FAQ na segurança Wireless do Cisco Aironet

Índice

Introdução

Este documento fornece informações sobre as perguntas mais frequentes (FAQ) sobre segurança wireless do Cisco Aironet.

Perguntas Frequentes Gerais

Q. Que é a necessidade para a segurança Wireless?

A. Em uma rede ligada com fio, os dados permanecem nos cabos que conectam os dispositivos finais. Mas as redes Wireless transmitem e recebem dados com uma transmissão de sinais RF no ar aberto. Devido à natureza da transmissão que uso WLAN, há uma ameaça de hackers maior ou os intrusos que possam alcançar ou corromper os dados. A fim aliviar este problema, todos os WLAN exigem a adição de:

1. Autenticação de usuário para impedir o acesso não autorizado aos recursos de rede.
2. Privacidade de dados para proteger a integridade e a privacidade dos dados transmitidos (igualmente conhecidos como a criptografia).

Q. Que são os métodos de autenticação diferentes que o padrão do 802.11 para o Sem fio LAN define?

A. O padrão do 802.11 define dois mecanismos de autenticação de clientes do Wireless LAN:

1. Autenticação aberta
2. Autenticação de chave compartilhada

Há outros dois mecanismos de uso geral também:

1. autenticação SSID-baseada
2. Autenticação do MAC address

Q. Que é autenticação aberta?

A. A autenticação aberta é basicamente um algoritmo da autenticação nula, assim que significa

que não há nenhuma verificação do usuário ou da máquina. A autenticação aberta permite todo o dispositivo que colocar um pedido de autenticação ao Access Point (AP). A autenticação aberta usa a transmissão da minuta para permitir que um cliente associe a um AP. Se o no encryption é permitido, todo o dispositivo que conhecer o SSID do WLAN pode aceder na rede. Se o Wired Equivalent Privacy (WEP) é permitido no AP, a chave de WEP torna-se meios do controle de acesso. Um dispositivo que não tenha a chave de WEP correta não pode transmitir dados com o AP mesmo se a autenticação é bem sucedida. Nenhuns podem tais dados do decrypt do dispositivo que o AP envia.

Q. Que etapas a autenticação aberta envolve para que um cliente associe com o AP?

1. O cliente envia um pedido da ponta de prova aos AP.
2. Os AP enviam para trás respostas da ponta de prova.
3. O cliente avalia as respostas AP e seleciona o melhor AP.
4. O cliente envia um pedido de autenticação ao AP.
5. O AP confirma a autenticação e registra o cliente.
6. O cliente envia então um pedido da associação ao AP.
7. O AP confirma a associação e registra o cliente.

Q. Que são as vantagens e desvantagem da autenticação aberta?

A. Estão aqui as vantagens e desvantagem da autenticação aberta:

Vantagens: A autenticação aberta é um mecanismo de autenticação básica, que você possa usar com dispositivos Wireless que não apoiam os algoritmos de autenticação complexos. A autenticação na especificação do 802.11 Conectividade-é orientada. Pelo projeto os requisitos de autenticação permitem que os dispositivos ganhem o acesso rápido à rede. Em tal caso, você pode usar a autenticação aberta.

Desvantagens: A autenticação aberta não fornece nenhuma maneira de verificar se um cliente é um cliente válido e não um cliente hacker. Se você não usa a criptografia de WEP com autenticação aberta, todo o usuário que conhecer o SSID do WLAN pode alcançar a rede.

Q. Que é autenticação de chave compartilhada?

A. A autenticação de chave compartilhada trabalha similar à autenticação aberta com uma diferença principal. Quando você usa a autenticação aberta com chave de criptografia de WEP, a chave de WEP está usada para cifrar e decifrar os dados, mas não usada na etapa da autenticação. Na autenticação de chave compartilhada, a criptografia de WEP é usada para a autenticação. Como a autenticação aberta, a autenticação de chave compartilhada exige o cliente e o AP ter a mesma chave de WEP. O AP que usa a autenticação de chave compartilhada envia um pacote de texto de desafio ao cliente. O cliente usa a chave de WEP localmente configurada para cifrar o texto de desafio e para responder com um pedido da autenticação subsequente. Se o AP pode decifrar o pedido de autenticação e recuperar o texto de desafio original, o AP responde com uma resposta de autenticação que conceda o acesso ao cliente.

