Esempio di configurazione di Infrastructure Management Frame Protection (MFP) con WLC e LAP

Sommario

Introduzione

In questo documento viene introdotta una nuova funzionalità di sicurezza nella tecnologia wireless denominata Management Frame Protection (MFP). In questo documento viene descritto anche come configurare le stampanti multifunzione nei dispositivi dell'infrastruttura, come i Lightweight Access Point (LAP) e i Wireless LAN Controller (WLC).

Prerequisiti

Requisiti

- Conoscenza di come configurare il WLC e il LAP per il funzionamento di base

- Conoscenze base dei frame di gestione IEEE 802.11

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 2000 WLC con firmware versione 4.1
- Cisco 1131AG LAP
- Cisco Aironet 802.11a/b/g Client Adapter con firmware versione 3.6
- Cisco Aironet Desktop Utility versione 3.6

Nota: la versione MFP è supportata dalla versione WLC 4.0.155.5 e successive, anche se la versione 4.0.206.0 offre prestazioni ottimali con la versione MFP. La funzionalità MFP client è supportata nella versione 4.1.171.0 e successive.

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.

Premesse

In 802.11, i frame di gestione come (de)autenticazione, (dis)associazione, beacon e probe sono sempre non autenticati e non crittografati. In altre parole, i frame di gestione 802.11 vengono sempre inviati in modo non protetto, a differenza del traffico di dati, che viene crittografato con protocolli quali WPA, WPA2 o, almeno, WEP e così via.

Ciò consente all'autore di un attacco di eseguire lo spoofing di un frame di gestione dall'access point per attaccare un client associato a un access point. Con i frame di gestione oggetto di spoofing, un utente non autorizzato può eseguire le azioni seguenti:

- Eseguire un DOS (Denial of Service) sulla WLAN
- Tentare un attacco Man in the Middle al client quando si riconnette
- Eseguire un attacco di dizionario non in linea

La tecnologia MFP consente di superare questi ostacoli grazie all'autenticazione dei frame di gestione 802.11 scambiati nell'infrastruttura di rete wireless.

Nota: questo documento è incentrato sull'**infrastruttura e sulla piattaforma multifunzione client**.

Nota: esistono alcune restrizioni per la comunicazione tra alcuni client wireless e dispositivi di infrastruttura abilitati per MFP. La funzione MFP aggiunge un lungo set di elementi di informazione a ciascuna richiesta di sonda o beacon SSID. Alcuni client wireless, ad esempio PDA, smartphone, scanner di codici a barre e così via, dispongono di memoria e CPU limitate. Non è quindi possibile elaborare queste richieste o questi beacon. Di conseguenza, non è possibile visualizzare completamente l'SSID o associarlo a questi dispositivi di infrastruttura a causa di

un'errata comprensione delle funzionalità SSID. Questo problema non riguarda solo le stampanti multifunzione. Ciò si verifica anche con qualsiasi SSID che dispone di più elementi di informazione (IE). È sempre consigliabile verificare gli SSID *abilitati per* MFP nell'ambiente con tutti i tipi di client disponibili prima di distribuirli in tempo reale.

Nota:

Questi sono i componenti della PSM infrastruttura:

- **Protezione del frame di gestione**: quando la protezione del frame di gestione è abilitata, AP aggiunge l'elemento di verifica dell'integrità dei messaggi (MIC IE) a ciascun frame di gestione trasmesso. Ogni tentativo di copiare, modificare o riprodurre il frame invalida il MIC. Un access point, configurato per convalidare i frame MFP, riceve un frame con MIC non valido e lo segnala al WLC.
- **Convalida del frame di gestione**: quando la convalida del frame di gestione è abilitata, l'access point convalida ogni frame di gestione ricevuto dagli altri access point nella rete. Assicura che MIC IE sia presente (quando il creatore è configurato per trasmettere i frame MFP) e corrisponde al contenuto del frame di gestione. Se riceve un frame che non contiene un MIC IE valido da un BSSID che appartiene a un punto di accesso configurato per trasmettere i frame MFP, segnala la discrepanza al sistema di gestione di rete.**Nota:** per il corretto funzionamento dei timestamp, tutti i WLC devono essere sincronizzati con il protocollo NTP (Network Time Protocol).
- **Report degli eventi**: il punto di accesso notifica il WLC quando rileva un'anomalia. WLC aggrega gli eventi anomali e li segnala al gestore della rete tramite trap SNMP.

Funzionalità MFP infrastruttura

In MFP, l'hash di tutti i frame di gestione viene eseguito per creare un controllo dell'integrità dei messaggi (MIC, Message Integrity Check). Il MIC viene aggiunto alla fine del frame (prima della sequenza di controllo del frame (FCS)).

