Vérification des modèles et des éléments d'information NetFlow Sensor

Table des matières

- Introduction
- Conditions préalables
- ID de modèle
- Éléments NetFlow standard
- Éléments spécifiques à l'entreprise
- Formats de modèles
  - Premier flux IPv4 - Modèle 317
  - IPv4 First Flow Deep - Modèle 318
  - Flux IPv4 - Modèle 319
  - Événement IPv4 - Modèle 320
  - Premier flux IPv6 - Modèle 321
  - IPv6 First Flow Deep - Modèle 322
  - Flux IPv6 - Modèle 323
  - Événement IPv6 - Modèle 324
  - Nombre d'e-mails source IPv4 - Modèle 325
  - IPv4 First Flow Response Time Monitoring (RTM) - Modèle 326
  - Surveillance approfondie du temps de réponse du premier flux IPv4 - Modèle 327
  - Surveillance du temps de réponse de flux IPv4 - Modèle 328
  - Surveillance du temps de réponse au premier flux IPv6 - Modèle 329
  - Surveillance approfondie du temps de réponse du premier flux IPv6 - Modèle 330
  - Surveillance du temps de réponse de flux IPv6 - Modèle 331
  - Nombre d'e-mails de destination IPv4 - Modèle 332
  - Nombre d'e-mails source IPv6 - Modèle 333
  - Nombre d'e-mails de destination IPv6 - Modèle 334
  - Modèle IPFIX de premier flux IPv4 335
  - IPFIX profond de premier flux IPv4 - Modèle 336
  - IPFIX de flux IPv4 - Modèle 337
  - IPFIX de l'événement IPv4 - Modèle 338
  - IPFIX de premier flux IPv6 - Modèle 339
  - IPFIX profond de premier flux IPv6 - Modèle 340
  - IPFIX de flux IPv6 - Modèle 341
  - IPFIX de l'événement IPv6 - Modèle 342
  - Nombre d'e-mails source IPv4 IPFIX - Modèle 343
  - Surveillance du temps de réponse au premier flux IPv4 - Modèle 344
  - Surveillance approfondie du temps de réponse du premier flux IPv4 - Modèle 345
  - Surveillance du temps de réponse de flux IPv4 IPFIX - Modèle 346

IPv6 First Flow Response Time Monitoring IPFIX - Modèle 347

IPv6 First Flow Deep RTM IPFIX - Modèle 348

Surveillance du temps de réponse de flux IPv6 - Modèle 349

Nombre d'e-mails de destination IPv4 IPFIX - Modèle 350

Nombre d'e-mails source IPv6 IPFIX - Modèle 351

Nombre d'e-mails de destination IPv6 IPFIX - Modèle 352

IPFIX IPv4 ETA Initial Data Packet (IDP) - Modèle 354

IPFIX de séquence ETA IPv4 de longueurs et d'heures de paquets (SPLT) - Modèle 356

IPFIX IPv6 ETA Initial Data Packet (IDP) - Modèle 364

Séquence ETA IPv6 de longueurs et d'heures des paquets (SPLT) IPFIX - Modèle 366

Introduction

Ce document décrit les modèles NetFlow utilisés par le SNA Flow Sensor. Il contient des informations sur les éléments spécifiques à l'entreprise.

Conditions préalables

Les ID d'élément NetFlow utilisés ici sont des protocoles NetFlow standard. Toutefois, les informations du modèle et les éléments inclus dans chaque modèle peuvent être modifiés à tout moment.

ID de modèle

Conseil : À partir de la version 7.3 de l'architecture SNA, le capteur de flux semble envoyer uniquement les ID de modèle 335-352 par défaut, qui sont les modèles IPFIX. Tous les modèles IPFIX sont envoyés ensemble toutes les 60 secondes, quel que soit le type de trafic vu par le port de surveillance du capteur de flux (par exemple IPv4 ou IPv6).

Remarque : Les modèles accompagnés d'un astérisque (*) contiennent les champs NetFlow v9/IPFIX de base de la liste IANA pour la création et l'analyse de flux standard.

```
IPV4_FIRST_FLOW_TEMPLATE_ID                    317*
IPV4_FIRST_FLOW_DEEP_TEMPLATE_ID              318*
IPV4_FLOW_TEMPLATE_ID                          319*
IPV4_EVENT_TEMPLATE_ID                          320
IPV6_FIRST_FLOW_TEMPLATE_ID                    321*
IPV6_FIRST_FLOW_DEEP_TEMPLATE_ID              322*
IPV6_FLOW_TEMPLATE_ID                          323*
IPV6_EVENT_TEMPLATE_ID                          324
IPV4_SRC_EMAIL_COUNTS_TEMPLATE_ID              325
IPV4_FIRST_FLOW_RTM_TEMPLATE_ID                326*
IPV4_FIRST_FLOW_DEEP_RTM_TEMPLATE_ID          327*
```

IPV4_FLOW_RTM_TEMPLATE_ID	328*
IPV6_FIRST_FLOW_RTM_TEMPLATE_ID	329*
IPV6_FIRST_FLOW_DEEP_RTM_TEMPLATE_ID	330*
IPV6_FLOW_RTM_TEMPLATE_ID	331*
IPV4_DST_EMAIL_COUNTS_TEMPLATE_ID	332
IPV6_SRC_EMAIL_COUNTS_TEMPLATE_ID	333
IPV6_DST_EMAIL_COUNTS_TEMPLATE_ID	334
IPV4_FIRST_FLOW_IPFIX_TEMPLATE_ID	335*
IPV4_FIRST_FLOW_DEEP_IPFIX_TEMPLATE_ID	336*
IPV4_FLOW_IPFIX_TEMPLATE_ID	337*
IPV4_EVENT_IPFIX_TEMPLATE_ID	338
IPV6_FIRST_FLOW_IPFIX_TEMPLATE_ID	339*
IPV6_FIRST_FLOW_DEEP_IPFIX_TEMPLATE_ID	340*
IPV6_FLOW_IPFIX_TEMPLATE_ID	341*
IPV6_EVENT_IPFIX_TEMPLATE_ID	342
IPV4_SRC_EMAIL_COUNTS_IPFIX_TEMPLATE_ID	343
IPV4_FIRST_FLOW_RTM_IPFIX_TEMPLATE_ID	344*
IPV4_FIRST_FLOW_DEEP_RTM_IPFIX_TEMPLATE_ID	345*
IPV4_FLOW_RTM_IPFIX_TEMPLATE_ID	346*
IPV6_FIRST_FLOW_RTM_IPFIX_TEMPLATE_ID	347*
IPV6_FIRST_FLOW_DEEP_RTM_IPFIX_TEMPLATE_ID	348*
IPV6_FLOW_RTM_IPFIX_TEMPLATE_ID	349*
IPV4_DST_EMAIL_COUNTS_IPFIX_TEMPLATE_ID	350
IPV6_SRC_EMAIL_COUNTS_IPFIX_TEMPLATE_ID	351
IPV6_DST_EMAIL_COUNTS_IPFIX_TEMPLATE_ID	352
IPV4_ETTA_IDP_TEMPLATE_ID	353
IPV4_ETTA_IDP_IPFIX_TEMPLATE_ID	354
IPV4_ETTA_SPLT_TEMPLATE_ID	355
IPV4_ETTA_SPLT_IPFIX_TEMPLATE_ID	356
IPV4_ETTA_BD_TEMPLATE_ID	357
IPV4_ETTA_BD_IPFIX_TEMPLATE_ID	358
IPV4_ETTA_TLS_TEMPLATE_ID	359
IPV4_ETTA_TLS_IPFIX_TEMPLATE_ID	360
IPV4_ETTA_SALT_TEMPLATE_ID	361
IPV4_ETTA_SALT_IPFIX_TEMPLATE_ID	362
IPV6_ETTA_IDP_TEMPLATE_ID	363
IPV6_ETTA_IDP_IPFIX_TEMPLATE_ID	364
IPV6_ETTA_SPLT_TEMPLATE_ID	365
IPV6_ETTA_SPLT_IPFIX_TEMPLATE_ID	366
IPV6_ETTA_BD_TEMPLATE_ID	367
IPV6_ETTA_BD_IPFIX_TEMPLATE_ID	368
IPV6_ETTA_TLS_TEMPLATE_ID	369
IPV6_ETTA_TLS_IPFIX_TEMPLATE_ID	370
IPV6_ETTA_SALT_TEMPLATE_ID	371
IPV6_ETTA_SALT_IPFIX_TEMPLATE_ID	372

