



Module 25: Dados de segurança de rede



CyberOps Associate v1.0

Prof. Clemilson Oliveira

clemilson.oliveira@edu.sc.senai.br

Objetivos do Módulo

Título do módulo: Dados de segurança de rede

Objetivo do módulo: Explique os tipos de dados de segurança de rede utilizados no monitoramento de segurança.

Topic Title	Topic Objective
Tipos de Dados de Segurança	Descreva os tipos de dados usados no monitoramento de segurança.
End Device Logs	Descreva os elementos de um arquivo de registro de dispositivo final.
Network Logs	Descreva os elementos de um arquivo de log de dispositivo de rede.

25.1 Types of Security Data

Dados de segurança de rede

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 um 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 de ferramentas NSM da Security Onion.

The screenshot shows the Sguil-0.9.0 interface connected to localhost. The top bar displays the date and time: 2020-06-03 14:58:25 GMT. The main window is divided into two panes. The left pane shows a list of alerts with columns: ST, CNT, Sensor, Alert ID, DateTime, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. The right pane shows a detailed view of a selected alert, including the alert ID, message, and packet details.

ST	CNT	Sensor	Alert ID	DateTime	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	seconion...	5.1482	2020-05-10 21:20:55	209.165.201.17	52332	209.165.200.235	80	6	ET WEB_SPECIFIC_APPS phpSkelSite theme parameter remote file inclusi
RT	1	seconion...	7.1795	2020-05-10 21:20:55	209.165.201.17	52332	209.165.200.235	80	6	ET WEB_SPECIFIC_APPS phpSkelSite theme parameter remote file inclusi
RT	1	seconion...	7.1688	2020-05-10 21:20:52	209.165.201.17	52298	209.165.200.235	80	6	ET WEB_SPECIFIC_APPS phpSkelSite theme parameter remote file inclusi
RT	1	seconion...	5.1375	2020-05-10 21:20:52	209.165.201.17	52298	209.165.200.235	80	6	ET WEB_SPECIFIC_APPS phpSkelSite theme parameter remote file inclusi
RT	1	seconion...	5.1580	2020-05-10 21:21:17	209.165.201.17	52414	209.165.200.235	80	6	ET WORM TheMoon.linksys.router.1
RT	1	seconion...	7.1893	2020-05-10 21:21:17	209.165.201.17	52414	209.165.200.235	80	6	ET WORM TheMoon.linksys.router.1
RT	4	seconion...	5.362	2020-05-10 20:58:01	209.165.200.235	6200	209.165.201.17	37071	6	GPL ATTACK_RESPONSE id check returned root
RT	4	seconion...	7.675	2020-05-10 20:58:01	209.165.200.235	6200	209.165.201.17	37071	6	GPL ATTACK_RESPONSE id check returned root
RT	12	seconion...	7.690	2020-05-10 21:20:25	209.165.201.17	52158	209.165.200.235	80	6	GPL EXPLOIT .crf access
RT	8	seconion...	5.377	2020-05-10 21:20:25	209.165.201.17	52158	209.165.200.235	80	6	GPL EXPLOIT .crf access
RT	8	seconion...	7.683	2020-05-10 21:20:25	209.165.201.17	52158	209.165.200.235	80	6	GPL EXPLOIT .httr access
RT	8	seconion...	5.370	2020-05-10 21:20:25	209.165.201.17	52158	209.165.200.235	80	6	GPL EXPLOIT .httr access
RT	1	seconion...	5.1055	2020-05-10 21:20:49	209.165.201.17	52238	209.165.200.235	80	6	GPL EXPLOIT /isadripwd/aexp2.httr access
RT	1	seconion...	7.1368	2020-05-10 21:20:49	209.165.201.17	52238	209.165.200.235	80	6	GPL EXPLOIT /isadripwd/aexp2.httr access

The detailed view of the selected alert shows the following information:

- Alert ID: 5.362
- Message: GPL ATTACK_RESPONSE id check returned root
- Packet Details: Source IP: 209.165.200.235, Dest IP: 209.165.201.17, Ver: 4, HL: 5, TOS: 0, Len: 76, ID: 13818, Flags: 0, Offset: 64, ChkSum: 53097
- TCP Details: Source Port: 6200, Dest Port: 37071, Seq #: 3537747796, Ack #: 3537747796, Window: 0, Res: 181, Up: 0, ChkSum: 10442
- DATA: 75 69 64 30 30 28 72 6F 6F 74 29 20 67 69 64 30 uid=0(root) gid=0(root).

