1.Introdução aos conceitos de segurança de rede

As redes de data centers são normalmente localizadas em uma instalação externa para armazenar dados confidenciais ou proprietários. Os data centers atuais armazenam grandes quantidades de informações confidenciais e críticas para os negócios. É fundamental garantir a segurança física para manter a sua operação. Ela protege o acesso às instalações e também protege as pessoas e equipamentos.

A **segurança fora do perímetro** pode incluir seguranças no local, cercas, portões, vigilância contínua por vídeo e alarmes de violação de segurança. Já **a segurança dentro do perímetro** pode incluir vigilância contínua por vídeo, detectores eletrônicos de movimento, traps de segurança e sensores biométricos de acesso e de saída.

A **computação em nuvem permite** que as organizações usem serviços como armazenamento de dados ou aplicativos baseados em nuvem, para estender sua capacidade ou recursos sem adicionar infraestrutura. Ela consiste em servidores físicos e virtuais que são normalmente alojados em data centers. A virtualização de servidores aproveita recursos ociosos e consolida o número de servidores necessários. No entanto, as VMs também são propensas a ataques direcionados específicos.

1.1 Hiperjacking

Um invasor pode sequestrar um hipervisor VM e usá-lo como um ponto de lançamento para atacar outros dispositivos na rede do data center.

1.2 Ativação instantânea

Quando uma VM que não foi usada por um período de tempo é colocada on-line, ela pode ter políticas de segurança desatualizadas que se desviam da segurança da linha de base e podem introduzir vulnerabilidades de segurança.

1.3 Tempestade de antivírus

Isso acontece quando todas as VMs tentam baixar arquivos de dados antivírus ao mesmo tempo.

A **proteção da infraestrutura de rede** é fundamental para a segurança geral da rede. Se um invasor obtém acesso a um roteador, a segurança e o gerenciamento de toda a rede podem ser comprometidos. A implementação do roteador de borda varia dependendo do tamanho da organização e da complexidade do projeto de rede necessário. As implementações de roteador podem incluir um único roteador que protege uma rede interna ou um roteador funcionando como a primeira linha de defesa em uma abordagem de defesa aprofundada.

2.Abordagem de roteador único

Um único roteador conecta a rede protegida ou a LAN à Internet. Todas as políticas de segurança são configuradas neste dispositivo. Isso é mais comumente implantado em

implementações de sites menores, como filiais, pequenos escritórios e escritórios domésticos (SOHO).

2.1 Abordagem de defesa em profundidade

É mais segura do que a abordagem de roteador único. Ele usa várias camadas de segurança antes do tráfego que entra na LAN protegida. Há três camadas primárias de defesa, o roteador de borda, o firewall e um roteador interno que se conecta à LAN protegida. O roteador de borda atua como a primeira linha de defesa e é conhecido como roteador de triagem. Depois de executar a filtragem de tráfego inicial, o roteador de borda passa todas as conexões que são pretendidas para a LAN interna para a segunda linha de defesa, o firewall.

O firewall normalmente pega onde o roteador de borda sai e executa filtragem adicional. Ele fornece controle de acesso adicional, rastreando o estado das conexões e atua como um dispositivo de ponto de verificação. Outras ferramentas de segurança, como IPSs, servidores Proxy e dispositivos de segurança de e-mail também podem ser implementados.

2.2 Abordagem DMZ

Inclui uma área intermediária, muitas vezes chamada de zona desmilitarizada. Pode ser usada para servidores que devem ser acessíveis a partir da Internet ou de alguma outra rede externa. A DMZ pode ser configurada entre dois roteadores, com um roteador interno conectando à rede protegida e um roteador externo que conecta à rede desprotegida. Alternativamente, a DMZ pode simplesmente ser uma porta adicional fora de um único roteador.

2.3 Segurança física

Coloque o roteador e os dispositivos físicos que conectam a ele em uma sala trancada seguran que é acessível apenas ao pessoal autorizado, livre de interferência eletrostática e magnética, tem supressão de fogo e controles de temperatura e umidade. Instale uma fonte de alimentação ininterrupta (UPS) ou gerador de energia de backup a diesel. Use fontes de alimentação redundantes em dispositivos de rede reduzindo a possibilidade de uma falha de rede de perda de energia ou equipamentos de energia com falha.

