Sécurité sans fil Cisco Aironet - Forum Aux Questions

Contenu

Introduction

Ce document fournit des informations sur les questions fréquemment posées au sujet de la sécurité sans fil de Cisco Aironet.

FAQ générales

Q. Quel est le besoin de la sécurité sans fil ?

A. Dans un réseau câblé, les données restent dans les câbles qui connectent les périphériques finaux. Mais les réseaux sans fil transmettent et reçoivent des données via une diffusion de signaux RF dans l'air libre. En raison de la nature de diffusion utilisée par les WLAN, les pirates informatiques ou les intrus qui peuvent accéder aux données ou les corrompre sont plus nombreux. Pour résoudre ce problème, tous les WLAN nécessitent l'ajout de :

1. Authentification de l'utilisateur pour empêcher l'accès non autorisé aux ressources réseau.
2. Confidentialité des données pour protéger l'intégrité et la confidentialité des données transmises (également appelée cryptage).

Q. Quelles sont les différentes méthodes d'authentification définies par la norme 802.11 pour les réseaux locaux sans fil ?

A. La norme 802.11 définit deux mécanismes d'authentification des clients LAN sans fil :

1. Authentification ouverte
2. Authentification à clé partagée

Il existe également deux autres mécanismes couramment utilisés :

1. Authentification SSID
2. Authentification de l'adresse MAC

Q. Qu'est-ce que l'authentification ouverte ?

A. L'authentification ouverte est essentiellement un algorithme d'authentification nul, ce qui signifie qu'il n'y a aucune vérification de l'utilisateur ou de la machine. Open Authentication permet à tout périphérique qui place une demande d'authentification au point d'accès (AP). L'authentification ouverte utilise la transmission en texte clair pour permettre à un client de s'associer à un point d'accès. Si aucun chiffrement n'est activé, tout périphérique qui connaît le SSID du WLAN peut accéder au réseau. Si le protocole WEP (Wired Equivalent Privacy) est activé sur le point d'accès, la clé WEP devient un moyen de contrôle d'accès. Un périphérique qui n'a pas la clé WEP correcte ne peut pas transmettre de données via le point d'accès même si l'authentification réussit. Un tel périphérique ne peut pas non plus décrypter les données que le point d'accès envoie.

Q. Quelles étapes l'authentification ouverte implique-t-elle pour qu'un client s'associe au point d'accès ?

1. Le client envoie une requête d'analyse aux points d'accès.
2. Les points d'accès envoient des réponses de sonde.
3. Le client évalue les réponses AP et sélectionne le meilleur AP.
4. Le client envoie une demande d'authentification au point d'accès.
5. Le point d'accès confirme l'authentification et enregistre le client.
6. Le client envoie ensuite une demande d'association au point d'accès.
7. Le point d'accès confirme l'association et enregistre le client.

Q. Quels sont les avantages et les inconvénients de l'authentification ouverte ?

A. Voici les avantages et les inconvénients de l'authentification ouverte :

Avantages : Open Authentication est un mécanisme d'authentification de base, que vous pouvez utiliser avec les périphériques sans fil qui ne prennent pas en charge les algorithmes d'authentification complexes. L'authentification dans la spécification 802.11 est orientée connectivité. En concevant les exigences d'authentification, vous autorisez les périphériques à accéder rapidement au réseau. Dans ce cas, vous pouvez utiliser l'authentification ouverte.

Inconvénients : L'authentification ouverte n'offre aucun moyen de vérifier si un client est un client valide et non un client pirate. Si vous n'utilisez pas le cryptage WEP avec l'authentification ouverte, tout utilisateur qui connaît le SSID du WLAN peut accéder au réseau.

Q. Qu'est-ce que l'authentification par clé partagée ?

A. L'authentification par clé partagée fonctionne comme l'authentification ouverte avec une différence majeure. Lorsque vous utilisez l'authentification ouverte avec la clé de chiffrement WEP, la clé WEP est utilisée pour chiffrer et déchiffrer les données, mais elle n'est pas utilisée dans l'étape d'authentification. Dans Shared Key Authentication, le chiffrement WEP est utilisé pour l'authentification. Comme pour l'authentification ouverte, l'authentification par clé partagée nécessite que le client et l'AP aient la même clé WEP. Le point d'accès qui utilise l'authentification à clé partagée envoie un paquet de texte de confirmation au client. Le client utilise la clé WEP configurée localement pour chiffrer le texte de la demande de confirmation et répondre par une demande d'authentification ultérieure. Si le point d'accès peut déchiffrer la demande d'authentification et récupérer le texte de la demande de confirmation initiale, le point d'accès répond par une réponse d'authentification qui accorde l'accès au client.

Q. Quelles étapes l'authentification par clé partagée implique-t-elle pour qu'un client s'associe au point d'accès ?

1. Le client envoie une requête d'analyse aux points d'accès.
2. Les points d'accès envoient des réponses de sonde.
3. Le client évalue les réponses AP et sélectionne le meilleur AP.
4. Le client envoie une demande d'authentification au point d'accès.
5. Le point d'accès envoie une réponse d'authentification qui contient le texte de la demande de confirmation non chiffré.
6. Le client chiffre le texte de la demande de confirmation avec la clé WEP et envoie le texte au point d'accès.
7. Le point d'accès compare le texte de défi non chiffré au texte de défi chiffré. Si l'authentification peut décrypter et récupérer le texte de la demande de confirmation d'origine, l'authentification réussit.

L'authentification par clé partagée utilise le cryptage WEP pendant le processus d'association du client.

Q. Quels sont les avantages et les inconvénients de l'authentification par clé partagée ?

A. Dans Shared Key Authentication, le client et le point d'accès échangent le texte du défi (texte clair) et le défi chiffré. Par conséquent, ce type d'authentification est vulnérable aux attaques de l'homme du milieu. Un pirate peut écouter les défis non chiffrés et chiffrés, et extraire la clé WEP (clé partagée) de ces informations. Lorsqu'un pirate connaît la clé WEP, l'ensemble du mécanisme d'authentification est compromis et le pirate peut accéder au réseau WLAN. C'est le principal inconvénient de l'authentification par clé partagée.

Q. Qu'est-ce que l'authentification d'adresse MAC ?

A. Bien que la norme 802.11 ne spécifie pas l'authentification d'adresse MAC, les réseaux WLAN utilisent généralement cette technique d'authentification. Par conséquent, la plupart des fournisseurs de périphériques sans fil, dont Cisco, prennent en charge l'authentification des adresses MAC.

Dans l'authentification d'adresse MAC, les clients sont authentifiés en fonction de leur adresse MAC. Les adresses MAC des clients sont vérifiées par rapport à une liste d'adresses MAC stockées localement sur le point d'accès ou sur un serveur d'authentification externe. L'authentification MAC est un mécanisme de sécurité plus puissant que les authentifications de clé ouverte et partagée fournies par 802.11. Cette forme d'authentification réduit encore davantage la probabilité que des périphériques non autorisés puissent accéder au réseau.

Q. Pourquoi l'authentification MAC ne fonctionne-t-elle pas avec le Wi-Fi Protected Access (WPA) dans le logiciel Cisco IOS Version 12.3(8)JA2 ?

A. Le seul niveau de sécurité pour l'authentification MAC est de vérifier l'adresse MAC du client par rapport à une liste d'adresses MAC autorisées. C'est considéré comme très faible. Dans les versions antérieures du logiciel Cisco IOS, vous pouvez configurer l'authentification MAC et le WPA pour chiffrer les informations. Mais comme WPA lui-même possède une adresse MAC qui vérifie, Cisco a décidé de ne pas autoriser ce type de configuration dans les versions ultérieures

du logiciel Cisco IOS et a décidé seulement d'améliorer les fonctionnalités de sécurité.

Q. Puis-je utiliser le SSID comme méthode d'authentification des périphériques sans fil ?

A. Le SSID (Service Set Identifier) est une valeur alphanumérique unique, sensible à la casse, que les WLAN utilisent comme nom de réseau. Le SSID est un mécanisme -qui permet la séparation logique des réseaux locaux sans fil. Le SSID ne fournit aucune fonction de confidentialité des données, pas plus que le SSID n'authentifie réellement le client au point d'accès. La valeur SSID est diffusée en texte clair dans les balises, les requêtes de sondage, les réponses de sondage et d'autres types de trames. Un écouteur peut facilement déterminer le SSID à l'aide d'un analyseur de paquets LAN sans fil 802.11, par exemple Sniffer Pro. Cisco ne vous recommande pas d'utiliser le SSID comme méthode de sécurisation de votre réseau WLAN.

Q. Si je désactive la diffusion SSID, puis-je améliorer la sécurité sur un réseau WLAN ?

A. Lorsque vous désactivez la diffusion SSID, le SSID n'est pas envoyé dans les messages Beacon. Cependant, d'autres trames telles que les requêtes de sondage et les réponses de sondage ont toujours le SSID en texte clair. Par conséquent, vous n'améliorez pas la sécurité sans fil si vous désactivez le SSID. Le SSID n'est pas conçu, ni destiné à être utilisé, comme mécanisme de sécurité. En outre, si vous désactivez les diffusions SSID, vous pouvez rencontrer des problèmes d'interopérabilité Wi-Fi pour les déploiements de clients mixtes. Par conséquent, Cisco ne vous recommande pas d'utiliser le SSID comme mode de sécurité.

Q. Quelles sont les vulnérabilités de la sécurité 802.11 ?

A. Les principales vulnérabilités de la sécurité 802.11 peuvent être résumées comme suit :

- Authentification limitée aux périphériques : Les périphériques clients sont authentifiés, pas les utilisateurs.
- Chiffrement des données faible : Le protocole WEP (Wired Equivalent Privacy) s'est avéré inefficace pour chiffrer les données.
- Aucune intégrité des messages : La valeur de contrôle d'intégrité (ICV) s'est révélée inefficace comme moyen de garantir l'intégrité des messages.

Q. Quel est le rôle de l'authentification 802.1x dans le WLAN ?

A. Afin de remédier aux lacunes et aux vulnérabilités de sécurité des méthodes d'authentification originales définies par la norme 802.11, le cadre d'authentification 802.1X est inclus dans le projet d'améliorations de sécurité de la couche MAC 802.11. Le groupe de travail i (TGi) IEEE 802.11 développe actuellement ces améliorations. La structure 802.1X fournit à la couche liaison une authentification extensible, normalement visible uniquement dans les couches supérieures.

Q. Quelles sont les trois entités définies par le cadre 802.1x ?

A. La structure 802.1x requiert ces trois entités logiques pour valider les périphériques sur un réseau WLAN.

1. **Supplicant** : le demandeur réside sur le client LAN sans fil et est également appelé client EAP.
2. **Authenticator** : l'authentificateur réside sur le point d'accès.
3. **Authentication Server** : le serveur d'authentification réside sur le serveur RADIUS.

Q. Comment se produit l'authentification d'un client sans fil lorsque j'utilise le cadre d'authentification 802.1x ?

A. Lorsque le client sans fil (client EAP) devient actif, le client sans fil s'authentifie avec une authentification ouverte ou partagée. 802.1x fonctionne avec l'authentification ouverte et démarre après que le client s'associe correctement au point d'accès. La station client peut s'associer, mais ne peut transmettre le trafic de données qu'après une authentification 802.1x réussie. Voici les étapes de l'authentification 802.1x :

1. L'AP (Authentificateur) configuré pour 802.1x demande l'identité de l'utilisateur au client.
2. Les clients répondent avec leur identité dans un délai prescrit.
3. Le serveur vérifie l'identité de l'utilisateur et commence l'authentification avec le client si l'identité de l'utilisateur est présente dans sa base de données.
4. Le serveur envoie un message de réussite au point d'accès.
5. Une fois le client authentifié, le serveur transfère la clé de chiffrement au point d'accès qui est utilisé pour chiffrer/déchiffrer le trafic envoyé au client et en provenance de celui-ci.
6. À l'étape 4, si l'identité de l'utilisateur n'est pas présente dans la base de données, le serveur abandonne l'authentification et envoie un message d'échec au point d'accès.
7. Le point d'accès transmet ce message au client et le client doit s'authentifier à nouveau avec les informations d'identification correctes.

Remarque : Tout au long de l'authentification 802.1x, le point d'accès transfère les messages d'authentification vers et depuis le client.

Q. Quelles sont les différentes variantes EAP que je peux utiliser avec le cadre d'authentification 802.1x ?

A. 802.1x définit la procédure d'authentification des clients. Le type EAP utilisé dans le cadre 802.1x définit le type d'informations d'identification et de méthode d'authentification utilisées dans l'échange 802.1x. La structure 802.1x peut utiliser l'une des variantes EAP suivantes :

- EAP-TLS : sécurité de la couche de transport du protocole d'authentification extensible
- EAP-FAST : authentification flexible EAP via tunnel sécurisé
- EAP-SIM : module d'identité d'abonné EAP
- Cisco LEAP : protocole d'authentification extensible léger
- EAP-PEAP : protocole EAP Protected Extensible Authentication Protocol
- EAP-MD5—Algorithme EAP-Message Digest 5

- EAP-OTP : mot de passe EAP en temps réel
- EAP-TTLS—Sécurité de la couche de transport tunnel EAP

Q. Comment choisir une méthode EAP 802.1x parmi les différentes variantes disponibles ?

A. Le facteur le plus important que vous devez considérer est de savoir si la méthode EAP est compatible avec le réseau existant ou non. En outre, Cisco vous recommande de choisir une méthode prenant en charge l'authentification mutuelle.

Q. Qu'est-ce que l'authentification EAP locale ?

A. Le protocole EAP local est un mécanisme dans lequel le WLC agit en tant que serveur d'authentification. Les informations d'identification des utilisateurs sont stockées localement sur le WLC pour authentifier les clients sans fil, qui agit comme un processus principal dans les bureaux distants lorsque le serveur tombe en panne. Les informations d'identification de l'utilisateur peuvent être récupérées soit à partir de la base de données locale sur le WLC, soit à partir d'un serveur LDAP externe. LEAP, EAP-FAST, EAP-TLS, PEAPv0/MSCHAPv2 et PEAPv1/GTC sont des authentifications EAP différentes prises en charge par EAP local.

Q. Qu'est-ce que Cisco LEAP ?

A. LEAP (Lightweight Extensible Authentication Protocol) est une méthode d'authentification propriétaire de Cisco. Cisco LEAP est un type d'authentification 802.1X pour les LAN sans fil (WLAN). Cisco LEAP prend en charge une authentification mutuelle forte entre le client et un serveur RADIUS via un mot de passe d'ouverture de session en tant que secret partagé. Cisco LEAP fournit des clés de cryptage dynamiques par utilisateur et par session. LEAP est la méthode la moins compliquée pour déployer 802.1x et ne nécessite qu'un serveur RADIUS. Référez-vous à Cisco LEAP pour plus d'informations sur LEAP.

Q. Comment fonctionne EAP-FAST ?

A. EAP-FAST utilise des algorithmes de clé symétrique pour réaliser un processus d'authentification par tunnel. L'établissement du tunnel repose sur un PAC (Protected Access Credential) qui permet à EAP-FAST d'être provisionné et géré dynamiquement par EAP-FAST via le serveur AAA (Authentication, Authorization, and Accounting) (tel que Cisco Secure Access Control Server [ACS] v. 3.2.3). Avec un tunnel mutuellement authentifié, EAP-FAST offre une protection contre les attaques de dictionnaire et les vulnérabilités de l'homme du milieu. Voici les phases de EAP-FAST :

EAP-FAST permet non seulement d'atténuer les risques liés aux attaques passives par dictionnaire et aux attaques de l'homme du milieu, mais également d'activer une authentification sécurisée basée sur l'infrastructure actuellement déployée.

- Phase 1 : Établir un tunnel mutuellement authentifié : le client et le serveur AAA utilisent PAC pour s'authentifier et établir un tunnel sécurisé.
- Phase 2 : Authentification du client dans le tunnel établi : le client envoie le nom d'utilisateur et le mot de passe pour authentifier et établir la stratégie d'autorisation du client.
- Éventuellement, Phase 0 : l'authentification EAP-FAST utilise rarement cette phase pour permettre au client d'être provisionné dynamiquement avec un PAC. Cette phase génère des

informations d'identification d'accès par utilisateur sécurisées entre l'utilisateur et le réseau. La phase 1 de l'authentification utilise ces informations d'identification par utilisateur, appelées PAC.

Référez-vous à Cisco EAP-FAST pour plus d'informations.

Q. Existe-t-il sur cisco.com des documents expliquant comment configurer EAP dans un réseau WLAN Cisco ?

A. Référez-vous à Authentification EAP avec serveur RADIUS pour plus d'informations sur la façon de configurer l'authentification EAP dans un réseau WLAN.

Référez-vous à Note d'application EAP protégée pour plus d'informations sur la façon de configurer l'authentification PEAP.

Référez-vous à Authentification LEAP avec un serveur RADIUS local pour plus d'informations sur la façon de configurer l'authentification LEAP.

Q. Quels sont les différents mécanismes de cryptage les plus couramment utilisés dans les réseaux sans fil ?

A. Voici les schémas de cryptage les plus couramment utilisés dans les réseaux sans fil :

- WEP
- TKIP
- AES

AES est une méthode de cryptage matériel, tandis que le cryptage WEP et TKIP est traité sur le micrologiciel. Grâce à une mise à niveau du micrologiciel, les périphériques WEP peuvent prendre en charge TKIP afin qu'ils soient interopérables. AES est la méthode la plus sécurisée et la plus rapide, tandis que WEP est la méthode la moins sécurisée.

