Couche de Cisco NAC 3 OOB avec ACLs

Contenu

Introduction

Le Cisco Network Admission Control (NAC) impose les stratégies de sécurité réseau d'une organisation sur tous les périphériques recherchant l'accès au réseau. Le Cisco NAC permet seulement les périphériques d'extrémité conformes et de confiance, tels que des PC, des serveurs, et des PDA, sur le réseau. Access est limité pour les périphériques non-conformes, qui limite le possible détérioration des menaces et des risques de Sécurité d'émergeant. Le Cisco NAC donne à des organismes une méthode puissante et basée sur rôles à empêcher l'accès non autorisé et améliore la résilience de réseau.

La solution de Cisco NAC fournit les avantages pour l'entreprise suivants :

- **Conformité de stratégie de sécurité** : S'assure que les points finaux se conforment à la stratégie de sécurité ; protège la productivité d'infrastructure et d'employés ; sécurise les ressources géré et en non pris en charge ; environnements internes et accès invité de supports ; conçoit en fonction des stratégies votre niveau de risque.
- **Protège des investissements existants** : Est compatible avec de tiers applications d'administration ; les options de déploiement flexible réduisent le besoin de mises à jour d'infrastructure.
- **Atténue des risques des virus, des vers, et de l'accès non autorisé** : Les contrôles et réduit des interruptions de grande puissance d'infrastructure ; réduit des dépenses d'exploitation en entreprenant des démarches, ajoute, et change dynamique et automatisé, qui active une efficacité informatique plus élevée ; intègre avec d'autres composants de Cisco Self-Defending Network pour fournir la protection de Sécurité complète.

Présentation de la solution

Cette section introduit brièvement la couche 3 hors bande (OOB) suivre des méthodes de liste de contrôle d'accès (ACL) pour implémenter une architecture du Cisco Network Admission Control (NAC).

Description de la solution

Le Cisco NAC est utilisé dans l'infrastructure réseau pour imposer la conformité de stratégie de sécurité sur tous les périphériques qui recherchent l'accès aux ressources de réseau. Le Cisco NAC permet à des administrateurs réseau pour authentifier et autoriser les utilisateurs et pour les évaluer et le remediate leurs ordinateurs associés avant qu'on leur accorde l'accès au réseau. Il y a plusieurs méthodes de configuration que vous pouvez employer pour accomplir cette tâche, mais pose 3 hors bande (OOB) a rapidement devenu des méthodologies de déploiement les plus populaires pour le NAC. Cette variation dans la popularité est basée sur des plusieurs dynamics, y compris une meilleure utilisation des ressources en matériel.

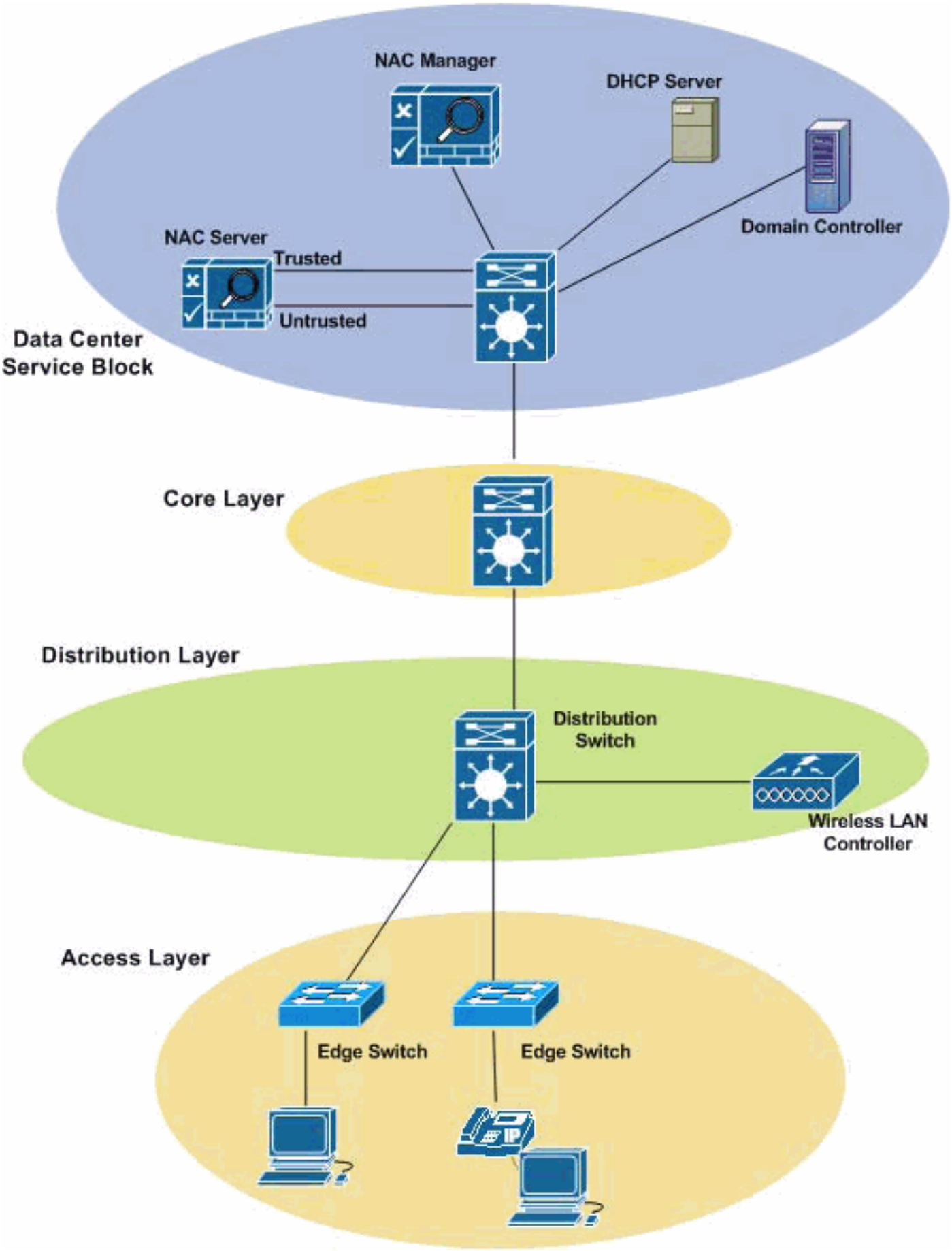
En déployant le Cisco NAC dans une méthodologie de la couche 3 OOB, une appliance simple de Cisco NAC (gestionnaire de Cisco NAC ou serveur de Cisco NAC) peut mesurer pour rendre service à plus d'utilisateurs. Il permet également des appliances NAC à situer centralement plutôt que distribuées à travers le campus ou l'organisation. Ainsi, les déploiements de la couche 3 OOB sont beaucoup plus rentables chacun des deux d'un point de vue de capital et de frais d'exploitation.

