Radio BYOD avec le Cisco Identity Services Engine

Contenu

Introduction

Le Logiciel Cisco Identity Services Engine (ISE) est le policy server de la deuxième génération de Cisco qui fournit l'infrastructure d'authentification et d'autorisation à la solution de Cisco TrustSec. Il fournit également deux autres services critiques :

- Le premier service est de fournir une manière de profiler le type de périphérique d'extrémité automatiquement basé sur des attributs que Cisco ISE reçoit de diverses sources d'informations. Ce service (appelé Profiler) fournit des fonctions équivalentes à ce que Cisco a précédemment offert avec l'appliance de Cisco NAC Profiler.
- Un autre important service que Cisco ISE fournit est de balayer la conformité de point final ; par exemple, l'installation de logiciel AV/AS et sa définition classent la validité (connue sous le nom de posture). Cisco avait précédemment fourni à cette fonction précise de posture seulement l'appliance de Cisco NAC.

Cisco ISE fournit un niveau équivalent de la fonctionnalité, et il est intégré avec des mécanismes d'authentification de 802.1X.

Cisco ISE intégré avec les contrôleurs LAN Sans fil (WLCs) peut fournir profiler des mécanismes des périphériques mobiles tels que des iDevices d'Apple (iPhone, iPad, et iPod), des smartphones basés sur Android, et d'autres. Pour des utilisateurs de 802.1X, Cisco ISE peut fournir le même niveau des services tels que le profilage et la lecture de posture. Des services d'invité sur Cisco ISE peuvent également être intégrés avec le Cisco WLC en réorientant des demandes d'authentification Web à Cisco ISE pour l'authentification.

Ce document introduit la solution Sans fil pour Bring Your Own Device (BYOD), comme fournir accès basé sur différencié sur des points finaux connus et la stratégie d'utilisateur. Ce document ne fournit pas la solution complète de BYOD, mais sert à expliquer un cas d'utilisation simple d'accès dynamique. D'autres exemples de configuration incluent utilisant le portail de sponsor ISE, où un utilisateur privilégié peut commanditer un invité pour l'accès invité sans fil de ravitaillement.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur LAN Sans fil 2504 ou 2106 de Cisco avec la version de logiciel 7.2.103
- Catalyst 3560 – 8 ports
- WLC 2504
- Cisco Identity Services Engine 1.0MR (version d'image de serveur de VMware)
- Serveur de Windows 2008 (image de VMware) — 512M, disque 20GBActive DirectoryDNDHCPServices de certificat

Topologie

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

RAYON Sans fil NAC de contrôleur LAN et aperçu CoA

Cette configuration permet au WLC de rechercher les paires AV de redirection URL provenant le serveur de RAYON ISE. C'est seulement sur un WLAN qui est attaché à une interface avec la configuration du RAYON NAC activée. Quand la paire AV de Cisco pour la redirection URL est reçue, le client est mis dans l'état POSTURE_REQD. C'est fondamentalement identique comme l'état WEBAUTH_REQD intérieurement dans le contrôleur.

Quand le serveur de RAYON ISE considère le client est Posture_Compliant, il émet un CoA ReAuth. Le Session_ID est utilisé pour l'attacher ensemble. Avec ce nouvel AuthC il (re-Auth) n'envoie pas les paires AV URL-Redirec. Puisqu'il n'y a aucun URL réorientez les paires AV, le WLC sait que le client n'a pas besoin de la posture plus longue.

Si la configuration du RAYON NAC n'est pas activée, le WLC ignore l'URL réoriente les VSAs.

CoA-ReAuth : Ceci est activé avec la configuration RFC 3576. La capacité de ReAuth a été ajoutée aux commandes existantes CoA qui ont été prises en charge précédemment.

La configuration du RAYON NAC est mutuellement - exclusivité de cette capacité, bien qu'on l'exige pour que le CoA fonctionne.

ACL de Pré-posture : Quand un client est dans l'état POSTURE_REQ, le comportement par défaut du WLC est de bloquer tout le trafic excepté DHCP/DNS. L'ACL de Pré-posture (qu'il s'appelle dans la paire AV d'URL-réorienter-acl) est appliqué au client, et ce qui est permis du fait est l'ACL ce que le client peut atteindre.

ACL de Pre-Auth contre le dépassement VLAN : Une quarantaine ou un AuthC VLAN qui sont différents du l'Access-VLAN n'est pas prise en charge dans 7.0MR1. Si vous placez un VLAN du policy server, ce sera le VLAN pour la session entière. Aucune modification VLAN n'est nécessaire après le premier AuthZ.

RAYON Sans fil NAC de contrôleur LAN et écoulement de

caractéristique CoA

La figure ci-dessous fournit des détails de l'échange de message quand le client est authentifié au serveur et à la validation principaux de position du NAC.

1. Le client authentifie utilisant l'authentification de dot1x.
2. Le RAYON Access reçoivent porte l'URL réorienté pour le port 80 et le pre-auth ACLs qui inclut permettre des adresses IP et des ports, ou la quarantaine VLAN.
3. Le client sera réorienté à l'URL fourni dans l'accès reçoivent, et ont mis dans un nouvel état jusqu'à ce que la validation de posture soit faite. Le client dans cet état parle au serveur ISE et se valide contre les stratégies configurées sur le serveur ISE NAC.
4. L'agent NAC sur le client initie la validation de posture (le trafic à port 80) : L'agent envoie la demande de détection de HTTP au port 80 que les redirect to de contrôleur que l'URL a fourni dans l'accès reçoivent. L'ISE sait que client essayant d'atteindre et répond directement au client. De cette façon que le client se renseigne sur l'IP de serveur ISE et dorénavant, le client parle directement avec le serveur ISE.
5. WLC permet ce trafic parce que l'ACL est configuré pour permettre ce trafic. En cas de dépassement VLAN, le trafic pont de sorte qu'il atteigne le serveur ISE.
6. Une fois que l'ISE-client se termine l'estimation, un CoA-Req de RAYON avec le service de reauth est envoyé au WLC. Ceci initie la ré-authentification du client (en envoyant EAP-START). Une fois que la ré-authentification réussit, l'ISE envoie l'accès reçoit avec un nouvel ACL (le cas échéant) et aucun URL réoriente, ou accède au VLAN.
7. WLC a le soutien du CoA-Req et le débranchement-Req selon RFC 3576. Le WLC doit prendre en charge le CoA-Req pour le service re-auth, selon RFC 5176.
8. Au lieu d'ACLs téléchargeable, ACLs préconfiguré sont utilisés sur le WLC. Le serveur ISE envoie juste le nom d'ACL, qui est déjà configuré dans le contrôleur.
9. Cette conception devrait fonctionner pour des cas VLAN et d'ACL. En cas de dépassement VLAN, nous réorientons juste le port 80 est réorientés et permet le reste (de passerelle) du trafic sur la quarantaine VLAN. Pour l'ACL, l'ACL de pre-auth reçu dans l'accès reçoivent est appliqué.