Q. Que etapas a autenticação de chave compartilhada envolve para que um cliente associe com o AP?

1. O cliente envia um pedido da ponta de prova aos AP.
2. Os AP enviam para trás respostas da ponta de prova.
3. O cliente avalia as respostas AP e seleciona o melhor AP.
4. O cliente envia um pedido de autenticação ao AP.
5. O AP envia uma resposta de autenticação que contenha o texto de desafio unencrypted.
6. O cliente cifra o texto de desafio com a chave de WEP e envia o texto ao AP.
7. O AP compara o texto de desafio unencrypted com o texto de desafio cifrado. Se a autenticação pode decifrar e recuperar o texto de desafio original, a autenticação é bem sucedida.

A autenticação de chave compartilhada usa a criptografia de WEP durante o processo da associação de cliente.

Q. Que são as vantagens e desvantagem da autenticação de chave compartilhada?

A. Na autenticação de chave compartilhada, o cliente e o AP trocam o texto de desafio (texto claro) e o desafio cifrado. Consequentemente, este tipo de autenticação é vulnerável ao ataque que envolva pessoas. Um hacker pode escutar o desafio unencrypted e o desafio cifrado, e extrai a chave de WEP (chave compartilhada) desta informação. Quando um hacker conhece a chave de WEP, o mecanismo da autenticação inteiro está comprometido e o hacker pode alcançar a rede de WLAN. Esta é a desvantagem principal com autenticação de chave compartilhada.

Q. Que é autenticação do MAC address?

A. Embora o padrão do 802.11 não especifique a autenticação do MAC address, as redes de WLAN usam geralmente esta técnica de autenticação. Daqui, a maioria dos vendedores do dispositivo Wireless, incluindo Cisco, apoiam a autenticação do MAC address.

Na autenticação do MAC address, os clientes são autenticados com base em seu MAC address que os endereços MAC dos clientes são verificados contra uma lista de endereços MAC armazenaram localmente no AP ou em um servidor de autenticação externa. A autenticação de MAC é um mecanismo de segurança mais forte do que aberta e as autenticações de chave compartilhada que o 802.11 fornece. Este formulário de autenticação mais adicional reduz a semelhança de dispositivos não autorizados que pode alcançar a rede.

Q. Por que a autenticação de MAC não trabalha com o Wi-Fi Protected Access (WPA) no Cisco IOS Software Release 12.3(8)JA2?

A. O único nível de segurança para a autenticação de MAC é verificar o MAC address do cliente contra uma lista de endereços permitidos MAC. Isto é considerado muito fraco. Em uns Cisco IOS Software Release mais adiantados, você poderia configurar a autenticação de MAC e o WPA para cifrar a informação. Mas porque o WPA próprio tem um MAC address que verificasse, Cisco decidiu não permitir o este tipo de configuração em uns Cisco IOS Software Release mais atrasados e decidido melhorar somente recursos de segurança.

Q. Posso eu usar o SSID como um método para autenticar dispositivos Wireless?

A. O Service Set Identifier (SSID) é um valor original, diferenciando maiúsculas e minúsculas, alfanumérico que os WLAN usem como um nome de rede. O SSID é a - o mecanismo que permite a separação lógica do Sem fio LAN. O SSID não fornece nenhuma funções da privacidade de dados, nem o SSID autentica verdadeiramente o cliente ao AP. O valor SSID é

transmissão como o texto claro nas balizas, nas respostas dos pedidos da ponta de prova, da ponta de prova, e nos outros tipos de quadros. Um eavesdropper pode facilmente determinar o SSID com o uso de um analisador de pacote do Wireless LAN do 802.11, por exemplo, Sniffer Pro. Cisco não recomenda que você usa o SSID como um método para fixar sua rede de WLAN.

Q. Se eu desabilito a transmissão SSID, posso eu conseguir a segurança avançada em uma rede de WLAN?

A. Quando você desabilita a transmissão SSID, o SSID não está enviado em mensagens da baliza. Contudo, outros quadros como, pedidos da ponta de prova e respostas da ponta de prova ainda têm o SSID no texto claro. Assim você não consegue a segurança Wireless aumentada se você desabilita o SSID. O SSID não é projetado, nem é pretendido para o uso, como um mecanismo de segurança. Além, se você desabilita transmissões SSID, você pode encontrar problemas com Interoperabilidade do Wi-fi para disposições do misturado-cliente. Consequentemente, Cisco não recomenda que você usa o SSID como um modo de segurança.

