¿Cómo hace la lista blanca I manualmente una página web en el dispositivo de seguridad de la red de Cisco (que ejecuta 5.2.0 y arriba) para desviar analizar WBRS, de Webroot o del McAfee?

Contenido

Pregunta:

¿Cómo hace la lista blanca I manualmente una página web en el dispositivo de seguridad de la red de Cisco (que ejecuta 5.2.0 y arriba) para desviar analizar WBRS, de Webroot o del McAfee?

Síntomas:

El usuario está intentando acceder un sitio legítimo, pero está siendo debido a una calificación baja WBRS (infección del virus del web server, del Spam siendo enviado a través del IP etc. del web server) o bloqueado debido a uno de los motores antis-malware que accionan en esa página.

Si el usuario es bloqueado debido a un WBRS bajo el usuario está viendo un mensaje del bloque MALWARE_GENERAL. La demostración de los accesslogs un WBRS debajo del umbral de bloqueo (el valor por defecto es -6.0).

Para una solución permanente, entre en contacto por favor el TAC de Cisco para poder revisar la página para ajustar el WBRS o señalar los falsos positivos al contra virus y a los vendedores antis-malware.

Usted puede también entrar en contacto el TAC de Cisco para recopilar más información sobre porqué se bloquea el sitio para poder notificar y pueda tomar el contacto o el administrador técnico del sitio web los pasos necesarios.
Aseegurese proporcionar los códigos de bloqueo y las líneas relevantes del accesslog al entrar en contacto el TAC de Cisco

Para desviar WBRS:

4. Haga clic en el link en la “reputación de la red y” la columna de filtración anti-Malware de su directiva creada recientemente del Acceso Web (debe leer la “política global” hasta ahora).
5. Selecto “defina la reputación Web y las configuraciones personalizadas antis-Malware

Nota: Si usted fija la acción “permita” en la categoría URL, esto daría lugar a desviar la exploración anti-Malware/del virus.

Para desviar WBRS y la exploración anti-malware:

Nota: Inhabilitar la exploración anti-malware (Webroot y/o McAfee) podría ser un riesgo de seguridad potencial. Esto se debe hacer solamente para los sitios que se pueden confiar en para no contener el malware.