Console Sguil mostrando alerta de teste do Snort IDS

Session and Transaction Data

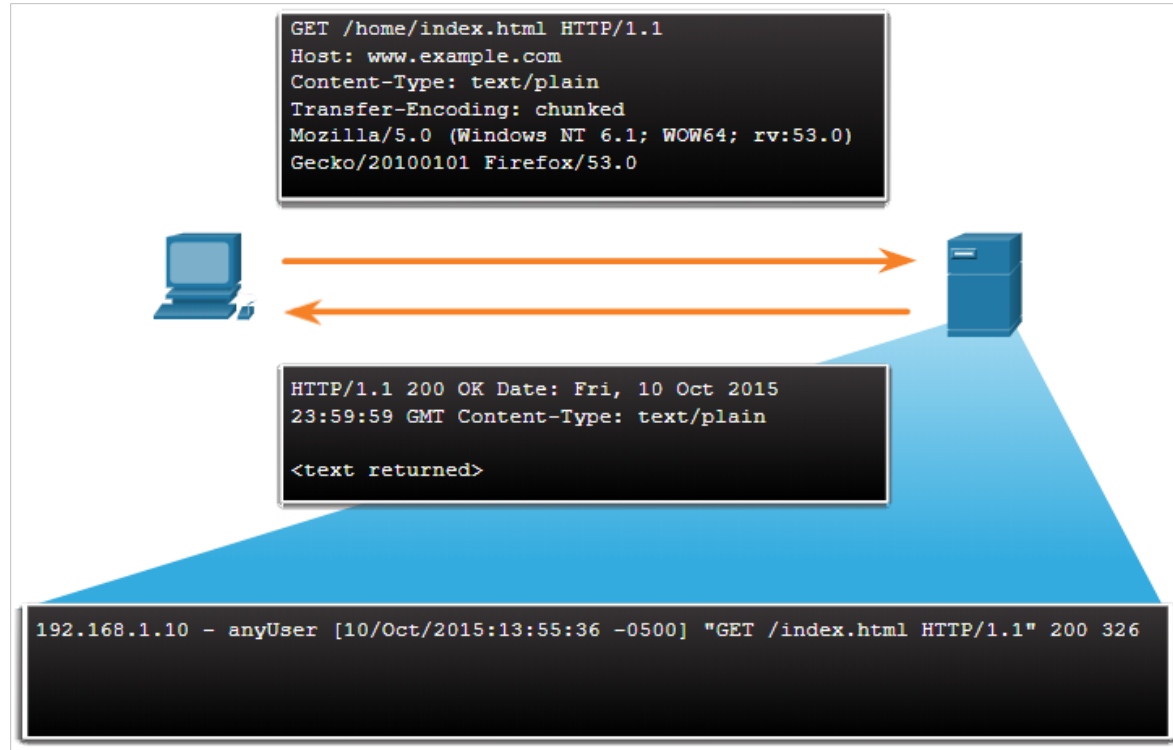
- Os dados da sessão são um registro de uma conversa entre dois pontos finais da rede.
- Ele inclui os cinco tuplas de endereços IP de origem e destino, números de porta de origem e destino e o código IP para o protocolo em uso.
- Os dados sobre a sessão incluem um ID de sessão, a quantidade de dados transferidos por fonte e destino e informações relacionadas à duração da sessão.
- A figura mostra uma saída parcial para três sessões HTTP de um registro de conexão Zeek.

1	2	3	4	5	6	7	8	9	10	11	12	13
ts	uid	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	service	duration	orig_bytes	resp_bytes	orig_pkts	resp_pkts
1320279567	CEv1Z54N5gT3PwJLog	192.168.2.76	52034	174.129.249.33	80	tcp	http	0.082899	389	1495	5	4
1320279567	Ci6Ueb3SkSJHwASNIN4	192.168.2.76	52035	184.72.234.3	80	tcp	http	2.56194	905	731	9	8
1320279567	CaTMSv1Sb8HtFunqj	192.168.2.76	52033	184.72.234.3	80	tcp	http	3.345539	1856	1445	15	13

1. **ts**: session start timestamp
2. **uid**: unique session ID
3. **id.orig_h**: IP address of host that originated the session (source address)
4. **id.orig_p**: protocol port for the originating host (source port)
5. **id.resp_h**: IP address of host responding to the originating host (destination address)
6. **id.resp_p**: protocol of responding host (destination port)
7. **proto**: transport layer protocol for session
8. **service**: application layer protocol
9. **duration**: duration of the session
10. **orig_bytes**: bytes from originating host
11. **resp_bytes**: bytes from responding host
12. **orig_packets**: packets from the originating host
13. **resp_packets**: packets from responding host

Session and Transaction Data (Contd.)

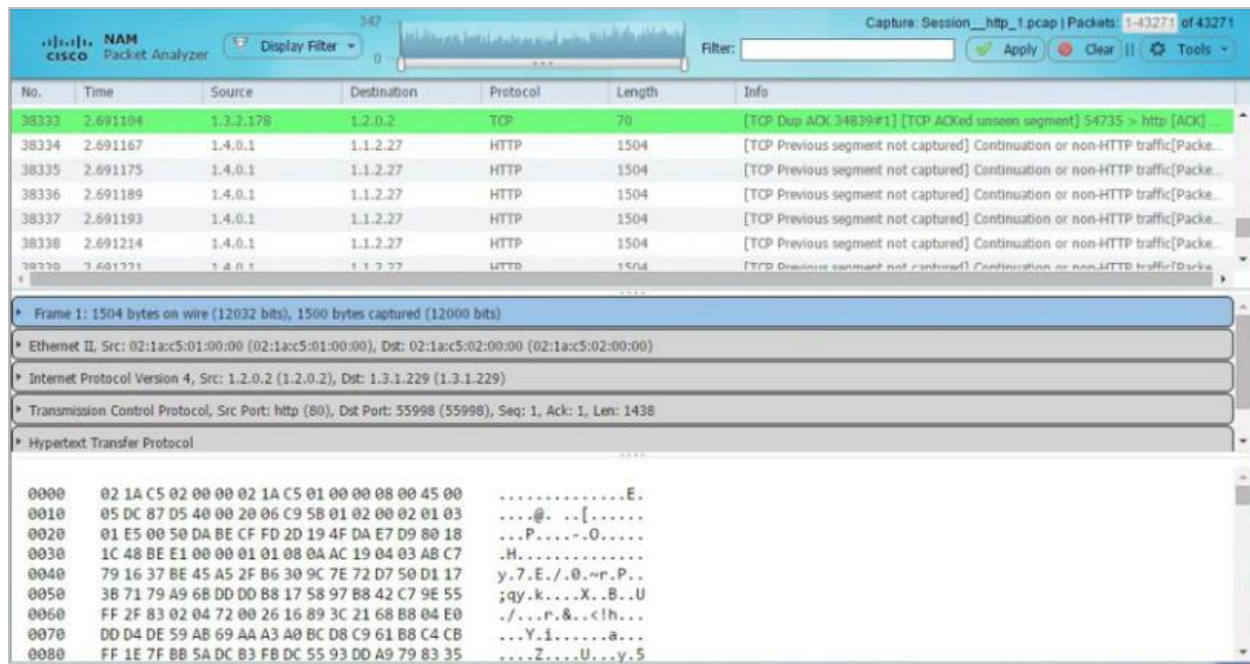
- Os dados de transação consistem nas mensagens que são trocadas durante as sessões de rede.
- Essas transações podem ser visualizadas em transcrições de captura de pacotes.
- As transações que representam as solicitações e respostas seriam registradas em um log de acesso em um servidor ou por um NIDS como zeek.
- Uma sessão pode incluir o download de conteúdo de um servidor web, como mostrado na figura.



