Matriz de Compatibilidade de Segurança de Camada 2 e Camada 3 da WLC

Contents

Introduction

Este documento fornece a matriz de compatibilidade para os mecanismos de segurança de Camada 2 e Camada 3 suportados no Wireless LAN Controller (WLC).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da configuração de APs leves e WLCs da Cisco
- Conhecimento básico do protocolo de AP leve (LWAPP)
- Conhecimento básico das soluções de segurança sem fio

Componentes Utilizados

As informações neste documento são baseadas em um Cisco 4400/2100 Series WLC que executa a versão do firmware 7.0.116.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Soluções Cisco Unified Wireless Network Security

O Cisco Unified Wireless Network suporta métodos de segurança de Camada 2 e Camada 3.

- Segurança de Camada 2
- Segurança de Camada 3 (para WLAN) ou segurança de Camada 3 (para LAN de convidado)

A segurança da camada 2 não é suportada em LANs Convidadas.

Esta tabela lista os vários métodos de segurança de Camada 2 e Camada 3 suportados no Controller de LAN Wireless. Esses métodos de segurança podem ser ativados na guia **Security** na página **WLANs > Edit** da WLAN.

<table>
<tr><th colspan="3">Mecanismo de segurança da camada 2</th></tr>
<tr><th colspan="2">Parâmetro</th><th>Descrição</th></tr>
<tr><td rowspan="6">Segurança de Camada 2</td><td>Nenhum</td><td>Nenhuma segurança de Camada 2 selecionada.</td></tr>
<tr><td>WPA+WPA2</td><td>Use essa configuração para habilitar o Wi-Fi Protected Access.</td></tr>
<tr><td>802.1X</td><td>Use essa configuração para habilitar a autenticação 802.1x.</td></tr>
<tr><td>WEP estático</td><td>Use essa configuração para habilitar a criptografia WEP estática.</td></tr>
<tr><td>WEP estático + 802.1x</td><td>Use essa configuração para habilitar os parâmetros WEP e 802.1x estáticos.</td></tr>
<tr><td>CKIP</td><td>Use essa configuração para habilitar o CKIP (Cisco Key Integrity Protocol). Funcional nos modelos AP 1100, 1130 e 1200, mas não no AP 1000. O Aironet IE precisa ser habilitado para que esse recurso funcione. O CKIP expande as chaves de criptografia para 16 bytes.</td></tr>
<tr><td>Filtragem MAC</td><td colspan="2">Selecione para filtrar clientes por endereço MAC. Configure localmente os clientes pelo endereço MAC na página Filtros MAC > Novo. Caso contrário, configure os clientes em um servidor RADIUS.</td></tr>
<tr><th colspan="3">Mecanismo de segurança da camada 3 (para WLAN)</th></tr>
<tr><th colspan="2">Parâmetro</th><th>Descrição</th></tr>
<tr><td>Segurança de</td><td>Nenhum</td><td>Nenhuma segurança de Camada 3 selecionada.</td></tr>
</table>

Camada 3	IPSec	Use essa configuração para habilitar o IPSec. Você precisa verificar a disponibilidade do software e a compatibilidade do hardware do cliente antes de implementar o IPSec. **Observação:** você deve ter o VPN/Enhanced Security Module (placa de processador de criptografia) opcional instalado para habilitar o IPSec. Verifique se ele está instalado em seu controlador na página Inventário.
	Passagem de VPN	Use essa configuração para habilitar a Passagem de VPN. **Observação:** essa opção não está disponível nos Cisco 5500 Series Controllers e Cisco 2100 Series Controllers. No entanto, você pode replicar essa funcionalidade em um Cisco 5500 Series Controller ou Cisco 2100 Series Controller criando uma WLAN aberta usando uma ACL.
Política da Web	Marque esta caixa de seleção para habilitar a Diretiva da Web. O controlador encaminha o tráfego DNS de e para clientes sem fio antes da autenticação. **Observação: a** Diretiva da Web não pode ser usada em combinação com opções de Passagem de IPsec ou VPN. Estes parâmetros são exibidos: • Autenticação—Se você selecionar esta opção, o usuário será solicitado a fornecer o nome de usuário e a senha ao conectar o cliente à rede sem fio. • Passagem—Se você selecionar esta opção, o usuário pode acessar a rede diretamente sem a autenticação de nome de usuário e senha. • Redirecionamento condicional da Web — Se você selecionar essa opção, o usuário poderá ser redirecionado condicionalmente	

	para uma página da Web específica após a autenticação 802.1X ser concluída com êxito. Você pode especificar a página e as condições de redirecionamento sob as quais o redirecionamento ocorre em seu servidor RADIUS. • Redirecionamento da Web para página de abertura — Se você selecionar essa opção, o usuário será redirecionado para uma página da Web específica após a autenticação 802.1X ser concluída com êxito. Após o redirecionamento, o usuário tem acesso total à rede. Você pode especificar a página da Web inicial no servidor RADIUS. • Em caso de falha do filtro MAC—Ativa falhas do filtro MAC na autenticação da Web.
ACL de pré-autenticação	Selecione a ACL a ser usada para o tráfego entre o cliente e o controlador.
Substituir configuração global	Será exibido se você selecionar Autenticação. Marque esta caixa para substituir a configuração de autenticação global definida na página de login da Web.
Tipo de Web Auth	Será exibido se você selecionar Web Policy (Política da Web) e Over-ride Global Config (Substituir configuração global). Selecione um tipo de autenticação da Web: • Interno • Personalizado (baixado) Página de login—Selecione uma página de login na lista suspensa.Página Falha de Login—Selecione uma página de login que será exibida ao cliente se a autenticação da Web falhar.Página de logoff — Selecione uma página de logon que será exibida ao cliente quando o usuário fizer logoff do sistema. • Externo (Redirecionar para servidor externo) URL — Digite o URL do servidor externo.
Entrada de e-mail	Será exibido se você selecionar Passagem. Se você selecionar essa opção, será solicitado que você informe seu endereço de e-mail ao conectar-se à rede.

Mecanismo de segurança da camada 3 (para LAN de convidado)		
Parâmetro		**Descrição**
Segurança de Camada 3	Nenhum	Nenhuma segurança de Camada 3 selecionada.
	Autenticação da Web	Se você selecionar essa opção, será solicitado que você forneça o nome de usuário e a senha ao conectar o cliente à rede.
	Passagem da Web	Se você selecionar essa opção, poderá acessar a rede diretamente sem a autenticação de nome de usuário e senha.
ACL de pré-autenticação		Selecione a ACL a ser usada para o tráfego entre o cliente e o controlador.
Substituir configuração global		Marque esta caixa para substituir a configuração de autenticação global definida na página de login da Web.
Tipo de Web Auth		Será exibido se você selecionar Substituir configuração global. Selecione um tipo de autenticação da Web: • Interno • Personalizado (baixado) Página de login—Selecione uma página de login na lista suspensa.Página Falha de Login—Selecione uma página de login que será exibida ao cliente se a autenticação da Web falhar.Página de logoff — Selecione uma página de logon que será exibida ao cliente quando o usuário fizer logoff do sistema. • Externo (Redirecionar para servidor externo) URL — Digite o URL do servidor externo.

Entrada de e-mail	Será exibida se você selecionar Passagem da Web. Se você selecionar essa opção, será solicitado que você informe seu endereço de e-mail ao conectar-se à rede.

Observação: no software release 4.1.185.0 ou posterior da controladora, o CKIP é suportado para uso apenas com WEP estático. Ele não é suportado para uso com WEP dinâmico. Portanto, um cliente sem fio configurado para usar o CKIP com WEP dinâmico não pode se associar a uma LAN sem fio configurada para o CKIP. A Cisco recomenda que você use WEP dinâmico sem CKIP (que é menos seguro) ou WPA/WPA2 com TKIP ou AES (que são mais seguros).

Controlador de LAN sem fio Camada 2 - Matriz de compatibilidade de segurança de Camada 3

Quando você configura a segurança em uma LAN sem fio, os métodos de segurança da Camada 2 e da Camada 3 podem ser usados em conjunto. No entanto, nem 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 de Camada 2 e Camada 3 suportados no Controller de LAN Wireless.

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	Passagem da Web	Inválido
WPA-PSK/WPA2-PSK	Passagem da Web	Válido
WPA+WPA2	Redirecionamento Condicional da Web	Válido
WPA+WPA2	Redirecionamento da Web para Página Inicial	Válido
WPA+WPA2	Passagem de VPN	Válido
802.1x	Nenhum	Válido
802.1x	Autenticação da Web	Inválido
802.1x	Passagem da	Inválido

	Web	
802.1x	Redirecionamento Condicional da Web	Válido
802.1x	Redirecionamento da Web para Página Inicial	Válido
802.1x	Passagem de VPN	Válido
WEP estático	Nenhum	Válido
WEP estático	Autenticação da Web	Válido
WEP estático	Passagem da Web	Válido
WEP estático	Redirecionamento Condicional da Web	Inválido
WEP estático	Redirecionamento da Web para Página Inicial	Inválido
WEP estático	Passagem de VPN	Válido
WEP+ 802.1x estático	Nenhum	Válido
WEP+ 802.1x estático	Autenticação da Web	Inválido
WEP+ 802.1x estático	Passagem da Web	Inválido
WEP+ 802.1x estático	Redirecionamento Condicional da Web	Inválido
WEP+ 802.1x estático	Redirecionamento da Web para Página Inicial	Inválido
WEP+ 802.1x estático	Passagem de VPN	Inválido
CKIP	Nenhum	Válido
CKIP	Autenticação da Web	Válido
CKIP	Passagem da Web	Válido
CKIP	Redirecionamento Condicional da Web	Inválido
CKIP	Redirecionamento da Web para Página Inicial	Inválido
CKIP	Passagem de	Válido

	VPN	

Informações Relacionadas

- Exemplo de configuração básica dos controladores LAN sem fio e do access point lightweight
- Registro de AP leve (LAP) em um Wireless LAN Controller (WLC)
- Guia de configuração do Cisco Wireless LAN Controller Release 7.0.116.0
- Perguntas frequentes sobre a controladora Wireless LAN (WLC)
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.