思科 ASA NetFlow 实施指南

本指南介绍如何配置 NetFlow 安全事件日志记录 （NSEL），以及如何通过 NSEL 处理事件和系统日志消息，以及如何使用 NetFlow 收集器。

关于 NSEL

Cisco ASA 支持 NetFlow 版本 9 服务。 NSEL ASA 的 ASASM 和实施提供 IP 状态流跟踪方法，该方法仅导出那些表示流中重大事件的记录。在状态流跟踪中，跟踪的流将经历一系列状态更改。

Netflow 数据不能手动从 ASA 设备中提取，且不能手动发送到收集器。 NSEL 事件用于导出有关流状态的数据，并由导致状态更改的事件触发。

跟踪的重要事件包括流创建、流断开、流拒绝 （不包括那些被 EtherType ACL 拒绝的流）和流更新。 NSEL 的 ASA 实施会生成定期 NSEL 事件 （称为 “ 流更新事件 ”），以便在流的持续时间内提供定期字节计数器。这些事件通常是由时间驱动的，这使它们更适合传统的 NetFlow。但是，它们也可能会通过流中的状态更改进行触发。

注 版本 9.0 (1) 中未提供流更新事件。它在版本 8.4 (5) 和 9.1 (2) 及更高版本中可用。

ASA 还会导出包含相同信息的系统日志消息。您可以禁用这些系统日志消息，以避免性能降低，方法是生成代表同一事件的 NSEL 记录和系统日志消息。

每个 NSEL 记录都有一个 “ 事件 ID” 和一个 “ 扩展事件 ID” 字段，用于描述流事件。

系统日志消息和 NSEL 事件

表 1 列出具有等效 NSEL 事件、事件 ID 和扩展事件 ID 的系统日志消息。扩展事件 ID 提供有关事件的更多详细信息 （例如，哪个入口或出口 ACL 已拒绝流）。

注 启用 NetFlow 以导出流信息会使列出在冗余中表 1 的系统日志消息。为了提高性能，建议您禁用冗余系统日志消息，因为相同的信息会通过 NetFlow 导出。您可以按照中禁用和重新启用与 NetFlow 相关的系统日志消息，第 23 页的操作步骤启用或禁用个别系统日志消息。

表 1 系统日志消息和等效 NSEL 事件

系统日志消息	说明	NSEL 事件 ID	NSEL 扩展事件 ID
106100	每当遇到 ACL 时生成。	1 — 已创建流 （如果 ACL 允许流）。 3 — 流被拒绝 （如果 ACL 拒绝流）。	0 — 如果 ACL 允许流。 1001 — 流被入口 ACL 拒绝。 1002 — 流被出口 ACL 拒绝。
106015	TCP 流被拒绝，因为第一个数据包不是 SYN 数据包。	3 — 流被拒绝。	1004 — TCP 流被拒绝，因为第一个数据包不是 SYN 数据包。
106023	当通过**访问组**命令连接到接口的 ACL 拒绝流时。	3 — 流被拒绝。	1001 — 流被入口 ACL 拒绝。 1002 — 流被出口 ACL 拒绝。
302013、 302015、 302017、 302020	TCP、 UDP、 GRE 和 ICMP 连接创建。	1 — 已创建流。	0 — 忽略。
302014、 302016、 302018、 302021	TCP、 UDP、 GRE 和 ICMP 连接断开。	2 — 已删除流。	0 — 忽略。 > 2000 — 流已断开。
313001	发送到设备的 ICMP 数据包被拒绝。	3 — 流被拒绝。	1003 — 由于配置，已拒绝传入流。
313008	发送到设备的 ICMP v6 数据包被拒绝。	3 — 流被拒绝。	1003 — 由于配置，已拒绝传入流。
710003	尝试连接到设备接口被拒绝。	3 — 流被拒绝。	1003 — 由于配置，已拒绝传入流。

注 当 NSEL 和系统日志消息均已启用时，不能保证两种日志记录类型之间的时间排序。

NSEL 收集器

每个 ASA 均会与收集器建立自己的连接。导出数据包报头中的字段包括系统正常运行时间和 UNIX 时间 （在整个群集中同步）。这些字段均为单个 ASA 的本地字段。 NSEL 收集器使用数据包的源 IP 地址和源端口组合来分隔不同的导出器。

每个 ASA 均独立管理和通告其模板。由于 ASA 支持群集内升级，因此不同的设备可能会在特定时间点运行不同的映像版本。因此，每个 ASA 支持的模板可能不同。

双向流量

大多数双向流已在内部进行组合，并被视为单个流。 ASA 上的 NSEL 报告的流记录描述了流的两个方向。数据记录显式定义连接的源 （发起方）和目标 （响应方），且如果收集器应用需要，您可以使用此信息确定流的方向。此外，某些 NSEL 记录包括两个字节计数器字段（NF_F_FWD_FLOW_DELTA_BYTES 和 NF_F_REV_FLOW_DELTA_BYTES），它们提供特定于方向的流量数据。

模板更新

RFC 3954、 Cisco Systems NetFlow 服务导出版本 9，指出模板可以按固定的时间间隔发送给用户，也可以在导出的数据记录数之后发送。这些更新间隔必须是可配置的。此实施仅按时间间隔支持模板更新。不支持基于数据记录数量的模板更新。

选项模板和数据记录

不会导出任何选项模板或数据记录。 CLI 中的 **show** 命令支持某些字段。收集器应用必须发出 **show** 命令，以获取特定字段的其他信息。此外，收集器必须具有唯一的主机名和 IP 地址。否则，检测行为将不可预测。

观察点和观察域

ASA 是一个观察域，每个接口也是一个观察点。通过所有接口创建的流均会导出，且不存在任何用于限制或将导出数据过滤到特定接口集的选项。连接到 ASA 的外部设备创建的流也会导出。

流过滤

例如，可能仅需导出特定流的记录，例如，ASA 可以为匹配 ACE 的流生成 NSEL 事件。您可以使用此方法限制为 NetFlow 生成的 NSEL 事件的数量。此实施支持根据流量和事件类型通过模块化策略框架过滤 NSEL 事件，并将记录发送到不同的收集器。

例如，对于两个收集器，您可以执行以下操作:

- 将所有流创建事件记录到收集器 1。
- 将与 ACL1 匹配的所有流拒绝事件记录到收集器 1。
- 将与 ACL1 匹配的所有事件记录到收集器 2。

如果没有为 NetFlow 配置模块化策略框架，则不会生成任何 NSEL 事件。

数据字段

表 2 列出通过 NSEL 从 ASA 中导出的数据元素。通过整合为导致 NSEL 记录导出的事件生成的系统日志消息导出的数据，即可生成所需数据元素的列表。

注 NetFlow 使用 IFC SNMP IF 索引报告基于 vpifNum 的接口。但是， vpifnum 没有有效的身份接口值。因此，从 ASA 版本 8.0 起，对于导出的 NetFlow 记录，接口身份号显示为 65535。

