Premiers pas avec Cisco Secure Workload

Les réseaux actuels comprennent des applications s'exécutant dans un environnement multinuage hybride qui utilise des charges de travail sans système d'exploitation, la virtualisation, et des charges de travail basées sur le nuage et les conteneurs. La difficulté principale dans un tel environnement est d'améliorer la sécurité des applications et des données sans sacrifier l'agilité. Cisco Secure Workload fournit une protection complète de la charge de travail en rapprochant la sécurité des applications et en adaptant la posture de sécurité qui est basée sur le comportement applicatif. Cisco Secure Workload réalise cette adaptation en utilisant des techniques avancées d'apprentissage automatique et d'analyse du comportement. Il s'agit d'une solution prête à l'emploi qui prend en charge les scénarios de sécurité suivants :

- Mettre en œuvre un modèle de confiance nulle avec des politiques de microsegmentation qui autorisent uniquement le trafic nécessaire à des fins d'entreprise.
- Détecter les anomalies dans les charges de travail à l'aide du référencement et de l'analyse comportementales.
- Détecter des vulnérabilités et des expositions courantes associées aux logiciels installés sur les serveurs
- Recommander la mise en quarantaine des serveurs si les vulnérabilités persistent après l'application des politiques et le blocage de la communication.

Charges de travail et adresses IP dans Cisco Secure Workload

Dans Cisco Secure Workload, une charge de travail est une adresse IP. Les hôtes sur lesquels des agents logiciels sont installés sont appelés des charges de travail et les hôtes sur lesquels aucun agent n'est installé sont des adresses IP.

Remarque Pour consulter le contrat de licence de l'utilisateur final et le contrat de licence d'utilisateur final supplémentaire pour votre produit, consultez le Contrat de licence d'utilisateur final et les contrats de licence d'utilisateur final supplémentaires.

- Navigateurs pris en charge, on page 2
- Assistant de démarrage rapide, à la page 2
- Premiers pas avec la segmentation et la microsegmentation, à la page 2

Navigateurs pris en charge

Cisco Secure Workload prend en charge les navigateurs Web suivants :

- Google Chrome
- Microsoft Edge

Assistant de démarrage rapide

Un assistant facultatif peut vous guider dans la création de la première branche de votre arborescence de portée, qui est une première étape vers la génération et l'application de politiques à l'application de votre choix. L'assistant présente les concepts et les avantages des étiquettes et de la portée.

Les rôles d'utilisateur suivants peuvent accéder à l'assistant :

- L'administrateur de site
- Assistance technique
- Propriétaire de portée racine

Pour accéder à l'assistant, effectuez l'une des opérations suivantes :

- Connectez-vous à Cisco Secure Workload.
- Cliquez sur le lien dans la bannière bleue. La bannière bleue s'affiche en haut de toutes les pages.
- Cliquez sur **Overview** (Présentation) dans le menu principal.

Remarque Vous ne pouvez pas accéder à l'assistant si des portées sont déjà définies dans **Organize (Organiser)** > **Scopes and Inventory (Portées et inventaire)** Supprimez les portées existantes pour accéder à l'assistant.

Premiers pas avec la segmentation et la microsegmentation

Utilisez les procédures générales données ici pour configurer des politiques de segmentation et de microsegmentation à l'aide de Cisco Secure Workload.

Processus général de mise en œuvre de la microsegmentation

Le but de la segmentation et de la microsegmentation est de n'autoriser que le trafic nécessaire à des fins commerciales et de bloquer tout autre trafic.

Procédure

Étape 1 Vérifiez que Cisco Secure Workload prend en charge les plateformes et les versions sur lesquelles vos charges de travail s'exécutent, et les systèmes qui fournissent des informations essentielles à vos politiques. Reportez-vous à la section Matrice de compatibilité de Cisco Secure Workload.

Étape 2 Installer les agents sur les charges de travail.

