#Configurazione# Come aggiungere nuove applicazioni proxy e bloccarle tramite policy

***Prodotto:** Sangfor NGAF

***Versione:** Sangfor NGAF 8.0.85

*1. Introduzione

1.1 Scenario

Oggigiorno, è importante avere il controllo del traffico che I client effettuano (compresi gli applicativi vpn non desiderati).

Alcune applicazioni usano porte comunemente conosciute per operare (per esempio Teamviewer, Skype, Hide.me e così via).

Se si vuole bloccare queste applicazioni, è impossibile applicare una regola firewall che blocchi una specifica porta o protocollo senza causare problemi di rete agli utenti.

Una soluzione a questo scenario è quella di creare una applicazione proxy per permettere al firewall Sangfor NGAF di ispezionare il traffico e bloccare il traffico non desiderato al fine di ottenere il blocco di specifici applicativi su client specifici nella rete.

1.2 Requisiti

1. La rete dell'utente deve avere Sangfor NGAF come firewall.

3. Occorre avere dei client ed un applicativo da bloccare

*2. Configurazione

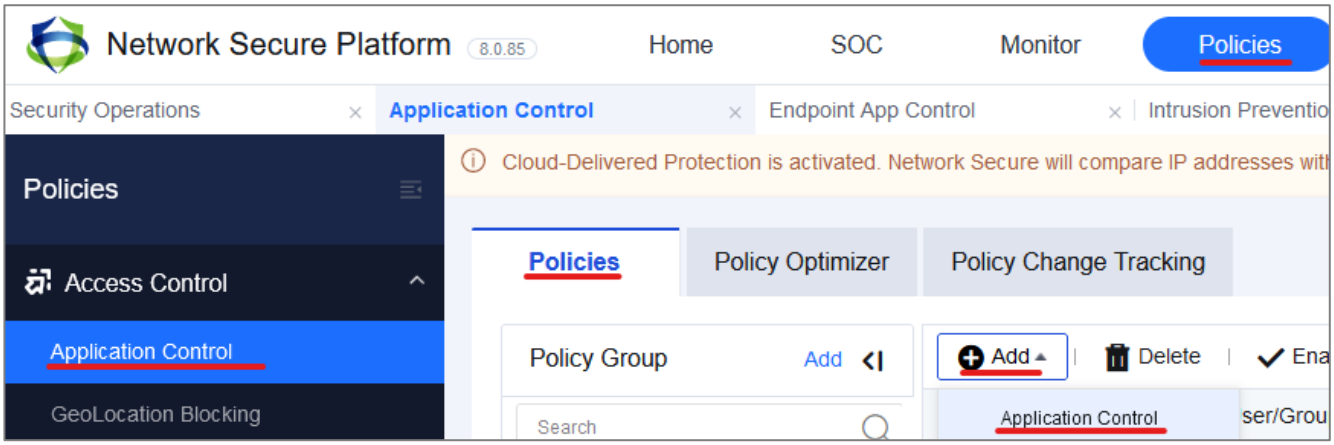
In questa guida vedremo come bloccare il software vpn hide.me per dei specifici client aventi ip statico.

2.1 Bloccare l'applicativo sui client con una policy su NGAF

Nell'interfaccia web di NGAF , dovremo creare una policy di controllo applicazioni per filtrare i pacchetti che vengono generati dall'applicativo hide.me.

