Cisco TrustSec

Un composant de base des réseaux sécurisés sans frontières

Répondre aux défis des clients

Les frontières physiques disparaissent. Les clients doivent prendre en charge une main-d'œuvre mobile, gérer l'externalisation et répondre à la « consumérisation » des technologies de l'information. En outre, en raison d'un environnement menaçant, une protection plus efficace de l'infrastructure des entreprises et des ressources d'information de valeur est devenue une obligation incontournable. Enfin, les obligations en termes de réglementation et d'industrie imposent des conditions strictes à de nombreuses organisations. En tant que composant de base visant à sécuriser des réseaux sans frontières, la solution Cisco® TrustSec aide les clients à mettre en œuvre une collaboration sécurisée, à renforcer la sécurité et à répondre aux exigences de conformité.

Fonctions essentielles

Cisco TrustSec sécurise de manière complète les réseaux et l'accès aux ressources critiques de l'entreprise en créant une visibilité et des contrôles qui s'appliquent à tous les utilisateurs et en détectant et surveillant les périphériques IP. Cette sécurisation est basée sur un contrôle d'accès reposant sur des stratégies, sur un réseau reconnaissant l'identité et sur une protection de la confidentialité et de l'intégrité des données sur le réseau.

Contrôle d'accès reposant sur des stratégies : Cisco TrustSec offre un contrôle de l'accès au réseau basé sur une politique cohérente, aux utilisateurs (employés, sous-traitants ou invités par exemple), aux terminaux (ordinateurs portables, téléphones IP, imprimantes) et aux périphériques de réseau (commutateurs, routeurs etc.). Cisco TrustSec peut contrôler l'autorisation d'accès à un utilisateur ou un périphérique, les stratégies de sécurité que doivent respectiver les terminaux, par exemple le contrôle de posture, et les ressources qu'un utilisateur est autorisé à utiliser sur le réseau.

Réseau reconnaissant l'identité : Cisco TrustSec utilise les informations sur l'utilisateur final et l'identité du périphérique ainsi que d'autres facteurs (comme l'heure, l'emplacement, le rôle de l'utilisateur au sein de l'organisation) pour fournir des contrôles de stratégie de sécurité précis. TrustSec fournit d'autres services réseau basés sur la notion de rôle, par exemple la prise en charge de Cisco Medianet et et une qualité de service pour les applications critiques de l'entreprise associée aux utilisateurs dans des rôles spécifiques.

Intégrité et confidentialité des données : Cisco TrustSec sécurise les chemins de données dans l'environnement de commutation avec le chiffrement offert par la norme IEEE 802.1AE. La confidentialité et l'intégrité des données sont assurées entre les équipements au niveau du port du commutateur, lien par lien. L'infrastructure de commutation Cisco gère les contrôles afin que les applications critiques de sécurité, comme les pare-feu, la prévention des intrusions et l'inspection des contenus puissent garder la visilibilité dans les flux des données.

Avantages

Permet une collaboration sécurisée : Cisco TrustSec affecte dynamiquement l'accès et les services aux utilisateurs et périphériques dans un contexte de main d'œuvre dynamique. Les fonctionnalités offertes par TrustSec permettent de créer un environnement de travail collaboratif sécurisé et une expérience utilisateur homogène.

Sécurité renforcée : Cisco TrustSec sécurise l'accès au réseau et aux ressources - filaires, sans fil ou VPN - garantissant que les terminaux sont autorisés et sûrs. TrustSec applique des stratégies de sécurité sur l'ensemble du réseau. En outre, TrustSec protège la confidentialité et l'intégrité des données du réseau grâce à un chiffrement au niveau du port du commutateur.

Conformité des adresses : Cisco TrustSec aide à respecter les conditions de conformité des adresses en sachant qui entre sur le réseau, ce que ces entrants y font et à quel type de ressources ils ont accès. Les clients peuvent utiliser ces informations et fonctionnalités pour les contrôles, l'audit et la génération de rapports dans le cadre de leurs efforts visant à respecter les conditions de conformité.

Gamme de produits

Cisco TrustSec inclut trois composantes : l'infrastructure, la politique de sécurité, et le client.

Composants d'infrastructure : les commutateurs Cisco Catalyst® gamme 2900/3560/3700/4500/6500 et les commutateurs Cisco Nexus™ 7000 interagissent avec les utilisateurs du réseau pour l'authentification et l'autorisation. L'accès au réseau est dicté par la politique de sécurité, l'identité de l'utilisateur et d'autres attributs. Les méthodes d'authentification souples incluent la norme 802.1X, l'authentification via un portail web et par adresses MAC, tous contrôlés dans une configuration unique pour chaque port de commutateur. En outre, les commutateurs Cisco peuvent marquer chaque paquet de données avec les informations d'identité de l'utilisateur afin que de plus amples contrôles puissent être déployés n'importe où sur le réseau. En outre, aujourd'hui, les commutateurs Cisco Nexus prennent en charge MACSec (chiffrement standard IEEE 802.1AE) pour la protection de la confidentialité et l'intégrité des données en mouvement.