- In un'architettura wireless centralizzata, il protocollo MFP dell'infrastruttura viene abilitato/disabilitato sul WLC (configurazione globale). La protezione può essere disabilitata in modo selettivo per ciascuna WLAN e la convalida può essere disabilitata in modo selettivo per ciascun access point.
- La protezione può essere disabilitata sulle WLAN utilizzate dai dispositivi che non sono in grado di gestire gli IE aggiuntivi.
- La convalida deve essere disabilitata sui punti di accesso sovraccarichi o sovraccarichi.

Quando il protocollo MFP è abilitato su una o più WLAN configurate nel WLC, il WLC invia una chiave univoca a ciascuna radio su ciascun AP registrato. I frame di gestione vengono inviati dall'access point sulle WLAN abilitate per MFP. Questi access point sono etichettati con un MIC IE di protezione dei frame. Ogni tentativo di modificare il frame invalida il messaggio, il che fa sì che l'access point ricevente configurato per rilevare i frame MFP segnali la discrepanza al controller WLAN.

Si tratta di un processo graduale di PFP implementato in un ambiente di roaming:

1. Se la funzionalità MFP è abilitata a livello globale, il WLC genera una chiave univoca per ogni punto di accesso/WLAN configurato per la funzionalità MFP. I WLC comunicano tra loro

in modo che tutti i WLC conoscano le chiavi di tutti gli AP/BSS in un dominio di mobilità.**Nota:** tutti i controller di un gruppo di dispositivi mobili/RF devono avere una configurazione MFP identica.
2. Quando un access point riceve un frame protetto da MFP per un BSS di cui non è a conoscenza, memorizza nel buffer una copia del frame e interroga il WLC per ottenere la chiave.
3. Se il BSSID non è noto sul WLC, restituisce il messaggio "Unknown BSSID" all'access point e l'access point scarta i frame di gestione ricevuti da quel BSSID.
4. Se il BSSID è noto sul WLC, ma il MFP è disabilitato su quel BSSID, il WLC restituisce un "BSSID disabilitato". L'access point presume quindi che tutti i frame di gestione ricevuti da quel BSSID non abbiano un MIC MFP.
5. Se il BSSID è noto e il protocollo MFP è abilitato, il WLC restituisce la chiave MFP all'access point richiedente (tramite il tunnel di gestione LWAPP crittografato AES).
6. Il punto di accesso memorizza nella cache le chiavi ricevute in questo modo. Questo tasto viene usato per convalidare o aggiungere MIC IE.

Funzionalità MFP client

La funzione MFP del client protegge i client autenticati da frame falsificati, impedendo l'efficacia di molti degli attacchi comuni alle LAN wireless. La maggior parte degli attacchi, ad esempio quelli di deautenticazione, ripristina semplicemente le prestazioni peggiorate quando sono in conflitto con client validi.

In particolare, la funzione MFP client cripta i frame di gestione inviati tra i punti di accesso e i client CCXv5 in modo che sia i punti di accesso che i client possano adottare misure preventive ed eliminare i frame di gestione di classe 3 contraffatti (ovvero, i frame di gestione passati tra un punto di accesso e un client autenticato e associato). La funzione MFP client sfrutta i meccanismi di sicurezza definiti da IEEE 802.11i per proteggere questi tipi di frame di gestione unicast di classe 3: disassociazione, deautenticazione e azione QoS (WMM). La funzionalità MFP client è in grado di proteggere una sessione del punto di accesso client dal tipo più comune di attacco Denial of Service. Protegge i frame di gestione di classe 3 con lo stesso metodo di crittografia utilizzato per i frame di dati della sessione. Se un frame ricevuto dal punto di accesso o dal client non viene decrittografato, viene eliminato e l'evento viene segnalato al controller.

Per utilizzare la funzionalità MFP client, i client devono supportare la funzionalità MFP CCXv5 e negoziare WPA2 con TKIP o AES-CCMP. Per ottenere la chiave PMK è possibile utilizzare EAP o PSK. La funzionalità CCKM e la gestione della mobilità dei controller vengono utilizzate per distribuire le chiavi di sessione tra i punti di accesso o il roaming veloce di layer 2 e layer 3.

Per evitare attacchi ai frame di trasmissione, gli access point che supportano CCXv5 non emettono frame di gestione di classe 3 (come disassociazione, deautenticazione o azione). I client e i punti di accesso CCXv5 devono eliminare i frame di gestione broadcast class 3.

La funzionalità MFP client integra la funzionalità MFP infrastruttura anziché sostituirla, in quanto la funzionalità MFP infrastruttura continua a rilevare e segnalare frame unicast non validi inviati a client che non supportano la funzionalità MFP client, nonché frame di gestione di classe 1 e 2 non validi. L'opzione di gestione delle infrastrutture viene applicata solo ai frame di gestione non protetti dall'opzione di gestione delle infrastrutture client.

Componenti MFP client

La funzionalità PMS client è costituita dai seguenti componenti:

- Generazione e distribuzione delle chiavi
- Protezione e convalida dei frame di gestione
- Segnalazioni errori

Generazione e distribuzione delle chiavi

La funzionalità di filtro multifunzione client non utilizza i meccanismi di generazione e distribuzione delle chiavi derivati per la funzionalità di filtro multifunzione infrastruttura. Al contrario, la funzione MFP client sfrutta i meccanismi di sicurezza definiti da IEEE 802.11i per proteggere anche i frame di gestione unicast di classe 3. Le stazioni devono supportare CCXv5 e devono negoziare TKIP o AES-CCMP per utilizzare l'MFP client. Per ottenere la chiave PMK è possibile utilizzare EAP o PSK.

Protezione dei frame di gestione

I frame di gestione unicast di classe 3 sono protetti con l'applicazione di AES-CCMP o TKIP in modo simile a quello già utilizzato per i frame dati. Parti dell'intestazione del frame vengono copiate nel componente payload crittografato di ciascun frame per una maggiore protezione, come descritto nelle sezioni seguenti.

Sono protetti i seguenti tipi di frame:

- Disassociazione
- Deautenticazione
- Frame azioni QoS (WMM)

I frame dati protetti da AES-CCMP e TKIP includono un contatore di sequenza nei campi IV, che viene utilizzato per impedire il rilevamento della riproduzione. Il contatore di trasmissione corrente viene utilizzato sia per i frame di dati che per i frame di gestione, ma un nuovo contatore di ricezione viene utilizzato per i frame di gestione. I contatori di ricezione vengono controllati per assicurarsi che ogni frame abbia un numero maggiore dell'ultimo frame ricevuto (per assicurarsi che i frame siano univoci e non siano stati riprodotti), quindi questo schema non importa che i valori ricevuti siano non sequenziali.

Segnalazioni errori

I meccanismi di reporting MFP-1 vengono utilizzati per segnalare gli errori di deincapsulamento del frame di gestione rilevati dai punti di accesso. In altri termini, il WLC raccoglie le statistiche sugli errori di convalida dei dispositivi multifunzione e inoltra periodicamente le informazioni raccolte al WCS.

Gli errori di violazione MFP rilevati dalle stazioni client vengono gestiti dalla funzionalità Roaming e Real Time Diagnostics di CCXv5 e non rientrano nell'ambito di questo documento.

Protezione frame gestione trasmissione

Per prevenire attacchi che utilizzano frame di trasmissione, i punti di accesso che supportano CCXv5 non trasmettono alcun frame di gestione di classe broadcast 3 (ovvero disassociazione, disassociazione, impostazione predefinita o azione), ad eccezione dei frame di

deautenticazione/disassociazione di contenimento non autorizzati. Le stazioni client compatibili con CCXv5 devono eliminare i frame di gestione broadcast di classe 3. Si presume che le sessioni MFP si trovino in una rete adeguatamente protetta (autenticazione avanzata più TKIP o CCMP), quindi non è un problema ignorare le trasmissioni di contenimento non autorizzate.

Analogamente, i punti di accesso eliminano i frame di gestione delle trasmissioni in entrata. Non sono attualmente supportati frame di gestione broadcast in ingresso, pertanto non sono necessarie modifiche del codice.

Piattaforme supportate

Queste piattaforme sono supportate:

- Controller WLAN200621064400WiSMCatalyst 3750 con controller 440x incorporatoRouter 26/28/37/38xx
- Access point LWAPPAP 1000AP 1100, 1130AP 1200, 1240, 1250AP 1310
- Software ClientADU 3.6.4 e versioni successive
- Sistemi di gestione della reteSistema colori Windows

l'access point 1500 Mesh LWAPP non è supportato in questa versione.

Modalità supportate

I punti di accesso basati su LWAPP che funzionano in queste modalità supportano le funzionalità MFP client:

Modalità Access Point Supportate	
Modalità	**Supporto MFP client**
Locale	Sì
Monitor (Monitora)	No
Sniffer	No
Rogue Detector	No
Hybrid REAP	Sì
REAP	No
Radice bridge	Sì
WGB	No

Supporto di celle miste

Le stazioni client non compatibili con CCXv5 possono essere associate a una WLAN MFP-2. I punti di accesso rilevano quali client sono compatibili con MFP-2 e quali non sono in grado di determinare se le misure di sicurezza MFP-2 vengono applicate ai frame di gestione unicast in uscita e previste nei frame di gestione unicast in entrata.

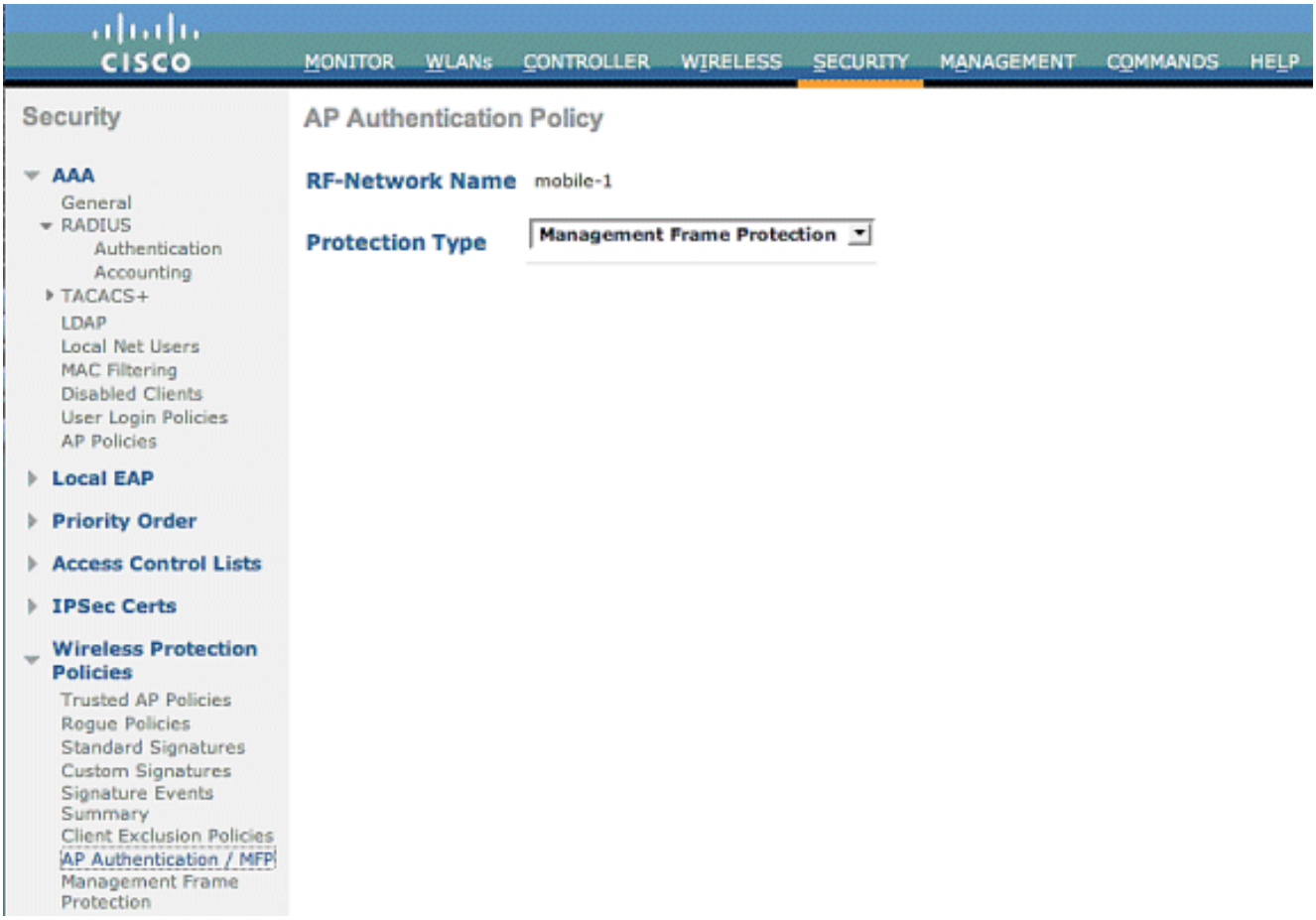
Configurazione

Configurare una stampante multifunzione su un controller

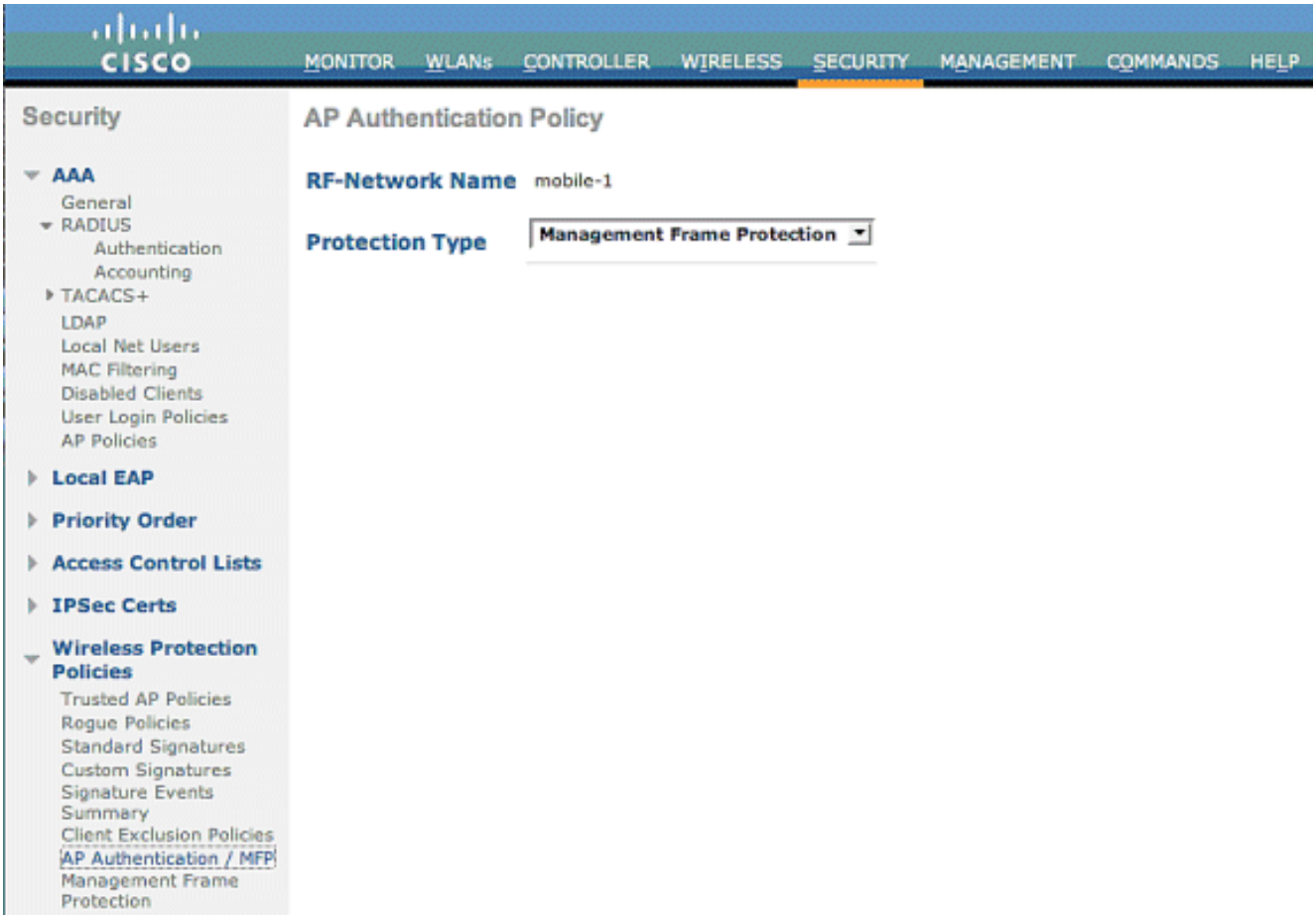
Èpossibile configurare le stampanti multifunzione su un controller a livello globale. Quando si esegue questa operazione, la **protezione e la convalida del frame di gestione vengono attivate per impostazione predefinita per ogni punto di accesso unito** e l'autenticazione del punto di accesso viene disattivata automaticamente.

Eseguire la procedura seguente per configurare le stampanti multifunzione a livello globale su un controller.

1. Dalla GUI del controller, fare clic su **Security** (Sicurezza). Nella schermata risultante, fare clic su **Autenticazione AP/MFP** in **Criteri di protezione wireless**.



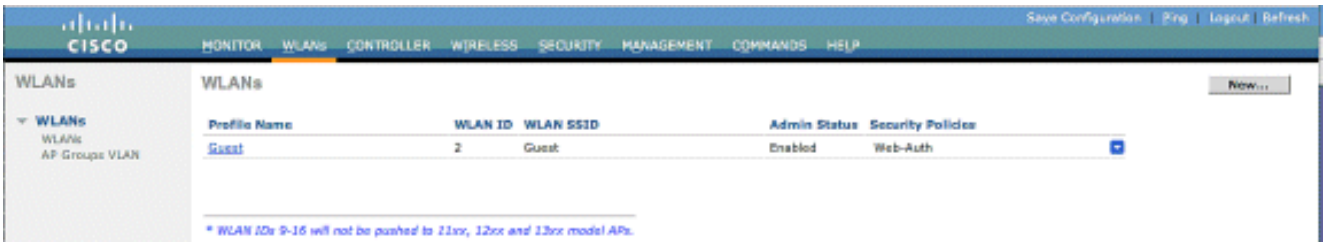
2. Nel criterio di autenticazione AP, scegliere **Protezione frame di gestione** dal menu a discesa **Tipo di protezione** e fare clic su **Applica**.



Configurazione di una stampante multifunzione su rete WLAN

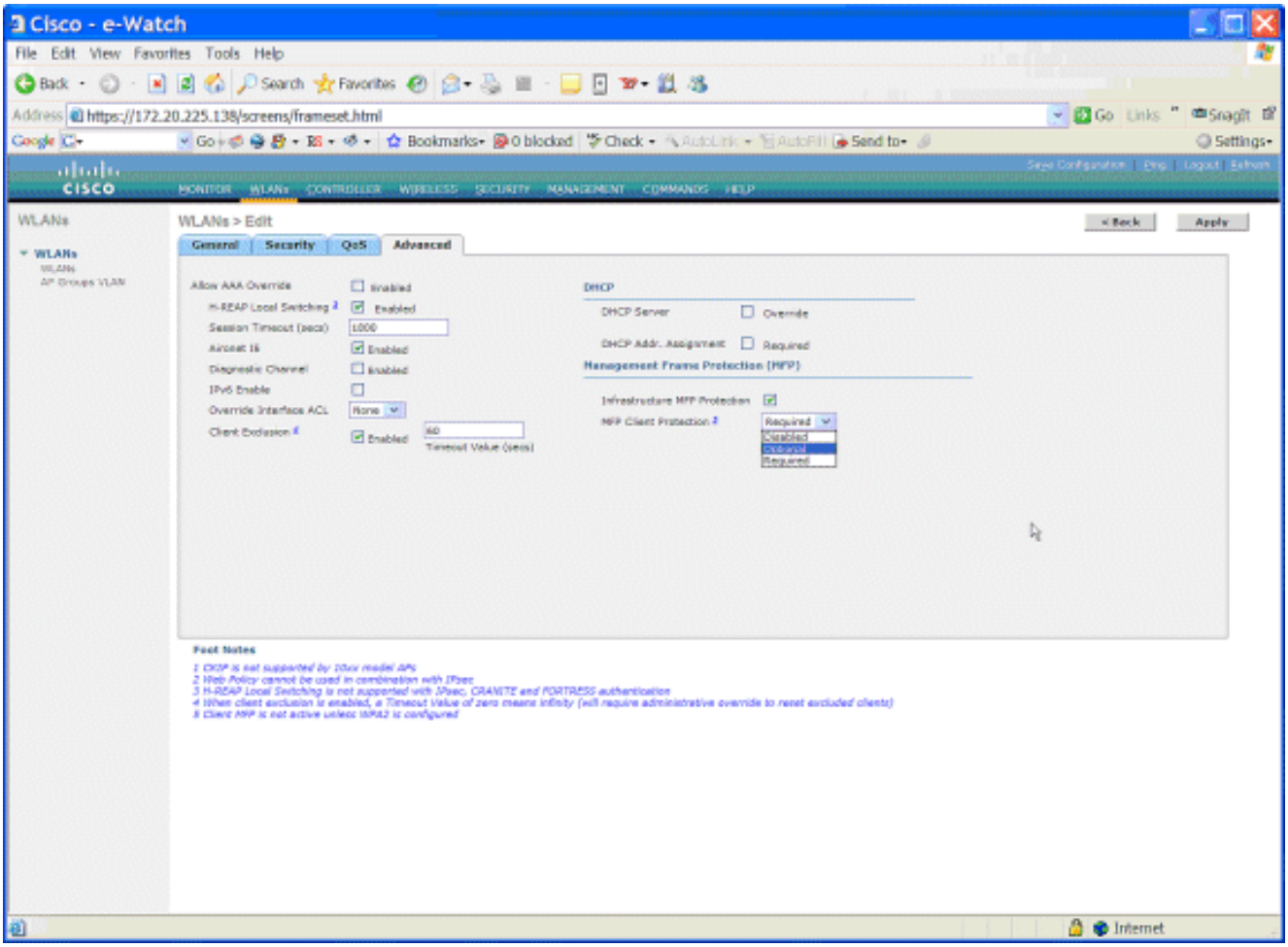
Èinoltre possibile abilitare/disabilitare la protezione MFP dell'infrastruttura e la MFP client su ciascuna WLAN configurata sul WLC. Entrambi i dispositivi sono abilitati per impostazione predefinita tramite la protezione MFP dell'infrastruttura, che è attiva solo se abilitata globalmente, e la protezione MFP del client è attiva solo se la WLAN è configurata con la protezione WPA2. Per abilitare la funzionalità MFP su una WLAN, attenersi alla procedura seguente:

1. Dall'interfaccia utente del WLC, fare clic su **WLAN**, quindi su **New** (Nuovo) per creare una nuova
WLAN.



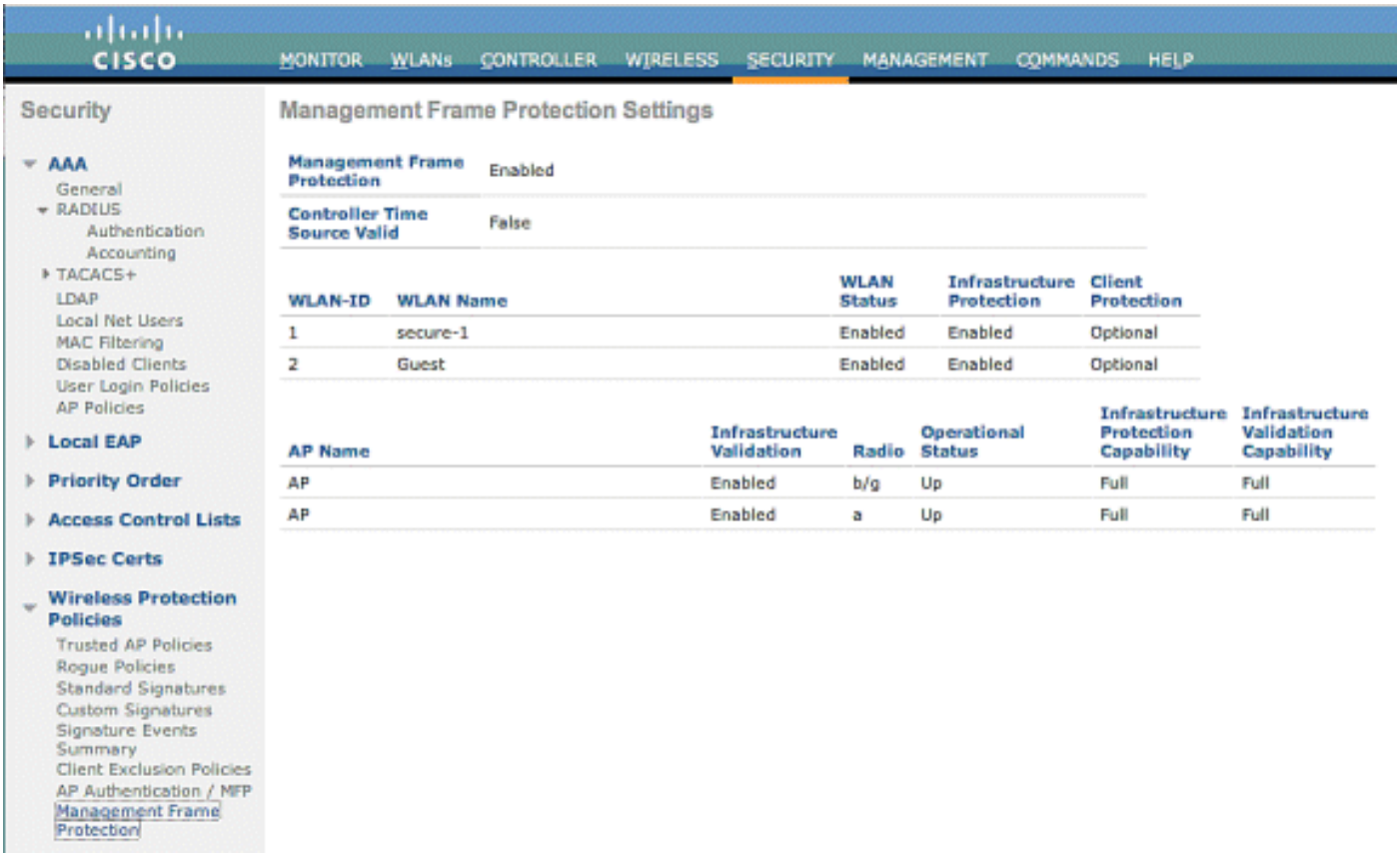
2. Nella pagina di modifica delle WLAN, andare alla scheda *Advanced* (Avanzate) e selezionare la casella di controllo **Infrastructure MFP Protection** (Protezione multifunzione infrastruttura) per abilitare la funzionalità Infrastructure MFP su questa WLAN. Per disabilitare la protezione della scheda multifunzione dell'infrastruttura per la WLAN, deselezionare questa casella di controllo. Per abilitare la funzione MFP client, scegliere l'opzione richiesta o facoltativa dal menu a discesa. Se si sceglie Client MFP= Obbligatorio, verificare che tutti i client dispongano del supporto per MFP-2 o che non siano in grado di connettersi. Se si sceglie l'opzione facoltativa, i client abilitati per le stampanti multifunzione e non possono connettersi alla stessa

WLAN.



Verifica

Per verificare le configurazioni MFP dalla GUI, fare clic su **Management Frame Protection** in Wireless Protection Policies (Criteri di protezione wireless) nella pagina Security (Sicurezza). Viene visualizzata la pagina Impostazioni MFP.



Nella pagina MFP Settings (Impostazioni MFP), è possibile visualizzare la configurazione MFP su WLC, LAP e WLAN. Questo è un esempio.

- Il campo Management Frame Protection (Protezione frame di gestione) mostra se MFP è abilitato a livello globale per il WLC.
- Il campo Origine tempo controller valido indica se l'ora WLC è impostata localmente (tramite l'immissione manuale dell'ora) o tramite un'origine esterna (ad esempio un server NTP). Se l'ora è impostata da un'origine esterna, il valore di questo campo è "True". Se l'ora è impostata localmente, il valore è "False". L'origine tempo viene usata per convalidare i frame di gestione tra punti di accesso di diversi WLC in cui è configurata anche la mobilità.**Nota:** se la funzionalità MFP è abilitata su tutti i WLC di un gruppo di mobilità/RF, si consiglia sempre di utilizzare un server NTP per impostare il tempo WLC in un gruppo di mobilità.
- Il campo **Protezione MFP** mostra se la funzionalità MFP è abilitata per le singole WLAN.
- Nel campo **Convalida PAM** viene indicato se la funzione PAM è abilitata per i singoli access point.

I comandi show possono essere utili:

- **show wps summary**: utilizzare questo comando per visualizzare un riepilogo dei criteri di protezione wireless correnti (tra cui MFP) del WLC.
- **show wps mfp summary**: per visualizzare l'impostazione MFP globale corrente del WLC, immettere questo comando.
- show ap config general *AP_name*: ***per visualizzare lo stato MFP corrente di un particolare punto di accesso, immettere questo comando.***

Questo è un esempio dell'output del comando **show ap config general *AP_name***:

```
(Cisco Controller) >show ap config general AP
```

```
Cisco AP Identifier.............................. 4
Cisco AP Name.................................... AP
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-AB    802.11a:-AB
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-A
Switch Port Number .............................. 29
MAC Address...................................... 00:19:2f:7e:3a:30
IP Address Configuration......................... DHCP
IP Address....................................... 172.20.225.142
IP NetMask....................................... 255.255.255.248
Gateway IP Addr.................................. 172.20.225.137
Cisco AP Location................................ default location
Cisco AP Group Name.............................. default-group
Primary Cisco Switch.............................
Secondary Cisco Switch..........................
Tertiary Cisco Switch...........................
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... H-Reap
Public Safety ................................... Global: Disabled, Local: Disabled
Remote AP Debug ................................. Disabled
S/W  Version .................................... 4.1.169.24
Boot  Version ................................... 12.3.7.1
Mini IOS Version ................................ 3.0.51.0
Stats Reporting Period .......................... 180
LED State........................................ Enabled
PoE Pre-Standard Switch.......................... Disabled
PoE Power Injector MAC Addr...................... Disabled
Number Of Slots.................................. 2
AP Model......................................... AIR-LAP1242AG-A-K9
IOS Version...................................... 12.4(20070414:021809)
Reset Button..................................... Enabled
AP Serial Number................................. FTX1035B3QX
AP Certificate Type.............................. Manufacture Installed
H-REAP Vlan mode :............................... Disabled
Management Frame Protection Validation........... Enabled
Console Login Name..............................
Console Login State.............................. Unknown
Ethernet Port Duplex............................. Auto
Ethernet Port Speed.............................. Auto
```

Questo è un esempio dell'output del comando **show wps mfp summary**:

```
(Cisco Controller) >show wps mfp summary

Global MFP state................................. enabled
Controller Time Source Valid..................... false


                                   WLAN       Infra.      Client
WLAN ID  WLAN Name                 Status     Protection  Protection
-------  ------------------------  ---------  ----------  ----------
1        secure-1                  Enabled    Enabled     Optional
2        Guest                     Enabled    Enabled     Optional but inactive (WPA2 not
configured)
```

```
                    Infra.              Operational     --Infra. Capability--
AP Name             Validation  Radio   State           Protection  Validation
------------------- ----------  -----   --------------  ----------  ----------
AP                  Enabled     b/g     Up              Full        Full
```

Questi comandi di debug possono essere utili;

- **debug wps mfp lwapp**: visualizza le informazioni di debug per i messaggi MFP.
- **debug wps mfp detail**: visualizza informazioni di debug dettagliate per i messaggi MFP.
- **debug wps mfp report**: visualizza le informazioni di debug per il report MFP.
- **debug wps mfp mm**: visualizza le informazioni di debug per i messaggi di mobilità MFP (tra controller).

Nota: ci sono anche diversi sniffer Wireless Packet gratuiti disponibili su Internet, che possono essere utilizzati per acquisire e analizzare i frame di gestione 802.11. Alcuni esempi di sniffer di pacchetti sono Omnipeek e Wireshark.

Informazioni correlate

- Configurazione delle soluzioni di sicurezza: Guida alla configurazione WLC
- Configurazione delle soluzioni di sicurezza in WCS
- Esempio di configurazione dell'autenticazione EAP con i controller WLAN (WLC)
- Esempio di configurazione degli ACL sui controller LAN wireless
- Esempio di configurazione dell'autenticazione Web esterna con i controller LAN wireless
- Esempio di assegnazione dinamica di VLAN con il server RADIUS e il controller LAN wireless
- Cisco Secure Services Client con autenticazione EAP-FAST
- FAQ WLC
- Pagina di supporto wireless
- Documentazione e supporto tecnico – Cisco Systems