Guida alla configurazione e alla distribuzione di ELM wIPS adattivo

Sommario

Introduzione

La soluzione Cisco Adaptive Wireless Intrusion Prevention System (wIPS) aggiunge la funzionalità ELM (Enhanced Local Mode), che consente agli amministratori di utilizzare i punti di accesso distribuiti per fornire una protezione completa senza la necessità di una rete di sovrapposizione separata (Figura 1). Prima di ELM e nella tradizionale implementazione Adaptive wIPS, i punti di accesso in modalità monitor (MM) dedicati sono necessari per soddisfare le esigenze di conformità PCI o per proteggere da accessi non autorizzati, penetrazioni e attacchi (Figura 2). ELM fornisce in modo efficace un'offerta paragonabile che facilita l'implementazione della sicurezza wireless riducendo al contempo i costi di capitale e i costi operativi. Questo documento si concentra solo su ELM e non modifica i vantaggi di distribuzione di wIPS esistenti con i punti di accesso MM.

Figura 1 - Distribuzione punto di accesso in modalità locale avanzata

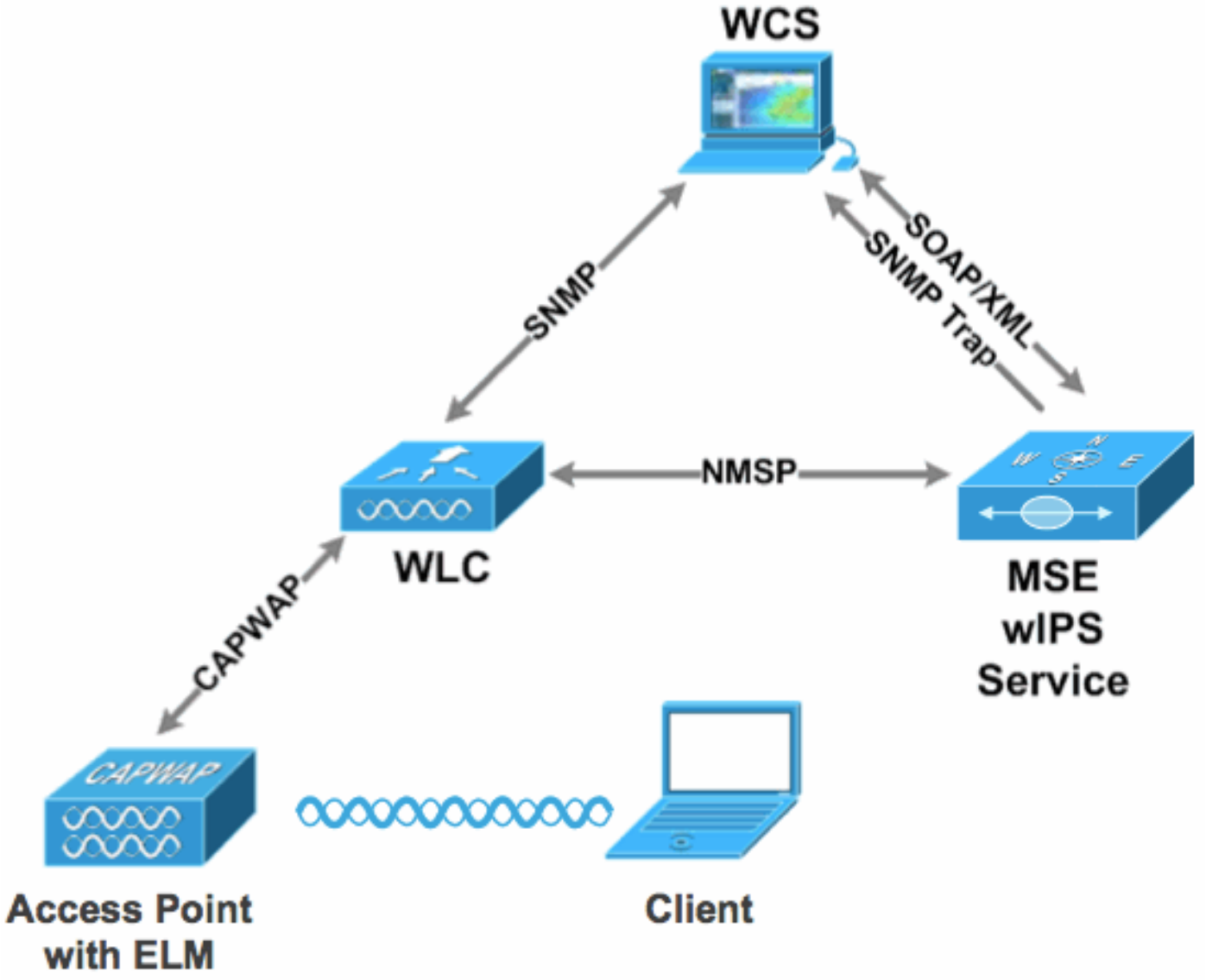
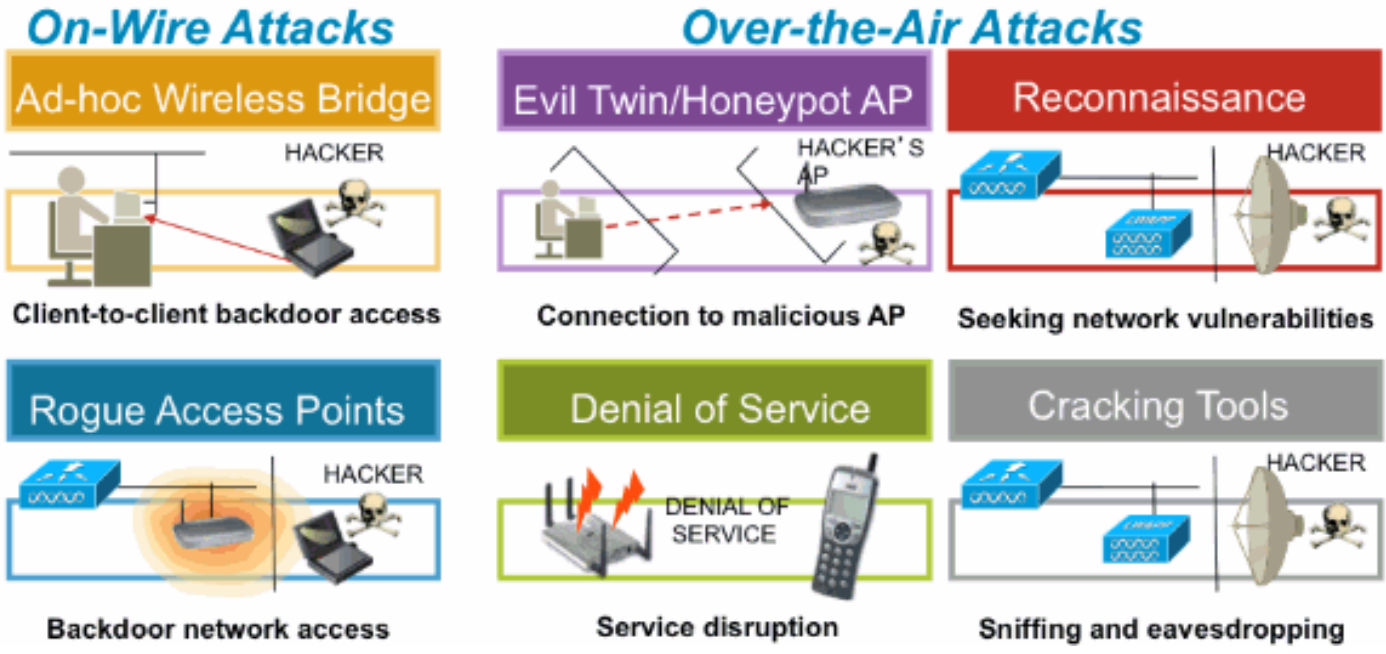


