Perguntas frequentes sobre o Cisco Aironet Wireless Security

Contents

Introduction

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

Perguntas Frequentes Gerais

P. Qual é a necessidade da segurança sem fio?

A. Em uma rede com fio, os dados permanecem nos cabos que conectam os dispositivos finais. Mas as redes sem fio transmitem e recebem dados através de uma transmissão de sinais de RF para o ar livre. Devido à natureza da transmissão que as WLANs usam, há uma ameaça maior de hackers ou invasores que podem acessar ou corromper os dados. Para aliviar esse problema, todas as WLANs 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 (também conhecidos como criptografia).

P. Quais são os diferentes métodos de autenticação que o padrão 802.11 para LANs sem fio define?

A. O padrão 802.11 define dois mecanismos para autenticação de clientes de LAN sem fio:

1. Autenticação aberta
2. Autenticação de chave compartilhada

Há dois outros mecanismos comumente usados:

1. Autenticação baseada em SSID
2. Autenticação de endereço MAC

P. O que é autenticação aberta?

A. A autenticação aberta é basicamente um algoritmo de autenticação nulo, o que significa que não há verificação do usuário ou da máquina. A autenticação aberta permite que qualquer dispositivo que coloque uma solicitação de autenticação no ponto de acesso (AP). A Autenticação Aberta usa transmissão em texto claro para permitir que um cliente se associe a um AP. Se nenhuma criptografia estiver habilitada, qualquer dispositivo que conheça o SSID da WLAN poderá obter acesso à rede. Se a WEP (Wired Equivalent Privacy) estiver habilitada no AP, a chave WEP se tornará um meio de controle de acesso. Um dispositivo que não tem a chave WEP correta não pode transmitir dados através do AP mesmo que a autenticação seja bem-sucedida. Nem um dispositivo desse tipo pode descriptografar dados que o AP envia.

P. Quais etapas a autenticação aberta envolve para que um cliente se associe ao AP?

1. O cliente envia uma solicitação de sondagem aos APs.
2. Os APs enviam respostas de sondagem de volta.
3. O cliente avalia as respostas do AP e seleciona o melhor AP.
4. O cliente envia uma solicitação de autenticação ao AP.
5. O AP confirma a autenticação e registra o cliente.
6. Em seguida, o cliente envia uma solicitação de associação ao AP.
7. O AP confirma a associação e registra o cliente.

P. Quais são as vantagens e desvantagens da autenticação aberta?

A. Aqui estão as vantagens e desvantagens da autenticação aberta:

Vantagens: A autenticação aberta é um mecanismo de autenticação básico, que você pode usar com dispositivos sem fio que não suportam os complexos algoritmos de autenticação. A autenticação na especificação 802.11 é orientada para conectividade. Com o projeto, os requisitos de autenticação permitem que os dispositivos obtenham acesso rápido à rede. Nesse caso, você pode usar a Autenticação Aberta.

Desvantagens: A Autenticação Aberta não fornece nenhuma forma de verificar se um cliente é um cliente válido e não um cliente hacker. Se você não usar a criptografia WEP com a Autenticação Aberta, qualquer usuário que conheça o SSID da WLAN pode acessar a rede.

P. O que é Autenticação de chave compartilhada?

A. A Autenticação de Chave Compartilhada funciona de forma semelhante à Autenticação Aberta com uma diferença principal. Quando você usa a Open Authentication com a chave de criptografia WEP, a chave WEP é usada para criptografar e descriptografar os dados, mas não é usada na etapa de autenticação. Na Shared Key Authentication, a criptografia WEP é usada para autenticação. Como a Autenticação Aberta, a Autenticação de Chave Compartilhada exige que o cliente e o AP tenham a mesma chave WEP. O AP que usa a autenticação de chave compartilhada envia um pacote de texto de desafio ao cliente. O cliente usa a chave WEP configurada localmente para criptografar o texto do desafio e responder com uma solicitação de autenticação subsequente. Se o AP puder descriptografar a solicitação de autenticação e recuperar o texto de desafio original, ele responderá com uma resposta de autenticação que concederá acesso ao cliente.

P. Quais etapas a Autenticação de chave compartilhada envolve para que um

cliente se associe ao AP?

1. O cliente envia uma solicitação de sondagem aos APs.
2. Os APs enviam respostas de sondagem de volta.
3. O cliente avalia as respostas do AP e seleciona o melhor AP.
4. O cliente envia uma solicitação de autenticação ao AP.
5. O AP envia uma resposta de autenticação que contém o texto de desafio não criptografado.
6. O cliente criptografa o texto do desafio com a chave WEP e envia o texto ao AP.
7. O AP compara o texto de desafio não criptografado com o texto de desafio criptografado. Se a autenticação puder descriptografar e recuperar o texto do desafio original, a autenticação será bem-sucedida.

A Shared Key Authentication usa criptografia WEP durante o processo de associação do cliente.

P. Quais são as vantagens e desvantagens da Shared Key Authentication?

A. Na Shared Key Authentication, o cliente e o AP trocam o texto do desafio (texto claro) e o desafio criptografado. Portanto, esse tipo de autenticação é vulnerável a ataques de pessoa no meio. Um hacker pode ouvir o desafio não criptografado e o desafio criptografado, e extrair a chave WEP (chave compartilhada) dessas informações. Quando um hacker conhece a chave WEP, todo o mecanismo de autenticação é comprometido e o hacker pode acessar a rede WLAN. Essa é a principal desvantagem da Shared Key Authentication.

P. O que é autenticação de endereço MAC?

A. Embora o padrão 802.11 não especifique a autenticação de endereço MAC, as redes WLAN geralmente usam essa técnica de autenticação. Portanto, a maioria dos fornecedores de dispositivos sem fio, incluindo a Cisco, suportam a autenticação de endereço MAC.

Na autenticação de endereço MAC, os clientes são autenticados com base em seu endereço MAC Os endereços MAC dos clientes são verificados em uma lista de endereços MAC armazenados localmente no AP ou em um servidor de autenticação externo. A autenticação MAC é um mecanismo de segurança mais forte do que as Autenticações de Chave Aberta e Compartilhada fornecidas pelo 802.11. Essa forma de autenticação reduz ainda mais a probabilidade de dispositivos não autorizados acessarem a rede.

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

A. O único nível de segurança para a autenticação MAC é verificar o endereço MAC do cliente em relação a uma lista de endereços MAC permitidos. Isso é considerado muito fraco. Nas versões anteriores do Cisco IOS Software, você pode configurar a autenticação MAC e a WPA para criptografar as informações. Mas como o próprio WPA tem um endereço MAC que verifica, a Cisco decidiu não permitir esse tipo de configuração em versões posteriores do Cisco IOS Software e decidiu apenas melhorar os recursos de segurança.

P. Posso usar o SSID como um método para autenticar dispositivos sem fio?

A. O SSID (Service Set Identifier) é um valor alfanumérico exclusivo, diferencia maiúsculas de minúsculas que as WLANs usam como nome de rede. O SSID é um mecanismo -que permite a

separação lógica de LANs sem fio. O SSID não fornece nenhuma função de privacidade de dados, nem o SSID autentica realmente o cliente para o AP. O valor SSID é transmitido como texto claro em Beacons, Solicitações de teste, Respostas de teste e outros tipos de quadros. Um bisbilhoteiro pode determinar facilmente o SSID com o uso de um analisador de pacotes de LAN sem fio 802.11, por exemplo, Sniffer Pro. A Cisco não recomenda que você use o SSID como um método para proteger sua rede WLAN.

P. Se eu desativar a transmissão SSID, posso obter segurança avançada em uma rede WLAN?

A. Quando você desabilita a transmissão de SSID, o SSID não é enviado em mensagens Beacon. No entanto, outros quadros, como Solicitações de Investigação e Respostas de Investigação, ainda têm o SSID em texto claro. Assim, você não alcançará a segurança sem fio aprimorada se desativar o SSID. O SSID não foi projetado, nem se destina ao uso, como um mecanismo de segurança. Além disso, se você desabilitar os broadcasts de SSID, poderá encontrar problemas com a interoperabilidade Wi-Fi para implantações de clientes mistos. Portanto, a Cisco não recomenda que você use o SSID como um modo de segurança.