Éléments NetFlow standard

NF_F_IN_BYTES	1
NF_F_IN_PKTS	2
NF_F_PROTOCOL	4
NF_F_SRC_TOS	5
NF_F_TCP_FLAGS	6
NF_F_L4_SRC_PORT	7
NF_F_SRC_ADDR_IPV4	8
NF_F_SRC_INTF_ID	10
NF_F_L4_DST_PORT	11

NF_F_DST_ADDR_IPV4	12
NF_F_DST_INTF_ID	14
NF_F_LAST_SWITCHED	21
NF_F_FIRST_SWITCHED	22
NF_F_SRC_ADDR_IPV6	27
NF_F_DST_ADDR_IPV6	28
NF_F_MIN_TTL	52
NF_F_IN_SRC_MAC	56
NF_F_OUT_DST_MAC	57
NF_F_SRC_VLAN	58
NF_F_MPLS_LABEL_1	70
NF_F_SYSTEM_INIT_TIME_MILLISECONDS	160
NF_F_TCP_SYN_TOTAL_COUNT	218
NF_F_TCP_FIN_TOTAL_COUNT	219
NF_F_TCP_RST_TOTAL_COUNT	220
NF_F_TCP_ACK_TOTAL_COUNT	222
NF_F_IP_SECTION_HEADER	313
NF_F_IP_SECTION_PAYLOAD	314

Éléments spécifiques à l'entreprise



Remarque : Le capteur de flux utilise les définitions d'identificateur d'élément d'information Lancope : Numéro d'entreprise privée (PEN) - 8712

Pour plus d'informations sur les éléments d'information pris en charge pour chaque version logicielle, reportez-vous aux guides des éléments d'information de la liste de références techniques

NF_F_FLOWSENSOR_INITIATOR	29794
NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT	29795
NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT	29796
NF_F_FLOWSENSOR_RTT	29797
NF_F_FLOWSENSOR_SVR_RESP	29798
NF_F_FLOWSENSOR_RETRANSMITS	29799
NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT	29800
NF_F_FLOWSENSOR_TCP_FRAG_TOTAL_COUNT	29801
NF_F_FLOWSENSOR_SRC_EMAIL_IN	29802
NF_F_FLOWSENSOR_SRC_EMAIL_OUT	29803
NF_F_FLOWSENSOR_SRC_EMAIL_IN_MESS	29804
NF_F_FLOWSENSOR_SRC_EMAIL_OUT_MESS	29805
NF_F_FLOWSENSOR_SRC_EMAIL_IN_TRYS	29806
NF_F_FLOWSENSOR_SRC_EMAIL_OUT_TRYS	29807
NF_F_FLOWSENSOR_DST_EMAIL_IN	29808
NF_F_FLOWSENSOR_DST_EMAIL_OUT	29809
NF_F_FLOWSENSOR_DST_EMAIL_IN_MESS	29810
NF_F_FLOWSENSOR_DST_EMAIL_OUT_MESS	29811
NF_F_FLOWSENSOR_DST_EMAIL_IN_TRYS	29812
NF_F_FLOWSENSOR_DST_EMAIL_OUT_TRYS	29813
NF_F_FLOWSENSOR_TRACES	29814
NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL	29817
NF_F_FLOWSENSOR_EMB_ICMP_TYPE	29818
NF_F_FLOWSENSOR_EMB_ICMP_CODE	29819
NF_F_FLOWSENSOR_APPLICATION_ID	29820

```
NF_F_FLOWSENSOR_BAD_FLAG_XMAS                    29821
NF_F_FLOWSENSOR_BAD_FLAG_SYN_FIN                 29822
NF_F_FLOWSENSOR_BAD_FLAG_BAD_RST                 29823
NF_F_FLOWSENSOR_BAD_FLAG_NO_ACK                    29824
NF_F_FLOWSENSOR_BAD_FLAG_URG                     29825
NF_F_FLOWSENSOR_BAD_FLAG_NOFLAG                    29826
NF_F_FLOWSENSOR_BAD_TCP_PROBE                    29827
NF_F_FLOWSENSOR_SHORT_FRAG_ATTACK                29828
NF_F_FLOWSENSOR_FRAG_PKT_TOO_SHORT                29829
NF_F_FLOWSENSOR_FRAG_PKT_TOO_LONG                29830
NF_F_FLOWSENSOR_FRAG_DIFFERENT_SIZES             29831
NF_F_FLOWSENSOR_APPLICATION_DETAILS                29832
```

Formats de modèles



Remarque : Chaque modèle inclut le nom du modèle et le nombre de champs, suivis des champs NetFlow/IPFIX individuels et de la taille de chaque champ (en octets).

Notez que les éléments IPFIX spécifiques à l'entreprise sont marqués d'un OU avec 0x8000 pour activer le bit haut, de sorte que le collecteur sache que le champ PEN (Private Enterprise Number) est présent.