Figura 2 - Principali minacce alla sicurezza wireless



Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Componenti richiesti ELM e versioni minime del codice

- Wireless LAN Controller (WLC) - versione 7.0.116.xx o successive
- AP - versione 7.0.116.xx o successive
- Wireless Control System (WCS) - versione 7.0.172.xx o successive
- Mobility Services Engine - versione 7.0.201.xx o successiva

Supporto delle piattaforme WLC

ELM è supportato sulle piattaforme WLC5508, WLC4400, WLC 2106, WLC2504, WiSM-1 e WiSM-2WLC.

Supporto dei punti di accesso

ELM è supportato sui punti di accesso 11n, tra cui 3500, 1250, 1260, 1040 e 1140.

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.

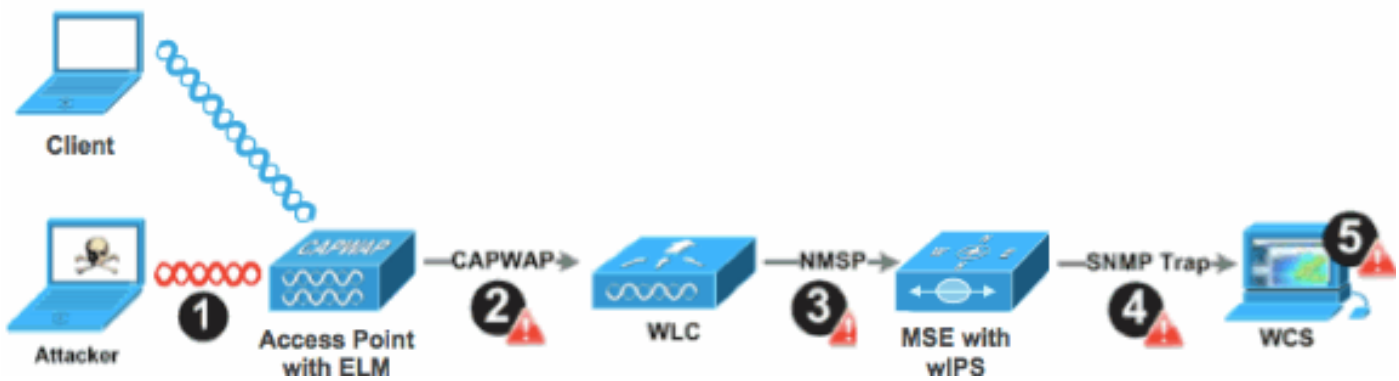
Flusso dell'allarme ELM wIPS

Gli attacchi sono rilevanti solo quando si verificano su punti di accesso dell'infrastruttura attendibili. Gli access point ELM rilevano e comunicano con il controller e sono correlati con il MSE per la creazione di report con la gestione del sistema WCS. La Figura 3 fornisce il flusso di allarme dal punto di vista di un amministratore:

1. Attacco lanciato contro un dispositivo dell'infrastruttura ("Trusted" AP)
2. Rilevato sull'access point ELM comunicato tramite CAPWAP al WLC

3. Trasmesso in modo trasparente a MSE tramite NMSP
4. Accesso al database IPS su MSE inviato a WCS tramite trap SNMP
5. Visualizzato in WCS