Cette figure fournit une représentation visuelle de cet écoulement de caractéristique :

ISE profilant l'aperçu

Le service de profileur de Cisco ISE fournit la fonctionnalité en découvrant, en localisant, et en déterminant les capacités de tous les points finaux reliés sur votre réseau, indépendamment de leurs types de périphérique, afin d'assurer et mettre à jour l'accès approprié à votre réseau d'entreprise. Il collecte principalement un attribut ou un ensemble d'attributs de tous les points finaux sur votre réseau et les classifie selon leurs profils.

Le profileur est composé de ces composants :

- Le capteur contient un certain nombre de sondes. Les sondes capturent des paquets du réseau en questionnant des périphériques d'accès au réseau, et expédient les attributs et leurs valeurs d'attribut qui sont collectés des points finaux à l'analyseur.
- Un analyseur évalue des points finaux utilisant les stratégies configurées et les groupes d'identité pour apparier les attributs et leurs valeurs d'attribut collectés, qui classifie des points finaux au groupe spécifié et enregistre des points finaux avec le profil apparié dans la base de

données de Cisco ISE.

Pour la détection de périphérique mobile, il est recommandent d'utiliser une combinaison de ces sondes pour l'identification de périphérique appropriée :

- RAYON (calling-station-id) : Fournit l'adresse MAC (OUI)
- DHCP (nom d'hôte) : Adresse Internet – l'adresse Internet par défaut peut inclure le type de périphérique ; par exemple : jsmith-ipad
- DN (consultation inverse IP) : FQDN - l'adresse Internet par défaut peut inclure le type de périphérique
- HTTP (Utilisateur-agent) : Détails sur le type de périphérique mobile spécifique

Dans cet exemple d'un iPad, le profileur capture les informations de navigateur Web de l'attribut d'Utilisateur-agent, aussi bien que d'autres attributs de HTTP des messages de demande, et les ajoute à la liste d'attributs de point final.

Créez les utilisateurs internes d'identité

Le Répertoire actif de MS (AD) n'est pas exigé pour un preuve-de-concept simple. ISE peut être utilisé comme mémoire unique d'identité, qui inclut différencier l'accès utilisateur pour l'accès et le contrôle granulaire de stratégie.

Àla release d'ISE 1.0, utilisant l'intégration d'AD, l'ISE peut utiliser des groupes d'AD dans des stratégies d'autorisation. Si la mémoire d'utilisateur interne ISE est utilisée (aucune intégration d'AD), des groupes ne peuvent pas être utilisés dans les stratégies en même temps que des groupes d'identité de périphérique (bogue identifiée à résoudre dans ISE 1.1). Par conséquent, seulement des utilisateurs individuels peuvent être différenciés, comme des employés ou des sous-traitants une fois utilisés en plus des groupes d'identité de périphérique.

Procédez comme suit :

1. Ouvrez une fenêtre du navigateur à l'adresse de https://ISEip.
2. Naviguez vers la **gestion > la Gestion de l'identité > les identités**.
3. **Les utilisateurs** choisis, cliquent sur Add alors (utilisateur d'accès au réseau). Écrivez ces valeurs d'utilisateur et les assignez au groupe des employés :Nom : employéMot de passe :
4. Cliquez sur **Submit**.Nom : sous-traitantMot de passe :
5. Confirmez les deux comptes sont créés.

Ajoutez le contrôleur LAN Sans fil à ISE

N'importe quel périphérique qui initie des demandes RADIUS à l'ISE doit avoir une définition dans ISE. Ces périphériques de réseau sont définis ont basé sur leur adresse IP. Les définitions de périphérique de réseau ISE peuvent spécifier des plages d'adresses IP permettant de ce fait à la définition pour représenter de plusieurs périphériques réels.

Au delà de ce qui est exigée pour la transmission de RAYON, les définitions de périphérique de réseau ISE contiennent des configurations pour l'autre transmission ISE/device, telle que le SNMP et le SSH.

Un autre important aspect de définition de périphérique de réseau groupe convenablement des périphériques de sorte que ce groupement puisse être accru dans la stratégie d'accès au réseau.

Dans cet exercice, les définitions de périphérique exigées pour votre laboratoire sont configurées.

Procédez comme suit :

1. D'ISE allez à la **gestion > aux ressources de réseau > aux périphériques de réseau**.
2. Des périphériques de réseau, cliquez sur Add. Écrivez l'adresse IP, masquez la configuration d'authentification de contrôle, puis écrivez « Cisco » pour le secret partagé.
3. Sauvegardez l'entrée WLC, et confirmez le contrôleur sur la liste.

Configurez ISE pour l'authentification Sans fil

L'ISE doit être configuré pour authentifier des clients sans fil de 802.1x et utiliser le Répertoire actif comme mémoire d'identité.

Procédez comme suit :

1. D'ISE naviguez vers la **stratégie > l'authentification**.
2. Cliquez sur pour développer le dot1x > le Wired_802.1X (-).
3. Cliquez sur en fonction l'icône d'équipement **pour ajouter la condition de la bibliothèque**.
4. Du déroulant de sélection de condition, choisissez l'**état composé > le Wireless_802.1X**.
5. Placez l'état exprès à **OU**.
6. Développez après permettent l'option de protocoles, et reçoivent les utilisateurs internes par défaut (par défaut).
7. Congé tout autrement au par défaut. **Sauvegarde de** clic pour se terminer les étapes.

Contrôleur LAN de radio de bootstrap

Connecter WLC à un réseau

Un guide Sans fil de déploiement de contrôleur LAN de Cisco 2500 est également disponible au guide de déploiement de contrôleur sans-fil de la gamme Cisco 2500 Series.

Configurez le contrôleur utilisant l'assistant de démarrage

```
(Cisco Controller)
 Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup
 Would you like to terminate autoinstall? [yes]: yes AUTO-INSTALL: process terminated
-- no configuration loaded System Name [Cisco_d9:24:44] (31 characters max):
   ISE-Podx Enter Administrative User Name (24 characters max): admin
   Enter Administrative Password
   (3 to 24 characters): Cisco123
   Re-enter Administrative Password: Cisco123
Management Interface IP Address: 10.10.10.5
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.10.10.10
 Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: ISE
 Network Name (SSID): PODx
```

```
Configure DHCP Bridging Mode [yes][NO]: no
Allow Static IP Addresses [YES][no]: no
 Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
 Enter Country Code list (enter 'help' for a list of countries) [US]: US

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes
 Configure a NTP server now? [YES][no]: no
Configure the ntp system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: mm/dd/yy
Enter the time in HH:MM:SS format: hh:mm:ss
Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
 Configuration saved!
 Resetting system with new configuration...
Restarting system.
```

Configuration voisine de commutateur

Le contrôleur est connecté au port Ethernet sur le commutateur voisin (Fast Ethernet 1). Le port de commutateur voisin est configuré comme joncteur réseau de 802.1Q et permet tous les VLAN sur le joncteur réseau. Le VLAN 10 indigène permet l'interface de gestion du WLC à connecter.

La configuration de port de commutateur de 802.1Q est comme suit :

```
switchport
switchport trunk encapsulation dot1q
switchport trunk native VLAN 10
switchport mode trunk
end
```

Ajoutez les serveurs d'authentification (ISE) à WLC

L'ISE doit être ajouté au WLC afin d'activer le 802.1X et la caractéristique CoA pour des points finaux Sans fil.

Procédez comme suit :

1. Ouvrez un navigateur, puis connectez à la zone WLC (utilisant le HTTP sécurisé) > https://wlc.
2. Naviguez vers la **Sécurité > l'authentification > nouveau**.
3. Écrivez ces valeurs :Adresse IP du serveur : 10.10.10.70 (affectation de contrôle)Secret partagé : CiscoLe prenez en charge pour RFC 3576 (CoA) : Activé (par défaut)Tout autrement : Par défaut
4. Cliquez sur Apply pour continuer.
5. **La comptabilité** choisie de **RAYON > ajoutent NOUVEAU**.
6. Écrivez ces valeurs :Adresse IP du serveur : 10.10.10.70Secret partagé : CiscoTout autrement : Par défaut
7. Cliquez sur Apply, puis sauvegardez la configuration pour le WLC.

Créez l'interface dynamique des employés WLC

Terminez-vous ces étapes afin d'ajouter une nouvelle interface dynamique pour le WLC et la tracer à l'employé VLAN :

1. De WLC, naviguez vers le **Controller > Interfaces**. Puis, cliquez sur New.
2. De WLC, naviguez vers le **Controller > Interfaces**. Entrez dans ce qui suit :Nom d'interface : EmployéId VLAN : 11
3. Entrez dans le suivant pour l'interface des employés :Numéro de port : 1Identifiant VLAN : 11Adresse IP : 10.10.11.5Netmask : 255.255.255.0Passerelle : 10.10.11.1DHCP : 10.10.10.10
4. Confirmez que la nouvelle interface dynamique des employés est créée.

Créez l'interface dynamique d'invité WLC

Terminez-vous ces étapes afin d'ajouter une nouvelle interface dynamique pour le WLC et la tracer à l'invité VLAN :

1. De WLC, naviguez vers le **Controller > Interfaces**. Puis, cliquez sur New.
2. De WLC, naviguez vers le **Controller > Interfaces**. Entrez dans ce qui suit :Nom d'interface : InvitéId VLAN : 12
3. Entrez dans ces derniers pour l'interface d'invité :Numéro de port : 1Identifiant VLAN : 12Adresse IP : 10.10.12.5Netmask : 255.255.255.0Passerelle : 10.10.12.1DHCP : 10.10.10.10
4. Confirmez que l'interface d'invité a été ajoutée.

Ajoutez le 802.1x WLAN

Du bootstrap initial de WLC, il pourrait y avoir eu un par défaut WLAN créé. Si oui, modifiez-le ou créez un nouveau WLAN pour prendre en charge l'authentification Sans fil de 802.1X comme indiqué dans le guide.

Procédez comme suit :

1. De WLC, naviguez vers **WLAN > créent nouveau**.
2. Pour le WLAN, entrez dans ce qui suit :Nom de profil : pod1xSSID : Mêmes
3. Pour les configurations > l'onglet Général WLAN, utilisez ce qui suit :Stratégie par radio : TousInterface/groupe : GestionTout autrement : par défaut
4. Pour le WLAN > l'onglet Sécurité > la couche 2, ont placé ce qui suit :Couche 2 Security:WPA+WPA2Stratégie WPA2/cryptage : Activé/AESClé authentique gestion : 802.1X
5. Pour le WLAN > l'onglet Sécurité > les serveurs d'AAA, ont placé ce qui suit :Interface par radio d'écraser de serveur : HandicapéServeurs d'authentification/comptabilité : ActivéServeur 1 : 10.10.10.70
6. Pour le WLAN > l'onglet Avancé, ont placé ce qui suit :Allow AAA Override : ActivéÉtat NAC : Rayon NAC (sélectionné)
7. De nouveau au le WLAN > l'onglet Général > activent WLAN (case).

Interfaces dynamiques du test WLC

Vous devez faire un rapide pour vérifier les interfaces valides des employés et d'invité. Utilisez n'importe quel périphérique pour s'associer au WLAN, puis changez l'affectation d'interface WLAN.

1. De WLC, naviguez vers **WLAN > WLAN**. Cliquez sur pour éditer votre SSID sécurisé créé dans l'exercice plus tôt.
2. Changez l'interface/groupe d'interface à l'**employé**, puis cliquez sur Apply.
3. Si configuré correctement, un périphérique reçoit une adresse IP de l'employé VLAN (10.10.11.0/24). Cet exemple affiche un périphérique IOS qui obtient une nouvelle adresse IP.
4. Une fois que l'interface précédente a été confirmée, changez l'affectation d'interface WLAN à l'**invité**, puis cliquez sur Apply.
5. Si configuré correctement, un périphérique reçoit une adresse IP du VLAN invité (10.10.12.0/24). Cet exemple affiche un périphérique IOS qui obtient une nouvelle adresse IP.
6. **IMPORTANT :** Changez l'affectation d'interface de nouveau à la Gestion d'origine.
7. Cliquez sur Apply et sauvegardez la configuration pour le WLC.