P. Quais são as vulnerabilidades encontradas na segurança 802.11?

A. As principais vulnerabilidades da segurança 802.11 podem ser resumidas da seguinte maneira:

- Autenticação fraca somente de dispositivo: Os dispositivos clientes são autenticados, não os usuários.
- Criptografia de dados fraca: A WEP (Wired Equivalent Privacy) tem sido comprovada como um meio de criptografia de dados.
- Sem integridade da mensagem: O valor da verificação de integridade (ICV) foi comprovado como ineficaz como meio de garantir a integridade da mensagem.

P. Qual é a função da autenticação 802.1x na WLAN?

A. Para resolver as falhas e vulnerabilidades de segurança nos métodos originais de autenticação definidos pelo padrão 802.11, a estrutura de autenticação 802.1X está incluída no rascunho para melhorias de segurança da camada MAC 802.11. O Grupo de Tarefas i (TGi) do IEEE 802.11 está desenvolvendo atualmente essas melhorias. A estrutura 802.1X fornece à camada de enlace autenticação extensível, normalmente vista apenas nas camadas superiores.

P. Quais são as três entidades que a estrutura 802.1x define?

A. A estrutura 802.1x exige que essas três entidades lógicas validem os dispositivos em uma rede WLAN.

1. **Requerente** — O requerente reside no cliente de LAN sem fio e também é conhecido como cliente EAP.
2. **Autenticador** — O autenticador reside no AP.
3. **Servidor de Autenticação** — O servidor de autenticação reside no servidor RADIUS.

P. Como ocorre uma autenticação de cliente sem fio quando uso a estrutura de autenticação 802.1x?

A. Quando o cliente sem fio (cliente EAP) se torna ativo, o cliente sem fio é autenticado com autenticação aberta ou compartilhada. O 802.1x funciona com autenticação aberta e começa depois que o cliente se associa com êxito ao AP. A estação cliente pode se associar, mas pode transmitir tráfego de dados somente após a autenticação 802.1x bem-sucedida. Aqui estão os passos da autenticação 802.1x:

1. O AP (Authenticator) configurado para 802.1x solicita a identidade do usuário do cliente.
2. Os clientes respondem com sua identidade dentro de um prazo estipulado.
3. O servidor verifica a identidade do usuário e inicia a autenticação com o cliente se a identidade do usuário estiver presente em seu banco de dados.
4. O servidor envia uma mensagem de êxito ao AP.
5. Quando o cliente é autenticado, o servidor encaminha a chave de criptografia para o AP que é usado para criptografar/descriptografar o tráfego enviado de e para o cliente.
6. Na etapa 4, se a identidade do usuário não estiver presente no banco de dados, o servidor descartará a autenticação e enviará uma mensagem de falha ao AP.
7. O AP encaminha essa mensagem para o cliente, e o cliente deve se autenticar novamente com as credenciais corretas.

Observação: na autenticação 802.1x, o AP simplesmente encaminha as mensagens de autenticação para e do cliente.

P. Quais são as diferentes variantes EAP que posso usar com a estrutura de autenticação 802.1x?

A. 802.1x define o procedimento para autenticar clientes. O tipo de EAP usado na estrutura 802.1x define o tipo de credenciais e o método de autenticação usados na troca 802.1x. A estrutura 802.1x pode usar qualquer uma destas variantes EAP:

- EAP-TLS—Extensible Authentication Protocol Transport Layer Security
- EAP-FAST—Autenticação flexível EAP via túnel seguro
- EAP-SIM—Módulo de identificação do assinante EAP
- Cisco LEAP—Lightweight Extensible Authentication Protocol
- EAP-PEAP—EAP Protected Extensible Authentication Protocol
- EAP-MD5 — Algoritmo de resumo de mensagem EAP 5
- EAP-OTP—Senha EAP em Tempo Real
- EAP-TTLS—EAP Tunneled Transport Layer Security (Segurança de camada de transporte em túnel EAP)

P. Como escolho um método 802.1x EAP a partir das diferentes variantes disponíveis?

A. O fator mais importante que você deve considerar é se o método EAP é compatível com a rede existente ou não. Além disso, a Cisco recomenda que você escolha um método que ofereça suporte à autenticação mútua.

