NP, controladores do Wireless LAN, e exemplo de configuração das redes Wireless

Índice

Introdução

Este documento fornece uma configuração de exemplo para o protocolo extensible authentication protegido (PEAP) com a autenticação da versão 2 do protocolo microsoft challenge handshake authentication (MS-CHAP) em uma rede de Cisco Unified Wireless com o servidor da política da rede Microsoft (NP) como o servidor Radius.

Pré-requisitos

Requisitos

Assegure-se de que você esteja familiar com estes procedimentos antes que você tente esta configuração:

- A instalação de Windows 2008 do conhecimento do gerenciamento de recursos básicos
- Conhecimento da instalação do controlador de Cisco

Assegure-se de que estas exigências estejam cumpridas antes que você tente esta configuração:

- Instale o sistema operacional 2008 do Microsoft Windows server em cada um dos server no laboratório de teste.
- Atualize todos os pacotes de serviços.
- Instale os controladores e o Lightweight Access Points (regaços).
- Configurar as atualizações de software mais recente.

Para a instalação inicial e a informação de configuração para os controladores wireless do Cisco 5508 Series, refira o guia de instalação do controlador wireless do Cisco 5500 Series.

Nota: Este documento é pretendido dar aos leitores um exemplo na configuração exigida em um servidor Microsoft para a autenticação PEAP-MS-CHAP. A configuração do Microsoft Windows server apresentada neste documento foi testada no laboratório e encontrada para trabalhar como esperado. Se você tem o problema com a configuração, contacte Microsoft para a ajuda. O centro de assistência técnica da Cisco (TAC) não apoia a configuração do Microsoft Windows server.

Microsoft Windows 2008 Guias de Instalação e Configuração pode ser encontrado na rede da tecnologia de Microsoft.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Controlador do Sem fio de Cisco 5508 que executa a versão de firmware 7.4
- Access Point (AP) do Cisco Aironet 3602 com protocolo de pouco peso do Access point (LWAPP)
- Servidor de empreendimento de Windows 2008 com NP, Certificate Authority (CA), protocolo de controle dinâmico de host (DHCP), e serviços do Domain Name System (DNS) instalado
- PC cliente de Microsoft Windows 7
- Cisco Catalyst 3560 Series Switch

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Vista geral PEAP

Segurança do nível do transporte dos usos PEAP (TLS) para criar um canal cifrado entre um cliente PEAP de autenticação, tal como um portátil wireless, e um autenticador PEAP, tal como Microsoft NP ou algum servidor Radius. O PEAP não especifica um método de autenticação, mas fornece a segurança adicional para outros protocolos extensible authentication (EAP), como EAP-MS-CHAP v2, que pode se operar através do canal TLS-cifrado fornecido pelo PEAP. O processo

de autenticação de PEAP consiste em duas fases principal.

PEAP fase um: Canal TLS-cifrado

Os associados do cliente Wireless com o AP. Uma associação da IEEE 802.11-based fornece um sistema aberto ou uma autenticação de chave compartilhada antes que uma associação segura esteja criada entre o cliente e o Access point. Depois que a associação da IEEE 802.11-based é estabelecida com sucesso entre o cliente e o Access point, a sessão TLS está negociada com o AP. Depois que a autenticação é terminada com sucesso entre o cliente Wireless e os NP, a sessão TLS está negociada entre o cliente e os NP. A chave que é derivada dentro desta negociação é usada para cifrar toda a comunicação subsequente.

Fase dois PEAP: Uma comunicação EAP-autenticada

Uma comunicação EAP, que inclua a negociação EAP, ocorre dentro do canal TLS criado pelo PEAP dentro da primeira fase do processo de autenticação de PEAP. Os NP autenticam o cliente Wireless com EAP-MS-CHAP v2. O REGAÇO e as mensagens dianteiras do controlador somente entre o cliente Wireless e o servidor Radius. O controlador do Wireless LAN (WLC) e o REGAÇO não podem decifrar estas mensagens porque não é o ponto final TLS.