Politique de sécurité : Cisco Secure ACS est un serveur de politique de sécurité simple mais puissant pour le contrôle centralisé de l'identité et de l'accès au réseau. Cisco Secure ACS inclut un modèle de politique reposant sur des règles et une nouvelle interface de gestion intuitive conçue pour un contrôle et une visibilité optimale. La dernière version de Cisco Secure ACS aide également les administrateurs système à identifier rapidement les problèmes potentiels grâce à une surveillance étendue et des fonctionnalités de dépannage.

Le gestionnaire du contrôleur d'accès au réseau Cisco (NAC Manager) est le centre de définition et de gestion des politiques, permettant de définir les stratégies d'accès utilisateur reposant sur des roles et un contrôle de conformité, dans un environnement de déploiement NAC reposant sur des appliances.

Cisco TrustSec

Un composant de base des réseaux sécurisés sans frontières

Cisco NAC Server évalue et applique la conformité aux politiques de sécurité dans un environnement de déploiement NAC reposant sur des appliances.

Cisco NAC Profiler aide à déployer un contrôle d'accès en fournissant une détection, un établissement de profil, et une surveillance post-connexion de tous les périphériques se connectant au réseau.

Cisco NAC Guest Server gère l'accès au réseau des invités, y compris la mise en service, la notification, la gestion et l'établissement de rapports pour tous les comptes utilisateur invité et toutes les activités du réseau.

Partie Cliente : Le client à service sécurisé Cisco (SSC) permet aux clients de déployer un système d'authentification unique pour accéder à la fois aux réseaux filaires et sans fil. Il fournit une authentification des utilisateurs et des périphériques 802.1X et gère l'identité des utilisateurs et des périphériques ainsi que les protocoles d'accès au réseau. Cisco NAC Agent est un agent léger en option fonctionnant sur un périphérique. Il effectue une inspection en profondeur du profil de sécurité du périphérique en analysant les paramètres, services et fichiers de registre. En plus des deux clients d'arrivée sus-mentionnés qui prennent en charge des périphériques standard, les téléphones IP Cisco incluent des fonctionnalités client incorporées avancées permettant de s'intégrer dans la solution Cisco TrustSec.

Services aux entreprises pour TrustSec

Des services aux entreprises intelligents et personnalisés de Cisco et de nos partenaires offrent une expertise dans le domaine de la vérification, de l'analyse et de la conception des politiques d'accès afin de préparer le réseau à déployer une solution TrustSec. Les services Cisco utilisent les meilleurs pratiques pour aider les organisations à déployer plus rapidement et à moindre coût une solution complète d'authentification et d'accès tout en procédant à un transfert de connaissance pour une efficacité opérationnelle permanente.

Exemples d'utilisation

Option de déploiement 1 : déploiement reposant sur la norme 802.1X

Dans ce scénario, Cisco Secure ACS est le serveur de politiques permettant l'authentification des utilisateurs qui se connectent au réseau filaire. Un périphérique d'accès au réseau (commutateur) fournit un accès au réseau et aux ressources sur la base des informations d'identification des utilisateurs (collectées par Cisco SSC) et de leurs rôles dans l'organisation. Vous pouvez appliquer une protection supplémentaire comme le marquage des groupes de sécurité (Security Group Tagging) et les listes de contrôle d'accès (ACL) basés sur les groupes de sécurité pour des contrôles plus précis. Vous pouvez également déployer Cisco NAC Profiler et Cisco NAC Guest Server avec la solution 802.1X.

Option de déploiement 2 : déploiement reposant sur des appliances

Avec une approche de ce type, Cisco NAC Manager est le serveur de politiques qui fonctionne avec Cisco NAC Server pour authentifier les utilisateurs et évaluer leurs périphériques sur des connexions LAN, sans fil ou VPN. L'accès au réseau et aux ressources est basé sur les informations d'identification des utilisateurs et leurs rôles dans l'organisation ainsi que sur la conformité des périphériques.

Innovations TrustSec

TrustSec offre de nombreuses innovations Cisco. La surveillance 802.1X et les modes de déploiements dits à faible impact permettent de déployer le contrôle d'accès réseau avec une visibilité accrue, des modes de test, permettant ainsi des déploiements plus souples et une plus grande facilité opérationnelle. L'intégration de Cisco NAC Profiler, Cisco Guest Server et de la téléphonie IP à la commutation Cisco dans un environnement 802.1X améliore grandement l'infrastructure informatique et la productivité des employés. Les listes de contrôle d'accès (ACL) des groupes de sécurité simplifient la gestion des politiques de sécurité en affectant les utilisateurs finaux à des groupes de sécurité ainsi que des règles d'accès aux ressources basées sur la notion de groupes, au lieu des ACL se reposant sur des adresses IP. TrustSec offre des technologies de sécurisation avancées telles que 802.1X-REV et MACSec aux clients.

Pourquoi choisir Cisco ?

Cisco TrustSec est une solution complète souple, conviviale et facile à déployer. Elle intègre la sécurité dans l'infrastructure pour prendre en charge des équipements gérés, non gérés et inconnus ainsi que les employés, les invités et les sous-traitants.

Les réseaux Cisco protégés par TrustSec offrent une visibilité et un contrôle complets. TrustSec améliore la fiabilité, la cohérence et l'évolutivité du réseau.

Cisco et ses partenaires fournissent des services aux entreprises pour aider les clients à satisfaire leurs besoins uniques en termes de conformité et de sécurité.

Pour plus d'informations, consultez le site http://www.cisco.com/go/trustsec.

C45-577269-00 01/10