**Introdução**

24.0.1

**Por que devo cursar este módulo?**

Os bons protocolos podem ter maus usos. Às vezes, os protocolos que usamos diariamente podem ser virados contra nós. Existem muitos protocolos diferentes que são usados nas operações diárias de uma rede. Este módulo explicará como esses protocolos interagem e impactam o monitoramento da segurança da rede.

24.0.2

**O que vou aprender neste módulo?**

**Título do módulo:** Tecnologias e protocolos

**Objetivo do módulo:** Explicar como as tecnologias de segurança afetam o monitoramento de segurança.﻿

| **Tópico** | **Objetivo do Tópico** |
| --- | --- |
| Monitorando protocolos comuns | Explicar o comportamento dos protocolos de rede comuns no contexto do monitoramento de segurança. |
| Tecnologias de segurança | Explicar como as tecnologias de segurança afetam a capacidade de monitorar protocolos de rede comuns. |

# Monitorando protocolos comuns

24.1.1

## 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.

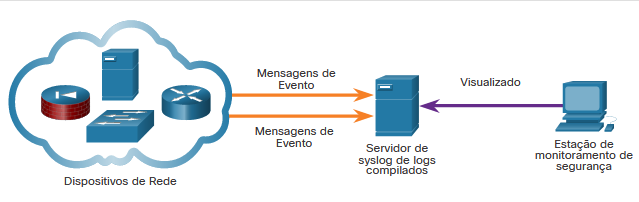
O padrão syslog é usado para registrar mensagens de eventos de dispositivos de rede e endpoints, conforme mostrado na figura. O padrão permite um meio neutro de sistema de transmissão, armazenamento e análise de mensagens. Muitos tipos de dispositivos de vários fornecedores diferentes podem usar syslog 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 as que envolvem exfiltração de dados, podem levar muito tempo para serem concluídas devido às formas muito lentas em que os dados são secretamente roubados da rede. 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 syslog para servidores, adulterar ou destruir dados de log ou adulterar 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.

Pesquise na Internet para obter mais informações sobre syslog-ng.

A figura mostra uma nuvem de dispositivos de rede à direita com duas setas de mensagens de evento apontando para um servidor syslog de logs compilados. À direita deste servidor está uma estação de monitoramento de segurança que tem uma seta exibida também apontando para o servidor.

### Syslog



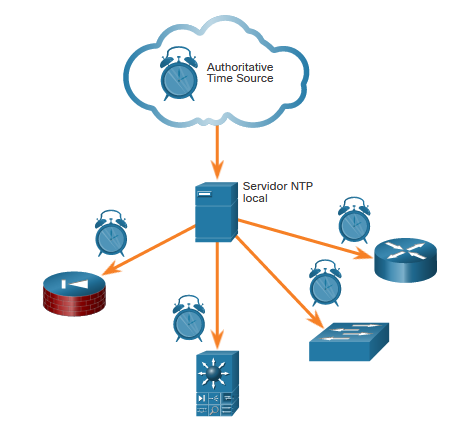
VisualizadoMensagens de EventoServidor de  
syslog de logs compiladosEstação de monitoramento de segurançaMensagens de EventoDispositivos de Rede

24.1.2

**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.



24.1.3

**DNS**

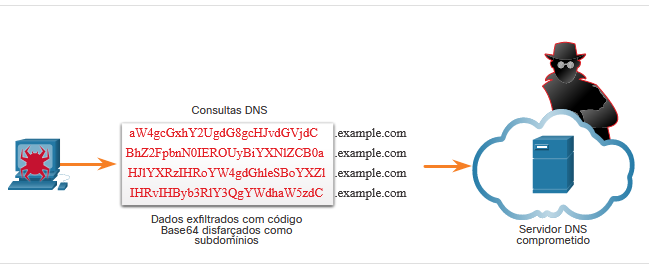
O Serviço de Nome de Domínio (DNS) é usado por milhões de pessoas diariamente. Por isso, muitas organizações têm políticas menos rigorosas para proteger contra ameaças baseadas em DNS do que precisam proteger contra outros tipos de explorações. Os invasores reconheceram isso e geralmente encapsulam diferentes 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.

Consultas DNS para nomes de domínio gerados aleatoriamente, ou subdomínios com aparência aleatória extremamente longos, devem ser consideradas suspeitas, especialmente se a ocorrência deles aumentar drasticamente na rede. Os logs de proxy DNS podem ser analisados para detectar essas condições. Como alternativa, serviços como o serviço DNS passivo do Cisco Umbrella podem ser usados para bloquear solicitações para CNC suspeitos e domínios de exploração.

### Exfiltração DNS



24.1.4

## 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.

O cliente p c à esquerda tem uma linha verde, roxa e laranja indo para um site confiável. A linha verde tem uma lupa com a letra I dentro dela. Palavras sob as linhas: A filtragem de reputação da Web da Cisco se aplica à página da Web solicitada e a todos os quadros. Palavras sob o ícone do site: página da Web acessada chama quadros de outros sites. Três são as mesmas linhas coloridas deixando o site indo para três servidores com as palavras servidores web não afiliados com site confiável pode abrigar software malicioso.

### Exploração de injeção iFrame de HTTP

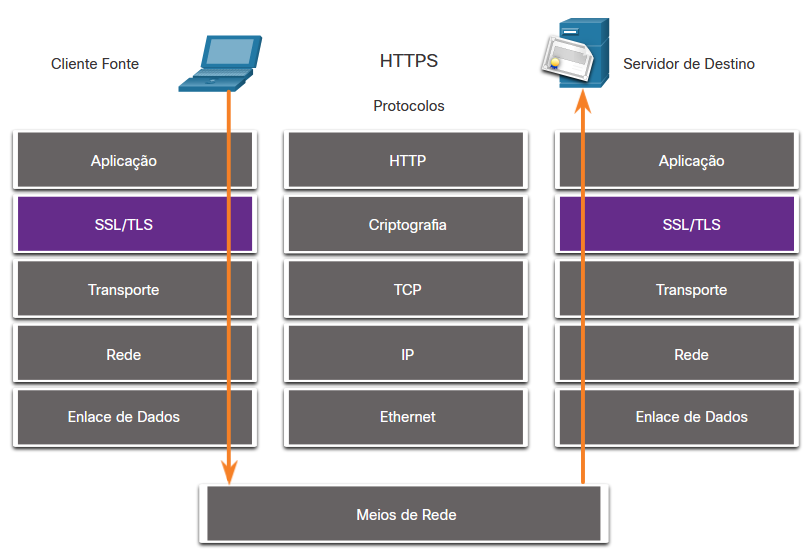


Para lidar com a alteração ou interceptação de dados confidenciais, muitas organizações comerciais adotaram HTTPS ou implementaram políticas somente HTTPS para proteger os visitantes de seus sites e serviços.

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.