A sequência do mensagem de RADIUS para uma tentativa da autenticação bem sucedida (onde o usuário forneceu credenciais senha-baseadas válidas com o PEAP-MS-CHAP v2) é:

1. Os NP enviam um mensagem request da identidade ao cliente: `EAP-pedido/identidade`.
2. O cliente responde com um mensagem de resposta da identidade: `EAP-resposta/identidade`.
3. Os NP enviam um mensagem de desafio MS-CHAP v2: `EAP-Request/EAP-Type=EAP MS-CHAP-V2 (desafio)`.
4. O cliente responde com um desafio e resposta MS-CHAP v2: `EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (resposta)`.
5. Os NP enviam para trás um pacote do sucesso MS-CHAP v2 quando o server autenticou com sucesso o cliente: `EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (sucesso)`.
6. O cliente responde com um pacote do sucesso MS-CHAP v2 quando o cliente autenticou com sucesso o server: `EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (sucesso)`.
7. Os NP enviam um EAP-tipo-comprimento-valor (TLV) que indique a autenticação bem sucedida.
8. O cliente responde com um mensagem de sucesso do estado EAP-TLV.
9. O server termina a autenticação e envia uma mensagem do EAP-sucesso no texto simples. Se os VLAN são distribuídos para o isolamento do cliente, os atributos VLAN estão incluídos nesta mensagem.

Configurar

Nesta seção, você é presentado com a informação para configurar PEAP-MS-CHAP v2.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Essa configuração utiliza esta configuração de rede:

Nesta instalação, um server de Microsoft Windows 2008 executa estes papéis:

- Controlador de domínio para o domínio wireless.com
- Server DHCP/DNS
- Server de CA
- NP? para autenticar os usuários Wireless
- Diretório ativo? para manter a base de dados de usuário

O server conecta à rede ligada com fio através de um switch de Camada 2 como mostrado. O WLC e o REGAÇO registrado igualmente conectam à rede através do switch de Camada 2.

Os clientes Wireless usam o acesso protegido por wi-fi 2 (WPA2) - autenticação PEAP-MS-CHAP v2 para conectar à rede Wireless.

Configurações

O objetivo deste exemplo é configurar o server de Microsoft 2008, o controlador do Wireless LAN, e o AP de pouco peso para autenticar os clientes Wireless com autenticação PEAP-MS-CHAP v2. Há três etapas principal neste processo:

1. Configurar o server de Microsoft Windows 2008.
2. Configurar o WLC e os AP de pouco peso.
3. Configurar os clientes Wireless.

Configurar o server de Microsoft Windows 2008

Neste exemplo, uma configuração completa do server de Microsoft Windows 2008 inclui estas etapas:

1. Configurar o server como um controlador de domínio.
2. Instale e configurar serviços DHCP.
3. instale e configurar o server como um server de CA.
4. Conecte clientes ao domínio.
5. Instale os NP.
6. Instale um certificado.
7. Configurar os NP para a autenticação de PEAP.
8. Adicionar usuários ao diretório ativo.

Configurar o server de Microsoft Windows 2008 como um controlador de domínio

Termine estas etapas a fim configurar o server de Microsoft Windows 2008 como um controlador de domínio:

1. Clique o **começo** > o **gerenciador do servidor**.

2. Clique **papéis do >** Add dos **papéis**.

3. Clique em Next.

4. Selecione os **serviços do domínio do diretório ativo do** serviço, e clique-os **em seguida**.

5. Reveja a introdução aos serviços do domínio do diretório ativo, e clique-a **em seguida**.

6. O clique **instala** para começar o processo de instalação.

   A instalação continua e termina.

7. Clique **perto este assistente e lance o wizard de instalação dos serviços do domínio do diretório ativo (dcpromo.exe)** para continuar a instalação e a configuração do diretório ativo.