Q. Qu'est-ce que le cryptage WEP ?

A. WEP signifie Wired Equivalent Privacy. WEP est utilisé pour chiffrer et déchiffrer les signaux de données qui transmettent entre les périphériques WLAN. WEP est fonctionnalité facultative de IEEE 802.11 qui empêche la divulgation et la modification de paquets en transit et fournit également un contrôle d'accès pour l'usage du réseau. WEP rend une liaison WLAN aussi sécurisée qu'une liaison câblée. Comme la norme le spécifie, WEP utilise l'algorithme RC4 avec une clé 40 bits ou 104 bits. RC4 est un algorithme symétrique, parce que RC4 utilise la même clé pour le cryptage et le décryptage des données. Lorsque WEP est activé, chaque station radio possède une clé. La clé est utilisée pour brouiller les données avant la transmission des données par les ondes hertziennes. Si une station reçoit un paquet qui n'est pas brouillé avec la clé appropriée, la station rejette le paquet et ne livre jamais un tel paquet à l'hôte.

Référez-vous à Configuration de WEP (Wired Equivalent Privacy) pour plus d'informations sur la façon de configurer WEP.

Q. Qu'est-ce que la rotation des clés de diffusion ? Quelle est la fréquence de la rotation des clés de diffusion ?

A. La rotation des clés de diffusion permet au point d'accès de générer la meilleure clé de groupe aléatoire possible. La rotation des clés de diffusion met périodiquement à jour tous les clients capables de gérer les clés. Lorsque vous activez la rotation des clés WEP de diffusion, l'AP fournit une clé WEP de diffusion dynamique et modifie la clé à l'intervalle que vous définissez. La rotation des clés de diffusion est une excellente alternative à TKIP si votre réseau local sans fil prend en charge les périphériques ou périphériques clients sans fil non Cisco que vous ne pouvez pas mettre à niveau vers le micrologiciel le plus récent pour les périphériques clients Cisco. Référez-vous à Activation et désactivation de la rotation des clés de diffusion pour plus d'informations sur la configuration de la fonction de rotation des clés de diffusion.

Q. Qu'est-ce que TKIP ?

A. TKIP signifie Temporal Key Integrity Protocol. TKIP a été introduit pour remédier aux lacunes du chiffrement WEP. TKIP est également connu sous le nom de hachage de clé WEP et a été initialement appelé WEP2. TKIP est une solution temporaire qui corrige le problème de réutilisation des clés WEP. TKIP utilise l'algorithme RC4 pour effectuer le chiffrement, qui est identique à WEP. Une différence majeure par rapport au protocole WEP est que TKIP modifie la clé temporelle de chaque paquet. La clé temporelle change chaque paquet car la valeur de hachage de chaque paquet change.

Q. Les périphériques qui utilisent TKIP peuvent-ils interagir avec les périphériques qui utilisent le cryptage WEP ?

A. L'un des avantages de TKIP est que les WLAN avec des points d'accès et des radios WEP existants peuvent effectuer une mise à niveau vers TKIP via de simples correctifs de micrologiciel. En outre, les équipements uniquement WEP fonctionnent toujours avec les périphériques compatibles TKIP qui utilisent WEP.

Q. Qu'est-ce que la vérification de l'intégrité des messages (MIC) ?

A. MIC est une autre amélioration pour répondre aux vulnérabilités du cryptage WEP. La MIC empêche les attaques de type binaire sur les paquets chiffrés. Au cours d'une attaque à rebours, un intrus intercepte un message chiffré, modifie le message et retransmet ensuite le message modifié. Le destinataire ne sait pas que le message est corrompu et non légitime. Afin de résoudre ce problème, la fonctionnalité MIC ajoute un champ MIC à la trame sans fil. Le champ MIC fournit une vérification de l'intégrité des trames qui n'est pas vulnérable aux mêmes défauts mathématiques que l'ICV. Le MIC ajoute également un champ de numéro de séquence à la trame sans fil. Le point d'accès abandonne les trames reçues dans le désordre.

Q. Qu'est-ce que le WPA ? En quoi le WPA 2 est-il différent du WPA ?

A. WPA est une solution de sécurisation basée sur standard de l'alliance de Wi-Fi qui traite des vulnérabilités dans les WLAN natifs. Le WPA fournit la protection des données améliorée et le contrôle d'accès pour des systèmes WLAN. WPA traite toutes les vulnérabilités WEP (Wired Equivalent Privacy) connues dans la mise en oeuvre de sécurité IEEE 802.11 d'origine et apporte une solution de sécurité immédiate aux réseaux WLAN dans les environnements d'entreprise et de petite entreprise, de bureau à domicile (SOHO).