Un exemple avec NetFlow v9 et des éléments IPFIX spécifiques à l'entreprise est inclus.

```
TEMPLATE_NAME, ## <-- Field Count (Total number of NF_F fields in the template)
    FIELD_NAME_V9, # <-- Field size (in bytes)
    ENTERPRISE_FIELD_NAME_IPFIX | 0x8000, # <-- Field size (in bytes)
    0000, 8712 <-- Private Enterprise Number (PEN)
```

Premier flux IPv4 - Modèle 317



Remarque : Ce modèle est utilisé pour l'exportation initiale v9 des informations de flux IPv4 à partir d'un emplacement de flux dans le moteur Flow Sensor.

```
IPV4_FIRST_FLOW_TEMPLATE_ID, 31
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SRC_ADDR_IPV4, 4
    NF_F_DST_ADDR_IPV4, 4
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_SRC_MAC, 6
    NF_F_OUT_DST_MAC, 6
    NF_F_IN_BYTES, 4
```

```
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_SRC_VLAN, 2
    NF_F_MPLS_LABEL_1, 3
    NF_F_MIN_TTL, 1
    NF_F_SRC_TOS, 1
    NF_F_FLOWSENSOR_INITIATOR, 1
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TRACES, 2
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL, 1
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE, 1
    NF_F_FLOWSENSOR_EMB_ICMP_CODE, 1
    NF_F_FLOWSENSOR_APPLICATION_ID, 4
```

IPv4 First Flow Deep - Modèle 318



Remarque : Ce modèle est utilisé pour l'exportation initiale v9 des informations de flux IPv4 à partir d'un emplacement de flux dans le moteur Flow Sensor lorsque la case à cocher Export Packet Payload est activée.

```
IPV4_FIRST_FLOW_DEEP_TEMPLATE_ID, 33
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SRC_ADDR_IPV4, 4
    NF_F_DST_ADDR_IPV4, 4
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_SRC_MAC, 6
    NF_F_OUT_DST_MAC, 6
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_SRC_VLAN, 2
    NF_F_MPLS_LABEL_1, 3
    NF_F_MIN_TTL, 1
    NF_F_SRC_TOS, 1
    NF_F_IP_SECTION_HEADER, 64
    NF_F_IP_SECTION_PAYLOAD, 26
    NF_F_FLOWSENSOR_INITIATOR, 1
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
```

```
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TRACES, 2
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL, 1
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE, 1
    NF_F_FLOWSENSOR_EMB_ICMP_CODE, 1
    NF_F_FLOWSENSOR_APPLICATION_ID, 4
```

Flux IPv4 - Modèle 319



Remarque : Ce modèle est utilisé pour les exportations v9 suivantes d'informations de flux IPv4 à partir d'un emplacement de flux dans le moteur de capteur de flux.

```
IPV4_FLOW_TEMPLATE_ID, 25
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SRC_ADDR_IPV4, 4
    NF_F_DST_ADDR_IPV4, 4
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_MIN_TTL, 1
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TRACES, 2
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL, 1
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE, 1
    NF_F_FLOWSENSOR_EMB_ICMP_CODE, 1
    NF_F_FLOWSENSOR_APPLICATION_ID, 4
```

Événement IPv4 - Modèle 320



Remarque : Ce modèle est utilisé pour les exportations v9 des nombres de combinaisons de fragments et d'indicateurs IPv4 erronés détectés par le moteur de détection de flux.

```
IPV4_EVENT_TEMPLATE_ID, 18
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SRC_ADDR_IPV4, 4
    NF_F_DST_ADDR_IPV4, 4
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_PROTOCOL, 1
    NF_F_FLOWSENSOR_BAD_FLAG_XMAS, 2
    NF_F_FLOWSENSOR_BAD_FLAG_SYN_FIN, 2
    NF_F_FLOWSENSOR_BAD_FLAG_BAD_RST, 2
    NF_F_FLOWSENSOR_BAD_FLAG_NO_ACK, 2
    NF_F_FLOWSENSOR_BAD_FLAG_URG, 2
    NF_F_FLOWSENSOR_BAD_FLAG_NOFLAG, 2
    NF_F_FLOWSENSOR_BAD_TCP_PROBE, 2
    NF_F_FLOWSENSOR_SHORT_FRAG_ATTACK, 2
    NF_F_FLOWSENSOR_FRAG_PKT_TOO_SHORT, 2
    NF_F_FLOWSENSOR_FRAG_PKT_TOO_LONG, 2
    NF_F_FLOWSENSOR_FRAG_DIFFERENT_SIZES, 2
```

Premier flux IPv6 - Modèle 321



Remarque : Ce modèle est utilisé pour l'exportation initiale v9 des informations de flux IPv6 à partir d'un emplacement de flux dans le moteur de capteur de flux.

```
IPV6_FIRST_FLOW_TEMPLATE_ID, 31
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SRC_ADDR_IPV6, 16
    NF_F_DST_ADDR_IPV6, 16
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_SRC_MAC, 6
    NF_F_OUT_DST_MAC, 6
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_SRC_VLAN, 2
    NF_F_MPLS_LABEL_1, 3
    NF_F_MIN_TTL, 1
    NF_F_SRC_TOS, 1
    NF_F_FLOWSENSOR_INITIATOR, 1
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TRACES, 2
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL, 1
```

```
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE, 1
    NF_F_FLOWSENSOR_EMB_ICMP_CODE, 1
    NF_F_FLOWSENSOR_APPLICATION_ID, 4
```

IPv6 First Flow Deep - Modèle 322



Remarque : Ce modèle est utilisé pour l'exportation initiale v9 des informations de flux IPv6 à partir d'un emplacement de flux dans le moteur Flow Sensor lorsque la case à cocher Export Packet Payload est activée.

```
IPV6_FIRST_FLOW_DEEP_TEMPLATE_ID, 33
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SRC_ADDR_IPV6, 16
    NF_F_DST_ADDR_IPV6, 16
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_SRC_MAC, 6
    NF_F_OUT_DST_MAC, 6
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_SRC_VLAN, 2
    NF_F_MPLS_LABEL_1, 3
    NF_F_MIN_TTL, 1
    NF_F_SRC_TOS, 1
    NF_F_IP_SECTION_HEADER, 64
    NF_F_IP_SECTION_PAYLOAD, 26
    NF_F_FLOWSENSOR_INITIATOR, 1
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TRACES, 2
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL, 1
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE, 1
    NF_F_FLOWSENSOR_EMB_ICMP_CODE, 1
    NF_F_FLOWSENSOR_APPLICATION_ID, 4
```

Flux IPv6 - Modèle 323



Remarque : Ce modèle est utilisé pour les exportations v9 suivantes d'informations de flux

IPv6 à partir d'un emplacement de flux dans le moteur de capteur de flux.

```
IPV6_FLOW_TEMPLATE_ID, 25
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SRC_ADDR_IPV6, 16
    NF_F_DST_ADDR_IPV6, 16
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_MIN_TTL, 1
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TRACES, 2
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL, 1
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE, 1
    NF_F_FLOWSENSOR_EMB_ICMP_CODE, 1
    NF_F_FLOWSENSOR_APPLICATION_ID, 4
```