Authentification Sans fil pour IOS (iPhone/iPad)

Associez au WLC par l'intermédiaire d'un SSID authentifié un utilisateur interne (ou a intégré, utilisateur d'AD) utilisant un périphérique IOS tel qu'un iPhone, un iPad, ou un iPod. Ignorez ces étapes sinon applicables.

1. Sur le périphérique IOS, allez aux configurations WLAN. Activez le Wifi, puis sélectionnez le SSID activé par 802.1X créé dans la section précédente.
2. Fournissez ces informations afin de se connecter :Nom d'utilisateur : employé (interne – Employé) ou sous-traitant (interne – sous-traitant)Mot de passe :
3. Cliquez sur pour recevoir le certificat ISE.
4. Confirmez que le périphérique IOS obtient une adresse IP de l'interface de la Gestion (VLAN10).
5. Sur WLC > Monitor > Clients, vérifient les informations de point final comprenant l'utilisation, l'état, et le type d'EAP.
6. De même, les informations de client peuvent être fournies par ISE > page de moniteur > d'authentification.
7. Cliquez sur l'icône de **détails** afin d'effectuer un zoom avant à la session pour les informations en profondeur de la session.

Ajoutez la posture réorientent l'ACL à WLC

La posture réorientent l'ACL est configurée sur le WLC, où ISE l'utilisera pour limiter le client pour la posture. Efficacement et à un minimum les autorisations d'ACL trafiquent entre ISE. Des règles facultatives peuvent être ajoutées dans cet ACL si nécessaires.

1. Naviguez vers **WLC > Sécurité > listes de contrôle d'accès > listes de contrôle d'accès**. Cliquez sur **New**.
2. Fournissez un nom (ACL-POSTURE-REDIRECT) pour l'ACL.
3. Cliquez sur Add la **nouvelle règle** pour le nouvel ACL. Placez les valeurs suivantes à l'ordre

#1 d'ACL. Cliquez sur Apply une fois terminé.Source : QuelsDestination : Adresse IP 10.10.10.70, 255.255.255.255Protocol : QuelsAction : Autorisation
4. Confirmez l'ordre a été ajouté.
5. Cliquez sur Add la **nouvelle règle**. Placez les valeurs suivantes à l'ordre #2 d'ACL. Cliquez sur Apply une fois terminé.Source : Adresse IP 10.10.10.70, 255.255.255.255Destination : QuelsProtocol : QuelsAction : Autorisation
6. Confirmez l'ordre a été ajouté.
7. Placez les valeurs suivantes à l'ordre #3 d'ACL. Cliquez sur Apply une fois terminé.Source : QuelsDestination : QuelsProtocol : UDPPort de source : DNDestination port : QuelsAction : Autorisation
8. Confirmez l'ordre a été ajouté.
9. Cliquez sur Add la **nouvelle règle**. Placez les valeurs suivantes à l'ordre #4 d'ACL. Cliquez sur Apply une fois terminé.Source : QuelsDestination : QuelsProtocol : UDPPort de source : QuelsDestination port : DNAction : Autorisation
10. Confirmez l'ordre a été ajouté.
11. Sauvegardez la configuration du courant WLC.

Enable profilant des sondes sur ISE

L'ISE doit être configuré comme sondes pour profiler efficacement des points finaux. Par défaut, ces options sont désactivées. Cette section affiche comment configurer ISE pour être des sondes.

1. De la Gestion ISE, naviguez vers la **gestion > le système > le déploiement**.
2. Choisissez **ISE**. Cliquez sur Edit l'**hôte ISE**.
3. De la page de noeud d'éditer, sélectionnez la configuration de profilage et configurez ce qui suit :DHCP : Activés, tous (ou par défaut)DHCPSPAN : Activés, tous (ou par défaut)HTTP : Activés, tous (ou par défaut)RAYON : Activé, NON APPLICABLEDN : Activé, NON APPLICABLE
4. Rassociez les périphériques (iPhone/iPads/Droids/Mac, etc.).
5. Confirmez les identités de point final ISE. Naviguez vers la **gestion > la Gestion de l'identité > les identités**. Cliquez sur en fonction les points finaux pour répertorier ce qui a été profilé.**Note**: Le profilage d'initiale est des sondes de RAYON.

Stratégies de profil de l'enable ISE pour des périphériques

Hors de la case, ISE fournit une bibliothèque de divers profils de point final. Terminez-vous ces étapes afin d'activer des profils pour des périphériques :

1. D'ISE, naviguez vers la **stratégie > en profilant**.
2. Du volet gauche, développez **profiler des stratégies**.
3. Cliquez sur l'**iPad de périphérique d'Apple > d'Apple**, et placez ce qui suit :Stratégie activée : ActivéCréez le groupe étant assorti d'identité : Sélectionné
4. Cliquez sur l'**iPhone de périphérique d'Apple > d'Apple**, placez ce qui suit :Stratégie activée : ActivéCréez le groupe étant assorti d'identité : Sélectionné
5. Le clic **Android**, a placé ce qui suit :Stratégie activée : ActivéCréez le groupe étant assorti d'identité : Sélectionné

Le profil d'autorisation ISE pour la détection de posture réorientent

Terminez-vous ces étapes afin de configurer une posture de stratégie d'autorisation réorientent permet de nouveaux périphériques à réorienter à ISE pour la détection et le profilage appropriés :

1. D'ISE, naviguez vers la **stratégie > les éléments > les résultats de stratégie**.
2. Développez l'**autorisation**. Cliquez sur les **profils d'autorisation** (volet gauche) et cliquez sur Add.
3. Créez le profil d'autorisation avec ce qui suit :Nom : Posture_RemediationType d'Access : Access_AcceptOutils communs :Détection de posture, activéeDétection de posture, ACL ACL-POSTURE-REDIRECT
4. Cliquez sur Submit pour se terminer cette tâche.
5. Confirmez que le nouveau profil d'autorisation est ajouté.

Créez le profil d'autorisation ISE pour l'employé

Ajouter un profil d'autorisation pour un employé permet à ISE pour autoriser et permettre l'accès avec les attributs assignés. L'employé VLAN 11 est assigné dans ce cas.

Procédez comme suit :

1. D'ISE, naviguez vers la **stratégie > les résultats**. Développez l'**autorisation**, puis cliquez sur les **profils d'autorisation** et cliquez sur Add.
2. Entrez dans le suivant pour le profil d'autorisation des employés :Nom : Employee_WirelessFonctionnalités usuelles :VLAN, activéVLAN, sous valeur 11
3. Cliquez sur Submit pour se terminer cette tâche.
4. Confirmez que le nouveau profil d'autorisation des employés a été créé.

