

Contenu

[Introduction](#)

[Comparaison des permis de caractéristique](#)

[Informations supplémentaires](#)

[Article relatif](#)

Introduction

Ce document fournit un aperçu des différents permis de caractéristique qui peuvent être installés sur une version de logiciel courante 5.2 de centre de Gestion de FireSIGHT (également connu sous le nom de centre de la défense).

Remarque: Si vous utilisez une plus grande version que 5.2, Cisco vous recommande pour lire les notes de mise à jour relatives pour les dernières informations concernant l'autorisation, car de nouvelles caractéristiques peuvent être introduites sur une dernière version du produit.

Comparaison des permis de caractéristique

Le tableau suivant compare les systèmes des licences sur la version de logiciel 5.2 :

	S'il est installé, il vous permet à...	S'il n'est pas installé, ou est désactivé/supprimé/expiré...
FireSIGHT	<ul style="list-style-type: none">- Exécutez la détection d'hôte, d'application, d'utilisateur et de réseau- Détermine le nombre de...- Hôtes et utilisateurs de personne que vous pouvez surveiller- Utilisateurs que vous pouvez utiliser pour exécuter le contrôle de l'utilisateur- Vous héberge peut entreposé dans votre carte du réseau <p>Remarque: La capacité des hôtes de FireSIGHT et des utilisateurs sont limités par le modèle matériel du centre de la défense. Pour DC750, DC1500, DC3500 et centre virtuel de la défense, les limites sont 2000, 50000, 300000 et 50000 respectivement.</p>	<p>Vous pouvez encore exécuter...</p> <ul style="list-style-type: none">- Configuration de système de base- Surveillance de la santé- Enregistrement- Se connecter de connexion- Profilage du trafic- Contrôle d'accès Fondé(e) sur le réseau (zone, réseau, VLAN, et états de règle de port)
Protégez	<ul style="list-style-type: none">- Exécutez la détection et la prévention	<ul style="list-style-type: none">- Si vous désactivez la

	<p>d'intrusion</p> <ul style="list-style-type: none"> - Contrôle d'accès de base (le filtrage de trafic et l'IPS) - Incidence d'événement (actionnée par FireSIGHT) - Accord Automated (actionné par FireSIGHT) - Contrôle de fichier 	<p>protection, vous désactivez le contrôle et le Filtrage URL aussi.</p>
<p>Contrôle (Exige le permis de protection)</p>	<ul style="list-style-type: none"> - Contrôle d'accès avancé (imposez l'application et le contrôle de l'utilisateur - l'agent d'utilisateur est exigé). - Exécutez la commutation et le routage (relais DHCP et NAT y compris). - Périphériques gérés de batterie dans un déploiement facilement disponible. 	<ul style="list-style-type: none"> - Sinon installé, vous pouvez pouvoir créer les Commutateurs et les Routeurs virtuels, mais vous... - Ne peuvent pas créer les interfaces commutées, conduites, ou hybrides - Ne peut pas créer des entrées NAT, ou configurez le relais DHCP pour les Routeurs virtuels. - Ne peut pas appliquer une configuration de périphérique qui inclut la commutation ou le routage à un périphérique géré où vous n'avez pas activé le contrôle. - Les Commutateurs et les Routeurs virtuels ne sont pas utiles sans interfaces commutées et conduites. - Ne peut pas établir le groupement entre les périphériques gérés. - Si le permis de contrôle est supprimé ou désactivé (en décochant la case) pour un appareil spécifique du C.C... - Les périphériques affectés ne cessent pas d'exécuter la commutation ou le routage. - Il ne cassera pas les batteries. - Vous ne pouvez pas réappliquer des stratégies existantes de contrôle d'accès s'ils incluent des règles avec l'utilisateur ou les états d'application. - Puisqu'un permis de contrôle est exigé pour le Filtrage URL, supprimer ou désactiver un permis de contrôle a le même effet que supprimant ou

		désactivant votre permis de Filtrage URL.
Filtrage des URL (Exige le permis de contrôle)	<p>- Écrivez les règles de contrôle d'accès qui déterminent le trafic qui peut traverser le réseau basé sur l'URLs demandé par les hôtes surveillés.</p> <p>- Corrélation avec les informations sur ces URL demandées, qui sont obtenues d'un service en nuage par le centre de la défense.</p> <p>Remarque: Le Filtrage URL exige l'abonnement annuel. À partir de la version de logiciel 5.3.0.1, le système de FireSIGHT n'exige plus un permis de contrôle d'activer le Filtrage URL. Seulement un permis de protection est exigé.</p>	<p>- Règles de contrôle d'accès avec l'arrêt d'états URL immédiatement filtrant l'URLs.</p> <p>- le C.C peut plus ne contacter le service en nuage.</p> <p>- Des stratégies existantes de contrôle d'accès ne peuvent pas être réappliquées, si elles incluent des règles avec des états URL.</p>
Malware	<p>- Détection Fondé(e) sur le réseau de malware.</p> <p>Remarque: Pour détecter et bloquer sur option vos utilisateurs de télécharger ou de télécharger certains types de fichier, un permis de protection est nécessaire.</p>	<p>- Vous ne pourrez pas détecter le malware dans des fichiers téléchargés et téléchargés par vos utilisateurs.</p> <p>Remarque: Pour recevoir la détection basée sur point de malware, un abonnement de FireAMP est nécessaire. Vous n'avez pas besoin d'un permis de FireSIGHT de recevoir des événements basés sur point de malware, utilisez l'abonnement de FireAMP de votre organisation.</p>

Informations supplémentaires

- Les permis sont la particularité modèle. Le système ne te permet pas pour activer un permis sur un périphérique géré à moins que le permis apparie le modèle du périphérique. Par exemple, si vous avez cinq 3D8250 et cinq périphériques 3D8140 et voulez autoriser tous avec la protection et le contrôle, vous devez acheter la protection cinq 3D8250 et contrôler des permis et la protection cinq 3D8140 et contrôler des permis.
- Tous les permis ci-dessus de caractéristique sont installés à un centre de Gestion de FireSIGHT ou au centre de la défense. Il n'y a aucun permis d'installer sur un périphérique géré.
- Les centres de la défense dans une paire facilement disponible ne partagent pas des permis.

Vous devez appliquer les permis équivalents à chaque membre des paires. Un permis est généré a basé sur la seule clé de licence de chaque centre de la défense, donc, vous ne pouvez pas utiliser les mêmes permis à différents centres de la défense.

Article relatif

- [Caractéristiques et capacités prises en charge de divers modèles matériels de système de FireSIGHT](#)