这些列包括以下信息:

- ID — 代表字段类型的唯一名称
- TYPE — 为此字段类型分配的值
- LEN — 为所选部分导出的记录中的字段长度 ASA
- DESC — 对字段类型所代表的含义的说明

表 2 已通过 NSEL 导出数据记录

ID	类型	LEN	说明
连接 ID 字段			
NF_F_CONN_ID	148	4	设备的唯一流标识符
流 ID 字段 (L3 IPv4)			
NF_F_SRC_ADDR_IPV4	8	4	源 IPv4 地址
NF_F_DST_ADDR_IPV4	12	4	目的 IPv4 地址
NF_F_PROTOCOL	4	1	IP 值
流 ID 字段 (L3 IPv6)			
NF_F_SRC_ADDR_IPV6	27	16	源 IPv6 地址
NF_F_DST_ADDR_IPV6	28	16	目的 IPv6 地址
流 ID 字段 （L4）			
NF_F_SRC_PORT	7	2	源端口
NF_F_DST_PORT	11	2	目标端口
NF_F_ICMP_TYPE	176	1	ICMP 类型值
NF_F_ICMP_CODE	177	1	ICMP 代码值
NF_F_ICMP_TYPE_IPV6	178	1	ICMP IPv6 类型值
NF_F_ICMP_CODE_IPV6	179	1	ICMP IPv6 代码值
流 ID 字段 （INTF）			
NF_F_SRC_INTF_ID	10	2	入口 IFC SNMP IF 索引
NF_F_DST_INTF_ID	14	2	出口 IFC SNMP IF 索引
映射的流 ID 字段 （第 3 层 IPv4）			
NF_F_XLATE_SRC_ADDR_IPV4	225	4	发布 NAT 源 IPv4 地址
NF_F_XLATE_DST_ADDR_IPV4	226	4	发布 NAT 目标 IPv4 地址
NF_F_XLATE_SRC_PORT	227	2	发布 NATT 源传输端口
NF_F_XLATE_DST_PORT	228	2	发布 NATT 目标传输端口

表 2 已通过 NSEL 导出数据记录 （续）

ID	类型	LEN	说明
已映射流 ID 字段 (L3 IPv6)			
NF_F_XLATE_SRC_ADDR_IPV6	281	16	发布 NAT 源 IPv6 地址
NF_F_XLATE_DST_ADDR_IPV6	282	16	发布 NAT 目标 IPv6 地址
状态或事件字段			
NF_F_FW_EVENT	233	1	高级别事件代码。值如下所示: • 0 — 默认值 （忽略） • 1 — 已创建流 • 2 — 已删除流 • 3 — 流被拒绝 • 4 — 流警报 • 5 — 流更新
NF_F_FW_EXT_EVENT	33002	2	扩展事件代码。这些值提供该事件的其他信息。
时间戳和统计信息字段			
NF_F_EVENT_TIME_MSEC	323	8	事件发生的时间，来自 IPFIX。使用 324 表示以微秒为单位的时间， 325 表示以毫微秒为单位的时间。时间已被计为毫秒，自 0000 UTC 1 月 1 日 1970。
NF_F_FLOW_CREATE_TIME_MSEC	152	8	创建流的时间，此时间包含在未提前发送流创建事件的扩展流断开事件中。流持续时间可以用事件时间来确定流断开和流创建时间。
NF_F_FWD_FLOW_DELTA_BYTES	231	4	从源到目标的增量字节数。
NF_F_REV_FLOW_DELTA_BYTES	232	4	从目标到源的增量字节数。
ACL 字段			
NF_F_INGRESS_ACL_ID	33000	12	已允许或拒绝流的输入 ACL 所有 ACL ID 均由以下三个四字节值组成: • ACL 名称的散列值或 ID • ACL 内的 ACE 的散列值、 ID 或行 • 扩展 ACE 配置的散列值或 ID
NF_F_EGRESS_ACL_ID	33001	12	已允许或拒绝流的输出 ACL
AAA 字段			
NF_F_USERNAME	4 万	20	AAA 用户名
NF_F_USERNAME_MAX	4 万	65	允许的最大大小的 AAA 用户名

事件 ID 字段

“ 事件 ID” 字段描述导致 NSEL 记录的事件。表 3 列出事件 ID 值。

表 3　　事件 ID 值

事件 ID	说明
0	忽略 — 此值表示字段必须被忽略，并且不会在当前版本中使用。
1	流已创建 — 此值表示已创建新流。
2	流已删除 — 此值表示已删除流。
3	流被拒绝 — 此值表示流被拒绝。
5	流已更新 — 此值表示流计时器已关闭或流已断开。

扩展事件 ID 字段

扩展事件 ID 提供有关特定事件的其他信息。此字段包含产品特定的字段 ID (33002)。表 4 列出扩展事件 ID 值。

表 4　　扩展事件 ID 值

扩展事件 ID	事件	说明
0	忽略	此值表示必须忽略该字段。
> 1000 人	流被拒绝	大于 1000 的值表示流被拒绝的各种原因。
1001	流被拒绝	流被入口 ACL 拒绝。
1002	流被拒绝	流被出口 ACL 拒绝。
1003	流被拒绝	可能的原因包括: • 尝试连接到 ASA 接口被拒绝。 • 发送到设备的 ICMP 数据包被拒绝。 • 发送到设备的 ICMPv6 数据包被拒绝。
1004	流被拒绝	TCP 上的第一个数据包不是 TCP SYN 数据包。
> 2000	已删除流	大于 2000 的值表示流被终止的各种原因。

事件时间字段

每个 NSEL 数据记录均具有事件时间字段 (NF_F_EVENT_TIME_MSEC)，即事件发生的时间（以毫秒为单位）。 NetFlow 数据包可能包含多个事件 ; 但是，发送数据包的时间并不代表事件发生的时间，因为 NetFlow 服务会等待多个事件将 NetFlow 数据包打包。

注　流生命周期中的不同事件可能会使用单独的 NetFlow 数据包发出，并且可能会无序到达收集器中。例如，包含流断开事件的数据包可能会在包含流创建事件的数据包之前到达收集器。因此，收集器应用使用 “ 事件时间 ” 字段来关联事件，这一点非常重要。

数据记录和模板

模板描述通过 NetFlow 导出的数据记录的格式。每个流事件都有多种记录格式或与之关联的模板:

