了解旧版数据结构

本附录包含之前版本的 Firepower 系统产品中受 eStreamer 支持的数据结构的相关信息。

如果您的客户端使用事件流请求并对比特位进行设置，以请求采用较旧版本格式的数据，您可以使用此附录中的信息识别您收到的数据消息的数据结构。

请注意，在版本 5.0 之前的版本中， ID 分配给单独的检测引擎。对于版本 5.0， ID 分配给设备。根据版本，数据结构可反映这一点。

注 此附录仅描述 Firepower 系统版本 4.9 及更高版本的数据结构。如果您需要有关较早数据结构版本的结构的文件，请联系 Cisco 客户支持。

有关详细信息，请参阅以下各节：

旧版入侵数据结构

入侵事件 (IPv4) 记录 5.0.x - 5.1

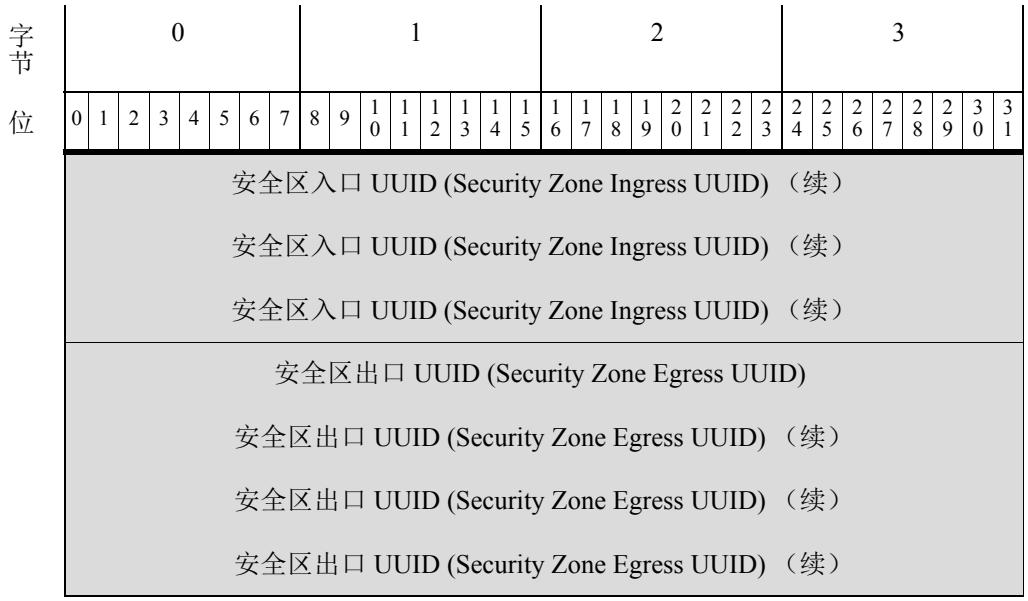
下图中的阴影部分表示入侵事件 (IPv4) 记录中的字段。记录类型为 207。

通过在请求消息中设置入侵事件标志或扩展请求标志可请求入侵事件记录。请参阅请求标志，第 2-11 页和提交扩展请求，第 2-4 页。

对于版本 5.0.x - 5.1 入侵事件，事件 ID、受管设备 ID 以及事件秒构成唯一标识符。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (207) （Record Type (207))															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp) （在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use) （在事件中，只有当位 23 已设置时）																																
设备 ID (Device ID)																																
事件 ID (Event ID)																																
事件秒 (Event Second)																																
事件微秒 (Event Microsecond)																																
规则 ID （签名 ID） (Rule ID (Signature ID))																																
生成器 ID (Generator ID)																																
规则修订 (Rule Revision)																																
分类 ID (Classification ID)																																
优先级 ID (Priority ID)																																
源 IPv4 地址																																
目的 IPv4 地址																																
源端口 (Source Port)																	目标端口 (Destination Port)															
IP 协议 ID (IP Protocol ID)									影响标志 (Impact Flags)								影响 (Impact)								已阻止 (Blocked)							

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
MPLS 标签 (MPLS Label)																																
VLAN ID																	Pad															
策略 UUID (Policy UUID)																																
策略 UUID (Policy UUID) （续）																																
策略 UUID (Policy UUID) （续）																																
策略 UUID (Policy UUID) （续）																																
用户 ID (User ID)																																
Web 应用 ID (Web Application ID)																																
客户端应用 ID (Client Application ID)																																
应用协议 ID (Application Protocol ID)																																
访问控制规则 ID (Access Control Rule ID)																																
访问控制策略 UUID (Access Control Policy UUID)																																
访问控制策略 UUID (Access Control Policy UUID) （续）																																
访问控制策略 UUID (Access Control Policy UUID) （续）																																
访问控制策略 UUID (Access Control Policy UUID) （续）																																
接口入口 UUID (Interface Ingress UUID)																																
接口入口 UUID (Interface Ingress UUID) （续）																																
接口入口 UUID (Interface Ingress UUID) （续）																																
接口入口 UUID (Interface Ingress UUID) （续）																																
接口出口 UUID (Interface Egress UUID)																																
接口出口 UUID (Interface Egress UUID) （续）																																
接口出口 UUID (Interface Egress UUID) （续）																																
接口出口 UUID (Interface Egress UUID) （续）																																
安全区入口 UUID (Security Zone Ingress UUID)																																



下表对每个入侵事件记录数据字段进行了说明。

表 B-1　　入侵事件 (IPv4) 记录字段

字段	数据类型	说明
设备 ID (Device ID)	unit32	包含检测受管设备的标识号。您可以通过请求版本 3 或 4 元数据获取受管设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
事件 ID (Event ID)	uint32	事件标识号。
事件秒 (Event Second)	uint32	事件检测的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）
事件微秒 (Event Microsecond)	uint32	事件检测的时间戳微秒 （一秒的百万分之一）增量。
规则 ID （签名 ID） (Rule ID (Signature ID))	uint32	与事件对应的规则标识号。
生成器 ID (Generator ID)	uint32	生成事件的 Firepower 系统预处理器的标识号。
规则修订 (Rule Revision)	uint32	规则版本号。
分类 ID (Classification ID)	uint32	事件分类消息的标识号。
优先级 ID (Priority ID)	uint32	与事件相关的优先级的标识号。
源 IPv4 地址 (Source IPv4 Address)	uint8[4]	事件中使用的源 IPv4 地址，采用地址八位组。

表 B-1　　入侵事件 (IPv4) 记录字段 （续）

字段	数据类型	说明
目标 IPv4 地址 (Destination IPv4 Address)	uint8[4]	事件中使用的目标 IPv4 地址，采用地址八位组。
源端口 (Source Port)	uint16	如果事件协议类型是 TCP 或 UDP，则为源端口号。
目标端口 (Destination Port)	uint16	如果事件协议类型是 TCP 或 UDP，则为目标端口号。
IP 协议号 (IP Protocol Number)	uint8	IANA 指定的协议号。例如： • 0 - IP • 1 - ICMP • 6 - TCP • 17 - UDP
影响标志 (Impact Flags)	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括： • 0x01 （位 0） - 源或目标主机位于系统监控的网络中。 • 0x02 （位 1） - 源或目标主机存在于网络映射中。 • 0x04 （位 2） - 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使 用 IP 协议。 • 0x08 （位 3） - 有漏洞映射到事件中的源或目标主机的操作系统。 • 0x10 （位 4） - 有漏洞映射到事件中检测到的服务器。 • 0x20 （位 5） - 事件导致受管设备丢弃会话 （仅当设备在内联、交换或路由式部署中运行时才使用）。对应于 Firepower 系统 Web 界面中的受阻状态。 • 0x40 （位 6） - 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 • 0x80 （位 7） - 有漏洞映射到事件中检测到的客户端。 以下影响级别值映射到 “ 防御中心 ”(Defense Center) 上的特定优先级中。 x 表示值可以为 0 或 1： • （0，未知）：00X00000 • 红色 （1，易受攻击）：XXXX1XXX、XXX1XXXX、X1XXXXXX、1XXXXXXX • 橙色 （2，可能易受攻击）：00X00111 • 黄色 （3，当前不易受攻击）：00X00011 • 蓝色 （4，未知目标）：00X00001

表 B-1 入侵事件 (IPv4) 记录字段 （续）

字段	数据类型	说明
影响 (Impact)	uint8	事件的影响标志值。其值如下： • 1 - 红色 （易受攻击） • 2 - 橙色 （可能易受攻击） • 3 - 黄色 （目前不易受攻击） • 4 - 蓝色 （未知目标） • 5 - （未知影响）
已阻止 (Blocked)	uint8	表示事件是否已被阻止的值。 • 0 - 未被阻止 • 1 - 已阻止 • 2 - 将被阻止 （但配置不允许）
MPLS 标签 (MPLS Label)	uint32	MPLS 标签。
VLAN ID	uint16	表示数据包起源的 VLAN 的 ID。
Pad	uint16	已保留供将来使用。
策略 UUID (Policy UUID)	uint8[16]	充当入侵策略的唯一标识符的策略 ID 号码。
用户 ID (User ID)	uint32	用户的内部标识号 （如适用）。
Web 应用 ID (Web Application ID)	uint32	Web 应用 （如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用 （如适用）的内部标别号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号 （如适用）。
访问控制规则 ID (Access Control Rule ID)	uint32	充当访问控制规则的唯一标识符的规则 ID 号码。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	充当访问控制策略的唯一标识符的策略 ID 号码。
入口接口 UUID (Ingress Interface UUID)	uint8[16]	充当入口接口的唯一标识符的接口 ID 号码。
出口接口 UUID (Egress Interface UUID)	uint8[16]	充当出口接口的唯一标识符的接口 ID 号码。

表 B-1　　入侵事件 (IPv4) 记录字段 （续）

字段	数据类型	说明
入口安全区 UUID (Ingress Security Zone UUID)	uint8[16]	充当入口安全区的唯一标识符的区域 ID 号码。
出口安全区 UUID (Egress Security Zone UUID)	uint8[16]	充当出口安全区的唯一标识符的区域 ID 号码。

入侵事件 (IPv6) 记录 5.0.x - 5.1

下图中的阴影部分表示入侵事件 (IPv6) 记录中的字段。记录类型为 208。

通过在请求消息中设置入侵事件标志或扩展请求标志可请求入侵事件记录。请参阅请求标志，第 2-11 页和提交扩展请求，第 2-4 页。

对于版本 5.0.x - 5.1 入侵事件，事件 ID、受管设备 ID 以及事件秒构成唯一标识符。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (208) （Record Type (208))															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp) （在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use) （在事件中，只有当位 23 已设置时）																																
设备 ID (Device ID)																																
事件 ID (Event ID)																																
事件秒 (Event Second)																																
事件微秒 (Event Microsecond)																																
规则 ID （签名 ID） (Rule ID (Signature ID))																																
生成器 ID (Generator ID)																																
规则修订 (Rule Revision)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
分类 ID (Classification ID)																																
优先级 ID (Priority ID)																																
源 IPv6 地址 (Source IPv6 Address) 源 IPv6 地址 (Source IPv6 Address) （续） 源 IPv6 地址 (Source IPv6 Address) （续） 源 IPv6 地址 (Source IPv6 Address) （续）																																
目的 IPv6 地址 (Destination IPv6 Address) 目标 IPv6 地址 (Destination IPv6 Address) （续） 目标 IPv6 地址 (Destination IPv6 Address) （续） 目标 IPv6 地址 (Destination IPv6 Address) （续）																																
源端口 /ICMP 类型 (Source Port/ICMP Type)																	目标端口 /ICMP 代码 (Destination Port/ICMP Code)														
IP 协议 ID (IP Protocol ID)									影响标志 (Impact Flags)								影响 (Impact)								已阻止 (Blocked)							
MPLS 标签 (MPLS Label)																																
VLAN ID																	Pad															
策略 UUID (Policy UUID) 策略 UUID (Policy UUID) （续） 策略 UUID (Policy UUID) （续） 策略 UUID (Policy UUID) （续）																																
用户 ID (User ID)																																
Web 应用 ID (Web Application ID)																																
客户端应用 ID (Client Application ID)																																
应用协议 ID (Application Protocol ID)																																
访问控制规则 ID (Access Control Rule ID)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
访问控制策略 UUID (Access Control Policy UUID)																																
访问控制策略 UUID (Access Control Policy UUID) （续）																																
访问控制策略 UUID (Access Control Policy UUID) （续）																																
访问控制策略 UUID (Access Control Policy UUID) （续）																																
接口入口 UUID (Interface Ingress UUID)																																
接口入口 UUID (Interface Ingress UUID) （续）																																
接口入口 UUID (Interface Ingress UUID) （续）																																
接口入口 UUID (Interface Ingress UUID) （续）																																
接口出口 UUID (Interface Egress UUID)																																
接口出口 UUID (Interface Egress UUID) （续）																																
接口出口 UUID (Interface Egress UUID) （续）																																
接口出口 UUID (Interface Egress UUID) （续）																																
安全区入口 UUID (Security Zone Ingress UUID)																																
安全区入口 UUID (Security Zone Ingress UUID) （续）																																
安全区入口 UUID (Security Zone Ingress UUID) （续）																																
安全区入口 UUID (Security Zone Ingress UUID) （续）																																
安全区出口 UUID (Security Zone Egress UUID)																																
安全区出口 UUID (Security Zone Egress UUID) （续）																																
安全区出口 UUID (Security Zone Egress UUID) （续）																																
安全区出口 UUID (Security Zone Egress UUID) （续）																																

下表对每个入侵事件记录数据字段进行了说明。

表 B-2 入侵事件 (IPv6) 记录字段

字段	数据类型	说明
设备 ID (Device ID)	unit32	包含检测设备的标识号。您可以通过请求版本 3 或 4 元数据获取受管设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
事件 ID (Event ID)	uint32	事件标识号。
事件秒 (Event Second)	uint32	事件检测的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）
事件微秒 (Event Microsecond)	uint32	事件检测的时间戳微秒 （一秒的百万分之一）增量。
规则 ID （签名 ID） (Rule ID (Signature ID))	uint32	与事件对应的规则标识号。
生成器 ID (Generator ID)	uint32	生成事件的 Firepower 系统预处理器的标识号。
规则修订 (Rule Revision)	uint32	规则版本号。
分类 ID (Classification ID)	uint32	事件分类消息的标识号。
优先级 ID (Priority ID)	uint32	与事件相关的优先级的标识号。
源 IPv6 地址 (Source IPv6 Address)	uint8[16]	事件中使用的源 IPv6 地址，采用地址八位组。
目标 IPv6 地址 (Destination IPv6 Address)	uint8[16]	事件中使用的目标 IPv6 地址，采用地址八位组。
源端口 /ICMP 类型 (Source Port/ICMP Type)	uint16	如果事件协议类型是 TCP 或 UDP，则为源端口号。如果协议类型为 ICMP，则这表示 ICMP 类型。
目标端口 /ICMP 代码 (Destination Port/ICMP Code)	uint16	如果事件协议类型是 TCP 或 UDP，则为目标端口号。如果协议类型为 ICMP，则这表示 ICMP 代码。
IP 协议号 (IP Protocol Number)	uint8	IANA 指定的协议号。例如： • 0 - IP • 1 - ICMP • 6 - TCP • 17 - UDP

表 B-2　　入侵事件 (IPv6) 记录字段 （续）

字段	数据类型	说明
影响标志 (Impact Flags)	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括： • 0x01 （位 0） - 源或目标主机位于系统监控的网络中。 • 0x02 （位 1） - 源或目标主机存在于网络映射中。 • 0x04 （位 2） - 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使 用 IP 协议。 • 0x08 （位 3） - 有漏洞映射到事件中的源或目标主机的操作系统。 • 0x10 （位 4） - 有漏洞映射到事件中检测到的服务器。 • 0x20 （位 5） - 事件导致受管设备丢弃会话 （仅当设备在内联、交换或路由式部署中运行时才使用）。对应于 Firepower 系统 Web 界面中的受阻状态。 • 0x40 （位 6） - 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 • 0x80 （位 7） - 有漏洞映射到事件中检测到的客户端。 以下影响级别值映射到 “ 防御中心 ”(Defense Center) 上的特定优先级中。 x 表示值可以为 0 或 1： • （0，未知）：00X00000 • 红色 （1，易受攻击）：XXXX1XXX、XXX1XXXX、X1XXXXXX、1XXXXXXX • 橙色 （2，可能易受攻击）：00X00111 • 黄色 （3，当前不易受攻击）：00X00011 • 蓝色 （4，未知目标）：00X00001
影响 (Impact)	uint8	事件的影响标志值。其值如下： • 1 - 红色 （易受攻击） • 2 - 橙色 （可能易受攻击） • 3 - 黄色 （目前不易受攻击） • 4 - 蓝色 （未知目标） • 5 - （未知影响）
已阻止 (Blocked)	uint8	表示事件是否已被阻止的值。 • 0 - 未被阻止 • 1 - 已阻止 • 2 - 将被阻止 （但配置不允许）
MPLS 标签 (MPLS Label)	uint32	MPLS 标签。（仅适用于 4.9+ 事件。）
VLAN ID	uint16	表示数据包起源的 VLAN 的 ID。（仅适用于 4.9+ 事件。）
Pad	uint16	已保留供将来使用。
策略 UUID (Policy UUID)	uint8[16]	充当入侵策略的唯一标识符的策略 ID 号码。

表 B-2 入侵事件 (IPv6) 记录字段 （续）

字段	数据类型	说明
用户 ID (User ID)	uint32	用户的内部标识号 （如适用）。
Web 应用 ID (Web Application ID)	uint32	Web 应用 （如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用 （如适用）的内部标别号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号 （如适用）。
访问控制规则 ID (Access Control Rule ID)	uint32	充当访问控制规则的唯一标识符的规则 ID 号码。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	充当访问控制策略的唯一标识符的策略 ID 号码。
入口接口 UUID (Ingress Interface UUID)	uint8[16]	充当入口接口的唯一标识符的接口 ID 号码。
出口接口 UUID (Egress Interface UUID)	uint8[16]	充当出口接口的唯一标识符的接口 ID 号码。
入口安全区 UUID (Ingress Security Zone UUID)	uint8[16]	充当入口安全区的唯一标识符的区域 ID 号码。
出口安全区 UUID (Egress Security Zone UUID)	uint8[16]	充当出口安全区的唯一标识符的区域 ID 号码。

入侵事件记录 5.2.x

下图中的阴影部分表示入侵事件记录中的字段。在系列 2 数据块组中，记录类型为 400，块类型为 34。

您可以通过扩展请求，仅从 eStreamer 请求 5.2.x 入侵事件，为此，您需要在流请求消息中请求事件类型代码 12 和版本代码 5 （有关提交扩展请求的信息，请参阅提交扩展请求，第 2-4 页）。

对于版本 5.2.x 入侵事件，事件 ID、受管设备 ID 以及事件秒构成唯一标识符。连接秒、连接实例以及连接计数器在一起构成与入侵事件相关的连接事件的唯一标识符。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (400) (Record Type (400))															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp) （在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use) （在事件中，只有当位 23 已设置时）																																
块类型 (34) (Block Type (34))																																
块长度 (Block Length)																																
设备 ID (Device ID)																																
事件 ID (Event ID)																																
事件秒 (Event Second)																																
事件微秒 (Event Microsecond)																																
规则 ID （签名 ID） (Rule ID (Signature ID))																																
生成器 ID (Generator ID)																																
规则修订 (Rule Revision)																																
分类 ID (Classification ID)																																
优先级 ID (Priority ID)																																
源 IP 地址 (Source IP Address)																																
源 IP 地址 (Source IP Address) （续）																																
源 IP 地址 (Source IP Address) （续）																																
源 IP 地址 (Source IP Address) （续）																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
目标 IP 地址 (Destination IP Address)																																
目标 IP 地址 (Destination IP Address) （续）																																
目标 IP 地址 (Destination IP Address) （续）																																
目标 IP 地址 (Destination IP Address) （续）																																
源端口或 ICMP 类型 (Source Port or ICMP Type)																	目标端口或 ICMP 代码 (Destination Port or ICMP Code)														
IP 协议 ID (IP Protocol ID)									影响标志 (Impact Flags)								影响 (Impact)								已阻止 (Blocked)							
MPLS 标签 (MPLS Label)																																
VLAN ID																	Pad															
策略 UUID (Policy UUID)																																
策略 UUID (Policy UUID) （续）																																
策略 UUID (Policy UUID) （续）																																
策略 UUID (Policy UUID) （续）																																
用户 ID (User ID)																																
Web 应用 ID (Web Application ID)																																
客户端应用 ID (Client Application ID)																																
应用协议 ID (Application Protocol ID)																																
访问控制规则 ID (Access Control Rule ID)																																
访问控制策略 UUID (Access Control Policy UUID)																																
访问控制策略 UUID (Access Control Policy UUID) （续）																																
访问控制策略 UUID (Access Control Policy UUID) （续）																																
访问控制策略 UUID (Access Control Policy UUID) （续）																																
接口入口 UUID (Interface Ingress UUID)																																
接口入口 UUID (Interface Ingress UUID) （续）																																
接口入口 UUID (Interface Ingress UUID) （续）																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
接口入口 UUID (Interface Ingress UUID) （续）																																
接口出口 UUID (Interface Egress UUID)																																
接口出口 UUID (Interface Egress UUID) （续）																																
接口出口 UUID (Interface Egress UUID) （续）																																
接口出口 UUID (Interface Egress UUID) （续）																																
安全区入口 UUID (Security Zone Ingress UUID)																																
安全区入口 UUID (Security Zone Ingress UUID) （续）																																
安全区入口 UUID (Security Zone Ingress UUID) （续）																																
安全区入口 UUID (Security Zone Ingress UUID) （续）																																
安全区出口 UUID (Security Zone Egress UUID)																																
安全区出口 UUID (Security Zone Egress UUID) （续）																																
安全区出口 UUID (Security Zone Egress UUID) （续）																																
安全区出口 UUID (Security Zone Egress UUID) （续）																																
连接时间戳 (Connection Timestamp)																																
连接实例 ID (Connection Instance ID)																	连接计数器 (Connection Counter)															
源国家 / 地区 (Source Country)																	目标国家 / 地区 (Destination Country)															

下表对每个入侵事件记录数据字段进行了说明。

表 B-3　　入侵事件记录 5.2.x 字段

字段	数据类型	说明
块类型 (Block Type)	unint32	启动入侵事件数据块。值始终为 34。
块长度 (Block Length)	unint32	入侵事件数据块中的字节总数，包括入侵事件块类型和长度字段的八个字节，加上随后的数据字节数。
设备 ID (Device ID)	unit32	包含检测受管设备的标识号。您可以通过请求版本 3 或 4 元数据获取受管设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
事件 ID (Event ID)	uint32	事件标识号。

表 B-3 入侵事件记录 5.2.x 字段 （续）

字段	数据类型	说明
事件秒 (Event Second)	uint32	事件检测的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）
事件微秒 (Event Microsecond)	uint32	事件检测的时间戳微秒 （一秒的百万分之一）增量。
规则 ID （签名 ID） (Rule ID (Signature ID))	uint32	与事件对应的规则标识号。
生成器 ID (Generator ID)	uint32	生成事件的 Firepower 系统预处理器的标识号。
规则修订 (Rule Revision)	uint32	规则版本号。
分类 ID (Classification ID)	uint32	事件分类消息的标识号。
优先级 ID (Priority ID)	uint32	与事件相关的优先级的标识号。
源 IP 地址 (Source IP Address)	uint8[16]	事件中使用的源 IPv4 或 IPv6 地址。
目标 IP 地址 (Destination IP Address)	uint8[16]	事件中使用的目标 IPv4 或 IPv6 地址。
源端口或 ICMP 类型 (Source Port or ICMP Type)	uint16	如果事件协议类型是 TCP 或 UDP，则为源端口号，或者如果事件是由 ICMP 流量引起的，则为 ICMP 类型。
目标端口或 ICMP 代码 (Destination Port or ICMP Code)	uint16	如果事件协议类型是 TCP 或 UDP，则为目标端口号，或者如果事件是由 ICMP 流量引起的，则为 ICMP 代码。
IP 协议号 (IP Protocol Number)	uint8	IANA 指定的协议号。例如： • 0 - IP • 1 - ICMP • 6 - TCP • 17 - UDP

表 B-3　　入侵事件记录 5.2.x 字段 （续）

字段	数据类型	说明
影响标志 (Impact Flags)	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括： • 0x01 （位 0） - 源或目标主机位于系统监控的网络中。 • 0x02 （位 1） - 源或目标主机存在于网络映射中。 • 0x04 （位 2） - 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使 用 IP 协议。 • 0x08 （位 3） - 有漏洞映射到事件中的源或目标主机的操作系统。 • 0x10 （位 4） - 有漏洞映射到事件中检测到的服务器。 • 0x20 （位 5） - 事件导致受管设备丢弃会话 （仅当设备在内联、交换或路由式部署中运行时才使用）。对应于 Firepower 系统 Web 界面中的受阻状态。 • 0x40 （位 6） - 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 • 0x80 （位 7） - 有漏洞映射到事件中检测到的客户端。（仅限版本 5.0+） 以下影响级别值映射到 “ 防御中心 ”(Defense Center) 上的特定优先级中。x 表示值可以为 0 或 1： • （0，未知）：00X00000 • 红色 （1，易受攻击）：XXXX1XXX、XXX1XXXX、X1XXXXXX、1XXXXXXX （仅限版本 5.0+） • 橙色 （2，可能易受攻击）：00X0011X • 黄色 （3，当前不易受攻击）：00X0001X • 蓝色 （4，未知目标）：00X00001
影响 (Impact)	uint8	事件的影响标志值。其值如下： • 1 - 红色 （易受攻击） • 2 - 橙色 （可能易受攻击） • 3 - 黄色 （目前不易受攻击） • 4 - 蓝色 （未知目标） • 5 - （未知影响）
已阻止 (Blocked)	uint8	表示事件是否已被阻止的值。 • 0 - 未被阻止 • 1 - 已阻止 • 2 - 将被阻止 （但配置不允许）
MPLS 标签 (MPLS Label)	uint32	MPLS 标签。
VLAN ID	uint16	表示数据包起源的 VLAN 的 ID。
Pad	uint16	已保留供将来使用。

表 B-3 入侵事件记录 5.2.x 字段 （续）

字段	数据类型	说明
策略 UUID (Policy UUID)	uint8[16]	充当入侵策略的唯一标识符的策略 ID 号码。
用户 ID (User ID)	uint32	用户的内部标识号 （如适用）。
Web 应用 ID (Web Application ID)	uint32	Web 应用 （如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用 （如适用）的内部标别号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号 （如适用）。
访问控制规则 ID (Access Control Rule ID)	uint32	充当访问控制规则的唯一标识符的规则 ID 号码。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	充当访问控制策略的唯一标识符的策略 ID 号码。
入口接口 UUID (Ingress Interface UUID)	uint8[16]	充当入口接口的唯一标识符的接口 ID 号码。
出口接口 UUID (Egress Interface UUID)	uint8[16]	充当出口接口的唯一标识符的接口 ID 号码。
入口安全区 UUID (Ingress Security Zone UUID)	uint8[16]	充当入口安全区的唯一标识符的区域 ID 号码。
出口安全区 UUID (Egress Security Zone UUID)	uint8[16]	充当出口安全区的唯一标识符的区域 ID 号码。
连接时间戳 (Connection Timestamp)	uint32	与入侵事件关联的连接事件的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）。
连接实例 ID (Connection Instance ID)	uint16	生成连接事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
源国家 / 地区 (Source Country)	uint16	源主机的国家 / 地区代码。
目标国家 / 地区 (Destination Country)	uint 16	目标主机的国家 / 地区代码。

入侵事件记录 5.3

下图中的阴影部分表示入侵事件记录中的字段。在系列 2 数据块组中，记录类型为 400，块类型为 41。

您可以通过扩展请求，仅从 eStreamer 请求 5.3 入侵事件，为此，您需要在流请求消息中请求事件类型代码 12 和版本代码 6（有关提交扩展请求的信息，请参阅提交扩展请求，第 2-4 页）。

对于版本 5.3 入侵事件，事件 ID、受管设备 ID 以及事件秒构成唯一标识符。连接秒、连接实例以及连接计数器在一起构成与入侵事件相关的连接事件的唯一标识符。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (400) (Record Type (400))															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp) （在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use)（在事件中，只有当位 23 已设置时）																																
块类型 (41) (Block Type (41))																																
块长度 (Block Length)																																
设备 ID (Device ID)																																
事件 ID (Event ID)																																
事件秒 (Event Second)																																
事件微秒 (Event Microsecond)																																
规则 ID（签名 ID） (Rule ID (Signature ID))																																
生成器 ID (Generator ID)																																
规则修订 (Rule Revision)																																
分类 ID (Classification ID)																																
优先级 ID (Priority ID)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
源 IP 地址 (Source IP Address)																																
源 IP 地址 (Source IP Address) （续）																																
源 IP 地址 (Source IP Address) （续）																																
源 IP 地址 (Source IP Address) （续）																																
目标 IP 地址 (Destination IP Address)																																
目标 IP 地址 (Destination IP Address) （续）																																
目标 IP 地址 (Destination IP Address) （续）																																
目标 IP 地址 (Destination IP Address) （续）																																
源端口或 ICMP 类型 (Source Port or ICMP Type)																	目标端口或 ICMP 代码 (Destination Port or ICMP Code)														
IP 协议 ID (IP Protocol ID)									影响标志 (Impact Flags)								影响 (Impact)								已阻止 (Blocked)							
MPLS 标签 (MPLS Label)																																
VLAN ID																	Pad															
策略 UUID (Policy UUID)																																
策略 UUID (Policy UUID) （续）																																
策略 UUID (Policy UUID) （续）																																
策略 UUID (Policy UUID) （续）																																
用户 ID (User ID)																																
Web 应用 ID (Web Application ID)																																
客户端应用 ID (Client Application ID)																																
应用协议 ID (Application Protocol ID)																																
访问控制规则 ID (Access Control Rule ID)																																
访问控制策略 UUID (Access Control Policy UUID)																																
访问控制策略 UUID (Access Control Policy UUID) （续）																																
访问控制策略 UUID (Access Control Policy UUID) （续）																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
访问控制策略 UUID (Access Control Policy UUID) （续）																																
接口入口 UUID (Interface Ingress UUID)																																
接口入口 UUID (Interface Ingress UUID) （续）																																
接口入口 UUID (Interface Ingress UUID) （续）																																
接口入口 UUID (Interface Ingress UUID) （续）																																
接口出口 UUID (Interface Egress UUID)																																
接口出口 UUID (Interface Egress UUID) （续）																																
接口出口 UUID (Interface Egress UUID) （续）																																
接口出口 UUID (Interface Egress UUID) （续）																																
安全区入口 UUID (Security Zone Ingress UUID)																																
安全区入口 UUID (Security Zone Ingress UUID) （续）																																
安全区入口 UUID (Security Zone Ingress UUID) （续）																																
安全区入口 UUID (Security Zone Ingress UUID) （续）																																
安全区出口 UUID (Security Zone Egress UUID)																																
安全区出口 UUID (Security Zone Egress UUID) （续）																																
安全区出口 UUID (Security Zone Egress UUID) （续）																																
安全区出口 UUID (Security Zone Egress UUID) （续）																																
连接时间戳 (Connection Timestamp)																																
连接实例 ID (Connection Instance ID)																	连接计数器 (Connection Counter)														
源国家 / 地区 (Source Country)																	目标国家 / 地区 (Destination Country)														
IOC 编号 (IOC Number)																																

下表对每个入侵事件记录数据字段进行了说明。

表 B-4 入侵事件记录 5.3 字段

字段	数据类型	说明
块类型 (Block Type)	unint32	启动入侵事件数据块。值始终为 34。
块长度 (Block Length)	unint32	入侵事件数据块中的字节总数，包括入侵事件块类型和长度字段的八个字节，加上随后的数据字节数。
设备 ID (Device ID)	unit32	包含检测受管设备的标识号。您可以通过请求版本 3 或 4 元数据获取受管设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
事件 ID (Event ID)	uint32	事件标识号。
事件秒 (Event Second)	uint32	事件检测的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）
事件微秒 (Event Microsecond)	uint32	事件检测的时间戳微秒 （一秒的百万分之一）增量。
规则 ID （签名 ID） (Rule ID (Signature ID))	uint32	与事件对应的规则标识号。
生成器 ID (Generator ID)	uint32	生成事件的 Firepower 系统预处理器的标识号。
规则修订 (Rule Revision)	uint32	规则版本号。
分类 ID (Classification ID)	uint32	事件分类消息的标识号。
优先级 ID (Priority ID)	uint32	与事件相关的优先级的标识号。
源 IP 地址 (Source IP Address)	uint8[16]	事件中使用的源 IPv4 或 IPv6 地址。
目标 IP 地址 (Destination IP Address)	uint8[16]	事件中使用的目标 IPv4 或 IPv6 地址。
源端口或 ICMP 类型 (Source Port or ICMP Type)	uint16	如果事件协议类型是 TCP 或 UDP，则为源端口号，或者如果事件是由 ICMP 流量引起的，则为 ICMP 类型。
目标端口或 ICMP 代码 (Destination Port or ICMP Code)	uint16	如果事件协议类型是 TCP 或 UDP，则为目标端口号，或者如果事件是由 ICMP 流量引起的，则为 ICMP 代码。
IP 协议号 (IP Protocol Number)	uint8	IANA 指定的协议号。例如： • 0 - IP • 1 - ICMP • 6 - TCP • 17 - UDP

表 B-4　　入侵事件记录 5.3 字段 （续）

字段	数据类型	说明
影响标志 (Impact Flags)	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括： • 0x01 （位 0） - 源或目标主机位于系统监控的网络中。 • 0x02 （位 1） - 源或目标主机存在于网络映射中。 • 0x04 （位 2） - 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使 用 IP 协议。 • 0x08 （位 3） - 有漏洞映射到事件中的源或目标主机的操作系统。 • 0x10 （位 4） - 有漏洞映射到事件中检测到的服务器。 • 0x20 （位 5） - 事件导致受管设备丢弃会话 （仅当设备在内联、交换或路由式部署中运行时才使用）。对应于 Firepower 系统 Web 界面中的受阻状态。 • 0x40 （位 6） - 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 • 0x80 （位 7） - 有漏洞映射到事件中检测到的客户端。（仅限版本 5.0+） 以下影响级别值映射到 “ 防御中心 ”(Defense Center) 上的特定优先级中。 x 表示值可以为 0 或 1： • （0，未知）：00X00000 • 红色 （1，易受攻击）：XXXX1XXX、XXX1XXXX、X1XXXXXX、1XXXXXXX （仅限版本 5.0+） • 橙色 （2，可能易受攻击）：00X0011X • 黄色 （3，当前不易受攻击）：00X0001X • 蓝色 （4，未知目标）：00X00001
影响 (Impact)	uint8	事件的影响标志值。其值如下： • 1 - 红色 （易受攻击） • 2 - 橙色 （可能易受攻击） • 3 - 黄色 （目前不易受攻击） • 4 - 蓝色 （未知目标） • 5 - （未知影响）
已阻止 (Blocked)	uint8	表示事件是否已被阻止的值。 • 0 - 未被阻止 • 1 - 已阻止 • 2 - 将被阻止 （但配置不允许）
MPLS 标签 (MPLS Label)	uint32	MPLS 标签。
VLAN ID	uint16	表示数据包起源的 VLAN 的 ID。
Pad	uint16	已保留供将来使用。

表 B-4 入侵事件记录 5.3 字段 （续）

字段	数据类型	说明
策略 UUID (Policy UUID)	uint8[16]	充当入侵策略的唯一标识符的策略 ID 号码。
用户 ID (User ID)	uint32	用户的内部标识号 （如适用）。
Web 应用 ID (Web Application ID)	uint32	Web 应用 （如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用 （如适用）的内部标别号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号 （如适用）。
访问控制规则 ID (Access Control Rule ID)	uint32	充当访问控制规则的唯一标识符的规则 ID 号码。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	充当访问控制策略的唯一标识符的策略 ID 号码。
入口接口 UUID (Ingress Interface UUID)	uint8[16]	充当入口接口的唯一标识符的接口 ID 号码。
出口接口 UUID (Egress Interface UUID)	uint8[16]	充当出口接口的唯一标识符的接口 ID 号码。
入口安全区 UUID (Ingress Security Zone UUID)	uint8[16]	充当入口安全区的唯一标识符的区域 ID 号码。
出口安全区 UUID (Egress Security Zone UUID)	uint8[16]	充当出口安全区的唯一标识符的区域 ID 号码。
连接时间戳 (Connection Timestamp)	uint32	与入侵事件关联的连接事件的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）。
连接实例 ID (Connection Instance ID)	uint16	生成连接事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
源国家 / 地区 (Source Country)	uint16	源主机的国家 / 地区代码。
目标国家 / 地区 (Destination Country)	uint 16	目标主机的国家 / 地区代码。
IOC 编号 (IOC Number)	uint16	与此事件相关的危害的 ID 号码。

入侵事件记录 5.1.1.x

下图中的阴影部分表示入侵事件记录中的字段。记录类型为 400，块类型为 25。

您可以通过扩展请求，仅从 eStreamer 请求 5.1.1.x 入侵事件，为此，您需要在流请求消息中请求事件类型代码 12 和版本代码 4 （有关提交扩展请求的信息，请参阅提交扩展请求，第 2-4 页）。

对于版本 5.1.1.x 入侵事件，事件 ID、受管设备 ID 以及事件秒构成唯一标识符。连接秒、连接实例以及连接计数器在一起构成与入侵事件相关的连接事件的唯一标识符。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (400) (Record Type (400))															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp) （在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use) （在事件中，只有当位 23 已设置时）																																
块类型 (25) (Block Type (25))																																
块长度 (Block Length)																																
设备 ID (Device ID)																																
事件 ID (Event ID)																																
事件秒 (Event Second)																																
事件微秒 (Event Microsecond)																																
规则 ID （签名 ID） (Rule ID (Signature ID))																																
生成器 ID (Generator ID)																																
规则修订 (Rule Revision)																																
分类 ID (Classification ID)																																
优先级 ID (Priority ID)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
源 IP 地址 (Source IP Address)																																
源 IP 地址 (Source IP Address) （续）																																
源 IP 地址 (Source IP Address) （续）																																
源 IP 地址 (Source IP Address) （续）																																
目标 IP 地址 (Destination IP Address)																																
目标 IP 地址 (Destination IP Address) （续）																																
目标 IP 地址 (Destination IP Address) （续）																																
目标 IP 地址 (Destination IP Address) （续）																																
源端口 /ICMP 类型 (Source Port/ICMP Type)																	目标端口 /ICMP 代码 (Destination Port/ICMP Code)														
IP 协议 ID (IP Protocol ID)									影响标志 (Impact Flags)								影响 (Impact)								已阻止 (Blocked)							
MPLS 标签 (MPLS Label)																																
VLAN ID																	Pad															
策略 UUID (Policy UUID)																																
策略 UUID (Policy UUID) （续）																																
策略 UUID (Policy UUID) （续）																																
策略 UUID (Policy UUID) （续）																																
用户 ID (User ID)																																
Web 应用 ID (Web Application ID)																																
客户端应用 ID (Client Application ID)																																
应用协议 ID (Application Protocol ID)																																
访问控制规则 ID (Access Control Rule ID)																																
访问控制策略 UUID (Access Control Policy UUID)																																
访问控制策略 UUID (Access Control Policy UUID) （续）																																
访问控制策略 UUID (Access Control Policy UUID) （续）																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
访问控制策略 UUID (Access Control Policy UUID) （续）																																
接口入口 UUID (Interface Ingress UUID)																																
接口入口 UUID (Interface Ingress UUID) （续）																																
接口入口 UUID (Interface Ingress UUID) （续）																																
接口入口 UUID (Interface Ingress UUID) （续）																																
接口出口 UUID (Interface Egress UUID)																																
接口出口 UUID (Interface Egress UUID) （续）																																
接口出口 UUID (Interface Egress UUID) （续）																																
接口出口 UUID (Interface Egress UUID) （续）																																
安全区入口 UUID (Security Zone Ingress UUID)																																
安全区入口 UUID (Security Zone Ingress UUID) （续）																																
安全区入口 UUID (Security Zone Ingress UUID) （续）																																
安全区入口 UUID (Security Zone Ingress UUID) （续）																																
安全区出口 UUID (Security Zone Egress UUID)																																
安全区出口 UUID (Security Zone Egress UUID) （续）																																
安全区出口 UUID (Security Zone Egress UUID) （续）																																
安全区出口 UUID (Security Zone Egress UUID) （续）																																
连接时间戳 (Connection Timestamp)																																
连接实例 ID (Connection Instance ID)																	连接计数器 (Connection Counter)														

下表对每个入侵事件记录数据字段进行了说明。

表 B-5 入侵事件记录 5.1.1 字段

字段	数据类型	说明
块类型	unint32	启动入侵事件数据块。值始终为 25。
块长度 (Block Length)	unint32	入侵事件数据块中的字节总数，包括入侵事件块类型和长度字段的八个字节，加上随后的数据字节数。
设备 ID (Device ID)	unit32	包含检测受管设备的标识号。您可以通过请求版本 3 或 4 元数据获取受管设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
事件 ID (Event ID)	uint32	事件标识号。
事件秒 (Event Second)	uint32	事件检测的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）
事件微秒 (Event Microsecond)	uint32	事件检测的时间戳微秒 （一秒的百万分之一）增量。
规则 ID （签名 ID） (Rule ID (Signature ID))	uint32	与事件对应的规则标识号。
生成器 ID (Generator ID)	uint32	生成事件的 Firepower 系统预处理器的标识号。
规则修订 (Rule Revision)	uint32	规则版本号。
分类 ID (Classification ID)	uint32	事件分类消息的标识号。
优先级 ID (Priority ID)	uint32	与事件相关的优先级的标识号。
源 IP 地址 (Source IP Address)	uint8[16]	事件中使用的源 IPv4 或 IPv6 地址。
目标 IP 地址 (Destination IP Address)	uint8[16]	事件中使用的目标 IPv4 或 IPv6 地址。
源端口 /ICMP 类型 (Source Port/ICMP Type)	uint16	如果事件协议类型是 TCP 或 UDP，则为源端口号，或者如果事件是由 ICMP 流量引起的，则为 ICMP 类型。
目标端口 /ICMP 代码 (Destination Port/ICMP Code)	uint16	如果事件协议类型是 TCP 或 UDP，则为目标端口号，或者如果事件是由 ICMP 流量引起的，则为 ICMP 代码。
IP 协议号 (IP Protocol Number)	uint8	IANA 指定的协议号。例如： • 0 - IP • 1 - ICMP • 6 - TCP • 17 - UDP

表 B-5　　入侵事件记录 5.1.1 字段 （续）

字段	数据类型	说明
影响标志 (Impact Flags)	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括： • 0x01 （位 0） - 源或目标主机位于系统监控的网络中。 • 0x02 （位 1） - 源或目标主机存在于网络映射中。 • 0x04 （位 2） - 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使 用 IP 协议。 • 0x08 （位 3） - 有漏洞映射到事件中的源或目标主机的操作系统。 • 0x10 （位 4） - 有漏洞映射到事件中检测到的服务器。 • 0x20 （位 5） - 事件导致受管设备丢弃会话 （仅当设备在内联、交换或路由式部署中运行时才使用）。对应于 Firepower 系统 Web 界面中的受阻状态。 • 0x40（位 6）- 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 • 0x80 （位 7） - 有漏洞映射到事件中检测到的客户端。 以下影响级别值映射到 “ 防御中心 ”(Defense Center) 上的特定优先级中。 x 表示值可以为 0 或 1： • （0，未知）：00X00000 • 红色 （1，易受攻击）：XXXX1XXX、XXX1XXXX、X1XXXXXX、1XXXXXXX • 橙色 （2，可能易受攻击）：00X00111 • 黄色 （3，当前不易受攻击）：00X00011 • 蓝色 （4，未知目标）：00X00001
影响 (Impact)	uint8	事件的影响标志值。其值如下： • 1 - 红色 （易受攻击） • 2 - 橙色 （可能易受攻击） • 3 - 黄色 （目前不易受攻击） • 4 - 蓝色 （未知目标） • 5 - （未知影响）
已阻止 (Blocked)	uint8	表示事件是否已被阻止的值。 • 0 - 未被阻止 • 1 - 已阻止 • 2 - 将被阻止 （但配置不允许）
MPLS 标签 (MPLS Label)	uint32	MPLS 标签。
VLAN ID	uint16	表示数据包起源的 VLAN 的 ID。
Pad	uint16	已保留供将来使用。

表 B-5 入侵事件记录 5.1.1 字段 （续）

字段	数据类型	说明
策略 UUID (Policy UUID)	uint8[16]	充当入侵策略的唯一标识符的策略 ID 号码。
用户 ID (User ID)	uint32	用户的内部标识号 （如适用）。
Web 应用 ID (Web Application ID)	uint32	Web 应用 （如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用 （如适用）的内部标别号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号 （如适用）。
访问控制规则 ID (Access Control Rule ID)	uint32	充当访问控制规则的唯一标识符的规则 ID 号码。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	充当访问控制策略的唯一标识符的策略 ID 号码。
入口接口 UUID (Ingress Interface UUID)	uint8[16]	充当入口接口的唯一标识符的接口 ID 号码。
出口接口 UUID (Egress Interface UUID)	uint8[16]	充当出口接口的唯一标识符的接口 ID 号码。
入口安全区 UUID (Ingress Security Zone UUID)	uint8[16]	充当入口安全区的唯一标识符的区域 ID 号码。
出口安全区 UUID (Egress Security Zone UUID)	uint8[16]	充当出口安全区的唯一标识符的区域 ID 号码。
连接时间戳 (Connection Timestamp)	uint32	与入侵事件关联的连接事件的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）。
连接实例 ID (Connection Instance ID)	uint16	生成连接事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。

入侵事件记录 5.3.1

下图中的阴影部分表示入侵事件记录中的字段。在系列 2 数据块组中，记录类型为 400，块类型为 42。

您可以通过扩展请求，仅从 eStreamer 请求 5.3.1 入侵事件，为此，您需要在流请求消息中请求事件类型代码 12 和版本代码 7（有关提交扩展请求的信息，请参阅提交扩展请求，第 2-4 页）。

对于版本 5.3.1 入侵事件，事件 ID、受管设备 ID 以及事件秒构成唯一标识符。连接秒、连接实例以及连接计数器在一起构成与入侵事件相关的连接事件的唯一标识符。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (400) (Record Type (400))															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp) （在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use)（在事件中，只有当位 23 已设置时）																																
块类型 (42) (Block Type (42))																																
块长度 (Block Length)																																
设备 ID (Device ID)																																
事件 ID (Event ID)																																
事件秒 (Event Second)																																
事件微秒 (Event Microsecond)																																
规则 ID（签名 ID） (Rule ID (Signature ID))																																
生成器 ID (Generator ID)																																
规则修订 (Rule Revision)																																
分类 ID (Classification ID)																																
优先级 ID (Priority ID)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
源 IP 地址 (Source IP Address)																																
源 IP 地址 (Source IP Address) （续）																																
源 IP 地址 (Source IP Address) （续）																																
源 IP 地址 (Source IP Address) （续）																																
目标 IP 地址 (Destination IP Address)																																
目标 IP 地址 (Destination IP Address) （续）																																
目标 IP 地址 (Destination IP Address) （续）																																
目标 IP 地址 (Destination IP Address) （续）																																
源端口或 ICMP 类型 (Source Port or ICMP Type)																	目标端口或 ICMP 代码 (Destination Port or ICMP Code)														
IP 协议 ID (IP Protocol ID)									影响标志 (Impact Flags)								影响 (Impact)								已阻止 (Blocked)							
MPLS 标签 (MPLS Label)																																
VLAN ID																	Pad															
策略 UUID (Policy UUID)																																
策略 UUID (Policy UUID) （续）																																
策略 UUID (Policy UUID) （续）																																
策略 UUID (Policy UUID) （续）																																
用户 ID (User ID)																																
Web 应用 ID (Web Application ID)																																
客户端应用 ID (Client Application ID)																																
应用协议 ID (Application Protocol ID)																																
访问控制规则 ID (Access Control Rule ID)																																
访问控制策略 UUID (Access Control Policy UUID)																																
访问控制策略 UUID (Access Control Policy UUID) （续）																																
访问控制策略 UUID (Access Control Policy UUID) （续）																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
访问控制策略 UUID (Access Control Policy UUID) （续）																																
接口入口 UUID (Interface Ingress UUID)																																
接口入口 UUID (Interface Ingress UUID) （续）																																
接口入口 UUID (Interface Ingress UUID) （续）																																
接口入口 UUID (Interface Ingress UUID) （续）																																
接口出口 UUID (Interface Egress UUID)																																
接口出口 UUID (Interface Egress UUID) （续）																																
接口出口 UUID (Interface Egress UUID) （续）																																
接口出口 UUID (Interface Egress UUID) （续）																																
安全区入口 UUID (Security Zone Ingress UUID)																																
安全区入口 UUID (Security Zone Ingress UUID) （续）																																
安全区入口 UUID (Security Zone Ingress UUID) （续）																																
安全区入口 UUID (Security Zone Ingress UUID) （续）																																
安全区出口 UUID (Security Zone Egress UUID)																																
安全区出口 UUID (Security Zone Egress UUID) （续）																																
安全区出口 UUID (Security Zone Egress UUID) （续）																																
安全区出口 UUID (Security Zone Egress UUID) （续）																																
连接时间戳 (Connection Timestamp)																																
连接实例 ID (Connection Instance ID)																	连接计数器 (Connection Counter)														
源国家 / 地区 (Source Country)																	目标国家 / 地区 (Destination Country)														
IOC 编号 (IOC Number)																	安全情景 (Security Context)														
安全情景 (Security Context) （续）																																
安全情景 (Security Context) （续）																																
安全情景 (Security Context) （续）																																
安全情景 (Security Context) （续）																																

下表对每个入侵事件记录数据字段进行了说明。

表 B-6 入侵事件记录 5.3.1 字段

字段	数据类型	说明
块类型 (Block Type)	unint32	启动入侵事件数据块。值始终为 42。
块长度 (Block Length)	unint32	入侵事件数据块中的字节总数，包括入侵事件块类型和长度字段的八个字节，加上随后的数据的字节数。
设备 ID (Device ID)	unit32	包含检测受管设备的标识号。您可以通过请求版本 3 或 4 元数据获取受管设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
事件 ID (Event ID)	uint32	事件标识号。
事件秒 (Event Second)	uint32	事件检测的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）
事件微秒 (Event Microsecond)	uint32	事件检测的时间戳微秒 （一秒的百万分之一）增量。
规则 ID （签名 ID） (Rule ID (Signature ID))	uint32	与事件对应的规则标识号。
生成器 ID (Generator ID)	uint32	生成事件的 Firepower 系统预处理器的标识号。
规则修订 (Rule Revision)	uint32	规则版本号。
分类 ID (Classification ID)	uint32	事件分类消息的标识号。
优先级 ID (Priority ID)	uint32	与事件相关的优先级的标识号。
源 IP 地址 (Source IP Address)	uint8[16]	事件中使用的源 IPv4 或 IPv6 地址。
目标 IP 地址 (Destination IP Address)	uint8[16]	事件中使用的目标 IPv4 或 IPv6 地址。
源端口或 ICMP 类型 (Source Port or ICMP Type)	uint16	如果事件协议类型是 TCP 或 UDP，则为源端口号，或者如果事件是由 ICMP 流量引起的，则为 ICMP 类型。
目标端口或 ICMP 代码 (Destination Port or ICMP Code)	uint16	如果事件协议类型是 TCP 或 UDP，则为目标端口号，或者如果事件是由 ICMP 流量引起的，则为 ICMP 代码。
IP 协议号 (IP Protocol Number)	uint8	IANA 指定的协议号。例如： • 0 - IP • 1 - ICMP • 6 - TCP • 17 - UDP

表 B-6　　入侵事件记录 5.3.1 字段 （续）

字段	数据类型	说明
影响标志 (Impact Flags)	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括： • 0x01 （位 0） - 源或目标主机位于系统监控的网络中。 • 0x02 （位 1） - 源或目标主机存在于网络映射中。 • 0x04 （位 2） - 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使 用 IP 协议。 • 0x08 （位 3） - 有漏洞映射到事件中的源或目标主机的操作系统。 • 0x10 （位 4） - 有漏洞映射到事件中检测到的服务器。 • 0x20 （位 5） - 事件导致受管设备丢弃会话 （仅当设备在内联、交换或路由式部署中运行时才使用）。对应于 Firepower 系统 Web 界面中的受阻状态。 • 0x40 （位 6） - 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 • 0x80 （位 7） - 有漏洞映射到事件中检测到的客户端。（仅限版本 5.0+） 以下影响级别值映射到 “ 防御中心 ”(Defense Center) 上的特定优先级中。x 表示值可以为 0 或 1： • （0，未知）：`00X00000` • 红色 （1，易受攻击）：`XXXX1XXX`、`XXX1XXXX`、`X1XXXXXX`、`1XXXXXXX` （仅限版本 5.0+） • 橙色 （2，可能易受攻击）：`00X0011X` • 黄色 （3，当前不易受攻击）：`00X0001X` • 蓝色 （4，未知目标）：`00X00001`
影响 (Impact)	uint8	事件的影响标志值。其值如下： • `1` - 红色 （易受攻击） • `2` - 橙色 （可能易受攻击） • `3` - 黄色 （目前不易受攻击） • `4` - 蓝色 （未知目标） • `5` - （未知影响）
已阻止 (Blocked)	uint8	表示事件是否已被阻止的值。 • `0` - 未被阻止 • `1` - 已阻止 • `2` - 将被阻止 （但配置不允许）
MPLS 标签 (MPLS Label)	uint32	MPLS 标签。
VLAN ID	uint16	表示数据包起源的 VLAN 的 ID。
Pad	uint16	已保留供将来使用。

表 B-6 入侵事件记录 5.3.1 字段 （续）

字段	数据类型	说明
策略 UUID (Policy UUID)	uint8[16]	充当入侵策略的唯一标识符的策略 ID 号码。
用户 ID (User ID)	uint32	用户的内部标识号 （如适用）。
Web 应用 ID (Web Application ID)	uint32	Web 应用 （如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用 （如适用）的内部标别号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号 （如适用）。
访问控制规则 ID (Access Control Rule ID)	uint32	充当访问控制规则的唯一标识符的规则 ID 号码。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	充当访问控制策略的唯一标识符的策略 ID 号码。
入口接口 UUID (Ingress Interface UUID)	uint8[16]	充当入口接口的唯一标识符的接口 ID 号码。
出口接口 UUID (Egress Interface UUID)	uint8[16]	充当出口接口的唯一标识符的接口 ID 号码。
入口安全区 UUID (Ingress Security Zone UUID)	uint8[16]	充当入口安全区的唯一标识符的区域 ID 号码。
出口安全区 UUID (Egress Security Zone UUID)	uint8[16]	充当出口安全区的唯一标识符的区域 ID 号码。
连接时间戳 (Connection Timestamp)	uint32	与入侵事件关联的连接事件的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）。
连接实例 ID (Connection Instance ID)	uint16	生成连接事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
源国家 / 地区 (Source Country)	uint16	源主机的国家 / 地区代码。
目标国家 / 地区 (Destination Country)	uint 16	目标主机的国家 / 地区代码。

表 B-6　　入侵事件记录 5.3.1 字段 （续）

字段	数据类型	说明
IOC 编号 (IOC Number)	uint16	与此事件相关的威胁的 ID 号码。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景 （虚拟防火墙）的 ID 号码。请注意，系统仅对 Firepower 系统情景模式下的 设备填充此字段。

入侵事件记录 5.4.x

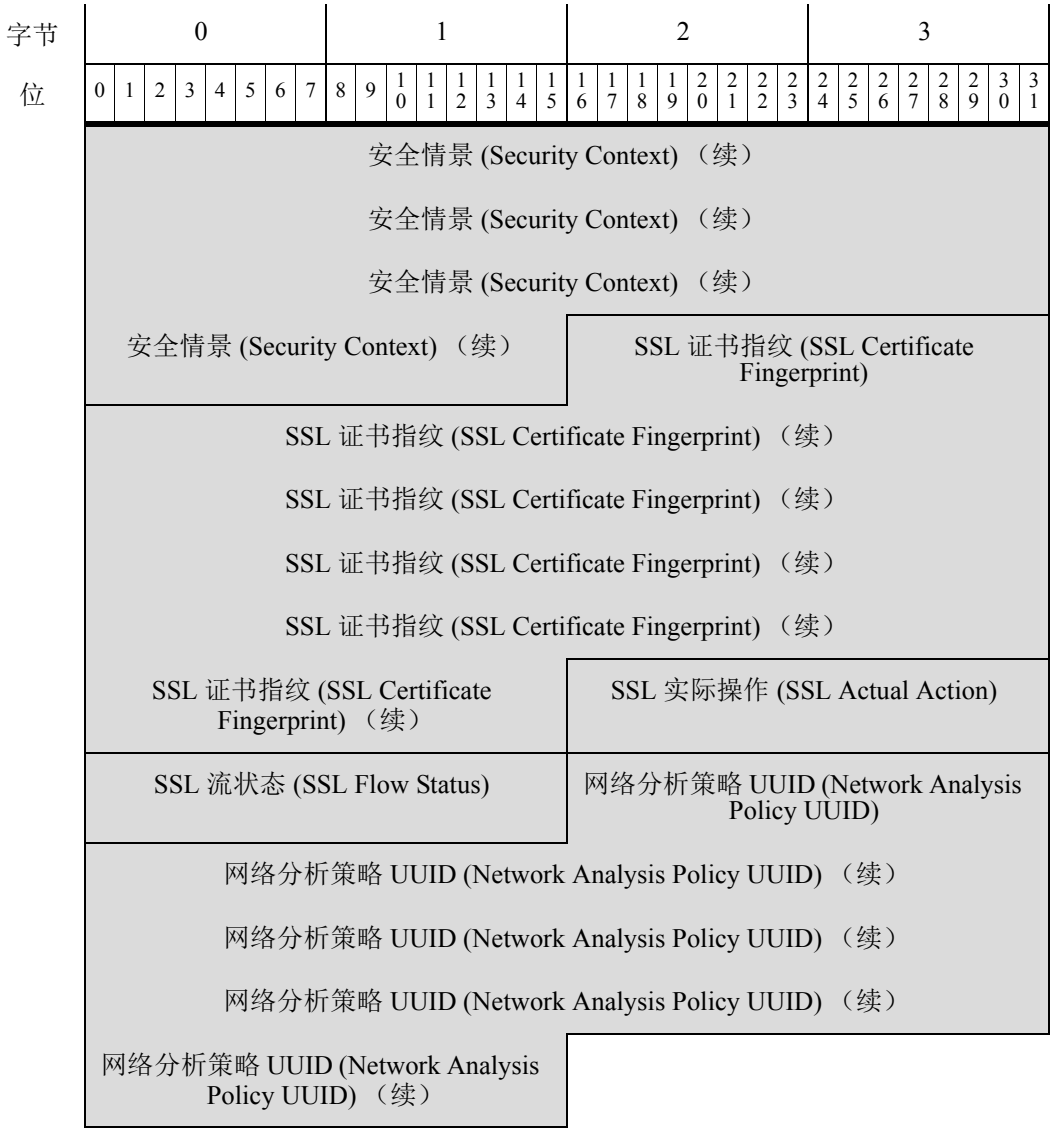
下图中的阴影部分表示入侵事件记录中的字段。在系列 2 数据块组中，记录类型为 400，块类型为 45。它替代了块类型 42，然后被块类型 60 替代。已添加用于 SSL 支持和网络分析策略的字段。

您可以通过扩展请求，仅从 eStreamer 请求 5.4.x 入侵事件，为此，您需要在流请求消息中请求事件类型代码 12 和版本代码 8 （有关提交扩展请求的信息，请参阅提交扩展请求，第 2-4 页）。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (400) (Record Type (400))															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp) （在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use) （在事件中，只有当位 23 已设置时）																																
块类型 (45) (Block Type (45))																																
块长度 (Block Length)																																
设备 ID (Device ID)																																
事件 ID (Event ID)																																
事件秒 (Event Second)																																
事件微秒 (Event Microsecond)																																
规则 ID （签名 ID） (Rule ID (Signature ID))																																
生成器 ID (Generator ID)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
规则修订 (Rule Revision)																																
分类 ID (Classification ID)																																
优先级 ID (Priority ID)																																
源 IP 地址 (Source IP Address) 源 IP 地址 (Source IP Address) （续） 源 IP 地址 (Source IP Address) （续） 源 IP 地址 (Source IP Address) （续）																																
目标 IP 地址 (Destination IP Address) 目标 IP 地址 (Destination IP Address) （续） 目标 IP 地址 (Destination IP Address) （续） 目标 IP 地址 (Destination IP Address) （续）																																
源端口或 ICMP 类型 (Source Port or ICMP Type)																	目标端口或 ICMP 代码 (Destination Port or ICMP Code)														
IP 协议 ID (IP Protocol ID)									影响标志 (Impact Flags)								影响 (Impact)								已阻止 (Blocked)							
MPLS 标签 (MPLS Label)																																
VLAN ID																	Pad															
策略 UUID (Policy UUID) 策略 UUID (Policy UUID) （续） 策略 UUID (Policy UUID) （续） 策略 UUID (Policy UUID) （续）																																
用户 ID (User ID)																																
Web 应用 ID (Web Application ID)																																
客户端应用 ID (Client Application ID)																																
应用协议 ID (Application Protocol ID)																																
访问控制规则 ID (Access Control Rule ID)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
访问控制策略 UUID (Access Control Policy UUID)																																
访问控制策略 UUID (Access Control Policy UUID) （续）																																
访问控制策略 UUID (Access Control Policy UUID) （续）																																
访问控制策略 UUID (Access Control Policy UUID) （续）																																
接口入口 UUID (Interface Ingress UUID)																																
接口入口 UUID (Interface Ingress UUID) （续）																																
接口入口 UUID (Interface Ingress UUID) （续）																																
接口入口 UUID (Interface Ingress UUID) （续）																																
接口出口 UUID (Interface Egress UUID)																																
接口出口 UUID (Interface Egress UUID) （续）																																
接口出口 UUID (Interface Egress UUID) （续）																																
接口出口 UUID (Interface Egress UUID) （续）																																
安全区入口 UUID (Security Zone Ingress UUID)																																
安全区入口 UUID (Security Zone Ingress UUID) （续）																																
安全区入口 UUID (Security Zone Ingress UUID) （续）																																
安全区入口 UUID (Security Zone Ingress UUID) （续）																																
安全区出口 UUID (Security Zone Egress UUID)																																
安全区出口 UUID (Security Zone Egress UUID) （续）																																
安全区出口 UUID (Security Zone Egress UUID) （续）																																
安全区出口 UUID (Security Zone Egress UUID) （续）																																
连接时间戳 (Connection Timestamp)																																
连接实例 ID (Connection Instance ID)																	连接计数器 (Connection Counter)														
源国家 / 地区 (Source Country)																	目标国家 / 地区 (Destination Country)														
IOC 编号 (IOC Number)																	安全情景 (Security Context)														



下表对每个入侵事件记录数据字段进行了说明。

表 B-7 入侵事件记录 5.4.x 字段

字段	数据类型	说明
块类型 (Block Type)	unint32	启动入侵事件数据块。值始终为 45。
块长度 (Block Length)	unint32	入侵事件数据块中的字节总数，包括入侵事件块类型和长度字段的八个字节，加上随后的数据的字节数。
设备 ID (Device ID)	unit32	包含检测受管设备的标识号。您可以通过请求版本 3 或 4 元数据获取受管设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
事件 ID (Event ID)	uint32	事件标识号。

表 B-7　　入侵事件记录 5.4.x 字段 （续）

字段	数据类型	说明
事件秒 (Event Second)	uint32	事件检测的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）
事件微秒 (Event Microsecond)	uint32	事件检测的时间戳微秒 （一秒的百万分之一）增量。
规则 ID （签名 ID） (Rule ID (Signature ID))	uint32	与事件对应的规则标识号。
生成器 ID (Generator ID)	uint32	生成事件的 Firepower 系统预处理器的标识号。
规则修订 (Rule Revision)	uint32	规则版本号。
分类 ID (Classification ID)	uint32	事件分类消息的标识号。
优先级 ID (Priority ID)	uint32	与事件相关的优先级的标识号。
源 IP 地址 (Source IP Address)	uint8[16]	事件中使用的源 IPv4 或 IPv6 地址。
目标 IP 地址 (Destination IP Address)	uint8[16]	事件中使用的目标 IPv4 或 IPv6 地址。
源端口或 ICMP 类型 (Source Port or ICMP Type)	uint16	如果事件协议类型是 TCP 或 UDP，则为源端口号，或者如果事件是由 ICMP 流量引起的，则为 ICMP 类型。
目标端口或 ICMP 代码 (Destination Port or ICMP Code)	uint16	如果事件协议类型是 TCP 或 UDP，则为目标端口号，或者如果事件是由 ICMP 流量引起的，则为 ICMP 代码。
IP 协议号 (IP Protocol Number)	uint8	IANA 指定的协议号。例如： • 0 - IP • 1 - ICMP • 6 - TCP • 17 - UDP

表 B-7　　入侵事件记录 5.4.x 字段 （续）

字段	数据类型	说明
影响标志 (Impact Flags)	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括： • 0x01 （位 0） - 源或目标主机位于系统监控的网络中。 • 0x02 （位 1） - 源或目标主机存在于网络映射中。 • 0x04 （位 2） - 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使 用 IP 协议。 • 0x08 （位 3） - 有漏洞映射到事件中的源或目标主机的操作系统。 • 0x10 （位 4） - 有漏洞映射到事件中检测到的服务器。 • 0x20 （位 5） - 事件导致受管设备丢弃会话 （仅当设备在内联、交换或路由式部署中运行时才使用）。对应于 Firepower 系统 Web 界面中的受阻状态。 • 0x40 （位 6） - 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 • 0x80 （位 7） - 有漏洞映射到事件中检测到的客户端。（仅限版本 5.0+） 以下影响级别值映射到 “ 防御中心 ”(Defense Center) 上的特定优先级中。x 表示值可以为 0 或 1： • 灰色 （0，未知）：`00X00000` • 红色 （1，易受攻击）：`XXXX1XXX`、`XXX1XXXX`、`X1XXXXXX`、`1XXXXXXX` （仅限版本 5.0+） • 橙色 （2，可能易受攻击）：`00X0011X` • 黄色 （3，当前不易受攻击）：`00X0001X` • 蓝色 （4，未知目标）：`00X00001`
影响 (Impact)	uint8	事件的影响标志值。其值如下： • `1` - 红色 （易受攻击） • `2` - 橙色 （可能易受攻击） • `3` - 黄色 （目前不易受攻击） • `4` - 蓝色 （未知目标） • `5` - 灰色 （未知影响）
已阻止 (Blocked)	uint8	表示事件是否已被阻止的值。 • `0` - 未被阻止 • `1` - 已阻止 • `2` - 将被阻止 （但配置不允许）
MPLS 标签 (MPLS Label)	uint32	MPLS 标签。
VLAN ID	uint16	表示数据包起源的 VLAN 的 ID。
Pad	uint16	已保留供将来使用。

表 B-7　　入侵事件记录 5.4.x 字段 （续）

字段	数据类型	说明
策略 UUID (Policy UUID)	uint8[16]	充当入侵策略的唯一标识符的策略 ID 号码。
用户 ID (User ID)	uint32	用户的内部标识号 （如适用）。
Web 应用 ID (Web Application ID)	uint32	Web 应用 （如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用 （如适用）的内部标别号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号 （如适用）。
访问控制规则 ID (Access Control Rule ID)	uint32	充当访问控制规则的唯一标识符的规则 ID 号码。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	充当访问控制策略的唯一标识符的策略 ID 号码。
入口接口 UUID (Ingress Interface UUID)	uint8[16]	充当入口接口的唯一标识符的接口 ID 号码。
出口接口 UUID (Egress Interface UUID)	uint8[16]	充当出口接口的唯一标识符的接口 ID 号码。
入口安全区 UUID (Ingress Security Zone UUID)	uint8[16]	充当入口安全区的唯一标识符的区域 ID 号码。
出口安全区 UUID (Egress Security Zone UUID)	uint8[16]	充当出口安全区的唯一标识符的区域 ID 号码。
连接时间戳 (Connection Timestamp)	uint32	与入侵事件关联的连接事件的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）。
连接实例 ID (Connection Instance ID)	uint16	生成连接事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
源国家 / 地区 (Source Country)	uint16	源主机的国家 / 地区代码。
目标国家 / 地区 (Destination Country)	uint 16	目标主机的国家 / 地区代码。

表 B-7 入侵事件记录 5.4.x 字段 （续）

字段	数据类型	说明
IOC 编号 (IOC Number)	uint16	与此事件相关的威胁的 ID 号码。
安全情景 (Security Context)	uint8[16]	流量通过的安全情景 （虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括： • 0 -‘ 未知 ’ • 1 -‘ 请勿解密 ’ • 2 -‘ 阻止 ’ • 3 -‘ 阻止并重置 ’ • 4 -‘ 解密 （已知密钥） ’ • 5 -‘ 解密 （更换秘钥） ’ • 6 -‘ 解密 （放弃） ’

表 B-7　　入侵事件记录 5.4.x 字段 （续）

字段	数据类型	说明
SSL 流状态 (SSL Flow Status)	uint16	SSL 流量的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括： • 0 -‘ 未知 ’ • 1 -‘ 不匹配 ’ • 2 -‘ 成功 ’ • 3 -‘ 非缓存会话 ’ • 4 -‘ 未知密码套件 ’ • 5 -‘ 不受支持的密码套件 ’ • 6 -‘ 不受支持的 SSL 版本 ’ • 7 -‘ 使用的 SSL 压缩 ’ • 8 -‘ 在被动模式中无法解密的会话 ’ • 9 -‘ 握手错误 ’ • 10 -‘ 解密错误 ’ • 11 -‘ 待处理服务器名称分类查找 ’ • 12 -‘ 待处理通用名称分类查找 ’ • 13 -‘ 内部错误 ’ • 14 -‘ 网络参数不可用 ’ • 15 -‘ 服务器证书处理无效 ’ • 16 -‘ 服务器证书指纹不可用 ’ • 17 -‘ 无法缓存持有者 DN’ • 18 -‘ 无法缓存颁发者 DN’ • 19 -‘ 未知 SSL 版本 ’ • 20 -‘ 外部证书列表不可用 ’ • 21 -‘ 外部证书指纹不可用 ’ • 22 -‘ 内部证书列表无效 ’ • 23 -‘ 内部证书列表不可用 ’ • 24 -‘ 内部证书不可用 ’ • 25 -‘ 内部证书指纹不可用 ’ • 26 -‘ 服务器证书验证不可用 ’ • 27 -‘ 服务器证书验证失败 ’ • 28 -‘ 操作无效 ’
网络分析策略 UUID (Network Analysis Policy UUID)	uint8[16]	创建入侵事件的网络分析策略的 UUID。

入侵影响警报数据

入侵影响警报事件包含影响事件的相关信息。当将入侵事件与系统网络映射数据进行比较且影响已确定时，系统传输入侵影响警报数据。该记录使用记录类型为 9 的标准记录报头，后面跟着数据块类型为系列 1 数据块组中的 20 的入侵影响警报数据块。（影响警报数据块是系列 1 类型的数据块。有关系列 1 数据块的详细信息，请参阅了解发现 （系列 1）块，第 4-63 页。）

您可以通过在请求消息的标志字段中设置位 5 来请求 eStreamer 只传输入侵影响事件。有关请求消息的详细信息，请参阅事件流请求消息格式，第 2-9 页。这些警报的版本 1 只处理 IPv4。5.3 中引入的版本 2 除了处理 IPv4 之外，还处理 IPv6 事件。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	报头版本 (1) (Header Version (1))																消息类型 (4) (Message Type (4))															
	消息长度 (Message Length)																															
	Netmap ID																记录类型 (9) (Record Type (9))															
	记录长度 (Record Length)																															
	入侵影响警报块类型 (20) （Intrusion Impact Alert Block Type (20))																															
	入侵影响警报块长度 (Intrusion Impact Alert Block Length)																															
	事件 ID (Event ID)																															
	设备 ID (Device ID)																															
	事件秒 (Event Second)																															
	影响 (Impact)																															
	源 IP 地址 (Source IP Address)																															
	目标 IP 地址 (Destination IP Address)																															
影响说明	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	说明 ...(Description...)																															