2.4 Software de sistema operacional

Equipar roteadores com a quantidade máxima de memória possível. A disponibilidade de memória pode ajudar a reduzir os riscos para a rede de alguns ataques de DoS enquanto suporta a mais ampla gama de serviços de segurança. Use a versão mais recente e estável do sistema operacional que atenda às especificações de recurso do roteador ou dispositivo de rede. Os recursos de segurança e criptografia em um sistema operacional são aprimorados e atualizados ao longo do tempo, o que torna fundamental ter a versão mais atualizada. Mantenha uma cópia segura das imagens do sistema operacional do roteador e dos arquivos de configuração do roteador como backups.

2.5 Endurecimento do roteador

Controle administrativo seguro. Certifique-se de que somente o pessoal autorizado tenha acesso e que seu nível de acesso seja controlado. Desativar portas e interfaces não utilizadas. Reduza o número de maneiras que um dispositivo pode ser acesso e desative serviços desnecessários. Semelhante a muitos computadores, um roteador tem serviços que são ativados por padrão. Alguns desses serviços são desnecessários e podem ser usados por um invasor para reunir informações sobre o roteador e a rede. Esta informação pode então ser usada em um ataque de exploração.

Várias tarefas importantes estão envolvidas na proteção do acesso administrativo a um dispositivo de infraestrutura. Restringir a acessibilidade do dispositivo, registro e conta para todos os acessos, autenticar acesso, autorizar ações, apresentar notificações legais e garantir a confidencialidade dos dados.

3.Acesso local

Todos os dispositivos de infraestrutura de rede podem ser acessados localmente. O acesso local a um roteador geralmente requer uma conexão direta a uma porta de console do roteador Cisco e usando um computador que esteja executando o software de emulação de terminal. O administrador deve ter acesso físico ao roteador e usar um cabo de console para se conectar à porta do console. O acesso local é usado tipicamente para a configuração inicial do dispositivo.

3.1 Acesso remoto

Os administradores também podem acessar dispositivos de infraestrutura remotamente, embora a opção de porta auxiliar esteja disponível, o método de acesso remoto mais comum envolve permitir conexões Telnet, SSH, HTTP/HTTPS ou SNMP ao roteador a partir de um computador. Se a conectividade de rede ao dispositivo estiver inativa, a única maneira de acessá-lo pode ser sobre linhas telefônicas.

Outras precauções devem ser tomadas ao acessar a rede remotamente. **Criptografe todo o tráfego entre o computador administrador** e o roteador. Estabelecer uma rede de gestão dedicada. A rede de gerenciamento deve incluir somente hosts de administração identificados e conexões a uma interface dedicada no roteador.

O acesso a esta rede pode ser rigorosamente controlado. Configurar um filtro de pacote de informações para permitir que somente os anfitriões de administração identificados e os protocolos preferidos alcancem o roteador. Configure e estabeleça uma conexão VPN à rede local antes de se conectar a uma interface de gerenciamento de roteador.

É importante usar senhas fortes para proteger os dispositivos de rede. Estas são as diretrizes padrão a serem seguidas:

- Use um comprimento de senha de pelo menos **oito (8) caracteres**, de preferência 10 ou mais caracteres.

- Use senhas complexas. Inclua uma combinação de **letras maiúsculas** e **minúsculas**, **números**, **símbolos** e **espaços**, se permitido.
- Evite as senhas com base em repetição, palavras comuns de dicionário, sequências de letras ou números, nomes de usuários, nomes de parentes ou de animais de estimação, informações biográficas, como datas de nascimento, números de identificação, nomes de antepassados ou outras informações facilmente identificáveis.
- Deliberadamente, soletre errado uma senha
- **Altere as senhas periodicamente**. Se uma senha for inconscientemente comprometida, a janela de oportunidade para o agente de ameaças usar a senha é limitada.
- **Não anote as senhas** e muito menos as deixe em locais óbvios, como em sua mesa ou no monitor.

4.Gerenciador de senha

Use um gerenciador de senha para proteger senhas para sua atividade on-line da Internet. Considerada a melhor prática para proteger as senhas, o gerenciador de senhas gera automaticamente senhas complexas para você e as inserirá automaticamente quando você acessar esses sites.

4.1 Autenticação multifator

Use a autenticação multifator quando disponível. Isso significa que a autenticação requer dois ou mais meios independentes de verificação.

Outra forma de abordagem para evitar exploits de malwares é para um administrador monitorar continuamente a rede e analisar os arquivos de log gerados por dispositivos de rede. As ferramentas do SOC, como SIEM e sistemas de orquestração de segurança, automação e resposta (SOAR), automatizam o processo de coleta e análise de arquivos de log. Tornou-se aceitável que o malware pode entrar na rede mesmo com a melhor segurança. Por essa razão, uma abordagem multicamada para proteção contra malware deve ser empregada.

A operação diária de uma rede consiste em padrões comuns de fluxo de tráfego, uso de largura de banda e acesso a recursos. Juntos, esses padrões identificam o comportamento normal da rede. Para determinar esse comportamento normal da rede, o monitoramento deve ser implementado. Várias ferramentas são usadas para ajudar a descobrir o comportamento normal da rede, incluindo IDS, analisadores de pacotes, SNMP, NetFlow e outros.

Um Tap de rede é normalmente um dispositivo de divisão passiva implementado em linha entre um dispositivo de interesse e a rede. Um Tap encaminha todo o tráfego, incluindo erros de camada física, para um dispositivo de análise, permitindo que o tráfego chegue ao destino pretendido.

Como a captura de dados para monitoramento de rede requer que todo o tráfego seja capturado, técnicas especiais devem ser empregadas para contornar o segmento de rede

imposta pelos switches de rede. O espelhamento de portas é uma dessas técnicas. Suportado por muitos switches corporativos, o espelhamento de portas permite que o switch copie quadros recebidos em uma ou mais portas para uma porta SPAN conectada a um dispositivo de análise.

A tabela abaixo identifica e descreve os tempos usados pelo recurso SPAN

Termo do SPAN	Descrição
Tráfego de entrada	Tráfego que entra no Switch
Tráfego de saída	Tráfego que sai do Switch
Porta de origem (SPAN)	As portas de origem são monitoradas à medida que o tráfego que as insere é replicado (espelhado para as portas de destino)
Porta de destino (SPAN)	Uma porta que espelha portas de origem. As portas SPAN de destino geralmente se conectam a dispositivos de análise, com um analisador de pacotes ou um IDS

Muitos ataques podem e, originam-se de dentro da rede. Portanto, a garantia de uma LAN interna é tão importante quanto garantir o perímetro externo da rede. Sem uma LAN segura, os usuários de uma organização ainda são suscetíveis a ameaças de rede e paralisações que podem afetar diretamente a produtividade e a margem de lucro de uma organização. Depois que um host interno é infiltrado, ele pode se tornar um ponto de partida para que um invasor obtenha acesso a dispositivos críticos do sistema, como servidores e as informações confidenciais que contêm.

Existem dois elementos LAN internos que devem ser protegidos:

5.Os Endpoints

Os **hosts** geralmente consistem em laptops, desktops, servidores e telefones IP que são suscetíveis a ataques relacionados com malware. Os endpoints também incluem câmeras de vídeo, dispositivos de ponto de venda e dispositivos na Internet das Coisas.

Os endpoints também usaram medidas de segurança tradicionais baseadas em host:

- **Software antivírus/antimalware:** É um software instalado em um host para detectar e mitigar vírus e malware. As empresas que fornecem software antivírus incluem Norton, TotalAV, McAfee, MalwareBytes e muitos outros.
- **IPS baseado em host:** É um software instalado no host local para monitorar e relatar a configuração do sistema e a atividade do aplicativo, fornecer análise de log, correlação de eventos, verificação de integridade, aplicação de política, detecção de rootkit e alertas. Os exemplos incluem Snort IPS, OSSEC e Malware Defender, entre outros.

- **Firewall baseado em host:** Este é um software instalado em um host que restringe as conexões de entrada e saída àquelas iniciadas por aquele host apenas. Alguns softwares de firewall também podem impedir que um host se infecte e impedir que hosts infectados espalhem malware para outros hosts. Incluído em alguns sistemas operacionais, como Windows, ou produzidos por empresas como NetDefender, Zonealarm, Comodo Firewall e muitos outros.

6.Infraestrutura de rede LAN

Os dispositivos de infraestrutura LAN interconectam pontos de extremidade e geralmente incluem switches, dispositivos sem fio e dispositivos de telefonia IP. A maioria desses dispositivos é suscetível a ataques relacionados à LAN, incluindo ataques de estouro de tabela de endereços MAC, ataques de falsificação, ataques relacionados a DHCP, ataques de tempestade de LAN, ataques de manipulação de STP e ataques de VLAN.

A rede evoluiu para incluir terminais tradicionais e terminais novos, leves, portáteis e consumerizados, como smartphones, tablets, wearables e outros. As novas necessidades de traga seu próprio dispositivo (BYOD) dos funcionários exigem uma maneira diferente de abordar a segurança de endpoint.

Existem alguns problemas com o método tradicional de fixação de endpoints. Em muitas redes, os dispositivos baseados em rede são diferentes e normalmente não compartilham informações entre si. Além disso, os novos dispositivos de endpoint não são bons candidatos para as soluções tradicionais de segurança de endpoint baseadas em host devido à variedade de dispositivos e à variedade de sistemas operacionais disponíveis nesses dispositivos.

Organizações maiores agora exigem **proteção antes**, **durante** e **após um ataque**. Os administradores de TI devem ser capazes de responder às seguintes perguntas:

- De onde veio o ataque ?
- Qual foi o método de exploração e ponto de entrada ?
- Quais sistemas foram afetados ?
- O que a façanha fez ?
- Como nos recuperamos da exploração ?
- Como podemos mitigar a vulnerabilidade e a causa raiz ?

As **novas arquiteturas de segurança** para a rede sem fronteiras enfrentam os desafios de segurança fazendo com que os endpoints usem elementos de varredura de rede. Esses dispositivos fornecem muito mais camadas de varredura do que um único ponto de extremidade possivelmente poderia. Dispositivos de prevenção de malware baseados em rede também são capazes de compartilhar informações entre si para tomar decisões melhor informadas.

Alguns exemplos destes dispositivos são:

- **Proteção avançada contra malware (AMP):** Isso fornece proteção de endpoint contra vírus e malware.
- **E-mail security Appliance (ESA):** Isso fornece filtragem de SPAM e e-mails potencialmente mal-intencionados antes que eles cheguem ao endpoint. Um exemplo é o Cisco ESA.
- **Web Security Appliance (WSA):** Fornece filtragem e bloqueio de sites para evitar que os hosts cheguem a locais perigosos na web. O Cisco WSA fornece controle sobre como os usuários acessam a Internet e pode impor políticas de uso aceitáveis, controlar o acesso a sites e serviços específicos e verificar se há malware.
- **Controle de admissão de rede (NAC):** Isso permite que somente sistemas autorizados e compatíveis se conectem à rede.

A **finalidade do controle de acesso à rede (NAC)** é permitir que somente sistemas autorizados e complacentes, gerenciados ou não gerenciados, alcançam a rede. Ele unifica tecnologias de segurança de endpoint com autenticação de usuário ou dispositivo e aplicação de políticas de segurança de rede. Um sistema NAC pode negar o acesso de rede aos dispositivos *noncompliant*, colocá-los em uma área quarentena, ou dar-lhes somente acesso restrito aos recursos de computação, impedindo assim que nós inseguros de infectar a rede.

Os sistemas NAC podem ter as seguintes capacidades:

- **Criação de perfil e visibilidade:** Reconhece e cria perfis de usuários e seus dispositivos antes que códigos maliciosos possam causar danos.
- **Acesso à rede de convidados:** Gerencia os convidados por meio de um portal de autoatendimento personalizável que inclui registro de convidados, autenticação de convidados, patrocínio de convidados e um portal de gerenciamento de convidados.
- **Verificação da postura de segurança:** Avalia a conformidade da política de segurança por tipo de usuário, tipo de dispositivo e sistema operacional.
- **Resposta a incidentes:** Atenuar as ameaças à rede ao aplicar políticas de segurança que bloqueiam, isolam e reparam máquinas incompatíveis sem a atenção do administrador.

O **padrão IEEE 802.1X** define um controle de acesso baseado em portas e o protocolo de autenticação que restringe os locais de trabalho não autorizados de se conectarem a uma LAN por meio de portas de switch que podem se acessadas publicamente

As funções 802.1x incluem:

- **Suplicante:** O dispositivo (workstation) que solicita acesso a LAN e Switch Services e responde a solicitações do computador. A estação de trabalho deve estar executando o software cliente compatível com 802.1x.
- **Autenticador (switch):** Este dispositivo controla o acesso físico à rede com base no status de autenticação do cliente. O switch atua como intermediário (proxy) entre o cliente (suplicante) e o servidor de autenticação, solicitando informações de identificação do cliente, verificando essas informações com o servidor de autenticação

e retransmitindo uma resposta ao cliente. O switch usa um agente de software RADIUS, responsável pelo encapsulamento e desencapsulamento dos quadros de EAP (Extensible Authentication Protocol), bem como a interação com o servidor de autenticação.

- **Servidor de autenticação:** Este servidor realiza a autenticação real do cliente. O servidor de autenticação valida a identidade do cliente e notifica o switch se o cliente está autorizado a acessar os serviços de LAN e de switch. Como o switch atua como proxy, o serviço de autenticação é transparente ao cliente. O sistema de segurança RADIUS com extensões de EAP é o único servidor de autenticação compatível.

Até que a estação de trabalho seja autenticada, o controle de acesso 802.1x permite apenas o protocolo de autenticação extensível sobre a LAN (EAPOL), o CDP (Cisco Discovery Protocol (CDP) e o tráfego de Protocolo de Árvore (STP) através da porta à qual a estação de trabalho está conectada. Após a autenticação ser bem-sucedida, o tráfego normal pode passar pela porta.

O estado da porta do switch determina se o cliente tem acesso concedido à rede. Quando configurado para autenticação baseada em porta 802.1X, a porta começa no estado não autorizado. Quando neste estado, a porta não permite todo o tráfego de ingresso e saída, exceto os pacotes do protocolo 802.1X, STP e CDP.

Quando um cliente é autenticado com sucesso, as transições de porta para o estado autorizado, permitindo que todo o tráfego para o cliente flua normalmente. Se o switch solicitar a identidade do cliente (iniciação do autenticador) e o cliente não suporta 802.1X, a porta permanece no estado não autorizado, e o cliente não é concedido acesso à rede.

Em contraste, quando um cliente 802.1X-habilitado conecta a uma porta e o cliente inicia o processo de autenticação (iniciação do suplicante) enviando o quadro EAPOL-início a um interruptor que não esteja executando o protocolo 802.1X, nenhuma resposta é recebida, e o cliente começa a enviar quadros como se a porta está no estado autorizado.

As organizações devem fornecer suporte para proteger os dados conforme eles trafegam pelos links. Isso pode incluir tráfego interno, mas é ainda mais importante proteger os dados que viajam para fora da organização para sites de filiais, sites de telecomutador e sites de parceiros.

Abaixo, estão os quatro elementos das comunicações seguras.

- **Integridade dos dados:** Garante que a mensagem não foi alterada. Quaisquer alterações nos dados em trânsito serão detectadas. A integridade é garantida pela implementação de um dos algoritmos Secure Hash.
- **Autenticação da origem:** Garante que a mensagem não é uma falsificação e realmente vem de quem afirma. Muitas redes modernas garantem autenticação com algoritmos como código de autenticação de mensagem baseado em hash (HMAC).