8. Clique **ao lado de** executam o wizard de instalação dos serviços do domínio do diretório ativo.

9. Reveja a informação no sistema operacional Compatbilty, e clique-a **em seguida**.

10. O clique **cria um domínio novo em uma floresta nova > em seguida** a fim criar um domínio novo.

11. Dê entrada com o nome de DNS completo para o domínio novo (wireless.com neste exemplo), e clique-o em seguida.

12. Selecione o nível funcional da floresta para seu domínio, e clique-o **em seguida**.

13. Selecione o nível funcional do domínio para seu domínio, e clique-o **em seguida**.

14. Assegure-se de que o servidor DNS esteja selecionado, e se clique **em seguida**.

15. Clique **sim** para que o wizard de instalação crie uma zona nova no DNS para o domínio.

16. Selecione os dobradores que o diretório ativo deve se usar para seus arquivos, e clique-os **em seguida**.

17. Incorpore a senha de administrador, e clique-a **em seguida**.

18. Reveja suas seleções, e clique-as **em seguida**.

    Os rendimentos da instalação.

19. **Revestimento do** clique para fechar o assistente.

20. Reinicie o server para que as mudanças tomem o efeito.

Instale e configurar serviços DHCP no server de Microsoft Windows 2008

O serviço DHCP no server de Microsoft 2008 é usado para fornecer endereços IP de Um ou Mais Servidores Cisco ICM NT aos clientes Wireless. Termine estas etapas a fim instalar e configurar serviços DHCP:

1. Clique o **começo** > o **gerenciador do servidor**.

2. Clique **papéis do >** Add dos **papéis**.

3. Clique em Next.

4. Selecione o **servidor DHCP do** serviço, e clique-o **em seguida**.

5. Reveja a introdução ao servidor DHCP, e clique-a **em seguida**.

6. Selecione a relação que o servidor DHCP deve monitorar para pedidos, e clique-a **em seguida**.

7. Configurar os ajustes que do padrão DNS o servidor DHCP deve fornecer aos clientes, e clique-os **em seguida**.

8. Configurar VITÓRIAS se a rede apoia VITÓRIAS.

9. O clique **adiciona** para usar o assistente para criar um escopo de DHCP ou o clique **ao lado de** cria um escopo de DHCP mais tarde. Clique em Avançar para continuar.

10. Permita ou desabilite o apoio DHCPv6 no server, e clique-o **em seguida**.

11. Configurar ajustes do IPv6 DNS se DHCPv6 foi permitido no passo precedente. Clique em Avançar para continuar.

12. Forneça credenciais do administrador de domínio para autorizar o servidor DHCP no diretório ativo, e clique-as **em seguida**.

13. Reveja a configuração na página da confirmação, e o clique **instala** para terminar a instalação.

    Os rendimentos da instalação.

14. O clique **perto de** fecha o assistente.

    O servidor DHCP é instalado agora.

15. Clique o **Iniciar > Ferramentas Administrativas** > o **DHCP** para configurar o serviço DHCP.

16. Expanda o servidor DHCP (win-mvz9z2umms.wireless.com neste exemplo), clicar com o botão direito o IPv4, e escolha o **espaço novo**. para criar um escopo de DHCP.

17. O clique **ao lado de** configura o espaço novo através do wizard de escopo novo.

18. Forneça um nome para o espaço novo (clientes Wireless neste exemplo), e clique-o **em seguida**.

19. Incorpore a escala dos endereços IP de Um ou Mais Servidores Cisco ICM NT disponíveis que podem ser usados para aluguéis de DHCP. Clique em Avançar para continuar.

20. Crie uma lista opcional de endereços excluídos. Clique em Avançar para continuar.

21. Configurar o Lease Time, e clique-o **em seguida**.

22. Clique **sim, eu quero configurar agora estas opções**, e clico **em seguida**.

23. Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do gateway padrão para este espaço, clique **adicionam > em seguida**.

24. Configurar o Domain Name e o servidor DNS DNS a ser usados pelos clientes. Clique em Avançar para continuar.

25. Incorpore a informação das VITÓRIAS para este espaço se a rede apoia VITÓRIAS. Clique em Avançar para continuar.

26. Para ativar este espaço, clique **sim, mim querem ativar agora > em seguida este espaço**.

27. Clique o **revestimento** para terminar e fechar o assistente.

Instale e configurar o server de Microsoft Windows 2008 como um server de CA

O PEAP com EAP-MS-CHAP v2 valida o servidor Radius baseado no certificado atual no server. Adicionalmente, o certificado de servidor deve ser emitido por um público CA que seja confiado pelo computador de cliente (isto é, o certificado de CA público já existe no dobrador da Autoridade de certificação de raiz confiável na loja do certificado do computador de cliente).

