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 sécurité sans fil ?

A. Dans un réseau câblé, les données demeurent dans les câbles qui connectent les périphériques d'extrémité. Mais les réseaux Sans fil transmettent et reçoivent des données par une émission des signaux rf dans l'air ouvert. En raison de la nature d'émission qui utilisation WLAN, il y a une plus grande menace des pirates informatiques ou des intrus qui peuvent accéder à ou corrompent les données. Afin d'alléger ce problème, tous les WLAN exigent l'ajout de :

1. Authentification de l'utilisateur pour empêcher l'accès non autorisé aux ressources de réseau.
2. Confidentialité des données pour protéger l'intégrité et l'intimité des données transmises (également connues sous le nom de cryptage).

Q. Quelles sont les différentes méthodes d'authentification que la norme de 802.11 pour des réseaux locaux Sans fil définit ?

A. La norme de 802.11 définit deux mécanismes pour l'authentification des clients Sans fil de RÉSEAU LOCAL :

1. Ouvrez l'authentification
2. Authentification principale partagée

Il y a deux autres mécanismes utilisés généralement aussi bien :

1. authentification basée sur SSID
2. Authentification d'adresse MAC

Q. Quelle est authentification ouverte ?

A. L'authentification ouverte est fondamentalement un algorithme nul d'authentification, ainsi il signifie qu'il n'y a aucune vérification de l'utilisateur ou de l'ordinateur. L'authentification ouverte permet n'importe quel périphérique qui place une demande d'authentification au Point d'accès (AP). L'authentification ouverte emploie la transmission de libellé pour permettre à un client pour s'associer à AP. Si aucun cryptage n'est activé, n'importe quel périphérique qui connaît le SSID du WLAN peut accéder dans le réseau. Si le Confidentialité équivalente aux transmissions par fil (WEP) est activé sur AP, la clé WEP devient des moyens de contrôle d'accès. Un périphérique qui n'a pas la clé WEP correcte ne peut pas transmettre des données par AP même si l'authentification est réussie. Ni l'un ni l'autre ne peuvent des telles données de déchiffrage de périphérique qu'AP envoie.

Q. Quelles étapes est-ce qu'authentification ouverte implique pour qu'un client s'associe avec AP ?

1. Le client envoie une demande de sonde aux aps.
2. Les aps renvoient des réponses de sonde.
3. Le client évalue les réponses AP et sélectionne meilleur AP.
4. Le client envoie une demande d'authentification à AP.
5. AP confirme l'authentification et enregistre le client.
6. Le client envoie alors une demande d'association à AP.
7. AP confirme l'association et enregistre le client.

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

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

Avantages : L'authentification ouverte est un mécanisme d'authentification de base, que vous pouvez utiliser avec les périphériques sans fil qui ne prennent en charge pas les algorithmes complexes d'authentification. L'authentification dans la spécification de 802.11 est orientée Connectivité. Par conception les conditions requises pour l'authentification permettent à des périphériques pour gagner à accès rapide au réseau. En pareil cas, vous pouvez utiliser l'authentification ouverte.

Inconvénients : L'authentification ouverte ne fournit aucune manière de vérifier si un client est un client valide et pas un client de pirate informatique. Si vous n'utilisez pas le cryptage WEP avec l'authentification ouverte, n'importe quel utilisateur qui connaît le SSID du WLAN peut accéder au réseau.

Q. Quelle est authentification principale partagée ?

A. L'authentification principale partagée fonctionne semblable pour ouvrir l'authentification avec une difference majeure. Quand vous utilisez l'authentification ouverte avec la clé de chiffrement WEP, la clé WEP est utilisée pour chiffrer et déchiffrer les données, mais n'est pas utilisée dans l'étape d'authentification. Dans l'authentification principale partagée, le cryptage WEP est utilisé pour l'authentification. Comme l'authentification ouverte, l'authentification principale partagée exige du client et de l'AP d'avoir la même clé WEP. AP qui utilise l'authentification principale partagée envoie un paquet de texte de défi au client. Le client emploie la clé WEP localement configurée pour chiffrer le texte de défi et pour répondre avec une demande d'authentification

ultérieure. Si AP peut déchiffrer la demande d'authentification et récupérer le texte de défi d'origine, AP répond avec une réponse d'authentification qui accorde l'accès au client.