Événement IPv6 - Modèle 324



Remarque : Ce modèle est utilisé pour les exportations v9 des nombres de combinaisons de fragments et d'indicateurs IPv6 erronés détectés par le moteur de détection de flux.

```
IPV6_EVENT_TEMPLATE_ID, 18
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SRC_ADDR_IPV6, 16
    NF_F_DST_ADDR_IPV6, 16
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_PROTOCOL, 1
    NF_F_FLOWSENSOR_BAD_FLAG_XMAS, 2
    NF_F_FLOWSENSOR_BAD_FLAG_SYN_FIN, 2
    NF_F_FLOWSENSOR_BAD_FLAG_BAD_RST, 2
    NF_F_FLOWSENSOR_BAD_FLAG_NO_ACK, 2
    NF_F_FLOWSENSOR_BAD_FLAG_URG, 2
    NF_F_FLOWSENSOR_BAD_FLAG_NOFLAG, 2
    NF_F_FLOWSENSOR_BAD_TCP_PROBE, 2
    NF_F_FLOWSENSOR_SHORT_FRAG_ATTACK, 2
    NF_F_FLOWSENSOR_FRAG_PKT_TOO_SHORT, 2
```

```
    NF_F_FLOWSENSOR_FRAG_PKT_TOO_LONG, 2
    NF_F_FLOWSENSOR_FRAG_DIFFERENT_SIZES, 2
```

Nombre d'e-mails source IPv4 - Modèle 325



Remarque : Ce modèle est utilisé pour les exportations v9 d'informations de comptage d'e-mails IPv4 provenant de l'adresse IP source telle que détectée par le moteur de détection de flux.

```
IPV4_SRC_EMAIL_COUNTS_TEMPLATE_ID, 8
    NF_F_SRC_ADDR_IPV4, 4
    NF_F_DST_ADDR_IPV4, 4
    NF_F_FLOWSENSOR_SRC_EMAIL_IN, 4
    NF_F_FLOWSENSOR_SRC_EMAIL_OUT, 4
    NF_F_FLOWSENSOR_SRC_EMAIL_IN_MESS, 4
    NF_F_FLOWSENSOR_SRC_EMAIL_OUT_MESS, 4
    NF_F_FLOWSENSOR_SRC_EMAIL_IN_TRYS, 4
    NF_F_FLOWSENSOR_SRC_EMAIL_OUT_TRYS, 4
```

IPv4 First Flow Response Time Monitoring (RTM) - Modèle 326



Remarque : Ce modèle est utilisé pour l'exportation initiale v9 des informations de flux IPv4 à partir d'un emplacement de flux dans le moteur Flow Sensor lorsque les données RTM ont été calculées.

```
IPV4_FIRST_FLOW_RTM_TEMPLATE_ID, 34
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SRC_ADDR_IPV4, 4
    NF_F_DST_ADDR_IPV4, 4
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_SRC_MAC, 6
    NF_F_OUT_DST_MAC, 6
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_SRC_VLAN, 2
    NF_F_MPLS_LABEL_1, 3
    NF_F_MIN_TTL, 1
    NF_F_SRC_TOS, 1
    NF_F_FLOWSENSOR_INITIATOR, 1
    NF_F_TCP_SYN_TOTAL_COUNT, 2
```

```
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TRACES, 2
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL, 1
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE, 1
    NF_F_FLOWSENSOR_EMB_ICMP_CODE, 1
    NF_F_FLOWSENSOR_RTT, 4
    NF_F_FLOWSENSOR_SVR_RESP, 4
    NF_F_FLOWSENSOR_RETRANSMITS, 2
    NF_F_FLOWSENSOR_APPLICATION_ID, 4
```

Surveillance approfondie du temps de réponse du premier flux IPv4 - Modèle 327



Remarque : Ce modèle est utilisé pour l'exportation initiale v9 des informations de flux IPv4 à partir d'un emplacement de flux dans le moteur de capteur de flux lorsque la case à cocher Exporter la charge utile des paquets est activée et que les données RTM ont été calculées.

```
IPV4_FIRST_FLOW_DEEP_RTM_TEMPLATE_ID, 36
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SRC_ADDR_IPV4, 4
    NF_F_DST_ADDR_IPV4, 4
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_SRC_MAC, 6
    NF_F_OUT_DST_MAC, 6
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_SRC_VLAN, 2
    NF_F_MPLS_LABEL_1, 3
    NF_F_MIN_TTL, 1
    NF_F_SRC_TOS, 1
    NF_F_IP_SECTION_HEADER, 64
    NF_F_IP_SECTION_PAYLOAD, 26
    NF_F_FLOWSENSOR_INITIATOR, 1
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TRACES, 2
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL, 1
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE, 1
```

```
    NF_F_FLOWSENSOR_EMB_ICMP_CODE, 1
    NF_F_FLOWSENSOR_RTT, 4
    NF_F_FLOWSENSOR_SVR_RESP, 4
    NF_F_FLOWSENSOR_RETRANSMITS, 2
    NF_F_FLOWSENSOR_APPLICATION_ID, 4
```

Surveillance du temps de réponse de flux IPv4 - Modèle 328



Remarque : Ce modèle est utilisé pour les exportations v9 de suivi d'informations de flux IPv4 à partir d'un emplacement de flux dans le moteur Flow Sensor lorsque les données RTM ont été calculées.

```
IPV4_FLOW_RTM_TEMPLATE_ID, 28
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SRC_ADDR_IPV4, 4
    NF_F_DST_ADDR_IPV4, 4
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_MIN_TTL, 1
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TRACES, 2
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL, 1
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE, 1
    NF_F_FLOWSENSOR_EMB_ICMP_CODE, 1
    NF_F_FLOWSENSOR_RTT, 4
    NF_F_FLOWSENSOR_SVR_RESP, 4
    NF_F_FLOWSENSOR_RETRANSMITS, 2
    NF_F_FLOWSENSOR_APPLICATION_ID, 4
```

Surveillance du temps de réponse au premier flux IPv6 - Modèle 329



Remarque : Ce modèle est utilisé pour l'exportation initiale v9 des informations de flux IPv6 à partir d'un emplacement de flux dans le moteur Flow Sensor lorsque les données

RTM ont été calculées.

```
IPV6_FIRST_FLOW_RTM_TEMPLATE_ID, 34
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SRC_ADDR_IPV6, 16
    NF_F_DST_ADDR_IPV6, 16
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_SRC_MAC, 6
    NF_F_OUT_DST_MAC, 6
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_SRC_VLAN, 2
    NF_F_MPLS_LABEL_1, 3
    NF_F_MIN_TTL, 1
    NF_F_SRC_TOS, 1
    NF_F_FLOWSENSOR_INITIATOR, 1
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TRACES, 2
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL, 1
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE, 1
    NF_F_FLOWSENSOR_EMB_ICMP_CODE, 1
    NF_F_FLOWSENSOR_RTT, 4
    NF_F_FLOWSENSOR_SVR_RESP, 4
    NF_F_FLOWSENSOR_RETRANSMITS, 2
    NF_F_FLOWSENSOR_APPLICATION_ID, 4
```

