Présentation abrégée

Cisco ISE (Identity Services Engine)

Le réseau de l'entreprise n'est plus confiné entre quatre murs. Il suit les déplacements des employés et des données. Les employés utilisent davantage de terminaux pour accéder aux ressources de l'entreprise via un nombre croissant de réseaux non professionnels. La mobilité et l'Internet of Everything (IoE) ont transformé la manière dont nous vivons et travaillons. Les entreprises doivent être capables de prendre en charge la multiplication des nouveaux appareils connectés au réseau, tout en se protégeant d'une multitude de malwares. Les violations de données récemment médiatisées sont la preuve qu'il est impératif de sécuriser des réseaux d'entreprise en constante évolution.

À mesure que le réseau moderne s'étend, le triage des ressources, la gestion des technologies de sécurité disparates et la maîtrise des risques se compliquent. Face à cette complexité à laquelle s'ajoutent la connectivité omniprésente de l'IoE et un manque manifeste de ressources IT, les éventuelles retombées d'une incapacité à identifier et à éliminer les malwares peuvent être très lourdes.

Une approche différente est nécessaire pour la gestion et la sécurité de l'entreprise mobile en constante évolution. Elle repose sur la solution Cisco® ISE (Identity Services Engine).

Bénéfices

- **Mettez en place un contrôle d'accès centralisé et ultrasécurisé** basé sur les rôles pour appliquer une politique cohérente d'accès au réseau, que les utilisateurs se connectent via un réseau filaire, sans fil ou un VPN.
- **Bénéficiez d'une meilleure visibilité et d'une identification plus précise des appareils** grâce au service de profilage des terminaux et aux flux d'informations associés de Cisco® ISE (Identity Services Engine), qui aident à réduire le nombre de terminaux inconnus.
- **Simplifiez l'expérience d'utilisation des invités** pour mieux les intégrer et mieux les gérer en proposant des portails d'accès personnalisés à l'image de votre entreprise pour les terminaux mobiles et de bureau. Ces portails se créent en quelques minutes grâce à des workflows visuels dynamiques qui vous permettent de gérer facilement chaque paramètre de l'accès des invités.

Soyez moins vulnérable et réduisez vos risques

Anticipez les attaques grâce à une meilleure visibilité et un meilleur contrôle. Bénéficiez d'une visibilité complète sur les utilisateurs et les terminaux qui accèdent à votre réseau, ainsi que d'un contrôle dynamique permettant de garantir que seuls les utilisateurs autorisés et détenteurs de terminaux autorisés peuvent accéder aux services de l'entreprise demandés.

La version 2.0 d'ISE a été repensée. Désormais, le contrôle d'accès sécurisé est le même pour les réseaux multifournisseurs filaires et sans fil, ainsi que pour les connexions VPN à distance. Grâce à ses capteurs réseau et à ses fonctionnalités intelligentes de profilage, Cisco ISE vous permet d'obtenir une visibilité intégrale sur les utilisateurs et les appareils qui accèdent aux ressources. En partageant des données contextuelles stratégiques par le biais de l'intégration sur les plates-formes partenaires de l'écosystème et par l'application de la politique Cisco TrustSec pour la segmentation définie par logiciel, Cisco ISE transforme la nature du réseau, qui passe du statut de simple vecteur de données à celui de garant de la sécurité permettant d'accélérer la détection et l'élimination des malwares.

- **Accélérez le BYOD et la mobilité de l'entreprise** grâce au déploiement d'une solution prête à l'emploi, à l'intégration et à la gestion de terminaux en libre-service, à la gestion interne de certificats de terminaux et à une solution partenaire de gestion de la mobilité d'entreprise pour l'intégration de terminaux sur et hors site.
- **Établissez une politique de segmentation définie par logiciel pour maîtriser les attaques du réseau** grâce à la technologie Cisco TrustSec®, qui permet de contrôler les accès en fonction des rôles des utilisateurs sur la couche de routage et de commutation. Segmentez dynamiquement l'accès sans la complexité liée au déploiement de plusieurs VLAN ou à la restructuration du réseau.
- **Échangez des données contextuelles détaillées avec des solutions partenaires de réseau et de sécurité** pour améliorer leur efficacité globale et réduire les délais de détection et d'élimination des attaques du réseau.
- **Maîtrisez automatiquement les malwares** grâce à l'intégration de Cisco Firepower Management Center et à ISE qui peut traiter, surveiller ou supprimer les terminaux infectés.

Les mises à jour et les améliorations de Cisco ISE 2.0 comprennent :

- L'intégration avec le moteur de services de mobilité (MSE) Cisco, qui permet de fournir des informations relatives à la localisation dans le but de créer et d'appliquer des règles d'accès en fonction de l'emplacement de l'utilisateur. Par exemple, autoriser le personnel de santé à accéder aux dossiers médicaux des patients uniquement depuis l'hôpital.
- L'amélioration de notre architecture ouverte pour certains partenaires de l'écosystème ISE, afin que les clients puissent utiliser leurs solutions de sécurité avec ISE, dans le but d'identifier, de maîtriser et d'éliminer plus rapidement les malwares.
- La prise en charge des appareils d'accès au réseau et des terminaux IPv6 tiers pour étendre les fonctionnalités de conformité des terminaux d'ISE à davantage de types de réseaux.
- La simplification de la gestion des politiques, et notamment de la gestion de l'authentification, de l'autorisation et de la traçabilité des appareils (AAA), avec les fonctionnalités d'accès TACACS+ et RADIUS afin de faciliter le déploiement des politiques de contrôle d'accès sécurisé sur les réseaux filaires.
- Cisco AnyConnect 4.2 comprend le nouveau module de visibilité du réseau (NVM) qui fournit des informations détaillées sur le trafic des applications, alors qu'elles n'étaient jusque-là pas disponibles pour les terminaux hors site.

De plus, ISE exploite la technologie Cisco Platform Exchange Grid (pxGrid) pour partager des données contextuelles riches avec les solutions intégrées de l'écosystème partenaire. Cette technologie optimise leur fonctionnement notamment pour identifier, atténuer et éliminer les malwares sur tout le réseau de l'entreprise. Globalement, le contrôle d'accès sécurisé est centralisé et simplifié pour garantir un provisionnement sans risque des services d'entreprise, renforcer la sécurité de l'infrastructure, faire respecter les critères de conformité et simplifier les opérations de service.

Grâce à son intégration avec les solutions de gestion des informations et des événements de sécurité (SIEM) et avec les solutions de protection contre les malwares (TD), ainsi qu'à la visibilité accrue qu'il fournit sur le réseau et à ses fonctionnalités de contrôle d'accès sécurisé, ISE joue un rôle essentiel au sein des solutions Cisco de cybersécurité et d'exploitation du réseau pour les détections et les interventions. Enfin, ISE offre la visibilité, le contexte et le contrôle dynamique dont l'entreprise a besoin pour mettre en œuvre une sécurité efficace tout au long du processus d'attaque. Elle peut contrôler l'accès au réseau avant l'attaque, identifier les malwares et les bloquer pendant l'attaque, et réduire les délais de détection et de résolution après l'attaque.

Étapes suivantes

Pour en savoir plus sur Cisco ISE, visitez http://www.cisco.com/go/ise ou contactez votre conseiller Cisco.

C45-654884-13 10/15