Ce guide décrit une implémentation basée sur acl de Cisco NAC dans un déploiement de la couche 3 OOB.

Architecture de solution

L'architecture de solution (voyez que le schéma 1) identifie les composants de la solution et les points principaux d'intégration.

Figure 1 : Placement d'appareils de Cisco NAC dans un campus universitaire typique



Les sections suivantes décrivent la couche d'accès, la couche de distribution, la couche de noyau, et les points d'intégration de services de centre de traitement des données qui composent une architecture typique de campus.

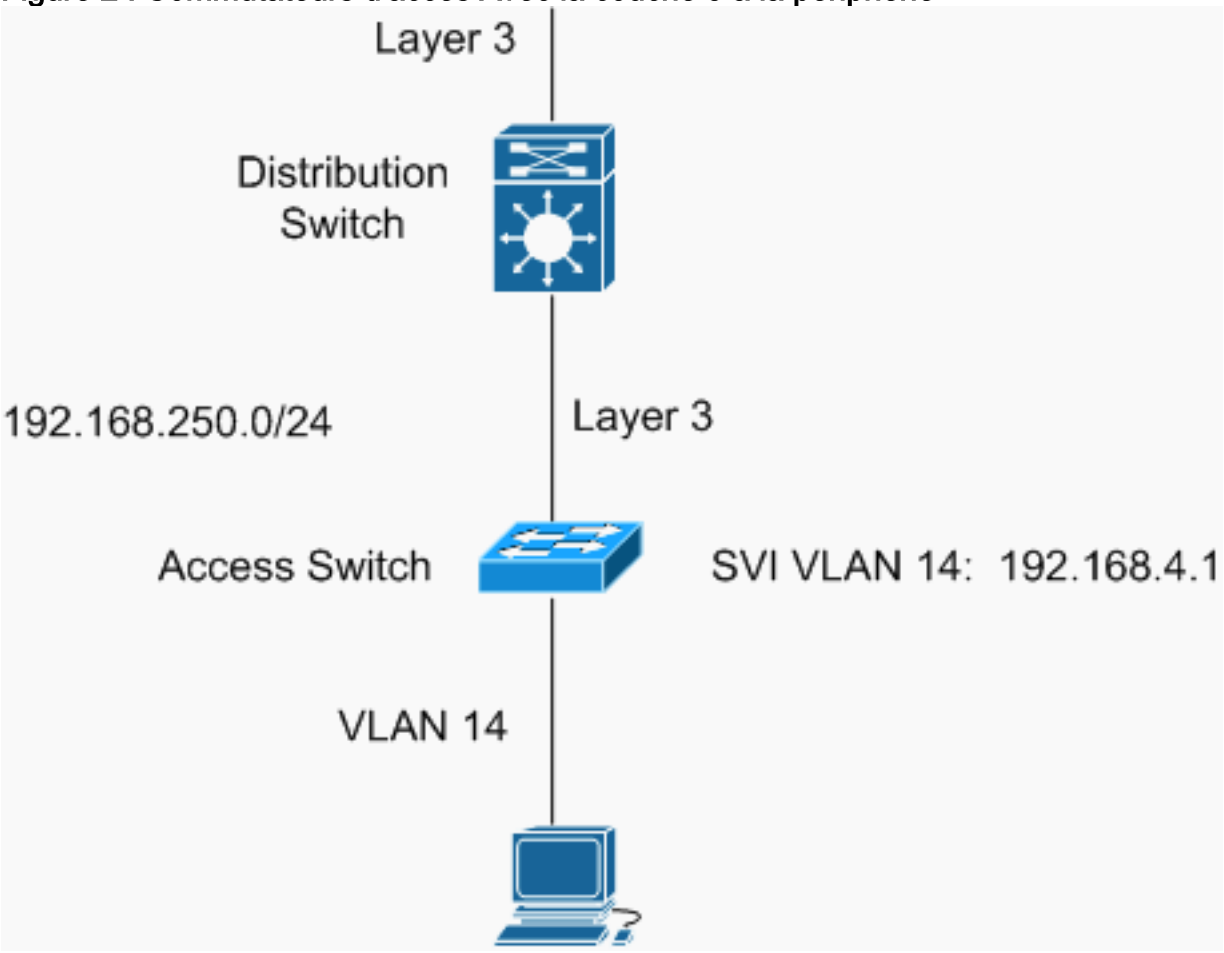
Couche d'accès

Cisco posent la solution 3 OOB NAC s'applique à une conception campus conduite d'accès. Dans le mode d'accès conduit, les interfaces virtuelles commutées de la couche 3 (SVI) sont configurées sur le commutateur d'accès, et il y ont un lien de la couche 3 entre l'accès et les commutateurs de distribution.

Remarque: Le terme « commutateur d'accès » et « commutateur de périphérie » sont utilisés l'un pour l'autre dans ce document.

Comme vu dans la figure 2, l'accès VLAN de la couche 3 (par exemple, VLAN 14) est configuré sur le commutateur de périphérie, posent 3 que le routage est pris en charge du commutateur au commutateur de distribution ou au routeur ascendant, et le gestionnaire de Cisco NAC gère les ports sur le commutateur d'accès.

Figure 2 : Commutateurs d'accès Avec la couche 3 à la périphérie



Couche de distribution

La couche de distribution est responsable du routage de la couche 3. À la différence d'une solution de la couche 2, le serveur de Cisco NAC n'a pas besoin se trouvent à la couche de distribution. Au lieu de cela, il est placé centralement au bloc de service de centre de traitement des données.

Principale couche

La principale couche utilise les Routeurs basés sur IOS de Cisco. La principale couche est

réservée pour le routage ultra-rapide, sans aucun services. Des services peuvent être placés sur un commutateur de service au centre de traitement des données.

Couche de services de Data Center

La couche de services de centre de traitement des données utilise les Routeurs et les Commutateurs basés sur IOS de Cisco. Le gestionnaire de Cisco NAC et le serveur de Cisco NAC sont centralement situés au bloc de service de centre de traitement des données.

Composants de la solution

Cette section décrit les composants de la solution d'appareils de Cisco NAC.

Gestionnaire de Cisco NAC

Le gestionnaire de Cisco NAC est le serveur de gestion et la base de données qui centralise la configuration et la surveillance de tous les serveurs, utilisateurs, et stratégies de Cisco NAC dans un déploiement d'appareils de Cisco NAC. Pour un déploiement OOB NAC, le gestionnaire fournit la Gestion OOB pour ajouter et des commutateurs de commande dans le domaine du gestionnaire et pour configurer des ports de commutateur.

Serveur de Cisco NAC

Le serveur de Cisco NAC est le point d'application entre le réseau (géré) non approuvé et le réseau (interne) de confiance. Le serveur impose maintient l'ordre défini dans le gestionnaire de Cisco NAC, et les points finaux communiquent avec le serveur pendant l'authentification. Dans cette conception, le serveur n'est pas placé logiquement ou physiquement « en ligne » pour séparer le réseau non approuvé et de confiance. Ce concept est adressé plus en détail plus tard dans la section « du mode (OOB) hors bande ».

Agent de Cisco NAC

L'agent de Cisco NAC est un composant facultatif de la solution de Cisco NAC. Quand l'agent est activé pour votre déploiement de Cisco NAC, l'agent s'assure que les ordinateurs qui accèdent à votre rassemblement de réseau les conditions requises de posture de système vous spécifient. L'agent de Cisco NAC est un en lecture seule, facile à utiliser, le programme d'encombrement réduit qui réside sur des ordinateurs d'utilisateur. Quand les tentatives d'un utilisateur d'accéder au réseau, l'agent vérifie le système client pour le logiciel vous exigez, et les utilisateurs d'aides saisissent n'importe quelles mises à jour ou logiciel manquantes.

Mode (OOB) hors bande

Dans le déploiement des appareils OOB de Cisco NAC, le serveur de Cisco NAC communique avec l'hôte d'extrémité seulement pendant la procédure d'authentification, pose l'estimation, et la correction. Après qu'on le certifie, l'hôte d'extrémité ne communique pas avec le serveur. En mode OOB, le gestionnaire de Cisco NAC utilise le Protocole SNMP (Simple Network Management Protocol) aux commutateurs de commande et aux affectations de set vlan pour des ports. Quand le Cisco NAC Manager and Server sont installés pour OOB, le gestionnaire peut contrôler les ports de commutateur des Commutateurs pris en charge. Pour une liste de Commutateurs pris en

charge, allez à :

http://www.cisco.com/en/US/docs/security/nac/appliance/support_guide/switch_spt.html#wp40017.

Les diagrammes à venir affichent comment le gestionnaire de Cisco NAC emploie OOB pour contrôler comment un utilisateur obtient l'accès au réseau. L'ordre est comme suit :

1. Un PC est physiquement connecté à un commutateur sur le réseau (voir le schéma 3).
2. Le commutateur envoie l'adresse MAC utilisant le SNMP au gestionnaire de Cisco NAC (voir le schéma 3).
3. Le gestionnaire de Cisco NAC vérifie si le PC « est certifié. »Si le PC n'est pas certifié, le gestionnaire de Cisco NAC demande au commutateur pour assigner le port de commutateur du PC à une authentification VLAN (voir le schéma 4). Continuez l'étape 4 à l'étape 6.Si le PC est certifié, passez à l'étape 5.
4. Le PC communique avec le serveur de Cisco NAC et passe par l'authentification, l'estimation de posture, et la correction (voir le schéma 4).
5. Le serveur de Cisco NAC informe le gestionnaire de Cisco NAC que le PC « est certifié » (voir le schéma 5).
6. Le PC est connecté au réseau comme périphérique de confiance.

Figure 3 : Transmission SNMP OOB (1 de 3)

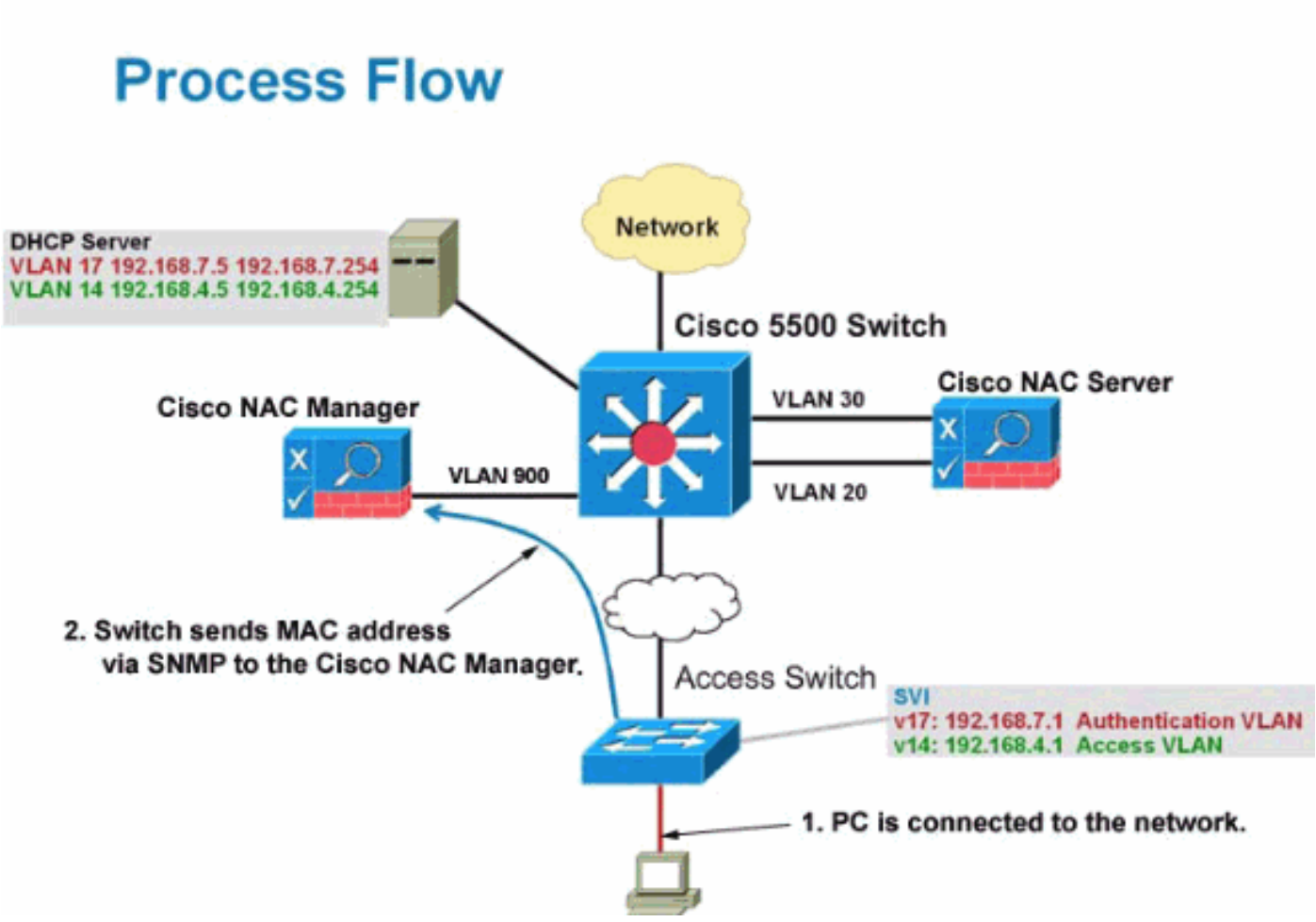


Figure 4 : Transmission SNMP OOB (2 de 3)

