Come è possibile rendere manualmente disponibile una pagina Web in Cisco Web Security Appliance (versione 5.2.0 e successive) in modo da ignorare le scansioni WBRS, WebRoot o McAfee?

Sommario

Domanda:

Come è possibile rendere manualmente disponibile una pagina Web in Cisco Web Security Appliance (versione 5.2.0 e successive) in modo da ignorare le scansioni WBRS, WebRoot o McAfee?

Sintomi:

L'utente sta tentando di accedere a un sito legittimo, ma è bloccato a causa di un punteggio WBRS basso (infezione da virus del server Web, spam inviato tramite l'IP del server Web e così via) o a causa di uno dei motori antimalware che attivano su quella pagina.

Se l'utente è bloccato a causa di un livello WBRS basso, viene visualizzato un messaggio di blocco MALWARE_GENERAL. Nei log degli accessi viene visualizzato un WBRS al di sotto della soglia di blocco (il valore predefinito è -6,0).

Per una soluzione permanente, contattare Cisco TAC in modo che la pagina possa essere rivista per modificare il WBRS o per segnalare falsi positivi ai fornitori di antivirus e antimalware.

Èinoltre possibile contattare Cisco TAC per raccogliere ulteriori informazioni sui motivi per cui il sito è bloccato, in modo da poter informare il contatto tecnico o l'amministratore del sito e adottare le misure necessarie.
Quando si contatta Cisco TAC, accertarsi di fornire i codici di blocco e le righe del log degli accessi pertinenti

Per ignorare WBRS:

4. Fare clic sul collegamento nella colonna "Web Reputation and Anti-Malware Filtering" (Reputazione Web e filtro antimalware) del criterio di accesso Web appena creato (dovrebbe essere visualizzato "criterio globale").

5. Selezionare 'Definisci reputazione Web e impostazioni personalizzate antimalware'
Nota: Se si imposta l'azione su "Allow" (Consenti) nella categoria URL, la scansione di antimalware/virus viene ignorata.

Per ignorare WBRS e l'analisi antimalware:

Nota: La disattivazione dell'analisi antimalware (Webroot e/o McAfee) potrebbe rappresentare un potenziale rischio per la sicurezza. Questa operazione deve essere eseguita solo per i siti attendibili in cui non è presente malware.