Sicherheitskompatibilitätsmatrix für Layer 2 und Layer 3 des WLC

Inhalt

Einleitung

Dieses Dokument enthält eine Kompatibilitätsmatrix für die Sicherheitsmechanismen von Layer 2 und Layer 3, die vom Wireless LAN Controller (WLC) unterstützt werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse der Konfiguration von Lightweight APs und Cisco WLCs
- Grundkenntnisse von Lightweight AP Protocol (LWAPP)
- Grundlegende Kenntnisse über Wireless-Sicherheitslösungen

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einem Cisco WLC der Serien 4400/2100, auf dem die Firmware-Version 7.0.116.0 ausgeführt wird.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips

Conventions (Technische Tipps von Cisco zu Konventionen).

Cisco Unified Wireless Network Security-Lösungen

Das Cisco Unified Wireless Network unterstützt Sicherheitsmethoden auf Layer 2 und Layer 3.

- Layer-2-Sicherheit
- Layer-3-Sicherheit (für WLAN) oder Layer-3-Sicherheit (für Gast-LAN)

Layer-2-Sicherheit wird in Gast-LANs nicht unterstützt.

In dieser Tabelle sind die verschiedenen Sicherheitsmethoden aufgeführt, die vom Wireless LAN Controller für Layer 2 und Layer 3 unterstützt werden. Diese Sicherheitsmethoden können über die Registerkarte **Security (Sicherheit)** auf der Seite **WLANs > Edit (WLANs > Bearbeiten)** aktiviert werden.

Layer-2-Sicherheitsmechanismus		
Parameter		**Beschreibung**
Layer-2-Sicherheit	None	Keine Layer-2-Sicherheit ausgewählt.
	WPA+WPA2	Verwenden Sie diese Einstellung, um Wi-Fi Protected Access zu aktivieren.
	802.1x	Verwenden Sie diese Einstellung, um die 802.1x-Authentifizierung zu aktivieren.
	Statisches WEP	Verwenden Sie diese Einstellung, um die statische WEP-Verschlüsselung zu aktivieren.
	Statisches WEP + 802.1x	Verwenden Sie diese Einstellung, um sowohl statische WEP- als auch 802.1x-Parameter zu aktivieren.
	CKIP	Verwenden Sie diese Einstellung, um das Cisco Key Integrity Protocol (CKIP) zu aktivieren. Funktioniert mit den AP-Modellen 1100, 1130 und 1200, jedoch nicht mit AP 1000. Damit diese Funktion funktioniert, muss Aironet IE aktiviert sein. CKIP

		erweitert die Verschlüsselungsschlüssel auf 16 Bytes.
MAC-Filterung	Aktivieren Sie diese Option, um Clients nach MAC-Adresse zu filtern. Konfigurieren Sie Clients lokal nach MAC-Adresse auf der Seite MAC Filters (MAC-Filter) > New (Neu). Andernfalls konfigurieren Sie die Clients auf einem RADIUS-Server.	
Layer-3-Sicherheitsmechanismus (für WLAN)		
Parameter		**Beschreibung**
Layer-3-Sicherheit	None	Keine Layer-3-Sicherheit ausgewählt.
	IPsec	Verwenden Sie diese Einstellung, um IPSec zu aktivieren. Vor der Implementierung von IPSec müssen Sie die Verfügbarkeit der Software und die Kompatibilität der Client-Hardware überprüfen. **Hinweis:** Zur Aktivierung von IPSec muss das optionale VPN/Enhanced Security Module (Crypto Processor Card) installiert sein. Überprüfen Sie, ob er auf dem Controller auf der Seite "Inventory" (Bestand) installiert ist.
	VPN-Passthrough	Verwenden Sie diese Einstellung, um VPN-Passthrough zu aktivieren. **Hinweis:** Diese Option steht bei Cisco Controllern der Serie 5500 und Cisco Controllern der Serie 2100 nicht zur Verfügung. Sie können diese Funktion jedoch auf einem Cisco Controller der Serie 5500 oder einem Cisco Controller der Serie

		2100 replizieren, indem Sie ein offenes WLAN mit einer ACL erstellen.
Webrichtlinie	Aktivieren Sie dieses Kontrollkästchen, um die Webrichtlinie zu aktivieren. Der Controller leitet DNS-Datenverkehr vor der Authentifizierung an Wireless-Clients weiter. **Hinweis:** Die Webrichtlinie kann nicht mit IPsec- oder VPN-Passthrough-Optionen kombiniert werden. Diese Parameter werden angezeigt: • Authentication (Authentifizierung) - Wenn Sie diese Option auswählen, wird der Benutzer zur Eingabe von Benutzername und Kennwort aufgefordert, während er die Verbindung zwischen Client und Wireless-Netzwerk herstellt. • Passthrough: Wenn Sie diese Option auswählen, kann der Benutzer ohne Benutzername- und Kennwortauthentifizierung direkt auf das Netzwerk zugreifen. • Conditional Web Redirect (Bedingte Webumleitung) - Wenn Sie diese Option auswählen, kann der Benutzer bedingt auf eine bestimmte Webseite umgeleitet werden, nachdem die 802.1x-Authentifizierung erfolgreich abgeschlossen wurde. Sie können die Umleitungsseite und die Bedingungen angeben, unter denen die Umleitung auf dem RADIUS-Server erfolgt. • Splash Page Web Redirect (Webumleitung für Splash-Seite): Wenn Sie diese Option auswählen, wird der Benutzer nach erfolgreicher 802.1x-Authentifizierung zu einer bestimmten Webseite umgeleitet. Nach der Umleitung hat der Benutzer vollen Zugriff auf das Netzwerk. Sie können die Splash-Webseite auf dem RADIUS-Server angeben. • On MAC Filter Failure (Bei MAC-Filterausfall): Aktiviert MAC-Filterausfälle für die Webauthentifizierung.	

Vorauthentifizierungs-ACL	Wählen Sie die ACL für den Datenverkehr zwischen dem Client und dem Controller aus.
Globale Konfiguration überschreiben	Wird angezeigt, wenn Sie Authentication (Authentifizierung) auswählen. Aktivieren Sie dieses Kontrollkästchen, um den globalen Authentifizierungskonfigurationssatz auf der Webanmeldeseite zu überschreiben.
Webauthentifizierungstyp	Wird angezeigt, wenn Sie "Web Policy" (Webrichtlinie) und "Over-ride Global Config" (Globale Konfiguration überschreiben) auswählen. Typ der Webauthentifizierung auswählen: • Intern • Benutzerdefiniert (heruntergeladen) Anmeldeseite - Wählen Sie eine Anmeldeseite aus der Dropdown-Liste aus.Anmeldefehler - Wählen Sie eine Anmeldeseite aus, die dem Client angezeigt wird, wenn die Webauthentifizierung fehlschlägt.Abmeldeseite - Wählen Sie eine Anmeldeseite aus, die dem Client angezeigt wird, wenn sich der Benutzer vom System abmeldet. • Extern (Umleitung zu externem Server) URL: Geben Sie die URL des externen Servers ein.
E-Mail-Eingabe	Wird angezeigt, wenn Sie Passthrough auswählen. Wenn Sie diese Option auswählen, werden Sie während der Verbindung mit dem Netzwerk zur Eingabe Ihrer E-Mail-Adresse aufgefordert.

Layer-3-Sicherheitsmechanismus (für Gast-LAN)		
Parameter		**Beschreibung**
Layer-3-Sicherheit	None	Keine Layer-3-Sicherheit ausgewählt.
	Webauthentifizierung	Wenn Sie diese Option auswählen, werden Sie zur Eingabe von Benutzername und Kennwort aufgefordert, während Sie die Verbindung des Clients mit dem Netzwerk herstellen.
	Web-	Wenn Sie diese Option

	Passthrough	auswählen, können Sie direkt ohne Benutzernamen- und Kennwortauthentifizierung auf das Netzwerk zugreifen.
Vorauthentifizierungs-ACL		Wählen Sie die ACL für den Datenverkehr zwischen dem Client und dem Controller aus.
Globale Konfiguration überschreiben		Aktivieren Sie dieses Kontrollkästchen, um den globalen Authentifizierungskonfigurationssatz auf der Webanmeldeseite zu überschreiben.
Webauthentifizierungstyp		Wird angezeigt, wenn Sie "Globale Konfiguration überschreiben" auswählen. Typ der Webauthentifizierung auswählen: • Intern • Benutzerdefiniert (heruntergeladen) Anmeldeseite - Wählen Sie eine Anmeldeseite aus der Dropdown-Liste aus.Anmeldefehler - Wählen Sie eine Anmeldeseite aus, die dem Client angezeigt wird, wenn die Webauthentifizierung fehlschlägt.Abmeldeseite - Wählen Sie eine Anmeldeseite aus, die dem Client angezeigt wird, wenn sich der Benutzer vom System abmeldet. • Extern (Umleitung

	zu externem Server) URL: Geben Sie die URL des externen Servers ein.
E-Mail-Eingabe	Wird angezeigt, wenn Sie Web-Passthrough auswählen. Wenn Sie diese Option auswählen, werden Sie während der Verbindung mit dem Netzwerk zur Eingabe Ihrer E-Mail-Adresse aufgefordert.

Hinweis: CKIP wird in der Controller-Software-Version 4.1.185.0 oder höher nur für die Verwendung mit statischem WEP unterstützt. Die Verwendung mit dynamischem WEP wird nicht unterstützt. Aus diesem Grund kann ein Wireless-Client, der für die Verwendung von CKIP mit dynamischem WEP konfiguriert ist, keine Verbindung zu einem Wireless LAN herstellen, das für CKIP konfiguriert ist. Cisco empfiehlt, entweder dynamisches WEP ohne CKIP (das weniger sicher ist) oder WPA/WPA2 mit TKIP oder AES (die sicherer sind) zu verwenden.

Wireless LAN Controller Layer 2 - Layer 3-Sicherheitskompatibilitätsmatrix

Wenn Sie die Sicherheit in einem Wireless-LAN konfigurieren, können Sie die Sicherheitsmethoden von Layer 2 und Layer 3 gleichzeitig verwenden. Es können jedoch nicht alle Sicherheitsmethoden von Layer 2 mit allen Sicherheitsmethoden von Layer 3 verwendet werden. Diese Tabelle zeigt die Kompatibilitätsmatrix für die Sicherheitsmethoden von Layer 2 und Layer 3, die vom Wireless LAN Controller unterstützt werden.

Layer-2-Sicherheitsmechanismus	Layer-3-Sicherheitsmechanismus	Kompatibilität
None	None	Gültig
WPA+WPA2	None	Gültig
WPA+WPA2	Webauthentifizierung	Ungültig
WPA-PSK/WPA2-PSK	Webauthentifizierung	Gültig
WPA+WPA2	Web-Passthrough	Ungültig
WPA-PSK/WPA2-PSK	Web-Passthrough	Gültig
WPA+WPA2	Bedingte Web-Umleitung	Gültig
WPA+WPA2	Webumleitung für Splash-Seite	Gültig
WPA+WPA2	VPN-Passthrough	Gültig
802.1x	None	Gültig

802.1x	Webauthentifizierung	Ungültig
802.1x	Web-Passthrough	Ungültig
802.1x	Bedingte Web-Umleitung	Gültig
802.1x	Webumleitung für Splash-Seite	Gültig
802.1x	VPN-Passthrough	Gültig
Statisches WEP	None	Gültig
Statisches WEP	Webauthentifizierung	Gültig
Statisches WEP	Web-Passthrough	Gültig
Statisches WEP	Bedingte Web-Umleitung	Ungültig
Statisches WEP	Webumleitung für Splash-Seite	Ungültig
Statisches WEP	VPN-Passthrough	Gültig
Statisch - WEP+ 802.1x	None	Gültig
Statisch - WEP+ 802.1x	Webauthentifizierung	Ungültig
Statisch - WEP+ 802.1x	Web-Passthrough	Ungültig
Statisch - WEP+ 802.1x	Bedingte Web-Umleitung	Ungültig
Statisch - WEP+ 802.1x	Webumleitung für Splash-Seite	Ungültig
Statisch - WEP+ 802.1x	VPN-Passthrough	Ungültig
CKIP	None	Gültig
CKIP	Webauthentifizierung	Gültig
CKIP	Web-Passthrough	Gültig
CKIP	Bedingte Web-Umleitung	Ungültig
CKIP	Webumleitung für Splash-Seite	Ungültig
CKIP	VPN-Passthrough	Gültig

Zugehörige Informationen

- Wireless LAN-Controller und Lightweight Access Point - Konfigurationsbeispiel
- Registrierung von Lightweight AP (LAP) bei einem Wireless LAN Controller (WLC)
- Konfigurationsleitfaden für Cisco Wireless LAN Controller, Version 7.0.116.0
- Wireless LAN Controller (WLC) – Häufig gestellte Fragen
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.