A figura mostra que tem três colunas principais com um laptop cliente de origem sobre a coluna esquerda, protocolos h t t p s sobre a coluna do meio e um ícone do servidor de destino sobre a coluna direita. Cada coluna tem cinco caixas de texto. Coluna esquerda: aplicação, realçado s s l/t l s, transporte, rede e ligação de dados. Na coluna central: h t t p, criptografia, t c p, i p e ethernet. Na coluna final: aplicação, destacado s s l/t l s, transporte, rede, link de dados. Uma seta vai do cliente de origem através das caixas à esquerda para baixo para uma caixa de texto de mídia de rede na parte inferior. Uma seta vai desta mesma caixa de texto através de todas as caixas dentro da coluna direita para o servidor de destino.

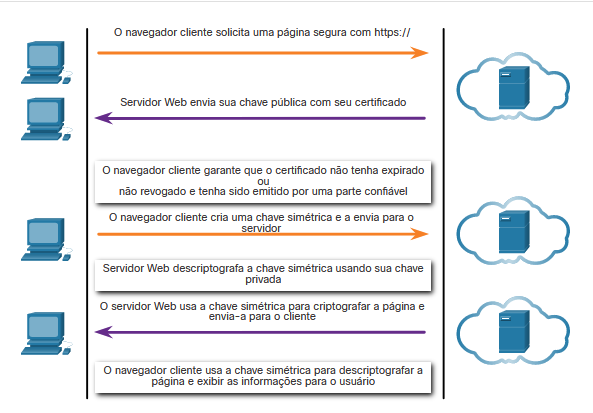
### Diagrama de protocolo HTTPS



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.

Um p c à esquerda tem uma seta que vai para um servidor na nuvem à direita: o navegador cliente solicita uma página segura com https://﻿. Uma seta vai do servidor para o servidor web p c: envia sua chave pública com seu certificado. A próxima seção: navegador cliente garante que o certificado não tenha expirado ou não revogado e tenha sido emitido por uma parte confiável. Uma seta vai do pc cliente para um servidor em uma nuvem: o navegador cliente cria uma chave simétrica e a envia para o servidor. Próxima seção: servidor web descriptografa a chave simétrica usando sua chave privada. Uma seta vai do servidor de nuvem para o servidor web p c: usa a chave simétrica para criptografar a página e enviá-la para o cliente. Na parte inferior: o navegador cliente usa a chave simétrica para descriptografar a página e exibir as informações para o usuário.

### Transações HTTPS



24.1.5

## Protocolos de e-mail

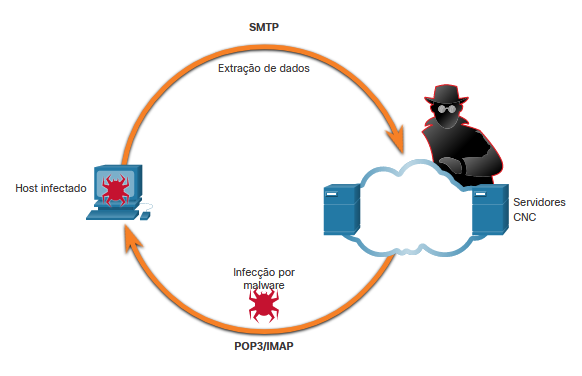
Protocolos de e-mail como SMTP, POP3 e IMAP podem ser usados por atores de ameaças para espalhar malware, exfiltrar dados ou fornecer canais para servidores CNC de malware, como mostrado na figura.

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.

A figura mostra um host infectado à esquerda e uma seta apontando para dois servidores em uma nuvem rotulada como servidores C n C e um ator de ameaça por eles. A seta é rotulada s m t p exfiltração de dados. Outra seta vai dos servidores de volta para o host infectado chamado pop 3/i mapear infecção por malware.

### Ameaças de protocolo de email



24.1.6

**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.

Pesquise na internet para uma explicação detalhada da conhecida exploração LOKI.

**Note**: Este site pode estar bloqueado pelo firewall da sua instituição.

Existem várias ferramentas para a criação de túneis. Procure na internet por Ping Tunnel para explorar uma dessas ferramentas.

# Tecnologias de segurança

24.2.1

## ⁪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.

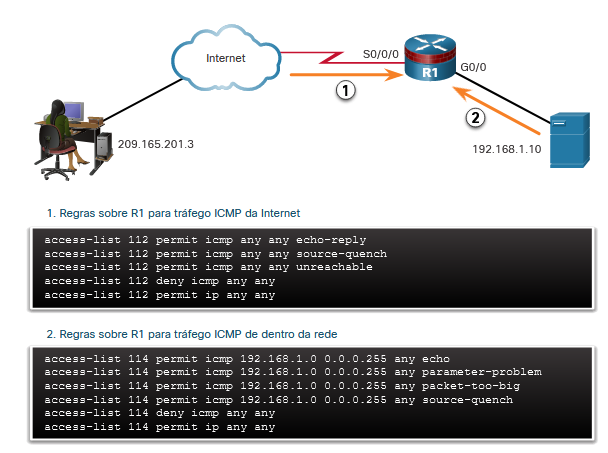
A figura ilustra o uso de ACLs para permitir apenas tipos específicos de tráfego ICMP (Internet Control Message Protocol). O servidor em 192.168.1.10 faz parte da rede interna e tem permissão para enviar solicitações de ping para o host externo em 209.165.201.3. O tráfego ICMP de retorno do host externo é permitido se for uma resposta ICMP, extinção de origem (informa a origem para reduzir o ritmo do tráfego) ou qualquer mensagem ICMP inacessível. Todos os outros tipos de tráfego ICMP são negados. Por exemplo, o host externo não pode iniciar uma solicitação de ping para o host interno. A ACL de saída está permitindo mensagens ICMP que relatam vários problemas. Isso permitirá túneis ICMP e exfiltração de dados.

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.

A figura mostra um usuário em uma estação de trabalho 209 ponto 165 ponto 201 ponto 3 que se conecta à internet. A internet se conecta através de s 0/0/0 no roteador R 1. Uma seta numerada 1 vai da internet para r 1. 1. Regras em R1 para tráfego icmp da internet e comandos: access-list 112 permit icmp any any echo-reply, access-list 112 permit icmp any any source-quench, access-list 112 permit icmp any any unreachable, access-list 112 deny icmp any any, access-list 112 permit ip any any. Roteador r 1 conecta-se a g 0/0 para o 192 ponto 168 ponto 1 ponto 10 servidor e uma seta numerada 2 vai do servidor para r 1. 2. regras em r1 para o tráfego icmp de dentro da rede. access-list 114 permit i c m p 192 dot 168 dot 1 dot 0 0 dot 0 dot 0 dot 255 any echo, access-list 114 permit i c m p 192 dot 168 dot 1 dot 0 0 dot 0 dot 0 dot 255 any parameter-problem, access-list 114 permit i c m p 192 dot 168 dot 1 dot 0 0 dot 0 dot 0 dot 255 any packet-too-big, access-list 114 permit i c m p 192 dot 168 dot 1 dot 0 0 dot 0 dot 0 dot 255 any source-quench, access-list 114 deny i c m p any any, access-list 114 permit i p any any

### Atenuante o abuso de ICMP



24.2.2

## 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).

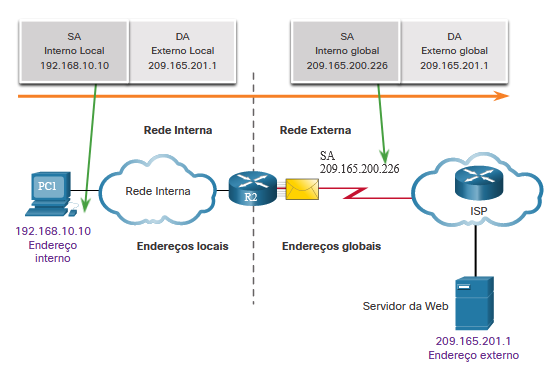
A figura ilustra a relação entre endereços internos e externos que são usados como endereços de origem (SA) e endereços de destino (DA). Esses endereços internos e externos estão em uma rede que está usando NAT para se comunicar com um destino na Internet. Se o PAT estiver em vigor e todos os endereços 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.

O NetFlow é discutido com mais detalhes posteriormente no módulo.

A figura mostra p c 1 192 ponto 168 ponto 10 ponto 10 endereço interno e uma nuvem de rede interna à direita. Palavras acima da nuvem estão dentro da rede e endereços locais. À direita da rede interna é r 2 que tem uma conexão serial a uma nuvem que contém um roteador rotulado I S P que também se conecta a um servidor web rotulado 209 ponto 165 ponto 201 ponto 1 endereço externo. Um envelope está deixando r 2 rotulado S A 209 ponto 165 ponto 200 ponto 226. Uma seta vai da extremidade esquerda através da página com uma seta à direita. Acima da linha é S A dentro local 192 ponto 168 ponto 10 D A fora local 209 ponto 165 ponto 201 ponto 1 e uma seta apontando para p c 1. No lado direito acima da rede externa estão duas caixas: S A dentro global 209 ponto 165 ponto 200 ponto 226 e D A fora global 209 ponto 165 ponto 201 ponto 1.

### Tradução do Endereço da Rede



24.2.3

**Criptografia, encapsulamento e encapsulamento**

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.

24.2.4

## 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.

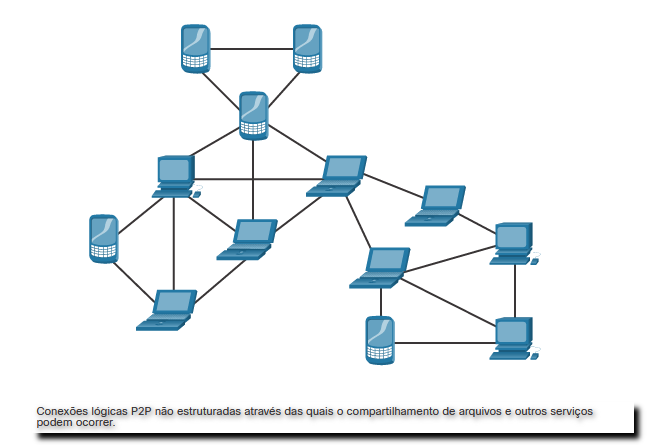
Sempre que os usuários desconhecidos recebem acesso aos recursos de rede, a segurança é uma preocupação. Aplicativos P2P de compartilhamento de arquivos não devem ser permitidos em redes corporativas. A atividade da rede P2P pode contornar as proteções de firewall e é um vetor comum para a propagação 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.

A figura mostra três telefones conectados um ao outro. Um dos telefones celulares se conecta a dois laptops e um p c. O pc também se conecta aos laptops e outro laptop, bem como um telefone celular. Um dos notebooks se conecta a outros três notebooks. Um desses laptops se conecta a um telefone celular e outro p c. palavras inferiores: conexões lógicas P2P não estruturadas através das quais o compartilhamento de arquivos e outros serviços podem ocorrer.

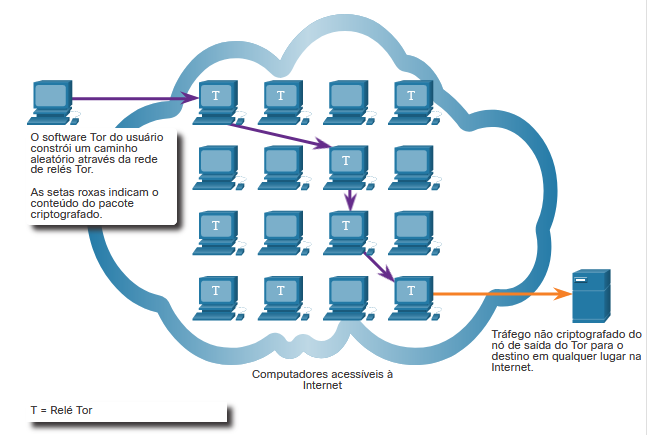
### P2P



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, “roteamento de cebola”) 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.

### Operação Tor



24.2.5

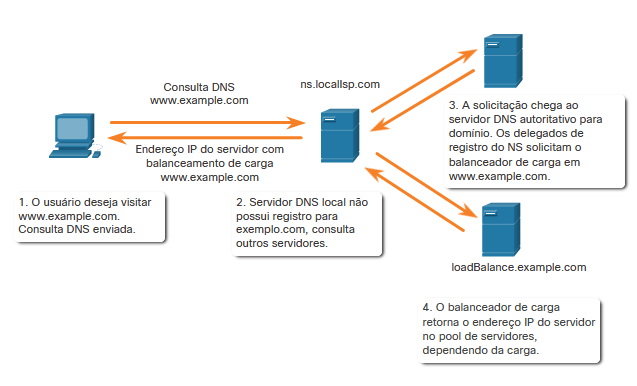
## Balanceamento de carga

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.

A figura mostra um PC à direita com 1. usuário quer visitar [www.example.com.](http://www.example.com.) dns consulta enviada. Uma seta rotulada dns consulta [www.example.com](http://www.example.com) aponta para um servidor rotulado ns.locallsp.com. Sob o servidor: 2. local d n s servidor não tem registro para example.com, consulta outros servidores. Há dois servidores à direita do servidor e uma seta apontando para cada um deles. O servidor no canto superior direito tem 3. solicitação atinge servidor autoritativo dns para domínio. Os delegados de registro do NS solicitam o balanceador de carga em [www.example.com.](http://www.example.com.) Uma seta volta para o servidor ns.locallsp.com. O outro servidor à direita rotulado Loadbalance.Example.com e 4. load balancer retorna i p endereço para o servidor no pool de servidores dependendo da carga. Uma seta também remonta ao servidor ns.locallsp.com. Outra seta vai do servidor ns.locallsp.com para o cliente e essa seta tem palavras: i p endereço do servidor balanceado de carga [www.example.com](http://www.example.com).