- 不同的事件有不同的模板。
- 每种事件类型下的 IPv4 和 IPv6 流都有不同的模板。
- 每种事件类型下的 IPV44、 IPV46、 IPV64 和 IPV66 流都有不同的模板。
- 流创建事件具有不同的模板，这些模板基于与流关联的用户名字段的大小。由于字符串字段的大小在 NetFlow 中固定不变，因此需要不同的模板。如果某个模板的字符串结果具有最大可能大小，则会浪费带宽，因为大多数字符串的长度比最大值要短得多。系统中已定义两种类型的用户名字段，这会导致每个类别都有两种类型的模板。
  - 用户名的常用用户名大小 （少于 20 个字符）
  - 用户名的最大用户名大小 （最多 65 个字符）
  - 每个模板都具有 “ 事件类型 ” 和 “ 扩展事件类型 ” 字段，这些字段可以对事件进行解析或操作。
- “ 流被拒绝 ” 和 “ 流删除 ” 事件具有 IPV46 和 IPV64 模板。其中，目标 IP 地址已由 NAT 规则转换，但源 IP 地址尚未由 NAT 规则转换。这会导致源 IP 地址和目标 IP 地址之间的 IP 版本不同。源 NAT 和目标 NAT 规则不会同时应用 （首先应用目标 NAT 规则），因此在应用两个 NAT 规则或仅有一个 NAT 规则可用时，可以生成 NetFlow 记录。

  流创建和延迟的流创建事件无需使用这些部分 NAT 转换模板，因为源和目标 IP 地址均需具有相同的 IP 版本，才能创建流。

注　模板定义均会发送到所有收集器，您应使用这些 ID 和定义来解析数据记录。

流创建事件的模板

流创建事件表示 ASA 已创建流。此事件也是 ASA 允许的流的日志。表 5 介绍用于流创建事件的模板。

表 5　　流创建事件的模板

说明	字段
使用常见用户名大小 （20 个字符）的 IPv44 流创建事件	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV4, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV4, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME
使用常见用户名大小 （65 个字符）的 IPv44 流创建事件	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV4, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV4, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME_MAX
使用常见用户名大小 （20 个字符）的 IPv66 流创建	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV6, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV6, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE_IPV6, NF_F_ICMP_CODE_IPV6, NF_F_XLATE_SRC_ADDR_IPV6, NF_F_XLATE_DST_ADDR_IPV6, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME

表 5　　流创建事件的模板 （续）

说明	字段
使用最大用户名大小 （65 个字符）的 IPv66 流创建	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV6, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV6, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE_IPV6, NF_F_ICMP_CODE_IPV6, NF_F_XLATE_SRC_ADDR_IPV6, NF_F_XLATE_DST_ADDR_IPV6, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME_MAX
使用常见用户名大小 （20 个字符）的 IPv46 流创建	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV4, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV4, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_XLATE_SRC_ADDR_IPV6, NF_F_XLATE_DST_ADDR_IPV6, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME
使用常见用户名大小 （65 个字符）的 IPv46 流创建事件	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV4, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV4, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_XLATE_SRC_ADDR_IPV6, NF_F_XLATE_DST_ADDR_IPV6, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME_MAX

表 5　　流创建事件的模板 （续）

说明	字段
使用常见用户名大小 （20 个字符）的 IPv64 流创建	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV6, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV6, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE_IPV6, NF_F_ICMP_CODE_IPV6, NF_F_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME
使用最大用户名大小 （65 个字符）的 IPv64 流创建	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV6, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV6, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE_IPV6, NF_F_ICMP_CODE_IPV6, NF_F_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME_MAX

流创建事件的延迟

对于短暂的流， NetFlow 收集设备无需处理两个事件：流创建和断开，只需处理单个事件即可，受益匪浅。因此，系统提供了一个可配置的 CLI 参数来延迟发送流创建事件。如果计时器触发，则发送流创建事件。但是，如果流在计时器到期之前被断开，则*只*发送流断开事件，不发送流创建事件。

流断开事件将会扩展并包括该流的所有信息；信息不会丢失。引入了新的模板，以容纳扩展的流断开事件。

扩展流断开事件的模板

表 6 介绍用于扩展流断开事件的模板。

表 6　　扩展流断开事件的模板

说明	字段
使用常见用户名大小（20 个字符）的扩展 IPv44 流断开	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV4, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV4, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME
使用最大用户名大小的扩展 IPv44 流断开（65 个字符）	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV4, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV4, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC,NF_F_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME_MAX
使用常见用户名大小（20 个字符）的扩展 IPv66 流断开	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV6, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV6, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE_IPV6, NF_F_ICMP_CODE_IPV6, NF_F_XLATE_SRC_ADDR_IPV6, NF_F_XLATE_DST_ADDR_IPV6, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME
使用最大用户名大小（65 个字符）的扩展 IPv66 流断开	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV6, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV6, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE_IPV6, NF_F_ICMP_CODE_IPV6, NF_F_XLATE_SRC_ADDR_IPV6, NF_F_XLATE_DST_ADDR_IPV6, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME_MAX

表 6　　扩展流断开事件的模板 （续）

使用常见用户名大小（20 个字符）的扩展 IPv46 流断开	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV4, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV4, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_XLATE_SRC_ADDR_IPV6, NF_F_XLATE_DST_ADDR_IPV6, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME
使用最大用户名大小（65 个字符）的扩展 IPv46 流断开	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV4, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV4, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_XLATE_SRC_ADDR_IPV6, NF_F_XLATE_DST_ADDR_IPV6, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC,NF_F_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME_MAX
使用常见用户名大小（20 个字符）的扩展 IPv64 流断开	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV6, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV6, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE_IPV6, NF_F_ICMP_CODE_IPV6, NF_F_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME
使用最大用户名大小（65 个字符）的扩展 IPv64 流断开	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV6, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV6, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE_IPV6, NF_F_ICMP_CODE_IPV6, NF_F_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME_MAX

流拒绝事件的模板

流拒绝事件表示流已被拒绝。表 7 介绍用于流拒绝事件的模板。

表 7　　流拒绝事件的模板

说明	字段
IPv44 流被拒绝	NF_F_SRC_ADDR_IPV4, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV4, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID
IPv4 流被拒绝，不存在 xlate 字段	NF_F_SRC_ADDR_IPV4, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV4, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID
IPv66 流被拒绝	NF_F_SRC_ADDR_IPV6, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV6, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE_IPV6, NF_F_XLATE_SRC_ADDR_IPV6, NF_F_XLATE_DST_ADDR_IPV6, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_ICMP_CODE_IPV6, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID
IPv6 流被拒绝，不存在 xlate 字段	NF_F_SRC_ADDR_IPV6, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV6, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE_IPV6, NF_F_ICMP_CODE_IPV6, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID
IPv46 流被拒绝	NF_F_SRC_ADDR_IPV4, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV4, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_XLATE_SRC_ADDR_IPV6, NF_F_XLATE_DST_ADDR_IPV6, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID
IPv46 流被拒绝，无源转换	NF_F_SRC_ADDR_IPV4, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV4, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV6, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID

表 7　　流拒绝事件的模板 （续）

说明	字段
IPv64 流被拒绝	NF_F_SRC_ADDR_IPV6, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV6, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE_IPV6, NF_F_ICMP_CODE_IPV6, NF_F_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID
IPv64 流被拒绝，无源转换	NF_F_SRC_ADDR_IPV6, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV6, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE_IPV6, NF_F_ICMP_CODE_IPV6, NF_F_XLATE_SRC_ADDR_IPV6, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID

流断开事件的模板

流断开事件表示流已终止。表 8 介绍用于流断开事件的模板。

表 8　　流断开事件的模板

说明	字段
IPv44 流断开	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV4, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV4, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC
IPv66 流断开	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV6, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV6, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE_IPV6, NF_F_ICMP_CODE_IPV6, NF_F_XLATE_SRC_ADDR_IPV6, NF_F_XLATE_DST_ADDR_IPV6, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC

表 8　　流断开事件的模板 （续）

说明	字段
IPv46 流断开	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV4, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV4, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_XLATE_SRC_ADDR_IPV6, NF_F_XLATE_DST_ADDR_IPV6, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC
IPv46 流断开，无源转换	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV4, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV4, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV6, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC
IPv64 流断开	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV6, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV6, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE_IPV6, NF_F_ICMP_CODE_IPV6, NF_F_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC
IPv64 流断开，无源转换	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV6, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV6, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE_IPV6, NF_F_ICMP_CODE_IPV6, NF_F_XLATE_SRC_ADDR_IPV6, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC

流更新事件的模板

流更新事件表示流的流更新计时器已关闭或流被断开。此事件充当流量的定期字节计数器。流更新事件还使用与流断开事件相同的模板，不包括部分 NAT 转换的相同模板。NF_F_FWD_FLOW_DELTA_BYTES 和 NF_F_REV_FLOW_DELTA_BYTES 字段包含自上一个计时器间隔以来的字节计数。 NF_F_FW_EXT_EVENT 字段未使用，且在流更新记录中将被忽略。有关用于流断开事件的模板，请参阅表 8。

流更新 （在计时器时）和流更新 （损毁）事件

ASA 为通过它的流设置流更新计时器，当计时器熄灭时， NSEL 问题流将更新 （在计时器中）记录。如果配置的时间间隔内没有流的活动，则不会为该间隔发送任何流更新 （在计时器中）记录。流更新 （正在损毁）记录通过流断开记录发送，以在最后时间间隔内捕获流量。如果在流量上没有最后间隔的流量，则不发送任何流量更新 （正在损毁）记录。此外，对于短期流（即，如果在发生第一个流更新 （在计时器）事件发生之前进行的断开），不会发送任何流量更新 （正在断开）记录。

系统未设置流更新计时器。如果在流创建时未配置流更新收集器，则系统不会再次设置计时器；如果在流更新事件期间，则会删除流更新收集器。在这些情况下，不会再次看到任何流更新（在计时器中）事件或流更新 （在断开时）事件。

流更新记录和故障转移

在进行故障转移之前和之后，尝试保持流更新记录保持一致。发生故障转移后，所有流更新记录都基于先前主用 ASA 的上次更新。只要流量流动，就会每 15 秒进行一次更新。如果故障转移对在不同时间处于开启状态，或者在主用 ASA 有机会向备用 ASA 发送更新之前发生故障转移，则流更新记录可能会不准确。

流更新事件和群集

对于流更新事件如何与故障转移进行交互以及如何与群集交互，会发生一个重大分歧。在群集中，在所有权更改之前，流导向器具有原始流的存根流副本，不会设置活动的刷新计时器。只有在原始流所有者关闭后，才会生成完整的流复制并设置活动的刷新计时器。这意味着在流更新计时器在原始流所有者上断开以及流更新计时器在新流所有者上断开之间，很有可能会发生明显的时间偏移。

当群集中的流量所有权更改后，所有流更新记录都基于流量导向器接收的上次更新。只要有流量，就会每 15 秒更新一次流信息。维护最新的流信息所使用的方法与为故障转移提供的方法相同。

NetFlow 和故障转移

NetFlow 数据记录和模板仅从主用 - 备用故障转移对的主用 （主）ASA 中发送。备用 （辅助）ASA 不会发送任何 NetFlow 相关信息。但在故障转移后，辅助 ASA 开始发送任何已复制流或新流的模板和 NetFlow 记录。在两个 ASA 之间，每个 NetFlow 收集器连接的源 IP 地址都是相同的，但源端口会有所不同。这意味着 NetFlow 收集器能够区分从主设备和辅助设备发送的数据包。

在主用 - 主用故障转移对中，两个 ASA 可以同时发送 NetFlow 数据记录和模板。每个场景只有主用设备发送 NetFlow 数据包，但备用设备不会发送，与主用 - 备用场景非常相似。对于 ASA 情景及其副本，每个 NetFlow 收集器连接的源 IP 地址都是相同的，但源端口会有所不同。

故障转移对中的每个 ASA 节点 （情景）均会自行建立与 NetFlow 收集器的连接，并独立通告其模板。该收集器使用数据包的源 IP 地址和源端口区分 NetFlow 导出器。

NetFlow 和群集

管理接口和常规数据接口均支持 NetFlow。但是，我们建议使用管理接口。仅在管理接口上配置 NetFlow 收集器连接之后，群集中的每台 ASA 均会使用其各自的每台设备的源 IP 地址和源端口发送 NetFlow 数据包。 NetFlow 可用于第 2 层模式和第 3 层模式下的两个数据接口。对于第 2 层模式下的数据接口，群集中的每个 ASA 都有相同的源 IP 地址，但源端口不同。虽然第 2 层模式旨在使群集显示为单个设备，但 NetFlow 收集器可以区分群集中的不同节点。对于第 3 层模式下的数据接口， NetFlow 的工作方式与管理专用接口的操作方式相同。

群集中的每个 ASA 节点均会自行建立与 NetFlow 收集器的连接，并独立通告其模板。该收集器使用数据包的源 IP 地址和源端口区分 NetFlow 导出器。

通过 CLI 对设备字段进行解码

要对 ASA 填充的某些字段值进行解码，可能需要直接与设备进行交互。建议您使用动态机制（例如， *expect* 脚本）从发出事件的设备的 CLI 获取所需的信息。

该设备支持控制台、 Telnet 和 SSH 安全外壳访问。但由于性能和安全性，建议使用 SSH 方法。

接口 ID 字段

您还可以使用来自设备接口 MIB 的 SNMP GET 请求解码接口 ID 字段。这是具有 MIB 支持的唯一字段。

您可以使用 **show interface detail** 命令获取设备上所有接口的列表。此输出在每个接口下包含一行，对应于在 NetFlow 字段中发送的接口 ID 值。在以下示例中，接口编号为 8。

```
ciscoasa(config)# show interface filter-outside detail
Interface GigabitEthernet4/3 "filter-outside", is up, line protocol is up
Hardware is i82571EB 4CU rev06, BW 1000 Mbps, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
MAC address 0015.1715.59 c7, MTU 1500
IP address 209.165.200.254, subnet mask 255.255.255.224
532594 packets input, 88376018 bytes, 0 no buffer
Received 3 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 L2 decode drops
675393 packets output, 53208679 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
input queue (curr/max packets): hardware (36/511) software (0/0)
output queue (curr/max packets): hardware (59/68) software (0/0)
Traffic Statistics for "filter-outside":
532594 packets input, 78636500 bytes
675393 packets output, 40866215 bytes
10837 packets dropped
1 minute input rate 0 pkts/sec, 0 bytes/sec
1 minute output rate 0 pkts/sec, 0 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 0 pkts/sec, 0 bytes/sec
5 minute output rate 0 pkts/sec, 0 bytes/sec
5 minute drop rate, 0 pkts/sec
Control Point Interface States:
Interface number is 8
Interface config status is active
Interface state is active
```