Surveillance approfondie du temps de réponse du premier flux IPv6 - Modèle 330



Remarque : Ce modèle est utilisé pour l'exportation initiale v9 des informations de flux IPv6 à partir d'un emplacement de flux dans le moteur Flow Sensor lorsque la case à cocher Export Packet Payload est activée et que les données RTM ont été calculées.

```
IPV6_FIRST_FLOW_DEEP_RTM_TEMPLATE_ID, 36
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SRC_ADDR_IPV6, 16
    NF_F_DST_ADDR_IPV6, 16
    NF_F_L4_SRC_PORT, 2
```

```
    NF_F_L4_DST_PORT, 2
    NF_F_IN_SRC_MAC, 6
    NF_F_OUT_DST_MAC, 6
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_SRC_VLAN, 2
    NF_F_MPLS_LABEL_1, 3
    NF_F_MIN_TTL, 1
    NF_F_SRC_TOS, 1
    NF_F_IP_SECTION_HEADER, 64
    NF_F_IP_SECTION_PAYLOAD, 26
    NF_F_FLOWSENSOR_INITIATOR, 1
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TRACES, 2
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL, 1
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE, 1
    NF_F_FLOWSENSOR_EMB_ICMP_CODE, 1
    NF_F_FLOWSENSOR_RTT, 4
    NF_F_FLOWSENSOR_SVR_RESP, 4
    NF_F_FLOWSENSOR_RETRANSMITS, 2
    NF_F_FLOWSENSOR_APPLICATION_ID, 4
```

Surveillance du temps de réponse de flux IPv6 - Modèle 331



Remarque : Ce modèle est utilisé pour les exportations v9 de suivi des informations de flux IPv6 à partir d'un emplacement de flux dans le moteur de capteur de flux lorsque les données RTM ont été calculées.

```
IPV6_FLOW_RTM_TEMPLATE_ID, 28
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SRC_ADDR_IPV6, 16
    NF_F_DST_ADDR_IPV6, 16
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_MIN_TTL, 1
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
```

```
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TRACES, 2
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL, 1
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE, 1
    NF_F_FLOWSENSOR_EMB_ICMP_CODE, 1
    NF_F_FLOWSENSOR_RTT, 4
    NF_F_FLOWSENSOR_SVR_RESP, 4
    NF_F_FLOWSENSOR_RETRANSMITS, 2
    NF_F_FLOWSENSOR_APPLICATION_ID, 4
```

Nombre d'e-mails de destination IPv4 - Modèle 332



Remarque : Ce modèle est utilisé pour les exportations v9 d'informations de comptage d'e-mails IPv4 reçues par l'adresse IP de destination, telles que détectées par le moteur de détection de flux.

```
IPV4_DST_EMAIL_COUNTS_TEMPLATE_ID, 8
    NF_F_SRC_ADDR_IPV4, 4
    NF_F_DST_ADDR_IPV4, 4
    NF_F_FLOWSENSOR_DST_EMAIL_IN, 4
    NF_F_FLOWSENSOR_DST_EMAIL_OUT, 4
    NF_F_FLOWSENSOR_DST_EMAIL_IN_MESS, 4
    NF_F_FLOWSENSOR_DST_EMAIL_OUT_MESS, 4
    NF_F_FLOWSENSOR_DST_EMAIL_IN_TRYS, 4
    NF_F_FLOWSENSOR_DST_EMAIL_OUT_TRYS, 4
```

Nombre d'e-mails source IPv6 - Modèle 333



Remarque : Ce modèle est utilisé pour les exportations v9 d'informations de comptage d'e-mails IPv6 provenant de l'adresse IP source telle que détectée par le moteur de détection de flux.

```
IPV6_SRC_EMAIL_COUNTS_TEMPLATE_ID, 8
    NF_F_SRC_ADDR_IPV6, 16
    NF_F_DST_ADDR_IPV6, 16
    NF_F_FLOWSENSOR_SRC_EMAIL_IN, 4
    NF_F_FLOWSENSOR_SRC_EMAIL_OUT, 4
    NF_F_FLOWSENSOR_SRC_EMAIL_IN_MESS, 4
    NF_F_FLOWSENSOR_SRC_EMAIL_OUT_MESS, 4
    NF_F_FLOWSENSOR_SRC_EMAIL_IN_TRYS, 4
    NF_F_FLOWSENSOR_SRC_EMAIL_OUT_TRYS, 4
```

Nombre d'e-mails de destination IPv6 - Modèle 334



Remarque : Ce modèle est utilisé pour les exportations v9 d'informations de comptage d'e-mails IPv6 reçues par l'adresse IP de destination, telles que détectées par le moteur de détection de flux.

```
IPV6_DST_EMAIL_COUNTS_TEMPLATE_ID, 8
    NF_F_SRC_ADDR_IPV6, 16
    NF_F_DST_ADDR_IPV6, 16
    NF_F_FLOWSENSOR_DST_EMAIL_IN, 4
    NF_F_FLOWSENSOR_DST_EMAIL_OUT, 4
    NF_F_FLOWSENSOR_DST_EMAIL_IN_MESS, 4
    NF_F_FLOWSENSOR_DST_EMAIL_OUT_MESS, 4
    NF_F_FLOWSENSOR_DST_EMAIL_IN_TRYS, 4
    NF_F_FLOWSENSOR_DST_EMAIL_OUT_TRYS, 4
```

Modèle IPFIX de premier flux IPv4 335



Remarque : Ce modèle est utilisé pour l'exportation IPFIX initiale des informations de flux IPv4 à partir d'un emplacement de flux dans le moteur de capteur de flux.

```
IPV4_FIRST_FLOW_IPFIX_TEMPLATE_ID, 33
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SYSTEM_INIT_TIME_MILLISECONDS, 8
    NF_F_SRC_ADDR_IPV4, 4
    NF_F_DST_ADDR_IPV4, 4
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_SRC_MAC, 6
    NF_F_OUT_DST_MAC, 6
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_SRC_VLAN, 2
    NF_F_MPLS_LABEL_1, 3
    NF_F_MIN_TTL, 1
    NF_F_SRC_TOS, 1
    NF_F_FLOWSENSOR_INITIATOR | 0x8000, 1
    0000, 8712
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
```

```
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TRACES | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_CODE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_ID | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_DETAILS | 0x8000, 65535
    0000, 8712
```

