais informações em segredo, é considerado o mais seguro na maioria dos casos. Como mais informações são codificadas, ele é ligeiramente mais lento, e como um novo pacote é criado, colocando-se dentro dele o pacote original, o consumo de banda é maior.

- **Transport mode**: destinado para a comunicação máquina a máquina. Nesse caso, a codificação da porção IP do pacote não traz ganhos de segurança.

A estrutura do IPSec é composta de dois protocolos:

- **AH**: provê os serviços de integridade e autenticação, porém os dados não são codificados. Serve para situações em que existe a necessidade de confirmar a origem do tráfego e ter garantias de que ele não foi alterado, sem que haja a necessidade de sigilo.

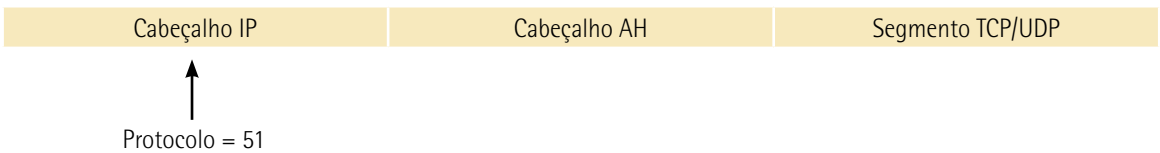

Figura 31 – Protocolo AH

- **ESP**: além das funcionalidades presentes no AH, oferece também confidencialidade, sendo o protocolo mais usado.

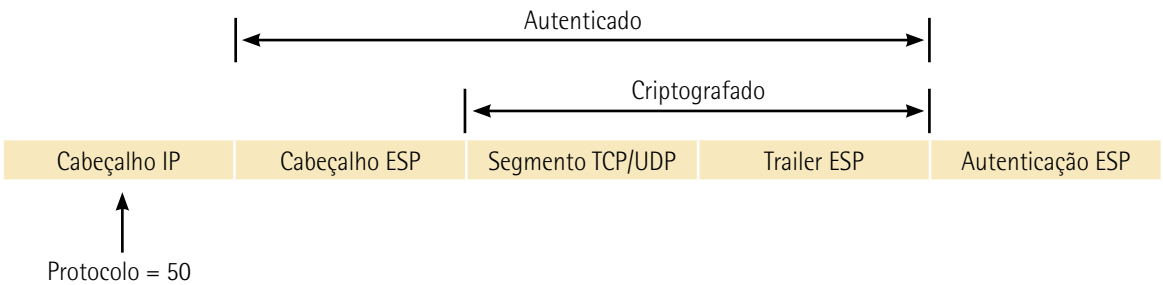

Figura 32 – Protocolo ESP

As conexões IPSec são estabelecidas através de SAs (security associations), as quais representam uma conexão lógica entre as duas máquinas que estão se comunicando e são unidirecionais. Portanto, para a maioria dos casos, uma comunicação bidirecional entre duas máquinas requer duas SAs, que contêm:

- **SPI (security parameter index)**: identifica de forma única duas SAs que porventura tenham os mesmos parâmetros de IP de destino e protocolo.

- **IP de destino**: identifica qual endereço de destino pode ser atingido por meio dessa conexão IPSec.

- **Protocolo**: identifica o tipo de protocolo presente na associação (ESP ou AH).

Em geral, uma SA é criada para cada protocolo, mas existem casos em que ambos são aplicados no mesmo pacote – algo raro, mas possível em situações específicas; nesses casos, serão necessárias duas SAs por protocolo, além de uma para cada direção, se a comunicação for bidirecional.

Para que uma comunicação IPSec seja estabelecida, ambas as máquinas precisam ter previamente acordados alguns parâmetros, como algoritmo usado para a criptografia dos dados, função hash utilizada para a integridade e chave empregada para a codificação, além de modo de funcionamento e protocolo. Como o algoritmo que codifica os dados é do tipo simétrico, convém que a chave utilizada no processo seja trocada de tempos em tempos.

O IPSec nativamente não tem suporte para fazer nenhuma dessas operações sozinho. Para isso, ele conta com outro protocolo, chamado IKE (internet key exchange), o qual tem ainda mecanismos de autenticação e negocia outros parâmetros – por exemplo, de quanto em quanto tempo as chaves criptográficas utilizadas para a codificação dos dados serão trocadas.

Resumo

Nesta unidade, vimos quatro ferramentas que, desenvolvidas para facilitar o tráfego da informação, também podem favorecer a segurança da informação: VPN, VLAN, WLAN e IPSec.

A VPN, segundo uma de suas definições possíveis, é uma rede em que a conectividade entre múltiplos usuários (ou sites) se estabelece sobre uma infraestrutura compartilhada, mas com as mesmas políticas de acesso e segurança de uma rede privada.

A VLAN é uma ferramenta a que se recorre para diminuir o impacto do tráfego de broadcast em redes de grande porte. A VLAN para uso externo destina-se a usuários que acessam serviços internos através de meios externos. A VLAN para uso interno, a mais comum, destina-se a ambientes internos.

A WLAN é uma rede local que se vale de ondas de rádio para a transmissão de dados e para a conexão à internet, sem a necessidade de empregar cabos para conectar os dispositivos.

O IPSec, por sua vez, é uma ferramenta que provê segurança para qualquer protocolo que vá encapsulado diretamente em cima do IP, ou seja, para praticamente todos os utilizados na internet.