P. O que é autenticação EAP local?

A. O EAP local é um mecanismo no qual a WLC atua como um servidor de autenticação. As credenciais de usuário são armazenadas localmente na WLC para autenticar clientes sem fio, que atuam como um processo de back-end em escritórios remotos quando o servidor fica inativo. As credenciais de usuário podem ser recuperadas do banco de dados local na WLC ou de um servidor LDAP externo. LEAP, EAP-FAST, EAP-TLS, PEAPv0/MSCHAPv2 e PEAPv1/GTC são autenticações EAP diferentes suportadas pelo EAP local.

P. O que é o Cisco LEAP?

A. O LEAP (Lightweight Extensible Authentication Protocol) é um método de autenticação proprietário da Cisco. O Cisco LEAP é um tipo de autenticação 802.1X para LANs sem fio (WLANs). O Cisco LEAP suporta uma autenticação mútua forte entre o cliente e um servidor RADIUS através de uma senha de início de sessão como o segredo partilhado. O Cisco LEAP fornece chaves de criptografia dinâmicas por usuário e por sessão. O LEAP é o método menos complicado para implantar o 802.1x e requer apenas um servidor RADIUS. Consulte o Cisco LEAP para obter informações sobre o LEAP.

P. Como funciona o EAP-FAST?

A. O EAP-FAST usa algoritmos de chave simétricos para obter um processo de autenticação em túnel. O estabelecimento do túnel depende de uma PAC (Protected Access Credential, Credencial de Acesso Protegido) que o EAP-FAST pode ser provisionado e gerenciado dinamicamente pelo EAP-FAST através do servidor de autenticação, autorização e contabilização (AAA - Authentication, Authorization, and Accounting) (como o Cisco Secure Access Control Server [ACS] v. 3.2.3). Com um túnel mutuamente autenticado, o EAP-FAST oferece proteção contra ataques de dicionário e vulnerabilidades de comunicação pessoal. Aqui estão as fases do EAP-FAST:

O EAP-FAST não só reduz os riscos de ataques de dicionários passivos e ataques de intermediários, como também permite a autenticação segura com base na infraestrutura atualmente implantada.

- Fase 1: Estabeleça um túnel mutuamente autenticado — o cliente e o servidor AAA usam a PAC para autenticar um ao outro e estabelecer um túnel seguro.
- Fase 2: Executar autenticação de cliente no túnel estabelecido — O cliente envia o nome de usuário e a senha para autenticar e estabelecer a política de autorização do cliente.
- Opcionalmente, Fase 0 — A autenticação EAP-FAST usa raramente essa fase para permitir que o cliente seja provisionado dinamicamente com uma PAC. Essa fase gera uma credencial de acesso por usuário com segurança entre o usuário e a rede. A fase 1 da autenticação usa essa credencial por usuário, conhecida como PAC.

Consulte o Cisco EAP-FAST para obter mais informações.

P. Há documentos no cisco.com que explicam como configurar o EAP em uma rede Cisco WLAN?

A. Consulte Autenticação EAP com servidor RADIUS para obter informações sobre como configurar a autenticação EAP em uma rede WLAN.

Consulte Nota de Aplicação EAP Protegida para obter informações sobre como configurar a autenticação PEAP.

Consulte Autenticação LEAP com um servidor RADIUS local para obter informações sobre como configurar a autenticação LEAP.

P. Quais são os diferentes mecanismos de criptografia mais comumente usados em redes sem fio?

A. Aqui estão os esquemas de criptografia mais usados em redes sem fio:

- WEP
- TKIP
- AES

AES é um método de criptografia de hardware, enquanto a criptografia WEP e TKIP é processada no firmware. Com uma atualização de firmware, os dispositivos WEP podem suportar TKIP para que sejam interoperáveis. O AES é o método mais seguro e mais rápido, enquanto o WEP é o menos seguro.