Termine estas etapas a fim configurar o server de Microsoft Windows 2008 como um server de CA que emita o certificado aos NP:

1. Clique o **começo** > o **gerenciador do servidor**.

2. Clique **papéis do** > Add dos **papéis**.

3. Clique em Next.

4. Selecione os **serviços certificados de diretório ativo do** serviço, e clique-os **em seguida**.

5. Reveja a introdução aos serviços certificados do diretório ativo, e clique-a **em seguida**.

6. Selecione o **Certificate Authority**, e clique-o **em seguida**.

7. Selecione a **empresa**, e clique-a **em seguida**.

8. Selecione a **CA raiz**, e clique-a **em seguida**.

9. Seleto **crie uma chave privada nova**, e clique-a **em seguida**.

10. Clique **em seguida em** configurar a criptografia para CA.

11. O clique **ao lado de** aceita o Common Name do padrão para este CA.

12. Selecione o intervalo de tempo que este certificado de CA é válido, e clique-o **em seguida**.

13. O clique **ao lado de** aceita a localização do base de dados do certificado do padrão.

14. Reveja a configuração, e o clique **instala** para enfiar os serviços certificados do diretório ativo.

15. Depois que a instalação é terminada, **fim do** clique.

Conecte clientes ao domínio

Termine estas etapas a fim conectar os clientes à rede ligada com fio e transferir a informação específica do domínio do domínio novo:

1. Conecte os clientes à rede ligada com fio com um cabo do Ethernet direto reto.
2. Carreg acima do cliente, e do início de uma sessão com o nome de usuário do cliente e a senha.
3. Clique o **Iniciar > Executar**, entre no **Cmd**, e clique a **APROVAÇÃO**.
4. No comando prompt, entre no **ipconfig**, e o clique **entra** para verificar que o DHCP trabalha corretamente e que o cliente recebeu um endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor DHCP.
5. A fim juntar-se ao cliente ao domínio, ao **começo do** clique, clicar com o botão direito o **computador**, escolher **propriedades**, e escolher **ajustes da mudança no** direita inferior.
6. **Mudança do** clique.
7. Clique o **domínio**, entre em **wireless.com**, e clique a **APROVAÇÃO**.

8. Incorpore o **administrador** username e o específico da senha ao domínio a que o cliente se junta. Esta é a conta de administrador no diretório ativo no server.

9. **APROVAÇÃO do** clique, e **APROVAÇÃO do** clique outra vez.

10. Clique **próximo > reinício agora** para reiniciar o computador.
11. Uma vez que o computador reinicia, entre com esta informação: Username = administrador; Password> da senha = do <domain; Domínio = Sem fio.
12. Clique o **começo**, clicar com o botão direito o **computador**, escolha **propriedades**, e escolha **ajustes da mudança no** direita inferior verificar que você está no domínio de wireless.com.
13. A próxima etapa é verificar que o cliente recebeu o certificado de CA (confiança) do server.

14. Clique o **começo**, incorpore o **mmc**, e pressione-o **entram**.
15. Clique o **arquivo**, e o clique **adiciona/remove pressão-**em.
16. Escolha **Certificados**, e o clique **adiciona**.

17. **Conta do computador do** clique, e clique **em seguida**.

18. **Computador local do** clique, e clique **em seguida**.

19. Clique em **OK**.
20. Expanda os dobradores dos **Certificados (computador local)** e das **Autoridades de certificação de raiz confiável**, e clique **Certificados**. Encontre o **CERT de CA do domínio Wireless na** lista. Neste exemplo, o CERT de CA é chamado wireless-WIN-MVZ9Z2UMNMS-CA.