Q. Que são as vulnerabilidades encontradas na Segurança do 802.11?

A. As vulnerabilidades principais da Segurança do 802.11 podem ser resumidas como segue:

- Autenticação fraca do dispositivo-somente: Os dispositivos do cliente são autenticados, não usuários.
- Criptografia de dados fraca: O Wired Equivalent Privacy (WEP) foi ineficaz provado como meios cifrar dados.
- Nenhuma integridade de mensagem: O valor da verificação de integridade (ICV) foi ineficaz provado como meios assegurar a integridade de mensagem.

Q. Que é o papel da autenticação do 802.1x no WLAN?

A. A fim endereçar os defeitos e as vulnerabilidades de segurança nos métodos originais da autenticação que o padrão do 802.11 define, o framework de autenticação do 802.1X é incluído no esboço para aprimoramentos de segurança da camada de MAC do 802.11. O grupo de tarefa do IEEE 802.11 eu (TGi) estou desenvolvendo atualmente estes realces. A estrutura do 802.1X fornece a camada de enlace a autenticação extensível, considerada normalmente somente nas camadas superior.

Q. Que são as três entidades que a estrutura do 802.1x define?

A. a estrutura do 802.1x exige estas três entidades lógica validar os dispositivos em uma rede de WLAN.

1. **Suplicante** — O suplicante reside no cliente do Wireless LAN, e é sabido igualmente como o

cliente EAP.
2. **Autenticador** — O autenticador reside no AP.
3. **Authentication Server** — O Authentication Server reside no servidor Radius.

Q. Como uma autenticação de cliente Wireless ocorre quando eu uso o framework de autenticação do 802.1x?

A. Quando o cliente Wireless (cliente EAP) se torna ativo, o cliente Wireless autentica com autenticação aberta ou compartilhada. o 802.1x trabalha com autenticação aberta e começa depois que o cliente associa com sucesso ao AP. A estação do cliente pode associar, mas pode passar o tráfego de dados somente depois a autenticação bem sucedida do 802.1x. Estão aqui as etapas na autenticação do 802.1x:

1. O AP (autenticador) configurado para o 802.1x pede a identidade do usuário do cliente.
2. Os clientes respondem com sua identidade dentro de um período de tempo estipulado.
3. O server verifica a identidade do usuário e começa a autenticação com o cliente se a identidade do usuário esta presente em seu base de dados.
4. O server envia um mensagem de sucesso ao AP.
5. Uma vez que o cliente é autenticado, o server para a frente que a chave de criptografia ao AP que é usado para cifrar/tráfego do decrypt enviou a e do cliente.
6. Em etapa 4, se a identidade do usuário não está atual no base de dados, o server deixa cair a autenticação e envia um mensagem de falha ao AP.
7. O AP encaminha esta mensagem ao cliente, e o cliente deve autenticar outra vez com credenciais corretas.

Nota: Durante todo a autenticação do 802.1x, o AP apenas encaminha os mensagens de autenticação a e do cliente.

Q. Que são as variantes EAP diferentes que eu posso usar com o framework de autenticação do 802.1x?

A. o 802.1x define o procedimento para autenticar clientes. O tipo EAP usado na estrutura do 802.1x define o tipo de credenciais e o método de autenticação usado na troca do 802.1x. A estrutura do 802.1x pode usar qualqueras um variantes EAP:

- EAP-TLS — Transport Layer Security do protocolo extensible authentication
- EAP-FAST — Autenticação Flexível de EAP através do túnel fixado
- EAP-SIM — Módulo de identidade de assinante EAP
- Cisco PULA — Protocolo lightweight extensible authentication
- EAP-PEAP — Protocolo extensible authentication protegido EAP
- EAP-MD5 — Algoritmo 5 do resumo de mensagem EAP
- EAP-OTP — Senha do tempo ligado EAP
- EAP-TTLS — Transport Layer Security em túnel EAP

Q. Como eu escolho um método de EAP do 802.1x das variações diferentes disponíveis?

A. A maioria de fator importante que você deve considerar é se o método de EAP é compatível com a rede existente ou não. Além, Cisco recomenda que você escolhe um método que apoie a

autenticação mútua.

Q. Que é autenticação de EAP local?

A. O EAP local é um mecanismo em que o WLC atua como um Authentication Server. As credenciais do usuário são armazenadas localmente no WLC para autenticar clientes Wireless, que atua como um processo backend nos escritórios remotos quando o server vai para baixo. As credenciais do usuário podem ser recuperadas do base de dados local no WLC ou de um servidor ldap externo. PULE, EAP-FAST, EAP-TLS, PEAPv0/MSCHAPv2, e PEAPv1/GTC são autenticações de EAP diferentes apoiadas pelo EAP local.

Q. Que é PULO de Cisco?

A. O protocolo lightweight extensible authentication (PULO) é um método proprietário de Cisco da autenticação. Cisco PULA é um tipo do autenticação do 802.1X para o Sem fio LAN (WLAN). Cisco PULA a autenticação mútua forte dos apoios entre o cliente e um servidor Radius com uma senha do fazer logon como o segredo compartilhado. Cisco PULA fornece o usuário per. dinâmico, por sessão chaves de criptografia. O PULO é menos método complicado para distribuir o 802.1x, e exige somente um servidor Radius. Refira o PULO de Cisco para obter informações sobre do PULO.

Q. Como EAP-FAST trabalha?

A. Algoritmos EAP-FAST da chave simétrica dos usos para conseguir um processo de autenticação em túnel. O estabelecimento de túnel confia em umas credenciais protegidas do acesso (PAC) que EAP-FAST possa ser fornecida e controle dinamicamente por EAP-FAST através do server do Authentication, Authorization, and Accounting (AAA) (tal como o [ACS] v. 3.2.3 do Serviço de controle de acesso Cisco Secure). Com um túnel mutuamente autenticado, uma proteção EAP-FAST das ofertas dos ataques do dicionário e umas vulnerabilidades homem-em--médias. Estão aqui as fases de EAP-FAST:

EAP-FAST abranda não somente riscos dos ataques do dicionário e dos ataques que envolva pessoas passivos, mas igualmente permite a autenticação segura baseada na infraestrutura atualmente distribuída.

- Fase 1: Estabeleça o túnel mutuamente autenticado — O cliente e o servidor AAA usam o PAC para autenticar-se e estabelecer um túnel seguro.
- Fase 2: Execute a authenticação do cliente no túnel estabelecido — O cliente envia o nome de usuário e a senha para autenticar e estabelecer a política de autorização de cliente.
- Opcionalmente, fase 0 — A autenticação EAP-FAST usa raramente esta fase para permitir o cliente de ser dinamicamente fornecida com um PAC. Esta fase gerencie umas credenciais do acesso de usuário per. firmemente entre o usuário e a rede. A fase 1 da autenticação usa estas credenciais do usuário per., conhecidas como o PAC.

Refira Cisco EAP-FAST para mais informação.

Q. Há os documentos em cisco.com que explicam como configurar o EAP em uma rede de WLAN de Cisco?

A. Refira a autenticação de EAP com o servidor Radius para obter informações sobre de como configurar a autenticação de EAP em uma rede de WLAN.

Consulte a nota do aplicativo protegida EAP para obter informações sobre de como configurar a autenticação de PEAP.

Refira a autenticação de leap com um servidor Radius local para obter informações sobre de como configurar a autenticação de leap.

Q. Que são os mecanismos de criptografia diferentes os mais de uso geral nas redes Wireless?

A. Estão aqui os esquemas de criptografia os mais de uso geral usados nas redes Wireless:

- WEP
- TKIP
- AES

O AES é um método de criptografia de hardware, visto que a criptografia WEP e TKIP é processada no firmware. Com upgrade de firmware um WEP os dispositivos podem apoiar o TKIP assim que são interoperáveis. O AES é o método o mais seguro e o mais rápido, visto que o WEP é o o mais menos seguro.