Network Security Data

Full Packet Captures

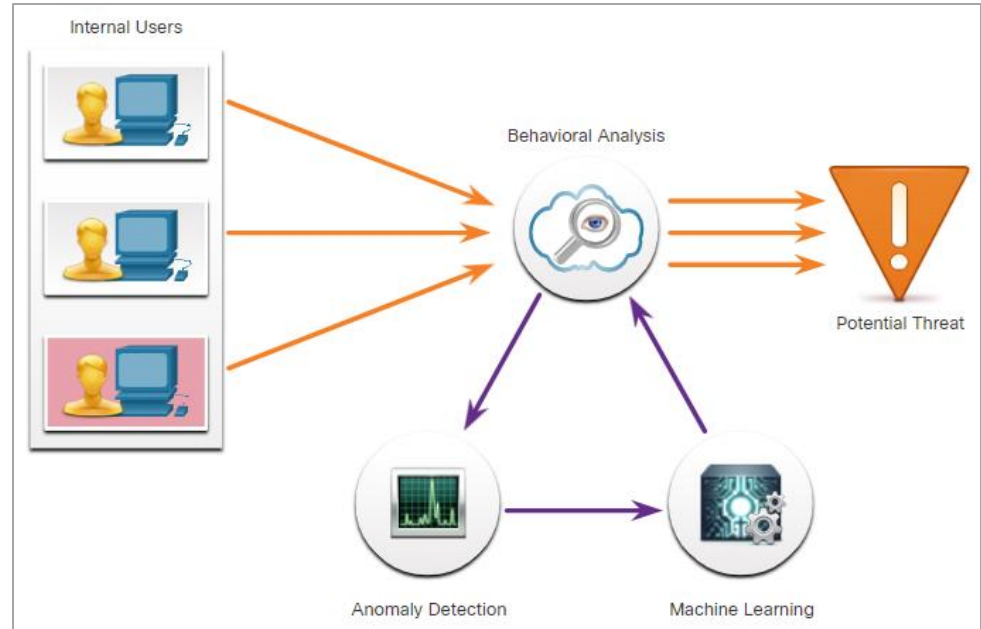
- Capturas completas de pacotes são os dados de rede mais detalhados que são geralmente coletados.
- Ele contém o conteúdo real das conversas, como texto de mensagens de e-mail, o HTML em páginas da Web e os arquivos que entram ou saem da rede.
- O conteúdo extraído pode ser recuperado de capturas completas de pacotes e analisado para malware ou comportamento do usuário que viola políticas de negócios e segurança.
- A figura aqui mostra a interface para o componente Monitor de Análise de Rede do sistema Cisco Prime Infrastructure, que pode exibir capturas completas de pacotes.



Network Security Data

Statistical Data

- Os dados estatísticos são sobre o tráfego de rede que é criado através da análise de outras formas de dados de rede.
- 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 dessas faixas.
- Um exemplo de uma ferramenta NSM que utiliza análise estatística é a Cisco Cognitive Threat Analytics.
- Ele é capaz de encontrar atividades maliciosas que contornaram controles de segurança ou entraram na rede através de canais não monitorados (incluindo mídia removível) e está operando dentro de um ambiente da organização.
- A figura mostra uma arquitetura para a Cisco Cognitive Threat Analytics.



25.2 End Device Logs

Host Logs

- Os sistemas de detecção de intrusão baseados em host (HIDS) são executados em hosts individuais.
- Muitas proteções baseadas em host enviam logs para um servidor centralizado de gerenciamento de log que pode ser pesquisado a partir de um local central usando ferramentas NSM.
- Os registros de host do Microsoft Windows são visíveis localmente através do Event Viewer. O Visualizador de Eventos mantém quatro tipos de logs:
- Registros de aplicativos – Estes contêm eventos registrados por vários aplicativos.
- Registros do sistema – Estes incluem eventos relativos à operação de drivers, processos e hardware.
- Registros de configuração – Essas informações de registro sobre a instalação de software, incluindo atualizações do Windows.
- Registros de segurança – Esses eventos de registro relacionados à segurança, como tentativas de logon e operações relacionadas ao gerenciamento de arquivos ou objetos e acesso.
- Logs de linha de comando – Invasores que tiveram 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 de registro fornecerá visibilidade sobre este tipo de incidente.

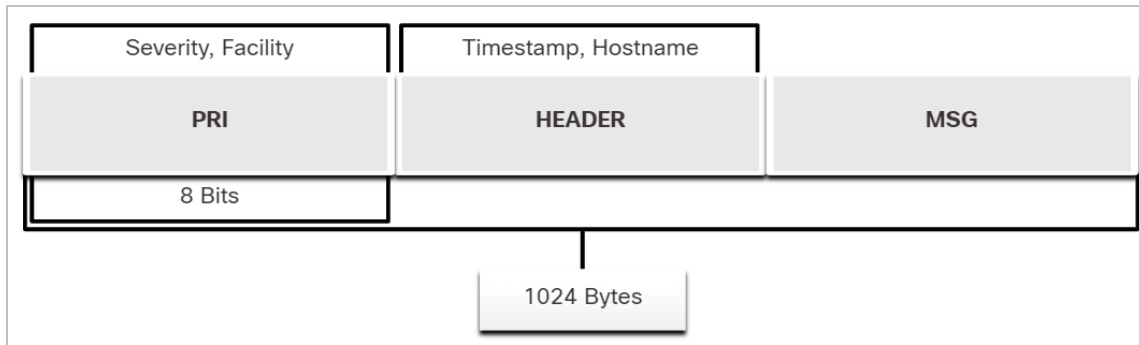
Host Logs (Contd.)