Q. Quelles étapes est-ce que l'authentification principale partagée implique-t-elle pour qu'un client associe avec AP ?

1. Le client envoie une demande de sonde aux aps.
2. Les aps renvoient des réponses de sonde.
3. Le client évalue les réponses AP et sélectionne meilleur AP.
4. Le client envoie une demande d'authentification à AP.
5. AP envoie une réponse d'authentification qui contient le texte de défi décrypté.
6. Le client chiffre le texte de défi avec la clé WEP et envoie le texte à AP.
7. AP compare le texte de défi décrypté au texte de défi chiffré. Si l'authentification peut déchiffrer et récupérer le texte de défi d'origine, l'authentification est réussie.

L'authentification principale partagée utilise le cryptage WEP pendant le processus d'association de client.

Q. Quels sont les avantages et les inconvénients Shared introduisent-ils l'authentification ?

A. Dans l'authentification principale partagée, le client et l'AP permutent le texte de défi (texte clair) et le défi chiffré. Par conséquent, ce type d'authentification est vulnérable à l'attaque homme-dans-le-moyenne. Un pirate informatique peut écouter le défi décrypté et le défi chiffré, et extrait la clé WEP (clé partagée) de ces informations. Quand un pirate informatique connaît la clé WEP, le mécanisme d'authentification entier est compromis et le pirate informatique peut accéder au réseau WLAN. C'est le principal inconvénient avec l'authentification principale partagée.

Q. Quelle est authentification d'adresse MAC ?

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

Dans l'authentification d'adresse MAC, des clients sont authentifiés ont basé sur leur adresse MAC que les adresses MAC des clients sont vérifiées contre une liste d'adresses MAC ont enregistré localement sur AP ou sur un serveur d'authentification externe. L'authentification MAC est un mécanisme de sécurité accrue que les authentifications principales ouvertes et partagées que le 802.11 fournit. Cette forme d'authentification autre réduit la probabilité des périphériques non autorisés qui peuvent accéder au réseau.

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

A. Le seul niveau de sécurité pour l'authentification MAC est de vérifier l'adresse MAC du client contre une liste d'adresses MAC permises. Ceci est considéré très faible. Dans des versions logicielles plus tôt de Cisco IOS, vous pourriez configurer l'authentification MAC et le WPA pour chiffrer les informations. Mais parce que WPA lui-même a une adresse MAC qui vérifie, Cisco a décidé de ne pas permettre ce type de configuration dans de plus défuntes versions logicielles de

Cisco IOS et décidée pour améliorer seulement des fonctionnalités de sécurité.

Q. Est-ce que je peux employer le SSID comme méthode pour authentifier des périphériques sans fil ?

A. L'Identifiant SSID (Service Set Identifier) est une seule, distinguant majuscules et minuscules, alphanumérique valeur que les WLAN utilisent comme nom de réseau. Le SSID est a - le mécanisme qui permet la séparation logique des réseaux locaux Sans fil. Le SSID ne fournit aucune fonction de confidentialité des données, ni le SSID authentifie vraiment le client à AP. La valeur SSID est émission en tant que texte clair dans les balises, les réponses de demandes de sonde, de sonde, et d'autres types de trames. Une oreille indiscrète peut facilement déterminer le SSID avec l'utilisation d'un analyseur Sans fil de paquet de RÉSEAU LOCAL de 802.11, par exemple, renifleur pro. Cisco ne recommande pas que vous employiez le SSID comme méthode pour sécuriser votre réseau WLAN.

Q. Si je désactive la diffusion SSID, est-ce que je peux réaliser la sécurité optimisée sur un réseau WLAN ?

A. Quand vous désactivez la diffusion SSID, le SSID n'est pas introduit des messages de balise. Cependant, d'autres trames comme, demandes de sonde et réponses de sonde ont toujours le SSID en texte clair. Ainsi vous ne réalisez pas la Sécurité Sans fil améliorée si vous désactivez le SSID. Le SSID n'est pas conçu, ni est destiné pour l'usage, comme mécanisme de sécurité. En outre, si vous désactivez des diffusions SSID, vous pouvez rencontrer des problèmes avec l'Interopérabilité de WiFi pour des déploiements de mélangé-client. Par conséquent, Cisco ne recommande pas que vous utilisiez le SSID comme mode de Sécurité.