下表对影响事件中的每个数据字段进行了说明。

表 B-8　　影响事件数据字段

字段	数据类型	说明
入侵影响警报块类型 (Intrusion Impact Alert Block Type)	uint32	表示后面是入侵影响警报数据块。此字段的值始终为 20。请参阅入侵事件和元数据记录类型，第 3-1 页。
入侵影响警报块长度 (Intrusion Impact Alert Block Length)	uint32	表示入侵影响警报数据块的长度，包括后面的所有数据以及入侵影响警报块类型和长度的 8 个字节。
事件 ID (Event ID)	uint32	表示事件标识号。
设备 ID (Device ID)	uint32	表示受管设备标识号。
事件秒 (Event Second)	uint32	表示检测到事件的秒数 （从 1970/01/01 起）。
影响 (Impact)	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括： • 0x01 （位 0） - 源或目标主机位于系统监控的网络中。 • 0x02 （位 1） - 源或目标主机存在于网络映射中。 • 0x04 （位 2） - 源或目标主机在事件中的端口上运行服务器 （如果为 TCP 或 UDP）或使 用 IP 协议。 • 0x08 （位 3） - 有漏洞映射到事件中的源或目标主机的操作系统。 • 0x10 （位 4） - 有漏洞映射到事件中检测到的服务器。 • 0x20 （位 5） - 事件导致受管设备丢弃会话 （仅当设备在内联、交换或路由式部署中运行时才使用）。对应于 Firepower 系统 Web 界面中的受阻状态。 • 0x40 （位 6） - 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 • 0x80 （位 7） - 有漏洞映射到事件中检测到的客户端。（仅限版本 5.0+） 以下影响级别值映射到 “ 防御中心 ”(Defense Center) 上的特定优先级中。 x 表示值可以为 0 或 1： • （0，未知）：00X00000 • 红色 （1，易受攻击）：XXXX1XXX、XXX1XXXX、X1XXXXXX、1XXXXXXX （仅限版本 5.0+） • 橙色 （2，可能易受攻击）：00X0011X • 黄色 （3，当前不易受攻击）：00X0001X • 蓝色 （4，未知目标）：00X00001
源 IP 地址 (Source IP Address)	uint8[4]	与影响事件相关的主机的 IP 地址，采用 IP 地址八位组。

表 B-8 影响事件数据字段 （续）

字段	数据类型	说明
目标 IP 地址 (Destination IP Address)	uint8[4]	与影响事件相关的目标 IP 地址的 IP 地址 （如适用），采用 IP 地址八位组。如果无目标 IP 地址，则此值为 0。
字符串块类型 (String Block Type)	uint32	启动包含影响名称的字符串数据块。此值始终设置为 0。有关字符串块的详细信息，请参阅字符串数据块，第 4-70 页。
字符串块长度 (String Block Length)	uint32	事件说明字符串块中的字节数。这包括字符串块类型的四个字节，字符串块长度的四个字节以及说明中的字节数。
说明 (Description)	字符串	影响事件的说明。

旧版恶意软件事件数据结构

恶意软件事件数据块 5.1

eStreamer 服务使用恶意软件事件数据块存储有关恶意软件事件的信息。这些事件包含关于在云内检测到或被隔离的恶意软件、检测方法以及受恶意软件影响的主机和用户的信息。恶意软件事件数据块的块类型为系列 2 数据块组中的 16。您可以通过在事件版本为 1 且事件代码为 101 的请求消息中设置恶意软件事件标志 （“ 请求标志 ”(Request Flags) 字段中的位 30），将该事件作为恶意软件事件记录的一部分进行请求。

下图显示恶意软件事件数据块的结构：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
恶意软件事件块类型 (16) （Malware Event Block Type (16)）																																
恶意软件事件块长度 (Malware Event Block Length)																																
代理 UUID (Agent UUID)																																
代理 UUID (Agent UUID) （续）																																
代理 UUID (Agent UUID) （续）																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	代理 UUID (Agent UUID) （续）																															
	云 UUID (Cloud UUID) 云 UUID (Cloud UUID) （续） 云 UUID (Cloud UUID) （续） 云 UUID (Cloud UUID) （续）																															
	时间戳 (Timestamp)																															
	事件类型 ID (Event Type ID)																															
	事件子类型 ID (Event Subtype ID)								主机 IP 地址 (Host IP Address)																							
检测名称 (Detection Name)	主机 IP 地址 (Host IP Address) （续）								检测器 ID (Detector ID)								字符串块类型 (0) (String Block Type (0))															
	字符串块类型 (0) (String Block Type (0)) （续）																字符串块长度 (String Block Length)															
	字符串块长度 (String Block Length) （续）																检测名称 ... (Detection Name...)															
用户	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户 ... (User...)																															
文件名 (File Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件名 ... (File Name...)																															
文件路径	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件路径 ... (File Path...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
文件 SHA 哈希	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件 SHA 散列 ... (File SHA Hash...)																															
	文件大小 (File Size)																															
	文件类型								文件时间戳 (File Timestamp)																							
父文件名称	文件时间戳 (File Timestamp) （续）								字符串块类型 (0) (String Block Type (0))																							
	字符串块类型 (0) (String Block Type (0)) （续）								字符串块长度 (String Block Length)																							
	字符串块长度 (String Block Length) （续）								父文件名 ... (Parent File Name...)																							
父文件 SHA 散列	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	父文件 SHA 散列 ... (Parent File SHA Hash...)																															
事件说明	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	事件说明 ... (Event Description...)																															

下表对恶意软件事件数据块中的字段进行了说明。

表 B-9　　恶意软件事件数据块字段

字段	数据类型	说明
恶意软件事件块类型 (Malware Event Block Type)	uint32	启动恶意软件事件数据块。值始终为 16。
恶意软件事件块长度 (Malware Event Block Length)	uint32	恶意软件事件数据块中的字节总数，包括恶意软件事件块类型和长度字段的八个字节，加上随后的数据字节数。

表 B-9　恶意软件事件数据块字段 （续）

字段	数据类型	说明
代理 UUID (Agent UUID)	uint8[16]	报告恶意软件事件的面向终端的 AMP 代理的内部唯一 ID。
云 UUID (Cloud UUID)	uint8[16]	发生恶意软件事件的恶意软件感知网络的内部唯一 ID。
时间戳 (Timestamp)	uint32	恶意软件事件生成时间戳。
事件类型 ID (Event Type ID)	uint32	恶意软件事件类型的内部 ID。
事件子类型 ID (Event Subtype ID)	uint8	导致恶意软件检测的操作的内部 ID。
主机 IP 地址 (Host IP Address)	uint32	与恶意软件事件相关的主机 IP 地址。
检测器 ID (Detector ID)	uint8	检测到恶意软件的检测技术的内部 ID。
字符串块类型 (String Block Type)	uint32	启动包含检测名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	检测名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 检测名称 ”(Detection Name) 字段中的字节数。
检测名称 (Detection Name)	字符串	检测到或被隔离的恶意软件的名称。
字符串块类型 (String Block Type)	uint32	启动包含用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 用户 ”(User) 字段中的字节数。
用户	字符串	安装 Cisco 代理并发生恶意软件事件的计算机的用户。请注意，这些用户未绑定到用户发现。
字符串块类型 (String Block Type)	uint32	启动包含文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 文件名 ”(File Name) 字段中的字节数。
文件名 (File Name)	字符串	被检测或隔离的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含文件路径的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件路径字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 文件路径 ”(File Path) 字段中的字节数。
文件路径 (File Path)	字符串	被检测或隔离的文件的文件路径，不包括文件名。
字符串块类型 (String Block Type)	uint32	启动包含文件 SHA 散列的字符串数据块。值始终为 0。

表 B-9 恶意软件事件数据块字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Length)	uint32	文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 文件 SHA 散列 ”(File SHA Hash) 字段中的字节数。
文件 SHA 散列 (File SHA Hash)	字符串	被检测或隔离的文件 SHA-256 哈希值。
文件大小 (File Size)	uint32	被检测或隔离的文件的大小 （字节）。
文件类型 (File Type)	uint8	被检测或隔离文件的文件类型。
文件时间戳 (File Timestamp)	uint32	被检测或隔离的文件的创建时间戳。
字符串块类型 (String Block Type)	uint32	启动包含父文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 父文件名 ”(Parent File Name) 字段中的字节数。
父文件名 (Parent File Name)	字符串	检测期间访问被检测或隔离文件的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含父文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 父文件 SHA 散列 ” (Parent File SHA Hash) 字段中的字节数。
父文件 SHA 散列 (Parent File SHA Hash)	字符串	检测期间访问被检测或隔离文件的父文件的 SHA-256 哈希值。
字符串块类型 (String Block Type)	uint32	启动包含事件说明的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	事件说明字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 事件说明 ”(Event Description) 字段中的字节数。
活动说明 (Event Description)	字符串	与事件类型相关的其他事件信息。

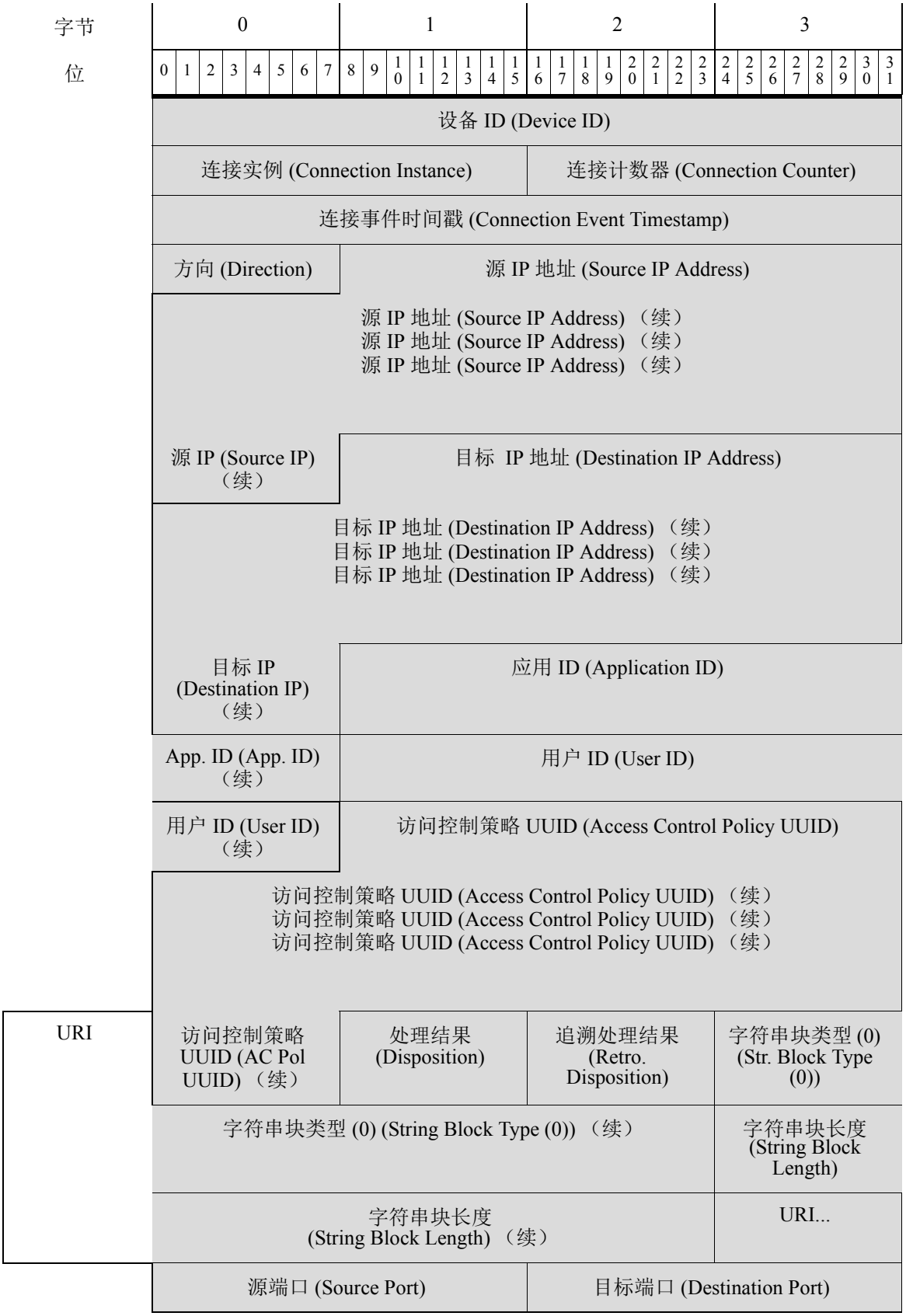
恶意软件事件数据块 5.1.1.x

eStreamer 服务使用恶意软件事件数据块存储有关恶意软件事件的信息。这些事件包含关于在云内检测到或被隔离的恶意软件、检测方法以及受恶意软件影响的主机和用户的信息。恶意软件事件数据块的块类型为系列 2 数据块组中的 24。您可以通过在事件版本为 2 且事件代码为 101 的请求消息中设置恶意软件事件标志 （“ 请求标志 ”(Request Flags) 字段中的位 30），将该事件作为恶意软件事件记录的一部分进行请求。

下图显示恶意软件事件数据块的结构：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	恶意软件事件块类型 (24) (Malware Event Block Type (24))																															
	恶意软件事件块长度 (Malware Event Block Length)																															
	代理 UUID (Agent UUID) 代理 UUID (Agent UUID) （续） 代理 UUID (Agent UUID) （续） 代理 UUID (Agent UUID) （续）																															
	云 UUID (Cloud UUID) 云 UUID (Cloud UUID) （续） 云 UUID (Cloud UUID) （续） 云 UUID (Cloud UUID) （续）																															
	恶意软件事件时间戳 (Malware Event Timestamp)																															
	事件类型 ID (Event Type ID)																															
	事件子类型 ID (Event Subtype ID)								主机 IP 地址 (Host IP Address)																							
检测名称 (Detection Name)	主机 IP 地址 (Host IP Address) （续）								检测器 ID (Detector ID)								字符串块类型 (0) (String Block Type (0))															
	字符串块类型 (0) (String Block Type (0)) （续）																字符串块长度 (String Block Length)															
	字符串块长度 (String Block Length) （续）																检测名称 ... (Detection Name...)															
用户	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户 ... (User...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
文件名 (File Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件名 ... (File Name...)																															
文件路径	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件路径 ... (File Path...)																															
文件 SHA 哈希	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件 SHA 散列 ... (File SHA Hash...)																															
	文件大小 (File Size)																															
	文件类型 (File Type)								文件时间戳 (File Timestamp)																							
父文件名称	文件时间戳 (File Timestamp) （续）								字符串块类型 (0) (String Block Type (0))																							
	字符串块类型 (0) (String Block Type (0)) （续）								字符串块长度 (String Block Length)																							
	字符串块长度 (String Block Length) （续）								父文件名 ... (Parent File Name...)																							
父文件 SHA 散列	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	父文件 SHA 散列 ... (Parent File SHA Hash...)																															
事件说明	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	事件说明 ... (Event Description...)																															


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
设备 ID (Device ID)
连接实例 (Connection Instance)
连接计数器 (Connection Counter)
连接事件时间戳 (Connection Event Timestamp)
方向 (Direction)
源 IP 地址 (Source IP Address)
源 IP 地址 (Source IP Address) （续）
源 IP 地址 (Source IP Address) （续）
源 IP 地址 (Source IP Address) （续）
源 IP (Source IP) （续）
目标 IP 地址 (Destination IP Address)
目标 IP 地址 (Destination IP Address) （续）
目标 IP 地址 (Destination IP Address) （续）
目标 IP 地址 (Destination IP Address) （续）
目标 IP (Destination IP) （续）
应用 ID (Application ID)
App. ID (App. ID) （续）
用户 ID (User ID)
用户 ID (User ID) （续）
访问控制策略 UUID (Access Control Policy UUID)
访问控制策略 UUID (Access Control Policy UUID) （续）
访问控制策略 UUID (Access Control Policy UUID) （续）
访问控制策略 UUID (Access Control Policy UUID) （续）
URI
访问控制策略 UUID (AC Pol UUID) （续）
处理结果 (Disposition)
追溯处理结果 (Retro. Disposition)
字符串块类型 (0) (Str. Block Type (0))
字符串块类型 (0) (String Block Type (0)) （续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length) （续）
URI...
源端口 (Source Port)
目标端口 (Destination Port)

下表对恶意软件事件数据块中的字段进行了说明。

表 B-10　　用于 5.1.1.x 的恶意软件事件数据块字段

字段	数据类型	说明
恶意软件事件块类型 (Malware Event Block Type)	uint32	启动恶意软件事件数据块。值始终为 24。
恶意软件事件块长度 (Malware Event Block Length)	uint32	恶意软件事件数据块中的字节总数，包括恶意软件事件块类型和长度字段的八个字节，加上随后的数据字节数。
代理 UUID (Agent UUID)	uint8[16]	报告恶意软件事件的面向终端的 AMP 代理的内部唯一 ID。
云 UUID (Cloud UUID)	uint8[16]	发生恶意软件事件的恶意软件感知网络的内部唯一 ID。
恶意软件事件时间戳 (Malware Event Timestamp)	uint32	恶意软件事件生成时间戳。
事件类型 ID (Event Type ID)	uint32	恶意软件事件类型的内部 ID。
事件子类型 ID (Event Subtype ID)	uint8	导致恶意软件检测的操作的内部 ID。
主机 IP 地址 (Host IP Address)	uint32	与恶意软件事件相关的主机 IP 地址。
检测器 ID (Detector ID)	uint8	检测到恶意软件的检测技术的内部 ID。
字符串块类型 (String Block Type)	uint32	启动包含检测名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	检测名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 检测名称 ”(Detection Name) 字段中的字节数。
检测名称 (Detection Name)	字符串	检测到或被隔离的恶意软件的名称。
字符串块类型 (String Block Type)	uint32	启动包含用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 用户 ”(User) 字段中的字节数。
用户	字符串	安装 Cisco 代理并发生恶意软件事件的计算机的用户。请注意，这些用户未绑定到用户发现。
字符串块类型 (String Block Type)	uint32	启动包含文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 文件名 ”(File Name) 字段中的字节数。
文件名 (File Name)	字符串	被检测或隔离的文件的名称。

表 B-10　用于 5.1.1.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明
字符串块类型 (String Block Type)	uint32	启动包含文件路径的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件路径字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 文件路径 ”(File Path) 字段中的字节数。
文件路径 (File Path)	字符串	被检测或隔离的文件的文件路径，不包括文件名。
字符串块类型 (String Block Type)	uint32	启动包含文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 文件 SHA 散列 ”(File SHA Hash) 字段中的字节数。
文件 SHA 散列 (File SHA Hash)	字符串	被检测或隔离的文件 SHA-256 散列值的呈现字符串。
文件大小 (File Size)	uint32	被检测或隔离的文件的大小 （字节）。
文件类型 (File Type)	uint8	被检测或隔离文件的文件类型。
文件时间戳 (File Timestamp)	uint32	创建被检测或隔离的文件的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）。
字符串块类型 (String Block Type)	uint32	启动包含父文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 父文件名 ”(Parent File Name) 字段中的字节数。
父文件名 (Parent File Name)	字符串	检测期间访问被检测或隔离文件的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含父文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 父文件 SHA 散列 ” (Parent File SHA Hash) 字段中的字节数。
父文件 SHA 散列 (Parent File SHA Hash)	字符串	检测期间访问被检测或隔离文件的父文件的 SHA-256 哈希值。
字符串块类型 (String Block Type)	uint32	启动包含事件说明的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	事件说明字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 事件说明 ”(Event Description) 字段中的字节数。
活动说明 (Event Description)	字符串	与事件类型相关的其他事件信息。
设备 ID (Device ID)	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或 IDS 事件相关联。

表 B-10 用于 5.1.1.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接事件时间戳 (Connection Event Timestamp)	uint32	连接事件的时间戳。
方向 (Direction)	uint8	表示文件是否已上传或下载。可能会有以下值： • 1 - 下载 • 2 - 上传 目前该值取决于协议 （例如，如果连接是 HTTP，则其值为 Download）。
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标 IP 地址 (Destination IP Address)	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。
用户 ID (User ID)	uint32	系统识别的登录目标主机的用户的标识号。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	作为触发事件的访问控制策略的唯一标识符的标别号。
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括： • 1 - CLEAN - 文件是安全的，不包含恶意软件。 • 2 - UNKNOWN - 不确定文件是否包含恶意软件。 • 3 - MALWARE - 文件包含恶意软件。 • 4 - CACHE_MISS - 软件无法向 Cisco 云发送请求以了解处置情况。 • 5 - NO_CLOUD_RESP - Cisco 云服务未响应此请求。
追溯处置情况 (Retrospective Disposition)	uint8	处置情况更新后的处置情况。如果处置情况未更新，则此字段包含的值与 “ 处置情况 ”(Disposition) 字段包含的值相同。可能值与 “ 处置情况 ”(Disposition) 字段包含的值相同。
字符串块类型 (String Block Type)	uint32	启动包含 URI 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	URI 数据块中的字节数，包括块类型和报头字段的八个字节，加上 URI 字段中的字节数。
URI	字符串	连接的 URI。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。

恶意软件事件数据块 5.2.x

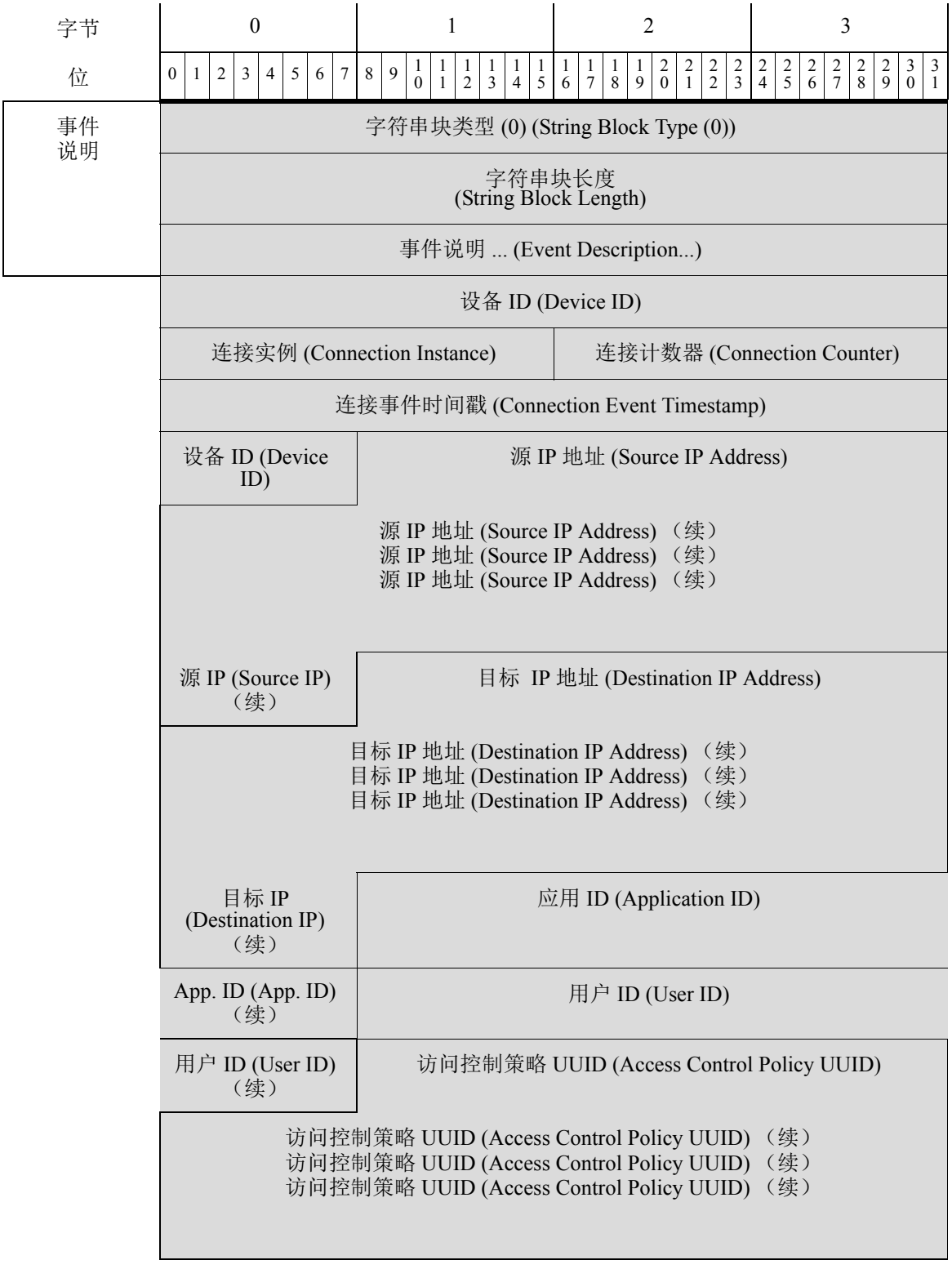
eStreamer 服务使用恶意软件事件数据块存储有关恶意软件事件的信息。这些事件包含关于在云内检测到或被隔离的恶意软件、检测方法以及受恶意软件影响的主机和用户的信息。恶意软件事件数据块的块类型为系列 2 数据块组中的 33。您可以通过在事件版本为 3 且事件代码为 101 的请求消息中设置恶意软件事件标志 （“ 请求标志 ”(Request Flags) 字段中的位 30），将该事件作为恶意软件事件记录的一部分进行请求。

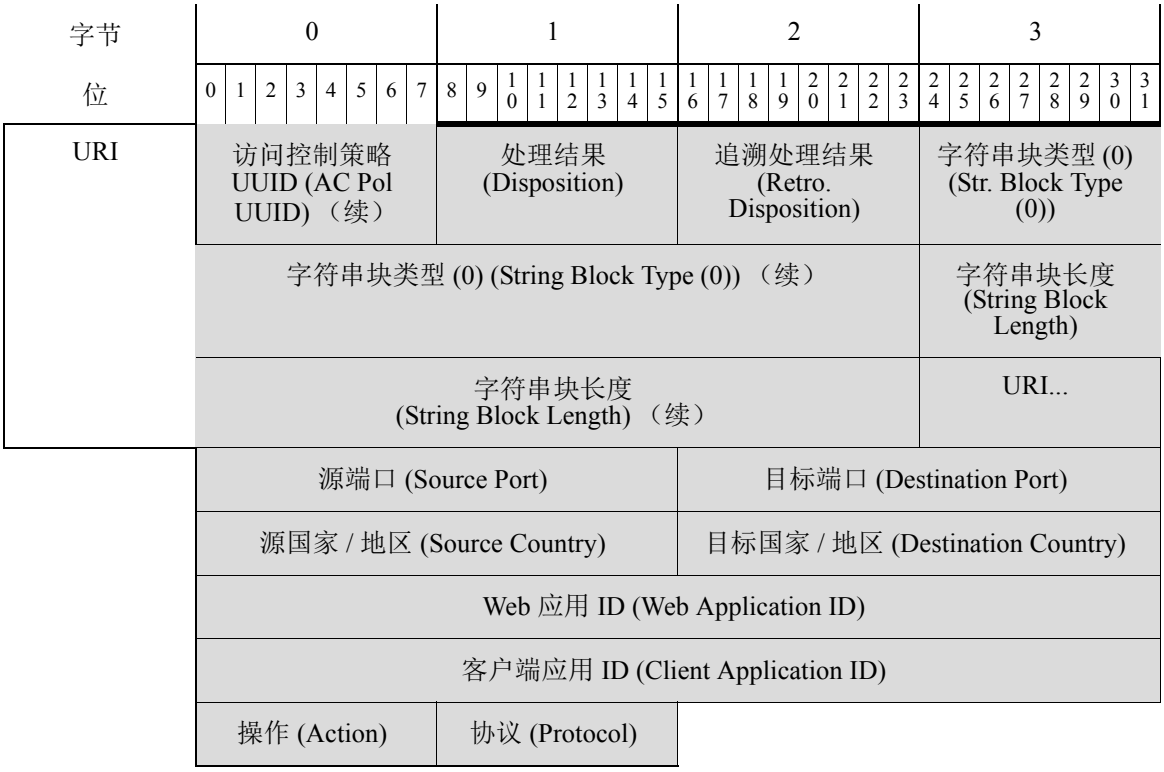
下图显示恶意软件事件数据块的结构：

字节	0				1			
位	0 1 2 3 4 5 6 7				8 9 10 11 12 13 14 15			
	恶意软件事件块类型 (33) (Malware Event Block Type (33))							
	恶意软件事件块长度 (Malware Event Block Length)							
	代理 UUID (Agent UUID)							
	代理 UUID (Agent UUID) （续）							
	代理 UUID (Agent UUID) （续）							
	代理 UUID (Agent UUID) （续）							
	云 UUID (Cloud UUID)							
	云 UUID (Cloud UUID) （续）							
	云 UUID (Cloud UUID) （续）							
	云 UUID (Cloud UUID) （续）							
	恶意软件事件时间戳 (Malware Event Timestamp)							
	事件类型 ID (Event Type ID)							
检测名称 (Detection Name)	事件子类型 ID (Event Subtype ID)				检测器 ID (Detector ID)			
	字符串块类型 (0) (String Block Type (0)) （续）							
	字符串块长度 (String Block Length) （续）							

字节	2				3			
位	16 17 18 19 20 21 22 23				24 25 26 27 28 29 30 31			
	恶意软件事件块类型 (33) (Malware Event Block Type (33))							
	恶意软件事件块长度 (Malware Event Block Length)							
	代理 UUID (Agent UUID)							
	代理 UUID (Agent UUID) （续）							
	代理 UUID (Agent UUID) （续）							
	代理 UUID (Agent UUID) （续）							
	云 UUID (Cloud UUID)							
	云 UUID (Cloud UUID) （续）							
	云 UUID (Cloud UUID) （续）							
	云 UUID (Cloud UUID) （续）							
	恶意软件事件时间戳 (Malware Event Timestamp)							
	事件类型 ID (Event Type ID)							
	字符串块类型 (0) (String Block Type (0))				字符串块长度 (String Block Length)			
	字符串块长度 (String Block Length) （续）				检测名称 ... (Detection Name...)			

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
用户	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户 ... (User...)																															
文件名	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件名 ... (File Name...)																															
文件路径	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件路径 ... (File Path...)																															
文件 SHA 哈希	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件 SHA 散列 ... (File SHA Hash...)																															
	文件大小 (File Size)																															
	文件类型 (File Type)																															
	文件时间戳 (File Timestamp)																															
父文件名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	父文件名 ... (Parent File Name...)																															
父文件 SHA 散列	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	父文件 SHA 散列 ... (Parent File SHA Hash...)																															


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
事件说明
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
事件说明 ... (Event Description...)
设备 ID (Device ID)
连接实例 (Connection Instance)
连接计数器 (Connection Counter)
连接事件时间戳 (Connection Event Timestamp)
设备 ID (Device ID)
源 IP 地址 (Source IP Address)
源 IP 地址 (Source IP Address) （续）
源 IP 地址 (Source IP Address) （续）
源 IP 地址 (Source IP Address) （续）
源 IP (Source IP) （续）
目标 IP 地址 (Destination IP Address)
目标 IP 地址 (Destination IP Address) （续）
目标 IP 地址 (Destination IP Address) （续）
目标 IP 地址 (Destination IP Address) （续）
目标 IP (Destination IP) （续）
应用 ID (Application ID)
App. ID (App. ID) （续）
用户 ID (User ID)
用户 ID (User ID) （续）
访问控制策略 UUID (Access Control Policy UUID)
访问控制策略 UUID (Access Control Policy UUID) （续）
访问控制策略 UUID (Access Control Policy UUID) （续）
访问控制策略 UUID (Access Control Policy UUID) （续）



下表对恶意软件事件数据块中的字段进行了说明。

表 B-11 用于 5.2.x 的恶意软件事件数据块字段

字段	数据类型	说明
恶意软件事件块类型 (Malware Event Block Type)	uint32	启动恶意软件事件数据块。值始终为 33。
恶意软件事件块长度 (Malware Event Block Length)	uint32	恶意软件事件数据块中的字节总数，包括恶意软件事件块类型和长度字段的八个字节，加上随后的数据字节数。
代理 UUID (Agent UUID)	uint8[16]	报告恶意软件事件的面向终端的 AMP 代理的内部唯一 ID。
云 UUID (Cloud UUID)	uint8[16]	发生恶意软件事件的恶意软件感知网络的内部唯一 ID。
恶意软件事件时间戳 (Malware Event Timestamp)	uint32	恶意软件事件生成时间戳。
事件类型 ID (Event Type ID)	uint32	恶意软件事件类型的内部 ID。
事件子类型 ID (Event Subtype ID)	uint8	导致恶意软件检测的操作的内部 ID。
检测器 ID (Detector ID)	uint8	检测到恶意软件的检测技术的内部 ID。

表 B-11　用于 5.2.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明
字符串块类型 (String Block Type)	uint32	启动包含检测名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	检测名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 检测名称 ”(Detection Name) 字段中的字节数。
检测名称 (Detection Name)	字符串	检测到或被隔离的恶意软件的名称。
字符串块类型 (String Block Type)	uint32	启动包含用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 用户 ”(User) 字段中的字节数。
用户 (User)	字符串	安装 Cisco 代理并发生恶意软件事件的计算机的用户。请注意，这些用户未绑定到用户发现。
字符串块类型 (String Block Type)	uint32	启动包含文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 文件名 ”(File Name) 字段中的字节数。
文件名 (File Name)	字符串	被检测或隔离的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含文件路径的字符串数据块。值始终为 0。
字符串块长度 (String Block Type)	uint32	文件路径字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 文件路径 ”(File Path) 字段中的字节数。
文件路径 (File Path)	字符串	被检测或隔离的文件的文件路径，不包括文件名。
字符串块类型 (String Block Type)	uint32	启动包含文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Type)	uint32	文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 文件 SHA 散列 ”(File SHA Hash) 字段中的字节数。
文件 SHA 散列 (File SHA Hash)	字符串	被检测或隔离的文件 SHA-256 散列值的呈现字符串。
文件大小 (File Size)	uint32	被检测或隔离的文件的大小 （字节）。
文件类型 (File Type)	uint8	被检测或隔离文件的文件类型。
文件时间戳 (File Timestamp)	uint32	创建被检测或隔离的文件的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）。
字符串块类型 (String Block Type)	uint32	启动包含父文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 父文件名 ”(Parent File Name) 字段中的字节数。

表 B-11 用于 5.2.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明
父文件名 (Parent File Name)	字符串	检测期间访问被检测或隔离文件的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含父文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 父文件 SHA 散列 ” (Parent File SHA Hash) 字段中的字节数。
父文件 SHA 散列 (Parent File SHA Hash)	字符串	检测期间访问被检测或隔离文件的父文件的 SHA-256 哈希值。
字符串块类型 (String Block Type)	uint32	启动包含事件说明的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	事件说明字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 事件说明 ”(Event Description) 字段中的字节数。
活动说明 (Event Description)	字符串	与事件类型相关的其他事件信息。
设备 ID (Device ID)	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或 IDS 事件相关联。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接事件时间戳 (Connection Event Timestamp)	uint32	连接事件的时间戳。
方向 (Direction)	uint8	表示文件是否已上传或下载。可能会有以下值： • 1 - 下载 • 2 - 上传 目前该值取决于协议 （例如，如果连接是 HTTP，则其值为 Download）。
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标 IP 地址 (Destination IP Address)	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。
用户 ID (User ID)	uint32	系统识别的登录目标主机的用户的标识号。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	作为触发事件的访问控制策略的唯一标识符的标别号。

表 B-11　用于 5.2.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括： • 1 - CLEAN - 文件是安全的，不包含恶意软件。 • 2 - NEUTRAL - 不确定文件是否包含恶意软件。 • 3 - MALWARE - 文件包含恶意软件。 • 4 - CACHE_MISS - 软件无法向 Cisco 云发送请求以了解处置情况，或 Cisco 云服务未响应此请求。
追溯处置情况 (Retrospective Disposition)	uint8	处置情况更新后的处置情况。如果处置情况未更新，则此字段包含的值与 “ 处置情况 ”(Disposition) 字段包含的值相同。可能值与 “ 处置情况 ”(Disposition) 字段包含的值相同。
字符串块类型 (String Block Type)	uint32	启动包含 URI 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	URI 数据块中的字节数，包括块类型和报头字段的八个字节，加上 URI 字段中的字节数。
URI	字符串	连接的 URI。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。
源国家 / 地区 (Source Country)	uint16	源主机的国家 / 地区代码。
目标国家 / 地区 (Destination Country)	uint 16	目标主机的国家 / 地区代码。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号 （如适用）。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号 （如适用）。
操作 (Action)	uint8	根据文件类型对文件执行的操作。可以具有以下值： • 1 - 检测 • 2 - 阻止 • 3 - 恶意软件云查找 • 4 - 恶意软件阻止 • 5 - 恶意软件允许列表
协议 (Protocol)	uint8	用户指定的 IANA 协议号。例如： • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP 目前仅限 TCP。

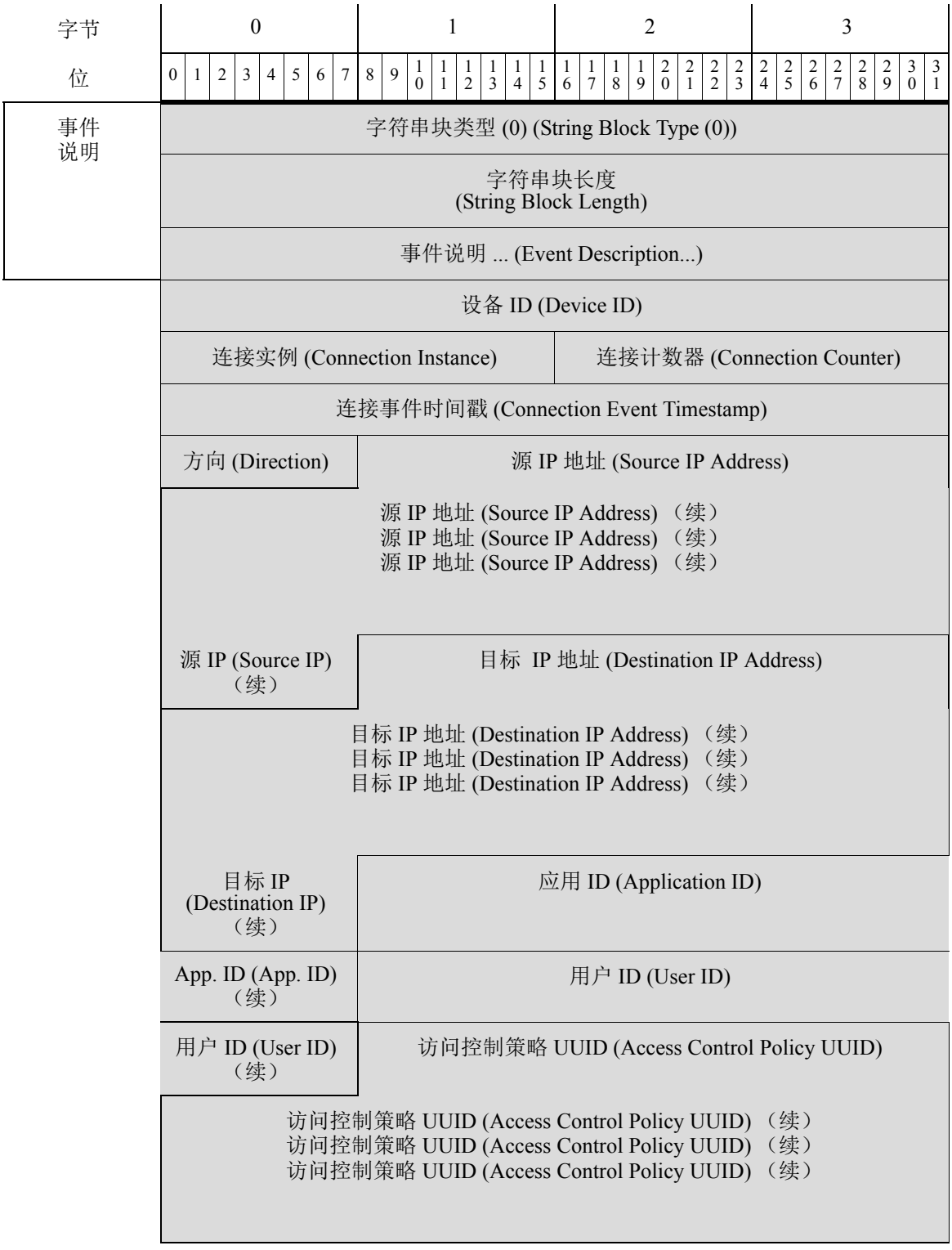
恶意软件事件数据块 5.3

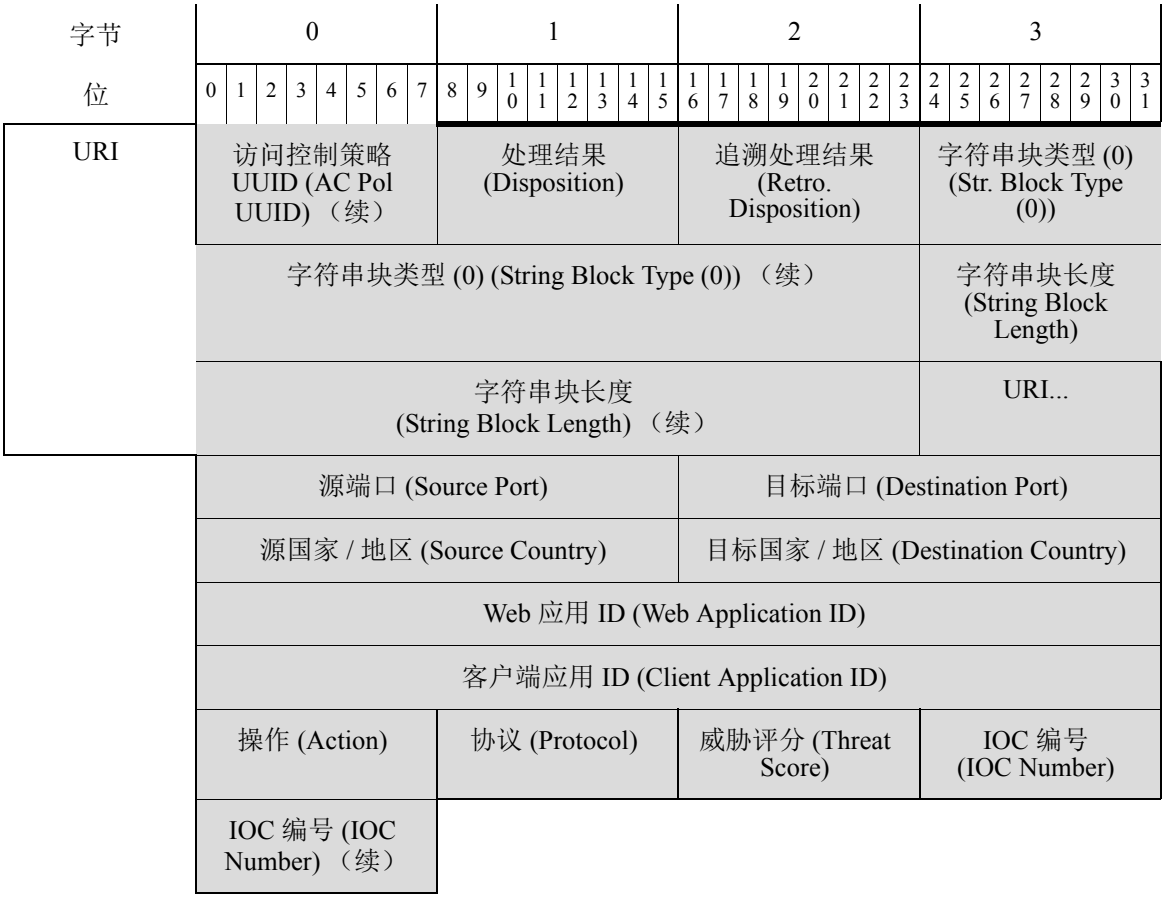
eStreamer 服务使用恶意软件事件数据块存储有关恶意软件事件的信息。这些事件包含关于在云内检测到或被隔离的恶意软件、检测方法以及受恶意软件影响的主机和用户的信息。恶意软件事件数据块的块类型为系列 2 数据块组中的 35。您可以通过在事件版本为 4 且事件代码为 101 的请求消息中设置恶意软件事件标志（“ 请求标志 ”(Request Flags) 字段中的位 30），将该事件作为恶意软件事件记录的一部分进行请求。

下图显示恶意软件事件数据块的结构：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
恶意软件事件块类型 (35) (Malware Event Block Type (35))																																
恶意软件事件块长度 (Malware Event Block Length)																																
代理 UUID (Agent UUID)																																
代理 UUID (Agent UUID) （续）																																
代理 UUID (Agent UUID) （续）																																
代理 UUID (Agent UUID) （续）																																
云 UUID (Cloud UUID)																																
云 UUID (Cloud UUID) （续）																																
云 UUID (Cloud UUID) （续）																																
云 UUID (Cloud UUID) （续）																																
恶意软件事件时间戳 (Malware Event Timestamp)																																
事件类型 ID (Event Type ID)																																
事件子类型 ID (Event Subtype ID)																																
检测名称 (Detection Name)	检测器 ID (Detector ID)								字符串块类型 (0) (String Block Type (0))																							
	字符串块类型 (0) (String Block Type (0)) （续）								字符串块长度 (String Block Length)																							
	字符串块长度 (String Block Length) （续）								检测名称 ... (Detection Name...)																							

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
用户	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户 ... (User...)																															
文件名	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件名 ... (File Name...)																															
文件路径	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件路径 ... (File Path...)																															
文件 SHA 哈希	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件 SHA 散列 ... (File SHA Hash...)																															
	文件大小 (File Size)																															
	文件类型 (File Type)																															
	文件时间戳 (File Timestamp)																															
父文件名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	父文件名 ... (Parent File Name...)																															
父文件 SHA 散列	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	父文件 SHA 散列 ... (Parent File SHA Hash...)																															


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
事件说明
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
事件说明 ... (Event Description...)
设备 ID (Device ID)
连接实例 (Connection Instance)
连接计数器 (Connection Counter)
连接事件时间戳 (Connection Event Timestamp)
方向 (Direction)
源 IP 地址 (Source IP Address)
源 IP 地址 (Source IP Address) （续）
源 IP 地址 (Source IP Address) （续）
源 IP 地址 (Source IP Address) （续）
源 IP (Source IP) （续）
目标 IP 地址 (Destination IP Address)
目标 IP 地址 (Destination IP Address) （续）
目标 IP 地址 (Destination IP Address) （续）
目标 IP 地址 (Destination IP Address) （续）
目标 IP (Destination IP) （续）
应用 ID (Application ID)
App. ID (App. ID) （续）
用户 ID (User ID)
用户 ID (User ID) （续）
访问控制策略 UUID (Access Control Policy UUID)
访问控制策略 UUID (Access Control Policy UUID) （续）
访问控制策略 UUID (Access Control Policy UUID) （续）
访问控制策略 UUID (Access Control Policy UUID) （续）



下表对恶意软件事件数据块中的字段进行了说明。

表 B-12　　用于 5.3 的恶意软件事件数据块字段

字段	数据类型	说明
恶意软件事件块类型 (Malware Event Block Type)	uint32	启动恶意软件事件数据块。值始终为 35。
恶意软件事件块长度 (Malware Event Block Length)	uint32	恶意软件事件数据块中的字节总数，包括恶意软件事件块类型和长度字段的八个字节，加上随后的数据字节数。
代理 UUID (Agent UUID)	uint8[16]	报告恶意软件事件的面向终端的 AMP 代理的内部唯一 ID。
云 UUID (Cloud UUID)	uint8[16]	发生恶意软件事件的恶意软件感知网络的内部唯一 ID。
恶意软件事件时间戳 (Malware Event Timestamp)	uint32	恶意软件事件生成时间戳。
事件类型 ID (Event Type ID)	uint32	恶意软件事件类型的内部 ID。

表 B-12 用于 5.3 的恶意软件事件数据块字段 （续）

字段	数据类型	说明
事件子类型 ID (Event Subtype ID)	uint32	导致恶意软件检测的操作的内部 ID。
检测器 ID (Detector ID)	uint8	检测到恶意软件的检测技术的内部 ID。
字符串块类型 (String Block Type)	uint32	启动包含检测名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	检测名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 检测名称 ”(Detection Name) 字段中的字节数。
检测名称 (Detection Name)	字符串	检测到或被隔离的恶意软件的名称。
字符串块类型 (String Block Type)	uint32	启动包含用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 用户 ”(User) 字段中的字节数。
用户 (User)	字符串	安装 Cisco 代理并发生恶意软件事件的计算机的用户。请注意，这些用户未绑定到用户发现。
字符串块类型 (String Block Type)	uint32	启动包含文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 文件名 ”(File Name) 字段中的字节数。
文件名 (File Name)	字符串	被检测或隔离的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含文件路径的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件路径字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 文件路径 ”(File Path) 字段中的字节数。
文件路径 (File Path)	字符串	被检测或隔离的文件的文件路径，不包括文件名。
字符串块类型 (String Block Type)	uint32	启动包含文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Type)	uint32	文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 文件 SHA 散列 ”(File SHA Hash) 字段中的字节数。
文件 SHA 散列 (File SHA Hash)	字符串	被检测或隔离的文件 SHA-256 散列值的呈现字符串。
文件大小 (File Size)	uint32	被检测或隔离的文件的大小 （字节）。
文件类型 (File Type)	uint8	被检测或隔离文件的文件类型。此字段的含义在随此事件提供的元数据中传输。有关详细信息，请参阅面向终端的 AMP 文件类型元数据，第 3-39 页。
文件时间戳 (File Timestamp)	uint32	创建被检测或隔离的文件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。

表 B-12　用于 5.3 的恶意软件事件数据块字段 （续）

字段	数据类型	说明
字符串块类型 (String Block Type)	uint32	启动包含父文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 父文件名 ”(Parent File Name) 字段中的字节数。
父文件名 (Parent File Name)	字符串	检测期间访问被检测或隔离文件的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含父文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 父文件 SHA 散列 ” (Parent File SHA Hash) 字段中的字节数。
父文件 SHA 散列 (Parent File SHA Hash)	字符串	检测期间访问被检测或隔离文件的父文件的 SHA-256 哈希值。
字符串块类型 (String Block Type)	uint32	启动包含事件说明的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	事件说明字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 事件说明 ”(Event Description) 字段中的字节数。
活动说明 (Event Description)	字符串	与事件类型相关的其他事件信息。
设备 ID (Device ID)	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或 IDS 事件相关联。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接事件时间戳 (Connection Event Timestamp)	uint32	连接事件的时间戳。
方向 (Direction)	uint8	表示文件是否已上传或下载。可能会有以下值： • 1 - 下载 • 2 - 上传 目前该值取决于协议 （例如，如果连接是 HTTP，则其值为 Download）。
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标 IP 地址 (Destination IP Address)	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。

表 B-12 用于 5.3 的恶意软件事件数据块字段 （续）

字段	数据类型	说明
用户 ID (User ID)	uint32	系统识别的登录目标主机的用户的标识号。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	作为触发事件的访问控制策略的唯一标识符的标别号。
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括： • 1 - CLEAN 文件是安全的，不包含恶意软件。 • 2 - UNKNOWN 不确定文件是否包含恶意软件。 • 3 - MALWARE 文件包含恶意软件。 • 4 - UNAVAILABLE 软件无法向 Cisco 云发送请求以了解处置情况，或 Cisco 云服务未响应此请求。 • 5 - CUSTOM SIGNATURE 文件与用户定义的散列匹配，并且以用户指定的方式进行处理。
追溯处置情况 (Retrospective Disposition)	uint8	处置情况更新后的处置情况。如果处置情况未更新，则此字段包含的值与 “ 处置情况 ”(Disposition) 字段包含的值相同。可能值与 “ 处置情况 ”(Disposition) 字段包含的值相同。
字符串块类型 (String Block Type)	uint32	启动包含 URI 的字符串数据块。值始终为 0。
字符串块长度 (String Block Type)	uint32	URI 数据块中的字节数，包括块类型和报头字段的八个字节，加上 URI 字段中的字节数。
URI	字符串	连接的 URI。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。
源国家 / 地区 (Source Country)	uint16	源主机的国家 / 地区代码。
目标国家 / 地区 (Destination Country)	uint 16	目标主机的国家 / 地区代码。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号 （如适用）。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号 （如适用）。
操作 (Action)	uint8	根据文件类型对文件执行的操作。可能会有以下值： • 1 - 检测 • 2 - 阻止 • 3 - 恶意软件云查找 • 4 - 恶意软件阻止 • 5 - 恶意软件允许列表

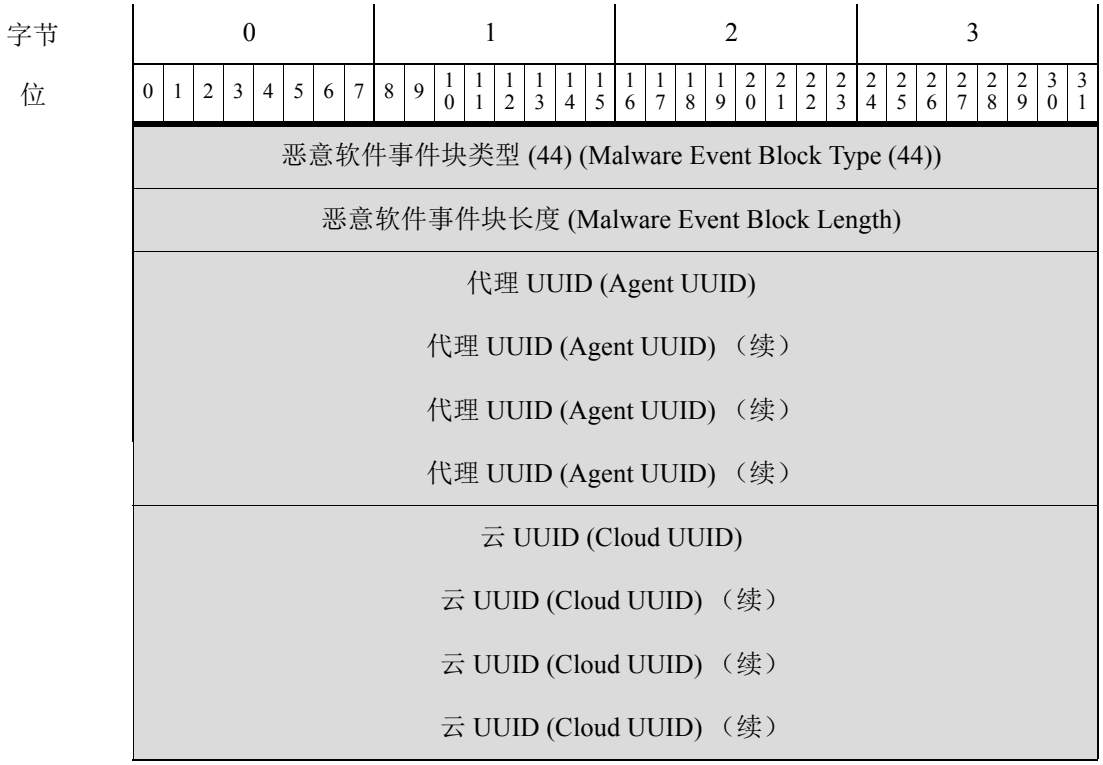
表 B-12　用于 5.3 的恶意软件事件数据块字段 （续）

字段	数据类型	说明
协议 (Protocol)	uint8	用户指定的 IANA 协议号。例如： • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP 目前仅限 TCP。
威胁评分 (Threat Score)	uint8	0 到 100 之间的数值，基于在动态分析期间观察到的潜在恶意行为而打出。
IOC 编号 (IOC Number)	uint16	与此事件相关的危害的 ID 号码。

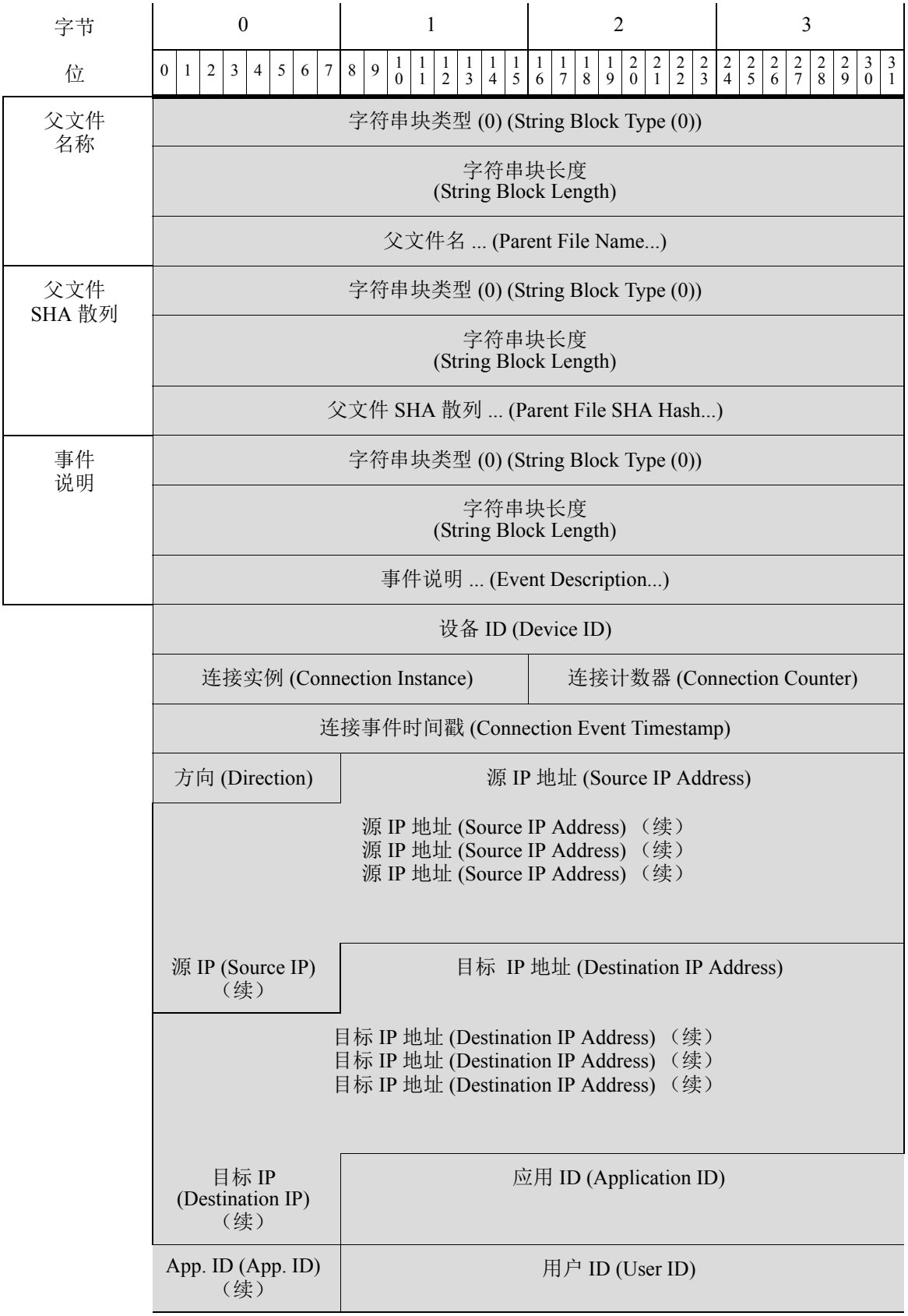
恶意软件事件数据块 5.3.1

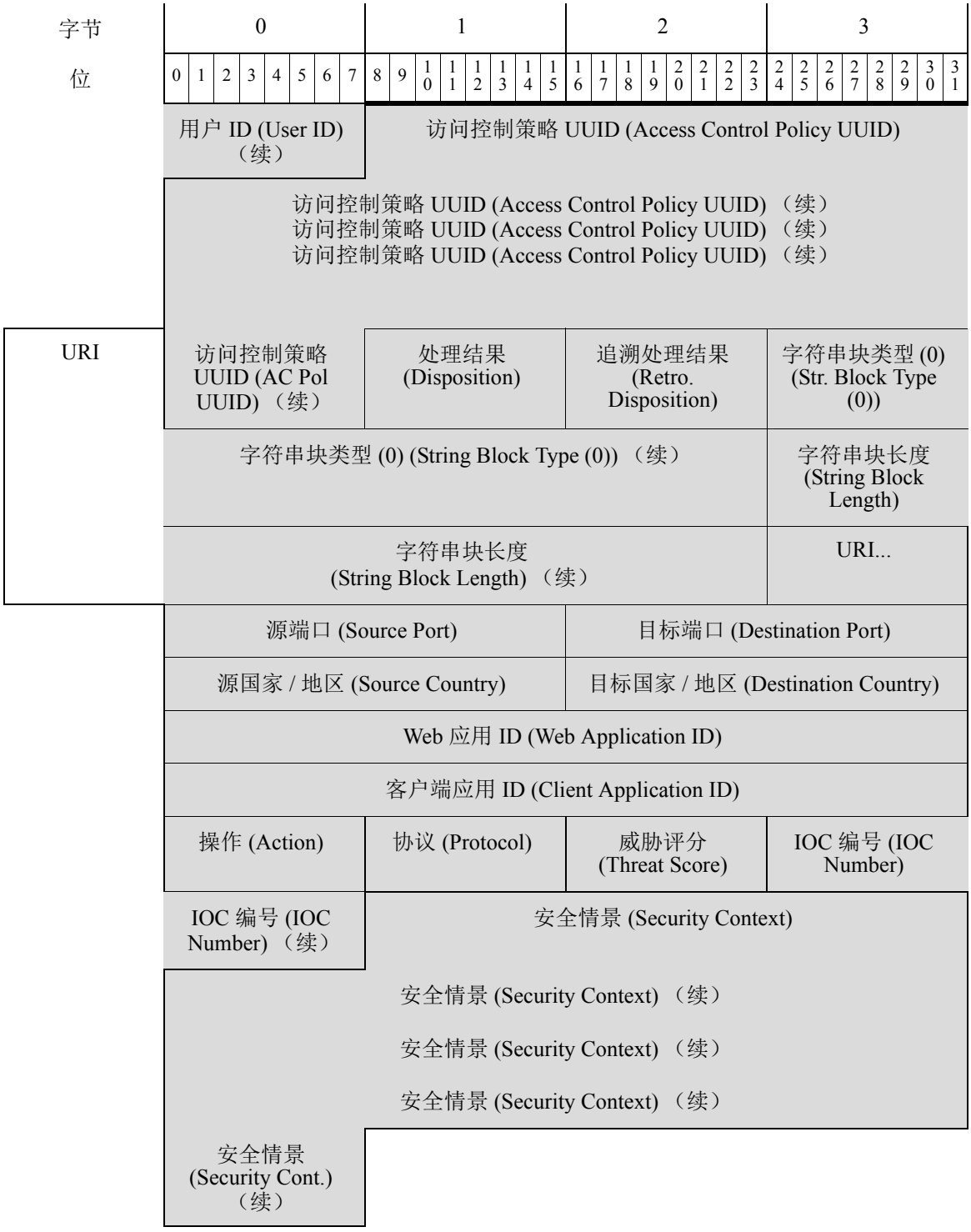
eStreamer 服务使用恶意软件事件数据块存储有关恶意软件事件的信息。这些事件包含关于在云内检测到或被隔离的恶意软件、检测方法以及受恶意软件影响的主机和用户的信息。恶意软件事件数据块的块类型为系列 2 数据块组中的 44。它替代了块 35。您可以通过在事件版本为 5 且事件代码为 101 的请求消息中设置恶意软件事件标志 （“ 请求标志 ”(Request Flags) 字段中的位 30），将该事件作为恶意软件事件记录的一部分进行请求。

下图显示恶意软件事件数据块的结构：



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	恶意软件事件时间戳 (Malware Event Timestamp)																															
	事件类型 ID (Event Type ID)																															
	事件子类型 ID (Event Subtype ID)																															
检测名称 (Detection Name)	检测器 ID (Detector ID)								字符串块类型 (0) (String Block Type (0))																							
	字符串块类型 (0) (String Block Type (0)) （续）								字符串块长度 (String Block Length)																							
	字符串块长度 (String Block Length) （续）								检测名称 ... (Detection Name...)																							
用户	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户 ... (User...)																															
文件名	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件名 ... (File Name...)																															
文件路径	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件路径 ... (File Path...)																															
文件 SHA 哈希	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件 SHA 散列 ... (File SHA Hash...)																															
	文件大小 (File Size)																															
	文件类型 (File Type)																															
	文件时间戳 (File Timestamp)																															


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
父文件名称
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
父文件名 ... (Parent File Name...)
父文件 SHA 散列
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
父文件 SHA 散列 ... (Parent File SHA Hash...)
事件说明
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
事件说明 ... (Event Description...)
设备 ID (Device ID)
连接实例 (Connection Instance)
连接计数器 (Connection Counter)
连接事件时间戳 (Connection Event Timestamp)
方向 (Direction)
源 IP 地址 (Source IP Address)
源 IP 地址 (Source IP Address) （续）
源 IP 地址 (Source IP Address) （续）
源 IP 地址 (Source IP Address) （续）
源 IP (Source IP) （续）
目标 IP 地址 (Destination IP Address)
目标 IP 地址 (Destination IP Address) （续）
目标 IP 地址 (Destination IP Address) （续）
目标 IP 地址 (Destination IP Address) （续）
目标 IP (Destination IP) （续）
应用 ID (Application ID)
App. ID (App. ID) （续）
用户 ID (User ID)



下表对恶意软件事件数据块中的字段进行了说明。

表 B-13　用于 5.3.1 的恶意软件事件数据块字段

字段	数据类型	说明
恶意软件事件块类型 (Malware Event Block Type)	uint32	启动恶意软件事件数据块。值始终为 44。
恶意软件事件块长度 (Malware Event Block Length)	uint32	恶意软件事件数据块中的字节总数，包括恶意软件事件块类型和长度字段的八个字节，加上随后的数据字节数。
代理 UUID (Agent UUID)	uint8[16]	报告恶意软件事件的面向终端的 AMP 代理的内部唯一 ID。
云 UUID (Cloud UUID)	uint8[16]	发生恶意软件事件的 思科高级恶意软件防护云的内部唯一 ID。
恶意软件事件时间戳 (Malware Event Timestamp)	uint32	恶意软件事件生成时间戳。
事件类型 ID (Event Type ID)	uint32	恶意软件事件类型的内部 ID。
事件子类型 ID (Event Subtype ID)	uint32	导致恶意软件检测的操作的内部 ID。
检测器 ID (Detector ID)	uint8	检测到恶意软件的检测技术的内部 ID。
字符串块类型 (String Block Type)	uint32	启动包含检测名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	检测名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 检测名称 ”(Detection Name) 字段中的字节数。
检测名称 (Detection Name)	字符串	检测到或被隔离的恶意软件的名称。
字符串块类型 (String Block Type)	uint32	启动包含用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 用户 ”(User) 字段中的字节数。
用户 (User)	字符串	安装代理思科高级恶意软件防护云发生恶意软件事件的计算机的用户。请注意，这些用户未绑定到用户发现。
字符串块类型 (String Block Type)	uint32	启动包含文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 文件名 ”(File Name) 字段中的字节数。
文件名 (File Name)	字符串	被检测或隔离的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含文件路径的字符串数据块。值始终为 0。

表 B-13 用于 5.3.1 的恶意软件事件数据块字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Type)	uint32	文件路径字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 文件路径 ”(File Path) 字段中的字节数。
文件路径 (File Path)	字符串	被检测或隔离的文件的文件路径，不包括文件名。
字符串块类型 (String Block Type)	uint32	启动包含文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Type)	uint32	文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 文件 SHA 散列 ”(File SHA Hash) 字段中的字节数。
文件 SHA 散列 (File SHA Hash)	字符串	被检测或隔离的文件 SHA-256 散列值的呈现字符串。
文件大小 (File Size)	uint32	被检测或隔离的文件的大小 （字节）。
文件类型 (File Type)	uint8	被检测或隔离文件的文件类型。此字段的含义在随此事件提供的元数据中传输。有关详细信息，请参阅面向终端的 AMP 文件类型元数据，第 3-39 页。
文件时间戳 (File Timestamp)	uint32	创建被检测或隔离的文件的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）。
字符串块类型 (String Block Type)	uint32	启动包含父文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 父文件名 ”(Parent File Name) 字段中的字节数。
父文件名 (Parent File Name)	字符串	检测期间访问被检测或隔离文件的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含父文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 父文件 SHA 散列 ” (Parent File SHA Hash) 字段中的字节数。
父文件 SHA 散列 (Parent File SHA Hash)	字符串	检测期间访问被检测或隔离文件的父文件的 SHA-256 哈希值。
字符串块类型 (String Block Type)	uint32	启动包含事件说明的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	事件说明字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 事件说明 ”(Event Description) 字段中的字节数。
活动说明 (Event Description)	字符串	与事件类型相关的其他事件信息。
设备 ID (Device ID)	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或 IDS 事件相关联。

表 B-13　用于 5.3.1 的恶意软件事件数据块字段 （续）

字段	数据类型	说明
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接事件时间戳 (Connection Event Timestamp)	uint32	连接事件的时间戳。
方向 (Direction)	uint8	表示文件是否已上传或下载。可能会有以下值： • 1 - 下载 • 2 - 上传 目前该值取决于协议 （例如，如果连接是 HTTP，则其值为 Download）。
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标 IP 地址 (Destination IP Address)	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。
用户 ID (User ID)	uint32	系统识别的登录目标主机的用户的标识号。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	作为触发事件的访问控制策略的唯一标识符的标别号。
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括： • 1 - CLEAN 文件是安全的，不包含恶意软件。 • 2 - UNKNOWN 不确定文件是否包含恶意软件。 • 3 - MALWARE 文件包含恶意软件。 • 4 - UNAVAILABLE 软件无法向 Cisco 云发送请求以了解处置情况，或 Cisco 云服务未响应此请求。 • 5 - CUSTOM SIGNATURE 文件与用户定义的散列匹配，并且以用户指定的方式进行处理。
追溯处置情况 (Retrospective Disposition)	uint8	处置情况更新后的处置情况。如果处置情况未更新，则此字段包含的值与 “ 处置情况 ”(Disposition) 字段包含的值相同。可能值与 “ 处置情况 ”(Disposition) 字段包含的值相同。
字符串块类型 (String Block Type)	uint32	启动包含 URI 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	URI 数据块中的字节数，包括块类型和报头字段的八个字节，加上 URI 字段中的字节数。
URI	字符串	连接的 URI。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。

表 B-13 用于 5.3.1 的恶意软件事件数据块字段 （续）

字段	数据类型	说明
源国家 / 地区 (Source Country)	uint16	源主机的国家 / 地区代码。
目标国家 / 地区 (Destination Country)	uint 16	目标主机的国家 / 地区代码。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号 （如适用）。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号 （如适用）。
操作 (Action)	uint8	根据文件类型对文件执行的操作。可能会有以下值： • 1 - 检测 • 2 - 阻止 • 3 - 恶意软件云查找 • 4 - 恶意软件阻止 • 5 - 恶意软件允许列表
协议 (Protocol)	uint8	用户指定的 IANA 协议号。例如： • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP 目前仅限 TCP。
威胁评分 (Threat Score)	uint8	0 到 100 之间的数值，基于在动态分析期间观察到的潜在恶意行为而打出。
IOC 编号 (IOC Number)	uint16	与此事件相关的危害的 ID 号码。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景 （虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。

恶意软件事件数据块 5.4.x

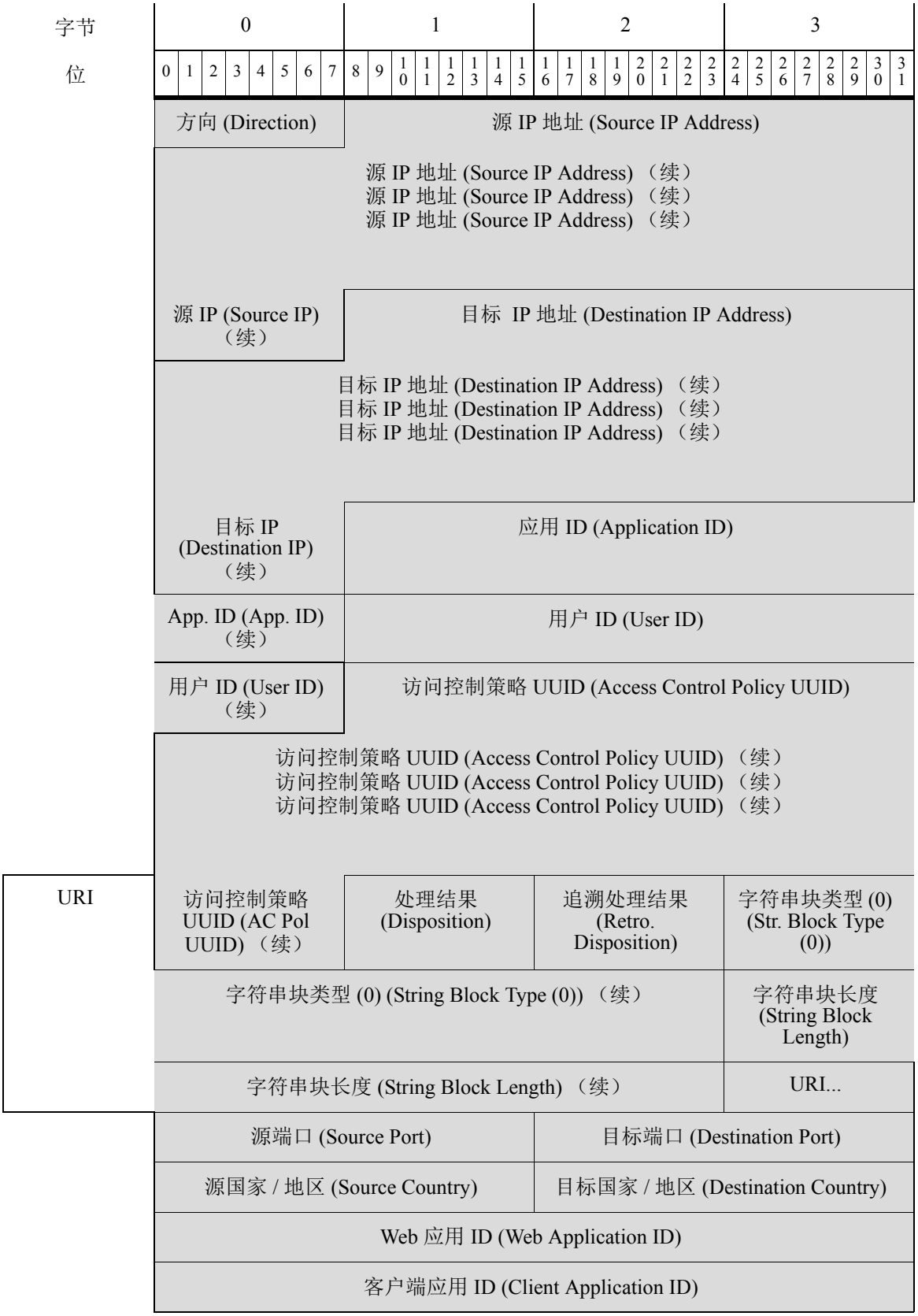
eStreamer 服务使用恶意软件事件数据块存储有关恶意软件事件的信息。这些事件包含关于在云内检测到或被隔离的恶意软件、检测方法以及受恶意软件影响的主机和用户的信息。恶意软件事件数据块的块类型为系列 2 数据块组中的 47。它替代了块 44，然后被块替代。已添加用于 SSL 和文件存档支持的字段。

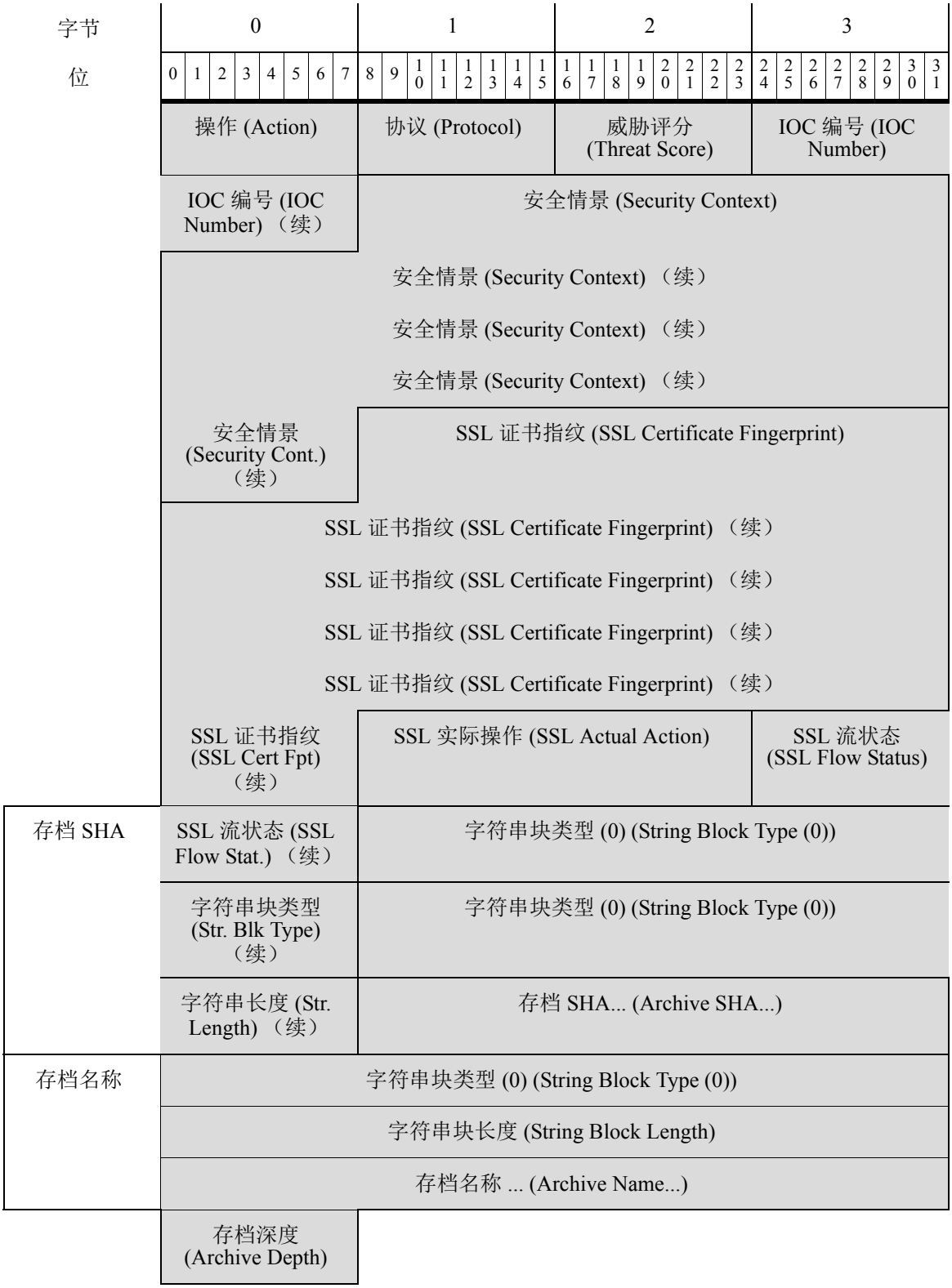
您可以通过在事件版本为 6 且事件代码为 101 的请求消息中设置恶意软件事件标志 （“ 请求标志 ”(Request Flags) 字段中的位 30），将该事件作为恶意软件事件记录的一部分进行请求。

下图显示恶意软件事件数据块的结构：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	恶意软件事件块类型 (47) (Malware Event Block Type (47))																															
	恶意软件事件块长度 (Malware Event Block Length)																															
	代理 UUID (Agent UUID)																															
	代理 UUID (Agent UUID) （续）																															
	代理 UUID (Agent UUID) （续）																															
	代理 UUID (Agent UUID) （续）																															
	云 UUID (Cloud UUID)																															
	云 UUID (Cloud UUID) （续）																															
	云 UUID (Cloud UUID) （续）																															
	云 UUID (Cloud UUID) （续）																															
	恶意软件事件时间戳 (Malware Event Timestamp)																															
	事件类型 ID (Event Type ID)																															
	事件子类型 ID (Event Subtype ID)																															
检测名称 (Detection Name)	检测器 ID (Detector ID)								字符串块类型 (0) (String Block Type (0))																							
	字符串块类型 (0) (String Block Type (0)) （续）								字符串块长度 (String Block Length)																							
	字符串块长度 (String Block Length) （续）								检测名称 ... (Detection Name...)																							
用户	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户 ... (User...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
文件名	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件名 ... (File Name...)																															
文件路径	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件路径 ... (File Path...)																															
文件 SHA 哈希	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件 SHA 散列 ... (File SHA Hash...)																															
	文件大小 (File Size)																															
	文件类型 (File Type)																															
	文件时间戳 (File Timestamp)																															
父文件名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	父文件名 ... (Parent File Name...)																															
父文件 SHA 散列	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	父文件 SHA 散列 ... (Parent File SHA Hash...)																															
事件说明	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	事件说明 ... (Event Description...)																															
	设备 ID (Device ID)																															
	连接实例 (Connection Instance)																连接计数器 (Connection Counter)															
	连接事件时间戳 (Connection Event Timestamp)																															


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
方向 (Direction)
源 IP 地址 (Source IP Address)
源 IP 地址 (Source IP Address) （续）
源 IP 地址 (Source IP Address) （续）
源 IP 地址 (Source IP Address) （续）
源 IP (Source IP) （续）
目标 IP 地址 (Destination IP Address)
目标 IP 地址 (Destination IP Address) （续）
目标 IP 地址 (Destination IP Address) （续）
目标 IP 地址 (Destination IP Address) （续）
目标 IP (Destination IP) （续）
应用 ID (Application ID)
App. ID (App. ID) （续）
用户 ID (User ID)
用户 ID (User ID) （续）
访问控制策略 UUID (Access Control Policy UUID)
访问控制策略 UUID (Access Control Policy UUID) （续）
访问控制策略 UUID (Access Control Policy UUID) （续）
访问控制策略 UUID (Access Control Policy UUID) （续）
URI
访问控制策略 UUID (AC Pol UUID) （续）
处理结果 (Disposition)
追溯处理结果 (Retro. Disposition)
字符串块类型 (0) (Str. Block Type (0))
字符串块类型 (0) (String Block Type (0)) （续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length) （续）
URI...
源端口 (Source Port)
目标端口 (Destination Port)
源国家 / 地区 (Source Country)
目标国家 / 地区 (Destination Country)
Web 应用 ID (Web Application ID)
客户端应用 ID (Client Application ID)



下表对恶意软件事件数据块中的字段进行了说明。

表 B-14　　用于 5.4.x 的恶意软件事件数据块字段

字段	数据类型	说明
恶意软件事件块类型 (Malware Event Block Type)	uint32	启动恶意软件事件数据块。值始终为 47。
恶意软件事件块长度 (Malware Event Block Length)	uint32	恶意软件事件数据块中的字节总数，包括恶意软件事件块类型和长度字段的八个字节，加上随后的数据字节数。
代理 UUID (Agent UUID)	uint8[16]	报告恶意软件事件的面向终端的 AMP 代理的内部唯一 ID。
云 UUID (Cloud UUID)	uint8[16]	发生恶意软件事件的 思科高级恶意软件防护云的内部唯一 ID。
恶意软件事件时间戳 (Malware Event Timestamp)	uint32	恶意软件事件生成时间戳。
事件类型 ID (Event Type ID)	uint32	恶意软件事件类型的内部 ID。
事件子类型 ID (Event Subtype ID)	uint32	导致恶意软件检测的操作的内部 ID。
检测器 ID (Detector ID)	uint8	检测到恶意软件的检测技术的内部 ID。
字符串块类型 (String Block Type)	uint32	启动包含检测名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Type)	uint32	检测名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 检测名称 ”(Detection Name) 字段中的字节数。
检测名称 (Detection Name)	字符串	检测到或被隔离的恶意软件的名称。
字符串块类型 (String Block Type)	uint32	启动包含用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 用户 ”(User) 字段中的字节数。
用户	字符串	安装 Cisco 代理并发生恶意软件事件的计算机的用户。请注意，这些用户未绑定到用户发现。
字符串块类型 (String Block Type)	uint32	启动包含文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 文件名 ”(File Name) 字段中的字节数。
文件名 (File Name)	字符串	被检测或隔离的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含文件路径的字符串数据块。值始终为 0。

表 B-14 用于 5.4.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Length)	uint32	文件路径字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 文件路径 ”(File Path) 字段中的字节数。
文件路径 (File Path)	字符串	被检测或隔离的文件的文件路径，不包括文件名。
字符串块类型 (String Block Type)	uint32	启动包含文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 文件 SHA 散列 ”(File SHA Hash) 字段中的字节数。
文件 SHA 散列 (File SHA Hash)	字符串	被检测或隔离的文件 SHA-256 散列值的呈现字符串。
文件大小 (File Size)	uint32	被检测或隔离的文件的大小 （字节）。
文件类型 (File Type)	uint8	被检测或隔离文件的文件类型。此字段的含义在随此事件提供的元数据中传输。有关详细信息，请参阅面向终端的 AMP 文件类型元数据，第 3-39 页。
文件时间戳 (File Timestamp)	uint32	创建被检测或隔离的文件的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）。
字符串块类型 (String Block Type)	uint32	启动包含父文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 父文件名 ”(Parent File Name) 字段中的字节数。
父文件名 (Parent File Name)	字符串	检测期间访问被检测或隔离文件的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含父文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 父文件 SHA 散列 ” (Parent File SHA Hash) 字段中的字节数。
父文件 SHA 散列 (Parent File SHA Hash)	字符串	检测期间访问被检测或隔离文件的父文件的 SHA-256 哈希值。
字符串块类型 (String Block Type)	uint32	启动包含事件说明的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	事件说明字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 事件说明 ”(Event Description) 字段中的字节数。
活动说明 (Event Description)	字符串	与事件类型相关的其他事件信息。
设备 ID (Device ID)	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或 IDS 事件相关联。

表 B-14　用于 5.4.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接事件时间戳 (Connection Event Timestamp)	uint32	连接事件的时间戳。
方向 (Direction)	uint8	表示文件是否已上传或下载。可能会有以下值： • 1 - 下载 • 2 - 上传 目前该值取决于协议 （例如，如果连接是 HTTP，则其值为 Download）。
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标 IP 地址 (Destination IP Address)	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 号码。
用户 ID (User ID)	uint32	系统识别的登录目标主机的用户的标识号。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	作为触发事件的访问控制策略的唯一标识符的标别号。
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括： • 1 - CLEAN 文件是安全的，不包含恶意软件。 • 2 - UNKNOWN 不确定文件是否包含恶意软件。 • 3 - MALWARE 文件包含恶意软件。 • 4 - UNAVAILABLE 软件无法向 Cisco 云发送请求以了解处置情况，或 Cisco 云服务未响应此请求。 • 5 - CUSTOM SIGNATURE 文件与用户定义的散列匹配，并且以用户指定的方式进行处理。
追溯处置情况 (Retrospective Disposition)	uint8	处置情况更新后的处置情况。如果处置情况未更新，则此字段包含的值与 “ 处置情况 ”(Disposition) 字段包含的值相同。可能值与 “ 处置情况 ”(Disposition) 字段包含的值相同。
字符串块类型 (String Block Type)	uint32	启动包含 URI 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	URI 数据块中的字节数，包括块类型和报头字段的八个字节，加上 URI 字段中的字节数。
URI	字符串	连接的 URI。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。

表 B-14 用于 5.4.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明
源国家 / 地区 (Source Country)	uint16	源主机的国家 / 地区代码。
目标国家 / 地区 (Destination Country)	uint 16	目标主机的国家 / 地区代码。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号 （如适用）。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号 （如适用）。
操作 (Action)	uint8	根据文件类型对文件执行的操作。可能会有以下值： • 1 - 检测 • 2 - 阻止 • 3 - 恶意软件云查找 • 4 - 恶意软件阻止 • 5 - 恶意软件允许列表 • 6 - 云查找超时 • 7 - 自定义检测 • 8 - 自定义检测阻止 • 9 - 存档阻止 （超出深度） • 10 - 存档阻止 （已加密） • 11 - 存档阻止 （检查失败）
协议 (Protocol)	uint8	用户指定的 IANA 协议号。例如： • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP 目前仅限 TCP。
威胁评分 (Threat Score)	uint8	0 到 100 之间的数值，基于在动态分析期间观察到的潜在恶意行为而打出。
IOC 编号 (IOC Number)	uint16	与此事件相关的危害的 ID 号码。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景 （虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。

表 B-14　用于 5.4.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括： • 0 -‘ 未知 ’ • 1 -‘ 请勿解密 ’ • 2 -‘ 阻止 ’ • 3 -‘ 阻止并重置 ’ • 4 -‘ 解密 （已知密钥） ’ • 5 -‘ 解密 （更换秘钥） ’ • 6 -‘ 解密 （放弃） ’

表 B-14 用于 5.4.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明
SSL 流状态 (SSL Flow Status)	uint16	SSL 流量的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括： • 0 -‘ 未知 ’ • 1 -‘ 不匹配 ’ • 2 -‘ 成功 ’ • 3 -‘ 非缓存会话 ’ • 4 -‘ 未知密码套件 ’ • 5 -‘ 不受支持的密码套件 ’ • 6 -‘ 不受支持的 SSL 版本 ’ • 7 -‘ 使用的 SSL 压缩 ’ • 8 -‘ 在被动模式中无法解密的会话 ’ • 9 -‘ 握手错误 ’ • 10 -‘ 解密错误 ’ • 11 -‘ 待处理服务器名称分类查找 ’ • 12 -‘ 待处理通用名称分类查找 ’ • 13 -‘ 内部错误 ’ • 14 -‘ 网络参数不可用 ’ • 15 -‘ 服务器证书处理无效 ’ • 16 -‘ 服务器证书指纹不可用 ’ • 17 -‘ 无法缓存持有者 DN’ • 18 -‘ 无法缓存颁发者 DN’ • 19 -‘ 未知 SSL 版本 ’ • 20 -‘ 外部证书列表不可用 ’ • 21 -‘ 外部证书指纹不可用 ’ • 22 -‘ 内部证书列表无效 ’ • 23 -‘ 内部证书列表不可用 ’ • 24 -‘ 内部证书不可用 ’ • 25 -‘ 内部证书指纹不可用 ’ • 26 -‘ 服务器证书验证不可用 ’ • 27 -‘ 服务器证书验证失败 ’ • 28 -‘ 操作无效 ’
字符串块类型 (String Block Type)	uint32	启动包含存档 SHA 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	存档 SHA 字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上入侵策略名称中的字节数。

表 B-14　用于 5.4.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明
存档 SHA (Archive SHA)	字符串	包含该文件的父存档的 SHA1 散列。
字符串块类型 (String Block Type)	uint32	启动包含 “ 存档名称 ”(Archive Name) 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	存档名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上入侵策略名称中的字节数。
存档名称 (Archive Name)	字符串	父存档的名称。
存档深度 (Archive Depth)	uint8	嵌套文件的层数。例如，如果文本文件位于压缩存档中，则此值为 1。

旧版发现数据结构

旧版发现事件报头

发现事件报头 5.0 - 5.1.1.x

发现和连接事件消息包含发现事件报头。它传送事件的类型和子类型、事件发生的时间、出现该事件的设备以及消息中事件数据的结构。报头后面是实际主机发现、用户或连接事件数据。按事件类型划分的主机发现结构，第 4-44 页中介绍了与不同事件类型 / 子类型值相关的结构。

发现事件报头的事件类型和事件子类型字段用于识别传输的事件消息的结构。一旦确定事件数据块的结构，您的程序即可对消息进行适当解析。

下图中的阴影行举例说明了发现事件报头的格式。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	报头版本 (1) (Header Version (1))																消息类型 (4) (Message Type (4))															
	消息长度 (Message Length)																															
	Netmap ID																记录类型 (Record Type)															

	记录长度 (Record Length)	
	eStreamer 服务器时间戳 (eStreamer Server Timestamp) （在事件中，只有当位 23 已设置时）	
	留作未来使用 (Reserved for Future Use)（在事件中，只有当位 23 已设置时）	
发现事件报头 (Discovery Event Header)	设备 ID (Device ID)	
	IP 地址	
	MAC 地址 (MAC Address)	
	MAC 地址 (MAC Address)（续）	留作未来使用 (Reserved for future use)
	事件秒 (Event Second)	
	事件微秒 (Event Microsecond)	
	保留（内部） (Reserved (Internal))	事件类型 (Event Type)
	事件子类型 (Event Subtype)	
	文件编号 (File Number)（仅限内部使用）	
	文件位置 (File Position)（仅限内部使用）	

下表对发现事件报头进行了说明。

表 B-15 发现事件报头字段

字段	数据类型	说明
设备 ID (Device ID)	uint32	生成发现事件的设备的 ID 号码。您可以通过请求版本 3 和版本 4 元数据获取设备的元数据。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
IP 地址	uint32	事件所涉及主机的 IP 地址。
MAC 地址 (MAC Address)	uint8[6]	事件所涉及主机的 MAC 地址。
留作未来使用 (Reserved for future use)	byte[2]	值设置为 0 的两个字节的填充。
事件秒 (Event Second)	uint32	系统生成事件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
事件微秒 (Event Microsecond)	uint32	系统生成事件的微秒（一秒的百万分之一）增量。

表 B-15　　发现事件报头字段 （续）

字段	数据类型	说明
保留 （内部） (Reserved (Internal))	字节	源自 Cisco 的内部数据，可忽略。
事件类型 (Event Type)	uint32	事件类型（新事件为 1000，变更事件为 1001，用户输入事件为 1002，完整主机配置文件为 1050）。有关可用事件类型列表，请参阅按事件类型划分的主机发现结构，第 4-44 页。
事件子类型 (Event Subtype)	uint32	事件子类型。有关可用事件子类型列表，请参阅按事件类型划分的主机发现结构，第 4-44 页。
文件编号 (File Number)	byte[4]	串行文件编号。此字段供 Cisco 内部使用，可以忽略。
文件位置 (File Position)	byte[4]	事件在串行文件中的位置。此字段供 Cisco 内部使用，可以忽略。

旧版服务器数据块

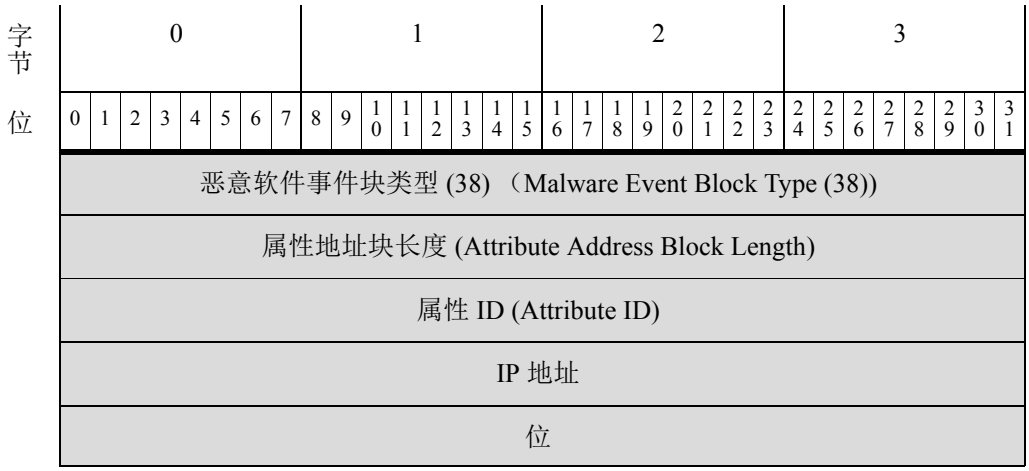
有关详细信息，请参阅以下各节：

- 用于 5.0 - 5.1.1.x 的属性地址数据块，第 B-93 页

用于 5.0 - 5.1.1.x 的属性地址数据块

属性地址数据块包含一个属性列表项目，在属性定义数据块中使用。它的块类型为 38。

下图显示属性地址数据块的基本结构：



下表对属性地址数据块的字段进行了说明。

表 B-16　　属性地址数据块字段

字段	数据类型	说明
属性地址块类型 (Attribute Address Block Type)	uint32	启动属性地址数据块。值始终为 38。
属性地址块长度 (Attribute Address Block Length)	uint32	属性地址数据块中的字节数，包括属性地址块类型和长度字段的八个字节，加上随后的属性地址数据的字节数。
属性 ID (Attribute ID)	uint32	受影响属性的标识号 （如适用）。
IP 地址 (IP Addresses)	uint8[4]	主机的 IP 地址 （如果地址已自动分配），采用 IP 地址八位组。
位 (Bit)	uint32	如果已自动分配 IP 地址，则包含用于计算网络掩码的有效位。

旧版客户端应用数据块

有关详细信息，请参阅以下各节：

- 用于 5.0 - 5.1 的用户客户端应用数据块，第 B-94 页

用于 5.0 - 5.1 的用户客户端应用数据块

用户客户端应用数据块包含客户端应用数据来源、添加数据的用户的标识号以及 IP 地址范围数据块列表的相关信息。用户客户端应用数据块的块类型为 59。

下图显示用户客户端应用数据块的基本结构：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户客户端应用块类型 (59) （User Client Application Block Type (59)）																															
	用户客户端应用块长度 (User Client Application Block Length)																															
IP 地址范围	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	IP 范围规格数据块 (IP Range Specification Data Blocks)*																															

	应用协议 ID (Application Protocol ID)
	客户端应用 ID (Client Application ID)
版本	字符串块类型 (0) (String Block Type (0))
	字符串块长度 (String Block Length)
	版本 ...(Version...)

下表对用户客户端应用数据块的字段进行了说明。

表 B-17　　用户客户端应用数据块字段

字段	字节数	说明
用户客户端应用块类型 (User Client Application Block Type)	uint32	启动用户客户端应用数据块。值始终为 。
用户客户端应用块长度 (User Client Application Block Length)	uint32	用户客户端应用数据块中的字节总数，包括用户客户端应用块类型和长度字段的八个字节，加上随后的用户客户端应用数据的字节数。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送 IP 地址范围数据的 IP 范围规格数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装 IP 范围规格数据块。
IP 范围规格数据块 (IP Range Specification Data Blocks) *	变量	包含用于用户输入的 IP 地址范围相关信息的 IP 范围规格数据块。有关此数据块的说明，请参阅表 4-59 用户服务器数据块字段，第 4-104 页。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号 （如适用）。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号 （如适用）。
字符串块类型 (String Block Type)	uint32	启动包含客户端应用版本的字符串数据块。值始终为 0。

表 B-17　用户客户端应用数据块字段 （续）

字段	字节数	说明
字符串块长度 (String Block Length)	uint32	客户端应用版本字符串数据块中的字节数，包括字符串块类型和长度字段，加上版本中的字节数。
版本 (Version)	字符串	客户端应用版本。

旧版扫描结果数据块

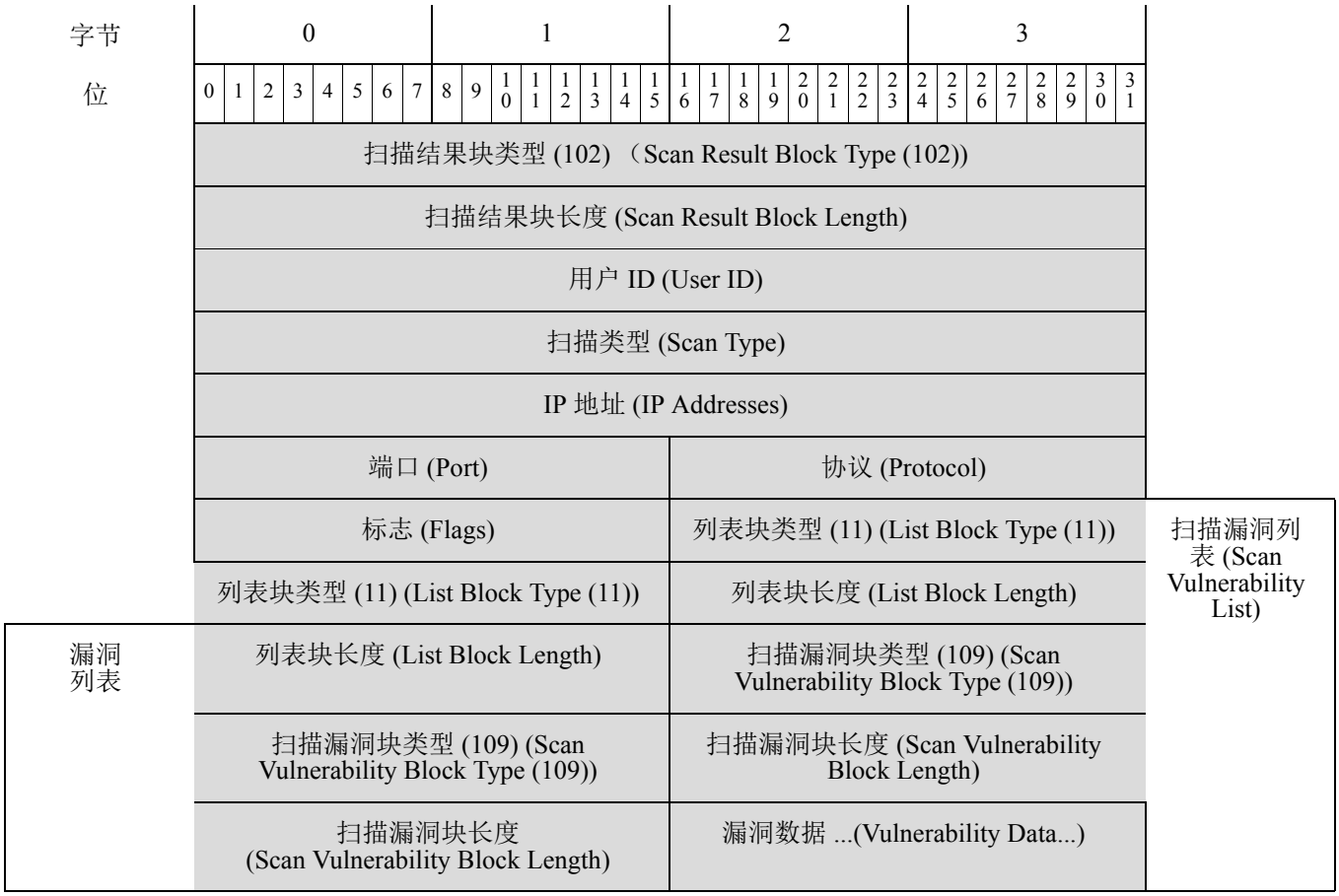
有关详细信息，请参阅以下各节：

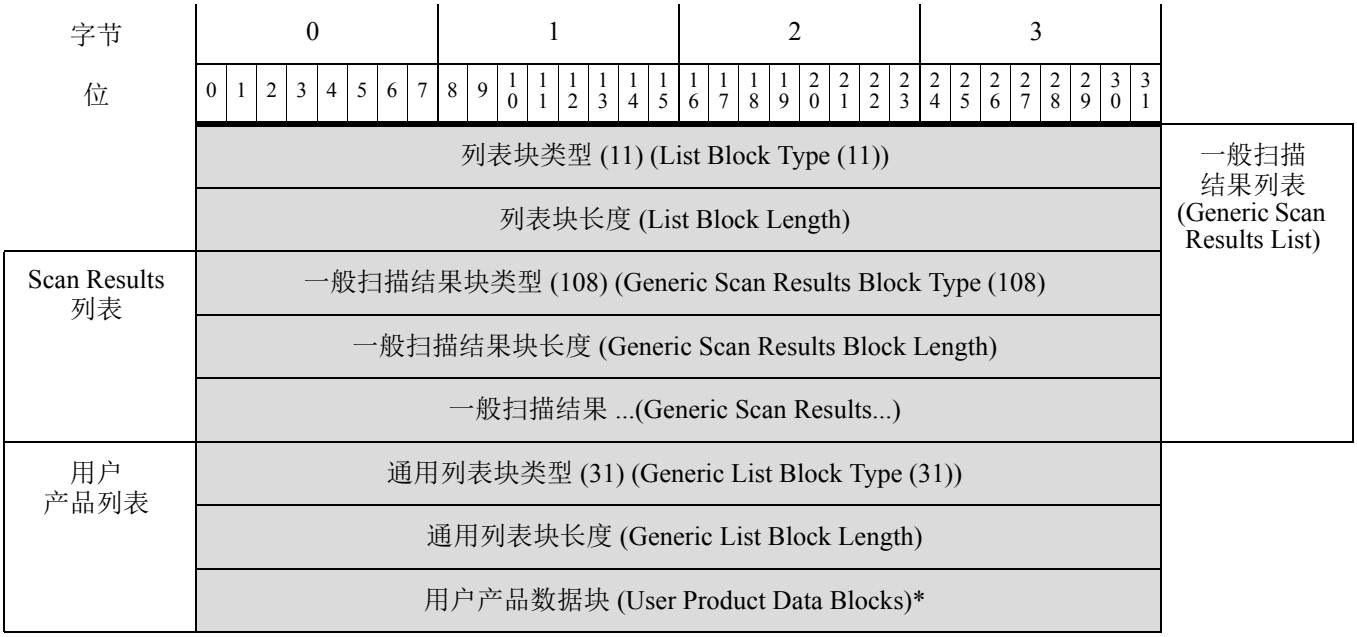
- 扫描结果数据块 5.0 - 5.1.1.x，第 B-96 页
- 用于 5.0.x 的用户产品数据块，第 B-99 页
- 用于 5.x 的用户信息数据块，第 B-120 页

扫描结果数据块 5.0 - 5.1.1.x

扫描结果数据块对漏洞进行说明，在添加扫描结果事件 （事件类型 1002，子类型 11）中使用。扫描结果数据块的块类型为 102。

下图显示扫描结果数据块的格式：





下表对扫描结果数据块的字段进行了说明。

表 B-18　　扫描结果数据块字段

字段	数据类型	说明
扫描结果块类型 (Scan Result Block Type)	uint32	启动扫描结果数据块。值始终为 `102`。
扫描结果块长度 (Scan Result Block Length)	uint32	扫描漏洞数据块中的字节数，包括扫描漏洞块类型和长度字段的八个字节，加上随后的扫描漏洞数据的字节数。
用户 ID (User ID)	uint32	包含导入扫描结果或运行产生该扫描结果的扫描的用户的用户标识号。
扫描类型 (Scan Type)	uint32	表明结果是如何添加到系统中的。
IP 地址 (IP Addresses)	uint32	受结果中的漏洞影响的主机的 IP 地址，采用 IP 地址八位组。
端口 (Port)	uint16	受结果中的漏洞影响的子服务器使用的端口。
协议 (Protocol)	uint16	IANA 协议号。例如： • `1` - ICMP • `4` - IP • `6` - TCP • `17` - UDP
标志 (Flags)	uint16	保留
列表块类型 (List Block Type)	uint32	启动由传送传输扫描漏洞数据的扫描漏洞数据块组成的列表数据块。值始终为 `11`。

表 B-18 扫描结果数据块字段 （续）

字段	数据类型	说明
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装扫描漏洞数据块。 此字段后面是零个或多个扫描漏洞数据块。
扫描漏洞块类型 (Scan Vulnerability Block Type)	uint32	启动对扫描期间检测到的漏洞进行说明的扫描漏洞数据块。值始终为 109。
扫描漏洞块长度 (Scan Vulnerability Block Length)	uint32	扫描漏洞数据块中的字节数，包括扫描漏洞块类型和长度字段的八个字节，加上随后的扫描漏洞数据中的字节数。
漏洞数据 (Vulnerability Data)	字符串	每个漏洞的相关信息。
列表块类型 (List Block Type)	uint32	启动由传送传输扫描漏洞数据的扫描漏洞数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装扫描漏洞数据块。 此字段后面是零个或多个扫描漏洞数据块。
一般扫描结果块类型 (Generic Scan Results Block Type)	uint32	启动对扫描期间检测到的服务器和操作系统数据进行说明的一般扫描结果数据块。值始终为 108。
一般扫描结果块长度 (Generic Scan Results Block Length)	uint32	一般扫描结果数据块中的字节数，包括一般扫描结果块类型和长度字段的八个字节，加上随后的扫描结果数据中的字节数。
一般扫描结果数据 (Generic Scan Results Data)	字符串	每个扫描结果的相关信息。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送第三方应用中的主机输入数据的用户产品数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装用户产品数据块。
用户产品数据块 (User Product Data Blocks) *	变量	包含主机输入数据的用户产品数据块。有关此数据块的说明，请参阅用户产品数据块 5.1+，第 4-176 页。

用于 5.0.x 的用户产品数据块

用户产品数据块传输从第三方应用导入的主机输入数据，包括第三方应用字符串映射。此数据块在连接统计信息数据块 6.0.x，第 B-212 页和用户服务器和操作系统消息，第 4-58 页中使用。在版本 4.10.x 中，用户产品数据块的块类型为 65，在版本 5.0 - 5.0.x 中，其块类型为 118。这两种块类型的结构相同。

注　下图中数据块名称旁边的星号 (*) 表示可能会出现多个数据块实例。

下图显示用户产品数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户产品数据块类型 (65 | 118) (User Product Data Block Type (65 | 118))																															
	用户产品块长度 (User Product Block Length)																															
	源 ID (Source ID)																															
	源类型 (Source Type)																															
IP 地址范围	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	IP 范围规格数据块 (IP Range Specification Data Blocks)*																															
	端口 (Port)																协议 (Protocol)															
	丢弃用户产品 (Drop User Product)																															
自定义供应商字符串 (Custom Vendor String)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	自定义供应商字符串 ...(Custom Vendor String...)																															
自定义产品字符串 (Custom Product String)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	自定义产品字符串 ...(Custom Product String...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
自定义版本字符串 (Custom Version String)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	自定义版本字符串 ...(Custom Version String...)																															
	软件 ID (Software ID)																															
	服务器 ID (Server ID)																															
	供应商 ID (Vendor ID)																															
	产品 ID (Product ID)																															
主版本字符串	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	主版本字符串 ...(Major Version String...)																															
次版本字符串	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	次版本字符串 ...(Minor Version String...)																															
修订字符串	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	修订版字符串 ...(Revision String...)																															
至主版本字符串	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	至主版本字符串 ...(To Major Version String...)																															
至次版本字符串	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	至次版本字符串 ...(To Minor Version String...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
至修订版字符串	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	至修订版字符串 ...(To Revision String...)																															
内部版本字符串 (Build String)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	内部版本字符串 ...(Build String...)																															
修补版本字符串 (Patch String)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	修补版本字符串 ...(Patch String...)																															
分机字符串	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	扩展版本字符串 ...(Extension String...)																															
操作系统 UUID (OS UUID)	操作系统 UUID (Operating System UUID)																															
	操作系统 UUID (Operating System UUID) （续）																															
	操作系统 UUID (Operating System UUID) （续）																															
	操作系统 UUID (Operating System UUID) （续）																															
修复列表 (List of Fixes)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	修复列表数据块 (Fix List Data Blocks)*																															

下表对用户产品数据块的组件进行了说明。

表 B-19 用于 4.10.x、5.0-5.0.x 的用户产品数据块字段

字段	数据类型	说明
用户产品数据块类型 (User Product Data Block Type)	uint32	启动用户产品数据块。在版本 4.10.x 中，此值为 65，在版本 5.0 - 5.0.x 中，此值为 118。
用户产品块长度 (User Product Block Length)	uint32	用户产品数据块中的字节总数，包括用户产品块类型和长度字段的八个字节，加上随后的用户产品数据中的字节数。
源 ID (Source ID)	uint32	导入数据的源的标识号。
源类型 (Source Type)	uint32	提供数据的源的源类型。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送 IP 地址范围数据的 IP 范围规格数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装 IP 范围规格数据块。
IP 范围规格数据块 (IP Range Specification Data Blocks) *	变量	包含用于用户输入的 IP 地址范围相关信息的 IP 范围规格数据块。有关此数据块的说明，请参阅用于 5.2+ 的 IP 地址范围数据块，第 4-96 页。
端口 (Port)	uint16	用户指定的端口。
协议 (Protocol)	uint16	用户指定的 IANA 协议号。例如： • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP
丢弃用户产品 (Drop User Product)	uint32	表示是否已从主机中删除用户操作系统定义： • 0 - 否 • 1 - 是
字符串块类型 (String Block Type)	uint32	启动包含在用户输入中指定的自定义供应商名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	自定义供应商字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上供应商名称中的字节数。
自定义供应商名称 (Custom Vendor Name)	字符串	在用户输入中指定的自定义供应商名称。
字符串块类型 (String Block Type)	uint32	启动包含在用户输入中指定的自定义产品名称的字符串数据块。值始终为 0。

表 B-19　用于 4.10.x、 5.0-5.0.x 的用户产品数据块字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Length)	uint32	自定义产品字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上产品名称中的字节数。
自定义产品名称 (Custom Product Name)	字符串	在用户输入中指定的自定义产品名称。
字符串块类型 (String Block Type)	uint32	启动包含在用户输入中指定的自定义版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	自定义版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上版本中的字节数。
自定义版本 (Custom Version)	字符串	在用户输入中指定的自定义版本。
软件 ID (Software ID)	uint32	Cisco 数据库中服务器或操作系统特定修订版的标识符。
服务器 ID (Server ID)	uint32	在用户输入中指定的主机服务器上的应用协议的 Cisco 应用标识符。
供应商 ID (Vendor ID)	uint32	在第三方操作系统映射到 Cisco 3D 操作系统定义时指定的第三方操作系统的供应商的标识符。
产品 ID (Product ID)	uint32	在第三方操作系统字符串映射到 Cisco 3D 操作系统定义时指定的第三方操作系统字符串的产品标识字符串。
字符串块类型 (String Block Type)	uint32	启动一个字符串数据块，此数据块包含用户输入中第三方操作系统字符串映射到的 Cisco 3D 操作系统定义的主版本号。值始终为 0。
字符串块长度 (String Block Length)	uint32	主版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上版本中的字节数。
主版本 (Major Version)	字符串	第三方操作系统字符串映射到的 Cisco 3D 操作系统定义的主版本。
字符串块类型 (String Block Type)	uint32	启动一个字符串数据块，此数据块包含第三方操作系统字符串映射到的 Cisco 3D 操作系统定义的次版本号。值始终为 0。
字符串块长度 (String Block Length)	uint32	次版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上版本中的字节数。
次版本 (Minor Version)	字符串	用户输入中的第三方操作系统字符串映射到的 Cisco 3D 操作系统定义的次版本号。
字符串块类型 (String Block Type)	uint32	启动包含用户输入中的第三方操作系统字符串映射到的 Cisco 操作系统定义的修订号的字符串数据块。值始终为 0。

表 B-19　　用于 4.10.x、5.0-5.0.x 的用户产品数据块字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Length)	uint32	修订版字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上修订号中的字节数。
修订版 (Revision)	字符串	用户输入中的第三方操作系统字符串映射到的 Cisco 3D 操作系统定义的修订号。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的 Cisco 3D 操作系统定义的最新主版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	至主版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上版本中的字节数。
至主版本 (To Major)	字符串	用户输入中的第三方操作系统字符串映射到的 Cisco 3D 操作系统定义的一系列主版本号中的最新版本号。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的 Cisco 3D 操作系统定义的最新次版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	至次版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上版本中的字节数。
至次版本 (To Minor)	字符串	用户输入中的第三方操作系统字符串映射到的 Cisco 3D 操作系统定义的一系列次版本号中的最新版本号。
字符串块类型 (String Block Type)	uint32	启动一个字符串数据块，此数据块包含第三方操作系统字符串映射到的 Cisco 3D 操作系统定义的最新修订号。值始终为 0。
字符串块长度 (String Block Length)	uint32	至修订版字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上修订号中的字节数。
至修订版 (To Revision)	字符串	用户输入中的第三方操作系统字符串映射到的 Cisco 3D 操作系统定义的一系列修订号中的最新修订号。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的 Cisco 3D 操作系统的内部版本号的字符串数据块。值始终为 0。
字符串块长度 (String Block Length	uint32	内部版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上内部版本号中的字节数。
内部版本 (Build)	字符串	用户输入中的第三方操作系统字符串映射到的 Cisco 3D 操作系统的内部版本号。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的 Cisco 3D 操作系统的修补版本号的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	修补版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上修补版本号中的字节数。

表 B-19　用于 4.10.x、5.0-5.0.x 的用户产品数据块字段 （续）

字段	数据类型	说明
修补 (Patch)	字符串	用户输入中的第三方操作系统字符串映射到的 Cisco 3D 操作系统的修补版本号。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的 Cisco 3D 操作系统的扩展版本号的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	扩展版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上扩展版本号中的字节数。
分机 (Extension)	字符串	用户输入中第三方操作系统字符串映射到的 Cisco 3D 操作系统的扩展版本号。
UUID	uint8 [x16]	包含操作系统的唯一标识号。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送有关应用到特定 IP 地址范围中指定主机的修复的用户输入数据的修复列表数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装修复列表数据块。
修复列表数据块 (Fix List Data Blocks) *	变量	包含应用到主机的修复的相关信息的修复列表数据块。有关此数据块的说明，请参阅修复列表数据块，第 4-103 页。

旧版用户登录数据块

有关详细信息，请参阅以下各节：

用于 5.0 - 5.0.2 的用户登录信息数据块

用户登录信息数据块在用户信息更新消息中使用，传送检测到的用户的登录信息变更。有关详细信息，请参阅用户信息更新消息块，第 4-62 页.

在版本 5.0 - 5.0.2 中，用户登录信息数据块的块类型为 121。

下图显示用户登录信息数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户登录信息块类型 (121) (User Login Information Block Type (121))																															
	用户登录信息块长度 (User Login Information Block Length)																															
	时间戳 (Timestamp)																															
	IP 地址 (IP Addresses)																															
用户名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户名 ... (User Name...)																															
	用户 ID (User ID)																															
	应用 ID (Application ID)																															
电子邮件	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电子邮件 ...(Email...)																															

下表对用户登录信息数据块的组件进行了说明。

表 B-20 用户登录信息数据块字段 5.0 - 5.0.2

字段	数据类型	说明
用户登录信息块类型 (User Login Information Block Type)	uint32	启动用户登录信息数据块。在版本 5.0 - 5.0.2 中，此值为 `121`。
用户登录信息块长度 (User Login Information Block Length)	uint32	用户登录信息数据块中的字节总数，包括用户登录信息块类型和长度字段的八个字节，加上随后的用户登录信息数据中的字节数。
时间戳 (Timestamp)	uint32	事件的时间戳。
IP 地址 (IP Addresses)	uint8[4]	检测到用户登录的主机的 IP 地址，采用 IP 地址八位组。

表 B-20　用户登录信息数据块字段 5.0 - 5.0.2 （续）

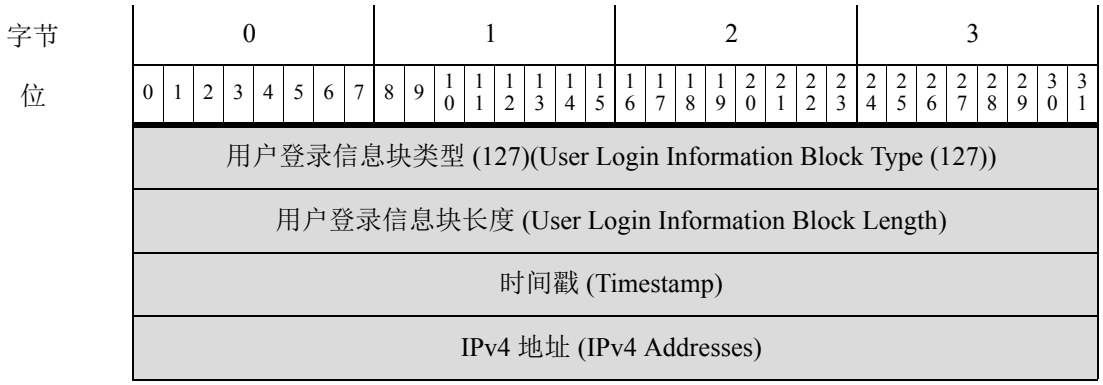
字段	数据类型	说明
字符串块类型 (String Block Type)	uint32	启动包含用户的用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户名 (Username)	字符串	用户的用户名。
用户 ID (User ID)	uint32	用户的标识号。
应用 ID (Application ID)	uint32	派生登录信息的连接中使用的应用协议的应用 ID。
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件地址的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	电子邮件地址字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上电子邮件地址中的字节数。
电子邮件 (Email)	字符串	用户的邮件地址。

用户登录信息数据块 5.1 - 5.4.x

用户登录信息数据块在用户信息更新消息中使用，传送检测到的用户的登录信息变更。有关详细信息，请参阅用户帐户更新消息数据块，第 4-184 页。

在版本 4.7 - 4.10.x 中，用户登录信息数据块的块类型为 73，在版本 5.0 - 5.0.2 中，块类型为系列 1 数据块组中的 121，在版本 5.1-5.4.x 中，块类型为系列 1 数据块组中的 127。

下图显示用户登录信息数据块的格式：



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
用户名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户名 ... (User Name...)																															
	用户 ID (User ID)																															
	应用 ID (Application ID)																															
电子邮件	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电子邮件 ...(Email...)																															
	IPv6 地址 (IPv6 Address)																															
	IPv6 地址 (IPv6 Address) （续）																															
	IPv6 地址 (IPv6 Address) （续）																															
	IPv6 地址 (IPv6 Address) （续）																															
报告者 (Reported By)	登录类型 (Login Type)								字符串块类型 (0) (String Block Type (0))																							
	字符串块类型 (0) (String Block Type (0)) （续）								字符串块长度 (String Block Length)																							
	字符串块长度 (String Block Length)								报告者 ... (Reported By...)																							

下表对用户登录信息数据块的组件进行了说明。

表 B-21 用户登录信息数据块字段

字段	数据类型	说明
用户登录信息块类型 (User Login Information Block Type)	uint32	启动用户登录信息数据块。在版本 5.1+ 中，此值为 127。
用户登录信息块长度 (User Login Information Block Length)	uint32	用户登录信息数据块中的字节总数，包括用户登录信息块类型和长度字段的八个字节，加上随后的用户登录信息数据中的字节数。

表 B-21　用户登录信息数据块字段 （续）

字段	数据类型	说明
时间戳 (Timestamp)	uint32	事件的时间戳。
IPv4 地址 (IPv4 Addresses)	uint32	保留此字段，但不再填充。 IPv4 地址存储在 IPv6 地址字段中。有关详细信息，请参阅 IP 地址，第 1-3 页。
字符串块类型 (String Block Type)	uint32	启动包含用户的用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户名 (Username)	字符串	用户的用户名。
用户 ID (User ID)	uint32	用户的标识号。
应用 ID (Application ID)	uint32	派生登录信息的连接中使用的应用协议的应用 ID。
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件地址的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	电子邮件地址字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上电子邮件地址中的字节数。
电子邮件 (Email)	字符串	用户的邮件地址。
IPv6 地址 (IPv6 Address)	uint8[16]	检测到用户登录的主机的 IPv6 地址，采用 IP 地址八位组。
登录类型 (Login Type)	uint8	检测到的用户登录类型。
字符串块类型 (String Block Type)	uint32	启动包含报告者值的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	报告者字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上 “ 报告者 ”(Reported By) 字段中的字节数。
报告者 (Reported By)	字符串	报告登录的 Active Directory 服务器的名称。

用户登录信息数据块 6.0.x

用户登录信息数据块在用户信息更新消息中使用，传送检测到的用户的登录信息变更。有关详细信息，请参阅用户帐户更新消息数据块，第 4-184 页。

在版本 6.0.x 中，用户登录信息数据块的块类型为 159。它具有新 ISE 集成终端配置文件、安全情报字段。

在版本 4.7 - 4.10.x 中，用户登录信息数据块的块类型为 73。在版本 5.0 - 5.0.2 中，块类型为系列 1 数据块组中的 121。在版本 5.1+ 中，块类型为系列 1 数据块组中的 127。有关详细信息，请参阅用户登录信息数据块 5.1 - 5.4.x，第 B-107 页。

下图显示用户登录信息数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户登录信息块类型 (159) (User Login Information Block Type (159))																															
	用户登录信息块长度 (User Login Information Block Length)																															
	时间戳 (Timestamp)																															
	IPv4 地址 (IPv4 Addresses)																															
用户名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户名 ...(User Name...)																															
域	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	域 ...(Domain...)																															
	用户 ID (User ID)																															
	领域 ID (Realm ID)																															
	终端配置文件 ID (Endpoint Profile ID)																															
	安全组 ID (Security Group ID)																															
	协议 (Protocol)																															
电子邮件	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电子邮件 ...(Email...)																															
	IPv6 地址 (IPv6 Address) IPv6 地址 (IPv6 Address) （续） IPv6 地址 (IPv6 Address) （续） IPv6 地址 (IPv6 Address) （续）																															
	位置 IPv6 地址 (Location IPv6 Address) 位置 IPv6 地址 (Location IPv6 Address) （续）																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
位置 IPv6 地址 (Location IPv6 Address) （续） 位置 IPv6 地址 (Location IPv6 Address) （续）																																
报告者 (Reported By)	登录类型 (Login Type)								身份验证类型 (Auth. Type)								字符串块类型 (0) (String Block Type (0))															
	字符串块类型 (0) (String Block Type (0)) （续）																字符串块长度 (String Block Length)															
	字符串块长度 (String Block Length) （续）																报告者 ...(Reported By...)															

下表对用户登录信息数据块的组件进行了说明。

表 B-22　　用户登录信息数据块字段

字段	数据类型	说明
用户登录信息块类型 (User Login Information Block Type)	uint32	启动用户登录信息数据块。在版本 6.0.x 中，此值为 159。
用户登录信息块长度 (User Login Information Block Length)	uint32	用户登录信息数据块中的字节总数，包括用户登录信息块类型和长度字段的八个字节，加上随后的用户登录信息数据中的字节数。
时间戳 (Timestamp)	uint32	事件的时间戳。
IPv4 地址 (IPv4 Addresses)	uint32	保留此字段，但不再填充。 IPv4 地址存储在 IPv6 地址字段中。有关详细信息，请参阅 IP 地址，第 1-3 页。
字符串块类型 (String Block Type)	uint32	启动包含用户的用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户名 (Username)	字符串	用户的用户名。
字符串块类型 (String Block Type)	uint32	启动包含域的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上域中的字节数。
域 (Domain)	字符串	用户登录的域。
用户 ID (User ID)	uint32	用户的标识号。
领域 ID (Realm ID)	uint32	与身份领域对应的整数 ID。

表 B-22 用户登录信息数据块字段 （续）

字段	数据类型	说明
终端配置文件 ID (Endpoint Profile ID)	uint32	连接终端使用的设备类型的 ID 号码。这是每个 DC 特有的，在元数据中进行解析。
安全组 ID (Security Group ID)	uint32	网络流量组的 ID 号码。
协议 (Protocol)	uint32	用于检测或报告用户的协议。可能的值如下： • 165 - FTP • 426 - SIP • 547 - AOL 即时通信工具 • 683 - IMAP • 710 - LDAP • 767 - NTP • 773 - Oracle 数据库 • 788 - POP3 • 1755 - MDNS
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件地址的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	电子邮件地址字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上电子邮件地址中的字节数。
电子邮件 (Email)	字符串	用户的邮件地址。
IPv6 地址 (IPv6 Address)	uint8[16]	检测到用户登录的主机的 IPv6 地址，采用 IP 地址八位组。
位置 IPv6 地址 (Location IPv6 Address)	uint8[16]	用户最新登录的 IP 地址。可以是 IPv4 或 IPv6 地址。
登录类型 (Login Type)	uint8	检测到的用户登录类型。
身份验证类型 (Authentication Type)	uint8	用户使用的身份验证类型。值可能是： • 0 - 无需授权 • 1 - 被动身份验证、 AD 代理或 ISE 会话 • 2 - 强制网络门户身份验证成功 • 3 - 强制网络门户访客身份验证 • 4 - 强制网络门户身份验证失败
字符串块类型 (String Block Type)	uint32	启动包含报告者值的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	报告者字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上 “ 报告者 ”(Reported By) 字段中的字节数。
报告者 (Reported By)	字符串	报告登录的 Active Directory 服务器的名称。

用户登录信息数据块 6.1.x

在版本 6.1+ 中，用户登录信息数据块的块类型为系列 1 数据块组中的 165。它具有新的端口和隧道字段。它替代块类型 159。有关详细信息，请参阅用户登录信息数据块 6.0.x，第 B-109 页。它被块类型 167 替代。

下图显示用户登录信息数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户登录信息块类型 (165) (User Login Information Block Type (159))																															
	用户登录信息块长度 (User Login Information Block Length)																															
	时间戳 (Timestamp)																															
	IPv4 地址 (IPv4 Addresses)																															
用户名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户名 ...(User Name...)																															
域	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	域 ...(Domain...)																															
	用户 ID (User ID)																															
	领域 ID (Realm ID)																															
	终端配置文件 ID (Endpoint Profile ID)																															
	安全组 ID (Security Group ID)																															
	协议 (Protocol)																															
	端口 (Port)																范围开始 (Range Start)															
	开始端口 (Start Port)																结束端口 (End Port)															
电子邮件	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电子邮件 ...(Email...)																															
	IPv6 地址 (IPv6 Address)																															
	IPv6 地址 (IPv6 Address) （续）																															
	IPv6 地址 (IPv6 Address) （续）																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	IPv6 地址 (IPv6 Address) （续）																															
	位置 IPv6 地址 (Location IPv6 Address) 位置 IPv6 地址 (Location IPv6 Address) （续） 位置 IPv6 地址 (Location IPv6 Address) （续） 位置 IPv6 地址 (Location IPv6 Address) （续）																															
报告者 (Reported By)	登录类型 (Login Type)								身份验证类型 (Auth. Type)								字符串块类型 (0) (String Block Type (0))															
	字符串块类型 (0) (String Block Type (0)) （续）																字符串块长度 (String Block Length)															
	字符串块长度 (String Block Length) （续）																报告者 ...(Reported By...)															

下表对用户登录信息数据块的组件进行了说明。

表 B-23 用户登录信息数据块字段

字段	数据类型	说明
用户登录信息块类型 (User Login Information Block Type)	uint32	启动用户登录信息数据块。在版本 6.1+ 中，此值为 165。
用户登录信息块长度 (User Login Information Block Length)	uint32	用户登录信息数据块中的字节总数，包括用户登录信息块类型和长度字段的八个字节，加上随后的用户登录信息数据中的字节数。
时间戳 (Timestamp)	uint32	事件的时间戳。
IPv4 地址 (IPv4 Addresses)	uint32	保留此字段，但不再填充。 IPv4 地址存储在 IPv6 地址字段中。有关详细信息，请参阅 IP 地址，第 1-3 页。
字符串块类型 (String Block Type)	uint32	启动包含用户的用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户名 (Username)	字符串	用户的用户名。
字符串块类型 (String Block Type)	uint32	启动包含域的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上域中的字节数。
域 (Domain)	字符串	用户登录的域。

表 B-23　用户登录信息数据块字段 （续）

字段	数据类型	说明
用户 ID (User ID)	uint32	用户的标识号。
领域 ID (Realm ID)	uint32	与身份领域对应的整数 ID。
终端配置文件 ID (Endpoint Profile ID)	uint32	连接终端使用的设备类型的 ID 号码。这是每个 DC 特有的，在元数据中进行解析。
安全组 ID (Security Group ID)	uint32	网络流量组的 ID 号码。
协议 (Protocol)	uint32	用于检测或报告用户的协议。可能的值如下： • 165 - FTP • 426 - SIP • 547 - AOL 即时通信工具 • 683 - IMAP • 710 - LDAP • 767 - NTP • 773 - Oracle 数据库 • 788 - POP3 • 1755 - MDNS
端口 (Port)	uint16	在其上检测到用户的端口号。
范围开始 (Range Start)	uint16	TS 代理使用的端口范围内的起始端口。
开始端口 (Start Port)	uint16	TS 代理分配给单个用户的端口范围内的起始端口。
结束端口 (End Port)	uint16	TS 代理分配给单个用户的端口范围内的结束端口。
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件地址的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	电子邮件地址字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上电子邮件地址中的字节数。
电子邮件 (Email)	字符串	用户的邮件地址。
IPv6 地址 (IPv6 Address)	uint8[16]	检测到用户登录的主机的 IPv6 地址，采用 IP 地址八位组。
位置 IPv6 地址 (Location IPv6 Address)	uint8[16]	用户最新登录的 IP 地址。可以是 IPv4 或 IPv6 地址。
登录类型 (Login Type)	uint8	检测到的用户登录类型。

表 B-23 用户登录信息数据块字段 （续）

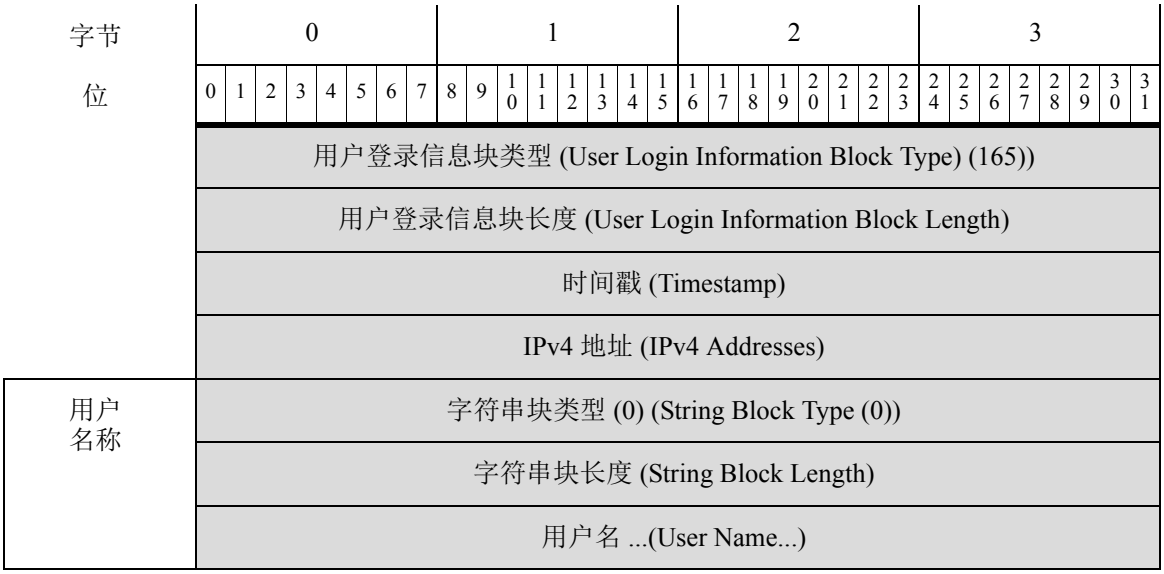
字段	数据类型	说明
身份验证类型 (Authentication Type)	uint8	用户使用的身份验证类型。值可能是： • 0 - 无需授权 • 1 - 被动身份验证、 AD 代理或 ISE 会话 • 2 - 强制网络门户身份验证成功 • 3 - 强制网络门户访客身份验证 • 4 - 强制网络门户身份验证失败
字符串块类型 (String Block Type)	uint32	启动包含报告者值的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	报告者字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上 “ 报告者 ”(Reported By) 字段中的字节数。
报告者 (Reported By)	字符串	报告登录的 Active Directory 服务器的名称。

用户登录信息数据块 6.1.x

用户登录信息数据块在用户信息更新消息中使用，传送检测到的用户的登录信息变更。有关详细信息，请参阅用户信息更新消息块，第 4-62 页。

在版本 6.1x 中，用户登录信息数据块的块类型为系列 1 数据块组中的 165。它具有新的端口和隧道字段。它替代块类型 159。它被块类型 167 替代。用户登录信息数据块 6.0.x，第 B-109 页有关详细信息，请参阅。

下图显示用户登录信息数据块的格式：



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
域	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	域 ...(Domain...)																															
	用户 ID (User ID)																															
	领域 ID (Realm ID)																															
	终端配置文件 ID (Endpoint Profile ID)																															
	安全组 ID (Security Group ID)																															
	协议 (Protocol)																															
	端口 (Port)																范围开始 (Range Start)															
	开始端口 (Start Port)																结束端口 (End Port)															
电子邮件	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电子邮件 ...(Email...)																															
	IPv6 地址 (IPv6 Address) IPv6 地址 (IPv6 Address) （续） IPv6 地址 (IPv6 Address) （续） IPv6 地址 (IPv6 Address) （续）																															
	位置 IPv6 地址 (Location IPv6 Address) 位置 IPv6 地址 (Location IPv6 Address) （续） 位置 IPv6 地址 (Location IPv6 Address) （续） 位置 IPv6 地址 (Location IPv6 Address) （续）																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报告者 (Reported By)	登录类型 (Login Type)								身份验证类型 (Auth. Type)								字符串块类型 (0) (String Block Type (0))															
	字符串块类型 (0) (String Block Type (0)) （续）																字符串块长度 (String Block Length)															
	字符串块长度 (String Block Length) （续）																报告者 ...(Reported By...)															
域	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	说明 ...(Description...)																															

下表对用户登录信息数据块的组件进行了说明。

表 B-24 用户登录信息数据块字段

字段	数据类型	说明
用户登录信息块类型 (User Login Information Block Type)	uint32	启动用户登录信息数据块。在版本 6.2+ 中，此值为 165。
用户登录信息块长度 (User Login Information Block Length)	uint32	用户登录信息数据块中的字节总数，包括用户登录信息块类型和长度字段的八个字节，加上随后的用户登录信息数据中的字节数。
时间戳 (Timestamp)	uint32	事件的时间戳。
IPv4 地址 (IPv4 Addresses)	uint32	保留此字段，但不再填充。 IPv4 地址存储在 IPv6 地址字段中。有关详细信息，请参阅 IP 地址，第 1-3 页。
字符串块类型 (String Block Type)	uint32	启动包含用户的用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户名 (Username)	字符串	用户的用户名。
字符串块类型 (String Block Type)	uint32	启动包含域的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上域中的字节数。
域 (Domain)	字符串	用户登录的域。
用户 ID (User ID)	uint32	用户的标识号。
领域 ID (Realm ID)	uint32	与身份领域对应的整数 ID。

表 B-24　　用户登录信息数据块字段 （续）

字段	数据类型	说明
终端配置文件 ID (Endpoint Profile ID)	uint32	连接终端使用的设备类型的 ID 号码。这是每个 DC 特有的，在元数据中进行解析。
安全组 ID (Security Group ID)	uint32	网络流量组的 ID 号码。
协议 (Protocol)	uint32	用于检测或报告用户的协议。可能的值如下： • 165 - FTP • 426 - SIP • 547 - AOL 即时通信工具 • 683 - IMAP • 710 - LDAP • 767 - NTP • 773 - Oracle 数据库 • 788 - POP3 • 1755 - MDNS
端口 (Port)	uint16	在其上检测到用户的端口号。
范围开始 (Range Start)	uint16	TS 代理使用的端口范围内的起始端口。
开始端口 (Start Port)	uint16	TS 代理分配给单个用户的端口范围内的起始端口。
结束端口 (End Port)	uint16	TS 代理分配给单个用户的端口范围内的结束端口。
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件地址的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	电子邮件地址字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上电子邮件地址中的字节数。
电子邮件 (Email)	字符串	用户的邮件地址。
IPv6 地址 (IPv6 Address)	uint8[16]	检测到用户登录的主机的 IPv6 地址，采用 IP 地址八位组。
位置 IPv6 地址 (Location IPv6 Address)	uint8[16]	用户最新登录的 IP 地址。可以是 IPv4 或 IPv6 地址。
登录类型 (Login Type)	uint8	检测到的用户登录类型。
身份验证类型 (Authentication Type)	uint8	用户使用的身份验证类型。值可能是： • 0 - 无需授权 • 1 - 被动身份验证、 AD 代理或 ISE 会话 • 2 - 强制网络门户身份验证成功 • 3 - 强制网络门户访客身份验证 • 4 - 强制网络门户身份验证失败

表 B-24 用户登录信息数据块字段 （续）

字段	数据类型	说明
字符串块类型 (String Block Type)	uint32	启动包含报告者值的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	报告者字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上 “ 报告者 ”(Reported By) 字段中的字节数。
报告者 (Reported By)	字符串	报告登录的 Active Directory 服务器的名称。

用于 5.x 的用户信息数据块

用户信息数据块在用户修改消息中使用，传送检测到、删除或丢弃的用户的信息。有关详细信息，请参阅用户修改消息，第 4-62 页

在版本 4.7 - 4.10.x 中，用户信息数据块的块类型为系列 1 数据块组中的 75，在版本 5.x 中，块类型为系列 1 数据块组中的 120。块类型 75 与块类型 120 的结构相同。

下图显示用户信息数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户信息块类型 (75 | 120) (User Information Block Type (75 | 120))																															
	用户信息块长度 (User Information Block Length)																															
	用户 ID (User ID)																															
用户名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户名 ... (User Name...)																															
	协议 (Protocol)																															
第一页名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	名字 ...(First Name...)																															
最后一页名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	姓氏 ...(Last Name...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
电子邮件	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电子邮件 ...(Email...)																															
部门	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	部门 ...(Department...)																															
电话	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电话 ...(Phone...)																															

下表对用户信息数据块的组件进行了说明。

表 B-25　　用户信息数据块字段

字段	数据类型	说明
用户信息块类型 (User Information Block Type)	uint32	启动用户信息数据块。在版本 4.7 - 4.10.x 中，此值为 `75`，在版本 5.0+ 中，此值为 `120` 。
用户信息块长度 (User Information Block Length)	uint32	用户信息数据块中的字节总数，包括用户信息块类型和长度字段的八个字节，加上随后的用户信息数据中的字节数。
用户 ID (User ID)	uint32	用户的标识号。
字符串块类型 (String Block Type)	uint32	启动包含用户的用户名的字符串数据块。值始终为 `0`。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户名 (Username)	字符串	用户的用户名。
协议 (Protocol)	uint32	用于包含用户信息的数据包的协议。
字符串块类型 (String Block Type)	uint32	启动包含用户的名字的字符串数据块。值始终为 `0`。
字符串块长度 (String Block Length)	uint32	名字字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上名字中的字节数。
名字 (First Name)	字符串	用户的名字。
字符串块类型 (String Block Type)	uint32	启动包含用户的姓氏的字符串数据块。值始终为 `0`。

表 B-25　　用户信息数据块字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Length)	uint32	用户姓氏字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上姓氏中的字节数。
姓氏 (Last Name)	字符串	用户的姓氏。
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件地址的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	电子邮件地址字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上电子邮件地址中的字节数。
电子邮件 (Email)	字符串	用户的邮件地址。
字符串块类型 (String Block Type)	uint32	启动包含用户所在部门的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	部门字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上部门中的字节数。
部门 (Dept)	字符串	用户所在部门。
字符串块类型 (String Block Type)	uint32	启动包含用户的电话号码的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	电话号码字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上电话号码中的字节数。
电话 (Phone)	字符串	用户的电话号码。

旧版主机配置文件数据块

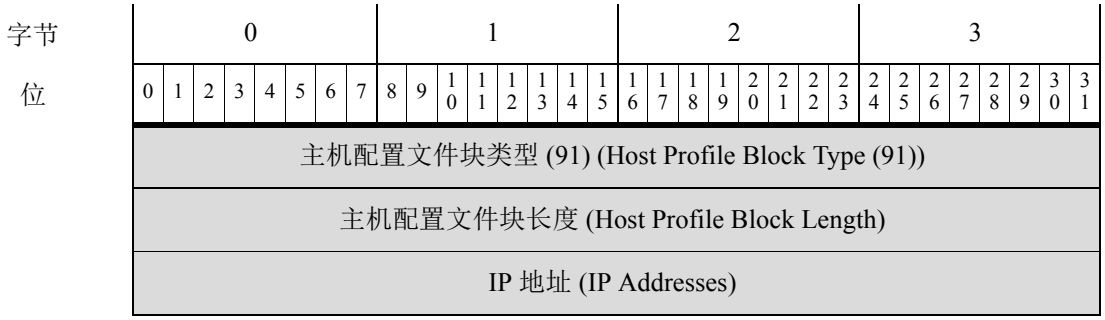
有关详细信息，请参阅以下各节：

- 用于 5.0 - 5.0.2 的主机配置文件数据块，第 B-122 页

用于 5.0 - 5.0.2 的主机配置文件数据块

下图显示版本 5.0 至 5.0.2 中主机配置文件数据块的格式。主机配置文件数据块也不包含主机临界值，但包含 VLAN 在线状态指示器。此外，主机配置文件数据块可以传输主机的 NetBIOS 名称。此主机配置文件数据块的块类型为 91。

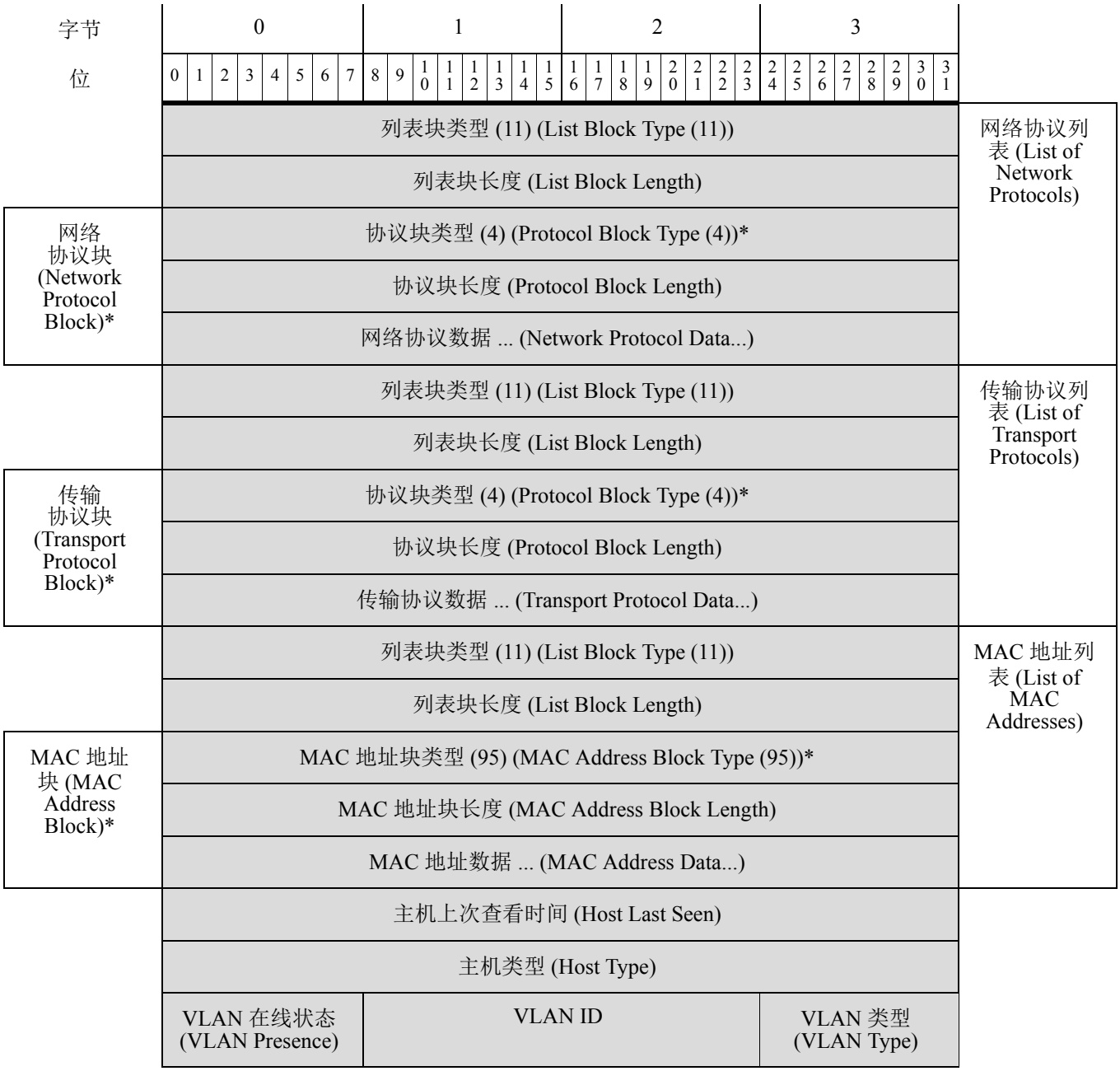
注　下图中块类型字段旁边的星号 (*) 表示该消息可能包含零个或多个系列 1 数据块实例。

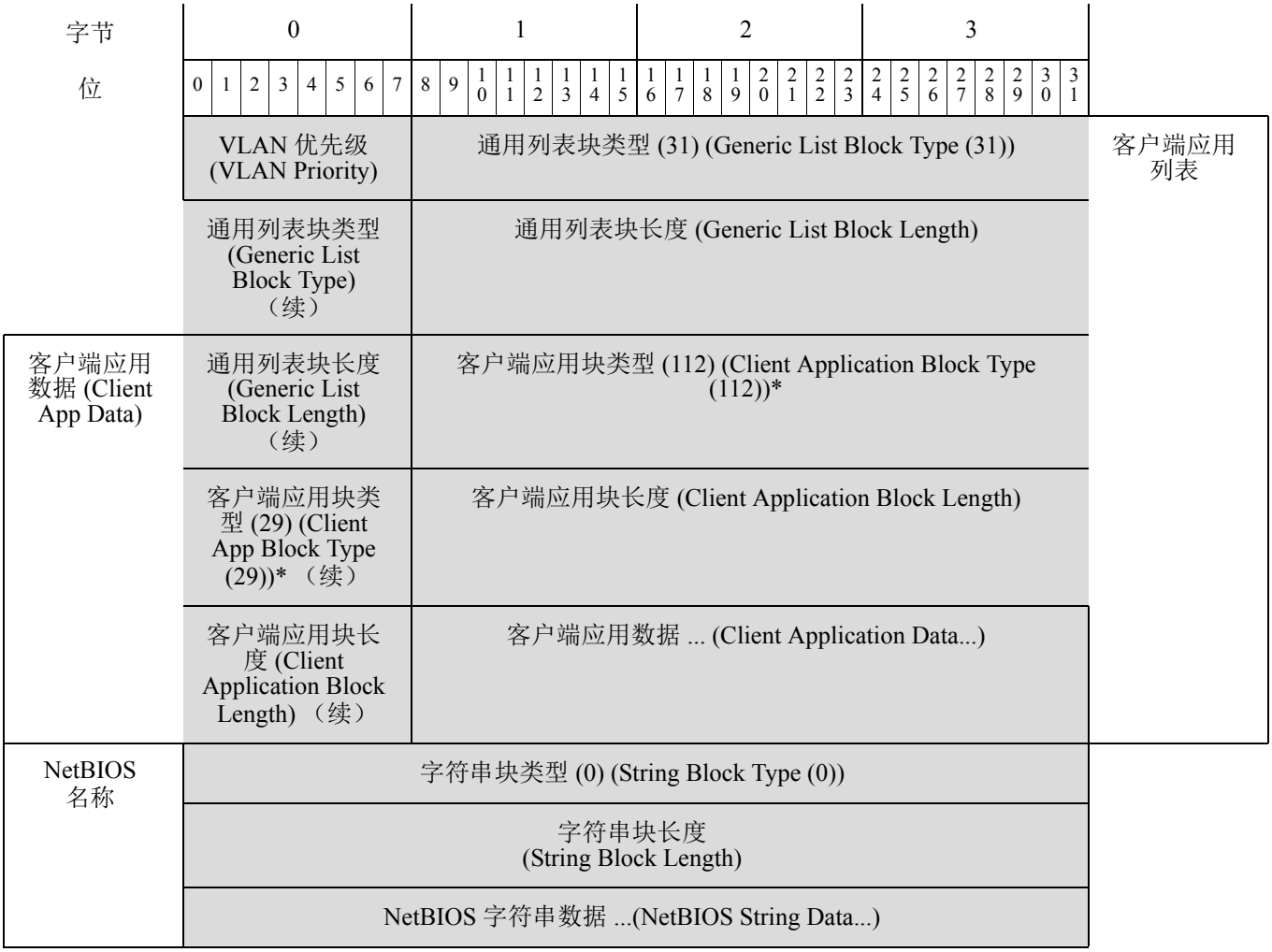


字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
服务器指纹	跳数 (Hops)								主要 / 次要 (Primary/Secondary)								通用列表块类型 (31) (Generic List Block Type (31))															
	通用列表块类型 (Generic List Block Type) （续）																通用列表块长度 (Generic List Block Length)															
	通用列表块长度 (Generic List Block Length) （续）																服务器指纹数据块 (Server Fingerprint Data Blocks)*															
客户端指纹	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	客户端指纹数据块 (Client Fingerprint Data Blocks)*																															
中小企业指纹	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	SMB 指纹数据块 (SMB Fingerprint Data Blocks)*																															
DHCP 指纹	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	DHCP 指纹数据块 (DHCP Fingerprint Data Blocks)*																															
TCP 服务器块 (TCP Server Block)*	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	服务器块类型 (36) (Server Block Type (36))																															
	服务器块长度 (Server Block Length)																															
	TCP 服务器数据 ... (TCP Server Data...)																															
UDP 服务器块 (TCP Server Block)*	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	服务器块类型 (36) (Server Block Type (36))*																															
	服务器块长度 (Server Block Length)																															
	UDP 服务器数据 ... (UDP Server Data...)																															

TCP 服务器列表 (List of TCP Servers)

UDP 服务器列表 (List of UDP Servers)


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
列表块类型 (11) (List Block Type (11))
列表块长度 (List Block Length)
网络协议列表 (List of Network Protocols)
网络协议块 (Network Protocol Block)*
协议块类型 (4) (Protocol Block Type (4))*
协议块长度 (Protocol Block Length)
网络协议数据 ... (Network Protocol Data...)
列表块类型 (11) (List Block Type (11))
列表块长度 (List Block Length)
传输协议列表 (List of Transport Protocols)
传输协议块 (Transport Protocol Block)*
协议块类型 (4) (Protocol Block Type (4))*
协议块长度 (Protocol Block Length)
传输协议数据 ... (Transport Protocol Data...)
列表块类型 (11) (List Block Type (11))
列表块长度 (List Block Length)
MAC 地址列表 (List of MAC Addresses)
MAC 地址块 (MAC Address Block)*
MAC 地址块类型 (95) (MAC Address Block Type (95))*
MAC 地址块长度 (MAC Address Block Length)
MAC 地址数据 ... (MAC Address Data...)
主机上次查看时间 (Host Last Seen)
主机类型 (Host Type)
VLAN 在线状态 (VLAN Presence)
VLAN ID
VLAN 类型 (VLAN Type)



下表对由版本 4.9 返回到版本 5.0.2 的主机配置文件数据块的字段进行了说明。

表 B-26　　用于 5.0 - 5.0.2 的主机配置文件数据块字段

字段	数据类型	说明
主机配置文件块类型 (Host Profile Block Type)	uint32	启动用于 4.9 至 5.0.2 的主机配置文件数据块。此数据块的块类型为 91。
主机配置文件块长度 (Host Profile Block Length)	uint32	主机配置文件数据块中的字节数，包括主机配置文件块类型和长度字段的八个字节，加上随后的主机配置文件数据中的字节数。
IP 地址 (IP Addresses)	uint8[4]	配置文件中描述的主机的 IP 地址，采用 IP 地址八位组。
跳数 (Hops)	uint8	从主机到设备的跳数。

表 B-26 用于 5.0 - 5.0.2 的主机配置文件数据块字段 （续）

字段	数据类型	说明
主 / 辅助 (Primary/Secondary)	uint8	表示主机是位于检测到其的设备的主网络中还是辅助网络中： • 0 - 主机位于主网络中。 • 1 - 主机位于辅助网络中。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用服务器指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（服务器指纹）数据块 (Operating System Fingerprint (Server Fingerprint) Data Blocks) *	变量	包含用服务器指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅用于 5.0 - 5.0.2 的操作系统指纹数据块，第 B-130 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用客户端指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（客户端指纹）数据块 (Operating System Fingerprint (Client Fingerprint) Data Blocks) *	变量	包含用客户端指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅用于 5.0 - 5.0.2 的操作系统指纹数据块，第 B-130 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用 SMB 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 B-26　用于 5.0 - 5.0.2 的主机配置文件数据块字段 （续）

字段	数据类型	说明
操作系统指纹（SMB 指纹）数据块 (Operating System Fingerprint (SMB Fingerprint) Data Blocks) *	变量	包含用 SMB 指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅用于 5.0 - 5.0.2 的操作系统指纹数据块，第 B-130 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用 DHCP 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（DHCP 指纹）数据块 (Operating System Fingerprint (DHCP Fingerprint) Data Blocks) *	变量	包含用 DHCP 指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅用于 5.0 - 5.0.2 的操作系统指纹数据块，第 B-130 页。
列表块类型 (List Block Type)	uint32	启动由传送 TCP 服务器数据的服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装服务器数据块。 此字段后面是零个或多个服务器数据块。
服务器块类型 (Server Block Type)	uint32	启动服务器数据块。值始终为 89。
服务器块长度 (Server Block Length)	uint32	服务器数据块中的字节数，包括服务器块类型和长度字段的八个字节，加上随后的 TCP 服务器数据的字节数。
TCP 服务器数据 (TCP Server Data)	变量	描述 TCP 服务器的数据字段 （按照产品早期版本的记录）。
列表块类型 (List Block Type)	uint32	启动由传送 UDP 服务器数据的服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装服务器数据块。 此字段后面是零个或多个服务器数据块。

表 B-26 用于 5.0 - 5.0.2 的主机配置文件数据块字段 （续）

字段	数据类型	说明
服务器块类型 (Server Block Type)	uint32	启动描述 UDP 服务器的服务器数据块。值始终为 89。
服务器块长度 (Server Block Length)	uint32	服务器数据块中的字节数，包括服务器块类型和长度字段的八个字节，加上随后的 UDP 服务器数据的字节数。
UDP 服务器数据 (UDP Server Data)	变量	描述 UDP 服务器的数据字段 （按照产品早期版本的记录）。
列表块类型 (List Block Type)	uint32	启动由传送网络协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块。 此字段后面是零个或多个协议数据块。
协议块类型 (Protocol Block Type)	uint32	启动描述网络协议的协议数据块。值始终为 4。
协议块长度 (Protocol Block Length)	uint32	协议数据块中的字节数，包括协议块类型和长度字段的八个字节，加上随后的协议数据中的字节数。
网络协议数据 (Network Protocol Data)	uint16	包含网络协议号的数据字段，如协议数据块，第 4-74 页中所记录。
列表块类型 (List Block Type)	uint32	启动由传送传输协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块。 此字段后面是零个或多个传输协议数据块。
协议块类型 (Protocol Block Type)	uint32	启动描述传输协议的协议数据块。值始终为 4。
协议块长度 (Protocol Block Length)	uint32	协议数据块中的字节数，包括协议块类型和长度的八个字节，加上随后的协议数据中的字节数。
传输协议数据 (Transport Protocol Data)	变量	包含传输协议号的数据字段，如协议数据块，第 4-74 页中所记录。
列表块类型 (List Block Type)	uint32	启动由 MAC 地址数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数，包括列表报头以及所有封装 MAC 地址数据块。

表 B-26　用于 5.0 - 5.0.2 的主机配置文件数据块字段 （续）

字段	数据类型	说明
主机 MAC 地址块类型 (Host MAC Address Block Type)	uint32	启动主机 MAC 地址数据块。值始终为 95。
主机 MAC 地址块长度 (Host MAC Address Block Length)	uint32	主机 MAC 地址数据块中的字节数，包括主机 MAC 地址块类型和长度字段的八个字节，加上随后的主机 MAC 地址数据中的字节数。
主机 MAC 地址数据 (Host MAC Address Data)	变量	主机 MAC 地址 4.9+，第 4-116 页中描述的主机 MAC 地址数据字段。
主机上次查看时间 (Host Last Seen)	uint32	表示系统上次检测到主机活动的 UNIX 时间戳。
主机类型 (Host Type)	uint32	表示主机类型。可能会出现以下值： • 0 - 主机 • 1 - 路由器 • 2 - 网桥 • 3 - NAT 设备 • 4 - LB （负载均衡器）
VLAN 在线状态 (VLAN Presence)	uint8	表示是否存在 VLAN： • 0 - 是 • 1 - 否
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
VLAN 类型 (VLAN Type)	uint8	VLAN 标签中封装的数据包类型。
VLAN 优先级 (VLAN Priority)	uint8	VLAN 标签中包含的优先级值。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送客户端应用数据的客户端应用数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装客户端应用数据块。
客户端应用块类型 (Client Application Block Type)	uint32	启动客户端应用块。值始终为 5。
客户端应用块长度 (Client Application Block Length)	uint32	客户端应用块中的字节数，包括客户端应用块类型和长度字段的八个字节，加上随后的客户端应用数据中的字节数。

表 B-26 用于 5.0 - 5.0.2 的主机配置文件数据块字段 （续）

字段	数据类型	说明
客户端应用数据 (Client Application Data...)	变量	描述客户端应用的客户端应用数据字段，如用于 5.0+ 的主机客户端应用数据块，第 4-160 页中所记录。
字符串块类型 (String Block Type)	uint32	启动 NetBIOS 名称的字符串数据块。此值设置为 0 以表示字符串数据。
字符串块长度 (String Block Length)	uint32	表示 NetBIOS 名称字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称的字节数。
NetBIOS 字符串数据 (NetBIOS String Data)	变量	包含主机配置文件中描述的主机的 NetBIOS 名称。

旧版操作系统指纹数据块

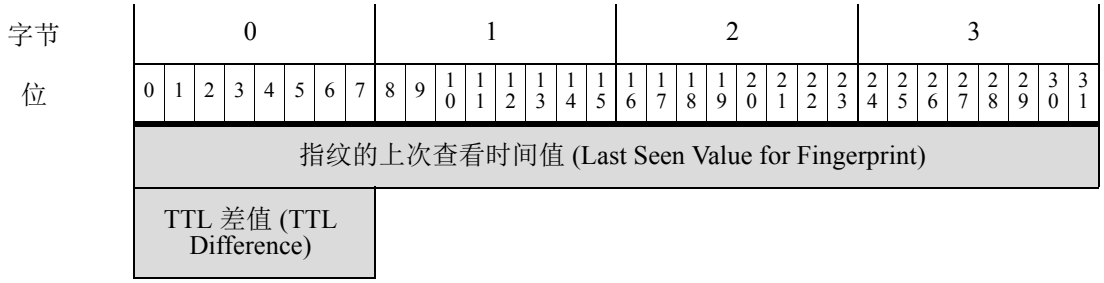
有关详细信息，请参阅以下各节：

- 用于 5.0 - 5.0.2 的操作系统指纹数据块，第 B-130 页

用于 5.0 - 5.0.2 的操作系统指纹数据块

操作系统指纹数据块的块类型为 87。块包括指纹通用唯一标识符 (UUID) 以及指纹类型、指纹源类型和指纹源 ID。下图显示用于版本 5.0 至版本 5.0.2 的操作系统指纹数据块的格式。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	操作系统指纹块类型 (87) (Operating System Fingerprint Block Type (87))																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
操作系统指纹 UUID	指纹 UUID (Fingerprint UUID)																															
	指纹 UUID (Fingerprint UUID) （续）																															
	指纹 UUID (Fingerprint UUID) （续）																															
	指纹 UUID (Fingerprint UUID) （续）																															
	指纹类型 (Fingerprint Type)																															
	指纹源类型 (Fingerprint Source Type)																															
	指纹源 ID (Fingerprint Source ID)																															



下表对操作系统指纹数据块的字段进行了说明。

表 B-27　　操作系统指纹数据块字段

字段	数据类型	说明
操作系统指纹数据块类型 (Operating System Fingerprint Data Block Type)	uint32	启动操作系统数据块。值始终为 87。
操作系统数据块长度 (Operating System Data Block Length)	uint32	操作系统指纹数据块中的字节数。此值应始终为 41：数据块类型和长度字段的八个字节，指纹 UUID 值的十六个字节，指纹类型的四个字节，指纹源类型的四个字节，指纹源 ID 的四个字节，上次查看时间值的四个字节以及 TTL 差值的一个字节。
指纹 UUID (Fingerprint UUID)	uint8[16]	采用八位组的指纹识别号，用作操作系统的唯一标识符。指纹 UUID 映射到漏洞数据库 (VDB) 中的操作系统名称、供应商和版本。
指纹类型 (Fingerprint Type)	uint32	表示指纹的类型。
指纹源类型 (Fingerprint Source Type)	uint32	表示提供操作系统指纹的源的类型 （即用户或扫描仪）。
指纹源 ID (Fingerprint Source ID)	uint32	表示提供操作系统指纹的源的 ID。
上次查看时间 (Last Seen)	uint32	表示上次在流量中看到指纹的时间。
TTL 差值 (TTL Difference)	uint8	表示指纹中的 TTL值与在用于采集主机指纹的数据包中看到的 TTL 值之间的差值。

旧版连接数据结构

有关详细信息，请参阅以下各节：

- 连接统计信息数据块 5.0 - 5.0.2，第 B-132 页
- 连接统计信息数据块 5.1，第 B-138 页
- 连接统计信息数据块 5.2.x，第 B-145 页
- 用于 5.0 - 5.1 的连接区块数据块，第 B-152 页

连接统计信息数据块 5.0 - 5.0.2

连接统计信息数据块在连接数据消息中使用。用于版本 5.0 - 5.0.2 的连接统计信息数据块的块类型为 115。

有关连接统计信息数据消息的详细信息，请参阅连接统计信息数据消息，第 4-54 页。

下图显示用于 5.0 - 5.0.2 的连接统计信息数据块的格式：

::

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
连接数据块类型 (115) (Connection Data Block Type (115))																																
连接数据块长度 (Connection Data Block Length)																																
设备 ID (Device ID)																																
入口区 (Ingress Zone) 入口区 (Ingress Zone) （续） 入口区 (Ingress Zone) （续） 入口区 (Ingress Zone) （续）																																
出口区 (Egress Zone) 出口区 (Egress Zone) （续） 出口区 (Egress Zone) （续） 出口区 (Egress Zone) （续）																																
入口接口 (Ingress Interface) 入口接口 (Ingress Interface) （续） 入口接口 (Ingress Interface) （续）																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
入口接口 (Ingress Interface) （续）																																
出口接口 (Egress Interface)																																
出口接口 (Egress Interface) （续）																																
出口接口 (Egress Interface) （续）																																
出口接口 (Egress Interface) （续）																																
发起方 IP 地址 (Initiator IP Address)																																
发起方 IP 地址 (Initiator IP Address) （续）																																
发起方 IP 地址 (Initiator IP Address) （续）																																
发起方 IP 地址 (Initiator IP Address) （续）																																
响应方 IP 地址 (Responder IP Address)																																
响应方 IP 地址 (Responder IP Address) （续）																																
响应方 IP 地址 (Responder IP Address) （续）																																
响应方 IP 地址 (Responder IP Address) （续）																																
策略修订 (Policy Revision)																																
策略修订 (Policy Revision) （续）																																
策略修订 (Policy Revision) （续）																																
策略修订 (Policy Revision) （续）																																
规则 ID (Rule ID)																																
规则操作 (Rule Action)																																
发起方端口 (Initiator Port)																	响应方端口 (Responder Port)														
TCP 标志 (TCP Flags)																	协议 (Protocol)								NetFlow 源 (NetFlow Source)							
Netflow 源 (Netflow Source) （续）																																
Netflow 源 (Netflow Source) （续）																																
Netflow 源 (Netflow Source) （续）																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
NetFlow 源 (NetFlow Source) （续）																									第一个数据包时间 (First Pkt Time)							
第一个数据包时间戳 (First Packet Timestamp) （续）																									最后一个数据包时间 (Last Pkt Time)							
最后一个数据包时间戳 (Last Packet Timestamp) （续）																									发送的数据包数 (Packets Sent)							
发送的数据包数 (Packets Sent) （续）																																
发送的数据包数 (Packets Sent) （续）																									接收的数据包数 (Packets Rcvd)							
接收的数据包数 (Packets Received) （续）																																
接收的数据包数 (Packets Received) （续）																									发送的字节数 (Bytes Sent)							
发送的字节数 (Bytes Sent) （续）																																
接收的数据包数 (Packets Received) （续）																									接收的字节数 (Bytes Rcvd)							
接收的字节数 (Bytes Received) （续）																																
接收的字节数 (Bytes Received) （续）																									用户 ID (User ID)							
用户 ID (User ID) （续）																									应用协议 ID (Application Protocol ID)							
应用协议 ID (Application Protocol ID) （续）																									URL 类别 (URL Category)							
URL 类别 (URL Category) （续）																									URL 信誉 (URL Reputation)							
URL 信誉 (URL Reputation) （续）																									客户端应用 ID (Client App ID)							
客户端应用 ID (Client Application ID) （续）																									Web 应用 ID (Web App ID)							
Web 应用 ID (Web Application ID) （续）																									字符串块类型 (0) (String Block Type (0))							

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
客户端应用 URL (Client App URL)	字符串块类型 (String Block Type) （续）																								字符串块长度 (String Block Length)							
	字符串块长度 (String Block Length) （续）																								客户端应用 URL... (Client Application URL...)							
NetBIOS 名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	NetBIOS 名称 .... (NetBIOS Name....)																															
客户端应用版本 (Client App Version)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	客户端应用版本 ...(Client Application Version...)																															

下表对用于 5.0 - 5.0.2 的连接统计信息数据块的字段进行了说明。

表 B-28　　连接统计信息数据块 5.0 - 5.0.2 字段

字段	数据类型	说明
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 5.0 至 5.0.2 的连接统计信息数据块。值始终为 115。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID (Device ID)	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。

表 B-28 连接统计信息数据块 5.0 - 5.0.2 字段 （续）

字段	数据类型	说明
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP Address)	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP Address)	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号 （如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符 （如适用）。
规则操作 (Rule Action)	uint32	在用户界面中选择的针对该规则的操作 （允许、阻止等）。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的 UNIX 时间戳。
发送的数据包数 (Packets Sent)	uint64	发起主机传输的数据包数。
接收的数据包数 (Packets Received)	uint64	响应主机传输的数据包数。
发送的字节数 (Bytes Sent)	uint64	发起主机传输的字节数。

表 B-28　连接统计信息数据块 5.0 - 5.0.2 字段 （续）

字段	数据类型	说明
接收的字节数 (Bytes Received)	uint64	响应主机传输的字节数。
用户 ID (User ID)	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号 （如适用）。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号 （如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的 URL （如适用）（例如， `/files/index.html`）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。

表 B-28 连接统计信息数据块 5.0 - 5.0.2 字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本 (Client Application Version)	字符串	客户端应用版本。

连接统计信息数据块 5.1

连接统计信息数据块在连接数据消息中使用。5.0.2 到 5.1 的连接数据块变更包括添加了具有 5.1 中引入的配置参数的新字段 （规则操作原因、监控器规则、安全情报源 / 目标、安全情报层）。用于版本 5.1 的连接统计信息数据块的块类型为 126。

有关连接统计信息数据消息的详细信息，请参阅连接统计信息数据消息，第 4-54 页。

下图显示用于 5.1 的连接统计信息数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
连接数据块类型 (126) (Connection Data Block Type (126))																																
连接数据块长度 (Connection Data Block Length)																																
设备 ID (Device ID)																																
入口区 (Ingress Zone) 入口区 (Ingress Zone) （续） 入口区 (Ingress Zone) （续） 入口区 (Ingress Zone) （续）																																
出口区 (Egress Zone) 出口区 (Egress Zone) （续） 出口区 (Egress Zone) （续） 出口区 (Egress Zone) （续）																																
入口接口 (Ingress Interface) 入口接口 (Ingress Interface) （续）																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
入口接口 (Ingress Interface) （续）																																
入口接口 (Ingress Interface) （续）																																
出口接口 (Egress Interface)																																
出口接口 (Egress Interface) （续）																																
出口接口 (Egress Interface) （续）																																
出口接口 (Egress Interface) （续）																																
发起方 IP 地址 (Initiator IP Address)																																
发起方 IP 地址 (Initiator IP Address) （续）																																
发起方 IP 地址 (Initiator IP Address) （续）																																
发起方 IP 地址 (Initiator IP Address) （续）																																
响应方 IP 地址 (Responder IP Address)																																
响应方 IP 地址 (Responder IP Address) （续）																																
响应方 IP 地址 (Responder IP Address) （续）																																
响应方 IP 地址 (Responder IP Address) （续）																																
策略修订 (Policy Revision)																																
策略修订 (Policy Revision) （续）																																
策略修订 (Policy Revision) （续）																																
策略修订 (Policy Revision) （续）																																
规则 ID (Rule ID)																																
规则操作 (Rule Action)																	规则原因 (Rule Reason)														
发起方端口 (Initiator Port)																	响应方端口 (Responder Port)														
TCP 标志 (TCP Flags)																	协议 (Protocol)								NetFlow 源 (NetFlow Source)							
Netflow 源 (Netflow Source) （续）																																
Netflow 源 (Netflow Source) （续）																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Netflow 源 (Netflow Source) （续）																																
NetFlow 源 (NetFlow Source) （续）																									第一个数据包时间 (First Pkt Time)							
第一个数据包时间戳 (First Packet Timestamp) （续）																									最后一个数据包时间 (Last Pkt Time)							
最后一个数据包时间戳 (Last Packet Timestamp) （续）																									发起方传输的数据包数 (Initiator Transmitted Packets)							
发起方传输的数据包数 (Initiator Transmitted Packets) （续）																																
发起方传输的数据包数 (Initiator Transmitted Packets) （续）																									响应方传输的数据包数 (Responder Transmitted Packets)							
响应方传输的数据包数 (Responder Transmitted Packets) （续）																																
响应方传输的数据包数 (Responder Transmitted Packets) （续）																									发起方传输的字节数 (Initiator Transmitted Bytes)							
发起方传输的字节数 (Initiator Transmitted Bytes) （续）																																
发起方传输的字节数 (Initiator Transmitted Bytes) （续）																									响应方传输的字节数 (Responder Transmitted Bytes)							
响应方传输的字节数 (Responder Transmitted Bytes) （续）																																
响应方传输的字节数 (Responder Transmitted Bytes) （续）																									用户 ID (User ID)							
用户 ID (User ID) （续）																									应用协议 ID (Application Protocol ID)							
应用协议 ID (Application Protocol ID) （续）																									URL 类别 (URL Category)							
URL 类别 (URL Category) （续）																									URL 信誉 (URL Reputation)							
URL 信誉 (URL Reputation) （续）																									客户端应用 ID (Client App ID)							

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	客户端应用 ID (Client Application ID) （续）																								Web 应用 ID (Web App ID)							
	Web 应用 ID (Web Application ID) （续）																								字符串块类型 (0) (String Block Type (0))							
客户端应用 URL (Client App URL)	字符串块类型 (String Block Type) （续）																								字符串块长度 (String Block Length)							
	字符串块长度 (String Block Length) （续）																								客户端应用 URL... (Client Application URL...)							
NetBIOS 名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	NetBIOS 名称 .... (NetBIOS Name....)																															
客户端应用版本 (Client App Version)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	客户端应用版本 ...(Client Application Version...)																															
	监控器规则 1 (Monitor Rule 1)																															
	监控器规则 2 (Monitor Rule 2)																															
	监控器规则 3 (Monitor Rule 3)																															
	监控器规则 4 (Monitor Rule 4)																															
	监控器规则 5 (Monitor Rule 5)																															
	监控器规则 6 (Monitor Rule 6)																															
	监控器规则 7 (Monitor Rule 7)																															
	监控器规则 8 (Monitor Rule 8)																															
	安全接口源 / 目标 (Sec. Int. Src/Dst)								安全接口代表层 (Sec. Int. Rep Layer)																									

下表对用于 5.1 的连接统计信息数据块的字段进行了说明。

表 B-29 连接统计信息数据块 5.1 字段

字段	数据类型	说明
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 5.1 的连接统计信息数据块。值始终为 126。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID (Device ID)	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP Address)	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP Address)	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号 （如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符 （如适用）。
规则操作 (Rule Action)	uint16	在用户界面中选择的针对该规则的操作 （允许、阻止等）。
规则原因 (Rule Reason)	uint16	规则触发事件的原因。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。

表 B-29　连接统计信息数据块 5.1 字段 （续）

字段	数据类型	说明
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址。
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的 UNIX 时间戳。
发起方传输的数据包数 (Initiator Transmitted Packets)	uint64	发起主机传输的数据包数。
响应方传输的数据包数 (Responder Transmitted Packets)	uint64	响应主机传输的数据包数。
发起方传输的字节数 (Initiator Transmitted Bytes)	uint64	发起主机传输的字节数。
响应方传输的字节数 (Responder Transmitted Bytes)	uint64	响应主机传输的字节数。
用户 ID (User ID)	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号 （如适用）。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号 （如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。

表 B-29 连接统计信息数据块 5.1 字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的 URL （如适用）（例如， `/files/index.html`）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 `0`。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 `0`。
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本 (Client Application Version)	字符串	客户端应用版本。
监控器规则 1 (Monitor Rule 1)	uint32	与连接事件关联的第一个监控器规则的 ID。
监控器规则 2 (Monitor Rule 2)	uint32	与连接事件关联的第二个监控器规则的 ID。
监控器规则 3 (Monitor Rule 3)	uint32	与连接事件关联的第三个监控器规则的 ID。
监控器规则 4 (Monitor Rule 4)	uint32	与连接事件关联的第四个监控器规则的 ID。
监控器规则 5 (Monitor Rule 5)	uint32	与连接事件关联的第五个监控器规则的 ID。
监控器规则 6 (Monitor Rule 6)	uint32	与连接事件关联的第六个监控器规则的 ID。
监控器规则 7 (Monitor Rule 7)	uint32	与连接事件关联的第七个监控器规则的 ID。
监控器规则 8 (Monitor Rule 8)	uint32	与连接事件关联的第八个监控器规则的 ID。

表 B-29　连接统计信息数据块 5.1 字段 （续）

字段	数据类型	说明
安全情报源 / 目标 (Security Intelligence Source/ Destination)	uint8	源或目标 IP 地址与 IP 阻止列表是否匹配。
安全情报层 (Security Intelligence Layer)	uint8	与 IP 阻止列表匹配的 IP 层。

连接统计信息数据块 5.2.x

连接统计信息数据块在连接数据消息中使用。版本 5.1.1 到版本 5.2 的连接数据块变更包括添加了用于支持地理位置的新字段。用于版本 5.2.x 的连接统计信息数据块的块类型为系列 1 数据块组中的 144。它否决了块类型 137，连接统计信息数据块 5.1.1.x，第 B-156 页。

有关连接统计信息数据消息的详细信息，请参阅连接统计信息数据消息，第 4-54 页。

下图显示用于 5.2.x 的连接统计信息数据块的格式：

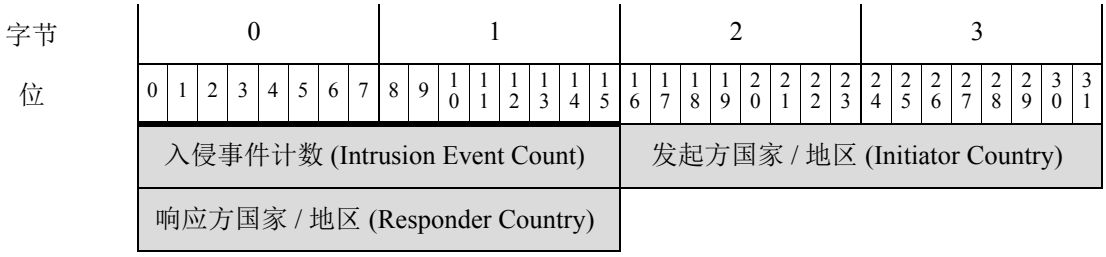
::

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
连接数据块类型 (144) (Connection Data Block Type (144))																																
连接数据块长度 (Connection Data Block Length)																																
设备 ID (Device ID)																																
入口区 (Ingress Zone) 入口区 (Ingress Zone) （续） 入口区 (Ingress Zone) （续） 入口区 (Ingress Zone) （续）																																
出口区 (Egress Zone) 出口区 (Egress Zone) （续） 出口区 (Egress Zone) （续） 出口区 (Egress Zone) （续）																																
入口接口 (Ingress Interface)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
入口接口 (Ingress Interface)																																
入口接口 (Ingress Interface) （续）																																
入口接口 (Ingress Interface) （续）																																
出口接口 (Egress Interface)																																
出口接口 (Egress Interface) （续）																																
出口接口 (Egress Interface) （续）																																
出口接口 (Egress Interface) （续）																																
发起方 IP 地址 (Initiator IP Address)																																
发起方 IP 地址 (Initiator IP Address) （续）																																
发起方 IP 地址 (Initiator IP Address) （续）																																
发起方 IP 地址 (Initiator IP Address) （续）																																
响应方 IP 地址 (Responder IP Address)																																
响应方 IP 地址 (Responder IP Address) （续）																																
响应方 IP 地址 (Responder IP Address) （续）																																
响应方 IP 地址 (Responder IP Address) （续）																																
策略修订 (Policy Revision)																																
策略修订 (Policy Revision) （续）																																
策略修订 (Policy Revision) （续）																																
策略修订 (Policy Revision) （续）																																
规则 ID (Rule ID)																																
规则操作 (Rule Action)																	规则原因 (Rule Reason)														
发起方端口 (Initiator Port)																	响应方端口 (Responder Port)														
TCP 标志 (TCP Flags)																	协议 (Protocol)								NetFlow 源 (NetFlow Source)							
Netflow 源 (Netflow Source) （续）																																


字节
位
0
1
2
3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Netflow 源 (Netflow Source) （续）
Netflow 源 (Netflow Source) （续）
Netflow 源 (Netflow Source) （续）
实例 ID (Instance ID)
实例 ID (Instance ID) （续）
连接计数器 (Connection Counter)
第一个数据包时间 (First Pkt Time)
第一个数据包时间戳 (First Packet Timestamp) （续）
最后一个数据包时间 (Last Pkt Time)
最后一个数据包时间戳 (Last Packet Timestamp) （续）
发起方传输的数据包数 (Initiator Transmitted Packets)
发起方传输的数据包数 (Initiator Transmitted Packets) （续）
发起方传输的数据包数 (Initiator Transmitted Packets) （续）
响应方传输的数据包数 (Resp. Tx Packets)
响应方传输的数据包数 (Responder Transmitted Packets) （续）
响应方传输的数据包数 (Responder Transmitted Packets) （续）
发起方传输的字节数 (Initiator Tx Bytes)
发起方传输的字节数 (Initiator Transmitted Bytes) （续）
发起方传输的字节数 (Initiator Transmitted Bytes) （续）
响应方传输的字节数 (Resp. Tx Bytes)
响应方传输的字节数 (Responder Transmitted Bytes) （续）
响应方传输的字节数 (Responder Transmitted Bytes) （续）
用户 ID (User ID)
用户 ID (User ID) （续）
应用协议 ID (Application Protocol ID)
应用协议 ID (Application Protocol ID) （续）
URL 类别 (URL Category)
URL 类别 (URL Category) （续）
URL 信誉 (URL Reputation)

	字节	0								1								2								3							
	位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
		URL 信誉 (URL Reputation) （续）																								客户端应用 ID (Client App ID)							
		客户端应用 ID (Client Application ID) （续）																								Web 应用 ID (Web App ID)							
客户端 URL		Web 应用 ID (Web Application ID) （续）																								字符串块类型 (0) (Str. Block Type (0))							
		字符串块类型 (String Block Type) （续）																								字符串块长度 (String Block Length)							
		字符串块长度 (String Block Length) （续）																								客户端应用 URL... (Client App. URL...)							
NetBIOS 名称		字符串块类型 (0) (String Block Type (0))																															
		字符串块长度 (String Block Length)																															
		NetBIOS 名称 ...(NetBIOS Name...)																															
客户端应用版本 (Client App Version)		字符串块类型 (0) (String Block Type (0))																															
		字符串块长度 (String Block Length)																															
		客户端应用版本 ...(Client Application Version...)																															
		监控器规则 1 (Monitor Rule 1)																															
		监控器规则 2 (Monitor Rule 2)																															
		监控器规则 3 (Monitor Rule 3)																															
		监控器规则 4 (Monitor Rule 4)																															
		监控器规则 5 (Monitor Rule 5)																															
		监控器规则 6 (Monitor Rule 6)																															
		监控器规则 7 (Monitor Rule 7)																															
		监控器规则 8 (Monitor Rule 8)																															
		安全接口源 / 目标 (Sec. Int. Src/Dst)								安全接口层 (Sec. Int. Layer)								文件事件计数 (File Event Count)															



下表对用于 5.2.x 的连接统计信息数据块的字段进行了说明：

表 B-30　　连接统计信息数据块 5.2.x 字段

字段	数据类型	说明
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 5.2.x 的连接统计信息数据块。值始终为 144。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID (Device ID)	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP Address)	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP Address)	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号 （如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符 （如适用）。
规则操作 (Rule Action)	uint16	在用户界面中选择的针对该规则的操作 （允许、阻止等）。
规则原因 (Rule Reason)	uint16	规则触发事件的原因。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。

表 B-30 连接统计信息数据块 5.2.x 字段 （续）

字段	数据类型	说明
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址。
实例 ID (Instance ID)	uint16	生成事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的 UNIX 时间戳。
发起方传输的数据包数 (Initiator Transmitted Packets)	uint64	发起主机传输的数据包数。
响应方传输的数据包数 (Responder Transmitted Packets)	uint64	响应主机传输的数据包数。
发起方传输的字节数 (Initiator Transmitted Bytes)	uint64	发起主机传输的字节数。
响应方传输的字节数 (Responder Transmitted Bytes)	uint64	响应主机传输的字节数。
用户 ID (User ID)	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号 （如适用）。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号 （如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。

表 B-30　连接统计信息数据块 5.2.x 字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的 URL （如适用）（例如，`/files/index.html`）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本 (Client Application Version)	字符串	客户端应用版本。
监控器规则 1 (Monitor Rule 1)	uint32	与连接事件关联的第一个监控器规则的 ID。
监控器规则 2 (Monitor Rule 2)	uint32	与连接事件关联的第二个监控器规则的 ID。
监控器规则 3 (Monitor Rule 3)	uint32	与连接事件关联的第三个监控器规则的 ID。
监控器规则 4 (Monitor Rule 4)	uint32	与连接事件关联的第四个监控器规则的 ID。
监控器规则 5 (Monitor Rule 5)	uint32	与连接事件关联的第五个监控器规则的 ID。
监控器规则 6 (Monitor Rule 6)	uint32	与连接事件关联的第六个监控器规则的 ID。
监控器规则 7 (Monitor Rule 7)	uint32	与连接事件关联的第七个监控器规则的 ID。
监控器规则 8 (Monitor Rule 8)	uint32	与连接事件关联的第八个监控器规则的 ID。
安全情报源 / 目标 (Security Intelligence Source/ Destination)	uint8	源或目标 IP 地址与 IP 阻止列表是否匹配。
安全情报层 (Security Intelligence Layer)	uint8	与 IP 阻止列表匹配的 IP 层。
文件事件计数 (File Event Count)	uint16	用于区别同一秒发生的文件事件的值。

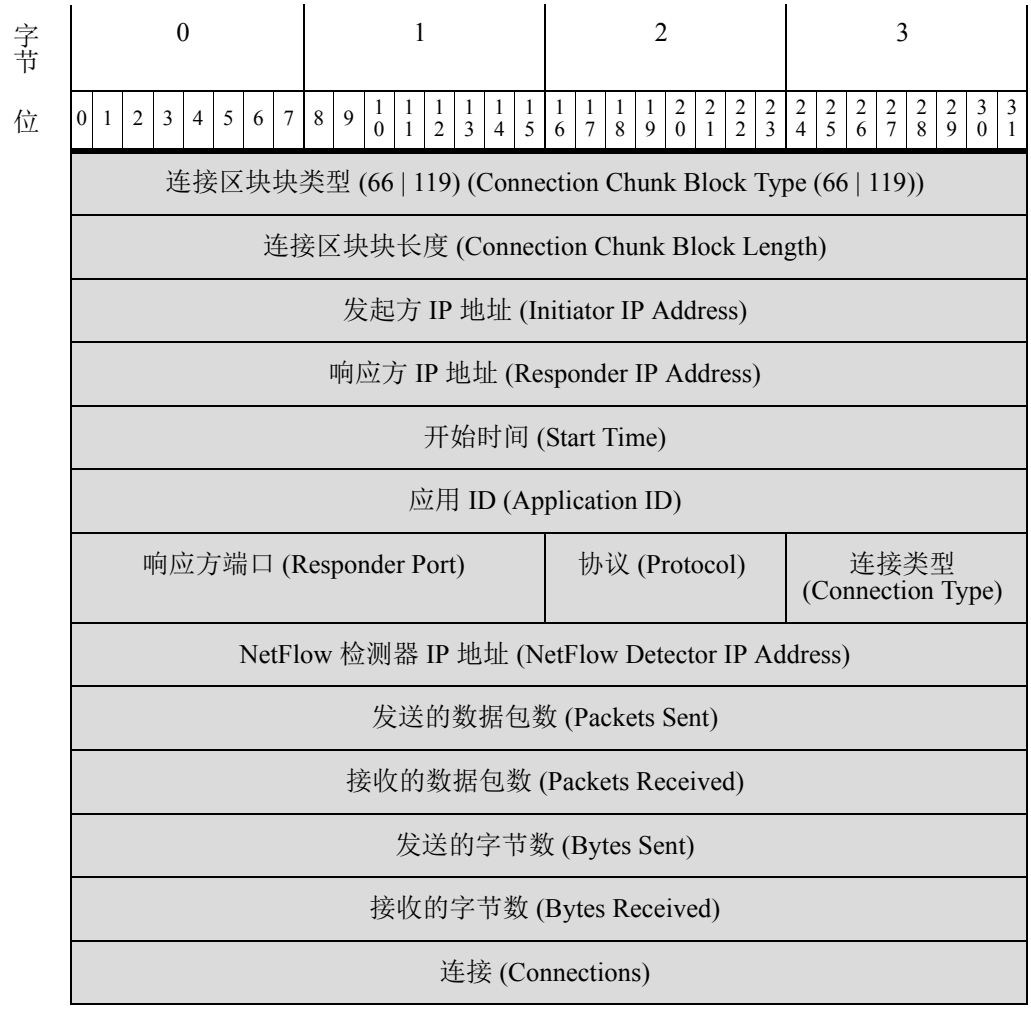
表 B-30　　连接统计信息数据块 5.2.x 字段 （续）

字段	数据类型	说明
入侵事件 (Intrusion Event) （续）	uint16	用于区别同一秒发生的入侵事件的值。
发起方国家 / 地区 (Initiator Country)	uint16	发起主机的国家 / 地区代码。
响应方国家 / 地区 (Responder Country)	uint16	响应主机的国家 / 地区代码。

用于 5.0 - 5.1 的连接区块数据块

连接区块数据块传送 NetFlow 设备检测到的连接数据。在 4.10.1 之前的版本中，连接区块数据块的块类型为 66。在版本 5.0 - 5.1 中，其块类型为 119。

下图显示连接区块数据块的格式：



下表对连接区块数据块的组件进行了说明：

表 B-31　　连接区块数据块字段

字段	数据类型	说明
连接区块块类型 (Connection Chunk Block Type)	uint32	启动连接区块数据块。在 4.10.1 之前的版本中，此值 66，在版本 5.0 中，此值为 119。
连接区块块长度 (Connection Chunk Block Length)	uint32	连接区块数据块中的字节总数，包括连接区块块类型和长度字段的八个字节，加上随后的连接区块数据中的字节数。
发起方 IP 地址 (Initiator IP Address)	uint8[4]	发起连接的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP Address)	uint8[4]	响应连接的主机的 IP 地址，采用 IP 地址八位组。
开始时间 (Start Time)	uint32	连接区块的开始时间。
应用 ID (Application ID)	uint32	连接中使用的应用协议的应用标识号。
响应方端口 (Responder Port)	uint16	响应者在连接区块中使用的端口。
协议 (Protocol)	uint8	用于包含用户信息的数据包的协议。
连接类型 (Connection Type)	uint8	连接的类型。
源设备 IP 地址 (Source 设备 IP Address)	uint8[4]	检测到连接的 NetFlow 设备的 IP 地址，采用 IP 地址八位组。
发送的数据包数 (Packets Sent)	uint32	在连接区块中发送的数据包数。
接收的数据包数 (Packets Received)	uint32	在连接区块中接收的数据包数。
发送的字节数 (Bytes Sent)	uint32	在连接区块中发送的字节数。
接收的字节数 (Bytes Received)	uint32	在连接区块中接收的字节数。
连接 (Connections)	uint32	在连接区块中进行的会话数。

用于 5.1.1-6.0.x 的连接区块数据块

连接区块数据块传送连接数据。它存储五分钟内汇聚的连接日志数据。连接区块数据块的块类型为系列 1 数据块组中的 136。它替代块类型 119。

下图显示连接区块数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
连接区块块类型 (136) (Connection Chunk Block Type (136))																																
连接区块块长度 (Connection Chunk Block Length)																																
发起方 IP 地址 (Initiator IP Address)																																
响应方 IP 地址 (Responder IP Address)																																
开始时间 (Start Time)																																
应用协议 (Application Protocol)																																
响应方端口 (Responder Port)																	协议 (Protocol)								连接类型 (Connection Type)							
NetFlow 检测器 IP 地址 (NetFlow Detector IP Address)																																
发送的数据包数 (Packets Sent) 发送的数据包数 (Packets Sent) （续）																																
接收的数据包数 (Packets Received) 接收的数据包数 (Packets Received) （续）																																
发送的字节数 (Bytes Sent) 发送的字节数 (Bytes Sent) （续）																																
接收的字节数 (Bytes Received) 接收的字节数 (Bytes Received) （续）																																
连接 (Connections)																																

下表对连接区块数据块的组件进行了说明。

表 B-32　　连接区块数据块字段

字段	数据类型	说明
连接区块块类型 (Connection Chunk Block Type)	uint32	启动连接区块数据块。值始终为 136。
连接区块块长度 (Connection Chunk Block Length)	uint32	连接区块数据块中的字节总数，包括连接区块块类型和长度字段的八个字节，加上随后的连接区块数据中的字节数。
发起方 IP 地址 (Initiator IP Address)	uint8(4)	此类型连接的发起方的 IP 地址。与响应方 IP 地址一起使用，以识别相同连接。
响应方 IP 地址 (Responder IP Address)	uint8(4)	此类型连接的响应方的 IP 地址。与发起方 IP 地址一起使用，以识别相同连接。
开始时间 (Start Time)	uint32	连接区块的开始时间。
应用协议 (Application Protocol)	uint32	连接中使用的协议的标识号。
响应方端口 (Responder Port)	uint16	响应者在连接区块中使用的端口。
协议 (Protocol)	uint8	用于包含用户信息的数据包的协议。
连接类型 (Connection Type)	uint8	连接的类型。
NetFlow 检测器 IP 地址 (NetFlow Detector IP Address)	uint8[4]	检测到连接的 NetFlow 设备的 IP 地址，采用 IP 地址八位组。
发送的数据包数 (Packets Sent)	uint64	在连接区块中发送的数据包数。
接收的数据包数 (Packets Received)	uint64	在连接区块中接收的数据包数。
发送的字节数 (Bytes Sent)	uint64	在连接区块中发送的字节数。
接收的字节数 (Bytes Received)	uint64	在连接区块中接收的字节数。
连接 (Connections)	uint32	五分钟内的连接数。

连接统计信息数据块 5.1.1.x

连接统计信息数据块在连接数据消息中使用。版本 5.1 到版本 5.1.1 的连接数据块变更包括添加了用于识别相关入侵事件的新字段。用于版本 5.1.1.x 的连接统计信息数据块的块类型为 137。它否决了块类型 126，连接统计信息数据块 5.1，第 B-138 页。

有关连接统计信息数据消息的详细信息，请参阅连接统计信息数据消息，第 4-54 页。

下图显示用于 5.1.1 的连接统计信息数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
连接数据块类型 (137) (Connection Data Block Type (137))																																
连接数据块长度 (Connection Data Block Length)																																
设备 ID (Device ID)																																
入口区 (Ingress Zone)																																
入口区 (Ingress Zone) （续）																																
入口区 (Ingress Zone) （续）																																
入口区 (Ingress Zone) （续）																																
出口区 (Egress Zone)																																
出口区 (Egress Zone) （续）																																
出口区 (Egress Zone) （续）																																
出口区 (Egress Zone) （续）																																
入口接口 (Ingress Interface)																																
入口接口 (Ingress Interface) （续）																																
入口接口 (Ingress Interface) （续）																																
入口接口 (Ingress Interface) （续）																																
出口接口 (Egress Interface)																																
出口接口 (Egress Interface) （续）																																
出口接口 (Egress Interface) （续）																																
出口接口 (Egress Interface) （续）																																
发起方 IP 地址 (Initiator IP Address)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
发起方 IP 地址 (Initiator IP Address) （续）																																
发起方 IP 地址 (Initiator IP Address) （续）																																
发起方 IP 地址 (Initiator IP Address) （续）																																
响应方 IP 地址 (Responder IP Address)																																
响应方 IP 地址 (Responder IP Address) （续）																																
响应方 IP 地址 (Responder IP Address) （续）																																
响应方 IP 地址 (Responder IP Address) （续）																																
策略修订 (Policy Revision)																																
策略修订 (Policy Revision) （续）																																
策略修订 (Policy Revision) （续）																																
策略修订 (Policy Revision) （续）																																
规则 ID (Rule ID)																																
规则操作 (Rule Action)																	规则原因 (Rule Reason)														
发起方端口 (Initiator Port)																	响应方端口 (Responder Port)														
TCP 标志 (TCP Flags)																	协议 (Protocol)								NetFlow 源 (NetFlow Source)						
Netflow 源 (Netflow Source) （续）																																
Netflow 源 (Netflow Source) （续）																																
Netflow 源 (Netflow Source) （续）																																
Netflow 源 (Netflow Source) （续）																									实例 ID (Instance ID)							
实例 ID (Instance ID) （续）									连接计数器 (Connection Counter)																				第一个数据包时间 (First Pkt Time)							
第一个数据包时间戳 (First Packet Timestamp) （续）																																
最后一个数据包时间 (Last Pkt Time)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
最后一个数据包时间戳 (Last Packet Timestamp) （续）																									发起方传输的数据包数 (Initiator Transmitted Packets)							
发起方传输的数据包数 (Initiator Transmitted Packets) （续）																																
发起方传输的数据包数 (Initiator Transmitted Packets) （续）																									响应方传输的数据包数 (Resp. Tx Packets)							
响应方传输的数据包数 (Responder Transmitted Packets) （续）																																
响应方传输的数据包数 (Responder Transmitted Packets) （续）																									发起方传输的字节数 (Initiator Tx Bytes)							
发起方传输的字节数 (Initiator Transmitted Bytes) （续）																																
发起方传输的字节数 (Initiator Transmitted Bytes) （续）																									响应方传输的字节数 (Resp. Tx Bytes)							
响应方传输的字节数 (Responder Transmitted Bytes) （续）																																
响应方传输的字节数 (Responder Transmitted Bytes) （续）																									用户 ID (User ID)							
用户 ID (User ID) （续）																									应用协议 ID (Application Protocol ID)							
应用协议 ID (Application Protocol ID) （续）																									URL 类别 (URL Category)							
URL 类别 (URL Category) （续）																									URL 信誉 (URL Reputation)							
URL 信誉 (URL Reputation) （续）																									客户端应用 ID (Client App ID)							
客户端应用 ID (Client Application ID) （续）																									Web 应用 ID (Web App ID)							

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
客户端 URL	Web 应用 ID (Web Application ID) （续）																								字符串块类型 (0) (Str. Block Type (0))							
	字符串块类型 (String Block Type) （续）																								字符串块长度 (String Block Length)							
	字符串块长度 (String Block Length （续）																								客户端应用 URL... (Client App. URL...)							
NetBIOS 名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	NetBIOS 名称 ...(NetBIOS Name...)																															
客户端应用版本 (Client App Version)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	客户端应用版本 ...(Client Application Version...)																															
	监控器规则 1 (Monitor Rule 1)																															
	监控器规则 2 (Monitor Rule 2)																															
	监控器规则 3 (Monitor Rule 3)																															
	监控器规则 4 (Monitor Rule 4)																															
	监控器规则 5 (Monitor Rule 5)																															
	监控器规则 6 (Monitor Rule 6)																															
	监控器规则 7 (Monitor Rule 7)																															
	监控器规则 8 (Monitor Rule 8)																															
	安全接口源 / 目标 (Sec. Int. Src/Dst)								安全接口层 (Sec. Int. Layer)								文件事件计数 (File Event Count)															
	入侵事件计数 (Intrusion Event Count)																															

下表对用于 5.1.1.x 的连接统计信息数据块的字段进行了说明。

表 B-33 连接统计信息数据块 5.1.1.x 字段

字段	数据类型	说明
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 5.1.1.x 的连接统计信息数据块。值始终为 137。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID (Device ID)	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP Address)	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP Address)	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号 （如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符 （如适用）。
规则操作 (Rule Action)	uint16	在用户界面中选择的针对该规则的操作 （允许、阻止等）。
规则原因 (Rule Reason)	uint16	规则触发事件的原因。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议	uint8	IANA 指定的协议号。
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址。

表 B-33　连接统计信息数据块 5.1.1.x 字段 （续）

字段	数据类型	说明
实例 ID (Instance ID)	uint16	生成事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的 UNIX 时间戳。
发起方传输的数据包数 (Initiator Transmitted Packets)	uint64	发起主机传输的数据包数。
响应方传输的数据包数 (Responder Transmitted Packets)	uint64	响应主机传输的数据包数。
发起方传输的字节数 (Initiator Transmitted Bytes)	uint64	发起主机传输的字节数。
响应方传输的字节数 (Responder Transmitted Bytes)	uint64	响应主机传输的字节数。
用户 ID (User ID)	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号 （如适用）。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号 （如适用）。

表 B-33 连接统计信息数据块 5.1.1.x 字段 （续）

字段	数据类型	说明
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的 URL （如适用）（例如， /files/index.html）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本 (Client Application Version)	字符串	客户端应用版本。
监控器规则 1 (Monitor Rule 1)	uint32	与连接事件关联的第一个监控器规则的 ID。
监控器规则 2 (Monitor Rule 2)	uint32	与连接事件关联的第二个监控器规则的 ID。
监控器规则 3 (Monitor Rule 3)	uint32	与连接事件关联的第三个监控器规则的 ID。
监控器规则 4 (Monitor Rule 4)	uint32	与连接事件关联的第四个监控器规则的 ID。
监控器规则 5 (Monitor Rule 5)	uint32	与连接事件关联的第五个监控器规则的 ID。
监控器规则 6 (Monitor Rule 6)	uint32	与连接事件关联的第六个监控器规则的 ID。
监控器规则 7 (Monitor Rule 7)	uint32	与连接事件关联的第七个监控器规则的 ID。
监控器规则 8 (Monitor Rule 8)	uint32	与连接事件关联的第八个监控器规则的 ID。

表 B-33　连接统计信息数据块 5.1.1.x 字段 （续）

字段	数据类型	说明
安全情报源 / 目标 (Security Intelligence Source/ Destination)	uint8	源或目标 IP 地址与 IP 阻止列表是否匹配。
安全情报层 (Security Intelligence Layer)	uint8	与 IP 阻止列表匹配的 IP 层。
文件事件计数 (File Event Count)	uint16	用于区别同一秒发生的文件事件的值。
入侵事件计数 (Intrusion Event Count)	uint16	用于区别同一秒发生的入侵事件的值。

连接统计信息数据块 5.3

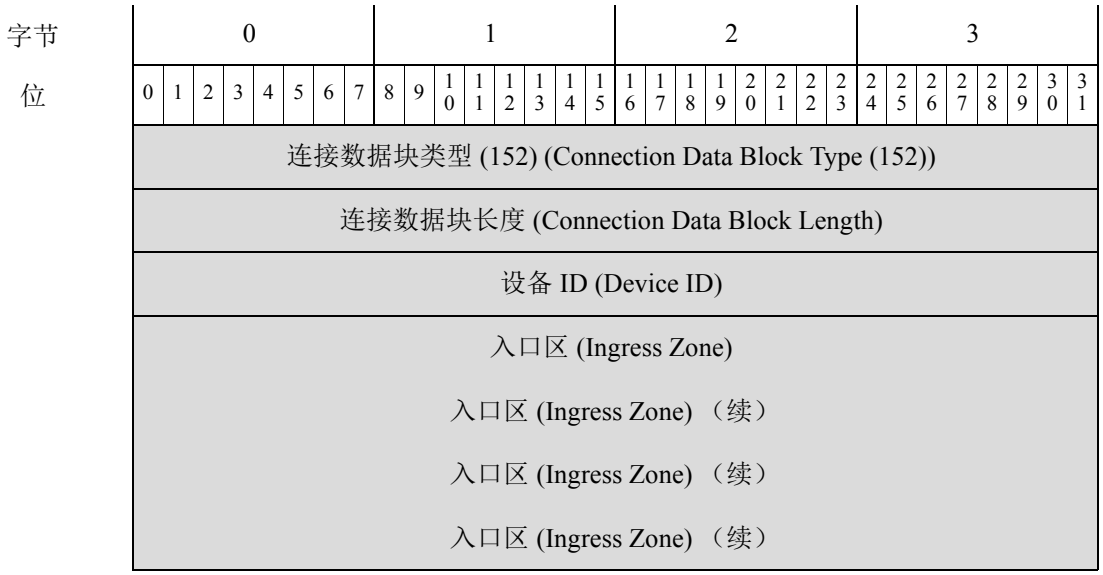
连接统计信息数据块在连接数据消息中使用。版本 5.2.x 到版本 5.3 的连接数据块变更包括添加了用于 NetFlow 信息的新字段。用于版本 5.3 的连接统计信息数据块的块类型为系列 1 数据块组中的 152。它否决了块类型 144，连接统计信息数据块 5.2.x，第 B-145 页。

您可以通过在事件版本为 10 且事件代码为 71 的请求消息中设置扩展事件标志 （请求标志字段中的位 30）请求扩展事件记录。请参阅请求标志，第 2-11 页。如果您启用位 23，则记录中会包含扩展事件报头。

有关连接统计信息数据消息的详细信息，请参阅连接统计信息数据消息，第 4-54 页。

下图显示用于 5.3+ 的连接统计信息数据块的格式：

::



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
出口区 (Egress Zone)																																
出口区 (Egress Zone) （续）																																
出口区 (Egress Zone) （续）																																
出口区 (Egress Zone) （续）																																
入口接口 (Ingress Interface)																																
入口接口 (Ingress Interface) （续）																																
入口接口 (Ingress Interface) （续）																																
入口接口 (Ingress Interface) （续）																																
出口接口 (Egress Interface)																																
出口接口 (Egress Interface) （续）																																
出口接口 (Egress Interface) （续）																																
出口接口 (Egress Interface) （续）																																
发起方 IP 地址 (Initiator IP Address)																																
发起方 IP 地址 (Initiator IP Address) （续）																																
发起方 IP 地址 (Initiator IP Address) （续）																																
发起方 IP 地址 (Initiator IP Address) （续）																																
响应方 IP 地址 (Responder IP Address)																																
响应方 IP 地址 (Responder IP Address) （续）																																
响应方 IP 地址 (Responder IP Address) （续）																																
响应方 IP 地址 (Responder IP Address) （续）																																
策略修订 (Policy Revision)																																
策略修订 (Policy Revision) （续）																																
策略修订 (Policy Revision) （续）																																
策略修订 (Policy Revision) （续）																																


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
规则 ID (Rule ID)
规则操作 (Rule Action)
规则原因 (Rule Reason)
发起方端口 (Initiator Port)
响应方端口 (Responder Port)
TCP 标志 (TCP Flags)
协议 (Protocol)
NetFlow 源 (NetFlow Source)
Netflow 源 (Netflow Source) （续）
Netflow 源 (Netflow Source) （续）
Netflow 源 (Netflow Source) （续）
Netflow 源 (Netflow Source) （续）
实例 ID (Instance ID)
实例 ID (Instance ID) （续）
连接计数器 (Connection Counter)
第一个数据包时间 (First Pkt Time)
第一个数据包时间戳 (First Packet Timestamp) （续）
最后一个数据包时间 (Last Pkt Time)
最后一个数据包时间戳 (Last Packet Timestamp) （续）
发起方传输的数据包数 (Initiator Transmitted Packets)
发起方传输的数据包数 (Initiator Transmitted Packets) （续）
响应方传输的数据包数 (Resp. Tx Packets)
响应方传输的数据包数 (Responder Transmitted Packets) （续）
响应方传输的数据包数 (Responder Transmitted Packets) （续）
发起方传输的字节数 (Initiator Tx Bytes)
发起方传输的字节数 (Initiator Transmitted Bytes) （续）
发起方传输的字节数 (Initiator Transmitted Bytes) （续）
响应方传输的字节数 (Resp. Tx Bytes)
响应方传输的字节数 (Responder Transmitted Bytes) （续）

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	响应方传输的字节数 (Responder Transmitted Bytes) （续）																								用户 ID (User ID)							
	用户 ID (User ID) （续）																								应用协议 ID (Application Protocol ID)							
	应用协议 ID (Application Protocol ID) （续）																								URL 类别 (URL Category)							
	URL 类别 (URL Category) （续）																								URL 信誉 (URL Reputation)							
	URL 信誉 (URL Reputation) （续）																								客户端应用 ID (Client App ID)							
	客户端应用 ID (Client Application ID) （续）																								Web 应用 ID (Web App ID)							
客户端 URL	Web 应用 ID (Web Application ID) （续）																								字符串块类型 (0) (Str. Block Type (0))							
	字符串块类型 (String Block Type) （续）																								字符串块长度 (String Block Length)							
	字符串块长度 (String Block Length) （续）																								客户端应用 URL... (Client App. URL...)							
NetBIOS 名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	NetBIOS 名称 ...(NetBIOS Name...)																															
客户端应用版本 (Client App Version)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	客户端应用版本 ...(Client Application Version...)																															
	监控器规则 1 (Monitor Rule 1)																															
	监控器规则 2 (Monitor Rule 2)																															
	监控器规则 3 (Monitor Rule 3)																															
	监控器规则 4 (Monitor Rule 4)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
监控器规则 5 (Monitor Rule 5)																																
监控器规则 6 (Monitor Rule 6)																																
监控器规则 7 (Monitor Rule 7)																																
监控器规则 8 (Monitor Rule 8)																																
安全接口源 / 目标 (Sec. Int. Src/Dst)									安全接口层 (Sec. Int. Layer)								文件事件计数 (File Event Count)															
入侵事件计数 (Intrusion Event Count)																	发起方国家 / 地区 (Initiator Country)														
响应方国家 / 地区 (Responder Country)																	IOC 编号 (IOC Number)														
源自治系统 (Source Autonomous System)																																
目标自治系统 (Destination Autonomous System)																																
SNMP 输入 (SNMP In)																	SNMP 输出 (SNMP Out)														
源 TOS (Source TOS)									目标 TOS (Destination TOS)								源掩码 (Source Mask)								目标掩码 (Destination Mask)							

下表对用于 5.3 的连接统计信息数据块的字段进行了说明。

表 B-34　　连接统计信息数据块 5.3+ 字段

字段	数据类型	说明
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 5.3 的连接统计信息数据块。值始终为 `152`。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID (Device ID)	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。

表 B-34 连接统计信息数据块 5.3+ 字段 （续）

字段	数据类型	说明
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP Address)	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP Address)	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号 （如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符 （如适用）。
规则操作 (Rule Action)	uint16	在用户界面中选择的针对该规则的操作 （允许、阻止等）。
规则原因 (Rule Reason)	uint16	规则触发事件的原因。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址。
实例 ID (Instance ID)	uint16	生成事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的 UNIX 时间戳。
发起方传输的数据包数 (Initiator Transmitted Packets)	uint64	发起主机传输的数据包数。

表 B-34　连接统计信息数据块 5.3+ 字段 （续）

字段	数据类型	说明
响应方传输的数据包数 (Responder Transmitted Packets)	uint64	响应主机传输的数据包数。
发起方传输的字节数 (Initiator Transmitted Bytes)	uint64	发起主机传输的字节数。
响应方传输的字节数 (Responder Transmitted Bytes)	uint64	响应主机传输的字节数。
用户 ID (User ID)	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号 （如适用）。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号 （如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。
字符串块长度 (String Block Type)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的 URL （如适用）（例如， `/files/index.html`）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。

表 B-34 连接统计信息数据块 5.3+ 字段 （续）

字段	数据类型	说明
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本 (Client Application Version)	字符串	客户端应用版本。
监控器规则 1 (Monitor Rule 1)	uint32	与连接事件关联的第一个监控器规则的 ID。
监控器规则 2 (Monitor Rule 2)	uint32	与连接事件关联的第二个监控器规则的 ID。
监控器规则 3 (Monitor Rule 3)	uint32	与连接事件关联的第三个监控器规则的 ID。
监控器规则 4 (Monitor Rule 4)	uint32	与连接事件关联的第四个监控器规则的 ID。
监控器规则 5 (Monitor Rule 5)	uint32	与连接事件关联的第五个监控器规则的 ID。
监控器规则 6 (Monitor Rule 6)	uint32	与连接事件关联的第六个监控器规则的 ID。
监控器规则 7 (Monitor Rule 7)	uint32	与连接事件关联的第七个监控器规则的 ID。
监控器规则 8 (Monitor Rule 8)	uint32	与连接事件关联的第八个监控器规则的 ID。
安全情报源 / 目标 (Security Intelligence Source/ Destination)	uint8	源或目标 IP 地址与 IP 阻止列表是否匹配。
安全情报层 (Security Intelligence Layer)	uint8	与 IP 阻止列表匹配的 IP 层。
文件事件计数 (File Event Count)	uint16	用于区别同一秒发生的文件事件的值。
入侵事件 (Intrusion Event) （续）	uint16	用于区别同一秒发生的入侵事件的值。
发起方国家 / 地区 (Initiator Country)	uint16	发起主机的国家 / 地区代码。

表 B-34　连接统计信息数据块 5.3+ 字段 （续）

字段	数据类型	说明
响应方国家 / 地区 (Responder Country)	uint 16	响应主机的国家 / 地区代码。
IOC 编号 (IOC Number)	uint16	与此事件相关的危害的 ID 号码。
源自治系统 (Source Autonomous System)	uint32	作为源或对等体的源自治系统的编号。
目标自治系统 (Destination Autonomous System)	uint32	作为源或对等体的目标自治系统的编号。
SNMP 输入 (SNMP Input)	uint16	输入接口的 SNMP 索引。
SNMP 输出 (SNMP Output)	uint16	输出接口的 SNMP 索引。
源 TOS (Source TOS)	uint8	传入接口的服务字节设置类型。
目标 TOS (Destination TOS)	uint8	传出接口的服务字节设置类型。
源掩码 (Source Mask)	uint8	源地址前缀掩码。
目标掩码 (Destination Mask)	uint8	目标地址前缀掩码。

连接统计信息数据块 5.3.1

连接统计信息数据块在连接数据消息中使用。从版本 5.3 到版本 5.3.1 对连接数据块进行的唯一变更是添加了安全情景字段。用于版本 5.3.1 的连接统计信息数据块的块类型为系列 1 数据块组中的 154。它否决了块类型 152，连接统计信息数据块 5.3，第 B-163 页。

您可以通过在事件版本为 11 且事件代码为 71 的请求消息中设置扩展事件标志 （请求标志字段中的位 30）请求扩展事件记录。请参阅请求标志，第 2-11 页。如果您启用位 23，则记录中会包含扩展事件报头。有关连接统计信息数据消息的详细信息，请参阅连接统计信息数据消息，第 4-54 页。

下图显示用于 5.3.1 的连接统计信息数据块的格式：

::

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
连接数据块类型 (154) (Connection Data Block Type (154))																																
连接数据块长度 (Connection Data Block Length)																																
设备 ID (Device ID)																																
入口区 (Ingress Zone)																																
入口区 (Ingress Zone) （续）																																
入口区 (Ingress Zone) （续）																																
入口区 (Ingress Zone) （续）																																
出口区 (Egress Zone)																																
出口区 (Egress Zone) （续）																																
出口区 (Egress Zone) （续）																																
出口区 (Egress Zone) （续）																																
入口接口 (Ingress Interface)																																
入口接口 (Ingress Interface) （续）																																
入口接口 (Ingress Interface) （续）																																
入口接口 (Ingress Interface) （续）																																
出口接口 (Egress Interface)																																
出口接口 (Egress Interface) （续）																																
出口接口 (Egress Interface) （续）																																
出口接口 (Egress Interface) （续）																																
发起方 IP 地址 (Initiator IP Address)																																
发起方 IP 地址 (Initiator IP Address) （续）																																
发起方 IP 地址 (Initiator IP Address) （续）																																
发起方 IP 地址 (Initiator IP Address) （续）																																
响应方 IP 地址 (Responder IP Address)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
响应方 IP 地址 (Responder IP Address) （续）																																
响应方 IP 地址 (Responder IP Address) （续）																																
响应方 IP 地址 (Responder IP Address) （续）																																
策略修订 (Policy Revision)																																
策略修订 (Policy Revision) （续）																																
策略修订 (Policy Revision) （续）																																
策略修订 (Policy Revision) （续）																																
规则 ID (Rule ID)																																
规则操作 (Rule Action)																	规则原因 (Rule Reason)														
发起方端口 (Initiator Port)																	响应方端口 (Responder Port)														
TCP 标志 (TCP Flags)																	协议 (Protocol)								NetFlow 源 (NetFlow Source)						
Netflow 源 (Netflow Source) （续）																																
Netflow 源 (Netflow Source) （续）																																
Netflow 源 (Netflow Source) （续）																																
Netflow 源 (Netflow Source) （续）																									实例 ID (Instance ID)							
实例 ID (Instance ID) （续）									连接计数器 (Connection Counter)																				第一个数据包时间 (First Pkt Time)							
第一个数据包时间戳 (First Packet Timestamp) （续）																									最后一个数据包时间 (Last Pkt Time)							
最后一个数据包时间戳 (Last Packet Timestamp) （续）																									发起方传输的数据包数 (Initiator Transmitted Packets)							
发起方传输的数据包数 (Initiator Transmitted Packets) （续）																																
发起方传输的数据包数 (Initiator Transmitted Packets) （续）																									响应方传输的数据包数 (Resp. Tx Packets)							

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	响应方传输的数据包数 (Responder Transmitted Packets) （续）																															
	响应方传输的数据包数 (Responder Transmitted Packets) （续）																								发起方传输的字节数 (Initiator Tx Bytes)							
	发起方传输的字节数 (Initiator Transmitted Bytes) （续）																															
	发起方传输的字节数 (Initiator Transmitted Bytes) （续）																								响应方传输的字节数 (Resp. Tx Bytes)							
	响应方传输的字节数 (Responder Transmitted Bytes) （续）																															
	响应方传输的字节数 (Responder Transmitted Bytes) （续）																								用户 ID (User ID)							
	用户 ID (User ID) （续）																								应用协议 ID (Application Protocol ID)							
	应用协议 ID (Application Protocol ID) （续）																								URL 类别 (URL Category)							
	URL 类别 (URL Category) （续）																								URL 信誉 (URL Reputation)							
	URL 信誉 (URL Reputation) （续）																								客户端应用 ID (Client App ID)							
	客户端应用 ID (Client Application ID) （续）																								Web 应用 ID (Web App ID)							
客户端 URL	Web 应用 ID (Web Application ID) （续）																								字符串块类型 (0) (Str. Block Type (0))							
	字符串块类型 (String Block Type) （续）																								字符串块长度 (String Block Length)							
	字符串块长度 (String Block Length) （续）																								客户端应用 URL... (Client App. URL...)							
NetBIOS 名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	NetBIOS 名称 ...(NetBIOS Name...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
客户端应用版本 (Client App Version)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	客户端应用版本 ...(Client Application Version...)																															
	监控器规则 1 (Monitor Rule 1)																															
	监控器规则 2 (Monitor Rule 2)																															
	监控器规则 3 (Monitor Rule 3)																															
	监控器规则 4 (Monitor Rule 4)																															
	监控器规则 5 (Monitor Rule 5)																															
	监控器规则 6 (Monitor Rule 6)																															
	监控器规则 7 (Monitor Rule 7)																															
	监控器规则 8 (Monitor Rule 8)																															
	安全接口源 / 目标 (Sec. Int. Src/Dst)								安全接口层 (Sec. Int. Layer)								文件事件计数 (File Event Count)															
	入侵事件计数 (Intrusion Event Count)																发起方国家 / 地区 (Initiator Country)															
	响应方国家 / 地区 (Responder Country)																IOC 编号 (IOC Number)															
	源自治系统 (Source Autonomous System)																															
	目标自治系统 (Destination Autonomous System)																															
	SNMP 输入 (SNMP In)																SNMP 输出 (SNMP Out)															
	源 TOS (Source TOS)								目标 TOS (Destination TOS)								源掩码 (Source Mask)								目标掩码 (Destination Mask)							
	安全情景 (Security Context) 安全情景 (Security Context) （续） 安全情景 (Security Context) （续） 安全情景 (Security Context) （续）																															

下表对用于 5.3.1 的连接统计信息数据块的字段进行了说明。

表 B-35 连接统计信息数据块 5.3.1 字段

字段	数据类型	说明
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 5.3.1+ 的连接统计信息数据块。值始终为 154。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID (Device ID)	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP Address)	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP Address)	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号 （如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符 （如适用）。
规则操作 (Rule Action)	uint16	在用户界面中选择的针对该规则的操作 （允许、阻止等）。
规则原因 (Rule Reason)	uint16	规则触发事件的原因。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。

表 B-35　　连接统计信息数据块 5.3.1 字段 （续）

字段	数据类型	说明
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址。
实例 ID (Instance ID)	uint16	生成事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的 UNIX 时间戳。
发起方传输的数据包数 (Initiator Transmitted Packets)	uint64	发起主机传输的数据包数。
响应方传输的数据包数 (Responder Transmitted Packets)	uint64	响应主机传输的数据包数。
发起方传输的字节数 (Initiator Transmitted Bytes)	uint64	发起主机传输的字节数。
响应方传输的字节数 (Responder Transmitted Bytes)	uint64	响应主机传输的字节数。
用户 ID (User ID)	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号 （如适用）。

表 B-35 连接统计信息数据块 5.3.1 字段 （续）

字段	数据类型	说明
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号 （如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的 URL （如适用）（例如， /files/index.html）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本 (Client Application Version)	字符串	客户端应用版本。
监控器规则 1 (Monitor Rule 1)	uint32	与连接事件关联的第一个监控器规则的 ID。
监控器规则 2 (Monitor Rule 2)	uint32	与连接事件关联的第二个监控器规则的 ID。
监控器规则 3 (Monitor Rule 3)	uint32	与连接事件关联的第三个监控器规则的 ID。
监控器规则 4 (Monitor Rule 4)	uint32	与连接事件关联的第四个监控器规则的 ID。
监控器规则 5 (Monitor Rule 5)	uint32	与连接事件关联的第五个监控器规则的 ID。
监控器规则 6 (Monitor Rule 6)	uint32	与连接事件关联的第六个监控器规则的 ID。

表 B-35　连接统计信息数据块 5.3.1 字段 （续）

字段	数据类型	说明
监控器规则 7 (Monitor Rule 7)	uint32	与连接事件关联的第七个监控器规则的 ID。
监控器规则 8 (Monitor Rule 8)	uint32	与连接事件关联的第八个监控器规则的 ID。
安全情报源 / 目标 (Security Intelligence Source/ Destination)	uint8	源或目标 IP 地址与 IP 阻止列表是否匹配。
安全情报层 (Security Intelligence Layer)	uint8	与 IP 阻止列表匹配的 IP 层。
文件事件计数 (File Event Count)	uint16	用于区别同一秒发生的文件事件的值。
入侵事件 (Intrusion Event)（续）	uint16	用于区别同一秒发生的入侵事件的值。
发起方国家 / 地区 (Initiator Country)	uint16	发起主机的国家 / 地区代码。
响应方国家 / 地区 (Responder Country)	uint 16	响应主机的国家 / 地区代码。
IOC 编号 (IOC Number)	uint16	与此事件相关的危害的 ID 号码。
源自治系统 (Source Autonomous System)	uint32	作为源或对等体的源自治系统的编号。
目标自治系统 (Destination Autonomous System)	uint32	作为源或对等体的目标自治系统的编号。
SNMP 输入 (SNMP Input)	uint16	输入接口的 SNMP 索引。
SNMP 输出 (SNMP Output)	uint16	输出接口的 SNMP 索引。
源 TOS (Source TOS)	uint8	传入接口的服务字节设置类型。
目标 TOS (Destination TOS)	uint8	传出接口的服务字节设置类型。

表 B-35　　连接统计信息数据块 5.3.1 字段 （续）

字段	数据类型	说明
源掩码 (Source Mask)	uint8	源地址前缀掩码。
目标掩码 (Destination Mask)	uint8	目标地址前缀掩码。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景 （虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。

连接统计信息数据块 5.4

连接统计信息数据块在连接数据消息中使用。用于 5.4 的连接统计信息数据块中添加了多个新字段，添加新字段是为了支持 SSL 连接、 HTTP 重定向以及网络分析策略。用于版本 5.4 的连接统计信息数据块的块类型为系列 1 数据块组中的 155。它否决了块类型 154，连接统计信息数据块 5.3.1，第 B-171 页。

您可以通过在事件版本为 12 且事件代码为 71 的请求消息中设置扩展事件标志 （请求标志字段中的位 30）请求扩展事件记录。请参阅请求标志，第 2-11 页。如果您启用位 23，则记录中会包含扩展事件报头。

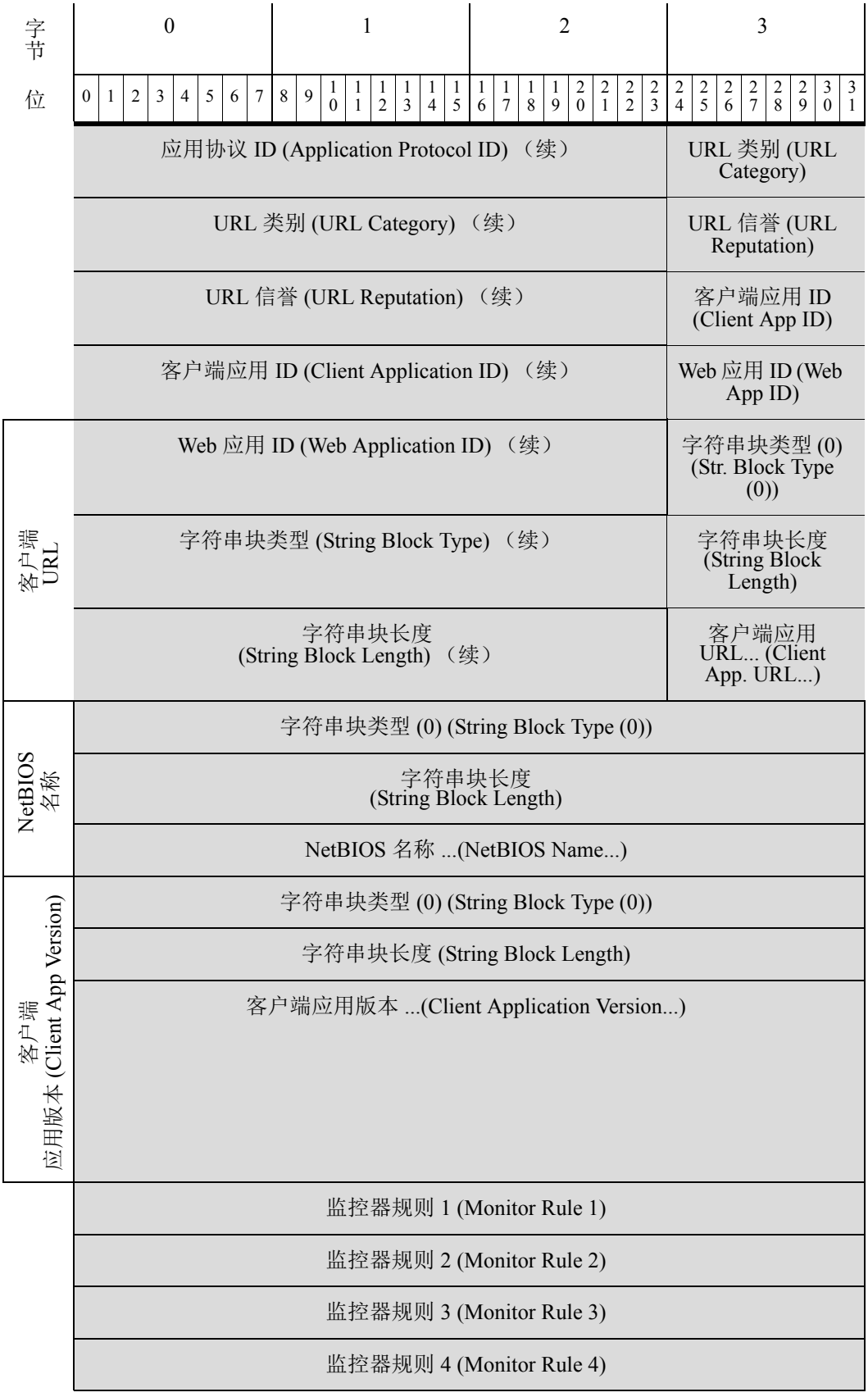
有关连接统计信息数据消息的详细信息，请参阅连接统计信息数据消息，第 4-54 页。

下图显示用于 5.4 的连接统计信息数据块的格式：

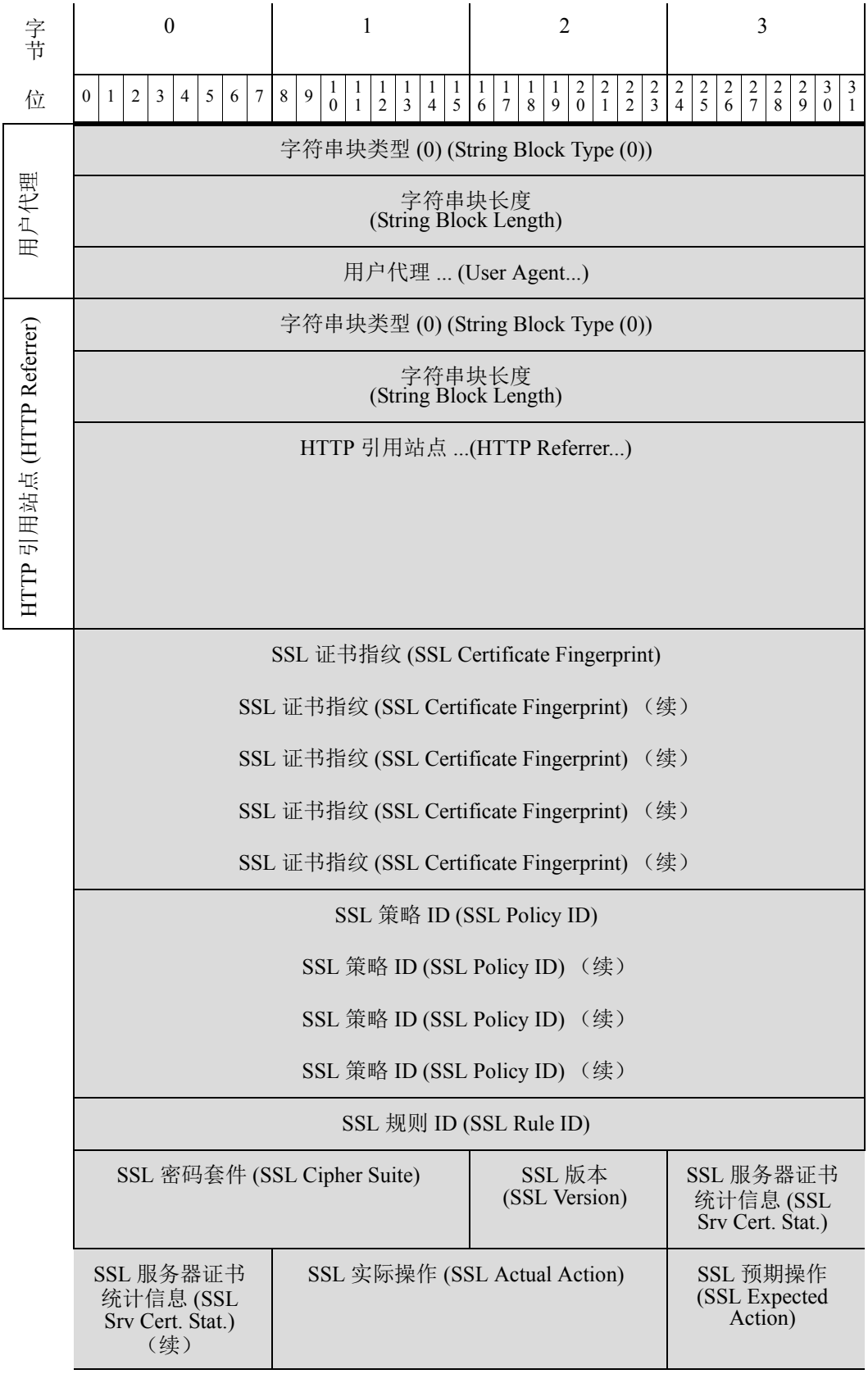
字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
连接数据块类型 (155) (Connection Data Block Type (155))																																
连接数据块长度 (Connection Data Block Length)																																
设备 ID (Device ID)																																
入口区 (Ingress Zone) 入口区 (Ingress Zone) （续） 入口区 (Ingress Zone) （续） 入口区 (Ingress Zone) （续）																																
出口区 (Egress Zone) 出口区 (Egress Zone) （续） 出口区 (Egress Zone) （续）																																

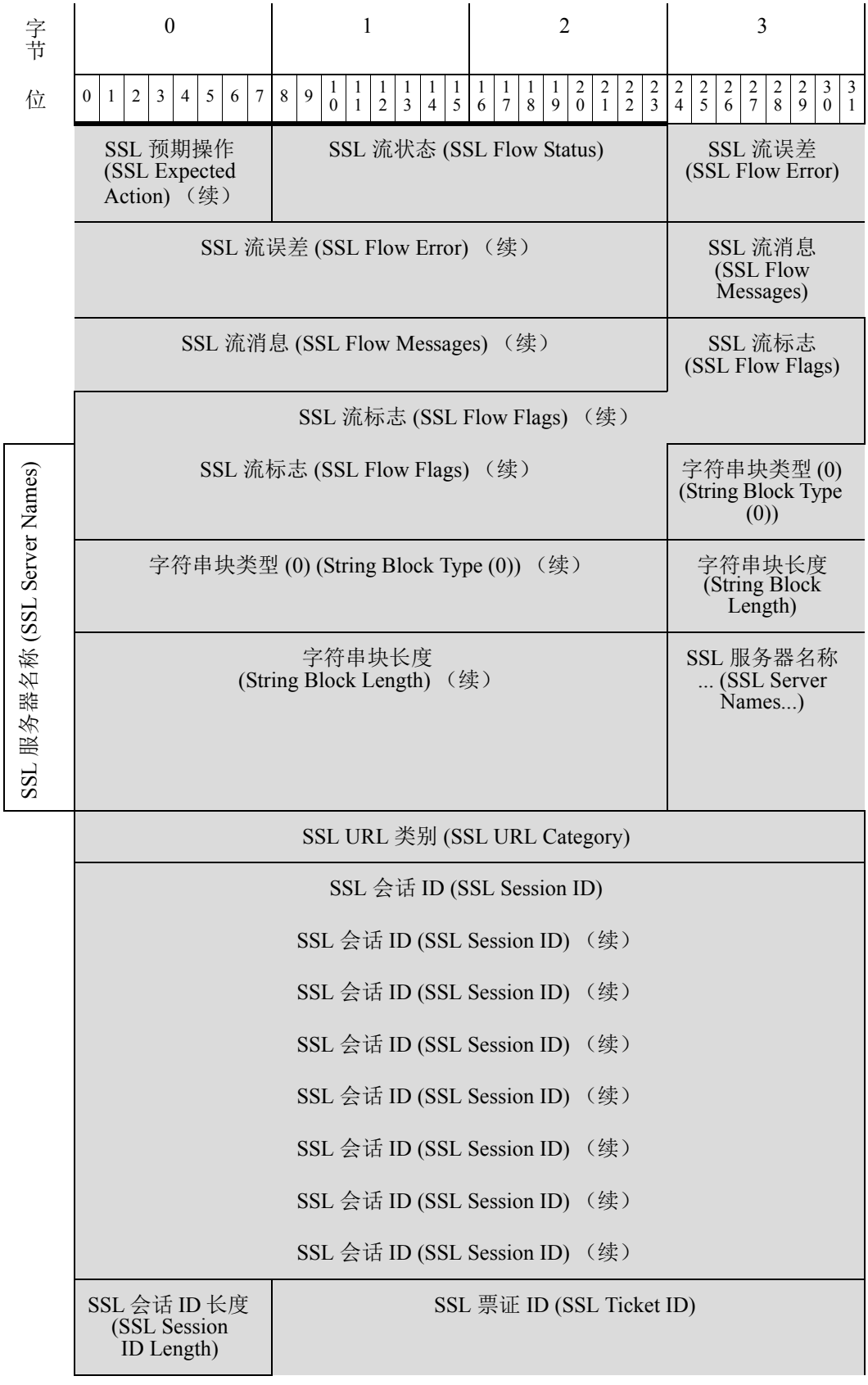
字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
出口区 (Egress Zone) （续）																																
入口接口 (Ingress Interface)																																
入口接口 (Ingress Interface) （续）																																
入口接口 (Ingress Interface) （续）																																
入口接口 (Ingress Interface) （续）																																
出口接口 (Egress Interface)																																
出口接口 (Egress Interface) （续）																																
出口接口 (Egress Interface) （续）																																
出口接口 (Egress Interface) （续）																																
发起方 IP 地址 (Initiator IP Address)																																
发起方 IP 地址 (Initiator IP Address) （续）																																
发起方 IP 地址 (Initiator IP Address) （续）																																
发起方 IP 地址 (Initiator IP Address) （续）																																
响应方 IP 地址 (Responder IP Address)																																
响应方 IP 地址 (Responder IP Address) （续）																																
响应方 IP 地址 (Responder IP Address) （续）																																
响应方 IP 地址 (Responder IP Address) （续）																																
策略修订 (Policy Revision)																																
策略修订 (Policy Revision) （续）																																
策略修订 (Policy Revision) （续）																																
策略修订 (Policy Revision) （续）																																
规则 ID (Rule ID)																																
规则操作 (Rule Action)																	规则原因 (Rule Reason)															
发起方端口 (Initiator Port)																	响应方端口 (Responder Port)															

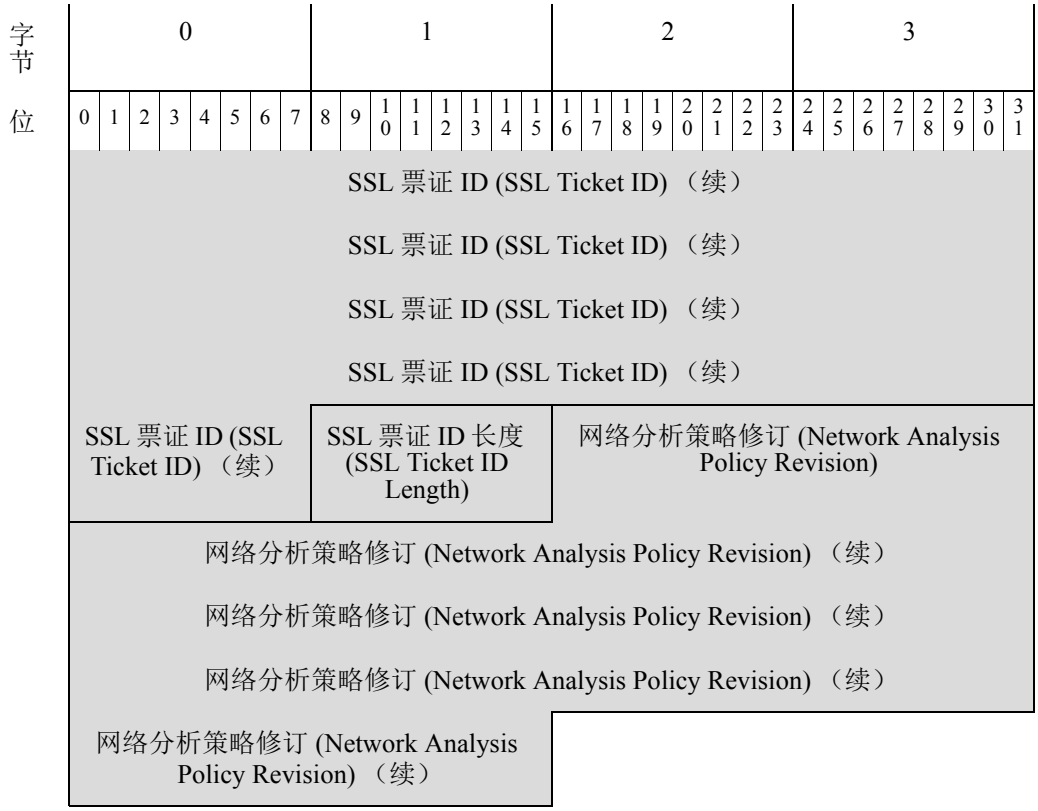

字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
TCP 标志 (TCP Flags)
协议 (Protocol)
NetFlow 源 (NetFlow Source)
Netflow 源 (Netflow Source) （续）
Netflow 源 (Netflow Source) （续）
Netflow 源 (Netflow Source) （续）
Netflow 源 (Netflow Source) （续）
实例 ID (Instance ID)
实例 ID (Instance ID) （续）
连接计数器 (Connection Counter)
第一个数据包时间 (First Pkt Time)
第一个数据包时间戳 (First Packet Timestamp) （续）
最后一个数据包时间 (Last Pkt Time)
最后一个数据包时间戳 (Last Packet Timestamp) （续）
发起方传输的数据包数 (Initiator Transmitted Packets)
发起方传输的数据包数 (Initiator Transmitted Packets) （续）
发起方传输的数据包数 (Initiator Transmitted Packets) （续）
响应方传输的数据包数 (Resp. Tx Packets)
响应方传输的数据包数 (Responder Transmitted Packets) （续）
响应方传输的数据包数 (Responder Transmitted Packets) （续）
发起方传输的字节数 (Initiator Tx Bytes)
发起方传输的字节数 (Initiator Transmitted Bytes) （续）
发起方传输的字节数 (Initiator Transmitted Bytes) （续）
响应方传输的字节数 (Resp. Tx Bytes)
响应方传输的字节数 (Responder Transmitted Bytes) （续）
响应方传输的字节数 (Responder Transmitted Bytes) （续）
用户 ID (User ID)
用户 ID (User ID) （续）
应用协议 ID (Application Protocol ID)


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
应用协议 ID (Application Protocol ID) （续）
URL 类别 (URL Category)
URL 类别 (URL Category) （续）
URL 信誉 (URL Reputation)
URL 信誉 (URL Reputation) （续）
客户端应用 ID (Client App ID)
客户端应用 ID (Client Application ID) （续）
Web 应用 ID (Web App ID)
客户端 URL
Web 应用 ID (Web Application ID) （续）
字符串块类型 (0) (Str. Block Type (0))
字符串块类型 (String Block Type) （续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length) （续）
客户端应用 URL... (Client App. URL...)
NetBIOS 名称
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
NetBIOS 名称 ...(NetBIOS Name...)
客户端应用版本 (Client App Version)
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
客户端应用版本 ...(Client Application Version...)
监控器规则 1 (Monitor Rule 1)
监控器规则 2 (Monitor Rule 2)
监控器规则 3 (Monitor Rule 3)
监控器规则 4 (Monitor Rule 4)

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	监控器规则 5 (Monitor Rule 5)																															
	监控器规则 6 (Monitor Rule 6)																															
	监控器规则 7 (Monitor Rule 7)																															
	监控器规则 8 (Monitor Rule 8)																															
	安全接口源 / 目标 (Sec. Int. Src/Dst)								安全接口层 (Sec. Int. Layer)								文件事件计数 (File Event Count)															
	入侵事件计数 (Intrusion Event Count)																发起方国家 / 地区 (Initiator Country)															
	响应方国家 / 地区 (Responder Country)																IOC 编号 (IOC Number)															
	源自治系统 (Source Autonomous System)																															
	目标自治系统 (Destination Autonomous System)																															
	SNMP 输入 (SNMP In)																SNMP 输出 (SNMP Out)															
	源 TOS (Source TOS)								目标 TOS (Destination TOS)								源掩码 (Source Mask)								目标掩码 (Destination Mask)							
	安全情景 (Security Context) 安全情景 (Security Context) （续） 安全情景 (Security Context) （续） 安全情景 (Security Context) （续）																															
引用的主机 (Referenced Host)	VLAN ID																字符串块类型 (0) (String Block Type (0))															
	字符串块类型 (0) (String Block Type (0)) （续）																字符串块长度 (String Block Length)															
	字符串块长度 (String Block Length) （续）																引用的主机 (Referenced Host).. .(Referenced Host...)															


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
用户代理
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
用户代理 ... (User Agent...)
HTTP 引用站点 (HTTP Referrer)
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
HTTP 引用站点 ...(HTTP Referrer...)
SSL 证书指纹 (SSL Certificate Fingerprint)
SSL 证书指纹 (SSL Certificate Fingerprint) （续）
SSL 证书指纹 (SSL Certificate Fingerprint) （续）
SSL 证书指纹 (SSL Certificate Fingerprint) （续）
SSL 证书指纹 (SSL Certificate Fingerprint) （续）
SSL 策略 ID (SSL Policy ID)
SSL 策略 ID (SSL Policy ID) （续）
SSL 策略 ID (SSL Policy ID) （续）
SSL 策略 ID (SSL Policy ID) （续）
SSL 规则 ID (SSL Rule ID)
SSL 密码套件 (SSL Cipher Suite)
SSL 版本 (SSL Version)
SSL 服务器证书统计信息 (SSL Srv Cert. Stat.)
SSL 服务器证书统计信息 (SSL Srv Cert. Stat.) （续）
SSL 实际操作 (SSL Actual Action)
SSL 预期操作 (SSL Expected Action)


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 预期操作 (SSL Expected Action) （续）
SSL 流状态 (SSL Flow Status)
SSL 流误差 (SSL Flow Error)
SSL 流误差 (SSL Flow Error) （续）
SSL 流消息 (SSL Flow Messages)
SSL 流消息 (SSL Flow Messages) （续）
SSL 流标志 (SSL Flow Flags)
SSL 流标志 (SSL Flow Flags) （续）
SSL 流标志 (SSL Flow Flags) （续）
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0)) （续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length) （续）
SSL 服务器名称 ... (SSL Server Names...)
SSL 服务器名称 (SSL Server Names)
SSL URL 类别 (SSL URL Category)
SSL 会话 ID (SSL Session ID)
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID 长度 (SSL Session ID Length)
SSL 票证 ID (SSL Ticket ID)



下表对用于 5.4+ 的连接统计信息数据块的字段进行了说明。

表 B-36　　连接统计信息数据块 5.4+ 字段

字段	数据类型	说明
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 5.4+ 的连接统计信息数据块。值始终为 155。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID (Device ID)	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。

表 B-36 连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP Address)	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP Address)	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号 （如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符 （如适用）。
规则操作 (Rule Action)	uint16	在用户界面中选择的针对该规则的操作 （允许、阻止等）。
规则原因 (Rule Reason)	uint16	规则触发事件的原因。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址。
实例 ID (Instance ID)	uint16	生成事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的 UNIX 时间戳。
发起方传输的数据包数 (Initiator Transmitted Packets)	uint64	发起主机传输的数据包数。

表 B-36　连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明
响应方传输的数据包数 (Responder Transmitted Packets)	uint64	响应主机传输的数据包数。
发起方传输的字节数 (Initiator Transmitted Bytes)	uint64	发起主机传输的字节数。
响应方传输的字节数 (Responder Transmitted Bytes)	uint64	响应主机传输的字节数。
用户 ID (User ID)	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号 （如适用）。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号 （如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的 URL （如适用）（例如，`/files/index.html`）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。

表 B-36 连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本 (Client Application Version)	字符串	客户端应用版本。
监控器规则 1 (Monitor Rule 1)	uint32	与连接事件关联的第一个监控器规则的 ID。
监控器规则 2 (Monitor Rule 2)	uint32	与连接事件关联的第二个监控器规则的 ID。
监控器规则 3 (Monitor Rule 3)	uint32	与连接事件关联的第三个监控器规则的 ID。
监控器规则 4 (Monitor Rule 4)	uint32	与连接事件关联的第四个监控器规则的 ID。
监控器规则 5 (Monitor Rule 5)	uint32	与连接事件关联的第五个监控器规则的 ID。
监控器规则 6 (Monitor Rule 6)	uint32	与连接事件关联的第六个监控器规则的 ID。
监控器规则 7 (Monitor Rule 7)	uint32	与连接事件关联的第七个监控器规则的 ID。
监控器规则 8 (Monitor Rule 8)	uint32	与连接事件关联的第八个监控器规则的 ID。
安全情报源 / 目标 (Security Intelligence Source/ Destination)	uint8	源或目标 IP 地址与 IP 阻止列表是否匹配。
安全情报层 (Security Intelligence Layer)	uint8	与 IP 阻止列表匹配的 IP 层。
文件事件计数 (File Event Count)	uint16	用于区别同一秒发生的文件事件的值。
入侵事件 (Intrusion Event) （续）	uint16	用于区别同一秒发生的入侵事件的值。
发起方国家 / 地区 (Initiator Country)	uint16	发起主机的国家 / 地区代码。

表 B-36　　连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明
响应方国家 / 地区 (Responder Country)	uint 16	响应主机的国家 / 地区代码。
IOC 编号 (IOC Number)	uint16	与此事件相关的危害的 ID 号码。
源自治系统 (Source Autonomous System)	uint32	作为源或对等体的源自治系统的编号。
目标自治系统 (Destination Autonomous System)	uint32	作为源或对等体的目标自治系统的编号。
SNMP 输入 (SNMP Input)	uint16	输入接口的 SNMP 索引。
SNMP 输出 (SNMP Output)	uint16	输出接口的 SNMP 索引。
源 TOS (Source TOS)	uint8	传入接口的服务字节设置类型。
目标 TOS (Destination TOS)	uint8	传出接口的服务字节设置类型。
源掩码 (Source Mask)	uint8	源地址前缀掩码。
目标掩码 (Destination Mask)	uint8	目标地址前缀掩码。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景 （虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
字符串块类型 (String Block Type)	uint32	启动包含引用的主机的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	引用的主机字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 引用的主机 ”(Referenced Host) 字段中的字节数。
引用的主机 (Referenced Host)	字符串	HTTP 或 DNS 中提供的主机名信息。
字符串块类型 (String Block Type)	uint32	启动包含用户代理的字符串数据块。值始终为 0。

表 B-36 连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Length)	uint32	用户代理字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 用户代理 ”(User Agent) 字段中的字节数。
用户代理 (User Agent)	字符串	会话中用户代理报头字段中的信息。
字符串块类型 (String Block Type)	uint32	启动包含 HTTP 引用站点的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	HTTP 引用站点字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “HTTP 引用站点 ”(HTTP Referrer) 字段中的字节数。
HTTP 引用站点 (HTTP Referrer)	字符串	页面起源的站点。该站点可在 HTTP 流量中引用的报头信息中找到。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 策略 ID (SSL Policy ID)	uint8[16]	处理连接的 SSL 策略的 ID 编号。
SSL 规则 ID (SSL Rule ID)	uint32	处理连接的 SSL 规则或默认操作的 ID 编号。
SSL 密码套件 (SSL Cipher Suite)	uint16	SSL 连接使用的加密套件。该值以十进制格式存储。有关该值指定的密码套件，请参阅 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml。
SSL 版本 (SSL Version)	uint8	用来加密连接的 SSL 或 TLS 协议版本。
SSL 服务器证书状态 (SSL Server Certificate Status)	uint16	SSL 证书的状态。可能的值包括： • 0 - 未检查 - 服务器证书状态未评估。 • 1 - 未知 - 服务器证书状态无法确定。 • 2 - 有效 - 服务器证书有效。 • 4 - 自签 - 服务器证书已自签。 • 16 - 颁发者无效 - 服务器证书的颁发者无效。 • 32 - 签名无效 - 服务器证书的签名无效。 • 64 - 过期 - 服务器证书已过期。 • 128 - 尚未生效 - 服务器证书尚未生效。 • 256 - 撤销 - 服务器证书已被撤销。

表 B-36　连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括： • 0 -‘ 未知 ’ • 1 -‘ 请勿解密 ’ • 2 -‘ 阻止 ’ • 3 -‘ 阻止并重置 ’ • 4 -‘ 解密 （已知密钥） ’ • 5 -‘ 解密 （更换秘钥） ’ • 6 -‘ 解密 （放弃） ’
SSL 预期操作 (SSL Expected Action)	uint16	根据 SSL 规则应该对连接执行的操作。可能的值包括： • 0 -‘ 未知 ’ • 1 -‘ 请勿解密 ’ • 2 -‘ 阻止 ’ • 3 -‘ 阻止并重置 ’ • 4 -‘ 解密 （已知密钥） ’ • 5 -‘ 解密 （更换秘钥） ’ • 6 -‘ 解密 （放弃） ’

表 B-36 连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明
SSL 流状态 (SSL Flow Status)	uint16	SSL 流量的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括： • 0 -‘ 未知 ’ • 1 -‘ 不匹配 ’ • 2 -‘ 成功 ’ • 3 -‘ 非缓存会话 ’ • 4 -‘ 未知密码套件 ’ • 5 -‘ 不受支持的密码套件 ’ • 6 -‘ 不受支持的 SSL 版本 ’ • 7 -‘ 使用的 SSL 压缩 ’ • 8 -‘ 在被动模式中无法解密的会话 ’ • 9 -‘ 握手错误 ’ • 10 -‘ 解密错误 ’ • 11 -‘ 待处理服务器名称分类查找 ’ • 12 -‘ 待处理通用名称分类查找 ’ • 13 -‘ 内部错误 ’ • 14 -‘ 网络参数不可用 ’ • 15 -‘ 服务器证书处理无效 ’ • 16 -‘ 服务器证书指纹不可用 ’ • 17 -‘ 无法缓存持有者 DN’ • 18 -‘ 无法缓存颁发者 DN’ • 19 -‘ 未知 SSL 版本 ’ • 20 -‘ 外部证书列表不可用 ’ • 21 -‘ 外部证书指纹不可用 ’ • 22 -‘ 内部证书列表无效 ’ • 23 -‘ 内部证书列表不可用 ’ • 24 -‘ 内部证书不可用 ’ • 25 -‘ 内部证书指纹不可用 ’ • 26 -‘ 服务器证书验证不可用 ’ • 27 -‘ 服务器证书验证失败 ’ • 28 -‘ 操作无效 ’
SSL 流误差 (SSL Flow Error)	uint32	详细的 SSL 错误代码。这些值可用于提供支持。

表 B-36　连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明
SSL 流消息 (SSL Flow Messages)	uint32	在 SSL 握手期间，客户端和服务器之间交换的消息。有关详细信息，请参阅 http://tools.ietf.org/html/rfc5246。 • 0x00000001 - NSE_MT__HELLO_REQUEST • 0x00000002 - NSE_MT__CLIENT_ALERT • 0x00000004 - NSE_MT__SERVER_ALERT • 0x00000008 - NSE_MT__CLIENT_HELLO • 0x00000010 - NSE_MT__SERVER_HELLO • 0x00000020 - NSE_MT__SERVER_CERTIFICATE • 0x00000040 - NSE_MT__SERVER_KEY_EXCHANGE • 0x00000080 - NSE_MT__CERTIFICATE_REQUEST • 0x00000100 - NSE_MT__SERVER_HELLO_DONE • 0x00000200 - NSE_MT__CLIENT_CERTIFICATE • 0x00000400 - NSE_MT__CLIENT_KEY_EXCHANGE • 0x00000800 - NSE_MT__CERTIFICATE_VERIFY • 0x00001000 - NSE_MT__CLIENT_CHANGE_CIPHER_SPEC • 0x00002000 - NSE_MT__CLIENT_FINISHED • 0x00004000 - NSE_MT__SERVER_CHANGE_CIPHER_SPEC • 0x00008000 - NSE_MT__SERVER_FINISHED • 0x00010000 - NSE_MT__NEW_SESSION_TICKET • 0x00020000 - NSE_MT__HANDSHAKE_OTHER • 0x00040000 - NSE_MT__APP_DATA_FROM_CLIENT • 0x00080000 - NSE_MT__APP_DATA_FROM_SERVER
SSL 流标志 (SSL Flow Flags)	uint64	加密连接的调试级别标志。可能的值包括： • 0x00000001 - NSE_FLOW__VALID - 必须设置此字段，其他字段才有效 • 0x00000002 - NSE_FLOW__INITIALIZED - 内部结构已准备就绪进行处理 • 0x00000004 - NSE_FLOW__INTERCEPT - SSL 会话已被拦截
字符串块类型 (String Block Type)	uint32	启动包含 SSL 服务器名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	SSL 服务器名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “SSL 服务器名称 ”(SSL Server Name) 字段中的字节数。

表 B-36 连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明
SSL 服务器名称 (SSL Server Name)	字符串	在 SSL 客户端欢迎界面中服务器名称显示中提供的名称。
SSL URL 类别 (SSL URL Category)	uint32	根据服务器名称和证书常用名识别的流量类别。
SSL 会话 ID (SSL Session ID)	uint8[32]	当客户端和服务器同意进行会话重用时， SSL 握手期间使用的会话 ID 值
SSL 会话 ID 长度 (SSL Session ID Length)	uint8	SSL 会话 ID 的长度。尽管会话 ID 不能超过 32 个字节，此值可能小于 32 个字节。
SSL 票证 ID (SSL Ticket ID)	uint8[20]	当客户端和服务器同意使用会话票证时使用的会话票证散列。
SSL 票证 ID 长度 (SSL Ticket ID Length)	uint8	SSL 票证 ID 的长度。尽管票证 ID 不能超过 20 个字节，此值可能小于 20 个字节。
网络分析策略修订 (Network Analysis Policy revision)	uint8[16]	与连接事件相关的网络分析策略的修订。

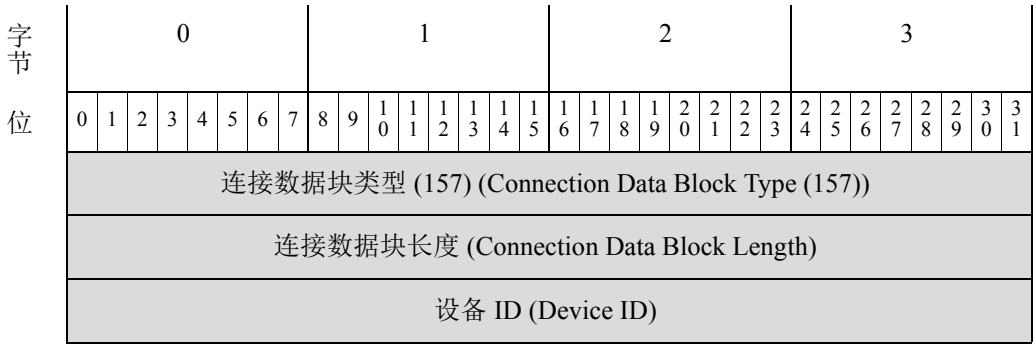
连接统计信息数据块 5.4.1

连接统计信息数据块在连接数据消息中使用。用于 5.4 的连接统计信息数据块中添加了多个新字段，添加新字段是为了支持 SSL 连接、HTTP 重定向以及网络分析策略。用于版本 5.4+ 的连接统计信息数据块的块类型为系列 1 数据块组中的 157。它否决了块类型 155，连接统计信息数据块 5.3.1，第 B-171 页。

您可以通过在事件版本为 12 且事件代码为 71 的请求消息中设置扩展事件标志 （请求标志字段中的位 30）请求扩展事件记录。请参阅请求标志，第 2-11 页。如果您启用位 23，则记录中会包含扩展事件报头。

有关连接统计信息数据消息的详细信息，请参阅连接统计信息数据消息，第 4-54 页。

下图显示用于 5.4+ 的连接统计信息数据块的格式：



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
入口区 (Ingress Zone)																																
入口区 (Ingress Zone) （续）																																
入口区 (Ingress Zone) （续）																																
入口区 (Ingress Zone) （续）																																
出口区 (Egress Zone)																																
出口区 (Egress Zone) （续）																																
出口区 (Egress Zone) （续）																																
出口区 (Egress Zone) （续）																																
入口接口 (Ingress Interface)																																
入口接口 (Ingress Interface) （续）																																
入口接口 (Ingress Interface) （续）																																
入口接口 (Ingress Interface) （续）																																
出口接口 (Egress Interface)																																
出口接口 (Egress Interface) （续）																																
出口接口 (Egress Interface) （续）																																
出口接口 (Egress Interface) （续）																																
发起方 IP 地址 (Initiator IP Address)																																
发起方 IP 地址 (Initiator IP Address) （续）																																
发起方 IP 地址 (Initiator IP Address) （续）																																
发起方 IP 地址 (Initiator IP Address) （续）																																
响应方 IP 地址 (Responder IP Address)																																
响应方 IP 地址 (Responder IP Address) （续）																																
响应方 IP 地址 (Responder IP Address) （续）																																
响应方 IP 地址 (Responder IP Address) （续）																																

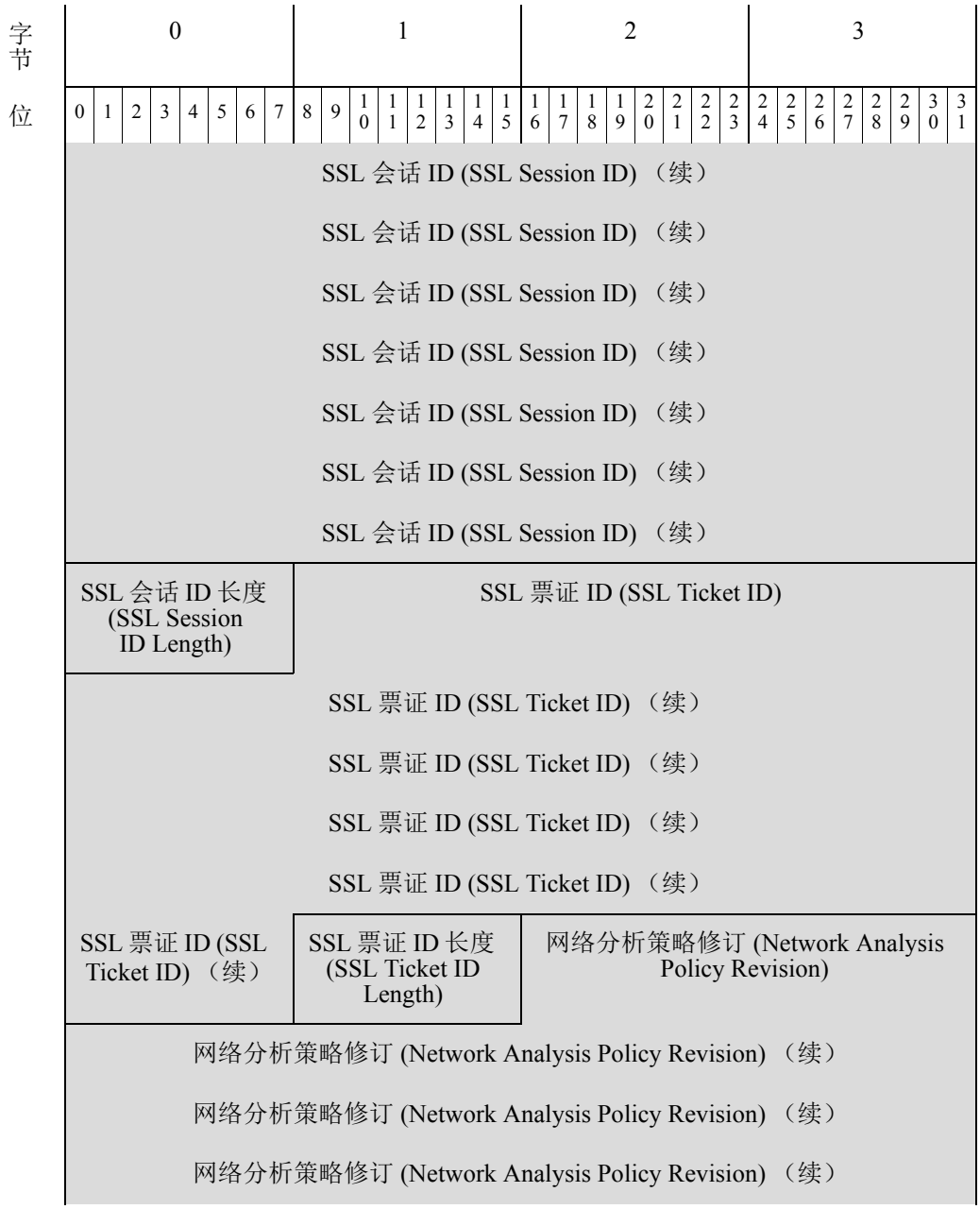

字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
策略修订 (Policy Revision)
策略修订 (Policy Revision) （续）
策略修订 (Policy Revision) （续）
策略修订 (Policy Revision) （续）
规则 ID (Rule ID)
规则操作 (Rule Action)
规则原因 (Rule Reason)
发起方端口 (Initiator Port)
响应方端口 (Responder Port)
TCP 标志 (TCP Flags)
协议 (Protocol)
NetFlow 源 (NetFlow Source)
Netflow 源 (Netflow Source) （续）
Netflow 源 (Netflow Source) （续）
Netflow 源 (Netflow Source) （续）
Netflow 源 (Netflow Source) （续）
实例 ID (Instance ID)
实例 ID (Instance ID) （续）
连接计数器 (Connection Counter)
第一个数据包时间 (First Pkt Time)
第一个数据包时间戳 (First Packet Timestamp) （续）
最后一个数据包时间 (Last Pkt Time)
最后一个数据包时间戳 (Last Packet Timestamp) （续）
发起方传输的数据包数 (Initiator Transmitted Packets)
发起方传输的数据包数 (Initiator Transmitted Packets) （续）
发起方传输的数据包数 (Initiator Transmitted Packets) （续）
响应方传输的数据包数 (Resp. Tx Packets)
响应方传输的数据包数 (Responder Transmitted Packets) （续）
响应方传输的数据包数 (Responder Transmitted Packets) （续）
发起方传输的字节数 (Initiator Tx Bytes)

	字节	0								1								2								3							
	位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
		发起方传输的字节数 (Initiator Transmitted Bytes) （续）																															
		发起方传输的字节数 (Initiator Transmitted Bytes) （续）																								响应方传输的字节数 (Resp. Tx Bytes)							
		响应方传输的字节数 (Responder Transmitted Bytes) （续）																															
		响应方传输的字节数 (Responder Transmitted Bytes) （续）																								用户 ID (User ID)							
		用户 ID (User ID) （续）																								应用协议 ID (Application Protocol ID)							
		应用协议 ID (Application Protocol ID) （续）																								URL 类别 (URL Category)							
		URL 类别 (URL Category) （续）																								URL 信誉 (URL Reputation)							
		URL 信誉 (URL Reputation) （续）																								客户端应用 ID (Client App ID)							
		客户端应用 ID (Client Application ID) （续）																								Web 应用 ID (Web App ID)							
客户端 URL		Web 应用 ID (Web Application ID) （续）																								字符串块类型 (0) (Str. Block Type (0))							
客户端 URL		字符串块类型 (String Block Type) （续）																								字符串块长度 (String Block Length)							
客户端 URL		字符串块长度 (String Block Length) （续）																								客户端应用 URL... (Client App. URL...)							
NetBIOS 名称		字符串块类型 (0) (String Block Type (0))																															
NetBIOS 名称		字符串块长度 (String Block Length)																															
NetBIOS 名称		NetBIOS 名称 ...(NetBIOS Name...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
客户端应用版本 (Client App Version)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	客户端应用版本 ...(Client Application Version...)																															
	监控器规则 1 (Monitor Rule 1)																															
	监控器规则 2 (Monitor Rule 2)																															
	监控器规则 3 (Monitor Rule 3)																															
	监控器规则 4 (Monitor Rule 4)																															
	监控器规则 5 (Monitor Rule 5)																															
	监控器规则 6 (Monitor Rule 6)																															
	监控器规则 7 (Monitor Rule 7)																															
	监控器规则 8 (Monitor Rule 8)																															
	安全接口源 / 目标 (Sec. Int. Src/Dst)								安全接口层 (Sec. Int. Layer)								文件事件计数 (File Event Count)															
	入侵事件计数 (Intrusion Event Count)																发起方国家 / 地区 (Initiator Country)															
	响应方国家 / 地区 (Responder Country)																IOC 编号 (IOC Number)															
	源自治系统 (Source Autonomous System)																															
	目标自治系统 (Destination Autonomous System)																															
	SNMP 输入 (SNMP In)																SNMP 输出 (SNMP Out)															
	源 TOS (Source TOS)								目标 TOS (Destination TOS)								源掩码 (Source Mask)								目标掩码 (Destination Mask)							
	安全情景 (Security Context) 安全情景 (Security Context) （续）																															


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
安全情景 (Security Context) （续）
安全情景 (Security Context) （续）
引用的主机 (Referenced Host)
VLAN ID
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0)) （续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length) （续）
引用的主机 (Referenced Host)... (Referenced Host...)
用户代理
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
用户代理 ... (User Agent...)
HTTP 引用站点 (HTTP Referrer)
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
HTTP 引用站点 ...(HTTP Referrer...)
SSL 证书指纹 (SSL Certificate Fingerprint)
SSL 证书指纹 (SSL Certificate Fingerprint) （续）
SSL 证书指纹 (SSL Certificate Fingerprint) （续）
SSL 证书指纹 (SSL Certificate Fingerprint) （续）
SSL 证书指纹 (SSL Certificate Fingerprint) （续）
SSL 策略 ID (SSL Policy ID)


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 策略 ID (SSL Policy ID) （续）
SSL 策略 ID (SSL Policy ID) （续）
SSL 策略 ID (SSL Policy ID) （续）
SSL 规则 ID (SSL Rule ID)
SSL 密码套件 (SSL Cipher Suite)
SSL 版本 (SSL Version)
SSL 服务器证书统计信息 (SSL Srv Cert. Stat.)
SSL 服务器证书统计信息 (SSL Srv Cert. Stat.) （续）
SSL 实际操作 (SSL Actual Action)
SSL 实际操作 （续）
SSL 预期操作 (SSL Expected Action)
SSL 流状态 (SSL Flow Status)
SSL 流状态 （续）
SSL 流误差 (SSL Flow Error)
SSL 流误差 (SSL Flow Error) （续）
SSL 流量消息 (SSL Flow Messages)
SSL 流消息 (SSL Flow Msg.) （续）
SSL 流标志 (SSL Flow Flags)
SSL 流标志 (SSL Flow Flags) （续）
SSL 流标志 (SSL Flow Flags) （续）
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0)) （续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length) （续）
SSL 服务器名称 ... (SSL Server Names...)
SSL 服务器名称 (SSL Server Names)
SSL URL 类别 (SSL URL Category)
SSL 会话 ID (SSL Session ID)


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID 长度 (SSL Session ID Length)
SSL 票证 ID (SSL Ticket ID)
SSL 票证 ID (SSL Ticket ID) （续）
SSL 票证 ID (SSL Ticket ID) （续）
SSL 票证 ID (SSL Ticket ID) （续）
SSL 票证 ID (SSL Ticket ID) （续）
SSL 票证 ID (SSL Ticket ID) （续）
SSL 票证 ID 长度 (SSL Ticket ID Length)
网络分析策略修订 (Network Analysis Policy Revision)
网络分析策略修订 (Network Analysis Policy Revision) （续）
网络分析策略修订 (Network Analysis Policy Revision) （续）
网络分析策略修订 (Network Analysis Policy Revision) （续）

下表对用于 5.4+ 的连接统计信息数据块的字段进行了说明。

表 B-37 连接统计信息数据块 5.4+ 字段

字段	数据类型	说明
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 5.4+ 的连接统计信息数据块。值始终为 157。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID (Device ID)	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP Address)	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP Address)	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号 （如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符 （如适用）。
规则操作 (Rule Action)	uint16	在用户界面中选择的针对该规则的操作 （允许、阻止等）。
规则原因 (Rule Reason)	uint16	规则触发事件的原因。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。

表 B-37　　连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址。
实例 ID (Instance ID)	uint16	生成事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的 UNIX 时间戳。
发起方传输的数据包数 (Initiator Transmitted Packets)	uint64	发起主机传输的数据包数。
响应方传输的数据包数 (Responder Transmitted Packets)	uint64	响应主机传输的数据包数。
发起方传输的字节数 (Initiator Transmitted Bytes)	uint64	发起主机传输的字节数。
响应方传输的字节数 (Responder Transmitted Bytes)	uint64	响应主机传输的字节数。
用户 ID (User ID)	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号 （如适用）。

表 B-37 连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号 （如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的 URL （如适用）（例如， /files/index.html）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本 (Client Application Version)	字符串	客户端应用版本。
监控器规则 1 (Monitor Rule 1)	uint32	与连接事件关联的第一个监控器规则的 ID。
监控器规则 2 (Monitor Rule 2)	uint32	与连接事件关联的第二个监控器规则的 ID。
监控器规则 3 (Monitor Rule 3)	uint32	与连接事件关联的第三个监控器规则的 ID。
监控器规则 4 (Monitor Rule 4)	uint32	与连接事件关联的第四个监控器规则的 ID。
监控器规则 5 (Monitor Rule 5)	uint32	与连接事件关联的第五个监控器规则的 ID。
监控器规则 6 (Monitor Rule 6)	uint32	与连接事件关联的第六个监控器规则的 ID。

表 B-37　连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明
监控器规则 7 (Monitor Rule 7)	uint32	与连接事件关联的第七个监控器规则的 ID。
监控器规则 8 (Monitor Rule 8)	uint32	与连接事件关联的第八个监控器规则的 ID。
安全情报源 / 目标 (Security Intelligence Source/ Destination)	uint8	源或目标 IP 地址与 IP 阻止列表是否匹配。
安全情报层 (Security Intelligence Layer)	uint8	与 IP 阻止列表匹配的 IP 层。
文件事件计数 (File Event Count)	uint16	用于区别同一秒发生的文件事件的值。
入侵事件 (Intrusion Event)（续）	uint16	用于区别同一秒发生的入侵事件的值。
发起方国家 / 地区 (Initiator Country)	uint16	发起主机的国家 / 地区代码。
响应方国家 / 地区 (Responder Country)	uint 16	响应主机的国家 / 地区代码。
IOC 编号 (IOC Number)	uint16	与此事件相关的危害的 ID 号码。
源自治系统 (Source Autonomous System)	uint32	作为源或对等体的源自治系统的编号。
目标自治系统 (Destination Autonomous System)	uint32	作为源或对等体的目标自治系统的编号。
SNMP 输入 (SNMP Input)	uint16	输入接口的 SNMP 索引。
SNMP 输出 (SNMP Output)	uint16	输出接口的 SNMP 索引。
源 TOS (Source TOS)	uint8	传入接口的服务字节设置类型。
目标 TOS (Destination TOS)	uint8	传出接口的服务字节设置类型。

表 B-37 连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明
源掩码 (Source Mask)	uint8	源地址前缀掩码。
目标掩码 (Destination Mask)	uint8	目标地址前缀掩码。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景 （虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
字符串块类型 (String Block Type)	uint32	启动包含引用的主机的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	引用的主机字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 引用的主机 ”(Referenced Host) 字段中的字节数。
引用的主机 (Referenced Host)	字符串	HTTP 或 DNS 中提供的主机名信息。
字符串块类型 (String Block Type)	uint32	启动包含用户代理的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户代理字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 用户代理 ”(User Agent) 字段中的字节数。
用户代理 (User Agent)	字符串	会话中用户代理报头字段中的信息。
字符串块类型 (String Block Type)	uint32	启动包含 HTTP 引用站点的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	HTTP 引用站点字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “HTTP 引用站点 ”(HTTP Referrer) 字段中的字节数。
HTTP 引用站点 (HTTP Referrer)	字符串	页面起源的站点。该站点可在 HTTP 流量中引用的报头信息中找到。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 策略 ID (SSL Policy ID)	uint8[16]	处理连接的 SSL 策略的 ID 编号。
SSL 规则 ID (SSL Rule ID)	uint32	处理连接的 SSL 规则或默认操作的 ID 编号。

表 B-37　连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明
SSL 密码套件 (SSL Cipher Suite)	uint16	SSL 连接使用的加密套件。该值以十进制格式存储。有关该值指定的密码套件，请参阅 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml。
SSL 版本 (SSL Version)	uint8	用来加密连接的 SSL 或 TLS 协议版本。
SSL 服务器证书状态 (SSL Server Certificate Status)	uint32	SSL 证书的状态。可能的值包括： • 0 - 未检查 - 服务器证书状态未评估。 • 1 - 未知 - 服务器证书状态无法确定。 • 2 - 有效 - 服务器证书有效。 • 4 - 自签 - 服务器证书已自签。 • 16 - 颁发者无效 - 服务器证书的颁发者无效。 • 32 - 签名无效 - 服务器证书的签名无效。 • 64 - 过期 - 服务器证书已过期。 • 128 - 尚未生效 - 服务器证书尚未生效。 • 256 - 撤销 - 服务器证书已被撤销。
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括： • 0 -‘ 未知 ’ • 1 -‘ 请勿解密 ’ • 2 -‘ 阻止 ’ • 3 -‘ 阻止并重置 ’ • 4 -‘ 解密 （已知密钥） ’ • 5 -‘ 解密 （更换秘钥） ’ • 6 -‘ 解密 （放弃） ’
SSL 预期操作 (SSL Expected Action)	uint16	根据 SSL 规则应该对连接执行的操作。可能的值包括： • 0 -‘ 未知 ’ • 1 -‘ 请勿解密 ’ • 2 -‘ 阻止 ’ • 3 -‘ 阻止并重置 ’ • 4 -‘ 解密 （已知密钥） ’ • 5 -‘ 解密 （更换秘钥） ’ • 6 -‘ 解密 （放弃） ’

表 B-37 连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明
SSL 流状态 (SSL Flow Status)	uint16	SSL 流量的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括： • 0 -‘ 未知 ’ • 1 -‘ 不匹配 ’ • 2 -‘ 成功 ’ • 3 -‘ 非缓存会话 ’ • 4 -‘ 未知密码套件 ’ • 5 -‘ 不受支持的密码套件 ’ • 6 -‘ 不受支持的 SSL 版本 ’ • 7 -‘ 使用的 SSL 压缩 ’ • 8 -‘ 在被动模式中无法解密的会话 ’ • 9 -‘ 握手错误 ’ • 10 -‘ 解密错误 ’ • 11 -‘ 待处理服务器名称分类查找 ’ • 12 -‘ 待处理通用名称分类查找 ’ • 13 -‘ 内部错误 ’ • 14 -‘ 网络参数不可用 ’ • 15 -‘ 服务器证书处理无效 ’ • 16 -‘ 服务器证书指纹不可用 ’ • 17 -‘ 无法缓存持有者 DN’ • 18 -‘ 无法缓存颁发者 DN’ • 19 -‘ 未知 SSL 版本 ’ • 20 -‘ 外部证书列表不可用 ’ • 21 -‘ 外部证书指纹不可用 ’ • 22 -‘ 内部证书列表无效 ’ • 23 -‘ 内部证书列表不可用 ’ • 24 -‘ 内部证书不可用 ’ • 25 -‘ 内部证书指纹不可用 ’ • 26 -‘ 服务器证书验证不可用 ’ • 27 -‘ 服务器证书验证失败 ’ • 28 -‘ 操作无效 ’
SSL 流误差 (SSL Flow Error)	uint32	详细的 SSL 错误代码。这些值可用于提供支持。

表 B-37　连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明
SSL 流消息 (SSL Flow Messages)	uint32	在 SSL 握手期间，客户端和服务器之间交换的消息。有关详细信息，请参阅 http://tools.ietf.org/html/rfc5246。 • 0x00000001 - NSE_MT__HELLO_REQUEST • 0x00000002 - NSE_MT__CLIENT_ALERT • 0x00000004 - NSE_MT__SERVER_ALERT • 0x00000008 - NSE_MT__CLIENT_HELLO • 0x00000010 - NSE_MT__SERVER_HELLO • 0x00000020 - NSE_MT__SERVER_CERTIFICATE • 0x00000040 - NSE_MT__SERVER_KEY_EXCHANGE • 0x00000080 - NSE_MT__CERTIFICATE_REQUEST • 0x00000100 - NSE_MT__SERVER_HELLO_DONE • 0x00000200 - NSE_MT__CLIENT_CERTIFICATE • 0x00000400 - NSE_MT__CLIENT_KEY_EXCHANGE • 0x00000800 - NSE_MT__CERTIFICATE_VERIFY • 0x00001000 - NSE_MT__CLIENT_CHANGE_CIPHER_SPEC • 0x00002000 - NSE_MT__CLIENT_FINISHED • 0x00004000 - NSE_MT__SERVER_CHANGE_CIPHER_SPEC • 0x00008000 - NSE_MT__SERVER_FINISHED • 0x00010000 - NSE_MT__NEW_SESSION_TICKET • 0x00020000 - NSE_MT__HANDSHAKE_OTHER • 0x00040000 - NSE_MT__APP_DATA_FROM_CLIENT • 0x00080000 - NSE_MT__APP_DATA_FROM_SERVER
SSL 流标志 (SSL Flow Flags)	uint64	加密连接的调试级别标志。可能的值包括： • 0x00000001 - NSE_FLOW__VALID - 必须设置此字段，其他字段才有效 • 0x00000002 - NSE_FLOW__INITIALIZED - 内部结构已准备就绪进行处理 • 0x00000004 - NSE_FLOW__INTERCEPT - SSL 会话已被拦截
字符串块类型 (String Block Type)	uint32	启动包含 SSL 服务器名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	SSL 服务器名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “SSL 服务器名称 ”(SSL Server Name) 字段中的字节数。

表 B-37 连接统计信息数据块 5.4+ 字段 （续）

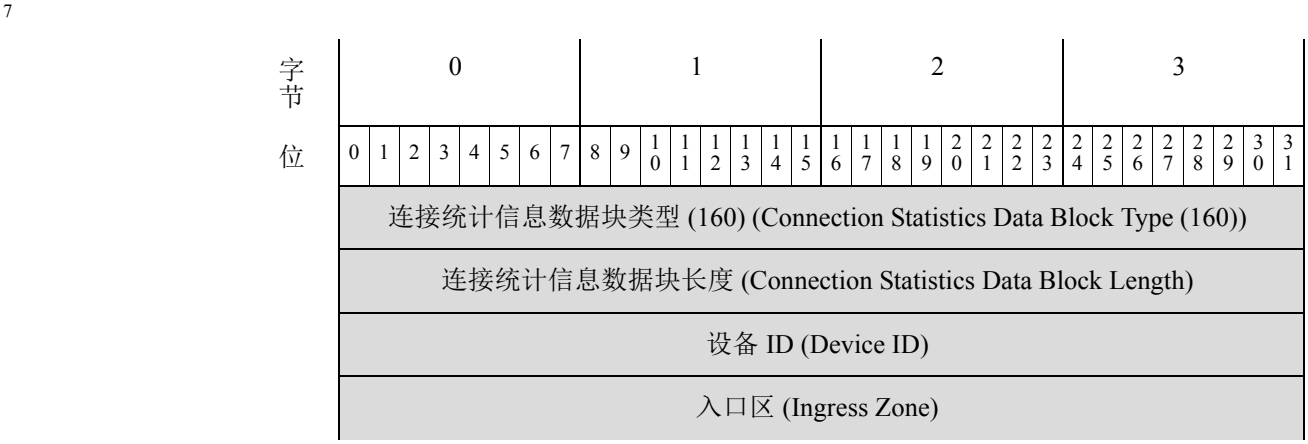
字段	数据类型	说明
SSL 服务器名称 (SSL Server Name)	字符串	在 SSL 客户端欢迎界面中服务器名称显示中提供的名称。
SSL URL 类别 (SSL URL Category)	uint32	根据服务器名称和证书常用名识别的流量类别。
SSL 会话 ID (SSL Session ID)	uint8[32]	当客户端和服务器同意进行会话重用时， SSL 握手期间使用的会话 ID 值
SSL 会话 ID 长度 (SSL Session ID Length)	uint8	SSL 会话 ID 的长度。尽管会话 ID 不能超过 32 个字节，此值可能小于 32 个字节。
SSL 票证 ID (SSL Ticket ID)	uint8[20]	当客户端和服务器同意使用会话票证时使用的会话票证散列。
SSL 票证 ID 长度 (SSL Ticket ID Length)	uint8	SSL 票证 ID 的长度。尽管票证 ID 不能超过 20 个字节，此值可能小于 20 个字节。
网络分析策略修订 (Network Analysis Policy revision)	uint8[16]	与连接事件相关的网络分析策略的修订。

连接统计信息数据块 6.0.x

连接统计信息数据块在连接数据消息中使用。用于 6.0 的连接统计信息数据块中添加了多个新字段。添加新字段是为了支持 ISE 集成和多个网络映射。用于版本 6.0.x 的连接统计信息数据块的块类型为系列 1 数据块组中的 160。它替代块类型 157，连接统计信息数据块 5.4.1，第 B-196 页。添加新字段是为了支持 DNS 查询和安全情报。

您可以通过在事件版本为 13 且事件代码为 71 的请求消息中设置扩展事件标志 （“ 请求标志 ” (Request Flags) 字段中的位 30）请求连接事件记录。请参阅请求标志，第 2-11 页。如果您启用位 23，则记录中会包含扩展事件报头。

下图显示用于 6.0.x 的连接统计信息数据块的格式：



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
入口区 (Ingress Zone) （续）																																
入口区 (Ingress Zone) （续）																																
入口区 (Ingress Zone) （续）																																
出口区 (Egress Zone)																																
出口区 (Egress Zone) （续）																																
出口区 (Egress Zone) （续）																																
出口区 (Egress Zone) （续）																																
入口接口 (Ingress Interface)																																
入口接口 (Ingress Interface) （续）																																
入口接口 (Ingress Interface) （续）																																
入口接口 (Ingress Interface) （续）																																
出口接口 (Egress Interface)																																
出口接口 (Egress Interface) （续）																																
出口接口 (Egress Interface) （续）																																
出口接口 (Egress Interface) （续）																																
发起方 IP 地址 (Initiator IP Address)																																
发起方 IP 地址 (Initiator IP Address) （续）																																
发起方 IP 地址 (Initiator IP Address) （续）																																
发起方 IP 地址 (Initiator IP Address) （续）																																
响应方 IP 地址 (Responder IP Address)																																
响应方 IP 地址 (Responder IP Address) （续）																																
响应方 IP 地址 (Responder IP Address) （续）																																
响应方 IP 地址 (Responder IP Address) （续）																																
策略修订 (Policy Revision)																																

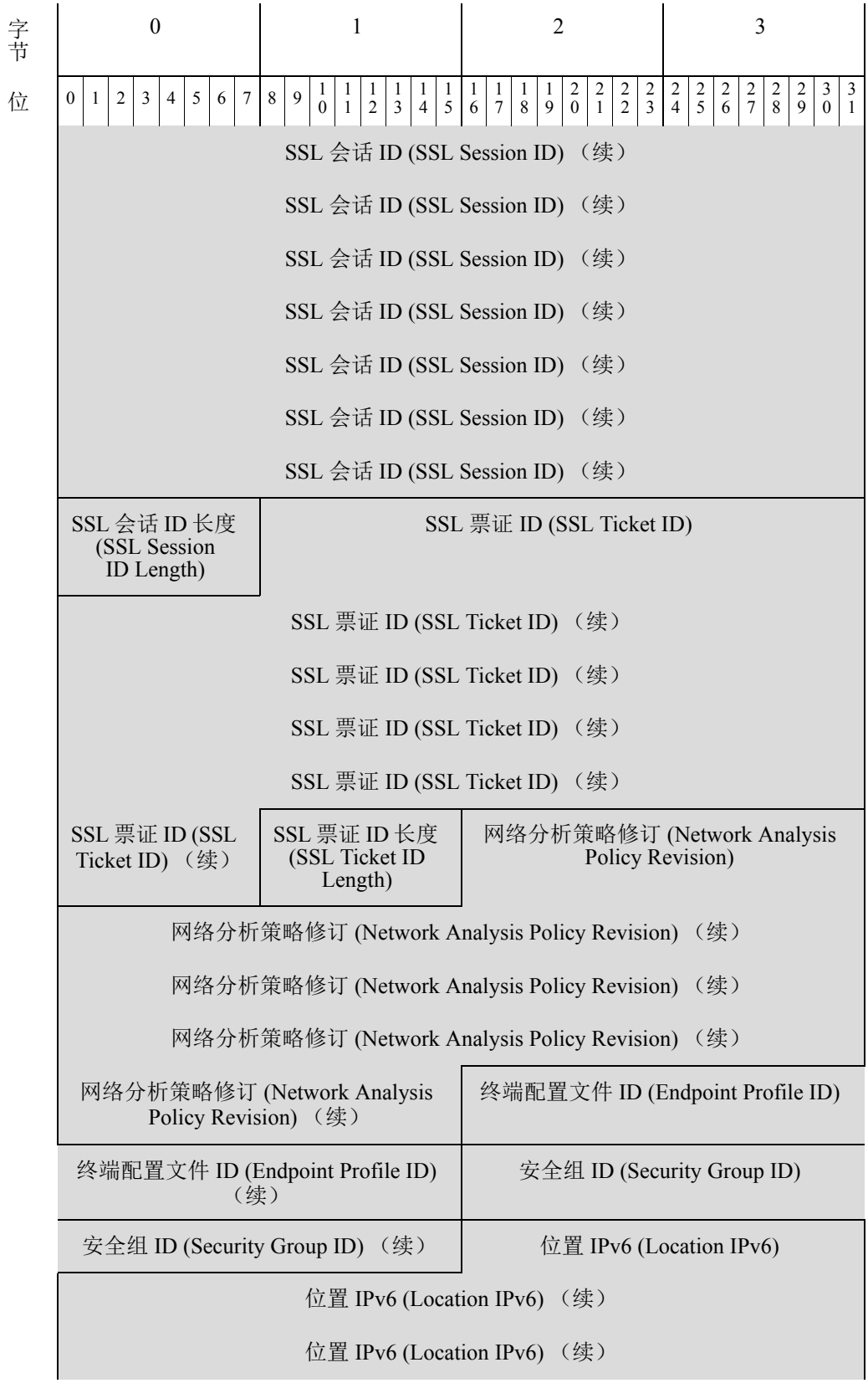

字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
策略修订 (Policy Revision) （续）
策略修订 (Policy Revision) （续）
策略修订 (Policy Revision) （续）
规则 ID (Rule ID)
规则操作 (Rule Action)
规则原因 (Rule Reason)
规则原因 (Rule Reason) （续）
发起方端口 (Initiator Port)
响应方端口 (Responder Port)
TCP 标志 (TCP Flags)
协议 (Protocol)
NetFlow 源 (NetFlow Source)
Netflow 源 (Netflow Source) （续）
Netflow 源 (Netflow Source) （续）
Netflow 源 (Netflow Source) （续）
NetFlow 源 （续）
实例 ID (Instance ID)
连接计数器 (Connection Counter)
连接计数器 (Cx Counter) （续）
第一个数据包时间戳 (First Packet Timestamp)
第一个数据包时间戳 (First Pkt Time) （续）
最后一个数据包时间戳 (Last Packet Timestamp)
最后一个数据包时间戳 (Last Pkt Time) （续）
发起方传输的数据包数 (Initiator Transmitted Packets)
发起方传输的数据包数 (Initiator Transmitted Packets) （续）
发起方传输的数据包数 (Initiator Tx Pkt) （续）
响应方传输的数据包数 (Responder Transmitted Packets)
响应方传输的数据包数 (Responder Transmitted Packets) （续）
响应方传输的数据包数 (Res. Tx Pkt) （续）
发起方传输的字节数 (Initiator Transmitted Bytes)

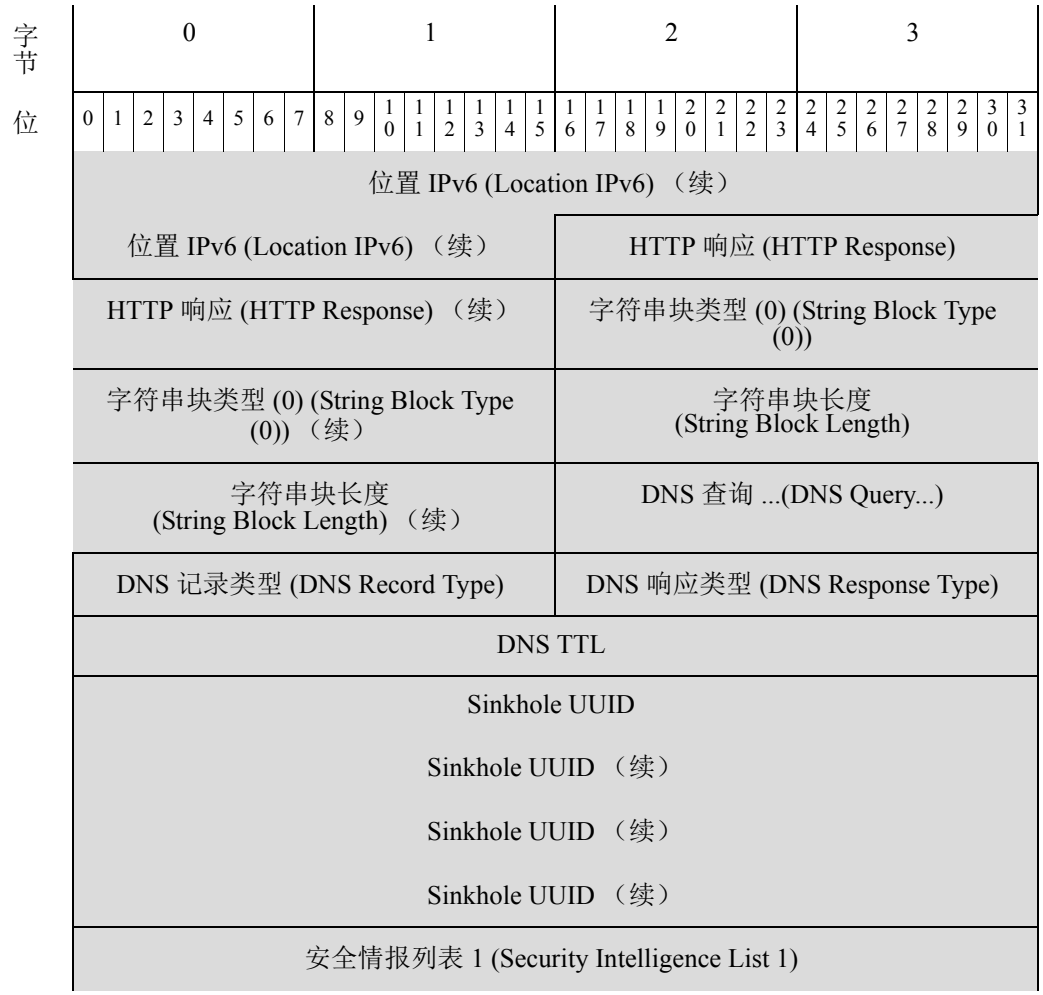

字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
发起方传输的字节数 (Initiator Transmitted Bytes) （续）
发起方传输的字节数 (Initiator Tx Bts) （续）
响应方传输的字节数 (Responder Transmitted Bytes)
响应方传输的字节数 (Responder Transmitted Bytes) （续）
响应方传输的字节数 (Res. Tx Bts) （续）
用户 ID (User ID)
用户 ID (User ID) （续）
应用协议 ID (Application Protocol ID)
应用协议 ID (Application Protocol ID) （续）
URL 类别 (URL Category)
URL 类别 (URL Category) （续）
URL 信誉 (URL Reputation)
URL 信誉 (URL Rep) （续）
客户端应用 ID (Client Application ID)
客户端应用 ID (Client App ID) （续）
Web 应用 ID (Web Application ID)
客户端 URL
Web 应用 ID (Web App ID) （续）
字符串块类型 (0) (Str. Block Type (0))
字符串块类型 (Str. Block Type) （续）
字符串块长度 (String Block Length)
字符串块长度 (Str. Block Len.) （续）
客户端应用 URL... (Client App. URL...)
NetBIOS 名称
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
NetBIOS 名称 ...(NetBIOS Name...)


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
客户端应用版本 (Client App Version)
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
客户端应用版本 ...(Client Application Version...)
监控器规则 1 (Monitor Rule 1)
监控器规则 2 (Monitor Rule 2)
监控器规则 3 (Monitor Rule 3)
监控器规则 4 (Monitor Rule 4)
监控器规则 5 (Monitor Rule 5)
监控器规则 6 (Monitor Rule 6)
监控器规则 7 (Monitor Rule 7)
监控器规则 8 (Monitor Rule 8)
安全接口源 / 目标 (Sec. Int. Src/Dst)
安全接口层 (Sec. Int. Layer)
文件事件计数 (File Event Count)
入侵事件计数 (Intrusion Event Count)
发起方国家 / 地区 (Initiator Country)
响应方国家 / 地区 (Responder Country)
IOC 编号 (IOC Number)
源自治系统 (Source Autonomous System)
目标自治系统 (Destination Autonomous System)
SNMP 输入 (SNMP In)
SNMP 输出 (SNMP Out)
源 TOS (Source TOS)
目标 TOS (Destination TOS)
源掩码 (Source Mask)
目标掩码 (Destination Mask)
安全情景 (Security Context)
安全情景 (Security Context) （续）


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
安全情景 (Security Context) （续）
安全情景 (Security Context) （续）
引用的主机 (Referenced Host)
VLAN ID
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0)) （续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length) （续）
引用的主机 (Referenced Host)...(Referenced Host...)
用户代理
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
用户代理 ... (User Agent...)
HTTP 引用站点 (HTTP Referrer)
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
HTTP 引用站点 ...(HTTP Referrer...)
SSL 证书指纹 (SSL Certificate Fingerprint)
SSL 证书指纹 (SSL Certificate Fingerprint) （续）
SSL 证书指纹 (SSL Certificate Fingerprint) （续）
SSL 证书指纹 (SSL Certificate Fingerprint) （续）
SSL 证书指纹 (SSL Certificate Fingerprint) （续）
SSL 策略 ID (SSL Policy ID)


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 策略 ID (SSL Policy ID) （续）
SSL 策略 ID (SSL Policy ID) （续）
SSL 策略 ID (SSL Policy ID) （续）
SSL 规则 ID (SSL Rule ID)
SSL 密码套件 (SSL Cipher Suite)
SSL 版本 (SSL Version)
SSL 服务器证书统计信息 (SSL Srv Cert. Stat.)
SSL 服务器证书统计信息 (SSL Srv Cert. Stat.) （续）
SSL 实际操作 (SSL Actual Action)
SSL 实际操作 (SSL actual Action) （续）
SSL 预期操作 (SSL Expected Action)
SSL 流状态 (SSL Flow Status)
SSL 流状态 （续）
SSL 流误差 (SSL Flow Error)
SSL 流误差 (SSL Flow Error) （续）
SSL 流量消息 (SSL Flow Messages)
SSL 流消息 (SSL Flow Msg) （续）
SSL 流标志 (SSL Flow Flags)
SSL 流标志 (SSL Flow Flags) （续）
SSL 流标志 (SSL Flow Flags) （续）
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0)) （续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length) （续）
SSL 服务器名称 ... (SSL Server Names...)
SSL 服务器名称 (SSL Server Names)
SSL URL 类别 (SSL URL Category)
SSL 会话 ID (SSL Session ID)


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID 长度 (SSL Session ID Length)
SSL 票证 ID (SSL Ticket ID)
SSL 票证 ID (SSL Ticket ID) （续）
SSL 票证 ID (SSL Ticket ID) （续）
SSL 票证 ID (SSL Ticket ID) （续）
SSL 票证 ID (SSL Ticket ID) （续）
SSL 票证 ID (SSL Ticket ID) （续）
SSL 票证 ID 长度 (SSL Ticket ID Length)
网络分析策略修订 (Network Analysis Policy Revision)
网络分析策略修订 (Network Analysis Policy Revision) （续）
网络分析策略修订 (Network Analysis Policy Revision) （续）
网络分析策略修订 (Network Analysis Policy Revision) （续）
网络分析策略修订 (Network Analysis Policy Revision) （续）
终端配置文件 ID (Endpoint Profile ID)
终端配置文件 ID (Endpoint Profile ID) （续）
安全组 ID (Security Group ID)
安全组 ID (Security Group ID) （续）
位置 IPv6 (Location IPv6)
位置 IPv6 (Location IPv6) （续）
位置 IPv6 (Location IPv6) （续）



下表对用于 6.0.x 的连接统计信息数据块的字段进行了说明。

表 B-38 连接统计信息数据块 6.0.x 字段

字段	数据类型	说明
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 6.0+ 的连接统计信息数据块。值始终为 160。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID (Device ID)	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。

表 B-38　　连接统计信息数据块 6.0.x 字段 （续）

字段	数据类型	说明
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP Address)	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP Address)	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号 （如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符 （如适用）。
规则操作 (Rule Action)	uint16	在用户界面中选择的针对该规则的操作 （允许、阻止等）。
规则原因 (Rule Reason)	uint32	规则触发事件的原因。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址。
实例 ID (Instance ID)	uint16	生成事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的 UNIX 时间戳。

表 B-38 连接统计信息数据块 6.0.x 字段 （续）

字段	数据类型	说明
发起方传输的数据包数 (Initiator Transmitted Packets)	uint64	发起主机传输的数据包数。
响应方传输的数据包数 (Responder Transmitted Packets)	uint64	响应主机传输的数据包数。
发起方传输的字节数 (Initiator Transmitted Bytes)	uint64	发起主机传输的字节数。
响应方传输的字节数 (Responder Transmitted Bytes)	uint64	响应主机传输的字节数。
用户 ID (User ID)	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号 （如适用）。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号 （如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的 URL （如适用）（例如， `/files/index.html`）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。

表 B-38　连接统计信息数据块 6.0.x 字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本 (Client Application Version)	字符串	客户端应用版本。
监控器规则 1 (Monitor Rule 1)	uint32	与连接事件关联的第一个监控器规则的 ID。
监控器规则 2 (Monitor Rule 2)	uint32	与连接事件关联的第二个监控器规则的 ID。
监控器规则 3 (Monitor Rule 3)	uint32	与连接事件关联的第三个监控器规则的 ID。
监控器规则 4 (Monitor Rule 4)	uint32	与连接事件关联的第四个监控器规则的 ID。
监控器规则 5 (Monitor Rule 5)	uint32	与连接事件关联的第五个监控器规则的 ID。
监控器规则 6 (Monitor Rule 6)	uint32	与连接事件关联的第六个监控器规则的 ID。
监控器规则 7 (Monitor Rule 7)	uint32	与连接事件关联的第七个监控器规则的 ID。
监控器规则 8 (Monitor Rule 8)	uint32	与连接事件关联的第八个监控器规则的 ID。
安全情报源 / 目标 (Security Intelligence Source/ Destination)	uint8	源或目标 IP 地址与 IP 阻止列表是否匹配。
安全情报层 (Security Intelligence Layer)	uint8	与 IP 阻止列表匹配的 IP 层。
文件事件计数 (File Event Count)	uint16	用于区别同一秒发生的文件事件的值。

表 B-38 连接统计信息数据块 6.0.x 字段 （续）

字段	数据类型	说明
入侵事件 (Intrusion Event)（续）	uint16	用于区别同一秒发生的入侵事件的值。
发起方国家 / 地区 (Initiator Country)	uint16	发起主机的国家 / 地区代码。
响应方国家 / 地区 (Responder Country)	uint 16	响应主机的国家 / 地区代码。
IOC 编号 (IOC Number)	uint16	与此事件相关的危害的 ID 号码。
源自治系统 (Source Autonomous System)	uint32	作为源或对等体的源自治系统的编号。
目标自治系统 (Destination Autonomous System)	uint32	作为源或对等体的目标自治系统的编号。
SNMP 输入 (SNMP Input)	uint16	输入接口的 SNMP 索引。
SNMP 输出 (SNMP Output)	uint16	输出接口的 SNMP 索引。
源 TOS (Source TOS)	uint8	传入接口的服务字节设置类型。
目标 TOS (Destination TOS)	uint8	传出接口的服务字节设置类型。
源掩码 (Source Mask)	uint8	源地址前缀掩码。
目标掩码 (Destination Mask)	uint8	目标地址前缀掩码。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
字符串块类型 (String Block Type)	uint32	启动包含引用的主机的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	引用的主机字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 引用的主机 ”(Referenced Host) 字段中的字节数。

表 B-38　连接统计信息数据块 6.0.x 字段 （续）

字段	数据类型	说明
引用的主机 (Referenced Host)	字符串	HTTP 或 DNS 中提供的主机名信息。
字符串块类型 (String Block Type)	uint32	启动包含用户代理的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户代理字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 用户代理 ”(User Agent) 字段中的字节数。
用户代理 (User Agent)	字符串	会话中用户代理报头字段中的信息。
字符串块类型 (String Block Type)	uint32	启动包含 HTTP 引用站点的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	HTTP 引用站点字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “HTTP 引用站点 ”(HTTP Referrer) 字段中的字节数。
HTTP 引用站点 (HTTP Referrer)	字符串	页面起源的站点。该站点可在 HTTP 流量中引用的报头信息中找到。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 策略 ID (SSL Policy ID)	uint8[16]	处理连接的 SSL 策略的 ID 编号。
SSL 规则 ID (SSL Rule ID)	uint32	处理连接的 SSL 规则或默认操作的 ID 编号。
SSL 密码套件 (SSL Cipher Suite)	uint16	SSL 连接使用的加密套件。该值以十进制格式存储。有关该值指定的密码套件，请参阅 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml。
SSL 版本 (SSL Version)	uint8	用来加密连接的 SSL 或 TLS 协议版本。
SSL 服务器证书状态 (SSL Server Certificate Status)	uint32	SSL 证书的状态。可能的值包括： • 0 - 未检查 - 服务器证书状态未评估。 • 1 - 未知 - 服务器证书状态无法确定。 • 2 - 有效 - 服务器证书有效。 • 4 - 自签 - 服务器证书已自签。 • 16 - 颁发者无效 - 服务器证书的颁发者无效。 • 32 - 签名无效 - 服务器证书的签名无效。 • 64 - 过期 - 服务器证书已过期。 • 128 - 尚未生效 - 服务器证书尚未生效。 • 256 - 撤销 - 服务器证书已被撤销。

表 B-38 连接统计信息数据块 6.0.x 字段 （续）

字段	数据类型	说明
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括： • 0 -‘ 未知 ’ • 1 -‘ 请勿解密 ’ • 2 -‘ 阻止 ’ • 3 -‘ 阻止并重置 ’ • 4 -‘ 解密 （已知密钥） ’ • 5 -‘ 解密 （更换秘钥） ’ • 6 -‘ 解密 （放弃） ’
SSL 预期操作 (SSL Expected Action)	uint16	根据 SSL 规则应该对连接执行的操作。可能的值包括： • 0 -‘ 未知 ’ • 1 -‘ 请勿解密 ’ • 2 -‘ 阻止 ’ • 3 -‘ 阻止并重置 ’ • 4 -‘ 解密 （已知密钥） ’ • 5 -‘ 解密 （更换秘钥） ’ • 6 -‘ 解密 （放弃） ’

表 B-38　连接统计信息数据块 6.0.x 字段 （续）

字段	数据类型	说明
SSL 流状态 (SSL Flow Status)	uint16	SSL 流量的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括： • 0 -‘ 未知 ’ • 1 -‘ 不匹配 ’ • 2 -‘ 成功 ’ • 3 -‘ 非缓存会话 ’ • 4 -‘ 未知密码套件 ’ • 5 -‘ 不受支持的密码套件 ’ • 6 -‘ 不受支持的 SSL 版本 ’ • 7 -‘ 使用的 SSL 压缩 ’ • 8 -‘ 在被动模式中无法解密的会话 ’ • 9 -‘ 握手错误 ’ • 10 -‘ 解密错误 ’ • 11 -‘ 待处理服务器名称分类查找 ’ • 12 -‘ 待处理通用名称分类查找 ’ • 13 -‘ 内部错误 ’ • 14 -‘ 网络参数不可用 ’ • 15 -‘ 服务器证书处理无效 ’ • 16 -‘ 服务器证书指纹不可用 ’ • 17 -‘ 无法缓存持有者 DN’ • 18 -‘ 无法缓存颁发者 DN’ • 19 -‘ 未知 SSL 版本 ’ • 20 -‘ 外部证书列表不可用 ’ • 21 -‘ 外部证书指纹不可用 ’ • 22 -‘ 内部证书列表无效 ’ • 23 -‘ 内部证书列表不可用 ’ • 24 -‘ 内部证书不可用 ’ • 25 -‘ 内部证书指纹不可用 ’ • 26 -‘ 服务器证书验证不可用 ’ • 27 -‘ 服务器证书验证失败 ’ • 28 -‘ 操作无效 ’
SSL 流误差 (SSL Flow Error)	uint32	详细的 SSL 错误代码。这些值可用于提供支持。

表 B-38 连接统计信息数据块 6.0.x 字段 （续）

字段	数据类型	说明
SSL 流消息 (SSL Flow Messages)	uint32	在 SSL 握手期间，客户端和服务器之间交换的消息。有关详细信息，请参阅 http://tools.ietf.org/html/rfc5246。 • 0x00000001 - NSE_MT__HELLO_REQUEST • 0x00000002 - NSE_MT__CLIENT_ALERT • 0x00000004 - NSE_MT__SERVER_ALERT • 0x00000008 - NSE_MT__CLIENT_HELLO • 0x00000010 - NSE_MT__SERVER_HELLO • 0x00000020 - NSE_MT__SERVER_CERTIFICATE • 0x00000040 - NSE_MT__SERVER_KEY_EXCHANGE • 0x00000080 - NSE_MT__CERTIFICATE_REQUEST • 0x00000100 - NSE_MT__SERVER_HELLO_DONE • 0x00000200 - NSE_MT__CLIENT_CERTIFICATE • 0x00000400 - NSE_MT__CLIENT_KEY_EXCHANGE • 0x00000800 - NSE_MT__CERTIFICATE_VERIFY • 0x00001000 - NSE_MT__CLIENT_CHANGE_CIPHER_SPEC • 0x00002000 - NSE_MT__CLIENT_FINISHED • 0x00004000 - NSE_MT__SERVER_CHANGE_CIPHER_SPEC • 0x00008000 - NSE_MT__SERVER_FINISHED • 0x00010000 - NSE_MT__NEW_SESSION_TICKET • 0x00020000 - NSE_MT__HANDSHAKE_OTHER • 0x00040000 - NSE_MT__APP_DATA_FROM_CLIENT • 0x00080000 - NSE_MT__APP_DATA_FROM_SERVER
SSL 流标志 (SSL Flow Flags)	uint64	加密连接的调试级别标志。可能的值包括： • 0x00000001 - NSE_FLOW__VALID - 必须设置此字段，其他字段才有效 • 0x00000002 - NSE_FLOW__INITIALIZED - 内部结构已准备就绪进行处理 • 0x00000004 - NSE_FLOW__INTERCEPT - SSL 会话已被拦截
字符串块类型 (String Block Type)	uint32	启动包含 SSL 服务器名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	SSL 服务器名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “SSL 服务器名称 ”(SSL Server Name) 字段中的字节数。

表 B-38　连接统计信息数据块 6.0.x 字段 （续）

字段	数据类型	说明
SSL 服务器名称 (SSL Server Name)	字符串	在 SSL 客户端欢迎界面中服务器名称显示中提供的名称。
SSL URL 类别 (SSL URL Category)	uint32	根据服务器名称和证书常用名识别的流量类别。
SSL 会话 ID (SSL Session ID)	uint8[32]	当客户端和服务器同意进行会话重用时， SSL 握手期间使用的会话 ID 值
SSL 会话 ID 长度 (SSL Session ID Length)	uint8	SSL 会话 ID 的长度。尽管会话 ID 不能超过 32 个字节，此值可能小于 32 个字节。
SSL 票证 ID (SSL Ticket ID)	uint8[20]	当客户端和服务器同意使用会话票证时使用的会话票证散列。
SSL 票证 ID 长度 (SSL Ticket ID Length)	uint8	SSL 票证 ID 的长度。尽管票证 ID 不能超过 20 个字节，此值可能小于 20 个字节。
网络分析策略修订 (Network Analysis Policy revision)	uint8[16]	与连接事件相关的网络分析策略的修订。
终端配置文件 ID (Endpoint Profile ID)	uint32	ISE 识别的连接终端使用的设备类型的 ID 号码。这是每个 DC 特有的，在元数据中进行解析。
安全组 ID (Security Group ID)	uint32	由 ISE 根据策略分配给用户的 ID 号码。
位置 IPv6 (Location IPv6)	uint8[16]	与 ISE 通信的接口的 IP 地址。可以是 IPv4 或 IPv6。
HTTP 响应 (HTTP Response)	uint32	HTTP 请求的响应代码。
字符串块类型 (String Block Type)	uint32	启动 DNS 查询的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 DNS 查询字符串中的字节数。
DNS 查询 (DNS Query)	字符串	发送到 DNS 服务器的查询的内容。
DNS 记录类型 (DNS Record Type)	uint16	DNS 记录类型的数字值。

表 B-38 连接统计信息数据块 6.0.x 字段 （续）

字段	数据类型	说明
DNS 响应类型 (DNS Response Type)	uint16	0 - NoError - 无错误 1 - FormErr - 格式错误 2 - ServFail - 服务器故障 3 - NXDomain - 域不存在 4 - NotImp - 未执行 5 - Refused - 查询被拒绝 6 - YXDomain - 名称在不应该存在的时候存在 7 - YXRRSet - RR 设置在不应该存在的时候存在 8 - NXRRSet - 应该存在的 RR 设置不存在 9 - NotAuth - 未授权 10 - NotZone - 区域中不包含名称 16 - BADSIG - TSIG 签名故障 17 - BADKEY - 密钥未识别 18 - BADTIME - 签名超出时间窗口 19 - BADMODE - 坏 TKEY 模式 20 - BADNAME - 密钥名称重复 21 - BADALG - 不支持算法 22 - BADTRUNC - 截断错误 3841 - NXDOMAIN - 防火墙的 NXDOMAIN 响应 3842 - SINKHOLE - 从防火墙发出黑洞 (Sinkhole) 响应
DNS TTL	uint32	DNS 响应的生存时间 （秒数）
Sinkhole UUID	uin8[16]	与此 sinkhole 对象关联的修订 UUID。
安全情报列表 1 (Security Intelligence List 1)	uint32	与事件关联的安全情报列表。这映射到关联元数据中的安全情报列表。可能存在两个与连接关联的安全情报列表。
安全情报列表 2 (Security Intelligence List 2)	uint32	与事件关联的安全情报列表。这映射到关联元数据中的安全情报列表。可能存在两个与连接关联的安全情报列表。

连接统计信息数据块 6.1.x

连接统计信息数据块在连接数据消息中使用。用于 6.1.x 的连接统计信息数据块中添加了多个新字段。添加新字段是为了支持 ISE 集成和多个网络映射。用于版本 6.1+ 的连接统计信息数据块的块类型为系列 1 数据块组中的 163。它替代块类型 160，连接统计信息数据块 6.0.x，第 B-212 页。添加新字段是为了支持 DNS 查询和安全情报。它被块类型 168 替代，连接统计信息数据块 6.2+，第 4-119 页，

您可以通过在事件版本为 13 且事件代码为 71 的请求消息中设置扩展事件标志 （“ 请求标志 ” (Request Flags) 字段中的位 30）请求连接事件记录。请参阅请求标志，第 2-11 页。如果您启用位 23，则记录中会包含扩展事件报头。

有关连接统计信息数据消息的详细信息，请参阅连接统计信息数据消息，第 4-54 页。

下图显示用于 6.1+ 的连接统计信息数据块的格式：

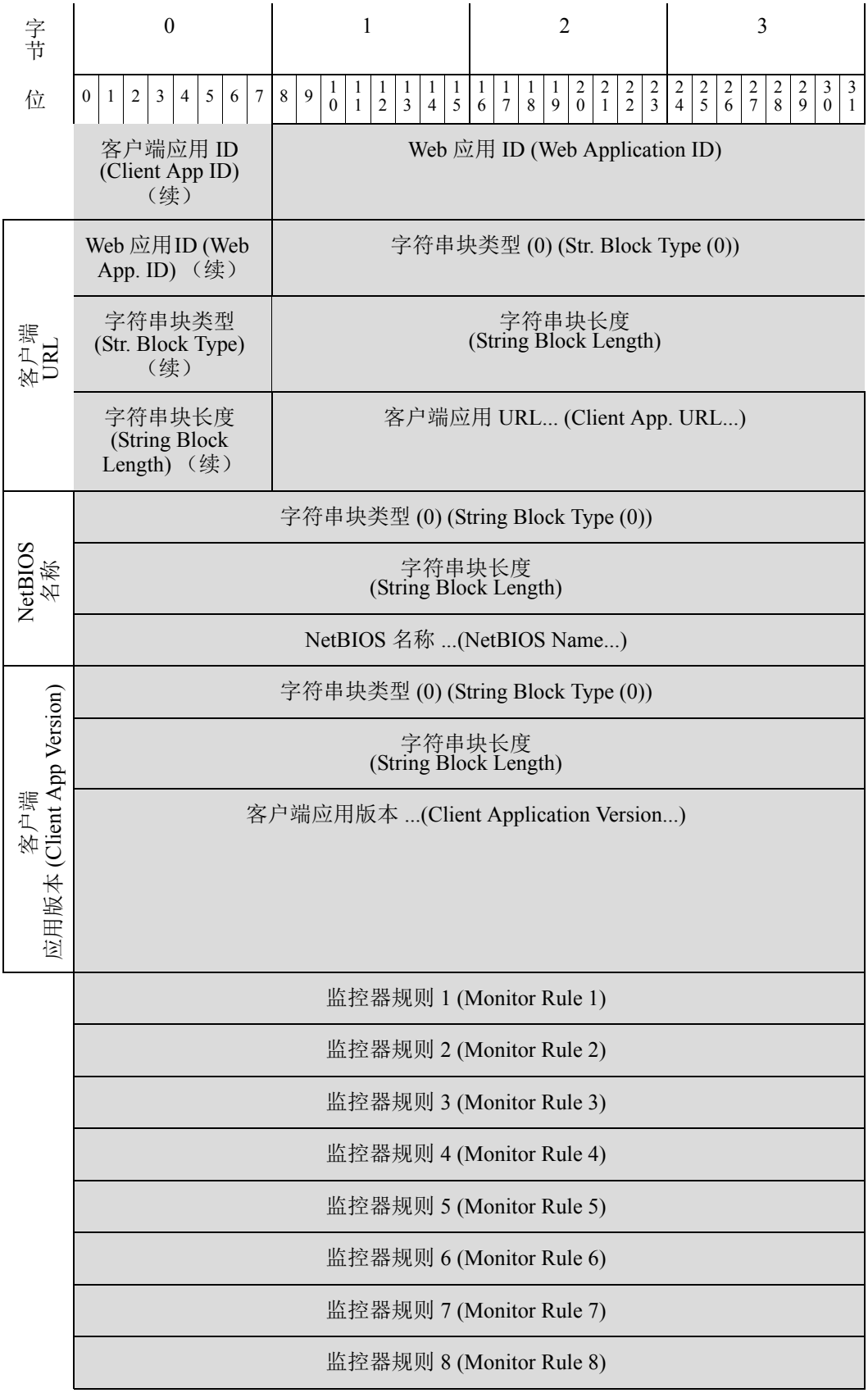
7

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
连接统计信息数据块类型 (163) (Connection Statistics Data Block Type (160))																																
连接统计信息数据块长度 (Connection Statistics Data Block Length)																																
设备 ID (Device ID)																																
入口区 (Ingress Zone) 入口区 (Ingress Zone) （续） 入口区 (Ingress Zone) （续） 入口区 (Ingress Zone) （续）																																
出口区 (Egress Zone) 出口区 (Egress Zone) （续） 出口区 (Egress Zone) （续） 出口区 (Egress Zone) （续）																																
入口接口 (Ingress Interface) 入口接口 (Ingress Interface) （续） 入口接口 (Ingress Interface) （续） 入口接口 (Ingress Interface) （续）																																
出口接口 (Egress Interface)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
出口接口 (Egress Interface) （续）																																
出口接口 (Egress Interface) （续）																																
出口接口 (Egress Interface) （续）																																
发起方 IP 地址 (Initiator IP Address)																																
发起方 IP 地址 (Initiator IP Address) （续）																																
发起方 IP 地址 (Initiator IP Address) （续）																																
发起方 IP 地址 (Initiator IP Address) （续）																																
响应方 IP 地址 (Responder IP Address)																																
响应方 IP 地址 (Responder IP Address) （续）																																
响应方 IP 地址 (Responder IP Address) （续）																																
响应方 IP 地址 (Responder IP Address) （续）																																
原始客户端 IP 地址 (Original Client IP Address)																																
原始客户端 IP 地址 (Original Client IP Address) （续）																																
原始客户端 IP 地址 (Original Client IP Address) （续）																																
原始客户端 IP 地址 (Original Client IP Address) （续）																																
策略修订 (Policy Revision)																																
策略修订 (Policy Revision) （续）																																
策略修订 (Policy Revision) （续）																																
策略修订 (Policy Revision) （续）																																
规则 ID (Rule ID)																																
隧道规则 ID (Tunnel Rule ID)																																
规则操作 (Rule Action)																	规则原因 (Rule Reason)															
规则原因 (Rule Reason) （续）																	发起方端口 (Initiator Port)															
响应方端口 (Responder Port)																	TCP 标志 (TCP Flags)															

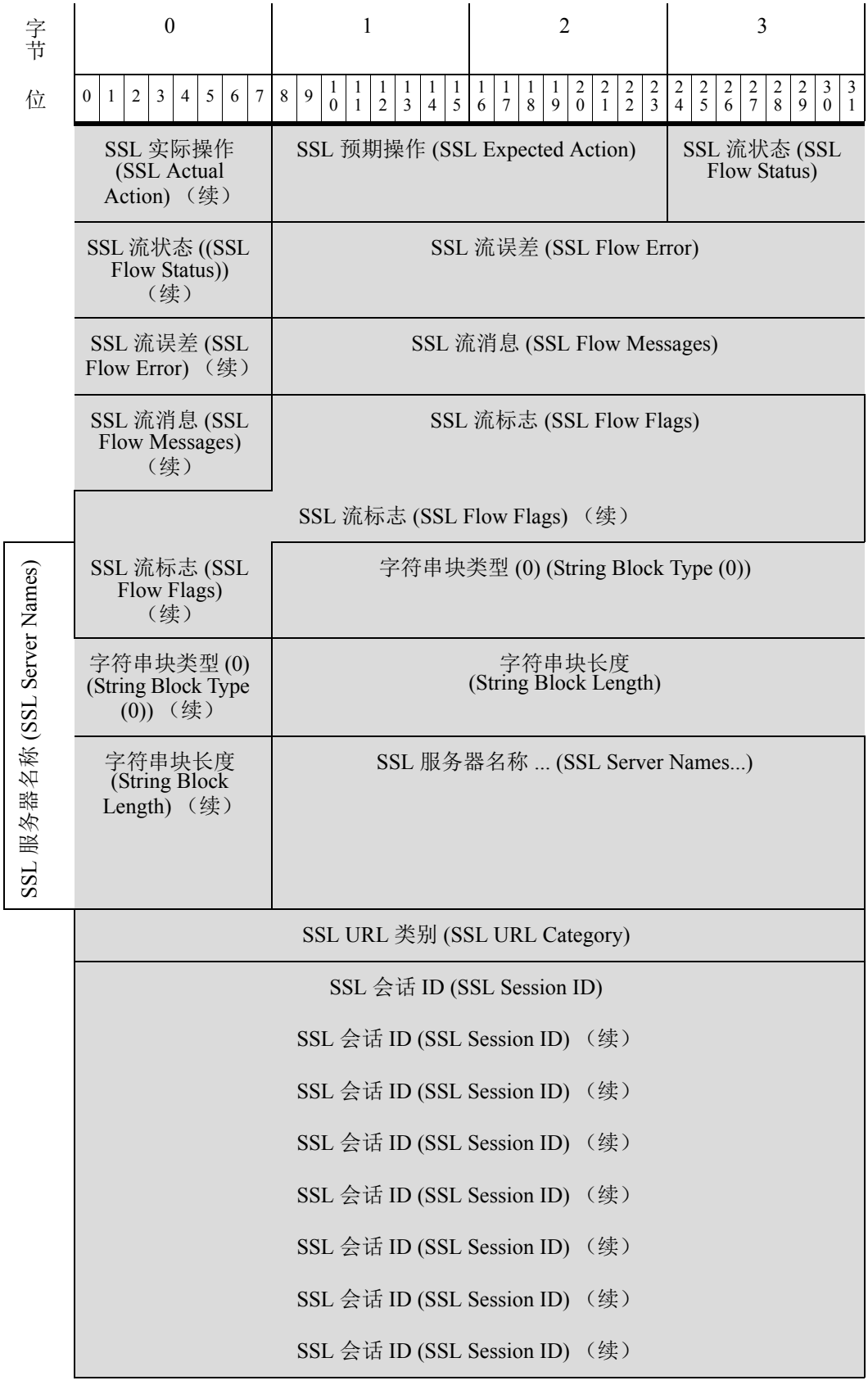

字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
协议 (Protocol)
NetFlow 源 (NetFlow Source)
Netflow 源 (Netflow Source) （续）
Netflow 源 (Netflow Source) （续）
Netflow 源 (Netflow Source) （续）
NetFlow 源 （续）
实例 ID (Instance ID)
连接计数器 (Connection Counter)
连接计数器 (Cx Counter) （续）
第一个数据包时间戳 (First Packet Timestamp)
第一个数据包时间戳 (First Pkt Time) （续）
最后一个数据包时间戳 (Last Packet Timestamp)
最后一个数据包时间戳 (Last Pkt Time) （续）
发起方传输的数据包数 (Initiator Transmitted Packets)
发起方传输的数据包数 (Initiator Transmitted Packets) （续）
发起方传输的数据包数 (Initiator Tx Pkt) （续）
响应方传输的数据包数 (Responder Transmitted Packets)
响应方传输的数据包数 (Responder Transmitted Packets) （续）
响应方传输的数据包数 (Res. Tx Pkt) （续）
发起方传输的字节数 (Initiator Transmitted Bytes)
发起方传输的字节数 (Initiator Transmitted Bytes) （续）
发起方传输的字节数 (Initiator Tx Bts) （续）
响应方传输的数据包数 (Responder Transmitted Packets)
响应方传输的字节数 (Responder Transmitted Bytes) （续）
响应方传输的字节数 (Res. Tx Bts) （续）
发起方丢弃的数据包数 (Initiator Packets Dropped)
发起方丢弃的数据包数 (Initiator Packets Dropped) （续）

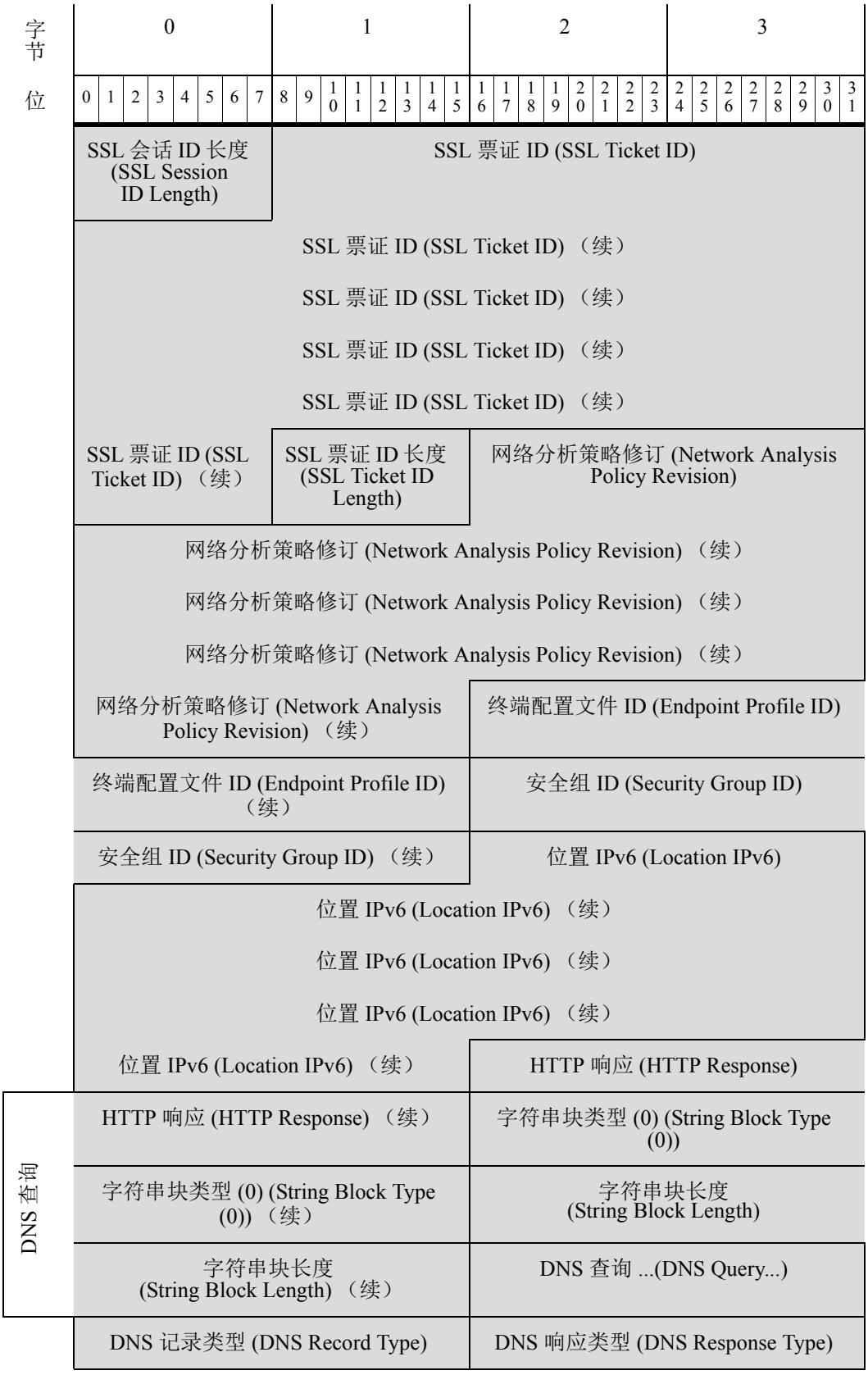
字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	发起方丢弃的数据包数 (Init. Pkt. Drop) （续）								响应方丢弃的数据包数 (Responder Packets Dropped)																							
	响应方丢弃的数据包数 (Responder Packets Dropped) （续）																															
	响应方丢弃的数据包数 (Resp. Pkt. Drop) （续）								发起方丢弃的字节数 (Initiator Bytes Dropped)																							
	发起方丢弃的字节数 (Initiator Bytes Dropped) （续）																															
	发起方丢弃的数据包数 (Init. Byte Drop) （续）								响应方丢弃的字节数 (Responder Bytes Dropped)																							
	响应方丢弃的字节数 (Responder Bytes Dropped) （续）																															
	响应方丢弃的数据包数 (Resp. Byte Drop) （续）								QOS 应用的接口 (QOS Applied Interface)																							
	QOS 应用的接口 (QOS Applied Interface) （续）																															
	QOS 应用的接口 (QOS Applied Interface) （续）																															
	QOS 应用的接口 (QOS Applied Interface) （续）																															
	QOS 应用的接口 (QOS Applied Interface) （续）								QOS 规则 ID (QOS Rule ID)																							
	QOS 规则 ID (QOS Rule ID) （续）								用户 ID (User ID)																							
	用户 ID (User ID) （续）								应用协议 ID (Application Protocol ID)																							
	应用协议 ID (Application Protocol ID) （续）								URL 类别 (URL Category)																							
	URL 类别 (URL Category) （续）								URL 信誉 (URL Reputation)																							
	URL 信誉 (URL Rep) （续）								客户端应用 ID (Client Application ID)																							

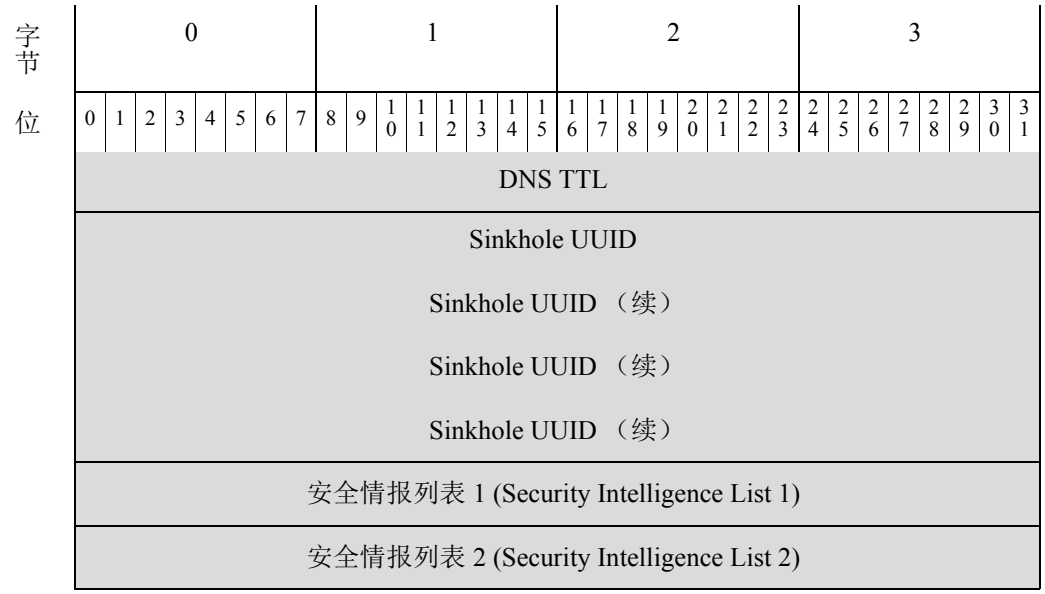

字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
客户端应用 ID (Client App ID) （续）
Web 应用 ID (Web Application ID)
客户端 URL
Web 应用ID (Web App. ID) （续）
字符串块类型 (0) (Str. Block Type (0))
字符串块类型 (Str. Block Type) （续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length) （续）
客户端应用 URL... (Client App. URL...)
NetBIOS 名称
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
NetBIOS 名称 ...(NetBIOS Name...)
客户端应用版本 (Client App Version)
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
客户端应用版本 ...(Client Application Version...)
监控器规则 1 (Monitor Rule 1)
监控器规则 2 (Monitor Rule 2)
监控器规则 3 (Monitor Rule 3)
监控器规则 4 (Monitor Rule 4)
监控器规则 5 (Monitor Rule 5)
监控器规则 6 (Monitor Rule 6)
监控器规则 7 (Monitor Rule 7)
监控器规则 8 (Monitor Rule 8)

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	安全接口源 / 目标 (Sec. Int. Src/Dst)								安全接口层 (Sec. Int. Layer)								文件事件计数 (File Event Count)															
	入侵事件计数 (Intrusion Event Count)																发起方国家 / 地区 (Initiator Country)															
	响应方国家 / 地区 (Responder Country)																原始客户端国家 / 地区 (Original Client Country)															
	IOC 编号 (IOC Number)																源自治系统 (Source Autonomous System)															
	源自治系统 (Source Autonomous System) （续）																目标自治系统 (Destination Autonomous System)															
	目标自治系统 (Destination Autonomous System)																SNMP 输入 (SNMP In)															
	SNMP 输出 (SNMP Out)																源 TOS (Source TOS)								目标 TOS (Destination TOS)							
	源掩码 (Source Mask)								目标掩码 (Destination Mask)								安全情景 (Security Context)															
	安全情景 (Security Context)																															
	安全情景 (Security Context) （续）																															
	安全情景 (Security Context) （续）																															
	安全情景 (Security Context) （续）																VLAN ID															
引用的主机 (Referenced Host)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	引用的主机 (Referenced Host)...(Referenced Host...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
用户代理	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户代理 ... (User Agent...)																															
HTTP 引用站点 (HTTP Referrer)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	HTTP 引用站点 ...(HTTP Referrer...)																															
	SSL 证书指纹 (SSL Certificate Fingerprint)																															
	SSL 证书指纹 (SSL Certificate Fingerprint) （续）																															
	SSL 证书指纹 (SSL Certificate Fingerprint) （续）																															
	SSL 证书指纹 (SSL Certificate Fingerprint) （续）																															
	SSL 证书指纹 (SSL Certificate Fingerprint) （续）																															
	SSL 策略 ID (SSL Policy ID)																															
	SSL 策略 ID (SSL Policy ID) （续）																															
	SSL 策略 ID (SSL Policy ID) （续）																															
	SSL 策略 ID (SSL Policy ID) （续）																															
	SSL 规则 ID (SSL Rule ID)																															
	SSL 密码套件 (SSL Cipher Suite)																SSL 版本 (SSL Version)								SSL 服务器证书统计信息 (SSL Srv Cert. Stat.)							
	SSL 服务器证书统计信息 (SSL Srv Cert. Stat.) （续）																								SSL 实际操作 (SSL Actual Action)							


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 实际操作 (SSL Actual Action) （续）
SSL 预期操作 (SSL Expected Action)
SSL 流状态 (SSL Flow Status)
SSL 流状态 ((SSL Flow Status)) （续）
SSL 流误差 (SSL Flow Error)
SSL 流误差 (SSL Flow Error) （续）
SSL 流消息 (SSL Flow Messages)
SSL 流消息 (SSL Flow Messages) （续）
SSL 流标志 (SSL Flow Flags)
SSL 流标志 (SSL Flow Flags) （续）
SSL 服务器名称 (SSL Server Names)
SSL 流标志 (SSL Flow Flags) （续）
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0)) （续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length) （续）
SSL 服务器名称 ... (SSL Server Names...)
SSL URL 类别 (SSL URL Category)
SSL 会话 ID (SSL Session ID)
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 会话 ID 长度 (SSL Session ID Length)
SSL 票证 ID (SSL Ticket ID)
SSL 票证 ID (SSL Ticket ID) （续）
SSL 票证 ID (SSL Ticket ID) （续）
SSL 票证 ID (SSL Ticket ID) （续）
SSL 票证 ID (SSL Ticket ID) （续）
SSL 票证 ID (SSL Ticket ID) （续）
SSL 票证 ID 长度 (SSL Ticket ID Length)
网络分析策略修订 (Network Analysis Policy Revision)
网络分析策略修订 (Network Analysis Policy Revision) （续）
网络分析策略修订 (Network Analysis Policy Revision) （续）
网络分析策略修订 (Network Analysis Policy Revision) （续）
网络分析策略修订 (Network Analysis Policy Revision) （续）
终端配置文件 ID (Endpoint Profile ID)
终端配置文件 ID (Endpoint Profile ID) （续）
安全组 ID (Security Group ID)
安全组 ID (Security Group ID) （续）
位置 IPv6 (Location IPv6)
位置 IPv6 (Location IPv6) （续）
位置 IPv6 (Location IPv6) （续）
位置 IPv6 (Location IPv6) （续）
位置 IPv6 (Location IPv6) （续）
HTTP 响应 (HTTP Response)
DNS 查询
HTTP 响应 (HTTP Response) （续）
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0)) （续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length) （续）
DNS 查询 ...(DNS Query...)
DNS 记录类型 (DNS Record Type)
DNS 响应类型 (DNS Response Type)



下表对用于 6.1+ 的连接统计信息数据块的字段进行了说明。

表 B-39 连接统计信息数据块 6.1+ 字段

字段	数据类型	说明
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 6.1.x 的连接统计信息数据块。值始终为 163。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID (Device ID)	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP Address)	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。

表 B-39　连接统计信息数据块 6.1+ 字段 （续）

字段	数据类型	说明
响应方 IP 地址 (Responder IP Address)	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
原始客户端 IP 地址 (Original Client IP Address)	uint8[16]	位于发起请求的代理后面的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号 （如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符 （如适用）。
隧道规则 ID (Tunnel Rule ID)	uint32	触发事件的隧道规则的内部标识符 （如适用）。
规则操作 (Rule Action)	uint16	在用户界面中选择的针对该规则的操作 （允许、阻止等）。
规则原因 (Rule Reason)	uint32	规则触发事件的原因。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址。
实例 ID (Instance ID)	uint16	生成事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的 UNIX 时间戳。
发起方传输的数据包数 (Initiator Transmitted Packets)	uint64	发起主机传输的数据包数。

表 B-39 连接统计信息数据块 6.1+ 字段 （续）

字段	数据类型	说明
响应方传输的数据包数 (Responder Transmitted Packets)	uint64	响应主机传输的数据包数。
发起方传输的字节数 (Initiator Transmitted Bytes)	uint64	发起主机传输的字节数。
响应方传输的字节数 (Responder Transmitted Bytes)	uint64	响应主机传输的字节数。
发起方丢弃的数据包数 (Initiator Packets Dropped)	uint64	由于速率限制而从会话发起方丢弃的数据包的数量。
响应方丢弃的数据包数 (Responder Packets Dropped)	uint64	由于速率限制而从会话响应方丢弃的数据包的数量。
发起方丢弃的字节数 (Initiator Bytes Dropped)	uint64	由于速率限制而从会话发起方丢弃的字节的数量。
响应方丢弃的字节数 (Responder Bytes Dropped)	uint64	由于速率限制而从会话响应方丢弃的字节的数量。
QOS 应用的接口 (QOS Applied Interface)	uint8[16]	对于速率受限的连接，是指应用了速率限制的接口的名称。
QOS 规则 ID (QOS Rule ID)	uint32	应用于连接的服务质量规则的内部 ID 号码 （如适用）。
用户 ID (User ID)	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号 （如适用）。

表 B-39　连接统计信息数据块 6.1+ 字段 （续）

字段	数据类型	说明
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号 （如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的 URL （如适用）（例如， `/files/index.html`）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本 (Client Application Version)	字符串	客户端应用版本。
监控器规则 1 (Monitor Rule 1)	uint32	与连接事件关联的第一个监控器规则的 ID。
监控器规则 2 (Monitor Rule 2)	uint32	与连接事件关联的第二个监控器规则的 ID。
监控器规则 3 (Monitor Rule 3)	uint32	与连接事件关联的第三个监控器规则的 ID。
监控器规则 4 (Monitor Rule 4)	uint32	与连接事件关联的第四个监控器规则的 ID。
监控器规则 5 (Monitor Rule 5)	uint32	与连接事件关联的第五个监控器规则的 ID。
监控器规则 6 (Monitor Rule 6)	uint32	与连接事件关联的第六个监控器规则的 ID。
监控器规则 7 (Monitor Rule 7)	uint32	与连接事件关联的第七个监控器规则的 ID。

表 B-39 连接统计信息数据块 6.1+ 字段 （续）

字段	数据类型	说明
监控器规则 8 (Monitor Rule 8)	uint32	与连接事件关联的第八个监控器规则的 ID。
安全情报源 / 目标 (Security Intelligence Source/ Destination)	uint8	源或目标 IP 地址与 IP 阻止列表是否匹配。
安全情报层 (Security Intelligence Layer)	uint8	与 IP 阻止列表匹配的 IP 层。
文件事件计数 (File Event Count)	uint16	用于区别同一秒发生的文件事件的值。
入侵事件 (Intrusion Event)（续）	uint16	用于区别同一秒发生的入侵事件的值。
发起方国家 / 地区 (Initiator Country)	uint16	发起主机的国家 / 地区代码。
响应方国家 / 地区 (Responder Country)	uint 16	响应主机的国家 / 地区代码。
原始客户端国家 / 地区 (Original Client Country)	uint 16	位于发起请求的代理后面的主机的国家 / 地区的代码。
IOC 编号 (IOC Number)	uint16	与此事件相关的危害的 ID 号码。
源自治系统 (Source Autonomous System)	uint32	作为源或对等体的源自治系统的编号。
目标自治系统 (Destination Autonomous System)	uint32	作为源或对等体的目标自治系统的编号。
SNMP 输入 (SNMP Input)	uint16	输入接口的 SNMP 索引。
SNMP 输出 (SNMP Output)	uint16	输出接口的 SNMP 索引。
源 TOS (Source TOS)	uint8	传入接口的服务字节设置类型。
目标 TOS (Destination TOS)	uint8	传出接口的服务字节设置类型。

表 B-39　连接统计信息数据块 6.1+ 字段 （续）

字段	数据类型	说明
源掩码 (Source Mask)	uint8	源地址前缀掩码。
目标掩码 (Destination Mask)	uint8	目标地址前缀掩码。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景 （虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
字符串块类型 (String Block Type)	uint32	启动包含引用的主机的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	引用的主机字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 引用的主机 ”(Referenced Host) 字段中的字节数。
引用的主机 (Referenced Host)	字符串	HTTP 或 DNS 中提供的主机名信息。
字符串块类型 (String Block Type)	uint32	启动包含用户代理的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户代理字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 用户代理 ”(User Agent) 字段中的字节数。
用户代理 (User Agent)	字符串	会话中用户代理报头字段中的信息。
字符串块类型 (String Block Type)	uint32	启动包含 HTTP 引用站点的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	HTTP 引用站点字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “HTTP 引用站点 ”(HTTP Referrer) 字段中的字节数。
HTTP 引用站点 (HTTP Referrer)	字符串	页面起源的站点。该站点可在 HTTP 流量中引用的报头信息中找到。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 策略 ID (SSL Policy ID)	uint8[16]	处理连接的 SSL 策略的 ID 编号。
SSL 规则 ID (SSL Rule ID)	uint32	处理连接的 SSL 规则或默认操作的 ID 编号。

表 B-39 连接统计信息数据块 6.1+ 字段 （续）

字段	数据类型	说明
SSL 密码套件 (SSL Cipher Suite)	uint16	SSL 连接使用的加密套件。该值以十进制格式存储。有关该值指定的密码套件，请参阅 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml。
SSL 版本 (SSL Version)	uint8	用来加密连接的 SSL 或 TLS 协议版本。
SSL 服务器证书状态 (SSL Server Certificate Status)	uint32	SSL 证书的状态。可能的值包括： • 0 - 未检查 - 服务器证书状态未评估。 • 1 - 未知 - 服务器证书状态无法确定。 • 2 - 有效 - 服务器证书有效。 • 4 - 自签 - 服务器证书已自签。 • 16 - 颁发者无效 - 服务器证书的颁发者无效。 • 32 - 签名无效 - 服务器证书的签名无效。 • 64 - 过期 - 服务器证书已过期。 • 128 - 尚未生效 - 服务器证书尚未生效。 • 256 - 撤销 - 服务器证书已被撤销。
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括： • 0 -‘ 未知 ’ • 1 -‘ 请勿解密 ’ • 2 -‘ 阻止 ’ • 3 -‘ 阻止并重置 ’ • 4 -‘ 解密 （已知密钥） ’ • 5 -‘ 解密 （更换秘钥） ’ • 6 -‘ 解密 （放弃） ’
SSL 预期操作 (SSL Expected Action)	uint16	根据 SSL 规则应该对连接执行的操作。可能的值包括： • 0 -‘ 未知 ’ • 1 -‘ 请勿解密 ’ • 2 -‘ 阻止 ’ • 3 -‘ 阻止并重置 ’ • 4 -‘ 解密 （已知密钥） ’ • 5 -‘ 解密 （更换秘钥） ’ • 6 -‘ 解密 （放弃） ’

表 B-39　连接统计信息数据块 6.1+ 字段 （续）

字段	数据类型	说明
SSL 流状态 (SSL Flow Status)	uint16	SSL 流量的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括： • 0 -‘ 未知 ’ • 1 -‘ 不匹配 ’ • 2 -‘ 成功 ’ • 3 -‘ 非缓存会话 ’ • 4 -‘ 未知密码套件 ’ • 5 -‘ 不受支持的密码套件 ’ • 6 -‘ 不受支持的 SSL 版本 ’ • 7 -‘ 使用的 SSL 压缩 ’ • 8 -‘ 在被动模式中无法解密的会话 ’ • 9 -‘ 握手错误 ’ • 10 -‘ 解密错误 ’ • 11 -‘ 待处理服务器名称分类查找 ’ • 12 -‘ 待处理通用名称分类查找 ’ • 13 -‘ 内部错误 ’ • 14 -‘ 网络参数不可用 ’ • 15 -‘ 服务器证书处理无效 ’ • 16 -‘ 服务器证书指纹不可用 ’ • 17 -‘ 无法缓存持有者 DN’ • 18 -‘ 无法缓存颁发者 DN’ • 19 -‘ 未知 SSL 版本 ’ • 20 -‘ 外部证书列表不可用 ’ • 21 -‘ 外部证书指纹不可用 ’ • 22 -‘ 内部证书列表无效 ’ • 23 -‘ 内部证书列表不可用 ’ • 24 -‘ 内部证书不可用 ’ • 25 -‘ 内部证书指纹不可用 ’ • 26 -‘ 服务器证书验证不可用 ’ • 27 -‘ 服务器证书验证失败 ’ • 28 -‘ 操作无效 ’
SSL 流误差 (SSL Flow Error)	uint32	详细的 SSL 错误代码。这些值可用于提供支持。

表 B-39 连接统计信息数据块 6.1+ 字段 （续）

字段	数据类型	说明
SSL 流消息 (SSL Flow Messages)	uint32	在 SSL 握手期间，客户端和服务器之间交换的消息。有关详细信息，请参阅 http://tools.ietf.org/html/rfc5246。 • 0x00000001 - NSE_MT__HELLO_REQUEST • 0x00000002 - NSE_MT__CLIENT_ALERT • 0x00000004 - NSE_MT__SERVER_ALERT • 0x00000008 - NSE_MT__CLIENT_HELLO • 0x00000010 - NSE_MT__SERVER_HELLO • 0x00000020 - NSE_MT__SERVER_CERTIFICATE • 0x00000040 - NSE_MT__SERVER_KEY_EXCHANGE • 0x00000080 - NSE_MT__CERTIFICATE_REQUEST • 0x00000100 - NSE_MT__SERVER_HELLO_DONE • 0x00000200 - NSE_MT__CLIENT_CERTIFICATE • 0x00000400 - NSE_MT__CLIENT_KEY_EXCHANGE • 0x00000800 - NSE_MT__CERTIFICATE_VERIFY • 0x00001000 - NSE_MT__CLIENT_CHANGE_CIPHER_SPEC • 0x00002000 - NSE_MT__CLIENT_FINISHED • 0x00004000 - NSE_MT__SERVER_CHANGE_CIPHER_SPEC • 0x00008000 - NSE_MT__SERVER_FINISHED • 0x00010000 - NSE_MT__NEW_SESSION_TICKET • 0x00020000 - NSE_MT__HANDSHAKE_OTHER • 0x00040000 - NSE_MT__APP_DATA_FROM_CLIENT • 0x00080000 - NSE_MT__APP_DATA_FROM_SERVER
SSL 流标志 (SSL Flow Flags)	uint64	加密连接的调试级别标志。可能的值包括： • 0x00000001 - NSE_FLOW__VALID - 必须设置此字段，其他字段才有效 • 0x00000002 - NSE_FLOW__INITIALIZED - 内部结构已准备就绪进行处理 • 0x00000004 - NSE_FLOW__INTERCEPT - SSL 会话已被拦截
字符串块类型 (String Block Type)	uint32	启动包含 SSL 服务器名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	SSL 服务器名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “SSL 服务器名称 ”(SSL Server Name) 字段中的字节数。

表 B-39　连接统计信息数据块 6.1+ 字段 （续）

字段	数据类型	说明
SSL 服务器名称 (SSL Server Name)	字符串	在 SSL 客户端欢迎界面中服务器名称显示中提供的名称。
SSL URL 类别 (SSL URL Category)	uint32	根据服务器名称和证书常用名识别的流量类别。
SSL 会话 ID (SSL Session ID)	uint8[32]	当客户端和服务器同意进行会话重用时， SSL 握手期间使用的会话 ID 值
SSL 会话 ID 长度 (SSL Session ID Length)	uint8	SSL 会话 ID 的长度。尽管会话 ID 不能超过 32 个字节，此值可能小于 32 个字节。
SSL 票证 ID (SSL Ticket ID)	uint8[20]	当客户端和服务器同意使用会话票证时使用的会话票证散列。
SSL 票证 ID 长度 (SSL Ticket ID Length)	uint8	SSL 票证 ID 的长度。尽管票证 ID 不能超过 20 个字节，此值可能小于 20 个字节。
网络分析策略修订 (Network Analysis Policy revision)	uint8[16]	与连接事件相关的网络分析策略的修订。
终端配置文件 ID (Endpoint Profile ID)	uint32	ISE 识别的连接终端使用的设备类型的 ID 号码。这是每个 DC 特有的，在元数据中进行解析。
安全组 ID (Security Group ID)	uint32	由 ISE 根据策略分配给用户的 ID 号码。
位置 IPv6 (Location IPv6)	uint8[16]	与 ISE 通信的接口的 IP 地址。可以是 IPv4 或 IPv6。
HTTP 响应 (HTTP Response)	uint32	HTTP 请求的响应代码。
字符串块类型 (String Block Type)	uint32	启动 DNS 查询的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 DNS 查询字符串中的字节数。
DNS 查询 (DNS Query)	字符串	发送到 DNS 服务器的查询的内容。
DNS 记录类型 (DNS Record Type)	uint16	DNS 记录类型的数字值。
DNS 响应类型 (DNS Response Type)	uint16	DNS 响应类型的数字值。

表 B-39 连接统计信息数据块 6.1+ 字段 （续）

字段	数据类型	说明
DNS TTL	uint32	DNS 响应的生存时间 （秒数）
Sinkhole UUID	uin8[16]	与此 sinkhole 对象关联的修订 UUID。
安全情报列表 1 (Security Intelligence List 1)	uint32	与事件关联的安全情报列表。这映射到关联元数据中的安全情报列表。可能存在两个与连接关联的安全情报列表。
安全情报列表 2 (Security Intelligence List 2)	uint32	与事件关联的安全情报列表。这映射到关联元数据中的安全情报列表。可能存在两个与连接关联的安全情报列表。

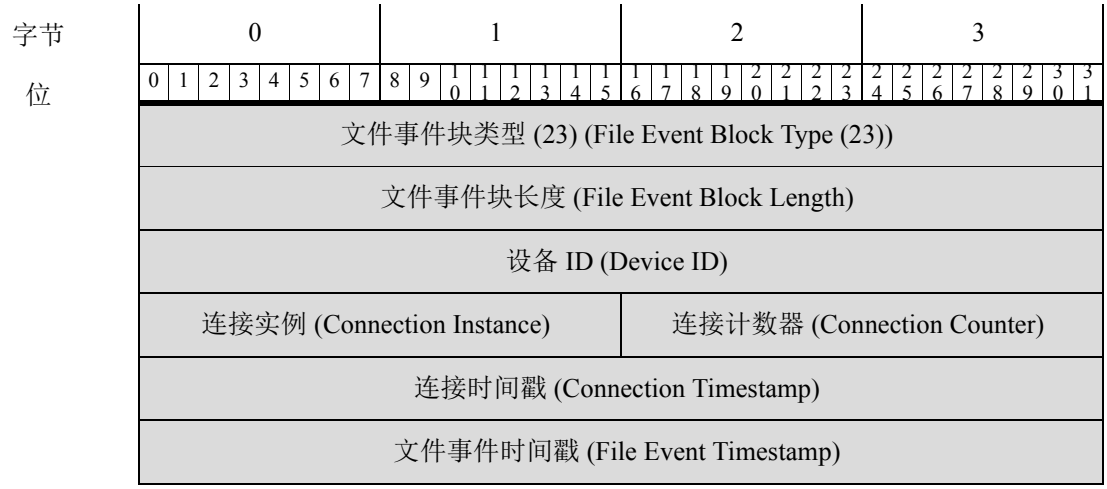
旧版文件事件数据结构

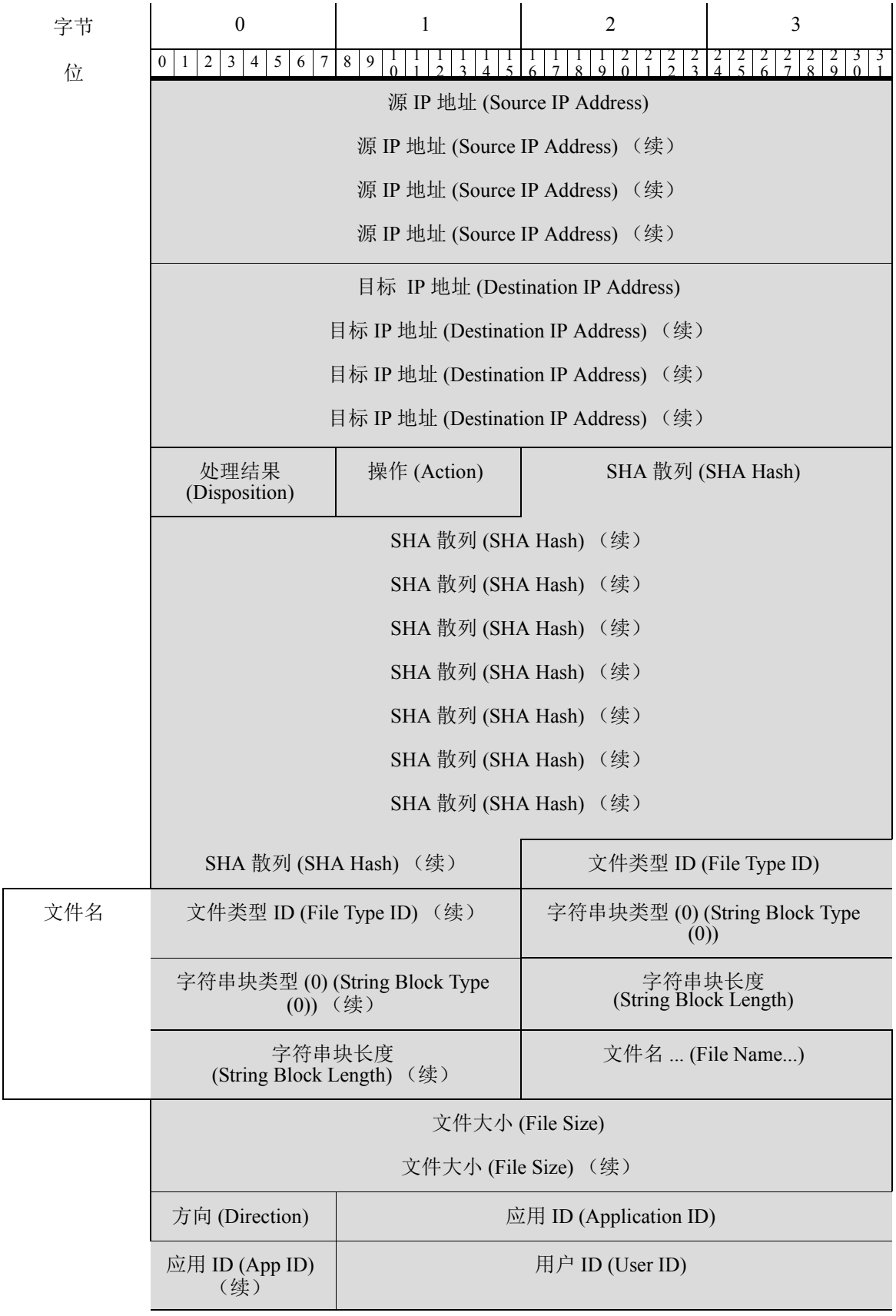
以下主题介绍其他旧版文件事件数据结构：

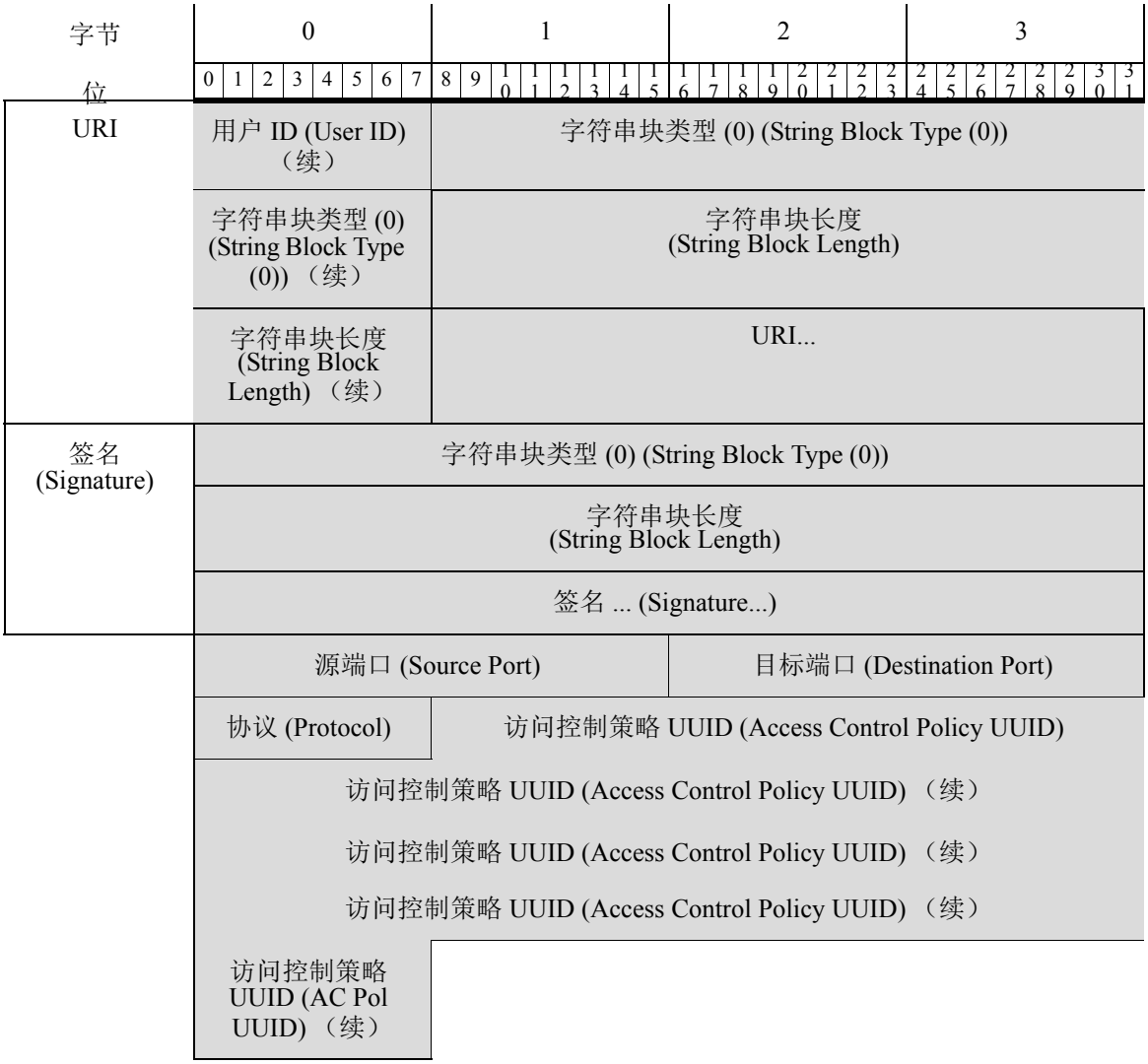
用于 5.1.1.x 的文件事件

该文件事件包含通过网络发送的文件的相关信息。这包括连接信息，文件是否是恶意软件以及用于识别文件的特定信息。文件事件的块类型为系列 2 数据块组中的 23。

下图显示文件事件数据块的结构：




字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
源 IP 地址 (Source IP Address)
源 IP 地址 (Source IP Address) （续）
源 IP 地址 (Source IP Address) （续）
源 IP 地址 (Source IP Address) （续）
目标 IP 地址 (Destination IP Address)
目标 IP 地址 (Destination IP Address) （续）
目标 IP 地址 (Destination IP Address) （续）
目标 IP 地址 (Destination IP Address) （续）
处理结果 (Disposition)
操作 (Action)
SHA 散列 (SHA Hash)
SHA 散列 (SHA Hash) （续）
SHA 散列 (SHA Hash) （续）
SHA 散列 (SHA Hash) （续）
SHA 散列 (SHA Hash) （续）
SHA 散列 (SHA Hash) （续）
SHA 散列 (SHA Hash) （续）
SHA 散列 (SHA Hash) （续）
SHA 散列 (SHA Hash) （续）
文件类型 ID (File Type ID)
文件名
文件类型 ID (File Type ID) （续）
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0)) （续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length) （续）
文件名 ... (File Name...)
文件大小 (File Size)
文件大小 (File Size) （续）
方向 (Direction)
应用 ID (Application ID)
应用 ID (App ID) （续）
用户 ID (User ID)



下表对文件事件数据块中的字段进行了说明：

表 B-40　　文件事件数据块字段

字段	数据类型	说明
文件事件块类型 (File Event Block Type)	uint32	启动文件事件数据块。值始终为 23。
文件事件块长度 (File Event Block Length)	uint32	文件事件块中的字节总数，包括文件事件块类型和长度字段的八个字节，加上随后的数据的字节数。
设备 ID (设备 ID)	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或入侵事件相关联。

表 B-40　　文件事件数据块字段 （续）

字段	数据类型	说明
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接时间戳 (Connection Timestamp)	uint32	相关连接事件的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）。
文件事件时间戳 (File Event Timestamp)	uint32	识别文件类型以及生成文件事件时的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）。
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标 IP 地址 (Destination IP Address)	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括： • 1 - CLEAN - 文件是安全的，不包含恶意软件。 • 2 - UNKNOWN - 不确定文件是否包含恶意软件。 • 3 - MALWARE - 文件包含恶意软件。 • 4 - CACHE_MISS - 软件无法向 Cisco 云发送请求以了解处置情况。 • 5 - NO_CLOUD_RESP - Cisco 云服务未响应此请求。
操作 (Action)	uint8	根据文件类型对文件执行的操作。可以具有以下值： • 1 - 检测 • 2 - 阻止 • 3 - 恶意软件云查找 • 4 - 恶意软件阻止 • 5 - 恶意软件允许列表
SHA 散列 (SHA Hash)	uint8[32]	二进制格式的文件的 SHA-256 散列。
文件类型 ID (File Type ID)	uint32	映射至文件类型的 ID 编号。
文件名 (File Name)	字符串	文件的名称。
文件大小 (File Size)	uint64	文件的大小 （字节数）。

表 B-40 文件事件数据块字段 （续）

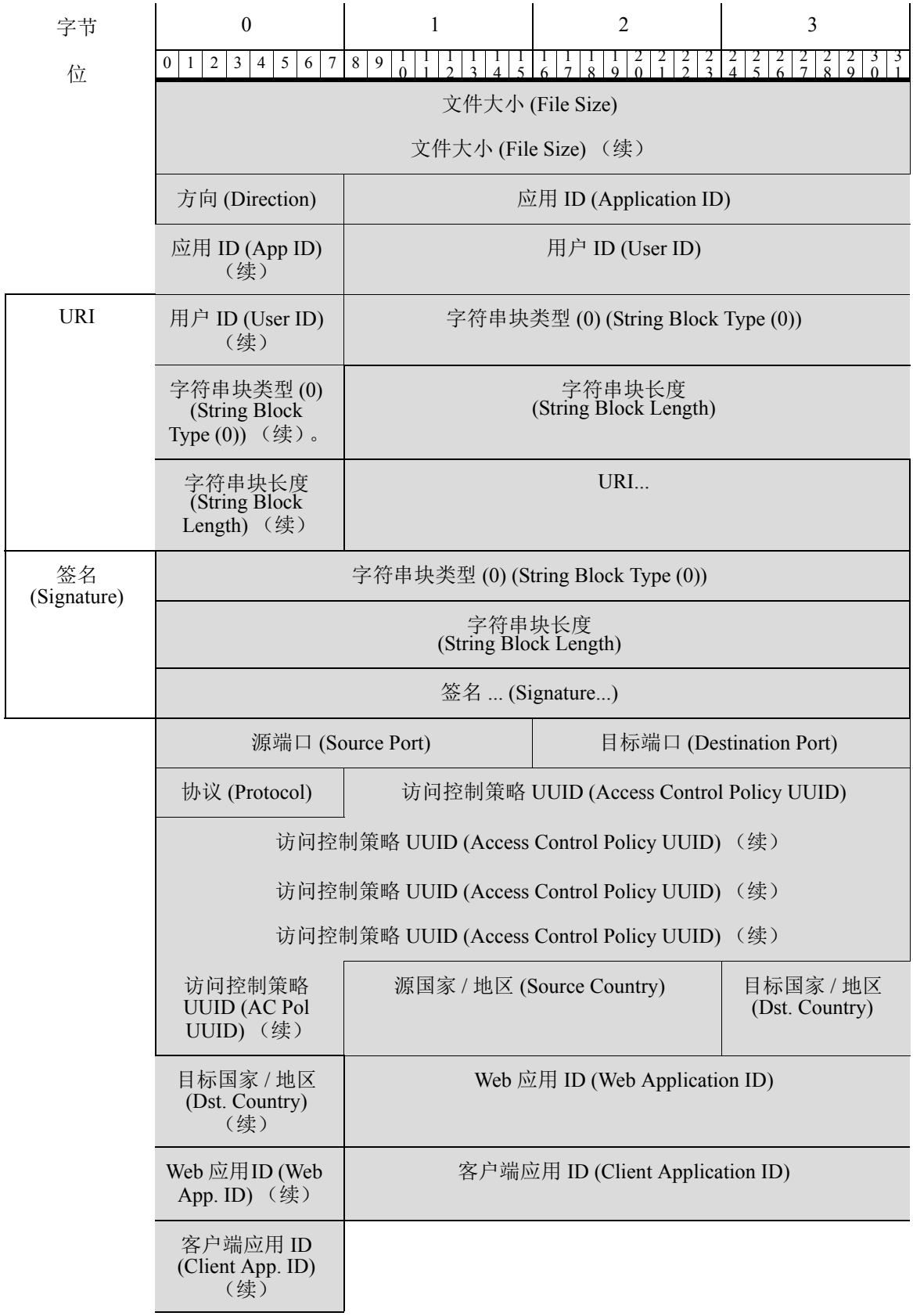
字段	数据类型	说明
方向 (Direction)	uint8	指示是否已上传或下载此文件的值。可能会有以下值： • 1 - 下载 • 2 - 上传 目前该值取决于协议 （例如，如果连接是 HTTP，则其值为 Download）。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。
用户 ID (User ID)	uint32	系统识别的登录目标主机的用户的 ID 号码。
URI	字符串	连接的统一资源标识符 (URI)。
签名 (Signature)	字符串	字符串格式的文件的 SHA-256 散列。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。
协议 (Protocol)	uint8	用户指定的 IANA 协议号。例如： • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP 目前仅限 TCP。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	触发事件的访问控制策略的唯一标识符。

用于 5.2 的文件事件

该文件事件包含通过网络发送的文件的相关信息。这包括连接信息，文件是否是恶意软件以及用于识别文件的特定信息。文件事件的块类型为系列 2 数据块组中的 32。它替代了块类型 23。已添加新字段以跟踪源和目标国家 / 地区以及客户端和 web 应用实例。

下图显示文件事件数据块的结构：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	设备 ID (Device ID)																															
	连接实例 (Connection Instance)																连接计数器 (Connection Counter)															
	连接时间戳 (Connection Timestamp)																															
	文件事件时间戳 (File Event Timestamp)																															
	源 IP 地址 (Source IP Address)																															
	源 IP 地址 (Source IP Address) （续）																															
	源 IP 地址 (Source IP Address) （续）																															
	源 IP 地址 (Source IP Address) （续）																															
	目标 IP 地址 (Destination IP Address)																															
	目标 IP 地址 (Destination IP Address) （续）																															
	目标 IP 地址 (Destination IP Address) （续）																															
	目标 IP 地址 (Destination IP Address) （续）																															
	处理结果 (Disposition)								操作 (Action)								SHA 散列 (SHA Hash)															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																文件类型 ID (File Type ID)															
文件名 (File Name)	文件类型 ID (File Type ID) （续）																字符串块类型 (0) (String Block Type (0))															
	字符串块类型 (0) (String Block Type (0)) （续）																字符串块长度 (String Block Length)															
	字符串块长度 (String Block Length) （续）																文件名 ... (File Name...)															


字节
位
0
1
2
3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
文件大小 (File Size)
文件大小 (File Size) （续）
方向 (Direction)
应用 ID (Application ID)
应用 ID (App ID) （续）
用户 ID (User ID)
URI
用户 ID (User ID) （续）
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0)) （续）。
字符串块长度 (String Block Length)
字符串块长度 (String Block Length) （续）
URI...
签名 (Signature)
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
签名 ... (Signature...)
源端口 (Source Port)
目标端口 (Destination Port)
协议 (Protocol)
访问控制策略 UUID (Access Control Policy UUID)
访问控制策略 UUID (Access Control Policy UUID) （续）
访问控制策略 UUID (Access Control Policy UUID) （续）
访问控制策略 UUID (Access Control Policy UUID) （续）
访问控制策略 UUID (AC Pol UUID) （续）
源国家 / 地区 (Source Country)
目标国家 / 地区 (Dst. Country)
目标国家 / 地区 (Dst. Country) （续）
Web 应用 ID (Web Application ID)
Web 应用ID (Web App. ID) （续）
客户端应用 ID (Client Application ID)
客户端应用 ID (Client App. ID) （续）

下表对文件事件数据块中的字段进行了说明：

表 B-41　　文件事件数据块字段

字段	数据类型	说明
文件事件块类型 (File Event Block Type)	uint32	启动文件事件数据块。值始终为 23。
文件事件块长度 (File Event Block Length)	uint32	文件事件块中的字节总数，包括文件事件块类型和长度字段的八个字节，加上随后的数据的字节数。
设备 ID (Device ID)	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或入侵事件相关联。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接时间戳 (Connection Timestamp)	uint32	相关连接事件的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）。
文件事件时间戳 (File Event Timestamp)	uint32	识别文件类型以及生成文件事件时的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）。
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标 IP 地址 (Destination IP Address)	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括： • 1 - CLEAN - 文件是安全的，不包含恶意软件。 • 2 - NEUTRAL - 不确定文件是否包含恶意软件。 • 3 - MALWARE - 文件包含恶意软件。 • 4 - CACHE_MISS - 软件无法向 Cisco 云发送请求以了解处置情况，或 Cisco 云服务未响应此请求。
操作 (Action)	uint8	根据文件类型对文件执行的操作。可以具有以下值： • 1 - 检测 • 2 - 阻止 • 3 - 恶意软件云查找 • 4 - 恶意软件阻止 • 5 - 恶意软件允许列表
SHA 散列 (SHA Hash)	uint8[32]	二进制格式的文件的 SHA-256 散列。

表 B-41 文件事件数据块字段 （续）

字段	数据类型	说明
文件类型 ID (File Type ID)	uint32	映射至文件类型的 ID 编号。
文件名 (File Name)	字符串	文件的名称。
文件大小 (File Size)	uint64	文件的大小 （字节数）。
方向 (Direction)	uint8	指示是否已上传或下载此文件的值。可能会有以下值： • 1 - 下载 • 2 - 上传 目前该值取决于协议 （例如，如果连接是 HTTP，则其值为 Download）。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。
用户 ID (User ID)	uint32	系统识别的登录目标主机的用户的 ID 号码。
URI	字符串	连接的统一资源标识符 (URI)。
签名 (Signature)	字符串	字符串格式的文件的 SHA-256 散列。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。
协议 (Protocol)	uint8	用户指定的 IANA 协议号。例如： • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP 目前仅限 TCP。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	触发事件的访问控制策略的唯一标识符。
源国家 / 地区 (Source Country)	uint16	源主机的国家 / 地区代码。
目标国家 / 地区 (Destination Country)	uint16	目标主机的国家 / 地区代码。

表 B-41　　文件事件数据块字段 （续）

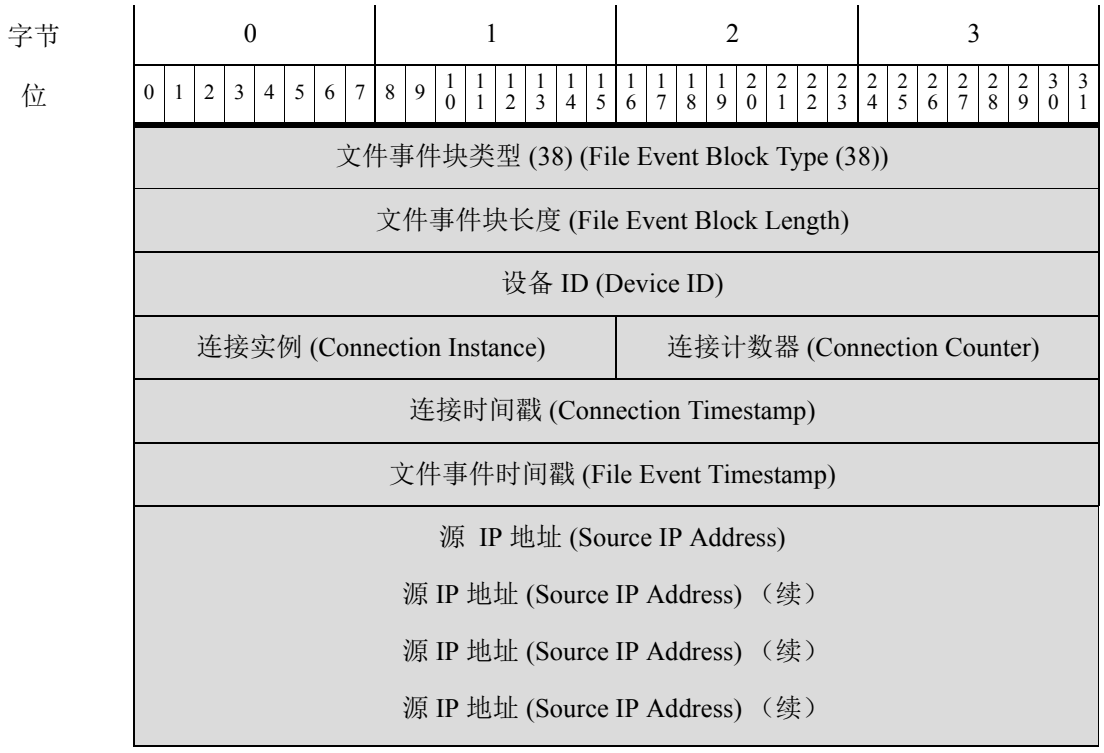
字段	数据类型	说明
Web 应用 ID (Web Application ID)	uint32	Web 应用 （如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用 （如适用）的内部标别号。

用于 5.3 的文件事件

该文件事件包含通过网络发送的文件的相关信息。这包括连接信息，文件是否是恶意软件以及用于识别文件的特定信息。文件事件的块类型为系列 2 数据块组中的 38。它替代了块类型 32。已添加新字段以跟踪动态文件分析和文件存储。

您可以通过在事件版本为 3 且事件代码为 111 的请求消息中设置文件事件标志 （“ 请求标志 ” (Request Flags) 字段中的位 30）请求文件事件记录。请参阅请求标志，第 2-11 页。如果您启用位 23，则记录中会包含扩展事件报头。

下图显示文件事件数据块的结构。



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	目标 IP 地址 (Destination IP Address)																															
	目标 IP 地址 (Destination IP Address) （续）																															
	目标 IP 地址 (Destination IP Address) （续）																															
	目标 IP 地址 (Destination IP Address) （续）																															
	处理结果 (Disposition)								SPERO 处置情况 (SPERO Disposition)								文件存储状态 (File Storage Status)								文件分析状态 (File Analysis Status)							
	存档文件状态 (Archive File Status)								威胁评分 (Threat Score)								操作 (Action)								SHA 散列 (SHA Hash)							
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																								文件类型 ID (File Type ID)							
文件名 (File Name)	文件类型 ID (File Type ID) （续）																								字符串块类型 (0) (String Block Type (0))							
	字符串块类型 (0) (String Block Type (0)) （续）																								字符串块长度 (String Block Length)							
	字符串块长度 (String Block Length) （续）																								文件名 ... (File Name...)							
	文件大小 (File Size)																															
	文件大小 (File Size) （续）																															
	方向 (Direction)								应用 ID (Application ID)																							
	应用 ID (App ID) （续）								用户 ID (User ID)																							

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
URI	用户 ID (User ID)（续）								字符串块类型 (0) (String Block Type (0))																							
	字符串块类型 (0) (String Block Type (0))（续）。								字符串块长度 (String Block Length)																							
	字符串块长度 (String Block Length)（续）								URI...																							
签名 (Signature)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	签名 ... (Signature...)																															
	源端口 (Source Port)																目标端口 (Destination Port)															
	协议 (Protocol)								访问控制策略 UUID (Access Control Policy UUID)																							
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (AC Pol UUID)（续）								源国家 / 地区 (Source Country)																目标国家 / 地区 (Dst. Country)							
	目标国家 / 地区 (Dst. Country)（续）								Web 应用 ID (Web Application ID)																							
	Web 应用ID (Web App. ID)（续）								客户端应用 ID (Client Application ID)																							
	客户端应用 ID (Client App. ID)（续）																															

下表对文件事件数据块中的字段进行了说明。

表 B-42 文件事件数据块字段

字段	数据类型	说明
文件事件块类型 (File Event Block Type)	uint32	启动文件事件数据块。值始终为 23。
文件事件块长度 (File Event Block Length)	uint32	文件事件块中的字节总数，包括文件事件块类型和长度字段的八个字节，加上随后的数据的字节数。
设备 ID (Device ID)	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或入侵事件相关联。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接时间戳 (Connection Timestamp)	uint32	相关连接事件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
文件事件时间戳 (File Event Timestamp)	uint32	识别文件类型以及生成文件事件时的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标 IP 地址 (Destination IP Address)	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括： • 1 - CLEAN 文件是安全的，不包含恶意软件。 • 2 - UNKNOWN 不确定文件是否包含恶意软件。 • 3 - MALWARE 文件包含恶意软件。 • 4 - UNAVAILABLE 软件无法向 Cisco 云发送请求以了解处置情况，或 Cisco 云服务未响应此请求。 • 5 - CUSTOM SIGNATURE 文件与用户定义的散列匹配，并且以用户指定的方式进行处理。
SPERO 处置情况 (SPERO Disposition)	uint8	表示文件分析中是否使用了 SPERO 签名。如果值为 1、2 或 3，则表示使用了 SPERO 分析。如果是任何其他值，则表示未使用 SPERO 分析。

表 B-42　　文件事件数据块字段 （续）

字段	数据类型	说明
文件存储状态 (File Storage Status)	uint8	文件的存储状态。可能的值如下： • 1 - 文件已存储 • 2 - 文件已存储 • 3 - 无法存储文件 • 4 - 无法存储文件 • 5 - 无法存储文件 • 6 - 无法存储文件 • 7 - 无法存储文件 • 8 - 文件太大 • 9 - 文件太小 • 10 - 无法存储文件 • 11 - 文件未存储，无法获取处置情况
文件分析状态 (File Analysis Status)	uint8	是否已发送该文件进行动态分析。可能的值如下： • 0 - 未发送文件进行分析 • 1 - 已发送进行分析 • 2 - 已发送进行分析 • 4 - 已发送进行分析 • 5 - 发送失败 • 6 - 发送失败 • 7 - 发送失败 • 8 - 发送失败 • 9 - 文件太小 • 10 - 文件太大 • 11 - 已发送进行分析 • 12 - 分析完成 • 13 - 故障 （网络问题） • 14 - 故障 （速率限制） • 15 - 故障 （文件太大） • 16 - 故障 （文件读取错误） • 17 - 故障 （内部库错误） • 19 - 文件未发送，无法获取处置情况 • 20 - 故障 （无法运行文件） • 21 - 故障 （分析超时） • 22 - 已发送进行分析 • 23 - 文件不受支持

表 B-42 文件事件数据块字段 （续）

字段	数据类型	说明
存档文件状态 (Archive File Status)	uint8	值始终为 0。
威胁评分 (Threat Score)	uint8	0 到 100 之间的数值，基于在动态分析期间观察到的潜在恶意行为而打出。
操作 (Action)	uint8	根据文件类型对文件执行的操作。可能会有以下值： • 1 - 检测 • 2 - 阻止 • 3 - 恶意软件云查找 • 4 - 恶意软件阻止 • 5 - 恶意软件允许列表
SHA 散列 (SHA Hash)	uint8[32]	二进制格式的文件的 SHA-256 散列。
文件类型 ID (File Type ID)	uint32	映射至文件类型的 ID 编号。此字段的含义在随此事件提供的元数据中传输。有关详细信息，请参阅面向终端的 AMP 文件类型元数据，第 3-39 页。
文件名 (File Name)	字符串	文件的名称。
文件大小 (File Size)	uint64	文件的大小 （字节数）。
方向 (Direction)	uint8	指示是否已上传或下载此文件的值。可能会有以下值： • 1 - 下载 • 2 - 上传 目前该值取决于协议 （例如，如果连接是 HTTP，则其值为 Download）。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。
用户 ID (User ID)	uint32	系统识别的登录目标主机的用户的 ID 号码。
URI	字符串	连接的统一资源标识符 (URI)。
签名 (Signature)	字符串	字符串格式的文件的 SHA-256 散列。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。
协议 (Protocol)	uint8	用户指定的 IANA 协议号。例如： • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP 目前仅限 TCP。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	触发事件的访问控制策略的唯一标识符。

表 B-42　　文件事件数据块字段 （续）

字段	数据类型	说明
源国家 / 地区 (Source Country)	uint16	源主机的国家 / 地区代码。
目标国家 / 地区 (Destination Country)	uint16	目标主机的国家 / 地区代码。
Web 应用 ID (Web Application ID)	uint32	Web 应用 （如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用 （如适用）的内部标别号。

用于 5.3.1 的文件事件

该文件事件包含通过网络发送的文件的相关信息。这包括连接信息，文件是否是恶意软件以及用于识别文件的特定信息。文件事件的块类型为系列 2 数据块组中的 43。它替代了块类型 38。已添加安全情景字段。

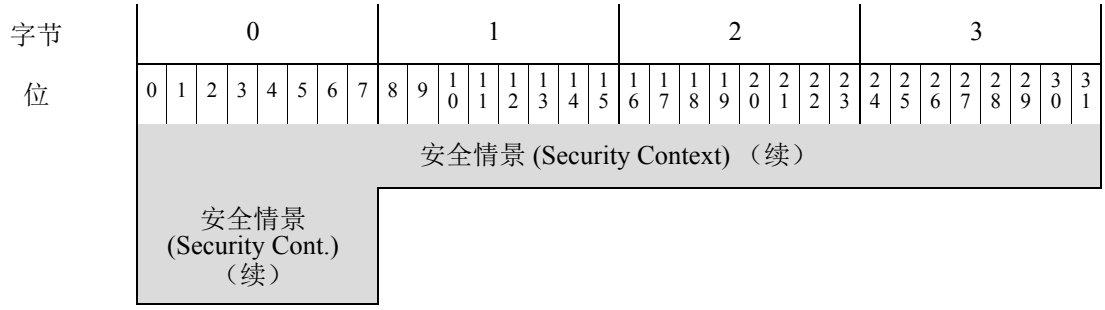
您可以通过在事件版本为 4 且事件代码为 111 的请求消息中设置文件事件标志 （“ 请求标志 ” (Request Flags) 字段中的位 30）请求文件事件记录。请参阅请求标志，第 2-11 页。如果您启用位 23，则记录中会包含扩展事件报头。

下图显示文件事件数据块的结构。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
文件事件块类型 (43) (File Event Block Type (43))																																
文件事件块长度 (File Event Block Length)																																
设备 ID (Device ID)																																
连接实例 (Connection Instance)																	连接计数器 (Connection Counter)														
连接时间戳 (Connection Timestamp)																																
文件事件时间戳 (File Event Timestamp)																																
源 IP 地址 (Source IP Address) 源 IP 地址 (Source IP Address) （续） 源 IP 地址 (Source IP Address) （续） 源 IP 地址 (Source IP Address) （续）																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	目标 IP 地址 (Destination IP Address)																															
	目标 IP 地址 (Destination IP Address) （续）																															
	目标 IP 地址 (Destination IP Address) （续）																															
	目标 IP 地址 (Destination IP Address) （续）																															
	处理结果 (Disposition)								SPERO 处置情况 (SPERO Disposition)								文件存储状态 (File Storage Status)								文件分析状态 (File Analysis Status)							
	存档文件状态 (Archive File Status)								威胁评分 (Threat Score)								操作 (Action)								SHA 散列 (SHA Hash)							
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																								文件类型 ID (File Type ID)							
文件名 (File Name)	文件类型 ID (File Type ID) （续）																								字符串块类型 (0) (String Block Type (0))							
	字符串块类型 (0) (String Block Type (0)) （续）																								字符串块长度 (String Block Length)							
	字符串块长度 (String Block Length) （续）																								文件名 ... (File Name...)							
	文件大小 (File Size)																															
	文件大小 (File Size) （续）																															
	方向 (Direction)								应用 ID (Application ID)																							
	应用 ID (App ID) （续）								用户 ID (User ID)																							

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
URI	用户 ID (User ID) （续）								字符串块类型 (0) (String Block Type (0))																							
	字符串块类型 (0) (String Block Type (0)) （续）。								字符串块长度 (String Block Length)																							
	字符串块长度 (String Block Length) （续）								URI...																							
签名 (Signature)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	签名 ... (Signature...)																															
	源端口 (Source Port)																目标端口 (Destination Port)															
	协议 (Protocol)								访问控制策略 UUID (Access Control Policy UUID)																							
	访问控制策略 UUID (Access Control Policy UUID) （续）																															
	访问控制策略 UUID (Access Control Policy UUID) （续）																															
	访问控制策略 UUID (Access Control Policy UUID) （续）																															
	访问控制策略 UUID (AC Pol UUID) （续）								源国家 / 地区 (Source Country)																目标国家 / 地区 (Dst. Country)							
	目标国家 / 地区 (Dst. Country) （续）								Web 应用 ID (Web Application ID)																							
	Web 应用ID (Web App. ID) （续）								客户端应用 ID (Client Application ID)																							
	客户端应用 ID (Client App. ID) （续）								安全情景 (Security Context)																							
	安全情景 (Security Context) （续）																															
	安全情景 (Security Context) （续）																															



下表对文件事件数据块中的字段进行了说明。

表 B-43 文件事件数据块字段

字段	数据类型	说明
文件事件块类型 (File Event Block Type)	uint32	启动文件事件数据块。值始终为 43。
文件事件块长度 (File Event Block Length)	uint32	文件事件块中的字节总数，包括文件事件块类型和长度字段的八个字节，加上随后的数据的字节数。
设备 ID (Device ID)	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或入侵事件相关联。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接时间戳 (Connection Timestamp)	uint32	相关连接事件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
文件事件时间戳 (File Event Timestamp)	uint32	识别文件类型以及生成文件事件时的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标 IP 地址 (Destination IP Address)	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括： • 1 - CLEAN 文件是安全的，不包含恶意软件。 • 2 - UNKNOWN 不确定文件是否包含恶意软件。 • 3 - MALWARE 文件包含恶意软件。 • 4 - UNAVAILABLE 软件无法向 Cisco 云发送请求以了解处置情况，或 Cisco 云服务未响应此请求。 • 5 - CUSTOM SIGNATURE 文件与用户定义的散列匹配，并且以用户指定的方式进行处理。
SPERO 处置情况 (SPERO Disposition)	uint8	表示文件分析中是否使用了 SPERO 签名。如果值为 1、2 或 3，则表示使用了 SPERO 分析。如果是任何其他值，则表示未使用 SPERO 分析。

表 B-43　　文件事件数据块字段 （续）

字段	数据类型	说明
文件存储状态 (File Storage Status)	uint8	文件的存储状态。可能的值如下： • 1 - 文件已存储 • 2 - 文件已存储 • 3 - 无法存储文件 • 4 - 无法存储文件 • 5 - 无法存储文件 • 6 - 无法存储文件 • 7 - 无法存储文件 • 8 - 文件太大 • 9 - 文件太小 • 10 - 无法存储文件 • 11 - 文件未存储，无法获取处置情况

表 B-43 文件事件数据块字段 （续）

字段	数据类型	说明
文件分析状态 (File Analysis Status)	uint8	是否已发送该文件进行动态分析。可能的值如下： • 0 - 未发送文件进行分析 • 1 - 已发送进行分析 • 2 - 已发送进行分析 • 4 - 已发送进行分析 • 5 - 发送失败 • 6 - 发送失败 • 7 - 发送失败 • 8 - 发送失败 • 9 - 文件太小 • 10 - 文件太大 • 11 - 已发送进行分析 • 12 - 分析完成 • 13 - 故障 （网络问题） • 14 - 故障 （速率限制） • 15 - 故障 （文件太大） • 16 - 故障 （文件读取错误） • 17 - 故障 （内部库错误） • 19 - 文件未发送，无法获取处置情况 • 20 - 故障 （无法运行文件） • 21 - 故障 （分析超时） • 22 - 已发送进行分析 • 23 - 文件不受支持 • 23 - 文件传输文件容量已处理 - 由于无法将文件提交到沙盒进行分析而导致文件容量已处理 （存储到传感器上） • 25 - 文件传输服务器限制超出容量已处理 - 服务器上的速率限制导致文件容量已处理 • 26 - 通信故障 - 云连接故障导致文件容量已处理 • 27 - 未发送 - 因配置原因导致文件未发送 • 28 - 预分类不匹配 - 未发送文件进行动态分析，因为预分类在文件中未找到任何嵌入式或可疑对象 • 29 - 传输已发送沙盒私有云 - 已将文件发送到私有云进行动态分析 • 30 - 传输未发送沙盒私有云 - 未将文件发送到私有云进行分析

表 B-43　文件事件数据块字段 （续）

字段	数据类型	说明
存档文件状态 (Archive File Status)	uint8	值始终为 0。
威胁评分 (Threat Score)	uint8	0 到 100 之间的数值，基于在动态分析期间观察到的潜在恶意行为而打出。
操作 (Action)	uint8	根据文件类型对文件执行的操作。可能会有以下值： • 1 - 检测 • 2 - 阻止 • 3 - 恶意软件云查找 • 4 - 恶意软件阻止 • 5 - 恶意软件允许列表
SHA 散列 (SHA Hash)	uint8[32]	二进制格式的文件的 SHA-256 散列。
文件类型 ID (File Type ID)	uint32	映射至文件类型的 ID 编号。此字段的含义在随此事件提供的元数据中传输。有关详细信息，请参阅面向终端的 AMP 文件类型元数据，第 3-39 页。
文件名 (File Name)	字符串	文件的名称。
文件大小 (File Size)	uint64	文件的大小 （字节数）。
方向 (Direction)	uint8	指示是否已上传或下载此文件的值。可能会有以下值： • 1 - 下载 • 2 - 上传 目前该值取决于协议 （例如，如果连接是 HTTP，则其值为 Download）。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。
用户 ID (User ID)	uint32	系统识别的登录目标主机的用户的 ID 号码。
URI	字符串	连接的统一资源标识符 (URI)。
签名 (Signature)	字符串	字符串格式的文件的 SHA-256 散列。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。
协议 (Protocol)	uint8	用户指定的 IANA 协议号。例如： • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP 目前仅限 TCP。

表 B-43 文件事件数据块字段 （续）

字段	数据类型	说明
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	触发事件的访问控制策略的唯一标识符。
源国家 / 地区 (Source Country)	uint16	源主机的国家 / 地区代码。
目标国家 / 地区 (Destination Country)	uint16	目标主机的国家 / 地区代码。
Web 应用 ID (Web Application ID)	uint32	Web 应用 （如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用 （如适用）的内部标别号。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景 （虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。

用于 5.4 的文件事件

该文件事件包含通过网络发送的文件的相关信息。这包括连接信息，文件是否是恶意软件以及用于识别文件的特定信息。文件事件的块类型为系列 2 数据块组中的 46。它替代了块类型 43。已添加用于 SSL 和文件存档支持的字段。

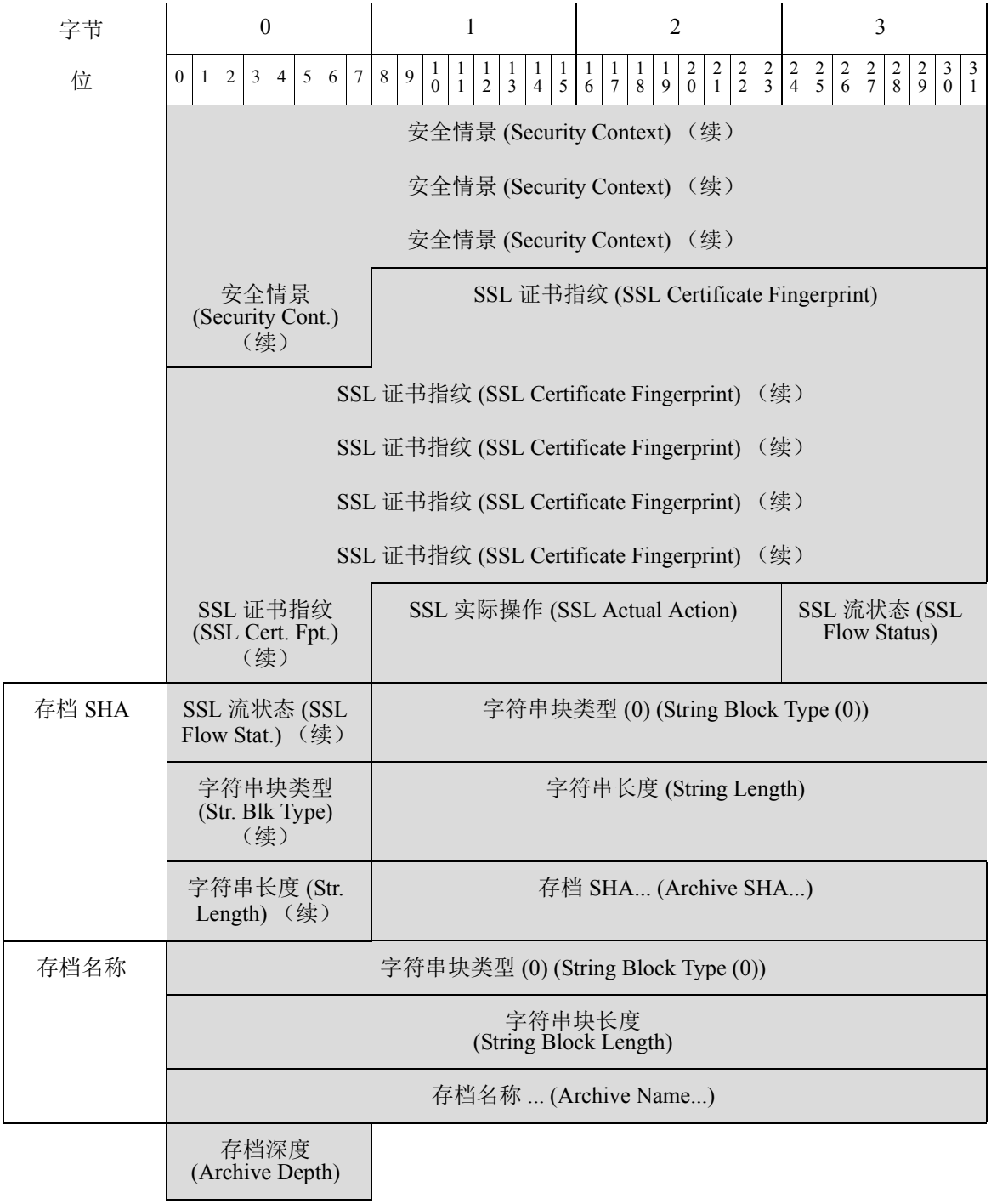
您可以通过在事件版本为 5 且事件代码为 111 的请求消息中设置文件事件标志 （“ 请求标志 ” (Request Flags) 字段中的位 30）请求文件事件记录。请参阅请求标志，第 2-11 页。如果您启用位 23，则记录中会包含扩展事件报头。

下图显示文件事件数据块的结构。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
文件事件块类型 (46) (File Event Block Type (46))																																
文件事件块长度 (File Event Block Length)																																
设备 ID (Device ID)																																
连接实例 (Connection Instance)																	连接计数器 (Connection Counter)														
连接时间戳 (Connection Timestamp)																																
文件事件时间戳 (File Event Timestamp)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	源 IP 地址 (Source IP Address)																															
	源 IP 地址 (Source IP Address) （续）																															
	源 IP 地址 (Source IP Address) （续）																															
	源 IP 地址 (Source IP Address) （续）																															
	目标 IP 地址 (Destination IP Address)																															
	目标 IP 地址 (Destination IP Address) （续）																															
	目标 IP 地址 (Destination IP Address) （续）																															
	目标 IP 地址 (Destination IP Address) （续）																															
	处理结果 (Disposition)								SPERO 处置情况 (SPERO Disposition)								文件存储状态 (File Storage Status)								文件分析状态 (File Analysis Status)							
	存档文件状态 (Archive File Status)								威胁评分 (Threat Score)								操作 (Action)								SHA 散列 (SHA Hash)							
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																								文件类型 ID (File Type ID)							
文件名 (File Name)	文件类型 ID (File Type ID) （续）																								字符串块类型 (0) (String Block Type (0))							
	字符串块类型 (0) (String Block Type (0)) （续）																								字符串块长度 (String Block Length)							
	字符串块长度 (String Block Length) （续）																								文件名 ... (File Name...)							

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	文件大小 (File Size)																															
	文件大小 (File Size) （续）																															
	方向 (Direction)								应用 ID (Application ID)																							
	应用 ID (App ID) （续）								用户 ID (User ID)																							
URI	用户 ID (User ID) （续）								字符串块类型 (0) (String Block Type (0))																							
	字符串块类型 (0) (String Block Type (0)) （续）。								字符串块长度 (String Block Length)																							
	字符串块长度 (String Block Length) （续）								URI...																							
签名 (Signature)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	签名 ... (Signature...)																															
	源端口 (Source Port)																目标端口 (Destination Port)															
	协议 (Protocol)								访问控制策略 UUID (Access Control Policy UUID)																							
	访问控制策略 UUID (Access Control Policy UUID) （续）																															
	访问控制策略 UUID (Access Control Policy UUID) （续）																															
	访问控制策略 UUID (Access Control Policy UUID) （续）																															
	访问控制策略 UUID (AC Pol UUID) （续）								源国家 / 地区 (Source Country)																目标国家 / 地区 (Dst. Country)							
	目标国家 / 地区 (Dst. Country) （续）								Web 应用 ID (Web Application ID)																							
	Web 应用ID (Web App. ID) （续）								客户端应用 ID (Client Application ID)																							
	客户端应用 ID (Client App. ID) （续）								安全情景 (Security Context)																							



下表对文件事件数据块中的字段进行了说明。

表 B-44 用于 5.4.x 的文件事件数据块字段

字段	数据类型	说明
文件事件块类型 (File Event Block Type)	uint32	启动文件事件数据块。值始终为 46。
文件事件块长度 (File Event Block Length)	uint32	文件事件块中的字节总数，包括文件事件块类型和长度字段的八个字节，加上随后的数据的字节数。
设备 ID (Device ID)	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或入侵事件相关联。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接时间戳 (Connection Timestamp)	uint32	相关连接事件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
文件事件时间戳 (File Event Timestamp)	uint32	识别文件类型以及生成文件事件时的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标 IP 地址 (Destination IP Address)	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括： • 1 - CLEAN 文件是安全的，不包含恶意软件。 • 2 - UNKNOWN 不确定文件是否包含恶意软件。 • 3 - MALWARE 文件包含恶意软件。 • 4 - UNAVAILABLE 软件无法向 云发送请求以了解 （续）情况，或 云服务 （续）响应此请求。 • 5 - CUSTOM SIGNATURE 文件与用户定义的散列匹配，并且以用户指定的方式进行处理。
SPERO 处置情况 (SPERO Disposition)	uint8	表示文件分析中是否使用了 SPERO 签名。如果值为 1、2 或 3，则表示使用了 SPERO 分析。如果是任何其他值，则表示未使用 SPERO 分析。

表 B-44　用于 5.4.x 的文件事件数据块字段 （续）

字段	数据类型	说明
文件存储状态 (File Storage Status)	uint8	文件的存储状态。可能的值如下： • 1 - 文件已存储 • 2 - 文件已存储 • 3 - 无法存储文件 • 4 - 无法存储文件 • 5 - 无法存储文件 • 6 - 无法存储文件 • 7 - 无法存储文件 • 8 - 文件太大 • 9 - 文件太小 • 10 - 无法存储文件 • 11 - 文件未存储，无法获取处置情况
文件分析状态 (File Analysis Status)	uint8	是否已发送该文件进行动态分析。可能的值如下： • 0 - 未发送文件进行分析 • 1 - 已发送进行分析 • 2 - 已发送进行分析 • 4 - 已发送进行分析 • 5 - 发送失败 • 6 - 发送失败 • 7 - 发送失败 • 8 - 发送失败 • 9 - 文件太小 • 10 - 文件太大 • 11 - 已发送进行分析 • 12 - 分析完成 • 13 - 故障 （网络问题） • 14 - 故障 （速率限制） • 15 - 故障 （文件太大） • 16 - 故障 （文件读取错误） • 17 - 故障 （内部库错误） • 19 - 文件未发送，无法获取处置情况 • 20 - 故障 （无法运行文件） • 21 - 故障 （分析超时） • 22 - 已发送进行分析 • 23 - 文件不受支持

表 B-44 用于 5.4.x 的文件事件数据块字段 （续）

字段	数据类型	说明
存档文件状态 (Archive File Status)	uint8	正在被检测的存档的状态。可能会有以下值： • 0 - 不适用 - 文件没有被作为存档进行检测 • 1 - 待处理 - 正在检测存档 • 2 - 提取 - 已成功检测，且无任何问题 • 3 - 失败 - 检测失败，系统资源不足 • 4 - 超出深度 - 成功，但存档超出了嵌套的检测深度 • 5 - 加密 - 部分成功，存档已加密或包含加密的存档 • 6 - 无法检出 - 部分成功，文件可能已变形或损坏
威胁评分 (Threat Score)	uint8	0 到 100 之间的数值，基于在动态分析期间观察到的潜在恶意行为而打出。
操作 (Action)	uint8	根据文件类型对文件执行的操作。可能会有以下值： • 1 - 检测 • 2 - 阻止 • 3 - 恶意软件云查找 • 4 - 恶意软件阻止 • 5 - 恶意软件允许列表 • 6 - 云查找超时 • 7 - 自定义检测 • 8 - 自定义检测阻止 • 9 - 存档阻止 （超出深度） • 10 - 存档阻止 （已加密） • 11 - 存档阻止 （检查失败）
SHA 散列 (SHA Hash)	uint8[32]	二进制格式的文件的 SHA-256 散列。
文件类型 ID (File Type ID)	uint32	映射至文件类型的 ID 编号。此字段的含义在随此事件提供的元数据中传输。有关详细信息，请参阅面向终端的 AMP 文件类型元数据，第 3-39 页。
文件名 (File Name)	字符串	文件的名称。
文件大小 (File Size)	uint64	文件的大小 （字节数）。
方向 (Direction)	uint8	指示是否已上传或下载此文件的值。可能会有以下值： • 1 - 下载 • 2 - 上传 目前该值取决于协议 （例如，如果连接是 HTTP，则其值为 Download）。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。

表 B-44　　用于 5.4.x 的文件事件数据块字段 （续）

字段	数据类型	说明
用户 ID (User ID)	uint32	系统识别的登录目标主机的用户的 ID 号码。
URI	字符串	连接的统一资源标识符 (URI)。
签名 (Signature)	字符串	字符串格式的文件的 SHA-256 散列。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。
协议 (Protocol)	uint8	用户指定的 IANA 协议号。例如： • 1 - ICMP • 4 - IP • 6 - TCP • 17 - UDP 目前仅限 TCP。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	触发事件的访问控制策略的唯一标识符。
源国家 / 地区 (Source Country)	uint16	源主机的国家 / 地区代码。
目标国家 / 地区 (Destination Country)	uint16	目标主机的国家 / 地区代码。
Web 应用 ID (Web Application ID)	uint32	Web 应用 （如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用 （如适用）的内部标别号。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景 （虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括： • 0 -‘ 未知 ’ • 1 -‘ 请勿解密 ’ • 2 -‘ 阻止 ’ • 3 -‘ 阻止并重置 ’ • 4 -‘ 解密 （已知密钥） ’ • 5 -‘ 解密 （更换秘钥） ’ • 6 -‘ 解密 （放弃） ’

表 B-44 用于 5.4.x 的文件事件数据块字段 （续）

字段	数据类型	说明
SSL 流状态 (SSL Flow Status)	uint16	SSL 流的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括： • 0 -‘ 未知 ’ • 1 -‘ 不匹配 ’ • 2 -‘ 成功 ’ • 3 -‘ 非缓存会话 ’ • 4 -‘ 未知密码套件 ’ • 5 -‘ 不受支持的密码套件 ’ • 6 -‘ 不受支持的 SSL 版本 ’ • 7 -‘ 使用的 SSL 压缩 ’ • 8 -‘ 在被动模式中无法解密的会话 ’ • 9 -‘ 握手错误 ’ • 10 -‘ 解密错误 ’ • 11 -‘ 待处理服务器名称分类查找 ’ • 12 -‘ 待处理通用名称分类查找 ’ • 13 -‘ 内部错误 ’ • 14 -‘ 网络参数不可用 ’ • 15 -‘ 服务器证书处理无效 ’ • 16 -‘ 服务器证书指纹不可用 ’ • 17 -‘ 无法缓存持有者 DN’ • 18 -‘ 无法缓存颁发者 DN’ • 19 -‘ 未知 SSL 版本 ’ • 20 -‘ 外部证书列表不可用 ’ • 21 -‘ 外部证书指纹不可用 ’ • 22 -‘ 内部证书列表无效 ’ • 23 -‘ 内部证书列表不可用 ’ • 24 -‘ 内部证书不可用 ’ • 25 -‘ 内部证书指纹不可用 ’ • 26 -‘ 服务器证书验证不可用 ’ • 27 -‘ 服务器证书验证失败 ’ • 28 -‘ 操作无效 ’
字符串块类型 (String Block Type)	uint32	启动包含存档 SHA 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	存档 SHA 字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上入侵策略名称中的字节数。

表 B-44　　用于 5.4.x 的文件事件数据块字段 （续）

字段	数据类型	说明
存档 SHA (Archive SHA)	字符串	包含该文件的父存档的 SHA1 散列。
字符串块类型 (String Block Type)	uint32	启动包含 “ 存档名称 ”(Archive Name) 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	存档名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上入侵策略名称中的字节数。
存档名称 (Archive Name)	字符串	父存档的名称。
存档深度 (Archive Depth)	uint8	嵌套文件的层数。例如，如果文本文件位于压缩存档中，则此值为 1。

用于 5.1.1-5.2.x 的文件事件 SHA 散列

eStreamer 服务使用文件事件 SHA 散列数据块以包含文件的 SHA 散列到其文件名的映射的元数据。块类型为系列 2 数据块列表中的 26。如果已在扩展请求中请求文件日志事件 （事件代码为 111）且已设置位 20 或已请求元数据 （事件版本为 4，事件代码为 21），则可以请求它。

下图显示文件事件散列数据块的结构：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	文件事件 SHA 散列块类型 (26) (File Event SHA Hash Block Type (26))																															
	文件事件 SHA 散列块长度 (File Event SHA Hash Block Length)																															
	SHA 散列 (SHA Hash)																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
	SHA 散列 (SHA Hash) （续）																															
文件名 (File Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件名或处置情况 ... (File Name or Disposition...)																															

下表对文件事件 SHA 散列数据块中的字段进行了说明。

表 B-45 文件事件 SHA 散列 5.1.1 - 5.2.x 数据块字段

字段	数据类型	说明
文件事件 SHA 散列块类型 (File Event SHA Hash Block Type)	uint32	启动文件事件 SHA 散列块。值始终为 `26`。
文件事件 SHA 散列块长度 (File Event SHA Hash Block Length)	uint32	文件事件 SHA 散列块中的字节总数，包括文件事件 SHA 散列块类型和长度字段的八个字节，加上随后的数据的字节数。
SHA 散列 (SHA Hash)	uint8[32]	二进制格式的文件的 SHA-256 散列。
字符串块类型 (String Block Type)	uint32	启动包含与文件相关的描述性名称的字符串数据块。值始终为 `0`。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 名称 ”(Name) 字段中的字节数。
文件名或处置情况 (File Name or Disposition)	字符串	文件的描述性名称或处置情况。如果文件是安全的，则值为 `Clean`。如果文件的处置情况未知，则值为 `Neutral`。如果文件包含恶意软件，则提供文件名。

旧版关联事件数据结构

以下主题介绍其他旧版关联 （合规性）数据结构：

- 用于 5.0 - 5.0.2 的关联事件，第 B-282 页
- 用于 5.1-5.3.x 的关联事件，第 B-290 页

用于 5.0 - 5.0.2 的关联事件

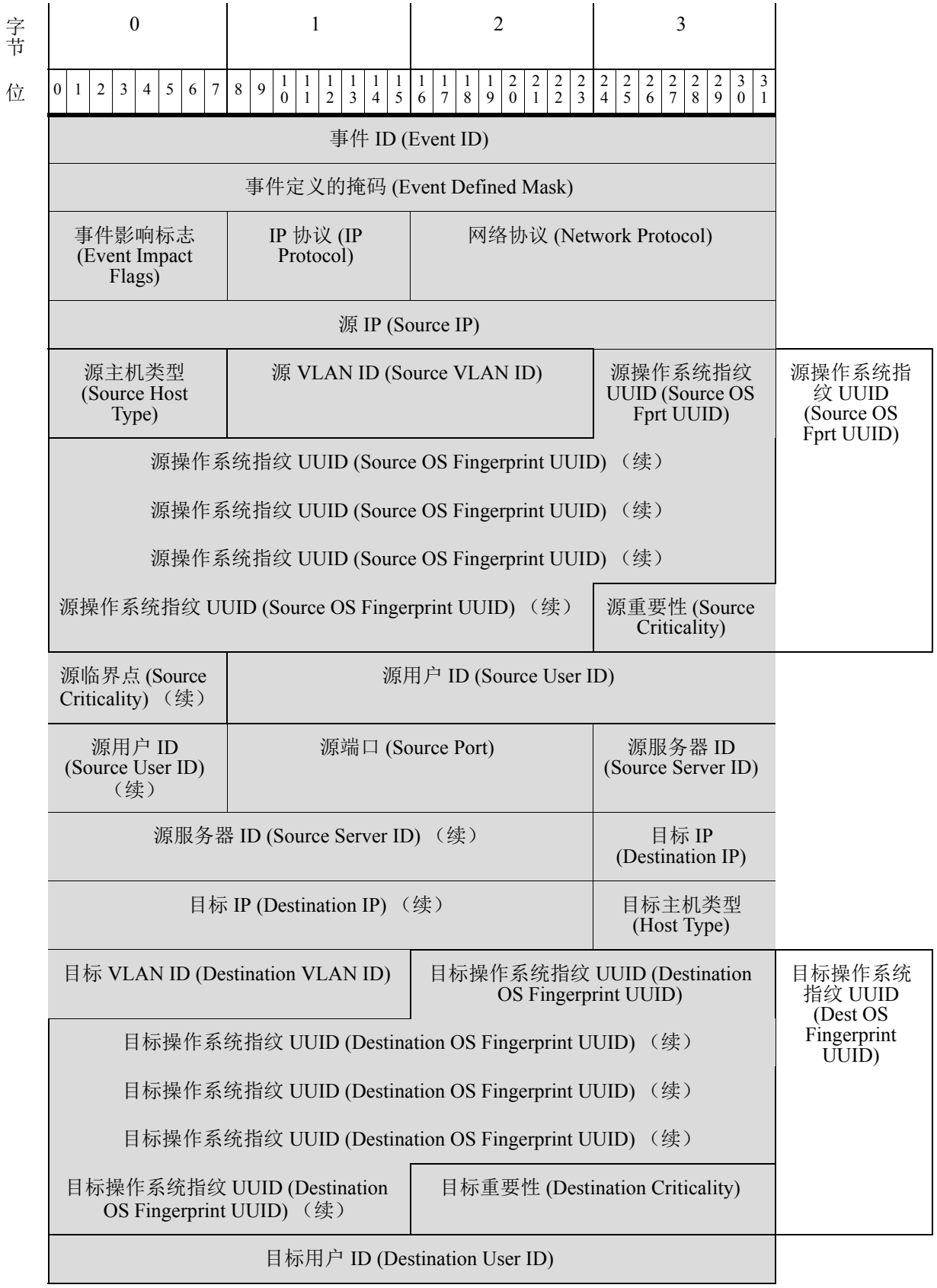
关联事件 （在 5.0 之前的版本中称为合规性事件）包含关联策略违规的相关信息。此消息使用标准 eStreamer 消息报头并指定记录类型为 112，随后是类型为 116 的关联数据块。数据块类型 116 与其前身 （块类型 107）的区别在于，其包含关联安全区和接口的其他相关信息。

只有通过扩展请求，才能从 eStreamer 请求 5.0 关联事件，要提交扩展请求，您需要在流请求消息中请求事件类型代码 31 和版本代码 7（请参阅提交扩展请求，第 2-4 页了解有关提交扩展请求的信息）。您可以选择启用初始事件流请求消息的标志字段中的位 23，以包含扩展事件报头。您也可以启用标志字段中的位 20，以包含用户元数据。

请注意，记录结构包含一个字符串块类型，该数据块为系列 1 中的数据块。有关系列 1 数据块的信息，请参阅了解发现 （系列 1）块，第 4-63 页。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (112) （Record Type (112))															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp) （在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use) （在事件中，只有当位 23 已设置时）																																
关联块类型 (116) (Correlation Block Type (116))																																
关联块长度 (Correlation Block Length)																																
设备 ID (Device ID)																																
（关联）事件秒 ((Correlation) Event Second)																																
事件 ID (Event ID)																																
策略 ID (Policy ID)																																
规则 ID (Rule ID)																																
优先级 (Priority)																																
字符串块类型 (0) (String Block Type (0))																																
字符串块长度 (String Block Length)																																
说明 ... (Description...)																									事件类型 (Event Type)							
事件设备 ID (Event 设备 ID)																																
签名 ID (Signature ID)																																
签名生成器 ID (Signature Generator ID)																																
（触发器）事件秒 ((Trigger) Event Second)																																
（触发器）事件微秒 ((Trigger) Event Microsecond)																																

事件说明


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
事件 ID (Event ID)
事件定义的掩码 (Event Defined Mask)
事件影响标志 (Event Impact Flags)
IP 协议 (IP Protocol)
网络协议 (Network Protocol)
源 IP (Source IP)
源主机类型 (Source Host Type)
源 VLAN ID (Source VLAN ID)
源操作系统指纹 UUID (Source OS Fprt UUID)
源操作系统指纹 UUID (Source OS Fprt UUID)
源操作系统指纹 UUID (Source OS Fingerprint UUID) （续）
源操作系统指纹 UUID (Source OS Fingerprint UUID) （续）
源操作系统指纹 UUID (Source OS Fingerprint UUID) （续）
源操作系统指纹 UUID (Source OS Fingerprint UUID) （续）
源重要性 (Source Criticality)
源临界点 (Source Criticality) （续）
源用户 ID (Source User ID)
源用户 ID (Source User ID) （续）
源端口 (Source Port)
源服务器 ID (Source Server ID)
源服务器 ID (Source Server ID) （续）
目标 IP (Destination IP)
目标 IP (Destination IP) （续）
目标主机类型 (Host Type)
目标 VLAN ID (Destination VLAN ID)
目标操作系统指纹 UUID (Destination OS Fingerprint UUID)
目标操作系统指纹 UUID (Dest OS Fingerprint UUID)
目标操作系统指纹 UUID (Destination OS Fingerprint UUID) （续）
目标操作系统指纹 UUID (Destination OS Fingerprint UUID) （续）
目标操作系统指纹 UUID (Destination OS Fingerprint UUID) （续）
目标操作系统指纹 UUID (Destination OS Fingerprint UUID) （续）
目标重要性 (Destination Criticality)
目标用户 ID (Destination User ID)

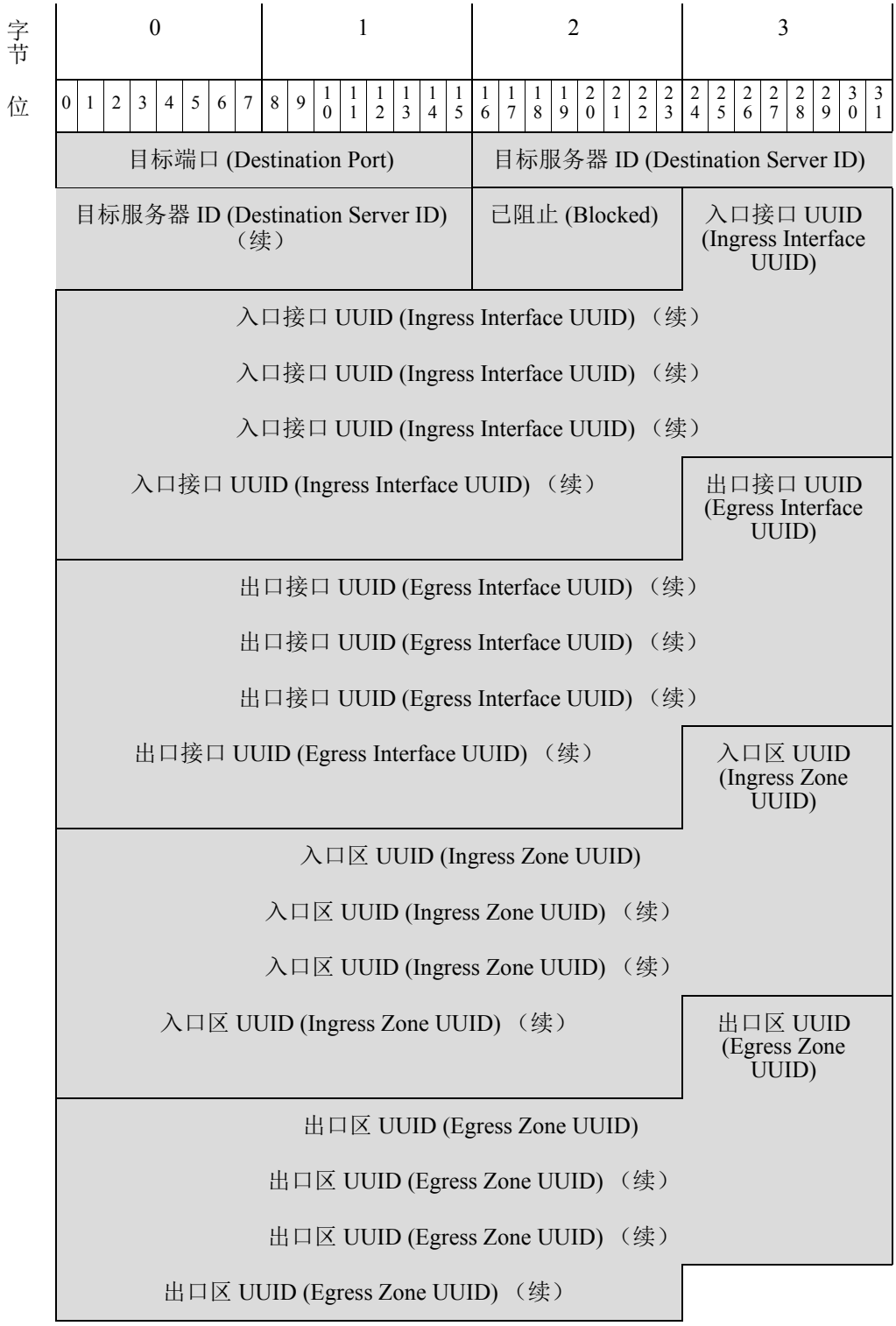

字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
目标端口 (Destination Port)
目标服务器 ID (Destination Server ID)
目标服务器 ID (Destination Server ID) （续）
已阻止 (Blocked)
入口接口 UUID (Ingress Interface UUID)
入口接口 UUID (Ingress Interface UUID) （续）
入口接口 UUID (Ingress Interface UUID) （续）
入口接口 UUID (Ingress Interface UUID) （续）
入口接口 UUID (Ingress Interface UUID) （续）
出口接口 UUID (Egress Interface UUID)
出口接口 UUID (Egress Interface UUID) （续）
出口接口 UUID (Egress Interface UUID) （续）
出口接口 UUID (Egress Interface UUID) （续）
出口接口 UUID (Egress Interface UUID) （续）
入口区 UUID (Ingress Zone UUID)
入口区 UUID (Ingress Zone UUID)
入口区 UUID (Ingress Zone UUID) （续）
入口区 UUID (Ingress Zone UUID) （续）
入口区 UUID (Ingress Zone UUID) （续）
出口区 UUID (Egress Zone UUID)
出口区 UUID (Egress Zone UUID)
出口区 UUID (Egress Zone UUID) （续）
出口区 UUID (Egress Zone UUID) （续）
出口区 UUID (Egress Zone UUID) （续）

表 B-46 关联事件 5.0 - 5.0.2 数据字段

字段	数据类型	说明
关联块类型 (Correlation Block Type)	uint32	表示随后的关联事件数据块。此字段的值始终为 107。请参阅了解发现 （系列 1）块，第 4-63 页。
关联块长度 (Correlation Block Length)	uint32	关联数据块的长度，包括关联块类型和长度的 8 个字节加上随后的关联数据。
设备 ID (Device ID)	uint32	生成关联事件的受管设备或防御中心的内部识别号。值 0 表示防御中心。您可以通过请求版本 3 元数据获取受管设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
（关联）事件秒 ((Correlation) Event Second)	uint32	表示生成关联事件的时间的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）。
事件 ID (Event ID)	uint32	关联事件标识号。
策略 ID (Policy ID)	uint32	违反的关联策略的标识号。有关如何从数据库获取策略标识号的信息，请参阅服务记录，第 4-14 页。
规则 ID (Rule ID)	uint32	触发策略违规事件的关联规则的标识号。有关如何从数据库获取策略标识号的信息，请参阅服务记录，第 4-14 页。
优先级 (Priority)	uint32	分配给事件的优先级。该项是从 0 到 5 的整数值。
字符串块类型 (String Block Type)	uint32	启动包含关联违规事件说明的字符串数据块。此值始终设置为 0。有关字符串块的详细信息，请参阅字符串数据块，第 4-70 页。
字符串块长度 (String Block Length)	uint32	事件说明字符串块中的字节数，包括字符串块类型的四个字节，字符串块长度的四个字节加上说明中的字节数。
说明 (Description)	字符串	关联事件的说明。
事件类型 (Event Type)	uint8	表示关联事件是由入侵事件、主机发现事件还是用户事件触发的： • 1 - 入侵 • 2 - 主机发现 • 3 - 用户
事件 ID (Event 设备 ID)	uint32	生成触发关联事件的事件的设备的标识号。您可以通过请求版本 3 元数据获取设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
签名 ID (Signature ID)	uint32	如果事件为入侵事件，则表示与事件对应的规则识别号。否则，该值为 0。
签名生成器 ID (Signature Generator ID)	uint32	如果事件为入侵事件，则表示生成事件的 Firepower 系统预处理器或规则引擎的 ID 号码。

表 B-46　关联事件 5.0 - 5.0.2 数据字段 （续）

字段	数据类型	说明
（触发器）事件秒 ((Trigger) Event Second)	uint32	表示事件触发关联策略规则的时间的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）
（触发器）事件微秒 ((Trigger) Event Microsecond)	uint32	检测到事件的微秒 （一秒的百万分之一）增量。
事件 ID (Event ID)	uint32	设备生成的事件的标识号。
事件定义的掩码 (Event Defined Mask)	bits[32]	此字段中的设置位表示后面消息中哪些是有效的字段。有关每个位值的列表，请参阅表 B-47 在第 B-290 页。
事件影响标志 (Event Impact Flags)	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括： • `0x01` （位 0） - 源或目标主机位于系统监控的网络中。 • `0x02` （位 1） - 源或目标主机存在于网络映射中。 • `0x04` （位 2） - 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使用 IP 协议。 • `0x08` （位 3） - 有漏洞映射到事件中的源或目标主机的操作系统。 • `0x10` （位 4） - 有漏洞映射到事件中检测到的服务器。 • `0x20` （位 5） - 事件导致受管设备丢弃会话 （仅当设备在内联、交换或路由式部署中运行时才使用）。对应于 Firepower 系统 Web 界面中的受阻状态。 • `0x40` （位 6） - 生成了此事件的规则包含将影响标志设置为红色的规则元数据 （位 6）。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 • `0x80` （位 7） - 有漏洞映射到事件中检测到的客户端。 以下影响级别值映射到 “ 防御中心 ”(Defense Center) 上的特定优先级中。 `x` 表示值可以为 0 或 1： • （0，未知）：`00X00000` • 红色 （1，易受攻击）：`XXXX1XXX`、`XXX1XXXX`、`X1XXXXXX`、`1XXXXXXX` • 橙色 （2，可能易受攻击）：`00X00111` • 黄色 （3，当前不易受攻击）：`00X00011` • 蓝色 （4，未知目标）：`00X00001`
IP 协议 (IP Protocol)	uint8	与事件关联的 IP 协议的标识符 （如适用）。
网络协议 (Network Protocol)	uint16	与事件关联的网络协议 （如适用）。

表 B-46 关联事件 5.0 - 5.0.2 数据字段 （续）

字段	数据类型	说明
源 IP (Source IP)	uint8[4]	事件中源主机的 IP 地址，采用 IP 地址八位组。
源主机类型 (Source Host Type)	uint8	源主机的类型： • 0 - 主机 • 1 - 路由器 • 2 - 网桥
源 VLAN ID (Source VLAN ID)	uint16	源主机的 VLAN 标识号 （如适用）。
源操作系统指纹 UUID (Source OS Fingerprint UUID)	uint8[16]	充当源主机操作系统的唯一标识符的指纹 ID 号码。 有关获取映射到指纹 ID 的值的信息，请参阅服务记录，第 4-14 页。
源重要性 (Source Criticality)	uint16	源主机的用户定义临界值： • 0 - 无 • 1 - 低 • 2 - 中 • 3 - 高
源用户 ID (Source User ID)	uint32	系统识别的登录源主机的用户的标识号。
源端口 (Source Port)	uint16	事件中的源端口。
源服务器 ID (Source Server ID)	uint32	源主机上运行的服务器的标识号。
目标 IP 地址 (Destination IP Address)	uint8[4]	与策略违规相关的目标主机的 IP 地址 （如适用）。如果无目标 IP 地址，则此值为 0。
目标主机类型 (Destination Host Type)	uint8	目标主机的类型： • 0 - 主机 • 1 - 路由器 • 2 - 网桥
目标 VLAN ID (Destination VLAN ID)	uint16	目标主机的 VLAN 标识号 （如适用）。

表 B-46　关联事件 5.0 - 5.0.2 数据字段 （续）

字段	数据类型	说明
目标操作系统指纹 UUID (Destination OS Fingerprint UUID)	uint8[16]	充当目标主机操作系统的唯一标识符的指纹 ID 号码。 有关获取映射到指纹 ID 的值的信息，请参阅服务记录，第 4-14 页。
目标重要性 (Destination Criticality)	uint16	目标主机的用户定义临界值： • 0 - 无 • 1 - 低 • 2 - 中 • 3 - 高
目标用户 ID (Destination User ID)	uint32	系统识别的登录目标主机的用户的标识号。
目标端口 (Destination Port)	uint16	事件中的目标端口。
目标服务 ID (Destination Service ID)	uint32	源主机上运行的服务器的标识号。
已阻止 (Blocked)	uint8	表示触发入侵事件的数据包发生了什么情况的值。 • 0 - 未丢弃入侵事件 • 1 - 已丢弃入侵事件 （当部署为内联、交换或路由式部署时丢弃） • 2 - 如果已向在内联、交换或路由式部署中配置的设备应用入侵策略，则触发事件的数据包本应已丢弃。
入口接口 UUID (Ingress Interface UUID)	uint8[16]	充当与关联事件相关的入口接口的唯一标识符的接口 ID。
出口接口 UUID (Egress Interface UUID)	uint8[16]	充当与关联事件相关的出口接口的唯一标识符的接口 ID。
入口区 UUID (Ingress Zone UUID)	uint8[16]	充当与关联事件相关的入口安全区的唯一标识符的区域 ID。
出口区 UUID (Egress Zone UUID)	uint8[16]	充当与关联事件相关的出口安全区的唯一标识符的区域 ID。

下表对每个事件定义的掩码值进行了说明。

表 B-47 事件定义的值

说明	掩码值
事件影响标志 (Event Impact Flags)	0x00000001
IP 协议 (IP Protocol)	0x00000002
网络协议 (Network Protocol)	0x00000004
源 IP (Source IP)	0x00000008
源主机类型 (Source Host Type)	0x00000010
源 VLAN ID (Source VLAN ID)	0x00000020
源指纹 ID (Source Fingerprint ID)	0x00000040
源临界点 (Source Criticality)	0x00000080
源端口 (Source Port)	0x00000100
源服务器 (Source Server)	0x00000200
目标 IP (Destination IP)	0x00000400
目标主机类型 (Destination Host Type)	0x00000800
目标 VLAN ID (Destination VLAN ID)	0x00001000
目标指纹 ID (Destination Fingerprint ID)	0x00002000
目标临界点 (Destination Criticality)	0x00004000
目标端口 (Destination Port)	0x00008000
目标服务器 (Destination Server)	0x00010000
源用户 (Source User)	0x00020000
目标用户 (Destination User)	0x00040000

用于 5.1-5.3.x 的关联事件

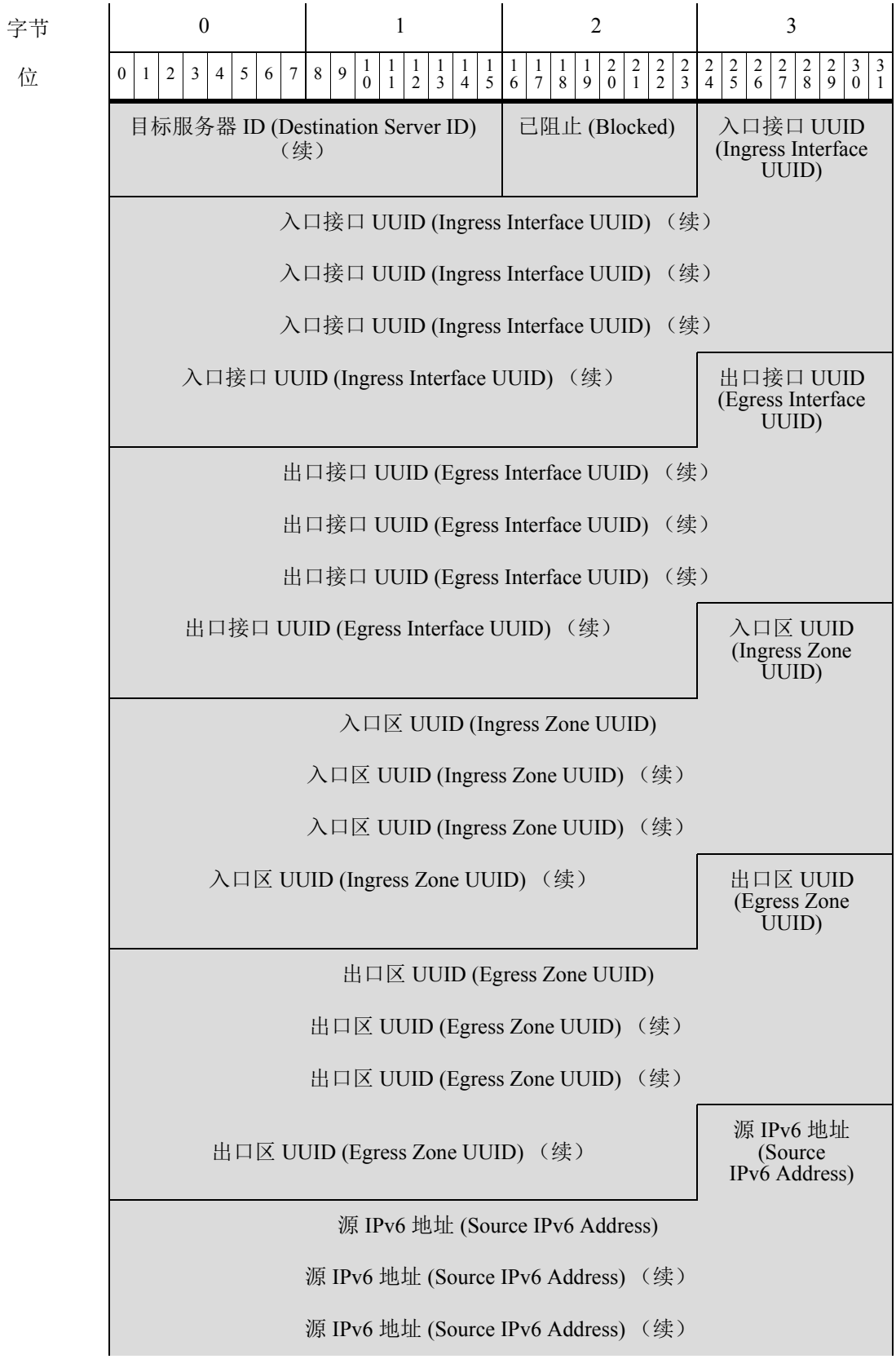
关联事件 （在 5.0 之前的版本中称为合规性事件）包含关联策略违规的相关信息。此消息使用标准 eStreamer 消息报头并指定记录类型为 112，随后是类型为系列 1 数据块组中的 128 的关联数据块。数据块类型 128 与其前身 （块类型 116）的区别在于其包含 IPv6 支持。

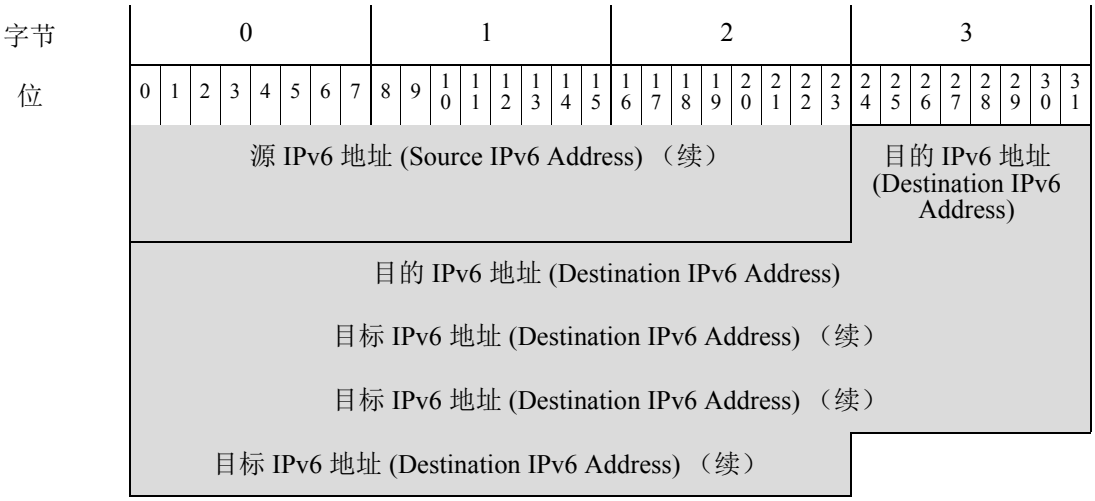
您可以通过扩展请求，仅从 eStreamer 请求 5.1-5.3.x 关联事件，为此，您需要在流请求消息中请求事件类型代码 31 和版本代码 8 （有关提交扩展请求的信息，请参阅提交扩展请求，第 2-4 页）。您可以选择启用初始事件流请求消息的标志字段中的位 23，以包含扩展事件报头。您也可以启用标志字段中的位 20，以包含用户元数据。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (112) （Record Type (112))															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp) （在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use) （在事件中，只有当位 23 已设置时）																																
关联块类型 (128) (Correlation Block Type (128))																																
关联块长度 (Correlation Block Length)																																
设备 ID (Device ID)																																
（关联）事件秒 ((Correlation) Event Second)																																
事件 ID (Event ID)																																
策略 ID (Policy ID)																																
规则 ID (Rule ID)																																
优先级 (Priority)																																
字符串块类型 (0) (String Block Type (0))																																
字符串块长度 (String Block Length)																																
说明 ... (Description...)																									事件类型 (Event Type)							
事件设备 ID (Event Device ID)																																
签名 ID (Signature ID)																																
签名生成器 ID (Signature Generator ID)																																
（触发器）事件秒 ((Trigger) Event Second)																																
（触发器）事件微秒 ((Trigger) Event Microsecond)																																
事件 ID (Event ID)																																

事件说明


字节
位
0
1
2
3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
事件定义的掩码 (Event Defined Mask)
事件影响标志 (Event Impact Flags)
IP 协议 (IP Protocol)
网络协议 (Network Protocol)
源 IP (Source IP)
源主机类型 (Source Host Type)
源 VLAN ID (Source VLAN ID)
源操作系统指纹 UUID (Source OS Fprt UUID)
源操作系统指纹 UUID (Source OS Fprt UUID)
源操作系统指纹 UUID (Source OS Fingerprint UUID) （续）
源操作系统指纹 UUID (Source OS Fingerprint UUID) （续）
源操作系统指纹 UUID (Source OS Fingerprint UUID) （续）
源操作系统指纹 UUID (Source OS Fingerprint UUID) （续）
源重要性 (Source Criticality)
源临界点 (Source Criticality) （续）
源用户 ID (Source User ID)
源用户 ID (Source User ID) （续）
源端口 (Source Port)
源服务器 ID (Source Server ID)
源服务器 ID (Source Server ID) （续）
目标 IP (Destination IP)
目标 IP (Destination IP) （续）
目标主机类型 (Host Type)
目标 VLAN ID (Destination VLAN ID)
目标操作系统指纹 UUID (Destination OS Fingerprint UUID)
目标操作系统指纹 UUID (Dest OS Fingerprint UUID)
目标操作系统指纹 UUID (Destination OS Fingerprint UUID) （续）
目标操作系统指纹 UUID (Destination OS Fingerprint UUID) （续）
目标操作系统指纹 UUID (Destination OS Fingerprint UUID) （续）
目标操作系统指纹 UUID (Destination OS Fingerprint UUID) （续）
目标重要性 (Destination Criticality)
目标用户 ID (Destination User ID)
目标端口 (Destination Port)
目标服务器 ID (Destination Server ID)


字节
位
0
1
2
3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
目标服务器 ID (Destination Server ID)（续）
已阻止 (Blocked)
入口接口 UUID (Ingress Interface UUID)
入口接口 UUID (Ingress Interface UUID)（续）
入口接口 UUID (Ingress Interface UUID)（续）
入口接口 UUID (Ingress Interface UUID)（续）
入口接口 UUID (Ingress Interface UUID)（续）
出口接口 UUID (Egress Interface UUID)
出口接口 UUID (Egress Interface UUID)（续）
出口接口 UUID (Egress Interface UUID)（续）
出口接口 UUID (Egress Interface UUID)（续）
出口接口 UUID (Egress Interface UUID)（续）
入口区 UUID (Ingress Zone UUID)
入口区 UUID (Ingress Zone UUID)
入口区 UUID (Ingress Zone UUID)（续）
入口区 UUID (Ingress Zone UUID)（续）
入口区 UUID (Ingress Zone UUID)（续）
出口区 UUID (Egress Zone UUID)
出口区 UUID (Egress Zone UUID)
出口区 UUID (Egress Zone UUID)（续）
出口区 UUID (Egress Zone UUID)（续）
出口区 UUID (Egress Zone UUID)（续）
源 IPv6 地址 (Source IPv6 Address)
源 IPv6 地址 (Source IPv6 Address)
源 IPv6 地址 (Source IPv6 Address)（续）
源 IPv6 地址 (Source IPv6 Address)（续）
源 IPv6 地址 (Source IPv6 Address)（续）



请注意，记录结构包含一个字符串块类型，该数据块为系列 1 中的数据块。有关系列 1 数据块的信息，请参阅了解发现 （系列 1）块，第 4-63 页。

表 B-48 关联事件 5.1-5.3.x 数据字段

字段	数据类型	说明
关联块类型 (Correlation Block Type)	uint32	表示随后的关联事件数据块。此字段的值始终为 128。请参阅了解发现 （系列 1）块，第 4-63 页。
关联块长度 (Correlation Block Length)	uint32	关联数据块的长度，包括关联块类型和长度的 8 个字节加上随后的关联数据。
设备 ID (Device ID)	uint32	生成关联事件的受管设备或防御中心的内部识别号。值 0 表示防御中心。您可以通过请求版本 3 元数据获取受管设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
（关联）事件秒 ((Correlation) Event Second)	uint32	表示生成关联事件的时间的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）。
事件 ID (Event ID)	uint32	关联事件标识号。
策略 ID (Policy ID)	uint32	违反的关联策略的标识号。有关如何从数据库获取策略标识号的信息，请参阅服务记录，第 4-14 页。
规则 ID (Rule ID)	uint32	触发策略违规事件的关联规则的标识号。有关如何从数据库获取策略标识号的信息，请参阅服务记录，第 4-14 页。
优先级 (Priority)	uint32	分配给事件的优先级。该项是从 0 到 5 的整数值。
字符串块类型 (String Block Type)	uint32	启动包含关联违规事件说明的字符串数据块。此值始终设置为 0。有关字符串块的详细信息，请参阅字符串数据块，第 4-70 页。
字符串块长度 (String Block Length)	uint32	事件说明字符串块中的字节数，包括字符串块类型的四个字节，字符串块长度的四个字节加上说明中的字节数。

表 B-48　关联事件 5.1-5.3.x 数据字段 （续）

字段	数据类型	说明
说明 (Description)	字符串	关联事件的说明。
事件类型 (Event Type)	uint8	表示关联事件是由入侵事件、主机发现事件还是用户事件触发的： • 1 - 入侵 • 2 - 主机发现 • 3 - 用户
事件设备 ID (Event Device ID)	uint32	生成触发关联事件的事件的设备的标识号。您可以通过请求版本 3 元数据获取设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
签名 ID (Signature ID)	uint32	如果事件为入侵事件，则表示与事件对应的规则识别号。否则，该值为 0。
签名生成器 ID (Signature Generator ID)	uint32	如果事件为入侵事件，则表示生成的 预处理器或规则引擎的 ID 号码。
（触发器）事件秒 ((Trigger) Event Second)	uint32	表示事件触发关联策略规则的时间的 UNIX 时间戳（自 1970/01/01 起经过的秒数）
（触发器）事件微秒 ((Trigger) Event Microsecond)	uint32	检测到事件的微秒 （一秒的百万分之一）增量。
事件 ID (Event ID)	uint32	设备 Cisco 生成的事件的标识号。
事件定义的掩码 (Event Defined Mask)	bits[32]	此字段中的设置位表示后面消息中哪些是有效的字段。有关每个位值的列表，请参阅表 B-47 在第 B-290 页。

表 B-48 关联事件 5.1-5.3.x 数据字段 （续）

字段	数据类型	说明
事件影响标志 (Event Impact Flags)	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括： • 0x01 （位 0） - 源或目标主机位于系统监控的网络中。 • 0x02 （位 1） - 源或目标主机存在于网络映射中。 • 0x04 （位 2） - 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使 用 IP 协议。 • 0x08 （位 3） - 有漏洞映射到事件中的源或目标主机的操作系统。 • 0x10 （位 4） - 有漏洞映射到事件中检测到的服务器。 • 0x20 （位 5） - 事件导致受管设备丢弃会话 （仅当设备在内联、交换或路由式部署中运行时才使用）。对应于 Firepower 系统 Web 界面中的受阻状态。 • 0x40 （位 6） - 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 • 0x80 （位 7） - 有漏洞映射到事件中检测到的客户端。（仅限版本 5.0+） 以下影响级别值映射到 “ 防御中心 ”(Defense Center) 上的特定优先级中。 x 表示值可以为 0 或 1： • （0，未知）：`00X00000` • 红色 （1，易受攻击）：`XXXX1XXX`、`XXX1XXXX`、`X1XXXXXX`、`1XXXXXXX` （仅限版本 5.0+） • 橙色 （2，可能易受攻击）：`00X0011X` • 黄色 （3，当前不易受攻击）：`00X0001X` • 蓝色 （4，未知目标）：`00X00001`
IP 协议 (IP Protocol)	uint8	与事件关联的 IP 协议的标识符 （如适用）。
网络协议 (Network Protocol)	uint16	与事件关联的网络协议 （如适用）。
源 IP 地址 (Source IP Address)	uint8[4]	保留此字段，但不再填充。源 IPv4 地址存储在源 IPv6 地址字段中。 有关详细信息，请参阅 IP 地址，第 1-3 页。
源主机类型 (Source Host Type)	uint8	源主机的类型： • 0 - 主机 • 1 - 路由器 • 2 - 网桥
源 VLAN ID (Source VLAN ID)	uint16	源主机的 VLAN 标识号 （如适用）。

表 B-48　关联事件 5.1-5.3.x 数据字段 （续）

字段	数据类型	说明
源操作系统指纹 UUID (Source OS Fingerprint UUID)	uint8[16]	充当源主机操作系统的唯一标识符的指纹 ID 号码。 有关获取映射到指纹 ID 的值的信息，请参阅服务记录，第 4-14 页。
源重要性 (Source Criticality)	uint16	源主机的用户定义临界值： • 0 - 无 • 1 - 低 • 2 - 中 • 3 - 高
源用户 ID (Source User ID)	uint32	系统识别的登录源主机的用户的标识号。
源端口 (Source Port)	uint16	事件中的源端口。
源服务器 ID (Source Server ID)	uint32	源主机上运行的服务器的标识号。
目标 IP 地址 (Destination IP Address)	uint8[4]	保留此字段，但不再填充。目标 IPv4 地址存储在目标 IPv6 地址字段中。有关详细信息，请参阅 IP 地址，第 1-3 页。
目标主机类型 (Destination Host Type)	uint8	目标主机的类型： • 0 - 主机 • 1 - 路由器 • 2 - 网桥
目标 VLAN ID (Destination VLAN ID)	uint16	目标主机的 VLAN 标识号 （如适用）。
目标操作系统指纹 UUID (Destination OS Fingerprint UUID)	uint8[16]	充当目标主机操作系统的唯一标识符的指纹 ID 号码。 有关获取映射到指纹 ID 的值的信息，请参阅服务记录，第 4-14 页。
目标重要性 (Destination Criticality)	uint16	目标主机的用户定义临界值： • 0 - 无 • 1 - 低 • 2 - 中 • 3 - 高
目标用户 ID (Destination User ID)	uint32	系统识别的登录目标主机的用户的标识号。

表 B-48 关联事件 5.1-5.3.x 数据字段 （续）

字段	数据类型	说明
目标端口 (Destination Port)	uint16	事件中的目标端口。
目标服务 ID (Destination Service ID)	uint32	源主机上运行的服务器的标识号。
已阻止 (Blocked)	uint8	表示触发入侵事件的数据包发生了什么情况的值。 • 0 - 未丢弃入侵事件 • 1 - 已丢弃入侵事件 （当部署为内联、交换或路由式部署时丢弃） • 2 - 如果已向在内联、交换或路由式部署中配置的设备应用入侵策略，则触发事件的数据包本应已丢弃。
入口接口 UUID (Ingress Interface UUID)	uint8[16]	充当与关联事件相关的入口接口的唯一标识符的接口 ID。
出口接口 UUID (Egress Interface UUID)	uint8[16]	充当与关联事件相关的出口接口的唯一标识符的接口 ID。
入口区 UUID (Ingress Zone UUID)	uint8[16]	充当与关联事件相关的入口安全区的唯一标识符的区域 ID。
出口区 UUID (Egress Zone UUID)	uint8[16]	充当与关联事件相关的出口安全区的唯一标识符的区域 ID。
源 IPv6 地址 (Source IPv6 Address)	uint8[16]	事件中源主机的 IP 地址，采用 IPv6 地址八位组。
目的 IPv6 地址 (Destination IPv6 Address)	uint8[16]	事件中目标主机的 IP 地址，采用 IPv6 地址八位组。

旧版主机数据结构

要请求这些结构，必须使用主机请求消息。要请求旧版结构，主机请求消息必须使用较旧的格式。有关详细信息，请参阅主机请求消息格式，第 2-24 页。

以下主题介绍旧版主机数据结构，包括主机配置文件结构和完整主机配置文件结构：

- 访问控制策略规则原因数据块，第 B-341 页

完整主机配置文件数据块 5.0 - 5.0.2

用于版本 5.0 - 5.0.2 的完整主机配置文件数据块包含一整套主机说明数据。其格式如下图中所示，并在下表中进行说明。请注意，除列表数据块之外，该图未显示封装数据块的字段。这些封装数据块在了解发现和连接数据结构，第 4-1 页中单独进行说明。完整主机配置文件数据块的块类型值为 111。

注　下图中块名称旁边的星号 (*) 表示可能会出现多个数据块实例。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	完整主机配置文件数据块 (111) (Full Host Profile Data Block (111))																															
	数据块长度 (Data Block Length)																															
	IP 地址 (IP Addresses)																															
	跳数 (Hops)								通用列表块类型 (31) (Generic List Block Type (31))																							
	通用列表块类型 (Generic List Block Type) （续）								通用列表块长度 (Generic List Block Length)																							
源自操作系统的指纹 (OS Derived Fingerprints)	通用列表块长度 (Generic List Block Length) （续）								操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																							
	操作系统指纹块类型 (130) (OS Fingerprint Block Type (130))* （续）								操作系统指纹块长度 (Operating System Fingerprint Block Length)																							
	操作系统指纹块长度 (OS Fingerprint Block Length) （续）								源自操作系统的指纹数据 ... (Operating System Derived Fingerprint Data...)																							
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
服务器指纹 (Server Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统服务器指纹数据 ... (Operating System Server Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
客户端指纹 (Client Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统客户端指纹数据 ... (Operating System Client Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
VDB 本机指纹 1 (VDB Native Fingerprints 1)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 VDB 指纹数据 ... (Operating System VDB Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
VDB 本机指纹 2 (VDB Native Fingerprints 2)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 VDB 指纹数据 ... (Operating System VDB Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
用户指纹 (User Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统用户指纹数据 ... (Operating System User Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	通用列表块长度 (Generic List Block Length)																															
扫描指纹 (Scan Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统扫描指纹数据 ... (Operating System Scan Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
应用指纹 (Application Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统应用指纹数据 ... (Operating System Application Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
冲突指纹 (Conflict Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统冲突指纹数据 ... (Operating System Conflict Fingerprint Data...)																															
(TCP) 完整服务器数据 ((TCP) Full Server Data)	列表块类型 (11)... (List Block Type (11))...																															
	列表块长度 ... (List Block Length)...																															
	(TCP) 完整服务器数据块 (104) ((TCP) Full Server Data Blocks (104))*																															
(UDP) 完整服务器数据 ((UDP) Full Server Data)	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	(UDP) 完整服务器数据块 (104) ((UDP) Full Server Data Blocks (104))*																															
网络协议数据 (Network Protocol Data)	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	（网络）协议数据块 (4) ((Network) Protocol Data Blocks (4))*																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
传输协议数据 (Transport Protocol Data)	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	（传输）协议数据块 (4) ((Transport) Protocol Data Blocks (4))*																															
MAC 地址数据 (MAC Address Data)	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	主机 MAC 地址数据块 (95) (Host MAC Address Data Blocks (95))*																															
	上次查看时间 (Last Seen)																															
	主机类型 (Host Type)																															
	业务临界点 (Business Criticality)																VLAN ID															
	VLAN 类型 (VLAN Type)								VLAN 优先级 (VLAN Priority)								通用列表块类型 (31) (Generic List Block Type (31))															
主机客户端数据	通用列表块类型 (Generic List Block Type) （续）																通用列表块长度 (Generic List Block Length)															
	通用列表块长度 (Generic List Block Length) （续）																完整主机客户端应用数据块 (112) (Full Host Client Application Data Blocks (112))*															
NetBIOS 名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	NetBIOS 名称字符串 ... (NetBIOS Name String...)																															
说明数据	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	注释字符串 ... (Notes String....)																															
(VDB) 主机漏洞 ((VDB) Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	(VDB) 主机漏洞数据块 (85) ((VDB) Host Vulnerability Data Blocks (85))*																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
（第三方 /VDB）主机漏洞 ((3rd Pty/VDB) Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	（第三方 /VDB）主机漏洞数据块 (85) ((Third Party/VDB) Host Vulnerability Data Blocks (85))*																															
第三方扫描主机漏洞 (3rd Pty Scan Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	（第三方扫描）具有原始漏洞 ID 的主机漏洞数据块 (85) ((Third Party Scan) Host Vulnerability Data Blocks with Original Vuln IDs (85))*																															
属性值数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	属性值数据块 (Attribute Value Data Blocks) *																															

下表对用于 5.0 - 5.0.2 记录的完整主机配置文件的组件进行了说明。

表 B-49　　完整主机配置文件记录 5.0 - 5.0.2 字段

字段	数据类型	说明
IP 地址 (IP Addresses)	uint8[4]	主机的 IP 地址，采用 IP 地址八位组。
跳数 (Hops)	uint8	从主机到设备的网络跳数。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送源自主机的现有指纹的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
源自操作系统的指纹数据块 (Operating System Derived Fingerprint Data Blocks) *	变量	包含源自主机的现有指纹的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用服务器指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。

表 B-49 完整主机配置文件记录 5.0 - 5.0.2 字段 （续）

字段	数据类型	说明
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（服务器指纹）数据块 (Operating System Fingerprint (Server Fingerprint) Data Blocks) *	变量	包含用服务器指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用客户端指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（客户端指纹）数据块 (Operating System Fingerprint (Client Fingerprint) Data Blocks) *	变量	包含用客户端指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用 Cisco VDB 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (VDB) 本机指纹 1) 数据块 (Operating System Fingerprint (VDB) Native Fingerprint 1) Data Blocks) *	变量	包含用 Cisco 漏洞数据库 (VDB) 中的指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用 Cisco VDB 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。

表 B-49　完整主机配置文件记录 5.0 - 5.0.2 字段 （续）

字段	数据类型	说明
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (VDB) 本机指纹 2) 数据块 (Operating System Fingerprint (VDB) Native Fingerprint 2) Data Blocks) *	变量	包含用 Cisco 漏洞数据库 (VDB) 中的指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用户添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（用户指纹）数据块 (Operating System Fingerprint (User Fingerprint) Data Blocks) *	变量	包含用户添加的主机上操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送漏洞扫描仪添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（扫描指纹）数据块 (Operating System Fingerprint (Scan Fingerprint) Data Blocks) *	变量	包含漏洞扫描仪添加的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送应用添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 B-49 完整主机配置文件记录 5.0 - 5.0.2 字段 （续）

字段	数据类型	说明
操作系统指纹（应用指纹）数据块 (Operating System Fingerprint (Application Fingerprint) Data Blocks) *	变量	包含应用添加的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送通过指纹冲突解决选择的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（冲突指纹）数据块 (Operating System Fingerprint (Conflict Fingerprint) Data Blocks) *	变量	包含通过指纹冲突解决选择的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
列表块类型 (List Block Type)	uint32	启动由传送 TCP 服务数据的完整服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装完整服务器数据块的长度。
(TCP) 完整服务器数据块 ((TCP) Full Server Data Blocks) *	变量	传输主机上的 TCP 服务相关数据的完整服务器数据块列表。有关此数据块的说明，请参阅完整主机服务器数据块 4.10.0+，第 4-143 页。
列表块类型 (List Block Type)	uint32	启动由传送 UDP 服务数据的完整服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装完整服务器数据块的长度。
(UDP) 完整服务器数据块 ((UDP) Full Server Data Blocks) *	变量	传输主机上的 UDP 子服务器相关数据的完整主机数据块列表。有关此数据块的说明，请参阅完整主机服务器数据块 4.10.0+，第 4-143 页。
列表块类型 (List Block Type)	uint32	启动由传送网络协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块的长度。

表 B-49　完整主机配置文件记录 5.0 - 5.0.2 字段 （续）

字段	数据类型	说明
（网络）协议数据块 ((Network) Protocol Data Blocks) *	变量	传输主机上的网络协议相关数据的协议数据块列表。有关此数据块的说明，请参阅协议数据块，第 4-74 页。
列表块类型 (List Block Type)	uint32	启动由传送传输协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块的长度。
（传输）协议数据块 ((Transport) Protocol Data Blocks) *	变量	传送主机上的传输协议相关数据的协议数据块列表。有关此数据块的说明，请参阅协议数据块，第 4-74 页。
列表块类型 (List Block Type)	uint32	启动包含主机 MAC 地址数据块的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数，包括列表报头以及所有封装主机 MAC 地址数据块。
主机 MAC 地址数据块 (Host MAC Address Data Blocks) *	变量	主机 MAC 地址数据块列表。有关此数据块的说明，请参阅主机 MAC 地址 4.9+，第 4-116 页。
上次查看时间 (Last Seen)	uint32	表示系统上次检测到主机活动的 UNIX 时间戳。
主机类型 (Host Type)	uint32	表示主机类型。值包括： • 0 - 主机 • 1 - 路由器 • 2 - 网桥 • 3 - NAT （网络地址转换设备） • 4 - LB （负载均衡器）
业务临界点 (Business Criticality)	uint16	表示主机到业务的临界点。
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
VLAN 类型 (VLAN Type)	uint8	VLAN 标签中封装的数据包类型。
VLAN 优先级 (VLAN Priority)	uint8	VLAN 标签中包含的优先级值。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送客户端应用数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装客户端应用数据块。

表 B-49 完整主机配置文件记录 5.0 - 5.0.2 字段 （续）

字段	数据类型	说明
完整主机客户端应用数据块 (Full Host Client Application Data Blocks) *	变量	客户端应用数据块列表。有关此数据块的说明，请参阅完整主机客户端应用数据块 5.0+，第 4-158 页。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动主机注释的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	注释字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上注释字符串中的字节数。
说明 (Description)	字符串	包含主机的主机属性注释的内容。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送 VDB 漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装数据块。
(VDB) 主机漏洞数据块 ((VDB) Host Vulnerability Data Blocks) *	变量	在 Cisco 漏洞数据库 (VDB) 中识别的漏洞的主机漏洞数据块列表。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-114 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送第三方扫描漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装数据块。
（第三方 /VDB）主机漏洞数据块 ((Third Party/VDB) Host Vulnerability Data Blocks) *	变量	源自第三方扫描仪且包含已收录到 Cisco 漏洞数据库 (VDB) 中的主机漏洞的相关信息的主机漏洞数据块。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-114 页。

表 B-49　完整主机配置文件记录 5.0 - 5.0.2 字段 （续）

字段	数据类型	说明
通用列表块类型 (Generic List Block Type)	uint32	启动由传送第三方扫描漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装数据块。
（第三方扫描）主机漏洞数据块 ((Third Party Scan) Host Vulnerability Data Blocks) *	变量	源自第三方扫描仪的主机漏洞数据块。请注意，这些数据块的主机漏洞 ID 为第三方扫描仪 ID，而不是 Cisco 检测到的 ID。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-114 页。
列表块类型 (List Block Type)	uint32	启动由传送属性数据的属性值数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表数据块中的字节数，包括列表报头以及所有封装数据块。
属性值数据块 (Attribute Value Data Blocks) *	变量	属性值数据块列表。有关此列表中的数据块的说明，请参阅属性值数据块，第 4-82 页。

完整主机配置文件数据块 5.1.1

用于版本 5.1.1 的完整主机配置文件数据块包含一整套主机说明数据。其格式如下图中所示，并在下表中进行说明。请注意，除列表数据块之外，该图未显示封装数据块的字段。这些封装数据块在了解发现和连接数据结构，第 4-1 页中单独进行说明。完整主机配置文件数据块的块类型值为 135。它否决了数据块 111。

注　下图中块名称旁边的星号 (*) 表示可能会出现多个数据块实例。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
完整主机配置文件数据块 (135) (Full Host Profile Data Block (135))																																
数据块长度 (Data Block Length)																																
IP 地址 (IP Addresses)																																
跳数 (Hops)									通用列表块类型 (31) (Generic List Block Type (31))																							

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	通用列表块类型 (Generic List Block Type)（续）								通用列表块长度 (Generic List Block Length)																							
源自操作系统的指纹 (OS Derived Fingerprints)	通用列表块长度 (Generic List Block Length)（续）								操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																							
	操作系统指纹块类型 (130) (OS Fingerprint Block Type (130))*（续）								操作系统指纹块长度 (Operating System Fingerprint Block Length)																							
	操作系统指纹块长度 (OS Fingerprint Block Length)（续）								源自操作系统的指纹数据 ... (Operating System Derived Fingerprint Data...)																							
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
服务器指纹 (Server Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统服务器指纹数据 ... (Operating System Server Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
客户端指纹 (Client Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统客户端指纹数据 ... (Operating System Client Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
VDB 本机指纹 1 (VDB Native Fingerprints 1)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 VDB 指纹数据 ... (Operating System VDB Fingerprint Data...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
VDB 本机指纹 2 (VDB Native Fingerprints 2)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 VDB 指纹数据 ... (Operating System VDB Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
用户指纹 (User Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统用户指纹数据 ... (Operating System User Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
扫描指纹 (Scan Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统扫描指纹数据 ... (Operating System Scan Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
应用指纹 (Application Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统应用指纹数据 ... (Operating System Application Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
冲突指纹 (Conflict Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统冲突指纹数据 ... (Operating System Conflict Fingerprint Data...)																															
(TCP) 完整服务器数据 ((TCP) Full Server Data)	列表块类型 (11)... (List Block Type (11))...																															
	列表块长度 ... (List Block Length)...																															
	(TCP) 完整服务器数据块 (104) ((TCP) Full Server Data Blocks (104))*																															
(UDP) 完整服务器数据 ((UDP) Full Server Data)	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	(UDP) 完整服务器数据块 (104) ((UDP) Full Server Data Blocks (104))*																															
网络协议数据 (Network Protocol Data)	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	（网络）协议数据块 (4) ((Network) Protocol Data Blocks (4))*																															
传输协议数据 (Transport Protocol Data)	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	（传输）协议数据块 (4) ((Transport) Protocol Data Blocks (4))*																															
MAC 地址数据 (MAC Address Data)	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	主机 MAC 地址数据块 (95) (Host MAC Address Data Blocks (95))*																															
	上次查看时间 (Last Seen)																															
	主机类型 (Host Type)																															
	业务临界点 (Business Criticality)																VLAN ID															
	VLAN 类型 (VLAN Type)								VLAN 优先级 (VLAN Priority)								通用列表块类型 (31) (Generic List Block Type (31))															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
主机客户端数据	通用列表块类型 (Generic List Block Type) （续）																通用列表块长度 (Generic List Block Length)															
	通用列表块长度 (Generic List Block Length) （续）																完整主机客户端应用数据块 (112) (Full Host Client Application Data Blocks (112))*															
NetBIOS 名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	NetBIOS 名称字符串 ... (NetBIOS Name String...)																															
说明数据	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	注释字符串 ... (Notes String....)																															
(VDB) 主机漏洞 ((VDB) Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	(VDB) 主机漏洞数据块 (85) ((VDB) Host Vulnerability Data Blocks (85))*																															
（第三方 /VDB）主机漏洞 ((3rd Pty/VDB) Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	（第三方 /VDB）主机漏洞数据块 (85) ((Third Party/VDB) Host Vulnerability Data Blocks (85))*																															
第三方扫描主机漏洞 (3rd Pty Scan Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	（第三方扫描）具有原始漏洞 ID 的主机漏洞数据块 (85) ((Third Party Scan) Host Vulnerability Data Blocks with Original Vuln IDs (85))*																															
属性值数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	属性值数据块 (Attribute Value Data Blocks) *																															
	移动 (Mobile)								Jailbroken								VLAN 在线状态 (VLAN Presence)															

下表对用于 5.1.1 记录的完整主机配置文件的组件进行了说明。

表 B-50 完整主机配置文件记录 5.1.1 字段

字段	数据类型	说明
IP 地址 (IP Addresses)	uint8[4]	主机的 IP 地址，采用 IP 地址八位组。
跳数 (Hops)	uint8	从主机到设备的网络跳数。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送源自主机的现有指纹的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
源自操作系统的指纹数据块 (Operating System Derived Fingerprint Data Blocks) *	变量	包含源自主机的现有指纹的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用服务器指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（服务器指纹）数据块 (Operating System Fingerprint (Server Fingerprint) Data Blocks) *	变量	包含用服务器指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用客户端指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 B-50　完整主机配置文件记录 5.1.1 字段 （续）

字段	数据类型	说明
操作系统指纹（客户端指纹）数据块 (Operating System Fingerprint (Client Fingerprint) Data Blocks) *	变量	包含用客户端指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用 Cisco VDB 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (VDB) 本机指纹 1) 数据块 (Operating System Fingerprint (VDB) Native Fingerprint 1) Data Blocks) *	变量	包含用 Cisco 漏洞数据库 (VDB) 中的指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用 Cisco VDB 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (VDB) 本机指纹 2) 数据块 (Operating System Fingerprint (VDB) Native Fingerprint 2) Data Blocks) *	变量	包含用 Cisco 漏洞数据库 (VDB) 中的指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用户添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 B-50 完整主机配置文件记录 5.1.1 字段 （续）

字段	数据类型	说明
操作系统指纹（用户指纹）数据块 (Operating System Fingerprint (User Fingerprint) Data Blocks) *	变量	包含用户添加的主机上操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送漏洞扫描仪添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（扫描指纹）数据块 (Operating System Fingerprint (Scan Fingerprint) Data Blocks) *	变量	包含漏洞扫描仪添加的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送应用添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（应用指纹）数据块 (Operating System Fingerprint (Application Fingerprint) Data Blocks) *	变量	包含应用添加的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送通过指纹冲突解决选择的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 B-50　完整主机配置文件记录 5.1.1 字段 （续）

字段	数据类型	说明
操作系统指纹（冲突指纹）数据块 (Operating System Fingerprint (Conflict Fingerprint) Data Blocks) *	变量	包含通过指纹冲突解决选择的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
列表块类型 (List Block Type)	uint32	启动由传送 TCP 服务数据的完整服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装完整服务器数据块的长度。
(TCP) 完整服务器数据块 ((TCP) Full Server Data Blocks) *	变量	传输主机上的 TCP 服务相关数据的完整服务器数据块列表。有关此数据块的说明，请参阅完整主机服务器数据块 4.10.0+，第 4-143 页。
列表块类型 (List Block Type)	uint32	启动由传送 UDP 服务数据的完整服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装完整服务器数据块的长度。
(UDP) 完整服务器数据块 ((UDP) Full Server Data Blocks) *	变量	传输主机上的 UDP 子服务器相关数据的完整主机数据块列表。有关此数据块的说明，请参阅完整主机服务器数据块 4.10.0+，第 4-143 页。
列表块类型 (List Block Type)	uint32	启动由传送网络协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块的长度。
（网络）协议数据块 ((Network) Protocol Data Blocks) *	变量	传输主机上的网络协议相关数据的协议数据块列表。有关此数据块的说明，请参阅协议数据块，第 4-74 页。
列表块类型 (List Block Type)	uint32	启动由传送传输协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块的长度。
（传输）协议数据块 ((Transport) Protocol Data Blocks) *	变量	传送主机上的传输协议相关数据的协议数据块列表。有关此数据块的说明，请参阅协议数据块，第 4-74 页。
列表块类型 (List Block Type)	uint32	启动包含主机 MAC 地址数据块的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数，包括列表报头以及所有封装主机 MAC 地址数据块。

表 B-50 完整主机配置文件记录 5.1.1 字段 （续）

字段	数据类型	说明
主机 MAC 地址数据块 (Host MAC Address Data Blocks) *	变量	主机 MAC 地址数据块列表。有关此数据块的说明，请参阅主机 MAC 地址 4.9+，第 4-116 页。
上次查看时间 (Last Seen)	uint32	表示系统上次检测到主机活动的 UNIX 时间戳。
主机类型 (Host Type)	uint32	表示主机类型。值包括： • 0 - 主机 • 1 - 路由器 • 2 - 网桥 • 3 - NAT （网络地址转换设备） • 4 - LB （负载均衡器）
业务临界点 (Business Criticality)	uint16	表示主机到业务的临界点。
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
VLAN 类型 (VLAN Type)	uint8	VLAN 标签中封装的数据包类型。
VLAN 优先级 (VLAN Priority)	uint8	VLAN 标签中包含的优先级值。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送客户端应用数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装客户端应用数据块。
完整主机客户端应用数据块 (Full Host Client Application Data Blocks) *	变量	客户端应用数据块列表。有关此数据块的说明，请参阅完整主机客户端应用数据块 5.0+，第 4-158 页。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动主机注释的字符串数据块。值始终为 0。

表 B-50　完整主机配置文件记录 5.1.1 字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Length)	uint32	注释字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上注释字符串中的字节数。
说明 (Description)	字符串	包含主机的主机属性注释的内容。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送 VDB 漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装数据块。
(VDB) 主机漏洞数据块 ((VDB) Host Vulnerability Data Blocks) *	变量	在 Cisco 漏洞数据库 (VDB) 中识别的漏洞的主机漏洞数据块列表。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-114 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送第三方扫描漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装数据块。
（第三方 /VDB）主机漏洞数据块 ((Third Party/VDB) Host Vulnerability Data Blocks) *	变量	源自第三方扫描仪且包含已收录到 Cisco 漏洞数据库 (VDB) 中的主机漏洞的相关信息的主机漏洞数据块。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-114 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送第三方扫描漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装数据块。
（第三方扫描）主机漏洞数据块 ((Third Party Scan) Host Vulnerability Data Blocks) *	变量	源自第三方扫描仪的主机漏洞数据块。请注意，这些数据块的主机漏洞 ID 为第三方扫描仪 ID，而不是 Cisco 检测到的 ID。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-114 页。
列表块类型 (List Block Type)	uint32	启动由传送属性数据的属性值数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表数据块中的字节数，包括列表报头以及所有封装数据块。

表 B-50 完整主机配置文件记录 5.1.1 字段 （续）

字段	数据类型	说明
属性值数据块 (Attribute Value Data Blocks) *	变量	属性值数据块列表。有关此列表中的数据块的说明，请参阅属性值数据块，第 4-82 页。
移动 (Mobile)	uint8	指示操作系统是否在移动设备上运行的一个真假标志。
Jailbroken	uint8	指示移动设备操作系统是否被越狱的一个真假标志。
VLAN 在线状态 (VLAN Presence)	uint8	表示是否存在 VLAN： • 0 - 是 • 1 - 否

完整主机配置文件数据块 5.2.x

用于版本 5.2.x 的完整主机配置文件数据块包含一整套主机说明数据。其格式如下图中所示，并在下表中进行说明。请注意，除列表数据块之外，该图未显示封装数据块的字段。这些封装数据块在了解发现和连接数据结构，第 4-1 页中单独进行说明。完整主机配置文件数据块的块类型值为 140。它替代了之前的版本，之前版本的块类型为 135。

注 下图中块名称旁边的星号 (*) 表示可能会出现多个数据块实例。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	完整主机配置文件数据块 (140) (Full Host Profile Data Block (140))																															
	数据块长度 (Data Block Length)																															
	主机 ID (Host ID) 主机 ID (Host ID) （续） 主机 ID (Host ID) （续） 主机 ID (Host ID) （续）																															
IP 地址 (IP Addresses)	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	IP 地址数据块 (143) (IP Address Data Blocks (143))*																															
	跳数 (Hops)								通用列表块类型 (31) (Generic List Block Type (31))																							

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	通用列表块类型 (Generic List Block Type)（续）								通用列表块长度 (Generic List Block Length)																							
源自操作系统的指纹 (OS Derived Fingerprints)	通用列表块长度 (Generic List Block Length)（续）								操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																							
	操作系统指纹块类型 (130) (OS Fingerprint Block Type (130))*（续）								操作系统指纹块长度 (Operating System Fingerprint Block Length)																							
	操作系统指纹块长度 (OS Fingerprint Block Length)（续）								源自操作系统的指纹数据 ... (Operating System Derived Fingerprint Data...)																							
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
服务器指纹 (Server Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统服务器指纹数据 ... (Operating System Server Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
客户端指纹 (Client Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统客户端指纹数据 ... (Operating System Client Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
VDB 本机指纹 1 (VDB Native Fingerprints 1)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 VDB 指纹数据 ... (Operating System VDB Fingerprint Data...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
VDB 本机指纹 2 (VDB Native Fingerprints 2)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 VDB 指纹数据 ... (Operating System VDB Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
用户指纹 (User Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统用户指纹数据 ... (Operating System User Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
扫描指纹 (Scan Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统扫描指纹数据 ... (Operating System Scan Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
应用指纹 (Application Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统应用指纹数据 ... (Operating System Application Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
冲突指纹 (Conflict Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统冲突指纹数据 ... (Operating System Conflict Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
移动指纹 (Mobile Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统移动指纹数据 ... (Operating System Mobile Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
IPv6 服务器指纹 (IPv6 Server Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 IPv6 服务器指纹数据 ... (Operating System IPv6 Server Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
Ipv6 客户端指纹 (IPv6 Client Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 Ipv6 客户端指纹数据 ... (Operating System Ipv6 Client Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
Ipv6 DHCP 指纹 (IPv6 DHCP Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 IPv6 DHCP 指纹数据 ... (Operating System IPv6 DHCP Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	通用列表块长度 (Generic List Block Length)																															
用户代理指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统用户代理指纹数据 ... (Operating System User Agent Fingerprint Data...)																															
(TCP) 完整服务器数据 ((TCP) Full Server Data)	列表块类型 (11)... (List Block Type (11))...																															
	列表块长度 ... (List Block Length)...																															
	(TCP) 完整服务器数据块 (104) ((TCP) Full Server Data Blocks (104))*																															
(UDP) 完整服务器数据 ((UDP) Full Server Data)	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	(UDP) 完整服务器数据块 (104) ((UDP) Full Server Data Blocks (104))*																															
网络协议数据 (Network Protocol Data)	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	（网络）协议数据块 (4) ((Network) Protocol Data Blocks (4))*																															
传输协议数据 (Transport Protocol Data)	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	（传输）协议数据块 (4) ((Transport) Protocol Data Blocks (4))*																															
MAC 地址数据 (MAC Address Data)	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	主机 MAC 地址数据块 (95) (Host MAC Address Data Blocks (95))*																															
	上次查看时间 (Last Seen)																															
	主机类型 (Host Type)																															
	业务临界点 (Business Criticality)																VLAN ID															
	VLAN 类型 (VLAN Type)								VLAN 优先级 (VLAN Priority)								通用列表块类型 (31) (Generic List Block Type (31))															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
主机客户端数据	通用列表块类型 (Generic List Block Type) （续）																通用列表块长度 (Generic List Block Length)															
	通用列表块长度 (Generic List Block Length) （续）																完整主机客户端应用数据块 (112) (Full Host Client Application Data Blocks (112))*															
NetBIOS 名称 (NetBIOS Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
名称	NetBIOS 名称字符串 ... (NetBIOS Name String...)																															
说明数据	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	注释字符串 ... (Notes String....)																															
(VDB) 主机漏洞 ((VDB) Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	(VDB) 主机漏洞数据块 (85) ((VDB) Host Vulnerability Data Blocks (85))*																															
（第三方 /VDB）主机漏洞 ((3rd Pty/VDB) Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	（第三方 /VDB）主机漏洞数据块 (85) ((Third Party/VDB) Host Vulnerability Data Blocks (85))*																															
第三方扫描主机漏洞 (3rd Pty Scan Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	（第三方扫描）具有原始漏洞 ID 的主机漏洞数据块 (85) ((Third Party Scan) Host Vulnerability Data Blocks with Original Vuln IDs (85))*																															
属性值数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	属性值数据块 (Attribute Value Data Blocks) *																															
	移动 (Mobile)								Jailbroken																							

下表对用于 5.2.x 记录的完整主机配置文件的组件进行了说明。

表 B-51 完整主机配置文件记录 5.2.x 字段

字段	数据类型	说明
主机 ID (Host ID)	uint8[16]	主机的唯一 ID 号码。这是一个 UUID。
列表块类型 (List Block Type)	uint32	启动由传送 TCP 服务数据的 IP 地址数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装 IP 地址数据块的长度。
IP 地址 (IP Addresses)	变量	主机的 IP 地址以及上次看到每个 IP 地址的时间。有关此数据块的说明，请参阅主机 IP 地址数据块，第 4-98 页。
跳数 (Hops)	uint8	从主机到设备的网络跳数。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送源自主机的现有指纹的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
源自操作系统的指纹数据块 (Operating System Derived Fingerprint Data Blocks) *	变量	包含源自主机的现有指纹的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用服务器指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（服务器指纹）数据块 (Operating System Fingerprint (Server Fingerprint) Data Blocks) *	变量	包含用服务器指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用客户端指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 B-51　完整主机配置文件记录 5.2.x 字段 （续）

字段	数据类型	说明
操作系统指纹（客户端指纹）数据块 (Operating System Fingerprint (Client Fingerprint) Data Blocks) *	变量	包含用客户端指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用 Cisco VDB 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (VDB) 本机指纹 1) 数据块 (Operating System Fingerprint (VDB) Native Fingerprint 1) Data Blocks) *	变量	包含用 Cisco 漏洞数据库 (VDB) 中的指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用 Cisco VDB 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (VDB) 本机指纹 2) 数据块 (Operating System Fingerprint (VDB) Native Fingerprint 2) Data Blocks) *	变量	包含用 Cisco 漏洞数据库 (VDB) 中的指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用户添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 B-51 完整主机配置文件记录 5.2.x 字段 （续）

字段	数据类型	说明
操作系统指纹（用户指纹）数据块 (Operating System Fingerprint (User Fingerprint) Data Blocks) *	变量	包含用户添加的主机上操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送漏洞扫描仪添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（扫描指纹）数据块 (Operating System Fingerprint (Scan Fingerprint) Data Blocks) *	变量	包含漏洞扫描仪添加的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送应用添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（应用指纹）数据块 (Operating System Fingerprint (Application Fingerprint) Data Blocks) *	变量	包含应用添加的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送通过指纹冲突解决选择的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 B-51　完整主机配置文件记录 5.2.x 字段 （续）

字段	数据类型	说明
操作系统指纹（冲突指纹）数据块 (Operating System Fingerprint (Conflict Fingerprint) Data Blocks) *	变量	包含通过指纹冲突解决选择的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送移动设备指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（移动）数据块 (Operating System Fingerprint (Mobile) Data Blocks) *	变量	包含移动设备主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用 IPv6 服务器指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（IPv6 服务器指纹）数据块 (Operating System Fingerprint (IPv6 Server Fingerprint) Data Blocks) *	变量	包含用 IPv6 服务器指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用 IPv6 客户端指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 B-51 完整主机配置文件记录 5.2.x 字段 （续）

字段	数据类型	说明
操作系统指纹（IPv6 客户端指纹）数据块 (Operating System Fingerprint (IPv6 Client Fingerprint) Data Blocks) *	变量	包含用 IPv6 客户端指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用 IPv6 DHCP 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (IPv6 DHCP) 数据块 (Operating System Fingerprint (IPv6 DHCP) Data Blocks) *	变量	包含用 IPv6 DHCP 指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用用户代理指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（用户代理）数据块 (Operating System Fingerprint (User Agent) Data Blocks) *	变量	包含用用户代理指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
列表块类型 (List Block Type)	uint32	启动由传送 TCP 服务数据的完整服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装完整服务器数据块的长度。
(TCP) 完整服务器数据块 ((TCP) Full Server Data Blocks) *	变量	传输主机上的 TCP 服务相关数据的完整服务器数据块列表。有关此数据块的说明，请参阅完整主机服务器数据块 4.10.0+，第 4-143 页。
列表块类型 (List Block Type)	uint32	启动由传送 UDP 服务数据的完整服务器数据块组成的列表数据块。值始终为 11。

表 B-51　完整主机配置文件记录 5.2.x 字段 （续）

字段	数据类型	说明
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装完整服务器数据块的长度。
(UDP) 完整服务器数据块 ((UDP) Full Server Data Blocks) *	变量	传输主机上的 UDP 子服务器相关数据的完整主机数据块列表。有关此数据块的说明，请参阅完整主机服务器数据块 4.10.0+，第 4-143 页。
列表块类型 (List Block Type)	uint32	启动由传送网络协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块的长度。
（网络）协议数据块 ((Network) Protocol Data Blocks) *	变量	传输主机上的网络协议相关数据的协议数据块列表。有关此数据块的说明，请参阅协议数据块，第 4-74 页。
列表块类型 (List Block Type)	uint32	启动由传送传输协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块的长度。
（传输）协议数据块 ((Transport) Protocol Data Blocks) *	变量	传送主机上的传输协议相关数据的协议数据块列表。有关此数据块的说明，请参阅协议数据块，第 4-74 页。
列表块类型 (List Block Type)	uint32	启动包含主机 MAC 地址数据块的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数，包括列表报头以及所有封装主机 MAC 地址数据块。
主机 MAC 地址数据块 (Host MAC Address Data Blocks) *	变量	主机 MAC 地址数据块列表。有关此数据块的说明，请参阅主机 MAC 地址 4.9+，第 4-116 页。
上次查看时间 (Last Seen)	uint32	表示系统上次检测到主机活动的 UNIX 时间戳。
主机类型 (Host Type)	uint32	表示主机类型。值包括： • 0 - 主机 • 1 - 路由器 • 2 - 网桥 • 3 - NAT （网络地址转换设备） • 4 - LB （负载均衡器）
业务临界点 (Business Criticality)	uint16	表示主机到业务的临界点。
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。

表 B-51 完整主机配置文件记录 5.2.x 字段 （续）

字段	数据类型	说明
VLAN 类型 (VLAN Type)	uint8	VLAN 标签中封装的数据包类型。
VLAN 优先级 (VLAN Priority)	uint8	VLAN 标签中包含的优先级值。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送客户端应用数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装客户端应用数据块。
完整主机客户端应用数据块 (Full Host Client Application Data Blocks) *	变量	客户端应用数据块列表。有关此数据块的说明，请参阅完整主机客户端应用数据块 5.0+，第 4-158 页。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动主机注释的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	注释字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上注释字符串中的字节数。
说明	字符串	包含主机的主机属性注释的内容。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送 VDB 漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装数据块。
(VDB) 主机漏洞数据块 ((VDB) Host Vulnerability Data Blocks) *	变量	在 Cisco 漏洞数据库 (VDB) 中识别的漏洞的主机漏洞数据块列表。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-114 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送第三方扫描漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。

表 B-51　完整主机配置文件记录 5.2.x 字段 （续）

字段	数据类型	说明
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装数据块。
（第三方 /VDB）主机漏洞数据块 ((Third Party/VDB) Host Vulnerability Data Blocks) *	变量	源自第三方扫描仪且包含已收录到 Cisco 漏洞数据库 (VDB) 中的主机漏洞的相关信息的主机漏洞数据块。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-114 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送第三方扫描漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装数据块。
（第三方扫描）主机漏洞数据块 ((Third Party Scan) Host Vulnerability Data Blocks) *	变量	源自第三方扫描仪的主机漏洞数据块。请注意，这些数据块的主机漏洞 ID 为第三方扫描仪 ID，而不是 Cisco 检测到的 ID。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-114 页。
列表块类型 (List Block Type)	uint32	启动由传送属性数据的属性值数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表数据块中的字节数，包括列表报头以及所有封装数据块。
属性值数据块 (Attribute Value Data Blocks) *	变量	属性值数据块列表。有关此列表中的数据块的说明，请参阅属性值数据块，第 4-82 页。
移动 (Mobile)	uint8	指示操作系统是否在移动设备上运行的一个真假标志。
Jailbroken	uint8	指示移动设备操作系统是否被越狱的一个真假标志。

用于 5.1.x 的主机配置文件数据块

下图显示主机配置文件数据块的格式。该数据块也不包含主机临界值，但包含 VLAN 在线状态指示器。此外，数据块还可以传输主机的 NetBIOS 名称。主机配置文件数据块的块类型为 132。

注　下图中块类型字段旁边的星号 (*) 表示该消息可能包含零个或多个系列 1 数据块实例。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	主机配置文件块类型 (132) (Host Profile Block Type (132))																															
	主机配置文件块长度 (Host Profile Block Length)																															
	IP 地址 (IP Addresses)																															
服务器指纹	跳数 (Hops)								主要 / 次要 (Primary/Secondary)								通用列表块类型 (31) (Generic List Block Type (31))															
	通用列表块类型 (Generic List Block Type) （续）																通用列表块长度 (Generic List Block Length)															
	通用列表块长度 (Generic List Block Length) （续）																服务器指纹数据块 (Server Fingerprint Data Blocks)*															
客户端指纹	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	客户端指纹数据块 (Client Fingerprint Data Blocks)*																															
中小企业指纹	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	SMB 指纹数据块 (SMB Fingerprint Data Blocks)*																															
DHCP 指纹	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	DHCP 指纹数据块 (DHCP Fingerprint Data Blocks)*																															
移动设备指纹 (Mobile Device Fingerprint)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	移动设备指纹数据块 (Mobile Device Fingerprint Data Blocks)*																															
TCP 服务器块 (TCP Server Block)*	列表块类型 (11) (List Block Type (11))																														TCP 服务器	
	列表块长度 (List Block Length)																															
	TCP 服务器数据块 (TCP Server Data Blocks)																															

字节	0								1								2								3								
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
UDP 服务器块 (UDP Server Block)*	列表块类型 (11) (List Block Type (11))																																UDP 服务器
	列表块长度 (List Block Length)																																
	UDP 服务器数据块 (UDP Server Data Blocks)																																
网络协议块 (Network Protocol Block)*	列表块类型 (11) (List Block Type (11))																																网络协议
	列表块长度 (List Block Length)																																
	网络协议数据块 (Network Protocol Data Blocks)																																
传输协议块 (Transport Protocol Block)*	列表块类型 (11) (List Block Type (11))																																传输协议
	列表块长度 (List Block Length)																																
	传输协议数据块 (Transport Protocol Data Blocks)																																
MAC 地址块 (MAC Address Block)*	列表块类型 (11) (List Block Type (11))																																MAC 地址
	列表块长度 (List Block Length)																																
	主机 MAC 地址数据块 (Host MAC Address Data Blocks)																																
	主机上次查看时间 (Host Last Seen)																																
	主机类型 (Host Type)																																
	移动 (Mobile)								Jailbroken								VLAN 在线状态 (VLAN Presence)								VLAN ID								
客户端应用数据	VLAN ID （续）								VLAN 类型 (VLAN Type)								VLAN 优先级 (VLAN Priority)								通用列表块类型 (31) (Generic List Block Type (31))								客户端应用
	通用列表块类型 (31) (Generic List Block Type (31)) （续）																								通用列表块长度 (Generic List Block Length)								
	通用列表块长度 (Generic List Block Length) （续）																								客户端应用数据块 (Client Application Data Blocks)								
NetBIOS 名称	字符串块类型 (0) (String Block Type (0))																																
	字符串块长度 (String Block Length)																																
	NetBIOS 字符串数据 ...(NetBIOS String Data...)																																

下表对版本 5.1.x 返回的主机配置文件数据块的字段进行了说明

表 B-52 主机配置文件数据块 5.1.x 字段

字段	数据类型	说明
主机配置文件块类型 (Host Profile Block Type)	uint32	启动用于 5.1.x 的主机配置文件数据块。值始终为 132。
主机配置文件块长度 (Host Profile Block Length)	uint32	主机配置文件数据块中的字节数，包括主机配置文件块类型和长度字段的八个字节，加上随后的主机配置文件数据中的字节数。
IP 地址 (IP Addresses)	uint8[4]	配置文件中描述的主机的 IP 地址，采用 IP 地址八位组。
跳数 (Hops)	uint8	从主机到设备的跳数。
主 / 辅助 (Primary/ Secondary)	uint8	表示主机是位于检测到其的设备的主网络中还是辅助网络中： • 0 - 主机位于主网络中。 • 1 - 主机位于辅助网络中。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用服务器指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（服务器指纹）数据块 (Operating System Fingerprint (Server Fingerprint) Data Blocks) *	变量	包含用服务器指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用客户端指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 B-52　主机配置文件数据块 5.1.x 字段 （续）

字段	数据类型	说明
操作系统指纹（客户端指纹）数据块 (Operating System Fingerprint (Client Fingerprint) Data Blocks) *	变量	包含用客户端指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用 SMB 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（SMB 指纹）数据块 (Operating System Fingerprint (SMB Fingerprint) Data Blocks) *	变量	包含用 SMB 指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用 DHCP 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（DHCP 指纹）数据块 (Operating System Fingerprint (DHCP Fingerprint) Data Blocks) *	变量	包含用 DHCP 指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用 DHCP 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 B-52 主机配置文件数据块 5.1.x 字段 （续）

字段	数据类型	说明
操作系统指纹（移动设备指纹）数据块 (Operating System Fingerprint (Mobile 设备 Fingerprint) Data Blocks) *	变量	包含用移动设备指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
列表块类型 (List Block Type)	uint32	启动由传送 TCP 服务器数据的服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装服务器数据块。 此字段后面是零个或多个服务器数据块。
TCP 服务器数据块 (TCP Server Data Blocks)	变量	描述 TCP 服务器的主机服务器数据块 （按照产品早期版本的记录）。
列表块类型 (List Block Type)	uint32	启动由传送 UDP 服务器数据的服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装服务器数据块。 此字段后面是零个或多个服务器数据块。
UDP 服务器数据块 (UDP Server Data Blocks)	uint32	描述 UDP 服务器的主机服务器数据块 （按照产品早期版本的记录）。
列表块类型 (List Block Type)	uint32	启动由传送网络协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块。 此字段后面是零个或多个协议数据块。
网络协议数据块 (Network Protocol Data Blocks)	uint32	描述网络协议的协议数据块。有关此数据块的说明，请参阅协议数据块，第 4-74 页。
列表块类型 (List Block Type)	uint32	启动由传送传输协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块。 此字段后面是零个或多个传输协议数据块。
传输协议数据块 (Transport Protocol Data Blocks)	uint32	描述传输协议的协议数据块。有关此数据块的说明，请参阅协议数据块，第 4-74 页。

表 B-52　主机配置文件数据块 5.1.x 字段 （续）

字段	数据类型	说明
列表块类型 (List Block Type)	uint32	启动由 MAC 地址数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数，包括列表报头以及所有封装 MAC 地址数据块。
主机 MAC 地址数据块 (Host MAC Address Data Blocks)	uint32	描述主机 MAC 地址的主机 MAC 地址数据块。有关此数据块的说明，请参阅主机 MAC 地址 4.9+，第 4-116 页。
主机上次查看时间 (Host Last Seen)	uint32	表示系统上次检测到主机活动的 UNIX 时间戳。
主机类型 (Host Type)	uint32	表示主机类型。可能会出现以下值： • 0 - 主机 • 1 - 路由器 • 2 - 网桥 • 3 - NAT 设备 • 4 - LB （负载均衡器）
移动 (Mobile)	uint8	指示主机是否为移动设备的一个真假标志。
Jailbroken	uint8	指示主机是否同样为已被越狱的移动设备的一个真假标志。
VLAN 在线状态 (VLAN Presence)	uint8	表示是否存在 VLAN： • 0 - 是 • 1 - 否
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
VLAN 类型 (VLAN Type)	uint8	VLAN 标签中封装的数据包类型。
VLAN 优先级 (VLAN Priority)	uint8	VLAN 标签中包含的优先级值。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送客户端应用数据的客户端应用数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装客户端应用数据块。
客户端应用数据块 (Client Application Data Blocks)	uint32	描述客户端应用的客户端应用数据块。有关此数据块的说明，请参阅完整主机客户端应用数据块 5.0+，第 4-158 页。
字符串块类型 (String Block Type)	uint32	启动 NetBIOS 名称的字符串数据块。此值设置为 0 以表示字符串数据。

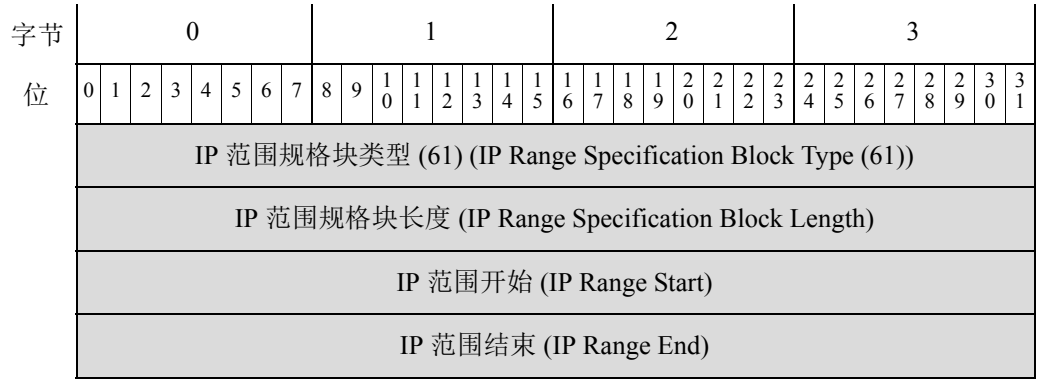
表 B-52 主机配置文件数据块 5.1.x 字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Length)	uint32	表示 NetBIOS 名称字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称的字节数。
NetBIOS 字符串数据 (NetBIOS String Data)	变量	包含主机配置文件中描述的主机的 NetBIOS 名称。

用于 5.0 - 5.1.1.x 的 IP 范围规格数据块

IP 范围规格数据块传输一系列 IP 地址。 IP 范围规格数据块在用户协议、用户客户端应用、地址规格、用户产品、用户服务器、用户主机、用户漏洞、用户临界点以及用户属性值数据块中使用。 IP 范围规格数据块的块类型为 61。

下图显示 IP 范围规格数据块的格式：



下表对 IP 范围规格数据块的组件进行了说明。

表 B-53 IP 范围规格数据块字段

字段	数据类型	说明
IP 范围规格块类型 (IP Range Specification Block Type)	uint32	启动 IP 范围规格数据块。值始终为 61。
IP 范围规格块长度 (IP Range Specification Block Length)	uint32	IP 范围规格数据块中的字节总数，包括 IP 范围规格块类型和长度字段的八个字节，加上随后的 IP 范围规格数据的字节数。

表 B-53　　IP 范围规格数据块字段 （续）

字段	数据类型	说明
IP 范围规格开始 (IP Range Specification Start)	uint32	IP 地址范围的开始 IP 地址。
IP 范围规格结束 (IP Range Specification End)	uint32	IP 地址范围的结束 IP 地址。

访问控制策略规则原因数据块

eStreamer 服务用访问控制规则策略规则原因数据块包含有关访问控制策略规则 ID 的信息。此数据块的块类型为系列 2 中的 21。

下图显示访问控制策略规则 ID 元数据块的结构。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	访问控制策略规则原因数据块类型 (21) (Access Control Policy Rule Reason Data Block Type (21))																															
	访问控制策略规则原因数据块长度 (Access Control Policy Rule Reason Data Block Length)																															
说明	原因 (Reason)																字符串块类型 (0) (String Block Type (0))															
	字符串块类型 (0) (String Block Type (0)) （续）																字符串块长度 (String Block Length)															
	字符串块长度 (String Block Length) （续）																说明 ... (Description...)															

下表对访问控制策略规则 ID 元数据块中的字段进行了说明。

表 B-54 访问控制策略规则原因数据块字段

字段	数据类型	说明
访问控制策略规则原因数据块类型 (Access Control Policy Rule Reason Data Block Type)	uint32	启动访问控制策略规则原因数据块。值始终为 21。
访问控制策略规则原因数据块长度 (Access Control Policy Rule Reason Data Block Length)	uint32	访问控制策略规则原因数据块中的字节总数，包括访问控制策略规则原因数据块类型和长度字段的八个字节，加上随后的数据的字节数。
原因 (Reason)	uint16	触发事件的规则的原因编号。
字符串块类型 (String Block Type)	uint32	启动包含访问控制策略规则原因的说明的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上说明 (Description) 字段中的字节数。
说明 (Description)	字符串	规则原因的说明。