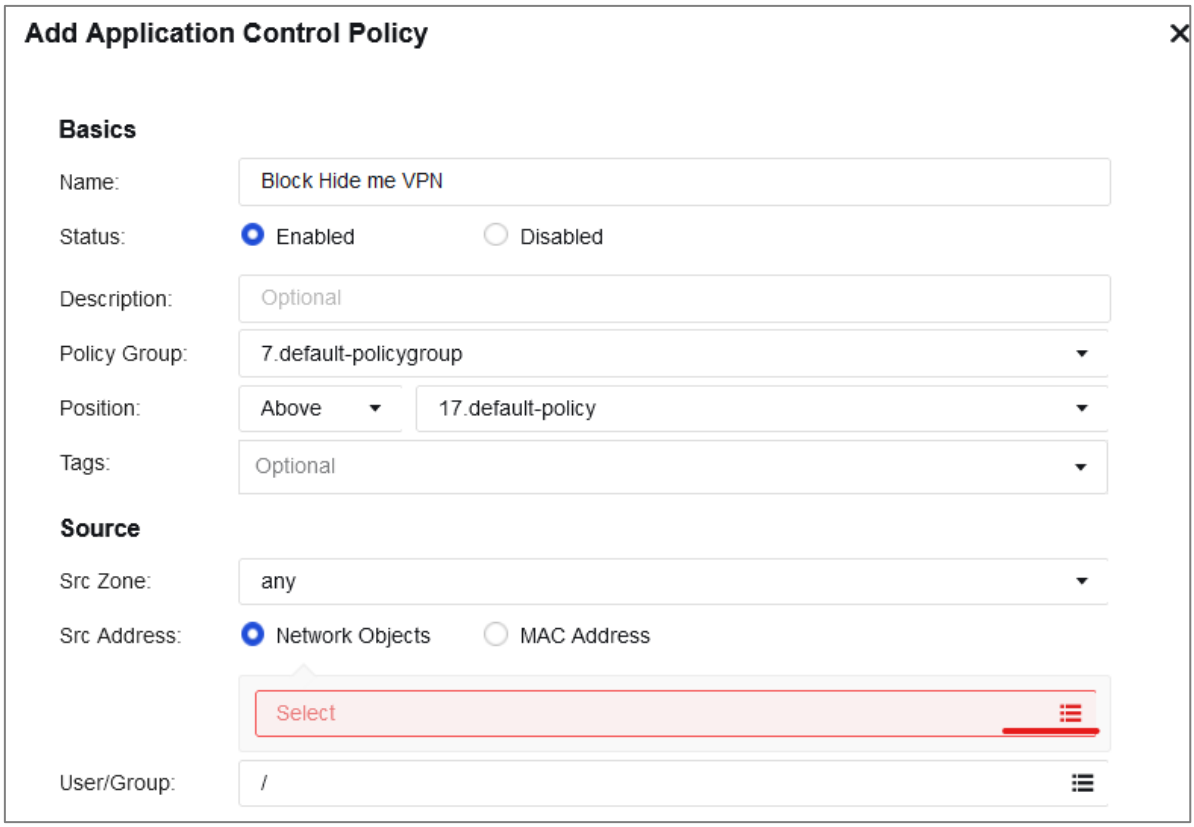
Per ottenere questo, bisogna recarsi sulla seguente sezione dell'interfaccia web di NGAF e creare una nuova Application Control policy:

Policies > Application Control > Policies > Add

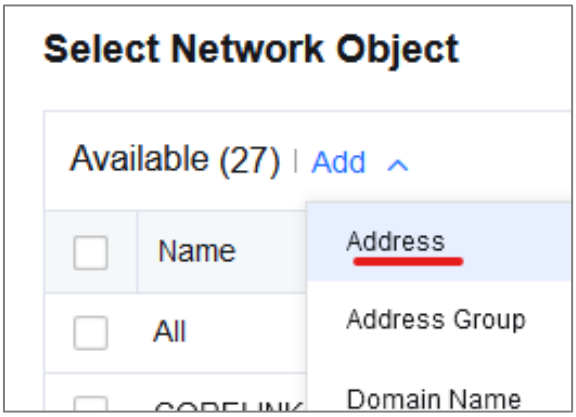


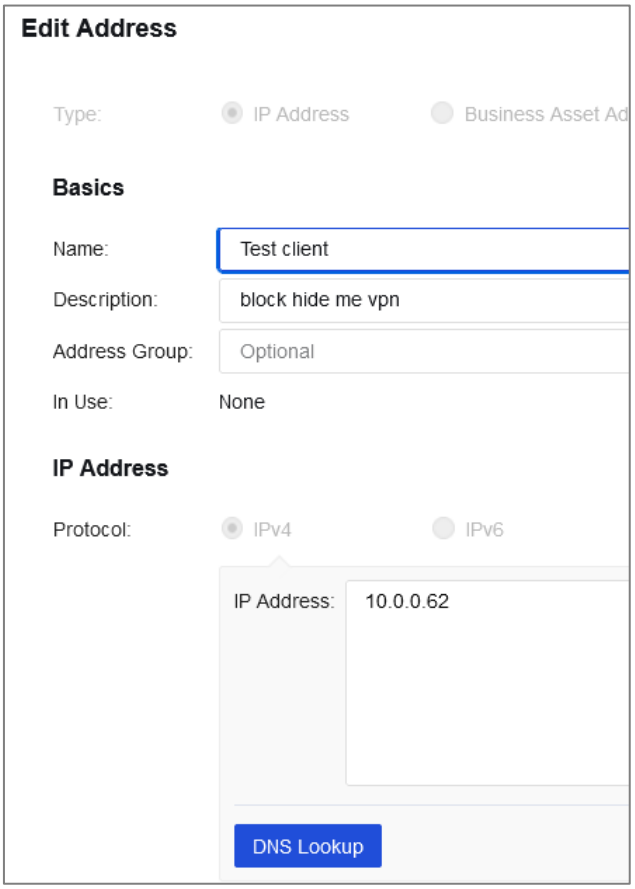
Nella nuova policy, si deve scegliere una posizione per la policy al fine di assicurarsi che funzioni senza interferire con altre policy esistenti.

Durante la creazione della policy applicativa, è possibile creare degli oggetti di rete al fine di mappare i client cui si vuole bloccare l'applicativo hide.me



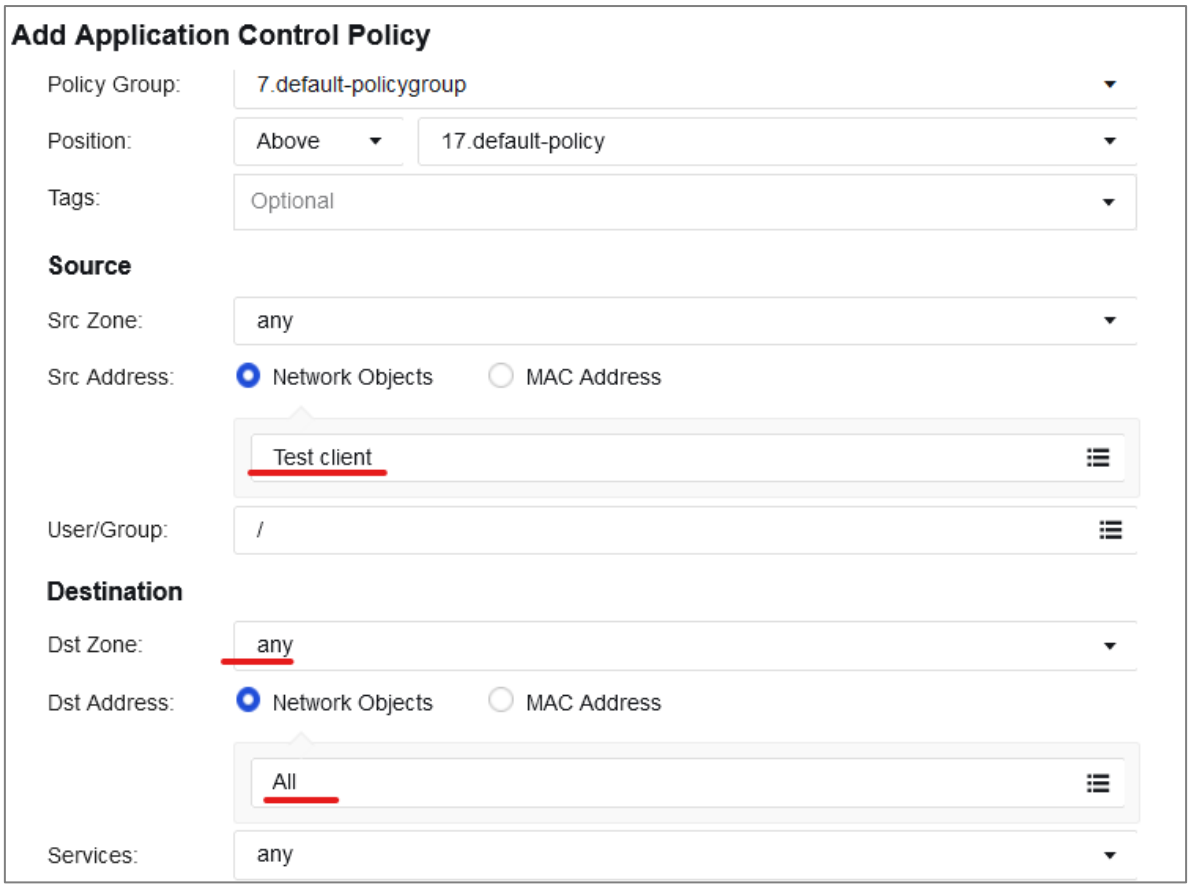
In questa guida, ho aggiunto un singolo ip di un specifico client:



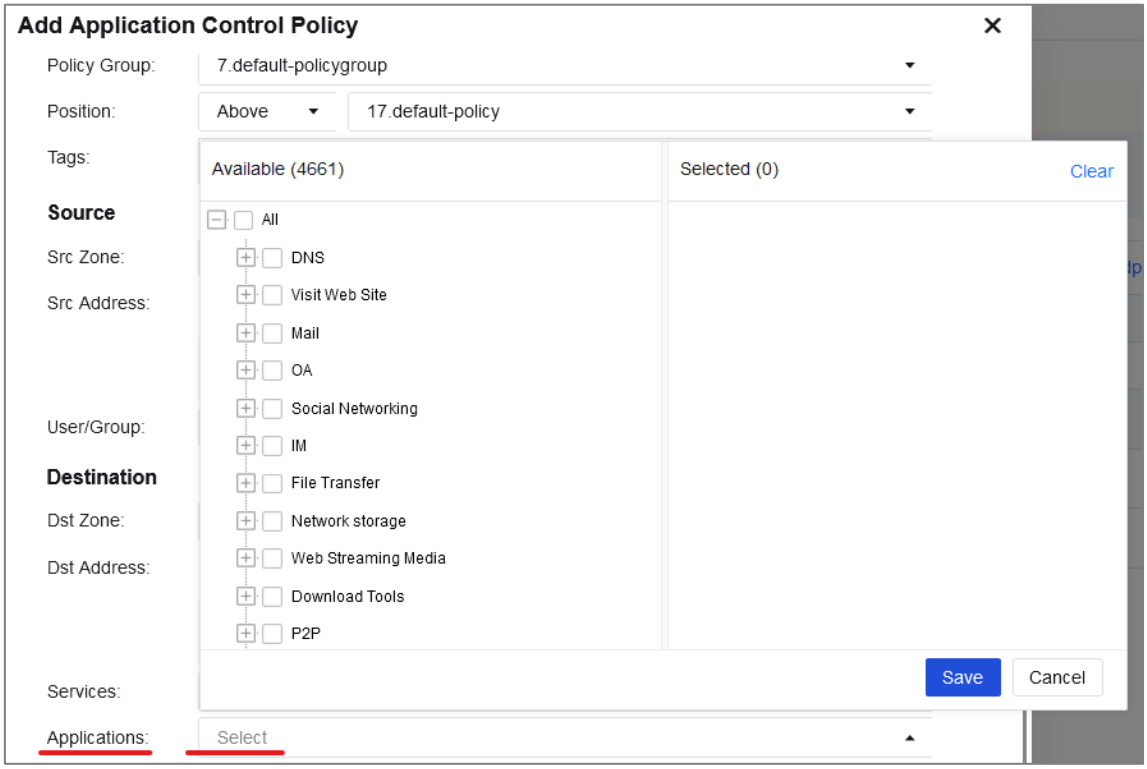


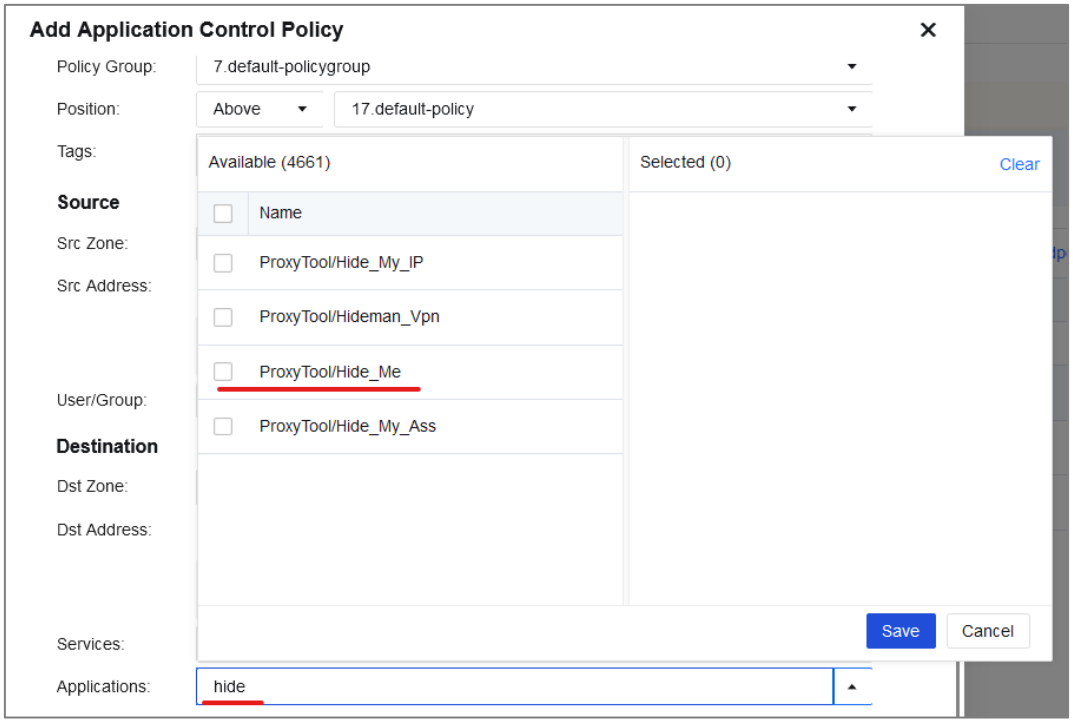
Dopo aver aggiunto quest'informazione, è possibile salvare e selezionare questo oggetto di rete sulla policy applicativa di controllo.

Ritornando nella procedura di creazione della policy di controllo applicativa, possiamo selezionare i nuovi oggetti di rete creati inerenti i client locali ed impostare tutte le impostazioni riguardo la zona esterna di destinazione come segue:



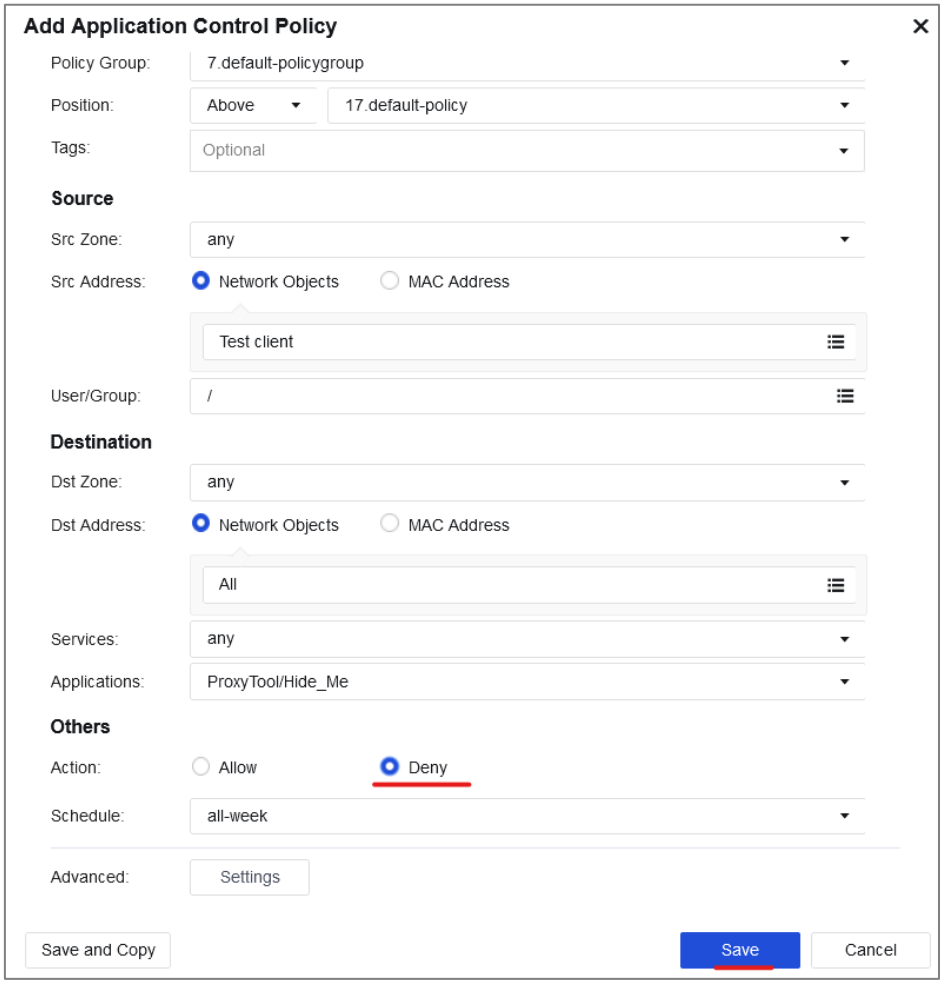
A questo punto, si deve selezionare l'applicativo hide.me da bloccare cliccando sulle opzioni applicazione ed iniziando a digitare il nome dell'applicativo



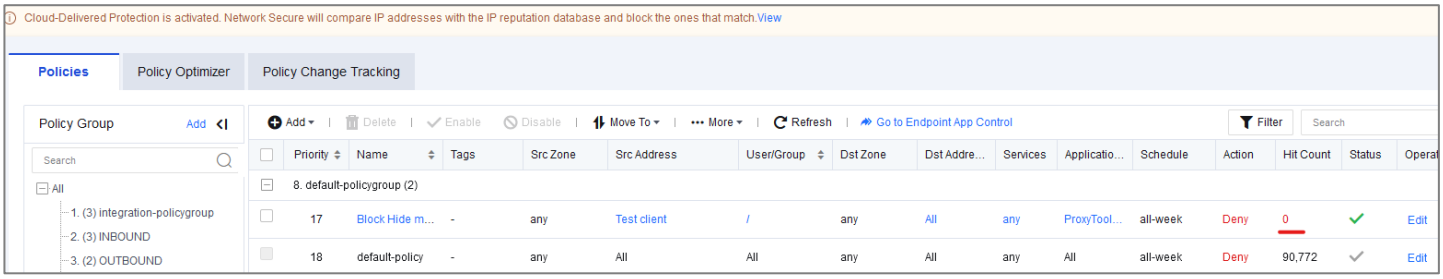


Selezionare l'applicativo e cliccare salva

Ora si deve scegliere nega come azione da intraprendere nella policy e cliccare su salva per confermare le modifiche.



Ora potete vedere se vi sono delle hit nel traffico generato dai clienti che vengono regolari dalla nuova policy



*3. Attenzione

1. Tenere a mente che se avete dei client con ip dinamico (dhcp), vi suggerisco di creare un oggetto di rete relativo ad un range di possibili ip che i client potrebbero avere.