Q. Quelles sont les vulnérabilités trouvées dans la Sécurité de 802.11 ?

A. Les principales vulnérabilités de la Sécurité de 802.11 peuvent être récapitulées comme suit :

- Authentification réservée au périphérique faible : Des périphériques de client ne sont authentifiés, pas des utilisateurs.
- Chiffrement de données faible : Le Confidentialité équivalente aux transmissions par fil (WEP) a été inefficace prouvé en tant que des moyens de chiffrer des données.
- Aucune intégrité des messages : La valeur de contrôle d'intégrité (ICV) a été inefficace prouvé en tant que des moyens d'assurer l'intégrité des messages.

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

A. Afin d'adresser les défauts et les failles de la sécurité dans les méthodes d'authentification d'origine que la norme de 802.11 définit, le cadre d'authentification de 802.1X est inclus dans l'ébauche pour des améliorations de la sécurité de couche de MAC de 802.11. Le groupe de travail d'IEEE 802.11 i (TGi) développe actuellement ces améliorations. Le cadre de 802.1X fournit à la couche de liaison l'authentification extensible, normalement vue seulement dans les couches plus élevées.

Q. Quelles sont les trois entités que le cadre de 802.1x définit ?

A. le cadre de 802.1x exige de ces trois entités logiques de valider les périphériques sur un

réseau WLAN.

1. **Suppliant** — Le suppliant réside sur le client Sans fil de RÉSEAU LOCAL, et est également connu en tant que client d'EAP.
2. **Authentificateur** — L'authentificateur réside sur AP.
3. **Serveur d'authentification** — Le serveur d'authentification réside sur le serveur de RAYON.

Q. Comment est-ce qu'une authentification de client sans fil se produit quand j'utilise le cadre d'authentification de 802.1x ?

A. Quand le client sans fil (client d'EAP) devient actif, le client sans fil authentifie avec l'authentification ouverte ou partagée. le 802.1x fonctionne avec l'authentification et les débuts ouverts après que le client s'associe avec succès à AP. La station client peut s'associer, mais peut passer le trafic de données seulement après l'authentification réussie de 802.1x. Voici les étapes dans l'authentification de 802.1x :

1. AP (authentificateur) configuré pour le 802.1x demande l'identité de l'utilisateur du client.
2. Les clients répondent avec son identité au cours d'un délai prévu stipulé.
3. Le serveur vérifie l'identité de l'utilisateur et commence l'authentification par le client si l'identité de l'utilisateur est présente dans sa base de données.
4. Le serveur envoie un message de succès à AP.
5. Une fois que le client est authentifié, le serveur en avant que la clé de chiffrement à AP qui est le trafic utilisé de to encrypt/decrypt a envoyé à et du client.
6. Dans l'étape 4, si l'identité de l'utilisateur n'est pas présente dans la base de données, le serveur relâche l'authentification et envoie un message d'échec à AP.
7. AP en avant ce message au client, et le client doivent authentifier de nouveau avec les qualifications correctes.

Remarque: Dans toute l'authentification de 802.1x, AP juste en avant les messages d'authentification à et du client.

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

A. le 802.1x définit la procédure pour authentifier des clients. Le type d'EAP utilisé dans le cadre de 802.1x définit le type de qualifications et la méthode d'authentification utilisée dans l'échange de 802.1x. Le cadre de 802.1x peut utiliser l'un de ces variantes d'EAP :

- EAP-TLS — Transport Layer Security d'Extensible Authentication Protocol
- EAP-FAST — Authentification flexible d'EAP par l'intermédiaire de tunnel sécurisé
- EAP-SIM — SIM d'EAP
- Cisco SAUTENT — Lightweight Extensible Authentication Protocol
- EAP-PEAP — Protected Extensible Authentication Protocol d'EAP
- EAP-MD5 — EAP – Algorithme 5 de condensé de message
- EAP-OTP — Mot de passe de période active d'EAP
- EAP-TTLS — Transport Layer Security percé un tunnel par EAP

Q. Comment est-ce que je choisis une méthode d'EAP de 802.1x des différentes variantes disponibles ?

A. Le facteur le plus important que vous devez considérer est, que la méthode d'EAP soit compatible avec le réseau existant ou pas. En outre, Cisco recommande que vous choisissiez une méthode qui prend en charge l'authentification mutuelle.