WPA2 est la nouvelle génération de sécurité Wi-Fi. WPA2 est la mise en oeuvre interopérable Wi-Fi Alliance de la norme IEEE 802.11i ratifiée. WPA2 implémente l'algorithme de chiffrement AES (Advanced Encryption Standard) recommandé par le National Institute of Standards and

Technology (NIST) avec l'utilisation du mode Compteur avec le protocole CCMP (Cipher Block Chaining Message Authentication Code Protocol). Le mode compteur AES est un cryptage par blocs qui crypte les blocs de données de 128 bits à la fois avec une clé de cryptage de 128 bits. Le WPA2 offre un niveau de sécurité supérieur au WPA. WPA2 crée de nouvelles clés de session sur chaque association. Les clés de chiffrement utilisées par WPA2 pour chaque client du réseau sont uniques et spécifiques à ce client. Finalement, chaque paquet qui est envoyé sans fil est crypté avec une clé unique.

WPA1 et WPA2 peuvent utiliser le cryptage TKIP ou CCMP. (Il est vrai que certains points d'accès et certains clients limitent les combinaisons, mais il existe quatre combinaisons possibles). La différence entre WPA1 et WPA2 réside dans les éléments d'information qui sont placés dans les balises, les trames d'association et les trames d'échange en 4 étapes. Les données de ces éléments d'information sont essentiellement les mêmes, mais l'identificateur utilisé est différent. La principale différence dans la connexion de clé est que WPA2 inclut la clé de groupe initiale dans la connexion en 4 étapes et que la première connexion de clé de groupe est ignorée, tandis que WPA doit effectuer cette connexion supplémentaire pour fournir les clés de groupe initiales. La nouvelle frappe de la clé de groupe se produit de la même manière. La connexion a lieu avant la sélection et l'utilisation de la suite de chiffrement (TKIP ou AES) pour la transmission des datagrammes utilisateur. Lors de la connexion WPA1 ou WPA2, la suite de chiffrement à utiliser est déterminée. Une fois sélectionnée, la suite de chiffrement est utilisée pour tout le trafic utilisateur. Par conséquent, WPA1 plus AES n'est pas WPA2. WPA1 autorise (mais est souvent limité côté client) le chiffrement TKIP ou AES.

Q. Qu'est-ce que AES ?

A. AES signifie Advanced Encryption Standard. AES offre un chiffrement beaucoup plus fort. AES utilise l'algorithme Rijndael, qui est un algorithme de chiffrement de bloc avec prise en charge des clés 128, 192 et 256 bits et est beaucoup plus puissant que RC4. Pour que les périphériques WLAN prennent en charge AES, le matériel doit prendre en charge AES au lieu de WEP.

Q. Quelles méthodes d'authentification sont prises en charge par un serveur Microsoft Internet Authentication Service (IAS) ?

A. IAS prend en charge ces protocoles d'authentification :

- Protocole PAP (Password Authentication Protocol)
- Protocole SPAP (Shiva Password Authentication Protocol)
- Protocole CHAP (Challenge Handshake Authentication Protocol)
- Protocole Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
- Protocole d'authentification à échanges confirmés Microsoft version 2 (MS-CHAP v2)
- Protocole d'authentification extensible - Digest de message 5 CHAP (EAP-MD5 CHAP)
- EAP-Transport Layer Security (EAP-TLS)
- Protected EAP-MS-CHAP v2 (PEAP-MS-CHAP v2) (également appelé PEAPv0/EAP-MSCHAPv2)

PEAP-TLS IAS dans Windows 2000 Server prend en charge PEAP-MS-CHAP v2 et PEAP-TLS lors de l'installation de Windows 2000 Server Service Pack 4. Pour plus d'informations, référez-vous à Méthodes d'authentification à utiliser avec IAS .

Q. Comment le VPN est-il mis en oeuvre dans un environnement sans fil ?

A. Le VPN est un mécanisme de sécurité de couche 3 ; des mécanismes de cryptage sans fil sont mis en oeuvre au niveau de la couche 2. VPN est mis en oeuvre sur 802.1x, EAP, WEP, TKIP et AES. Lorsqu'un mécanisme de couche 2 est en place, le VPN ajoute une surcharge à la mise en oeuvre. Dans des endroits comme les points d'accès publics et les hôtels où aucune sécurité n'est mise en oeuvre, le VPN serait une solution utile à mettre en oeuvre.

FAQ sur le dépannage et la conception

Q. Existe-t-il des meilleures pratiques pour déployer la sécurité sans fil dans un LAN sans fil extérieur ?

A. Reportez-vous aux Méthodes Recommandées Pour La Sécurité Sans Fil Extérieure. Ce document fournit des informations sur les meilleures pratiques de sécurité pour déployer un réseau local sans fil extérieur.

Q. Puis-je utiliser un serveur Windows 2000 ou 2003 avec Active Directory pour un serveur RADIUS afin d'authentifier les clients sans fil ?