P. O que é criptografia WEP?

A. O WEP representa o Wired Equivalent Privacy. A WEP é usada para criptografar e descriptografar sinais de dados que transmitem entre dispositivos 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. Como o padrão especifica, o WEP usa o algoritmo RC4 com uma chave de 40 ou 104 bits. 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.

Consulte Configuração da WEP (Wired Equivalent Privacy) para obter informações sobre como configurar a WEP.

P. O que é Rotação da Chave de Broadcast? Qual é a frequência da Rotação da Chave de Broadcast?

A. A rotação da chave de broadcast permite que o AP gere a melhor chave de grupo aleatória possível. A rotação da chave de broadcast atualiza periodicamente todos os clientes com capacidade de gerenciamento de chaves. Quando você ativa a rotação da chave WEP de broadcast, o AP fornece uma chave WEP de broadcast dinâmica e altera a chave no intervalo definido. A rotação da chave de broadcast é uma excelente alternativa para o TKIP se a sua LAN sem fio suportar dispositivos ou dispositivos de clientes sem fio que não sejam da Cisco e que você não possa atualizar para o firmware mais recente para dispositivos de cliente da Cisco. Consulte Habilitando e Desabilitando Rotação de Chave de Broadcast para obter informações sobre como configurar o recurso de rotação da chave de broadcast.

P. O que é o TKIP?

A. TKIP significa Temporal Key Integrity Protocol. O TKIP foi introduzido para corrigir as falhas na criptografia WEP. O TKIP também é conhecido como hashing de chave WEP e foi inicialmente chamado de WEP2. O TKIP é uma solução temporária que corrige o problema de reutilização da chave WEPs. O TKIP usa o algoritmo RC4 para executar a criptografia, que é igual ao WEP. Uma grande diferença do WEP é que o TKIP altera a chave temporal de cada pacote. A chave temporal altera cada pacote porque o valor de hash para cada pacote é alterado.

P. Os dispositivos que usam TKIP podem interoperar com dispositivos que usam criptografia WEP?

A. Uma vantagem com o TKIP é que as WLANs com APs e rádios baseados em WEP podem atualizar para o TKIP através de simples patches de firmware. Além disso, o equipamento somente WEP ainda interopera com dispositivos habilitados para TKIP que usam WEP.

P. O que é verificação de integridade de mensagem (MIC)?

A. O MIC é mais um aprimoramento para tratar das vulnerabilidades na criptografia WEP. O MIC evita ataques bit-flip em pacotes criptografados. Durante um ataque bit-flip, um intruso intercepta uma mensagem criptografada, altera a mensagem e depois retransmite a mensagem alterada. O receptor não sabe que a mensagem está corrompida e não é legítima. Para resolver esse problema, o recurso MIC adiciona um campo MIC ao quadro sem fio. O campo MIC fornece uma verificação da integridade do quadro que não é vulnerável às mesmas falhas matemáticas que o ICV. O MIC também adiciona um campo de número de sequência ao quadro sem fio. O AP descarta quadros recebidos fora de ordem.

P. O que é WPA? Qual é a diferença entre WPA2 e WPA?

A. O WPA é uma solução de segurança padrão da Wi-Fi Alliance que resolve as vulnerabilidades nas WLANs nativas. O WPA oferece proteção avançada de dados e controle de acesso para sistemas WLAN. A WPA aborda todas as vulnerabilidades WEP (Wired Equivalent Privacy) conhecidas na implementação de segurança original do IEEE 802.11 e oferece uma solução de segurança imediata para redes WLAN em ambientes corporativos e de pequenos escritórios, escritórios domésticos (SOHO).

A WPA2 é a próxima geração de segurança Wi-Fi. A WPA2 é a implementação interoperável da Wi-Fi Alliance do padrão IEEE 802.11i ratificado. A WPA2 implementa o algoritmo de criptografia AES (Advanced Encryption Standard) recomendado pelo National Institute of Standards and Technology (NIST) com o uso do Counter Mode com Cipher Block Chaining Message Authentication Code Protocol (CCMP). O modo de contador do AES é uma cifra de bloco que criptografa blocos de dados de 128 bits de cada vez com uma chave de criptografia de 128 bits. A WPA2 oferece um nível de segurança mais alto do que a WPA. A WPA2 cria novas chaves de sessão em cada associação. As chaves de criptografia que o WPA2 usa para cada cliente na rede são exclusivas e específicas para esse cliente. Por fim, cada pacote enviado remotamente é criptografado com uma chave exclusiva.

WPA1 e WPA2 podem usar a criptografia TKIP ou CCMP. (É verdade que alguns pontos de acesso e alguns clientes restringem as combinações, mas há quatro combinações possíveis). A diferença entre WPA1 e WPA2 está nos elementos de informação que são colocados nos beacons, quadros de associação e quadros de handshake de 4 vias. Os dados nestes elementos

de informação são basicamente os mesmos, mas o identificador utilizado é diferente. A principal diferença no handshake principal é que a WPA2 inclui a chave de grupo inicial no handshake de 4 vias e o primeiro handshake de chave de grupo é ignorado, enquanto a WPA precisa fazer esse handshake extra para entregar as chaves de grupo iniciais. A rechaveamento da chave de grupo acontece da mesma maneira. O handshake ocorre antes da seleção e uso do conjunto de cifras (TKIP ou AES) para a transmissão de datagramas do usuário. Durante o handshake WPA1 ou WPA2, o conjunto de cifras a ser usado é determinado. Depois de selecionado, o conjunto de cifras é usado para todo o tráfego do usuário. Assim, WPA1 mais AES não é WPA2. O WPA1 permite (mas frequentemente é limitado ao lado do cliente) a cifra TKIP ou AES.

P. O que é AES?

A. AES significa Advanced Encryption Standard (Padrão de criptografia avançada). O AES oferece criptografia muito mais forte. O AES usa o algoritmo Rijndael, que é uma cifra de bloco com suporte a chaves de 128, 192 e 256 bits e é muito mais forte que o RC4. Para que os dispositivos WLAN suportem AES, o hardware deve suportar AES em vez de WEP.

P. Que métodos de autenticação são suportados por um servidor Microsoft Internet Authentication Service (IAS)?

A. O IAS suporta estes protocolos de autenticação:

- Protocolo de autenticação de senha (PAP - Password Authentication Protocol)
- Protocolo de autenticação de senha Shiva (SPAP - Shiva Password Authentication Protocol)
- Challenge Handshake Authentication Protocol (CHAP)
- Protocolo de Autenticação de Handshake Desafio da Microsoft (MS-CHAP)
- Microsoft Challenge Handshake Authentication Protocol versão 2 (MS-CHAP v2)
- Protocolo de Autenticação Extensível - Resumo de Mensagem 5 CHAP (EAP-MD5 CHAP)
- EAP-Transport Layer Security (EAP-TLS)
- EAP-MS-CHAP v2 (PEAP-MS-CHAP v2) (também conhecido como PEAPv0/EAP-MSCHAPv2)

O PEAP-TLS IAS no Windows 2000 Server suporta PEAP-MS-CHAP v2 e PEAP-TLS quando o Windows 2000 Server Service Pack 4 está instalado. Para obter mais informações, consulte Métodos de Autenticação para uso com IAS .

P. Como a VPN é implementada em um ambiente sem fio?

A. A VPN é um mecanismo de segurança de Camada 3; os mecanismos de criptografia sem fio são implementados na Camada 2. A VPN é implementada em 802.1x, EAP, WEP, TKIP e AES. Quando um mecanismo de Camada 2 está instalado, a VPN adiciona sobrecarga à implementação. Em locais como hotspots públicos e hotéis onde não há segurança implementada, a VPN seria uma solução útil para implementar.

Perguntas frequentes sobre solução de problemas e projeto

P. Há alguma prática recomendada para implantar a segurança sem fio em uma LAN sem fio externa?

A. Consulte Melhores Práticas para Segurança Wireless Externa. Este documento fornece

informações sobre as melhores práticas de segurança para implantar uma LAN sem fio externa.

P. Posso usar um servidor Windows 2000 ou 2003 com Ative Diretory para um servidor RADIUS para autenticar clientes sem fio?

A. O servidor Windows 2000 ou 2003 com um diretório ativo pode funcionar como um servidor RADIUS. Para obter informações sobre como configurar este servidor RADIUS, você precisa entrar em contato com a Microsoft, pois a Cisco não oferece suporte à configuração do servidor Windows.

P. Meu site está prestes a migrar de uma rede sem fio aberta (350 e 1200 Series APs) para uma rede PEAP. Eu gostaria que o SSID ABERTO (um SSID configurado para autenticação aberta) e o SSID PEAP (um SSID configurado para autenticação PEAP) funcionassem no mesmo AP ao mesmo tempo. Isso nos dá tempo para migrar os clientes para o SSID PEAP. Há uma maneira de hospedar simultaneamente um SSID aberto e um SSID PEAP no mesmo AP?

A. Os APs Cisco suportam VLANs (somente camada 2). Esta é, na verdade, a única forma de conseguir o que se quer fazer. Você precisa criar duas VLANs (nativa e outra VLAN). Depois, você pode ter uma chave WEP para uma chave WEP e nenhuma chave WEP para outra. Dessa forma, você pode configurar uma das VLANs para autenticação aberta e a outra VLAN para autenticação PEAP. Consulte Uso de VLANs com o Cisco Aironet Wireless Equipment se quiser entender como configurar VLANs.

Observe que você precisa configurar seus switches para dot1Q e para roteamento entre VLANs, seu switch L3 ou seu roteador.

P. Quero configurar meu Cisco AP 1200 VxWorks para que os usuários sem fio se autentiquem em um Cisco 3005 VPN Concentrator. Que configuração precisa estar presente no AP e nos clientes para fazer isso?

A. Não há nenhuma configuração específica necessária no AP ou nos clientes para este cenário. Você deve fazer todas as configurações no VPN Concentrator.

P. Estou implantando um AP Cisco 1232 AG. Gostaria de saber o método mais seguro que posso implantar com esse AP. Não tenho um servidor AAA e meus únicos recursos são o AP e um domínio do Windows 2003. Estou familiarizado com como usar chaves WEPs estáticas de 128 bits, SSID sem broadcast e restrições de endereço MAC. Os usuários trabalham principalmente com estações de trabalho do Windows XP e alguns PDAs. Qual é a implementação mais segura para essa configuração?

A. Se você não tiver um servidor RADIUS como o Cisco ACS, poderá configurar seu AP como um servidor RADIUS local para autenticação LEAP, EAP-FAST ou MAC.

Observação: um ponto muito importante que você deve considerar é se deseja usar seus clientes com LEAP ou EAP-FAST. Em caso afirmativo, seus clientes devem ter um utilitário para suportar LEAP ou EAP-FAST. O utilitário do Windows XP suporta apenas PEAP ou EAP-TLS.

P. A autenticação PEAP falha com o erro "Falha na autenticação EAP-TLS ou PEAP durante o handshake SSL". Por quê?

A. Esse erro pode ocorrer devido à ID de bug da Cisco CSCee06008 **(somente clientes registrados)** . O PEAP falha com ADU 1.2.0.4. A solução para esse problema é usar a versão mais recente do ADU.

P. Posso ter a autenticação WPA e MAC local no mesmo SSID?

A. O AP da Cisco não suporta autenticação MAC local e chave de pré-compartilhamento de acesso protegido Wi-Fi (WPA-PSK - Wi-Fi Protected Access Pre-share Key) no mesmo SSID (Service Set Identifier). Quando você habilita a autenticação MAC local com WPA-PSK, a WPA-PSK não funciona. Esse problema ocorre porque a autenticação MAC local remove a linha de senha ASCII WPA-PSK da configuração.

P. Atualmente, temos três APs sem fio Cisco 1231 configurados com criptografia WEP de 128 bits para nossa VLAN de dados. Não transmitimos o SSID. Não temos um servidor RADIUS separado em nosso ambiente. Alguém conseguiu determinar a chave WEP através de uma ferramenta de análise e utilizou a ferramenta durante algumas semanas para monitorizar o nosso tráfego sem fios. Como podemos evitar isso e tornar a rede segura?