Figura 3 - Rilevamento delle minacce e flusso degli allarmi



Considerazioni sulla distribuzione di ELM

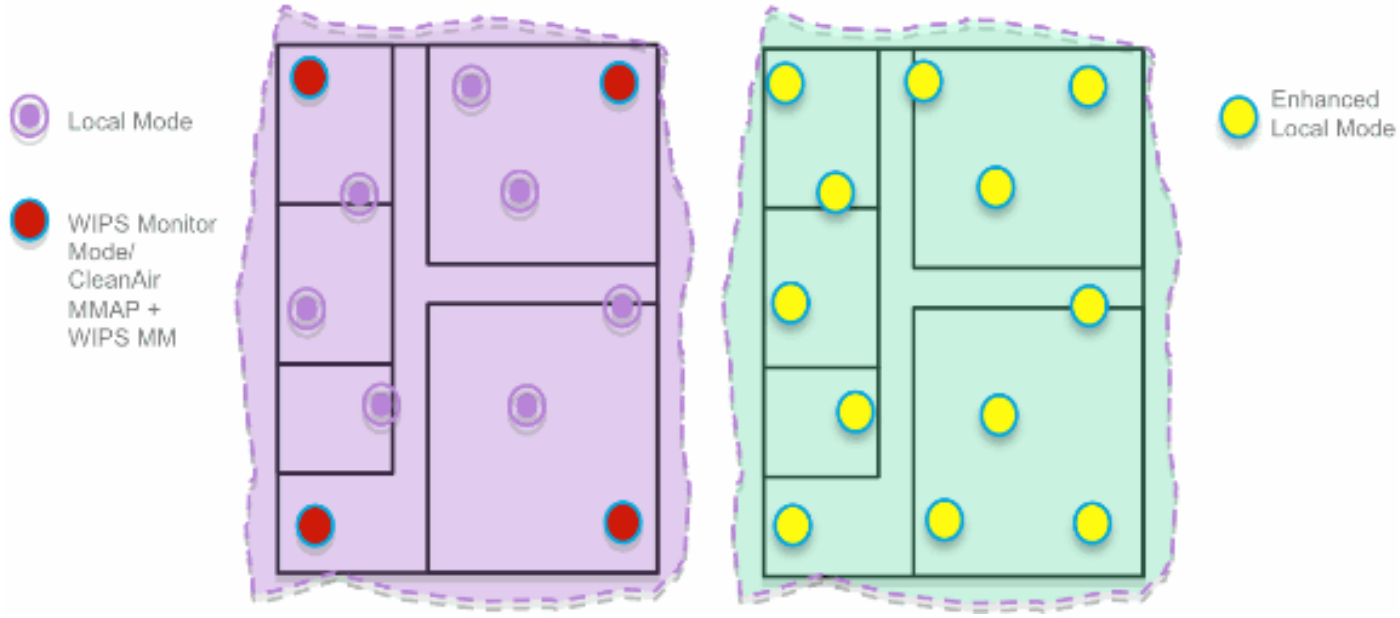
Cisco consiglia di abilitare la modalità ELM su ogni access point in rete per soddisfare la maggior parte delle esigenze di sicurezza dei clienti quando una sovrapposizione di rete e/o i costi sono considerati. La funzione principale ELM funziona in modo efficiente per gli attacchi su canale, senza compromettere le prestazioni su client dati, voce e video e servizi.

Confronto tra ELM e MM dedicati

La Figura 4 fornisce un contrasto generale tra le implementazioni standard dei punti di accesso MMM wIPS e ELM. In sede di riesame, l'intervallo di copertura tipico per entrambe le modalità suggerisce:

- Il punto di accesso WIPS MM dedicato copre in genere 15.000-35.000 piedi quadrati
- Il punto di accesso client-serving copre in genere un'area compresa tra 3.000 e 5.000 metri quadrati

Figura 4 - Sovrapposizione di MM rispetto a tutti i punti di accesso ELM



Nella tradizionale implementazione di IPS adattivi, Cisco consiglia un rapporto di 1 MM per ogni 5 access point in modalità locale, che può variare anche in base alla progettazione della rete e alle indicazioni degli esperti per una copertura ottimale. Considerando ELM, l'amministratore abilita semplicemente la funzionalità software ELM per tutti i punti di accesso esistenti, aggiungendo in modo efficace le operazioni MwIPS al punto di accesso locale in modalità server dati mantenendo le prestazioni.

Prestazioni on-channel e off-channel

Un access point MMM utilizza il 100% del tempo della radio per la scansione di tutti i canali, in quanto non serve alcun client WLAN. La funzione principale di ELM funziona in modo efficace per gli attacchi su canale, senza compromettere le prestazioni su client e servizi dati, voce e video. La differenza principale è nella modalità locale che varia la scansione off-channel; a seconda dell'attività, la scansione off-channel fornisce un tempo di permanenza minimo per raccogliere informazioni sufficienti per classificare e determinare l'attacco. Ad esempio, potrebbe trattarsi di client voce associati e in cui la scansione RRM di AP viene rinviata fino a quando il client voce non viene disassociato per garantire che il servizio non venga influenzato. Per questa considerazione, il rilevamento ELM durante l'utilizzo fuori canale è considerato il miglior sforzo possibile. I punti di accesso ELM adiacenti che funzionano su tutti i canali, nazionali o DCA aumentano l'efficacia, pertanto è consigliabile attivare ELM su ogni punto di accesso in modalità locale per garantire la massima copertura di protezione. Se il requisito è la scansione dedicata a tempo pieno su tutti i canali, si consiglia di installare i punti di accesso MM.

Di seguito vengono descritte le differenze tra i punti di accesso in modalità locale e i punti di accesso mobili:

- Local Mode AP: serve i client WLAN con la scansione del tempo fuori canale, ascolta per 50 ms su ogni canale e offre la scansione configurabile per tutti i canali/country/DCA.
- Modalità di monitoraggio AP: non serve i client WLAN, dedicati solo alla scansione, resta in ascolto di 1,2 s su ogni canale e analizza tutti i canali.

ELM su collegamenti WAN

Cisco ha compiuto notevoli sforzi per ottimizzare le funzionalità in scenari impegnativi, ad esempio l'installazione di access point ELM su collegamenti WAN a larghezza di banda ridotta. La funzione ELM prevede la pre-elaborazione nella determinazione delle firme di attacco nell'access point ed è ottimizzata per funzionare su collegamenti lenti. Come best practice, si consiglia di testare e misurare la baseline per convalidare le prestazioni con ELM su WAN.