A. Le serveur Windows 2000 ou 2003 avec un répertoire actif peut fonctionner comme serveur RADIUS. Pour plus d'informations sur la configuration de ce serveur RADIUS, vous devez contacter Microsoft, car Cisco ne prend pas en charge la configuration du serveur Windows.

Q. Mon site est sur le point de migrer d'un réseau sans fil ouvert (AP des gammes 350 et 1200) vers un réseau PEAP. Je souhaite que le SSID OPEN (un SSID configuré pour l'authentification ouverte) et le SSID PEAP (un SSID configuré pour l'authentification PEAP) fonctionnent simultanément sur le même AP. Cela nous donne le temps de migrer les clients vers le SSID PEAP. Existe-t-il un moyen d'héberger simultanément un SSID Open et un SSID PEAP sur le même AP ?

A. Les points d'accès Cisco prennent en charge les VLAN (couche 2 uniquement). C'est en fait la seule façon d'atteindre ce que vous voulez faire. Vous devez créer deux VLAN (natif et votre autre VLAN). Ensuite, vous pouvez avoir une clé WEP pour l'une et aucune clé WEP pour l'autre. De cette manière, vous pouvez configurer l'un des VLAN pour l'authentification ouverte et l'autre VLAN pour l'authentification PEAP. Reportez-vous à Utilisation de VLAN avec l'équipement sans fil Cisco Aironet si vous voulez comprendre comment configurer des VLAN.

Notez que vous devez configurer vos commutateurs pour dot1Q et pour le routage entre VLAN, votre commutateur L3 ou votre routeur.

Q. Je veux configurer mon point d'accès Cisco 1200 VxWorks pour que les utilisateurs sans fil s'authentifient auprès d'un concentrateur VPN Cisco 3005. Quelle configuration doit être présente sur le point d'accès et les clients pour y parvenir ?

A. Aucune configuration spécifique n'est nécessaire sur le point d'accès ou les clients pour ce scénario. Vous devez effectuer toutes les configurations sur le concentrateur VPN.

Q. Je déploie un point d'accès Cisco 1232 AG. Je voudrais connaître la méthode la

plus sécurisée que je puisse déployer avec ce point d'accès. Je n'ai pas de serveur AAA et mes seules ressources sont l'AP et un domaine Windows 2003. Je sais comment utiliser des clés WEP 128 bits statiques, des restrictions sur les SSID et les adresses MAC sans diffusion. Les utilisateurs travaillent principalement avec les stations de travail Windows XP et certains assistants numériques personnels. Quelle est la mise en oeuvre la plus sécurisée pour cette configuration ?

A. Si vous n'avez pas de serveur RADIUS tel que Cisco ACS, vous pouvez configurer votre point d'accès en tant que serveur RADIUS local pour l'authentification LEAP, EAP-FAST ou MAC.

Remarque : Un point très important que vous devez prendre en considération est de savoir si vous voulez utiliser vos clients avec LEAP ou EAP-FAST. Si c'est le cas, vos clients doivent disposer d'un utilitaire pour prendre en charge LEAP ou EAP-FAST. L'utilitaire Windows XP prend uniquement en charge PEAP ou EAP-TLS.

Q. L'authentification PEAP échoue avec l'erreur « EAP-TLS ou l'authentification PEAP a échoué pendant la connexion SSL ». Pourquoi ?

A. Cette erreur peut se produire en raison de l'ID de bogue Cisco CSCee06008 **(clients enregistrés uniquement).** Le protocole PEAP échoue avec ADU 1.2.0.4. La solution de contournement de ce problème consiste à utiliser la dernière version de l'ADU.

Q. Puis-je avoir une authentification WPA et MAC locale sur le même SSID ?

A. Le point d'accès Cisco ne prend pas en charge l'authentification MAC locale et la clé de pré-partage WPA-PSK (Wi-Fi Protected Access Pre-Share Key) dans le même SSID (Service Set Identifier). Lorsque vous activez l'authentification MAC locale avec WPA-PSK, WPA-PSK ne fonctionne pas. Ce problème se produit car l'authentification MAC locale supprime de la configuration la ligne de mot de passe ASCII WPA-PSK.

Q. Nous avons actuellement trois points d'accès sans fil Cisco 1231 configurés avec le cryptage WEP 128 bits Ciphers pour notre VLAN de données. Nous ne diffusons pas le SSID. Nous n'avons pas de serveur RADIUS distinct dans notre environnement. Quelqu'un a pu déterminer la clé WEP à l'aide d'un outil d'analyse et l'a utilisé pendant deux semaines pour surveiller notre trafic sans fil. Comment éviter cela et sécuriser le réseau ?