A. A WEP estática é vulnerável a esse problema e pode ser derivada se um hacker capturar pacotes suficientes e conseguir obter dois ou mais pacotes com o mesmo vetor de inicialização (IV).

Há várias maneiras de evitar a ocorrência deste problema:

1. Usar chaves WEP dinâmicas.
2. Usar WPA.
3. Se você tiver apenas adaptadores Cisco, ative Por chave de pacote e MIC.

P. Se eu tiver duas WLANs diferentes, ambas configuradas para WPA (Wi-Fi Protected Access)-PSK (Pre-Shared Key), as chaves pré-compartilhadas podem ser diferentes por WLAN? Se forem diferentes, isso afeta a outra WLAN configurada com uma chave pré-compartilhada diferente?

A. A configuração da WPA-PSK deve ser por WLAN. Se você alterar uma WPA-PSK, ela não deverá afetar a outra WLAN configurada.

P. No meu ambiente, uso principalmente Intel Pro/Wireless, Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) e Cisco Secure Access Control Server (ACS) 3.3 vinculados a contas do Windows Ative Diretory (AD). O problema é que quando a senha do usuário está prestes a expirar, o Windows não solicita que o usuário altere a senha. Eventualmente, a conta expirará. Existe uma solução para fazer com que o Windows solicite ao usuário que altere a senha?

A. O recurso de envelhecimento de senha do Cisco Secure ACS permite forçar os usuários a alterar suas senhas sob uma ou mais das seguintes condições:

- Após um número especificado de dias (regras por data de vencimento)
- Depois de um número especificado de logins (regras por uso)
- A primeira vez que um novo usuário faz logon (regra de alteração de senha)

Para obter detalhes sobre como configurar o Cisco Secure ACS para esse recurso, consulte Ativando o envelhecimento da senha para o banco de dados do usuário do CiscoSecure.

P. Quando um usuário faz login sem fio usando o LEAP, ele recebe seu script de login para mapear unidades de rede. No entanto, usando o WPA (Wi-Fi Protected Access) ou WPA2 com autenticação PEAP, os scripts de login não são executados. Tanto o cliente quanto o ponto de acesso são Cisco como o RADIUS (ACS). Por que o script de login não é executado no RADIUS (ACS)?

A. A autenticação de máquina é obrigatória para scripts de login funcionarem. Isso permite que os usuários sem fio obtenham acesso à rede para carregar scripts antes que o usuário faça logon.

Para obter informações sobre como configurar a autenticação da máquina com PEAP-MS-CHAPv2, consulte Configuração do Cisco Secure ACS para Windows v3.2 com autenticação da máquina PEAP-MS-CHAPv2.

P. Com o Cisco Aironet Desktop Utility (ADU) versão 3.0, quando um usuário configura a autenticação de máquina para EAP-TLS (Extensible Authentication Protocol-Transport Layer Security), a ADU não permite que o usuário crie um perfil. Por quê?

A. Isso ocorre devido à ID de bug da Cisco CSCsg32032 (somente clientes registrados) . Isso pode acontecer se o PC cliente tiver o certificado da máquina instalado e não tiver um certificado de usuário.

A solução é copiar o certificado da máquina para o repositório de usuários, criar um perfil EAP-TLS e, em seguida, remover o certificado do repositório de usuários para a configuração somente de autenticação da máquina.

P. Há alguma maneira de atribuir VLAN na LAN sem fio com base no endereço MAC do cliente?

A. Não, não é possível. A atribuição de VLAN do servidor RADIUS só funciona com 802.1x, não com autenticação MAC. Você pode usar o RADIUS para enviar VSAs com autenticação MAC, se os endereços MAC forem autenticados no servidor RADIUS (definido como userid/password no LEAP/PEAP).

Informações Relacionadas

- Segurança de rede sem fio
- White paper sobre segurança de LAN sem fio
- Visão geral da segurança de LAN sem fio

- Guia de implantação EAP-TLS para redes LAN sem fio
- Cisco LEAP
- Configuração do protocolo WEP
- Suporte de produtos Wireless
- Suporte Técnico e Documentação - Cisco Systems