Présentation de la découverte du réseau

Les rubriques suivantes traitent de la découverte de réseau :

À propos de la détection des données de l'hôte, de l'application et de l'utilisateur

Les politiques de découverte de réseau ne peuvent être configurées que pour les périphériques Cisco Secure Firewall Threat Defense qui envoient des événements à un gestionnaire d'analyse réseau. (Network Analytics Manager est un Cisco Secure Firewall Management Center local configuré pour fournir des analyses d'événements uniquement.)

Le système utilise des politiques de *découverte de réseau* et *d'identité* pour recueillir des données sur l'hôte, les applications et les utilisateurs pour le trafic sur votre réseau. Vous pouvez utiliser certains types de données de découverte et d'identité pour créer une carte complète de vos actifs de réseau, effectuer des analyses détaillées, le profilage comportemental, le contrôle d'accès, et atténuer et répondre aux vulnérabilités et aux exploitations dont votre entreprise est susceptible.

Données d'hôte et d'application

Les données d'hôte et d'application sont collectées par les sources d'identité de l'hôte et les détecteurs d'applications selon les paramètres de votre politique de découverte de réseau. Les périphériques gérés observent le trafic sur les segments de réseau que vous spécifiez.

Pour en savoir plus, consultez Principes fondamentaux de détection des hôtes et des applications, à la page 2.

Données d'utilisateur

Les données des utilisateurs sont collectées par les sources d'identité des utilisateurs en fonction des paramètres de vos politiques de découverte de réseau et d'identité. Vous pouvez utiliser les données pour la sensibilisation et le contrôle de l'utilisateur.

Pour en savoir plus, consultez À propos des identités d'utilisateur.

La journalisation des données de découverte et d'identité vous permet de profiter de nombreuses fonctionnalités du système, notamment :

- Affichage de la cartographie du réseau, qui est une représentation détaillée de vos ressources et de votre topologie réseau que vous pouvez afficher en regroupant les hôtes et les périphériques réseau, les attributs d'hôte, les protocoles d'application ou les vulnérabilités.
- Effectuer le contrôle des applications et des utilisateurs; c'est-à-dire l'écriture de règles de contrôle d'accès à l'aide de conditions d'attributs d'application, de domaine, d'utilisateur, de groupe d'utilisateurs et d'attributs ISE.
- L'affichage des profils d'hôte, qui sont des vues complètes de toutes les informations disponibles pour vos hôtes détectés.
- L'affichage des tableaux de bord, qui (entre autres fonctionnalités) peut vous donner un aperçu de vos ressources réseau et de l'activité de vos utilisateurs.
- Affichage d'informations détaillées sur les événements de découverte et l'activité des utilisateurs enregistrés par le système.
- Associer les hôtes et tous les serveurs ou clients qu'ils exécutent aux exploits dont ils sont sensibles.

  Cela vous permet de cerner et d'atténuer les vulnérabilités, d'évaluer l'incidence des incidents d'intrusion sur votre réseau et de régler les états des règles de prévention des intrusions pour qu'ils fournissent une protection maximale pour les ressources de votre réseau.
- Alerte par courriel, déroutement SNMP ou journal système lorsque le système génère un incident d'intrusion avec un indicateur d'impact précis, ou un type particulier d'événement de découverte
- Surveiller la conformité de votre organisation avec une autoriser des systèmes d'exploitation, des clients, des protocoles d'application et des protocoles autorisés
- Créer des politiques de corrélation avec des règles qui déclenchent et génèrent des événements de corrélation lorsque le système génère des événements de découverte ou détecte une activité utilisateur
- La journalisation et l'utilisation des connexions NetFlow, le cas échéant;

Principes fondamentaux de détection des hôtes et des applications

Vous pouvez configurer votre politique de découverte de réseau pour effectuer la détection des hôtes et des applications.

Pour plus de renseignements, consultez les sections Présentation : collecte des données de l'hôte et Présentation : détection d'applications.

Détection passive des données du système d'exploitation et de l'hôte

La détection passive est la méthode par défaut du système pour remplir la cartographie du réseau en analysant le trafic réseau (et toutes les données NetFlow exportées). La détection passive fournit des informations contextuelles sur les actifs de votre réseau, tels que les systèmes d'exploitation et les applications en cours d'exécution.