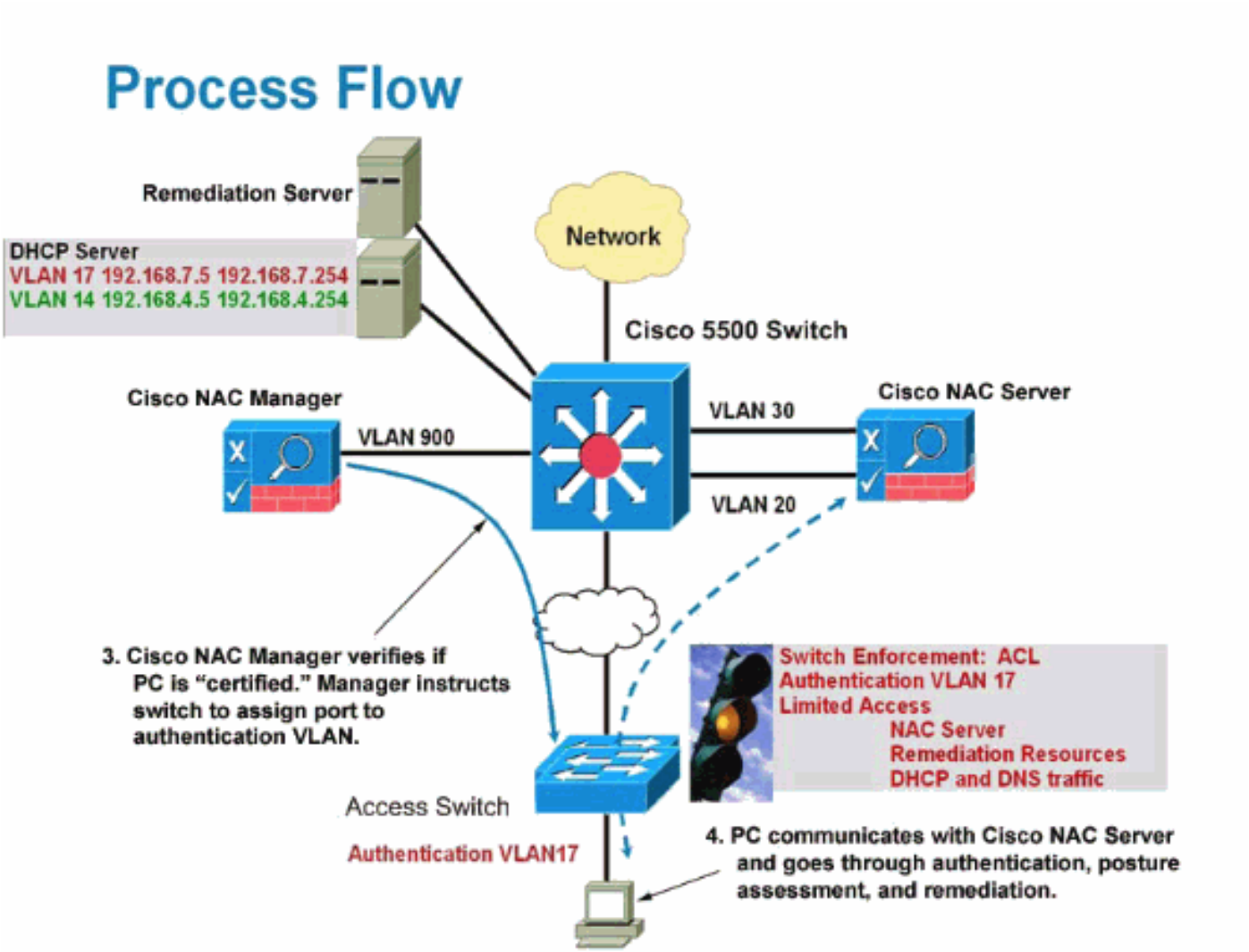
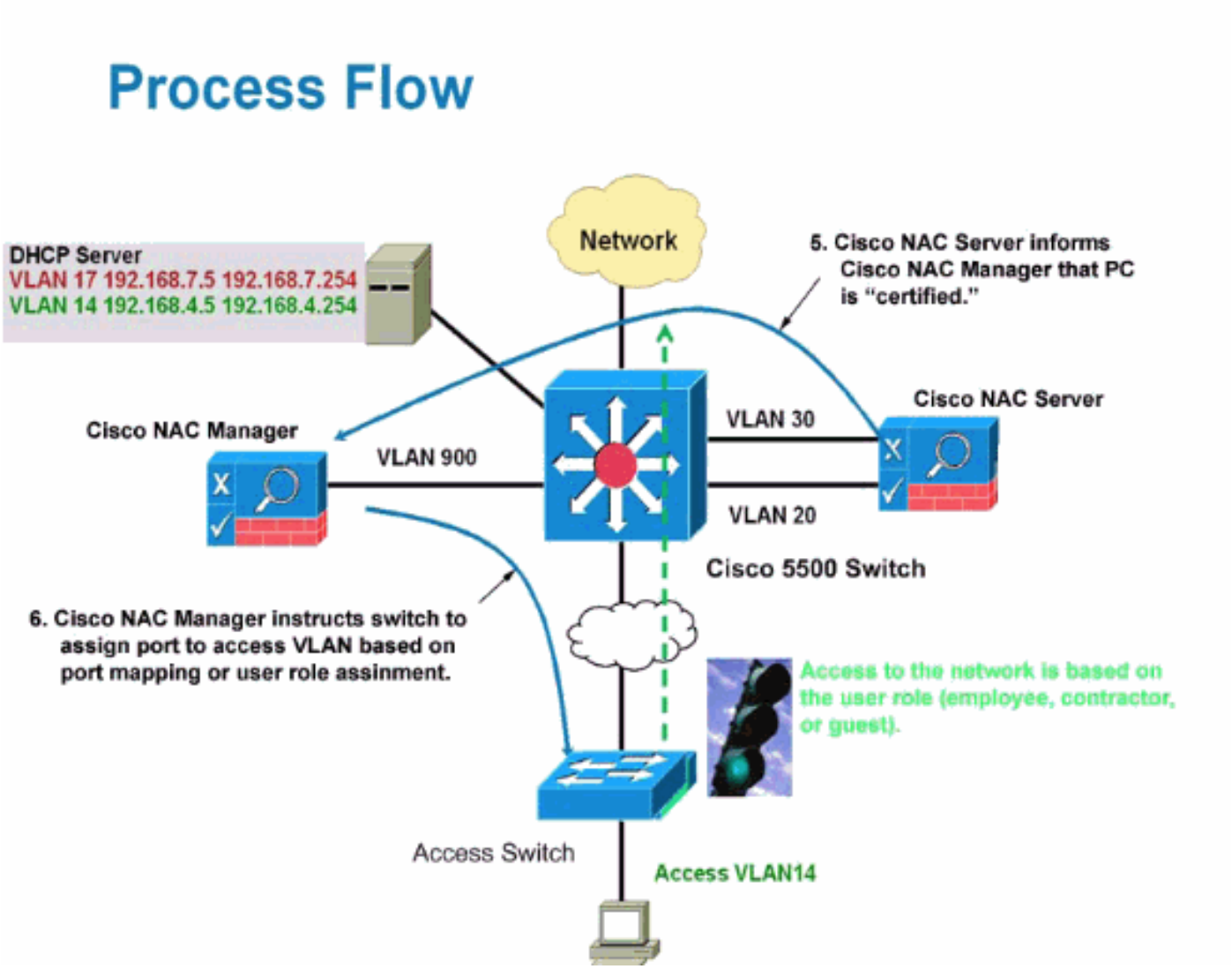


Figure 5 : Transmission SNMP OOB (3 de 3)



Considérations de conception

Quand vous considérez un déploiement de la couche 3 OOB NAC, vous devriez passer en revue plusieurs considérations de conception. Ces considérations sont répertoriées ont discuté dans les paragraphes suivants, et une brève discussion de leur importance est incluse.

Classification de point final

Plusieurs facteurs contribuent à la classification de point final, y compris des types de périphérique et des rôles de l'utilisateur. Le type de périphérique et le rôle de l'utilisateur affectent le rôle de point final.

Types de périphérique possibles

- Périphériques entreprise
- périphériques Non-entreprise
- Périphériques Non-PC

Rôles de l'utilisateur possibles

- Employé
- Sous-traitant

- Invités

Au commencement, tous les points finaux sont assignés au VLAN unauthenticated. Access aux autres rôles est permis après l'identité et le processus de posture est complet.

Rôles de point final

Le rôle de chaque type de point final doit être au commencement déterminé. Un déploiement typique de campus inclut plusieurs rôles, tels que des employés, des invités, et des sous-traitants, et d'autres points finaux, tels que des imprimantes, des points d'accès sans fil, et des caméras IP. Des rôles sont tracés au commutateur VLAN de périphérie.

Remarque: Le rôle Unauthenticated trace au commencement tous les utilisateurs à un VLAN unauthenticated pour l'authentification pour la première fois.