Q. Que é criptografia de WEP?

A. O WEP representa o Wired Equivalent Privacy. O WEP é usado para cifrar e decifrar os sinais de dados que transmitem entre dispositivos de WLAN. O WEP é uma característica opcional do IEEE 802.11 que previne a divulgação e a alteração dos pacotes no trânsito e também forneça o controle de acesso para o uso da rede. O WEP faz um link WLAN tão seguro como um link cabeado. Enquanto o padrão especifica, o WEP usa o algoritmo RC4 com uma chave 40-bit ou de 104-bit. O RC4 é um algoritmo simétrico porque o RC4 usa a mesma chave para a criptografia e a decifração dos dados. Quando a WEP está habilitada, cada "estação" de rádio possui uma chave. A chave é usada para misturar os dados antes da transmissão dos dados através das ondas de rádio. Se uma estação recebe um pacote que não esteja misturado com a chave apropriada, a estação rejeita o pacote e nunca entrega tal pacote ao host.

Refira configurar o Wired Equivalent Privacy (WEP) para obter informações sobre de como configurar o WEP.

Q. Que é rotação da chave da transmissão? Que é a frequência da rotação da chave da transmissão?

A. A rotação chave da transmissão permite que o AP gerencia a chave aleatória melhor possível do grupo. Transmita a rotação chave atualiza periodicamente todos os clientes capazes do gerenciamento chave. Quando você permite a rotação da chave de WEP da transmissão, o AP fornece uma chave de WEP dinâmica da transmissão e muda a chave no intervalo que você se ajusta. A rotação chave da transmissão é uma alternativa excelente ao TKIP se seu Wireless LAN apoia os dispositivos do cliente Wireless não-Cisco ou os dispositivos que você não pode promover ao firmware mais recente para dispositivos do cliente Cisco. Refira a rotação chave de possibilidade e de desabilitação da transmissão para obter informações sobre de como configurar a característica da rotação da chave da transmissão.

Q. Que é TKIP?

A. O TKIP representa o protocolo chave temporal da integridade. O TKIP foi introduzido para endereçar os defeitos na criptografia de WEP. O TKIP é sabido igualmente como o hashing da chave de WEP e foi chamado inicialmente WEP2. O TKIP é uma solução temporária que fixe o problema da reutilização da chave WEP. O TKIP usa o algoritmo RC4 para executar a criptografia, que é a mesma que o WEP. Uma diferença principal do WEP é que o TKIP muda a chave temporal cada pacote. As mudanças chaves temporais cada pacote porque o valor de hash para cada pacote muda.

Q. Podem os dispositivos que use o TKIP interoperam com dispositivos que usam a criptografia de WEP?

A. Uma vantagem com TKIP é que os WLAN com os AP WEP-baseados existentes e os rádios podem promover ao TKIP através das correções de programa simples do firmware. Também, o equipamento WEP-somente ainda interopera com dispositivos TKIP-permitidos que usam o WEP.

Q. Que é o Message Integrity Check (MIC)?

A. O MIC é contudo um outro realce para endereçar as vulnerabilidades na criptografia de WEP. O MIC impede ataques da bit-aleta em pacotes criptografado. Durante um ataque da bit-aleta, um intruso intercepta um mensagem codificada, altera a mensagem e retransmite então a mensagem alterada. O receptor não sabe que a mensagem é corrompida e não legítimo. A fim endereçar esta edição, a característica MIC adiciona um campo MIC ao wireless frame. O campo MIC fornece uma verificação de integridade do quadro que não seja vulnerável aos mesmos defeitos matemáticos que o ICV. O MIC igualmente adiciona um campo de número de sequência ao wireless frame. O AP deixa cair quadros recebeu fora de serviço.

Q. Que é WPA? Como é o WPA2 diferente do WPA?

A. O WPA é uma solução com base em padrões da Segurança do Wi-fi Alliance que enderece as vulnerabilidades em WLAN nativos. O WPA fornece a proteção de dados e o controle de acesso aumentados para sistemas de WLAN. O WPA endereça todas as vulnerabilidades conhecidas do Wired Equivalent Privacy (WEP) na implementação de segurança original do IEEE 802.11 e traz uma solução imediata da Segurança às redes de WLAN em ambientes da empresa e do escritório pequeno, escritório home (SOHO).

