WEBROOT®
opentext™ Security Solutions

SecureAnywhere®
Protezione DNS
Guida introduttiva

Sommario

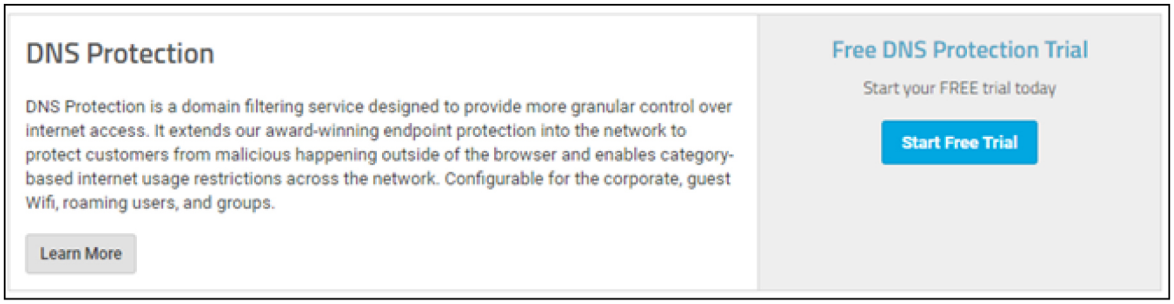
Panoramica

Questo documento è progettato come guida introduttiva per l'installazione e l'utilizzo di Protezione Webroot SecureAnywhere DNS. È concepito come risorsa tecnica per gli amministratori di rete e per coloro che configureranno la Protezione DNS. Per informazioni più dettagliate, consultare la guida dell'amministratore di Protezione Webroot SecureAnywhere DNS.

Protezione DNS dispone di due componenti: una soluzione basata su agenti che consente un controllo granulare di DNS indipendente dalla rete e una soluzione basata sulla rete progettata per proteggere l'intera rete. Anche se è possibile eseguire ogni componente singolarmente, essi sono progettati per integrarsi a vicenda e lavorare in parallelo per proteggere in modo completo la rete e i sistemi collegati.

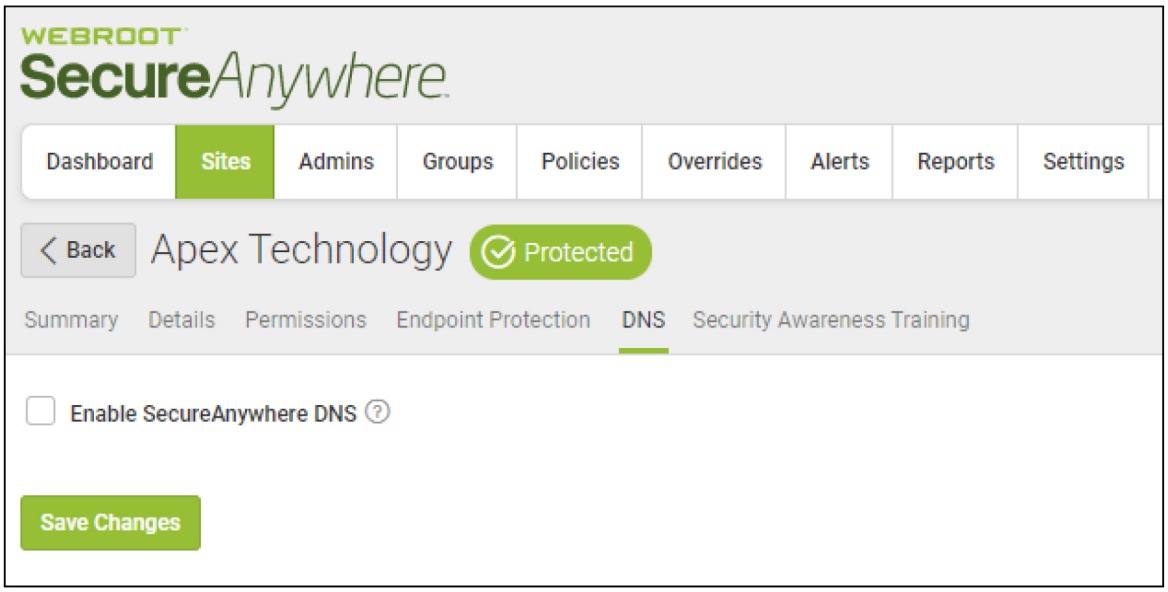
Passaggio 1: avviare la versione di prova della Protezione DNS

Il primo passaggio consiste nell'attivare la Protezione DNS per la console. Questa operazione viene eseguita nella scheda Impostazioni. Qui è possibile avviare una versione di prova facendo clic sul pulsante **Avvia la versione di prova**. Una volta che la versione di prova è attiva o è stata acquistata, è possibile utilizzare la scheda Impostazioni per conoscere i giorni rimanenti della versione di prova o lo stato dell'abbonamento.