A tabela explica o significado dos cinco tipos de eventos de log de host do Windows.

Event Type	Description
Error	É um evento que indica um problema significativo, como perda de dados ou funcionalidade. Por exemplo, se um serviço não carregar durante a inicialização, um evento de erro será registrado.
Warning	É um evento que não é necessariamente significativo, mas pode indicar um possível problema futuro. Por exemplo, quando o espaço do disco está baixo, um evento de aviso é registrado. Se um aplicativo se recuperar de um evento sem perda de funcionalidade ou dados, ele pode classificar o evento como um evento de aviso.
Information	Ele descreve a operação bem sucedida de um aplicativo, driver ou serviço. Por exemplo, quando um driver de rede carrega com sucesso, pode ser apropriado registrar um evento de informações. Observe que geralmente é inapropriado para um aplicativo de desktop registrar um evento cada vez que ele é iniciado.
Success Audit	É um evento que registra uma tentativa de acesso de segurança auditada que é bem sucedida. Por exemplo, a tentativa bem sucedida de um usuário de fazer logon no sistema é um evento de auditoria de sucesso.
Failure Audit	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 será registrada como um evento de auditoria de falha.

Syslog

- O Syslog inclui especificações para formatos de mensagens, uma estrutura de aplicativos cliente-servidor e protocolo de rede. É um protocolo cliente/servidor.
- Muitos tipos diferentes de dispositivos de rede podem ser configurados para usar o padrão syslog para registrar eventos em servidores de syslog centralizados.
- O formato completo de uma mensagem Syslog tem três partes distintas: PRI (prioridade), CABEÇALHO, MSG (texto de mensagem).
- O PRI consiste em dois elementos, a Instalação e a Gravidade da mensagem, que são ambos valores inteiros.
- A Instalação consiste em fontes que geraram a mensagem, como sistema, processo ou aplicativo.
- A Gravidade é um valor de 0-7 que define a gravidade da mensagem.



End Device Logs

Syslog (Contd.)

Instalação

Os códigos de instalação entre 15 e 23 (local0-local7) não são atribuídos a uma palavra-chave ou nome.

Eles podem ser atribuídos a diferentes significados, dependendo do contexto de uso. Além disso, vários sistemas operacionais foram encontrados para utilizar ambas as instalações 9 e 15 para mensagens de relógio.

Severidade

Value	Severity
0	Emergency: sistema é inutilizável
1	Alert: ação deve ser tomada imediatamente
2	Critical: condições críticas que devem ser corrigidas imediatamente e indica falha em um sistema
3	Error: uma falha que não é urgente, deve ser resolvida dentro de um determinado tempo
4	Warning: um erro não existe atualmente; mas, um erro ocorrerá no futuro se a condição não for tratada
5	Notice: um evento que não é um erro, mas que é considerado incomum. Não requer ação imediata.
6	Informational: mensagens emitidas sobre o funcionamento normal
7	Debug: mensagens de interesse para desenvolvedores

Syslog (Contd.)

Prioridade

O valor de Prioridade (PRI) é calculado multiplicando o valor da instalação por 8 e, em seguida, adicionando-o ao valor de gravidade, como mostrado abaixo

$$\text{Prioridade} = (\text{Facilidade} * 8) + \text{Gravidade}$$

O valor prioritário é o primeiro valor em um pacote e ocorre entre suportes angulares <>.

Server Logs

- Os registros de servidores são uma fonte essencial de dados para monitoramento de segurança de rede.
- Os registros de servidor proxy DNS que documentam todas as consultas e respostas DNS que ocorrem na rede são especialmente importantes.
- Dois arquivos de log importantes são os registros de acesso do servidor web Apache e os registros de acesso do Microsoft Internet Information Server (IIS).

Apache Access Log

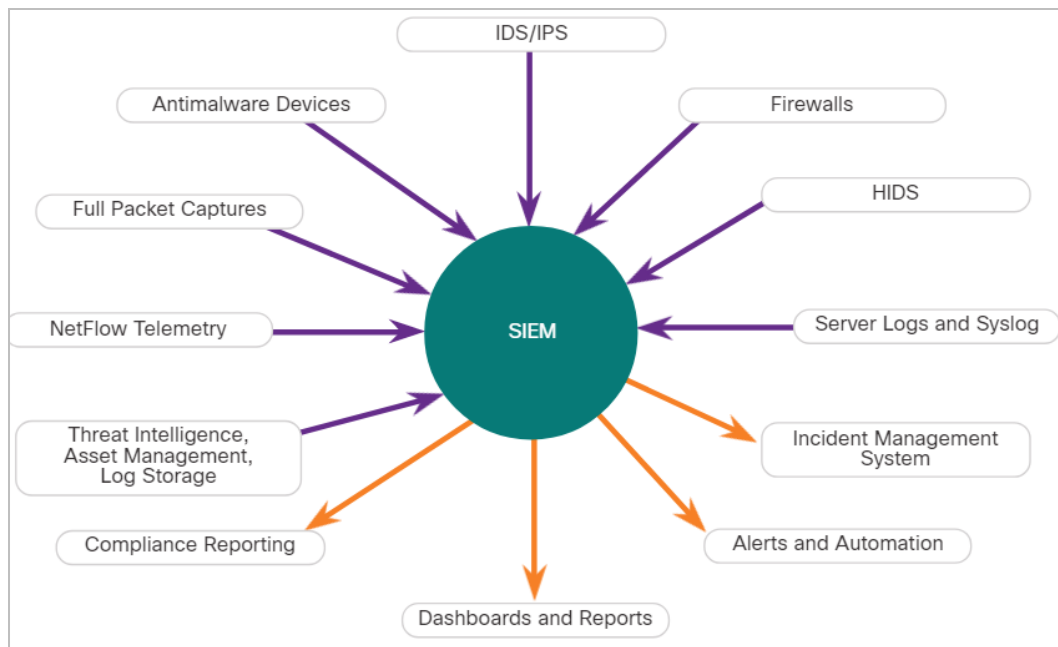
```
203.0.113.127 - dsmith [10/Oct/2016:10:26:57 - 0500] "GET /logo_sm.gif HTTP/1.0" 200 2254  
""http://www.example.com/links.html"" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101  
Firefox/47.0"
```