A. Le protocole WEP statique est vulnérable à ce problème et peut être dérivé si un pirate capture suffisamment de paquets et est capable d'obtenir deux paquets ou plus avec le même vecteur d'initialisation (IV).

Il existe plusieurs façons d'empêcher que ce problème se produise :

1. Utilisez des clés WEP dynamiques.
2. Utilisez WPA.
3. Si vous n'avez que des adaptateurs Cisco, activez Per Packet Key et MIC.

Q. Si je dispose de deux WLAN différents, tous deux configurés pour Wi-Fi

Protected Access (WPA)-Pre-Shared Key (PSK), les clés pré-partagées peuvent-elles être différentes par WLAN ? Si elles sont différentes, cela affecte-t-il l'autre WLAN configuré avec une clé pré-partagée différente ?

A. Le paramètre WPA-PSK doit être défini par WLAN. Si vous modifiez un WPA-PSK, il ne doit pas affecter l'autre WLAN configuré.

Q. Dans mon environnement, j'utilise principalement Intel Pro/Wireless, Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) et Cisco Secure Access Control Server (ACS) 3.3 liés aux comptes Windows Active Directory (AD). Le problème est que lorsque le mot de passe utilisateur est sur le point d'expirer, Windows n'invite pas l'utilisateur à modifier le mot de passe. Finalement, le compte expire. Existe-t-il une solution permettant à Windows d'inviter l'utilisateur à modifier le mot de passe ?

A. La fonction de vieillissement des mots de passe Cisco Secure ACS vous permet de forcer les utilisateurs à modifier leurs mots de passe dans une ou plusieurs des conditions suivantes :

- Après un nombre de jours spécifié (règles d'âge par date)
- Après un nombre spécifié de connexions (règles d'âge par utilisation)
- Première connexion d'un nouvel utilisateur (règle de modification du mot de passe)

Pour plus d'informations sur la configuration de Cisco Secure ACS pour cette fonctionnalité, référez-vous à Activation du vieillissement des mots de passe pour la base de données utilisateur CiscoSecure.

Q. Lorsqu'un utilisateur se connecte sans fil à l'aide de LEAP, il obtient son script de connexion pour mapper les lecteurs réseau. Cependant, à l'aide de Wi-Fi Protected Access (WPA) ou WPA2 avec authentification PEAP, les scripts de connexion ne s'exécutent pas. Le client et le point d'accès sont tous deux Cisco, tout comme RADIUS (ACS). Pourquoi le script de connexion ne s'exécute-t-il pas sur RADIUS (ACS) ?

A. L'authentification de la machine est obligatoire pour que les scripts de connexion fonctionnent. Cela permet aux utilisateurs sans fil d'accéder au réseau pour charger des scripts avant que l'utilisateur ne se connecte.

Pour plus d'informations sur la configuration de l'authentification des machines avec PEAP-MS-CHAPv2, référez-vous à Configuration de Cisco Secure ACS pour Windows v3.2 avec l'authentification des machines PEAP-MS-CHAPv2.

Q. Avec Cisco Aironet Desktop Utility (ADU) version 3.0, lorsqu'un utilisateur configure l'authentification de la machine pour EAP-TLS (Extensible Authentication Protocol-Transport Layer Security), ADU ne permet pas à l'utilisateur de créer un profil. Pourquoi ?

A. Ceci est dû au bogue Cisco ID CSCsg32032 (clients enregistrés uniquement). Cela peut se produire si le certificat de machine est installé sur le PC client et qu'il n'y a pas de certificat utilisateur.

La solution de contournement consiste à copier le certificat de l'ordinateur dans le magasin d'utilisateurs, à créer un profil EAP-TLS, puis à supprimer le certificat du magasin d'utilisateurs pour la configuration de l'authentification de l'ordinateur uniquement.

Q. Existe-t-il un moyen d'attribuer le VLAN sur le LAN sans fil en fonction de l'adresse MAC du client ?

A. Non. Ce n'est pas possible. L'affectation de VLAN à partir du serveur RADIUS fonctionne uniquement avec 802.1x, et non avec l'authentification MAC. Vous pouvez utiliser RADIUS pour envoyer des VSA avec authentification MAC, si les adresses MAC sont authentifiées sur le serveur RADIUS (défini comme ID utilisateur/mot de passe dans LEAP/PEAP).

Informations connexes

- Sécurité du réseau sans fil
- Livre blanc sur la sécurité des LAN sans fil
- Présentation de la sécurité LAN sans fil
- Guide de déploiement EAP-TLS pour les réseaux LAN sans fil
- LEAP Cisco
- Configuration de WEP (Wired Equivalent Privacy)
- Assistance produit sans fil
- Support et documentation techniques - Cisco Systems