IPFIX profond de premier flux IPv4 - Modèle 336



Remarque : Ce modèle est utilisé pour l'exportation IPFIX initiale des informations de flux IPv4 à partir d'un emplacement de flux dans le moteur de capteur de flux lorsque la case à cocher Exporter la charge utile des paquets est activée.

```
IPV4_FIRST_FLOW_DEEP_IPFIX_TEMPLATE_ID, 35
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SYSTEM_INIT_TIME_MILLISECONDS, 8
    NF_F_SRC_ADDR_IPV4, 4
    NF_F_DST_ADDR_IPV4, 4
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_SRC_MAC, 6
    NF_F_OUT_DST_MAC, 6
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_SRC_VLAN, 2
    NF_F_MPLS_LABEL_1, 3
    NF_F_MIN_TTL, 1
    NF_F_SRC_TOS, 1
    NF_F_IP_SECTION_HEADER, 64
    NF_F_IP_SECTION_PAYLOAD, 26
    NF_F_FLOWSENSOR_INITIATOR | 0x8000, 1
    0000, 8712
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT | 0x8000, 2
```

```
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TRACES | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_CODE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_ID | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_DETAILS | 0x8000, 65535
    0000, 8712
```

IPFIX de flux IPv4 - Modèle 337



Remarque : Ce modèle est utilisé pour les exportations IPFIX de suivi d'informations de flux IPv4 à partir d'un emplacement de flux dans le moteur de capteur de flux.

```
IPV4_FLOW_IPFIX_TEMPLATE_ID, 27
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SYSTEM_INIT_TIME_MILLISECONDS, 8
    NF_F_SRC_ADDR_IPV4, 4
    NF_F_DST_ADDR_IPV4, 4
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_MIN_TTL, 1
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TRACES | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE | 0x8000, 1
    0000, 8712
```

```
    NF_F_FLOWSENSOR_EMB_ICMP_CODE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_ID | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_DETAILS | 0x8000, 65535
    0000, 8712
```

IPFIX de l'événement IPv4 - Modèle 338



Remarque : Ce modèle est utilisé pour les exportations IPFIX de nombres de combinaisons de fragments et d'indicateurs IPv4 erronés détectés par le moteur de détection de flux.

```
IPV4_EVENT_IPFIX_TEMPLATE_ID, 19
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SYSTEM_INIT_TIME_MILLISECONDS, 8
    NF_F_SRC_ADDR_IPV4, 4
    NF_F_DST_ADDR_IPV4, 4
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_PROTOCOL, 1
    NF_F_FLOWSENSOR_BAD_FLAG_XMAS | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_BAD_FLAG_SYN_FIN | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_BAD_FLAG_BAD_RST | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_BAD_FLAG_NO_ACK | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_BAD_FLAG_URG | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_BAD_FLAG_NOFLAG | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_BAD_TCP_PROBE | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_SHORT_FRAG_ATTACK | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_FRAG_PKT_TOO_SHORT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_FRAG_PKT_TOO_LONG | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_FRAG_DIFFERENT_SIZES | 0x8000, 2
    0000, 8712
```

IPFIX de premier flux IPv6 - Modèle 339



Remarque : Ce modèle est utilisé pour l'exportation IPFIX initiale des informations de flux

IPv6 à partir d'un emplacement de flux dans le moteur de capteur de flux.

```
IPV6_FIRST_FLOW_IPFIX_TEMPLATE_ID, 33
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SYSTEM_INIT_TIME_MILLISECONDS, 8
    NF_F_SRC_ADDR_IPV6, 16
    NF_F_DST_ADDR_IPV6, 16
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_SRC_MAC, 6
    NF_F_OUT_DST_MAC, 6
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_SRC_VLAN, 2
    NF_F_MPLS_LABEL_1, 3
    NF_F_MIN_TTL, 1
    NF_F_SRC_TOS, 1
    NF_F_FLOWSENSOR_INITIATOR | 0x8000, 1
    0000, 8712
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TRACES | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_CODE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_ID | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_DETAILS | 0x8000, 65535
    0000, 8712
```

IPFIX profond de premier flux IPv6 - Modèle 340



Remarque : Ce modèle est utilisé pour l'exportation IPFIX initiale des informations de flux IPv6 à partir d'un emplacement de flux dans le moteur de capteur de flux lorsque la case à cocher Exporter la charge utile des paquets est activée.

```
IPV6_FIRST_FLOW_DEEP_IPFIX_TEMPLATE_ID, 35
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SYSTEM_INIT_TIME_MILLISECONDS, 8
    NF_F_SRC_ADDR_IPV6, 16
    NF_F_DST_ADDR_IPV6, 16
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_SRC_MAC, 6
    NF_F_OUT_DST_MAC, 6
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_SRC_VLAN, 2
    NF_F_MPLS_LABEL_1, 3
    NF_F_MIN_TTL, 1
    NF_F_SRC_TOS, 1
    NF_F_IP_SECTION_HEADER, 64
    NF_F_IP_SECTION_PAYLOAD, 26
    NF_F_FLOWSENSOR_INITIATOR | 0x8000, 1
    0000, 8712
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TRACES | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_CODE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_ID | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_DETAILS | 0x8000, 65535
    0000, 8712
```

IPFIX de flux IPv6 - Modèle 341



Remarque : Ce modèle est utilisé pour les exportations IPFIX de suivi des informations de flux IPv6 à partir d'un emplacement de flux dans le moteur de capteur de flux.

```
IPV6_FLOW_IPFIX_TEMPLATE_ID, 27
```

```
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SYSTEM_INIT_TIME_MILLISECONDS, 8
    NF_F_SRC_ADDR_IPV6, 16
    NF_F_DST_ADDR_IPV6, 16
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_MIN_TTL, 1
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TRACES | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_CODE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_ID | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_DETAILS | 0x8000, 65535
    0000, 8712
```

IPFIX de l'événement IPv6 - Modèle 342



Remarque : Ce modèle est utilisé pour les exportations IPFIX de nombres de combinaisons de fragments et d'indicateurs IPv6 erronés détectés par le moteur de détection de flux.

```
IPV6_EVENT_IPFIX_TEMPLATE_ID, 19
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SYSTEM_INIT_TIME_MILLISECONDS, 8
    NF_F_SRC_ADDR_IPV6, 16
    NF_F_DST_ADDR_IPV6, 16
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_PROTOCOL, 1
    NF_F_FLOWSENSOR_BAD_FLAG_XMAS | 0x8000, 2
    0000, 8712
```

```
    NF_F_FLOWSENSOR_BAD_FLAG_SYN_FIN | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_BAD_FLAG_BAD_RST | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_BAD_FLAG_NO_ACK | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_BAD_FLAG_URG | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_BAD_FLAG_NOFLAG | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_BAD_TCP_PROBE | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_SHORT_FRAG_ATTACK | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_FRAG_PKT_TOO_SHORT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_FRAG_PKT_TOO_LONG | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_FRAG_DIFFERENT_SIZES | 0x8000, 2
    0000, 8712
```