O WPA2 é a próxima geração de Segurança do Wi-fi. O WPA2 é a aplicação interoperáveis de Alliance do Wi-fi do padrão ratificado da IEEE 802.11i. O WPA2 executa o National Institute of Standards and Technology (NIST) - algoritmo de criptografia recomendado do Advanced Encryption Standard (AES) com o uso do modo contrário com protocolo do código de autenticação de mensagens do Cipher Block Chaining (CCMP). O modo de contador AES é uma cifra de bloco que cifre blocos do 128-bit de dados em um momento com uma chave de criptografia do 128-bit. O WPA2 oferece um de mais alto nível da Segurança do que o WPA. O WPA2 cria chaves de sessão frescas em cada associação. As chaves de criptografia que o WPA2 usa para cada cliente na rede são originais e específicas a esse cliente. Finalmente, cada pacote que é enviado sobre o ar é cifrado com uma chave original.

WPA1 e o WPA2 podem usar a criptografia TKIP ou CCMP. (É verdadeiro que alguns Access point e alguns clientes restringem as combinações, mas lá são quatro combinações possíveis). A diferença entre WPA1 e WPA2 está nos elementos de informação que obtêm postos nas balizas, nos quadros da associação, e nos quadros do aperto de mão 4-way. Os dados nestes elementos de informação são basicamente os mesmos, mas o identificador usado é diferente. O principal

diferença no aperto de mão chave é que o WPA2 inclui a chave inicial do grupo no aperto de mão 4-way e o aperto de mão chave do primeiro grupo está saltado, visto que o WPA precisa de fazer este aperto de mão extra para entregar as chaves iniciais do grupo. Re-fechar da chave do grupo acontece da mesma forma. O aperto de mão ocorre antes da seleção e do uso da série da cifra (TKIP ou AES) para a transmissão dos datagram de usuário. Durante o aperto de mão WPA1 ou WPA2, a série da cifra a usar-se é determinada. Uma vez que selecionada, a série da cifra é usada para todo o tráfego de usuário. Assim WPA1 mais o AES não é WPA2. WPA1 permite (mas é frequentemente limitado lateral do cliente) a cifra TKIP ou AES.

Q. Que é AES?

A. O AES representa o Advanced Encryption Standard. O AES oferece uma criptografia muito mais forte. O AES usa o algoritmo Rijndael, que é uma cifra de bloco com 128-, 192-, e apoio da chave do 256-bit e é muito mais forte do que o RC4. Para que os dispositivos de WLAN apoiem o AES, o hardware deve apoiar o AES em vez do WEP.

Q. Que métodos de autenticação são apoiados por um server do Internet Authentication Service de Microsoft (IAS)?

A. IAS apoia estes Protocolos de autenticação:

- Protocolo password authentication (PAP)
- Protocolo de autenticação de senha shiva (SPAP)
- Protocolo de autenticação de cumprimento do desafio (RACHADURA)
- Protocolo microsoft challenge handshake authentication (MS-CHAP)
- Versão 2 do protocolo microsoft challenge handshake authentication (MS-CHAP v2)
- RACHADURA do resumo de mensagem de protocolo 5 da autenticação extensível (RACHADURA do EAP-MD5)
- Segurança da camada do EAP-transporte (EAP-TLS)
- EAP-MS-CHAP protegido v2 (PEAP-MS-CHAP v2) (igualmente conhecido como PEAPv0/EAP-MSCHAPv2)

PEAP-TLS IAS no servidor do Windows 2000 apoia PEAP-MS-CHAP v2 e PEAP-TLS quando o pacote de serviços 4 do servidor do Windows 2000 é instalado. Para mais informação, refira métodos de autenticação para o uso com IAS .

Q. Como o VPN é executado em um envrionment wireless?

A. O VPN é um mecanismo de segurança da camada 3; os mecanismos de criptografia wireless são executados na camada 2. VPN são executados sobre o 802.1x, o EAP, o WEP, o TKIP, e o AES. Quando um mecanismo da camada 2 é no lugar, o VPN adiciona em cima à aplicação. Nos lugares como pontos quentes públicos e hotéis onde nenhuma Segurança é executada, o VPN seria uma solução útil a executar.

Pesquisa de defeitos e projeto FAQ

Q. Há algum melhor prática distribuir a segurança Wireless em um Outdoor Wireless LAN?

A. Refira melhores prática para a Segurança do Outdoor Wireless. Este documento fornece a informação em melhores prática da Segurança distribuir um Outdoor Wireless LAN.