ACL ID 字段

12 个字节的原始 ACL ID 必须分为三个组成部分，如下所示：

- 前四个字节是 ACL 名称 ID。
- 接下来的四个字节是 ACL 条目 ID (ACE)/ 对象组 ID。
- 最后四个字节是扩展 ACL 条目 ID。

可以从 ASA 的 **show access-list** 命令的输出中查找这些单独的值。 ACL 名称 ID 在此输出的 ACL 第一行的末尾。 ACE ID 在每个单独的 ACL 条目行的末尾。

注 如果在访问列表中使用对象组，则第二个四字节 ID 实际上不是 ACE ID，而是对象组 ID。扩展 ACE ID （最后四字节部分）是指实际的单个 ACL 条目 ID。以下示例显示了这些条目：

```
ciscoasa  (config) # show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
access-list foo; 2 elements; name hash: 0x102154c1
access-list foo line 1 extended permit tcp object-group host_grp_1 any eq www 0xd0e5806e
access-list foo line 1 extended permit tcp host 209.165.200.254 any eq www (hitcnt=4)
0x7e5ad93b
access-list foo line 1 extended permit tcp host 209.165.201.1 any eq www (hitcnt=0)
0xe0c1846b
access-list bar; 1 elements; name hash: 0x5da9bb69
access-list bar line 1 extended deny tcp any any (hitcnt=41) 0x84434b4b
```

此示例类似于示例 2：使用 PAT 接口的出口的拒绝流所示的示例。在被拒绝的流示例中，ACL ID 分为多个组成部分，如下所示：

- NF_F_INGRESS_ACL_ID: InAcl: 0x102154c1d0e5806e7e5ad93b

  其中， 0x102154c1 是前四个字节， 0xd0e5806e 是第二个四个字节， 0x7e5ad93b 是最后四个字节。

- NF_F_EGRESS_ACL_ID: 0x5da9bb6984434b4b00000000

  其中， 0x5da9bb69 是前四个字节， 0x84434b4b 是第二个四个字节， 0x00000000 是最后四个字节。

注 其中每个 ID 对应于 **show access list** 命令示例中的行。

从这些 ID 中，您可以推断出已在输入接口上应用访问列表 *foo* ，且已在输出接口上应用访问列表 *bar*。这些信息也可通过 **show run access-group** 命令获取，但这些 ACL ID 的额外益处在于：您可以识别导致允许或拒绝操作的单个 ACE。由于此流在出口上被拒绝 （通过扩展事件代码确定），因此您知道入口 ACL ID 标识允许流的 ACE 行，且出口 ACL ID 标识拒绝流的 ACE。

事件代码

您必须将事件代码硬编码至收集器中，因为 ASA 仅发布四种不同的高级事件类型（创建、断开、拒绝和更新）。

扩展事件代码

在四个高级事件代码中，只有两个有扩展事件代码：“ 流拒绝 ” 和 “ 流断开 ” 事件类型。对于流拒绝事件，表 4 的扩展事件代码列表应当足以确定流被拒绝的原因。但是，对于流断开事件，此文档中会列出过多的事件代码，并且也会列出相当多的原因。

NSEL 指南

支持的功能

- IPv6 用于 **class-map**、 **match access-list** 和 **match any** 命令。
- 仅限 UDP 负载。

其他规定

- 如果您先前已使用 **flow-export enable** 命令配置流导出操作，且已升级到更高版本，则配置会自动转换为新的模块化策略框架 **flow-export event-type** 命令，该命令在 **policy-map** 命令下进行了说明。
- 如果先前已使用 **flow-export event-type all** 命令配置流导出操作，且已升级到更高版本，则 NSEL 会根据需要自动开始发布流更新记录。
- 基于接口的策略中不支持流导出操作。只能使用 **match access-list**、 **match any** 或 **class-default** 命令在类映射中配置流导出操作。只能在全局服务策略中应用流导出操作。
- 您必须使用威胁检测功能查看 NetFlow 记录的带宽使用情况 （无法实时获得）。
- 请确保在 NetFlow 配置中分配唯一的 IP 地址和主机名。
- 有关实施的更多详细信息，请参阅以下文章:
  - https://supportforums.cisco.com/docs/DOC-6113
  - https://supportforums.cisco.com/docs/DOC-6114

配置 NSEL 收集器 (CLI)

您必须具有至少一个已配置的收集器，才能使用 NSEL，并且必须先配置 NSEL 收集器，然后才能通过模块化策略框架配置过滤器。

要配置 NSEL 收集器，请执行以下步骤:

程序

步骤 1 添加可向其发送 NetFlow 数据包的 NSEL 收集器。

flow-export destination *interface-name ipv4-address | hostname udp-port*

示例:

```
ciscoasa(config)# flow-export destination inside 209.165.200.225 2002
```

destination 关键字表示正在配置 NSEL 收集器。 *interface-name* 参数是可以通过其收集器访问的 ASA 和 ASA 服务模块 接口的名称。 *ipv4-address* 参数是运行收集器应用的计算机的 IP 地址。 *hostname* 参数是收集器的目标 IP 地址或名称。 *udp-port* 参数是 NetFlow 数据包发送到的 UDP 端口号。

您最多可以配置五个收集器。配置收集器后，模板记录会自动发送到所有已配置的 NSEL 收集器。

注　请确保收集器应用使用 " 事件时间 " 字段来关联事件。

步骤 2　重复第一步以配置更多收集器。

通过模块化策略框架配置流导出操作

要通过模块化策略框架配置流导出操作。请执行以下步骤:

程序

步骤 1　定义用于标识需要导出 NSEL 事件的流量的类映射。

class-map *flow_export_class*

示例:

```
ciscoasa(config-pmap)# class-map flow_export_class
```

Flow_export_class 参数是类映射的名称。

步骤 2　选择以下选项之一:

- 配置 ACL 以匹配特定流量。

  match access-list *flow_export_acl*

  示例:

  ```
  ciscoasa(config-cmap)# match access-list flow_export_acl
  ```

  flow_export_acl 参数是 ACL 的名称。

- 匹配任何流量。

  match any

  示例:

  ```
  ciscoasa(config-cmap)# match any
  ```

步骤 3　定义策略映射，以将流导出操作应用于已定义的类。

policy-map *flow_export_policy*

示例:

```
ciscoasa(config)# policy-map flow_export_policy
```

Flow_export_policy 参数是策略映射的名称。

如果创建新的策略映射，并根据将其全局应用步骤 6，则会停用剩余的检查策略。

或者，在 **policy map global_policy** 命令后输入 **class flow_export_class** 命令，以在现有策略中插入 NetFlow 类。

有关创建或修改模块化策略框架的详细信息，请参阅防火墙配置指南。

步骤 4 定义要应用流导出操作的类。

class *flow_export_class*

示例：

```
ciscoasa(config-pmap)# class flow_export_class
```

Flow_export_class 参数是类的名称。

步骤 5 配置流导出操作。

flow export event-type *event-type* **destination** *flow_export_host1* [*flow_export_host2*]

示例：

```
ciscoasa(config-pmap-c)# flow-export event-type all destination 209.165.200.230
```

Event_type 关键字是过滤的受支持事件的名称。 **Destination** 关键字是已配置的收集器的 IP 地址。 *Flow_export_host* 参数是主机的 IP 地址。

步骤 6 全局添加服务策略。

service-policy *flow_export_policy* **global**

示例：

```
ciscoasa(config)# service-policy flow_export_policy global
```

Flow_export_policy 参数是策略映射的名称。

配置模板超时间隔

要配置模板超时间隔，请执行以下步骤：

程序

步骤 1 指定将模板记录发送到所有已配置的输出目标的时间间隔。

flow-export template timeout-rate *minutes*

示例：

```
ciscoasa(config)# flow-export template timeout-rate 15
```

template 关键字表示特定于模板的配置。 **Timeout rate** 关键字指定重新发送模板之前的时间。 *minutes* 参数指定重新发送模板的时间间隔 （以分钟为单位）。默认值为 30 分钟。

更改将流更新事件发送到收集器的时间间隔

要更改将流更新事件发送到收集器的时间间隔，请执行以下步骤:

程序

步骤 1 为活动连接配置 NetFlow 参数。

flow-export active refresh-interval *value*

示例:

```
ciscoasa(config)# flow-export active refresh-interval 30
```

value 参数指定在流更新事件之间的时间间隔 （以分钟为单位）。有效值为 1 到 60 分钟。默认值为 1 分钟。

如果已配置 **flow-export delay flow-create** 命令，然后使用比延迟值长不到 5 秒的间隔值来配置 **flow-export active refresh-interval** 命令，则在控制台上显示以下警告消息:

```
WARNING: The current delay flow-create value configuration may cause flow-update events to
appear before flow-creation events.
```

如果已配置 **flow-export active refresh-interval** 命令，然后使用比间隔值长不到 5 秒的延迟值来配置 **flow-export delay flow-create** 命令，则在控制台上显示以下警告消息:

```
WARNING: The current delay flow-create value configuration may cause flow-update events to
appear before flow-creation events.
```

延迟发送流创建事件

要延迟发送流创建事件，请执行以下步骤:

程序

步骤 1 按指定的秒数延迟发送流创建事件。

flow-export delay flow-create *seconds*

示例:

```
ciscoasa(config)# flow-export delay flow-create 10
```

Seconds 参数 表示延迟允许的时间量 （以秒为单位）。如果未配置此命令，则不会延迟，并会在创建流后立即导出流创建事件。如果流在配置的延迟时间之前中断，则不会发送流创建事件，而是会发送延期流断开事件。

禁用和重新启用与 NetFlow 相关的系统日志消息

要禁用和重新启用与 NetFlow 相关的系统日志消息，请执行以下步骤：

程序

步骤 1 禁用因 NSEL 而变得冗余的系统日志消息。

logging flow-export-syslogs disable

示例：

```
ciscoasa(config)# logging flow-export-syslogs disable
```

注 虽然您在全局配置模式下执行此命令，但它不会存储在配置中。只有 **no logging message** *xxxxxx* 命令才存储于配置中。

步骤 2 单独重新启用系统日志消息，其中 *xxxxxx* 是要重新启用的指定系统日志消息。

logging message *xxxxxx*

示例：

```
ciscoasa(config)# logging message 302013
```

步骤 3 同时重新启用所有 NSEL 事件。

logging flow-export-syslogs enable

示例：

```
ciscoasa(config)# logging flow-export-syslogs enable
```

重置运行时计数器

要重置运行时计数器，请执行以下步骤：

程序

步骤 1 将 NSEL 的所有运行时计数器重置为零。

clear flow-export counters

示例：

```
ciscoasa# clear flow-export counters
```

启用 NetFlow (ASDM)

要启用 NetFlow，请执行以下步骤:

程序

步骤 1 选择**配置** > **设备管理** > **日志记录** > **NetFlow**。

步骤 2 输入模板超时速率，即将模板记录发送到所有已配置收集器的间隔 （以分钟为单位）。默认值为 30 分钟。

步骤 3 输入流更新间隔，指定流更新事件之间的时间间隔 （以分钟为单位）。有效值为 1 到 60 分钟。默认值为 1 分钟。

步骤 4 选中 “ **延迟导出短期流的流创建事件** ” 复选框，然后在延迟**方式** （**delay By** ） 字段中输入延迟以延迟导出流创建事件，并处理单个流断开事件而不是流创建事件和流断开事件，

步骤 5 指定将向其发送 NetFlow 数据包的收集器。您最多可以配置五个收集器。单击**添加**可显示**添加 NetFlow 收集器**对话框以配置收集器，并执行以下步骤:

a. 从下拉列表中选择 NetFlow 数据包将被发送到的接口。

b. 在关联字段中输入 IP 地址或主机名和 UDP 端口号。

c. 单击**确定**。

步骤 6 重复步骤 5 此步骤以配置更多收集器。

步骤 7 启用 NetFlow 后，某些系统日志消息会变得冗余。为了保持系统性能，建议您禁用冗余系统日志消息，因为相同的信息会通过 NetFlow 导出。选中**禁用冗余系统日志消息**复选框以禁用所有冗余系统日志消息。单击**显示冗余系统日志消息**以显示冗余系统日志消息及其状态。

系统将显示**冗余系统日志消息**对话框。**系统日志 ID** 字段显示冗余系统日志消息编号。**已禁用**字段指示指定的系统日志消息是否已禁用。单击 **OK** 以关闭此对话框。

选择**配置** > **设备管理** > **日志记录** > **系统设置**以启用单个冗余系统日志消息。

步骤 8 单击**应用**以保存您的更改，或单击**重置** 以输入新设置。

将 NetFlow 事件与配置的收集器进行匹配

要将 NetFlow 事件与任何已配置的收集器进行匹配，请执行以下步骤:

步骤 1 依次选择配置 > 防火墙 > 服务策略规则。

步骤 2 要添加服务策略规则，请执行以下步骤:

a. 单击**添加**以显示**添加服务策略规则向导**。有关服务策略规则的详细信息，请参阅防火墙配置指南。

b. 单击**全局应用于所有接口**单选按钮 ，将规则应用于全局策略。单击**下一步**。

c. 选中**源和目标 IP 地址 （使用 ACL）**复选框或**任何流量**复选框作为流量匹配条件，或单击**使用 class-default 作为流量类**单选按钮。单击**下一步**继续执行**规则操作**屏幕。

注 NetFlow 操作仅适用于全局服务策略规则，且仅适用于 class-default 流量类以及流量匹配条件为 “ 源和目标 IP 地址 (使用 ACL)” 或 “ 任何流量 ” 的流量类。

步骤 3　单击规则操作屏幕中的 **NetFlow** 选项卡。

步骤 4　单击**添加**以显示**添加流事件**对话框并指定流事件，然后执行以下步骤：

a. 从下拉列表中选择流事件类。可用事件包括已创建、已断开、已被拒绝、已更新或所有的事件。

注　版本 9.0 (1) 中未提供流更新事件。它在版本 8.4 (5) 和 9.1 (2) 及更高版本中可用。

b. 通过选中**发送**列中的对应复选框，选择要向其发送事件的收集器。

c. 单击**管理**以显示**管理 NetFlow 收集器**对话框，您可以在其中添加、编辑或删除收集器，或配置其他 NetFlow 设置 （例如，系统日志消息）。单击**确定**以关闭**管理 NetFlow 收集器**对话框，然后返回到**添加流事件**对话框。有关配置收集器的详细信息，请参阅启用 NetFlow (ASDM)，第 24 页中的步骤 5。

步骤 5　单击**确定**以关闭**添加流事件**对话框，然后返回 **NetFlow** 选项卡。

步骤 6　单击**完成**以退出向导。

步骤 7　要编辑 NetFlow 服务策略规则，请执行以下步骤：

a. 在**服务策略规则**表中选择它，然后单击**编辑**。

b. 单击**规则操作**选项卡，然后单击 **NetFlow** 选项卡。

监控 NSEL

您可以使用系统日志消息来帮助对错误进行故障排除或监控系统使用情况和性能。您可以在单独的窗口中查看已保存在日志缓冲区中的实时系统日志消息，其中包括对消息的说明、有关消息的详细信息以及建议采取的操作 （如有必要），以解决错误。有关详细信息，请参阅系统日志消息和 NSEL 事件，第 2 页。

要监控 NSEL，请输入以下命令之一：

命令	目的
show flow-export counters	显示 NSEL 的运行时间计数器，其中包括统计数据和错误数据。
show logging flow-export-syslogs	列出由 NSEL 事件捕获的所有系统日志消息。
show running-config flow-export	显示当前配置的 NetFlow 命令。
show running-config logging	显示已禁用的系统日志消息，它们是冗余的系统日志消息，因为它们通过 NetFlow 导出相同的信息。

要在 ASDM 中监控 NSEL，请执行以下步骤：

步骤 1　在 ASDM 中，选择**工具 > 命令行界面。**

步骤 2　选择以下选项之一：

- 在**命令**字段中，输入 **show flow export counter** 命令以显示运行时计数器 （其中包括 NSEL 的统计数据和错误数据），然后单击**发送**。
- 在**命令**字段中，输入 **show logging flow-export-syslogs** 命令以列出 NSEL 事件捕获的所有系统日志消息，然后单击**发送**。
- 在**命令**字段中，输入 **show running-config flow-export** 命令以显示当前配置的 NetFlow 命令，然后单击**发送**。
- 在**命令**字段中，输入 **show running-config logging** 命令以显示已禁用的系统日志消息 （这些消息为冗余消息，因为它们通过 NetFlow 导出相同的信息），然后单击**发送**。

NSEL (CLI) 示例

以下示例显示生成事件的流，并包含有关如何在 ASA 中为 NSEL 字段实施收集器支持的信息。

示例 1：使用 PAT 接口允许的流

此示例显示使用 PAT 接口的允许流。输出接口 IP 地址为 209.165.200.225。该用户经身份认证为用户 A。未指定 ACL，但该流为出站流，因此默认情况下允许使用。根据图 1 和提供的说明，将发出流创建事件。

图 1　　使用 PAT 接口允许的流示例

生成的 NSEL 记录将包含以下字段和值：

字段	值
NF_F_CONN_ID	xxxx
NF_F_SRC_ADDR_IPV4	209.165.200.254
NF_F_SRC_PORT	56789
NF_F_SRC_INTF_ID	1
NF_F_DST_ADDR_IPV4	209.165.200.225
NF_F_DST_PORT	80
NF_F_DST_INTF_ID	0
NF_F_PROTOCOL	6
NF_F_ICMP_TYPE	0
NF_F_ICMP_CODE	0
NF_F_XLATE_SRC_ADDR_IPV4	209.165.201.1
NF_F_XLATE_DST_ADDR_IPV4	209.165.200.225
NF_F_XLATE_SRC_PORT	1024
NF_F_XLATE_DST_PORT	80
NF_F_FW_EVENT	1
NF_F_FW_EXT_EVENT	0
NF_F_EVENT_TIME_MSEC	YYYYYYYY
NF_F_INGRESS_ACL_ID	0
NF_F_EGRESS_ACL_ID	0
NF_F_USERNAME	用户 A

示例 2：使用 PAT 接口的出口的拒绝流

此示例显示通过使用 PAT 接口的出口 ACL 所拒绝的流。输出接口 IP 地址为 209.165.200.225。该用户经身份验证为用户 A。输入 ACL (foo) 允许该流，但输出 ACL (bar) 会拒绝该流。输入 ACL (foo) 使用对象组指定：

```
ciscoasa# object-group network host_grp_1
network-object host 209.165.200.254
network-object host 209.165.201.1
ciscoasa(config)# access-list foo extended permit tcp object-group host_grp_1 any eq www
ciscoasa  (config)  # access list bar extended deny tcp any any
ciscoasa(config)# access-group foo in interface inside
ciscoasa(config)# access-group bar out interface outside
```

根据图 1 和提供的说明，将发出流被拒绝事件。

生成的 NSEL 记录将包含以下字段和值：

字段	值
NF_F_SRC_ADDR_IPV4	209.165.200.254
NF_F_SRC_PORT	37518
NF_F_SRC_INTF_ID	7
NF_F_DST_ADDR_IPV4	209.165.200.225
NF_F_DST_PORT	80
NF_F_DST_INTF_ID	8
NF_F_PROTOCOL	6
NF_F_ICMP_TYPE	0
NF_F_ICMP_CODE	0
NF_F_XLATE_SRC_ADDR_IPV4	209.165.201.1
NF_F_XLATE_DST_ADDR_IPV4	209.165.200.225
NF_F_XLATE_SRC_PORT	48264
NF_F_XLATE_DST_PORT	80
NF_F_FW_EVENT	3
NF_F_FW_EXT_EVENT	1002 (egress ACL)
NF_F_EVENT_TIME_MSEC	1187374131808
NF_F_INGRESS_ACL_ID	0x102154c1d0e5806e7e5ad93b
NF_F_EGRESS_ACL_ID	0x5da9bb6984434b4b00000000
NF_F_USERNAME	用户 A