### Balanceamento de carga com delegação DNS



# Technologies and Protocols Summary

24.3.1

## O que aprendi neste módulo?

**Monitorando protocolos comuns**

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. Como o syslog é tão importante para o monitoramento de segurança, os servidores syslog podem ser um alvo para atores de ameaças. Os hackers podem tentar bloquear a transferência de dados de clientes syslog para servidores, adulterar ou destruir dados de log ou adulterar software que cria e transmite mensagens de log. As mensagens do Syslog geralmente são carimbadas de data e hora. 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). 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 informações de tempo usadas para correlacionar eventos de rede registrados ou usar sistemas NTP para direcionar ataques DDoS por meio de vulnerabilidades no software cliente ou servidor.

Os invasores 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 podem ser usados para camuflar os dados e evitar medidas básicas de prevenção de perda de dados (DLP). É provável que a parte do subdomínio de tais consultas seria muito mais longa do que as solicitações habituais.

O Hypertext Transfer Protocol (HTTP) é o protocolo de backbone da World Wide Web. 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. Uma exploração comum de HTTP é chamada de injeção iFrame (quadro inline). Um agente 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. 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 SSL (Secure Socket Layer), tornando os dados HTTP ilegíveis à medida que deixa o computador de origem até chegar ao servidor. 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.

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. SMTP envia dados de um host para um servidor de email e entre servidores de email. 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. 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. O monitoramento de segurança pode identificar quando um anexo de e-mail 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.

A funcionalidade ICMP 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. Ele 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.

**Tecnologias de segurança**

As ACLs podem dar uma falsa sensação de segurança se forem excessivamente confiadas. Os invasores podem determinar quais endereços IP, protocolos e portas são permitidos pelas ACLs. Isso pode ser feito por varredura de portas ou 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.

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). 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 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 exfiltrar dados da rede.

Na rede ponto a ponto (P2P), 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. 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. Arquivos compartilhados são frequentemente infectados com malware, e os atores de ameaças podem posicionar seu malware em clientes P2P para distribuição a outros usuários.

Tor é uma plataforma de software e rede de hosts P2P que funcionam como roteadores de internet na rede Tor. Isso permite que os usuários naveguem na internet anonimamente. Os usuários acessam a rede Tor usando um navegador especial. O navegador constrói um caminho de ponta a ponta em camadas na rede do servidor Tor que é criptografado. 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. 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.

O balanceamento de carga envolve a distribuição do tráfego entre dispositivos ou caminhos de rede para evitar recursos de rede sobrecarregados com muito tráfego. 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. Isso pode resultar em uma única transação de Internet sendo representada por vários endereços IP nos pacotes de entrada, o que pode fazer com que recursos suspeitos apareçam em capturas de pacotes. Alguns dispositivos do gerenciador de balanceamento de carga (LBM) usam testes para testar o desempenho de diferentes caminhos e a integridade de diferentes dispositivos. 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.

# Introdução

25.0.1

## Por que devo cursar este módulo?

Que tipos de dados são necessários para realizar o monitoramento de segurança? Que tipo de registro será necessário para capturar os dados necessários para o monitoramento de segurança? Que tipo de informação está incluída nos vários ficheiros de registo que são utilizados para capturar dados para monitorização de segurança? Continue lendo neste módulo para ver como os dados de segurança de rede são coletados, processados e usados para tomar decisões de segurança de rede.

25.0.2

## O que vou aprender neste módulo?

**Título do Módulo:** Segurança de rede de dados

**Objetivo do Módulo:** Explique os tipos de dados de segurança de rede usados no monitoramento de segurança.

| **Título do Tópico** | **Objetivo do Tópico** |
| --- | --- |
| Tipos de dados de segurança | Descreva os tipos de dados usados no monitoramento de segurança. |
| Logs de dispositivos finais | Descrever os elementos de um arquivo de log de dispositivo final. |
| Logs de rede | Descrever os elementos de um arquivo de log de dispositivo de rede. |

# Tipos de dados de segurança

25.1.1

## 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.

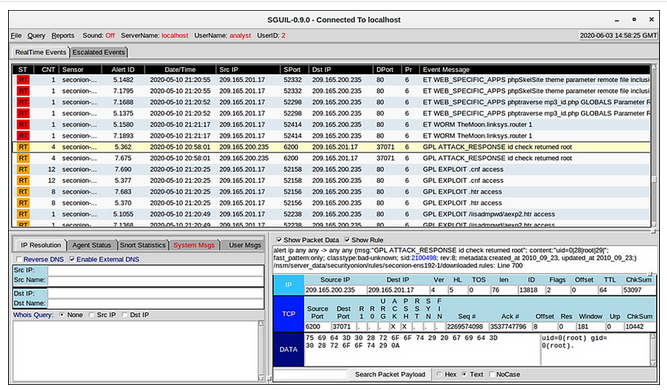
A regra Snort que é acionada é:

alert ip any any -> any any (msg:"GPL ATTACK\\_RESPONSE id check returned root"; content:"uid=0|28|root|29|"; fast\\_pattern:only; classtype:bad-unknown; sid:2100498; rev:8;)

Essa regra gera um alerta se **any IP address** 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 returned 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.

### Console Sguil mostrando o alerta de teste do Snort IDS



25.1.2

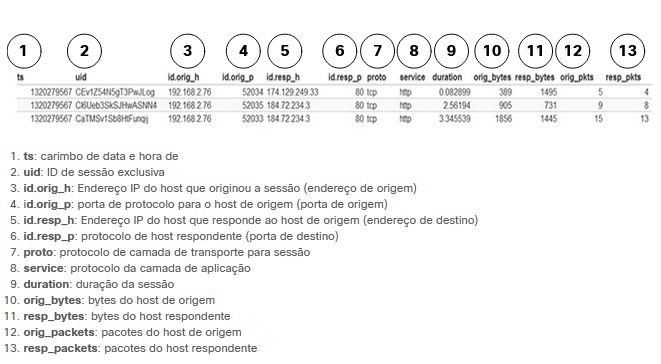
## Dados de Sessão e Transação

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 em laboratórios mais tarde no curso. A figura mostra uma saída parcial para três sessões HTTP a partir de um log de conexão Zeek. As explicações dos campos são mostradas abaixo da figura.