Integrazione CleanAir

La funzione ELM è complementare alle operazioni CleanAir con prestazioni e vantaggi simili all'installazione dei punti di accesso MM con i seguenti vantaggi esistenti:

- Intelligenza RF dedicata al silicio
- Riconoscimento dello spettro, riparazione automatica e ottimizzazione automatica
- Rilevamento e mitigazione di minacce e interferenze da parte di canali non standard
- Rilevamento non Wi-Fi come Bluetooth, microonde, telefoni senza fili, ecc.
- Rilevare e individuare gli attacchi DOS dei livelli RF, ad esempio i jammer RF

Caratteristiche e vantaggi di ELM

- Scansione wIPS adattiva nei server dati dei punti di accesso locali e H-REAP
- Protezione senza necessità di una rete di sovrapposizione separata
- Disponibile come download gratuito del software per i clienti wIPS esistenti
- Supporta la conformità PCI per le LAN wireless
- Rilevamento di attacchi completi 802.11 e non 802.11
- Aggiunge funzionalità di analisi legale e reporting
- Integrazione con la gestione CUWM e WLAN esistente
- Flessibilità di impostazione dei punti di accesso MM integrati o dedicati
- Pre-elaborazione presso i punti di accesso per ridurre al minimo il backhaul dei dati (vale a dire, funziona su collegamenti con larghezza di banda molto ridotta)
- Basso impatto sui dati del server

Licenze ELM

ELM wIPS aggiunge una nuova licenza all'ordine:

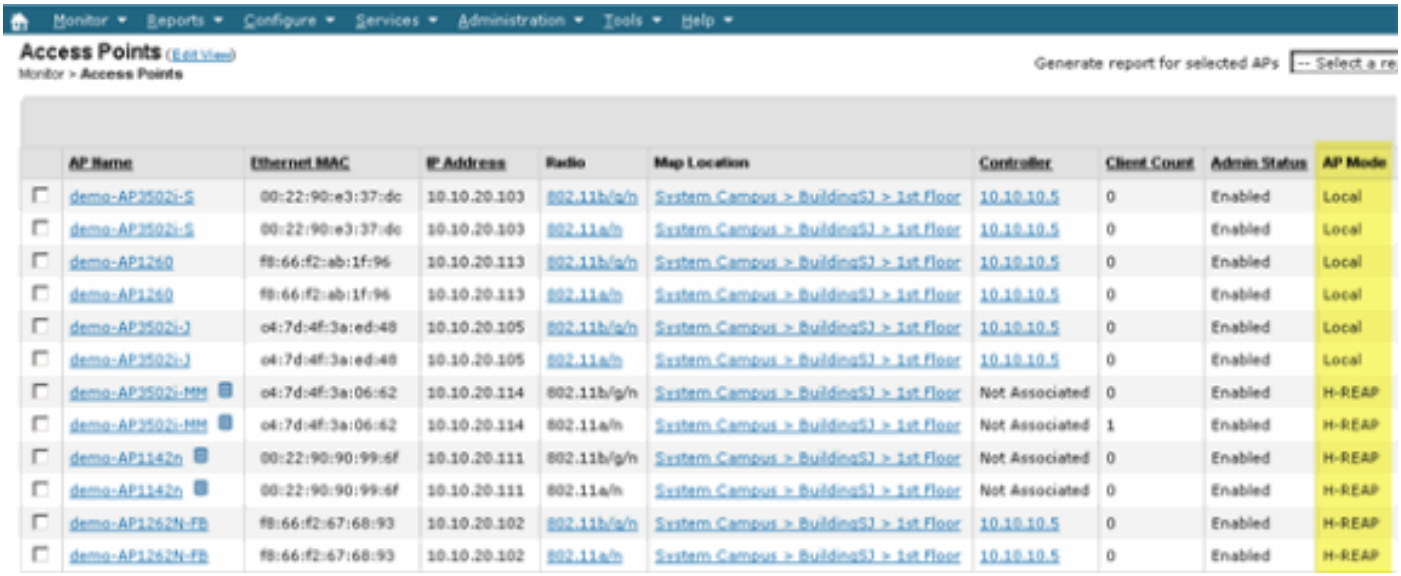
- AIR-LM-WIPS-xx - Licenza Cisco ELM wIPS
- AIR-WIPS-AP-xx - Licenza Cisco Wireless WIPS

Note aggiuntive sulle licenze ELM:

- Se gli SKU delle licenze wIPS MM AP sono già installati, è possibile utilizzare tali licenze anche per gli access point ELM.
- Le licenze wIPS e le licenze ELM concorrono a definire i limiti delle licenze di piattaforma per il motore wIPS; 2000 AP su 3310 e 3000 AP su 335x, rispettivamente.
- La licenza di valutazione comprenderà 10 punti di accesso per i servizi senza filo e 10 per i servizi di ELM per un periodo massimo di 60 giorni. Prima di ELM, la licenza di valutazione consentiva fino a 20 punti di accesso wIPS MM. È necessario soddisfare i requisiti minimi delle versioni software che supportano ELM.

Configurazione di ELM con WCS

Figura 5 - Utilizzo di Sistema colori Windows per la configurazione di ELM

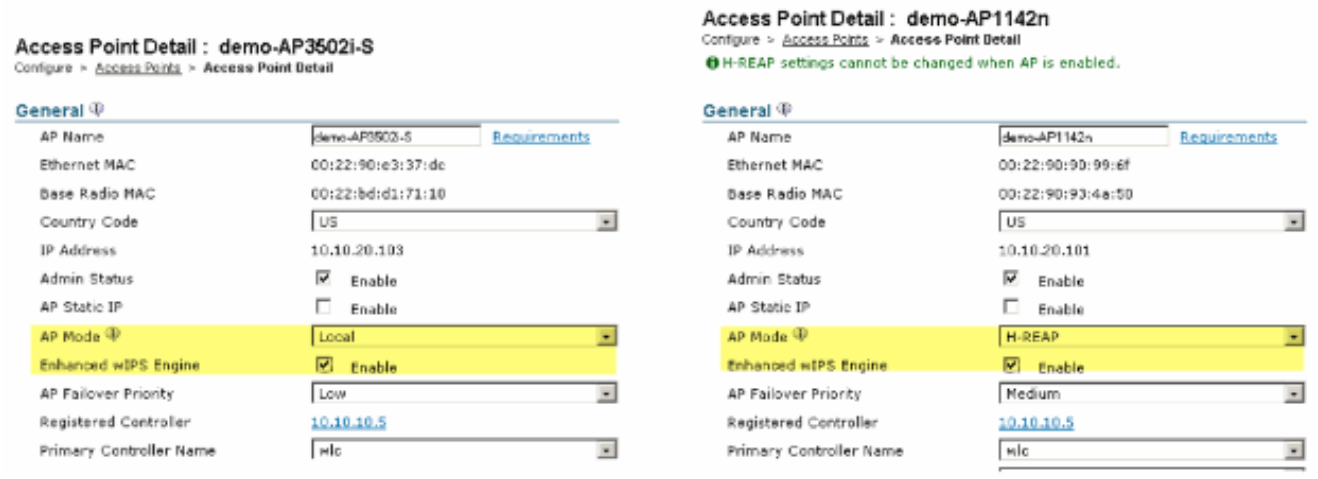


1. Da WCS, disabilitare le radio 802.11b/g e 802.11a dell'access point prima di abilitare "Enhanced wIPS Engine".

   Nota: tutti i client associati verranno disconnessi e non verranno collegati fino a quando le radio non saranno abilitate.