IIS Access Log

```
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
```


SIEM and Log Collection

A tecnologia SIEM (Security Information and Event Management, gerenciamento de informações e eventos) é usada em muitas organizações para fornecer relatórios em tempo real e análise de longo prazo de eventos de segurança, como mostra a figura.



SIEM Inputs and Outputs

SIEM and Log Collection (Contd.)

O SIEM combina as funções essenciais das ferramentas SEM e SIM para fornecer uma visão da rede corporativa usando as seguintes funções:

Coleta de registros – Registros de eventos de fontes em toda a organização fornecem informações forenses importantes e ajudam a atender aos requisitos de relatórios de conformidade.

Normalização – Isso mapeia mensagens de registro de diferentes sistemas em um modelo de dados comum, permitindo que a organização se conecte e analise eventos relacionados, mesmo que sejam inicialmente conectados diferentes formatos de origem.

Correlação – Isso vincula logs e eventos de sistemas ou aplicativos diferentes, acelerando a detecção e reação a ameaças à segurança.

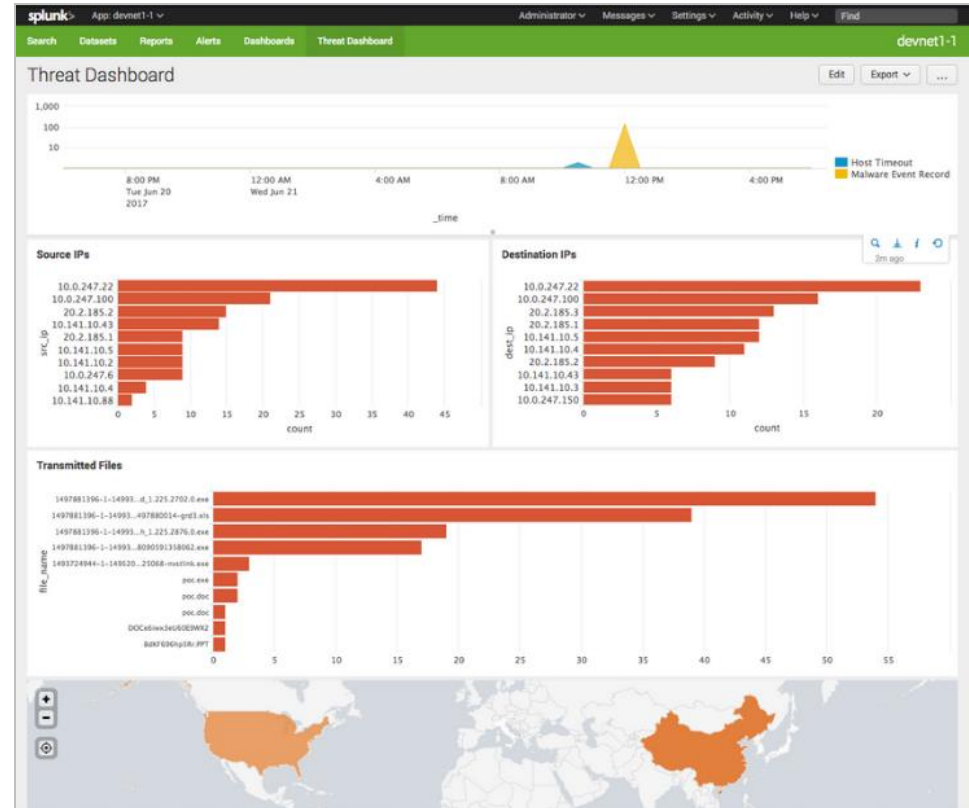
Agregação – Isso reduz o volume de dados do evento consolidando registros duplicados de eventos.

Relatórios – Isso apresenta os dados de eventos correlacionados e agregados em monitoramento em tempo real e resumos de longo prazo, incluindo painéis interativos gráficos.

Conformidade – Este é o relatório para satisfazer os requisitos de várias normas de conformidade.

- nifica
cisco

Splunk Threat Dashboard



25.3 Network Logs

Tcpdump

- A ferramenta de linha de comando `tcpdump` é um analisador de pacotes muito popular.
- Ele pode exibir capturas de pacotes em tempo real ou gravar capturas de pacotes em um arquivo.
- Ele captura dados detalhados do protocolo de pacotes e do conteúdo.
- Wireshark é uma GUI construída sobre a funcionalidade `tcpdump`.
- A estrutura de capturas de `tcpdump` varia dependendo do protocolo capturado e dos campos solicitados.

NetFlow

- NetFlow é um protocolo que foi desenvolvido pela Cisco como uma ferramenta para solução de problemas de rede e contabilidade baseada em sessão.
- O NetFlow fornece um importante conjunto de serviços para aplicativos IP, incluindo contabilidade de tráfego de rede, faturamento de rede baseado em uso, planejamento de rede, segurança, negação de serviço capacidades de monitoramento e monitoramento de rede.
- Ele também fornece informações sobre usuários de rede e aplicativos, horários de pico de uso e roteamento de tráfego.
- Ele registra informações sobre o fluxo do pacote, incluindo metadados. A Cisco desenvolveu o NetFlow e, em seguida, permitiu que ele fosse usado como base para um padrão IETF chamado IPFIX.
- As informações do NetFlow podem ser visualizadas com ferramentas como o nfdump.
- O nfdump fornece um utilitário de linha de comando para visualizar os dados do NetFlow do daemon de captura nfcapd ou coletor.