Q. Posso eu usar um Windows 2000 ou um server 2003 com diretório ativo para que um servidor Radius autentique clientes Wireless?

A. O Windows 2000 ou o server 2003 com um diretório ativo podem trabalhar como um servidor Radius. Para obter informações sobre de como configurar este servidor Radius, você precisa de contactar Microsoft, porque Cisco não apoia a configuração de Windows Server.

Q. Meu local está a ponto de migrar de uma rede Wireless aberta (350 e 1200 Series AP) a uma rede PEAP. Eu gostaria de ter o SSID ABERTO (um SSID configurado para a autenticação aberta) e o trabalho PEAP SSID (um SSID configurado para a autenticação de PEAP) no mesmo AP ao mesmo tempo. Isto dá-nos a hora de migrar os clientes ao PEAP SSID. Há uma maneira de hospedar simultaneamente um SSID aberto e um PEAP SSID no mesmo AP?

A. Cisco AP apoia VLAN (camada 2 somente). Esta é realmente a única maneira de conseguir o que você quer fazer. Você precisa de criar dois VLAN, (nativo e seu outro VLAN). Então você pode não ter uma chave de WEP para uma e nenhuma chave de WEP para outra. Esta maneira, você pode configurar um dos VLAN para a autenticação aberta e do outro VLAN para a autenticação de PEAP. Refira a utilização de VLAN com equipamento Wireless do Cisco Aironet se você quer compreender como configurar VLAN.

Note por favor que você precisa de configurar seu Switches para o dot1q e para o inter VLAN que distribui, seu interruptor L3 ou seu roteador.

Q. Eu quero estabelecer meu Cisco AP1200 VxWorks para mandar os usuários Wireless autenticar a Cisco 3005 um concentrador VPN. Que configuração precisa esta presente no AP e nos clientes para realizar isto?

A. Não há nenhuma configuração específica necessária no AP ou nos clientes para esta encenação. Você deve fazer todas as configurações no concentrador VPN.

Q. Eu estou distribuindo um AG AP de Cisco 1232. Eu gostaria de conhecer o método que o mais seguro eu posso distribuir com este AP. Eu não tenho um servidor AAA e meus somente recursos são o AP e um domínio de Windows 2003. Eu sou familiar com como usar chaves estáticas do 128-bit WEP, o SSID sem transmissão e as limitações do MAC address. Os usuários trabalham na maior parte com estações de trabalho de Windows XP e alguns PDA. Que é a aplicação a mais segura para esta instalação?

A. Se você não tem um servidor Radius como Cisco ACS, você pode configurar seu AP como um servidor Radius local para o PULO, EAP-FAST ou a autenticação de MAC.

Nota: Muito um ponto importante que você deva considerar é se você quer usar seus clientes com PULO ou EAP-FAST. Em caso afirmativo, seus clientes devem ter uma utilidade para apoiar o PULO ou EAP-FAST. A utilidade de Windows XP apoia somente o PEAP ou o EAP-TLS.

Q. A autenticação de PEAP falha com o erro “EAP-TLS ou autenticação de PEAP falhado durante a saudação de SSL”. Por quê?

A. Este erro pode ocorrer devido à identificação de bug Cisco CSCee06008 (clientes registrados somente). O PEAP falha com ADU 1.2.0.4. A ação alternativa para este problema é usar a versão a mais atrasada do ADU.

Q. Posso eu ter o WPA e a autenticação do MAC local no mesmo SSID?

A. Cisco AP não apoia a chave da autenticação do MAC local e da PRE-parte do acesso protegido por wi-fi (WPA-PSK) no mesmo Service Set Identifier (SSID). Quando você permite a autenticação do MAC local com WPA-PSK, o WPA-PSK não trabalha. Este problema ocorre porque a autenticação do MAC local remove a linha da senha WPA-PSK ASCII da configuração.

Q. Nós temos atualmente três Cisco 1231 AP wireless setup com criptografia de WEP do 128-bit das cifras para nosso VLAN de dados. Nós não transmitimos o SSID. Nós não temos um servidor Radius separado em nosso ambiente. Alguém podia determinar a chave de WEP através de uma ferramenta da exploração, e usava a ferramenta por um par semanas para monitorar nosso tráfego Wireless. Como podemos nós impedir este e fazer a rede segura?