Q. Qu'est authentification EAP locale ?

A. L'EAP local est un mécanisme dans lequel le WLC agit en tant que serveur d'authentification. Des identifiants utilisateurs sont enregistrés localement sur le WLC pour authentifier des clients sans fil, qui agit en tant que processus principal dans les bureaux distants quand le serveur descend. Des identifiants utilisateurs peuvent être récupérés de la base de données locale sur le WLC ou d'un serveur LDAP externe. Le LEAP, l'EAP-FAST, l'EAP-TLS, les PEAPv0/MSCHAPv2, et les PEAPv1/GTC sont différentes authentifications EAP prises en charge par EAP local.

Q. Quel est LEAP de Cisco ?

A. Le Lightweight Extensible Authentication Protocol (LEAP) est une méthode d'authentification de classe des propriétaires de Cisco. Cisco SAUTENT est un type d'authentification de 802.1X pour les réseaux locaux Sans fil (WLAN). Cisco SAUTENT l'authentification mutuelle forte de supports entre le client et un serveur de RAYON par un mot de passe de connexion comme secret partagé. Cisco SAUTENT fournit le par-utilisateur dynamique, des clés de chiffrement de par-session. Le LEAP est la moins méthode compliquée pour déployer le 802.1x, et exige seulement un serveur de RAYON. Référez-vous au LEAP de Cisco pour les informations sur le LEAP.

Q. Comment l'EAP-FAST fonctionne-t-il ?

A. L'EAP-FAST emploie les algorithmes principaux symétriques pour réaliser une procédure d'authentification percée un tunnel. L'établissement de tunnel se fonde sur un laisser-passer de Protected Access (PAC) que cet EAP-FAST peut provisioned et géré dynamiquement par EAP-FAST par le serveur d'Authentification, autorisation et comptabilité (AAA) (tel que le Cisco Secure Access Control Server [ACS] V. 3.2.3). Avec un tunnel mutuellement authentifié, l'EAP-FAST offre la protection contre des attaques par dictionnaire et des vulnérabilités homme-dans-le-moyennes. Voici les phases de l'EAP-FAST :

L'EAP-FAST atténue non seulement des risques des attaques par dictionnaire passives et des attaques homme-dans-le-moyennes, mais également les enables sécurisent l'authentification basée sur l'infrastructure actuellement déployée.

- Phase 1 : Établissez le tunnel mutuellement authentifié — Le client et le serveur d'AAA emploient le PAC pour s'authentifier et pour établir un tunnel sécurisé.
- Phase 2 : Exécutez l'authentification 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 de client.
- Sur option, phase 0 — L'authentification d'EAP-FAST emploie rarement cette phase pour permettre au client de provisioned dynamiquement avec un PAC. Cette phase génère un laisser-passer d'accès de par-utilisateur sécurisé entre l'utilisateur et le réseau. Le Phase 1 de l'authentification utilise ce laisser-passer de par-utilisateur, connu sous le nom de PAC.

Référez-vous au pour en savoir plus d'EAP-FAST de Cisco.

Q. Y a-t-il des documents sur cisco.com qui expliquent comment configurer l'EAP dans un réseau de WLAN Cisco ?

A. Référez-vous à l'authentification EAP avec le serveur de RAYON pour les informations sur la façon dont configurer l'authentification EAP dans un réseau WLAN.

Référez-vous à la note d'application protégée en EAP pour les informations sur la façon dont configurer l'authentification PEAP.

Référez-vous à l'authentification de LEAP avec un serveur local de RAYON pour les informations sur la façon dont configurer l'authentification de LEAP.

Q. Quels sont les différents mécanismes de chiffrement les plus utilisés généralement dans les réseaux Sans fil ?

A. Voici les structures de chiffrement les plus utilisées généralement utilisées dans les réseaux Sans fil :

- WEP
- TKIP
- AES

AES est une méthode de chiffrement matériel, tandis que le cryptage WEP et TKIP est traité sur le micrologiciel. Avec la mise à jour du firmware un WEP les périphériques peuvent prendre en charge le TKIP ainsi ils sont interopérables. AES est la méthode sécurisée et la plus rapide de la plupart, tandis que le WEP est le mineur sécurisé.

Q. Quel est cryptage WEP ?

A. Le WEP signifie Wired Equivalent Privacy. Le 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. Pendant que la norme spécifie, le WEP utilise l'algorithme RC4 avec une clé 40-bit ou 104-bit. RC4 est un algorithme symétrique, parce que RC4 utilise la même clé pour le cryptage et le décryptage des données. Quand le WEP est activé, chaque « station » par radio a 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 configurer le Confidentialité équivalente aux transmissions par fil (WEP) pour les informations sur la façon dont configurer le WEP.

Q. Quelle est rotation de clé d'émission ? Quelle est la fréquence de la rotation de clé d'émission ?

A. La rotation principale d'émission permet à AP pour générer la meilleure clé aléatoire de groupe. Annoncez la rotation principale met à jour périodiquement tous les clients capables de la gestion des clés. Quand vous activez la rotation de clé WEP d'émission, AP fournit une clé WEP dynamique d'émission et change la clé à l'intervalle que vous placez. La rotation principale d'émission est une excellente alternative au TKIP si votre RÉSEAU LOCAL Sans fil prend en charge les périphériques de client sans fil de non-Cisco ou les périphériques que vous ne pouvez pas améliorer au dernier micrologiciel pour des périphériques de client de Cisco. Référez-vous à activer et à désactiver la rotation principale d'émission pour les informations sur la façon dont configurer la caractéristique de rotation de clé d'émission.

Q. Quel est TKIP ?

A. Le TKIP signifie le Temporal Key Integrity Protocol. Le TKIP a été introduit pour adresser les défauts dans le cryptage WEP. Le TKIP est également connu comme hachage de clé WEP et s'est au commencement appelé le WEP2. Le TKIP est une solution provisoire qui répare le problème de réutilisation de clé WEP. Le TKIP emploie l'algorithme RC4 pour exécuter le cryptage, qui est identique que le WEP. Une difference majeure de WEP est que le TKIP change la clé temporelle chaque paquet. Les modifications principales temporelles chaque paquet parce que la valeur de hachage pour chaque paquet change.

Q. Les périphériques qu'utilisez le TKIP peuvent-ils interopèrent avec les périphériques qui utilisent le cryptage WEP ?

A. Un avantage avec le TKIP est que les WLAN avec des aps basés sur WEP existants et des radios peuvent améliorer au TKIP par les correctifs simples de micrologiciel. En outre, le matériel réservé à la WEP interopère toujours avec les périphériques TKIP-activés qui utilisent le WEP.

Q. Quel est le Message Integrity Check (MIC) ?

A. La MIC est encore une autre amélioration pour adresser les vulnérabilités dans le cryptage WEP. La MIC empêche des attaques de bit-secousse sur les paquets chiffrés. Pendant une attaque de bit-secousse, un intrus intercepte un message crypté, modifie le message et puis retransmet le message modifié. Le récepteur ne sait pas que le message est corrompu et pas légitime. Afin d'aborder cette question, la caractéristique MIC ajoute un champ MIC à la trame Sans fil. Le champ MIC fournit un contrôle d'intégrité de trame qui n'est pas vulnérable aux mêmes défauts mathématiques que l'ICV. La MIC ajoute également un gisement de numéro de séquence à la trame Sans fil. AP relâche des trames a reçu en panne.

Q. Quel est WPA ? Comment le WPA2 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. Le WPA adresse toutes les vulnérabilités connues de Confidentialité équivalente aux transmissions par fil (WEP) dans la mise en œuvre d'un système de sécurité d'origine d'IEEE 802.11 et apporte une solution de sécurité immédiate aux réseaux WLAN dans l'entreprise et le petit bureau, des environnements du bureau à domicile (SOHO).

Le WPA2 est la nouvelle génération de sécurité wifi. Le WPA2 est l'implémentation interopérable de Wi-Fi Alliance de la norme ratifiée d'IEEE 802.11i. Le WPA2 implémente le National Institute of Standards and Technology (NIST) - algorithme de chiffrement recommandé de Norme AES (Advanced Encryption Standard) avec l'utilisation du contre- mode avec le Cipher Block Chaining Message Authentication Code Protocol (CCMP). 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 supérieur de Sécurité que le WPA. Le WPA2 crée des clés de session fraîches sur chaque association. Les clés de chiffrement que le WPA2 utilise pour chaque client sur le réseau sont seules 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 quelques Points d'accès et quelques clients limitent les combinaisons, mais là sont quatre combinaisons possibles). La différence entre WPA1 et WPA2 est dans les éléments d'information qui obtiennent

