WLC Layer 2 en Layer 3 Security compatibiliteitsmatrix

Inhoud

Inleiding

Dit document biedt de compatibiliteitsmatrix voor de beveiligingsmechanismen Layer 2 en Layer 3 die op de draadloze LAN-controller (WLC) worden ondersteund.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van de configuratie van lichtgewicht AP's en Cisco WLC's
- Basiskennis van Lichtgewicht AP Protocol (LWAPP)
- Basiskennis van draadloze beveiligingsoplossingen

Gebruikte componenten

De informatie in dit document is gebaseerd op een Cisco 4400/2100 Series WLC die firmware-versie 7.0.16.0 uitvoert

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor

meer informatie over documentconventies.

Cisco Unified Wireless Network Security oplossingen

Het Cisco Unified Wireless Network ondersteunt Layer 2 en Layer 3-beveiligingsmethoden.

- Layer 2-beveiliging
- Layer 3-beveiliging (voor WLAN) of Layer 3-beveiliging (voor gastLAN)

Layer 2-beveiliging wordt niet ondersteund op Guest LAN's.

Deze tabel toont de verschillende beveiligingsmethoden van Layer 2 en Layer 3 die op de draadloze LAN-controller worden ondersteund. Deze beveiligingsmethoden kunnen worden ingeschakeld vanaf het tabblad **Beveiliging** op de **WLAN's > De** pagina **Bewerken** van het WLAN.

Layer 2-beveiligingsmechanisme		
Parameter		**Beschrijving**
Layer 2-beveiliging	None	Geen Layer 2-beveiliging geselecteerd.
	WPA+WPA2	Gebruik deze instelling om Wi-Fi Protected Access in te schakelen.
	802.1X	Gebruik deze instelling om 802.1x-verificatie in te schakelen.
	Statische WEP	Gebruik deze instelling om statische WEP-codering in te schakelen.
	Statisch WEP + 802.1x	Gebruik deze instelling om zowel statische WEP- als 802.1x-parameters in te schakelen.
	CKIP	Gebruik deze instelling om Cisco Key Integrity Protocol (CKIP) in te schakelen. Functioneel op AP-modellen 1100, 1130 en 1200, maar niet op AP 1000. Aironet IE moet ingeschakeld zijn om deze functie te laten werken. CKIP breidt de coderingssleutels uit tot 16 bytes.
MAC-filtering	Selecteer deze optie om clients te filteren op MAC-adres. Configureer de clients lokaal op MAC-adres in de MAC Filters > Nieuwe pagina. Anders configureert u de clients op een RADIUS-server.	
Layer 3 Security Mechanism (voor WLAN)		
Parameter		**Beschrijving**

Layer 3-beveiliging	None	Geen Layer 3-beveiliging geselecteerd.
	IPSEC	Gebruik deze instelling om IPSec in te schakelen. U moet de beschikbaarheid van software en de compatibiliteit van de clienthardware controleren voordat u IPSec implementeert. **Opmerking:** de optionele VPN/Enhanced Security Module (crypto-processorkaart) moet zijn geïnstalleerd om IPSec mogelijk te maken. Controleer of het op uw controller is geïnstalleerd op de pagina Inventaris.
	VPN-doorgifte	Gebruik deze instelling om VPN Pass-Through in te schakelen. **Opmerking:** deze optie is niet beschikbaar voor Cisco 5500 Series controllers en Cisco 2100 Series controllers. U kunt deze functionaliteit echter repliceren op een Cisco 5500 Series controller of Cisco 2100 Series controller door een open WLAN te maken met een ACL.
Webbeleid	Selecteer dit selectievakje om webbeleid in te schakelen. De controller verstuurt DNS-verkeer naar en van draadloze clients vóór de verificatie. **Opmerking:** webbeleid kan niet worden gebruikt in combinatie met opties voor IPsec of VPN-doorgifte. Deze parameters worden weergegeven: • Verificatie—Als u deze optie selecteert, wordt de gebruiker gevraagd om een gebruikersnaam en wachtwoord tijdens de verbinding van de client met het draadloze netwerk. • Passthrough-Als u deze optie selecteert, kan de gebruiker rechtstreeks toegang tot het netwerk krijgen zonder de gebruikersnaam en wachtwoordverificatie. • Voorwaardelijk Web Redirect-als u deze optie selecteert, kan de gebruiker voorwaardelijk worden omgeleid naar een	

	bepaalde webpagina nadat de 802.1X-verificatie met succes is voltooid. U kunt de omleidingspagina en de voorwaarden waaronder de omleiding op uw RADIUS-server plaatsvindt, specificeren. • Splitspagina Web Redirect - Als u deze optie selecteert, wordt de gebruiker omgeleid naar een bepaalde webpagina nadat de 802.1X-verificatie met succes is voltooid. Nadat de omleiding is uitgevoerd, heeft de gebruiker volledige toegang tot het netwerk. U kunt de splash-webpagina opgeven op uw RADIUS-server. • Op MAC Filter fout-laat Web authentificatie toe de filtermislukkingen van MAC.
ACL-verificatie vooraf	Selecteer de ACL die moet worden gebruikt voor verkeer tussen de client en de controller.
Mondiale configuratie met override	Hier wordt weergegeven als u Verificatie selecteert. Schakel dit selectievakje in om de globale verificatieconfiguratie op de webpagina voor inloggen te negeren.
Type webautorisatie	Hier wordt weergegeven als u Webbeleid selecteert en Globale Config override. Selecteer een type webverificatie: • Intern • Aangepast (gedownload) Aanmelden Pagina-Selecteer een inlogpagina in de vervolgkeuzelijst.Aanmeldingsfout pagina—Selecteer een aanmeldpagina die wordt weergegeven aan de client als de webverificatie mislukt.Uitlogingspagina - Selecteer een inlogpagina die wordt weergegeven aan de client wanneer de gebruiker zich afmeldt van het systeem. • Extern (omleiden naar externe server) URL—Voer de URL van de externe server in.
E-mail invoer	Toont dit als u Passthrough selecteert. Als u deze optie selecteert, wordt u gevraagd uw e-mailadres op te geven wanneer u verbinding maakt met het netwerk.
Layer 3 Security Mechanism (voor gastnetwerk)	
Parameter	**Beschrijving**

Layer 3-beveiliging	None	Geen Layer 3-beveiliging geselecteerd.
	Web verificatie	Als u deze optie selecteert, wordt u gevraagd om een gebruikersnaam en wachtwoord tijdens het verbinden van de client met het netwerk.
	Web Passthrough	Als u deze optie selecteert, kunt u rechtstreeks toegang tot het netwerk krijgen zonder de gebruikersnaam en wachtwoordverificatie.
ACL-verificatie vooraf		Selecteer de ACL die moet worden gebruikt voor verkeer tussen de client en de controller.
Mondiale configuratie met override		Schakel dit selectievakje in om de globale verificatieconfiguratie op de webpagina voor inloggen te negeren.
Type webautorisatie		Hier wordt weergegeven als u Override Global Config selecteert. Selecteer een type webverificatie: • Intern • Aangepast (gedownload) Aanmelden Pagina- Selecteer een inlogpagina in de vervolgkeuzelijst.Aanmeldingsfout pagina—Selecteer een aanmeldpagina die wordt weergegeven aan de client als de webverificatie mislukt.Uitlogingspagina - Selecteer een inlogpagina die wordt weergegeven aan de client wanneer de gebruiker zich afmeldt van het systeem. • Extern (omleiden naar externe server) URL—Voer de URL van de externe server in.

E-mail invoer	Vertoningen als u Web Passthrough selecteert. Als u deze optie selecteert, wordt u gevraagd uw e-mailadres op te geven wanneer u verbinding maakt met het netwerk.

Opmerking: in controller softwarerelease 4.1.185.0 of hoger wordt CKIP alleen ondersteund voor gebruik met statische WEP. Het wordt niet ondersteund voor gebruik met dynamisch WEP. Daarom kan een draadloze client die is geconfigureerd om CKIP met dynamisch WEP te gebruiken, niet worden gekoppeld aan een draadloos LAN dat voor CKIP is geconfigureerd. Cisco raadt u aan dynamisch WEP te gebruiken zonder CKIP (dat minder veilig is) of WPA/WPA2 met TKIP of AES (die beter beveiligd zijn).

Draadloze LAN-controllerlaag 2 - Layer 3 security compatibiliteitsmatrix

Wanneer u beveiliging op een draadloos LAN configureert, kunnen zowel Layer 2 als Layer 3-beveiligingsmethoden samen worden gebruikt. Niet alle Layer 2-beveiligingsmethoden kunnen echter worden gebruikt met alle Layer 3-beveiligingsmethoden. Deze tabel toont de compatibiliteitsmatrix voor Layer 2 en Layer 3-beveiligingsmethoden die op de draadloze LAN-controller worden ondersteund.

Layer 2-beveiligingsmechanisme	Layer 3-beveiligingsmechanisme	Compatibiliteit
None	None	geldig
WPA+WPA2	None	geldig
WPA+WPA2	Web verificatie	Ongeldig
WPA-PSK/WPA2-PSK	Web verificatie	geldig
WPA+WPA2	Web Passthrough	Ongeldig
WPA-PSK/WPA2-PSK	Web Passthrough	geldig
WPA+WPA2	Voorwaardelijke omleiding van web	geldig
WPA+WPA2	Webomleiding spraakpagina	geldig
WPA+WPA2	VPN-doorgifte	geldig
802.1x	None	geldig
802.1x	Web verificatie	Ongeldig
802.1x	Web Passthrough	Ongeldig
802.1x	Voorwaardelijke omleiding van web	geldig
802.1x	Webomleiding spraakpagina	geldig

802.1x	VPN-doorgifte	geldig
Statische WEP	None	geldig
Statische WEP	Web verificatie	geldig
Statische WEP	Web Passthrough	geldig
Statische WEP	Voorwaardelijke omleiding van web	Ongeldig
Statische WEP	Webomleiding spraakpagina	Ongeldig
Statische WEP	VPN-doorgifte	geldig
Statisch-WEP+ 802.1x	None	geldig
Statisch-WEP+ 802.1x	Web verificatie	Ongeldig
Statisch-WEP+ 802.1x	Web Passthrough	Ongeldig
Statisch-WEP+ 802.1x	Voorwaardelijke omleiding van web	Ongeldig
Statisch-WEP+ 802.1x	Webomleiding spraakpagina	Ongeldig
Statisch-WEP+ 802.1x	VPN-doorgifte	Ongeldig
CKIP	None	geldig
CKIP	Web verificatie	geldig
CKIP	Web Passthrough	geldig
CKIP	Voorwaardelijke omleiding van web	Ongeldig
CKIP	Webomleiding spraakpagina	Ongeldig
CKIP	VPN-doorgifte	geldig

Gerelateerde informatie

- Basisconfiguratievoorbeeld van draadloze LAN-controller en lichtgewicht access point
- Lichtgewicht AP (LAP)-registratie voor een draadloze LAN-controller (WLC)
- Configuratiehandleiding voor Cisco draadloze LAN-controllers, release 7.0.16.0
- Veelgestelde vragen over wireless LAN-controller (WLC)
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.