2. Configurare un access point o utilizzare un modello di configurazione WCS per più access point lightweight. Vedere la Figura 6.

   Figura 6 - Attivazione della modalità secondaria Enhanced wIPS Engine (ELM)



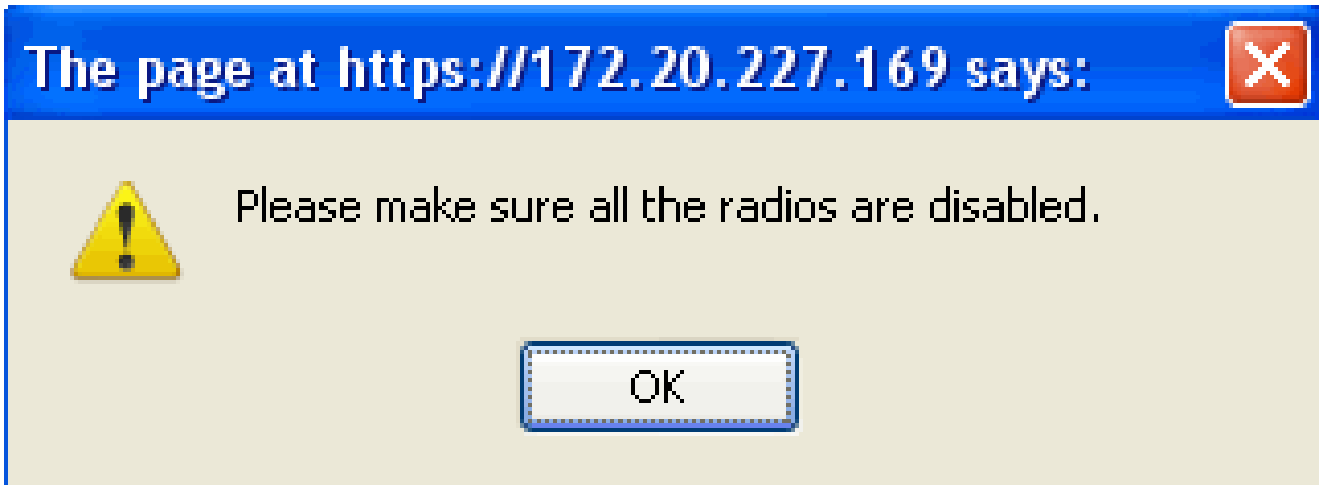
3. Scegliere Enhanced wIPS Engine, quindi fare clic su Salva.

    a. L'attivazione di Enhanced wIPS Engine non comporta il riavvio dell'access point.

    b. H-REAP è supportato; abilitare la stessa procedura utilizzata per l'access point in modalità locale.

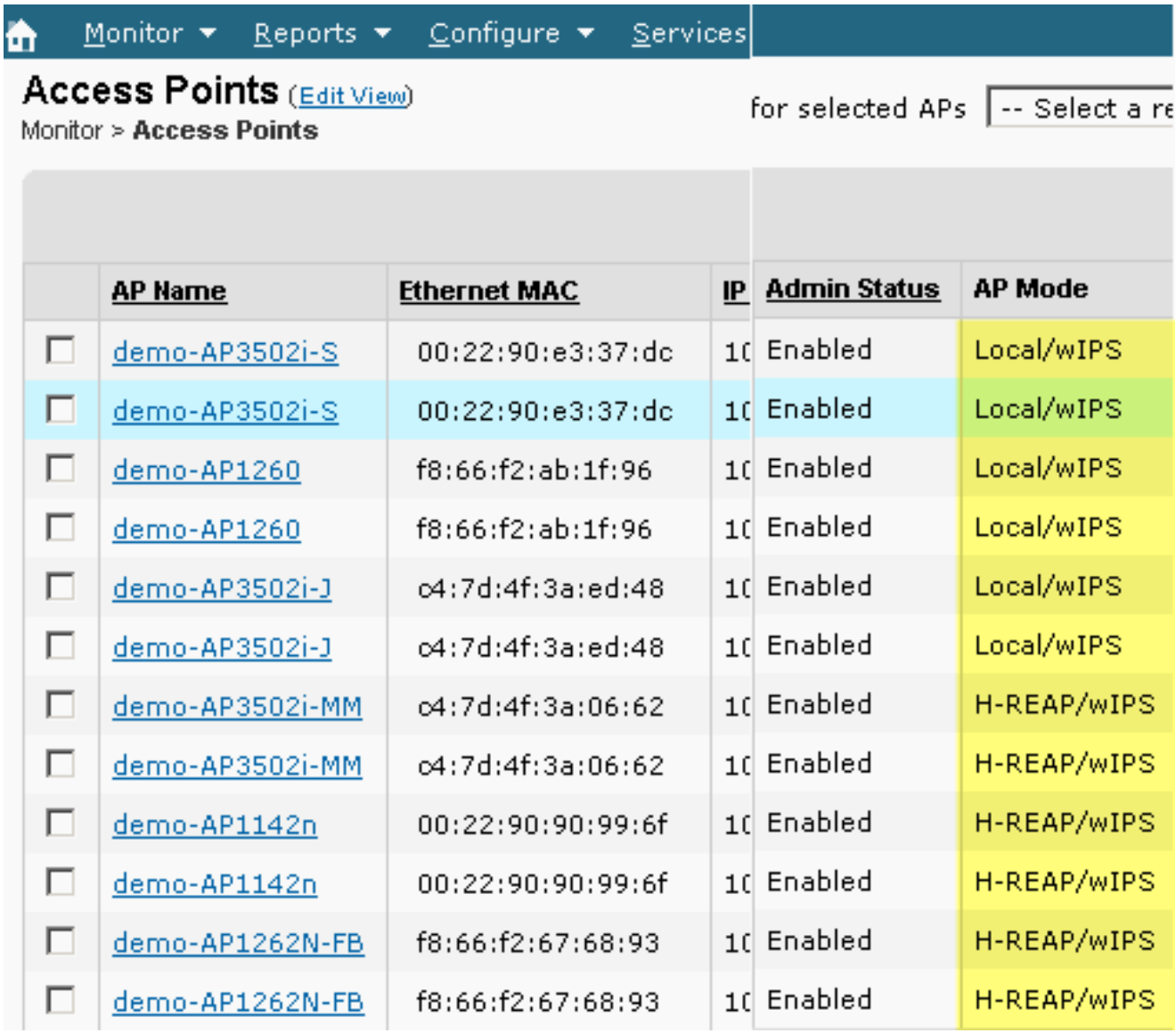
    Nota: se una delle radio di questo access point è abilitata, WCS ignorerà la configurazione e genererà l'errore nella Figura 7.