mis dans les balises, les trames d'association, et les trames de la prise de contact 4-way. Les données dans ces éléments d'information sont fondamentalement identique, mais l'identifiant utilisé est différent. La principale différence dans la prise de contact principale est que le WPA2 inclut la clé initiale de groupe dans la prise de contact 4-way et la prise de contact principale du premier groupe est ignorée, tandis que le WPA doit faire cette prise de contact supplémentaire pour fournir les clés initiales de groupe. La nouvelle saisie de la clé de groupe se produit de la même manière. La prise de contact se produit avant la sélection et l'utilisation de la suite de chiffrement (TKIP ou AES) pour la transmission des datagrammes d'utilisateur. Pendant la prise de contact WPA1 ou WPA2, la suite de chiffrement à l'utiliser est déterminée. Une fois que sélectionnée, la suite de chiffrement est utilisée pour tout le trafic d'utilisateur. Ainsi WPA1 plus AES n'est pas WPA2. WPA1 tient compte de (mais est souvent côté client limité) le chiffrement TKIP ou AES.

Q. Quel est AES ?

A. AES signifie l'Advanced Encryption Standard. AES offre beaucoup de chiffrement plus fort. AES utilise l'algorithme de Rijndael, qui est un chiffre par bloc avec 128-, 192-, et support de la clé 256-bit et est beaucoup plus fort que le RC4. Pour que les périphériques WLAN prennent en charge AES, le matériel doit prendre en charge AES au lieu du WEP.

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

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

- Password Authentication Protocol (PAP)
- Shiva protocole d'identification de mot de passe (SPAP)
- Protocole d'authentification CHAP (Challenge Handshake Authentication Protocol)
- Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
- Version 2 (MS-CHAP v2) de Microsoft Challenge Handshake Authentication Protocol
- CHAP de Digest 5 de Protocol-message d'authentification extensible (CHAP EAP-MD5)
- EAP-Transport Layer Security (EAP-TLS)
- EAP-MS-CHAP protégé v2 (PEAP-MS-CHAP v2) (également connu sous le nom de PEAPv0/EAP-MSCHAPv2)

PEAP-TLS IAS dans le Windows 2000 Server prend en charge PEAP-MS-CHAP v2 et PEAP-TLS quand le Service Pack 4 de Windows 2000 Server est installé. Le pour en savoir plus, se rapportent à des méthodes d'authentification pour l'usage avec IAS .

Q. Comment le VPN est-il mis en application dans un envrionment Sans fil ?

A. Le VPN est un mécanisme de sécurité de la couche 3 ; des mécanismes de chiffrement sans fil sont mis en application à la couche 2. VPN est mis en application au-dessus du 802.1x, de l'EAP, du WEP, du TKIP, et de l'AES. Quand un mécanisme de la couche 2 est en place, le VPN ajoute au-dessus à l'implémentation. Dans les endroits comme des hotspots publics et des hôtels où aucune Sécurité n'est mise en application, le VPN serait une solution utile à implémenter.

Foire aux questions de dépannage et de conception

Q. Y a-t-il des pratiques recommandées de déployer la Sécurité Sans fil dans un

RÉSEAU LOCAL de Technologie sans fil d'extérieur ?

A. Référez-vous aux pratiques recommandées pour le degré de sécurité de Technologie sans fil d'extérieur. Ce document fournit des informations sur des pratiques recommandées de Sécurité de déployer un RÉSEAU LOCAL de Technologie sans fil d'extérieur.

Q. Est-ce que je peux utiliser le Windows 2000 ou le serveur 2003 avec le Répertoire actif pour qu'un serveur de RAYON authentifie des clients sans fil ?

A. Le Windows 2000 ou le serveur 2003 avec un répertoire actif peut fonctionner en tant que serveur de RAYON. Pour les informations sur la façon dont configurer ce serveur de RAYON, vous devez contacter Microsoft, parce que Cisco ne prend en charge pas la configuration du serveur de fenêtres.