Passaggio 2: abilitare la Protezione DNS

Protezione DNS viene abilitata dal sito. Per poterla attivare, fare clic sul pulsante **Gestisci** accanto al sito corrispondente, quindi fare clic sulla scheda **DNS**.



La Lista bypass agenti (Intranet) è progettata per contenere Active Directory. Se si eseguirà l'agente di Protezione DNS in un ambiente Active Directory, assicurarsi di aggiungere il dominio AD alla Lista bypass agenti, sia specifica sia con caratteri jolly.

Passaggio 3: installare l'agente

Per poter installare l'agente di Protezione DNS, è necessario soddisfare tre condizioni. Se, in qualsiasi momento, questi criteri non vengono soddisfatti, l'agente DNS verrà disinstallato.

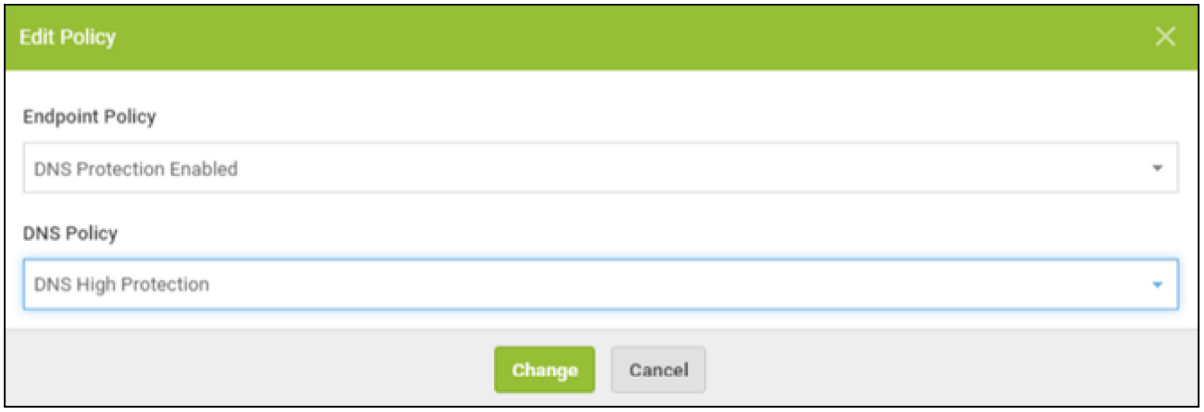
- Nella console deve essere attiva una versione di prova o un abbonamento per la Protezione DNS. Questa condizione è illustrata nel passaggio 1.
- Nel sito deve essere attiva Protezione DNS. Questa condizione è illustrata nel passaggio 2.
- Agli endpoint desiderati deve essere assegnato un criterio con l'opzione Installa protezione DNS attivata. Questa condizione viene illustrata di seguito.

Assegnazione di un criterio con Protezione DNS attivata

È possibile creare una copia dell'attuale criterio workstation esistente, quindi modificare l'impostazione o, in alternativa, utilizzare l'opzione DNS abilitato raccomandato fornita.

Per assegnarlo a un sistema, selezionare la scheda **Gruppi**, selezionare il sito appena abilitato, quindi scegliere i sistemi che si desidera installare.

Successivamente, fare clic sul pulsante **Modifica criterio** e specificare il criterio endpoint con DNS abilitato, nonché il criterio DNS. Una volta fatto clic sul pulsante **Cambia**, al successivo controllo con la console da parte del sistema, l'agente DNS verrà installato e inizierà a filtrare le richieste DNS.



Passaggio 4: proteggere la rete

L'abilitazione della Protezione DNS per la rete consentirà di filtrare le richieste DNS per ogni dispositivo nella rete, anche se non eseguono l'agente DNS; in questo modo sarà possibile proteggere computer portatili, stampanti e persino dispositivi IOT ospiti.

Sono disponibili due passaggi:

- Registrare l'IP WAN
- Configurare server d'inoltro DNS

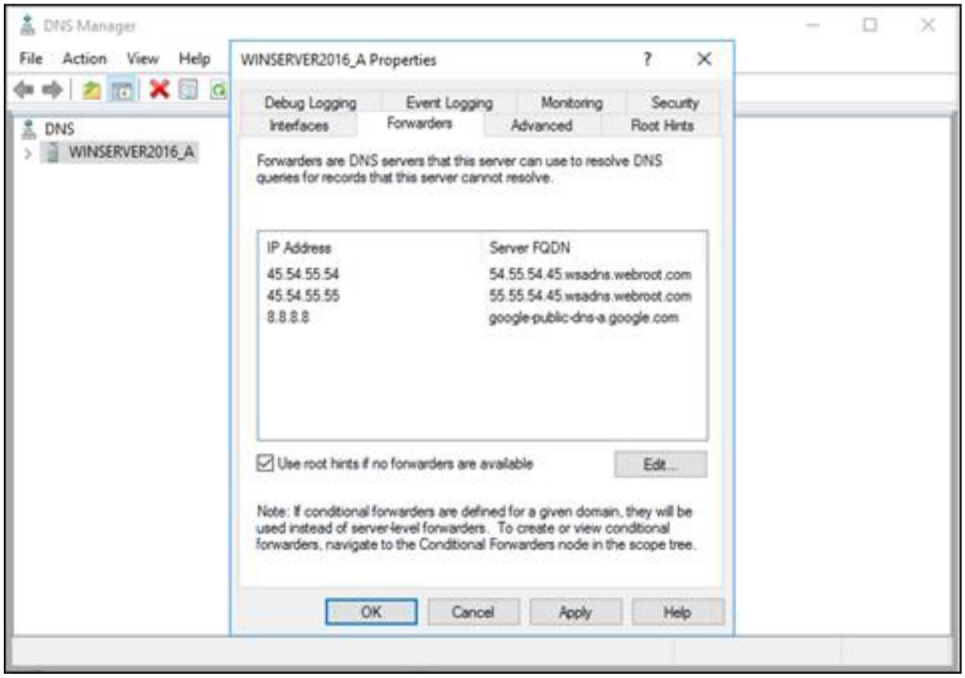
Registrare l'IP WAN

- In Impostazioni di rete nella scheda DNS selezionare **Aggiungi riga**.
- Inserire l'indirizzo IP WAN e selezionare un criterio DNS.

Configurare server d'inoltro DNS

Questa impostazione deve essere gestita nel router o, in caso di server Windows, nei server d'inoltro DNS.

- DNS1: 45.54.55.54.
- DNS2: 45.54.55.55.
- DNS3: failover di server DNS (fornito da ISP).

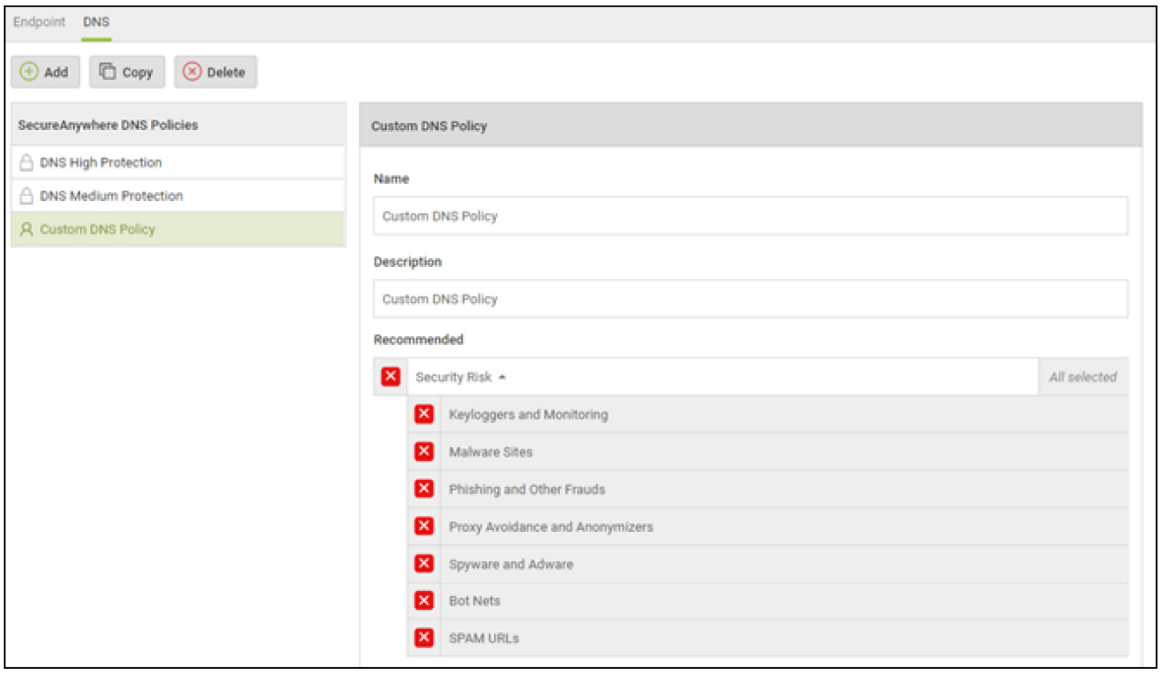


Passaggio 5: personalizzare le impostazioni

- Creare criteri
- Filtro eccezioni
- Blocco pagina

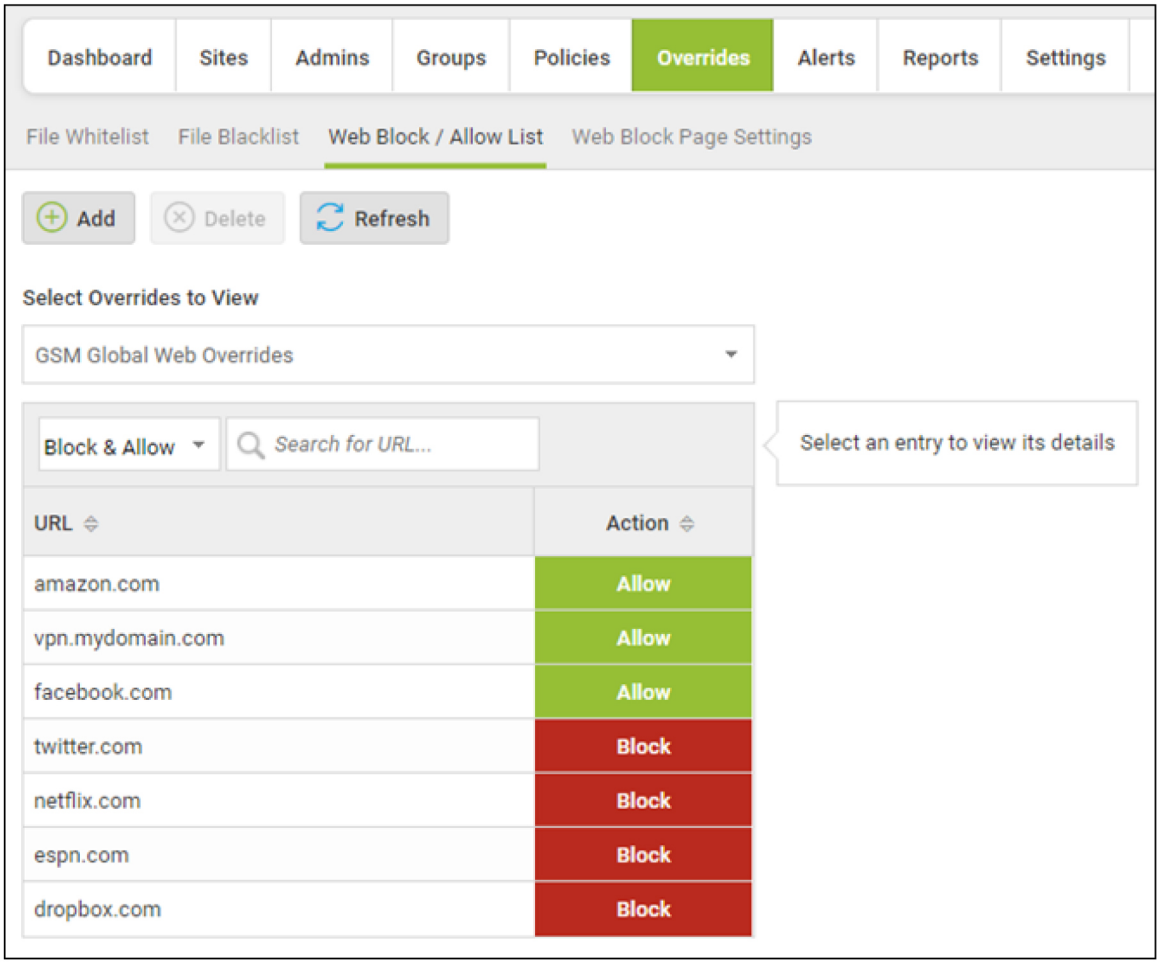
Creare criteri

I criteri personalizzati possono essere definiti nella scheda Criteri selezionando DNS. Per creare un nuovo criterio, fare clic sul pulsante **Aggiungi**.



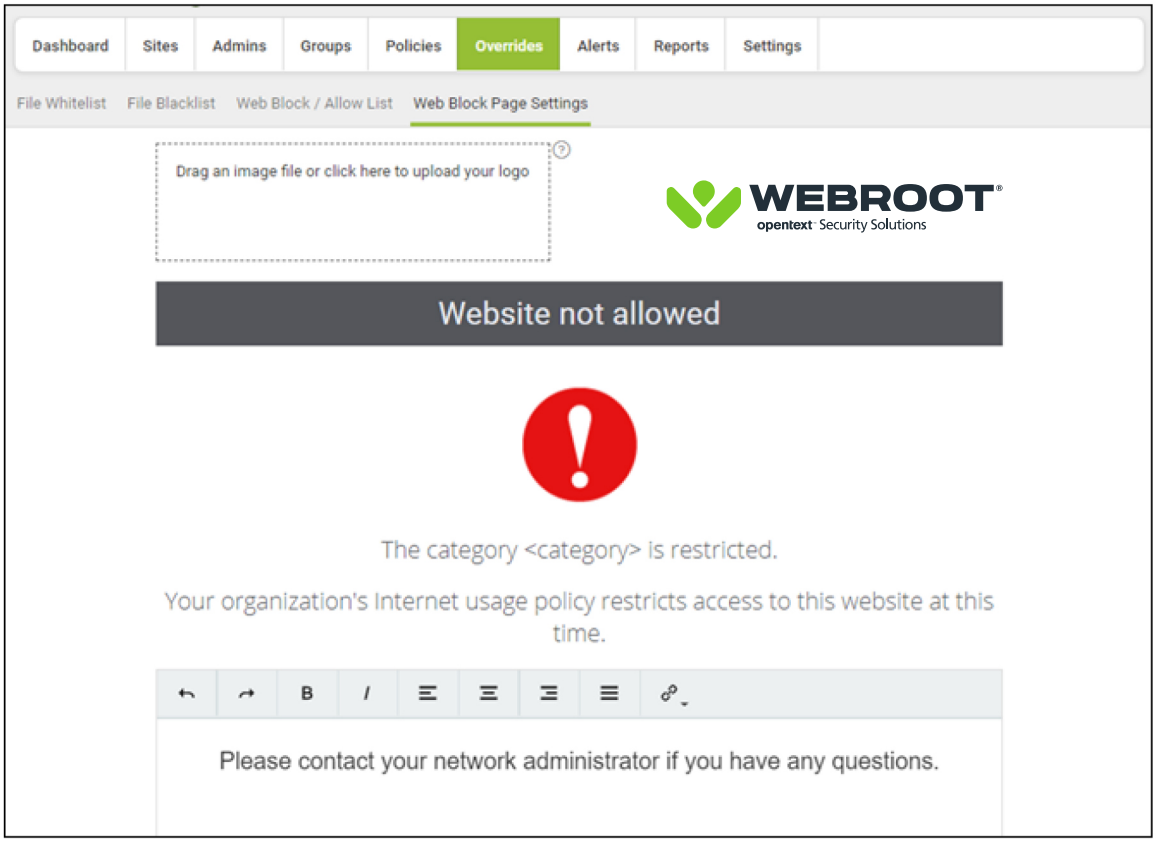
Filtro eccezioni

Per aggiungere eccezioni ai criteri, selezionare Esegui override, Elenco blocchi/permessi Web. Qui è possibile aggiungere domini e sottodomini per consentire eccezioni specifiche. Tali eccezioni possono essere applicate a tutti i siti o ai singoli siti.



Blocco pagina

Il messaggio fornito all'utente quando un sito richiesto viene bloccato può essere definito nella scheda Esegui override, Impostazioni blocco pagina Web.



Conclusioni

I passaggi forniti consentono la configurazione iniziale di Protezione DNS. Tutte le richieste DNS per la rete devono essere protette dai server di protezione DNS e tutti i sistemi che eseguono l'agente devono essere protetti indipendentemente dalla rete a cui sono collegati.

Per ulteriori informazioni, tra cui strategie di installazione aggiuntive, report, test e risoluzione dei problemi, considerazioni su Active Directory e gestione di firewall, consultare la guida dell'amministratore di Protezione Webroot SecureAnywhere DNS.

Per ulteriori informazioni sulla console Web e sulla gestione dei criteri, consultare la guida dell'amministratore di Webroot SecureAnywhere Endpoint Protection per le aziende.