Si le trafic provenant d'un hôte surveillé n'offre pas de preuve concluante du système d'exploitation de l'hôte, la cartographie du réseau affiche le système d'exploitation le plus probable. Par exemple, un périphérique NAT peut sembler exécuter plusieurs systèmes d'exploitation en raison des hôtes « derrière » le périphérique

NAT. Pour faire cette détermination la plus probable, le système utilise une valeur de confiance qu'il affecte à chaque système d'exploitation détecté, et la quantité de données concordantes parmi les systèmes d'exploitation détectés.

Remarque Le système ne prend pas en compte les applications et les systèmes d'exploitation « `inconnus` » signalés dans sa détermination.

Si la détection passive identifie de manière inexacte vos actifs réseau, réfléchissez au positionnement de vos périphériques gérés. Vous pouvez également augmenter les capacités de détection passive du système à l'aide d'empreintes digitales de système d'exploitation et des détecteurs d'application personnalisés. Vous pouvez aussi utiliser *la détection active*, qui n'est pas basée sur une analyse du trafic, mais qui vous permet de mettre à jour directement la cartographie du réseau à l'aide des résultats de l'analyse ou d'autres sources d'information.

Détection active des données du système d'exploitation et de l'hôte

La détection active ajoute aux mappages du réseau les informations sur l'hôte collectées par les sources actives. Par exemple, vous pouvez utiliser l'analyseur Nmap pour analyser activement les hôtes que vous ciblez sur votre réseau. Nmap détecte les systèmes d'exploitation et les applications sur les hôtes.

En outre, la fonction d'entrée de l'hôte vous permet d'ajouter activement *des données d'entrée de l'hôte* aux mappages du réseau. Il existe deux catégories différentes de données d'entrée d'hôte :

- *données d'entrée de l'utilisateur* : données ajoutées par l'intermédiaire de l'interface utilisateur du système Firepower. Vous pouvez modifier le système d'exploitation d'un hôte ou l'identité d'application au moyen de cette interface.
- *données d'entrée importées de l'hôte* : données importées à l'aide d'un utilitaire de ligne de commande.

Le système conserve une identité pour chaque source active. Lorsque vous exécutez une instance d'analyse Nmap, par exemple, les résultats de l'analyse précédente sont remplacés par les nouveaux résultats de l'analyse. Cependant, si vous exécutez une analyse Nmap puis remplacez ces résultats par les données d'un client dont les résultats sont importés via la ligne de commande, le système conserve à la fois les identités des résultats Nmap et les identités du client d'importation. Le système utilise ensuite les priorités définies dans la politique de découverte de réseau pour déterminer l'identité active à utiliser comme identité actuelle.

Notez que les entrées de l'utilisateur sont considérées comme une source, même si elle provient de différents utilisateurs. Par exemple, si l'Utilisateur A définit le système d'exploitation via le profil d'hôte, puis l'Utilisateur B modifie cette définition via le profil d'hôte, la définition définie par l'Utilisateur B est conservée et la définition définie par l'Utilisateur A est supprimée. En outre, notez que l'entrée de l'utilisateur remplace toutes les autres sources actives et est utilisée comme identité actuelle, si elle existe.

Identités actuelles des applications et des systèmes d'exploitation

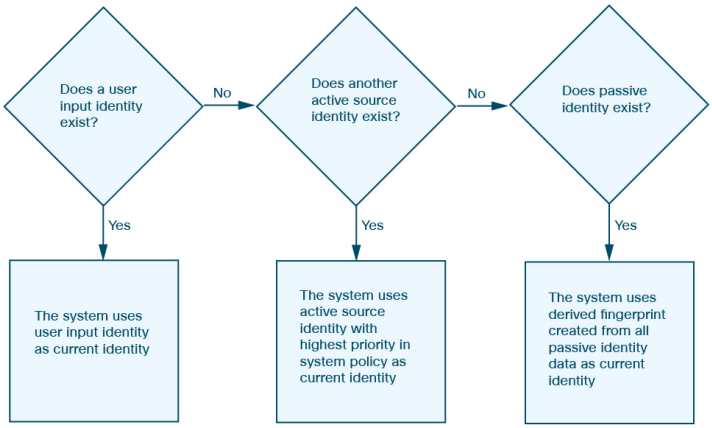
L' *identité actuelle* d'une application ou d'un système d'exploitation sur un hôte est l'identité que le système juge la plus susceptible d'être correcte.

Le système utilise l'identité actuelle d'un système d'exploitation ou d'une application aux fins suivantes :

- affecter des vulnérabilités à un hôte
- pour l'évaluation des incidences

- lors de l'évaluation des règles de corrélation écrites par rapport aux identifications du système d'exploitation, aux qualifications du profil d'hôte et aux listes de conformité autoriser
- à afficher dans les tableaux Hôtes et Serveurs des flux de travail
- à afficher dans le profil d'hôte
- pour calculer les statistiques du système d'exploitation et des applications sur la page des statistiques de découverte

Le système utilise les priorités de source pour déterminer quelle identité active doit être utilisée comme identité actuelle pour une application ou un système d'exploitation.



Par exemple, si un utilisateur définit le système d'exploitation sur Windows Server 2003 sur un hôte, Windows 2003 Server est l'identité actuelle. Les attaques qui ciblent les vulnérabilités de Windows 2003 Server sur cet hôte ont une incidence plus importante, et les vulnérabilités répertoriées pour cet hôte dans le profil d'hôte incluent les vulnérabilités de Windows 2003 Server.

La base de données peut conserver des informations provenant de plusieurs sources pour le système d'exploitation ou pour une application particulière sur un hôte.

Le système traite une identité de système d'exploitation ou d'application comme l'identité actuelle lorsque la source des données a la priorité de source la plus élevée. Les sources possibles ont l'ordre de priorité suivant :

1. utilisateur

2. l'analyseur et l'application (définis dans la politique de découverte de réseau)

3. périphériques gérés

4. enregistrements NetFlow

Une nouvelle identité d'application de priorité supérieure ne remplacera pas une identité d'application actuelle si elle comporte moins de détails que l'identité actuelle.

En outre, lorsqu'un conflit d'identité survient, la résolution du conflit dépend des paramètres de la politique de découverte de réseau ou de votre résolution manuelle.

Identités actuelles des utilisateurs

Lorsque le système détecte plusieurs connexions au même hôte par différents utilisateurs, il suppose qu'un seul utilisateur est connecté à un hôte à la fois et que l'utilisateur actuel d'un hôte est le dernier utilisateur faisant autorité à la connexion. Si seules des connexions d'utilisateur ne faisant pas autorité ont été connectées à l'hôte, la dernière connexion d'utilisateur ne faisant pas autorité est considérée comme l'utilisateur actuel. Si plusieurs utilisateurs sont connectés par l'intermédiaire de sessions à distance, le dernier utilisateur signalé par le serveur est celui signalé à la centre de gestion.

Lorsque le système détecte plusieurs connexions au même hôte par le même utilisateur, le système enregistre la première fois qu'un utilisateur se connecte à un hôte spécifique et ignore les connexions ultérieures. Si un utilisateur est la seule personne à se connecter à un hôte particulier, la seule connexion enregistrée par le système est la connexion d'origine.

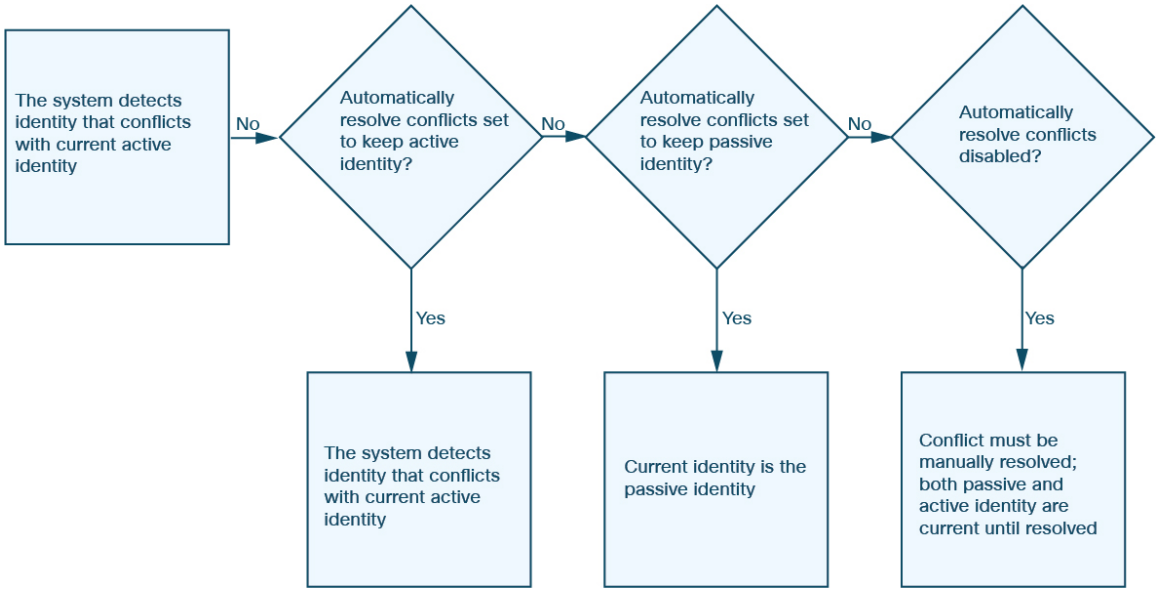
Si un autre utilisateur se connecte à cet hôte, le système enregistre la nouvelle connexion. Ensuite, si l'utilisateur initial se reconnecte, sa nouvelle connexion est enregistrée.