Q. Mon site est sur le point de migrer d'un réseau Sans fil ouvert (gammes 350 et 1200 aps) vers un réseau PEAP. Je voudrais avoir le SSID OUVERT (un SSID configuré pour l'authentification Open) et le travail PEAP SSID (un SSID configuré pour l'authentification PEAP) sur même AP en même temps. Ceci nous donne l'heure de migrer les clients vers le PEAP SSID. Y a-t-il une manière de héberger simultanément un SSID ouvert et un PEAP SSID sur même AP ?

A. Le support VLAN (couche 2 de Cisco aps seulement). C'est réellement la seule manière de réaliser ce que vous voulez faire. Vous devez créer deux VLAN, (indigène et votre autre VLAN). Alors vous ne pouvez avoir une clé WEP pour une et aucune clé WEP pour des autres. De cette façon, vous pouvez configurer un des VLAN pour l'authentification Open et de l'autre VLAN pour l'authentification PEAP. Référez-vous en utilisant des VLAN avec l'équipement sans fil de Cisco Aironet si vous voulez comprendre comment configurer des VLAN.

Veuillez noter que vous devez configurer vos Commutateurs pour dot1Q et pour le routage inter VLAN, votre commutateur L3 ou votre routeur.

Q. Je veux installer mon Cisco AP 1200 VxWorks pour faire authentifier aux utilisateurs de sans fil à Cisco 3005 VPN un concentrateur. Quelle configuration doit être présente sur AP et les clients pour accomplir ceci ?

A. Il n'y a aucune configuration spécifique nécessaire sur AP ou les clients pour ce scénario. Vous devez faire tout les configurations sur le concentrateur VPN.

Q. Je déploie un AG AP de Cisco 1232. Je voudrais connaître les la plupart méthode sécurisée que je peux me déployer avec cet AP. Je n'ai pas un serveur d'AAA et mes seulement ressources sont AP et un domaine de Windows 2003. Je suis familiarisé avec la façon utiliser des clés 128-bit WEP, la non-émission SSID et des restrictions statiques d'adresse MAC. Les utilisateurs travaillent en grande partie avec des postes de travail de Windows Xp et quelques PDA. Quelles sont les la plupart implémentation sécurisée pour cette installation ?

A. Si vous n'avez pas un serveur de RAYON comme Cisco ACS, vous pouvez configurer votre AP en tant que serveur local de RAYON pour le LEAP, l'EAP-FAST ou l'authentification MAC.

Remarque: Très un point important que vous devez considérer est si vous voulez utiliser vos clients avec le LEAP ou l'EAP-FAST. Si oui, vos clients doivent avoir un utilitaire pour prendre en charge le LEAP ou l'EAP-FAST. L'utilitaire de Windows XP prend en charge seulement le PEAP ou l'EAP-TLS.

Q. L'authentification PEAP échoue avec l'erreur « échec de l'authentification d'EAP-TLS ou PEAP pendant la prise de contact SSL ». Pourquoi ?

A. Cette erreur peut se produire en raison de l'ID de bogue Cisco CSCee06008 (clients enregistrés seulement). Le PEAP échoue avec ADU 1.2.0.4. Le contournement pour ce problème est d'utiliser la dernière version de l'ADU.

Q. Est-ce que je peux avoir le WPA et l'authentification MAC locale sur le même SSID ?

A. Cisco AP clé ne prend en charge pas Pré-partage local d'authentification MAC et d'accès protégé par Wi-Fi (WPA-PSK) dans le même Identifiant SSID (Service Set Identifier). Quand vous activez l'authentification MAC locale avec le WPA-PSK, le WPA-PSK ne fonctionne pas. Ce problème se pose parce que l'authentification MAC locale retire la ligne de mot de passe du WPA-PSK ASCII de la configuration.

Q. Nous avons actuellement trois Cisco 1231 aps Sans fil installés avec le cryptage WEP des chiffrements 128-bit pour nos données VLAN. Nous n'annonçons pas le SSID. Nous n'avons pas un serveur distinct de RAYON dans notre environnement. Quelqu'un pouvait déterminer la clé WEP par un outil de lecture, et a utilisé l'outil pendant quelques semaines pour surveiller notre trafic Sans fil. Comment pouvons-nous empêcher ceci et rendre le réseau sécurisé ?

A. Le WEP statique est vulnérable à cette question, et peut être dérivé si un pirate informatique capture assez de paquets et peut obtenir deux paquets ou plus avec le même vecteur d'initialisation (iv).