21. Repita este procedimento para adicionar mais clientes ao domínio.

Instale o server da política de rede no server de Microsoft Windows 2008

Nesta instalação, os NP são usados como um servidor Radius para autenticar clientes Wireless com autenticação de PEAP. Termine estas etapas a fim instalar e configurar NP no server de Microsoft Windows 2008:

1. Clique o **começo** > o **gerenciador do servidor**.

2. Clique **papéis do** > Add dos **papéis**.

3. Clique em Next.

4. Selecione os **serviços da política de rede e do acesso do** serviço, e clique-os **em seguida**.

5. Reveja a introdução aos serviços da política de rede e do acesso, e clique-a **em seguida**.

6. Selecione o **server da política de rede**, e clique-o **em seguida**.

7. Reveja a confirmação, e o clique **instala**.

Depois que a instalação é terminada, uma tela similar a esta está indicada.

8. Clique em Close.

Instale um certificado

Termine estas etapas a fim instalar o certificado do computador para os NP:

1. Clique o **começo**, incorpore o **mmc**, e pressione-o **entram**.
2. O > Add do **arquivo do** clique**/remove Pressão-em**.
3. Escolha **Certificados**, e o clique **adiciona**.

4. Escolha a **conta do computador**, e clique-a **em seguida**.

5. Selecione o **computador local**, e clique o **revestimento**.

6. Clique a **APROVAÇÃO** para retornar ao Microsoft Management Console (MMC).

7. Expanda os **Certificados (computador local)** e **pastas pessoal**, e clique **Certificados**.

8. Clicar com o botão direito no whitespace abaixo do certificado de CA, e escolha **todas as tarefas > certificado novo do pedido**.

9. Clique em Next.

10. Selecione o **controlador de domínio**, e o clique **registra-se**.

11. **Revestimento do** clique uma vez que o certificado é instalado.

O certificado NP é instalado agora.

12. Assegure-se de que a finalidade pretendida do certificado leia a **authenticação do cliente, autenticação de servidor**.

Configurar o serviço do servidor da política de rede para a autenticação PEAP-MS-CHAP v2

Termine estas etapas a fim configurar os NP para a autenticação:

1. Clique o **Iniciar > Ferramentas Administrativas** > o **server da política de rede**.
2. Clicar com o botão direito os **NP (locais)**, e escolha o **server do registro no diretório ativo**.

3. Clique em **OK**.

4. Clique em **OK**.

5. Adicionar o controlador do Wireless LAN como um cliente do Authentication, Authorization, and Accounting (AAA) nos NP.
6. Expanda **clientes RADIUS e server**. Clicar com o botão direito **clientes RADIUS**, e escolha o **cliente RADIUS novo**.

7. Incorpore um nome amigável (WLC neste exemplo), o endereço IP de gerenciamento do WLC (192.168.162.248 neste exemplo) e um segredo compartilhado. O mesmo segredo compartilhado é usado para configurar o WLC.

8. Clique a **APROVAÇÃO** para retornar à tela precedente.

9. Crie uma política de rede nova para usuários Wireless. Expanda **políticas**, clicar com o botão direito **políticas de rede**, e escolha **novo**.

10. Dê entrada com um nome da política para esta regra (Sem fio PEAP neste exemplo), e clique-o **em seguida**.

11. Para mandar esta política permitir somente usuários do domínio Wireless, adicionar estas três circunstâncias, e clique-as **em seguida**:

    - Grupos de Windows - Usuários de domínio
    - Tipo de porta NAS - Sem fio - IEEE 802.11
    - Tipo do autenticação - EAP

12. **O acesso do** clique **concedido** para conceder as tentativas de conexão que combinam esta política, e clica **em seguida**.

13. Desabilite todos os métodos de autenticação sob métodos de autenticação menos seguros.

14. O clique **adiciona**, PEAP seleto, e **APROVAÇÃO do** clique para permitir o PEAP.

15. Selecione **Microsoft: O EAP protegido (PEAP)**, e o clique **editam**. Assegure que o certificado previamente criado do controlador de domínio está selecionado na lista de drop-down emitida certificado, e clique a **aprovação**.