Les agents recueillent les données de flux et d'autres informations nécessaires à Cisco Secure Workload pour regrouper les charges de travail et déterminer les politiques appropriées. Les agents appliquent également les politiques approuvées. Pour en savoir plus, y compris les liens vers les listes des plateformes prises en charge et la configuration requise, consultez Déploiement des agents logiciels.

Étape 3 Rassemblez ou téléversez des étiquettes qui décrivent vos charges de travail.

Les étiquettes vous permettent de comprendre facilement l'objectif de chaque charge de travail et fournissent d'autres renseignements clés sur chaque charge de travail.

Vous avez besoin de ces informations pour regrouper les charges de travail, appliquer les politiques appropriées et comprendre les politiques suggérées par Cisco Secure Workload. Les étiquettes constituent la base de la gestion des groupes qui simplifient la gestion des politiques. Pour en savoir plus, consultez les sections Étiquettes de charge de travail et Importation d'étiquettes personnalisées.

Étape 4 Créez une arborescence de portée en fonction de vos étiquettes de charge de travail.

Les groupes logiques de charges de travail que les étiquettes vous aident à créer sont appelés portées, et un ensemble d'étiquettes bien choisi vous aide à créer une carte hiérarchique de votre réseau appelée arborescence de portées. Cette vue hiérarchique des charges de travail sur votre réseau est essentielle pour créer et maintenir efficacement des politiques. La vue hiérarchique vous permet de créer une politique une seule fois et de l'appliquer automatiquement à chaque charge de travail sur cette branche de l'arborescence. Cette vue vous permet également de déléguer la responsabilité de certaines applications (ou parties de votre réseau) à des personnes qui ont l'expertise nécessaire pour déterminer les politiques appropriées pour ces charges de travail.

Vous pouvez interroger les charges de travail et les regrouper dans des portées en fonction de leurs étiquettes. Par exemple, vous pouvez créer une portée appelée App Courriel qui inclut toutes les charges de travail ayant les étiquettes Application = App Courriel et Environnement = Production. Vous pouvez créer une portée parente pour la portée Application = App Courriel en utilisant la requête Environnement = Production. La portée de la production comprend l'application de courriel de production et toutes les autres charges de travail étiquetées Environnement = Production.

Pour en savoir plus, consultez Portées et inventaire.

Si vous n'avez encore créé aucune portée, vous pouvez utiliser l'assistant de démarrage rapide pour créer une arborescence de portées. Pour en savoir plus, consultez Assistant de démarrage rapide, à la page 2.

Étape 5 Créez un espace de travail pour chaque portée pour laquelle vous souhaitez créer des politiques.

L'espace de travail est l'endroit où vous gérez les politiques pour les charges de travail de cette portée. Pour en savoir plus, consultez Espaces de travail.

Étape 6 Créez manuellement des politiques qui s'appliquent à votre réseau.

Par exemple, vous pouvez autoriser l'accès de toutes les charges de travail internes à votre serveur NTP et refuser tout le trafic externe, ou refuser l'accès de tous les hôtes non internes, à moins que cela ne soit explicitement autorisé. Les politiques peuvent être absolues, ce qui signifie qu'elles ne peuvent pas être remplacées par des politiques plus spécifiques, ou par défaut, où elles peuvent être remplacées par des politiques plus spécifiques.

Pour en savoir plus, consultez Créer manuellement des politiques.

Cisco Secure Workload propose des modèles de politiques qui facilitent la création de ces dernières. Pour en savoir plus, consultez Modèles de politiques.

Vous pouvez appliquer les politiques créées manuellement sans attendre qu'elles soient découvertes. Pour en savoir plus, consultez Appliquer des politiques.

Étape 7 Détectez automatiquement les politiques en fonction des schémas de trafic existants.

Cisco Secure Workload analyse le trafic entre les charges de travail, regroupe les charges de travail en fonction de leur comportement et propose un ensemble de politiques visant à autoriser le trafic dont votre entreprise a besoin pour que vous puissiez bloquer tout autre trafic.