Il y a plusieurs manières d'empêcher l'occurrence de cette question :

1. Clés WEP dynamiques d'utilisation.
2. Utilisation WPA.
3. Si vous avez seulement des adaptateurs de Cisco, activez par clé de paquet et MIC.

Q. Si j'ai deux WLAN différents, est-ce que chacun des deux ont configuré pour le Protocole WPA (Wi-Fi Protected Access) - la clé pré-partagée (PSK), les clés pré-partagées peuvent-elles être différentes par WLAN ? S'ils sont différents, affecte-t-il l'autre WLAN configuré avec une clé pré-partagée différente ?

A. La configuration du WPA-PSK devrait être par WLAN. Si vous changez un WPA-PSK, il ne devrait pas affecter l'autre WLAN qui est configuré.

Q. Dans mon environnement j'utilise en grande partie Intel pro/radio, authentification Protocol-flexible d'authentification extensible par l'intermédiaire du Tunnellisation

sécurisé (EAP-FAST), et Cisco Secure Access Control Server (ACS) 3.3 liés aux comptes de Répertoire actif de Windows (AD). Le problème est quand le mot de passe utilisateur est sur le point d'expirer, Windows n'incite pas l'utilisateur à changer le mot de passe. Par la suite, le compte expire. Y a-t-il une solution pour inciter à demande de Windows l'utilisateur pour changer le mot de passe ?

A. La caractéristique vieillissante de mot de passe de Cisco Secure ACS te permet de forcer des utilisateurs pour changer leurs mots de passe dans un ou plusieurs de ces conditions :

- Après un nombre spécifié de jours (règles d'âge-par-date)
- Après un nombre spécifié de procédures de connexion (règles d'âge-par-utilisations)
- La première fois qu'un nouvel utilisateur ouvre une session (la règle de modification de mot de passe)

Pour des détails sur la façon dont configurer le Cisco Secure ACS pour cette caractéristique, référez-vous à activer le vieillissement de mot de passe pour la base de données utilisateur de CiscoSecure.

Q. Quand un utilisateur ouvre une session sans fil utilisant le LEAP ils obtiennent leur script de connexion pour tracer des lecteurs réseau. Cependant, utilisant le Protocole WPA (Wi-Fi Protected Access) ou le WPA2 avec l'authentification PEAP, les scripts de connexion ne fonctionnent pas. Le client et le Point d'accès sont Cisco de même que le RAYON (ACS). Pourquoi le script de connexion ne fonctionne-t-il pas sur le RAYON (ACS) ?

A. Il est obligatoire pour que les scripts de connexion fonctionnent authentification de machine. Ceci permet aux utilisateurs de sans fil de gagner l'accès au réseau pour charger des scripts avant les logins d'utilisateur.

Pour les informations sur la façon dont configurer l'authentification de machine avec PEAP-MS-CHAPv2, référez-vous à configurer le Cisco Secure ACS pour Windows v3.2 avec l'authentification de machine PEAP-MS-CHAPv2.

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

A. C'est en raison de l'ID de bogue Cisco CSCsg32032 (clients enregistrés seulement). Ceci peut se produire si le PC client a le certificat d'ordinateur installé et n'a pas un certificat utilisateur.

Le contournement est de copier le certificat d'ordinateur sur la mémoire d'utilisateur, crée un profil d'EAP-TLS et puis retire le certificat de la mémoire d'utilisateur pour la configuration d'authentification de machine seulement.

Q. Y a-t-il une manière d'assigner le VLAN sur le RÉSEAU LOCAL Sans fil basé sur l'adresse MAC du client ?

A. Non. Ce n'est pas possible. L'affectation VLAN du serveur de RAYON fonctionne seulement

avec le 802.1x, pas authentification MAC. Vous pouvez employer le RAYON pour pousser les VSAs avec l'authentification MAC, si les adresses MAC sont authentifiées au serveur de RAYON (défini comme ID utilisateur/mot de passe dans LEAP/PEAP).

Informations connexes

- Sécurité des réseaux sans fils
- Livre Blanc Sans fil de Sécurité LAN
- Aperçu Sans fil de Sécurité LAN
- Guide de déploiement d'EAP-TLS pour des réseaux LAN sans fil
- Cisco SAUTENT
- Configurer le Confidentialité équivalente aux transmissions par fil (WEP)
- Assistance produit sans fil
- Support et documentation techniques - Cisco Systems