Créez le profil d'autorisation ISE pour le sous-traitant

Ajouter un profil d'autorisation pour un sous-traitant permet à ISE pour autoriser et permettre l'accès avec les attributs assignés. Le sous-traitant VLAN 12 est assigné dans ce cas.

Procédez comme suit :

1. D'ISE, naviguez vers la **stratégie > les résultats**. Développez l'**autorisation**, puis cliquez sur les **profils d'autorisation** et cliquez sur Add.
2. Entrez dans le suivant pour le profil d'autorisation des employés :Nom : Employee_WirelessFonctionnalités usuelles :VLAN, activéVLAN, sous valeur 12
3. Cliquez sur Submit pour se terminer cette tâche.
4. Confirmez que le profil d'autorisation de sous-traitant a été créé.

Stratégie d'autorisation pour la posture/le profilage de périphérique

Peu d'informations sont connues au sujet d'un nouveau périphérique quand elles sont livré d'abord sur le réseau, un administrateur créeront la stratégie appropriée pour permettre des points finaux inconnus à identifier avant de permettre l'accès. Dans cet exercice, la stratégie d'autorisation sera créée de sorte qu'un nouveau périphérique soit réorienté à ISE pour l'estimation de posture (pour des périphériques mobiles soyez agentless, donc seulement le profilage est approprié) ; des points finaux seront réorientés au portail captif ISE et identifiés.

Procédez comme suit :

1. D'ISE, naviguez vers la **stratégie > l'autorisation**.
2. Il y a une stratégie pour des Téléphones IP Profiled Cisco. C'est hors de la case. Éditez ceci comme stratégie de posture.
3. Écrivez les valeurs suivantes pour cette stratégie :Nom de règle : Posture_RemediationGroupes d'identité : QuelsD'autres conditions > créent nouveau : Session (avancée) > PostureStatusPostureStatus > égaux : Inconnu
4. Placez le suivant pour des autorisations :Autorisations > norme : Posture_Remediation
5. Cliquez sur **Save**.**Note**: Des éléments de stratégie alternativement faite sur commande peuvent être créés pour ajouter la simplicité d'utilisation.

Stratégie de test de correction de posture

Àla démonstration simple peut être exécuté pour prouver qu'ISE profile correctement un nouveau périphérique basé sur la stratégie de posture.

1. D'ISE, naviguez vers la **gestion > la Gestion de l'identité > les identités**.
2. **Points finaux de** clic. Associez et connectez un périphérique (un iPhone dans cet exemple).
3. Régénérez la liste de points finaux. Observez quelles informations sont fournies.
4. Du périphérique d'extrémité, parcourez à :URL : http://www (ou 10.10.10.10)Le périphérique est réorienté. Recevez n'importe quelle demande pour des Certificats.
5. Après que le périphérique mobile ait complètement réorienté, d'ISE régénérez la liste de points finaux de nouveau. Observez ce qui a changé. Le point final précédent (par exemple, Apple-périphérique) devrait avoir changé à « Apple-iPhone » etc. La raison est que la sonde de HTTP obtient efficacement les informations d'utilisateur-agent, en tant qu'élément du processus de l'réorientation au portail de captif.

Stratégie d'autorisation pour Access différencié

Après avoir avec succès testé l'autorisation de posture, continuez à établir des stratégies pour prendre en charge l'accès différencié pour l'employé et le sous-traitant avec les périphériques connus et la particularité différente d'affectation VLAN au rôle de l'utilisateur (à ces scénario, employé et sous-traitant).

Procédez comme suit :

1. Naviguez vers **ISE > stratégie > autorisation**.
2. Ajoutez/insertion une nouvelle règle au-dessus de la stratégie/de ligne de correction de posture.
3. Écrivez les valeurs suivantes pour cette stratégie :Nom de règle : EmployéGroupes d'identité

(développez) : Groupes d'identité de point finalGroupes d'identité de point final : ProfiléProfilé : Android, Apple-iPad ou Apple-iPhone
4. Afin de spécifier des types de périphérique supplémentaire, cliquez sur **+** et ajoutez plus de périphériques (si nécessaire) :Groupes d'identité de point final : ProfiléProfilé : Android, Apple-iPad ou Apple-iPhone
5. Spécifiez les valeurs des autorisations suivantes pour cette stratégie :D'autres conditions (développez) : Créez le nouvel état (l'option avancée)Condition > expression (de la liste) : InternalUser > nomInternalUser > nom : employé
6. Ajoutez une condition pour la session de posture conforme :Les autorisations > profile > norme : Employee_Wireless
7. Cliquez sur **Save**. Confirmez que la stratégie a été ajoutée correctement.
8. Continuez en ajoutant la stratégie de sous-traitant. Dans ce document, la stratégie précédente est reproduite afin d'accélérer le processus (ou, vous pouvez manuellement configurer pour la bonne pratique).De la stratégie > des actions des employés, **doublon de** clic **ci-dessous**.
9. Éditez les champs suivants pour cette stratégie (copie en double) :Nom de règle : Sous-traitantLes autres conditions > InternalUser > nom : sous-traitantAutorisations : Contractor_Wireless
10. Cliquez sur **Save**. Confirmez que la copie reproduite précédente (ou la nouvelle stratégie) est configurée correctement.
11. Afin de visionner les stratégies préalablement, Stratégie-à-un-**regard de** clic.La stratégie visualisent d'un coup d'oeil fournit consolidé récapitulé et facile de voir des stratégies.

CoA de test pour Access différencié

Les profils et les stratégies d'autorisation étant préparé pour différencier l'accès, il est temps de tester. Ayant un WLAN sécurisé simple, un employé sera assigné l'employé VLAN et un sous-traitant sera pour le sous-traitant VLAN. Apple iPhone/iPad est utilisé dans les exemples suivants.

Procédez comme suit :

1. Connectez au WLAN sécurisé (POD1x) au périphérique mobile et utilisez ces qualifications :Nom d'utilisateur : employéMot de passe :
2. Le clic **se joignent**. Confirmez que l'employé est assigné VLAN 11 (employé VLAN).
3. Le clic **oublient ce réseau**. Confirmez en cliquant sur **oublient**.
4. Allez à WLC et enlevez les connexions client existantes (si le même était utilisé dans les étapes précédentes). Naviguez vers le **Monitor > Clients > l'adresse MAC**, puis cliquez sur **retirent**.
5. Une autre manière sûre d'effacer les sessions de client précédentes est de désactiver/enable le WLAN.Allez à **WLC > WLAN > WLAN**, puis cliquez sur le WLAN pour éditer.l'ONU-contrôle **activé > s'appliquent** (pour désactiver).Cochez la case pour **activé > s'appliquent** (pour réactiver).
6. Retournez au périphérique mobile. Connectez de nouveau au même WLAN à ces qualifications :Nom d'utilisateur : sous-traitantMot de passe :
7. Le clic **se joignent**. Confirmez que l'utilisateur de sous-traitant est assigné VLAN 12 (sous-traitant/VLAN invité).
8. Vous pouvez regarder la vue en temps réel de log ISE dans **ISE > moniteur > autorisations**. Vous devriez voir que les utilisateurs individuels (employé, sous-traitant) obtiennent des

profils différenciés d'autorisation (Employee_WirelessvsContractor_Wireless) dans différents VLAN.

Invité WLAN WLC

Terminez-vous ces étapes afin d'ajouter un WLAN invité pour permettre à des invités pour accéder au portail d'invité de sponsor ISE :

1. De WLC, naviguez vers des **WLAN > des WLAN > ajoutent nouveau**.
2. Entrez dans le suivant pour le nouveau WLAN invité :Nom de profil : pod1guestSSID : pod1guest
3. Cliquez sur **Apply**.
4. Entrez dans le suivant sous le WLAN invité > l'onglet Général :État : HandicapéInterface/groupe d'interface : Invité
5. Naviguez vers le WLAN invité **> la Sécurité > le Layer2** et entrez dans ce qui suit :Degré de sécurité de la couche 2 : Aucun
6. Naviguez vers le WLAN invité **> la Sécurité > l'**onglet **Layer3** et entrez dans ce qui suit :Degré de sécurité de la couche 3 : AucunStratégie de Web : ActivéValeur de sous-titre de stratégie de Web : AuthentificationACL de Préauthentification : ACL-POSTURE-REDIRECTType authentique de Web : Externe (réorientez au serveur externe)URL : https://10.10.10.70:8443/guestportal/Login.action
7. Cliquez sur **Apply**.
8. Veillez **à sauvegarder la configuration WLC**.

Test de l'invité WLAN et du portail d'invité

Maintenant, vous pouvez tester la configuration du WLAN invité. Il devrait réorienter les invités au portail d'invité ISE.

Procédez comme suit :

1. D'un périphérique IOS tel qu'un iPhone, naviguez vers des **réseaux > l'enable de WiFi**. Puis, sélectionnez le réseau d'invité de ZONE.
2. Votre périphérique IOS devrait afficher une adresse IP valide du VLAN invité (10.10.12.0/24).
3. Ouvrez le navigateur de safari et connectez à :URL : http://10.10.10.10Une authentification Web réorientent apparaît.
4. Le clic **continuent** jusqu'à ce que vous soyez arrivé à la page du portail d'invité ISE.Le prochain tir d'écran témoin affiche le périphérique IOS sur une procédure de connexion de portail d'invité. Ceci confirme que l'installation correcte portail pour WLAN et ISE invité est en activité.

La radio ISE a commandité l'accès invité

ISE peut être configuré pour permettre des invités à commanditer. Dans ce cas vous configurerez des stratégies d'invité ISE pour permettre les utilisateurs internes ou d'AD de domaine (si intégré) pour commanditer l'accès invité. Vous configurerez également ISE pour permettre à des sponsors pour visualiser le mot de passe d'invité (facultatif), qui est utile à ce laboratoire.

Procédez comme suit :

1. Ajoutez l'utilisateur des employés au groupe de SponsorAllAccount. Il y a différentes manières de faire ceci : allez directement au groupe, ou éditez l'utilisateur et affectez le groupe. Pour cet exemple, naviguez vers la **gestion > la Gestion de l'identité > les groupes > les groupes d'identité de l'utilisateur**. Puis, le clic **SponsorAllAccount** et ajoutent l'utilisateur des employés.
2. Naviguez vers des **groupes de gestion > de Gestion > de sponsor d'invité**.
3. Cliquez sur Edit, puis choisissez **SponsorAllAccounts**.
4. Les niveaux choisis d'autorisation et ont placé ce qui suit :Mot de passe d'invité de vue : Oui
5. **Sauvegarde de** clic afin de se terminer cette tâche.

Invité de commanditaire

Précédemment, vous avez configuré la stratégie et les groupes appropriés d'invité pour permettre à l'utilisateur de domaine d'AD pour commanditer les invités provisoires. Ensuite, vous accéderez au sponsor portail et créerez un accès invité provisoire.

Procédez comme suit :

1. D'un navigateur, naviguez vers l'un ou l'autre de ces l'URLs : <ise ip>:8080/sponsorportal/ de http:// **ou** <ise ip>:8443/sponsorportal/ de https://. Puis, procédure de connexion avec ce qui suit :Nom d'utilisateur : aduser (Répertoire actif), employé (utilisateur interne)Mot de passe :
2. De la page de sponsor, le clic **créent le compte utilisateur simple d'invité**.
3. Pour un invité provisoire, ajoutez ce qui suit :Prénom : Requis (par exemple, Sam)Nom de famille : Requis (par exemple, Jones)Rôle de groupe : InvitéProfil de temps : DefaultOneHourFuseau horaire : Quels/par défaut
4. Cliquez sur **Submit**.
5. Un invité que le compte est créé a basé sur votre entrée précédente. Notez que le mot de passe est visible (de l'exercice précédent) par opposition au *** d'informations parasites.
6. Laissez à cette fenêtre l'apparence ouverte le nom d'utilisateur et mot de passe pour l'invité. Vous les emploierez pour tester la procédure de connexion portaile d'invité (ensuite).

Invité de test Access portail

Le nouveau compte d'invité étant créé par un utilisateur/sponsor d'AD, il est temps de tester le portail et l'accès d'invité.

Procédez comme suit :

1. Sur un périphérique préféré (dans ce cas un IOS d'Apple/iPad), connectez à l'invité SSID de zone et vérifiez l'adresse IP /connectivity.
2. Utilisez le navigateur et le tentez de naviguer vers http://www.Vous êtes réorienté à la page de connexion de portail d'invité.
3. Procédure de connexion utilisant le compte d'invité créé dans l'exercice précédent.Si réussie, la page de politique d'utilisation acceptable paraît.
4. Le contrôle **reçoivent des termes et conditions générales**, puis cliquent sur **reçoivent**.L'URL d'original est terminé, et le point final est permis l'accès comme invité.

Configuration de certificat

Les communications protégées avec ISE, déterminent si la transmission est authentification associée ou pour la Gestion ISE. Par exemple, pour la configuration utilisant le Web UI ISE, les Certificats X.509 et les chaînes de confiance de certificat doivent être configurés pour activer le cryptage asymétrique.

Procédez comme suit :

1. De votre PC connecté de câble, ouvrez une fenêtre du navigateur à https://AD/certsrv.**Note**: Utilisez le HTTP sécurisé.**Note**: Utilisation Mozilla Firefox ou MS Internet Explorer afin d'accéder à ISE.
2. Procédure de connexion comme administrator/Cisco123.
3. Cliquez sur Download un **certificat de CA, une chaîne de certificat, ou un CRL**.
4. Cliquez sur Download le **certificat de CA** et sauvegardez-le (notez l'emplacement de sauvegarde).
5. Ouvrez une fenêtre du navigateur au <Pod-ISE> de https://.
6. Allez aux **Certificats de gestion > de système > de Certificats > d'autorité de Certificats**.
7. **L'autorité de certification** choisie **délivre un certificat l'**exécution et parcourt au CERT précédemment téléchargé CA.
8. **La confiance** choisie **pour le client avec l'EAP-TLS**, soumettent alors.
9. Confirmez que le CA a été ajouté a fait confiance comme racine CA.
10. D'un navigateur, allez aux **Certificats de gestion > de système > de Certificats > d'autorité de Certificats**.
11. Cliquez sur Add, puis **générez la demande de signature de certificat**.
12. Soumettez ces valeurs :Objet de certificat : CN=ise.corp.rf-demo.comLongueur principale : 2048
13. Demandes ISE que le CSR est disponible dans la page CSR. Cliquez sur **OK**.
14. Sélectionnez le CSR de la page CSR ISE et cliquez sur l'**exportation**.
15. Sauvegardez le fichier à n'importe quel emplacement (par exemple, des téléchargements, etc.)
16. Le fichier sera enregistré comme *.pem.
17. Localisez le fichier CSR et l'éditez avec l'un ou l'autre de Notepad/Wordpad/TextEdit.
18. Copiez le contenu (sélectionnez tous > copie).
19. Ouvrez une fenêtre du navigateur à https:// <Pod-AD>/certsrv.
20. **Demande de** clic un **certificat**.
21. Cliquez sur pour soumettre une **demande avancée de certificat**.
22. Collez le contenu CSR dans le domaine enregistré de demande.
23. **Le serveur Web** choisi comme modèle de certificat, cliquent sur Submit alors.
24. **DER** choisis **encodés**, cliquent sur Download alors le **certificat**.
25. Sauvegardez le fichier à un emplacement connu (par exemple, les téléchargements)
26. Allez aux **Certificats de gestion > de système > de Certificats > d'autorité de Certificats**.
27. Cliquez sur Add **> certificat de CA de grippage**.
28. Parcourez au certificat de CA précédemment téléchargé.
29. Sélectionnez l'**EAP** et l'**interface de gestion de Protocol**, puis cliquez sur Submit.
30. Confirmez que le CA a été ajouté a fait confiance comme racine CA.

Intégration de Répertoire actif de Windows 2008

ISE peut communiquer directement avec le Répertoire actif (AD) pour l'utilisateur/authentification de machine ou pour récupérer des attributs d'utilisateur des informations d'autorisation. Afin de communiquer avec l'AD, ISE doit « être joint » à un domaine d'AD. Dans cet exercice vous joindrez ISE à un domaine d'AD, et confirmez la transmission d'AD fonctionne correctement.

Procédez comme suit :

1. Afin de joindre ISE au domaine d'AD, d'ISE allez à la **gestion > à la Gestion de l'identité > des sources extérieures d'identité**.
2. Du volet gauche (sources extérieures d'identité), **Répertoire actif** choisi.
3. Du côté droit, sélectionnez l'**onglet Connection** et entrez dans ce qui suit :Nom de domaine : corp.rf-demo.comNom de mémoire d'identité : AD1
4. **Connexion de test de** clic. Écrivez le nom d'utilisateur d'AD (aduser/Cisco123), puis cliquez sur OK.
5. Confirmez que les expositions d'état du test **testent réussi**.
6. Sélectionnez le log détaillé par exposition et observez les détails utiles pour le dépannage. Cliquez sur **OK** pour continuer.
7. **Save configuration de** clic.
8. Le clic **se joignent**. Présentez l'utilisateur d'AD (administrator/Cisco123), puis cliquez sur OK.
9. Confirmez qui joignent les expositions d'état d'exécution **réussies**, puis cliquent sur OK pour continuer.Les expositions d'état de connexion au serveur **CONNECTÉES**. Si ce les changements d'état à tout moment, une connexion de test aideront à dépanner des questions avec les exécutions d'AD.

Ajoutez les groupes de Répertoire actif

Quand des groupes d'AD sont ajoutés, on permet un contrôle plus granulaire des stratégies ISE. Par exemple, des groupes d'AD peuvent être différenciés par des rôles fonctionnels, tels que des groupes des employés ou de sous-traitant, sans bogue relative étant éprouvée dans des exercices précédents ISE 1.0 où des stratégies ont été limitées seulement aux utilisateurs.

Dans ce laboratoire, seulement les utilisateurs de domaine et/ou le groupe des employés sont utilisés.

Procédez comme suit :

1. D'ISE, allez à la **gestion > à la Gestion de l'identité > des sources extérieures d'identité**.
2. Onglet choisi de **Répertoire actif > de groupes**.
3. Cliquez sur **+Add**, puis **sélectionnez les groupes à partir du répertoire**.
4. Dans la fenêtre complémentaire (groupes choisis de répertoire), recevez les par défaut pour le domaine (corp-rf-demo.com) et filtrez (*). Puis, clic RetrieveGroups**.**
5. Sélectionnez les cases pour des groupes d'**utilisateurs** et d'**employés de domaine**. Cliquez sur OK une fois terminé.
6. Confirmez que les groupes ont été ajoutés à la liste.

Ajoutez l'ordre de source d'identité

Par défaut, ISE est placé pour utiliser des utilisateurs internes pour la mémoire d'authentification. Si l'AD est ajouté, une commande prioritaire de l'ordre peut être créée pour inclure l'AD qu'ISE l'utilisera pour vérifier l'authentification.