NetFlow (Contd.)

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

```

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 estão disponíveis. O registro IANA de entidades IPFIX lista várias centenas, sendo as primeiras 128 as mais comuns.
- O NetFlow é uma ferramenta útil na análise de incidentes de segurança de rede. Ele pode ser usado para construir uma linha do tempo de compromisso, entender o comportamento individual do host ou para rastrear o movimento de um invasor ou explorar de host para host dentro de uma rede.

Visibilidade e controle do aplicativo

- O sistema Cisco Application Visibility and Control (AVC) combina múltiplas tecnologias para reconhecer, analisar e controlar mais de 1000 aplicações.
- Estes incluem voz e vídeo, e-mail, compartilhamento de arquivos, jogos, aplicativos peer-to-peer (P2P) e baseados na nuvem.
- A AVC usa a versão 2 de reconhecimento de aplicativos baseada em rede cisco (NBAR2), também conhecida como NBAR de última geração, para descobrir e classificar os aplicativos em uso na rede.
- O mecanismo de reconhecimento de aplicativos NBAR2 suporta mais de 1000 aplicações de rede.
-

Visibilidade e controle do aplicativo (Contd.)



Application Recognition

Identifique aplicativos usando dados L3 a L7.

1000+ applications

- Cloud services
- Cisco WebEx
- YouTube
- Skype
- P2P

NBAR2



Metrics Collection

Coletar métricas para exportação para ferramenta de gerenciamento

Bandwidth usage

- Response time
- Latency
- Packet loss
- Jitter
- P2P

Netflow9 Flexible Netflow
IPFIX



Management and Reporting

Provisione a rede, colete dados e informe sobre o desempenho dos aplicativos

- Report generation
- Policy Management

Cisco Prime Other 3rd
Party Software



High: VoIP
Medium: Browsing
Low: Streaming
Blocked: P2P

Control

Controlar o uso do aplicativo para maximizar o desempenho da rede

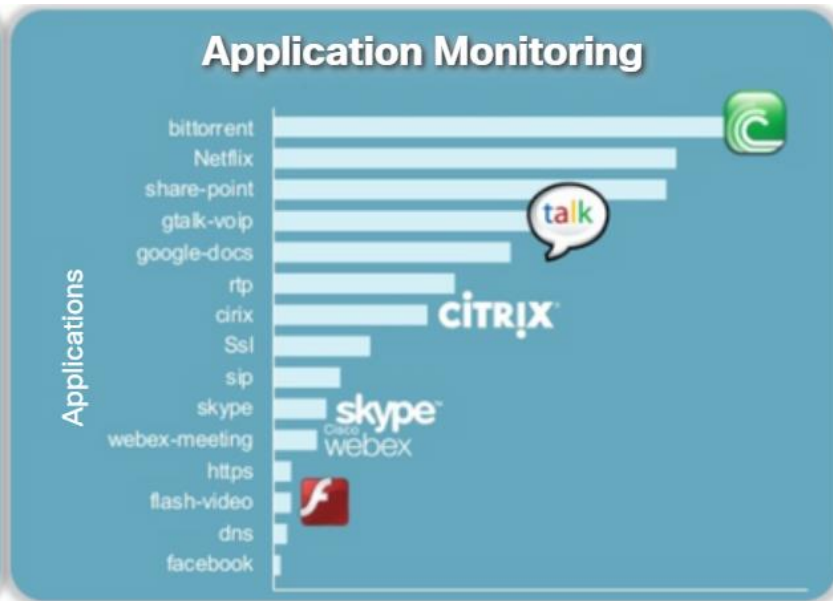
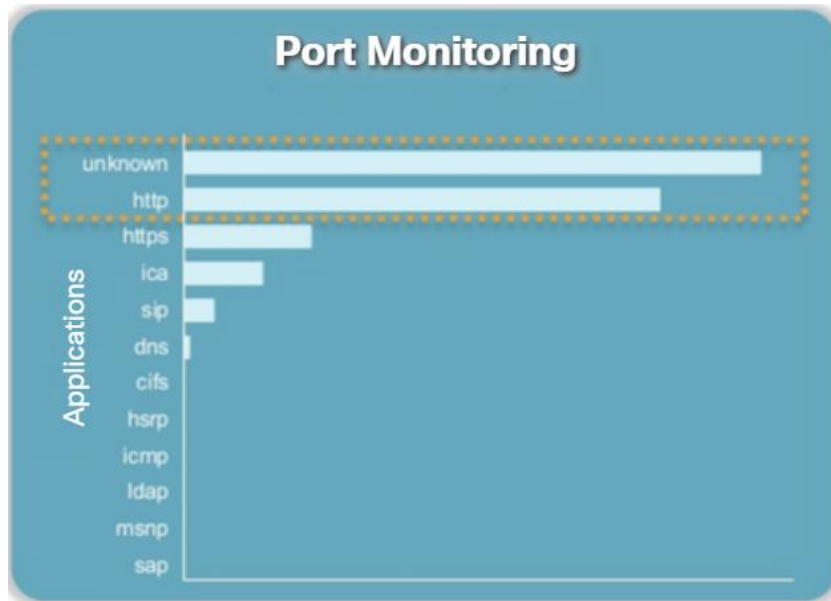
- Application prioritization
- Application bandwidth enforcement

QoS

Application Visibility and Control (Contd.)

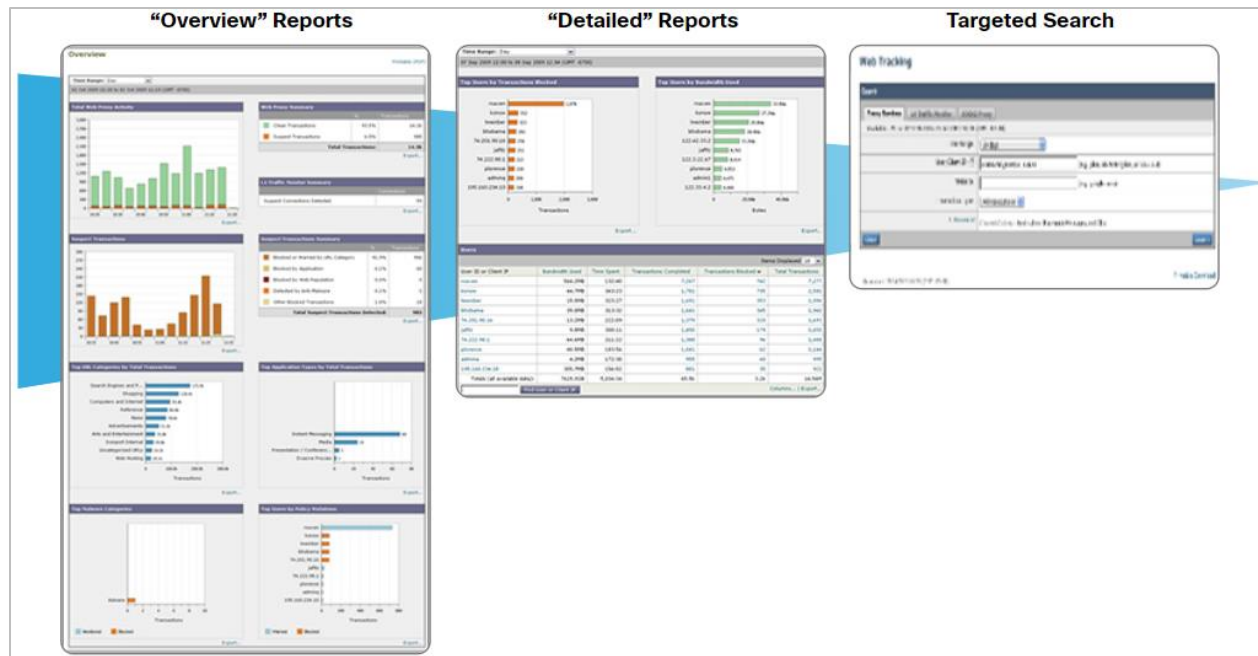
Port Monitoring vs. Application Monitoring

Um sistema de gerenciamento e relatórios analisa e apresenta os dados de análise do aplicativo em relatórios de painel para uso por pessoal de monitoramento de rede. O uso de aplicativos também pode ser controlado através da qualidade da classificação do serviço e políticas com base nas informações de AVC.



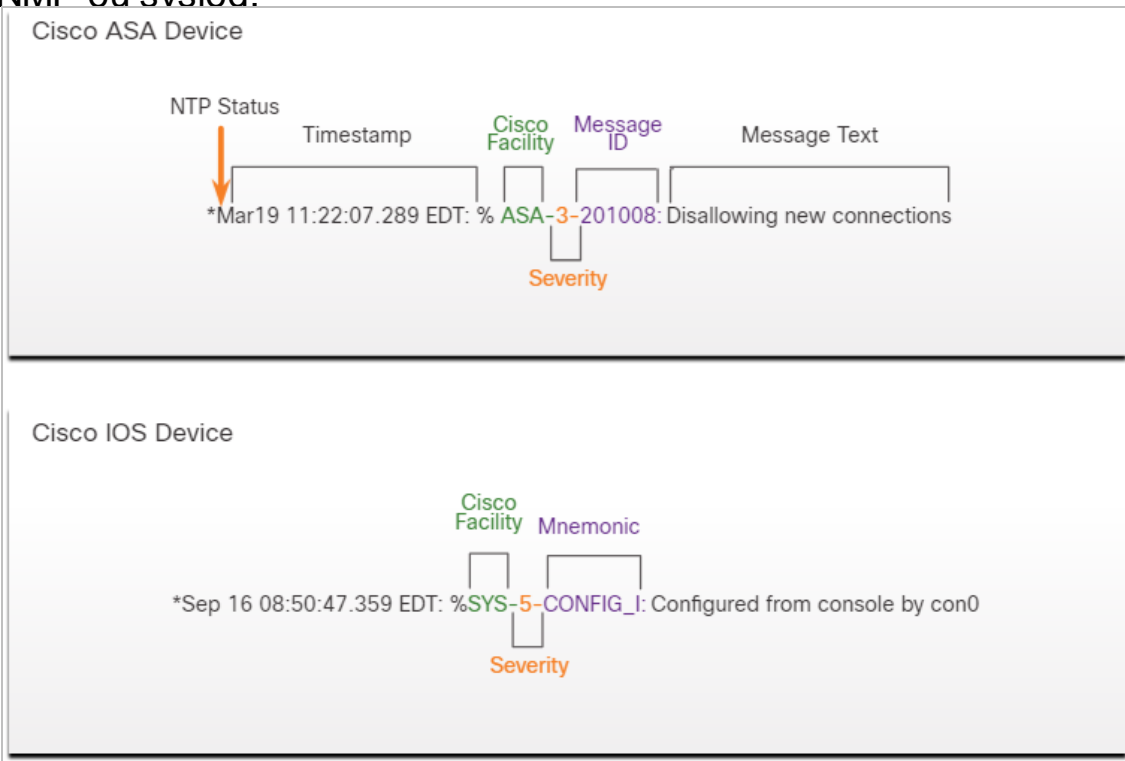
Content Filter Logs

- 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 segurança monitorização.
- A figura mostra os painéis dos dispositivos de filtragem de conteúdo cisco. Ao clicar em componentes dos relatórios de visão geral, são exibidos detalhes mais relevantes. As buscas de alvo fornecem as informações focadas.



Logging from Cisco Devices

- Os dispositivos de segurança Cisco podem ser configurados para enviar eventos e alertas para plataformas de gerenciamento de segurança usando SNMP ou svslog.
- A figura mostra uma mensagem de syslog gerada por um dispositivo Cisco ASA e uma mensagem de syslog gerada por um dispositivo Cisco IOS.
- Existem dois significados usados para a instalação de termo em mensagens syslog Cisco.
- O primeiro é o conjunto padrão de valores de facilidade que foram estabelecidos pelas normas de syslog.
- O outro valor de Instalação é atribuído pela Cisco e ocorre na parte MSG da mensagem syslog.



Proxy Logs

- 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.
- O servidor proxy solicita os recursos e os devolve ao cliente e gera registros de todas as solicitações e respostas.
- Esses logs podem então 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 Explora.
- Também é possível usar proxies web para inspecionar o tráfego de saída como meio de prevenção de perda de dados (DLP).
- O DLP envolve digitalizar o tráfego de saída para detectar se os dados que estão saindo da web contêm informações confidenciais, confidenciais ou secretas.

Proxy Logs (Contd.)

Cisco Umbrella

A Cisco Umbrella, anteriormente OpenDNS, oferece um serviço de DNS hospedado que amplia a capacidade do DNS para incluir melhorias de segurança.

A Cisco Umbrella aplica muito mais recursos para gerenciar DNS do que a maioria das organizações pode pagar. Cisco Umbrella funciona em parte como um super proxy DNS a este respeito.

O conjunto de produtos de segurança Cisco Umbrella aplica inteligência de ameaça em tempo real para gerenciar o acesso ao DNS e a segurança dos registros de DNS.

Um exemplo de um log proxy DNS aparece abaixo.

```
"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"
```


Next-Generation Firewalls

- Os dispositivos de firewall de próxima geração ou NextGen estendem a segurança da rede além de endereços IP e números de porta da Camada 4 para a camada de aplicativo e além.
- NexGen Firewalls são dispositivos avançados que forneceram muito mais funcionalidade do que as gerações anteriores de dispositivos de segurança de rede.
- Uma funcionalidade é relatar painéis com recursos interativos que permitem relatórios rápidos de ponto e clique em informações muito específicas sem a necessidade de SIEM ou outros correlatores de eventos.
- Os dispositivos NextGen Firewall (NGFW) usam o Firepower Services para consolidar várias camadas de segurança em uma única plataforma.
- Os serviços de poder de fogo incluem visibilidade e controle de aplicativos, IPS de última geração do Firepower (NGIPS), filtragem de URL baseada em reputação e categoria e PROTEÇÃO avançada de malware (AMP).
-

Next-Generation Firewalls (Contd.)

Os eventos comuns do NGFW

incluem:

Evento de conexão

Evento de intrusão

Evento de hospedagem ou
endpoint

Evento de detecção de rede

Evento de fluxo líquido

Services Provided by NGFW



Packet Tracer - Explore a NetFlow Implementation

Nesta atividade do Rastreador de pacotes, você fará o seguinte:
Explorar uma implementação do NetFlow.

Packet Tracer - Logging from Multiple Sources

Nesta atividade do Rastreador de pacotes, você fará o seguinte:

Use o Packet Tracer para comparar dados de rede gerados por várias fontes, incluindo syslog, AAA e NetFlow.

25.4 Resumo de dados de segurança de rede

What Did I Learn in this Module?

- 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 ao assinatura de uma exploração conhecida.
- Dentro do conjunto de ferramentas NSM da Security Onion, os alertas são gerados pelo Snort e são legíveis e pesquisáveis pelos aplicativos Sguil, Squert e Kibana.
- Os dados da sessão incluirão a identificação de informações como as cinco tuplas de endereços IP de origem e destino, números de porta de origem e destino e o código IP para o protocolo em uso.
- Os dados sobre a sessão geralmente incluem um ID de sessão, a quantidade de dados transferidos por fonte e destino e informações relacionadas à duração da sessão.
- As capturas completas de pacotes contêm o conteúdo real das conversas de dados, como o texto das mensagens de e-mail, o HTML em páginas da Web e os arquivos que entram ou saem da rede.
- Os dados estatísticos são criados através da análise de várias formas de dados de rede.

What Did I Learn in this Module? (Contd.)

- Os sistemas de detecção de intrusão baseados em host (HIDS) são executados em hosts individuais.
- O Syslog incude especificações para formatos de mensagens, uma estrutura de aplicativos cliente-servidor e protocolo de rede.
- Os registros de servidores são uma fonte essencial de dados para monitoramento de segurança de rede.
- Os registros do servidor proxy DNS documentam todas as consultas e respostas do DNS que ocorrem na rede.
- Os registros de proxy DNS são úteis para identificar hosts que podem ter visitado sites perigosos e para identificar exfiltração de dados DNS e conexões para servidores de comando e controle de malware.
- O SIEM combina as funções essenciais das ferramentas de gerenciamento de eventos de segurança (SEM) e de gerenciamento de informações de segurança (SIM) para fornecer uma visão abrangente da rede corporativa usando o log coleta, normalização, correlação, agregação, emissão de relatórios e conformidade.

What Did I Learn in this Module? (Contd.)

- 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.
- O NetFlow fornece informações valiosas sobre usuários de rede e aplicativos, horários de pico de uso e roteamento de tráfego.
- A Visibilidade e Controle de Aplicativos Cisco usa a versão 2 de reconhecimento de aplicativos baseada em rede cisco na próxima geração (NBAR2), também conhecida como NBAR de última geração.
- 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 conteúdo filtragem.
- Servidores proxy são dispositivos que atuam como intermediários para clientes de rede.
- Os dispositivos NextGen Firewall estendem a segurança da rede além dos endereços IP e dos números de porta da Camada 4 para a camada de aplicativo e além.

