Matrice di compatibilità della sicurezza dei layer 2 e 3 del WLC

Sommario

Introduzione

Questo documento fornisce la matrice di compatibilità per i meccanismi di sicurezza di livello 2 e 3 supportati sul controller WLC.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base della configurazione di Lightweight Access Point e Cisco WLC
- Conoscenze base di LWAPP (Lightweight AP Protocol)
- Conoscenze base delle soluzioni per la sicurezza wireless

Componenti usati

Per questo documento, è stato usato un Cisco serie 4400/2100 WLC con firmware versione 7.0.116.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni

nei suggerimenti tecnici.

Soluzioni Cisco Unified Wireless Network Security

Cisco Unified Wireless Network supporta i metodi di sicurezza di livello 2 e 3.

- Sicurezza di livello 2
- Sicurezza di livello 3 (per WLAN) o di livello 3 (per LAN guest)

La sicurezza di layer 2 non è supportata sulle LAN guest.

In questa tabella vengono elencati i vari metodi di sicurezza di livello 2 e 3 supportati dal controller LAN wireless. Questi metodi di sicurezza possono essere abilitati dalla scheda **Sicurezza** nella pagina **WLAN > Modifica** della WLAN.

Meccanismo di sicurezza di livello 2		
Parametro		**Descrizione**
Sicurezza di livello 2	Nessuna	Nessuna protezione di livello 2 selezionata.
	WPA+WPA2	Utilizzare questa impostazione per abilitare l'accesso protetto Wi-Fi.
	802.1X	Utilizzare questa impostazione per abilitare l'autenticazione 802.1x.
	WEP statico	Utilizzare questa impostazione per abilitare la crittografia WEP statica.
	WEP statico + 802.1x	Utilizzare questa impostazione per abilitare entrambi i parametri WEP statici e 802.1x.
	CKIP	Utilizzare questa impostazione per abilitare il protocollo CKIP (Cisco Key Integrity Protocol). Funzionale sui modelli AP 1100, 1130 e 1200, ma non su AP 1000. Per il corretto funzionamento di questa funzionalità, è necessario abilitare Aironet IE. CKIP espande le chiavi di crittografia a 16 byte.
Filtro MAC	Selezionare per filtrare i client in base all'indirizzo MAC. Configurare localmente i client in base all'indirizzo MAC nella pagina Filtri MAC > Nuovo. In caso contrario, configurare i client su un server RADIUS.	
Meccanismo di sicurezza di layer 3 (per WLAN)		

Parametro		Descrizione
Sicurezza di livello 3	Nessuna	Nessuna protezione di livello 3 selezionata.
	IPSec	Utilizzare questa impostazione per abilitare IPSec. Prima di implementare IPSec, è necessario verificare la disponibilità del software e la compatibilità hardware dei client. **Nota:** per abilitare IPSec, è necessario che sia installata la scheda del processore di crittografia (VPN/Enhanced Security Module) opzionale. Verificare che sia installato sul controller nella pagina Inventario.
	Pass-through VPN	Utilizzare questa impostazione per abilitare il pass-through VPN. **Nota:** questa opzione non è disponibile sui Cisco serie 5500 Controller e sui Cisco serie 2100 Controller. Tuttavia, è possibile replicare questa funzionalità su un controller Cisco serie 5500 o Cisco serie 2100 creando una WLAN aperta con un ACL.
Criteri Web	Selezionare questa casella di controllo per attivare i criteri Web. Il controller inoltra il traffico DNS da e verso i client wireless prima dell'autenticazione. **Nota:** i criteri Web non possono essere utilizzati in combinazione con le opzioni pass-through IPsec o VPN. Vengono visualizzati i seguenti parametri: • Autenticazione: se si seleziona questa opzione, all'utente viene richiesto di immettere il nome utente e la password durante la connessione del client alla rete wireless. • Pass-through: se si seleziona questa opzione, l'utente può accedere direttamente alla rete senza l'autenticazione del nome utente e della password. • Reindirizzamento Web condizionale: se si	

	seleziona questa opzione, l'utente può essere reindirizzato in modo condizionale a una pagina Web specifica dopo il completamento dell'autenticazione 802.1X. È possibile specificare la pagina di reindirizzamento e le condizioni in cui si verifica il reindirizzamento sul server RADIUS. • Reindirizzamento Web pagina iniziale: se si seleziona questa opzione, l'utente viene reindirizzato a una pagina Web specifica dopo il completamento dell'autenticazione 802.1X. Dopo il reindirizzamento, l'utente ha accesso completo alla rete. È possibile specificare la pagina Web iniziale sul server RADIUS. • In caso di errore del filtro MAC: abilita gli errori del filtro MAC di autenticazione Web.
ACL preautenticazione	Selezionare l'ACL da utilizzare per il traffico tra il client e il controller.
Ignora configurazione globale	Viene visualizzato se si seleziona Autenticazione. Selezionare questa casella per ignorare la configurazione di autenticazione globale impostata nella pagina di accesso Web.
Tipo di autenticazione Web	Viene visualizzato se si seleziona Criteri Web e Ignora configurazione globale. Selezionare un tipo di autenticazione Web: • Interno • Personalizzato (scaricato) Pagina di login: selezionare una pagina di login dall'elenco a discesa.Pagina Login non riuscito: selezionare una pagina di login da visualizzare al client se l'autenticazione Web non riesce.Pagina di disconnessione: selezionare una pagina di accesso che viene visualizzata al client quando l'utente si disconnette dal sistema. • Esterno (reindirizzamento su server esterno) URL: immettere l'URL del server esterno.
Input e-mail	Viene visualizzato se si seleziona Passthrough. Se si seleziona questa opzione, durante la connessione alla rete verrà richiesto di specificare l'indirizzo e-mail.
Meccanismo di sicurezza di livello 3 (per LAN guest)	
Parametro	**Descrizione**

Sicurezza di livello 3	Nessuna	Nessuna protezione di livello 3 selezionata.
	Autenticazione Web	Se si seleziona questa opzione, verrà richiesto di immettere il nome utente e la password durante la connessione del client alla rete.
	Pass-through Web	Se si seleziona questa opzione, è possibile accedere direttamente alla rete senza autenticazione del nome utente e della password.
ACL preautenticazione		Selezionare l'ACL da utilizzare per il traffico tra il client e il controller.
Ignora configurazione globale		Selezionare questa casella per ignorare la configurazione di autenticazione globale impostata nella pagina di accesso Web.
Tipo di autenticazione Web		Viene visualizzato se si seleziona Ignora configurazione globale. Selezionare un tipo di autenticazione Web: • Interno • Personalizzato (scaricato) Pagina di login: selezionare una pagina di login dall'elenco a discesa.Pagina Login non riuscito: selezionare una pagina di login da visualizzare al client se l'autenticazione Web non riesce.Pagina di disconnessione: selezionare una pagina di accesso che viene visualizzata al client quando l'utente si disconnette dal sistema. • Esterno

	(reindirizzamento su server esterno) URL: immettere l'URL del server esterno.
Input e-mail	Viene visualizzato se si seleziona Web PassThrough. Se si seleziona questa opzione, durante la connessione alla rete verrà richiesto di specificare l'indirizzo e-mail.

Nota: nel software controller versione 4.1.185.0 o successive, CKIP è supportato solo per l'uso con WEP statico. Non è supportato per l'utilizzo con WEP dinamico. Pertanto, un client wireless configurato per utilizzare CKIP con WEP dinamico non è in grado di associarsi a una LAN wireless configurata per CKIP. Cisco consiglia di utilizzare il protocollo WEP dinamico senza CKIP (che è meno sicuro) o WPA/WPA2 con TKIP o AES (che è più sicuro).

Matrice di compatibilità della sicurezza di layer 3 e layer 2 del controller LAN wireless

Quando si configura la protezione su una LAN wireless, è possibile utilizzare entrambi i metodi di protezione di livello 2 e 3. Tuttavia, non tutti i metodi di protezione di livello 2 possono essere utilizzati con tutti i metodi di protezione di livello 3. Nella tabella viene mostrata la matrice di compatibilità per i metodi di sicurezza di livello 2 e 3 supportati nel controller LAN wireless.

Meccanismo di sicurezza di livello 2	Meccanismo di sicurezza di livello 3	Compatibilità
Nessuna	Nessuna	Valido
WPA+WPA2	Nessuna	Valido
WPA+WPA2	Autenticazione Web	Non valido
WPA-PSK/WPA2-PSK	Autenticazione Web	Valido
WPA+WPA2	Pass-through Web	Non valido
WPA-PSK/WPA2-PSK	Pass-through Web	Valido
WPA+WPA2	Reindirizzamento Web condizionale	Valido
WPA+WPA2	Reindirizzamento Web pagina iniziale	Valido
WPA+WPA2	VPN-PassThrough	Valido
802.1x	Nessuna	Valido
802.1x	Autenticazione Web	Non valido
802.1x	Pass-through Web	Non valido

802.1x	Reindirizzamento Web condizionale	Valido
802.1x	Reindirizzamento Web pagina iniziale	Valido
802.1x	VPN-PassThrough	Valido
WEP statico	Nessuna	Valido
WEP statico	Autenticazione Web	Valido
WEP statico	Pass-through Web	Valido
WEP statico	Reindirizzamento Web condizionale	Non valido
WEP statico	Reindirizzamento Web pagina iniziale	Non valido
WEP statico	VPN-PassThrough	Valido
Static-WEP+ 802.1x	Nessuna	Valido
Static-WEP+ 802.1x	Autenticazione Web	Non valido
Static-WEP+ 802.1x	Pass-through Web	Non valido
Static-WEP+ 802.1x	Reindirizzamento Web condizionale	Non valido
Static-WEP+ 802.1x	Reindirizzamento Web pagina iniziale	Non valido
Static-WEP+ 802.1x	VPN-PassThrough	Non valido
CKIP	Nessuna	Valido
CKIP	Autenticazione Web	Valido
CKIP	Pass-through Web	Valido
CKIP	Reindirizzamento Web condizionale	Non valido
CKIP	Reindirizzamento Web pagina iniziale	Non valido
CKIP	VPN-PassThrough	Valido

Informazioni correlate

- Esempio di configurazione base di Wireless LAN Controller e Lightweight Access Point
- Registrazione di un Lightweight AP (LAP) su un Wireless LAN Controller (WLC)
- Guida alla configurazione di Cisco Wireless LAN Controller, versione 7.0.116.0
- Domande frequenti sui Wireless LAN Controller (WLC)
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).