    Figura 7 - Promemoria WCS per la disattivazione delle radio AP prima dell'attivazione di ELM



4. La corretta configurazione può essere verificata osservando la modifica nella modalità AP da "Local or H-REAP" a Local/wIPS o H-REAP/wIPS. Vedere la Figura 8.

    Figura 8 - Modalità di visualizzazione WCS per includere wIPS con Local e/o H-REAP

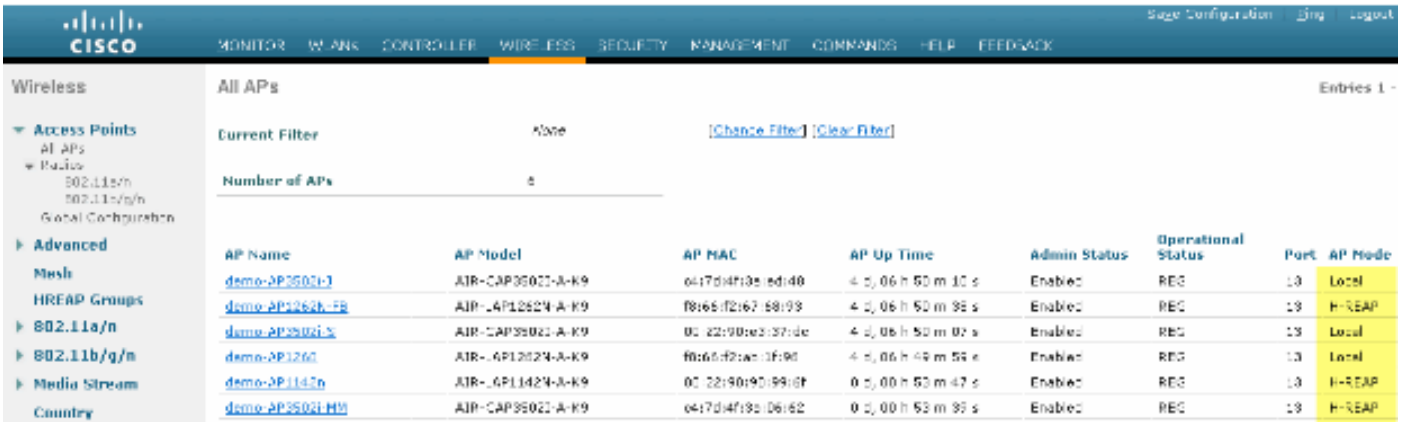


5. Abilitare le radio che sono state disabilitate al punto 1.
6. Creare il profilo wIPS e spingerlo sul controller per completare la configurazione.

   Nota: per informazioni complete sulla configurazione di IPSw, consultare la Guida alla distribuzione di IPSw adattivi Cisco.

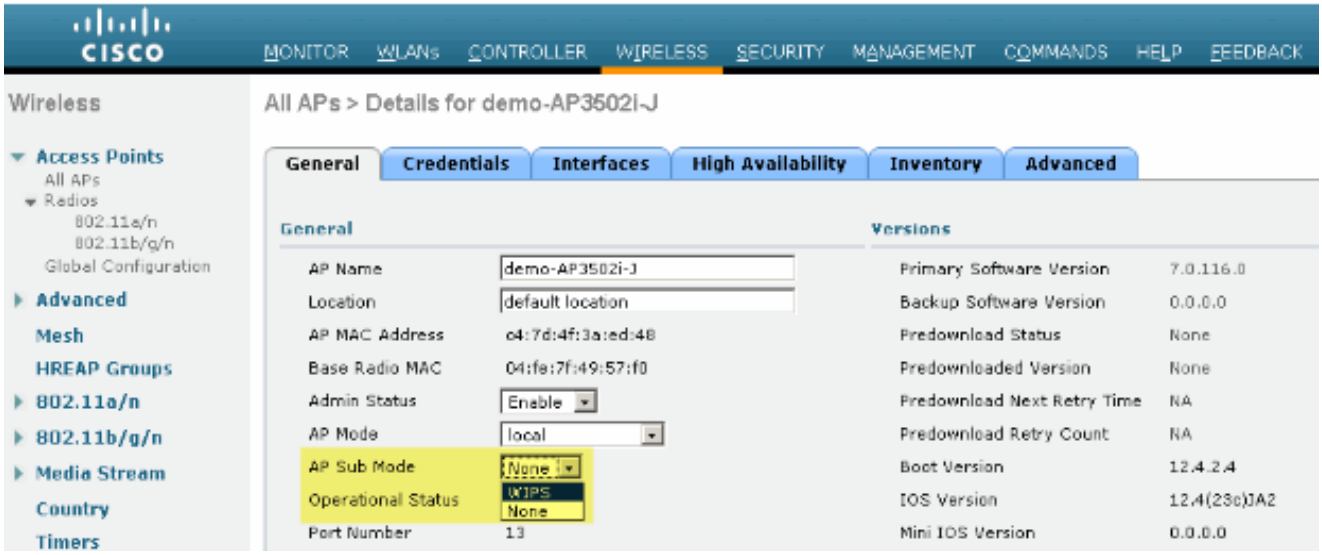
Configurazione da WLC

Figura 9 - Configurazione di ELM con WLC



1. Scegliere un access point dalla scheda Wireless.

   Figura 10 - Cambio della modalità secondaria dell'access point in Includi ELM wIPS



2. Dal menu a discesa AP Sub Mode (Modalità secondaria AP), scegliere wIPS (Figura 10).

3. Applicare e salvare la configurazione.

Nota: per il corretto funzionamento della funzionalità ELM, con le licenze wIPS sono richiesti MSE e WCS. La modifica della modalità secondaria dell'access point da solo da WLC non abiliterà ELM.

Attacchi rilevati in ELM

Tabella 1 - Matrice di supporto per le firme wIPS

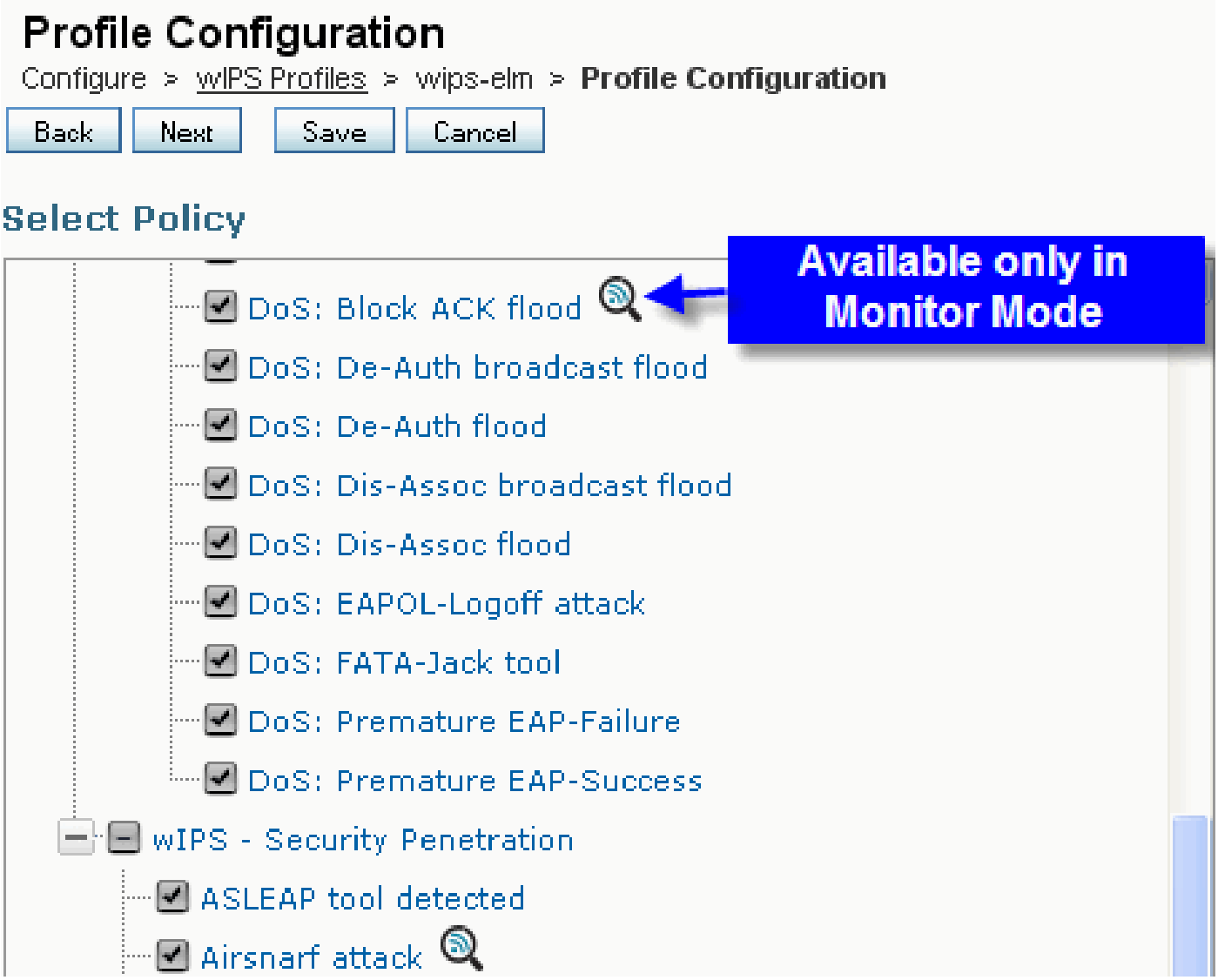
Attacchi rilevati	OLMO	MM
Attacco DoS contro AP		
Association Flood	Y	Y
Overflow della tabella di associazione	Y	Y
Authentication Flood	Y	Y

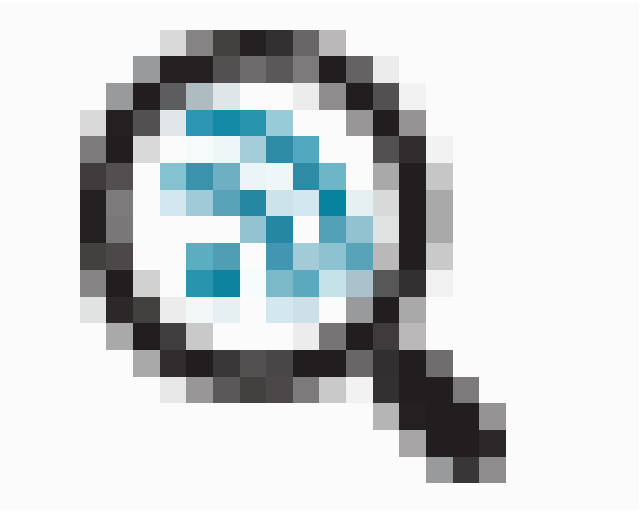
Attacco EAPOL-Start	Y	Y
Inondazione PS-Poll	Y	Y
Inondazione richiesta di sonda	N	Y
Associazione non autenticata	Y	Y
Attacco DoS contro l'infrastruttura		
Inondazione CTS	N	Y
Utilizzo della Queensland University of Technology	N	Y
Instabilità RF	Y	Y
Inondazione RTS	N	Y
Attacco vettore virtuale	N	Y
Attacco DoS contro la stazione		
Attacco di autenticazione non riuscita	Y	Y
Blocca flusso ACK	N	Y
De-Auth broadcast flood	Y	Y
Inondazione della De-Auth	Y	Y
Dis-Assoc broadcast flood	Y	Y
Alluvione Dis-Assoc	Y	Y
Attacco EAPOL-Logoff	Y	Y
FATA-Jack, strumento	Y	Y
Errore EAP prematuro	Y	Y
EAP prematuro	Y	Y
Attacchi di penetrazione della sicurezza		
Rilevato strumento ASLEAP	Y	Y
Attacco a Airsnarf	N	Y
Attacco ChopChop	Y	Y
Attacco Day-Zero da parte di un'anomalia di sicurezza della WLAN	N	Y
Attacco Day-Zero per anomalia di sicurezza del dispositivo	N	Y
Probe del dispositivo per access point	Y	Y
Attacco dizionario ai metodi EAP	Y	Y
Attacco EAP all'autenticazione 802.1x	Y	Y
Rilevati falsi access point	Y	Y

È stato rilevato un server DHCP falso	N	Y
Rilevato strumento di interruzione FAST WEP	Y	Y
Attacco di frammentazione	Y	Y
Rilevato punto di accesso Honeypot	Y	Y
Rilevato strumento Hotspot	N	Y
Frame di trasmissione non corretti	N	Y
Rilevati pacchetti 802.11 non validi	Y	Y
L'uomo nel mezzo dell'attacco	Y	Y
Rilevato Netstumbler	Y	Y
Rilevata vittima Netstumbler	Y	Y
Rilevata violazione PSPF	Y	Y
Rilevato punto di accesso soft o host	Y	Y
Rilevato indirizzo MAC oggetto di spoofing	Y	Y
Rilevato traffico sospetto fuori orario	Y	Y
Associazione non autorizzata per elenco fornitori	N	Y
Rilevata associazione non autorizzata	Y	Y
Rilevato Wellener	Y	Y

Nota: l'aggiunta di CleanAir consente anche il rilevamento di attacchi non 802.11.

Figura 11 - Visualizzazione profilo WCS wIPS





Nella Figura 11, configurare il profilo wIPS da WCS, l'icona indica che l'attacco sarà rilevato solo quando l'access point è in millimetri, mentre la soluzione migliore è in ELM.

Risoluzione dei problemi relativi a ELM

Controllare quanto segue:

- Verificare che NTP sia configurato.
- Assicurarsi che l'ora MSE sia impostata su UTC.
- Se il gruppo di dispositivi non funziona, sovrapporre SSID profilo con Any. Riavviare il punto di accesso.
- Verificare che la licenza sia configurata (attualmente i punti di accesso ELM utilizzano licenze KAM)
- Se i profili wIPS vengono modificati troppo spesso, sincronizzare di nuovo MSE-Controller. Verificare che il profilo sia attivo sul WLC.
- Verificare che il WLC faccia parte di MSE utilizzando MSE CLI:

    1. SSH o telnet per il server MSE.
    2. Execute/opt/mse/wips/bin/wips_cli - Questa console può essere utilizzata per accedere ai seguenti comandi e raccogliere informazioni relative allo stato del sistema WIPS adattivo.
    3. show wlc all: problema nella console wIPS. Questo comando è usato per verificare i controller che stanno comunicando attivamente con il servizio wIPS su MSE. Vedere la Figura 12.

       Figura 12 - Verifica del WLC attivo dall'interfaccia CLI di MSE con i servizi WIPS di MSE

       <#root>

       ```
       wIPS>

       show wlc all


       WLC MAC              Profile             Profile
       Status                  IP
       Onx Status Status
       ------------------------------------------------
       ------------------------------------------------
       ----
       00:21:55:06:F2:80    WCS-Default         Policy
       active on controller     172.20.226.197
       Active
       ```

- Verificare che gli allarmi vengano rilevati su MSE utilizzando le CLI di MSE.
    - show alarm list - Problema all'interno della console wIPS. Questo comando viene utilizzato per elencare gli allarmi attualmente contenuti nel database del servizio wIPS. Il campo chiave è la chiave hash univoca assegnata all'allarme specifico. Il campo Tipo indica il tipo di avviso. Questo grafico nella Figura 13 mostra un elenco di ID e

descrizioni degli allarmi:

Figura 13 - Comando MSE CLI show alarm list

```
<#root>

wIPS>

show alarm list


Key         Type  Src MAC
LastTime              Active          First Time
-----------------------------------------------
-----------------------------------------
89          89    00:00:00:00:00:00     2008/09/04
18:19:26  2008/09/07 02:16:58   1
65631       95    00:00:00:00:00:00     2008/09/04
17:18:31  2008/09/04 17:18:31   0
1989183     99    00:1A:1E:80:5C:40     2008/09/04
18:19:44  2008/09/04 18:19:44   0
```

I campi Prima ora e Ultima ora indicano i timestamp quando l'allarme è stato rilevato; questi sono memorizzati in ora UTC. Il campo Attivo viene evidenziato se l'allarme viene attualmente rilevato.

- Cancellare il database MSE.
  - Se si verifica una situazione in cui il database MSE è danneggiato o non sono disponibili altri metodi per la risoluzione dei problemi, è consigliabile cancellare il database e ricominciare.

Figura 14 - Comando servizi MSE

```
1. /etc/init.d/msed stop
2. Remove the database using the command 'rm
/opt/mse/locserver/db/linux/server-eng.db'
3. /etc/init.d/msed start
```

Informazioni correlate

- Guida alla configurazione di Cisco Wireless LAN Controller, versione 7.0.116.0
- Guida alla configurazione di Cisco Wireless Control System, versione 7.0.172.0
- 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).