1.2

Ativos - qualquer coisa de valor para uma organização que deva ser protegida, incluindo servidores, dispositivos de infraestrutura, dispositivos finais e o maior ativo, dados.

Há quatro etapas para identificação e classificação de ativos: 1. Determinar uma categoria de identificação de ativos adequada. Estabeleça a responsabilização, identificando o proprietário de todos os ativos de informações e de softwares de aplicativos. Determinar os critérios de classificação. e 4 Implemente um esquema de classificação.

Vulnerabilidades - Uma fraqueza em um sistema ou em seu design que pode ser explorada por um agente ameaçador.

Ameaças - Qualquer perigo potencial para um ativo.

O gerenciamento de ativos consiste em inventários de todos os ativos e, em seguida, desenvolver e implementar políticas e procedimentos para cobri-los.

Ciclos de um ativo

Aquisição

Implementação

Utilização

Manutenção

Eliminação

Defesas em profundidade

Uma analogia comumente usada para descrever uma abordagem de defesa em profundidade é chamada de “cebola de segurança”. Como ilustrado na figura, um ator de ameaça teria que descascar as defesas de uma rede camada por camada de uma maneira semelhante a descascar uma cebola. Só depois de penetrar cada camada, o ator da ameaça alcançaria os dados ou o sistema de destino.

O cenário em mudança da rede, como a evolução das redes sem fronteiras, mudou essa analogia para a “alcachofra de segurança”, que beneficia o ator de ameaça.

Conforme ilustrado na figura, os atores da ameaça não precisam mais descascar cada camada. Eles só precisam remover certas “folhas de alcachofra”. O bônus é que cada “folha” da rede pode revelar dados eventuais que não estejam bem protegidos.

Por exemplo, é mais fácil para um agente ameaçador comprometer um dispositivo móvel do que comprometer um computador ou servidor interno protegido por camadas de defesa. Cada dispositivo móvel é uma folha. E folha após folha, tudo leva o hacker a mais dados. O coração da alcachofra é onde os dados mais convenientes são encontrados. Cada folha fornece uma camada de proteção enquanto fornece simultaneamente um caminho para o ataque.

Nem todas as folhas precisam ser removidas para chegar ao coração da alcachofra. O hacker arrancou uma armadura de segurança ao longo do perímetro para chegar à “coração” da empresa.

estratégia de defesa

Sobreposição

Para garantir que as informações e os dados permaneçam disponíveis, uma empresa precisa criar diferentes camadas de proteção. Um bom exemplo de camadas é uma empresa que armazena seus documentos ultra-secretos em um servidor protegido por senha em um prédio trancado e cercado por uma cerca elétrica.

Uma abordagem em camadas oferece a proteção mais abrangente porque, mesmo que os crimes cibernéticos penetrem em uma camada, eles ainda precisam enfrentar várias outras defesas. Idealmente, cada camada deve ser mais complicada de superar!

A defesa em profundidade não fornecerá um escudo cibernético impenetrável, mas ajudará a empresa a minimizar riscos, mantendo-se um passo à frente das violações virtuais.

[17:23, 19/03/2025] Eduardo: Limitação

Limitar o acesso aos dados e às informações reduz a possibilidade de uma ameaça. Uma empresa deve restringir o acesso para que os usuários tenham apenas o nível de acesso necessário para fazer o seu trabalho.

Uma empresa deve ter ferramentas e configurações certas, como permissões de arquivo, para limitar o acesso, bem como medidas processuais certas, que definem etapas específicas para fazer qualquer coisa que possa afetar a segurança. Por exemplo, um procedimento de restrições que exige que os funcionários sempre consultem documentos provisórios em uma sala com CCTV garante que eles nunca removam esses documentos das instalações.

[17:23, 19/03/2025] Eduardo: Diversidade

Se todas as camadas protegidas fossem as mesmas, não seria muito difícil, para os crimes virtuais, realizar um ataque bem-sucedido. As camadas devem ser diferentes para que, se uma camada for penetrada, a mesma técnica não funcione em todas as outras, o que comprometeria todo o sistema. Uma empresa pode usar diferentes algoritmos de criptografia ou sistemas de autenticação para proteger os dados em diferentes estados.

Para atingir o objetivo de diversidade nas defesas, as empresas podem usar produtos de segurança de diferentes empresas como diferentes fatores de autenticação, como um cartão de furto de uma empresa e um leitor de impressão digital fabricado por uma empresa diferente, bem como medidas de segurança variadas, como bloqueios de tempo nos armários e supervisão por um membro da equipe de segurança ao desbloqueá-lo.

[17:24, 19/03/2025] Eduardo: Ofuscação

A ofuscação de informações também pode proteger dados e informações. Uma empresa não deve revelar informações que as infrações virtuais podem usar para descobrir a versão do sistema operacional em execução em um servidor ou o tipo de equipamento que ele usa.

Por exemplo, as mensagens de erro não devem conter nenhum detalhe que os crimes virtuais possam usar para determinar as vulnerabilidades que estão presentes. Ocultar certos tipos de informação dificulta ataques de crimes virtuais a um sistema.

[17:24, 19/03/2025] Eduardo: Simplicidade

A complexidade não garante, necessariamente, a segurança. Se uma empresa implementa sistemas complexos que são difíceis de entender e solucionar problemas, o “tiro pode sair pela culatra”. Se os funcionários não entendem como configurar uma solução complexa corretamente, pode ser tão fácil quando em uma solução mais simples para os crimes virtuais comprometerem esses sistemas.

Para manter a disponibilidade, uma solução de segurança deve ser simples, do ponto de vista de dentro da empresa, mas complexa do ponto de vista externo.

[17:32, 19/03/2025] Eduardo: 1.2

O gerenciamento de configuração refere-se à identificação, controle e auditoria de melhorias e de quaisquer alterações feitas na linha de base exigidas de um sistema.

A configuração da linha de base inclui todas as definições definidas para um sistema que fornece uma base para todos os sistemas semelhantes, como um tipo de modelo.

[17:33, 19/03/2025] Eduardo: Um log registra todos os eventos que ocorrem. As entradas de log contêm um arquivo de log e uma entrada de log contém todas as informações relacionadas a um evento específico. Registros precisos e completos são muito importantes na segurança digital.

[17:33, 19/03/2025] Eduardo: O gerenciamento de dados do log de segurança do computador deve determinar os procedimentos para o seguinte:

Gerando arquivos de log

Transmissão de arquivos de log

Armazenamento de arquivos de log

Análise de dados

Baixando dados de log

[17:37, 19/03/2025] Eduardo: O analisador de pacotes captura cada pacote, mostra os valores de vários campos no pacote e analisa o conteúdo. Um sniffer pode capturar o tráfego em redes com e sem fio.

Os analisadores de pacotes executam as seguintes funções:

Log de tráfego

Análise de problemas de rede

Detecção de uso indevido da rede

Detecção de tentativa de invasão da rede

Isolamento do sistema explorado

[17:38, 19/03/2025] Eduardo: Logs do sistema operacional

O sistema operacional registra eventos de registro que estão vinculados às ações relacionadas ao sistema operacional. Os eventos do sistema incluem o seguinte:

Solicitações de cliente e respostas do servidor, como autenticações de usuário bem-sucedidas

Informações de uso que contêm o número e o tamanho das transações em um determinado período de tempo

[17:38, 19/03/2025] Eduardo: Segurança de aplicações

As empresas utilizam software de segurança pela rede ou pelo sistema para detectar atividades mal-intencionadas.

Esse software gera um log de segurança para fornecer dados de segurança do computador. Os logs são úteis para a realização de análise de auditorias e para a identificação de tendências e de problemas no longo prazo. Os registros também permitem que uma empresa forneça documentação que mostre que está em conformidade com as leis e os requisitos regulamentares.

1.3

Politica de Identificação e Autenticação

Especifica pessoas autorizadas que podem ter acesso a recursos de rede e procedimentos de verificação de identidade.

Politicas de senha

Garante que as senhas atendam aos requisitos minimos e sejam alteradas regularmente.

Politica de Uso Aceitável (AUP)

Identifica os aplicativos e usos de rede que são aceitáveis para a organização. Também podem identificar as consequências, se esta politica for violada.

Politica de Acesso Remoto

Identifica como os usuários remotos podem acessar uma rede e o que é acessivel por meio de conectividade remota.

Politicas de Manutenção de Rede

Especifica procedimentos de atualização de sistemas operacionais dos dispositivos de rede e de aplicativos de usuário final.

Procedimentos de tratamento de incidentes

Descreve como os incidentes de segurança são tratados.

1.3.1

Uma política de segurança BYOD deve ser desenvolvida para realizar o seguinte:

Especifique os objetivos do programa BYOD.

Identifique quais funcionários podem trazer seus próprios dispositivos.

Identifique quais dispositivos serão suportados.

Identificar o nível de acesso que os funcionários são concedidos ao usar dispositivos pessoais.

Descrever os direitos de acesso e as atividades permitidas ao pessoal de segurança no dispositivo.

Identifique quais regulamentos devem ser cumpridos ao usar dispositivos de funcionários.

Identifique as salvaguardas a serem implementadas se um dispositivo for comprometido.

A tabela lista as práticas recomendadas de segurança BYOD para ajudar a mitigar vulnerabilidades BYOD.

Acesso protegido por senha

Use senhas exclusivas para cada dispositivo e conta.

Controle manualmente a conectividade sem fio

Desative a conectividade Wi-Fi e Bluetooth quando não estiver em uso. Conecte-se apenas a redes confiáveis.

Mantenha-se atualizado

Mantenha sempre o sistema operacional do dispositivo e outros softwares atualizados. O software atualizado geralmente contém patches de segurança para mitigar contra as ameaças ou explorações mais recentes.

Dados de backup

Ative o backup do dispositivo caso ele seja perdido ou roubado.

Ativar "Localizar meu dispositivo"

Assine um serviço de localizador de dispositivos com o recurso de apagamento remoto.

Fornece software antivirus

Fornecer software antivirus para dispositivos BYOD aprovados.

Use um software gerenciamento de dispositivos móveis (MDM)

O software MDM permite que as equipes de Ti implementem configurações de segurança e configurações de software em todos os dispositivos que se conectam às redes da empresa.

2.1

**Cercas e barreiras físicas**

**Barreiras físicas**

**As barreiras físicas podem ter os seguintes componentes:**

**Sistema de cerca de perímetro**

**Sistema de portão de segurança**

**Cabeços de amarração (postes curtos usados para impedir invasões em veículos)**

**Barreiras de entrada de veículo**

**Abrigos de proteção**

**Cercamento**

**Barreiras físicas**

**As barreiras físicas podem ter os seguintes componentes:**

**Sistema de cerca de perímetro**

**Sistema de portão de segurança**

**Cabeços de amarração (postes curtos usados para impedir invasões em veículos)**

**Barreiras de entrada de veículo**

**Abrigos de proteção**

**Cercamento**

Sistemas de autenticação de biometria incluem medições da face, impressão digital, geometria da mão, íris, retina, assinatura e voz.

Ao selecionar sistemas biométricos, há vários fatores importantes a serem considerados, incluindo:

* Precisão
* taxa de transferência
* Aceitação para usuários
* Exclusividade do órgão biométrico e ação
* Resistência à falsificação
* Confiabilidade
* Requisitos de armazenamento de dados
* Tempo de inscrição
* Intrusão na verificação

O mais importante desses fatores é a precisão, que é expressa em tipos de erro e taxas.

A primeira taxa de erro é erros de tipo I ou rejeições falsas. Um erro de tipo I rejeita uma pessoa que se registra e é um usuário autorizado. No controle de acesso, em que o objetivo principal é afastar os criminosos digitais, a falsa rejeição é o erro menos importante. Isso significa que alguém que deve obter acesso não tem acesso.

Aceitação falsa é um erro Tipo II. Os erros de tipo II permitem a entrada de pessoas que não deveriam ter acesso, o que significa que um criminoso digital pode obter acesso. Erros de tipo II permitem a entrada de invasores e, portanto, são considerados o erro mais importante em um sistema de controle de acesso de biometria.

A taxa de aceitação também é um conceito importante aqui. A taxa de aceitação é indicada como uma percentagem e é a taxa na qual um sistema aceita indivíduos que cancelaram a inscrição ou impostores como usuários autênticos.

**2.1.5 Vigilância**

Guardas e escoltas

Vigilância eletrônica e por vídeo

Vigilância sem fio e RFID - RFID (Radio Frequency Identification, Identificação por radiofrequência)

**2.2.2 Desenvolvimento de Aplicativos**

Desenvolvimento e teste

O software é desenvolvido e atualizado em um ambiente de desenvolvimento, onde pode ser desenvolvido, testado e depurado antes de ser implantado. Um ambiente de desenvolvimento é menos restritivo do que o ambiente ativo e tem um nível de segurança mais baixo. O software de controle de versão ajuda a rastrear e gerenciar alterações no código do software. Os desenvolvedores também podem trabalhar em um ambiente de sandbox para que o código não seja substituído à medida que o desenvolve.

Durante o teste, os desenvolvedores analisam como o código interage com o ambiente normal. A garantia de qualidade (QA) pode encontrar falhas no software. É muito mais fácil corrigir qualquer defeito encontrado nessa fase.

Preparo e produção

Os ambientes de preparação devem corresponder ao ambiente de produção da empresa.

Ao testar em um ambiente intermediário, os desenvolvedores podem verificar se o software é executado sob as configurações de segurança necessárias. Depois que o desenvolvedor executa e testa a segurança, o programa pode ser implantado em produção.

Provisionamento e desprovisionamento

Provisionamento é a criação ou atualização de software. O desprovisionamento é sua remoção.

Uma empresa pode usar um portal de autoatendimento para automatizar o desprovisionamento e o provisionamento de software.

normalização

A normalização é usada para organizar dados em um banco de dados e ajudar a manter a integridade dos dados. A normalização converte uma sequência de entrada em sua forma mais simples conhecida para garantir que todas as sequências tenham representações binárias exclusivas e que qualquer entrada mal-intencionada seja identificada.

 procedimento armazenado

Um procedimento armazenado é um grupo de instruções SQL pré-compiladas armazenadas em um banco de dados que executa uma tarefa. Se você usar um procedimento armazenado para aceitar parâmetros de entrada de clientes que usam dados de entrada diferentes, reduzirá o tráfego de rede e obterá resultados mais rápidos.

ofuscação e a camuflagem

Um desenvolvedor pode usar a ofuscação e a camuflagem para impedir que o software seja reprojetado. A ofuscação oculta dados originais com caracteres ou dados aleatórios. A camuflagem substitui os dados confidenciais por dados fictícios realistas.

reutilização de código

A reutilização de código significa usar o software atual para criar um novo software, economizando tempo e custos de desenvolvimento. É preciso ter cuidado, no entanto, para evitar a introdução de vulnerabilidades.

Kits de desenvolvimento de software e bibliotecas de terceiros (SDKs)

Kits de desenvolvimento de software e bibliotecas de terceiros (SDKs) fornecem um repositório de códigos úteis para tornar o desenvolvimento de aplicativos mais rápido e mais barato. A desvantagem é que qualquer vulnerabilidade em SDKs ou bibliotecas de terceiros pode afetar muitos aplicativos.

2.2.6 Regras de Validação

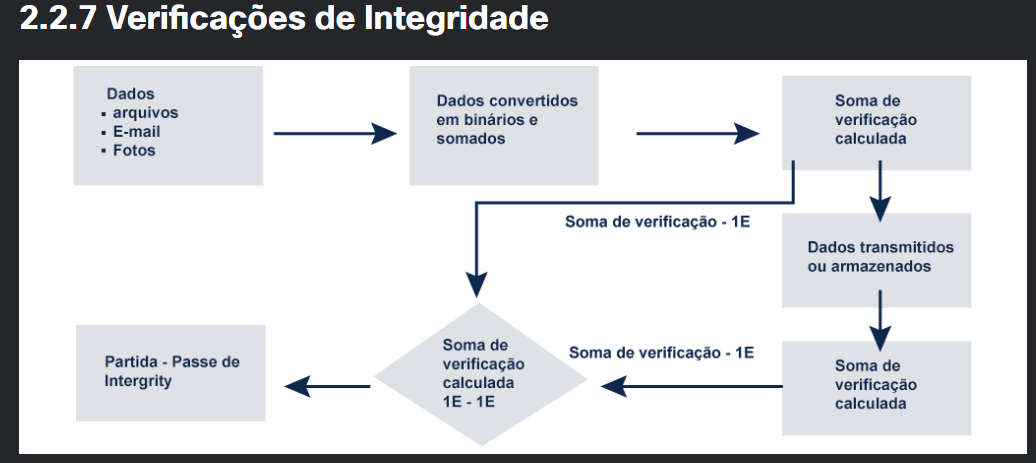
Uma regra de validação verifica se os dados estão nos parâmetros definidos pelo projetista de banco de dados. Uma regra de validação ajuda a garantir a integridade, a precisão e a consistência dos dados. Os critérios usados na regra de validação incluem o seguinte:

* Tamanho – verifica o número de caracteres em um item de dados
* Formato – verifica se os dados estão de acordo com um formato especificado
* Consistência – verifica a consistência dos códigos nos itens de dados relacionados
* Intervalo – verifica se os dados estão dentro de valores mínimo e máximo
* Dígito de verificação – efetua um cálculo extra para gerar um dígito de verificação para detecção de erros

**dígito de verificação.**

**Multiplique o primeiro dígito do ISBN por 10, o segundo dígito por 9,...o nono dígito por 2. Somar todos os números.**

**O dígito de verificação é o número necessário para obter o total a ser adicionado a um múltiplo de 11.**



 A verificação de integridade executa uma **função hash** para obter um instantâneo de dados e, em seguida, usa esse instantâneo para garantir que os dados permaneçam inalterados. Um **checksum** é um exemplo de uma função hash.

Como funciona um checksum

Uma checksum verifica a integridade de arquivos, ou de strings de caracteres, antes e depois de serem transferidos de um dispositivo para outro por uma rede local ou pela Internet. As checksum simplesmente convertem cada conjunto de informações para um valor e soma o total. Para testar a integridade de dados, um sistema de recebimento apenas repete o processo. Se as duas somas forem iguais, os dados são válidos. Caso contrário, uma alteração ocorreu em algum lugar ao longo do caminho.

Funções hash

Funções hash comuns incluem MD5, SHA-1, SHA-256 e SHA-512. Eles usam algoritmos matemáticos complexos para comparar dados com um valor de hash. Por exemplo, depois de baixar um arquivo, o usuário pode verificar a integridade do arquivo, comparando os valores de hash da fonte com o valor gerado por qualquer calculadora de hash.

Controle de versão

As empresas usam controle de versão para evitar alterações acidentais por usuários autorizados. O controle de versão significa que dois usuários não podem atualizar o mesmo objeto, como um arquivo, registro de banco de dados ou transação, ao mesmo tempo. Por exemplo, o primeiro usuário a abrir um documento tem a permissão para alterar esse documento. A segunda pessoa tem uma versão somente leitura.

Backups

Backups precisos ajudam a manter a integridade de dados, se os dados forem corrompidos. Uma empresa precisa verificar o seu processo para garantir a integridade do backup, antes que ocorra perda de dados.

Autorização

A autorização determina quem tem acesso aos recursos da empresa, de acordo com a necessidade de cada um. Por exemplo, controles de acesso de usuário e permissões de arquivo garantem que apenas determinados usuários possam modificar os dados. Um administrador pode definir as permissões de um arquivo como somente leitura. Como resultado, um usuário que acessa esse arquivo não pode fazer nenhuma alteração.

**2.2.8 Outras práticas de segurança de aplicativos**

Assinatura de código

A assinatura de código ajuda a provar que um software é autêntico.

Os executáveis projetados para instalar e executar em um dispositivo são assinados digitalmente para validar a identidade do autor e fornecer garantia de que o código de software não foi alterado desde que foi assinado.

Cookies seguros

O uso de cookies seguros protege as informações armazenadas em cookies contra hackers.

Quando o sistema do cliente interage com um servidor, o servidor envia uma resposta HTTP que instrui o navegador a criar pelo menos um cookie. O cookie armazena dados para solicitações futuras enquanto você estiver navegando no site.

Os desenvolvedores da Web devem usar cookies com HTTPS para proteger os cookies e impedir que eles sejam transmitidos por HTTP não criptografado.

**2.2.10 Controle de ameaças a aplicativos**

Acesso não autorizado a data centers, salas de computador e armário de cabos

 Período de inatividade do sistema

* Desenvolver um plano de continuidade de negócios para aplicativos essenciais para manter a disponibilidade das operações.
* Desenvolver um plano de recuperação de desastres para aplicativos e dados essenciais.

Vulnerabilidade de software do sistema operacional de rede

* Desenvolver uma política para lidar com atualizações de software de aplicativo e do sistema operacional.
* Instale correções e atualizações regularmente.

Acesso não autorizado a sistemas

* Use a autenticação multifatorial.
* Monitorar arquivos de log

Perda de dados

* Implementar padrões de classificação de dados.
* Implementar procedimentos de backup.

Vulnerabilidades de desenvolvimento de software

* Realizar testes antes do lançamento do software.

**2.3.2 Serviços de rede e de roteamento**

Para verificar os serviços de rede não protegidos, verifique se um dispositivo tem portas abertas usando um scanner de porta. Um scanner de porta envia uma mensagem para cada porta e espera por uma resposta, indicando como a porta é usada e se está aberta.

Protocolo de Configuração Dinâmica de Host (DHCP)

O DHCP usa um servidor para atribuir um endereço IP e outras informações de configuração automaticamente aos dispositivos de rede. Na realidade, o dispositivo está obtendo uma permissão do servidor DHCP para usar a rede. Os invasores podem direcionar servidores DHCP para negar o acesso a dispositivos na rede, mas medidas de segurança como rastreamento de DHCP impedem que servidores DHCP invasores forneçam endereços IP para clientes ao validar mensagens de fontes que não são confiáveis.

A Figura 1 fornece uma lista de verificação de segurança para DHCP:

* Proteja fisicamente o servidor DHCP.
* Aplique as correções de software.
* Localize o servidor DHCP atrás de um firewall.
* Monitore a atividade do DHCP analisando os registros do DHCP.
* Mantenha uma solução antivírus forte.
* Desinstale qualquer serviço e aplicação não utilizado.
* Feche as portas não utilizadas.

Domain Name System (DNS)

O DNS converte um URL ou endereço de site, como www.cisco.com, em um endereço IP numérico. Quando os usuários digitam um endereço da Web na barra de endereços, o servidor DNS reconhece o endereço IP. Os invasores podem direcionar os servidores DNS para negar o acesso aos recursos da rede ou redirecionar o tráfego para sites falsos. Use serviço e autenticação seguros entre servidores DNS para protegê-los contra esses ataques.

As DNS Security Extensions (DNSSEC) usam assinaturas digitais para fortalecer a autenticação e proteger contra ameaças ao DNS.

Uma checklist de segurança para DNS:

* Manter softwares DNS atualizados.
* Impeça que a string de versão revele informações.
* Separe os servidores DNS internos e externos.
* Restrinja as transações permitidas pelo endereço IP do cliente.
* Use assinaturas de transação para autenticar transações.
* Desative ou restrinja as transferências de zona e as atualizações dinâmicas o máximo possível.
* Habilitar o log e analisar logs.
* Use Domain Name System Security Extensions (DNSSEC).
* Assine zonas.
* Protocolo de mensagens de controle da Internet (ICMP)
* Dispositivos de rede usam ICMP para enviar mensagens de erro como quando um serviço solicitado não está disponível ou se o host não pode acessar o roteador.
* O comando ping é um utilitário de rede que usa o ICMP para testar a acessibilidade de um host em uma rede. O ping envia mensagens ICMP para o host e aguarda uma resposta. Os criminosos digitais podem alterar o uso do ICMP para executar ataques de canal secreto e reconhecimento, negação de serviço (DoS). Muitas redes filtram solicitações de ICMP para evitar esses ataques.
* Routing Information Protocol (RIP)
* O RIP limita o número de saltos permitidos em um caminho em uma rede do dispositivo de origem para o destino. O número máximo de saltos permitidos para o RIP é 15. O RIP é um protocolo de roteamento usado para trocar informações de roteamento sobre quais redes cada roteador pode acessar e a que distância estão essas redes.
* O RIP calcula a melhor rota com base na contagem de saltos, mas os criminosos digitais também podem direcionar roteadores e o protocolo RIP. Esses ataques a serviços de roteamento podem afetar o desempenho e a disponibilidade; alguns ataques podem até resultar em redirecionamento de tráfego. Use os serviços seguros com autenticação e implemente patches e atualizações de sistema para proteger serviços de roteamento como o RIP.
* Network Time Protocol (NTP)
* Ter o tempo correto nas redes é importante. Carimbos de data e hora corretos são necessários para rastrear com precisão os eventos da rede, como as violações de segurança. Além disso, a sincronização do relógio é fundamental para a interpretação correta dos eventos nos arquivos de dados syslog, bem como para os certificados digitais.
* O NTP (Network Time Protocol, Protocolo de tempo de rede) é um protocolo que sincroniza os relógios de sistemas de computadores em redes de dados. O NTP permite que os dispositivos de rede sincronizem as configurações de hora com um servidor NTP. Os criminosos virtuais atacam servidores de tempo para interromper a comunicação segura que depende de certificados digitais e esconder informações do ataque, como carimbos de data e hora. Use a autenticação NTP para verificar se o servidor é confiável.

2.3.3 Telnet, SSH e SCP

**O Secure Shell (SSH)** é um protocolo que fornece uma conexão com um dispositivo remoto de natureza segura (criptografada) e baseada em uma linha de comando. **O Telnet** é um protocolo mais antigo que usa transmissão de texto não criptografado, não protegido, tanto para autenticação de logon (nome de usuário e senha) quanto para dados transmitidos entre os dispositivos de comunicação. O SSH deve ser usado em vez do Telnet para gerenciar conexões, pois ele oferece criptografia forte. O SSH usa a porta TCP 22. Já o Telnet usa a porta 23.

**A SCP (Secure Copy, cópia segura)** , transfere, com segurança, arquivos de computador entre dois sistemas remotos. O SCP usa o SSH para a transferência de dados (incluindo o elemento de autenticação), para que o SCP garanta a autenticidade e a confidencialidade dos dados em trânsito.

**2.3.4 Protocolos seguros**

Protocolo de Gerenciamento Simples de Rede (SNMP)

O SNMP coleta estatísticas de dispositivos TCP / IP para monitorar a rede e equipamentos de computador. O SNMPv3 é o padrão atual - ele usa criptografia para evitar a espionagem e garantir que os dados não tenham sido violados durante o trânsito.

HTTP

O Hypertext Transfer Protocol (HTTP) fornece conectividade básica da Web e usa a porta 80. O HTTP contém segurança interna limitada e é aberto ao monitoramento de tráfego durante a transmissão de conteúdo, deixando o computador do usuário aberto para ataques. Vamos ver como outros protocolos fornecem uma conexão mais segura:

* A Secure Sockets Layer (SSL) gerencia a criptografia usando um handshake de SSL no início de uma sessão para fornecer confidencialidade e evitar a interceptação e a violação.
* O Transport Layer Security (TLS) é um substituto atualizado e mais seguro para SSL.
* O SSL / TLS criptografa a comunicação entre o cliente e o servidor. Onde for usado, o usuário verá HTTPS no campo de URL de um navegador em vez de HTTP.
* FTP
* O File Transfer Protocol (FTP) oferece a capacidade de transferir arquivos entre um cliente e um servidor. No FTP, o cliente usa um nome de usuário e uma senha de texto sem formatação para se conectar. O File Transfer Protocol Secure (FTPS) é mais seguro - ele adiciona suporte a TLS e SSL para evitar a interceptação, a violação e a falsificação de mensagens trocadas.
* POP, IMAP e MIME
* O e-mail usa Post Office Protocol (POP), IMAP (Internet Message Access Protocol) e MIME (Multipurpose Internet Mail Extensions) para anexar dados sem texto, como imagens ou vídeos, a uma mensagem de e-mail.
* Para proteger o POP (porta 110) ou IMAP (porta 143), use SSL / TLS para criptografar e-mails durante a transmissão. O protocolo Secure / Multipurpose Internet Mail Extensions (S / MIME) oferece um método seguro de transmissão. Ele envia mensagens digitalmente assinadas e criptografadas que fornecem autenticação, integridade de mensagem e não-repudiação.

**2.4.2 Redes da área local virtuais (VLANs)**

As VLANs fornecem uma forma de agrupar dispositivos em uma LAN e em switches individuais. VLANs não são iguais a LANs: LANs virtuais são baseadas em conexões lógicas, enquanto LANs são baseadas em conexões físicas. Portas individuais de um switch podem ser atribuídas a uma VLAN específica. Outras portas podem ser usadas para interconectar fisicamente os switches e permitir o tráfego de várias VLANs entre os switches. Essas portas são chamadas Trunks (troncos).

**2.4.3 Zona Desmilitarizada (DMZ)**

Uma zona desmilitarizada (DMZ) é uma pequena rede entre uma rede privada confiável e a Internet.

Acesso a redes não confiáveis

Os servidores Web e de correio geralmente são colocados na DMZ para permitir que os usuários acessem uma rede não confiável, como a Internet, sem comprometer a rede interna.

Zonas de risco

A maioria das redes tem de duas a quatro zonas de risco: a LAN privada confiável, a DMZ, a Internet e uma extranet.

* Na zona de LAN, o nível de risco é baixo e o nível de confiança é alto.
* Na zona da extranet, o nível de risco é médio-baixo e o nível de confiança médio-alto.
* Na DMZ, o nível de risco é médio-alto e o nível de confiança é médio-baixo.
* Na zona da Internet, o nível de risco é alto e o nível de confiança é baixo.
* Modelo zero-trust
* Os firewalls gerenciam o tráfego de ponta a ponta (tráfego que vai entre os servidores no data center da empresa) e o tráfego de ponta a ponta (dados que entram e saem da rede da empresa).
* Para proteger sua rede, uma empresa pode implementar um **modelo de confiança zero**. Confiar em usuários e endpoints automaticamente na empresa pode colocar qualquer rede em risco, já que usuários confiáveis podem se mover por toda a rede para acessar dados. A rede Zero Trust monitora constantemente todos os usuários na rede, independentemente de status ou função.

2.5.2 Segurança de dispositivos sem fio

A Wired Equivalent Privacy (WEP) foi o primeiro protocolo de segurança usado para redes sem fio. Isso foi substituído pelo Wi-Fi Protected Access (WPA), que melhorou a segurança das conexões sem fio.

Configuração de WPA

O Wi-Fi Protected Access (WPA) foi a resposta do setor de computadores para enfraquecer a utilização do padrão WEP. A configuração mais comum de WPA é WPA-PSK (Pre-Shared Key, Chave pré-compartilhada). As chaves usadas pelo WPA são 256 bits, um aumento significativo sobre as chaves de 64 bits e 128 bits usadas no sistema WEP.

Recursos do WPA

O padrão WPA forneceu várias melhorias de segurança. Primeiro, o WPA fornecia verificações de integridade da mensagem (Message Integrity Checks - MIC) que poderiam detectar se um invasor tinha capturado e alterado os dados transmitidos entre o ponto de acesso sem fio e um cliente sem fio. Outra melhoria importante de segurança foi o protocolo TKIP (Temporal Key Integrity Protocol, Protocolo de integridade da chave temporal). O padrão TKIP proporcionou a capacidade de tratar, proteger e alterar melhor as chaves de criptografia. O AES (Advanced Encryption Standard, Padrão de criptografia avançada) substituiu o TKIP por um melhor gerenciamento de chaves e proteção de criptografia.

WPA2 - Wi-Fi Protected Access II

Como resultado, o lançamento do padrão WPA2 (Wi-Fi Protected Access II, Acesso protegido por Wi-Fi II) aconteceu em 2006. Isso introduziu o uso obrigatório de algoritmos AES e substituiu o TKIP pelo modo de cifra de contador pelo protocolo de código de autenticação de mensagens de cadeia de bloco (CCMP).

WPA3 - Wi-Fi Protected Access III

O WPA3 adicionou mais recursos ao WPA2, como a manutenção de algoritmos criptográficos robustos e a melhoria da troca de chaves.

Como utilizar o Wi-Fi Protected Setup (WPS)

A Configuração protegida por Wi-Fi (WPS) pode ser usada para configurar uma rede doméstica sem fio segura. Conectar dispositivos de IoT à rede sem fio No entanto, o WPS apresenta uma grande vulnerabilidade de segurança, pois o PIN do usuário pode ser descoberto através de um ataque de força bruta. Por isso, o WPS não deve ser usado e deve ser desativado por completo.

**2.5.5 Autenticação**

**Autenticação de sistema aberto.**

**Qualquer dispositivo sem fio pode se conectar à rede sem fio. Use esse método em situações em que a segurança não seja uma preocupação.**

**Autenticação de chave compartilhada**

**Fornece mecanismos para autenticar e criptografar dados entre um cliente sem fio e um AP ou roteador sem fio.**

**2.5.6 Protocolos de autenticação**

**O protocolo de autenticação extensível (EAP) é uma estrutura de autenticação usada em redes sem fio. Vamos descobrir como isso funciona.**

1. **O usuário solicita a conexão à rede sem fio através de um access point.**
2. **O access point solicita dados de identificação (nome de usuário) do usuário, que é então enviado para um servidor de autenticação.**
3. **O servidor de autenticação solicita a prova de que a ID é válida.**
4. **O access point solicita prova de que a ID é válida do usuário, na forma de uma senha.**
5. **O usuário fornece a senha ao access point. O access point envia de volta para o servidor de autenticação.**
6. **O servidor confirma que o nome de usuário e a senha estão corretos e passa essas informações para o access point e o usuário.**
7. **Conecte-se à rede sem fio.**
8. EAP-TLS
9. Requer certificado de cliente: Sim  
   Requer certificado de servidor: Sim  
   Implantável facilmente: Dificuldade  
   de segurança : alta
10. PEAP
11. Requer certificado de cliente: Não  
    Requer certificado de servidor: Sim  
    Implantável facilmente: Dificuldade  
    de segurança: média
12. EAP-TTLS
13. Requer certificado de cliente: Não  
    Requer certificado de servidor: Sim  
    Implantável facilmente: Dificuldade  
    de segurança: média
14. EAP-FAST
15. Requer certificado de cliente: Não  
    Requer certificado de servidor: Não  
    Implantável facilmente: Dificuldade  
    de segurança: média

**2.5.8 Autenticação mútua**

Access points não autorizados

Um access point é qualquer dispositivo de hardware que permite que outros dispositivos sem fio se conectem a uma rede com fio. Qualquer dispositivo que tenha uma interface transmissora sem fio e cabeada ligada a uma rede pode, possivelmente, agir como access point não autorizado.

Como evitar ataques

Quando você se conecta a um access point não autorizado, o impostor que o configura pode solicitar e copiar dados do seu dispositivo. Esse tipo de ataque man in the middle é muito difícil de detectar e pode resultar em credenciais de logon roubadas e dados lidos.

A autenticação mútua é a autenticação de duas vias que pode impedir access points não autorizados. É um processo no qual as duas entidades em um link de comunicação se autenticam antes de se conectarem. Isso permite que os clientes detectem access points não autorizados e evitem esses ataques MitM.

**2.5.10 Métodos de comunicação**

Os dispositivos móveis usam comunicações por celular para se conectar a um provedor de serviços. Provedores sem fio usam redes LTE 5G IP para acessar a Internet e outros serviços de dados, por exemplo.

WiFi e Bluetooth

Os dispositivos móveis podem usar sinais sem fio, como Wi-Fi e Bluetooth. Você pode configurar o acesso sem fio através do menu de configurações do dispositivo. O Bluetooth é comumente usado para conectar fones de ouvido ou emparelhar um telefone com um sistema de som de carro.

Comunicações de campo próximo (Near-Field)

A comunicação de campo próximo (NFC) permite a comunicação sem contato entre dispositivos. Os chips NFC usam campos eletromagnéticos para permitir pagamentos sem contato, o que significa, por exemplo, que você só precisa manter seu dispositivo próximo a um terminal de pagamento para processar o pagamento.

Infravermelho

Infravermelho (IR) fornece comunicação de curto alcance usando um receptor de IR. Por exemplo, o IR permite que você controle sua televisão pelo telefone celular

Comunicação USB

O único tipo de comunicação nessa lista co fio, a comunicação USB permite que você use seu smartphone para armazenamento de dados ou áudio. A conectividade USB também permite que um dispositivo móvel funcione como um modem ou fax. Você pode conectar um dispositivo móvel a dispositivos de aquisição forense pela porta USB se precisar coletar informações para uma investigação.

2.5.11 Gerenciamento de dispositivos móveis

Um dispositivo móvel emitido por uma empresa pode conter dados pessoais e organizacionais; ele pode ser de propriedade da corporação ou habilitado pessoalmente (COPE).

**Segmentação e conteinerização do armazenamento**

A segmentação do armazenamento e a conteinerização permitem separar o conteúdo pessoal e do trabalho em um dispositivo. Ele fornece uma área autenticada e criptografada que separa as informações confidenciais da empresa dos dados pessoais do usuário.

A conteinerização também nos permite:

* Isolar os aplicativos.
* Controle as funções do aplicativo.
* Exclua as informações do container.
* Bloqueie ou limpe o dispositivo remotamente.
* **Gerenciamento de conteúdo**
* Uma empresa precisa considerar os riscos de segurança envolvidos no uso de aplicativos que compartilham dados, por exemplo, Dropbox, Box, Google Drive e iCloud. Um sistema de segurança de gerenciamento de identidades pode ser usado para controlar quais dados um usuário pode acessar.
* **Gerenciamento de aplicativos**
* A lista de permissão permite que você **assine digitalmente** as aplicações para que você possa autorizar as aplicações que os usuários podem instalar. Isso ajuda a garantir que as aplicações instaladas sejam provenientes de fontes confiáveis.
* A autenticação usando senhas fortes é uma prática recomendada para os aplicativos que exigem credenciais de usuário.

**2.5.12 Proteções de dispositivo móvel**

**Jailbreaking, root e sideloading**

**Jailbreaking, root e sideload são formas de contornar as limitações de um dispositivo para fazer coisas que o dispositivo está impedido de fazer. Os usuários podem tentar fazer o jailbreak (dispositivos da Apple) ou root (dispositivos Android) para executar um aplicativo que não está autorizado ou não está disponível na loja.**

**O jailbreak remove a restrição de que apenas aplicativos autorizados pela Apple podem ser executados no dispositivo. O enraizamento ignora a arquitetura de segurança do Android para permitir acesso administrativo completo ao dispositivo. Ambos representam um risco para a empresa.**

**Há soluções disponíveis que podem detectar um dispositivo com "jailbroken" ou "rooteado". Um dispositivo é então marcado como não compatível e removido da rede ou tem o acesso negado a aplicativos organizacionais.**

**As lojas de aplicativos de terceiros também podem representar um risco para as empresas porque os aplicativos aos quais elas fornecem acesso não foram avaliados corretamente. O sideloading (carregamento lateral) ocorre quando o usuário percorre as configurações de aplicativo aprovado para instalar aplicativos não aprovados. Isso é menos invasivo do que fazer jailbreaking ou rooting, mas ainda é um risco.**

Quais são as proteções?

As proteções contra ameaças a dispositivos móveis incluem:

* Os **bloqueios de tela** exigem uma senha, um PIN ou um padrão para acessar o dispositivo.
* A **autenticação biométrica** usa uma característica física exclusiva (impressão digital, face, íris ou voz).
* A **autenticação com reconhecimento de contexto** usa aprendizado de máquina para determinar o acesso com base no comportamento normal do usuário.
* A **limpeza remota** exclui os dados do dispositivo, caso ele seja roubado ou perdido.
* A **criptografia completa** do dispositivo pode criptografar todos os dados em um dispositivo móvel.

**2.5.13 Rastreamento de GPS**

O GPS (Global Positioning System, Sistema de posicionamento Global) usa satélites e computadores para determinar a localização de um dispositivo. A tecnologia de GPS é um recurso padrão em smartphones e oferece rastreamento de posição em tempo real que normalmente pode localizar um local a aproximadamente 5 metros.

Alguns aplicativos usam a delimitação geográfica ou geolocalização, que usa a identificação por radiofrequência (RFID) para determinar uma área geográfica.

**2.6.2 Alta disponibilidade**

Sistemas de alta disponibilidade normalmente incluem estes três princípios de projeto.

**Eliminar pontos únicos de falha**

O primeiro princípio que define os sistemas de alta disponibilidade começa com a identificação de todos os dispositivos e componentes do sistema cuja falha resultaria em falha em todo o sistema. Os métodos para eliminação de pontos únicos de falhas incluem dispositivos de hot standby, componentes redundantes e várias conexões ou caminhos.

**Fornecer transição confiável**

Fontes de alimentação redundantes, sistemas de energia de backup e sistemas de comunicação de backup proporcionam transição confiável.

**Detectar falhas à medida que ocorrem**

O monitoramento ativo do dispositivo e do sistema detecta vários tipos de eventos, incluindo falhas do dispositivo e do sistema. Os sistemas de monitoramento podem até acionar o sistema de backup em caso de falha.

2.6.3 Os Cinco Noves

Toda empresa quer poder operar ininterruptamente, mesmo em condições extremas, como durante um ataque.

Dentre as práticas mais populares de alta disponibilidade estão os cinco noves. Ela recebe esse nome do objetivo de atingir uma taxa de disponibilidade de 99,999%, ou seja, cinco noves em seguida. Isso significa que o período de inatividade é menos de 5,26 minutos por ano.

Sistemas padronizados

A padronização dos sistemas propicia que os sistemas usem os mesmos componentes. Os inventários de peças são mais fáceis de manter, e é possível trocar componentes durante uma emergência.

Clustering

Clusters de vários dispositivos agrupados proporcionam um serviço que parece ser uma única entidade para um usuário. Se um dispositivo falhar, os outros dispositivos permanecem disponíveis.

Sistemas de componente compartilhado

Os sistemas são criados para que um sistema completo possa substituir um que falhou.

2.6.4 pontos únicos de falha

Únicos pontos de falha são links fracos na cadeia que podem provocar interrupção das operações da empresa. Um único ponto de falha é qualquer parte da operação da empresa cuja falha significa falha completa de todo o sistema - em outras palavras, se falhar, o sistema inteiro falhará.

2.6.6 Redundância N + 1

A redundância N+1 garante a disponibilidade do sistema, no caso de falha de um componente. Os componentes (N) precisam ter, no mínimo, um componente de backup (+1).

**2.6.7 RAID**

**O RAID obtém os dados normalmente armazenados em um único disco e os espalha entre várias unidades. Se qualquer disco único RAID0 for perdido, o usuário poderá recuperar os dados de outros discos que também hospedam os dados.**

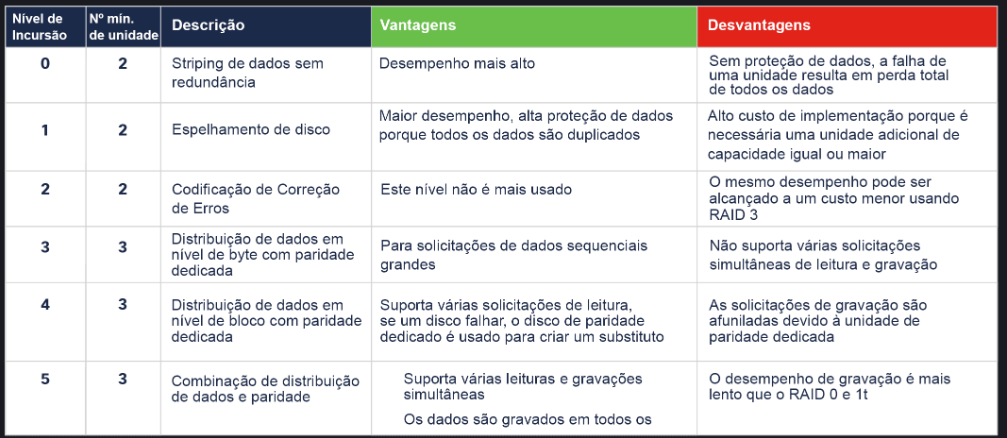
**O RAID também pode aumentar a velocidade da recuperação de dados, já que várias unidades recuperarão os dados solicitados mais rapidamente do que um disco fazendo o mesmo.**

**Uma solução RAID pode ser baseada em software ou hardware. Uma solução baseada em hardware requer um controlador de hardware especializado, no sistema que contenha as unidades RAID.**

**Os termos a seguir descrevem as várias maneiras pelas quais o RAID pode armazenar dados na matriz de discos.**

* **Espelhamento - Armazena dados duplicados em uma segunda unidade.**
* **Distribuição - Grava dados em várias unidades para que segmentos consecutivos sejam armazenados em unidades diferentes.**
* **Paridade - mais precisamente, tirar a paridade. Após a distribuição, as somas de verificação são geradas para verificar se não há erros nos dados distribuídos. Essas somas de verificação são armazenadas em uma terceira unidade.**

**Existem outras arquiteturas RAID, que combinam principalmente os elementos acima.**



**2.6.8 Spanning Tree**

**O Spanning Tree Protocol (STP) soluciona esses problemas. A função básica do STP é prevenir loops em uma rede, quando os switches se interconectarem por vários caminhos. O STP garante que os links físicos redundantes estejam livres de loop e que apenas um caminho lógico seja executado entre todos os destinos na rede. O STP bloqueia intencionalmente os caminhos redundantes que poderiam provocar um loop.**

**2.6.9 Redundância de roteador**

**o roteador de encaminhamento e o roteador standby usam um protocolo de redundância para determinar qual roteador deve assumir o papel ativo na redundância. Cada roteador está configurado com um endereço IP físico e um endereço IP do roteador virtual. Dispositivos finais usam o endereço IP virtual como o gateway padrão.**

**O roteador de encaminhamento e o roteador standby usam seus endereços IP físicos para trocar mensagens periódicas. O objetivo dessas mensagens é ter certeza de que os dois ainda estão on-line e disponíveis.**

A capacidade de uma rede de se recuperar dinamicamente da falha de um dispositivo que atua como um gateway padrão é conhecida como **redundância de primeiro salto**.

**2.6.10 Redundância de local**

Replicação síncrona

* Sincroniza os dois locais em tempo real
* Requer alta largura de banda
* Os locais devem ser próximos um do outro, para reduzir a latência

Replicação assíncrona

* Não sincronizados em tempo real, mas muito próximo disso
* Requer menos largura de banda
* Os sites podem estar mais distantes, pois a latência é o menor dos problemas

Point-in-time-Replication (Replicação de um ponto no tempo)

* Atualiza periodicamente a localização dos dados de backup
* Mais conservador em termos de largura de banda, pois não exige uma conexão constante

O equilíbrio correto entre custo e disponibilidade determinará a escolha correta para uma empresa.

2.6.11 Design resiliente

Resiliência representa os métodos e configurações usados para tornarem um sistema ou rede tolerante a falhas.

Como visto nos exemplos acima, o design resiliente é mais do que apenas adicionar redundância. É fundamental entender as necessidades comerciais da empresa e, em seguida, incorporar a redundância para criar uma rede resiliente.

**Resiliência de aplicativo**

* **Hardware tolerante a falhas** (mais complexo e mais caro) é um sistema projetado com a colocação de múltiplos componentes essenciais em um mesmo computador.
* **Arquitetura de cluster**é um grupo de servidores que funcionam como se fossem um único sistema.
* **Backup e restauração** Cópias de backup de arquivos com a finalidade de poder restaurá-los se ocorrer perda de dados (menos complexo e menos caro).
* **Resiliência do IOS**
* O IOS (Interwork Operating System, Sistema operacional Interwork) para roteadores e switches Cisco incluem um atributo resiliente de configuração. Permite recuperação mais rápida se alguém, intencionalmente ou não, reformatar a memória flash ou apagar o arquivo de configuração de inicialização. Este atributo mantém uma cópia de trabalho segura do arquivo de imagem do IOS do roteador e uma cópia do arquivo de configuração de execução. O usuário não pode remover esses arquivos seguros, também conhecidos como o bootset primário.

**2.6.12 Sistema e backups de dados**

**Frequência**

**Os backups podem levar muito tempo. Às vezes é mais fácil fazer um backup completo mensal ou semanal, e depois backups parciais frequentes de todos os dados que tiverem mudado, desde o último backup completo. No entanto, ter muitos backup parciais aumenta o tempo necessário para restaurar os dados.**

**2.6.14 Potência**

* Data centers devem estar em uma fonte de alimentação diferente do resto do edifício.
* Fontes de alimentação redundantes: dois ou mais feeds (fontes de alimentação) provenientes de duas ou mais subestações elétricas.
* Condições de alimentação.
* Backup de sistemas de energia são, muitas vezes, necessários.
* Uma UPS deve estar disponível para sistemas de desligamento normais.

**termos padrão vinculados a eventos do sistema de energia elétrica.**

**Excesso de energia**

* Pico: alta tensão momentânea.
* Sobrecarga: alta tensão prolongada.

**Perda de energia**

* Falha: perda momentânea de energia.
* Blackout: Perda completa de energia.

**Degradação de energia**

* Sag/dip: baixa tensão momentânea.
* Queda de energia: baixa tensão prolongada.
* Corrente de Inrush (Pico de Corrente): sobrecarga inicial de energia.

**2.6.15 Aquecimento, ventilação e ar-condicionado (HVAC)**

Empreiteiro de sistemas de HVAC

Sistemas HVAC comerciais e outros sistemas de gerenciamento de edifício agora se conectam à Internet para monitoramento e controle remotos. Mas os eventos recentes mostraram que esses sistemas "inteligentes" também geram grandes problemas de segurança, pois eles são acessados e gerenciados por fornecedores de sistemas HVAC ou de terceiros.

2.7.2 Ameaças a setores importantes de indústrias

Ao longo da última década, ataques cibernéticos como Stuxnet provaram que um ataque cibernético pode destruir ou interromper infraestruturas essenciais. O ataque Stuxnet, especificamente, foi direcionado ao sistema SCADA (Supervisory Control and Data Acquisition, Controle de supervisão e aquisição de dados) e foi usado para controlar e monitorar processos industriais. O SCADA e outros sistemas de controle industrial (ICSs) são usados nos sistemas de manufatura, produção, energia e comunicação.

**Sistemas integrados**

Por que os sistemas integrados estão vulneráveis a ataques?

Os ataques contra sistemas integrados exploram vulnerabilidades de segurança nos componentes de software e hardware. Eles são suscetíveis a ataques de tempo, em que os invasores descobrem vulnerabilidades estudando quanto tempo o sistema leva para responder a diferentes entradas. Um ataque de tempo é considerado um ataque de canal lateral.

Esse tipo de ataque se baseia nas informações obtidas com a implementação de um sistema, e não nos pontos fracos do software. Informações de tempo, consumo de energia, vazamentos eletromagnéticos ou até mesmo som podem ser essa fonte de informações.

Como os sistemas integrados podem ser protegidos?

Uma técnica é usar a tecnologia **System on Chip (SoC)**. A tecnologia SoC é um módulo de hardware "Small Form Factor" (SFF). Exemplos de clientes incluem dispositivos como Raspberry Pi e Arduino. Esses dispositivos são computadores de placa única que podem ser implementados usando um "Field-Programmable Gate Array" (FGPA), um circuito integrado que pode ser programado ou modificado em campo. Isso significa que o usuário pode fazer alterações após a implantação do dispositivo.

O SoC integra um microcontrolador, uma aplicação ou microprocessador e periféricos como uma GPU, um módulo de Wi-Fi ou um coprocessador. O processador pode executar um sistema operacional como Windows, Linux ou Android.

Muitos desses dispositivos de SoC têm autenticação ruim e / ou não podem ser atualizados ou corrigidos. Devido à natureza desses dispositivos, um nível de confiança implícita é necessário, pois não há nenhum programa formal para verificar os controles de segurança.

**2.7.5 Internet das Coisas (IoT)**

**Usam um sistema operacional em tempo real(RTOS) um pequeno sistema operacional que permite a troca rápida em tarefas que se concentram no tempo e não na taxa de transferência. Esses aplicativos são executados com tempo preciso e alta confiabilidade**

**As vulnerabilidades associadas ao RTOS são injeção de código, ataques de Ddos e inversão de propriedade (onde uma tarefa de alta prioridade e trocada por uma de prioridade mais baixa)**

**Usar um scanner de IoT, como a Shodan, é uma maneira fácil de saber se um dispositivo de automação residencial está vulnerável a ataques. Os dispositivos de IoT se comunicam usando métodos de curto, médio ou longo alcance e incluem celular (4G, 5G), rádio e Zigbee. O Zigbee é um conjunto sem fio de protocolos para redes pessoais de área (WPANs).**

**2.7.8 Equipamento VoIP**

**Voz sobre IP (VoIP) usa redes como a Internet para fazer e receber chamadas de telefone.**

**De que equipamento você precisa?**

**Você precisa de uma conexão com a Internet e um telefone para VoIP. Várias opções estão disponíveis como configuração do telefone:**

* **Um telefone tradicional, com um adaptador (o adaptador atua como uma interface de hardware entre um telefone tradicional, analógico e uma linha digital VoIP)**
* **Um telefone ativado para VoIP**
* **Software VoIP instalado em um computador**

**Como você pode proteger seu serviço de VoIP?**

**Implemente as seguintes contramedidas para proteger o VoIP:**

* **Criptografe os pacotes de mensagens de voz para proteger contra espionagem.**
* **Use o SSH para proteger gateways e switches.**
* **Altere todas as senhas padrão.**
* **Use um sistema de detecção de invasão para detectar ataques, como envenenamento ARP.**
* **Use autenticação forte para mitigar o spoofing de registro (os criminosos virtuais roteiam todas as chamadas recebidas da vítima para eles), representação de proxy (engana a vítima para se comunicar com um proxy falso configurado pelos criminosos virtuais) e sequestro de chamadas (a chamada é interceptada e reencaminhada para um caminho diferente, antes de chegar ao destino).**
* **Implemente firewalls que reconhecem VoIP para monitorar os streams e filtrar sinais anormais.**

**2.7.11 Tecnologias de enganação**

**Um honeypot é um sistema de isca configurado para imitar um servidor na rede da empresa. Ela é intencionalmente deixada exposta para atrair invasores. Quando um invasor vai atrás do honeypot, suas atividades são registradas e monitoradas para posterior análise. O honeypot distrai o invasor dos recursos de rede reais da empresa.**

**Uma empresa pode até criar uma rede de mel, uma coleção de honeypots (honeynet), para imitar sua rede e distrair os invasores. Enquanto isso, os arquivos Honey são arquivos falsos que atraem um invasor, mas não contêm informações reais.**

**Um sinkhole DNS impede a resolução de nomes de host para URLs específicas e pode afastar os usuários de recursos mal-intencionados.**

**3.1 Controles de acesso**

**exploraremos exemplos de controles físicos, lógicos e administrativos antes de analisar de perto como o acesso é controlado por 'AAA' - autorização, autenticação e contabilidade.**

**3.1.2 Controles de acesso físico**

**3.1.3 Controles de acesso lógicos**

**Controles de acesso lógico são as soluções de hardware e software usadas para gerenciar o acesso aos recursos e sistemas. Essas soluções baseadas em tecnologia incluem ferramentas e protocolos que os sistemas de computador usam para identificação, autenticação, autorização e auditoria.**

**Exemplos de controle de acesso lógico incluem:**

* **A criptografia é o processo de pegar o texto claro e criar o texto codificado.**
* **Os cartões inteligentes possuem um microchip integrado.**
* **As senhas são strings de caracteres protegidos.**
* **A biometria se refere às características físicas dos usuários.**
* **As listas de controle de acesso (ACLs) definem o tipo de tráfego permitido em uma rede.**
* **Os protocolos são conjuntos de regras que regem a troca de dados entre os dispositivos.**
* **Os firewalls impedem o tráfego de rede indesejado.**
* **Os roteadores conectam pelo menos duas redes.**
* **Os sistemas de detecção de invasão monitoram as atividades suspeitas de uma rede.**
* **Os níveis de corte são determinados pelos limites permitidos para erros antes de acionar uma bandeira vermelha.**

**3.1.5 Controles de Acesso Administrativos em Detalhes**

**O conceito de controles de acesso administrativo envolve três serviços de segurança: autenticação, autorização e contabilidade (AAA).**

**Autenticação**

**O primeiro A no AAA representa a autenticação. A autenticação verifica a identidade de um usuário para evitar o acesso não autorizado.**

**Além disso, os usuários precisam verificar sua identidade fornecendo um dos seguintes:**

* **Algo que saibam (como uma senha)**
* **Algo que tenham (como um token ou cartão)**
* **Algo que eles são (como uma impressão digital)**

**No caso da autenticação de dois fatores, que está se tornando cada vez mais a regra, o sistema requer uma combinação de duas das alternativas acima, em vez de apenas uma, para verificar a identidade de alguém.**

**Autorização**

**Alguns sistemas fazem isso usando uma lista de controle de acesso, ou uma ACL. Uma ACL determina se um usuário tem certos privilégios de acesso depois de se autenticar. Só porque você pode fazer logon na rede corporativa não significa que você tenha permissão para usar a impressora colorida de alta velocidade, por exemplo.**

**Contabilidade**

**Não relacionada à contabilidade financeira, a contabilidade em AAA acompanha o que os usuários fazem – incluindo o que eles acessam, a quantidade de tempo que acessam os recursos e quaisquer alterações que fazem.** **O Accounting controla e monitora em tempo real.**

**3.1.6 O que é identificação?**

**A identificação aplica as regras estabelecidas pela política de autorização. Sempre que o acesso a um recurso é solicitado, os controles de acesso determinam se o acesso deve ser concedido ou negado.**

**3.1.8 Gerenciamento de Identidade Federada**

**O gerenciamento de identidades federadas refere-se a várias empresas que permitem que seus usuários usem as mesmas credenciais de identificação para obter acesso às redes de todas as empresas do grupo. Infelizmente, isso amplia o escopo e aumenta a probabilidade de um efeito em cascata caso ocorra um ataque.**

**3.1.9 Métodos de Autenticação**

**O que você sabe**

**Senhas, frases secretas ou PINs são exemplos de algo que o usuário *conhece*. As senhas são o método mais popular usado para autenticação.**

**Os termos frase secreta, código de acesso, chave de acesso ou PIN são chamados genericamente de senha. Uma senha é uma string de caracteres protegidos usada para comprovar a identidade de um usuário.**

**O que você tem**

**Cartões inteligentes e chaveiros de segurança são exemplos de algo que os usuários possuem e que podem ser usados para fins de autenticação.**

**Um cartão inteligente é um pequeno cartão de plástico, do tamanho de um cartão de crédito, com um pequeno chip embutido nele. O chip é um portador de dados inteligente, capaz de processar, armazenar e proteger dados.** **Na maioria dos casos, as chaves de segurança são usadas para autenticação de dois fatores (2FA)**

**Quem você é**

**Características físicas únicas, como impressão digital, retina ou voz, que identificam uma pessoa específica são chamadas de biometria. A segurança biométrica compara as características físicas aos perfis armazenados para autenticar os usuários.**

**Existem dois tipos de identificadores biométricos:**

* **Características fisiológicas – Incluem impressões digitais, DNA, rosto, mãos, retina ou ouvido**
* **Características comportamentais - padrões de comportamento como gestos, voz, andar ou ritmo de digitação.**

**A implementação da biometria envolve um leitor ou dispositivo de digitalização, um software que converte as informações digitalizadas em formato digital e um banco de dados que possui dados biométricos armazenados para comparação.**

**3.1.12 Autorização**

**A autorização controla o que um usuário pode e não pode fazer na rede após a autenticação com sucesso.**

**Quando implementar a autorização**

**A autorização usa um conjunto de atributos que descreve o acesso do usuário à rede para responder à pergunta: "Quais privilégios de leitura, cópia, edição, criação e exclusão esse usuário tem?"** **Os administradores do sistema configuraram a rede para implementar a autorização imediatamente após a autenticação do usuário.**

**Usando autorização**

**Definir as regras de autorização é a primeira etapa no controle de acesso. Uma política de autorização estabelece essas regras.**

**Uma política de associação baseada em grupo define a autorização com base nos membros de um grupo específico. Uma política de nível de autoridade define as permissões de acesso com base na posição de um funcionário na organização.**

**3.1.15 Implementação de Auditabilidade**

**O que é accountability (auditabilidade)?**

**A auditabilidade rastreia uma ação de volta a uma pessoa ou processo que faz essa mudança em um sistema. A auditabilidade então coleta essas informações e relata os dados de uso.**

**Implementação de Auditabilidade**

**A implementação da auditabilidade consiste em tecnologias, políticas, procedimentos e educação. Os arquivos de log fornecem as informações de detalhes com base nos parâmetros escolhidos.** **As políticas e procedimentos da empresa determinam quais ações devem ser registadas e como os arquivos de log são gerados, revisados e armazenados.**

**Oferecer responsabilidade**

**A retenção de dados, eliminação de mídia e requisitos de conformidade geram auditabilidade. Muitas leis exigem a implementação de medidas para proteger diferentes tipos de dados. Essas leis orientam uma empresa sobre o caminho certo para manusear, armazenar e eliminar dados.**

**3.2.1 Segurança Zero Trust**

**Zero Trust é uma abordagem abrangente para proteger todo o acesso em redes, aplicações e ambientes. Essa abordagem ajuda a proteger o acesso de usuários, dispositivos de usuário final, APIs, IoT, microsserviços, contêineres e muito mais. Ele protege a força de trabalho, as cargas de trabalho e o local de trabalho de uma organização. O princípio de uma abordagem de confiança zero é: “Nunca confie, sempre verifique”. Assumir confiança zero sempre que alguém ou algo solicitar acesso a ativos.** **Os três pilares da confiança zero são força de trabalho, cargas de trabalho e local de trabalho.**

**Confiança zero para a força de trabalho**

**Este pilar consiste em pessoas (por exemplo, funcionários, prestadores de serviços, parceiros e fornecedores) que acessam aplicativos de trabalho usando seus dispositivos pessoais ou gerenciados por empresas. Esse pilar garante que apenas os usuários certos e dispositivos seguros possam acessar aplicativos, independentemente da localização.**

**Confiança zero para cargas de trabalho**

**Esse pilar está preocupado com aplicativos que estão sendo executados na nuvem, em data centers e outros ambientes virtualizados que interagem uns com os outros. Ele se concentra no acesso seguro quando uma API, um microsserviço ou um contêiner está acessando um banco de dados dentro de um aplicativo.**

**Confiança zero para o local de trabalho**

**Este pilar se concentra no acesso seguro para qualquer e todos os dispositivos, inclusive na Internet das Coisas (IoT), que se conectam a redes empresariais, como terminais de usuário, servidores físicos e virtuais, impressoras, câmeras, sistemas de AVAC, quiosques, bombas de infusão, sistemas de controle industrial e muito mais.**

**3.2.2 Modelos de controle de acesso**

**Discretionary access control (DAC)**

* **Este é o modelo menos restritivo e permite que os usuários controlem o acesso aos seus dados como proprietários desses dados.**
* **O DAC pode usar ACLs ou outros métodos para especificar quais usuários ou grupos de usuários têm acesso às informações.**

**Controle de acesso obrigatório (MAC)**

* **Isso aplica o controle de acesso mais rigoroso e é normalmente usado em aplicações militares ou de missão crítica.**
* **Ele atribui rótulos de nível de segurança às informações e permite que os usuários tenham acesso com base em sua autorização de nível de segurança.**

**Controle de acesso baseado em funções (RBAC)**

* **As decisões de acesso são baseadas nas funções e responsabilidades de um indivíduo dentro da organização.**
* **Diferentes funções recebem privilégios de segurança e indivíduos são atribuídos ao perfil RBAC para a função.**
* **As funções podem incluir diferentes posições, classificações de cargo ou grupos de classificações de emprego.**
* **Também conhecido como um tipo de controle de acesso não discricionário.**
* **Controle de acesso baseado em atributos (ABAC)**
* O ABAC permite o acesso com base em atributos do objeto (recurso) a ser acessado, o sujeito (usuário) acessando o recurso e fatores ambientais sobre como o objeto deve ser acessado, como a hora do dia.

**Controle de acesso baseado em regras (RBAC)**

* **A equipe de segurança de rede especifica conjuntos de regras ou condições associadas ao acesso a dados ou sistemas.**
* **Essas regras podem especificar endereços IP permitidos ou negados, ou determinados protocolos e outras condições.**
* **Também conhecido como RBAC Baseado em Regras.**
* **Controle de acesso baseado em tempo (TAC)**
* TAC Permite o acesso a recursos de rede com base na hora e no dia.
* Outro modelo de controle de acesso é o princípio do privilégio mínimo, que especifica uma abordagem limitada, conforme necessário, para conceder direitos de acesso ao usuário e ao processo a informações e ferramentas específicas. O princípio do privilégio mínimo afirma que os usuários devem receber a quantidade mínima de acesso necessária para desempenhar sua função de trabalho.
* Uma exploração comum é conhecida como escalação de privilégios. Nesta exploração, vulnerabilidades em servidores ou sistemas de controle de acesso são exploradas para conceder a um usuário não autorizado, ou processo de software, níveis de privilégio mais altos do que deveriam ter. Depois que o privilégio é concedido, o agente de ameaça pode acessar informações confidenciais ou assumir o controle de um sistema.

**3.2.3 Sistemas de controle de acesso à rede (NAC)**

**Network Access Control (NAC) são compatíveis com o gerenciamento de acesso ao aplicar políticas organizacionais relacionadas às pessoas e aos dispositivos que estão tentando acessar a rede. Os sistemas NAC permitem que profissionais de cyberscurity monitorem os usuários e dispositivos conectados à rede e controlem manualmente o acesso conforme necessário.**

**Os sistemas de controle de acesso à rede oferecem os seguintes recursos:**

* **Aplicação rápida de políticas de acesso que foram criadas para diferentes condições operacionais.**
* **Reconhecer e criar perfis de usuários e dispositivos conectados para evitar que softwares mal-intencionados em sistemas não compatíveis causem danos.**
* **Fornecer acesso seguro aos convidados da rede, geralmente através de portais de registro.**
* **Avaliar a conformidade do dispositivo com as políticas de segurança por tipo de usuário, tipo de dispositivo e sistema operacional antes de permitir o acesso à rede.**
* **Atenuar os incidentes de segurança ao bloquear, isolar ou reparar dispositivos não compatíveis.**

**Como as redes BYOD e IoT expandem muito a superfície de ataque da rede, os recursos de automação do sistema NAC tornam prático o controle focado do acesso à rede por esses dispositivos. O sistema NAC está configurado para impor políticas organizacionais. As políticas relevantes são decretadas para permitir ou negar o acesso à rede de acordo com uma ampla gama de fatores que o sistema NAC detecta nos dispositivos que estão tentando acessar. Sem os sistemas NAC, seria impossível para o pessoal de segurança cibernética avaliar os milhares de dispositivos que poderiam tentar acessar a rede.**

**3.3.2 Tipos de conta**

**Como provedor de identidade (Idp), a empresa é responsável por autenticar sua identidade.**

**3.3.3 Contas privilegiadas**

**Os criminosos digitais têm como alvo contas privilegiadas. Por quê? Porque essas são as contas mais poderosas da empresa com acesso elevado e irrestrito aos sistemas. Os administradores usam essas contas para implantar e gerenciar sistemas operacionais, aplicativos e dispositivos de rede.**

**As organizações devem adotar práticas robustas para proteger contas privilegiadas.**

* **Identificar e reduzir o número de contas com privilégios**
* **Aplicação do princípio do privilégio mínimo. O princípio significa que usuários, sistemas e processos só têm acesso a recursos (redes, sistemas e arquivos) que são absolutamente necessários para executar a função atribuída.**
* **Revogar os direitos de acesso quando os funcionários deixarem ou mudarem de emprego.**
* **Eliminar contas compartilhadas com senhas que não expiram**
* **Proteger o armazenamento de senha.**
* **Eliminar as credenciais compartilhadas por vários administradores**
* **Alterar automaticamente as senhas de contas com privilégio a cada 30 ou 60 dias**
* **Registro de sessões com privilégios**
* **Implementar um processo para alterar senhas incorporadas para scripts e contas de serviço**
* **Registrar todas as atividades do usuário**
* **Gerar alertas para comportamento incomum**
* **Desativar contas inativas com privilégios**
* **Use a autenticação de vários fatores para todos os acessos administrativos**
* **Implemente um gateway entre o usuário final e os ativos confidenciais para limitar a exposição da rede a malware.**

**3.3.4 Controle de acesso de arquivos**

**As permissões são regras definidas para limitar o acesso de um indivíduo ou grupo. Por exemplo, não é necessário poder acessar todos os arquivos de um servidor, se você só precisar acessar uma única pasta. Pode ser mais fácil fornecer acesso a toda a unidade, mas é mais seguro limitar o acesso apenas à massa necessária. Esse é o princípio do menor privilégio e intimamente ligado ao conceito de acesso "preciso saber".**

**Controle Total**

**Os usuários podem:**

* **Veja o conteúdo de um arquivo ou pasta.**
* **Alterar e excluir arquivos e pastas existentes.**
* **Criar novos arquivos e pastas.**
* **Executar programas em uma pasta.**
* Modificar

* Os usuários podem alterar e excluir os arquivos e as pastas existentes, mas não podem criar novos.
* Ler e executar

* Os usuários podem visualizar o conteúdo de arquivos e pastas existentes e podem executar programas em uma pasta.
* Gravação

* Os usuários podem criar novos arquivos e pastas e fazer alterações nos arquivos e pastas existentes.
* Leitura

* Os usuários podem visualizar o conteúdo de uma pasta e abrir arquivos e pastas.

**Depois que as permissões da pasta pai forem definidas, as pastas e os arquivos criados dentro da pasta pai herdam suas permissões. Além disso, a localização dos dados e a ação realizada nos dados determinam como as permissões são propagadas:**

* **Os dados movidos para o mesmo volume manterão as permissões originais.**
* **Os dados copiados para o mesmo volume herdarão novas permissões.**
* **Os dados movidos para um volume diferente herdarão novas permissões.**
* **Os dados copiados para um volume diferente herdarão novas permissões.**

**É importante observar que ao alterar as permissões de uma pasta, você também tem a opção de aplicar as mesmas permissões a todas as subpastas. Chamado de propagação de permissão, esta é uma maneira fácil de alterar rapidamente as permissões de muitos arquivos e pastas.**

**3.3.7 Políticas de conta no Windows**

**Na maioria das redes que usam computadores Windows, um administrador configura o Active Directory com domínios em um servidor Windows. Os computadores Windows que ingressam no domínio se tornam membros do domínio.**

**O administrador configura uma política de segurança de domínio que se aplica a todos os computadores que ingressam no domínio. Por exemplo, as políticas de conta são definidas automaticamente quando um usuário faz login no Windows.**

**Quando um computador não faz parte de um domínio do Active Directory, o usuário configura políticas por meio da Política de Segurança Local do Windows Em todas as versões do Windows exceto na Home Edition, digite secpol. msc no comando Executar para abrir a ferramenta de Política de Segurança Local.**

**Política de senhas**

**Um administrador pode configurar políticas de conta de usuário, como políticas de senha e políticas de bloqueio.**

**Política de bloqueio de conta**

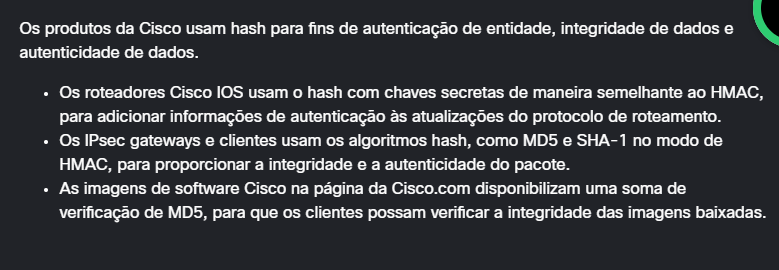
**Uma política de bloqueio de conta bloqueia uma conta por um período definido quando ocorrem muitas tentativas de login incorretas.**

**Política de auditoria**

**Mais configurações de segurança estão disponíveis selecionando a pasta 'políticas locais' no Windows. Uma política de auditoria cria um arquivo de log de segurança usado para rastrear os seguintes eventos:**

**3.3.8 Gerenciamento de Autenticação**

* **Uma solução de logon único (SSO) permite que o usuário use um conjunto de credenciais de login para autenticar em vários aplicativos. Dessa forma, o usuário só precisa lembrar uma senha forte.**
* **OAuth é um padrão que permite que as informações de conta de um usuário sejam usadas por serviços de terceiros, como o Facebook ou o Google.**
* **Um cofre de senha pode proteger e armazenar as credenciais do usuário com uma única senha forte necessária para acessá-las.**
* **Muitas empresas implementam a autenticação baseada em conhecimento (KBA) para fornecer uma redefinição de senha caso um usuário esqueça sua senha. A KBA é baseada em informações pessoais conhecidas pelo usuário ou em uma série de perguntas.**
* 3.3.10 Código de autenticação de mensagem baseado em hash (HMAC)
* O Código de autenticação de mensagem com base em hash (HMAC) usa uma chave de criptografia com uma função de hash para autenticar um usuário da Web. Muitos serviços da Web usam a autenticação básica, que não criptografa o nome de usuário e a senha durante a transmissão. Usando o HMAC, o usuário envia um identificador com chave privada e um HMAC. O servidor procura a chave privada do usuário e cria um HMAC. O HMAC do usuário deve ser compatível com o calculado pelo servidor.
* As VPNs que usam IPsec contam com as funções HMAC para autenticar a origem de cada pacote e fornecer a verificação de integridade de dados.

****

**3.3.12 Protocolos e tecnologias de autenticação**

**Um protocolo de autenticação autentica os dados entre duas entidades para impedir o acesso não autorizado. Um protocolo descreve o tipo de informação que precisa ser compartilhada para se autenticar e se conectar.**

**Protocolo de autenticação extensível (EAP)**

**Uma senha do cliente é enviada usando um hash para o servidor de autenticação. O servidor de autenticação tem um certificado (o cliente não precisa de um certificado).**

**PAP (Password Authentication Protocol)**

**Um nome de usuário e uma senha são enviados para um servidor de acesso remoto em texto sem formatação. A maioria dos servidores remotos de sistema operacional de rede é compatível com PAP.**

**CHAP (Challenge Handshake Authentication Protocol)**

**CHAP valida a identidade de clientes remotos usando uma função de hash unidirecional criada pelo cliente. O serviço também calcula o valor esperado de hash. O servidor (o autenticador) compara os dois valores. Se os valores corresponderem, a transmissão continua. CHAP também verifica periodicamente a identidade do cliente durante a transmissão.**

**802.1x**

**Uma empresa autentica sua identidade e autoriza o acesso à rede. Sua identidade é determinada com base em credenciais ou em um certificado confirmado por um servidor RADIUS.**

**RADIUS**

**Quando a autenticação simples de nome de usuário/senha for necessária, use RADIUS para aceitar ou negar acesso. RADIUS criptografa apenas a senha do usuário do cliente RADIUS para o servidor RADIUS. O nome de usuário, a contabilidade e os serviços autorizados são transmitidos em texto não criptografado. Quando o RADIUS é integrado a um produto, são necessárias medidas de segurança que protegem contra ataques de repetição.**

**TACACS+**

**TACACS + usa TCP como protocolo de transporte. TACACS + criptografa todos os dados (nome de usuário, senha, contabilidade e serviços autorizados) entre o cliente e o servidor. Como os administradores de rede podem definir ACLs, filtros e privilégios de usuário, TACACS + é a melhor escolha para redes corporativas que exigem etapas de autenticação mais sofisticadas e controle sobre atividades de autorização.**

**Kerberos**

**Kerberos usa criptografia forte, solicitando que um cliente comprove sua identidade para um servidor, com o servidor, por sua vez, se autenticando no cliente.**

**O servidor Kerberos contém IDs de usuário e senhas com hash para todos os usuários que terão autorizações para serviços de região. O servidor Kerberos também tem chaves secretas compartilhadas com todos os servidores aos quais concederá tíquetes de acesso. A base para a autenticação em um ambiente Kerberos é o tíquete. Os tíquetes são usados em um processo de duas etapas com o cliente. O primeiro tíquete é um tíquete de concessão de tíquete emitido pelo serviço de autenticação para um cliente solicitante. O cliente pode então apresentar esse tíquete ao servidor Kerberos com uma solicitação de tíquete para acessar um servidor específico.**

**Esse tíquete do cliente para o servidor (também conhecido como tíquete de serviço) é usado para obter acesso ao serviço de um servidor. Como toda a sessão pode ser criptografada, isso elimina a transmissão inerentemente insegura de itens (como senhas) que podem ser interceptados na rede. Os tickets têm o carimbo de hora e expiram, portanto, qualquer tentativa de reutilização de um ticket não será bem-sucedida.**

**3.3.13 Aplicações de Funções de Hash Criptográficas**

* **Para fornecer prova de autenticidade quando usado com uma chave de autenticação secreta simétrica, como segurança IP (IPsec) ou autenticação de protocolo de roteamento.**
* **Fornecer autenticação gerando respostas únicas e unidirecionais aos desafios nos protocolos de autenticação.**
* **Para fornecer prova de verificação de integridade da mensagem (como os usados em contratos assinados digitalmente) e certificados de infraestrutura de chave pública (PKI) (como os aceitos ao acessar um site seguro).**

**Ao escolher um algoritmo de hash, use o SHA-256 ou superior, pois são os mais seguros atualmente. Evite SHA-1 e MD5 devido a falhas de segurança que foram descobertas.**

**3.3.15 Estratégias de controle de acesso**

**Controle de acesso obrigatório**

**O controle de acesso obrigatório restringe as ações que um usuário pode realizar em um objeto (como um arquivo, uma porta ou um dispositivo). Uma regra de autorização impõe se um usuário pode acessar o objeto.**

**As organizações usam o controle de acesso obrigatório onde existem diferentes níveis de classificações de segurança. Cada objeto tem uma etiqueta e cada usuário tem uma autorização. Um sistema de controle de acesso obrigatório restringe um usuário com base na classificação de segurança do objeto e na etiqueta anexada ao usuário.**

**Controle de acesso discricionário**

**Em sistemas que empregam controles de acesso discricionários, o proprietário de um objeto pode decidir quais usuários podem acessar esse objeto e qual acesso específico eles podem ter.**

**Permissões e listas de controle de acesso podem ser usadas para implementar o controle de acesso discricionário. O proprietário de um arquivo pode especificar quais permissões (como ler, gravar ou executar) outros usuários podem ter. Uma lista de controle de acesso usa regras para determinar qual tráfego pode entrar ou sair de uma rede.**

**Controle de acesso por função**

**O controle de acesso baseado em função depende da função ou função de trabalho do usuário. Funções específicas exigem permissões para executar determinadas operações e os usuários adquirem permissões por meio de sua função.**

**O controle de acesso por função pode funcionar em combinação com controles de acesso discricionários ou obrigatórios, aplicando as políticas de qualquer um deles. O controle de acesso baseado em função ajuda a implementar a administração de segurança em grandes organizações com centenas de usuários e milhares de permissões possíveis. As organizações aceitam amplamente o uso de controle de acesso baseado em função para gerenciar permissões de computador em um sistema ou aplicativo como uma prática recomendada.**

**Controle de acesso baseado em regras**

**O controle de acesso baseado em regras usa listas de controle de acesso para ajudar a determinar se o acesso deve ser concedido. Uma série de regras está contida na lista de controle de acesso e a decisão de conceder acesso depende dessas regras. Por exemplo, uma regra que determina que nenhum funcionário pode ter acesso ao arquivo da folha de pagamento fora do expediente ou nos finais de semana.**

**Assim como no controle de acesso obrigatório, os usuários não podem alterar as regras de acesso. É importante ressaltar que as organizações podem combinar o controle de acesso baseado em regras com outras estratégias para implementar restrições de acesso. Por exemplo, métodos obrigatórios de controle de acesso podem utilizar uma abordagem baseada em regras para implementação.**

**3.4.1 Operação AAA**

**Autenticação**

* **Os usuários e administradores devem provar quem são.**
* **A autenticação pode ser estabelecida usando combinações de nome de usuário e senha, perguntas e respostas de desafio, tokens e outros métodos.**
* **A autenticação AAA fornece uma maneira centralizada de controlar o acesso à rede.**

**Autorização**

* **Após a autenticação do usuário, os serviços de autorização determinam quais recursos o usuário pode acessar e quais operações ele tem permissão para executar.**
* **Um exemplo é "O usuário 'aluno' pode acessar o servidor host XYZ usando apenas SSH".**

**Accounting (Contabilidade)**

* **O accounting registra o que o usuário faz, incluindo o que é acessado, a quantidade de tempo em que o recurso é acessado e todas as alterações efetuadas.**
* **O accounting rastreia como os recursos de rede são usados.**
* **Um exemplo é "O usuário 'aluno' acessou o servidor host XYZ usando SSH por 15 minutos".**

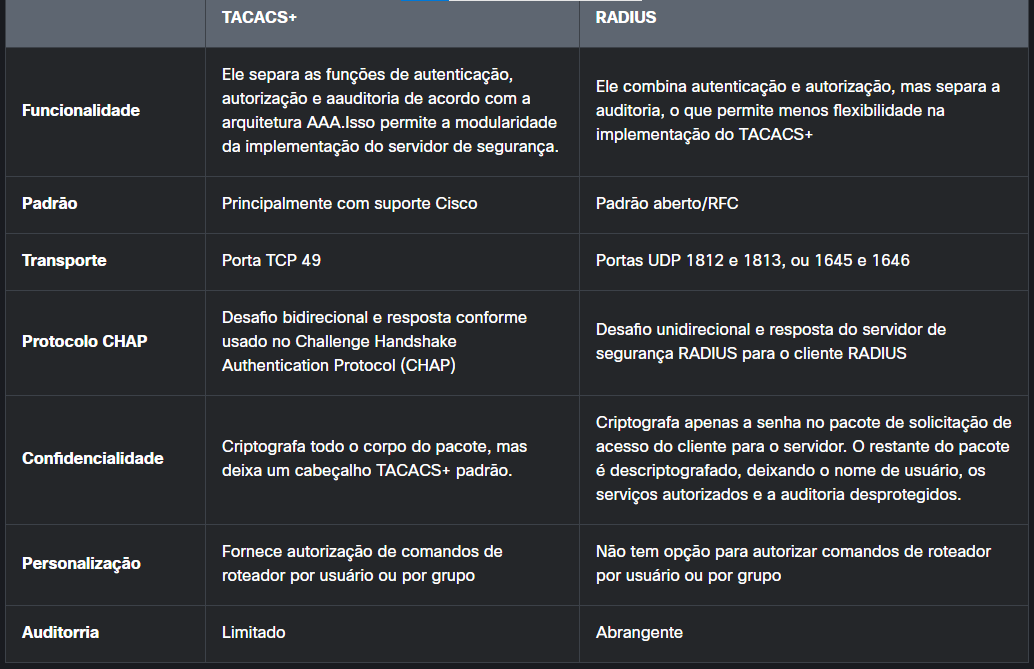
**3.4.2 autenticação AAA**

**Autenticação de AAA local**

**Esse método às vezes é conhecido como autenticação autônoma porque autentica usuários contra nomes de usuário e senhas armazenados localmente, como mostrado na figura. O AAA local é ideal para redes pequenas.**

**Autenticação de AAA com base em servidor**

**Esse método se autentica em um servidor AAA central que contém os nomes de usuário e senhas para todos os usuários, conforme mostrado na figura. A autenticação AAA baseada em servidor é apropriada para redes de médio a grande porte.**

****

**3.4.3 Registros de Contabilidade AAA**

**O AAA centralizado também permite o uso do método de contabilidade. Os registros contábeis de todos os dispositivos são enviados para repositórios centralizados, o que simplifica a auditoria das ações do usuário.**

**AAA Accounting coleta e relata dados de uso em registros AAA. Esses logs são úteis para auditoria de segurança. Os dados coletados podem incluir os horários de conexão inicial e final, comandos executados, número de pacotes e número de bytes.**

**Um uso amplamente difundido da contabilidade é combiná-lo com a autenticação AAA. Isso ajuda a gerenciar o acesso a dispositivos de interrede pela equipe administrativa da rede.**

1. **Quando um usuário realiza autenticação, o processo de contabilização AAA gera uma mensagem inicial para iniciar a contabilização.**
2. **Quando o usuário termina, uma mensagem de parada é inserida e o processo contábil finaliza.**

**Contabilidade de Rede**

**A contabilidade de rede captura informações para todas as sessões PPP (Point-to-Point Protocol), incluindo contagens de pacotes e bytes.**

**Contabilidade de Conexão**

**Contabilidade de conexão captura informações sobre todas as conexões de saída feitas a partir do cliente AAA, como por SSH.**

**Contabilidade EXEC**

**A contabilidade EXEC captura informações sobre sessões de terminal EXEC do usuário (shells do usuário) no servidor de acesso à rede, incluindo nome de usuário, data, horas de início e parada e o endereço IP do servidor de acesso**

**Contabilidade do Sistema**

**A contabilidade do sistema captura informações sobre todos os eventos no nível do sistema (por exemplo, quando o sistema é reinicializado ou quando a contabilidade é ativada ou desativada).**

**Contabilidade de Comando**

**A contabilidade de comandos captura informações sobre os comandos do shell EXEC para um nível de privilégio especificado, bem como a data e hora em que cada comando foi executado e o usuário que o executou.**

**Contabilidade de Recursos**

**A implementação da Cisco de contabilidade AAA captura o suporte de registro de “iniciar” e “parar” para conexões que passaram pela autenticação do usuário. O recurso adicional de geração de registros de “parada” para conexões que falham na autenticação como parte da autenticação do usuário também é suportado. Esses registros são necessários para que os usuários que empregam registros contábeis gerenciem e monitorem suas redes.**

**Contabilidade de Recursos**

**A implementação da Cisco de contabilidade AAA captura o suporte de registro de “iniciar” e “parar” para conexões que passaram pela autenticação do usuário. O recurso adicional de geração de registros de “parada” para conexões que falham na autenticação como parte da autenticação do usuário também é suportado. Esses registros são necessários para que os usuários que empregam registros contábeis gerenciem e monitorem suas redes.**

**Contabilidade**

**Usa um conjunto criado de atributos que descreve o acesso do usuário à rede**

**autorização**

**Estabelecido usando combinações de nome de usuário e senha, perguntas de desafio e resposta, cartões de token e outros métodos**

**Autenticação**

**Coleta e relata dados de uso para que possam ser utilizados para fins como auditoria ou faturamento**

**Contabilidade**

**Os usuários e administradores devem provar que são quem dizem ser**

**Auteticação**

**O que um usuário pode e não pode fazer na rede**

**Autorização**

**Quais recursos o usuário pode acessar e quais operações o usuário tem permissão para realizar**

**Autorização**

**Fornece alavancagem contra indivíduos que executam ações mal**

**Contabilidade**

**Uma forma de controlar quem tem permissão para acessar uma rede**

**Autenticação**

**4.1.1 O que é uma ACL?**

Os roteadores tomam decisões de roteamento com base nas informações no cabeçalho do pacote. O tráfego que entra na interface do roteador é roteado apenas com base nas informações da tabela de roteamento. O roteador compara o endereço IP de destino com as rotas na tabela de roteamento para encontrar a melhor correspondência e, em seguida, encaminha o pacote com base na melhor rota de correspondência. Esse mesmo processo pode ser usado para filtrar tráfego usando uma lista de controle de acesso (ACL).

Uma ACL é uma série de comandos do IOS usados para filtrar pacotes com base nas informações encontradas no cabeçalho do pacote. Por padrão, um roteador não tem nenhuma ACLs configurada. Entretanto, quando uma ACL for aplicada a uma interface, o roteador executará a tarefa adicional de avaliar todos os pacotes de rede que passam pela interface para determinar se o pacote pode ser enviado.

Uma ACL usa uma lista sequencial de instruções de permissão ou negação, conhecidas como entradas de controle de acesso (ACEs).

**Nota**: As ACEs também são comumente chamadas de declarações da ACL.

Quando o tráfego da rede passa através de uma interface configurada com uma ACL, o roteador compara as informações no pacote com cada ACE, em ordem sequencial, para determinar se o pacote corresponde a uma das ACEs. Esse processo é chamado de filtragem de pacote.

Limitam o tráfego e aumentam o desempenho da rede

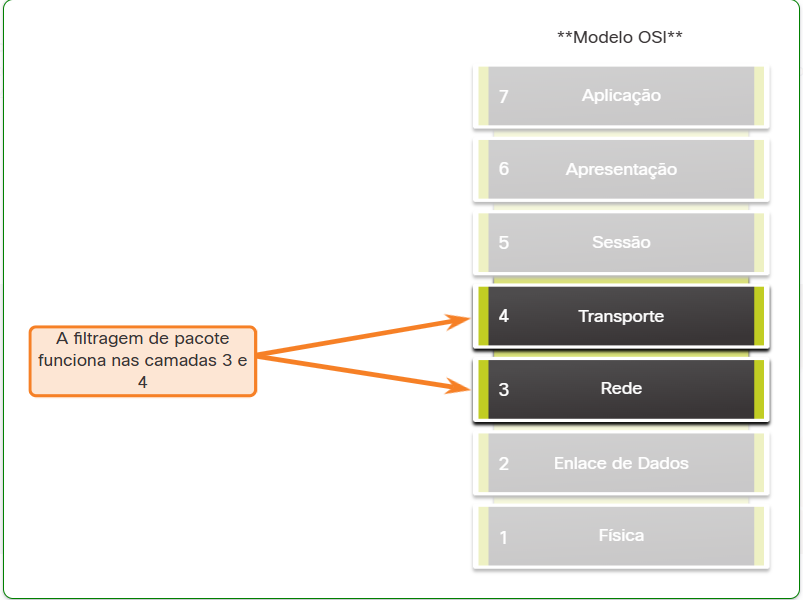
* Uma política corporativa proíbe o tráfego de vídeo na rede para reduzir a carga da rede.
* Uma política pode ser aplicada usando ACLs para bloquear o tráfego de vídeo.

Fornecer prioridade a determinadas classes de tráfego de rede

* O tráfego corporativo especifica que o tráfego de voz seja encaminhado o mais rápido possível para evitar qualquer interrupção.
* Uma política pode ser implementada usando serviços ACLs e QoS para identificar o tráfego de voz e processá-lo imediatamente.

4.1.2 Filtragem de pacote:

A filtragem de pacotes controla o acesso a uma rede analisando os pacotes de entrada e / ou saída e encaminhando-os ou descartando-os com base nos critérios fornecidos. A filtragem de pacotes pode ocorrer na camada 3 ou camada 4, como mostrado na figura.

****

* **ACLs padrão** - As ACLs filtram apenas na Camada 3 usando apenas o endereço IPv4 de origem.
* **ACLs estendidas** - Os ACLs filtram na Camada 3 usando o endereço IPv4 de origem e / ou destino. Eles também podem filtrar na Camada 4 usando TCP, portas UDP e informações de tipo de protocolo opcional para controle mais fino.

4.1.3 ACLs nomeadas e numeradas

**ACLs numeradas**

ACLs número 1 a 99, ou 1300 a 1999 são ACLs padrão, enquanto ACLs número 100 a 199, ou 2000 a 2699 são ACLs estendidas, conforme mostrado na saída.

**ACLs nomeadas**

ACLs nomeadas é o método preferido a ser usado ao configurar ACLs. Especificamente, as ACLs padrão e estendidas podem ser nomeadas para fornecer informações sobre a finalidade da ACL. Por exemplo, nomear uma ACL FTP-FILTER estendida é muito melhor do que ter uma ACL 100 numerada.

O comando **ip access-list** na configuração global é usado para criar uma ACL nomeada, como mostrado no exemplo a seguir.

O seguinte resume as regras a seguir para ACLs nomeadas:

* Atribua um nome para identificar o objetivo da ACL.
* Os nomes podem conter caracteres alfanuméricos.
* Os nomes não podem conter espaços ou pontuação.
* Sugerimos que o nome seja escrito em LETRAS MAIÚSCULAS.
* É possível adicionar ou excluir entradas na ACL.

**Nota**: ACLs não atuam em pacotes originados do próprio roteador.

Uma ACL de entrada filtra pacotes antes de serem roteados para a interface de saída. Uma ACL de entrada é eficiente porque salva a sobrecarga de pesquisas de roteamento se o pacote é descartado. Se o pacote for permitido pela ACL, ele será processado para roteamento. As ACLs de entrada são mais usadas para filtrar pacotes quando a rede conectada a uma interface de entrada é a única origem dos pacotes que precisa ser examinada.

Uma ACL de saída filtra pacotes após seu roteamento, independentemente da interface de entrada. Pacotes de entrada são roteados para a interface de saída e são processados através da ACL de saída. As ACLs de saída são mais usadas quando o mesmo filtro é aplicado aos pacotes que vêm de várias interfaces de entrada antes de saírem da mesma interface de saída.

Quando uma ACL é aplicada a uma interface, ela segue um procedimento operacional específico. Por exemplo, aqui estão as etapas operacionais usadas quando o tráfego entrou em uma interface de roteador com uma ACL IPv4 configurada no padrão de entrada .

1. O roteador extrai o endereço IPv4 de origem do cabeçalho do pacote.
2. O roteador inicia na parte superior da ACL e compara o endereço IPv4 de origem a cada ACE em uma ordem sequencial.
3. Quando houver correspondência, o roteador realizará a instrução, permitindo ou negando o pacote.
4. Se o endereço IPv4 de origem não corresponder a nenhuma ACEs na ACL, o pacote será descartado porque há uma ACE de negação implícita aplicada automaticamente a todas as ACLs.

A última instrução ACE de uma ACL é sempre uma negação implícita que bloqueia todo o tráfego. Por padrão, essa instrução é automaticamente implícita no final de uma ACL, mesmo que esteja oculta e não exibida na configuração.

**Nota**: Uma ACL deve ter pelo menos uma declaração de permissão, caso contrário, todo o tráfego será negado devido à declaração de negação ACE implícita.

**4.2.1 Visão geral da máscara curinga**

**No tópico anterior, você aprendeu sobre o propósito dos ACLs. Este tópico explica como os ACLs usam máscaras curingas. Uma ACE IPv4 usa uma máscara curinga de 32 bits para determinar quais bits do endereço examinar para uma correspondência. As máscaras curinga também são usadas pelo protocolo de roteamento Open Shortest Path First (OSPF).**

**Uma máscara curinga é semelhante a uma máscara de sub-rede na vez que usa o processo de ANDing para identificar quais bits em um endereço IPv4 devem corresponder. No entanto, eles diferem na forma como combinam 1s e Os binários. Diferente de uma máscara de sub-rede, na qual o binário 1 é igual a uma correspondência e o binário 0 não é uma correspondência, em uma máscara curinga, o inverso é verdadeiro.**

**As máscaras curinga utilizam as seguintes regras para corresponder ao binário 1s e Os:**

**Máscara curinga bit 0 - Corresponde ao valor do bit correspondente no endereço**

**Máscara curinga bit 1 - Ignora o valor do bit correspondente no endereço**

**A tabela lista alguns exemplos de máscaras curinga e o que eles identificariam.**

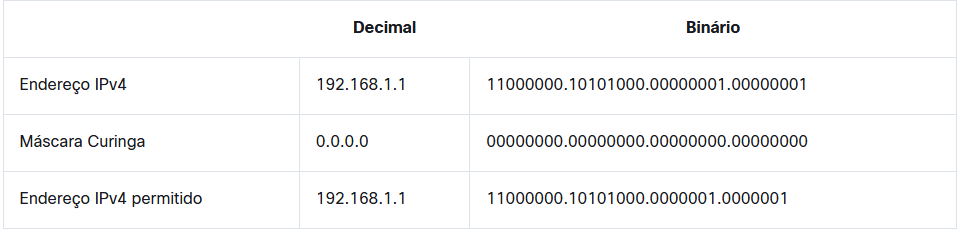
****

**Curinga para corresponder a um host**

Neste exemplo, a máscara curinga é usada para corresponder a um endereço IPv4 de host específico. Suponha que a ACL 10 precisa de uma ACE que permita apenas o host com endereço IPv4 192.168.1.1. Lembre-se que “0” é igual a uma correspondência e “1” é igual a ignorar. Para corresponder a um endereço IPv4 de host específico, é necessária uma máscara curinga que consiste em todos os zeros (ou seja, 0.0.0.0).

A tabela lista em binário, o endereço IPv4 do host, a máscara curinga e o endereço IPv4 permitido.

A máscara curinga 0.0.0.0 estipula que cada bit deve corresponder exatamente. Portanto, quando a ACE é processada, a máscara curinga permitirá apenas o endereço 192.168.1.1. A ACE resultante na ACL 10 seria **access-list 10 permit 192.168.1.1 0.0.0.0**.



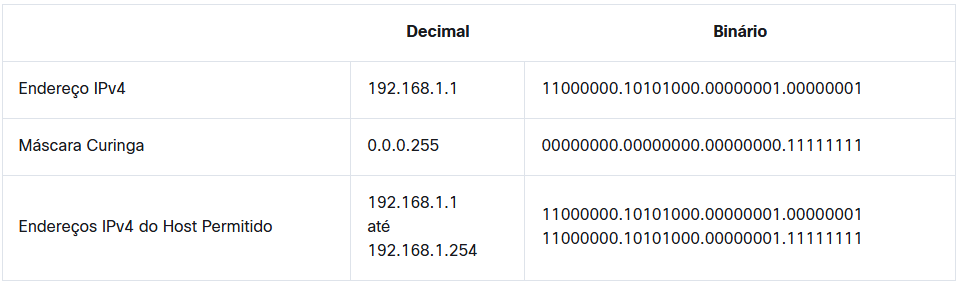
**Máscara curinga para corresponder a uma sub-rede IPv4**

**Máscara curinga para corresponder a uma sub-rede IPv4**

**Neste exemplo, a ACL 10 precisa de uma ACE que permita todos os hosts na rede 192.168.1.0/24. A máscara curinga 0.0.0.255 estipula que os três primeiros octetos devem corresponder exatamente, mas o quarto octeto não.**

**A tabela lista em binário, o endereço IPv4 do host, a máscara curinga e os endereços IPv4 permitidos.**

**Quando processado, a máscara curinga 0.0.0.255 permite todos os hosts na rede 192.168.1.0/24. A ACE resultante na ACL 10 seria a lista de acesso 10 permitir 192.168.1.0 0.0.255.**

****

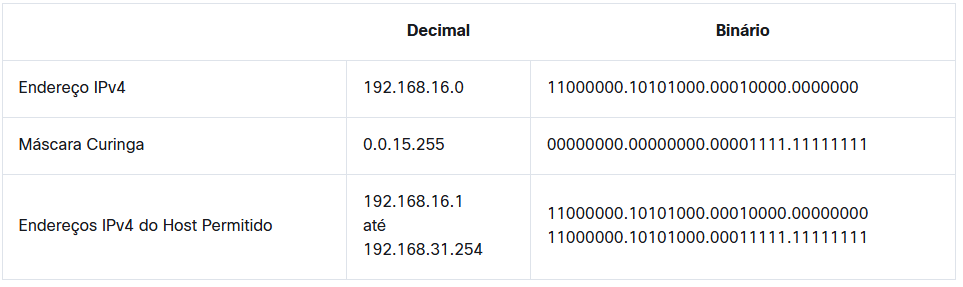
**Máscara curinga para corresponder a um intervalo de endereços IPv4**

**Máscara curinga para corresponder a um intervalo de endereços IPv4**

**Neste exemplo, a ACL 10 precisa de uma ACE que permita todos os hosts nas redes 192.168.16.0/24, 192.168.17.0/24,..., 192.168.31.0/24. A máscara curinga 0.0.15.255 filtraria corretamente esse intervalo de endereços.**

**A tabela lista em binário o endereço IPv4 do host, a máscara curinga e os endereços IPv4 permitidos.**

**Os bits de máscara curinga realçados identificam quais bits do endereço IPv4 devem corresponder. Quando processada, a máscara curinga 0.0.15.255 permite que todos os hosts nas redes 192.168.16.0/24 a 192.168.31.0/24. A ACE resultante na ACL 10 seria access-list 10 permit 192.168.16.0 0.0.15.255.**

****

**4.2.3 Cálculo da máscara curinga**

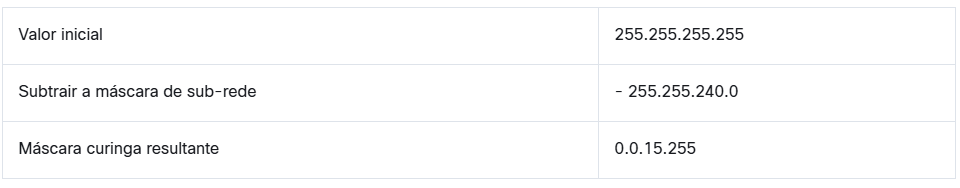
**Calcular as máscaras curinga pode ser um desafio. Um método de atalho é subtrair a máscara de sub-rede de 255.255.255.255. Consulte os exemplos para saber como calcular a máscara curinga usando a máscara de sub-rede.**

**Exemplo 4**

**Exemplo 4**

**Considere um exemplo no qual você precisa de um número de ACL 10 para corresponder a redes no intervalo entre 192.168.16.0/24 e 192.168.31.0/24. Esse intervalo de rede pode ser resumido como 192.168.16.0/20, que é uma máscara de sub-rede de 255.255.240.0. Portanto, subtraia 255.255.240.0 máscara de sub-rede de 255.255.255.255, conforme mostrado na tabela.**

**Esta solução produz a máscara curinga 0.0.15.255. Portanto, o ACE seria access-list 10 permit 192.168.3.0 0.0.0.255.**

****

**4.2.4 Palavras-chave de máscara curinga**

**Trabalhar com representações decimais de bits binários de máscara curinga pode ser entediante. Para simplificar esta tarefa, o Cisco IOS fornece duas palavras-chave para identificar os usos mais comuns do mascaramento de curinga. As palavras-chave reduzem os pressionamentos de teclas da ACL, mas, mais importante, as palavras-chave facilitam a leitura da ACE.**

**As duas palavras-chave são:**

* **host - Esta palavra-chave substitui a máscara 0.0.0.0. Essa máscara indica que todos os bits do endereço IPv4 precisam corresponder para filtrar apenas um endereço de host.**
* **any- Esta palavra-chave substitui a máscara 255.255.255.255. Essa máscara instrui o sistema a ignorar todo o endereço IPv4 ou a aceitar qualquer endereço.**

****

**4.3.1 Criar uma ACL**

* **Use um editor de texto e escreva as especificidades da política a ser implementada.**
* **Adicione os comandos de configuração do IOS para realizar essas tarefas.**
* **Incluir observações para documentar a ACL.**
* **Copie e cole os comandos no dispositivo.**
* **Sempre teste minuciosamente uma ACL para garantir que ela aplica corretamente a política desejada.**

**4.3.2 Sintaxe numerada da ACL IPv4 padrão**

**Para criar uma ACL padrão numerada, use o seguinte comando de configuração global:**

**Router(config)# access-list *access-list-number* {deny | permit | remark *text*} *source* [*source-wildcard*] [log]**

**Utilize os comandos de configuração global no access-list *access-list-number* para remover a ACL padrão numerada.**

|  |  |
| --- | --- |
| **Parâmetro** | |
| **access-list-number**   * **Este é o número decimal da ACL.** * **O intervalo de números ACL padrão é de 1 a 99 ou 1300 a 1999.** | |
| **Deny**  **Isto nega o acesso se as condições corresponderem.** | |
| **Permit**  **Isto permite o acesso se as condições corresponderem.** | |
| **remark text**   * **(Opcional) Isso adiciona uma entrada de texto para fins de documentação.** * **Comentários são extremamente úteis, especialmente em ACLs mais longas ou mais complexas.** * **Cada comentário é limitada a 100 caracteres.** | |
| **Source**   * **Isto identifica o endereço de origem de host ou de rede a ser filtrado.** * **Usar a palavra-chave any para especificar todas as redes.** * **Usar a palavra-chave host com o *ip-address*, ou simplesmente digitar o *ip-address* (sem a palavra-chave host) para identificar um endereço IP específico.** | |
| **source-wildcard**  **(Opcional) Esta é uma máscara curinga de 32 bits aplicadas à origem. Se omitida, uma máscara padrão 0.0.0.0 é assumida.** | |
| **Log**   * **(Opcional) Esta palavra-chave gera uma mensagem informacional sempre que a ACE dá combinação.** * **A mensagem inclui o número da ACL, a condição correspondida (ex: permitido ou negado), endereço de origem e número de pacotes.** * **Esta mensagem é gerada para o primeiro pacote correspondido.** * **Infelizmente, o registro de atividades da ACL pode utilizar intesivamente a CPU e afetar negativamente outras funções, portanto, deve ser implementado apenas para solução de problemas ou por razões de segurança.** | |
|  | |

**4.3.3 Sintaxe nomeada da ACL IPv4 padrão**

**Nomear uma ACL facilita entender sua função. Para criar uma ACL padrão nomeada, use o seguinte comando de configuração global:**

**Router(config)# ip access-list standard *access-list-name***

**Os nomes das ACLs são alfanuméricos, diferenciam maiúsculas de minúsculas e devem ser exclusivos.**

**Nota: Use o comando no ip access-list standard access-list-name global configuration para remover uma ACL IPv4 padrão nomeada.**

**No exemplo, é criada uma ACL IPv4 padrão denominada NO-ACCESS. Observe que o prompt muda para o modo de configuração de ACL padrão nomeado. As instruções ACE são inseridas no modo de subconfiguração ACL padrão nomeado. Use o recurso de ajuda para exibir todas as opções de ACL padrão nomeadas.**

**As três opções realçadas são configuradas de forma semelhante à ACL padrão numerada. Ao contrário do método ACL numerado, não há necessidade de repetir o comando ip access-list para cada ACE.**

**R1(config)# ip access-list standard NO-ACCESS**

**R1(config-std-nacl)# ?**

**Standard Access List configuration commands:**

**<1-2147483647> Sequence Number**

**default        Set a command to its defaults**

**deny           Specify packets to reject**

**exit           Exit from access-list configuration mode**

**no             Negate a command or set its defaults**

**permit         Specify packets to forward**

**remark         Access list entry comment**

**R1(config-std-nacl)#**

**4.3.4 Sintaxe numerada da ACL IPv4 padrão**

**As etapas de procedimentos para configurar ACLs estendidas são as mesmas usadas para ACL padrão. ACL estendida é configurada em primeiro lugar e é ativada em uma interface. No entanto, a sintaxe de comandos e os parâmetros são mais complexos para suportar recursos adicionais fornecidos pelas ACLs estendidas.**

**Para criar uma ACL estendida numerada, use o seguinte comando de configuração global:**

**Router(config)# access-list *access-list-number* {deny | permit | remark *text*} *protocol source source-wildcard* [ *operator* {*port*}] *destination destination-wildcard* [*operator* {*port*}] [established] [log]**

**Use o comando de configuração global no access-list *access-list-number* remover uma ACL estendida.**

**Embora existam muitas palavras-chave e parâmetros para ACLs estendidas, não é necessário usá-las ao configurar uma ACL estendida. A tabela fornece uma explicação detalhada da sintaxe para uma ACL estendida.**

|  |  |
| --- | --- |
| **Parâmetro** | **Descrição** |
| **access-list-number**   * **Este é o número decimal da ACL.**   **O número do intervalo da ACL Extendida é de 100 à 199 e 2000 à 2699.** |  |
| **Deny**  **Isto nega o acesso se as condições corresponderem.** |  |
| **Permit**  **Isto permite o acesso se as condições corresponderem.** |  |
| **remark text**   * **(Opcional) Isso adiciona uma entrada de texto para fins de documentação.**   **Cada comentário é limitada a 100 caracteres.** |  |
| **Protocol**   * **Nome ou número de um protocolo da internet.** * **Palavras-chave comuns incluem ip, tcp, udp, e icmp.**   **A palavra-chave ip dá combinação com todos os protocolos IP.** |  |
| **Source**   * **Isto identifica o endereço de origem de host ou de rede a ser filtrado.** * **Usar a palavra-chave any para especificar todas as redes.**   **Usar a palavra-chave host com o ip-address keyword ou simplesmente digitar o ip-address (sem a palavra-chave host) para identificar um endereço IP específico.** |  |
| **source-wildcard**  **(Opcional) Esta é uma máscara curinga de 32 bits que é aplicada à origem.** |  |
| **destination-wildcard**  **(Opcional) Esta é uma máscara curinga de 32 bits que é aplicada ao destino.** |  |
| **Destination**   * **Isto identifica o endereço de destino de host ou de rede.** * **Usar a palavra-chave any para especificar todas as redes.**   **Usar a palavra-chave host*ip-address* ou apenas*ip-address*.** |  |
| **Established**   * **(Opcional) Somente para o protocolo TCP.**   **Este é um recurso de firewall de primeira geração.** |  |
| **Port**  **(Opcional) O número decimal ou o nome de uma porta TCP ou UDP.** |  |
| **Operator**   * **(Opcional) Isto compara as portas de origem ou de destino.**   **Alguns operadores incluem lt (menor que), gt (maior que), eq (igual), e neq (diferente).**  **Log**   * **(Opcional) Esta palavra-chave gera uma mensagem informacional sempre que a ACE dá combinação.** * **A mensagem inclui o número da ACL, a condição correspondida (ex: permitido ou negado), endereço de origem e número de pacotes.** * **A mensagem inclui o número da ACL, a condição correspondida (ex: permitido ou negado), endereço de origem e número de pacotes.** * **Esta mensagem é gerada para o primeiro pacote correspondido.**   **Esta palavra-chave deve apenas ser implementado apenas para solução de problemas ou por razões de segurança.** |  |
|  |  |

**O comando para aplicar uma ACL IPv4 estendida a uma interface é o mesmo que o comando usado para ACLs IPv4 padrão.**

**Router(config-if)# ip access-group {*access-list-number* | *access-list-name*} {in | out}**

**Para remover uma ACL em uma interface, primeiro digite o comando no ip access-group na interface. Para remover a ACL do roteador, use o comando de configuração global no access-list .**

**Nota: A lógica interna aplicada à ordenação de instruções ACL padrão não se aplica a ACLs estendidas. A ordem em que as instruções são fornecidas durante a configuração é ordem em que são exibidas e processadas.**

**4.3.5 Protocolos e números de porta**

**Opções de Protocolo**

**Opções de Protocolo**

**Os quatro protocolos destacados são as opções mais populares.**

**Nota: Use a ? para obter ajuda ao inserir uma ACE mais complexa.**

**Note: Se um protocolo da internet não estiver listado, o número do protocolo IP pode ser especificado. Por exemplo, o protocolo ICMP usa o número 1, TCP é 6 e UDP é 17.**

**R1(config)# access-list 100 permit ?**

**Opções de palavra-chave da porta**

**Selecionar um *protocolo* influencia as opções de*porta*. Por exemplo, selecionando a opção:**

* **tcp protocol forneceria opções de portas relacionadas ao TCP**
* **udp protocol forneceria opções de portas relacionadas ao UDP**
* **icmp protocol forneceria opções de portas relacionadas ao ICMP (ex: tipo de mensagem)**

**Novamente, observe quantas opções de porta TCP estão disponíveis. As portas destacadas são opções populares.**

**Nomes de porta ou número podem ser especificados. No entanto, os nomes de portas facilitam a compreensão do propósito de uma ACE. Observe como alguns nomes de portas comuns (por exemplo, ssh e https) não estão listados. Para estes protocolos, os números de porta terão que ser especificados.**

**R1(config)# access-list 100 permit tcp any any eq ?**

**4.3.6 Exemplos de configuração de protocolos e números de porta**

**As ACLs estendidas podem filtrar em diferentes opções de número de porta e nome de porta. Este exemplo configura uma ACL 100 estendida para filtrar tráfego HTTP. A primeira ACE usa o nome da porta www. O segundo ACE usa o número da porta 80. Ambos os ACEs atingem exatamente o mesmo resultado.**

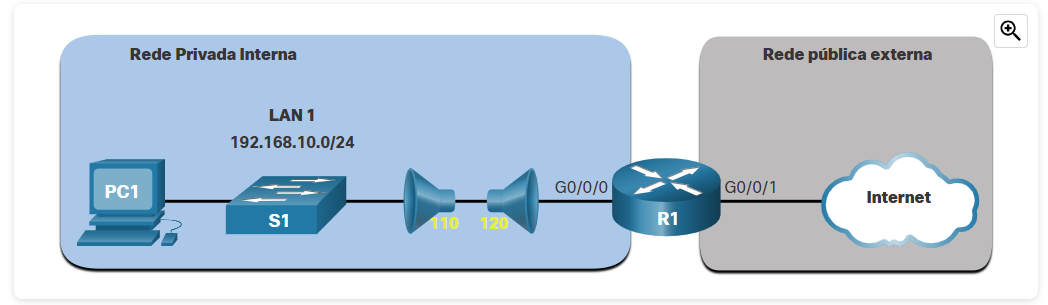
**R1(config)# access-list 100 permit tcp any any eq www**

**R1(config)# !or...**

**R1(config)# access-list 100 permit tcp any any eq 80**

**4.3.7 ACL estendida estabelecida TCP**

**O TCP também pode executar serviços básicos de firewall stateful usando a palavra-chave TCP stablished. A palavra-chave permite que o tráfego interno saia da rede privada interna e permite que o tráfego de resposta retornado entre na rede privada interna, como mostrado na figura.**

****

**No exemplo, a ACL 120 está configurada para permitir apenas o retorno do tráfego da Web para os hosts internos. A nova ACL é então aplicada de saída na interface R1 G0/0/0. O comando show access-lists exibe ambos os ACLs. Observe a partir das estatísticas de correspondência que dentro de hosts têm acessado os recursos da Web seguros a partir da Internet.**

**R1(config)# access-list 100 permit tcp any any eq 22**

**R1(config)# access-list 100 permit tcp any any eq 443**

**R1(config)#**

**R1(config)# access-list 120 permit tcp any 192.168.10.0 0.0.0.255 established**

**R1(config)# interface g0/0/0**

**R1(config-if)# ip access-group 120 out**

**R1(config-if)# end**

**R1# show access-lists**

**Extended IP access list 110**

**10 permit tcp 192.168.10.0 0.0.0.255 any eq www**

**20 permit tcp 192.168.10.0 0.0.0.255 any eq 443 (657 matches)**

**Extended IP access list 120**

**10 permit tcp any 192.168.10.0 0.0.0.255 established (1166 matches)**

**R1#**

**Observe que os contadores HTTPS seguros de permissão (ou seja, eq 443) na ACL 110 e os contadores estabelecidos de retorno na ACL 120 aumentaram.**

**O parâmetro established permite que apenas as respostas para o tráfego originário da rede 192.168.10.0/24 retornem a essa rede. Especificamente, uma correspondência ocorre se o segmento TCP retornando tem os bits de sinalizador ACK ou redefinir (RST) definido. Isso indica que o pacote pertence a uma conexão existente. Sem o parâmetro established na instrução ACL, os clientes poderiam enviar tráfego para um servidor da Web e receber tráfego retornando do servidor da Web. Todo o tráfego seria permitido.**

**4.3.8 Sintaxe da ACL IPv4 estendida nomeada**

**Nomear uma ACL facilita entender sua função. Para criar uma ACL estendida nomeada, use o seguinte comando de configuração global:**

**Router(config)# ip access-list extended *access-list-name***

**Este comando entra no modo de configuração estendida nomeado. Os nomes das ACLs são alfanuméricos, diferenciam maiúsculas de minúsculas e devem ser exclusivos.**

**No exemplo, uma ACL estendida nomeada chamada NO-FTP-ACCESS é criada e o prompt foi alterado para o modo de configuração de ACL estendida nomeada. As instruções ACE são inseridas no modo de subconfiguração de ACL estendida nomeado.**

**R1(config)# ip access-list extended NO-FTP-ACCESS**

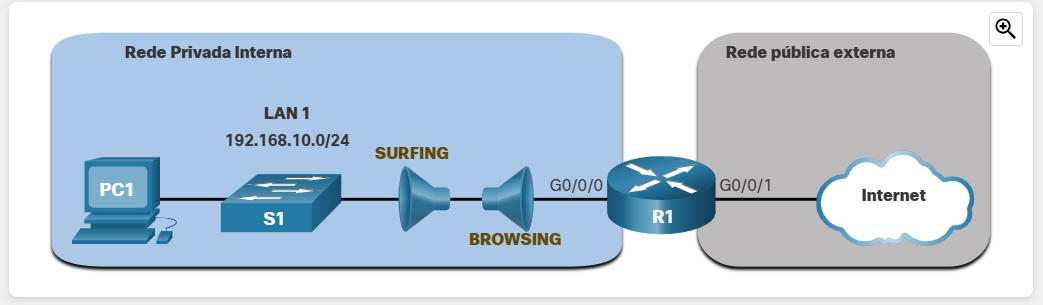
**R1(config-ext-nacl)#**

**4.3.9 Exemplo de ACL IPv4 estendida nomeada**

**As ACLs estendidas nomeadas são criadas essencialmente da mesma forma que as ACL padrão.**

**A topologia na figura é usada para demonstrar a configuração e aplicação de duas ACLs IPv4 estendidas nomeadas a uma interface:**

* **SURFING - Isso permitirá que o tráfego HTTP e HTTPS saia para a Internet.**
* **BROWSING - Isso só permitirá retornar tráfego da Web para os hosts internos enquanto todo o tráfego que sai da interface R1 G0/0/0 for negado implicitamente.**

****

**O exemplo mostra a configuração para a ACL de SURFING de entrada e a ACL de BROWSING de saída.**

**A ACL SURFING permite que o tráfego HTTP e HTTPS de usuários internos saia da interface G0 / 0/1 conectada à Internet. O tráfego da Web retornando da Internet é permitido de volta para a rede privada interna pela ACL de navegação.**

**A ACL SURFING é aplicada de entrada e a ACL BROWSING aplicada de saída na interface R1 G0/0/0/0, conforme mostrado na saída.**

**Os hosts internos têm acessado os recursos da Web seguros da Internet. O comando show access-lists é usado para verificar as estatísticas de ACL. Observe que os contadores HTTPS seguros de permissão (ou seja, eq 443) na ACL SURFING e os contadores de retorno estabelecidos na ACL BROWSING aumentaram.**

**R1(config)# ip access-list extended SURFING**

**R1(config-ext-nacl)# Remark Permits inside HTTP and HTTPS traffic**

**R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 80**

**R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 443**

**R1(config-ext-nacl)# exit**

**R1(config)#**

**R1(config)# ip access-list extended BROWSING**

**R1(config-ext-nacl)# Remark Only permit returning HTTP and HTTPS traffic**

**R1(config-ext-nacl)# permit tcp any 192.168.10.0 0.0.0.255 established**

**R1(config-ext-nacl)# exit**

**R1(config)# interface g0/0/0**

**R1(config-if)# ip access-group SURFING in**

**R1(config-if)# ip access-group BROWSING out**

**R1(config-if)# end**

**R1# show access-lists**

**Extended IP access list SURFING**

**10 permit tcp 192.168.10.0 0.0.0.255 any eq www**

**20 permit tcp 192.168.10.0 0.0.0.255 any eq 443 (124 matches)**

**Extended IP access list BROWSING**

**10 permit tcp any 192.168.10.0 0.0.0.255 established (369 matches)**

**R1#**

**4.4.1 Dois métodos para modificar uma ACL**

**4.4.2 Método do Editor de Texto**

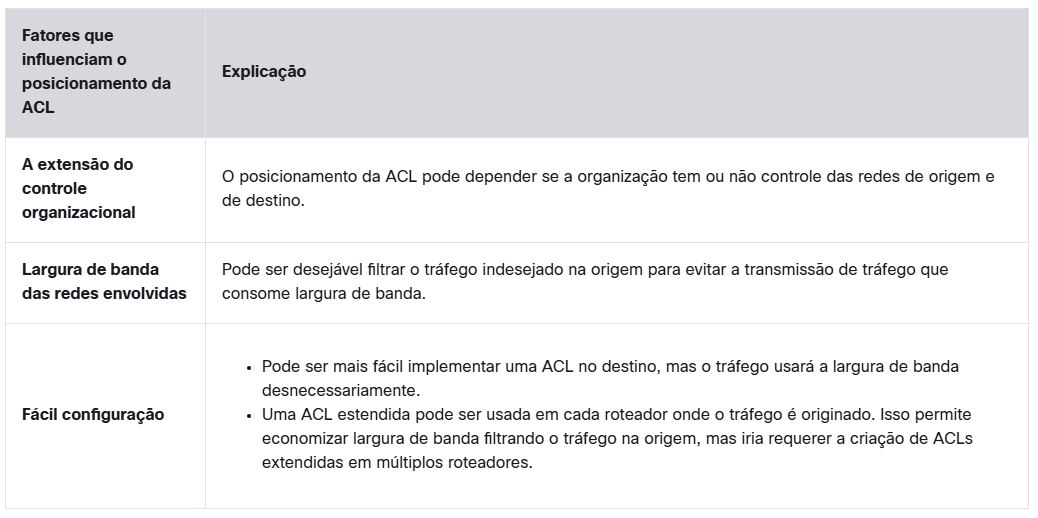
**ACLs com várias ACEs devem ser criadas em um editor de texto. Isso permite planejar as ACEs necessárias, criar a ACL e colá-la na interface do roteador. Ele também simplifica as tarefas para editar e corrigir uma ACL.**

**Para corrigir o erro:**

* **Copie a ACL da configuração em execução e cole-a no editor de texto.**
* **Faça as alterações necessárias.**
* **Remova a ACL configurada anteriormente no roteador. Caso contrário, a colação dos comandos ACL editados só acrescentará (isto é, adicionar) aos Aces ACL existentes no roteador.**
* **Copie e cole a ACL editada de volta para o roteador.**
* 4.4.3 Método de número de seqüência
* Uma ACL ACE também pode ser excluída ou adicionada usando os números de sequência ACL. Os números de sequência são atribuídos automaticamente quando uma ACE é inserida. Esses números são alistados no comando **show access-lists**. O comando**show running-config** não exibe a sequência de números.
* No exemplo anterior, a ACE incorreta para ACL 1 está usando o número de seqüência 10, como mostrado no exemplo.
* R1# **show access-lists**
* Standard IP access list 1
* 10 deny 19.168.10.10
* 20 permit 192.168.10.0, wildcard bits 0.0.0.255
* R1#
* Utilize o comando **ip access-list standard** para editar uma ACL. As instruções não podem ser substituídas usando o mesmo número de sequência que uma instrução existente. Portanto, a declaração atual deverá excluir os primeiros com o comando**no 10** . Em seguida, a ACE correta pode ser adicionada usando o número de sequência 10 é configurado. Verifique as mudanças utilizando o comando **show access-lists** .
* R1# **conf t**
* R1(config)# **ip access-list standard 1**
* R1(config-std-nacl)# **no 10**
* R1(config-std-nacl)# **10 deny host 192.168.10.10**
* R1(config-std-nacl)# **end**
* R1# **show access-lists**
* Standard IP access list 1
* 10 deny 192.168.10.10
* 20 permit 192.168.10.0, wildcard bits 0.0.0.255
* R1#
* 4.5.2 Aplique uma ACL
* Depois de criar uma ACL, o administrador pode aplicá-lo de várias maneiras diferentes. O seguinte mostra a sintaxe de comando para aplicar uma ACL a uma interface ou para as linhas VTY.
* Router(config-if)# **ip access-group** {*acl-#* | *name*} {**in** | **out**}
* Router(config-line)# **ip access-class** {*acl-#* | *name*} {**in** | **out**}

**As ACLs estendidas são normalmente colocadas próximo à origem.**

**As ACLs padrão são normalmente colocadas próximo ao destino.**

****

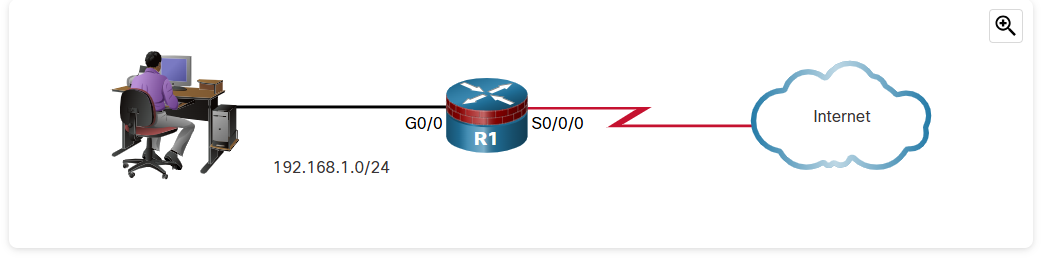
**4.6.1 Mitigar Ataques Spoofing**

**As ACLs podem ser usadas para mitigar muitas ameaças de rede, como falsificação de endereço IP e ataques de negação de serviço (DoS). A maioria dos ataques usa algum tipo de falsificação. Spoofing de endereço IP substitui o processo de criação de pacotes normais inserindo um cabeçalho IP personalizado com um endereço IP de origem diferente. Os invasores podem esconder sua identidade, falsificando o endereço IP de origem.**

**Existem muitas classes conhecidas de endereços IP que nunca devem ser vistas como endereços IP de origem para o tráfego que entram na rede de uma organização. Por exemplo, na figura a interface S0/0/0 é anexada à Internet e nunca deve aceitar pacotes de entrada dos seguintes endereços:**

* **Todos os endereços de zeros**
* **Endereços de transmissão**
* **Endereços de host local (127.0.0.0/8)**
* **Endereços de Endereçamento IP Privado Automático (APIPA) (169.254.0.0/16)**
* **Endereços privados reservados (RFC 1918)**
* **Intervalo de endereço IP multicast (224.0.0.0/4)**

**A rede 192.168.1.0/24 é anexada à interface R1 G0 / 0. Essa interface deve permitir apenas pacotes de entrada com um endereço de origem dessa rede. A ACL para G0 / 0 mostrada na figura só permitirá pacotes de entrada da rede 192.168.1.0/24. Todos os outros serão descartados.**



**Inbound em S0 / 0/0:**

**R1(config)# access-list 150 deny ip host 0.0.0.0 any**

**R1(config)# access-list 150 deny ip 10.0.0.0 0.255.255.255 any**

**R1(config)# access-list 150 deny ip 127.0.0.0 0.255.255.255 any**

**R1(config)# access-list 150 deny ip 172.16.0.0 0.15.255.255 any**

**R1(config)# access-list 150 deny ip 192.168.0.0 0.0.255.255 any**

**R1(config)# access-list 150 deny ip 224.0.0.0 15.255.255.255 any**

**R1(config)# access-list 150 deny ip host 255.255.255.255 any**

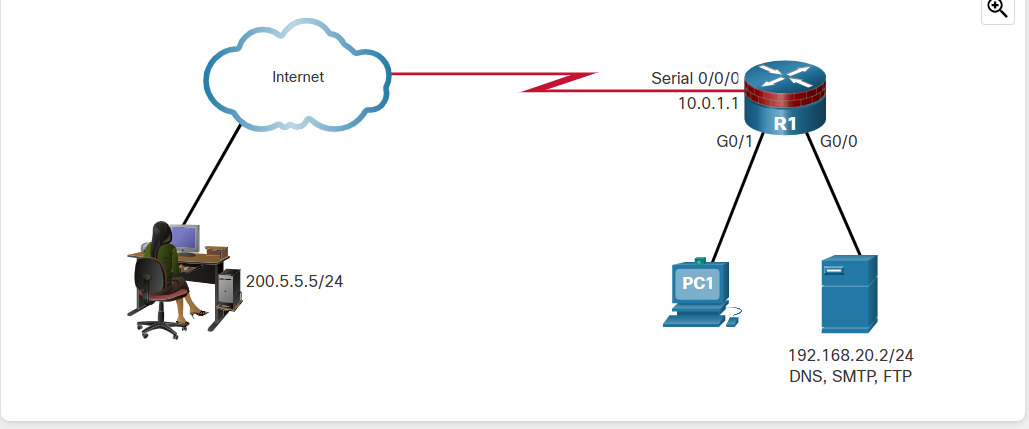
**Inbound em G0 / 0:**

**R1(config)# access-list 105 permit ip 192.168.1.0 0.0.0.255 any**

**4.6.2 Permitir o tráfego necessário através de um firewall**

**Uma estratégia eficaz para atenuar ataques é permitir explicitamente apenas alguns tipos de tráfego através de um firewall. Por exemplo, o sistema de nome de domínio (DNS), o protocolo SMTP (Simple Mail Transfer Protocol) e o Protocolo de Transferência de Arquivos (FTP) são os serviços que geralmente devem ser permitidos por meio de um firewall. Também é comum configurar um firewall para que permita os administradores acesso remoto através do firewall. Secure Shell (SSH), Syslog e Simple Rede Gerenciamento Protocolo (SNMP) são exemplos de serviços que um roteador pode precisar incluir.**

**A figura mostra um exemplo de topologia com configurações de ACL para permitir serviços específicos na interface serial 0/0/0.**

****

**Inbound em S0 / 0/0:**

**R1(config)# access-list 180 permit udp any host 192.168.20.2 eq domain**

**R1(config)# access-list 180 permit tcp any host 192.168.20.2 eq smtp**

**R1(config)# access-list 180 permit tcp any host 192.168.20.2 eq ftp**

**R1(config)# access-list 180 permit tcp host 200.5.5.5 host 10.0.1.1 eq 22**

**R1(config)# access-list 180 permit udp host 200.5.5.5 host 10.0.1.1 eq syslog**

**R1(config)# access-list 180 permit udp host 200.5.5.5 host 10.0.1.1 eq snmptrap**

**4.6.3 Mitigar Ataques ICMP**

**Os hackers podem usar pacotes de eco de protocolo de mensagem de controle da Internet (ICMP) para descobrir sub-redes e hosts em uma rede protegida e gerar ataques de inundação dos DOS. Hackers podem usar mensagens de redirecionamento ICMP para alterar as tabelas de roteamento do host. Tanto as mensagens do ICMP Echo e Redirect devem ser bloqueadas de entrada pelo roteador.**

**Várias mensagens ICMP são recomendadas para operação adequada de rede e devem ser permitidas na rede interna:**

** Echo reply - Permite que os usuários façam ping em hosts externos.**

** Source quench - Solicita que o remetente diminua a taxa de tráfego das mensagens.**

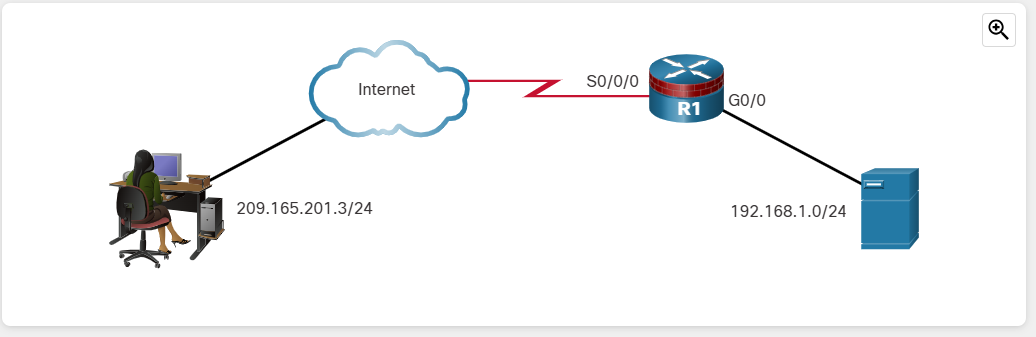
** Unreachable - Gerado para pacotes que são negados administrativamente por uma ACL.**

**Várias mensagens ICMP são necessárias para a operação de rede adequada e devem ser permitidas para sair da rede:**

* **Echo - Permite que os usuários façam ping em hosts externos.**
* **Parâmetro problem - Informa o host sobre problemas de cabeçalho de pacote.**
* **Packet too big - Habilita a descoberta da unidade máxima de transmissão do pacote (MTU).**
* **Source quench - Reduz o tráfego quando necessário.**

**Como regra, bloqueie todos os outros tipos de mensagens ICMP de saída.**

**Os ACLs são usados para bloquear o Spoofing de Endereços IP, permitem marcar seletivamente serviços específicos por meio de um firewall e permitir que somente as mensagens ICMP necessárias. A figura mostra uma topologia de amostra e possíveis configurações ACL para permitir serviços específicos do ICMP nas interfaces G0 / 0 e S0 / 0/0.**

**Inbound em S0 / 0/0:**

**R1(config)# access-list 112 permit icmp any any echo-reply**

**R1(config)# access-list 112 permit icmp any any source-quench**

**R1(config)# access-list 112 permit icmp any any unreachable**

**R1(config)# access-list 112 deny icmp any any**

**R1(config)# access-list 112 permit ip any any**

**Inbound em S0 / 0/0:**

**R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any echo**

**R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any parameter-problem**

**R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any packet-too-big**

**R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any source-quench**

**R1(config)# access-list 114 deny icmp any any**

**R1(config)# permit ip any any**

**4.6.4 Mitigar Ataques SNMP**

**Protocolos de gerenciamento, como SNMP, são úteis para monitoramento remoto e gerenciamento de dispositivos em rede. No entanto, eles ainda podem ser explorados. Se o SNMP for necessário, a exploração de vulnerabilidades SNMP pode ser mitigada aplicando ACLs de interface para filtrar pacotes SNMP de sistemas não autorizados. Uma exploração ainda pode ser possível se o pacote SNMP for provido de um endereço que foi falsificado e é permitido pela ACL.**

**Essas medidas de segurança são úteis, mas os meios mais eficazes de prevenção de exploração é desativar o servidor SNMP em dispositivos iOS para os quais não é necessário. Como mostrado na figura, use o comando no snmp-server para desativar os serviços SNMP nos dispositivos Cisco IOS.**

**Router(config)# no snmp-server**

**4.7.1 Visão geral do IPv6 ACL**

**Nos últimos anos, muitas redes começaram a transição para um ambiente IPv6. Parte da necessidade da transição para IPv6 é por causa das fraquezas inerentes no IPv4.**

**Infelizmente, como a migração para o IPv6 continua, os ataques IPv6 estão se tornando mais difundidos. IPv4 não desaparecerá durante a noite. O IPv4 coexistirá com o IPv6 e, em seguida, será gradualmente substituído pelo IPv6. Isso cria potenciais furos de segurança. Um exemplo de uma preocupação de segurança é que os atores de ameaça que alavancam o IPv4 para explorar o IPv6 em ambientes de pilha dupla. Dual Stack é um método de integração no qual um dispositivo tem conectividade para as redes IPv4 e IPv6. Em dispositivos de ambiente de pilha dupla operam com duas pilhas de protocolo IP.**

**O ator de ameaças pode realizar ataques furtivos que resultam na exploração da confiança usando anfitriões empilhados duplos, as mensagens do NDP) do vizinho desonesto (NDP) e técnicas de tunelamento. O Teredo Tunneling, por exemplo, é uma tecnologia de transição IPv6 que fornece atribuição automática de endereços IPv6 quando os hosts IPv4 / IPv6 estão localizados por trás dos dispositivos Tradução de Endereços de Rede IPv4 (NAT). Isso realiza isso incorporando os pacotes IPv6 dentro dos pacotes IPv4 UDP. O ator de ameaça ganha uma posição na rede IPv4. O host comprometido envia anúncios de rogue roteador (RAS), que acionam hosts duplos empilhados para obter um endereço IPv6. O ator de ameaças pode então usar essa posição para se movimentar ou pivô, dentro da rede. O ator de ameaças pode comprometer anfitriões adicionais antes de enviar o tráfego de volta da rede, conforme mostrado na figura.**

**4.7.2 Sintaxe da ACL IPv6**

**A funcionalidade do ACL no IPv6 é semelhante às ACLs no IPv4. No entanto, não há equivalente a ACLs padrão IPv4. Além disso, todos os ACLs IPv6 devem ser configurados com um nome. A ACLs IPv6 permitem filtrar com base nos endereços de origem e de destino que estão viajando de entrada e saída para uma interface específica. Eles também suportam a filtragem de tráfego com base em cabeçalhos de opção IPv6 e informações opcionais do tipo de protocolo de camada superior para a granularidade mais fina de controle, semelhante a ACLs estendidas no IPv4. Para configurar uma ACL IPv6, use o comando ipv6 access-list para entrar no modo de configuração da ACL IPv6. Em seguida, use a sintaxe mostrada na figura para configurar cada entrada da lista de acesso para permitir ou negar especificamente o tráfego. A sintaxe mostrada é uma versão simplificada da sintaxe do IPv6 ACE. Existem opções adicionais. Deve ser claro a partir da sintaxe fornecida que os ACLs IPv6 são consideravelmente mais flexíveis que os ACLs IPv4.**

**Aplique uma ACL IPv6 a uma interface com o comando ipv6 traffic-filter.**

**Router(config)# ipv6 access-list *access-list-name***

**Router(config-ipv6-acl)# deny | permit *protocol* {*source-ipv6-prefix* / *prefix-length* | any | host *source-ipv6-address*} [ *operator* [ *port-number* ]] { *destination-ipv6-prefix* / *prefix-length* | any | host *destination-ipv6-address* } [ *operator* [ *port-number* ]] [ dscp *value* ] [ fragments ] [ log ] [ log-input ] [ sequence *value* ] [ time-range *name* ]**

****

**4.7.3 Configurar ACLs de IPv6**

**Uma ACL do IPv6 contém uma negação implícita no deny ipv6 any any. Cada IPv6 ACL também contém regras de licença implícitas para permitir a descoberta vizinha do IPv6. O IPv6 Neighbor Discovery Protocol (NDP) requer o uso da camada de rede IPv6 para enviar anúncios vizinhos (NAS) e solicitações vizinhas (NSS). Se um administrador configurar o comando deny ipv6 any Sem permitir explicitamente permitir o neighbor discovery, o NDP será desativado.**

**Na figura, R1 está permitindo o tráfego de entrada em G0 / 0 a partir de 2001: DB8: 1: 1 :: / 64 rede. Os pacotes Na e NS são explicitamente permitidos. O tráfego proveniente de qualquer outro endereço IPv6 é explicitamente negado. Se o administrador configurasse apenas a primeira instrução de permissão, a ACL teria o mesmo efeito. No entanto, é uma boa prática documentar as declarações implícitas explicitamente configurando-as.**

**R1(config)# ipv6 access-list LAN\_ONLY**

**R1(config-ipv6-acl)# permit 2001:db8:1:1::/64 any**

**R1(config-ipv6-acl)# permit icmp any any nd-na**

**R1(config-ipv6-acl)# permit icmp any any nd-ns**

**R1(config-ipv6-acl)# deny ipv6 any any**

**R1(config-ipv6-acl)# end**

**R1# show ipv6 access-list**

**IPv6 access list LAN\_ONLY**

**permit ipv6 2001:DB8:1:1::/64 any sequence 10**

**permit icmp any any nd-na sequence 20**

**permit icmp any any nd-ns sequence 30**

**deny ipv6 any any sequence 40**

**R1#**

**4.8.1 O que aprendi neste módulo?**

**expand\_less**

**Introdução às listas de controle de acesso**

**Uma ACL é uma série de comandos do IOS usados para filtrar pacotes com base nas informações encontradas no cabeçalho do pacote. Por padrão, um roteador não tem nenhuma ACLs configurada. Uma ACL usa uma lista seqüencial de instruções de permissão ou negação, conhecidas como ACEs. O processo de filtragem de pacotes ocorre quando o tráfego de rede passa por uma interface configurada com uma ACL, e o roteador compara as informações dentro do pacote contra cada ACE, em ordem sequencial, para determinar se o pacote corresponde a um dos ACEs. A filtragem de pacote pode ocorrer na camada 3 ou 4. Cisco roteadores suportam ACLs padrão e ACLs estendidos. A ACLS número 1 a 99, ou 1300 a 1999 são ACLs padrão enquanto os ACLs número 100 a 199, ou 2000 a 2699 são ACLs estendidos. ACLs nomeadas são o método preferido a ser usado ao configurar ACLs. O nome fornece informações sobre o objetivo da ACL. As listas de acesso expressam o conjunto de regras que permitem maior controle dos pacotes que chegam às interfaces de entrada, pacotes que são retransmitidos através do roteador e pacotes que saem das interfaces do roteador.**

**Máscara curinga**

**Uma ACE IPv4 usa uma máscara curinga de 32 bits para determinar quais bits do endereço examinar para uma correspondência. As máscaras curingas também são usadas pelo protocolo de roteamento OSPF. Uma máscara curinga é semelhante a uma máscara de sub-rede na vez que usa o processo de ANDing para identificar quais bits em um endereço IPv4 devem corresponder. No entanto, eles diferem na forma como combinam 1s e 0s binários. Diferente de uma máscara de sub-rede, na qual o binário 1 é igual a uma correspondência e o binário 0 não é uma correspondência, em uma máscara curinga, o inverso é verdadeiro. Um método de atalho para calcular máscaras curingas é subtrair a máscara de sub-rede de 255.255.255.255. O Cisco IOS fornece duas palavras-chaves host e any**

**Implementar ACLs**

**Ao configurar e aplicar uma ACL, esteja ciente das diretrizes resumidas nesta lista:**

* **Crie um ACL globalmente e aplique-a.**
* **Garanta que a última declaração seja uma implícita deny any ou deny ip any any.**
* **Lembre-se de que a ordem da declaração é importante porque os ACLs são processados de cima para baixo.**
* **Assim que uma declaração é correspondida ao ACL, é saído.**
* **Sempre filtre o mais específico para o mais genérico. Por exemplo, negue um host específico e permita todos os outros hosts.**
* **Lembre-se que apenas uma ACL é permitida por interface, por protocolo, por direção.**
* **Lembre-se que novas declarações para uma ACL existente são adicionadas à parte inferior da ACL por padrão.**
* **Lembre-se que os pacotes gerados por roteador não são filtrados por ACLs de saída.**
* **Coloque os ACL padrão o mais próximo possível do destino.**
* **Coloque ACLs estendidos o mais próximo possível da origem.**

**Cada ACL deve ser colocado onde é o mais eficiente. As ACLs estendidas devem estar localizadas o mais perto possível da origem do tráfego a ser filtrada. As ACLs padrão devem ser localizadas o mais perto possível do destino. Fatores que influenciam a colocação da ACL incluem a extensão do controle organizacional, a largura de banda das redes envolvidas e a facilidade de configuraçã**

5.1.1 Firewalls

Um firewall é um sistema ou grupo de sistemas que aplica uma política de controle de acesso entre redes.

Propriedades comuns do Firewall

Todos os firewalls compartilham algumas propriedades comuns:

* Os firewalls são resistentes a ataques de rede.
* Firewalls são o único ponto de trânsito entre redes corporativas internas e redes externas porque todo o tráfego flui através do firewall.
* Firewalls reforçam a política de controle de acesso.

Benefícios do firewall

Existem vários benefícios do uso de um firewall em uma rede:

* Eles impedem a exposição de hosts, recursos e aplicações sensíveis a usuários não confiáveis.
* Eles sanitizam o fluxo do protocolo, o que impede a exploração de falhas no protocolo.
* Eles bloqueiam dados maliciosos de servidores e clientes.
* Eles reduzem a complexidade do gerenciamento de segurança descarregando a maior parte do controle de acesso à rede para alguns firewalls na rede.

Limitações do Firewall

Os firewalls também têm algumas limitações:

* Um firewall mal configurado pode ter sérias conseqüências para a rede, como se tornar um único ponto de falha.
* Os dados de muitos aplicativos não podem ser transmitidos por firewalls com segurança.
* Os usuários podem procurar proativamente maneiras de contornar o firewall para receber material bloqueado, o que expõe a rede a possíveis ataques.
* O desempenho da rede pode diminuir.
* O tráfego não autorizado pode ser encapsulado ou escondido como tráfego legítimo através do firewall.

**Firewall de filtragem de pacotes (sem estado)**

Os firewalls de filtragem de pacotes geralmente fazem parte de um firewall de roteador, que permite ou nega tráfego com base nas informações da Camada 3 e da Camada 4. Eles são firewalls sem estado que usam uma simples pesquisa de tabela de políticas que filtra o tráfego com base em critérios específicos.

Por exemplo, os servidores SMTP escutam a porta 25 por padrão. Um administrador pode configurar o firewall de filtragem de pacotes para bloquear a porta 25 de uma estação de trabalho específica para evitar que ela transmita um vírus de e-mail.

Os firewalls de filtragem de pacotes geralmente fazem parte de um firewall de roteador

Existem várias vantagens de usar um firewall de filtragem de pacotes:

* Os filtros de pacote implementam conjuntos de regras de permissão simples ou negam.
* Os filtros de pacotes têm um baixo impacto no desempenho da rede.
* Os filtros de pacotes são fáceis de implementar e são suportados pela maioria dos roteadores.
* Os filtros de pacote fornecem um grau inicial de segurança na camada de rede.
* Os filtros de pacotes executam quase todas as tarefas de um firewall high-end a um custo muito menor.

Existem várias desvantagens de usar um firewall de filtragem de pacotes:

* Os filtros de pacote de informação são suscetíveis à falsificação de IP. Os atores de ameaça podem enviar pacotes arbitrários que atendem aos critérios ACL e passam pelo filtro.
* Os filtros de pacotes não filtram de forma confiável pacotes fragmentados. Como os pacotes IP fragmentados carregam o cabeçalho TCP no primeiro fragmento e filtro de filtros de pacote na informação de cabeçalho TCP, todos os fragmentos após o primeiro fragmento são passados incondicionalmente. As decisões de usar filtros de pacote supõem que o filtro do primeiro fragmento impõe com precisão a política.
* Os filtros de pacotes usam ACLs complexas, que podem ser difíceis de implementar e manter.
* Os filtros de pacotes não podem filtrar dinamicamente determinados serviços. Por exemplo, as sessões que usam negociações de porta dinâmica são difíceis de filtrar sem abrir o acesso a toda uma variedade de portas.

**Firewall com monitoração de estado**

**Rede**

Firewalls com estado são as tecnologias de firewall mais versáteis e mais comuns em uso. Os firewalls stateful fornecem filtragem de pacotes stateful usando informações de conexão mantidas em uma tabela de estado. Filtragem com estado é uma arquitetura de firewall classificada na camada de rede. Ele também analisa o tráfego na camada 4 da OSI e na camada 5.

**Firewall de gateway de aplicativo**

Um firewall de gateway de aplicação (firewall proxy), conforme mostrado na figura, filtra as informações nas camadas 3, 4, 5 e 7 do modelo de referência OSI. A maior parte do controle e filtragem do firewall é feita em software. Quando um cliente precisa acessar um servidor remoto, ele se conecta a um servidor proxy. O servidor proxy se conecta ao servidor remoto em nome do cliente. Portanto, o servidor só vê uma conexão do servidor proxy.

**Firewall de última geração**

Os firewalls de última geração (NGFW) vão além dos firewalls de estado, fornecendo:

* Prevenção de intrusão integrada
* Reconhecimento e controle de aplicativos para ver e bloquear aplicativos arriscados
* Caminhos de atualização para incluir futuros feeds de informações
* Técnicas para lidar com ameaças de segurança em evolução
* **Firewalls baseados em host** - é um PC ou servidor com software de firewall em execução nele.
* **Um firewall transparente** - filtra o tráfego IP entre um par de interfaces em ponte.
* **Firewall híbrido** - Uma combinação dos vários tipos de firewall. Por exemplo, um firewall de inspeção de aplicações combina um firewall com estado com um firewall de gateway de aplicativo.
* Camada 7
* Aplicação
* Camada 6
* Apresentação
* Camada 5
* Sessão
* Camada 4
* Transporte
* Camada 3
* Rede
* Camada 2
* Enlace de Dados
* Camada 1
* Física

**5.1.5 Vantagens e limitações do Firewall de estado**

Existem vários benefícios em usar um firewall com estado em uma rede:

Firewalls com estado são frequentemente usados como um meio primário de defesa, filtrando tráfego indesejado ou desnecessário.

Firewalls com estado fortalecem a filtragem de pacotes fornecendo um controle mais rigoroso sobre a segurança.

Firewalls com estado melhoram o desempenho em relação aos filtros de pacotes ou servidores proxy.

Firewalls com estado se defendem contra ataques de falsificação e DoS, determinando se os pacotes pertencem a uma conexão existente ou são de uma origem não autorizada.

Firewalls com estado fornecem mais informações de log do que um firewall de filtragem de pacotes.

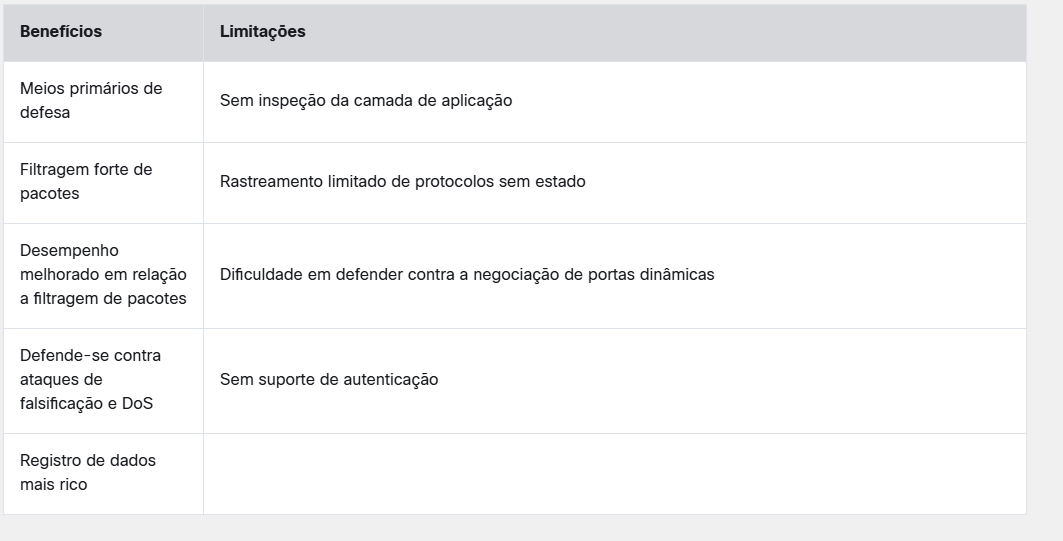
<

Os firewalls com estado também apresentam algumas limitações:

Firewalls com estado não podem evitar ataques à camada de aplicativo porque não examinam o conteúdo real da conexão HTTP.

Nem todos os protocolos são stateful. Por exemplo, o UDP e o ICMP não geram informações de conexão para uma tabela de estado e, portanto, não conseguem tanto suporte para filtragem.

É difícil rastrear conexões que usam negociação de porta dinâmica. Algumas aplicações abrem várias conexões. Isso requer uma nova gama de portas que devem ser abertas para permitir esta segunda conexão.

Firewalls com estado não suportam autenticação de usuário. ****

**5.2.1 Arquiteturas comuns de segurança**

**Privado e Público**

**Como mostrado na figura, a rede pública (ou rede externa) não é confiável e a rede privada (ou rede interna) é confiável.**

**Normalmente, um firewall com duas interfaces é configurado da seguinte forma:**

* **O tráfego proveniente da rede privada é permitido e inspecionado à medida que viaja em direção à rede pública. É permitido o tráfego inspecionado que retorna da rede pública e associado ao tráfego originado da rede privada.**
* **O tráfego originado da rede pública e que viaja para a rede privada geralmente é bloqueado.**

**Zona Desmilitarizada**

**Uma zona desmilitarizada (DMZ) é um projeto de firewall onde normalmente há uma interface interna conectada à rede privada, uma interface externa conectada à rede pública e uma interface DMZ, conforme mostrado na figura.**

* **O tráfego proveniente da rede privada é inspecionado à medida que ele viaja para a rede pública ou DMZ. Este tráfego é permitido com pouca ou nenhuma restrição. Tráfego inspecionado que retorna da DMZ ou da rede pública para a rede privada é permitido.**
* **O tráfego originado da rede DMZ e que viaja para a rede privada geralmente é bloqueado.**
* **O tráfego originado da rede DMZ e viajando para a rede pública é permitido seletivamente com base nos requisitos de serviço.**
* **O tráfego proveniente da rede pública e que viaja em direção à DMZ é seletivamente permitido e inspecionado. Esse tipo de tráfego normalmente é tráfego de email, DNS, HTTP ou HTTPS. O tráfego de retorno da DMZ para a rede pública é permitido dinamicamente.**
* **O tráfego originado da rede pública e que viaja para a rede privada está bloqueado.**
* **Firewalls de política baseados em zona**
* Os firewalls de política baseados em zona (ZPFs) usam o conceito de zonas para fornecer flexibilidade adicional. Uma zona é um grupo de uma ou mais interfaces que têm funções ou recursos semelhantes. As zonas ajudam a especificar onde uma regra ou política de firewall do Cisco IOS deve ser aplicada. Na figura, as políticas de segurança para LAN 1 e LAN 2 são semelhantes e podem ser agrupadas em uma zona para configurações de firewall. Por padrão, o tráfego entre interfaces na mesma zona não está sujeito a nenhuma política e passa livremente. No entanto, todo o tráfego de zona para zona está bloqueado. Para permitir o tráfego entre as zonas, uma política que permite ou inspeciona o tráfego deve ser configurada.
* A única exceção a esta política padrão **deny any** é a zona própria do roteador. A zona auto é o próprio roteador e inclui todos os endereços IP da interface do roteador. As configurações de política que incluem a zona automática aplicar-se-iam ao tráfego destinado e proveniente do roteador. Por padrão, não há nenhuma política para esse tipo de tráfego. O tráfego que deve ser considerado ao projetar uma política para a auto zona inclui o tráfego de plano de gerenciamento e plano de controle, como SSH, SNMP e protocolos de roteamento.

**5.2.2 Defesa em camadas**

**5.2.2 Defesa em camadas**

1. **Segurança do núcleo da rede - Protege contra software malicioso e anomalias de tráfego, impõe políticas de rede e garante capacidade de sobrevivência**
2. **Segurança de perímetro - Protege limites entre zonas**
3. **Segurança das comunicações - Fornece garantia de informação**
4. **Segurança do endpoint - Fornece identidade e conformidade com a política de segurança do dispositivo**

**Uma defesa em camadas usa diferentes tipos de firewalls que são combinados em camadas para adicionar profundidade à segurança de uma organização. As políticas podem ser aplicadas entre as camadas e dentro das camadas. Estes pontos de aplicação da política determinam se o tráfego é encaminhado ou descartado. Por exemplo, o tráfego que vem dentro da rede não confiável encontra primeiramente um filtro de pacote no roteador de borda. Se permitido pela política, o tráfego vai ao Firewall selecionado ou ao sistema host bastion que aplica mais regras ao tráfego e descarta pacotes suspeitos. Um host bastion é um computador endurecido que normalmente está localizado na DMZ. Então o tráfego vai para um roteador de triagem interior. O tráfego move-se para o host de destino interno somente após passar com sucesso todos os pontos de imposição da política entre o roteador externo e a rede interna. Esse tipo de configuração DMZ é chamado de configuração de sub-rede rastreada.**

**Uma abordagem de defesa em camadas não é tudo o que é necessário para garantir uma rede interna segura. Um administrador de rede deve considerar muitos fatores ao construir uma defesa completa em profundidade:**

* **Os firewalls normalmente não interrompem as intrusões provenientes de hosts dentro de uma rede ou zona.**
* **Firewalls não protegem contra instalações de ponto de acesso desonestos.**
* **Os firewalls não substituem os mecanismos de backup e recuperação de desastres resultantes de ataques ou falhas de hardware.**
* **Os firewalls não substituem administradores e usuários informados.**
* Posicione firewalls nos limites de segurança. Os firewalls são uma parte crítica da segurança de rede, mas não é sensato confiar exclusivamente em um firewall para segurança.
* Negue todo o tráfego por padrão.
* Permitir apenas serviços que são necessários.
* Assegure-se de que o acesso físico ao firewall esteja controlado.
* Monitore regularmente logs de firewall.
* Pratique o gerenciamento de alterações para alterações de configuração de firewall.
* Lembre-se de que os firewalls protegem principalmente contra ataques técnicos originários do exterior.

**6.1.1 Benefícios de um ZPF**

**Há dois modelos de configuração para o Cisco IOS Firewall:**

* **Firewall clássico - o modelo de configuração tradicional em que a política de firewall é aplicada em interfaces.**
* **Firewall de política baseado em zona (ZPF) - O modelo de configuração na qual as interfaces são atribuídas a zonas de segurança, e a política de firewall é aplicada ao tráfego em movimento entre as zonas.**

**Existem vários benefícios de um ZPF:**

* **Não é dependente de ACL.**
* **A postura de segurança do roteador é bloquear a menos que explicitamente permitido.**
* **As políticas são fáceis de ler e pesquisar defeitos com o Cisco Common Classification Policy Language (C3PL). C3PL é um método estruturado para criar políticas de tráfego com base em eventos, condições e ações. Isto fornece a escalabilidade porque uma política afeta todo o tráfego dado, em vez de precisar de ACLs múltiplos e ações da inspeção para tipos diferentes de tráfego.**
* **Interfaces virtuais e físicas podem ser agrupadas em zonas.**
* **As políticas são aplicadas ao tráfego unidirecional entre zonas.**

**Ao decidir se deseja implementar o iOS Classic Firewall ou um ZPF, é importante observar que ambos os modelos de configuração podem ser ativados simultaneamente em um roteador. No entanto, os modelos não podem ser combinados em uma única interface. Por exemplo, uma interface não pode ser configurada simultaneamente como membro da zona de segurança e para inspeção de IP.**

**6.1.2 Projeto ZPF**

**Etapa 1. Determine as zonas**

**O administrador se concentra na separação da rede em zonas. Zonas estabelecem as fronteiras de segurança de uma rede. Uma zona define um limite onde o tráfego é submetido a restrições políticas à medida que cruza para outra região da rede. Por exemplo, a rede pública seria uma zona e a rede interna seria outra zona.**

**Etapa 2. Estabelecer políticas entre zonas**

**Para cada par de zonas "fonte de destino" (por exemplo, da rede interna para a Internet externa), defina as sessões que os clientes nas zonas de origem podem solicitar os servidores nas zonas de destino. Essas sessões são mais frequentemente as sessões TCP e UDP, mas também podem ser sessões ICMP, como o ICMP ECHO. Para o tráfego que não é baseado no conceito de sessões, o administrador deve definir fluxos de tráfego unidirecionais da fonte para o destino e vice-versa. As políticas são unidirecionais e são definidas com base nas zonas de origem e destino, que são conhecidas como pares de zona.**

**Etapa 3. Projete a infraestrutura física**

**Após as zonas terem sido identificadas e os requisitos de tráfego entre eles documentados, o administrador deve projetar a infraestrutura física. O administrador deve levar em conta os requisitos de segurança e disponibilidade ao projetar a infraestrutura física. Isso inclui ditar o número de dispositivos entre zonas mais seguras e menos seguras e determinar dispositivos redundantes.**

**Etapa 4. identificar subconjuntos dentro de zonas e mesclar requisitos de tráfego**

**Para cada dispositivo de firewall no projeto, o administrador deve identificar subconjuntos de zonas que estão conectados às suas interfaces e mesclar os requisitos de tráfego para essas zonas. Por exemplo, várias zonas podem ser ligadas indiretamente a uma única interface de um firewall. Isso resultaria em uma política interzone específica do dispositivo. Embora uma consideração importante, os subconjuntos de zona de implementação estão além do escopo deste currículo.**

**exemplos de projetos do ZPF.**

**Lan-to-internet**

**Firewall-with-public-servers-1**

**Firewall-with-public-servers-2**

**Firewalls redundantes**

**Firewall complexo**

**6.2.1 Ações ZPF**

**As políticas identificam ações que o ZPF executará no tráfego de rede. Três ações possíveis podem ser configuradas para processar o tráfego por protocolo, zonas de origem e destino (pares de zonas) e outros critérios.**

* **Inspect - Isso realiza inspeção de pacotes de estado de Cisco IOS.**
* **Drop - Isso é análogo a deny uma declaração em uma ACL. Opção log vai logar os pacotes rejeitados.**
* **Pass - Isso é análogo a uma declaração permit em uma ACL. A ação de aprovação não rastreia o estado das conexões ou das sessões no tráfego.**

**6.2.2 Regras para tráfego de trânsito**

**As regras dependem se as interfaces de entrada e saída e saída são membros da mesma zona:**

**Se nenhuma das relações é um membro da zona, a seguir a ação resultante é passar o tráfego.**

**Se ambas as relações são membros da mesma zona, a seguir a ação resultante é passar o tráfego.**

**Se uma relação é um membro da zona, mas a outra não é, a seguir a ação resultante é deixar cair o tráfego apesar de um zona-par existir.**

**Se ambas as relações pertencem ao mesmo zona-par e uma política existe, a seguir a ação resultante é inspecionar, permitir, ou cair conforme definido pela política.**

**A tabela resume essas regras.**

****

**6.2.3 Regras para Tráfego para a Zona Self**

**A autoza é o próprio roteador e inclui todos os endereços IP atribuídos às interfaces do roteador. Este é o tráfego que se origina no roteador ou é endereçado a uma interface de roteador. Especificamente, o tráfego é para o gerenciamento de dispositivos, por exemplo, SSH ou controle de encaminhamento de tráfego, como o tráfego de protocolo de roteamento. As regras para um ZPF são diferentes para a autoza. Para o exemplo do tráfego da autoza, consulte a topologia mostrada na figura anterior.**

**As regras dependem se o roteador é a fonte ou o destino do tráfego, conforme mostrado na tabela. Se o roteador for a fonte ou o destino, todo o tráfego será permitido. A única exceção é se a origem e o destino são um par de zona com uma política específica de serviço. Nesse caso, a política é aplicada a todo o tráfego.**

****

**6.3.1 Configurar um ZPF**

**6.3.1 Configurar um ZPF**

**Etapa 1: Crie as zonas.**

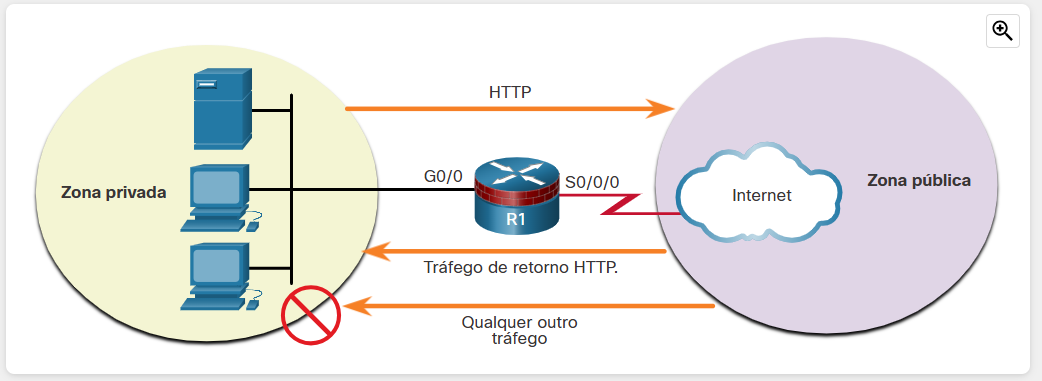
**Etapa 2: Identifique o tráfego com um mapa de classe.**

**Etapa 3: Defina uma ação com um mapa de política.**

**Etapa 4: Identifique um par de zonas e combine-o a um mapa de política.**

**Etapa 5: Atribua zonas às relações apropriadas.**

**A topologia mostrada na figura será usada durante todo o restante deste tópico para demonstrar a configuração do ZPF. A sequência de etapas não é necessária. No entanto, algumas configurações devem ser concluídas em ordem. Por exemplo, configure um class-map antes de atribuí-lo a um policy-map. Da mesma forma, você não pode atribuir um policy-map a um zone-pair, até que tenha configurado a política. Se você tentar configurar uma seção que depende de outra parte da configuração que ainda não configurou, o roteador responde com uma mensagem de erro.**

****

**6.3.2 Etapa 1. Crie as zonas**

**O primeiro passo, é criar as zonas. No entanto, antes de criar as zonas, responda a algumas perguntas:**

* **Quais interfaces devem ser incluídas nas zonas?**
* **Qual será o nome para cada zona?**
* **Que tráfego é necessário entre as zonas e em que direção?**

**Na topologia de exemplo, temos duas interfaces, duas zonas e tráfego fluindo em uma direção. O tráfego proveniente da zona pública não será permitido. Crie as zonas privadas e públicas para o firewall com o comando zone security, segundo as indicações aqui.**

**Router(config)# zone security *zone-name***

**6.3.3 Etapa 2. Identifique o tráfego**

**A segunda etapa é usar um mapa de classe para identificar o tráfego a que uma política será aplicada. Uma classe é uma maneira de identificar um conjunto de pacotes com base em seus conteúdos usando condições de "correspondência". Normalmente, você define uma classe para que você possa aplicar uma ação ao tráfego identificado que reflita uma política. Uma classe é definida com mapas de classe.**

**A figura mostra a sintaxe do comando class-map . Existem vários tipos de mapas de classe. Para uma configuração ZPF, use a palavra -chave inspect para definir um mapa de classe. Determine como os pacotes são avaliados quando existem vários critérios de correspondência. Os pacotes devem atender a um dos critérios de correspondência (match-any) ou todos os critérios de correspondência (match-all) para serem considerados um membro da classe.**

**Router(config)# class-map type inspect [match-any | match-all] *class-map-name***

**match access-group**

**Configura os critérios de coincidência para um mapa de classe com base no número ou nome da ACL especificada.**

**match protocol**

**Configura os critérios de correspondência para um mapa de classe com base no protocolo especificado.**

**match class-map**

**Usa outro mapa de classe para identificar o tráfego.**

**Na topologia, o tráfego HTTP está sendo permitido cruzar R1 do privado para a zona pública. Ao permitir o tráfego HTTP, é recomendável incluir espectros especificamente HTTPS e DNS, conforme mostrado no exemplo abaixo. O tráfego pode corresponder a qualquer uma das declarações para se tornar um membro da classe HTTP-Traffic.**

**R1(config)# class-map type inspect match-any HTTP-TRAFFIC**

**R1(config-cmap)# match protocol http**

**R1(config-cmap)# match protocol https**

**R1(config-cmap)# match protocol dns**

**6.3.4 Etapa 3. Definir uma ação**

**A terceira etapa é usar um mapa de política para definir que ação deve ser tomada para o tráfego que é um membro de uma classe. O exemplo abaixo mostra a sintaxe de comando para configurar um mapa de políticas. Uma ação é uma funcionalidade específica. É associado tipicamente a uma classe de tráfego. Por exemplo, inspect, drop, e pass são ações.**

**inspect**

**Uma ação que oferece controle de tráfego baseado em estado. O roteador mantém informações de sessão para TCP e UDP e permite o tráfego de retorno.**

**drop**

**Descarta tráfego não desejado.**

**pass**

**Uma ação sem estado que permite que o roteador encaminhe o tráfego de uma zona para outra.**

* **Inspect- Esta ação oferece controle de tráfego baseado em estado. Por exemplo, se o tráfego que viaje da zona privada para a zona pública for inspecionado, o roteador mantém informações de conexão ou sessão para o tráfego TCP e UDP. O roteador permitiria então o tráfego de retorno enviado de hospedeiros de zona pública em resposta às solicitações de conexão de zona privada.**
* **Drop - Esta é a ação padrão para todo o tráfego. Semelhante ao implícito deny anyno final de cada ACL, há um explícito drop aplicado pelo IOS ao fim de cada mapa da política. listado como class class-default listado na ultima parte da configuração de qualquer policy-map. Outros mapas de classe dentro de um mapa de políticas também podem ser configurados para diminuir o tráfego indesejado. Ao contrário do ACLs, o tráfego é silenciosamente descartado, e nenhuma mensagem inacessível ICMP é enviada para a origem do tráfego.**
* **Aprovar — essa ação permite que o roteador encaminhe o tráfego de uma zona até a outra. A ação de aprovação não rastreia o estado das conexões. A aprovação permite apenas o tráfego em uma direção. Uma política correspondente deve ser aplicada para permitir que o tráfego de retorno seja transmitido na direção oposta. A ação de passe é ideal para protocolos seguros com comportamento previsível, como IPsec. No entanto, a maior parte do tráfego de aplicações é melhor tratada no ZFW com a ação de inspect.**

**6.3.5 Etapa 4. Identificar um Zona-Par e combinar a uma política**

**A quarta etapa é identificar um par de zonas e associar esse par de zonas a um mapa de política. O exemplo abaixo mostra a sintaxe do comando. Crie uma zona-par com o comando zone-pair security. Use então o comando service-policy type inspect anexar um mapa de política e sua ação associada ao zona-par.**

**Router(config)# zone-pair security zone-pair-name source {*source-zone-name* | self} destination {*destination-zone-name* | self}**

**Router(config-sec-zone-pair)# service-policy type inspect *policy-map-name***

**source source-zone-**

**name**

**Descrição**

**Especifica o nome da zona a partir do qual o tráfego é originado.**

**>**

**destination**

**destination-zone-**

**Especifica o nome da zona para a qual o tráfego é destinado.**

**name**

**self**

**Especifica a zona definida pelo sistema. Indica se o tráfego vai para ou vem do próprio roteador.**

**O exemplo abaixo mostra um exemplo de uma configuração de par de zona. Um par de zona nomeado PRIP-PUB é criado com privado atribuído como a zona de origem e o público atribuído como a zona de destino. Em seguida, o mapa de políticas criado na etapa anterior está associado ao par de zona.**

**Depois que a política do firewall tiver sido configurada, o administrador a aplica ao tráfego entre um par de zonas usando o comando de segurança do par de zona. Para aplicar uma política, ela é atribuída a um par de zona. O par de zona precisa especificar a zona de origem, a zona de destino e a política de lidar com o tráfego entre as zonas de origem e destino.**

**R1(config)# zone-pair security PRIV-PUB source PRIVATE destination PUBLIC**

**R1(config-sec-zone-pair)# service-policy type inspect PRIV-TO-PUB-POLICY**

**6.3.6 Etapa 5. Atribuir zonas a interfaces**

**A quinta etapa é atribuir zonas às interfaces apropriadas. Associar uma zona a uma interface aplicará imediatamente a política de serviço que foi associada à zona. Se nenhuma serviço-política é configurada ainda para a zona, todo o tráfego de trânsito será deixado cair. Use o comando zone-member security atribuir uma zona a uma interface.**

**Router(config-if)# zone-member security *zone-name***

**No exemplo a seguir, GigabiteEthernet 0/0 é atribuído a zona PRIVADA, e Serial 0/0/0 é atribuído a zona PUBLIC.**

**R1(config)# interface GigabitEthernet 0/0**

**R1(config-if)# zone-member security PRIVATE**

**R1(config-if)# interface Serial 0/0/0**

**R1(config-if)# zone-member security PUBLIC**

**A política de serviço agora está ativa. O tráfego HTTP, HTTPS e DNS fornecido da zona privada e destinado à zona pública será inspecionado. O tráfego proveniente da zona pública e destinado à zona privada só será permitido se for parte das sessões inicialmente iniciadas por hosts de zona privada.**

**6.3.7 Verifique uma configuração do ZPF**

**Verifique uma configuração ZPF visualizando a configuração em execução. Observe que o mapa de classe está listado primeiro. Então o mapa de política faz uso do mapa de classe. Além disso, observe os class class-default destacados que vão descartar todo o outro tráfego que não é membro da classe HTTP-Traffic.**

**As configurações de zona seguem as configurações do mapa de política com nomeação de zona, emparelhamento de zonas e associando uma política de serviço ao par de zonas. Finalmente, as interfaces são zonas atribuídas.**

**6.3.9 Considerações de configuração do ZPF**

**Ao configurar um ZPF com o CLI, há vários fatores a considerar:**

* **O roteador nunca filtra o tráfego entre interfaces na mesma zona.**
* **Uma interface não pode pertencer a várias zonas. Para criar uma união de zonas de segurança, especifique uma nova zona e um mapa de política apropriado e pares de zonas.**
* **O ZPF pode coexistir com o Firewall clássico embora não possa ser usado na mesma interface. Remova o comando ip inspect interface configuration antes de aplicar o comando zone-member security .**
* **O tráfego nunca pode fluir entre uma interface atribuída a uma zona e uma interface sem uma atribuição de zona. O comando zone-member sempre resulta em uma interrupção temporária de serviço até que o outro membro da zona esteja configurado.**
* **A política entre zonas padrão é deixar cair todo o tráfego a menos que especificamente permitido de outra forma pela serviço-política configurada para o zona-par.**
* **O comando zone-member não protege o próprio roteador (tráfego de e do roteador não é afetado), a menos que os pares de zona sejam configurados usando a zona auto predefinida.**

**7.1.2 O Ambiente Virtual**

**Máquinas virtuais**

**Um hypervisor é um programa de software ou hardware que permite executar vários sistemas operacionais independentes em um sistema físico. Ele é um componente chave da virtualização. Existem dois métodos de virtualização:**

* **Virtualização de hardware (hypervisor tipo 1) - o sistema operacional convidado é executado diretamente em uma plataforma de hardware, sob o controle do sistema host.**
* **Virtualização hospedada (hypervisor tipo II) - um aplicativo em execução na máquina host é usado para criar máquinas virtuais que consistem totalmente em software e não contêm componentes de hardware.**

**Os ambientes de máquinas virtuais usam um sistema operacional, portanto, eles precisam ser corrigidos. As máquinas virtuais compartilham hardware e são executadas com privilégios muito altos. Esteja ciente de que um invasor que comprometa uma máquina virtual pode comprometer a máquina host.**

**Contêineres**

**Ao contrário de uma máquina virtual, um contêiner consiste apenas no aplicativo e suas dependências. Um contêiner usa um mecanismo para emulação de sistema operacional. O Docker é uma plataforma aberta que usa a virtualização no SO para distribuir software em pacotes (contêineres). Você pode facilmente mover contêineres e o aplicativo será executado. Um software especializado como o Kubernetes permite gerenciar seus contêineres.**

**Se um usuário ou aplicativo tiver privilégios elevados em um contêiner, o sistema operacional subjacente poderá ser comprometido.**

**infraestrutura de desktops virtuais (VDI)**

**Os ambientes de desktop do usuário podem ser armazenados remotamente em um servidor usando thin client ou desktops virtuais. Isso torna muito fácil criar, excluir, copiar, arquivar ou baixar configurações com rapidez em uma rede. A virtualização de desktop requer alta disponibilidade e capacidade de armazenamento.**

**Esteja ciente de que há algumas desvantagens associadas a ambientes virtuais. A expansão de VM ocorre quando muitos servidores virtualizados e subutilizados consomem mais recursos e espaço do que o necessário para o trabalho que está fazendo.** **Também é importante proteger contra a fuga de VM. Isso acontece quando a máquina virtual interrompe e interage com o sistema operacional do host.**

**7.1.4 Tecnologia na nuvem**

**os três principais modelos de serviços de computação, conhecidos coletivamente como XaaS ("qualquer coisa como serviço").**

**Software as a Service (SaaS) permite que os usuários acessem software de aplicativos e bancos de dados. Os provedores de nuvem gerenciam a infraestrutura enquanto os usuários armazenam dados nos servidores do provedor de nuvem.**

**Platform as a Service (PaaS) permite que uma organização acesse remotamente as ferramentas e serviços de desenvolvimento usados para entregar tais aplicativos, por assinatura.**

**Infrastructure as a Service (IaaS) fornece recursos de computação virtualizados pela Internet. O provedor hospeda o hardware, software, servidores e componentes de armazenamento, e o usuário paga por uma assinatura desses recursos.**

**7.1.5 Computação em Nuvem**

**Também chamada de nuvem interna, corporativa ou empresarial, uma nuvem privada é hospedada em uma plataforma privada. Uma nuvem privada oferece à empresa mais controle sobre seus dados, mas pode ser mais caro do que outros serviços de nuvem devido aos custos de infraestrutura, manutenção e administração.**

**Uma nuvem pública é hospedada por um provedor de serviços em uma instalação externa. Os usuários pagam uma taxa de uso mensal ou anual para acessar a nuvem. Essa opção custa menos à empresa para infraestrutura, manutenção e administração. No entanto, a empresa tem menos controle sobre seus dados.**

**Uma nuvem híbrida combina a nuvem privada e pública ao oferecer o controle de dados organizacionais, que ainda são hospedados em uma nuvem pública.**

**Uma nuvem da comunidade é um esforço colaborativo no qual mais de uma empresa compartilha e usa a mesma plataforma. Esse tipo de nuvem é voltado para as necessidades de um setor, como saúde ou energia.**

**A explosão dos dispositivos de IoT levou à computação em neblina (fog computing) e à computação de borda (edge computing).**

**A Fog Computing (computação em neblina) distribui a computação entre o dispositivo e o data center em nuvem. Ela desempenha um papel fundamental em aplicações onde milissegundos são importantes, como veículos autônomos, linhas aéreas e aplicações de manufatura.**

**Na fog computing, os dados são processados dentro de um gateway de IoT, ou fog node, que fica na rede de área local. Na edge computing (computação de borda), os dados são processados no dispositivo ou no sensor sem serem transferidos para um data center.**

**7.1.7 Principais ameaças à computação em nuvem**

* **Use os recursos de computação em nuvem para atingir outras entidades online.**
* **Hospede malware em provedores de nuvem respeitados que parecerão inofensivos ou até mesmo legítimos.**
* **Abusa dos serviços em nuvem para lançar ataques de DDoS, hospedar conteúdo pirata, enviar spam de e-mail e realizar campanhas de phishing.**

**Violação de dados**

**Isso ocorre quando dados confidenciais protegidos são acessados por uma entidade não autorizada.**

**Configuração incorreta de nuvem**

**Isso ocorre quando o recurso de computação em nuvem é configurado incorretamente, tornando-o vulnerável a ataques.**

**Estratégia de arquitetura de segurança de nuvem ruim**

**A segurança da nuvem privada é de responsabilidade da empresa. No entanto, a segurança para nuvens públicas, nuvens híbridas e nuvens da comunidade se torna uma responsabilidade compartilhada entre a empresa e o provedor. Isso pode gerar vulnerabilidades se a arquitetura de segurança da nuvem não for totalmente compreendida ou se for implementada corretamente.**

**Credênciais de contas comprometidas**

**Isso ocorre quando contas de usuário ou privilégios de acesso não são devidamente protegidos e são invadidas por agentes de ameaças. Isso pode levar a uma grande ameaça à segurança se a conta tiver altos privilégios. Por exemplo, em nuvens públicas, uma conta de serviço tem o maior privilégio de acessar e gerenciar ativos de nuvem. Uma conta de serviço sequestrada permitiria que um agente de ameaças controlasse todos os recursos da nuvem.**

**Ameaça interna**

**Isso ocorre quando um funcionário, empreiteiro ou parceiro de negócios compromete o serviço em nuvem de forma mal-intencionada ou não.**

**Interface de usuário de software (UI) insegura ou interface de programação de aplicativo (API)**

**A computação em nuvem usa UIs e APIs de software para que os clientes interajam com seus serviços em nuvem. Essas interfaces são os pontos mais expostos à Internet e, portanto, são alvos dos agentes de ameaças.**

**Visibilidade limitada do uso da nuvem**

**Isso ocorre quando o cliente de nuvem não tem visibilidade completa do serviço em nuvem, dificultando a identificação de arquivos seguros ou mal-intencionados.**

**7.2.1 Domínios da segurança da nuvem**

Desenvolvido pela Cloud Security Alliance (CSA)

Conceitos e arquiteturas de Computação em Nuvem

O domínio define a terminologia da computação em nuvem e detalha as estruturas lógicas e arquitetônicas gerais usadas no documento de orientações de segurança.

Governança e Gerenciamento de Riscos Corporativos

O domínio descreve quatro áreas afetadas pela computação em nuvem:

* Governança
* Gerenciamento de riscos empresariais
* Gerenciamento de riscos de informações
* Segurança da Informação

Questões jurídicas, contratos e descoberta eletrônica

O domínio descreve questões legais associadas à computação em nuvem, incluindo a transferência de dados para a nuvem, a contratação de provedores de serviços em nuvem e o gerenciamento de solicitações de descoberta eletrônica em litígios.

Gerenciamento de conformidade e auditoria

O domínio descreve os desafios de disponibilizar, medir e comunicar a conformidade quando as empresas migram dos data centers tradicionais para a nuvem.

Governança da informação

O domínio descreve a necessidade de garantir que o uso de dados e informações esteja em conformidade com as políticas, os padrões e a estratégia da empresa, incluindo os objetivos regulatórios, contratuais e comerciais.

Plano de gerenciamento e continuidade dos negócios

O domínio descreve a necessidade de proteger o plano de gerenciamento da computação em nuvem (ou seja, os protocolos e os recursos usados para gerenciar a nuvem). Ele também descreve a continuidade dos negócios e os procedimentos de recuperação de desastres que devem ser usados pelo provedor e pelo cliente em nuvem.

Segurança como Serviço

O domínio abrange os serviços de segurança em constante evolução fornecidos pela nuvem.

Segurança de infraestrutura

O domínio descreve aspectos específicos da nuvem da segurança de infraestrutura e a base para operar com segurança na nuvem.

Virtualização e Contêineres

O domínio descreve a necessidade de proteger a tecnologia de virtualização e os ativos virtuais que são a base para a computação em nuvem.

Resposta a incidentes

O domínio descreve os aspectos críticos da resposta a incidentes (IR), incluindo o ciclo de vida de resposta a incidentes e considerações para respondentes enquanto trabalham em um ambiente de nuvem.

Segurança de aplicações

O domínio oferece orientação sobre como criar e implantar aplicações com segurança em ambientes de computação em nuvem, especificamente para PaaS e IaaS.

Segurança e criptografia de dados

A segurança de dados deve ser baseada em risco, pois não é apropriado proteger tudo de forma igual. O domínio descreve os controles relacionados à proteção dos próprios dados, dos quais a criptografia é uma das mais importantes.

Gerenciamento de identidade, direito e acesso (IAM)

O domínio descreve como a identidade de nuvem é diferente do gerenciamento de identidade tradicional.

Tecnologias relacionadas

O domínio fornece informações e recomendações para tecnologias que dependem quase exclusivamente da computação em nuvem para operar e para tecnologias que não dependem necessariamente da nuvem, mas são comumente vistas em implantações em nuvem.

7.3.1 Segurança de infraestrutura

O domínio Segurança da infraestrutura descreve aspectos específicos da nuvem da segurança da infraestrutura e a base para operar com segurança na nuvem.

A infraestrutura em nuvem é a base sobre a qual os recursos de nuvem virtualizada, como computação, rede e armazenamento de dados, são construídos e implantados.

Há duas camadas principais de infraestrutura na computação em nuvem:

* A computação física e lógica (CPU, memória, etc), as redes e o armazenamento são combinados para criar uma nuvem.
* A infraestrutura virtual gerenciada por um usuário da nuvem, ou seja, a computação, a rede e os recursos de armazenamento que eles acessam nos pools de recursos.

Devido à natureza da computação em nuvem, as medidas tradicionais de segurança de infraestrutura com base no controle de caminhos de comunicação física e na inserção de dispositivos de segurança não funcionam.

Ferramentas de segurança de nuvem personalizadas incluem dispositivos virtuais e agentes de software que são usados para proteger ambientes virtuais. No entanto, essas ferramentas podem apresentar gargalos ao acessar recursos ou levar à sobrecarga do processador. Portanto, o uso de dispositivos virtuais deve ser cuidadosamente avaliado e implantado.

As redes definidas por software (SDN) permitem novos tipos de controles de segurança e proporcionam um ganho geral para a segurança de rede, incluindo:

* Fácil isolamento de rede sem restrições de hardware físico
* Firewalls SDN (grupos de segurança em computação em nuvem) aplicados a ativos com base em critérios mais flexíveis do que os firewalls de hardware

7.3.2 Responsabilidades da segurança em nuvem

A computação em nuvem envolve clientes e provedores de serviços de nuvem (CSPs). Portanto, a segurança da nuvem funciona em um modelo de responsabilidade compartilhada.

Um CSP é responsável pelos serviços em nuvem para o cliente, mas o cliente é responsável pelo restante dos serviços. O compartilhamento de responsabilidades varia de acordo com o tipo de implantação da nuvem.

A tabela a seguir exibe a responsabilidade de implementação de segurança entre um cliente e um CSP em diferentes modelos de serviço em nuvem.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Responsabilidade de segurança** | **No local** | **IaaS** | **PaaS** | **SaaS** |  |
| Dados | Cliente | Cliente | Cliente | Cliente |  |
| Endpoints | Cliente | Cliente | Cliente | Compartilhado |  |
| Gerenciamento de identidades | Cliente | Cliente | Compartilhado | Compartilhado |  |
| Aplicação | Cliente | Cliente | Compartilhado | CSP |  |
| Controle de rede | Cliente | Cliente | Compartilhado | CSP |  |
| Controle de rede | Cliente | Cliente | CSP | CSP |  |
| Infraestrutura física | Cliente | CSP | CSP | CSP |  |

Políticas de segurança da empresa

Uma empresa pode permitir que os usuários baixem ferramentas de software desconhecidas. Esses aplicativos não autorizados podem aumentar a produtividade dos funcionários ao permitir que eles baixem e usem suas ferramentas de software favoritas. No entanto, aplicativos não monitorados podem criar lacunas de segurança e pontos cegos.

Políticas de segurança da empresa estabelecidas e bem definidas e conscientização dos usuários são formas eficazes de gerenciar aplicativos desconhecidos.

Segurança em camadas

Os recursos de nuvem podem ser visualizados em quatro camadas: camadas de hardware, infraestrutura, plataforma e aplicações. Estratégias de defesa em profundidade podem ser aplicadas a cada uma dessas camadas.

Algumas opções de segurança em camadas são:

* As plataformas de nuvem normalmente têm segurança integrada na plataforma para proteger os recursos de nuvem do cliente. Por exemplo, alguns CSPs fornecem serviço de DDoS integrado que os clientes não precisam configurar.
* Uma nuvem privada virtual aloca sub-redes privadas que são logicamente isoladas da Internet.
* Embora os clientes não tenham acesso para configurar dispositivos físicos de firewall, os CSPs normalmente oferecem funções equivalentes de firewall, ou firewalls virtuais, como negar e permitir regras e grupos de segurança de host.
* Os logs de fluxo são usados para monitorar o tráfego que atravessa as interfaces de rede individuais.
* As VPNs são usadas para fornecer acesso de usuário remoto aos recursos de nuvem, bem como conexões de site para site usadas em cenários de várias nuvens ou conexões entre uma nuvem e data centers locais.
* Os serviços de gerenciamento de identidade e acesso (IAM) oferecem gerenciamento de credenciais de usuário e gerenciamento de autenticação e autorização de usuário. O uso adequado do IAM é fundamental para proteger os recursos de nuvem contra abusos.

Microssegmentação

A microssegmentação (também conhecida como hipersegregação) aproveita topologias de rede virtual para executar várias redes menores, mais isoladas e sem incorrer em custos adicionais de hardware. Como as redes são totalmente definidas em software sem muitos dos problemas de endereçamento tradicionais, é muito mais viável executar esses vários ambientes definidos por software.

As técnicas de microssegmentação permitem um controle mais granular da segurança do tráfego e dos fluxos de trabalho na nuvem.

**7.4.4 Regras de Validação**

* Tamanho – verifica o número de caracteres em um item de dados
* Formato – verifica se os dados estão de acordo com um formato especificado
* Consistência – verifica a consistência dos códigos nos itens de dados relacionados
* Intervalo – verifica se os dados estão dentro de valores mínimo e máximo
* Dígito de verificação – efetua um cálculo extra para gerar um dígito de verificação para detecção de erros

**7.5.1 Os estados dos dados**

Dados em repouso (data at rest)

Refere-se a dados armazenados. Os dados estão nesse estado quando nenhum usuário ou processo os acessa, solicita ou altera. Os dados inativos podem ser armazenados em dispositivos locais, como um disco rígido em um computador ou uma rede centralizada, como um servidor da empresa. Na computação em nuvem, os dados inativos podem ser armazenados em uma nuvem e podem ser acessados em qualquer computador conectado à Internet, geralmente com assinatura. Todos os dados que não estão em trânsito nem em andamento são considerados dados inativos.

Dados em trânsito (data in transit)

Refere-se aos dados que estão sendo transmitidos. Portanto, os dados não estão inativos nem estão sendo processados. A transmissão pode ocorrer em um único servidor ao longo das linhas de barramento da placa-mãe, entre dispositivos em uma única rede ou entre redes e, possivelmente, através da Internet. Usar a criptografia e o hash para proteger dados em trânsito é essencial para a computação em nuvem.

Dados em processamento (data in process)

Esse estado se refere aos dados durante a entrada inicial, a modificação, o cálculo ou a saída. Os dados estão nesse estado quando não estão em trânsito nem em repouso. Portanto, são os dados que estão sendo processados.

7.5.2 Criptografia

A criptografia é a ciência de criar e quebrar códigos.

Ao armazenar e transmitir dados criptografados, apenas o destinatário pretendido pode lê-los ou processá-los e somente se eles tiverem o conhecimento adequado do segredo usado no algoritmo de criptografia.

A encriptação é o processo de embaralhamento de dados para impedir que uma pessoa não autorizada leia os dados com facilidade.

Ao habilitar a encriptação, os dados legíveis são chamados de texto simples ou texto claro, enquanto a versão criptografada é chamada de texto criptografado ou texto cifrado. A criptografia converte a mensagem legível de texto claro em texto codificado, que é a mensagem ilegível disfarçada. A descriptografia reverte o processo.

A encriptação também precisa de uma chave, que desempenha um papel crítico para criptografar e descriptografar uma mensagem. A pessoa que possui a chave pode descriptografar o texto codificado para texto claro.

Há duas classes de algoritmos de criptografia:

* Os algoritmos simétricos usam a mesma chave pré-compartilhada para criptografar e descriptografar dados, um método também conhecido como criptografia com chave privada. O Advanced Encryption Standard (AES) é um algoritmo de criptografia simétrica que possui um tamanho de bloco fixo de 128 bits com um tamanho de chave de 128, 192 ou 256 bits. O governo norte-americano usa o AES para proteger as informações confidenciais.
* A criptografia assimétrica, também chamada de criptografia de chave pública, utiliza uma chave de criptografia que é diferente da chave usada para descriptografia. Os algoritmos de criptografia assimétrica incluem Rivest-Shamir-Adleman (RSA), Diffie-Hellman, EIGamal e Elliptic Curve Cryptography (ECC).

7.5.3 Hashing

O hash é uma ferramenta que garante a integridade dos dados ao considerar dados binários (por exemplo, uma mensagem) e produzir uma representação de comprimento fixo chamada de valor de hash (por exemplo, um message digest).

Hashes são usados para verificar e garantir a integridade dos dados. A ferramenta de hash também pode verificar a autenticação. Ele funciona usando uma função de hash criptográfico para substituir senhas de texto simples ou chaves de criptografia.

Uma função hash criptográfica tem as seguintes propriedades:

* A entrada pode ser de qualquer comprimento.
* A saída tem um comprimento fixo.
* A função hash é unidirecional e não é reversível.
* Dois valores de entrada diferentes quase nunca resultarão no mesmo hash.

O Instituto Nacional de Padrões e Tecnologia (NIST) dos EUA desenvolveu o SHA, o algoritmo especificado no padrão hash seguro (SHS). O NIST publicou o SHA-1 em 1994.

**Observação:**o Message Digest 5 (MD5) foi outro algoritmo de hash popular que não é mais considerado seguro.

O SHA-2 substituiu o SHA-1 com quatro funções hash adicionais para formar a família de SHA:

* SHA-224 (224 bits)
* SHA-256 (256 bits)
* SHA-384 (384 bits)
* SHA-512 (512 bits)

O SHA-2 é um algoritmo mais forte e está substituindo o MD5. SHA-256, SHA-384 e SHA-512 são os algoritmos de próxima geração.

**7.6.1 Proteção de máquinas virtuais**

Planeje o posicionamento da sub-rede.

Escolha com cuidado a sub-rede de cada instância para que ela tenha apenas o acesso necessário ao mundo exterior.

Desative serviços e porta desnecessários.

Ative apenas as portas e os serviços necessários para reduzir a exposição desnecessária a ambientes externos.

Aplique o gerenciamento de contas e políticas.

O sistema operacional em uma VM tem uma conta de usuário padrão. Desative todas as contas de usuário padrão e crie contas de usuário com políticas de gerenciamento de conta de práticas recomendadas, como complexidade de senha e acesso com menos privilégios.

Instale o software antivírus/antimalware e mantenha-o atualizado.

Isso pode ser feito através do SO da VM ou estar disponível como um serviço na plataforma de nuvem.

Instale o firewall / software do host e o IDP/IPS

Isso pode ser feito através do SO da VM ou estar disponível como um serviço na plataforma de nuvem.

**7.6.2 Proteção de VMs contra ataques de propagação de VM**

Um cliente de computação em nuvem deve implementar políticas para registrar e auditar os recursos de nuvem que estão sendo usados. A expansão de VM não apenas apresenta riscos potenciais, mas também consome serviços em nuvem desnecessariamente, como instâncias de VM, armazenamento e endereços IP públicos não atribuídos. Ao registrar o uso de recursos de nuvem, monitorar as VMs em execução e auditar o uso real, uma empresa pode gerenciar e proteger melhor as VMs de que realmente precisa.

8.1.1 Confidencialidade de dados

Existem duas classes de criptografia usadas para fornecer confidencialidade de dados; assimétrico e simétrico. Essas duas classes diferem na maneira como usam as chaves.

Algoritmos de criptografia simétrica, como Data Encryption Standard (DES), 3DES e Advanced Encryption Standard (AES), baseiam-se na premissa de que cada parte que se comunica conhece a chave pré-compartilhada. A confidencialidade dos dados também pode ser garantida usando algoritmos assimétricos, incluindo Rivest, Shamir e Adleman (RSA) e a infraestrutura de chave pública (PKI).

**Nota:**O DES é um algoritmo legado e não deve ser usado. 3DES deve ser evitado, se possível.

Criptografia Simétrica

Usa a mesma chave para criptografar e descriptografar dados.

O comprimento das chaves são pequenos (40

bits - 256 bits).

Mais rápido que a criptografia assimétrica.

Geralmente usado para criptografar dados em massa, como no tráfego da VPN.

Criptografia Assimétrica

Usa chaves diferentes para criptografar e descriptografar dados.

Os comprimentos das chaves são longos (512 bits 4096 bits).

Computationally taxing therefore slower than symmetric encryption.

Geralmente usado para transações rápidas de dados, como HTTPS, ao acessar seus dados bancários.

8.1.2 Criptografia Simétrica

Os algoritmos simétricos usam a mesma chave pré-compartilhada para criptografar e descriptografar dados. Uma chave pré-compartilhada, também chamada de chave secreta, é conhecida pelo remetente e pelo receptor antes que qualquer comunicação criptografada possa ocorrer.

Hoje, algoritmos de criptografia simétrica são comumente usados com o tráfego VPN. Isso ocorre porque os algoritmos simétricos usam menos recursos da CPU do que os algoritmos de criptografia assimétrica. Isso permite que a criptografia e a descriptografia de dados sejam rápidas ao usar uma VPN. Ao usar algoritmos de criptografia simétrica, como qualquer outro tipo de criptografia, quanto maior a chave, mais tempo levará para alguém descobrir a chave. A maioria das chaves de criptografia tem entre 112 e 256 bits. Para garantir que a criptografia é segura, um comprimento mínimo de chave de 128 bits deve ser usado. Use uma chave mais longa para comunicações mais seguras.

Algoritmos de criptografia simétrica às vezes são classificados como uma cifra de bloco ou uma cifra de fluxo.

bloco de cifra

**As cifras de bloco** transformam um bloco de texto simples de comprimento fixo em um bloco comum de texto cifrado de 64 ou 128 bits. As cifras de bloco comuns incluem DES com um tamanho de bloco de 64 bits e AES com um tamanho de bloco de 128 bits.

**As cifras de fluxo**

criptografam o texto simples um byte ou um bit de cada vez. As cifras de fluxo são basicamente uma cifra de bloco com um tamanho de bloco de um byte ou bit. As cifras de fluxo geralmente são mais rápidas do que as cifras de bloco porque os dados são criptografados continuamente. Exemplos de cifras de fluxo incluem RC4 e A5, que é usado para criptografar comunicações de telefone celular GSM.

 um tamanho de bloco de um byte ou bit. As cifras de fluxo geralmente são mais rápidas do que as cifras de bloco porque os dados são criptografados continuamente. Exemplos de cifras de fluxo incluem RC4 e A5, que é usado para criptografar comunicações de telefone celular GSM.

Algoritmos de criptografia simétrica mais conhecidos são descritos na tabela.

|  |  |
| --- | --- |
| **Algoritmos de criptografia simétrica** | **Descrição** |
| Data Encryption Standard (DES) | Este é um algoritmo de criptografia simétrica legado. Ele usa um comprimento de chave curto que o torna inseguro para a maioria dos usos atuais. |
| 3DES (Triple DES) | O 3DES é o substituto do DES e repete o processo do algoritmo DES três vezes.  Deve ser evitado, se possível, uma vez que está programado para ser aposentado em 2023. Se implementado, use durações de chave muito curtas. |
| Advanced Encryption Standard (AES) | AES é um algoritmo de criptografia simétrica popular e recomendado. Ele oferece combinações de chaves de 128, 192 ou 256 bits para criptografar blocos de dados de 128, 192 ou 256 bits. |
| Software-Optimized Encryption Algorithm (SEAL) | O SEAL é um algoritmo de criptografia simétrica alternativo mais rápido ao AES. SEAL é uma cifra de fluxo que usa uma chave de criptografia de 160 bits e tem um impacto menor na CPU em comparação com outros algoritmos baseados em software. |
| Algoritmos da série Rivest ciphers (RC) | Este algoritmo foi desenvolvido por Ron Rivest. Diversas variações foram desenvolvidas, mas o RC4 foi o mais prevalente em uso. RC4 é uma cifra de fluxo usada para proteger o tráfego da web. Verificou-se que tem múltiplas vulnerabilidades que o tornaram inseguro. O RC4 não deve ser utilizado. |

8.1.3 Criptografia Simétrica

Os algoritmos assimétricos, também chamados algoritmos de chave pública, são projetados para que a chave usada para criptografia seja diferente da chave usada para descriptografia, conforme mostrado na figura. A chave de descriptografia não pode, em uma quantidade razoável de tempo, ser calculada a partir da chave de criptografia e vice-versa.

Criptografia Assimétrica

Algoritmos assimétricos usam uma chave pública e uma chave privada. Ambas as chaves são capazes do processo de criptografia, mas a chave emparelhada complementar é necessária para descriptografia. O processo também é reversível. Os dados criptografados com a chave pública requerem a chave privada para descriptografar. Algoritmos assimétricos alcançam confidencialidade e autenticidade usando este processo.

Como nenhuma das partes possui um segredo compartilhado, é necessário usar comprimentos de chave muito longos. A criptografia assimétrica pode usar comprimentos de chave entre 512 e 4.096 bits. Comprimentos de chave maiores ou iguais a 2.048 bits podem ser confiáveis, enquanto comprimentos de chave de 1.024 ou menores são considerados insuficientes.

Exemplos de protocolos que usam algoritmos de chave assimétrica incluem:

Internet Key Exchange (IKE) - Este é um componente fundamental das VPNs IPsec.

Secure Socket Layer (SSL) - Agora isso é implementado como TLS (Transport Layer Security) padrão da IETF.

Secure Shell (SSH) - Este protocolo fornece uma conexão segura de acesso remoto a dispositivos de rede.

Pretty Good Privacy (PGP) - Este programa de computador fornece privacidade e autenticação criptográficas. É frequentemente usado para aumentar a segurança das comunicações por email.

Exemplos comuns de algoritmos de criptografia assimétrica são descritos na tabela.

|  |  |  |
| --- | --- | --- |
| **Algoritmo de criptografia assimétrica** | **comprimento da chave** | **Descrição** |
| Diffie-Hellman (DH) | 512, 1024, 2048, 3072, 4096 | O algoritmo Diffie-Hellman permite que duas partes concordem com uma chave que elas podem usar para criptografar as mensagens que desejam enviar uma para a outra. A segurança desse algoritmo depende da suposição de que é fácil aumentar um número para uma determinada potência, mas difícil calcular qual potência foi usada, dado o número e o resultado. |
| Digital Signature Standard (DSS) e Digital Signature Algorithm (DSA) | 512 - 1024 | O DSS especifica o DSA como o algoritmo para assinaturas digitais. DSA é um algoritmo de chave pública baseado no esquema de assinatura ElGamal. A velocidade de criação da assinatura é semelhante ao RSA, mas é 10 a 40 vezes mais lenta para verificação. |
| Algoritmos de criptografia Rivest, Shamir e Adleman (RSA) | 512 até 2048 | O RSA é para criptografia de chave pública que se baseia na dificuldade atual de fatorar números muito grandes. É o primeiro algoritmo conhecido por ser adequado para assinatura, bem como criptografia. É amplamente utilizado em protocolos de comércio eletrônico e acredita-se ser seguro, dadas chaves suficientemente longas e o uso de implementações atualizadas. |
| EIGamal | 512 - 1024 | Um algoritmo de criptografia de chave assimétrica para criptografia de chave pública que se baseia no contrato de chave Diffie-Hellman. Uma desvantagem do sistema ElGamal é que a mensagem criptografada se torna muito grande, aproximadamente o dobro do tamanho da mensagem original e, por esse motivo, é usada apenas para mensagens pequenas, como chaves secretas. |
| Técnicas de curva elíptica | 224 ou superior | A criptografia de curva elíptica pode ser usada para adaptar muitos algoritmos criptográficos, como Diffie-Hellman ou ElGamal. A principal vantagem da criptografia de curva elíptica é que as chaves podem ser muito menores. |

8.1.4 Criptografia Assimétrica - Confidencialidade

Algoritmos assimétricos são usados para fornecer confidencialidade sem pré-compartilhar uma senha. O objetivo de confidencialidade dos algoritmos assimétricos é iniciado quando o processo de criptografia é iniciado com a chave pública.

O processo pode ser resumido usando a fórmula:

**Chave pública (criptografar) + chave privada (descriptografar) = confidencialidade**

Quando a chave pública é usada para criptografar os dados, a chave privada deve ser usada para descriptografar os dados. Apenas um host tem a chave privada; portanto, a confidencialidade é alcançada.

8.1.5 Criptografia assimétrica - autenticação

O objetivo de autenticação de algoritmos assimétricos é iniciado quando o processo de criptografia é iniciado com a chave privada.

O processo pode ser resumido usando a fórmula:

**Chave privada (criptografar) + chave pública (descriptografar) = autenticação**

Quando a chave privada é usada para criptografar os dados, a chave pública correspondente deve ser usada para descriptografar os dados. Como apenas um host tem a chave privada, somente esse host poderia ter criptografado a mensagem, fornecendo autenticação do remetente.

8.1.6 Criptografia assimétrica - integridade

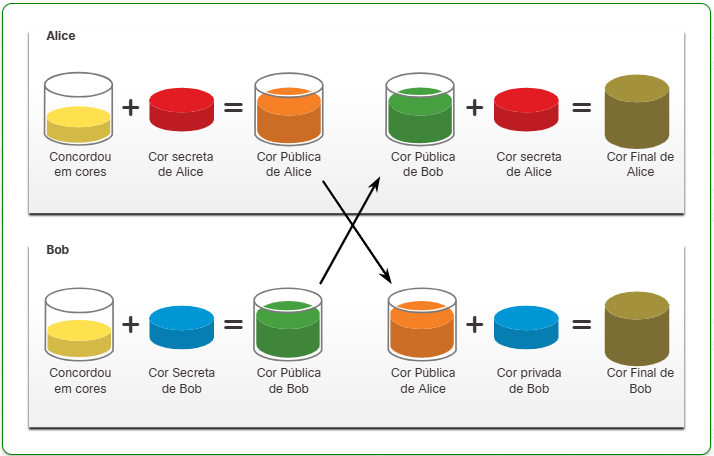
Combinar os dois processos de criptografia assimétrica fornece confidencialidade, autenticação e integridade da mensagem.

8.1.7 Diffie-Hellman

Diffie-Hellman (DH) é um algoritmo matemático assimétrico que permite que dois computadores gerem um segredo compartilhado idêntico sem terem se comunicado antes. A nova chave compartilhada nunca é realmente trocada entre o remetente e o destinatário. No entanto, como as duas partes o conhecem, a chave pode ser usada por um algoritmo de criptografia para criptografar o tráfego entre os dois sistemas.

Aqui estão dois exemplos de casos em que DH é comumente usado:

* Os dados são trocados usando uma VPN IPsec
* Dados SSH são trocados



s cores na figura serão usadas em vez de números longos complexos para simplificar o processo de contrato de chave DH. A troca de chaves DH começa com Alice e Bob concordando com uma cor comum arbitrária que não precisa ser mantida em segredo. A cor combinada em nosso exemplo é amarelo.

Em seguida, Alice e Bob selecionarão uma cor secreta. Alice escolheu vermelho enquanto Bob escolheu azul. Essas cores secretas nunca serão compartilhadas com ninguém. A cor secreta representa a chave privada secreta escolhida de cada parte.

Alice e Bob agora misturam a cor comum compartilhada (amarelo) com suas respectivas cores secretas para produzir uma cor pública. Portanto, Alice vai misturar o amarelo com sua cor vermelha para produzir uma cor pública de laranja. Bob irá misturar o amarelo e o azul para produzir uma cor pública de verde.

Alice envia sua cor pública (laranja) para Bob e Bob envia sua cor pública (verde) para Alice.

Alice e Bob misturam a cor que receberam com a sua própria cor secreta original (vermelho para Alice e azul para Bob). O resultado é uma mistura final de cor marrom que é idêntica à mistura de cor final do parceiro. A cor marrom representa a chave secreta compartilhada resultante entre Bob e Alice.

A segurança do DH se baseia-se no fato de que ele usa números muito grandes em seus cálculos. Por exemplo, um número DH 1024 bits é aproximadamente igual a um número decimal de 309 dígitos. Considerando que um bilhão é 10 dígitos decimais (1.000.000.000), pode-se facilmente imaginar a complexidade de trabalhar não com um, mas com vários números decimais de 309 dígitos.

Diffie-Hellman usa diferentes grupos DH para determinar a força da chave que é usada no processo de acordo de chave. Os números de grupo mais altos são mais seguros, mas exigem tempo adicional para calcular a chave. O seguinte identifica os grupos DH suportados pelo Cisco IOS Software e seu valor de número primo associado:

* Grupo DH 1:768 bits
* Grupo DH 2:1024 bits
* Grupo DH 5:1536 bits
* Grupo DH 14:2048 bits
* Grupo DH 15:3072 bits
* Grupo DH 16:4096 bits

**Nota**: Um acordo de chave DH também pode ser baseado em criptografia de curva elíptica. Os grupos DH 19, 20 e 24, que são baseados em criptografia de curva elíptica, também são suportados pelo Cisco IOS Software.

8.2.2 Técnicas de mascaramento de dados

A tecnologia de mascaramento de dados protege dados, substituindo as informações confidenciais por uma versão pública. A versão não confidencial parece e atua como o original para que um processo organizacional possa usar dados não confidenciais sem nenhuma mudança necessária para as aplicações de suporte ou instalações de armazenamento de dados.

* **A substituição** troca os dados por valores que parecem autênticos para tornar os registros de dados anônimos.
* **O embaralhamento** origina um conjunto de substituição da mesma coluna de dados que um usuário deseja mascarar. Esta técnica funciona bem para informações financeiras em um banco de dados de teste, por exemplo.
* A **anulação**aplica um valor nulo a um campo específico, que impede totalmente a visibilidade dos dados.

8.2.3 esteganografia

A estenografia esconde dados (a mensagem) em outro arquivo, como um gráfico, áudio ou outro arquivo de texto.

A vantagem da estenografia em relação à criptografia é que a mensagem secreta não atrai atenção especial. Ao visualizar o arquivo de forma eletrônica ou impressa, ninguém saberá que uma imagem, na realidade, contém uma mensagem secreta.

Existem vários componentes envolvidos na ocultação de dados. Primeiro, existem os dados integrados que compõem a mensagem secreta. O texto de capa (ou imagem de capa ou áudio de capa) oculta os dados integrados, produzindo o estego-texto (ou estego-imagem ou estego-áudio). Uma estego-chave (stego-key) controla o processo de ocultação.

Técnicas de estenografia

A abordagem usada para integrar dados em uma imagem de capa é o uso de Bits Menos Significativos (LSB). Esse método usa os bits de cada pixel na imagem.

* Um pixel é a unidade básica de cor programável em uma imagem de computador.
* A cor específica de um pixel é uma mistura de três cores - vermelho, verde e azul (RGB).
* Três bytes de dados especificam a cor de um pixel (um byte para cada cor). Um sistema de cores de 24 bits usa todos os três bytes.
* O LSB usa um pouco de cada um dos componentes das cores vermelho, verde e azul. Cada pixel pode armazenar 3 bits.

A figura mostra três pixels de uma imagem colorida de 24 bits. Uma das letras na mensagem secreta é a letra T e a inserção do caractere T muda somente dois bits da cor. O olho humano não consegue reconhecer as alterações efetuadas nos bits menos significativos.

Em média, no máximo, metade dos bits de uma imagem precisará ser alterada para ocultar uma mensagem secreta eficazmente.

estenografia social

A estenografia social oculta informações de visão simples, criando uma mensagem que pode ser lida de certa forma pela pessoa que receber a mensagem.

As outras pessoas que visualizarem a mensagem de modo normal não a verão. Os adolescentes nas redes sociais usam essa tática para se comunicar com seus amigos mais próximos, evitando que as outras pessoas, como seus pais, percebam o que a mensagem realmente significa. Por exemplo, a frase "ir ao cinema" pode significar "ir à praia".

Detecção

A esteganoanálise é a descoberta de que existem informações ocultas. O objetivo da esteganoanálise é descobrir as informações ocultas.

Os padrões da estego-imagem levantam suspeita. Por exemplo, um disco pode ter áreas reservadas ainda não utilizadas, que são reservadas porque ocultam informações. As utilidades de análise do disco podem relatar informações ocultas em clusters não utilizados de dispositivos de armazenamento. Os filtros podem capturar pacotes de dados que contêm informações ocultas nos cabeçalhos dos pacotes. Esses dois métodos usam usando assinaturas de estenografia.

**8.3.1 Comunicações seguras**

Estes são os quatro elementos das comunicações seguras:

* **Integridade de 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 (SHA-2 ou SHA-3). O algoritmo de resumo de mensagens MD5 ainda está amplamente em uso, no entanto, é inerentemente inseguro e cria vulnerabilidades em uma rede. O uso de MD5 deve ser evitado.
* **Autenticação de origem** - Garante que a mensagem não é uma falsificação e realmente vem de quem é declarada. 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.
* **Não Repúdio de Dados** - Garante que o remetente não pode 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.

8.3.2 Funções criptográficas de hash

Hashes são usados para verificar e garantir a integridade dos dados. O hash é baseado em uma função matemática unilateral que é relativamente fácil de calcular, mas significativamente mais difícil de reverter.

Como mostrado na figura, uma função hash leva um bloco variável de dados binários, chamado de mensagem, e produz uma representação condensada de comprimento fixo, chamado hash. O hash resultante também é às vezes chamado de mensagem digest, digest ou impressão digital.

Com funções hash, é computacionalmente inviável que dois conjuntos diferentes de dados apresentem a mesma saída hash. Cada vez que os dados são modificados ou alterados, o valor de hash também muda. Por isso, muitas vezes os valores criptográficos de hash são chamados de impressões digitais. Eles podem ser usados para detectar arquivos de dados duplicados, alterações de versão de arquivo e aplicativos semelhantes. Esses valores são usados para proteger contra uma alteração acidental ou intencional dos dados ou corrupção acidental dos dados.

8.3.3 Operação de hash criptográfico

Matematicamente, a equação***h = H (x)*** é usada para explicar como um algoritmo de hash opera.

O exemplo na figura resume o processo matemático. Uma função hash criptográfica deve ter as seguintes propriedades:

* A entrada pode ser de qualquer comprimento.
* A saída tem um comprimento fixo.
* H(x) é relativamente fácil de calcular para qualquer x.
* H (x) é um caminho e não reversível.
* H(x) é livre de colisões, o que significa que dois valores de entrada diferentes resultarão em valores de hash diferentes.

Se uma função hash é difícil de inverter, ela é considerada um hash unidirecional. Difícil de inverter significa que, dado um valor de hash de*h, é computacionalmente inviável encontrar uma entrada para x tal que* *H=h (x).*

**8.3.4 MD5 e SHA**

Existem quatro funções hash bem conhecidas:

* **MD5 com digest de 128 bits** - Desenvolvido por Ron Rivest e usado em uma variedade de aplicações de internet, MD5 é uma função unidirecional que produz uma mensagem hash de 128 bits. MD5 é considerado um algoritmo legado e deve ser evitado e usado apenas quando não houver alternativas melhores disponíveis. Recomenda- se que SHA-2 ou SHA-3 sejam usados em vez disso.
* **SHA-1 -** Desenvolvido pela Agência de Segurança Nacional dos EUA (NSA) em 1995. É muito semelhante às funções hash MD5. Existem várias versões. O SHA-1 cria uma mensagem de 160 bits e é um pouco mais lento que o MD5. O SHA-1 possui falhas conhecidas e é um algoritmo antigo.
* **SHA-2 –** Desenvolvido pela NSA. Inclui SHA-224 (224 bits), SHA-256 (256 bits), SHA-384 (384 bits) e SHA-512 (512 bits). Se você estiver usando SHA-2, então os algoritmos SHA-256, SHA-384 e SHA-512 devem ser usados sempre que possível.
* **SHA-3**- SHA-3 é o mais novo algoritmo de hash e foi introduzido pelo NIST como uma alternativa e eventual substituição para a família SHA-2 de algoritmos de hash. SHA-3 inclui SHA3-224 (224 bits), SHA3-256 (256 bits), SHA3-384 (384 bits) e SHA3-512 (512 bits). A família SHA-3 são algoritmos de última geração e devem ser usados sempre que possível.

Não há informações de identificação única do remetente no procedimento de hash. Isso significa que qualquer pessoa pode processar um hash para quaisquer dados, desde que tenha a função hash correta.

Portanto, hash é vulnerável a ataques man in the middle e não oferece segurança aos dados transmitidos. Para fornecer autenticação de integridade e origem, é necessário algo mais.

8.3.5 Autenticação de Origem

Para adicionar autenticação de origem e garantia de integridade, use um código de autenticação de mensagem hash com chave (HMAC). HMACs usam uma chave secreta adicional como entrada à função hash.

**Observação:** Outros métodos MAC (Message Authentication Code) também são usados. No entanto, o HMAC é usado em muitos sistemas, incluindo SSL, IPsec e SSH.

Algoritmo de hash HMAC

um HMAC é calculado usando qualquer algoritmo criptográfico que combina uma função hash criptográfica com uma chave secreta. As funções de hash são a base do mecanismo de proteção dos HMACs.

Somente o remetente e o destinatário têm conhecimento da chave secreta e agora a saída da função hash depende dos dados de entrada e da chave secreta. Apenas as partes que têm acesso a essa chave secreta podem calcular o digest de uma função HMAC. Isso derrota os ataques man-in-the-middle e fornece autenticação da origem dos dados.

Se duas partes compartilharem uma chave secreta e usarem as funções HMAC para autenticação, uma mensagem HMAC adequadamente construída, a parte recebeu indica que a outra parte foi a originadora da mensagem. Isso ocorre porque a outra parte possui a chave secreta.

Criação do valor de HMAC

o dispositivo de envio insere dados (como o pagamento de Terry Smith de US $ 100 e a chave secreta) no algoritmo de hash e calcula o HMAC Digest de comprimento fixo. Esse Digest autenticado é anexado à mensagem e enviado ao destinatário.

Verificação do valor de HMAC

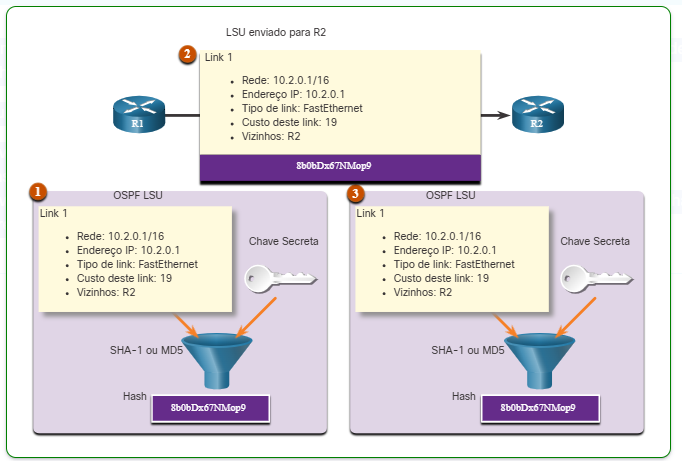
o dispositivo receptor remove o Digest da mensagem e usa a mensagem de texto sem formatação com sua chave secreta como entrada na mesma função de hash. Se o Digest calculado pelo dispositivo receptor for igual ao resumo enviado, a mensagem não foi alterada. Adicionalmente, a origem da mensagem é autenticada porque apenas o remetente possui uma cópia da chave secreta compartilhada. A função HMAC garantiu a autenticidade da mensagem.

Exemplo Cisco Router HMAC

A figura mostra como os HMACs são usados pelos roteadores Cisco configurados para usar a autenticação de roteamento Open Shortest Path First (OSPF).

R1 está enviando uma atualização de estado do link (LSU) referente a uma rota para a rede 10.2.0.0/16:

1. R1 calcula o valor do hash usando a mensagem LSU e a chave secreta.
2. O valor do hash resultante é enviado com o LSU para o R2.
3. R2 calcula o valor do hash usando o LSU e sua chave secreta. R2 aceita a atualização se os valores de hash corresponderem. Se eles não corresponderem, o R2 descartará a atualização.

8.4.1 Arquivos de hash e meios de comunicação digital

A integridade assegura que os dados e informações estejam completos e inalterados no momento da aquisição.

Para verificar a integridade de todas as imagens IOS, a Cisco oferece checksums MD5 e SHA. O usuário pode fazer uma comparação entre esse MD5 digest e o MD5 digest de uma imagem do IOS instalada em um dispositivo Agora o usuário pode ter certeza de que ninguém violou ou modificou o arquivo de imagem do IOS.

o avaliador cria um hash e uma cópia de bit a bit da mídia que contém os arquivos, para produzir um clone digital. O avaliador compara o hash da mídia original com a cópia. Se os dois valores forem compatíveis, as cópias são idênticas. O fato de que um conjunto de bits é idêntico ao conjunto original de bits estabelece **invariabilidade**. A invariabilidade ajuda a responder várias perguntas:

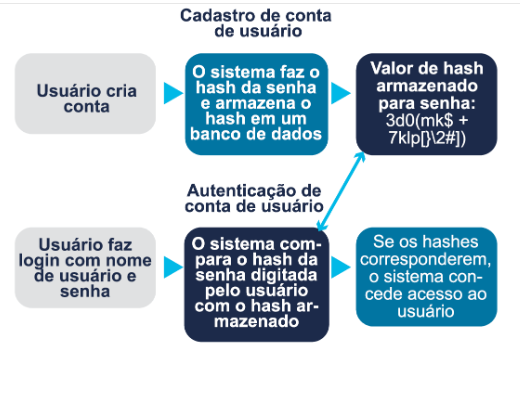
* O avaliador tem os arquivos que ele esperava?
* Os dados foram corrompidos ou alterados?
* O avaliador pode comprovar que os arquivos não estão corrompidos?

8.4.3 Senhas de hash

Os algoritmos hash transformam qualquer quantidade de dados em um hash digital ou impressão digital de tamanho fixo. Ninguém pode reverter um hash digital para descobrir a entrada original. Se a entrada mudar completamente, o resultado será um hash diferente.

Isso funciona para proteger as senhas. Um sistema precisa armazenar uma senha de modo a protegê-la, mas que ainda possa verificar se a senha do usuário está correta.

A figura mostra o fluxo de trabalho para o registo e autenticação da conta do usuário usando um sistema de hash. O sistema nunca registra a senha no disco rígido, ele apenas armazena o hash digital. Dessa forma, a senha é conhecida apenas pelo usuário que a definiu.



8.4.4 Como decifrar hashes

Para decifrar um hash, um invasor deve adivinhar a senha. O ataque de dicionário e o ataque de força bruta são os dois principais ataques usados para adivinhar senhas.

Dicionario

Um ataque de dicionário usa um arquivo que contém palavras, frases e senhas comuns. O arquivo tem os hashes calculados. Um ataque de dicionário compara os hashes no arquivo com os hashes de senha. Se um hash for compatível, o invasor descobrirá um grupo de senhas potencialmente boas.

Força bruta

Um ataque de força bruta tenta todas as combinações possíveis de caracteres até determinado tamanho. Um ataque de força bruta consome muito tempo e energia do processador. Em teoria, é apenas uma questão de tempo até que esse método descubra a senha. O tamanho das senhas precisa ser grande o suficiente para que o tempo gasto para executar um ataque de força bruta valha a pena. As senhas de hash dificultam muito o trabalho do criminoso em recuperar as senhas.

8.4.7 Salteando

O salting torna o hash de senhas mais seguro.

Se dois usuários têm a mesma senha, eles também terão os mesmos hashes de senha. Um SALT, que é uma cadeia de caracteres aleatória, é uma entrada adicional à senha antes do hash.

Isso cria um resultado de hash diferente para as duas senhas, conforme mostrado na figura. Um banco de dados armazena o hash e o SALT. Na figura, a mesma senha gera um hash diferente porque o salt de cada caso é diferente. O salt não precisa ser confidencial porque é um número aleatório.



8.4.8 Implementação de salting

Um Gerador Numérico Pseudo Randômico de Criptografia Segura "Cryptographically Secure Pseudo-Random Number Generator" (CSPRNG) é a melhor opção para gerar o salt.

CSPRNGs geram um número aleatório que tem um alto nível de aleatoriedade e é completamente imprevisível, portanto, é criptograficamente confiável.

As recomendações a seguir ajudarão a garantir a implementação bem-sucedida da salt:

* O salt deve ser exclusivo para cada senha de usuário.
* Nunca reutilize um salt.
* O tamanho do sal deve corresponder ao tamanho da saída da função hash.
* Sempre execute o hash no servidor em um aplicativo da Web.

O uso de uma **técnica chamada alongamento (key stretching)** de chave também ajudará a proteger contra ataques. O alongamento de chaves faz com que as tentativas de descobrir senhas trabalhem muito lentamente. Isso impede o hardware de ponta que pode calcular bilhões de hashes por segundo menos eficazes.

Para armazenar uma senha

Use CSPRNG para gerar um salt longo e aleatório.

Adicione salt no começo da senha.

Execute o hash SHA-256, uma função hash criptográfica padrão.

Salve o salt e o hash como parte do registro do banco de dados do usuário.

Para Validar uma senha

Recupere o salt e hash de um usuário do banco de dados.

Adicione salt à senha e faça o hash com a mesma função hash.

Compare o hash da senha em questão ao armazenado no banco de dados.

Se os hashes não corresponderem, a senha está incorreta.

8.4.9 Como evitar ataques

O salting impede que um invasor use um ataque de dicionário para tentar adivinhar senhas. O salting também torna impossível o uso de tabelas de pesquisa e rainbow tables para decifrar um hash.

tabelas de pesquisa

Uma tabela de pesquisa armazena os hashes de senhas pré-calculados em um dicionário de senha, juntamente com a senha correspondente. Uma tabela de pesquisa é uma estrutura de dados que processa centenas de pesquisas de hash por segundo.

tabelas de pesquisa reversa

Esse ataque permite que o criminoso virtual lance um ataque de dicionário ou um ataque de força bruta em vários hashes, sem a tabela de pesquisa pré-calculada. O criminoso virtual cria uma tabela de pesquisa que traça cada hash de senha a partir do banco de dados da conta violada para uma lista de usuários. O criminoso virtual executa um hash para cada palpite de senha e usa a tabela de pesquisa para obter uma lista de usuários cuja senha é compatível com o palpite do criminoso virtual, como mostrado na figura. O ataque funciona perfeitamente, pois muitos usuários têm a mesma senha.

Rainbow tables

As rainbow tables sacrificam a velocidade de quebra de senha para diminuir o tamanho das tabelas de pesquisa. Uma tabela menor significa que a tabela pode armazenar as soluções para mais hashes na mesma quantidade de espaço.

8.5.1 Uso de assinaturas digitais

As assinaturas digitais são uma técnica matemática usada para fornecer autenticidade, integridade e não repúdio. As assinaturas digitais têm propriedades específicas que permitem autenticação de entidade e integridade de dados. Além disso, as assinaturas digitais fornecem não repúdio da transação. Em outras palavras, a assinatura digital serve como prova legal de que o intercâmbio de dados ocorreu. As assinaturas digitais usam criptografia assimétrica.

Autenticidade

A assinatura não pode ser falsificada e fornece prova de que o signatário, e ninguém mais, assinou o documento.

Inalterável

Após assinar um documento, ele não pode ser alterado.

Não reutilizável

A assinatura do documento não pode ser transferida para outro documento.

Não repudiado

O documento assinado é considerado o mesmo que um documento físico. A assinatura é a prova de que o documento foi assinado pela pessoa real.

As assinaturas digitais são comumente usadas nas duas situações a seguir:

1. **Assinatura de código -** Isso é usado para fins de integridade de dados e autenticação. A assinatura de código é usada para verificar a integridade dos arquivos executáveis baixados do site de um fornecedor. Ela também usa certificados digitais assinados para autenticar e verificar a identidade do site que é a origem dos arquivos.
2. **Certificados digitais -**São semelhantes a um cartão de identificação virtual e usados para autenticar a identidade do sistema com o site de um fornecedor e estabelecer uma conexão criptografada para trocar dados confidenciais.

Existem três algoritmos DSS (Digital Signature Standard) que são usados para gerar e verificar assinaturas digitais:

Algorítimo de assinatura digital - Digital Signature Algorithm (DSA)

DSA é o padrão original para gerar pares de chaves públicas e privadas e para gerar e verificar assinaturas digitais.

Algoritmo Rivest-Shamir Adleman (RSA)

RSA é um algoritmo assimétrico comumente usado para gerar e verificar assinaturas digitais.

Algoritmo de Assinatura Digital de Curvas Elípticas (ECDSA)

ECDSA é uma variante mais recente de DSA e fornece autenticação de assinatura digital e não repúdio com os benefícios adicionais de eficiência computacional, tamanhos de assinatura pequenos e largura de banda mínima.

8.5.2 Assinaturas digitais para assinatura de código

As assinaturas digitais são comumente usadas para garantir a autenticidade e integridade do código de software. Os arquivos executáveis são empacotados em um envelope assinado digitalmente, o que permite ao usuário final verificar a assinatura antes de instalar o software.

Assinar digitalmente o código fornece várias garantias sobre o código:

* O código é autêntico e é realmente originado pela editora.
* O código não foi modificado desde que saiu do editor do software.
* A editora publicou inegavelmente o código. Isso fornece não repúdio do ato de publicação.

A Publicação 140-3 do FIPS (Federal Information Processing Standard) do Governo dos EUA especifica que o software disponível para download na internet deve ser assinado e verificado digitalmente.

8.5.3 Assinaturas digitais para certificados digitais

Um certificado digital é equivalente a um passaporte eletrônico. Ele permite que usuários, hosts e organizações troquem informações com segurança pela Internet. Especificamente, um certificado digital é usado para autenticar e verificar se um usuário que está enviando uma mensagem é quem afirma ser. Os certificados digitais também podem ser usados para fornecer confidencialidade ao receptor com os meios de criptografar uma resposta.

O certificado digital verifica de forma independente uma identidade. Assinaturas digitais são usadas para verificar se um artefato, como um arquivo ou mensagem, é enviado pelo indivíduo verificado. Em outras palavras, um certificado verifica a identidade, uma assinatura verifica se algo vem dessa identidade.

Esse cenário ajudará você a entender como uma assinatura digital é usada. Bob está confirmando um pedido com Alice. Alice está encomendando do site do Bob. Alice se conectou com o site de Bob, e depois que o certificado foi verificado, o certificado de Bob é armazenado no site de Alice. O certificado contém a chave pública de Bob. A chave pública é usada para verificar a assinatura digital do Bob.

1. Bob confirma a ordem e seu computador cria um hash da confirmação. O computador criptografa o hash com a chave privada do Bob. O hash criptografado, que é a assinatura digital, é anexado ao documento. A confirmação do pedido é então enviada para Alice através da internet. O dispositivo receptor de Alice aceita a confirmação do pedido com a assinatura digital e obtém a chave pública de Bob.
2. O computador de Alice descodifica a assinatura usando a chave pública de Bob. Esta etapa revela o valor de hash assumido do dispositivo de envio.
3. O computador de Alice cria um hash do documento recebido, sem sua assinatura, e compara esse hash com o hash de assinatura descriptografado. Se os hashes corresponderem, o documento é autêntico. Isso significa que a confirmação foi enviada por Bob e que ela não mudou desde que foi assinada.

8.6.1 Gerenciamento de Chave Pública

O tráfego da Internet consiste no tráfego entre duas partes. Ao estabelecer uma conexão assimétrica entre dois hosts, os hosts trocarão suas informações de chave pública.

Um certificado SSL é um certificado digital que confirma a identidade de um domínio de site. Para implementar SSL em seu site, você compra um certificado SSL para seu domínio de um provedor de Certificado SSL. O empresa terceirizada de confiança faz uma investigação aprofundada antes da emissão das credenciais. Após essa investigação aprofundada, o terceiro emite credenciais (ou seja, certificado digital) que são difíceis de falsificar. Desse ponto em diante, todos os indivíduos que confiam no terceiro simplesmente aceitam as credenciais que o terceiro emite. Quando os computadores tentam se conectar a um site via HTTPS, o navegador verifica o certificado de segurança do site e verifica se ele é válido e originado com uma autoridade de certificação confiável. Isso valida que a identificação do site é verdadeira. O certificado é salvo localmente pelo navegador da Web e, em seguida, é usado em transações subsequentes. A chave pública do site está incluída no certificado e é usada para verificar futuras comunicações entre o site e o cliente.

A Infraestrutura de Chave Pública (PKI) consiste em especificações, sistemas e ferramentas que são usados para criar, gerenciar, distribuir, usar, armazenar e revogar certificados digitais. A autoridade de certificação (CA) é uma organização que cria certificados digitais vinculando uma chave pública a uma identificação confirmada, como um site ou indivíduo. O PKI é um sistema complexo que é projetado para proteger identidades digitais contra hackers até mesmo os atores de ameaças mais sofisticados ou estados-nação.

Alguns exemplos de Autoridades de Certificação são IDentrust, DigiCert, Sectigo, GlobalSign e GoDaddy. Essas CAs cobram por seus serviços. Let's Encrypt é uma CA sem fins lucrativos que oferece certificados gratuitamente.

8.6.2 A infraestrutura de chave pública

A PKI é necessária para oferecer suporte à distribuição em larga escala e à identificação de chaves de criptografia públicas. A estrutura PKI facilita uma relação de confiança altamente escalável.

Consiste em hardware, software, pessoas, políticas e procedimentos necessários para criar, gerenciar, armazenar, distribuir e revogar certificados digitais.

1. Os certificados PKI contêm a chave pública de uma entidade ou de um indivíduo, a sua finalidade, a autoridade de certificação (AC) que validou e emitiu o certificado, o intervalo de datas durante o qual o certificado é válido e o algoritmo usado para criar a assinatura.
2. O armazenamento de certificados reside em um computador local e armazena certificados emitidos e chaves privadas.
3. O Certificado de Autoridade PKI (CA) é um terceiro confiável que emite certificados PKI para entidades e indivíduos após verificar sua identidade. Ele assina esses certificados usando sua chave privada.
4. O banco de dados de certificados armazena todos os certificados aprovados pela autoridade de certificação.

* Neste exemplo, Bob recebeu seu certificado digital da CA. Este certificado é usado sempre que Bob se comunica com outras partes.
* Bob se comunica com Alice.
* Quando Alice recebe o certificado digital de Bob, ela se comunica com a autoridade de certificação confiável para validar a identidade de Bob.

**Observação**: nem todos os certificados PKI são recebidos diretamente de uma autoridade de certificação. Uma autoridade de registro (RA) é uma autoridade de certificação subordinada e é certificada por uma autoridade de certificação raiz para emitir certificados para usos específicos.

8.6.3 O Sistema de Autoridades PKI

Muitos fornecedores fornecem servidores da CA como um serviço gerenciado ou como um produto de usuário final. Alguns desses fornecedores incluem Symantec Group (VeriSign), Comodo, Go Daddy Group, GlobalSign e DigiCert, entre outros.

As organizações também podem implementar PKIs privadas usando o Microsoft Server ou Open SSL.

As autoridades de certificação, especialmente aquelas que são terceirizadas, emitem certificados baseados em classes que determinam a confiabilidade de um certificado.

|  |  |
| --- | --- |
| **Classe** | **Descrição** |
| 0 | Usado para testes em situações em que não foram realizadas verificações. |
| 1 | Usado por indivíduos que exigem verificação de e-mail. |
| 2 | Usado por organizações para as quais a prova de identidade é necessária. |
| 3 | Usado para servidores e assinatura de software. A verificação independente e a verificação de identidade e autoridade são feitas pela autoridade de certificação. |
| 4 | Usado para transações comerciais on-line entre empresas. |
| 5 | Usado para organizações privadas ou segurança do governo. |

A tabela fornece uma descrição das classes. O número de classe é determinado pelo rigor do procedimento que verificou a identidade do titular quando o certificado foi emitido. Quanto maior o número da classe, mais confiável será o certificado. Portanto, um certificado de classe 5 é muito mais confiável do que um certificado de classe inferior.

Teste de componentes do iFrame

Por exemplo, um certificado de classe 1 pode exigir uma resposta por e-mail do titular para confirmar que deseja se inscrever. Este tipo de confirmação é uma autenticação fraca do titular. Para um certificado de classe 3 ou 4, o futuro titular deve provar a identidade e autenticar a chave pública aparecendo pessoalmente com pelo menos dois documentos de identificação oficiais.

Algumas chaves públicas da CA são pré-carregadas, como as listadas em navegadores da Web.

**Nota**: Uma empresa também pode implementar PKI para uso interno. A PKI pode ser usada para autenticar funcionários que estão acessando a rede. Nesse caso, a empresa é sua própria CA.

**8.6.4 O Sistema de Confiança PKI**

**Topologia PKI de raiz única**

PKIs podem formar diferentes topologias de confiança. O mais simples é a topologia PKI de raiz única.

Como mostrado na figura abaixo, uma única autoridade de certificação, chamada de CA raiz, emite todos os certificados para os usuários finais, que geralmente estão dentro da mesma organização. O benefício desta abordagem é a sua simplicidade. No entanto, é difícil dimensionar para um ambiente grande porque requer uma administração estritamente centralizada, o que cria um único ponto de falha.

**CA com certificação cruzada**

Em redes maiores, as CAs PKI podem ser vinculadas usando duas arquiteturas básicas:

**Topologias de AC certificadas cruzadas** - Conforme mostrado na figura abaixo, este é um modelo ponto a ponto no qual as ACs individuais estabelecem relações de confiança com outras ACs através da certificação cruzada de certificados de AC. Os usuários em ambos os domínios da CA também têm a certeza de que podem confiar uns nos outros. Isso fornece redundância e elimina o ponto único de falha.

**CA hierárquica**

**Topologias de CA hierárquicas** - Conforme mostrado na figura abaixo, a CA de nível mais alto é chamada de CA raiz. Ele pode emitir certificados para usuários finais e para uma autoridade de certificação subordinada. As subCAs podem ser criadas para suportar várias unidades de negócios, domínios ou comunidades de confiança. A autoridade de certificação raiz mantém a “comunidade de confiança” estabelecida garantindo que cada entidade na hierarquia esteja em conformidade com um conjunto mínimo de práticas. Os benefícios dessa topologia incluem maior escalabilidade e capacidade de gerenciamento. Esta topologia funciona bem na maioria das grandes organizações. No entanto, pode ser difícil determinar a cadeia do processo de assinatura.

Uma topologia hierárquica e de certificação cruzada pode ser combinada para criar uma infraestrutura híbrida. Um exemplo seria quando duas comunidades hierárquicas querem certificar-se entre si para que os membros de cada comunidade confiem uns nos outros.

8.6.5 Interoperabilidade de diferentes fornecedores de PKI

A interoperabilidade entre uma PKI e seus serviços de suporte, como o Lightweight Directory Access Protocol (LDAP) e diretórios X.500, é uma preocupação porque muitos fornecedores de CA propuseram e implementaram soluções proprietárias em vez de aguardar o desenvolvimento de padrões.

**Observação**: LDAP e X.500 são protocolos usados para consultar um serviço de diretório, como o Microsoft Active Directory, para verificar um nome de usuário e senha.

Para resolver esse problema de interoperabilidade, o IETF publicou o Internet X.509 Public Key Infrastructure Policy and Certification Practices Framework (RFC 2527). O padrão X.509 versão 3 (X.509 v3) define o formato de um certificado digital.

Consulte a figura para obter mais informações sobre aplicativos X.509 v3. Como mostrado na figura, o formato X.509 já é amplamente utilizado na infra-estrutura da internet.

**Aplicações x.509v3**

A figura mostra um servidor Web externo rotulado com o número circulado 1 e S S L que se conecta a um firewall. O firewall tem outra conexão com um concentrador V P N abaixo dele rotulado com o número 2 circulado e as palavras I P s e c. O firewall tem uma terceira conexão com uma nuvem rotulada Internet. O firewall tem outra conexão com uma nuvem de rede corporativa que inclui um servidor CA, um servidor de email da Internet que tem o número circulado 3 e S/MIME ao lado dele, e servidores que têm o Cisco Secure ACS ao lado dele e o número circulado quatro palavras EAP - TLS ao lado dele.

1. **SSL** - Servidores Web seguros Use X.509.v3 para autenticação do site nos protocolos SSL e TLS, enquanto os navegadores da Web usam X.509V3 para implementar certificados de cliente HTTPS. SSL é a autenticação baseada em certificado mais utilizada.
2. **IPsec** - IPsec VPNS usa certificados X.509 quando a autenticação baseada em RSA é usada para a Intercâmbio de chaves da Internet (IKE).
3. **S/MIME** - Agentes de correio de utilizador que suportam protecção de correio com o protocolo S/MIME (Secure/Multipurpose Internet Mail Extensions) utilizam certificados X.509.
4. **EAP - TLS** - Os switches Cisco podem usar certificados para autenticar dispositivos finais que se conectam a portas lan usando 802.1.x entre os dispositivos adjacentes. A autenticação pode ser proxy para um ACS central por meio do Extensible Authentication Protocol with TLS (EAP-TLS).

8.6.6 Inscrição, autenticação e revogação de certificados

A primeira etapa no procedimento de autenticação da autoridade de certificação é obter com segurança uma cópia da chave pública da autoridade de certificação. Todos os sistemas que utilizam a PKI devem ter a chave pública da autoridade de certificação, que é chamada de certificado autoassinado. A chave pública da autoridade de certificação verifica todos os certificados emitidos pela autoridade de certificação e é vital para o bom funcionamento da PKI.

**Observação**: somente uma autoridade de certificação raiz pode emitir um certificado autoassinado reconhecido ou verificado por outras autoridades de certificação dentro da PKI.

Para muitos sistemas, como navegadores da Web, a distribuição de certificados de CA é processada automaticamente. O navegador da Web vem pré-instalado com um conjunto de certificados raiz de CA públicos. As organizações e seus domínios do site enviam seus certificados públicos para os visitantes do site. As autoridades de certificação e os registradores de domínio de certificado criam e distribuem certificados privados e públicos para clientes que compram certificados.

O processo de registro de certificado é usado por um sistema host para se inscrever com uma PKI. Para fazer isso, os certificados de CA são recuperados em banda através de uma rede e a autenticação é feita fora de banda (OOB) usando o telefone. O registro do sistema com a PKI entra em contato com uma autoridade de certificação para solicitar e obter um certificado de identidade digital para si mesmo e para obter o certificado autoassinado da autoridade de certificação. O estágio final verifica se o certificado da autoridade de certificação foi autêntico e é executado usando um método fora de banda, como o sistema de telefone antigo simples (POTS), para obter a impressão digital do certificado de identidade da autoridade de certificação válido.

A autenticação não requer mais a presença do servidor da autoridade de certificação e cada usuário troca seus certificados contendo chaves públicas.

Os certificados devem, por vezes, ser revogados. Por exemplo, um certificado digital pode ser revogado se a chave for comprometida ou se não for mais necessário.

**Clique em cada título para obter os métodos mais comuns de revogação**

Lista de revogação de certificados (CRL)

Uma lista de números de série de certificados revogados que foram invalidados porque expiraram. As entidades PKI pesquisam regularmente o repositório CRL para receber a CRL atual.

Protocolo de status de certificado on-line (OCSP)

Um protocolo de Internet usado para consultar um servidor OCSP para o status de revogação de um certificado digital X.509. As informações de revogação são imediatamente enviadas para um banco de dados on-line.

8.7.1 Aplicações PKI

Onde a PKI pode ser usada por uma empresa? O seguinte fornece uma pequena lista de usos comuns de PKIs:

* Autenticação de peer baseada em certificado SSL/TLS
* Proteja o tráfego de rede usando VPNs IPsec
* Tráfego da web HTTPS
* Controle o acesso à rede usando a autenticação 802.1x
* E-mail seguro usando o protocolo S/MIME
* Mensagens instantâneas seguras
* Aprovar e autorizar aplicativos com assinatura de código
* Proteja os dados do usuário com o sistema de arquivos de criptografia (EFS)
* Implementar autenticação de dois fatores com cartões inteligentes
* Protegendo dispositivos de armazenamento USB

8.7.2 Transações de rede criptográfica

Um analista de segurança deve ser capaz de reconhecer e resolver possíveis problemas relacionados à permissão de soluções relacionadas à PKI na rede corporativa.

Considere como o aumento do tráfego SSL/TLS representa um grande risco de segurança para as empresas porque o tráfego é criptografado e não pode ser interceptado e monitorado por meios normais. Os usuários podem introduzir malware ou vazar informações confidenciais através de uma conexão SSL/TLS.

Os atores de ameaças podem usar SSL/TLS para introduzir violações de conformidade regulatória, vírus, malware, perda de dados e tentativas de intrusão em uma rede.

Outros problemas relacionados a SSL/TLS podem estar associados à validação do certificado de um servidor Web. Quando isso ocorre, os navegadores da Web exibirão um aviso de segurança. Os problemas relacionados à PKI associados a avisos de segurança incluem:

* **Intervalo de datas de validade** - Os certificados X.509v3 especificam datas “não antes” e “não depois”. Se a data atual estiver fora do intervalo, o navegador da Web exibirá uma mensagem. Os certificados expirados podem simplesmente ser o resultado da supervisão do administrador, mas também podem refletir condições mais graves.
* **Erro de validação de assinatura**- Se um navegador não puder validar a assinatura do certificado, não há garantia de que a chave pública do certificado seja autêntica. A validação de assinatura falhará se o certificado raiz da hierarquia da autoridade de certificação não estiver disponível no armazenamento de certificados do navegador.

Alguns desses problemas podem ser evitados devido ao fato de que os protocolos SSL/TLS são extensíveis e modulares. Isto é conhecido como um conjunto de cifras. Os principais componentes do conjunto de cifras são o MAC (Message Authentication Code Algoritmo), o algoritmo de criptografia, o algoritmo de troca de chaves e o algoritmo de autenticação. Estes podem ser alterados sem substituir todo o protocolo. Isso é muito útil porque os diferentes algoritmos continuam a evoluir. À medida que a criptoanálise continua a revelar falhas nesses algoritmos, o conjunto de cifras pode ser atualizado para corrigir essas falhas. Quando as versões de protocolo dentro do conjunto de cifras mudam, o número de versão do SSL/TLS também muda.

8.7.3 Criptografia e monitoramento de segurança

O monitoramento de rede torna-se mais desafiador quando os pacotes são criptografados. No entanto, os analistas de segurança devem estar cientes desses desafios e enfrentá-los da melhor forma possível. Por exemplo, quando VPNs site a site são usadas, o IPS deve ser posicionado para que ele possa monitorar o tráfego não criptografado.

No entanto, o aumento do uso de HTTPS na rede empresarial introduz novos desafios. Como o HTTPS introduz tráfego HTTP criptografado de ponta a ponta (via TLS/SSL), não é tão fácil espiar o tráfego do usuário.

Os analistas de segurança devem saber como contornar e resolver esses problemas. Aqui está uma lista de algumas das coisas que um analista de segurança pode fazer:

* Configure regras para distinguir entre tráfego SSL e não-SSL, tráfego SSL HTTPS e não-HTTPS.
* Melhore a segurança através da validação de certificados de servidor utilizando CRLs e OCSP.
* Implemente proteção antimalware e filtragem de URL de conteúdo HTTPS.
* Implante um Cisco SSL Appliance para descriptografar o tráfego SSL e enviá-lo para dispositivos IPS (Intrusion Prevention System, sistema de prevenção de intrusões) para identificar riscos normalmente ocultos pelo SSL.

A criptografia é dinâmica e está sempre mudando. Um analista de segurança deve manter um bom entendimento de algoritmos criptográficos e operações para ser capaz de investigar incidentes de segurança relacionados à criptografia.

Há duas maneiras principais em que a criptografia afeta as investigações de segurança. Primeiro, os ataques podem ser direcionados especificamente para os próprios algoritmos de criptografia. Após o algoritmo ter sido rachado e o invasor obter as chaves, todos os dados criptografados que foram capturados podem ser descriptografados pelo invasor e lidos, expondo assim dados privados. Em segundo lugar, a investigação de segurança também é afetada porque os dados podem ser escondidos à vista, encriptando-os. Por exemplo, o tráfego de comando e controle criptografado com TLS/SSL provavelmente não pode ser visto por um firewall. O tráfego de comando e controle entre um servidor de comando e controle e um computador infectado em uma rede segura não pode ser interrompido se não puder ser visto e compreendido. O invasor seria capaz de continuar usando comandos criptografados para infectar mais computadores e, possivelmente, criar uma botnet. Esse tipo de tráfego pode ser detectado descriptografando o tráfego e comparando-o com assinaturas de ataque conhecidas ou detectando tráfego TLS/SSL anômalo. Isso é muito difícil e demorado, ou um processo de acerto ou erro.

9.1.1 Syslog e NTP

Vários protocolos que geralmente aparecem em redes têm recursos que os tornam de especial interesse no monitoramento de segurança. Por exemplo, syslog e Network Time Protocol (NTP) são essenciais para o trabalho do analista de segurança cibernética.

O padrão syslog é usado para registrar mensagens de eventos de dispositivos de rede e endpoints, conforme mostrado na figura. O padrão permite um meio neutro de sistema de transmissão, armazenamento e análise de mensagens. Muitos tipos de dispositivos de vários fornecedores diferentes podem usar syslog para enviar entradas de log para servidores centrais que executam um daemon syslog. Esta centralização da coleta de logs ajuda a tornar o monitoramento de segurança prático. Os servidores que executam syslog normalmente escutam na porta UDP 514.

Como o syslog é tão importante para o monitoramento de segurança, os servidores syslog podem ser um alvo para atores de ameaças. Algumas explorações, como aquelas que envolvem extração de dados, podem levar muito tempo para serem concluídas. Isso ocorre porque as maneiras pelas quais os dados são roubados secretamente da rede podem ser muito lentos. Alguns atacantes podem tentar ocultar o fato de que a exfiltração está ocorrendo. Eles atacam servidores syslog que contêm as informações que podem levar à detecção da exploração. Os hackers podem tentar bloquear a transferência de dados de clientes de syslog para servidores. Eles podem violar ou destruir dados de log ou o software que cria e transmite mensagens de log. A implementação do syslog de próxima geração (ng), conhecida como syslog-ng, oferece aprimoramentos que podem ajudar a evitar algumas das explorações que visam o syslog.

Search the internet for more information about syslog-ng.

9.1.2 NTP

As mensagens do Syslog geralmente são carimbadas de data e hora. Isso permite que mensagens de diferentes fontes sejam organizadas pelo tempo para fornecer uma visão dos processos de comunicação de rede. Como as mensagens podem vir de muitos dispositivos, é importante que os dispositivos compartilhem um timeclock consistente. Uma maneira que isso pode ser alcançado é para os dispositivos usarem o Network Time Protocol (NTP). O NTP usa uma hierarquia de fontes de tempo autoritativas para compartilhar informações de tempo entre dispositivos na rede, conforme mostrado na figura. Dessa forma, as mensagens de dispositivo que compartilham informações de tempo consistentes podem ser enviadas para o servidor syslog. O NTP opera na porta UDP 123.

Como os eventos conectados a uma exploração podem deixar rastros em todos os dispositivos de rede em seu caminho para o sistema de destino, os carimbos de data/hora são essenciais para detecção. Os atores de ameaças podem tentar atacar a infraestrutura NTP para corromper as informações de tempo usadas para correlacionar eventos de rede registrados. Isso pode servir para ofuscar vestígios de explorações em curso. Além disso, os atores de ameaças têm sido conhecidos por usar sistemas NTP para direcionar ataques DDoS por meio de vulnerabilidades no software cliente ou servidor. Embora esses ataques não resultem necessariamente em dados de monitoramento de segurança corrompidos, eles podem interromper a disponibilidade da rede.

9.1.3 DNS

O Serviço de Nome de Domínio (DNS) é usado por milhões de pessoas diariamente. Por isso, muitas organizações têm políticas menos rigorosas para proteger contra ameaças baseadas em DNS do que precisam proteger contra outros tipos de explorações. Os invasores reconheceram isso e geralmente encapsulam diferentes protocolos de rede no DNS para evitar dispositivos de segurança. O DNS agora é usado por muitos tipos de malware. Algumas variedades de malware usam DNS para se comunicar com servidores de comando e controle (CNC) e para exfiltrar dados no tráfego disfarçados como consultas DNS normais. Vários tipos de codificação, como Base64, binário de 8 bits e Hex podem ser usados para camuflar os dados e evitar medidas básicas de prevenção de perda de dados (DLP).

Por exemplo, malware pode codificar dados roubados como a parte de subdomínio de uma pesquisa DNS para um domínio onde o servidor de nomes está sob controle de um invasor. Uma pesquisa de DNS para 'long string-of-exfiltrated-data.example.com' seria encaminhada para o servidor de nomes de example.com, que gravaria 'long string-of-exfiltrated-data' e responderia de volta ao malware com uma resposta codificada. Este uso do subdomínio DNS é mostrado na figura. Os dados exfiltrados são o texto codificado mostrado na caixa. O ator de ameaças coleta esses dados codificados, decodifica e combina e agora tem acesso a um arquivo de dados inteiro, como um banco de dados de nome de usuário/senha.

É provável que a parte do subdomínio de tais solicitações seria muito mais longa do que as solicitações usuais. Analistas cibernéticos podem usar a distribuição dos comprimentos de subdomínios dentro de solicitações DNS para construir um modelo matemático que descreva a normalidade. Eles podem então usar isso para comparar suas observações e identificar um abuso do processo de consulta DNS. Por exemplo, não seria normal ver um host em sua rede enviando uma consulta para AW4GCGXHy2UGDG8GCHJVDGVJDC.Example.com.

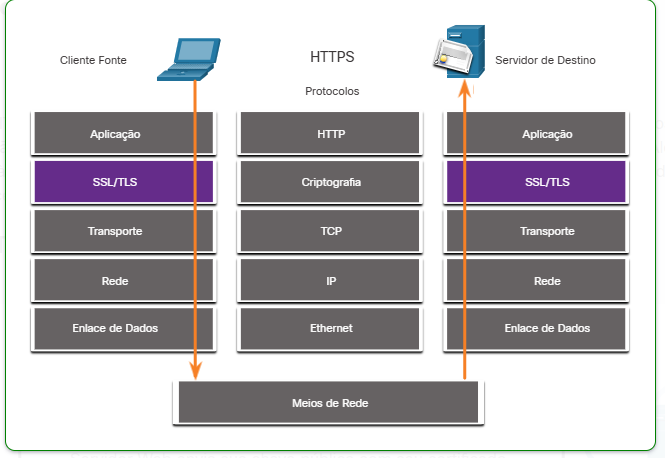
9.1.4 HTTP e HTTPS

O Hypertext Transfer Protocol (HTTP) é o protocolo de backbone da World Wide Web. No entanto, todas as informações transportadas em HTTP são transmitidas em texto simples do computador de origem para o destino na internet. O HTTP não protege os dados contra alteração ou interceptação por partes mal-intencionadas, o que é uma séria ameaça à privacidade, identidade e segurança das informações. Todas as atividades de navegação devem ser consideradas em risco.

Uma exploração comum de HTTP é chamada de injeção iFrame (quadro inline). A maioria das ameaças baseadas na Web consiste em scripts de malware que foram plantados em servidores web. Esses servidores da Web direcionam os navegadores para servidores infectados carregando iframes. Na injeção iFrame, um ator de ameaça compromete um servidor da Web e planta código malicioso que cria um iFrame invisível em uma página da Web comumente visitada. Quando o iFrame é carregado, o malware é baixado, freqüentemente de um URL diferente da página da Web que contém o código iFrame. Os serviços de segurança de rede, como a filtragem Cisco Web Reputation, podem detectar quando um site tenta enviar conteúdo de um site não confiável para o host, mesmo quando enviado de um IFrame, conforme mostrado na figura.

Para lidar com a alteração ou interceptação de dados confidenciais, muitas organizações comerciais adotaram HTTPS ou implementaram políticas somente HTTPS para proteger os visitantes de seus sites e serviços.

HTTPS adiciona uma camada de criptografia ao protocolo HTTP usando Secure Socket Layer (SSL), como mostrado na figura. Isso torna os dados HTTP ilegíveis, pois deixam o computador de origem até chegar ao servidor. Observe que HTTPS não é um mecanismo para a segurança do servidor Web. Ele só protege o tráfego de protocolo HTTP enquanto está em trânsito.



Infelizmente, o tráfego HTTPS criptografado complica o monitoramento de segurança de rede. Alguns dispositivos de segurança incluem descriptografia e inspeção SSL; no entanto, isso pode apresentar problemas de processamento e privacidade. Além disso, o HTTPS adiciona complexidade às capturas de pacotes devido às mensagens adicionais envolvidas no estabelecimento da conexão criptografada. Esse processo é resumido na figura e representa sobrecarga adicional sobre HTTP.

9.1.5 Protocolos de email

Protocolos de e-mail como SMTP, POP3 e IMAP podem ser usados por atores de ameaças para espalhar malware, exfiltrar dados ou fornecer canais para servidores CNC de malware, como mostrado na figura.

SMTP envia dados de um host para um servidor de email e entre servidores de email. Como DNS e HTTP, é um protocolo comum para ver sair da rede. Como há muito tráfego SMTP, ele nem sempre é monitorado. No entanto, o SMTP foi usado no passado por malware para exfiltrar dados da rede. No 2014 hack da Sony Pictures, uma das explorações usou SMTP para exfiltrar detalhes do usuário de hosts comprometidos para servidores CNC. Essas informações podem ter sido usadas para ajudar a desenvolver explorações de recursos protegidos na rede Sony Pictures. O monitoramento de segurança pode revelar esse tipo de tráfego com base nos recursos da mensagem de email.

IMAP e POP3 são usados para baixar mensagens de email de um servidor de email para o computador host. Por esse motivo, eles são os protocolos de aplicativos que são responsáveis por trazer malware para o host. O monitoramento de segurança pode identificar quando um anexo de malware entrou na rede e qual host ele infectou pela primeira vez. A análise retrospectiva pode então rastrear o comportamento do malware a partir desse ponto em diante. Desta forma, o comportamento do malware pode ser melhor compreendido e a ameaça identificada. As ferramentas de monitoramento de segurança também podem permitir a recuperação de anexos de arquivos infectados para envio a caixas de proteção de malware para análise.

9.1.6 ICMP

ICMP tem muitos usos legítimos, no entanto, a funcionalidade ICMP também tem sido usada para criar vários tipos de explorações. O ICMP pode ser usado para identificar hosts em uma rede, a estrutura de uma rede e determinar os sistemas operacionais em uso na rede. Ele também pode ser usado como um veículo para vários tipos de ataques DoS.

ICMP também pode ser usado para exfiltração de dados. Devido à preocupação de que o ICMP possa ser usado para vigiar ou negar o serviço de fora da rede, o tráfego ICMP de dentro da rede às vezes é ignorado. No entanto, algumas variedades de malware usam pacotes ICMP criados para transferir arquivos de hosts infectados para agentes ameaçadores usando esse método, conhecido como tunelamento ICMP.

9.2.1 ACLs

Muitas tecnologias e protocolos podem ter impacto no monitoramento de segurança. Listas de Controle de Acesso (ACLs) estão entre essas tecnologias. As ACLs podem dar uma falsa sensação de segurança se forem excessivamente confiadas. As ACLs e a filtragem de pacotes em geral são tecnologias que contribuem para um conjunto em evolução de proteções de segurança de rede.

Os invasores podem determinar quais endereços IP, protocolos e portas são permitidos pelas ACLs. Isso pode ser feito por varredura de portas, testes de penetração ou através de outras formas de reconhecimento. Os atacantes podem criar pacotes que usam endereços IP de origem falsificados. Os aplicativos podem estabelecer conexões em portas arbitrárias. Outros recursos do tráfego de protocolo também podem ser manipulados, como o sinalizador estabelecido em segmentos TCP. As regras não podem ser antecipadas e configuradas para todas as técnicas de manipulação de pacotes emergentes.

Para detectar e reagir à manipulação de pacotes, comportamentos mais sofisticados e medidas baseadas em contexto precisam ser tomadas. Os firewalls de próxima geração da Cisco, o AMP (Advanced Malware Protection) e os appliances de conteúdo de e-mail e Web são capazes de resolver as deficiências das medidas de segurança baseadas em regras.

9.2.2 NAT e PAT

Conversão de Endereços de Rede (NAT) e Tradução de Endereço de Porta (PAT) podem complicar o monitoramento de segurança. Vários endereços IP são mapeados para um ou mais endereços públicos visíveis na Internet, ocultando os endereços IP individuais que estão dentro da rede (endereços internos).

A figura ilustra a relação entre endereços internos e externos que são usados como endereços de origem (SA) e endereços de destino (DA). Esses endereços internos e externos estão em uma rede que está usando NAT para se comunicar com um destino na Internet. Se o PAT estiver em vigor e todos os endereços IP que saem da rede usarem o endereço global 209.165.200.226 interno para tráfego na Internet, pode ser difícil registrar o dispositivo interno específico que está solicitando e recebendo o tráfego quando ele entra na rede.

Esse problema pode ser especialmente relevante com dados NetFlow. Os fluxos de NetFlow são unidirecionais e são definidos pelos endereços e portas que eles compartilham. O NAT basicamente quebrará um fluxo que passa por um gateway NAT, tornando as informações de fluxo além desse ponto indisponíveis. A Cisco oferece produtos de segurança que irão “costurar” fluir juntos mesmo que os endereços IP tenham sido substituídos pelo NAT.

9.2.3 Criptografia, encapsulamento e tunelamento

Como mencionado com HTTPS, a criptografia pode apresentar desafios para o monitoramento de segurança tornando os detalhes do pacote ilegíveis. A criptografia faz parte das tecnologias VPN. Nas VPNs, um protocolo comum, como IP, é usado para transportar tráfego criptografado. O tráfego criptografado essencialmente estabelece uma conexão virtual ponto a ponto entre redes através de instalações públicas. A criptografia torna o tráfego ilegível para outros dispositivos, exceto os endpoints VPN.

Uma tecnologia semelhante pode ser usada para criar uma conexão virtual ponto a ponto entre um host interno e dispositivos de atores de ameaças. O malware pode estabelecer um túnel criptografado que usa um protocolo comum e confiável e usá-lo para extrair dados da rede. Um método semelhante de exfiltração de dados foi discutido anteriormente para DNS.

9.2.4 Rede ponto a ponto e Tor

Na rede ponto a ponto (P2P), mostrada na figura, os hosts podem operar em funções de cliente e servidor. Existem três tipos de aplicativos P2P: compartilhamento de arquivos, compartilhamento de processadores e mensagens instantâneas. No compartilhamento de arquivos P2P, os arquivos em uma máquina participante são compartilhados com membros da rede P2P. Exemplos disso são os outrora populares Napster e Gnutella. Bitcoin é uma operação P2P que envolve o compartilhamento de um banco de dados distribuído, ou razão, que registra saldos e transações Bitcoin. BitTorrent é uma rede de compartilhamento de arquivos P2P.

Sempre que os usuários desconhecidos recebem acesso aos recursos de rede, a segurança é uma preocupação. Aplicativos P2P de compartilhamento de arquivos não devem ser permitidos em redes corporativas. A atividade da rede P2P pode contornar as proteções de firewall e é um vetor comum para a propagação de malware. P2P é inerentemente dinâmico. Ele pode operar conectando-se a vários endereços IP de destino e também pode usar numeração dinâmica de portas. Arquivos compartilhados são frequentemente infectados com malware, e os atores de ameaças podem posicionar seu malware em clientes P2P para distribuição a outros usuários.

As redes P2P de compartilhamento de processadores doam ciclos de processador para tarefas computacionais distribuídas. Pesquisa de câncer, pesquisa de extraterrestres, e pesquisa científica usam ciclos de processador doados para distribuir tarefas computacionais.

Mensagens instantâneas (IM) também é considerado um aplicativo P2P. IM tem valor legítimo dentro de organizações que têm equipes de projeto distribuídas geograficamente. Nesse caso, aplicativos de IM especializados estão disponíveis, como a plataforma Webex Teams, que são mais seguras do que as mensagens instantâneas que usam servidores públicos.

Tor é uma plataforma de software e rede de hosts P2P que funcionam como roteadores de internet na rede Tor. A rede Tor permite que os usuários naveguem na internet anonimamente. Os usuários acessam a rede Tor usando um navegador especial. Quando uma sessão de navegação é iniciada, o navegador constrói um caminho de ponta a ponta em camadas na rede do servidor Tor que é criptografado, como mostrado na figura. Cada camada criptografada é “removida” como as camadas de uma cebola (portanto, “onion routing”) à medida que o tráfego atravessa um retransmissor do Tor. As camadas contêm informações criptografadas do próximo salto que só podem ser lidas pelo roteador que precisa ler as informações. Dessa forma, nenhum dispositivo único conhece todo o caminho para o destino e as informações de roteamento só podem ser lidas pelo dispositivo que as requer. Finalmente, no final do caminho do Tor, o tráfego atinge seu destino na internet. Quando o tráfego é retornado à origem, um caminho criptografado em camadas é construído novamente.

Tor apresenta uma série de desafios aos analistas de segurança cibernética. Primeiro, o Tor é amplamente utilizado por organizações criminosas na “Dark Net”. Além disso, Tor tem sido usado como um canal de comunicação para malware CNC. Como o endereço IP de destino do tráfego Tor é ofuscado pela criptografia, com apenas o nó Tor de próximo salto conhecido, o tráfego Tor evita listas negras configuradas em dispositivos de segurança.

9.2.5 Balanceamento de carga

O balanceamento de carga envolve a distribuição do tráfego entre dispositivos ou caminhos de rede para evitar recursos de rede sobrecarregados com muito tráfego. Se existirem recursos redundantes, um algoritmo ou dispositivo de balanceamento de carga funcionará para distribuir o tráfego entre esses recursos, conforme mostrado na figura.

Uma maneira de fazer isso na internet é através de várias técnicas que usam DNS para enviar tráfego para recursos que têm o mesmo nome de domínio, mas vários endereços IP. Em alguns casos, a distribuição pode ser para servidores que são distribuídos geograficamente. Isso pode resultar em uma única transação de Internet sendo representada por vários endereços IP nos pacotes de entrada. Isso pode fazer com que recursos suspeitos apareçam em capturas de pacotes. Além disso, alguns dispositivos do gerenciador de balanceamento de carga (LBM) usam testes para testar o desempenho de diferentes caminhos e a integridade de diferentes dispositivos. Por exemplo, um LBM pode enviar testes para os diferentes servidores para os quais ele está balanceando o tráfego de carga, a fim de detectar que os servidores estão operando. Isso é feito para evitar o envio de tráfego para um recurso que não está disponível. Esses testes podem parecer tráfego suspeito se o analista de segurança cibernética não estiver ciente de que esse tráfego faz parte da operação do LBM.

10.1.1 Dados de alerta

Os dados de alerta consistem em mensagens geradas por sistemas de prevenção de intrusões (IPSs) ou sistemas de detecção de intrusões (IDSs) em resposta ao tráfego que viola uma regra ou corresponde à assinatura de uma exploração conhecida. Um IDS de rede (NIDS), como o Snort, vem configurado com regras para explorações conhecidas. Os alertas são gerados pelo Snort e são legíveis e pesquisáveis pelos aplicativos Sguil e Squert, que fazem parte do conjunto Security Onion de ferramentas NSM.

Um site de teste que é usado para determinar se o Snort está funcionando é o site tesmyids. Procure por ele na internet. Consiste em uma única página da Web que exibe apenas o seguinte texto **uid=0(root) gid=0(root) groups=0(root)**. Se o Snort estiver funcionando corretamente e um host visitar este site, uma assinatura será correspondida e um alerta será acionado. Esta é uma maneira fácil e inofensiva de verificar se o NIDS está em execução.

A regra Snort que é acionada é:

Esta regra gera um alerta se **qualquer endereço IP** na rede receber dados de uma fonte externa que contenha conteúdo com texto correspondente ao padrão de **uid=0 (root)**. O alerta contém a mensagem **GPL ATTACK\_RESPONSE id check retornou root**. O ID da regra Snort que foi acionada é **2100498**.

A linha destacada na figura exibe um alerta Sguil que foi gerado visitando o site testmyids. A regra Snort e os dados do pacote para o conteúdo recebido da página da Web testmyvids são exibidos na área inferior direita da interface Sguil.

10.1.2 Dados de Sessão e Transação

1. **ts**: carimbo de data e hora
2. **uid**: ID de sessão única
3. **id.orig\_h**: Endereço IP do host que originou a sessão (endereço de origem)
4. **id.orig\_p**: porta de protocolo para o host de origem (porta de origem)
5. **id.resp\_h**: Endereço IP do host que responde ao host de origem (endereço de destino)
6. **id.resp\_p**: protocolo de host respondente (porta de destino)
7. **proto**: protocolo de camada de transporte para sessão
8. **service**: protocolo de camada de aplicativo
9. **duration**: duração da sessão
10. **orig\_bytes**: bytes do host de origem
11. **resp\_bytes**: bytes do host respondente
12. **orig\_packets**: pacotes do host de origem
13. **resp\_packets**:pacotes do host respondente

Os dados de sessão são um registro de uma conversa entre dois pontos de extremidade de rede, que geralmente são um cliente e um servidor. O servidor pode estar dentro da rede corporativa ou em um local acessado pela Internet. Dados de sessão são dados sobre a sessão, não os dados recuperados e usados pelo cliente. Os dados da sessão incluirão informações de identificação, como **as cinco tuplas** de endereços IP de origem e destino, números de porta de origem e destino, e o código IP do protocolo em uso. Os dados sobre a sessão geralmente incluem um ID de sessão, a quantidade de dados transferidos por origem e destino e informações relacionadas à duração da sessão.

Zeek, anteriormente Bro, é uma ferramenta de monitoramento de segurança de rede que você usará

Os dados de transação consistem nas mensagens que são trocadas durante sessões de rede. Essas transações podem ser exibidas em transcrições de captura de pacotes. Os logs de dispositivos mantidos por servidores também contêm informações sobre as transações que ocorrem entre clientes e servidores. Por exemplo, uma sessão pode incluir o download de conteúdo de um servidor web, como mostrado na figura. As transações que representam as solicitações e respostas seriam registradas em um log de acesso no servidor ou por um NIDS como Zeek. A sessão é todo o tráfego envolvido na elaboração da solicitação, a transação é a própria solicitação.

10.1.3 Capturas completas de pacotes

Capturas completas de pacotes são os dados de rede mais detalhados que geralmente são coletados. Devido à quantidade de detalhes, eles também são os tipos de dados mais intensos de armazenamento e recuperação usados no NSM. As capturas completas de pacotes contêm não apenas dados sobre conversas de rede, como dados de sessão. As capturas completas de pacotes também contêm o conteúdo real das conversas. As capturas completas de pacotes contêm o texto das mensagens de email, o HTML nas páginas da Web e os arquivos que entram ou saem da rede. O conteúdo extraído pode ser recuperado de capturas completas de pacotes e analisado quanto a malware ou comportamento do usuário que viola as políticas de negócios e de segurança. A ferramenta familiar Wireshark é muito popular para visualizar capturas de pacotes completos e acessar os dados associados a conversas de rede.

10.1.4 Dados Estatísticos

Como dados de sessão, dados estatísticos são sobre tráfego de rede. Os dados estatísticos são criados através da análise de outras formas de dados de rede. Podem ser feitas conclusões que descrevem ou predizem o comportamento da rede a partir dessas análises. As características estatísticas do comportamento normal da rede podem ser comparadas ao tráfego de rede atual em um esforço para detectar anomalias. As estatísticas podem ser usadas para caracterizar quantidades normais de variação nos padrões de tráfego de rede, a fim de identificar condições de rede que estão significativamente fora desses intervalos. Diferenças estatisticamente significativas devem gerar alarmes e investigação imediata.

A NBA (Network Behavior Analysis) e a Network Behavior Anomaly Detection (NBAD) são abordagens para monitoramento de segurança de rede que usam técnicas analíticas avançadas para analisar dados de telemetria de rede NetFlow ou IPFIX (Internet Protocol Flow Information Export). Técnicas como análise preditiva e inteligência artificial realizam análises avançadas de dados de sessão detalhados para detectar possíveis incidentes de segurança.

**Observação**: IPFIX é a versão padrão IETF do Cisco NetFlow versão 9.

Um exemplo de uma ferramenta NSM que utiliza análise estatística é o Cisco Cognitive Threat Analytics. Ele é capaz de encontrar atividades mal-intencionadas que ignorou os controles de segurança ou entrou na rede por meio de canais não monitorados (incluindo mídia removível) e está operando dentro do ambiente de uma organização.

10.2.1 Logs de hosts

Conforme discutido anteriormente, os sistemas de detecção de intrusão baseados em host (HIDS) são executados em hosts individuais. HIDS não só detecta intrusões, mas na forma de firewalls baseados em host, também pode impedir intrusões. Este software cria logs e os armazena no host. Isso pode dificultar a visão do que está acontecendo em hosts na empresa, pois muitas proteções baseadas em host têm uma maneira de enviar logs para servidores centralizados de gerenciamento de logs. Dessa forma, os logs podem ser pesquisados a partir de um local central usando as ferramentas NSM.

Os sistemas HIDS podem usar agentes para enviar logs para servidores de gerenciamento. O OSSEC, um HIDS de código aberto popular, inclui uma funcionalidade robusta de coleta e análise de logs.

Os logs de host do Microsoft Windows são visíveis localmente pelo Visualizador de Eventos. O Visualizador de Eventos mantém cinco tipos de logs:

* **Logs de aplicativos** — Eles contêm eventos registrados por vários aplicativos.
* **Registros do sistema** — Isso inclui eventos relacionados à operação de drivers, processos e hardware.
* **Registros de instalação** — Estes registram informações sobre a instalação de software, incluindo atualizações do Windows.
* **Registros de segurança** — Esses eventos registram relacionados à segurança, como tentativas de logon e operações relacionadas ao gerenciamento e acesso de arquivos ou objetos.
* **Logs da linha de comando** - Os invasores que obtiveram acesso a um sistema e alguns tipos de malware executam comandos da interface de linha de comando (CLI) em vez de uma GUI. A execução da linha de comando em log fornecerá visibilidade para esse tipo de incidente.

Vários logs podem ter diferentes tipos de eventos. Os logs de segurança consistem apenas em mensagens de falha ou êxito de auditoria. Em computadores Windows, o log de segurança é realizado pelo Local Security Authority Subsystem Service (LSASS), que também é responsável por impor diretivas de segurança em um host Windows. O LSASS é executado como lsass.exe. Ele é frequentemente falsificado por malware. Ele deve estar sendo executado a partir do diretório System32 do Windows. Se um arquivo com esse nome, ou um nome camuflado, como 1sass.exe, estiver em execução ou em execução a partir de outro diretório, ele pode ser malware.

Os Eventos do Windows são identificados por números de ID e descrições breves. Uma enciclopédia de IDs de eventos de segurança, algumas com detalhes adicionais, está disponível no Ultimate Windows Security na Web.

A tabela explica o significado dos cinco tipos de eventos de log de host do Windows.

|  |  |
| --- | --- |
| **Tipo de evento** | **Descrição** |
| Erro | Um erro é um evento que indica um problema significativo, como perda de dados ou perda de funcionalidade. Por exemplo, se um serviço falhar ao carregar durante a inicialização, um evento de erro será registrado. |
| Aviso | Um aviso é um evento que não é necessariamente significativo, mas pode indicar um possível problema futuro. Por exemplo, quando o espaço em disco é baixo, um evento de aviso é registrado. Se um aplicativo pode se recuperar de um evento sem perda de funcionalidade ou dados, ele geralmente pode classificar o evento como um evento de aviso. |
| Informações | Um evento informativo descreve a operação bem-sucedida de um aplicativo, driver ou serviço. Por exemplo, quando um driver de rede é carregado com êxito, pode ser apropriado registrar um evento de informações. Observe que geralmente é inapropriado para um aplicativo de área de trabalho registrar um evento cada vez que ele é iniciado. |
| Sucesso na Auditoria | Uma auditoria bem-sucedida é um evento que registra uma tentativa de acesso de segurança auditada com êxito. For example, a user's successful attempt to log on to the system is logged as a success audit event. |
| Falha ne Auditoria | Uma auditoria de falha é um evento que registra uma tentativa de acesso de segurança auditada que falha. Por exemplo, se um usuário tentar acessar uma unidade de rede e falhar, a tentativa é registrada como um evento de auditoria de falha. |

10.2.2 Syslog

O Syslog inclui especificações para formatos de mensagem, uma estrutura de aplicativos cliente-servidor e protocolo de rede. Muitos tipos diferentes de dispositivos de rede podem ser configurados para usar o padrão syslog para registrar eventos em servidores syslog centralizados.

Syslog é um protocolo cliente / servidor. O Syslog foi definido dentro do grupo de trabalho Syslog do IETF (RFC 5424) e é suportado por uma grande variedade de dispositivos e receptores em várias plataformas.

O remetente do Syslog envia uma pequena mensagem de texto (menos de 1 KB) para o receptor do Syslog. O receptor Syslog é comumente chamado de “syslogd”, “Syslog daemon” ou “Syslog server.“ As mensagens do Syslog podem ser enviadas via UDP (porta 514) e/ou TCP (normalmente, porta 5000). Embora existam algumas exceções, como wrappers SSL, esses dados são normalmente enviados em texto simples pela rede.

O formato completo de uma mensagem Syslog que é visto na rede tem três partes distintas, como mostrado na figura.

* PRI (prioridade)
* HEADER
* MSG (texto da mensagem)

O PRI consiste em dois elementos, a Facilidade e a Gravidade da mensagem, que são ambos valores inteiros. O recurso consiste em amplas categorias de fontes que geraram a mensagem, como o sistema, o processo ou a aplicação. O valor Facility pode ser usado por servidores de log para direcionar a mensagem para o arquivo de log apropriado. A gravidade é um valor de 0 a 7 que define a gravidade da mensagem.

**Formato de pacote do Syslog**

Instalação

**Nota**: Códigos de instalação entre 15 e 23 (local0-local7) não recebem uma palavra-chave ou nome. Eles podem ser atribuídos a diferentes significados dependendo do contexto de uso. Além disso, vários sistemas operacionais foram encontrados para utilizar ambas as instalações 9 e 15 para mensagens de relógio.

Severidade

|  |  |
| --- | --- |
| **Valor** | **Severidade** |
| 0 | **Emergência**: sistema está inutilizável |
| 1 | **Alerta**: a ação deve ser tomada imediatamente |
| 2 | **Crítico**: condições críticas que devem ser corrigidas imediatamente e indica falha em um sistema |
| 3 | **Erro**: uma falha que não é urgente, deve ser resolvida dentro de um determinado tempo |
| 4 | **Aviso**: um erro não existe atualmente; no entanto, um erro ocorrerá no futuro se a condição não for resolvida |
| 5 | **Aviso**: Qual ferramenta está incluída no Security Onion que é usada pelo Snort para baixar automaticamente novas regras? |
| 6 | **Informativo**: mensagens emitidas relativas ao funcionamento normal |
| 7 | **Depuração**: mensagens de interesse para desenvolvedores |

Prioridade

O valor de Prioridade (PRI) é calculado multiplicando o valor de Facilidade por 8 e, em seguida, adicionando-o ao valor de Gravidade, conforme mostrado abaixo.

**Prioridade = (Facilidade \* 8) + Severidade**

O valor Prioridade é o primeiro valor em um pacote e ocorre entre colchetes angulados **<>**.

A seção **HEADER** da mensagem contém o carimbo de data/hora no formato **MMM DD HH:MM:SS**. Se o carimbo de data/hora for precedido pelos símbolos de ponto (.) ou asterisco (\*), um problema é indicado com NTP. A seção HEADER também inclui o nome do host ou endereço IP do dispositivo que é a origem da mensagem.

A parte **MSG** contém o significado da mensagem syslog. Isso pode variar entre os fabricantes de dispositivos e pode ser personalizado. Portanto, essa parte da mensagem é a mais significativa e útil para o analista de segurança cibernética.

10.2.3 Logs do servidor

Os logs do servidor são uma fonte essencial de dados para o monitoramento da segurança da rede. Os servidores de aplicativos de rede, como servidores de e-mail e Web, mantêm registros de acesso e erros. Os logs do servidor proxy DNS que documentam todas as consultas DNS e respostas que ocorrem na rede são especialmente importantes. Os logs de proxy DNS são úteis para identificar hosts que possam ter visitado sites perigosos e para identificar a exfiltração de dados DNS e conexões a servidores de comando e controle de malware. Muitos servidores UNIX e Linux usam syslog. Outros podem usar o registro proprietário. O conteúdo dos eventos do arquivo de log depende do tipo de servidor.

10.2.4 SIEM e coleta de registros

A tecnologia SIEM (Security Information and Event Management, gerenciamento de eventos e informações de segurança) é usada em muitas organizações para fornecer relatórios em tempo real e análise de longo prazo de eventos de segurança, conforme mostrado na figura.

**Entradas e Saídas SIEM**

O SIEM combina as funções essenciais de gerenciamento de eventos de segurança (SEM) e ferramentas de gerenciamento de informações de segurança (SIM) para fornecer uma visão abrangente da rede empresarial usando as seguintes funções:

* **Coleta de logs** — Os registros de eventos de origens em toda a organização fornecem informações forenses importantes e ajudam a atender aos requisitos de relatórios de conformidade.
* **Normalização** — Mapeia mensagens de log de diferentes sistemas em um modelo de dados comum, permitindo que a organização se conecte e analise eventos relacionados, mesmo que sejam inicialmente registradas em diferentes formatos de origem.
* **Correlação** — Isso vincula registros e eventos de sistemas ou aplicativos diferentes, acelerando a detecção e reação a ameaças de segurança.
* **Agregação** — Isso reduz o volume de dados de eventos consolidando registros de eventos duplicados.
* **Relatórios** — Apresenta os dados de eventos agregados e correlacionados em monitoramento em tempo real e resumos de longo prazo, incluindo painéis gráficos interativos.
* **Conformidade** — são relatórios para atender aos requisitos de várias regulamentações de conformidade.

Um SIEM popular é o Splunk, que é feito por um parceiro Cisco. A figura mostra um Painel de Ameaças Splunk. Splunk é amplamente utilizado em SOCs. Outra solução SIEM popular é Security Onion com ELK, que consiste nos aplicativos integrados Elasticsearch, Logstash e Kibana. Security Onion inclui outras ferramentas de monitoramento de segurança de rede de código aberto.

Como sabemos, a orquestração, a automação e a resposta de segurança (SOAR) levam o SIEM e vão além para automatizar fluxos de trabalho de resposta de segurança e facilitar a resposta de incidência. Devido à importância da segurança de rede, inúmeras empresas trouxeram excelentes produtos para o mercado de ferramentas de segurança. No entanto, essas ferramentas não têm compatibilidade e exigem monitoramento de vários painéis de produtos independentes para processar os muitos alertas que eles geram. Devido à falta de profissionais de segurança cibernética para monitorar e analisar o grande volume de dados de segurança, é importante que as ferramentas de vários fornecedores possam ser integradas em uma única plataforma. As plataformas de segurança integradas vão além do SIEM e do SOAR para unificar várias tecnologias de segurança, processos e pessoas em uma equipe unificada cujos componentes se baseiam em vez de impedirem uns aos outros. Plataformas de segurança como Cisco SecureX, Fortinet Security Fabric e Paloalto Networks Cortex XDR prometem lidar com a complexidade do monitoramento de segurança de rede integrando várias funções e fontes de dados em uma única plataforma que aumentará consideravelmente a precisão dos alertas, oferecendo defesa robusta.

**10.3 Logs de rede**

**10.3.1 Tcpdump**

A ferramenta de linha de comando tcpdump é um analisador de pacotes muito popular. Ele pode exibir capturas de pacotes em tempo real ou gravar capturas de pacotes em um arquivo. Ele captura dados detalhados de protocolo de pacotes e conteúdo. Wireshark é uma GUI construída sobre a funcionalidade tcpdump.

A estrutura das capturas tcpdump varia dependendo do protocolo capturado e dos campos solicitados.

10.3.2 NetFlow

NetFlow é um protocolo desenvolvido pela Cisco como uma ferramenta para solução de problemas de rede e contabilidade baseada em sessão. O NetFlow fornece com eficiência um importante conjunto de serviços para aplicativos IP, incluindo contabilidade de tráfego de rede, faturamento de rede com base no uso, planejamento de rede, segurança, recursos de monitoramento de negação de serviço e monitoramento de rede. O NetFlow fornece informações valiosas sobre usuários e aplicativos de rede, tempos de uso de pico e roteamento de tráfego.

O NetFlow não faz uma captura completa de pacote ou captura o conteúdo real no pacote. O NetFlow registra informações sobre o fluxo de pacotes, incluindo metadados. A Cisco desenvolveu o NetFlow e, em seguida, permitiu que ele fosse usado como base para um padrão IETF chamado IPFIX. O IPFIX é baseado no Cisco NetFlow Versão 9.

As informações do NetFlow podem ser visualizadas com ferramentas como o nfdump. Semelhante ao tcpdump, o nfdump fornece um utilitário de linha de comando para visualizar dados NetFlow a partir do daemon de captura nfcapd ou coletor. Existem ferramentas que adicionam funcionalidade GUI à visualização de fluxos.

Tradicionalmente, um Fluxo de IP é baseado em um conjunto de 5 a 7 atributos de pacotes IP que fluem em uma única direção. Um fluxo consiste em todos os pacotes transmitidos até que a conversa TCP termine. Os atributos de pacote IP usados pelo NetFlow são:

* Endereço IP origem
* Endereço IP de destino
* Porta de origem
* Porta de destino
* Tipo de protocolo da camada 3
* Classe de Serviço
* Interface de roteador ou switch

Todos os pacotes com o mesmo endereço IP de origem/destino, portas de origem/destino, interface de protocolo e classe de serviço são agrupados em um fluxo e, em seguida, pacotes e bytes são contabilizados. Essa metodologia de impressão digital ou determinação de um fluxo é escalável porque uma grande quantidade de informações de rede é condensada em um banco de dados de informações do NetFlow chamado cache do NetFlow.

Todos os registros de fluxo NetFlow conterão os primeiros cinco itens na lista acima e carimbos de data/hora de início e fim do fluxo. As informações adicionais que podem aparecer são altamente variáveis e podem ser configuradas no dispositivo NetFlow Exporter. Os exportadores são dispositivos que podem ser configurados para criar registros de fluxo e transmitir esses registros de fluxo para armazenamento em um dispositivo coletor NetFlow.

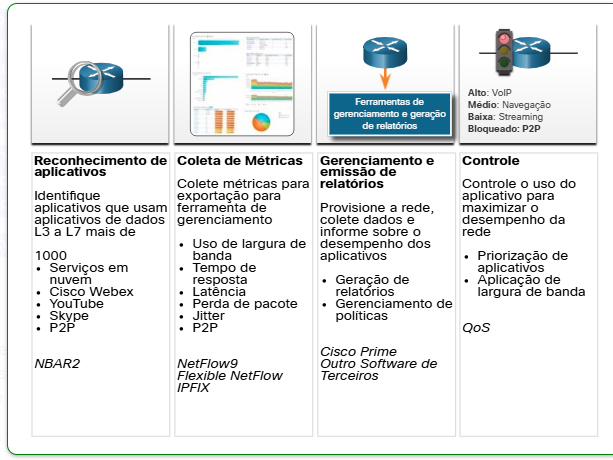
Embora o NetFlow não tenha sido inicialmente concebido como ferramenta para o monitoramento de segurança de rede, ele é visto como uma ferramenta útil na análise de incidentes de segurança de rede. Ele pode ser usado para construir uma linha do tempo de comprometimento, entender o comportamento individual do host ou para rastrear a movimentação de um invasor ou explorar de host para host dentro de uma rede. A tecnologia Cisco/Lancope Stealthwatch melhora o uso de dados NetFlow para NSM.

10.3.3 Visibilidade e controle da aplicação

O sistema Cisco Application Visibility and Control (AVC), que é mostrado na figura, combina várias tecnologias para reconhecer, analisar e controlar mais de 1000 aplicativos. Estes incluem voz e vídeo, e-mail, compartilhamento de arquivos, jogos, ponto a ponto (P2P) e aplicativos baseados em nuvem. A AVC usa o reconhecimento de aplicativos baseados em rede de última geração da Cisco versão 2 (NBAR2), também conhecido como NBAR de próxima geração, para descobrir e classificar os aplicativos em uso na rede. O mecanismo de reconhecimento de aplicativos NBAR2 suporta mais de 1000 aplicativos de rede.

Para entender verdadeiramente a importância desta tecnologia, considere a figura. A identificação de aplicativos de rede por porta fornece pouca granularidade e visibilidade do comportamento do usuário. No entanto, a visibilidade do aplicativo através da identificação de assinaturas de aplicativos identifica o que os usuários estão fazendo, seja teleconferência ou download de filmes para seus telefones.

**Cisco Application Visibility and Control**



Um sistema de gerenciamento e geração de relatórios, como o Cisco Prime, analisa e apresenta os dados de análise de aplicativos em relatórios de painel para uso pelo pessoal de monitoramento de rede. O uso de aplicativos também pode ser controlado por meio de políticas e classificação de qualidade de serviço com base nas informações do AVC.

10.3.4 Logs de filtro de conteúdo

Os dispositivos que fornecem filtragem de conteúdo, como o Cisco Email Security Appliance (ESA) e o Cisco Web Security Appliance (WSA), fornecem uma ampla gama de funcionalidades para monitoramento de segurança. O log está disponível para muitas dessas funcionalidades.

O ESA, por exemplo, tem mais de 30 logs que podem ser usados para monitorar a maioria dos aspectos da entrega de e-mail, funcionamento do sistema, antivírus, operações antispam e decisões de lista negra e lista branca. A maioria dos logs são armazenados em arquivos de texto e podem ser coletados em servidores syslog, ou podem ser enviados para servidores FTP ou SCP. Além disso, os alertas sobre o funcionamento do próprio equipamento e seus subsistemas podem ser monitorados por e-mail para administradores responsáveis pelo monitoramento e operação do dispositivo.

Os dispositivos WSA oferecem uma profundidade de funcionamento semelhante. O WSA atua efetivamente como um proxy da Web, o que significa que ele registra todas as informações de transação de entrada e saída para tráfego HTTP. Esses logs podem ser bastante detalhados e são personalizáveis. Eles podem ser configurados em um formato de compatibilidade W3C. O WSA pode ser configurado para enviar os logs para um servidor de várias maneiras, incluindo syslog, FTP e SCP.

Outros logs disponíveis para o WSA incluem logs de decisão da ACL, logs de varredura de malware e logs de filtragem de reputação da Web.

10.3.5 Logando de Dispositivos Cisco

Os dispositivos de segurança Cisco podem ser configurados para enviar eventos e alertas para plataformas de gerenciamento de segurança usando SNMP ou syslog. A figura ilustra uma mensagem syslog gerada por um dispositivo Cisco ASA e uma mensagem syslog gerada por um dispositivo Cisco IOS.

Observe que há dois significados usados para o recurso termo nas mensagens do syslog da Cisco. O primeiro é o conjunto padrão de valores de Facilidade que foram estabelecidos pelos padrões syslog. Esses valores são usados na parte da mensagem PRI do pacote syslog para calcular a prioridade da mensagem. A Cisco usa alguns dos valores entre 15 e 23 para identificar as Instalações de log da Cisco, dependendo da plataforma. Por exemplo, os dispositivos Cisco ASA usam syslog Facility 20 por padrão, o que corresponde a local4. O outro valor Facility é atribuído pela Cisco e ocorre na parte MSG da mensagem syslog.

Os dispositivos Cisco podem usar formatos de mensagem syslog ligeiramente diferentes e podem usar mnemônicos em vez de IDs de mensagem, conforme mostrado na figura. Um dicionário de mensagens de syslog do Cisco ASA está disponível no site da Cisco.

10.3.6 Registros de Proxy

Os servidores proxy, como os usados para solicitações Web e DNS, contêm logs valiosos que são uma fonte primária de dados para monitoramento de segurança de rede.

Servidores proxy são dispositivos que atuam como intermediários para clientes de rede. Por exemplo, uma empresa pode configurar um proxy da Web para lidar com solicitações da Web em nome de clientes. Em vez de solicitações de recursos da Web serem enviadas diretamente para o servidor do cliente, a solicitação é enviada primeiro para um servidor proxy. O servidor proxy solicita os recursos e os retorna ao cliente. O servidor proxy gera logs de todas as solicitações e respostas. Esses logs podem ser analisados para determinar quais hosts estão fazendo as solicitações, se os destinos são seguros ou potencialmente maliciosos, e também para obter insights sobre o tipo de recursos que foram baixados.

Proxies da Web fornecem dados que ajudam a determinar se as respostas da Web foram geradas em resposta a solicitações legítimas ou foram manipuladas para parecer respostas, mas são, de fato, explorações. Também é possível usar proxies da web para inspecionar o tráfego de saída como meio de prevenção de perda de dados (DLP). O DLP envolve a varredura do tráfego de saída para detectar se os dados que estão saindo da Web contêm informações confidenciais, confidenciais ou secretas. Exemplos de proxies populares da Web são Squid, CCProxy, Apache Traffic Server e WinGate.

Um exemplo de um log de proxy da web do Squid na forma nativa do Squid aparece abaixo. Explicações dos valores de campo aparecem na tabela abaixo da entrada de log.

**Exemplo de log de proxy DNS**

|  |  |
| --- | --- |
| **Valor de log de proxy** | **Explicação** |
| 1265939281.764 | **Tempo**- Timestamp em milliseconds no formato Unix epoch |
| 19478 | **Duração**- o tempo decorrido para a solicitação e resposta do Squid |
| 172.16.167.228 | **cliente** Endereço IP do |
| TCP\_MISS/200 | **Resultado**- Códigos de resultado do Squid e código de status HTTP separados por uma barra |
| 864 | **Tamanho** - os bytes de dados entregues |
| GET | **Solicitação** - solicitação HTTP feita pelo client |
| http://www.example.com//images/home.png | **URI/URL** - endereço do recurso que foi solicitado |
| - | **Identidade do cliente** - valor RFC 1413 para o cliente que fez a solicitação. Não usado por padrão. |
| NONE/- | **Código de peering/Host de peer** - Consulta ao servidor de cache vizinho |
| image/png | **Tipo** - tipo de conteúdo MIME do valor Content-Type no cabeçalho de resposta HTTP |

**Observação**: Proxies da Web abertos, que são proxies que estão disponíveis para qualquer usuário da Internet, podem ser usados para ofuscar endereços IP de atores de ameaças. Endereços de proxy abertos podem ser usados na lista negra do tráfego da Internet.

**Cisco Umbrella**

O Cisco Umbrella, anteriormente OpenDNS, oferece um serviço DNS hospedado que amplia a capacidade do DNS para incluir aprimoramentos de segurança. Em vez de organizações que hospedam e mantêm listas negras, proteção contra phishing e outras seguranças relacionadas a DNS, o Cisco Umbrella fornece essas proteções em seu próprio serviço DNS. O Cisco Umbrella é capaz de aplicar muito mais recursos ao gerenciamento de DNS do que a maioria das organizações pode pagar. O Cisco Umbrella funciona em parte como um super proxy DNS nesse sentido. O pacote Cisco Umbrella de produtos de segurança aplica inteligência contra ameaças em tempo real para gerenciar o acesso DNS e a segurança dos registros DNS. Os logs de acesso DNS estão disponíveis no Cisco Umbrella para a empresa assinada. Em vez de usar servidores DNS locais ou ISP, uma organização pode optar por assinar o Cisco Umbrella para DNS e outros serviços de segurança. Um exemplo de um log de proxy DNS aparece abaixo. A tabela explica o significado dos campos na entrada de log.

**Exemplo de log de proxy DNS**

|  |  |  |
| --- | --- | --- |
| **Campo** | **Exemplo** | **Explicação** |
| Timestamp | 2015-01-16 17:48:41 | Isso ocorre quando essa solicitação foi feita em UTC. Isso é diferente do painel Umbrella, que converte a hora para o fuso horário especificado. |
| Policy Identity | ActiveDirectoryUserName | A primeira identidade que correspondeu à solicitação. |
| Identities | ActiveDirectoryUserName,ADSite,Network | Todas as identidades associadas a esta solicitação. |
| Internal Ip | 10.10.1.100 | O endereço IP interno que fez a solicitação. |
| External Ip | 24.123.132.133 | O endereço IP externo que fez a solicitação. |
| Action | Allowed | Se a solicitação foi permitida ou bloqueada. |
| QueryType | 1 (A) | O tipo de solicitação DNS que foi feita. |
| ResponseCode | NOERROR | O código de retorno DNS para esta solicitação. |
| Domain | domain-visited.com. | Este é o domínio que foi solicitado. |
| Categories | Chat,Photo Sharing,Social Networking | As categorias de segurança ou conteúdo correspondentes ao destino. |

10.3.7 Firewalls de Última Geração

Os dispositivos de firewall da próxima geração ou NextGen estendem a segurança da rede além dos endereços IP e dos números de porta da Camada 4 para a camada do aplicativo e além. Os Firewalls NexGen são dispositivos avançados que forneceram muito mais funcionalidades do que as gerações anteriores de dispositivos de segurança de rede. Uma dessas funcionalidades é relatar painéis com recursos interativos que permitem relatórios rápidos de apontar e clicar sobre informações muito específicas sem a necessidade de SIEM ou outros correladores de eventos.

A linha de dispositivos NextGen Firewall (NGFW) da Cisco usa o Firepower Services para consolidar várias camadas de segurança em uma única plataforma. Isso ajuda a conter custos e simplificar o gerenciamento. Os serviços da potência de fogo incluem visibilidade e controle de aplicativos, IPS de última geração da potência de fogo (NGIPS), filtragem de URL baseada em categoria e reputação e proteção avançada contra malware (AMP). Dispositivos Firepower permitem monitorar a segurança da rede por meio de uma GUI habilitada para Web chamada Visualizador de Eventos.

Eventos comuns do NGFW incluem:

* **Evento de Conexão** - Os logs de conexão contêm dados sobre sessões que são detectadas diretamente pelo NGIPS. Os eventos de conexão incluem propriedades básicas de conexão, como carimbos de data/hora, endereços IP de origem e destino, e metadados sobre por que a conexão foi registrada, como qual regra de controle de acesso registrou o evento.
* **Evento de intrusão** - O sistema examina os pacotes que atravessam a rede em busca de atividades mal-intencionadas que possam afetar a disponibilidade, integridade e confidencialidade de um host e seus dados. Quando o sistema identifica uma possível intrusão, ele gera um evento de intrusão, que é um registro da data, hora, tipo de exploração e informações contextuais sobre a origem do ataque e seu destino.
* **Host ou evento de ponto final** - Quando um host aparece na rede, ele pode ser detectado pelo sistema e os detalhes do hardware do dispositivo, endereçamento IP e a última presença conhecida na rede podem ser registrados.
* **Evento de descoberta de rede** - eventos de descoberta de rede representam alterações que foram detectadas na rede monitorada. Essas alterações são registradas em resposta às diretivas de descoberta de rede que especificam os tipos de dados a serem coletados, os segmentos de rede a serem monitorados e as interfaces de hardware do dispositivo que devem ser usadas para coleta de eventos.
* **Evento de fluxo de** rede - A descoberta de rede pode usar vários mecanismos, um dos quais é usar registros de fluxo NetFlow exportados para gerar novos eventos para hosts e servidores.

11.1.1 Cebola Segurança

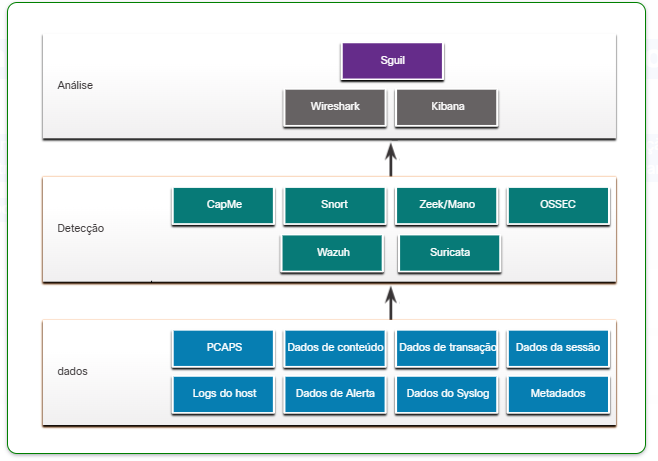
O Cebola Segurança é um pacote de código aberto de ferramentas de Monitoramento de Segurança de Rede (NSM) que é executado em uma distribuição Ubuntu Linux. As ferramentas Cebola Segurança fornecem três funções principais para o analista de segurança cibernética: captura completa de pacotes e tipos de dados, sistemas de detecção de intrusão baseados em rede e em host e ferramentas de analistas de alerta. Cebola Segurança pode ser instalado como uma instalação autônoma ou como um sensor e plataforma de servidor. Alguns componentes do Cebola Segurança são de propriedade e mantidos por corporações, como Cisco e Riverbend Technologies, mas são disponibilizados como código aberto.

**Observação:** em alguns recursos, você pode ver Cebola Segurança abreviado como SO. Neste curso, usaremos Cebola Segurança.

11.1.2 Ferramentas de detecção para coleta de dados de alerta

Cebola Segurança contém muitos componentes. É um ambiente integrado projetado para simplificar a implantação de uma solução NSM abrangente. A figura ilustra uma visão simplificada da maneira como alguns dos componentes do Cebola Segurança trabalham juntos.

**Uma arquitetura do Cebola Segurança**



CapMe

Esta é uma aplicação web que permite a visualização de transcrições pcap renderizadas com as ferramentas tcpflow ou Zeek. O CapMe pode ser acessado a partir da ferramenta ELSA (Enterprise Log Search and Archive). O CapMe oferece ao analista de segurança cibernética um meio fácil de ler para visualizar uma sessão inteira da Camada 4. O CapMe atua como um plugin para o ELSA e fornece acesso a arquivos pcap relevantes que podem ser abertos no Wireshark.

Snort

Este é um Sistema de Detecção de Intrusão de Rede (NIDS). É uma importante fonte de dados de alerta indexados na ferramenta de análise Sguil. O Snort usa regras e assinaturas para gerar alertas. O Snort pode baixar automaticamente novas regras usando o componente PulledPork do Cebola Segurança. Snort e PulledPork são ferramentas de código aberto que são patrocinadas pela Cisco.

O Zeek

Anteriormente conhecido como Bro. Este é um NIDS que usa mais uma abordagem baseada em comportamento para detecção de intrusões. Em vez de usar assinaturas ou regras, o Zeek usa políticas, na forma de scripts que determinam quais dados registrar e quando emitir notificações de alerta. O Zeek também pode enviar anexos de arquivos para análise de malware, bloquear o acesso a locais mal-intencionados e desligar um computador que parece estar violando políticas de segurança.

**Observação:** Algumas interfaces dentro do Cebola Segurança ainda não foram atualizadas com a alteração de nome de Bro para Zeek.

OSSEC

Este é um sistema de detecção de intrusão baseado em host (HIDS) integrado ao Cebola Segurança. Ele monitora ativamente as operações do sistema host, incluindo a realização de monitoramento de integridade de arquivos, monitoramento de log local, monitoramento de processos do sistema e detecção de rootkit. Alertas OSSEC e dados de log estão disponíveis para Sguil e Kibana. O OSSEC requer que um agente seja executado nos computadores Windows da empresa.

Wazuh

Wazuh é um HIDS que substituirá OSSEC em Cebola Segurança. É uma solução completa que fornece um amplo espectro de mecanismos de proteção de terminais, incluindo análise de arquivos de log do host, monitoramento de integridade de arquivos, detecção de vulnerabilidades, avaliação de configuração e resposta a incidentes. Assim como o OSSEC, ele exige que os agentes estejam sendo executados em hosts de rede.

Suricata

Este é um NIDS que usa uma abordagem baseada em assinaturas. Ele também pode ser usado para prevenção de intrusões em linha. É semelhante ao Zeek; no entanto, o Suricata usa multithreading nativo, que permite a distribuição do processamento de fluxo de pacotes em vários núcleos de processadores. Ele também inclui alguns recursos adicionais, como bloqueio baseado em reputação e suporte para multithreading de unidade de processamento gráfico (GPU) para melhorar o desempenho.

11.1.3 Ferramentas de Análise

O Cebola Segurança integra esses vários tipos de dados e logs do Sistema de Detecção de Intrusões (IDS) em uma única plataforma através das seguintes ferramentas:

* **Sguil** - Isso fornece um console de alto nível para investigar alertas de segurança de uma ampla variedade de fontes. Sguil serve como ponto de partida na investigação de alertas de segurança. Uma grande variedade de fontes de dados está disponível para o analista de segurança cibernética, girando diretamente do Sguil para outras ferramentas.
* **Kibana** - É uma interface de painel interativo para dados Elasticsearch. Ele permite a consulta de dados do NSM e fornece visualizações flexíveis desses dados. Ele fornece recursos de análise de dados de exploração de dados e aprendizado de máquina. É possível girar do Sguil diretamente para o Kibana para ver exibições contextualizadas com base nos endereços IP de origem e destino associados a um alerta. Pesquise na internet e visite o site elastic.co para saber mais sobre os muitos recursos do Kibana.
* **Wireshark** - Este é um aplicativo de captura de pacotes integrado ao conjunto Cebola Segurança. Ele pode ser aberto diretamente de outras ferramentas e exibirá capturas completas de pacotes relevantes para uma análise.
* **Zeek** - Este é um analisador de tráfego de rede que serve como um monitor de segurança. O Zeek inspeciona todo o tráfego em um segmento de rede e permite uma análise aprofundada desses dados. A rotação do Sguil para o Zeek fornece acesso a logs de transações muito precisos, conteúdo de arquivos e saída personalizada.

11.1.4 Geração de alertas

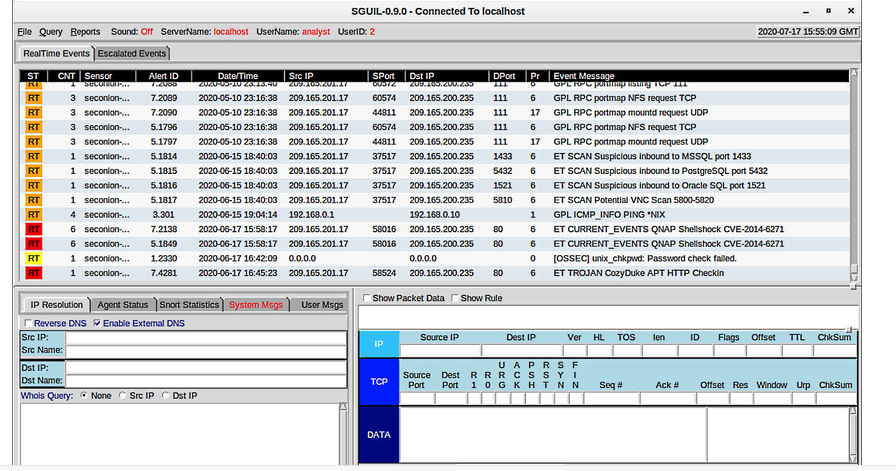
Alertas de segurança são mensagens de notificação geradas por ferramentas, sistemas e dispositivos de segurança do NSM. Os alertas podem vir em várias formas, dependendo da fonte. Por exemplo, o syslog fornece suporte para classificações de gravidade que podem ser usadas para alertar analistas de segurança cibernética sobre eventos que exigem atenção.

No Cebola Segurança, o Sguil fornece um console que integra alertas de várias fontes em uma fila com carimbo de data/hora. Um analista de segurança cibernética pode trabalhar na fila de segurança investigando, classificando, escalonando ou retirando alertas. Em vez de usar um sistema de gerenciamento de fluxo de trabalho dedicado, como o RTIR (Request Tracker for Incident Response), um analista de segurança cibernética usaria a saída de um aplicativo como o Sguil para orquestrar uma investigação do NSM.

Os alertas geralmente incluem informações de cinco tuplas quando disponíveis, bem como carimbos de data/hora e informações que identificam qual dispositivo ou sistema gerou o alerta. Lembre-se de que as cinco tuplas incluem as seguintes informações para rastrear uma conversa entre um aplicativo de origem e destino:

* **SRCIP** - o endereço IP de origem para o evento.
* **SPORt** - a porta de Camada 4 de origem (local) para o evento.
* **DSTip** - o IP de destino para o evento.
* **DPort** - a porta de Camada 4 de destino para o evento.
* **Pr**- o número do protocolo IP para o evento.

Informações adicionais podem ser se uma decisão de permissão ou negação foi aplicada ao tráfego, alguns dados capturados da carga útil do pacote ou um valor de hash para um arquivo baixado ou qualquer um dos vários dados.



Os campos disponíveis para os eventos em tempo real são os seguintes:

* **ST** - Este é o status do evento. RT significa tempo real. O evento é codificado por cor por prioridade. As prioridades são baseadas na categoria do alerta. Há quatro níveis de prioridade: muito baixo, baixo, médio e alto. As cores variam de amarelo claro a vermelho à medida que a prioridade aumenta.
* **CNT** - Esta é a contagem do número de vezes que este evento foi detectado para o mesmo endereço IP de origem e destino. O sistema determinou que este conjunto de eventos está correlacionado. Em vez de relatar cada um em uma série potencialmente longa de eventos correlacionados nesta janela, o evento é listado uma vez com o número de vezes que foi detectado nesta coluna. Números altos aqui podem representar um problema de segurança ou a necessidade de ajuste das assinaturas de eventos para limitar o número de eventos potencialmente falsos que estão sendo relatados.
* **Sensor** - Este é o agente que relata o evento. Os sensores disponíveis e seus números de identificação podem ser encontrados na guia Status do agente do painel, que aparece abaixo da janela de eventos à esquerda. Esses números também são usados na coluna ID de alerta. No painel Status do Agente, podemos ver que os sensores OSSEC, pcap e Snort estão reportando ao Sguil. Além disso, podemos ver os nomes de host padrão para esses sensores, que inclui a interface de monitoramento. Observe que cada interface de monitoramento tem dados pcap e Snort associados a ele.
* **Alert ID** - Este número de duas partes representa o sensor que relatou o problema e o número de evento desse sensor. Podemos ver a partir da figura que o maior número de eventos que são exibidos são do sensor OSSEC (1). O sensor OSSEC relatou oito conjuntos de eventos correlacionados. Destes eventos, 232 foram relatados com ID de evento 1.24.
* **Date/Time** - Este é o carimbo de data/hora do evento. No caso de eventos correlacionados, é o carimbo de data/hora do primeiro evento.
* **Event Message** - Este é o texto de identificação para o evento. Isso é configurado na regra que disparou o alerta. A regra associada pode ser visualizada no painel direito, logo acima dos dados do pacote. Para exibir a regra, a caixa de seleção **Show Rule** deve estar marcada.

Dependendo da tecnologia de segurança, os alertas podem ser gerados com base em regras, assinaturas, anomalias ou comportamentos. Não importa como eles são gerados, as condições que acionam um alerta devem ser predefinidas de alguma maneira.

Os alertas podem vir de várias fontes:

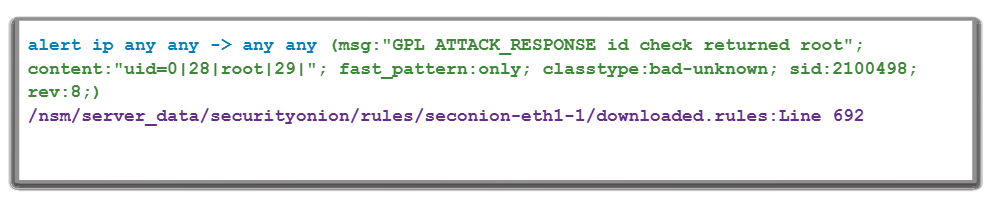
* **NIDS** - Snort, Zeek e Suricata
* **HIDS** - OSSEC, Wazuh
* **Gerenciamento e monitoramento de ativos** - Sistema de detecção de ativos passivos (PADS)
* **Transações HTTP, DNS e TCP** - Registradas pelo Zeek e pcaps
* **Mensagens do Syslog** - Várias fontes

As informações encontradas nos alertas que são exibidos no Sguil serão diferentes no formato de mensagem porque elas vêm de fontes diferentes.

O alerta Sguil na figura foi acionado por uma regra que foi configurada no Snort. É importante que o analista de segurança cibernética seja capaz de interpretar o que acionou o alerta para que o alerta possa ser investigado. Por esse motivo, o analista de segurança cibernética deve entender os componentes das regras do Snort, que são uma das principais fontes de alertas em Cebola Segurança.

11.1.6 Estrutura de Regra Snort

As regras de Snort consistem em duas seções, como mostrado na figura: o cabeçalho da regra e as opções da regra. O cabeçalho da regra contém a ação, o protocolo, os endereços IP de origem e destino e as máscaras de rede e as informações da porta de origem e destino. A seção Opções de regra contém mensagens de alerta e informações sobre quais partes do pacote devem ser inspecionadas para determinar se a ação da regra deve ser executada. A localização da regra às vezes é adicionada pelo Sguil. Local da Regra é o caminho para o arquivo que contém a regra e o número da linha em que a regra aparece para que ela possa ser encontrada e modificada, ou eliminada, se necessário.



**Estrutura da regra Snort e informações fornecidas pelo SGUI**

|  |  |  |
| --- | --- | --- |
| **Componente** | **Exemplo (abreviado...)** | **Explicação** |
| cabeçalho da regra | alert ip any any -> any any | Contém a ação a ser tomada, endereços e porta de origem e destino e a direção do fluxo de tráfego |
| opções de regra | (msg:”GPL ATTACK\_RESPONSE ID CHECK RETURNED ROOT”;…) | Inclui a mensagem a ser exibida, detalhes do conteúdo do pacote, tipo de alerta, ID de origem e detalhes adicionais, como uma referência para a regra ou vulnerabilidade |
| local da regra | /nsm/server\_data/securityonion/rules/… | Adicionado pelo Sguil para indicar a localização da regra na estrutura do arquivo Cebola Segurança e no arquivo de regra especificado |

**O cabeçalho da regra**

O cabeçalho da regra contém a ação, o protocolo, o endereçamento e as informações da porta, conforme mostrado na figura. Além disso, a direção do fluxo que acionou o alerta é indicada. A estrutura da parte do cabeçalho é consistente entre as regras de alerta Snort.

O Snort pode ser configurado para usar variáveis para representar endereços IP internos e externos. Essas variáveis, **$HOME\_NET** e **$EXTERNAL\_NET**, aparecem nas regras Snort. Eles simplificam a criação de regras, eliminando a necessidade de especificar endereços e máscaras específicos para cada regra. Os valores dessas variáveis são configurados no arquivo **snort.conf**. O Snort também permite que endereços IP individuais, blocos de endereços ou listas de ambos sejam especificados em regras. Os intervalos de portas podem ser especificados separando os valores superior e inferior do intervalo com dois pontos. Outros operadores também estão disponíveis.

**Estrutura do cabeçalho da regra Snort**

|  |  |
| --- | --- |
| **Componente** | **Explicação** |
| alerta | a ação a ser tomada é emitir um alerta, outras ações são registradas e passadas |
| ip | o protocolo |
| any any | a fonte especificada é qualquer endereço IP e qualquer porta da Camada 4 |
| -> | a direção do fluxo é da origem para o destino |
| any any | o destino especificado é qualquer endereço IP e qualquer porta da Camada 4 |

**As Opções de Regra**

A estrutura da seção de opções da regra é variável. É a parte da regra que está entre parênteses, como mostrado na figura. Ele contém a mensagem de texto que identifica o alerta. Ele também contém metadados sobre o alerta, como um URL que fornece informações de referência para o alerta. Outras informações podem ser incluídas, como o tipo de regra e um identificador numérico exclusivo para a regra e a revisão da regra. Além disso, os recursos da carga do pacote podem ser especificados nas opções. O manual de usuários do Snort, que pode ser encontrado na internet, fornece detalhes sobre regras e como criá-las.

Mensagens de regra de snifar podem incluir a origem da regra. Três fontes comuns para as regras do Snort são:

* **GPL** - Regras mais antigas do Snort que foram criadas pelo Sourcefire e distribuídas sob uma GPLv2. O conjunto de regras GPL não é certificado pelo Cisco Talos. Inclui Snort SIDs 3464 e abaixo. O conjunto de regras GPL pode ser baixado do site do Snort e está incluído no Cebola Segurança.
* **ET**- Regras Snort de ameaças emergentes. Emerging Threats é um ponto de coleta para regras Snort de várias fontes. As regras ET são de código aberto sob uma licença BSD. O conjunto de regras ET contém regras de várias categorias. Um conjunto de regras ET está incluído com Cebola Segurança. Emerging Threats é uma divisão da Proofpoint, Inc.
* **VRT**- Essas regras estão imediatamente disponíveis para assinantes e são liberadas para usuários registrados 30 dias após sua criação, com algumas limitações. Eles agora são criados e mantidos pelo Cisco Talos.

As regras podem ser baixadas automaticamente do Snort.org usando o utilitário de gerenciamento de regras PulledPork que está incluído com o Cebola Segurança.

Alertas que não são gerados pelas regras do Snort são identificados pelas tags OSSEC ou PADS, entre outras. Além disso, regras locais personalizadas podem ser criadas.

**Estrutura de Opções de Regras Snort**

A figura mostra o texto em fonte normal:

|  |  |
| --- | --- |
| **Componente** | **Explicação** |
| msg: | Texto que descreve o alerta. |
| content: | Refere-se ao conteúdo do pacote. Neste caso, um alerta será enviado se o texto literal "uid=O(root)" aparecer em qualquer lugar nos dados do pacote. Valores especificando a localização do texto na carga de dados podem ser fornecidos. |
| reference: | Isso não é mostrado na figura. Muitas vezes, é um link para uma URL que fornece mais informações sobre a regra. Nesse caso, o sid é hipervinculado à origem da regra na Internet. |
| classtype: | Uma categoria para o ataque. O Snort inclui um conjunto de categorias padrão que têm um dos quatro valores de prioridade. |
| sid: | Um identificador numérico exclusivo para a regra. |
| rev: | A revisão da regra que é representada pelo sid. |

**11.2.1 A necessidade de avaliação de alertas**

**Ferramentas primárias para o analista de segurança cibernética de nível 1**

Os analistas de segurança cibernética de nível 1 costumam trabalhar em filas de alertas em uma ferramenta como Sguil, girando para ferramentas como Zeek, Wireshark e Kibana para verificar se um alerta representa uma exploração real.

11.2.2 Avaliando Alertas

Os incidentes de segurança são classificados usando um esquema emprestado de diagnósticos médicos. Este esquema de classificação é usado para orientar ações e avaliar procedimentos de diagnóstico. Por exemplo, quando um paciente visita um médico para um exame de rotina, uma das tarefas do médico é determinar se o paciente está doente. Um dos resultados pode ser uma determinação correta de que a doença está presente e o paciente está doente. Outro resultado pode ser que não há doença e o paciente é saudável.

A preocupação é que o diagnóstico pode ser preciso, ou verdadeiro, ou impreciso, ou falso. Por exemplo, o médico pode perder os sinais de doença e fazer a determinação incorreta de que o paciente está bem quando está de fato doente. Outro erro possível é decidir que um paciente está doente quando esse paciente é de fato saudável. Os falsos diagnósticos são caros ou perigosos.

* **Verdadeiro positivo**: o alerta foi verificado como um incidente de segurança real.
* **Falso Positivo**: O alerta não indica um incidente de segurança real. A atividade benigna que resulta em um falso positivo é às vezes referida como um gatilho benigno.

Uma situação alternativa é que um alerta não foi gerado. A ausência de um alerta pode ser classificada como:

* **Verdadeiro negativo**: Nenhum incidente de segurança ocorreu. A atividade é benigna.
* **Falso Negativo**: Ocorreu um incidente não detectado.

**Verdadeiros positivos** são o tipo de alerta desejado. Eles significam que as regras que geram alertas funcionaram corretamente.

**Falsos positivos** não são desejáveis. Embora eles não indiquem que ocorreu uma exploração não detectada, eles são caros porque os analistas de segurança cibernética devem investigar alarmes falsos; portanto, o tempo é retirado da investigação de alertas que indicam verdadeiras explorações.

**Verdadeiros negativos** são desejáveis. Eles indicam que o tráfego normal benigno é corretamente ignorado e alertas errôneos não estão sendo emitidos.

**Falsos negativos** são perigosos. Eles indicam que as explorações não estão sendo detectadas pelos sistemas de segurança que estão em vigor. Esses incidentes podem passar despercebidos por um longo período de tempo, e a perda e danos contínuos de dados podem resultar.

Eventos benignos são aqueles que não devem acionar alertas. Os eventos benignos em excesso indicam que algumas regras ou outros detectores precisam ser melhorados ou eliminados.

Quando os verdadeiros positivos são suspeitos, um analista de segurança cibernética às vezes é obrigado a escalar o alerta para um nível mais alto para investigação. O investigador avançará com a investigação, a fim de confirmar o incidente e identificar qualquer dano potencial que possa ter sido causado. Essas informações serão usadas por mais funcionários de segurança sênior que trabalharão para isolar os danos, solucionar vulnerabilidades, mitigar a ameaça e lidar com os requisitos de relatórios.

Um analista de segurança cibernética também pode ser responsável por informar o pessoal de segurança de que falsos positivos estão ocorrendo na medida em que o tempo do analista de segurança cibernética é seriamente afetado. Esta situação indica que os sistemas de monitoramento de segurança precisam ser ajustados para se tornarem mais eficientes. Alterações legítimas na configuração da rede ou nas regras de detecção recém-baixadas podem resultar em um pico repentino de falsos positivos também.

Falsos negativos podem ser descobertos bem depois de uma exploração ter ocorrido. Isso pode acontecer por meio da análise de segurança retrospectiva (RSA). A RSA pode ocorrer quando regras recém-obtidas ou outras informações sobre ameaças são aplicadas a dados de segurança de rede arquivados. Por esse motivo, é importante monitorar as informações sobre ameaças para conhecer novas vulnerabilidades e explorações e avaliar a probabilidade de que a rede estava vulnerável a elas em algum momento no passado. Além disso, a exploração deve ser avaliada em relação aos danos potenciais que a empresa pode sofrer. Pode determinar-se que a adição de novas técnicas de atenuação é suficiente ou que deve ser realizada uma análise mais pormenorizada.

11.2.3 Análise Determinística e Análise Probabilística

Técnicas estatísticas podem ser usadas para avaliar o risco de que as explorações serão bem-sucedidas em uma determinada rede. Esse tipo de análise pode ajudar os tomadores de decisão a avaliar melhor o custo de mitigar uma ameaça com os danos que uma exploração poderia causar.

Duas abordagens gerais utilizadas para isso são a análise determinística e probabilística. A análise determinística avalia o risco com base no que é conhecido sobre uma vulnerabilidade. Ele pressupõe que, para que uma exploração seja bem-sucedida, todas as etapas anteriores do processo de exploração também devem ser bem-sucedidas. Este tipo de análise de risco só pode descrever o pior caso. No entanto, muitos atores ameaçadores, embora conscientes do processo para realizar uma exploração, podem não ter conhecimento ou experiência para concluir com sucesso cada passo no caminho para uma exploração bem-sucedida. Isso pode dar ao analista de segurança cibernética a oportunidade de detectar a exploração e impedi-la antes que ela prossiga.

A análise probabilística estima o sucesso potencial de uma exploração, estimando a probabilidade de que, se uma etapa de uma exploração tiver sido concluída com sucesso, a próxima etapa também será bem-sucedida. A análise probabilística baseia-se em técnicas estatísticas que são projetadas para estimar a probabilidade de que um evento ocorrerá com base na probabilidade de ocorrerem eventos anteriores. Usando esse tipo de análise, os caminhos mais prováveis que uma exploração tomará podem ser estimados e a atenção do pessoal de segurança pode ser focada em prevenir ou detectar a exploração mais provável.

Em uma análise determinística, toda a informação para realizar uma exploração é assumida como sendo conhecida. As características da exploração, como o uso de números de porta específicos, são conhecidas de outras instâncias da exploração ou porque portas padronizadas estão em uso. Na análise probabilística, presume-se que os números de porta que serão utilizados só podem ser previstos com algum grau de confiança. Nessa situação, uma exploração que usa números de porta dinâmicos, por exemplo, não pode ser analisada deterministicamente. Tais explorações foram otimizadas para evitar a detecção por firewalls que usam regras estáticas.

As duas abordagens são resumidas a seguir.

* **Análise Determinística** - Para que uma exploração seja bem-sucedida, todas as etapas anteriores da exploração também devem ser bem-sucedidas. O analista de segurança cibernética conhece as etapas para uma exploração bem-sucedida.
* **Análise Probabilística** - Técnicas estatísticas são usadas para determinar a probabilidade de que uma exploração bem-sucedida ocorrerá com base na probabilidade de que cada etapa da exploração seja bem-sucedida.