- **Confidencialidade dos dados:** Garante que apenas usuários autorizados possam ler a mensagem. Se a mensagem for interceptada, ela não poderá ser decifrada dentro de um razoável período de tempo. A confidencialidade dos dados é implementada usando algoritmos de criptografia simétrica e assimétrica.
- **Dados não repudiáveis:** Garante que o remetente não possa repudiar ou refutar a validade de uma mensagem enviada. O não repúdio depende do fato de que apenas o remetente possui as características ou a assinatura exclusivas de como essa mensagem é tratada.

Os dois principais protocolos IPSec são o protocolo de s**egurança de autenticação (AH)** e **segurança de encapsulamento (ESP)**. O protocolo IPsec é o primeiro bloco de construção da estrutura. A escolha de AH ou ESP estabelece quais outros blocos de construção estão disponíveis.

AH usa o Protocolo IP 51 e é apropriado apenas quando a confidencialidade não é necessária ou permitida. Ele fornece autenticação e integridade de dados, mas não fornece confidencialidade de dados (criptografia). Todo o texto é transportado sem criptografia.

ESP usa o protocolo IP 50 e fornece confidencialidade e autenticação. Ele fornece confidencialidade executando a criptografia no pacote IP. O ESP fornece autenticação para o pacote IP interno e o cabeçalho ESP. A autenticação fornece autenticação de origem de dados e integridade de dados.

AH atinge a autenticidade aplicando uma função de hash unidirecional de um pacote para criar um hash ou digestão de mensagens. O hash é combinado com o texto e é transmitido em texto simples.

O receptor detecta alterações em qualquer parte do pacote que ocorre durante o trânsito executando a mesma função de hash unidirecional no pacote recebido e comparando o resultado para o valor da mensagem digere que o remetente forneceu.

A função AH é aplicada a todo o pacote, exceto para quaisquer campos de cabeçalho IP que normalmente mudam em trânsito. Os campos que normalmente mudam durante o trânsito são chamados de campos mutáveis.

O processo AH ocorre nesta ordem:
- O cabeçalho IP e a carga útil dos dados são hashed usando a chave secreta compartilhada
- O hash constrói um novo cabeçalho AH, que é inserido no pacote original
- O novo pacote é transmitido para o roteador de peer IPsec
- O roteador de pares hashes, o cabeçalho IP e a carga útil de dados usando a chave secreta compartilhada, extrai o hash transmitido do cabeçalho AH e compara os dois hashes

Os hashes devem corresponder exatamente. Se um bit for alterado no pacote transmitido, a saída do hash nas alterações do pacote recebido e o cabeçalho AH não corresponderá. AH suporta algoritmos MD5 e SHA. AH pode não funcionar se o ambiente usa NAT.

Se o ESP for selecionado como o protocolo IPSec, um algoritmo de criptografia também deve ser selecionado.

O ESP também pode fornecer integridade e autenticação. Primeiro, a carga útil é criptografada. Em seguida, a carga útil criptografada é enviada através de um algoritmo HASH, como SHA-256 ou superior. O HASH fornece autenticação e integridade de dados para a carga útil dos dados. Note que o MD5 e o SHA-1 devem ser evitados.

Opcionalmente, o ESP também pode impor a proteção anti-replay. A proteção anti-replay verifica se cada pacote é único e não é duplicado. Essa proteção garante que um hacker não possa interceptar pacotes e inserir pacotes alterados no fluxo de dados. Anti-Replay funciona, mantendo a faixa dos números de sequência de pacotes e usando uma janela deslizante na extremidade de destino.

Quando a autenticação e a criptografia são selecionadas, a criptografia é executada primeiro. Uma razão para essa ordem de processamento é que ela facilita a detecção rápida e a rejeição de pacotes repetidos ou falsos pelo dispositivo de recebimento. Antes de descriptografar o pacote, o receptor pode autenticar pacotes de entrada. Ao fazer isso, pode detectar rapidamente problemas e potencialmente reduzir o impacto dos ataques dos DOS. Para reiterar, o ESP fornece confidencialidade com a criptografia e fornece integridade com a autenticação.