L'analyse d'un plus grand nombre de flux de données sur une période plus longue permet de formuler des suggestions de politiques plus précises.

Vous pouvez découvrir les politiques de manière itérative. Vous trouverez plus d'informations à ce sujet dans la suite de cette procédure).

1. Découvrez les politiques pour une branche de votre arborescence de portée.

   Si vous venez de commencer, vous pouvez avoir un ensemble temporaire de politiques en place et fournir une protection contre les menaces futures.

2. Découvrez les politiques des portées uniques.

   En règle générale, vous effectuez cette opération pour les portées qui se trouvent au bas de votre arborescence ou près du bas de celle-ci. Ces portées comprennent généralement les charges de travail pour une seule application.

Pour en savoir plus, consultez Découverte automatique des politiques et Découvrir les politiques relatives à une portée ou à une branche de l'arborescence de la portée.

Étape 8 Examinez et analysez vos politiques.

Examinez attentivement vos politiques pour vous assurer qu'elles produisent les effets escomptés et qu'il n'y a pas d'effets secondaires imprévus.

Collaborez avec des experts de domaine et des propriétaires d'applications de votre organisation pour comprendre les besoins et la pertinence des politiques suggérées.

a) Passez en revue les politiques et les grappes suggérées par Cisco Secure Workload.

   (Les grappes sont des groupes de charges de travail au sein d'une portée qui sont étroitement liées et peuvent nécessiter des politiques plus adaptées que les politiques visant l'ensemble de la portée. Pour en savoir plus, consultez Regroupement des charges de travail : grappes et filtres d'inventaire).

   Pour en savoir plus, consultez Consulter les politiques découvertes automatiquement.

b) Analysez vos politiques pour voir leur incidence sur le trafic réel sur votre réseau.

   Utilisez l'analyse des politiques et les autres outils de Cisco Secure Workload pour confirmer que vos politiques autorisent le trafic dont votre entreprise a besoin pour exercer ses activités. Pour en savoir plus, consultez Analyse en direct. et Représentation visuelle des politiques.

   Lorsque vous analysez les résultats de vos politiques, gardez les points suivants à l'esprit :

   - Les politiques dans les espaces de travail pour les portées supérieures d'une branche peuvent affecter les charges de travail des portées inférieures de la branche. Pour en savoir plus, consultez Héritage des politiques et arborescence de portée.

- La microsegmentation crée un pare-feu miniature autour de chaque charge de travail. Pour qu'une connexion soit réussie, le consommateur et le fournisseur de la transaction doivent avoir des politiques autorisant le trafic. Si les deux charges de travail ne se trouvent pas dans la même portée, la création de ces politiques peut nécessiter des étapes supplémentaires. Pour en savoir plus, consultez Lorsque le consommateur et le fournisseur se trouvent dans des portées différentes : options de politiques.

Étape 9 Détectez les politiques de façon itérative, en fonction des besoins.

Un flux de trafic plus important produit des suggestions de politiques plus précises. Par exemple, pour un rapport mensuel, même trois semaines de données peuvent ne pas saisir tout le trafic essentiel. Continuez de découvrir les politiques et passer en revue et analyser de nouvelles suggestions de politiques. Chaque exécution de découverte propose des politiques en fonction des flux de trafic actuels.

Vous pouvez également procéder à une découverte itérative des politiques afin de prendre en compte les modifications apportées aux paramètres de découverte des politiques et aux grappes approuvées. Pour en savoir plus, consultez Réviser les politiques de manière itérative.

Avant de réexécuter la découverte automatique des politiques, assurez-vous d'approuver les politiques et les grappes que vous souhaitez conserver.

Chaque fois que vous redécouvrez des politiques, vous devez les passer en revue et les analyser.

Étape 10 Lorsque vous êtes prêt, appliquez les politiques.

Une fois que vous avez déterminé que les politiques associées à un espace de travail (et donc la portée associée) sont appropriées et qu'elles bloqueront le trafic indésirable sans interrompre les services essentiels, vous pouvez appliquer ces politiques.

Vous pouvez appliquer les politiques de manière itérative; par exemple, vous pourriez initialement appliquer uniquement les politiques créées manuellement dans des portées situés près du sommet de votre arborescence, puis, au fil du temps, appliquer les politiques découvertes dans des portées inférieurs de l'arborescence.

Pour en savoir plus, consultez Appliquer des politiques.

Configurer la microsegmentation pour les charges de travail s'exécutant sur des machines sans système d'exploitation ou des machines virtuelles

Procédure

Étape 1 Rassemblez les adresses IP des charges de travail sur votre réseau.

Pour chaque charge de travail, vous voudrez également le nom de l'application, le propriétaire de l'application, l'environnement (de production ou hors production) et d'autres renseignements comme la région géographique qui détermineront les politiques à appliquer.

Si vous n'avez pas de base de données de gestion des configurations (CMDB), vous pouvez recueillir cette information dans une feuille de calcul.

Pour commencer, choisissez une seule application sur laquelle vous pouvez vous concentrer.

Étape 2 Installez les agents sur les charges de travail virtuelles ou sans système d'exploitation prises en charge.

Pour en savoir plus, consultez la section Déploiement des agents logiciels.

Étape 3 Téléchargez des étiquettes qui décrivent ces charges de travail.

Pour en savoir plus, consultez les sections Étiquettes de charge de travail et Importation d'étiquettes personnalisées.

Vous pouvez également exécuter l'assistant de démarrage rapide pour créer des étiquettes et la première branche de votre arborescence de portée . Pour en savoir plus sur l'assistant, consultez Assistant de démarrage rapide.

Étape 4 Si nécessaire, créez ou mettez à jour votre arborescence de portée en fonction de vos étiquettes.

Pour en savoir plus, consultez Portées et inventaire.

Étape 5 Créez un espace de travail pour chaque portée pour laquelle vous souhaitez appliquer des politiques.

Pour en savoir plus, consultez Espaces de travail.

Étape 6 Créez des politiques manuelles qui s'appliquent à votre réseau.

Pour en savoir plus, consultez Créer manuellement des politiques.

Étape 7 Pour en savoir plus sur les politiques spécifiques à la plateforme, consultez Politiques spécifiques à la plateforme.

Étape 8 Détectez automatiquement les politiques dans les espaces de travail associés à des portées de niveau inférieur.

Pour en savoir plus, consultez Découverte automatique des politiques et ses sous-sections.

Étape 9 Examinez et analysez les politiques suggérées.

Pour en savoir plus, consultez Examiner et analyser les politiques et les sous-sections.

Étape 10 Détectez les politiques de façon itérative, en fonction des besoins.

Pour en savoir plus, consultez Réviser les politiques de manière itérative et les sous-sections.

Étape 11 Lorsque vous êtes prêt, appliquez les politiques.

Vous pouvez appliquer des politiques lorsque vous êtes satisfait du comportement des politiques dans chaque espace de travail.

Vous devez appliquer les politiques à la fois dans l'espace de travail et dans la configuration de l'agent.

Pour en savoir plus, consultez Appliquer des politiques.

Configurer la microsegmentation pour les charges de travail en nuage

Procédure

Étape 1 Installez des agents sur vos charges de travail infonuagique, si nécessaire;

Les connecteurs infonuagique offrent une granularité de niveau VPC/VNet pour la découverte et l'application des politiques. Installez les agents sur des plateformes prises en charge si vous avez besoin de la découverte et de l'application des politiques à un niveau plus granulaire.

Installez les agents en fonction du système d'exploitation sur lequel votre service infonuagique est exécuté. Pour en savoir plus, consultez la section Déploiement des agents logiciels.

Étape 2 Configurez des connecteurs infonuagique pour recueillir des étiquettes et des données de flux.

Pour en savoir plus, consultez ;

- Connecteur AWS.
- Connecteur Azure.
- Connecteur GCP

Étape 3 Créez des espaces de travail pour les portées créées par le connecteur.

Pour en savoir plus, consultez Espaces de travail.

Étape 4 Découvrir automatiquement les politiques.

Découvrez les politiques pour chaque portée définie par le VPC/VNet et, le cas échéant, pour des portées plus granulaires.

Pour en savoir plus, consultez la section Découverte automatique des politiques.

Étape 5 Examinez et analysez les politiques suggérées.

Consultez Examiner et analyser les politiques et les sous-sections.

Étape 6 Détectez les politiques de façon itérative, en fonction des besoins.

Consultez Réviser les politiques de manière itérative et les sous-sections.

Étape 7 Approuvez et appliquez les politiques pour chaque portée.

Vous devez activer l'application dans l'espace de travail concerné et dans le connecteur pour chaque VPC ou VNet, ainsi que pour tous les agents installés sur des charges de travail individuelles.

- Pour en savoir plus, consultez Appliquer des politiques et les sous-sections.
- Pour en savoir plus :
  - Pour les charges de travail basées sur AWS, consultez Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire AWS.
  - Pour les charges de travail basées sur Azure, consultez Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire Azure.
  - Pour les charges de travail basées sur GCP, consultez Bonnes pratiques lors de l'application de la politique de segmentation pour l'inventaire GCP.

Configurer la microsegmentation pour les charges de travail basées sur Kubernetes

Procédure

Étape 1 Installer les agents sur les charges de travail basées sur Kubernetes. Assurez-vous de vérifier les exigences et les conditions préalables.

Pour en savoir plus, consultez Agents Kubernetes/Openshift - Visibilité approfondie et mise en application.

Les agents sont automatiquement installés sur toutes les charges de travail futures gérées par le service Kubernetes applicable.

Étape 2 Rassemblez des étiquettes pour vos charges de travail basées sur Kubernetes.

Pour en savoir plus :

- Pour les charges de travail Kubernetes et OpenSource standard, voir Orchestrateurs externes dans Cisco Secure Workload et Kubernetes/OpenShift.
- Pour Elastic Kubernetes Services (EKS) fonctionnant sur Amazon Web Services (AWS), consultez Connecteur AWS et Services gérés Kubernetes s'exécutant sur AWS (EKS).
- Pour Azure Kubernetes Services (AKS), voir Connecteur Azure et Services gérés Kubernetes fonctionnant sur Azure (AKS)
- Pour Google Kubernetes Engine (GKE) fonctionnant sur Google Cloud Platform (GCP), consultez Services gérés Kubernetes s'exécutant sur GCP (GKE).

Étape 3 Créez ou mettez à jour votre arborescence de portée en fonction de vos étiquettes.

Pour en savoir plus, consultez Portées et inventaire.

Étape 4 Créez un espace de travail pour chaque portée pour laquelle vous souhaitez appliquer des politiques.

Pour en savoir plus, consultez Espaces de travail.

Étape 5 Détectez automatiquement les politiques pour chaque portée de bas niveau.

Pour en savoir plus, consultez la section Découverte automatique des politiques.

Étape 6 Pour en savoir plus sur les options supplémentaires applicables, consultez Politiques spécifiques à la plateformel.

Étape 7 Examinez et analysez les politiques suggérées.

Pour en savoir plus, consultez Examiner et analyser les politiques.

Étape 8 Découvrir, passer en revue et analyser les politiques de manière itérative, le cas échéant.

Pour en savoir plus, consultez Réviser les politiques de manière itérative.

Étape 9 Lorsque vous êtes prêt, approuvez et appliquez les politiques pour chaque portée.

Vous devez activer l'application des politiques dans l'espace de travail et pour les agents.

Pour plus de renseignements, consultez les sections Appliquer des politiques et Application des conteneurs.

Prochaine étape

Renseignements connexes

- Étiquettes de charge de travail
- Portées et inventaire
- Déployer des agents logiciels
- Gérer le cycle de vie des politiques dans Cisco Secure Workload
- Guide de démarrage rapide Cisco Secure Workload

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.