Procédez comme suit :

1. D'ISE, naviguez vers des **ordres de source de gestion > de Gestion de l'identité > d'identité**.
2. Clic **+Add** afin d'ajouter un nouvel ordre.
3. Écrivez le nouveau nom : **AD_Internal**. Ajoutez toutes les sources disponibles au champ sélectionné. Puis, commandez à nouveau pendant que nécessaire de sorte qu'AD1 soit déplacé au haut de la liste. Cliquez sur **Submit**.
4. Confirmez que l'ordre a été ajouté à la liste.

Accès invité commandité Sans fil ISE avec l'AD intégré

ISE peut être configuré pour permettre des invités à commanditer avec des stratégies afin de permettre à des utilisateurs de domaine d'AD pour commanditer l'accès invité.

Procédez comme suit :

1. D'ISE, naviguez vers la **gestion > la Gestion > les configurations d'invité**.
2. Développez le **sponsor**, et cliquez sur la **source d'authentification**. Puis, **AD_Internal** choisi en tant qu'ordre de mémoire d'identité.
3. Confirmez AD_Internal comme l'ordre de mémoire d'identité. Cliquez sur **Save**.
4. Naviguez vers la **Gestion de gestion > d'invité > la stratégie de groupe de sponsor**.
5. Insérez la nouvelle stratégie au-dessus de la première règle (cliquez sur l'icône d'**actions de la** droite).
6. Pour la nouvelle stratégie de groupe de sponsor, créez ce qui suit :Nom de règle : Utilisateurs de domaineGroupes d'identité : QuelsD'autres conditions : (Créez nouveau/avez avancé) > AD1AD1 : Groupes externesLes groupes AD1 externes > égale > des utilisateurs de corp.rf-demo.com/Users/Domain
7. Dans des groupes de sponsor, placez ce qui suit :Groupes de sponsor : SponsorAllAccounts
8. Naviguez vers des **groupes de gestion > de Gestion > de sponsor d'invité**.
9. Sélectionnez pour éditer > **SponsorAllAccounts**.
10. Les niveaux choisis d'autorisation et ont placé ce qui suit :Mot de passe d'invité de vue : Oui

Configurez l'ENVERGURE sur le commutateur

Configurez l'ENVERGURE - Le mgt ISE/interface de sonde est L2 à côté d'interface de gestion WLC. Le commutateur peut être configuré POUR LE RÉPARTIR et d'autres interfaces, telles que des interfaces vlan des employés et d'invité.

```
Podswitch(config)#monitor session 1 source vlan10 , 11 , 12
Podswitch(config)#monitor session 1 destination interface Fa0/8
ISE virtual probe interface.
```

Référence : Authentification Sans fil pour le MAC OS X d'Apple

Associez-vous au WLC par l'intermédiaire d'un SSID authentifié en tant qu'utilisateur interne (ou a intégré, utilisateur d'AD) utilisant un ordinateur portable sans fil de Mac OS X d'Apple. Saut sinon applicable.

1. Sur un MAC, allez aux configurations WLAN. Activez le Wifi, puis le sélectionnez et connectez à la ZONE activée par 802.1X SSID créée dans l'exercice précédent.
2. Fournissez les informations suivantes pour se connecter :Nom d'utilisateur : aduser (si utilisant l'AD), employé (– employé), sous-traitant (interne – sous-traitant interne)Mot de passe :802.1X : AutomatiqueCertificat de TLS : AucunÀce moment, l'ordinateur portable ne pourrait pas se connecter. En outre, ISE peut jeter un événement défectueux comme suit :
```
Authentication failed :12514 EAP-TLS failed SSL/TLS handshake because of
an unknown CA in the client certificates chain
```
3. Allez à la **Préférence Système > au réseau > à l'aéroport > au 802.1X** plaçant et placez la nouvelle authentification de profil de la ZONE SSID/WPA en tant que :TLS : HandicapéPEAP : ActivéTTL : HandicapéEAP-FAST : Handicapé
4. Cliquez sur OK pour continuer et permettre la configuration à enregistrer.
5. Sur l'écran Réseau, sélectionnez l'approprié profil SSID + de 802.1X WPA et le clic **se connectent**.
6. Le système pourrait inciter pour un nom d'utilisateur et mot de passe. Entrez l'utilisateur d'AD et le mot de passe (), puis cliquez sur OK.Le client devrait afficher **connecté** par l'intermédiaire du PEAP à une adresse IP valide.

Référence : Authentification Sans fil pour Microsoft Windows XP

Associez-vous au WLC par l'intermédiaire d'un SSID authentifié en tant qu'utilisateur interne (ou a intégré, utilisateur d'AD) utilisant un ordinateur portable sans fil de Windows XP. Saut sinon applicable.

Procédez comme suit :

1. Sur l'ordinateur portable, allez aux configurations WLAN. Activez le Wifi et connectez à la ZONE activée par 802.1X SSID créée dans l'exercice précédent.
2. Accédez aux propriétés du réseau pour l'interface de Wifi.
3. Naviguez vers les **réseaux sans fil que** tableau sélectionnent les propriétés du réseau de la zone SSID > l'onglet d'authentification > le type d'EAP = l'EAP protégé (PEAP).
4. Cliquez sur l'EAP Properties.
5. Placez ce qui suit :Validez le certificat de serveur : HandicapéMéthode d'authentification : Mot de passe sécurisé (EAP-MSCHAP v2)
6. Cliquez sur OK sur toutes les fenêtres pour se terminer cette tâche de configuration.
7. Demandes de client de Windows XP pour le nom d'utilisateur et mot de passe. Dans cet exemple, c'est.
8. Confirmez la connexion réseau, l'adressage IP (v4).

Référence : Authentification Sans fil pour Microsoft Windows 7

Associez-vous au WLC par l'intermédiaire d'un SSID authentifié en tant qu'utilisateur interne (ou a intégré, utilisateur d'AD) utilisant un ordinateur portable sans fil de Windows 7.

1. Sur l'ordinateur portable, allez aux configurations WLAN. Activez le Wifi et connectez à la ZONE activée par 802.1X SSID créée dans l'exercice précédent.
2. Accédez à Wireless Manager et éditez le nouveau profil de radio de ZONE.
3. Placez ce qui suit :Méthode d'authentification : PEAPSouvenez-vous mes qualifications… : HandicapéValidez le certificat de serveur (paramètre avancé) : HandicapéMéthode d'authentification (adv. Établissement) : EAP-MSCHAP v2Utilisez automatiquement ma connexion de Windows… : Handicapé

Informations connexes

- Support et documentation techniques - Cisco Systems