A figura mostra as seguintes colunas numeradas de 1 a 13: t s, u i d, id.orig\_h, id.orig\_p, id.resp\_h, id.resp\_p, serviço proto, duração, orig\_bytes, resp\_bytes, orig\_pkts, resp\_pkts. A primeira linha tem os seguintes dados: 1320279567, CEV1Z545GT3PWJLog, 192 ponto 168 ponto 2 ponto 76, 52034, 174 ponto 129 ponto 249 ponto 33, 80, t c p, h t t t p, 0,082899, 389, 1495, 5, 4. 1. ts: data e hora de início da sessão, 2. u i d: sessão exclusiva i d, 3. id.orig\_h: i p endereço 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: i p endereço do host respondendo ao host de origem (endereço de destino), 6. id.resp\_p: protocolo de host respondendo (porta de destino), 7. proto: protocolo de camada de transporte para sessão, 8. serviço: protocolo de camada de aplicativo, 9. duração: duração da sessão, 10. orig\_bytes: bytes de host de origem, 11. resp\_bytes: bytes de host de resposta, 12. orig\_packets: pacotes de origem host e 13. resp\_packets: pacotes do host respondente

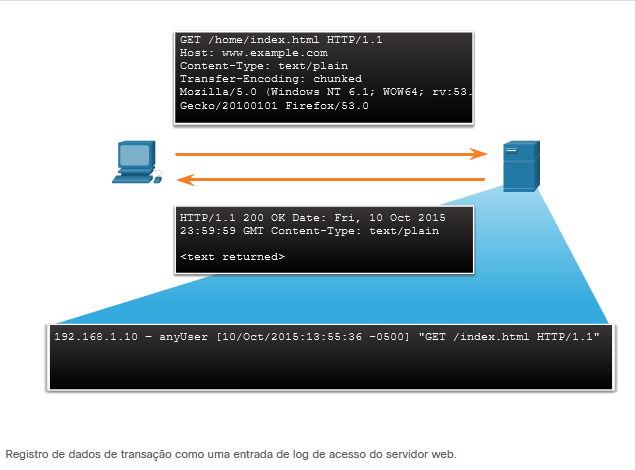
### Dados de Sessão Zeek - Conteúdo Parcial



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.

A figura mostra um p c à esquerda e um servidor à direita. Uma seta vai entre o p c apontando para o servidor. Acima da seta está uma caixa de texto com o seguinte: GET /home/index.html HTTP/1.1, Host: [www.example.com](http://www.example.com), Content-Type: text/plain, Transfer-Coding: fragmentado, Mozilla/5.0 (Windows NT 6.1; WOW64; rv:53.0), Gecko/20100101 Firefox/53.0. Uma seta vai do servidor apontando para p c e a seguinte caixa de texto abaixo da seta: HTTP/1.1 200 OK Data: Sex, 10 Oct 2015 23:59:59 GMT Content-Type: text/plain, <text returned>. Uma seção de breakout do servidor tem texto: 192 ponto 168 ponto 1 ponto 10 - AnyUser [10/Oct/ 2015:13:55:36 -0500] GET /index.html HTTP/1.1 200 326. Palavras inferiores: Registro de dados de transação como uma entrada de log de acesso do servidor web.

### Dados de transação



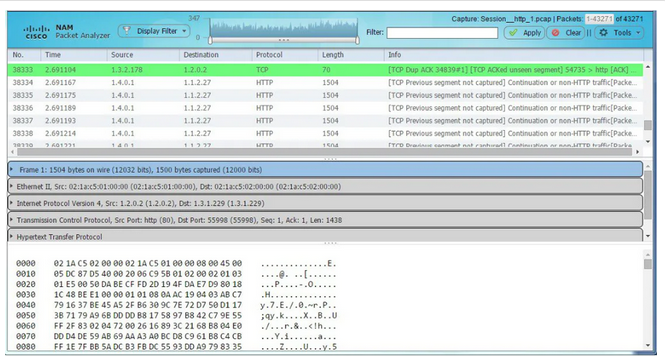
25.1.3

## Capturas de pacotes completos

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.

A figura ilustra a interface do componente Monitor de Análise de Rede do sistema Cisco Prime Infrastructure, que, como o Wireshark, pode exibir capturas completas de pacotes.

### Módulo de análise de rede Cisco Prime - Captura Completa de Pacotes



25.1.4

## 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.

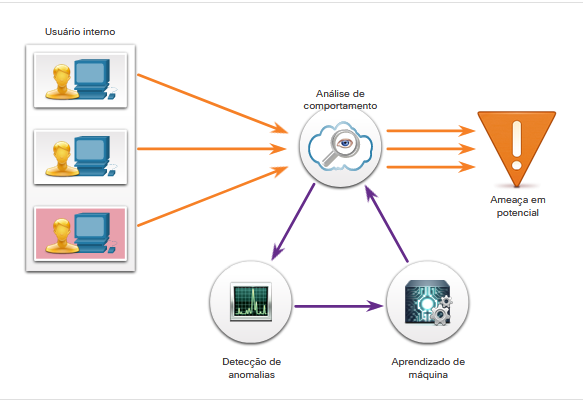
A NBA (Network Behavior Analysis) e a Network Behavior Anomaly Detection (NBAD) são abordagens para monitoramento de segurança de rede que usam técnicas analíticas avançadas para analisar dados de telemetria de rede NetFlow ou IPFIX (Internet Protocol Flow Information Export). Técnicas como análise preditiva 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. O Cognitive Threat Analytics é um produto baseado em nuvem que usa aprendizado de máquina e modelagem estatística de redes. Ele cria uma linha de base do tráfego em uma rede e identifica anomalias. Ele analisa o comportamento do usuário e do dispositivo e o tráfego da Web para descobrir comunicações de comando e controle, exfiltração de dados e aplicativos potencialmente indesejados que operam na infraestrutura. A figura ilustra uma arquitetura para o Cisco Cognitive Threat Analytics.

A figura mostra três usuários internos com cada ícone tendo uma seta apontando para o ícone de análise comportamental. Outro conjunto de três setas vai do ícone de análise comportamental para o ícone de ameaça potencial à direita. Abaixo da análise comportamental estão mais dois ícones: detecção de anomalias e aprendizado de máquina. Uma seta vai da análise comportamental à detecção de anomalias, da detecção de anomalias ao aprendizado de máquina e do aprendizado de máquina apontando para análise comportamental.

### Cisco Cognitive Threat Analytics



Que tipo de dados de monitoramento de rede inclui informações detalhadas sobre protocolo e carga útil para todo o tráfego em um segmento de rede? – Captura de pacote completo

Que tipo de dados de monitoramento de rede resume ou analisa dados de fluxo ou desempenho da rede?- Dados estatísticos

Que tipo de dados de monitoramento de rede inclui logs de servidor e host específicos do dispositivo? – Dados de transação

Que tipo de dados de monitoramento de rede inclui arquivos que estão anexados a e-mails ou que foram baixados da Internet? – Conteúdo extraído

Que tipo de dados de monitoramento de rede contém detalhes dos fluxos de rede, incluindo o 5-tuplas a quantidade de dados transmitidos e a duração da transmissão de dados? – Dados de sessão

Que tipo de dados de monitoramento de rede são gerados por dispositivos IPS ou IDS quando um tráfego suspeito é detectado? – Dados de alerta

O que é usado para gerar e visualizar capturas completas de pacotes? – Tcpdump

Quais dois valores fazem parte de todos os registros de fluxo NetFlow? (Escolha duas.) – Carimbo de data/hora inicial e Carimbo de data/hora final

O que o AVC (Visibilidade e Controle de Aplicativos) usa para descobrir os aplicativos responsáveis pelo tráfego de rede? – NBAR2

Quais dois dispositivos criarão logs de conteúdo suspeito detectado no tráfego de aplicativos? (Escolha duas.) - Dispositivo de segurança de email e dispositivo de segurança da web

# Registros de dispositivos finais

25.2.1

## Logs de host

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. Pesquise OSSEC na internet para saber mais. O Microsoft Windows inclui vários métodos para coleta e análise automatizadas de logs de host. Tripwire oferece um HIDS para Linux que inclui funcionalidade semelhante. Todos podem ser dimensionados para grandes empresas.

Os logs de host do Microsoft Windows são visíveis localmente pelo Visualizador de Eventos. O Visualizador de Eventos mantém quatro 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. |
| Auditoriacom êxito | Uma auditoria bem-sucedida é um evento que registra uma tentativa de acesso de segurança auditada com êxito. Por exemplo, a tentativa bem-sucedida de um usuário para fazer logon no sistema é registrada como um evento de auditoria bem-sucedido. |
| 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. |

Fonte: https://msdn.microsoft.com/en-us/library/windows/desktop/aa363662(v=vs.85).aspx

[Ir para o conteúdo](https://contenthub.netacad.com/cyberops/23.3.1#chunks-container)

*                                                                                                          
*     

1. Dados de segurança de rede
2. Registros de dispositivos finais

# Registros de dispositivos finais

25.2.1

## Logs de host

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. Pesquise OSSEC na internet para saber mais. O Microsoft Windows inclui vários métodos para coleta e análise automatizadas de logs de host. Tripwire oferece um HIDS para Linux que inclui funcionalidade semelhante. Todos podem ser dimensionados para grandes empresas.

Os logs de host do Microsoft Windows são visíveis localmente pelo Visualizador de Eventos. O Visualizador de Eventos mantém quatro 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. |
| Auditoriacom êxito | Uma auditoria bem-sucedida é um evento que registra uma tentativa de acesso de segurança auditada com êxito. Por exemplo, a tentativa bem-sucedida de um usuário para fazer logon no sistema é registrada como um evento de auditoria bem-sucedido. |
| 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. |

Fonte: https://msdn.microsoft.com/en-us/library/windows/desktop/aa363662(v=vs.85).aspx

25.2.2

## 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.

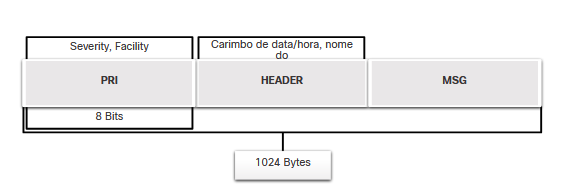
O formato completo de uma mensagem Syslog que é visto na rede tem três partes distintas, como mostrado na figura.

* 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.

A figura mostra três seções principais, a seção p r i de 8 bits que tem as palavras gravidade, facilidade sobre ele, cabeçalho com as palavras timestamp, hostname sobre ele, e msg. Na parte inferior está 1024 bytes.

### 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.

Gravidade

|  |  |
| --- | --- |
| **Value** | **Gravidade** |
| 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**: um evento que não é um erro, mas que é considerado incomum. Não requer ação imediata. |
| 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.

**Priority = (Facility \* 8) + Severity**

O valor Prioridade é o primeiro valor em um pacote e ocorre entre colchetes angulados <>.

A **HEADER** seção da mensagem contém o carimbo de data/hora no **MMM DD HH:MM:SS** formato. 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 **MSG** parte 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.

## 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.

Dois arquivos de log importantes para se familiarizar são os logs de acesso do servidor web Apache e os logs de acesso do Microsoft Internet Information Server (IIS). Exemplos de cada um são mostrados abaixo.

### Log de acesso do Apache

203.0.113.127 – dsmith [10/Oct/2016:10:26:57 - 0500] "GET /logo\_sm.gif HTTP/1.0" 200 2254 "http://www.example.com/links.html" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0"

### Log de acesso do IIS

6/14/2016, 16:22:43, 203.0.113.24, -, W3SVC2, WEB3, 198.51.100.10, 80, GET, /home.htm, -, 200, 0, 15321, 159, 15, HTTP/1.1, Mozilla/5.0 (compatible; MSIE 9.0; Windows Phone OS 7.5; Trident/5.0; IEMobile/9.0), -, http://www.example.com

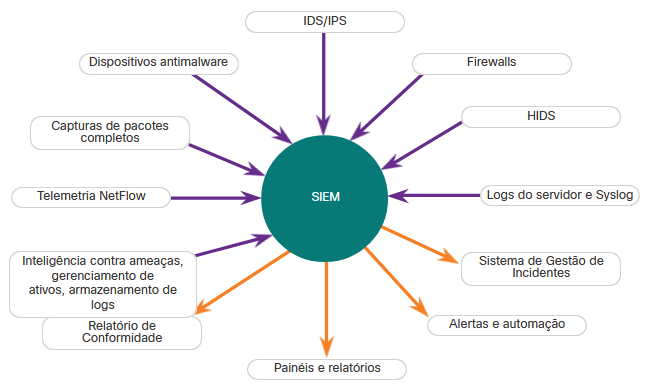
25.2.4

## SIEM e coleta de logs

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.

A figura mostra o círculo S I E M no meio com caixas de texto ao redor da parte superior e cada caixa de texto tem uma seta apontando para s i e m. Caixas de texto: inteligência contra ameaças, gerenciamento de ativos, armazenamento de log; telemetria de fluxo de rede; capturas de pacotes completos; dispositivos antimalware; i d s/i p s; firewalls; h i d s; logs do servidor e syslog. Quatro setas saem do círculo s i e m e cada seta tem uma caixa de texto: relatórios de conformidade, painéis e relatórios, alertas e automação e sistema de gerenciamento de incidentes.

### Entradas e Saídas SIEM

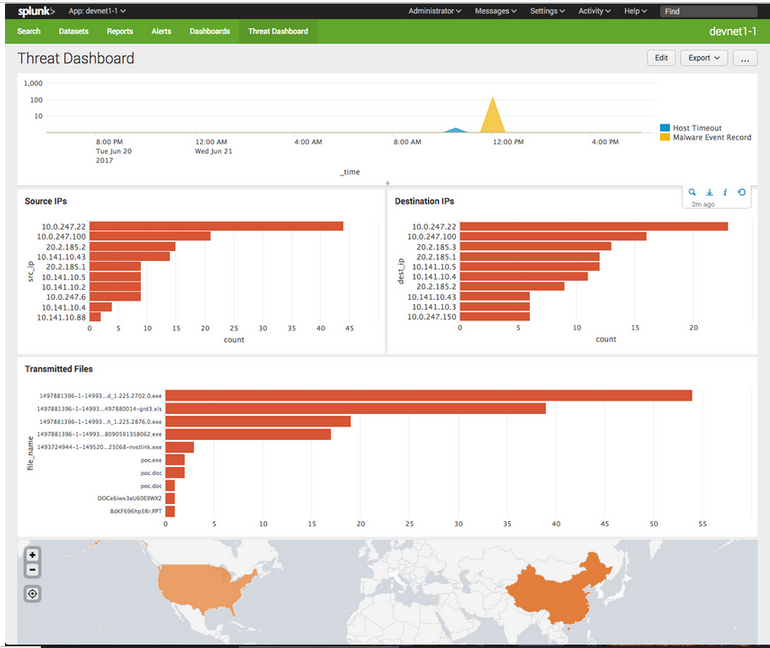


O SIEM combina as funções essenciais de gerenciamento de eventos de segurança (SEM) e ferramentas de gerenciamento de informações de segurança (SIM) para fornecer uma visão abrangente da rede empresarial usando as seguintes funções:

* **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.

### Painel de ameaças do Splunk



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.

# Logs de rede

25.3.1

## Tcpdump

### Um Domínio de Broadcast Grande



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.

25.3.2

## 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. A figura mostra uma tela da ferramenta FlowViewer de código aberto.

### Painel de dados da sessão do NetFlow Flow



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. Um exemplo de um registro básico de fluxo NetFlow, em dois formatos diferentes, é mostrado na figura.

### Registros NetFlow v5 simples

Date flow start Duration Proto Src IP Addr:Port Dst IP Addr:Port Flags Tos Packets Bytes Flows2017-08-30 00:09:12.596 00.010 TCP 10.1.1.2:80 -> 13.1.1.2:8974 .AP.SF 0 62 3512 1

Traffic Contribution: 8% (3/37)Flow information:IPV4 SOURCE ADDRESS:10.1.1.2IPV4 DESTINATION ADDRESS:13.1.1.2INTERFACE INPUT:Se0/0/1TRNS SOURCE PORT:8974TRNS DESTINATION PORT:80IP TOS:0x00IP PROTOCOL:6FLOW SAMPLER ID:0FLOW DIRECTION:Inputipv4 source mask:/0ipv4 destination mask:/8counter bytes:205ipv4 next hop address:13.1.1.2tcp flags:0x1binterface output:Fa0/0counter packets:5timestamp first:00:09:12.596timestamp last:00:09:12.606ip source as:0ip destination as:0

Um grande número de atributos para um fluxo está disponível. O registro IANA de entidades IPFIX lista várias centenas, sendo os primeiros 128 os mais comuns.

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.

25.3.3

## 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.

A figura tem 4 colunas. A coluna mais à esquerda tem um roteador com uma lupa em cima dela: O reconhecimento de aplicativos identifica aplicativos usando L3 a L7 dados 1000+ aplicativos: serviços de nuvem, Cisco Web ex, Você tubo, Skype, P 2 P. Em itálico é N bar 2. A próxima coluna é um gráfico de gráficos, coleta de métricas, métricas de coleta para exportação para ferramenta de gerenciamento: uso de largura de banda, tempo de resposta, latência, perda de pacote, jitter, P 2 P e o seguinte em itálico: fluxo líquido 9, fluxo líquido flexível e correção i p. A terceira coluna tem um roteador com as ferramentas de gerenciamento e geração de relatórios: gerenciamento e geração de relatórios provisionam a rede, coletam dados e relatam o desempenho dos aplicativos: geração de relatórios e gerenciamento de políticas, e em itálico Cisco Prime e outros softwares de terceiros. A última coluna tem um roteador com uma luz vermelha ao lado dele, alta: v o i p, navegação média, baixa transmissão e p 2 p bloqueada.

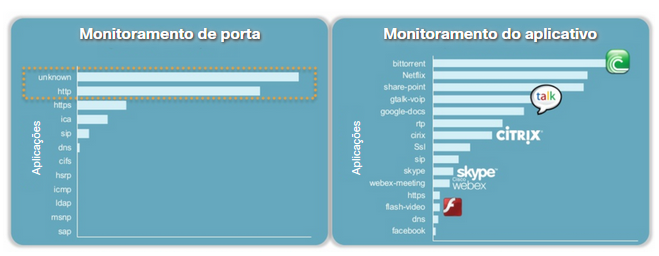
### Cisco Application Visibility and Control



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.

A figura mostra no monitoramento da porta esquerda com aplicativos abaixo do lado desconhecido, h t t p, h t t p s, i c a, s i p, d n s, c i f s, h s r p, i c m p, l d a p, m s n p, e s a p. t t p e estes tem uma caixa pontilhada em torno deles. Na seção de monitoramento de aplicativos, os aplicativos são listados à esquerda com uma barra horizontal ao lado de cada um. A barra horizontal mais longa é com o primeiro aplicativo listado com cada barra horizontal que segue sendo menor em tamanho. Maçãs: bittorrent, net flix, ponto de compartilhamento, gtalk v o i p, google docs, r t p, citrix, s s l, s i p, skype, web ex meeting, h t t p s, flash video, d n s, e livro facial.

### Monitoramento de portas versus monitoramento de



25.3.4

## Logs de filtro de conteúdo

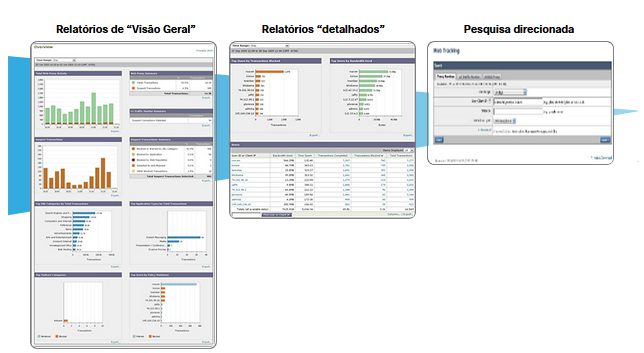
Os dispositivos que fornecem filtragem de conteúdo, como o Cisco Email Security Appliance (ESA) e o Cisco Web Security Appliance (WSA), fornecem uma ampla gama de funcionalidades para monitoramento de segurança. O log está disponível para muitas dessas funcionalidades.

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.

A figura ilustra os painéis de “detalhamento” disponíveis nos dispositivos de filtragem de conteúdo da Cisco. Ao clicar em componentes dos relatórios Visão geral, detalhes mais relevantes são exibidos. As buscas de destino fornecem as informações mais focadas.



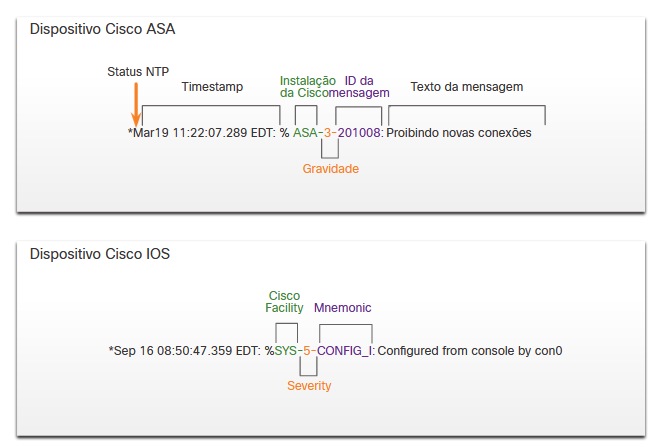
25.3.5

## Registro 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.

A figura mostra Cisco a s um dispositivo. A linha começa com um asterisco e tem as palavras n t p status apontando para baixo para a letra m de Mar. O carimbo de data/hora é Mar19 11:22:07 .289 EDT:% então a s a que é a instalação Cisco - 3 que é a gravidade - 201008 que é a mensagem i d seguida pelo texto da mensagem: não permitindo novas conexões. A figura também mostra o dispositivo Cisco I O S e uma linha que começa com \*Sep 16 08:50:47 .359 EDT:% e S Y S para a instalação cisco - 5 para a gravidade - CONFIG\_I para o mnemônico seguido por Configurado do console por con0.

### Formatos de mensagens Cisco Syslog



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.

25.3.6

## Logs 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

1265939281.764 19478 172.16.167.228 TCP\_MISS/200 864 GEThttp://www.example.com//images/home.png - NONE/- image/png

| **Valor de log de proxy** | **Explicação** |
| --- | --- |
| 1265939281.764 | **Hora** -em formato Unix epoch timestamp com milissegundos |
| 19478 | **Duração** - o tempo decorrido para a solicitação e resposta de Squid |
| 172.16.167.228 | **Endereço IP do** cliente |
| TCP\_MISS/200 | **Resultado** - Códigos de resultado Squid e código de status HTTP separados por uma barra |
| 864 | **Tamanho** - os bytes de dados entregues |
| GET | **Solicitação** - solicitação HTTP feita pelo cliente |
| http://www.example.com//images/home.png | **URI/URL** - endereço do recurso que foi solicitado |
| - | **Identidade do cliente** - valorRFC 1413 para o cliente que fez a solicitação. Não usado por padrão. |
| NONE/- | **Código de peering /host de peer** - servidor de cache vizinho consultado |
| 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

"2015-01-16 17:48:41","ActiveDirectoryUserName",

"ActiveDirectoryUserName,ADSite,Network",

"10.10.1.100","24.123.132.133","Allowed","1 (A)",

"NOERROR","domain-visited.com.",

"Chat,Photo Sharing,Social Networking,Allow List"

| **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. |
| Identidade da política | ActiveDirectoryUserName | A primeira identidade que correspondeu à solicitação. |
| Identidades | ActiveDirectoryUserName,ADSite,Network | Todas as identidades associadas a esta solicitação. |
| IP interno | 10.10.1.100 | O endereço IP interno que fez a solicitação. |
| IP externo | 24.123.132.133 | O endereço IP externo que fez a solicitação. |
| Ação | Permitido | 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. |
| Domínio | domain-visited.com. | Este é o domínio que foi solicitado. |
| Categorias | Chat, Compartilhamento de fotos, Redes sociais | As categorias de segurança ou conteúdo correspondentes ao destino. |

25.3.7

## Cisco Firepower estão disponíveis

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.

A figura mostra 7 seções com ícones dentro de cada seção: prevenção de intrusões (assinatura), visibilidade e controle de aplicativos, análise de poder de fogo e automação, proteção avançada contra malware e sandboxing (assinatura), criação de perfil de rede, filtragem u r l (assinatura), e identificar política controle e v p n.

### Serviços prestados pela NGFW



# Resumo de dados de segurança de rede

25.4.1

## O que aprendi neste módulo?

**Tipos de dados de segurança**

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. Dentro do conjunto Security Onion de ferramentas NSM, os alertas são gerados pelo Snort e são legíveis e pesquisáveis pelos aplicativos Sguil, Squert e Kibana.

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. 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.

Capturas completas de pacotes são os dados de rede mais detalhados que geralmente são coletados. As capturas completas de pacotes exigem o maior armazenamento. As capturas completas de pacotes contêm o conteúdo real de conversas de dados, como o texto de mensagens de email, o HTML em páginas da Web e os arquivos que entram ou saem da rede. O conteúdo extraído pode ser recuperado de capturas completas de pacotes e ser analisado quanto a malware ou comportamento do usuário que viola as políticas de negócios e de segurança.

Os dados estatísticos são criados através da análise de várias formas de dados de rede. 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.

**Registros de dispositivos finais**

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. Muitas proteções baseadas em host têm uma maneira de enviar logs para servidores centralizados de gerenciamento de logs, fornecendo uma maneira de pesquisar logs a partir de um local central usando ferramentas NSM. O OSSEC, um HIDS de código aberto popular, inclui uma funcionalidade robusta de coleta e análise de logs.

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.

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 documentam todas as consultas DNS e respostas que ocorrem na rede. 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.

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 corporativa usando coleta de logs, normalização, correlação, agregação, relatórios e conformidade.

**Logs de rede**

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. As capturas incluem protocolo de pacote detalhado e dados de conteúdo que podem ser visualizados com o Wireshark.

O NetFlow fornece com eficiência um importante conjunto de serviços em um formato baseado em sessão para aplicativos IP, incluindo contabilidade de tráfego de rede, faturamento de rede baseado em 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 Cisco Application Visibility and Control 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.

Dispositivos como o Cisco Email Security Appliance (ESA) e o Cisco Web Security Appliance (WSA) fornecem uma ampla gama de funcionalidades para monitoramento de segurança utilizando filtragem de conteúdo. O log está disponível para muitas dessas funcionalidades.

Servidores proxy são dispositivos que atuam como intermediários para clientes de rede. 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 que podem ser analisadas para determinar quais hosts estão fazendo as solicitações, se os destinos são seguros ou potencialmente mal-intencionados, e também para obter insights sobre o tipo de recursos que foram baixados.

Os dispositivos NextGen Firewall 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 fornecem muito mais funcionalidade do que as gerações anteriores de dispositivos de segurança de rede. Os painéis de relatórios do NextGen Firewall com recursos interativos permitem relatórios rápidos de apontar e clicar sobre informações muito específicas sem a necessidade de SIEM ou outros correladores de eventos.

Que tipo de evento ocorre quando ocorrem atividades mal-intencionadas que podem afetar a disponibilidade, integridade e confidencialidade de um host e seus dados? – Intrusão

Que tipo de evento é registrado quando um host aparece pela primeira vez na rede?– Host ou dispositivo final

Que tipo de evento é usado quando o NetFlow detecta um novo host na rede? – Netflow

Que tipo de eventos dizem respeito a sessões entre hosts descobertos diretamente pelo NextGen Firewall? – Conexão

Que tipo de evento ocorre quando são detectadas alterações em hosts de rede e aplicativos conhecidos pela rede? – Descoberta de rede