A. O WEP estático é vulnerável a esta edição, e pode ser derivado se um hacker captura bastante pacotes e pode obter dois ou mais pacotes com o mesmo vetor de inicialização (iv).

Há diversas maneiras de impedir a ocorrência desta edição:

1. Use chaves de WEP dinâmicas.
2. Use o WPA.
3. Se você tem somente adaptadores Cisco, permita pela chave do pacote e o MIC.

Q. Se eu tenho dois WLAN diferentes, ambos configuraram para o Wi-Fi Protected Access (WPA) - a chave pré-compartilhada (PSK), podem as chaves pré-compartilhada ser diferentes pelo WLAN? Se são diferentes, afeta o outro WLAN configurado com uma chave pré-compartilhada diferente?

A. O ajuste do WPA-PSK deve ser pelo WLAN. Se você muda um WPA-PSK, não deve afetar o outro WLAN que é configurado.

Q. Em meu ambiente eu uso na maior parte Intel PRO/Sem fio, autenticação Protocolo flexível da autenticação extensível através do Tunelamento seguro (EAP-FAST), e Serviço de controle de acesso Cisco Secure (ACS) 3.3 ligados às contas do diretório ativo de Windows (AD). O problema é quando a senha do usuário está a ponto de expirar, Windows não alerta o usuário mudar a senha. Eventualmente, a conta expira. Há uma solução para fazer a alerta de Windows o usuário para mudar a senha?

A. A característica do envelhecimento de senha do Cisco Secure ACS permite-o de forçar usuários a mudar suas senhas sob umas ou várias destas circunstâncias:

- Após um número especificado de dias (regras da idade-por-data)
- Após um número especificado de inícios de uma sessão (regras dos idade-por-usos)
- A primeira vez que um novo usuário entra (regra da mudança da senha)

Para detalhes em como configurar o Cisco Secure ACS para esta característica, refira a possibilidade do envelhecimento de senha para a base de dados de usuário do CiscoSecure.

Q. Quando um usuário entra sem fio usando o PULO conseguem seu script do início de uma sessão traçar driveres de rede. Contudo, usando o Wi-Fi Protected Access (WPA) ou o WPA2 com autenticação de PEAP, os scripts do início de uma sessão não são executado. O cliente e o Access point são Cisco como é o RAIO (ACS). Por que o script do início de uma sessão não é executado no RAIO (ACS)?

A. A autenticação da máquina é imperativa para que os scripts do início de uma sessão trabalhem. Isto permite os usuários Wireless de ganhar o acesso de rede para carregar scripts antes que o usuário entre.

Para obter informações sobre de como configurar a autenticação da máquina com PEAP-MS-CHAPv2, refira configurar o Cisco Secure ACS for Windows v3.2 com autenticação da máquina PEAP-MS-CHAPv2.

Q. Com utilitário de desktop do Cisco Aironet (ADU) libere o 3.0, quando um usuário configura a autenticação da máquina para a Segurança da camada do Protocolo-transporte da autenticação extensível (EAP-TLS), ADU não permite que o usuário crie um perfil. Por quê?

A. Isto é devido à identificação de bug Cisco CSCsg32032 (clientes registrados somente). Isto pode acontecer se o PC cliente tem o certificado da máquina instalado e não tem um certificado de usuário.

A ação alternativa é copiar o certificado da máquina à loja do usuário, cria um perfil do EAP-TLS e remove então o certificado da loja do usuário para a configuração da autenticação da máquina somente.

Q. Há alguma maneira de atribuir o VLAN no Wireless LAN baseado no MAC address do cliente?

A. Não. Isto não é possível. A atribuição de VLAN do servidor Radius trabalha somente com 802.1x, não autenticação de MAC. Você pode usar o RAIO para empurrar VSA com autenticação de MAC, se os endereços MAC são autenticados no servidor Radius (definido como o userid/senha em LEAP/PEAP).

Informações Relacionadas

- Segurança da rede Wireless
- White Paper da Segurança para LAN Wireless
- Vista geral da Segurança para LAN Wireless
- Guia de distribuição EAP-TLS para redes de Wireless LAN
- Cisco LEAP

- Configurando a Privacidade Equivalente com Fios (WEP)
- Suporte de produtos Wireless
- Suporte Técnico e Documentação - Cisco Systems