Nombre d'e-mails source IPv4 IPFIX - Modèle 343



Remarque : Ce modèle est utilisé pour les exportations IPFIX d'informations de comptage de messages IPv4 provenant de l'adresse IP source, telles que détectées par le moteur de détection de flux.

```
IPV4_SRC_EMAIL_COUNTS_IPFIX_TEMPLATE_ID, 8
    NF_F_SRC_ADDR_IPV4, 4
    NF_F_DST_ADDR_IPV4, 4
    NF_F_FLOWSENSOR_SRC_EMAIL_IN | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_SRC_EMAIL_OUT | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_SRC_EMAIL_IN_MESS | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_SRC_EMAIL_OUT_MESS | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_SRC_EMAIL_IN_TRYS | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_SRC_EMAIL_OUT_TRYS | 0x8000, 4
    0000, 8712
```

Surveillance du temps de réponse au premier flux IPv4 - Modèle 344



Remarque : Ce modèle est utilisé pour l'exportation IPFIX initiale des informations de flux IPv4 à partir d'un emplacement de flux dans le moteur de capteur de flux lorsque les

données RTM ont été calculées.

```
IPV4_FIRST_FLOW_RTM_IPFIX_TEMPLATE_ID, 36
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SYSTEM_INIT_TIME_MILLISECONDS, 8
    NF_F_SRC_ADDR_IPV4, 4
    NF_F_DST_ADDR_IPV4, 4
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_SRC_MAC, 6
    NF_F_OUT_DST_MAC, 6
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_SRC_VLAN, 2
    NF_F_MPLS_LABEL_1, 3
    NF_F_MIN_TTL, 1
    NF_F_SRC_TOS, 1
    NF_F_FLOWSENSOR_INITIATOR | 0x8000, 1
    0000, 8712
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TRACES | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_CODE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_RTT | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_SVR_RESP | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_RETRANSMITS | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_ID | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_DETAILS | 0x8000, 65535
    0000, 8712
```

Surveillance approfondie du temps de réponse du premier flux IPv4 - Modèle 345



Remarque : Ce modèle est utilisé pour l'exportation IPFIX initiale des informations de flux IPv4 à partir d'un emplacement de flux dans le moteur de capteur de flux lorsque la case à cocher Exporter la charge utile des paquets est activée.

```
IPV4_FIRST_FLOW_DEEP_RTM_IPFIX_TEMPLATE_ID, 38
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SYSTEM_INIT_TIME_MILLISECONDS, 8
    NF_F_SRC_ADDR_IPV4, 4
    NF_F_DST_ADDR_IPV4, 4
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_SRC_MAC, 6
    NF_F_OUT_DST_MAC, 6
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_SRC_VLAN, 2
    NF_F_MPLS_LABEL_1, 3
    NF_F_MIN_TTL, 1
    NF_F_SRC_TOS, 1
    NF_F_IP_SECTION_HEADER, 64
    NF_F_IP_SECTION_PAYLOAD, 26
    NF_F_FLOWSENSOR_INITIATOR | 0x8000, 1
    0000, 8712
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TRACES | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_CODE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_RTT | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_SVR_RESP | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_RETRANSMITS | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_ID | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_DETAILS | 0x8000, 65535
    0000, 8712
```

Surveillance du temps de réponse de flux IPv4 IPFIX - Modèle 346



Remarque : Ce modèle est utilisé pour les exportations IPFIX de suivi d'informations de flux IPv4 à partir d'un emplacement de flux dans le moteur Flow Sensor lorsque les données RTM ont été calculées.

```
IPV4_FLOW_RTM_IPFIX_TEMPLATE_ID, 30
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SYSTEM_INIT_TIME_MILLISECONDS, 8
    NF_F_SRC_ADDR_IPV4, 4
    NF_F_DST_ADDR_IPV4, 4
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_MIN_TTL, 1
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TRACES | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_CODE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_RTT | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_SVR_RESP | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_RETRANSMITS | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_ID | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_DETAILS | 0x8000, 65535
    0000, 8712
```

IPv6 First Flow Response Time Monitoring IPFIX - Modèle 347



Remarque : Ce modèle est utilisé pour l'exportation IPFIX initiale des informations de flux IPv6 à partir d'un emplacement de flux dans le moteur de capteur de flux lorsque les données RTM ont été calculées.

```
IPV6_FIRST_FLOW_RTM_IPFIX_TEMPLATE_ID, 36
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SYSTEM_INIT_TIME_MILLISECONDS, 8
    NF_F_SRC_ADDR_IPV6, 16
    NF_F_DST_ADDR_IPV6, 16
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_SRC_MAC, 6
    NF_F_OUT_DST_MAC, 6
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_SRC_VLAN, 2
    NF_F_MPLS_LABEL_1, 3
    NF_F_MIN_TTL, 1
    NF_F_SRC_TOS, 1
    NF_F_FLOWSENSOR_INITIATOR | 0x8000, 1
    0000, 8712
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TRACES | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_CODE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_RTT | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_SVR_RESP | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_RETRANSMITS | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_ID | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_DETAILS | 0x8000, 65535
    0000, 8712
```

IPv6 First Flow Deep RTM IPFIX - Modèle 348



Remarque : Ce modèle est utilisé pour l'exportation IPFIX initiale des informations de flux IPv6 à partir d'un emplacement de flux dans le moteur de capteur de flux lorsque la case à cocher Exporter la charge utile des paquets est activée.

```
IPV6_FIRST_FLOW_DEEP_RTM_IPFIX_TEMPLATE_ID, 38
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SYSTEM_INIT_TIME_MILLISECONDS, 8
    NF_F_SRC_ADDR_IPV6, 16
    NF_F_DST_ADDR_IPV6, 16
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_SRC_MAC, 6
    NF_F_OUT_DST_MAC, 6
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_SRC_VLAN, 2
    NF_F_MPLS_LABEL_1, 3
    NF_F_MIN_TTL, 1
    NF_F_SRC_TOS, 1
    NF_F_IP_SECTION_HEADER, 64
    NF_F_IP_SECTION_PAYLOAD, 26
    NF_F_FLOWSENSOR_INITIATOR | 0x8000, 1
    0000, 8712
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TRACES | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_CODE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_RTT | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_SVR_RESP | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_RETRANSMITS | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_ID | 0x8000, 4
    0000, 8712
```

```
    NF_F_FLOWSENSOR_APPLICATION_DETAILS | 0x8000, 65535
    0000, 8712
```