Isolation de rôle

Il est essentiel d'isoler les rôles de point final quand vous implémentez la solution de Cisco NAC. Sélectionnez un mécanisme d'application approprié pour fournir l'isolation du trafic et de chemin pour tout le trafic provenant des ordinateurs hôte unauthenticated et non autorisés. Dans un environnement de la couche 3 OOB, le commutateur de périphérie de la couche 3 (utilisant ACLs) agit en tant que point d'application qui assure la ségrégation entre « nettoient » et les réseaux « unauthenticated ».

La circulation

Le processus NAC commence quand un point final se connecte à un commutateur NAC-géré. Le trafic classifié en tant que « unauthenticated » est limité par l'ACLs appliqué sur le VLAN unauthenticated. On permet au le point final pour communiquer à l'interface « non approuvée » du serveur de Cisco NAC pour continuer par le processus d'estimation et de correction de posture (il y a plusieurs méthodes pour exécuter l'estimation et la correction de posture qui sont discutées plus tard dans les « stratégies de mise à jour de Cisco.com sur le gestionnaire de Cisco NAC. » section). Après authentification, le point final est déplacé au VLAN de confiance.

Mode de serveur de Cisco NAC

Un serveur de Cisco NAC peut être déployé en mode virtuel de passerelle (passerelle) ou mode de la passerelle vrai-IP (conduite).

Mode virtuel de passerelle (passerelle)

Le mode virtuel de passerelle (passerelle) est typiquement utilisé quand le serveur de Cisco NAC est la couche 2 à côté des points finaux. En ce mode, le serveur agit en tant que passerelle et n'est pas impliqué dans la décision de routage du trafic réseau.

Remarque: Le mode virtuel de passerelle (passerelle) s'applique pas applicable pour la conception d'ACL de la couche 3 OOB.

Mode de la passerelle Vrai-IP (conduite)

Le mode de la passerelle vrai-IP (conduite) s'applique quand le serveur de Cisco NAC est de

plusieurs sauts à partir du point final. Quand vous utilisez le serveur comme passerelle vrai-IP, spécifiez les adresses IP de ses deux interfaces : une adresse IP pour le côté de confiance (pour prévoir la Gestion du gestionnaire de Cisco NAC) et une adresse IP pour le côté non approuvé. Les deux adresses devraient être sur des différents sous-réseaux. L'adresse IP non approuvée d'interface est utilisée pour communiquer avec le point final sur le sous-réseau non approuvé. Un déploiement de la couche 3 OOB utilisant ACLs exige du point final de communiquer avec l'interface non approuvée pour des buts d'authentification et d'autorisation. Puisque le mode vrai-IP utilise une adresse IP valide pour l'interface non approuvée, le serveur de Cisco NAC doit être configuré pour fonctionner en mode de la passerelle vrai-IP.

Évolutivité

Un serveur standard de Cisco NAC peut gérer jusqu'à 5000 utilisateurs finaux simultanés. La conception d'ACL de la couche 3 OOB approprié à un site ne servant pas plus de 5000 utilisateurs. Si vous avez des plusieurs sites, vous pouvez avoir les serveurs supplémentaires par site. Si vous avez un site unique qui doit servir plus de 5000 utilisateurs, vous pouvez employer des techniques externes d'Équilibrage de charge (par exemple, équilibreur de charge d'engine de contrôle d'application (ACE)) pour mesurer plus de 5000 utilisateurs pour le site unique.

Remarque: La discussion d'équilibreur de charge d'ACE est hors de portée de ce document.

Hôte de détection

L'hôte de détection est le nom de domaine complet (FQDN) ou adresse IP non approuvée d'interface utilisée par l'agent de Cisco NAC pour découvrir sauts localisés par serveur de Cisco NAC les plusieurs loin sur le réseau. L'agent initie le processus de découverte en envoyant des paquets UDP au host address connu de détection. Les paquets de détection doivent atteindre l'interface non approuvée de serveur NAC pour recevoir une réponse. Dans le cas d'un déploiement de la couche 3 OOB, le serveur n'est pas dans le chemin du trafic de données sur l'authentification VLAN. Par conséquent, la configuration d'hôte de détection doit être configurée pour être l'adresse IP de l'interface non approuvée du serveur de Cisco NAC de sorte que l'agent puisse envoyer les paquets de détection directement au serveur.

Expérience utilisateur (avec l'agent de Cisco NAC)

Typiquement, les administrateurs de réseau d'entreprise installent l'agent de Cisco NAC sur des machines cliente avant d'émettre ces ordinateurs sur des utilisateurs. L'adresse IP d'hôte de détection ou le nom résoluble dans l'agent de Cisco NAC déclenche des paquets de détection à envoyer à l'interface non approuvée du serveur NAC, qui guide automatiquement la machine cliente par le processus NAC.

Expérience utilisateur (sans agent de Cisco NAC)

Les points finaux sans agent de Cisco NAC (invités le plus susceptibles, sous-traitants, et ressources non-entreprises) peuvent automatiquement ne pas continuer par le processus NAC. Les méthodes manuelles et guidées existent pour aider les points finaux qui n'ont pas l'agent. Pour plus de détail, voir « point final la section de Cisco NAC de serveur à transmission ».