ESP e AH podem ser aplicados a pacotes IP em dois modos diferentes, modo de transporte e modo de túnel.

6.1 Modo de transporte

No modo de transporte, a segurança é fornecida apenas para a camada de transporte do modelo OSI e acima. O modo de transporte protege a carga útil do pacote, mas deixa o endereço IP original em texto simples. O endereço IP original é usado para encaminhar o pacote através da Internet. O modo de transporte ESP é usado entre os hosts.

6.2 Modo de túnel

O modo de túnel fornece segurança para o pacote IP original completo. O pacote IP original é criptografado e, em seguida, é encapsulado em outro pacote IP. Isso é conhecido como criptografia IP-IN-IP. O endereço IP no pacote IP externo é usado para encaminhar o pacote através da Internet.

O modo de túnel ESP é usado entre um host e um gateway de segurança, ou entre dois gateways de segurança. Para aplicativos host-to-gateway, um escritório em casa pode não ter um roteador para realizar o encapsulamento e a criptografia IPsec. Nesse caso, um cliente IPsec em execução no PC executa o encapsulamento e a criptografia IPsec IP-IN-IP. Para aplicativos de gateway-to-gateway, em vez de carregar o IPSec em todos os computadores nos escritórios remotos e corporativos, é mais fácil ter os gateways de segurança executar a criptografia e encapsulamento IP-IN-IP. No escritório corporativo, o roteador de-encapsula e descriptografa o pacote.

O **protocolo da Internet Key Exchange (IKE)** é um padrão de protocolo de gerenciamento de chaves. IKE é usado em conjunto com o padrão IPsec. IKE aprimora o IPsec adicionando recursos e simplifica a configuração do padrão IPsec. Sem IKE no lugar, a configuração do IPsec seria um processo complexo de configuração manual que não iria dimensionar bem.

O IKE é um protocolo híbrido que implementa protocolos de câmbio dentro da estrutura Isakmp Protocol (Isakmp) da Internet Association Security Association. ISAKMP define o formato da mensagem, a mecânica de um protocolo de troca de chaves e o processo de negociação para construir um SA para IPsec.

Em vez de transmitir chaves diretamente em uma rede, **o IKE calcula chaves compartilhadas** com base na troca de uma série de pacotes de dados. Isso desativa que um terceiro descriptografe as chaves, mesmo que o terceiro tenha capturado todos os dados trocados que foram usados para calcular as chaves.

IKE usa ISAKMP para a Fase 1 e a Fase 2 da Negociação Chave. A fase 1 negocia uma associação de segurança (uma chave) entre dois pares IKE. A chave negociada na Fase 1 permite que os pares Ike se comuniquem firmemente na fase 2. Durante a negociação da Fase 2, o IKE estabelece chaves (associações de segurança) para outras aplicações, como o IPsec.

Na fase 1, dois pares IPsec realizam a negociação inicial do SAS. O objetivo básico da fase 1 é negociar a política ISAKMP, autenticar os pares e configurar um túnel seguro entre os pares. Este túnel será então usado na fase 2 para negociar a política IPsec.

A fase 1 pode ser implementada no modo principal ou no modo agressivo. Quando o modo principal é usado, as identidades dos dois pares IKE estão ocultos. O modo agressivo leva menos tempo do que o modo principal para negociar chaves entre os pares. No entanto, uma vez que o hash de autenticação é enviado não criptografado antes que o túnel seja estabelecido, o modo agressivo é vulnerável a ataques de força bruta.

O objetivo do IKE Fase 2 é negociar os parâmetros de segurança IPsec que serão usados para proteger o túnel IPsec. O IKE Fase 2 é chamado de modo rápido e só pode ocorrer após o IKE estabeleceu um túnel seguro na fase 1. A SAS é negociada pelo processo IKE ISAKMP em nome do IPSec, que precisa de chaves de criptografia para a operação. O Modo

Rápido negocia a fase 2 SAS da IKE. Nesta fase, o SAS que o IPsec usa são unidirecionais, portanto, uma troca de chaves separada é necessária para cada fluxo de dados.