Sem fio BYOD com Identity Services Engine

Índice

Introdução

O Cisco Identity Services Engine (ISE) é o servidor da política da próxima geração de Cisco que fornece a infraestrutura da authentication e autorização à solução de Cisco TrustSec. Igualmente proporciona outros dois serviços críticos:

- O primeiro serviço é fornecer uma maneira de perfilar o tipo de dispositivo de ponto final baseado automaticamente em atributos que Cisco ISE recebe dos vários origens de informação. Este serviço (chamado Perfilador) fornece funções equivalentes ao que Cisco tem oferecido previamente com o dispositivo do Cisco NAC Profiler.
- Um outro serviço importante que Cisco ISE proporcione é fazer a varredura da conformidade do valor-limite; por exemplo, instalação de software AV/AS e sua validez do arquivo de definição (conhecidas como a postura). Cisco tem fornecido previamente esta função exata da postura somente a ferramenta NAC de Cisco.

Cisco ISE fornece um nível equivalente da funcionalidade, e é integrado com mecanismos da autenticação do 802.1X.

Cisco ISE integrado com controladores do Wireless LAN (WLC) pode fornecer o perfilamento de mecanismos dos dispositivos móveis tais como iDevices de Apple (iPhone, iPad, e iPod), Android-baseou smartphones, e outro. Para usuários do 802.1X, Cisco ISE pode fornecer o mesmo nível dos serviços tais como o perfilamento e a exploração da postura. Os serviços do convidado em Cisco ISE podem igualmente ser integrados com Cisco WLC reorientando pedidos da autenticação da Web a Cisco ISE para a autenticação.

Este documento introduz a solução Wireless para Bring Your Own Device (BYOD), como o fornecimento do acesso diferenciado baseado em valores-limite conhecidos e na política de usuário. Este documento não fornece a solução completa de BYOD, mas servir-la para demonstrar um exemplo simples do uso do acesso dinâmico. Outros exemplos de configuração incluem usando o portal do patrocinador ISE, onde um usuário privilegiado pode patrocinar um convidado para o acesso wireless do convidado do abastecimento.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Controlador de LAN 2504 ou 2106 do Cisco Wireless com versão de software 7.2.103
- Portas do catalizador 3560 – 8
- WLC 2504
- Identity Services Engine 1.0MR (versão da imagem do server de VMware)
- Server de Windows 2008 (imagem de VMware) — 512M, disco 20GBDiretório ativoDNSDHCPServiços certificados

Topologia

Convenções

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

RAIO NAC do controlador do Wireless LAN e vista geral CoA

Este ajuste permite o WLC de procurar os pares AV da reorientação URL que vêm do servidor Radius ISE. Isto está somente em um WLAN que seja amarrado a uma relação com o ajuste do RAIO NAC permitido. Quando o par Cisco AV para a reorientação URL é recebido, o cliente está posto no estado POSTURE_REQD. Este é basicamente o mesmo como o estado WEBAUTH_REQD internamente no controlador.

Quando o servidor Radius ISE julga o cliente é Posture_Compliant, ele emite um CoA ReAuth. O Session_ID é usado para amarrá-lo junto. Com este AuthC novo (re-AUTH) não envia os pares AV URL-Redirec. Porque não há nenhuma URL reoriente pares AV, o WLC sabe que o cliente não exige a postura mais por muito tempo.

Se o ajuste do RAIO NAC não é permitido, o WLC ignora a URL reorienta VSA.

CoA-ReAuth: Isto é permitido com o ajuste do RFC 3576. A capacidade de ReAuth foi adicionada aos comandos existentes CoA que foram apoiados previamente.

O ajuste do RAIO NAC é mutuamente exclusivos desta capacidade, embora se exija para que o CoA trabalhe.

PRE-postura ACL: Quando um cliente está no estado POSTURE_REQ, o comportamento padrão do WLC é obstruir todo o tráfego exceto DHCP/DNS. A PRE-postura ACL (que é chamado no par AV URL-reorientar-ACL) é aplicada ao cliente, e o que é permitido nesse ACL é o que o cliente pode alcançar.

PRE-AUTH ACL contra a ultrapassagem VLAN: Uma quarentena ou um AuthC VLAN que sejam diferentes do Acesso-VLAN não são apoiados em 7.0MR1. Se você ajusta um VLAN do servidor da política, será o VLAN para a sessão inteira. Nenhuma alteração de VLAN é precisada após primeiro AuthZ.

RAIO NAC do controlador do Wireless LAN e fluxo da característica CoA

A figura abaixo fornece detalhes da troca da mensagem quando o cliente é autenticado à validação do servidor backend e da postura NAC.

1. O cliente autentica usando a autenticação do dot1x.
2. O acesso radius aceita leva a URL reorientada para a porta 80 e o PRE-AUTH ACL que inclui permitir endereços IP de Um ou Mais Servidores Cisco ICM NT e portas, ou a quarentena VLAN.
3. O cliente estará reorientado à URL fornecida no acesso aceita, e põe em um estado novo até que a validação da postura esteja feita. O cliente neste estado fala ao server ISE e valida-se contra as políticas configuradas no server ISE NAC.
4. O agente NAC no cliente inicia a validação da postura (tráfego à porta 80): O agente envia o pedido da descoberta HTTP à porta 80 que o controlador reorienta à URL fornecida no acesso aceita. O ISE sabe que cliente que tenta alcançar e responde diretamente ao cliente. Esta maneira que o cliente aprende sobre o IP de servidor ISE e a partir de agora, o cliente fala diretamente com o server ISE.
5. O WLC permite este tráfego porque o ACL é configurado para permitir este tráfego. Em caso da ultrapassagem VLAN, o tráfego é construído uma ponte sobre de modo que alcance o server ISE.
6. Uma vez que o ISE-cliente termina a avaliação, um CoA-req do RAIO com serviço do reauth está enviado ao WLC. Isto inicia a reautenticação do cliente (enviando o EAP START). Uma vez que a reautenticação sucede, o ISE envia o acesso aceita com um ACL novo (eventualmente) e nenhuma URL reorienta, ou alcança o VLAN.
7. O WLC tem o apoio para o CoA-req e o Disconexão-req conforme o RFC 3576. O WLC precisa de apoiar o CoA-req para o serviço do re-AUTH, conforme o RFC 5176.
8. Em vez dos ACL carregável, os ACL PRE-configurados são usados no WLC. O server ISE apenas envia o nome ACL, que é configurado já no controlador.
9. Este projeto deve trabalhar para casos VLAN e ACL. Em caso da ultrapassagem VLAN, nós apenas reorientamos a porta 80 somos reorientados e permitimos o resto (da ponte) do tráfego na quarentena VLAN. Para o ACL, o PRE-AUTH ACL recebido no acesso aceita é aplicado.

Esta figura fornece uma representação visual deste fluxo da característica:

ISE que perfila a vista geral

O serviço do perfilador de Cisco ISE fornece a funcionalidade em descobrir, em encontrar, e em determinar as capacidades de todos os valores-limite anexados em sua rede, apesar de seus tipos de dispositivo, a fim assegurar e manter o acesso apropriado a sua rede de empreendimento. Recolhe primeiramente um atributo ou um grupo de atributos de todos os valores-limite em sua rede e classifica-os de acordo com seus perfis.

O perfilador é compreendido destes componentes:

- O sensor contém um número de pontas de prova. As pontas de prova capturam pacotes de rede perguntando dispositivos do acesso de rede, e enviam os atributos e seus valores de atributo que são recolhidos dos valores-limite ao analisador.
- Um analisador avalia valores-limite usando as políticas configuradas e os grupos da identidade para combinar os atributos e seus valores de atributo recolhidos, que classifique valores-limite ao grupo especificado e armazene valores-limite com o perfil combinado no

base de dados de Cisco ISE.

Para a detecção do dispositivo móvel, é recomenda usar uma combinação destas pontas de prova para a identificação de dispositivo apropriada:

- RAIO (Chamar-Estação-ID): Fornece o MAC address (o OUI)
- DHCP (hostname): Hostname – o hostname de padrão pode incluir o tipo de dispositivo; por exemplo: jsmith-ipad
- DNS (consulta reversa IP): O FQDN - hostname de padrão pode incluir o tipo de dispositivo
- HTTP (agente de usuário): Detalhes no tipo de dispositivo móvel específico

Neste exemplo de um iPad, o perfilador captura a informação do navegador da Web do atributo do agente de usuário, assim como outros atributos HTTP dos mensagens request, e adicionar-los à lista de atributos do valor-limite.

Crie usuários internos da identidade

O diretório ativo MS (AD) não é exigido para um proof-of-concept simples. O ISE pode ser usado como a única loja da identidade, que inclui a diferenciação do acesso de usuários para o acesso e o controle de política granulado.

Na liberação de ISE 1.0, usando a integração AD, o ISE pode usar grupos AD em políticas da autorização. Se a loja do usuário interno ISE está usada (nenhuma integração AD), os grupos não podem ser usados nas políticas conjuntamente com grupos da identidade do dispositivo (erro identificado a ser resolvido em ISE 1.1). Consequentemente, somente os usuários individuais podem ser diferenciados, como empregados ou contratantes quando usados além do que grupos da identidade do dispositivo.

Conclua estes passos:

1. Abra uma janela de navegador ao endereço de https://ISEip.
2. Navegue à **administração > ao Gerenciamento de identidades > às identidades**.
3. Selecione **usuários**, a seguir clique-os **adicionam** (usuário do acesso de rede). Incorpore estes valores de usuário e atribua-os ao grupo do empregado:Nome: empregadoSenha: XXXX
4. Clique em Submit.Nome: contratanteSenha: XXXX
5. Confirme ambas as contas são criados.

Adicionar o controlador do Wireless LAN ao ISE

Todo o dispositivo que iniciar requisições RADIUS ao ISE deve ter uma definição no ISE. Estes dispositivos de rede são definidos com base em seu endereço IP de Um ou Mais Servidores Cisco ICM NT. As definições do dispositivo de rede ISE podem especificar os intervalos de endereço IP que permitem assim que a definição represente dispositivos reais múltiplos.

Além do que é exigida para uma comunicação do RAIO, as definições do dispositivo de rede ISE contêm ajustes para a outra comunicação ISE/device, tal como o SNMP e o SSH.

Um outro aspecto importante da definição do dispositivo de rede está agrupando apropriadamente dispositivos de modo que este que agrupa possa ser leveraged na política do acesso de rede.

Neste exercício, as definições de dispositivo exigidas para seu laboratório são configuradas.

Conclua estes passos:

1. Do ISE vá à **administração > aos recursos de rede > aos dispositivos de rede**.
2. Dos dispositivos de rede, o clique **adiciona**. Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT, mascare o ajuste da autenticação da verificação, a seguir incorpore “Cisco” para o segredo compartilhado.
3. Salvar a entrada WLC, e confirme o controlador na lista.

Configurar o ISE para a autenticação wireless

O ISE precisa de ser configurado para clientes Wireless de autenticação do 802.1x e de usar o diretório ativo como a loja da identidade.

Conclua estes passos:

1. Do ISE navegue à **política > à autenticação**.
2. Clique para expandir o dot1x > o Wired_802.1X (-).
3. Clique sobre o ícone da engrenagem **para adicionar a condição da biblioteca**.
4. Da gota-para baixo da seleção da circunstância, escolha a **condição composta > o Wireless_802.1X**.
5. Ajuste a condição expressa a **OU**.
6. Expanda após permitem a opção dos protocolos, e aceitam os usuários internos do padrão (padrão).
7. Deixe tudo outro no padrão. Clique a **salvaguarda** para terminar as etapas.

Amarre o controlador do Wireless LAN

Conectando o WLC a uma rede

Um guia de distribuição do controlador do Wireless LAN de Cisco2500 está igualmente disponível no guia de distribuição wireless do controlador do Cisco 2500 Series.

Configurar o controlador que usa o assistente Startup

```
(Cisco Controller)
 Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup
 Would you like to terminate autoinstall? [yes]: yes AUTO-INSTALL: process terminated
-- no configuration loaded System Name [Cisco_d9:24:44] (31 characters max):
   ISE-Podx Enter Administrative User Name (24 characters max): admin
   Enter Administrative Password
   (3 to 24 characters): Cisco123
   Re-enter Administrative Password: Cisco123
Management Interface IP Address: 10.10.10.5
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.10.10.10
```

```
 Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: ISE
 Network Name (SSID): PODx
Configure DHCP Bridging Mode [yes][NO]: no
Allow Static IP Addresses [YES][no]: no
 Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
 Enter Country Code list (enter 'help' for a list of countries) [US]: US

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes
 Configure a NTP server now? [YES][no]: no
Configure the ntp system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: mm/dd/yy
Enter the time in HH:MM:SS format: hh:mm:ss
Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
 Configuration saved!
 Resetting system with new configuration...
Restarting system.
```

Configuração do switch vizinho

O controlador é conectado à porta Ethernet no switch confinante (Fast Ethernet 1). A porta do switch vizinho é configurada como um tronco 802.1Q e permite todos os VLAN no tronco. O VLAN nativo 10 permite que a interface de gerenciamento do WLC seja conectada.

A configuração de porta do 802.1Q Switch é como segue:

```
switchport
switchport trunk encapsulation dot1q
switchport trunk native VLAN 10
switchport mode trunk
end
```

Adicionar os Authentication Server (ISE) ao WLC

O ISE precisa de ser adicionado ao WLC a fim permitir o 802.1X e a característica CoA para pontos finais Wireless.

Conclua estes passos:

1. Abra um navegador, a seguir conecte-o à vagem WLC (que usa o HTTP seguro) > https://wlc.
2. Navegue a **Security > Authentication > novo**.
3. Incorpore estes valores:Endereço IP do servidor: 10.10.10.70 (atribuição da verificação)Segredo compartilhado: ciscoApoio para o RFC 3576 (CoA): Permitido (padrão)Tudo mais: Padrão
4. O clique **aplica-se** para continuar.
5. Selecione o **> Add da contabilidade do RAIO NOVO**.
6. Incorpore estes valores:Endereço IP do servidor: 10.10.10.70Segredo compartilhado: ciscoTudo mais: Padrão
7. O clique **aplica**, a seguir salvar a configuração para o WLC.

Crie a interface dinâmica do empregado WLC

Termine estas etapas a fim adicionar uma interface dinâmica nova para o WLC e traçá-la ao empregado VLAN:

1. Do WLC, navegue ao **controlador > às relações**. Então, clique **novo**.
2. Do WLC, navegue ao **controlador > às relações**. Entre no seguinte:Nome da relação: EmpregadoIdentificação VLAN: 11
3. Entre no seguinte para a relação do empregado:Número de porta: 1Identificador de VLAN: 11Endereço IP: 10.10.11.5Máscara de rede: 255.255.255.0Gateway: 10.10.11.1DHCP: 10.10.10.10
4. Confirme que a interface dinâmica nova do empregado está criada.

Crie a interface dinâmica do convidado WLC

Termine estas etapas a fim adicionar uma interface dinâmica nova para o WLC e traçá-la ao convidado VLAN:

1. Do WLC, navegue ao **controlador > às relações**. Então, clique **novo**.
2. Do WLC, navegue ao **controlador > às relações**. Entre no seguinte:Nome da relação: ConvidadoIdentificação VLAN: 12
3. Entre nestes para a relação do convidado:Número de porta: 1Identificador de VLAN: 12Endereço IP: 10.10.12.5Máscara de rede: 255.255.255.0Gateway: 10.10.12.1DHCP: 10.10.10.10
4. Confirme que a relação do convidado esteve adicionada.

Adicionar o 802.1x WLAN

Da tira de bota inicial do WLC, pôde ter havido um padrão WLAN criado. Em caso afirmativo, altere-o ou crie-o um WLAN novo para apoiar a autenticação wireless do 802.1X como indicado no guia.

Conclua estes passos:

1. Do WLC, navegue a **WLAN > criam novo**.
2. Para o WLAN, entre no seguinte:Nome de perfil: pod1xSSID: Mesmos
3. Para os ajustes > o tab geral WLAN, use o seguinte:Transmita por rádio a política: TodosRelação/grupo: GerenciamentoTudo mais: padrão
4. Para a aba do > segurança WLAN > a camada 2, ajuste o seguinte:Mergulhe 2 Security:WPA+WPA2Política WPA2/criptografia: Permitido/AESAUTH Mgmt chave: 802.1X
5. Para a aba > os servidores AAA do > segurança WLAN, ajuste o seguinte:O server de rádio Overwrite a relação: DesabilitadoAutenticação/servidores de contabilidade: HabilitadoServidor1: 10.10.10.70
6. Para o WLAN > o guia avançada, ajustaram o seguinte:Permita a ultrapassagem AAA: HabilitadoEstado NAC: Raio NAC (selecionado)
7. De volta ao o WLAN > o tab geral > permitem WLAN (caixa de verificação).

Teste interfaces dinâmica WLC

Você precisa de fazer uma verificação rápida para relações válidas do empregado e do convidado. Use todo o dispositivo para associar ao WLAN, a seguir mude a atribuição da relação WLAN.

1. Do WLC, navegue a **WLAN > WLAN**. Clique para editar seu SSID seguro criado no exercício mais adiantado.
2. Mude a relação/grupo de interface ao **empregado**, a seguir clique-os **aplicam-se**.
3. Se configurado corretamente, um dispositivo recebe um endereço IP de Um ou Mais Servidores Cisco ICM NT do empregado VLAN (10.10.11.0/24). Este exemplo mostra um dispositivo iOS que obtenha um endereço IP de Um ou Mais Servidores Cisco ICM NT novo.
4. Uma vez que a relação precedente foi confirmada, mude a atribuição da relação WLAN ao **convidado**, a seguir clique-a **aplicam-se**.
5. Se configurado corretamente, um dispositivo recebe um endereço IP de Um ou Mais Servidores Cisco ICM NT do convidado VLAN (10.10.12.0/24). Este exemplo mostra um dispositivo iOS que obtenha um endereço IP de Um ou Mais Servidores Cisco ICM NT novo.
6. **IMPORTANTE:** Mude a atribuição da relação de volta ao Gerenciamento original.
7. O clique **aplica** e salvar a configuração para o WLC.

Autenticação wireless para iOS (iPhone/iPad)

Associe ao WLC através de um SSID autenticado um usuário interno (ou o usuário integrada, AD) usando um dispositivo iOS tal como um iPhone, um iPad, ou um iPod. Salte estas etapas se não aplicáveis.

1. No dispositivo iOS, vá aos ajustes WLAN. Permita WIFI, a seguir selecione o SSID permitido 802.1X criado na seção anterior.
2. Forneça esta informação a fim conectar:Nome de usuário: empregado (interno – Empregado) ou contratante (interno – contratante)Senha: XXXX
3. Clique para aceitar o certificado ISE.
4. Confirme que o dispositivo iOS está obtendo um endereço IP de Um ou Mais Servidores Cisco ICM NT da relação do Gerenciamento (VLAN10).
5. No o WLC > o monitor > os clientes, verificam a informação do valor-limite que inclui o uso, o estado, e o tipo EAP.
6. Similarmente, a informação cliente pode ser fornecida por ISE > página do monitor > da autenticação.
7. Clique o ícone dos **detalhes** a fim furar para baixo à sessão para a informação detalhada da sessão.

Adicionar a postura reorientam o ACL ao WLC

A postura reorienta o ACL é configurada no WLC, onde o ISE se usará para restringir o cliente para a postura. Eficazmente e em um mínimo o ACL permite o tráfego entre o ISE. As regras opcionais podem ser adicionadas neste ACL se necessárias.

1. Navegue ao **> segurança > às listas de controle de acesso > às listas de controle de acesso**

WLC. Clique em **New**.
2. Forneça um nome (ACL-POSTURE-REDIRECT) para o ACL.
3. O clique **adiciona a regra nova** para o ACL novo. Ajuste os seguintes valores à sequência #1 ACL. O clique **aplica-se** quando terminado.Fonte: AlgunsDestino: Endereço IP 10.10.10.70, 255.255.255.255Protocolo: AlgunsAção: Licença
4. Confirme a sequência foi adicionado.
5. O clique **adiciona a regra nova**. Ajuste os seguintes valores à sequência #2 ACL. O clique **aplica-se** quando terminado.Fonte: Endereço IP 10.10.10.70, 255.255.255.255Destino: AlgunsProtocolo: AlgunsAção: Licença
6. Confirme a sequência foi adicionado.
7. Ajuste os seguintes valores à sequência #3 ACL. O clique **aplica-se** quando terminado.Fonte: AlgunsDestino: AlgunsProtocolo: UDPPorta de origem: DNSPorta do destino: AlgunsAção: Licença
8. Confirme a sequência foi adicionado.
9. O clique **adiciona a regra nova**. Ajuste os seguintes valores à sequência #4 ACL. O clique **aplica-se** quando terminado.Fonte: AlgunsDestino: AlgunsProtocolo: UDPPorta de origem: AlgunsPorta do destino: DNSAção: Licença
10. Confirme a sequência foi adicionado.
11. Salvar a configuração atual WLC.

Permita o perfilamento de pontas de prova no ISE

O ISE precisa de ser configurado como as pontas de prova para perfilar eficazmente valores-limite. À revelia, estas opções são desabilitadas. Esta seção mostra como configurar o ISE para ser pontas de prova.

1. Do Gerenciamento ISE, navegue à **administração > ao sistema > ao desenvolvimento**.
2. Escolha o **ISE**. O clique **edita o host ISE**.
3. Da página do nó da edição, selecione a configuração de perfilamento e configurar o seguinte:DHCP: Permitido, tudo (ou padrão)DHCPSPAN: Permitido, tudo (ou padrão)HTTP: Permitido, tudo (ou padrão)RAIO: Permitido, N/ADNS: Permitido, N/A
4. Reassocie os dispositivos (iPhone/iPads/Droids/Mac, etc.).
5. Confirme identidades do valor-limite ISE. Navegue à **administração > ao Gerenciamento de identidades > às identidades**. Clique sobre valores-limite para alistar o que foi perfilado.**Note**: O perfilamento da inicial é das pontas de prova do RAIO.

Permita políticas do perfil ISE para dispositivos

Fora da caixa, o ISE fornece uma biblioteca de vários perfis do valor-limite. Termine estas etapas a fim permitir perfis para dispositivos:

1. Do ISE, navegue à **política > perfilando**.
2. Do painel esquerdo, expanda o **perfilamento de políticas**.
3. Clique o **iPad do dispositivo de Apple > do Apple**, e ajuste o seguinte:Política permitida: HabilitadoCrie o grupo de harmonização da identidade: Selecionado
4. **O iPhone do dispositivo de Apple do** clique **> do Apple**, ajustou o seguinte:Política permitida: HabilitadoCrie o grupo de harmonização da identidade: Selecionado

5. O clique **Android**, ajustou o seguinte:Política permitida: HabilitadoCrie o grupo de harmonização da identidade: Selecionado

O perfil da autorização ISE para a descoberta da postura reorienta

Termine estas etapas a fim configurar uma postura da política da autorização reorientam permite que os dispositivos novos sejam reorientados ao ISE para a descoberta apropriada e o perfilamento:

1. Do ISE, navegue à **política > aos elementos > aos resultados da política**.
2. Expanda a **autorização**. Clique **perfis da autorização** (painel esquerdo) e o clique **adiciona**.
3. Crie o perfil da autorização com o seguinte:Nome: Posture_RemediationTipo de acesso: Access_AcceptFerramentas comuns:Descoberta da postura, permitidaDescoberta da postura, ACL ACL-POSTURE-REDIRECT
4. O clique **submete-se** para terminar esta tarefa.
5. Confirme que o perfil novo da autorização está adicionado.

Crie o perfil da autorização ISE para o empregado

Adicionar um perfil da autorização para um empregado permite que o ISE autorize e permita o acesso com os atributos atribuídos. O VLAN 11 do empregado é atribuído neste caso.

Conclua estes passos:

1. Do ISE, navegue à **política > aos resultados**. Expanda a **autorização**, a seguir clique **perfis da autorização** e o clique **adiciona**.
2. Entre no seguinte para o perfil da autorização do empregado:Nome: Employee_WirelessTarefas comuns:VLAN, permitidoVLAN, valor 11 do sub
3. O clique **submete-se** para terminar esta tarefa.
4. Confirme que o perfil novo da autorização do empregado esteve criado.

Crie o perfil da autorização ISE para o contratante

Adicionar um perfil da autorização para um contratante permite que o ISE autorize e permita o acesso com os atributos atribuídos. O VLAN 12 do contratante é atribuído neste caso.

Conclua estes passos:

1. Do ISE, navegue à **política > aos resultados**. Expanda a **autorização**, a seguir clique **perfis da autorização** e o clique **adiciona**.
2. Entre no seguinte para o perfil da autorização do empregado:Nome: Employee_WirelessTarefas comuns:VLAN, permitidoVLAN, valor 12 do sub
3. O clique **submete-se** para terminar esta tarefa.
4. Confirme que o perfil da autorização do contratante esteve criado.

Política da autorização para a postura/o perfilamento do dispositivo

Pouca informação é sabida sobre um dispositivo novo quando vem primeiramente na rede, um administrador criará a política apropriada para permitir que os valores-limite desconhecidos sejam identificados antes de permitir o acesso. Neste exercício, a política da autorização será criada de modo que um dispositivo novo seja reorientado ao ISE para a avaliação da postura (para dispositivos móveis seja agentless, consequentemente somente perfilar é relevante); os valores-limite serão reorientados ao portal prisioneiro ISE e identificados.

Conclua estes passos:

1. Do ISE, navegue à **política > à autorização**.
2. Há uma política para Telefones IP Profiled Cisco. Isto é fora da caixa. Edite isto como uma política da postura.
3. Incorpore os seguintes valores para esta política:Nome da regra: Posture_RemediationGrupos da identidade: AlgunsOutras circunstâncias > criam novo: Sessão (avançada) > PostureStatusPostureStatus > iguais: Desconhecido
4. Ajuste o seguinte para permissões:Permissões > padrão: Posture_Remediation
5. Click **Save**.**Note**: Os elementos da política alternativamente feita sob encomenda podem ser criados para adicionar a acessibilidade.

Política de teste da remediação da postura

Àdemonstração simples pode ser executado para mostrar que o ISE está perfilando corretamente um dispositivo novo baseado na política da postura.

1. Do ISE, navegue à **administração > ao Gerenciamento de identidades > às identidades**.
2. Clique **valores-limite**. Associe e conecte um dispositivo (um iPhone neste exemplo).
3. Refresque a lista dos valores-limite. Observe que informação é dada.
4. Do dispositivo de ponto final, consulte a:URL: http://www (ou 10.10.10.10)O dispositivo é reorientado. Aceite toda a alerta para Certificados.
5. Depois que o dispositivo móvel reorientou completamente, do ISE refresque a lista dos valores-limite outra vez. Observe o que mudou. O valor-limite precedente (por exemplo, Apple-dispositivo) deve ter mudado a “Apple-iPhone” etc. A razão é que a prova HTTP obtém eficazmente a informação do agente de usuário, como parte do processo de reorientação ao portal prisioneiro.

Política da autorização para o acesso diferenciado

Após com sucesso ter testado a autorização da postura, continue a construir políticas para apoiar o acesso diferenciado para o empregado e o contratante com dispositivos conhecidos e o específico diferente da atribuição de VLAN ao papel de usuário (nestes encenação, empregado e contratante).

Conclua estes passos:

1. Navegue a **ISE > política > autorização**.
2. Adicionar/inserção uma regra nova acima da política/linha da remediação da postura.
3. Incorpore os seguintes valores para esta política:Nome da regra: EmpregadoGrupos da identidade (expanda): Grupos da identidade do valor-limiteGrupos da identidade do valor-limite: PerfiladoPerfilado: Android, Apple-iPad ou Apple-iPhone
4. A fim especificar tipos de dispositivo adicionais, clique **+** e adicionar mais dispositivos (se necessário):Grupos da identidade do valor-limite: PerfiladoPerfilado: Android, Apple-iPad ou Apple-iPhone
5. Especifique os valores das seguintes permissões para esta política:Outras circunstâncias (expanda): Crie a condição nova (a opção avançada)Circunstância > expressão (da lista): InternalUser > nomeInternalUser > nome: empregado
6. Adicionar uma condição para a sessão da postura complacente:As permissões > perfilam > padrão: Employee_Wireless
7. Click **Save**. Confirme que a política esteve adicionada corretamente.
8. Continue adicionando a política do contratante. Neste documento, a política precedente é duplicada a fim expedir o processo (ou, você pode manualmente configurar para a boa prática).Da política > das ações do empregado, **duplicata do** clique **abaixo**.
9. Edite os seguintes campos para esta política (cópia duplicada):Nome da regra: ContratanteAs outras circunstâncias > InternalUser > nome: contratantePermissões: Contractor_Wireless
10. Click **Save**. Confirme que a cópia duplicada precedente (ou a política nova) estão configuradas corretamente.
11. A fim inspecionar as políticas, clique o Política-em-um-**relance**.A política vê duma olhada fornece políticas resumidas e fáceis de ver consolidado.

CoA de teste para o acesso diferenciado

Com os perfis e as políticas da autorização preparados diferenciando o acesso, é hora de testar. Tendo um único WLAN fixado, um empregado será atribuído o empregado VLAN e um contratante será para o contratante VLAN. Apple iPhone/iPad é usado nos exemplos seguintes.

Conclua estes passos:

1. Conecte ao WLAN fixado (POD1x) com o dispositivo móvel e use estas credenciais:Nome de usuário: empregadoSenha:
2. O clique **junta-se**. Confirme que o empregado é o vlan designada 11 (empregado VLAN).
3. O clique **esquece esta rede**. Confirme clicando **esquecem**.
4. Vá ao WLC e remova as conexões de cliente existentes (se o mesmo foi usado em etapas precedentes). Navegue **para monitorar > clientes > MAC address**, a seguir clique **removem**.
5. Uma outra certo maneira de cancelar sessões cliente precedentes é desabilitar/permite o WLAN.Vão ao **WLC > os WLAN > o WLAN**, a seguir clicam o WLAN para editar.a Un-verificação **permitida > aplica-se** (para desabilitar).Verifique a caixa para ver se há **permitido > aplicam-se** (re-para permitir).
6. Vá para trás ao dispositivo móvel. Conecte outra vez ao mesmo WLAN com estas credenciais:Nome de usuário: contratanteSenha: XXXX
7. O clique **junta-se**. Confirme que o usuário do contratante é o vlan designada 12 (contratante/convidado VLAN).
8. Você pode olhar a opinião do log do tempo real ISE em **ISE > monitor > autorizações**. Você

deve ver que os usuários individuais (empregado, contratante) obtêm perfis diferenciados da autorização (Employee_WirelessvsContractor_Wireless) em VLAN diferentes.

Convidado WLAN WLC

Termine estas etapas a fim adicionar um convidado WLAN para permitir que os convidados alcancem o portal do convidado do patrocinador ISE:

1. Do WLC, navegue a **> Add WLAN > WLAN novo**.
2. Entre no seguinte para o convidado novo WLAN:Nome de perfil: pod1guestSSID: pod1guest
3. Clique em Apply.
4. Entre no seguinte sob o convidado WLAN > tab geral:Status: DesabilitadoRelação/grupo de interface: Convidado
5. Navegue ao **> segurança do** convidado **WLAN > ao Layer2** e entre no seguinte:Segurança da camada 2: Nenhum
6. Navegue ao **> segurança do** convidado **WLAN > à** aba **Layer3** e entre no seguinte:Segurança da camada 3: NenhumPolítica da Web: HabilitadoValor do sub da política da Web: AutenticaçãoACL Pré-autenticação: ACL-POSTURE-REDIRECTTipo do AUTH da Web: Externo (reoriente ao servidor interno)URL: https://10.10.10.70:8443/guestportal/Login.action
7. Clique em Apply.
8. Certifique-se **salvar a configuração WLC**.

Testando o convidado WLAN e o portal do convidado

Agora, você pode testar a configuração do convidado WLAN. Deve reorientar os convidados ao portal do convidado ISE.

Conclua estes passos:

1. De um dispositivo iOS tal como um iPhone, navegue às **redes do Wi-fi > permitem**. Então, selecione a rede de convidado da VAGEM.
2. Seu dispositivo iOS deve mostrar um endereço IP válido do convidado VLAN (10.10.12.0/24).
3. Abra o navegador do safari e conecte-o a:URL: http://10.10.10.10Uma autenticação da Web reorienta aparece.
4. O clique **continua** até que você chegue na página do portal do convidado ISE.O tiro de tela seguinte da amostra mostra o dispositivo iOS em um início de uma sessão do portal do convidado. Isto confirma que a instalação correta para portal do convidado WLAN e ISE é ativa.

O Sem fio ISE patrocinou o acesso do convidado

O ISE pode ser configurado para permitir que os convidados sejam patrocinados. Neste caso você configurará políticas do convidado ISE para permitir os usuários internos ou AD do domínio (se integrado) para patrocinar o acesso do convidado. Você igualmente configurará o ISE para permitir que os patrocinadores ver a senha do convidado (opcional), que é útil a este laboratório.

Conclua estes passos:

1. Adicionar o usuário do empregado ao grupo de SponsorAllAccount. Há umas maneiras diferentes de fazer isto: vá diretamente ao grupo, ou edite o usuário e atribua o grupo. Para este exemplo, navegue à **administração > ao Gerenciamento de identidades > aos grupos > aos grupos da identidade do usuário**. Então, o clique **SponsorAllAccount** e adiciona o usuário do empregado.
2. Navegue aos **grupos da administração > do Gerenciamento > do patrocinador do convidado**.
3. O clique **edita**, a seguir escolhe **SponsorAllAccounts**.
4. Selecione níveis da autorização e ajuste o seguinte:Veja a senha do convidado: Yes
5. **Salvaguarda do** clique a fim terminar esta tarefa.

Convidado de patrocínio

Previamente, você configurou a política e os grupos apropriados do convidado para permitir que o usuário de domínio AD patrocine convidados provisórios. Em seguida, você alcançará o portal do patrocinador e criará um acesso provisório do convidado.

Conclua estes passos:

1. De um navegador, navegue a qualquer uma destas URL: <ise ip>:8080/sponsorportal/ de http:// **ou** <ise ip>:8443/sponsorportal/ de https://. Então, início de uma sessão com o seguinte:Nome de usuário: aduser (diretório ativo), empregado (usuário interno)Senha: XXXX
2. Da página do patrocinador, o clique **cria a única conta de usuário convidado**.
3. Para um convidado provisório, adicionar o seguinte:Nome: Exigido (por exemplo, Sam)Sobrenome: Exigido (por exemplo, Jones)Papel do grupo: ConvidadoPerfil do tempo: DefaultOneHourZona de hora (fuso horário): Alguns/padrão
4. Clique em Submit.
5. Uma conta do convidado é criada com base em sua entrada anterior. Note que a senha é visível (do exercício precedente) ao contrário do *** da mistura.
6. Deixe a este indicador a exibição aberta o nome de usuário e senha para o convidado. Você usá-los-á para testar o início de uma sessão portal do convidado (em seguida).

Acesso de teste do portal do convidado

Com a conta nova do convidado criada por um usuário/patrocinador AD, é hora de testar o portal e o acesso do convidado.

Conclua estes passos:

1. Em um dispositivo preferido (neste caso um iOS de Apple/iPad), conecte ao convidado SSID da vagem e verifique o endereço IP de Um ou Mais Servidores Cisco ICM NT /connectivity.
2. Use o navegador e tente navegar a http://www.Você é reorientado à página de login do portal do convidado.
3. Início de uma sessão usando a conta do convidado criada no exercício precedente.Se bem sucedida, a página da política de uso aceitável publica-se.
4. A verificação **aceita termos e condição**, a seguir clica-os **aceita**.A URL original é terminada, e

o valor-limite é acesso permitido como o convidado.

Configuração do certificado

As comunicações seguras com ISE, determinam se a comunicação é autenticação relativa ou para o Gerenciamento ISE. Por exemplo, para a configuração usando a Web UI ISE, os Certificados X.509 e as correntes da confiança do certificado precisam de ser configurados para permitir a criptografia assimétrica.

Conclua estes passos:

1. De seu PC conectado prendido, abra uma janela de navegador a https://AD/certsrv.**Note**: Use o HTTP seguro.**Note**: Use Mozilla Firefox ou MS Internet Explorer a fim alcançar o ISE.
2. Entre como administrator/Cisco123.
3. Clique a **transferência um certificado de CA, um certificate chain, ou um CRL**.
4. Clique o **certificado de CA da transferência** e salvar o (note o lugar da salvaguarda).
5. Abra uma janela de navegador ao <Pod-ISE> de https://.
6. Vá aos **Certificados da administração > do sistema > dos Certificados > da autoridade dos Certificados**.
7. Selecione a operação dos **Certificados do Certificate Authority** e consulte ao CERT previamente transferido de CA.
8. **A confiança** seleta **para o cliente com EAP-TLS**, submete-se então.
9. Confirme que CA esteve adicionado confiou como a CA raiz.
10. De um navegador, vá aos **Certificados da administração > do sistema > dos Certificados > da autoridade dos Certificados**.
11. O clique **adiciona**, a seguir **gerencie a solicitação de assinatura de certificado**.
12. Submeta estes valores:Assunto do certificado: CN=ise.corp.rf-demo.comComprimento chave: 2048
13. Alertas ISE que o CSR está disponível na página CSR. Click **OK**.
14. Selecione o CSR da página ISE CSR e clique a **exportação**.
15. Salvar o arquivo a todo o lugar (por exemplo, transferências, etc.)
16. O arquivo salvar como *.pem.
17. Encontre o arquivo CSR e edite-o com um ou outro bloco de notas/Wordpad/TextEdit.
18. Copie o índice (selecione tudo > cópia).
19. Abra uma janela de navegador a https:// <Pod-AD>/certsrv.
20. Clique o **pedido um certificado**.
21. Clique para submeter um **pedido do certificado avançado**.
22. Cole o índice CSR no campo da solicitação salva.
23. Selecione o **servidor de Web** como o molde de certificado, a seguir clique-o **submetem-se**.
24. Selecione o **DER codificado**, a seguir clique o **certificado da transferência**.
25. Salvar o arquivo a um lugar conhecido (por exemplo, as transferências)
26. Vá aos **Certificados da administração > do sistema > dos Certificados > da autoridade dos Certificados**.
27. O clique **adiciona > certificado de CA do ligamento**.
28. Consulte ao certificado de CA previamente transferido.
29. Selecione o **protocolo EAP** e a **interface de gerenciamento**, a seguir clique-os **submetem-se**.

30. Confirme que CA esteve adicionado confiou como a CA raiz.

Integração do ative directory de Windows 2008

O ISE pode comunicar-se diretamente com o diretório ativo (AD) para a autenticação do usuário/máquina ou para recuperar atributos de usuário da informação de autorização. A fim comunicar-se com o AD, o ISE deve “ser juntado” a um domínio AD. Neste exercício você juntar-se-á ao ISE a um domínio AD, e confirma uma comunicação AD está trabalhando corretamente.

Conclua estes passos:

1. A fim juntar-se ao ISE ao domínio AD, do ISE vai à **administração > ao Gerenciamento de identidades > fontes externos da identidade**.
2. Do painel esquerdo (fontes externos da identidade), selecione o **diretório ativo**.
3. No lado direito, selecione a aba da **conexão** e entre no seguinte:Domain Name: corp.rf-demo.comNome da loja da identidade: AD1
4. **Conexão de teste do** clique. Incorpore username AD (aduser/Cisco123), a seguir clique a **APROVAÇÃO**.
5. Confirme que o status de teste mostra o **teste sucedido**.
6. Selecione o log detalhado mostra e observe os detalhes úteis pesquisando defeitos. Clique em OK para continuar.
7. Clique a **configuração da salvaguarda**.
8. O clique **junta-se**. Inscreva o usuário AD (administrator/Cisco123), a seguir clique a **APROVAÇÃO**.
9. Confirme que se juntam às mostras do status de operação **sucedidas**, a seguir clicam a **APROVAÇÃO** para continuar.As mostras do estado da conexão de servidor **CONECTADAS**. Se este as alterações de status a qualquer hora, uma conexão de teste ajudarão a pesquisar defeitos edições com as operações AD.

Adicionar grupos do diretório ativo

Quando os grupos AD são adicionados, um controle mais granulado está permitido sobre políticas ISE. Por exemplo, os grupos AD podem ser diferenciados por papéis funcionais, tais como grupos do empregado ou de contratante, sem o erro relacionado que está sendo experimentado nos exercícios precedentes ISE 1.0 onde as políticas foram limitadas somente aos usuários.

Neste laboratório, somente os usuários de domínio e/ou o grupo do empregado são usados.

Conclua estes passos:

1. Do ISE, vão à **administração > ao Gerenciamento de identidades > as fontes externos da identidade**.
2. Selecione a aba do **diretório ativo > dos grupos**.
3. Clique **+Add**, a seguir **selecione grupos do diretório**.
4. No indicador da continuação (grupos seletos do diretório), aceite os padrões para o domínio (corp-rf-demo.com) e filtre-os (*). Então, clique RetrieveGroups**.**
5. Selecione as caixas para grupos dos **usuários de domínio** e do **empregado**. Clique a **APROVAÇÃO** quando terminado.

6. Confirme que os grupos estiveram adicionados à lista.

Adicionar a sequência da fonte da identidade

Àrevelia, o ISE é ajustado para usar usuários internos para a loja da autenticação. Se o AD é adicionado, uma ordem da prioridade de sequência pode ser criada para incluir o AD que o ISE se usará para verificar para ver se há a autenticação.

Conclua estes passos:

1. Do ISE, navegue às **sequências da fonte da administração > do Gerenciamento de identidades > da identidade**.
2. Clique **+Add** a fim adicionar uma sequência nova.
3. Dê entrada com o novo nome: **AD_Internal**. Adicionar todas as fontes disponíveis ao campo selecionado. Então, requisite novamente como necessário de modo que AD1 seja movido para a parte superior da lista. Clique em Submit.
4. Confirme que a sequência esteve adicionada à lista.

O Sem fio ISE patrocinou o acesso do convidado com AD integrado

O ISE pode ser configurado para permitir os convidados sejam patrocinados com políticas a fim permitir que os usuários de domínio AD patrocinem o acesso do convidado.

Conclua estes passos:

1. Do ISE, navegue à **administração > ao Gerenciamento > aos ajustes do convidado**.
2. Expanda o **patrocinador**, e clique a **fonte da autenticação**. Então, **AD_Internal** seleto como a sequência da loja da identidade.
3. Confirme AD_Internal como a sequência da loja da identidade. Click **Save**.
4. Navegue ao **Gerenciamento da administração > do convidado > à política do grupo do patrocinador**.
5. Introduza a política nova acima da primeira regra (clique o ícone das **ações do** direito).
6. Para a política nova do grupo do patrocinador, crie o seguinte:Nome da regra: Usuários de domínioGrupos da identidade: AlgunsOutras circunstâncias: (Crie novo/o avançou) > AD1AD1: Grupos externosOs grupos externos AD1 > igualam > usuários de corp.rf-demo.com/Users/Domain
7. Em grupos do patrocinador, ajuste o seguinte:Grupos do patrocinador: SponsorAllAccounts
8. Navegue aos **grupos da administração > do Gerenciamento > do patrocinador do convidado**.
9. Selecione para editar > **SponsorAllAccounts**.
10. Selecione níveis da autorização e ajuste o seguinte:Veja a senha do convidado: Yes

Configurar o PERÍODO no interruptor

Configurar o PERÍODO - O mgt ISE/relação da ponta de prova é L2 junto à interface de gerenciamento WLC. O interruptor pode ser configurado PARA MEDIR e outras relações, tais como a relação VLAN do empregado e do convidado.

```
Podswitch(config)#monitor session 1 source vlan10 , 11 , 12
Podswitch(config)#monitor session 1 destination interface Fa0/8
ISE virtual probe interface.
```

Referência: Autenticação wireless para Apple MAC OS X

Associado ao WLC através de um SSID autenticado como um usuário interno (ou o usuário integrada, AD) usando um portátil do Sem fio de Apple Mac OS X. Faixa clara se não aplicável.

1. Em um Mac, vá aos ajustes WLAN. Permita WIFI, a seguir selecione-o e conecte-o à VAGEM permitida 802.1X SSID criada no exercício precedente.
2. Forneça a informação seguinte para conectar:Nome de usuário: aduser (se usando o AD), empregado (– empregado), contratante (interno – contratante interno)Senha: XXXX802.1X: AutomáticoCertificado TLS: NenhumNeste tempo, o portátil não pôde conectar. Além, o ISE pode jogar um evento falhado como segue:
   ```
   Authentication failed :12514 EAP-TLS failed SSL/TLS handshake because of
   an unknown CA in the client certificates chain
   ```
3. Vá à **preferência > à rede > ao aeroporto > ao 802.1X do sistema que** ajusta-se e ajuste a autenticação nova do perfil da VAGEM SSID/WPA como:TLS: DesabilitadoPEAP: HabilitadoTTL: DesabilitadoEAP-FAST: Desabilitado
4. Clique a **APROVAÇÃO** para continuar e permitir que o ajuste sido salvar.
5. Na tela da rede, selecione o apropriado perfil SSID + de 802.1X WPA e o clique **conecta**.
6. O sistema pôde alertar para um nome de usuário e senha. Incorpore o usuário AD e a senha (), a seguir clique a **APROVAÇÃO**.O cliente deve mostrar **conectado** através do PEAP com um endereço IP válido.

Referência: Autenticação wireless para o Microsoft Windows XP

Associado ao WLC através de um SSID autenticado como um usuário interno (ou o usuário integrada, AD) usando um portátil do Sem fio de Windows XP. Faixa clara se não aplicável.

Conclua estes passos:

1. No portátil, vá aos ajustes WLAN. Permita WIFI e conecte-o à VAGEM permitida 802.1X SSID criada no exercício precedente.
2. Alcance as propriedades de rede para a relação de WIFI.
3. Navegue à aba das **redes Wireless**. Selecione as propriedades de rede da vagem SSID > a aba da autenticação > o tipo EAP = EAP protegido (PEAP).
4. Clique as propriedades EAP.
5. Ajuste o seguinte:Valide o certificado de servidor: DesabilitadoMétodo de autenticação: Senha fixada (EAP-MSCHAP v2)
6. **APROVAÇÃO do** clique em todos os indicadores para terminar estas tarefas de configuração.
7. Alertas do cliente de Windows XP para o nome de usuário e senha. Neste exemplo, é.
8. Confirme a conectividade de rede, o endereçamento de IP (v4).

Referência: Autenticação wireless para Microsoft Windows 7

Associado ao WLC através de um SSID autenticado como um usuário interno (ou o usuário integrada, AD) usando um portátil do Sem fio de Windows 7.

1. No portátil, vá aos ajustes WLAN. Permita WIFI e conecte-o à VAGEM permitida 802.1X SSID criada no exercício precedente.
2. Alcance o gerente wireless e edite o perfil novo do Sem fio da VAGEM.
3. Ajuste o seguinte:Método de autenticação: PEAPRecorde minhas credenciais…: DesabilitadoValide o certificado de servidor (ajuste avançado): DesabilitadoMétodo de autenticação (adv. Ajuste): EAP-MSCHAP v2Use automaticamente meu fazer logon de Windows…: Desabilitado

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems