Índice

Introdução

Este documento fornece a matriz de compatibilidade para os mecanismos de segurança da camada 2 e da camada 3 apoiados no controlador do Wireless LAN (WLC).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da configuração de AP de pouco peso e de Cisco WLC
- Conhecimento básico do protocolo de pouco peso AP (LWAPP)
- Conhecimento básico de soluções da segurança Wireless

Componentes Utilizados

A informação neste documento é baseada no o 4400/2100 Series WLC de Cisco que executa a versão de firmware 7.0.116.0

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.

Soluções da segurança de rede do Cisco Unified Wireless

A rede de Cisco Unified Wireless apoia métodos de segurança da camada 2 e da camada 3.

- Segurança da camada 2
- Segurança da camada 3 (para o WLAN) ou Segurança da camada 3 (para o convidado LAN)

A Segurança da camada 2 não é apoiada no convidado LAN.

Esta tabela alista os vários métodos de segurança da camada 2 e da camada 3 apoiados no controlador do Wireless LAN. Estes métodos de segurança podem ser permitidos da **ABA de segurança no WLAN > editam a** página do WLAN.

Mecanismo de segurança da camada 2		
Parâmetro		**Descrição**
Segurança da camada 2	Nenhum	Nenhuma Segurança da camada 2 selecionada.
	WPA+WPA2	Use este ajuste a fim permitir o acesso protegido por wi-fi.
	802.1X	Use este ajuste a fim permitir a autenticação do 802.1x.
	WEP estático	Use este ajuste a fim permitir a criptografia do WEP estático.
	WEP estático + 802.1x	Use este ajuste a fim permitir parâmetros do WEP estático e do 802.1x.
	CKIP	Use este ajuste a fim permitir o protocolo chave da integridade de Cisco (CKIP). Funcional no AP modela 1100, 1130, e 1200, mas não AP 1000. Aironet IE precisa de ser permitido para que esta característica trabalhe. CKIP expande as chaves de criptografia a 16 bytes.

Filtração MAC		Selecione para filtrar clientes pelo MAC address. Configurar localmente clientes pelo MAC address no MAC filtra > página nova. Se não, configurar os clientes em um servidor Radius.
Mecanismo de segurança da camada 3 (para o WLAN)		
Parâmetro		**Descrição**
Segurança da camada 3	Nenhum	Nenhuma Segurança da camada 3 selecionada.
	IPSec	Use este ajuste a fim permitir o IPsec. Você precisa de verificar a disponibilidade de software e a compatibilidade do hardware do cliente antes que você execute o IPsec. **Nota:** Você deve ter o módulo opcional da Segurança VPN/Enhanced (placa de processador cripto) instalado para permitir o IPsec. Verifique que está instalado em seu controlador na página do inventário.
	VPN Passagem-através de	Use este ajuste a fim permitir o VPN Passagem-através de. **Nota:** Esta opção não está disponível em controladores do Cisco 5500 Series e em controladores do Cisco 2100 Series. Contudo, você pode replicate esta funcionalidade em um Cisco 5500 Series controlador

		ou no controlador do Cisco 2100 Series criando um WLAN aberto usando um ACL.
Política da Web	Selecione esta caixa de verificação para permitir a política da Web. Do controlador o tráfego para a frente DNS a e dos clientes Wireless antes da autenticação. **Nota:** A política da Web não pode ser usada em combinação com o IPsec ou o VPN Passagem-através das opções. Estes parâmetros são indicados: • Autenticação? Se você seleciona esta opção, o usuário está alertado para o nome de usuário e senha ao conectar o cliente à rede Wireless. • Transmissão? Se você seleciona esta opção, o usuário pode alcançar a rede diretamente sem a autenticação do nome de usuário e senha. • A Web condicional reorienta? Se você seleciona esta opção, o usuário pode condicionalmente ser reorientado a um página da web particular depois que a autenticação do 802.1X termina com sucesso. Você pode especificar a página e as condições de redirecionamento sob as quais o redirecionamento ocorre em seu servidor RADIUS. • A Web da página do respingo reorienta? Se você seleciona esta opção, o usuário está reorientado a um página da web particular depois que a autenticação do 802.1X termina com sucesso. Depois que a reorientação, o usuário tem o acesso direto à rede. Você pode especificar o página da web do respingo em seu servidor Radius. • Na falha do filtro MAC? Permite falhas do filtro da autenticação da	

	Web MAC.
ACL Pré-autenticação	Selecione o ACL para ser usado para o tráfego entre o cliente e o controlador.
Cancele o config global	Indicadores se você seleciona a autenticação. Verifique esta caixa a fim cancelar a configuração da autenticação global ajustada na página de login da Web.
Tipo do AUTH da Web	Indicadores se você seleciona a política da Web e cancela o config global. Selecione um tipo de autenticação da Web: • Interno • Personalizado (transferido) Página de login? Selecione uma página de login da lista de drop-down.Página da falha no login? Selecione uma página de login que indique ao cliente se a autenticação da Web falha.Logout a página? Selecione uma página de login que indique ao cliente quando os log de usuário fora do sistema. • Externo (reoriente ao servidor interno) URL? Incorpore a URL do servidor interno.
Envie por correio eletrónico a entrada	Indicadores se você seleciona a transmissão. Se você seleciona esta opção, você está alertado para seu endereço email ao conectar à rede.

Mecanismo de segurança da camada 3 (para o convidado LAN)		
Parâmetro		**Descrição**
Segurança da camada 3	Nenhum	Nenhuma Segurança da camada 3 selecionada.
	Autenticação da Web	Se você seleciona esta opção, você está alertado para o nome de usuário e senha ao conectar o cliente à rede.
	Transmissão da	Se você seleciona

	Web	esta opção, você pode alcançar a rede diretamente sem a autenticação do nome de usuário e senha.
ACL Pré-autenticação		Selecione o ACL para ser usado para o tráfego entre o cliente e o controlador.
Cancele o config global		Verifique esta caixa a fim cancelar a configuração da autenticação global ajustada na página de login da Web.
Tipo do AUTH da Web		Indicadores se você seleciona o config global da ultrapassagem. Selecione um tipo de autenticação da Web: • Interno • Personalizado (transferido) Página de login? Selecione uma página de login da lista de drop-down.Página da falha no login? Selecione uma página de login que indique ao cliente se a autenticação da Web falha.Logout a página? Selecione uma página de login que indique ao cliente quando os log de

	usuário fora do sistema. • Externo (reoriente ao servidor interno) URL? Incorpore a URL do servidor interno.
Envie por correio eletrónico a entrada	Indicadores se você seleciona a transmissão da Web. Se você seleciona esta opção, você está alertado para seu endereço email ao conectar à rede.

Nota: O software release em 4.1.185.0 do controlador ou em mais tarde, CKIP é apoiado para o uso somente com WEP estático. Não é apoiado para o uso com WEP dinâmico. Consequentemente, um cliente Wireless que seja configurado para usar CKIP com WEP dinâmico é incapaz de associar a um Wireless LAN que é configurado para CKIP. Cisco recomenda que você usa o WEP dinâmico sem CKIP (que é menos seguro) ou WPA/WPA2 com TKIP ou AES (que são mais seguros).

Camada 2 do controlador do Wireless LAN? Matriz de compatibilidade da Segurança da camada 3

Quando você configura a Segurança em um Wireless LAN, mergulhe 2 e mergulhe 3 métodos de segurança pode ser usado na junção. Contudo, não todos os métodos de segurança da camada 2 podem ser usados com todos os métodos de segurança da camada 3. Esta tabela mostra a matriz de compatibilidade para os métodos de segurança da camada 2 e da camada 3 apoiados no controlador do Wireless LAN.

Mecanismo de segurança da camada 2	Mecanismo de segurança da camada 3	Compatibilidade
Nenhum	Nenhum	Válido
WPA+WPA2	Nenhum	Válido
WPA+WPA2	Autenticação da Web	Inválido
WPA-PSK/WPA2-PSK	Autenticação da Web	Válido
WPA+WPA2	Transmissão da Web	Inválido

WPA-PSK/WPA2-PSK	Transmissão da Web	Válido
WPA+WPA2	A Web condicional reorienta	Válido
WPA+WPA2	A Web da página do respingo reorienta	Válido
WPA+WPA2	VPN-transmissão	Válido
802.1x	Nenhum	Válido
802.1x	Autenticação da Web	Inválido
802.1x	Transmissão da Web	Inválido
802.1x	A Web condicional reorienta	Válido
802.1x	A Web da página do respingo reorienta	Válido
802.1x	VPN-transmissão	Válido
WEP estático	Nenhum	Válido
WEP estático	Autenticação da Web	Válido
WEP estático	Transmissão da Web	Válido
WEP estático	A Web condicional reorienta	Inválido
WEP estático	A Web da página do respingo reorienta	Inválido
WEP estático	VPN-transmissão	Válido
802.1x Static-WEP+	Nenhum	Válido
802.1x Static-WEP+	Autenticação da Web	Inválido
802.1x Static-WEP+	Transmissão da Web	Inválido
802.1x Static-WEP+	A Web condicional reorienta	Inválido
802.1x Static-WEP+	A Web da página do respingo reorienta	Inválido
802.1x Static-WEP+	VPN-transmissão	Inválido
CKIP	Nenhum	Válido
CKIP	Autenticação da	Válido

	Web	
CKIP	Transmissão da Web	Válido
CKIP	A Web condicional reorienta	Inválido
CKIP	A Web da página do respingo reorienta	Inválido
CKIP	VPN-transmissão	Válido

Informações Relacionadas

- Exemplo de Configuração Básica de Controladoras de Wireless LAN e Pontos de Acesso Lightweight
- Registro de AP leve (LAP) em um Wireless LAN Controller (WLC)
- Manual de configuração do controlador de LAN do Cisco Wireless, liberação 7.0.116.0
- Controlador do Wireless LAN (WLC) FAQ
- Suporte Técnico e Documentação - Cisco Systems