示例 3：过滤 NSEL 事件

这些示例显示如何过滤已配置指定收集器的 NSEL 事件：

- **flow-export destination inside 209.165.200.2055**
- **flow-export destination outside 209.165.201.29 2055**
- **flow-export destination outside 209.165.201.27 2055**

记录主机 209.165.200.224 和主机 209.165.201.224 之间目标为 209.165.200.230 的所有事件，并记录目标为 209.165.201.29 的所有其他事件；

```
ciscoasa (config) # access list flow_export_acl 允许 ip host 209.165.200.224 host
209.165.201.224
ciscoasa(config)# class-map flow_export_class
ciscoasa(config-cmap)# match access-list flow_export_acl
ciscoasa(config)# policy-map flow_export_policy
ciscoasa(config-pmap)# class flow_export_class
ciscoasa(config-pmap-c)# flow-export event-type all destination 209.165.200.230
ciscoasa(config-pmap)# class class-default
ciscoasa(config-pmap-c)# flow-export event-type all destination 209.165.201.29
ciscoasa(config)# service-policy flow_export_policy global
```

记录目标为 209.165.200.230 的流创建事件、目标为 209.165.201.29 的流断开事件、目标为 209.165.201.27 的流被拒绝事件以及目标为 209.165.200.230 的流更新事件:

```
ciscoasa(config)# policy-map flow_export_policy
ciscoasa(config-pmap)# class class-default
ciscoasa (config-pmap) # flow-export event-type flow- 创建 destination 209.165.200.230
ciscoasa(config-pmap-c)# flow-export event-type flow-teardown destination 209.165.201.29
ciscoasa(config-pmap-c)# flow-export event-type flow-denied destination 209.165.201.27
ciscoasa(config-pmap-c)# flow-export event-type flow-update destination 209.165.200.230
ciscoasa(config)# service-policy flow_export_policy global
```

记录主机 209.165.200.224 和 209.165.200.230 之间目标为 209.165.201.29 的所有流创建事件，并记录目标为 209.165.201.27 的所有流被拒绝事件。

```
ciscoasa(config)# access-list flow_export_acl permit ip host 209.165.200.224 host
209.165.200.230
ciscoasa(config)# class-map flow_export_class
ciscoasa(config)# match access-list flow_export_acl
ciscoasa(config)# policy-map flow_export_policy
ciscoasa(config-pmap)# class flow_export_class
ciscoasa (config-pmap) # flow-export event-type flow-create destination 209.165.200.29
ciscoasa(config-pmap-c)# flow-export event-type flow-denied destination 209.165.201.27
ciscoasa(config-pmap)# class class-default
ciscoasa(config-pmap-c)# flow-export event-type flow-denied destination 209.165.201.27
ciscoasa(config)# service-policy flow_export_policy global
```

注　您必须输入以下命令:

```
ciscoasa(config-pmap-c)# flow-export event-type flow-denied destination 209.165.201.27

for flow_export_acl
```

，因为第一次匹配后未检查流量，您必须显式定义该操作以记录与 flow_export_acl 匹配的流被拒绝事件。

记录除主机 209.165.201.27 和 209.165.201.50 之间目标为 209.165.201.27 以外的所有流量:

```
ciscoasa(config)# access-list flow_export_acl deny ip host 209.165.201.27 host
209.165.201.50
ciscoasa(config)# access-list flow_export_acl permit ip any any
ciscoasa(config)# class-map flow_export_class
ciscoasa(config-cmap)# match access-list flow_export_acl
ciscoasa(config)# policy-map flow_export_policy
ciscoasa(config-pmap)# class flow_export_class
ciscoasa(config-pmap-c)# flow-export event-type all destination 209.165.201.27
ciscoasa(config)# service-policy flow_export_policy global
```

NSEL 的历史记录

表 9　　NSEL 的历史记录

功能名称	平台版本	功能信息
NetFlow	8.1(1)	新 NetFlow 功能会通过 NetFlow 协议记录基于流的事件，由此增强了 ASA 日志记录功能。NetFlow 版本 9 服务用于导出从开始到完成的流的进度信息。NetFlow 实施会导出指示流生命周期内重大事件的记录。此实施与传统 NetFlow 不同，后者以固定间隔导出有关流的数据。 NetFlow 模块还会导出有关 ACL 拒绝的流的记录。您可以将 ASA 5580 配置为使用 NetFlow 发送以下事件：流创建、流断开和流被拒绝（仅报告被 ACL 拒绝的流）。 引入了以下命令：**清除流导出计数器、流导出启用、流导出目标、流导出模板超时速率、日志流导出系统日志启用、日志流导出系统日志禁用、显示流量导出计数器，show 日志记录流 - 导出 - 系统日志。** 引入了以下屏幕：配置 > 设备管理 > 日志记录 > NetFlow。
NetFlow 过滤	8.1(2)	您可以根据流量和事件类型过滤 NetFlow 事件，然后将记录发送到不同的收集器。例如，可以将所有流创建事件记录到一个收集器，而将流拒绝的事件记录到另一个收集器。 我们已修改以下命令：**class、class-map、low-export event-type destination、match access-list、 policy-map、 service-policy。** 对于短暂的流， NetFlow 收集器无需处理两个事件：流创建和断开，只需处理单个事件即可，受益匪浅。您可以在发送流创建事件之前配置延迟。如果流在计时器到期之前被断开，则只发送流断开事件。断开事件包括有关流的所有信息；信息不会丢失。 引入了以下命令：**流导出延迟流 - 创建。** 修改了以下屏幕：配置 > 防火墙 > 服务策略规则。
NSEL	8.2(1)	NetFlow 功能已移植到所有可用的 ASA 型号。
群集	9.0(1)	NetFlow 功能支持群集。
NSEL		添加了新的 NetFlow 错误计数器，源端口分配失败。 修改了以下命令：**show flow-export counters。** 版本 9.0 (1) 中不提供流更新事件功能。
NSEL	9.1(2)	引入了 Flow-update 事件，以便定期提供数据流流量的字节计数器。您可以更改系统向 NetFlow 收集器发送 flow-update 事件的时间间隔。您可以对 flow-update 记录被发送到的收集器进行过滤。 引入了以下命令：**flow-export active refresh-interval。** 修改了以下命令：**flow-export event-type。** 修改了以下屏幕：配置 > 防火墙 > 服务策略规则 > 添加服务策略规则向导 - 规则操作 > NetFlow > 添加流事件 配置 > 设备管理 > 日志记录 > NetFlow。