Surveillance du temps de réponse de flux IPv6 - Modèle 349



Remarque : Ce modèle est utilisé pour les exportations IPFIX de suivi d'informations de flux IPv6 à partir d'un emplacement de flux dans le moteur Flow Sensor lorsque les données RTM ont été calculées.

```
IPV6_FLOW_RTM_IPFIX_TEMPLATE_ID, 30
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SYSTEM_INIT_TIME_MILLISECONDS, 8
    NF_F_SRC_ADDR_IPV6, 16
    NF_F_DST_ADDR_IPV6, 16
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_IN_BYTES, 4
    NF_F_IN_PKTS, 4
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_TCP_FLAGS, 1
    NF_F_MIN_TTL, 1
    NF_F_TCP_SYN_TOTAL_COUNT, 2
    NF_F_TCP_ACK_TOTAL_COUNT, 2
    NF_F_TCP_FIN_TOTAL_COUNT, 2
    NF_F_TCP_RST_TOTAL_COUNT, 2
    NF_F_FLOWSENSOR_TCP_BAD_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SRS_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TCP_SYN_ACK_TOTAL_COUNT | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_TRACES | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_PROTOCOL | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_TYPE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_EMB_ICMP_CODE | 0x8000, 1
    0000, 8712
    NF_F_FLOWSENSOR_RTT | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_SVR_RESP | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_RETRANSMITS | 0x8000, 2
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_ID | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_APPLICATION_DETAILS | 0x8000, 65535
    0000, 8712
```

Nombre d'e-mails de destination IPv4 IPFIX - Modèle 350



Remarque : Ce modèle est utilisé pour les exportations IPFIX d'informations de comptage d'e-mails IPv4 reçues par l'adresse IP de destination, telles que détectées par le moteur de détection de flux.

```
IPV4_DST_EMAIL_COUNTS_IPFIX_TEMPLATE_ID, 8
    NF_F_SRC_ADDR_IPV4, 4
    NF_F_DST_ADDR_IPV4, 4
    NF_F_FLOWSENSOR_DST_EMAIL_IN | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_DST_EMAIL_OUT | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_DST_EMAIL_IN_MESS | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_DST_EMAIL_OUT_MESS | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_DST_EMAIL_IN_TRYS | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_DST_EMAIL_OUT_TRYS | 0x8000, 4
    0000, 8712
```

Nombre d'e-mails source IPv6 IPFIX - Modèle 351



Remarque : Ce modèle est utilisé pour les exportations IPFIX d'informations de comptage de messages IPv6 provenant de l'adresse IP source, telles que détectées par le moteur de détection de flux.

```
IPV6_SRC_EMAIL_COUNTS_IPFIX_TEMPLATE_ID, 8
    NF_F_SRC_ADDR_IPV6, 16
    NF_F_DST_ADDR_IPV6, 16
    NF_F_FLOWSENSOR_SRC_EMAIL_IN | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_SRC_EMAIL_OUT | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_SRC_EMAIL_IN_MESS | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_SRC_EMAIL_OUT_MESS | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_SRC_EMAIL_IN_TRYS | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_SRC_EMAIL_OUT_TRYS | 0x8000, 4
    0000, 8712
```

Nombre d'e-mails de destination IPv6 IPFIX - Modèle 352



Remarque : Ce modèle est utilisé pour les exportations IPFIX d'informations de comptage d'e-mails IPv6 reçues par l'adresse IP de destination, telles que détectées par le moteur de détection de flux.

```
IPV6_DST_EMAIL_COUNTS_IPFIX_TEMPLATE_ID, 8
    NF_F_SRC_ADDR_IPV6, 16
    NF_F_DST_ADDR_IPV6, 16
    NF_F_FLOWSENSOR_DST_EMAIL_IN | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_DST_EMAIL_OUT | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_DST_EMAIL_IN_MESS | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_DST_EMAIL_OUT_MESS | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_DST_EMAIL_IN_TRYS | 0x8000, 4
    0000, 8712
    NF_F_FLOWSENSOR_DST_EMAIL_OUT_TRYS | 0x8000, 4
    0000, 8712
```

IPFIX IPv4 ETA Initial Data Packet (IDP) - Modèle 354



Remarque : Ce modèle est utilisé pour les flux IPFIX qui incluent l'élément Paquet de données initial (IDP) lorsque l'option de traitement ETA est sélectionnée sur le capteur de flux

```
IPV4_ETTA_IDP_IPFIX_TEMPLATE_ID, 11
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SYSTEM_INIT_TIME_MILLISECONDS, 8
    NF_F_SRC_ADDR_IPV4, 4
    NF_F_DST_ADDR_IPV4, 4
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_INITIAL_DATA_PACKET | 0x8000, 1300
    0000, 9
```

IPFIX de séquence ETA IPv4 de longueurs et d'heures de paquets (SPLT) - Modèle 356



Remarque : Ce modèle est utilisé pour les flux IPFIX qui incluent l'élément Sequence of Packet Lengths and Times (SPLT) lorsque l'option de traitement de l'ETA est sélectionnée sur le capteur de flux

```
IPV4_ETTA_SPLT_IPFIX_TEMPLATE_ID, 11
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SYSTEM_INIT_TIME_MILLISECONDS, 8
    NF_F_SRC_ADDR_IPV4, 4
    NF_F_DST_ADDR_IPV4, 4
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_SEQUENCE_PKT_LENGTH_TIME | 0x8000, 40
    0000, 9
```

IPFIX IPv6 ETA Initial Data Packet (IDP) - Modèle 364



Remarque : Ce modèle est utilisé pour les flux IPFIX IPv6 qui incluent l'élément Paquet de données initial (IDP) lorsque l'option de traitement ETA est sélectionnée sur le capteur de flux

```
IPV6_ETTA_IDP_IPFIX_TEMPLATE_ID, 11
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SYSTEM_INIT_TIME_MILLISECONDS, 8
    NF_F_SRC_ADDR_IPV6, 16
    NF_F_DST_ADDR_IPV6, 16
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_INITIAL_DATA_PACKET | 0x8000, 1300
    0000, 9
```

Séquence ETA IPv6 de longueurs et d'heures des paquets (SPLT) IPFIX - Modèle 366



Remarque : Ce modèle est utilisé pour les flux IPFIX IPv6 qui incluent l'élément Sequence

of Packet Lengths and Times (SPLT) lorsque l'option de traitement ETA est sélectionnée sur le capteur de flux

```
IPV6_ETTA_SPLT_IPFIX_TEMPLATE_ID, 11
    NF_F_FIRST_SWITCHED, 4
    NF_F_LAST_SWITCHED, 4
    NF_F_SYSTEM_INIT_TIME_MILLISECONDS, 8
    NF_F_SRC_ADDR_IPV6, 16
    NF_F_DST_ADDR_IPV6, 16
    NF_F_L4_SRC_PORT, 2
    NF_F_L4_DST_PORT, 2
    NF_F_SRC_INTF_ID, 2
    NF_F_DST_INTF_ID, 2
    NF_F_PROTOCOL, 1
    NF_F_SEQUENCE_PKT_LENGTH_TIME | 0x8000, 40
    0000, 9
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.