16. Clique em Next.

17. Clique em Next.

18. Clique em Next.

19. Clique em Finish.

Adicionar usuários ao diretório ativo

Neste exemplo, a base de dados de usuário é mantida no diretório ativo. Termine estas etapas a fim adicionar usuários ao base de dados do diretório ativo:

1. Abra usuários e computadores de diretório ativo. Clique o **Iniciar > Ferramentas Administrativas** > os **usuários e os computadores de diretório ativo**.
2. Na árvore de console dos usuários e dos computadores de diretório ativo, expanda o domínio, clicar com o botão direito **usuários > novo**, e escolha o **usuário**.
3. No objeto novo? A caixa de diálogo do usuário, dá entrada com o nome do usuário Wireless. Este exemplo usa o cliente1 do nome no campo de nome e o cliente1 no campo de nome de logon do usuário. Clique em Next.

4. No objeto novo? A caixa de diálogo do usuário, incorpora uma senha de sua escolha à senha e confirma campos de senha. Desmarcar o **usuário deve mudar a senha na** caixa de verificação **seguinte do fazer logon**, e clicam **em seguida**.

5. No objeto novo? Caixa de diálogo do usuário, **revestimento do** clique.

6. Repita etapas 2 a 4 a fim criar contas de usuário adicionais.

Configurar o controlador e os regaços do Wireless LAN

Configurar os dispositivos Wireless (os controladores e os regaços do Wireless LAN) para esta instalação.

Configurar o WLC para a autenticação RADIUS

Configurar o WLC para usar os NP como o Authentication Server. O WLC deve ser configurado a fim enviar as credenciais do usuário a um servidor de raio externo. O servidor de raio externo então valida as credenciais do usuário e fornece o acesso aos clientes Wireless.

Termine estas etapas a fim adicionar os NP como um servidor Radius na página da **Segurança** > da **autenticação RADIUS**:

1. Escolha a **Segurança** > o **RAIO** > a **autenticação da** relação do controlador para indicar a página dos servidores de autenticação RADIUS. Clique **novo** a fim definir um servidor Radius.

2. Defina os parâmetros do servidor Radius. Estes parâmetros incluem o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius, o segredo compartilhado, o número de porta, e o status de servidor. O usuário de rede e as caixas de verificação de gerenciamento determinam se a autenticação Raio-baseada se aplica aos usuários do Gerenciamento e da rede (Sem fio). Este exemplo usa os NP como o servidor Radius com

um endereço IP de Um ou Mais Servidores Cisco ICM NT de 192.168.162.12. Clique em Apply.

Configurar um WLAN para os clientes

Configurar o conjunto de serviço mais identfier (SSID) (WLAN) a que os clientes Wireless conecta. Neste exemplo, crie o SSID, e nomeie-o PEAP.

Defina a autenticação da camada 2 como o WPA2 de modo que os clientes executem a autenticação EAP-baseada (PEAP-MS-CHAP v2 neste exemplo) e usem o Advanced Encryption Standard (AES) como o mecanismo de criptografia. Deixe todos valores restantes em seus padrões.

Nota: Este documento liga o WLAN com as interfaces de gerenciamento. Quando você tem vlan múltiplos em sua rede, você pode criar um VLAN separado e ligá-lo ao SSID. Para obter informações sobre de como configurar VLAN em WLC, refira VLAN no exemplo de configuração dos controladores do Wireless LAN.

Termine estas etapas a fim configurar um WLAN no WLC:

1. Clique **WLAN da** relação do controlador a fim indicar a página WLAN. Esta página alista os WLAN que existem no controlador.
2. Escolha **novo** a fim criar um WLAN novo. Incorpore o ID de WLAN e o WLAN SSID para o WLAN, e o clique **aplica-se**.

3. Para configurar o SSID para o 802.1x, termine estas etapas: Clique o **tab geral** e permita o WLAN.

   Clique as abas da **Segurança** > da **camada 2**, ajuste a Segurança da camada 2 a **WPA + WPA2**, verifique os boxesas da verificação dos parâmetros WPA+WPA2 (por exemplo, WPA2 AES) necessários, e clique o **802.1x** como o Gerenciamento de chave de autenticação.

   Clique as abas da **Segurança** > dos **servidores AAA**, escolha o endereço IP de Um ou Mais Servidores Cisco ICM NT dos NP da lista de drop-down do **servidor1**, e o clique **aplica-se**.