Conflits d'identité entre applications et système d'exploitation

Un *conflit d'identité* se produit lorsque le système signale une nouvelle identité passive qui est en conflit avec l'identité active actuelle et des identités passives précédemment signalées. Par exemple, l'identité passive précédente pour un système d'exploitation est Windows 2000, puis une identité active de Windows XP devient l'identité active de Windows XP. Ensuite, le système détecte une nouvelle identité passive d'Ubuntu Linux 8.04.1. Les identités de Windows XP et d'Ubuntu Linux sont en conflit.

En cas de conflit d'identité pour l'identité du système d'exploitation de l'hôte ou de l'une des applications de l'hôte, le système répertorie les deux identités en conflit comme actuelles et les utilise pour évaluer l'impact jusqu'à ce que le conflit soit résolu.

Un utilisateur disposant de privilèges d'administrateur peut résoudre automatiquement les conflits d'identité en choisissant de toujours utiliser l'identité passive ou de toujours utiliser l'identité active. Sauf si vous désactivez la résolution automatique des conflits d'identité, les conflits d'identité sont toujours résolus de cette manière.



Un utilisateur disposant de privilèges d'administrateur peut également configurer le système pour générer un événement en cas de conflit d'identité. Cet utilisateur peut ensuite configurer une politique de corrélation avec une règle de corrélation qui utilise une analyse Nmap comme réponse de corrélation. Lorsqu'un événement se produit, Nmap analyse l'hôte pour obtenir les mises à jour du système d'exploitation et des données d'application de l'hôte.

Données NetFlow

NetFlow est une application de Cisco IOS qui fournit des statistiques sur les paquets circulant dans un routeur. Il est disponible sur les périphériques réseau Cisco et peut également être intégré dans les périphériques Juniper, FreeBSD et OpenBSD.

Lorsque NetFlow est activé sur un périphérique réseau, une base de données sur le périphérique (le cache NetFlow) stocke les enregistrements des flux qui passent par le routeur. Un flux, appelé *connexion* dans le système, est une séquence de paquets qui représente une session entre un hôte source et un hôte de destination, à l'aide de ports, d'un protocole et d'un protocole d'application spécifiques. Le périphérique réseau peut être configuré pour exporter ces données NetFlow. Dans cette documentation, les périphériques réseau configurés de cette manière sont appelés *exportateurs NetFlow*.

Les périphériques gérés peuvent être configurés pour collecter les enregistrements des exportateurs NetFlow, générer des événements de fin de connexion unidirectionnels en fonction des données de ces enregistrements et finalement envoyer ces événements à centre de gestion pour être enregistrés dans la base de données des événements de connexion. Vous pouvez également configurer la politique de découverte de réseau pour ajouter des informations sur l'hôte et le protocole d'application à la base de données en fonction des informations des connexions NetFlow.

Vous pouvez utiliser ces données de découverte et de connexion pour compléter les données recueillies directement par vos périphériques gérés. Cette fonction est particulièrement utile si des exportateurs NetFlow surveillent des réseaux que les appareils gérés ne peuvent pas surveiller.

Exigences relatives à l'utilisation des données NetFlow

Avant de configurer le système Firepower pour analyser les données NetFlow, vous devez activer la fonction NetFlow sur les routeurs ou autres périphériques réseau compatibles avec NetFlow que vous prévoyez utiliser, et configurer les périphériques pour diffuser des données NetFlow vers un réseau de destination où l'interface de détection d'un périphérique géré est connecté.

Le système Firepower peut analyser les enregistrements NetFlow version 5 et version 9. Les exportateurs NetFlow **doivent** utiliser l'une de ces versions si vous souhaitez exporter les données vers le système Firepower. En outre, le système exige la présence de champs précis dans les modèles et les enregistrements NetFlow exportés. Si vos exportateurs NetFlow utilisent la version 9, que vous pouvez personnaliser, vous **devez** vous assurer que les modèles et les enregistrements exportés contiennent les champs suivants, dans n'importe quel ordre :

- IN_BYTES (1)
- IN_PKTS (2)
- PROTOCOL (4)
- TCP_FLAGS (6)
- L4_SRC_PORT (7)
- IPV4_SRC_ADDR (8)

- L4_DST_PORT (11)
- IPV4_DST_ADDR (12)
- LAST_SWITCHED (21)
- FIRST_SWITCHED (22)
- IPV6_SRC_ADDR (27)
- IPV6_DST_ADDR (28)

Comme le système Firepower utilise des périphériques gérés pour analyser les données NetFlow, votre déploiement doit inclure au moins un périphérique géré qui peut surveiller les exportateurs NetFlow. Au moins une interface de détection sur ce périphérique géré doit être connectée à un réseau où elle peut collecter les données NetFlow exportées. Comme les interfaces de détection sur les périphériques gérés n'ont généralement pas d'adresses IP, le système ne prend pas en charge la collecte directe des enregistrements NetFlow.

Notez que la fonctionnalité NetFlow échantillonné disponible sur certains périphériques réseau collecte les statistiques NetFlow uniquement sur un sous-ensemble de paquets qui passent par les périphériques. Bien que l'activation de cette fonctionnalité puisse améliorer l'utilisation du processeur sur le périphérique réseau, elle peut affecter les données NetFlow que vous collectez pour les analyser par le système Firepower.

Différences entre NetFlow et les données de périphérique géré

Le trafic représenté par les données NetFlow n'est pas directement analysé. Au lieu de cela, il convertit les enregistrements NetFlow exportés en journaux de connexion et en données de protocole d'hôte et d'application.

Par conséquent, il existe plusieurs différences entre les données NetFlow converties et les données de découverte et de connexion recueillies directement par vos appareils gérés. Vous devez garder ces différences à l'esprit lorsque vous effectuez une analyse qui nécessite :

- Des statistiques sur le nombre de connexions détectées
- Des système d'exploitation et autres informations relatives à l'hôte (y compris sur les vulnérabilités)
- Données d'application, y compris les renseignements sur le client, les renseignements sur l'application Web et les renseignements sur le fournisseur et le serveur de version
- Savoir quel hôte dans une connexion est l'initiateur et quel hôte est le répondeur

La politique de découverte de réseau par rapport à la politique de contrôle d'accès

Vous configurez la collecte de données NetFlow, y compris la journalisation des connexions, en utilisant les règles de la politique de découverte de réseau. Comparez cela à la journalisation des connexions détectées par les périphériques gérés, que vous configurez par règle de contrôle d'accès.

Types d'événements de connexion

Comme la collecte de données NetFlow est liée à des réseaux plutôt qu'à des règles de contrôle d'accès, vous n'exercez pas une gestion granulaire sur les connexions NetFlow que le système enregistre.

Les données NetFlow ne peuvent pas générer d'événements de renseignements de sécurité.

Les événements de connexion NetFlow peuvent uniquement être stockés dans la base de données des événements de connexion; vous ne pouvez pas les envoyer au journal système ou à un serveur d'interruption SNMP.

Nombre d'événements de connexion générés par session surveillée

Pour les connexions détectées directement par les périphériques gérés, vous pouvez configurer la règle de contrôle d'accès pour consigner un événement de connexion bidirectionnelle au début ou à la fin d'une connexion, ou les deux.

En revanche, comme les enregistrements NetFlow exportés contiennent des données de connexion unidirectionnelles, le système génère au moins deux événements de connexion pour chaque enregistrement NetFlow qu'il traite. Cela signifie également que le nombre de connexions apparaissant dans le résumé s'accroit de deux lors de chaque connexion basée sur des données NetFlow. Cela produit un nombre exagéré de connexions par rapport aux connexions qui se produisent réellement sur votre réseau.

Étant donné que l'exportateur NetFlow produit des enregistrements à intervalle fixe, même si une connexion est toujours en cours, des sessions longues peuvent entraîner l'exportation de plusieurs enregistrements, chacun générant un événement de connexion. Par exemple, si l'exportateur NetFlow exporte toutes les cinq minutes et qu'une connexion donnée dure douze minutes, le système génère six événements de connexion pour cette session :

- Une paire d'événements pour les cinq premières minutes
- Une paire pour les cinq secondes suivantes
- Une paire finale lorsque la connexion est terminée

Données de l'hôte et du système d'exploitation

Les hôtes ajoutés à la carte réseau à partir des données NetFlow ne disposent pas d'informations sur le système d'exploitation, NetBIOS ou le type d'hôte (hôte par rapport au périphérique réseau). Vous pouvez toutefois définir manuellement l'identité du système d'exploitation d'un hôte en utilisant la fonction de saisie de l'hôte.

Données d'application

Pour les connexions détectées directement par les périphériques gérés, le système peut définir les protocoles d'application, les clients et les applications Web en examinant les paquets dans la connexion.

Lorsque le système traite les enregistrements NetFlow, il utilise une corrélation de ports dans `/etc/sf/services` pour extrapoler l'identité du protocole d'application. Cependant, il n'y a aucune information sur le fournisseur ou la version de ces protocoles d'application. De plus, les journaux de connexion ne contiennent pas d'informations sur les applications client ou Web utilisées dans la session. Vous pouvez toutefois fournir manuellement ces informations à l'aide de la fonction de saisie de l'hôte.

Notez qu'une simple corrélation de ports signifie que les protocoles d'application exécutés sur des ports non standard peuvent être non identifiés ou mal identifiés. En outre, si aucune corrélation n'existe, le système marque le protocole d'application comme inconnu (`unknown`) dans les journaux de connexion.

Cartographie des vulnérabilités

Le système ne peut pas cartographier les vulnérabilités aux hôtes surveillés par les exportateurs NetFlow, sauf si vous utilisez la fonction de saisie d'hôte pour définir manuellement l'identité du système d'exploitation d'un hôte ou l'identité du protocole d'application. Notez que comme il n'y a aucune information client dans les connexions NetFlow, vous ne pouvez pas associer les vulnérabilités des clients aux hôtes créés à partir des données NetFlow.

Renseignements sur l'initiateur et le répondeur dans les connexions

Pour les connexions détectées directement par les périphériques gérés, le système peut déterminer quel hôte est l'initiateur ou la source, et qui est le répondeur ou la destination. Cependant, les données NetFlow ne contiennent pas d'informations sur l'initiateur ou le répondeur.

Lorsque le système traite les enregistrements NetFlow, il utilise un algorithme pour déterminer ces renseignements en se basant sur les ports que chaque hôte utilise, et si ces ports sont bien connus :

- Si les deux ports ou aucun des ports utilisés est un port bien connu, le système considère que l'hôte utilisant le port de numéro inférieur est le répondeur.
- Si un seul des hôtes utilise un port connu, le système considère que cet hôte est le répondeur.

À cette fin, un port connu est tout port numéroté de 1 à 1023 ou contenant des informations sur le protocole d'application dans `/etc/sf/services` sur le périphérique géré.

En outre, pour les connexions détectées directement par les périphériques gérés, le système enregistre deux décomptes dans l'événement de connexion correspondant :

- Le champ **Initiator Bytes** enregistre les octets envoyés.
- Le champ**Responder Bytes** enregistre les octets reçus.

Les événements de connexion basés sur des enregistrements NetFlow unidirectionnels ne contiennent qu'un seul octet, que le système affecte aux octets **Initiator Bytes** ou **Responder Bytes**, en fonction de l'algorithme basé sur le port. Le système définit l'autre champ sur 0. Notez que si vous consultez les récapitulatifs de connexion (données de connexion agrégées) des enregistrements NetFlow, les deux champs peuvent être renseignés.

Champs des événements de connexion NetFlow uniquement

Un petit nombre de champs ne sont présents que dans les événements de connexion générés par les enregistrements NetFlow.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.