Remarque: Pour la meilleure expérience utilisateur possible, Certificats d'utilisation qui sont de confiance par le navigateur de l'utilisateur. Utilisant les Certificats auto-générés sur le Cisco NAC le serveur n'est pas recommandé pour un environnement de production.

Écoulements de processus de Cisco NAC

Cette section explique l'écoulement d'opération de base pour une solution NAC OOB. Les scénarios sont des deux décrits avec et sans un agent de Cisco NAC installé sur la machine cliente. Cette section affiche comment le gestionnaire de Cisco NAC contrôle les ports de commutateur utilisant le SNMP comme support de contrôle. Ces écoulements de processus sont macroanalytiques en nature et contiennent seulement les étapes fonctionnelles de décision. Les écoulements de processus n'incluent pas chaque option ou font un pas qui se produit et n'incluent pas les décisions d'autorisation qui sont basées sur des critères d'estimation de point final.

Référez-vous à l'organigramme de processus affiché dans la figure 7 pour les étapes cerclées affichées dans la figure 6.

Figure 6 : Écoulement de processus NAC pour la solution hors bande de la couche 3 NAC

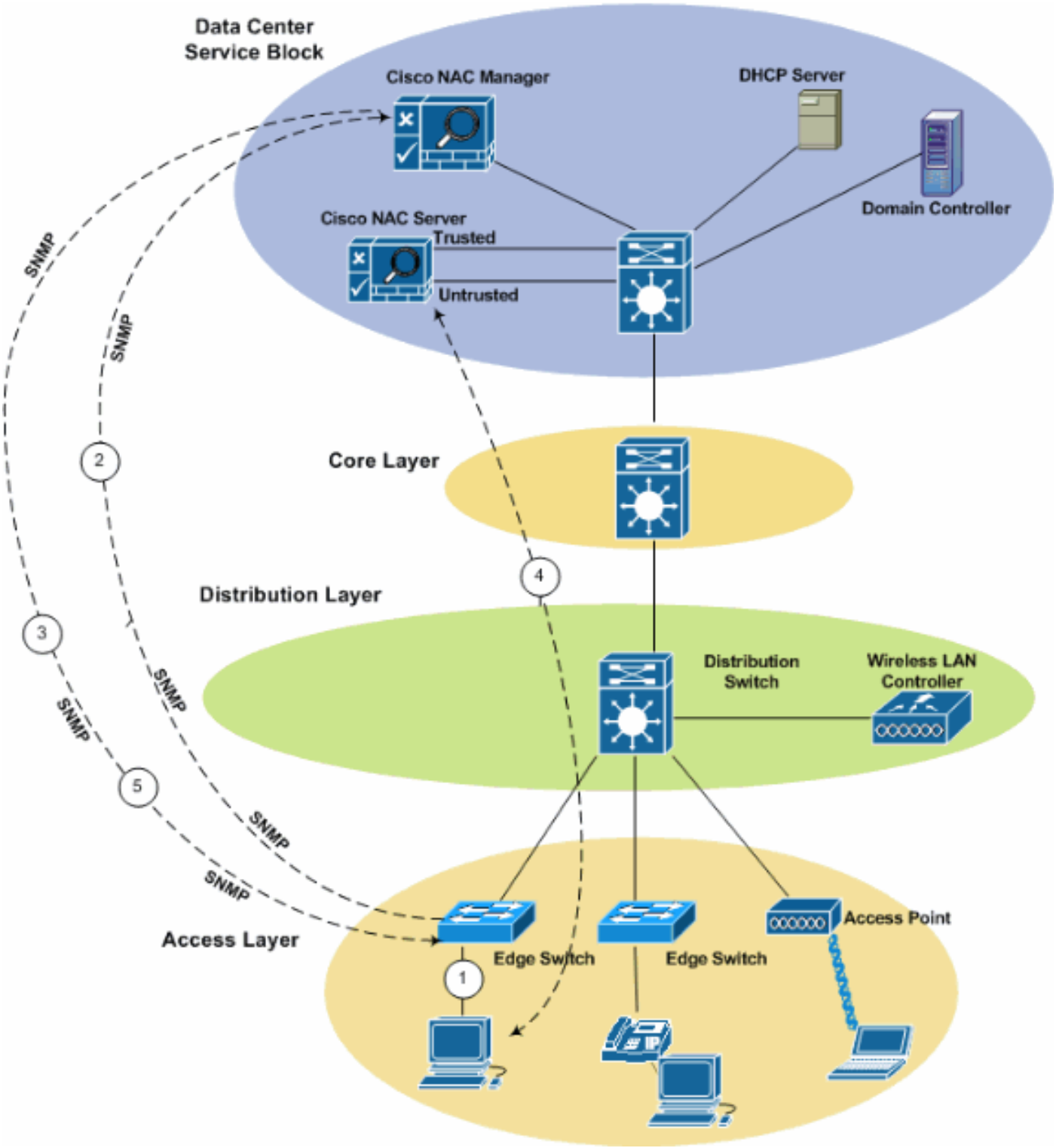


Figure 7 : Organigramme de processus