Configurar os clientes Wireless para a autenticação PEAP-MS-CHAP v2

Termine estas etapas para configurar o cliente Wireless com Windows zero ferramentas da configuração para conectar ao PEAP WLAN.

1. Clique o **ícone de rede na** barra de tarefas. Clique o **PEAP** SSID, e o clique **conecta**.

2. O cliente deve agora ser conectado à rede.

3. Se a conexão falha, tente reconectar ao WLAN. Se a edição persiste, refira a seção da pesquisa de defeitos.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Se seu cliente não conectou ao WLAN, esta seção fornece a informação que você pode se usar para pesquisar defeitos a configuração.

Há duas ferramentas que podem ser usadas para diagnosticar falhas de autenticação do 802.1x: **o comando client debugar** e o **visualizador de eventos em** Windows.

Executando um cliente debugar do WLC não é repleto de recursos e não faz serviço do imnpact. Para começar uma sessão debugar, para abrir o comando line interface(cli) do WLC, e para entrá-lo **debugar o endereço MAC de cliente**, onde o MAC address é o MAC address wireless do cliente Wireless que é incapaz de conectar. Quando isto debugar corridas, tente conectar o cliente; lá deve ser output no CLI do WLC que olha similar a este exemplo:

Este é um exemplo de uma edição que poderia ocorrer com um misconfiguration. Aqui, o WLC debuga mostras que o WLC se moveu no estado de autenticação, que significa que o WLC está esperando uma resposta dos NP. Isto é geralmente devido a um segredo compartilhado incorreto no WLC ou nos NP. Você pode confirmar este através do visualizador de eventos de Windows Server. Se você não encontra um log, o pedido nunca fê-lo aos NP.

Um outro exemplo que seja encontrado do WLC debuga é uma rejeição de acesso. Uma rejeição de acesso mostra que os NP receberam e rejeitaram as credenciais do cliente. Este é um exemplo de um cliente que recebe uma rejeição de acesso:

Quando você vê uma rejeição de acesso, verifique entra os log de eventos de Windows Server para determinar porque os NP responderam ao cliente com uma rejeição de acesso.

Uma autenticação bem sucedida manda uma aceitação de acesso no cliente debugar, como visto neste exemplo:

Pesquisar defeitos rejeições de acesso e timeouts de resposta exige o acesso ao servidor Radius. O WLC atua como um autenticador que passe mensagens EAP entre o cliente e o servidor Radius. Um servidor Radius que responde com uma rejeição de acesso ou um timeout de resposta deve ser examinado e diagnosticado pelo fabricante do serviço de raio.

Nota: O TAC não fornece o Suporte técnico para servidores Radius da terceira; contudo, entra o servidor Radius explicam geralmente porque um pedido do cliente foi rejeitado ou ignorado.

A fim pesquisar defeitos rejeições de acesso e timeouts de resposta dos NP, examine os NP entra o visualizador de eventos de Windows no server.

1. Clique o **Ferramentas > Visualizador de Evento do começo >** do **administrador** para ligar o visualizador de eventos e para rever os logs NP.
2. Expanda **vistas > papéis do servidor >** a **política de rede e o acesso feitos sob encomenda**.

Nesta seção da opinião do evento, há uns logs do passado e autenticações falha. Examine estes logs para pesquisar defeitos porque um cliente não está passando a autenticação. Passado e as autenticações falha aparecem como informativo. O rolo através dos logs para encontrar o username que tem a autenticação falha e recebe uma rejeição de acesso de acordo com o WLC debuga.

Este é um exemplo dos NP que negam um acesso de usuário:

Ao rever uma instrução de negação no visualizador de eventos, examine a seção dos detalhes da autenticação. Neste exemplo, você pode ver que os NP negaram o acesso de usuário devido a um nome de usuário incorreto:

A opinião do evento nos NP igualmente ajuda com Troubleshooting se o WLC não recebe uma resposta para trás dos NP. Isto é causado geralmente por um segredo compartilhado incorreto entre os NP e o WLC.

Neste exemplo, os NP rejeitam o pedido do WLC devido a um segredo compartilhado incorreto:

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems